TREND MICRO™

9.0

趨勢科技™ 行動安全防護™ 系統管理員手冊

企業版攜帶型裝置全面性安全解決方案

端點安全

文件編號：TSTM96390/140410

發行日期：2014 年 3 月

「趨勢科技™ 企業版行動安全防護 9.0 SP1 版」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

前言 vii
對象 viii
行動安全防護文件 viii
文件慣例 ix

第 1 章：簡介

瞭解行動裝置威脅 1-2
關於趨勢科技行動安全防護 9.0 版 SP1 1-2
行動安全防護系統架構 1-3
行動安全防護系統元件 1-3
比較本機與雲端通訊伺服器 1-5
此版本（9.0 版 SP1）的新功能 1-6
此版本（8.0 版 SP1）的新功能 1-7
此版本（8.0 版）的新功能 1-8
此版本（7.1 版）的新功能 1-9
此版本（7.0 版）的新功能 1-10
行動裝置代理程式的主要功能 1-11
支援的行動裝置作業系統功能 1-13

第 2 章：開始使用行動安全防護

管理 Web 主控台 2-2
存取管理 Web 主控台 2-2
關閉 Internet Explorer 中的相容性檢視 2-4
產品授權 2-4

報表資訊 2-5
自訂「報表」 2-7

管理設定 2-10
進行 Active Directory (AD) 設定 2-10
設定裝置驗證 2-10
進行資料庫設定 2-10
進行通訊伺服器設定 2-10
管理系統管理員帳號 2-10

指令佇列管理 2-17

Exchange 伺服器整合 2-18
進行 Exchange 伺服器整合設定 2-18
設定 MS Exchange 行動安全整合 2-18

管理憑證 2-19
上傳憑證 2-19
刪除憑證 2-19

第 3 章：管理行動裝置

受管理裝置標籤 3-2
行動安全防護的群組 3-2
管理群組 3-3
管理行動裝置 3-4
行動裝置狀態 3-8

行動裝置代理程式工作 3-10
更新行動裝置代理程式 3-10
遺失裝置防護 3-11
遠端重設密碼 3-14
匯出資料 3-16

邀請的裝置標籤 3-17
檢視邀請清單 3-17
重新傳送邀請訊息 3-18
取消作用中邀請 3-19
從清單移除邀請 3-19

Exchange ActiveSync 裝置標籤 3-20
邀請 Exchange ActiveSync 行動裝置 3-20

允許或封鎖存取 Exchange 伺服器 3-21
清除遠端 ActiveSync 行動裝置 3-21
移除 ActiveSync 行動裝置 3-22
與 Trend Micro Control Manager 整合 3-23
在 Control Manager 中建立安全防護政策 3-23
刪除或修改安全防護政策 3-23
Control Manager 的安全防護政策狀態 3-24

第 4 章：利用政策來保護裝置

關於安全防護政策 4-3
管理政策 4-4
建立政策 4-4
編輯政策 4-5
在群組中指派或移除政策 4-5
複製政策 4-6
刪除政策 4-6
行動安全防護中的安全防護政策 4-6
一般政策 4-7
Wi-Fi 政策 4-8
Exchange ActiveSync 政策 4-9
VPN 政策 4-9
全域 HTTP Proxy 政策 4-9
憑證政策 4-9
單一登入政策 4-9
惡意程式防護政策 4-10
垃圾簡訊防護政策 4-12
來電過濾政策 4-15
防火牆政策 4-17
Web 威脅防護政策 4-18
加密與密碼政策 4-18
功能鎖定政策 4-22
合規政策 4-23
應用程式監控與控管政策 4-23
大量購買方案政策 4-25

第 5 章：管理企業應用程式商店

關於企業應用程式商店 5-2
管理企業應用程式 5-2
新增應用程式 5-2
編輯應用程式資訊 5-4
刪除應用程式商店中的應用程式 5-4
管理應用程式類別 5-5
新增應用程式類別 5-5
編輯應用程式類別 5-5
刪除應用程式類別 5-6

第 6 章：更新元件

關於元件更新 6-2
更新行動安全防護元件 6-2
手動更新 6-2
預約更新 6-4
指定下載來源 6-5
手動更新本機 AU 伺服器 6-7

第 7 章：檢視及維護記錄

關於行動裝置代理程式記錄 7-2
檢視行動裝置代理程式記錄 7-2
記錄維護 7-4
預約記錄刪除 7-4
手動刪除記錄 7-5

第 8 章：使用通知和報告

關於通知訊息和報告 8-2
正在設定通知設定 8-2
設定電子郵件通知 8-2
進行簡訊發送器設定 8-3
處理簡訊發送器用戶端應用程式 8-6

系統管理員通知和預約報告 8-8
設定系統管理員通知 8-9
使用者通知 8-9
設定使用者通知 8-10

第 9 章：疑難排解及聯絡技術支援

疑難排解 9-2
聯絡技術支援前 9-5
聯絡技術支援 9-5
將中毒檔案傳送給趨勢科技 9-6
iTrendLabs 9-6
關於軟體更新 9-7
已知問題 9-8
其他有用的資源 9-8
關於趨勢科技 9-8

索引

索引 IN-1

序言

前言

歡迎使用《趨勢科技™企業版行動安全防護 9.0 版 SP1 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 第 viii 頁
- 行動安全防護文件 第 viii 頁
- 文件慣例 第 ix 頁

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（如 Smartphone 和 Pocket PC/Pocket PC Phone）
- 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 9.0 版 SP1」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 第 1-2 頁
- 關於趨勢科技行動安全防護 9.0 版 SP1 第 1-2 頁
- 行動安全防護系統架構 第 1-3 頁
- 行動安全防護系統元件 第 1-3 頁
- 此版本（9.0 版 SP1）的新功能 第 1-6 頁
- 行動裝置代理程式的主要功能 第 1-11 頁
- 支援的行動裝置作業系統功能 第 1-13 頁

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。

行動裝置除了惡意程式、垃圾郵件和其他不想要內容所產生的威脅之外，現在也容易受到駭客和拒絕服務 (DoS) 攻擊。現在，行動裝置成了這類攻擊的目標。許多行動裝置已具備相當的網路連線功能，以往只有筆記型電腦和桌上型電腦這類大型運算裝置才具備這樣的能力。

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 9.0 版 SP1

「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。

整合式防火牆與過濾功能可讓「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。

此外，「行動安全防護」也提供通用加密模組，可為 Symbian 與 Windows Mobile 裝置提供登入密碼防護與資料加密功能。此加密模組有助於防止資料在行動裝置遺失或遭竊時外洩。

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、簡訊管理和防火牆防護）的軟體產品可能會與「行動安全防護」不相容。

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式實行「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（雙伺服器安裝）與雲端通訊伺服器
- 強化安全模式（雙伺服器安裝）與本機通訊伺服器
- 基本安裝模式（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
Management 伺服器	「Management 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「Management 伺服器」和「行動裝置代理程式」之間的通訊。 「趨勢科技行動安全防護」提供兩種類型的「通訊伺服器」： • 本機通訊伺服器 (LCS) — 這是部署在您網路本機上的「通訊伺服器」。 • 雲端通訊伺服器 (CCS) — 這是部署在雲端的「通訊伺服器」，您不必安裝此伺服器。趨勢科技會管理「雲端通訊伺服器」，您只需從「Management 伺服器」連線至該伺服器即可。 請參閱比較本機與雲端通訊伺服器 第 1-5 頁。	必要
簡訊發送器	您可以使用「簡訊發送器」將簡訊傳送給使用者。	選用
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 伺服器通訊，並偵測使用 Exchange ActiveSync 服務的裝置。	選用
行動裝置代理程式 (MDA)	「行動裝置代理程式」安裝在受管理的行動裝置上。代理程式會與「行動安全防護」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 代管行動安全防護伺服器的資料庫。	必要
Active Directory	「行動安全防護」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」管理安全防護認證與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) 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
APNs 憑證	「行動安全防護」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	「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 5 與更新版的行動裝置則為必要。
BES User Administration Tool	必須有 BES User Administration Tool，才能支援管理在 BES 伺服器中註冊的 BlackBerry 裝置。	如果您想要管理 BlackBerry 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」伺服器取得報告，並傳送邀請給使用者。	選用

比較本機與雲端通訊伺服器

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	雲端通訊伺服器	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	不支援	支援
管理 Symbian 行動裝置	不支援	支援
管理 Windows Mobile 裝置	不支援	支援

此版本（9.0 版 SP1）的新功能

下表說明「趨勢科技™企業版行動安全防護 9.0 版 SP1」提供的新功能。

功能名稱	說明
獨立式 Management 伺服器	此版本的「趨勢科技行動安全防護」不依賴 OfficeScan，可直接安裝在 Windows 電腦上。
選用的雲端通訊伺服器	除了安裝在本機上的「通訊伺服器」（本機通訊伺服器）外，此版本也提供選項可使用部署在雲端的「通訊伺服器」（雲端通訊伺服器）。系統管理員不需要安裝「雲端通訊伺服器」，該伺服器由趨勢科技維護。
Exchange 伺服器整合	與 Microsoft Exchange 伺服器整合，並支援使用 Exchange ActiveSync 服務的 iOS、Android 及 Windows Phone 行動裝置。
以範本為基礎的政策	可讓您建立、複製或刪除安全防護政策，並將政策指派給特定的行動裝置群組。
支援多個系統管理員帳號	可讓您建立多個不同角色的系統管理員帳號，並可視需要予以自訂。
更新的裝置狀態	透過經過更新的裝置狀態清單，為行動裝置顯示更適合的目前狀態。
iOS 裝置佈建	可讓您將「設定資料檔」推播到 iOS 行動裝置，以設定 VPN、Wi-Fi 與 Exchange ActiveSync 設定。
iOS 行動裝置的監督裝置管理	此版本也新增對受監督 iOS 行動裝置的支援。
報表畫面管理	可讓您管理在「報表」畫面上以 W idget 形式顯示的資訊。您可以根據需求新增或移除 W idget。
伺服器指令確認	提供「指令佇列管理」介面，其中顯示每個從伺服器執行之指令的目前狀態。
使用類別控管應用程式	可讓您透過使用「核可的清單」與「封鎖的清單」，允許或封鎖安裝在 iOS 與 Android 行動裝置上屬於特定類別的應用程式。

功能名稱	說明
使用 QR 碼註冊行動裝置	引進使用 QR 碼（內含在傳送給使用者的電子郵件中）註冊行動裝置的功能。
功能鎖定政策增強	新增更多的功能與作業系統元件至功能鎖定清單，讓系統管理員能夠控管其在行動裝置上的可用性。
iOS 大量購買方案支援	可讓您將透過 Apple 的「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。
更新的行動裝置代理程式介面	引進 Android 與 iOS 行動裝置代理程式的新使用者介面。
與 MARS 整合	提供與「趨勢科技行動應用程式信譽評等服務」(MARS) 整合的伺服器及 Android 行動裝置代理程式，以瞭解應用程式安全威脅與資源使用狀況。
下載系統管理員報告	可讓您從「行動安全防護」管理 Web 主控台下載「系統管理員報告」。
政策違規記錄	提供 Android 行動裝置適用的政策違規記錄。
與 Trend Micro Control Manager 整合	「趨勢科技行動安全防護」可與 Trend Micro Control Manager 整合。此整合能讓 Control Manager 系統管理員將公司政策傳送至行動裝置，並且允許在 Control Manager 中檢視「行動安全防護」的「報表」畫面。

此版本（8.0 版 SP1）的新功能

下表說明「趨勢科技™ 企業版行動安全防護 8.0 版 Service Pack 1 (SP1)」引進的新功能。

功能名稱	說明
根據裝置識別碼的驗證	可讓您使用 IMEI 號碼和/或 Wi-Fi MAC 位址驗證一批行動裝置。
Android 與 iOS 的未受管理群組	引進「未受管理」群組，其適用於「裝置管理員」停用的 Android 行動裝置，以及註冊資料檔已移除的 iOS 行動裝置。

功能名稱	說明
增強的事件記錄	提供與行動裝置密碼重設、遠端尋找、遠端鎖定及遠端清除相關的增強事件記錄。
可自訂註冊 URL	提供簡短且可自訂的 URL 以註冊行動裝置。
簡單 iOS 用戶端	引進 iOS 用戶端，讓使用者可採用使用者電子郵件信箱輕鬆地驗證與註冊。iOS 用戶端也可供存取行動裝置上的「企業應用程式商店」。

此版本（8.0 版）的新功能

下表說明「趨勢科技™ 企業版行動安全防護 8.0 版」引進的新功能。

功能名稱	說明
代理程式自訂	可讓您在 Android 安裝套件中預設伺服器 IP 位址和通訊埠號碼。
Android 的 Web Proxy 支援	可讓您在 Android 行動裝置中設定 Web Proxy。
Android 的 HTTP(S) 推播通知設定	提供可讓您為 Android 行動裝置啟動或關閉 HTTP(S) 推播通知的設定。
簡化佈建	可讓您先在 Android 行動裝置中設定伺服器 IP 位址、網域名稱與伺服器通訊埠號碼，以減少行動裝置的部署與註冊所需的工作。
病毒碼更新完成後進行掃瞄	在病毒碼更新成功後自動開始掃瞄行動裝置上的安全威脅，並在通知列中顯示進度。
Web 威脅防護政策	可讓您從「行動安全防護」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。
為 Android 新增 SD 卡限制	可讓您控管 SD 卡在 Android 行動裝置上的可用性。

功能名稱	說明
應用程式資產清單	維護行動裝置上已安裝的應用程式清單，並將其顯示於裝置狀態畫面上。
應用程式控管	可讓您透過核可與封鎖清單，允許或封鎖特定應用程式在行動裝置上的安裝。
應用程式推播	可讓您將應用程式安裝套件或應用程式的 Web 連結推播至行動裝置，以進行安裝。
選擇性清除	可讓您從伺服器中刪除所有的公司資料，而不刪除使用者的個人資料。
合規檢查	可讓您在伺服器上設定合格條件，並檢查行動裝置是否合格。
使用 Active Directory 的選用驗證	可讓您使用 Active Directory (AD) 或「行動安全防護」資料庫，為 Symbian、Windows Mobile、iOS 與 Android 行動裝置設定註冊的使用者驗證。
報表畫面	採用「報表」畫面來取代 Web 主控台舊有的「摘要」畫面，可提供伺服器元件和行動裝置的狀態摘要。
預約報告	可讓您設定「行動安全防護」以依照預先定義的間隔傳送預約報告。
快速設定驗證畫面	採用「行動安全防護設定與驗證」畫面來讓您快速驗證「行動安全防護」的設定，以及找出潛在的問題。組態設定驗證畫面偵測到任何不正確的組態設定時，會提供更正建議。
iOS 及 Android 的手動遠端密碼重設	可讓您使用 Web 主控台從遠端重設 iOS 及 Android 行動裝置的密碼。
企業應用程式商店	可讓您建立 Web 剪輯和應用程式的清單，以供使用者在行動裝置上下載並安裝。

此版本（7.1 版）的新功能

下表說明「趨勢科技™ 企業版行動安全防護 7.1 版」引進的新功能。

功能名稱	說明
支援 iOS 與 Blackberry 行動裝置	「行動安全防護 7.1 版」新增 iOS 及 Blackberry 行動裝置的支援。
與 Active Directory 整合	「行動安全防護 7.1 版」可運用公司的 Active Directory (AD) 匯入使用者及執行使用者驗證。
更新的架構	「行動安全防護 7.1 版」引進單一和雙重伺服器部署模式。7.1 版另移除簡訊閘道。
佈建政策	此版本引進行動裝置佈建政策。

此版本（7.0 版）的新功能

下節說明「趨勢科技™ 企業版行動安全防護 7.0 版」引進的新功能。

功能名稱	說明
支援 Android 行動裝置	「行動安全防護 7.0 版」新增 Android 2.1 或以上版本行動裝置的支援。
來電過濾政策	可讓系統管理員控制 Android 行動裝置上的來電或撥出通話。
更新的功能鎖定	可讓系統管理員控制 Android 行動裝置位於某個（某些）無線網路存取點範圍內時可用的元件。
尋找遠端裝置	可讓系統管理員透過無線網路或使用行動裝置的 GPS 來尋找遠端裝置，並將裝置的位置顯示在 Google 地圖中。這項新功能有助於尋找遺失、遭竊或放錯位置的行動裝置。
更新的架構	「行動安全防護 7.0 版」將「簡訊閘道」新增為用來傳送簡訊給行動裝置之「簡訊發送器」的備用選項。

行動裝置代理程式的主要功能

功能名稱	說明
惡意程式防護掃瞄	「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，同時讓您隔離及刪除中毒檔案而設計的產品。
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
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，每個行動裝置都有一位相關聯的使用者。使用者必須輸入密碼（也稱為開機密碼），才能登入行動裝置。
資料加密	「行動安全防護」可為儲存在行動裝置與記憶卡上的資料提供動態資料加密功能。您可以指定要加密的資料類型以及要使用的加密演算法。
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。
防火牆（僅限 BlackBerry、Symbian 及 Windows Mobile）	「行動安全防護」含有趨勢科技防火牆模組，其中有預先定義的網路流量過濾安全層級。您也可以定義自己的過濾規則，過濾來自特定 IP 位址和特定通訊埠上的網路流量。入侵偵測系統 (IDS) 可讓您阻止持續將多個封包傳送給行動裝置的嘗試。這類嘗試一般是拒絕服務 (DoS) 攻擊，會讓行動裝置過於忙碌而無法接受其他連線。

功能名稱	說明

記錄	「Management 伺服器」提供以下「行動裝置代理程式」記錄：
	• 惡意程式防護記錄
	• Web 威脅防護記錄
	• 加密記錄
	• 防火牆記錄
	• 事件記錄
	• 違規記錄
	您可以在行動裝置上檢視以下記錄：
	• Windows Mobile 與 Symbian：
	  • 病毒/惡意程式記錄
	  • 防火牆記錄
	  • 垃圾簡訊防護記錄
	  • WAP Push 防護記錄
	  • 工作記錄
	• Android：
	  • 惡意程式掃瞄記錄
	  • 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 9.0 版 SP1 功能列表

政策	功能	設定					
佈建	Wi-Fi	標準 Wi-Fi 設定	●	●	●		
		傳統熱點設定	●				
		熱點 2.0 設定	●				
	Exchange ActiveSync	Exchange ActiveSync 設定	●				
	VPN	VPN 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	●				
裝置安全	惡意程式防護	即時掃瞄		●		●	●
		記憶卡掃瞄				●	●
		病毒碼更新完成後進行掃瞄		●			

政策	功能	設定					
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」		●		●	●
	來電過濾	伺服器端控管		●	●		
		使用「封鎖的清單」		●	●		
		使用「核可的清單」		●	●		
	防火牆	啟動防火牆			●	●	●
		啟動入侵偵測系統 (IDS)				●	●
	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」		●			
		僅允許特定網站	●				
		允許限制的成人內容	●				

政策	功能	設定					
資料安全防護	密碼設定	使用登入密碼	●	●	●	●	
		系統管理員密碼				●	
		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	●	●	●	●	
	加密	PIM 加密				●	
		文件加密				●	
		記憶卡加密				●	
	功能鎖定	相機	●	●		●	
		FaceTime	●				
		螢幕擷取	●				
		應用程式安裝	●				

政策	功能	設定					
資料安全防護	功能鎖定	漫遊時同步	●				
		語音撥號	●		●		
		In-app purchase	●				
		多人玩家遊戲	●				
		新增遊戲中心好友	●				
		Game Center（僅限監督）	●				
		強制使用加密備份	●				
		不當的音樂、播客與 iTunes U	●				
		裝置鎖定時使用 Passbook	●				
		藍芽與藍芽搜索		●		●	
		紅外線				●	
		USB 儲存				●	
		WLAN/Wi-Fi		●		●	
		3G 資料網路		●			

政策	功能	設定					
資料安全防護	功能鎖定	數據連線		●			
		開發人員模式		●			
		序列裝置				●	
		喇叭/免持聽筒/麥克風			●	●	
		Microsoft ActiveSync				●	
		MMS/簡訊				●	
		限制記憶卡		●		●	
		限制 GPS				●	
		Siri	●				
		裝置鎖定時使用 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	●				
		相片串流	●				

政策	功能	設定					
資料安全防護	功能鎖定	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 iTunes 儲存密碼	●				
		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）	●				

政策	功能	設定					
資料安全防護	功能鎖定	色情書刊（僅限監督）	●				
		設定資料檔安裝（僅限監督）	●				
		iMessage（僅限監督）	●				
		為區域分級	●				
		電影	●				
		電視節目	●				
		應用程式	●				
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	●	●	●	●	

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「Management 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：

- 存取管理 Web 主控台 第 2-2 頁
- 報表資訊 第 2-5 頁
- 管理設定 第 2-10 頁
- 指令佇列管理 第 2-17 頁
- Exchange 伺服器整合 第 2-18 頁
- 管理憑證 第 2-19 頁

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

程序

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「Management 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” 及「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，請務必執行下列項目：

- 「網站相容性檢視」選項為關閉。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

如果您無法使用 Metro 模式中的 Internet Explorer 10 在 Windows 2012 中存取管理 Web 主控台，請確認 Internet Explorer 的「加強的受保護模式」選項為關閉。

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）。

程序

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」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」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「Management 伺服器」的授權升級指示，請在「行動安裝防護」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」— 顯示裝置健康狀態，以及裝置的作業系統摘要。
- 「健康」— 顯示元件和政策更新，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」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」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」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」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。

    如有下列其中一種情況，行動裝置即可能尚未註冊：
    - 與「通訊伺服器」的連線不成功
    - 行動裝置使用者已刪除註冊簡訊
  - 檢視行動裝置程式 Patch 與元件更新狀態：
    - 「目前版本」—「行動裝置代理程式」或「行動安全防護」伺服器上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」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

- 「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。
- 「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：
  - 檢視行動裝置已破解/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
- 「防護」— 顯示前五 (5) 大安全威脅和前五 (5) 名最多人封鎖之網站的清單。

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

程序

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 W idget 的配置。
   - 「自動調整」：選取「開啟」或「關閉」以啟動或關閉標籤上的 W idget 設定。
3. 按一下「儲存」。

移除標籤

程序

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

程序

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 W idget 隨即出現「報表」上。

移除 Widget

程序

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

程序

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

程序

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

程序

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。

設定裝置驗證

「趨勢科技行動安全防護」可讓您根據 Active Directory (AD) 或「行動安全防護」資料庫設定裝置驗證。您也可以讓行動裝置無需經過驗證即可向「行動安全防護」伺服器註冊。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。

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 Management 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。請參閱編輯系統管理員帳號 第 2-14 頁以取得瞭解詳細的程序。

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
	電子郵件信箱	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。請參閱編輯系統管理員角色 第 2-16 頁以取得詳細的程序。

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
	Management 伺服器設定	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
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
應用程式商店	應用程式商店	支援	不支援

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
	邀請裝置	支援	僅支援受管理群組
	Exchange ActiveSync 裝置	支援	僅支援受管理群組

新增系統管理員帳號

程序

1. 登入「行動安全防護」管理 Web 主控台。
2. 按一下「管理 > 系統管理員帳號管理」。
3. 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。
4. 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「Management 伺服器」的名稱。
     - 「全名」：使用者全名。
     - 「密碼」（與「確認密碼」）。
     - 「電子郵件信箱」：使用者的電子郵件信箱。

- 「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，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。

5. 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

6. 按一下「儲存」。

編輯系統管理員帳號

程序

1. 登入「行動安全防護」管理 Web 主控台。
2. 按一下「管理 > 系統管理員帳號管理」。
3. 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。

4. 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「Management 伺服器」的名稱。

- 「全名」：使用者全名。
- 「電子郵件信箱」：使用者的電子郵件信箱。
- 「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」：選取下拉式清單中的系統管理員角色。

    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。

5. 按一下「儲存」。

刪除系統管理員帳號

程序

1. 登入「行動安全防護」管理 Web 主控台。
2. 按一下「管理 > 系統管理員帳號管理」。
3. 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」。

建立系統管理員角色

程序

1. 登入「行動安全防護」管理 Web 主控台。
2. 按一下「管理 > 系統管理員帳號管理」。

3. 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。

4. 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

5. 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。

6. 按一下「儲存」。

編輯系統管理員角色

程序

1. 登入「行動安全防護」管理 Web 主控台。
2. 按一下「管理 > 系統管理員帳號管理」。
3. 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。

4. 視需要修改角色詳細資訊，並按一下「儲存」。

刪除系統管理員角色

程序

1. 登入「行動安全防護」管理 Web 主控台。
2. 按一下「管理 > 系統管理員帳號管理」。

3. 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」。

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，請瀏覽至「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」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」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。

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。

程序

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」伺服器 IP 位址。
   - 「HTTPS 通訊埠」— 管理 Web 主控台的「行動安全防護」伺服器 HTTPS 通訊埠號碼。

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」伺服器。

上傳憑證

程序

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

程序

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

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「Management 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 第 3-2 頁
- 管理群組 第 3-3 頁
- 管理行動裝置 第 3-4 頁
- 行動裝置狀態 第 3-8 頁
- 行動裝置代理程式工作 第 3-10 頁
- 更新行動裝置代理程式 第 3-10 頁
- 遺失裝置防護 第 3-11 頁
- 遠端重設密碼 第 3-14 頁
- 邀請的裝置標籤 第 3-17 頁
- Exchange ActiveSync 裝置標籤 第 3-20 頁
- 與 Trend Micro Control Manager 整合 第 3-23 頁

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）
- 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、清除/鎖定/尋找遠端裝置以及更新政策
- 設定「行動裝置代理程式」資訊
- 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 —「行動安全防護」伺服器會自動建立此群組。如果「裝置註冊設定」中的「裝置驗證」已啟動，則會使用行動裝置清單進行驗證。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。

注意

「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」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

程序

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. 輸入「群組名稱」，並從下拉式清單中選您要套用到該群組的「政策」。
5. 按一下「新增」。

重新命名群組

程序

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

程序

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」畫面上將邀請傳送給行動裝置、編輯行動裝置資訊、刪除行動裝置，或變更行動裝置群組。

將邀請傳送給行動裝置

程序

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. 您現在可以邀請一個行動裝置、一批行動裝置，並可從 Active Directory 邀請使用者或電子郵件群組（通訊群組清單）：

   - 若要邀請行動裝置：

     a. 按一下「邀請使用者 > 邀請單一使用者」。

        「邀請單一使用者」快顯視窗隨即顯示。

     b. 在「邀請單一使用者」視窗中設定以下欄位：

        - 「電話號碼」— 輸入行動裝置的電話號碼。若要確保行動裝置可順利接收來自簡訊發送器的通知訊息，您可以輸入國碼（1-5 位數）。您無需輸入國際冠碼。
        - 「電子郵件」— 輸入使用者電子郵件地址以傳送通知電子郵件。
        - 「使用者名稱」— 輸入可在裝置樹狀結構中識別裝置的行動裝置名稱。
        - 「群組」— 從下拉式清單選取行動裝置隸屬的群組名稱。您可以隨時變更「行動裝置代理程式」隸屬的群組。

        

        秘訣

        若要邀請更多裝置，請按一下⊞按鈕。

   - 若要邀請一批行動裝置：

     a. 按一下「邀請使用者 > 邀請批次」。

     b. 在顯示的視窗上，使用下列格式將裝置資訊輸入文字方塊中：

        電話號碼, 電子郵件地址, 裝置名稱, 群組名稱, 資產號碼（選用）, 說明（選用）;

        

        注意

        使用分號 (;) 或 "CR" 分隔每個裝置資訊。

     c. 按一下「驗證」以驗證裝置資訊是否符合指定格式。

- 若要從 Active Directory 邀請使用者或電子郵件群組（通訊群組清單）：

  a. 按一下「邀請使用者 > 從 Active Directory 邀請」。

  b. 在提供的搜尋欄位中輸入使用者資訊，然後按一下「搜尋」。

  c. 從搜尋結果選取使用者，然後按一下「邀請裝置」。

4. 按一下「儲存」。

行動安全防護會將邀請簡訊與電子郵件傳送給受邀裝置的使用者。

編輯行動裝置資訊

程序

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。若要確保行動裝置可順利接收來自簡訊發送器的通知訊息，您可以輸入國碼（1-5 位數）。您無需輸入國際冠碼。
   - 「電子郵件」 — 用以傳送通知電子郵件的使用者電子郵件信箱。
   - 「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 3-7 頁
- 刪除多個行動裝置 第 3-7 頁

刪除單一行動裝置

程序

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「行動安全防護」伺服器之間再也沒有註冊關係。

刪除多個行動裝置

程序

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」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。

程序

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」— 顯示行動裝置的加密狀態，以及行動裝置是否已破解。
- 「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）及行動裝置國碼 (MCC) 和行動裝置網路碼 (MNC) 等資訊。
- 「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。

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「管理」畫面中輸入資訊，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。

程序

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
   - 「資產號碼」 — 行動裝置的資產號碼
   - 「說明」 — 行動裝置的說明

- 「作業系統」 — 行動裝置執行的作業系統
- 「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
- 「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
- 「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。

裝置樹狀結構檢視選項

如果您選取裝置樹狀結構中的一個群組，您可以使用「欄」下拉式清單方塊選取其中一個預先定義的檢視：「一般檢視」與「檢視全部」。這可讓您快速檢視裝置樹狀結構中所顯示的資訊。顯示在裝置樹狀結構中的資訊會隨著選取的選項而改變。

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。

程序

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 6-2 頁。

在 Windows Mobile 或 Symbian 行動裝置上，如果您尚未啟動「行動安全防護」的簡訊功能，便需要在「一般政策」畫面中設定更新預約（請參閱一般政策 第 4-7 頁）以定期更新元件。然而在 Android 行動裝置上，如果您尚未啟動「行動安全防護」的簡訊功能，依然可以透過推播指示來更新元件及同步處理政策。

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。「行動安全防護」伺服器會在 Google 地圖上顯示行動裝置位置。

此功能僅供 Android 行動裝置使用。

程序

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」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 主控台寄出鎖定指示，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、iOS、BlackBerry 及 Windows Mobile 裝置支援此功能。

若要讓 Windows Mobile 裝置使用此功能，行動裝置上的加密功能必須啟動。

Windows Mobile 裝置只能透過使用簡訊通知訊息予以鎖定。如果您想要鎖定 Windows Mobile 裝置，請確定您已設定簡訊發送器。如需設定詳細資訊，請參閱《*安裝與部署手冊*》。

程序

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. 按一下「遠端鎖定」，再按一下確認對話方塊上的「確定」。

   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 2-17 頁。

清除遠端行動裝置

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

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。

注意

僅 Android、iOS、BlackBerry 及 Windows Mobile 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 3-21 頁。

程序

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。」核取方塊。
   - 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

使用者忘記解鎖密碼時，您可以從「Management 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、iOS 及 Windows Mobile 裝置支援此功能。

重設 Android 行動裝置密碼

程序

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

程序

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。

重設 Windows Mobile 裝置的密碼

若要重設 Windows Mobile 裝置的密碼，您必須先要求使用者在行動裝置上產生驗證碼（16 位數的十六進位號碼），您才能遠端解除鎖定行動裝置。

程序

1. 取得行動裝置名稱和使用者在行動裝置上產生的驗證碼。請讓使用者參閱《行動裝置代理程式說明》或*使用手冊*》中有關產生驗證碼的指示。
2. 登入「行動安全防護」管理 Web 主控台。
3. 按一下功能表列上的「裝置」。

   「裝置」畫面隨即出現。
4. 在「受管理裝置」標籤上，從裝置樹狀結構中按一下您要重設其密碼的行動裝置。
5. 按一下「重設密碼」，再按一下「遠端解除鎖定」畫面中的「選取裝置」。裝置樹狀結構隨即出現。
6. 選取要從遠端解除鎖定的行動裝置，然後按一下「選取」。
7. 在欄位中輸入驗證碼，然後按一下「產生」。
8. 「行動安裝防護」伺服器會產生回應碼，並將代碼顯示在快顯畫面中。
9. 要求使用者在行動裝置上按一下「密碼」畫面中的「下一步」，然後輸入回應碼以解除鎖定行動裝置。

匯出資料

在「裝置」畫面的「受管理裝置」標籤上，您可以匯出資料以供進一步分析或備份。

程序

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 檔檢視行動裝置資訊。

邀請的裝置標籤

「裝置」畫面中的「邀請的裝置」標籤會保留「行動安全防護」傳送給行動裝置的註冊邀請記錄。

預設的邀請電子郵件包含下列資訊：

- 趨勢科技行動安全防護簡介
- 行動裝置代理程式下載 URL
- 欲註冊行動裝置的伺服器資訊
- 可供輕鬆註冊的 QR 碼

在「邀請的裝置」標籤上，您可以：

- 檢視邀請清單
- 將邀請訊息重新傳送給行動裝置
- 取消目前邀請
- 移除舊的邀請記錄

檢視邀請清單

程序

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「邀請的裝置」標籤。

   下表提供「邀請的裝置」標籤上所顯示所有邀請狀態的說明。

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。

重新傳送邀請訊息

程序

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「邀請的裝置」標籤。
4. 從清單中選取您要將邀請訊息重新傳送到哪一個行動裝置。

5. 按一下「重新傳送邀請」。

取消作用中邀請

程序

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「邀請的裝置」標籤。
4. 從清單中選取您要取消邀請的行動裝置。
5. 按一下「取消邀請」。

從清單移除邀請

注意

您只能移除狀態為「已使用」或「已取消」的邀請訊息。

程序

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「邀請的裝置」標籤。
4. 從清單中選取您要移除其邀請記錄的行動裝置。

5. 按一下「移除邀請」。

Exchange ActiveSync 裝置標籤

啟動「行動安全防護」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：

- 邀請行動裝置
- 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 行動裝置

透過邀請 Exchange ActiveSync 行動裝置，請務必確認您已在「Management 伺服器」上設定通知/報告設定。請參閱《*安裝與部署手冊*》中的＜*設定通知/報告設定*＞主題。

程序

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. 選取您要邀請存取 Exchange ActiveSync 的行動裝置。

5. 按一下「邀請」，再按一下確認畫面上的「確定」。

   「行動安全防護」會將邀請簡訊與電子郵件訊息傳送給受邀行動裝置的使用者。行動裝置向「行動安全防護」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

程序

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

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。

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。

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。

程序

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

您從遠端所清除「行動安全防護」伺服器中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」伺服器中遠端清除的行動裝置。

程序

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」。

與 Trend Micro Control Manager 整合

「趨勢科技行動安裝防護」與 Trend MicroControl 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「行動安全防護報表」畫面

如需有關 Trend MicroControl 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，並將所有的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_ 字首。

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

利用政策來保護裝置

本章示範如何設定安全防護政策，以及如何將安全防護政策套用至「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：

- 關於安全防護政策 第 4-3 頁
- 管理政策 第 4-4 頁
- 一般政策 第 4-7 頁
- Wi-Fi 政策 第 4-8 頁
- Exchange ActiveSync 政策 第 4-9 頁
- VPN 政策 第 4-9 頁
- 全域 HTTP Proxy 政策 第 4-9 頁
- 憑證政策 第 4-9 頁
- 單一登入政策 第 4-9 頁
- 惡意程式防護政策 第 4-10 頁
- 垃圾簡訊防護政策 第 4-12 頁
- 來電過濾政策 第 4-15 頁

- 防火牆政策 第 4-17 頁
- Web 威脅防護政策 第 4-18 頁
- 加密與密碼政策 第 4-18 頁
- 功能鎖定政策 第 4-22 頁
- 合規政策 第 4-23 頁
- 應用程式監控與控管政策 第 4-23 頁
- 大量購買方案政策 第 4-25 頁

關於安全防護政策

您可以在 Management 伺服器中設定「行動安全防護」群組的安全防護政策。這些政策適用於群組中的所有行動裝置。您可以藉由選取「行動裝置」群組（根群組）來將安全防護政策套用至所有「行動安全防護」群組。下表列出「行動安全防護」提供的安全防護政策。

表 4-1. 行動安全防護中的安全防護政策

政策群組	政策	參考
一般	一般政策	請參閱一般政策 第 4-7 頁。
佈建	Wi-Fi 政策	請參閱 Wi-Fi 政策 第 4-8 頁。
	Exchange ActiveSync 政策	請參閱 Exchange ActiveSync 政策 第 4-9 頁。
	VPN 政策	請參閱 VPN 政策 第 4-9 頁。
	全域 HTTP Proxy 政策	請參閱全域 HTTP Proxy 政策 第 4-9 頁。
	憑證政策	請參閱憑證政策 第 4-9 頁。
	單一登入政策	請參閱單一登入政策 第 4-9 頁。
裝置安全	惡意程式防護政策	請參閱惡意程式防護政策 第 4-10 頁。
	垃圾簡訊防護政策	請參閱垃圾簡訊防護政策 第 4-12 頁。
	來電過濾政策	請參閱來電過濾政策 第 4-15 頁。
	防火牆政策	請參閱防火牆政策 第 4-17 頁。
	Web 威脅防護政策	請參閱 Web 威脅防護政策 第 4-18 頁。
裝置	加密與密碼政策	請參閱加密與密碼政策 第 4-18 頁。
	功能鎖定政策	請參閱功能鎖定政策 第 4-22 頁。
	合規政策	請參閱合規政策 第 4-23 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 4-23 頁。
	大量購買方案政策	請參閱大量購買方案政策 第 4-25 頁。

管理政策

「行動安全防護」可讓您使用預設的安全防護政策範本快速地建立政策。

使用「政策」畫面建立、編輯、複製或刪除行動裝置的安全防護政策。

建立政策

程序

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」。

   「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 4-5 頁。

編輯政策

程序

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」。

   「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

程序

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」。

   「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，選取您要套用到群組的政策，再按一下「>」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，再按一下「<」將群組移至左側「可用的群組」清單。
5. 按一下「儲存」。

複製政策

程序

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」。

   「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 4-5 頁。

程序

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」。

   「政策」畫面隨即出現。
3. 選取您要刪除的政策，再按一下「刪除」。

行動安全防護中的安全防護政策

本節介紹「行動安全防護」中的安全防護政策。

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」。

在「一般政策」中，您也可以指派 BlackBerry 行動裝置政策。

- 「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 4-12 頁、垃圾郵件 WAP-Push 防護政策 第 4-14 頁及 Web 威脅防護政策 第 4-18 頁。

- 「更新設定」：您可以選擇讓「行動安全防護」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」伺服器上是否有任何元件或組態設定更新。

在啟動無線連線通知選項時，提示畫面會在「行動裝置代理程式」透過無線連線（如 3G 或 GPRS）連接「通訊伺服器」時出現在行動裝置上。使用者可以選擇接受或拒絕連線要求。

圖 4-1. 一般政策的更新設定部分

- 「記錄設定」：「行動裝置代理程式」偵測到安全威脅（如中毒檔案或防火牆違規）時，會在行動裝置上產生記錄。如果加密模組已啟動，它也會產生加密記錄。您可以設定行動裝置以將這些記錄傳送給「行動安全防護」伺服器。如果您想要分析中毒的項目數量，或找出可能的網路攻擊並採取適當的處理行動來阻止威脅擴散，請採行以上設定。
- 「通知/報告設定」：選取當「行動裝置代理程式」嘗試建立與「通訊伺服器」之間的連線時，是否要在行動裝置上顯示提示畫面。
- 「BlackBerry 設定」：可讓您針對 BlackBerry 行動裝置設定一般政策設定。

注意

您必須先在「通訊伺服器」設定中設定「BlackBerry 設定」，才能進行政策設定。請先參閱《*安裝與部署手冊*》中的＜*設定 BlackBerry 通訊伺服器設定*＞主題。

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 政策設定可讓您為組織建立 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 App Store 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」。

惡意程式防護政策

您可以設定包含以下項目的威脅防護政策：掃瞄類型（即時掃瞄或記憶卡掃瞄）、針對惡意程式採取的處理行動、要掃瞄的壓縮層數量及檔案類型。

若要設定惡意程式防護政策設定，請按一下「政策」，再按一下「政策名稱」，最後按一下「惡意程式防護政策」。

- 「掃瞄類型」：「行動安全防護」提供數種掃瞄類型來協助行動裝置抵禦惡意程式。
  - 「即時掃瞄」：「行動裝置代理程式」能即時掃瞄行動裝置上的檔案。如果「行動裝置代理程式」未偵測到安全威脅，使用者可以繼續開啟或儲存檔案。如果「行動裝置代理程式」偵測到安全威脅，它會顯示掃瞄結果、顯示檔案名稱及顯示具體的安全威脅。「行動安全防護」會在行動裝置上產生含掃瞄結果的記錄。您可以將掃瞄記錄傳送至「行動安全防護」資料庫並加以儲存。
  - 「插入 SD 卡後進行掃瞄」：如果您選取「惡意程式防護政策」畫面中的這個選項，當記憶卡插入行動裝置時，「行動安全防護」會掃瞄記憶卡中的資料。這樣可預防中毒檔案擴散到整個記憶卡。
  - 「病毒碼更新完成後進行掃瞄」：如果您選取「惡意程式防護政策」畫面中的這個選項，當 Android 行動裝置上的病毒碼成功更新後，「行動安全防護」會執行自動掃瞄以找尋安全威脅。
- 掃瞄選項
  - 「發現惡意程式時的處理行動」：在行動裝置上偵測到惡意程式時，「行動安全防護」能刪除或隔離中毒檔案。如果檔案正在使用中，作業系統可能會拒絕該檔案的存取。
    - 隔離 — 重新命名中毒檔案並將檔案移動到行動裝置的隔離目錄：`\TmQuarantine` (Windows Mobile) 或 `{Disk Label}\TmQuarantine` (Symbian OS)。
    - 刪除 — 移除中毒檔案。

    連接時，「行動裝置代理程式」會將惡意程式記錄傳送給「行動安全防護」伺服器。

    
    注意

    掃瞄處理行動只適用於即時掃瞄。
  - 「進行掃瞄的壓縮層」：對於 ZIP 或 CAB 檔案，您可以指定要掃瞄的壓縮層數量。如果 ZIP/CAB 檔案中的壓縮層數量超過此數值，「行動安全防護」便不會掃瞄該檔案。除非您指定適當的壓縮層數量，否則「行動安全防護」將不會採取進一步的處理行動。

您可以選取選項以讓「行動安全防護」掃瞄行動裝置上的執行檔、ZIP/CAB 檔案或所有檔案。

- 「掃瞄位置」：對於 Android 行動裝置，請選取是否掃瞄行動裝置的內部記憶體和/或插入的 SD 卡。對於 Symbian 行動裝置，讓「行動安全防護」掃瞄行動裝置的內建記憶體與插入的 SD 卡。
- 「檔案型態」：選取要在行動裝置上掃瞄的檔案型態。

垃圾簡訊防護政策

「行動安全防護」中的垃圾郵件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 4-2. 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
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。

垃圾郵件 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。以下功能是在設定 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

將伺服器政策傳送至行動裝置後，個人設定將會清除。

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。

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 4-3. 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

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。
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。

防火牆政策

「行動安全防護」防火牆能使用狀態式檢測、高效能的網路流量控管及入侵偵測系統 (IDS) 來保護網路中的行動裝置。您可以建立規則來依照 IP 位址、通訊埠號碼或通訊協定過濾連線，然後將規則套用至特定「行動安全防護」群組中的行動裝置。

注意

趨勢科技建議您先解除安裝行動裝置上其他軟體形式的防火牆應用程式，然後部署並啟動「行動安全防護」防火牆。在同一部電腦上安裝多家廠商的防火牆會導致無法預期的結果。

若要設定防火牆政策設定，請按一下「政策」，再按一下「政策名稱」，最後按一下「防火牆政策」。

防火牆政策包含以下項目：

- 防火牆政策：啟動/關閉「行動安全防護」防火牆和 IDS。另包含能封鎖或允許行動裝置上所有內送和（或）所有外送流量的一般政策
  - 啟動入侵偵測系統 (IDS)：「行動安全防護」防火牆藉由結合入侵偵測系統 (IDS) 來預防 SYN Flood 攻擊（一種拒絕服務攻擊）。SYN Flood 攻擊會使程式傳送多個 TCP 同步處理 (SYN) 封包給電腦，導致行動裝置持續傳送同步處理確認 (SYN/ACK) 回應。如此會使系統資源耗盡，讓行動裝置無法處理其他要求。
  - 安全層級：「行動安全防護」防火牆提供三個預先定義的安全層級，可讓您快速設定防火牆政策。這些安全層級能根據流量方向限制網路流量。
    - 「低」— 允許所有內送和外送流量。
    - 「一般」— 允許所有外送流量，但封鎖所有內送流量。
    - 「高」— 封鎖所有內送和外送流量。
- 「例外」：例外規則含有比較具體的設定，可讓您依據行動裝置的通訊埠號碼和 IP 位址來允許或封鎖不同種類的流量。清單中的規則會覆寫安全層級政策。

例外規則設定包含下列項目：

- 「處理行動」— 封鎖或允許/記錄符合規則條件的流量
- 「方向」— 行動裝置上的內送或外送網路流量
- 「通訊協定」— 流量的類型：TCP、UDP、ICMP
- 「通訊埠」— 執行處理行動的行動裝置通訊埠
- 「IP 位址」— 要套用流量條件之網路裝置的 IP 位址

Web 威脅防護政策

可讓您從「行動安全防護」伺服器管理 Web 威脅防護政策，並將其部署到 Android 和 iOS 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。

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」。

加密與密碼政策

加密與密碼模組能在行動裝置上提供密碼驗證和資料加密功能。這些功能可預防未經授權的使用者存取行動裝置上的資料。

若要設定加密與密碼政策設定，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「加密與密碼政策」。

密碼安全防護設定

安裝「行動裝置代理程式」後，每個行動裝置會與一個使用者產生關聯。使用者必須輸入正確的開機密碼才能登入行動裝置。當使用者忘記開機密碼時，您可以輸入系統管理員密碼來解除鎖定行動裝置。

下表描述您可設定解鎖密碼政策：

選項	說明
密碼類型	密碼只能含有數字或英數字元。
密碼長度下限	密碼長度必須大於指定的字元數。
密碼複雜度	對於英數字元密碼，使用者必須設定含大寫字元、小寫字元、特殊字元或數字等項目的密碼，以加深猜測的難度。
初次行動裝置代理程式密碼	在安裝「行動裝置代理程式」和加密模組後，允許使用者登入 Windows Mobile 裝置的密碼。預設值為 "123456"。
系統管理員密碼	系統管理員用來解除鎖定行動裝置的密碼。
到期期間	登入密碼的有效天數。密碼到期後，使用者必須設定新的密碼才能登入。
未作用逾時	在行動裝置自動進入安全模式及顯示登入畫面之前，沒有使用者活動的分鐘數。
登入次數限制	限制登入的嘗試次數以預防暴力密碼攻擊。達到限制時可採取的處理行動包括： • 「軟重設」— 重新啟動行動裝置。 • 「僅限系統管理員存取」— 要求使用系統管理員密碼登入。 • 「硬重設」— 將行動裝置重設為出廠預設政策。 • 「清除所有資料」— 將行動裝置重設為出廠預設政策，並刪除行動裝置和插入的記憶卡中所有的資料。 警告! 在「清除所有資料」處理行動後，使用者需要將記憶卡重新格式化，才能再次使用記憶卡儲存資料。
變更初次開機密碼	要求使用者在首次登入後變更初次密碼。
忘記密碼問題	當使用者忘記開機密碼時，這項功能可讓使用者藉由回答選取的問題來解除鎖定行動裝置及設定新密碼。

注意

在指定初次密碼或管理員密碼的字元時，請留意行動裝置使用的輸入法。否則，裝置使用者可能無法在啟動加密後解除鎖定裝置。

加密設定

「行動裝置代理程式」能提供即時加密功能來保護行動裝置上的資料。可用的加密演算法有兩種：進階加密標準（AES，提供 128 位元、192 位元或 256 位元金鑰）和 XTS 進階加密標準 (AES)。

注意

「行動安全防護」只能管理 Windows Mobile 裝置上的資料安全防護政策。

在 Windows Mobile 裝置上，您可以選取要加密的特定檔案類型、要使用的加密演算法、允許存取加密資料的信任應用程式，或將資料加密套用至插入行動裝置的記憶卡。

「行動裝置代理程式」不會加密動態連結程式庫 (`*.DLL`) 檔案。「行動裝置代理程式」只會加密使用者修改過的檔案。讀取檔案後不做任何修改即關閉檔案並不符合檔案加密的條件。

在啟動「加密模組」後，特定的檔案型態與 PIM 資訊會加密。這些檔案型態和 PIM 資訊列示於下表。

經過加密的資訊	類型
檔案類型	• doc • txt • ppt • pxl • pdf • xls • psw • docx
PIM 資訊	• 聯絡人 • 郵件 • 工作 • 行事曆 • 簡訊 • MMS

「加密模組」僅允許信任的應用程式存取加密的資料。因此，您必須將這些應用程式新增至信任的應用程式清單中。若要將軟體新增至信任的應用程式清單，請將完整的軟體路徑新增至此項目下的適當清單中：「允許更多應用程式存取加密的資料」。

注意

如需進階組態設定，您可以設定「行動安全防護」以加密其他類型的檔案。若要啟動自訂檔案型態的加密，請將檔案 TmOMSM.ini（位於 \Trend Micro\Mobile Security 中）的 Enable_Custom_Extension 參數設為 1。將 TmOMSM.ini 檔案中的參數設定為 "1" 時，「加密其他檔案型態」欄位即會出現在「資料安全防護政策」畫面中。請在此欄位中指定檔案類型。

若要關閉此功能，請將 Enable_Custom_Extension 參數設為 0。將 TmOMSM.ini 檔案中的參數設定為 "0" 時，「加密其他檔案類型」欄位不會出現在「資料安全防護政策」畫面中。

在變更 TmOMSM.ini 檔案後，請重新啟動「行動安全防護管理模組服務」服務以讓變更生效。

警告!

趨勢科技不建議使用者自訂加密的檔案類型。您不能加密某些類型的檔案（如 .exe、.cert、.dll 等）。將「行動安全防護」設定為將不應加密的檔案類型加密，可能會發生無法預期的系統錯誤。

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。

注意

Symbian 行動裝置不提供「功能鎖定政策」。

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。

注意

您可能需要重新啟動 Windows Mobile 裝置才能讓變更生效。

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」將封鎖 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，即使這些應用程式使用您已啟動的服務。

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：
  - 「行動安全防護」如果偵測到不在「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：
  - 「行動安全防護」如果偵測到在「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」偵測到在「封鎖的清單」中的任何應用程式，「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」會檢查是否有受限制的應用程式，並將電子郵件警訊傳送給使用者：

- 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「行動安裝防護」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 5-2 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。

第 5 章

管理企業應用程式商店

本章說明如何管理 iOS 與 Android 行動裝置的企業應用程式商店。

本章包含以下小節：

- 關於企業應用程式商店 第 5-2 頁
- 管理企業應用程式 第 5-2 頁
- 管理應用程式類別 第 5-5 頁

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

程序

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「應用程式商店」。

   隨即顯示「企業應用程式商店」畫面。
3. 按一下「iOS 應用程式」標籤或「Android 應用程式」標籤。
4. 按一下「新增」。

   「新增應用程式」視窗會隨即顯示。
5. 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，並使用行動裝置上的預設網路瀏覽器開啟連結。

- (iOS)「請輸入搜尋關鍵字」— 輸入您要搜尋的 VPP 應用程式名稱，並選取一個國家以便在該國的 Apple 應用程式商店中搜尋該應用程式，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 4-25 頁。

6. 按一下「繼續」。

   「編輯應用程式」畫面會隨即顯示。

7. 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」：選取以下其中一個：
     - 「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。

8. 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

程序

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「應用程式商店」。

   隨即顯示「企業應用程式商店」畫面。
3. 按一下「iOS 應用程式」標籤或「Android 應用程式」標籤。
4. 按一下您要編輯其資訊的應用程式名稱。

   「編輯應用程式」視窗隨即出現。
5. 修改畫面的詳細資訊。
6. 按一下「繼續」。

刪除應用程式商店中的應用程式

程序

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「應用程式商店」。

   隨即顯示「企業應用程式商店」畫面。

3. 按一下「iOS 應用程式」標籤或「Android 應用程式」標籤。
4. 選取您要刪除的應用程式。
5. 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

程序

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「應用程式商店」。

   隨即顯示「企業應用程式商店」畫面。
3. 按一下「iOS 應用程式」標籤或「Android 應用程式」標籤。
4. 按一下「管理類別」。
5. 按一下「新增」。

   「新增類別」視窗隨即顯示。
6. 輸入類別名稱與說明，再按一下「儲存」。

編輯應用程式類別

程序

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「應用程式商店」。

隨即顯示「企業應用程式商店」畫面。

3. 按一下「iOS 應用程式」標籤或「Android 應用程式」標籤。
4. 按一下「管理類別」。
5. 按一下您要編輯的類別名稱。

   「編輯類別」視窗隨即顯示。
6. 修改類別詳細資訊，再按一下「儲存」。

刪除應用程式類別

程序

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「應用程式商店」。

   隨即顯示「企業應用程式商店」畫面。
3. 按一下「iOS 應用程式」標籤或「Android 應用程式」標籤。
4. 按一下「管理類別」。
5. 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」。

第 6 章

更新元件

本章示範如何設定預約和手動伺服器更新，以及指定主動式更新的更新來源。您也可以學到如何在特定的「行動裝置代理程式」上執行元件更新。

本章包含以下小節：

- 關於元件更新 第 6-2 頁
- 手動更新 第 6-2 頁
- 預約更新 第 6-4 頁
- 手動更新本機 AU 伺服器 第 6-7 頁

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」偵測這些危險檔案的能力。趨勢科技會定期更新病毒碼檔案，以確實抵禦最新威脅。
- 「惡意程式掃瞄引擎」— 執行實際掃瞄和清除功能的元件。掃瞄引擎採用病毒碼比對技術，利用病毒碼檔案中的簽章來偵測惡意程式。趨勢科技會不定期發行新的掃瞄引擎，以整合新技術。
- 「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。
- 「行動裝置代理程式」Patch — 含有行動裝置上安裝的「行動裝置代理程式」最新所適用的更新程式 Patch 檔案。

更新行動安全防護元件

您可以在「行動安全防護」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「行動安全防護」伺服器後，「行動安全防護」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 6-5 頁）。

程序

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。

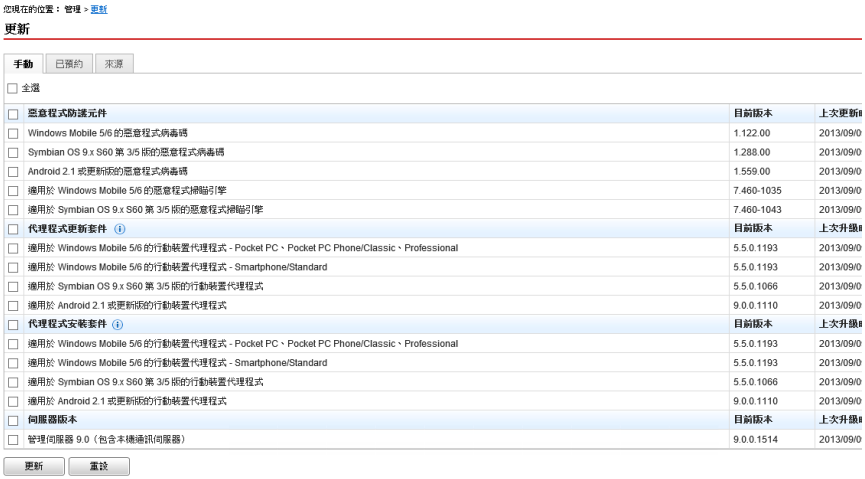

圖 6-1. 「更新」畫面上的「手動」標籤

4. 選取要更新元件的核取方塊。選取「惡意程式防護元件」、「程式」及/或「程式安裝套件」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 6-2 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 6-5 頁）。

程序

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。

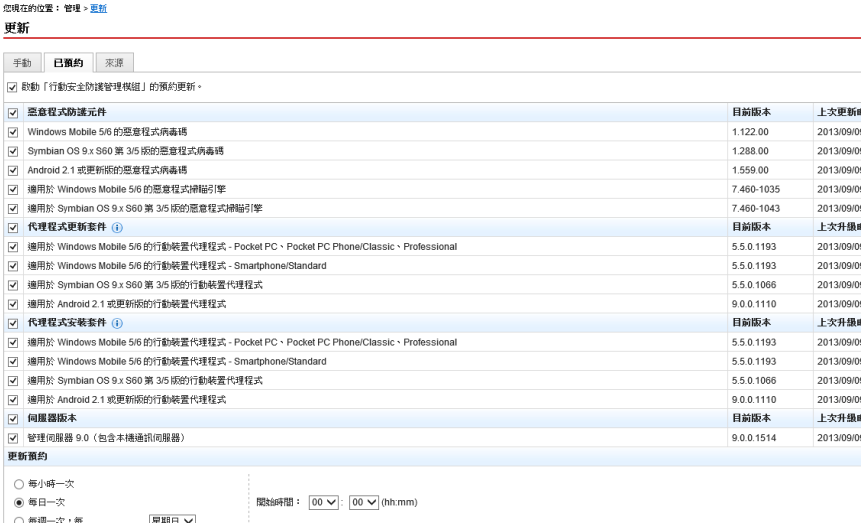

圖 6-2. 「更新」畫面上的「已預約」標籤

4. 選取要更新元件的核取方塊。選取「惡意程式防護元件」、「代理程式更新套件」、「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」、「每日一次」、「每週一次」及「每月一次」。

   - 對於每週一次的排程，請指定星期幾（例如星期日、星期一等）。
   - 對於每月一次的排程，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「每日一次」、「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 x 小時內的某個時間發生。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。

程序

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 6-2 頁；如需預約更新的詳細資訊，請參閱預約更新 第 6-4 頁。

3. 按一下「來源」標籤。

圖 6-3.「更新」畫面上的「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

     更新元件必須可自更新來源（Web 伺服器）取得。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（而非「行動安全防護」Management 伺服器），便無法連線到網路。在這種情況下，請先手動更新本機 AU 伺服器，然後進行「伺服器/裝置更新」。

程序

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 7 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「行動裝置代理程式」記錄，以及如何進行記錄刪除設定。

本章包含以下小節：

- 關於行動裝置代理程式記錄 第 7-2 頁
- 檢視行動裝置代理程式記錄 第 7-2 頁
- 記錄維護 第 7-4 頁

關於行動裝置代理程式記錄

「行動裝置代理程式」產生惡意程式防護記錄、Web 威脅防護記錄、防火牆記錄、加密記錄、政策違規記錄或事件記錄時，會將記錄傳送至「行動安全防護」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」伺服器上檢視所有「行動裝置代理程式」記錄。在「行動安全防護」伺服器上，您可以檢視下列的「行動裝置代理程式」記錄：

- 惡意程式防護記錄 — 在行動裝置上偵測到惡意程式時，「行動裝置代理程式」會產生記錄。這些記錄可讓您追蹤偵測到的惡意程式和採取的抵禦措施。
- Web 威脅防護記錄 —「行動安全防護代理程式」封鎖危險或感染惡意程式的網頁時會產生記錄，同時也會將記錄上傳至伺服器。
- 防火牆記錄 — 在符合防火牆規則，或防火牆功能（如預先定義的安全層級或 IDS）封鎖連線時，即會產生這些記錄。
- 加密記錄 — 包含使用者登入成功次數與達到登入嘗試次數上限後所要執行的動作之類的訊息。
- 事件記錄 — 這些記錄會在伺服器與「行動裝置代理程式」執行特定動作時產生。
- 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。

程序

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。

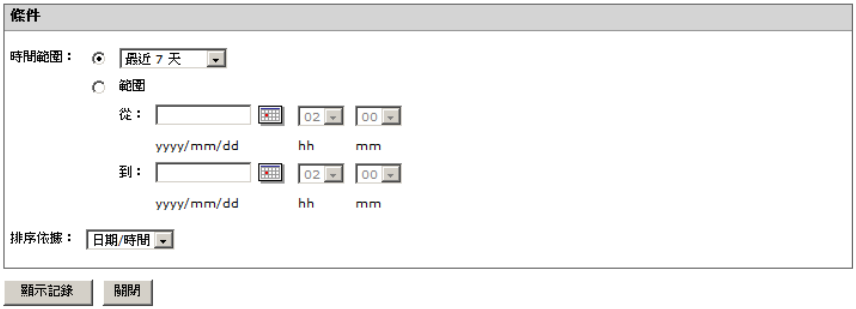

圖 7-1.「記錄查詢」畫面

3. 為您要檢視的記錄指定查詢條件。參數為：
   - 「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。
   - 「管理員名稱」— 輸入您要搜尋其產生記錄的系統管理員名稱。
   - 「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」記錄的大小免於佔用太多硬碟空間，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

程序

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：惡意程式、防火牆、加密、事件或政策違規。
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

程序

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 8 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 第 8-2 頁
- 正在設定通知設定 第 8-2 頁
- 設定電子郵件通知 第 8-2 頁
- 進行簡訊發送器設定 第 8-3 頁
- 處理簡訊發送器用戶端應用程式 第 8-6 頁
- 系統管理員通知和預約報告 第 8-8 頁
- 使用者通知 第 8-9 頁

關於通知訊息和報告

您可以設定「行動安全防護」以透過電子郵件和簡訊將通知傳送給系統管理員和（或）使用者。

- 「系統管理員通知/報告」— 發生任何系統異常狀況時，傳送電子郵件通知和報告給系統管理員。
- 「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」。

正在設定通知設定

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。

程序

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/報告設定」畫面隨即出現。
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」。

相關資訊

↪ 設定簡訊發送器清單

進行簡訊發送器設定

「Management 伺服器」會控管和監控與伺服器連線的「簡訊發送器」。簡訊發送器能傳送訊息給行動裝置以執行「行動裝置代理程式」安裝、註冊、元件更新、安全防護政策設定及遠端清除/鎖定/尋找。

使用「簡訊發送器設定」可以：

- 設定簡訊發送器電話號碼
- 檢視簡訊發送器連線狀態
- 設定「行動裝置代理程式」安裝訊息
- 設定簡訊發送器中斷連線通知

簡訊發送器清單

您需要先設定簡訊發送器裝置電話號碼，「Management 伺服器」才能指示簡訊發送器傳送訊息給行動裝置。

注意

如果您未在簡訊發送器清單中設定簡訊發送器的電話號碼，「Management 伺服器」會阻止簡訊發送器傳送訊息給行動裝置。

程序

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/報告設定」畫面隨即出現。簡訊發送器電話號碼清單和連線狀態會出現在「簡訊發送器設定」區段中。如果簡訊發送器已成功連線至「Management 伺服器」，「狀態」欄位會顯示：「已連線」。

注意

在三 (3) 次不成功的簡訊傳送嘗試後，行動裝置會顯示「已中斷連線」。

設定簡訊發送器清單

指定簡訊發送器的電話號碼，以讓「行動安全防護」伺服器管理簡訊發送器。簡訊發送器能傳送訊息以通知行動裝置執行以下作業：

- 下載及安裝「行動裝置代理程式」
- 向「行動安全防護管理模組」註冊
- 向「行動安全防護管理模組」取消註冊
- 更新「行動裝置代理程式」元件
- 與「行動安全防護管理模組」同步處理安全政策設定
- 遠端清除行動裝置
- 遠端鎖定行動裝置
- 遠端尋找行動裝置

程序

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/報告設定」畫面隨即出現。
3. 在「簡訊發送器設定」區段中按一下「新增」，輸入簡訊發送器的電話號碼，然後按一下「儲存」。簡訊發送器隨即出現在清單中。
4. 檢查所設定號碼的「狀態」欄位是否顯示「已連線」。如果「狀態」欄位顯示「已中斷連線」，請務必將簡訊發送器連接「Management 伺服器」。

注意

按一下電話號碼可修改現有的簡訊發送器。

監控簡訊發送器

「行動安全防護」可監控簡訊發送器的狀態，並在簡訊發送器的連線中斷超過十分鐘時傳送電子郵件通知。此外，簡訊發送器裝置也會顯示連線狀態：「代理程式已停止」、「代理程式執行中」、「代理程式非使用中」、「代理程式已中斷連線」。如需設定詳細資訊，請參閱系統管理員通知和預約報告 第 8-8 頁。

編輯簡訊發送器

程序

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/報告設定」畫面隨即出現。
3. 在「簡訊發送器設定」區段中，按一下您要編輯的電話號碼。

   對話方塊隨即出現。
4. 在提供的欄位中編輯電話號碼，然後按一下「儲存」。
5. 按一下「儲存」以儲存設定。

刪除簡訊發送器

程序

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/報告設定」畫面隨即出現。

3. 在「簡訊發送器」區段中，選取您要刪除的簡訊發送器，再按一下「刪除」。

4. 按一下「儲存」以儲存設定。

處理簡訊發送器用戶端應用程式

設定簡訊發送器用戶端應用程式

程序

1. 在 Android 行動裝置上開啟簡訊發送器應用程式。

2. 點選「設定」，接著點選以下項目進行設定：

   - 「伺服器位址」：輸入「Management 伺服器」名稱或 IP 位址，並點選「確定」。
   - 「伺服器通訊埠」：輸入管理 Web 主控台通訊埠號碼，並點選「確定」。
   - 「電話號碼」：輸入簡訊發送器的電話號碼。
   - 「通訊埠類型」：選取用於傳送訊息的 HTTP 或 HTTPS 通訊協定。

3. 點選「開始」以啟動簡訊發送器。

停止簡訊發送器

程序

1. 在 Android 行動裝置上開啟簡訊發送器應用程式。

2. 點選「停止」以停止簡訊發送器。

簡訊發送器狀態

「行動安全防護」會在行動裝置上更新簡訊發送器的狀態。根據連線狀態，裝置上會出現下列狀態：

- 一般：「簡訊發送器」與「Management 伺服器」連線。
- 已停止：「簡訊發送器」目前已停止。
- 未使用：「簡訊發送器」應用程式的設定不符合「行動安裝防護」伺服器的設定。

檢視簡訊發送器記錄

程序

1. 在 Android 行動裝置上開啟簡訊發送器應用程式。
2. 點選「記錄」以檢視傳送至行動裝置的訊息。

檢視簡訊發送器執行中記錄

程序

1. 在 Android 行動裝置上啟動簡訊發送器應用程式。
2. 點選「執行中記錄」以檢視簡訊發送器執行中事件記錄。

系統管理員通知和預約報告

您可以使用「系統管理員通知/報告」畫面來設定以下項目：

- 通知：
  - 「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%> 及 <%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%> 將取代為行動裝置的名稱。
  - 「APNs 憑證到期警告」—當 APNs 憑證到期時傳送電子郵件通知給系統管理員。
- 報告：
  - 「裝置資產清單報告」—「行動安全防護」所管理全部行動裝置的全方位報告。
  - 「合規違規報告」—「行動安全防護」所管理全部的行動裝置中未遵守所設定政策的行動裝置報告。
  - 「惡意程式偵測報告」—「行動安全防護」管理的行動裝置上偵測到的所有安全威脅報告。
  - 「Web 威脅防護報告」—「行動安全防護」管理的行動裝置上存取的所有不安全 URL 報告。
  - 「應用程式資產清單報告」— 安裝「行動安全防護」所管理的行動裝置上所有應用程式的報告。
  - 「裝置註冊報告」—「行動安全防護」所管理行動裝置註冊資訊的報告。
  - 「裝置解除委任報告」—「行動安全防護」所管理行動裝置解除委任資訊的報告。

- 「政策違規報告」— 是違反安全防護政策的行動裝置報告。

設定系統管理員通知

程序

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/報告設定」畫面隨即出現。
3. 選取要透過電子郵件接收的通知和報告，然後分別按一下要修改內容的通知和報告。

   注意

   選取要接收的報告時，您也可以在每個報告之後的下拉式清單個別調整報告的頻率。

   注意

   編輯電子郵件通知訊息中的「訊息」欄位時，請確實包含 <%PROBLEM%>、<%REASON%> 及 <%SUGGESTION%> 等 Token 變數，這些變數在電子郵件中將由實際的值所取代。
4. 完成時按一下「儲存」，返回「系統管理員通知/報告」畫面。

使用者通知

使用「使用者通知」畫面，可設定以下電子郵件和（或）簡訊通知：

- 「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%> 將由設定套件中的實際 URL 所取代。

- 「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%> 在電子郵件中將由行動裝置的名稱和行動裝置違反的政策所取代。

設定使用者通知

程序

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/報告設定」畫面隨即出現。
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。

     注意

     編輯「訊息」欄位時，請確實包含 <%DOWNLOADURL%> 或 <%DEVICE_NAME%> 和 <%VIOLATION%> 等 Token 變數，這些變數在電子郵件中將由實際的 URL 所取代。
   - 若要設定通知簡訊，請在「訊息」欄位中更新訊息的內文。

     注意

     編輯「訊息」欄位時，請確實包含 <%DOWNLOADURL%> Token 變數，此變數在簡訊中將由實際的 URL 所取代。
4. 完成時按一下「儲存」，返回「使用者通知」畫面。

第 9 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 第 9-2 頁
- 聯絡技術支援前 第 9-5 頁
- 聯絡技術支援 第 9-5 頁
- 將中毒檔案傳送給趨勢科技 第 9-6 頁
- iTrendLabs 第 9-6 頁
- 關於軟體更新 第 9-7 頁
- 其他有用的資源 第 9-8 頁
- 關於趨勢科技 第 9-8 頁

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。

- 「行動安全防護代理程式」無法透過公用 DNS 名稱接收伺服器的簡訊通知或連線至伺服器。

  對於 Windows Mobile 平台，支援 DNS 名稱的「行動裝置代理程式」為高於 5.0.0.1099 的版本，對於 Symbian OS 9.x S60 第 3 版平台，則為高於 5.0.0.1061 的版本。舊版只能透過 IP 位址連線。

- 在啟動加密模組後，有應用程式無法運作。

  使用者在裝置上使用加密模組時，有些現有的應用程式可能無法運作。這是因為這些現有應用程式可能未包含於信任清單中。啟動「加密模組」後，會將特定檔案型態加密（例如 `doc`、`txt`、`ppt`、`pdf`、`xls` 等等）。「加密模組」僅允許信任的應用程式存取加密資料。因此，系統管理員必須將這些應用程式新增至信任的應用程式清單中。如需詳細資訊，請參閱加密設定 第 4-20 頁。

- 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「Management 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」。

- 「Management 伺服器」無法從 BlackBerry Enterprise Server (BES) 接收政策。

  如果政策名稱中包含特殊字元，「通訊伺服器」即無法從 BlackBerry Enterprise Server (BES) 接收政策。請檢查政策名稱中是否包含特殊字元，若有則將其取代為字母與數字。

- 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 2005 或 SQL Server 2005 Express。

  未設定 SQL Server 2005 接受遠端連線時，即可能發生此問題。根據預設，SQL Server 2005 Express 版與 SQL Server 2005 Developer 版不允許遠端連線。若要設定 SQL Server 2005 允許遠端連線，請完成下列所有步驟：

  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，請執行下列步驟：

  1. 移至 `<Visual Studio installation folder>\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，便可能發生此問題。在這種情況下，Internet Explorer 會封鎖對於含有多重框架的安全網站所進行的存取。若要解決此問題，請將「行動安全防護」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」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

聯絡技術支援

趨勢科技為所有已註冊的使用者提供為期一年的技術支援、病毒碼下載與程式更新，一年期滿後，您即須購買維護合約。如果您需要協助或有任何問題，請不吝與我們聯絡。我們也歡迎您提供意見。

- 從以下網址取得全球支援辦公室清單：http://esupport.trendmicro.com/zh-tw/default.aspx

- 從以下網址取得最新的趨勢科技產品文件：http://docs.trendmicro.com/zh-TW/home.aspx

在美國地區，您可以透過電話、傳真或電子郵件與趨勢科技代表聯絡：

```
Trend Micro, Inc.
10101 North De Anza Blvd.,
Cupertino, CA 95014
Toll free: +1 (800) 228-5651 (sales)
Voice: +1 (408) 257-1500 (main)
Fax: +1 (408) 257-2003
Web address: http://www.trendmicro.com
Email: support@trendmicro.com
```

將中毒檔案傳送給趨勢科技

您可以將惡意程式和其他中毒檔案傳送給趨勢科技。具體來說，如果您認為某個檔案是惡意程式，但掃瞄引擎並未加以偵測或清除，您可以使用以下網址將可疑檔案送交給趨勢科技：

http://esupport.trendmicro.com/srf/srfmain.aspx

請在訊息中簡短說明所遇到的症狀。我們的惡意程式工程師團隊將會剖析檔案以釐清並找出檔案所含的惡意程式，然後將已清除的檔案歸還給您，這個程序通常能在 48 小時之內完成。

iTrendLabs

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 是將單一客戶回報的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

管理伺服器, Inc. 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

符號

「超級系統管理員」角色內容, 2-11

A

Android 與 iOS 的未受管理群組, 1-7

E

Exchange ActiveSync 裝置標籤, 3-20
Exchange 伺服器整合, 1-6

H

HTTP(S) 推播通知設定, 1-8

I

iOS 裝置佈建, 1-6

M

MARS, 1-7
MDA 記錄
- Web 威脅防護記錄, 7-2
- 手動刪除, 7-5
- 加密記錄, 7-2
- 防火牆記錄, 7-2
- 事件記錄, 7-2
- 政策違規記錄, 7-2
- 查詢條件, 7-3
- 記錄類型, 7-2
- 惡意程式防護記錄, 7-2
- 預約刪除, 7-4
- 關於, 7-2

O

OfficeScan, 1-6

Q

QR 碼, 1-7

R

root 帳號內容, 2-11

S

SD 卡限制, 1-8

T

TrendLabs, 9-6

W

WAP-Push 防護, 1-12
Web Proxy 支援, 1-8
Web 威脅防護政策, 1-8
Web 網頁安全, 1-11
Widget, 1-6

一畫

一般政策
- Blackberry 設定, 4-8
- 更新設定, 4-7
- 記錄設定, 4-8
- 通知/報告設定, 4-8
- 解除安裝防護功能, 4-7

三畫

下載系統管理員報告, 1-7
大量購買方案, 1-7
已知問題, 9-8

四畫

元件更新
- 下載來源, 6-6
- 已預約, 6-4
- 手動, 6-2
- 本機 AU 伺服器, 6-7
- 關於, 6-2

支援 Android 行動裝置, 1-10
支援 Blackberry 行動裝置, 1-10
支援 iOS 行動裝置, 1-10

五畫

以範本為基礎的政策, 1-6
代理程式自訂, 1-8
加密與密碼
    PIM 資訊, 4-20
    加密演算法, 4-20
    信任的應用程式清單, 4-21
    解鎖密碼政策, 4-18
    檔案型態, 4-20
可自訂註冊 URL, 1-8

六畫

企業憑證, 1-6
企業應用程式商店, 1-9
    關於, 5-2
全球支援辦公室, 9-5
合規政策
    檢查清單, 4-23
合規檢查, 1-9
多個系統管理員帳號, 1-6
行動安全防護
    Active Directory, 1-4
    BES User Administration Tool, 1-5
    Management 伺服器, 1-3
    Microsoft SQL Server, 1-4
    MS Exchange 行動安全整合, 1-4
    OfficeScan, 1-2
    SMTP 伺服器, 1-5
    子群組, 3-2
    不當網路通訊, 1-2
    元件, 1-3
    加密軟體相容性, 1-2
    加密模組, 1-2
    本機通訊伺服器, 1-4
    行動裝置代理程式, 1-4
    架構, 1-3
    基本安全模式, 1-3
    強化安全模式
        本機通訊伺服器, 1-3
        雲端通訊伺服器, 1-3
    通訊方式, 1-3
    通訊伺服器, 1-4
    通訊伺服器類型, 1-4
    部署模式, 1-3
    雲端通訊伺服器, 1-4
    憑證
        APNs 憑證, 1-5
        SCEP, 1-4
        SSL 憑證, 1-5
        公用與私密金鑰, 1-4
        安全防護認證, 1-4
        授權, 1-4
        管理, 2-19
    簡訊發送器, 1-4
    關於, 1-2
行動裝置威脅, 1-2
    垃圾簡訊, 1-2
    拒絕服務攻擊, 1-2
行動裝置註冊, 1-7
行動裝置驗證, 1-12

七畫

伺服器指令確認, 1-6
佈建政策, 1-10
完整版授權, 2-4
快速設定驗證畫面, 1-9
技術支援網站, 9-5
更新的 MDA 介面, 1-7
更新的功能鎖定, 1-10
更新的架構, 1-10

更新的裝置狀態, 1-6
防火牆, 1-12
防火牆政策
IDS, 4-17
SYN Flood 攻擊, 4-17
安全層級, 4-17
例外規則設定, 4-18

八畫
使用者帳號詳細資訊, 2-13
來電過濾, 1-11
政策, 1-10
過濾清單格式, 4-16
過濾清單設定, 4-15
受管理裝置標籤, 3-2
垃圾郵件
WAP-Push, 4-14
核可的清單格式, 4-14
垃圾簡訊
簡訊, 4-12
過濾清單格式, 4-14
過濾清單設定, 4-12
垃圾簡訊防護, 1-11
定期更新, 1-12

九畫
指令狀態, 2-17

八畫
政策違規記錄, 1-7

九畫
相容性檢視, 2-4

十畫
根據裝置識別碼的驗證, 1-7
病毒碼更新完成後進行掃瞄, 1-8

十一畫
密碼
重設密碼, 1-9, 3-14
解除安裝防護, 9-2
驗證碼, 3-15
常見問題集, 9-5
清除行動裝置上的公司資料, 3-13
軟體更新
Readme 檔, 9-8
版本項目, 9-7
關於, 9-7
通知和報告
Token 變數, 8-9, 8-10
通知, 8-8
報告, 8-8
簡訊代理程式狀態, 8-7
簡訊設定, 8-9
簡訊發送器, 8-3
關於, 8-2

十二畫
最新文件, 9-6
報表
Patch 與元件更新狀態, 2-5
已破解/Root 權限狀態, 2-6
加密狀態, 2-6
行動裝置狀態, 2-5
伺服器更新狀態, 2-6
畫面, 1-9
資訊管理, 1-6
應用程式控制狀態, 2-7
尋找遠端裝置, 1-10
惡意程式防護政策
掃瞄選項, 4-11
掃瞄類型, 4-11
惡意程式防護掃瞄, 1-11

十三畫
傳送電子郵件警訊, 4-25
新功能
7.0 版, 1-10
7.1 版, 1-9
8.0 版, 1-8
8.0 版 SPQ, 1-7
9.0 版, 1-6
資料加密, 1-12
資源
網路式工具與服務, 9-8
預約報告, 1-9

十四畫
疑難排解提示, 9-2
.pac 自動組態設定檔, 9-4
BES, 9-3
devenv.exe.config 組態設定檔, 9-3
SCEP 憑證, 9-2
SQL Server 2005, 9-3
SQL Server 2008 R2, 9-3
SQL Server Express, 9-3
加密模組, 9-2
未同步, 9-4
用戶端裝置清單, 9-4
系統時鐘, 9-2
通訊伺服器, 9-2
監督的裝置管理, 1-6
管理 Web 主控台, 2-2, 2-4
URL, 2-2
作業, 2-2
使用者名稱與密碼, 2-3
與 Active Directory 整合, 1-10

十五畫
增強的事件記錄, 1-8

十六畫
獨立式 Management 伺服器, 1-6
選用的雲端通訊伺服器, 1-6
選用驗證, 1-9
選擇性清除, 1-9
應用程式控管, 1-6, 1-9
應用程式推播, 1-9
應用程式資產清單, 1-9

十七畫
趨勢科技
關於, 9-8
邀請的裝置標籤, 3-17
邀請狀態, 3-18
邀請電子郵件資訊, 3-17

十八畫
簡化佈建, 1-8
簡單 iOS 用戶端, 1-8
鎖定 Windows Mobile 裝置, 3-12
鎖定政策增強, 1-7

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: TSTM96390/140410