适用于企业的管理式 Apple ID 概览

在企业组织内使用 Apple 产品时，请务必了解管理式 Apple ID 如何为员工提供其所需的服务支持。管理式 Apple ID 是专为企业组织设计的帐户，使其能够访问关键 Apple 服务。

企业组织可以利用 Apple 商务管理自动为员工创建管理式 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 中访问企业数据。使用联合身份验证，这些帐户与每个企业组织拥有并管理的现有基础架构使用相同的凭证。

什么是管理式 Apple ID?

像其他 Apple ID 一样，管理式 Apple ID 用于对设备进行个性化设置。还用于访问 Apple app 和服务，并使 IT 团队能够访问 Apple 商务管理。与 Apple ID 不同的是，管理式 Apple ID 由每个企业组织拥有和管理，包括密码重置和基于角色的管理。

Apple 商务管理可以轻松为企业组织中的每位员工创建唯一的管理式 Apple ID。由于与 Microsoft Azure Active Directory 进行整合，企业组织可以使用其现有的企业凭证向员工提供管理式 Apple ID。

如果企业组织利用 iOS、iPadOS 和 macOS Catalina 中的“用户注册”，则可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 (也是唯一的) 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。

使用 Apple ID 部署设备没有任何技术要求。不使用 Apple ID 的情况下，也可以管理 Apple 设备并向设备分发 app。查看贵企业组织计划使用的服务，然后评估转换到管理式 Apple ID 的最佳途径。由于管理式 Apple ID 仅用于商业用途，因此禁用了某些功能以保护各企业组织的安全。

适用于企业组织的功能

- **访问 Apple 服务。**员工可以使用 Apple 服务，包括 iCloud 以及通过 iWork 和“备忘录”进行协作)。电子邮件功能已禁用，并且只有当管理式 Apple ID 是设备上的唯一 Apple ID 时，才能使用 FaceTime 通话和 iMessage 信息。
- **用户帐户查找。**使员工能够搜索 Apple 商务管理的企业组织中其他用户的联系方式，从而让员工更轻松地通过 app 相互协作。
- **帐户创建，化繁为简。**使用 Apple 商务管理，员工首次登录 Apple 设备时会自动创建帐户。
- **联合身份验证。**管理员可以将 Apple 商务管理与 Microsoft Azure Active Directory 进行连接，以便使用其现有的企业凭证自动为其员工进行设置。
- **角色和权限。**管理员可以为 IT 团队创建并分配角色和权限，以使用 Apple 商务管理中的不同功能。
- **内置的隐私和安全保护。**管理式 Apple ID 使用与标准 Apple ID 相同的数据加密保护，并且屏蔽了 Apple 广告平台上的定向广告。交易功能已被停用，同样也无法使用 Apple Pay 和“钱包”等服务。“查找”功能已被停用，因为企业组织可以通过 MDM 使用“丢失模式”功能。

联合身份验证

通过联合身份验证，你可以将 Apple 商务管理与 Microsoft Azure Active Directory (Azure AD) 进行连接，使员工可以将其现有用户名和密码作为管理式 Apple ID 使用。

Microsoft Azure AD 是身份识别提供程序 (IdP)，其中包含你想要在 Apple 商务管理中使用的帐户的用户名和密码。

通过与 Microsoft Azure AD 整合，管理式 Apple ID 遵循完全相同的密码策略，因为它们是与现有凭证联合在一起的。

用户登录其 Apple 设备时，系统会自动创建管理式 Apple ID，因此 IT 管理员无需花时间来事先完成各项创建。

然后，员工可以使用其现有的 Azure AD 凭证访问 Apple 服务，包括“iCloud 云盘”、“备忘录”、“提醒事项”和协作功能。

鉴于由企业组织管理身份，因此所有密码策略和重置均由企业组织或 Microsoft Azure AD 中的用户来处理。

使用联合身份验证的要求

- **Microsoft Azure Active Directory**。如果你已设置了 Microsoft Azure Active Directory，就可以开始使用联合身份验证了。
- **本地 Active Directory**。还需要完成其他一些设置步骤，才能与 Azure AD 同步。以下是 Microsoft 提供的文档和同步工具链接。

设置联合身份验证的方法

1. **通过 Apple 验证域名**。以“管理员”或“人员经理”的身份登录 Apple 商务管理，添加你希望使用联合身份验证的一个或多个域名。
2. **连接到 Microsoft Azure Active Directory 并授予 Apple 商务管理访问权限**。使用“全局管理员”或“应用程序管理员”帐户登录到 Azure AD，并接受允许 Apple 商务管理读取用户配置文件的权限。
3. **通过 Microsoft Azure Active Directory 验证域名所有权**。建立信任关系后，继续进行验证域名过程。使用一个以你打算联合的域名结尾的帐户，从 Apple 商务管理登录到 Microsoft Azure AD。此步骤可验证域名设置并证明其所有权。
4. **检查域冲突**。Apple 商务管理将检查你的域中与任何现有 Apple ID 存在的潜在冲突。冲突可能是由于个人 Apple ID 或其他企业组织设置的管理式 Apple ID 使用了相同的域名造成的。
5. **启动域冲突解决**。如果 Apple 商务管理在你打算联合的域中检测到个人 Apple ID，这些用户会收到通知，并需要更改其 Apple ID 的电子邮件地址。所有购买内容和数据仍将与用户的个人 Apple ID 保持关联。
6. **迁移现有帐户**。如果你已拥有管理式 Apple ID，则可以通过更改其详细信息以使其与联合身份验证域名和用户名匹配，将其迁移到联合身份验证。

资源

- Apple 商务管理入门指南
- Apple 商务管理使用手册
- 了解在 Apple 商务管理中创建管理式 Apple ID 的方法
- Apple 商务管理联合验证简介
- 进一步了解有关与现有 Apple ID 冲突的信息
- 进一步了解将本地 AD 与 Azure AD 集成的方法