iPhone 和 iPod touch
企业级部署指南

第三版

Apple
1 Infinite Loop
Cupertino, CA 95014-2084
408-996-1010
www.apple.com

本手册英文版在美国和加拿大同时出版。

CH019-1373/2008-09

目录

iPhone 在企业中的应用

了解如何将 iPhone 和 iPod touch 与企业系统结合起来。

本指南是专为系统管理员编写的。手册包含关于在企业环境里部署并支持 iPhone 和 iPod touch 的信息。

系统要求

阅读这一部分，以简要了解系统要求以及可用来将 iPhone 和 iPod touch 与企业系统结合起来的各种组件。

iPhone 和 iPod touch

与企业级网络配合使用的 iPhone 和 iPod touch 设备必须升级到 iPhone 软件 2.1 或更高版本。

iTunes

设置设备要求 iTunes 8.0 或更高版本。安装 iPhone 或 iPod touch 的软件更新、安装应用程序以及与 Mac 或 PC 同步音乐、视频或其他数据也需要这个版本的软件。

要使用 iTunes，您需要一台拥有 USB 2.0 端口并符合下列规格的 Mac 或 PC。

Mac OS X 电脑

- Mac OS X v10.4.10 Tiger 或更高版本
- 1 GHz 或速度更快的处理器
- 256 MB 内存
- QuickTime 7.1.6 或更高版本

Windows 电脑

- Windows XP Service Pack 2 或 Windows Vista
- 500 MHz 或速度更快的奔腾处理器
- 256 MB 内存
- QuickTime 7.1.6 或更高版本

某些 iTunes 功能（如使用 iTunes Store）需要额外的要求。有关更多信息，请参阅随 iTunes 安装器附带的文稿。

iPhone Configuration Utility

iPhone Configuration Utility（iPhone 配置实用工具）允许您创建设备的配置描述文件 (configuration profile)。

该实用工具的 Mac OS X 版本还允许您管理描述文件、安装应用程序以及从已连接的设备中查看控制台日志。此版本要求：

- Mac OS X v10.5 Leopard

基于 Web 版本的该实用工具要求：

- Microsoft Windows Vista （仅 32 位）、装有 .NET Framework 2.0 版的 Microsoft Windows XP 或 Mac OS X v10.5 Leopard
- Microsoft Internet Explorer 7、 Firefox 2 或 Safari 3

Microsoft Exchange ActiveSync

iPhone 和 iPod touch 支持以下版本的 Microsoft Exchange：

- Exchange ActiveSync 的 Exchange Server (EAS) 2003 Service Pack 2 版
- Exchange ActiveSync 的 Exchange Server (EAS) 2007 Service Pack 1 版

所支持的 Exchange ActiveSync 策略

支持以下 Exchange 策略：

- 在设备上强制使用密码
- 最短密码长度
- 最多密码尝试失败次数
- 要求数字与字母
- 不活跃时间 （以分钟计）

有关每条策略的描述，请参阅 Exchange ActiveSync 文稿。

【重要事项】在 Exchange 2003 上启用“要求数字与字母”策略或在 Exchange 2007 上启用 “要求字母密码”策略会要求用户输入至少含有一个复杂字符的 iPhone 密码。

远程擦除

您可以远程擦除 iPhone 和 iPod touch 上的内容。执行此操作会快速删除设备中的所有数据和配置信息，然后设备上的内容会被安全抹掉，并且设备会被还原为原始的出厂设置。每 8GB 设备容量，该过程需要大约一小时完成。

使用 Exchange Server 2007，您可以通过 Exchange Management Console、 Outlook Web Access 或 Exchange ActiveSync Mobile Administration Web Tool 发起远程擦除。

使用 Exchange Server 2003，您可以通过 Exchange ActiveSync Mobile Administration Web Tool 发起远程擦除。

用户也可以通过从 “通用”设置的 “复位”菜单中选取 “抹掉全部内容和设置”来擦除其拥有的设备。

【重要事项】由于擦除设备花费的时间较长，所以请将设备的充电器接上。如果设备由于电量低而关机，当设备连接到电源时擦除过程会继续进行。

Microsoft Direct Push

如果蜂窝数据连接可用， Exchange 服务器会将电子邮件、通讯录和日历事件自动传送到 iPhone。使用 iPod touch 时（或者当 iPhone 没有蜂窝数据信号时），信息不会自动被推送到设备中；当您尝试查看数据或选取“设置”>“获取新数据”时会取回这些信息。

Microsoft Exchange Autodiscovery

支持 Exchange Server 2007 的 Autodiscover 服务。当手动配置 iPhone 或 iPod touch 时， Autodiscover 会使用您的电子邮件地址和密码来自动确定正确的 Exchange 服务器信息。有关启用 Autodiscover 服务的信息，请参阅 http://technet.microsoft.com/en-us/library/cc539114.aspx。

Microsoft Exchange Global Address List

iPhone 和 iPod touch 会从您的公司的 Exchange 服务器公司目录取回联络人信息。在“通讯录”中进行搜索时，您可以访问该目录；并且在输入电子邮件地址时，会自动访问该目录以完成电子邮件地址。

不支持的 Exchange ActiveSync 功能

不是所有的 Exchange 功能都被支持，例如包括：

- 文件夹管理
- 打开电子邮件中指向保存在 Sharepoint 服务器上的文稿的链接
- 任务同步
- 设定 “外出”自动回复信息
- 创建会议邀请
- 给信息打上旗标以方便跟进

VPN

iPhone 和 iPod touch 可与支持以下协议和认证方式的 VPN 服务器配合使用：

- L2TP/IPSec （通过 MS-CHAPV2 密码、 RSA SecurID 和 CryptoCard 进行用户认证，以及通过共享密钥进行机器认证）。
- PPTP （通过 MS-CHAPV2 密码、 RSA SecurID 和 CryptoCard 进行用户认证）。
- Cisco IPSec（通过密码、 RSA SecurID 或 CryptoCard 进行用户认证，以及通过共享密钥和证书进行机器认证） 。有关兼容的 Cisco VPN 服务器和配置建议，请参阅 “附录 A”。

网络安全

iPhone 和 iPod touch 支持以下由 Wi-Fi Alliance 定义的 802.11i 无线联网安全标准：

- WEP
- WPA 个人级
- WPA 企业级
- WPA2 个人级
- WPA2 企业级

此外， iPhone 和 iPod touch 还支持以下适用于 WPA 企业级和 WPA2 企业级网络的 802.1X 认证方式：

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

证书

iPhone 和 iPod touch 可使用以下原始格式的证书：

- PKCS1 (.cer、 .crt、 .der)
- PKSC12 (.p12、 .pfx)

电子邮件帐户

iPhone 和 iPod touch 支持包括 Windows、 UNIX、 Linux 和 Mac OS X 等大量服务器平台上符合工业标准的 IMAP4 和 POP3 邮件系统。除了配合直接推送使用的 Exchange 帐户，您还可以使用 IMAP 访问 Exchange 帐户中的电子邮件。

附加资源

除了本指南之外，以下出版物和网站也提供了有用的信息：

- 《iPhone 使用手册》，可在 www.asia.apple.com/support/iphone 下载
- iPhone 指导教程，网址为 www.apple.com/iphone/guidedtour
- iPod touch 指导教程，网址为 www.apple.com/cn/ipodtouch/guidedtour
- iPhone 网页，网址为 www.asia.apple.com/iphone
- iPod touch 网页，网址为 www.apple.com/cn/ipodtouch
- iPhone 在企业中的应用网页，网址为 www.asia.apple.com/iphone
- iPhone 支持网页，网址为 www.asia.apple.com/support/iphone
- iPod touch 支持网页，网址为 www.apple.com/cn/support/ipodtouch
- iTunes 网页，网址为 www.apple.com/cn/itunes
- Exchange Product Overview （Exchange 产品概览），网址为 http://technet.microsoft.com/en-us/library/bb124558.aspx
- Deploying Exchange ActiveSync （部署 Exchange ActiveSync），网址为 http://technet.microsoft.com/en-us/library/aa995962.aspx
- Exchange 2003 Technical Documentation Library （Exchange 2003 技术文章资料库）：http://technet.microsoft.com/en-us/library/bb123872(EXCHG.65).aspx
- Managing Exchange ActiveSync Security（管理 Exchange ActiveSync 安全性），网址为 http://technet.microsoft.com/en-us/library/bb232020(EXCHG.80).aspx
- 企业级 Wi-Fi 网页，网址为 www.wi-fi.org/enterprise.php
- iPhone VPN Connectivity to Cisco Adaptive Security Appliances (ASA) （iPhone VPN 对 Cisco ASA 的连接性），网址为 www.cisco.com/en/US/docs/security/vpn_client/cisco_vpn_client/iPhone/2.0/connectivity/guide/iphone.html

部署 iPhone 和 iPod touch

1

本章概括了如何在您的企业中部署 iPhone 和 iPod touch。

iPhone 和 iPod touch 已被设计成轻松地与 Microsoft Exchange 2003、 Microsoft Exchange 2007、基于 802.1X 的安全无线网络以及 Cisco IPSec 虚拟专用网络等企业系统整合起来。如同任何企业解决方案一样，做好计划并理解不同的部署选择，可以更轻松地为您和您的用户进行部署而且效率更高。

计划 iPhone 和 iPod touch 的部署时，请考虑以下问题：

- 您公司的 iPhone 将如何激活无线蜂窝服务？
- 您的用户需要访问哪些企业网络服务、应用程序和数据？
- 您想要在设备上设定什么策略来保护敏感的公司数据？
- 您想要手动配置单个设备，还是使用简化的流程来配置大批设备？

企业环境的特殊性质、IT 策略、无线运营商以及计算和通信要求都会影响您如何调整部署战略。

激活设备

每部 iPhone 都必须通过无线运营商激活之后才能用于拨打和接听电话、发送短信或连接到蜂窝数据网络。请联系您的运营商以了解普通用户和企业用户的话音与数据资费以及激活说明。

您或您的用户将需要在 iPhone 中安装 SIM 卡。安装了 SIM 卡之后，iPhone 必须连接到安装了 iTunes 的电脑才能完成激活过程。如果 SIM 卡已经是活跃的，iPhone 将立即可以使用；不然的话， iTunes 将引导您完成激活新服务号码的全过程。

虽然 iPod touch 不配备蜂窝服务或 SIM 卡，但它也必须连接到安装了 iTunes 的电脑才能解锁。

由于需要 iTunes 来完成 iPhone 和 iPod touch 的激活过程，因此您必须决定要在每个用户的 Mac 或 PC 上安装 iTunes，还是只在自己的电脑上安装 iTunes 以完成每部设备的激活。

激活之后，设备不需要 iTunes 与企业系统配合使用，但仍需要用它来与电脑同步音乐、视频和 Web 浏览器书签。下载和安装设备的软件更新以及安装企业级应用程序也需要它。

有关激活设备和使用 iTunes 的更多信息，请参阅第 4 章。

准备访问网络服务和企业数据

iPhone 2.0 软件启用了（现有 Microsoft Exchange Server 2003 或 2007 解决方案的）安全推送电子邮件、推送通讯录和推送日历，也实现了全局地址查照 (Global Address Lookup)、远程擦除 (Remote Wipe) 和设备密码策略强制等功能。它还允许用户通过以下方式安全地连接到公司资源：使用 802.1X 无线认证通过 WPA 企业级和 WPA2 企业级无线网络进行连接；使用 PPTP、IPSec 上的 L2P 或 Cisco IPSec 协议通过 VPN 进行连接。

如果您的公司不使用 Microsoft Exchange，您的用户仍可以使用 iPhone 或 iPod touch 以无线方式与大多数基于标准 POP 或 IMAP 的服务器和服务同步电子邮件。它们可以使用 iTunes 从 Mac OS X iCal 和“地址簿”同步日历事件和通讯录；或者在 Windows PC 上与 Microsoft Outlook 同步这些内容。

当您确定想让用户访问哪些网络服务时，您应当了解以下情况：

Microsoft Exchange

iPhone 通过 Microsoft Exchange ActiveSync (EAS) 直接与 Microsoft Exchange Server 通信。Exchange ActiveSync 在 Exchange Server 和 iPhone 之间维持一个连接，以便当新电子邮件信息或会议邀请到达时，iPhone 立即得到更新。iPod touch 没有蜂窝连接，因此只有当它已激活并连接到 Wi-Fi 网络时才能收到推送通知。

如果您的公司当前支持 Exchange Server 2003 或 Exchange Server 2007 上的 Exchange ActiveSync，则您已经具备必要的服务。对于 Exchange Server 2007，请确定已安装了 Client Access Role。对于 Exchange Server 2003，请确定您已启用了 Outlook Mobile Access (OMA)。

如果您有 Exchange Server，但您的公司尚不支持 Exchange ActiveSync，请检查以下问题：

网络配置

- 请确定防火墙上的端口 443 是打开的。如果您的公司使用 Outlook Web Access，则端口 443 很可能已经打开。
- 验证服务器证书是否已经安装在前端 Exchange 服务器上，并且在 “认证方式”属性中只打开了基本认证，以要求 SSL 连接到 IIS 的 Microsoft Server ActiveSync 目录。
- 如果您使用的是 Microsoft Internet Security and Acceleration (ISA) Server，请验证服务器证书是否已安装，并更新公共 DNS 以正确解析从外面进入的连接。
- 请确定您的网络的 DNS 将单一的、外部可路由的地址返回给 Exchange ActiveSync 服务器，以便供企业内网客户端和 Internet 客户端使用。要求这样做是因为当两种类型的连接都活跃时，设备可以使用相同的 IP 地址与服务器进行通信。
- 如果您使用的是 Microsoft ISA Server，请创建 Web 监听器 (web listener) 和 Exchange Web 客户端访问发布规则。有关详细信息，请参阅 Microsoft 的文稿。
- 对于所有防火墙和网络个人设备，请将闲置会话超时设定为 30 分钟。请参阅 Microsoft Exchange 文稿以了解有关检测信号 (heartbeat) 和超时时间间隔 (timeout interval) 的信息，网址为 http://technet.microsoft.com/en-us/library/cc182270.aspx。

Exchange 帐户设置

- 使用 Active Directory 服务为特定用户或组别启用 Exchange ActiveSync。在 Exchange Server 2003 和 Exchange Server 2007 中，默认情况下，这些设置已经为组织级的所有移动设备所启用。对于 Exchange Server 2007，请参阅 “Exchange 管理控制台”中的 “收件人配置”。
- 使用 “Exchange 系统管理器”来配置移动功能、策略和设备安全性设置。对于 Exchange Server 2007，这是在 “Exchange 管理控制台”中进行的。
- 下载并安装 Microsoft Exchange ActiveSync Mobile Administration Web Tool，这个工具需要用来发起远程擦除。对于 Exchange Server 2007，远程擦除也可以使用 Outlook Web Access 或 Exchange Management Console 来发起。

WPA/WPA2 企业级 Wi-Fi 网络

支持 WPA 企业级和 WPA2 企业级确保可以在 iPhone 和 iPod touch 上安全地访问公司无线网络。 WPA/WPA2 企业级使用 AES 128 位加密，这是一种经过实践证明的基于块的加密方法，它提供了高级别的保证，确保公司数据受到保护。

有了对 802.1X 认证的支持， iPhone 和 iPod touch 可以被整合到广阔的 RADIUS 服务器环境中。 802.1X 无线认证方法是被支持的，并且包括 EAP-TLS、 EAP-TTLS、EAP-FAST、 PEAPv0、 PEAPv1 和 LEAP。

WPA/WPA2 企业级网络配置

- 验证网络个人设备的兼容性并选择 iPhone 和 iPod touch 支持的一种认证类型（EAP 类型）。请确定认证服务器上已启用了 802.1X，如果需要，请安装服务器证书并给用户和组别分配网络访问权限。
- 为 802.1X 认证配置无线访问点并输入相应的 RADIUS 服务器信息。
- 用一台 Mac 或 PC 来测试您的 802.1X 部署以确定 RADIUS 认证的配置是正确的。
- 如果您计划使用基于证书的认证，请确定通过相应的密钥分发流程，已经将公共密钥基础设施配置成支持基于设备和基于用户的证书。
- 验证证书格式和认证服务器兼容性。iPhone 和 iPod touch 支持 PKCS1 (.cer、.crt、.der) 和 PKCS12 (.p12、 .pfx)。

虚拟专用网络

iPhone 和 iPod touch 支持使用 Cisco IPSec、 IPSec 上的 L2TP 和 PPTP 虚拟专用网络协议安全访问专用网络。如果您的组织支持这些协议的其中一种，则不需要另外的网络配置或第三方应用程序便可以配合 VPN 基础设施使用您的设备。

Cisco IPSec 部署可以通过符合工业标准的 x.509 数码证书 (PKCS1、PKCS12) 来利用基于证书的认证。对于基于令牌的双重身份认证， iPhone 和 iPod touch 支持 RSA SecurID 和 CryptoCard。用户在建立 VPN 连接时，直接在他们的设备上输入 PIN 和由令牌产生的一次性密码。有关兼容的 Cisco VPN 服务器和配置建议，请参阅 “附录 A”。

iPhone 和 iPod touch 还支持用于 Cisco IPSec 和 L2TP/IPSec 部署的共享密钥认证，和用于基本用户名称和密码认证的 MS-CHAPv2。

VPN 设置指导

- iPhone 整合了大多数现有的 VPN 网络，因此只需要最小配置即可使 iPhone 能够访问网络。准备部署的最佳方法是检查 iPhone 是否支持您公司现有的 VPN 协议和认证方法。
- 确保与 VPN 集中器提供的标准相兼容。最好检查一下至 RADIU 或认证服务器的认证路径，以确定实现的网络中启用了 iPhone 支持的标准。
- 请咨询解决方案的提供者以确认您的软件和设备具备最新的安全补丁和固件。

IMAP 电子邮件

如果使用的不是 Microsoft Exchange，您仍可以通过使用支持 IMAP 并且被配置为要求用户认证和 SSL 的任何电子邮件服务器，实现安全且符合标准的电子邮件解决方案。这些服务器可以位于 DMZ 子网之内，也可以位于公司防火墙后面，或者两者皆可。

通过使用 SSL，iPhone 和 iPod touch 支持 128 位加密和主要证书机构签发的 X.509 根证书。它们还支持强力认证方法，包括符合工业标准的 MD5 Challenge-Response 和 NTLMv2。

IMAP 网络设置指导

- 为了得到附加的安全性保护，请在服务器上安装信任的证书机构 (CA) 提供的数码证书。安装 CA 提供的证书是一个重要步骤，目的是为了确保代理服务器是您的公司基础设施内受信任的实体。
- 要允许 iPhone 和 iPod touch 设备从服务器取回电子邮件，请打开防火墙中的端口 993 并确定代理服务器被设定为 SSL 上的 IMAP。
- 要允许设备发送电子邮件，端口 587、465 或 25 必须打开。首先使用端口 587，这是最佳选择。

企业级应用程序

如果您计划部署企业 iPhone 和 iPod touch 应用程序，请使用 Mac OS X 版 iPhone 配置实用工具或 iTunes （Mac 和 Windows 版）在设备上安装应用程序。一旦将应用程序部署到用户的设备，如果每个用户都在他们的 Mac 或 PC 上安装了 iTunes，更新那些应用程序将会变得更加容易。

确定设备密码策略

一旦您决定了用户将访问哪些网络服务和数据，您应当确定想要实现哪些设备密码策略。

对于其网络、系统或应用程序不要求密码或认证令牌的公司，建议在设备上设定需要输入密码。如果您将基于证书的认证用于 802.1X 网络或 Cisco IPSec VPN，或者您的企业级应用程序存储了您的登录凭证，您应当要求用户设定设备密码和较短的超时时间，以便不知道设备密码的人不能使用丢失或被盗的设备。

您可以用以下两种方法之一在 iPhone 和 iPod touch 上设定策略。如果设备被配置为访问 Microsoft Exchange 帐户， Exchange ActiveSync 策略会以无线方式推送到设备。这允许您实施和更新策略，而不需要用户执行任何操作。有关 EAS 策略的信息，请参阅第 6 页 “所支持的 Exchange ActiveSync 策略”。

如果使用的不是 Microsoft Exchange，您可以通过创建配置描述文件，在设备上设定相似的策略。您通过电子邮件或设备可访问的网站来分发描述文件。如果您想要更改策略，则必须将已更新的描述文件递交或发送给用户，以便他们安装。有关设备密码策略的信息，请参阅第 22 页 “密码设置”。

配置设备

下一步，您需要决定将如何配置每部 iPhone 和 iPod touch。部署方法很大程度上受您在不同时间计划部署和管理的设备的数量的影响。如果数量相对较小，对您或您的用户而言，您可能会发现手动配置每部设备更简单。这包括使用设备来输入每个邮件帐户的设置、 Wi-Fi 设置和 VPN 配置信息。有关手动配置的详细信息，请参阅第 3 章。

如果您计划部署大批设备，或者您有大量的电子邮件设置、网络设置和证书需要安装，则不妨通过创建并分发配置描述文件来配置设备。配置描述文件能快速地将设置和授权信息载入到设备上。另外，有些 VPN 和 Wi-Fi 设置只能通过配置描述文件来设定，而且如果使用的不是 Microsoft Exchange，您将需要使用配置描述文件来设定设备密码策略。

无论您是手动配置设备，还是使用配置描述文件，您都需要决定是亲自配置设备，还是将此任务委派给您的用户。选择哪一种取决于用户的位置、公司关于用户管理他们自己的 IT 设备的策略以及您打算部署的设备配置的复杂性。配置描述文件非常适用于大型企业、远程员工或无法自己设置设备的用户。

如果您想要让用户自己激活他们的设备，或者如果他们需要安装或更新企业级应用程序，则必须在每个用户的 Mac 或 PC 上安装 iTunes。iPhone 和 iPod touch 的软件更新也需要 iTunes，因此如果您决定不将 iTunes 分发给用户，请谨记这点。有关部署 iTunes 的信息，请参阅第 4 章。

其他资源

有关在企业中使用 iPhone 和 iPod touch 的更多有帮助的信息和资源，请参阅 www.asia.apple.com/iphone。

创建与部署配置描述文件

2

配置描述文件定义 iPhone 和 iPod touch 如何与企业系统配合使用。

配置描述文件 (configuration profile) 为 XML 文件，安装之后它提供的信息供 iPhone 和 iPod touch 用来连接到企业系统并与之通信。这些信息包括 VPN 配置信息、设备安全策略、 Exchange 设置、 邮件设置和证书。

您是通过电子邮件或使用网页来分发配置描述文件的。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。

如果不喜欢创建并分发配置描述文件，您可以手动配置 iPhone 或 iPod touch 设备。有关手动配置的信息，请参阅第 3 章。

关于 iPhone Configuration Utility

您是使用 iPhone Configuration Utility 来创建配置描述文件的。 iPhone ConfigurationUtility 共有两个版本：一个是 Mac OS X 应用程序，另一个是基于 Web 的版本，适用于 Mac OS X 或 Windows。

iPhone Configuration Utility （Mac OS X 版）

当运行 iPhone Configuration Utility 安装器时，iPhone Configuration Utility（Mac OS X 版）会被安装在 “/ 应用程序 / 实用工具 /”文件夹内。

当打开 iPhone Configuration Utility 时，会出现与下图所示相似的窗口。

在边栏中选择项目时，窗口中主要部分的内容会随之更改。

边栏会显示 “资料库”，该资料库包含以下类别：

- **设备**会显示曾经连接到电脑的 iPhone 和 iPod touch 设备列表。
- **预置描述文件**会列出那些允许使用设备来进行 iPhone OS 开发的描述文件 （由 Apple Developer Connection 开发者联盟授权）。有关信息，请参阅第 5 章。
- **配置描述文件**会列出您之前已创建的配置描述文件，并允许您编辑所输入的信息，或者创建一个新的配置以便可以发送给用户让其在设备上安装。
- **应用程序**会列出应用程序，可将它们安装在与电脑相连的设备上。

边栏还会显示 **“已连接的设备”**，它显示当前已连接在电脑 USB 端口的 iPhone 或 iPod touch 的信息。已连接的设备的有关信息会被自动添加到 “设备”列表中，这样您就可以再次查看它而不必连接该设备。

当设备已连接时，您可以查看控制台日志和任何可用的崩溃日志。在 Mac OS X 上的 Xcode 开发环境中，有相同的设备日志可供查看。

iPhone Configuration Utility （Web 版）

基于 Web 版本的 iPhone Configuration Utility 允许您为您的设备创建配置描述文件。请按照下列适用于您使用的平台的说明进行操作。

在 Mac OS X 上安装

要在 Mac OS X v10.5 Leopard 上安装此实用工具，请打开 “iPhone Web Config 安装器”并按照屏幕指示进行操作。安装结束后便可以使用此实用工具。请参阅第 18 页 “访问 iPhone Configuration Utility （Web 版）”。

在 Windows XP 和 Windows Vista 上安装

要在 Windows 上安装此实用工具，请执行以下操作：

1. 在 Windows XP 上，请从 www.microsoft.com/downloads 下载并运行 Microsoft .NET Framework Version 2.0 Redistributable Package (x86) 安装程序。
2. 运行 iPhoneConfigWebUtilSetup.exe。
3. 要配置实用工具，使它能直接将配置描述文件通过电子邮件发送给用户，请编辑此文件：**安装驱动器：** Program Files\Apple\iPhone Configuration Web Utility\config\environments\production.rb，以使 ActionMailer::Base.smtp_settings 方法中的参数适合于您的网络。

   要确认该实用工具正在运行，请打开“服务”控制面板并确定 iPhone Configuration Utility Web 服务正在运行。

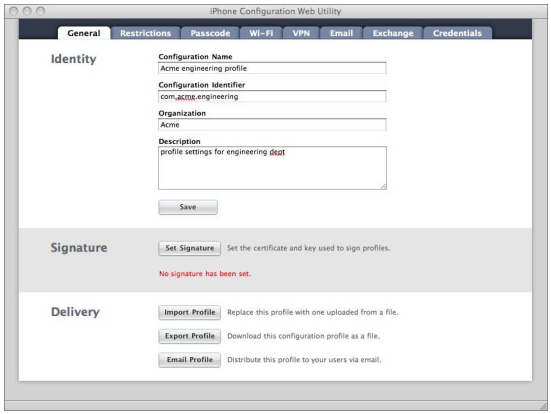
访问 iPhone Configuration Utility （Web 版）

要访问此实用工具，请按照以下步骤操作。

1. 打开 Web 浏览器并前往：http://localhost:3000

   如果已将此实用工具安装在其他电脑上，请使用其名称或地址来替换上述地址中的 localhost。有关所支持的 Web 浏览器的信息，请参阅第 6 页 “iPhone Configuration Utility”。
2. 请使用用户名称 “admin”和密码 “admin”来登录。

将会出现一个与下图所示类似的屏幕。



有关使用该实用工具的信息，请参阅下面的 “创建配置描述文件”。

更改 iPhone Configuration Utility （Web 版）的用户名称和密码

要更改用于访问实用工具的用户名称和密码，请编辑以下文件：

- **安装路径** /Apple/iPhone Configuration Web Utility/config/authentication.rb

默认的安装位置是：

- Mac OS X：/usr/local/iPhoneConfigService/
- Windows：\Program Files\Apple\iPhone Configuration Web Utility

更改 iPhone Configuration Utility （Web 版）的 Web 服务器端口号

默认情况下，实用工具监听端口 3000 上的 HTTP 连接。要更改端口号，请在下列文件中找到文本 “`:port => 3000`”，然后将 “`3000`”更改为尚未使用的端口。

- Mac OS X：**安装路径** /vendor/rails/railties/lib/commands/servers/mongrel.rb
- Windows：**安装路径** \vendor\rails\railties\lib\commands\webrick.rb

默认的安装位置是：

- Mac OS X：/usr/local/iPhoneConfigService/
- Windows：Program Files\Apple\iPhone Configuration Web Utility

更改端口号后，请停止实用工具运行并重新启动它。请参阅以下说明。

启动或重新启动 iPhone Configuration Utility （Web 版）

在 Windows 上，实用工具由安装程序来自动启动；在 Mac OS X 中，当需要它时，它便会启动。但是如果您遇到问题，或者更改邮件设置、端口号或用户名称与密码设置，您应该停止实用工具运行并重新启动它。请按照以下步骤操作：

要在 Windows 上重新启动实用工具

1. 请前往 “控制面板” > “管理工具” > “服务”。
2. 选择 Apple iPhone Configuration Web Utility。
3. 从 “操作”菜单中选择 “重新启动”。

要在 Mac OS X 上重新启动实用工具

1. 打开 “终端”。
2. 输入 “`sudo -s`”并使用管理员密码认证。
3. 输入 “`launchctl unload /System/Library/LaunchDaemons/com.apple.iPhoneConfigService.plist`”
4. 输入 “`launchctl load /System/Library/LaunchDaemons/com.apple.iPhoneConfigService.plist`”

创建配置描述文件

要创建新的配置描述文件，请点按 iPhone Configuration Utility （Mac OS X 版）或 iPhone Configuration Utility （Web 版）工具栏中的 “新建描述文件” (New Profile) 按钮。然后使用主窗口底部的面板来编辑描述文件。

尽管可以创建单独一个含有全部所需信息的配置描述文件，请仍然考虑为证书和设置创建各自分开的描述文件，因此您可以分开更新和分发每种类型的信息。这样还允许用户在安装含有 VPN 或帐户设置的新描述文件时保留已经安装了的证书。

要将信息添加到配置描述文件，请选择相应的面板，点按 “配置” (Configure) 按钮，然后填入屏幕上要求的信息 （如下所述）。必需的栏位标有红色箭头。

对于某些设置 （如 Wi-Fi 设置），您可以点按添加按钮 (+) 来添加附加的配置。要删除配置，请点按配置详细信息窗口中的删除按钮 (–)。

通用设置

您就是在这里提供此描述文件的名称和标识符。

配置名称是必需的。您指定的名称会出现在描述文件列表中，且安装配置描述文件后，它会显示在设备上。尽管该名称不必是唯一的，但您应该使用可识别此描述文件的描述性名称。

配置标识符必须唯一识别此描述文件，且格式必须为：com.companyname.identifier，其中“identifier”用来说明该描述文件。例如：com.mycompany.homeoffice。

标识符非常重要，因为安装一个描述文件时，会与已存在于设备上的描述文件比较“配置标识符”值。如果“配置标识符”值与所有已安装的描述文件都不同，则描述文件中的信息就会被添加到设备中。如果标识符与已安装的一个描述文件相符，则描述文件中的信息会替换设备上已经存在的设置。

描述文件可通过对其签名得以验证，但已签名的描述文件并不是必需的。如果没有给描述文件签名，在设备上查看时，它的状态会显示为 “未签名”。

如果您选取给描述文件签名，且该签名在设备上可以被验证，则它的状态就是“已验证”。如果设备上没有验证签名所必需的证书，或者如果信任链不能被链接到设备上受信任的根锚，则描述文件的状态就是“未验证”。已签名的描述文件用以下带勾的图标表示：

要给描述文件签名，请点按 “通用”面板 “签名”部分中的 “应用签名”。在出现的“配置签名”窗口中，请添加认证签名所必需的数码证书。支持 PKCS1（.cer、.der 和 .crt）和 PKCS12 （.p12 和 .pfx）格式的证书。

下一步，选择您的专用密钥（必须是未加密的 .pem 文件），然后点按 “签名”。在此处选择的证书不会被添加到设备中，仅在签名过程中用来验证您的签名。要将证书添加到设备中，以便安装描述文件时签名可以被验证，请参阅第 25 页 “凭证设置”。

一旦给描述文件签名，只有通过在 “通用”面板中点按 “删除签名”来删除签名后才能修改它。

密码设置

如果您没有使用 Exchange 密码策略，请使用此面板来设定设备策略。您可以指定使用设备时是否需要密码，还可以指定密码的特征及更换频率。载入配置描述文件时，会立即要求用户输入符合所选择的密码策略的密码，否则将不安装该描述文件。

如果同时使用设备策略和 Exchange 密码策略，两组策略会合并，且会实施最严格的设置。有关 Exchange 策略的信息，请参阅第 6 页 “Microsoft Exchange ActiveSync”。

以下策略可用：

- **要求设备密码：**要求用户输入密码才能使用设备。否则，任何持有该设备的人都可以访问它的所有功能和数据。
- **允许简单值：**允许用户在密码中使用重复的字符。例如，这允许将密码设定为 “3333”或 “A4A4”。
- **要求字母和数字值：**要求密码由字母和数字组成。
- **最短的密码长度：**指定密码所包含字符的最少数目。
- **必须包含的复杂字符的最少数目：**密码必须包含的非字母和数字字符 （如 $、 & 和 !）的数目。

- **最多可允许的失败次数：**您选择的值会决定尝试输入密码失败几次之后设备才会被擦除。默认情况下，密码尝试失败六次后，设备会强制延迟一段时间后才可以再次输入密码。延迟时间会随着尝试失败次数的增多而增加。尝试失败十一次后，设备中的所有数据和设置都会被安全地抹掉。密码时间延迟总是在第六次尝试后开始，所以如果将此值设定为 6 或更小，就不会强制时间延迟，并且超过尝试次数之后设备就会被抹掉。您不能指定大于 11 的值蜒当用户连续输入错误的密码达到 11 次之后，设备都会擦除它的数据。
- **最长的密码有效期（单位：天）：**要求用户在指定的时间间隔后更改他们的密码。
- **密码锁定 （单位：分钟）：**在闲置此段时间后，设备将自动锁定。输入密码使它解除锁定。

Wi-Fi 设置

使用此面板来设定设备如何连接到无线网络。您可以通过点按添加按钮 (+) 来添加多个网络配置。

必须指定这些设置且设置必须与网络要求相符，以便用户进行网络连接。

- **服务集标识符：**输入要连接到的无线网络的服务集标识符 (SSID)。
- **隐藏网络：**指定网络是否在广播其身份。
- **安全类型：**选择网络的认证方式。以下选择可用于个人和企业网络。
  - **无：**网络没有使用认证。
  - WEP：网络仅使用 WEP 认证。
  - WPA/WPA 2：网络仅使用 WPA 认证。
  - **任一：**设备在连接网络时采用 WEP 或 WPA 认证，但不会连接到未认证的网络。

企业级设置

在 Wi-Fi 面板的此部分中，您可以指定用于连接到企业级网络的设置。只有在 “安全类型”弹出式菜单中选取了企业级设置时才会出现面板的此部分。

在 “协议”标签中，您可以指定使用何种 EAP 方式进行认证并配置 EAP-FAST 保护性访问凭证 （EAP-FAST Protected Access Credential）设置。

在 “鉴定”标签中，您可以指定登录设置 （如用户名称和认证协议）。如果已使用 “凭证”标签安装了身份证书，您可以使用 “身份证书”弹出式菜单来选取它。

在 “信任”标签中，您可以指定哪些证书应当被视为信任的，以便为 Wi-Fi 连接验证认证服务器。“可信的证书”列表会显示已使用 “凭证”标签添加了的证书，并允许您选择哪些证书应当被视为信任的。请将要信任的认证服务器的名称添加到“可信的服务器证书的名称”列表。您可以指定特定的服务器（如 server.mycompany.com）或部分名称（如 *.mycompany.com）。

“允许信任例外”选项可允许用户在信任链无法建立时决定信任某个服务器。要避免这些提示并只允许连接到可信的服务，请关闭此选项并将所有必需的证书嵌入到描述文件中。

VPN 设置

使用此面板来输入 VPN 设置以连接到网络。通过点按添加按钮 (+) 您可以添加多组 VPN 连接。

有关所支持的 VPN 协议和认证方式的信息，请参阅第 8 页 “VPN”。

电子邮件设置

使用此面板来为用户配置 POP 或 IMAP 邮件帐户。安装描述文件后，这些帐户将被添加到设备中，而且和 Exchange 帐户一样，用户需要手动输入描述文件中被忽略的信息（如帐户密码）。

用户可以修改您在描述文件中提供的某些邮件设置，比如帐户名称、密码和备选 SMTP 服务器。如果在描述文件中忽略了任何此类信息，用户在访问帐户时会被要求输入该信息。

【重要事项】当用户删除描述文件时，邮件帐户及其所有数据都会被删除。

通过点按添加按钮 (+) 您可以添加多个邮件帐户。

Exchange 设置

使用此面板输入用户的设置来访问 Exchange 服务器。您可以通过指定用户名称、主机名称和电子邮件地址来为特定用户创建描述文件。或者您可以只提供主机名称，这样的话在安装描述文件过程中会提示用户填入其余的值。

如果在描述文件中指定了用户名称、主机名称和 SSL 设置，则用户不能在设备上更改这些设置。

每部设备只能配置一个 Exchange 帐户。当安装里面含有 Exchange 配置的描述文件时，之前使用 iTunes 同步到设备上的所有联络人和日历数据都会被抹掉并替换为 Exchange 帐户中的数据。添加 Exchange 帐户时，其他电子邮件帐户（包括任何 Exchange IMAP 帐户）不受影响。

默认情况下，Exchange 会同步通讯录、日历和电子邮件。用户可以在设备上的“设置”>“帐户”中更改这些设置（包括要同步多少天前的数据）。当设备被配置为与 Exchange 同步日历或通讯录时， iTunes 将不再与桌面电脑同步数据。

如果选择了“使用 SSL”选项，请务必使用“凭证”面板添加对连接进行认证所必需的证书。

凭证设置

使用此面板将证书添加到设备中。支持原始格式 PKCS1（.cer、.der、.crt）和 PKCS12（.p12、 .pfx）的证书。

当将身份证书安装到设备时，请确认文件包含证书而不是仅包含专用密钥。如果只安装专用密钥而没有必需的证书，则身份无效。如果安装没有专用密钥的身份证书，设备每次使用该证书时都会要求用户输入专用密钥。

此外，请确认发布服务器证书的证书代理在设备上是可信的。您不必添加根证书，它们已经由 Apple 添加到设备中了。要查看预安装的系统根证书列表，请参阅 Apple 支持文章，网址为： http://support.apple.com/kb/HT2185?viewlocale=zh_CN。

除了使用描述文件安装证书外，您可以让用户使用 Safari 从网页直接将证书下载到设备中。或者，您可以通过电子邮件将证书发送给用户。有关更多信息，请参阅第 37 页“安装身份和根证书”。

要添加多个凭证，请点按添加按钮 (+)。

高级设置

“高级”面板允许您更改设备的“访问点名称”（APN）设置。 APN 设置可定义设备如何连接到运营商的网络。只有在运营商网络专业人员的明确指导下才可以更改这些设置。如果这些设置不正确，则设备无法使用蜂窝网络访问数据。要还原由于疏忽而对这些设置所做的更改，请从设备上删除描述文件。Apple 建议您将 APN 设置与其他企业级设置定义在分开的配置描述文件中。

编辑配置描述文件

在 iPhone Configuration Utility （Mac OS X 版）中，请在 “配置”列表中选择一个描述文件，然后使用设置面板来进行更改。您还可以通过选取 “文件”>“添加到资料库”然后选择一个 .mobileconfig 文件来导入描述文件。如果看不到设置面板，请点按工具栏中的 “显示编辑器”按钮。

在基于 Web 版本的 iPhone Configuration Utility 中，点按 “导入描述文件” (Import Profile) 来载入您想要编辑的描述文件。

如果描述文件已被签名，则您必须先在 “通用”面板中点按 “移去签名”后才可以编辑它。

“通用”面板中的 “配置标识符”栏位被设备用来确定描述文件是新的，还是对现有描述文件的更新。如果想用更新的描述文件替换用户已安装的描述文件，请不要更改配置标识符。

准备配置描述文件用于部署

创建描述文件后，请决定是想要通过电子邮件将其分发给用户，还是通过将其递交到网站上来将其分发给用户。当用户使用他们的设备打开电子邮件信息或从 Web 网页下载描述文件时，会提示他们开始安装过程。有关信息，请参阅第 28 页 “安装配置描述文件”。

描述文件中所包含的某些信息晦涩难懂，以防被人随意偷看，但描述文件并未被加密。请确定该文件只能被授权用户访问。

通过电子邮件分发配置描述文件

要通过电子邮件来发送描述文件，请点按电子邮件按钮。如果您使用的是 Mac OS X 版本的 iPhone Configuration Utility，一封新的 Mail 邮件会打开，描述文件作为未压缩的附件已被添加到邮件中。如果您使用的是基于 Web 版本的实用工具，描述文件将通过电子邮件发送到您指定的地址。

在 Web 上分发配置描述文件

要将描述文件递交到网页以便在 iPhone 或 iPod touch 上使用 Safari 下载，请点按“导出” (Export) 按钮。此操作会在您指定的位置创建一个 .mobileconfig 文件，供您发布到您的站点。

请不要压缩 .mobileconfig 文件，否则设备将不能识别描述文件。此外，您必须配置 Web 服务器以使 .mobileconfig 文件可作为 application/x-apple-aspen-config 文件来传输。

Mac OS X Server

如果您的 Web 服务器使用的是 Mac OS X Server v10.5.3 Leopard 或更高版本，它已经过了配置以正确传输 .mobileconfig 文件。

对于 Mac OS X Server v10.5.3 以前的版本，请使用 Server Admin 将下列 MIME 类型添加到 “MIME 类型”设置中：

```
application/x-apple-aspen-config mobileconfig
```

这将确保所有的 .mobileconfig 文件（无论其储存在 Web 服务器的何处）都将被正确地发送到客户端。

也可以将 MIME 类型添加到 httpd.conf 或它的某个子配置文件中（假如 Apache 配置允许进行目录覆盖的话）：

```
AddType application/x-apple-aspen-config mobileconfig
```

IIS Web 服务器

如果您的 Web 服务器使用的是 IIS，请使用 “ISS 管理器”在服务器的 “属性”页面添加 MIME 类型。扩展名为 “`mobileconfig`”并且文件类型是 “`application/x-apple-aspen-config`”。

您也可以使用网站属性面板的 “HTTP 表头” (HTTP Headers) 部分，将此信息添加到特定的站点。

安装配置描述文件

在使用企业特定信息来设置设备之前，将 URL 提供给用户（用户可以通过该 URL 将描述文件下载到他们的设备上），或将描述文件发送到用户的电子邮件帐户中（用户可以使用设备访问该电子邮件帐户）。

在任一情况下，设备都会识别描述文件，且安装过程会在用户轻按“安装”时开始。

安装过程中，会询问用户以输入任何必需的信息，比如 Exchange 帐户密码和其他您指定的设置所需要的信息。

设备会从服务器取回 Exchange ActiveSync 策略，并在随后的每次连接时都会刷新这些策略（如果有更改）。如果设备或 Exchange ActiveSync 策略强制使用密码设置，则用户必须输入遵循策略的密码以完成安装。

此外，还会要求用户输入任何必需的密码，以使用描述文件中包含的证书。

如果安装没有成功完成，则可能是因为 Exchange 服务器无法连接或用户取消了安装过程。用户所输入的任何信息都不会保留。

用户可能想更改要同步到设备中的数据的天数。默认设置是三天。此设置可在“设置”>“邮件、通讯录、日历”>“**Exchange 帐户名称**”中更改。

删除和更新配置描述文件

由配置描述文件实施的设置不能在设备上更改。要更改设置，您必须安装更新的描述文件。

要删除由描述文件安装的 Exchange 帐户，请删除该描述文件。

【重要事项】删除配置描述文件会删除储存在设备上的策略和所有 Exchange 帐户的数据，以及 VPN 设置、证书和描述文件相关的其他信息。

配置描述文件更新不会被推送给用户。要分发一个新的配置描述文件，您必须使用电子邮件将其发送给用户或让用户从网站下载新的版本。只要描述文件中的配置标识符相符，新描述文件就替换设备上的描述文件，并根据新描述文件所指定的来添加、更新或删除信息和设置。

手动配置设备

3

本章说明如何手动配置 iPhone 和 iPod touch。

如果您不提供自动配置描述文件，用户可以手动配置他们的设备。有些设置 （例如密码策略）只能通过使用配置描述文件来设定。

VPN 设置

要更改 VPN 设置，请前往 “设置” > “通用” > “网络” > “VPN”。

配置 VPN 设置时，设备会根据它从 VPN 服务器收到的响应要求您输入信息。例如，如果服务器要求 RSA SecurID 令牌，设备会要求您输入一个。

您不能配置基于证书的 VPN 连接，除非合适的证书已安装在设备上。有关更多信息，请参阅第 37 页 “安装身份和根证书”。

Cisco IPSec 设置

当您手动配置设备用于 Cisco IPSec VPN 时，会出现与下图类似的屏幕：

请使用下面的图表来验明您输入的设置和信息：

栏位	描述
描述	一个识别这组设置的描述性标题。
服务器	连接到的 VPN 服务器的 DNS 名称或 IP 地址。
帐户	用户的 VPN 登录帐户的用户名称。不要在此栏位中输入组别名称。
密码	用户的 VPN 登录帐户的口令。对于 RSA SecurID 和 CryptoCard 认证，或者如果您想让用户在每次尝试连接时手动输入他们的密码，请让它保持空白。
使用证书	只有当您已经安装了 .p12 或 .pfx 身份 （含有为远程访问定制的证书**和**证书的专用密钥）时，此选项才可用。当 “使用证书”打开时，“组别名称”和 “共享密钥”栏位会被替换成 “身份”栏位，可让您从已安装的兼容 VPN 的身份列表中挑选。
组别名称	用户所属组别的名称，它已在 VPN 服务器上定义。
密钥	组别的共享密钥。这对用户被分配的组别的每个成员都是相同的。它**不是**用户的密码，必须指定以发起连接。

PPTP 设置

当您手动配置设备用于 PPTP VPN 时，会出现与下图类似的屏幕：

请使用下面的图表来验明您输入的设置和信息：

栏位	描述
描述	一个识别这组设置的描述性标题。
服务器	连接到的 VPN 服务器的 DNS 名称或 IP 地址。
帐户	用户的 VPN 登录帐户的用户名称。
RSA SecurID	如果您使用的是 RSA SecurID 令牌，请打开此选项，以便隐藏“密码”栏位。
密码	用户的 VPN 登录帐户的口令。
加密级别	默认为“自动”，会选择可用的最高加密级别，从“128 位”开始，接着是“40 位”，然后是“无”。最高只能是“128 位”。“无”会关闭加密。
发送全部流量	默认为“打开”。通过 VPN 链接发送所有网络通信。关闭该设置以启用隧道分离，从而只通过服务器传送要抵达 VPN 内部的服务器的通信。其他通信则直接传送到 Internet。

L2TP 设置

当您手动配置设备用于 L2TP VPN 时，会出现与下图类似的屏幕：

请使用下面的图表来验明您输入的设置和信息：

栏位	描述
描述	一个识别这组设置的描述性标题。
服务器	连接到的 VPN 服务器的 DNS 名称或 IP 地址。
帐户	用户的 VPN 登录帐户的用户名称。
密码	用户的 VPN 登录帐户的口令。
密钥	L2TP 帐户的共享密钥（预共享密钥）。这对所有 LT2P 用户来说都是相同的。
发送全部流量	默认为 “打开” 。通过 VPN 链接发送所有网络通信。关闭该设置以启用隧道分离，从而只通过服务器传送要抵达 VPN 内部的服务器的通信。其他通信则直接传送到 Internet。

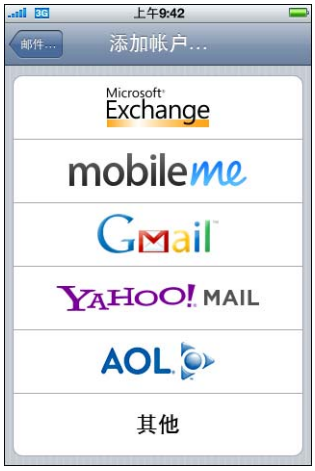
Wi-Fi 设置

要更改 Wi-Fi 设置，请前往 “设置” > “通用” > “网络” > “Wi-Fi”。如果您处在要添加的网络的覆盖范围内，请从可用网络的列表中选择它。否则，请轻按 “其他”。

请确定您的网络基础设施使用 iPhone 和 iPod touch 支持的认证和加密。有关技术规格的信息，请参阅第 8 页 “网络安全”。有关安装 PKCS1 和 PKCS12 证书用于认证的信息，请参阅第 37 页 “安装身份和根证书”。

Exchange 设置

每部设备只能配置一个 Exchange 帐户。要添加 Exchange 帐户，请前往 “设置” > “邮件、通讯录、日历”，然后轻按 “添加帐户”。在 “添加帐户” 屏幕上，轻按 “Microsoft Exchange”。



当您手动配置设备用于 Exchange 时，请使用下面的图表来验明您输入的设置和信息：

栏位	描述
电子邮件	用户的完整电子邮件地址。
域	用户的 Exchange 帐户的域。
用户名称	用户的 Exchange 帐户的用户名称。
密码	用户的 Exchange 帐户的口令。
描述	一个识别这组设置的描述性标题。

iPhone 和 iPod touch 支持 Microsoft 的 Autodiscover 服务，该服务使用您的用户名称和密码来确定前端 Exchange 服务器的地址。如果不能确定服务器的地址，将会要求您输入该地址。

成功配置 Exchange 帐户之后，服务器的密码策略会被实施。如果用户的当前密码不符合 Exchange ActiveSync 策略的规定，则会提示用户更改或设定密码。设备将不会与 Exchange 服务器通信，直到用户设定符合规定的密码为止。

下一步，设备会立即与 Exchange 服务器同步。如果您选取这次不同步，则以后可以在“设置”>“邮件、通讯录、日历”中打开日历和通讯录同步。默认情况下，Exchange ActiveSync 会在新数据到达服务器时将它们推送到您的设备。如果您更喜欢按计划时间获取新数据或只是手动提取新数据，请使用“设置”>“获取新数据”以更改设置。

【重要事项】当您配置设备与 Exchange 同步时，设备上所有现有的日历和联络人信息会被覆盖。另外，iTunes 不再与桌面电脑同步通讯录和日历。您仍可以使用 MobileMe 服务以无线方式同步设备。

要更改将多少天的数据同步到设备，请前往“设置”>“邮件、通讯录、日历”。默认设置是“3 天”。

安装身份和根证书

如果您不使用描述文件来分发证书，则通过使用设备从网站下载它们或打开电子邮件信息中的附件，用户可以手动安装它们。设备能够识别含有以下 MIME 类型和文件扩展名的证书：

- application/x-pkcs12、.p12、.pfx
- application/x-x509-ca-cert、.cer、.crt、.der

身份由 x.509 证书和专用密钥组成，用于向服务器识别用户。iPhone 和 iPod touch 支持导入正好包含一个身份的 P12 文件。安装身份时，会提示用户输入能够对它进行保护的口令。

根证书是自签发的锚 (self-signed anchors)，用来进行 X.509 证书链评估。这些根证书被 Safari、“邮件”、VPN 及其他应用程序所执行的所有 x.509 证书链评估使用。

您不必添加根证书，它们已经由 Apple 添加到设备中了。要查看预安装的系统根证书的列表，请参阅 Apple 支持文章，网址为 http://support.apple.com/kb/HT2185?viewlocale=zh_CN。

证书被下载到设备之后，“安装描述文件”屏幕会出现。描述指出证书的类型：身份或证书机构（根证书）。要安装证书，请轻按“安装”。

要查看或移走已安装的证书，请前往“设置”>“通用”>“描述文件”。如果您移走的证书是访问某个帐户或网络所必需的，设备将不能连接到那些服务。

其他邮件帐户

虽然您只能配置一个 Exchange 帐户，但您可以添加多个 POP 和 IMAP 帐户。例如，这个帐户可用来访问 Lotus Notes 或 Novell Groupwise 邮件服务器上的邮件。前往“设置”>“帐户”>“邮件、通讯录、日历”。然后轻按“其他”。有关添加 IMAP 帐户的更多信息，请参阅《iPhone 使用手册》或《iPod touch 使用手册》。

其他资源

Apple 制作了一些视频教程可在标准 Web 浏览器中观看，这些教程向用户展示了如何设置并使用 iPhone 和 iPod touch 的功能：

- iPhone 指导教程，网址为 www.apple.com/iphone/guidedtour
- iPod touch 指导教程，网址为 www.apple.com/cn/ipodtouch/guidedtour
- iPhone 支持网页，网址为 www.asia.apple.com/support/iphone
- iPod touch 支持网页，网址为 www.apple.com/cn/support/ipodtouch

每个设备还有一本 PDF 格式的使用手册，介绍了附加的技巧和使用详细信息：

- 《iPhone 使用手册》：http://manuals.info.apple.com/en/iPhone_User_Guide.pdf
- 《iPod touch 使用手册》：
  http://manuals.info.apple.com/en/iPod_touch_User_Guide.pdf

配置 iTunes

4

您使用 iTunes 来同步音乐和视频、安装应用程序以及进行其他操作。

本章说明如何部署 iTunes 和企业级应用程序，并定义您可以指定的设置和限制。

安装 iTunes

iTunes 使用标准的 Macintosh 安装器和 Windows 安装程序。最新版本的 iTunes 可在 www.apple.com/cn/itunes 下载。有关 iTunes 系统要求的更多信息，请参阅第 5 页“iTunes”。

在 Windows 电脑上安装 iTunes

当在 Windows 电脑上安装 iTunes 时，通常还安装最新版本的 QuickTime、 Bonjour 和 Apple Software Update （Apple 软件更新）。您可以通过向 iTunes 安装程序传递参数或者只推送想要安装到用户电脑中的组件来忽略这些组件。

使用 iTunesSetup.exe 在 Windows 上安装

如果要使用常规的 iTunes 安装过程，但要忽略某些组件，您可以使用命令行向 iTunesSetup.exe 传递属性。

属性	含义
NO_AMDS=1	不安装 Apple Mobile Device Services。此组件是 iTunes 同步和管理移动设备所必需的组件。
NO_ASUW=1	不安装 Apple Software Update（Windows 版）。此应用程序会提醒用户安装新版本的 Apple 软件。
NO_BONJOUR=1	不安装 Bonjour。Bonjour 提供了零配置网络发现功能，无需配置即可发现打印机、共享的 iTunes 资料库及其他服务。
NO_QUICKTIME=1	不安装 QuickTime。此组件是使用 iTunes 必需的组件。请不要忽略 QuickTime，除非您确定客户端电脑已经安装了最新的版本。

在 Windows 上静默安装

要将 iTunes 推送到客户端电脑，请从 iTunesSetup.exe 中提取各个 .msi 文件。

要从 iTunesSetup.exe 中提取 .msi 文件：

1. 运行 iTunesSetup.exe。
2. 打开 “%temp%”并找到名称为 “IXPnnn.TMP”的文件夹。其中，“%temp%”是您的临时目录 （一般是：**引导驱动器**：\documents and Settings\user\Local Settings\temp\），且 “nnn”是一个三位数的随机数字。
3. 将 .msi 文件从该文件夹拷贝到其他位置。
4. 退出由 iTunesSetup.exe 打开的安装程序。

然后使用 “组策略对象编辑器”（位于 Microsoft 管理控制台内）将 .msi 文件添加到 “电脑配置”策略。请确定将配置添加到 “电脑配置”策略，而非 “用户配置”策略。

【重要事项】 iTunes 需要 QuickTime，且 Apple Mobile Device Services (AMDS) 是与 iTunes 配合使用 iPod touch 或 iPhone 所必需的。

在 Macintosh 电脑上安装 iTunes

Mac 电脑已装有 iTunes。最新版本的 iTunes （包含 QuickTime）可在 www.apple.com/cn/itunes 获得。要将 iTunes 推送到 Mac 客户端，您可以使用 Workgroup Manager （Mac OS X Server 附带的一款管理工具）。

使用 iTunes 迅速激活设备

在一部新的 iPhone 或 iPod touch 可以使用之前，必须先通过将其连接到正在运行 iTunes 的电脑上来激活它。通常，激活设备后， iTunes 会尝试将设备与电脑同步。要在为其他人设置设备时避免此情况，请打开仅激活模式。这使 iTunes 在激活设备后自动推出它。然后，设备准备好进行配置，但没有任何媒体或数据。

要在 Mac OS X 上打开仅激活模式：

1. 请确定 iTunes 没有在运行，然后打开 “终端”。
2. 在 “终端”中，输入命令：
   - 要打开仅激活模式：
     ```
     defaults write com.apple.iTunes StoreActivationMode -integer 1
     ```
   - 要关闭仅激活模式：
     ```
     defaults write com.apple.iTunes StoreActivationMode -integer 0
     ```

要激活设备，请参阅下面的 “使用仅激活模式”。

要在 Windows 上打开仅激活模式：

1 请确定 iTunes 没有在运行，然后打开命令提示符窗口。

2 输入命令：

- 要打开仅激活模式：

```
C:\Program Files\iTunes\iTunes.exe /setPrefInt StoreActivationMode 1
```

- 要关闭仅激活模式：

```
C:\Program Files\iTunes\iTunes.exe /setPrefInt StoreActivationMode 0
```

您也可以创建一个快捷方式或编辑已有的 iTunes 快捷方式来包括这些命令，以便您可以迅速切换仅激活模式。

使用仅激活模式

请确定您已按照上述操作打开了仅激活模式，然后按照这些步骤来操作。

1 如果您正在激活 iPhone，请插入已激活的 SIM 卡。使用 SIM 卡推出工具或已拉直的回形针来推出 SIM 卡托架。有关详细信息，请参阅《iPhone 使用手册》。

2 将 iPhone 或 iPod touch 连接到电脑。要激活设备，电脑必须连接到 Internet。

iTunes 会打开（如果需要）并激活设备。当设备被成功激活后，会出现一则信息。

3 断开设备。

您可以立即连接并激活其他设备。当仅激活模式打开时，iTunes 将不会与任何设备同步，因此如果您打算正常使用 iTunes，请记得关闭仅激活模式。

设定 iTunes 限制

您可以限制用户使用 iTunes 的某些功能。此功能有时与家长控制类似。可限制以下功能：

- 检查新版本 iTunes 和设备软件更新（自动检查和用户发起的检查）。
- 浏览或播放媒体时显示 iTunes MiniStore
- 设备连接时自动同步
- 取回专辑插图
- 使用可视化效果插件
- 输入流媒体的 URL
- 自动发现 Apple TV 系统
- 向 Apple 注册新设备
- 订购 podcast
- 播放 Internet 广播

- 访问 iTunes Store
- 与局域网电脑共享音乐
- 播放已标记为不良内容的 iTunes 媒体
- 播放影片
- 播放电视节目
- 玩游戏

为 Mac OS X 设定 iTunes 限制

在 Mac OS X 中，通过使用 plist 文件中的键来控制访问。在 Mac OS X 中，以上所示的键的值可以通过使用 Workgroup Manager（Mac OS X Server 附带的一款管理工具）编辑 “~/ 资源库 /Preferences/com.apple.iTunes.plist” 文件来为每个用户指定。

有关说明，请参阅 Apple 支持文章，网址为：
http://docs.info.apple.com/article.html?artnum=303099-zh。

为 Windows 设定 iTunes 限制

在 Windows 中，通过设定以下一个注册表键内的注册表值来控制访问：

在 Windows XP 和 32 位 Windows Vista 中：

- HKEY_LOCAL_MACHINE\Software\Apple Computer, Inc.\iTunes\[SID]\Parental Controls\
- HKEY_CURRENT_USER\Software\Apple Computer, Inc.\iTunes\Parental Controls

在 64 位 Windows Vista 中：

- HKEY_LOCAL_MACHINE\Software\Wow6432Node\Apple Computer, Inc.\iTunes\[SID]\Parental Controls\
- HKEY_CURRENT_USER\Software\Wow6432Node\Apple Computer, Inc.\iTunes\Parental Controls

有关说明，请参阅 Apple 支持网站，网址为
http://support.apple.com/kb/HT2102?viewlocale=zh_CN。

手动更新 iTunes 和 iPhone 软件

如果在 iTunes 中关闭了自动的和用户发起的软件更新检查，则您将需要将软件更新分发给用户来手动安装。

要更新 iTunes，请参阅本文稿前面所讲解的安装和部署步骤。将 iTunes 分发给用户也是按照相同的过程进行。

要更新 iPhone 软件，请按照以下步骤操作：

1. 在一台没有关闭 iTunes 软件更新的电脑上，使用 iTunes 来下载 iPhone 软件更新。要执行此操作，请在 iTunes 中选择一个已连接的设备，点按 “摘要”标签，然后点按 “检查更新”按钮。
2. 下载后，请拷贝在以下位置找到的更新程序文件 (.ipsw)：
   - **在 Mac OS X 中：** ~/ 资源库 /iTunes/iPhone Software Updates/
   - **在 Windows 中：引导驱动器：** \Documents and Settings\user\Application Data\Apple Computer\iTunes\iPhone Software Updates\
3. 将 .ipsw 文件分发给用户，或者将其放在他们可以访问的网络驱动器上。
4. 请告诉用户，在应用软件更新以前要先备份他们的设备。手动更新过程中，iTunes 不会在安装前自动备份设备。要创建新的备份，请在 iTunes 边栏中右键单击 (Windows) 或按住 Control 键点按 (Mac) 设备。然后从出现的关联菜单中选取 “备份”。
5. 用户通过先将设备连接到 iTunes，然后再选择他们的设备的“摘要”标签来安装更新。下一步，他们要按住 Option (⌥) 键 (Mac) 或 Shift 键 (Windows) 并点按或单击“检查更新”按钮。
6. 会出现一个文件选择对话框。用户应该选择 .ipsw 文件，然后点按 “打开”来开始更新过程。

部署 iPhone 应用程序

5

您可以将 iPhone 和 iPod touch 应用程序分发给用户。

如果您想要安装您开发的 iPhone OS 应用程序，请将应用程序分发给用户，他们再使用 iTunes 来安装该应用程序。

在线 App Store 中的应用程序可以在 iPhone 和 iPod touch 运行而无需任何附加步骤。如果开发想要自己分发的应用程序，则必须使用 Apple 颁发的证书对其进行数码签名。您还必须向用户提供分配预置描述文件 (distribution provisioning profile) 以允许他们的设备使用该应用程序。

部署您自己的应用程序的过程为：

- 向 Apple 注册企业级开发。
- 使用您的证书签发应用程序。
- 创建企业级分配预置描述文件，它可以授权设备使用您已签名的应用程序。
- 将应用程序和企业级分配预置描述文件部署到用户的电脑中。
- 指导用户使用 iTunes 安装应用程序和描述文件。

有关每个步骤的更多信息，请参阅下列内容。

注册应用程序开发

要为 iPhone 和 iPod touch 开发并部署定制的应用程序，您需要在 www.apple.com/cn/developer 注册 iPhone Enterprise Developer Program （iPhone 企业级开发者计划）。

一旦完成注册过程，您将收到如何使应用程序能在设备上运行的说明。

签发应用程序

分发给用户的应用程序必须使用您的分配证书来签名。有关如何获得并使用证书的说明，请参阅 iPhone Developer Center （iPhone 开发者中心），网址为：http://developer.apple.com/cn/iphone。

创建分配预置描述文件

分配预置描述文件允许您的用户可以在他们的 iPhone 或 iPod touch 上使用您创建的应用程序。您通过指定由描述文件授权的 AppID，为特定的应用程序或多个应用程序创建企业级分配预置描述文件。如果用户有应用程序却没有描述文件授权使用它，用户就不能使用该应用程序。

Enterprise Program Portal （企业计划门户，网址为：http://developer.apple.com/cn/iphone）给企业委派的 Team Agent（团队代理）可以创建分配预置描述文件。有关说明，请参阅该网站。

一旦创建好企业级分配预置描述文件，请下载 .mobileprovision 文件，然后将它和应用程序一起安全地分发出去。

使用 iTunes 安装预置描述文件

用户已安装的 iTunes 自动安装位于以下文件夹中的预置描述文件：

Mac OS X

- ~/ 资源库 /MobileDevice/Provisioning Profiles/
- / 资源库 /MobileDevice/Provisioning Profiles/
- 由 ~/ 资源库 /Preferences/com.apple.itunes 文件中的 ProvisioningProfilesPath 键指定的路径

Windows XP

- **引导驱动器：** \Documents and Settings\username\Application Data\Apple Computer\MobileDevice\Provisioning Profiles
- **引导驱动器：** \Documents and Settings\All Users\Application Data\Apple Computer\MobileDevice\Provisioning Profiles
- HKCU 或 HKLM 中由 SOFTWARE\Apple Computer, Inc\iTunes 中的 ProvisioningProfilesPath 注册表键指定的路径

Windows Vista

- **引导驱动器：** \Users\username\AppData\Roaming\Apple Computer\MobileDevice\Provisioning Profiles
- **引导驱动器：** \ProgramData\Apple Computer\MobileDevice\Provisioning Profiles
- HKCU 或 HKLM 中由 SOFTWARE\Apple Computer, Inc\iTunes 中的 ProvisioningProfilesPath 注册表键指定的路径

iTunes 会将在以上位置中找到的预置描述文件自动安装到与其进行同步的设备中。一经安装，就可以在设备上的“设置”>“通用”>“描述文件”中查看预置描述文件。

您也可以将 .mobileprovision 文件分发给用户并让他们将该文件拖移到 iTunes 应用程序图标上，iTunes 会将文件拷贝到以上定义的正确位置中。

使用 iPhone Configuration Utility（Mac OS X 版）安装预置描述文件

您可以使用 iPhone Configuration Utility（Mac OS X 版）将预置描述文件安装到已连接的设备中。请按照以下步骤操作：

1. 在 iPhone Configuration Utility 中选取“文件”>“打开”，然后选择想要安装的预置描述文件。

   该描述文件会被添加到 iPhone Configuration Utility 中，并可以通过选择“资料库”中的“预置描述文件”类别来查看。
2. 在“已连接的设备”列表中选择一个设备。
3. 点按“预置”标签。
4. 在列表中选择该预置描述文件，然后点按它的“安装”按钮。

使用 iTunes 安装应用程序

用户可以使用 iTunes 在他们的设备上安装应用程序。请将应用程序安全地分发给用户，然后让他们按照以下步骤进行操作：

1. 在 iTunes 中选取“文件”>“添加到资料库”，然后选择您提供的应用程序 (.app)。

   您也可以将 .app 文件拖移到 iTunes 应用程序图标上。
2. 将设备连接到电脑，然后在 iTunes 的“设备”列表中选择它。
3. 点按“应用程序”标签，然后在列表中选择应用程序。
4. 点按“应用”来安装应用程序，和位于所指定的文件夹内的所有分配预置描述文件（在第 45 页“使用 iTunes 安装预置描述文件”中已详述）。

使用 iPhone Configuration Utility（Mac OS X 版）安装应用程序

您可以使用 iPhone Configuration Utility（Mac OS X 版）将应用程序安装到已连接的设备中。请按照以下步骤操作：

1 在 iPhone Configuration Utility 中选取 “文件” > “打开”，然后选择想要安装的应用程序。

该应用程序会被添加到 iPhone Configuration Utility 中，并可以通过选择 “资料库” 中的 “应用程序” 类别来查看。

2 在 “已连接的设备” 列表中选择一个设备。

3 点按 “应用程序” 标签。

4 在列表中选择该应用程序，然后点按它的 “安装” 按钮。

使用企业级应用程序

当用户运行未被 Apple 签名的应用程序时，设备会查找授权使用该应用程序的分配预置描述文件。如果找不到描述文件，将不会打开该应用程序。

其他资源

有关创建应用程序和预置描述文件的更多信息，请参阅：

- iPhone Developer Center （iPhone 开发者中心），网址为：http://developer.apple.com/cn/iphone

Cisco VPN 服务器配置

使用这些指导来配置 Cisco VPN 服务器以配合 iPhone 和 iPod touch 工作。

支持的 Cisco 平台

iPhone 支持 Cisco ASA 5500 Security Appliances 和配置了 7.2.x 软件或更高版本的 PIX Firewalls。强烈建议您安装最新的 8.0.x 软件版本（或更高版本）。Cisco IOS VPN 路由器和 VPN 3000 集中器系列都不支持 iPhone VPN 功能。

认证方法

iPhone 支持以下认证方法：

- 预共享密钥 IPSec 认证与通过 xauth 进行的用户认证。
- 客户端和服务器证书，用于 IPSec 认证与通过 xauth 进行的用户认证 （用户认证为可选）。
- 混合认证 —— 为了进行 IPSec 认证，服务器提供证书而客户端提供预共享密钥。用户认证要求通过 xauth 进行。
- 用户认证是通过 xauth 提供的，包括以下认证方法：
  - 用户名称和密码
  - RSA SecurID
  - CryptoCard

认证组别

Cisco Unity 协议基于一组共同的认证及其他参数，使用认证组别将用户组合在一起。您应当为 iPhone 和 iPod touch 用户创建认证组别。对于预共享密钥认证和混合认证，组别名称必须在设备上配置，并且使用组别的共享密钥（预共享密钥）作为组别密码。

使用证书认证时，将不会使用任何共享密钥，用户的组别根据证书中的字段确定。Cisco 服务器设置可用于将证书中的字段对应到用户组别。

证书

设置和安装证书时，请确定以下情况：

- 服务器身份证书在主题备用名称 (SubjectAltName) 字段中必须包含服务器的 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。您可以使用通配符（例如 vpn.*.mycompany.com，以提高适应性）来指定 SubjectAltName，以使每段都匹配。如果未指定 SubjectAltName，DNS 名称可以放在公共名称字段中。
- 签署服务器的证书的 CA 证书应当安装在设备上。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被信任。
- 如果使用客户端证书，请确定签署客户端证书的被信任的 CA 证书已安装在 VPN 服务器上。
- 证书和证书机构必须是有效的（例如，未过期）。
- 通过服务器发送证书链是不被支持的，必须关掉。
- 使用基于证书的认证时，请确定服务器已被设置为基于客户端证书中的字段来识别用户的组别。请参阅第 49 页 “认证组别”。

IPSec 设置

使用以下 IPSec 设置：

- **模式：**隧道模式
- **IKE 交换模式：**“野蛮模式”适用于预共享密钥认证和混合认证，“主模式”适用于证书认证。
- **加密算法：**3DES、 AES-128、 AES-256
- **认证算法：**HMAC-MD5、 HMAC-SHA1
- **Diffie Hellman 组别：**预共享密钥认证和混合认证需要 Group 2。对于证书认证，请将 Group 2 配合 3DES 和 AES-128 使用。将 Group 2 或 Group 5 配合 AES-256 使用。
- **PFS （完全正向保密）：**对于 IKE phase 2，如果使用 PFS，则 Diffie-Hellman 组别必须与用于 IKE phase 1 的相同。
- **模式配置：**必须启用。
- **失效同层检测：**建议使用。
- **标准 NAT 穿越：**被支持，需要时可以启用。（TCP 上的 IPSec 不被支持）。
- **负载均衡：**被支持，需要时可以启用。
- **Phase 1 的密钥更新：**当前不被支持。建议将服务器上的密钥更新时间设定为一小时左右。
- **ASA 地址掩码：**确定所有设备地址池掩码未设定或设定为 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
```

使用建议的地址掩码时，VPN 配置所假定的有些规则可能会被忽略。要避免发生这种情况，请确定路由表包含所有必要的规则，并且验证子网地址可以访问，然后再进行部署。

其他被支持的功能

iPhone 和 iPod touch 支持以下功能：

- **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。
- **网页标识：**如果在服务器上配置了网页标识，网页标识会显示在设备上，用户必须接受它，否则断开连接。
- **分离隧道：**支持隧道分离。
- **分离 DNS：**支持分离 DNS。
- **默认域：**支持默认域。

配置描述文件格式

本附录详细说明 mobileconfig 文件的格式，供想要创建自己的工具的开发者参考。

本文稿假设您熟悉 Apple XML DTD 和一般的属性列表格式。Apple plist 格式的一般描述可从 www.apple.com/DTDs/PropertyList-1.0.dtd 获得。

本文稿使用到术语**有效负载** (payload) 和**描述文件** (profile)。描述文件是在 iPhone 或 iPod touch 上配置某些（一个或多个）设置的一个完整文件。有效负载是描述文件的单个组件。

根层次

在根层次上，配置文件是一个词典，带有以下键 / 值对：

键	值
PayloadVersion	数字（必须）。整个配置描述文件的版本。此版本号指定了整个描述文件（而不是单个有效负载）的格式。
PayloadUUID	字符串（必须）。这通常是经合成后产生的一个唯一的标识字符串。此字符串的确切内容是不相关的；但是，它必须是全局唯一的。在 Mac OS X 上，您可以使用“/usr/bin/uuidgen”来生成 UUID。
PayloadType	字符串（必须）。目前，只有“Configuration”是此键的有效值。
PayloadOrganization	字符串（可选）。此值说明描述文件的签发机构，显示给用户看。
PayloadIdentifier	字符串（必须）。按照惯例，此值是用圆点分隔的字符串（例如“com.myCorp.iPhone.mailSettings”或“edu.myCollege.students.vpn”），用来唯一地说明描述文件。这就是用来辨别描述文件的字符串；如果安装的描述文件与另一个描述文件的标识符相符，则描述文件会覆盖它（而不是被添加）。

键	值
PayloadDisplayName	字符串（必须）。此值决定显示给用户看的很短的字符串，它用来说明描述文件，如“VPN 设置”。它不必是唯一的。
PayloadDescription	字符串（可选）。此值决定在整个描述文件的“详细信息”屏幕上向用户显示哪些自由格式的描述性文本。此字符串应当能清楚地识别描述文件，以便用户可以决定是否安装它。
PayloadContent	数组（可选）。此值是描述文件的实际内容。如果它被忽略，整个描述文件就没有任何功能性的意义。

有效负载内容

PayloadContent 数组是一个词典数组，每个词典说明描述文件的单个有效负载。每个功能性的描述文件在这个数组里有至少一个或多个条目。无论有效负载的类型如何，此数组中的每个词典都有一些共同属性。其他属性对于每种有效负载类型来说都是专用且唯一的。

键	值
PayloadVersion	数字（必须）。单个有效负载的版本。每个描述文件可以由包含不同版本号的有效负载组成。例如，VPN 版本号可以在将来增加一个点，而“Mail”版本号则不增加。
PayloadUUID	字符串（必须）。这通常是经合成后产生的一个唯一的标识字符串。此字符串的确切内容是不相关的；但是，它必须是全局唯一的。
PayloadType	字符串（必须）。此键 / 值对决定描述文件中单个有效负载的类型。
PayloadOrganization	字符串（可选）。此值说明描述文件的签发机构，它会显示给用户看。它可以与根层次的 PayloadOrganization 相同，但这不是必须的。
PayloadIdentifier	字符串（必须）。按照惯例，此值是用圆点分隔的字符串，用来描述有效负载。它通常是根 PayloadIdentifier 后面追加一个子标识符，描述特定的有效负载。
PayloadDisplayName	字符串（必须）。此值是显示给用户看的很短的字符串，它用来说明描述文件，如“VPN 设置”。它不必是唯一的。
PayloadDescription	字符串（可选）。此值决定在该特定有效负载的“详细信息”屏幕上向用户显示哪些自由格式的描述性文本。

密码策略有效负载

密码策略有效负载是由 com.apple.mobiledevice.passwordpolicy 有效负载类型 (PayloadType) 值指定的。此有效负载类型的存在提示 iPhone 向用户显示字母数字密码输入机制，该机制允许输入任意长度的复杂密码。

除了与所有有效负载相同的设置之外，此有效负载定义了以下内容：

键	值
allowSimple	布尔值（可选）。默认为 “YES”。决定是否允许使用简单密码。简单密码是定义为包含重复的字符或递增 / 递减字符（例如 123 或 CBA）。将此值设定为 “NO”与将 minComplexChars 设定为 “1”是相同的。
forcePIN	布尔值（可选）。默认为“NO”。决定是否强制用户设定 PIN。简易设定此值 （而不是其他值）会强制用户输入密码，但不会限制密码的长度或质量。
maxFailedAttempts	数字 （可选）。默认为 “11”。允许的范围是 [2...11]。指定允许在 iPhone 锁定屏幕上尝试输入密码失败的次数。一旦超过该次数，设备会被锁定，并且必须连接到其指定的 iTunes 才能解锁。
maxInactivity	数字 （可选）。默认为 “Infinity”。指定系统锁定设备之前，设备可以闲置（没有被用户解锁）的天数。一旦达到此限制，设备会被锁定并且必须输入密码。
maxPINAgeInDays	数字 （可选）。默认为 “Infinity”。指定密码可以保持不变的天数。过去那些天之后，用户会被强制更改密码才能将设备解锁。
minComplexChars	数字 （可选）。默认为 “0”。指定密码必须包含最少多少个复杂字符。“复杂”字符是数字或字母之外的字符，例如 &%$#。
minLength	数字 （可选）。默认为 “0”。指定密码的最小整体长度。此参数独立于同样为可选项的 minComplexChars 参数。
requireAlphanumeric	布尔值 （可选）。默认为 “NO”。指定用户是否必须输入字母字符 (“abcd”)，还是输入数字就足够了。

电子邮件有效负载

电子邮件有效负载是由 com.apple.mail.managed 有效负载类型 (PayloadType) 值指定的。此有效负载会在设备上创建一个电子邮件帐户。除了与所有有效负载相同的设置之外，此有效负载定义了以下内容:

键	值
EmailAccountDescription	字符串（可选）。用户可见的电子邮件帐户描述，显示在“邮件”和“设置”应用程序中。
EmailAccountName	字符串（可选）。帐户的完整用户名称。在已发出的电子邮件信息中和其他地方会出现这个用户名称。
EmailAccountType	字符串（必须）。允许的值是 EmailTypePOP 和 EmailTypeIMAP。定义用于该帐户的协议。
EmailAddress	字符串（必须）。指定帐户的完整电子邮件地址。如果有效负载中不存在，安装描述文件过程中，设备会提示输入此字符串。
IncomingMailServerAuthentication	字符串（必须）。指定收到的邮件的认证方案。允许的值是 EmailAuthPassword 和 EmailAuthNone。
IncomingMailServerHostName	字符串（必须）。指定收件服务器主机名称（或 IP 地址）。
IncomingMailServerPortNumber	数字（可选）。指定收件服务器端口号。如果未指定端口号，则会使用给定协议的默认端口。
IncomingMailServerUseSSL	布尔值（可选）。默认为“YES”。指定收件服务器是否使用 SSL 进行认证。
IncomingMailServerUsername	字符串（必须）。指定电子邮件帐户的用户名称（通常与电子邮件地址中 @ 符号以前的部分相同）。如果有效负载中不存在，并且帐户被设置为要求对收到的电子邮件进行认证，安装描述文件过程中，设备将提示输入此字符串。
OutgoingMailServerAuthentication	字符串（必须）。指定发出的邮件的认证方案。允许的值是 EmailAuthPassword 和 EmailAuthNone。
OutgoingMailServerHostName	字符串（必须）。指定发件服务器主机名称（或 IP 地址）。
OutgoingMailServerPortNumber	数字（可选）。指定发件服务器端口号。如果未指定端口号，则按照顺序使用端口 25、 587 和 465。
OutgoingMailServerUseSSL	布尔值（可选）。默认为“YES”。指定发件服务器是否使用 SSL 进行认证。
OutgoingMailServerUsername	字符串（必须）。指定电子邮件帐户的用户名称（通常与电子邮件地址中 @ 符号以前的部分相同）。如果有效负载中不存在，并且帐户被设置为要求对发出的电子邮件进行认证，安装描述文件过程中，设备会提示输入此字符串。

APN 有效负载

APN （访问点名称）有效负载是由 com.apple.apn.managed 有效负载类型 (PayloadType) 值指定的。除了与所有有效负载相同的设置之外，此有效负载定义了以下内容：

键	值
DefaultsData	词典 （必须）。此词典含有两组键 / 值对。
DefaultsDomainName	字符串（必须）。唯一允许的值是 com.apple.managedCarrier。
apns	数组 （必须）。此数组含有任意个数的词典，每个词典描述一个 APN 配置，它们包含以下键 / 值对。
apn	字符串 （必须）。此字符串指定访问点名称。
username	字符串（必须）。此字符串指定此 APN 的用户名称。如果缺少此字符串，安装描述文件过程中，设备会提示输入此字符串。
password	数据 （可选）。此数据代表此 APN 的用户密码。为了达到迷惑目的，它已被编码。如果有效负载中缺少此字符串，安装描述文件过程中，设备会提示输入此字符串。

Exchange 有效负载

Exchange 有效负载是由 com.apple.eas.account 有效负载类型 (PayloadType) 值指定的。此有效负载会在设备上创建一个 Microsoft Exchange 帐户。除了与所有有效负载相同的设置之外，此有效负载定义了以下内容：

键	值
EmailAddress	字符串 （必须）。如果有效负载中不存在，安装描述文件过程中，设备会提示输入此字符串。指定帐户的完整电子邮件地址。
Host	字符串 （必须）。指定 Exchange 服务器主机名称 （或 IP 地址）。
SSL	布尔值 （可选）。默认为 “YES”。指定 Exchange 服务器是否使用 SSL 进行认证。
UserName	字符串 （必须）。此字符串指定此 Exchange 帐户的用户名称。如果缺少此字符串，安装描述文件过程中，设备会提示输入此字符串。

VPN 有效负载

VPN 有效负载是由 com.apple.vpn.managed 有效负载类型 (PayloadType) 值指定的。除了与所有有效负载类型相同的设置之外， VPN 有效负载还定义了以下键。

键	值
UserDefinedName	字符串。 VPN 连接的描述，会显示在设备上。
OverridePrimary	布尔值。指定是否通过 VPN 接口发送所有通信。如果该值为真，所有网络通信都会通过 VPN 发送。
VPNType	字符串。决定有效负载中可用于此类型的 VPN 连接的设置。它可以有三个可能的值：“L2TP”、“PPTP”或“IPSec”，分别代表 L2TP、 PPTP 和 Cisco IPSec。

在顶层、键“PPP”和“IPSec”下面有两个可能存在的词典。下面描述这两个词典内的键，以及使用了这些键的 VPNType 值。

PPP 词典键

以下元素用于 PPP 类型的 VPN 有效负载。

键	值
AuthName	字符串。 VPN 帐户用户名称。用于 L2TP 和 PPTP。
AuthPassword	字符串（可选）。仅当 TokenCard 为假时才可见。用于 L2TP 和 PPTP。
TokenCard	布尔值。是否使用令牌卡（例如 RSA SecurID）进行连接。用于 L2TP。
CommRemoteAddress	字符串。 VPN 服务器的 IP 地址或主机名称。用于 L2TP 和 PPTP。
AuthEAPPlugins	数组。仅当使用 RSA SecurID 时才存在，在这种情况下，该数组含有一个条目，这个条目就是含有值“EAP-RSA”的字符串。用于 L2TP 和 PPTP。
AuthProtocol	数组。仅当使用 RSA SecurID 时才存在，在这种情况下，该数组含有一个条目，这个条目就是含有值“EAP”的字符串。用于 L2TP 和 PPTP。
CCPMPPE40Enabled	布尔值。请参阅 CCPEnabled 下面的说明。用于 PPTP。
CCPMPPE128Enabled	布尔值。请参阅 CCPEnabled 下面的说明。用于 PPTP。
CCPEnabled	布尔值。启用加密连接。如果此键和 CCPMPPE40Enabled 为真，则代表自动加密级别；如果此键和 CCPMPPE128Enabled 为真，则代表最高加密级别。如果未使用加密，则没有一个 CCP 键为真。用于 PPTP。

IPSec 词典键

以下元素用于 IPSec 类型的 VPN 有效负载。

键	值
RemoteAddress	字符串。VPN 服务器的 IP 地址或主机名称。用于 Cisco IPSec。
AuthenticationMethod	字符串。不是“SharedSecret”就是“Certificate”。用于 L2TP 和 Cisco IPSec。
XAuthName	字符串。 VPN 帐户的用户名称。用于 Cisco IPSec。
XAuthEnabled	整数。如果 XAUTH 为 ON 则为 1；如果 XAUTH 为 OFF 则为 0。用于 Cisco IPSec。
LocalIdentifier	字符串。仅当 AuthenticationMethod 等于 SharedSecret 时才会存在。要使用的组别的名称。如果使用“混合认证”，则字符串必须以“[hybrid]”结尾。用于 Cisco IPSec。
LocalIdentifierType	字符串。仅当 AuthenticationMethod 等于 SharedSecret 时才会存在。该值是“KeyID”。用于 L2TP 和 Cisco IPSec。
SharedSecret	数据。此 VPN 帐户的共享密钥。仅当 AuthenticationMethod 等于 SharedSecret 时才会存在。用于 L2TP 和 Cisco IPSec。
PayloadCertificateUUID	字符串。证书的 UUID，用于帐户凭证。仅当 AuthenticationMethod 等于 Certificate 时才会存在。用于 Cisco IPSec。
PromptForVPNPIN	布尔值。连接时是否提示输入 PIN。用于 Cisco IPSec。

Wi-Fi 有效负载

Wi-Fi 有效负载是由 com.apple.wifi.managed 有效负载类型 (PayloadType) 值指定的。该值描述版本 0 的 PayloadVersion 值。除了与所有有效负载类型相同的设置之外，有效负载还定义了以下键。

键	值
SSID_STR	字符串。要使用的 Wi-Fi 网络的 SSID。此键名称在 <Apple80211/Apple80211API.h> 中声明为 APPLE80211KEY_SSID_STR。
HIDDEN_NETWORK	布尔值。除 SSID 外，设备还使用广播类型和加密类型等信息来辨别网络。默认情况下，假定配置的所有网络都是开放的或广播的。要指定隐藏网络，您需要给键“HIDDEN_NETWORK”或“APPLE80211KEY_HIDDEN_NETWORK”赋一个布尔值。

键	值
EncryptionType	字符串。“EncryptionType”的可能值是 “WEP”、“WPA”或“Any” 。“WPA”对应 WPA 和 WPA2，应用于这两种加密类型。请确定这些值与网络访问点的能力完全相符。如果您不确定加密类型是哪种，或者您更希望它应用于所有加密类型，请使用值 “Any”。
Password	字符串 （可选）。缺少密码不会防止网络被添加到已知网络的列表中。连接到该网络时，用户最终会被提示提供密码。

对于 802.1X 企业级网络，必须提供 EAPClientConfiguration 词典。

EAPClientConfiguration 词典

除了标准加密类型之外，还可能会通过 “EAPClientConfiguration”键为给定的网络指定一个企业级描述文件。此键在 <EAP8021X/EAPOLControlTypes.h> 中声明为 kEAPOLControlEAPClientConfiguration。如果存在的话，它的值就是含有以下键的词典。

键	值
UserName	字符串 （可选）。除非您知道准确的用户名称，否则此属性将不会出现在导入的配置中。进行认证时，用户可以输入此信息。
AcceptEAPTypes	整数值数组。以下 EAP 类型会被接受： 13 = TLS 17 = LEAP 21 = TTLS 25 = PEAP 43 = EAP-FAST
TLSTrustedCertificates	数据值数组 （可选）。这是将被信任的、用来进行此认证的证书的列表。每个数据元素都包含 .cer 格式的相应证书。 此键可让您手工制作准备用于给定网络的证书列表，并且避免要求用户动态地设定对某个证书是否信任。 如果指定了此属性，动态信任 （证书对话）会被停用，除非 TLSAllowTrustExceptions 也被指定了值 “TRUE”（请参阅下文）。

键	值
TLSTrustedServerCommonNames	字符串值数组 （可选）。这是能够被接受的服务器证书常用名称的列表。如果服务器的证书不在此列表中，它将不会被信任。 在单独使用或与TLSTrustedCertificates 组合使用的情况下，该属性可让用户小心地手工设定，所给定的网络信任哪些证书，并且避免动态信任的证书。 如果指定了此属性，动态信任 （证书对话）会被停用，除非 TLSAllowTrustExceptions 也被指定了值 “TRUE”（请参阅下文）。
TLSAllowTrustExceptions	布尔值（可选）。允许 / 不允许用户做出的动态信任决定。动态信任是证书不被信任时出现的证书对话。如果该值为 “FALSE”且证书还没有被信任，则认证失败。请参阅上文的 TLSTrustedCertificates 和 TLSTrustedServerCommonNames。 此属性的默认值是 “TRUE”，除非提供了 TLSTrustedCertificates 或 TLSTrustedServerCommonNames （这种情况下默认值是 “FALSE”）。
TTLSInnerAuthentication	字符串 （可选）。这是 TTLS 模块所使用的内部认证。默认值是 “MSCHAPv2”。 可能的值是“PAP”、“CHAP”、“MSCHAP”和“MSCHAPv2”。
OuterIdentity	字符串 （可选）。此键只与 TTLS、 PEAP 和 EAP-FAST 相关。 这允许用户隐藏他 （或她）的身份。用户的实际名称只会出现在加密隧道内部。例如，它可以被设定为 “anonymous”、“anon”或 “anon@mycompany.net”。 它可以提高安全性，因为攻击者无法以明文形式看到认证用户的名称。

EAP-Fast 支持

在 EAPClientConfiguration 词典中， EAP-FAST 模块使用以下属性。

键	值
EAPFASTUsePAC	布尔值 （可选）。
EAPFASTProvisionPAC	布尔值 （可选）。
EAPFASTProvisionPACAnonymously	布尔值 （可选）。

这些键实际上是有层次的：如果 EAPFASTUsePAC 为 “FALSE”，则不会考虑其他两个属性。类似地，如果 EAPFASTProvisionPAC 为 “FALSE”，则不会考虑 EAPFASTProvisionPACAnonymously。

如果 EAPFASTUsePAC 为 “FALSE”，则认证步骤与 PEAP 或 TTLS 十分相似：服务器每次都使用证书来验证它的身份。

如果 EAPFASTUsePAC 为“TRUE”，则会使用现有的 PAC（如果它存在的话）。目前，在设备上获得 PAC 的唯一方法是允许 PAC 供给 (PAC provisioning)。因此，您需要启用 EAPFASTProvisionPAC，而且如果需要的话，也要启用 EAPFASTProvisionPACAnonymously。 EAPFASTProvisionPACAnonymously 有安全性弱点：它不使用证书来认证服务器；它依赖用户密码的共享密钥。

证书

如同 VPN 配置一样，将证书身份配置与 Wi-Fi 配置相关联是可能做到的。定义凭证以建立安全的企业级网络时，这样做很有帮助。要关联一个身份，请通过“PayloadCertificateUUID”键来指定它的有效负载 UUID。

键	值
PayloadCertificateUUID	字符串。为证书有效负载的 UUID，用于身份凭证。