Serious Talks about MDM Migrations

Hi, I’m Rick

@refreshingapathy on MacAdmins Slack
@rickheil on Github
Slides available now: rickheil.com/psu2023

In this talk, we'll cover…

- Selecting and working with potential vendors
- Running effective trial evaluations
- Choosing and implementing your migration method
- Planning and executing a successful migration program

Quick Poll

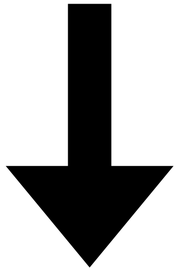
A note on commercial vs open source.


Getting started on your migration journey

Document Requirements

- List your needs (“what” - end state)
- Distill into requirements (“how” - method to end state)
- Categorize and rank your list
- Get feedback

NEEDS

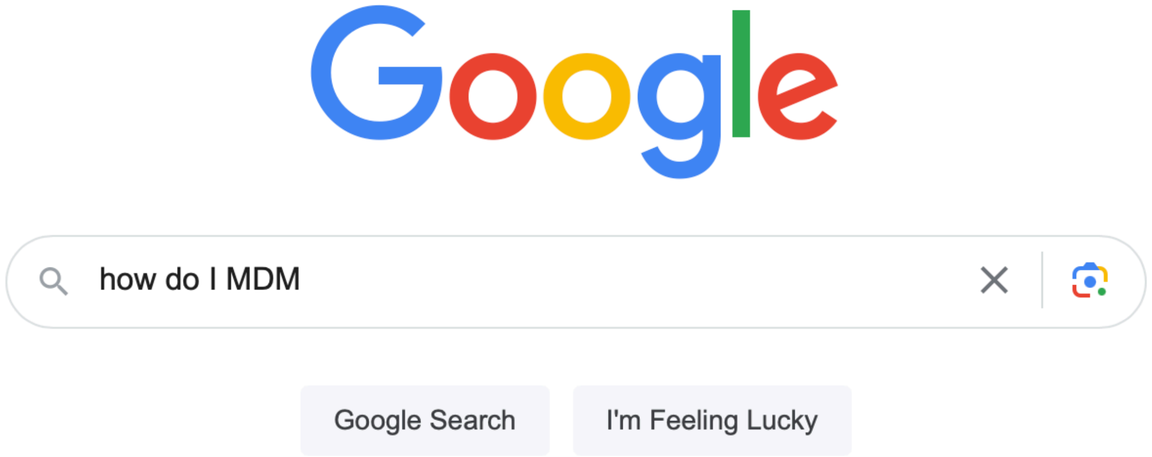


REQUIREMENTS

	A	B	C	D	E	F
1						
2	SAML/Okta integration for admin login	Y	Y	Y	Y	Y
3	Role-based access control	N	P	Y	P	Y
4	Grouping concept for machines	Tags	Blueprints	Groups	Device Groups	IDP Groups
5	Inheritance or group stacking	Y	N	N	Y	Y
6	Custom config profile support	Y	Y	Y	Y	Y
7	Custom config profile editor (browser)	N	N	Y	N	P
8	"Settings Builder" / GUI for:					
9	System Extensions	N	Y	Y	N	Y
10	Network Filters	N	N	Y	N	N
11	VPN Connections	Y	Y	Y	N	Y
12	WiFi	Y	Y	Y	N	Y
13	Printers	N	Y	Y	N	Y
14	Certificates	Y	Y	Y	N	Y
15	FileVault	Y	Y	Y	Y	Y
16	Firewall	N	Y	Y	Y	Y
17	Firmware / EFI passwords	N	Y	Y	N	N
18	Passcode policy	N	Y	Y	P	Y
19	Screensaver policy	N	Y	Y	Y	Y
20	Restrictions	Y	Y	Y	P	Y
21	Notification settings	N	P	Y	Y	Y
22	macOS Software Update Delays	N	Y	Y	Y	Y
23	SCEP	Y	Y	Y	N	Y
24	Target configurations by OS version	N	N	Y	N	N
25	Target configurations by hardware type	N	Y	Y	Y	P
26	Target configurations by architecture	N	Y	Y	N	N
27	Variable support for:					
28	custom config profiles	N	N	Y	N	N
29	group-wide values	N	N	Y	N	N

Finding Vendors

- Good ol’ Google
- Ask your VARs, MacAdmins Slack, or local MacAdmin friends
- Go check out the sponsors of this conference who are MDM vendors!



Engaging with Vendors

- Use your requirements
- Be up front on your schedule and process
- Ask about their post-purchase timing
- Build in appropriate growth
- Be reasonably cautious about promised new features

I’m not a procurement professional
(but I did stay at the Penn Stater last night)

- Always ask about volume discounts or pricing tiers
- If you have them, lean on your Finance or Procurement teams for help in negotiations
- Gather security or compliance documents ahead of time
- Longer commits can mean less cost

Running Proofs of Concept

- Test the whole device lifecycle
- Bandwidth (yours, not internet)
- Use your requirements list to score
- Deploy the same configs to each evaluated tool

Trial Config Set

Requirement	Deploy Process	Successful?	Notes
FileVault enabled, 2 deferrals	enable in GUI, set to two deferrals	Yes	
FileVault PRK escrow	check box to enable in GUI	Yes	
Trust CA root	Upload .cer file to GUI and assign	Yes	
Chrome configuration profile	Upload .mobileconfig to GUI and assign	Yes	
PPPC Management	use GUI to create profile, then add individual entries.	Yes	
Background Task Management	use GUI to create profile, then add individual entries.	Yes	
System Extension Allowlist	use GUI to create profile, then add individual entries.	Yes	
Network Content Filter Allowlist	Needed to upload custom config profile	Yes	Would prefer this to be a GUI builder.
Munki configuration profile	Needed to upload custom config profile	Yes	
SCEP - Device Cert	Needed to upload custom config profile	Yes	Would prefer this be a GUI builder.
WiFi authentication	use GUI to create profile, then assign	Yes	
Software Update profile	Can use GUI to assign but no variable support	Partial	Would prefer we have variable support in the GUI builder
Scope InstallApplications	upload signed pkg to GUI, assign to group	Yes	Must assign specific pkg - no version grouping

Choose a vendor

There can be only one

- Who meets the requirements best?
- Who has the best SLA and support?
- Whose roadmap matches my vision of the platform?
- Who has the best value for money?

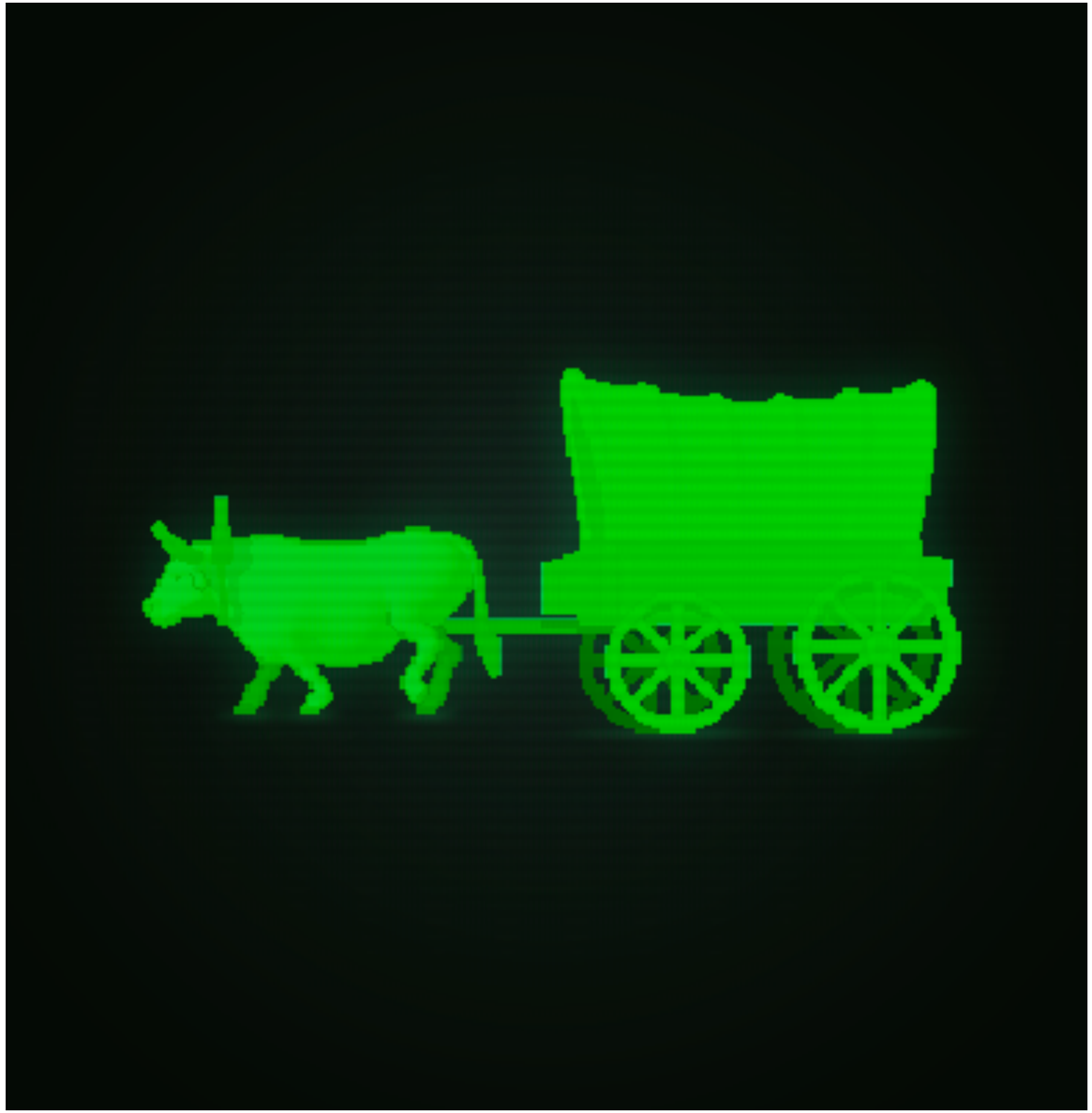
You bought the thing!

Now make it work.

- Read The Manual / Documentation
- Pick a naming scheme and stick with it
- Set up your configurations
- Document as you go
- Test the whole device lifecycle (again)

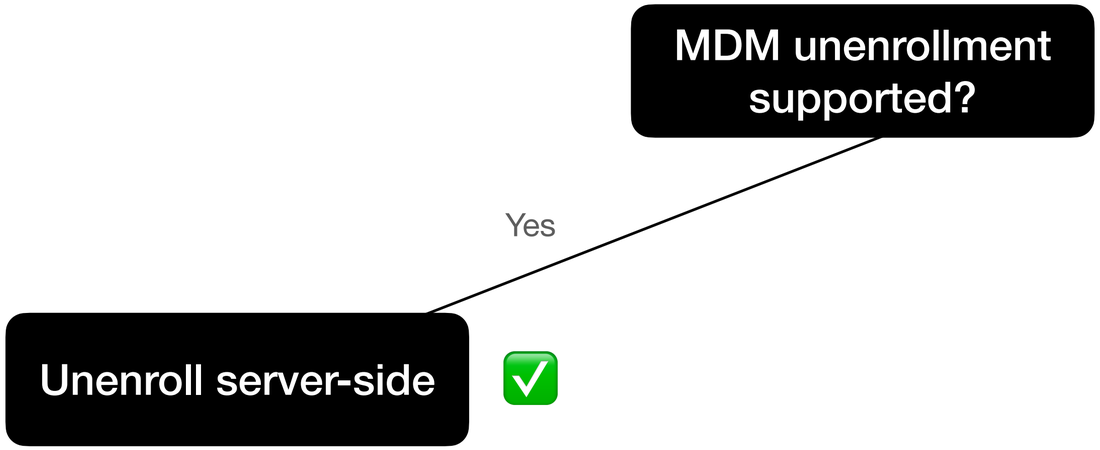
Planning Your Profile Migration Journey

An adventure, hopefully without snakebites

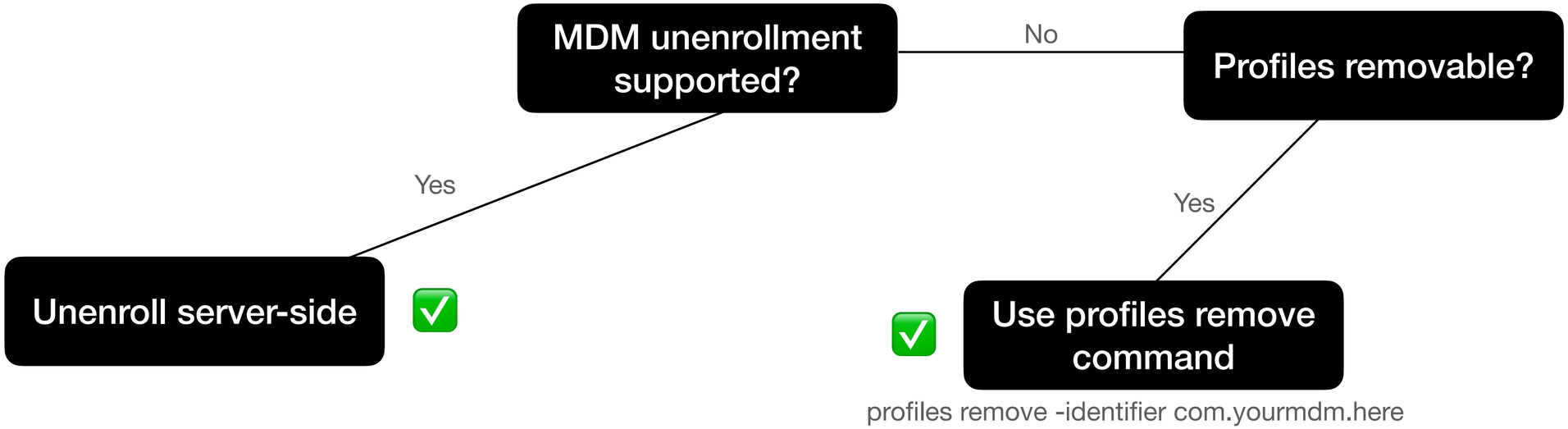


How will you unenroll and re-enroll devices?

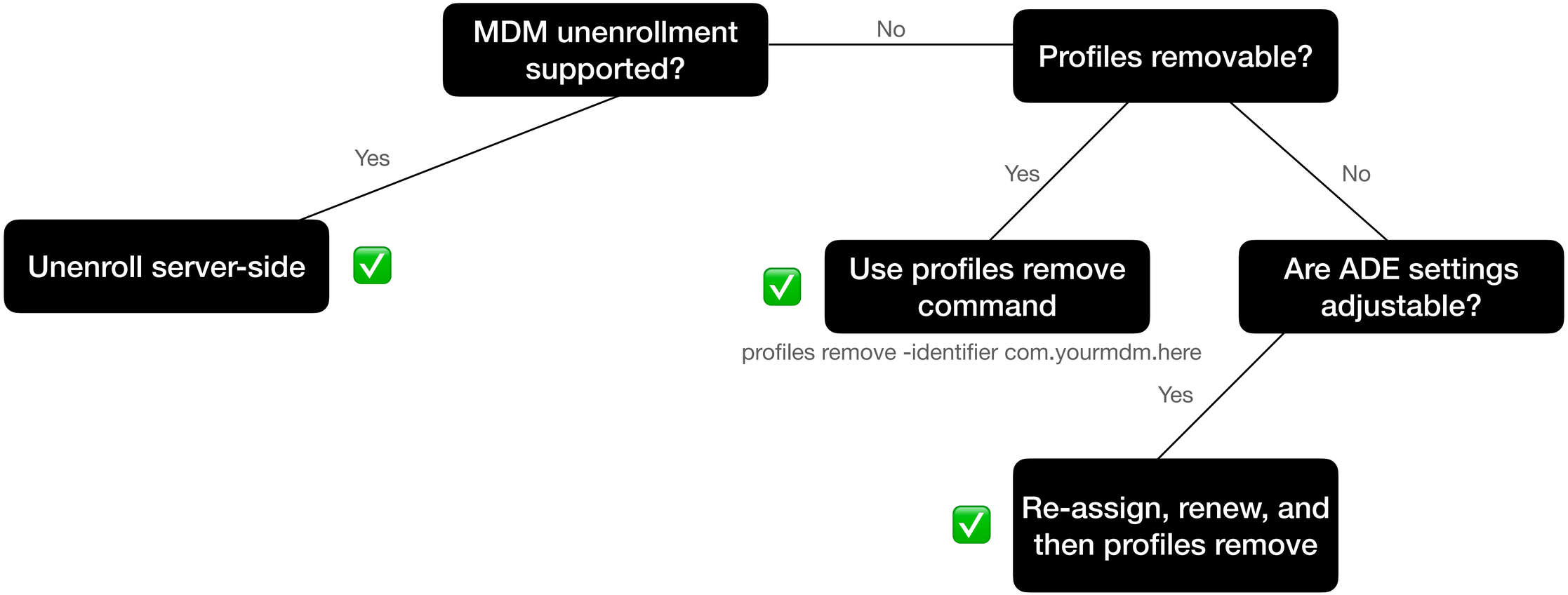
Decision Tree: Mac Profile Removal Method



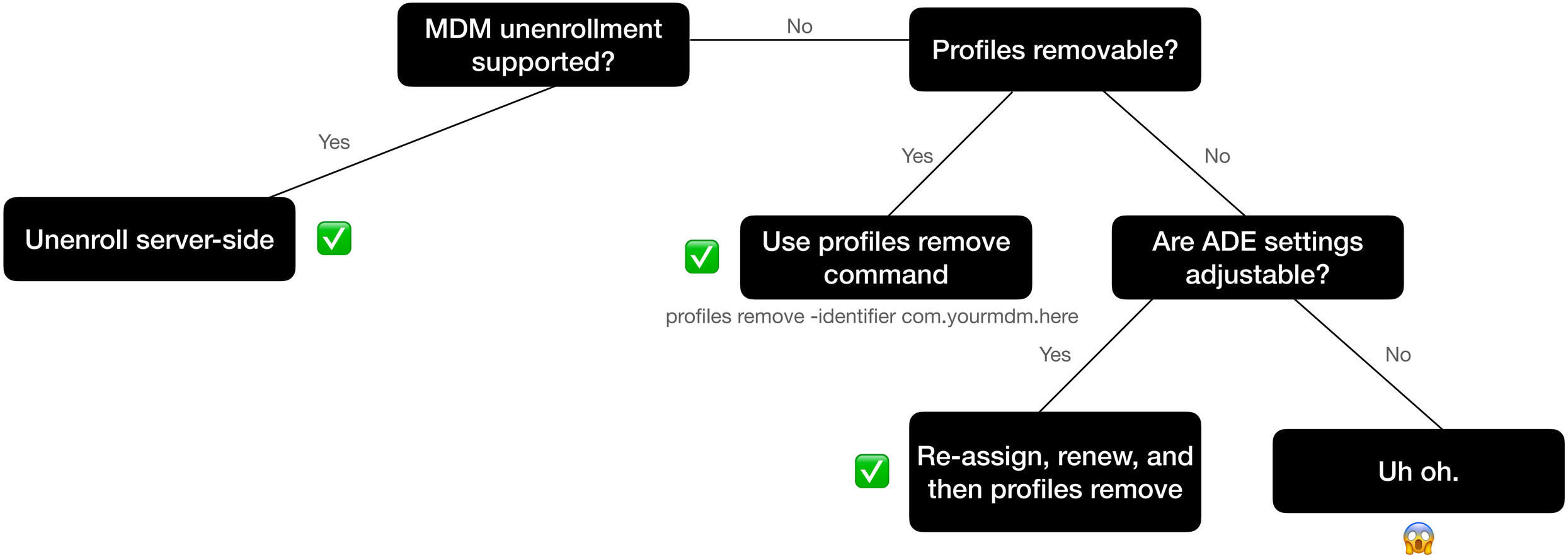
Decision Tree: Mac Profile Removal Method



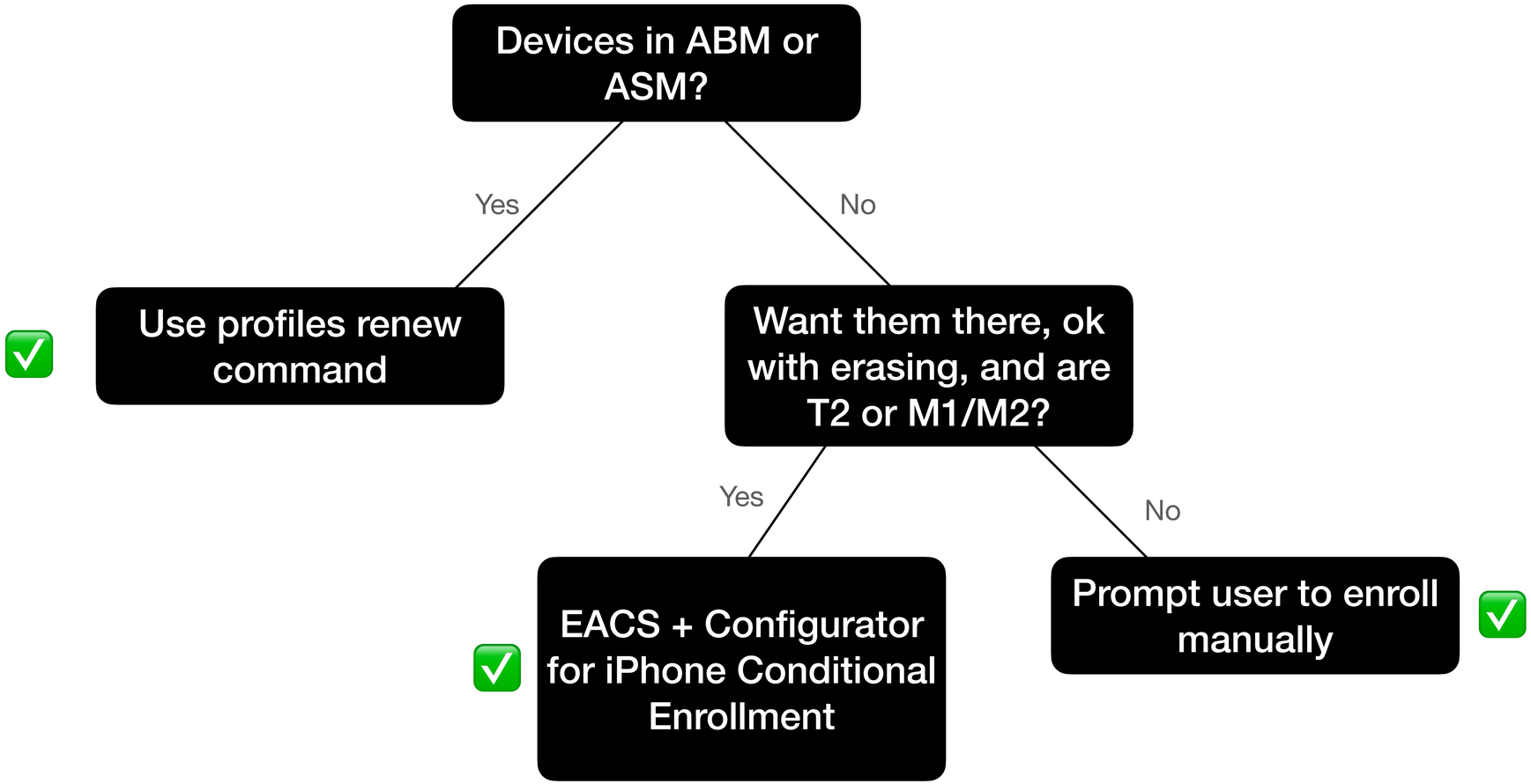
Decision Tree: Mac Profile Removal Method



Decision Tree: Mac Profile Removal Method



Decision Tree: Mac Profile Install Method



MDM Enrollment

Username:	Erik
Serial Number:	
User Approved MDM:	No
Days Remaining	125

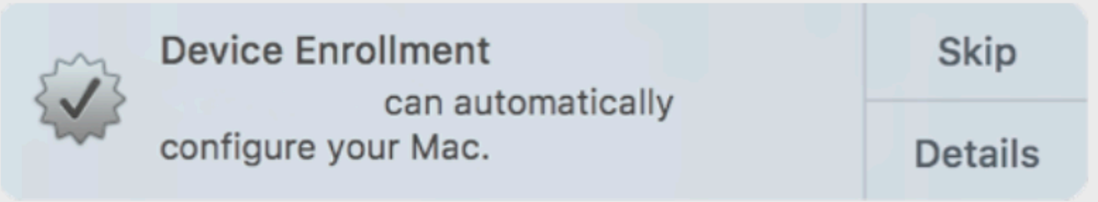
A friendly reminder from your local IT team

MDM Enrollment is required by 12/31/2018 (No Restart Required)

Enrollment into MDM is required to ensure that IT can protect your computer with basic security necessities like encryption and threat detection.

If you do not enroll into MDM you will lose the ability to connect to Wi-Fi, VPN and Managed Software Center.

To enroll, just look for the below notification, and click Details. Once prompted, log in with your username and password.



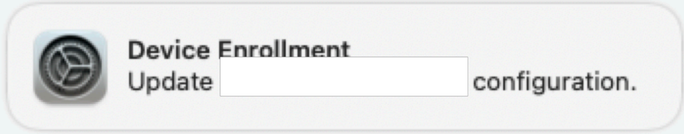
More Info

Close

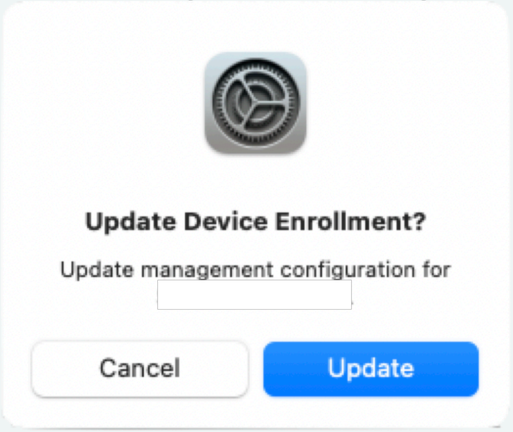
Device Management Update

As part of our ongoing improvements to device management, Client Platform Engineering needs you to update your MDM profile. When you have a moment, please do the following:

1. Click 'Ok, I'm Ready' below
2. Watch for this notification to pop up in the top right corner:



3. Click on the notification
4. Install the updated MDM profile by clicking Update.

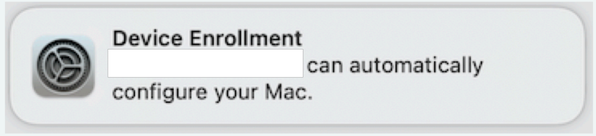


Not Now | Ok, I'm Ready

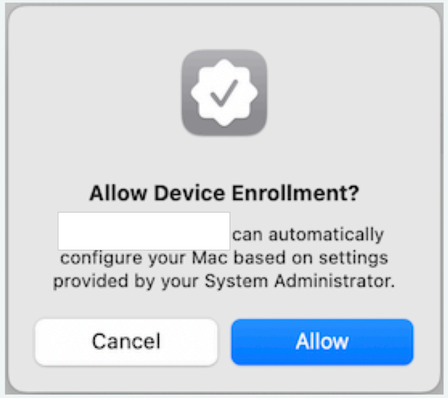
Device Management Update

IMPORTANT: During this process, your laptop may be disconnected from the internet for up to 10 minutes, and you will need to reboot your laptop at the end.

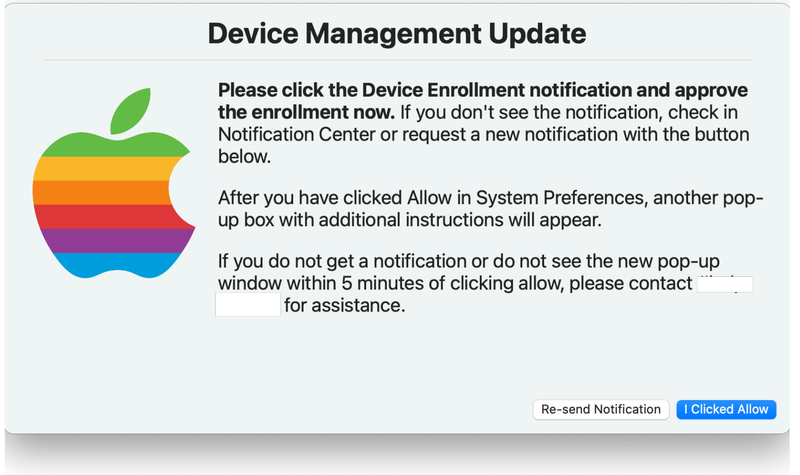
1. Click 'Ok, I'm Ready' below, and watch for this notification to pop up:

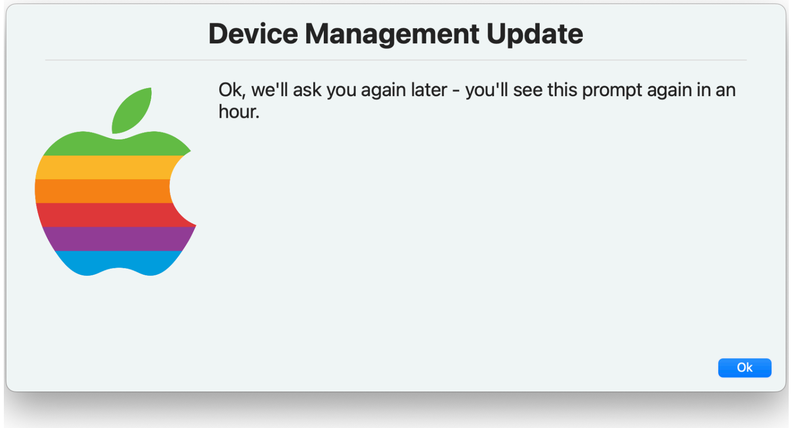


2. Click on the notification and install the profile by clicking the Allow button in System Settings / System Preferences.

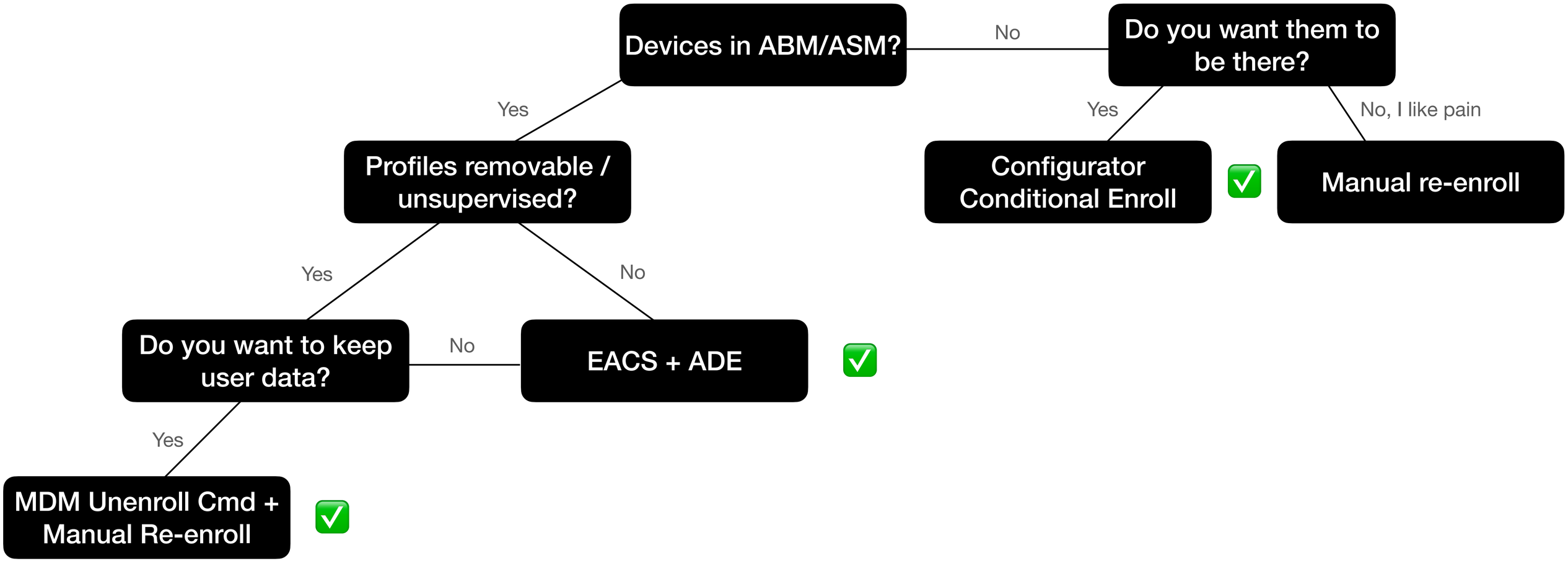


Not Now | Ok, I'm Ready





Decision Tree: iOS Migration Method

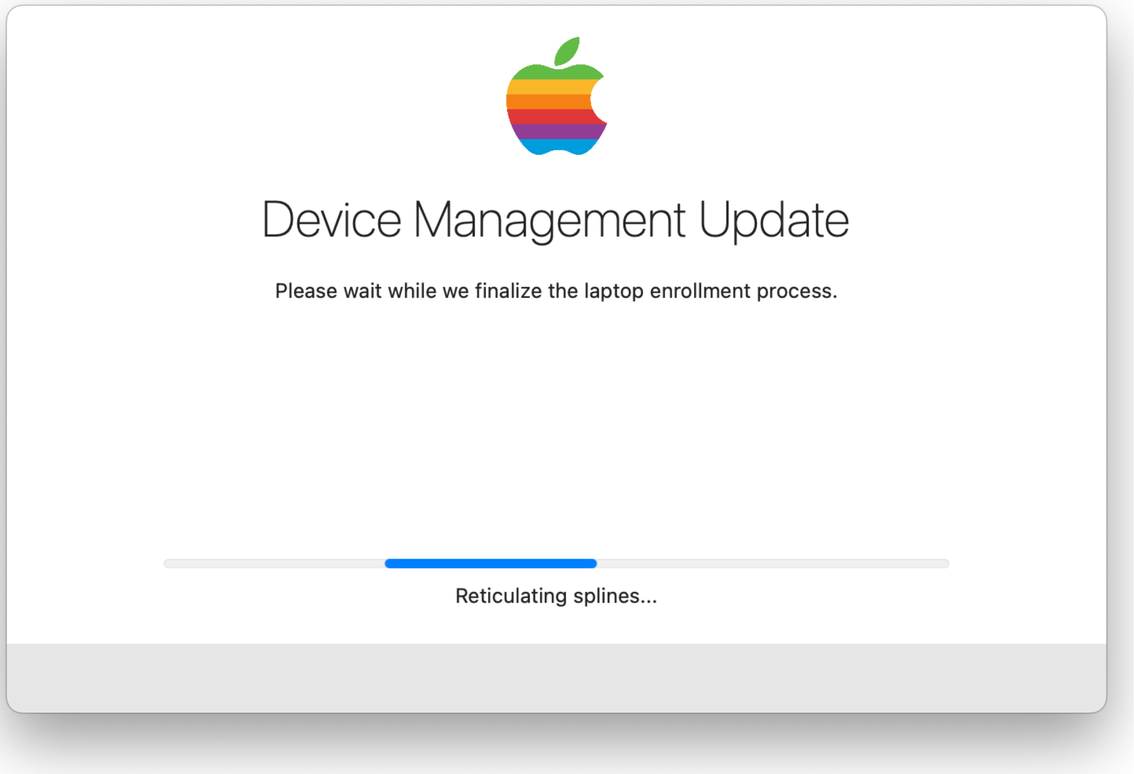


Post-Migration Tasks

- Knock-on effects with other tools
  - Anything with system extensions
  - Client certificates (SCEP/ ACME)
  - Other certificates (trusting a CA root maybe?)
  - How do apps react to being unconfigured and reconfigured?
- Clean up old agents/configs

Post-Migration Example

- InstallApplications for orchestration
- Messaging through DEPNotify and SwiftDialog
- Runs Munki
- Prompts the user to authenticate to rotate PRK
- Prompts the user to reboot



TEST TEST TEST TEST TEST TEST

Also don’t forget to test.

Other Considerations

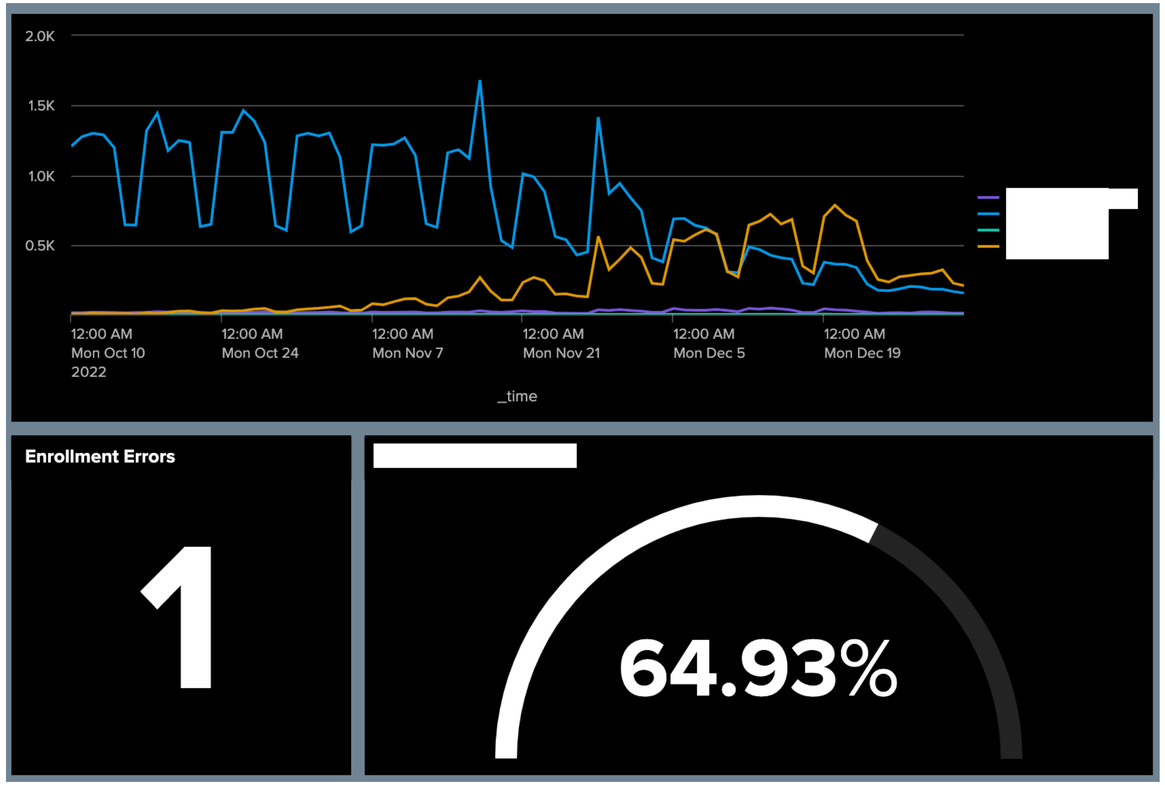
Stale / stolen / lost devices

- Have a plan for what to do about these devices
- Set a cutoff date
- Set ownership
- Keep in mind that devices that are enrolled to an MDM server that doesn’t exist any more won’t queue a command

Metrics

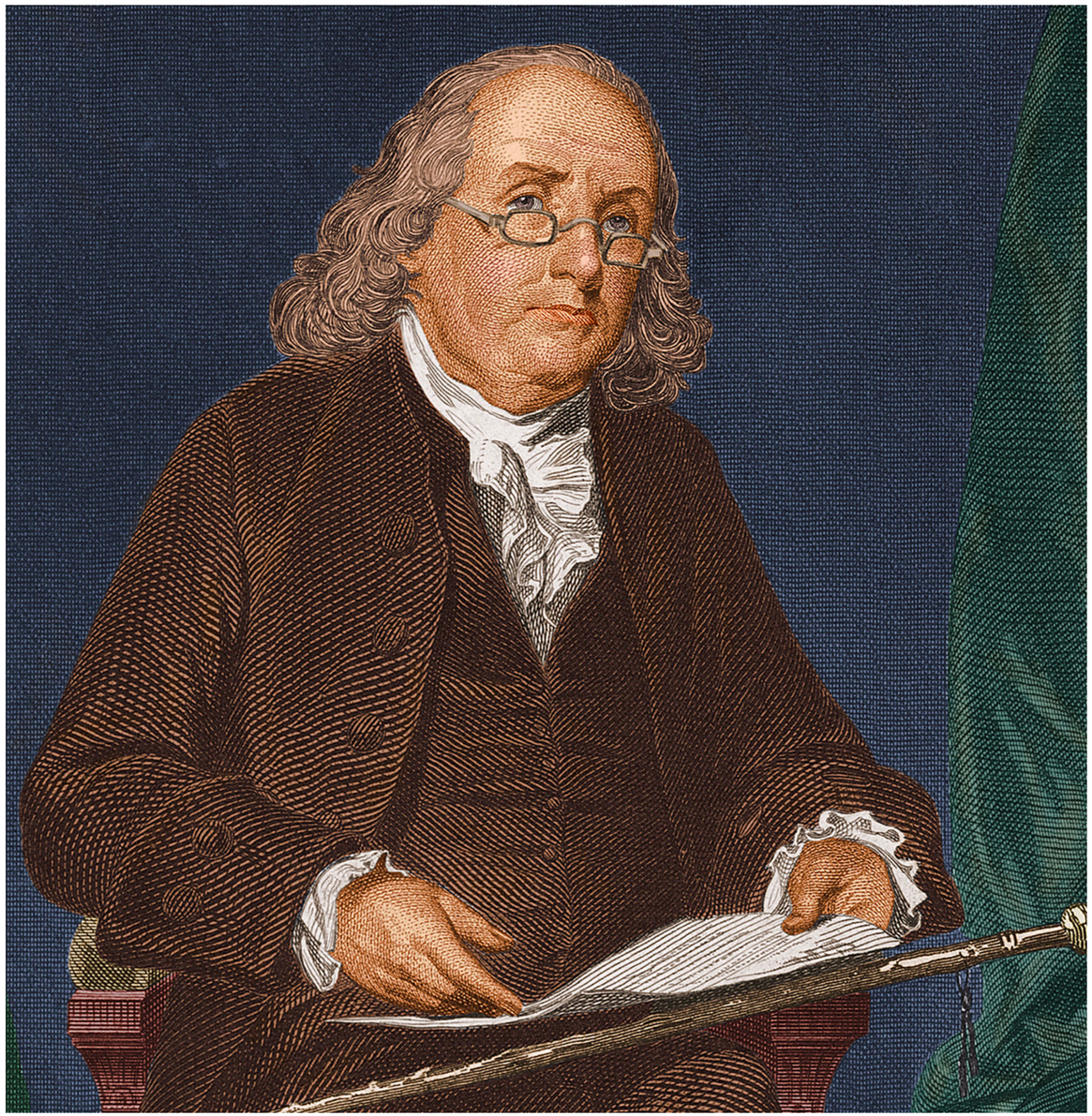
Because who doesn’t love a pretty graph?

- Track each migration state
- Tie data to a serial number or user
- Define acceptable “overdue” thresholds



Some writing…

- “Heads up!”
- “Your turn!”
- “You’re late!”
- “You’re in trouble”
- Don’t forget the how to



A little more writing

- Socialize your release schedule and communications with management
- Use screenshots or screen capture video where appropriate
- Offer live training for your colleagues and support team(s)


United States
Atlantis


SELF-CARE
ISN'T
SELFISH

Deploy to new laptops first.

Push tools in “lurk mode”.

Don’t do it all at once.

Don’t be afraid to pause.

Support your support.

Leverage your metrics.

Bother overdue users. A lot.

Celebrate when you’re done.

Q&A