



iOS 和 iPadOS 部署概述

简介

iPhone 和 iPad 可以为你的业务模式以及员工的工作方式带来彻底的改变。它们可以显著提升工作效率，使员工无论在办公室内还是外出期间，都能以全新方式自由灵活地开展工作。采用这种现代化的工作方式将为整个企业带来诸多益处。用户可以更好地访问相关信息，借助更强大的功能以创新的方式解决问题。

通过为 iOS 和 iPadOS 提供支持，IT 部门的工作重心不再仅限于解决技术问题和削减成本，而是制定业务战略和解决实际问题。最终每个人都会从中受益，不仅员工工作热情高涨，新的业务机会更将不断涌现。

在整个公司内设置和部署 iPhone 和 iPad 从未如此简单。借助 Apple 商务管理和第三方移动设备管理 (MDM) 解决方案，你所在的企业可以轻松大规模部署 iOS 和 iPadOS 设备以及 app。

- 移动设备管理让你能够配置和管理设备，并能通过无线方式分发和管理 app。
- Apple 商务管理在 MDM 解决方案中自动注册 Apple 设备，通过无需 IT 部门人工干预的配置简化部署。
- 借助 Apple 商务管理，你还可以批量购买 app，并通过无线方式将它们分发给用户。
- 此外，借助 Apple 商务管理，你可以通过 Microsoft Azure AD 使用联合身份验证来为员工创建管理式 Apple ID。

本文稿为如何在企业中部署 iOS 和 iPadOS 设备提供了指导，可帮助你制定最符合贵企业环境的部署计划。本文中所介绍的主题在在线《iPhone 和 iPad 部署参考》中均有详细介绍：

support.apple.com/zh-cn/guide/deployment-reference-ios

所有权模式

评估所有权模式并为你的企业选出最佳模式，是部署中极为重要的第一步。部署方法多种多样，具体取决于设备归谁所有。首先需要确定哪种模式最适合你的企业。

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

由于大多数企业都有自己的首选模式，因此你可能会在自己的部署环境中遇到多种模式。例如，企业办公室可能会部署“用户拥有”策略，即在保证公司资源受到良好保护和管理并且不影响用户个人数据和 app 的前提下，允许员工设置个人 iPad。而企业的零售店可能会部署“企业拥有”策略，即允许多名员工共享 iOS 和 iPadOS 设备，以便处理顾客交易。

通过探索这些模式，你可以为贵企业特有的环境选择一个最佳做法。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”模式下，你可以向员工提供设备供他们日常使用，也可以让员工共享设备完成常见任务，或者将设备配置为锁定在单个 app 中，用于特定目的。最终用户可以对提供给单个用户的设备进行个性化设置。通常情况下，最终用户无法对锁定到单个 app 的设备或多名用户共享的设备进行个性化设置。通过组合使用这些模式、关键 Apple 技术和 MDM 解决方案，你可以实现设备设置和配置的全面自动化。

个性化部署。在采用个性化部署策略时，你可以让每位用户选取自己的设备并在 MDM 解决方案中注册设备，以便通过无线方式获取企业设置和 app。对于直接从 Apple 或参与计划的 Apple 授权经销商或运营商处购买的设备，你还可以利用 Apple 商务管理在 MDM 解决方案中自动注册新设备，这一过程称为自动化设备注册。配置之后，除了可以使用企业帐户或由企业提供的 app 外，设备的用户还可通过自己的 app 和数据对设备进行个性化设置。

非个性化部署。当设备由多人共用或者仅用于一个用途时 (例如在餐馆或酒店中), IT 管理员通常会集中配置和管理这些设备, 而不是依赖个人用户来进行设置。采用非个性化部署时, 通常情况下不允许用户在设备上安装 app 或存储任何个人数据。利用 Apple 商务管理进行的自动化设备注册也有助于对非个性化设备进行自动化设置。以下图表列出了管理员和用户在“企业拥有”部署策略的每一步骤中需要执行的操作。除非另有注明, 否则这些操作对个性化部署和非个性化部署皆适用。

	管理员	用户
准备	<ul style="list-style-type: none"> 评估基础架构 选择 MDM 解决方案 注册 Apple 商务管理 	不需要用户操作
设置	<ul style="list-style-type: none"> 配置设备 分发 App 	不需要用户操作
部署	<ul style="list-style-type: none"> 分发设备 <p>只限个性化部署</p> <ul style="list-style-type: none"> 允许用户进行个性化设置 	<p>只限个性化部署</p> <ul style="list-style-type: none"> 下载并安装 app 使用 Apple ID、App Store 以及 iCloud 帐户 (如果适用) <p>只限非个性化部署</p> <ul style="list-style-type: none"> 不需要用户操作
管理	<ul style="list-style-type: none"> 管理设备 部署和管理其他内容 	<p>只限个性化部署</p> <ul style="list-style-type: none"> 发现其他要使用的 app <p>只限非个性化部署</p> <ul style="list-style-type: none"> 不需要用户操作

用户拥有的设备

如果设备由用户进行购买和设置, 即通常所说的 BYOD (自带设备部署), 你仍可以通过 iOS 13 和 iPadOS 中新的用户注册选项使用 MDM 提供 Wi-Fi、邮件和日历等企业服务的访问权限。

BYOD 部署允许用户设置并配置自己的设备。用户可以在企业的 MDM 解决方案中注册设备, 以便获得企业资源的访问权限、配置各种设置、安装配置描述文件或安装企业 app。用户必须注册企业的 MDM 解决方案。

适用于个人设备的“用户注册”不仅能够以安全方式管理企业资源和数据, 同时尊重用户的隐私、个人数据和 app。IT 只能强制配置特定设置、监控企业政策的遵守情况和移除企业数据和 app, 最终用户设备上的个人数据和 app 不会受到任何影响。

“用户注册”包括以下内容：

- **管理式 Apple ID。**“用户注册”与管理式 Apple ID 集成，以便在设备上建立用户身份，并提供对 Apple 服务的访问。管理式 Apple ID 可以与用户已经登录的个人 Apple ID 一起使用。管理式 Apple ID 在 Apple 商务管理中创建，并通过联合身份验证提供给 Microsoft Azure Active Directory。
- **数据隔离。**“用户注册”能够为设备上的托管帐户、app 和数据创建单独的 APFS 宗卷。该托管宗卷能够以加密方式与设备的其他内容隔离。
- **适用于 BYOD 的精细化管理。**“用户注册”专为用户拥有的设备设计，因此，IT 人员可以管理一组配置和策略，同时限制某些管理任务，例如远程擦除整个设备或收集个人信息。

以下图表列出了管理员和用户“用户拥有”部署策略的每个步骤中需要执行的操作。

	管理员	用户
准备	<ul style="list-style-type: none"> • 评估基础架构 • 选择 MDM 解决方案 • 注册 Apple 商务管理 	<ul style="list-style-type: none"> • 使用个人 Apple ID 和管理式 Apple ID、App Store 和 iCloud 帐户 (如果适用)
设置	<ul style="list-style-type: none"> • 配置设备设置 • 分发 App 	<ul style="list-style-type: none"> • 选择加入公司的 MDM 解决方案 • 下载并安装 app
部署	不需要管理员操作	不需要用户操作
管理	<ul style="list-style-type: none"> • 管理设备 • 部署和管理其他内容 	发现其他要使用的 app

进一步了解 MDM 中的“用户注册”：

support.apple.com/zh-cn/guide/mdm

进一步了解联合身份验证：

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

部署步骤

本部分将逐一详细介绍设备与内容部署过程中的四个步骤：准备环境、设置设备、部署设备和管理设备。所用的步骤将取决于设备拥有者是企业还是用户。

1. 准备

在确定了适合企业的部署模式后，遵循以下步骤开始为部署打下坚实基础；你甚至可以在拥有设备前就进行这些操作。

评估基础架构

iPhone 和 iPad 可以无缝整合到大多数标准的企业 IT 环境。请务必评估你的现有网络基础架构，以确保企业充分利用 iOS 和 iPadOS 提供的各项功能。

无线网络

对于设置和配置 iOS 和 iPadOS 设备而言，稳定可靠的无线网络连接至关重要。请确认贵公司的 Wi-Fi 网络能够支持多台设备，允许你的所有用户同时连接。如果设备无法访问 Apple 的激活服务器、iCloud 或 App Store，你可能需要配置网络代理或防火墙端口。Apple 和 Cisco 也优化了 iPhone 和 iPad 与 Cisco 无线网络的通信方式，为实现快速漫游和 app 服务质量 (QoS) 优化等其他高级联网功扫清了障碍。

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 设备以安全方式远程访问公司资源。考虑使用 iOS 和 iPadOS 的“按需连接 VPN”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。

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。一些 app 还使用 Bonjour 来发现其他可进行协作和共享的设备。

进一步了解无线网络：

support.apple.com/zh-cn/guide/deployment-reference-ios

进一步了解 Bonjour：

developer.apple.com/library

邮件、通讯录和日历

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 设备数量准备数量充足的许可。iOS 和 iPadOS 还支持 Office 365 新式验证，利用 OAuth 2.0 和多重身份验证。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。

内容缓存

内容缓存是 macOS High Sierra 或更高版本集成的一项功能，可将用户经常向 Apple 服务器请求的内容的本地副本存储下来，进而最大限度地减少在你的网络中下载内容所需的带宽。内容缓存可加快通过 App Store 和 Mac App Store 下载和交付软件的速度。

它还可以缓存软件更新，以便更快速地下载至 iOS 和 iPadOS 设备。内容缓存包含连接缓存服务，利用这项功能，Mac 可以与通过 USB 连接的众多 iOS 和 iPadOS 设备共享其互联网连接。

进一步了解内容缓存：

support.apple.com/zh-cn/guide/deployment-reference-macos

进一步了解连接缓存：

support.apple.com/zh-cn/HT207523

选择 MDM 解决方案

适用于 iOS 和 iPadOS 的 Apple 管理框架使企业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、监控企业政策的遵守情况、部署 app、以及远程擦除或锁定托管设备。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。在选择一种解决方案之前，请参考下面列出的资源，以便评估哪些管理功能与你的企业最为相关。除第三方 MDM 解决方案外，还可使用 Apple 提供的“描述文件管理器”解决方案，这一解决方案是 macOS 服务器的一项功能。

进一步了解如何管理设备和企业数据：

apple.com.cn/cn/business/docs/resources/Managing_Devices_and_Corporate_Data_on_iOS.pdf

注册 Apple 商务管理

Apple 商务管理是一个网络门户，IT 管理员只需要在一个地方即可部署 iPhone、iPad、iPod touch 和 Mac。Apple 商务管理与移动设备管理 (MDM) 解决方案无缝协作，可以轻松实现设备部署自动化、购买 app 并部署内容，以及为员工创建管理式 Apple ID。

设备注册计划 (DEP) 和批量购买计划 (VPP) 现已完全集成到 Apple 商务管理中，因此企业组织可以将部署 Apple 设备所需的一切整合在一起。从 2019 年 12 月 1 日起将不再提供这些计划。

设备

Apple 商务管理支持自动设备注册，使企业组织得以用快捷简单的方式来部署企业拥有的 Apple 设备，并且无需实际接触或准备每台设备即可在 MDM 中进行注册。

- 通过简化“设置助理”中的步骤来简化用户的设置过程，从而确保员工在设备激活后能立即获得正确的配置。现在，IT 团队可以通过向员工提供同意书文本、企业品牌或现代身份验证方法来进一步自定义这种体验。
- 通过使用监管来对企业拥有的设备实现更高级别的控制，这种方式提供了其他部署模型不具备的额外设备管理控制，包括不可移除的 MDM。
- 通过设置基于设备类型的默认服务器，可以更轻松地管理默认 MDM 服务器。现在，无论你是通过何种方式获取 iPhone 和 iPad，你都可以使用 Apple Configurator 2 对其进行手动注册。

内容

Apple 商务管理让企业组织能够轻松地批量购买内容。无论你的员工使用 iPhone、iPad，还是 Mac，你都可以通过灵活且安全的分发方式为他们提供适用于工作的优质内容。

- 批量购买 app 和定制 app，包括内部开发的 app。轻松在不同地点之间转移 app 许可证，以及在同一地点的不同购买者之间共享许可证。可以查看统一的购买历史记录列表，包括当前通过 MDM 使用的许可证数量。
- 将 app 直接分发给托管设备或授权用户，轻松跟踪已经为哪些用户或设备分发了哪些内容。借助托管分发，可以控制整个分发过程，同时保留对这些 app 的完整所有权。设备或用户不需要的 app 可以在企业组织内撤销和重新分配。
- 使用多种付款方式支付，包括信用卡和采购订单。企业组织可以从 Apple 或 Apple 授权经销商处以特定当地货币金额购买批量信用额 (如果提供的话)，该金额以电子方式通过商店信用额的形式交付给帐户持有人。
- 将 app 分发给提供该 app 的任何国家/地区内的设备或用户，从而实现跨国分发。开发者可以通过标准 App Store 发布流程，向多个国家/地区提供 app。

注：某些国家/地区不支持 Apple 商务管理中的“图书”购买。要了解哪些功能在哪些地区提供以及支持的购买方法，请访问 support.apple.com/zh-cn/HT207305。

人员

Apple 商务管理使企业组织能够为员工创建并管理帐户，这些帐户可以与现有基础架构整合，并拥有 Apple app 和服务以及 Apple 商务管理的访问权限。

- 为员工创建管理式 Apple ID，以便员工能够通过 Apple app 和服务进行协作，并且能够在使用 iCloud 云盘的托管 app 中访问工作数据。这些帐户由每个企业组织拥有并管控。

- 通过关联 Apple 商务管理和 Microsoft Azure Active Directory，充分利用联合身份验证。当每位员工首次在兼容的 Apple 设备上使用现有的凭证登录时，将自动创建管理式 Apple ID。
- 使用 iOS 13、iPadOS 和 macOS Catalina 中新的用户注册功能，在员工拥有的设备上同时使用管理式 Apple ID 与个人 Apple ID。另外，管理式 Apple ID 可以在任何设备上作为主要 (唯一) Apple ID 使用。首次在 Apple 设备上登录后，管理式 Apple ID 还可以在网页上访问 iCloud。
- 为企业组织中的 IT 团队指定其他角色，从而在 Apple 商务管理中有效地管理设备、app 和帐户。如果需要，使用管理员角色接受条款和条件，如果有人离职，也能轻松转移职责。

注：iCloud 云盘目前不支持“用户注册”功能。当管理式 Apple ID 是设备的唯一 Apple ID 时，则可以用于 iCloud 云盘。

进一步了解 Apple 商务管理：www.apple.com.cn/business/it

在 Apple Developer Enterprise Program 中注册

Apple Developer Enterprise Program 提供了一整套工具，用来开发和测试 app 并分发给用户。你可以将 app 托管在网络服务器上或通过 MDM 解决方案进行分发。可以使用 Developer ID 为 Mac app 和安装器签名和公证并将其用于门禁功能，以便保护 macOS 免受恶意软件的侵害。

进一步了解 Developer Enterprise Program：
developer.apple.com/cn/programs/enterprise

2. 设置

在这一步中，利用 Apple 商务管理、MDM 解决方案或可选的 Apple Configurator 2 来配置设备并分发内容。对于设置可以采取多种方式，具体取决于设备归谁所有以及你的首选部署类型。

配置设备

可通过多种方式配置用户对企业服务的访问权限。IT 部门可以通过分发放置描述文件来设置设备。受监管设备有另外的配置选项。

使用 MDM 配置设备

在设备安全注册到 MDM 服务器后，将使用配置描述文件（一个包含 iOS 和 iPadOS 设备配置信息的 XML 文件）启用管理。这些描述文件可以自动配置设置、帐户、限制和凭证。这些描述文件可以从 MDM 解决方案通过无线方式交付，非常适合多台设备的简化配置。描述文件还可以作为电子邮件附件发送，可以从网页中下载，或通过 Apple Configurator 2 安装到设备上。

- **企业拥有的设备。**激活设备时，可以使用 Apple 商务管理启用用户设备的自动 MDM 注册。添加到 Apple 商务管理的所有 iOS 和 iPadOS 设备始终通过强制 MDM 注册受到监管。
- **用户拥有的设备。**员工可自主决定是否需要在 MDM 中注册他们的设备。而且，他们可以随时从 MDM 取消关联，只需从设备移除配置描述文件即可，这样也会移除企业数据和设置。不过，应考虑借助激励手段来鼓励用户保持托管状态。例如，你可以使用 MDM 解决方案自动提供无线凭证，以此要求用户必须先完成 MDM 注册，然后才能访问 Wi-Fi 网络。

设备注册完成后，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。只要有网络连接，设备便可以在全球任意地点接收 APN 命令。但机密或专有信息不会通过 APN 进行传输。

使用 Apple Configurator 2 配置设备 (可选)

如果是初次在本地部署多台设备，企业可以使用 Apple Configurator 2。通过这款免费的 macOS app，你可以将 iOS 和 iPadOS 设备通过 USB 连接到 Mac 电脑，并将 iOS 和 iPadOS 设备更新到最新版本，以配置设备设置和访问限制，并安装 app 及其他内容。初始设置完成后，你可以继续使用 MDM 通过无线方式进行管理。

Apple Configurator 2 的用户界面主要用于管理你的设备以及你希望在这些设备上执行的非连续性任务。这款 app 与 Apple 商务管理集成，让设备能够使用企业的设置在 MDM 中自动注册。通过使用 Blueprint 来组合非连续性任务，你可以在 Apple Configurator 2 中创建自定义工作流程。

进一步了解 Apple Configurator 2:

support.apple.com/apple-configurator

受监管设备

监管手段可以为你企业拥有的 iOS 和 iPadOS 设备提供额外的管理功能，从而实施禁用隔空投送或将设备置于单 App 模式等限制。它还提供相应的功能，可通过全局代理启用网络过滤来达到某些目的，例如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。在默认情况下，所有 iOS 和 iPadOS 设备都不受监管。你可以使用 Apple 商务管理来启用监管，或者也可以使用 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它们进行监管，便于将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，你就不得不擦除已部署的设备。监管并不是锁定设备，而是通过扩展管理功能优化公司拥有的设备。从长远来看，监管可以为企业提供更多选择。

进一步了解受监管设备的限制：

support.apple.com/zh-cn/guide/mdm

分发 App

Apple 提供了丰富的计划来帮助你的企业充分利用适用于 iOS 和 iPadOS 的优质 app 和内容。借助这些功能，你可以向设备和用户分发通过 Apple 商务管理购买的 app，或者你在企业内部开发的 app，从而为用户提供高效工作所需的一切资源。在购买时，你需要确定分发方式：托管分发或兑换代码。

托管分发

对于托管分发，你可以使用 MDM 解决方案或 Apple Configurator 2 来管理从任何提供相关 app 的国家/地区的 Apple 商务管理商店购买的 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 商务管理帐户。在连接到 MDM 服务器后，你可以分配 Apple 商务管理 app，即使设备上的 App Store 被禁用也无妨。

- **将 app 分配给设备。**使用 MDM 解决方案或 Apple Configurator 2，将 app 直接分配给设备。在初次部署时，这种方法可以省略几个步骤，这会让你的部署变得更快、更轻松，同时保持对托管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。而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 在其设备上登录以接受邀请。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和用户，这样一来，企业可保持对所购 app 的完全所有权和控制力。

兑换代码

你还可以使用兑换代码分发内容。如果企业无法在最终用户的设备上使用 MDM（例如，在连锁经营的场景下），这种方法会非常有用。此方法会将 app 永久转让给兑换代码的用户。兑换代码以电子表格格式提供。会根据已购数量为每个 app 提供一个唯一代码。每次兑换代码时，电子表格都会在 Apple 商务管理商店中更新，方便你随时查看兑换代码的数量。使用 MDM、Apple Configurator 2、电子邮件或内部网站分发代码。

使用 Apple Configurator 2 安装 app 和内容 (可选)

除基本设置和配置外，Apple Configurator 2 还可以用来为你要替用户设置的设备安装 app 和内容。对于个性化部署，你可以预先安装 app，从而节省时间和网络带宽。而对于非个性化部署，你可以对整个设备进行设置，甚至包括主屏幕布局。使用 Apple Configurator 2 配置设备时，你可以安装 App Store app、企业内部 app 和文稿。App Store app 需要使用 Apple 商务管理。可为支持文件共享的 app 提供文稿。要查看或检索 iOS 和 iPadOS 设备中的文稿，可将这些设备连接到运行 Apple Configurator 2 的 Mac。

3. 部署

借助 iPhone 和 iPad，员工开箱即可轻松启用他们的设备，无需 IT 的帮助。

分发设备

在前两步中完成了设备的准备和设置后，接下来就可以分发了。对于个性化部署，请将设备提供给用户，之后用户可以使用简化的“设置助理”来进一步进行个性化设置，并最终完成设置。对于非个性化部署，请将设备分发给当班的员工，或放到用于给设备充电并提供保护的 Kiosk 中。

设置助理

利用“设置助理”，iOS 用户在开箱后立即就能激活他们的设备、配置基本设置并开始工作。在完成初始设置后，用户还可以自己设定个人偏好设置，例如语言、位置、Siri、iCloud 和“查找我的 iPhone”。已注册 Apple 商务管理的设备将在设置助理中自动注册 MDM。

允许用户进行个性化设置

对于个性化部署和 BYOD 部署，允许用户使用其 Apple ID 来个性化设备可以提高工作效率，因为用户可以选择能够帮助他们以最佳方式完成任务和目标的 app 和内容。

Apple ID 和管理式 Apple ID

当员工使用 Apple ID 登录 Apple 服务 (例如 FaceTime 通话、iMessage 信息、App Store 和 iCloud) 时，他们可以访问丰富的内容，从而简化工作任务、提高工作效率以及支持协作。

像其他 Apple ID 一样，管理式 Apple ID 用于登录个人设备。还可用于访问 Apple 服务 (包括 iCloud，以及使用 iWork 和“备忘录”开展协作)，以及 Apple 商务管理。与 Apple ID 不同的是，管理式 Apple ID 由企业拥有和管理，例如密码重置和基于角色的管理。管理式 Apple ID 有部分设置是受到限制的。

通过“用户注册”注册的设备需要管理式 Apple ID。“用户注册”可选择支持个人 Apple ID 选项；其他注册选项仅支持个人 Apple ID 或管理式 Apple ID 中的一个。只有“用户注册”支持多个 Apple ID。

要充分利用这些服务，用户应使用为其创建的 Apple ID 或管理式 Apple ID。没有 Apple ID 的用户，在收到设备之前就可以自行创建一个 Apple ID。如果用户还没有个人 Apple ID，则可以使用设置助理创建一个。用户无需使用信用卡即可创建 Apple ID。

进一步了解管理式 Apple ID：

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

iCloud

iCloud 让用户能够自动同步文稿和个人内容 (如通讯录、日历、文稿和照片)，并使这些内容在多台设备之间保持最新。“查找”让用户可以查找丢失或被盗的 Mac、iPhone、iPad 或 iPod touch。iCloud 的部分服务 (如 iCloud 钥匙串和 iCloud 云盘) 可以通过在设备上手动输入限制条件或通过 MDM 设置限制条件来禁用。企业可以更全面地掌控哪些数据存储在哪个帐户中。

进一步了解如何管理 iCloud：

support.apple.com/zh-cn/guide/deployment-reference-ios

4. 管理

用户启动设备并开始工作后，可通过各种管理功能来持续管理和维护设备及内容。

管理设备

MDM 服务器可通过一组特定的任务来管理托管设备。这些任务包括查询设备信息以及启动管理任务，以便对那些违反政策、丢失或失窃的设备进行管理。

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 Wi-Fi MAC 地址；以及一些软件详情，例如 iOS 或 iPadOS 版本和设备上安装的所有 app 的详细列表。MDM 解决方案可以使用这些信息来维护最新的库存信息、做出明智的管理决策，以及自动执行管理任务，例如确保用户始终装有所需的一组 app。

管理任务

当设备处于托管状态时，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一个当前的隔空播放会话。

管理式软件更新

你可以阻止用户在指定时间内以无线方式手动更新受监管设备。在实施这个限制时，默认延迟期为 30 天，而且这会在 Apple 发布 iOS 或 iPadOS 更新时触发。不过，你可以更改默认的阻止更新天数，从 1 天到 90 天不等。你还可以利用 MDM 解决方案，在受监管设备上安排软件更新的时间。

丢失模式

你的 MDM 解决方案可以远程将受监管的设备置于丢失模式。此操作会锁定设备并允许在锁定屏幕上显示电话号码信息。处于丢失模式时，丢失或被盗的受监管设备可以被定位，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“查找我的 iPhone”处于启用状态。

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”时启用激活锁。这样一来，你的企业既能从激活锁的防盗功能中获益，又可以在用户无法使用其 Apple ID 验证身份时绕过此功能。

部署和管理其他内容

企业经常需要分发一些 app 以帮助员工提高工作效率。与此同时，企业需要控制这些 app 与内部资源的连接方式，或是如何在用户离开企业后确保数据安全，这一切都要兼顾用户的个人 app 和数据隐私。

内部 App 门户

大部分 MDM 服务器都提供内部 app 门户作为其解决方案的一部分。你也可以为员工创建自己的内部 app 门户，他们可以通过此门户轻松查找适用于其 iPhone 或 iPad 的 app。此门户可以链接企业内部 app、App Store app 网址或 Apple 商务管理代码或定制 app，用户只需访问这一个目的地即可获得所有相关资源。你可以集中管理和保护这一站点。通过内部 app 门户，员工可以轻松查找他们需要的已获批准资源，而无需联系 IT 部门。

托管内容

托管内容涉及到 App Store app 和定制企业内部 app、帐户和文稿的安装、配置、管理和删除。

- **托管 App。**在 iOS 和 iPadOS 中，托管 app 允许企业使用 MDM 通过无线方式分发免费、付费和企业 app，从而在保护企业数据和尊重用户隐私之间取得适当平衡。托管 app 可以通过 MDM 服务器远程删除，或者当用户从 MDM 删除自己的设备时，也会同时删除托管 app。删除 app 时将同时删除与之关联的数据。如果 app 仍然通过 Apple 商务管理分配给用户，或者用户使用个人 Apple ID 兑换 app 代码，则可以从 App Store 重新下载该 app，但它不会由 MDM 管理。
- **托管帐户。**MDM 可自动设置用户的邮件和其他帐户，帮助他们迅速开始工作。根据具体的 MDM 解决方案提供商以及与内部系统的集成方式，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)。

托管 App 配置

App 开发者可以标识出那些在作为托管 app 安装时可启用的 app 设置和功能。这些配置设置可以在托管 app 安装之前或之后进行安装。例如，IT 可以为 Sharepoint app 建立一组默认偏好设置，使用户无需手动配置服务器设置。

领先的 MDM 解决方案提供商成立了 AppConfig 社区并构建了一个标准模式，供所有 app 开发者用于支持托管 app 配置。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。该社区有助于确立一种更加一致、开放和简约的方式，来配置和保护移动 app，从而提高商务活动中的移动 app 采用率。

进一步了解 AppConfig 社区：

appconfig.org

托管数据流

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

- **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、域以及一些扩展功能也需要遵守托管打开方式限制。
- **单 App 模式。**这一设置让 iOS 或 iPadOS 设备限制为仅运行一个 app，非常适合 Kiosk 或单一用途设备，例如零售销售点或医院签到设备。开发者也可以在他们的 app 内启用这一功能，以便 app 可以自主进入和退出单 App 模式。
- **防止备份。**此限制可防止托管 app 将数据备份到 iCloud 或电脑。如果禁止备份，可在 MDM 删除托管 app 而后用户又重新安装这一 app 时，防止恢复 app 数据。

支持选项

Apple 为 iOS 和 iPadOS 用户以及 IT 管理员提供了各种计划和支持选项。

AppleCare for Enterprise 企业版

对于寻求全方位保障服务的企业而言，AppleCare for Enterprise 企业版可通过电话为你的员工提供每周 7 天的 24 小时技术支持，从而减轻企业内部 Help Desk 的工作量，并对具有重要优先级别的问题一小时内进行回应。该计划可为所有 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 专业支持

AppleCare OS Support 专业支持为 IT 部门提供了针对 iOS 和 iPadOS、macOS 以及 macOS 服务器部署的企业级电话和电子邮件支持。此项服务提供每周 7 天的 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。

面向 iOS 和 iPadOS 设备用户的 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期起 90 天内免费电话技术支持。如果购买适用于 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，此服务的保障期限可以延长至自原始购买日期起两年。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障服务，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 AppleCare 或前往 Apple Store 零售店。如有必要，你的企业可以直接订购更换用的 iPhone、iPad、iPod touch 或随附配件。

进一步了解 AppleCare 计划：

apple.com/cn/support/professional

总结

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，来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 的部署、管理和安全功能：

support.apple.com/zh-cn/guide/deployment-reference-ios

了解适用于 IT 的移动设备管理设置：

support.apple.com/zh-cn/guide/mdm

了解 Apple 商务管理：

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

了解适用于企业的管理式 Apple ID：

[apple.com/business/docs/site/](https://apple.com/business/docs/site/Overview_of_Managed_Apple_IDs_for_Business.pdf)

[Overview_of_Managed_Apple_IDs_for_Business.pdf](https://apple.com/business/docs/site/Overview_of_Managed_Apple_IDs_for_Business.pdf)

了解 Apple at Work：

www.apple.com.cn/business/

了解 IT 功能：

www.apple.com.cn/business/it

了解 Apple 平台安全性：

www.apple.com/security/

浏览可选的 AppleCare 计划：

www.apple.com.cn/support/professional/

了解 Apple 培训与认证：

training.apple.com

联系 Apple 专业服务团队：

consultingservices@apple.com

一些 app 和图书可能无法提供，具体取决于国家或地区和开发者是否选择加入；查看[计划和内容提供情况](#)。某些功能要求使用无线网络连接。某些功能仅适用于部分国家或地区。有关 iCloud 的最低建议系统要求，请访问 support.apple.com/zh-cn/HT204230。

© 2019 Apple Inc. 保留所有权利。Apple、Apple 标志、隔空投送、隔空播放、隔空打印、Apple TV、Bonjour、FaceTime 通话、iMessage 信息、iPad、iPhone、iPod touch、iWork、Mac、macOS 和 Siri 是 Apple Inc. 在美国和其他国家/地区的注册商标。iPadOS 是 Apple Inc. 的商标。App Store、AppleCare、Apple Store、Apple Books、iCloud、iCloud 云盘和 iCloud 钥匙串是 Apple Inc. 在美国和其他国家/地区注册的服务商标。IOS 是 Cisco 在美国和其他国家/地区的商标或注册商标，并已获授权使用。本材料中提及的其他产品和公司名称可能是其各自公司的商标。产品规格会根据情况变动，恕不另行通知。本资料中的信息仅供参考。Apple 对其使用不承担责任。