概述

在 iOS 上管理设备和企业数据

概述

目录

全球各地的企业都在通过 iPhone 和 iPad 助他们的员工一臂之力。

要实现成功的移动策略，关键在于平衡 IT 控制与用户权责。用户可用自己的 app 和内容对 iOS 设备实施个性化设置，从而更有效地管理和保护自己的设备，全面提升参与度和工作效率。这得益于 Apple 的管理框架，可提供各种智能方式，单独管理企业数据和 app，将工作数据和个人数据无缝分隔。此外，用户了解其设备的管理方式并相信自己的隐私权得到了保护。

本文稿针对如何在实现基本 IT 控制的同时为用户提供工作所需的最佳工具给予了指导。本文稿是对《iOS 部署参考》的补充，后者是关于部署和管理企业 iOS 设备的综合在线技术参考。

要参阅《iOS 部署参考》，请访问：help.apple.com/deployment/ios?lang=zh-cn。

基本管理功能

借助 iOS，你可以通过一系列内置技术简化 iPhone 和 iPad 部署，这包括简化帐户设置、配置策略、分发 app，以及远程应用设备限制。

Apple 的简易框架

采用 Apple 在 iOS、macOS、tvOS 中内置的统一管理框架，IT 不仅可以配置和更新设置、部署应用程序、监控合规性、查询设备，还能远程擦除或锁定设备。该框架支持企业拥有、用户拥有以及个人拥有的设备。Apple 在 iOS 中内置的统一管理框架是移动设备管理的基础。这个框架内置于 iOS，支持企业以少量干预的方式管理必须管理的内容，而非仅仅局限于锁定功能或停用功能。因此，Apple 在 iOS 中内置的统一管理框架允许通过第三方移动设备管理 (MDM) 解决方案实现对设备、app 和数据的精确控制。最重要的是，你可以获得所需的控制权，而不会降低用户体验或损害员工隐私。

市场中的其他设备管理方法可能使用不同的名称描述 MDM 功能，例如企业移动管理 (EMM) 或移动应用程序管理 (MAM)。这些解决方案拥有相同的目标，即以无线方式管理贵企业的设备和企业数据。由于 Apple 的管理框架内置于 iOS，因此你无需从 MDM 解决方案提供商那里获取另外的代理应用程序。

分隔管理工作和个人数据

无论贵企业是支持用户拥有的设备还是公司拥有的设备，你都可以在实现 IT 管理目标的同时让用户在工作中保持优异的工作效率。将工作数据和个人数据分开管理，而用户体验始终完整一致。这样一来，最热门的效率类 app 就能够与你的企业 app 同时保留在用户设备上，让员工更自由地开展工作。iOS 实现这一目标而无需使用容器等第三方解决方案，因为那会影响用户体验，给用户带来不便。

了解不同的管理模式

其他平台往往会通过构建容器来解决问题，而此类问题在 iOS 上并不存在。一些容器使用双重身份策略，也就是在同一个设备上创建两个独立的运行环境。还有其他一些容器则主要通过基于代码的集成或 app 封装解决方案自行封装 app。所有这些方法都会给用户的工作效率带来不利影响，不论是登录和退出多个工作空间，还是对专有代码的更多依赖，通常都会造成 app 与操作系统更新不兼容。

不再使用容器的企业会发现，iOS 中的原生管理控制可以为用户提供优化的个人体验，并帮助他们提高工作效率。你可以使用策略控制在后台无缝管理数据流，而不会妨碍用户使用自己的设备完成工作任务和个人活动。

管理企业数据

有了 iOS，你无需锁定你的设备。关键技术会控制企业数据在 app 间的流动，并防止数据泄露到用户的个人 app 或云服务中。

托管内容

托管内容涵盖 App Store app 以及定制内部 app、帐户、图书和域的安装、配置、管理和移除。

- 托管 **app**。使用 MDM 安装的 app 称为托管 app。它们可以是来自 App Store 的免费或付费 app，也可以是定制内部 app，所有这些 app 都可以使用 MDM 以无线方式安装。托管 app 通常包含敏感信息，可控制程度高于用户下载的 app。MDM 服务器可以根据需要删除托管 app 及其相关数据，或指定在删除 MDM 描述文件时是否删除 app。此外，MDM 服务器还可以防止托管 app 数据备份到 iTunes 和 iCloud。
- 托管帐户。MDM 可自动设置用户的邮件和其他帐户，帮助他们更快开始工作。根据具体的 MDM 解决方案提供商以及与内部系统的集成情况，帐户有效负载还可以预先填充用户的名称、邮件地址以及用于认证和签名的证书标识 (如果适用)。MDM 可以配置以下类型的帐户：IMAP/POP、CalDAV、订阅的日历、CardDAV、Exchange ActiveSync 和 LDAP。
- 托管图书。使用 MDM，图书、ePub 图书和 PDF 文稿可以自动推送到用户设备，方便员工随时获取所需内容。托管图书只能与其他托管 app 共享，或者使用托管帐户通过电子邮件发送。当不再需要资料时，可以远程将其删除。
- 托管域。通过 Safari 浏览器下载的文稿，如果是源自托管域，则会被视为托管文稿。可以托管特定 URL 和子域。例如，如果用户通过托管域下载 PDF 文稿，该域会要求 PDF 符合所有托管文稿设置。域名后面的路径通过默认方式管理。

托管分发

你可通过托管分发使用 MDM 解决方案或 Apple Configurator 2 来管理从 Apple 商务管理购买的 app 和图书。要启用托管分发，你需要先使用安全令牌将 MDM 解决方案关联到 Apple 商务管理帐户。一旦将你的 MDM 服务器连接到 Apple 商务管理，便可直接将 app 分配到设备，甚至无需用户提供 Apple ID。当 app 准备好安装到设备上时，系统会提示用户。如果设备受到监管，app 将以静默方式推送至该设备，而不会提示用户。

通过 MDM 解决方案保持对 app 的完全控制，直接将 app 分配到设备。

托管 App 配置

通过托管 app 配置，MDM 使用原生 iOS 管理框架在部署期间或之后对 app 进行配置。此框架可以帮助开发者识别当 app 作为托管 app 安装时应实施的配置设置。对于按照这种方式配置的 app，员工可以立即开始使用，而无需自定义设置。IT 可以确保 app 中的企业数据以安全方式处理，无需专用 SDK 或 app 封装。

App 开发者可以通过使用托管 app 配置实现诸多功能，例如 app 配置、阻止 app 备份、禁用屏幕截图功能，以及远程擦除 app。

AppConfig 社区专注于提供与移动操作系统中原生功能相关的工具和最佳做法。该社区的领先 MDM 解决方案提供商建立了标准模式，供所有 app 开发者用于支持托管 app 配置。通过启用更为统一、开放且简洁的方法来配置和保护移动 app，该社区有助于提高商务领域的移动设备普及率。

要了解有关 AppConfig 社区的更多信息，请访问：www.appconfig.org。

托管数据流

MDM 解决方案提供特定功能，可实现企业数据的精细化管理，防止数据泄露到用户的个人 app 或云服务中。

保护企业数据，只有由 MDM 安装和管理的 app 可以打开此工作文件。

- **托管打开方式。**打开方式管理通过一组限制来防止托管源中的附件或文稿在非托管目标位置中被打开，反之亦然。

  例如，你可以防止企业托管邮箱帐户中的机密电子邮件附件在任何用户的个人 app 中打开。只有由 MDM 安装和管理的 app 才能打开此工作文稿。用户的非托管个人 app 不会显示在可打开附件的 app 列表中。除托管 app 之外，帐户、图书、域以及一些扩展功能，也需要遵守托管打开方式限制。

- **托管扩展。**借助 app 扩展，第三方开发者可以将功能扩展至其他 app 或 iOS 内置的关键系统 (如通知中心)，在 app 之间实现全新的业务流程。使用托管打开方式可以防止非托管扩展功能与托管 app 进行交互。以下示例展示了不同的扩展功能类型：

  – **“文稿提供者”扩展功能**允许效率类 app 通过各种云服务打开文稿，无需创建不必要的副本。

  – **“操作”扩展功能**允许用户在其他 app 的环境中操作或查看内容。例如，用户可以使用某项操作直接在 Safari 浏览器中翻译另一语言的文本。

  – **“自定义键盘”扩展功能**可提供除 iOS 内置键盘以外的键盘。托管打开方式能够防止未经授权的键盘出现在你的企业 app 中。

  – **“今天”扩展功能**也称为 Widget，用于在通知中心的“今天”视图中提供摘要信息。借助这种方式，用户只需通过简单互动，即可进入完整 app 查看更多信息，是从 app 中即时获取最新信息的绝佳途径。

  – **“共享”扩展功能**可让用户以便捷的方式与其他实体分享内容，例如社交分享网站或上传服务。例如，在包含“分享”按钮的 app 中，用户可以选择代表社交分享网站的“分享”扩展功能，然后用它发布评论或其他内容。

灵活的管理选项

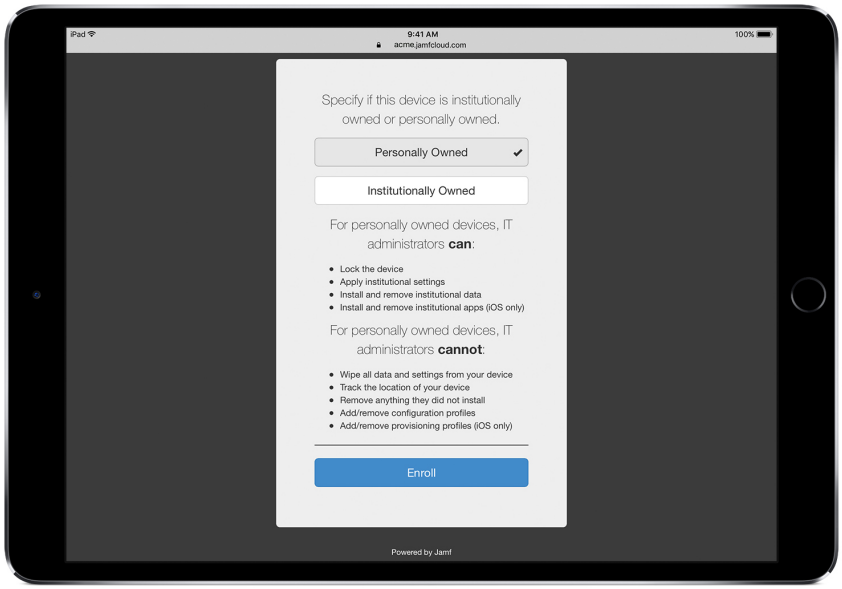
Apple 在 iOS 中内置的统一管理框架十分灵活，帮助你管理企业中用户拥有的设备和公司拥有的设备时，同时兼顾两者的需求。通过在 iOS 中应用第三方 MDM 解决方案，你可以确保设备管理选项，无论是应用高度开放的方法，还是精确掌控，都能按需实现，流畅无间。

所有权模式

根据你企业的设备所有权模式，你可按照不同的方式管理设备和 app。企业常用的两种 iOS 设备所有权模式是用户拥有和公司拥有。

用户拥有的设备

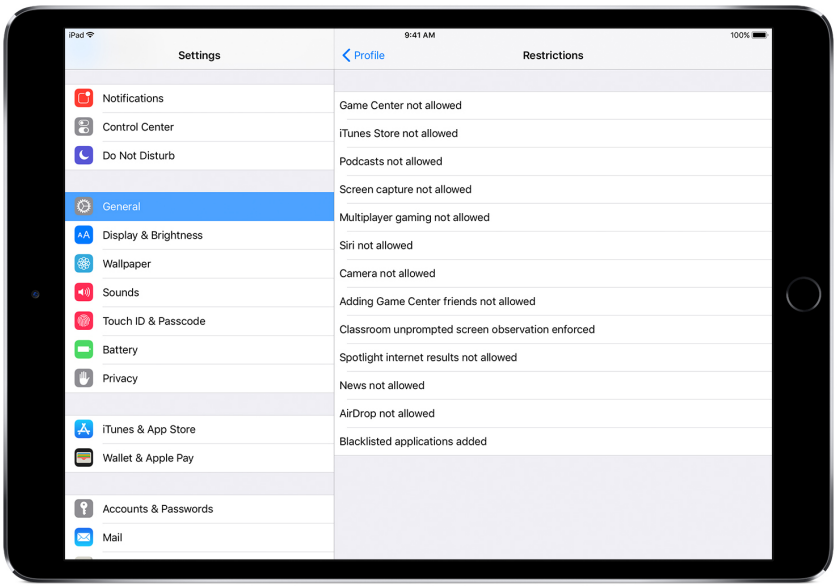
采用用户拥有的部署模式时，iOS 支持用户执行个性化设置，允许用户清楚了解设备配置方式，还可以确保企业无法访问用户的个人数据。



第三方 MDM 解决方案通常会为员工提供直观易用的界面，这样他们在注册时会更愿意选择加入。*

*屏幕图片由 Jamf 提供。

- **执行和取消注册。**当设备是由用户购买并进行设置 (通常称为“BYOD”) 时，你仍然可以提供对企业服务的访问权限，例如 Wi-Fi、邮件和日历。用户只需注册加入企业的 MDM 解决方案即可。当用户在 iOS 设备上首次注册加入 MDM 时，系统会给他们提供相关信息，告诉他们 MDM 服务器可访问其设备上的哪些信息，以及将要配置哪些功能。这样可以让用户清楚了解托管内容，让你与用户之间建立充分的信任。务必让用户知晓，如果他们无法接受这种管理方式，可随时将管理描述文件从设备中删除，从而取消注册。当他们这么做时，MDM 安装的所有公司帐户和 app 都将被移除。
- **高度透明。**用户注册 MDM 之后，员工可以通过“设置”轻松查看处于托管状态的 app、图书和帐户，还可以了解实施了哪些限制。由 MDM 安装的所有企业设置、帐户和内容都被 iOS 标记为“托管”。



用户可以通过“设置”中配置描述文件的用户界面准确了解自己设备上已经配置的内容。

- **用户隐私。**虽然 MDM 服务器允许你与 iOS 设备交互，但是系统不会显示所有设置和帐户信息。你可以管理通过 MDM 预置的企业帐户、设置和信息，但是不能访问用户的个人帐户。实际上，确保数据在企业托管 app 中得到安全保护的功能，还可以防止用户的个人内容进入企业数据流。

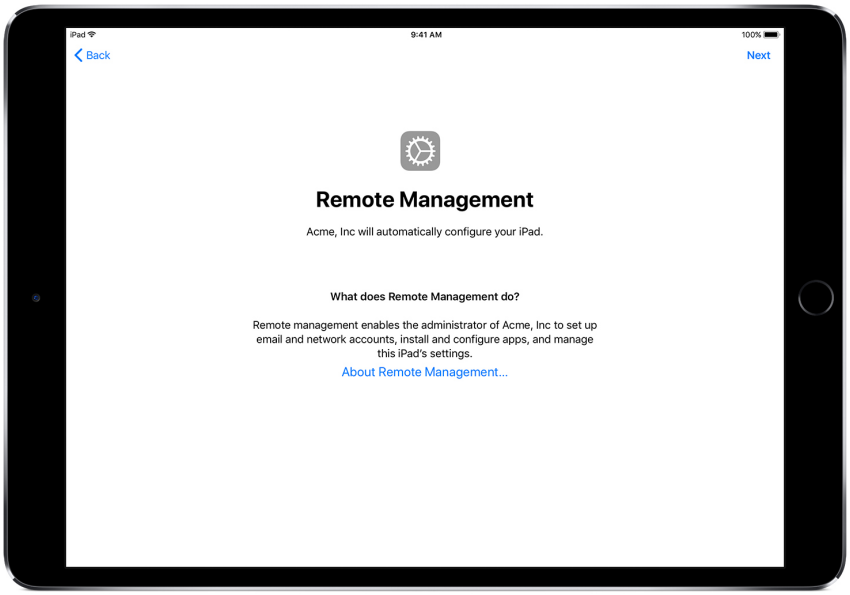
示例展示了第三方 MDM 服务器在个人 iOS 设备上可以查看和无法查看的内容：

MDM 可以查看：	**MDM 无法查看个人数据，例如：**
设备名称	个人或工作邮件、日历、通讯录
电话号码	短信或 iMessage 信息
序列号	Safari 浏览器历史记录
型号名称和编号	FaceTime 通话或电话呼叫记录
可用容量和空间	个人提醒事项和备忘录
iOS 版本号	app 使用频率
已安装 app	设备位置

- **个性化设置设备。**企业发现，允许用户使用自己的 Apple ID 对设备进行个性化设置，可以让用户更有效地管理和保护自己的设备，并能提高其工作效率，因为他们现在可以选择所需的 app 和内容来最有成效地完成工作。

企业拥有的设备

采用企业拥有的部署模式时，你可以为每位用户提供一台设备，这称作“个性化部署”；或者你也可以让多个用户轮流使用设备，也就是所谓的“非个性化部署”。自动注册、可锁定 MDM 设置、设备监管以及始终打开 VPN 等 iOS 功能可确保设备根据企业特定要求进行配置，这种方式不仅能增强控制，还能保证企业数据的安全。



采用 Apple 商务管理，你的 MDM 解决方案可在设置助理期间自动配置 iOS 设备。

- 自动进行注册。采用 Apple 商务管理，你可以在企业拥有的 iPhone 和 iPad 设备以及 Mac 系统的初始设置期间自动完成 MDM 注册。你可以将注册设置为强制操作，且不可移除。你也可以在注册的过程中将设备设为监管模式，并允许用户跳过部分设置步骤。
- 受监管设备。监管功能为企业拥有的 iOS 设备提供了更多管理功能。它还提供相应的功能，通过全局代理启用网络过滤，以确保用户的网络流量符合企业的要求，防止用户将设备重置为出厂状态等。默认情况下，所有 iOS 设备都不受监管。使用 Apple 商务管理自动启用监管模式，或使用 Apple Configurator 2 手动启用监管。

即使你现在不打算使用任何仅限受监管设备的功能，也不妨在设置设备时对其进行监管，以便能在未来使用仅限受监管设备的功能。否则，一旦将来需要使用此类功能时，你就不得不擦除已经部署完毕的设备。监管并不是锁定设备，而是通过扩展管理功能优化企业拥有的设备。从长远来看，监管可以为企业提供更多选择。

有关受监管设置的完整列表，请参阅 iOS 部署参考。

限制

iOS 支持以下限制类别，你可以在不影响用户的情况下，根据企业的需求以无线方式对其进行配置：

- AirPrint
- App 安装
- App 使用
- 课堂 app
- 设备
- iCloud
- 描述文件管理器用户和用户组限制
- Safari
- 安全性和隐私设置
- Siri

以下类别中也存在可由 MDM 解决方案配置的选项：

- 自动完成 MDM 注册设置
- 设置助理屏幕

其他管理功能

查询设备

除了配置设备，MDM 服务器还可以向设备查询各种信息，例如设备详情、网络、应用程序以及合规性和安全性数据。此类信息有助于确保设备始终遵循策略要求。MDM 服务器决定收集信息的频率。

以下是可以在 iOS 设备上查询的信息示例：

- 设备详情 (名称)
- 型号、iOS 版本、序列号
- 网络信息
- 漫游状态、MAC 地址
- 安装的应用程序
- App 名称、版本、大小
- 合规性和安全性数据
- 已安装的设置、策略、证书
- 加密状态

管理任务

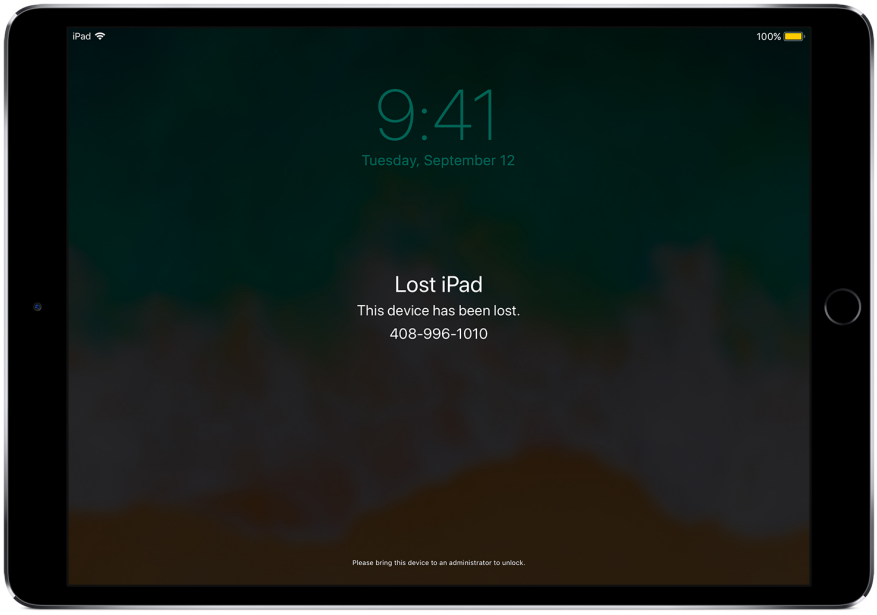
当设备处于托管状态时，MDM 服务器可以执行很多种管理任务，包括无需用户介入自动更改配置设置、在密码锁定的设备上执行 iOS 更新、远程锁定或擦除设备、或者清除密码锁定以便用户可以重置遗忘的密码等。MDM 服务器还可以请求 iOS 设备开始向特定目标进行隔空播放镜像或终止一个当前的隔空播放会话。

丢失模式

在 iOS 9.3 或更高版本中，你的 MDM 解决方案可通过远程方式将受监管的设备设置为丢失模式。这一操作会锁定设备，并在锁定屏幕上显示一个带有电话号码的信息。

借助丢失模式，可以定位丢失或被盗的受监管设备，因为 MDM 可以远程查询这些设备上次在线时的位置。丢失模式不需要启用“查找我的 iPhone”。

如果 MDM 远程解除丢失模式，则设备将被解锁，其位置信息将被收集。为保持透明度，用户会收到关于丢失模式被关闭的通知。



MDM 将丢失设备设为丢失模式时，它将锁定设备，允许在屏幕上显示消息，并识别设备位置。

激活锁

在 iOS 7.1 或更高版本中，你可以使用 MDM 在用户打开受监管设备上的“查找我的 iPhone”时启用激活锁。这样一来，你所在的企业就能从激活锁的防盗功能中获得帮助，并能在某些情况下绕过此功能，比如说，如果用户在尚未使用其 Apple ID 移除激活锁的情况下，离开了贵企业。

你的 MDM 解决方案可以获取绕过码，并准许用户基于以下情况启用设备上的激活锁：

- 如果你的 MDM 解决方案允许启用激活锁，而“查找我的 iPhone”正处于开启状态，那么激活锁即刻就会启用。
- 如果你的 MDM 解决方案允许启用激活锁，而“查找我的 iPhone”正处于关闭状态，那么激活锁会在用户下一次开启“查找我的 iPhone”时启用。

总结

Apple 在 iOS 中内置的统一管理框架为你提供了两全其美的体验：IT 能够配置、管理和保护设备，并在这些过程中对企业数据流进行充分控制；与此同时，用户能够使用自己喜爱的设备，从而出色地完成工作。