iOS 和 iPadOS 部署概述

简介

目录

iPhone 和 iPad 与 iOS 和 iPadOS 强强联手，让员工能随时随地出色完成工作。此外，它们还能帮助 IT 部门减少管理设备的时间，让工作重心不再局限于解决技术问题和削减成本，而是制定业务策略。

本文稿为如何在组织中部署 iOS 和 iPadOS 设备提供了指导，并且有助于你为制定最符合组织环境的部署计划打好基础。

如需更详细地了解本文所述主题，包括利用最新的 iOS 和 iPadOS 更新进行部署的最新内容，请查阅在线资源：“Apple 平台部署”指南

所有权模式

企业中通常会使用以下两种 iOS 和 iPadOS 设备所有权模式：

- 企业拥有
- 用户拥有

两种模式各有其优势，因此，选择最适合贵组织的模式至关重要。虽然大多数组织都有自己的首选模式，但你可能会在自己的部署环境中使用多种模式。

当你选出最适合贵企业的模式后，你的团队便可进一步探索 Apple 的部署和管理功能。

企业拥有的设备

在企业拥有设备的模式下，设备由企业或参与计划的 Apple 授权经销商或运营商采购。如果向每位用户提供一部设备，则称为“一对一部署”。设备也可以由用户轮换使用，这种方式通常称为“共享部署”。“共享 iPad”就是共享部署的一个示例，这种所有权模式能让多位用户在无需共享信息的情况下共享 iPad 设备。企业可在整个企业环境中结合使用共享部署和一对一部署模式。

使用企业拥有模式时，IT 可以通过监督和自动设备注册实现更高级别的控制，从设备开箱起，企业就可以配置和管理设备。

进一步了解针对受监督设备的限制：
support.apple.com/guide/deployment/welcome/web

对于受监督的 Apple 设备，IT 拥有更多控制权。

- 配置账户
- 配置全局代理
- 安装、配置与删除 app
- 要求提供复杂的密码
- 强制实施所有限制
- 访问全部 app 的清单
- 远程抹掉整个设备
- 管理软件更新
- 移除系统 app
- 修改墙纸
- 锁定到单个 app
- 绕过激活锁
- 强制开启无线局域网
- 将设备设置为丢失模式

用户拥有的设备

在用户拥有的模式中，用户购买、设置和配置设备。这类部署通常称为 BYOD (自带设备) 部署。为了使用组织服务 (例如无线局域网、邮件和日历)，或者为了配置设备以满足特定的教育或商务要求，用户通常会将设备注册到组织的移动设备管理 (MDM) 解决方案中。其间需使用一项名为“用户注册”的 Apple 功能。

用户注册不仅能以安全方式管理企业资源和数据，同时也能保护用户的隐私、个人数据和 app。IT 部门可以强制执行、访问和管理特定功能，具体功能如下表所列。

要在自己的设备上访问企业数据，用户需要使用自己的管理式 Apple ID。管理式 Apple ID 是“用户注册”描述文件的一部分，用户必须成功地进行身份验证，才能完成注册。管理式 Apple ID 可与用户已经登录的个人 Apple ID 一起使用，两者互不影响。这会在设备上实现数据独立。对于拥有 iCloud 存储空间的企业，将会为所有管理式 Apple ID 下管理的所有数据创建独立的 iCloud 云盘。

进一步了解 MDM 解决方案中的用户注册：
support.apple.com/guide/deployment/welcome/web

在个人设备上，MDM 功能有使用限制。

- ✓ 配置账户
- ✓ 配置“为 App 单独设置 VPN”
- ✓ 安装和配置 app
- ✓ 要求提供密码
- ✓ 强制执行特定的限制
- ✓ 访问工作 app 目录
- ✓ 仅移除工作数据
- ✗ 访问个人信息
- ✗ 访问个人 app 目录
- ✗ 移除任何个人数据
- ✗ 收集设备上的任何日志
- ✗ 接管任何个人 app
- ✗ 要求提供复杂的密码
- ✗ 远程擦除整部设备
- ✗ 访问设备位置

部署步骤

这个部分将概括介绍设备与内容部署过程中的五个步骤：准备环境、设置设备、部署设备和管理设备。你使用的步骤取决于设备是归企业还是员工所有。

如需更详细地查看这些步骤，请访问在线资源：“Apple 平台部署”指南。

1. 集成与设置

在确定了适合贵企业的部署模式后，必须为部署奠定基础。

MDM 解决方案。适用于 iOS 和 iPadOS 的 Apple 管理框架使组织能够在企业环境中以安全方式注册设备、以无线方式配置和更新设置、监控政策的遵守情况、部署 app、以及远程擦除或锁定受管理的设备。这些管理功能由第三方 MDM 解决方案来实现。有很多第三方 MDM 解决方案可以支持不同的服务器平台。每种解决方案各自有不同的管理控制台、功能和定价。

Apple 商务管理。IT 管理员可以利用这个网页版门户，从一处部署 iPhone、iPad、iPod touch 和 Mac。Apple 商务管理可以与你的 MDM 解决方案默契配合，从而轻松实现设备部署自动化、购买 app 和分发内容，以及为员工创建管理式 Apple ID。

管理式 Apple ID。与个人 Apple ID 一样，管理式 Apple ID 用于登录 Apple 设备和服务，例如 FaceTime 通话、iMessage 信息、App Store、iCloud、iWork 和备忘录，让用户能够访问众多有助提高工作效率和促进协作的内容和功能。但管理式 Apple ID 归组织所有，是 Apple 设备管理不可或缺的一部分。借助这类账户，你的组织可以管理各种事项，例如密码重设和基于职务的权限分配，而且还可对特定设置实施限制。

进一步了解管理式 Apple ID：
support.apple.com/guide/apple-business-manager

无线局域网及网络连接。Apple 设备内置安全的无线网络连接功能。请确认你所在公司的无线网络能够支持多台设备，允许你的所有用户同时接入。你还应确保对网络基础架构进行设置，使之可正常运行 Bonjour，这是 Apple 提供的基于标准的零配置网络协议。Bonjour 使设备可以自动查找网络上的服务。iOS 和 iPadOS 设备通过 Bonjour 连接至兼容隔空打印的打印机和兼容隔空播放的设备。一些 app 还使用 Bonjour 来发现其他可进行协作和共享的设备。

进一步了解无线局域网及网络连接：

support.apple.com/guide/deployment/welcome/web

进一步了解 Bonjour：

developer.apple.com/bonjour

VPN。请评估你的 VPN 基础架构，以确保用户可以通过他们的 iOS 和 iPadOS 设备安全地远程访问公司资源。考虑使用 iOS 和 iPadOS 的“请求 VPN 域”或“为 App 单独设置 VPN”功能，以便仅在需要时启动 VPN 连接。如果打算使用“为 App 单独设置 VPN”，请确保你的 VPN 网关支持此类功能，并购买足够数量的许可，确保所需数量的用户和连接都能获得相应许可。

邮件、内容和日历。iPhone、iPad 和 Mac 可运行 Microsoft Exchange、Office 365 及 Google Workspace 等其他常用电子邮件服务，通过加密的 SSL 连接实现快捷访问，以推送电子邮件、日历、通讯录和任务。如果你使用 Microsoft Exchange，请验证 ActiveSync 服务是否为最新，并且已配置为支持网络上的所有用户。如果你使用基于云的 Office 365，请务必根据预计将要连接的 iOS 和 iPadOS 设备数量备足许可。iOS 和 iPadOS 还支持使用 OAuth 2.0 和多重身份验证的 Office 365 新式身份验证。如果你不使用 Exchange，则 iOS 和 iPadOS 可与基于标准的服务器配合使用，包括 IMAP、POP、SMTP、CalDAV、CardDAV 和 LDAP。

2. 身份管理

除了准备好环境，IT 团队还需要选择管理身份验证和授权的方式，进一步为部署奠定基础。这有助于确保设备和数据的安全。

身份验证。身份验证方法有很多种。使用单点登录和 Apple 服务，例如管理式 Apple ID、iCloud、iMessage 信息等，确保用户能够安全地通信、在线创建文稿和备份个人数据，且不泄露组织的数据。每项服务都使用其自身的安全架构，以确保以下几点：安全处理数据 (无论数据存储在 Apple 设备上还是通过无线网络进行传输)；保护用户的个人信息；防范威胁，阻止对信息和服务进行恶意或未经授权的访问。MDM 解决方案可用于限制和管理对 Apple 设备上特定服务的访问。

进一步了解单点登录：
support.apple.com/guide/deployment/depfdbf18f55/1/web/1.0

进一步了解 Kerberos 单点登录：
support.apple.com/guide/deployment/depe6a1cda64/1/web/1.0

授权。授权与身份验证有所不同。身份验证是用来证明你是谁，授权则是用来规定你可以做什么。例如，你可以通过向 IdP 提供用户名和密码来进行授权。在这个示例中，颁发机构是身份识别提供程序或 Active Directory，断言是用户名和密码，令牌是成功登录后收到的数据。也可以使用其他断言，包括证书、智能卡和其他多重认证设备。

联合身份验证。身份联合要求管理员将域设置为相互信任，并就识别用户的方法达成一致。一个常见的示例是使用企业账户登录云身份识别提供程序。IT 团队可以启用 Microsoft Azure Active Directory (Azure AD) 和 Apple 商务管理之间的联合身份验证，从而简化为组织创建管理式 Apple ID 等流程。然后，用户将使用现有的 Azure AD 凭证登录 iCloud 或与 Apple 商务管理相关联的 Apple 设备。

3. 部署规划和配置

打好基础之后，就可以配置设备并准备好分发你的内容。无论采用哪种所有权和部署模式，搭配使用 MDM 解决方案和 Apple 商务管理或 Apple Configurator 2 时效果最佳。

自动设备注册

通过这种注册方法，你可以简便快捷地部署企业拥有的 Apple 设备并将其注册到 MDM 中，无需实际接触或准备每台设备。对于最终用户，IT 团队可通过简化设置助理中的步骤来简化设置流程，确保员工在激活设备后立即获得正确的配置。只有直接从 Apple 或从参与计划的 Apple 授权经销商或运营商处购买的设备，才能通过自动设备注册进行部署。

设备注册

你也可以通过 Apple Configurator 2 和贵企业的 MDM 解决方案，以手动方式部署设备。企业或用户拥有的设备都可通过设备注册进行部署。手动受管理的设备与任何其他已分配设备一样，也会受到强制监督并进行 MDM 注册。如果 IT 团队需要管理不是直接从 Apple 购买或通过参与 Apple 授权经销商或运营商购买的设备，那么这种部署方法非常适合。

进一步了解 Apple Configurator 2：
support.apple.com/zh-cn/apple-configurator

用户注册

IT 部门可通过用户注册来配置和部署用户拥有的设备，无需锁定设备即可保护企业数据。请参阅所有权模式部分，了解有关用户注册的更多信息。

无论设备是归企业还是用户所有，在分发设备时，IT 团队都可以通过设置助理保持对设置体验的控制。设置助理功能由贵企业的 MDM 解决方案进行配置，让用户能够立即在其设备上工作。

完成设备注册后，管理员便可以启动 MDM 策略、选项或命令；针对设备可用的管理操作也因监管和注册方法而有所不同。随后，iOS 或 iPadOS 设备将通过 Apple 推送通知服务 (APNs) 接收管理员的操作通知，以便通过安全连接直接与 MDM 服务器通信。通过网络连接，APNs 可以向世界各地的设备发送命令。但是 APNS 不会传输任何机密或专有信息。

4. 配置管理

Apple 设备内置安全的管理框架，以便 IT 人员使用各种管理功能来管理设备。这一管理框架可分为四个部分：

配置描述文件

配置描述文件包含用于将设置和授权信息加载到 Apple 设备上的有效负载。配置描述文件可以自动配置设置、账户、限制和凭证。根据具体的 MDM 解决方案提供商以及与内部系统的集成方式，账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)。

限制

借助限制，你可以强制执行安全策略，并在不锁定设备的情况下帮助用户保持专注。限制的示例包括了以下功能：受管理的打开方式，可防止受管理的来源中的附件或文稿在未受管理的目标位置打开；单 App 模式，可将设备限制到单个 app；防止备份，可防止对受管理的 app 将数据备份到 iCloud 或设备。

管理任务

当设备处于受管理状态时，MDM 服务器可以执行多种管理任务，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软件更新、远程锁定或擦除设备，或者清除密码锁定以便用户可以重设遗忘的密码等。MDM 服务器还可以请求 iPhone 或 iPad 开始向特定目标进行隔空播放镜像或终止当前的隔空播放会话。在长达 90 天内，你可以阻止用户以无线方式手动更新受监督的设备。也可以使用贵企业的 MDM 解决方案为受监督设备安排软件更新。

查询

MDM 服务器可查询设备的各种信息，包括硬件详情，例如序列号、设备 UDID 或无线局域网 MAC 地址，以及软件详情，例如 iOS 或 iPadOS 版本和设备上安装的所有 app 的详细列表。你的 MDM 解决方案可使用这些信息来保持库存信息为最新，做出明智的管理决策，并自动执行管理任务，例如确保用户保留相应的一组 app。

5. 内容分发

注册后，管理员现在还可以使用受管理分发。这样一来，在任何提供相关 app 的国家/地区，MDM 解决方案或 Apple Configurator 2 都能管理从 Apple 商务管理商店购买的所有 app。要启用托管分发，你必须先使用安全令牌将 MDM 解决方案关联到 Apple 商务管理账户。在连接到 MDM 服务器后，你可以将 Apple 商务管理 app 分配给用户，即使设备上的 App Store 被禁用也无妨。

有一种可以向用户分发的内容，即：受管理的 app。受管理的 app 可以通过 MDM 服务器部署和移除，或当用户从 MDM 移除自己的设备时，也会同时移除受管理的 app。移除 app 时，与之关联的数据也会随之移除。

将内容分发给用户的两种方式包括：

将 app 分配到设备。你可以使用 MDM 解决方案或 Apple Configurator 2 将 app 直接分配到设备。在初次部署时，这种方法可以省略几个步骤，让你的部署变得更轻松快捷，同时保持对受管理的设备和内容的完全控制。在将 app 分配给设备后，相应 app 会通过 MDM 推送到该设备，而无需用户邀请。使用该设备的任何人都可以访问这个 app。

将 app 分配给用户。另一种方法是使用 MDM 解决方案通过电子邮件或推送通知消息来邀请用户下载 app。用户可以使用个人 Apple ID 在其设备上登录接受邀请。该 Apple ID 是通过 Apple 商务管理服务注册的，但仍然是完全私密的，而且管理员无法看到。用户同意邀请后，会连接到你的 MDM 服务器，以便开始接收分配的 app。App 可在所有用户的设备上自动下载，无需任何其他操作或费用。

当设备或用户不再需要你已分配的 app 时，可将它们撤销并重新分配给其他设备或用户，这样一来，组织可保持对所购 app 的完全所有权和控制力。

设备安全

从设计之初，Apple 就将先进的安全功能集成到设备中。设备设置完成后，IT 团队可借助 MDM 带来的内置安全功能和其他控制措施，管理和保护企业数据。跨 app 的通用框架使得设置的配置和持续管理成为可能。

进一步了解 Apple 平台安全保护：
support.apple.com/guide/security/welcome/web

保护工作数据。IT 部门可以通过 MDM 执行和监控安全策略。例如，在 iOS 和 iPadOS 设备上要求提供密码会自动启用数据保护功能，为设备提供文件加密。MDM 还可以用于配置无线局域网、VPN，以及部署证书以提高安全性。

MDM 解决方案可实现精细化设备管理，无需使用存储容器，即可保护企业数据安全。有了受管理的打开方式，IT 部门可设置限制，防止附件或文稿在非托管目标位置中被打开。

锁定、定位和擦除。设备丢失时，贵企业的数据不一定会随之丢失。在 iOS 和 iPadOS 设备上，IT 部门可以远程锁定并抹掉所有敏感数据，以保护公司的信息。在受监督的 iOS 和 iPadOS 设备上，IT 部门可以启用丢失模式，以查看设备的位置。IT 团队还拥有管理企业 app 的工具，可以立即从设备中删除这些 app，而无需抹掉个人数据。

App。得益于通用的架构和受控制的生态系统，Apple 平台上的 app 均采用高度安全的设计。我们的开发者计划会验证每位开发人员的身份，而各款 app 在 App Store 上发布之前均须经过系统验证。Apple 为开发者提供签名、app 扩展、授权和沙盒等多项功能的框架，以确保提供更高级别的安全保障。

丢失模式。你的 MDM 解决方案可以远程将受监督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。处于丢失模式时，丢失或被盗的受监督设备可以被定位，因为 MDM 能远程查询它们上次在线时的位置。丢失模式不要求查找功能处于启用状态。

激活锁。你可以使用 MDM 在用户打开受监督设备上的查找功能时启用激活锁。激活锁的防盗功能对企业有益，与此同时，如果用户无法使用自己的 Apple ID 验证身份，你也可以选择绕过此功能。

支持选项

Apple 提供了各种计划和支持资源。

AppleCare for Enterprise 企业版

对于寻求全方位保障的公司而言，AppleCare for Enterprise 企业版可帮助减轻企业内部 Help Desk 的工作量。它通过电话为员工提供全天候技术支持，并对具有重要优先级别的问题在一小时内进行回应。这个计划可为所有 Apple 硬件和软件，以及复杂的部署和整合情境 (包括 MDM 和 Active Directory) 提供 IT 部门级支持。

AppleCare OS Support

AppleCare OS Support 为 IT 部门提供了针对 iOS 和 iPadOS 部署的企业级电话和电子邮件支持。此项服务提供每周 7 日的 24 小时支持，并可指派技术客户经理，具体视购买的支持级别而定。通过 AppleCare OS Support 专业支持，IT 人员可以在整合、迁移以及高级服务器操作问题方面直接获得技术人员的帮助，从而提高 IT 员工在部署和管理设备以及解决问题时的效率。

AppleCare Help Desk Support

通过 AppleCare Help Desk Support，可以优先从 Apple 的高级技术支持人员处获得电话支持。它还包含一套用来对 Apple 硬件进行诊断和故障排除的工具，可以帮助大型企业更高效地管理其资源、提高响应速度并降低培训成本。AppleCare Help Desk Support 提供不限次数的支持服务，范围涵盖硬件和软件诊断与故障排除，以及对 iOS 和 iPadOS 设备进行问题隔离。

适用于 iPad 的 AppleCare+ 服务计划、适用于 iPhone 的 AppleCare+ 服务计划和适用于 iPod touch 的 AppleCare+ 服务计划

每台 iOS 和 iPadOS 设备均附带一年期有限保修以及自购买日起 90 天内免费电话技术支持。如购买适用于 iPhone 的 AppleCare+ 服务计划、适用于 iPad 的 AppleCare+ 服务计划或适用于 iPod touch 的 AppleCare+ 服务计划，此服务的期限可延长至自原始购买日起两年。你可以随时通过电话联系 Apple 技术支持专家来解答你的问题。当设备需要维修时，Apple 还提供便捷的服务选项。此外，该计划最多提供两次意外损坏保修服务，每次需收取相应的服务费。

iOS 直接服务计划

作为 AppleCare+ 服务计划的优势之一，iOS 直接服务计划使你的 Help Desk 可以筛查设备问题，而无需致电 Apple 支持或前往 Apple Store 零售店。如有必要，你的组织可以直接通过该计划订购更换用的 iPhone、iPad、iPod touch 或随附配件。

进一步了解 AppleCare 计划：

apple.com.cn/support/professional

总结和资源

无论你的公司要将 iPhone 或 iPad 部署到一部分用户还是整个企业，都有多种方案可选，方便你轻松部署和管理这些设备。为你的企业选择适当的部署策略可帮助员工提高工作效率，并让他们能以全新的方式来完成工作。

了解 iOS 和 iPadOS 部署、管理和安全功能：

support.apple.com/guide/deployment/welcome/web

了解 Apple 商务管理：

support.apple.com/guide/apple-business-manager

了解适用于企业的管理式 Apple ID：

apple.com.cn/business/docs/site/Overview_of_Managed_Apple_IDs_for_Business.pdf

了解 Apple at Work：

apple.com.cn/business

了解 IT 功能：

apple.com.cn/business/it

了解 Apple 平台安全保护：

apple.com/security

浏览可选的 AppleCare 计划：

apple.com.cn/support/professional

了解 Apple 培训与认证：

training.apple.com

测试 Beta 版软件、访问测试计划并提供反馈：

beta.apple.com/zh-CN