Getting Started Guide

Apple Business Manager

Overview

Contents

Apple Business Manager is a web-based portal for IT administrators to deploy iPhone, iPad, iPod touch, Apple TV, and Mac all from one place. Working seamlessly with your mobile device management (MDM) solution, Apple Business Manager makes it easy to automate device deployment, purchase apps and distribute content, and create Managed Apple IDs for employees.

The Device Enrollment Program (DEP) and the Volume Purchase Program (VPP) are now completely integrated into Apple Business Manager, so organizations can bring together everything needed to deploy Apple devices. These programs will no longer be available starting December 1, 2019.

Devices

Apple Business Manager enables automated device enrollment, giving organizations a fast, streamlined way to deploy corporate-owned Apple devices and enroll in MDM without having to physically touch or prepare each device.

- Simplify the setup process for users by streamlining steps in Setup Assistant, ensuring that employees receive the right configurations immediately upon activation. IT teams can now further customize this experience by providing consent text, corporate branding or modern authentication to employees.
- Enable a higher level of control for corporate-owned devices by using supervision, which provides additional device management controls that are not available for other deployment models, including non-removable MDM.
- More easily manage default MDM servers by setting a default server that's based on device type. And you can now manually enroll iPhone, iPad, and Apple TV using Apple Configurator 2, regardless of how you acquired them.

Content

Apple Business Manager enables organizations to easily buy content in volume. Whether your workforce uses iPhone, iPad, or Mac, you can provide great content that's ready for work with flexible and secure distribution options.

- Purchase apps, books, and custom apps in bulk, including apps you develop internally. Easily transfer app licenses between locations and share licenses between purchasers within the same location. And see a unified listing of purchase history, including the current number of licenses in use with MDM.
- Distribute apps and books directly to managed devices or authorized users, and easily keep track of what content has been assigned to which user or device. With managed distribution, control the entire distribution process, while retaining full ownership of apps. Apps that aren't needed by a device or user can be revoked and reassigned within the organization.
- Pay using multiple payment options, including credit cards and purchase orders. Organizations can buy Volume Credit (where available) from Apple or from an Apple Authorized Reseller in specified amounts of local currency, which is delivered electronically to the account holder as store credit.

- Distribute an app to devices or users in any country where the app is available, enabling multinational distribution. Developers can make their apps available in multiple countries through the standard App Store publishing process.

Note: Book purchases in Apple Business Manager are not available in certain countries or regions. To learn which features and purchasing methods are available where, visit support.apple.com/HT207305.

People

Apple Business Manager provides organizations with the ability to create and manage accounts for employees that integrate with existing infrastructure and provide access to Apple apps and services as well as Apple Business Manager.

- Create Managed Apple IDs for employees to collaborate with Apple apps and services, as well as access work data in managed apps that use iCloud Drive. These accounts are owned and controlled by each organization.
- Leverage federated authentication by connecting Apple Business Manager with Microsoft Azure Active Directory. Managed Apple IDs will be created automatically as each employee signs in for the first time with their existing credentials on a compatible Apple device.
- Use Managed Apple IDs on an employee-owned device alongside a personal Apple ID with the new User Enrollment features in iOS 13, 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.
- Designate other roles for IT teams in your organization to effectively manage devices, apps and accounts within Apple Business Manager. Use the Administrator role to accept terms and conditions if needed and easily transfer responsibility if someone leaves the organization.

Note: iCloud Drive is not currently supported with User Enrollment. iCloud Drive can be used with a Managed Apple ID when it is the device's only Apple ID.

Getting Started

Signing Up for Apple Business Manager

Enrollment is simple and takes only a few minutes, so you can get started with Apple Business Manager quickly. Any business is eligible to participate, subject to the service terms and conditions. Apple reserves the right to determine program eligibility for each organization.

To get started, complete the online enrollment process and provide information about your organization, including name, phone number, and a valid D-U-N-S number for your company. D-U-N-S numbers are assigned to qualified businesses by Dun & Bradstreet (D&B), and are maintained in the D&B database.

Click here to look up an existing D-U-N-S number or to obtain a new one. Apple will cross-check program enrollees with the D&B database. If any information you provide doesn't match the information on file with D&B, you'll be notified so you can check and correct it. If you feel the information you provided is accurate, contact D&B to ensure its database records are up to date.

You'll need to provide an email address that's associated with your business. Consumer email addresses from services such as Gmail or Yahoo Mail won't be accepted. The account associated with this email address becomes the initial administrator for Apple Business Manager and can't be associated with an existing Apple ID or any other Apple services.

Provide a verification contact who can confirm the initial site administrator and verify that they have the authority to bind your organization to the Apple Business Manager terms and conditions. This administrator will also be responsible for accepting the terms and conditions and for setting up additional administrators to manage the service on behalf of your company.

Apple will review the information you submit on your program enrollment form. During the review process, you and your verification contact may be asked for additional information by phone or email before your enrollment is approved. Make sure that filters allow mail from all apple.com domains. Return missed phone calls or emails quickly so the enrollment process can proceed smoothly.

When your business is approved, the verification contact will receive an email requesting that they confirm the initial administrator or delegate administration. After confirmation, the administrator will be asked to create the initial administrator Managed Apple ID and agree to the Apple Business Manager agreement and any additional terms and conditions.

Upgrading to Apple Business Manager

If your organization currently uses the legacy Device Enrollment Program or Volume Purchase Program, you need to upgrade to Apple Business Manager before December 1, 2019. For more information, visit support.apple.com/HT208817

If your organization is already enrolled in Apple Deployment Programs, you can upgrade by logging in to deploy.apple.com using your Apple Deployment Programs Agent account and following the onscreen instructions. The upgrade process takes only a few minutes. After you upgrade, Apple Business Manager will have your accounts, MDM servers, devices, server tokens, device orders, and other items associated with your account.

Your organization might have one or more separate VPP accounts. If you have VPP Purchasers that were not included when you upgraded to Apple Business Manager, learn how to invite them into Apple Business Manager by visiting support.apple.com/HT208817.

After you upgrade to Apple Business Manager, you'll no longer have access to the Apple Deployment Programs website.

Configuration

Now that your organization has enrolled in Apple Business Manager, you can add additional accounts, enter purchase information, and assign roles to begin managing devices and content.

Create additional administrators and assign roles

At first login, the initial administrator will be alerted that only one administrator account exists. To create additional administrators:

1. Click Accounts in the sidebar.
2. Click the Add a new account button at the top of the window.
3. Enter the required information, which includes first and last name, Managed Apple ID, administrator role and location, and email address.
4. If necessary, enter the middle name, which is optional.
5. Click Save at the bottom right of the window.

Every Apple Business Manager account has one or more roles assigned to it, which define what the user of the account can do. For example, an account might have the roles of both Device Manager and Content Manager.

In addition, certain roles can manage other roles. For example, an account with the role of People Manager can act on an account that has the role of Content Manager. In this way, the People Manager role can also buy apps and books. It's a good idea to plan role assignments and review role types before creating accounts and assigning privileges.

Configure Federated Authentication

You can use federated authentication to link Apple Business Manager to your instance of Microsoft Azure Active Directory (AD). As a result, your users can leverage their Microsoft Azure AD user names and passwords as Managed Apple IDs. They can then use their Microsoft Azure AD credentials to sign in to a compatible Apple device and even iCloud on the web. To get started:

1. In Apple Business Manager, sign in with an account that has the role of Administrator or People Manager.
2. Go to Accounts under Settings and click Edit in the Federated Authentication section, then click Connect.
3. Select "Sign in to Microsoft Azure" using an account with Microsoft Azure AD Global Administrator, Application Administrator, or Cloud Application Administrator administrative role.
4. Enter the domain name you want to use. Only domains that haven't been claimed by another organizations can be added to federation.
5. Select "Open Microsoft Sign In" and enter credentials for a Microsoft Azure AD Global Administrator, Application Administrator, or Cloud Application Administrator account that exists in the domain specified in the previous step.

When you configure federated authentication, Apple Business Manager checks to learn whether your domain name is already part of any existing Apple IDs. If someone else is using an Apple ID that contains the domain you want to use, that Apple ID user name can be reclaimed from the user so that your organization can use it. For more information, visit support.apple.com/HT209349

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. If a different organization has Managed Apple IDs in the domain that you want to use, Apple will investigate who owns the domain and notify you when the investigation is complete. If more than one organization has a valid claim to the domain, no organization can federate it.

After you've completed a successful administrator account sign-in and the user name conflict check is complete, you can turn on federated authentication by doing the following:

1. In Apple Business Manager, sign in with an account that has the role of Administrator or People Manager.
2. Select Settings at the bottom of the sidebar, select Accounts, then select Edit in the Federated Authentication section.
3. Turn on federated authentication for the domains that have been successfully added to Apple Business Manager.

For more information about setting up federated authentication with Microsoft Azure AD, visit the Apple Business Manager User Guide at support.apple.com/guide/apple-business-manager.

Enter purchase information

To use automated device enrollment, you'll need to review and update the information regarding how you purchase devices. Select Device Management Settings, then add your Apple Customer Number or Reseller ID. If your organization purchases directly from Apple and from a participating Apple Authorized Reseller or carrier, you should enter both your Apple Customer Number and the reseller's Reseller ID.

- **Apple Customer Number.** If you purchase hardware or software directly from Apple, your organization is assigned an account number. This number is required to connect eligible orders and devices to Apple Business Manager. If you don't know the number, contact your purchasing agent or finance department. Your organization might have multiple Apple Customer Numbers, which you can add into Apple Business Manager once you're approved.
- **Organization ID.** Once enrolled in the program, you'll be assigned an Organization ID, found in Apple Business Manager in the Settings section. If you purchase Apple devices from a participating Apple Authorized Reseller or carrier, you'll need to provide this number to the reseller or carrier to enroll your device purchases into Apple Business Manager.

- **Reseller ID.** If you purchase hardware or software directly from a participating Apple Authorized Reseller or carrier, you'll need to provide your reseller's Reseller ID. If you don't know this number, contact your reseller. If you purchase from multiple resellers, enter the Reseller ID of each. You must also provide your Organization ID to your reseller so that they can submit your device purchases. Providing the Reseller ID alone is insufficient to enroll your devices in Apple Business Manager.
- **Apps and Books.** To enable app and book purchases, go to Apps and Books under Settings. Follow the steps to agree to the Apps and Books terms and to update billing information. You can also review purchase history and transfer purchases from one location to another in Apps and Books settings.

Manage device assignments

Apple Business Manager integrates all the existing features from the Device Enrollment Program (DEP). Additionally, MDM servers can now be set as default based on device type, enabling you to set one server as default for Mac and another as default for iPhone and iPad.

Link your MDM solution. To link your MDM solution go to Settings > Device Management Settings, you'll establish a connection to your MDM server or servers. Servers listed in Apple Business Manager are linked to your physical MDM servers. You can add servers at any time.

Add a new MDM server by providing a name and authorization information. Each server must be known to Apple and authorized to manage your devices. A two-step verification process is used to securely authorize an MDM server. Your MDM vendor can provide documentation on the specifics for implementation.

Assign devices. You can assign devices to your servers by order number or by serial number. Only eligible devices will be available for assignment to your MDM server on the program website.

You can search for orders you placed directly with Apple after March 1, 2011, either by order or by serial number. If you've placed orders from a participating Apple Authorized Reseller or carrier, your look-back period will be at the discretion of the reseller. Your order will be available in Apple Business Manager within 24 hours after the reseller successfully posts it.

You can also download a comma-separated value (CSV) file that contains the full list of all devices in a specific order or orders. Devices are listed by serial number in the CSV file. By typing 'All Available' in the order field, a complete listing of all of the devices will be available. By designating a MDM server as the default, you can automatically assign newly purchased devices to it.

If you've acquired devices from sources other than Apple or participating Apple Authorized Resellers or carriers, they can also be added to Apple Business Manager using Apple Configurator 2. Manually enrolled devices you set up behave like any other enrolled device, with mandatory supervision and MDM enrollment. However, the user has a 30-day provisional period to remove the device from enrollment, supervision, and MDM.

Learn more about how to manually enroll devices: support.apple.com/guide/apple-configurator-2/cad99bc2a859

Note: Per the terms of the agreement, devices that are sold, lost, returned to the reseller, or otherwise retired from service should be permanently removed from your organization's list of managed devices using Apple Business Manager. However, once a device is removed, it can't be added back again, unless it is enrolled manually through Apple Configurator 2 for supported devices.

Review assignments. Once you've set up your MDM servers and assigned devices, you can review several aspects of your device assignment, including:

- Assignment date
- Order numbers
- Name of the MDM server to which the devices are assigned
- Total number of devices, listed by device type

Purchase content

Apple Business Manager provides a streamlined purchasing process. You can search for content, specify the quantity you want to purchase, and quickly complete the transaction using VPP Credit or a corporate credit card.

Search for an app or a book. To narrow your search options, select media type iOS and iPadOS apps, Mac apps, or Books. Click the Category pull-down menu to find apps and books by category. Universal apps that work on both iPhone and iPad are identified with the universal badge.

Enter the quantity. Once you've found the content you're interested in, select the name in the search list, review the content details, and enter the quantity you want to purchase.

Distribute and download content

With managed distribution, use your MDM solution or Apple Configurator 2 to manage apps and books distribution.

Link your MDM solution. To use MDM for distribution, you must first link your MDM solution to a location in Apple Business Manager using a secure token. To download your token, go Settings > Apps and Books and select the appropriate location token. Upload this token to your MDM server to establish the link.
Note: Secure tokens expire after one year.

If you're using Apple Configurator 2 to manage devices and content, simply sign in with the applicable Content Manager account using the Account menu. With iOS 10 and macOS Sierra and later, you can save time and network bandwidth by preloading apps for all your deployments through this method.

Once connected to your MDM server, you can assign apps and books—including newly assigned apps and app updates—in a variety of ways to devices and users, even if the App Store is disabled.

Assign apps to devices. If your organization needs to retain full control over managed devices and content, or if it's not practical for every user to obtain an Apple ID, you can assign apps directly to devices using your MDM solution or Apple Configurator 2. After an app is assigned to a device, it's pushed to that device by MDM or added by Apple Configurator 2; no invitation is required. Anyone using that device has access to the app. To assign apps to devices, you'll need one managed distribution license per device.

Assign apps and books to users. Use your MDM solution to invite users through email or a push notification message. To accept the invitation, users sign in on their devices with a personal Apple ID. Although your business can assign apps and books to a user's Apple ID, the Apple ID remains completely private and not visible to the administrator. Once users agree to the invitation and accept the terms and conditions, they're connected to your MDM server and they can download assigned apps and books. Or you can install the app silently on supervised iOS and iPadOS devices. Assigned apps are automatically available for download on all of a user's devices, with no additional effort or cost to you. To assign apps and books to users, you'll need one managed distribution license per user.

Note: If you previously assigned apps to users, MDM solutions can perform a silent migration from per-user assignments to per-device assignments. The device must be enrolled in an MDM solution. Refer to your MDM solution's documentation for support.

Revoke and reassign apps. When apps you've assigned are no longer needed by a device or a user, you can revoke and reassign them to different devices or users. If the app is assigned to a user, the user will have the opportunity to buy a personal copy. If the app was deployed as a managed app with MDM for iOS or iPadOS, the administrator has the additional option of removing the app and all data immediately. In this case, it's a best practice to give users some notice or a grace period before removing apps from their devices. Once distributed, books remain the property of the recipient and can't be revoked or reassigned.

Important Information about app assignment

Admins can assign apps to devices in any country or region where an app is sold through the App Store. For example, an app purchased from an account in the United States can be assigned to devices or users in France as long as the app is available through the App Store in France.

You can use an MDM solution to assign apps only to users whose devices are running iOS 7 or later and macOS 10.9 or later. Assigning apps directly to devices without an Apple ID requires iOS 9 or later and macOS 10.10 or later.

Purchase and distribute custom apps

By collaborating with a third-party developer, you can have unique iOS and iPadOS apps tailored to your business needs, then distribute them at scale to your organization along with off-the-shelf App Store apps—further extending the use of iPhone and iPad. Whether you outsource development to an independent contractor or a commercial developer, or distribute your own apps internally, distributing custom apps through Apple Business Manager is the simplest method for both you and your organization.

Custom apps built for your business are made available to only you; no other organization can see or get them, making the transaction both secure and private. Apple reviews custom apps before they're available to your account, so you can be assured that they've been verified technically and checked for quality. Pricing for custom apps is set by the developer or designated as free.

Common ways to customize apps include incorporating company branding into the user interface or adding unique capabilities that are pertinent to a business process or workflow. Developers can also add a specific configuration for your environment or add features tailored to a business partner, dealer, or franchise.

Work with your developer. To get started, get in touch with a developer. Developers who are registered in the Apple Developer Program and who have agreed to the latest Program License Agreement can submit apps for custom app distribution through App Connect. If your preferred developer or business partner isn't registered in the Apple Developer Program, refer them to developer.apple.com/programs to enroll. Once the developer has created an app and identified you as the authorized purchaser, they can offer the app for free or set a price just for you. Provide your developer with either the Organization ID from Apple Business Manager or the Managed Apple ID of your administrator.

Work with your internal app developers. For apps developed in-house, use the same method described above to distribute a custom app to your own organization. This does not require the use of the Developer Enterprise Program and enables your app to take advantage of advanced App Store features like app thinning, analytics and more. Additionally, unlike the Developer Enterprise Program, there is no need to update and maintain certificates for distribution.

Obtain the custom app. Your developer will need to associate the custom app to your organization and will notify you when it's available for download. To do this the developer will need your Organization ID which can be found by going to Setting > Enrollment Information. When you sign in to Apple Business Manager, you'll see a Custom Apps section in the sidebar below Content. Custom apps are available to only the businesses specified by the developer and are not visible to other organizations.

Important Information about custom apps

- **App review.** Each app, as well as each version (update) of the app, submitted for custom app distribution goes through an app review process with Apple. The same app review guidelines for App Store apps apply to custom apps.
- **App security.** If your app contains sensitive business data, you might want to include an authentication mechanism within the app. Custom apps by themselves are not secured by Apple, and the security of data within the app is the responsibility of the developer. Apple highly recommends using iOS and iPadOS best practices for in-app authentication and encryption. For more information on secure coding best practices, visit the Developer Library.
- **App verification.** To verify that custom apps meet the review guidelines, Apple needs to be able to sign in and operate the app. Work with your developer or business partner to determine how to meet this requirement with appropriate handling of proprietary or sensitive business data. You might want to provide test accounts or sanitized sample data to protect confidentiality.

Resources

For more detailed information, view the Apple Business Manager User Guide at support.apple.com/guide/apple-business-manager

Explore the following for additional information on Apple Business Manager:

- Apple Business Manager: business.apple.com
- Apple Business Manager release notes: support.apple.com/HT208802
- Upgrading to Apple Business Manager: support.apple.com/HT208817
- Learn more about Managed Apple IDs: support.apple.com
- Learn more about Microsoft Azure AD
- IT Resources: www.apple.com/business/it/
- Business Support: www.apple.com/support/business