July 17, 2025

Migrate MDM servers with this one simple trick!

...

MacAdmins Conference
July 17, 2025

MDM Migration Demystified: Best Practices for MacAdmins

...

Kevin M. Cox
Manager, Client Platform Engineering at DoorDash
Houston Apple Admins co-founder
@kevinmcox on MacAdmins Slack
https://www.kevinmcox.com/links

Changing MDMs is disruptive

😵 Changing MDMs is disruptive

- Requires user interaction and work disruption for companies utilizing commercial MDM providers

- The potential for disruption prevents companies from changing vendors when they want to (in my opinion)

- Minimizing this disruption is the primary goal

Thankfully, Apple makes it easier every year.

macOS 12: Erase All Content and Settings

“MDM can perform Erase All Content and Settings on Mac computers with Apple silicon or the Apple T2 Security Chip.”

macOS 13: Internet required during Setup Assistant

“Mac computers registered to an organization must connect to a network during Setup Assistant after being erased or reset.”

macOS 14: Full screen “DEP nag” with deadline

“Automated Device Enrollment can be enforced after Setup Assistant.”

macOS 15: Standard users can authorize MDM enrollment

"*profiles renew -type enrollment* no longer requires admin credentials if you are not already enrolled in MDM."

macOS 26: MDM migration from ABM/ASM

“Apple School Manager and Apple Business Manager support migrating to a new device management service.”

Thanks Apple!

macOS 12: Erase All Content and Settings

macOS 13: Internet required during Setup Assistant

macOS 14: Full screen “DEP nag” with deadline

macOS 15: Standard users can authorize MDM enrollment

macOS 26: MDM migration from ABM/ASM

Living the dream!

🏝️ Living the Dream!

- Great for MacAdmins!
- The historical barriers to MDM migration no longer apply
- You no longer have to deploy anything to the Macs
- MDM vendor participation is not required
  - No more artificial lock-in
  - While most vendors allow you to easily unenroll devices in bulk via API, not all of them do
  - MDM vendors will be forced to compete on features, support and price
- Great end user experience allowing them to migrate on their own schedule up until the deadline

Let’s go?

🐌 Don’t forget to consider...

- Macs not in Apple Business Manager / Apple School Manager
- Macs not currently enrolled in MDM via ABM/ASM
- Macs running old versions of macOS
- Official documentation:
    - https://support.apple.com/guide/deployment/migrate-managed-devices-dep4acb2aa44/web

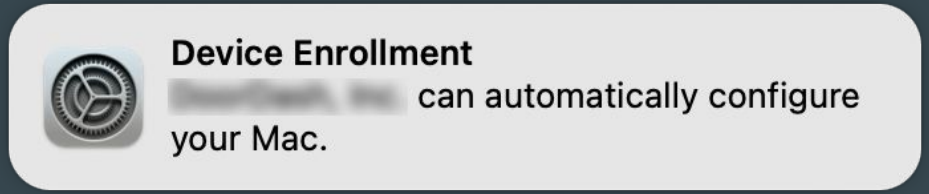
Our MDM Migration Story

Historically, re-enrollment was not intuitive

In macOS 13 Ventura and older, the built-in dialogs are not effective for timely re-enrollments

Historically, re-enrolling to a new MDM was not intuitive

- The “DEP nag” was easily missed



- Users could ignore it indefinitely

- There was no native ability to force re-enrollment

GUI needed

- Other companies have shared examples of using tools like swiftDialog to build their own UI for the process

- We were fully prepared to go down this road as well

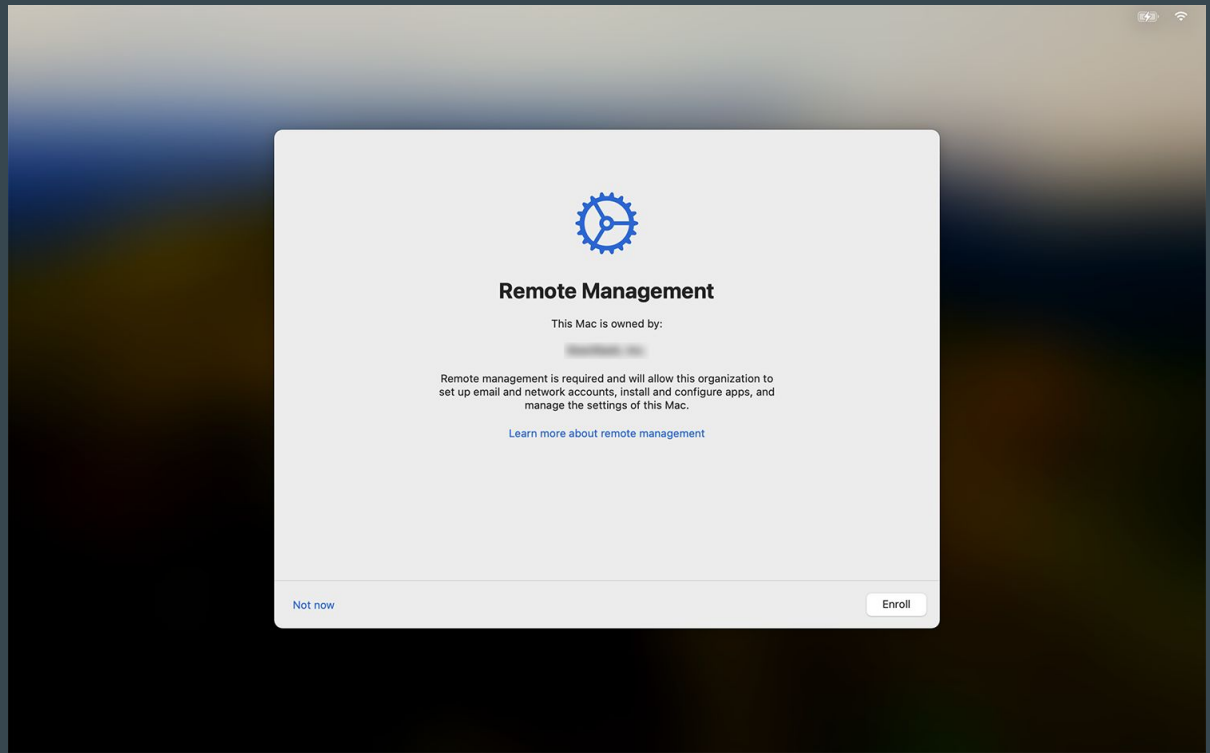
- Until WWDC 2023 when macOS 14 Sonoma was announced!

macOS 14 Sonoma

“Automated Device Enrollment can be enforced after Setup Assistant.”

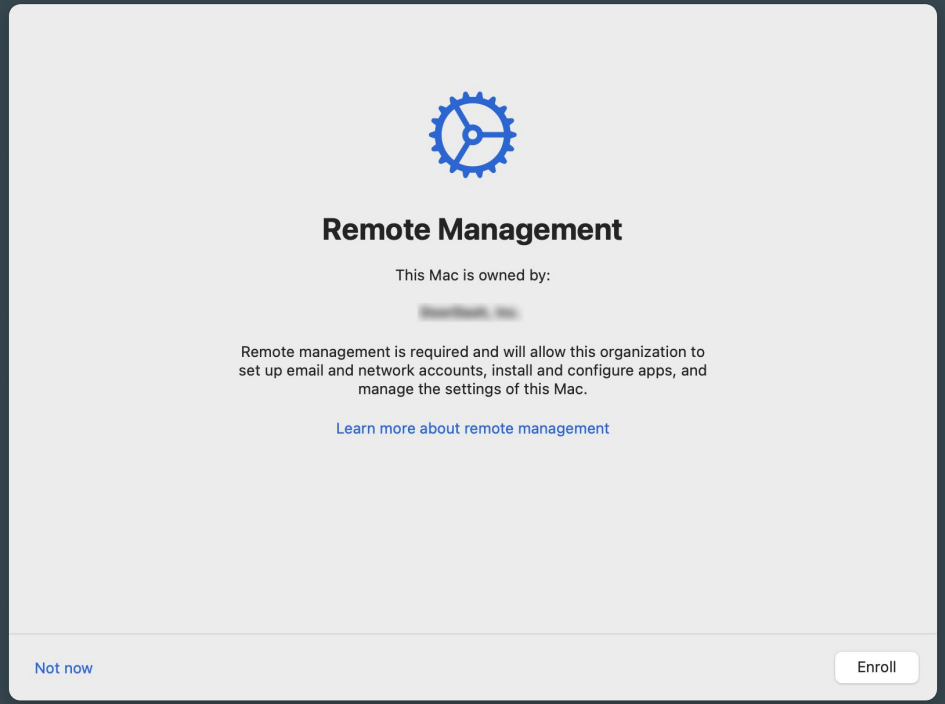
Native experience

- Full screen dialog replaces the traditional “DEP Nag” in Notification Center



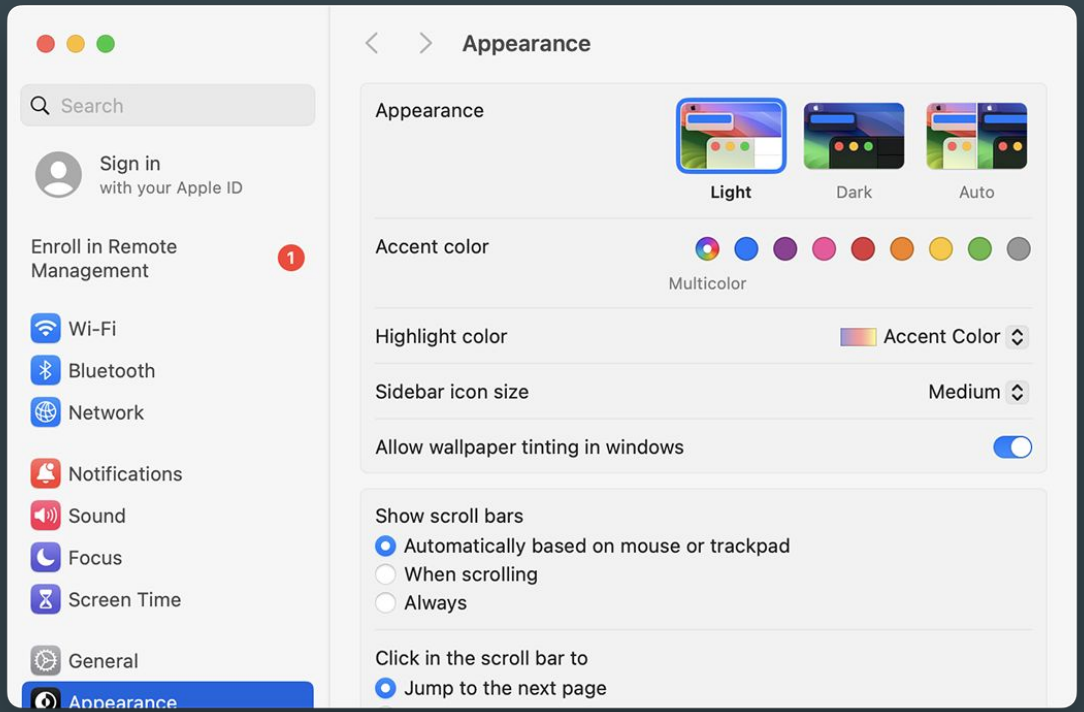
Native experience

- Users can defer for eight hours by selecting “Not now”



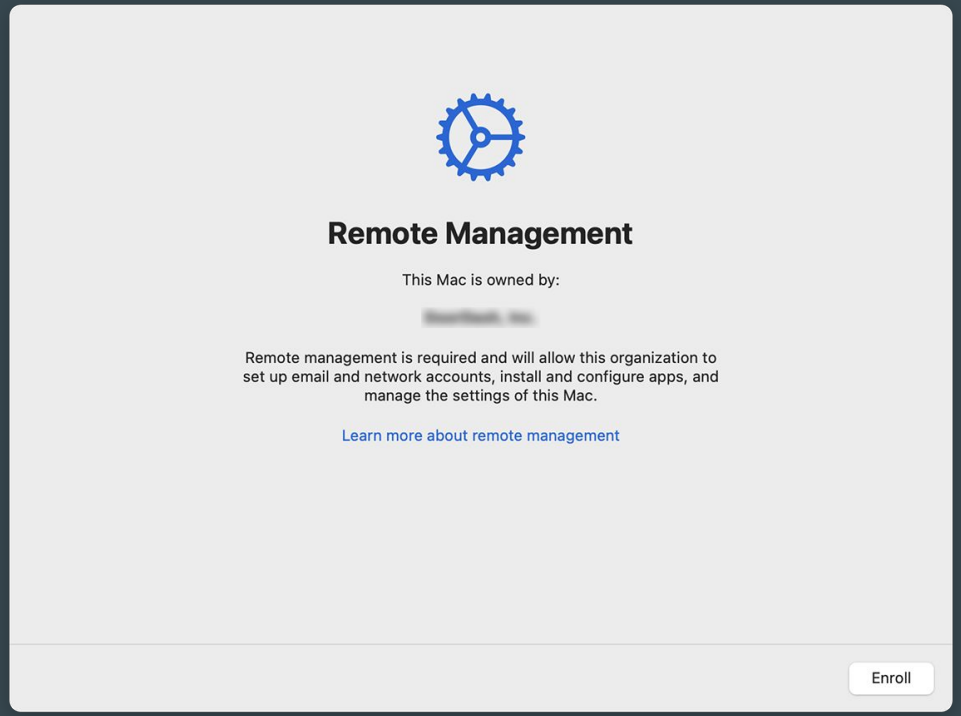
Native experience

- Users can resume the process at anytime by visiting System Settings



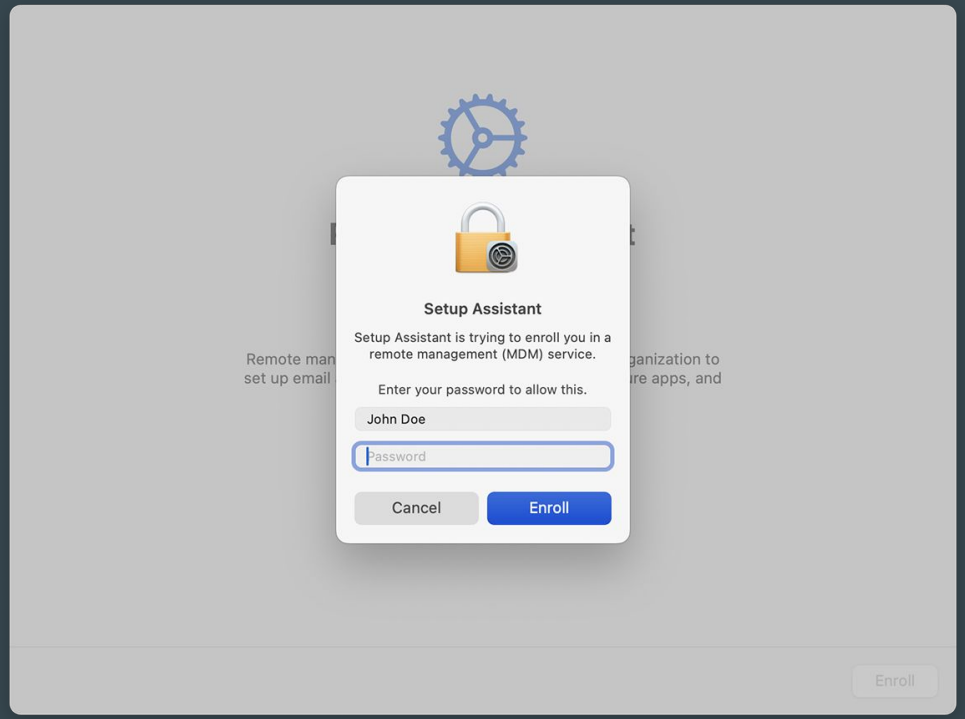
Native experience

- After eight hours the fullscreen dialog returns with no ability to defer



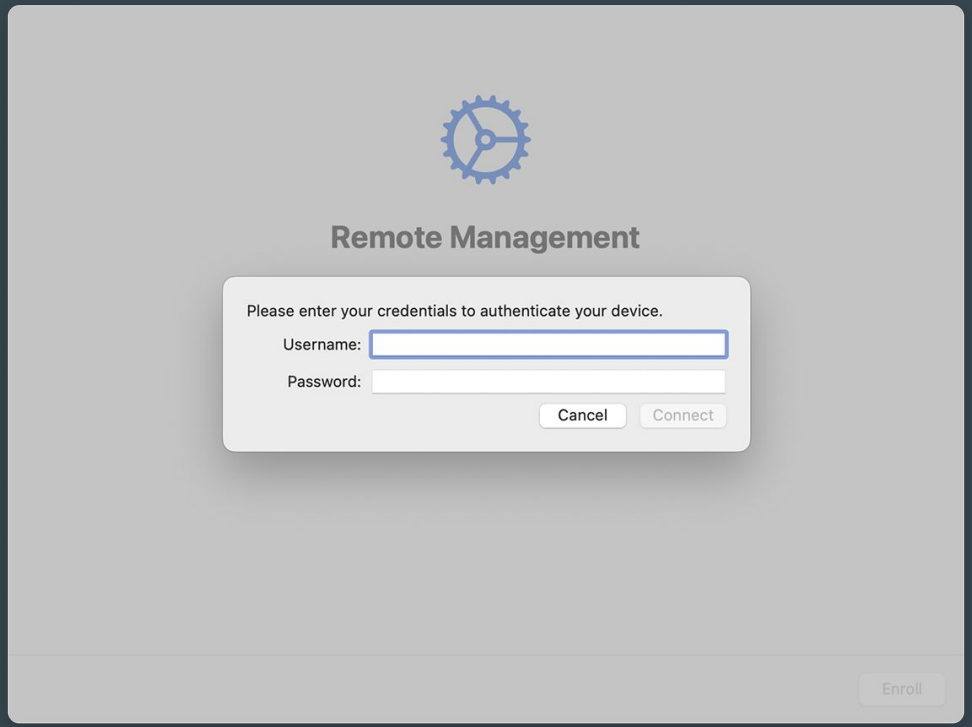
Native experience

- In macOS 14, but not macOS 15, users are still required to be local admins



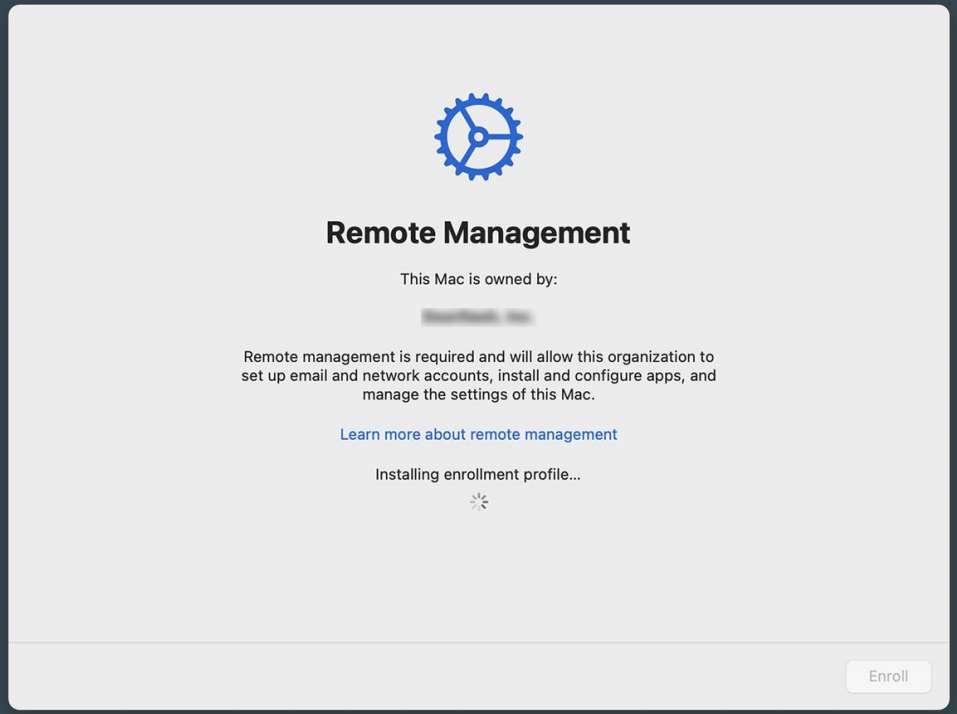
Native experience

- If you require authentication for ADE enrollment that comes next



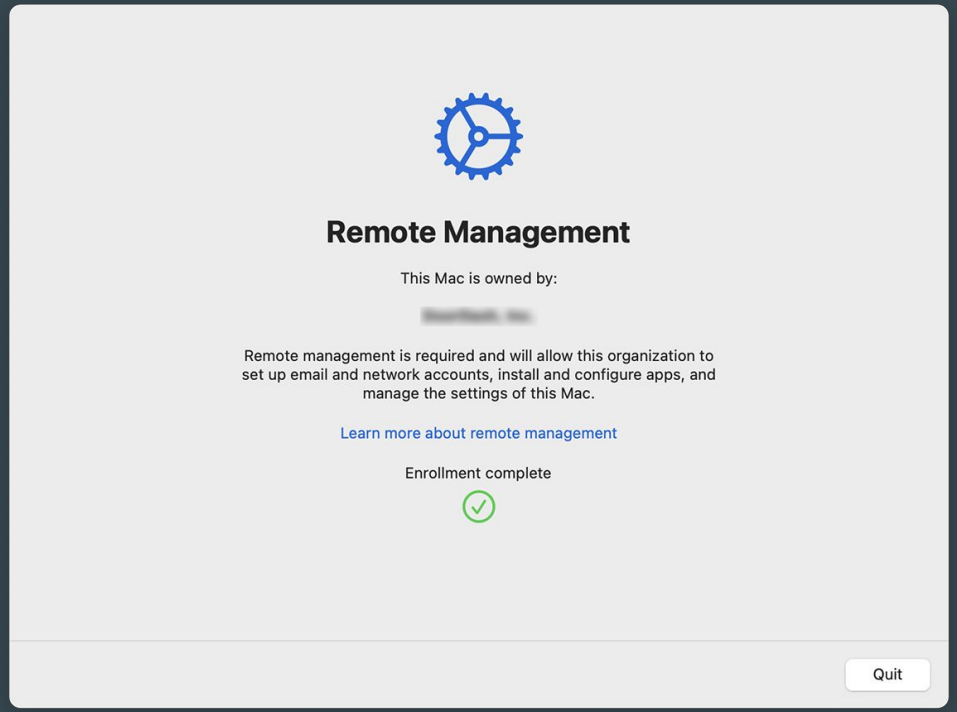
Native experience

- The Enrollment profile is installed



Native experience

- And just like that, Enrollment is complete and users can exit to the desktop



Trade-offs

- Could we give users a choice to migrate on their schedule?
- Some MDM vendors provide a “tool” to facilitate migration, but many require deploying an API key to every device
- We built a POC to use our CI/CD as an intermediary, but didn’t utilize it
- We decided that we didn’t have time to mix a custom UI with the new built-in dialog and solve the security concerns by our deadline

Limitations

- The new dialog must be purposefully launched (in an MDM migration scenario)
  - Simply unenrolling a Mac or changing MDM assignments in ABM is not enough to trigger it
- If a user defers, the dialog is not seen again until eight hours later
  - At that point they must complete enrollment
- This new dialog only exists on macOS 14, so everyone had to upgrade first
- Devices must be in Apple Business Manager
- To workaround the limitations we needed to build the logic to craft our ideal user experience

🗣️ Communication is key

- Coordinated with Internal Communications department
- First mention was during a company all-hands one month prior
- Company-wide email went out two weeks prior
- Company-wide Slack post the week we started
- A detailed FAQ that was updated as new questions got asked
- Detailed screenshots for each step of the process
- A dedicated Slack channel for questions and support
- Direct messages from our IT Bot on Slack to communicate scheduling, provide instructions, confirm completion and remind users on an individual basis
    - This included addressing them by name and specifying the serial number of their device(s)

Crafting the user experience: Slack notifications

- Notify users who had not upgraded to Sonoma yet
  - Notification to managers for users who failed to update after a week
- Notify users the day before their migration
  - A direct message addressing them by name, listing the serial number to be migrated and explaining what was happening
  - Add them to a dedicated Slack channel to find documentation, allow them to ask questions or request to migrate earlier or later
- Remind users 1 hour before their migration
  - Direct message and a post in the channel
- Inform them the process is starting
  - Direct message and a post in the channel
- Thank them once complete
  - Direct message and remove them from the channel

Crafting the user experience: Slack notifications

[ACTION REQUIRED] YOU ARE SCHEDULED FOR TRANSITION TOMORROW

Hi {real_name},

Tomorrow at 10:00 AM Pacific you are scheduled to complete the company-wide MDM transition for MacBook *{serial}*. For details please reference the announcement: {url}

This process will take less than five minutes and does not require closing any of your applications or restarting your computer.

If you are in the office when this occurs, you will be disconnected from the Wifi. Please note the password for the DoorDash WiFi network, as you will need to manually connect to complete the process.

You have been added to the <#{migration_channel}> channel where we are happy to answer any questions and provide assistance.

Thank you for helping keep DoorDash secure!

-- DoorDash IT

Crafting the user experience: macOS dialog timing

- A single alert before the deadline was not enough
- We wanted to provide users with an escalation of alerts and sense of urgency as the eight hour deadline approached
- Every hour for the first four hours
- Every 30 minutes for the next two hours
- Every 15 minutes for the last two hours
- Of course none of these repetitive dialogs were needed for users who completed the process right away

On-device deployment

- All we needed to deploy to the Macs was a LaunchDaemon and python script
  - We also wrote the Munki configuration to disk so we still had some ability to manage Macs while the configuration profile was missing

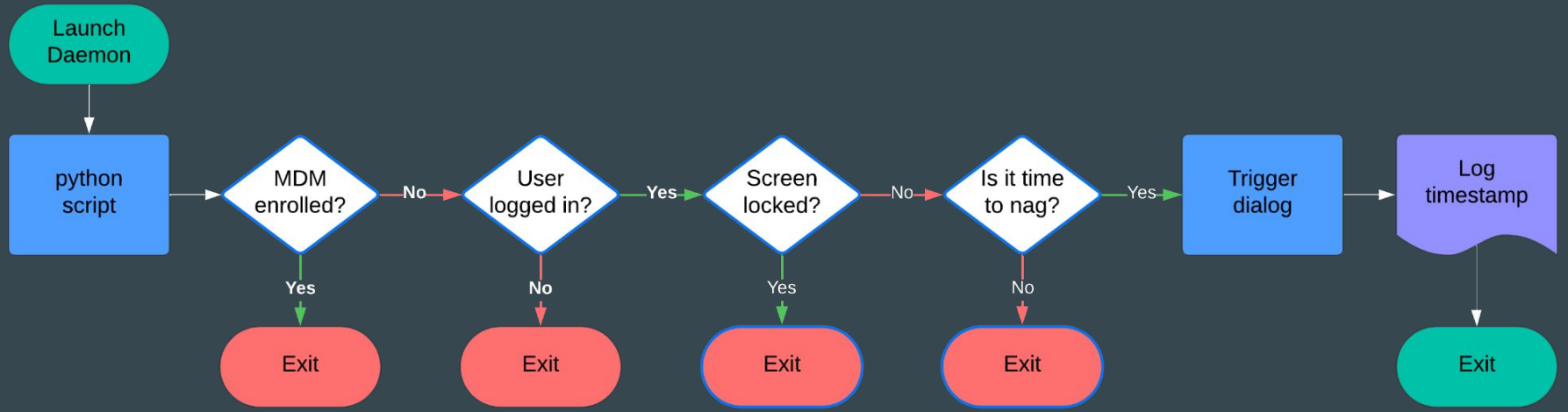
- We decided on a five minute interval for the LaunchDaemon

- Munki delivered these via package well before we started the process and ensured they remained installed and loaded

The python script

- A single python script contained all the logic needed to automate the on-device experience for our users
- Basic checks
  - Is the device unenrolled?
  - Is a user logged in?
  - Is the screen unlocked?
  - Have we prompted recently?
- Calculate the deadline and prompt timing
  - We used “`com.apple.mdm.depnag.plist`” to calculate the deadline for the prompt timing
- Display the prompt
  - Run “`sudo profiles renew -type enrollment`” as the user
- Log it all!

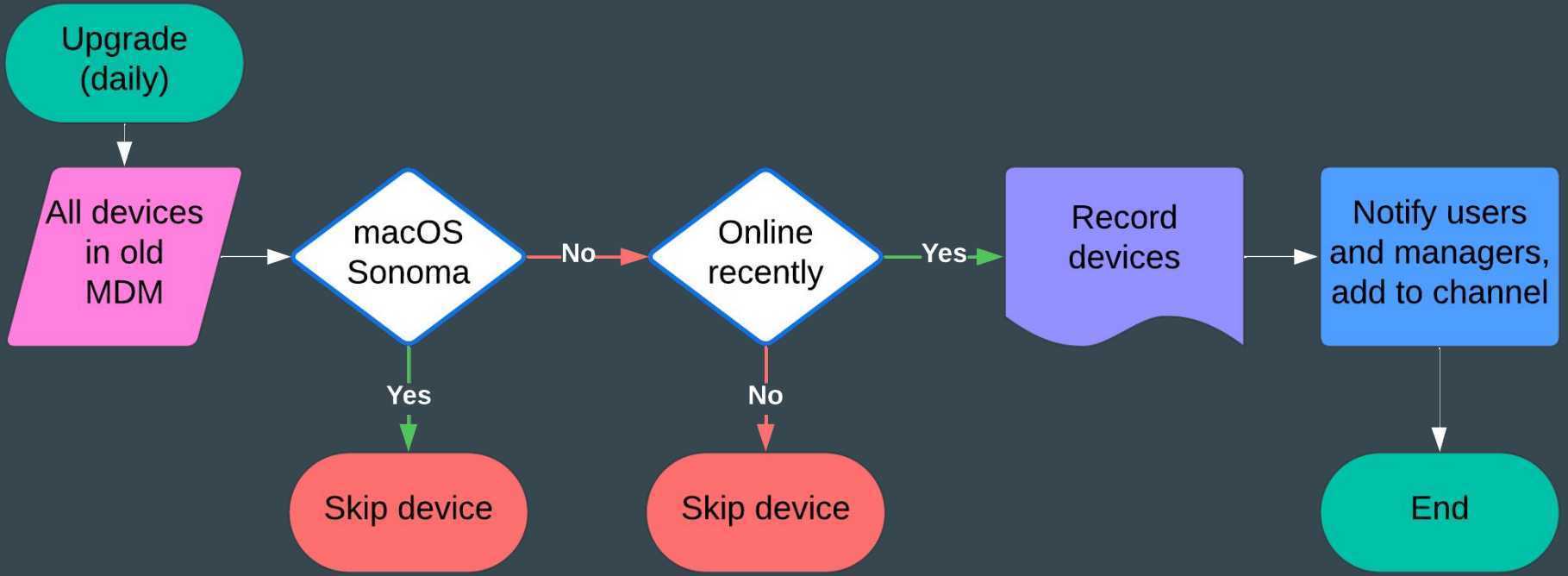
On-device logic



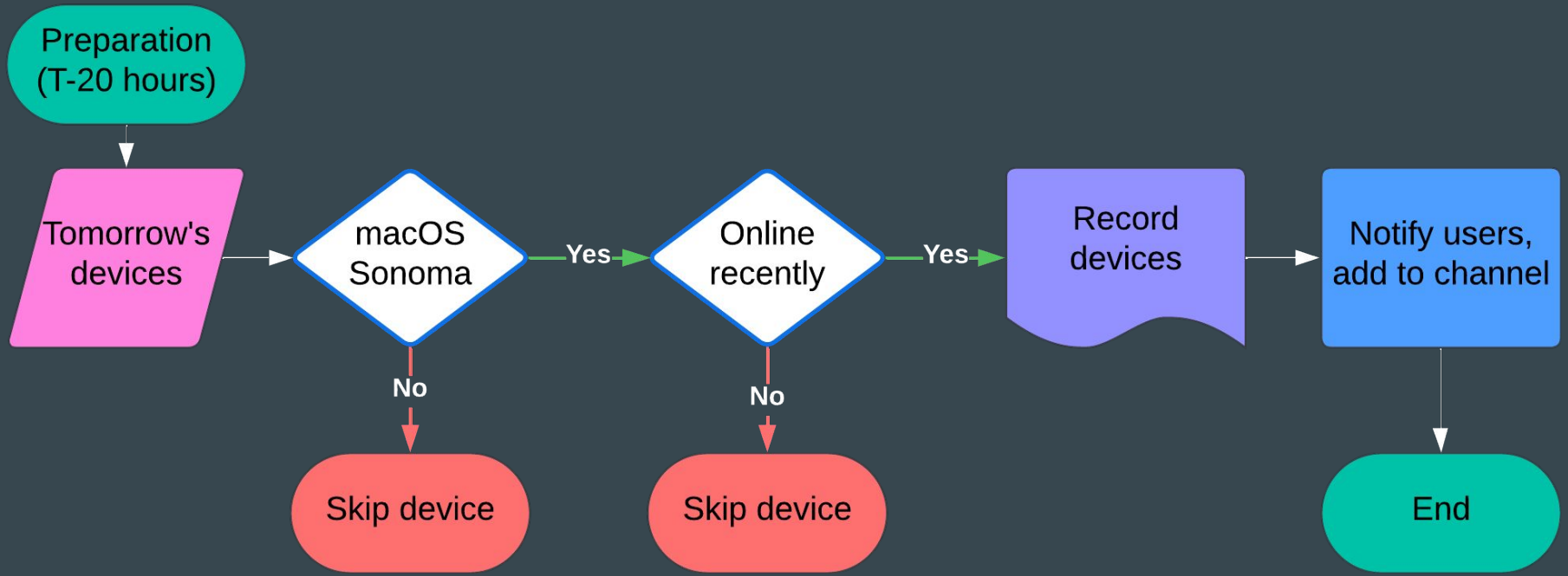
Automating the Process: Planning

- It needed to run unattended on our CI/CD platform using the vendor APIs
- Over 11,000 Macs in old MDM
  - Although only 8,200 migrated due to cycling through the warehouse
- Divided the Macs into 100 random groups
  - Allowed us to control how many computers migrated per day
    - Scale up or down as needed based on support load
  - Avoided entire departments or teams migrating at the same time
- Changed all assignments in ABM as soon as the new MDM was ready
  - This allowed devices shipping from the warehouse to enroll directly to the new MDM without the users needing to go through migration
- Identified devices not in ABM, exempted them the automation and replaced them
  - There were only around 25 devices not in ABM
- Lots of testing!

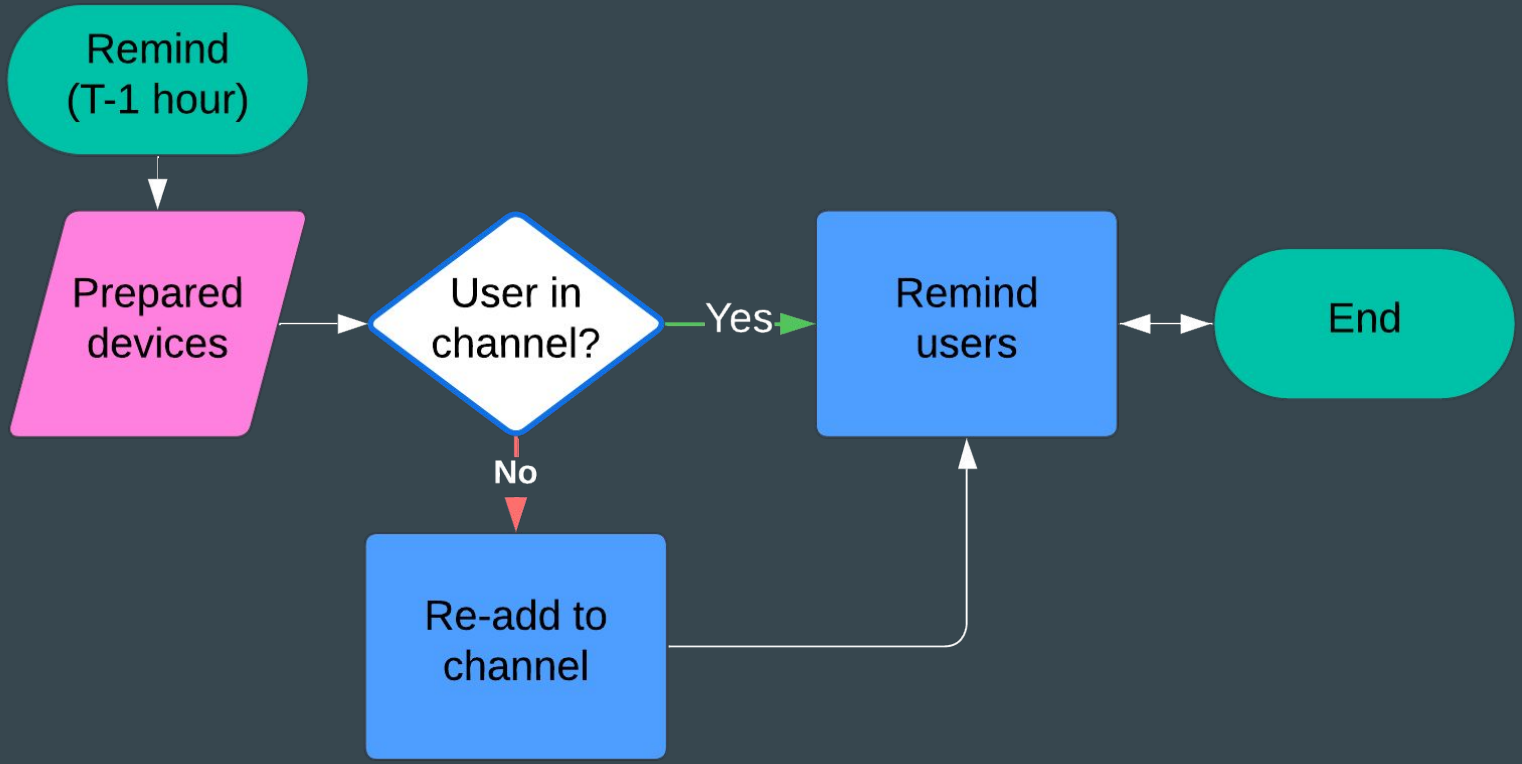
Automating the Process: Upgrade



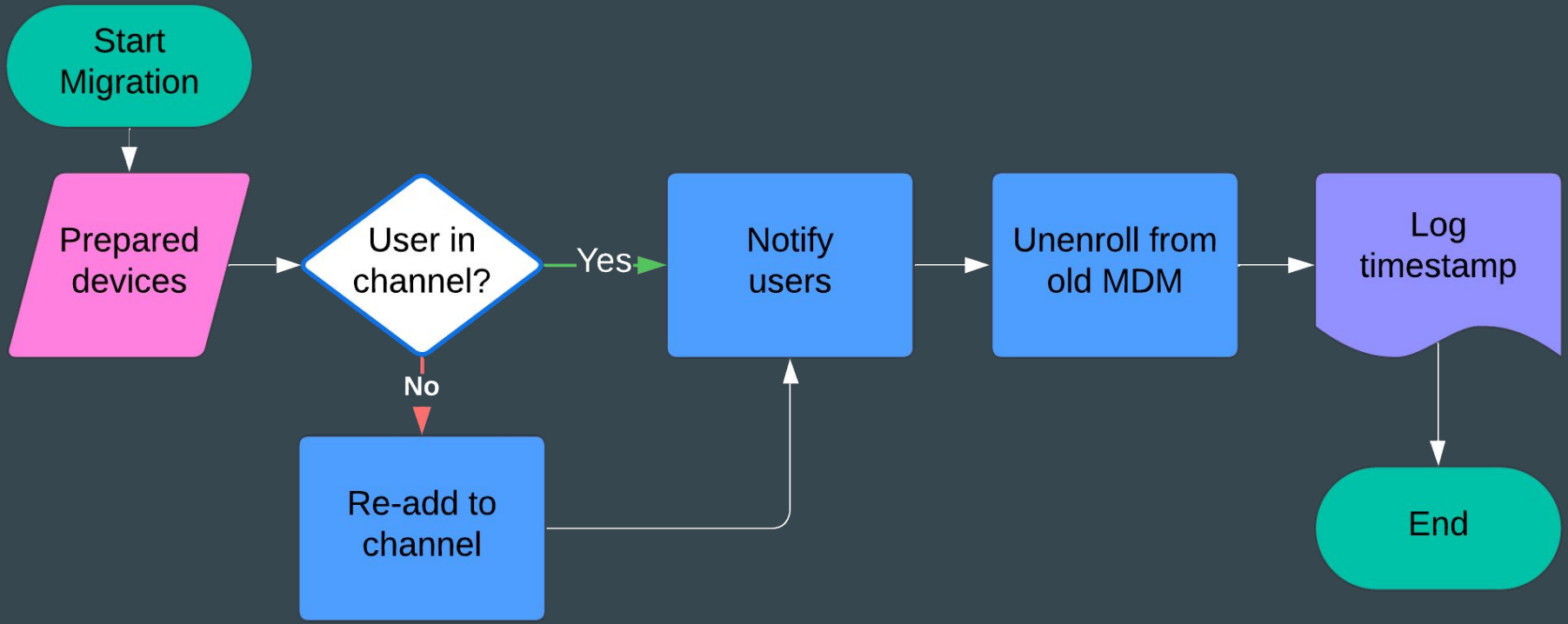
Automating the Process: Preparation



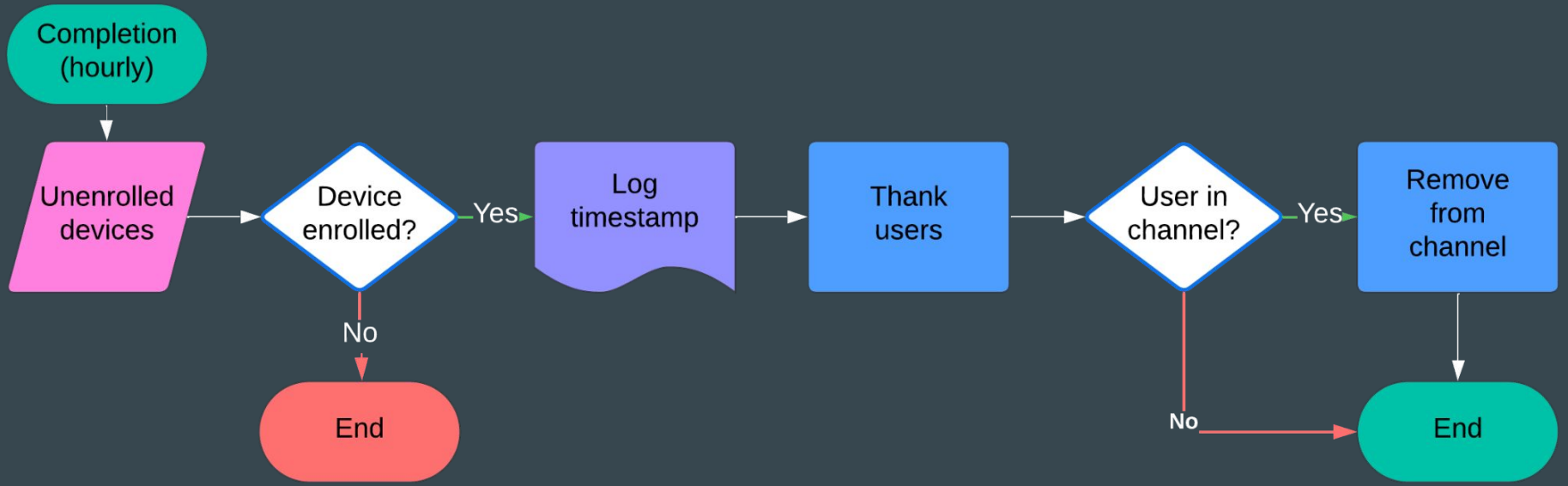
Automating the Process: Remind



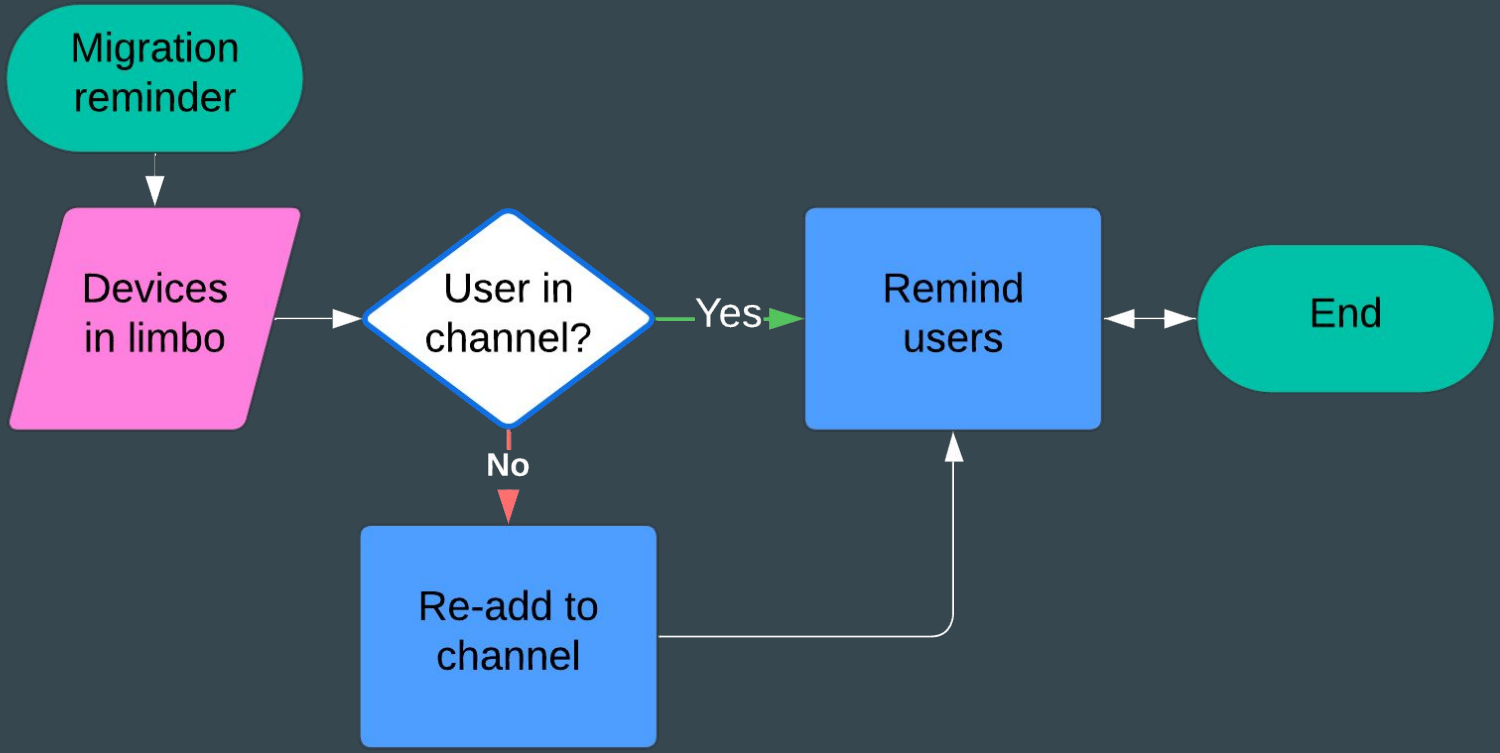
Automating the Process: Start Migration



Automating the Process: Completion



Automating the Process: Follow-up



Results

By the Numbers

100%

Active Devices

By the Numbers

100%

Active Devices

99.13%

Total Devices

By the Numbers

100%

Active Devices

99.13%

Total Devices

93%

Migrated by week 3

By the Numbers

100%

Active Devices

99.13%

Total Devices

93%

Migrated by week 3

129

Manual

By the Numbers

100%

Active Devices

99.13%

Total Devices

93%

Migrated by week 3

129

Manually Processed

12

in Limbo

By the Numbers

100%
Active Devices

99.13%
Total Devices

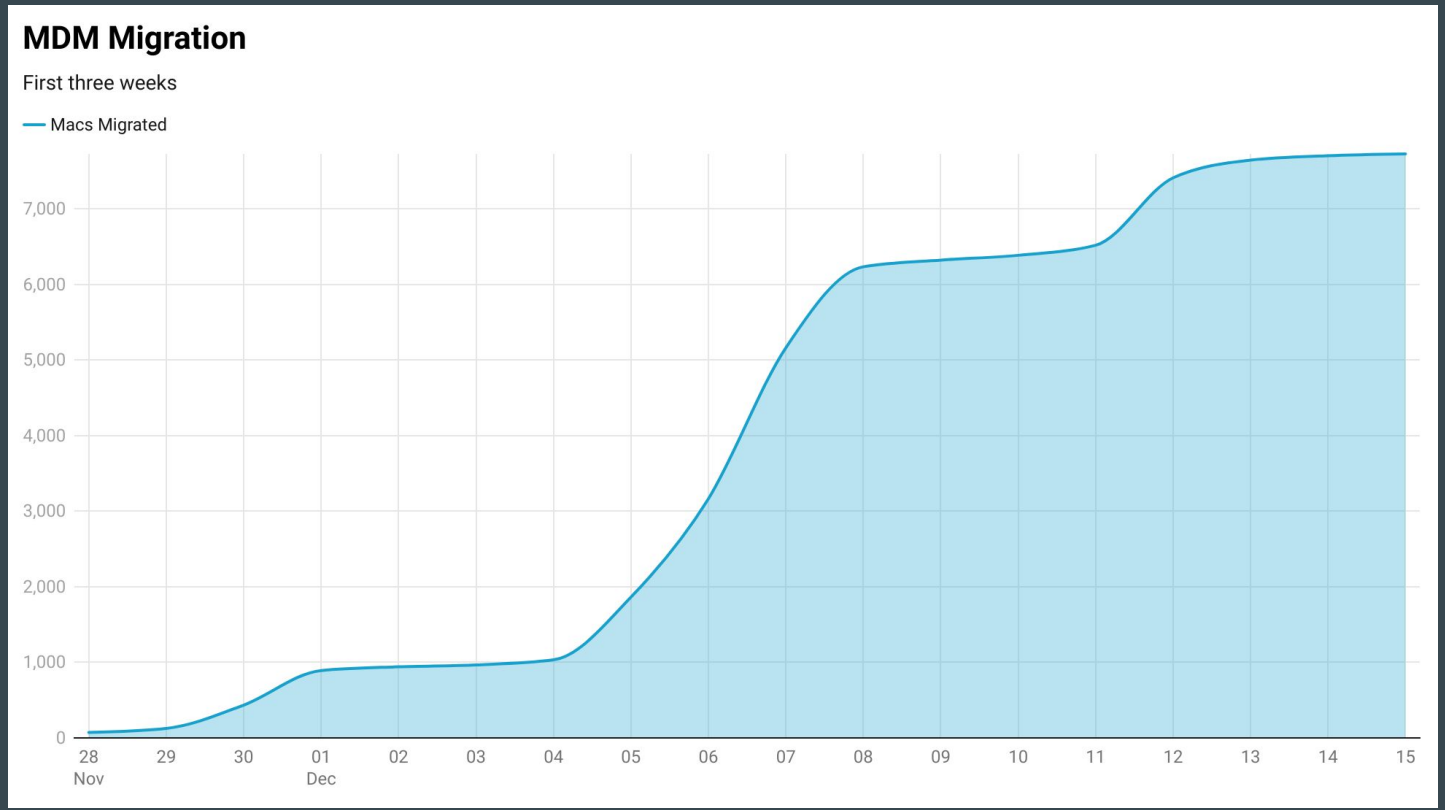
93%
Migrated
by week 3

129
Manually
Processed

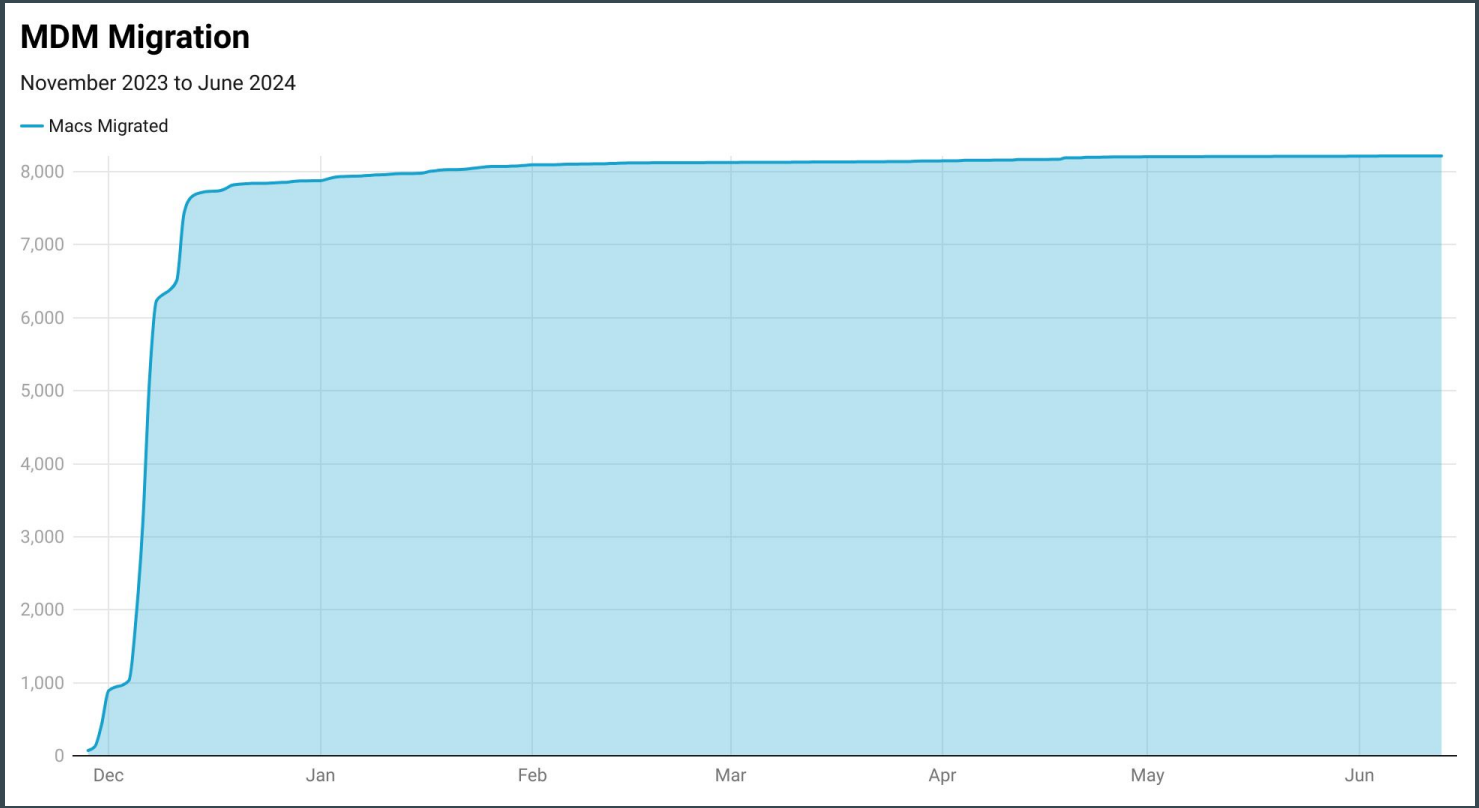
12
in Limbo

1
Angry User

Timeline: First three weeks



Timeline: November 2023 to June 2024



Devices in Limbo

On your mark, get set, go!

Fastest
Enrollment

35

Seconds!

Slow and steady wins the race?

Fastest Enrollment

35

Seconds!

Slowest Enrollment

171

Days

Setting the pace...

Fastest Enrollment

35

Seconds!

Slowest Enrollment

171

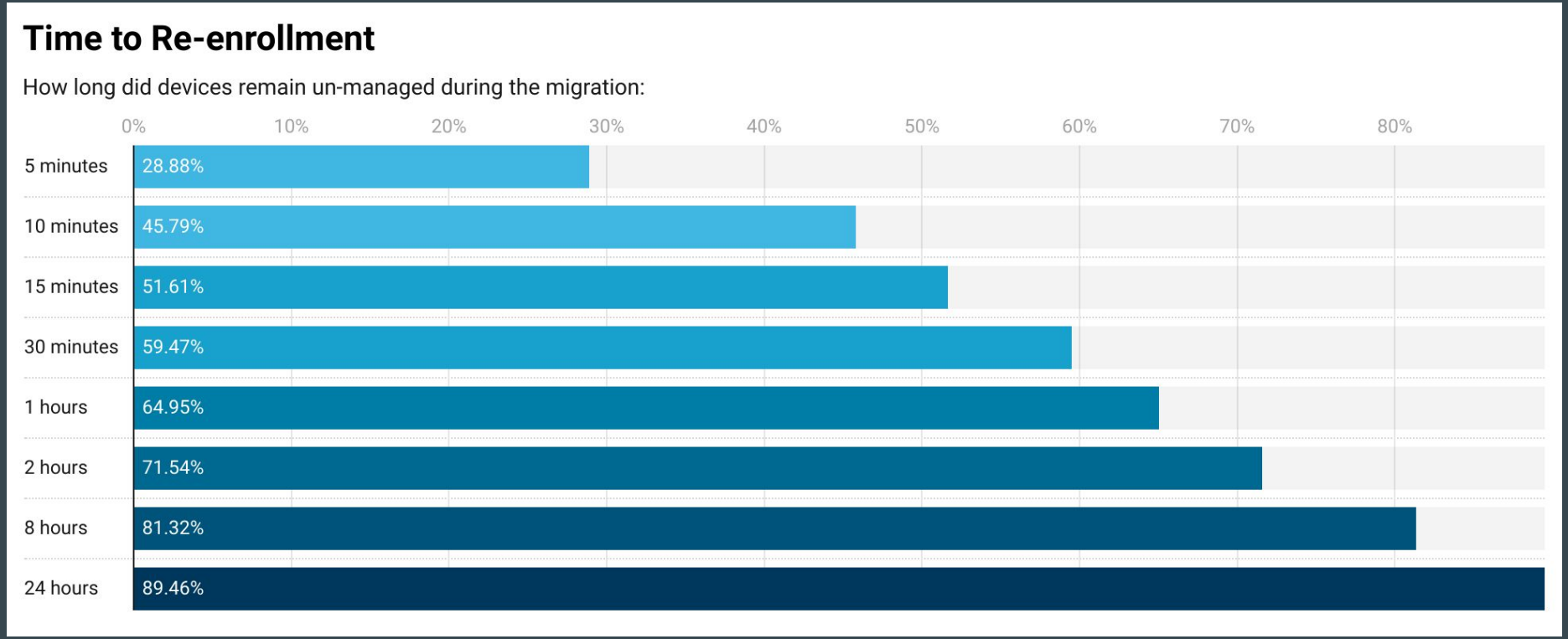
Days

Average Enrollment

24

Hours

Risk Window


Time to Re-enrollment
How long did devices remain un-managed during the migration:
0%
10%
20%
30%
40%
50%
60%
70%
80%
5 minutes
28.88%
10 minutes
45.79%
15 minutes
51.61%
30 minutes
59.47%
1 hours
64.95%
2 hours
71.54%
8 hours
81.32%
24 hours
89.46%

User Feedback

User feedback

- “This feels like one of the most supported tech-rollouts I’ve seen in my 2.5 years at DoorDash.”
- “Omg that was so fast! thank you!”
- “Just want to appreciate the lean IT support servicing a 2500+ person slack channel. 🫡”
- “For everyone worried: my computer just did it and took like a minute. My computer didn’t restart and my zoom call was still in progress.”
- A huge thanks to the IT team for coordinating this and providing us with info. No easy task 👏”
- “Just wanted to say how seamless of a process it was for me to do my device transition with your instructions. Thank you for all you do!!”

User feedback

- “Who on your team is the PM or lead behind the transition? Whoever it is has done a terrific job with the comms (look and feel), the planning, the forced transition plan, etc!”
- “It was unbelievably smooth. It was super painless on my end, so really appreciated the effort!”
- “I’m in! Thank you! So fast!”
- “Nice, quick and easy, appreciate it!”
- “Went through the process and it worked perfectly.”
- “It was super simple, and the FAQs were really helpful 🙂”

Lessons Learned

What worked well?

- Support from leadership
  - Knowing the what/why/when prepared leadership to intercede in case of problems (thankfully not needed)
- Service Desk assistance
  - Having front-line IT support in the loop allowed them to handle routine aspects, freeing CPE to focus on the overall process
  - This included our Executive Support lead who went above and beyond
- Allies
  - Allies outside of IT who shared their experience went a long way to setting the tone
- Communication
  - The vast majority of users were not surprised and directed those who were to documentation
- Forced schedule
  - While some were skeptical at first, it really helped keep things on track

What didn’t work?

- Letting users self manage their migration
  - iPhones and iPads require a wipe to migrate MDMs, so we took a different approach with these users
  - We provided instructions, a dedicated Slack channel for assistance and a deadline to complete the process
  - Only 26% of users had completed the process by the deadline
  - Only 87% had completed the process by the time our old MDM contract expired
- Unclear communication with secondary stakeholders
  - We didn’t set clear expectations with all of our cross functional partners which lead to some confusion and a little conflict I wish we had avoided

What could we have done better?

- Communicate via both Slack and email
  - We focused on communicating via Slack because most employees don't check email often
  - There are always outliers and a few folks, including the one angry user, said email would have been more effective for them
- Start sooner
  - We should have started on the technical components sooner
  - Since renewing with our existing vendor was a real possibility, I think we waited longer than we should have to begin building the automation process

Planning an MDM Migration

Define the Goal

 What is the goal of switching MDM vendors?

- Saving money?
- Gaining features?
- Better support?

Make sure to define clear goals before beginning your RFP!

Outline the Schedule

🗓️ Outline the schedule

- Evaluate outside factors like upcoming contract expiration
  - Do you have a required notification period with the current vendor?
  - Can you go month-to-month if needed?
- Be realistic; under promise, over deliver
- Take other projects into account
  - What else might require your team's attention?
  - What are your other stakeholders working on?
- Be prepared for the timeline to change

Conduct an RFP

📑 How does the RFP process work at your organization?

- Is there a formal process or is it more casual?
- Is there a specific template you need to use?
- Who needs to be involved?
- Are there a minimum number of vendors that must be included?
- How long does the process typically take?
- Can you initiate contact with vendors or does someone else need to do that?
- Who can sign the contract?

✍️ Craft the RFP

- Really think about what features are must-have and which are only nice-to-have
- What are the long term consequences of losing a feature you have now
- Get the input of other teams
    - But be clear about how much influence they will have on the final decision
- Map out all dependencies and integrations
- Use very specific language

🔎 Evaluating proposals

- Compare notes with other internal stakeholders
- Trust but verify
- Talk to the MacAdmins community
- Ask to speak to other current customers
- Ask the hard questions

🔽 Narrow it down

- Schedule demos to go more in-depth on the written responses
  - Ask the hard questions!
- Ask for live evaluation tenants to get your hands dirty
  - Replicate real world workflows and scenarios
  - Test the features the vendor says they support
- Take your time

🎗 Remember

- Nobody pays list price
  - Negotiate volume discounts
- There are no perfect platforms
  - You'll have to sacrifice *something* no matter who you choose
- Your don't have to migrate!
  - Deciding the grass isn't greener is a valid end result
- Make sure everything is important is in the contract
  - Promises from sales calls don't matter if they aren't in the contract

Building the New Tenant

🏗️ Building the new tenant

- Start fresh; this is a great opportunity to audit your existing setup
  - Only include the things you need going forward
  - Change things you always hated about your existing setup
- Keep the live evaluation tenant around as your sandbox
  - Make sure this is in your contract
- Build and test everything in the sandbox
  - Test SSO setup and configuration
  - Make sure integrations work
  - Validate API differences for automations
- Don’t configure the production environment until testing is complete

🛠️ Building the new tenant: other considerations

- Third party app deployment and patching
  - If you used the MDM for this, can you seamlessly transition?
- FileVault key escrow
  - If you escrow to MDM Apple has this covered, but also check out Escrow Buddy just in case
    - github.com/macadmins/escrow-buddy
- Custom configuration profiles
  - Some vendors use a full .mobileconfig while others only need the payload XML
- Reporting
  - Is anyone depending on custom reports generated by your old MDM?

💡 Building the new tenant: Tips

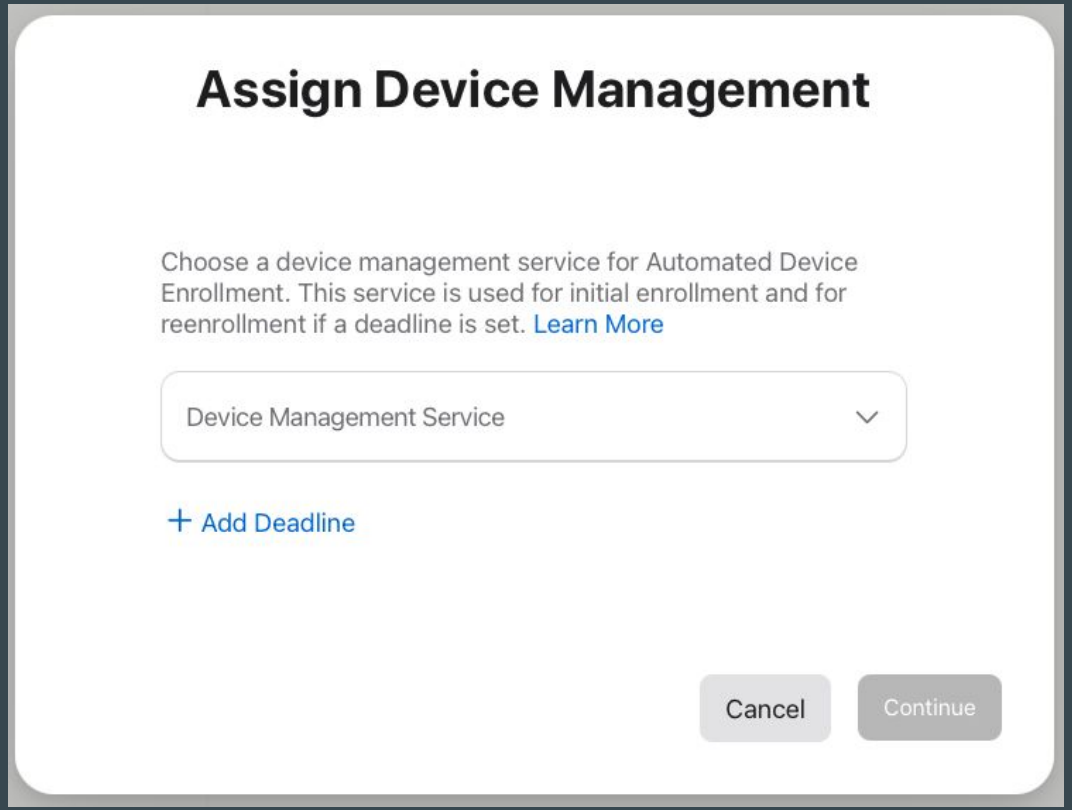
- Avoid the GUI for configuration profiles
  - MDM interfaces are notorious for including configurations you didn't intend
  - Custom configuration profiles allow you to be fully in control
  - Unfortunately this isn't possible for everything, like DDM declarations
- Decouple as much as possible from MDM
  - By using standalone systems you reduce the number of variables in an MDM migration
  - There are likely free open source tools that do a better job for many things
    - Munki / AutoPkg for app deployment and patching
    - Crypt for FileVault key escrow
    - MunkiReport or Sal for reporting

Easy Button

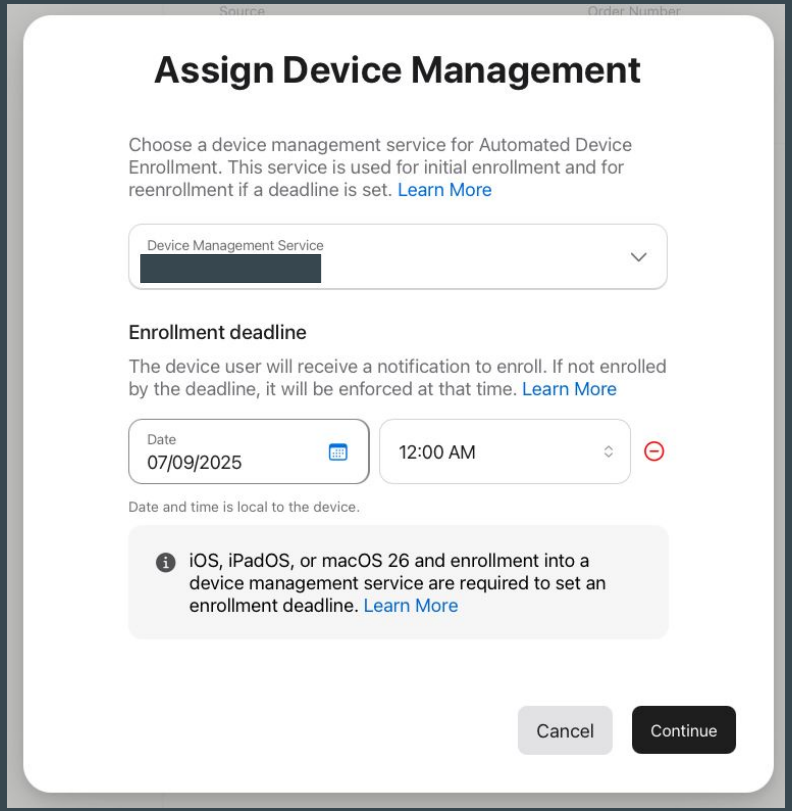
✅ Easy Mode: Requirements

- macOS 26 (still in beta, start testing now and file feedback!)
- Macs must be in Apple Business Manager / Apple School Manager
- Macs must be currently enrolled in an MDM via Automated Device Enrollment
- If the Mac has a “managed user” that is who must complete the migration
  - If there is not a “managed user” then any user can complete the process
  - Identifying MDM-managed user accounts on macOS Sequoia
    - https://derflounder.wordpress.com/2025/04/04/identifying-mdm-managed-user-accounts-on-macos-sequoia/
- Official documentation:
  - https://support.apple.com/guide/deployment/migrate-managed-devices-dep4acb2aa44/web

✅ Easy Mode: ABM/ASM



✅ Easy Mode: ABM/ASM



✅ Easy Mode: ABM/ASM

MacBook Air

Device Management Service Assigned

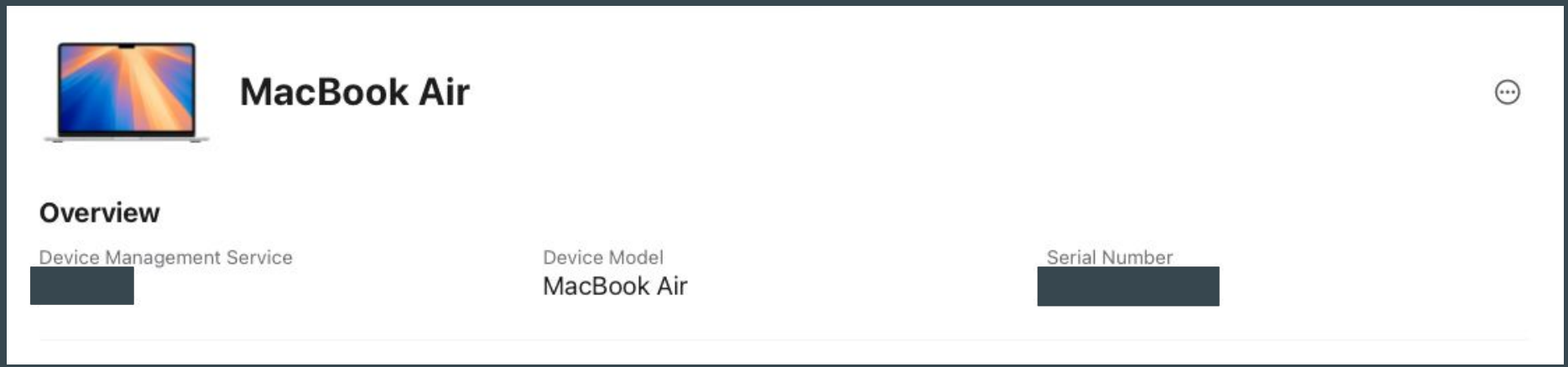
Management of this device has been assigned to Mosyle with an enrollment deadline of July 10, 2025 at 12:00 AM.

Change Deadline

Overview

Device Management Service	Device Model	Serial Number
[redacted]	MacBook Air	[redacted]

✅ Easy Mode: ABM/ASM



✅ Easy Mode: macOS

- On device the dialogs looks very similar to what we are used to starting with macOS 14
- After the migration deadline is set, users receive notifications to confirm reenrollment, with more frequent notifications leading up to the deadline.
- Notifications are displayed daily, and hourly 24 hours before the deadline.
- For the last hour before the deadline, the user is notified at sixty, thirty, ten and one minute.

Not so Easy Button

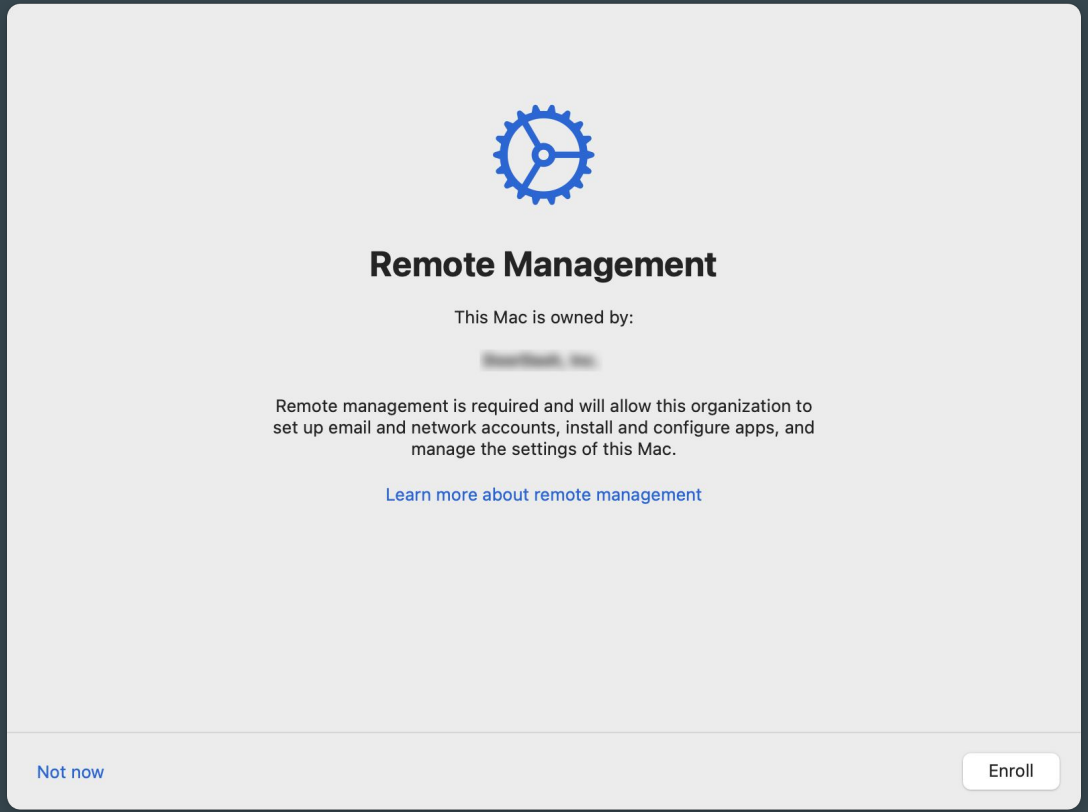
⛔ Not so Easy Mode

- You can’t wait until macOS 26 is released to migrate
- Even after release you have devices that you can’t upgrade to macOS 26
- You have Macs that are not in Apple Business Manager / Apple School Manager
- You have Macs that are manually enrolled in MDM
- Other scenarios that haven’t been discovered yet (start testing macOS 26 today!)

🟡 Not so Easy Mode: macOS 14 in ABM/ASM

- If you can’t wait for or utilize macOS 26 for whatever reason
- Your Macs are in Apple Business Manager / Apple School Manager
- Your Macs are running at least macOS 14 Sonoma
    - You can still take advantage of of the full screen dialog and eight hour deadline
    - You’ll only need to deploy a script and LaunchDaemon

Not so Easy Mode: macOS 14 in ABM/ASM

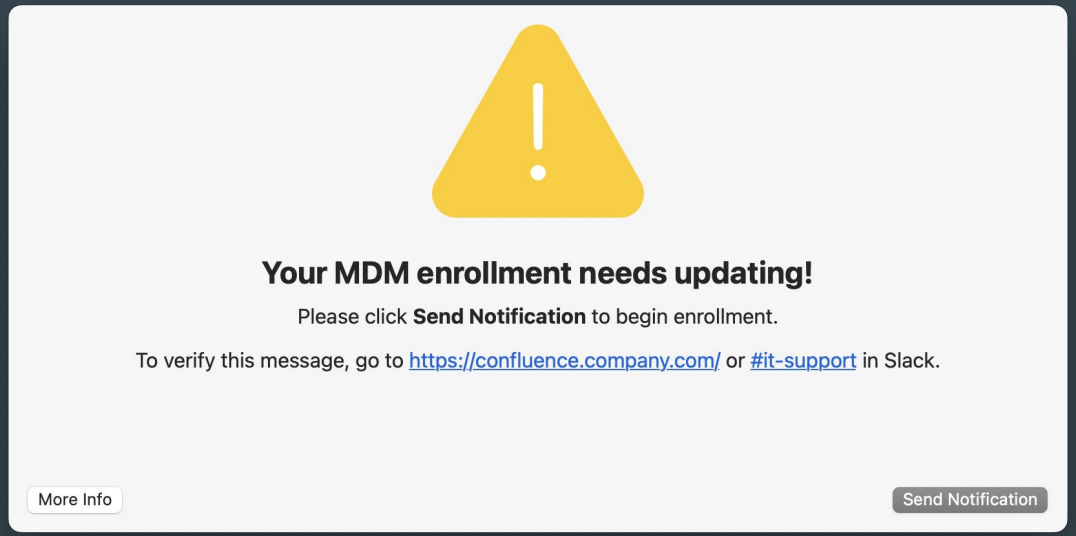


🔴 Not so Easy Mode: No ABM; older macOS; manual enrollment

- If you have Macs that are not in Apple Business Manager / Apple School Manager
- Are manually enrolled in MDM
- Are running macOS 13 or older
- You will need to develop and deploy an on-device GUI to guide users through migration

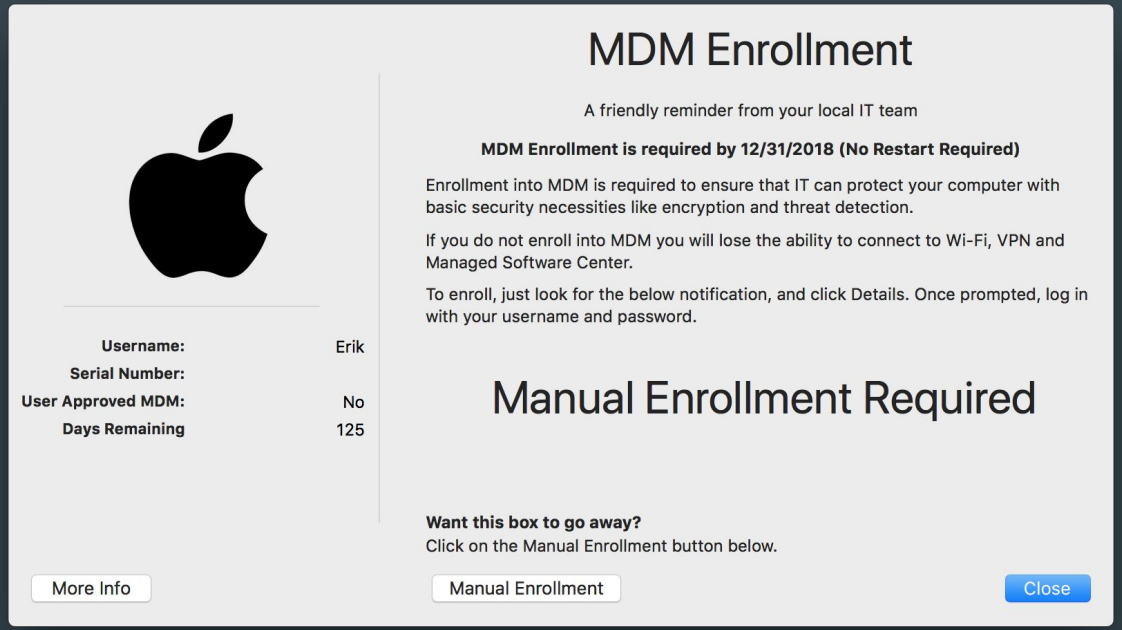
swiftDialog

- IMO, the logical choice if you don't want to develop your own native app



https://github.com/swiftDialog

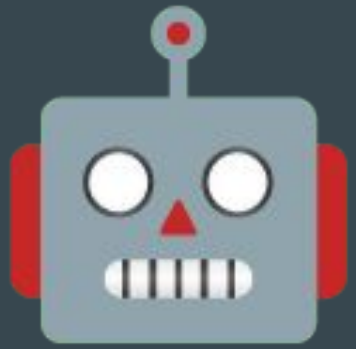
UMAD: Universal MDM Approval Dialog



https://github.com/macadmins/umad

⬆️ Level Up macOS 14 and 15 migrations

- You can combine the two methods mentioned above if you want to “Level Up” MDM migrations of macOS 14 and 15
- Rather than forcing users to migrate on a strict schedule as we did last year, you can empower them to migrate on their own schedule, triggering unenrollment on demand and ensuring the native macOS deadline starts immediately



Automation

🤖 Automation

- If you are Living the Dream with macOS 26, there isn't anything you can automate yet
  - The ABM / ASM API doesn't support setting a deadline for MDM migrations
- If you are using the macOS 14/15 migration method you can look to automate the unenrollment of devices from the old MDM
- Either way, automate your reporting

Test, test, test!

🧪 Test, test, test!

- You should be absolutely sick of moving Macs between MDMs when done
  - Look for edge cases and think about worst case scenarios
- Make sure integrations and automations are interfacing with both the old and new MDM during the migration
- Ask other members of IT to participate in the testing, especially service desk
- Find allies in other departments to go through the process and provide feedback
  - Look for both tech-savy and non-technical users to provide feedback
  - Don’t make assumptions about how easy or hard the process will be for them
- Consider both remote and in-office employees
- Demonstrate the process for leadership and make sure they are comfortable

Communicate

🗣️ Communication

- Utilize your internal communications department if available
- Meet users where they are: Slack, Email, etc.
- Provide detailed documentation and FAQs
    - Don’t forget prompts users may get during their time in limbo
- Outline a clear timeline for the migration
- Explain not only what is happening, but why
- Make it easy for end users to ask questions and get help

Go time!

🚀 Go time!

- Change default assignments in ABM / ASM to the new MDM as soon as the production tenant is ready
    - This avoids making new hires go through the migration
- Reassign all devices in ABM / ASM to the new MDM (setting a deadline for macOS 26)
- Kick off any automations that will facilitate the migration (for older Macs)
- Be ready to provide support

Measure Results

📊 Measure results

- How many devices migrated per day?
- How long did devices remain unenrolled?
- How many users required support to complete the migration?
- What other metrics will your leadership want measured?

Wrap Up

🏁 Wrap up

- Disable any integrations or automations still accessing the old MDM
- Remove the old MDM from ABM / ASM
- Make sure to close out your old MDM and stop billing
    - Don’t assume this will happen automatically
    - Formally request the old vendor to delete the tenant and customer data
- Report your successful migration to leadership!

Keys to Success

🔑 Keys to Success

- Communication
- Support from leadership
- Service Desk participation
- Allies outside of IT
- Firm deadlines
- Focus on the user experience
- Remember you can’t make everyone happy

Mergers and Acquisitions

🤝 Mergers and Acquisitions

- M&A is driving all of our upcoming MDM migrations
- We are executing one in the next month
- We’re planning for another later this year
- We anticipate a third in early 2026
- So M&A MDM migration is a scenario I’ve been thinking about a lot lately

🤝 Mergers and Acquisitions: differences

- The goals and problems to solve are different
- You might not control the timeline
- You may be blocked by other transitions and migrations that must complete first
- Responsibilities might be unclear during the confusion of an M&A

🤝 Mergers and Acquisitions: things to consider

- Things to consider:
  - Security software / EDR
  - Third party app deployment and patching
  - FileVault key escrow
  - Configuration differences
  - Device Trust / Conditional Access
  - Admin vs. standard user accounts
  - Hidden admin accounts
  - Authentication for MDM enrollment (IDP accounts)
- Most importantly, remember to approach all of this with empathy!
  - These are your new co-workers and teammates; they might be nervous about being acquired so you don’t want to make a bad first impression

🤝 Mergers and Acquisitions: our plan

- We're planning to use the "Level Up" method with swiftDialog for now
  - The first migration has to happen on macOS 15
  - The second migration involves devices not in ABM and manually enrolled
- Our on-device GUI utilizes swiftDialog, is powered by Bash, a LaunchDaemon, configuration profile and a remote automation server to process unenrollments when triggered while logging it all
  - It will allow us to enforce a deadline
  - Allow end users to migrate on their schedule anytime before the deadline
  - Will be adaptable for both ADE and manual enrollment scenarios

When to start planning?

Yesterday!

Questions?

Thank you!