Mac 部署概述

简介

目录

Mac 与 macOS 强强联手，让员工能够随时随地出色地完成工作。此外，它还能帮助 IT 部门减少管理设备的时间，让他们的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。

本文稿为如何在企业中部署 macOS 设备提供了指导，并且有助于你为制定最符合贵企业环境的部署计划打好基础。

这些主题，包括使用最新 macOS 更新进行部署的最新内容，都在线上“Apple 平台部署”指南中有详细介绍。

所有权模式

以下是企业中用于 macOS 设备的两种常用所有权模式：

- 企业拥有
- 用户拥有

两种模式各有其优势，因此，选择最适合你的企业的模式至关重要。虽然大多数企业都有自己的首选模式，但你可能会在自己的部署环境中遇到多种模式。

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”。“共用的 iPad”就是共享部署的一个示例，这种所有权模式能让多个用户无需共享信息的情况下共用 iPad 设备。企业可在整个企业环境中结合使用“共享部署模式”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。

进一步了解受监督设备的访问限制：
support.apple.com/zh-cn/guide/mdm

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
- 强制执行各项限制
- 访问全部 app 的清单
- 远程抹掉整个设备
- 管理软件更新
- 删除系统 app
- 修改墙纸
- 锁定到单个 app
- 绕过激活锁
- 强制开启 Wi-Fi
- 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，即自带设备办公部署。虽然 BYOD 部署不太常用于 macOS 设备，但你企业仍有可能使用这种模式。要使用企业服务 (例如 Wi-Fi、邮件和日历) 或者配置设备以满足特定的教育或商务要求，用户通常会在企业的移动设备管理 (MDM) 解决方案中注册其设备。这个操作叫做“用户注册”。

“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。这会在设备上创建数据独立。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/zh-cn/guide/mdm

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”
- ✓ 安装与配置 app
- ✓ 要求提供密码
- ✓ 强制执行特定的限制
- ✓ 访问工作 app 清单
- ✓ 仅移除工作数据
- ✗ 访问个人信息
- ✗ 访问个人 app 清单
- ✗ 移除任意个人数据
- ✗ 收集设备上的任何日志
- ✗ 接管个人 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四个步骤：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 Apple 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。Apple 的 macOS 管理框架使企业能够在企业环境中安全地注册设备、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。通过 Apple ID，用户能登录 Apple 服务 (如 FaceTime 通话，iMessage 信息，App Store 和 iCloud)，从而访问各种可提高效率、支持协作的内容和服务。与任何 Apple ID 一样，管理式 Apple ID 用于登录个人设备，是 Apple 设备管理不可或缺的一部分。使用管理式 Apple ID，可以访问 Apple 服务 (包括 iCloud 以及使用 iWork 和“备忘录”app 进行协作)，与个人 Apple ID 的访问方式相同。但管理式 Apple ID 由贵企业拥有和管理，用于密码重置和基于角色的管理等。管理式 Apple ID 有部分设置是受到限制的。

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

Wi-Fi 和联网。Apple 设备内置安全的无线网络连接。请确认你所在公司的 Wi-Fi 网络能够支持多台设备，允许你的所有用户同时连接。Apple 和 Cisco 也优化了 Mac 电脑与 Cisco 无线网络的通信方式，为 macOS 中的高级联网功能 (例如服务质量 (QoS)) 提供了支持。如果你拥有 Cisco 联网设备，请与你的内部团队合作，确保 Mac 能够优化关键流量。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。macOS 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。还有一些 app 和 macOS 的内置功能使用 Bonjour 来发现其他可进行协作和共享的设备。

进一步了解 Wi-Fi 和联网：
support.apple.com/zh-cn/guide/deployment-reference-ios

进一步了解如何为 MDM 配置网络
support.apple.com/zh-cn/HT210060

进一步了解 Bonjour：
developer.apple.com/library

VPN。评估 VPN 基础架构，确保用户可以安全地远程访问企业资源。可以考虑使用 macOS 的 VPN On Demand 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 网关支持这些功能，并购买足够数量的许可证，以便覆盖适当数量的用户和连接。

邮件、内容和日历。iPhone、iPad 和 Mac 可运行 Microsoft Exchange、Office 365 及 G Suite 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 macOS 设备数量准备数量充足的许可。

管理身份。为了管理身份和其他用户数据，macOS 可以访问包含 Active Directory、Open Directory 和 LDAP 的目录服务。一些 MDM 供应商会提供相应的工具，用于将他们的管理解决方案与 Active Directory 和 LDAP 目录快速集成起来。借助 macOS Catalina 中的 Kerberos 单点登录扩展等额外工具，无需传统绑定和移动账户，即可与 Active Directory 策略和功能集成。你的 MDM 解决方案可以管理来自内部和外部证书颁发机构 (CA) 办法的各类证书，以便加入信任白名单，免于认证。

进一步了解新的 Kerberos 单点登录扩展：
support.apple.com/zh-cn/guide/deployment

进一步了解目录集成：
support.apple.com/zh-cn/guide/deployment

核心员工服务。验证 Microsoft Exchange 服务是否为最新，并且已配置为支持网络上的所有用户。如果你不使用 Exchange，macOS 还可与基于标准的服务器配合使用，包括 IMAP、POP、SMTP、CalDAV、CardDAV 和 LDAP。测试电子邮件、通讯录和日历的基本工作流程，以及用户在日常工作中经常用到的其他企业效率与协作软件。

进一步了解如何配置 Microsoft Exchange：
support.apple.com/zh-cn/guide/deployment

进一步了解基于标准的服务：
support.apple.com/zh-cn/guide/deployment

内容缓存。macOS 中内置的缓存服务会存储用户经常向 Apple 服务器请求的内容的本地副本，有助于最大限度地减少在你的网络中因下载内容而被占用的带宽。你可以使用缓存来加快在 Mac App Store 中下载和交付软件的速度。这一功能还可缓存软件更新，以便更快将软件更新下载至企业的 macOS、iOS 或 iPadOS 设备。通过来自 Cisco 和 Akamai 的第三方解决方案还可以缓存其他内容。

进一步了解内容缓存：
support.apple.com/zh-cn/guide/deployment

2. 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。所有的所有权和部署模式在与 MDM 和 Apple 商务管理搭配使用时或通过 MDM 和 Apple Configurator 2 使用时效果最佳。

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 设备并将设备注册到 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。但是，可能有一些 Mac 电脑是从支持“自动设备注册”的常规渠道之外购买或捐赠的。针对这些情况，Apple 推出了适用于新 app：iPhone 版 Apple Configurator。有了 iPhone 版 Apple Configurator，你可以将任何运行 macOS Monterey 的受支持 Mac 分配到贵企业的 Apple 商务管理账户，以便 IT 团队充分利用自动设备注册支持的各种强大设备管理功能。

进一步了解 iPhone 版 Apple Configurator：
support.apple.com/zh-cn/guide/apple-configurator/welcome/ios

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。企业拥有的和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，让用户能够立即开始在其设备上工作。

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，macOS 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。

3. 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。限制包括的功能如抹掉所有内容和设置，从而将 Mac 快速重置为当前操作系统版本，并在重置过程中，以加密方式移除所有用户数据。

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、执行 macOS 更新、远程锁定或擦除设备，或者管理密码。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 Wi-Fi MAC 地址，以及软件详情，例如 macOS 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。此外，MDM 还可以查询关键安全功能的状态，如文件保险箱或内置防火墙。

管理式软件更新

IT 人员可以让用户在最新的操作系统发布时，选择是否升级到最新版本。通过测试 macOS 的预发布版本，IT 人员可以确保尽早发现应用程序兼容性问题，并在最终发布前由开发者解决相关问题。IT 人员可以通过 Apple Beta 版软件计划或 AppleSeed for IT 参与测试每个发布版本。采用全面的措施使 Mac 电脑保持系统最新状态，以保护用户及其数据。确定工作流程与新版本的 macOS 兼容后，需经常进行升级。

MDM 可以自动将 macOS 更新推送到已注册的 Mac 设备。如果关键系统尚未就绪，还可以将已注册的 Mac 设备配置为推迟更新和通知 (最多为 90 天)。在移除相关策略或 MDM 发送安装命令之前，用户将无法手动进行更新。

Apple 不推荐也不支持通过整体系统映像升级 macOS。与 iPhone 和 iPad 一样，Mac 电脑常常需要安装特定于机型的固件更新。同样，更新 Mac 操作系统时也必须直接从 Apple 安装这些固件更新。最可靠的策略是使用 macOS 安装器或 MDM 命令进行更新。

受管理的其他软件

企业通常需要向用户分发初始设定以外的其他 app。对于关键应用程序和更新，这可以由 MDM 自动处理，也可按需分发，即允许员工使用 MDM 解决方案提供的自助服务门户来请求应用程序。这些门户可以完成各种工作，包括通过 Apple 商务管理安装在 App Store 上购买的软件，或非 App Store app、脚本和其他实用工具。

虽然大多数软件可以自动安装，但某些安装可能需要用户介入。为了提高安全性，要求内核扩展的 app 现在需要获得用户同意才能载入。这称为“用户批准的内核扩展载入”，并可由 MDM 进行管理。

4. 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，在任何销售 app 的国家/地区，MDM 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。

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，更快捷，同时保持对受管理的设备和内容的完全控制。将 App 分配到设备后，会通过 MDM 推送到该设备，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。另一个方式是使用你的 MDM 解决方案，通过电子邮件或推送通知信息，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到其他设备和用户，因此，贵企业可保留对所购 app 的完全所有权和控制。

准备其他内容。借助 MDM 解决方案，你可以分发内容并非来自 Mac App Store 的其他软件包。这是个很常见的方法，适用于很多企业软件包，如内部自定义应用程序或 Chrome、Firefox 等 app。可以通过此方法推送所需的软件，并在注册完成后自动安装。字体、脚本或其他内容也可以通过软件包安装并执行。确保已使用 Developer Enterprise Program 中的 Developer ID 对这些软件包正确地进行了签名。

设备安全

Apple 设备从设计上保证安全性。设备设置完成后，你可以通过贵企业的 MDM 解决方案提供的内置安全功能和其他控制措施来管理和保护企业数据。IT 部门可借助 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/zh-cn/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 macOS 设备上通过 MDM 要求提供密码会自动启用“数据保护”，为设备提供文件加密。MDM 还可以用于配置 Wi-Fi、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。内置的各种安全功能可让 IT 部门加密数据，保护设备免受恶意软件的攻击，并强制执行安全设置，而无需第三方工具。

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、iPadOS 和 macOS 设备上，IT 部门可以远程锁定并抹掉所有敏感数据，保护你公司的信息。对于受监督的 macOS 设备，IT 人员可以启用“查找”来查看设备的位置。IT 部门还可使用各种工具来管理企业 app，这些 app 可即时从设备上删除，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 在发布于 App Store 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，带来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管的设备置于丢失模式。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督设备，因为 MDM 可以远程查询这些设备上次在线时的位置。丢失模式不要求“查找我的 ”处于启用状态。

激活锁。在 macOS Catalina 或更新系统中，你可以使用 MDM 解决方案在用户打开受监督设备上的“查找”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

许多企业发现，Mac 用户几乎不需要 IT 部门的技术支持。为了鼓励用户自行解决问题并提高支持质量，大多数 IT 团队都会开发自助工具。例如，开发强大的 Mac 支持网页、提供自助论坛、设立现场技术帮助台等。MDM 解决方案还可以让用户执行一些支持任务，例如通过自助服务门户网站安装或更新软件。

最佳的做法是，企业不应让用户完全依靠企业的支持，而应该采用协作的方式来解决问题。鼓励用户积极参与该流程，让他们在致电 Help Desk 之前，先自行调查并排查问题。

让用户分担支持责任可缩短员工的停机时间，并降低对支持成本和员工的总体影响。对于需要更多支持的企业，AppleCare 提供了多种计划和服务，以补充针对员工和 IT 的内部支持结构。

AppleCare for Enterprise 企业版

对于寻求全方位保修服务的企业而言，AppleCare for Enterprise 企业版通过电话为你的员工提供每周 7 日的 24 小时技术支持，从而减轻企业内部服务台的工作量，并对具有重要优先级别的问题在一小时内进行回应。这个计划能够提供 IT 部门级的整合服务 (包括 MDM 和 Active Directory)。

AppleCare OS Support

AppleCare OS Support 为 IT 部门提供了针对 iOS、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，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 员工在部署管理设备和解决问题时的效率。

AppleCare Help Desk Support

通过 AppleCare Help Desk Support，可以从 Apple 的高级技术支持人员处获得优先电话支持。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 Mac 的 AppleCare 和 AppleCare+ 服务计划

每台 Mac 电脑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。如购买适用于 Mac 的 AppleCare+ 服务计划或 AppleCare Protection Plan 全方位服务计划，此服务的保修期限可以延长至自原始购买日期起三年。员工可以就 Apple 硬件和软件问题致电 Apple 支持团队。当设备需要维修时，Apple 还提供便捷的服务选项。此外，适用于 Mac 的 AppleCare+ 服务计划提供若干次数的意外损坏保修服务，每次均需支付服务费。

进一步了解 AppleCare 支持方案：
apple.com.cn/support/professional

总结和资源

无论你的企业要将 Mac 电脑部署到一部分用户还是整个企业，都有多种方案可选，让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完成工作。

了解 macOS 部署、管理和安全功能：
support.apple.com/zh-cn/guide/deployment/welcome/web

Apple Configurator 使用手册：
support.apple.com/zh-cn/guide/apple-configurator/welcome/ios

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.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

探索 Apple 培训和认证：
training.apple.com

测试 Beta 版软件、访问测试计划并提供反馈：
appleseed.apple.com/sp/zh/welcome