TREND MICRO™

9.8 趨勢科技™ 行動安全防護

系統管理員手冊

（適用於安全掃瞄部署模式）

企業版攜帶型裝置全面性安全解決方案

Endpoint Security

文件編號：TSCM98145/180126

發行日期：2017 年 11 月

「趨勢科技™企業版行動安全防護」的使用者文件介紹產品的主要功能，並針對您的產品環境提供安裝指示。安裝或使用產品前，請先讀完文件。

如需如何使用產品特定功能的詳細資訊，請參閱「線上說明」和趨勢科技網站的常見問題集。

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或建議，請與我們聯絡，電子郵件信箱為：docs@trendmicro.com。

請移至以下網站評估本文件：

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

目錄

前言

第 1 章：簡介

第 2 章：開始使用行動安全防護

第 3 章：與其他 MDM 解決方案整合

第 4 章：管理行動裝置

第 8 章：更新元件

第 9 章：檢視及維護記錄

第 10 章：使用通知和報告

第 11 章：疑難排解及聯絡技術支援

索引

序言

前言

歡迎使用《趨勢科技™ 企業版行動安全防護 9.8 版管理手冊》。本手冊提供所有「行動安全防護」設定選項的詳細資訊。涵蓋的主題包括如何更新軟體以將保護效力維持在最新狀態，以期抵禦最新的安全威脅、如何設定及使用政策來支援安全目標、設定掃瞄功能、同步處理行動裝置上的政策，以及使用記錄和報告。

本前言討論以下主題：

對象

「行動安全防護」文件的適用對象為負責在企業環境中管理「行動裝置代理程式」的系統管理員，以及行動裝置使用者。

系統管理員對 Windows 系統管理作業和行動裝置政策應具備中級到進階的知識，包括：

- 安裝及設定 Windows 伺服器
- 在 Windows 伺服器上安裝軟體
- 設定及管理行動裝置
- 網路概念（如 IP 位址、網路遮罩、拓樸及 LAN 設定）
- 各種網路拓樸
- 網路裝置和裝置的管理
- 網路組態設定（如 VLAN 的使用、HTTP 及 HTTPS）

行動安全防護文件

「行動安全防護」文件包含以下文件：

- 《*安裝與部署手冊*》— 本手冊介紹「行動安全防護」，並協助您進行網路的規劃和安裝等作業，讓您立即上手。
- 《*管理手冊*》— 本手冊提供詳細的「行動安全防護」設定政策和技術。
- 《*線上說明*》—《線上說明》的目的在於提供主要產品工作的知識、使用建議及欄位特有的資訊（如有效的參數範圍和最佳值）。
- 《*Readme*》—《Readme》含有線上或紙本文件未包含的最新產品資訊。其中包括新功能之說明、安裝提示、已知問題及發行記錄等主題。
- 《*常見問題集*》—《常見問題集》是收錄解決問題和疑難排解資訊的線上資料庫。它能提供已知產品問題的最新資訊。若要存取「常見問題集」，請開啟：

http://www.trendmicro.com.tw/solutionbank/corporate/default.asp

秘訣

趨勢科技建議您查閱「下載專區」(http://www.trendmicro.com/download/zh-tw/)中對應的連結，以取得產品文件的更新資訊。

文件慣例

本文件採用下列慣例。

表 1. 文件慣例

慣例	說明
大寫	縮寫、簡稱，以及某些指令和鍵盤按鍵的名稱
粗體字	功能表和功能表指令、指令按鈕、標籤及選項
斜體字	其他文件的參考
`Monospace`	範例指令行、程式碼、網頁 URL、檔案名稱及程式輸出
「瀏覽 > 路徑」	到達特定畫面的瀏覽路徑 例如，「檔案 > 儲存」，表示按一下介面上的「檔案」，再按一下「儲存」
注意	組態設定注意事項
秘訣	建議
重要	必要或預設設定與產品限制的相關資訊

慣例	說明
 警告!	重要處理行動與設定選項

第 1 章

簡介

「趨勢科技™企業版行動安全防護 9.8 版」是行動裝置的整合安全解決方案。請閱讀本章以瞭解「行動安全防護」元件和功能，以及它如何保護您的行動裝置。

本章包含以下小節：

瞭解行動裝置威脅

行動裝置隨著平台的標準化和日益增加的連線，也較容易受到更多的威脅。在行動平台上執行的惡意程式數目也逐漸增加，而且透過簡訊也傳送了越來越多的垃圾簡訊。也會透過新的內容來源（例如：WAP 及 WAP Push）傳送不想要的資料。

此外，行動裝置遭竊也可能導致個人資料或機密資料外洩。

關於趨勢科技行動安全防護

「趨勢科技™企業版行動安全防護」是行動裝置專用的全面性安全解決方案。「行動安全防護」整合了趨勢科技的惡意程式防護技術，能夠有效地防禦針對行動裝置的最新威脅。

整合式過濾功能可讓「行動安全防護」防止不當網路通訊進入行動裝置。

此版本的「行動安全防護」不依賴 OfficeScan™，能夠個別安裝在 Windows 電腦上成為獨立式應用程式。

警告!

趨勢科技無法保證「行動安全防護」與檔案系統加密軟體是否相容。提供類似功能（例如，惡意程式防護掃瞄）的軟體產品可能會與「行動安全防護」不相容。

關於趨勢科技行動安全防護中的 Machine Learning

「趨勢科技 Machine Learning」使用進階機器學習技術，能夠透過數位 DNA 特徵鑑別、API 對應和其他檔案特徵，進行威脅資訊的關聯比對、執行深入的檔案分析，以偵測新興的未知安全風險。Machine Learning 是一項強大的工具，可協助將不明威脅與零時差攻擊擋在您的環境之外。

「行動安全防護」在偵測到未知或少見的檔案後，會使用新一代的行動引擎掃瞄檔案，以便擷取檔案特徵，並且傳送報告給「趨勢科技主動雲端截毒技術」

上所代管的 Machine Learning 引擎。透過使用惡意程式建模，Machine Learning 會將樣本與惡意程式模型相比較、指定可能性評分，然後判斷檔案是否為惡意檔案。「行動安全防護」可防止安裝受影響的檔案，而且可提醒使用者解除安裝或移除該等檔案。

行動安全防護系統架構

視您公司的需求而定，您可以使用不同的用戶端伺服器通訊方法實行「行動安全防護」。您也可以選擇在網路中設定一個或任何用戶端伺服器通訊方法組合。

「趨勢科技行動安全防護」支援三種不同的部署模式：

- 強化安全模式與雲端通訊伺服器（雙伺服器安裝）
- 強化安全模式與本機通訊伺服器（雙伺服器安裝）
- 基本安全模式（單一伺服器安裝）

如需詳細資訊，請參閱《*安裝與部署手冊*》。

行動安全防護系統元件

下表說明「行動安全防護」元件。

表 1-1. 行動安全防護系統元件

元件	說明	必要或選用
管理伺服器	「管理伺服器」可讓您從管理 Web 主控台管理「行動裝置代理程式」。向伺服器註冊行動裝置後，您便可以設定「行動裝置代理程式」政策及執行更新。	必要

元件	說明	必要或選用
通訊伺服器	「通訊伺服器」能處理「管理伺服器」和「行動裝置代理程式」之間的通訊。 Trend Micro Mobile Security 提供兩種類型的 Communication Server： • 本機通訊伺服器 (LCS) — 這是部署在您網路本機上的 Communication Server。 • Cloud Communication Server (CCS)— 這是部署在雲端的 Communication Server，您不必安裝此伺服器。趨勢科技會管理 Cloud Communication Server，您只需從「管理伺服器」連線至該伺服器即可。 請參閱比較本機與通訊伺服器 第 1-5 頁。	必要
行動裝置代理程式 (MDA)	「行動裝置代理程式」安裝在受管理的 Android 和 iOS 行動裝置上。代理程式會與「行動安全防護通訊伺服器」通訊，並在行動裝置上執行指令與政策設定。	必要
Microsoft SQL Server	Microsoft SQL Server 代管「行動安全防護管理伺服器」的資料庫。	必要
Active Directory	「行動安全防護管理伺服器」會從 Active Directory 匯入使用者與群組。	選用
憑證授權	「憑證授權」可管理安全防護認證以及用於安全通訊的公用與私密金鑰。	選用
SCEP	「簡單憑證註冊通訊協定」(SCEP) 是為私密憑證授權提供網路前端的通訊協定。 在某些環境中，確保公司設定和政策免遭窺探是非常重要的。若要提供此防護，iOS 允許您加密資料檔，以便它們只能由單一裝置讀取。加密的資料檔就像是一般的設定資料檔，只是設定資料檔負載是透過與裝置 X.509 身分相關聯的公用金鑰加密的。 SCEP 使用「憑證授權」在大型企業發行憑證。它會處理數位憑證的發行與撤銷。SCEP 與「憑證授權」可安裝在同一台伺服器上。	選用

元件	說明	必要或選用
SSL 憑證	（僅限「完整版」部署模式和搭配未列出之 MDM 廠商的「安全掃瞄」部署模式。） 「趨勢科技行動安全防護」須有經認可的公用憑證授權單位發行的 SSL 伺服器憑證，才能使用 HTTPS 在行動裝置和「通訊伺服器」之間進行安全通訊。	如果您想要管理 iOS 行動裝置，則為必要
SMTP 伺服器	請與 SMTP 伺服器連線，務必確認系統管理員可從「行動安全防護管理伺服器」取得報告，並傳送邀請給使用者。	選用

比較本機與通訊伺服器

下表比較「本機通訊伺服器」(LCS) 與「雲端通訊伺服器」(CCS)。

表 1-2. 比較本機與雲端通訊伺服器

功能	Cloud Communication Server	本機通訊伺服器
必須安裝	否	是
支援的使用者授權方法	註冊金鑰	Active Directory 或註冊金鑰
Android 的代理程式自訂	支援	支援

此版本（9.8 版）的新功能

Trend Micro Mobile Security9.8 提供下列新功能：

功能	說明
邀請電子郵件（僅限 Android）	可讓系統管理員在透過 AirWatch 部署「行動裝置代理程式」時，傳送邀請電子郵件給所有使用者。

功能	說明
更多安全掃瞄與偵測功能：	支援掃瞄行動裝置上是否有下列問題： • 惡意 SSL 憑證 • 惡意 iOS 資料檔（僅限 iOS） • 網路流量解密問題 • 不安全的無線網路存取點 (Wi-Fi) • 開發人員選項與 USB 偵錯（僅限 Android） • 被竄改的應用程式
新的 Widget、系統管理員通知與報告	針對惡意 SSL 憑證、惡意 iOS 資料檔、網路流量解密問題、不安全的無線網路存取點 (Wi-Fi)、開發人員選項、USB 偵錯、被竄改的應用程式以及已開放 Root 權限/已破解的行動裝置，引入新的 Widget、系統管理員通知與報告。
應用程式核可的清單	引入核可的清單，供系統管理員將被偵測為惡意程式、易受攻擊、有隱私風險或被竄改的應用程式新增為安全的應用程式，讓此類應用程式得以安裝到行動裝置上。
iOS 行動裝置代理程式支援	支援讓 iOS 行動裝置代理程式在「安全掃瞄」模式下運作（限搭配 AirWatch 和 MobileIron）。

此版本（9.7 版 Patch 3）的新功能

Trend Micro Mobile Security9.7 版 Patch 3 提供下列新功能：

功能	說明
提供 QR 碼以供快速部署代理程式 （僅限安全掃瞄部署模式）	在代理程式部署設定畫面上使用 QR 碼提供註冊資訊，以便簡單快速地部署代理程式。 此功能僅能在與 AirWatch 和 MobileIron 整合時的安全掃瞄部署模式下使用。
支援 Machine Learning	支援使用趨勢科技 Machine Learning 執行深入的檔案分析，以便偵測新興的已知安全威脅。

此版本（9.7 版 Patch 2）的新功能

Trend Micro Mobile Security 9.7 版 Patch 2 提供下列新功能：

功能	說明
與 MobileIron 行動裝置管理解決方案整合	提供對 Android 與 iOS 行動裝置的安全掃瞄功能，同時可與下列 MobileIron 行動裝置管理解決方案整合： • 已代管 MobileIron Core • MobileIron Core 內部部署
整合線上說明	將所有 UI 畫面連結到趨勢科技線上說明中心提供的說明檔案。
支援 iOS 啟動鎖定 （僅限完整版部署模式）	「啟動鎖定」是「尋找我的 iPhone」的功能，內建於搭載 iOS 7 和更新版本的行動裝置。這項功能會要求任何人在關閉「尋找我的 iPhone」、刪除或重新啟用和使用行動裝置之前，必須先輸入使用者的 Apple ID 和密碼，以防止重新啟用遺失或遭竊的行動裝置。

此版本（9.7 版）的新功能

Trend Micro Mobile Security 9.7 提供下列新功能：

功能	說明
多重部署模式	可讓您使用下列模式部署「Trend Micro Mobile Security」： • 「完整版」部署模式，包括「Trend Micro Mobile Security」的所有功能。 • 「僅有安全掃瞄功能」部署模式，提供對 Android 與 iOS 行動裝置的安全掃瞄功能，同時可與其他行動裝置管理 (MDM) 解決方案整合。
與 AirWatch 整合	提供對 Android 與 iOS 行動裝置的安全掃瞄功能，同時可與 AirWatch 行動裝置管理解決方案整合。

功能	說明
報表畫面上的網路安全新聞 Widget	包括「報表」畫面上的 Widget，會顯示由趨勢科技發佈的有關行動裝置的網路安全新聞。
Android 裝置上的伺服器憑證驗證	可讓您對 Android 行動裝置執行伺服器憑證驗證。
提供安全掃瞄功能的新 MARS API	與最新的行動應用程式信譽評等服務 (MARS) API 整合，來強化弱點偵測與說明。
支援最新的 Android 與 iOS 版本	新增 Android 7 與 iOS 10 支援。

此版本（9.6 SP1 版）的新功能

Trend Micro Mobile Security 9.6 SP1 提供下列新功能：

功能	說明
勒索軟體偵測 Widget	「報表」上的新 Widget 可讓管理員檢視勒索軟體偵測統計資料。
Android 應用程式版本選取	管理員可以選擇要為 Android 與 iOS 裝置部署「完整版」或「僅有安全掃瞄功能」應用程式。
在 Android 裝置上進行自動應用程式啟動	此版本的「行動安全防護」提供在應用程式部署期間，於 Android 裝置上進行自動啟動。
Exchange 伺服器資料清除 （僅限完整版部署模式）	管理員可以先執行資料清除，然後再將資料移轉到另一部 Exchange 伺服器。如此，即可讓管理員在「行動安全防護」上移除現有的 MS Exchange 行動安全整合與 Exchange ActiveSync 裝置資料。
多個 Active Directory 使用者的群組設定	管理員可以將群組設定套用到多個 Active Directory 使用者。
報告產生（依裝置平台）	報告產生功能的增強功能可讓管理員產生所選取裝置平台的報告。

功能	說明
裝置資訊更新	管理員可以在下一個已預約更新之前，更新受管理行動裝置的裝置資訊。

此版本（9.6 版）的新功能

Trend Micro Mobile Security 9.6 提供下列新功能：

功能	說明
使用者管理	讓系統管理員可以分別管理使用者和邀請。
視需要報告	系統管理員現在可以視需要產生報告。
預約掃瞄	讓系統管理員根據指定的預約（每日、每週或每月）執行惡意程式和安全掃瞄。
適用於 Android 的安全掃瞄	除了隱私掃瞄外，「行動安全防護」現在還支援弱點掃瞄和被竄改的應用程式掃瞄，提高了安全性。
全新 Widget	此版本引入了五個用於顯示 Android 安全掃瞄和 iOS 惡意程式掃瞄相關資訊的全新 Widget。
全新的 iOS 應用程式版本	系統管理員可以選擇部署全新的 iOS 應用程式版本，該版本僅支援安全掃瞄，並且可以搭配協力廠商行動裝置管理 (MDM) 應用程式使用。

行動裝置代理程式的主要功能

功能名稱	說明		ANDROID	IOS
安全掃瞄	「行動安全防護」納入了趨勢科技的惡意程式防護技術，以有效偵測威脅，防止攻擊者利用行動裝置的弱點進行入侵。「行動安全防護」是專為掃瞄行動裝置威脅而設計。	惡意程式掃瞄	●	●
		隱私掃瞄	●	
		弱點掃瞄	●	
		被竄改的應用程式掃瞄	●	●
		USB 偵錯掃瞄	●	
		開發人員選項掃瞄	●	
		已開放 Root 權限的行動裝置掃瞄	●	
		已破解的行動裝置掃瞄		●
		惡意 iOS 資料檔掃瞄		●
		網路流量解密問題掃瞄	●	●
		惡意 SSL 憑證掃瞄	●	●
		不安全的無線網路存取點 (Wi-Fi) 掃瞄	●	
驗證	安裝「行動裝置代理程式」後，行動裝置使用者需要提供驗證資訊以向「行動安全防護管理伺服器」註冊行動裝置。		●	●

功能名稱	說明		ANDROID	IOS
定期更新	要防範最新的威脅，您可以手動更新「行動安全防護」，或將其設定為自動更新。若要節省成本，您也可以為“漫遊中”的行動裝置設定不同的更新頻率。更新的內容包括元件更新和「行動安全防護」程式 Patch 更新。		●	
行動裝置代理程式記錄	「管理伺服器」上提供「行動裝置代理程式」記錄。	應用程式掃瞄記錄	●	●
		裝置弱點記錄	●	●
		網路安全防護記錄	●	●
		Web 威脅防護記錄	●	
	「行動裝置代理程式」會在行動裝置上留存使用者記錄。	惡意程式掃瞄記錄	●	
		弱點掃瞄記錄	●	
		被竄改的應用程式掃瞄記錄	●	
		隱私掃瞄記錄	●	
		網頁封鎖記錄	●	

支援的行動裝置作業系統功能

下表顯示「趨勢科技行動安全防護」在每個平台上支援的功能清單。

表 1-3. 趨勢科技行動安全防護 9.8 功能列表

政策	功能	設定		
裝置安全	安全設定	即時掃瞄		●
		病毒碼更新完成後進行掃瞄		●

政策	功能	設定		
		手動掃瞄	●	●
資料安全防護	Web 威脅防護	伺服器端控管		●
		使用封鎖的清單		●
		使用核可的清單		●
		僅限特定網站		●
		允許限制的成人內容		●

第 2 章

開始使用行動安全防護

本節協助您開始使用「行動安全防護」及提供基本的使用指示。在繼續閱讀之前，請務必安裝「管理伺服器」、「通訊伺服器」，以及將「行動裝置代理程式」安裝在行動裝置上。

本章包含以下小節：

管理 Web 主控台

您可以透過「行動安全防護」管理 Web 主控台存取設定畫面。

Web 主控台是在整個公司網路進行「行動安全防護」管理和監控的中心點。主控台提供一組預設設定和值，不過您也可以根據安全需求和規格來加以設定。

您可以使用 Web 主控台來執行以下作業：

- 管理安裝在行動裝置上的「行動裝置代理程式」
- 設定「行動裝置代理程式」的安全政策
- 設定單一或多部行動裝置上的掃瞄設定
- 將裝置劃分為邏輯群組，以利組態設定和管理
- 檢視註冊和更新資訊

存取管理 Web 主控台

步驟

1. 使用下列 URL 結構登入管理 Web 主控台：

   ```
   https://
   <External_domain_name_or_IP_address>:<HTTPS_port>/mdm/web
   ```

   注意

   以實際的 IP 位址取代 <External_domain_name_or_IP_address>，以「管理伺服器」的實際通訊埠號碼取代 <HTTPS_port>。

隨即顯示以下畫面。

圖 2-1. 管理 Web 主控台登入畫面

2. 在提供的欄位中輸入使用者名稱與密碼，再按一下「登入」。

注意

管理 Web 主控台的預設「使用者名稱」為 “root” ，「密碼」為 “mobilesecurity” 。

在您第一次登入後請務必變更 "root" 使用者的系統管理員密碼。請參閱編輯系統管理員帳號 第 2-14 頁中該程序的相關說明。

重要

如果您使用 Internet Explorer 存取管理 Web 主控台，請務必符合以下條件：

- 「網站相容性檢視」選項已關閉。如需詳細資料，請參閱關閉 Internet Explorer 中的相容性檢視 第 2-4 頁。
- 瀏覽器上的 JavaScript 為啟動。

注意

如果您在 Windows 2012 中無法使用 Metro 模式的 Internet Explorer 10 存取管理 Web 主控台，請確認 Internet Explorer 的「加強的受保護模式」選項已關閉。

關閉 Internet Explorer 中的相容性檢視

「趨勢科技行動安全防護」不支援 Internet Explorer 上的「相容性檢視」。如果您使用 Internet Explorer 存取「行動安全防護」管理 Web 主控台，請在網路瀏覽器上關閉該網站的「相容性檢視」（若已啟動）。

步驟

1. 開啟 Internet Explorer，並按一下「工具 > 相容性檢視設定」。

   「相容性檢視設定」視窗隨即出現。

2. 如果管理主控台已新增至「相容性檢視」清單中，請選取該網站並按一下「移除」。

3. 清除「在相容性檢視下顯示內部網路網站」與「在相容性檢視下顯示所有網站」核取方塊，然後按一下「關閉」。

產品授權

當試用版授權到期後，所有程式功能都將關閉。完整版授權可讓您繼續使用所有功能，即使授權到期後依然可以使用。然而請注意，由於「行動裝置代理程式」將無法從伺服器取得更新，因此惡意程式防護元件將容易受到最新安全威脅的侵擾。

當授權到期時，您需要使用新的啟動碼註冊「行動安全防護管理伺服器」。如需詳細資訊，請洽詢當地的趨勢科技銷售代表。

若要下載更新及允許遠端管理，「行動裝置代理程式」必須向「行動安全防護管理伺服器」註冊。如需在行動裝置上手動註冊「行動裝置代理程式」的指示，請參閱《*安裝與部署手冊*》。

若要檢視「管理伺服器」的授權升級指示，請在「行動安全防護」的「產品使用授權」畫面中按一下「檢視授權升級指示」連結。

報表資訊

當您存取「管理伺服器」時，「報表」畫面隨即先出現。此畫面能提供行動裝置註冊狀態和元件詳細資料的總覽。

報表畫面分成兩標籤：

- 「摘要」— 顯示與行動裝置、行動裝置健康情況/安全狀態及行動裝置作業系統版本摘要相關的網路安全新聞。
- 「安全」— 顯示 Android 裝置弱點掃瞄摘要、iOS 裝置弱點掃瞄摘要、Android 網路安全防護摘要、iOS 網路安全防護摘要、Android 應用程式風險摘要、iOS 應用程式風險摘要。在這個類別中，您可以看到以下 Widget 和狀態：
    - Android/iOS 弱點摘要：
        - 已開放 Root 權限：（僅限 Android）已開放 Root 權限的行動裝置數目
        - USB 偵錯：（僅限 Android）已啟動 USB 偵錯模式的行動裝置數目
        - 開發人員選項：（僅限 Android）已啟動開發人員模式的行動裝置數目
        - 已破解：（僅限 iOS）已破解的行動裝置數目
        - 惡意 iOS 資料檔：（僅限 iOS）已安裝惡意 iOS 資料檔的行動裝置數目
    - Android/iOS 網路安全防護摘要：
        - 不安全的無線網路存取點 (Wi-Fi)：（僅限 Android）與可疑或不安全（密碼很弱或未設密碼）的無線網路存取點 (Wi-Fi) 連線的行動裝置數目

- 網路流量解密問題：被偵測到網路流量遭解密的行動裝置數目
- 惡意 SSL 憑證：已安裝惡意 SSL 憑證的行動裝置數目

- Android/iOS 應用程式風險摘要：
  - 「惡意程式」：已安裝但被偵測為惡意程式的應用程式數目
  - 易受攻擊的應用程式：（僅限 Android）已安裝但被偵測為易受攻擊的應用程式數目
  - 隱私風險：（僅限 Android）已安裝但被偵測到洩漏隱私的應用程式數目
  - 被竄改的應用程式：以被竄改的應用程式套件安裝的應用程式數目

自訂「報表」

「行動安全防護」可讓您根據需求自訂「報表」資訊。

新增標籤

步驟

1. 在「報表」畫面上，按一下  按鈕。
2. 在「新標籤」快顯視窗中進行以下設定：
   - 「標題」：輸入標籤名稱。
   - 「配置」：選取標籤上所顯示 Widget 的配置。
   - 「自動調整」：選取「開啟」或「關閉」以啟動或關閉標籤上的 Widget 設定。
3. 按一下「儲存」。

移除標籤

步驟

1. 按一下標籤，再按一下標籤上顯示的 × 按鈕。
2. 按一下確認快顯對話方塊中的「確定」。

新增 Widget

步驟

1. 在「報表」畫面上，按一下您要新增 Widget 的標籤。
2. 按一下標籤右上角的「新增 Widget」。

   「新增 Widget」畫面隨即顯示。
3. 從左側功能表中選取類別，並/或在搜尋欄位中輸入關鍵字，以顯示相關的 Widget 清單。
4. 選取您要新增的 Widget，再按一下「新增」。

   所選的 Widget 隨即出現「報表」上。

移除 Widget

步驟

1. 在「報表」畫面上，按一下您要移除 Widget 的標籤。
2. 在您要移除的 Widget，按一下 Widget 右上角的 × 。

變更 Widget 的位置

步驟

1. 在「報表」畫面上，按一下您要重新排列位置其 Widget 的標籤。
2. 按一下 Widget 標題列不放，然後將它拖放到新的位置上。

重新整理 Widget 的資訊

步驟

1. 在「報表」畫面上，按一下您要重新整理其 Widget 的標籤。
2. 在您要重新整理的 Widget，按一下 Widget 右上角的 。

檢視或修改標籤設定

步驟

1. 在「報表」畫面上，按一下您要檢視或修改其設定的標籤。
2. 按一下「標籤設定」。
3. 視需要修改設定，再按一下「儲存」。

管理設定

進行 Active Directory (AD) 設定

「趨勢科技行動安全防護 」可讓您根據 Active Directory (AD) 設定使用者授權。您也可以使用 AD 將行動裝置新增至裝置清單中。如需詳細的設定步驟，請參閱《*安裝與部署手冊*》的＜*初始伺服器設定*＞一節。

設定使用者驗證

「趨勢科技行動安全防護」可讓您根據 Active Directory (AD) 或透過註冊金鑰設定使用者驗證。如需詳細的設定步驟，請參閱《*安裝與部署手冊*》的＜*初始伺服器設定*＞一節。

進行資料庫設定

如需詳細的設定步驟，請參閱《*安裝與部署手冊*》的＜*初始伺服器設定*＞一節。

進行通訊伺服器設定

如需詳細的設定步驟，請參閱《*安裝與部署手冊*》的＜*初始伺服器設定*＞一節。

進行部署設定

如需詳細的設定步驟，請參閱《*安裝與部署手冊*》的＜*初始伺服器設定*＞一節。

從完整版部署模式切換到安全掃瞄部署模式

您隨時都可以切換「行動安全防護」的部署模式。

請參閱以下有關從「完整版」部署模式切換到「安全掃瞄」部署模式的知識庫文章：

https://success.trendmicro.com/solution/1115884

設定 AirWatch 與趨勢科技行動安全防護的整合

「趨勢科技行動安全防護」讓您能與 AirWatch 裝置管理解決方案進行整合。

如需詳細資訊，請參閱與 AirWatch 整合 第 3-2 頁主題。

設定 MobileIron 與趨勢科技行動安全防護的整合

「趨勢科技行動安全防護」讓您能與 MobileIron 裝置管理解決方案進行整合。

如需詳細資訊，請參閱與 MobileIron 整合 第 3-15 頁主題。

管理系統管理員帳號

「系統管理員帳號管理」畫面可讓您建立具備不同 管理伺服器存取角色的使用者帳號。

預設系統管理員帳號名稱與角色

預設系統管理員帳號為 “root”（密碼：“mobilesecurity”）。root 帳號無法刪除，只能修改。如需詳細程序，請參閱編輯系統管理員帳號 第 2-14 頁。

表 2-1. root 帳號內容

ROOT 帳號內容		是否可修改？
系統管理員帳號	帳號名稱	否
	全名	是
	密碼	是
	電子郵件地址	是
	行動電話號碼	是
系統管理員角色	系統管理員角色修改	否

預設的系統管理員角色為「超級系統管理員」，具備所有設定的最大存取權限。「超級系統管理員」角色無法刪除，只能修改。如需詳細程序，請參閱編輯系統管理員角色 第 2-16 頁。

表 2-2.「超級系統管理員」角色內容

「超級系統管理員」角色內容		是否可修改？
角色詳細資訊	系統管理員角色	否
	說明	是
群組管理控管	受管理群組	否

表 2-3.「超級系統管理員」與「群組管理員」的存取權限

伺服器元件	權限	超級管理員	群組管理員
管理	更新	支援	不支援
	系統管理員帳號管理	可修改所有帳號	只能修改自己的帳號資訊
	裝置註冊設定	支援	不支援
	憑證管理	支援	支援
	指令佇列管理	可管理所有的指令	只能檢視相關群組的指令
	資料庫設定	支援	不支援
	通訊伺服器設定	支援	不支援
	Active Directory 設定	支援	不支援
	管理伺服器設定	支援	不支援
	部署設定	支援	不支援
	設定與驗證	支援	不支援
	產品授權	支援	不支援
通知/報告	記錄查詢	所有群組	僅受管理群組
	記錄維護	所有群組	僅受管理群組
	系統管理員通知/報告	支援	不支援
	使用者通知	支援	不支援
	設定	支援	不支援
應用程式		支援	僅支援受管理群組

伺服器元件	權限	超級管理員	群組管理員
政策	建立政策	支援	僅支援受管理群組
	檢視政策	支援	僅支援受管理群組
	複製政策	支援	僅支援受管理群組
	刪除政策	支援	僅支援受管理群組
裝置	檢視裝置	支援	僅支援受管理群組
	新增群組	支援	支援
使用者	邀請使用者	支援	僅支援受管理群組

新增系統管理員帳號

步驟

1. 在「行動安全防護」管理 Web 主控台上，移至「管理 > 系統管理員帳號管理」。
2. 在「系統管理員帳號」標籤中，按一下「建立」以新增新的帳號。

   「建立系統管理員帳號」畫面隨即顯示。
3. 在「帳號詳細資訊」區段下，進行以下設定：
   - 選取「趨勢科技行動安全防護使用者」，並指定下列使用者帳號詳細資訊：
     - 「帳號名稱」：用於登入「管理伺服器」的名稱。
     - 「全名」：使用者全名。
     - 「密碼」（與「確認密碼」）。
     - 「電子郵件地址」：使用者的電子郵件地址。
     - 「行動電話號碼」：使用者的電話號碼。
   - 選取「Active Directory 使用者」，進行以下設定：

a. 在搜尋欄位中輸入使用者名稱，然後按一下「搜尋」。

b. 從左邊的清單選取使用者名稱，然後按一下 > 將這些使用者移至右邊的「選取的使用者」清單。

注意

若要將使用者從右邊的「選取的使用者」清單中移除，請選取使用者名稱，並按一下 <。

按一下使用者名稱時同時按住 Ctrl 或 Shift 鍵不放，也可以同時選取多個使用者。

4. 在「系統管理員角色」區段下，從「選擇系統管理員角色：」下拉式清單中選取角色。

請參閱建立系統管理員角色 第 2-15 頁中有關建立系統管理員角色的程序

5. 按一下「儲存」。

編輯系統管理員帳號

步驟

1. 在「行動安全防護」管理 Web 主控台上，移至「管理 > 系統管理員帳號管理」。
2. 在「系統管理員帳號」標籤中，按一下「建立」以新增新的帳號。

「編輯系統管理員帳號」畫面隨即顯示。

3. 修改系統管理員帳號詳細資訊，並視需要存取角色。
   - 帳號詳細資訊
     - 「帳號名稱」：用於登入「管理伺服器」的名稱。
     - 「全名」：使用者全名。
     - 「電子郵件地址」：使用者的電子郵件地址。

- 「行動電話號碼」：使用者的電話號碼。
- 「密碼」：按一下「重設密碼」變更使用者帳號密碼，在「新密碼」與「確認密碼」欄位中輸入新密碼，然後按一下「儲存」。

- 系統管理員角色
  - 「選取系統管理員角色」：從下拉式清單中選取系統管理員角色。

    如需建立系統管理員角色的程序，請參閱建立系統管理員角色 第 2-15 頁。

4. 按一下「儲存」。

刪除系統管理員帳號

步驟

1. 在「行動安全防護」管理 Web 主控台上，移至「管理 > 系統管理員帳號管理」。
2. 在「系統管理員帳號」標籤上，選取您要刪除的系統管理員帳號，然後按一下「刪除」。

   隨即出現確認訊息。

建立系統管理員角色

步驟

1. 在「行動安全防護」管理 Web 主控台上，移至「管理 > 系統管理員帳號管理」。
2. 在「系統管理員角色」標籤上按一下「建立」。

   「建立系統管理員角色」畫面隨即顯示。

3. 在「角色詳細資訊」區段下提供下列資訊：
   - 系統管理員角色
   - 說明
4. 在「群組管理控管」區段下，選取此系統管理員角色可管理的行動裝置群組。
5. 按一下「儲存」。

編輯系統管理員角色

步驟

1. 在「行動安全防護」管理 Web 主控台上，移至「管理 > 系統管理員帳號管理」。
2. 在「系統管理員角色」標籤上按一下「建立」。

   「建立系統管理員角色」畫面隨即顯示。
3. 視需要修改角色詳細資訊，然後按一下「儲存」。

刪除系統管理員角色

步驟

1. 在「行動安全防護」管理 Web 主控台上，移至「管理 > 系統管理員帳號管理」。
2. 在「系統管理員角色」標籤上，選取您要刪除的系統管理員角色，然後按一下「刪除」。

   隨即出現確認訊息。

變更系統管理員密碼

請參閱編輯系統管理員帳號 第 2-14 頁主題中有關變更系統管理員帳號密碼的程序。

指令佇列管理

「行動安全防護」可保留您從 Web 主控台執行過的所有指令，並可讓您視需要取消或重新傳送指令。您也可以將執行過但不需要顯示在清單上的指令移除。

若要存取「指令佇列管理」畫面，請移至「管理 > 指令佇列管理」。

下表描述「指令佇列管理」畫面上所有的指令狀態。

指令狀態	說明
等待傳送	「行動安全防護管理伺服器」正在處理將指令傳送到行動裝置。 當指令為此狀態時，您可以將它取消。
等待確認	「行動安全防護管理伺服器」已將指令傳送至行動裝置，並正在等待行動裝置的確認。
未成功	無法在行動裝置上執行指令。
成功	已成功在行動裝置上執行指令。
已取消	在行動裝置上執行指令前先將指令取消。

若要使指令的大小不佔用太多硬碟空間，請手動刪除指令，或設定「行動安全防護」管理 Web 主控台，使其根據「指令佇列維護」畫面中的預約自動刪除指令。

設定預約刪除舊指令

步驟

1. 按一下「管理 > 指令佇列管理」。

   「指令佇列管理」畫面隨即顯示。

2. 在「指令佇列管理」標籤中選取「啟動預約刪除指令」。
3. 指定要刪除存留期超過幾天的指令。
4. 指定指令佇列刪除的頻率和時間。
5. 按一下「儲存」。

手動刪除舊指令

步驟

1. 按一下「管理 > 指令佇列管理」。

   「指令佇列管理」面隨即顯示。

2. 在「指令佇列管理」標籤中選取「啟動預約刪除指令」。
3. 指定要刪除存留期超過幾天的指令。
4. 按一下 「立即刪除」。

管理憑證

使用「憑證管理」畫面將 `.pfx`、`.p12`、`.cer`、`.crt` 及 `.der` 憑證上傳至「行動安全防護管理伺服器」。

上傳憑證

步驟

1. 登入「行動安全防護」管理 Web 主控台。
2. 按一下「管理 > 憑證管理」。
3. 按一下「新增」。

   「新增憑證」視窗隨即出現。
4. 按一下「選擇檔案」，再選取.pfx、.p12、.cer、.crt、.der 憑證檔案。
5. 在「密碼」欄位中輸入新的憑證密碼。
6. 按一下「儲存」。

刪除憑證

步驟

1. 登入「行動安全防護」管理 Web 主控台。
2. 按一下「管理 > 憑證管理」。
3. 選取您要刪除的憑證，再按一下「刪除」。

第 3 章

與其他 MDM 解決方案整合

「趨勢科技行動安全防護」讓您能將其他行動裝置管理解決方案與「行動安全防護」進行整合。

本章說明設定「行動安全防護」與其他行動裝置管理解決方案整合的程序。

本章涵蓋主題如下：

與 AirWatch 整合

「趨勢科技行動安全防護」讓您能將 AirWatch MDM 解決方案與「行動安全防護」進行整合。

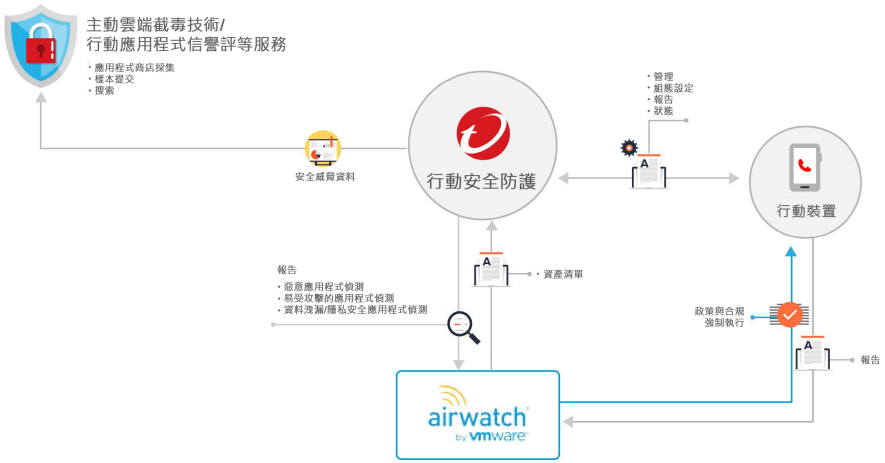
整合先決條件

若要將其他 MDM 解決方案與「趨勢科技行動安全防護」，您必須使用以下項目：

- 企業版行動安全防護 9.7 或更新版本
- 行動安全防護中設有本機通訊伺服器或雲端通訊伺服器
- AirWatch 9.1 或更新版本
- AirWatch 管理 Web 主控台上的系統管理員帳號

AirWatch 整合架構

下圖顯示與 AirWatch 整合的高階架構。



「行動應用程式信譽評等」是以雲端為基礎的技術，可根據應用程式行為自動識別行動裝置威脅、從多個 Android 市場抓取與收集大量的 Android 應用程式、識別現有和全新的行動裝置惡意程式、識別可能濫用隱私/裝置資源的應用程式。這是全球第一個自動行動應用程式評估服務。

「趨勢科技主動雲端截毒技術」提供主動式全球威脅資訊來防範零時差威脅，以確保您始終受到防護。趨勢科技運用即時威脅資訊，可立即消滅攻擊，使其無法危害您。所有趨勢科技產品與服務均以「主動雲端截毒技術」作為後盾。

「行動安全防護」使用主動雲端截毒技術和行動應用程式信譽評等服務來找出行動裝置安全問題，並運用 AirWatch 合規政策管理您的行動裝置。

整合功能

「趨勢科技行動安全防護」提供下列與 AirWatch 整合的功能：

功能	說明
行動裝置自動分組	「行動安全防護」會根據風險等級，對行動裝置加上「Dangerous」、「Risky」和「No_TMMS」尾碼做為標籤。 如需詳細資料，請參閱行動裝置自動分組 第 3-4 頁。
應用程式自動分組	「行動安全防護」會根據風險等級，對行動應用程式加上「Malware」、「Vulnerability」和「Privacy」前置碼來進行分組。 如需詳細資料，請參閱行動應用程式自動分組 第 3-4 頁。
自動更新 AirWatch 的政策違規應用程式黑名單	此功能可讓您將違反 AirWatch 合規政策（根據安全掃瞄結果）的應用程式列入黑名單，並傳送電子郵件警訊給使用者。 如需詳細資料，請參閱設定 AirWatch 的應用程式黑名單合規政策 第 3-5 頁。

功能	說明
自動部署行動安全防護用戶端應用程式	您可以設定 AirWatch 將行動裝置代理程式自動部署至行動裝置。 • Android: 如需相關程序，請參閱透過行動安全防護伺服器部署 Android 代理程式 第 3-11 頁。 您也可以設定 Samsung 行動裝置自動在行動裝置上啟動行動裝置代理程式。如需詳細資訊和相關程序，請參閱設定 Android 行動裝置自動啟動 第 3-12 頁。 • iOS: 如需相關程序，請參閱部署 iOS 代理程式 第 3-13 頁。

行動裝置自動分組

「行動安全防護」會使用前置碼來建立三 (3) 種級別（Dangerous、Risky 和 NO_TMMS），並將風險裝置標記如下：

- PREDEFINEDPREFIX_Dangerous
- PREDEFINEDPREFIX _Risky
- PREDEFINEDPREFIX _NO_TMMS

「行動安全防護」可讓您在管理 Web 主控台上定義前置碼 (PREDEFINEDPREFIX)。「行動安全防護」在偵測到不同安全層級的行動裝置時，會自動變更裝置的智慧型群組。

例如，如果「行動安全防護」偵測到行動裝置上出現惡意程式，它會自動將行動裝置移至 PREDEFINEDPREFIX _Dangerous 群組。

行動應用程式自動分組

「行動安全防護」會根據風險應用程式所帶來的風險類型，將這些應用程式自動分組在「應用程式群組」之下。

- PREDEFINEDPREFIX _Malware_App_Android
- PREDEFINEDPREFIX _Privacy_App_Android
- PREDEFINEDPREFIX _Vulnerability_App_Android
- PREDEFINEDPREFIX _Malware_App_iOS

「行動安全防護」可讓您在管理 Web 主控台上定義前置碼 (PREDEFINEDPREFIX)。

設定 AirWatch 的應用程式黑名單合規政策

進行 AirWatch 整合設定後，您可以在 AirWatch 管理 Web 主控台上建立合規政策，將惡意應用程式新增到 AirWatch 的「黑名單」。

步驟

1. 登入 AirWatch Web 主控台，然後瀏覽至「裝置 > 合規政策 > 清單檢視」。
2. 按一下「新增」、選取平台（Android 或 Apple iOS），然後從下拉式清單中選取「應用程式清單」和「包含列入黑名單的應用程式.」
3. 按一下「下一步」。
4. 在「處理行動」標籤上，設定處理行動：
   a. 選取「標示為不合規」。
   b. 從下拉式清單中選取「通知」和「傳送電子郵件給使用者」。
   c. 按一下「下一步」。
5. 在「指定」標籤上，設定下列項目：
   - 管理者：趨勢科技
   - 指定群組
   - 排除
6. 按一下「下一步」。

7. 在「摘要」標籤上，設定名稱和說明。

8. 按一下「完成並啟動」。

在行動裝置上偵測到惡意程式時，「行動安全防護」即會將應用程式列入 AirWatch 黑名單，且行動裝置將會標為不合規。

適用於整合的 AirWatch 帳戶權限需求

「行動安全防護」可支援與 AirWatch 整合。若要將「行動安全防護」與 AirWatch 整合，您必須具有 AirWatch 帳戶，且該帳戶必須具有在「行動安全防護」伺服器與 AirWatch 之間通訊所需的權限。

若要在 AirWatch 上建立帳戶，您有三種不同的權限選項可選：

- 選項 1：建立 AirWatch 管理員帳戶，以便在擁有所有權限的情況下進行通訊

  在 AirWatch 管理主控台上，瀏覽至「帳戶 > 管理員 > 清單檢視 > 新增 > 新增管理員」，然後建立具有以下角色與權限的帳戶：

  ```
  AirWatch Administrator AirWatch Admins (Internal or External) Access to all
  ```

- 選項 2：建立僅能使用 API、具有所有 REST API 權限的使用者

  在 AirWatch 管理主控台上，瀏覽至「帳戶 > 管理員 > 清單檢視 > 新增 > 新增管理員」，然後建立具有以下角色與權限的帳戶：

  ```
  API Only Only provides access to REST APIs
  ```

- 選項 3：透過僅能使用 API、具有自訂 REST API 權限的使用者

  此選項可讓您選取「行動安全防護」所用的特定 REST API。

  執行以下操作：

  1. 在 AirWatch 管理主控台上，瀏覽至「帳戶 > 管理員 > 角色」，然後建立具有「行動安全防護」所用特定 REST API 權限的角色，這些權限如下表所示：

類別	名稱
管理員使用者管理	搜尋管理員使用者
WTag 管理	建立標籤
	搜尋標籤
	新增裝置至標籤
	從標籤移除裝置
	擷取具有特定標籤的裝置
智慧型群組管理	建立智慧型群組
	搜尋智慧型群組
	刪除智慧型群組
應用程式群組管理	建立應用程式群組
	搜尋應用程式群組
	擷取應用程式群組詳細資訊
	新增應用程式至應用程式群組
	從應用程式群組刪除應用程式
應用程式管理	內部應用程式安裝：上傳應用程式區塊（iOS 和 Android）
	內部應用程式安裝：開始內部應用程式安裝
裝置管理	擷取裝置資訊
	裝置廣泛搜尋
	裝置計數資訊

2. 瀏覽至「帳戶 > 管理員 > 清單檢視 > 新增 > 新增管理員」，然後以新建立的角色新增帳戶。

注意

AirWatch REST 權限設定頁面上雖然沒有每個 API 的權限，但是提供了許多 API 系列（例如「管理 API」、「APP API」等）。若要知道設定頁面上必須啟動哪些 REST API 權限，請聯絡 AirWatch 技術支援。

設定 AirWatch 整合

步驟

1. 登入「行動安全防護」管理 Web 主控台。
2. 按一下功能表列上的「管理 > 通訊伺服器設定」，並確認已進行通訊伺服器設定。如果尚未設定，請參閱《*安裝與部署手冊*》中的〈*進行通訊伺服器設定*〉主題，瞭解設定步驟。
3. 按一下「管理 > 部署設定」。
4. 在「伺服器」區段下，選取「安全掃瞄」，然後從下拉式清單中選取「AirWatch MDM 解決方案」。
5. 在「註冊服務」區段下，進行以下 AirWatch 設定：
   - API URL
   - API 金鑰
   - 帳號
   - 密碼
6. 按一下「驗證設定」，確認「行動安全防護」可以連線至 AirWatch 伺服器。
7. 在「資料同步設定」區段下，進行以下設定：
   - 安全類別前置碼

注意

「行動安全防護」會使用前置碼來建立三 (3) 種級別（Dangerous、Risky 和 NO_TMMS），並將風險裝置標記如下：

- XXXX_Dangerous
- XXXX_Risky
- XXXX_NO_TMMS

風險裝置與應用程式會分別分組到「智慧型群組」與「應用程式群組」下，而且加入的應用程式其名稱前會加上標籤和類別做為前置碼。

- 智慧型群組：XXXX_Dangerous、XXXX_Risky、XXXX_NO_TMMS
- 應用程式群組：XXXX_Malware_App_Android、XXXX_Privacy_App_Android、XXXX_Vulnerability_App_Android、XXXX_Malware_App_iOS

代理程式部署

「趨勢科技行動安全防護」可讓您從兩個不同來源部署用戶端代理程式：

- Google Play 商店：您將需要設定 AirWatch，以便部署行動裝置代理程式並提供註冊資訊給使用者（以簡訊或 QR 碼的形式）。使用者可以使用註冊資訊或是掃瞄 QR 碼來向伺服器註冊。註冊資訊包括伺服器 IP 位址、通訊埠號碼，以及註冊碼（可在「部署設定」畫面的「Android 代理程式」標籤找到）。

  安裝行動裝置代理程式後，使用者就必須手動向「行動安全防護」伺服器註冊。如果您從 Google Play 商店部署行動裝置代理程式，行動裝置使用者便可透過 Google Play 接收即時更新。

- 行動安全防護伺服器：通知使用者從 AirWatch 應用程式商店下載名稱為「企業行動安全」的行動裝置代理程式。

  如果您使用此部署選項，將需要提供註冊資訊給使用者（以簡訊或 QR 碼的形式）。使用者可以使用註冊資訊或是掃瞄 QR 碼來向伺服器註冊。註冊資訊包括伺服器 IP 位址、通訊埠號碼，以及註冊碼（可在「部署設

定」畫面的「Android 代理程式」標籤找到）。使用者只要啟動行動裝置代理程式，就必須向「行動安全防護」伺服器註冊應用程式。您也可以設定應用程式自動註冊。不過，每當有更新可用時，行動裝置使用者就必須手動更新其行動裝置代理程式。

在 Samsung 行動裝置上，AirWatch 管理主控台可讓您自動部署與設定行動裝置代理程式。

透過 Google Play 商店部署 Android 代理程式

步驟

1. 登入 AirWatch Web 主控台，然後瀏覽至「應用程式與書籍 > 清單檢視 > 公開 (標籤) > 新增應用程式」。
2. 在「新增應用程式」畫面上，設定以下欄位：
   - 管理者：輸入 `Trend Micro`。
   - 平台：從下拉式清單中選取 Android。
   - 來源：選取「搜尋應用程式商店」。
   - 「名稱」：輸入企業行動安全來搜尋應用程式商店。
3. 按一下「下一步」。
4. 從搜尋結果中，選取「Enterprise Mobile Security」。
5. 在「新增應用程式」畫面上，按一下「指定」標籤，然後從「指定群組」欄位中選取指定群組。
6. 按一下「儲存並發佈」。
7. 按一下「上傳」。

「行動安全防護」會以註冊碼重新封裝 Android 代理程式，並將它上傳到伺服器。如果沒有設定預設註冊碼，「行動安全防護」會在重新封裝 Android 代理程式之前產生註冊碼。

注意

針對 Samsung 行動裝置，您也可以在 AirWatch Web 主控台上設定「行動安全防護」Android 代理程式的自動啟動功能。如需詳細資訊，請參閱以下文章：

http://esupport.trendmicro.com/solution/zh-TW/1115842.aspx

接下來需執行的動作

部署 Android 代理程式後，請提供註冊資訊給使用者（以簡訊或 QR 碼的形式）。使用者可以使用註冊資訊或是掃瞄 QR 碼來向伺服器註冊。註冊資訊包括伺服器 IP 位址、通訊埠號碼，以及註冊碼（可在「部署設定」畫面的「Android 代理程式」標籤找到）。

透過行動安全防護伺服器部署 Android 代理程式

步驟

1. 登入「行動安全防護」管理 Web 主控台。
2. 按一下功能表列上的「管理 > 裝置註冊設定」。
3. 在「驗證」標籤上，選取「使用註冊金鑰驗證」，然後選取「使用預設註冊金鑰」。
4. 按一下「管理 > 部署設定 > Android 代理程式 (標籤)」。
5. 選取「從 TMMS 伺服器下載」，然後選取「自動註冊」。
6. 按一下「儲存」以儲存設定。
7. 按一下「上傳」，然後選取修改後的「行動安全防護」代理程式檔案，以將它上傳到 AirWatch 伺服器。

   行動裝置代理程式隨即上傳並出現在 AirWatch 管理 Web 主控台上。

接下來需執行的動作

部署 Android 代理程式後，請提供註冊資訊給使用者（以簡訊或 QR 碼的形式）。使用者可以使用註冊資訊或是掃瞄 QR 碼來向伺服器註冊。註冊資訊包

括伺服器 IP 位址、通訊埠號碼，以及註冊碼（可在「部署設定」畫面的「Android 代理程式」標籤找到）。

設定 Android 行動裝置自動啟動

開始之前

執行此程序之前，您必須先執行透過行動安全防護伺服器部署 Android 代理程式 第 3-11 頁中所述的所有步驟。

步驟

1. 登入 AirWatch Web 主控台，然後瀏覽至「裝置 > 暫存與佈建 > 元件 > 檔案/處理行動」。
2. 從 AirWatch 主控台設定「檔案/處理行動」。執行以下操作：
   a. 瀏覽至「裝置 > 暫存與佈建 > 元件 > 檔案/處理行動」。
   b. • 按一下「新增 > Android」。
   c. 在「一般」標籤上，為「名稱」和「說明」欄位提供資訊。
   d. 在「資訊清單」標籤上，按一下「安裝資訊清單」區段下的「新增處理行動」。
   e. 在「新增資訊清單」選項上，設定以下資訊，然後按一下「儲存」：
      - 要執行的處理行動：執行方式
      - 要執行的命令列和引數：

        ```
        mode=explicit,broadcast=false,action=android.intent.action.MAIN,package=com.trendmicro.tmmssuite.enterprise,class=com.trendmicro.tmmssuite.enterprise.ui.TmmsEnterpriseSplashScreen
        ```

      - 逾時：[您所需的任何持續時間]
   f. 在「新增檔案/處理行動」畫面上，按一下「儲存」。
3. 設定產品。執行以下操作：

a. 瀏覽至「裝置 > 暫存與佈建 > 產品清單檢視」。

b. • 按一下「新增產品 > Android」。

c. 在「一般」標籤上，為「名稱」、「說明」和「指定群組」欄位提供資訊。

d. 在「資訊清單」標籤上，按一下「新增」來新增資訊清單。

e. 在「新增資訊清單」選項上，設定以下資訊，然後按一下「儲存」：

- 要執行的處理行動：安裝檔案/處理行動
- 檔案/處理行動：

  `TestLauncher`

f. 在「新增產品」畫面上，按一下「儲存」。

4. 設定應用程式。執行以下步驟：

a. 將 TMMS 代理程式指定給智慧型群組。

b. 將「推播模式」設為「自動」。

部署 iOS 代理程式

步驟

1. 登入 AirWatch Web 主控台，然後瀏覽至「應用程式與書籍 > 應用程式 > 清單檢視」。
2. 在「公開」標籤上，按一下「新增應用程式」。
3. 在「新增應用程式」畫面上，設定以下欄位：
   - 管理者：輸入 `Trend Micro`。
   - 平台：選取 Apple iOS。
   - 來源：選取「搜尋應用程式商店」。

- 「名稱」：輸入企業行動安全

4. 按一下「下一步」。

5. 從搜尋結果中，按一下「Mobile Security for Enterprise Agent」前面的「選取」。

6. 在「部署」標籤上，選取「傳送應用程式組態設定」，然後在「應用程式組組態設定」欄位下設定應用程式。

   若要確認應用程式組態設定值，請參閱「行動安全防護」管理 Web 主控台上的「部署設定」畫面，如下圖所示。（管理 > 部署設定）

組態設定金鑰	值類型	組態設定值
CmdType	字串	註冊
EK	字串	<註冊碼>
ServerUrl	字串	<實際伺服器 URL>

組態設定金鑰	值類型	組態設定值
ServerPort	字串	<實際伺服器通訊埠號碼>
DeviceSerialNumber	字串	{DeviceSerialNumber}
DeviceWLANMac	字串	{DeviceWLANMac}

7. 按一下「儲存並發佈」。
8. 在「檢視裝置指定」畫面上，按一下「發佈」。

與 MobileIron 整合

「趨勢科技行動安全防護」讓您能將下列 MobileIron MDM 解決方案與「行動安全防護」進行整合：

- 已代管 MobileIron Core
- MobileIron Core 內部部署

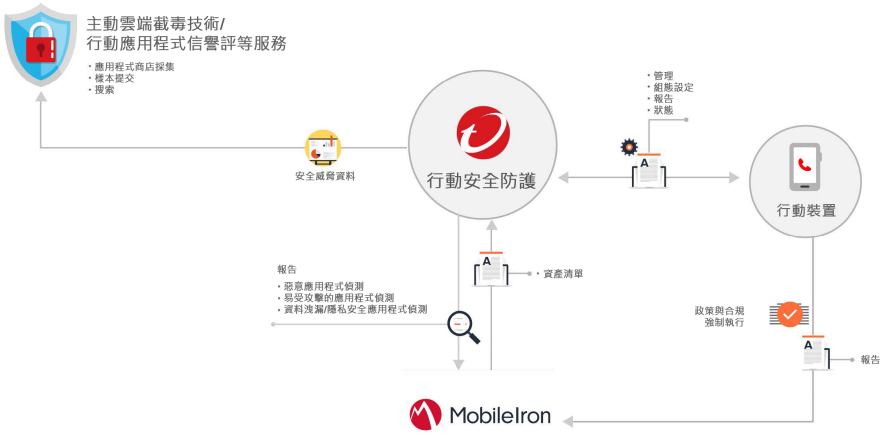
整合先決條件

若要將其他 MDM 解決方案與「趨勢科技行動安全防護」，您必須使用以下項目：

- 企業版行動安全防護 9.7 或更新版本
- 行動安全防護中設有本機通訊伺服器或雲端通訊伺服器
- MobileIron 9.3 或更新版本
- MobileIron 管理 Web 主控台上的系統管理員帳號

MobileIron 整合架構

下圖顯示與 MobileIron 整合的高階架構。



「行動應用程式信譽評等」是以雲端為基礎的技術，可根據應用程式行為自動識別行動裝置威脅、從多個 Android 市場抓取與收集大量的 Android 應用程式、識別現有和全新的行動裝置惡意程式、識別可能濫用隱私/裝置資源的應用程式。這是全球第一個自動行動應用程式評估服務。

「趨勢科技主動雲端截毒技術」提供主動式全球威脅資訊來防範零時差威脅，以確保您始終受到防護。趨勢科技運用即時威脅資訊，可立即消滅攻擊，使其無法危害您。所有趨勢科技產品與服務均以「主動雲端截毒技術」作為後盾。

「行動安全防護」使用主動雲端截毒技術和行動應用程式信譽評等服務來找出行動裝置安全問題，並運用 MobileIron 合規政策管理您的行動裝置。

整合功能

「趨勢科技行動安全防護」提供下列與 AirWatch 整合的功能：

功能	說明
行動裝置自動分組	「行動安全防護」會根據風險等級，對行動裝置加上「Dangerous」、「Risky」和「No_TMMS」尾碼做為標籤。 如需詳細資料，請參閱行動裝置自動分組 第 3-17 頁。
自動部署行動安全防護用戶端應用程式	您可以設定 MobileIron 將行動裝置代理程式自動部署至行動裝置。 • Android: 如需相關程序，請參閱透過行動安全防護伺服器部署 Android 代理程式 第 3-20 頁。 • iOS: 如需相關程序，請參閱部署 iOS 代理程式 第 3-21 頁。

行動裝置自動分組

「行動安全防護」會使用前置碼來建立三 (3) 種級別（Dangerous、Risky 和 NO_TMMS），並將風險裝置標記如下：

- PREDEFINEDPREFIX_Dangerous
- PREDEFINEDPREFIX _Risky
- PREDEFINEDPREFIX _NO_TMMS

「行動安全防護」可讓您在管理 Web 主控台上定義前置碼 (PREDEFINEDPREFIX)。當「行動安全防護」偵測到惡意應用程式時，它會自動變更裝置的智慧型群組。

例如，如果「行動安全防護」偵測到行動裝置上出現惡意程式，它會自動將行動裝置移至 PREDEFINEDPREFIX _Dangerous 群組。

設定 MobileIron 整合

步驟

1. 登入「行動安全防護」管理 Web 主控台。
2. 按一下功能表列上的「管理 > 通訊伺服器設定」，並確認已進行通訊伺服器設定。如果尚未設定，請參閱《*安裝與部署手冊*》中的〈*進行通訊伺服器設定*〉主題，瞭解設定步驟。
3. 按一下「管理 > 部署設定」。
4. 在「伺服器」區段下，選取「安全掃瞄」，然後從下拉式清單中選取「已代管 MobileIron Core」或「MobileIron Core 內部部署」MDM 解決方案。
5. 在「服務註冊」區段下，進行以下 MobileIron 設定：
   - API URL
   - 帳號名稱
   - 密碼
6. 按一下「驗證設定」，確認「行動安全防護」可以連線至 MobileIron 伺服器。
7. 在「資料同步設定」區段下，進行以下設定：
   - 安全類別前置碼

   注意

   「行動安全防護」會使用前置碼來建立三 (3) 種級別（Dangerous、Risky 和 NO_TMMS），並將風險裝置標記如下：

   - XXXX_Dangerous
   - XXXX_Risky
   - XXXX_NO_TMMS

代理程式部署

「趨勢科技行動安全防護」可讓您從兩個不同來源部署用戶端代理程式：

- Google Play 商店：您將需要設定 MobileIron，以便部署行動裝置代理程式和提供註冊資訊給使用者（以簡訊或 QR 碼的形式）。使用者可以使用註冊資訊或是掃瞄 QR 碼來向伺服器註冊。註冊資訊包括伺服器 IP 位址、通訊埠號碼，以及註冊碼（可在「部署設定」畫面的「Android 代理程式」標籤找到）。

  安裝行動裝置代理程式後，使用者就必須手動向「行動安全防護」伺服器註冊。如果您從 Google Play 商店部署行動裝置代理程式，行動裝置使用者便可透過 Google Play 接收即時更新。

- 行動安全防護伺服器：通知使用者從 MobileIron 應用程式商店下載名稱為「企業行動安全」的行動裝置代理程式。

  如果您使用此部署選項，將需要提供註冊資訊給使用者（以簡訊或 QR 碼的形式）。使用者可以使用註冊資訊或是掃瞄 QR 碼來向伺服器註冊。註冊資訊包括伺服器 IP 位址、通訊埠號碼，以及註冊碼（可在「部署設定」畫面的「Android 代理程式」標籤找到）。使用者只要啟動行動裝置代理程式，就必須向「行動安全防護」伺服器註冊應用程式。您也可以設定應用程式自動註冊。不過，每當有更新可用時，行動裝置使用者就必須手動更新其行動裝置代理程式。

透過 Google Play 商店部署 Android 代理程式

步驟

1. 登入 MobileIron Web 主控台，然後按一下功能表列上的「應用程式類別」。
2. 按一下「新增+」，然後選取 Google Play。
3. 在「應用程式名稱」欄位中輸入企業行動安全，然後按一下「搜尋」。
4. 從搜尋結果中，選取「Enterprise Mobile Security」，然後按一下「下一步」。

5. 新增「nterprise Mobile Security」的說明，然後從「類別」下拉式清單中選取要將此應用程式置於哪個類別。
6. 按一下「完成」。
7. 按一下功能表列上的 Apps@Work。
8. 在「APPS@WORK 類別」區段下，選取「將此應用程式設為 Apps@Work 類別的精選應用程式」。
9. 按一下「儲存」。

接下來需執行的動作

部署 Android 代理程式後，請提供註冊資訊給使用者（以簡訊或 QR 碼的形式）。使用者可以使用註冊資訊或是掃瞄 QR 碼來向伺服器註冊。註冊資訊包括伺服器 IP 位址、通訊埠號碼，以及註冊碼（可在「部署設定」畫面的「Android 代理程式」標籤找到）。

透過行動安全防護伺服器部署 Android 代理程式

步驟

1. 登入「行動安全防護」管理 Web 主控台。
2. 按一下功能表列上的「管理 > 裝置註冊設定」。
3. 在「驗證」標籤上，選取「使用註冊金鑰驗證」，然後選取「使用預設註冊金鑰」。
4. 按一下「管理 > 部署設定 > Android 代理程式 (標籤)」。
5. 選取「從 TMMS 伺服器下載」，然後選取「自動註冊」。
6. 按一下「儲存」以儲存設定。
7. 按一下「上傳」，然後選取修改後的「行動安全防護」代理程式檔案，以將它上傳到 AirWatch 伺服器。

   行動裝置代理程式隨即上傳並出現在 AirWatch 管理 Web 主控台上。

接下來需執行的動作

部署 Android 代理程式後，請提供註冊資訊給使用者（以簡訊或 QR 碼的形式）。使用者可以使用註冊資訊或是掃瞄 QR 碼來向伺服器註冊。註冊資訊包括伺服器 IP 位址、通訊埠號碼，以及註冊碼（可在「部署設定」畫面的「Android 代理程式」標籤找到）。

部署 iOS 代理程式

步驟

1. 登入 MobileIron Web 主控台，然後按一下「應用程式類別」。
2. 按一下「新增+」，然後選取 iTunes。
3. 在搜尋欄位中輸入企業行動安全，然後按一下「搜尋」。
4. 選取「Mobile Security for Enterprise Agent」，然後按一下「下一步」。
5. 不變更資訊，按一下「下一步」。
6. 在「APPS@WORK 類別」區段下，選取「將此應用程式設為 Apps@Work 類別的精選應用程式」，然後按一下「下一步」。
7. 按一下「完成」。
8. 登入「行動安全防護」管理 Web 主控台。
9. 按一下「管理 > 部署設定 > iOS 代理程式 (標籤)」。
10. 按一下「下載」以下載組態設定檔。

注意

如果「下載」按鈕未啟用，請確認您已正確進行前面步驟中的所有設定。

11. 在 MobileIron 管理 Web 主控台上，瀏覽至「政策與設定」。
12. 按一下「新增 > iOS 和 OS X > 受管理應用程式組態設定」。
13. 輸入以下資訊：
    - 名稱
    - 說明
    - 套件識別碼
14. 按一下「下載」以下載組態設定檔。
15. 選取新建立的組態設定檔，然後按一下「更多處理行動 > 套用至標籤」。
16. 按一下「套用」。

    「行動安全防護」會將「應用程式安裝」通知推播至 iOS 行動裝置。

第 4 章

管理行動裝置

本章協助您開始使用「行動安全防護」。其內容提供基本的設定和使用指示。在繼續閱讀之前，請務必安裝「管理伺服器」、「通訊伺服器」，以及將「行動裝置代理程式」安裝在行動裝置上。

本章包含以下小節：

受管理裝置標籤

「裝置」畫面上的「受管理裝置」標籤可讓您執行與「行動裝置代理程式」的設定、組織或搜尋相關的工作。裝置樹狀結構檢視器上方的工具列可讓您執行下列工作：

- 設定裝置樹狀結構（例如建立、刪除或重新命名群組，以及建立或刪除行動裝置代理程式）
- 設定「行動裝置代理程式」資訊
- 搜尋及顯示行動裝置代理程式狀態
- 手動的「行動裝置代理程式」元件更新、掃瞄裝置以及更新政策
- 匯出資料以進行進一步分析或備份

行動安全防護的群組

「行動安全防護管理伺服器」會自動建立「行動裝置」根群組，以及下列子群組：

- 預設 — 此群組包含不屬於任何其他群組的「行動裝置代理程式」。您無法將「行動安全防護」裝置樹狀結構中的預設群組刪除或重新命名。

如需相關指示，請參閱「行動安全防護管理伺服器」的《線上說明》。

管理群組

您可以在「行動裝置」根群組下新增、編輯或刪除群組。然而，您無法將「行動裝置」根群組與「預設」群組重新命名或刪除。

新增群組

步驟

1. 登入「行動安全防護」管理 Web 主控台。
2. 按一下功能表列上的「裝置」。

   「裝置」畫面隨即出現。
3. 在「受管理裝置」標籤上按一下「行動裝置」根群組，再按一下「新增群組」。
4. 設定下列項目：
   - 「父群組」：選取您要在其下建立子群組的群組。
   - 「群組名稱」：輸入群組的名稱。
   - 「政策」：從下拉式清單中選取您要套用到群組的政策。
5. 按一下「新增」。

重新命名群組

步驟

1. 登入「行動安全防護」管理 Web 主控台。
2. 按一下功能表列上的「裝置」。

   「裝置」畫面隨即出現。
3. 在「受管理裝置」標籤上，按一下您要重新命名的群組。
4. 按一下「編輯」。
5. 修改群組名稱，再按一下「重新命名」。

刪除群組

步驟

1. 登入「行動安全防護」管理 Web 主控台。
2. 按一下功能表列上的「裝置」。

   「裝置」畫面隨即出現。
3. 在「受管理裝置」標籤上，按一下您要刪除的群組。
4. 按一下「刪除」，再按一下確認畫面上的「確定」。

管理行動裝置

您可以在「裝置」畫面上編輯行動裝置資訊、刪除行動裝置，或變更行動裝置群組。

重新指定裝置

步驟

1. 在「行動安全防護」管理 Web 主控台上，移至「裝置 > 受管理裝置」。

   「裝置」畫面隨即出現。
2. 從裝置樹狀結構中，選取要重新指定的裝置。

   裝置資訊隨即出現。
3. 按一下「變更使用者」，然後在提供的欄位中修改使用者名稱。
4. 按一下「儲存」。

編輯行動裝置資訊

步驟

1. 登入「行動安全防護」管理 Web 主控台。
2. 按一下功能表列上的「裝置」。

   「裝置」畫面隨即出現。
3. 在「受管理裝置」標籤上，從裝置樹狀結構中按一下您所要編輯資訊的行動裝置。
4. 按一下「編輯」。
5. 更新以下欄位中的資訊：
   - 「電話號碼」 — 行動裝置的電話號碼。
   - 「裝置名稱」 — 用以在裝置樹狀結構中識別行動裝置的名稱。
   - 「群組」 — 下拉式清單中行動裝置隸屬的群組名稱。
   - 「資產號碼」 — 輸入指派給行動裝置的資產號碼。
   - 「說明」—任何與行動裝置或使用者相關的其他資訊或注意事項。
6. 按一下「儲存」。

刪除行動裝置

「行動安全防護」提供下列兩個選項可供刪除行動裝置：

- 刪除單一行動裝置 第 4-6 頁
- 刪除多個行動裝置 第 4-6 頁

刪除單一行動裝置

步驟

1. 登入「行動安全防護」管理 Web 主控台。
2. 按一下功能表列上的「裝置」。

   「裝置」畫面隨即出現。
3. 在「受管理裝置」標籤上，從裝置樹狀結構中按一下您要刪除的行動裝置。
4. 按一下「刪除」，再按一下確認對話方塊上的「確定」。

行動裝置隨即自行動裝置樹狀結構中刪除，且與「Mobile Security 管理伺服器」之間再也沒有註冊關係。

刪除多個行動裝置

步驟

1. 登入「行動安全防護」管理 Web 主控台。
2. 按一下功能表列上的「裝置」。

   「裝置」畫面隨即出現。
3. 在「受管理裝置」標籤上，從裝置樹狀結構中按一下您要刪除其行動裝置的群組。
4. 在右窗格的清單選取行動裝置，按一下「刪除」，然後按一下確認對話方塊中的「確定」。

   行動裝置隨即自行動裝置樹狀結構中刪除，且與「行動安全防護管理伺服器」之間再也沒有註冊關係。

將行動裝置移至另一個群組

您可以將某個群組的行動裝置移至另一個群組。「行動安全防護」會自動將有關您已套用到群組的政策相關通知傳送給使用者。

步驟

1. 登入「行動安全防護」管理 Web 主控台。
2. 按一下功能表列上的「裝置」。

   「裝置」畫面隨即出現。
3. 在「受管理裝置」標籤上，按一下您要將其行動裝置移至另一個群組的群組。
4. 從右窗格的清單中選取行動裝置，然後按一下「移動」。

   「移動裝置」對話方塊隨即顯示。
5. 從下拉式清單中選取目標群組，然後按一下「確定」。

行動裝置狀態

在「裝置」畫面中「受管理裝置」標籤上，選取行動裝置可將裝置的狀態資訊顯示在右側窗格中。行動裝置的資訊分佈於以下區段中：

- 「基本」— 包括註冊狀態、電話號碼、LDAP 帳號及平台資訊。
- 「硬體、作業系統」— 顯示詳細的行動裝置資訊，包括裝置和機型名稱、作業系統版本、記憶體資訊、行動電話通訊技術、IMEI 和 MEID 號碼及韌體版本資訊。
- 「安全」— 顯示行動裝置在以下方面的狀態：破解/開放 Root 權限、開發人員選項、USB 偵錯、網路流量解密問題；惡意 iOS 資料檔數目、惡意 SSL 憑證數目、惡意應用程式數目、被竄改的應用程式數目、易受攻擊的應用程式數目、會洩漏隱私的應用程式數目；以及已連線的無線網路存取點 (Wi-Fi)。

基本行動裝置代理程式搜尋

若要根據行動裝置的名稱或電話號碼來搜尋「行動裝置代理程式」，請在「裝置」畫面提供的搜尋欄位中輸入資訊，然後按一下「搜尋」。搜尋結果會顯示在裝置樹狀結構中。

進階行動裝置代理程式搜尋

您可以使用「進階搜尋」畫面來指定其他「行動裝置代理程式」搜尋條件。

步驟

1. 在「裝置」畫面中按一下「進階搜尋」連結。快顯視窗隨即顯示。
2. 選取搜尋條件，然後在提供的欄位中輸入值（如果適用）：
   - 「裝置名稱」 — 用以識別行動裝置的描述性名稱
   - 「電話號碼」 — 行動裝置的電話號碼
   - 「使用者名稱」— 行動裝置的使用者名稱
   - 「資產號碼」 — 行動裝置的資產號碼
   - IMEI — 行動裝置的 IMEI 號碼
   - 「序號」 — 行動裝置的序號
   - 「Wi-Fi MAC 位址」 — 行動裝置的 Wi-Fi MAC 位址
   - 「說明」 — 行動裝置的說明
   - 「作業系統」 — 將搜尋範圍限制為行動裝置執行的特定作業系統；或限制為 Android 和 iOS 的版本號碼。
   - 「群組」 — 行動裝置隸屬的群組
   - 「代理程式版本」 — 行動裝置上的「行動裝置代理程式」版本號碼
   - 「上次連線時間」— 行動裝置上次連線到「行動安全防護」伺服器的時間範圍

- 「惡意程式病毒碼版本」 — 行動裝置上的「惡意程式病毒碼」檔案版本號碼
- 「惡意程式掃瞄引擎版本」 — 行動裝置上的「惡意程式掃瞄引擎」版本號碼
- 「應用程式名稱」 — 安裝在行動裝置上的應用程式
- 「中毒行動裝置代理程式」 — 將搜尋範圍限制為偵測到之惡意程式數量為指定數量的行動裝置

3. 按一下「搜尋」。搜尋結果會顯示在裝置樹狀結構中。

行動裝置代理程式工作

「趨勢科技行動安全防護」可讓您從「裝置」畫面在行動裝置上執行不同的工作。

更新行動裝置代理程式

您可以從「裝置」畫面的「受管理裝置」標籤，將更新通知傳送給元件或安全防護政策過期的行動裝置。

步驟

1. 登入「行動安全防護」管理 Web 主控台。
2. 按一下功能表列上的「裝置」。

   「裝置」畫面隨即出現。
3. 在「受管理裝置」標籤上，按一下您要更新其行動裝置的群組。
4. 按一下「更新」。

「行動安全防護」會將更新通知傳送給其元件或安全防護政策過期的所有行動裝置。

您也可使用「更新」畫面設定「行動安全防護」，以自動將更新通知傳送到其元件或政策過期的行動裝置，或手動開始程序。

如需詳細資訊，請參閱更新行動安全防護元件 第 8-2 頁。

更新行動裝置資訊

「行動安全防護」伺服器會按照排定的間隔時間，自動從受管理行動裝置取得裝置資訊，然後在「裝置」畫面顯示裝置資訊。

您可以在下一個預約的自動更新之前，於「受管理裝置」標籤更新受管理裝置的裝置資訊。

步驟

1. 登入「行動安全防護」管理 Web 主控台。
2. 按一下功能表列上的「裝置」。

   「裝置」畫面隨即出現。
3. 在「受管理裝置」標籤上，從裝置樹狀結構中選取行動裝置。
4. 按一下「更新」。

匯出資料

您可以從「裝置」畫面的「受管理裝置」標籤匯出資料，以供進一步分析或備份。

步驟

1. 登入「行動安全防護」管理 Web 主控台。

2. 按一下功能表列上的「裝置」。

   「裝置」畫面隨即出現。

3. 從裝置樹狀結構中選取您要匯出其資料的行動裝置群組。

4. 按一下「匯出」。

5. 視需要按一下所顯示快顯視窗中的「儲存」，將 .zip 檔案儲存在您的電腦上。

6. 將下載的 .zip 檔案內容解壓縮，並開啟 .csv 檔案檢視行動裝置資訊。

與 Trend Micro Control Manager 整合

「趨勢科技行動安全防護」可與 Trend Micro Control Manager（亦稱做 Control Manager 或 TMCM）整合。此整合可讓 Control Manager 管理員：

- 建立、編輯或刪除「行動安全防護」的安全防護政策
- 將安全防護政策傳送給已註冊的行動裝置
- 檢視「行動安全防護」的「報表」畫面

如需有關 Trend Micro Control Manager 及如何在 Control Manager 上處理「行動安全防護」政策的詳細資訊，請參閱下列 URL 的產品文件：

http://docs.trendmicro.com/en-us/enterprise/control-manager.aspx

在 Control Manager 中建立安全防護政策

Trend Micro Control Manager Web 主控台顯示與「行動安全防護」提供相同的安全防護政策。如果 Control Manager 系統管理員為「行動安全防護」建立安全防護政策，則「行動安全防護」會為此政策建立新的群組，並將所有目標行動裝置移至此群組。為了區分「行動安全防護」中建立的政策與在 Control Manager 中建立的政策，「行動安全防護」會在群組名稱前加 TMCM_ 首碼。

刪除或修改安全防護政策

Control Manager 系統管理員可隨時修改政策，政策會立即部署到行動裝置上。

Trend Micro Control Manager 每 24 小時會將政策與「趨勢科技行動安全防護」同步。如果您刪除或修改使用 Control Manager 建立與部署的政策，則在同步後政策會回復為原始設定或再次建立。

Control Manager 的安全防護政策狀態

在 Trend Micro Control Manager Web 主控台上，會顯示安全防護政策的下列狀態：

- 「暫停中」：政策建立在 Control Manager Web 主控台上，尚未傳送至行動裝置。
- 「已部署」：政策已傳送，並部署在所有的目標行動裝置上。

第 5 章

檢視使用者

本章示範如何檢視已向「行動安全防護」註冊的使用者。

本章包含以下小節：

使用者標籤

您可以使用「使用者」標籤，檢視所有已向「行動安全防護」註冊的行動裝置。

檢視使用者清單

步驟

1. 在「行動安全防護」管理 Web 主控台上，移至「使用者」。

   「使用者」畫面隨即出現。

2. 若要將清單排序，請按一下任何資料行標題。

   - 使用者名稱
   - 電子郵件
   - 裝置
   - 上次邀請日期

3. 若要搜尋使用者，請在「搜尋」列中輸入使用者名稱或電子郵件地址，然後按下 Enter。

   如果使用者存在於清單中，則「行動安全防護」會顯示資訊。

第 6 章

利用政策來保護裝置

本章示範如何設定安全政策，以及如何將安全政策套用至「行動安全防護」群組中的行動裝置。您可以使用與佈建、裝置安全及資料防護相關的政策。

本章包含以下小節：

關於政策

您可以針對「管理伺服器」上的某個「行動安全防護」群組，或針對所有已向「行動安全防護」註冊的行動裝置設定政策。

表 6-1. 行動安全防護中的裝置政策

政策	參考
核可的清單	請參閱應用程式核可的清單 第 6-2 頁。
信任的網路流量解密問題憑證清單	請參閱信任的網路流量解密問題憑證清單 第 6-3 頁。

表 6-2. 行動安全防護中的群組政策

政策群組	政策	參考
一般	一般政策	請參閱一般政策 第 6-6 頁。
裝置安全	安全政策	請參閱安全政策 第 6-6 頁。

適用於所有裝置的政策

本節介紹「行動安全防護」中針對所有行動裝置提供的政策。

應用程式核可的清單

「應用程式核可的清單」包含所有被偵測為具有安全風險（惡意程式、易受攻擊、有隱私風險或被竄改的應用程式）、但經系統管理員核可安裝到行動裝置上的應用程式。

若要管理「應用程式核可的清單」，請按一下「政策 > 適用於所有裝置的政策」。

信任的網路流量解密問題憑證清單

如果「行動安全防護」將偵測到的 SSL 憑證視為惡意，就會將這些憑證顯示在「偵測 > 惡意 SSL 憑證」畫面上。不過，您可以將這些「惡意」的憑證新增至「信任的網路流量解密問題憑證清單」，讓「行動安全防護」在掃瞄期間略過這些憑證，並且在「惡意 SSL 憑證」畫面上將這些憑證隱藏起來。

若要管理「信任的網路流量解密問題憑證清單」，請按一下「政策 > 適用於所有裝置的政策」。

管理適用於所有裝置的政策

「行動安全防護」可讓您維護應用程式核可的清單以及信任的網路流量解密問題憑證清單，以便讓使用者得以使用這些應用程式與網路解密憑證，而不會受到限制或看到警告。

使用「適用於所有裝置的政策」畫面，即可針對行動裝置建立、編輯、複製或刪除政策。

新增應用程式至核可的清單

步驟

1. 登入「行動安全防護」管理 Web 主控台。
2. 請執行以下任一項工作：
   - 將已安裝並經過「行動安全防護」掃瞄的應用程式新增至「核可的清單」。
     a. 按一下功能表列上的「偵測 > 應用程式安全狀態」。
     b. 按一下「Android」或「iOS」標籤，然後在偵測到的應用程式清單中，選取要新增至「核可的清單」的應用程式。
     c. 按一下「新增至『核可的清單』」。
   - 手動新增應用程式至「核可的清單」。

a. 按一下功能表列上的「政策 > 適用於所有裝置的政策」。

b. 在「應用程式核可的清單」區段下，按一下「Android」或「iOS」標籤，然後按一下「新增至『核可的清單』」。

「匯入應用程式」畫面隨即出現。

c. 在提供的欄位中，輸入應用程式識別碼、名稱與說明。請使用分號 (;) 分隔每項應用程式資訊。

d. 按一下「匯入應用程式」畫面上的「儲存」。

e. 按一下「適用於所有裝置的政策」畫面上的「儲存」。

從核可的清單移除應用程式

步驟

1. 登入「行動安全防護」管理 Web 主控台。
2. 請執行以下任一項工作：
   - 從「核可的清單」移除已安裝並經過「行動安全防護」掃瞄的應用程式
     a. 按一下功能表列上的「偵測 > 應用程式安全狀態」。
     b. 按一下「Android」或「iOS」標籤，然後在偵測到的應用程式清單中，選取要從「核可的清單」移除的應用程式。
     c. 按一下「從『核可的清單』移除」。
   - 直接從「核可的清單」移除應用程式。
     a. 按一下功能表列上的「政策 > 適用於所有裝置的政策」。
     b. 在「應用程式核可的清單」區段下，按一下「Android」或「iOS」標籤，然後選取要從該清單移除的應用程式。
     c. 按一下「從『核可的清單』移除」。

d. 按一下「適用於所有裝置的政策」畫面上的「儲存」。

新增信任的網路流量解密問題憑證

步驟

1. 登入「行動安全防護」管理 Web 主控台。
2. 按一下功能表列上的「政策 > 適用於所有裝置的政策」。

   「適用於所有裝置的政策」畫面隨即出現。
3. 在「信任的網路流量解密問題憑證清單」區段下，按一下「新增」。

   「新增憑證」畫面隨即出現。
4. 選取本機硬碟上的憑證檔案，然後在「說明」欄位中輸入憑證檔案的說明。
5. 按一下「確定」。
6. 按一下「適用於所有裝置的政策」畫面上的「儲存」。

刪除信任的網路流量解密問題憑證

步驟

1. 登入「行動安全防護」管理 Web 主控台。
2. 按一下功能表列上的「政策 > 適用於所有裝置的政策」。

   「適用於所有裝置的政策」畫面隨即出現。
3. 在「信任的網路流量解密問題憑證清單」區段下，選取您要刪除的憑證檔案，然後按一下「刪除」。
4. 按一下「適用於所有裝置的政策」畫面上的「儲存」。

適用於所有群組的政策

本節介紹「行動安全防護」中針對所有群組提供的政策。

使用超級使用者帳號，您可以指定任何政策作為範本，供群組管理員在 Mobile Security 中建立更多安全防護政策。但是，一旦您指定某個安全防護政策作為範本，便無法再將該安全防護政策指定給任何群組。

一般政策

「一般政策」提供行動裝置的一般安全防護政策。若要設定一般安全防護政策設定，請按一下「政策」，再按一下政策名稱，最後按一下「一般政策」。

- 「使用者權限」：
  - 您可以選取是否要允許使用者設定「行動安全防護」裝置代理程式設定。

    如果您未選取「允許使用者進行「行動安全防護」用戶端設定」核取方塊，使用者便無法變更「行動裝置代理程式」設定。然而當此選項已選取時，「Web 威脅防護政策」的過濾清單不會受到影響。如需詳細資訊，請參閱安全政策 第 6-6 頁。
  - 您可以選取自動檢查選項，讓「行動裝置代理程式」定期檢查「行動安全防護管理伺服器」上是否有任何元件或組態設定更新。

安全政策

您可以從「安全政策」畫面設定「安全設定」。

注意

行動安全防護 Web 威脅防護僅支援行動裝置上的預設 Android 瀏覽器與 Google Chrome。

若要進行安全防護政策設定，請按一下「政策」，接著按一下政策名稱，然後按一下「安全政策」。

下表說明此政策的可用設定。

表 6-3. 安全政策設定

區段	項目	說明	支援的行動裝置作業系統
安全設定	僅掃瞄已安裝的應用程式	如果只想掃瞄已安裝的應用程式，請選取此選項	
	掃瞄已安裝的應用程式和檔案	如果想要掃瞄已安裝的應用程式以及行動裝置上儲存的其他檔案，請選取此選項。 如果選取此選項，請指定僅掃瞄 APK 檔案還是掃瞄所有檔案。	
	病毒碼更新完成後進行掃瞄	如果您想要在每個病毒碼更新完成後執行惡意程式掃瞄，請啟動此選項。 當 Android 行動裝置上的病毒碼成功更新後，「行動安全防護」會自動執行掃瞄。	
	應用程式掃瞄	如果您想要掃瞄應用程式是否有惡意程式、隱私風險、易受攻擊以及被竄改（重新封裝）的應用程式，請啟動此選項。	
	網路安全掃瞄	這些設定會掃瞄是否有網路流量解密問題、不安全的無線網路存取點 (Wi-Fi) 或已安裝的惡意 SSL 憑證。此類別下的所有選項均為預設啟動的選項，且無法修改。	
	易受攻擊的應用程式掃瞄	這些設定會掃瞄行動裝置上是否有因以下原因而起的弱點：USB 偵錯、開發人員選項、惡意資料	

區段	項目	說明	支援的行動裝置作業系統
		檔，以及已開放 Root 權限或已破解的行動裝置。	
	偵測到網路流量解密問題時封鎖網路	啟動此選項，行動安全防護就會在通訊期間偵測到資料外洩時，防堵網路流量解密問題。	
	將可疑的無線網路存取點 (Wi-Fi) 偵測為高度風險時封鎖網路	啟動此選項，即可在偵測到網路連線疑似不實時，中斷行動裝置與網路的連線。	
	「掃瞄預約」下的「啟用預約掃瞄」	選取「每天一次」、「每週一次」或「每月一次」，以指定要每天、每週還是每月執行掃瞄一次。	
Web 威脅防護設定	啟動集中控管 Web 威脅防護政策	這項功能可讓您從伺服器端控制 Web 威脅防護政策。您可以依照本身需求來設定以下防護等級： • 低：針對線上詐騙及網站上的其他惡意活動攻擊，此設定僅可提供最低的防護。 • 一般：此設定提供線上安全威脅防護，且無需封鎖大多數的網站。趨勢科技建議您使用此預設設定。 • 高：針對線上詐騙及其他網站的攻擊，此設定可提供最高的防護；只允許開啟信譽評等良好的網站，並封鎖其他所有信譽評等不良網站。	
	過濾清單	「行動安全防護」會封鎖所有新增至「封鎖的清單」的 URL，並允許位於「核可的清單」中的所有 URL。	

區段	項目	說明	支援的行動裝置作業系統
	重新評估 URL	若您遇到認為被錯誤分類的 URL，可將任何此類 URL 透過以下網站通知趨勢科技： http://sitesafety.trendmicro.com/	

Web 威脅防護政策

可讓您從「行動安全防護管理伺服器」管理 Web 威脅防護政策，並將其部署到 Android 行動裝置上。另外也可讓 Android 行動裝置將 Web 威脅防護記錄傳回至伺服器。

注意

行動安全防護 Web 威脅防護僅支援預設的 Android 瀏覽器和 Google Chrome。

若要設定「Web 威脅防護政策」設定，請按一下「政策」，再按一下「政策名稱」，最後按一下「Web 威脅防護政策」。

管理適用於所有群組的政策

「行動安全防護」可讓您使用預設的政策範本快速建立政策。

使用「適用於所有群組的政策」畫面，即可針對行動裝置建立、編輯、複製或刪除政策。

建立政策

步驟

1. 登入「行動安全防護」管理 Web 主控台。

2. 按一下功能表列上的「政策 > 適用於群組的政策」。

   「政策」畫面隨即出現。

3. 按一下「建立」。

   「建立政策」畫面隨即顯示。

4. 在政策名稱與說明欄位中輸入其各自的內容，再按一下「儲存」。

   「行動安全防護」會以預設的設定建立政策。然而，政策並未指派給群組。若要將政策指派給群組，請參閱在群組中指派或移除政策 第 6-11 頁。

5. （僅限超級系統管理員）如果您要將此政策用作範本，請按一下「政策」畫面上「類型」欄下的箭號按鈕。群組管理員可以使用「超級系統管理員」建立的範本為其指派的群組建立政策。

   注意

   - 無法將範本指派給任何群組。
   - 還可以將範本轉換為政策。但是，如果某個範本未指派給任何群組，則只能將其轉換為政策。

編輯政策

步驟

1. 登入「行動安全防護」管理 Web 主控台。
2. 按一下功能表列上的「政策 > 適用於群組的政策」。

   「政策」畫面隨即出現。

3. 在政策清單中，按一下您所要編輯詳細資訊的政策名稱。

   「編輯政策」畫面隨即顯示。

4. 修改政策詳細資訊，再按一下「儲存」。

在群組中指派或移除政策

步驟

1. 登入「行動安全防護」管理 Web 主控台。
2. 按一下功能表列上的「政策 > 適用於群組的政策」。

   「政策」畫面隨即出現。
3. 在政策的「套用的群組」欄上，按一下群組名稱。如果政策尚未指派給群組，請按一下「無」。
4. 請執行以下任一項工作：
   - 若要將政策指派給群組：從左側的「可用的群組」清單中，選取您要套用政策的群組，然後按一下 > 將該群組移至右側。
   - 若要將政策從群組中移除：從右側的群組清單中，選取您要移除的群組，然後按一下 < 將群組移至左側「可用的群組」清單。
5. 按一下「儲存」。

複製政策

步驟

1. 登入「行動安全防護」管理 Web 主控台。
2. 按一下功能表列上的「政策 > 適用於群組的政策」。

   「政策」畫面隨即出現。
3. 選取您要複製的政策，再按一下「複製」。

刪除政策

您無法刪除「預設」政策，以及任何套用到該群組的政策。在刪除政策前，請確定先將該政策自所有的群組中移除。如需相關程序，請參閱在群組中指派或移除政策 第 6-11 頁。

步驟

1. 登入「行動安全防護」管理 Web 主控台。
2. 按一下功能表列上的「政策 > 適用於群組的政策」。

   「政策」畫面隨即出現。
3. 選取您要刪除的政策，再按一下「刪除」。

第 7 章

檢視及管理偵測

本章示範如何管理在 iOS 與 Android 行動裝置上偵測到的惡意應用程式，以及如何檢視 SSL 憑證和 iOS 資料檔。

本章包含以下小節：

關於「可疑的應用程式」畫面

「可疑的應用程式」畫面會針對所有安裝在行動裝置上的應用程式，顯示該等應用程式的名稱、版本、安全掃瞄狀態、安裝數目以及上次掃瞄時間。

如果您認為此畫面上顯示的任何應用程式其實很安全，也可以將該等應用程式新增至「核可的清單」。同理，您也可以將先前新增至「核可的清單」、但現在覺得不安全的應用程式移除。

如需相關程序，請參閱新增應用程式至核可的清單 第 6-3 頁和從核可的清單移除應用程式 第 6-4 頁。

按一下表格右上角的「管理核可的清單」連結，即可瀏覽至「核可的清單」畫面來管理清單。

下表列出 Android 和 iOS 應用程式的可用資訊。

表 7-1. 應用程式安全狀態

資訊	說明	ANDROID	IOS
應用程式名稱	應用程式的名稱	●	●
版本	應用程式版本號碼	●	●
惡意程式掃瞄結果	惡意程式掃瞄可能產生下列任何一種結果： • 一般 — 未偵測到惡意程式 • PUA — 潛在的垃圾應用程式（簡稱 PUA）是指可能對使用者安全和/或隱私帶來巨大風險的可能的資安威脅程式應用程式。 如需詳細資訊，請參閱 http://about-threats.trendmicro.com/zh-tw/definition/potentially-unwanted-app。 • 惡意程式 — 已知的惡意程式 • 未知 — 無可用資訊	●	●

資訊	說明	ANDROID	iOS
弱點掃瞄結果	弱點掃瞄可能產生下列任何一種風險評等： • 一般 • 中 • 高 • 未知 – 無可用資訊	●	
隱私掃瞄結果	隱私掃瞄可能產生下列任何一種風險評等： • 一般 • 中 • 高 • 未知 – 無可用資訊	●	
被竄改	被竄改的應用程式掃瞄可能產生下列任何一種結果： • 有– 原始應用程式已被竄改或重新封裝以用於可能的惡意用途 • 沒有 – 原始應用程式未被竄改 • 未知 – 無可用資訊	●	●
安裝數量	已安裝應用程式的裝置數量	●	●
上次掃瞄時間	上次掃瞄的日期和時間	●	●

「行動安全防護」掃瞄應用程式是否有安全風險時，會根據安全掃瞄結果採取下列處理行動：

- 在「Android/iOS 應用程式風險摘要」Widget 的「報表」畫面顯示該筆偵測
- 在「裝置」畫面的相關類別下，顯示針對行動裝置所偵測到的安全風險數目
- 產生記錄項目

檢視可疑的 Android 應用程式

步驟

1. 在「行動安全防護」Web 主控台上，移至「偵測 > 可疑的應用程式 > Android」標籤。

   「Android」標籤隨即出現。

2. 若要檢視應用程式的掃瞄詳細資訊，請按一下下列任何資料行下的結果。

   - 弱點掃瞄結果
   - 隱私掃瞄結果

   所選結果的掃瞄詳細資訊頁面隨即出現。

3. 若要檢視已安裝某個應用程式的裝置，請在「安裝數量」欄下方按一下數量。

   「裝置」畫面隨即顯示，並在「受管理裝置」標籤下方顯示裝置的清單。

4. 若要檢視關於特定應用程式的資訊，請在「搜尋」列中輸入應用程式名稱，然後按下 Enter。

   如果應用程式存在於清單中，表格中會顯示應用程式資訊。

檢視可疑的 iOS 應用程式

步驟

1. 在「行動安全防護」Web 主控台上，移至「偵測 > 可疑的應用程式 > iOS」標籤。

   「iOS」標籤隨即出現。

2. 若要檢視已安裝某個應用程式的裝置，請在「安裝數量」欄下方按一下數量。

「裝置」畫面隨即顯示，並在「受管理裝置」標籤下方顯示裝置的清單。

3. 若要檢視關於特定應用程式的資訊，請在「搜尋」列中輸入應用程式名稱，然後按下 Enter。

   如果應用程式存在於清單中，表格中會顯示應用程式資訊。

檢視惡意 SSL 憑證

「惡意 SSL 憑證」畫面會顯示「行動安全防護」在 Android 或 iOS 行動裝置上所偵測到已安裝、但視為惡意的 SSL 憑證。如果您信任「惡意 SSL 憑證」畫面所列的任何憑證，可以將該等憑證新增至信任的網路流量解密問題憑證清單 第 6-3 頁，使其在「惡意 SSL 憑證」畫面上隱藏起來。

「行動安全防護」偵測到惡意憑證時，會採取下列處理行動：

- 在「惡意 SSL 憑證」畫面上顯示該惡意 SSL 憑證
- 在「網路安全防護摘要」Widget 的「報表」畫面顯示該筆偵測
- 將裝置安全狀態更新為「危險」
- 傳送通知電子郵件給系統管理員
- 產生記錄項目

「惡意 SSL 憑證」畫面上顯示的憑證詳細資訊包括憑證名稱與詳細資訊、行動裝置上的安裝數目，以及上次掃瞄時間。

步驟

1. 在「行動安全防護」Web 主控台上，移至「偵測 > 惡意 SSL 憑證」。

   「惡意 SSL 憑證」畫面隨即出現。

2. 按一下「Android」或「iOS」標籤。

3. 若要檢視關於特定應用程式的資訊，請在「搜尋」列中輸入應用程式名稱，然後按下 Enter。

如果應用程式存在於清單中，表格中會顯示應用程式資訊。

檢視惡意 iOS 資料檔

「惡意 iOS 資料檔」畫面會顯示「行動安全防護」在 iOS 行動裝置上所偵測到已安裝、但視為惡意的 iOS 資料檔。

「行動安全防護」偵測到惡意 iOS 資料檔時，會採取下列處理行動：

- 在「惡意 iOS 資料檔」畫面上顯示該惡意 iOS 資料檔
- 在「iOS 網路安全防護摘要」Widget 的「報表」畫面顯示該筆偵測
- 將裝置狀態更新為「危險」
- 傳送通知電子郵件給系統管理員
- 產生記錄項目

「惡意 iOS 資料檔」畫面上顯示的資料檔詳細資訊包括資料檔名稱、其類型、掃瞄結果、行動裝置上的安裝數目，以及上次掃瞄時間。

步驟

1. 在「行動安全防護」Web 主控台上，移至「偵測 > 惡意 iOS 資料檔」。

   「惡意 iOS 資料檔」畫面隨即出現。

2. 若要檢視關於特定 iOS 資料檔的資訊，請在「搜尋」列中輸入憑證名稱，然後按下 Enter。

   如果憑證存在於清單中，表格中便會顯示應用程式資訊。

第 8 章

更新元件

本章示範如何更新「行動安全防護」元件。

本章包含以下小節：

關於元件更新

在「行動安全防護」中，會透過趨勢科技的網路式元件更新功能「主動式更新」來更新下列元件或檔案：

- 「行動安全防護伺服器」— 行動安全防護通訊伺服器的程式安裝套件。
- 「惡意程式病毒碼」— 含有數千個惡意程式簽章的檔案，能決定「行動安全防護」偵測危險檔案的能力。趨勢科技會定期更新病毒碼檔案，以確實抵禦最新威脅。
- 「行動裝置代理程式」安裝程式 —「行動裝置代理程式」的程式安裝套件。

更新行動安全防護元件

您可以在「行動安全防護管理伺服器」上設定預約或手動元件更新，以從主動式更新伺服器取得最新的元件檔案。在將新版本的元件下載至「管理伺服器」後，「管理伺服器」會自動通知行動裝置更新元件。

手動更新

您可以在「更新」畫面的「手動」標籤上執行手動伺服器與「行動裝置代理程式」更新。您應先在「來源」畫面中設定下載來源（如需詳細資訊，請參閱指定下載來源 第 8-4 頁）。

步驟

1. 登入「行動安全防護」管理 Web 主控台。
2. 按一下「管理 > 更新」。

   「更新」畫面隨即出現。
3. 按一下「手動」標籤。

4. 選取要更新元件的核取方塊。選取「惡意程式防護元件」、「代理程式安裝套件」及/或「伺服器版本」等核取方塊，以選取該群組內的所有元件。此畫面也會顯示每個元件的目前版本，以及上次更新元件的時間。如需各個更新元件的詳細資訊，請參閱關於元件更新 第 8-2 頁。

5. 按一下「更新」，以啟動元件更新程序。

預約更新

預約更新能在無使用者互動的情況下執行定期更新，因此能減輕您的負擔。您應先在「來源」畫面中設定下載來源（如需詳細資訊，請參閱指定下載來源 第 8-4 頁）。

步驟

1. 登入「行動安全防護」管理 Web 主控台。

2. 按一下「管理 > 更新」。

   「更新」畫面隨即出現。

3. 按一下「已預約」標籤。

4. 選取要更新元件的核取方塊。選取「惡意程式防護元件」、「代理程式安裝套件」及/或「伺服器版本」等核取方塊，以選取該群組內的所有元件。此畫面也會顯示每個元件的目前版本，以及元件的上次更新時間。

5. 在「更新預約」下設定執行伺服器更新的時間間隔。選項包括「每小時一次」、「每天一次」、「每週一次」及「每月一次」。

   - 對於每週一次的更新，請指定星期幾（例如星期日、星期一等）。
   - 對於每月一次的更新，請指定每個月的哪一天（例如每個月的第一天（1 日）等）。

注意

「為時 x 小時的更新」功能適用於「每天一次」、「每週一次」及「每月一次」等選項。這表示更新作業會在於「開始時間」欄位中選取的時間到達後，於指定的小時數內的某個時間發生。這項功能有助於平衡主動式更新伺服器的負載。

- 當您想要「行動安全防護」開始更新程序時，請選取「開始時間」。

6. 按一下「儲存」以儲存設定。

指定下載來源

您可以將「行動安全防護」設定為使用預設的主動式更新伺服器來源，或使用指定的伺服器更新下載來源。

步驟

1. 登入「行動安全防護」管理 Web 主控台。
2. 按一下「管理 > 更新」。

   「更新」畫面隨即出現。如需更新的詳細資訊，請參閱手動更新 第 8-2 頁；如需預約更新的詳細資訊，請參閱預約更新 第 8-3 頁。
3. 按一下「來源」標籤。
4. 選取以下其中一個下載來源：
   - 「趨勢科技主動式更新伺服器」— 預設的更新來源。
   - 「其他更新來源」 — 指定 HTTP 或 HTTPS 網站（如近端 Intranet 網站），包括供「行動裝置代理程式」用來下載更新的通訊埠號碼。

注意

更新來源（Web 伺服器）上必須有更新過的元件。提供主機名稱或 IP 位址，以及目錄（如 `https://12.1.123.123:14943/source`）。

- 「包含目前檔案副本的 Intranet 位置」— 本機 Intranet 更新來源。指定下列項目：
  - 「UNC 路徑」：輸入來源檔所在的路徑。
  - 「使用者名稱」和「密碼」：如果來源位置需要驗證，請輸入使用者名稱與密碼。

手動更新本機 AU 伺服器

如果伺服器/裝置是透過本機 AutoUpdate 伺服器更新，但「管理伺服器」無法連線到網路，請先手動更新本機 AU 伺服器，然後進行「伺服器/裝置更新」。

步驟

1. 向趨勢科技代表取得安裝套件。
2. 解壓縮安裝套件。
3. 將資料夾複製到本機 AutoUpdate 伺服器。

注意

在使用本機 AutoUpdate 伺服器時，您應定期檢查更新。

第 9 章

檢視及維護記錄

本章示範如何在「行動安全防護」管理 Web 主控台上檢視記錄，以及如何進行記錄刪除設定。

本章包含以下小節：

關於記錄

「行動安全防護」會維護下列類型的記錄：

- 系統管理員記錄：只要系統管理員在系統管理員 Web 主控台執行任何設定，「行動安全防護」就會在「管理伺服器」上產生記錄。
- 行動裝置代理程式記錄：「行動裝置代理程式」產生應用程式掃瞄記錄、裝置弱點記錄、網路安全防護記錄或 Web 威脅防護記錄時，會將記錄傳送至「行動安全防護管理伺服器」。如此可將「行動裝置代理程式」記錄儲存在集中位置，以便評估組織的防護政策，同時找出中毒或攻擊威脅程度較高的行動裝置。

檢視行動裝置代理程式記錄

您可以在行動裝置上檢視「行動裝置代理程式」記錄，或在「行動安全防護管理伺服器」上檢視所有「行動裝置代理程式」記錄。在「管理伺服器」上，您可以檢視下列「行動裝置代理程式」記錄：

- 應用程式掃瞄記錄：「行動裝置代理程式」在行動裝置上偵測到惡意程式、隱私威脅、弱點風險或是被竄改的應用程式時，就會產生這些記錄。
- 裝置弱點記錄：已啟動開發人員選項或 USB 偵錯模式、在行動裝置上偵測到惡意 iOS 資料檔，或是偵測到行動裝置已開放 Root 權限/已破解時，就會產生這些記錄。
- 網路安全防護記錄：在行動裝置上偵測到網路流量解密問題、不安全的無線網路存取點 (Wi-Fi) 或惡意 SSL 憑證時，就會產生這些記錄。
- Web 威脅防護記錄：「行動裝置代理程式」封鎖危險或感染惡意程式的網頁時會產生 Web 威脅防護記錄，然後將記錄上傳至伺服器。

步驟

1. 登入「行動安全防護」管理 Web 主控台。
2. 按一下「通知和報告 > 記錄查詢」。

「記錄查詢」畫面隨即出現。

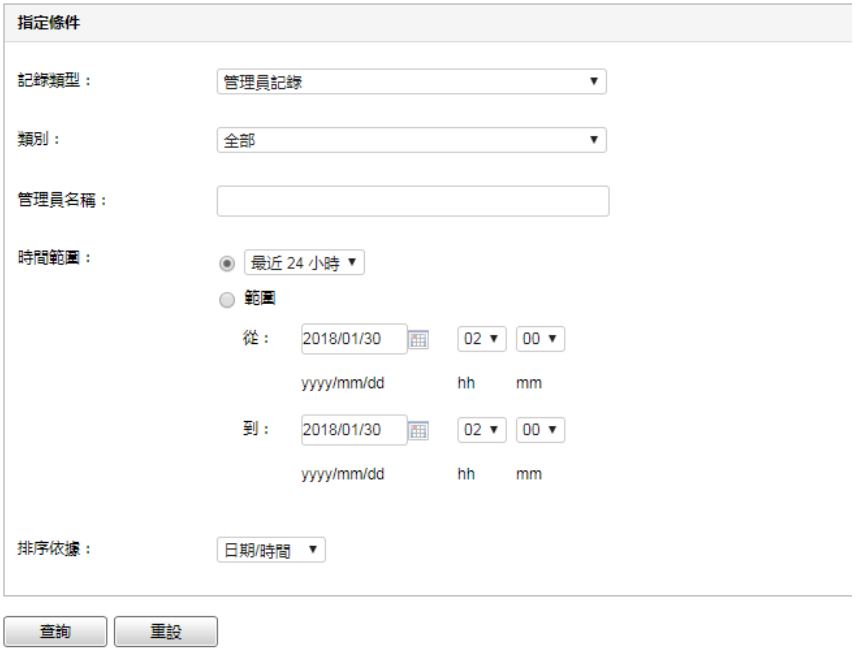


圖 9-1.「記錄查詢」畫面

3. 為您要檢視的記錄指定查詢條件。參數包括：

- 「記錄類型」— 從下拉式功能表中選取記錄類型。
- 「類別」— 從下拉式功能表中選取記錄類別。
- 「系統管理員名稱」或「裝置名稱」— 輸入您要搜尋其相關記錄的系統管理員或裝置名稱。
- 「時間範圍」— 選取預先定義的日期範圍。選項有：「所有」、「最近 24 小時」、「最近 7 天」及「最近 30 天」。如果上述選項未涵蓋您所需的期間，請選取「範圍」，然後指定日期範圍。
    - 「從」— 為您要檢視的最早記錄輸入日期。按一下圖示可從行事曆中選取日期。

- 「到」— 為您要檢視的最新記錄輸入日期。按一下圖示可從行事曆中選取日期。
- 「排序依據」 — 指定記錄的順序與群組。

4. 按一下「查詢」開始進行查詢。

記錄維護

「行動裝置代理程式」產生有關安全威脅偵測的事件記錄時，會將記錄傳送及儲存在「行動安全防護管理模組」中。您可以使用這些記錄來評估組織的防護政策，以及找出中毒或攻擊威脅程度較高的行動裝置。

若要使「行動裝置代理程式」記錄的大小不佔用太多硬碟空間，請手動刪除記錄，或設定「行動安全防護」管理 Web 主控台，使其根據「記錄維護」畫面中的預約自動刪除記錄。

預約記錄刪除

步驟

1. 登入「行動安全防護」管理 Web 主控台。
2. 按一下「通知和報告 > 記錄維護」。

   「記錄維護」畫面隨即出現。
3. 選取「啟動預約刪除記錄」。
4. 選取要刪除的記錄類型。
5. 選取要刪除全部所選記錄類型的記錄，或刪除比指定天數舊的記錄。
6. 指定記錄刪除作業的頻率和時間。
7. 按一下「儲存」。

手動刪除記錄

步驟

1. 登入「行動安全防護」管理 Web 主控台。
2. 按一下「通知和報告 > 記錄維護」。

   「記錄維護」畫面隨即出現。
3. 選取要刪除的記錄類型。
4. 選取要刪除全部所選記錄類型的記錄，或僅刪除比指定天數舊的記錄。
5. 按一下「立即刪除」。

第 10 章

使用通知和報告

本章示範如何在「行動安全防護」中設定及使用通知和報告。

本章包含以下小節：

關於通知訊息和報告

您可以將「行動安全防護」設定為透過電子郵件傳送通知和報告給系統管理員和/或使用者。

- 「系統管理員通知」— 發生任何系統異常狀況時，傳送電子郵件通知給系統管理員。
- 報告 — 傳送報告給指定的電子郵件收件者。
- 「使用者通知」— 傳送電子郵件和（或）簡訊，以通知行動裝置下載並安裝「行動裝置代理程式」。

進行通知設定

設定電子郵件通知

如果您想要傳送電子郵件通知給使用者，必須進行以下設定。

步驟

1. 登入「行動安全防護」管理 Web 主控台。
2. 按一下「通知和報告 > 設定」。

   「通知和報告設定」畫面隨即顯示。
3. 在「電子郵件設定」區段下輸入「寄件者」電子郵件信箱、SMTP 伺服器 IP 位址及通訊埠號碼。
4. 如果 SMTP 伺服器需要驗證，請選取「驗證」並輸入使用者名稱和密碼。
5. 按一下「儲存」。

系統管理員通知

您可以使用「系統管理員通知」畫面來設定以下項目：

- 「即時惡意程式偵測警告」— 代理程式偵測到惡意程式時傳送電子郵件通知給系統管理員。
- 「惡意憑證警告」— 代理程式在偵測到惡意憑證時，傳送電子郵件通知給系統管理員。
- 「惡意 iOS 資料檔警告」— 代理程式在偵測到惡意 iOS 資料檔時，傳送電子郵件通知給系統管理員。
- 「系統錯誤」— 發生任何系統異常狀況時，傳送電子郵件通知給系統管理員。Token 變數 `<%PROBLEM%>`、`<%REASON%>` 和 `<%SUGGESTION%>` 將取代為實際的問題、原因及解決問題的建議。
- 「APNs 憑證到期警告」—在 APNs 憑證到期前一個月傳送電子郵件通知給系統管理員。

啟動系統管理員通知

步驟

1. 移至「通知和報告 > 系統管理員通知」。

   「系統管理員通知」畫面隨即顯示。

2. 選取您要透過電子郵件接收的通知和報告。
3. 按一下「儲存」。

進行系統管理員通知設定

步驟

1. 移至「通知和報告 > 系統管理員通知」。

   「系統管理員通知」畫面隨即顯示。

2. 在「通知設定」下，按一下通知名稱。

   所選通知的「電子郵件設定」畫面隨即出現。

3. 視需要更新下列項目：

   - 「收件者」：系統管理員的電子郵件地址。

     注意

     使用分號 “;” 分隔多個電子郵件地址。

   - 「主旨」：通知電子郵件的主旨行。
   - 「訊息」：通知的訊息內文。

4. 按一下「儲存」。

報告

「行動安全防護」可讓您產生及傳送下列報告：

- 「安全報告」— 顯示以下方面的資訊：偵測到的惡意程式、被竄改的應用程式、隱私風險、易受攻擊的應用程式、網路流量解密問題、不安全的無線網路存取點 (Wi-Fi)、惡意 SSL 憑證、惡意 iOS 資料檔、開發人員選項、USB 偵錯狀態、已開放 Root 權限/破解狀態，以及前十名 (10) 最多人封鎖的網站。
- 「裝置資產清單報告」— 顯示所有受管理裝置的完整資訊。
- 「裝置註冊報告」— 顯示裝置註冊的相關資訊。

您可以從「報告」畫面執行下列工作。

表 10-1. 報告工作

工作	說明
產生	您可以隨時產生新報告。 如需詳細資訊，請參閱產生報告 第 10-5 頁。
檢視	您可以從「視需要」標籤檢視最近產生的報告。 如需詳細資訊，請參閱檢視報告 第 10-6 頁。
傳送	您可以隨時選擇透過電子郵件傳送報告。 如需詳細資訊，請參閱傳送報告 第 10-7 頁。
排程	您可以指定將報告傳送給系統管理員和其他使用者的固定排程。 如需詳細資訊，請參閱預約報告 第 10-8 頁。

產生報告

注意

「行動安全防護」在伺服器上針對每種類型的報告僅會留一份副本。

請先將最新報告儲存一份，再產生新版本。

步驟

1. 在「行動安全防護」管理 Web 主控台上，移至「通知和報告 > 報告 > 視需要」。

   「視需要」畫面隨即出現。

2. 選取時間範圍。
   - 今天
   - 最近 7 天
   - 最近 30 天

3. 選取全部或一個裝置平台。
   - 所有類型
   - iOS
   - Android
4. 選取要納入報告的使用者資訊。
   - 全部
   - 特定
5. 選取要產生的報告。
6. 按一下「產生」。

   「行動安全防護」會產生所選報告，並覆寫所有現有版本。

檢視報告

步驟

1. 在「行動安全防護」管理 Web 主控台上，移至「通知和報告 > 報告」。
2. 從下列任何標籤中，找到要檢視的報告。
   - 視需要 — 選取即可檢視視需要報告。
   - 已預約 — 選取即可檢視預約的報告。
3. 按一下「檢視」。

注意

如果您沒有看見該連結，則必須先產生報告。

如需詳細資訊，請參閱產生報告 第 10-5 頁

所選的報告即會在新的標籤或視窗中開啟。

傳送報告

步驟

1. 在「行動安全防護」管理 Web 主控台上，移至「通知和報告 > 報告 > 視需要」。

   「視需要」畫面隨即出現。

2. 從「報告」表格中，找到所要的報告。

3. 按一下「傳送」。

   注意

   如果您沒有看見該連結，則必須先產生報告。

   如需詳細資訊，請參閱 產生報告 第 10-5 頁

   「傳送報告」畫面隨即出現。

4. 輸入收件者的電子郵件地址。

5. 您可以選擇修改電子郵件主旨與訊息。

6. 按一下「傳送」。

   隨即出現確認訊息。

預約報告

步驟

1. 在「行動安全防護」管理 Web 主控台上，移至「通知和報告 > 報告 > 已預約」。

   「已預約」畫面隨即出現。

2. 從下拉式清單中選取報告頻率。

   - 每天一次
   - 「每週一次」：使用下拉式清單指定要在星期幾送出報告。
   - 「每月一次」：使用下拉式清單指定要在每個月的哪一天送出報告。

3. 按一下「儲存」。

修改電子郵件範本

步驟

1. 在「行動安全防護」管理 Web 主控台上，移至「通知和報告 > 報告 > 已預約」。

   「已預約」畫面隨即出現。

2. 按一下報告名稱。

   所選報告的「電子郵件設定」畫面隨即出現。

3. 視需要更新下列項目：

   - 「收件者」：系統管理員的電子郵件地址。

     注意

     使用分號 “;” 分隔多個電子郵件地址。

- 「主旨」：報告電子郵件的主旨行。
- 「訊息」：報告的訊息內文。

4. 按一下「儲存」。

   隨即出現確認訊息。

使用者通知

可使用「使用者通知」螢幕設定以下電子郵件通知：

- 「行動裝置註冊」— 傳送電子郵件和（或）簡訊，以通知行動裝置下載並安裝「行動裝置代理程式」。Token 變數 <%DOWNLOADURL%> 將取代為設定套件的實際 URL。

設定使用者通知

步驟

1. 登入「行動安全防護」管理 Web 主控台。
2. 按一下「通知和報告 > 使用者通知」。

   「使用者通知」畫面隨即顯示。

3. 選取您要透過電子郵件或簡訊傳送給使用者的通知，然後按一下個別的通知以修改其內容。
   - 若要設定電子郵件通知訊息，請視需要更新下列詳細資料：
     - 「主旨」：電子郵件的主旨。
     - 「訊息」：電子郵件的內文。
   - 若要設定通知簡訊，請在「訊息」欄位中更新訊息的內文。

4. 完成時按一下「儲存」，返回「使用者通知」畫面。

第 11 章

疑難排解及聯絡技術支援

本章提供常見問題的解答和取得其他「行動安全防護」資訊的方式。

本章包含以下小節：

疑難排解

本節將針對您在使用「行動安全防護」時可能遇到的問題提供處理提示。

- 在取消「通訊伺服器」的解除安裝程序後，「通訊伺服器」無法正常運作。

  如果解除安裝程序在停止前已開始刪除對「通訊伺服器」的正常運作具有重要性的檔案與服務，「通訊伺服器」即可能無法正常運作。若要解決此問題，請重新安裝並設定「通訊伺服器」。

- 如果使用 SQL Server Express，即無法儲存「資料庫設定」。

  如果您使用 SQL Server Express，在「伺服器位址」欄位中請使用下列格式：`<SQL Server Express IP 位址>\sqlexpress`。

  注意

  請將 `<SQL Server Express IP 位址>` 取代為 SQL Server Express 的 IP 位址。

- 無法連線至 SQL Server。

  未設定 SQL Server 接受遠端連線時，即可能發生此問題。根據預設，SQL Server Express 和 SQL Server Developer 版本不允許遠端連線。若要設定 SQL Server 允許遠端連線，請執行下列步驟：

  1. 在要從遠端電腦連接的 SQL Server 實體上，啟動遠端連線。
  2. 開啟 SQL Server 瀏覽器服務。
  3. 設定防火牆，以允許 SQL Server 和 SQL Server 瀏覽器服務的相關網路流量。

- 無法連線至 SQL Server 2008 R2。

  如果 Visual Studio 2008 未安裝在預設位置上，而使 SQL Server 2008 安裝程式找不到 devenv.exe.config 組態設定檔，即可能發生此問題。若要解決此問題，請執行以下步驟：

  1. 移至 `<Visual Studio 安裝資料夾>\Microsoft Visual Studio 9.0\Common7\IDE` 資料夾，找到 `devenv.exe.config` 檔案並予以複

製，然後將檔案貼至下列資料夾（您可能必須在資料夾選項中啟動已知檔案類型的顯示副檔名功能）：

- 若是 64 位元作業系統：

  ```
  C:\Program Files (x86)\Microsoft Visual Studio 9.0\Common7\IDE
  ```

- 若是 32 位元作業系統：

  ```
  C:\Program Files\Microsoft Visual Studio 9.0\Common7\IDE
  ```

2. 重新執行 SQL Server 2008 安裝程式，然後將 BIDS 功能新增至現有的 SQL Server 2008 實體。

- 無法在「裝置管理」中匯出用戶端裝置清單。

  如果 Internet Explorer 中關閉加密檔案的下載功能，即可能發生此問題。請執行下列步驟，以啟動加密檔案下載功能：

  1. 在 Internet Explorer 上移至「工具 > 網際網路選項」，然後按一下「網際網路選項」視窗上的「進階」標籤。
  2. 在「安全性」部分下，清除「不要將加密的網頁存到磁碟」。
  3. 按一下「確定」。

- 「政策」快顯視窗的內容無法顯示，且遭到 Internet Explorer 封鎖。

  將 Internet Explorer 設定為使用 .pac 自動組態設定檔時，會發生此問題。在這種情況下，Internet Explorer 會封鎖對於含有多重框架的安全網站的存取。若要解決此問題，請將「行動安全防護管理伺服器」位址新增至 Internet Explorer 的「信任的網站」安全性區域。若要進行此項作業，請執行以下步驟：

  1. 啟動 Internet Explorer。
  2. 移至「工具 > 網際網路選項」。
  3. 按一下「安全」標籤中的「信任的網站」，然後按一下「網站」。
  4. 在「將此網站加到該區域」文字欄位中輸入「行動安全防護管理伺服器」的 URL，然後按一下「新增」。

5. 按一下「確定」。

如需此問題的詳細資料，請參閱以下 URL：

http://support.microsoft.com/kb/908356

聯絡技術支援前

與技術支援人員聯絡前，您可以很快地試試以下兩種方式，以找出問題的解決方案：

- 「查閱文件」— 手冊和線上說明提供「行動安全防護」的詳盡資訊。請一併搜尋兩份文件以查看其中是否含有合適的解決方案。
- 「瀏覽技術支援網站」— 我們的技術支援網站稱為常見問題集，其中包含所有趨勢科技產品的最新相關資訊。支援網站提供對於先前使用者的問題所提出的解答。

  若要搜尋常見問題集，請瀏覽：

  http://www.trendmicro.com.tw/solutionbank/corporate/default.asp

聯絡趨勢科技

您可以透過電話、傳真或電子郵件與趨勢科技代表聯絡：

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
傳真	(886) 2-23780993
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://tw.trendmicro.com/tw/about/contact_us/index.html

- 趨勢科技產品文件：

  http://docs.trendmicro.com/zh-tw/home.aspx

將可疑內容傳送給趨勢科技

您可以使用數個選項將可疑內容傳送給趨勢科技以進行進一步分析。

檔案信譽評等服務

收集系統資訊並將可疑檔案內容提交給趨勢科技：

http://esupport.trendmicro.com/solution/zh-tw/1059565.aspx

記錄案件編號以供追蹤之用。

TrendLabs

趨勢科技 TrendLabs℠ 是全球防毒研究與產品支援中心形成的關係網絡，為全球的趨勢科技客戶永續提供全天候的服務。

TrendLabs 是由超過 250 名工程師和技術精良的支援人員所組成的團隊，專屬服務中心能為世界各地的任何病毒疫情爆發或緊急客戶支援問題做出迅速的回應。

TrendLabs 現代化的總部在 2000 年因高品質的管理程序而獲得 ISO 9002 認證。TrendLabs 也是最先獲得認證的防毒研究與支援設施之一。趨勢科技相信 TrendLabs 是防毒產業中最頂尖的服務和支援團隊。

如需 TrendLabs 的詳細資訊，請瀏覽：

http://us.trendmicro.com/us/about/company/trendlabs/

關於軟體更新

產品發行後，趨勢科技通常會開發軟體更新來強化產品效能、新增功能或解決已知問題。由於發行更新的原因不盡相同，更新的種類也有所差異。

以下是趨勢科技發行的項目相關的摘要：

- Hot fix — Hot fix 是將客戶回報的單一問題予以解決的因應措施或解決方案。由於 Hot fix 是以問題為導向，因此不會發行給所有客戶。Windows 的 Hot fix 含有安裝程式，不過非 Windows 的 Hot fix 沒有（通常您需要停止程式精靈、複製檔案並覆寫安裝中的對應項目，然後重新啟動精靈）。
- 安全 Patch — 安全 Patch 是指著重於安全問題且適合部署給所有客戶的 Hot fix。Windows 的安全 Patch 含有安裝程式，不過非 Windows 的 Patch 通常含有安裝程式檔。
- Patch — Patch 是一組解決多個程式問題的 Hot fix 和安全 Patch。趨勢科技會定期釋出 Patch。Windows 的 Patch 含有安裝程式，不過非 Windows 的 Patch 通常含有安裝程式檔。
- Service Pack — Service Pack 是足以視為產品升級的 Hot fix、Patch 及功能強化內容。Windows 和非 Windows 的 Service Pack 都含有安裝程式和安裝程式檔。

請查閱趨勢科技常見問題集以搜尋發行的 Hot fix：

http://www.trendmicro.com.tw/solutionbank/corporate/default.asp

請定期造訪趨勢科技網站以下載 Patch 和 Service Pack：

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

所有版本均含有 Readme 檔，其中包含安裝、部署及設定產品所需的資訊。安裝 Hot fix、Patch 或 Service Pack 檔案之前，請詳加閱讀 Readme 檔。

已知問題

已知問題是「行動安全防護」中暫時需要因應措施的內容。已知問題通常會記載於產品隨附的 Readme 文件中。您也可以在趨勢科技下載專區找到趨勢科技產品的 Readme：

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

您可以在技術支援常見問題集中找到已知問題的相關資訊：

http://www.trendmicro.com.tw/solutionbank/corporate/default.asp

趨勢科技建議您隨時查閱 Readme 內容，以瞭解可能會影響安裝或效能之已知問題的資訊，以及特定版本的新功能說明、系統需求或其他提示。

其他有用的資源

「行動安全防護」透過網站 (http://www.trendmicro.com) 提供許多服務。

網路式工具與服務包括：

- 「病毒分佈圖」— 監控全球的惡意程式事件
- 「病毒威脅評估」— 適用於公司網路的趨勢科技線上惡意程式防護評估程式。

關於趨勢科技

趨勢科技是網路惡意程式防護以及網路內容安全軟體與服務的全球領導品牌。趨勢科技創立於 1988 年，其引導以桌上型電腦為始的惡意程式防護移轉到網路伺服器和網路閘道，並以卓越的洞察力和技術創新廣受好評。

如今，趨勢科技致力於提供集中控管的伺服器惡意程式防護和內容過濾等產品與服務，進而為客戶提供全方位的安全政策，協助客戶管理資訊威脅所造成的影響。藉由保護流經 Internet 閘道、電子郵件伺服器及檔案伺服器的資訊，趨勢科技使全球各地的用戶得以保護其電腦，免於惡意程式和其他惡意程式碼的威脅。

如需詳細資訊或下載試用版的趨勢科技產品，請造訪獲獎肯定的網站：

http://www.trendmicro.com

索引

TREND MICRO™

趨勢科技股份有限公司
台北市敦化南路二段 198 號 8 樓
電話：(886) 2-23789666　傳真：(886) 2-23780993　info@trendmicro.com

www.trendmicro.com

Item Code: TSCM98145/180126