管理设备和企业数据

目录

概述

数据是企业最重要的资产之一。无论用户是在个人设备还是企业提供的设备上访问企业数据，确保个人数据和企业数据彼此独立，都能有效保护数据免受恶意攻击和用户失误的影响。Apple 为 IT 提供了便利，方便他们在帮助用户高效工作的同时，轻松为不同级别的设备管理提供支持。

对于企业拥有的设备，IT 团队可以利用 Apple 商务管理自动完成其注册，无需实际接触或准备每台设备，即可轻松快捷地将设备交付用户。借助监督功能，IT 可以使用其他部署模式无法实现的控制措施，包括额外的安全配置、不可移除的 MDM 以及软件更新管理。

对于通过用户注册管理的个人设备，IT 团队可分别使用管理式 Apple ID 和个人 Apple ID 来区分企业和个人数据，确保企业数据独立于个人数据妥善存放。当员工离职或不再需要访问 app 时，其个人设备中的企业数据均将移除。

Apple 设备管理

Apple 提供了出色的管理工具，让 IT 团队既能顺利实施必要的管控，又不会干扰设备的正常使用。而这离不开 Apple 管理框架与移动设备管理 (MDM) 解决方案的深度整合。

Apple 的设备管理方法

Apple 将管理框架内置于 iOS、iPadOS、Apple 和 macOS 之中，让 IT 团队不仅可以配置和更新设置、部署 app、监控合规性、查询设备，还能远程擦除或锁定设备。该框架支持企业和员工拥有的设备，为设备部署和管理奠定了良好的基础。得益于 Apple 操作系统内置的这一框架，企业能够灵活地进行精细化管理，而不是直接锁定或停用功能。如此一来，IT 团队既能实施必要的管控，又不会影响用户体验，而且仍能保障员工隐私。

什么是 MDM?

Apple 和 MDM 解决方案默契配合，方便 IT 轻松部署设备、分发 app 和配置各项设置，并保护每台设备的安全。

MDM 支持为每台设备配置 app、账户和数据，其中包括各项整合功能，例如密码和策略强制执行。各项控制操作对员工是透明的，同时也确保其个人信息的私密性。如果设备遗失，IT 团队还可安全地远程抹除信息。

无论企业采用云端还是本地服务器，众多 MDM 解决方案供应商将提供丰富的功能与价位选择，帮助企业灵活部署。

有些设备管理方案对于 MDM 功能的命名可能有所不同，例如将其称为企业移动管理 (EMM) 或统一端点管理 (UEM)。不过，万变不离其宗，这些方案都是为了以无线方式管理企业的设备和数据。

MDM 对企业用户有何影响

有了 Apple 的助力，IT 团队能够轻松部署和管理设备，同时仍能保障员工隐私，而且不会干扰日常工作。这意味着，无论设备是归企业还是员工所有，企业都能够更灵活地锁定或停用设备和功能，并进一步限制数据的收集和使用。

这是因为 Apple 实现了企业 app 和数据与个人资源的彼此独立。而且，得益于 Apple 框架与大多数第三方 MDM 解决方案的紧密整合，IT 能够轻松管理 Apple 设备，同时限制接触到的具体信息和设置。无论企业采用何种部署模式，MDM 框架绝不会访问个人信息，包括电子邮件、信息和浏览器历史记录等。

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
- ✓ 强制实施特定的限制
- ✓ 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
- ✗ 远程擦除整个设备
- ✗ 访问设备位置

适合不同设备归属的管理方法

设备可以归企业或员工所有。企业拥有的设备通常采用一对一部署：每位用户都会被分配一台专属设备，并由 IT 团队实施控制。不过，企业拥有的设备也可以供多位员工共用，例如，不同班次的轮班工人共用设备，或零售人员共用一台设备作为手持销售终端 (POS)，都属于共用设备部署。为了管理企业拥有的设备，IT 可以利用监督功能，在不锁定设备的情况下，对配置和限制进行额外的控制。

用户拥有的设备也称为“自带设备”(BYOD)，通过“用户注册”进行管理。得益于这种管理方法，员工能够使用自己的个人设备开展工作。

无论企业选择哪种设备所有权模式，Apple 都支持不同级别的设备管理，同时注重隐私、安全和数据独立。

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

企业拥有的设备

IT 可以配置企业拥有的设备，仅提供员工履行工作职能所需的数据、app 和设置。这些设备可以通过企业的 MDM 解决方案自动部署。直接从 Apple 购买或通过 Apple 授权经销商购买的设备可自动注册到 Apple 商务管理中，并通过零接触部署方式部署，无需 IT 团队逐台配置。

通过部署企业拥有的设备，企业可以实现更高级别的管控，同时保障用户隐私安全，且不会干扰设备的正常使用。在企业拥有的设备注册到位后，IT 团队可控制 Wi-Fi、VPN、邮件和日历设置、配置账户并添加限制，还可以实施多项限制，防止用户在设备上设置个人账户。

在企业拥有的设备上，用户可以使用管理式 Apple ID 或个人 Apple ID，也可以完全不使用，但推荐做法是使用管理式 Apple ID。管理式 Apple ID 可作为企业的专属账户，独立于个人创建的 Apple ID。与个人 Apple ID 不同，管理式 Apple ID 可以访问的服务由 IT 管理员负责管理。此外，通过监督功能，IT 能够使用其他部署模式无法实现的控制措施，包括额外的安全配置、不可移除的 MDM 及软件更新管理。

无论配置的设备是人手一台，还是由参与协作的多位员工共享，企业均可轻松地保护设备上所有数据的安全。

用户拥有的设备

对于使用个人设备工作的员工，IT 可以通过用户注册来管理企业数据。用户注册专为 BYOD 方案而打造，让员工能够保护自己的隐私，同时确保企业数据安全独立并时刻受到保护，从而提供更胜以往的设备个性化体验。IT 团队能够强制执行限定的设置、监控企业的合规情况，还能仅移除企业数据和 app，但无法远程擦除设备、获取设备位置，或者访问设备上的个人信息或 app。用户可以随时移除 MDM 描述文件，这会移除所有企业 app 和数据。而且，与使用企业拥有的设备相比，用户在更新和其他配置方面拥有更多控制权。

要使用用户注册，用户需要同意将设备注册到企业的 MDM 解决方案中。此后，他们便可访问企业资源、配置各种设置，并安装配置描述文件和各类企业 app。

用户注册允许在一台设备上使用个人 Apple ID 和管理式 Apple ID。现有的个人 Apple ID 用于访问用户的所有个人 iCloud 数据。管理式 Apple ID 由企业提供，会将所有企业 iCloud 数据存储在企业的受管理 iCloud 云盘和备忘录中。

在 iOS 15 和 iPadOS 15 中，用户现可直接通过设置 app 注册设备。他们需要前往“设置”，依次选择“通用”、“VPN 与设备管理”，然后轻点“登录工作或学校帐户”，输入管理式 Apple ID 用户名和密码，之后便会进入到身份验证流程。

借助这种数据管理方式，用户能够更加自主地使用自己的设备，同时通过备忘录和 iCloud 云盘 app，将企业数据单独存储在受到加密保护的 Apple 文件系统 (APFS) 宗卷中，从而增强企业数据的安全性。对 BYOD 计划而言，这种方案能够更好地兼顾安全、隐私和用户体验。如果用户因更换受管理设备或离职而取消注册设备，APFS 宗卷中的所有数据都会销毁。

保持企业数据独立的丰富工具

Apple 拥有丰富多样的工具，无论企业选择何种设备所有权模式，均能轻松区分设备上的企业和个人数据。在这一部分，你将了解如何管理保存在受管理的 app、设置、账户中的数据，以及其他相关内容。

受管理的 App

要获得企业分配的 app，设备需要先在 MDM 解决方案中注册。MDM 会将分配的 app 推送到相应的设备。如果企业拥有的设备是通过监督管理的，则 app 会以静默方式安装，无需用户执行操作或提供 Apple ID。

无论设备是归企业还是用户所有，当 IT 或用户从 MDM 中取消设备注册时，存储在受管理 app 中的数据均会删除。IT 团队可以阻止受管理的 app 将数据备份到访达、iTunes 或 iCloud。当用户重新安装 MDM 解决方案移除的受管理 app 时，如果启用了阻止备份这项限制，便可防止用户恢复相应的 app 数据。

受管理的设置

注册到 MDM 之后，用户可以在设置 app 中轻松查看哪些 app 和账户处于受管理的状态，了解实施了哪些限制。由 MDM 安装的所有企业设置、账户和内容都标记为“受管理”。这包括 Wi-Fi 和 VPN 配置以及密码要求。所有设置都可以随时更新或删除。

限制

为了保护企业数据安全，IT 团队需要限制某些共享选项或特定 app 的下载权限。借助 Apple 和 MDM 解决方案，IT 可以利用监督功能，对企业拥有的设备实现更高级别的控制。他们可使用其他部署模式无法实现的控制措施 (例如不可移除的 MDM)，进行额外的设备管理。此外，团队可以实施各种限制，例如停用 iPhone 摄像头、停用 iCloud、停用 Siri 等。

受管理的账户

IT 团队可以管理设备上的企业电子邮件、日历和通讯录，帮助用户更快完成设置并开始使用设备。通过账户管理功能，企业可以阻止用户添加个人的电子邮件、日历和通讯录，以防止用户进行个性化设置，并加强 IT 对设备端数据的掌控。

受管理的扩展

借助 app 扩展，第三方开发者可以将功能扩展至其他 app，乃至操作系统内置的关键系统，在 app 之间实现全新的业务流程。扩展管理可以防止未受管理的扩展功能与受管理的 app 进行交互。比如，文件提供程序扩展允许效率 app 打开各种云服务上的文件，共享扩展让用户能够便捷地与其他实体共享内容，操作扩展允许用户在另一 app 中查看或处理内容。

受管理的打开方式 (适用于 iOS 和 iPadOS)

受管理的打开方式使用以下三个独立的功能来保护企业数据：

- **允许被管理的目的位置中包含来自未被管理的来源中的文稿。**实施这一限制后，可防止来自用户个人来源和账户的文稿在企业的受管理目标位置打开。例如，此限制可阻止用户在企业的 PDF app 中打开任意网站上的 PDF。
- **允许未被管理的目的位置中包含来自被管理的来源中的文稿。**实施这一限制后，可防止来自受管理企业来源和账户的文稿在用户的个人目标位置打开。此限制可防止受管理电子邮件企业账户中的机密附件在用户的任何个人 app 中打开。

- **受管理的粘贴板。**在 iOS 15、iPadOS 15 或更高版本中，此限制有助于控制在受管理和未受管理的目标位置间粘贴内容。实施上述限制后，在第三方或 Apple app (如日历、文件、邮件和备忘录) 之间进行的内容粘贴操作，将遵循受管理的打开方式这一界限。有了这项限制，当内容超出受管理的界限时，app 便无法访问粘贴板中的项目。

归根结底，这三个功能有助于在受管理的设备上区分出两个独立的环境：一个用于访问受管理的企业 app 和数据，另一个则用于未受管理的个人 app 和数据。

使用受管理的打开方式来保持数据独立，有助于打造更积极的用户体验。与锁定整台设备相比，Apple 的管理方法更契合用户需求，同时也能让 IT 团队掌握必要的信息，以便他们能够管理数据来源和目标位置，而不必实施传统的严控手段。

受管理的域名 (适用于 iOS 和 iPadOS)

IT 可以管理 iPhone 和 iPad 上的特定 URL 和子域。例如，如果用户从某个受管理的域下载 PDF，该域会要求 PDF 符合所有受管理的文件设置。域名后面的路径通过默认方式管理。

丢失或被盗的设备

天有不测风云，办公设备有时会丢失或被盗。有了 Apple 和 MDM 解决方案，即使设备丢失，亦可阻止个人随意访问企业数据。MDM 解决方案可以设置通过密码自动开启的数据保护。此外，受管理的各项设置可确保每一台受管理的设备都设有难以破解的密码，为用户提供周全保护。

通过远程锁定丢失的 macOS 设备，或为丢失的 iOS 或 iPadOS 设备启用丢失模式，IT 团队可以轻松锁定设备，直到用户输入正确的密码才允许访问。如果找不到设备，MDM 解决方案可以远程锁定并擦除设备，确保其他任何人都无法访问敏感的企业数据。

身份管理

不管企业以何种规模部署 Apple 设备，也不管用户需要访问的是设备、网站、app 还是服务，身份识别都已成为用户身份验证的一大核心。身份识别已紧密整合到所有操作系统之中，可为用户提供干净利落的无缝体验。得益于此，不仅用户能够随时随地工作，IT 团队也能获得所需的透明度和控制力。借助卓有成效的身份管理做法，IT 团队既能防患于未然，也能在发生数据泄露后采取明确的对策。为此，Apple 开发了丰富的工具和技术，以下是几个具体的例子。

设备身份验证

Apple 设备的身份管理始于设备身份验证 (即锁定屏幕或登录窗口)，用户验证通过，便可访问整台设备。无论员工共用的是 iPad 还是 Mac，都可以选择自己的账户，输入自己的凭证并获得个性化设备体验。通过设备身份验证，IT 团队可以清楚地了解命令的数据链，例如谁访问了哪些文件，以及与谁共享了这些文件。在共用的 iPad 上，设备身份验证通过管理式 Apple ID 实现；在共用的 Mac 上，用户可以通过本地或网络账户登录设备。

单点登录扩展

单点登录 (SSO) 扩展通过 MDM 解决方案进行配置，让原生 app 和 WebKit 能够提供更流畅的单点登录体验。这意味着，企业用户能够使用现有凭证安全访问 app，而无需另外创建登录名和密码。在 macOS Big Sur 和 iPadOS 14 中，IT 团队可以通过共用的 Mac 和 iPad 在 macOS 和 iPadOS 上配置 SSO 扩展。在 macOS 中，借助 Kerberos 单点登录扩展等额外工具，无需传统绑定和移动账户，即可充分整合 Active Directory 策略和功能。MDM 解决方案可以管理来自内部和外部证书颁发机构 (CA) 的证书，因此，在用户访问受管理员信任的安全服务时，系统便可使用客户端证书进行透明的身份验证。

管理式 Apple ID

在 Apple 商务管理中，IT 团队使用管理式 Apple ID 来管理其企业的设备和 app 购买项目。通过管理式 Apple ID，IT 团队还可以充分利用联合身份验证这一简单又安全的身份管理框架。借助使用管理式 Apple ID 的联合身份验证，Apple 商务管理中的注册企业能够与其现有的身份验证系统关联。这一功能会自动为用户设置 Apple 服务访问权限，而无需创建新的登录凭证。换言之，当用户首次使用联合身份验证登录 Apple 设备时，系统会自动创建访问 Apple 服务所需的管理式 Apple ID。对于 IT 团队和用户来说，联合身份验证减少了账户方面的开销，可确保企业内所有投入使用的 app 和服务都能贯彻身份管理策略。

总结

哪里有员工，哪里就有企业数据，因此确保企业数据受到保护至关重要。借助 Apple 管理框架和企业的 MDM 解决方案，无论用户在何处办公，Apple 都能助其一展所长。

管理企业的所有设备和完善数据独立框架，皆非一日之功。在这个不断精进的过程中，请别忘了以下要点：

- 部署企业拥有的设备，让 IT 部门更能有力管控和保护企业数据。
- 通过用户注册管理用户拥有的设备，既能妥善保护企业数据，又无需访问个人数据，让用户隐私得到保障。
- 保护用户的隐私和安全，与保护企业数据同等重要。
- 企业上下齐心协力，才能有效管理设备和数据，而卓越的 IT 团队还会兼顾用户体验。

其他资源

了解 Apple 设备部署：
support.apple.com/zh-cn/guide/deployment/welcome/web

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

了解 Apple 培训与认证：
training.apple.com