Updating Your District's Legacy Apple Environment

Spotlight on **Activation Lock** and **Managed Apple ~~IDs~~ Accounts**

Philip Bauchan
Missisquoi Valley School District
IT Help Desk Technician

Apple IDs is crossed out because Apple recently rebranded them to being Apple Accounts. The first of many "updates" to managing Apple devices that this presentation covers.

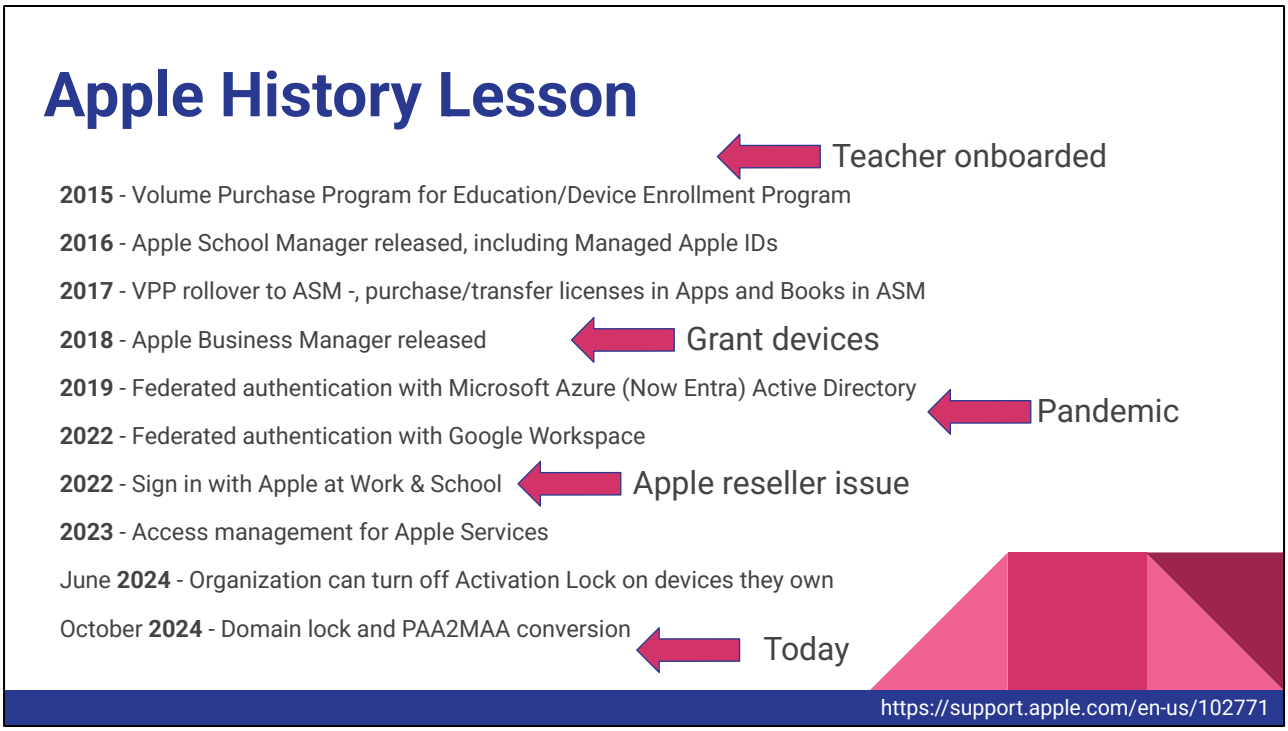
Preface and Outline

- Beyond the basics
- Only about ASM, not MDM
- Not about Apps/tokens
- Technical know-how, not organizational strategy
- Improve security posture and prepare for the future

1. Apple History Lesson
2. Activation Lock
3. Managed Apple Accounts

Left column is some prefatory comments on what the talk is about while the right column is a basic outline of the presentation.

A plug for the Mac Admins Foundation and especially the Mac Admins Slack as the best place to learn about and asking questions related to Apple management.



A brief timeline of all of the major changes to managing Apple devices in Apple School Manager over the last decade. The arrows indicate various “events” for a typical district that, when carried over, have likely produced circumstances of being at odds with current best practices. In short, it’s understandable that school’s find themselves with conflicting arrangements because these now-legacy ways of doing things used to be *the* way of managing devices with Apple, with many of these changes being extremely recent.

Activation Lock

You don’t need it, root it out!

The basic gist of this section. It is a consumer-grade feature of Apple devices (even if Apple has made some accommodations for it for organizations, as will be seen).

When Activation Lock is turned on, it's difficult for anyone else to use or sell a person's iPhone, iPad, Mac, or Apple Watch. Managing Activation Lock with an MDM solution lets your organization benefit from its theft-deterrent functionality while simultaneously providing you the ability to turn off Activation Lock for devices your organization owns. There are two types of Activation Lock available:
Organization-linked: Organization-linked Activation Lock requires Apple School Manager, Apple Business Manager, or Apple Business Essentials and is generally simpler to manage for organizations. It allows an MDM solution to fully control turning Activation Lock on and off through server-side interactions. User-linked: User-linked Activation Lock requires the user to have a personal Apple Account (not a Managed Apple Account) and for them to turn on Find My. This method allows the user to lock an organization-linked device to their personal Apple Account if the MDM solution has allowed Activation Lock.
Note: Some MDM solutions support both Activation Lock methods; if an attempt is made to use both, the first successful Activation Lock event takes precedence. Turn off Activation Lock
In Apple School Manager, Apple Business Manager, or Apple Business Essentials, a user with Manage Device privileges can turn off organization-linked and user-linked Activation Lock for an iPhone, iPad, Mac, Apple Watch, or Apple Vision Pro that their organization owns. The device must appear in Apple School Manager, Apple Business Manager, or Apple Business Essentials; however, it doesn't need to be assigned to an MDM server. For more information, see: Apple School Manager User Guide: Turn off Activation Lock Apple Business Manager User Guide: Turn off Activation Lock Apple Business Essentials User Guide: Turn off Activation Lock Organization-linked Activation Lock for iPhone and iPad
Allowing organization-linked Activation Lock means the MDM solution (not the user) contacts Apple servers directly to lock or unlock the device. Since this is done entirely server-side, there are no dependencies on user actions or the state of their device. The MDM solution creates its own bypass code, and sends it to Apple servers when it needs to turn on or turn off Activation Lock for the device. Suppose that your MDM solution is unsuccessful in removing Activation Lock. Then on the Activation Lock Screen, enter the user name and password of the account that created the MDM server token that links the MDM solution to Apple School Manager, Apple Business Manager, or Apple Business Essentials. This is an account with the role of Administrator, Site Manager (Apple School Manager only), or Device Enrollment Manager. Important: If your devices are assigned to an MDM solution linked to Apple School Manager, Apple Business Manager, or Apple Business Essentials, you should use this method.
In contrast with organization-linked Activation Lock, user-linked Activation Lock lets users lock devices your organization owns with their personal iCloud account. In this case, MDM solutions can allow users to turn on Activation Lock on an organization-linked supervised device. Because Activation Lock is disallowed by default on supervised devices, the MDM solution should fetch a bypass code created by the device and store it before allowing the user to turn on Activation Lock. In case the user is unable to authenticate with their Apple Account for any reason, including if they've left the organization, this bypass code can be used to turn off Activation Lock remotely with MDM, or directly on the device, when the device needs to be erased and assigned to a new user. On iPhone and iPad, the bypass codes are available for up to 15 days after the device is first supervised, or until an MDM solution has obtained—and then cleared—the code explicitly. If an MDM solution hasn't retrieved the bypass code within 15 days, that bypass code is unretrievable. Mac computers require Apple silicon or the Apple T2 Security Chip to be eligible to use Activation Lock. If an eligible Mac computer is using Device Enrollment and is upgraded to macOS 10.15 or later, Activation Lock is disallowed by default and can optionally be allowed. Managing Activation Lock on installations (not upgrades) of macOS 10.15 or later require the device to be supervised. In macOS 11 or later, if a device is supervised using Device Enrollment, Activation Lock can't be managed until the point at which the device is enrolled into MDM. That means it may be possible for Activation Lock to already be turned on when the device is enrolled in MDM and becomes supervised. In that case, it can't be turned off using MDM and won't be disallowed by default until it is first turned off by the user. If you have physical possession of the device, on an iPhone or iPad, enter the MDM Activation Lock bypass code on the Activation Lock Screen in the Apple Account password field, and leave the user name field blank. On a Mac, the bypass code can be entered by clicking Recovery Assistant in the menu bar and selecting the "Activate with MDM key" option. Consult your MDM vendor's documentation on where to locate the bypass code. When MDM allows user-linked Activation Lock, the following occurs: If Find My is on when your MDM solution allows Activation Lock, Activation Lock is turned on at that time. If Find My is off when your MDM solution allows Activation Lock, Activation Lock is turned on the next time the user turns on Find My. Using bypass codes to clear Activation Lock
To manage Activation Lock, your MDM solution must store two bypass codes: The device-generated bypass code. The MDM solution retains this code until it receives a different, nonempty code from the device. For more information, see the Get the Bypass Code for Activation Lock query. The bypass code the server creates when initiating Activation Lock through MDM. The bypass codes that the MDM solution uses to manage Activation Lock are crucial to your ability to clear Activation Lock. These bypass codes should be secured and backed up regularly. If a change in MDM vendors is made, make sure that you're provided with a copy of those bypass codes, or that Activation Lock is cleared for all enrolled devices. To clear the Activation Lock on Apple devices that support dual SIMs, the MDM solution must include both IMEI (International Mobile Equipment Identity) values in the request. For MDM vendors, see Creating and Using Bypass Codes on the Apple Developer website. If your MDM solution is unable to remove Activation Lock, contact your MDM vendor support resources or see the Apple Support article How to remove Activation Lock.

https://support.apple.com/guide/deployment/activation-lock-depf4ab94ef1/web

If you DO want to use Activation Lock in your domain, this is a copy/paste of the technical documentation Apple has for understanding Activation Lock and how it works.

What is Activation Lock?

Activation Lock is effectively a server flag for claiming ownership. Next slide explains in more details.

What is Activation Lock?

A “flag” in Apple’s server that *locks* a device to a certain Apple ID at *activation*

Flag = OWNERSHIP

User-linked (via Find My)

Organization-linked (via MDM)

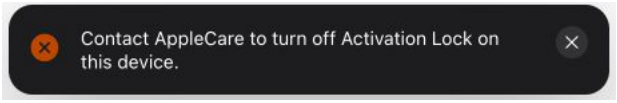
User-linked but MDM-allowed

A basic statement as to what Activation Lock is and how to think of it. As stated, it is a flag that is used to claim ownership of a device.
The bottom are the three types of Activation Lock configurations that are possible. User-linked is the one most common and the one most people are familiar with. Organization-linked is when the Apple Account that generates the APNS token for the device is used to initiate Activation Lock on device(s), which must be managed by an MDM. Most MDM enrollment flows, by default, disable user-linked Activation Lock but it can technically be allowed, which can also be overridden using an MDM command similar to the organization-linked version.

How to Deal with It

Ask: “When was the flag planted?”

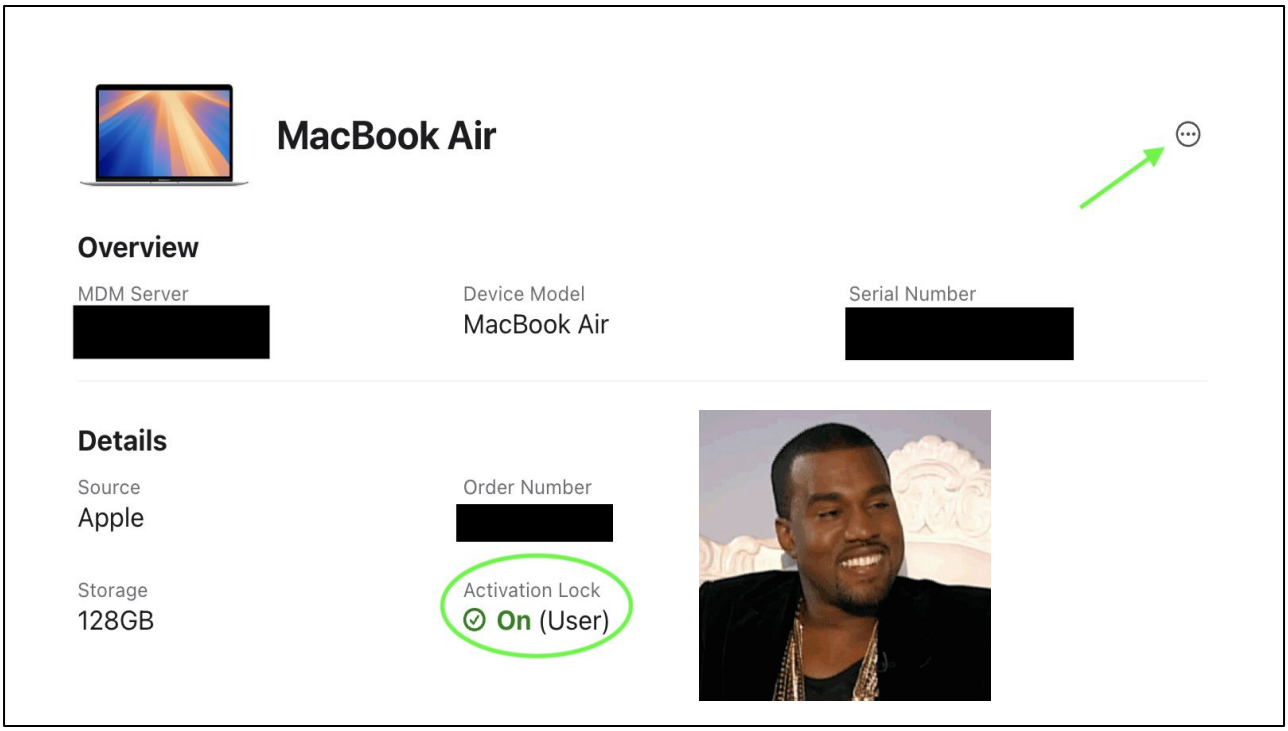
- Planted, but device not in ASM? **SOL**
- Device in ASM, then planted? **Turn off in ASM**
- Planted, *then* device added to ASM? **Manual Process***



If both user- and organization-linked are attempted, first applied takes precedence

https://al-support.apple.com/#/getsupport

How you deal with Activation Lock on an organization device is dependent upon when Activation Lock was turned on. Just because a device is “organization owned” does not mean Apple recognizes that fact, as seen in the case of a device that is not listed in Apple School Manager. The new feature Apple added is for the second scenario. However, the third scenario is still possible and the only route is to manually submit a request to Apple at the URL posted in the bottom right corner. This is the same whether the device was added with AC2 or an Authorized Reseller. AppleCare support allows for expedited responses,while general Apple support can take a week or more. There is also an Open Source tool that can help you manage user-linked Activation Lock if none of these routes work: https://github.com/bvanpeski/unActivationLock



This is what it looks like when Activation Lock is enabled on a device in your Apple School Manager instance. Click on the meatball menu icon to disable it. When you see this you smile like Kanye knowing you can turn it off, but then you realize that this doesn't actually do anything to stop a user from re-enabling Activation Lock on your device afterwards. That requires actions via your MDM.

Activation Lock Summary

- Not needed!
- “Flag” on Apple’s server
- What type of flag?
- When was it planted?

Lost Mode and automatic re-enrollment in iOS/iPadOS/macOS is the Apple preferred manner for organizations to manage their devices in a manner akin to Activation Lock.

Managed Apple Accounts cannot use **Find My** and so cannot use **Activation Lock**

Transition between the two main topics - if you use Managed Apple Accounts in your organization then Activation Lock can’t even be turned on by a user because MAAs do not have access to Find My!

Managed Apple Accounts

What they do (and don't do)

1. Apple services - Handoff, iMessages, iCloud storage, Apple Classroom
    a. ASM allows you to control what kind of device a MAA can sign into, but currently no MDM payload that allows you to determine what kind of AA can sign into your devices
2. Apple *User Enrollment* for BYOD
    a. Can only have one version of the app on the phone
3. ***Platform SSO
    a. Sign in with Apple - the future with Platform SSO?

Quick overview of what MAAs do. Principally they are used for Apple services, which your organization might not use. They can also be used for device enrollment, in particular BYOD devices that allow some organization management of an otherwise personally owned device. Lastly, while not tied to Platform SSO, Apple is continually expanding its offering and it possible that MAAs may come to play a larger role in managing Apple devices.

In short - it’s entirely possible to have an organization that doesn’t make use of Apple Accounts in any form. MAAs give some tools for organizational management of Apple devices, but they are no silver bullet.

Apple (Old) School Manager

Verify

Add TXT record to DNS

Federate

Start process to Federate by connecting to your IdP. Once you've connected to your IdP, you can click Enable Federation, which allows you to send a notification to those accounts that have used your organization's email address to create a PAA informing them that they need to change to a new email address to something that is not your domain, plus it gives you a static count of how many conflicts there are, but no list of user names. After precisely 60 days, your domain has been reclaimed with absolutely no updates along the way. After those 60 days, you can ultimately decide to Federate or not as a final step.

The real ease of use for MAAs comes from having them federated with an IDP. This documents the old process for how federating your Apple instance went - two steps, but with many convoluted sub-components as part of that federation process.

Apple School Manager

1. Verify
2. Lock
3. Capture
4. Federate

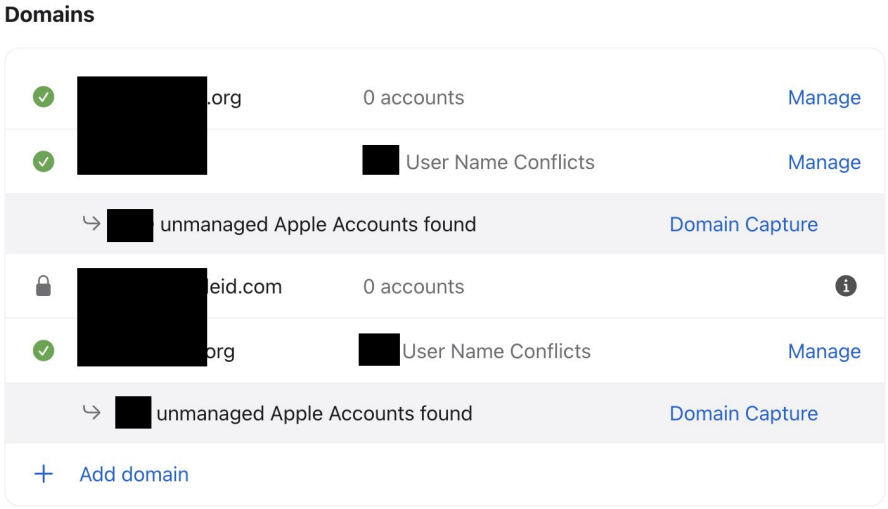
The new process - four steps, any one of which can be as far as your organization goes with the process.

Apple School Manager

1. Claim it
2. Lock it
3. Catch it
4. Fuse it

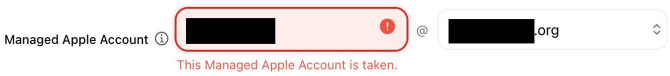
The process repeated to the beat of Daft Punk's "Technologic."

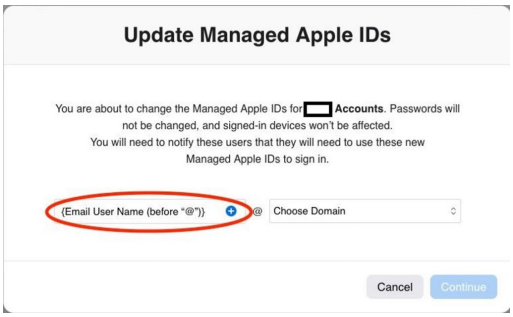
Verify



What it looks like on the domain page. Green checkboxes indicate a verified domain. The gray lock is for the default domain that Apple gives you when you set up ASM. The “User Name Conflicts” is the count that a particular domain has for Apple Accounts that already exist that use your domain’s email address but yet are not created in ASM and so not Managed Apple Accounts.

Pierce the Apple Veil



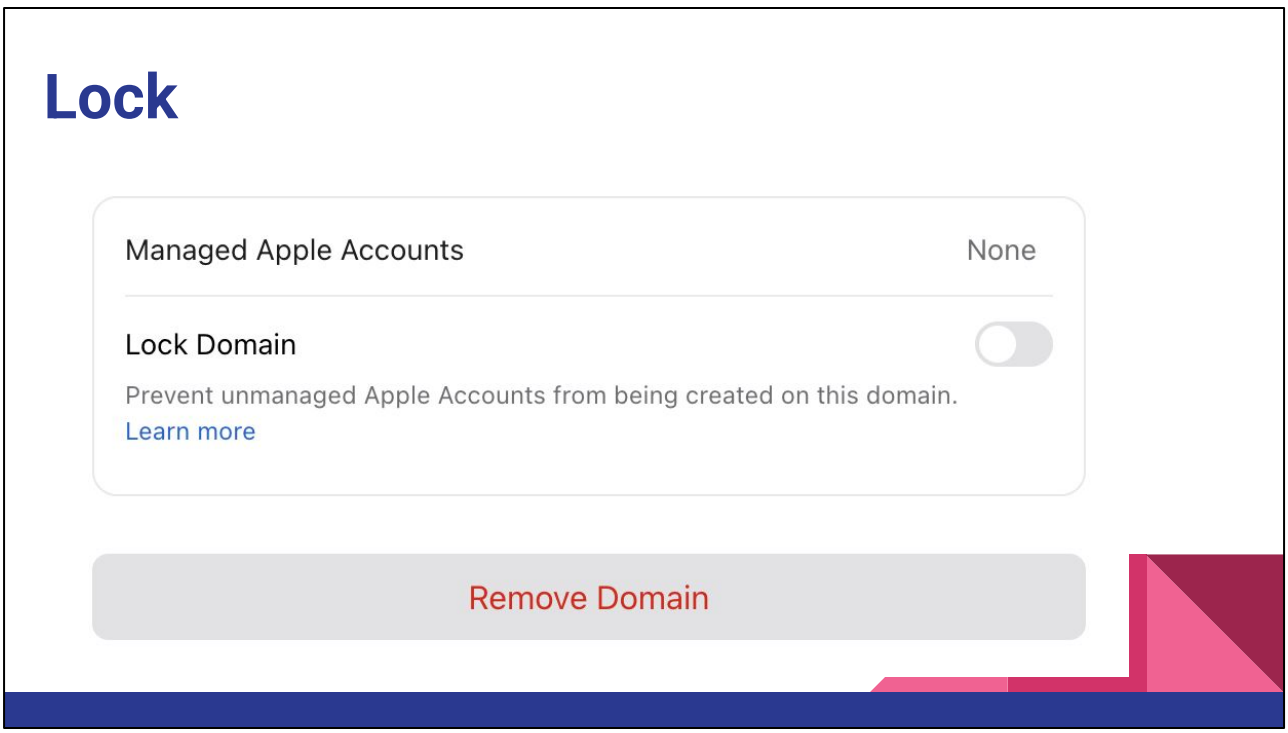


emailusername1@yourdomain.org

https://layersofabstraction.blog/2024/08/12/identify-personal-apple-accounts-on-your-domain/

Apple will only give you a COUNT of those conflicts but otherwise doesn't give you a list of emails so you can address it with your users. However, you can "massage" ASM to give your a list by trying the bulk edit action where you set your MAA to be the format of your organization's email. If you do that, it adds a 1 on the end. Blog post gives details of how the process can work to get you a list of user conflicts.

Lock

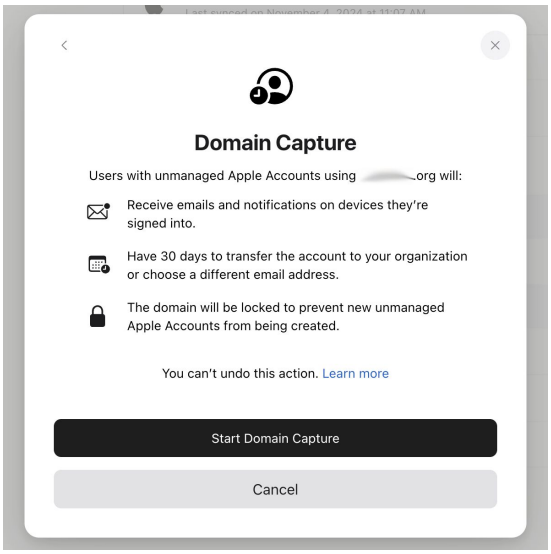


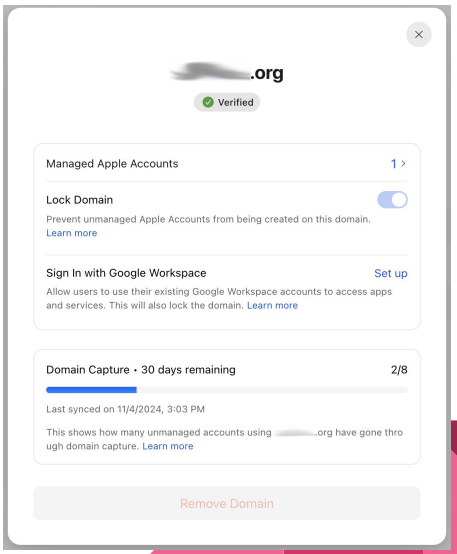
Domain lock prevents Apple Accounts being created on your domain unless done through ASM. Once locked, the only way to remove the lock is to remove the domain (which can then be re-added).

Lock your domains, people!

Best practices would have you at least limit the ability of users to create Apple Accounts outside of your organization’s control, even if you don’t go through the process of re-capturing those emails into organizational management.

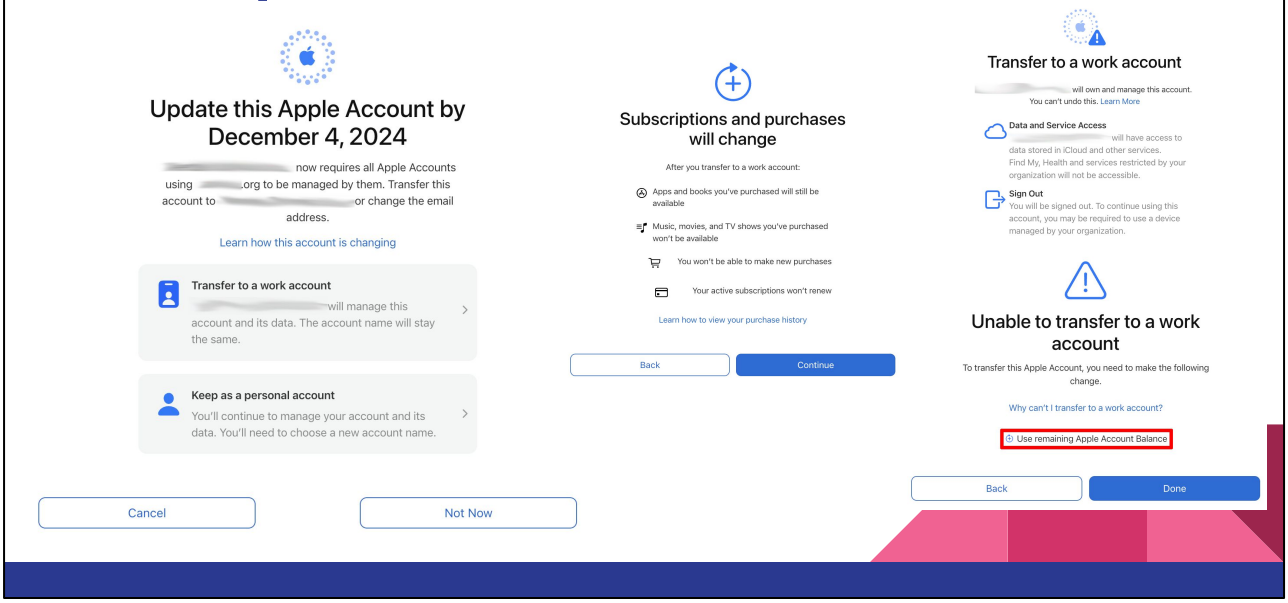
Domain Capture and PAA Conversion





What the process of domain capture looks like from within the ASM UI. You get a countdown of the now 30 day process, and a count of how many accounts have gone through the process (but again no list of emails/users).

User Experience of PAA Conversion



What the process of PAA conversion looks like for a user.

Managed Apple Accounts Summary

- Federated MAAs
- BYOD
- Future Apple functionality

Reiterate that with these new functionalities rolled out by Apple it is time to revisit Apple Accounts in your domain.

Traditional	Initial	Advanced

❏ No ASM
❏ PAAs
❏ Manual provision of devices
❏ Activation Lock
	❏ Verified & Locked ASM Domains
	❏ MAAs (no PAAs)
	❏ ASM enrolled devices
	❏ MDM management
		❏ Reclaimed Domain
		❏ Federated MAAs
		❏ ADE enrolled devices
		  ❏ Auto re-enroll
		  ❏ Blocks AL

CISA ZTMM

Looking at how ASM might be configured as seen through the lens of CISA's Zero Trust Maturity Model.