iPhone OS
企业级部署指南

第二版，适用于 3.2 或更高版本

Apple Inc.
© 2010 Apple Inc. 保留一切权利。

未经 Apple 的书面同意，不得拷贝本手册的全部或部分内容。

Apple 标志是 Apple Inc. 在美国及其他国家和地区注册的商标。事先未经 Apple 书面同意，将 “键盘” Apple 标志 (Option-Shift-K) 用于商业用途可能会违反美国联邦和州法律，并可能被指控侵犯商标权和进行不公平竞争。

我们已尽力确保本手册上的信息准确。 Apple 对印刷或文字错误概不负责。

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

Apple、苹果、 Apple 标志、 Bonjour、 iPhone、 iPod、 iPod touch、 iTunes、 Keychain、 Leopard、 Mac、 Macintosh、 Mac 标志、 Mac OS、 QuickTime 和 Safari 是 Apple Inc. 在美国及其他国家和地区注册的商标。

iPad 是 Apple Inc. 的商标。

iTunes Store 和 App Store 是 Apple Inc. 在美国及其他国家和地区注册的服务标记。 MobileMe 是 Apple Inc. 的服务标记。

这里提及的其他公司和产品名称是其相应公司的商标。提及的第三方产品仅作参考，并不代表 Apple 之认可或推荐。 Apple 对这些产品的性能或使用概不负责。

本手册英文版在美国和加拿大同时出版。

CH019-1835/2010-04

目录

iPhone 在企业中的应用

了解如何将 iPhone、 iPod touch 和 iPad 与企业系统整合在一起。

本指南是专为系统管理员编写的。本手册包含有关在企业环境中部署并支持 iPhone、 iPod touch 和 iPad 的信息。

iPhone OS 3.0 及更高版本中用于企业的新功能

iPhone OS 3.x 包括许多增强功能，其中包括以下特别吸引企业用户的增强功能:

- 支持 CalDAV 日历无线同步。
- LDAP 服务器支持在 Mail、地址簿和 SMS 中查找联系人。
- 配置描述文件可被加密和锁定给设备，因此要删除它们就需要管理员密码。
- “iPhone 配置实用工具”可让您直接在通过 USB 与电脑连接的设备上添加和删除加密的配置描述文件。
- 支持使用在线证书状态协议 (OCSP) 来撤销证书。
- 现在支持随需应变型基于证书的 VPN 连接。
- 支持通过配置描述文件和 VPN 服务器的 VPN 代理配置。
- Microsoft Exchange 用户可以邀请他人参加会议。 Microsoft Exchange 2007 用户还可以查看回复状态。
- 支持基于 Exchange ActiveSync 客户端证书的鉴定。
- 除了 EAS 协议 12.1 以外，还支持附加的 EAS 策略。
- 提供附加的设备限制，包括指定设备可以保持多长时间的解锁状态、是否停用相机以及是否阻止用户拍摄设备显示屏的屏幕快照。
- 本地邮件和日历事件可被搜索。对于 IMAP、 MobileMe 和 Exchange 2007，位于服务器上的邮件同样可被搜索。
- 可以指定附加的邮件文件夹用于推送电子邮件传输。
- 可以使用配置描述文件来指定 APN 代理设置。
- 可以使用配置描述文件来安装 Web Clip。
- 现在支持 802.1x EAP-SIM。
- 可以使用简单证书注册协议 (SCEP) 服务器以无线方式鉴定和注册设备。

- iTunes 可以将设备备份以加密格式储存。
- “iPhone 配置实用工具”支持通过脚本来创建描述文件。
- “iPhone 配置实用工具 2.2”支持 iPad、 iPhone 和 iPod touch。要求 Mac OS X v10.6 Snow Leopard。还支持 Windows 7。

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、 iPod touch 和 iPad 与企业系统整合在一起的各种组件。

iPhone 和 iPod touch

与企业级网络配合使用的 iPhone 和 iPod touch 设备必须更新到 iPhone OS 3.1.x。

iPad

iPad 必须更新到 iPhone OS 3.2.x。

iTunes

需要 iTunes 9.1 或更高版本才能设置设备。在安装 iPhone、 iPod touch 和 iPad 的软件更新时，也需要 iTunes。此外，使用 iTunes 来安装应用程序，并与 Mac 或 PC 同步音乐、视频、备忘录或其他数据。

要使用 iTunes，您需要一台带有 USB 2.0 端口并满足 iTunes 网站上列出的最低要求的 Mac 或 PC。请参阅 www.apple.com.cn/itunes/download/ 网址。

iPhone 配置实用工具

“iPhone 配置实用工具”可让您创建、加密和安装配置描述文件，记录及安装预置描述文件和授权的应用程序，还能采集设备信息 （如控制台日志）。

“iPhone 配置实用工具”要求以下一项内容：

- Mac OS X v10.5 Leopard
- Windows XP Service Pack 3，安装了 .NET Framework 3.5 Service Pack 1
- Windows Vista Service Pack 1，安装了 .NET Framework 3.5 Service Pack 1
- Windows 7，安装了 .NET Framework 3.5 Service Pack 1

“iPhone 配置实用工具”在 64 位版本的 Windows 上以 32 位模式运行。

您可以从以下网址下载 .Net Framework 3.5 Service Pack 1 安装程序：
http://www.microsoft.com/downloads/details.aspx?familyid=ab99342f-5d1a-413d-8319-81da479ab0d7

实用工具允许您创建一封 Outlook 邮件，而配置描述文件则作为附件包含在内。此外，您可以从桌面的地址簿中将用户的姓名和电子邮件地址分配给与实用工具连接的设备。这两项功能均需要 Outlook，但与 Outlook Express 不兼容。要在 Windows XP 电脑上使用这些功能，您可能需要安装 2007 Microsoft Office 系统更新：Redistributable Primary Interop Assemblies。如果 Outlook 安装于 .NET Framework 3.5 Service Pack 1 之前，则这一步很有必要。

Primary Interop Assemblies 安装程序可从以下网址下载：
http://www.microsoft.com/downloads/details.aspx?FamilyID=59daebaa-bed4-4282-a28c-b864d8bfa513

Microsoft Exchange ActiveSync

iPhone、 iPod touch 和 iPad 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 版

为了支持 Exchange 2007 的策略和功能， Service Pack 1 是必需的。

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
- 要求数字和字母
- 不活跃时间 （以分钟计）

还支持以下 Exchange 2007 策略：

- 允许或禁止简单密码
- 密码到期
- 密码历史记录
- 策略刷新间隔时间
- 密码中复杂字符的最小数目
- 漫游时要求手动同步
- 允许使用相机
- 要求设备加密

有关每条策略的描述，请参阅 Exchange ActiveSync 文稿。

iPhone 3GS、 iPod touch （2009 年秋季推出的型号，储存容量为 32 GB 或更高）和 iPad 支持要求设备加密 (RequireDeviceEncryption) 的 Exchange 策略。 iPhone、iPhone 3G 和其他 iPod touch 型号不支持设备加密，将无法连接到要求设备加密的 Exchange Server。

如果在 Exchange 2003 上启用 “要求数字和字母”策略或在 Exchange 2007 上启用“要求提供字母数字密码”策略，则用户必须输入至少包含一个复杂字符的设备密码。

由不活跃时间策略指定的值 （MaxInactivityTimeDeviceLock 或 AEFrequencyValue）用于设定用户在 “设置” > “通用” > “自动锁定”以及 “设置” > “通用” > “密码锁定” > “需要密码”中可以选择的最大值。

远程擦除

您可以远程擦除 iPhone、 iPod touch 或 iPad 上的内容。执行擦除操作会删除设备中的所有数据和配置信息。会安全地抹掉设备内容，并将设备恢复为原始的出厂设置。

【重要事项】在 iPhone 和 iPhone 3G 上，执行擦除操作会覆盖设备上的数据 （每 8 GB 的设备容量大约需要 1 小时） 。擦除前，请将设备与电源连接。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。在 iPhone 3GS 和 iPad 上，执行擦除操作会删除数据 （使用 256 位 AES 加密） 的加密密钥并即刻完成。

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 “还原”菜单中选取 “抹掉全部内容和设置”来擦除其拥有的设备。设备还可以被配置为在几次输入错误的密码后自动启动擦除功能。

如果您恢复因遗失而擦除了数据的设备，请通过 iTunes 使用设备最新的备份进行恢复。

Microsoft Direct Push

如果蜂窝电话连接或 Wi-Fi 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 和 iPad Wi-Fi + 3G。 iPod touch 和 iPad Wi-Fi 不具备蜂窝电话连接，因此只有在它们已激活并连接到 Wi-Fi 网络时，才能收到推送通知。

Microsoft Exchange Autodiscovery

支持 Exchange Server 2007 的 Autodiscover 服务。当您手动配置设备时，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 网址。

Microsoft Exchange Global Address List

iPhone、 iPod touch 和 iPad 会从您公司的 Exchange 服务器公司目录取回联络信息。在 “通讯录”中搜索时，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补全电子邮件地址。

额外支持的 Exchange ActiveSync 功能

除了已经描述的特性和功能以外， iPhone OS 还支持：

- 创建日历邀请。使用 Microsoft Exchange 2007，您还可以看到您发出的邀请的回复状态。
- 为日历事件设定 “空闲”、“正忙”、“暂定”或 “离开办公室”状态。
- 在服务器上搜索邮件信息。需要 Microsoft Exchange 2007。
- Exchange ActiveSync 客户端基于证书的鉴定。

不支持的 Exchange ActiveSync 功能

不是所有的 Exchange 功能都受支持，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
- 给信息打上旗标以方便跟进

VPN

iPhone OS 可以与支持以下协议和鉴定方式的 VPN 服务器配合使用：

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

Cisco IPSec （基于证书的鉴定）针对配置时指定的域支持 “请求 VPN 域”。有关详细信息，请参阅第 32 页 “VPN 设置”。

网络安全

iPhone OS 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 OS 还支持以下适用于 WPA 企业级和 WPA2 企业级网络的 802.1X 鉴定方式：

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

证书和身份

iPhone、 iPod touch 和 iPad 可以配合 RSA 密钥来使用 X.509 证书。可以识别的文件扩展名包括 .cer、 .crt 和 .der。证书链评估由 Safari、 Mail、 VPN 和其他应用程序执行。

使用只包含一个身份的 P12 （PKCS #12 标准）文件。可以识别的文件扩展名包括 .p12 和 .pfx。安装身份时，会提示用户输入能够对它进行保护的口令。

建立到信任的根证书的证书链所必需的证书可以手动安装，也可以使用配置描述文件安装。您不必添加根证书，它们已经由 Apple 添加到设备中了。要查看预装的系统根证书的列表，请参阅网址 http://support.apple.com/kb/HT3580?viewlocale=zh_CN 上的 Apple 支持文章。

通过 SCEP，证书可以无线方式被安全地安装。有关更多信息，请参阅第 21 页“已鉴定的注册和配置过程概览”。

电子邮件帐户

iPhone、 iPod touch 和 iPad 支持各种服务器平台（包括 Windows、 UNIX、 Linux 和 Mac OS X）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。

当用户搜索邮件时，他们可以选择在邮件服务器上继续搜索。此功能适用于 Microsoft Exchange Server 2007 以及大多数基于 IMAP 的帐户。

用户的电子邮件帐户信息 （包括 Exchange 用户 ID 和密码）安全地储存于设备中。

LDAP 服务器

iPhone、 iPod touch 和 iPad 会从您公司的 LDAPv3 服务器公司目录取回联络信息。在 “通讯录”中搜索时，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补全电子邮件地址。

CalDAV 服务器

iPhone、 iPod touch 和 iPad 会与您公司的 CalDAV 服务器同步日历数据。设备与服务器之间会定期更新以反映日历的更改。

您还可以订阅发布的只读型日历，例如节日日历或那些带有同事日程安排的日历。

CalDAV 帐户不支持从设备上创建并发送新的日历邀请。

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 在企业中的应用网页，网址为 www.apple.com.cn/iphone/enterprise/
- iPad 在商业机构中的应用网页，网址为 www.apple.com.cn/ipad/business/
- “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），网址为 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
- 《iPhone **使用手册**》，可从 www.apple.com.cn/support/iphone/ 网址下载；要在 iPhone 上查看手册，请在 Safari 中轻按 《iPhone 使用手册》书签或访问 http://help.apple.com/iphone/ 网址。
- iPhone 指导教程，网址为 www.apple.com.cn/iphone/guidedtour/
- 《iPod touch **使用手册**》，可从 www.apple.com.cn/support/ipodtouch 网址下载；要在 iPod touch 上查看手册，请在 Safari 中轻按 《iPod touch 使用手册》或访问 http://help.apple.com/ipodtouch/ 网址。
- iPod touch 指导教程，网址为 www.apple.com.cn/ipodtouch/guidedtour/

- 《iPad 使用手册》，可从 www.apple.com.cn/support/ipad 网址下载；要在 iPad 上查看手册，请在 Safari 中轻按 《iPad 使用手册》或访问 http://help.apple.com/ipad/ 网址
- iPad 指导教程，网址为 www.apple.com/ipad/guided-tours/

部署 iPhone 和 iPod touch

1

本章概括了如何在您的企业中部署 iPhone, iPod touch 和 iPad。

iPhone、 iPod touch 和 iPad 已被设计成可轻松地与 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相整合。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、 iPod touch 和 iPad 的部署时，请考虑以下问题：

- 您公司的 iPhone 和 iPad （Wi-Fi + 3G 型号）将如何激活无线蜂窝电话服务？
- 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量设备？

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客户的话音与数据资费以及激活说明。

您或您的用户需要在 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 立即可以使用；否则， iTunes 会引导您完成激活新服务号码的全过程。

iPad 必须连接到安装了 iTunes 的电脑才能激活。如果在美国使用 iPad Wi-Fi + 3G，请使用 iPad 来注册和管理 （或取消） AT&T 数据计划。前往 “设置” > “蜂窝数据” > “显示帐户”。 iPad 已解锁，因此您可以使用您的首选运营商。请联系您的运营商以设置帐户，并获得兼容的微型 SIM 卡。在美国， iPad Wi-Fi + 3G 会附带与 AT&T 兼容的微型 SIM 卡。

虽然 iPod touch 和 iPad Wi-Fi 不配备蜂窝电话服务或 SIM 卡，但它们也必须连接到安装了 iTunes 的电脑才能激活。

因为需要 iTunes 才能完成激活过程，所以您必须决定是在每个用户的 Mac 或 PC 上安装 iTunes，还是只在自己的电脑上安装 iTunes 以完成每个设备的激活。

激活之后，设备与企业系统配合使用不需要 iTunes，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 OS 3.x 软件配合现有的 Microsoft Exchange Server 2003 或 Microsoft Exchange Server 2007 解决方案，启用了安全推送电子邮件、推送通讯录和推送日历，也实现了 “全局地址查找”、“远程擦除”和设备密码策略实施等功能。它还允许用户通过以下方式安全地连接到公司资源：使用 802.1 X 无线鉴定通过 WPA 企业级和 WPA2 企业级无线网络进行连接；使用 PPTP、LT2P over IPSec 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。为了以无线方式访问日历和目录，它支持 CalDAV 和 LDAP。

当您确定想要用户访问哪些网络服务时，请参阅以下部分中的信息。

Microsoft Exchange

iPhone 通过 Microsoft Exchange ActiveSync (EAS) 直接与 Microsoft Exchange Server 通信。 Exchange ActiveSync 在 Exchange Server 和 iPhone 或 iPad Wi-Fi + 3G 之间维持一个连接，这样，当新电子邮件信息或会议邀请到达时，设备会立即得到更新。 iPod touch 和 iPad Wi-Fi 不具备蜂窝电话连接，因此只有在它们已激活并连接到 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，但您的公司刚刚开始使用 Exchange ActiveSync，请检查以下部分中的信息。

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 “鉴定方式”属性中只打开了基本鉴定，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 Intranet 客户端和互联网客户端使用。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。有关检测信号 (heartbeat) 和超时时间间隔 (timeout interval) 的信息，请参阅网址 http://technet.microsoft.com/en-us/library/cc182270.aspx 上的 Microsoft Exchange 文章。

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、 iPod touch 和 iPad 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。

由于支持 802.1X 鉴定， iPhone OS 设备可以整合到各种 RADIUS 服务器环境。支持 802.1X 无线鉴定方式，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、 iPod touch 和 iPad 支持的鉴定类型（EAP 类型）。请确定鉴定服务器上已启用了 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 鉴定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 鉴定的配置是正确的。
- 如果您计划使用基于证书的鉴定，请确定通过相应的密钥分发流程，已经将公开密钥基础设施配置成支持基于设备和基于用户的证书。
- 验证您的证书格式与设备及您的鉴定服务器的兼容性。有关证书的信息，请参阅第 11 页 “证书和身份”。

虚拟专用网络

iPhone、 iPod touch 和 iPad 支持使用 Cisco IPSec、L2TP over IPSec 和 PPTP 虚拟专用网络协议来安全地访问专用网络。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 证书来利用基于证书的鉴定。此外，基于证书的鉴定允许您利用 “请求 VPN 域”，它可以提供对您企业级网络的无缝、安全的无线访问。

对于基于令牌的双重身份鉴定， iPhone OS 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、 iPod touch 和 iPad 还支持用于 Cisco IPSec 和 L2TP/IPSec 部署的共享密钥鉴定以及用于基本用户名称和密码鉴定的 MS-CHAPv2。

“VPN 代理”自动配置 （PAC 和 WPAD）也受支持，它允许您指定用于访问特定 URL 的代理服务器设置。

VPN 设置指导

- iPhone OS 可以与大多数现有的 VPN 网络相整合，因此只需最低限度的配置即可使设备访问您的网络。准备部署的最佳途径是检查 iPhone 是否支持您公司现有的 VPN 协议和鉴定方式。
- 确保与 VPN 集中器提供的标准相兼容。最好检查一下至 RADIUS 或鉴定服务器的鉴定路径，以确定实现的网络中启用了 iPhone OS 支持的标准。
- 请咨询解决方案的提供商以确认您的软件和设备具备最新的安全补丁和固件。
- 如果您想要配置特定 URL 的代理设置，请将 PAC 文件放置在使用基本 VPN 设置即可访问的 Web 服务器上，并确保为其提供 MIME 类型的 application/x-ns-proxy-autoconfig。此外，还要配置您的 DNS 或 DHCP 以提供服务器 （可通过类似方式访问）上的 WPAD 文件的位置。

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鉴定和 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。例如，您可以使用此技术访问 Lotus Notes/Domino 或 Novell GroupWise 电子邮件。邮件服务器可以位于 DMZ 子网内，也可以位于公司防火墙后面，或者两种情况同时存在。

通过使用 SSL， iPhone OS 支持 128 位加密和主要证书颁发机构签发的 X.509 证书。它还支持强力鉴定方式，包括符合工业标准的 MD5 Challenge-Response 和 NTLMv2。

IMAP 网络设置指导

- 要获得附加的安全性保护，请在服务器上安装信任的证书颁发机构 (CA) 提供的数字证书。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。有关在 iPhone 上安装证书的信息，请参阅第 35 页 “凭证设置”。
- 要让 iPhone OS 设备从服务器取回电子邮件，请打开防火墙中的端口 993 并确定代理服务器已设定为 “IMAP over SSL”。

- 要让设备发送电子邮件，端口 587、 465 或 25 必须是打开的。首先使用端口 587，这是最佳选择。

LDAP 目录

iPhone OS 可让您访问基于标准的 LDAP 目录服务器，并提供全局地址目录或其他与 Microsoft Exchange 中的 “全球通讯簿”类似的信息。

在设备上配置好 LDAP 帐户后，该设备会在服务器的根层次搜索属性 `namingContexts` 以识别默认的搜索基准。搜索范围默认被设定为子树。

CalDAV 日历

iPhone OS 中的 CalDAV 支持可以为不使用 Microsoft Exchange 的组织提供全局日历和日程安排。 iPhone OS 可以配合支持 CalDAV 标准的日历服务器工作。

订阅的日历

如果您想要将公司事件 （如节日或特殊事件安排）日历以只读形式发布， iPhone OS 设备可订阅日历并在 Microsoft Exchange 日历和 CalDAV 日历中显示该信息。 iPhone OS 可以处理标准 iCalendar (.ics) 格式的日历文件。

将订阅的日历分发给用户的一个简单方法是，使用 SMS 或电子邮件将完整有效的 URL 发送给用户。当用户轻按链接时，该设备会订阅指定的日历。

企业级应用程序

要部署企业级 iPhone OS 应用程序，您可以使用 “iPhone 配置实用工具”或 iTunes 将这些应用程序安装在设备上。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。

在线证书状态协议

当您为 iPhone OS 设备提供数字证书时，请考虑签发它们，以使它们启用 OCSP。这将允许设备在使用证书前询问 OCSP 服务器证书是否已被撤销。

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，您应该确定想要实现哪些设备密码策略。

对于其网络、系统或应用程序不需要密码或鉴定令牌的公司，建议在设备上设定需要输入密码。如果您将基于证书的鉴定用于 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，您应该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。

可以用以下两种方法之一在 iPhone、 iPod touch 和 iPad 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。这可让您实施和更新策略，而不需执行任何用户操作。有关 EAS 策略的信息，请参阅第 8 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。如果您想要更改策略，您必须将已更新的描述文件递交或发送给用户，或者使用 “iPhone 配置实用工具”来安装该描述文件。有关设备密码策略的信息，请参阅第 30 页 “密码设置”。

如果您使用 Microsoft Exchange，则还可以使用配置策略来补充 EAS 策略。例如，这可让您访问 Microsoft Exchange 2003 中未提供的策略，或者可让您专门为 iPhone OS 设备定义策略。

配置设备

您需要决定将如何配置每个 iPhone、 iPod touch 或 iPad。配置方法在某种程度上受您在不同时间计划部署和管理的设备数量的影响。如果数量较少，对您或您的用户而言，您可能会发现手动配置每个设备更简单。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。

如果您部署大量设备，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。有些 VPN 和 Wi-Fi 设置只能使用配置描述文件来设定，而且如果您使用的不是 Microsoft Exchange，则将需要使用配置描述文件来设定设备密码策略。

配置描述文件可被加密和签名，这会允许您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。您还可以将描述文件标记为锁定到设备，这样一旦安装后，描述文件将不能被删除，除非擦除设备的所有数据，或者做为可选方案，您可以设置管理密码。

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。选取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 OS 软件更新也需要 iTunes，因此如果您决定不将 iTunes 分发给用户，请牢记这一点。有关部署 iTunes 的信息，请参阅第 4 章。

无线注册和配置

注册是鉴定设备和用户的过程，以便您可以自动化证书分发过程。数字证书让用户受益颇多。它们可用来鉴定对关键企业级服务 （如 Microsoft Exchange ActiveSync、 WPA2 企业级无线网络和公司 VPN 连接）的访问。基于证书的鉴定还会允许使用 “请求 VPN 域”以无缝访问公司网络。

除了使用无线注册功能来颁发您的公司的公开密钥基础设施 (PKI) 的证书外，您还可以部署设备配置描述文件。这不仅确保了只有被信任的用户才能访问公司服务，也确保了他们的设备是根据您公司的 IT 策略来配置的。由于配置描述文件既是加密了的，又是被锁定的，所以设置不能被删除、更改或与其他人共享。您既可以在以无线方式进行处理的过程中 （如下所述）使用这些功能，也可以在使用 “iPhone 配置实用工具”来配置设备 （设备已连接到您的管理员电脑上）时使用这些功能。要了解如何使用 “iPhone 配置实用工具”，请参阅第 2 章。

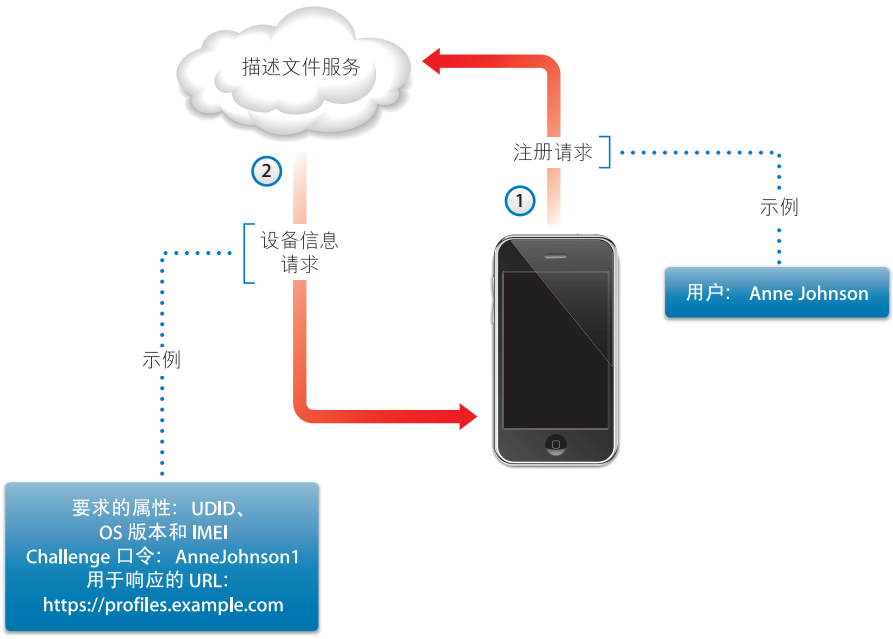
实现无线注册和配置需要开发并整合鉴定、目录和证书服务。这个过程可以使用标准的 Web 服务来部署，部署完成后，它会允许您的用户通过安全并经过鉴定的方式来设置他们的设备。

已鉴定的注册和配置过程概览

要实现此过程，您需要创建您自己的**描述文件分发服务**，该服务会接受 HTTP 连接、鉴定用户身份、创建 mobileconfig 描述文件以及管理本部分中所描述的整个过程。

您还需要 CA （证书颁发机构）来使用简单证书注册协议 (SCEP) 颁发设备凭证。有关 PKI、 SCEP 和相关主题的链接，请参阅第 26 页 “其他资源”。

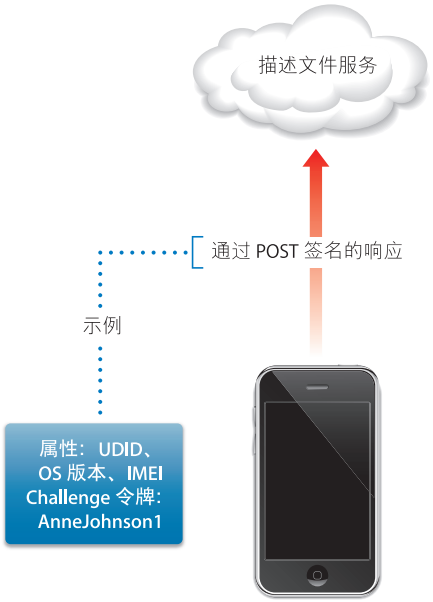
下面的图表显示 iPhone 所支持的注册和配置过程。



阶段 1 – 开始注册：当用户使用 Safari 访问您创建的描述文件分发服务的 URL 时，注册便会开始。您可以通过 SMS 或电子邮件分发此 URL。注册请求（如图表中的步骤 1 所示）应该鉴定用户的身份。鉴定可以和基本鉴定一样简单，或者您可以将其绑定到您的现有目录服务中。

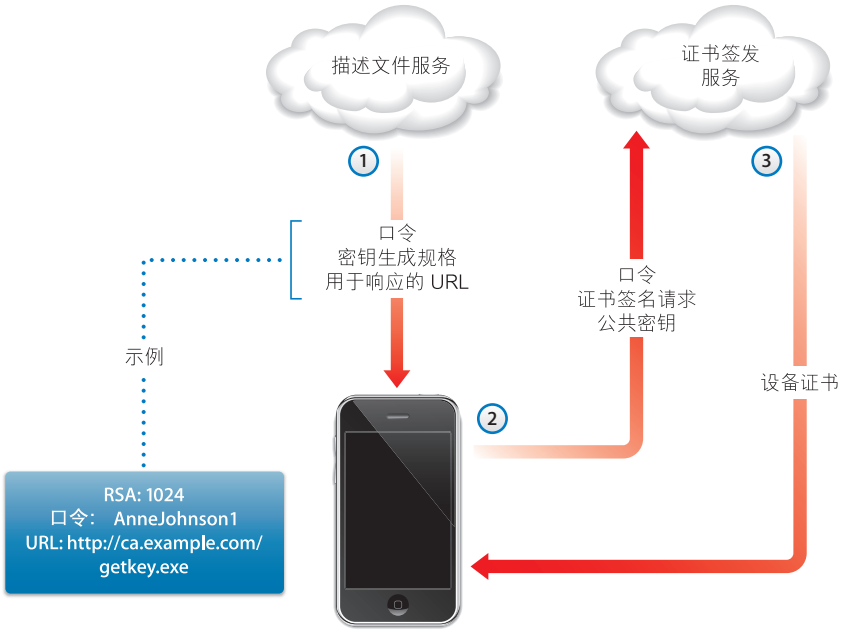
在步骤 2 中，您的服务在响应中发送了一个配置描述文件 (.mobileconfig)。此响应指定了设备在下次回复中必须提供的属性的列表以及在此过程中可传送用户身份的预共享密钥（口令），以便您可以为每个用户自定配置过程。服务可以请求的设备属性有 iPhone OS 版本、设备 ID（MAC 地址）、产品类型（iPhone 3GS 返回 iPhone2,1）、电话 ID (IMEI) 以及 SIM 信息 (ICCID)。

有关此阶段的配置描述文件示例，请参阅第 77 页 “阶段 1 服务器响应示例”。



阶段 2 – 设备鉴定：在用户同意安装从阶段 1 中接收到的描述文件后，设备会查找所请求的属性，添加口令响应（如果已提供），使用设备的内建身份（由 Apple 颁发的证书）给响应签名，然后使用 HTTP Post 将该响应发送回描述文件分发服务。

有关此阶段的配置描述文件示例，请参阅第 78 页“阶段 2 设备响应示例”。

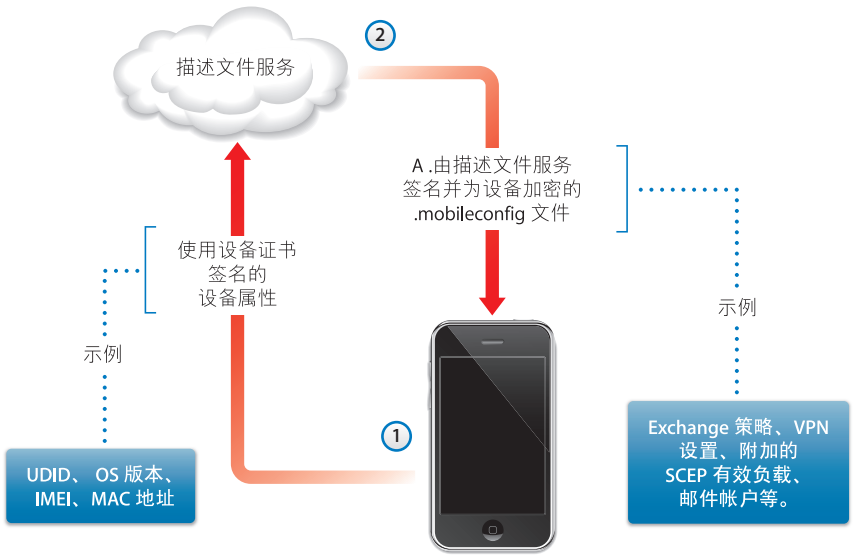


阶段 3 – 证书安装：在步骤 1 中，描述文件分发服务回应设备用来生成密钥 (RSA 1024) 的规格以及使用 SCEP （简单证书注册协议）返回认证的位置。

在步骤 2 中， SCEP 请求必须通过使用 SCEP 包中的口令来鉴定请求以在自动模式中处理。

在步骤 3 中， CA 回应适用于设备的加密证书。

有关此阶段的配置描述文件示例，请参阅第 78 页 “阶段 3 SCEP 规格的服务器响应示例”。



阶段 4 – 设备配置：在步骤 1 中，设备回复了属性列表 （已使用在上一个阶段中由 CA 提供的加密证书进行签名）。

在步骤 2 中，描述文件服务回应已加密的 .mobileconfig 文件，该文件会自动安装。描述文件服务应该给 .mobileconfig 文件签名。例如，它的 SSL 证书可用于此目的。

除了通用设置外，此配置描述文件应该还定义您想要强制实施的企业级策略，且它应该是锁定的描述文件，因此用户不能从设备将其删除。配置描述文件可以包含附加的使用 SCEP 的身份注册请求，该请求会在安装描述文件的过程中执行。

类似地，当使用 SCEP 安装的证书过期或者已经无效时，设备会要求用户更新描述文件。如果用户授权了请求，设备会重复上述过程以获得一个新的证书和描述文件。

有关此阶段的配置描述文件示例，请参阅第 80 页 “阶段 4 设备响应示例”。

其他资源

- 适用于 IPSec VPN 的数字证书 PKI，网址为 https://cisco.hosted.jivesoftware.com/docs/DOC-3592
- 公开密钥基础设施，网址为 http://en.wikipedia.org/wiki/Public_key_infrastructure
- IETF SCEP 协议规格，网址为 http://www.ietf.org/internet-drafts/draft-nourse-scep-18.txt

有关在企业中使用 iPhone、 iPod touch 和 iPad 的其他信息和资源，请参阅 www.apple.com.cn/iphone/enterprise/ 网址和 www.apple.com.cn/ipad/business/ 网址。

创建与部署配置描述文件

2

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

配置描述文件是 XML 文件，包含以下内容：设备的安全策略和限制、 VPN 配置信息、 Wi-Fi 设置、电子邮件帐户和日历帐户以及可允许 iPhone、 iPod touch 和 iPad 配合您的企业系统使用的鉴定凭证。

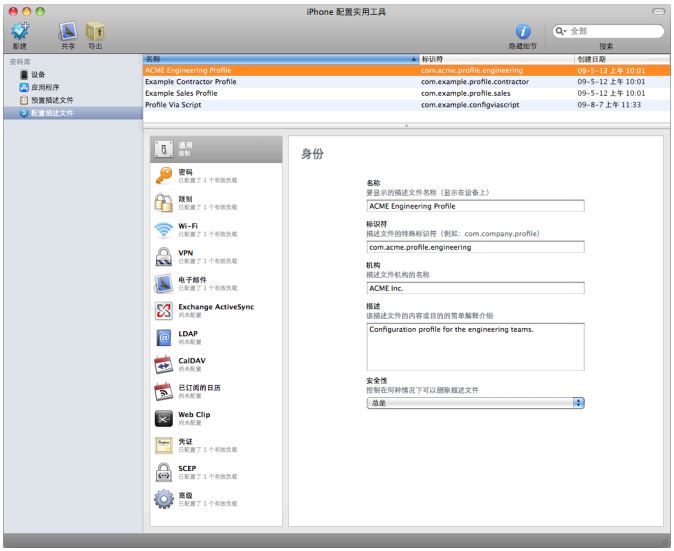
您可以使用 “iPhone 配置实用工具”将配置描述文件安装到通过 USB 端口与电脑连接的设备上，或者您也可以通过电子邮件或使用网页分发配置描述文件。当用户在他们的设备上打开电子邮件附件或使用 Safari 下载描述文件时，会提示他们开始执行安装过程。

如果不喜欢创建并分发配置描述文件，您可以手动配置设备。有关信息，请参阅第 3 章。

关于 “iPhone 配置实用工具”

“iPhone 配置实用工具”能让您轻松地创建、加密和安装配置描述文件、记录及安装预置描述文件和授权的应用程序，还能采集包括控制台日志在内的设备信息。当运行 “iPhone 配置实用工具”安装器或安装程序时，该实用工具会被安装在“/ 应用程序 / 实用工具 /”中 (Mac OS X)，或者安装在“Programs\iPhone 配置实用工具 \”中 (Windows)。

当打开 “iPhone 配置实用工具”时，会出现与下图类似的窗口。



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。
- **应用程序**会列出可用于安装在与电脑相连的设备上的应用程序。在设备上运行某些应用程序可能会需要预置描述文件。
- **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。预置描述文件还允许设备运行未使用 iTunes Store 分发的企业级应用程序。
- **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，或者您也可以创建一个新的配置以发送给用户或安装在连接的设备上。

边栏还会显示 **“已连接的设备”**，它显示当前连接在电脑 USB 端口上的 iPhone OS 设备的信息。已连接设备的相关信息会自动添加到 “设备”列表中，这样您就可以再次查看它而不必重新连接设备。连接设备后，您还可以加密描述文件以便仅在该设备上使用。

连接设备后，您可以使用 “iPhone 配置实用工具”在设备上安装配置描述文件和应用程序。有关详细信息，请参阅第 37 页 “使用 “iPhone 配置实用工具”安装配置描述文件”、第 61 页 “使用 “iPhone 配置实用工具”安装应用程序”和第 60 页 “使用 “iPhone 配置实用工具”安装预置描述文件”。

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。

创建配置描述文件

本文稿使用到术语**配置 (configuration)** **描述文件 (profile)** 和**有效负载 (payload)**。配置描述文件是一个完整文件，用于配置 iPhone、 iPod touch 或 iPad 的某些 （一项或多项）设置。有效负载是配置描述文件中，某类设置 （如 VPN 设置）的单独合集。

尽管您可以创建一个配置描述文件以包含组织机构所需的所有有效负载，但还是应该考虑单独为证书创建一个描述文件，为其他设置创建另一个 （或多个）描述文件，以便可以分别更新和分发各类信息。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。

许多有效负载都允许您指定用户名称和密码。如果忽略此信息，则描述文件可被多个用户使用，但在安装描述文件时将要求用户输入缺少的信息。如果为各个用户个性化描述文件，包括密码，您应该以加密格式分发描述文件以保护其中内容。有关更多信息，请参阅第 37 页 “安装配置描述文件”。

要创建新的配置描述文件，请在 “iPhone 配置实用工具”的工具栏中点按 “新建”按钮。使用有效负载列表可以将有效负载添加到描述文件中。然后，您可以在编辑面板中通过输入和选择选项来编辑有效负载。必需的栏位标有红色箭头。对于某些设置 （如 W-Fi 设置），您可以点按添加按钮 (+) 来添加配置。要删除一项配置，请点按编辑面板中的删除按钮 (–)。

要编辑有效负载，请在有效负载列表中选择合适的项目，然后点按 “配置”按钮，并填写如下所述的信息。

自动化配置描述文件创建

您还可以在 Mac 上使用 AppleScript 或在 Windows 上使用 C# 脚本来自动化配置文件的创建。要查看支持的方法和相关的语法，请执行以下操作:

- Mac OS X：使用 “脚本编辑程序”打开 “iPhone 配置实用工具”的 AppleScript 字典。
- Windows：使用 Visual Studio 查看 iPCUScripting.dll 提供的方法调用。

要执行脚本，在 Mac 上，请使用 AppleScript Tell 命令。在 Windows 上，请将脚本名称作为命令行参数传递给 “iPhone 配置实用工具”。

有关示例，请参阅附录 C “示例脚本”。

通用设置

在这里您可以为此描述文件提供名称和标识符，并指定在安装后是否允许用户删除描述文件。

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。名称不必是唯一的，但您应该使用描述性名称，以识别该描述文件。

描述文件标识符必须唯一标识此描述文件，且格式必须为：com.companyname.identifier，其中 “identifier”用于说明该描述文件。（例如 com.mycompany.homeoffice。）

标识符非常重要，因为安装描述文件时，该值会与已存在于设备上的描述文件进行比较。如果标识符是唯一的，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描述文件匹配，则描述文件中的信息就会替换设备上的已有设置， Exchange 设置除外。要更改 Exchange 帐户，必须首先手动删除描述文件，这样才能消除与帐户相关的数据。

要阻止用户删除已安装在设备上的描述文件，请从 “安全性”弹出式菜单中选取一个选项。“使用授权”选项能让您指定一个授权密码以允许删除设备上的描述文件。如果您选择 “永不”选项，则描述文件可以使用新版本进行更新，但不能被删除。

密码设置

如果您没有使用 Exchange 密码策略，则请使用此有效负载设定设备策略。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策略的密码，否则描述文件将不会被安装。

如果同时使用设备策略和 Exchange 密码策略，则两组策略会合并，且会实施最严格的设置。有关所支持的 Exchange ActiveSync 策略的信息，请参阅第 8 页“Microsoft Exchange ActiveSync”。

以下策略可用：

- **需要设备密码：**需要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所有的功能和数据。
- **允许简单值：**允许用户在密码中使用连续的或重复的字符。例如，此选项允许将密码设定为 “3333”或 “DEFG”。
- **要求字母和数字值：**要求密码包含至少一个字母字符。
- **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。
- **自动锁定 （单位：分钟）：**在闲置此段时间后，设备将自动锁定。输入密码将它解锁。
- **密码历史记录：**如果新密码与以前使用过的密码匹配，则它将不会被接受。您可以指定记住多少组以前使用的密码来执行此项比较。
- **设备锁定的宽限期：**指定设备在使用后的多久时间内，无需再次提示输入密码即可解锁。
- **最多可允许的尝试失败次数：**确定尝试输入密码失败几次之后设备会被擦除。如果您不更改此设置，则在尝试输入密码失败六次之后，设备会强加一个时间延迟，然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。

限制设置

使用此有效负载可指定允许用户使用哪些设备功能。

- **允许不良内容：**关闭此项时，从 iTunes Store 购买的不良音乐或视频内容就会被隐藏。当通过 iTunes Store 销售不良内容时，内容提供商 （如唱片公司）会将它们标记为不良内容。
- **允许使用 Safari：**关闭此选项时，Safari Web 浏览器应用程序将被停用，并且它的图标也将从主屏幕中去掉。这同样也阻止了用户打开 Web Clip。
- **允许使用 YouTube：**关闭此选项时， YouTube 应用程序将被停用，并且它的图标也将从主屏幕中去掉。
- **允许使用 iTunes Music Store：**关闭此选项时， iTunes Music Store 将被停用，并且它的图标也将从主屏幕中去掉。用户将不能试听、购买或下载内容。
- **允许安装应用程序：**关闭此选项时， App Store 将被停用，并且它的图标也将从主屏幕中去掉。用户将无法安装或更新他们的应用程序。

- **允许使用相机：**关闭此选项时，相机会被完全停用并且其图标也会从主屏幕去掉。用户将无法拍照。
- **允许屏幕抓图：**关闭此选项时，用户将无法存储显示屏的屏幕快照。

Wi-Fi 设置

使用此有效负载可设定设备如何连接到无线网络。您可以通过在编辑面板中点按添加按钮 (+) 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匹配，以便用户发起连接。

- **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：**选择网络的鉴定方式。以下选择可用于个人级和企业级网络。
  - **无：**网络没有使用鉴定。
  - WEP：网络仅使用 WEP 鉴定。
  - WPA/WPA 2：网络仅使用 WPA 鉴定。
  - **任一：**设备在连接网络时采用 WEP 或 WPA 鉴定，但不会连接到未鉴定的网络。
- **密码：**输入加入无线网络所需的密码。如果留空，将要求用户输入密码。

企业级设置

在这部分中您可以指定用于连接企业级网络的设置。当您在“安全类型”弹出式菜单中选取一个企业级设置时，这些设置就会出现。

在“协议”标签中，您可以指定使用何种 EAP 方式进行鉴定并配置 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（如用户名称和鉴定协议）。如果已使用“凭证”部分安装了身份，则您可以使用“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该被视为信任的，以便为 Wi-Fi 连接验证鉴定服务器。“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该被视为可信的。请将要信任的鉴定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

使用此有效负载可输入 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 协议和鉴定方式的信息，请参阅第 10 页“VPN”。可用的选项根据您选择的协议和鉴定方式而有所变化。

请求 VPN 域

对于基于证书的 IPSec 配置，您可以打开 “请求 VPN 域”以便在访问某些域时自动建立 VPN 连接。

“请求 VPN 域”选项有：

设置	描述
总是	为与指定的域相匹配的任何地址发起 VPN 连接。
永不	不会为与指定的域相匹配的地址发起 VPN 连接，但如果 VPN 已经处于活跃状态，则它可以被使用。
需要时建立	仅在 DNS 查找失败之后，才会为与指定的域相匹配的地址发起 VPN 连接。

此操作应用于所有匹配的地址。地址使用简单的字符串匹配进行比较，从末尾开始反向比较。地址 “.example.org”与 “support.example.org”和 “sales.example.org”相匹配，但与 “www.private-example.org”不匹配。不过，如果您将匹配域指定为 “example.com”（注意开头没有句点），则它会与 “www.private-example.com”和所有其他地址相匹配。

请注意， LDAP 连接不会发起 VPN 连接；如果 VPN 尚未由其他应用程序 （如 Safari）建立，则 LDAP 查找将失败。

VPN 代理

iPhone 支持手动 VPN 代理，以及使用 PAC 或 WPAD 的自动代理配置。要指定 VPN 代理，请从 “代理设置”弹出式菜单中选择一个选项。

对于基于 PAC 的自动代理配置，请从弹出式菜单中选择 “自动”，然后输入 PAC 文件的 URL。有关 PACS 功能和文件格式的信息，请参阅第 51 页 “其他资源”。

对于 Web Proxy Autodiscovery (WPAD) 配置，请从弹出式菜单中选择 “自动”。留空 “代理服务器 URL”栏， iPhone 将使用 DHCP 和 DNS 请求 WPAD 文件。有关 WPAD 的信息，请参阅第 51 页 “其他资源”。

电子邮件设置

使用此有效负载来为用户配置 POP 邮件帐户或 IMAP 邮件帐户。如果您要添加 Exchange 帐户，请参阅下面的 Exchange 设置。

用户可以修改您在描述文件中提供的某些邮件设置，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。

通过点按添加按钮 (+) 您可以添加多个邮件帐户。

Exchange 设置

使用此有效负载可输入用户的设置以访问 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；或者您也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。

每个设备只能配置一个 Exchange 帐户。添加 Exchange 帐户时，其他电子邮件帐户（包括 Exchange via IMAP 帐户）不受影响。当描述文件被删除时，使用描述文件添加的 Exchange 帐户也会被删除，除此方式外，它不能被删除。

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）。

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鉴定所必需的证书。

要提供一个能使 Exchange ActiveSync 服务器识别用户身份的证书，请点按添加按钮 (+) 然后从 Mac OS X 钥匙串或 Windows 证书库中选择一个身份证书。添加证书后，如果对于您的 ActiveSync 配置有必要，可以指定鉴定凭证名称。您还可以在配置描述文件中嵌入证书的口令。如果没有提供口令，则在安装描述文件时，用户会被要求输入口令。

LDAP 设置

使用此有效负载可输入设置以连接 LDAPv3 目录。您可以为每个目录指定多个搜索基准，并且通过点按添加按钮 (+) 您可以配置多个目录连接。

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鉴定所必需的证书。

CalDAV 设置

使用此有效负载可提供帐户设置以连接到兼容 CalDAV 的日历服务器。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）。

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鉴定所必需的证书。

通过点按添加按钮 (+) 您可以配置多个帐户。

订阅的日历的设置

使用此有效负载可向设备的 “日历”应用程序添加只读类型的日历订阅。通过点按添加按钮 (+) 您可以配置多个订阅。

您可以订阅的公共日历列表可在 www.apple.com.cn/downloads/macosx/calendars/ 网址获取。

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鉴定所必需的证书。

Web Clip 设置

使用此有效负载可为用户设备的主屏幕添加 Web Clip。Web Clip 提供了对喜爱的网页的快速访问。

请确定输入的 URL 包含前缀 http:// 或 https:// －这是 « Web Clip 正常工作所必需的。例如，要向主屏幕添加 《**iPhone 使用手册**》的在线版本，请指定 Web Clip URL：http://help.apple.com/iphone/

要添加自定图标，请选择一个格式为 gif、 jpeg 或 png，大小为 59 x 60 像素的图形文件。该图像会自动缩放和裁剪至适合大小，如有必要，还会转换为 png 格式。

凭证设置

使用此有效负载可向设备添加证书和身份。有关所支持的格式的信息，请参阅第 11 页 “证书和身份”。

安装凭证时，还会安装中间证书，它是建立到设备上被信任的证书的证书链所必需的。要查看预装的根证书的列表，请参阅网址 http://support.apple.com/kb/HT2185?viewlocale=zh_CN 上的 Apple 支持文章。

如果您要添加一个身份以配合 Microsoft Exchange 使用，请使用 Exchange 有效负载替代。请参阅第 34 页 “Exchange 设置”。

在 Mac OS X 上添加凭证：

1. 点按添加按钮 (+)。
2. 在出现的文件对话框中，选择 PKCS1 或 PKSC12 文件，然后点按 “打开”。

   如果您想要安装的证书或身份位于钥匙串中，请使用 “钥匙串访问”将其导出为 .p12 格式。“钥匙串访问”位于 “/ 应用程序 / 实用工具”目录下。有关帮助信息，请参阅 “钥匙串访问帮助”（“钥匙串访问”打开后位于 “帮助”菜单中）。

要向配置描述文件添加多个凭证，请再次点按添加按钮 (+)。

在 Windows 上添加凭证：

1. 点按添加按钮 (+)。
2. 从 Windows 证书库中选择您想要安装的凭证。

如果凭证不在您的个人证书库中，则必须添加它，并且专用密钥必须被标记为可导出（这是证书导入向导中的其中一个步骤）。请注意，添加根证书需要以管理员身份访问电脑，并且证书必须被添加到个人证书库中。

如果您使用了多个配置描述文件，请确定证书不重复。您不能安装同一证书的多个副本。

除了使用配置描述文件安装证书外，您还可以让用户使用 Safari 从网页直接将证书下载到设备上。或者，您也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 50 页 “安装身份和根证书”。您还可以使用 SCEP 设置 （如下所述）来指定安装描述文件时设备如何以无线方式获取证书。

SCEP 设置

SCEP 有效负载可让您指定设置以允许设备使用 “简单证书注册协议” (SCEP) 从证书颁发机构 (CA) 获取证书。

设置	描述
URL	这是 SCEP 服务器的地址。
名称	这可以是任何字符串，只要能让证书颁发机构理解，例如，它可以用于区分实例。
主体	表示为 OID 数组和值的 X.500 名称的描述。例如，/C=US/O=Apple Inc./CN=foo/1.2.5.3=bar，将被转换为：[[[“C”,“US”]], [[“O”,“Apple Inc.”]], ..., [[“1.2.5.3”,“bar”]]]
口令	一个预先共享的密钥， SCEP 服务器可用它来识别请求或用户。
密钥大小和用途	选择一个密钥大小，并使用此栏下方的注记格接受密钥的使用。
手印	如果您的证书颁发机构使用 HTTP，请使用此栏提供 CA 的证书的手印，设备将使用该证书在注册过程中确认 CA 的回应的真实性。您可以输入 SHA1 或 MD5 手印，或者选择一个证书以导入其签名。

有关 iPhone 如何以无线方式获取证书的更多信息， 请参阅第 21 页 “无线注册和配置”。

高级设置

“高级”有效负载可让您更改设备的访问点名称 (APN) 和蜂窝网络代理设置。这些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电话网络访问数据。要撤销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 建议您在一个单独的配置描述文件中定义 APN 设置，独立于其他企业设置，因为指定 APN 信息的描述文件必须由您的蜂窝电话服务商签名。

iPhone OS 支持长达 20 个字符的 APN 用户名称，和长达 32 个字符的密码。

编辑配置描述文件

在 “iPhone 配置实用工具”中，从 “配置描述文件”列表中选择一个描述文件，然后使用有效负载列表和编辑面板进行更改。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。如果设置面板不可见，请选取 “显示”>“显示细节”。

“通用”有效负载中的 “标识符”栏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，请不要更改标识符。

安装预置描述文件和应用程序

“iPhone 配置实用工具”可以在电脑连接的设备上安装应用程序和分配预置描述文件。有关详细信息，请参阅第 58 页第 5 章 “部署应用程序”。

安装配置描述文件

创建描述文件后，您可以连接设备并使用 “iPhone 配置实用工具”安装该描述文件。

另外，您还可以通过发送电子邮件或在网站上发布的方式将描述文件分发给用户。当用户使用其设备打开电子邮件信息或从 Web 上下载描述文件时，会提示他们开始安装过程。

使用 “iPhone 配置实用工具”安装配置描述文件

如果设备已更新为 iPhone OS 3.0 或更高版本，且连接在电脑上，则您可以直接在设备上安装配置描述文件。您还可以使用 “iPhone 配置实用工具”删除以前安装的描述文件。

要安装配置描述文件：

1. 使用 USB 电缆将设备与电脑连接。

   稍等片刻之后，设备会出现在 “iPhone 配置实用工具”的 “设备”列表中。
2. 选择设备，然后点按 “配置描述文件”标签。
3. 从列表中选择配置描述文件，然后点按 “安装”。
4. 在设备上，轻按 “安装”以安装描述文件。

   当您使用 USB 直接在设备上安装时，配置描述文件会自动签名和加密，然后才会传输给设备。

通过电子邮件分发配置描述文件

您可以使用电子邮件分发配置描述文件。用户通过在设备上接收电子邮件，然后轻按附件来安装描述文件。

要通过电子邮件发送配置描述文件：

1 在 “iPhone 配置实用工具”的工具栏中点按 “共享”按钮。

在出现的对话框中，选择安全选项：

a **无：**这会创建一个纯文本 .mobileconfig 文件。它可以被安装在任何设备上。文件中的某些内容晦涩难懂，以防在检查文件时被人随意偷看。

b **给配置描述文件签名：**.mobileconfig 文件在签名后，如果发生更改，则将无法由设备进行安装。某些字段晦涩难懂，以防止检查文件时被人随意偷看。安装以后，描述文件将只能被拥有相同标识符、由同一 “iPhone 配置实用工具”副本签名的描述文件更新。

c **给描述文件签名和加密描述文件：**描述文件在签名后不能更改，并且在加密所有内容后不能检查该描述文件，而只能将该描述文件安装在特定设备上。如果描述文件包含密码，则建议选中此选项。这将为您从 “设备”列表中选择的每个设备创建单独的 .mobileconfig 文件。如果设备没有出现在列表中，则说明它以前没有被连接到电脑，因此未获得加密密钥，又或者它尚未被升级到 iPhone OS 3.0 或更高版本。

2 点按 “共享”，一封新的 Mail (Mac OS X) 或 Outlook (Windows) 邮件会打开，描述文件作为未压缩的附件被添加在邮件中。文件必须是未压缩的，以便设备识别并安装描述文件。

在 Web 上分发配置描述文件

您可以通过网站分发配置描述文件。用户可以在设备上使用 Safari 将描述文件下载后进行安装。要方便地将 URL 分发给用户，请使用 SMS 进行发送。

要导出配置描述文件：

1 在 “iPhone 配置实用工具”的工具栏中点按 “导出”按钮。

在出现的对话框中，选择安全选项：

a **无：**这会创建一个纯文本 .mobileconfig 文件。它可以被安装在任何设备上。文件中的某些内容晦涩难懂，以防在检查文件时被人随意偷看，不过，您应该确定当您将文件放置在网站上时，它仅被授权用户访问。

b **给配置描述文件签名：**.mobileconfig 文件在签名后，如果发生更改，则将无法由设备进行安装。安装以后，描述文件将只能被拥有相同标识符、由同一 “iPhone 配置实用工具”副本签名的描述文件更新。描述文件中的某些信息晦涩难懂，以防在检查文件时被人随意偷看，您应该确定当您将文件放置在网站上时，它仅被授权用户访问。

c **给描述文件签名和加密描述文件：**描述文件在签名后不能更改，并且在加密所有内容后不能检查该描述文件，而只能将该描述文件安装在特定设备上。这将为您从 “设备”列表中选择的每个设备创建单独的 .mobileconfig 文件。

2 点按 “导出”，然后选择用于存储 .mobileconfig 文件的位置。

文件已经准备好被发布在网站上。请勿压缩 .mobileconfig 文件或更改其扩展名，否则设备将不能识别或安装描述文件。

用户安装已下载的配置描述文件

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）。

当用户从 Web 上下载描述文件，或者使用 Mail 打开附件时，设备会将 .mobileconfig 扩展名识别为描述文件并在用户轻按 “安装”后开始安装。

安装过程中，会要求用户输入任何必需的信息，例如未在描述文件中指定的密码，以及您指定的设置所需的其他信息。

设备还会从服务器取回 Exchange ActiveSync 策略，并将在随后的每次连接时都刷新策略，以防策略发生更改。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 （可能是因为 Exchange 服务器无法连接或者用户取消了安装过程），则用户输入的任何信息都不会保留。

用户不妨更改设置，以确定将多少天内的邮件同步到设备中，以及除收件箱外的哪些邮件文件夹需要被同步。默认值为三天和所有文件夹。用户可以在 “设置” > “邮件、通讯录、日历” > “Exchange **帐户名称**”中更改这些设置。

删除和更新配置描述文件

配置描述文件更新不会被推送给用户。请将更新后的描述文件分发给用户，以让他们安装。只要描述文件标识符匹配，并且如果已签名（被“iPhone 配置实用工具”的同一副本所签名），新的描述文件就会替换设备上的描述文件。

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。如果描述文件已签名，则它只能由 “iPhone 配置实用工具”的同一副本所签名的描述文件进行替换。新旧描述文件中的标识符必须匹配，这样更新后的描述文件才能被识别为替换文件。有关标识符的更多信息，请参阅第 30 页“通用设置”。

【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的 Exchange 帐户数据，以及与描述文件相关的 VPN 设置、证书和其他信息 （包括邮件）。

如果描述文件的 “通用设置”有效负载指定它不能被用户删除，则 “删除”按钮将不会显现。如果设置允许使用授权密码执行删除操作，则用户轻按 “删除”后将被要求输入密码。有关描述文件安全设置的更多信息，请参阅第 30 页 “通用设置”。

手动配置设备

3

本章描述如何手动配置 iPhone、 iPod touch 和 iPad。

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 （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 50 页 “安装身份和根证书”。

“请求 VPN 域”不能在设备上配置，您需要使用配置描述文件来设置它。请参阅第 33 页 “请求 VPN 域”

VPN 代理设置

对于所有配置，您都可以指定 VPN 代理。要为所有连接配置同一个代理，请轻按 “手动”并提供地址、端口以及鉴定信息 （如果需要）。要给设备提供自动代理配置文件，请轻按 “自动”并指定 PACS 文件的 URL。要指定使用 WPAD 进行自动代理配置，请轻按 “自动”。设备将查询 DHCP 和 DNS 以获得 WPAD 设置。有关 PACS 文件示例和资源，请参阅本章结尾部分的 “其他资源”。

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 鉴定，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（含有为远程访问预置的证书**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，从而只通过服务器发送要抵达 VPN 内部的服务器的通信。其他通信则直接发送到互联网。

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 登录帐户的密码。
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，从而只通过服务器发送要抵达 VPN 内部的服务器的通信。其他通信则直接发送到互联网。

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 支持的鉴定和加密。有关技术规格的信息，请参阅第 10 页 “网络安全”。有关安装证书用于鉴定的信息，请参阅第 50 页 “安装身份和根证书”。

Exchange 设置

每个设备只能配置一个 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 帐户的密码。
描述	一个识别此帐户的描述性标题。

iPhone、 iPod touch 和 iPad 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。

如果您的 Exchange 服务器监听连接的端口不是 443，请在 “服务器”栏使用格式 “exchange.example.com:portnumber”来指定端口号。

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” > “邮件、通讯录、日历” > “获取新数据”以更改设置。

要更改将多少天的邮件信息同步到设备，请前往 “设置” > “邮件、通讯录、日历”，然后选择 Exchange 帐户。除了收件箱外，您还可以选择在推送电子邮件传输中包括哪些文件夹。

要更改日历数据的设置，请前往 “设置” > “邮件、通讯录、日历” > “同步”。

LDAP 设置

iPhone、 iPod touch 和 iPad 可以在 LDAP 目录服务器上查找联络信息。要添加 LDAP 服务器，请前往 “设置” > “邮件、通讯录、日历” > “添加帐户” > “其他”。然后轻按 “添加 LDAP 帐户”。

输入 LDAP 服务器地址以及用户名称和密码 （如果需要），然后轻按 “下一步”。如果服务器可以访问并给设备提供了默认的搜索设置，则将使用该设置。

支持以下 “搜索范围”设置：

“搜索范围”设置	描述
基准	仅搜索基准对象。
一级	搜索基准对象下一级对象，但不搜索基准对象本身。
子树	搜索基准对象及其下级所有对象的整个树。

您可以为每个服务器定义多组搜索设置。

CalDAV 设置

iPhone、 iPod touch 和 iPad 与提供组别日历和日程安排的 CalDAV 日历服务器配合使用。要添加 CalDAV 服务器，请前往 “设置” > “邮件、通讯录、日历” > “添加帐户” > “其他”。然后轻按 “添加 CalDAV 帐户”。

输入 CalDAV 服务器地址以及用户名称和密码 （如果需要），然后轻按 “下一步”。与服务器建立连接后，会出现一些额外的字段，可允许您设定更多选项。

日历订阅设置

您可以添加只读日历，如项目计划表或节日。要添加日历，请前往 “设置” > “邮件、通讯录、日历” > “添加帐户” > “其他”，然后轻按 “添加已订阅的日历”。

输入 iCalendar (.ics) 文件的 URL 以及用户名称和密码 （如果需要），然后轻按“存储”。您还可以指定将日历添加到设备上时，是否删除已在日历中设定好的提醒。

除了手动添加日历订阅以外，您也可以向用户发送 webcal://URL （或指向 .ics 文件的 http:// 链接），当用户轻按该链接后，设备会主动将它添加为已订阅的日历。

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

有关所支持的格式及其他要求的更多信息，请参阅第 11 页 “证书和身份”。

证书或身份被下载到设备之后，“安装描述文件”屏幕会出现。描述会指出类型：身份或证书颁发机构。要安装证书，请轻按 “安装”。如果它是身份证书，将要求您输入证书的密码。

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

其他邮件帐户

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。请前往“设置”>“帐户”>“邮件、通讯录、日历”>“添加帐户”>“其他”。有关添加 IMAP 帐户的更多信息，请参阅《iPhone 使用手册》、《iPod touch 使用手册》或《iPad 使用手册》。

更新和删除描述文件

有关用户如何更新或删除配置描述文件的信息，请参阅第 39 页 “删除和更新配置描述文件”。

有关安装分配预置描述文件的信息，请参阅第 58 页 “部署应用程序”。

其他资源

有关由 VPN 代理设置所使用的自动代理配置文件的格式和功能的信息，请参阅以下内容：

- 代理自动配置 (PAC)，网址为 http://en.wikipedia.org/wiki/Proxy_auto-config
- “Web Proxy Autodiscovery Protocol”（Web 代理自动发现协议），网址为 http://en.wikipedia.org/wiki/Wpad
- Microsoft TechNet “Using Automatic Configuration, Automatic Proxy, and Automatic Detection”（使用自动配置、自动代理和自动检测），网址为 http://technet.microsoft.com/en-us/library/dd361918.aspx

Apple 制作了若干视频教程，可供用户在标准 Web 浏览器中观看，这些教程向用户说明如何设置并使用 iPhone、 iPod touch 和 iPad 的功能：

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

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/zh_CN/iPhone_User_Guide_CH.pdf
- 《iPod touch 使用手册》：http://manuals.info.apple.com/zh_CN/iPod_touch_3.1_User_Guide_CH.pdf
- 《iPad 使用手册》：http://manuals.info.apple.com/zh_CN/iPad_User_Guide_CH.pdf

部署 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。

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

iPhone、 iPod touch 和 iPad 每次只能将每种类型的数据 （音乐、媒体等）同步到一台电脑。例如，您可以与台式电脑同步音乐，与便携式电脑同步书签，方法是在两台电脑上对 iTunes 的同步选项进行适当设定。有关同步选项的更多信息，请参阅 “iTunes 帮助”（iTunes 打开时可从 “帮助”菜单访问）。

安装 iTunes

iTunes 使用标准的 Macintosh 安装器和 Windows 安装程序。最新版本和系统要求列表可从 www.apple.com.cn/itunes 网址下载。

有关分发 iTunes 的许可要求的信息，请参阅:
http://developer.apple.com/softwarelicensing/agreements/itunes.html

在 Windows 电脑上安装 iTunes

默认情况下，在 Windows 电脑上安装 iTunes 时，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在用户电脑上安装的组件来忽略这些组件。

使用 iTunesSetup.exe 在 Windows 上安装

如果要计划使用常规的 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。

属性	含义
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。请勿忽略 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

要静默安装 iTunes，请从 iTunesSetup.exe 中提取各个 .msi 文件，然后将这些文件推送给客户端电脑。

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，这里的 %temp% 是您的临时目录，nnn 是一个三位随机数字。在 Windows XP 上，该临时目录通常是**引导驱动器**:\Documents and Settings\ **用户** \Local Settings\temp\。在 Windows Vista 上，该临时目录通常是 \Users\ **用户** \AppData\Local\Temp\。
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 和 Apple Application Support。Apple Application Support 必须先于 iTunes 被安装。Apple Mobile Device Services (AMDS) 是配合 iPhone、iPad 或 iPod touch 使用 iTunes 所必需的。

推送 .msi 文件之前，您需要先选择要安装 iTunes 的哪些本地化版本。要执行此操作，请在 ORCA 工具中打开 .msi 文件，该工具由 Windows SDK 安装 (Orca.msi)，位于 “bin\”中。然后编辑摘要信息流并去掉不想安装的语言。（Locale ID1033 指的是英文。）此外，也可以使用 “组策略对象编辑器”将 .msi 文件的部署属性更改为 “忽略语言”。

在 Macintosh 电脑上安装 iTunes

Mac 电脑已装有 iTunes。最新版本的 iTunes 可从 www.apple.com.cn/itunes 网址获得。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

在可以使用一个新 iPhone、iPod touch 或 iPad 之前，必须先通过将它连接到正在运行 iTunes 的电脑来激活它。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 在激活设备后自动将其推出。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 delete com.apple.iTunes StoreActivationMode
     ```

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。

要验证 iTunes 是否处于仅激活模式，请选取 iTunes > “关于 iTunes”并在 iTunes 版本和版号标识符下面查找 “仅激活模式”文本。

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，然后按照这些步骤进行操作。

1 如果您要激活 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、 iPod touch 或 iPad 连接到电脑。要激活设备，电脑必须接入互联网。

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，因此如果您打算使用 iTunes 同步设备，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 Genius 建议
- 设备连接时自动同步
- 下载专辑插图
- 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
- 播放互联网广播
- 访问 iTunes Store
- 与本地网络中同时运行 iTunes 的电脑共享资料库
- 播放已标记为不良内容的 iTunes 媒体
- 播放影片
- 播放电视节目

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，如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，请参阅网址 http://docs.info.apple.com/article.html?artnum=303099-zh 上的 Apple 支持文章。

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 iTunes 注册表值的信息，请参阅网址 http://support.apple.com/kb/HT2102?viewlocale=zh_CN 上的 Apple 支持文章。

有关编辑 Windows 注册表的通用信息，请参阅网址 http://support.microsoft.com/kb/136393 上的 Microsoft 帮助和支持文章。

手动更新 iTunes 和 iPhone OS

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 OS，请按照这些步骤进行操作：

1. 在一台未关闭 iTunes 软件更新的电脑上，请使用 iTunes 来下载软件更新。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 XP 上：** **引导驱动器** :\Documents and Settings\ **用户** \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上。
4. 请告诉用户，在应用软件更新之前要先使用 iTunes 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。

使用 iTunes 来备份设备

iPhone、 iPod touch 或 iPad 和 iTunes 同步后，设备设置会自动备份到电脑。从 App Store 购买的应用程序会被拷贝到 iTunes 资料库中。

您自己开发并使用企业级分发描述文件分发给您的用户的应用程序将不会备份或传输到用户的电脑中。但设备备份将包括您的应用程序创建的任何数据文件。

可通过在 iTunes 的摘要面板中为设备选择 “加密备份”选项，以加密格式储存设备备份。文件使用 AES256 加密。该密钥会安全地储存在 iPhone OS 钥匙串中。

【重要事项】如果正在备份的设备安装了任何已加密的描述文件，则 iTunes 会要求用户启用备份加密。

部署应用程序

5

您可以将 iPhone、 iPod touch 和 iPad 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、 iPod touch 和 iPad 上运行，而无需执行任何附加步骤。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字签名。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。
- 使用您的证书给应用程序签名。
- 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 OS 开发并部署自定的应用程序，请先在网站 http://developer.apple.com/ 上注册 “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。

给应用程序签名

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，请参阅网址 http://developer.apple.com/iphone 上的 “iPhone Developer Center”（iPhone 开发者中心）。

创建分配预置描述文件

分配预置描述文件可让您创建应用程序，供用户在他们的设备上使用。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。

网址 http://developer.apple.com/iphone 上的 “Enterprise Program Portal”（企业计划门户）可以给企业委派的 “Team Agent”（团队代理）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 副本会自动安装位于以下文件夹 （在本节中定义）中的预置描述文件。如果这些文件夹不存在，请使用所示名称来创建它们。

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 会将文件拷贝到上面定义的正确位置中。

使用 “iPhone 配置实用工具”安装预置描述文件

您可以使用 “iPhone 配置实用工具”将预置描述文件安装到已连接的设备中。请按照这些步骤进行操作:

1. 在 “iPhone 配置实用工具”中，选取 “文件” > “添加到资料库”，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 配置实用工具”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 “预置描述文件”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，然后让他们按照这些步骤进行操作:

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”来安装应用程序以及位于所指定的文件夹内的所有分配预置描述文件 （在第 59 页 “使用 iTunes 安装预置描述文件”中已详述）。

使用 “iPhone 配置实用工具”安装应用程序

您可以使用 “iPhone 配置实用工具”将应用程序安装到已连接的设备中。请按照这些步骤进行操作:

1. 在 “iPhone 配置实用工具”中，选取 “文件” > “添加到资料库”，然后选择想要安装的应用程序。

   该应用程序会被添加到 “iPhone 配置实用工具”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。

停用企业级应用程序

如果您需要停用内部应用程序，您可以通过撤销用于给该分配预置描述文件签名的身份来实现。该应用程序将不再能够安装，如果已经安装，它将不再能够打开。

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/iphone/

Cisco VPN 服务器配置

使用这些指导将 Cisco VPN 服务器配置成配合 iPhone、iPod touch 和 iPad 工作。

支持的 Cisco 平台

iPhone OS 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）。 iPhone OS 也支持 IOS 版本为 12.4(15)T 或更高版本的 Cisco IOS VPN 路由器。 VPN 3000 系列集中器不支持 iPhone 的 VPN 功能。

鉴定方式

iPhone OS 支持以下鉴定方式：

- 预共享密钥 IPSec 鉴定与通过 xauth 进行的用户鉴定
- 客户端和服务器证书，用于 IPSec 鉴定与通过 xauth 进行的用户鉴定 （用户鉴定为可选）
- 混合鉴定，为了进行 IPSec 鉴定，服务器提供证书，而客户端提供预共享密钥；必须通过 xauth 进行用户鉴定。
- 用户鉴定是通过 xauth 提供的，包括以下鉴定方式：
  - 用户名称和密码
  - RSA SecurID
  - CryptoCard

鉴定组别

Cisco Unity 协议基于一组共同的鉴定及其他参数，使用鉴定组别将用户组合在一起。您应该为 iPhone OS 设备用户创建鉴定组别。对于预共享密钥鉴定和混合鉴定，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。

使用证书鉴定时，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体备用名称 (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 （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。
- 给服务器的证书签名的 CA 证书应该安装在设备上。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，请确定给客户端证书签名的被信任的 CA 证书已安装在 VPN 服务器上。
- 证书和证书颁发机构必须是有效的 （例如，未过期）。
- 不支持通过服务器发送证书链，必须关掉此功能。
- 使用基于证书的鉴定时，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 63 页 “鉴定组别”。

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”适用于预共享密钥鉴定和混合鉴定，“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 组别：**预共享密钥鉴定和混合鉴定需要 Group 2。对于证书鉴定，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 阶段 2，如果使用 PFS，则 Diffie-Hellman 组别必须与用于 IKE 阶段 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：**受支持，需要时可以启用。（不支持 IPSec over TCP）。
- **负载均衡：**受支持，需要时可以启用。
- **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 配置所假定的有些路由可能会被忽略。要避免发生这种情况，请确定路由表包含所有必要的路由，并且验证子网地址可以访问，然后再进行部署。

其他支持的功能

iPhone、 iPod touch 和 iPad 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。要着手开始，请使用“iPhone 配置实用工具”创建一个您能够使用此附录中的信息进行修改的框架文件。

本文稿使用到术语**有效负载** (payload) 和**描述文件** (profile)。描述文件是一个完整文件，用于在 iPhone、 iPod touch 或 iPad 上配置某些（一个或多个）设置。有效负载是描述文件的单个组件。

根层次

在根层次上，配置文件是一个字典，带有以下键 / 值对：

键	值
PayloadVersion	数字（必需）。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（必需）。这通常是经合成后产生的一个唯一的标识符字符串。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（必需）。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（必需）。按照惯例，此值是用圆点分隔的字符串（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匹配，则描述文件会覆盖它（而不是被添加）。
PayloadDisplayName	字符串（必需）。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。

键	值
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。此字符串应该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。
PayloadRemovalDisallowed	布尔值（可选）。默认为“No”。设定后，用户将无法删除描述文件。只有当描述文件的标识符匹配且由同一颁发机构签名时，拥有此设定的描述文件才可以通过 USB 或 Web/ 电子邮件进行更新。如果提供了删除密码，则描述文件可以通过指定密码来删除。 对于已签名且已加密的描述文件，在普通视图中拥有此锁定位没有影响，因为描述文件不能被更改且此设置也会显示在设备上。

有效负载内容

PayloadContent 数组是一个字典数组，每个字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，此数组中的每个字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（必需）。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（必需）。这通常是经合成后产生的一个唯一的标识符字符串。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（必需）。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（必需）。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（必需）。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。

描述文件删除密码有效负载

“删除密码”有效负载是由 PayloadType 的 com.apple.profileRemovalPassword 值指定的。其目的是对允许用户从设备上删除配置描述文件的密码进行编码。如果此有效负载存在且已设定了密码值，则当用户轻按描述文件的 “删除”按钮时，设备将要求用户输入该密码。此有效负载同描述文件的其余内容一起被加密。

键	值
RemovalPassword	字符串 （可选）。指定描述文件的删除密码。

密码策略有效负载

“密码策略”有效负载是由 PayloadType 的 com.apple.mobiledevice.passwordpolicy 值指定的。此有效负载类型的存在，会提示设备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（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]。指定允许在设备的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”。指定在系统锁定设备之前，设备可以闲置 （没有被用户解锁）的分钟数。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，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 自变量。
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。
pinHistory	数字 （可选）。当用户更改密码时，该密码必须不同于历史记录中最近的 N 个条目。最小值为 1，最大值为 50。

键	值
manualFetchingWhenRoaming	布尔值（可选）。设定后，所有推送操作在漫游时都将被停用。用户必须手动获取新数据。
maxGracePeriod	数字（可选）。将电话解锁而不输入密码的最长宽限期（以分钟为单位）。默认为 0，也就是没有宽限期，这要求立即输入密码。

电子邮件有效负载

电子邮件有效负载是由 PayloadType 的 com.apple.mail.managed 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。在已发出邮件中和其他地方会出现此用户名称。
EmailAccountType	字符串（必需）。允许的值是 EmailTypePOP 和 EmailTypeIMAP。定义用于该帐户的协议。
EmailAddress	字符串（必需）。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（必需）。指定收到的邮件的鉴定方案。允许的值是 EmailAuthPassword 和 EmailAuthNone。
IncomingMailServerHostName	字符串（必需）。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 进行鉴定。
IncomingMailServerUsername	字符串（必需）。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鉴定，安装描述文件过程中，设备将提示输入此字符串。
IncomingPassword	字符串（可选）。收件服务器的密码。仅配合已加密的描述文件使用。
OutgoingPassword	字符串（可选）。发件服务器的密码。仅配合已加密的描述文件使用。
OutgoingPasswwordSameAsIncomingPassword	布尔值（可选）。设定后，将只提示用户输入密码一次，它将被用于发送邮件和接收邮件。
OutgoingMailServerAuthentication	字符串（必需）。指定发出的邮件的鉴定方案。允许的值是 EmailAuthPassword 和 EmailAuthNone。
OutgoingMailServerHostName	字符串（必需）。指定发件服务器主机名称（或 IP 地址）。

键	值
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 进行鉴定。
OutgoingMailServerUsername	字符串 （必需）。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鉴定，安装描述文件过程中，设备会提示输入此字符串。

Web Clip 有效负载

Web Clip 有效负载是由 PayloadType 的 com.apple.webClip.managed 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
URL	字符串 （必需）。点按 Web Clip 时， Web Clip 应该打开的 URL。该 URL 必须以 HTTP 或 HTTPS 开头，否则它将不能工作。
Label	字符串 （必需）。显示在主屏幕上的 Web Clip 的名称。
Icon	数据 （可选）。要显示在主屏幕上的 PNG 图标。其大小应该为 59 x 60 像素。如果不指定，将显示白色方框。
IsRemovable	布尔值 （可选）。如果设定为 “No”，则用户不能删除 Web Clip，但如果删除描述文件，则它将被删除。

限制有效负载

“限制”有效负载是由 com.apple.applicationaccess 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
allowAppInstallation	布尔值 （可选）。当它为 “FALSE”时， App Store 会被停用并且其图标会从主屏幕去掉。用户将无法安装或更新他们的应用程序。
allowCamera	布尔值 （可选）。当它为 “FALSE”时，相机会被完全停用并且其图标会从主屏幕去掉。用户将无法拍照。
allowExplicitContent	布尔值 （可选）。当它为 “FALSE”时，从 iTunes Store 购买的不良音乐或视频内容会被隐藏。当通过 iTunes Store 销售不良内容时，内容提供商 （如唱片公司）会将它们标记为不良内容。
allowScreenShot	布尔值 （可选）。当它为 “FALSE”时，用户将无法存储显示屏的屏幕快照。
allowYouTube	布尔值 （可选）。当它为 “FALSE”时， YouTube 应用程序会被停用并且其图标会从主屏幕去掉。

键	值
allowiTunes	布尔值（可选）。当它为“FALSE”时，iTunes Music Store 会被停用并且其图标会从主屏幕去掉。用户将不能试听、购买或下载内容。
allowSafari	布尔值（可选）。当它为“FALSE”时，Safari Web 浏览器应用程序会被停用并且其图标会从主屏幕去掉。这同样也阻止了用户打开 Web Clip。

LDAP 有效负载

LDAP 有效负载是由 PayloadType 的 com.apple.ldap.account 值指定的。从 LDAP 帐户到 LDAPSearchSettings 存在一对多的关系。可以将 LDAP 看作树。每个 SearchSettings 对象都表示树中的一个从其开始搜索的节点，以及搜索范围（节点、子节点的下一级节点、子节点的所有下级节点）。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
LDAPAccountDescription	字符串（可选）。帐户的描述。
LDAPAccountHostName	字符串（必需）。主机。
LDAPAccountUseSSL	布尔值（必需）。是否要使用 SSL。
LDAPAccountUserName	字符串（可选）。用户名称。
LDAPAccountPassword	字符串（可选）。仅配合已加密的描述文件使用。
LDAPSearchSettings	顶层容器对象。一个帐户可以有这些值中的多个值。应该至少有一个帐户的值是有效的。
LDAPSearchSettingDescription	字符串（可选）。此搜索设置的描述。
LDAPSearchSettingSearchBase	字符串（必需）。从概念上来说，指的是到节点的路径，以从“ou=people,o=example corp”开始搜索
LDAPSearchSettingScope	字符串（必需）。定义要在搜索中使用的递归式。 可以是以下 3 个值中的一个： LDAPSearchSettingScopeBase：只是由 SearchBase 指向的最近的节点 LDAPSearchSettingScopeOneLevel：节点加上与其最接近的子节点。 LDAPSearchSettingScopeSubtree：节点加上所有子节点，不论深度如何。

CalDAV 有效负载

CalDAV 有效负载是由 PayloadType 的 com.apple.caldav.account 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
CalDAVAccountDescription	字符串 （可选）。帐户的描述。
CalDAVHostName	字符串 （必需）。服务器地址
CalDAVUsername	字符串 （必需）。用户的登录名称。
CalDAVPassword	字符串 （可选）。用户的密码
CalDAVUseSSL	布尔值 （必需）。是否要使用 SSL。
CalDAVPort	数字 （可选）。要连接到服务器的端口。
CalDAVPrincipalURL	字符串 （可选）。指向用户日历的基本 URL。

日历订阅有效负载

CalSub 有效负载是由 PayloadType 的 com.apple.subscribedcalendar.account 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
SubCalAccountDescription	字符串 （可选）。帐户的描述。
SubCalAccountHostName	字符串 （必需）。服务器地址。
SubCalAccountUsername	字符串 （可选）。用户的登录名称
SubCalAccountPassword	字符串 （可选）。用户的密码。
SubCalAccountUseSSL	布尔值 （必需）。是否要使用 SSL。

SCEP 有效负载

SCEP （简单证书注册协议）有效负载是由 PayloadType 的 com.apple.encrypted-profile-service 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
URL	字符串 （必需）。
名称	字符串 （可选）。可被 SCEP 服务器理解的任何字符串。例如，它可能是诸如 example.org 的域名。如果证书颁发机构有多个 CA 证书，此字段可用于判别需要哪一个。
主体	数组 （可选）。表示为 OID 数组和值的 X.500 名称的描述。例如， /C=US/O=Apple Inc./CN=foo/1.2.5.3=bar，将被转换为： [[[“C”,“US”]], [[“O”,“Apple Inc.”]], ..., [[“1.2.5.3”,“bar”]]] OID 可被表示为带圆点的数字，且有以下缩写：C、 L、 ST、 O、 OU、 CN （国家 / 地区、所在地、州 / 省、组织、组织单位、通用名称）。

键	值
口令	字符串 （可选）。预共享密钥。
Keysize	数字 （可选）。 keysize 以位为单位，可以是 1024 或 2048。
Key Type	字符串 （可选）。当前始终为 “RSA”。
Key Usage	数字 （可选）。表示密钥用途的位掩码。 1 表示签名， 4 表示加密， 5 表示签名和加密。某些 CA （如 Windows CA）仅支持加密或签名，而不是同时支持两者。

SubjectAltName 字典键

SCEP 有效负载可以指定一个可选的 SubjectAltName 字典，以提供 CA 颁发证书所需的值。您可以给每个键指定单个字符串或字符串数组。指定的值取决于所使用的 CA，但可能会包括 DNS 名称、 URL 或电子邮件值。有关示例，请参阅第 78 页“阶段 3 SCEP 规格的服务器响应示例”。

GetCACaps 字典键

如果您添加一个带有 GetCACaps 键的字典，设备会使用您提供的字符串作为有关您 CA 的功能的权威的信息源。否则，设备会向 CA 查询 GetCACaps 并使用响应中获得的应答。如果 CA 没有响应，设备会默认为 GET 3DES 和 SHA-1 请求。

APN 有效负载

APN （访问点名称）有效负载是由 PayloadType 的 com.apple.apn.managed 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	字典 （必需）。此字典含有两组键 / 值对。
DefaultsDomainName	字符串 （必需）。唯一允许的值是 com.apple.managedCarrier。
apns	数组 （必需）。此数组含有任意个数的字典，每个字典描述一个 APN 配置，它们包含以下键 / 值对。
apn	字符串 （必需）。此字符串指定访问点名称。
username	字符串 （必需）。此字符串指定此 APN 的用户名称。如果缺少此值，安装描述文件过程中，设备会提示输入此值。
password	数据 （可选）。此数据表示此 APN 的用户密码。用于迷惑他人，已编码。如果有效负载中缺少此值，安装描述文件过程中，设备会提示输入此值。
proxy	字符串 （可选）。 APN 代理的 IP 地址或 URL。
proxyPort	数字 （可选）。 APN 代理的端口号。

Exchange 有效负载

Exchange 有效负载是由 PayloadType 的 com.apple.eas.account 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（必需）。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（必需）。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 进行鉴定。
UserName	字符串（必需）。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。
密码	字符串（可选）。帐户的密码。仅配合已加密的描述文件使用。
Certificate	可选。适用于允许通过证书（使用 NSData 气泡格式的 .p12 身份证书）进行鉴定的帐户。
CertificateName	字符串（可选）。指定证书的名称或描述。
CertificatePassword	可选。适用于 p12 身份证书的必需密码。仅配合已加密的描述文件使用。

VPN 有效负载

VPN 有效负载是由 PayloadType 的 com.apple.vpn.managed 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“TRUE”，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”，分别表示 L2TP、 PPTP 和 Cisco IPSec。

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

PPP 字典键

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 “FALSE”时才可见。用于 L2TP 和 PPTP。
TokenCard	布尔值。是否使用令牌卡（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 下面的讨论。用于 PPTP。
CCPMPPE128Enabled	布尔值。请参阅 CCPEnabled 下面的讨论。用于 PPTP。
CCPEnabled	布尔值。启用加密连接。如果此键和 CCPMPPE40Enabled 为 “TRUE”，则表示自动加密级别；如果此键和 CCPMPPE128Enabled 为 “TRUE”，则表示最高加密级别。如果未使用加密，则没有一个 CCP 键为 “TRUE”。用于 PPTP。

IPSec 字典键

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 “混合鉴定”，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。

键	值
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 PayloadType 的 com.apple.wifi.managed 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。
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”赋一个布尔值。
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功能完全匹配。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”。
密码	字符串（可选）。缺少密码不会阻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 字典。

EAPClientConfiguration 字典

除了标准加密类型之外，还可能会通过 “EAPClientConfiguration”密钥为给定的网络指定一个企业级描述文件。如果存在的话，它的值就是含有以下键的字典。

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。进行鉴定时，用户可以输入此信息。
AcceptEAPTypes	整数值数组。以下这些 EAP 类型会被接受: 13 = TLS 17 = LEAP 21 = TTLS 25 = PEAP 43 = EAP-FAST

键	值
PayloadCertificateAnchorUUID	字符串数组 （可选）。识别被信任进行此鉴定的证书。每个条目都必须包含证书有效负载的 UUID。使用此键可阻止设备询问用户是否信任所列出的证书。 如果指定了此属性，则动态信任 （证书对话）会被停用，除非 TLSAllowTrustExceptions 也被指定了值 “TRUE”。
TLSTrustedServerNames	字符串值数组 （可选）。这是能够被接受的服务器证书通用名称的列表。您可以使用通配符来指定名称，如 wpa.*.example.com。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，并避免动态信任的证书。 如果指定了此属性，则动态信任 （证书对话）会被停用，除非 TLSAllowTrustExceptions 也被指定了值 “TRUE”。
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，则鉴定失败。请参阅上文的 PayloadCertificateAnchorUUID 和 TLSTrustedNames。 此属性的默认值是 “TRUE”，除非提供了 PayloadCertificateAnchorUUID 或 TLSTrustedServerNames （这种情况下默认值是 “FALSE”）。
TTLSInnerAuthentication	字符串 （可选）。这是 TTLS 模块所使用的内部鉴定。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鉴定用户的名称。

EAP-Fast 支持

在 EAPClientConfiguration 字典中， 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”，则鉴定步骤与 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：它不会鉴定服务器的身份，所以连接会受中间人攻击的伤害。

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。

配置描述文件示例

本部分包括了阐述无线注册和配置阶段的描述文件示例。这些内容只是摘要，而您的实际要求将与示例不尽相同。有关语法帮助，请参阅本附录前文提供的详细信息。有关每个阶段的描述，请参阅第 21 页 “无线注册和配置”。

阶段 1 服务器响应示例

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple Inc//DTD PLIST 1.0//EN" "http://
     www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
    <key>PayloadContent</key>
    <dict>
        <key>URL</key>
        <string>https://profileserver.example.com/iphone</string>
        <key>DeviceAttributes</key>
        <array>
                <string>UDID</string>
  <string>IMEI</string>
  <string>ICCID</string>
  <string>VERSION</string>
  <string>PRODUCT</string>
        </array>
    <key>Challenge</key>
     <string>optional challenge</string>
     or
     <data>base64-encoded</data>
    </dict>
```

```
    <key>PayloadOrganization</key>
    <string>Example Inc.</string>
    <key>PayloadDisplayName</key>
    <string>Profile Service</string>
    <key>PayloadVersion</key>
    <integer>1</integer>
    <key>PayloadUUID</key>
    <string>fdb376e5-b5bb-4d8c-829e-e90865f990c9</string>
    <key>PayloadIdentifier</key>
    <string>com.example.mobileconfig.profile-service</string>
    <key>PayloadDescription</key>
    <string>Enter device into the Example Inc encrypted profile service</
     string>
    <key>PayloadType</key>
     <string>Profile Service</string>
</dict>
</plist>
```

阶段 2 设备响应示例

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/
     DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
    <key>UDID</key>
    <string></string>
    <key>VERSION</key>
    <string>7A182</string>
    <key>MAC_ADDRESS_EN0</key>
    <string>00:00:00:00:00:00</string>
    <key>CHALLENGE</key>
either:
    <string>String</string>
or:
    <data>"base64 encoded data"</data>
</dict>
</plist>
```

阶段 3 SCEP 规格的服务器响应示例

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple Inc//DTD PLIST 1.0//EN" "http://
     www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
  <dict>
    <key>PayloadVersion</key>
    <integer>1</integer>
    <key>PayloadUUID</key>
```

```
<string>Ignored</string>
<key>PayloadType</key>
<string>Configuration</string>
<key>PayloadIdentifier</key>
<string>Ignored</string>
<key>PayloadContent</key>
<array>
  <dict>
    <key>PayloadContent</key>
    <dict>
      <key>URL</key>
      <string>https://scep.example.com/scep</string>
      <key>Name</key>
      <string>EnrollmentCAInstance</string>
      <key>Subject</key>
      <array>
        <array>
          <array>
            <string>O</string>
            <string>Example, Inc.</string>
          </array>
        </array>
        <array>
          <array>
            <string>CN</string>
            <string>User Device Cert</string>
          </array>
        </array>
      </array>
      <key>Challenge</key>
      <string>...</string>
      <key>Keysize</key>
      <integer>1024</integer>
      <key>Key Type</key>
      <string>RSA</string>
      <key>Key Usage</key>
      <integer>5</integer>
    </dict>
    <key>PayloadDescription</key>
    <string>Provides device encryption identity</string>
    <key>PayloadUUID</key>
    <string>fd8a6b9e-0fed-406f-9571-8ec98722b713</string>
    <key>PayloadType</key>
    <string>com.apple.security.scep</string>
    <key>PayloadDisplayName</key>
    <string>Encryption Identity</string>
    <key>PayloadVersion</key>
```

```
        <integer>1</integer>
        <key>PayloadOrganization</key>
        <string>Example, Inc.</string>
        <key>PayloadIdentifier</key>
        <string>com.example.profileservice.scep</string>
      </dict>
    </array>
  </dict>
</plist>
```

阶段 4 设备响应示例

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/
     DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
    <key>UDID</key>
    <string></string>
    <key>VERSION</key>
    <string>7A182</string>
    <key>MAC_ADDRESS_EN0</key>
    <string>00:00:00:00:00:00</string>
</dict>
</plist>
```

示例脚本

本附录提供了用于 iPhone OS 部署任务的示例脚本。

本部分中的脚本应做适当修改以适应您的需要和配置。

“iPhone 配置实用工具”的 C# 示例脚本

此示例脚本演示如何使用 “iPhone 配置实用工具 （Windows 版）”创建配置文件。

```
using System;
using Com.Apple.iPCUScripting;

public class TestScript : IScript
  {
  private IApplication _host;

  public TestScript()
     {
     }

  public void main(IApplication inHost)
     {
     _host = inHost;

     string msg = string.Format("# of config profiles : {0}",
     _host.ConfigurationProfiles.Count);
     Console.WriteLine(msg);

     IConfigurationProfile profile = _host.AddConfigurationProfile();
     profile.Name = "Profile Via Script";
     profile.Identifier = "com.example.configviascript";
     profile.Organization = "Example Org";
     profile.Description = "This is a configuration profile created via the
     new scripting feature in iPCU";

     // passcode
     IPasscodePayload passcodePayload = profile.AddPasscodePayload();
     passcodePayload.PasscodeRequired = true;
     passcodePayload.AllowSimple = true;
```

```
    // restrictions
    IRestrictionsPayload restrictionsPayload =
    profile.AddRestrictionsPayload();
    restrictionsPayload.AllowYouTube = false;

    // wi-fi
    IWiFiPayload wifiPayload = profile.AddWiFiPayload();
    wifiPayload.ServiceSetIdentifier = "Example Wi-Fi";
    wifiPayload.EncryptionType = WirelessEncryptionType.WPA;
    wifiPayload.Password = "password";

    wifiPayload = profile.AddWiFiPayload();
    profile.RemoveWiFiPayload(wifiPayload);

    // vpn
    IVPNPayload vpnPayload = profile.AddVPNPayload();
    vpnPayload.ConnectionName = "Example VPN Connection";

    vpnPayload = profile.AddVPNPayload();
    profile.RemoveVPNPayload(vpnPayload);

    // email
    IEmailPayload emailPayload = profile.AddEmailPayload();
    emailPayload.AccountDescription = "Email Account 1 Via Scripting";

    emailPayload = profile.AddEmailPayload();
    emailPayload.AccountDescription = "Email Account 2 Via Scripting";

    // exchange
    IExchangePayload exchangePayload = profile.AddExchangePayload();
    exchangePayload.AccountName = "ExchangePayloadAccount";

    // ldap
    ILDAPPayload ldapPayload = profile.AddLDAPPayload();
    ldapPayload.Description = "LDAP Account 1 Via Scripting";

    ldapPayload = profile.AddLDAPPayload();
    ldapPayload.Description = "LDAP Account 2 Via Scripting";

    // webclip
    IWebClipPayload wcPayload = profile.AddWebClipPayload();
    wcPayload.Label = "Web Clip 1 Via Scripting";

    wcPayload = profile.AddWebClipPayload();
    wcPayload.Label = "Web Clip 2 Via Scripting";

    }
}
```

“iPhone 配置实用工具”的 AppleScript 示例

此示例脚本演示如何使用 “iPhone 配置实用工具 （Mac OS X 版）”创建配置文件。

```
tell application "iPhone Configuration Utility"
  log (count of every configuration profile)
  set theProfile to make new configuration profile with properties
     {displayed name:"Profile Via Script", profile
     identifier:"com.example.configviascript", organization:"Example Org.",
     account description:"This is a configuration profile created via
     AppleScript"}
  tell theProfile
     make new passcode payload with properties {passcode required:true,
     simple value allowed:true}
     make new restrictions payload with properties {YouTube allowed:false}
     make new WiFi payload with properties {service set identifier:"Example
     Wi-Fi", security type:WPA, password:"password"}
     set theWiFiPayload to make new WiFi payload
     delete theWiFiPayload
     make new VPN payload with properties {connection name:"Example VPN
     Connection"}
     set theVPNPayload to make new VPN payload
     delete theVPNPayload
     make new email payload with properties {account description:"Email
     Account 1 Via Scripting"}
     make new email payload with properties {account description:"Email
     Account 2 Via Scripting"}
     make new Exchange ActiveSync payload with properties {account
     name:"ExchangePayloadAccount"}
     make new LDAP payload with properties {account description:"LDAP
     Account 1 Via Scripting"}
     make new LDAP payload with properties {account description:"LDAP
     Account 2 Via Scripting"}
     make new web clip payload with properties {label:"Web Clip Account 1
     Via Scripting"}
     make new web clip payload with properties {label:"Web Clip Account 2
     Via Scripting"}
  end tell
end tell
```