



MacDevOps:YVR
June 20, 2024

Migrate MDM servers with this one simple trick!



MacDevOps:YVR
June 20, 2024

MDM Migration with macOS Sonoma



Kevin M. Cox

Staff Client Platform Engineer 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 (which is most companies)
- The potential for disruption prevents companies from changing vendors when they want to (in my opinion)
- Minimizing this disruption is the primary goal

Historically, re-enrollment is not intuitive

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

- The “DEP nag” was easily missed



Device Enrollment

XXXXXXXXXX, INC. can automatically configure your Mac.

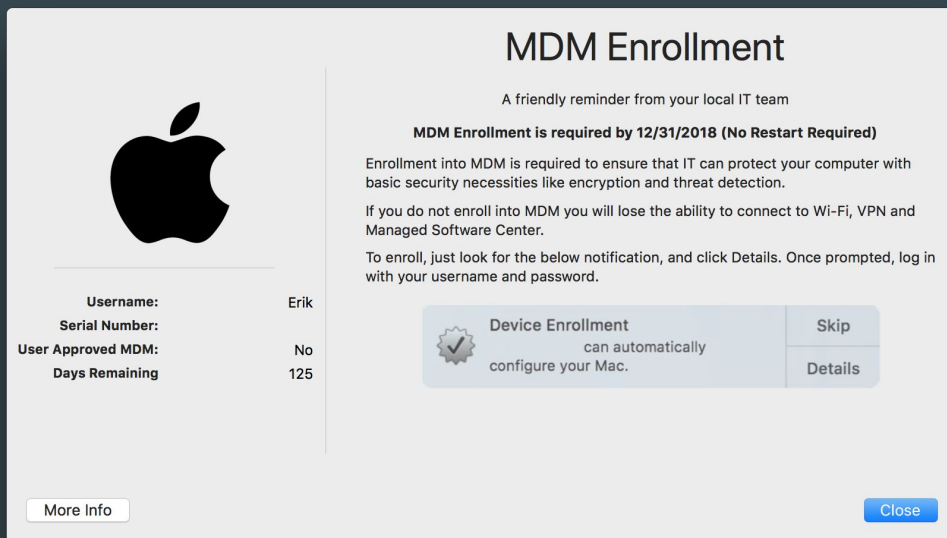
- Users could ignore it indefinitely
- There was no native ability to force re-enrollment



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

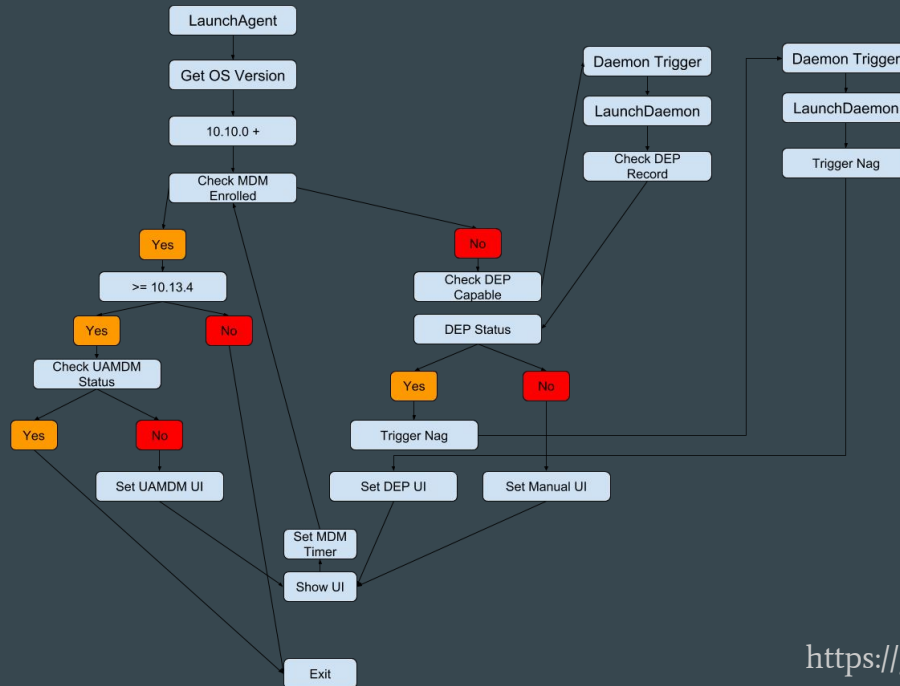
UMAD: Universal MDM Approval Dialog

- Five years ago Erik Gomez looked to help solve this problem by writing UMAD



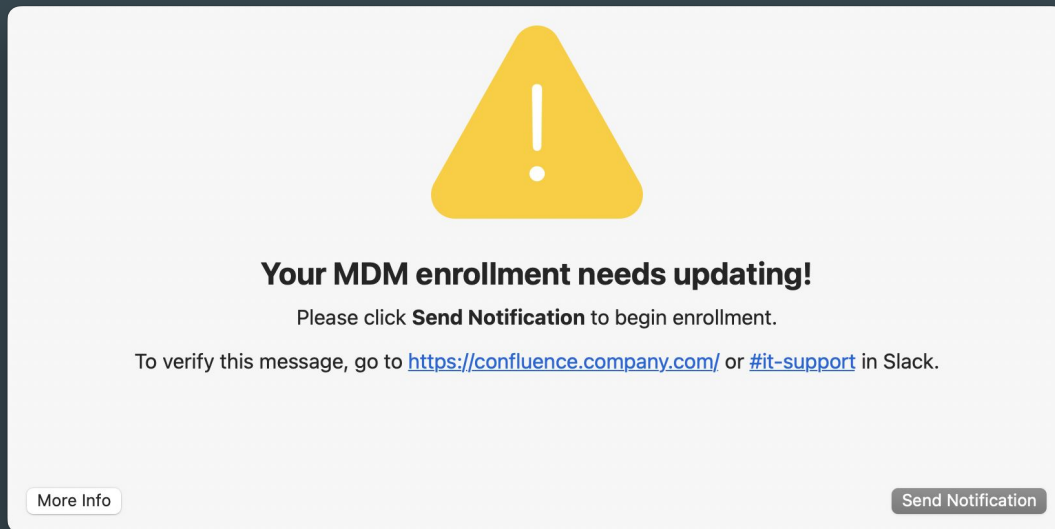
UMAD: Universal MDM Approval Dialog

- UMAD has logic to check for MDM enrollment and trigger a dialog if needed



Other options

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



Other options

- 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.”

Enforce Automated Device Enrollment

“For a Mac registered with Apple School Manager, Apple Business Manager, or Apple Business Essentials, the notification that requests the user enroll in MDM is replaced with a full screen Setup Assistant experience.

“The user can then chose "Not now" once, which causes the screen to be dismissed for 8 hours.

“After the time expires, the user is required to perform the enrollment or erase their Mac. During this time, the user sees a follow-up option in System Settings to start the enrollment even before the dismissal expires.”

This changes everything

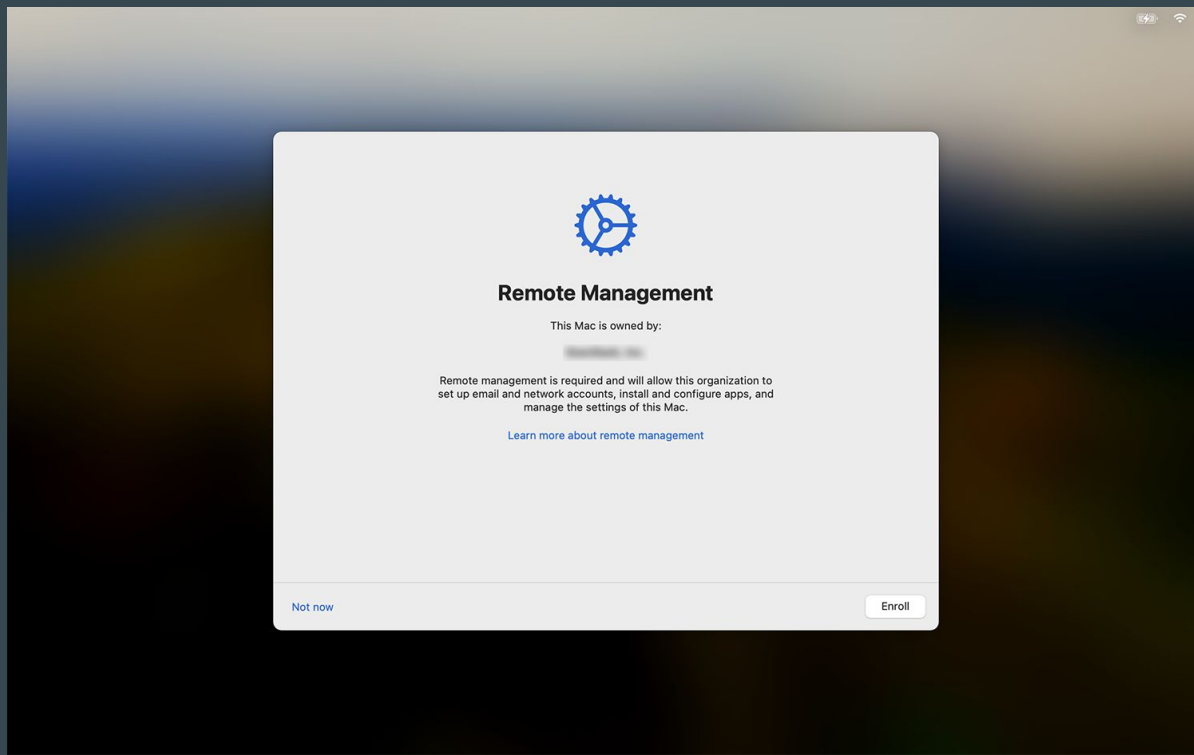
- Our team immediately saw the potential for this new macOS feature to drive our migration experience
- I tested it extensively and opened cases with Apple during the macOS beta cycle
- By the time macOS 14.0 released in September 2023 we were confident we could utilize it as the user-facing part of our migration

Retroactive Automated Device Enrollment

<https://www.kevinmcox.com/2023/09/retroactive-automated-device-enrollment-in-macos-sonoma/>

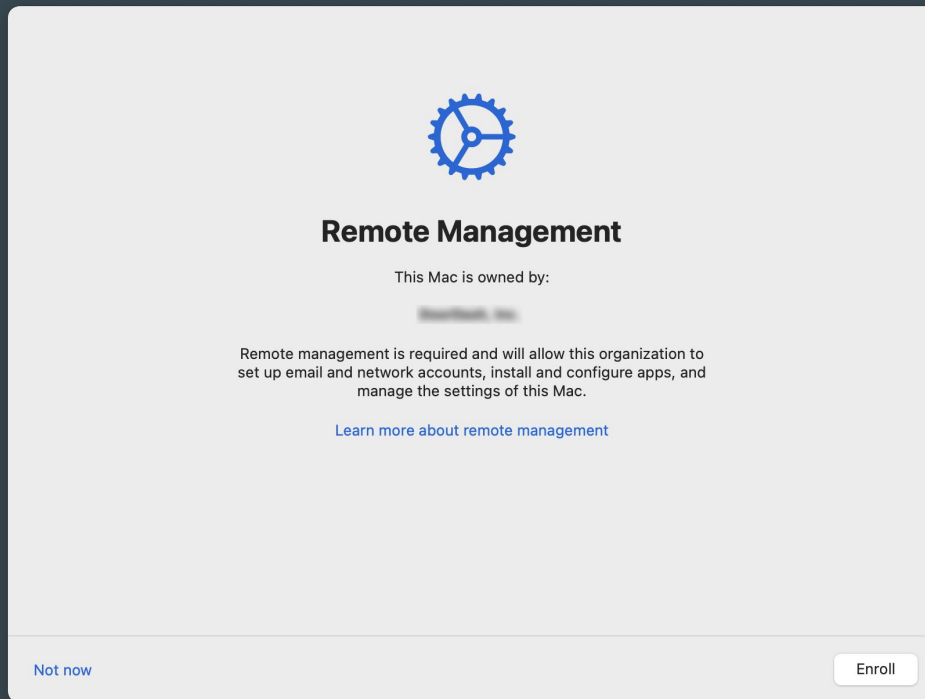
Native experience

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



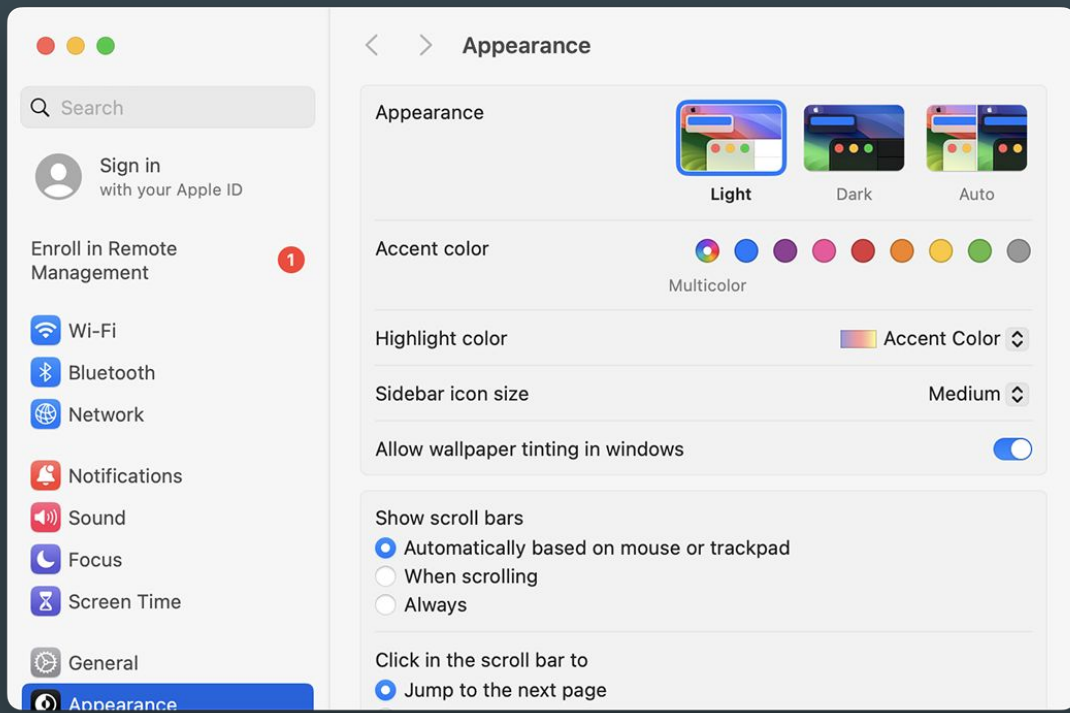
Native experience

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



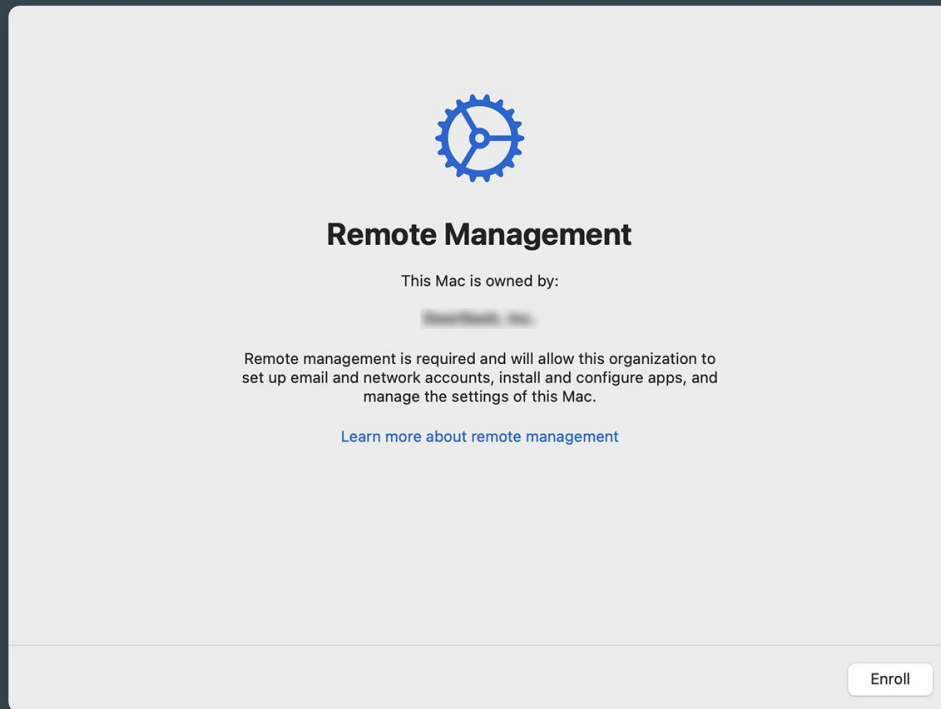
Native experience

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



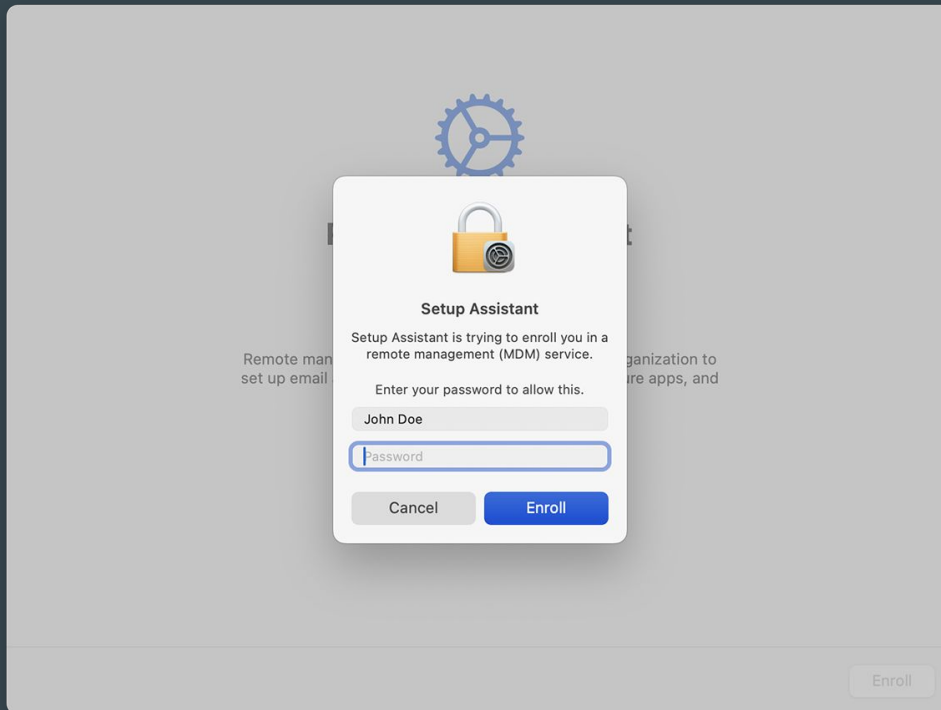
Native experience

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



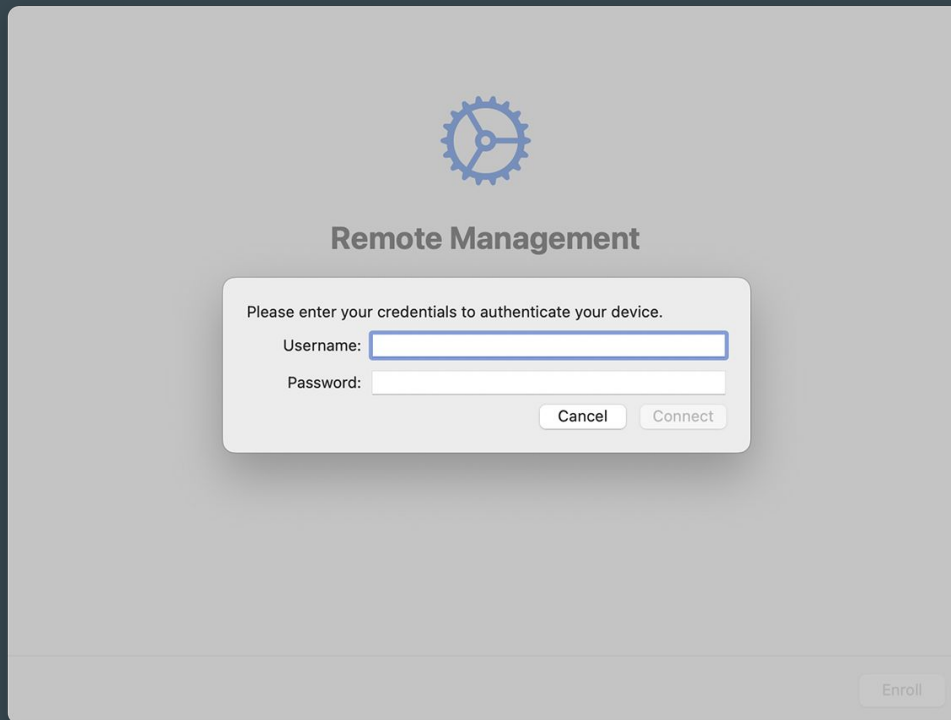
Native experience

- In macOS 14 😊, users are still required to be local admins...




Native experience

- If you require authentication for ADE enrollment that comes next



The image shows a macOS-style dialog box titled "Remote Management". At the top center is a blue gear icon. Below the icon, the title "Remote Management" is displayed in a bold, dark font. The main content of the dialog is a white rounded rectangle containing the text "Please enter your credentials to authenticate your device." followed by two input fields: "Username:" and "Password:". The "Username:" field has a blue border, while the "Password:" field is a simple white box. At the bottom right of this white box are two buttons: "Cancel" and "Connect". In the bottom right corner of the entire dialog window, there is a faint "Enroll" button.



Remote Management

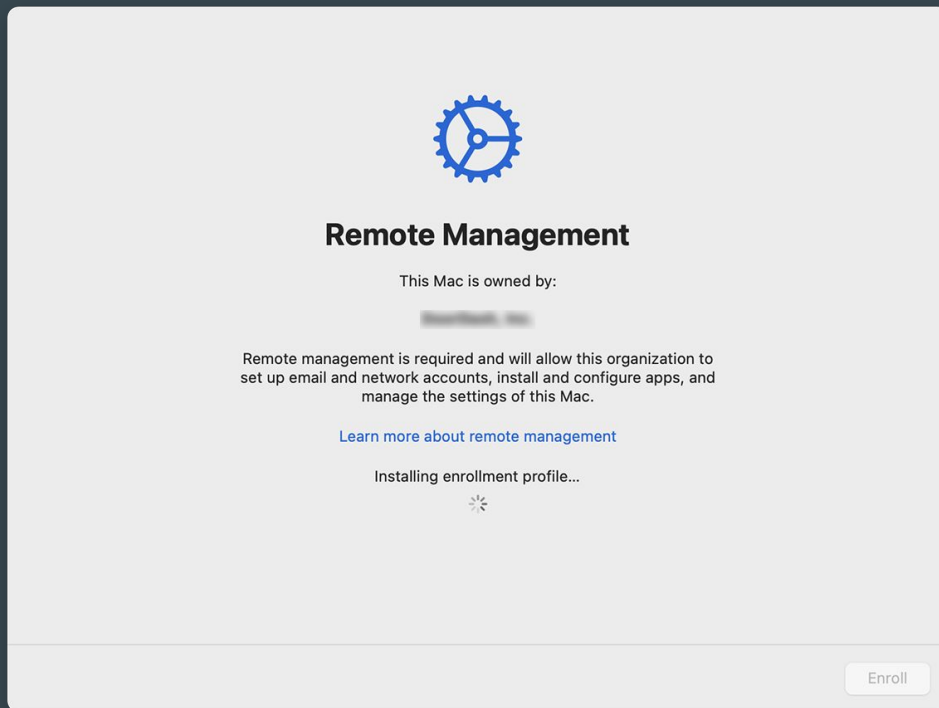
Please enter your credentials to authenticate your device.

Username:

Password:

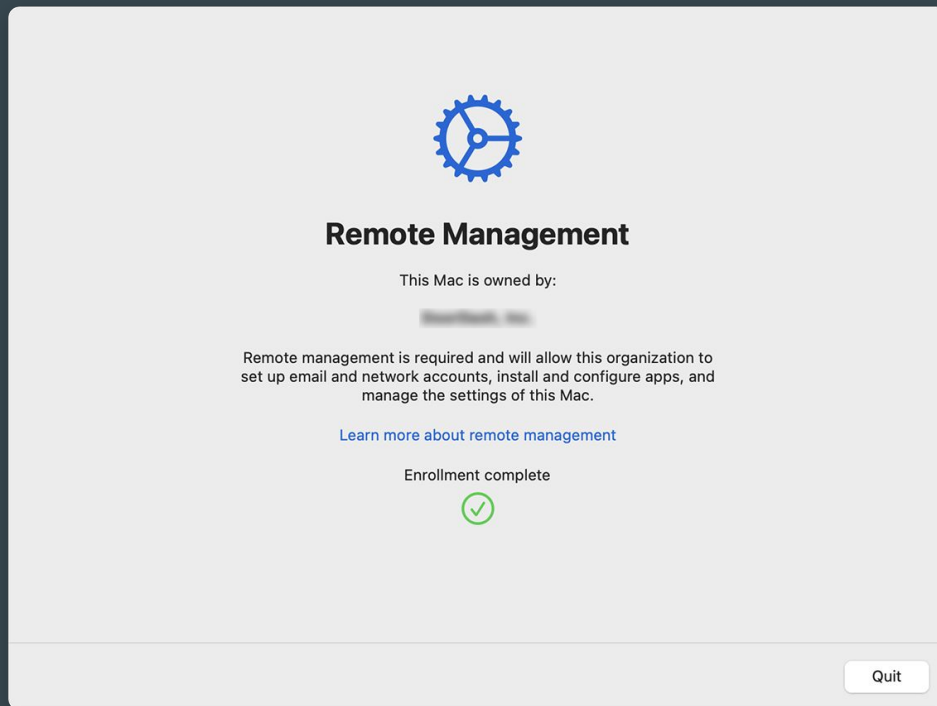
Native experience

- 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 trying to mix a custom UI with the new built-in dialog and solve the security concern wasn't worth the effort

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

Our MDM Migration Process

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

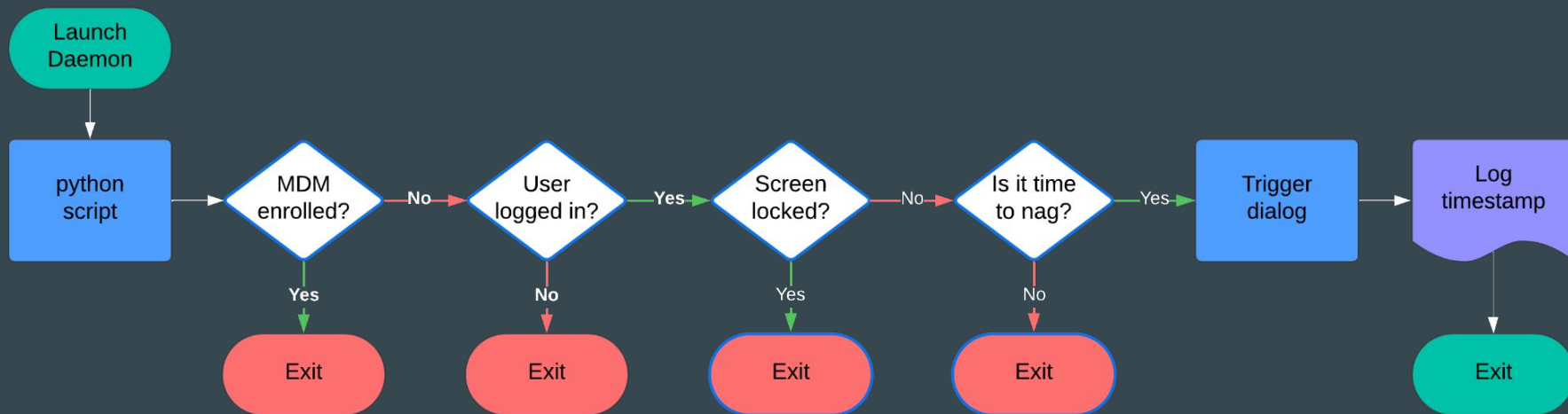
On-device deployment

- 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!

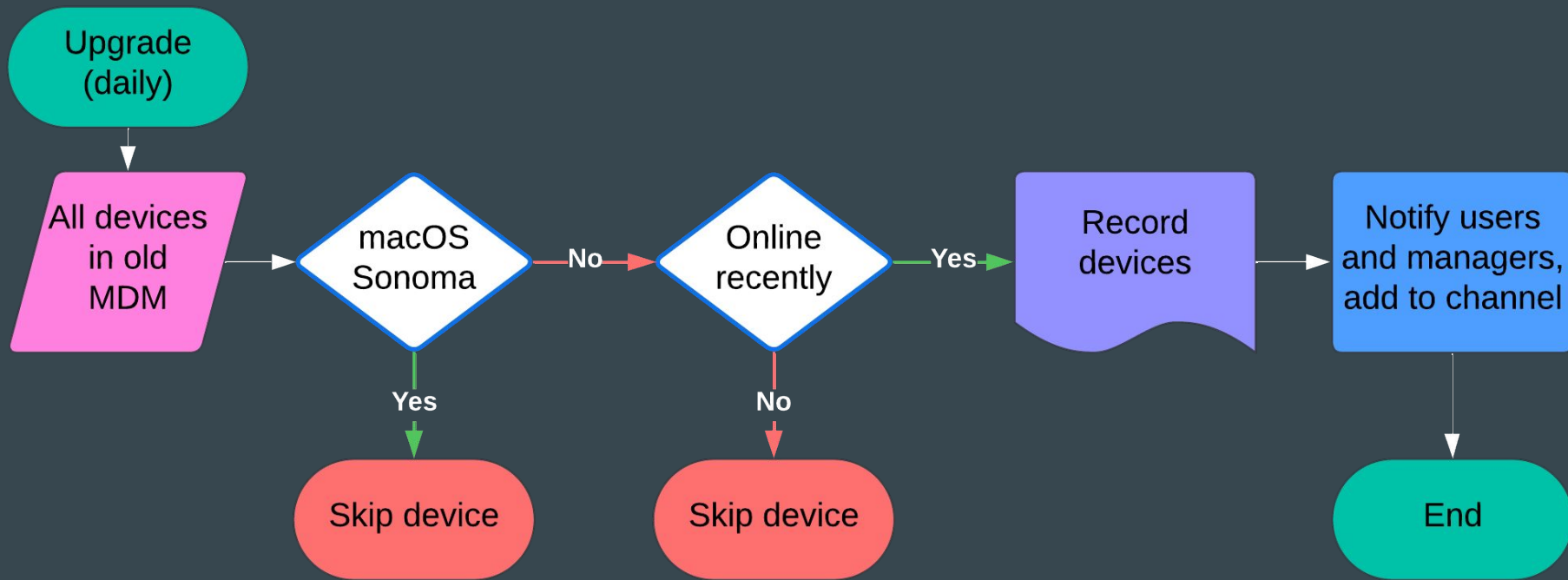
On-device logic



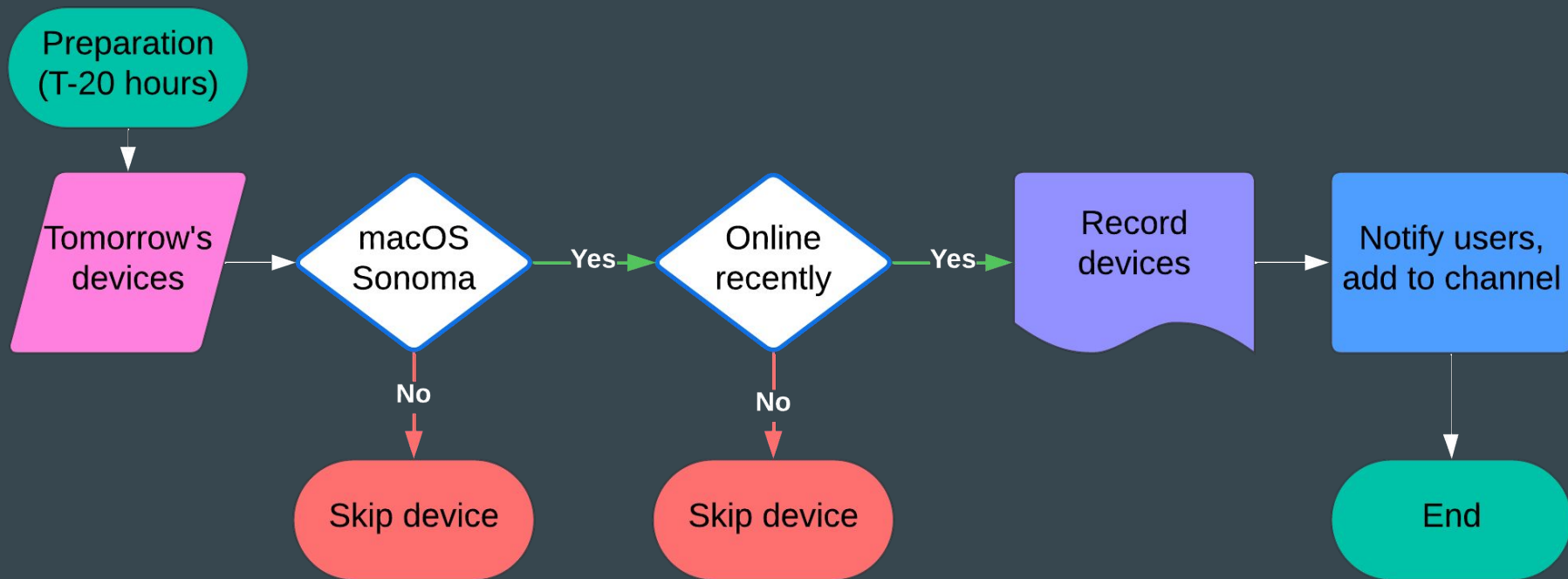
Automating the Process: Planning

- 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!

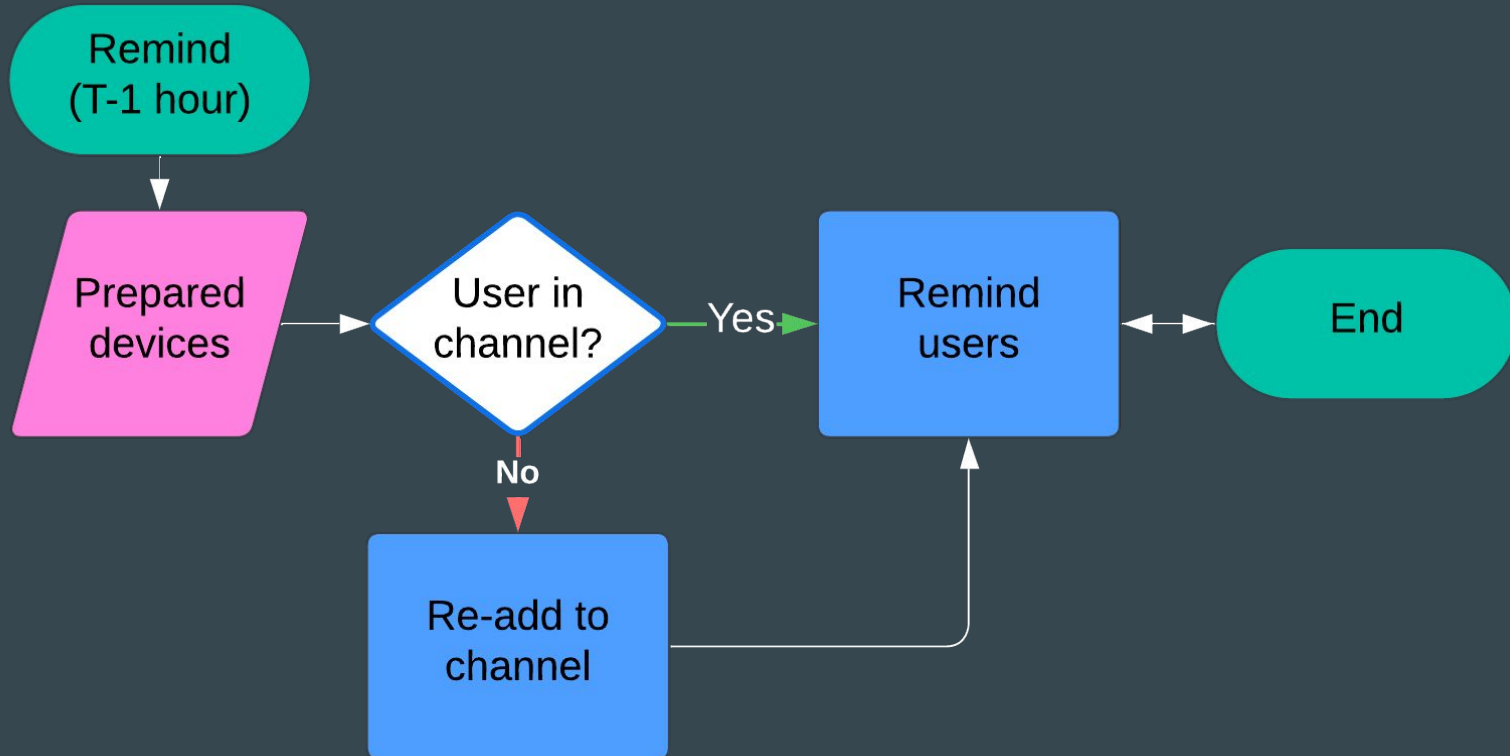
Automating the Process: Upgrade



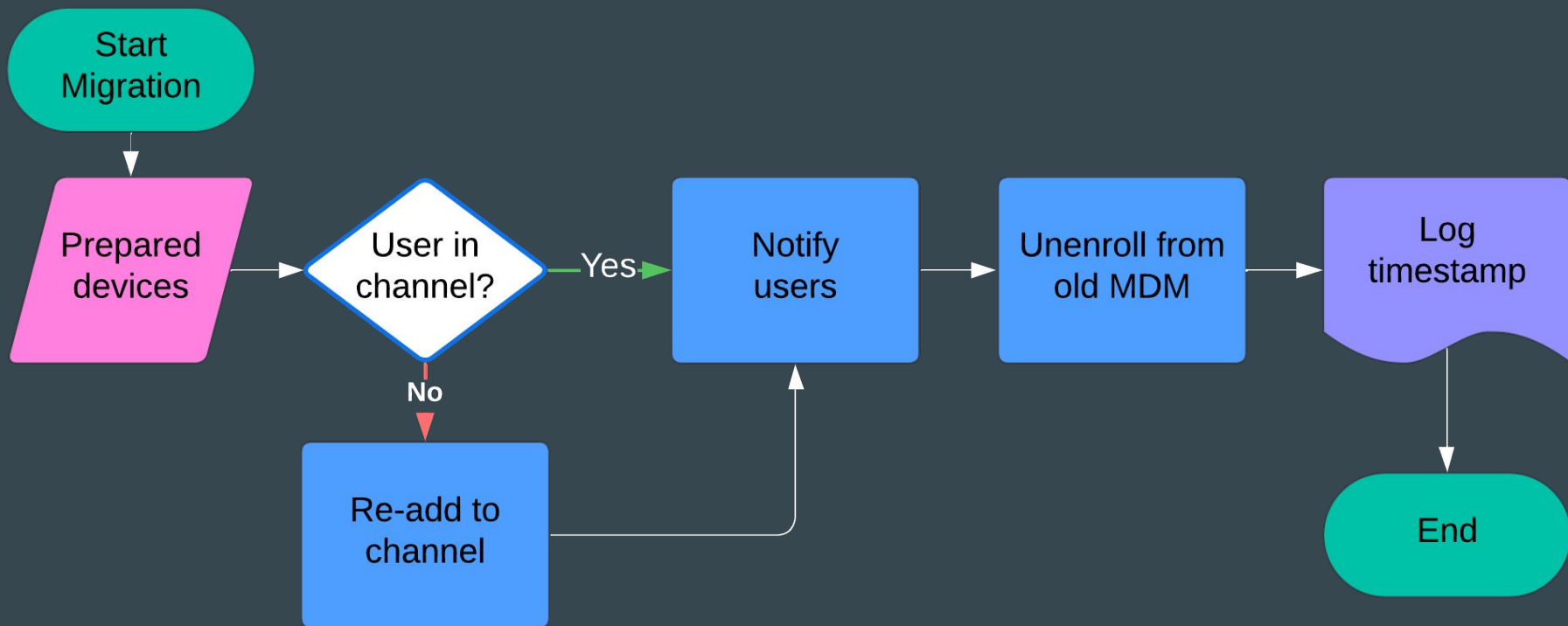
Automating the Process: Preparation



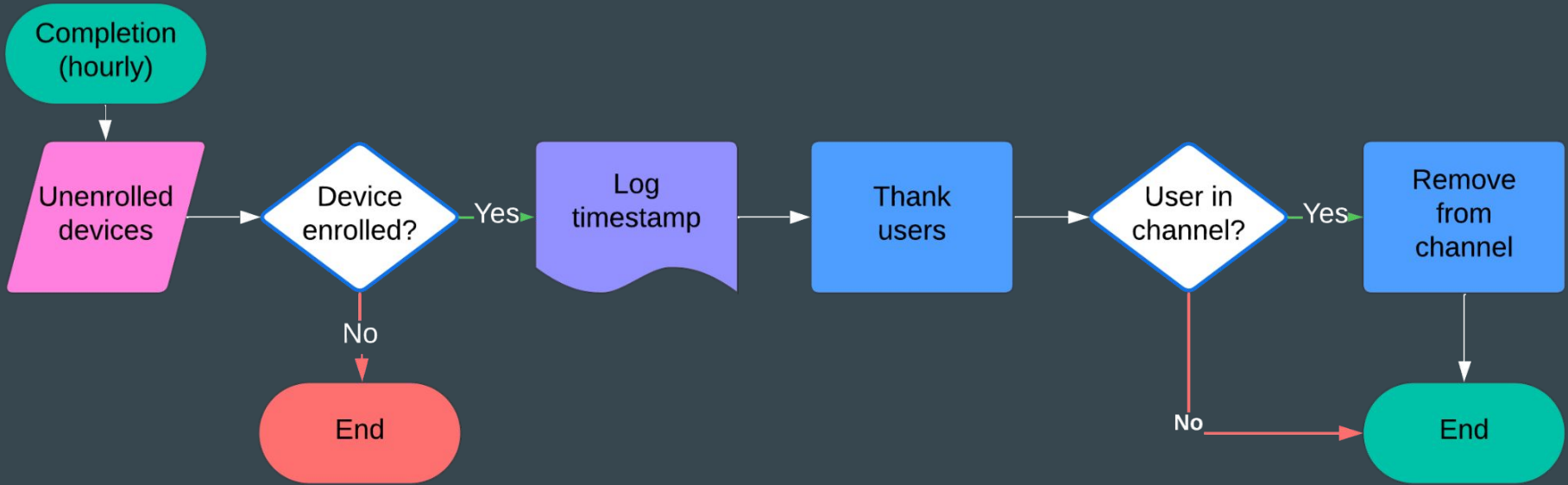
Automating the Process: Remind



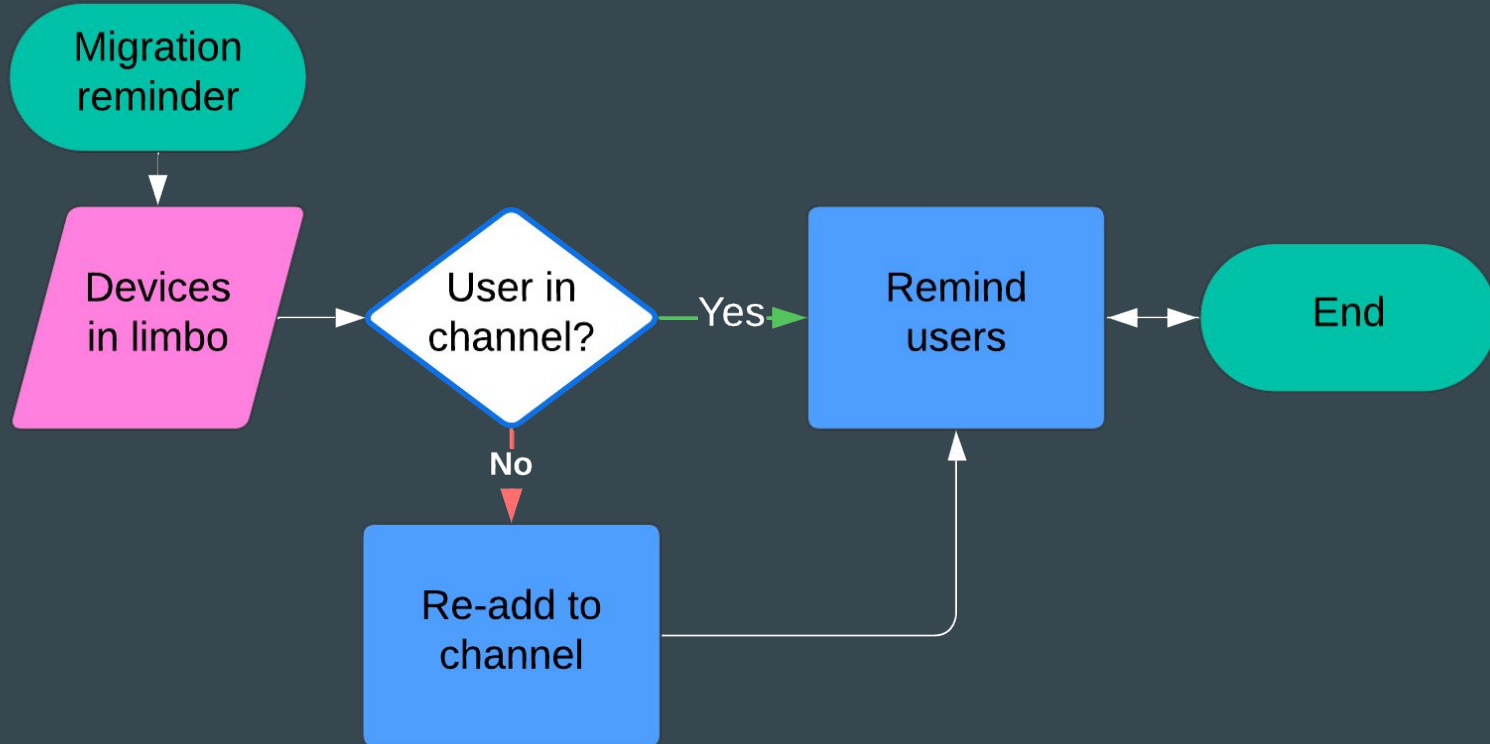
Automating the Process: Start Migration



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

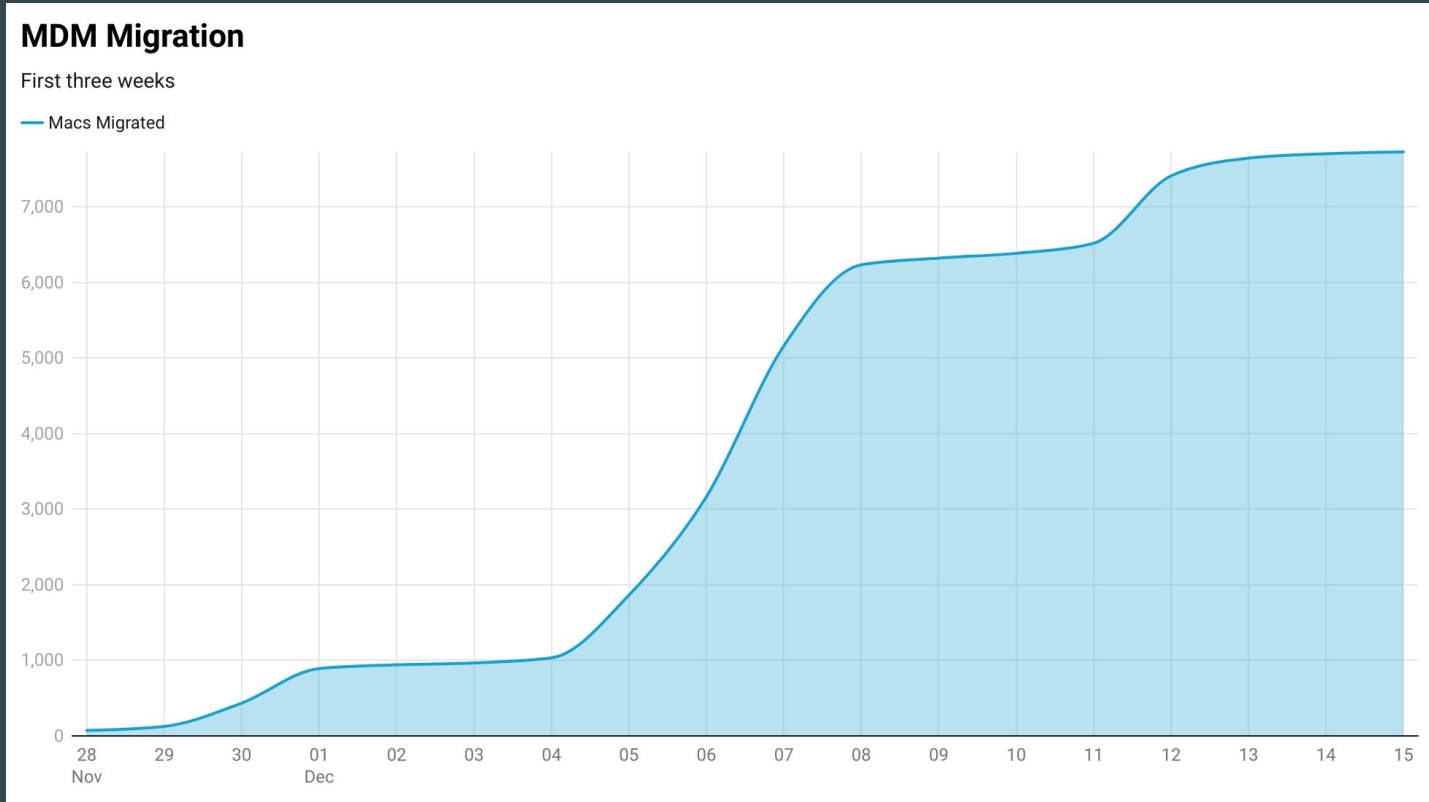
in Limbo

1

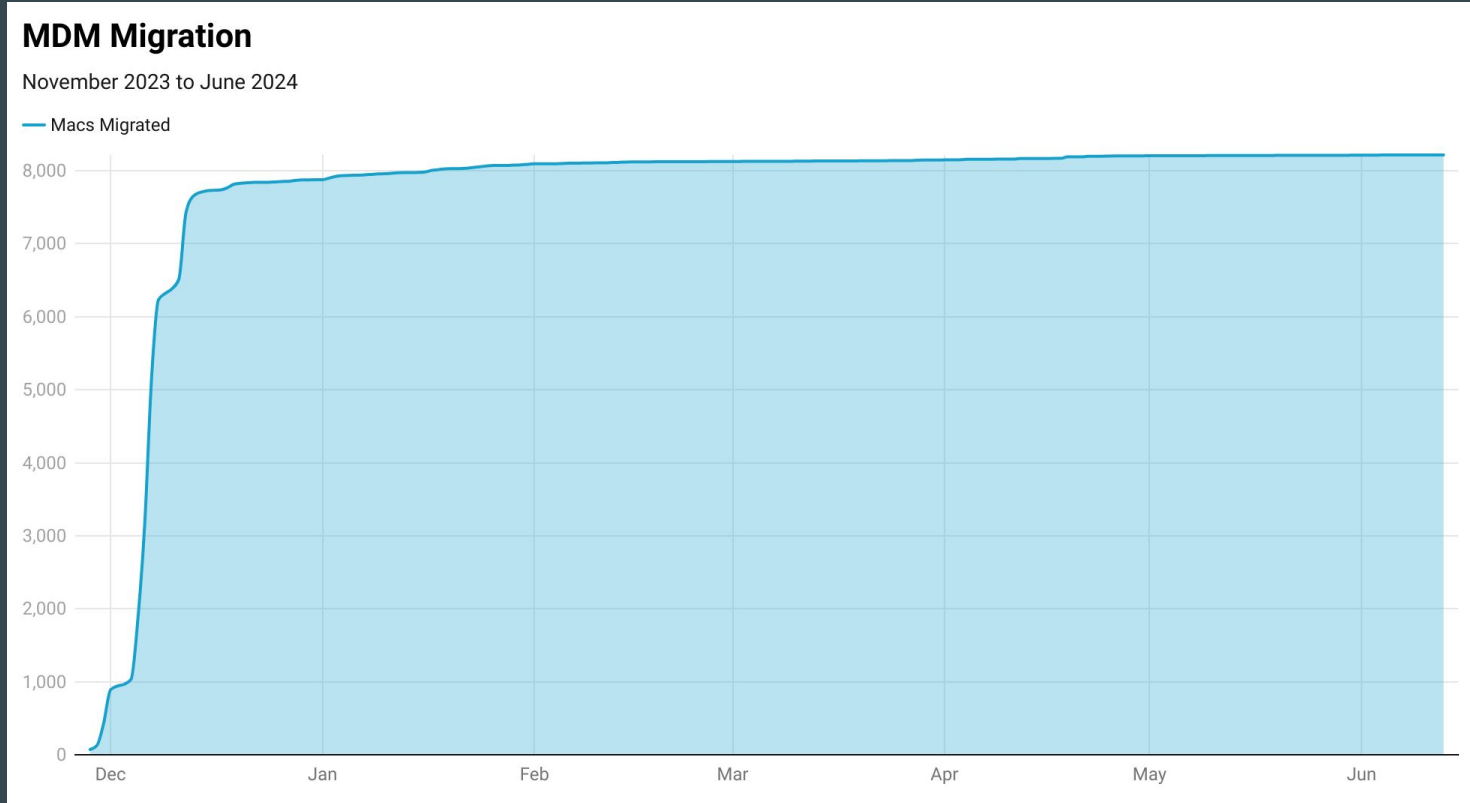
Angry User



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

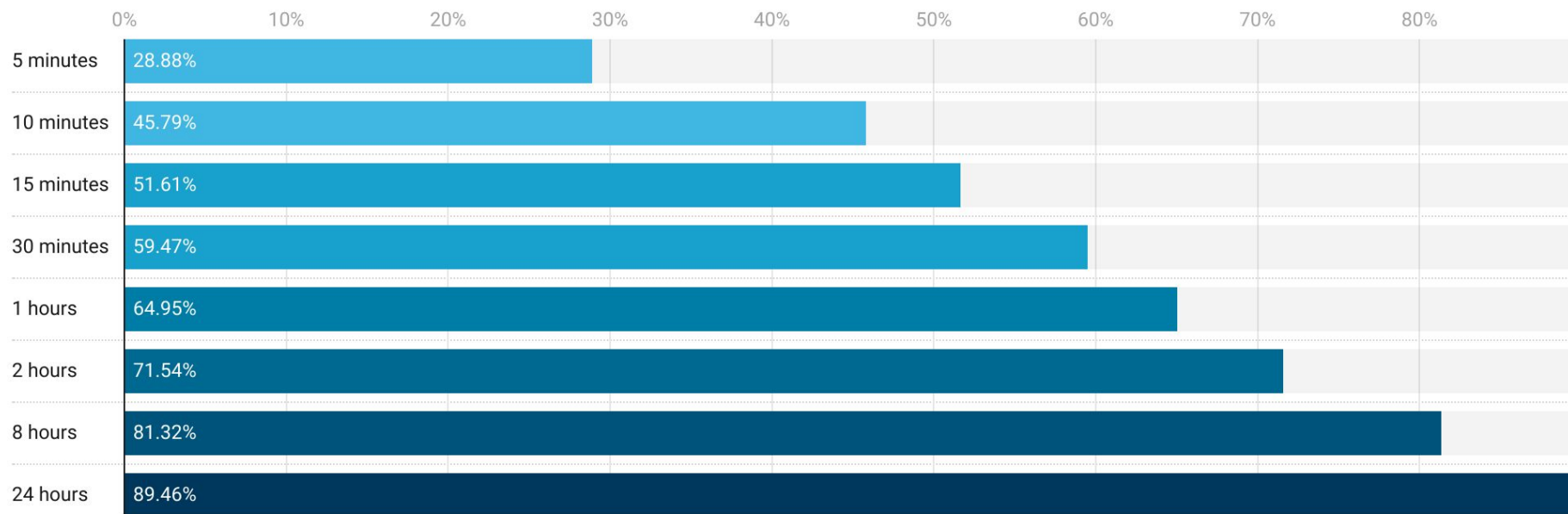
Hours



Risk Window

Time to Re-enrollment

How long did devices remain un-managed during the migration:



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
- Trying to make everyone happy
 - Our RFP took substantially longer than planned due to us trying to let too many other teams weigh-in

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



Windows

But that's a different conference...

Questions?

Thank you!