# iOS 部署
# 技術參考

iOS 7.1

2014 年 5 月

# 目錄

# 簡介

本指南是寫給想要在內部網路中支援 iOS 裝置的 IT 管理者。其中提供在企業或學校這類大規模的組織裡部署與支援 iPhone、iPad 與 iPod touch 的相關資訊，也說明了 iOS 裝置如何提供鉅細靡遺的安全防護功能、與現有基礎設施整合的方式，以及部署時可用的強大工具。

深入了解 iOS 所支援的主要技術，可以協助您順利執行部署策略，為使用者提供最佳經驗。在組織裡部署 iOS 裝置時，可以參考下列幾章的技術資訊：

**整合。**iOS 裝置為各種網路基礎設施提供了內建支援。在這一章裡，您將認識 iOS 所支援的技術，以及與 Microsoft Exchange、Wi-Fi、VPN 或其他標準服務整合的最佳做法。

**安全性。**iOS 的設計可供安全地存取企業服務並保護重要資料。它會針對傳輸中的資料提供強大的加密功能、以經過證明的認證方式存取企業服務，並且為裝置中儲存的所有資料進行硬碟加密。請閱讀本章內容以進一步了解 iOS 的各項安全防護功能。

**設定與管理。**iOS 支援先進的工具與技術，以確保您能輕鬆地設定 iOS 裝置、依需求進行配置，並在大規模環境下輕鬆管理。本章包含行動管理裝置 (MDM) 的簡介。

**發佈 App。** 在組織裡部署 app 與內容的方式有好幾種。「iOS 企業開發人員計畫」(iOS Developer Enterprise Program) 能讓您的組織為內部使用者製作與部署 app。請利用本章內容，深入瞭解如何部署專為內部使用而製作的 app。

下列附錄提供了額外的技術細節與需求條件：

**Wi-Fi 基礎設施。**詳細說明 iOS 支援的 Wi-Fi 標準，以及規劃大型 Wi-Fi 網路時應有的考量。

**限制。**詳細介紹在設定 iOS 裝置時，可以使用哪些限制來達成您對安全性、密碼與其他方面的要求。

**以無線方式安裝內部專用 App。**說明使用您的入口網站發佈內部專用 App 的相關細節與需求。

### 其他資源

如需相關實用資訊，請參閱 下列網站：

www.apple.com/ipad/business/it

www.apple.com/iphone/business/it

www.apple.com/education/it

# 第 1 章：整合

iOS 裝置為各種網路基礎設施提供了內建支援。
其中包含：

- Microsoft Exchange 等常見的協力廠商系統
- 與符合業界標準的郵件、目錄、行事曆與其他系統的整合
- 資料傳輸與加密時使用的標準 Wi-Fi 協定
- 虛擬私人網路 (VPN)，包含 app 層級的 VPN
- 可在 app 或服務連接網路時簡化認證程序的單一登入功能
- 認證使用者並保護通訊安全的數位憑證

由於 iOS 已內建上述支援功能，您的 IT 部門只需要完成幾個設定步驟，即可在現有的基礎設施裡整合 iOS 裝置。請繼續往下閱讀，進一步了解 iOS 支援的技術與整合的最佳作法。

## Microsoft Exchange

iOS 可以透過 Microsoft Exchange ActiveSync (EAS) 直接與 Microsoft Exchange Server 進行通訊，可推播電子郵件、行事曆、通訊錄和其他工作。Exchange ActiveSync 也為使用者提供了存取全域通訊列表 (GAL) 的功能，並為管理員提供了執行密碼規則和遠端清除功能。iOS 為 Exchange ActiveSync 同時提供了基本和憑證架構的驗證。

如果您的公司目前正在使用 Exchange ActiveSync，即已具備支援 iOS 所需的服務，不必再進行其他設定。

### 需求條件

iOS 7 或以上版本的裝置支援下列版本的 Microsoft Exchange：

- Exchange Server 2003 SP 2 (EAS 2.5)
- Exchange Server 2007 (使用 EAS 2.5)
- Exchange Server 2007 SP 1 (EAS 12.1)
- Exchange Server 2007 SP 2 (EAS 12.1)
- Exchange Server 2007 SP 3 (EAS 12.1)
- Exchange Server 2010 (EAS 14.0)
- Exchange Server 2010 SP 1 (EAS 14.1)
- Exchange Server 2010 SP 2 (使用 EAS 14.1)
- Exchange Server 2013 (使用 EAS 14.1)
- Office 365 (使用 EAS 14.1)

### Microsoft Direct Push

只要有行動網路或 Wi-Fi 資料連線可用，Exchange Server 就會自動將電子郵件、工作、聯絡資訊和行事曆事件傳送到 iOS 裝置。iPod touch 和某幾款 iPad 機型不具備行動網路連線能力，只能在連接到 Wi-Fi 網路時接收推播通知。

### Microsoft Exchange Autodiscovery

iOS 支援 Microsoft Exchange Server 2007 和 Microsoft Exchange Server 2010 的 Autodiscover 服務。當您手動設定裝置時，Autodiscover 會使用您的電子郵件位址和密碼來決定正確的 Exchange Server 資訊。

更多關於啟用 Autodiscover 服務的資訊，請參閱自動探索服務。

### Microsoft Exchange 全域通訊清單

iOS 裝置會從您公司的 Exchange Server 企業目錄中擷取聯絡資訊。您可以在搜尋「聯絡資訊」時取用目錄，在輸入電子郵件位址時，裝置也會自動取用目錄來協助您完成填寫。iOS 6 或以上版本支援 GAL 照片 (必須有 Exchange Server 2010 SP 1 或以上版本)。

### 不支援的 Exchange ActiveSync 功能

iOS 不支援下列 Exchange 功能：

- 打開電子郵件中儲存在 SharePoint 伺服器上的文件連結
- 設定外出自動回覆訊息

### 透過 Exchange 識別 iOS 版本

當 iOS 裝置連接 Exchange Server 時，裝置會報告其 iOS 版本。此版本編號會透過要求標頭中的「使用者代理程式」欄位傳送，看起來類似 Apple-iPhone2C1/705.018。分隔符號 (/) 之後的數字就是 iOS 的版次編號，每一版 iOS 都有其專屬的號碼。

若要在裝置上檢視版次編號，請前往「設定」(Settings) >「一般」(General) >「關於本機」(About)。您將會看到版本編號和版次編號，如 4.1 (8B117A)。括號中的數字即是版次編號，其可識別裝置正在執行的版次。

當版次編號傳送給 Exchange Server 時，它會從 NANNNA 格式 (其中 N 為數值，而 A 為字母字元) 轉換為 NNN.NNN 的 Exchange 格式。數值會被保留，但字母會被轉換成其在字母表中的位置值。例如，「F」會被轉換成「06」，因為其為字母表中的第六個字母。如有需要，數字前面會補零以符合 Exchange 格式。

在此範例中，版次編號 7E18 便會轉換成 705.018。

第一個數字 7 仍會是「7」。字母 E 是字母表中的第五個字母，所以會轉換成「05」。句號 (.) 會依格式要求插入在轉換的版本中。下一個數字 18 前面會補零並轉換成「018」

如果版次編號以字母結束，如 5H11A，編號會如上述進行轉換，最後字元的數值會被附加到字串中 (以 3 個零分隔)。因此 5H11A 便變成 508.01100001。

### 遠端清除

您可以使用 Exchange 提供的功能從遠端清除 iOS 裝置的內容。清除的動作會從裝置移除所有資料和設定資訊，裝置會被安全清除並回復至其原始出廠設定。清除的動作也會移除資料的加密密鑰 (使用 256 位元 AES 加密)，此動作會立即讓所有資料無法回復。

如果是 Microsoft Exchange Server 2007 或以上版本，您可以使用 Exchange Management Console、Outlook Web Access 或 Exchange ActiveSync Mobile Administration Web Tool 來執行遠端清除。如果是 Microsoft Exchange Server 2003，您可以使用 Exchange ActiveSync Mobile Administration Web Tool 來啟動遠端清除。

使用者可以前往「設定」(Settings) >「一般」(General) >「重置」(Reset)，然後選擇「清除所有內容和設定」(Erase All Content and Settings)，來清除其自己的裝置。裝置也可以設定為在輸入密碼失敗達指定次數後自動移除。

## 共通標準的服務

藉由支援 IMAP 郵件通訊協定、LDAP 目錄服務、CalDAV 行事曆和 CardDAV 聯絡資訊通訊協定，iOS 幾乎可與所有符合共通標準的環境順利整合。如果您的網路環境是設定為要求使用者認證與 SSL，iOS 提供了可安全取用共通標準的公司電子郵件、行事曆、工作與聯絡資訊的功能。透過 SSL，iOS 支援 128 位元加密以及由主要憑證管理中心發佈的 X.509 根憑證。

在典型的部署中，iOS 裝置會與 IMAP 與 SMTP 郵件伺服器建立直接連線，以透過無線傳輸方式收發電子郵件，也可以與 IMAP 伺服器的記事進行無線同步。iOS 裝置可以連接到您公司的 LDAPv3 公司目錄，讓使用者取用「郵件」、「聯絡資訊」和「訊息」應用程式裡的公司聯絡資訊。若與您的 CalDAV 伺服器同步，使用者即可透過無線方式建立與接受行事曆邀請、接收行事曆更新，並與「提醒事項」app 同步工作。CardDAV 還能讓使用者以 vCard 格式維護一組與您的 CardDAV 伺服器同步的聯絡資訊。所有網路伺服器都可以位於 DMZ 子網路內或公司防火牆後，或同時位於兩者中。

## Wi-Fi

iOS 裝置在開箱之後即可安全地連接到公司或訪客 Wi-Fi 網路，使用者無論在學校或路上都可以輕鬆快速地加入可用的無線網路。

### 加入 Wi-Fi

使用者可以設定讓 iOS 裝置自動加入可用的 Wi-Fi 網路。iOS 裝置會快速連接到要求輸入登入認證資訊或其他資訊的 Wi-Fi 網路 (透過 Wi-Fi 設定或「郵件」等 app)，不需要另外開啟瀏覽器工作時段。而低耗電且持續的 Wi-Fi 連線也可讓 app 使用 Wi-Fi 網路來傳送推播通知。

### WPA2 企業級

iOS 支援 WPA2 企業級等符合業界標準的無線網路通訊協定，確保使用者可以從 iOS 裝置安全連接公司無線網路。WPA2 企業級使用 128 位元 AES 加密 (經過證明的區塊式加密方法)，可為使用者提供最高等級的保障，確保他們的資料持續受到保護。

iOS 支援 802.1X，因此可整合至各種 RADIUS 認證環境中。iOS 上支援的 802.1X 無線認證方式包括 EAP-TLS、EAP-TTLS、EAP-FAST、PEAPv0、PEAPv1 及 LEAP。

### 漫遊

若要在大型企業 Wi-Fi 網路上漫遊，iOS 支援 802.11k 和 802.11r。802.11k 會利用來自 Wi-Fi 基地台的報告，協助 iOS 裝置在各個基地台之間切換，而 802.11r 可以在裝置切換基地台時簡化 802.1X 認證過程。

若要快速地設定和部署，可以使用設定描述檔或 MDM 來設定無線網路、安全功能、代理伺服器和認證設定。

## 虛擬專用網路

iOS 透過已行之多年的業界標準虛擬專用網路 (VPN) 通訊協定，讓使用者安全地連接公司專用網路。iOS 一開箱即可支援 Cisco IPSec、L2TP over IPSec 與 PPTP。如果您的組織支援這些協定，可以直接將 iOS 裝置連接到您的 VPN，無需進行其他網路設定或使用協力廠商 app。

此外，iOS 也支援常見 VPN 供應商的 SSL VPN。使用者只要從 App Store 下載由這些公司開發的 VPN 用戶端 app，就可以開始作業。和 iOS 所支援的其他 VPN 通訊協定一樣，SSL VPN 也可以在裝置上手動設定，或透過設定描述檔或 MDM 來設定。

iOS 支援 IPv6、代理伺服器和分割通道等業界標準的技術，讓使用者在連接公司網路時有多樣化的 VPN 選擇。而且 iOS 可以使用多種認證方式，包括密碼、雙因素 Token 和數位憑證。為了簡化憑證式認證環境裡的連線，iOS 支援「隨選即用 VPN」，以便在需要時啟用 VPN 工作階段來連接特定網域。

在 iOS 7 裡，可以設定個別的 app 使用 VPN 連線，裝置上的其他 app 則不受影響。這樣可以確保公司資料永遠是透過 VPN 連線傳送，而其他資料 (如員工從 App Store 下載的私人 app) 則否。詳細資訊請參閱本章後面的「App 層級的 VPN」一節。

### 支援的通訊協定與認證方式

**SSL VPN。**支援使用密碼、雙因素 Token 與憑證的使用者認證。

**Cisco IPSec。**支援使用密碼與雙因素 Token 的使用者認證，以及使用共享密鑰與憑證的機器認證。

**L2TP over IPSec。**支援使用 MS-CHAP v2 密碼與雙因素 Token 的使用者認證，以及使用共享密鑰的機器認證。

**PPTP。**支援使用 MS-CHAP v2 密碼與雙因素 Token 的使用者認證。

### SSL VPN 用戶端

多家 SSL VPN 供應商皆已製作了 app，能協助使用者設定 iOS 裝置來與其解決方案搭配使用。若要設定裝置使用特定的解決方案，請安裝相關的 app，您也可以選擇提供包含必要設定的設定描述檔。SSL VPN 解決方案包括：

- **Juniper Junos Pulse SSL VPN。**iOS 支援 Juniper Networks SA Series SSL VPN Gateway (執行 6.4 版或以上版本) 與 Juniper Networks IVE 套件 7.0 或以上版本。如要設定，請從 App Store 下載安裝 Junos Pulse app。

更多資訊請參閱 Juniper Networks application note。

- **F5 SSL VPN**。iOS 支援 F5 BIG-IP Edge Gateway、Access Policy Manager 和 FirePass SSL VPN 解決方案。如要設定，請從 App Store 下載安裝 F5 BIG-IP Edge Client app。

  更多資訊請參閱 F5 技術簡介文件：Secure iPhone Access to Corporate Web Applications。

- **Aruba Networks SSL VPN**。iOS 支援 Aruba Networks Mobility Controller。如要設定，請從 App Store 下載安裝 Aruba Networks VIA app。

  相關聯絡資訊請參閱 Aruba Networks 網站。

- **SonicWALL SSL VPN**。iOS 支援 10.5.4 或以上版本的 SonicWALL Aventall E-Class Secure Remote Access 應用程式、5.5 或以上版本的 SonicWALL SRA 應用程式和執行 SonicOS 5.8.1.0 或以上版本的 SonicWALL Next-Generation Firewall 應用程式，包含 TZ、NSA 和 E-Class NSA。如要設定，請從 App Store 下載安裝 SonicWALL Mobile Connect app。

  相關聯絡資訊請參閱 SonicWALL 網站。

- **Check Point Mobile SSL VPN**。iOS 支援包含完整 Layer-3 VPN 通道的 Check Point Security Gateway。如要設定，請從 App Store 下載安裝 Check Point Mobile app。

- **OpenVPN SSL VPN**。iOS 支援 OpenVPN Access Server、Private Tunnel 和 OpenVPN Community。如要設定，請從 App Store 下載安裝 OpenVPN Connect app。

- **Palo Alto Networks GlobalProtect SSL VPN**。iOS 支援 Palo Alto Networks 的 GlobalProtect 匣道器。如要設定，請從 App Store 下載安裝 GlobalProtect for iOS app。

- **Cisco AnyConnect SSL VPN**。iOS 支援執行軟體映像檔 8.0(3).1 或以上版本的 Cisco Adaptive Security Appliance (ASA)。如要設定，請從 App Store 下載安裝 Cisco AnyConnect app。

## VPN 設定準則

### Cisco IPSec 設定準則

請使用這些準則來設定您的 Cisco VPN 伺服器，來和 iOS 裝置搭配使用。iOS 支援以 7.2.x 軟體或以上版本設定的 Cisco ASA 5500 Security Appliances 和 PIX Firewalls。建議使用最新的軟體 (8.0.x 或以上版本)。iOS 也支援 Cisco IOS VPN 路由器與 IOS 12.4(15)T 或以上版本。VPN 3000 Series Concentrators 不支援 iOS VPN 功能。

### 設定代理伺服器

您也可以指定一台 VPN 代理伺服器供所有設定使用。若要設定單一代理伺服器以用於所有連線，請選擇「手動」設定，並提供位址、連接埠與認證 (如有需要)。若要為裝置提供使用 PAC 或 WPAD 的自動代理伺服器設定描述檔，請選擇「自動」設定。針對 PAC，請指定 PAC 檔的 URL。針對 WPAD，iOS 會向 DHCP 和 DNS 詢問適合的設定。

**認證方式**

iOS 支援下列認證方式：

- 使用預先共享的密鑰 IPSec 認證加上使用者認證 (透過 xauth)。
- IPSec 認證的用戶端與和伺服器憑證加上選擇性使用者認證 (透過 xauth)。
- 混合認證，其中伺服器會提供憑證，而用戶端提供預先共享的密鑰來進行 IPSec 認證。使用者認證需要透過 xauth。
- 使用者認證是透過 xauth 提供，並包含下列認證方式：
  - 使用者名稱與密碼
  - RSA SecurID
  - CRYPTOCard

**認證群組**

Cisco Unity 通訊協定使用認證群組，依據一組通用的認證參數和其他參數來將使用者分組。您應該要 為 iOS 使用者建立一個認證群組。針對預先共享的密鑰和混合認證，群組名稱必須使用群組的共享密鑰 (預先共享密鑰) 做為群組密碼在裝置上完成設定。

在使用憑證認證時，不會使用共享的密鑰。使用者群組會依據憑證中的欄位決定。Cisco 伺服器設定可用來將憑證中的欄位對應到使用者群組。

RSA-Sig 在 ISAKMP 優先順序列表上應具有最高的優先順序。

**憑證**

在設定和安裝憑證時，請確定下列事項：

伺服器識別身分憑證在主題替代名稱 (SubjectAltName) 欄位中，必須包含伺服器的 DNS 名稱和 (或) IP 位址。裝置會使用此資訊來驗證憑證屬於該伺服器。為了取得更大彈性，您可以使用萬用字元來指定 SubjectAltName，以符合個別的區段，例如 vpn.*.mycompany.com。若未指定 SubjectAltName，則 DNS 名稱可以放在一般名稱欄位中。

簽署伺服器憑證之 CA 的憑證必須安裝在裝置上。如果其不是根憑證，請安裝信任鏈的剩餘項目以便信任憑證。若您使用用戶端憑證，請確定受信任之 CA 憑證 (簽署用戶端的憑證) 已安裝在 VPN 伺服器上。在使用憑證式認證時，請確定已設定伺服器依據用戶端憑證中的欄位來識別使用者的群組。

憑證和憑證授權必須有效 (例如，尚未過期)。不支援由伺服器傳送憑證鏈，您應將其關閉。

**IPSec 設定**

請使用下列 IPSec 設定：

- **模式。**通道模式
- **IKE 交換模式。**預先共享密鑰與混合認證適用「嚴格模式」，或憑證認證適用「主要模式」。
- **加密演算法。**3DES、AES-128、AES-256。
- **認證演算法。** HMAC-MD5、HMAC-SHA1。
- **Diffie-Hellman 群組。**預先共享密鑰和混合認證需有 Group 2。若為憑證認證，請使用 Group 2 搭配 3DES 和 AES-128。請使用 Group 2 或 5 搭配 AES-256。
- **PFS (Perfect Forward Secrecy)。**若為 IKE 階段 2，如果使用 PFS，則 Diffie-Hellman 群組必須與 IKE 階段 1 使用的群組相同。
- **模式設定。**必須啟用。
- **斷線端偵測 (DPD)。**建議使用。
- **標準虛擬網址轉換。**已支援且可啟用 (不支援 IPSec over TCP)。
- **負載平衡。**已支援且可啟用。
- **階段 1 的更新密鑰。**目前不支援。建議您將伺服器上的更新密鑰時間設為一小時。
- **ASA 位址遮罩。**確定所有裝置的位址庫遮罩並未設定，或者設為 255.255.255.255，例如：asa(config-webvpn)# ip local pool vpn_users 10.0.0.1-10.0.0.254 遮罩 255.255.255.255。

若您使用建議的位址遮罩，可能會忽略一些由 VPN 設定所假設的路徑。若要避免此情形，請確定您的路徑規劃表包含所有必要的路徑，並確認子網路位址在部署前可供連接。

## 其他支援的功能

- **應用程式版本。**用戶端軟體版本會傳送給伺服器，依據裝置軟體版本允許伺服器接受或拒絕連線。
- **提示標語。**提示標語 (如果伺服器上有設定的話) 會顯示在裝置上，而使用者必須接受或中斷連線。
- **分割通道。**支援分割通道。
- **分割 DNS。**支援分割 DNS。
- **預設網域。**支援預設網域。

### 隨選即用 VPN

「隨選即用 VPN」能讓 iOS 自動建立安全連線，無需經由使用者操作。iOS 會根據設定描述檔裡所定義的規則，在需要時自動啟動 VPN 連線。

在 iOS 7 裡，「隨選即用 VPN」的設定是透過設定描述檔的 VPN 承載資料裡的 OnDemandRules 鍵值。規則的套用分為兩個階段：

- **網路偵測階段。**此階段要套用的規則，是在裝置的主要網路連線改變時，用來定義 VPN 必要條件的規則。
- **連線評估階段。**此階段要套用的規則，是在根據需求來請求連接網域名稱時，用來定義 VPN 必要條件的規則。

例如，規則可以用來：

- 辨別 iOS 裝置是連接到內部網路，不需要使用 VPN。
- 辨別 iOS 裝置正連接到未知的 Wi-Fi 網路，所有網路活動都必須使用 VPN。
- 當 DNS 無法取得要求的特定網域名稱時，必須使用 VPN。

#### 網路偵測階段

當裝置的主要網路介面改變，例如 iOS 裝置改用了不同的 Wi-Fi 網路，或從 Wi-Fi 切換成行動網路時，iOS 就會評估「隨選即用 VPN」規則。如果主要介面是虛擬介面 (如 VPN 介面)，則會忽略「隨選即用 VPN」規則。

每一組 (字典) 裡的比對規則必須完全符合，才會執行相關動作；如果有任何一項規則不符，評估會跳到陣列中的下一個字典，直到 OnDemandRules 陣列裡的字典都接受過評估為止。

最後一個字典應該要定義「預設」設定，也就是沒有任何比對規則，而只有「動作」。這樣會偵測到所有未符合之前規則的連線。

#### 連線評估階段

使用者可以根據對於特定網域的連線要求，在需要時啟動 VPN，而不是只根據網路介面中斷連接或連接 VPN。

#### 隨選即用的比對規則

請指定一或多個下列比對規則：

- **InterfaceTypeMatch。**選用。Wi-Fi 或行動網路的字串。當主要介面硬體屬於指定的類型，即符合此規則。
- **SSIDMatch。**選用。與目前網路做比對的 SSID 陣列。如果網路不是 Wi-Fi 網路，或其 SSID 未出現在列表裡，即不符合此規則。若要忽略 SSID，請忽略此鍵值及其陣列
- **DNSDomainMatch。**選用。搜尋網域字串的陣列。如果目前主要網路所設定的 DNS 搜尋網域包含於此陣列裡，即符合此規則。支援萬用前置碼 (*)，例如 *.example.com 即為 anything.example.com。
- **DNSServerAddressMatch。**選用。DNS 伺服器位址字串的陣列。如果主要介面目前所設定的所有 DNS 伺服器位址都在陣列裡，即符合此規則。支援萬用字元 (*)，如 1.2.3.* 即等於任何前置碼為 1.2.3. 的 DNS 伺服器。
- **URLStringProbe。**選用。探測聯繫可能性的伺服器。不支援轉址。URL 應指向信任的 HTTPS 伺服器。裝置會傳送 GET 要求，以驗證伺服器是否可連接。

**動作**

當所有指定的比對規則的評估皆符合時，此鍵值將定義 VPN 的行為。此鍵值為必要。「動作」鍵值的參數如下：

- **Connect。**在下一次嘗試連接網路時，無條件啟動 VPN 連線。
- **Disconnect。**中止 VPN 連線，且不要視需要啟動任何新連線。
- **Ignore。**繼續所有既有的 VPN 連線，但不要視需要啟動任何新連線。
- **Allow。**針對安裝 iOS 6 或以上版本的 iOS 裝置。請參閱本節後面的「關於向下相容性」。
- **EvaluateConnection。**在每次嘗試連線時評估 ActionParameter。使用此參數時，必須搭配 ActionParameter (如下所述) 來指定評估規則。

**ActionParameter**

包含下述鍵值的字典陣列，評估時會依照出現的先後順序。必須在「動作」為 EvaluateConnection 時使用。

- **Domains。**必要。用來定義需要評估的網域的字串陣列。支援萬用前置碼，如 *.example.com。
- **DomainAction。**必要。根據網域來定義 VPN 行為。DomainAction 鍵值的參數包括：
  - **ConnectIfNeeded。**如果 DNS 網域解析失敗，如 DNS 伺服器表示無法解析網域名稱，或 DNS 回應被轉址，或是連線失敗或逾時，則會啟動 VPN。
  - **NeverConnect。**針對這些網域不要啟動 VPN。

當 DomainAction 為 ConnectIfNeeded 時，您也可以在連線評估字典裡指定下列鍵值：

- **RequiredDNSServers。**選用。用來解析網域的 DNS 伺服器的 IP 位址陣列。這些伺服器不需要包含在裝置目前的網路設定裡。如果無法聯繫這些 DNS 伺服器，就會啟動 VPN，並設定一個內部 DNS 伺服器或信任的外部 DNS 伺服器。
- **RequiredURLStringProbe。**選用。供探測用的 HTTP 或 HTTPS (建議使用) URL，探測時使用 GET 要求。如果此伺服器的 DNS 解析沒問題，探測也一定會成功。若探測失敗，即會啟動 VPN。

**關於向下相容性**

在 iOS 7 之前，網域啟動規則的設定是透過名為 OnDemandMatchDomainAlways、OnDemandMatchDomainOnRetry 和 OnDemandMatchDomainNever 的網域陣列。iOS 7 仍支援 OnRetry 與 Never 的情況，但較傾向使用 EvaluateConnection 動作。

若要建立一個可同時用於 iOS 7 與之前版本的描述檔，請同時使用新的 EvaluateConnection 鍵值和 OnDemandMatchDomain 陣列。無法識別 EvaluateConnection 的舊版 iOS 會使用舊的陣列，而 iOS 7 和以上版本則會使用 EvaluateConnection。

指定 Allow 動作的舊版設定描述檔可以在 iOS 7 裡使用，但 OnDemandMatchDomainsAlways 網域除外。

## App 層級的 VPN

iOS 7 新增了為個別 app 建立 VPN 連線的功能，可以針對通過 VPN 的資料進行更精細的控制。在整個裝置共用的 VPN 連線裡，所有資料無論來源為何，都是透過專用網路傳輸。當組織裡有愈來愈多人使用私人裝置時，「App 層級的 VPN」可以為內部使用的 app 提供安全的網路連線，同時又能維護私人裝置活動的隱私。

「App 層級的 VPN」能讓受行動裝置管理 (MDM) 的每個 app 透過安全通道與專用網路通訊，並能阻擋裝置上其他非託管的 app 使用專用網路。此外，託管的 app 可以設定使用不同的 VPN 連線，以進一步保護資料。例如，銷售報價 app 可以使用與應付帳款 app 完全不同的數據中心，而使用者私下瀏覽網頁時則使用公用的 Internet。這種在 app 層級隔離流量的功能可以將私人資料與屬於組織的資料分開來。

要使用「App 層級的 VPN」，app 必須透過 MDM 管理，並使用標準的 iOS 網路 API。「App 層級的 VPN」是透過 MDM 設定檔來設定，檔案中指定了哪些 app 和 Safari 網域可以使用這組設定。更多關於 MDM 的資訊請參閱「第 3 章：設定與管理」

## 單一登入 (SSO)

在 iOS 7 裡，app 可以利用您內部現有的透過 Kerberos 的單一登入基礎設施。單一登入只要求使用者輸入一次密碼，可以節省使用者的時間。它也可以確保密碼絕對不會透過無線方式傳輸，藉此提高每日使用 app 的安全性。

iOS 7 使用的 Kerberos 認證系統符合業界標準，也是全球最普遍採用的單一登入技術。如果您有 Active Directory、eDirectory 或 OpenDirectory，很可能已經具備可供 iOS 7 使用的 Kerberos 系統。iOS 裝置需要能夠透過網路連線來聯絡 Kerberos 服務，以便認證使用者。

### 支援的 app

iOS 能為使用 NSURLConnection 或 NSURLSession 類別來管理網路連線與認證的所有 app 提供 Kerberos 單一登入 (SSO) 的彈性支援。Apple 為所有開發者提供這些高階架構，讓他們的 app 可以無縫進行網路連線。Apple 也提供 Safari 做為範例，協助您以原生方式開始使用 SSO 網站。

### 設定 SSO

單一登入的設定要使用設定描述檔，而設定描述檔可以選擇以手動安裝或透過 MDM 管理。SSO 帳號的承載資料可以自由設定。SSO 可以開放給所有 app 使用，或依據 app 識別碼、服務 URL 或同時依據這兩者來予以限制。

比對 URL 時，是使用簡單的型態比對，且 URL 必須以 http:// 或 https:// 為開頭。比對時看的是完整的 URL，所以請確定 URL 完全一樣。舉例來說，https://www.example.com/ 的 URLPrefixMatches 值就和 https://www.example.com:443/ 不同。您可以為安全或一般的 HTTP 服務指定 http:// 或 https:// 來限制 SSO 的使用。例如，使用 https:// 的 URLPrefixMatches 值會讓 SSO 帳號只能用於安全的 HTTPS 服務。如果 URL 比對型態並未以斜線 (/) 結尾，iOS 會自動加上斜線 (/)。

AppIdentifierMatches 陣列必須包含符合 app 套件識別碼的字串。這些字串可以是完全一致的 (如 com.mycompany.myapp)，或使用萬用字元 (*) 與前置碼來做為套件識別碼的比對項目。萬用字元必須出現在句點 (.) 後面，且只能位於字串尾端 (如 com.mycompany.*)。如果使用了萬用字元，所有以此前置碼做為套件識別碼開頭的 app 都具有帳號的取用權限。

## 數位憑證

數位憑證是一種身分識別形式，可提供簡化的認證、資料完整性以及加密功能。數位憑證包括公用密鑰、使用者相關資訊及核發該憑證的憑證授權組織。iOS 支援數位憑證，讓組織能夠以安全、簡化的方式存取內部服務。

憑證有各式各樣的使用方式。以數位憑證簽署資料，有助於確保資訊不被更改。憑證還可用於確保作者或「簽名者」的身分。此外，它們也能用來為設定描述檔及網路通訊加密，進一步保護機密或私人資訊。

例如，Safari 瀏覽器會檢查 X.509 數位憑證的有效性，並設定具有 256 位元 AES 加密的安全區段。這樣可以確認網站的身分是否合法，以及與網站之間的通訊是否受到保護，以避免私人與機密資料遭到攔截。

支援的憑證和識別身分格式：

- iOS 支援具有 RSA 密鑰的 X.509 憑證。
- 可辨識 .cer、.crt、.der、.p12 與 .pfx 等附檔名。

### 在 iOS 裡使用憑證

#### 根憑證

iOS 一開箱即包含多個預先安裝的根憑證。更多資訊請參閱這篇 Apple 技術支援文章裡的列表。

如果預先安裝的憑證遭盜用，iOS 可以透過無線方式更新憑證。若要停用此功能，可以啟用能避免以無線傳輸方式更新憑證的限制。

如果您使用的不是預先安裝的根憑證，像是您的組織所製作的自簽根憑證，可以透過下列方式來發佈。

#### 發佈與安裝憑證

發佈憑證到 iOS 裝置很簡單。收到憑證時，使用者只需輕點即可查看內容，而後再輕點將憑證添加到裝置中。當安裝識別身分憑證之後，系統會提示使用者輸入用來保護識別身分的密碼。如果憑證的真實性無法驗證，憑證會顯示為不受信任，使用者可以決定是否要將憑證加入到裝置裡。

#### 透過設定描述檔安裝憑證

如果是使用設定描述檔發佈 Exchange、VPN 或 Wi-Fi 等公司服務的設定，可以將憑證加入到描述檔裡來簡化部署。這也包含透過 MDM 發佈憑證的功能。

#### 透過「郵件」或 Safari 安裝憑證

如果是透過電子郵件傳送憑證，憑證會以附件顯示。也可以使用 Safari 從網頁下載憑證。您可以將憑證放在安全的網站上，再將 URL 提供給使用者，讓他們下載憑證到裝置上。

#### 移除與撤銷憑證

要手動移除安裝的憑證，請選擇「設定」(Settings) >「一般」(General) >「描述檔」(Profiles)，再選擇要移除的憑證。如果使用者移除了連接帳號或網路所需的憑證，裝置將無法連接這些服務。

行動裝置管理伺服器可以檢視裝置上所有憑證，也可以移除它所安裝的任何憑證。

此外也支援以「線上憑證狀態通訊協定」(OCSP) 與 CRL (憑證撤銷列表) 通訊協定來檢查憑證的狀態。使用經 OCSP 或 CRL 認可的憑證時，iOS 會定期進行驗證，以確保憑證未被撤銷。

## Bonjour

Bonjour 是 Apple 推出的零設定網路通訊協定，這款符合共通標準的協定能讓裝置找到網路上的服務。iOS 裝置使用 Bonjour 來尋找與 AirPrint 相容的印表機，以及與 AirPlay 相容的裝置，如 Apple TV。某些點對點 app 也要求使用 Bonjour。您必須確定您的網路基礎設施與 Bonjour 都經過正確的設定，可以順利搭配使用。

iOS 7.1 裝置也可以透過 Bluetooth 搜尋 AirPlay 來源。一旦找到相容的 Apple TV，AirPlay 資料就會透過 Wi-Fi 網路傳輸。若要啟用 Bluetooth 搜尋功能，必須使用 Apple TV 6.1 或以上版本，且 iOS 裝置與 Apple TV 必須連接相同的子網路，才能播放或鏡像輸出內容。

更多關於 Bonjour 的資訊，請參閱這個 Apple 網頁。

# 第 2 章：
# 安全性

iOS 內建多層級的安全防護功能。此設計可讓 iOS 裝置安全地存取網路服務，並保護重要資料。iOS 針對傳輸中的資料強式加密，採用經過證明的認證方式存取企業服務，並且為裝置中儲存的所有資料進行硬碟加密。iOS 也會使用能以無線傳輸方式傳送並執行的密碼規則來提供安全保護。另外，如果裝置落入他人手中，使用者和 IT 管理者可以啟動遠端清除指令來清除私人資訊。

針對企業用途考量 iOS 的安全性時，了解下列資訊會有很大的幫助：

- **裝置控制。**防止他人未經授權使用裝置的方法
- **加密與資料保護。**保護裝置裡的資料，即使裝置遺失或遭竊，資料也能受到保護
- **網路安全性。**網路通訊協定以及為傳輸中的資料加密
- **App 安全性。**讓 app 安全地執行，同時無損平台的完整性
- **Internet 服務。**Apple 用以進行傳訊、同步與備份的網路基礎設施

這些功能可協同合作，提供一個安全的行動運算平台。

## 裝置安全性

建立嚴密的 iOS 存取政策是保護企業資訊的關鍵。要防止未經授權的存取，首要步驟就是設定裝置密碼，而 iOS 的裝置密碼可以透過無線傳輸方式設定與執行。iOS 裝置藉由每位使用者所建立的獨有密碼來產生強大的加密 密鑰，為裝置上的郵件與機密的應用程式資料提供高度保護。此外，若必須在 IT 環境中採用特定的設定、規則或限制時，iOS 也提供了安全的裝置設定方式。這些方式提供了彈性的選項，為授權的使用者建立標準層級的保護。

### 密碼規則

裝置密碼能防止未經授權的使用者存取資料，或取得裝置的使用權限。iOS 為滿足您對安全的需求，提供了全面性的密碼規則，包括逾時期間、密碼強度，以及密碼必須更換的頻率。

**iOS 支援以下密碼規則：**

- 要求裝置設定密碼
- 要求密碼需包含字母與數字
- 最短密碼長度
- 最少複雜字元數量
- 最長密碼使用期限
- 自動鎖定前的時間
- 密碼記錄
- 裝置鎖定的寬限期
- 最大嘗試失敗次數

### 規則的執行

規則可以放入設定描述檔，隨之發佈給使用者進行安裝。您可以定義描述檔的內容，例如在輸入管理者密碼後才能刪除描述檔，或是將描述檔鎖定在裝置上，必須完全清除所有裝置內容後才能移除。此外，您可以透過行動裝置管理 (MDM) 解決方案直接將規則推播到裝置上，從遠端設定密碼。這樣一來，規則的執行與更新都不需要經過使用者操作。

如果設定裝置取用 Microsoft Exchange 帳號，Exchange ActiveSync 規則會透過無線傳輸方式推播到裝置。可用的規則會根據 Exchange ActiveSync 和 Exchange Server 的版本而變。如果同時使用了 Exchange 和 MDM 規則，則會套用其中較嚴格的規則。

### 安全裝置設定

設定描述檔是 XML 檔案，其中含有裝置安全性規則與限制、VPN 設定資訊、Wi-Fi 設定、電子郵件和行事曆帳號，以及允許 iOS 裝置與您的 IT 系統搭配使用的認證身分。在設定描述檔裡建立密碼規則加上裝置的設定，能確保組織裡的裝置都經過妥善的設定，且符合 IT 部門所制定的安全標準。此外，由於設定描述檔可以加密與鎖定，其中的設定皆無法被移除、更動或與他人共用。

設定描述檔可同時經過簽署與加密。簽署設定 描述檔能確保它所套用的設定無法以任何方式變更。為設定描述檔加密可以保護檔案的內容，並能確保只安裝在目標裝置上。設定描述檔使用 CMS (加解密訊息語法，RFC 3852) 進行加密，可支援 3DES 與 AES-128。

初次發佈加密的設定描述檔時，可以使用 Apple Configurator 透過 USB 來安裝，或使用「無線描述檔傳輸與設定」通訊協定或 MDM 等無線方式來安裝。後續的加密設定描述檔可以透過電子郵件附件傳送、放在使用者可以取用的網站上，或透過 MDM 解決方案推播到裝置。

更多資訊請參閱 iOS Developer Library 網站上的 Over-the-Air Profile Delivery and Configuration protocol。

### 裝置限制

裝置限制會判斷使用者可以存取裝置中的哪些功能。一般來說，這包括會用到網路的應用程式 (例如 Safari、YouTube 或 iTunes Store)，但是限制也可以控制 app 安裝或相機的使用等裝置功能。限制能夠讓您依照自己的需求條件來設定裝置，同時能讓使用者以符合組織內部規則的方式來使用裝置。要設定限制，可以在每台裝置上手動進行，或透過設定描述檔來套用，或是透過 MDM 解決方案從遠端建立。此外，密碼規則、相機或網頁瀏覽等限制可以透過 Microsoft Exchange Server 2007 和 2010 以無線傳輸方式執行。您也可以設定限制來防止使用者在不同帳號中搬移郵件，或將某個帳號裡收到的郵件轉寄到其他帳號。

關於 iOS 支援的限制，詳情請參閱「附錄 B」。

# 加密與資料保護

對於任何擁有敏感資訊的環境，保護 iOS 裝置上所儲存的資料是相當重要的。iOS 除了為傳輸中的資料加密，也為裝置上所儲存的所有資料提供硬體加密，此外也為電子郵件與應用程式資料提供額外的加密，以進一步保護資料。

## 加密

iOS 裝置提供硬體加密功能。硬體加密採用 256 位元 AES 來保護裝置中的所有資料。加密會保持啟用狀態且無法停用。此外，備份至使用者電腦中的 iTunes 資料也可以進行加密。這個功能可由使用者啟用，或使用設定描述檔中的裝置限制設定來執行。iOS 的郵件也支援 S/MIME，讓使用者能夠檢視和傳送加密的電子郵件訊息。

iOS 7 和 iOS 6 裡的加密模組經過驗證，符合美國聯邦資訊處理標準 (FIPS) 140-2 第 1 級規範。這也確保了正確使用 iOS 加密服務的 Apple app 與協力廠商 app 都具備完整的加密程序。

更多資訊請參閱 iOS 產品安全性：驗證與指導方針以及 iOS 7：Apple FIPS iOS 加解密模組 v4.0。

## 資料保護

使用 iOS 內建的資料保護功能，可進一步保護裝置上存放的電子郵件訊息與附件。資料保護會搭配使用 iOS 裝置中每位使用者獨有的裝置密碼以及硬體加密功能，以產生強大的加密密鑰。在裝置鎖定時，此密鑰可防止他人存取資料，甚至當裝置受到入侵時，仍可確保重要資訊安全無虞。

若要開啟資料保護功能，只要在裝置中建立密碼即可。資料保護的效用取決於強式密碼，因此，在建立密碼規則時，要求並強制執行比四位數密碼更為嚴謹的密碼是相當重要的。使用者可以透過檢視密碼設定畫面，來確認裝置中的資料保護是否已啟用。行動裝置管理解決方案也可以查詢裝置中的這項資訊。

資料保護 API 也可供開發人員使用，並可用來保護 App Store app 或企業自行研發的內部專用 App 的資料安全。自 iOS 7 起，應用程式儲存的資料在預設上屬於「初次使用者認證前保護」安全類別，類似桌上型電腦上的全磁碟加密，可防止資料遭到利用重新開機進行的攻擊。

**注意**：如果裝置曾從 iOS 6 升級，原本儲存的資料並未轉換到此新類別。若將 app 移除再重新安裝，即可受到新類別的保護。

## Touch ID

Touch ID 是 iPhone 5s 內建的指紋感應系統，能讓使用者在高度的安全保護下，以更輕鬆快速的方式存取裝置。這項深具前瞻性的技術能從任何角度讀取指紋，並能隨時間學習認識使用者的指紋，且每次使用時，感應器都會學習辨識重疊的指腹，持續擴大能識別的指紋範圍。

Touch ID 讓使用更長、更複雜的密碼變得更為可行，因為使用者不需要經常輸入。Touch ID 也能解決使用密碼鎖定的不便之處，但做法不是取而代之，而是在縝密的範圍與時間限制內，安全地提供裝置的取用權限。

啟用 Touch ID 時，iPhone 5s 會在使用者按下「睡眠/喚醒」按鈕時立即鎖定。只以密碼做為安全功能時，許多使用者都會設定解鎖的寬限期，以避免在每次使用裝置時都要輸入密碼。若啟用 Touch ID，iPhone 5s 在每次進入睡眠時都會鎖定，並在被喚醒時要求提供指紋 (也可以選擇輸入密碼)。

Touch ID 與 Apple A7 晶片內所裝配的協同處理器 Secure Enclave 搭配運作。Secure Enclave 本身具有受到保護並加密的記憶體空間，能安全地與 Touch ID 感應器溝通。當 iPhone 5s 鎖定時，「資料保護」層級「完整」的密鑰是由 Secure Enclave 的加密記憶體裡的密鑰保護。這個密鑰最多保留 48 小時，如果 iPhone 5s 重新開機或使用了五次無法識別的指紋，密鑰會被丟棄。如果 iPhone 5s 能識別指紋，Secure Enclave 會提供密鑰來解開「資料保護」密鑰，而裝置就會解鎖。

### 遠端清除

iOS 支援遠端清除。如果裝置遺失或遭竊，管理者或裝置持有人可以發送遠端清除指令，移除所有資料並停用裝置。如果裝置使用 Exchange 帳號進行設定，管理者可以透過 Exchange 管理主控台 (Exchange Server 2007) 或是 Exchange ActiveSync 行動系統管理網路工具 (Exchange Server 2003 或 2007) 啟動遠端清除。Exchange Server 2007 的使用者也可以透過 Outlook Web Access 啟動遠端清除。即使未使用 Exchange 企業服務，也可以透過 MDM 解決方案或使用 iCloud 的「尋找我的 iPhone」功能來啟動遠端清除指令。

### 本機清除

裝置可設定成數度嘗試密碼失敗後，自動啟動本機清除。這樣能防範他人以暴力破解密碼的方式取得裝置的使用權限。若已建立密碼，使用者就能直接在設定裡進行本機清除。依照預設，iOS 會在 10 次嘗試輸入密碼失敗後自動清除裝置。和其他密碼規則一樣，若要設定嘗試失敗的次數上限，可以透過設定描述檔、MDM 伺服器，或透過 Microsoft Exchange ActiveSync 規則以無線傳輸方式執行。

### 「尋找我的 iPhone」與「啟用鎖定」

如果裝置遺失或遭竊，停用並清除裝置是很重要的一步。在 iOS 7 裡，若啟用了「尋找我的 iPhone」，則一定要輸入持有人的 Apple ID 認證資訊才能啟用裝置。建議您監管組織所持有的裝置，或制定相關規則來讓使用者停用功能，這樣當組織要將裝置指定給其他人使用時，就不會受到「尋找我的 iPhone」的影響。

在 iOS 7.1 或以上版本中，當使用者開啟「尋找我的 iPhone」時，您可以使用相容的 MDM 解決方案來啟用「啟用鎖定」。MDM 解決方案可在「啟用鎖定」啟用時儲存旁路代碼，然後在您需要清除裝置並將它部署給新使用者時，使用此代碼自動解除「啟用鎖定」。詳情請參閱您的 MDM 解決方案文件。

更多關於「尋找我的 iPhone」與「啟用鎖定」的資訊，請參閱 iCloud 支援文章以及行動裝置管理與尋找我的 iPhone 啟用鎖定。

**網路安全性**

- 內建 Cisco IPSec、L2TP、PPTP VPN
- 透過 App Store app 使用 SSL VPN
- 使用 X.509 憑證的 SSL/TLS
- 使用 802.1X 認證的 WPA/WPA2 企業級
- 憑證型驗證
- RSA SecurID、CRYPTOCard

**VPN 通訊協定**

- Cisco IPSec
- L2TP/IPSec
- PPTP
- SSL VPN

**認證方式**

- 密碼 (MSCHAPv2)
- RSA SecurID
- CRYPTOCard
- X.509 數位憑證
- 共享密鑰

**802.1X 認證通訊協定**

- EAP-TLS
- EAP-TTLS
- EAP-FAST
- EAP-SIM
- PEAP v0、v1
- LEAP

**支援的憑證格式**

iOS 支援具有 RSA 密鑰的 X.509 憑證。可辨識 .cer、.crt 與 .der 等副檔名。

## 網路安全性

行動使用者必須要能隨時隨地存取企業資訊網路，不過，確保使用者具有授權且資料在傳輸期間可受到保護，也是相當重要的。iOS 提供經過證明的技術，可在 Wi-Fi 與行動資料網路連線方面達成這些安全性目標。

除了既有基礎設施之外，每一次的 FaceTime 通話和 iMessage 對談都會全程加密。iOS 替每位使用者建立各自不同的 ID，以確保溝通都經適當加密、排定及連接。

### VPN

許多企業環境都建立了某種形式的虛擬專用網路 (VPN)。這些安全的網路服務可能早已部署，而且通常只需要基本的安裝與設定，就可以搭配 iOS 裝置一起運作。iOS 一開箱即整合了多種常用的 VPN 技術。詳情請參閱第 1 章「虛擬專用網路」一節。

### SSL/TLS

iOS 支援 SSL v3 以及「傳輸層安全性」(TLS v1.0、1.1 與 1.2)。Safari、「行事曆」、「郵件」與其他 Internet 應用程式會自動啟動這些機制，以在 iOS 與企業服務間啟用加密的通訊頻道。

### WPA/WPA2

iOS 支援 WPA2 企業級，為您的企業無線網路提供經過認證的存取。WPA2 使用 128 位元 AES 加密，能在使用者透過 Wi-Fi 網路連線進行通訊時保護其資料，為使用者提供最高層級的安全防護。iOS 也支援 802.1X，可讓 iPhone 與 iPad 整合至各種 RADIUS 認證環境中。

## App 安全性

iOS 是以安全性為設計核心的平台。它採用沙箱技術為應用程式提供執行階段防護，並要求應用程式簽署憑證以防止 app 遭到竄改。它的架構也可以確保應用程式和網路服務認證資訊安全地儲存在名為「鑰匙圈」的加密儲存位置裡。iOS 也為開發人員提供「常用加密」架構，可用來為儲存的應用程式資料加密。

### 執行階段保護

裝置上的 app 皆以沙箱模式執行，無法存取其他 app 所儲存的資料。此外，檔案系統、資源與核心會與使用者的應用程式空間加以區隔。如果 app 需要存取來自其他 app 的資料，只能使用由 iOS 提供的 API 與服務。iOS 也能防止程式碼產生。

### 強制程式碼簽名

所有 iOS app 都必須進行簽署。裝置隨附的 app 會由 Apple 簽署。協力廠商 app 會由具有 Apple 所簽發憑證的開發人員簽署。這可確保 app 沒有遭到竄改或變更。此外也會進行執行階段檢查，以確認 app 並未在最後一次使用後變成不受信任。

針對自行開發的企業內部專用 App 的使用，則可透過佈建 描述檔來控制。使用者必須安裝佈建描述檔，才能執行應用程式。佈建描述檔可以透過 MDM 解決方案以無線傳輸方式安裝。管理者也可以限制特定裝置上對於某個應用程式的使用。

### 安全的認證架構

iOS 提供安全的加密鑰匙圈來存放數位識別身分、使用者名稱與密碼。鑰匙圈資料會進行分割，因此儲存在協力廠商 app 裡的認證資訊無法由不同身分的 app 存取。如此一來，便能針對企業在 iOS 裝置中使用的各種應用程式與服務提供保護認證身分的機制。

### 常見加密架構

應用程式開發人員可以使用加密 API，進一步保護其應用程式資料。資料可以透過 AES、RC4 或 3DES 等經過證明的方式，以對稱形式加密。此外，iOS 裝置也為 AES 加密與 SHA1 雜湊提供硬體加速，讓應用程式發揮最好的效能。

### 應用程式資料保護

App 也可以利用 iOS 裝置內建的硬體加密，進一步保護機密的應用程式資料。開發人員可以針對特定檔案進行資料保護，指示系統為檔案內容加密，讓 app 與任何在裝置鎖定時可能的入侵者都無法存取檔案內容。

### App 授權

根據預設，iOS app 的權限極為有限，開發人員必須明確給予權限，才能讓 app 使用大部分的功能，如 iCloud、背景處理或共享鑰匙圈。這樣能確保 app 無法賦予自己權限來存取非部署範圍內的資料。此外，iOS app 必須經過使用者明確同意，才能使用 GPS 定位、使用者聯絡資訊、相機或儲存的照片等許多 iOS 功能。

## Internet 服務

Apple 提供了一組陣容堅強的服務，包含 iMessage、FaceTime、Siri、iCloud、iCloud 備份與 iCloud 鑰匙圈，讓裝置能夠發揮最大的效用，並提高使用者的生產力。

而且這些 Internet 服務的安全性，就和 iOS 平台所致力達到的目標一致。這些安全性目標包括為裝置上的資料與透過無線網路傳輸的資料提供安全防護、保護使用者的私人資訊，以及防止資訊和服務受到惡意威脅或未經授權的存取。每個服務都使用其強大的安全架構，同時仍維持 iOS 簡單易用的特性。

### iMessage

iMessage[1] 是 iOS 裝置與 Mac 電腦上的傳訊服務。iMessage 支援文字與附件，如照片、聯絡資訊與位置。訊息會出現在使用者註冊過的所有裝置上，因此使用者可以從任何一台裝置繼續對話。iMessage 大量使用了 Apple 推播通知服務 (APNs)。它採用點對點加密，這種加密方式會使用只有收發兩端的裝置知道的密鑰。Apple 無法解密訊息，訊息也不會被記錄。

### FaceTime

FaceTime[2] 是 Apple 的視訊與語音通話服務。FaceTime 通話首先使用 Apple 推播通知服務來建立連線，接著透過「Internet 連線能力建立」(ICE) 與「對話起始通訊協定」(SIP) 來建立加密串流。

### Siri

使用者只要像平常一樣說話，即可透過 Siri[3] 傳送訊息、排定會議時間、打電話或執行其他動作。Siri 使用語音辨識、文字轉語音的功能以及用戶端伺服器模式來回應各式各樣的請求。Siri 所支援的任務經過特別設計，能將用到私人資訊的機會減到最少，且私人資訊也會受到完整的保護。Siri 的請求與語音錄音無法做為個人身分的辨識，而且 Siri 的功能會盡可能透過裝置執行，而不會透過伺服器。

### iCloud

iCloud[4] 會儲存音樂、照片、app、行事曆、文件等內容，並自動將其推播到使用者的所有裝置。iCloud 也可以每天透過 Wi-Fi 備份資訊，包括裝置設定、app 資料以及文字和 MMS 訊息。它採取以下措施來保護內容的安全：將透過 Internet 傳送的內容加密、以加密格式儲存內容，並使用安全 Token 進行認證。此外，包括「照片串流」、「文件與資料」和「備份」等 iCloud 功能都可透過設定描述檔停用。

更多關於 iCloud 安全性和隱私權的資訊，請參閱 iCloud 安全性和隱私權概覽。

### iCloud 備份

iCloud 也可以每天透過 Wi-Fi 備份資訊，包括裝置設定、app 資料以及文字和 MMS 訊息。它採取以下措施來保護內容的安全：將透過 Internet 傳送的內容加密、以加密格式儲存內容，並使用安全 Token 進行認證。只有在裝置為鎖定狀態、已連接電源並可透過 Wi-Fi 連接 Internet 時，iCloud 備份才會開始執行。由於 iOS 採用了加密功能，因此在自動進行增量備份或回復時，系統的設計依然能保護資料安全無虞。

### iCloud 鑰匙圈

iCloud 鑰匙圈能讓使用者在 iOS 裝置與 Mac 電腦之間安全地同步密碼，也不必擔心 Apple 會看到這些資訊。iCloud 鑰匙圈在設計與架構上的考量，除了提供強大的隱私保護與安全性，也相當重視使用的簡便性與恢復鑰匙圈的能力。iCloud 鑰匙圈包含兩種服務：鑰匙圈同步與鑰匙圈恢復。鑰匙圈同步時，只有經過使用者同意的裝置才能參與同步，而且每個可以同步的鑰匙圈項目會透過 iCloud 密鑰值儲存功能，以個別裝置的加密方式來交換。這些項目是暫存的，同步之後不會繼續留在 iCloud 裡。鑰匙圈恢復可以讓使用者把鑰匙圈交給 Apple 保管，但 Apple 無法讀取其中的密碼與其他資料。即便使用者只有一台裝置，還是可以利用鑰匙圈恢復來避免資料遺失的風險。如果使用了 Safari 來為網頁帳號隨機產生強式密碼，鑰匙圈恢復就顯得格外重要，因為只有鑰匙圈會記錄這些密碼。鑰匙圈恢復服務的基礎在於次要驗證與安全的保管服務，這是 Apple 特別為此功能提供的支援。使用者的鑰匙圈會以強式密碼加密，而保管服務只會在一組嚴密的條件均符合的情況下才提供鑰匙圈。

關於安全性的詳細資訊，請參閱 iOS Security 指南。

# 第 3 章：
# 設定與管理

若能使用一些管理技巧來簡化帳號的設定、為組織內部設定規則、發佈 app 以及套用裝置限制，iOS 的部署可以變得輕鬆又有效率。絕大部分的設定工作都可以交給使用者，讓他們自己透過 iOS 內建的「設定輔助程式」來進行。等 iOS 裝置在 MDM 裡完成設定與登記，即可由 IT 人員透過無線方式管理。

本章說明了如何使用設定描述檔與行動裝置管理來支援您的 iOS 部署。

## 設定與啟用裝置

使用者在開箱取出 iOS 裝置之後，即可透過內建的「設定輔助程式」啟用裝置、進行基本設定並立即開始使用。除了基本設定，使用者也可以調整私人的偏好設定，如語言、位置、Siri、iCloud 和「尋找我的 iPhone」。如果使用者尚未有 Apple ID，也能透過「設定輔助程式」來建立。

### Apple ID

Apple ID 是一種識別身分，可以用來登入 FaceTime、iMessage、iTunes、App Store、iCloud 與 iBooks Store 等多種 Apple 服務。使用者在擁有 Apple ID 後，即可安裝來自 iTunes Store、App Store 或 iBooks Store 的 app、書籍與內容。Apple ID 也能讓使用者註冊取得 iCloud 帳號，用以在多個裝置上存取與共享內容。

若要讓這些服務發揮最大的效用，使用者應該要使用自己專用的 Apple ID。如果他們沒有 Apple ID，可以在取得裝置之前就先建立好，以加快之後設定的速度。

若要了解如何申請 Apple ID，請參閱我的 Apple ID。

### 以 Apple Configurator 準備裝置

若裝置是由 IT 集中管理，而非由個別使用者自行設定，可以使用 Apple Configurator 來快速啟用、定義與套用設定、進行監管、安裝 app 以及更新為最新的 iOS 版本。Apple Configurator 是為 OS X 提供的應用程式，可以從 Mac App Store 免費下載。裝置必須透過 USB 連接到 Mac 才能執行前述工作。您也可以將備份回復到裝置，這個作法可以套用裝置設定與主畫面佈局，並可安裝 app 資料。

## 設定描述檔

設定描述檔是 XML 檔案，其中含有裝置安全性規則與限制、VPN 設定資訊、Wi-Fi 設定、電子郵件和行事曆帳號，以及允許 iOS 裝置與您的 IT 系統搭配使用的認證身分。設定描述檔會快速將設定和授權資訊載入到裝置上。部分 VPN 和 Wi-Fi 設定只能使用設定描述檔來加以設定，且如果您不是使用 Microsoft Exchange，則需要使用設定描述檔來設定裝置的密碼規則。

設定描述檔可以透過「無線描述檔傳輸」或行動裝置管理 (MDM) 來發佈。您也可以透過 USB 使用 Apple Configurator 來將設定描述檔安裝在電腦所連接的裝置上，或者也可透過電子郵件或在網頁上發佈設定描述檔。當使用者在其裝置上使用 Safari 打開電子郵件附件或下載描述檔時，便會收到開始安裝程序的提示。如果您使用的是 MDM 伺服器，可先發佈一個僅含有伺服器設定資訊的描述檔，然後讓裝置以無線方式取得所有其他描述檔。

設定描述檔可加以加密和簽署，這可讓您將這些描述檔的用途限制在特定裝置上，並避免任何人更改描述檔包含的設定。您也可以將描述檔標示為鎖定至裝置，因此一旦安裝後，只可以透過清除裝置的所有資料或選擇輸入密碼來移除描述檔。

除了密碼之外，使用者無法更改設定描述檔中所提供的設定。此外，使用描述檔設定的帳號 (例如 Exchange 帳號) 僅能透過刪除描述檔的方式移除。

更多資訊請參閱 iOS Developer Library 網站上的 Configuration Profile Key Reference。

## 行動裝置管理 (MDM)

iOS 具有內建 MDM 架構，可讓協力廠商 MDM 解決方案以無線方式與 iOS 裝置互動。此輕巧架構專為 iOS 裝置設計，威力強大且靈活，可完整設定與管理組織內的所有 iOS 裝置。

藉由 MDM 解決方案，IT 管理者可以安全地在企業環境裡登記裝置、設定和更新選項、監控是否遵守公司規則，還可遠端清除或鎖定受管理的裝置。iOS MDM 讓 IT 人員可以輕鬆地為使用者提供網路服務的取用權限，同時能確保無論裝置的持有人為何，裝置都經過妥善的設定。

MDM 解決方案使用 Apple 推播通知服務 (APNs) 來與公用和專用網路上的裝置持續進行溝通。MDM 需要多項憑證才能執行，包括能與用戶端交談的 APNs 憑證，以及針對通訊安全性的 SSL 憑證。MDM 解決方案也能使用憑證來簽署描述檔。

包括 APNs 憑證在內的大多數憑證都必須每年更新。憑證過期時，MDM 伺服器將無法與用戶端溝通，直到憑證更新為止。請在到期之前更新所有 MDM 憑證。

更多關於 MDM 憑證的資訊，請參閱 Apple Push Certificates Portal。

### 登記

登記裝置將有助於建立目錄和資產管理。登記過程採用了「簡單憑證登記通訊協定」(SCEP)，因此 iOS 裝置可以建立並登記獨有的身分憑證來進行組織服務的認證。

在多數情況下，是由使用者決定是否要在 MDM 裡登記裝置，他們也可以隨時與 MDM 取消登記。組織應提供誘因，讓使用者願意維持受到管理的狀態。例如，使用 MDM 解決方案自動提供無線認證資訊，藉此要求使用者必須登記 MDM 才能連接 Wi-Fi 網路。當使用者離開 MDM，裝置會試著通知 MDM 伺服器。

### 設定

裝置登記後，即可由行動裝置管理伺服器動態進行設定與套用規則，伺服器會傳送設定描述檔到裝置上，由裝置在無需使用者操作的情況下自動安裝。

設定描述檔可以簽署、加密與鎖定 (以避免他人變更或共用設定)，這樣能確保只有根據您的要求進行設定且受到信任的使用者與裝置才能連接您的網路與服務。如果使用者取消在 MDM 裡登記裝置，所有透過 MDM 安裝的設定都會移除。

### 帳號

行動裝置管理可以自動為您組織裡的使用者設定郵件與其他帳號，協助他們快速上手。視 MDM 產品及其與您內部系統的整合情況而定，帳號承載資料可以預先填入使用者名稱、郵件位址，以及供認證與簽署用的憑證識別身分 (如果有的話)。MDM 可以設定以下類型的帳號：

- 郵件
- 行事曆
- 已訂閱的行事曆
- 聯絡資訊
- Exchange ActiveSync
- LDAP

受到管理的郵件與行事曆帳號會遵守 iOS 7 裡新增的「受管理的打開方式」(Managed Open In) 限制。

### 查詢

行動裝置管理伺服器可以查詢各種裝置資訊，包括序號、裝置的 UDID 或 Wi-Fi MAC 位址等硬體資訊，以及 iOS 版本和裝置上所安裝的 app 完整列表等軟體資訊。這些資訊有助於確保使用者裝置上擁有適當的 app 組合。

若使用了 Apple TV 軟體 5.4 或以上版本，MDM 還可以查詢登記的 Apple TV 裝置的資產資訊，如語言、地區與組織。

### 指令

當裝置受到管理時，可以由行動裝置管理伺服器透過一組特定的動作來加以管理。管理工作包括：

- **更改設定值。**MDM 可以傳送指令來為裝置安裝新版或更新的設定描述檔。設定的變更會於背景進行，無需使用者操作。
- **鎖定裝置。**如果裝置需要立即鎖定，可以傳送指令來以設定好的密碼鎖住裝置。
- **遠端清除裝置。**如果裝置遺失或遭竊，可以傳送指令來清除裝置上所有資料。一旦裝置收到遠端清除指令，動作即無法還原。
- **清除密碼鎖定。**清除密碼後，裝置會立即要求使用者輸入新密碼。當使用者忘記密碼，需要 IT 人員重新設定時，即可採取此作法。
- **要求進行 AirPlay 鏡像輸出功能和停止 AirPlay 鏡像輸出功能。**iOS 7 新增了一個指令，可以要求受監管的 iOS 裝置開始對特定目標進行 AirPlay 鏡像輸出功能，或結束進行中的 AirPlay 工作階段。

### 託管的 app

組織經常需要發佈軟體，以維持使用者在工作或學習上的效率。組織也需要控制軟體如何連接內部資源，以及如何在有使用者離開組織時維護資料的安全，而同時又要顧及使用者的私人 app 與資料。iOS 7 中託管的 app 可以讓組織透過 MDM 以無線傳輸方式發佈企業自行開發的 app，同時在組織的安全與使用者個人化之間取得適當的平衡。

MDM 伺服器可以透過無線傳輸方式同時部署 App Store app 和企業內部的 app。

託管的 app 可以透過 MDM 伺服器來進行遠端清除，在使用者從 MDM 取消裝置登記時也會移除。若移除 app，與該 app 連結的資料也會一併移除。

iOS 7 和行動裝置管理為 iOS 7 裡託管的 app 新增了一組額外的限制與功能，以提供更出色的安全性與使用者經驗：

- **受管理的打開方式。**提供了兩個實用的功能來保護組織內的 app 資料：
  - **允許在託管的 app 內開啟使用非託管的 app 建立的文件。**若套用此限制，可以避免使用者以私人的 app 與帳號來開啟組織中託管的 app 裡的文件。舉例來說，這項限制可以避免使用者以自己的 Keynote 來開啟組織的 PDF 檢視 app 裡的簡報 PDF。這項限制也可以避免使用者以私人 iCloud 帳號來開啟組織的 Pages 裡的文書處理附檔。
  - **允許在非託管的 app 內開啟使用託管的 app 建立的文件。**若套用此限制，便可避免組織裡託管的 app 與帳號開啟使用者私人 app 裡的文件。這項限制可以避免使用者以任何私人 app 來開啟組織中受管理的郵件帳號裡的機密郵件附檔。
- **App 設定。**App 開發人員可以識別託管的 app 上所能進行的設定。這些設定可以在託管的 app 安裝前或安裝後進行安裝。
- **App 意見回饋。**製作 app 的開發人員可以使用 MDM 來識別託管的 app 能讀取的 app 設定。例如，開發人員可以為 app 意見回饋指定「DidFinishSetup」鍵值，讓 MDM 伺服器能查詢此鍵值來判定該 app 是否已經啟動與設定。
- **防止備份。**這項限制可避免託管的 app 備份資料至 iCloud 或 iTunes。若某個 app 從 MDM 移除後，又由使用者重新安裝，啟用防止備份的限制可以避免恢復託管的 app 資料。

## 監管裝置

所有 iOS 裝置在預設上都是未受監管的。若要啟用額外的設定選項和限制，可以選擇使用 Apple Configurator 來監管組織所持有的 iOS 裝置。

將裝置指派給方案裡的 MDM 伺服器後，可以使用您組織裡的 MDM 伺服器來套用描述檔和其他功能。

這些功能包括：

- 監管裝置
- 強制性設定
- 可鎖定的 MDM 設定
- 略過「設定輔助程式」裡的步驟

可以略過的「設定輔助程式」畫面包括：

- **密碼。**略過密碼設定
- **定位。**不要啟用「定位服務」
- **從備份回復。**不要從備份回復
- **Apple ID。**不要提示您以 Apple ID 登入
- **服務條款。**略過「服務條款」
- **Siri。**不要啟用 Siri
- **傳送診斷資訊。**不要自動傳送診斷資訊

### 受監管的裝置

監管功能提供了停用 iMessage 或 Game Center 等額外的限制，能對組織所持有的裝置進行更嚴密的管理。它也提供額外的裝置設定與功能，像是網頁內容過濾，或在無提示的情況下安裝 app。您可以透過 Apple Configurator 以無線方式在裝置上啟用監管功能。

關於受監管的裝置上所能啟用的特定限制，請參閱「附錄 B」。

# 第 4 章：
# 發佈 App

iOS 隨附一組 app，能讓您組織裡的人員執行每日例行工作，如電子郵件、管理行事曆、追蹤聯絡資訊與取用網頁上的內容。絕大多數能提高使用者生產力的功能，是來自 App Store 上數以萬計的協力廠商 iOS app，或是企業自行研發的內部專用 App。

如果參與了「iOS 企業開發人員計劃」，即可建立與部署您自行開發的內部專用 app。本章將說明為使用者部署 app 的方式。

## 內部專用 App

如果您自行開發 iOS app 供組織使用，可以透過「iOS 企業開發人員計劃」來部署這些內部專用 App。部署內部專用 App 的流程為：

- 註冊「iOS 企業開發人員計劃」。
- 準備要發佈的 app。
- 製作供企業發佈用的佈建描述檔，以便授權裝置來使用您已簽署的 app。
- 使用佈建描述檔建立 app。
- 將 app 部署給您的使用者。

### 註冊參與 app 開發

若要開發與部署內部專用的 iOS app，請先註冊 iOS 企業開發人員計劃。

註冊之後，您可以要求取得開發人員憑證和開發人員佈建描述檔。您要在開發期間使用這些項目來建立和測試 app。開發用的佈建描述檔允許以您的開發人員憑證簽署的 app 在註冊的裝置上執行。請在「iOS 佈建入口網站」(iOS Provisioning Portal) 製作開發人員佈建描述檔。ad hoc 描述檔會在三個月後到期，且會指定哪些裝置 (依據裝置識別碼) 可以執行您的 app 的開發版次。您可將開發人員簽署版次，以及開發用的佈建描述檔發佈給您的 app 團隊和測試人員。

### 準備要進行發佈的 app

完成開發和測試，且準備部署 app 時，請使用您的發佈憑證來簽署 app，並以佈建描述檔加以封裝。針對您計劃會員資格所指派的小組專員 (Team Agent) 或管理者會在 iOS 佈建入口網站製作憑證和描述檔。

產生發佈憑證的作業包含使用「憑證輔助程式」(其為 OS X 開發系統上「鑰匙圈存取」應用程式的一部分) 來產生「憑證簽署要求」(CSR)。您要將 CSR 上傳至「iOS 佈建入口網站」，並收到所回應的發佈憑證。當您在「鑰匙圈」中安裝此憑證時，可以設定 Xcode 使用它來簽署您的 app。

### 佈建內部專用 App

供企業發佈用的佈建描述檔允許在不限數量的 iOS 裝置上安裝您的 app。您可以為特定的 app 或多個 app 製作一份供企業發佈用的佈建描述檔。

在您的 Mac 上安裝企業發佈憑證和佈建描述檔之後，您要使用 Xcode 來簽署和建立 app 的正式發行版本。企業發佈憑證的有效期限為三年，到期後，您必須使用更新的憑證來再次簽署和建立 app。app 的佈建描述檔有效期限為一年，因此您需要每年發佈一次新的佈建描述檔。詳細資訊請參閱「附錄 C」裡的「提供更新的 App」一節。

限制發佈憑證及其密鑰的取用權限相當重要。請使用 OS X 上的「鑰匙圈存取」來以 p12 格式輸出和備份這些項目。如果密鑰遺失，將無法恢復或再次下載。除了保護憑證和密鑰安全之外，您應該將取用權限制給負責最終驗收 app 的人員。以發佈憑證來簽署 app，即表示公司認可 app 的內容及功能，並遵守「企業開發人員協議」(Enterprise Developer Agreement) 授權條款。

## 部署 App

部署 app 有四種方式：

- 使用 iTunes 將 app 發佈給您的使用者進行安裝。
- 讓 IT 管理者使用 Apple Configurator 在裝置上安裝 app。
- 將 app 張貼到安全的網頁伺服器；使用者可透過無線方式連線和執行安裝。請參閱「附錄 C：以無線方式安裝內部專用 App」。
- 使用 MDM 伺服器指示受管理的裝置來安裝內部專用 app 或 App Store app (若您的 MDM 伺服器支援此功能)。

### 使用 iTunes 安裝 app

如果您的使用者是使用 iTunes 在裝置上安裝 app，請使用安全方式將應用程式發佈給使用者，並要求他們遵循下列步驟：

1. 在 iTunes 中，選擇「檔案」(File) >「加入資料庫」(Add to Library)，然後選擇檔案 (.app、.ipa 或 .mobileprovision)。
   使用者也可以將檔案拖移至 iTunes 應用程式圖像上。
2. 將裝置連接到電腦，然後在 iTunes 的「裝置」(Devices) 列表中將其選取。
3. 按一下「應用程式」(Apps) 標籤頁，然後在列表中選取 app。
4. 按一下「套用」(Apply)。

如果使用者的電腦受到管理，您可以將檔案部署至他們的電腦並要求他們同步裝置，而非要求他們將檔案加入 iTunes 中。iTunes 會自動安裝在 iTunes 的 Mobile Applications 和 Provisioning Profiles 檔案夾中找到的檔案。

### 用 Apple Configurator 安裝 app

Apple Configurator 是可從 Mac App Store 免費下載的 OS X 應用程式，可供 IT 管理者用來安裝內部專用 App 或來自 App Store 的 app。

來自 App Store 的 app 或企業內部專用 app 可以直接輸入到 Apple Configurator，並安裝在不限數量的裝置上。

### 使用 MDM 安裝 app

MDM 伺服器可以管理 App Store 中的協力廠商 app 以及內部專用 App。使用 MDM 安裝的 app 稱為「託管的 app」。MDM 伺服器可以指定當使用者從 MDM 取消登記時，是否要保留託管的 app 及其資料。另外，伺服器還可以避免將託管的 app 資料備份至 iTunes 與 iCloud。這可讓 IT 在管理可能包含機密業務資訊的 app 時，能夠擁有比管理使用者直接下載的 app 更多的控制。

MDM 伺服器會將安裝指令傳送到裝置，以安裝託管的 app。在未受監管的裝置上，託管的 app 會在取得使用者同意之後才進行安裝。

託管的 app 可以使用 iOS 7 提供的額外控制功能。例如可以針對 app 指定 VPN 連線，這表示只有該 app 的網路流量會在受保護的 VPN 通道裡。這樣可以維護私人資料的隱私，也不會與公用資料混淆。

託管的 app 也支援 iOS 7 上的「受管理的打開方式」。這表示託管的 app 將無法透過使用者的私人 app 傳送資料，讓企業確保機密資料不會遭到盜用。

## 快取伺服器

iOS 能讓使用者輕鬆連接並取用數位內容，而部分使用者可能需要在連接組織的無線網路時，下載容量高達好幾 GB 的 app、書籍與軟體更新項目。對這些資產的需求會在幾個階段達到高峰，首先是在初次部署裝置時，接著則是在使用者發現新內容或隨時間不斷更新內容時不定期地發生。下載這些內容可能會導致對 Internet 頻寬的需求暴增。

OS X Server 內建的「快取伺服器」(Caching Server) 功能可以將請求的內容的副本儲存在區域網路上，以減少專用網路 (RFC1918) 上連外的 Internet 頻寬。若有多個「快取伺服器」，對大型網路而言將是一大福音。在許多部署的情況下，只要啟用服務即可設定「快取伺服器」。伺服器和所有使用該伺服器的裝置都必須位於 NAT 環境裡。

更多資訊請參閱 OS X Server: Advanced Administration。

執行 iOS 7 的 iOS 裝置會自動聯絡附近的「快取伺服器」，不需要另外設定裝置。以下說明「快取伺服器」工作流程如何在 iOS 裝置上透明清楚地執行：

1. 當某個擁有多個「快取伺服器」的網路上有 iOS 裝置向 iTunes Store 或「軟體更新」伺服器請求內容時，iOS 裝置的請求會被轉介給「快取伺服器」。
2. 「快取伺服器」會先查看其本機快取裡是否已有請求的內容。如果有，它會立即提供內容給 iOS 裝置。
3. 如果「快取伺服器」沒有請求的資產，它會試著從其他來源下載。OS X Mavericks 的「快取伺服器 2」包含端點複製功能，如果網路上其他「快取伺服器」已下載過請求的內容，該功能會使用那些伺服器。
4. 當「快取伺服器」接收下載資料時，它會立即將資料轉發給所有請求該資料的用戶端，同時快取副本到磁碟上。

iOS 7 支援以下類型的快取內容：

- iOS 軟體更新項目
- App Store app
- App Store 更新項目
- iBooks Store 的書籍

iTunes 也支援「快取伺服器 2」。iTunes 11.0.4 或以上版本 (Mac 與 Windows 版) 支援以下類型的內容：

- App Store app
- App Store 更新項目
- iBooks Store 的書籍

### 國家或地區限制

基於散佈授權和稅務相關法令，在某些國家或地區可能無法快取某些內容。自 2013 年 12 月起，巴西、墨西哥、中國與葡萄牙無法快取 iTunes 下載項目，而加拿大則無法快取 iBook 下載項目。

如果根據 IP 位址所判斷的客戶所在國家或地區，與其所使用的 iTunes Store 的國家不同，將無法快取 iTunes 下載項目。

例如，位於舊金山的 iPad 使用者可以下載德國 iTunes Store 裡的 app，但無法使用快取服務。

# 附錄 A：
# Wi-Fi 基礎設施

在為 iOS 的部署準備 Wi-Fi 基礎設施時，有幾個因素必須加以考慮：

- 所需覆蓋的範圍
- 使用 Wi-Fi 網路的裝置數量和密度
- 裝置的類型及其 Wi-Fi 功能
- 傳輸的資料類型與數量
- 存取無線網路時的安全需求
- 加密需求

儘管此一列表並非完整，但它代表了最關鍵的 Wi-Fi 網路設計要素。

**請注意**：本章內容是以美國的 Wi-Fi 網路設計為主，其他國家的設計可能有所不同。

### 覆蓋範圍和密度的規劃

為 iOS 裝置的使用地點提供 Wi-Fi 覆蓋範圍很重要，為使用區域規劃裝置密度也同樣重要。

目前，許多企業級基地台都可連接多達 50 個 Wi-Fi 用戶端，然而，若單一基地台連接太多裝置，連線品質可能會令人失望。每一部裝置的使用者經驗，都取決於使用頻道的無線頻寬，以及共享所有頻寬的裝置數量。越多裝置使用相同的基地台，這些裝置的網路速度就會相對降低。因此，在設計 Wi-Fi 網路時，必須要考慮到 iOS 裝置的預期使用模式。

### 2.4GHz vs. 5GHz

在美國，運作於 2.4GHz 頻段的 Wi-Fi 網路允許 11 個頻道。但是，由於考慮到頻道干擾，所以僅在網路設計中僅使用頻道 1、6 和 11。

5GHz 訊號無法像 2.4GHz 訊號一樣穿透牆壁和其他屏障，所以覆蓋範圍較小。因此，如果是封閉式空間中具有高密度裝置的設計環境下 (例如在教室中)，5GHz 網路可能較為適合。5GHz 頻段所提供的頻道數量視各家基地台廠商與不同國家而定，不過至少都會有 8 個頻道。

5GHz 的頻道為非重疊頻道，這和 2.4GHz 頻段僅提供三個非重疊頻道有很大的差異。在為高度密集的 iOS 裝置架設 Wi-Fi 網路時，額外的 5GHz 頻道會是規劃時的主要考量。

### 覆蓋範圍的設計

建築物的隔間方式也會影響您的 Wi-Fi 網路設計。例如在一間公司裡，使用者可能會與其他員工在會議室或辦公室裡見面，因此他們整天都會在大樓裡四處走動。在這樣的情境下，網路連線的主要用途是收信、檢視行事曆和上網，所以 Wi-Fi 覆蓋範圍是優先考量。這時可以採用這樣的 Wi-Fi 網路設計：在每層樓架設兩到三個基地台來供所有辦公室使用，並在每間會議室架設一個基地台。

### 密度的設計

對照上述使用情境，再設想一間擁有 1000 名學生和 30 名教師，分佈在兩層樓的校園建築物。每位學生都發給一台 iPad，每位老師則有 MacBook Air 和 iPad。每一間教室約可容納 35 名學生，且教室都彼此相鄰。學生整天會透過 Internet 做研究、觀賞課程影片，並在 LAN 上的檔案伺服器拷貝檔案。

由於這個情境下的行動裝置密度較高，Wi-Fi 網路設計也會較為複雜。每間教室都有約 35 位學生使用，因此可以在每間教室各架設一個基地台。而針對公共區域，則必須考慮設置多個基地台，以提供足夠的覆蓋範圍。公共區域的實際基地台數量都不盡相同，主要取決於這些場所中的 Wi-Fi 裝置密度。

如果僅支援 802.11b 或 802.11g 標準的裝置也必須加入網路，可以考慮啟用 802.11b/g，但前提是必須有雙頻段的基地台。另一種方法，是為較新型的裝置提供一個使用 5GHz 802.11n 的 SSID，再提供第二個 2.4GHz 的 SSID 來支援 802.11b 和 802.11g 裝置。但須注意，應避免產生過多的 SSID。

在兩種設計方案中，都應避免使用隱藏式 SSID。對 Wi-Fi 裝置來說，要重新加入一個隱藏的 SSID (Hidden SSID)，要比加入一個廣播 SSID (Broadcast SSID) 更加困難，而且隱藏 SSID 對於安全的幫助也不大。使用者可能會經常改變其 iOS 裝置的位置，所以隱藏式 SSID 可能會延遲連結網路的時間。

### Apple 產品的 Wi-Fi 標準

Apple 產品對各種 Wi-Fi 規格的支援如下所列，其中包含下列詳細資訊：

- **802.11 相容性。**802.11b/g、802.11a、802.11n
- **頻段。**2.4 GHz 或 5 GHz
- **MCS Index。**「調變和編碼架構」(MCS) 指標定義了 802.11n 裝置在溝通時的最大傳輸速率。
- **頻道合併功能。**HD20 或 HD40
- **保護間隔 (GI)。**保護間隔 (Guard interval) 是兩個符元從一個裝置傳送到另一個裝置的間隔 (時間)。802.11n 標準定義了較短的 400ns 保護間隔，可允許整體傳輸量增加，不過裝置也可以使用較長的 800ns 保護間隔。

**iPhone 5s**
802.11n @ 2.4GHz 與 5GHz
802.11a/b/g
MCS Index 7 / HT40 / 400ns GI

**iPhone 5c**
802.11n @ 2.4GHz 與 5GHz
802.11a/b/g
MCS Index 7 / HT40 / 400ns GI

**iPhone 5**
802.11n @ 2.4GHz 與 5GHz
802.11a/b/g
MCS Index 7 / HD40 / 400ns GI

**iPhone 4s**
802.11n @ 2.4GHz
802.11b/g
MCS Index 7 / HD20 / 800ns GI

**iPhone 4**
802.11n @ 2.4GHz
802.11b/g
MCS Index 7 / HD20 / 800ns GI

**iPad Air 與配備 Retina 顯示器的 iPad mini**
802.11n @ 2.4GHz 與 5GHz
802.11a/b/g
MCS Index 15 / HT40 / 400ns GI

**iPad (第四代) 與 iPad mini**
802.11n @ 2.4GHz 與 5GHz
802.11a/b/g
MCS Index 7 / HD40 / 400ns GI

**iPad (第一、第二和第三代)**
802.11n @ 2.4GHz 與 5GHz
802.11a/b/g
MCS Index 7 / HD20 / 800ns GI

**iPod touch (第五代)**
802.11n @ 2.4GHz 與 5GHz
802.11a/b/g
MCS Index 7 / HD40 / 400ns GI

**iPod touch (第四代)**
802.11n @ 2.4GHz
802.11b/g
MCS Index 7 / HD20 / 800ns GI

# 附錄 B：限制

iOS 支援下列規則與限制，且這些規則與限制都可以根據您組織的需求來設定。

### 裝置功能

- 允許安裝 app
- 允許 Siri
- 鎖定時允許 Siri
- 允許使用攝影機
- 允許 FaceTime
- 允許螢幕畫面擷取
- 允許漫遊時自動同步
- 允許同步最近的郵件
- 允許語音撥接
- 允許 App 內的購買
- 每次購買都必須提供商店密碼
- 允許多人遊戲
- 允許加入 Game Center 裡的朋友
- 設定允許的內容分級
- 允許 Touch ID
- 允許從鎖定畫面取用「控制中心」
- 允許從鎖定畫面取用「通知中心」
- 允許從鎖定畫面取用「今日」顯示方式
- 允許在鎖定畫面取用 Passbook 通知

### 應用程式

- 允許使用 iTunes Store
- 允許使用 Safari
- 設定 Safari 安全性偏好設定

### iCloud

- 允許備份
- 允許文件同步以及鑰匙圈同步
- 允許「我的照片串流」
- 允許 iCloud 照片共享

**安全性與隱私**

- 允許診斷資料傳送至 Apple
- 允許使用者接受不受信任的憑證
- 備份強制加密
- 允許在託管的 app 裡開啟非託管的 app 的檔案
- 允許在非託管的 app 裡開啟託管的 app 的檔案
- 在初次 AirPlay 配對時要求輸入密碼
- 允許以無線傳輸方式更新 PKI
- 要求「限制廣告追蹤」

**以下限制僅適用於受監管的裝置**

- 單一 App 模式
- 輔助使用設定
- 允許 iMessage
- 允許 Game Center
- 允許移除 app
- 允許 iBooks Store
- 允許 iBooks Store 上的成人書籍
- 啟用 Siri 粗話過濾器
- 允許手動安裝設定描述檔
- HTTP 全球網路代理伺服器
- 允許與電腦配對以同步內容
- 以安全列表和選擇性的連線密碼來限制 AirPlay 的連線
- 允許 AirDrop
- 允許修改帳號
- 允許修改行動數據設定
- 允許「尋找我的朋友」
- 允許主機配對 (iTunes)
- 允許「啟用鎖定」

# 附錄 C：
# 以無線方式安裝內部專用 App

iOS 支援以無線傳輸方式安裝自行開發的內部專用 App，無需使用 iTunes 或 App Store。

需求條件：

- 可供授權使用者取用的安全網頁伺服器
- 格式為 .ipa 的 iOS app，其製作用途為搭配企業佈建描述檔來正式發行
- XML 資訊檔 (本附錄後面會提到)
- 允許裝置連接 Apple iTunes 伺服器的網路設定

安裝 app 是很簡單的。使用者可將資訊檔從您的網站下載到他們的 iOS 裝置中。資訊檔會指示裝置下載並安裝資訊檔中提及的 app。

您可以透過 SMS 或電子郵件來發佈下載此資訊檔的 URL，或者將其嵌入到您製作的其他企業 app。

您可以決定是否要設計或提供用來發佈 app 的網站。請確定使用者已進行認證 (可使用基本認證或目錄式認證)，並確定網站可經由您的內部網路或 Internet 連接。您可以將 app 和資訊檔放至隱藏的目錄中，或是其他可使用 HTTPS 讀取的位置。

如果建立了自助式入口網站，可以考慮將 Web Clip 加入到使用者的主畫面螢幕，方便他們連接入口網站來取得後續的部署資訊，如新的設定描述檔、推薦的 App Store app，以及在行動裝置管理解決方案裡登記。

### 準備要進行無線發佈的內部專用 App

若要準備內部專用 App 來進行無線發佈，您要建立封存版本 (.ipa 檔) 及資訊檔來啟用 app 的無線發佈和安裝功能。

您可以使用 Xcode 來製作 app 封存。使用您的發佈憑證簽署 app，並在封存檔中包含您的企業部署佈建描述檔。更多關於建立與封存 app 的資訊，請參訪 iOS Dev Center 或參閱 *Xcode User Guide* (位於 Xcode 的「輔助說明」選單裡)。

### 關於無線資訊檔

資訊檔為 XML plist 檔案。iOS 裝置會使用它來從您的網頁伺服器中尋找、下載和安裝 app。Xcode 會使用您在分享封存的 app 以供企業發佈時，所提供的資訊來製作資訊檔。請參閱前面有關準備 app 來進行發佈的章節。

下列欄位為必填項目：

| 項目 | 說明 |
| --- | --- |
| URL | App (.ipa) 檔案的完整 HTTPS URL。 |
| 顯示影像 | 在下載與安裝期間顯示的 57 x 57 像素 PNG 影像。請指定影像的完整 URL。 |
| 完整大小的影像 | 在 iTunes 中代表 app 的 512 x 512 像素 PNG 影像。 |
| 套件識別碼 | App 的套件識別碼，與 Xcode 計畫案中所指定的識別碼完全相同。 |
| 套件版本 | App 的套件版本，如 Xcode 計畫案中所指定。 |
| 名稱 | App 的名稱，會在下載和安裝期間顯示。 |

僅「書報攤」app 需填寫下列欄位：

| 項目 | 說明 |
| --- | --- |
| 書報攤影像 | 在「書報攤」書架上顯示的完整大小 PNG 影像。 |
| UINewsstandBindingEdge<br>UINewsstandBindingType | 這些鍵值必須符合「書報攤」app 的 info.plist 中的鍵值。 |
| UINewsstandApp | 表示 app 為「書報攤」app。 |

您可以選用的鍵值會在範例資訊檔中說明。例如， 如果 app 檔案較大，而且除了 TCP 通訊的例行性錯誤檢查，您還想要確保下載完整性，便可使用 MD5 鍵值。

您可以指定其他項目陣列的成員，來以單一資訊檔安裝多個 app。

本附錄結尾隨附範例資訊檔。

### 建構您的網站

將這些項目上傳到您網站中某個可供認證使用者連接的區域：

- App (.ipa) 檔案
- 資訊檔 (.plist)

您的網站可以設計成只連結到資訊檔的單一頁面。當使用者點一下網頁連結，便會下載資訊檔，而資訊檔會啟動其所描述之 app 的下載和安裝動作。

連結範例：<a href=」itms-services://?action=download-manifest&url=http://example.com/manifest.plist”>安裝 App</a>

請勿將網頁的連結加入封存的 app (.ipa) 中。當資訊檔載入後，裝置會下載 .ipa 檔案。雖然 URL 的通訊協定部分是 itms-services，但 iTunes Store 並未納入此程序中。

也請確定您的 .ipa 檔案可以透過 HTTPS 存取，且您的網站是以 iOS 所信任的憑證簽署。如果自簽憑證沒有受信任的來源，也無法通過 iOS 裝置的驗證，則安裝將會失敗。

### 設定伺服器 MIME 類型

您可能會需要設定網頁伺服器，以正確地傳輸資訊檔和 app 檔案。

對於 OS X Server，請將下列 MIME 類型加入到網頁伺服器的「MIME 類型」設定：

application/octet-stream ipa text/xml plist

若為 IIS，請使用 IIS Manager 來將 MIME 類型加到伺服器的「屬性」頁面中：

.ipa application/octet-stream.plist text/xml

### 無線 app 發佈的問題診斷

如果無法透過無線方式發佈 app，並出現「無法下載」的訊息，請檢查下列項目：

- 確定 app 已正確簽署。使用 Apple Configurator 將應用程式安裝到裝置上來加以測試，並查看是否有任何錯誤發生。
- 確定資訊檔的連結正確，且網頁使用者可取用資訊檔。
- 確定 .ipa 檔案的 URL (位於資訊檔中) 是正確的，且網頁使用者可透過 HTTPS 取用該 .ipa 檔案。

### 網路設定需求

如果裝置是連接封閉的內部網路，您應允許 iOS 裝置連接下列項目：

| URL | 原因 |
| --- | --- |
| ax.init.itunes.apple.com | 裝置會透過行動網路取得下載 app 的目前檔案大小限制。如果無法連接此網站，安裝可能會失敗。 |
| ocsp.apple.com | 裝置會聯繫此網站，以檢查用來簽署佈建描述檔的發佈憑證狀態。請參閱下方「憑證的驗證」一節。 |

### 提供更新的 app

您自己發佈的 app 不會自動更新。當您有新版本可供使用者安裝時，請通知他們有更新項目，並指導他們安裝 app。請考慮讓 app 檢查更新項目，並在其打開時通知使用者。如果您使用的是無線 app 發佈，通知裡會有已更新 app 的資訊檔連結。

如果您想要讓使用者保留其裝置上儲存的 app 資料，請確定新版本與其要取代之版本使用相同的 bundle-identifier (套件識別碼)，並告知使用者不要在安裝新版本前刪除舊有版本。如果 bundle-identifier 相符的話，新版本將會取代舊有版本並保留裝置上儲存的資料。

發佈用的佈建描述檔會在發出後的 12 個月到期。過了到期日，描述檔會移除，且 app 將無法啟動。

在佈建描述檔到期前，請使用 iOS Development Portal 來為 app 製作新的描述檔。以新的佈建描述檔製作新的 app 封存 (.ipa)，提供給首次安裝該 app 的使用者。

對於已擁有 app 的使用者，建議您規劃下一版發行的時間，以便在新版本裡加入新的佈建描述檔。若您不想這麼做，也可以只發佈新的 .mobileprovision 檔案，讓使用者無需再次安裝 app。新的佈建描述檔會覆蓋 app 封存中原有的檔案。

佈建描述檔可以使用 MDM 來安裝和管理，或由使用者從您提供的安全網站來下載及安裝，或是以電子郵件附件發佈給使用者來打開並安裝。

當您的發佈憑證過期後，app 便無法啟動。發佈憑證的有效期限為發出後三年，或直到您的「企業開發人員計劃」會員資格到期為止，視何者先到期。若要避免憑證過早到期，請確定在到期前更新您的會員資格。關於發佈憑證的檢查方式，請參閱下方的「憑證的驗證」一節。

您可以同時讓兩個發佈憑證為有效狀態；兩者為互相獨立。第二個憑證是用來提供延長的期限，以便在第一個憑證過期後用來更新您的 app。向 iOS Dev Center 要求第二個發佈憑證時，請確定您並未撤銷第一個憑證。

### 憑證的驗證

使用者初次打開 app 時，裝置會聯絡 Apple 的 OCSP 伺服器來驗證發佈憑證。除非憑證已遭撤銷，否則便會允許執行 app。若無法聯絡 OCSP 伺服器或從伺服器取得回應，並不會被視為撤銷。若要驗證狀態，該裝置必須可以連接 ocsp.apple.com。請參閱本附錄前面的「網路設定需求」。

OCSP 回應會以快取儲存在裝置上，儲存的時間長短由 OCSP 伺服器指定，目前是介於 3 至 7 天。憑證的有效性將會等到裝置重新啟動且快取的回應已過期時，才會再次進行檢查。

如果在此時收到撤銷，app 將無法執行。

撤銷發佈憑證會使您已簽署的所有 app 無效。除非您確定密鑰已遺失或是認為憑證遭盜用，否則不要輕易撤銷憑證。

**範例 app 資訊檔**

```
<!DOCTYPE plist PUBLIC “-//Apple//DTD PLIST 1.0//EN” “http://www.apple.com/
DTDs/PropertyList-1.0.dtd”>
<plist version=”1.0”>
<dict>
 <!-- array of downloads. -->
 <key>items</key>
 <array>
  <dict>
    <!-- an array of assets to download -->
    <key>assets</key>
    <array>
     <!-- software-package: the ipa to install. -->
     <dict>
       <!-- required. the asset kind. -->
       <key>kind</key>
       <string>software-package</string>
       <!-- optional. md5 every n bytes. will restart a chunk if md5 fails. -->
       <key>md5-size</key>
       <integer>10485760</integer>
       <!-- optional. array of md5 hashes for each “md5-size” sized chunk. -->
       <key>md5s</key>
       <array>
         <string>41fa64bb7a7cae5a46bfb45821ac8bba</string>
         <string>51fa64bb7a7cae5a46bfb45821ac8bba</string>
       </array>
       <!-- required. the URL of the file to download. -->
       <key>url</key>
       <string>http://www.example.com/apps/foo.ipa</string>
     </dict>
     <!-- display-image: the icon to display during download.-->
     <dict>
       <key>kind</key>
       <string>display-image</string>
       <!-- optional. indicates if icon needs shine effect applied. -->
       <key>needs-shine</key>
       <true/>
       <key>url</key>
       <string>http://www.example.com/image.57x57.png</string>
     </dict>
     <!-- full-size-image: the large 512x512 icon used by iTunes. -->
     <dict>
       <key>kind</key>
       <string>full-size-image</string>
       <!-- optional. one md5 hash for the entire file. -->
       <key>md5</key>
       <string>61fa64bb7a7cae5a46bfb45821ac8bba</string>
       <key>needs-shine</key>
       <true/>
       <key>url</key><string>http://www.example.com/image.512x512.jpg</
string>
```

```
    </dict>
     </array><key>metadata</key>
     <dict>
       <!-- required -->
       <key>bundle-identifier</key>
       <string>com.example.fooapp</string>
       <!-- optional (software only) -->
       <key>bundle-version</key>
       <string>1.0</string>
       <!-- required. the download kind. -->
       <key>kind</key>
       <string>software</string>
       <!-- optional. displayed during download; typically company name -->
       <key>subtitle</key>
       <string>Apple</string>
       <!-- required. the title to display during the download. -->
       <key>title</key>
       <string>Example Corporate App</string>
     </dict>
    </dict>
  </array>
</dict>
</plist>
```

[1]可能適用一般電信數據傳輸費率。無法使用 iMessage 時，可能會以簡訊方式傳送訊息；適用一般電信傳訊費用。
[2]FaceTime 通話需要收、發話雙方均使用支援 FaceTime 功能的裝置與 Wi-Fi 連線。透過行動網路使用 FaceTime，需要具行動數據功能的 iPhone 4s 或後續機種、配備 Retina 顯示器的 iPad 或 iPad mini。是否能夠透過行動網路進行通話，取決於電信業者政策；數據服務可能需要付費。 [3]Siri 可能不適用於所有語言或地區，且功能會因地區而異。需要 Internet 連線；行動數據服務可能需要付費。 [4]部分功能必須有 Wi-Fi 連線。部分功能不適用於所有國家或地區。部分服務的存取數目上限為 10 台裝置。