TREND MICRO™

9.8 趨勢科技™ 行動安全防護

系統管理員手冊

（適用於完整版部署模式）

企業版攜帶型裝置全面性安全解決方案

Endpoint Security

文件編號：TSCM98144/180126

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：管理行動裝置

第 8 章：檢視及維護記錄

第 9 章：使用通知和報告

第 10 章：更新元件

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。此類不當網路通訊包括：透過 3G/GPRS 連線接收的簡訊、WAP Push 郵件與資料。

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，惡意程式防護掃瞄和簡訊管理）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
MS Exchange 行動安全整合	「趨勢科技行動安全防護」使用「MS Exchange 行動安全整合」與 Microsoft Exchange 伺服器進行通訊，偵測所有使用 Exchange ActiveSync 服務的行動裝置，並將其顯示在 Mobile Security Web 主控台上。 Microsoft Exchange 伺服器與 Mobile Security 整合可讓系統管理員監控存取 Microsoft Exchange 伺服器的行動裝置。啟動並設定此功能後，Mobile Security 系統管理員可以執行「遠端清除」，並封鎖此類行動裝置對 Microsoft Exchange 伺服器的存取。 Microsoft Exchange 伺服器與 Mobile Security 整合還可讓系統管理員控制使用者對合作資料（如電子郵件、行事曆及聯絡人等）的存取。	選用
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

元件	說明	必要或選用
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
APNs 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。） 「行動安全防護通訊伺服器」透過「Apple 推播服務」(APNs) 與 iOS 裝置通訊。	如果您想要管理 iOS 行動裝置，則為必要
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
與 Trend Micro Control Manager (TMCM) 7.0 整合	支援與 TMCM 7.0 完全整合。
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。

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。
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。

功能	說明
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。
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。

功能	說明
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	●	

功能名稱	說明	ANDROID	IOS
Web 網頁安全	由於行動裝置的技術不斷成長，行動裝置威脅的精密度也日益增加。「趨勢科技行動安全防護」提供了「網頁信譽評等」與「家長防護網」，可協助您的行動裝置抵禦不安全的網站，以及所含內容可能會對兒童、青少年與其他家庭成員造成負面影響的網站。您可以根據需求來修改 Web 威脅防護和家長防護網的設定層級。「行動安全防護」也會保存「網頁信譽評等」與「家長防護網」在其特定記錄中封鎖之網站的記錄。	●	
垃圾簡訊防護	行動裝置經常會透過簡訊服務收到不想要的簡訊或垃圾郵件。若要將不想要的簡訊過濾到垃圾郵件資料夾，您可以指定所傳送的任何簡訊均可視為垃圾郵件的電話號碼，或指定核可的電話號碼清單並設定「行動安全防護」，使其過濾不在核可清單內的寄件者所傳送的任何簡訊。您也可以過濾不明來電號碼傳來的簡訊，或是根本沒顯示來電號碼的簡訊。您的行動裝置會自動將這些簡訊儲存在收件匣內的垃圾郵件資料夾。 注意 「垃圾簡訊防護」功能不適用於不具電話功能的行動裝置。	●	
來電過濾	「行動安全防護」可讓您過濾伺服器的來電或撥出通話。您可以設定「行動安全防護」封鎖來自特定電話號碼的來電，也可以指定可從行動裝置去電的核可電話號碼清單。「行動安全防護」也可讓行動裝置使用者指定自己的封鎖或核可清單，以過濾不想接聽的來電。 注意 「來電過濾」功能不適用於不具電話功能的行動裝置。	●	

功能名稱	說明	ANDROID	IOS
WAP Push 防護	WAP Push 是自動將內容傳送給行動裝置的有效方法。為了開始傳送內容，使用者會收到特殊的訊息（稱為 WAP Push 訊息）。這些訊息通常含有內容的相關資訊，同時也是供使用者接受或拒絕內容的方法。 惡意使用者會送出不正確或未提供資訊的 WAP Push 訊息，誘使使用者接受含不想要的應用程式、系統設定或甚至惡意程式等內容。「行動安全防護」能讓您使用信任的寄件者清單來過濾 WAP Push 訊息，阻止不想要的內容進入行動裝置。 WAP Push 防護功能不適用於沒有電話功能的行動裝置。	●	
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。	●	●
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。	●	

功能名稱	說明		ANDROID	IOS
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	●	●
		政策違規記錄	●	●
		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	●	
		來電過濾記錄	●	
		簡訊過濾記錄	●	
		更新記錄	●	

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		
佈建	Wi-Fi	標準 Wi-Fi 設定	●	●

政策	功能	設定		
		傳統熱點設定	●	
		熱點 2.0 設定	●	
	Exchange ActiveSync	Exchange ActiveSync 組態設定	●	
	VPN	VPN 組態設定	●	
	全域 HTTP Proxy	全域 HTTP Proxy 設定	●	
	單一登入	單一登入設定	●	
	憑證	憑證設定	●	
	行動數據網路	行動數據網路設定	●	
	AirPlay/AirPrint	AirPlay/AirPrint 設定	●	
	佈景主題（僅限監督模式）	桌布設定	●	
		字型設定	●	
	受管理網域	未標記的電子郵件網域	●	
		受管理的 Safari Web 網域	●	
裝置安全	安全設定	即時掃瞄		●
		病毒碼更新完成後進行掃瞄		●
		手動掃瞄	●	●
資料安全防護	垃圾簡訊防護	伺服器端控管		●
		使用封鎖的清單		●
		使用核可的清單		●
	垃圾簡訊 WAP Push 防護	伺服器端控管		●
		使用核可的清單		●

政策	功能	設定		
	來電過濾	伺服器端控管		●
		使用封鎖的清單		●
		使用核可的清單		●
	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		●
資料安全防護	密碼設定	使用登入密碼	●	●
		允許簡單密碼	●	●
		要求英數字元密碼	●	●
		密碼長度下限	●	●
		密碼到期	●	●
		密碼記錄	●	●
		自動鎖定	●	●
		密碼不正確處理行動	●	●
	功能鎖定	相機	●	●
		FaceTime	●	
		螢幕擷取	●	
		應用程式安裝	●	
		漫遊時同步	●	

政策	功能	設定		
		語音撥號	●	
		In-app purchase	●	
		多人玩家遊戲	●	
		新增 Game Center 好友	●	
		Game Center（僅限監督）	●	
		強制使用加密備份	●	
		不當的音樂、播客與 iTunes U	●	
		裝置鎖定時允許存摺	●	
		藍芽與藍芽搜索		●
		WLAN/Wi-Fi		●
		3G 資料網路		●
		數據連線		●
		開發人員模式		●
		喇叭/免持聽筒/麥克風		
		限制記憶卡		●
		Siri	●	
		裝置鎖定時允許 Siri	●	
		啟動髒話過濾器	●	
		啟動存取 iCloud 服務	●	
		雲端備份	●	
		雲端文件同步	●	

政策	功能	設定		
		相片串流	●	
		共享相片串流	●	
		診斷資料	●	
		接受不信任的傳輸層安全性 (TLS)	●	
		強制要求輸入 iTunes Store 密碼	●	
		YouTube	●	
		從其他應用程式中的受管理應用程式開啟文件	●	
		從受管理應用程式中的其他應用程式開啟文件	●	
		iTunes	●	
		Safari 網路瀏覽器	●	
		自動填寫	●	
		JavaScript	●	
		快顯	●	
		強制執行詐騙警告	●	
		接受 Cookie	●	
		移除應用程式（僅限監督）	●	
		書店（僅限監督）	●	
		色情書刊（僅限監督）	●	
		設定資料檔安裝（僅限監督）	●	
		iMessage（僅限監督）	●	

政策	功能	設定		
		為區域分級	●	
		電影	●	
		電視節目	●	
		應用程式	●	
		帳號修改（僅限監督）	●	
		AirDrop（僅限監督）	●	
		應用程式行動數據資料修改（僅限監督）	●	
		小幫手（Siri）使用者產生的內容（僅限監督）	●	
		雲端鑰匙圈同步	●	
		Find My Friends 修改（僅限監督）	●	
		解除裝置鎖定所用的指紋	●	
		主機配對（僅限監督）	●	
		鎖定畫面控制中心	●	
		鎖定畫面通知檢視	●	
		鎖定畫面今日檢視	●	
		透過 Air Public Key Infrastructure (OTAPKI) 更新	●	
		強制限制廣告追蹤	●	
		強制 AirPlay 傳出要求配對密碼	●	
		允許受管理應用程式在 iCloud 中儲存資料	●	

政策	功能	設定		
		允許備份企業通訊錄	●	
		允許設定限制	●	
		允許刪除所有內容和設定	●	
		允許轉接	●	
		允許焦點中的網路結果	●	
		允許同步企業通訊錄的附註和好友動向	●	
		允許使用 AirDrop 分享管理的文件	●	
		允許 iCloud 照片庫	●	
		允許從裝置安裝應用程式	●	
		允許鍵盤快速鍵	●	
		允許配對 Apple Watch	●	
		允許修改密碼	●	
		允許修改裝置名稱	●	
		允許修改桌布	●	
		允許自動下載應用程式	●	
		允許信任企業應用程式	●	
	合規設定	已開放 Root 權限/已破解	●	●
		已取消加密	●	●
		作業系統版本檢查	●	●
應用程式管理	應用程式監控與控管	需要的應用程式	●	●

政策	功能	設定		
		允許的應用程式	●	●
		鎖定至應用程式（僅限監督）	●	
	大量購買方案	大量購買方案	●	
遠端控制	註冊		●	●
	更新		●	●
	防竊取	遠端尋找		●
		遠端鎖定	●	●
		遠端清除	●	●
		重設密碼	●	●
	Samsung KNOX Workspace	建立容器		●
		移除容器		●
		鎖定容器		●
		解除鎖定容器		●
		重設容器密碼		●
Samsung KNOX Workspace 政策	容器帳號設定	封鎖的清單		●
		核可的清單		●
	限制設定	允許使用者使用相機		●
		允許透過應用程式清單顯示共用		●
	瀏覽器設定	啟動自動填寫設定		●
		啟動 Cookie 設定		●
		啟動快顯設定		●

政策	功能	設定		
		啟動強制執行詐騙警告設定		●
		啟動 JavaScript 設定		●
		啟動 Web Proxy		●
Samsung KNOX Workspace 政策	容器密碼設定	啟用密碼可見性		●
		密碼變更長度下限		●
		密碼長度下限		●
		未作用逾時上限		●
		失敗嘗試次數上限		●
		密碼記錄		●
		密碼有效時間上限		●
		密碼中必要的特殊字元數量上限		●
		密碼複雜度		●
	應用程式設定	核可的安裝清單		●
		封鎖的安裝清單		●
		需要的應用程式		●
		關閉的應用程式		●
裝置註冊方案			●	

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 2-16 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。

報表畫面分成五標籤：

- 「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

- 「健康情況」— 顯示伺服器元件和政策更新，以及行動裝置的健康狀態。在此類別中，您可以：
  - 檢視行動裝置的狀態：
    - 「狀況良好」— 表示裝置已向「行動安全防護管理伺服器」註冊，且行動裝置上的元件和政策為最新版本。
    - 「不合規」— 表示裝置已向「行動安全防護管理伺服器」註冊，但不符合伺服器政策。
    - 「未同步」— 表示裝置已向「行動安全防護管理伺服器」註冊，但元件或政策已過期。
    - 「離線」— 表示裝置尚未向「行動安全防護管理伺服器」註冊。
  - 檢視受「行動安全防護」管理之已註冊和未註冊行動裝置的總數。

    如果與「通訊伺服器」的連線失敗，則行動裝置可能尚未註冊。
  - 檢視行動裝置程式 Patch 與元件更新狀態：
    - 「目前版本」—「Mobile Security 管理伺服器」上的「行動裝置代理程式」或元件目前的版本號碼
    - 「最新版本」—「行動裝置代理程式」版本或元件已更新的行動裝置數量

- 「過期版本」— 目前仍使用已過期之元件的行動裝置數量
- 「更新率」— 使用最新版本之元件的行動裝置百分比
- 「已升級」— 使用最新版本之「行動裝置代理程式」的行動裝置數量
- 「未升級」— 尚未升級且沿用舊版「行動裝置代理程式」的行動裝置數量
- 「升級率」— 使用最新版本之「行動裝置代理程式」的行動裝置百分比

- 檢視伺服器更新狀態：
  - 「伺服器」— 模組的名稱
  - 「位址」— 裝載模組之機器的網域名稱或 IP 位址
  - 「目前版本」—「行動安全防護管理伺服器」模組目前的版本號碼
  - 「上次更新時間」— 上次更新的時間和日期

- 「合規」— 顯示行動裝置的應用程式控管、加密及已破解/Root 權限狀態。在此類別中，您可以：
  - 檢視行動裝置破解/Root 權限狀態：
    - 「已破解/已開放 Root 權限」— 已破解/已開放 Root 權限的行動裝置數量
    - 「未破解/未開放 Root 權限」— 未破解/未開放 Root 權限的行動裝置數量
  - 檢視行動裝置加密狀態：
    - 「已加密」— 已加密的行動裝置數量
    - 「未加密」— 未加密的行動裝置數量
  - 檢視行動裝置應用程式控制狀態：
    - 「合規」— 符合「行動安全防護」安全規範與應用程式控管政策的行動裝置數

- 「不合規」— 不符合「行動安全防護」安全規範與應用程式控管政策的行動裝置數量

- 「資產清單」— 顯示行動裝置作業系統版本摘要、電信業者摘要、行動裝置廠商摘要及前 10 名最多人安裝的應用程式。

注意

在「報表」畫面中的每個 Widget 上，您可以選取「全部」或是下拉式清單中的群組名稱，以顯示相關裝置上的資訊。

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

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 2-16 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 2-18 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
Exchange 伺服器網域控管	網域選擇	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
	Exchange 伺服器整合	支援	不支援
	設定與驗證	支援	不支援
	產品授權	支援	不支援

伺服器元件	權限	超級管理員	群組管理員
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	企業應用程式商店	支援	不支援
	已安裝的應用程式	支援	僅支援受管理群組
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
	Exchange ActiveSync 裝置	支援	僅支援受管理群組
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 2-17 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 2-17 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 2-16 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」。

Exchange 伺服器整合

進行 Exchange 伺服器整合設定

如需詳細的設定步驟，請參閱《*安裝與部署手冊*》中的＜*進行 Exchange 伺服器整合設定*＞主題。

設定 MS Exchange 行動安全整合

您可以設定每次有更新版本時，「MS Exchange 行動安全整合」便會自動更新。

步驟

1. 在有安裝「MS Exchange 行動安全整合」的電腦上，按一下 Windows 工作列上系統匣（在系統時鐘旁）中的「顯示隱藏的圖示」按鈕。

2. 在「MS Exchange 行動安全整合」圖示上按一下滑鼠右鍵，再按一下「關於趨勢科技 MS Exchange 行動安全整合」。

   「關於趨勢科技 MS Exchange 行動安全整合」畫面隨即顯示。

3. 設定下列項目：

   - 「啟動自動升級」— 若有選取，每當有新的版本時，「MS Exchange 行動安全整合」便會自動升級至新的版本。
   - 「伺服器位址」—「行動安全防護管理伺服器」IP 位址。
   - 「HTTPS 通訊埠」— 管理 Web 主控台的「行動安全防護管理伺服器」HTTPS 通訊埠號碼。

移轉到新的 Exchange 伺服器

若要移轉至新的 Exchange 伺服器，請完成下列步驟：

步驟

1. 在安裝 MS Exchange 行動安全整合的電腦上停止現有的 MS Exchange 行動安全整合服務。
2. 登入「行動安全防護」管理 Web 主控台。
3. 按一下「管理 > Exchange 伺服器整合」。
4. 按一下「資料清除」。
5. 將新的 MS Exchange 行動安全整合下載並安裝到電腦。

   如需詳細資訊，請參閱《*安裝與部署手冊*》。

6. 進行 MS Exchange 行動安全整合設定。

   請參閱設定 MS Exchange 行動安全整合 第 2-21 頁。

第 3 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
- 將簡訊傳送到行動裝置
- 手動的「行動裝置代理程式」元件更新、清除/鎖定/尋找遠端裝置以及更新政策
- 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，以及下列兩個子群組：

- 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。
- 未經授權— 如果「裝置註冊設定」中的「裝置驗證」已啟動，而且使用行動裝置清單進行驗證，「行動安全防護管理伺服器」會自動建立此群組。如果有已註冊的行動裝置不在行動裝置清單中，「行動安全防護」會將此類行動裝置移至未經授權群組。「行動安全防護」也會建立其他群組，並根據您使用的清單將所有的行動裝置重新分組。

注意

- 如果您啟用「裝置註冊設定」中的「裝置驗證」，並上傳空白行動裝置清單進行驗證，則「行動安全防護」會將目前所有已註冊的行動裝置移至「未經授權」群組。
- 「裝置驗證」僅支援 Android 與 iOS 行動裝置。

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 3-6 頁
- 刪除多個行動裝置 第 3-6 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、韌體版本資訊及最新 iCloud 備份。
- 「安全」— 顯示行動裝置在以下方面的狀態：加密、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；已連線的無線網路存取點 (Wi-Fi) 與作用中的 iTunes 帳號。
- 「網路」— 顯示積體電路卡 ID (ICCID)、藍芽和 WiFi MAC 資訊、網路詳細資訊（包括電信業者網路名稱、設定版本、行動狀態）、行動裝置國碼 (MCC) 和行動裝置網路碼 (MNC) 資訊及個人熱點狀態。
- 「政策」— 顯示上次更新設定與安全防護政策的時間。
- 「安裝的應用程式」— 顯示行動裝置上所安裝的所有應用程式的清單，以及合規檢查結果。此標籤僅適用於 Android 與 iOS 行動裝置。
- 「Samsung KNOX 資訊」— 顯示支援 Samsung KNOX 之行動裝置的其他資訊。

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
- 「由使用者解除安裝的行動裝置代理程式」 — 將搜尋範圍限制為使用者解除安裝行動裝置代理程式所在的行動裝置
- 「已開放 Root 權限的行動裝置」 — 將搜尋範圍限制為已開放 Root 權限的行動裝置
- 「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
- 「裝置狀態」 — 將搜尋範圍限制為所選行動裝置的狀態

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 10-2 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」。

遺失裝置防護

使用者將行動裝置遺失或放錯位置時，您可以在遠端尋找、鎖定或刪除該行動裝置上的所有資料。

尋找遠端行動裝置

您可以透過無線網路或使用行動裝置的 GPS 找到行動裝置。「管理伺服器」會在 Google 地圖上顯示行動裝置的位置。

注意

此功能僅適用於 Android 與 iOS 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尋找的行動裝置。
4. 按一下「裝置尋找」，再按一下確認畫面上的「確定」。

   「行動安全防護管理伺服器」會嘗試尋找行動裝置，並在「遠端尋找裝置」畫面上顯示 Google 地圖連結。
5. 按一下「遠端尋找裝置」畫面上的 Google 地圖連結，即可在地圖上看見該行動裝置最近的 GPS 位置。

鎖定遠端行動裝置

您可以從管理 Web 主控台傳送鎖定指示，以遠端鎖定行動裝置。使用者必須輸入解鎖密碼，才能將行動裝置解除鎖定。

注意

僅 Android 和 iOS 行動裝置支援此功能。

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鎖定的行動裝置。
4. 請執行以下任一項工作：

若為 Android 行動裝置，按一下「遠端鎖定」，然後按一下確認對話方塊上的「確定」。

若為 iOS 行動裝置，按一下「遠端鎖定」，輸入使用者的電話號碼和要傳送給使用者的訊息，然後按一下「鎖定」。

如果成功產生鎖定指令，則在畫面上會顯示「成功」訊息。若要檢查是否成功鎖定行動裝置，您可以在「指令佇列管理」畫面中檢查命令狀態。如需詳細資料，請參閱指令佇列管理 第 2-18 頁。

清除遠端行動裝置

警告!

使用這項功能時請多加留意，因為此動作是無法復原的。所有資料都將遺失，且無法復原。

您可以從遠端將行動裝置重設回原廠設定，並清除行動裝置內部記憶體/SD 卡。這項功能有助於確保遺失、遭竊或放錯位置之行動裝置的資料安全。您也可以選擇僅清除行動裝置上的以下公司資料：

- Android：Exchange 郵件、行事曆與聯絡人
- iOS：MDM 資料檔、相關政策、設定及資料

注意

僅 Android 和 iOS 行動裝置支援此功能。

如需清除使用 Exchange ActiveSync 的行動裝置相關指示，請參閱清除遠端 ActiveSync 行動裝置 第 3-20 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「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清除的行動裝置。

4. 按一下「遠端清除」。

   「遠端清除裝置」畫面隨即顯示。

5. 選取適當的「裝置名稱」核取方塊。

6. 請執行以下任一項工作：

   - 若為 Android 行動裝置，請選取下列其中一項：
     - 清除所有資料並回復為原廠設定（將移除所有的應用程式與儲存的資料。插入的記憶卡將格式化。此動作無法復原）。
     - 「清除電子郵件、行事曆和聯絡人清單」— 亦即所謂的「選擇性清除功能」。

       如果您選取此選項，也可以選取「如果選擇性清除功能運作失敗，請清除所有資料並回復為原廠設定」。
   - 若為 iOS 行動裝置，請選取下列其中一項：
     - 清除所有資料並回復為原廠設定（將移除所有的應用程式與儲存的資料。插入的記憶卡將格式化。此動作無法復原）。
     - 清除所有佈建的資料檔、政策、設定及其相關資料。

7. 按一下「遠端清除裝置」。

   所選的資料會從行動裝置中刪除，並向伺服器取消註冊「行動裝置代理程式」。

遠端重設密碼

如果使用者忘記開機密碼，您可以從「管理伺服器」遠端重設密碼並解除鎖定行動裝置。成功解除鎖定行動裝置後，使用者即可變更解鎖密碼。

注意

僅 Android 和 iOS 行動裝置支援此功能。

重設 Android 行動裝置密碼

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. 在樹狀結構中選取行動裝置，然後按一下「密碼重設」。
4. 在顯示的快顯對話方塊中輸入並確認新的六位數密碼。

移除 iOS 行動裝置密碼

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. 在樹狀結構中選取行動裝置，然後按一下「密碼重設」。
4. 在出現的確認對話方塊中按一下「確定」。所選 iOS 行動裝置的開機密碼即會遭到移除。

從遠端管理 Samsung KNOX Workspace

您可以從 Mobile Security 管理 Web 主控台傳送指令，以便管理 Samsung KNOX 工作區。這些指令包括建立容器、移除容器、鎖定容器、解除鎖定容器及重設容器密碼。此功能僅供 Samsung 行動裝置使用。

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要管理的 Samsung 行動裝置。
4. 請執行以下任一項工作：
   - 若要在行動裝置上建立 KNOX Workspace，請按一下「KNOX 作業 > 建立容器」。
   - 若要移除行動裝置上的 Workspace，請按一下「KNOX 作業 > 移除容器」。
   - 若要讓使用者重設 Workspace 密碼，請按一下「KNOX 作業 > 重設密碼」。
   - 若要鎖定行動裝置上的 Workspace，請按一下「KNOX 作業 > 鎖定容器」。
   - 若要解除鎖定行動裝置上的 Workspace，請按一下「KNOX 作業 > 解除鎖定容器」。

遠端修改 iOS 設定

您可以利用遠端方式從管理 Web 主控台變更 iOS 行動裝置設定。這些設定包括數據漫遊、語音漫遊及個人熱點。

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要管理的 iOS 行動裝置。
4. 請執行以下任一項工作：
   - 若要啟動數據漫遊，請按一下「iOS 作業 > 啟動數據漫遊」。
   - 若要關閉數據漫遊，請按一下「iOS 作業 > 關閉數據漫遊」。
   - 若要啟動語音漫遊，請按一下「iOS 作業 > 啟動語音漫遊」。
   - 若要關閉語音漫遊，請按一下「iOS 作業 > 關閉語音漫遊」。
   - 若要啟動個人熱點，請按一下「iOS 作業 > 啟動個人熱點」。
   - 若要關閉個人熱點，請按一下「iOS 作業 > 關閉個人熱點」。
   - 若要啟動 Airplay 鏡像，請按一下「iOS 作業 > 要求 AirPlay 鏡像」。
   - 若要停止 Airplay 鏡像，請按一下「iOS 作業 > 停止 AirPlay 鏡像」。

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。

將訊息傳送給行動裝置

您可以從「裝置」畫面中的「受管理裝置」標籤，將簡訊傳送至使用者或群組。

注意

當您將簡訊傳送到 iOS 裝置時，此資訊不會出現在「指令佇列管理」畫面上。

步驟

1. 登入「行動安全防護」管理員 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，選取您要將簡訊傳送到的行動裝置或裝置群組。
4. 按一下「傳送訊息」。

   「傳送簡訊」畫面隨即出現。
5. 在提供的欄位中輸入訊息，然後按一下「傳送」。

Exchange ActiveSync 裝置標籤

啟動「行動安全防護管理伺服器」上的「Exchange 伺服器整合」後，「裝置」畫面上的「Exchange ActiveSync 裝置」標籤會顯示透過 ActiveSync 服務與 Exchange 伺服器連線的行動裝置清單。

在「Exchange ActiveSync 裝置」標籤，您可以執行下列處理行動：

- 允許或封鎖存取 Exchange 伺服器
- 手動遠端清除
- 取消遠端清除指令
- 從清單移除選取的行動裝置

邀請 Exchange ActiveSync 使用者

邀請 Exchange ActiveSync 使用者之前，請務必確認您已在「管理伺服器」上設定通知和報告設定。請參閱《安裝與部署手冊》中的＜設定通知和報告設定＞主題。

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. 按一下「Exchange ActiveSync 裝置」標籤。
4. 針對您想要邀請加入「行動安全防護」的使用者，選取為該使用者指定的行動裝置。
5. 按一下「邀請」，然後在出現的確認畫面上按一下「確定」。

「行動安全防護」會向邀請的使用者傳送電子郵件。行動裝置向「行動安全防護管理伺服器」註冊後，「受管理裝置」欄會顯示行動裝置代理程式的狀態。

允許或封鎖存取 Exchange 伺服器

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. 按一下「Exchange ActiveSync 裝置」標籤。
4. 選取您要允許或封鎖存取 Exchange 伺服器的行動裝置。
5. 按一下「允許存取」或「封鎖存取」，再按一下確認對話方塊上的「確定」。

   在行動裝置與 Exchange 伺服器同步化後，「Exchange 存取狀態」欄中的行動裝置狀態會顯示新狀態。

清除遠端 ActiveSync 行動裝置

警告!

使用這項功能時請多加留意，因為此動作是無法復原的。所有資料都將遺失，且無法復原。

您可以從遠端將 ActiveSync 行動裝置重設回出廠設定，並清除行動裝置內部記憶體/SD 卡。這項功能有助於確保遺失、遭竊或放錯位置之行動裝置的資料安全。

如需清除不使用 ActiveSync 的行動裝置相關指示，請參閱清除遠端行動裝置 第 3-13 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「裝置」。

   「裝置」畫面隨即出現。
3. 按一下「Exchange ActiveSync 裝置」標籤。
4. 選取您要清除的行動裝置。
5. 按一下「遠端清除」。

   隨即快顯「遠端清除裝置」畫面。
6. 選取裝置，然後按一下「遠端清除裝置」。

移除 ActiveSync 行動裝置

您從「行動安全防護管理伺服器」遠端清除的行動裝置將再也無法存取 Exchange 伺服器。您可以從「裝置」畫面的「Exchange ActiveSync 裝置」標籤中移除此類行動裝置資訊。

注意

您只能移除從「行動安全防護管理伺服器」中遠端清除的行動裝置。

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. 按一下「Exchange ActiveSync 裝置」標籤。
4. 選取您要從清單中移除的行動裝置。
5. 按一下「移除」，再按一下確認畫面上的「確定」。

裝置註冊方案標籤

裝置註冊方案 (DEP) 提供一種快速、簡化的方法來部署公司擁有的 iOS 行動裝置。您可以向 DEP 方案註冊您的公司。

Trend Micro Mobile Security 會與 Apple 裝置註冊方案整合，針對公司所發放直接向 Apple 購買的 iOS 7 至 iOS 11 行動裝置，簡化其註冊流程。如果已設定與裝置註冊方案整合，當使用者獲得發放的公司擁有的 iOS 行動裝置，並採用 iOS 啟動程序設定行動裝置時，系統會提示其向「行動安全防護」註冊。

將「行動安全防護」與 DEP 整合表示您不需要向使用者傳達註冊指示，但仍可確保當使用者第一次使用時，所有行動裝置均已註冊。此外，此整合亦會消除相關支援費用。

裝置註冊方案使用者體驗

如果您設定「行動安全防護」與 Apple 裝置註冊方案的整合，則使用者體驗如下：

- 使用者收到公司發放的全新 iOS 行動裝置，拆開包裝，然後將其開啟。
- 行動裝置連線至 Apple。
- 透過行動裝置 ID，Apple 伺服器偵測到該裝置已新增至裝置註冊方案帳號中，並且會傳送裝置設定與連線詳細資料以部署 Mobile Security。
- 接著，使用者透過 iOS 設定助理完成行動裝置的初始啟動，其中包括向 Mobile Security 註冊。

當您設定與裝置註冊方案的整合時，可以決定 iOS 設定助理所顯示的畫面。這可讓您略過透過裝置管理進行設定的設定畫面，進一步簡化啟動程序。例如，

如果您計劃要求將裝置上的定位服務做為地理圍欄設定的一部分來啟動，則可以將 iOS 設定助理設定為略過讓使用者選擇是否啟動定位服務的畫面。

在裝置啟動程序中，系統會提示使用者向 Mobile Security 註冊。使用者不需要輸入認證或電子郵件地址，且不需要瞭解 Mobile Security 的連線詳細資料。您設定與裝置註冊方案的整合時管理員自動建立的特定裝置註冊方案資料檔會部署到裝置。

針對裝置註冊方案設定行動安全防護

請先確保您已在下列 Apple 網站上向 DEP 方案註冊您的公司，然後才能針對裝置註冊方案 (DEP) 設定 Mobile Security。

http://deploy.apple.com/

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. 按一下「裝置註冊方案」標籤。
4. 按一下「設定」。
5. 按一下「公開金鑰」前的「下載」連結，從「Mobile Security 管理伺服器」將公開金鑰下載至本機電腦。
6. 按一下「部署」前的「Apple 部署方案」連結。

   「Apple 部署方案」Web 入口網站隨即在 Internet 網路瀏覽器中開啟。
7. 使用從「Mobile Security 管理伺服器」下載的公開金鑰登入「裝置註冊方案」帳號並建立新的 MDM 伺服器。如需向「裝置註冊方案」註冊的詳細步驟，請參閱以下文件。

   https://www.apple.com/iphone/business/docs/DEP_Business_Guide_EN_Feb14.pdf

8. 在 MDM 伺服器上，產生存取 Token 並將 Token 檔案儲存至合適位置，然後指派要向 MDM 伺服器註冊的行動裝置。

9. 將透過「Apple 部署方案」Web 入口網站產生的 Token 檔案上傳至「Mobile Security 管理伺服器」。等候直到上傳完成。

   上傳完成後，「裝置註冊方案設定」畫面隨即出現。

10. 在「裝置註冊方案詳細資訊」區段下，針對行動裝置進行以下設定資料檔設定。

    - 「資料檔名稱」：顯示在行動裝置上的設定資料檔的名稱。
    - 「要求監督」：將透過「裝置註冊方案」註冊的行動裝置置於監督模式。
    - 「可移除設定」：允許使用者從透過「裝置註冊方案」註冊的裝置移除裝置管理設定。
    - 「允許配對」：讓透過「裝置註冊方案」註冊的裝置能夠藉由 iTunes 和 Apple Configurator 等 Apple 工具進行管理。
    - 「必要設定」：防止使用者在裝置啟動程序中略過 Mobile Security 註冊步驟。
    - 「業務單位」：將行動裝置指派到的部門名稱。
    - 「唯一服務識別碼」：如果您有多個 Mobile Security 部署，請在「唯一服務識別碼」方塊中輸入可唯一識別要設定之部署的名稱。
    - 「支援電話號碼」：使用者致電以尋求協助的電話號碼。
    - 「必要的設定項目」：使用者必須設定的設定項目。依預設，需要具備所有設定項目。如果關閉其中任何項目，使用者皆可在設定期間略過該項目。

11. 按一下「儲存」。

    「行動安全防護管理伺服器」將行動裝置清單與 Apple「裝置註冊方案」伺服器同步，並且在「裝置」畫面上的「裝置註冊方案」標籤中顯示行動裝置。

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 4 章

管理使用者和邀請

本章示範如何在「行動安全防護」中管理使用者與邀請清單。

本章包含以下小節：

使用者標籤

「使用者」標籤可讓您執行下列工作：

- 邀請使用者註冊
- 再次邀請使用者並變更指派的群組
- 編輯使用者資訊
- 刪除使用者
- 搜尋使用者

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。

再次邀請使用者

注意

本主題僅適用於搭配未列出之 MDM 解決方案在「安全掃瞄」模式下進行的「行動安全防護」部署。

如果您的「行動安全防護」與 AirWatch 或 MobileIron 整合，則會關閉此功能。

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. 選取使用者，然後按一下「再次邀請」。

   「再次邀請」畫面隨即出現。

3. 從下拉式清單中選取群組。

4. 按一下「儲存」。

   隨即出現確認訊息。

編輯使用者資訊

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. 從清單中按一下使用者名稱。

   「編輯使用者資訊」畫面隨即顯示。

3. 視需要修改使用者名稱和電子郵件地址。

4. 按一下「儲存」。

「行動安全防護」會更新使用者資訊。

刪除使用者

注意

您只能刪除未向手機防護精靈伺服器註冊裝置的使用者。

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. 從清單中選取使用者，然後按一下「刪除」。

3. 在出現的確認訊息中，按一下「確定」。

   「行動安全防護」會刪除選取的使用者。

邀請標籤

「使用者」畫面上的「邀請」標籤可讓您執行下列工作：

- 檢視邀請清單
- 重新傳送邀請
- 取消作用中邀請
- 從清單移除邀請
- 搜尋邀請

檢視邀請清單

步驟

1. 在「行動安全防護」管理 Web 主控台上，移至「使用者 > 邀請」。

   「邀請」標籤隨即出現。

2. 若要篩選清單，請從下拉式清單選取邀請狀態。

邀請狀態	說明
作用中	邀請為有效，且使用者可使用邀請訊息中的資訊註冊。
已到期	邀請已到期，且使用者再也無法使用邀請訊息中的資訊註冊。
已使用	使用者已使用邀請訊息中的資訊註冊，「註冊金鑰」變成無效。 注意 此狀態只在「裝置註冊設定」的「註冊金鑰使用限制選項」設為「一次使用」時才會顯示。
已取消	邀請已被伺服器取消，且使用者無法使用邀請訊息中的資訊註冊。

3. 若要搜尋邀請，請在「搜尋」列中輸入使用者名稱、電話號碼或電子郵件地址，然後按下 Enter。

   如果邀請存在於清單中，則「行動安全防護」會顯示資訊。

重新傳送邀請

步驟

1. 在「行動安全防護」管理 Web 主控台上，移至「使用者 > 邀請」。
2. 從清單中選取邀請。

3. 按一下「重新傳送邀請」。

   「行動安全防護」會重新傳送邀請給選取的使用者。

取消作用中邀請

步驟

1. 在「行動安全防護」管理 Web 主控台上，移至「使用者 > 邀請」。
2. 從清單中選取邀請。
3. 按一下「取消邀請」。

   所選邀請即已取消。

從清單移除邀請

注意

您只能移除狀態為「已使用」或「已取消」的邀請。

步驟

1. 在「行動安全防護」管理 Web 主控台上，移至「使用者 > 邀請」。
2. 從清單中選取邀請。
3. 按一下「移除邀請」。

   選取的邀請即已自清單中移除。

第 5 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 5-1. 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 5-4 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 5-4 頁。

表 5-2. 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 5-8 頁。

政策群組	政策	參考
佈建	Wi-Fi 政策	請參閱 Wi-Fi 政策 第 5-8 頁。
	Exchange ActiveSync 政策	請參閱 Exchange ActiveSync 政策 第 5-9 頁。
	憑證政策	請參閱憑證政策 第 5-9 頁。
	VPN 政策	請參閱 VPN 政策 第 5-9 頁。
	全域 HTTP Proxy 政策	請參閱全域 HTTP Proxy 政策 第 5-9 頁。
	單一登入政策	請參閱單一登入政策 第 5-10 頁。
	行動數據網路政策	請參閱行動數據網路政策 第 5-11 頁。
	AirPlay/AirPrint 政策	請參閱 AirPlay/AirPrint 政策 第 5-11 頁。
	佈景主題政策	請參閱佈景主題政策 第 5-11 頁。
	受管理網域政策	請參閱受管理的網域政策 第 5-11 頁。
裝置安全	安全政策	請參閱安全政策 第 5-12 頁。
	垃圾簡訊防護政策	請參閱垃圾簡訊防護政策 第 5-15 頁。
	來電過濾政策	請參閱來電過濾政策 第 5-17 頁。
裝置	密碼政策	請參閱密碼政策 第 5-19 頁。
	功能鎖定政策	請參閱功能鎖定政策 第 5-20 頁。
	合規政策	請參閱合規政策 第 5-20 頁。

政策群組	政策	參考
應用程式管理	應用程式監控與控管政策	請參閱應用程式監控與控管政策 第 5-21 頁。
	大量購買方案政策：	請參閱大量購買方案政策 第 5-23 頁。
Samsung KNOX	容器政策	請參閱容器政策 第 5-23 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」或是「應用程式 > 已安裝的應用程式」。
     b. 按一下「Android」或「iOS」標籤，然後在偵測到或已安裝的應用程式清單中，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」或是「應用程式 > 已安裝的應用程式」。
     b. 按一下「Android」或「iOS」標籤，然後在偵測到或已安裝的應用程式清單中，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」：您可以將允許使用者解除安裝「行動裝置代理程式」的功能啟動或關閉。此外，您也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。

  以下是有關解除安裝防護的功能清單：

  - 從管理主控台開啟/關閉解除安裝防護。
  - 密碼長度必須介於六 (6) 到十二 (12) 個字元之間；密碼能包含數字、字元或符號。
  - 可從管理主控台針對每個群組設定密碼。

  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，「垃圾簡訊防護政策」、「來電過濾政策」及「Web 威脅防護政策」的過濾清單不會受到影響。如需詳細資訊，請參閱垃圾簡訊防護政策 第 5-15 頁、垃圾簡訊 WAP Push 防護政策 第 5-16 頁及安全政策 第 5-12 頁。

- 更新設定：您可以選擇讓「行動安全防護管理伺服器」在有新的可用更新元件時通知「行動裝置代理程式」。您也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。
- 記錄設定：「行動裝置代理程式」偵測到安全威脅（如 Android 作業系統上的惡意程式）時，會在行動裝置上產生記錄。

Wi-Fi 政策

Wi-Fi 政策可讓您將組織的 Wi-Fi 網路資訊，包括網路名稱、安全防護類型與密碼，傳送到 Android 與 iOS 行動裝置。

若要設定 Wi-Fi 政策設定，請按一下「政策」，再按一下「政策名稱」，最後按一下「Wi-Fi 政策」。

Exchange ActiveSync 政策

Exchange ActiveSync 政策可讓您為組織建立 Exchange ActiveSync 政策，並傳送到 iOS 行動裝置。

若要設定 Exchange ActiveSync 政策設定，請按一下「政策」，再按一下「政策名稱」，最後按一下「Exchange ActiveSync 政策」。

VPN 政策

VPN 政策設定可讓您為公司建立 VPN 政策，並傳送到 iOS 行動裝置。

若要設定 VPN 政策設定，請按一下「政策」，再按一下政策名稱，最後按一下「VPN 政策」。

全域 HTTP Proxy 政策

「全域 HTTP Proxy 政策」可讓您將組織的 Proxy 資訊傳送給行動裝置。此政策僅適用於監督模式的 iOS 行動裝置。

若要設定「全域 HTTP Proxy 政策」設定，請按一下「政策」再按一下「政策名稱」，最後按一下「全域 HTTP Proxy 政策」

憑證政策

「憑證政策」可讓您匯入必須在 iOS 行動裝置上部署的憑證。

若要設定憑證政策設定，請按一下「政策」，再按一下「政策名稱」，最後按一下「憑證政策」。

單一登入政策

單一登入 (SSO) 政策可讓使用者在不同的應用程式之間（包括「行動安全防護」與來自應用程式商店的應用程式）使用相同的認證。每個使用 SSO 憑證設定的新應用程式會驗證企業資源的使用者權限，並且無需要求使用者重新輸入密碼即可登入。

單一登入政策包含下列資訊：

- 「名稱」：Kerberos 主體名稱。
- 「領域」：Kerberos 領域名稱。

  Kerberos 領域名稱應採用正確的大寫形式。
- 「URL 首碼」（選用）：必須相符的 URL 清單，以使用帳號透過 HTTP 進行 Kerberos 驗證。如果此欄位為空白，表示此帳號符合所有 HTTP 與 HTTPS URL。URL 符合模式必須以 http 或 https 開頭。

  這個清單的每個項目都必須包含 URL 首碼。只有以帳號中某個字串開頭的 URL，才能存取 Kerberos 票證。URL 符合模式必須包含配置。例如，http://www.example.com/。對於結尾不是 / 的符合模式，會自動向 URL 新增 /。
- 「應用程式識別碼」（選用）：允許使用此帳號的應用程式識別碼清單。如果此欄位為空白，則此帳號符合所有應用程式識別碼。

  「應用程式識別碼」陣列必須包含符合應用程式套件識別碼的字串。這些字串可能是完全相符的字串（例如 com.mycompany.myapp），或者可使用 * 萬用字元根據套件識別碼指定首碼符合字串。萬用字元必須顯示在句號字元 (.) 的後面，並且只能顯示在字串的結尾（例如 com.mycompany.*）。使用萬用字元時，套件識別碼以該首碼開頭的任何應用程式都將獲得此帳號的存取權。

若要設定「適用於 iOS 的單一登入政策」設定，請按一下「政策」，再按一下政策名稱，最後按一下「單一登入政策」。

AirPlay/AirPrint 政策

AirPlay/AirPrint 政策設定可讓您為公司建立 AirPlay 和 AirPrint 政策，並傳送到 iOS 行動裝置。

若要設定 AirPlay 和（或）AirPrint 政策設定，請按一下「政策」，再按一下政策名稱，最後按一下「AirPlay/AirPrint 政策」。

行動數據網路政策

行動數據網路政策設定可讓您為組織配置行動數據網路設定，並傳送到 iOS 行動裝置。

若要設定行動數據網路政策設定，請按一下「政策」，再按一下政策名稱，最後按一下「行動數據網路政策」。

佈景主題政策

佈景主題政策設定可讓您針對 iOS 行動裝置為主畫面和鎖定畫面推播字型並設定桌布。此政策僅適用於處於監督模式的 iOS 行動裝置。

若要配置佈景主題政策設定，請按一下「政策」，再按一下政策名稱，最後按一下「佈景主題政策」。

受管理的網域政策

受管理的網域政策讓您可以設定您的公司所管理的電子郵件和/或 Web 網域。

- 未標示的電子郵件網域：當使用者使用系統電子郵件用戶端撰寫電子郵件時，輸入的任何不符合已設定的網域的電子郵件地址將會以紅色亮顯（標記）。系統管理員應該考慮使用此功能，以警告可能無意中試圖傳送敏感資訊給不受信任的電子郵件地址的使用者。
- 受管理的 Safari Web 網域：您可以指定使用 Safari 從特定網域下載的檔案只能使用受管理的應用程式開啟。例如，從 internal.example.com 下載的

PDF 能夠使用 Adobe Reader（受管理的應用程式）開啟，但不能使用 Dropbox（不受管理的應用程式）開啟。這可以改善 Safari 的傳輸，並擴展其作為企業瀏覽器的使用範圍。

重要

您必須在功能鎖定政策中關閉以下 iOS 功能。否則，受管理的 Safari Web 網域設定將不起任何作用，因為下載的檔案無法使用其他（不受管理的）應用程式開啟：

- 在其他應用程式（7.0 或更高版本）中從受管理的應用程式開啟文件
- 在受管理的應用程式中從其他應用程式（7.0 或更高版本）開啟文件

若要設定受管理的網域政策設定，請按一下「政策」，再按一下政策名稱，最後按一下「受管理的網域政策」。

安全政策

您可以從「安全政策」畫面設定「安全設定」。

「安全政策」畫面還可讓您管理 Android 行動裝置適用的 Web 威脅防護政策。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 5-3. 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。	

區段	項目	說明	支援的行動裝置作業系統
	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。	
	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/	

垃圾簡訊防護政策

「行動安全防護」中的垃圾簡訊防護政策能抵禦垃圾郵件 WAP Push 和簡訊。

若要設定垃圾簡訊防護政策設定，請按一下「政策」，再按一下政策名稱，最後按一下「垃圾簡訊防護政策」。

垃圾簡訊防護政策

這項功能可讓您從伺服器端控管垃圾簡訊防護政策。以下是在設定垃圾簡訊防護政策時可用的功能：

- 啟動或關閉行動裝置的垃圾簡訊防護
- 設定行動裝置以使用封鎖清單、核可清單，或關閉行動裝置的垃圾簡訊防護功能
- 從管理主控台設定核可的清單
- 從管理主控台設定封鎖的清單

請參閱下表中有關「核可的清單」或「封鎖的過濾清單」設定詳細資訊。

表 5-4. 垃圾簡訊防護政策的過濾清單設定

中央控管	使用者控管	說明
已關閉	已啟動	使用者可在行動裝置代理程式上編輯「核可的清單」或「封鎖的清單」。 「行動安全防護」會根據下列優先順序允許或封鎖訊息： 1. 行動裝置代理程式的核可的清單 2. 行動裝置代理程式的封鎖的清單

中央控管	使用者控管	說明
已啟動	已關閉	僅允許使用者在行動裝置代理程式上編輯「核可的清單」或「封鎖的清單」。 「行動安全防護」會根據下列優先順序允許或封鎖訊息： 1. 伺服器上的核可的清單或封鎖的清單 2. 行動裝置代理程式的核可的清單 3. 行動裝置代理程式的封鎖的清單
已啟動	已啟動	使用者可檢視或編輯由系統管理員定義的「核可的清單」/「封鎖的清單」，也可以在行動裝置代理程式上使用「核可的清單」/「封鎖的清單」。 當安全防護政策與行動裝置代理程式同步時，便不會將過濾清單同步化，並根據政策更新所有其他的設定。 「行動安全防護」會根據下列優先順序允許或封鎖訊息： 1. 行動裝置代理程式的核可的清單 2. 行動裝置代理程式的封鎖的清單 3. 伺服器上的核可的清單或封鎖的清單

注意

簡訊的「核可的清單」與「封鎖的清單」必須使用下列格式："[name1:]number1;[name2:]number2;..."。

'name' 的長度不得超過 30 個字元；電話號碼的長度應介於 4 到 20 個字元之間，並且能包含以下項目：0-9、+、-、#、(、) 及空格。項目的數量上限不得超過 200 個。

垃圾簡訊 WAP Push 防護政策

這項功能可讓您從伺服器端控管 WAP Push 防護。在啟動後，您可以選取是否要使用 WAP 核可清單。

注意

WAP 核可清單必須使用下列格式："[name1:]number1;[name2:]number2;...".

'name' 的長度不得超過 30 個字元；電話號碼的長度應介於 4 到 20 個字元之間，並且能包含以下項目：0-9、+、-、#、(、) 及空格。項目的數量上限不得超過 200 個。

以下是在設定 WAP Push 防護政策時可用的功能清單：

- 從行動裝置啟動或關閉 WAP Push 防護
- 設定行動裝置以使用核可清單或關閉行動裝置上的 WAP Push 防護
- 從管理主控台設定核可的清單
- 如果系統管理員已啟動伺服器端控管，使用者便無法變更由系統管理員定義的 WAP Push 防護類型
- 如果系統管理員已關閉伺服器端控管，並允許使用者在行動裝置上設定「行動安全防護」設定，則使用者無法檢視或編輯由系統管理員設定的 WAP Push 防護清單，但他們能在行動裝置端編輯個人的 WAP Push 防護

注意

在「行動裝置代理程式」上套用垃圾簡訊防護政策後，將清除使用者的垃圾簡訊個人設定。

來電過濾政策

這項功能可讓您從伺服器端控管來電過濾政策。若要設定來電過濾政策設定，請按一下「政策」，再按一下「政策名稱」，最後按一下「過濾政策」。

以下是在設定來電過濾政策時可用的功能：

- 啟動或關閉行動裝置的來電過濾
- 設定行動裝置以使用封鎖清單或核可清單
- 從管理主控台設定核可的清單

- 從管理主控台設定封鎖的清單

請參閱下表中有關「核可的清單」或「封鎖的過濾清單」設定詳細資訊。

表 5-5. 來電過濾政策的過濾清單設定

中央控管	使用者控管	說明
已關閉	已啟動	使用者可在行動裝置代理程式上編輯「核可的清單」或「封鎖的清單」。 「行動安全防護」會根據下列優先順序允許或封鎖 URL： 1. 行動裝置代理程式的核可的清單 2. 行動裝置代理程式的封鎖的清單
已啟動	已關閉	僅允許使用者在行動裝置代理程式上編輯「核可的清單」或「封鎖的清單」。 「行動安全防護」會根據下列優先順序允許或封鎖來電： 1. 伺服器上的封鎖的清單 2. 行動裝置代理程式的核可的清單 3. 行動裝置代理程式的封鎖的清單 您也可以在 Android 行動裝置上為撥出通話設定伺服器端控管功能。

中央控管	使用者控管	說明
已啟動	已啟動	使用者可檢視或編輯由系統管理員定義的「核可的清單」/「封鎖的清單」，也可以在行動裝置代理程式上使用「核可的清單」/「封鎖的清單」。 當安全防護政策與行動裝置代理程式同步時，便不會將過濾清單同步化，並根據政策更新所有其他的設定。 「行動安全防護」會根據下列優先順序允許或封鎖來電： 1. 行動裝置代理程式的核可的清單 2. 行動裝置代理程式的封鎖的清單 3. 伺服器上的封鎖的清單 您也可以在 Android 行動裝置上為撥出通話設定伺服器端控管功能。

注意

來電過濾核可的清單與封鎖的清單必須使用下列格式："[name1:]number1;[name2:]number2;..."。

'name' 的長度不得超過 30 個字元；電話號碼的長度應介於 4 到 20 個字元之間，並且能包含以下項目：0-9、+、-、#、(、) 及空格。項目的數量上限不得超過 200 個。

密碼政策

密碼政策可預防未經授權的使用者存取行動裝置上的資料。

若要配置密碼政策設定，請按一下「政策」，再按一下政策名稱，最後按一下左邊的功能表的「密碼政策」。

功能鎖定政策

這項功能可讓您限制（關閉）或允許（啟動）某些行動裝置功能/元件的使用。例如，您可以關閉某個群組中所有行動裝置的相機。

若要設定「功能鎖定政策」設定，請按一下「政策」，再按一下政策名稱，最後按一下左邊的功能表的「功能鎖定政策」。

如需支援的功能/元件清單，請參閱支援的行動裝置作業系統功能 第 1-13 頁。

警告!

關閉 WLAN/WIFI 和（或）Microsoft ActiveSync 時請務必謹慎。如果行動裝置無法使用這兩個選項，可能會無法與伺服器通訊。

對於 Android 行動裝置，您也可以新增存取點，以控管存取點範圍內的裝置元件可用性。

合規政策

合規政策可讓您設定行動裝置的合格條件。如果有任何不合格的行動裝置，「行動安全防護」會將行動裝置的不合規狀態顯示在伺服器 UI 中。「行動安全防護」也會傳送電子郵件至不合格的 iOS 行動裝置，但對於不合格的 Android 行動裝置則會在裝置上顯示通知。合規檢查清單包括：

- 「已開放 Root 權限/已破解」— 檢查行動裝置是否已開放 Root 權限/已破解。
- 「未加密」— 檢查行動裝置上的加密功能是否已啟動。
- 「作業系統版本檢查」— 檢查作業系統版本是否符合定義的條件。

若要設定合規政策設定，請按一下「政策」，再按一下「政策名稱」，最後按一下「合規政策」。

應用程式監控與控管政策

應用程式監控與控管政策能讓您從伺服器端控管安裝在行動裝置上的應用程式，以及將必要應用程式推播到行動裝置。

若要設定應用程式監控與控管政策設定，請按一下「政策」，再按一下政策名稱，最後按一下「應用程式監控與控管政策」。

- 「必要應用程式」 — 使用此選項能將新增至清單中的所有應用程式推播到行動裝置。您也可以將 VPN 連結至應用程式，讓應用程式總是使用此 VPN 來連線至網路。
- 「允許的應用程式」 — 藉由使用「核可的清單」和「封鎖的清單」，來控管安裝在行動裝置上的應用程式。

  對於 iOS 行動裝置，若有任何應用程式不符合政策，「行動安全防護」便會傳送通知給系統管理員與使用者。

  對於 Android 行動裝置，「行動安全防護」會封鎖不符合政策的應用程式，並允許所有其他符合政策的應用程式。

  - 「啟動系統應用程式封鎖」（僅限 Android）：

    若已選取，「行動安全防護」會封鎖 Android 行動裝置上的所有系統應用程式。

  - 「啟動應用程式類別」：選取您要在行動裝置上啟動或關閉的應用程式類別。如需例外處理，您也可以將屬於這些類別的應用程式新增至「核可的清單」或「封鎖的清單」。例如，如果您已關閉「遊戲」類別類型，「行動安全防護」便會封鎖屬於這個類別的所有應用程式，但位於「核可的清單」中的這類應用程式除外。

    「行動安全防護」會根據下列優先順序允許或封鎖應用程式：

    1. 「核可的清單」—「行動安全防護」允許啟動「核可的清單」中的應用程式，即使這些應用程式屬於您已關閉的類別。
    2. 「封鎖的清單」—「行動安全防護」會封鎖「封鎖的清單」中的應用程式，即使這些應用程式屬於您已啟動的類別。
    3. 「應用程式權限」—「行動安全防護」會根據您為應用程式所屬類別選取的權限狀態來允許或封鎖應用程式。

- 「啟動應用程式權限」（僅限 Android）：選取您要在 Android 行動裝置上啟動或關閉的應用程式服務。如需例外處理，您也可以將使用這些服務的應用程式新增至「核可的清單」或「封鎖的清單」。例如，如果您已關閉「讀取資料」服務類型，「行動安全防護」便會封鎖使用「讀取資料」服務的所有應用程式，但在「核可的清單」中的這類應用程式除外。

  「行動安全防護」會根據下列優先順序允許或封鎖應用程式：

  1. 「核可的清單」—「行動安全防護」允許啟動「核可的清單」中的應用程式，即使這些應用程式使用您已關閉的服務。
  2. 「封鎖的清單」—「行動安全防護」會封鎖「封鎖的清單」中的應用程式，即使這些應用程式屬於您已啟動的服務。
  3. 「應用程式權限」—「行動安全防護」會根據您為應用程式所使用服務選取的權限狀態來允許或封鎖應用程式。

- 「僅允許下列應用程式」：將您要允許使用者在其行動裝置上使用的應用程式新增至「核可的清單」。若已啟動：
  - 如果「行動安全防護」偵測到不在「核可的清單」中的應用程式，便會在 Android 行動裝置上顯示快顯警告訊息。
  - 在 iOS 行動裝置上，如果「行動安全防護」偵測到任何不在「核可的清單」中的應用程式，「行動安全防護」便會傳送電子郵件通知給使用者。
- 「僅封鎖下列應用程式」：將您不希望使用者在其行動裝置上使用的應用程式新增至「封鎖的清單」。若已啟動：
  - 如果「行動安全防護」偵測到在「封鎖的清單」中的應用程式，便會在 Android 行動裝置上顯示快顯警告訊息。
  - 在 iOS 行動裝置上，如果「行動安全防護」偵測到任何在「封鎖的清單」中的應用程式，「行動安全防護」便會傳送電子郵件通知給使用者。
- 「鎖定至應用程式（僅限於監督模式）」— 將 iOS 行動裝置限制為指定的應用程式。

「行動安全防護」會檢查受限制的應用程式並傳送電子郵件警訊給使用者：

- 根據「管理 > 通訊伺服器設定 > 一般設定 (標籤)」中的「資訊收集頻率」設定自動傳送電子郵件警訊，或
- 當您更新「管理 > 通訊伺服器設定 > 一般設定 (標籤)」中的「資訊收集頻率」時傳送電子郵件警訊。

大量購買方案政策

此政策可讓系統管理員將透過 Apple 「大量購買方案」購買的 iOS 應用程式匯入到「行動安全防護」管理 Web 主控台。「行動安全防護」會將「大量購買方案」清單中的所有應用程式發送至群組中的行動裝置。

若要設定「大量購買方案」政策：

1. 將應用程式新增至「企業應用程式商店」。如需相關程序，請參閱新增應用程式 第 6-2 頁。
2. 按一下「政策」，再按一下政策名稱，最後按一下「大量購買方案政策」。
3. 按一下「匯入」，再選取要從「企業應用程式商店」匯入的應用程式。
4. 按一下「儲存」將所有的應用程式發送到 iOS 行動裝置。

容器政策

此政策可讓您管理 Samsung KNOX 容器安全設定。您可以針對帳號設定核可的清單或封鎖的清單、套用限制，以及配置瀏覽器、密碼及應用程式設定。

注意

啟動此政策之前，請先在 Mobile Security 中設定 KNOX 授權。若要設定 KNOX 授權，請在管理 Web 主控台中瀏覽至「管理 > 產品授權」。

- 帳號設定：使用核可和（或）封鎖的清單，指定可在 Samsung KNOX 容器上新增或限制的帳號。

- 限制設定：在 Samsung KNOX 容器上關閉相機或檔案共用。
- 瀏覽器設定：在 Samsung KNOX 容器上配置原生 Android 網路瀏覽器的安全設定。
- 密碼設定：配置 Samsung KNOX 容器的密碼安全設定。
- 應用程式設定：設定以下清單：
  - 過濾應用程式清單：在 Samsung KNOX 容器上設定核可或封鎖的清單，以限制應用程式安裝。
  - 必要的應用程式：設定必要應用程式清單，以指定必須安裝在 Samsung KNOX 上的應用程式。
  - 關閉應用程式：設定關閉應用程式清單，以關閉行動裝置上的某些應用程式。如果此清單中的應用程式已安裝在行動裝置上，系統不會將其移除，不過使用者將無法使用這些應用程式。

若要配置容器政策設定，請按一下「政策」，再按一下政策名稱，最後按一下「容器政策」。

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 5-26 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 5-26 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」。

設定應用程式可用性

「行動安全防護」可讓您針對特定政策設定要提供給 iOS 和 Android 行動裝置的應用程式。

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「政策 > 適用於群組的政策」。

   「政策」畫面隨即出現。
3. 在「可用的應用程式」欄下方按一下政策的應用程式數量。

   「可用的應用程式」畫面隨即顯示。
4. 按一下「iOS 應用程式」或「Android 應用程式」標籤。
5. 請執行以下任一項工作：
   - 若要啟動或關閉應用程式，請針對要切換的應用程式按一下「權限」欄下方的按鈕。

- 若要啟動或關閉所有應用程式，請按一下「全部啟動」或「全部關閉」。

6. 在「權限」欄中切換應用程式的可用性。

第 6 章

管理應用程式

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：

關於企業應用程式商店

「企業應用程式商店」可讓您建立 Web 剪輯與應用程式清單，供使用者下載與安裝在其 Android 或 iOS 行動裝置上。

您也可以在「行動安全防護」管理 Web 主控台上將從 Apple「大量購買方案」購買的 iOS 應用程式上傳到「企業應用程式商店」。

管理企業應用程式

新增應用程式

步驟

1. 在「行動安全防護」管理 Web 主控台上，移至「應用程式 > 企業應用程式商店」。

   隨即顯示「企業應用程式商店」畫面。

2. 按一下「Android」或「iOS」標籤。

3. 按一下「新增」。

   「新增應用程式」視窗會隨即顯示。

4. 您現在可以使用下列選項將應用程式新增至清單中：

   - 「從本機電腦新增」— 選取 Android 或 iOS 行動裝置的安裝檔。
   - 新增 Web 剪輯 — 輸入應用程式 URL 後，應用程式的圖示會出現在使用者的行動裝置主畫面中，並且會使用行動裝置上的預設網路瀏覽器開啟連結。
   - (Android)「從外部應用程式商店新增」— 輸入外部應用程式商店中的應用程式連結。應用程式的圖示會出現在使用者行動裝置的主畫面中，並且會使用行動裝置上的預設網路瀏覽器開啟連結。
   - (iOS)「從 iTunes Store 新增應用程式連結— 在「搜尋關鍵字」欄位中輸入您要搜尋的 VPP 應用程式名稱，選取要在哪個國家/地區的

Apple 應用程式商店搜尋該應用程式，然後從搜尋結果中選取您要新增的應用程式。一旦新增後，VPP 應用程式只會出現在「行動安全防護」管理 Web 主控台的「應用程式商店」中。若要將應用程式推播到行動裝置，您必須將應用程式新增到「大量購買方案政策」。如需相關程序，請參閱大量購買方案政策 第 5-23 頁。

5. 按一下「繼續」。

「編輯應用程式」畫面會隨即顯示。

6. 設定下列項目：

- 應用程式名稱：輸入應用程式的名稱。
- 應用程式圖示：如果應用程式圖示未出現，請按一下「上傳應用程式圖示」以選取並上傳應用程式圖示。
- 應用程式識別碼：如果應用程式識別碼未出現，請輸入應用程式識別碼。
- 「VPP 代碼檔案」：對於 iOS VPP 應用程式，請上傳您從 Apple 收到的「大量購買代碼檔案」。
- 類別：為應用程式選取類別。

注意

您必須從下拉式清單選取一個類別。若要新增或刪除類別，請按一下「類別」按鈕。

- 說明：輸入應用程式的說明。
- 發佈：選取以下其中一項：
  - 「不要發佈」— 將伺服器上的應用程式上傳，但對行動裝置則隱藏該應用程式。
  - 「發佈為生產版本」— 將伺服器上的應用程式上傳，並將它發佈以供行動裝置下載。
  - 發佈為 Beta 版本 — 將伺服器上的應用程式上傳，並將它發佈為 Beta 版本以供行動裝置下載。

- 螢幕擷取畫面：選取並上傳應用程式螢幕擷取畫面。

7. 按一下「繼續」。

   應用程式隨即出現在應用程式清單中。

編輯應用程式資訊

步驟

1. 在「行動安全防護」管理 Web 主控台上，移至「應用程式 > 企業應用程式商店」。

   隨即顯示「企業應用程式商店」畫面。

2. 按一下「Android」或「iOS」標籤。

3. 按一下您要編輯其資訊的應用程式名稱。

   「編輯應用程式」視窗隨即顯示。

4. 修改畫面的詳細資訊。

5. 按一下「繼續」。

刪除應用程式商店中的應用程式

步驟

1. 在「行動安全防護」管理 Web 主控台上，移至「應用程式 > 企業應用程式商店」。

   隨即顯示「企業應用程式商店」畫面。

2. 按一下「Android」或「iOS」標籤。

3. 選取您要刪除的應用程式。

4. 按一下「刪除」，再按一下確認對話方塊上的「確定」。

管理應用程式類別

新增應用程式類別

步驟

1. 在「行動安全防護」管理 Web 主控台上，移至「應用程式 > 企業應用程式商店」。

   隨即顯示「企業應用程式商店」畫面。

2. 按一下「Android」或「iOS」標籤。
3. 按一下「管理類別」。
4. 按一下「新增」。

   「新增類別」視窗隨即顯示。

5. 輸入類別名稱與說明，然後按一下「儲存」。

編輯應用程式類別

步驟

1. 在「行動安全防護」管理 Web 主控台上，移至「應用程式 > 企業應用程式商店」。

   隨即顯示「企業應用程式商店」畫面。

2. 按一下「iOS 應用程式」標籤或「Android 應用程式」標籤。
3. 按一下「管理類別」。

4. 按一下您要編輯的類別名稱。

   「編輯類別」視窗隨即顯示。

5. 修改類別詳細資訊，再按一下「儲存」。

刪除應用程式類別

步驟

1. 在「行動安全防護」管理 Web 主控台上，移至「應用程式 > 企業應用程式商店」。

   隨即顯示「企業應用程式商店」畫面。

2. 按一下「Android」或「iOS」標籤。

3. 按一下「管理類別」。

4. 選取您要刪除的類別，按一下「刪除」，然後按一下確認對話方塊中的「確定」。

透過「大量購買方案」管理購買的應用程式

重要

VPP 僅在某些地區適用。請確定您的公司符合資格。如需詳細資料，請參閱以下連結：

http://www.apple.com/business/vpp/

Apple 使用兌換代碼和「大量購買方案」(VPP) 授權購買大量應用程式。由於您無法將兌換代碼轉換為 VPP 授權，因此 Mobile Security 支援這兩個選項。

「大量購買方案」可讓您將 VPP 授權散發給 iOS 應用程式的使用者或裝置。

可以透過監控剩餘授權數量和回收授權來管理 VPP 應用程式。即使使用者尚未在其行動裝置上安裝 Mobile Security 用戶端應用程式，也可以使用 VPP 應用程式。

注意

「行動安全防護」不會將 VPP 應用程式推播至行動裝置。使用者需要從 Apple 應用程式商店的下列位置手動將 VPP 應用程式下載到其行動裝置：「應用程式商店 > 更新 > 已購買」。

設定大量購買方案授權

步驟

1. 瀏覽至以下 URL：

   http://www.apple.com/business/vpp/

2. 使用您的 Apple 帳號登入，並從 Apple 大量購買方案 Web 入口網站下載服務 Token 檔案。

3. 在「行動安全防護」管理 Web 主控台上，移至「應用程式 > 企業應用程式商店 > iOS」。

   「iOS 企業應用程式商店」畫面隨即顯示。

4. 移至「大量購買方案 (VPP) 管理 > VPP 設定」。

5. 在提供的欄位中上傳從 Apple Web 入口網站下載的 Token 檔案，並等待上傳完成。

6. 按一下「立即同步」。

指定或回收 VPP 授權

「行動安全防護」可讓您將透過「大量購買方案」購買的應用程式授權指定給使用者或裝置，或回收這些授權。

重要

指定或回收應用程式之前，請確定「大量購買方案授權」已準備就緒。

如需詳細資訊，請參閱設定大量購買方案授權 第 6-7 頁。

步驟

1. 在「行動安全防護」管理 Web 主控台上，移至「應用程式 > 企業應用程式商店 > iOS > 大量購買方案 (VPP) 管理」。
2. 在「應用程式清單」下，找到應用程式，然後按一下「指定/回收」。

   「指定/回收授權」畫面隨即出現。
3. 若要指定授權，請執行下列步驟。
   - 指定授權給裝置：
     a. 在「裝置」標籤上，選取狀態為「已取消指定」的一或多個裝置。
     b. 按一下「指定」。

     注意

     在指定應用程式給裝置時，「大量購買方案」具有下列限制：
     - 您只能將 VPP 應用程式指定給執行 iOS 9 或更新版本的裝置。
     - 應用程式開發人員必須同意裝置指定。
   - 指定授權給使用者：
     a. 在「使用者」標籤上，選取狀態為「已取消指定」的一或多個使用者。
     b. 按一下「指定」。

注意

在指定 VPP 授權後，「行動安全防護」會傳送通知給使用者。

若要修改使用者通知設定，請移至「通知和報告 > 使用者通知 > VPP 使用者通知」。

成功指定授權。

4. 若要回收授權，請執行下列步驟。
   - 從裝置回收授權：
     a. 在「裝置」標籤上，選取狀態為「已指定」的一或多個裝置。
     b. 按一下「回收」。
   - 從使用者回收授權：
     a. 在「使用者」標籤上，選取狀態為「已指定」的一或多個使用者。
     b. 按一下「回收」。

   成功回收授權。

檢查 VPP 使用者的狀態

步驟

1. 在「行動安全防護」管理 Web 主控台上，移至「應用程式 > 企業應用程式商店 > iOS」。

   「iOS 企業應用程式商店」畫面隨即顯示。

2. 移至「大量購買方案 (VPP) 管理 > VPP 使用者清單」。
3. 在「狀態」欄下，查看使用者狀態。

   「狀態」欄可能會顯示下列其中一種狀態：

   - -：您尚未將任何應用程式指派給此使用者。

- 「已註冊」：您已至少指派一個應用程式給使用者，但該使用者尚未將 Apple ID 與電子郵件地址關聯。
- 「已關聯」：您已至少指派一個應用程式給使用者，且該使用者已將 Apple ID 與電子郵件地址關聯。
- 「已淘汰」：您已回收指派給此使用者的所有授權。

從使用者回收所有授權

「行動安全防護」可讓您回收使用者的所有授權。

步驟

1. 在「行動安全防護」管理 Web 主控台上，移至「應用程式 > 企業應用程式商店 > iOS」。

   「iOS 企業應用程式商店」畫面隨即顯示。

2. 按一下「大量購買方案 (VPP) 管理 > VPP 使用者清單」。
3. 從清單中選取使用者，然後按一下「淘汰」。
4. 按一下「使用者清單」畫面上的「關閉」。

關於已安裝的應用程式

「已安裝的應用程式」畫面會列出所有受管理的 Android 和 iOS 裝置上安裝的所有應用程式。

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 5-5 頁和從核可的清單移除應用程式 第 5-6 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 6-1. 已安裝的應用程式資訊

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	●	●
安裝數量	已安裝應用程式的裝置數量	●	●

檢視已安裝的應用程式

步驟

1. 在「行動安全防護」Web 主控台上，移至「應用程式 > 安裝的應用程式」。

   「安裝的應用程式」標籤隨即出現。

2. 按一下「Android」或「iOS」標籤。

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。

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 5-5 頁和從核可的清單移除應用程式 第 5-6 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 5-4 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

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、政策違規記錄、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。

注意

您可以在行動裝置上檢視垃圾簡訊防護、WAP Push 防護及來電過濾等記錄。

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。
- 政策違規記錄 — 這些記錄包含「行動裝置代理程式」的政策合規狀態的相關資訊。
- 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。

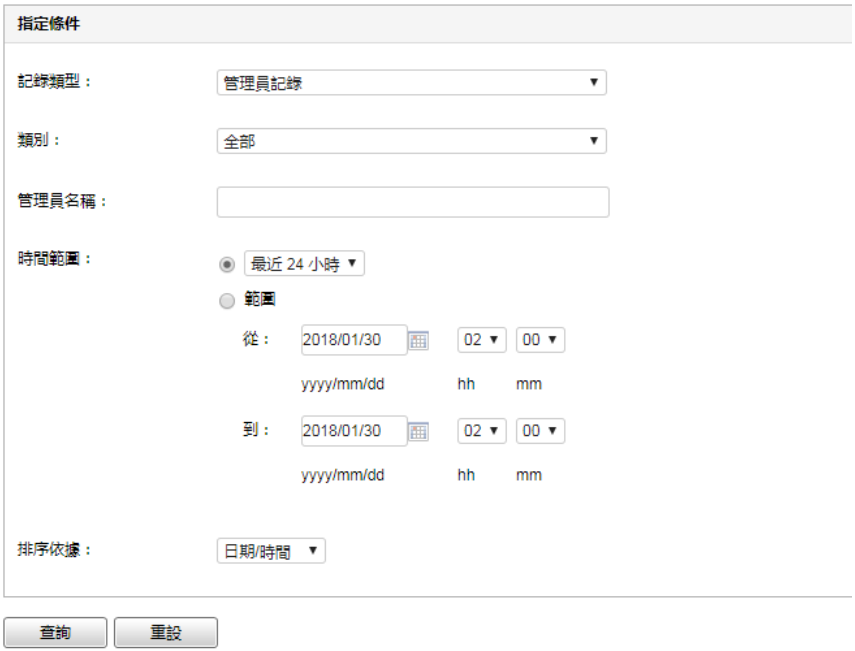

圖 8-1.「記錄查詢」畫面

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 9 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。
- 「已關閉行動安全防護的裝置管理員」— 在任何 Android 行動裝置的「裝置管理員」清單中關閉「行動安全防護」時，傳送電子郵件通知給系統管理員。在電子郵件中，Token 變數 <%DEVICE%> 將取代為行動裝置名稱。
- 「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。
- 「VPP Token 到期警告」—在 VPP Token 到期前 15 天傳送電子郵件通知給系統管理員。
- 「DEP Token 到期警告」—在 DEP Token 到期前 15 天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。

     重要

     修改通知訊息時，請包含預設電子郵件範本中提供的 Token 變數。

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。
- 「合規違規報告」— 顯示合規違規的相關資訊。
- 「應用程式資產清單報告」— 顯示最多人在 Android 和 iOS 裝置上安裝的應用程式的相關資訊。
- 「裝置註冊報告」— 顯示裝置註冊的相關資訊。
- 「裝置取消註冊報告」— 顯示裝置取消註冊的相關資訊。

您可以從「報告」畫面執行下列工作。

表 9-1. 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 9-6 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 9-7 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 9-7 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 9-8 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 9-6 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 9-6 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。

- 「政策違規」— 行動裝置與合格條件不符時，傳送電子郵件通知給行動裝置。Token 變數 <%DEVICE%> 和 <%VIOLATION%> 將取代為電子郵件中行動裝置的名稱和行動裝置違反的政策。
- 「VPP 使用者通知」—當系統管理員指定 VPP 應用程式給使用者時傳送電子郵件通知給行動裝置。

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 10 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 10-4 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 10-2 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 10-4 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 10-2 頁；如需預約更新的詳細資訊，請參閱預約更新 第 10-3 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 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。

- 使用者無法在裝置上輸入 Nanoscale 密碼。

  行動裝置數字鍵台僅支援特定字元集。「行動安全防護」建議，系統管理員應編譯裝置所支援的字元清單。編譯支援的字元清單後，系統管理員接著可從管理主控台使用支援的字元清單設定解除安裝防護密碼。

- 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」。

- iOS 行動裝置無法順利向「管理伺服器」註冊，並顯示「URL 不受支援」錯誤訊息。

  如果 SCEP 伺服器的系統時鐘設為不正確的時間，或「趨勢科技行動安全防護」未取得「簡單憑證註冊通訊協定」(SCEP) 憑證，即可能發生此問題。請務必將 SCEP 伺服器的系統時鐘設為正確的時間。如果問題持續發生，請執行下列步驟：

  1. 登入「行動安全防護」管理 Web 主控台。
  2. 按一下「管理 > 通訊伺服器設定」。
  3. 不變更設定，按一下「儲存」。

- 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」。

- 某些 Android 行動裝置的狀態一直都是「未同步」。

  這是因為該行動裝置未啟動「行動安全防護」裝置管理員。如果使用者未在「裝置管理員」清單中啟動「行動安全防護」，「行動安全防護」即無法對行動裝置同步處理伺服器政策，而會將其狀態顯示為「未同步」。

- 「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: TSCM98144/180126