Overview of Managed Apple IDs for Business

When using Apple products within your organization, it's important to understand how Managed Apple IDs support the services your employees may need. Managed Apple IDs are accounts designed specifically for businesses that enable access to key Apple services.

Organizations can use Apple Business Manager to automatically create Managed Apple IDs for employees to collaborate with Apple apps and services, as well as access corporate data in managed apps that use iCloud Drive. With federated authentication, these accounts use the same credentials as existing infrastructure that is owned and managed by each organization.

What are Managed Apple IDs?

Like any Apple ID, Managed Apple IDs are used to personalize a device. They're also used to access Apple apps and services, and for IT teams to be able to access Apple Business Manager. Unlike Apple IDs, Managed Apple IDs are owned and managed by each organization, including password resets and role-based administration.

Apple Business Manager makes it easy to create a unique Managed Apple ID for each employee in an organization. Because of integration with Microsoft Azure Active Directory, organizations can provide Managed Apple IDs to employees using their existing corporate credentials.

Managed Apple IDs can be used alongside a personal Apple ID on employee-owned devices when organizations leverage User Enrolment in iOS, iPadOS, and macOS Catalina. Alternatively, Managed Apple IDs can be used on any device as the primary—and only—Apple ID. Managed Apple IDs can also access iCloud on the web after signing in to an Apple device for the first time.

There is no technical requirement to deploy devices with an Apple ID. Apple devices can be managed and apps can be distributed to devices without an Apple ID. Review the services that your organization plans to use and assess the best path for transitioning to Managed Apple IDs. Because Managed Apple IDs are for business purposes only, certain features are disabled to protect each organization.

Features for organizations

- **Access to Apple services.** Employees can use Apple services including iCloud and collaboration with iWork and Notes. Email is disabled and use of FaceTime or iMessage is only available when a Managed Apple ID is the only Apple ID on a device.
- **User account lookup.** Enable employees to search for the contact information of other users in your Apple Business Manager organization, making it easier for employees to collaborate with each other across apps.
- **Streamlined account creation.** With Apple Business Manager, accounts are automatically created when employees sign-in on an Apple device for the first time.
- **Federated authentication.** Administrators can connect Apple Business Manager with Microsoft Azure Active Directory so that their employees are automatically set up using their existing corporate credentials.
- **Roles and privileges.** Administrators can create and assign roles and privileges for IT teams to use different functions within Apple Business Manager.
- **Privacy and security built-in.** Managed Apple IDs use the same data encryption protections as standard Apple IDs and are blocked from targeted advertising on Apple's ad platform. Commerce is disabled, as well as access to services like Apple Pay and Wallet. Find My is disabled because organizations can use Lost Mode using MDM.

Federated Authentication

With federated authentication, you can connect Apple Business Manager to Microsoft Azure Active Directory (Azure AD) enabling employees to use their existing user names and passwords as Managed Apple IDs.

Microsoft Azure AD is the Identity Provider (IdP), which contains the user names and passwords for the accounts you want to use with Apple Business Manager.

By integrating with Microsoft Azure AD, Managed Apple IDs follow the exact same password policies because they are federated with existing credentials.

Managed Apple IDs are automatically created when users sign in on their Apple device so IT administrators don't need to spend time to create everything in advance.

Employees can then use their existing Azure AD credentials to access Apple services including iCloud Drive, Notes, Reminders, and collaboration.

Since the organization already manages the identity, all password policies and resets are handled by the organization or the user in Microsoft Azure AD.

Federated Authentication Requirements

- **Microsoft Azure Active Directory.** Get started with federated authentication if you already have this in place.
- **On-premise Active Directory.** There are additional setup steps to synchronized with Azure AD. Microsoft offers documentation and a sync tool linked below.

How to Set Up Federated Authentication

1. **Verify domain with Apple**. Sign in to Apple Business Manager as an Administrator or People Manager and add the domain(s) you wish to federate.
2. **Connect to Microsoft Azure Active Directory and grant access to Apple Business Manager.** Use a Global Administrator or Application Administrator account to sign in to Azure AD and accept permissions to allow Apple Business Manager to read user profiles.
3. **Verify domain ownership with Microsoft Azure Active Directory.** With trust established, continue the process to verify the domain(s). From Apple Business Manager, sign in to Microsoft Azure AD with an account that ends in the domain you intend to federate. This step verifies domain set up and proves ownership.
4. **Check for domain conflicts.** Apple Business Manager will check for potential conflicts with existing Apple IDs in your domain(s). These may be personal Apple IDs or Managed Apple IDs set up by another organization using the same domain.
5. **Initiate domain conflict resolution**. If Apple Business Manager detects a personal Apple ID in the domain(s) you intend to federate, these users will be notified and will need to change the email addresses for their Apple IDs. All purchases and data will remain associated with a user's personal Apple ID.
6. **Migrate pre-existing accounts.** If you have existing Managed Apple IDs, you can migrate them to federated authentication by changing their details to match the federated domain and username.

Resources

- Apple Business Manager Getting Started Guide
- Apple Business Manager User Guide
- Learn more about creating Managed Apple IDs in Apple Business Manager
- Intro to federated authentication with Apple Business Manager
- Learn more about conflicts with existing Apple IDs
- Learn more about integrating on-premise AD with Azure AD