Software Update

The Missing Manual

Tom Bridge, JumpCloud

Software Update

discoveryd (2): Electric Bugaloo

Tom Bridge, JumpCloud

Software Update

Threat Or Menace?

Tom Bridge, JumpCloud

jumpcloud™

Software Update

A Guide to Safe Use

Tom Bridge, JumpCloud

Software Update

Where We're Going, Where We've Been

Tom Bridge, JumpCloud

How do macOS & iOS Update in 2023?

Key Resource: Platform Deployment Guide

Key Resource: Platform Security Guide

Key Vocabulary

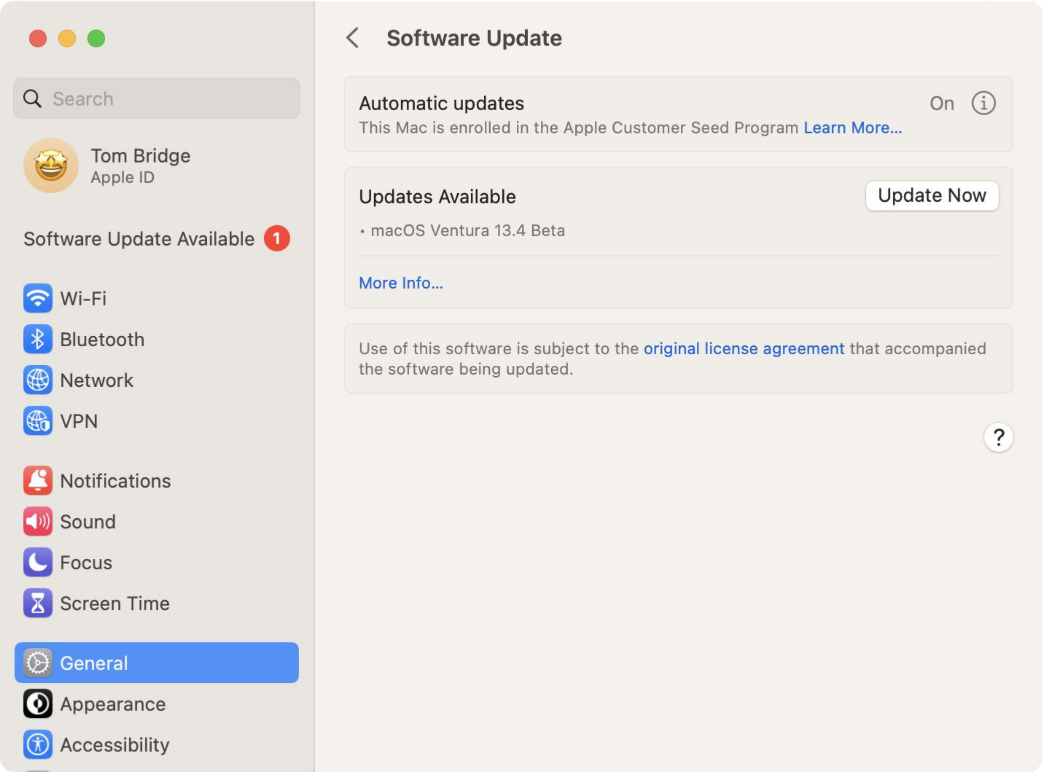
Update: A minor release of macOS - from 13.2.1 to 13.3

Upgrade: A major release of macOS - From 12.x to 13.x

Over the Air (OTA) Update: An update that does not require the entire monolithic installer for macOS. New in macOS 12.3 and later. Specific data necessary to go from current version to the newest version.

Universal Mac Assistant (UMA): An app-driven update to the operating system.

The Update Process - System Settings



Software Update

Automatic updates On

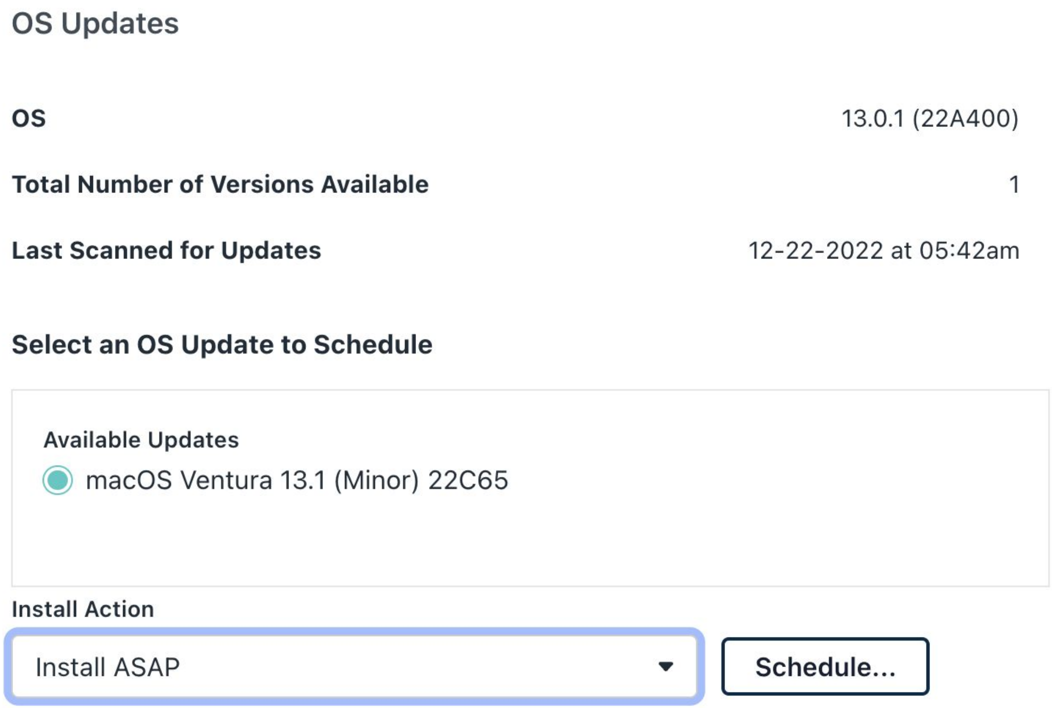
This Mac is enrolled in the Apple Customer Seed Program Learn More...

Updates Available

- macOS Ventura 13.4 Beta

Use of this software is subject to the original license agreement that accompanied the software being updated.

The Update Process - Via MDM



OS Updates

OS	13.0.1 (22A400)
Total Number of Versions Available	1
Last Scanned for Updates	12-22-2022 at 05:42am

Select an OS Update to Schedule

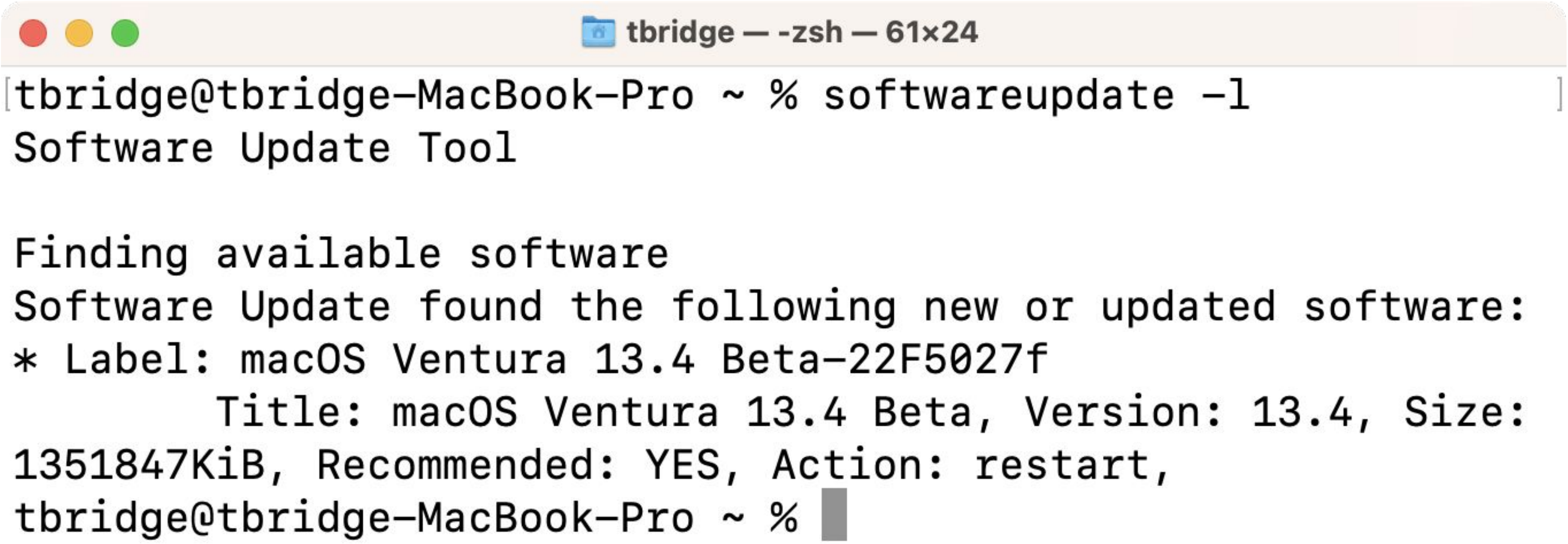
Available Updates

● macOS Ventura 13.1 (Minor) 22C65

Install Action

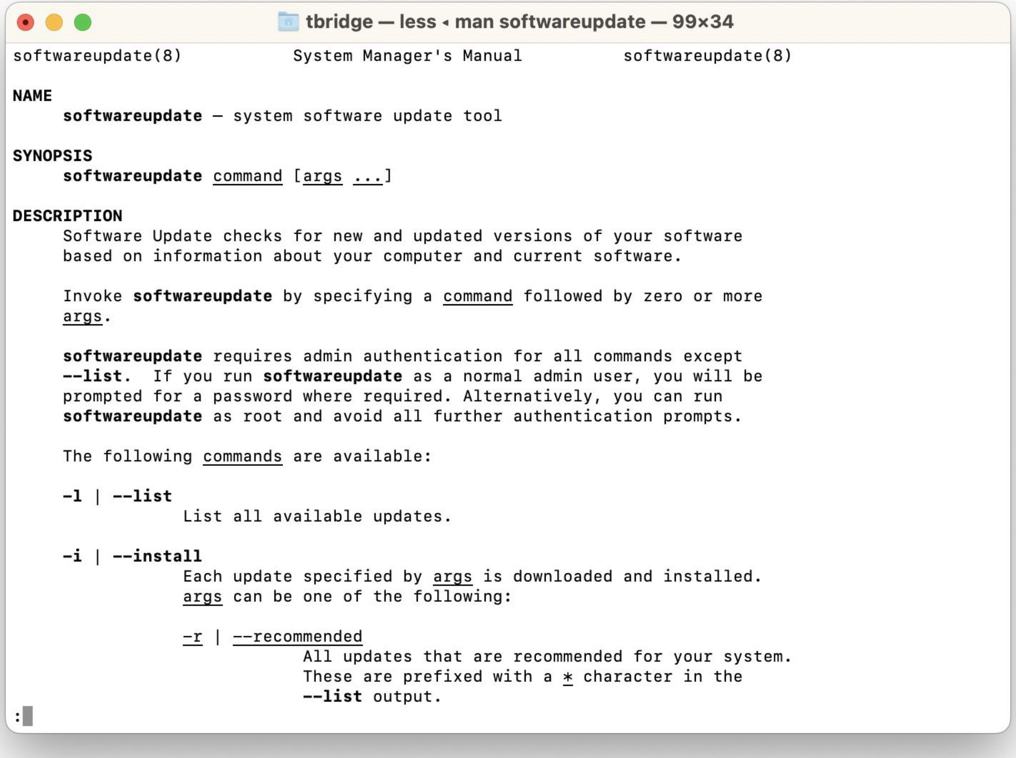
Install ASAP ▾

The Update Process - Via Terminal



```
tbridge@tbridge-MacBook-Pro ~ % softwareupdate -l
Software Update Tool

Finding available software
Software Update found the following new or updated software:
* Label: macOS Ventura 13.4 Beta-22F5027f
        Title: macOS Ventura 13.4 Beta, Version: 13.4, Size:
1351847KiB, Recommended: YES, Action: restart,
tbridge@tbridge-MacBook-Pro ~ % 
```

The Update Process - Via Terminal

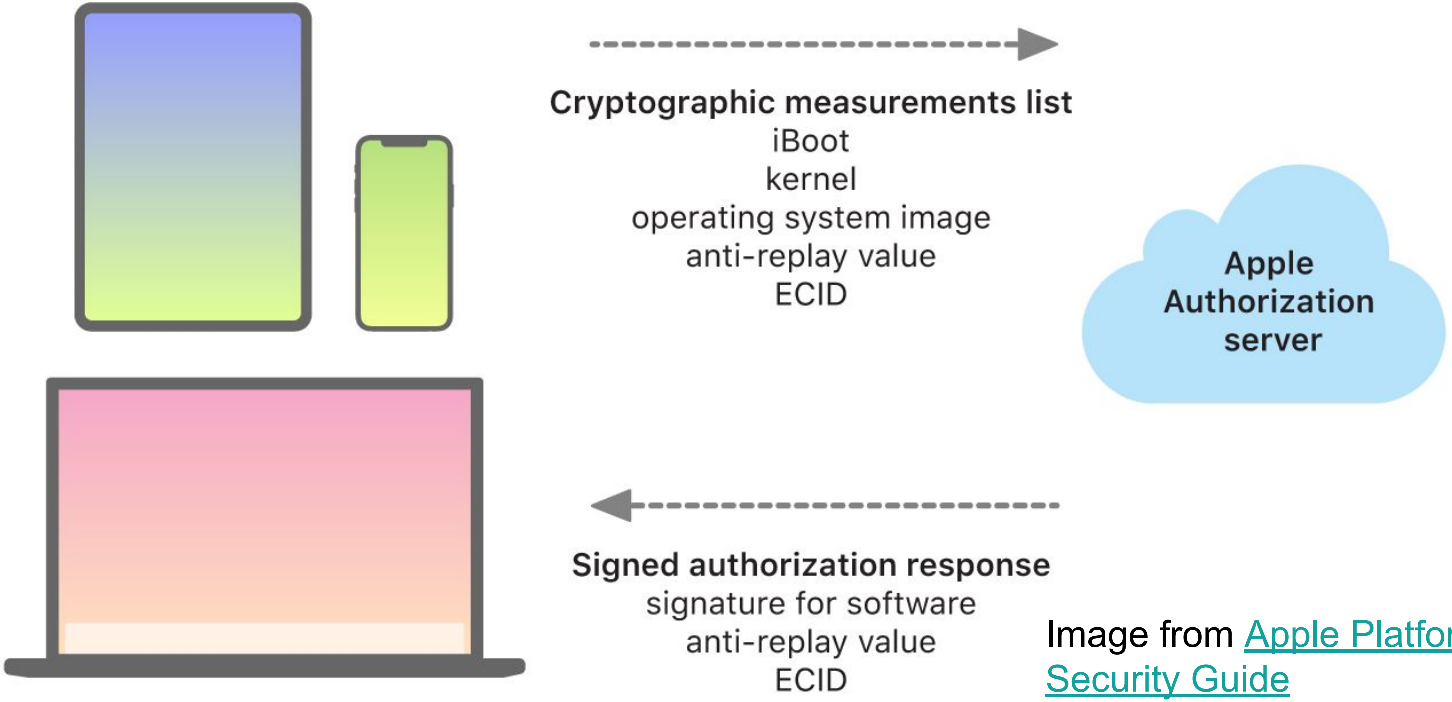


```
softwareupdate(8)            System Manager's Manual           softwareupdate(8)

NAME
     softwareupdate – system software update tool

SYNOPSIS
     softwareupdate command [args ...]

DESCRIPTION
     Software Update checks for new and updated versions of your software
     based on information about your computer and current software.

     Invoke softwareupdate by specifying a command followed by zero or more
     args.

     softwareupdate requires admin authentication for all commands except
     --list.  If you run softwareupdate as a normal admin user, you will be
     prompted for a password where required. Alternatively, you can run
     softwareupdate as root and avoid all further authentication prompts.

     The following commands are available:

     -l | --list
                 List all available updates.

     -i | --install
                 Each update specified by args is downloaded and installed.
                 args can be one of the following:

                 -r | --recommended
                             All updates that are recommended for your system.
                             These are prefixed with a * character in the
                             --list output.
:
```

So you have the bits…

Now what?

The Update Process - Personalization



Cryptographic measurements list
iBoot
kernel
operating system image
anti-replay value
ECID

Apple Authorization server

Signed authorization response
signature for software
anti-replay value
ECID

Image from Apple Platform Security Guide

The Update Process - Personalization

During upgrades and updates, a connection is made to the Apple installation authorization server, which includes a list of cryptographic measurements for each part of the installation bundle to be installed (for example, iBoot, the kernel, and the operating system image), a random anti-replay value (the nonce), and the device’s unique Exclusive Chip Identification (ECID).

Text from Apple Platform Security Guide

Traffic to and from Apple

- Don’t Attempt to Inspect SSL/TLS Traffic to/from Apple
- Don’t Block Outbound Connections to Apple
- If You Have A Proxy, Skip It for Apple Traffic
- Content Caching is Fine! Reposado Isn’t, Anymore

Knowledge Base Article HT210060: Use Apple Products on Enterprise Networks

A Brief Interlude on History

Software Updates In Recent Apple History

The Past Is Prologue

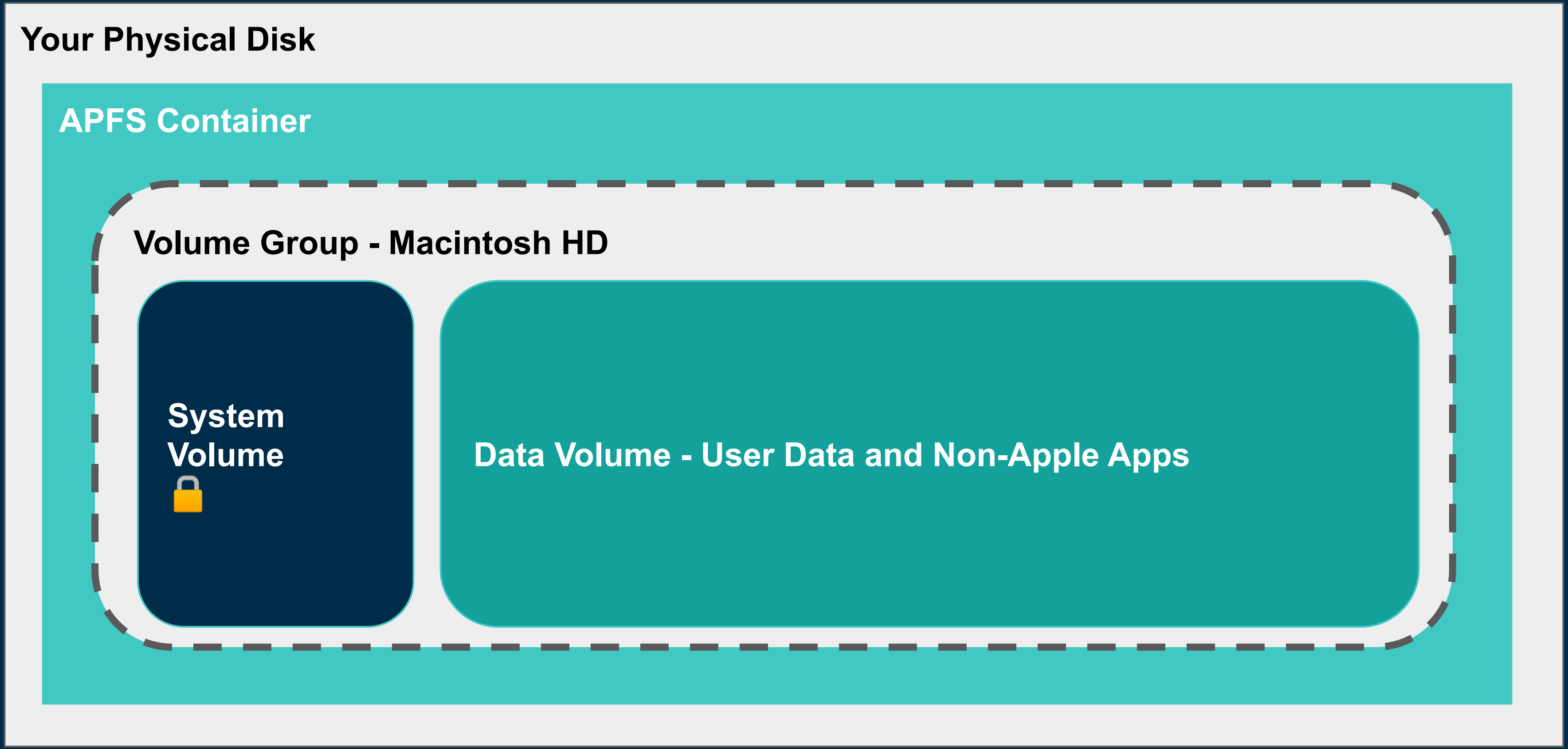
- El Capitan (OS X 10.11) introduces System Integrity Protection (SIP)
- Some directories on disk are read-only without special permissions granted only to Apple

The Past Is Prologue

- Sierra (OS X 10.12) introduces APFS, first for solid state drives
- APFS has a number of improvements over the previous HFS+ filesystem

The Past Is Prologue

- Catalina (macOS 10.15) creates an APFS Volume Group and moves the System to a read-only volume.
- Can technically be mounted read-write and changed, but shouldn’t be.
- Software Catalogs are Formally Deprecated.



Your Physical Disk

APFS Container

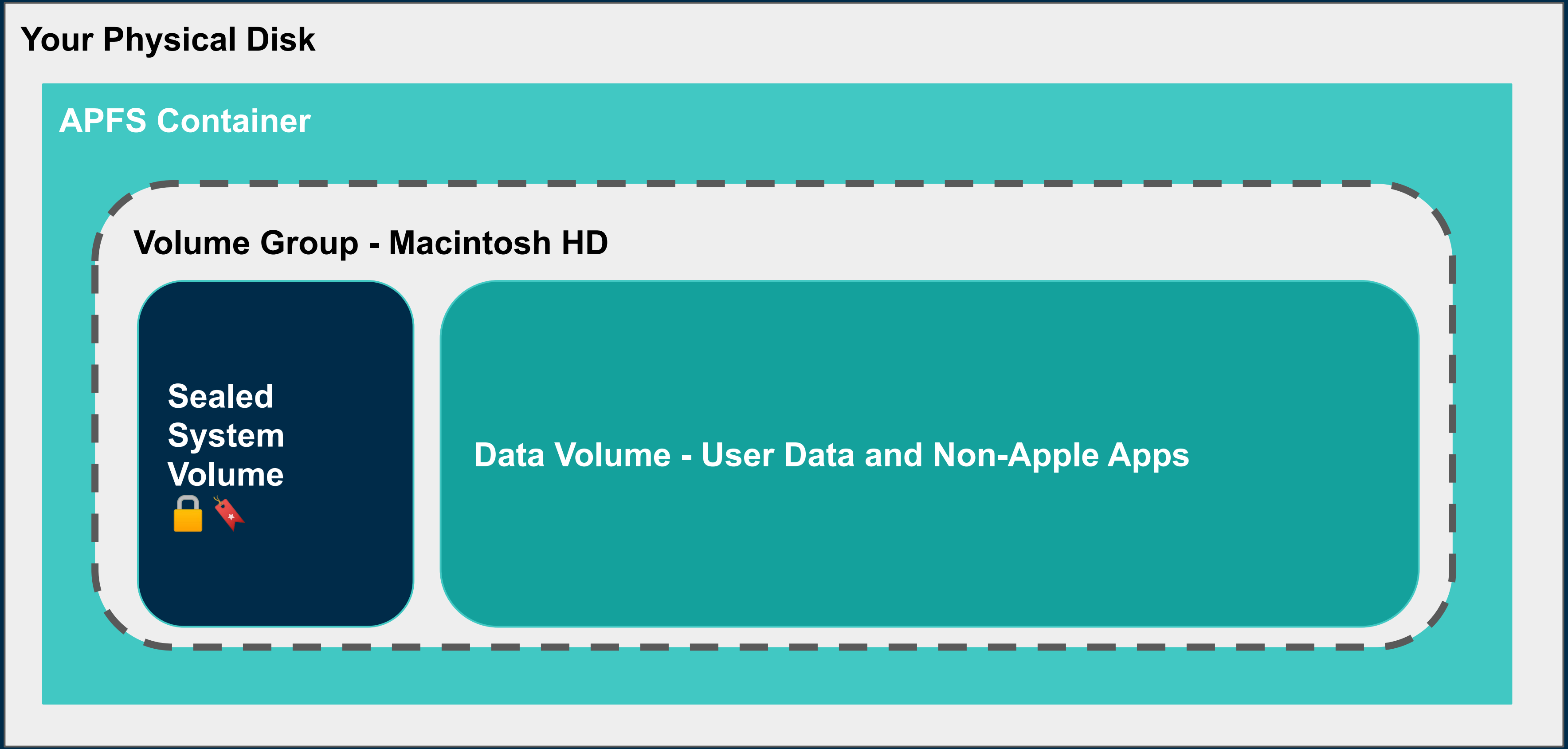
Volume Group - Macintosh HD

System Volume 🔒

Data Volume - User Data and Non-Apple Apps

The Past Is Prologue

- Big Sur (macOS 11) locks down that System Volume with a cryptographic seal.
- Booting is now accomplished by mounting a snapshot of that APFS volume.



Your Physical Disk

APFS Container

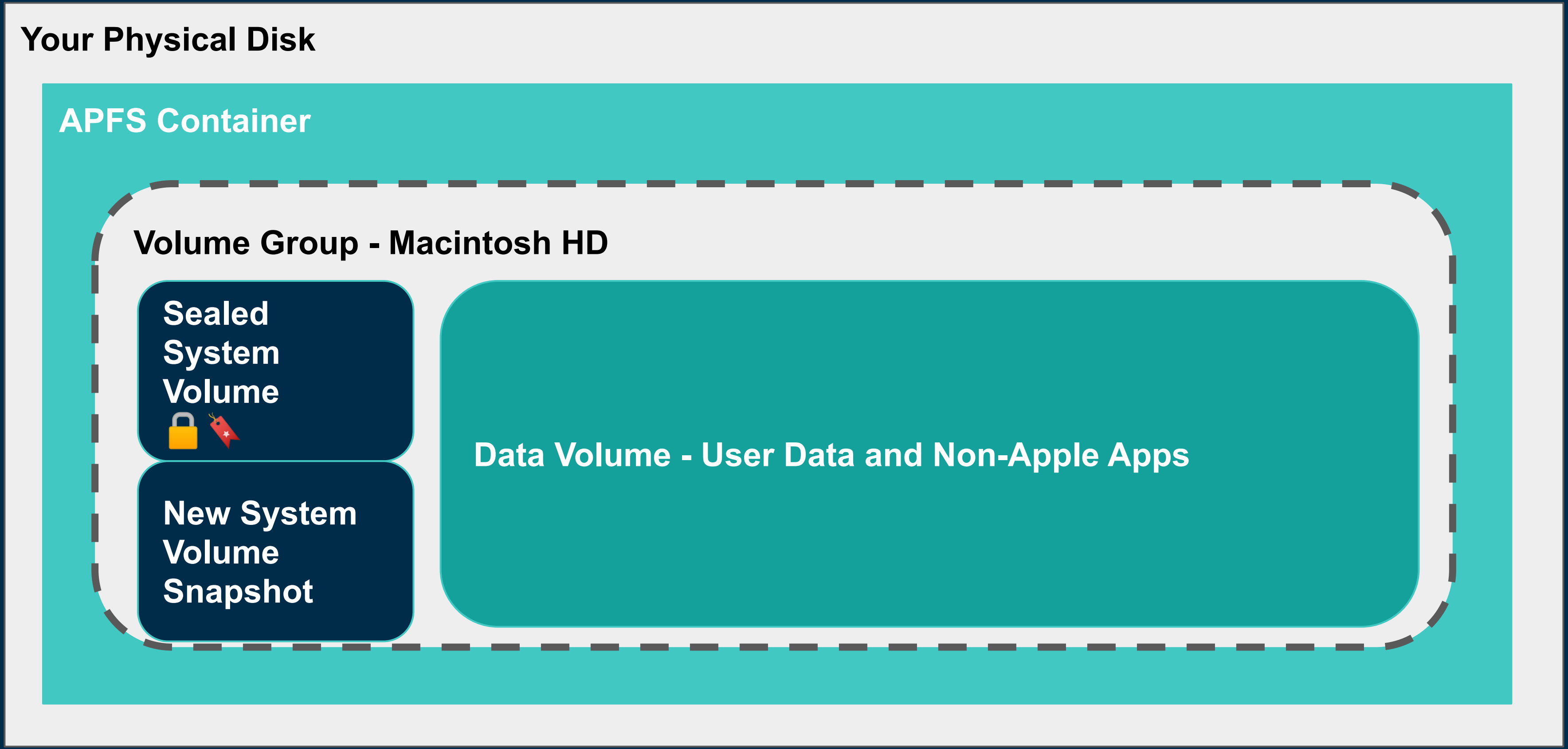
Volume Group - Macintosh HD

Sealed System Volume 🔒 🔖

Data Volume - User Data and Non-Apple Apps

Okay, but Updates?

Right. Stay on topic, Thomas.



Your Physical Disk

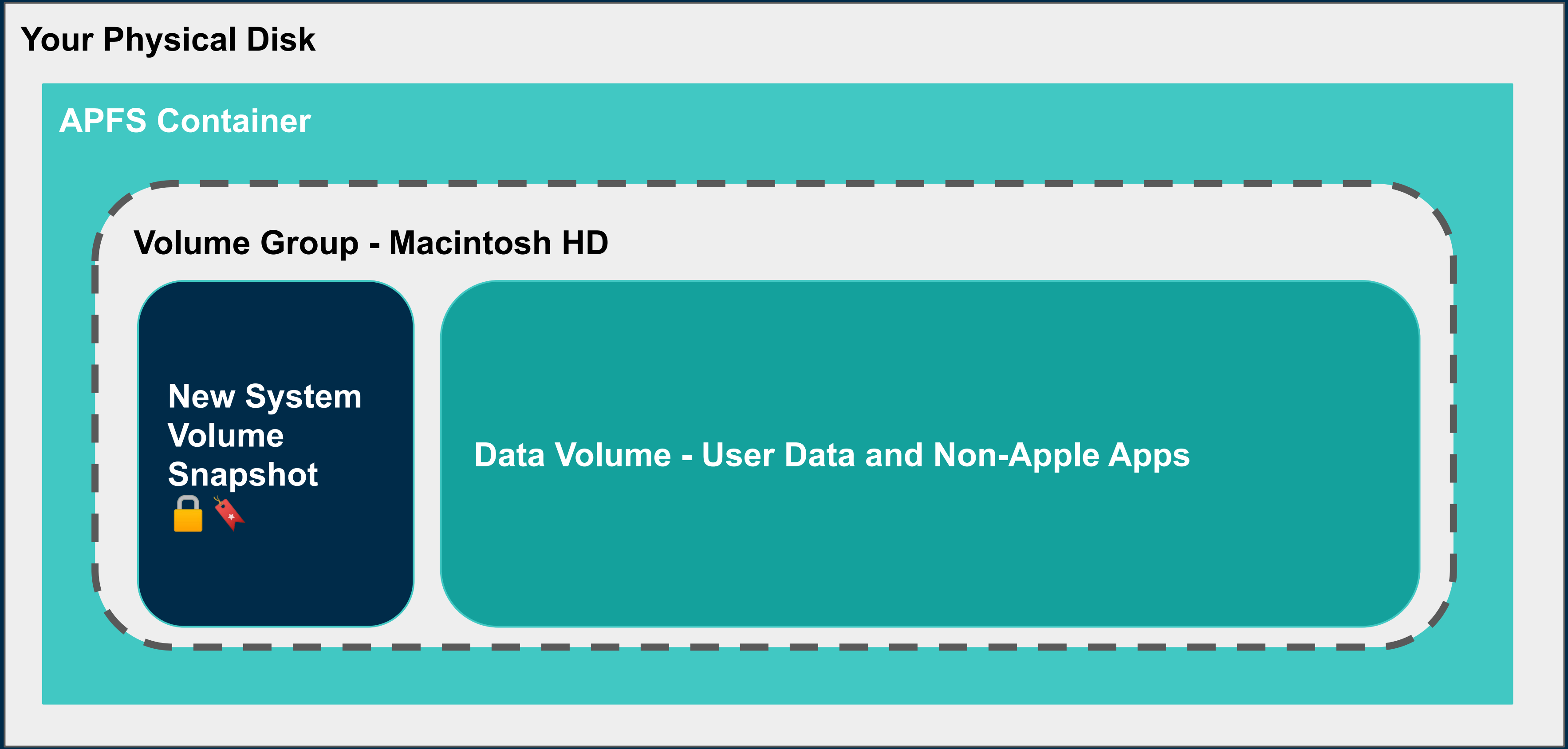
APFS Container

Volume Group - Macintosh HD

Sealed System Volume 🔒 🏷️

New System Volume Snapshot

Data Volume - User Data and Non-Apple Apps



Your Physical Disk

APFS Container

Volume Group - Macintosh HD

New System Volume Snapshot 🔒 🔖

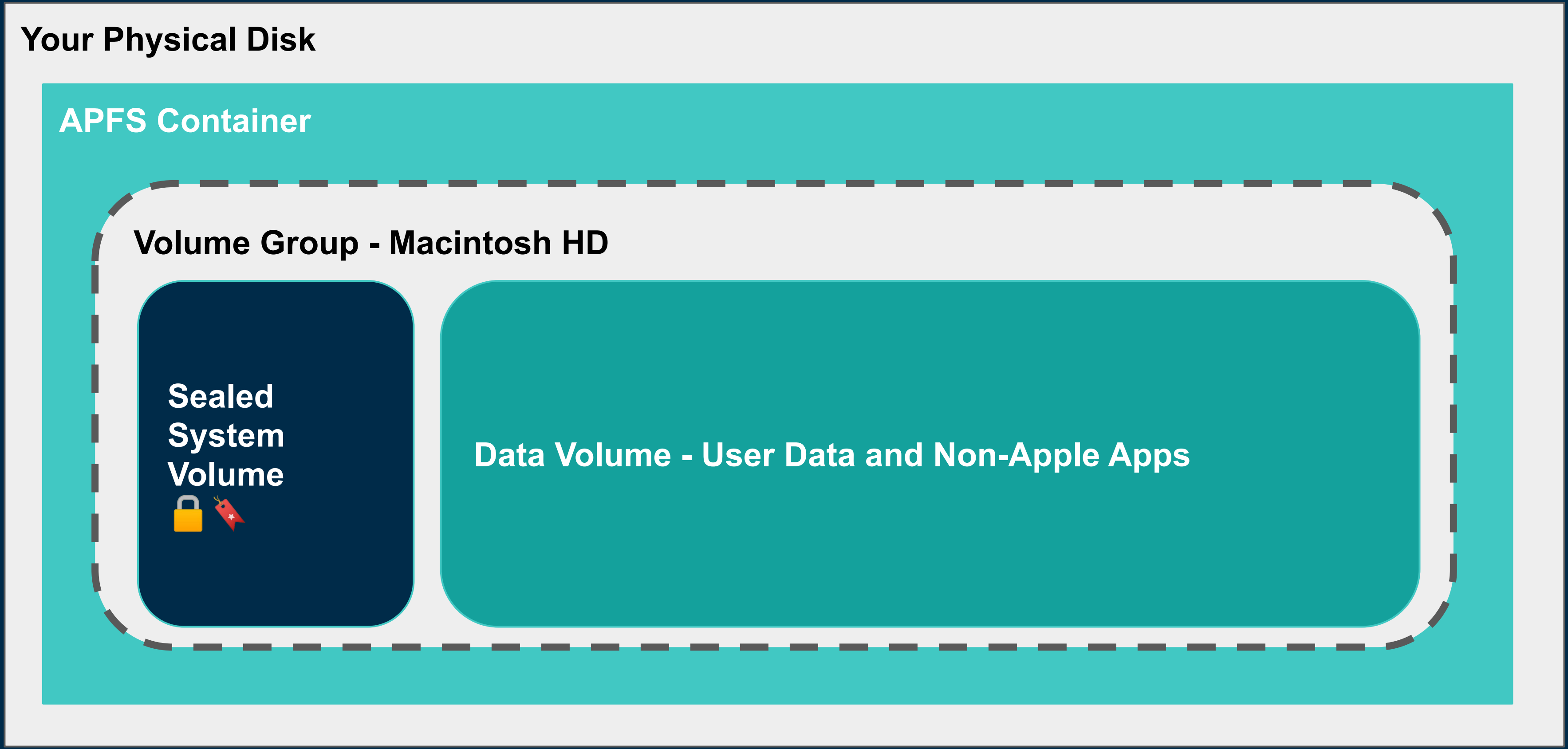
Data Volume - User Data and Non-Apple Apps

Wait, There’s More

Software Update is also about Hardware!

A Note on Erase All Contents & Settings

macOS 12's Single Best Feature



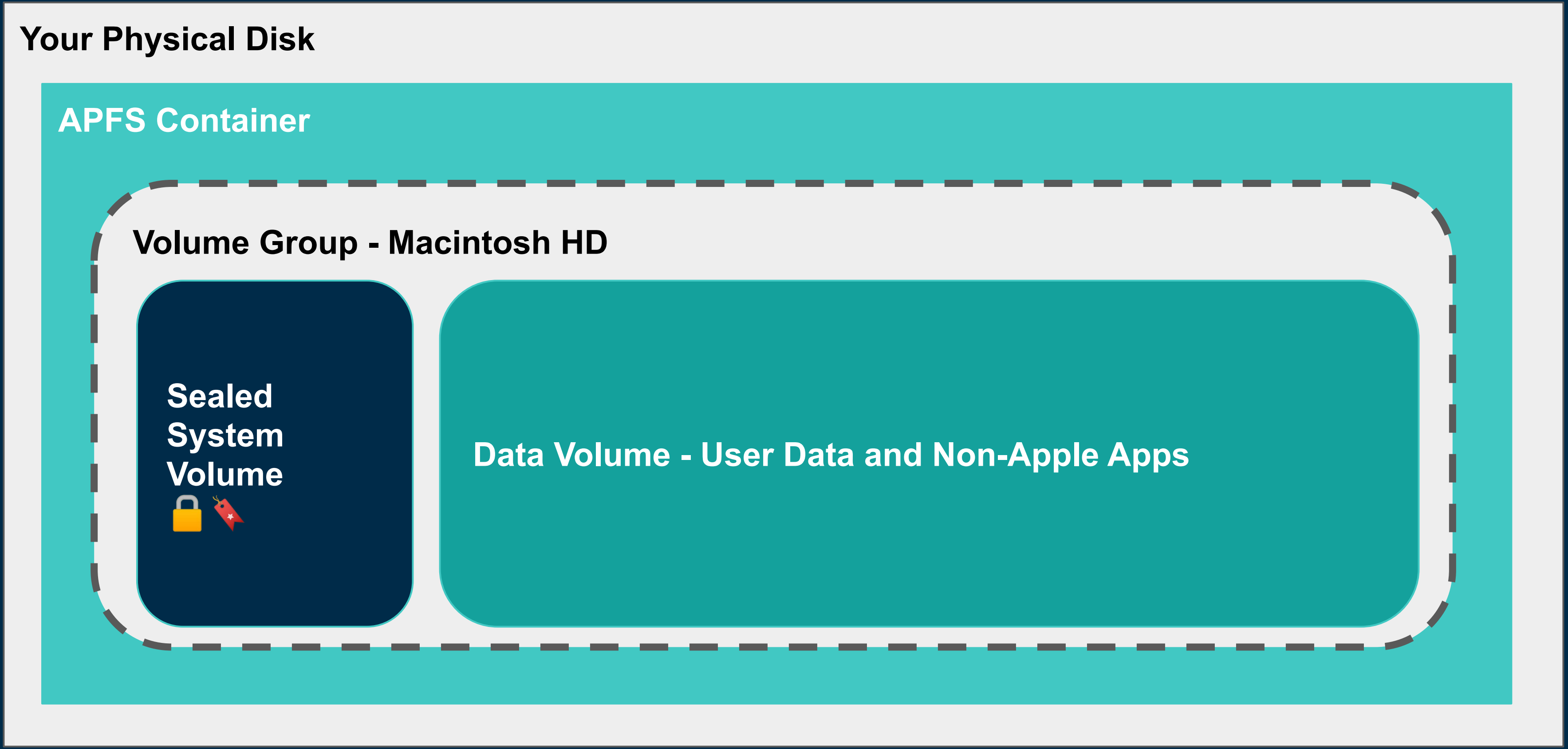
Your Physical Disk

APFS Container

Volume Group - Macintosh HD

Sealed System Volume 🔒 🔖

Data Volume - User Data and Non-Apple Apps



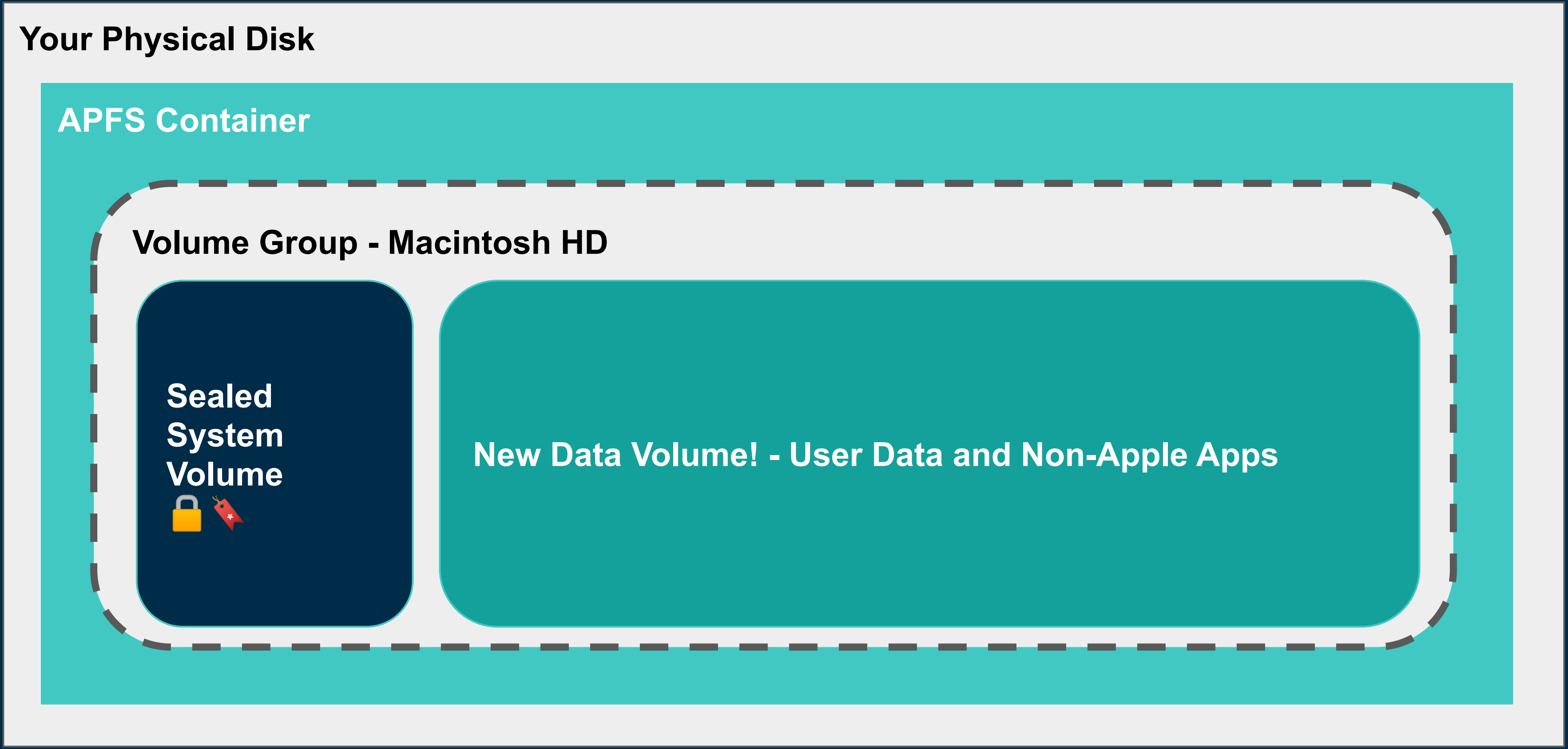
Your Physical Disk

APFS Container

Volume Group - Macintosh HD

Sealed System Volume 🔒 🔖

Data Volume - User Data and Non-Apple Apps



Your Physical Disk

APFS Container

Volume Group - Macintosh HD

Sealed System Volume 🔒 🔖

New Data Volume! - User Data and Non-Apple Apps

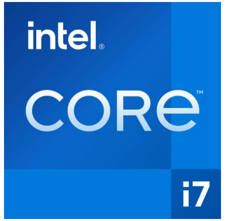
Booting macOS

Secure Boot is the underpinning of a secure update process

Intel Macs with T2 chips

T2 Boots First

- Validates the Boot ROM
- Validates Bootloader
- Validates Kernel Cache Signature on file
- Validates UEFI Signature on file
- Loads EFI



Intel Chip Boots Next

- Evaluates boot.efi
- Boot.efi reviews macOS Signature

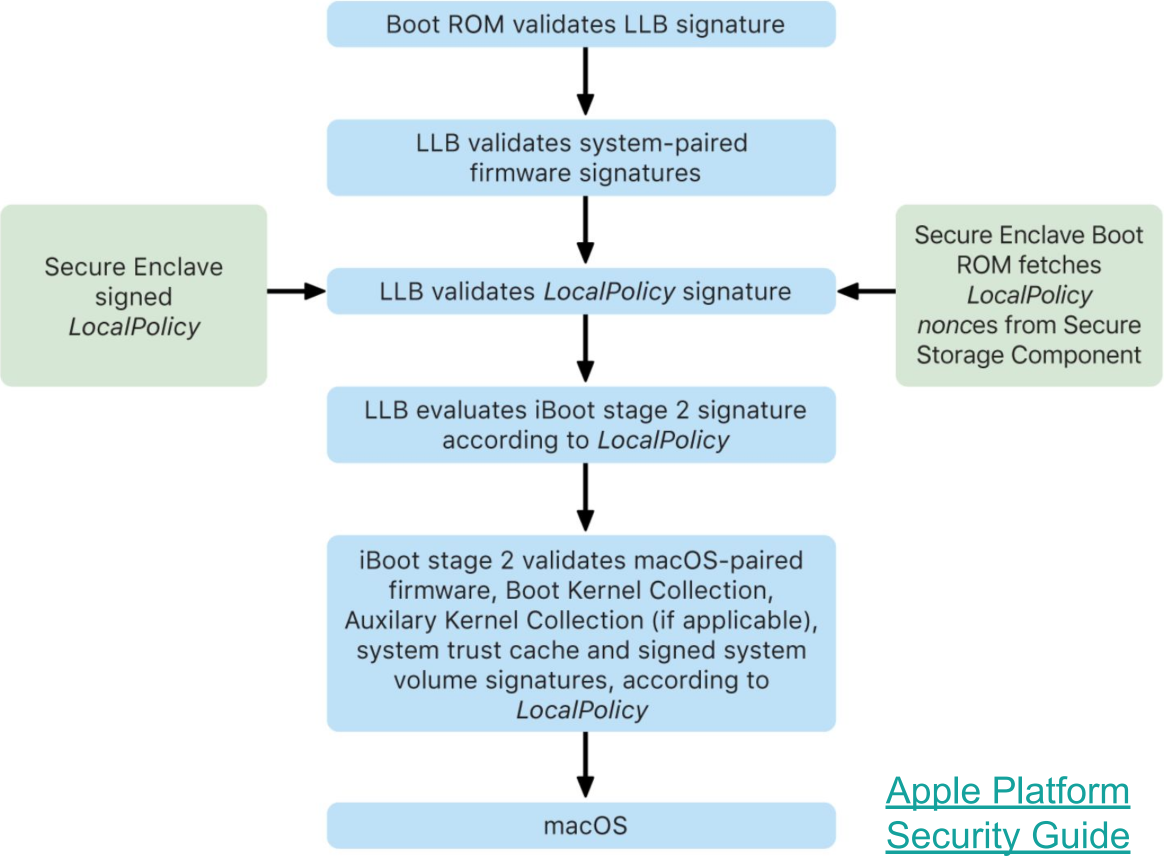
BridgeOS Upgrades on T2 chips

T2 Processors upgrade like other Apple Silicon platforms, through communication with Apple, but occasionally, problems occur with those updates.

Apple Configurator 2 is valuable for **reviving** these devices in the event that something goes wrong that is recoverable.

It can also be used to handle **restoring** things if you need to.

Macs with Apple silicon



Boot ROM validates LLB signature

LLB validates system-paired firmware signatures

Secure Enclave signed *LocalPolicy*

LLB validates *LocalPolicy* signature

Secure Enclave Boot ROM fetches *LocalPolicy nonces* from Secure Storage Component

LLB evaluates iBoot stage 2 signature according to *LocalPolicy*

iBoot stage 2 validates macOS-paired firmware, Boot Kernel Collection, Auxilary Kernel Collection (if applicable), system trust cache and signed system volume signatures, according to *LocalPolicy*

macOS

Apple Platform Security Guide

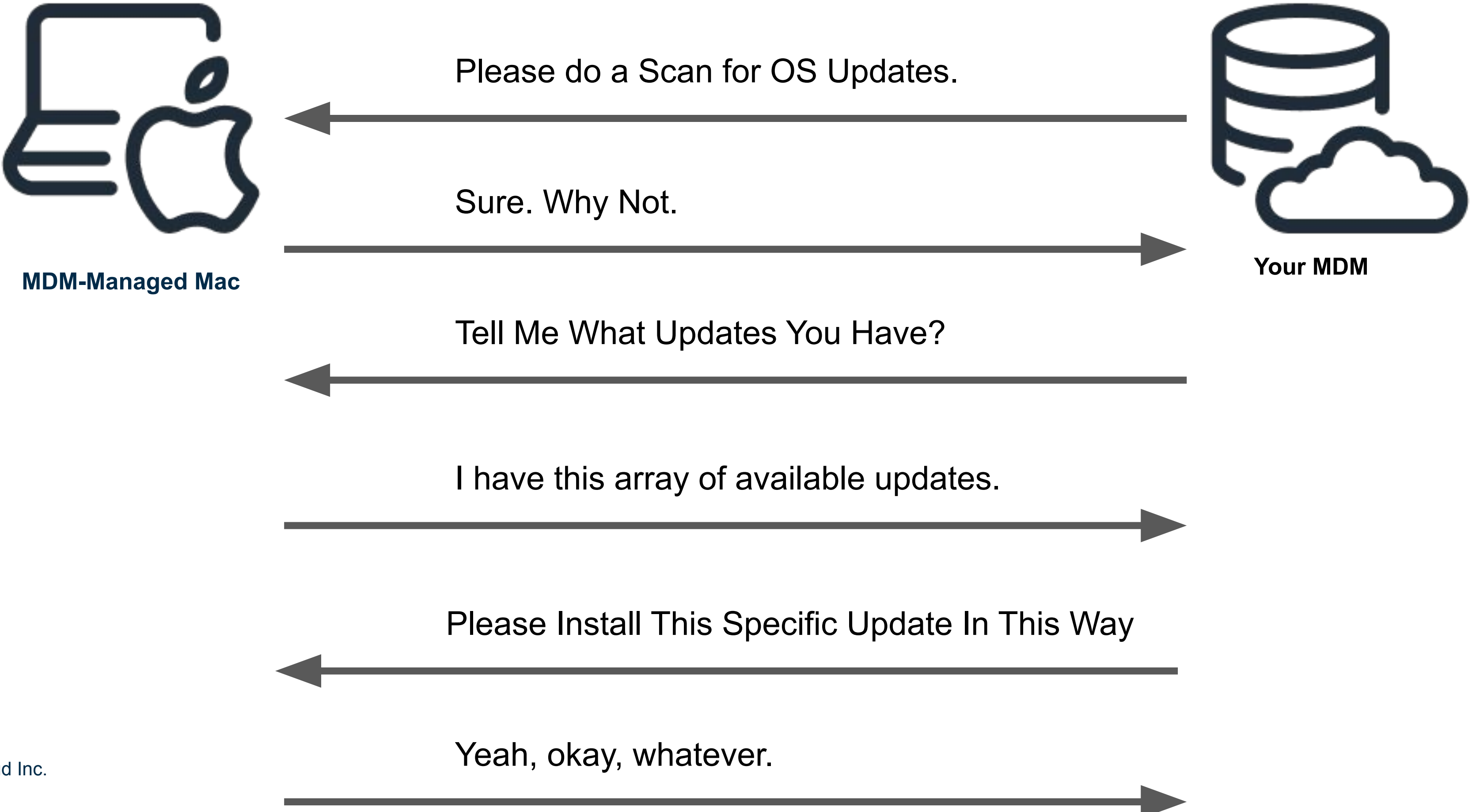
Managing Software Versions

And other lies we tell ourselves

Requirements for Software Update

- You need an MDM to do anything interesting.
- You probably need more than just an MDM.
- Beginning with macOS 14 Sonoma,
  DDM is very helpful

How Do MDM Updates Work?



MDM-Managed Mac

Your MDM

Please do a Scan for OS Updates.

Sure. Why Not.

Tell Me What Updates You Have?

I have this array of available updates.

Please Install This Specific Update In This Way

Yeah, okay, whatever.

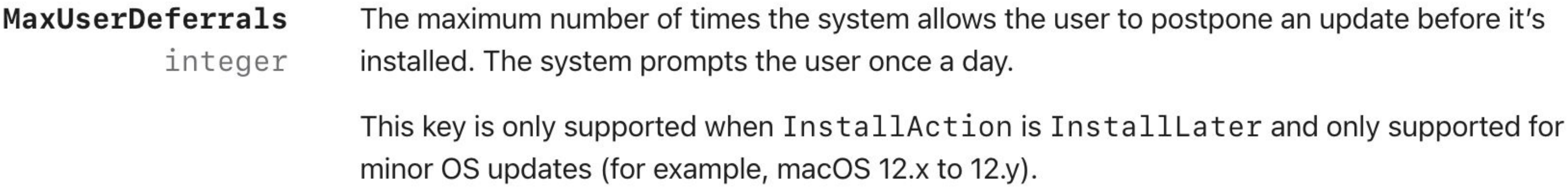
What About iOS?

User Enrolled Device	❌
Manually Enrolled Device	❌
Supervised Devices	✅

	Major	Minor
Default	✅	✅
DownloadOnly	✅	✅
InstallASAP	✅	✅
NotifyOnly	✅	✅
InstallLater	❌	✅
InstallForceRestart	✅	✅

Deferrals

Introduced in macOS 12, Deferrals are meant to help admins deploy software updates without direct user involvement.



`MaxUserDeferrals`
`integer`

The maximum number of times the system allows the user to postpone an update before it's installed. The system prompts the user once a day.

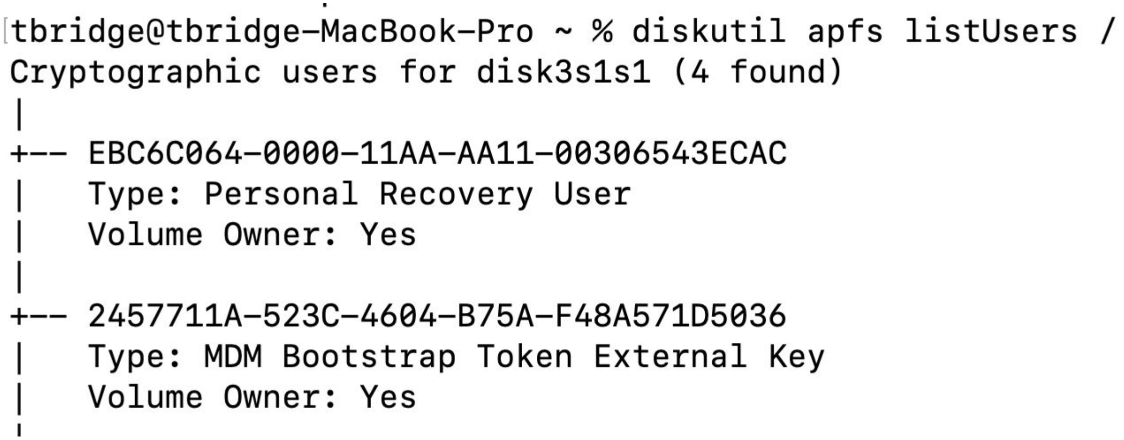
This key is only supported when `InstallAction` is `InstallLater` and only supported for minor OS updates (for example, macOS 12.x to 12.y).

`InstallLater` updates happen during system quiet period, which is traditionally 1-5am local time, but is actually influenced by the end user's activity. Generally requires power or a full battery (50%+)

Bootstrap Tokens

🥾🪙

- Gathered by your MDM via Command
- Can Unlock the System Volume



```
[tbridge@tbridge-MacBook-Pro ~ % diskutil apfs listUsers /
Cryptographic users for disk3s1s1 (4 found)
|
+-- EBC6C064-0000-11AA-AA11-00306543ECAC
|   Type: Personal Recovery User
|   Volume Owner: Yes
|
+-- 2457711A-523C-4604-B75A-F48A571D5036
|   Type: MDM Bootstrap Token External Key
|   Volume Owner: Yes
|
```

- Used by **`InstallLater`** to unlock the system volume during the quiet period.

Rapid Security Response

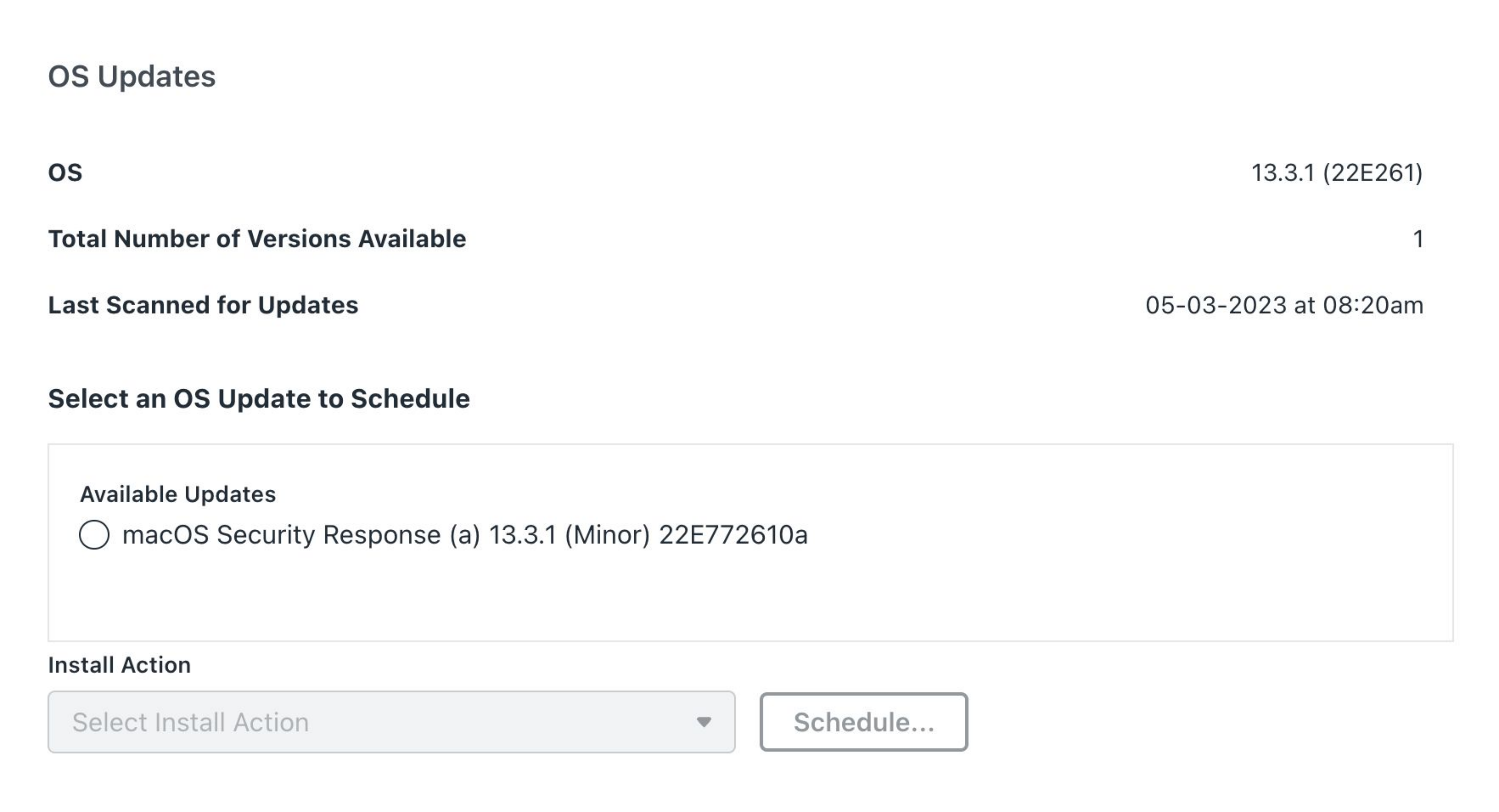
When is an update NOT an update?

What is an RSR update?

- Added to macOS with macOS 13 Ventura
- First update on 1 May 2023
- Updates are styled as 13.3.1 (a) (b) or (n)
- RSR Updates can be removed, by the user
- RSR Update install and removal can be controlled by the admin with an MDM Profile
- JumpCloud Supports Managing RSR Updates with a profile

What is an RSR update?

- Contain special updates for Safari or other Apple apps on iOS or macOS
- Require a reboot to become fully functional
- These updates are very, very fast to install, unlike current updates.
- Based on Cryptex



OS Updates

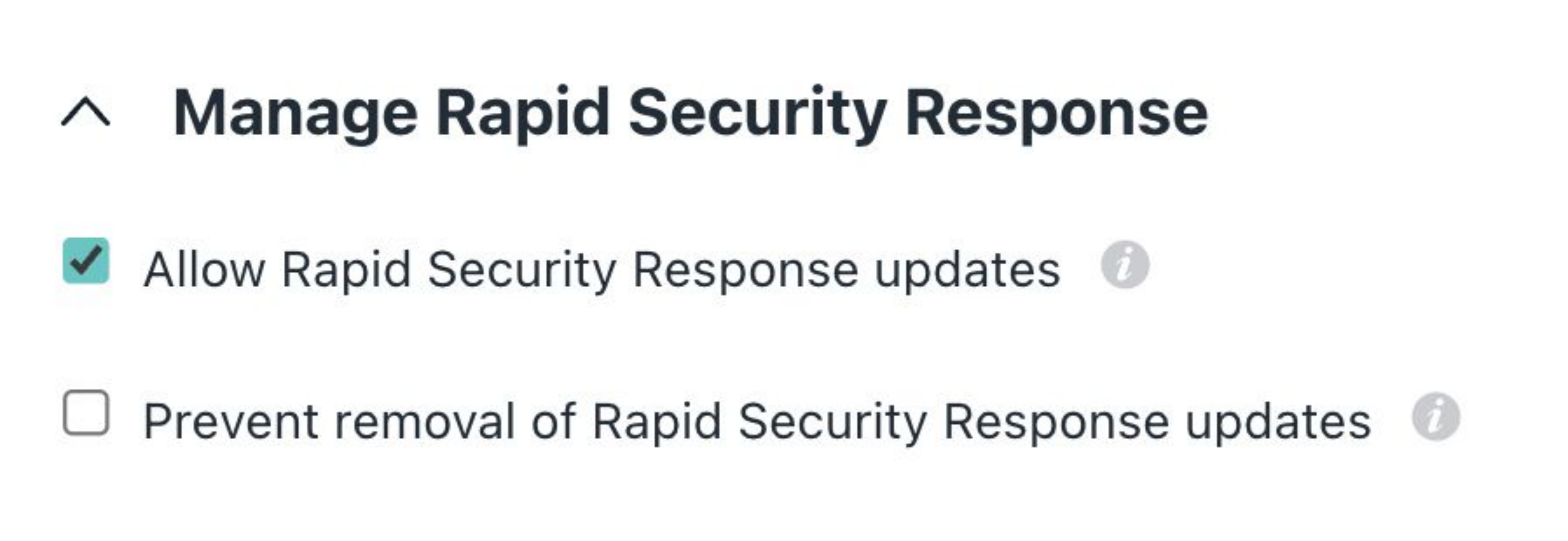
OS	13.3.1 (22E261)
Total Number of Versions Available	1
Last Scanned for Updates	05-03-2023 at 08:20am

Select an OS Update to Schedule

Available Updates

○ macOS Security Response (a) 13.3.1 (Minor) 22E772610a

Install Action



Manage Rapid Security Response

☑ Allow Rapid Security Response updates

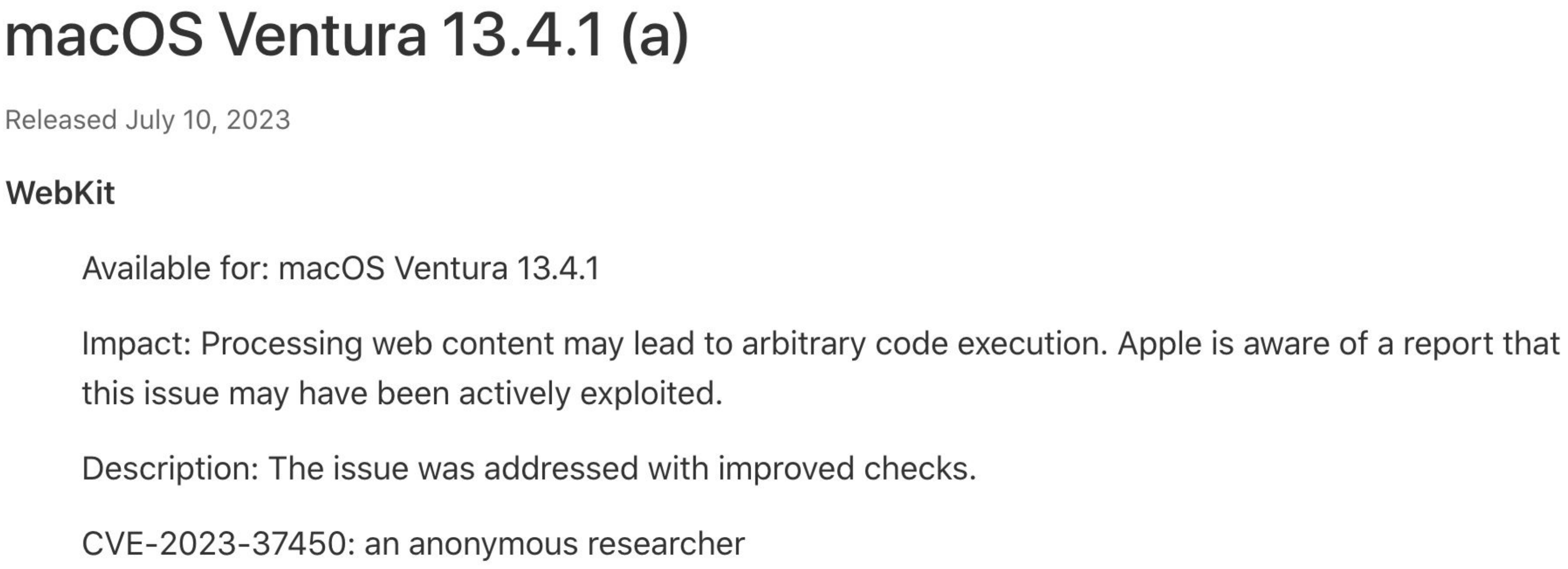
□ Prevent removal of Rapid Security Response updates

How Should I Think About Rapid Security Response?

These ephemeral updates are for patching the worst flaws.

What is an RSR update?

- **Limited Utility**, but when you need it, you need it.
- **Limited Lifespan**, all updates rolled into the next minor release.
- **Limited Testing**, RSR updates don’t go through the same flow as point release updates.
- **Limited Application**, only applies to non-kernelspace changes



macOS Ventura 13.4.1 (a)

Released July 10, 2023

WebKit

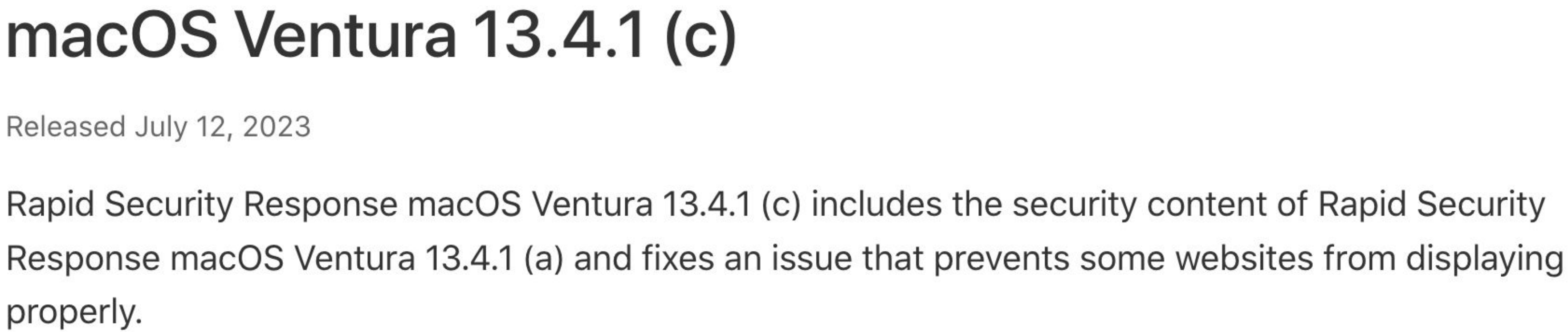
Available for: macOS Ventura 13.4.1

Impact: Processing web content may lead to arbitrary code execution. Apple is aware of a report that this issue may have been actively exploited.

Description: The issue was addressed with improved checks.

CVE-2023-37450: an anonymous researcher

About the security content of Rapid Security Responses for macOS Ventura 13.4.1



macOS Ventura 13.4.1 (c)

Released July 12, 2023

Rapid Security Response macOS Ventura 13.4.1 (c) includes the security content of Rapid Security Response macOS Ventura 13.4.1 (a) and fixes an issue that prevents some websites from displaying properly.

About the security content of Rapid Security Responses for macOS Ventura 13.4.1

A Wish List for Software Update Commands

Wish List Items

- Deadlines for install based on Apple release dates.
- Close deferral escape paths.
- Update alerts triggered by MDM should be customizable in time and persistence.
- Install Later should apply to Major Upgrades.
- Takeover the job of Nudge or Super.
- Spot problems that might result in Recovery Mode during the preflight and act appropriately.

WWDC23
Overview
Topics
Sessions
Labs
Activities
Forums
Beyond WWDC

What Changed in Software Update?

“Software Update takes advantage of declarative device management and now allows IT administrators to enforce software updates to specific deadlines with improved user transparency.”

– What’s New in Managing Apple Devices, 2023

How Does DDM Enforcement Work?

Declarative Device Management - Software Update Configurations

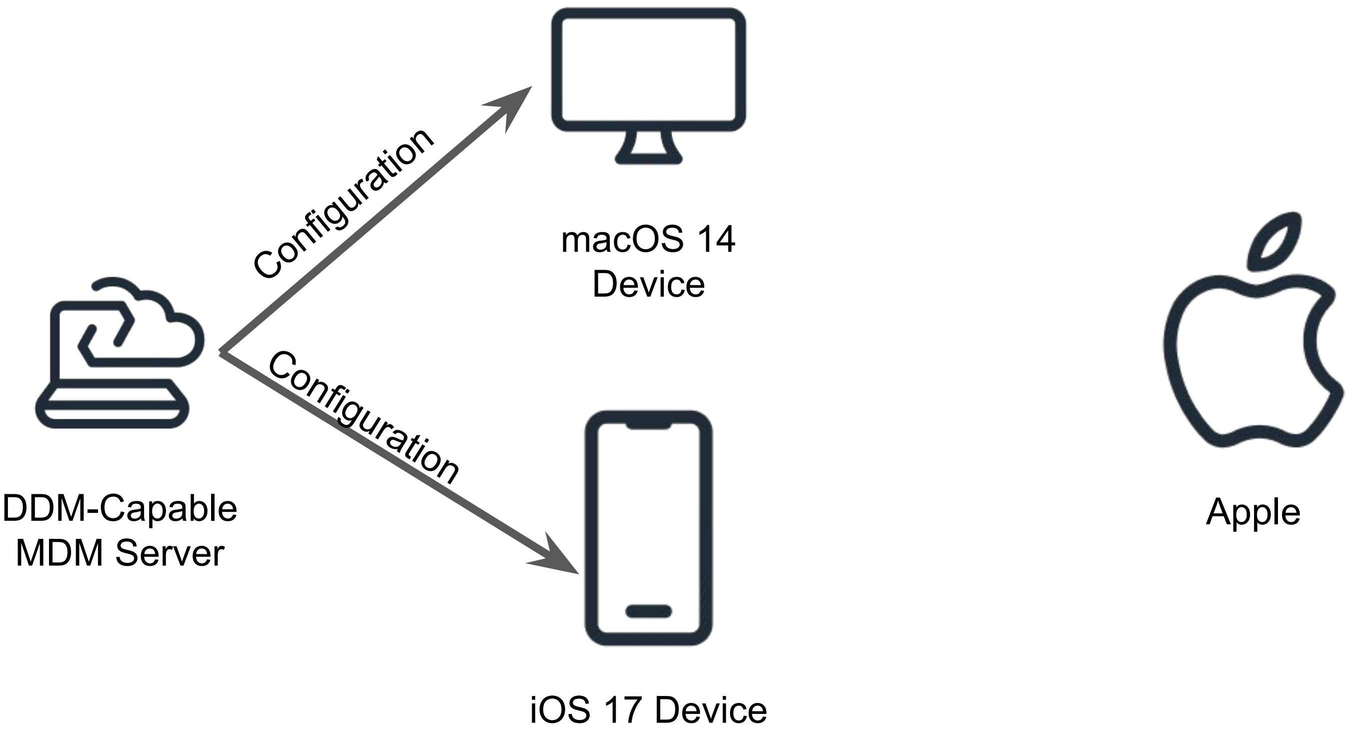
macOS 14
Device

DDM-Capable
MDM Server

Apple

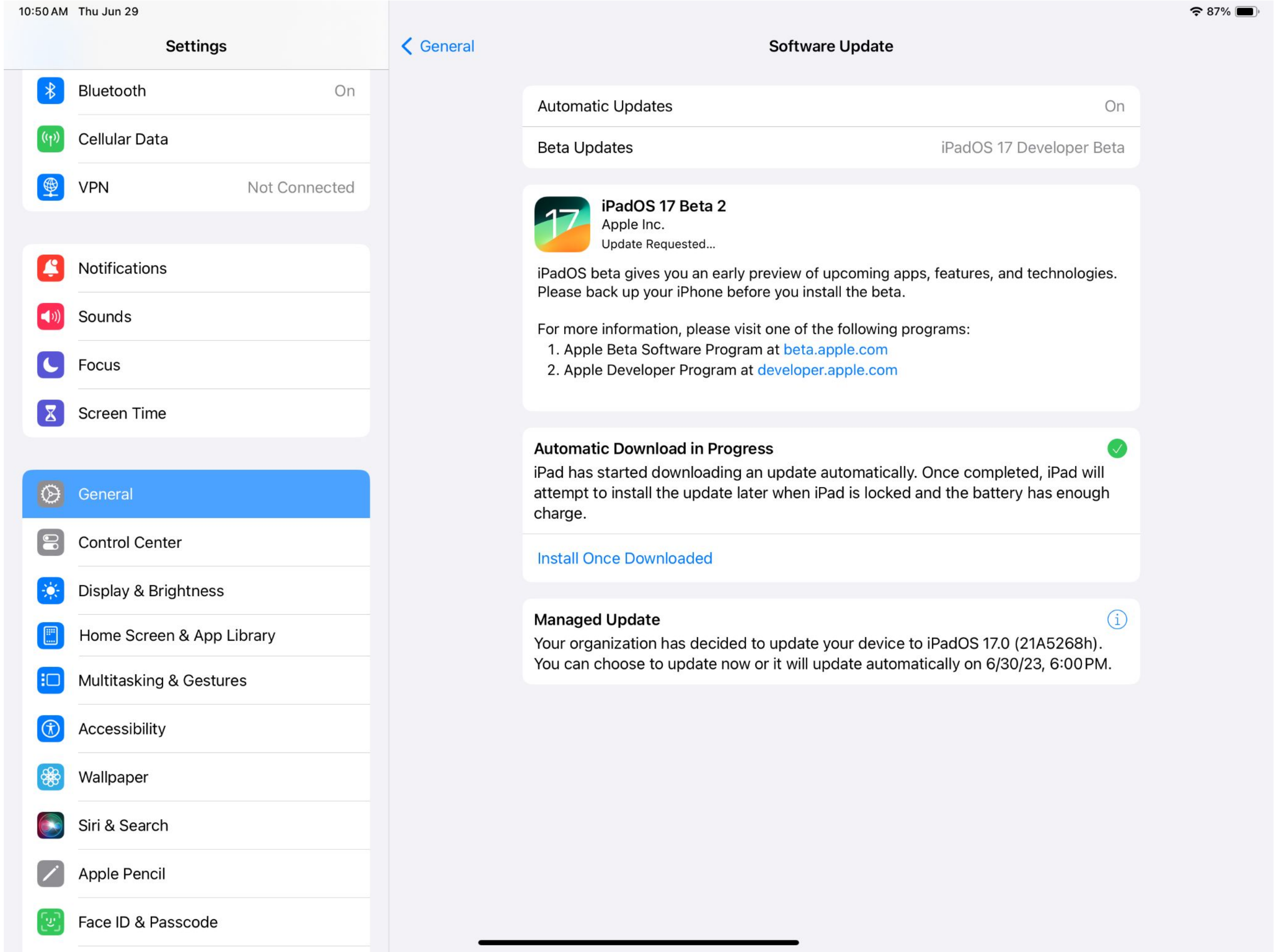
iOS 17 Device

Declarative Device Management - Software Update Configurations



Declarative Device Management - Software Update Configurations

```
{
   "Type":
"com.apple.configuration.softwareupdate.enforcement.specific",
   "Identifier": "tom.ios.enforcement",
   "Payload": {
      "DetailsURL": "https://youtube.com/watch?v=sVdaFQhS86E",
         "TargetLocalDateTime": "2023-06-30T18:00:00",
         "TargetOSVersion": "17.0",
         "TargetBuildVersion": "21A5268h"
   }
 }
```



Software Update

Automatic Updates On

Beta Updates iPadOS 17 Developer Beta

iPadOS 17 Beta 2
Apple Inc.
Update Requested...

iPadOS beta gives you an early preview of upcoming apps, features, and technologies. Please back up your iPhone before you install the beta.

For more information, please visit one of the following programs:

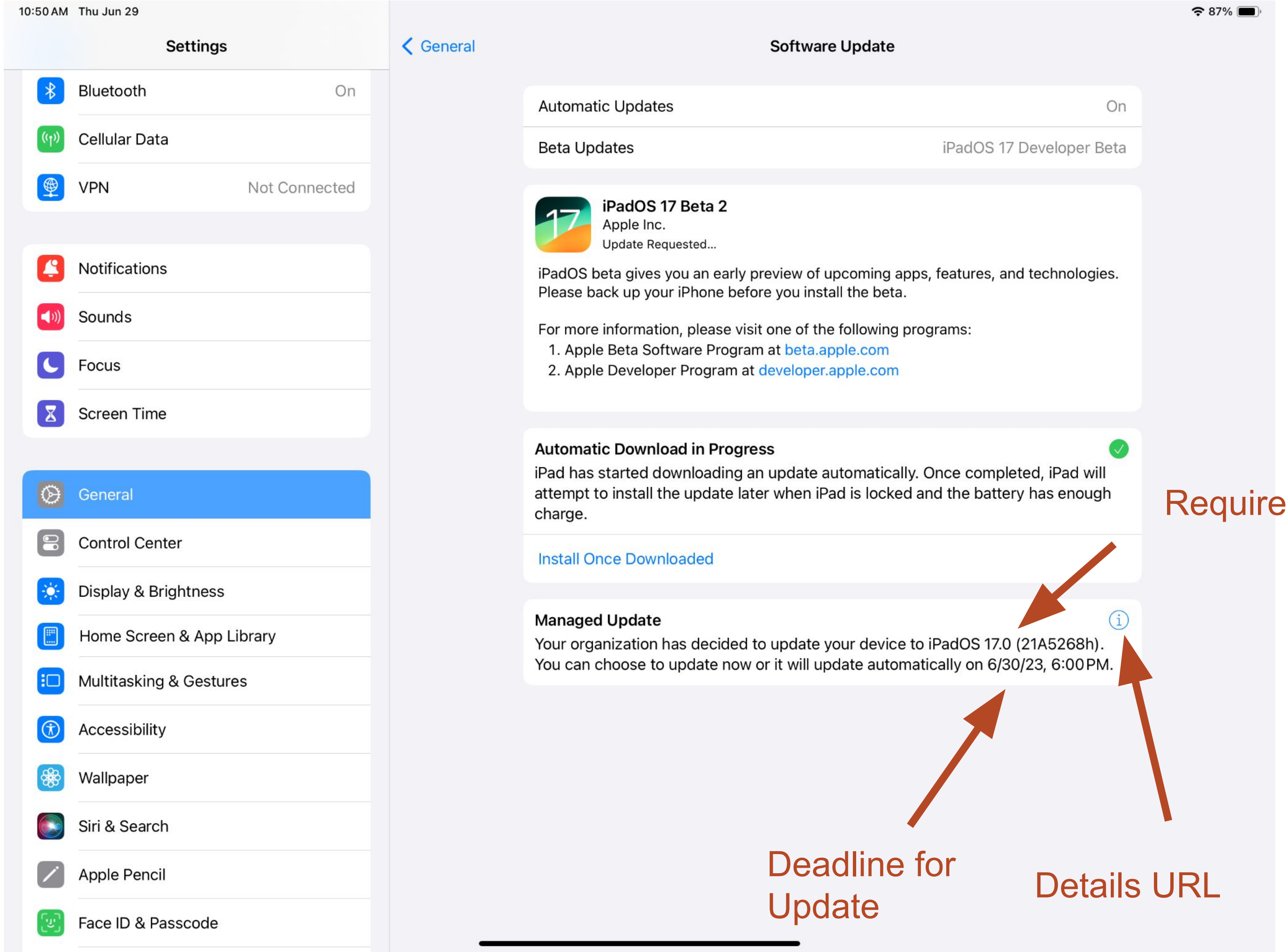
1. Apple Beta Software Program at beta.apple.com
2. Apple Developer Program at developer.apple.com

Automatic Download in Progress ✓

iPad has started downloading an update automatically. Once completed, iPad will attempt to install the update later when iPad is locked and the battery has enough charge.

Managed Update

Your organization has decided to update your device to iPadOS 17.0 (21A5268h). You can choose to update now or it will update automatically on 6/30/23, 6:00PM.



10:50 AM Thu Jun 29

87%

Settings

- Bluetooth On
- Cellular Data
- VPN Not Connected
- Notifications
- Sounds
- Focus
- Screen Time
- General
- Control Center
- Display & Brightness
- Home Screen & App Library
- Multitasking & Gestures
- Accessibility
- Wallpaper
- Siri & Search
- Apple Pencil
- Face ID & Passcode

< General

Software Update

Automatic Updates On

Beta Updates iPadOS 17 Developer Beta

iPadOS 17 Beta 2
Apple Inc.
Update Requested...

iPadOS beta gives you an early preview of upcoming apps, features, and technologies. Please back up your iPhone before you install the beta.

For more information, please visit one of the following programs:

1. Apple Beta Software Program at beta.apple.com
2. Apple Developer Program at developer.apple.com

Automatic Download in Progress

iPad has started downloading an update automatically. Once completed, iPad will attempt to install the update later when iPad is locked and the battery has enough charge.

Install Once Downloaded

Managed Update

Your organization has decided to update your device to iPadOS 17.0 (21A5268h). You can choose to update now or it will update automatically on 6/30/23, 6:00 PM.

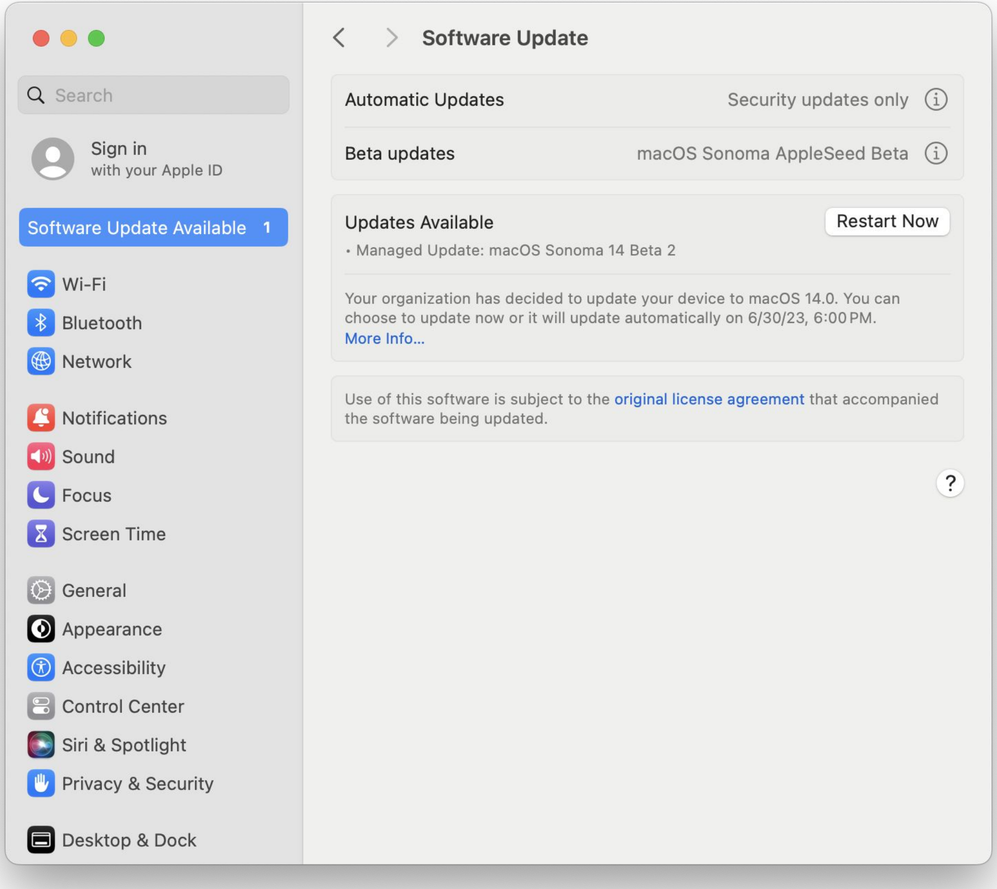
Required Version Info

Deadline for Update

Details URL

Declarative Device Management - Software Update Configurations

```
{
   "Type":
"com.apple.configuration.softwareupdate.enforcement.specific",
   "Identifier": "tom.beta.enforcement",
   "Payload": {
      "DetailsURL": "https://youtu.be/5IsSpAOD6K8?t=29",
         "TargetLocalDateTime": "2023-06-30T18:00:00",
         "TargetOSVersion": "14.0",
         "TargetBuildVersion": "23A5276g"
   }
 }
```



Software Update

Automatic Updates: Security updates only

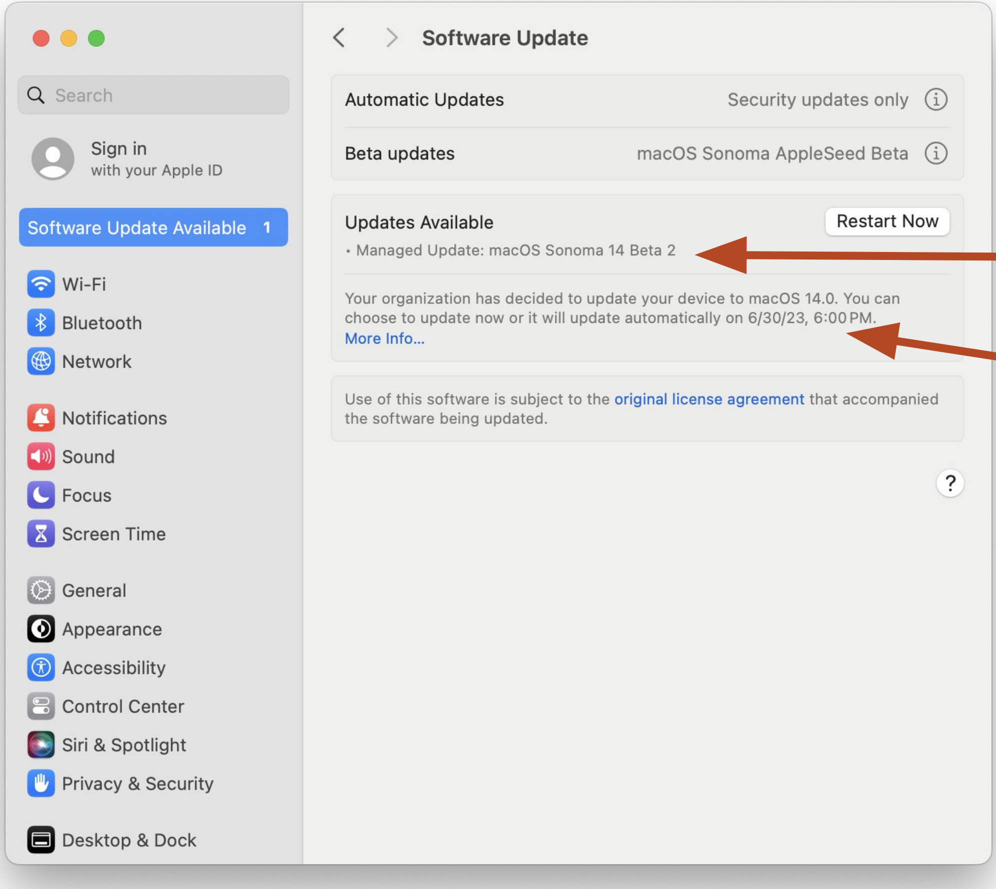
Beta updates: macOS Sonoma AppleSeed Beta

Updates Available

- Managed Update: macOS Sonoma 14 Beta 2

Your organization has decided to update your device to macOS 14.0. You can choose to update now or it will update automatically on 6/30/23, 6:00 PM.
More Info...

Use of this software is subject to the original license agreement that accompanied the software being updated.



Software Update

Automatic Updates: Security updates only

Beta updates: macOS Sonoma AppleSeed Beta

Updates Available

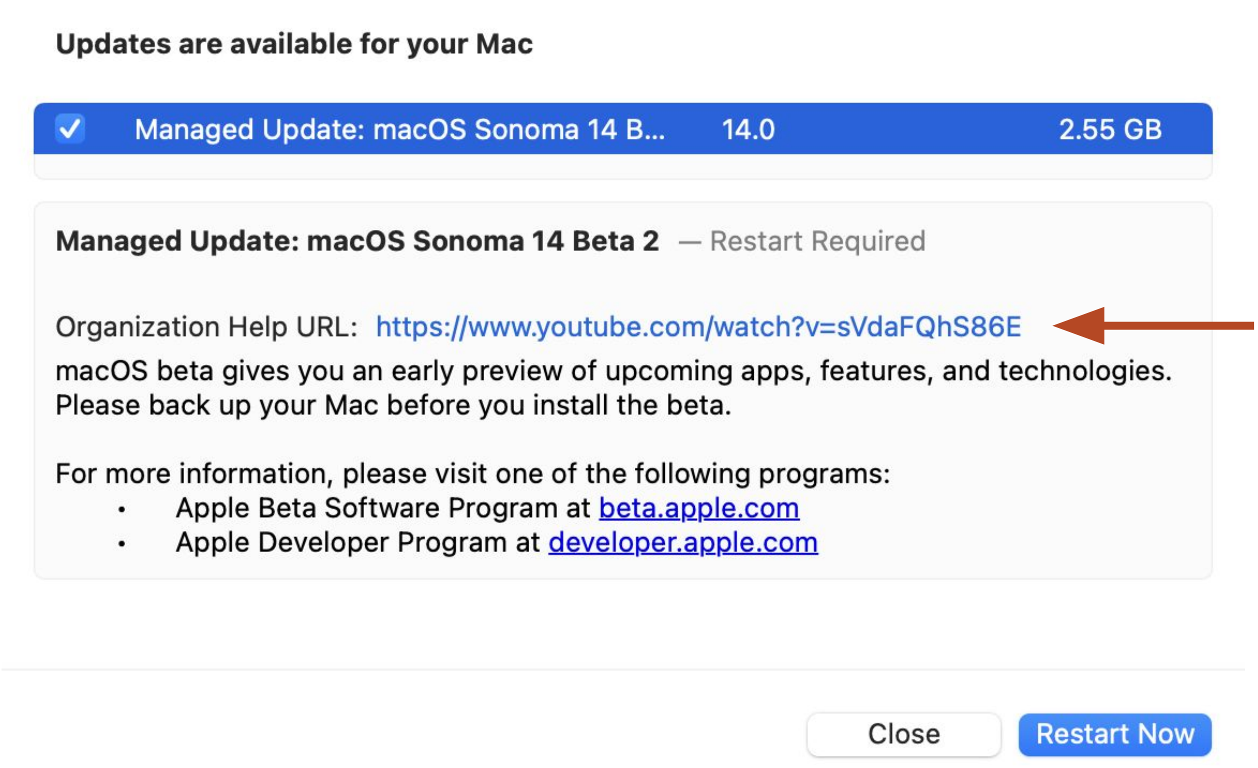
- Managed Update: macOS Sonoma 14 Beta 2

Your organization has decided to update your device to macOS 14.0. You can choose to update now or it will update automatically on 6/30/23, 6:00 PM.
More Info...

Use of this software is subject to the original license agreement that accompanied the software being updated.

Required Version Info

Deadline



Updates are available for your Mac

☑ Managed Update: macOS Sonoma 14 B... 14.0 2.55 GB

Managed Update: macOS Sonoma 14 Beta 2 — Restart Required

Organization Help URL: https://www.youtube.com/watch?v=sVdaFQhS86E

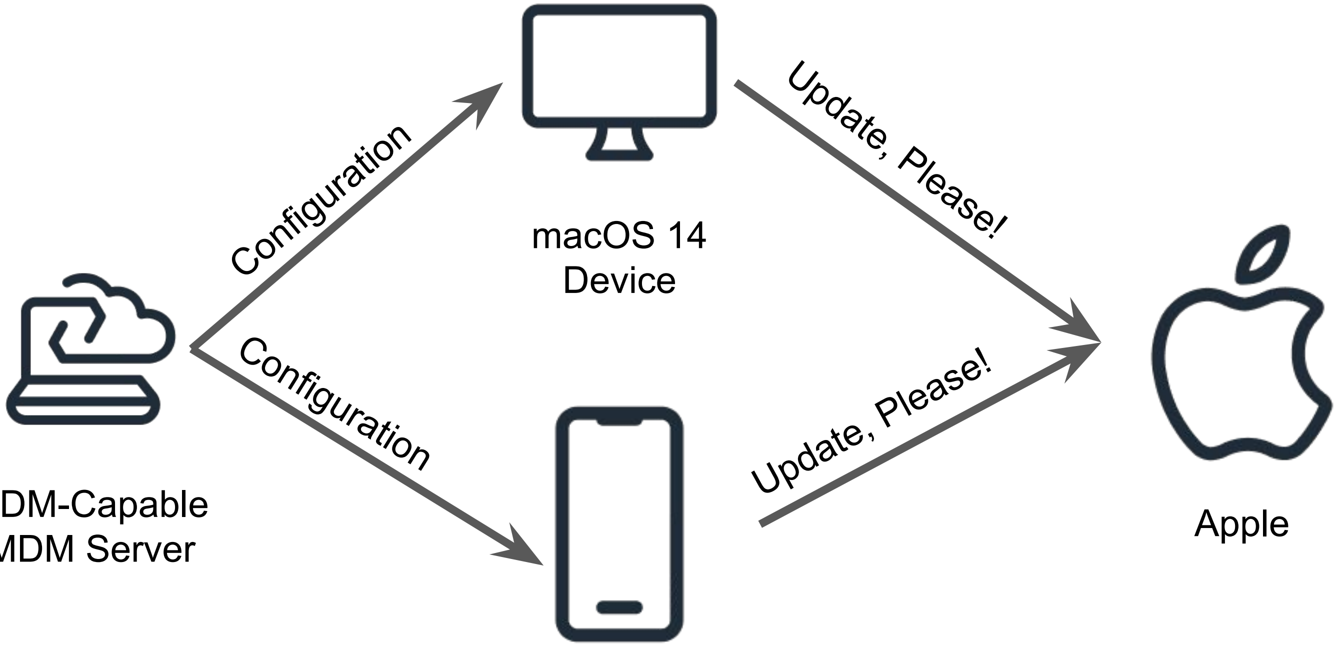
macOS beta gives you an early preview of upcoming apps, features, and technologies. Please back up your Mac before you install the beta.

For more information, please visit one of the following programs:

- Apple Beta Software Program at beta.apple.com
- Apple Developer Program at developer.apple.com

Details URL

Declarative Device Management - Software Update Configurations



DDM-Capable MDM Server

Configuration

Configuration

macOS 14 Device

iOS 17 Device

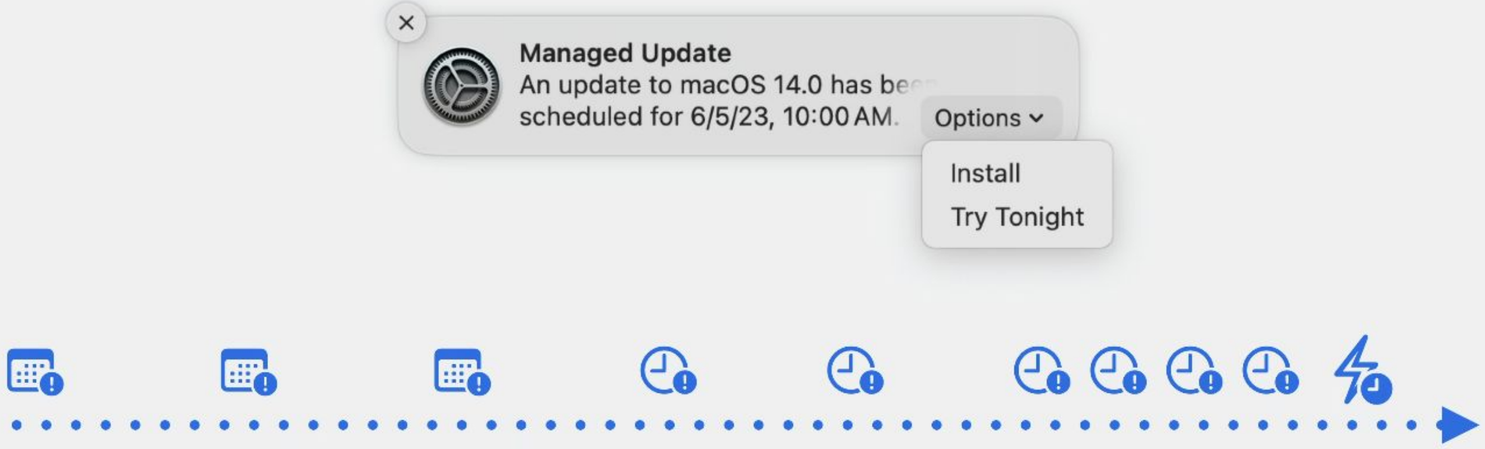
Update, Please!

Update, Please!

Apple

So What Happens When You Ignore The Alerts?

Update available notification



Managed Update

An update to macOS 14.0 has bee
scheduled for 6/5/23, 10:00 AM.

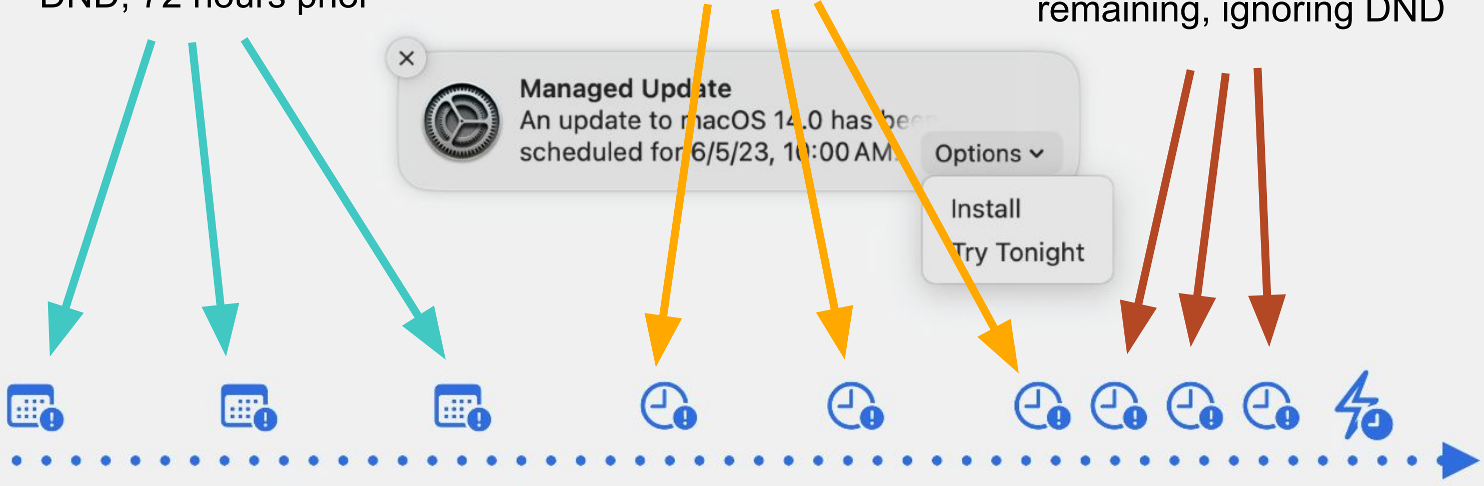
Image from Apple

Update available notification

Daily Alerts, ignoring DND, 72 hours prior

Hourly Alerts, ignoring DND, at 24 hours prior

30-, 20-, and 10-minutes remaining, ignoring DND

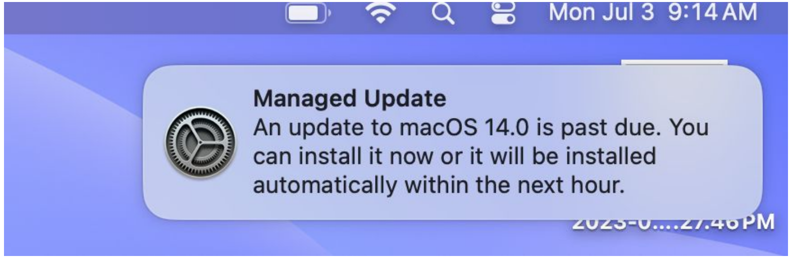


Managed Update

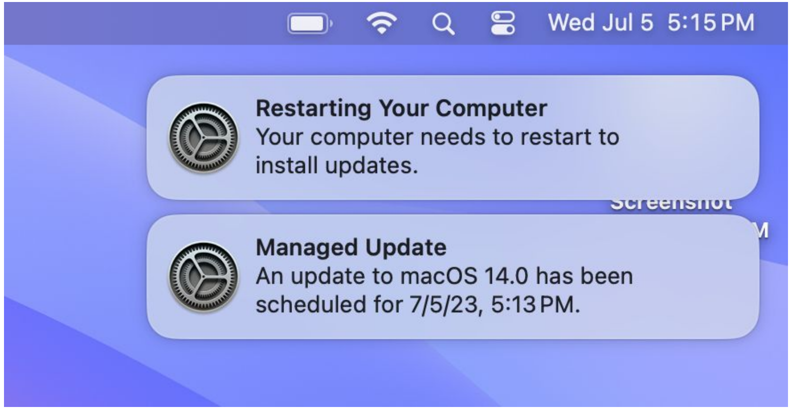
An update to macOS 14.0 has bee
scheduled for 6/5/23, 10:00 AM.

Image from Apple

So What Happens When You Ignore The Deadline?

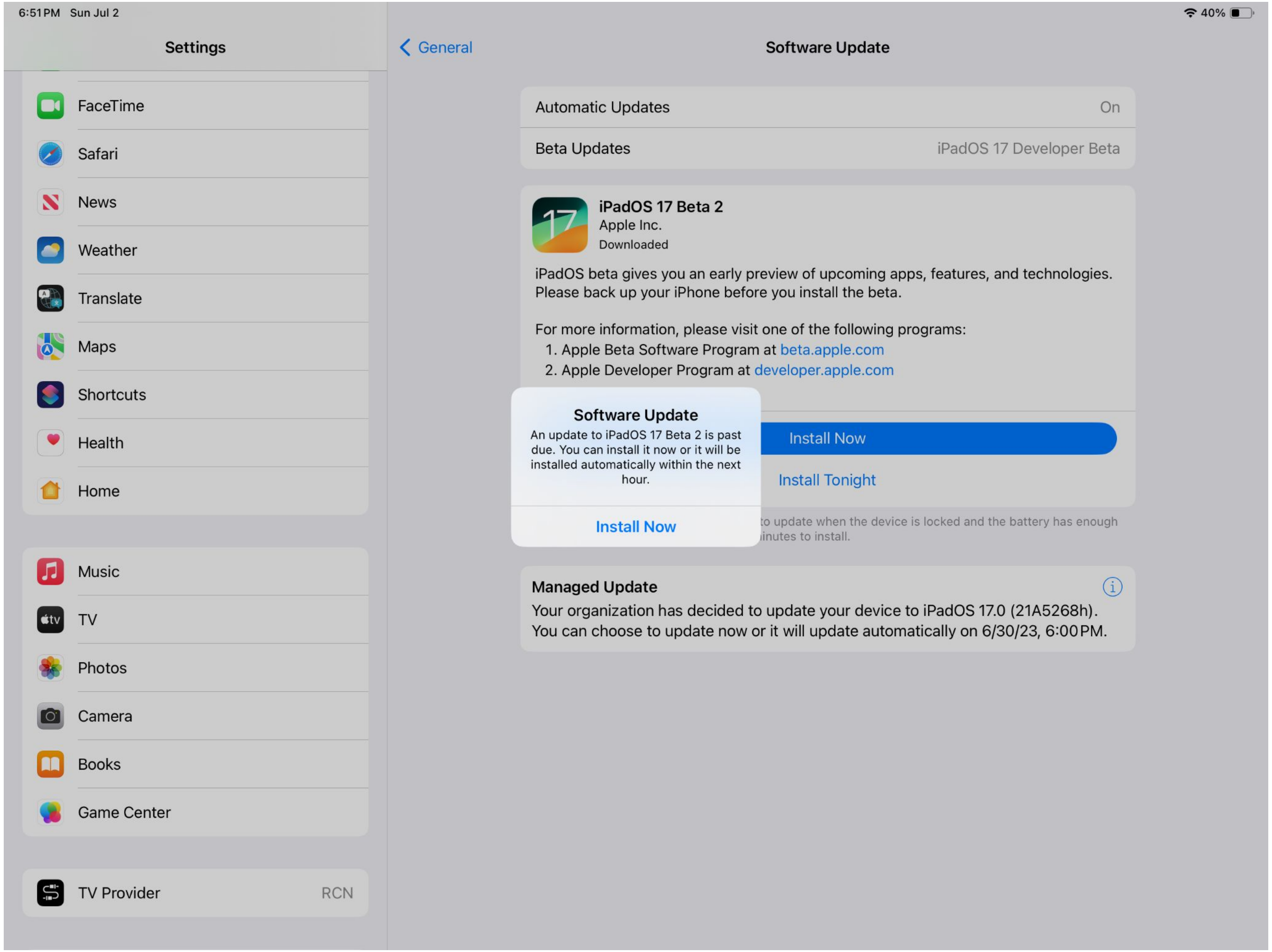


Managed Update
An update to macOS 14.0 is past due. You can install it now or it will be installed automatically within the next hour.



Restarting Your Computer
Your computer needs to restart to install updates.

Managed Update
An update to macOS 14.0 has been scheduled for 7/5/23, 5:13 PM.



Software Update

Automatic Updates On

Beta Updates iPadOS 17 Developer Beta

iPadOS 17 Beta 2
Apple Inc.
Downloaded

iPadOS beta gives you an early preview of upcoming apps, features, and technologies. Please back up your iPhone before you install the beta.

For more information, please visit one of the following programs:

1. Apple Beta Software Program at beta.apple.com
2. Apple Developer Program at developer.apple.com

Software Update

An update to iPadOS 17 Beta 2 is past due. You can install it now or it will be installed automatically within the next hour.

Install Now

to update when the device is locked and the battery has enough inutes to install.

Managed Update

Your organization has decided to update your device to iPadOS 17.0 (21A5268h). You can choose to update now or it will update automatically on 6/30/23, 6:00 PM.

But What If My User Was on Vacation? What Then?

Other details for using Software Deadlines

- Must be using a DDM-capable management solution
- Must have a Bootstrap Token
- Multiple versions can be specified in a Configuration, each with their own deadline
- A very large number are supported

Wish List Items

- ~~Deadlines for install based on Apple release dates.~~
- ~~Close deferral escape paths.~~
- Update alerts triggered by MDM should be customizable in time and persistence.
- Install Later should apply to Major Upgrades.
- ~~Takeover the job of Nudge or Super.~~
- Spot problems that might result in Recovery Mode during the preflight and act appropriately.

Coping Mechanisms

Mac Admins Community to the Rescue!

Nudge

Nudge

- LaunchDaemon + Configuration/JSON
- Drives user to apply their own updates
- Can takeover the screen, be customized easily
- Supported by a Jamf Schema
- Used by JumpCloud MDM as part of Patch Management
- Great Community Support in #nudge

Super

Super

- Scripts + IBM Notifier
- API Access for Jamf Pro required today
- Other MDMs may be supported in the future
- Combines notifications with API Commands for **`ScheduleOSUpdate`**

softwareupdate CLI

CLI Tools

- Basically, Don’t Do This.

CLI Tools

But if you have to, there’s stuff you need to know:

- As of macOS 13, it’s not a good idea to use the **`sudo launchctl kickstart -k system/com.apple.softwareupdated`** construct as an automated, repeated action.
- Authenticated Restarts will required a volume owner’s credentials.

Feedback as an Art

Tom's Rules for Great Feedback

1. Start from what you expected
2. Then explained what happened instead
3. Describe time & effort savings desired
4. Provide examples and code
5. Center yourself with context
6. Clarity is the true soul of wit

Suggested Topic Areas

1. MDM Commands Not Being Reliable
2. MDM Command Escapes Are Too Easy
3. `InstallLater` doesn't work with Majors
4. `InstallLater` with Deferrals are too unpredictable

jumpcloud™