APPLE DEVICE ADMINISTRATION 101

Getting Started with Apple Business Manager & MDM

Goetch Stone
Slack @Goetch Stone
goetch.stone@gmail.com

Thanks for coming. This is Apple Device Admin 101; this is genuinely a beginner-level workshop. If you're running thousands of devices, hang around anyway and jump in with your stories — it makes this better for everyone. My name is Goetch Stone, I am the Director of IT for Saybrook Home, a home furnishings and apparel retailer based in Old Saybrook CT.

Resources

- https://www.macadmins.org/
- https://github.com/macadmins
- https://it-training.apple.com/tutorials/apt-deployment
- https://www.apple.com/business/docs/site/Apple_Business_Manager_Getting_Started_Guide.pdf

Before we begin, as this is a beginner workshop, let’s ensure you all are on the Mac Admins Slack. Is anyone not familiar with the MacAdmins Slack? This is the #1 resource as important as an MDM or Apple Business Manager / Apple School Manager. If you are unaware, channels go up for each room, and there are hive notes for the workshop. Mac Admins Open Source exists to provide the code signing certificates to open source projects which are used in SMB, enterprise and education environments across the globe. This workshop and much of the content are from the Apple deployment guide.

Agenda

- Apple Business Manager (ABM) and Apple School Manager(ASM)
- Onboarding Workflow
- Managed Apple Accounts
- MDM Basics
- Security

Today, we're diving into the basics of Apple Business Manager (ABM) and Apple School Manager (ASM) and the associated tools. Several key topics: What is ABM or ASM, and why is it essential for your organization? We'll review the requirements for ABM, walk through the enrollment process, and explain how to configure an e-commerce portal with Apple. Understand the role of Identity Providers (IDP) and learn how to create managed Apple accounts effectively. Discover the basics of MDM, why it's a critical component of your IT strategy, and how it integrates with ABM. Explore the concept of "declarative" management—what it means and its practical implications. We will give an example of an Onboarding Workflow: Follow the onboarding process from IDP to ABM, MDM, and finally to the end user. Learn how to assign devices automatically, establish a minimum baseline for security, and balance risk against convenience. By the end of our session, I hope you'll have a clear roadmap for integrating ABM and MDM into your IT operations, making device management more efficient and secure. Feel free to ask, raise your hand, and I'll throw the "Catch Box." Hopefully, you will catch it and can ask questions or comment.

Why

Why be enrolled in ABM or ASM, and why have an MDM?

Summer of 21

- Had Multiple Locations
- Their Own Apparel Line
- Great Website

In the summer of 2021, we partnered with a regional apparel retailer. We had a solid apparel business for over a decade, and while it showed a profit on paper, it was draining us regarding cash flow. The idea was: bring in a seasoned retail partner to fix the cash issues and grow the business. I had impostor syndrome. I assumed, “They’ve got multiple stores, they must have a real IT team. They’ll know what they’re doing.” I better be on my A game. So I emailed their tech contact and asked, What do you need from me? What would you expect from a tech partner at this point? What do you think happened? I didn’t hear back. Months went by. Then, about two months before the switchover, we got iPads and payment hardware delivered to us. I was thrilled. Awesome, iPads. This’ll be easy. At the time, our internal network used 802.1X with certificate-based authentication—not because we needed to, it was more a can I do this, so I did it sort of thing—one of the benefits of being a department of one. Since I had no idea what their needs would be, it was a 50 - 50 partnership. Instead of treating them fully separately, the owner wanted to share some resources if needed, so he decided to keep them on our network instead of setting up their own. Assuming they had ABM and an MDM in place, I sent over the certificates needed to join the network and even sent over generic profiles they should have been able to deploy if they had the right tools. Changeover day arrives. Their team shows up—six people, POS terminals, new store design, the whole deal. This should’ve been a couple of hours: Turn on iPads, Join the guest network, Let enrollment kick in Updates install Apps deploy via MDM. We even had a local caching server to speed things up. I was on-site that morning. Asked them multiple times: “Need anything from me?” “Nope, we’re all good.”So I leave at 2:30 like normal.

At 4:30, I get the call. “Goetch, the iPads aren’t working. They won’t connect. We can’t run anything.” I ask, “Did they use the setup instructions I gave?” “They couldn’t connect. Nothing’s installed.”
So I tell my boss: “Have them use the guest network. Leave the devices on my desk. I’ll look tomorrow.”
The Shitshow Revealed, The next day, I open one up and realize…They had no management system. The iPads all used the same personal Apple ID. They had no idea how to install a certificate. They had no way to deploy network profiles. They couldn’t even spell MDM, let alone implement it. I had overestimated them entirely.
So now, I’m scrambling. And I have a choice:c Stick to my secure, segmented 802.1X setup and fight them tooth and nail, Or make life easier and get this mess working. I went with option 2. I created a temporary WPA3 network. I pushed a new configuration profile to my devices. Noted the devices that did not get the new network profile (about 4). Reconfigured the primary network to WPA3. Resent a new profile to my fleet with the new network and settings. Noted if any devices didn’t get the new payload. Removed the tertiary network and manually added Wi-Fi settings to their unmanaged iPads. And my devices that didn’t get the new profiles. Then, I updated the OSes. Manually installed apps using their shared Apple ID. All because they didn’t have Apple Business Manager, and they didn’t use MDM.

Apple Business Manager (ABM)
Apple School Manager (ASM)

- Enrollment Requirements
- Enrollment Process
- Linking to a reseller

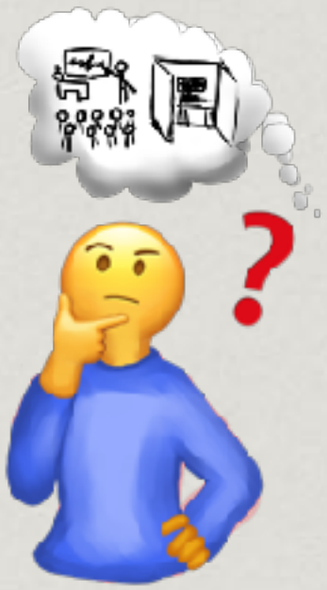
Let’s cover the basics: What is Apple Business Manager? What are the enrollment requirements? How do you enroll and finally link to a reseller or Apple e-commerce portal?

What are ABM and ASM

- Automated Device Enrollment
- Volume Content Purchase
- Managed Apple Accounts
- https://www.apple.com/business/docs/site/Apple_Business_Manager_Getting_Started_Guide.pdf

What is Apple Business Manager? Apple Business Manager (ABM) is a web-based portal designed for IT administrators to efficiently deploy and manage Apple devices, all from one centralized location. Seamlessly integrating with your mobile device management (MDM) solution, ABM automates device enrollment, app purchasing, content distribution, and the creation of Managed Apple Accounts for employees. Key Features
Automated Device Enrollment: which is the process automatically enrolls devices into your MDM solution upon activation, eliminating the need for manual configuration. Volume Content Purchase: Enables bulk purchasing of apps and books, allowing them to be assigned to devices or users to ensure consistent deployment across your organization. Managed Apple Accounts: Facilitates the creation and management of Managed Apple Accounts for employees, providing access to Apple services while maintaining organizational control over user accounts.

Enrollment Requirements



- D-U-N-S Number
- Business Email
- Verification Contact

So that’s a basic synopsis of ABM and ASM. What are the enrollment requirements? Can you use AMB or ASM for your family? What do you need to enroll? A DUNS number, a business email, and a verification contact. This is not an instant process.

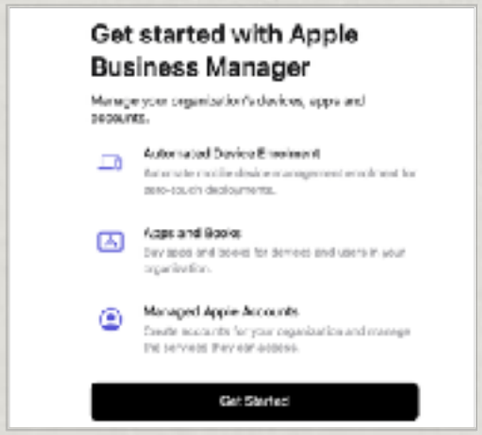
D-U-N-S

- What is a D-U-N-S
- How to find/obtain one
- https://www.dnb.com/duns-number/lookup.html

Who the Heck is a DUNS? Dun & Bradstreet (D&B) is a business data and analytics company that provides credit ratings, risk assessments, and business identity verification services. Why Does Apple Use D&B for ABM Enrollment? Apple doesn't verify businesses directly—it relies on D&B's existing database to confirm whether a company is legit before allowing it to enroll in Apple Business Manager (ABM). How D&B Works in This Context:
 D&B assigns a D-U-N-S Number (a unique 9-digit ID) to every registered business. Apple checks this number to verify your company before approving ABM enrollment. If your business operates under a DBA (Doing Business As) name, your legal name in D&B's database might not match, causing delays. First-hand experience here, we are actually Saybrook Country Barn DBA Saybrook Home, we decided to change our name after going to the NRF Big show in NYC, and people asked if we sold farm equipment….

Enrollment

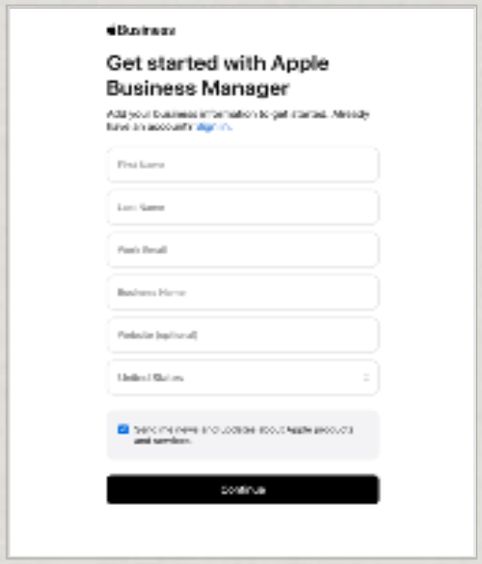
- https://business.apple.com/signup



If you have your ducks in a row, you can now go to business.apple.com/signup

Enter Business Info

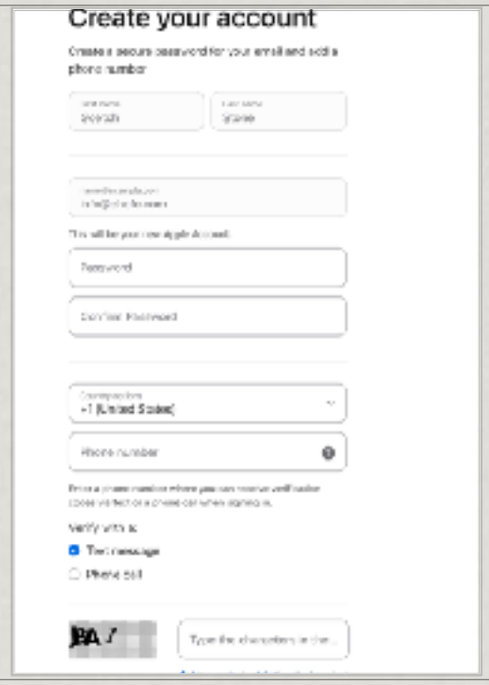
- First and Last Name
- Work Email
- Business Name
- Website



Sign up your organization. Go to https://business.apple.com/. Select “Sign up now.” Enter the following organization information: The first and last names of the individual enrolling on behalf of the organization
Important: This must be a legal, human name. First and last names, such as “IT Coordinator” or “Apple Deployment,” will be returned to you to correct the information. A work email address not associated with an App Store or iCloud account and hasn’t been used as an Apple Account for any other Apple service or website.
*Note: This email address becomes your administrator-managed Apple Account.
The name of your organization
*Note: This name may change when you verify your organization.
The website URL
*Note: This is optional, but providing it can expedite your organization’s verification process.
Select whether to get news and updates about Apple Business Essentials, then select Continue.

Apple Account

- Create and confirm a new password



Create and confirm a new password for your new account, then select a region code and enter your phone number. A one-time verification code is sent to your email address first, then a different code is sent to your phone number. Follow the remaining steps, then select Get Started to use Apple Business Manager.

Terms

- Read and accept the terms
- No you cannot change them

You will need to accept the terms. Now I have not read them, like not at all. I am curious, has anyone actually read these? Has anyone had to take them to legal? Better yet, has anyone tried? For most of us, I would imagine it is a no, but you are binding your organization to these terms. (South Park HumanCentiPad)

But wait, there’s more

- Time to verify

But wait, there's more…

Verify D-U-N-S and Contact

- Enter your DUNS
- Enter the authorized contact
- Hurry up and wait

Select Verify, then enter your organization’s D-U-N-S Number. Enter verification contact information (name, email, and Role/Job title) that Apple can call to verify your organization. Examples include your CEO, CTO, or CFO. Check your email for a message from Apple Business Manager with the subject line, “Your enrollment is in review.” During the review process, your verification contact is asked to confirm information about you and your organization before your enrollment is approved. Make sure that any filters allow mail from all apple.com domains. Return any missed phone calls quickly so the enrollment process can proceed smoothly. After your organization is approved, immediately create at least one additional user who has the role of Administrator. See Add administrators. In my org, the owner. Important: If you forget or lose your password before creating at least one additional administrator, use the iforgot.apple.com website to reset your password.

ASM Checklist

- Same as ABM
- No DUNS
- Must be an EDU

The Apple school manager has the exact requirements as the business manager, except that no DUNS is needed. They will verify that you are an EDU.

Why Have an E-commerce Portal

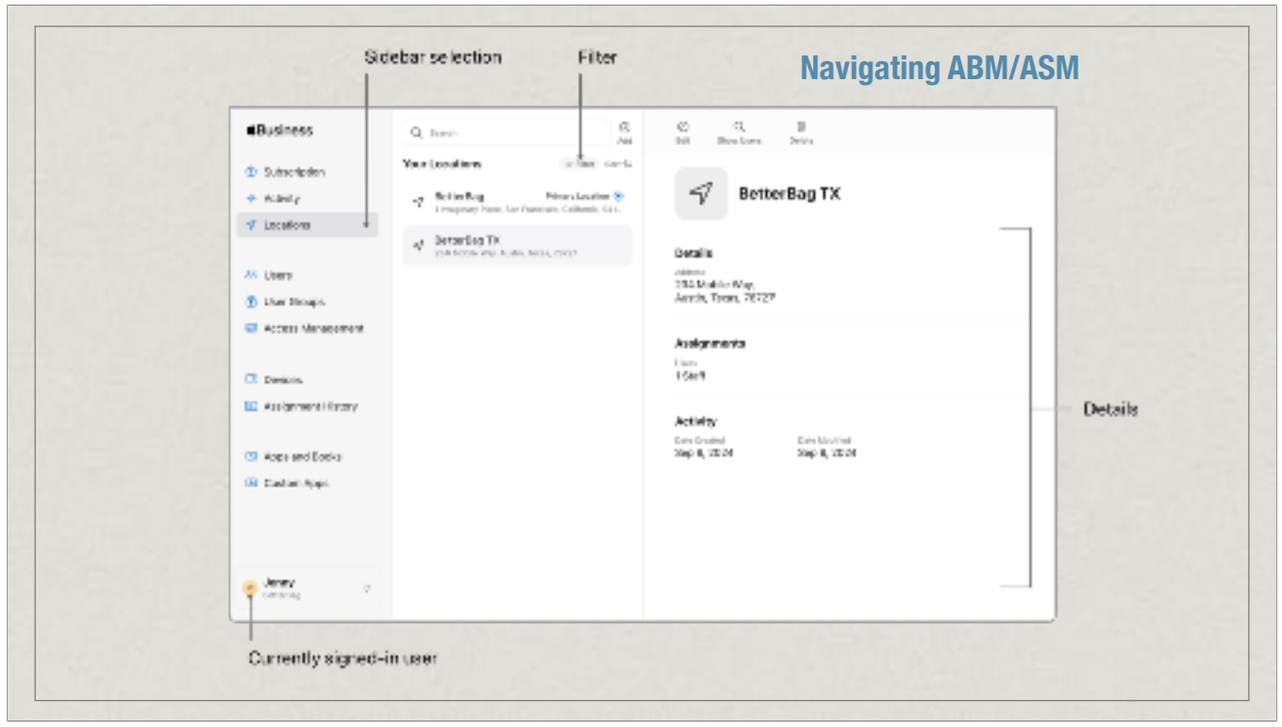
- New purchases are automatically added to ABM
- Provides direct access to bulk discounts
- Allows for business roles

Next, my recommendation would be to set up an e-commerce portal. An e-commerce portal ensures new purchases are automatically added to ABM. Provides direct access to bulk discounts and allows for business roles. It gives you the ability to create proposals and preferred builds.

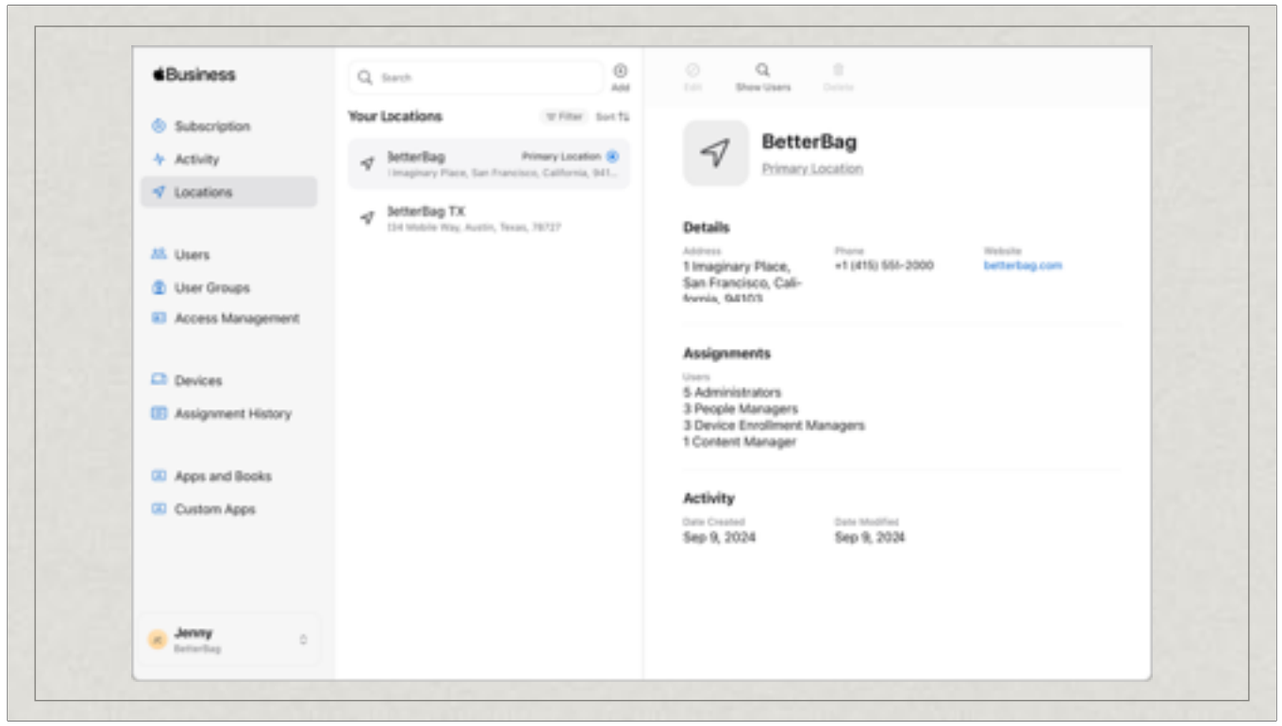
Apple E-commerce Portal

- Ensure ABM is set up first!
- Contact the Apple business team nearest you
- They will guide you through the process
- Or contact a trusted VAR

We just contacted the business team at our local store, and they guided us through the process. We chose to work with the local Apple Store business team. If you work with a Value Added Reseller, ensure your VAR has your Apple customer number. Your Apple customer number is under preferences —> organization information in ABM or ASM.
< Break to show Ecommerce Portal >
< Potential First 50 Break >

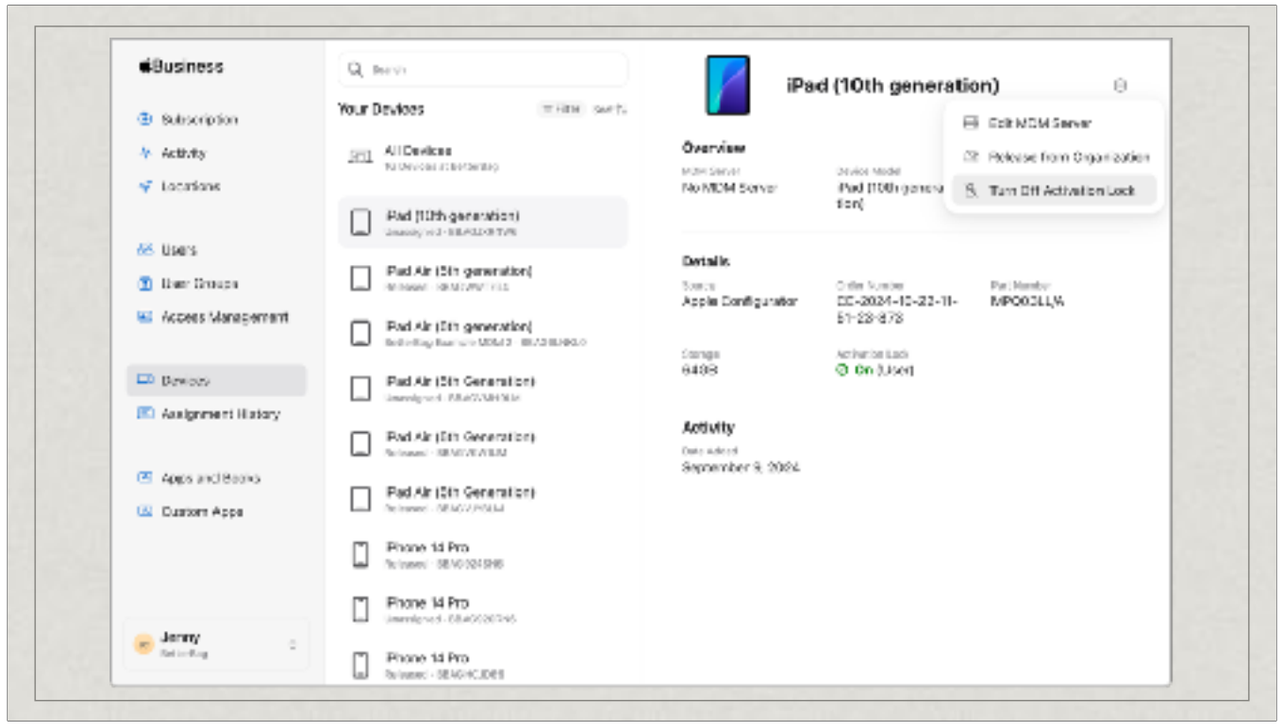


Once you have set up ABM or ASM and your organization is approved, you should get used to the navigation. On the left side, Subscription (Apple Business Essentials), Locations, Users, Groups, Access Management, Devices, Assignment History, Apps and Books, Custom Apps, and preferences.

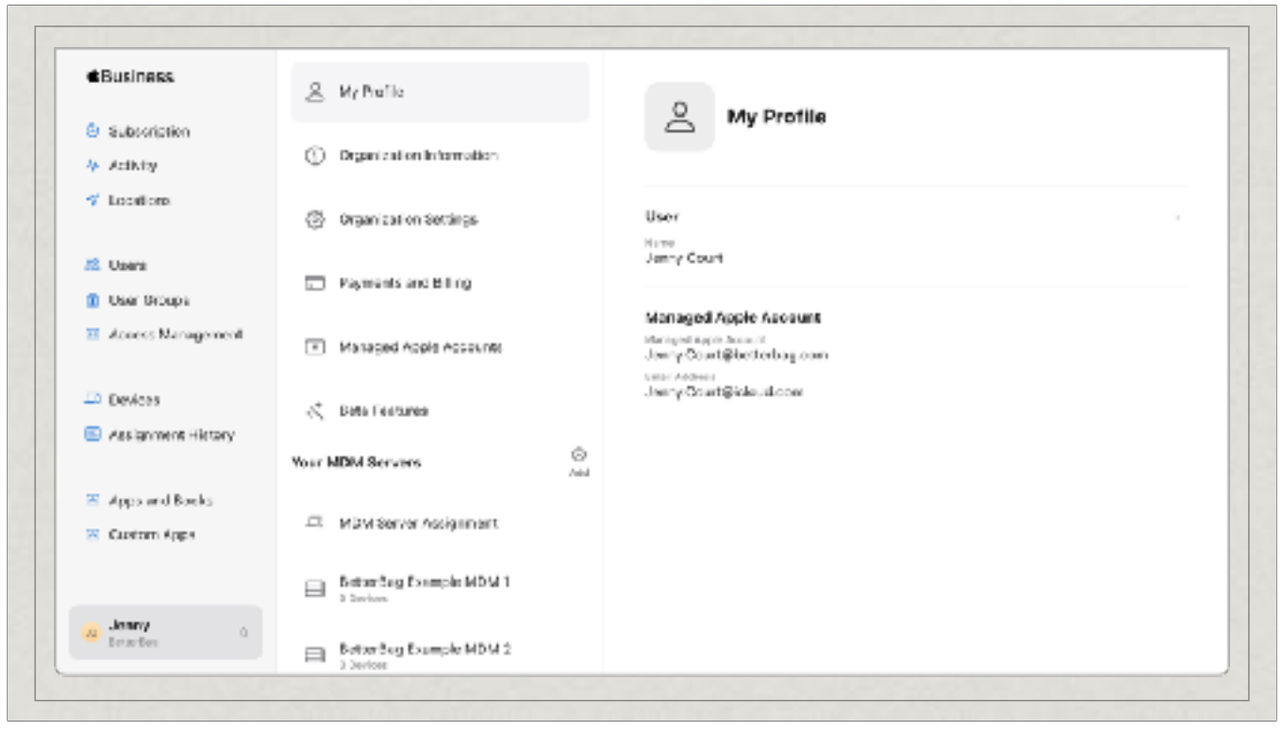


Locations

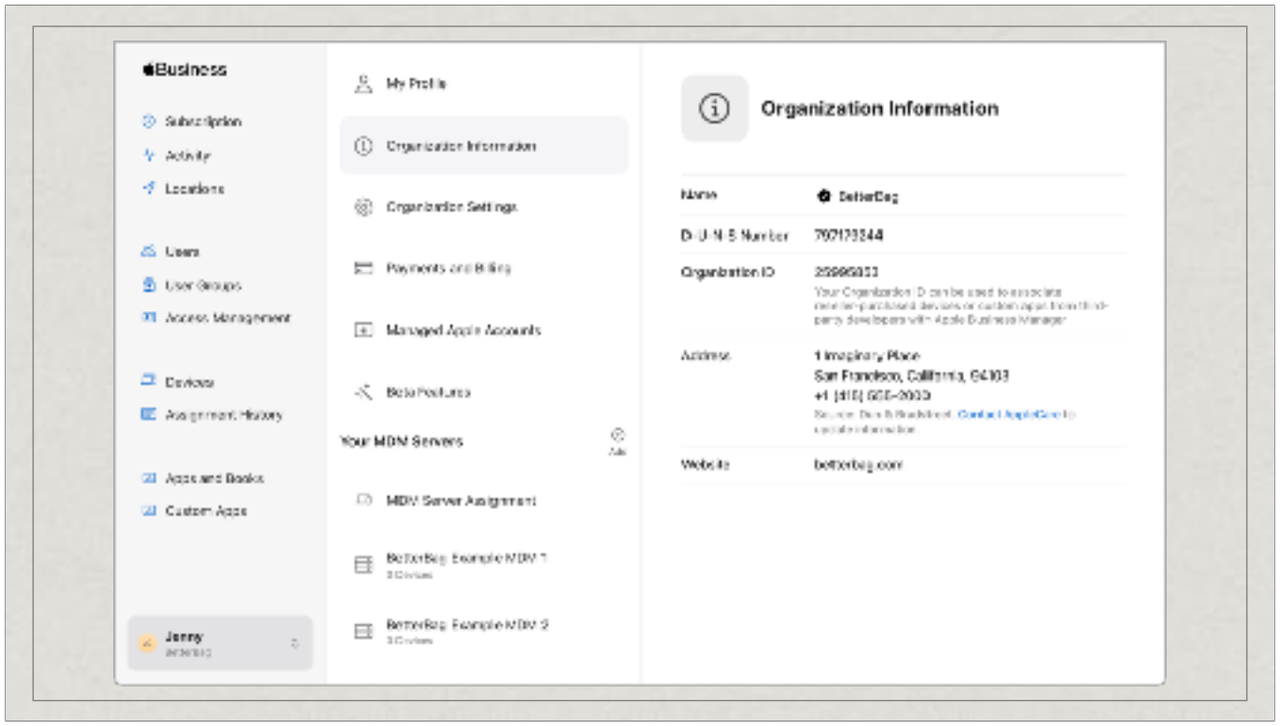
When you sign up for Apple Business Manager, the first location is automatically created (called the primary location) and reflects your organization's name. As you expand your implementation, you can add more locations for more granular control. Locations can mirror physical locations or organizational units. Apps and Books are provisioned to specific locations.



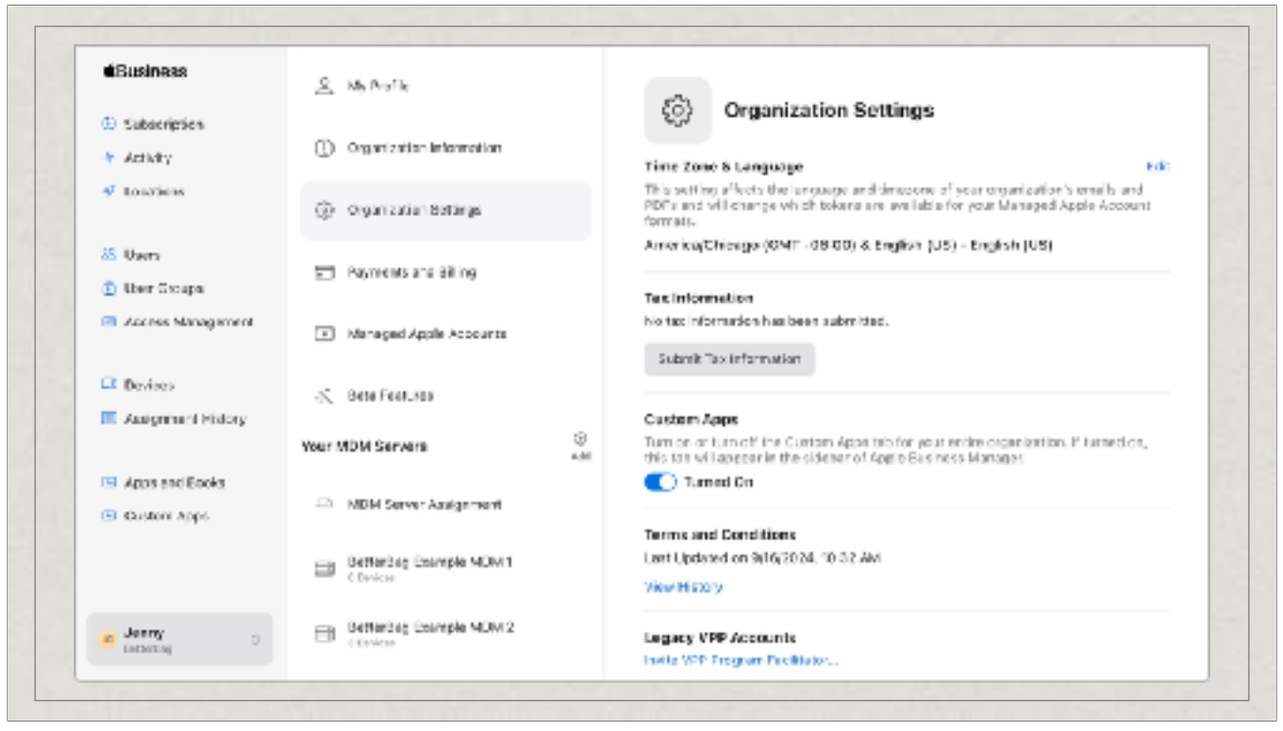
Devices:
The Devices tab shows all devices enrolled in ABM. You can edit the MDM server assignment, release devices, and turn off activation lock.



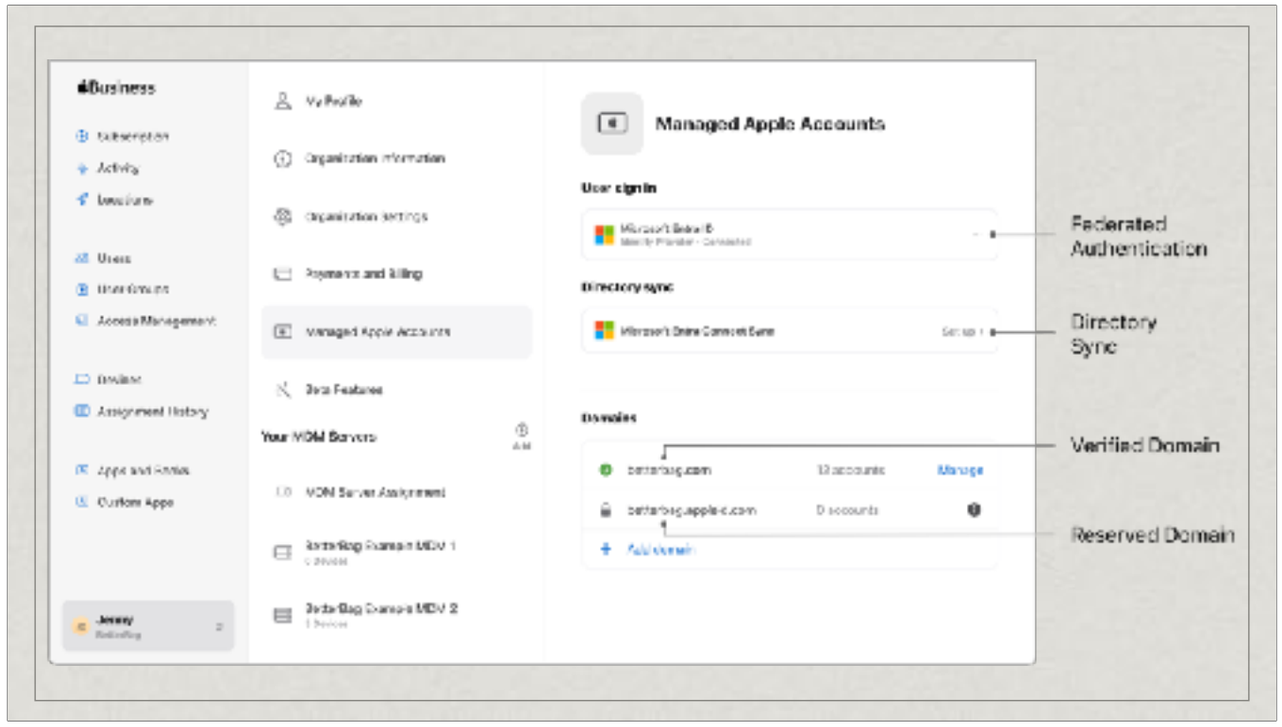
Preferences:
To access preferences, click your user account at the bottom of the left sidebar, then choose Preferences from the pop-up menu. Under My Profile, you will see your account's email address and phone number. If you click Manage, you can change your email address or phone number for two-step verification. You can also add alternative phone numbers.



Organization Information: This View shows your organization’s details such as Name, D-U-N-S Number, Organization ID, Address, and Website. Here is where that customer number is that your reseller needs.



Organization Settings View your organization’s enrollment information. You can perform these tasks:
Change your account’s time zone and language. This setting affects the language and time zone of your organization’s emails and PDFs. It also changes which tokens are available for your Managed Apple Account formats. Submit tax information. Enable custom apps for your entire organization. If enabled, Custom Apps appears in the sidebar near



Managed Apple Accounts:
With User Enrollment or Device Enrollment, you can allow users to use Managed Apple Accounts alongside their personal Apple Accounts on personal devices. With their Managed Apple Accounts, users can access Apple services, including iCloud, and use them to collaborate. Unlike personal Apple Accounts, your organization owns and manages Managed Apple Accounts and controls password resets and role-based administration.
Managed Apple Accounts are created after you do any of the following:
Use federated authentication with Google Workspace, Microsoft Entra ID, or another identity provider (IdP). Use Directory Sync to import user data from Google Workspace, Microsoft Entra ID, or another IdP Use Apple School Manager to import accounts from your student information system (SIS). Manually create accounts in Apple Business Manager or Apple School Manager.

Domains:
View the domain or domains associated with your Apple Business Manager or Apple School Manager account. A reserved domain is automatically created for your account. You can use the reserved domain if no custom domain is available.
You can also manage custom domains and verify them. After you verify a domain, you have three options available, all of which you can enable for each domain:
Lock a domain — Use this option to require that all new Apple Accounts created on the domain be only Managed Apple Accounts.

Domain capture — Use this option to ensure that any account using your domain is a Managed Apple Account. This option includes the possibility to convert existing Apple Accounts (which may have been created previously using your organization’s domain) into Managed Apple Accounts.

Federated authentication — If there are no unmanaged Apple Accounts conflicts, or after the domain capture process has started, users with the role of Administrator and People Manager can optionally continue to turn on federated authentication with an IdP.

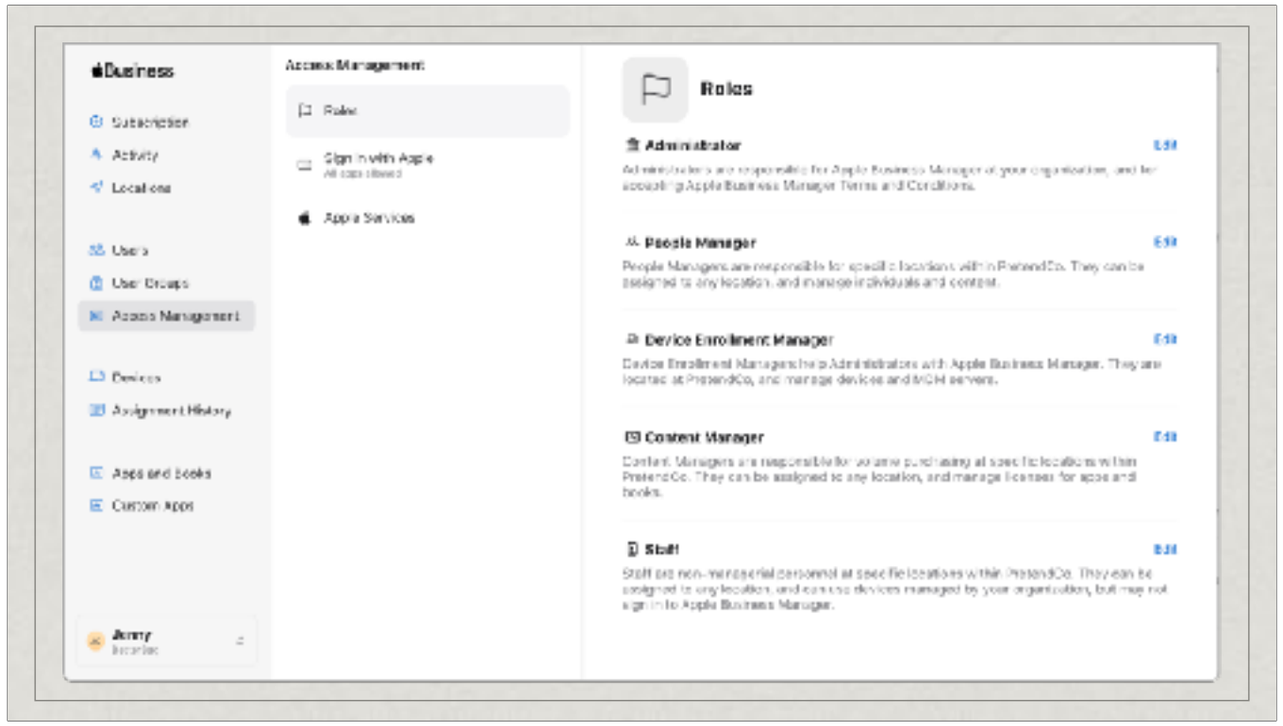
With federated authentication, you can use an account’s user name and password from one directory system in other systems. You use federated authentication to link Apple Business Manager or Apple School Manager to your instance of Google Workspace, Microsoft Entra ID, or another IdP. Then users can use their Google Workspace, Microsoft Entra ID, or IdP user names and passwords as Managed Apple Accounts. When federated authentication is turned on, Managed Apple Accounts are automatically created for new users the first time they sign in.

Why Set This Up Before MDM?

- Ensures users have organization-managed Apple IDs instead of personal ones.
- MDM enrollment & authentication work seamlessly with federated accounts.
- Reduces friction during onboarding by enforcing identity policies upfront.

How to Set Up Federation with ABM

- Step 1: Go to Settings → Accounts → Identity Providers in ABM.
- Step 2: Choose Google Workspace or Microsoft Azure AD.
- Step 3: Verify domain ownership & configure authentication settings.



Access Management.
Here you can change some settings and privileges if needed. Apple is the dungeon master here; if they let you change a setting, this is where you can do it.

Roles and privileges in ABM

- Administrator
- People Manager
- Device Enrollment Manager
- Content Manager
- Staff

Once you set up ABM, depending on your organization’s size and structure, you may need to assign roles and privileges. Once your IDP is connected, you can sync users and set roles if required.

Different roles: Administrator…. Probably you, the person who hired you.. The person who set everything up and has the ability to sign contracts on behalf of the organization.
People Manage.. Potentially HR. Device Enrollment Manager .. If you have a team of people, these would be the ones to assign devices to specific MDMs Content Manager is the person who makes software and other “content” purchases

Basic privilege	Admin	People Manager	Device Enrollment	Content Manager
Accept terms and conditions	✅	❌	❌	❌
Edit role privileges	✅	✅	❌	❌
Add Apple Customer Numbers and Reseller Numbers	✅	❌	❌	❌
Set tax status information	✅	❌	❌	❌
Configure federated authentication	✅	✅	❌	❌
Create, edit, and delete locations	✅	✅	❌	❌
Set default Managed Apple Account user name formats	✅	✅	❌	❌
Administer AppleSeed for IT	✅ D	❌ D	❌	❌
Participate in AppleSeed for IT	✅ D	✅ D	✅ D	✅ D
Use managed devices	✅	✅	✅	✅
Sign in to iCloud.com with a Managed Apple Account	✅	✅	✅	✅
Use managed apps and books	✅	✅	✅	✅

The basic permissions of each role. Would anyone like to dive deeper into this? Do we have any questions?

People Privileges

People privilege	Administrator	People Manager	Device Enrollment Manager	Content Manager
Create, edit, and delete Managed Apple Accounts	✅	✅	❌	❌
Assign roles to users	✅	✅	❌	❌
Change account status of users	✅	✅	❌	❌
Reset passwords for users	✅	✅	❌	❌
Create, edit, and delete user groups	✅	✅	❌	❌
Use FaceTime	❌ D	❌ D	❌ D	❌ D
Use iMessage	❌ D	❌ D	❌ D	❌ D

People privileges…. Again, most settings are either on or off.

Device Privileges

Device privilege	Administrator	People Manager	Device Enrollment Manager	Content Manager
Manage MDM servers	✅	❌	✅	❌
Add, assign, and unassign devices to MDM servers	✅	❌	✅	❌
Assign devices to organization	✅	❌	✅	❌
Turn off Activation Lock	✅	❌	✅ D	❌
Release devices	✅	❌	✅ D	❌

Content Privileges

Content privilege	Administrator	People Manager	Device Enrollment Manager	Content Manager
View apps and books	✅	❌	❌	✅
Buy apps and books	✅	❌	❌	✅
Reassign licenses for apps	✅	❌	❌	✅
Hold unassigned licenses for apps and books	✅	❌	❌	✅

Staff privileges

Staff privilege	Access
Use managed devices	✅
Sign in to iCloud.com with a Managed Apple Account	✅
Use managed apps and books	✅
Participate in AppleSeed for IT	✅ D
Use FaceTime	❌ D
Use iMessage	❌ D

Staff is what everyone.

Roles and privileges in ASM

- Administrator
- Site Manager
- People Manager
- Device Enrollment Manager
- Content Manager
- Staff
- Instructor
- Student

ASM you have a Site Manager, Instructor, and Student

Basic privilege	Administrator	Site Manager	People Manager	Device Enrollment Manager	Content Manager	Manager
Accept terms and conditions	✅	❌	❌	❌	❌	❌
Edit role privileges	✅	✅	✅	❌	❌	❌
Add Apple Customer Numbers and	✅	❌	❌	❌	❌	❌
Set tax status information	✅	❌	❌	❌	❌	❌
Configure federated authentication	✅	✅ D	✅	❌	❌	❌
Integrate with SIS	✅	✅ D	✅	❌	❌	❌
Create, edit, and delete locations	✅	✅ D	✅	❌	❌	❌
Set default Managed Apple Account user	✅	✅ D	✅	❌	❌	❌
Set the default password policy for new	✅	✅ D	✅	❌	❌	❌
Turn on Student Progress	✅	✅ D	✅	❌	❌	❌
Administer AppleSeed for IT	✅ D	✅ D	❌ D	❌	❌	❌
Participate in AppleSeed for IT	✅ D	✅ D	✅ D	✅	✅ D	✅ D
Use managed devices	✅	✅	✅	✅	✅	✅
Sign in to iCloud.com with a Managed	✅	✅	✅	✅	✅	✅
Use managed apps and books	✅	✅	✅	✅	✅	✅

People privilege	Administrator	Site Manager	People Manager	Device Enrollment Manager	Content Manager
Create, edit, and delete Managed Apple Accounts	✅	✅ D	✅	❌	❌
Assign roles to users	✅	✅ D	✅	❌	❌
Change students' password policies	✅	✅ D	✅	❌	❌
Change account status of users	✅	✅ D	✅	❌	❌
Inspect user accounts	✅	✅ D	✅	❌	❌
View account inspection log	✅	✅ D	✅	❌	❌
Create, edit, and delete classes	✅	✅ D	✅	❌	❌
Reset passwords for users	✅	✅ D	✅	❌	❌
Generate verification codes	✅	✅ D	✅	❌	❌
Use FaceTime	❌ D	❌ D	❌ D	❌ D	❌ D
Use iMessage	❌ D	❌ D	❌ D	❌ D	❌ D

Content privilege	Administrator	Site Manager	People Manager	Device Enrollment Manager	Content Manager	Manager
View apps and books	✅	✅ D	❌	❌	✅	✅ D
Buy apps and books	✅	✅ D	❌	❌	✅	❌ D
Reassign licenses for apps	✅	✅ D	❌	❌	✅	❌ D
Hold unassigned licenses for apps and books	✅	✅ D	❌	❌	✅	❌ D

Staff privilege	Access
Use managed devices	✅
Sign in to iCloud.com with a Managed Apple Account	✅
Use managed apps and books	✅
Participate in AppleSeed for IT	✅ D
Use FaceTime	❌ D
Use iMessage	❌ D

Instructor privilege	Access	Instructor privilege	Access
Participate in AppleSeed for IT	✅ D	Assign roles to individuals	❌ D
Use managed devices	✅	Change the password policy for students	❌ D
Sign in to iCloud.com with a Managed Apple Account	✅	Change the account status of students	❌ D
Use managed apps and books	✅	Use FaceTime	❌ D
Inspect student accounts	❌ D	Use iMessage	❌ D
View account inspection log	❌ D	View apps and books	❌ D
Create, edit, and delete classes	✅ D	Buy apps and books	❌ D
Reset passwords for students	✅ D	Reassign licenses for apps and books	❌ D
Generate verification codes for students	✅ D	Hold unassigned licenses for apps and books	❌ D
Create, edit, and delete Managed Apple Accounts	❌ D	View Student Progress Dashboard	✅

Student privilege	Student
Use managed devices	✅
Sign in to iCloud.com with a Managed Apple Account	✅
Use managed apps and books	✅
Participate in AppleSeed for IT	❌
Use FaceTime	❌ D
Use iMessage	❌ D

Some things to note: Administrator, Site Manager, and People Manager can integrate with SIS That is a basic rundown of how to get up and running with ABM and/or ASM. If you want to change any defaults, you can in ABM ASM under Access Management

Let’s pause, do we have any questions so far? That apparel partner could have gone through these steps, but that’s only half of it. Not only do you need ABM or ASM, but you also need an MDM to actually manage and deploy your devices.

MDM

- What is MDM
- Are DDM and MDM the same?
- Do we really need an MDM?

Centralized system for enrolling, configuring, and managing Apple devices. Enables remote setup, security enforcement, and app deployment. Are DDM (Declarative Device Management) and MDM the Same? No, DDM is an evolution of MDM, not a replacement. DDM gives devices more autonomy to apply configurations based on conditions. MDM is still required—DDM is a feature within MDM, not a separate system. So, do you need an MDM? Yes—an MDM isn't optional if you manage more than a handful of devices. It’s required for:

- Automated Device Enrollment
- Enforcing security policies
- Maintaining compliance

If you’re not using an MDM, you do everything manually, which doesn’t scale.

Winter of 2025

Going back to that apparel retailer.
We recently took the apparel store back. This time?
I created a proposal for the bean counters via my Apple e-commerce portal for two iPads. Bossman approved the purchase. I logged back in, pulled up the proposal, and hit order.

The Setup

- Automatically assigned
- New users synced
- Groups deployed

The iPads were automatically assigned to our MDM via ABM settings.
I added the new employees to our Identity Provider. Federation with the workspace and our MDM synced users to our MDM and ABM. One iPad got the standard register configuration (a guest account with our security and network requirements). The other got our shared iPad enrollment profile. Users were assigned by group to the shared iPad.

Deployment

- Opened the box
- Join open Wi-Fi network
- Let Apple take over

When they showed up, we: Opened the box, Joined an open Wi-Fi network, Let automated device enrollment take over The profiles pushed. Apps installed. Bookmarks came via Chrome management. The shared iPad was automatically configured login access for the pre-defined apparel user group. We were live in under an hour.
No tech drive-down. No duct tape. No fire drill, as zero touch as possible.

Audible

Then we used them, and with our pos system, the iPads just hindered our checkout lanes; they were the wrong tool for the job. So we decided to switch to iMacs. Ordered them through the same portal. Assigned them their own MDM profiles for their POS role.. Via our MDM I gave them generic logins and StorePrefixRegister# and set the password for each in the enrollment profile. I set an Admin user too, and for enhanced security, I let the MDM set the admin password. I do find this a bit of a pain for me, but security is often a pain in the ass. Devices came online. Profiles applied. Apps deployed. Bookmarks there. Everything current. No delays. No exceptions. I can now ensure they stay updated. And when software updates cooperate, they actually do.

Link an MDM Server

- Preferences —> MDM Servers —> +
- Enter a unique name
- Download the public key from the MDM Server
- Upload public key
- Download server token
- Upload token to MDM

ABM is only part of the solution, you need to link to an MDM to get the benefits. How do you link your MDM to ABM or ASM? Step 1In Apple Business Manager, click your account name at the bottom of the sidebar, then choose Preferences from the pop-up menu. Step 2
In your MDM Servers, click the Add (+) button. Step 3 Enter a unique name for the server.
The name doesn’t need to be the same as the MDM service hostname, but choose a name that clearly refers to the relevant MDM server. Before continuing, you must download the public key certificate file from your MDM solution. This Privacy-Enhanced Mail (PEM) certificate contains a public key that your portal uses to encrypt its server token.

To learn how to download the public key certificate from your MDM solution, consult your MDM vendor’s documentation. Every MDM vendor is different.

Step 4 Below MDM Server Settings, click Upload Certificate, and select the public key certificate file from your MDM solution. After you upload the certificate, you must click Save. Saving a public certificate to Apple Business Manager generates a server token.
Step 5 Click Download MDM Server Token. The portal server token downloads to your computer.
To complete the link, you upload the server token to your MDM solution. The server token is a P7M file that your MDM server uses to securely connect to Apple Business Manager or Apple School Manager. To learn how to upload the server token to your MDM solution, consult your MDM vendor’s documentation.
Again, each MDM vendor is different
Step 7 After you upload the server token to your MDM solution, refresh the browser window that contains Apple Business Manager to verify the connection.

Buying Content Through Apps and Books

- Payments and billing
- Download server token
- Upload to MDM

Step 1 Click your account name at the bottom of the sidebar, then choose Preferences from the pop-up menu.
Step 2 Click Payments and Billing.
Step 3 In Payments and Billing, click the Apps and Books tab. Then, below Content Tokens, click Download for a location to download the server token. The server token is an encrypted file that connects your MDM solution to the volume purchasing feature.

Note
You can upload the server token to only one MDM solution.
To complete the link, you upload the server token to your MDM solution. Your MDM server uses the server token to securely connect with Apple Business Manager or Apple School Manager to manage purchased content.

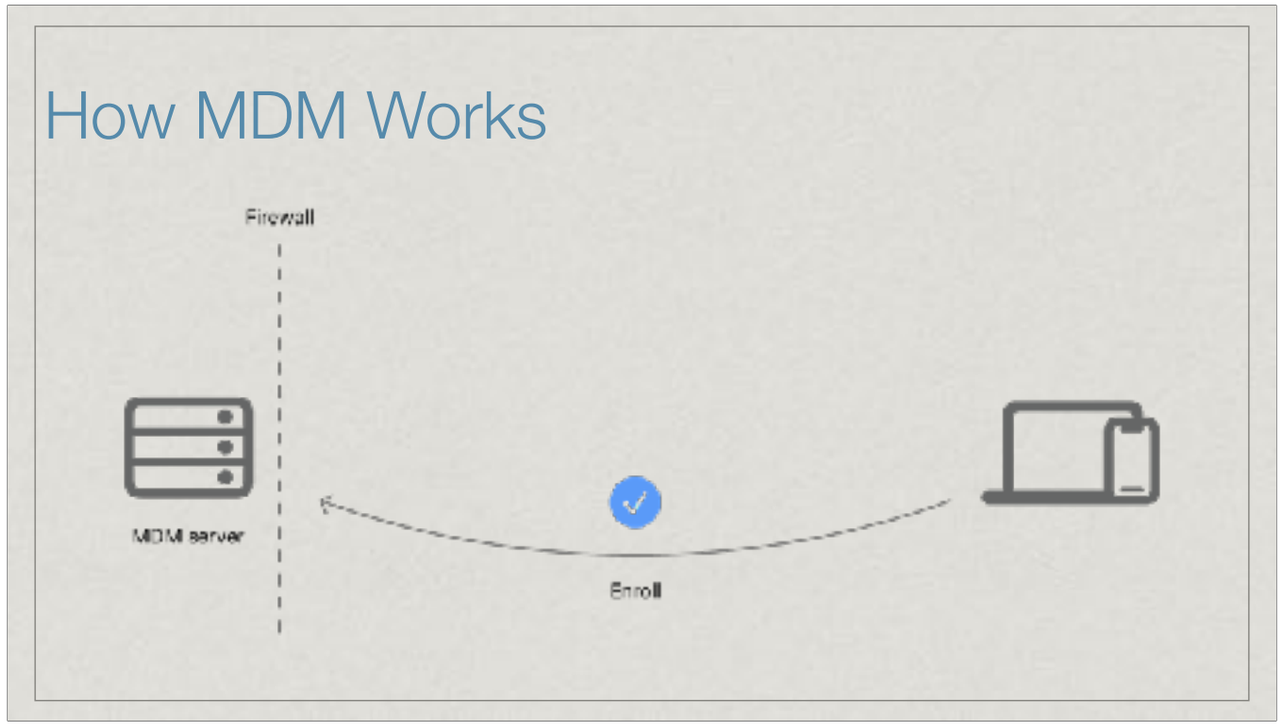
Distribution

- Managed Device Distribution
- Managed User Distribution

Managed Distribution to Devices
With device-based app assignment, you control distribution from start to finish, including app update management.
For device-based assignment, you need one managed distribution license per device. Your organization retains ownership of the app licenses, whether you assign them to users or devices. When a device or user no longer needs an app, you can reassign it to a different device or user. You can use this distribution model for devices enrolled with Automated Device Enrollment or Device Enrollment. If your organization has a lot of users who bring their own devices, User Enrollment might be ideal. You can then distribute user-assigned apps.

Managed Distribution to Users
You can use this distribution model for organization-owned personalized devices or user-owned devices. Don’t use this model for organization-owned shared devices.
You can use your MDM solution to automatically and silently enroll users with Managed Apple Accounts in managed distribution. You can then assign apps and books to those users.
Users with personal Apple Accounts must first be invited and accept the invitation to participate in distribution of Apps and Books content. Unsupervised devices ask the user to accept the installation of an app. On supervised devices, apps install silently without asking. You can also assign more apps and books at any time.

<Might be short if no questions>.
< second 50 Break >



Now that you have ABM up and running and have linked an MDM solution, devices must enroll with an MDM solution to get the benefits.

Installing an Enrollment Profile

An enrollment profile is used to enroll devices into an MDM.

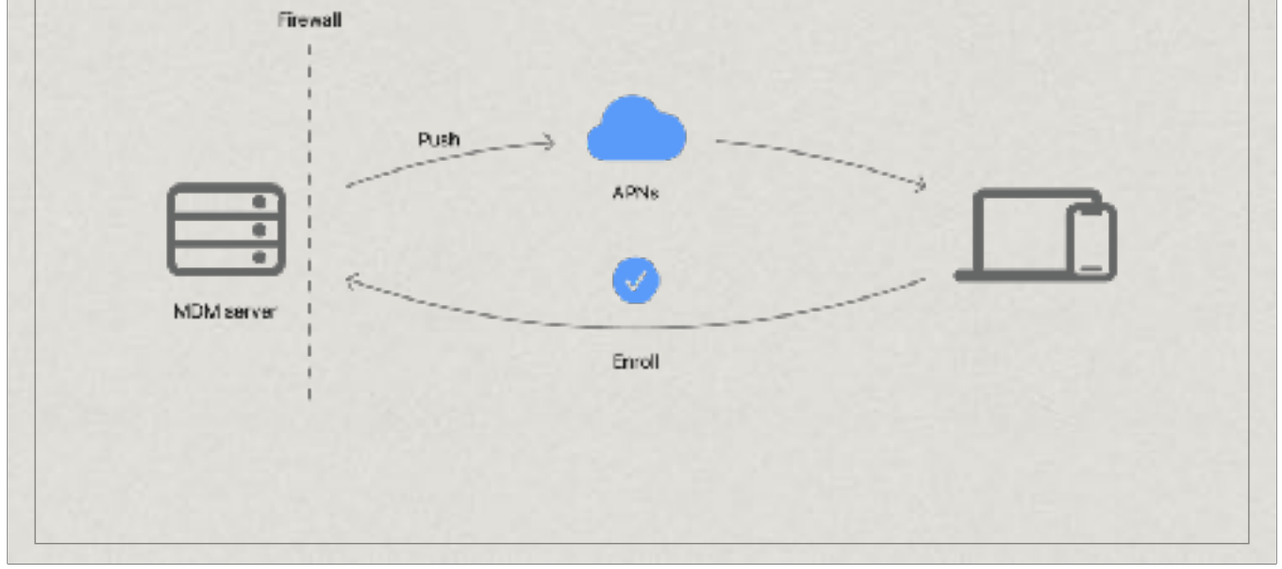
Enrollment Types

- Automated
- URL or MDM portal
- Account-driven device enrollment
- Account-driven user enrollment

Automated Device Enrollment is the ideal way to enroll your organization’s devices in your MDM solution. However, this method requires a device to be new or reset to factory settings and at the first Setup Assistant screen. Use Device Enrollment to manually enroll devices that have been donated or are already in the field and those bought outside official Apple procurement channels.

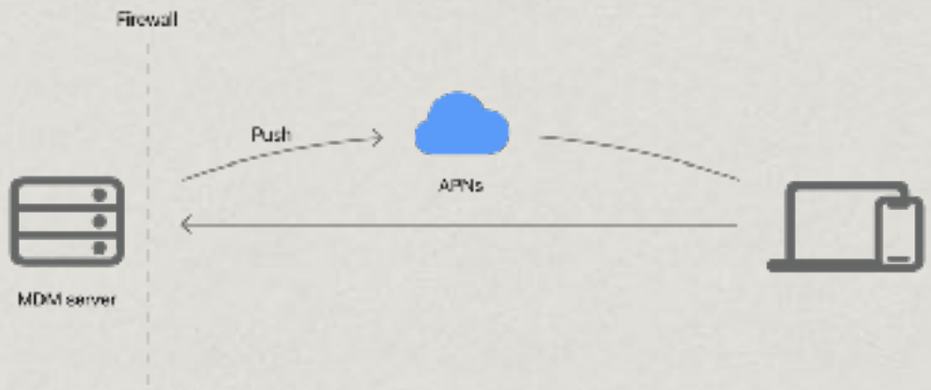
Account-driven User Enrollment and account-driven Device Enrollment provide a secure way for users and organizations to set up Apple devices by signing in with a Managed Apple Account. This approach allows both a Managed Apple Account and a personal Apple Account to be signed in on the same device, with complete separation of work and personal data. Users maintain privacy over their personal information, and IT supports work-related apps, settings, and accounts. To support this separation, the following changes have been made to the way apps and backups are handled: All configurations and settings are removed when the enrollment profile is removed. Managed Apps are always removed during unenrollment. If you install apps before enrolling in a device management service, you can’t convert them into Managed Apps. Restoring from a backup doesn’t restore device management service enrollment. Users who sign in with their personal Apple Account can’t accept an invitation for Managed App distribution. Although you can create Managed Apple Accounts manually, organizations can take advantage of federation.

Notifying the Device



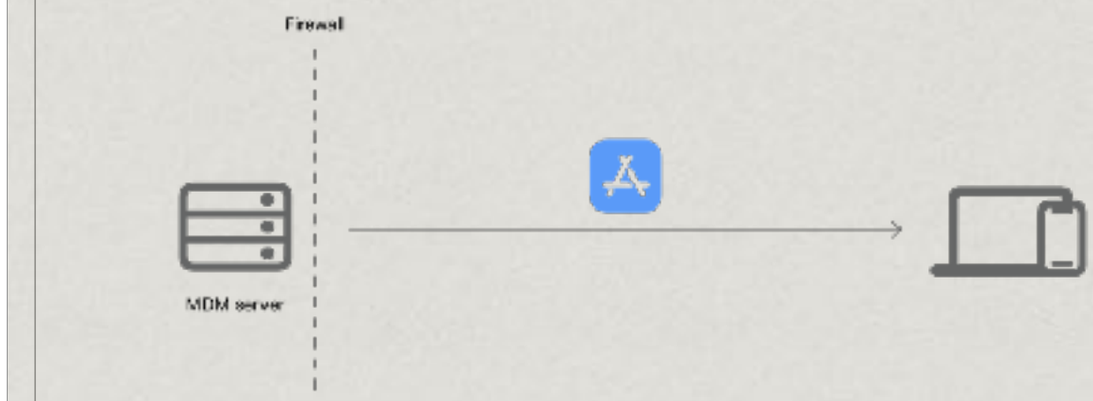
The MDM server queues up a command for the device and sends a notification to the device through the Apple Push Notification service (APNs). MDM solutions use APNs to maintain persistent communication with devices across both public and private networks. To use APNs, devices need a persistent network connection to Apple’s servers. That may mean opening ports on firewalls if your network is heavily restricted.

Contacting the Server



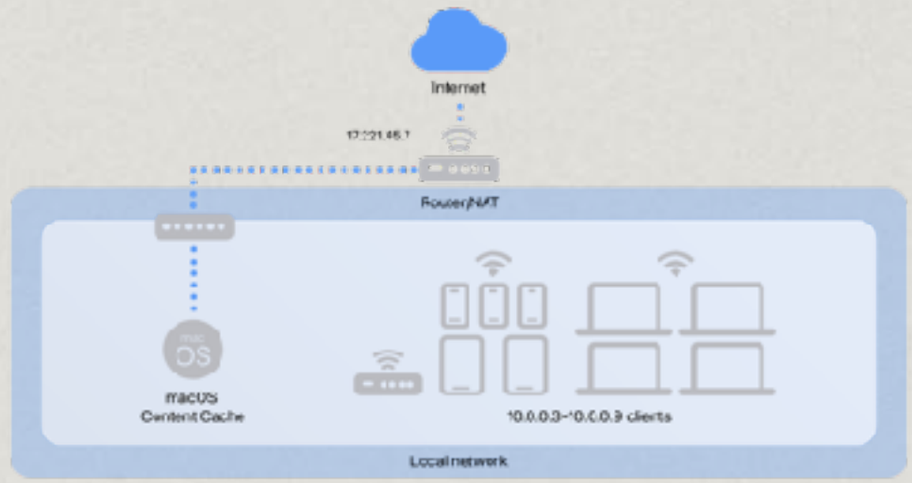
The device receives the notification and contacts the MDM server.

Delivering Content

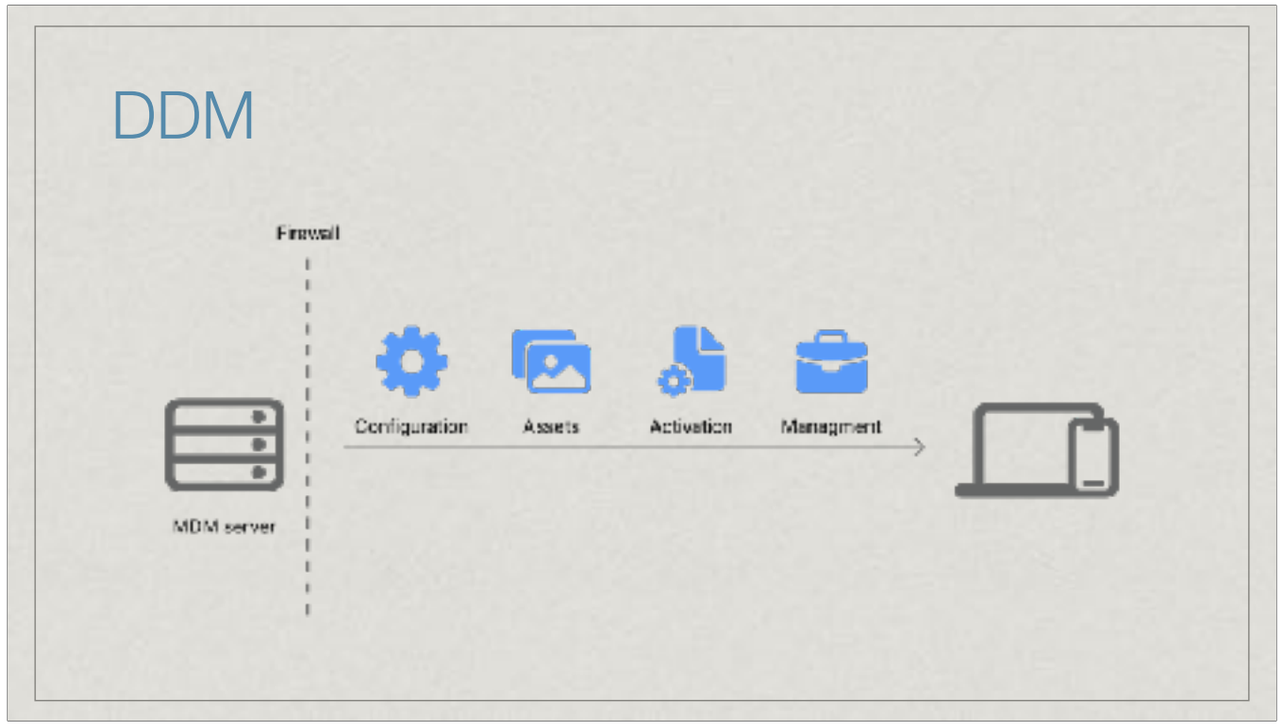


After it’s connected to the MDM server, the device downloads and acts on the queued command. When your MDM solution wants to install an app, it sends a push notification to the device. The device checks in and processes an InstallApplication command and then fetches the actual app file from the App Store or from a local network caching server.

Content Caching



You can enable one or more Mac computers on your network to act as content caches. Declaring your Mac as a content cache registers it with Apple content servers. Because an Apple server retains your public IP address and your content cache's local private address, a registration and discovery process can locate your network's cache. When an Apple device on your network tries to download Apple content that could be cached, the Apple content server instructs the device to check with the local network's cache first. If the content isn't available there, the content cache requests the content from the Apple server and stores it in the local network's cache. That content is then available for other Apple devices to retrieve without downloading it from the internet. Because a local network normally shares data much faster than the internet, subsequent devices can download cached content faster. Supported content includes operating-system updates, apps, books, iCloud content, and more.



Declarative device management is an update to the existing management protocol that works with the MDM protocol. It uses declarations to asynchronously update the device settings, restrictions, assets, and more. With status channels, devices proactively report the status of objects like passcode compliance and MDM-installed apps — without constant polling from the MDM server.

Traditional MDM is imperative:

“Hey phone, install this profile
now… tell me when you’re done…
now set this password rule…”

Declarative Device Management (DDM) is declarative:

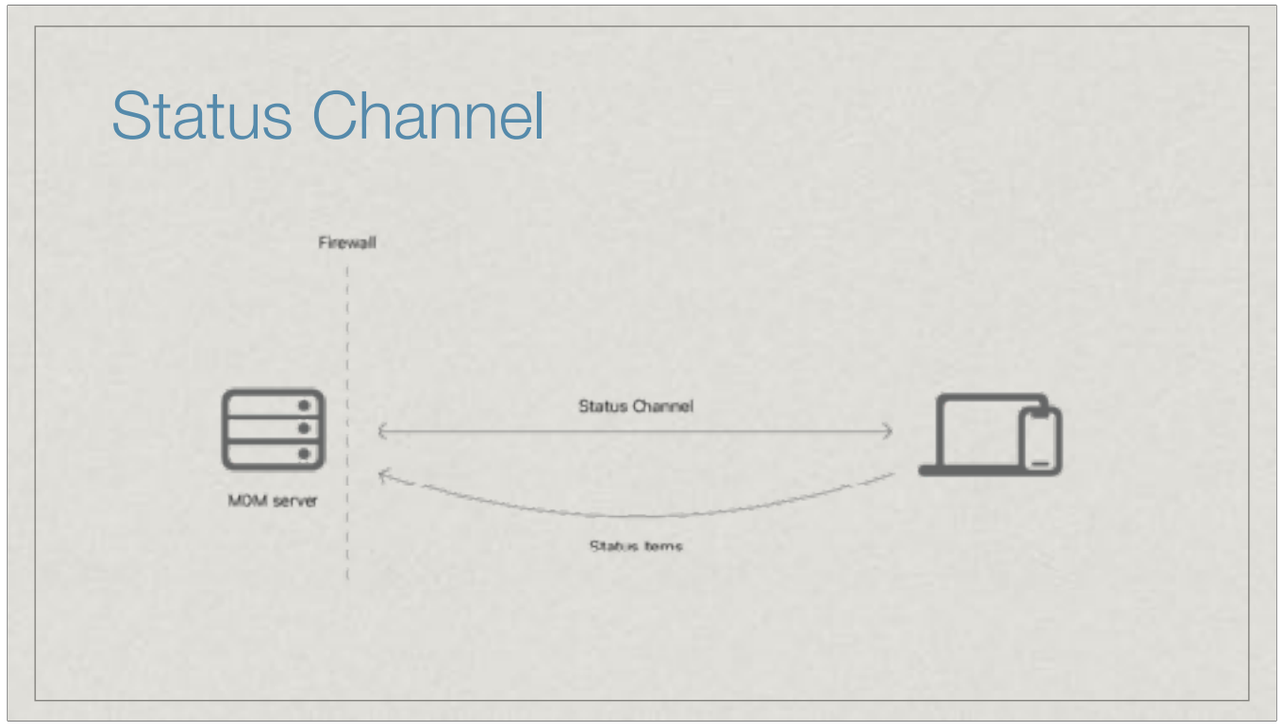
“Here are the rules that should always be true for any device that matches X-Y-Z. Keep yourself in that state and let me know if something drifts.”

Because the device knows the “desired state,” it can enforce policies locally, work while offline, and proactively tell the server when something changes—no constant polling required.

Part	What it is	Analogy
Configurations	Settings	Rules in a classroom
Assets	Things the configs need	Handouts that go along with the rules
Activations	Configs plus a condition	Lesson plan: hand out the exam on Friday to the 10th grade
Management Properties	Key/value pairs the server can send	Sticky notes on a rule board

Declarations are payloads representing policies the MDM server defines and sends to devices. There are four types of declarations:
Configurations are similar to the device management existing profile payloads; for example, accounts, settings, and restrictions. Assets consist of reference data that's required by configurations for large data items and per-user data; assets have a one-to-many relationship with configurations. Activations are a set of configurations that are applied atomically to the device and can include predicates, such as "device type is iPad" or "operating system version greater than iPadOS 16.1." There is a many-to-many relationship between activations and configurations. Activations can use an extended predicate syntax—including status items—to support complex predicate expressions.

In addition, a management properties declaration allows servers to set arbitrary properties on the device, which can be directly used in activation predicates. and Management conveys the overall management state to the device, describing details about the organization and the capabilities of the device management service.



With declarative device management, the device proactively updates the server with new information about itself. The MDM server subscribes to a device's status item, and updates to the device's information for this specific item are then incrementally reported back to the server.

Security

- Updates
- Passcodes
- Restrictions
- Managed Apple accounts
- Device Attestation

What is the minimum security baseline? It will depend on your environment. At a minimum, you need a device enrolled in MDM.

Updates

- Test beta software
- DDM (Maybe)
- Deferrals

Deploying software updates is critical to maintaining the security and integrity of Apple devices. Updating not only keeps your environment secure but also allows users to benefit from and enjoy the latest features and security fixes. Consequently, it's important for your organization to evaluate each key area that works together in your environment, all year long, so that you're ready to deploy each release as soon as possible.

Declarative device management can manage updates in iOS, iPadOS, and macOS. It provides new options for when and how a software update or upgrade should be enforced. Users get additional information in Settings on iPhone and iPad, and System Settings on Mac, when an update is requested and when it's enforced. You can also provide the URL of a webpage to provide more information and context about the update for users. Using declarative status reports, MDM solutions can also get increased transparency about the status of the update, for example, waiting for, downloading, or installing the update.

You can defer software updates for supervised Mac computers and iPhone, iPad, and Apple TV devices enrolled in an MDM solution. When you implement this restriction, the default deferral period is 30 days since update publication. You can specify a custom value anywhere from 1 to 90 days. You can set different deferral values for minor and major updates of macOS. However, an MDM solution can send specific updates to devices on any platform regardless of deferral restrictions.

Passcodes

- Allow simple
- Require alpha
- Min length
- Max age

About Passcodes and Passwords

When you prepare to deploy Apple devices, identify the security and privacy policies that you must implement. With MDM, you can configure payloads on enrolled devices to meet your organization's security requirements, including passcode requirements. You can require users to create device passcodes on enrolled iPhone or iPad devices, or local user account passwords on Mac computers, and set specific rules for passcode or password creation.

Here are some passcode and password configuration options:

Allow simple value — Permits the use of repeating, ascending, and descending character sequences

Require alpha-numeric value — Requires passcodes to contain at least one letter and one number

Minimum passcode length — Sets the minimum required number of characters

Maximum passcode age — Sets the number of days after which the user must change their passcode

Maximum number of failed attempts — Sets the number of failed passcode attempts that someone can make before iPhone or iPad is erased or the user account on the Mac is disabled

After the Passcode payload is installed on iPhone or iPad, users have 60 minutes to enter a new, compliant passcode. If users don't do so within that time frame, the payload forces them to enter a passcode using the specified settings.

On a Mac, you can use the Passcode payload to force the user to enter a new password the next time they authenticate. To support more complex requirements, the Passcode payload and declaration allow you to specify a password policy as a regular expression in macOS. Password compliance handling has changed so that when you apply new or changed password requirements without a user being logged in, compliance is verified during the next user login. If the user is logged in and the requirements appear to be as strict as the previous ones, the user is asked to verify their password compliance and, if necessary, update their password.

You can distribute a profile that enables the Passcode restriction to be enforced before Setup Assistant is complete. When using Automated Device Enrollment, you can configure Setup Assistant options so that the user can't finish setting up the device unless the password or passcode meets the criteria defined in the managed settings.

Restrictions

- Prevent an app or service
- Camera
- Facetime

Restrictions for Apple devices help meet your organization’s security, data protection, and user privacy goals. You can enable or, in some cases, disable restrictions to prevent users from accessing a specific app, service, or function of an Apple device that’s enrolled in an MDM solution. For example, you can add a restriction that prevents iPhone, iPad, Mac, or Apple Vision Pro from using the camera to take pictures or videos. Some restrictions require a device to be supervised. You configure restrictions in separate payloads for devices.
Organizations can use a new restriction in iOS 18, iPadOS 18, and macOS 15 to prevent ChatGPT integration in Siri and Writing Tools.
Note
If you have multiple configuration profiles that contain restriction payloads with different settings for the same specific restriction on iPhone or iPad, the more restrictive one takes effect.

Declarative management can also help you meet your organization’s security, data protection, and user privacy goals for Apple devices. You can set declarative configurations to manage the built-in Math and Calculator app settings on iPhone, iPad, and Mac devices enrolled in MDM. Use the settings to control the available modes, conversions, behaviors, and math notes.

Lost Devices

- Enabling lost mode
- Locating
- Disable
- Wipe

You can use your MDM solution to place a supervised device or device group into Lost Mode and issue Lost Mode commands to a supervised iPhone or iPad. When enabling Lost Mode on a device, you can customize the Lock Screen with a message, add a contact phone number, and include a note. You can use MDM to issue commands to locate a lost iPhone or iPad by selecting a device you want to locate in your MDM solution. When a supervised device is in Lost Mode, you can request the device's location depending on your MDM solution's features. When the request is successful, you can view the device location.
You can use MDM to issue commands to disable Lost Mode on a supervised iPhone or iPad. You can disable Lost Mode if it's erroneously enabled or enabled on a retrieved device.
You can select a device or device group with Lost Mode enabled and use your MDM settings to disable Lost Mode.
When the MDM solution remotely disables Managed Lost Mode, it unlocks the device. When unlocking the device screen, the MDM solution also notifies the user that it enabled Managed Lost Mode and collected the device's location.
For most supervised Apple devices, you can use MDM to wipe devices without touching them using the "Erase All Content and Settings" option. When you initiate a remote wipe command through MDM, the Apple device sends an acknowledgment back to the MDM solution and performs the wipe.
When the operating system is first installed or when the device is wiped by a user, a random volume key gets created that encrypts the metadata of all files in the data volume file system. When the encrypted file system key is stored, an additional "effaceable key" wraps the encrypted file system key which is stored in Effaceable Storage, protected by Secure Enclave anti-replay mechanism.
This process allows the key to be quickly erased on demand (by the user with the "Erase All Content and Settings" option, or by a user or administrator issuing a remote wipe command from a mobile device management (MDM) solution, Microsoft Exchange ActiveSync, or iCloud).

Managed Apple Accounts

- Work
- Personal

Managed Apple Account Security
A Managed Apple Account is a type of Apple Account designed specifically for use in an organization, like a business or school. You create and manage it through Apple Business Manager or Apple School Manager. Employees or students can sign in to a Managed Apple Account on devices, apps, and services and keep their data synced across devices without needing to use a personal Apple Account. The organization owns both the Managed Apple Account and data on it. With support from your MDM solution, you can take advantage of enhanced features that are available to the Managed Apple Accounts in your organization, including the following:
Supporting iCloud Keychain, Wallet, and Continuity, using account-driven Device Enrollment to enroll iPhone and iPad devices and Mac computers in management without a user needing to manually install a profile Configuring access management to control where users can sign in to Managed Apple Accounts and what apps and services they can use Integrating identity providers with Apple Business Manager or Apple School Manager to support federated authentication, directory sync, and account security events

Work and Personal Data
On Apple devices, you can manage work and personal data separately, without segmenting the user experience. Users can install personal and organizational apps on their devices. Apple devices enrolled in an MDM solution with either User Enrollment or account-driven Device Enrollment keep data separate without using third-party solutions.

Device Attestation

- What is it
- What does it protect against

Managed Device Attestation
Managed Device Attestation is a feature in iOS 16, iPadOS 16.1, macOS 14, tvOS 16, or later. It provides strong evidence about which device properties you can use as part of a trust evaluation. This cryptographic declaration of device properties is based on the security of the Secure Enclave and the Apple attestation servers.
Managed Device Attestation helps protect against these threats: A compromised device lying about its properties, A compromised device providing an outdated attestation A compromised device sending a different device's identifiers A private key extraction for use on a rogue device An attacker hijacking a certificate request to trick the certificate authority (CA) into issuing the attacker a certificate
Managed Device Attestation with ACME certificate enrollment requests
An organization's issuing Certification Authority (CA) ACME service can request an attestation of the enrolling device's properties. This attestation provides strong assurances that the properties of the device (for example, the serial number) are legitimate and not spoofed. The issuing CA's ACME service can cryptographically validate the integrity of the attested device properties and optionally cross-reference them against the organization's device inventory and, upon successful verification, confirm that the device is the organization's device. If you use attestation, the operating system generates a hardware-bound private key inside the device's Secure Enclave as part of the certificate-signing request. For this request, the ACME-issuing CA can then issue a client certificate. This key is tied to the Secure Enclave and is therefore available only on a specific device. You can use it on iPhone, iPad, Apple TV, and Apple Watch with configurations supporting specification of a certificate identity. On a Mac, you can use hardware-bound keys for authentication with a device management service, Microsoft Exchange, Kerberos, 802.1X networks, the built-in VPN client, and built-in network relay.

Important Links

- https://support.apple.com/en-ca/guide/apple-business-manager/welcome/web
- https://github.com/macadmins
- https://support.apple.com/en-ca/guide/apple-school-manager/welcome/1/web
- https://it-training.apple.com/tutorials/apt-deployment
- https://www.macadmins.org/
- https://www.dnb.com/duns-number/lookup.html

Ok, so let’s open it up for some Q and A.