iOS 部署
技术参考

iOS 7.1

2014 年 5 月

目录

简介

本指南面向希望为网络中的 iOS 设备提供支持的 IT 管理员。其中提供了有关在大型组织（大企业或教育机构）中部署和支持 iPhone、iPad 和 iPod touch 的信息。本指南说明了 iOS 设备如何提供全面的安全防护、如何与现有基础架构集成，以及如何凭借强大的工具进行部署。

通过了解 iOS 中支持的关键技术，有助于实施适当的部署策略，为用户提供最佳体验。当你在组织中部署 iOS 设备时，可使用以下几章内容作为技术参考：

集成。iOS 设备本身支持多种网络基础架构。在本节中，你将了解 iOS 支持的与 Microsoft Exchange、WLAN、VPN 和其他标准服务相集成的技术和最佳做法。

安全。iOS 可安全地访问企业服务并保护重要数据。iOS 对传输中的数据进行强加密，采用切实有效的鉴定方法访问企业服务，并对所有静态数据进行硬件加密。请阅读本章，详细了解 iOS 在安全方面提供的功能。

配置和管理。iOS 支持多种高级工具和技术，可确保 iOS 设备易于设置，能够根据需要进行配置，并可在大型环境中轻松进行管理。本章概述了移动设备管理 (MDM)。

App 分发。 有多种方法可用于在组织中部署 app 和内容。利用 iOS 开发者企业计划，你的组织可以为内部用户构建和部署 app。通过本章可深入了解如何部署为内部使用而构建的 app。

以下附录提供了其他技术细节和要求：

WLAN 基础架构。详细介绍 iOS 支持的 WLAN 标准以及规划大型 WLAN 网络时的注意事项。

限制。详细介绍可用于配置 iOS 设备以满足安全、密码和其他要求的限制。

以无线方式安装企业内部 App。详细介绍如何使用自有的基于 Web 的门户分发企业内部 app 及相关要求。

其他资源

要获取相关的帮助信息，请访问以下网站：

www.apple.com/ipad/business/it

www.apple.com/iphone/business/it

www.apple.com/education/it

第 1 章：
集成

iOS 设备本身支持多种网络基础架构。其中包括：

- 常见的第三方系统，例如 Microsoft Exchange
- 与基于标准的邮件、目录、日历和其他系统集成
- 用于数据传输和加密的标准 WLAN 协议
- 虚拟专用网络 (VPN)，包括为 app 单独设置 VPN
- 用于简化联网 app 和服务鉴定的单点登录
- 用于鉴定用户和保护通信安全的数字证书

由于 iOS 中已内置这种支持，IT 部门只需配置为数不多的几项设置，即可将 iOS 设备集成到现有基础架构中。请继续阅读，详细了解 iOS 支持的技术和最佳做法。

Microsoft Exchange

iOS 可通过 Microsoft Exchange ActiveSync (EAS) 直接与 Microsoft Exchange Server 通信，因而可以推送电子邮件、日历、通讯录、备忘录和任务。Exchange ActiveSync 还向用户提供访问全局地址列表 (GAL) 的功能，并向管理员提供密码策略实施和远程擦除功能。iOS 同时支持 Exchange ActiveSync 基本鉴定和基于证书的鉴定。

如果你所在的公司当前启用了 Exchange ActiveSync，则已具备支持 iOS 所需的服务，不必再进行其他配置。

要求

安装了 iOS 7 或更高版本的设备支持以下版本的 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

如果存在蜂窝或 WLAN 数据连接，Exchange Server 可自动将电子邮件、任务、通讯录和日历事件发送至 iOS 设备。iPod touch 和某些 iPad 机型没有蜂窝连接，因此只有当它们连接到 WLAN 网络时才会接收推送通知。

Microsoft Exchange“自动发现”

iOS 支持 Microsoft Exchange Server 2007 和 Microsoft Exchange Server 2010 的“自动发现”服务。手动配置设备时，“自动发现”会使用你的电子邮件地址和密码来确定正确的 Exchange Server 信息。

有关启用“自动发现”服务的更多信息，请参阅“自动发现”服务。

Microsoft Exchange 全局地址列表

iOS 设备会从你所在公司的 Exchange Server 企业目录取回联络信息。你可以在搜索“通讯录”的同时访问此目录，当你输入电子邮件地址时，可自动访问此目录来补全电子邮件地址。iOS 6 或更高版本支持 GAL 照片（需要 Exchange Server 2010 SP 1 或更高版本）。

不支持的 Exchange ActiveSync 功能

不支持下列 Exchange 功能：

- 打开电子邮件中指向 Sharepoint 服务器上储存的文稿的链接
- 设定“不在办公室”自动回复信息

通过 Exchange 确定 iOS 版本

当 iOS 设备连接到 Exchange Server 时，该设备会报告其 iOS 版本。版本号是通过请求标头的“用户代理”栏来发送的，看起来类似于 Apple-iPhone2C1/705.018。分隔符 (/) 后面的数字是 iOS 版号，每个 iOS 版本的版号都是唯一的。

若要在设备上查看版号，请前往“设置”>“通用”>“关于”。你将看到版本号和版号，例如 4.1 (8B117A)。圆括号中的数字是版号，用来标识设备所运行的版本。

版号在发送到 Exchange Server 后，会从格式 NANNNA（其中 N 是数字，而 A 是字母字符）转换成 Exchange 格式 NNN.NNN。数值会予以保留，而字母会转换成其在字母表中的位置值。例如，“F”会转换成“06”，因为它是字母表中的第六个字母。如果需要，数字会使用零进行补白，以适合 Exchange 格式。

在本示例中，版号 7E18 会转换成 705.018。

第一个数字 7，仍然是“7”。字符 E 是字母表中的第五个字母，因此会转换成“05”。系统将根据格式需要，在转换后的结果中插入句点 (.)。后一个数字 18 会使用零进行补白，转换成“018”。

如果版号以字母结尾（如 5H11A），则数字会根据如上所述进行转换，结束字符的数值会被追加到字符串（字符串和该数值使用 3 个零进行分隔）。因此 5H11A 会变成 508.01100001。

远程擦除

你可以使用 Exchange 提供的功能远程擦除 iOS 设备上的内容。执行擦除操作会移除设备中的所有数据和配置信息，然后设备会被安全抹掉，并还原为原始的出厂设置。执行擦除操作会移除数据（已使用 256 位 AES 加密方法进行加密）的加密密钥，这会即刻导致所有数据不可恢复。

对于 Microsoft Exchange Server 2007 或更高版本，你可以使用 Exchange Management Console、Outlook Web Access 或 Exchange ActiveSync Mobile Administration Web Tool 执行远程擦除。对于 Microsoft Exchange Server 2003，你可以使用 Exchange ActiveSync Mobile Administration Web Tool 发起远程擦除。

此外，用户可以擦除自己的设备，方法是前往“设置”>“通用”>“还原”，然后选取“抹掉所有内容和设置”。设备还可以配置为在密码输入失败一定次数之后自动执行擦除。

基于标准的服务

由于 iOS 支持 IMAP 邮件协议、LDAP 目录服务、CalDAV 日历和 CardDAV 通讯录协议，因此几乎可以与任何基于标准的环境相集成。如果你的网络环境配置为需要用户鉴定和 SSL，iOS 可提供安全的方法来访问基于标准的公司电子邮件、日历、任务和通讯录。对于 SSL，iOS 支持 128 位加密和主要证书颁发机构颁发的 X.509 根证书。

在典型的部署中，iOS 设备可直接访问 IMAP 和 SMTP 邮件服务器，以无线方式收发电子邮件，并可与基于 IMAP 的服务器无线同步备忘录。iOS 设备可连接至公司的 LDAPv3 企业目录，用户因此能够在“邮件”、“通讯录”和“信息”应用程序中访问公司通讯录。通过与 CalDAV 服务器同步，用户可以无线方式创建和接受日历邀请、接收日历更新，并与“提醒事项”app 同步任务。凭借对 CardDAV 的支持，用户可使用 vCard 格式让一组联系人与 CardDAV 服务器保持同步。所有网络服务器可位于 DMZ 子网之内和/或公司防火墙之后。

WLAN

iOS 设备开箱即可安全连接到企业或来宾 WLAN 网络，这使用户可以快速、轻松地加入可用的无线网络，而无论他们是处于园区内还是路途之中。

加入 WLAN

用户可以将 iOS 设备设置成自动加入可用的 WLAN 网络。对于需要提供登录凭证或其他信息的 WLAN 网络，无需从 WLAN 设置或“邮件”等 app 中打开单独的浏览器会话，即可快速进行访问。凭借低能耗的持久 WLAN 连接，各种 app 可使用 WLAN 网络推送通知。

WPA2 企业级

iOS 支持符合行业标准的无线网络协议，包括 WPA2 企业级协议，确保能够从 iOS 设备安全地访问企业无线网络。WPA2 企业级使用 128 位 AES 加密，这是一种可靠的、基于块的加密方法，可为用户提供最高级别的数据保护。

由于 iOS 支持 802.1X，因此可以集成到广泛的 RADIUS 鉴定环境中。iOS 支持的 802.1X 无线鉴定方法包括 EAP-TLS、EAP-TTLS、EAP-FAST、PEAPv0、PEAPv1 和 LEAP。

漫游

iOS 支持 802.11k 和 802.11r，可在大型企业 WLAN 网络上漫游。802.11k 利用接入点的报告帮助 iOS 设备在 WLAN 接入点之间切换，而 802.11r 则可在设备于接入点间切换时简化 802.1X 鉴定。

为快速完成设置和部署，支持使用配置描述文件或 MDM 配置无线网络、安全、代理和鉴定设置。

虚拟专用网络

使用成熟的行业标准虚拟专用网络 (VPN) 协议，可在 iOS 中安全地访问专用公司网络。iOS 开箱即支持 Cisco IPSec、L2TP over IPSec 和 PPTP。如果你所在的组织支持上述某个协议，则无需额外的网络配置或第三方 app 即可将 iOS 设备连接至 VPN。

此外，iOS 还支持主流 VPN 提供商的 SSL VPN。用户只需从 App Store 下载由其中一家公司开发的 VPN 客户端 app，即可开始使用。SSL VPN 与 iOS 中支持的其他 VPN 协议一样，既可在设备上手动配置，也可以通过配置描述文件或 MDM 进行配置。

iOS 支持行业标准技术，例如 IPv6、代理服务器和隧道分离，可在连接至公司网络时提供丰富的 VPN 体验。iOS 还兼容多种鉴定方法，包括密码、双因素令牌和数字证书。对于基于证书进行鉴定的环境，iOS 提供了 VPN On Demand 来简化连接过程，该功能可在需要连接至指定的域时发起 VPN 会话。

通过 iOS 7，可将每个 app 配置为独立于设备上的其他 app 使用 VPN 连接。这样可以确保公司数据始终通过 VPN 连接传输，而其他数据（例如员工从 App Store 获得的个人 app）则不然。有关详细信息，请参阅本章后文中的“为 App 单独设置 VPN”。

支持的协议和鉴定方法

SSL VPN。支持使用密码、双因素令牌和证书进行用户鉴定。

Cisco IPSec。支持使用密码、双因素令牌进行用户鉴定，以及使用共享密钥和证书进行机器鉴定。

L2TP over IPSec。支持使用 MS-CHAP v2 密码、双因素令牌进行用户鉴定，以及使用共享密钥进行机器鉴定。

PPTP。支持使用 MS-CHAP v2 密码和双因素令牌进行用户鉴定。

SSL VPN 客户端

某些 SSL VPN 提供商创建了专门的 app，用来帮助配置 iOS 设备，以便与他们的解决方案结合使用。要配置设备以使用特定的解决方案，可安装配套的 app，也可以提供包含必要设置的配置描述文件。SSL VPN 解决方案包括：

- **Juniper Junos Pulse SSL VPN。**iOS 支持包含 Juniper Networks IVE package 7.0 和更高版本的 Juniper Networks SA Series SSL VPN Gateway 6.4 或更高版本。要进行配置，请安装 Junos Pulse app，该 app 可从 App Store 获取。

有关更多信息，请参阅 Juniper Networks 应用程序说明。

- **F5 SSL VPN**。iOS 支持 F5 BIG-IP Edge Gateway、Access Policy Manager 和 FirePass SSL VPN 解决方案。要进行配置，请安装 F5 BIG-IP Edge Client app，该 app 可从 App Store 获取。

  有关更多信息，请参阅 F5 技术简介保护 iPhone 访问公司 Web 应用程序时的安全。

- **Aruba Networks SSL VPN**。iOS 支持 Aruba Networks Mobility Controller。要进行配置，请安装 Aruba Networks VIA app，该 app 可从 App Store 获取。

  如需获取联系信息，请访问 Aruba Networks 网站。

- **SonicWALL SSL VPN**。iOS 支持 10.5.4 版或更高版本的 SonicWALL Aventall E-Class Secure Remote Access 设备、5.5 版或更高版本的 SonicWALL SRA 设备，以及 SonicWALL Next-Generation Firewall 设备（包括运行 SonicOS 5.8.1.0 或更高版本的 TZ、NSA 和 E-Class NSA）。要进行配置，请安装 SonicWALL Mobile Connect app，该 app 可从 App Store 获取。

  如需获取联系信息，请访问 SonicWALL 网站。

- **Check Point Mobile SSL VPN**。iOS 支持包含完全第 3 层 VPN 隧道的 Check Point Security Gateway。要进行配置，请安装 Check Point Mobile app，该 app 可从 App Store 获取。

- **OpenVPN SSL VPN**。iOS 支持 OpenVPN Access Server、Private Tunnel 和 OpenVPN Community。要进行配置，请安装 OpenVPN Connect app，该 app 可从 App Store 获取。

- **Palo Alto Networks GlobalProtect SSL VPN**。iOS 支持 Palo Alto Networks 的 GlobalProtect 网关。要进行配置，请安装 GlobalProtect for iOS app，该 app 可从 App Store 获取。

- **Cisco AnyConnect SSL VPN**。iOS 支持运行软件镜像 8.0(3).1 或更高版本的 Cisco Adaptive Security Appliance (ASA)。要进行配置，请安装 Cisco AnyConnect app，该 app 可从 App Store 获取。

VPN 设置指南

Cisco IPSec 设置指南

参考这些指南可配置 Cisco VPN 服务器，以便与 iOS 设备结合使用。iOS 支持 Cisco ASA 5500 Security Appliances 和 Cisco PIX Firewalls（软件版本为 7.2.x 或更高）。建议使用最新的 8.0.x 软件版本（或更高版本）。iOS 也支持 IOS 版本为 12.4(15)T 或更高的 Cisco IOS VPN 路由器。VPN 3000 系列集中器不支持 iOS VPN 功能。

代理设置

在进行所有这些配置时，还可以指定 VPN 代理。要为所有连接配置单一代理，请使用“手动”设置，提供地址、端口，并在必要时进行鉴定。要使用 PAC 或 WPAD 为设备提供自动代理配置文件，请使用“自动”设置。对于 PAC，请指定 PAC 文件的 URL。对于 WPAD，iOS 将在 DHCP 和 DNS 中查询适当的设置。

鉴定方式

iOS 支持以下鉴定方式：

- 预共享密钥 IPSec 鉴定，通过 xauth 进行用户鉴定。
- 利用客户端和服务器证书进行 IPSec 鉴定，可选择通过 xauth 进行用户鉴定。
- 混合鉴定，服务器提供证书，客户端提供预共享密钥，进行 IPSec 鉴定。用户鉴定必须通过 xauth 进行。
- 用户鉴定通过 xauth 提供，包括以下鉴定方式：
  - 用户名和密码
  - RSA SecurID
  - CRYPTOCard

鉴定群组

Cisco Unity 协议根据一组常见鉴定参数及其他参数，使用鉴定群组来分组用户。应当为 iOS 用户创建一个鉴定群组。对于预共享密钥鉴定和混合鉴定，群组名称必须在设备上配置，并且使用群组的共享密钥（预共享密钥）作为群组密码。

使用证书鉴定时，不会使用任何共享密钥。用户的群组根据证书中的栏位来确定。Cisco 服务器设置可用于将证书中的栏位对应到用户群组。

在 ISAKMP 优先级列表中，RSA-Sig 应该拥有最高优先级。

证书

设置和安装证书时，请确定符合以下要求：

服务器身份证书的主体备用名称 (SubjectAltName) 栏必须包含服务器的 DNS 名称和/或 IP 地址。设备使用此信息来验证证书是否属于服务器。为了获得更高的灵活性，可以使用通配符来指定 SubjectAltName，以达到按名称段匹配的目的，如 vpn.*.mycompany.com。如果未指定 SubjectAltName，可以将 DNS 名称放在通用名称栏中。

为服务器证书签名的 CA 证书需要安装在设备上。如果该证书不是根证书，请安装信任链的剩余部分以便证书得到信任。如果使用客户端证书，请确保为客户端证书签名的可信 CA 证书已安装在 VPN 服务器上。 使用基于证书的鉴定时，请确保服务器已设置为根据客户端证书中的栏位来识别用户的群组。

证书和证书颁发机构必须有效（例如，未过期）。不支持通过服务器发送证书链，应该关闭此功能。

IPSec 设置
使用以下 IPSec 设置：

- **模式。**隧道模式
- **IKE 交换模式。**“积极模式”（适用于预共享密钥鉴定和混合鉴定）或“主模式”（适用于证书鉴定）。
- **加密算法。**3DES、AES-128、AES-256。
- **鉴定算法。**HMAC-MD5、HMAC-SHA1。
- **Diffie-Hellman 群组。**预共享密钥鉴定和混合鉴定需要群组 2。对于证书鉴定，请配合 3DES 和 AES-128 使用群组 2。配合 AES-256 使用群组 2 或群组 5。
- **PFS（完全正向保密）。**对于 IKE 阶段 2，如果使用 PFS，则 Diffie-Hellman 群组必须与用于 IKE 阶段 1 的群组相同。
- **模式配置。**必须启用。
- **失效同层检测。**推荐。
- **标准 NAT 遍历。**受支持并且可以启用（不支持 IPSec over TCP）。
- **负载均衡。**受支持且可以启用。
- **阶段 1 的密钥更新。**当前不受支持。建议将服务器上的密钥更新时间设定为一小时。
- **ASA 地址掩码。**确保所有设备地址池掩码都未设定或都设定为 255.255.255.255。例如：asa(config-webvpn)# ip local pool vpn_users 10.0.0.1-10.0.0.254 mask 255.255.255.255。

如果使用建议的地址掩码，则可能会忽略 VPN 配置所采用的某些路由。若要避免发生这种情况，请确保路由表包含所有必要的路由，并且验证子网地址可以访问，然后再进行部署。

支持的其他功能

- **应用程序版本。**客户端软件版本会被发送到服务器，使服务器能够根据设备的软件版本接受或拒绝连接。
- **横幅。**横幅（如果是在服务器上配置的）会显示在设备上，用户必须接受它，否则会断开连接。
- **分离隧道。**支持分离隧道。
- **分离 DNS。**支持分离 DNS。
- **默认域。**支持默认域。

VPN On Demand

VPN On Demand 可使 iOS 自动建立安全连接，无需用户干预。系统会按照配置描述文件中定义的规则，在需要时启动 VPN 连接。

在 iOS 7 中，VPN On Demand 通过配置描述文件的 VPN 有效负载中的 OnDemandRules 键配置。系统分两个阶段应用规则：

- **网络检测阶段。**定义当设备的主要网络连接发生更改时适用的 VPN 要求。
- **连接计算阶段。**定义根据需要向域名发起连接请求时的 VPN 要求。

例如，规则可用于：

- 识别因 iOS 设备连接至内部网络而不需要 VPN 的情况。
- 识别因使用未知 WLAN 网络而需要对所有网络活动采取 VPN 的情况。
- 在针对指定域名的 DNS 请求失败后要求使用 VPN。

网络检测阶段

当设备的主要网络接口发生变化时，例如当 iOS 设备切换至不同的 WLAN 网络或者从 WLAN 切换至蜂窝网络时，将对 VPN On Demand 规则进行计算。如果主要接口为虚拟接口，例如 VPN 接口，将忽略 VPN On Demand 规则。

只有当每个组（字典）中的匹配规则全部匹配时，才会执行关联的操作；如果有任何一项规则不匹配，将对列表中的下一个字典进行计算，直至抵达 OnDemandRules 列表末尾。

最后一个字典应定义“默认”配置，即没有对应的规则，只有操作。这将找出没有与之前的规则匹配的所有连接。

连接计算阶段

VPN 可基于对某些域的连接请求按需触发，而不是基于网络接口单方面断开或连接 VPN。

按需匹配规则

指定以下一个或多个匹配规则：

- **InterfaceTypeMatch。**可选。WLAN 或蜂窝的字符串值。如果指定此规则，则当主要接口硬件为指定的类型时，即与此规则匹配。
- **SSIDMatch。**可选。要基于当前网络匹配的 SSID 列表。如果网络不是 WLAN 网络，或者其 SSID 未显示在列表中，则匹配失败。如果省略此键及其列表，将忽略 SSID。
- **DNSDomainMatch。**可选。搜索域字符串列表。如果为当前主要网络配置的 DNS 搜索域包括在此列表中，将与此属性匹配。支持通配符前缀 (*)；例如 *.example.com 将与 anything.example.com 匹配。

- **DNSServerAddressMatch**。可选。DNS 服务器地址字符串列表。如果当前为主要接口配置的所有 DNS 服务器地址都位于列表中，则将与此属性匹配。支持通配符 (*)；例如 1.2.3.* 将与带有 1.2.3. 前缀的任何 DNS 服务器匹配。
- **URLStringProbe**。可选。要探查其可访问性的服务器。不支持重定向。URL 应当为可信的 HTTPS 服务器。设备会发送 GET 请求来验证是否可以访问该服务器。

Action

此键定义当指定的所有匹配规则都计算为真时的 VPN 行为。此为必选键。Action 键的值包括：

- **Connect**。在下一次尝试建立网络连接时无条件启动 VPN 连接。
- **Disconnect**。断开 VPN 连接，不按需触发任何新的连接。
- **Ignore**。保留任何现有的 VPN 连接，但不按需触发任何新的连接。
- **Allow**。对于配备 iOS 6 或更低版本的 iOS 设备。请参阅本节后文中的“向后兼容性说明”。
- **EvaluateConnection**。对每次连接尝试计算 ActionParameters。使用此值时，需要通过键 ActionParameters（见下文）指定计算规则。

ActionParameters

具有如下所述的键的字典列表，按键的显示顺序计算。当 Action 为 EvaluateConnection 时，此为必选键。

- **Domains**。必选。定义此计算规则适用的域的字符串列表。支持通配符前缀，例如 *.example.com。
- **DomainAction**。必选。定义 Domains 的 VPN 行为。DomainAction 键的值包括：
  - **ConnectIfNeeded**。如果对 Domains 的 DNS 解析失败，例如 DNS 服务器指示其不能解析域名、DNS 响应遭到重定向或者连接失败或超时，将触发 VPN。
  - **NeverConnect**。不对 Domains 触发 VPN。

当 DomainAction 为 ConnectIfNeeded 时，还可以在连接计算字典中指定以下键：

- **RequiredDNSServers**。可选。要用于解析 Domains 的 DNS 服务器的 IP 地址列表。这些服务器不必是设备当前网络配置的一部分。如果无法访问这些 DNS 服务器，将触发 VPN。请配置内部 DNS 服务器或可信的外部 DNS 服务器。
- **RequiredURLStringProbe**。可选。要使用 GET 请求探查的 HTTP 或 HTTPS（首选）URL。如果对此服务器的 DNS 解析成功，则探查也一定会成功。如果探查失败，将触发 VPN。

向后兼容性说明
在 iOS 7 之前，域触发规则通过名为 OnDemandMatchDomainAlways、OnDemandMatchDomainOnRetry 和 OnDemandMatchDomainNever 的域的列表配置。iOS 7 仍然支持 OnRetry 和 Never 情形，尽管它们已被 EvaluateConnection 操作取代。

要创建同时适用于 iOS 7 和更早版本的描述文件，除了使用 OnDemandMatchDomain 列表外，还要使用新的 EvaluateConnection 键。iOS 的先前版本无法识别 EvaluateConnection 并将使用旧的列表，iOS 7 和更高版本将使用 EvaluateConnection。

指定 Allow 操作的旧配置描述文件仍适用于 iOS 7，但 OnDemandMatchDomainsAlways 域除外。

为 App 单独设置 VPN

iOS 7 新增了基于 app 建立 VPN 连接的功能。通过这种方式，可以更精确地控制哪些数据可以通过 VPN，哪些则不能如此。采用设备级 VPN 时，所有数据都通过专用网络传输，而不论其来自何处。随着组织中使用的个人自有设备越来越多，为 App 单独设置 VPN 可为供内部使用的 app 提供安全的网络连接，同时保护个人设备活动的隐私。

通过为 App 设置单独的 VPN，可使每个处于移动设备管理 (MDM) 范围内的 app 通过安全隧道与专用网络通信，同时禁止设备上未处于管理范围内的其他 app 使用专用网络。此外，对于处于管理范围内的每个 app，可以配置不同的 VPN 连接以进一步保护数据安全。例如，销售报价 app 可使用完全不同于应付帐款 app 的数据中心，而用户的个人 Web 浏览通信则使用公共互联网。这种在 app 层分离通信的功能为分离个人数据和组织数据创造了条件。

要为 App 设置单独的 VPN，app 必须由 MDM 管理并使用标准 iOS 网络 API。为 App 设置单独的 VPN 时，需要通过 MDM 配置来指定哪些 app 和 Safari 域可以使用此设置。有关 MDM 的更多信息，请参阅“第 3 章：配置和管理”。

单点登录 (SSO)

在 iOS 7 中，app 可通过 Kerberos 利用现有的企业内部单点登录基础架构。通过单点登录，用户只需输入一次密码，因而有助于改善用户体验。它还可以确保从不无线传送密码，从而提高日常使用 app 的安全性。

iOS 7 使用的 Kerberos 鉴定系统属于行业标准，是世界上部署最广泛的单点登录技术。如果你配置了 Active Directory、eDirectory 或 OpenDirectory，则可能已有Kerberos 系统可供 iOS 7 使用。为了进行用户鉴定，iOS 设备需要能够通过网络连接联系 Kerberos 服务。

支持的 app

对于使用 NSURLConnection 或 NSURLSession 类来管理网络连接和鉴定的 app，iOS 提供灵活的 Kerberos 单点登录 (SSO) 支持。Apple 向所有开发人员提供这些高级框架，以便他们将网络连接无缝集成到自己的 app 中。为帮助你入门，Apple 还以 Safari 为例说明如何在本机使用支持 SSO 的网站。

配置 SSO

单点登录通过配置描述文件进行配置，这些描述文件可以手动安装，也可以通过 MDM 管理。SSO 帐户有效负载允许进行灵活的配置。SSO 可向所有 app 开放，也可以按 app 标识符和/或服务 URL 进行限制。

在 URL 匹配方面，采用简单模式匹配，URL 必须以 http:// 或 https:// 开头。系统会基于整个 URL 进行匹配，因此请确保它们完全相同。例如，值为 https://www.example.com/ 的 URLPrefixMatches 将不会与 https://www.example.com:443/ 匹配。你可以指定 http:// 或 https:// 来仅对安全或常规 HTTP 服务使用 SSO。例如，使用值为 https:// 的 URLPrefixMatches 将只能对安全的 HTTPS 服务使用 SSO。如果 URL 匹配模式不是以斜杠 (/) 结尾，则在其末尾追加斜杠 (/)。

AppIdentifierMatches 列表必须包含与 app 捆绑包 ID 匹配的字符串。这些字符串可以是完全匹配项（例如 com.mycompany.myapp），也可以通过使用通配符 (*) 指定与捆绑包 ID 匹配的前缀。通配符必须位于句点字符 (.) 之后，并且只能位于字符串末尾（例如 com.mycompany.*）。在使用通配符的情况下，捆绑包 ID 以此前缀开头的任何 app 都将可以访问帐户。

数字证书

数字证书是一种身份识别形式，支持简化的鉴定、数据完整性和加密。数字证书由公钥、有关用户的信息和颁发证书的证书颁发机构组成。iOS 支持数字证书，从而使组织可以安全、简便地访问企业服务。

证书有多种用途。使用数字证书为数据签名有助于确保信息无法改动。证书还可用于确保作者或“签名者”身份的真实性。此外，可以使用证书对配置描述文件和网络通信进行加密，从而进一步保护机密或隐私信息。

例如，Safari 浏览器可以检查 X.509 数字证书的有效性，并使用最多 256 位的 AES 加密建立安全会话。这可以确保网站的身份合法，且与网站的通信受到保护，从而避免个人或机密数据遭到拦截。

支持的证书和身份格式：

- iOS 支持带有 RSA 密钥的 X.509 证书。
- 可以识别的文件扩展名包括 .cer、.crt、.der、.p12 和 .pfx。

在 iOS 中使用证书

根证书

iOS 开箱即提供一系列预安装的根证书。有关更多信息，请参阅此 Apple 支持文章中的列表。

一旦任何预安装的根证书遭到破坏，iOS 可无线更新证书。要停用此功能，可限制无线更新证书的操作。

如果你使用的根证书并非预安装的证书，例如由你所在的组织创建的自签名根证书，则可以使用下列方式之一进行分发。

分发和安装证书

将证书分发至 iOS 设备的操作非常简单。收到证书后，用户只需轻按即可查看内容，然后再次轻按即可将此证书添加到他们的设备。安装身份证书时，系统将提示用户输入可对此证书进行保护的密码。如果无法验证证书的真实性，则将其显示为不可信证书，用户可决定是否仍要将其添加到自己的设备中。

通过配置描述文件安装证书

如果使用配置描述文件分发企业服务（例如 Exchange、VPN 或 WLAN）的设置，则可将证书添加到描述文件中来简化部署。这包括通过 MDM 分发证书的功能。

通过“邮件”或 Safari 安装证书

如果证书是通过电子邮件发送的，它将显示为附件。还可以使用 Safari 从网页中下载证书。你可以将证书托管在安全的网站上，并向用户提供 URL，以便他们将证书下载到自己的设备上。

删除和撤销证书

要手动删除已经安装的证书，请选择“设置”>“通用”>“描述文件”，然后选择要删除的相应证书。如果用户删除的证书是访问帐户或网络所必需的，设备将无法再连接到这些服务。

通过移动设备管理服务器可以查看设备上的所有证书，以及删除其中已安装的任何证书。

此外，支持通过在线证书状态协议 (OCSP) 和 CRL（证书撤销清单）协议来检查证书的状态。使用支持 OCSP 或 CRL 的证书时，iOS 会定期对证书进行验证，确保它没有被撤销。

Bonjour

Bonjour 是 Apple 基于标准的零配置网络协议，可帮助设备找到网络上的服务。iOS 设备使用 Bonjour 发现兼容 AirPrint 的打印机和兼容 AirPlay 的设备。某些对等 app 也需要使用 Bonjour。你需要确保网络基础架构和 Bonjour 都得到正确配置，才能使二者配合工作。

iOS 7.1 设备还将通过蓝牙查找 AirPlay 来源。

有关 Bonjour 的更多信息，请参阅此 Apple 网页。

第 2 章：
安全

iOS 设有多个安全层。这种设计使 iOS 设备能够安全地访问网络服务和保护重要数据。iOS 对传输中的数据进行强加密，采用切实有效的鉴定方法访问企业服务，并对所有静态数据进行硬件加密。iOS 还使用可无线传递和强制实施的密码策略来提供安全保护。如果设备落入不法之徒手中，用户和 IT 管理员可以启动远程擦除命令擦除私人信息。

当考虑在企业中使用 iOS 的安全防护功能时，了解以下概念会很有帮助：

- **设备控制。**防止未经授权使用设备的方法
- **加密和数据保护。**保护静态数据的安全，即使设备丢失或被盗时也不例外
- **网络安全。**传输中数据的网络协议和加密
- **App 安全。**支持 app 安全运行而不损害平台的完整性
- **互联网服务。**Apple 基于网络的通信、同步和备份基础架构

这些功能协同工作，提供安全的移动计算平台。

设备安全

制定强有力的 iOS 访问策略对于保护企业信息至关重要。设备密码是防止未授权访问的第一道防线，可进行无线配置和强制执行。iOS 设备使用每位用户设立的唯一密码生成强大的加密密钥，进一步保护设备上的邮件和敏感的应用程序数据。此外，iOS 提供了一系列安全的方法用于在 IT 环境中配置设备，该环境必须已配置特定的设置、策略和限制。通过选择这些方法，可以灵活地为授权用户设立标准保护级别。

密码策略

设备密码可防止未经授权的用户访问数据或以其他方式使用设备。iOS 允许你根据自己的安全需求从大量的密码策略中进行选择，这些策略包括超时时间、密码强度和必须更换密码的频率。

支持下列密码策略：

- 要求设备密码
- 要求字母数字值
- 最短的密码长度
- 必须包含的复杂字符的最少数目
- 密码的最长有效期
- 自动锁定前的时间
- 密码历史记录
- 设备锁定宽限期
- 最多可允许的尝试失败次数

策略强制执行

策略可纳入配置描述文件并分发给用户安装。描述文件可采取特殊的定义方式，以便只有在提供管理密码的情况下才能将其删除，或者将描述文件绑定到设备，不完全擦除设备内容就无法将其删除。此外，密码设置可使用能够直接向设备推送策略的移动设备管理 (MDM) 解决方案进行配置。这样，用户无需执行任何操作，即可强制执行和更新策略。

如果设备配置为访问 Microsoft Exchange 帐户，则向设备无线推送 Exchange ActiveSync 策略。可用的策略集因 Exchange ActiveSync 和 Exchange Server 的版本而异。如果同时存在 Exchange 策略和 MDM 策略，将应用较为严格的那一种策略。

安全的设备配置

配置描述文件是 XML 文件，其中包含下列内容：设备安全策略和限制、VPN 配置信息、WLAN 设置、电子邮件和日历帐户，以及可使 iOS 设备与 IT 系统结合使用的鉴定凭证。这种在配置描述文件中设立密码策略和设备设置的功能，可确保按照 IT 部门制定的安全标准正确配置组织中的设备。此外，由于配置描述文件可以加密和锁定，因此这些设置无法被删除、篡改或与他人共享。

配置描述文件可以同时进行签名和加密。通过对配置描述文件签名，可确保不能以任何方式篡改它所强制执行的设置。通过加密配置描述文件，可保护描述文件的内容，并只允许将其安装在既定的目标设备上。配置描述文件采用支持 3DES 和 AES-128 的 CMS（加密消息语法 RFC 3852）进行加密。

首次分发经过加密的配置描述文件时，可使用 Apple Configurator 通过 USB 安装，或者使用无线描述文件传送和配置协议或 MDM 无线安装。后续加密的配置描述文件可通过电子邮件附件传送、托管在可供用户访问的网站上，或者推送至使用 MDM 解决方案的设备上。

有关更多信息，请参阅 iOS 开发人员资料库网站上的无线描述文件传送和配置协议。

设备限制

设备限制可决定用户能够在设备上访问哪些功能。通常，这些功能涉及支持网络的应用程序，例如 Safari、YouTube 或 iTunes Store，但限制还可以控制诸如 app 安装或摄像头使用之类的设备功能。通过限制可按照自身要求配置设备，同时允许用户按照组织的策略使用设备。你可以在每台设备上手动配置限制、使用配置描述文件强制执行限制，或者通过 MDM 解决方案远程设立限制。此外，与密码策略一样，可通过 Microsoft Exchange Server 2007 和 2010 强制执行摄像头或 Web 浏览限制。限制还可用于防止邮件在不同的帐户之间迁移，或者在一个帐户中收到的邮件被转发给另一个帐户。

有关支持的限制的信息，请参阅附录 B。

加密和数据保护

对于包含敏感信息的任何环境而言，保护 iOS 设备上存储的数据都至关重要。除了对传输中的数据进行加密外，iOS 设备还对设备上存储的所有数据提供硬件加密，并对电子邮件和应用程序数据提供额外加密，以增强数据保护。

加密

iOS 设备采用基于硬件的加密。硬件加密使用 256 位 AES 来保护设备上的所有数据。加密始终处于启用状态，无法停用。此外，还可以加密 iTunes 中备份到用户电脑中的数据。该功能可由用户启用或通过配置描述文件中的设备限制设置强制执行。iOS 还在邮件中支持 S/MIME，让用户可以查看和发送加密的电子邮件。

经验证，iOS 7 和 iOS 6 中的加密模块符合美国联邦信息处理标准 (FIPS) 140-2 级别 1。这证明，在使用 iOS 加密服务的 Apple app 和第三方 app 中，加密操作具有完整性。

有关更多信息，请参阅 iOS 产品安全性：验证和指导和 iOS 7：Apple FIPS iOS 加密模块 v4.0。

数据保护

存储在设备上的电子邮件和附件可通过使用 iOS 内置的数据保护功能获得进一步的保护。数据保护利用每个用户唯一的设备密码和 iOS 设备上的硬件加密生成强大的加密密钥。此密钥可在设备被锁定时禁止访问数据，即使在设备被盗的情况下也能确保重要信息的安全。

要打开数据保护功能，只需在设备上设置一个密码即可。数据保护的有效性取决于密码强度，因此在建立密码策略时，必须要求并强制使用超过四位数的密码，这一点至关重要。用户可以通过查看密码设置屏幕来验证是否已在设备上启用了数据保护。移动设备管理解决方案也能从设备上查询此信息。

数据保护 API 还向开发人员开放，并可用于保护 App Store app 或定制开发的企业内部 app 中的数据安全。从 iOS 7 开始，应用程序存储的数据在默认情况下属于“在首次用户鉴定之前提供保护”安全级别，这与台式机上的完整磁盘加密类似，可保护数据免遭涉及重新启动的攻击。

注：如果设备自 iOS 6 升级而来，原来存储的数据不会转换为这一新级别。通过删除并重新安装 app，可使 app 获得新的安全级别。

Touch ID

Touch ID 是 iPhone 5s 中内置的指纹感应系统，有助于更快、更轻松地对设备进行高度安全的访问。此前瞻性技术可从任意角度读取指纹，感应器会在每次使用时识别更多重叠的节点，从而不断扩展指纹图，逐步加深对用户指纹的认识。

Touch ID 让使用更长、更复杂的密码变得更加实际，因为用户无需经常输入密码。Touch ID 还克服了基于密码进行锁定的不便，它并不取代密码锁定机制，而是允许在精心设计的边界和限制内安全地访问设备。

启用 Touch ID 后，iPhone 5s 会在按下“睡眠/唤醒”按钮时立即锁定。在仅使用密码的安全机制下，许多用户设置解锁宽限期，以免每次使用设备时都输入密码。借助 Touch ID，iPhone 5s 每次进入睡眠模式时都会锁定，而每次唤醒时都需要提供指纹，也可以选择提供密码。

Touch ID 可与 Secure Enclave 配合使用，后者是 Apple A7 芯片中的协处理器。Secure Enclave 拥有自己的内存空间（已加密和保护），并能够与 Touch ID 感应器安全通信。当 iPhone 5s 锁定时，将使用 Secure Enclave 加密内存中的密钥保护数据保护级别为“完全”的密钥。该密钥最长存放 48 小时，如果重新启动 iPhone 5s 或者使用五次无法识别的指纹，将丢弃该密钥。如果可以识别指纹，Secure Enclave 将提供用于释放数据保护密钥的密钥，从而使设备得到解锁。

远程擦除

iOS 支持远程擦除。如果设备丢失或被盗，管理员或设备所有者可发出远程擦除命令，该命令将删除所有数据并禁用该设备。如果设备使用 Exchange 帐户进行配置，则管理员可使用 Exchange Management Console (Exchange Server 2007) 或 Exchange ActiveSync Mobile Administration Web Tool（Exchange Server 2003 或 2007）启动远程擦除命令。Exchange Server 2007 用户还可以使用 Outlook Web Access 直接启动远程擦除命令。远程擦除命令还可以通过 MDM 解决方案或使用 iCloud 的“查找我的 iPhone”功能发起，即使没有使用 Exchange 企业服务，也不例外。

本地擦除

设备还可配置为在若干次密码输入尝试失败后，自动启动本地擦除。这可以防止强力侵入设备的尝试。设立密码后，用户可以在设置中直接启用本地擦除。默认情况下，iOS 会在 10 次输入密码失败后自动擦除设备。与其他密码策略一样，最大失败尝试次数可通过配置描述文件或 MDM 设定，或者通过 Microsoft Exchange ActiveSync 策略以无线方式强制执行。

“查找我的 iPhone”和激活锁

如果设备丢失或被盗，则停用设备和抹掉设备上的数据非常重要。在 iOS 7 中，如果启用了“查找我的 iPhone”，则必须输入所有者的 Apple ID 凭证，才能重新激活设备。对于机构拥有的设备，最好实施监督，或者设立策略供用户停用此功能，以免“查找我的 iPhone”妨碍组织将设备分配给其他人使用。

在 iOS 7.1 或更高版本中，某个用户开启“查找我的 iPhone”时，你可以使用兼容的 MDM 解决方案来启用激活锁。在激活锁启用后，你的 MDM 解决方案会存储一个绕过码，之后如需抹掉设备上的数据并将其部署给新用户时，可使用该代码自动清除激活锁。请参阅 MDM 解决方案文档以了解详细信息。

有关“查找我的 iPhone”和激活锁的更多信息，请参阅 iCloud 支持和移动设备管理和“查找我的 iPhone”激活锁。

网络安全
- 内置 Cisco IPSec、L2TP、PPTP VPN
- 通过 App Store app 的 SSL VPN
- 采用 X.509 证书的 SSL/TLS
- 采用 802.1X 的 WPA/WPA2 企业级协议
- 基于证书的鉴定
- RSA SecurID、CRYPTOCard

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

鉴定方式
- 密码 (MSCHAPv2)
- RSA SecurID
- CRYPTOCard
- X.509 数字证书
- 共享密钥

802.1X 鉴定协议
- EAP-TLS
- EAP-TTLS
- EAP-FAST
- EAP-SIM
- PEAP v0、v1
- LEAP

支持的证书格式

iOS 支持带有 RSA 密钥的 X.509 证书。可以识别的文件扩展名包括 .cer、.crt 和 .der。

网络安全

移动用户必须可以在世界的任何地方都能访问公司的网络信息，但是确保用户已获得授权并且数据在传输过程中受到保护也是非常重要的。iOS 提供久经验证的技术，可在 WLAN 和蜂窝数据网络连接中实现这些安全目标。

除了现有的基础架构，每一次 FaceTime 会话和 iMessage 对话也都进行了端到端加密。iOS 为每位用户创建一个唯一的 ID，确保通信已正确地加密、路由和连接。

VPN

许多企业环境都设有某种形式的虚拟专用网络 (VPN)。这些安全网络服务已经过部署，通常只需要很少的设置和配置就能与 iOS 配合使用。iOS 开箱即可与多种常用的 VPN 技术相集成。有关详细信息，请参阅第 1 章中的“虚拟专用网络”。

SSL/TLS

iOS 支持 SSL v3 和传输层安全（TLS v1.0、1.1 和 1.2）。
Safari、“日历”、“邮件”和其他互联网应用程序会自动启动这些机制，在 iOS 和企业服务之间形成加密的通信渠道。

WPA/WPA2

iOS 支持 WPA2 企业级网络，以便通过鉴定方式访问你的企业无线网络。WPA2 企业级采用 128 位 AES 加密，为用户提供最高级别的保障，在用户通过 WLAN 网络连接发送和接收通信时，使其数据始终处于保护之下。由于支持 802.1X，iPhone 和 iPad 可以集成到广泛的 RADIUS 鉴定环境中。

App 安全

iOS 以确保安全为核心设计宗旨。它以沙箱方式进行应用程序运行时保护和应用程序签名，可确保 app 不会遭到篡改。iOS 还提供了一个框架，有助于将应用程序和网络服务凭证安全存放在一个加密的存储位置（称为钥匙串）。对于开发人员，它提供了通用加密架构，可用于加密应用程序数据存储。

运行时保护

设备上的 app 都在沙箱模式下运行，可限制其访问由其他 app 存储的数据。此外，系统文件、资源和内核会与用户的应用程序空间保持屏蔽。如果某个 app 需要访问来自其他 app 的数据，它只能使用 iOS 提供的 API 和服务来完成此操作。这还可以防止生成代码。

强制代码签名

所有 iOS app 都必须经过签名。设备附带的 app 由 Apple 签名。第三方 app 由开发者使用 Apple 颁发的证书进行签名。这可确保 app 未被篡改或更改。此外，还会执行运行时检查，确保 app 自上次使用后仍然可信。

对于自定开发的企业内部 app，可使用预置描述文件来控制其 使用。用户必须安装预置描述文件才能执行应用程序。预置描述文件可通过 MDM 解决方案以无线方式安装。管理员还可以只允许特定的设备使用应用程序。

安全的鉴定框架

iOS 提供安全、加密的钥匙串来存储数字身份、用户名和密码。钥匙串数据是分区的，以使第三方 app 存储的凭证不会被使用其他身份的 app 访问。这为企业内 iOS 设备上的一系列应用程序和服务的鉴定凭证提供了保护机制。

通用加密架构

应用程序开发人员可访问加密 API，用来进一步保护其数据。它可使用 AES、RC4 或 3DES 等经过验证的方法进行对称加密。此外，iOS 设备对 AES 加密和 SHA1 哈希提供硬件加速，可最大限度地提高应用程序的性能。

应用程序数据保护

App 也可利用 iOS 设备内置的硬件加密以进一步保护敏感的应用程序数据。开发者可以指定要进行数据保护的具体文件，要求系统在设备锁定时将该文件的内容加密，app 和任何潜在入侵者都不得访问。

App 授权

默认情况下，iOS app 仅具有非常有限的权限。开发人员必须明确添加授权才能使用 iCloud、后台处理或共享钥匙串等大部分功能。这可以确保 app 无法为自己授予本来不具备的数据访问权限。此外，iOS app 在使用许多 iOS 功能（例如 GPS 定位、用户通讯录、摄像头或存储的照片）之前，必须得到用户的明确准许。

互联网服务

Apple 构建了一系列强大的服务来帮助用户更充分地使用设备并提高工作效率，其中包括 iMessage、FaceTime、Siri、iCloud、iCloud 云备份和 iCloud 钥匙串。

这些互联网服务在设计上继承了 iOS 在整个平台中推行的安全目标。这些目标包括：安全处理数据，无论数据存储在设备上还是在通过无线网络进行传输；保护用户的个人信息；防范威胁，阻止对信息和服务进行恶意或未经授权的访问。每一种服务都采用自己强大的安全架构，丝毫不会影响 iOS 的整体易用性。

iMessage

iMessage[1] 是一种适用于 iOS 设备和 Mac 电脑的通信服务。iMessage 支持文本和附件，例如照片、通讯录和位置。信息显示在用户注册的所有设备上，用户可使用任一设备继续之前的谈话。iMessage 大量使用 Apple 推送通知服务 (APN)。iMessage 采用端到端加密方式，只有发送和接收设备知道密钥。Apple 无法对信息解密，也不会记录这些信息。

FaceTime

FaceTime[2] 是 Apple 的视频和音频呼叫服务。FaceTime 通话使用 Apple 推送通知服务建立初始连接，然后使用互联网连接设立 (ICE) 和会话启动协议 (SIP) 创建加密的数据流。

Siri

用户只需自然发声即可通过 Siri[3] 发送信息、安排会议、拨打电话及执行其他操作。Siri 采用语音识别、文本语音转换以及“客户端-服务器”模式，可响应多种请求。Siri 支持的任务经过专门设计，可确保只使用尽可能少的个人信息，并对这些信息提供全面保护。Siri 的请求和录音都没有可用于识别个人身份的因素，而且 Siri 功能都尽可能在设备而非服务器上执行。

iCloud

iCloud[4] 可以存储音乐、照片、app、日历、文稿等内容，并自动将它们推送至用户的所有设备。iCloud 也可以每天通过 WLAN 备份信息，包括设备设置、app 数据以及短信和彩信。iCloud 通过以下方式来确保内容的安全：通过互联网发送内容时对内容进行加密、以加密方式储存内容以及使用安全令牌进行鉴定。另外，可以通过配置描述文件停用 iCloud 功能，包括照片流、文稿同步和备份。

有关 iCloud 安全性和隐私政策的更多信息，请参阅 iCloud 安全性与隐私政策概览。

iCloud 云备份

iCloud 也可以每天通过 WLAN 备份信息，包括设备设置、app 数据以及短信和彩信。iCloud 通过以下方式来确保内容的安全：通过互联网发送内容时对内容进行加密、以加密方式储存内容以及使用安全令牌进行鉴定。只有当设备已经锁定、连接到电源并且能够通过 WLAN 访问互联网时，才会发生 iCloud 云备份。由于 iOS 采用独特的加密技术，因此系统经过专门设计，既可保护数据安全，又能进行无人值守式增量备份和还原。

iCloud 钥匙串

iCloud 钥匙串可帮助用户在 iOS 设备和 Mac 电脑之间安全地同步密码，而不会将此信息泄露给 Apple。除了强大的隐私和安全性能外，对 iCloud 钥匙串的设计和架构起到重大影响的其他目标还有易用性，以及恢复钥匙串的能力。iCloud 钥匙串由两项服务构成：钥匙串同步和钥匙串恢复。在钥匙串同步中，设备只有经过用户批准才能加入同步过程，符合同步条件的每个钥匙串项通过 iCloud 密钥值存储与每个设备的加密密钥进行交换。这些项均为临时项，同步完毕后不会留在 iCloud 中。钥匙串恢复提供了一条途径，可使用户将其钥匙串交由 Apple 管理，而不让 Apple 读取其中包含的密码和其他数据。即使用户只有一部设备，钥匙串恢复也可以提供安全的网络来防止数据丢失。当使用 Safari 为 Web 帐户生成随机的强大密码时，这一点就特别重要，因为这些密码的唯一记录就存储在钥匙串中。钥匙串恢复包含两大基本要素：二次鉴定和安全托管服务，后者是 Apple 专为支持此功能而创建的服务。用户的钥匙串通过强大的密码加密，只有在满足一组严格的条件时，托管服务才会提供钥匙串的拷贝。

有关安全性的详细信息，请参阅 iOS 安全指南。

第 3 章：
配置和管理

iOS 部署可通过一系列管理技术进行简化，这包括简化帐户设置、配置机构策略、分发 app 和应用设备限制。用户随后可使用 iOS 中内置的设置助理自行完成大部分配置工作。在 MDM 中配置并注册 iOS 设备后，即可由 IT 进行无线管理。

本章介绍如何使用配置描述文件和移动设备管理来支持 iOS 部署。

设备设置和激活

iOS 开箱即允许用户通过 iOS 中的设置助理来激活设备、配置基本设置并立即开展工作。除基本设置外，用户还可以自定他们的个人偏好设置，例如语言、位置、Siri、iCloud 和“查找我的 iPhone”。通过设置助理，用户还可以创建个人 Apple ID（如果还没有此 ID）。

Apple ID

Apple ID 是一种身份，用于登录各种 Apple 设备，例如 FaceTime、iMessage、iTunes、App Store、iCloud 和 iBooks Store。凭借 Apple ID，每个用户都可以从 iTunes Store、App Store 或 iBooks Store 安装 app、图书和内容。用户还可以使用 Apple ID 注册 iCloud 帐户，以便在多部设备上访问和共享内容。

为充分利用这些服务，用户应使用自己的个人 Apple ID。如果用户还没有 Apple ID，可在获得设备之前就创建一个，这样可以尽快地完成配置。

要了解如何注册 Apple ID，请参阅我的 Apple ID。

使用 Apple Configurator 准备设备

对于由 IT 集中管理而非由各个用户分别设置的设备，Apple Configurator 可用于快速激活设备、定义和应用配置、监管设备、安装 app 以及将设备更新至最新的 iOS 版本。Apple Configurator 是一款适用于 OS X 的免费应用程序，可从 Mac App Store 下载。设备需要通过 USB 连接至 Mac 才能执行这些任务。你还可以将备份还原到设备，这会应用设备设置和主屏幕布局，并安装 app 数据。

配置描述文件

配置描述文件是 XML 文件，其中包含下列内容：设备安全策略和限制、VPN 配置信息、WLAN 设置、电子邮件和日历帐户，以及可使 iOS 设备与 IT 系统结合使用的鉴定凭证。配置描述文件能快速地将设置和授权信息载入到设备上。有些 VPN 和 WLAN 设置只能使用配置描述文件来设定，而且如果你使用的不是 Microsoft Exchange，则将需要使用配置描述文件来设定设备密码策略。

配置描述文件可使用无线描述文件传送或通过移动设备管理 (MDM) 进行分发。你还可以使用 Apple Configurator 将配置描述文件安装在通过 USB 连接到电脑的设备上，或者通过电子邮件或网页来分发配置描述文件。当用户在他们的设备上打开电子邮件附件或使用 Safari 下载描述文件时，会提示他们开始安装过程。如果你使用的是 MDM 服务器，则可以分发仅包含服务器配置信息的初始描述文件，然后让设备以无线方式获取所有其他描述文件。

配置描述文件可被加密和签名，这会允许你将它们限制用于特定设备并阻止任何人更改描述文件所含有的设置。你还可以将描述文件标记为锁定到设备，这样描述文件在安装后就不能移除，除非擦除设备上的所有数据，或者输入密码（可选）。

用户不能更改配置描述文件中提供的设置，除非使用密码。此外，由描述文件配置的帐户（如 Exchange 帐户）只能通过删除相应的描述文件来删除。

有关更多信息，请参阅 iOS 开发人员资料库网站上的配置描述文件重要参考。

移动设备管理 (MDM)

iOS 具有内置 MDM 框架，允许第三方 MDM 解决方案与 iOS 设备无线交互。这款轻便框架完全针对 iOS 设备而设计，功能强大且可以扩展，足以配置和管理一所组织内的所有 iOS 设备。

有了 MDM 解决方案，IT 管理员可将设备安全融入企业环境中。不仅能配置和更新设置，监督企业策略的贯彻情况，还可远程擦除或锁定被管理的设备。iOS MDM 为 IT 提供了一种简便的方式来支持用户对网络服务的访问，同时确保设备得到适当配置，而不论它们归谁所有。

MDM 解决方案使用 Apple 推送通知服务 (APN)，以通过公共和专用网络与设备持续通信。MDM 需要多个证书才能运行，包括与客户端通信的 APN 证书和用于安全通信的 SSL 证书。MDM 解决方案还可以通过证书签署描述文件。

大多数证书（包括 APNS 证书）必须手动续订。证书过期后，MDM 服务器将无法与客户端通信，直到证书得到更新。在证书过期之前，请做好更新所有 MDM 证书的准备。

有关 MDM 证书的更多信息，请参阅 Apple 推送证书门户。

注册

注册设备后，将启用编录和资产管理。注册过程可利用简单证书注册协议 (SCEP)，它允许 iOS 设备创建并注册唯一的身份证书，供机构服务进行使用鉴定。

在大多数情况下，用户可决定是否在 MDM 中注册其设备，并可以随时取消与 MDM 的关联。各机构应考虑采取一些激励措施，鼓励用户保持托管状态。例如，通过使用 MDM 解决方案自动提供无线凭证，要求完成 MDM 注册才能访问 WLAN 网络。当用户离开 MDM 时，设备会尝试通知 MDM 服务器。

配置

设备一旦注册，移动设备管理服务器就可以动态配置其设置和策略，此服务器会向设备发送配置描述文件，而设备会以自动和静默的方式安装这些描述文件。

配置描述文件可进行签名、加密和锁定（防止更改或共享设置），从而确保仅允许按照你的具体要求而配置的可信用户和设备访问你的网络和服务。如果用户将设备与 MDM 解除关联，则通过 MDM 安装的所有设置都会被删除。

帐户

移动设备管理可自动设置组织用户的邮件和其他帐户，帮助他们更快上手。根据 MDM 产品以及与内部系统的集成情况，帐户有效负载还可以预先填充用户的名称、邮件地址以及用于鉴定和签名的证书标识（如果适用）。MDM 可配置以下类型的帐户：

- 邮件
- 日历
- 已订阅的日历
- 通讯录
- Exchange ActiveSync
- LDAP

托管邮件和日历帐户遵守 iOS 7 中的“托管打开方式”限制。

查询

移动设备管理服务器能够查询设备的各种信息。这包括诸如序列号、设备 UDID 或 WLAN MAC 地址等硬件信息，以及 iOS 版本和设备上安装的所有 app 的详细列表等软件信息。这些信息可用来帮助确保用户维护一组适当的 app。

命令

当设备处于托管状态时，移动设备管理服务器可通过一组特定的操作对其进行管理。管理任务包括：

- **更改配置设置。**可发送一个命令，以便在设备上安装新的或更新后的配置描述文件。配置更改可静默进行，无需与用户进行交互。
- **锁定设备。**如果需要立即锁定设备，则可发送一个命令，以便使用当前设定的密码将其锁定。
- **远程擦除设备。**如果设备丢失或被窃，则可发送一个命令，以便抹掉设备上的所有数据。一旦收到远程擦除命令，此操作便无法还原。
- **清除密码锁定。**清除设备的密码后，设备会立即要求用户输入新密码。当用户忘记密码并希望 IT 为其重设密码时，可使用此命令。
- **请求 AirPlay 镜像和停止 AirPlay 镜像。**iOS 7 添加了一个命令，用来提示受监管的 iOS 设备开始向特定位置进行 AirPlay 镜像或终止当前的 AirPlay 会话。

托管 app

组织经常需要分发软件来帮助他们的用户提高工作效率或课堂效率。与此同时，组织需要控制该软件如何连接内部资源或在用户离开组织后如何处理数据安全问题，这一切都要与用户的个人 app 和数据共存。借助 iOS 7 中的托管 app，组织可以使用 MDM 无线分发企业 app，同时在机构安全与用户个性化之间取得适当平衡。

MDM 服务器可以将 App Store app 和企业内部 app 以无线方式部署到设备。

托管 app 可由 MDM 服务器远程删除，或在用户从 MDM 删除其自有设备时删除。删除 app 时将同时删除与之关联的数据。

iOS 7 和移动设备管理为 iOS 7 中的托管 app 添加了一套附加限制和功能，以便提供更高的安全性和更好的用户体验：

- **托管打开方式。**提供两种有用的功能，用来保护组织的 app 数据：
  - **允许在托管 app 中打开使用非托管 app 创建的文稿。**实施这一限制可防止用户的个人 app 和帐户打开组织的托管 app 中的文稿。例如，这样的限制可以防止用户使用 Keynote 打开保护机构内部的 PDF 阅读器中的 PDF 文稿。此限制还可防止用户的个人 iCloud 帐户在组织的 Pages 副本中打开文字处理文稿附件。
  - **允许在非托管 app 中打开使用托管 app 创建的文稿。**实施这一限制可防止组织的托管 app 和帐户在用户的个人 app 中打开文稿。此限制可防止在用户的任何个人 app 中打开组织托管电子邮件帐户中的机密电子邮件附件。
- **App 配置。**App 开发者可以标识出那些在作为托管 app 安装时可配置的 app 设置。这些配置设置可以在安装托管 app 之前或之后安装。
- **App 反馈。**构建 app 的开发者可以标识出可使用 MDM 从托管 app 中读取的 app 设置。例如，开发者可以指定一个“DidFinishSetup”键用于 app 反馈，MDM 服务器可以查询此键以确定 app 是否已启动和设置。
- **防止备份。**此限制可防止托管 app 将数据备份到 iCloud 或 iTunes。如果禁止备份，则在通过 MDM 删除托管 app，然后用户又重新安装该 app 后，可防止恢复 app 数据。

设备监管

默认情况下，所有 iOS 设备都不受监管。要启用附加配置选项和限制，你可以选择使用 Apple Configurator 监管归组织所有的 iOS 设备。

当在计划中将设备分配给 MDM 服务器后，可使用组织的 MDM 服务器应用描述文件和附加功能。

这些功能包括：

- 设备监管
- 强制配置
- 可锁定 MDM 设置
- 跳过设置助理中的步骤

可跳过的设置助理屏幕包括：

- **密码。**跳过密码设置
- **位置。**不启用定位服务
- **从备份恢复。**不从备份恢复
- **Apple ID。**不提示你使用 Apple ID 登录
- **服务条款。**跳过服务条款
- **Siri。**不启用 Siri
- **发送诊断。**不自动发送诊断信息

受监管的设备

监管功能为归组织所有的设备提供了更高的设备管理水平，可以实现诸如关闭 iMessage 或 Game Center 等附加限制。它还提供了诸如 Web 内容过滤等附加设备配置和功能，还可以实现静默安装 app。可以在设备上使用 Apple Configurator 以无线方式启用监管。

请参见附录 B，了解可在受监管设备上启用的具体限制。

第 4 章：
App 分发

iOS 附带一套 app，可供组织内的用户执行日常所需的全部任务，例如，电子邮件、管理日历、跟踪记录联系人，以及通过 Web 消费内容。很多能够帮助用户提高效率的功能均来自 App Store 中提供的成千上万的第三方 iOS app，或定制开发的企业内部 app。

iOS 开发者企业计划的成员可以创建和部署自己的企业内部 app。本章介绍可用于向用户部署 app 的方法。

企业内部 App

如果你自行开发 iOS app 来供你的组织使用，则可通过 iOS 开发者企业计划部署企业内部 app。部署企业内部 app 的过程如下：

- 注册 iOS 开发者企业计划。
- 准备好要进行分发的 app。
- 创建企业分发预置描述文件，用于授权设备使用你已签名的 app。
- 使用预置描述文件构建 app。
- 为用户部署 app。

注册以进行 app 开发

要开发和部署 iOS 企业内部 app，首先需要注册 iOS 开发者企业计划。

一旦注册，你便可以请求开发者证书和开发者预置描述文件。你在开发过程中使用这些文件来构建和测试你的 app。开发预置描述文件允许那些使用你的开发者证书进行签名的 app 在注册设备上运行。你可以在 iOS Provisioning Portal 上创建开发者预置描述文件。该临时描述文件在 3 个月后过期，并会按设备 ID 指定哪些设备可以运行 app 的开发版本。你可以将开发者签名的版本和开发预置描述文件分发给你的 app 团队和测试人员。

准备好要进行分发的 app

在完成开发和测试并准备好部署你的 app 后，你可以使用分发证书给 app 签名，并将其与预置描述文件一起打包。为你的计划成员资格指定的团队代理或管理员会在 iOS Provisioning Portal 上创建该证书和描述文件。

在生成分发证书的过程中，会使用“证书助理”（OS X 开发系统上“钥匙串访问”app 的一部分）来生成证书签名请求 (CSR)。你应将 CSR 上传到 iOS Provisioning Portal，然后会收到分发证书作为回复。当你在“钥匙串”中安装此证书时，可以设定 Xcode 使用此证书为你的 app 签名。

预置企业内部 app

利用企业分发预置描述文件，可以将你的 app 安装到任意数量的 iOS 设备上。你可以为特定 app 或多个 app 创建企业分发预置描述文件。

当你在 Mac 上同时安装企业分发证书和预置描述文件后，便可以使用 Xcode 来签署和构建 app 的发行/生产版本。企业分发证书的有效期是 3 年，有效期过后，你必须使用续订的证书再次签署和构建你的 app。App 预置描述文件的有效期是一年，所以你需要每年发布一次新预置描述文件。请参见附录 C 中的“提供更新后的 app”以了解更多详情。

你应限制对你的分发证书及其专用密钥的访问，这非常重要。使用 OS X 上的“钥匙串访问”可利用 p12 格式导出和备份这些项目。如果专用密钥丢失，则无法再次恢复或下载。除了确保证书和专用密钥的安全外，你还应该限制对负责最终接受 app 的人员的接触。使用分发证书给应用程序签名相当于批准 app 的内容和功能，表明遵循企业开发者协议的许可条款。

部署 App

你可以通过四种方式来部署 app：

- 分发 app 以便用户使用 iTunes 进行安装。
- 让 IT 管理员使用 Apple Configurator 将 app 安装到设备上。
- 将 app 发布到安全的 Web 服务器；用户以无线方式访问和执行安装。请参阅“附录 C：以无线方式安装企业内部 App”。
- 使用你的 MDM 服务器来指示托管设备安装企业内部 app 或 App Store app（如果你的 MDM 服务器支持该功能）。

使用 iTunes 安装 app

如果你的用户使用 iTunes 在他们的设备上安装 app，请将 app 安全地分发给用户，并让他们遵循下列步骤：

1. 在 iTunes 中，选取“文件”>“添加到资料库”，然后选择文件（.app、.ipa 或 .mobileprovision）。用户也可以将文件拖到 iTunes app 图标上。
2. 将设备连接到电脑，然后在 iTunes 的“设备”列表中将其选中。
3. 点按“应用程序”标签，然后在列表中选择 app。
4. 点按“应用”。

如果用户的电脑处于托管状态，则无需要求他们将文件添加到 iTunes，只需将文件部署到他们的电脑并要求他们对其设备进行同步。iTunes 会自动安装位于 iTunes 的“Mobile Applications”和“Provisioning Profiles”文件夹中的文件。

使用 Apple Configurator 安装 app

Apple Configurator 是一种可在 Mac App Store 中下载的免费 OS X 应用程序，IT 管理员可用它来安装企业内部 app 或来自 App Store 的 app。

App Store 中的 app 或企业内部 app 可直接导入 Apple Configurator，并安装到任意数量的设备上。

使用 MDM 安装 app

MDM 服务器可以管理来自 App Store 的第三方 app，也可以管理企业内部 app。使用 MDM 安装的 app 称为“托管 app”。MDM 服务器可以指定当用户从 MDM 取消注册后是否保留托管 app 及其数据。此外，服务器还可以防止托管 app 数据备份到 iTunes 和 iCloud。这可以使 IT 在管理可能包含敏感业务信息的 app 时，拥有比用户直接下载的 app 更多的控制权。

为了安装托管 app，MDM 服务器会向设备发送安装命令。在受监管的设备上，托管 app 需要获得用户的同意才能安装。

托管 app 可以从 iOS 7 的附加控制措施中受益。VPN 连接现在可在 app 层指定，这意味着仅该 app 的网络通信才会在受保护的 VPN 通道中。这可以确保专用数据保持隐私性，而不会与共有数据相混合。

托管 app 还支持 iOS 7 中的“托管打开方式”功能。这意味着可限制托管 app 与用户的个人 app 之间相互传输数据，从而使企业可以确保敏感数据留在应有的位置。

高速缓存服务器

iOS 便于用户轻松访问和消费数字内容，一些用户可能会在连接到组织的无线网络时请求数千兆字节的 app、图书和软件更新。对这些资源的需求会以高峰形式出现，首先会随初始设备部署而发生一波高峰，之后，随着用户发现新的内容或内容随时间而更新，也会零星出现需求高峰。由于这些内容下载，可能会导致对互联网带宽的需求激增。

OS X Server 中的高速缓存服务器功能可以将所请求内容的缓存副本存储在局域网内，从而减少专用网络上的出站互联网带宽 (RFC1918)。通过设置多台高速缓存服务器，规模较大的网络将会从中受益。对于很多部署来说，配置高速缓存服务器就像开启服务一样简单。服务器及所有利用此服务器的设备需要一种 NAT 环境。

有关更多信息，请参阅 OS X Server：高级管理。

运行 iOS 7 的 iOS 设备将自动联系附近的高速缓存服务器，无需任何附加设备配置。以下说明了高速缓存服务器工作流程如何对 iOS 设备以透明方式运行：

1. 在具有一个或多个高速缓存服务器的网络上，当一部 iOS 设备向 iTunes Store 或软件更新服务器请求内容时，此 iOS 设备将被引荐给一个高速缓存服务器。
2. 此高速缓存服务器首先将查看其本地缓存中是否已经具有所请求的内容。如果有，它将立即开始向 iOS 设备供应内容。
3. 如果此高速缓存服务器没有所请求的资源，则将尝试从其他来源下载内容。OS X Mavericks 的高速缓存服务器 2 具备一种对等复制功能，可以使用网络上的其他高速缓存服务器（如果这些服务器已经下载所请求的内容）。
4. 当高速缓存服务器收到下载数据后，它将立即转发给请求数据的任何客户端，同时将副本缓存到磁盘。

iOS 7 支持以下类型的缓存内容：

- iOS 软件更新
- App Store app
- App Store 更新
- iBooks Store 中的图书

iTunes 还支持高速缓存服务器 2。iTunes 11.0.4 或更高版本（包括 Mac 和 Windows）支持以下类型的内容：

- App Store app
- App Store 更新
- iBooks Store 中的图书

国家/地区限制

由于许可分发和税法方面的原因，某些内容可能无法在某些国家/地区缓存。自 2013 年 12 月起，iTunes 下载项目无法在巴西、墨西哥、中国和葡萄牙缓存，且 iBooks 下载项目无法在加拿大缓存。

如果根据客户端的 IP 地址，其所在国家/地区与使用 iTunes Store 的国家/地区不同，则 iTunes 下载项目将无法缓存。例如，旧金山的 iPad 用户可以从德国的 iTunes Store 下载 app，但是无法使用缓存服务。

附录 A：
WLAN 基础架构

在为 iOS 部署准备 WLAN 基础架构时，需要考虑以下几个因素：

- 所需的覆盖区域
- 使用 WLAN 网络的设备数量和密度
- 设备类型及其 WLAN 功能
- 要传输的数据类型及数量
- 无线网络访问方面的安全要求
- 加密要求

尽管此列表并不详尽，但它代表了一些最相关的 WLAN 网络设计因素。

提醒：本章重点介绍美国的 WLAN 网络设计。此设计在其他国家/地区可能有所不同。

规划覆盖范围和密度

尽管在要使用 iOS 设备的地点提供 WLAN 覆盖至关重要，但针对给定区域内的设备密度进行规划也必不可少。

大多数现代、企业级接入点最多能够处理 50 个 WLAN 客户端，但如果将如此之多的设备与单个接入点相关联，用户体验可能会令人失望。每台设备上的体验取决于在用通道上的可用无线带宽以及共享总带宽的设备数量。随着使用同一接入点的设备越来越多，这些设备的相对网络速度将会降低。在进行 WLAN 网络设计时，你应该考虑 iOS 设备的预期使用模式。

2.4GHz 和 5GHz

在美国，在 2.4GHz 下运行的 WLAN 网络允许建立 11 个频道。但是，考虑到频道干扰问题，在网络设计中只应使用频道 1、6 和 11。

5GHz 信号与 2.4GHz 信号一样无法穿透墙壁和其他障碍物，导致覆盖区域较小。因此，在为封闭空间（例如教室）内的高密度设备设计网络时，可能会首选 5GHz 网络。5GHz 频段内的可用频道数量因接入点供应商和国家/地区而异，但是至少有 8 个频道始终可用。

5GHz 频道都是不重叠的，这明显不同于 2.4GHz 频段内的三个不重叠频道。在为高密度 iOS 设备设计 WLAN 网络时，5GHz 下提供的附加频道将成为一个战略性的规划考虑因素。

设计覆盖范围

建筑物的物理布局可能会对你的 WLAN 网络设计产生影响。例如，在企业环境内，用户可能会在会议室或办公室与其他员工会面。因此，用户一天里会在建筑物内不断移动。这种情况下，大多数网络访问来自于检查电子邮件、日历和上网浏览，因此 WLAN 覆盖范围的优先级最高。设计 WLAN 时可以在每层楼包含两个或三个接入点，用以为办公室提供网络覆盖，同时在每间会议室各包含一个接入点。

设计密度

与上面的场景相对，假设一间学校有 1000 名学生和 30 名教师，全部位于一幢两层建筑中。学校为每名学生配备了一台 iPad，并为每位教师配备了一台 MacBook Air 和一台 iPad。每间教室大约可容纳 35 名学生，并且教室彼此相邻。学生一整天都在互联网上进行研究、观看课程视频，并不断从 LAN 上的文件服务器上复制文件或将文件复制到服务器。

这种情况下，由于移动设备的密度更高，因此 WLAN 网络设计更为复杂。鉴于每间教室大约有 35 名学生，所以每间教室可以部署一个接入点。应该考虑在公共区域部署多个接入点，以便提供足够的网络覆盖。各公共区域的实际接入点数量将有所不同，具体取决于这些区域中 WLAN 设备的密度。

如果需要将仅支持 802.11b 或 802.11g 标准的设备加入到网络，可选方案之一是直接启用 802.11b/g（如果已部署双频接入点）。另一种方案是：针对较新的设备预置一个使用 5GHz 802.11n 的 SSID，然后再预置一个 2.4GHz 的 SSID 以支持 802.11b 和 802.11g 设备。但是，请注意不要创建过多的 SSID。

两种设计方案都应避免使用隐藏 SSID。与广播 SSID 相比，WLAN 设备重新连接隐藏 SSID 会比较困难，并且隐藏 SSID 几乎没有安全优势。用户倾向于经常携带他们的 iOS 设备改变位置，因此隐藏 SSID 可能会延长网络关联时间。

Apple 产品中的 WLAN 标准

随后的列表中详细介绍了 Apple 产品对各种 WLAN 规格的支持情况，其中包括以下信息：

- **802.11. 兼容性。**802.11b/g、802.11a、802.11n
- **频段。**2.4GHz 或 5GHz
- **MCS 指数。**调制和编码方案 (MCS) 指数用于定义 802.11n 设备通信时可达到的最大传输速率。
- **通道绑定。**HD20 或 HD40

- **保护间隔 (GI)**。保护间隔是从一台设备传输到另一台设备的符号之间的时间间隔。802.11n 标准定义了较短的 400ns 保护间隔以实现更高的整体吞吐量，但是设备可以使用较长的 800ns 保护间隔。

iPhone 5s
802.11n @ 2.4GHz 和 5GHz
802.11a/b/g
MCS 指数 7/HT40/400ns GI

iPhone 5c
802.11n @ 2.4GHz 和 5GHz
802.11a/b/g
MCS 指数 7/HT40/400ns GI

iPhone 5
802.11n @ 2.4GHz 和 5GHz
802.11a/b/g
MCS 指数 7/HD40/400ns GI

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

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

iPad Air 和配备 Retina 显示屏的 iPad mini
802.11n @ 2.4GHz 和 5GHz
802.11a/b/g
MCS 指数 15/HT40/400ns GI

iPad（第 4 代）与 iPad mini
802.11n @ 2.4GHz 和 5GHz
802.11a/b/g
MCS 指数 7/HD40/400ns GI

iPad（第 1 代、第 2 代和第 3 代）
802.11n @ 2.4GHz 和 5GHz
802.11a/b/g
MCS 指数 7/HD20/800ns GI

iPod touch（第 5 代）
802.11n @ 2.4GHz 和 5GHz
802.11a/b/g
MCS 指数 7/HD40/400ns GI

iPod touch（第 4 代）
802.11n @ 2.4GHz
802.11b/g
MCS 指数 7/HD20/800ns GI

附录 B：限制

iOS 支持以下政策和限制，它们全部可根据组织的需要进行配置。

设备功能

- 允许安装 app
- 允许 Siri
- 在锁定时允许 Siri
- 允许使用摄像头
- 允许 FaceTime
- 允许屏幕捕捉
- 允许漫游时自动同步
- 允许同步邮件最近使用的项目
- 允许语音拨号
- 允许 App 内购买
- 所有购买均需要提供零售店密码
- 允许多人游戏
- 允许添加 Game Center 好友
- 设置允许的内容分级
- 允许 Touch ID
- 允许锁屏状态下访问控制中心
- 允许锁屏状态下访问通知中心
- 允许锁屏状态下显示“今天”视图
- 允许锁屏状态下显示 Passbook 通知

应用程序

- 允许使用 iTunes Store
- 允许使用 Safari
- 设置 Safari 安全偏好设置

iCloud

- 允许备份
- 允许文稿同步和钥匙串同步
- 允许我的照片流
- 允许 iCloud 照片共享

安全和隐私

- 允许将诊断数据发送给 Apple
- 允许用户接受不受信任的证书
- 执行加密备份
- 允许从非托管 app 打开到托管 app
- 允许从托管 app 打开到非托管 app
- 首次 AirPlay 配对时需要密码
- 允许以无线方式进行 PKI 更新
- 需要限制广告跟踪

仅限受监管设备的限制

- 单一 App 模式
- “辅助功能”设置
- 允许 iMessage
- 允许 Game Center
- 允许删除 app
- 允许 iBooks Store
- 允许 iBooks Store 中的色情图书
- 启用 Siri 脏话过滤器
- 允许手动安装配置描述文件
- HTTP 的全球网络代理
- 允许配对到电脑以进行内容同步
- 使用白名单和可选连接密码限制 AirPlay 连接
- 允许 AirDrop
- 允许帐户修改
- 允许蜂窝数据设置修改
- 允许“查找我的朋友”
- 允许主机配对 (iTunes)
- 允许激活锁定

附录 C：
以无线方式安装企业内部 App

iOS 支持以无线方式安装定制开发的企业内部 app，而无需使用 iTunes 或 App Store。

要求：

- 已鉴定的用户可访问的安全 Web 服务器
- .ipa 格式的 iOS app，使用企业预置描述文件为发行/生产而构建
- 此附录中描述的 XML 清单文件
- 允许设备访问 Apple iTunes 服务器的网络配置

安装 app 很简单。用户可以将清单文件从你的网站下载到他们的 iOS 设备。该清单文件会指示设备下载和安装文件中所引用的 app。

你可以通过 SMS 或电子邮件分发用于下载清单文件的 URL，或将其嵌入你所创建的另一企业 app 中。

你负责设计和托管用于分发 app 的网站。确保用户已通过鉴定（可能是使用基本鉴定或基于目录的鉴定），并确定网站可通过内联网或互联网进行访问。你可以将 app 和清单文件放入隐藏目录，或其他任何可使用 HTTPS 读取的位置。

在创建自助服务门户时，请考虑在用户主页屏幕中添加一个 Web Clip，以便用户轻松返回门户以获取未来部署信息，例如，新的配置描述文件、推荐的 App Store app，以及移动设备管理解决方案的注册信息。

准备好要以无线方式分发的企业内部 app

要使你的企业内部 app 做好无线分发的准备，你需要构建一个归档版本（.ipa 文件），以及一个清单文件，此文件用于实现 app 的无线分发和安装。

你可以使用 Xcode 来创建 app 归档。使用你的分发证书给 app 签名，并在归档中包括你的企业开发预置描述文件。有关构建和归档 app 的更多信息，请访问 iOS Dev Center 或参阅 *Xcode* 用户指南，此指南可通过 Xcode 中的“帮助”菜单获得。

关于无线清单文件

清单文件是 XML plist 格式。iOS 设备使用它从你的 Web 服务器上查找、下载和安装 app。清单文件是由 Xcode 创建的，使用的是你在共享用于企业分发的归档 app 时所提供的信息。请参见上一节，了解如何准备好要进行分发的 app。

以下栏是必填项：

项目	说明
URL	App (.ipa) 文件的完全限定 HTTPS URL。
display-image	一幅 57 x 57 像素 PNG 图像，在下载和安装过程中显示。指定图像的完全限定 URL。
full-size-image	一幅 512 x 512 像素 PNG 图像，用来在 iTunes 中表示相应 app。
bundle-identifier	你的 app 的包标识符，与 Xcode 项目中指定的完全一样。
bundle-version	你的 app 的包版本，在 Xcode 项目中指定。
title	下载和安装过程中显示的 app 的名称。

仅对于“报刊杂志”app 来说，以下栏才是必填项：

项目	说明
newsstand-image	一幅完整大小的 PNG 图像，用于显示在“报刊杂志”书架上。
UINewsstandBindingEdge UINewsstandBindingType	这些键必须与“报刊杂志”app 的 info.plist 中的键相符。
UINewsstandApp	表明相应 app 是“报刊杂志”app。

示例清单文件中描述了你可以使用的一些可选键。例如，如果你的 app 文件太大并且想要在执行错误检验（TCP 通信通常会执行该检验）的基础上确保下载的完整性，则可以使用 MD5 键。

通过指定项目数组的附加成员，你可以使用一个清单文件安装多个 app。

此附录末尾包含一个示例清单文件。

构建网站

将这些项目上传到你网站上可供已鉴定的用户访问的区域：

- app (.ipa) 文件
- 清单 (.plist) 文件

你的网站设计可以非常简单，就像链接到清单文件的单个页面一样。当用户轻按 Web 链接时，将会下载清单文件，并触发下载和安装它所描述的 app。

以下是一个示例链接：安装 App

请勿添加归档 app (.ipa) 的 Web 链接。载入清单文件时，设备会下载该 .ipa 文件。虽然 URL 的协议部分是 itms-services，但 iTunes Store 并不参与此过程。

此外，请确保你的 .ipa 文件可通过 HTTPS 进行访问，并且你的站点已使用 iOS 信任的证书进行了签名。如果自签名证书没有受信任的锚点并且无法由 iOS 设备验证，安装将失败。

设定服务器 MIME 类型

你可能需要配置你的 Web 服务器，以便正确地传输清单文件和 app 文件。

对于 OS X Server，请将以下 MIME 类型添加到 Web 服务的“MIME 类型”设置：

application/octet-stream ipa
text/xml plist

对于 IIS，请使用 IIS Manager 在服务器的“属性”页面中添加 MIME 类型：

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

无线 app 分发故障诊断

如果无线 app 分发失败并显示“无法下载”信息，请进行以下检查：

- 确定 app 已正确进行签名。测试方法是使用 Apple Configurator 将其安装到设备上，然后查看是否发生错误。
- 确定清单文件的链接是正确的，且清单文件可供 Web 用户访问。
- 确定 .ipa 文件（在清单文件中）的 URL 是正确的，并且该 .ipa 文件可供 Web 用户通过 HTTPS 进行访问。

网络配置要求

如果设备连接到封闭式内部网络，你应该允许 iOS 设备访问以下站点：

URL	原因
ax.init.itunes.apple.com	设备会获取通过蜂窝移动网络下载 app 的当前文件大小限制。如果无法访问此站点，则安装可能会失败。
ocsp.apple.com	设备会联系此站点，以检查用来给预置描述文件签名的分发证书的状态。请参阅下面的“证书验证”。

提供更新的 app

你自己分发的 app 不会自动更新。当你有新版本可供用户安装时，应通知他们进行更新并指导他们安装 app。请考虑让 app 检查更新，并在打开 app 时通知用户。如果你使用的是无线 app 分发，则在通知中可以提供更新版 app 的清单文件链接。

如果你想要用户保留他们的设备上存储的 app 数据，请确保新版本与它要替换的版本使用相同的捆绑标识符，并告知用户在安装新版本之前不要删除他们的旧版本。如果捆绑标识符相匹配，新版本将会替换旧版本并保留设备上存储的数据。

分发预置描述文件自签发之日起 12 个月后过期。过期后，系统将删除描述文件，而 app 将不会启动。

请在预置描述文件过期之前，使用 iOS Development Portal（iOS 开发门户）为 app 创建新描述文件。对于首次安装 app 的用户，请使用新预置描述文件创建新的 app 归档 (.ipa)。

对于已经拥有该 app 的用户，你可能想要设定发布下一个版本的时间，以便它包括新预置描述文件。如果你不想这样做，则可以仅分发新的 .mobileprovision 文件，这样用户便不必再次安装该 app。新的预置描述文件将覆盖 app 归档中已有的描述文件。

预置描述文件可以使用 MDM 进行安装和管理，也可以由用户从你提供的安全网站上进行下载和安装，或者，作为电子邮件附件分发给用户，供用户打开和安装。

当你的分发证书过期后，app 将不会启动。分发证书自签发之日起三年内有效，或者在你的企业开发者计划成员资格过期之前一直有效，二者以先到者为准。若要防止证书提前到期，请确保在成员资格过期之前进行续订。有关如何检查分发证书的信息，请参见下面的“证书验证”。

你可以同时让两个证书处于活跃状态，并且彼此独立。第二个证书是为了提供一个重叠期，让你能够在第一个证书过期前更新你的 app。从 iOS Dev Center 请求第二个分发证书时，请确保不要撤销第一个证书。

证书验证

用户首次打开 app 时，系统会通过联系 Apple 的 OCSP 服务器来验证分发证书。除非证书已被撤销，否则将允许 app 运行。如不能联系 OCSP 服务器或不能从 OCSP 服务器获得响应，这种情况不会被视为撤销。为了验证状态，设备必须能够访问 ocsp.apple.com。请参见此附录前面部分的“网络配置要求”。

OCSP 响应会在设备上缓存一段时间（由 OCSP 服务器指定），当前为介于 3 到 7 天之间。在重新启动设备和缓存的响应过期之前，将不会再次检查证书的有效性。

如果那时收到撤销命令，则系统将阻止 app 运行。

如果撤销分发证书，则使用该证书签名的所有 app 都会失效。你只应在万不得已时撤销证书，比如你确定专用密钥已丢失或确信证书已遭破解。

示例 app 清单文件

```
<!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]可能需支付一般运营商数据资费。iMessage 无法使用时，文本信息可能以短信发送，需支付运营商信息资费。[2]FaceTime 视频通话要求通话双方使用支持 FaceTime 的设备和 WLAN 连接。通过蜂窝网络进行 FaceTime 视频通话时，需要具备蜂窝网络数据功能的 iPhone 4s 或更新机型、配备 Retina 显示屏的 iPad 或 iPad mini。能否通过蜂窝网络使用此功能取决于运营商政策；可能需要支付数据费用。[3]Siri 可能仅支持部分语言或地区，并且功能可能因地区而异。需要使用互联网连接。可能需要支付蜂窝数据费用。[4]某些功能要求使用 WLAN 网络连接。某些功能仅适用于部分国家或地区。某些服务仅限 10 部设备进行访问。