TREND MICRO™

9.7 趨勢科技™ 行動安全防護 Patch 2 安裝與部署手冊

企業版攜帶型裝置全面性安全解決方案

Endpoint Security

文件編號：TSTM97808/170419

發行日期：2017 年 4 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：規劃伺服器安裝

第 2 章：設定環境

第 3 章：安裝、更新及移除伺服器元件

第 4 章：設定伺服器元件

第 5 章：處理行動裝置代理程式

序言

前言

歡迎使用《趨勢科技™企業版行動安全防護　9.7 版 Patch 2 *安裝與部署手冊*》。本手冊可協助系統管理員部署與管理「趨勢科技™企業版行動安全防護 9.7 版 Patch 2」。本手冊說明各種「行動安全防護」元件和不同的行動裝置代理程式部署方法。

如需「行動安全防護」的更新資訊（包括行動裝置支援和最新版本的 Build），請瀏覽 http://www.trendmicro.tw/tw/enterprise/product-security/mobile-security/index.html。

注意

此《*安裝與部署手冊*》僅適用於「行動安全防護 9.7 版 Patch 2」。不適用於其他版本的「行動安全防護」。趨勢科技支援僅限於「行動安全防護」的使用。若要取得本手冊提及之協力廠商應用程式的支援，請聯絡相關廠商。

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

規劃伺服器安裝

本章可協助系統管理員規劃「趨勢科技™ 企業版行動安全防護 9.7 版 Patch 2」的伺服器元件。

本章包含以下小節：

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）

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」支援在雲端部署「通訊伺服器」。下圖顯示典型「強化安全模式」中每個「行動安全防護」元件的所在位置。

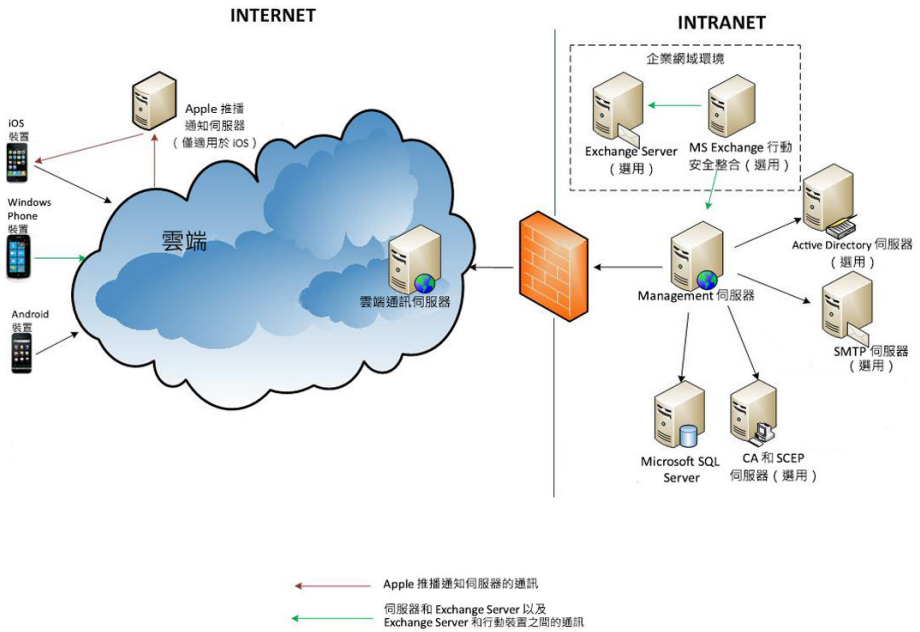

圖 1-1. 強化安全模式與雲端通訊伺服器

強化安全模式與本機通訊伺服器（雙伺服器安裝）

「強化安全模式」支援將「通訊伺服器」與「管理伺服器」安裝在兩台不同的電腦上。下圖顯示典型「強化安全模式」中每個「行動安全防護」元件的所在位置。

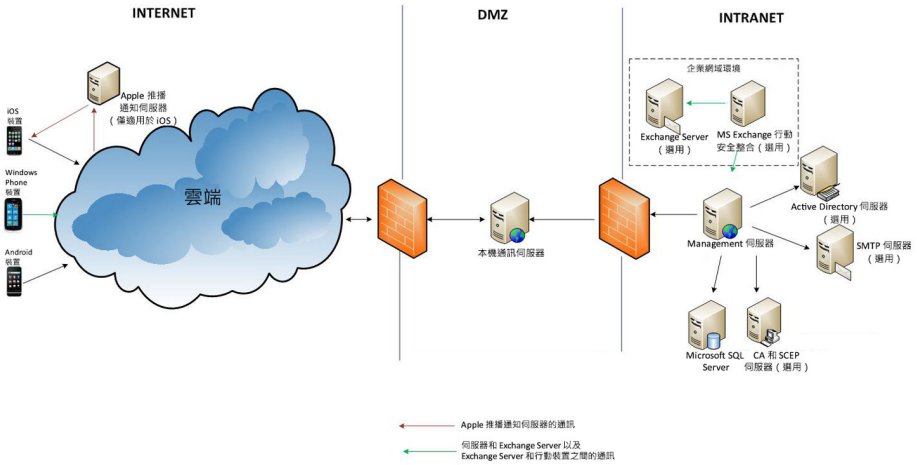

圖 1-2. 強化安全模式與本機通訊伺服器

基本安全模式（單一伺服器安裝）

「基本安全模式」支援將「通訊伺服器」與「管理伺服器」安裝在同一台電腦上。下圖顯示典型「基本安全模式」中每個「行動安全防護」元件的所在位置。

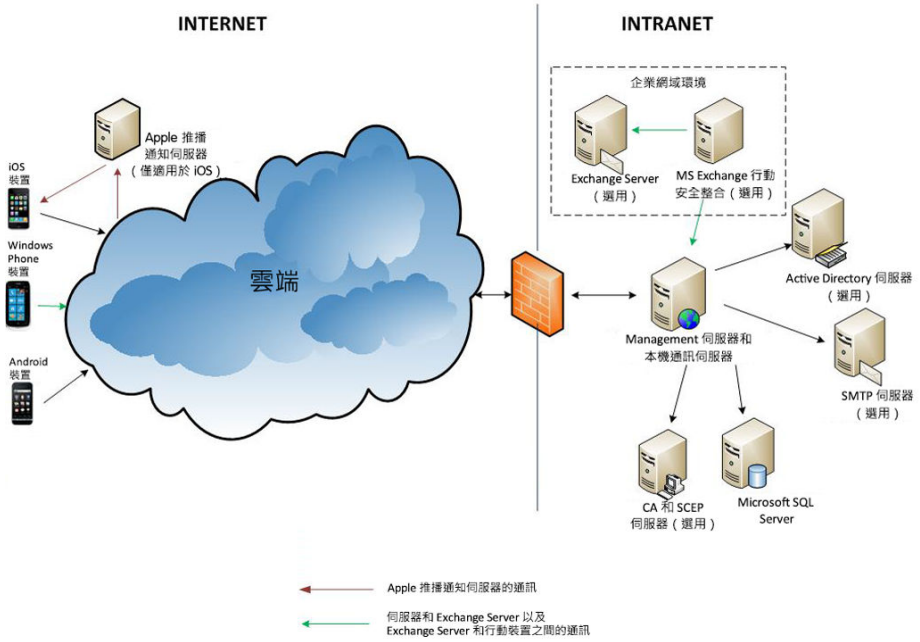

圖 1-3. 基本安全模式

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
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。 • 雲端通訊伺服器 (CCS)— 這是部署在雲端的 Communication Server，您不必安裝此伺服器。趨勢科技會管理雲端通訊伺服器，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 1-8 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

元件	說明	必要或選用
Microsoft SQL Server	Microsoft SQL Server 代管「行動安全防護管理伺服器」的資料庫。	必要
Active Directory	「行動安全防護管理伺服器」會從 Active Directory 匯入使用者與群組。	選用
憑證授權	「憑證授權」可管理安全防護認證以及用於安全通訊的公用與私密金鑰。	選用
SCEP	「簡單憑證註冊通訊協定」(SCEP) 是為私密憑證授權提供網路前端的通訊協定。 在某些環境中，確保公司設定和政策免遭窺探是非常重要的。若要提供此防護，iOS 允許您加密資料檔，以便它們只能由單一裝置讀取。加密的資料檔就像是一般的設定資料檔，只是設定資料檔負載是透過與裝置 X.509 身分相關聯的公用金鑰加密的。 SCEP 使用「憑證授權」在大型企業發行憑證。它會處理數位憑證的發行與撤銷。SCEP 與「憑證授權」可安裝在同一台伺服器上。	選用
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 Windows Phone 或 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	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	支援	支援
管理 Windows Phone	不支援	支援

系統需求

在網路中安裝各個「行動安全防護」元件之前，請先檢閱以下需求。

表 1-3. 系統需求

元件	需求
管理伺服器與通訊伺服器	建議平台 • Windows Server 2008 R2 Enterprise 版 • Windows Server 2008 Enterprise 版 SP1 • Windows Server 2008 Standard 版 • Windows Web Server 2008 版 SP1 • Windows Server 2016 其他平台 • Windows 2008 Server 系列 • Windows 2008 R2 Server 系列 • Windows 2012 Server 系列 • Windows Server 2012 R2 系列
	硬體 • 1-GHz Intel™ Pentium™ 處理器或同等級處理器 • 至少 1 GB 的 RAM • 至少 400 MB 的可用磁碟空間 • 支援 256 色或更多顏色的 1024 x 768 解析度螢幕

元件	需求
管理伺服器的 IIS Web 伺服器	Microsoft Internet Information Server (IIS) 7.0/7.5/8.0 注意 • IIS 是 Microsoft Windows 的必要部分，且 IIS 版本號碼與所安裝的 Windows 版本對應。 • 保留預設的設定並選取 當為「管理伺服器」使用 IIS 7.0 或更新版本時，請保留預設的設定，並在「應用程式開發」中啟動及安裝「CGI」與「ISAPI 延伸」，在「一般 HTTP 功能」中設定「HTTP 重新導向」，在「管理工具」中設定「IIS6 管理相容性」。 注意 「趨勢科技行動安全防護」並「不」支援 Apache Web 伺服器。
Microsoft Exchange Server	• Microsoft Exchange 伺服器 2007 • Microsoft Exchange 伺服器 2010 • Microsoft Exchange 伺服器 2013
網路瀏覽器	• Internet Explorer 9.0 或以上版本 • Chrome 17 或以上版本 • Firefox 14 或以上版本 • Mac 的 Safari 6 或以上版本 注意 「行動安全防護」管理 Web 主控台需要 Adobe Flash Player。

元件	需求
SQL Server	• Microsoft SQL Server 2008 • Microsoft SQL Server 2008 Express 版 • Microsoft SQL Server 2008 R2 • Microsoft SQL Server 2008 R2 Express 版 • Microsoft SQL Server 2012 • Microsoft SQL Server 2012 Express 版 • Microsoft SQL Server 2014 • Microsoft SQL Server 2014 Express 版
MS Exchange 行動安全整合	平台 • Windows Server 2008 R2（64 位元） • Windows Server 2012（64 位元） • Windows Server 2012 R2（64 位元） 硬體 • 1-GHz Intel™ Pentium™ 處理器或同等級處理器 • 至少 1 GB 的 RAM • 至少 200 MB 的可用磁碟空間 其他 • Microsoft .Net Framework 3.5 SP1

安裝摘要

以下步驟介紹如何安裝 Trend Micro Mobile Security：

1. 設定「行動安全防護」安裝的環境。

   如需詳細資料，請參閱設定行動安全防護安裝的環境 第 2-2 頁。

a. 將 Microsoft IIS Web 伺服器安裝在您計劃安裝「管理伺服器」的電腦上。

   如需詳細資料，請參閱安裝 Microsoft IIS Web Server 第 2-5 頁。

b. （選用）安裝資料庫。

   如果您在此階段略過此步驟，Mobile Security 會在安裝期間自動安裝 Microsoft SQL Server 2008 Express 版。

   如需詳細資料，請參閱安裝 SQL Server（選用） 第 2-6 頁。

c. （選用）設定 Active Directory 帳號存取權限。

   如果您想要從公司的 Active Directory 伺服器匯入使用者，請執行此步驟。

   如需詳細資料，請參閱設定 Active Directory 帳號存取權限（選用） 第 2-7 頁。

d. （選用）安裝 Microsoft Exchange 伺服器管理工具。

   將 Exchange 伺服器與「管理伺服器」整合，以管理 Windows Phone、Android、iOS 行動裝置。

   如需詳細資料，請參閱安裝 Microsoft Exchange Server 管理工具（選用） 第 2-7 頁。

e. 套用網路存取規則。

   如需詳細資料，請參閱套用行動安全防護的網路存取規則 第 2-8 頁。

2. （選用）為 iOS 行動裝置設定環境。

   如需詳細資訊，請參閱設定 iOS 行動裝置環境（選用） 第 2-3 頁。

3. 安裝伺服器元件。

   如需詳細資訊，請參閱安裝伺服器元件 第 3-2 頁。

   a. 安裝行動安裝防護管理伺服器。

      如需詳細程序，請參閱安裝管理伺服器 第 3-3 頁。

b. 登入「企業版行動安全防護」管理 Web 主控台。

如需詳細程序，請參閱存取管理 Web 主控台 第 3-8 頁。

c. 註冊產品。

如需詳細程序，請參閱註冊產品 第 3-10 頁。

d. （選用）下載並安裝「本機通訊伺服器」(LCS)。

如果您計劃使用「雲端通訊伺服器」(CCS)，可以略過此步驟。

如需詳細程序，請參閱安裝本機通訊伺服器 第 3-11 頁。

e. （選用）設定「Exchange 伺服器整合」。

如果您不想要管理使用 Exchange ActiveSync 的行動裝置，可以略過此步驟。

如需詳細程序，請參閱安裝 MS Exchange 行動安全整合 第 3-17 頁。

i. 確保已安裝「Microsoft Exchange 伺服器管理工具」。

如需安裝程序，請參閱安裝 Microsoft Exchange Server 管理工具（選用） 第 2-7 頁。

ii. 設定 MS Exchange 行動安全整合的帳號。

提供 MS Exchange 行動安全整合的存取權。

如需詳細程序，請參閱設定 MS Exchange 行動安全整合的帳號 第 3-15 頁。

iii. 安裝 MS Exchange 行動安全整合。

在「管理伺服器」與 Exchange 伺服器之間建立通訊。

如需詳細程序，請參閱安裝 MS Exchange 行動安全整合 第 3-17 頁。

iv. 設定 Exchange 伺服器整合設定。

如需詳細程序，請參閱進行 Exchange 伺服器整合設定 第 4-16 頁。

4. 設定伺服器元件。

如需詳細資料，請參閱初始伺服器設定 第 4-3 頁。

a. 進行伺服器部署設定。

   如需詳細程序，請參閱進行部署設定 第 4-11 頁。

b. 進行資料庫設定。

   如需詳細程序，請參閱進行資料庫設定 第 4-5 頁。

c. 進行「通訊伺服器」設定。

   如需詳細程序，請參閱進行一般通訊伺服器設定 第 4-6 頁。

d. （選用）針對 Android 設定「通訊伺服器」。

   如果您不想要管理 Android 行動裝置，可以略過此步驟。

   如需詳細程序，請參閱進行 Android 通訊伺服器設定 第 4-8 頁。

e. （選用）針對 iOS 設定「通訊伺服器」。

   如果您不想要管理 iOS 行動裝置，可以略過此步驟。

   如需詳細程序，請參閱進行 iOS 通訊伺服器設定 第 4-9 頁。

f. 進行「裝置註冊」設定。

   如需詳細程序，請參閱進行裝置註冊設定 第 4-12 頁。

g. （選用）自訂「行動安全防護使用規範」。

   如果您想要使用預設的「行動安全防護使用規範」，可以略過此步驟。

   如需詳細程序，請參閱自訂「行動安全防護使用規範」 第 4-14 頁。

h. （選用）進行 Active Directory 設定。

   如果您不想要從 Active Directory 伺服器匯入使用者，可以略過此步驟。

   如需詳細程序，請參閱進行 Active Directory (AD) 設定 第 4-15 頁。

i. （選用）進行「管理伺服器」設定。

如果您的「管理伺服器」不使用 Proxy 存取網路，且您想要使用預設的伺服器 IP 位址與通訊埠號碼，可以略過此步驟。

如需詳細程序，請參閱進行管理伺服器設定 第 4-16 頁。

j. （選用）進行「Exchange 伺服器整合」設定。

如果您不想要管理使用 Exchange ActiveSync 的行動裝置，可以略過此步驟。

如需詳細程序，請參閱進行 Exchange 伺服器整合設定 第 4-16 頁。

k. （選用）進行通知和報告設定。

如果您不想要傳送邀請電子郵件給使用者，可以略過此步驟。

請參閱進行通知和報告設定 第 4-19 頁。

l. （選用）設定系統管理員通知。

如果您不想要透過電子郵件收到錯誤訊息通知和定期的預約報告，可以略過此步驟。

如需詳細程序，請參閱設定系統管理員通知 第 4-19 頁。

m. 驗證「行動安全防護」設定（建議）。

如需相關程序，請參閱驗證行動安全防護設定 第 4-20 頁。

n. 變更管理 Web 主控台的系統管理員帳號密碼。

如需相關程序，請參閱《*管理手冊*》中的＜*編輯系統管理員帳號*＞主題。

5. 設定行動裝置代理程式。

設定行動裝置代理程式 第 5-3 頁

a. （選用）設定行動裝置的通知設定。

如需詳細程序，請參閱進行通知和報告設定 第 4-19 頁。

b. （選用）設定 Mobile Security 要以電子郵件和/或簡訊傳送給使用者的安裝訊息。

安裝訊息包含使用者存取以下載與安裝 MDA 設定套件的 URL。

如需詳細程序，請參閱設定安裝訊息 第 5-3 頁。

c. （選用）將邀請傳送給使用者。

如需詳細程序，請參閱邀請使用者註冊 第 5-4 頁。

d. 在行動裝置上安裝 MDA。

如需詳細程序，請參閱在行動裝置上安裝 MDA 第 5-8 頁。

e. 向「管理伺服器」註冊 MDA。

如需詳細程序，請參閱向行動安全防護管理伺服器註冊 MDA 第 5-16 頁。

第 2 章

設定環境

本章提供安裝「趨勢科技™企業版行動安全防護 9.7 版 Patch 2」前設定環境所需的資訊。

本章包含以下小節：

設定行動安全防護安裝的環境

下表說明設定「行動安全防護」安裝環境的程序。

表 2-1. 設定行動安全防護安裝環境的程序

步驟	處理行動	說明
步驟 1	將 Microsoft IIS Web 伺服器安裝在您計劃安裝「管理伺服器」的電腦上。	如需詳細資料，請參閱安裝 Microsoft IIS Web Server 第 2-5 頁。
步驟 2	（選用）安裝資料庫。	如果您現在略過此步驟，「行動安全防護」在安裝期間會自動安裝 Microsoft SQL Server 2008 Express 版。 如需詳細資料，請參閱安裝 SQL Server（選用） 第 2-6 頁。
步驟 3	（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。） （選用）設定 Active Directory 帳號存取權限。	如果您想要從公司的 Active Directory 伺服器匯入使用者，請執行此步驟。 如需詳細資料，請參閱設定 Active Directory 帳號存取權限（選用） 第 2-7 頁。
步驟 4	（僅限「完整版」部署模式。） （選用）安裝 Microsoft Exchange 伺服器管理工具。	將 Exchange 伺服器與「行動安全防護管理伺服器」整合，以管理 Windows Phone、Android、iOS 行動裝置。 如需詳細資料，請參閱安裝 Microsoft Exchange Server 管理工具（選用） 第 2-7 頁。
步驟 5	套用網路存取規則。	如需詳細資料，請參閱套用行動安全防護的網路存取規則 第 2-8 頁。 如需完整的網路通訊埠設定，請參閱網路通訊埠組態設定 第 A-1 頁。

步驟	處理行動	說明
步驟 6	（選用）設定管理 iOS 行動裝置的環境。	如果您想要管理 iOS 行動裝置，則此步驟為必要。 請參閱設定 iOS 行動裝置環境（選用） 第 2-3 頁。

設定 iOS 行動裝置環境（選用）

警告!

設定可管理 iOS 行動裝置的環境前，請先務必執行在下表中提及的所有步驟。

下表說明設定環境以管理 iOS 行動裝置的程序。

表 2-2. iOS 行動裝置環境設定程序

步驟	處理行動	說明
步驟 1	（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。） 設定 Apple 推播通知服務 (APNs) 憑證。	如果您要管理 iOS 行動裝置，必須設定 APNs 憑證。 如需詳細程序，請參閱產生及設定 APNs 憑證 第 C-1 頁。

步驟	處理行動	說明
步驟 2	（僅限「完整版」部署模式。） （選用）從經認可的公用憑證授權單位取得 SSL 伺服器憑證。	SSL 憑證用於行動裝置與「通訊伺服器」之間的安全通訊。 如果您要管理 Windows Phone 或 iOS 行動裝置，或計劃使用「本機通訊伺服器」，則此步驟是必要的。「本機通訊伺服器」安裝期間，您必須匯入公用 SSL 憑證。 您可以略過此步驟： • 如果您要使用私人 SSL 憑證。「行動安全防護」將在「本機通訊伺服器」安裝期間建立該憑證。 • 如果您計劃使用「雲端通訊伺服器」。
步驟 3	（僅限「完整版」部署模式。） （選用）設定簡單憑證註冊通訊協定 (SCEP) 以獲得額外的安全防護	在行動裝置與「通訊伺服器」之間提供安全的通訊。 如需詳細資料，請參閱設定 SCEP 第 B-5 頁。 如果您已在環境中設定 SCEP，則可略過此步驟。 注意 如果不想要將 SCEP 用於 iOS 行動裝置，您需要在「管理伺服器」和 Communication Server 安裝完成後，於「通訊伺服器設定」中將其關閉。如需相關程序，請參閱進行 iOS 通訊伺服器設定 第 4-9 頁。

步驟	處理行動	說明
步驟 4	在「本機通訊伺服器」上設定網路通訊埠 2195 (TCP)，在 Wi-Fi 網路上設定通訊埠 5223。	TCP 通訊埠 2195 — 允許從「通訊伺服器」的 TCP 通訊埠 2195 連線至「Apple 推播通知服務」的外送連線。Apple 推播通知服務的主機名稱為 gateway.push.apple.com。 通訊埠 5223　可讓　iOS 裝置接收來自 Apple 伺服器的推播通知，尤其是當裝置透過通訊埠 5223 遭封鎖的 Wi-Fi 網路連接時。不過如果行動裝置位在 3G 網路中，您不需要設定此通訊埠。 如需完整的網路通訊埠設定，請參閱網路通訊埠組態設定 第 A-1 頁。

安裝 Microsoft IIS Web Server

此作業是設定「行動安全防護」安裝環境程序中的一個步驟。

請參閱設定行動安全防護安裝的環境 第 2-2 頁。

程序

- 瀏覽至以下其中一個 URL 以進行 IIS 安裝程序：
  - Windows 2008 或 Windows Server 2008 R2（IIS 7.0 或 7.5）

    http://www.iis.net/learn/install/installing-iis-7
  - Windows 2012 (IIS 8.0)

    http://www.iis.net/learn/get-started/whats-new-in-iis-8/installing-iis-8-on-windows-server-2012

注意

當為「管理伺服器」使用 IIS 7.0 或更新版本時，請保留預設的設定，並在「應用程式開發」中啟動及安裝「CGI」與「ISAPI 延伸」，在「一般 HTTP 功能」中設定「HTTP 重新導向」，在「管理工具」中設定「IIS6 管理相容性」。

安裝 SQL Server（選用）

注意

如果您不想要安裝任何特定的 SQL Server 版本，請略過此步驟。「行動安全防護」在安裝期間會自動安裝 Microsoft SQL Server 2008 Express 版。

此作業是設定「行動安全防護」安裝環境程序中的一個步驟。

請參閱設定行動安全防護安裝的環境 第 2-2 頁。

程序

- 瀏覽至以下其中一個 URL 以進行 SQL Server 安裝程序：
  - Microsoft SQL Server 2008/2008 R2（或 Express 版）：

    http://msdn.microsoft.com/en-us/library/ms143219(v=SQL.100).aspx
  - Microsoft SQL Server 2012（或 Express 版）：

    http://msdn.microsoft.com/en-us/library/bb500395(v=SQL.110).aspx

注意

趨勢科技建議您將 SQL Server 驗證方法用於 SQL Server，避免使用 Windows 驗證。不過，您也可以為 SQL Server 設定 Windows 驗證。如需詳細資料，請參閱將 Windows 驗證用於 SQL Server 第 B-2 頁。

設定 Active Directory 帳號存取權限（選用）

注意

本主題僅適用於「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。

注意

如果您計劃將 Active Directory 用於使用者驗證或從 Active Directory 匯入使用者，只需要執行此步驟。否則請略過此步驟。

如果您尚未安裝 Active Directory，請參閱下列 URL 中的詳細安裝程序：

http://technet.microsoft.com/en-us/library/cc757211(WS.10).aspx

此作業是設定「行動安全防護」安裝環境程序中的一個步驟。

請參閱設定行動安全防護安裝的環境 第 2-2 頁。

程序

- 為「行動安全防護 9.7 版 Patch 2」建立 Active Directory 服務帳號，並至少指定 Active Directory 的唯讀權限。請參閱下列 URL 中有關建立 Windows 2008 的 Active Directory 帳號說明：

  http://technet.microsoft.com/zh-tw/library/dd894463(WS.10).aspx

安裝 Microsoft Exchange Server 管理工具（選用）

注意

本主題僅適用於「完整版」部署模式。

「Microsoft Exchange Server 管理工具」讓 Exchange Server 與「管理伺服器」整合，以管理 Windows Phone、Android 和 iOS 行動裝置。

此作業是設定「行動安全防護」安裝環境程序中的一個步驟。

請參閱設定行動安全防護安裝的環境 第 2-2 頁。

程序

- 瀏覽至以下其中一個 URL 以進行「Exchange Server 管理工具」的安裝程序：
  - 安裝 Exchange Server 管理工具 2007：

    http://technet.microsoft.com/zh-tw/library/bb232090(v=EXCHG.80).aspx
  - 安裝 Exchange Server 管理工具 2010：

    http://technet.microsoft.com/library/bb232090(v=EXCHG.141)
  - 安裝 Exchange Server 管理工具 2013：

    http://technet.microsoft.com/zh-tw/library/bb232090(v=exchg.150).aspx

套用行動安全防護的網路存取規則

此作業是設定「行動安全防護」安裝環境程序中的一個步驟。

請參閱設定行動安全防護安裝的環境 第 2-2 頁。

程序

- 套用下列網路存取規則：
  - 如果您計劃使用 Active Directory，則「管理伺服器」應能夠連線至 Active Directory 伺服器。如果您正在使用防火牆，請務必在「管理伺服器」的防火牆設定中新增例外。

- 「管理伺服器」應該能連線至安裝「趨勢科技行動安全防護」資料庫的 SQL Server。如果您正在使用防火牆，請務必在 SQL Server 和「管理伺服器」的防火牆設定中新增例外。
- 為通訊埠 4343 新增例外，以確保「管理伺服器」與「通訊伺服器」之間能夠進行 HTTPS 連線：

  如果您需要自訂此通訊埠號碼，請參閱設定通訊伺服器通訊埠 第 B-4 頁以取得詳細資料。
- 為通訊埠號碼 80 與 443 新增例外，以確定所有的行動裝置能夠連線至「通訊伺服器」。

第 3 章

安裝、更新及移除伺服器元件

本章將引導系統管理員安裝「趨勢科技™企業版行動安全防護 9.7 版 Patch 2」伺服器元件。並引導系統管理員移除伺服器元件。

本章包含以下小節：

安裝伺服器元件

安裝之前

在您繼續安裝「行動安全防護」伺服器元件前：

- 請務必確保「行動安全防護」元件符合指定的系統需求。

  請參閱系統需求 第 1-8 頁。您可能也需要評估網路拓樸，以及決定要安裝的「行動安全防護」伺服器元件。

- 請務必執行設定環境 第 2-1 頁一章所述的所有先決條件步驟。

趨勢科技行動安全防護安裝工作流程

下表說明安裝「趨勢科技行動安全防護」的基本方法。

表 3-1. 趨勢科技行動安全防護安裝工作流程

步驟	處理行動	說明
步驟 1	安裝行動安裝防護管理伺服器。	如需詳細程序，請參閱安裝管理伺服器 第 3-3 頁。
步驟 2	登入「企業版行動安全防護」管理 Web 主控台。	如需詳細程序，請參閱存取管理 Web 主控台 第 3-8 頁。
步驟 3	註冊產品。	如需詳細程序，請參閱註冊產品 第 3-10 頁。
步驟 4	（選用）下載並安裝「本機通訊伺服器」。	如果您計劃使用「雲端通訊伺服器」(CCS)，可以略過此步驟。 如需詳細程序，請參閱安裝本機通訊伺服器 第 3-11 頁。

步驟	處理行動	說明
步驟 5	（僅限「完整版」部署模式。） （選用）安裝 MS Exchange 行動安全整合。	如果您不想要管理使用 Exchange ActiveSync 的行動裝置，可以略過此步驟。 如需詳細程序，請參閱安裝 MS Exchange 行動安全整合 第 3-17 頁。

安裝管理伺服器

注意

「行動安全防護」需要 Java Runtime Environment (JRE) 才能從「管理伺服器」上的「應用程式管理」模組上傳 .apk 檔案。JRE 會自動隨著「管理伺服器」一同安裝。然而，如果安裝「管理伺服器」的電腦已安裝 JRE，「管理伺服器」安裝程式便不會安裝 JRE。如果現有的 JRE 版本比 1.6 舊，您將需要手動解除安裝 JRE，然後安裝 1.6 或以上版本。

程序

1. 從下列位置下載「管理伺服器」安裝程式：

   http://downloadcenter.trendmicro.com/index.php?clk=left_nav&clkval=all_download&regs=TW

2. 將下載的檔案解壓縮，然後執行「管理伺服器」安裝程式：`MdmServerSetup.exe`.

   「歡迎」畫面隨即出現。

3. 按一下「下一步」。

   「授權合約」畫面隨即顯示。

4. 勾選「我同意」核取方塊，再按一下「下一步」。

注意

「行動安全防護」會要求您安裝 Microsoft Visual C++ 2005 可轉散發項目檔案。如果您已將這些檔案安裝在您的電腦上，則 Microsoft Visual C++ 2005 可轉散發項目檔案安裝步驟在安裝期間不會出現。如果 Microsoft Visual C++ 2005 可轉散發項目檔案安裝畫面顯示，請按一下畫面上的「下一步」繼續安裝。

「資料庫選項」畫面隨即顯示。

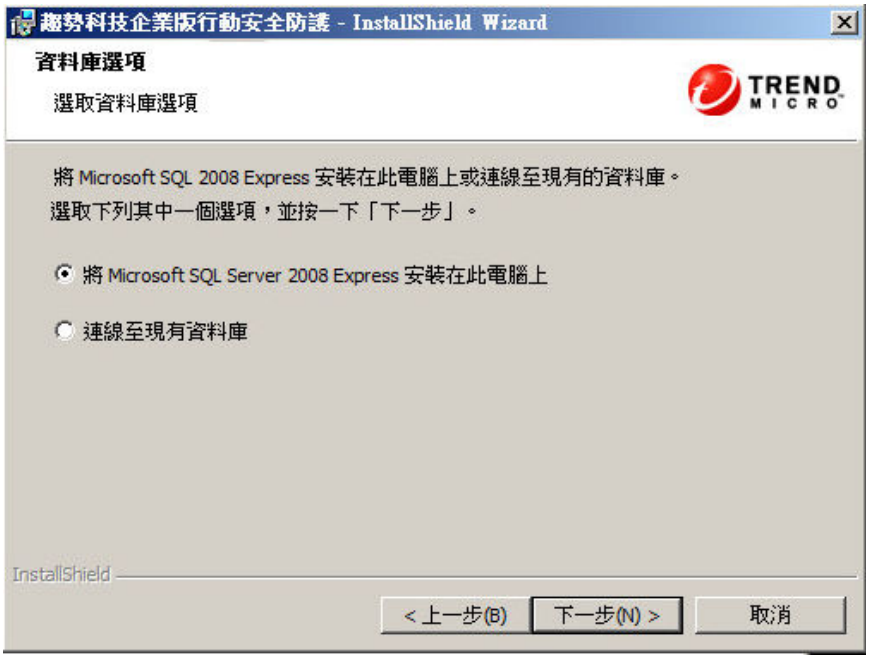

圖 3-1.「資料庫選項」畫面

5. 請執行以下任一項工作：

- 如果您沒有任何已安裝的資料庫，或是想要為「行動安全防護」建立新的資料庫：

  a. 選取「將 Microsoft SQL Server 2008 Express 安裝在此電腦上」，並按一下「下一步」。

「資料庫安裝」畫面隨即顯示。

圖 3-2. 新資料庫的「資料庫安裝」畫面

b. 為您的新資料庫輸入密碼，並按一下「下一步」。

「安裝進度」畫面隨即顯示，並顯示目前的安裝狀態。

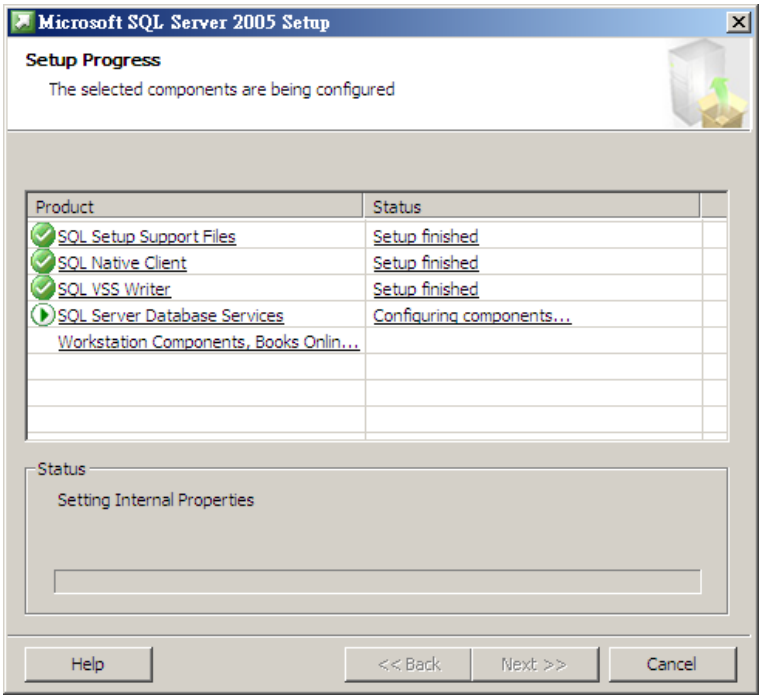

圖 3-3.「安裝進度」畫面

c. 安裝完成後，按一下「下一步」。

「伺服器連線設定」畫面隨即出現。

- 如果您已經有安裝好的資料庫，並想要使用現有的資料庫：

a. 選取「連線至現有資料庫」，並按一下「下一步」。

「現有資料庫」畫面隨即顯示。

圖 3-4. 現有資料庫伺服器資訊

b. 輸入您的現有資料庫伺服器資訊，並按一下「下一步」

「伺服器連線設定」畫面隨即出現。

6. 從下拉式清單中選取 IP 位址，並輸入伺服器通訊埠號碼，並按一下「下一步」。

7. 選取您要安裝「行動安全防護」的位置，然後按一下「下一步」。

注意

按一下「變更」可選取不同的位置。

8. 按一下「安裝」以開始安裝。

安裝進度視窗隨即出現。安裝完成後，便會顯示「趨勢科技行動安全防護安裝完成」畫面。

9. 按一下「完成」。

接下來需執行的動作

請參閱趨勢科技行動安全防護安裝工作流程 第 3-2 頁中下一個組態設定工作的描述。

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「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 3-5. 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《管理手冊》中的＜編輯系統管理員帳號＞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 3-9 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）。

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」。

註冊產品

趨勢科技會在指定期間內提供所有註冊使用者技術支援、惡意程式病毒碼下載及產品更新，待指定期間過後，您就必須購買續約維護才能繼續享有以上服務。請註冊「行動安全防護」伺服器以確保您能接收最新的安全更新及其他產品和維護服務。

您只需要在「管理伺服器」上使用啟動碼註冊「行動安全防護」伺服器。行動裝置與伺服器連線並向伺服器註冊後，「行動裝置代理程式」將會自動從「行動安全防護」伺服器取得授權資訊。

啟動碼的格式如下所示：

xx-xxxx-xxxxx-xxxxx-xxxxx-xxxxx-xxxxx

程序

1. 登入管理 Web 主控台。

   如果這是您首次存取管理主控台，「產品使用授權」畫面將會出現；如果不是，請按一下「管理 > 產品使用授權」，然後按一下「新的啟動碼」。

2. 在提供的欄位中輸入啟動碼，然後按一下「儲存」。

圖 3-6. 安裝完成後註冊「行動安全防護」

3. 驗證產品註冊順利完成。按一下「報表」以顯示「報表」畫面。

   如果產品註冊順利完成，您應看見「“趨勢科技行動安全防護 9.7 Patch 2 已啟動。”」訊息。

註冊完成後，「行動安全防護設定與驗證」畫面會顯示並引導您逐步完成初始設定。

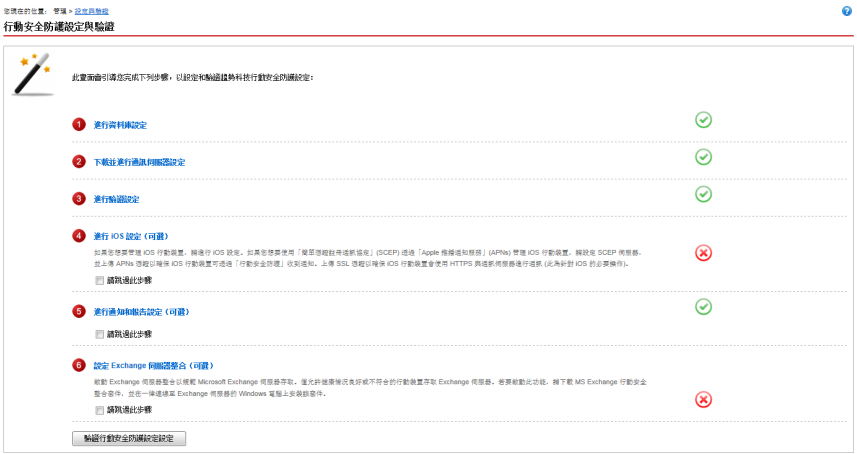

圖 3-7. 行動安全防護設定與驗證畫面

接下來需執行的動作

請參閱趨勢科技行動安全防護安裝工作流程 第 3-2 頁中下一個組態設定工作的描述。

安裝本機通訊伺服器

程序

1. 在您要安裝「通訊伺服器」的電腦上登入管理 Web 主控台。
2. 按一下「管理 > 通訊伺服器設定」。
3. 按一下「一般設定」標籤。
4. 從下拉式清單中選取「本機通訊伺服器」，然後按「按一下這裡以下載」。

5. 按兩下安裝檔以啟動安裝程序。

   「歡迎」畫面隨即出現。

6. 按一下「下一步」。

   「授權合約」畫面隨即顯示。

7. 選取「我接受合約」，然後按一下「下一步」。

   「行動裝置的通訊伺服器連線設定」畫面隨即顯示。

8. 從下拉式清單中選取 IP 位址，並輸入「通訊伺服器」的 HTTP 與 HTTPs 通訊埠號碼。

   此畫面上的 IP 位址和通訊埠號碼用於讓「通訊伺服器」與行動裝置通訊。

   注意

   趨勢科技建議您選取「全部」IP 位址。

9. 按一下「下一步」。

   「管理伺服器的通訊伺服器連線設定」畫面隨即顯示。

10. 從下拉式清單中選取 IP 位址，並輸入「通訊伺服器」的 HTTPs 通訊埠號碼。

    此畫面上的 IP 位址和通訊埠號碼用於讓「通訊伺服器」與「管理伺服器」通訊。

    注意

    趨勢科技建議您選取「全部」IP 位址。

11. 按一下「下一步」。

    「伺服器憑證」畫面隨即出現。

12. 請執行以下任一項工作：

    - 如果您已經有 SSL 憑證可註冊 iOS 行動裝置，請執行以下作業：

a. 選取「匯入現有 .pfx 或 .p12 憑證檔案」，並按一下「下一步」。

「匯入憑證」畫面隨即顯示。

b. 按一下「瀏覽」，並從硬碟中選取公用憑證。

c. 在「密碼」欄位中鍵入憑證密碼。如果憑證沒有密碼，請將此欄位保留空白。

d. 按一下「下一步」。

- 如果您沒有 SSL 憑證可註冊 iOS 行動裝置，或需要建立新的憑證，請執行以下作業：

a. 選取「建立新私密憑證」，並按一下「下一步」。

「建立憑證」畫面隨即顯示。

b. 在「通用名稱」欄位中輸入「通用伺服器」的 IP 位址，並在「密碼」欄位中輸入憑證密碼。

c. 按一下「下一步」。

13. 選取您要安裝「行動安全防護」的位置，然後按「下一步」。

注意

按一下「變更」可選取不同的位置。

14. 按一下「安裝」以開始安裝。

安裝進度視窗隨即出現。安裝完成後，便會顯示「安裝完成」畫面。

15. 按一下「完成」。

接下來需執行的動作

請參閱趨勢科技行動安全防護安裝工作流程 第 3-2 頁中下一個組態設定工作的描述。

設定 Exchange 伺服器整合

注意

本主題僅適用於「完整版」部署模式。

若要在「管理伺服器」與 Exchange 伺服器之間建立通訊，則必須整合 Exchange 伺服器。

注意

「趨勢科技行動安全防護」僅支援 Exchange 伺服器 2007 或更新版本，並提供 Windows Phone、iOS 及 Android 行動裝置的 Exchange 伺服器整合支援。

下表說明「趨勢科技行動安全防護」的 Exchange 伺服器整合設定程序。

表 3-2. Exchange 伺服器整合設定程序

步驟	處理行動	說明
步驟 1	安裝 Microsoft Exchange 伺服器管理工具。	在設定 Exchange 伺服器設定之前，請確保 Microsoft Exchange 伺服器管理工具已安裝在您要安裝 MS Exchange 行動安全整合的電腦上。 如需安裝程序，請參閱安裝 Microsoft Exchange Server 管理工具（選用） 第 2-7 頁。
步驟 2	設定 MS Exchange 行動安全整合的帳號。	提供 MS Exchange 行動安全整合的存取權。 如需詳細程序，請參閱設定 MS Exchange 行動安全整合的帳號 第 3-15 頁。
步驟 3	安裝 MS Exchange 行動安全整合。	在「管理伺服器」與 Exchange 伺服器之間建立通訊。 如需詳細程序，請參閱安裝 MS Exchange 行動安全整合 第 3-17 頁。

步驟	處理行動	說明
步驟 4	設定 Exchange 伺服器整合設定。	如需詳細程序，請參閱進行 Exchange 伺服器整合設定 第 4-16 頁。

設定 MS Exchange 行動安全整合的帳號

注意

本主題僅適用於「完整版」部署模式。

程序

1. 在 Active Directory 伺服器中建立使用者帳號。
2. 在您要安裝「MS Exchange 行動安全整合」的電腦上，瀏覽至「開始 > 系統管理工具 > 電腦管理」，並進行以下設定。
   a. 展開左側樹狀結構的「本機使用者和群組」資料夾，再按兩下「群組」。
   b. 在「系統管理員」上按一下滑鼠右鍵，然後按一下「內容」。
   c. 按一下「一般」標籤上的「新增」按鈕，並進行以下設定：
      i. 在「登入名稱」欄位中輸入您在此程序的步驟 1 第 3-15 頁 中建立的使用者名稱，並按一下「搜尋」。

         「選取使用者、電腦、服務、帳號或群組」對話方塊隨即顯示。
      ii. 在「輸入要選取的物件名稱」欄位中，輸入使用者名稱與網域名稱（例如：domainname\username），並按一下「檢查名稱」。
      iii. 按一下「確定」。
   d. 按一下「系統管理員內容」對話方塊上的「確定」。
3. 在 Active Directory 伺服器上進行以下設定：
   a. 瀏覽至「開始 > 系統管理工具 > Active Directory 使用者和電腦」。

b. 從左側的樹狀結構中展開「使用者」資料夾。

c. 在此程序的步驟 1 第 3-15 頁中建立的帳號（使用者名稱）上按一下滑鼠右鍵，並按一下「加入群組」。

d. 請執行以下任一項工作：

- 若為 Exchange Server 2007，請在「輸入要選取的物件名稱」欄位中輸入「Exchange Organization Administrators」，並按一下「檢查名稱」。
- 若為 Exchange Server 2010 和 2013，請在「輸入要選取的物件名稱」欄位中輸入「組織管理」，並按一下「檢查名稱」。

e. 按一下「確定」，再按一下確認畫面上的「確定」。

4. 在 Active Directory 伺服器上進行以下設定：

a. 瀏覽至「開始 > 系統管理工具 > Active Directory 使用者和電腦」。

b. 按一下功能表列中的「檢視｜進階功能」。 >

c. 從左側的樹狀結構中展開「使用者」資料夾。

d. 在此程序的步驟 1 第 3-15 頁 中建立的帳號（使用者名稱）上按一下滑鼠右鍵，然後按一下「內容」。

e. 在「安全性」標籤上，按一下「新增」。

f. 將在步驟 1 第 3-15 頁 中建立的使用者名稱和網域名稱（例如：domainname\username）輸入於「輸入要選取的物件名稱」欄位中，並按一下「檢查名稱」，然後按一下「確定」。

g. 選取「群組或使用者名稱」清單中的使用者名稱，再按一下「進階」。

h. 選取「從此物件的父項包括繼承權限」，並按一下「確定」。

i. 按一下「內容」對話方塊上的「確定」。

安裝 MS Exchange 行動安全整合

注意

本主題僅適用於「完整版」部署模式。

注意

您必須在符合以下條件的電腦上安裝「MS Exchange 行動安全整合」：

- 已安裝「Microsoft Exchange 伺服器管理工具」、
- 與 Exchange 伺服器在相同的網域中，以及
- 能夠與「管理伺服器」連線。

程序

1. 登入管理 Web 主控台。
2. 按一下「管理 > Exchange 伺服器整合」。
3. 按一下「按一下這裡以下載」，並將 `ExchangeConnector.zip` 檔案儲存到您的電腦上。
4. 將 `ExchangeConnector.zip` 檔案內容解壓縮，並執行 `ExchangeConnector.exe` 檔。

   「MS Exchange 行動安全整合」安裝精靈隨即顯示。
5. 按一下「歡迎」畫面上的「下一步」。
6. 選取「我接受合約」，然後按一下「下一步」。

安裝程式立即檢查「Microsoft Exchange 管理工具」是否已安裝在電腦上。如果已安裝，安裝程式會顯示下列畫面。

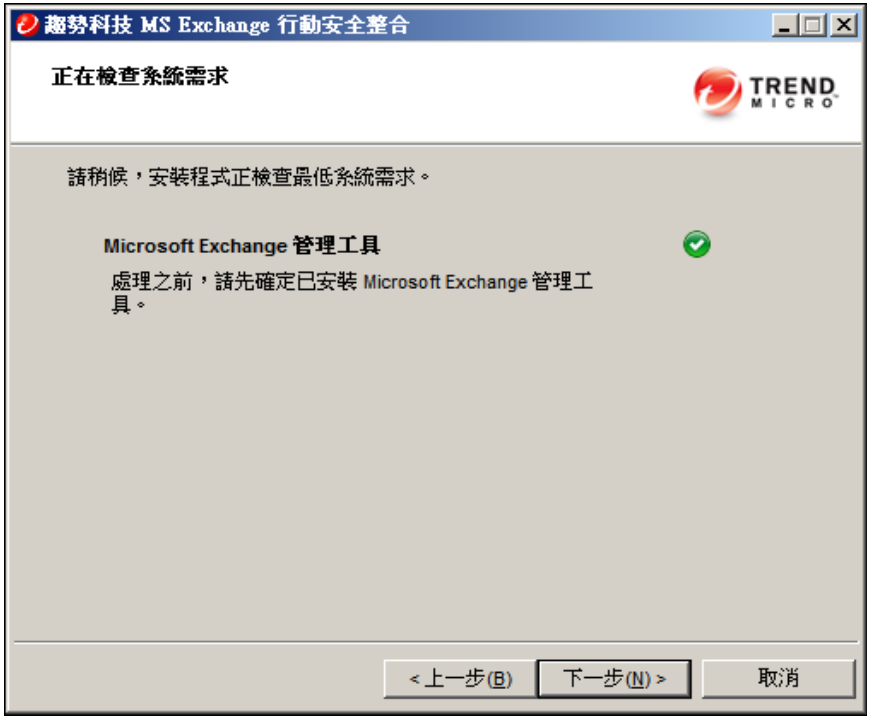

圖 3-8. Exchange 管理安裝檢查成功

7. 按一下「正在檢查系統需求」畫面上的「下一步」。
8. 按一「瀏覽」，並選取您要安裝「MS Exchange 行動安全整合」的目的地資料夾，然後按一下「下一步」。

   「服務帳號」畫面隨即顯示。
9. 輸入用於存取「Exchange 管理工具」的使用者名稱、密碼與網域名稱（您在設定 MS Exchange 行動安全整合的帳號 第 3-15 頁中建立的），並按一下「下一步」。
10. 檢閱「檢閱設定」畫面上的設定，並按一下「安裝」。

安裝程式隨即開始安裝「MS Exchange 行動安全整合」。

11. 安裝完成時，按一下「下一步」，再按一下「完成」。

> **注意**
>
> 從 Exchange 伺服器將行動裝置資訊匯入至「管理伺服器」所需的時間取決於您想要匯入的行動裝置數量。例如，從 Exchange 伺服器將 5000 個行動裝置的資訊匯入至「管理伺服器」約需數小時時間。

接下來需執行的動作

請參閱趨勢科技行動安全防護安裝工作流程 第 3-2 頁中有關其他設定工作的描述。

請參閱設定 Exchange 伺服器整合 第 3-14 頁中有關設定「Exchange 伺服器整合」的下一個工作描述。

更新元件

關於「行動安全防護」升級

「趨勢科技行動安全防護」僅支援從 9.0 版或更新版本升級。

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」—「行動安全防護管理伺服器」和「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，能讓「行動安全防護」偵測這些危險檔案。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。

「趨勢科技行動安全防護」僅支援從 9.0 版或更新版本升級。若從 9.0 之前的版本升級，趨勢科技提供移轉工具，可將資料從舊版移轉到 9.0 版 Patch 1。您接著便可以升級到「行動安全防護 9.7 版 Patch 2」。

如需將舊版資料移轉至 9.7 版 Patch 2 的詳細程序，請參閱以下連結：

http://esupport.trendmicro.com/solution/en-US/1098095.aspx

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 3-22 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。

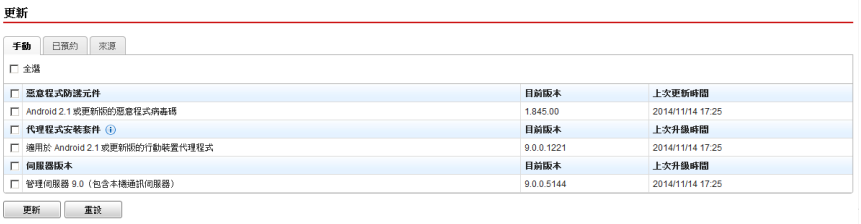

圖 3-9. 「更新」畫面上的「手動」標籤

4. 選取要更新元件的核取方塊。選取「惡意程式防護元件」、「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。

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 3-22 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。

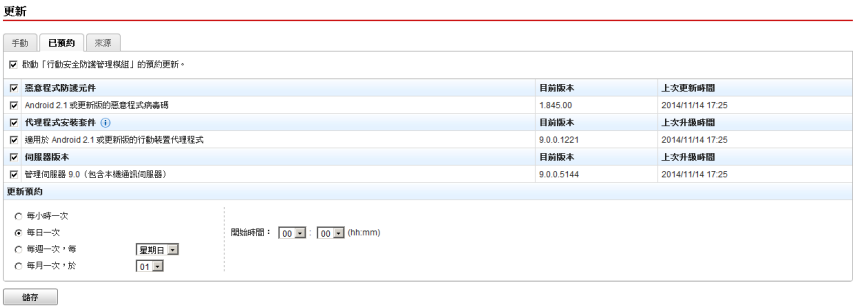

圖 3-10. 「更新」畫面上的「已預約」標籤

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。

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 3-20 頁；如需預約更新的詳細資訊，請參閱預約更新 第 3-21 頁。
3. 按一下「來源」標籤。

圖 3-11. 「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」。

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。

移除伺服器元件

本節引導您逐步完成移除「管理伺服器」和「通訊伺服器」所需執行的步驟。

程序

1. 在 Windows 控制台中按兩下「程式和功能」。

   「解除安裝或變更程式」視窗隨即出現。

2. 選取以下其中一個：
   - 「趨勢科技本機通訊伺服器」— 解除安裝「通訊伺服器」
   - 「趨勢科技行動安全防護」— 解除安裝「管理伺服器」
3. 按一下「解除安裝」。

   對話方塊隨即出現。
4. 在對話方塊中選取「自動關閉應用程式並在安裝完成後嘗試重新啟動」，然後按一下「確定」。

第 4 章

設定伺服器元件

本章可協助系統管理員設定「趨勢科技™企業版行動安全防護 9.7 版 Patch 2」的伺服器元件。

本章包含以下小節：

初始伺服器設定

下表說明「趨勢科技行動安全防護」安裝後的初始伺服器設定。

表 4-1.「行動安全防護」伺服器初始設定

步驟	處理行動	說明
步驟 1	進行資料庫設定。	如需詳細程序，請參閱進行資料庫設定 第 4-5 頁。
步驟 2	進行 Communication Server 設定。	如需詳細程序，請參閱進行一般通訊伺服器設定 第 4-6 頁。
步驟 3	（僅限「完整版」部署模式。） （選用）針對 Android 進行 Communication Server 設定。	如果您不想要管理 Android 行動裝置，可以略過此步驟。 如需詳細程序，請參閱進行 Android 通訊伺服器設定 第 4-8 頁。
步驟 4	（僅限「完整版」部署模式。） （選用）針對 iOS 進行 Communication Server 設定。	如果您不想要管理 iOS 行動裝置，可以略過此步驟。 如需詳細程序，請參閱進行 iOS 通訊伺服器設定 第 4-9 頁。
步驟 5	進行部署模式設定。	如需詳細程序，請參閱進行部署設定 第 4-11 頁。
步驟 6	進行「裝置註冊」設定。	如需詳細程序，請參閱進行裝置註冊設定 第 4-12 頁。
步驟 7	（僅限「完整版」部署模式。） （選用）自訂「行動安全防護使用規範」。	如果您想要使用預設的「行動安全防護使用規範」，可以略過此步驟。 如需詳細程序，請參閱自訂「行動安全防護使用規範」 第 4-14 頁。

步驟	處理行動	說明
步驟 8	（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。） （選用）進行 Active Directory 設定。	如果您不想要從 Active Directory 伺服器匯入使用者，可以略過此步驟。 如需詳細程序，請參閱進行 Active Directory (AD) 設定 第 4-15 頁。
步驟 9	（選用）進行「管理伺服器」設定。	如果您的「管理伺服器」不使用 Proxy 存取網路，且您想要使用預設的伺服器 IP 位址與通訊埠號碼，可以略過此步驟。 如需詳細程序，請參閱進行管理伺服器設定 第 4-16 頁。
步驟 10	（僅限「完整版」部署模式。） （選用）進行「Exchange 伺服器整合」設定。	如果您不想要管理使用 Exchange ActiveSync 的行動裝置，可以略過此步驟。 如需詳細程序，請參閱進行 Exchange 伺服器整合設定 第 4-16 頁。
步驟 11	（選用）進行通知和報告設定。	如果您不想要傳送邀請電子郵件給使用者，可以略過此步驟。 請參閱進行通知和報告設定 第 4-19 頁。
步驟 12	（選用）設定系統管理員通知。	如果您不想要透過電子郵件收到錯誤訊息通知和定期的預約報告，可以略過此步驟。 如需詳細程序，請參閱設定系統管理員通知 第 4-19 頁。
步驟 13	驗證「行動安全防護」設定（建議）。	使用「設定與驗證」畫面驗證「行動安全防護」設定。 如需相關程序，請參閱驗證行動安全防護設定 第 4-20 頁。
步驟 14	變更管理 Web 主控台的系統管理員帳號密碼。	登入管理 Web 主控台後，使用「管理帳號管理」畫面。 請參閱《*管理手冊*》中的＜*編輯系統管理員帳號*＞主題。

注意

您必須完成「行動安全防護」伺服器的初始伺服器設定，才能繼續在行動裝置上安裝「行動裝置代理程式」。

進行資料庫設定

程序

1. 登入管理 Web 主控台。
2. 按一下「管理 > 資料庫設定」。
3. 輸入伺服器名稱或 IP 位址、您的使用者名稱、密碼及資料庫名稱。

   注意

   如果您使用特定的 SQL Server 或 SQL Server Express 通訊埠，請使用以下格式：

   <SQL server name or IP address>,<Port>

4. 按一下「儲存」。

接下來需執行的動作

請參閱初始伺服器設定 第 4-3 頁中下一個組態設定工作的描述。

進行通訊伺服器設定

「通訊伺服器設定」畫面提供下列設定：

- 「一般設定」— 設定「通訊伺服器」的基本設定。
- 「Android 設定」— 設定 Android 行動裝置管理的通知與代理程式自訂設定。

- 「iOS 設定」— 進行 SCEP 設定，並上傳 APN 與 SSL 憑證，以管理 iOS 行動裝置。
- 「Windows Phone 設定」— 設定預約，定義 Windows Phone 行動裝置連線「通訊伺服器」來更新政策設定和指令的頻率。

注意

「Android 設定」、「iOS 設定」和「Windows Phone 設定」只能在「完整版」部署模式下使用。

進行一般通訊伺服器設定

程序

1. 登入管理 Web 主控台。
2. 按一下「管理 > 通訊伺服器設定」。
3. 按一下「一般設定」標籤。
4. 在「通訊伺服器類型」區段下，選取以下兩個選項之一：
   - 「本機通訊伺服器」— 如果您已在您網路的本機安裝「通訊伺服器」。
   - 「雲端通訊伺服器」— 如果您要使用部署在雲端中的「通訊伺服器」。
5. 在「通訊伺服器和行動裝置之間的通訊設定」區段之下，進行以下設定：
   - 「外部網域名稱或 IP 位址」—「本機通訊伺服器」的網域名稱或 IP 位址。
   - 「HTTP 通訊埠」與「HTTPS 通訊埠」—供「本機通訊伺服器」用於與行動裝置通訊。

     預設的 HTTP 與 HTTPS 通訊埠為 8080 與 4343。

注意

如果您設定這兩個通訊埠，則行動裝置將使用 HTTPS 通訊埠與「通訊伺服器」通訊。行動裝置只有在無法使用 HTTPS 通訊埠進行通訊時，才會使用 HTTP 通訊埠。

6. 在「通訊伺服器和管理伺服器之間的通訊設定」區段之下，進行以下設定：

   - 「通訊伺服器名稱或 IP 位址」—「本機通訊伺服器」的網域名稱或 IP 位址。
   - 「HTTPS 通訊埠」—用於「本機通訊伺服器」與「管理伺服器」通訊。

注意

如果您需要自訂 HTTPS 通訊埠，請參閱設定通訊伺服器通訊埠 第 B-4 頁以取得詳細資料。

7. （僅限「完整版」部署模式）在「資訊收集頻率」區段下，進行以下設定：

   - 「資訊收集頻率」— 選取「行動安全防護」收集與行動裝置上所安裝應用程式相關資訊的頻率。
   - 「行動裝置漫遊時的資訊收集頻率」— 選取當行動裝置漫遊時，「行動安全防護」收集與行動裝置上所安裝應用程式相關資訊的頻率。

注意

此設定僅適用於 Android 與 iOS 行動裝置。

「行動安全防護」將在行動裝置註冊時收集行動裝置上所安裝應用程式的相關資訊，然後根據您選取的頻率收集。

變更頻率將會重設計時器。

8. （僅限「完整版」部署模式）如果您想要自動選擇性清除已開放 Root 權限或已破解的行動裝置，請在「偵測已開放 Root 權限/已破解的裝置」區段下選取「若裝置已開放 Root 權限或已破解，請選擇性地清除裝置」。

9. 按一下「儲存」。

接下來需執行的動作

請參閱初始伺服器設定 第 4-3 頁中下一個組態設定工作的描述。

進行 Android 通訊伺服器設定

注意

本主題僅適用於「完整版」部署模式。

程序

1. 登入管理 Web 主控台。
2. 按一下「管理 > 通訊伺服器設定」。
3. 按一下「Android 設定」標籤。
4. 如果您要將推播通知傳送到 Android 行動裝置，請在「推播通知設定」區段下選取「啟動推播通知」。

   注意

   如果您未啟用此設定，Android 行動裝置使用者必須手動更新行動裝置的公司政策。

5. 在「代理程式自訂」區段下，選取「啟動代理程式自訂」可將伺服器 IP 位址和通訊埠號碼加入使用者從「行動安全防護通訊伺服器」下載的 Android 用戶端應用程式中。如果在「裝置註冊設定」中有選取「啟動預設註冊金鑰」選項，則也會自動將預設的「註冊金鑰」新增至 Android 用戶端應用程式。

   這表示，此設定能將伺服器 IP 位址、通訊埠號碼與預設的「註冊金鑰」自動填入用戶端應用程式中，因此使用者不需要手動輸入這些資訊。

6. 如果您要為行動裝置上的系統設定提供密碼防護，請在「系統設定的密碼防護」區段下，選取「啟動系統設定的密碼防護」，然後在「密碼」欄位中輸入密碼。

7. 按一下「儲存」。

接下來需執行的動作

請參閱初始伺服器設定 第 4-3 頁中下一個組態設定工作的描述。

進行 iOS 通訊伺服器設定

注意

本主題僅適用於「完整版」部署模式。

程序

1. 在「行動安全防護」管理 Web 主控台上，移至「管理 > 通訊伺服器設定 > iOS 設定」。

   「iOS 設定」標籤隨即顯示。

2. 在「Apple 推播通知服務 (APNs) 設定」下，進行以下設定：

   - 「憑證類型」：選取您的憑證類型。
   - 「憑證」：從下拉式清單選取 APNs 憑證或上傳新憑證。

3. 在「簡單憑證註冊通訊協定 (SCEP) 設定」下，進行以下設定：

   a. 選取「啟動 SCEP」。

   b. 啟動後，您必須填寫以下資訊：

      - 「SCEP 使用者 URL」：

        http://SCEP_IP/certsrv/mscep

      - 「SCEP 系統管理員 URL」：

Windows Server 2008：

http://SCEP_IP/certsrv/mscep_admin

注意

如需 SCEP 的相關資訊，請參閱行動安全防護系統元件 第 1-5 頁。

4. 在「用戶端資料檔簽署認證」下，進行以下設定：

   - 「用戶端資料檔簽署認證」：從下拉式清單選取簽署認證的憑證或上傳新憑證。

注意

為了在 iOS 行動裝置上設定「行動裝置代理程式」，「行動安全防護」會在行動裝置上安裝「安裝資料檔」。必須提供「用戶端資料檔簽署認證」，才能將「安裝資料檔」的狀態變更為「已驗證」。如果不進行此設定，「安裝資料檔」狀態會顯示為「尚未驗證」。

如果進行此設定，會在行動裝置上將「安裝資料檔」狀態顯示為「已驗證」。

5. 按一下「儲存」。

接下來需執行的動作

請參閱初始伺服器設定 第 4-3 頁中下一個組態設定工作的描述。

進行 Windows Phone 通訊伺服器設定

注意

本主題僅適用於「完整版」部署模式。

程序

1. 登入管理 Web 主控台。
2. 按一下「管理 > 通訊伺服器設定」。

3. 按一下「Windows Phone 設定」標籤。
4. 在「Windows Phone 同步間隔」中設定頻率，定義 Windows Phone 行動裝置連接「行動安全防護通訊伺服器」來更新政策設定和指令的頻率。

進行部署設定

「行動安全防護」允許您與其他 MDM 解決方案進行整合。請使用「部署設定」畫面，以便在以下其中一個模式下部署「行動安全防護」：

- 「完整版」：此選項提供行動裝置管理 (MDM) 與安全掃瞄功能。
- 「安全掃瞄」：此選項僅提供安全掃瞄功能，以及允許與其他行動裝置管理 (MDM) 解決方案進行整合。

程序

1. 在「行動安全防護」管理 Web 主控台上，瀏覽至「管理 > 部署設定」。
2. 在「伺服器」標籤上，選取「行動安全防護」部署模式。
   - 完整版
   - 安全掃瞄，然後從下拉式清單中選取「MDM 解決方案」。

     如果您從「MDM 解決方案」下拉式清單中選取「AirWatch」或「MobileIron」，請設定顯示在畫面上的 AirWatch 或 MobileIron 設定來使其與「行動安全防護」整合。
3. （僅限搭配未列出之 MDM 廠商的「安全掃瞄」部署模式）在「Android 代理程式」標籤上，選取下列其中一個選項：
   - 「從 Google Play 商店下載」— 如果您選取此選項，則使用者必須手動從 Google Play 商店下載並安裝用戶端應用程式。然而，每當行動裝置上的用戶端應用程式在 Google Play 商店上進行更新時，此用戶端應用程式也會自動更新。
   - 「從行動安全防護伺服器下載」— 如果您選取此選項，則使用者可以從通知電子郵件中指定的 URL 進行下載。

您也可以選取「自動註冊」，使用伺服器 IP 位址、通訊埠號碼和預設註冊碼來預先設定用戶端應用程式。

4. （僅限搭配未列出之 MDM 廠商的「安全掃瞄」部署模式）在「iOS 代理程式」標籤上，選取「啟動對 iOS (7.1 或更新版本) 的安全掃瞄支援」，然後遵循畫面上顯示的程序來完成設定。

5. 按一下「儲存」。

進行裝置註冊設定

程序

1. 登入管理 Web 主控台。
2. 按一下「管理 > 裝置註冊設定」。
3. 按一下「驗證」標籤。
4. 在「使用者驗證」區段下，選取以下其中一項：
   - 使用 Active Directory 驗證 — 使用 Active Directory 中的使用者資訊來驗證使用者。
   - 「使用註冊金鑰驗證」 — 使用註冊金鑰來驗證使用者。

     「行動安全防護」將自動產生註冊金鑰，並透過邀請訊息將金鑰傳送給使用者。

     - 「註冊金鑰使用限制」— 選取以下其中一項：
       - 「多次使用」 — 若要讓使用者在註冊多個裝置時使用同一組註冊金鑰，請選取此選項。
       - 「一次使用」 — 若要防止使用者重複使用註冊金鑰，請選取此選項。您將必須向每個需要註冊多個裝置的使用者傳送多份邀請。

- 「註冊金鑰到期剩餘時間」— 如果您想要在某段時間後停止使用自動產生的註冊金鑰，請選取此設定，然後從下拉式清單中選取該段時間。
- 「使用預設註冊金鑰」— 如果您想要手動產生註冊金鑰，請選取此選項，然後按一下「產生」即可產生註冊金鑰。系統不會將此註冊金鑰以邀請訊息傳送給使用者。
- 「註冊金鑰到期日」— 如果您想要在某個日期停止使用手動產生的註冊金鑰，請選取此選項，然後從行事曆選取日期。

注意

僅限在「完整版」部署模式以及搭配未列出之 MDM 廠商的「安全掃瞄」部署模式下，提供「使用 Active Directory 驗證」設定。

5. （僅限「完整版」部署模式）在「裝置驗證」區段下，選取以下其中一項：

- 「關閉此設定」— 停用行動裝置的裝置驗證。
- 「使用 IMEI 或 Wi-Fi MAC 位址驗證」— 此設定可讓您上傳您要驗證的行動裝置清單。

a. 按一下「匯出已允許裝置的清單範本」以下載範本並建立已允許裝置清單。

b. 在您建立清單後，按一下「瀏覽」以選取並匯入您在上個步驟中建立的行動裝置清單。

c. 按一下「檢查資料格式」以驗證已允許裝置清單中的資料格式。驗證後，「行動安全防護」會在「已允許裝置的狀態」清單中顯示所有的行動裝置。

d. 選取以下其中一個選項：

- 「刪除未驗證的裝置」— 刪除已存在於「裝置管理」畫面中，但並不存在於您所匯入的已允許裝置清單之行動裝置。
- 「在未驗證群組中顯示未驗證的裝置」— 將所有已存在於「裝置管理」畫面中，但並不存在於您所匯入的已允許裝置清單中的已註冊行動裝置移動至「未驗證」群組。

注意

如果您使用「裝置驗證」，則「行動安全防護」會根據您使用的已允許裝置清單對所有的行動裝置重新群組。

6. 按一下「儲存」。

接下來需執行的動作

請參閱初始伺服器設定 第 4-3 頁中下一個組態設定工作的描述。

自訂「行動安全防護使用規範」

您可以為要下載、安裝與使用「行動裝置代理程式」的使用者自訂「使用規範」。

程序

1. 登入管理 Web 主控台。
2. 按一下「管理 > 裝置註冊設定」。
3. 在「使用規範自訂」標籤上，按一下「下載使用規範範例」，並將 `Eula_agreement.zip` 檔儲存到您的電腦上。
4. 解壓縮 `Eula_agreement.zip` 檔案內容。
5. 使用 HTML 編輯器開啟 `Eula_agreement.html` 檔案，並視需要進行修改，然後儲存檔案。
6. 在「裝置註冊設定」畫面的「自訂使用規範」標籤上，按一下「瀏覽」，然後選取您在此程序的上一個步驟（步驟 5 第 4-14 頁）中修改的檔案，然後按一下「開啟」。

   「預覽使用規範」隨即更新為所上傳的檔案內容。
7. 按一下「儲存」。

接下來需執行的動作

請參閱初始伺服器設定 第 4-3 頁中下一個組態設定工作的描述。

進行 Active Directory (AD) 設定

注意

本主題僅適用於「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 9.7 版 Patch 2」提供根據 Active Directory (AD) 設定使用者授權的選項。完成設定後，您也將可使用貴公司的 Active Directory 將行動裝置新增至裝置清單。

如果您不想使用 Active Directory 進行使用者驗證，或不想從 Active Directory 新增使用者，即無需進行這項設定。

程序

1. 登入管理 Web 主控台。
2. 按一下「管理 > Active Directory 設定」。
3. 輸入主機名稱或主機 IP 位址、主機通訊埠號碼、您的網域使用者名稱和密碼。
4. 按一下「儲存」。

接下來需執行的動作

請參閱初始伺服器設定 第 4-3 頁中下一個組態設定工作的描述。

進行管理伺服器設定

程序

1. 登入管理 Web 主控台。
2. 按一下「管理 > 管理伺服器設定」。
3. 按一下「連線」標籤，並指定「管理伺服器」名稱或 IP 位址及其通訊埠號碼。「管理伺服器」的預設通訊埠號碼為 443。

   注意

   此畫面上的 IP 位址與通訊埠號碼用於透過網路瀏覽器存取管理 Web 主控台。

4. 如果「管理伺服器」使用 Proxy 伺服器連線至 Internet，請在「Proxy」標籤中指定 Proxy 設定：
   a. 在「Proxy」標籤上，選取「針對管理伺服器使用下列 Proxy 設定」，並指定 Proxy 伺服器名稱或 IP 位址及其通訊埠號碼。
   b. 如果 Proxy 伺服器需要驗證，請在「Proxy 驗證」區段中輸入使用者 ID 與密碼。
5. 按一下「儲存」。

   現在您必須使用新的 IP 位址與通訊埠號碼，才能登入管理 Web 主控台。

接下來需執行的動作

請參閱初始伺服器設定 第 4-3 頁中下一個組態設定工作的描述。

進行 Exchange 伺服器整合設定

注意

本主題僅適用於「完整版」部署模式。

程序

1. 在「行動安全防護」管理 Web 主控台上，移至「管理 > Exchange 伺服器整合」。

   「Exchange 伺服器整合」畫面隨即出現。

2. 在「MS Exchange 行動安全整合」下，選取「啟動此選項以確保僅相容行動裝置可存取 Exchange 伺服器」。

   有關「Exchange 伺服器整合」畫面上顯示的「MS Exchange 行動安全整合」不同狀態，請參閱 MS Exchange 行動安全整合狀態 第 4-18 頁。

3. 在「Exchange 存取控制」下，視需要更新下列項目：

   - 選取「自動封鎖未受管理的裝置存取 Exchange 伺服器」。

     注意

     未向 Mobile Security 伺服器註冊的裝置稱為未受管理的裝置。這包括最近向 Exchange 伺服器註冊的裝置。

   - 選取「允許下列裝置存取公司資料（電子郵件、行事曆、聯絡人等）」，然後選取以下其中一項：

     - 僅健康狀態良好的裝置
     - 健康狀態良好與不相容的裝置

     注意

     請參閱《管理手冊》的＜報表資訊＞主題中有關不同行動裝置註冊狀態的說明。

   - 選取「自動為所有受管理裝置啟動「自動允許/封鎖存取」選項」。

     注意

     啟動此選項會視受管理裝置的狀態，自動允許或封鎖存取 Exchange 伺服器。

- 使用下拉式清單指定天數，封鎖的裝置在過了這段時間後就無法存取 Exchange 伺服器。

4. 按一下「儲存」。

接下來需執行的動作

請參閱初始伺服器設定 第 4-3 頁中下一個組態設定工作的描述。

如需設定「Exchange 伺服器整合」的其他步驟，請參閱設定 Exchange 伺服器整合 第 3-14 頁。

MS Exchange 行動安全整合狀態

注意

本主題僅適用於「完整版」部署模式。

下表列出「Exchange 伺服器整合」畫面上顯示不同的 MS Exchange 行動安全整合狀態。

表 4-2. MS Exchange 行動安全整合狀態

狀態	說明
一般	「MS Exchange 行動安全整合」與「管理伺服器」連線。
正在等待 MS Exchange 行動安全整合	「管理伺服器」正在等待「MS Exchange 行動安全整合」連線至「管理伺服器」。
警告	「MS Exchange 行動安全整合」未與「管理伺服器」連線超過五分鐘。
已中斷連線	「MS Exchange 行動安全整合」未與「管理伺服器」連線超過九分鐘。
已關閉	「MS Exchange 行動安全整合」與「管理伺服器」連線，但在「行動安全防護」的「Exchange 伺服器整合設定」中為關閉。

進行通知和報告設定

您可以設定通知來源將通知電子郵件傳送給系統管理員。

程序

1. 登入管理 Web 主控台。
2. 按一下「通知和報告 > 設定」。
3. 輸入「寄件者」電子郵件地址、SMTP 伺服器 IP 位址及其通訊埠號碼。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。

接下來需執行的動作

請參閱初始伺服器設定 第 4-3 頁中下一個組態設定工作的描述。

如需設定「行動裝置代理程式」的其他步驟，請參閱設定行動裝置代理程式 第 5-3 頁。

設定系統管理員通知

您可以進行系統管理員通知和報告設定，以透過電子郵件接收錯誤訊息通知和定期的預約報告。

程序

1. 登入管理 Web 主控台。
2. 按一下「通知和報告 > 系統管理員通知和報告」。
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。完成時按一下「儲存」，返回「系統管理員通知和報告」畫面。

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。

4. 按一下「儲存」。

接下來需執行的動作

請參閱初始伺服器設定 第 4-3 頁中下一個組態設定工作的描述。

驗證行動安全防護設定

「行動安全防護」提供「設定與驗證」畫面驗證您所設定的所有設定是否正確。

程序

1. 登入管理 Web 主控台。
2. 按一下「管理 > 設定與驗證」。
3. 按一下「驗證行動安全防護設定」。

接下來需執行的動作

請參閱初始伺服器設定 第 4-3 頁中下一個組態設定工作的描述。

第 5 章

處理行動裝置代理程式

本章提供行動裝置需求，以及「行動裝置代理程式」支援的模式，並討論不同平台上不同的行動裝置代理程式部署方法。

本章包含以下小節：

支援的行動裝置和平台

注意

請務必確認行動裝置能透過 Wi-Fi、3G/GPR 或使用主電腦上的網路連線連接「通訊伺服器」。

將「行動安全防護」行動裝置代理程式（亦稱為「行動裝置代理程式」）安裝在行動裝置上之前，請確認行動裝置符合下列需求。

裝置儲存和記憶體

表 5-1. 系統需求

作業系統	記憶體 (MB)	儲存體 (MB)
Android	10	8
iOS	4	3

注意

Windows Phone 行動裝置不需要安裝任何「行動安全防護」用戶端軟體（「行動裝置代理程式」）。

設定行動裝置代理程式

表 5-2. 行動裝置代理程式設定程序

步驟	處理行動	說明	
步驟 1	（選用）設定行動裝置的通知設定。	如果您要使用電子郵件將安裝與註冊詳細資訊傳送給使用者，請執行這些步驟。	如需詳細程序，請參閱進行通知和報告設定 第 4-19 頁。
步驟 2	（選用）設定「行動安全防護」要以電子郵件和／或簡訊傳送給使用者的安裝訊息。		安裝訊息包含使用者存取以下載與安裝 MDA 設定套件的 URL。 如需詳細程序，請參閱設定安裝訊息 第 5-3 頁。
步驟 3	（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。） （選用）將邀請傳送給使用者。		如需詳細程序，請參閱邀請使用者註冊 第 5-4 頁。
步驟 4	在行動裝置上安裝 MDA。	如需詳細程序，請參閱在行動裝置上安裝 MDA 第 5-8 頁。	
步驟 5	向「行動安全防護管理伺服器」註冊 MDA。	如需詳細程序，請參閱向行動安全防護管理伺服器註冊 MDA 第 5-16 頁。	

設定伺服器的邀請訊息功能（選用）

您可以設定邀請訊息，以使用電子郵件將安裝與註冊詳細資訊傳送給使用者。

如果您不想要使用邀請訊息傳送 MDA 安裝與註冊資訊，可略過本節。

設定安裝訊息

使用「安裝訊息」畫面來輸入要顯示的訊息。

此作業是設定「行動裝置代理程式」程序中的一個步驟。

請參閱設定行動裝置代理程式 第 5-3 頁。

程序

1. 登入管理 Web 主控台。
2. 按一下「通知和報告 > 使用者通知」。
3. 按一下「行動裝置註冊」文字以開啟「行動裝置註冊組態設定」畫面。
4. 檢查相關文字方塊中的預設主旨、電子郵件及/或簡訊，並視需要修改。

   注意

   編輯「訊息」欄位時，若您包含 Token 變數 `<%DOWNLOADURL%>`，該變數會取代為實際的 URL，可讓使用者從伺服器下載 Mobile Device Agent 安裝檔案。

   例如：`<a href=<%DOWNLOADURL%>><%DOWNLOADURL%></a>`

   注意

   電子郵件通知只會傳送供下載用戶端安裝檔的下載連結，不會自動將伺服器 IP 位址和通訊埠號碼填入註冊畫面。

5. 按一下「儲存」。
6. 按一下「通知和報告 > 使用者通知」。
7. 選取「行動裝置註冊」，並按一下「儲存」。

邀請使用者註冊

注意

本主題僅適用於「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。

此作業是設定 Mobile Device Agent 程序中的一個步驟。

請參閱設定行動裝置代理程式 第 5-3 頁。

程序

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. 在「使用者」標籤上，按一下「邀請使用者」，然後選取下列其中一個選項。

方法	說明
手動邀請使用者	此方法可讓您透過填寫表單來逐一新增使用者資訊。 如需詳細資訊，請參閱手動邀請使用者 第 5-5 頁。
從 CSV 檔案邀請使用者	此選項可讓您從 CSV 檔案中複製並貼上使用者資訊。 如需詳細資訊，請參閱從 CSV 檔案邀請使用者 第 5-6 頁。
從 Active Directory 邀請使用者	此方法可讓您從 Active Directory 中選取使用者。 如需詳細資訊，請參閱從 Active Directory 邀請使用者 第 5-7 頁。

手動邀請使用者

使用此選項，您可以使用表單逐一新增使用者資訊來邀請使用者。

程序

1. 在「行動安全防護」管理 Web 主控台上，移至「使用者 > 邀請使用者 > 手動」。

「手動邀請使用者」畫面隨即出現。

2. 在「手動邀請使用者」視窗中填寫以下欄位。

   - 電話號碼 — 輸入與使用者相關聯的電話號碼。
   - 「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 — 輸入可用以在裝置樹狀結構中識別裝置的使用者名稱。
   - 群組 — 從下拉式清單中選取群組。

   秘訣

   您稍後可以從「裝置」畫面中，為使用者重新指派至其他群組。

3. 若要邀請更多使用者，請按一下 ⊞ 按鈕，然後重複步驟 2。

4. 按一下「儲存」。

   隨即出現確認訊息。

從 CSV 檔案邀請使用者

此選項可讓您從使用了必要資料格式的 CSV 檔案中，複製使用者資訊。「行動安全防護」會自動偵測並轉換資料來填寫使用者資訊表單。

程序

1. 在「行動安全防護」管理 Web 主控台上，移至「使用者 > 邀請使用者 > 從 CSV」。

   「從 CSV 邀請使用者」畫面隨即出現。

2. 在文字方塊中，使用下列格式輸入使用者資訊：

   電話號碼 1, 電子郵件 1, 使用者名稱 1, 群組名稱 1;

注意

使用分號 (;) 或分行符號分隔每個使用者的資訊。

3. 按一下「驗證」以驗證資訊是否遵循指定格式。

   隨即有快顯訊息顯示驗證結果。

注意

如果格式不正確，請修正錯誤然後再試一次。

4. 按一下「儲存」。

   隨即出現確認訊息。

從 Active Directory 邀請使用者

注意

本主題僅適用於「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。

此選項可讓您從 Active Directory 中選取使用者或群組。

程序

1. 在「行動安全防護」管理 Web 主控台上，移至「使用者 > 邀請使用者 > 從 Active Directory」。

   「從 Active Directory 邀請使用者」畫面隨即出現。

2. 在提供的搜尋欄位中輸入使用者資訊，然後按一下「搜尋」。

3. 從搜尋結果選取使用者或群組，然後按一下「邀請」。

   邀請清單會顯示已選取的使用者。

注意

如果您選取群組，則邀請清單會顯示屬於該群組的所有使用者。

4. 若要手動將使用者新增到邀請清單，請按一下「處理行動」欄中的「新增」按鈕 (+)。若要刪除使用者，請按一下「刪除」按鈕 (-)。
5. 若要將第一個使用者的群組設定套用到所有使用者，請完成以下步驟：
   a. 從第一個使用者的「群組」下拉式清單中選取選項。
   b. 按一下「全部套用」。
   c. 按一下「確定」。
6. 按一下「儲存」。

   隨即出現確認訊息。

在行動裝置上安裝 MDA

此作業是設定「行動裝置代理程式」程序中的一個步驟。

請參閱設定行動裝置代理程式 第 5-3 頁。

iOS 行動裝置

程序

1. 執行您的行動安全防護 iOS 應用程式版本所適用的安裝步驟。
   - 完整版
     a. 移至 Apple 商店，搜尋應用程式「Trend Micro ENT Security」。
     b. 點選「安裝」。
   - 僅有安全掃瞄功能

a. 移至邀請電子郵件中指定的下載 URL。

b. 下載並安裝行動安全防護 iOS 應用程式。

2. 若要開始使用「行動安全防護」，您必須先執行下列步驟。

a. 在您的 iOS 裝置上，移至「一般 > 資料檔與裝置管理」。

b. 點選「Trend Micro Incorporate (Ent)」。

c. 點選「信任「Trend Micro Incorporate (Ent)」」。

Android 行動裝置

您可以使用下列其中一個方法為 Android 行動裝置安裝 MDA：

- 安裝方法 I — 從 Google Play 商店下載 MDA 並直接安裝在行動裝置上。在 Google Play 中搜尋「趨勢科技企業版行動安全防護」，然後從 Trend Micro 下載並安裝「企業版行動安全防護」應用程式。
- 安裝方法 II — 從「管理伺服器」下載 MDA 並直接安裝在行動裝置上。如需相關程序，請參閱安裝方法 II 第 5-10 頁。
- 安裝方法 III — 使用網路瀏覽器將 MDA 安裝套件下載到電腦上，再傳輸到行動裝置並進行安裝。如需相關程序，請參閱安裝方法 III 第 5-11 頁。
- 安裝方法 IV — 使用「行動裝置管理」主控台將 MDA 安裝套件下載到電腦上，再傳輸到行動裝置並進行安裝。如需相關程序，請參閱安裝方法 IV 第 5-12 頁。

傳送給使用者的預設邀請電子郵件會指示使用者從 Google Play 商店下載並安裝 MDA 應用程式 (方法 I)。如果您想要使用者使用其他方法安裝應用程式，請修改傳送給使用者的邀請電子郵件。請參閱《管理手冊》中的＜設定使用者通知＞主題。

安裝方法 I

此方法可讓您從 Google Play 商店下載 MDA 並直接安裝在行動裝置上。

如需其他方法，請參閱 Android 行動裝置 第 5-9 頁。

程序

1. 在行動裝置上，開啟「Google Play 商店」。
2. 搜尋「趨勢科技企業版行動安全防護」，然後從搜尋結果中點選「企業版行動安全防護」。
3. 點選「安裝」，然後點選「接受」以開始安裝程序。

   在安裝程序完成後，點選「開啟」啟動應用程式。

安裝方法 II

此方法可讓您從「Mobile Security 管理伺服器」下載 MDA 並直接安裝在行動裝置上。

如需其他方法，請參閱 Android 行動裝置 第 5-9 頁。

程序

1. 請執行以下任一項工作：
   - 如果您正在使用「本機通訊伺服器」或「雲端通訊伺服器」，請開啟來自「行動安全防護」的簡訊或電子郵件，並在您要安裝 MDA 的行動裝置上存取 URL，以下載安裝套件。
   - 如果您使用的是「本機通訊伺服器」，請使用您要安裝 MDA 之行動裝置上的網路瀏覽器存取以下其中一個 URL，以下載安裝套件：

     ```
     http://External_domain_name_or_IP_address:HTTP_port/
     mobile
     ```

     或

     ```
     https://External_domain_name_or_IP_address:HTTPS_port/
     mobile
     ```

注意

- 依照您在「管理 > 通訊伺服器設定 > 一般設定 > 通訊伺服器和行動裝置之間的通訊設定」中設定的內容，取代 External_domain_name_or_IP_address、HTTP_port 和 HTTPS_port。
- 如果使用 HTTPS 下載「行動裝置代理程式」，您必須設定公用憑證。如需詳細資料，請參閱以下 URL：

  http://esupport.trendmicro.com/solution/en-us/1106466.aspx

2. 如果安裝未自動啟動，請啟動安裝套件並完成安裝。

安裝方法 III

如果您正在使用「本機通訊伺服器」，則此方法可讓您使用網路瀏覽器將 MDA 安裝套件下載到電腦上，再傳輸到行動裝置並進行安裝。

如需其他方法，請參閱 Android 行動裝置 第 5-9 頁。

程序

1. 在電腦上，瀏覽至下列其中一個 URL，以下載安裝套件：

   ```
   http://External_domain_name_or_IP_address:HTTP_port/mobile
   ```

   或

   ```
   https://External_domain_name_or_IP_address:HTTPS_port/
   mobile
   ```

   注意

   - 使用指定給 External_domain_name_or_IP_address、HTTP_port 和 HTTPS_port 的值。若要查看這些值，請移至「管理 > 通訊伺服器設定 > 一般設定 > 通訊伺服器和行動裝置之間的通訊設定」。
   - 如果使用 HTTPS 下載「行動裝置代理程式」，您必須設定公用憑證。如需詳細資料，請參閱以下 URL：

     http://esupport.trendmicro.com/solution/en-us/1106466.aspx

2. 選取行動裝置的作業系統以下載安裝套件。
3. 將安裝套件複製到行動裝置。
4. 啟動安裝套件並完成安裝。

安裝方法 IV

本主題僅適用於「完整版」部署模式。

此方法可讓您使用管理 Web 主控台將 MDA 安裝套件下載到電腦上，再傳輸到行動裝置並進行安裝。

如需其他方法，請參閱 Android 行動裝置 第 5-9 頁。

程序

1. 登入管理 Web 主控台。
2. 按一下「管理 > 裝置註冊設定」。
3. 在「代理程式安裝」標籤上，選取代理程式安裝套件，並按一下「下載」將 ZIP 檔案下載到您的電腦上。
4. 將 ZIP 檔案解壓縮，並將安裝套件複製到行動裝置。
5. 啟動安裝套件並完成安裝。

Windows Phone 行動裝置

本主題僅適用於「完整版」部署模式。

您可以使用「本機通訊伺服器」位址來註冊 Windows Phone 行動裝置：

注意

「行動安全防護」不支援 Windows Phone 使用 Cloud Communication Server。

「行動安全防護」需要公開簽署的 SSL 接聽程式憑證，才能註冊 Windows Phone 10 行動裝置。

註冊 Windows Phone 8.0

注意

本主題僅適用於「完整版」部署模式。

程序

1. 在主畫面上點選「設定」圖示。
2. 點選公司應用程式。
3. 在「公司應用程式」畫面中點選「新增帳號」，然後輸入以下資訊：
   - 「電子郵件地址」：您的公司電子郵件地址
   - 「密碼」：您的網域帳號密碼或註冊碼
4. 點選「登入」。
5. 在下一個畫面中輸入以下資訊：
   - 「使用者名稱」：如果您使用 Active Directory 進行註冊，請輸入網域帳號使用者名稱；如果您使用註冊碼，請將此欄位保留空白。
   - 「網域」：如果您使用 Active Directory 進行註冊，請輸入帳號網域的名稱；如果您使用註冊碼，請將此欄位保留空白。
   - 「伺服器」：<ip_address:port>/mobile.

   注意

   請將 <ip_address:port> 取代為伺服器 IP 位址和通訊埠號碼。
6. 點選「登入」。

7. 如果出現「憑證問題」訊息，請點選「繼續」。
8. 如果出現「建立新密碼」畫面，請點選「設定」，接著在「新密碼」和「確認密碼」等欄位中輸入新密碼，然後點選「完成」。
9. 在「帳號已加入」畫面中點選「完成」。

註冊 Windows Phone 8.1

注意

本主題僅適用於「完整版」部署模式。

程序

1. 在主畫面上點選「設定」。
2. 點選「工作地點」。
3. 在「工作地點」畫面中點選「新增帳號」，接著輸入電子郵件地址，然後點選「登入」。
4. 在下一個畫面的「伺服器」欄位輸入以下資訊：<ip_address:port>/mobile，然後點選「登入」。

   注意

   請將 <ip_address:port> 取代為伺服器 IP 位址和通訊埠號碼。

5. 如果出現「憑證問題」訊息，請按一下「繼續」。
6. 在下一個畫面中輸入以下資訊：
   - 「密碼」：您的網域帳號密碼或註冊碼。
   - 「使用者名稱」：如果您使用 Active Directory 進行註冊，請輸入網域帳號使用者名稱；如果您使用註冊碼，請將此欄位保留空白。
   - 「網域」：如果您使用 Active Directory 進行註冊，請輸入帳號網域的名稱；如果您使用註冊碼，請將此欄位保留空白。

7. 點選「登入」。
8. 如果出現「建立新密碼」畫面，請點選「設定」，接著在「新密碼」和「確認密碼」等欄位中輸入新密碼，然後點選「完成」。
9. 在「帳號已加入」畫面中點選「完成」。

註冊 Windows Phone 10

注意

本主題僅適用於「完整版」部署模式。

程序

1. 在主畫面上點選「設定」。
2. 點選「帳戶」，然後選取「存取公司或學校資源」。
3. 在「連線至公司或學校帳戶」畫面，點選「連線」，在「電子郵件地址」欄位輸入您的公司電子郵件地址，然後點選「下一步」。
4. 在下一個畫面輸入下列資訊。
   - 「電子郵件地址」：您的公司電子郵件地址
   - 「伺服器」：<ip_address:port>/mobile
5. 點選「下一步」。
6. 在下一個畫面輸入下列資訊：
   - 「網域」:如果您使用 Active Directory 進行註冊，請輸入帳號網域的名稱；如果您使用註冊碼，則 Active Directory 帳號為選填。
   - 「密碼」：您的網域帳號密碼或註冊碼
7. 點選「下一步」。
8. 在「您已就緒」畫面，點選「完成」。

向行動安全防護管理伺服器註冊 MDA

如果您手動安裝 MDA 或當自動註冊程序不成功時，您需要手動向「行動安全防護」註冊 MDA。

此作業是設定「行動裝置代理程式」程序中的一個步驟。

Android 行動裝置

您可以使用下列其中一種方法註冊 MDA：

- 使用 QR 碼註冊。

  如果您正在使用「本機通訊伺服器」或「雲端通訊伺服器」，請使用此方法。

- 使用伺服器位址註冊。

  如果您正在使用「本機通訊伺服器」，請使用此方法。

- 不使用伺服器位址註冊。

  如果您正在使用「雲端通訊伺服器」，請使用此方法。

使用 QR 碼註冊

程序

1. 在行動裝置上啟動「行動裝置代理程式」。
2. 點選「使用 QR 碼註冊」。
3. 在電腦或其他行動裝置上開啟電子郵件邀請，然後使用行動裝置的相機掃瞄電子郵件邀請裡的 QR 碼。
4. 若有需要，請在提供的欄位中輸入使用者名稱和密碼，然後點選「確定」。

系統將向「行動安全防護管理伺服器」註冊「行動裝置代理程式」。

使用伺服器位址註冊

程序

1. 在行動裝置上啟動「行動裝置代理程式」。
2. 點選「手動註冊」。
3. 點選「本機伺服器」標籤、在相關欄位中輸入伺服器位址以及通訊埠號碼，然後點選「下一步」。
4. 在相關欄位中輸入註冊金鑰或使用者名稱和密碼，然後點選「下一步」。

   系統將向「行動安全防護管理伺服器」註冊「行動裝置代理程式」。

不使用伺服器位址註冊

程序

1. 在行動裝置上啟動「行動裝置代理程式」。
2. 點選「手動註冊」。
3. 點選「雲端伺服器」標籤，輸入邀請電子郵件中的「註冊金鑰」，然後點選「下一步」。

   系統將向「行動安全防護管理伺服器」註冊「行動裝置代理程式」。

iOS 行動裝置

若要從「行動安全防護管理伺服器」管理 iOS 行動裝置，您必須在行動裝置上安裝佈建資料檔。此佈建資料檔必須要能識別您（藉由開發憑證）和您的裝置（藉由列出唯一的裝置識別碼）。

警告!

您必須為 iOS 行動裝置上的 Safari 啟動 JavaScript 才能進行註冊。否則註冊將不會成功。

您可以使用下列其中一種方法註冊 MDA：

- 使用 QR 碼註冊。

  如果您正在使用「本機通訊伺服器」或「雲端通訊伺服器」，請使用此方法。

- 使用伺服器位址註冊。

  如果您正在使用「本機通訊伺服器」，請使用此方法。

- 不使用伺服器位址註冊。

  如果您正在使用 Cloud Communication Server，請使用此方法。

使用 QR 碼註冊

程序

1. 在行動裝置上啟動「行動裝置代理程式」。
2. 點選「使用 QR 碼註冊」。
3. 在電腦或其他行動裝置上開啟電子郵件邀請，然後使用行動裝置的相機掃瞄電子郵件邀請裡的 QR 碼。

   注意

   可能會出現一個對話方塊，要求您安裝針對「本機通訊伺服器」設定的「根 CA」。如果您沒有看到此對話方塊，請略過步驟 4 到步驟 6，直接執行步驟 7。

4. 點選「確定」。

   TMMSMDM-CA 的「安裝資料檔」畫面隨即出現。

5. 在「安裝設定檔」畫面上，點選「安裝」，然後在「警告」畫面上點選「安裝」。
6. 資料檔安裝完成後，按一下「已安裝資料檔」畫面中的「完成」。
7. 視需要在提供的欄位中輸入使用者名稱和密碼，並點選「登入」。

   「MDM 註冊設定檔」的「安裝資料檔」畫面隨即出現。
8. 點選「安裝資料檔」畫面中的「安裝」，然後點選確認快顯對話方塊中的「立即安裝」。
9. 如果行動裝置需要密碼，請在出現的「輸入密碼」畫面中輸入密碼，然後點選「完成」。

   「安裝資料檔」畫面隨即出現。
10. 點選「警告」確認畫面中的「安裝」。

    資料檔安裝程序隨即開始。資料檔安裝程序完成後，便會顯示「已安裝資料檔」畫面。
11. 點選「完成」。

使用伺服器位址註冊

程序

1. 在行動裝置上啟動「行動裝置代理程式」。
2. 點選「手動註冊」。
3. 在「本機伺服器」標籤上，輸入伺服器位址和通訊埠號碼，然後點選「註冊」。
4. 輸入註冊金鑰或使用者名稱和密碼，然後點選「下一步」。

   可能會出現一個對話方塊，要求您安裝針對「本機通訊伺服器」設定的「根 CA」。如果您沒有看到此對話方塊，請略過步驟 5 到步驟 7，直接執行步驟 8。
5. 按一下「確定」。

TMMSMDM-CA 的「安裝資料檔」畫面隨即出現。

6. 在「安裝資料檔」畫面上，點選「安裝」。
7. 如果行動裝置需要密碼，請在出現的「輸入密碼」畫面中輸入密碼，然後點選「完成」。
8. 在出現的「警告」畫面上，點選「安裝」。

   「安裝資料檔」確認訊息隨即出現。
9. 點選「安裝」。
10. 在安裝資料檔後，點選「完成」。

    「MDM 註冊資料檔」適用的「安裝資料檔」畫面隨即出現。
11. 點選「安裝」。
12. 如果行動裝置需要密碼，請在出現的「輸入密碼」畫面中輸入密碼，然後點選「完成」。
13. 在出現的「警告」畫面上，點選「安裝」。

    「遠端管理」確認訊息隨即出現。
14. 點選「信任」。
15. 在安裝資料檔後，點選「完成」。

不使用伺服器位址註冊

程序

1. 在行動裝置上啟動「行動裝置代理程式」。
2. 點選「手動註冊」。
3. 在「雲端伺服器」標籤，輸入驗證代碼並點選「註冊」。

   「MDM 註冊設定檔」的「安裝資料檔」畫面隨即出現。

4. 點選「安裝資料檔」畫面中的「安裝」，然後點選確認快顯對話方塊中的「立即安裝」。
5. 如果行動裝置需要密碼，請在出現的「輸入密碼」畫面中輸入密碼，然後點選「完成」。

   「安裝資料檔」畫面隨即出現。
6. 點選「警告」確認畫面中的「安裝」。

   資料檔安裝程序隨即開始。資料檔安裝程序完成後，便會顯示「已安裝資料檔」畫面。
7. 點選「完成」。

Windows Phone 行動裝置

本主題僅適用於「完整版」部署模式。

您可以使用「本機通訊伺服器」位址來註冊 Windows Phone 行動裝置：

注意

「行動安全防護」不支援 Windows Phone 使用 Cloud Communication Server。

「行動安全防護」需要公開簽署的 SSL 接聽程式憑證，才能註冊 Windows Phone 10 行動裝置。

註冊 Windows Phone 8.0

注意

本主題僅適用於「完整版」部署模式。

程序

1. 在主畫面上點選「設定」圖示。
2. 點選公司應用程式。

3. 在「公司應用程式」畫面中點選「新增帳號」，然後輸入以下資訊：
   - 「電子郵件地址」：您的公司電子郵件地址
   - 「密碼」：您的網域帳號密碼或註冊碼
4. 點選「登入」。
5. 在下一個畫面中輸入以下資訊：
   - 「使用者名稱」：如果您使用 Active Directory 進行註冊，請輸入網域帳號使用者名稱；如果您使用註冊碼，請將此欄位保留空白。
   - 「網域」：如果您使用 Active Directory 進行註冊，請輸入帳號網域的名稱；如果您使用註冊碼，請將此欄位保留空白。
   - 「伺服器」：<ip_address:port>/mobile.

   注意

   請將 <ip_address:port> 取代為伺服器 IP 位址和通訊埠號碼。
6. 點選「登入」。
7. 如果出現「憑證問題」訊息，請點選「繼續」。
8. 如果出現「建立新密碼」畫面，請點選「設定」，接著在「新密碼」和「確認密碼」等欄位中輸入新密碼，然後點選「完成」。
9. 在「帳號已加入」畫面中點選「完成」。

註冊 Windows Phone 8.1

注意

本主題僅適用於「完整版」部署模式。

程序

1. 在主畫面上點選「設定」。

2. 點選「工作地點」。
3. 在「工作地點」畫面中點選「新增帳號」，接著輸入電子郵件地址，然後點選「登入」。
4. 在下一個畫面的「伺服器」欄位輸入以下資訊：<ip_address:port>/mobile，然後點選「登入」。

> **注意**
> 請將 <ip_address:port> 取代為伺服器 IP 位址和通訊埠號碼。

5. 如果出現「憑證問題」訊息，請按一下「繼續」。
6. 在下一個畫面中輸入以下資訊：
   - 「密碼」：您的網域帳號密碼或註冊碼。
   - 「使用者名稱」：如果您使用 Active Directory 進行註冊，請輸入網域帳號使用者名稱；如果您使用註冊碼，請將此欄位保留空白。
   - 「網域」：如果您使用 Active Directory 進行註冊，請輸入帳號網域的名稱；如果您使用註冊碼，請將此欄位保留空白。
7. 點選「登入」。
8. 如果出現「建立新密碼」畫面，請點選「設定」，接著在「新密碼」和「確認密碼」等欄位中輸入新密碼，然後點選「完成」。
9. 在「帳號已加入」畫面中點選「完成」。

在行動裝置上升級 MDA

升級「Mobile Security 管理伺服器」之後，執行下列程序以在行動裝置上升級 MDA。

Android 行動裝置

在「行動安全防護管理伺服器」升級後，該伺服器會將升級通知自動傳送至 Android 行動裝置。

程序

1. 在 Android 行動裝置上，點選從伺服器收到的升級通知。
2. 點選快顯視窗訊息中的「確定」，以啟動升級。

iOS 行動裝置

當 iTunes 商店中有新版本可用時，會將升級通知自動傳送至 iOS 行動裝置。

程序

1. 在 iOS 行動裝置上開啟「應用程式商店」。
2. 點選「更新」。
3. 點選「企業行動安全」應用程式後的「更新」，以啟動更新。

Windows 行動裝置

Windows 行動裝置不需要使用 MDA 來連線至「Mobile Security 管理伺服器」。因此，無須升級 Windows 行動裝置。

附錄 A

網路通訊埠組態設定

本附錄提供在安裝「趨勢科技行動安全防護」時所需的所有網路通訊埠設定。

本附錄包含以下小節：

含雲端通訊伺服器的強化安全模式網路通訊埠設定

如果您使用的是含「雲端通訊伺服器」的強化安全模式（雙伺服器安裝），請針對「行動安全防護」元件設定以下網路通訊埠：

元件	網路通訊埠	詳細資訊

管理伺服器	開啟以下通訊埠：
	• 針對以下項目開啟 HTTPS 連接埠 443：
	  • 「管理伺服器」的內送連線。
	  • 如果您想要從 Google Play 新增外部應用程式。
	  Google Play 商店的主機名稱為：play.google.com.
	  • 如果您想要運用趨勢科技的行動應用程式信譽評等服務 (MARS)，以及查看上傳之 APK 檔案的安全資訊。
	  MARS 伺服器的主機名稱為：rest.mars.trendmicro.com
	注意
	這是預設的 HTTPS 通訊埠號碼。如果您要變更供「管理伺服器」使用的 HTTPS 通訊埠號碼，請參閱進行管理伺服器設定 第 4-16 頁以取得詳細資訊。
	• 針對以下項目開啟 HTTP 連接埠 80：
	  • 授權伺服器
	  授權伺服器的主機名稱為：licenseupdate.trendmicro.com
		用於存取「行動安全防護」管理 Web 主控台。

元件	網路通訊埠	詳細資訊
	• 如果您將趨勢科技主動式更新伺服器當做更新來源。 主動式更新伺服器的主機名稱為 mobilesecurity.activeupdate.trendmicro.com。	
管理伺服器	開啟以下通訊埠： • 針對以下項目開啟 HTTP 連接埠 80 和 HTTPS 連接埠 443： • 前往雲端通訊服務的外送連線 • 如果您想要從 Apple 應用程式商店新增外部 iOS 應用程式 Apple 應用程式商店的主機名稱為：itunes.apple.com. • 如果您想要針對 iOS 行動裝置使用目錄式應用程式控制 在防火牆例外中新增以下兩部雲端通訊服務主機： • ccs.trendmicro.com • ccs01.trendmicro.com • ccs02.trendmicro.com	用於存取「行動安全防護」管理 Web 主控台。
簡單憑證註冊通訊協定 (SCEP) 伺服器	針對通訊伺服器和 iOS 行動裝置開啟 HTTP 通訊埠 80。	（僅限「完整版」部署模式。） 用於 iOS 行動裝置註冊。 如果您未使用 SCEP 伺服器來管理 iOS 行動裝置，即不需要此通訊埠。
SQL Server	開啟以下通訊埠： • 針對「管理伺服器」開啟 TCP 通訊埠 1433。	建立「管理伺服器」與遠端 SQL Server 之間的連線。

元件	網路通訊埠	詳細資訊
	• 針對「管理伺服器」開啟 UDP 通訊埠 1434。 注意 此通訊埠是用來連接 SQL Server 的預設 TCP 通訊埠。不過，如果需要，您也可以將不同通訊埠用於 SQL Server。	

含本機通訊伺服器的強化安全模式網路通訊埠設定

如果您使用的是含「本機通訊伺服器」的強化安全模式（雙伺服器安裝），請針對「行動安全防護」元件設定以下網路通訊埠：

元件	網路通訊埠	詳細資訊

管理伺服器	開啟以下通訊埠：
	• 針對以下項目開啟 HTTPS 連接埠 443：
	  • 「管理伺服器」的內送連線。
	  • 如果您想要從 Google Play 新增外部應用程式。
	
	Google Play 商店的主機名稱為：play.google.com.
	  • 如果您想要運用趨勢科技的行動應用程式信譽評等服務 (MARS)，以及查看上傳之 APK 檔案的安全資訊。
	
	MARS 伺服器的主機名稱為：rest.mars.trendmicro.com
		用於存取「行動安全防護」管理 Web 主控台。

元件	網路通訊埠	詳細資訊
	注意 這是預設的 HTTPS 通訊埠號碼。如果您要變更供「管理伺服器」使用的 HTTPS 通訊埠號碼，請參閱進行管理伺服器設定 第 4-16 頁以取得詳細資訊。 • 針對以下項目開啟 HTTP 連接埠 80： • 授權伺服器 授權伺服器的主機名稱為：licenseupdate.trendmicro.com • 如果您將趨勢科技主動式更新伺服器當做更新來源。 主動式更新伺服器的主機名稱為 mobilesecurity.activeupdate.trendmicro.com。	
管理伺服器	開啟以下通訊埠： • 針對以下項目開啟 HTTP 連接埠 80 和 HTTPS 連接埠 443： • 如果您想要從 Apple 應用程式商店新增外部 iOS 應用程式 Apple 應用程式商店的主機名稱為：itunes.apple.com. • 如果您想要針對 iOS 行動裝置使用目錄式應用程式控制	用於存取「行動安全防護」管理 Web 主控台。
通訊伺服器	開啟 HTTP 通訊埠 8080。	用於行動裝置與 Communication Server 之間的通訊。

元件	網路通訊埠	詳細資訊
	注意 此通訊埠是雙重伺服器組態設定的預設 HTTP 通訊埠號碼。如果您要變更供行動裝置於安裝期間用於與通訊伺服器通訊的 HTTP 通訊埠號碼，請參閱進行一般通訊伺服器設定 第 4-6 頁以取得詳細資訊。	
	開啟 HTTPS 通訊埠 4343。 注意 此通訊埠是雙重伺服器組態設定的預設 HTTPS 通訊埠號碼。	用於行動裝置與 Communication Server 之間的安全通訊。
	針對「Apple 推播通知服務」(APNs) 伺服器開啟 TCP 通訊埠 2195。Apple 推播通知服務的主機名稱為 `gateway.push.apple.com`。	使 Apple 的 APNs 伺服器得以管理 iOS 行動裝置。 如果您未使用 APNs 伺服器來管理 iOS 行動裝置，即不需要此通訊埠。
	開啟 TCP 通訊埠 4343。這是預設的通訊埠，允許從「管理伺服器」到「通訊伺服器」的內送連線。如果您要變更供行動裝置於安裝期間用於與通訊伺服器通訊的 HTTP 通訊埠號碼，請參閱進行一般通訊伺服器設定 第 4-6 頁以取得詳細資訊。	建立「管理伺服器」與 Communication Server 之間的連線。
	開啟 TCP 通訊埠 443。	建立「本機通訊伺服器」與 Cloud Communication Server 之間的連線。
Active Directory	開啟以下任一通訊埠： • 針對 管理伺服器開啟 TCP 通訊埠 389（網域控制器）	用於使用 Active Directory 進行使用者驗證。 如果您未使用 Active Directory 驗證或匯入使

元件	網路通訊埠	詳細資訊
	• 針對 管理伺服器開啟 TCP 通訊埠 3268（全域類別）	用者，即不需要此通訊埠。
簡單憑證註冊通訊協定 (SCEP) 伺服器	針對通訊伺服器和 iOS 行動裝置開啟 HTTP 通訊埠 80。	用於 iOS 行動裝置註冊。 如果您未使用 SCEP 伺服器來管理 iOS 行動裝置，即不需要此通訊埠。
SQL Server	開啟以下通訊埠： • 針對 管理伺服器開啟 TCP 通訊埠 1433 • 針對 管理伺服器開啟 UDP 通訊埠 1434 注意 TCP 通訊埠 1433 是用來連接 SQL Server 的預設通訊埠。不過，如果需要，您也可以將不同 TCP 通訊埠用於 SQL Server。	利用遠端 SQL Server 建立「通信伺服器」和「管理伺服器」之間的連線。

基本安全模式的網路通訊埠設定

如果您使用的是基本安全模式（單一伺服器安裝），請針對「行動安全防護」元件設定以下網路通訊埠：

元件	網路通訊埠	詳細資訊
管理伺服器與本機通訊伺服器	開啟以下通訊埠： • 針對以下項目開啟 HTTPS 連接埠 443： • 「Mobile Security 管理伺服器」的內送連線。	用於存取「行動安全防護」管理 Web 主控台。

元件	網路通訊埠	詳細資訊
	• 如果您想要從 Google Play 新增外部應用程式。 Google Play 商店的主機名稱為：play.google.com. • 如果您想要運用趨勢科技的行動應用程式信譽評等服務 (MARS)，以及查看上傳之 APK 檔案的安全資訊。 MARS 伺服器的主機名稱為：rest.mars.trendmicro.com **注意** 這是預設的 HTTPS 通訊埠號碼。如果您要變更供「管理伺服器」使用的 HTTPS 通訊埠號碼，請參閱進行管理伺服器設定 第 4-16 頁以取得詳細資訊。 • 針對以下項目開啟 HTTP 連接埠 80： • 授權伺服器 授權伺服器的主機名稱為：licenseupdate.trendmicro.com • 如果您將趨勢科技主動式更新伺服器當做更新來源。 主動式更新伺服器的主機名稱為 mobilesecurity.activeupdate.trendmicro.com。	
管理伺服器與本機通訊伺服器	開啟以下通訊埠： • 針對以下項目開啟 HTTP 連接埠 80 和 HTTPS 連接埠 443： • 如果您想要從 Apple 應用程式商店新增外部 iOS 應用程式 Apple 應用程式商店的主機名稱為：itunes.apple.com.	用於存取「行動安全防護」管理 Web 主控台。

元件	網路通訊埠	詳細資訊
	• 如果您想要針對 iOS 行動裝置使用目錄式應用程式控制	
管理伺服器與本機通訊伺服器	開啟 HTTP 通訊埠 8080。 注意 此通訊埠是雙重伺服器組態設定的預設 HTTP 通訊埠號碼。	用於行動裝置與「行動安全防護 Communication Server」之間的通訊。
	開啟 HTTPS 通訊埠 4343。 注意 此通訊埠是雙重伺服器組態設定的預設 HTTPS 通訊埠號碼。如果您要變更供行動裝置於安裝期間用於與通訊伺服器通訊的 HTTP 通訊埠號碼，請參閱進行一般通訊伺服器設定 第 4-6 頁以取得詳細資訊。	用於行動裝置與「行動安全防護 Communication Server」之間的安全通訊。
	針對「Apple 推播通知服務」(APNs) 伺服器開啟 TCP 通訊埠 2195。Apple 推播通知服務的主機名稱為 `gateway.push.apple.com`。	使 Apple 的 APNs 伺服器得以管理 iOS 行動裝置。 如果您未管理 iOS 行動裝置，即不需要此通訊埠。
	開啟 TCP 通訊埠 443。	建立「本機通訊伺服器」與 Cloud Communication Server 之間的連線。
Active Directory	開啟以下任一通訊埠： • 針對 管理伺服器開啟 TCP 通訊埠 389（網域控制器） • 針對 管理伺服器開啟 TCP 通訊埠 3268（全域類別）	用於使用 Active Directory 進行使用者驗證。 如果您未使用 Active Directory 驗證或匯入使用者，即不需要此通訊埠。

元件	網路通訊埠	詳細資訊
簡單憑證註冊通訊協定 (SCEP) 伺服器	針對通訊伺服器和 iOS 行動裝置開啟 HTTP 通訊埠 80。	用於 iOS 行動裝置註冊。 如果您未使用 SCEP 伺服器來管理 iOS 行動裝置，即不需要此通訊埠。
SQL Server	開啟以下通訊埠： • 針對「行動安全防護管理伺服器」開啟 TCP 通訊埠 1433。 • 針對「行動安全防護管理伺服器」開啟 UDP 通訊埠 1434。 注意 此通訊埠是用來連接 SQL Server 的預設 TCP 通訊埠。不過，如果需要，您也可以將不同通訊埠用於 SQL Server。	建立「行動安全防護管理伺服器」與遠端 SQL Server 之間的連線。

附錄 B

選用組態設定

本附錄提供能在安裝「趨勢科技行動安全防護」時執行的選用組態設定程序。

本附錄包含以下小節：

將 Windows 驗證用於 SQL Server

趨勢科技建議您將 SQL Server 驗證方法用於 SQL Server，避免使用 Windows 驗證。不過，您也可以為 SQL Server 設定 Windows 驗證。

程序

1. 使用「行動安全防護」資料庫存取權在 Active Directory 伺服器中建立使用者帳號。如果您的使用者帳號具有必要的存取權限，您可以略過此步驟。

   a. 在 Active Directory 伺服器中建立使用者帳號。

   b. 啟動 SQL Server Management Studio 並連線至「行動安全防護」資料庫。

   c. 從「物件總管」的樹狀結構中展開 `Security` 資料夾。

   d. 在「登入」上按一下滑鼠右鍵，然後按一下「新登入」。

   e. 按一下左側「選取頁面」上的「一般」，並執行以下作業：

      i. 在「登入名稱」欄位中輸入您在此程序的步驟 a 第 B-2 頁 中建立的使用者名稱，並按一下「搜尋」。

         「選取使用者或群組」的對話方塊隨即顯示。

      ii. 將使用者名稱與網域名稱（例如：*domainname**username*）輸入到「輸入要選取的物件名稱」欄位中，並按一下「檢查名稱」。

      iii. 按一下「確定」。

   f. 從左側的「選取頁面」中選取「伺服器角色」，並選取下列角色：

      - 公用
      - 系統管理員

   g. 按一下「確定」。

      使用者帳號隨即出現在「物件總管」的 `Logins` 資料夾中。

2. 將「行動安全防護管理伺服器」新增到與 Active Directory 伺服器相同的網域中。

3. 在「管理伺服器」上，瀏覽至「開始 > 系統管理員工具 > 電腦管理」，並進行以下設定。

   a. 展開左側樹狀結構的「本機使用者和群組」資料夾，再連按兩下「群組」。

   b. 在「系統管理員」上按一下滑鼠右鍵，並按一下「內容」。

   c. 按一下「一般」標籤上的「新增」按鈕，並進行以下設定：

      i. 在「登入名稱」欄位中輸入您在此程序的步驟 a 第 B-2 頁 中建立的使用者名稱，並按一下「搜尋」。

         「選取使用者、電腦、服務、帳號或群組」的對話方塊隨即顯示。

      ii. 將使用者名稱與網域名稱（例如：*domainname**username*）輸入到「輸入要選取的物件名稱」欄位中，並按一下「檢查名稱」。

      iii. 按一下「確定」。

   d. 按一下「系統管理員內容」對話方塊上的「確定」。

4. 在「管理伺服器」上，移至下列位置：

   ```
   C:\Program Files\Trend Micro\ Mobile Security\
   ```

   或

   ```
   C:\Program Files(x86)\Trend Micro \Mobile Security\)
   ```

5. 使用文字編輯器開啟 `TmDatabase.ini`。如果 `TmDatabase.ini` 檔案不存在，請使用文字編輯器建立一個檔案並將它命名為 `TmDatabase.ini`。

6. 將下列文字新增至 `TmDatabase.ini` 檔案：

```
ConnectionStringFormat=Provider=sqloledb;Data Source=
%server%;Initial Catalog=%database%;Integrated
Security=SSPI;
```

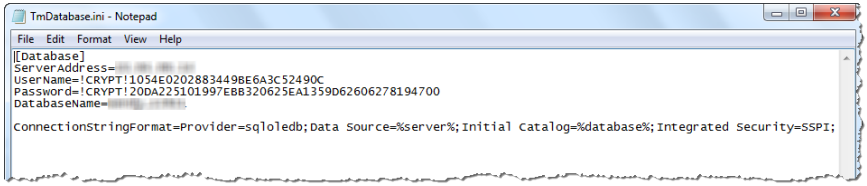

圖 B-1. TmDatabase.ini 檔

7. 在「管理伺服器」上，開啟「Windows 服務」，並按兩下「行動安全防護管理模組服務」。

8. 在「登入」標籤上選取「此帳號：」，並輸入將用來存取資料庫的帳號名稱，在「密碼」和「確認密碼」欄位中輸入其密碼，然後按一下「確定」。

9. 在服務清單中以滑鼠右鍵按一下「行動安全防護管理模組服務」，然後按一下「重新啟動」。

10. 在管理 Web 主控台上進行資料庫設定：

    a. 登入管理 Web 主控台。

    b. 按一下「管理 > 資料庫設定」。

    c. 輸入資料庫伺服器名稱 IP 位址、使用者名稱、密碼及資料庫名稱。

    d. 按一下「儲存」。

設定通訊伺服器通訊埠

「趨勢科技行動安全防護 9.7 版 Patch 2」可讓您自訂「通訊伺服器」用來與「管理伺服器」建立連線的通訊埠。

程序

1. 在安裝「通訊伺服器」的電腦上，使用文字編輯器開啟 `configuration.xml` 檔案（位於 `C:\Program Files\Trend Micro \Communication Server\` 或 `C:\Program Files(x86)\Trend Micro \Communication Server\` 中）
2. 將「mdms_https_port」的值修改成為您需要的通訊埠號碼。
3. 儲存並關閉 `configuration.xml` 檔案。
4. 開啟 Windows 服務，以滑鼠右鍵按一下「行動安全防護通訊服務」，然後按一下「重新啟動」。
5. 登入管理 Web 主控台。
6. 按一下「管理 > 通訊伺服器設定 > 一般設定」。
7. 在「通訊伺服器和管理伺服器之間的通訊設定」區段下，將「HTTPS 通訊埠」的值變更為您在此程序的步驟 2 第 B-5 頁 中設定的通訊埠號碼。
8. 按一下「儲存」。

設定 SCEP

注意

本主題僅適用於「完整版」部署模式。

設定「簡單憑證註冊通訊協定」(SCEP) 可為 iOS 行動裝置提供額外的安全防護。

請參閱設定 iOS 行動裝置環境（選用） 第 2-3 頁。

程序

1. 安裝憑證授權

   如需憑證授權的詳細安裝程序，請參閱以下 URL：

http://msdn.microsoft.com/en-us/library/ff720354.aspx

注意

如果您不想要使用 SCEP，便不需要安裝憑證授權。

2. 設定簡單憑證註冊通訊協定 (SCEP) 設定

   如果您已在 Windows Server 2008 上設定 SCEP，請為 Windows Server 安裝網路裝置註冊服務。如需網路裝置註冊服務的安裝和部署程序，請參閱以下 URL：

   http://esupport.trendmicro.com/solution/en-us/1060187.aspx

   或

   http://technet.microsoft.com/en-us/library/ff955646(WS.10).aspx

   注意

   如果您要使用 SCEP，趨勢科技建議您在 Windows Server 2008 上使用。

3. 驗證系統時鐘

   請務必將 SCEP 伺服器、「通訊伺服器」及「管理伺服器」的系統時鐘設為正確的時間。

4. 針對憑證授權修改政策模組內容：

   a. 在安裝憑證授權的電腦上開啟「憑證授權」管理主控台。

   b. 依序按一下「政策模組」標籤和「內容」。

   c. 選取「遵循憑證範本中可套用的設定值，否則將自動發行憑證」。

   d. 按一下「確定」。

5. 套用以下規則集：

   - iOS 行動裝置都應該能連線至「通訊伺服器」。
   - 「通訊伺服器」應該能連線至 SCEP 伺服器。

- 當 iOS 行動裝置在向「行動安全防護管理伺服器」註冊時，應該要能直接連線至 SCEP 伺服器。

6. 檢查 SCEP 安裝（選用）：

   對於在 Windows Server 2008 上運作的 SCEP，請從「通訊伺服器」存取以下 URL：

   http://SCEPServerIP/certsrv/mscep_admin

   注意

   將 *SCEPServerIP* 取代為 URL 中實際的 SCEP 伺服器 IP 位址。

   如果您看見與以下相似的網頁，表示您的伺服器設定是正確的：

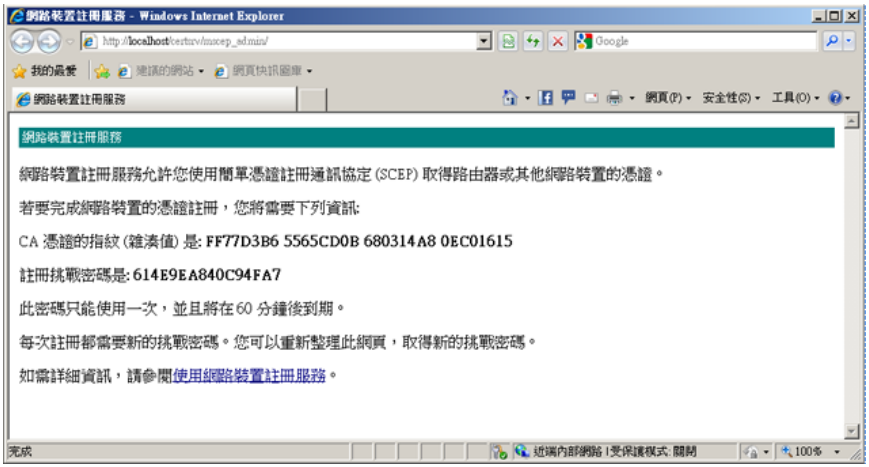

圖 B-2. 設定驗證

注意

iOS 行動裝置進行註冊時，將能存取下 URL：

http://SCEPServerIP/certsrv/mscep

iOS 行動裝置唯有在進行註冊時才需要連線至 SCEP，除此之外，不會在其他作業中使用此連線。

附錄 C

產生及設定 APNs 憑證

「趨勢科技行動安全防護」須有 Apple 推播通知服務 (APNs) 憑證才能管理 iOS 行動裝置。本附錄介紹產生 APNs 憑證並將憑證上傳至「行動安全防護管理伺服器」的詳細程序。

如需其他的設定需求，請參閱設定 iOS 行動裝置環境（選用） 第 2-3 頁。

本附錄包含以下小節：

瞭解 APNs 憑證

Apple 推播通知服務 (APNs) 可讓「趨勢科技企業版行動安全防護」伺服器安全地透過無線網路與裝置通訊。每個組織都需要有自己的 APNs 憑證，才能維護安全的機制讓裝置透過 Apple 的推播通知網路通訊。

系統管理員要求資訊或管理 iOS 裝置時，「趨勢科技企業版行動安全防護」會使用您的 APNs 憑證來傳送通知給裝置。唯有通知會透過 APNs 伺服器傳送。

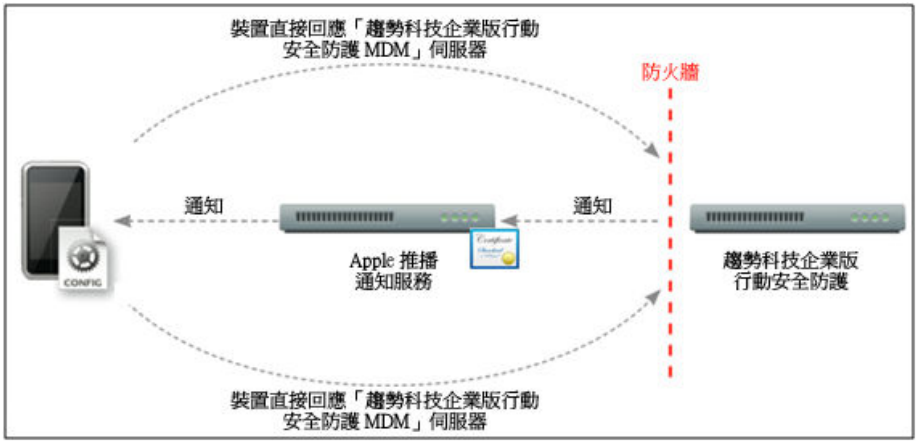

圖 C-1. 通知程序

產生 APNs 憑證

本節說明產生 Apple 推播通知服務憑證以供管理 iOS 行動裝置的程序。

程序

1. 從 Windows Server 或 Mac 工作站產生憑證簽署要求 (CSR)。
2. 讓趨勢科技或 Apple 簽署 CSR。
   - 使用經趨勢科技簽署的憑證：趨勢科技提供簡易的簽署 CSR 程序：

a. 請移至「趨勢科技 APNs 憑證簽署入口網站」，以提供貴公司的資訊、您的產品啟動碼，以及您 CSR 的副本：

   http://forms.trendmicro.com/download_trials/csr/?dom=us

   將要求提交到入口網站後，系統會寄給您一封附有已簽署 CSR 的電子郵件。

b. 使用經過驗證的 Apple ID 將已簽署的 CSR 上傳至 Apple Push Certificates Portal。

   Apple 將產生 APNs 憑證。

- 使用經 Apple 簽署的憑證：如果您想使用經 Apple 簽署的憑證，請先確定您已具備下列項目，再繼續進行：
  - 現有的 Apple Enterprise Developer 帳號 (http://developer.apple.com/programs/ios/enterprise)
  - 指派為 Agent 的開發人員帳號角色（Admin 角色不適用）
  - 您 Windows Server 或 Mac OS X 工作站上的系統管理員權限

  若要使用經 Apple 簽署的權限，請參閱 Windows 適用的使用經 Apple 簽署的憑證 第 C-10 頁或 Mac 適用的使用經 Apple 簽署的憑證 第 C-19 頁。

3. 將 APNs 憑證安裝在您的 Windows Server 或 Mac 工作站上，然後將憑證匯出以儲存在您的電腦上。

   在您匯出憑證後，繼續將此憑證上傳到「趨勢科技行動安全防護管理伺服器」。

從 Windows Server 產生 APNs 憑證

以下步驟會引導您從 Windows Server 產生 APNs 憑證。如果您已從 Mac OS X 工作站產生憑證，請略過本小節並將憑證上傳至「趨勢科技企業版行動安全防護 MDM」伺服器。

步驟 1：產生憑證簽署要求 (CSR)

程序

1. 瀏覽至開始」「系統管理工具」「Internet Information Services (IIS) 管理員」，然後選取伺服器名稱。

2. 按兩下「伺服器憑證」圖示。

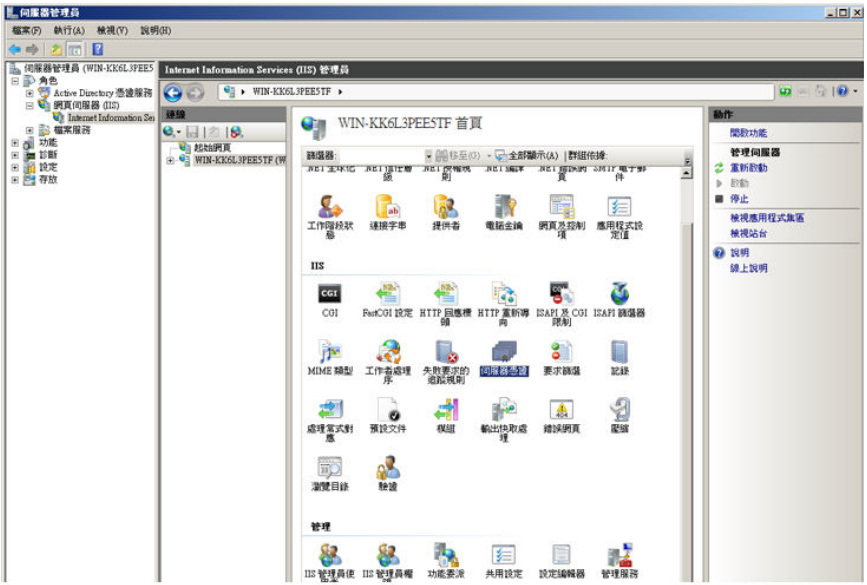

圖 C-2. 存取伺服器憑證

注意

在本文件中，我們使用 IIS 7.0 版來設定 APNs 憑證。

3. 在右側的「動作」窗格中按一下「建立憑證要求」。

「要求憑證」精靈隨即出現。

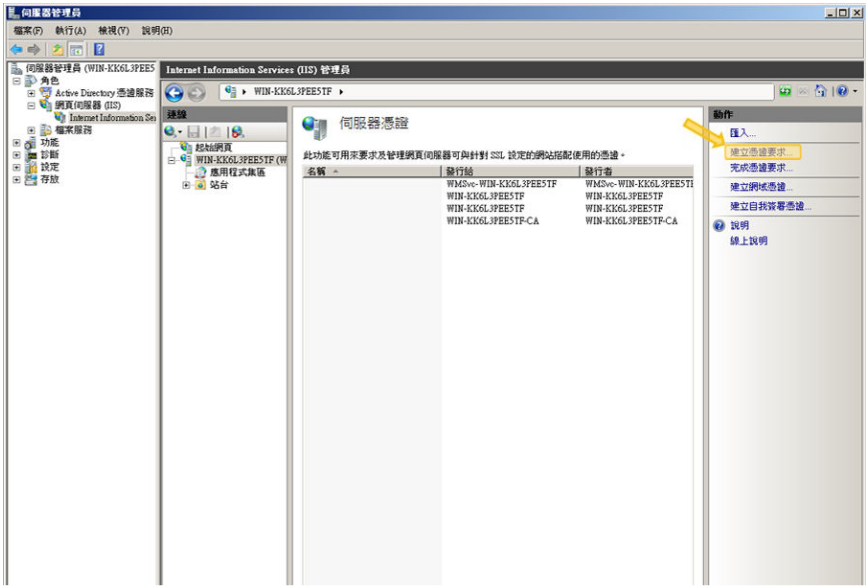

圖 C-3. 啟動要求憑證精靈

4. 在「分辨名稱屬性」視窗中輸入以下內容：
   - 「一般名稱」— 與 Apple Developer 帳號相關的名稱
   - 「組織」— 組織/公司的法定註冊名稱
   - 「組織單位」— 組織中的部門名稱
   - 「縣市/位置」— 組織所在的縣市
   - 「省份」— 組織所在的省份

- 「國家（地區）」— 組織所在的國家或地區

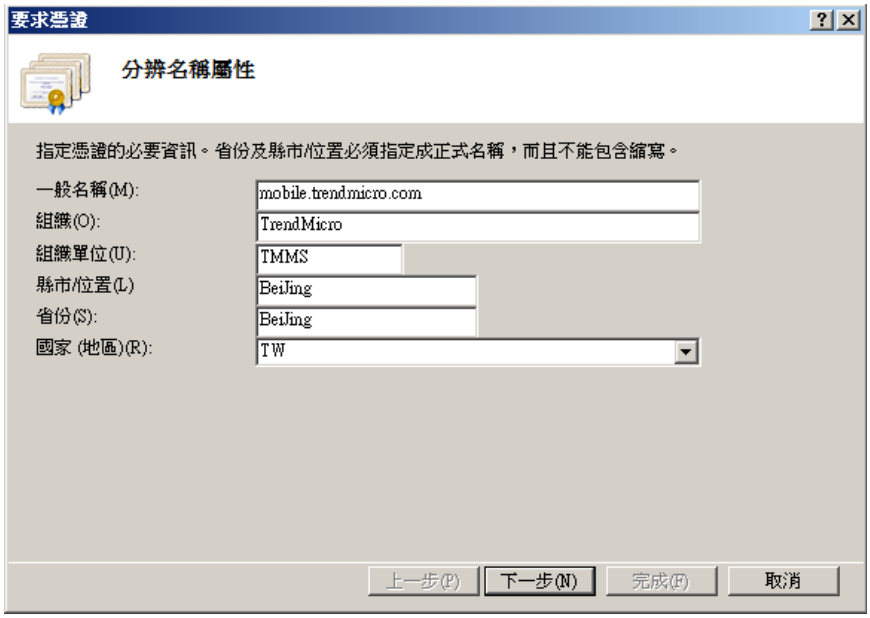

圖 C-4. 「分辨名稱屬性」畫面

5. 按一下「下一步」。

   「密碼編譯服務提供者內容」視窗隨即出現。

6. 在「密碼編譯服務提供者」欄位中選取「Microsoft RSA SChannel Cryptographic Provider」，並在「位元長度」欄位中選取「2048」，然後按一下「下一步」。

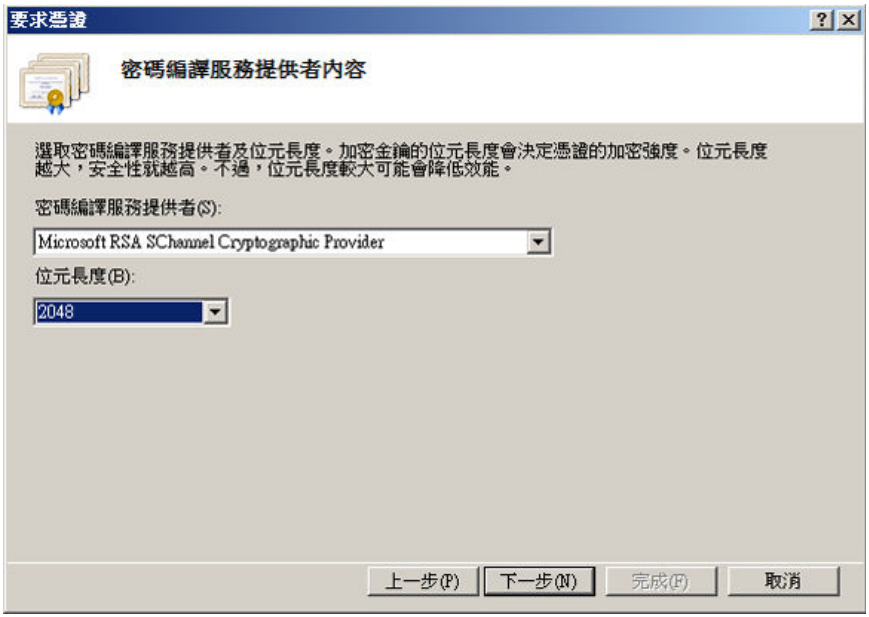

圖 C-5.「密碼編譯服務提供者內容」畫面

7. 選取憑證要求檔案的儲存位置。

   務必記得檔案名稱和檔案的儲存位置。

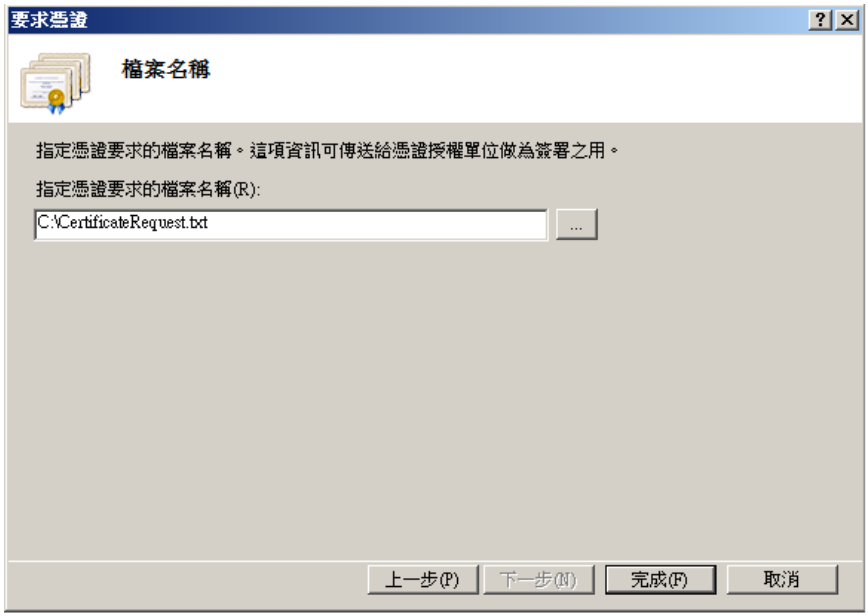

圖 C-6.「檔案名稱」畫面

8. 按一下「完成」。

您現在已經建立 CSR，可準備將其上傳至 Apple 開發人口網站。

重要

趨勢科技建議您將剛剛建立的 CSR 檔儲存在安全的位置。您下次要將您的 APNs 憑證續約時，必須再次使用該檔案。若使用不同的 APNs 憑證，您必須再次向「行動安全防護管理伺服器」註冊所有的 iOS 行動裝置。如需詳細資料，請參閱續約 APNs 憑證 第 C-24 頁。

步驟 2：上傳 CSR 並產生 APNs 憑證

產生 CSR 後，您現在可以執行以下任一項工作：

- 將 CSR 上傳至「趨勢科技 CSR 簽署入口網站」讓趨勢科技進行簽署，再使用它產生 APNs 憑證。

- 將 CSR 上傳至「Apple 開發人口網站」讓 Apple 進行簽署，再使用它產生 APNs 憑證。

注意

下列程序假設您使用趨勢科技簽署的 APNs 憑證。

如果您要使用 Apple 簽署的 APNs 憑證，請略過此程序並參閱使用經 Apple 簽署的憑證 第 C-10 頁 (Windows) 或使用經 Apple 簽署的憑證 第 C-19 頁 (Mac)。

程序

1. 開啟網路瀏覽器並瀏覽以下 URL：

   http://forms.trendmicro.com/download_trials/csr/?dom=us

2. 填寫適當的欄位，並上傳您剛剛產生的 CSR，再按一下「繼續」。

   趨勢科技會簽署並將簽署的憑證歸還給您。

3. 從趨勢科技入口網站或從您收到的電子郵件下載簽署的憑證。

4. 將 CSR 上傳至 Apple Push Certificates Portal：

   a. 開啟網路瀏覽器並瀏覽以下 URL：

      https://identity.apple.com/pushcert/

   b. 使用 Apple ID 和密碼登入。

      「開始使用」頁面隨即出現。

   c. 按一下「建立憑證」按鈕。

      「使用規範」畫面隨即出現。

   d. 按一下「接受」以同意條款內容。

      「建立新的推播憑證」畫面隨即出現。

   e. 按一下「瀏覽」並選取趨勢科技簽署過的檔案，然後按一下「上傳」。等候直到入口網站產生 APNs 憑證 (`.pem`) 檔案。

   f. 按一下「下載」以將 `.pem` 檔案儲存到電腦。

g. 將剛下載的 .pem 重新命名為 .cer 並繼續步驟 3：安裝您的 APNs 憑證 第 C-11 頁 (針對 Windows)。

使用經 Apple 簽署的憑證

注意

如果您使用趨勢科技簽署的 APNs 憑證，請略過此程序。

程序

1. 在網路瀏覽器上瀏覽以下 URL：

   https://developer.apple.com/

2. 按一下「Member Center」連結。

3. 使用 Apple ID 和密碼登入。

4. 按一下「iOS Provisioning Portal」。

   注意

   如果您未看見 iOS Provisioning Portal，表示您尚未建立 iOS 開發用的開發帳號。

5. 按一下左側窗格中的「App ID」，然後按一下「新增 App ID」。

6. 填寫適當的欄位。「Bundle Identifier (App ID Suffix) notation」欄位必須是：com.apple.mgmt.mycompany.tmms.

   - 請將 mycompany 取代您的公司名稱。
   - 記下「The Bundle Identifier (App ID Suffix) notation」值。設定「行動安全防護管理伺服器」時將需要使用這個值。

7. 按一下「送出」。

   剛新增的「App ID」會出現在清單中。

8. 按一下「設定」。

秘訣

如果您未看見或無法按一下「設定」，請驗證是否以 Agent 角色登入。

9. 選取「啟動 Apple 推送通知服務」，然後按一下「生產推送 SSL 憑證」的「設定」。

   如果您無法選取「啟動 Apple 推送通知服務」，請嘗試使用 Safari 或 Firefox 網路瀏覽器，並驗證是否以 Agent 角色登入。

10. 「SSL 憑證小幫手」精靈隨即出現，指示您建立憑證簽署要求（已在步驟 1：產生憑證簽署要求 (CSR) 第 C-17 頁建立）。按一下「繼續」。

11. 按一下「選擇檔案」，然後上傳在步驟 1：產生憑證簽署要求 (CSR) 第 C-17 頁建立的憑證簽署要求檔案。（例如，CertificateSigningRequest.certSigningRequest2）。

12. 按一下「產生」。

    完成時，畫面會出現以確認您的 APNs SSL 憑證已產生。

13. 按一下「繼續」。

    「下載並安裝您的 Apple 推播通知伺服器 SSL 憑證」畫面隨即顯示。

14. 按一下「下載」以將 `.cer` 檔案儲存到電腦，然後繼續進行步驟 3：安裝您的 APNs 憑證 第 C-21 頁 (Mac)。

步驟 3：安裝您的 APNs 憑證

程序

1. 移至「開始 > 系統管理工具 > Internet Information Services (IIS) 管理員」，並選取伺服器名稱，然後按兩下「伺服器憑證」。

2. 在右側的「動作」窗格中按一下「完成憑證要求」。

「完成憑證要求」精靈隨即出現。

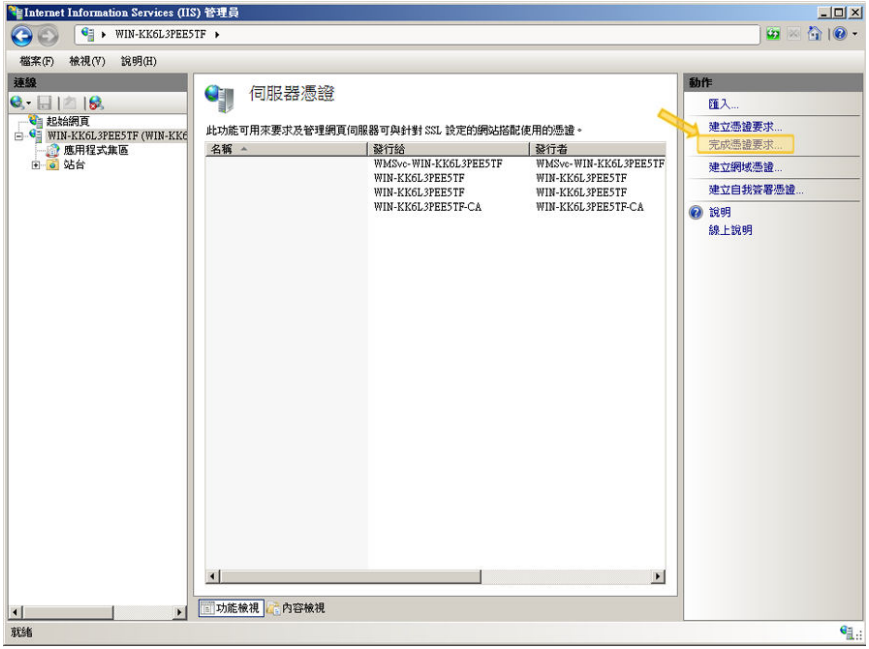

圖 C-7. 完成憑證要求

注意

如果您使用 IIS 7.5，按一下「完成憑證要求」時會顯示以下錯誤訊息：

無法建立憑證鏈結到受信任的根授權單位。

發生此錯誤時，請參閱設定 IIS 7.5 以安裝 APNs 憑證 第 C-16 頁以取得解決此問題的程序。

---

3. 選取從 Apple Developer Portal 下載的 `.cer` 憑證檔案，然後在「好記的名稱」欄位中輸入 `Trend Micro Mobile Security for Enterprise MDM APNs`。

注意

如果您從 Mac 工作站產生憑證檔案，必須手動將 .pem 副檔名變更為 .cer。

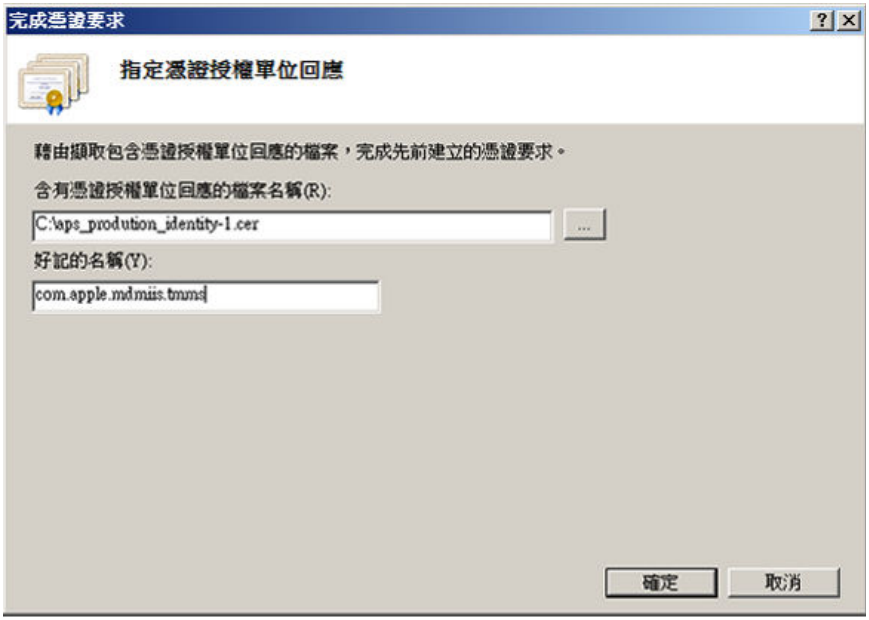

圖 C-8.「指定憑證授權單位回應」畫面

秘訣

好記的名稱並不是憑證本身的一部分，不過它能讓伺服器管理員輕易地區別憑證。

4. 按一下「確定」。

   憑證隨即安裝在伺服器上。

5. 驗證 Apple Production Push Services 憑證出現在「伺服器憑證」清單中。如果您可以看見憑證，請遵循後續的步驟將其匯出，然後上傳至「趨勢科技企業版行動安全防護管理伺服器」。

6. 在「伺服器憑證」清單中以滑鼠右鍵按一下憑證，然後按一下「匯出」。

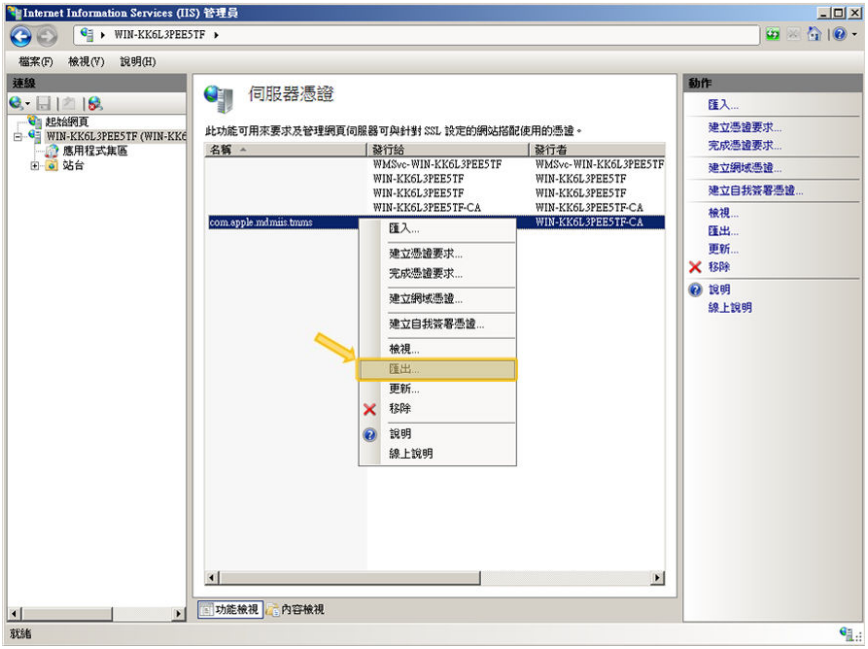

圖 C-9. 匯出憑證

7. 選取檔案的儲存位置，並選擇匯出作業的密碼，然後按一下「確定」。

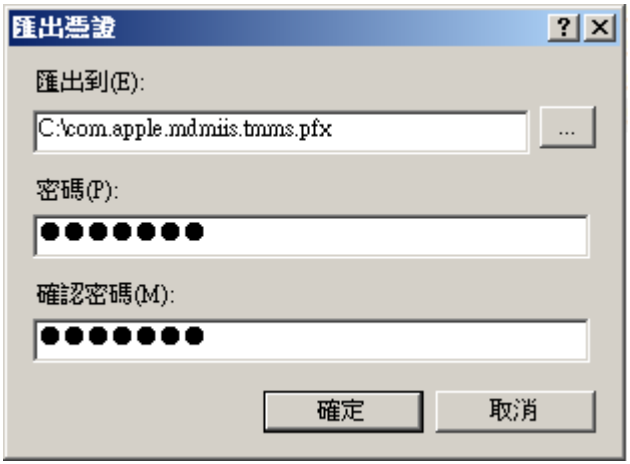

圖 C-10. 指定憑證的密碼

秘訣

如果您只能選擇儲存為 .cer 檔案（而非 .pfx），表示您的憑證匯出不正確。確認您選取了正確的匯出檔案。

注意

務必記住密碼或將密碼保存在安全的場所。在將憑證上傳至「趨勢科技企業版行動安全防護管理伺服器」時需使用該密碼。

完成以上所有步驟後，您應具備以下項目：

- APNs 憑證（.pfx 格式，非 .cer 格式）
- 匯出憑證時設定的密碼

您現在已準備就緒，可將憑證上傳至「趨勢科技行動安全防護管理伺服器」。如需相關程序，請參閱將 APNs 憑證上傳至行動安全防護管理伺服器 第 C-22 頁。

設定 IIS 7.5 以安裝 APNs 憑證

如果您使用 IIS 7.5，將憑證上傳至 IIS 可能會不成功，並出現以下訊息：

無法建立憑證鏈結到受信任的根授權單位。

此錯誤發生的原因如下：

- APNs 憑證是由 Apple 根 CA 簽署的，而非公用 CA。
- IIS 7.5 增強了信任根 CA 的檢查。

程序

1. 從以下 URL 下載 Apple Root 憑證和 Application Integration 憑證：

   http://www.apple.com/certificateauthority/

2. 按兩下 Apple Root 憑證，然後按一下「憑證」視窗中的「安裝憑證」。
3. 在「歡迎使用」畫面中按一下「下一步」。
4. 選取「將所有憑證放入以下的存放區」，然後按一下「瀏覽」。
5. 在「選擇憑證存放區」視窗中選取「顯示實體存放區」，並選取「信任的根憑證授權 > 本機電腦」然後按一下「確定」。
6. 在「憑證匯入精靈」畫面中按一下「下一步」，然後按一下「完成」。
7. 針對 Application Integration 憑證重複步驟 2 第 C-16 頁 到 5 第 C-16 頁。然而，在步驟 4 第 C-16 頁 中請選取「中繼憑證授權 > 本機電腦」，而非「信任的根憑證授權 > 本機電腦」。

從 Mac 工作站產生 APNs 憑證

以下程序將引導您使用 Mac OS X 工作站產生 APNs 憑證。如果您使用 Windows Server，請略過本節並繼續閱讀從 Windows Server 產生 APNs 憑證 第 C-3 頁。

步驟 1：產生憑證簽署要求 (CSR)

程序

1. 在 Mac 電腦上，移至「應用程式 > 工具程式 > 鑰匙圈存取。
2. 在左側窗格的「鑰匙圈」區段中選取「登入」，然後在「類別」區段選取「憑證」。
3. 在頂端的功能表列選取鑰匙圈存取 > 憑證小幫手 > 要求來自憑證授權單位的憑證」。

   「憑證小幫手」精靈隨即出現。
4. 在「使用者電子郵件地址」和「一般名稱」等欄位中輸入電子郵件地址和註冊的 Apple Developer 帳號名稱並選取「已儲存至磁碟」，然後按一下「繼續」。
5. 選取檔案的儲存位置，然後按一下「儲存」。

   您現在已經建立 CSR，可準備將其上傳至 Apple 開發入口網站。

重要

趨勢科技建議您將剛剛建立的 CSR 檔儲存在安全的位置。您下次要將您的 APNs 憑證續約時，必須再次使用該檔案。若使用不同的 APNs 憑證，您必須再次向「Mobile Security 管理伺服器」註冊所有的 iOS 行動裝置。如需詳細資料，請參閱續約 APNs 憑證 第 C-24 頁。

步驟 2：上傳 CSR 並產生 APNs 憑證

產生 CSR 後，您現在可以執行以下任一項工作：

- 將 CSR 上傳至「趨勢科技 CSR 簽署入口網站」讓趨勢科技進行簽署，再使用它產生 APNs 憑證。
- 將 CSR 上傳至「Apple 開發入口網站」讓 Apple 進行簽署，再使用它產生 APNs 憑證。

注意

下列程序假設您使用趨勢科技簽署的 APNs 憑證。

如果您要使用 Apple 簽署的 APNs 憑證，請略過此程序並參閱使用經 Apple 簽署的憑證 第 C-10 頁 (Windows) 或使用經 Apple 簽署的憑證 第 C-19 頁 (Mac)。

程序

1. 開啟網路瀏覽器並瀏覽以下 URL：

   http://forms.trendmicro.com/download_trials/csr/?dom=us

2. 填寫適當的欄位，並上傳您剛剛產生的 CSR，再按一下「繼續」。

   趨勢科技會簽署並將簽署的憑證歸還給您。

3. 從趨勢科技入口網站或從您收到的電子郵件下載簽署的憑證。

4. 將 CSR 上傳至 Apple Push Certificates Portal：

   a. 開啟網路瀏覽器並瀏覽以下 URL：

      https://identity.apple.com/pushcert/

   b. 使用 Apple ID 和密碼登入。

      「開始使用」頁面隨即出現。

   c. 按一下「建立憑證」按鈕。

      「使用規範」畫面隨即出現。

   d. 按一下「接受」以同意條款內容。

      「建立新的推播憑證」畫面隨即出現。

   e. 按一下「瀏覽」並選取趨勢科技簽署過的檔案，然後按一下「上傳」。等候直到入口網站產生 APNs 憑證 (`.pem`) 檔案。

   f. 按一下「下載」以將 `.pem` 檔案儲存到電腦。

g. 將剛下載的 .pem 重新命名為 .cer 並繼續步驟 3：安裝您的 APNs 憑證 第 C-21 頁 (針對 Mac)。

使用經 Apple 簽署的憑證

注意

如果您使用趨勢科技簽署的 APNs 憑證，請略過此程序。

程序

1. 在網路瀏覽器上瀏覽以下 URL：

   https://developer.apple.com/

2. 按一下「Member Center」連結。
3. 使用 Apple ID 和密碼登入。
4. 按一下「iOS Provisioning Portal」。

   注意

   如果您未看見 iOS Provisioning Portal，表示您尚未建立 iOS 開發用的開發帳號。

5. 按一下左側窗格中的「App ID」，然後按一下「新增 App ID」。
6. 填寫適當的欄位。「Bundle Identifier (App ID Suffix) notation」欄位必須是：com.apple.mgmt.mycompany.tmms.

   - 請將 mycompany 取代您的公司名稱。
   - 記下「The Bundle Identifier (App ID Suffix) notation」值。設定「行動安全防護管理伺服器」時將需要使用這個值。

7. 按一下「送出」。

   剛新增的「App ID」會出現在清單中。

8. 按一下「設定」。

秘訣

如果您未看見或無法按一下「設定」，請驗證是否以 Agent 角色登入。

9. 選取「啟動 Apple 推送通知服務」，然後按一下「生產推送 SSL 憑證」的「設定」。

   如果您無法選取「啟動 Apple 推送通知服務」，請嘗試使用 Safari 或 Firefox 網路瀏覽器，並驗證是否以 Agent 角色登入。

10. 「SSL 憑證小幫手」精靈隨即出現，指示您建立憑證簽署要求（已在步驟 1：產生憑證簽署要求 (CSR) 第 C-17 頁建立）。按一下「繼續」。

11. 按一下「選擇檔案」，然後上傳在步驟 1：產生憑證簽署要求 (CSR) 第 C-17 頁建立的憑證簽署要求檔案。（例如，CertificateSigningRequest.certSigningRequest2）。

12. 按一下「產生」。

    完成時，畫面會出現以確認您的 APNs SSL 憑證已產生。

13. 按一下「繼續」。

    「下載並安裝您的 Apple 推播通知伺服器 SSL 憑證」畫面隨即顯示。

14. 按一下「下載」以將 `.cer` 檔案儲存到電腦，然後繼續進行步驟 3：安裝您的 APNs 憑證 第 C-11 頁 (Windows)。

注意

若要在 Windows 電腦上安裝 APNs 憑證，您必須手動將 `.pem` 副檔名變更為 `.cer`。

步驟 3：安裝您的 APNs 憑證

程序

1. 移至下載檔案的位置，然後按兩下檔案以自動將其上傳至 Keychain Access 及完成簽署要求。
2. 瀏覽至「應用程式 > 工具程式 > 鑰匙圈存取。
3. 在左側窗格的「鑰匙圈」區段中選取「登入」，然後在「類別」區段選取「憑證」。
4. 驗證 Apple 生產推送服務憑證出現在清單中，且將其展開時有相關的私密金鑰位在下方。如果您可以看見憑證，請遵循後續的步驟將其匯出，然後上傳至「行動安全防護管理伺服器」。

注意

如果看不見 APNs 憑證或私密金鑰未顯示，請驗證您是否選取「登入鑰匙圈」、「憑證」類別，並且已展開憑證金鑰。如果您仍然無法看見憑證，請重複以上所有步驟。

5. 在私密金鑰上按一下滑鼠右鍵（或按住 Ctrl 鍵不放並再按一下滑鼠左鍵），然後按一下「匯出」。
6. 選擇檔案名稱和檔案的儲存位置，然後選取「個人資訊交換 (.p12)」檔案格式。

秘訣

如果您只能選擇儲存為 .cer 檔案（而非 .p12），表示您的憑證匯出不正確。務必在上個步驟選取要匯出的「私密金鑰」，且您的檔案格式為「個人資訊交換 (.p12)」。

7. 按一下「儲存」。
8. 選擇匯出作業的密碼，然後按一下「確定」。

秘訣

務必記住密碼或將密碼保存在安全的場所。將憑證上傳至「企業版 Mobile Security 管理伺服器」時需使用該密碼。

完成以上所有步驟後，您應具備以下項目：

- APNs 憑證（.p12 格式，非 .cer 格式）
- 匯出憑證時設定的密碼

您現在已準備就緒，可將憑證上傳至「Mobile Security 管理伺服器」。如需相關程序，請參閱將 APNs 憑證上傳至行動安全防護管理伺服器 第 C-22 頁。

將 APNs 憑證上傳至行動安全防護管理伺服器

本節說明將 Apple 推播通知服務 (APNs) 憑證上傳至「趨勢科技企業版行動安全防護」伺服器以便管理 iOS 裝置的程序。

注意

開始之前，請您務必備妥以下各項：

- APNs 憑證檔案（.pfx 或 .p12 格式，非 .cer 格式）
- 匯出憑證時設定的密碼
- 「趨勢科技企業版行動安全防護 MDM」伺服器的系統管理員帳號

程序

1. 登入管理 Web 主控台。
2. 請執行以下任一項工作：

- 按一下「管理 > 憑證管理」，並按一下「新增」，接著從硬碟選取「Apple 推播通知伺服器」憑證，然後按一下「儲存」。

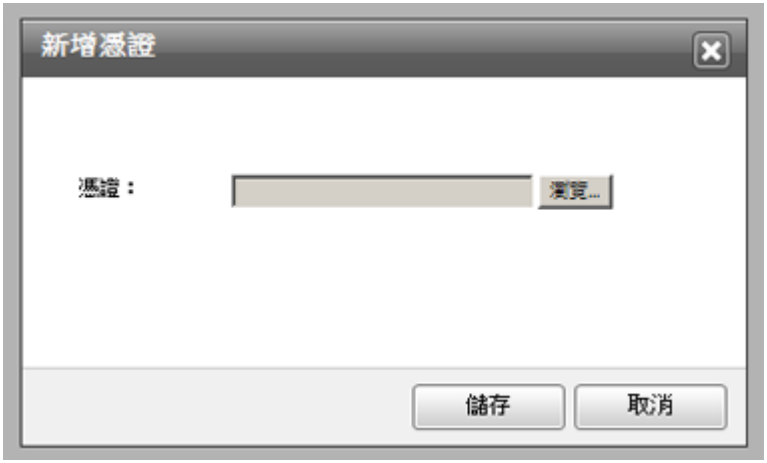

圖 C-11. 透過「憑證管理」新增憑證

- 按一下「管理 > 通訊伺服器設定」，並按一下「iOS 設定」標籤，接著在「憑證」欄位中從硬碟選取 Apple 推播通知伺服器憑證，然後按一下「儲存」。

圖 C-12. 透過「通訊伺服器設定」新增憑證

完成以上步驟後，即可管理 iOS 行動裝置。

續約 APNs 憑證

您必須在 APNs 憑證過期前進行續約，才能繼續管理 iOS 行動裝置。

若要將 APNs 憑證續約，請執行與建立新憑證相同的步驟。接著造訪 Apple Push Certificates Portal 並上傳新憑證。

登入後，您會看到現有憑證，或可能會看到從先前 Apple Developer 帳號匯入的憑證。在 Certificates Portal 上，將憑證續約時的唯一不同是按一下「續約」。

注意

您必須在 Certificates Portal 有開發人員帳號才能存取該網站。

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: TSTM97808/170419