Mac 部署概述

简介

目录

Apple 相信，只要让员工用上最好的工具和技术，他们就能把工作做到最好。我们所有的产品都旨在帮助员工提高创造力和效率，使员工无论在办公室还是外出期间，都能以全新方式开展工作。这也符合员工对现代工作方式的期望，让他们能够接触更丰富的信息，实现零阻力协作和共享，灵活自由地保持连接，随时随地开展工作。

在当今的商务环境中，设置和部署 Mac 电脑从未如此简单。借助 Apple 提供的几项关键服务，结合第三方移动设备管理 (MDM) 解决方案，你的企业可以轻松地大规模部署和支持 Mac。如果你的企业已经在内部部署了 iOS 和 iPadOS 设备，那么很有可能实施 macOS 所需的大部分基础架构工作都已经完成。

凭借 Mac 近期在安全、管理和部署方面的改进，企业可以从整体镜像和传统的目录绑定，过渡到以每个用户为中心的无缝配置模式和部署流程，并且几乎只需用到 macOS 的内置工具。

本文围绕大规模部署 Mac 所涉及的方方面面提供了指导，其中包括了解现有的基础架构、设备管理和精简配置等等。在线《Mac 部署参考》对本文中所介绍的主题有更详细的叙述：
support.apple.com/zh-cn/guide/deployment-reference-macos

准备开始

部署过程中，首先要做的是评估员工目前使用 macOS 的情况，并制定部署策略和推行计划。要确保相关的团队及早参与进来，并与所选计划的愿景和目标保持一致。有些团队一开始会进行小范围概念验证，以发现他们所处环境面临的独特挑战。在现阶段，邀请现有客户参与进来作为更广泛试点的一部分十分关键，这样可以了解设备在整个企业中的使用情况，以及团队是否需要关注某些问题。

根据这个阶段中收集的信息，可以帮助确定哪些岗位和职能会因使用 Mac 而受益最多。然后，IT 部门就能评估是应该让整个企业的员工都能选择使用 macOS，还是向特定工作职能的员工提供这样的选择权。

通常，在这一阶段，还会了解在广泛推行 Mac 之前，需要确保哪些内部 app 和工具能与 Mac 兼容。首先应重点关注那些能够满足大多数用户需求的核心效率、协作和通讯 app。一些关键的企业内部服务 (例如：企业内网、目录和报销管理软件) 也十分重要，可以让企业的大多数部门保持高效运转。

而对于其他内部工具，应记录和传达变通办法或备选方案，同时鼓励每个应用程序负责人根据需要对其进行现代化改造。向用户清楚说明他们在选择 Mac 后可以使用的各种商务 app，并按用户需求确定各种现代化改造的优先顺序。必要时，与应用程序负责人一起制定一份计划，阐明如何利用 macOS SDK 和 Swift 以及可能有助于开发的各种企业合作伙伴，对其 app 进行升级。

Mac 电脑通常会作为企业拥有设备配发。一些企业可能会允许员工通过自带设备 (BYOD) 计划在工作时使用 Mac。无论采用何种所有权模式，让员工自行选择想用的 Apple 产品，都可以为整个企业带来诸多益处：提高员工的效率、创造力、参与度和工作满意度，如果把剩余价值和技术支持考虑在内，还能降低成本。企业还可以利用各种租赁和分期付款方案来降低前期成本。企业也可以让员工以薪资扣款的形式出资参与设备升级，或者让员工在租赁或设备生命周期结束时买下设备，以此来补偿成本。

企业可以根据试点过程中收集的信息，对本文中所描述的企业策略以及部署、管理和支持流程进行调整。每个用户对于策略、设置和 app 的需求不尽相同，正如企业内部不同部门和团队之间的需求往往千差万别。

部署步骤

部署 macOS 有四个主要步骤：准备好环境、设置 MDM，然后将设备部署给员工并完成持续管理任务。

1. 准备

无论是怎样的部署，第一步都是要考虑现有的环境。其中包括深入了解公司的网络和关键基础架构，以及搭建好成功部署所需的系统。

评估基础架构

尽管 Mac 可以无缝集成到大多数标准的企业 IT 环境中，但仍务必要评估公司的现有基础架构，以确保能够充分利用 macOS 提供的各项功能。如果你的企业在这方面需要帮助，可以向 Apple 专业服务团队寻求帮助，也可以从渠道合作伙伴或经销商的技术团队处获得协助。

无线网络

在设置和配置 macOS 设备时，稳定可靠的无线网络至关重要。应当仔细确认企业的 Wi-Fi 网络是否设计合理，要认真考虑接入点的位置和功率，以确保满足漫游和容量需求。

如果设备无法访问 Apple 服务器、Apple 推送通知服务 (APNs)、iCloud 或 iTunes Store，则你可能还需要调整 Web 代理或防火墙端口的配置。就像 iPad 和 iPhone 一样，Mac 部署过程的某些部分 (尤其是较新的 Mac 硬件) 需要访问这些服务，比如在安装过程中更新固件。

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。

企业还需要评估 VPN 基础架构，确保用户能够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。

确保你的网络基础架构设置正确，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 和 macOS 的内置功能还使用 Bonjour 来发现其他可进行协作和共享的设备。

进一步了解 Wi-Fi 网络设计：
support.apple.com/zh-cn/guide/deployment-reference-macos

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

管理身份

macOS 可以通过访问目录服务来管理身份和其他用户数据，包括 Active Directory、Open Directory 和 LDAP。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。而借助 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帐户，即可与 Active Directory 策略和功能集成。MDM 解决方案还可以管理内部和外部证书颁发机构 (CA) 颁发的各类证书，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-reference-macos

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

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-reference-macos

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

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-reference-macos

创建管理解决方案

借助 MDM，企业能够在企业环境中安全地注册 Mac、以无线方式配置和更新设置、部署 app、监控企业策略的合规情况、查询设备，以及远程擦除或锁定托管设备。IT 能够轻松创建描述文件来管理用户帐户、配置系统设置、实施限制及设置密码策略 — 这与当今在 iPhone 和 iPad 上所采用的移动设备管理解决方案是一样的。

所有 Apple 平台的后台都采用了 Apple 的通用管理框架，这使得企业能够使用第三方提供的各种 MDM 解决方案。Jamf、VMware 和 MobileIron 等多家第三方公司提供了众多设备管理解决方案。虽然 macOS 与 iOS 和 iPadOS 的许多设备管理框架都是相同的，但这些第三方 MDM 解决方案在管理功能、操作系统支持、定价结构和托管模式上略有不同。另外，这些第三方解决方案提供的集成、培训和支持服务可能也有所不同。在选择解决方案之前，应评估哪些功能最适合你所在的企业。

选择好使用哪种 MDM 后，你需要访问 Apple 推送证书门户，并在登录后创建一个新的 MDM 推送证书。

进一步了解 MDM 部署：
support.apple.com/zh-cn/guide/deployment-reference-macos

访问 Apple 推送证书门户：
identity.apple.com/pushcert/

注册 Apple 商务管理

Apple 商务管理是一个网页版门户，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 商务管理支持自动化设备注册，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”方案。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：apple.com.cn/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

在设置部署阶段，需要制定企业策略并准备好移动设备管理解决方案，从而为员工配置 Mac。

了解 macOS 的安全性

所有的 Apple 硬件、软件和服务都把安全和隐私放在第一位。我们使用了强大的加密技术，以严格的策略来管理数据的处理方式，从而保护客户的隐私。为了给 Apple 设备提供安全的计算平台，我们采取了以下措施：

- 使用专门的方法来防止他人未经授权使用设备
- 保护静态数据的安全，即使设备丢失或被盗时也不例外
- 在传输中使用网络协议和数据加密
- 驱动 app 安全运行而不损害平台的完整性

所有 Apple 设备均设计了多层安全机制，以便安全地访问网络服务并保护重要数据。macOS、iOS 和 iPadOS 还通过密码和密码策略来提高安全性，密码策略可以借助 MDM 进行分发并执行。如果设备落入他人之手，用户或管理员可以使用远程命令来擦除所有隐私信息。

IT 可以使用 MDM 部署一系列策略来保证设备安全。例如，使用 MDM 执行文件保险箱和恢复密钥托管，强制实施特定的密码策略或屏幕保护程序锁定，以及启用内置的防火墙。

进一步了解 Apple 平台安全性：support.apple.com/zh-cn/guide/security/welcome/web

制定企业策略

制定企业策略的第一步是建立涵盖大多数 Mac 用户的常规策略。MDM 解决方案可以为每个用户自定义策略，如帐户或对某些 app 的访问权限。你还可以为组织团体或其他规模更小的用户群设置特定策略，例如针对不同的部门部署不同的软件或设置。

与内部团队一起更新现有的企业策略，以纳入有关使用 Mac 电脑的内容。一些核心策略在所有平台上均保持不变，如密码复杂度和更换要求、屏幕保护程序超时以及可接受的使用方式。

如果你的企业策略要求使用已在其他平台上使用的特定技术，请了解潜在问题并重新制定策略，以涵盖 macOS 的内置技术。这并非要求所有的电脑都使用特定第三方解决方案来加密整个磁盘，而是应考虑制定一个策略，要求使用文件保险箱对企业数据进行静态加密。如果策略要求使用特定软件来保护设备免受恶意软件的侵害，应培训内部团队使用“门禁”等内置功能，然后更新策略以允许使用这些功能。

在 MDM 中配置设置

为了管理企业策略并确保员工可以访问必要的资源，须在 MDM 解决方案中安全地注册每台 Mac。然后，MDM 解决方案会使用配置描述文件来应用策略和设置。配置描述文件是由 MDM 解决方案创建的 XML 文件，用于向设备分发设置。这些配置描述文件可以自动配置帐户、设置、策略、限制和凭证。可以对其进行签名和加密，以提高系统的安全性。

在 MDM 中完成设备注册后，管理员便可以启动 MDM 策略、查询或命令。只要有网络连接，设备就会通过 Apple 推送通知服务 (APNs) 接收通知，该通知会指示设备通过安全连接直接与 MDM 解决方案通信，从而处理管理员的操作。由于通信仅在 MDM 解决方案和设备之间进行，因此 APNs 不会传输机密信息或专有信息。如果解除对设备的管理，则由相关配置描述文件控制的设置和策略也会被移除。如果需要，企业也可以远程擦除设备。

许多企业会将 MDM 解决方案加入到现有的目录服务中。在自动化设备注册时，macOS 中的“设置助理”可以提醒用户使用他们的目录服务凭证进行登录。在 macOS Catalina 中，新的注册自定义选项允许“设置助理”显示来自云身份识别提供程序的身份验证。在设备被分配给特定用户后，MDM 可以对个人或部门的配置和帐户进行自定义。例如，用户的个人 Microsoft Exchange 帐户可以在注册期间自动配置。还可以使用 802.1x、VPN 等技术的证书标识。

鉴于这些系统所提供的控制性，通常情况下，企业会授予用户对其 Mac 的管理访问权限。这使得企业可以根据需要进行完全个性化的设置，安装 app 并对问题进行故障诊断，同时通过 MDM 保证其对公司策略的控制权。此模式会密切监视用户在被监管状态下对企业 iPhone 或 iPad 所具有的权限类型和控制。

进一步了解配置描述文件：
support.apple.com/zh-cn/guide/deployment-reference-macos

为自动化设备注册做好准备

要在 MDM 中注册设备，最简单的方法就是利用 Apple 商务管理中的自动化设备注册功能运行设置助理。这样可以在无需 IT 参与的情况下进行注册，并且可以简化“设置助理”的某些界面，帮助用户更快地完成注册。

要配置自动化设备注册，你需要通过安全令牌将 MDM 解决方案关联到 Apple 商务管理帐户。两步验证过程可安全地为 MDM 解决方案授权。你的 MDM 供应商可以提供有关具体实施细节的文档。

如果设备已被员工使用或为个人所拥有，则用户可以打开单个配置描述文件，并在“系统偏好设置”中进行验证以完成注册。这称为“用户批准的 MDM 注册”。注册必须通过“设备注册”或通过“用户批准的 MDM 注册”来完成，并管理某些安全敏感设置 (例如内核扩展策略和隐私偏好设置策略控制)。

进一步了解内核扩展载入：
support.apple.com/zh-cn/guide/deployment-reference-macos

进一步了解隐私偏好设置策略控制：
support.apple.com/zh-cn/guide/mdm

为分发 app 做好准备

Apple 提供了广泛的计划来帮助你的企业充分利用一些适用于 macOS 的出色 app 和内容。有了这些功能，你可以向员工分发通过 Apple 商务管理购买的 app，以及自己的内部应用程序，从而为他们提供高效工作所需的一切资源。MDM 也可以分发 app，并为 Mac App Store 中不提供的软件安装软件包。

对于从 Apple 商务管理购买的可在任意国家/地区提供的 app，MDM 解决方案可以通过托管分发进行分发。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 解决方案后，你可以将 app 分配给用户，即使设备上的 App Store 被禁用也无妨。也可以将 app 直接分配到设备上，这样设备上的每个用户都能获取 app，因而更加轻松地完成部署。

进一步了解如何在 Apple 商务管理上购买内容：
support.apple.com/zh-cn/guide/apple-business-manager

进一步了解如何分发 app：
support.apple.com/zh-cn/guide/apple-business-manager

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。

进一步了解如何安装其他内容：
support.apple.com/zh-cn/guide/deployment-reference-macos

3. 部署

macOS 可助你轻松部署设备，根据需要进行个性化设置，而且无需 IT 人员介入即可熟悉并使用设备。

利用设置助理

员工可在电脑启动后使用 macOS 中的设置助理实用工具来设置语言和地区偏好设置，并连接到网络。在连接到互联网后，用户会看到一系列设置助理窗口，这些窗口会引导他们完成设置新 Mac 的基本步骤。在此过程中，已在 Apple 商务管理中注册的设备可自动在 MDM 中注册。还可将已注册设备的 Mac 系统配置为跳过某些界面，如条款和条件、Apple ID 登录、定位服务等等。

在使用设置助理完成初始配置后，可以使用 MDM 部署各种设置，包括定义用户是否对他们的电脑具有完全的管理权限。与在 iPhone 和 iPad 上一样，这既让用户能够控制他们的设备，同时又可确保遵守由 MDM 管理的企业策略和设置。为了让用户在设置助理运行完毕后可以立即展开高效工作，应仅在后台开始下载和安装最关键的应用程序和软件包，且不会干扰员工开始他们的工作。可将较大的应用程序安排在后台下载和安装，或稍后由用户在 MDM 解决方案的自助工具中下载和安装。

配置企业帐户

MDM 可以自动设置邮件和其他用户帐户。根据你使用的 MDM 解决方案及其与内部系统的集成方式，帐户有效负载还可以预先填入用户的名称、电子邮件地址以及用于认证和签名的证书标识。

支持用户个性化设置

让用户对他们的设备进行个性化设置有助于提高工作效率，因为用户可以选择那些最称手的 app 和内容来帮助他们最有效地完成任务和目标。现在，有了管理式 Apple ID 和 macOS Catalina 中的“用户注册”，企业有了新的选择，那就是使用企业所有的 Apple ID 或同时使用个人 Apple ID 来为用户提供 Apple 服务的访问权限。

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)，还有 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员权限。管理式 Apple ID 的部分设置受限。

通过“用户注册”注册的设备需要管理式 Apple ID。“用户注册”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/deployment-reference-macos

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-macos

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 解决方案可以通过一组特定任务管理托管设备。这些任务包括查询设备信息以及启动管理任务，以便对那些违反策略、丢失或被盗的设备进行管理。

查询

MDM 解决方案可查询设备的各种信息，以帮助确保用户维持适当的应用程序和设置。这些查询可能与硬件有关，如序列号或设备型号，也可能与软件有关，如 macOS 版本或已安装应用程序的列表。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。

管理任务

当设备处于托管状态时，MDM 解决方案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。

进一步了解管理任务：
support.apple.com/zh-cn/guide/deployment-reference-macos

管理软件更新

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更新通知 (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，以求变得更完善。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。

管理其他软件

除了一组初始 app 之外，企业经常需要向用户分发其他 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，包括安装通过 Apple 商务管理在 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。

保障设备安全

除了在设备部署之前建立一组初始安全策略之外，你的团队还需要持续监控设备的合规情况，并通过你的 MDM 解决方案尽可能多地提取报告。这可能包括监控每台设备的安全状态或收集有关软件补丁安装的信息。尽管大多数企业愿意使用原生工具来加密和保护每台 Mac，但一些企业可能还需要使用其他文件同步和共享服务或防范数据丢失的工具，以防止企业数据泄露并提供有关敏感数据的深入报告。

iCloud 的“查找我的 Mac”功能可以发起远程擦除，从丢失或被盗的 Mac 上移除所有数据并停用该设备。IT 团队也可以使用 MDM 进行远程擦除。

重新配置设备

当某员工从企业离职时，使用“互联网恢复”和本地“恢复分区”即可轻松地重新配置该员工的 Mac，方便其他用户使用。这一操作会擦除 Mac 中的内容，并安装最新版本的操作系统。Apple 商务管理中分配给特定 MDM 的 Mac 会在“设置助理”阶段通过 MDM 自动完成重新注册、为新用户配置设置、应用企业策略并完成全部适用软件部署。可以通过相同的流程擦除和重新配置未注册的 Mac 电脑，然后手动重新注册。

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，企业不应强制要求用户完全自行解决问题，而是应鼓励用户采用协作的方式来解决问题，而且关键是要为用户提供相应的工具，方便他们在致电服务台之前自行对问题进行故障诊断。鼓励用户积极参与该流程，让他们在致电寻求帮助之前先自行调查问题。

让用户分担支持责任可缩短员工的停机时间，并减少总的支持成本和人员占用。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 专业支持

AppleCare OS Support 专业支持为 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 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 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 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 支持选项：
apple.com.cn/cn/support/professional/

总结

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-reference-macos

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/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：
support.apple.com/zh-cn/guide/security/welcome/web

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