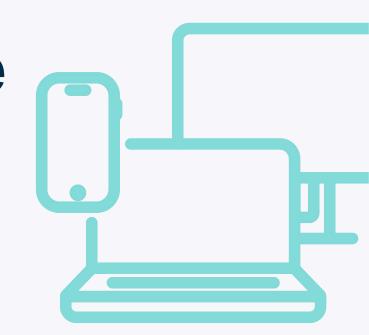
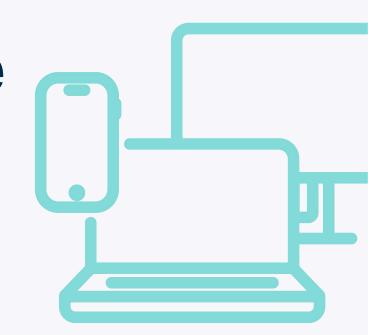


## **The Missing Manual**



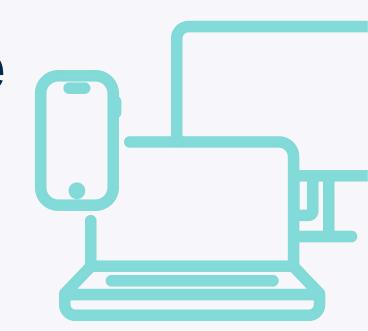


discoveryd (2): Electric Bugaloo



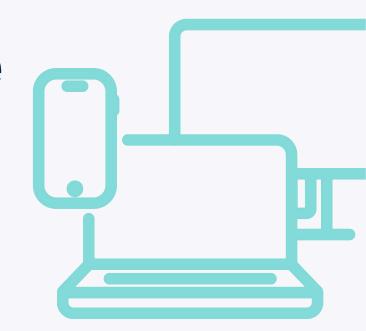


### **Threat Or Menace?**





Where We're Going, Where We've Been





# 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

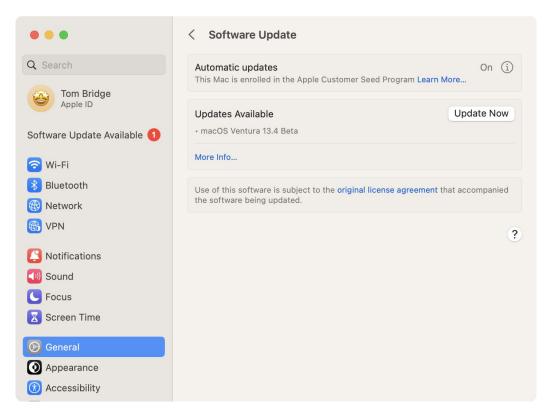
**Upgrade:** A major release of macOS - From 12.x to 13.x

**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. Requires disk ownership to use.

**Universal Mac Assistant (UMA):** An app-driven update to the operating system. Available via CLI, App Store, Mist and other tools. Requires admin rights to use.



### **The Update Process - System Settings**





### The Update Process - Via MDM

**OS Updates** OS 13.0.1 (22A400) **Total Number of Versions Available 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 Schedule...

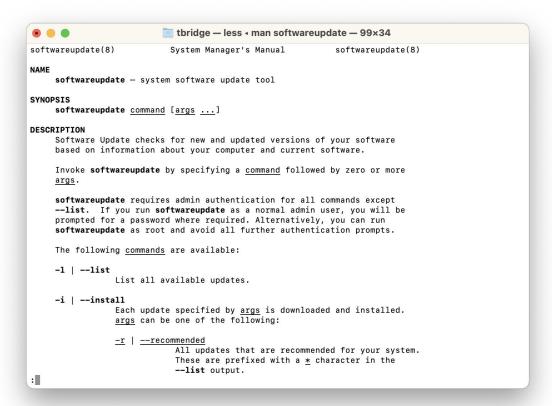


### The Update Process - Via Terminal

```
tbridge — -zsh — 61×24
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**



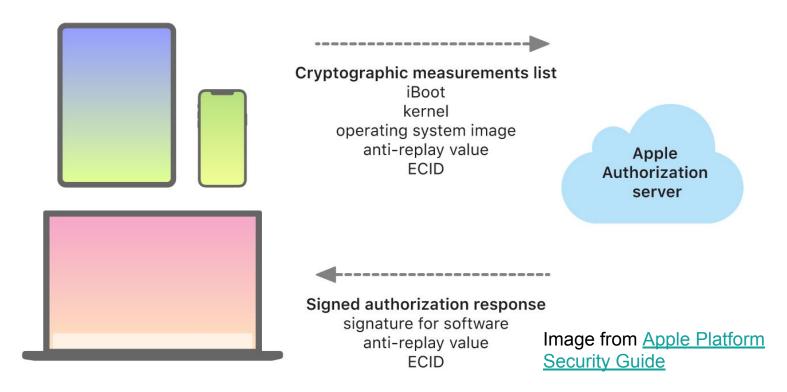


## So you have the bits...

Now what?



### **The Update Process - Personalization**





### **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



- 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

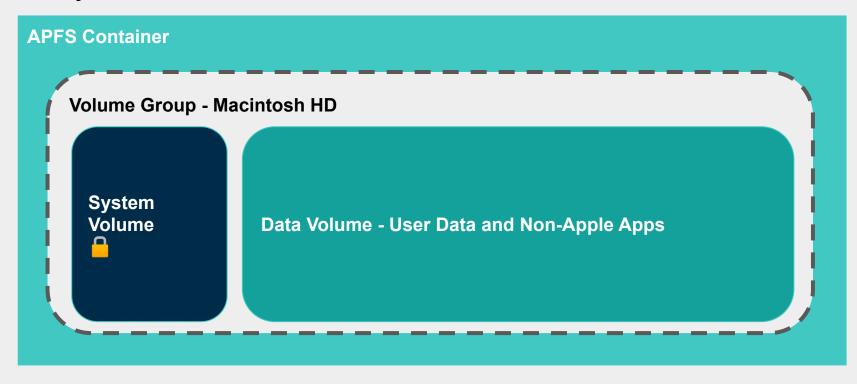


- Sierra (OS X 10.12) introduces APFS,
   first for solid state drives
- APFS has a number of improvements over the previous HFS+ filesystem



- 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.







- 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.







# Okay, but Updates?

Right. Stay on topic, Thomas.



#### **APFS Container**

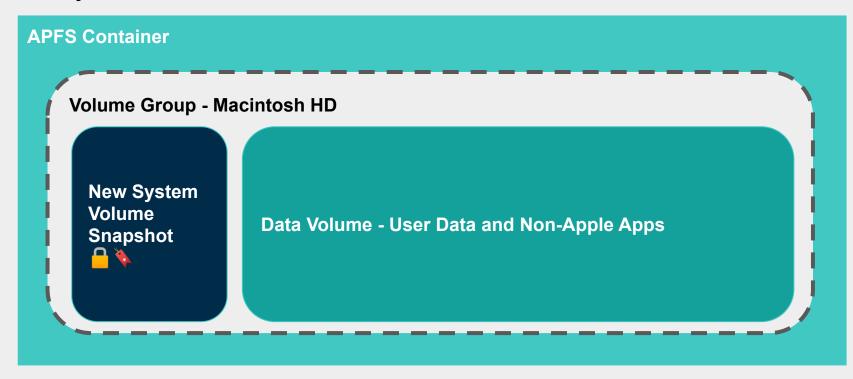
**Volume Group - Macintosh HD** 

Sealed System Volume



New System Volume Snapshot **Data Volume - User Data and Non-Apple Apps** 







## Wait, There's More

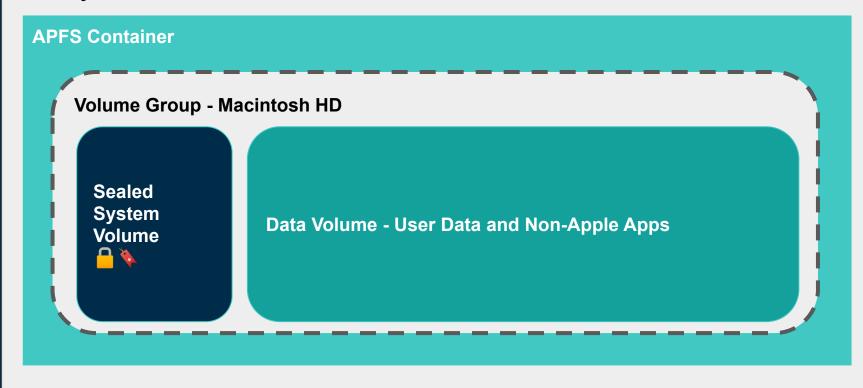
Software Update is also about Hardware!



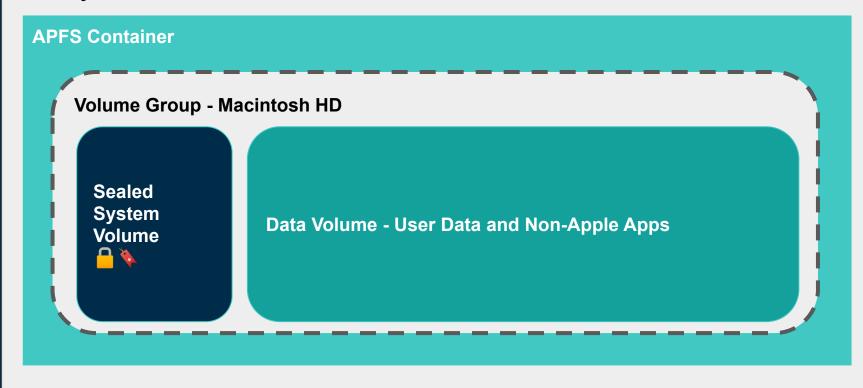
# A Note on Erase All Contents & Settings

macOS 12's Single Best Feature

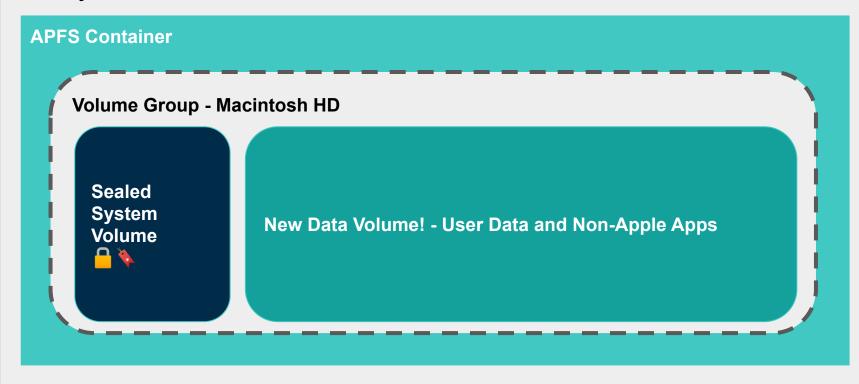














## **Booting macOS**

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.

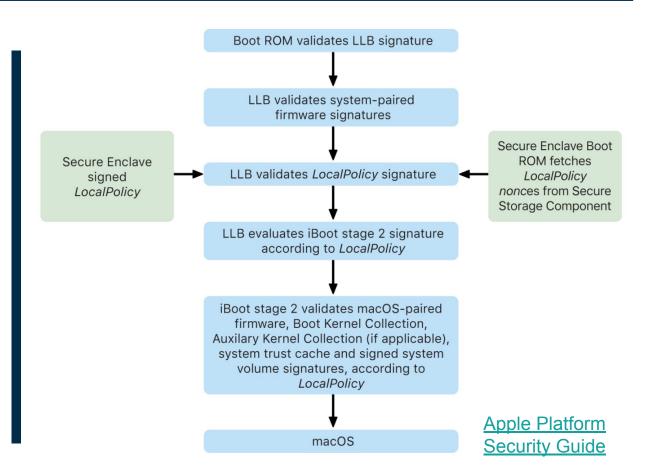
Apple Configurator 2 is valuable for **reviving** these devices in the event that something goes wrong that is recoverable.

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



# Macs with Apple silicon







# Managing Software Versions

And other lies we tell ourselves

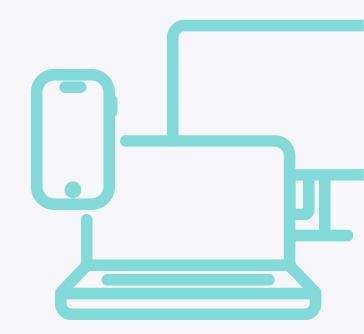


### Requirements for Software Update

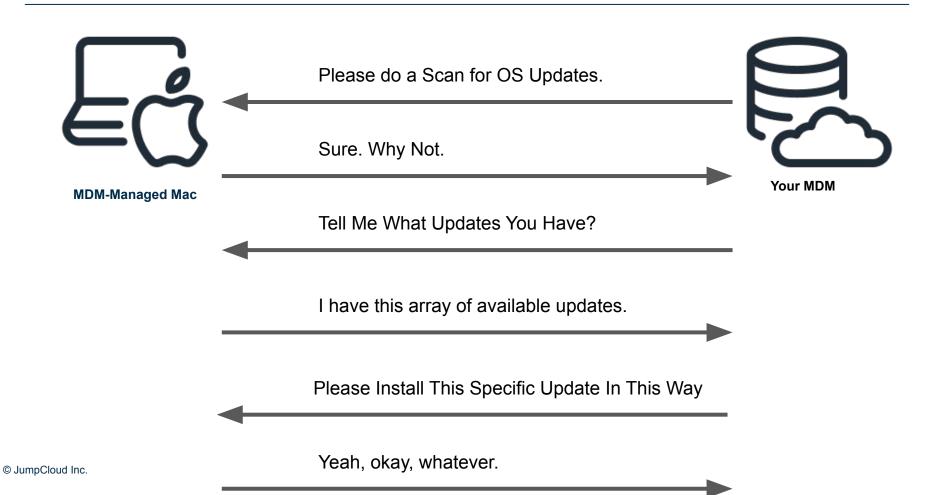
- You need an MDM to do anything interesting.
- You probably need more than just an MDM.
- Beginning with macOS 14 Sonoma & iOS 17, DDM is very helpful



### How Do MDM Updates Work?

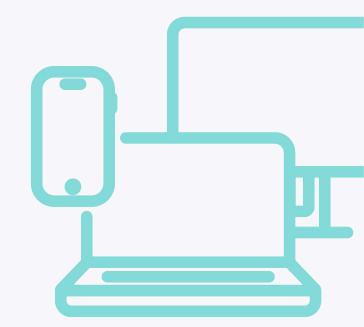








### A Brief Moment of Confusion



#### **OS Updates**

Select Install Action

OS 13.5.2 (22G91) **Total Number of Versions Available** 3 **Last Scanned for Updates** 09-29-2023 at 02:32pm Select an OS Update to Schedule Major updates can only be scheduled as install ASAP. **Available Updates** macOS Sonoma 14.0 (Major) macOS Sonoma 14.0 (Minor) 23A344 macOS Ventura 13.6 (Minor) 22G120 **Install Action** 

Schedule...

```
"allows_install_later": true,
      "restart_required": true,
      "metadata_url": "",
      "is_config_data_update": false,
      "human_readable_name": "macOS Sonoma 14.0",
      "app_identifiers_to_close": [],
      "product_name": "",
      "version": "14.0",
      "is_firmware_update": false,
      "requires_bootstrap_token": true,
      "human_readable_name_locale": "en-US",
      "product_key":
"MSU_UPDATE_23A344_patch_14.0_major",
      "install_size": 0,
      "build": "23A344",
      "deferred_until": "2023-10-26T00:00:00Z",
      "is_major_os_update": false,
      "download_size": 6447059124,
      "is critical": false
```



```
"allows_install_later": false,
  "restart_required": true,
  "metadata_url": "",
  "is_config_data_update": false,
  "human_readable_name": "macOS Sonoma",
  "app_identifiers_to_close": [],
  "product_name": "",
  "version": "14.0",
  "is_firmware_update": false,
 "requires_bootstrap_token": true,
  "human_readable_name_locale": "",
  "product_key": "_MACOS_14.0",
  "install_size": 0,
  "build": "",
  "is_major_os_update": true,
  "download_size": 12856486405,
  "is critical": false
},
```







#### **MDM**

User Enrolled Device

Manually Enrolled Device

Supervised Devices











#### **DDM**

User Enrolled Device

Manually Enrolled Device

Supervised Devices











#### Major

**V** 

**DownloadOnly** 

**InstallASAP** 

**Default** 

**NotifyOnly** 

InstallLater

InstallForceRestart

1

#### **Minor**













© JumpCloud Inc.



### 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 patching for the file system.

#### **OS Updates**

**OS** 13.3.1 (22E261)

Total Number of Versions Available

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**

Select Install Action

Schedule...



#### 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.





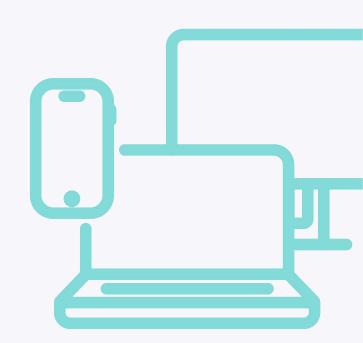
# What Changed in Software Update?

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

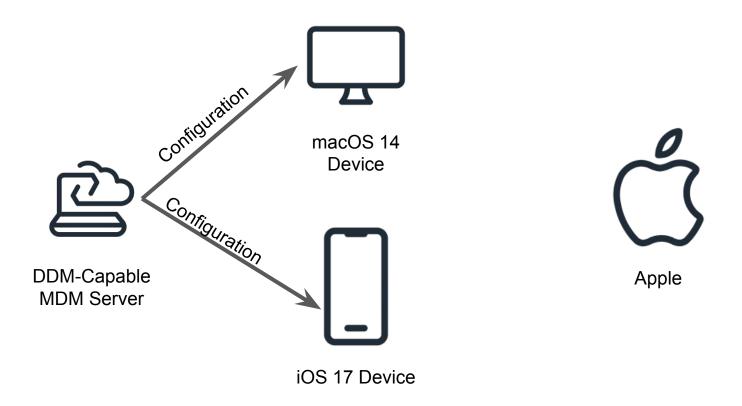
What's New in Managing Apple
 Devices, 2023



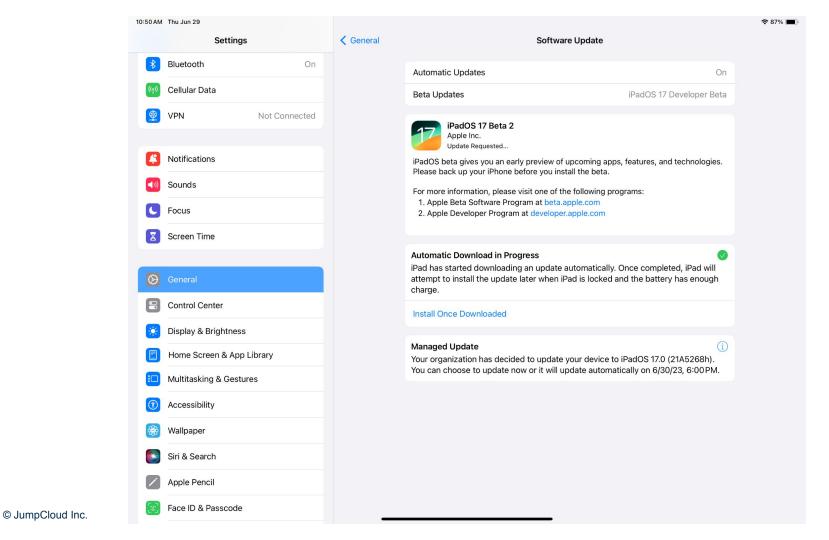
# How Does DDM Enforcement Work?

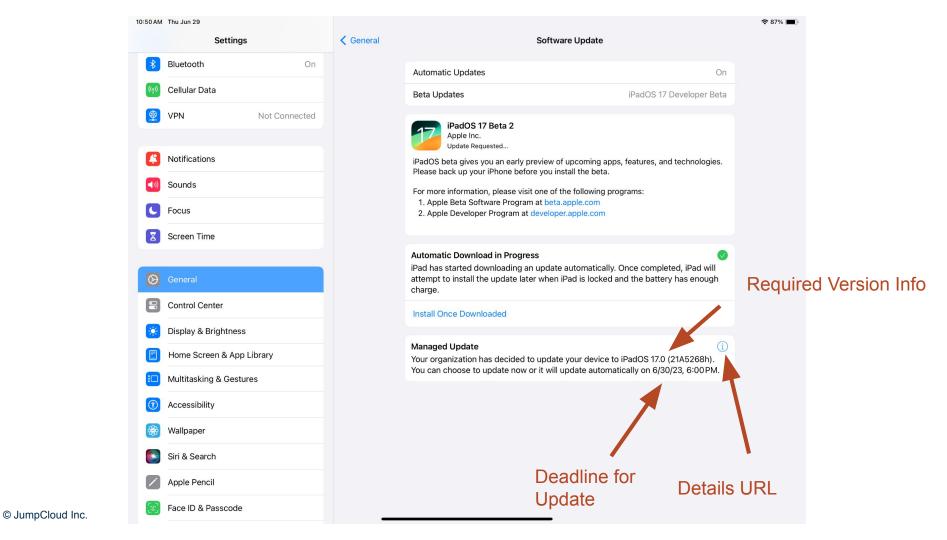






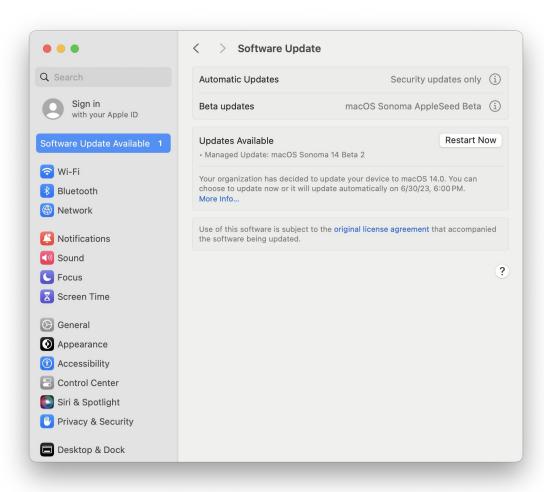
```
"Type":
"com.apple.configuration.softwareupdate.enforcement.specific",
   "Identifier": "tom.ios.enforcement",
   "Payload": {
       "DetailsURL": "<a href="https://youtube.com/watch?v=sVdaFQhS86E"">https://youtube.com/watch?v=sVdaFQhS86E</a>",
           "TargetLocalDateTime": "2023-10-05T18:00:00".
           "TargetOSVersion": "17.1",
           "TargetBuildVersion": "21B530"
```

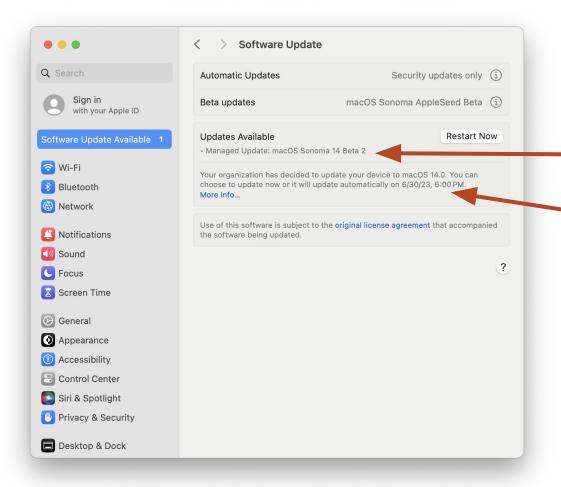




```
"Type":
"com.apple.configuration.softwareupdate.enforcement.specific",
   "Identifier": "tom.beta.enforcement",
   "Payload": {
       "DetailsURL": "<a href="https://youtu.be/5IsSpA0D6K8?t=29"">https://youtu.be/5IsSpA0D6K8?t=29</a>",
           "TargetLocalDateTime": "2023-10-05T18:00:00".
           "TargetOSVersion": "14.1",
           "TargetBuildVersion": "23A350"
```



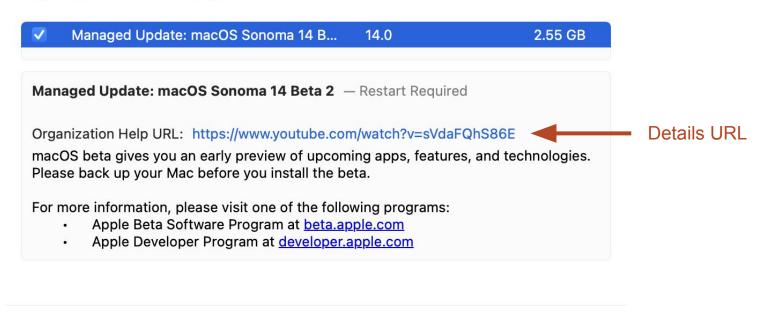




Required Version Info

Deadline

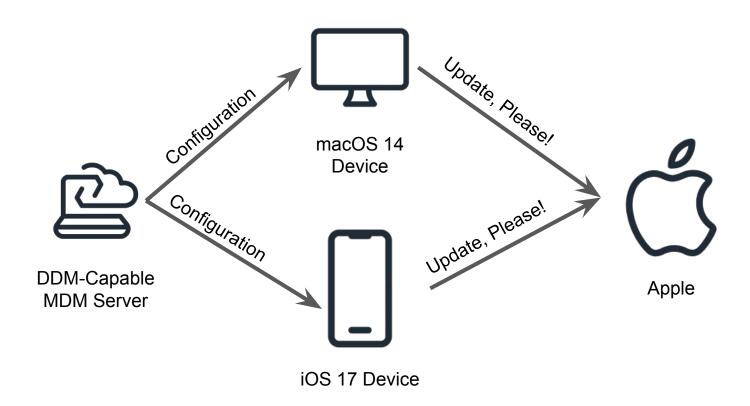
#### Updates are available for your Mac



Close

**Restart Now** 

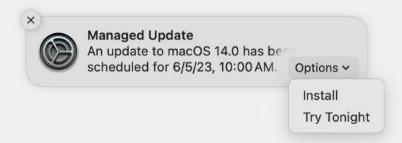
#### **Declarative Device Management - Software Update Configurations**

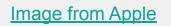




## So What Happens When You Ignore The Alerts?

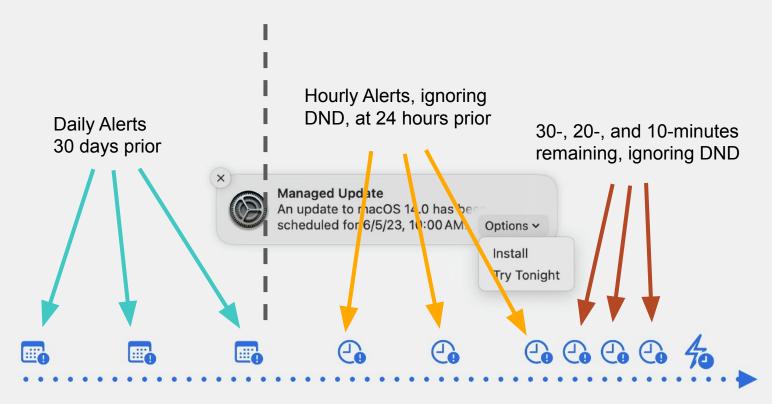
#### Update available notification





@ @ @ @ %

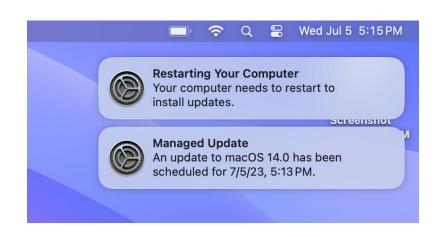
#### Update available notification

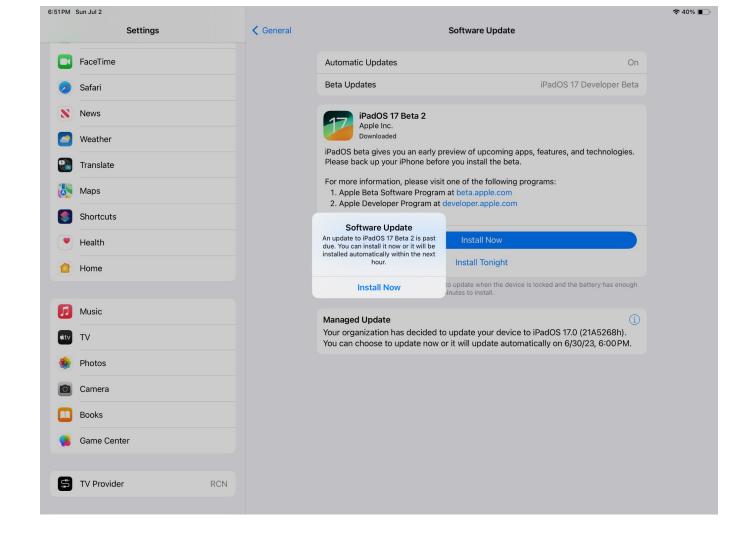




## So What Happens When You Ignore The Deadline?







## We Will See



## 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
- Describe time & effort savings desired
- 4. Provide examples and code
- 5. Center yourself with context
- 6. Clarity is the true soul of wit
- 7. More Bananas. 🝌 🝌



### Suggested Topic Areas

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

