From Zero-Touch to Zero-Trust: Managing macOS with Intune

By Marc Nahum

Sponsors

onedeploy
Windows Deployment Reimagined

ZERO TOUCH

Insight

control up

PATCH MY PC

Rimo3

robopack

numecent

Microsoft

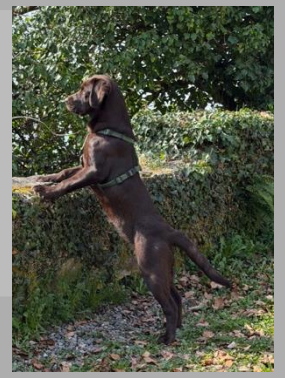
Marc Nahum

Marc Nahum
Microsoft

Role
Intune Senior Product Manager

Focus
Apple devices managed by Intune

Blog, Hobbies and more
A young labrador ...



Agenda

- **macOS management**
  Roadmap, migration,Copilot
- **Security, Standard user**
  Recovery lock, LAPS,DDM
- **Platform SSO**
  Simple or not
- **Tools for next steps**

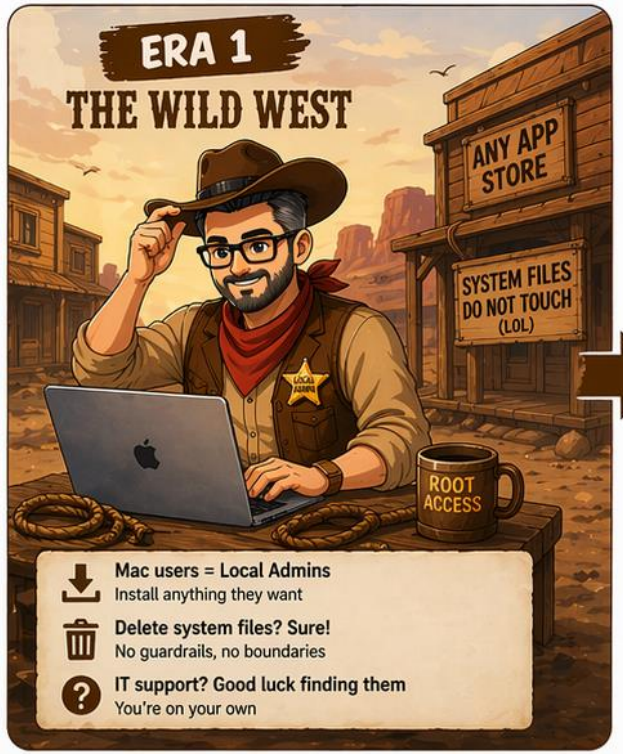
From chaos to control

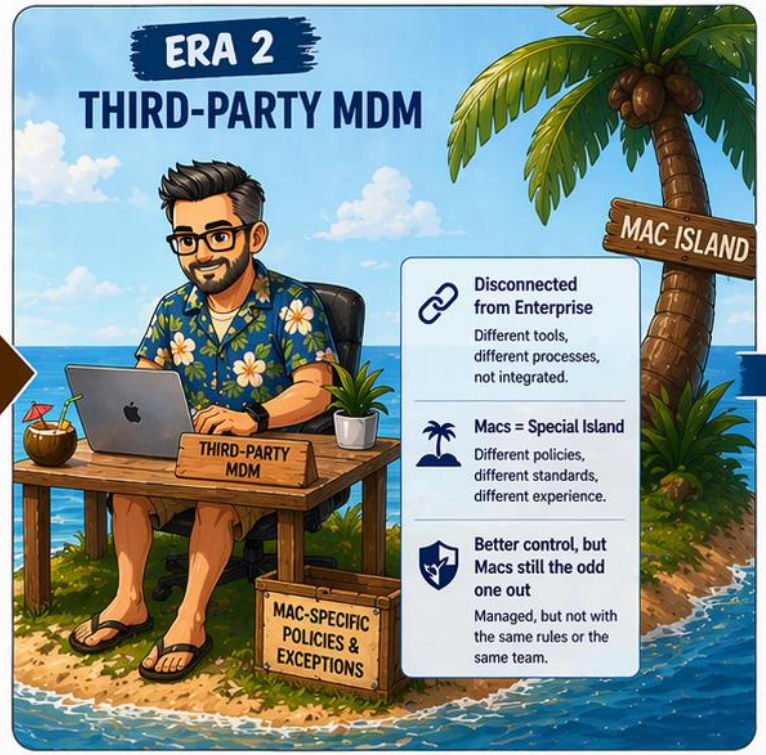
From chaos to control

From chaos to control

THE EVOLUTION OF MAC MANAGEMENT IN ENTERPRISE

From Wild West to Fully Integrated





ERA 1
THE WILD WEST
Mac users = Local Admins

ERA 2
THIRD-PARTY MDM
Macs = Special Island

ERA 3
MANAGED BY INTUNE
Macs are NOT Exception Anymore – Part of the Enterprise

STRONGER SECURITY
Consistent policies and protection across all devices

BETTER USER EXPERIENCE
Seamless, consistent experience for Mac users

LOWER RISK
Reduced exceptions, less complexity, more control

ONE IT. ONE PLATFORM.
Manage all devices together with Microsoft Intune

The **Microsoft Secure Productivity Stack** on macOS

PRODUCTIVITY

M365 + Copilot
Word · Excel · Outlook · Teams
VS Code · Copilot for M365

DATA

Microsoft Purview
Sensitivity Labels · Endpoint DLP
Information Protection · Insider risk

THREAT

Microsoft Defender
EDR · Vulnerability Management
Anti-malware · Real-time Protection

MANAGEMENT

Microsoft Intune
Zero-Touch Enrolment with LAPS · ADE/ABM
DDM · MDM Migration · Compliance

IDENTITY

Microsoft Entra ID
Platform SSO · Enterprise SSO
Conditional Access · MFA

OPERATING SYSTEM

macOS
Secure Enclave · SIP · Gatekeeper
Native MDM · Apple Silicon

Few questions?

Who have Macs in his enterprises?

Who managed them?

Who managed them with Intune?

Who still have the users as permanent admins?

Intune macOS capabilities: Recent updates

Aug-Oct 23

- Pin web clips to dock
- Settings Catalog+
- Defender policy enhancements
- macOS Sonoma support
- DDM software Update

Nov-Jan 24

- Defender policy enhancements
- Settings Catalog+
- Custom PKG support
- Date picker for DDM software updates
- DMG and PKG size increase to 8GB

Feb-Apr 24

- Await final config
- Local account management
- Custom PKG Pre + Post-install scripts
- Settings Catalog+
- Cloud PKI support + Remote Help

May-Jul 24

- Platform SSO public preview
- Company Portal supports DMG and PKG
- ACME protocol support
- Settings Catalog+
- View recovery key in Company Portal

Aug-Dec 24

- Sequoia day-zero settings
- OS version, CPU architecture as filters
- Shell script max size increases to 1 MB
- User channel support in RA profiles

Jan-Apr 25

- Auto-enforce latest software update (DDM)
- Remote Desktop management command
- VPP enhancements (VPP v2)

May-July 25

- Enhanced inventory
- Managed admin account
- Local Admin Password Solution (LAPS)

Aug-Dec 2025

- Platform SSO – GA
- DDM software update reporting
- macOS Tahoe Support

Jan -Mar 2026

- **DDM Filters**
- **Recovery lock password**

New in last 12 months

Remote Device Action: rotate Recovery Lock passcode

Summarize this article for me

> **Note**
>
> This feature is gradually rolling out and may not yet be available in your tenant. Full availability is expected by late April 2026.

Intune macOS capabilities: Coming soon (Actively working on the subject, dates are subject to change)

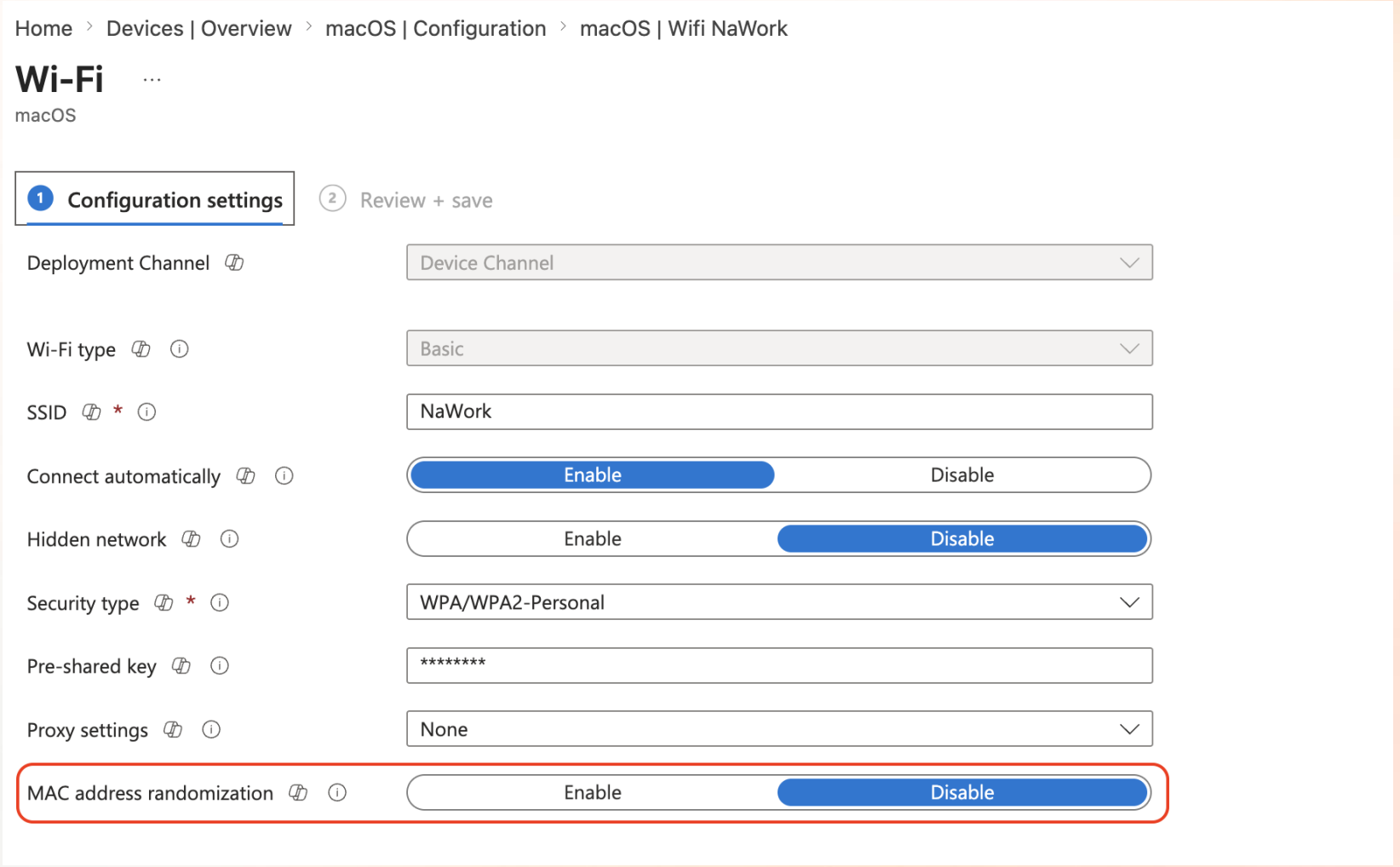
macOS Roadmap Highlights

- Setting to disable MAC address randomization
- Platform SSO during Setup Assistant
- Deploy unique SCEP
- Introduce custom compliance for macOS

- ACME certificates for future attestation
- Add Defender risk score for compliance

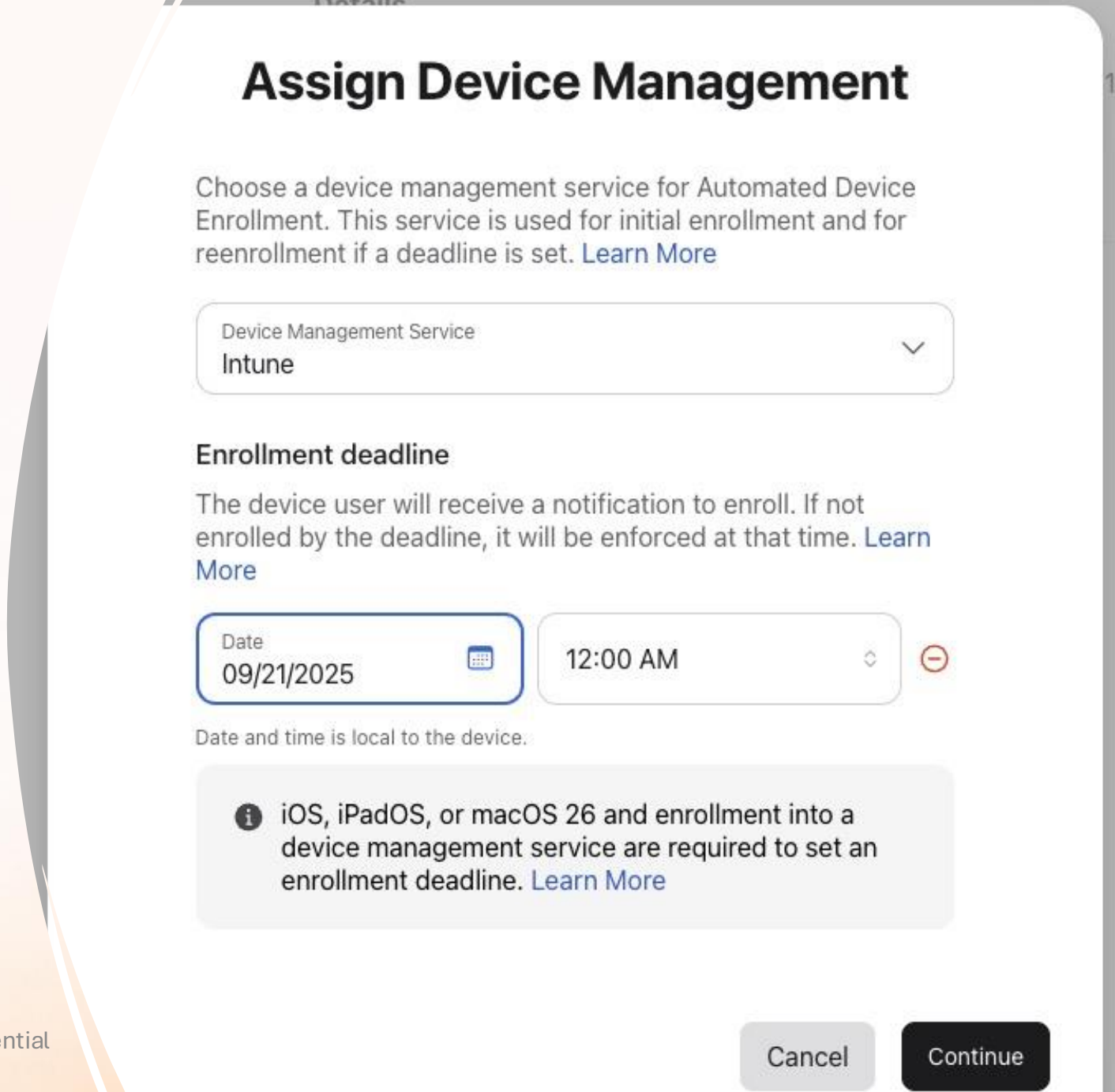
- Enable enrollment time grouping
- Support DDM apps and Managed App Framework

MAC address randomization



MDM Migration with macOS 26

Just Works ....



Microsoft confidential

MDM Migration with macOS 26

Almost

Just Works ….

- Check the removal of the agent and applications from previous MDM provider.
- Sync every 8h, Script exist to schedule it
- Activate await configuration
- Add FileVault rotation setting
- Test, test and test
- Communication with the users is a key part of the success

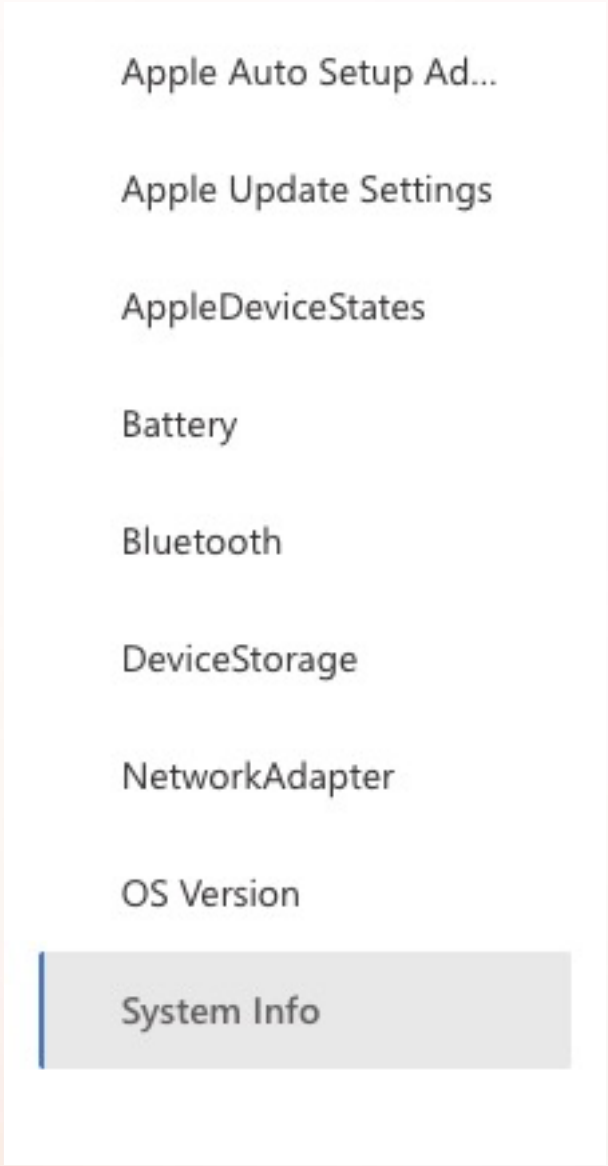
Microsoft confidential

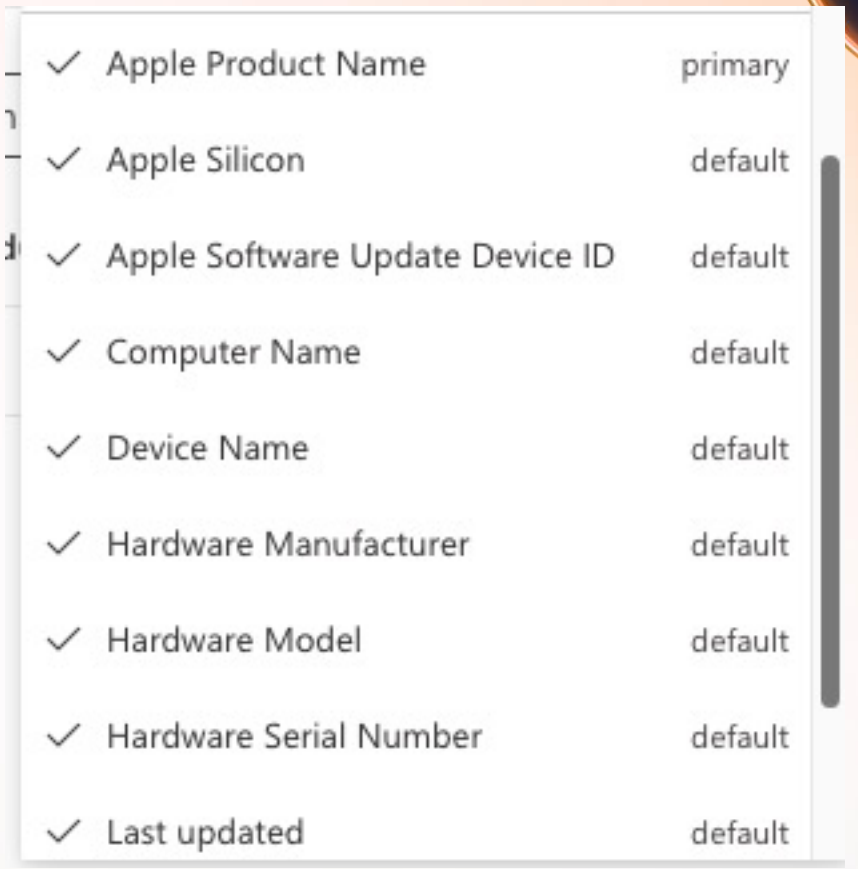
Migrate to Intune StepByStep

- Move your macOS26 device in ABM
  - Select your device on ABM
  - Choose assign device management from the 3 dots on the top right
  - Select “Add Deadline” (optional but recommended, only appear on os26 devices)
- Wait or force a sync on the new Intune console (8h, manual, script)

Microsoft confidential

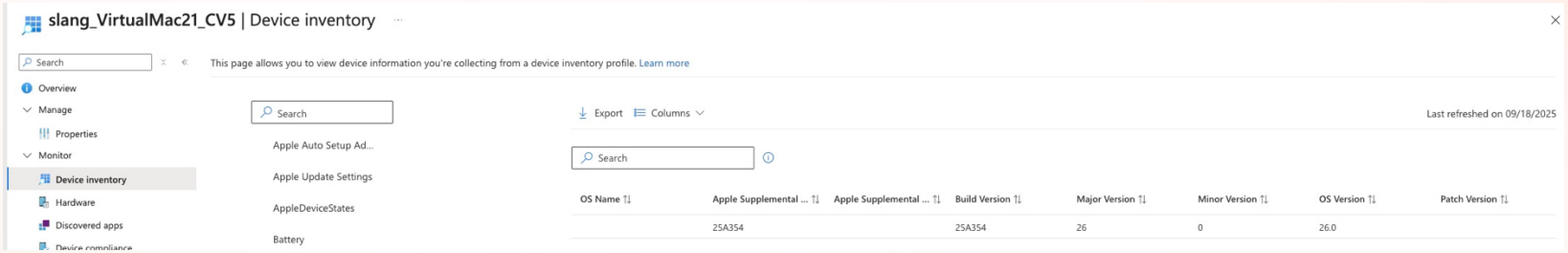
Device Inventory, a new inventory?



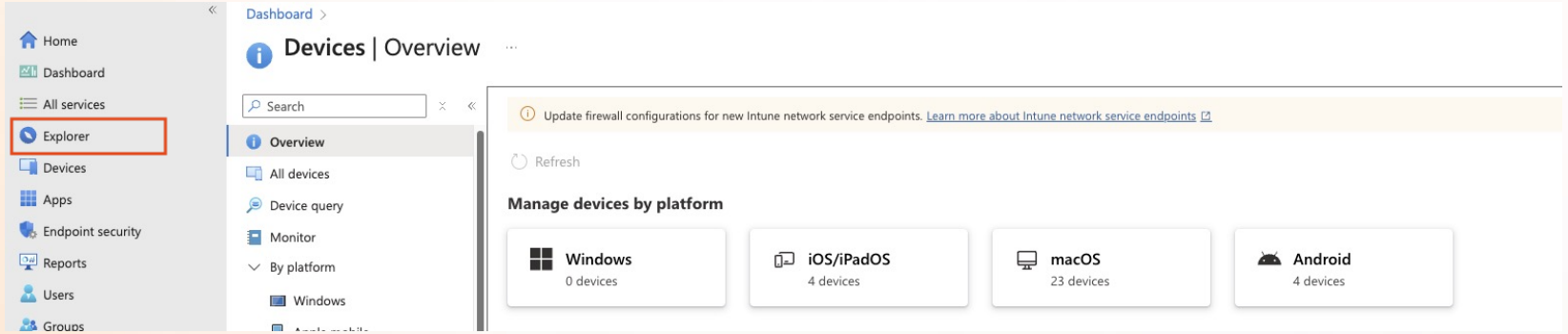


Microsoft

Device Inventory is not Explorer



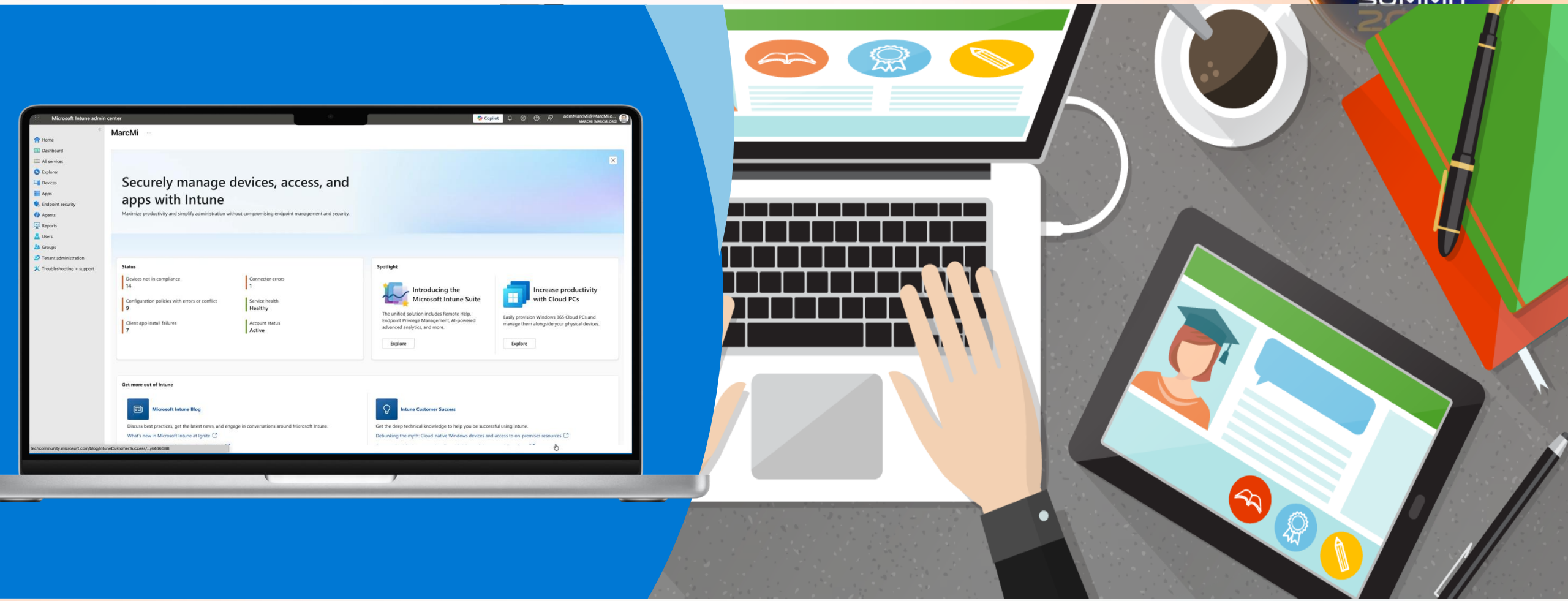
- Intune Core
- All MDM apple Inventory (76 values)
- Source of Data for device Query (Intune Suite)



- Based on Intune Copilot (Security Copilot)
- Now predefined questions
- Will evolved a lot this year (use feedback)

Microsoft

Demo


Microsoft Intune admin center
Copilot
admMarcMi@MarcMi.o...
MARCMI (MARCMI.ORG)
Home
Dashboard
All services
Explorer
Devices
Apps
Endpoint security
Agents
Reports
Users
Groups
Tenant administration
Troubleshooting + support
MarcMi
Securely manage devices, access, and apps with Intune
Maximize productivity and simplify administration without compromising endpoint management and security.
Status
Devices not in compliance
14
Connector errors
1
Configuration policies with errors or conflict
9
Service health
Healthy
Client app install failures
7
Account status
Active
Spotlight
Introducing the Microsoft Intune Suite
The unified solution includes Remote Help, Endpoint Privilege Management, AI-powered advanced analytics, and more.
Explore
Increase productivity with Cloud PCs
Easily provision Windows 365 Cloud PCs and manage them alongside your physical devices.
Explore
Get more out of Intune
Microsoft Intune Blog
Discuss best practices, get the latest news, and engage in conversations around Microsoft Intune.
What's new in Microsoft Intune at Ignite
Intune Customer Success
Get the deep technical knowledge to help you be successful using Intune.
Debunking the myth: Cloud-native Windows devices and access to on-premises resources
techcommunity.microsoft.com/blog/intuneCustomerSuccess/.../4466688

Agenda

- **macOS management**
  Roadmap, migration,Copilot
- **Security, Standard user**
  Recovery lock, LAPS,DDM
- **Platform SSO**
  Simple or not
- **Tools for next steps**

Demo


Select Your Country or Region
Switzerland
Afghanistan
Åland Islands
Albania
Algeria
American Samoa
Andorra
Angola
Anguilla
Antarctica
Antigua & Barbuda
Continue
Press the escape key to hear how to set up your Mac with VoiceOver.
Triple-click Touch ID to view accessibility options.

Recovery partition

Recovery partition is:

- Hidden dedicated bootable environment
- Isolated from the main macOS system volume
- Runs a minimal version of macOS with system tools

Recovery partition on macOS is used for:

- Reinstall macOS
- Reset admin password using FileVault recovery key
- Repair or erase disks with Disk Utility
- Modify Secure Boot and external boot settings
- Restore a system from Time Machine backup

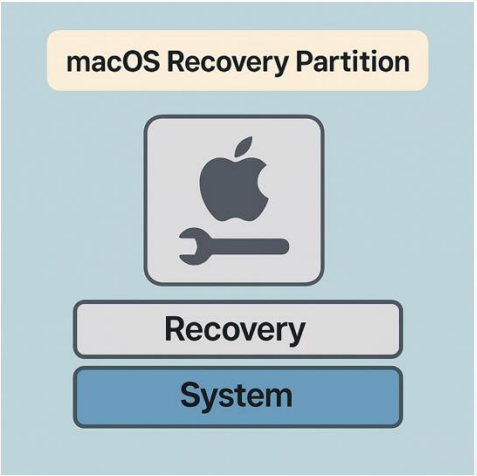
Or

Recovery partition on macOS is accessed with:

- Admin account password
- The FileVault recovery key

The FileVault recovery key is :

Accessible by the user from the Company portal



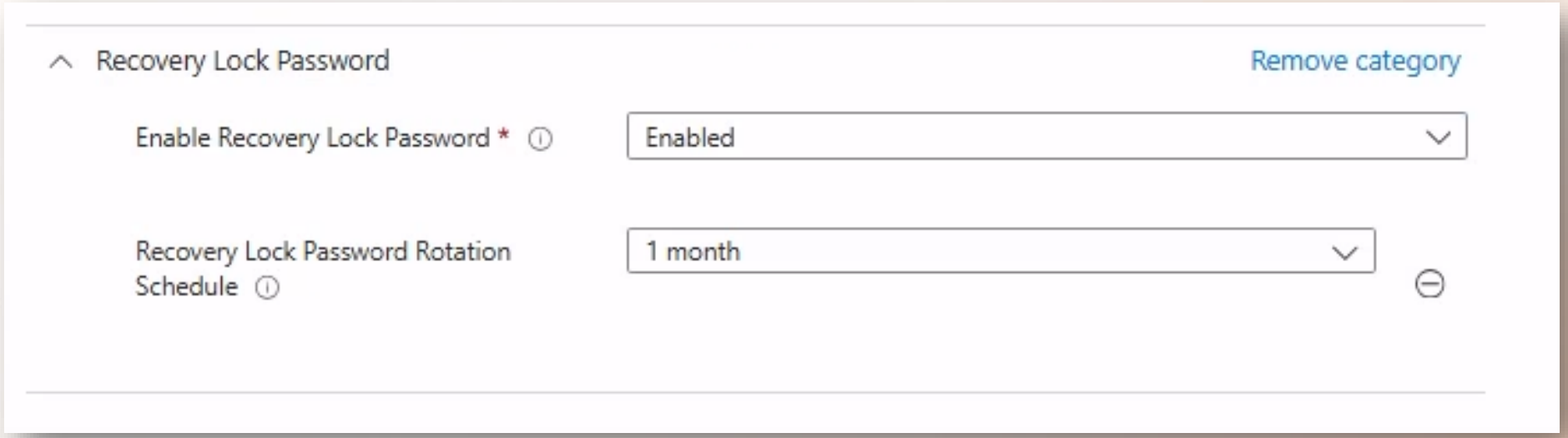
Microsoft confidential

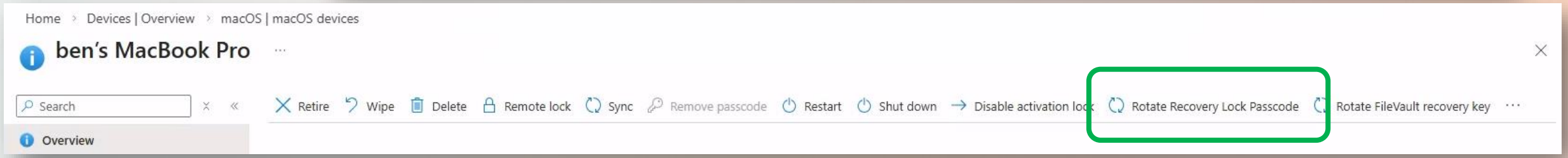
What is recovery lock?

- Recovery lock is an MDM managed password for the recovery partition (recoveryOS)
- Intune can:
  - Generate and set password on devices via settings catalog
  - Rotate password via action or policy
  - Display password to admins
- PW can be cleared by:
  - manually entering
  - unassigning policy
  - unenrolling
- Available for Apple silicon Macs running 11.5 +

Admin experience

- Enabled via settings catalog
- Auto rotation schedule in months (like FileVault)





MODERN ENDPOINT MANAGEMENT SUMMIT 2026

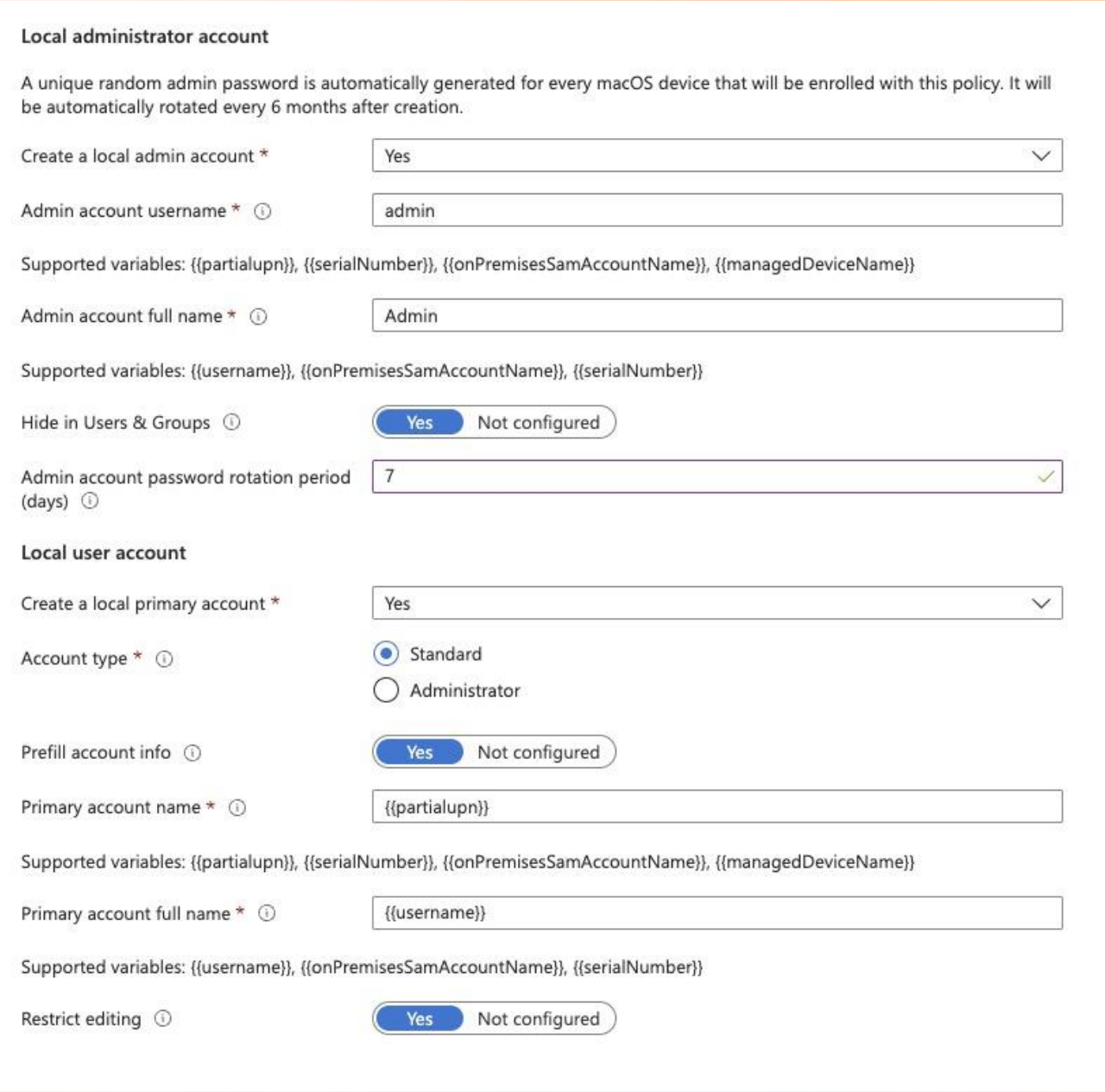
LAPS for macOS

Create a local admin account for **management**

- Using variables
- Hide from the users

Enforce configuration for your **primary** user

- Using variables
- Standard or Admin account*
- Information prefilled from Entra ID
- Cannot be modified

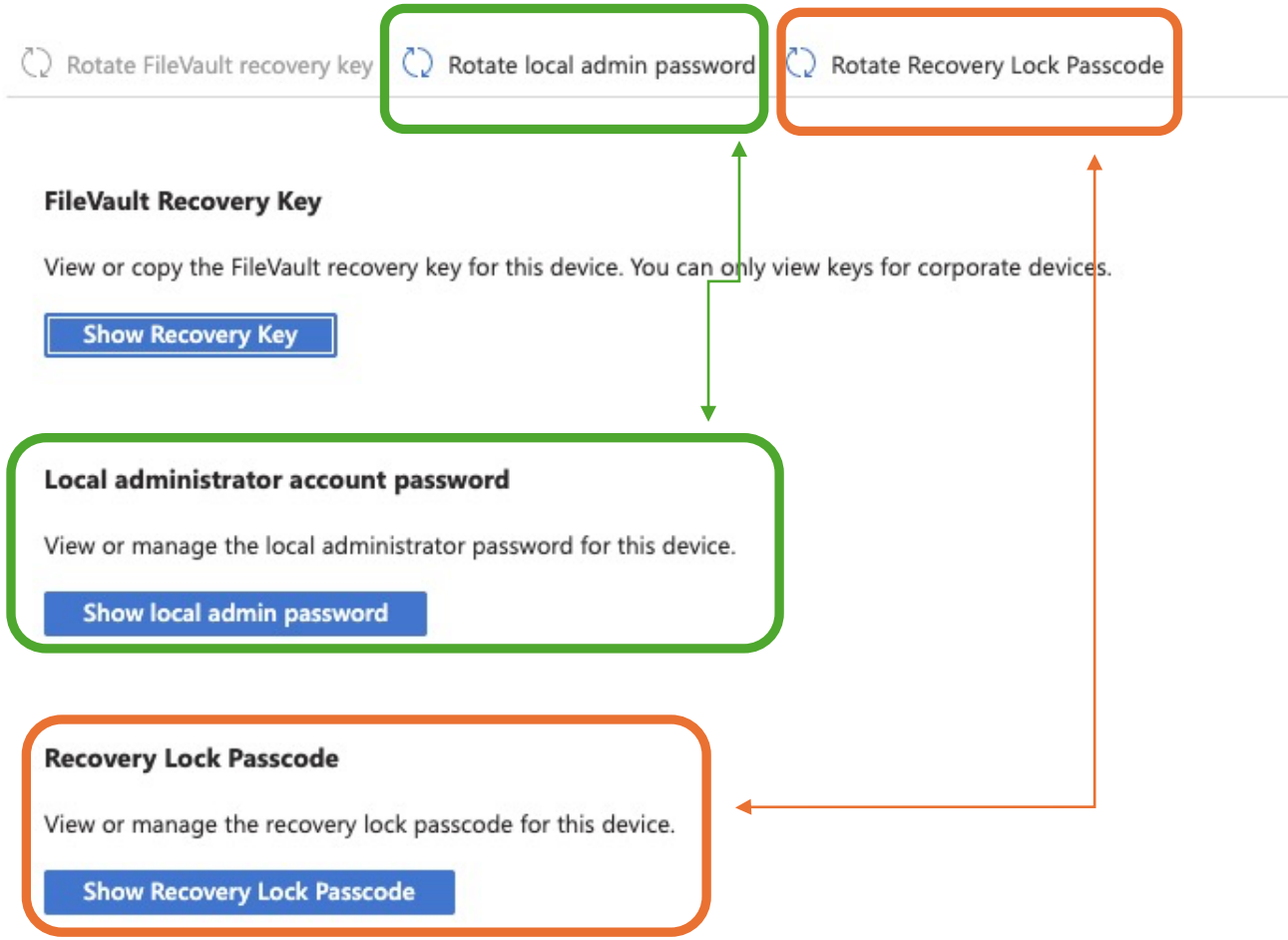


*Compatible with PSSO during setup Assistant in macOS26. PSSO always win

LAPS for macOS / Recovery Lock

Passwords are:

- RBAC protected (Read / Rotate)
- Change are audited
- Random
- Complex
- Can be manually rotated



For LAPS

- Automatic Password rotation once every 6 months
- Manual Auto rotation 1-180 days

Do not use that 2 parameters if not in macOS 26.4 :

- Maximum Passcode Age in Days (**DDM**)
- Max PIN Age In Days (**MDM**)

LAPS is only supported for new enrolled ADE Macs

LAPS

Local administrator account

A unique random admin password is automatically generated for every macOS device that will be enrolled with this policy. It will be automatically rotated every 6 months after creation.

Create a local admin account * : Yes

Admin account username * : admin

Supported variables: {{partialupn}}, {{serialNumber}}, {{onPremisesSamAccountName}}, {{managedDeviceName}}

Admin account full name * : Admin

Supported variables: {{username}}, {{onPremisesSamAccountName}}, {{serialNumber}}

Hide in Users & Groups : Yes | Not configured

Admin account password rotation period (days) : 30

Local user account

Create a local primary account * : Yes

Account type * : Standard / Administrator

Prefill account info : Yes | Not configured

Primary account name * : {{partialupn}}

Supported variables: {{partialupn}}, {{serialNumber}}, {{onPremisesSamAccountName}}, {{managedDeviceName}}

Primary account full name * : {{username}}

Supported variables: {{username}}, {{onPremisesSamAccountName}}, {{serialNumber}}

Restrict editing : Yes | Not configured

Platform SSO

Account Display Name : MarcMi

Authentication Method : UserSecureEnclaveKey

Non Platform SSO Accounts

Delete | Sort | Import | Export

Admin

Use Shared Device Keys : Enabled

User Authorization Mode : Standard

Registration Token : {{DEVICEREGISTRATION}}

Screen Locked Behavior : Do Not Handle

Team Identifier : UBF8T346G9

Type * : Redirect

URLs

Delete | Sort | Import | Export

https://login.chinacloudapi.cn

https://login.microsoft.com

https://login.microsoftonline.com

https://login.microsoftonline.us

https://login.partner.microsoftonline.cn

Microsoft confidential

Custom Compliance

macOS custom compliance will enable admins to leverage discovery script and compliance policy w/ JSON file to define device compliance status.

Step 1: Discovery script

- Device compliance > script

Step 2: Compliance policy

- Devices > custom compliance
- Discovery scripts pre-created is linked to the policy
- JSON file upload to set policy details

Experience mirrors Windows and Linux Custom Compliance feature.

Declarative Software Updates

DDM configuration for software update enforcement!

Specify OS/build to install by an exact time

Only Version and date are mandatory

No cross-version parameter use.

Software Update

Target Date Time	9/30/2025, 1:00:00 PM
Target OS Version	26

Software Update Settings

Allow Standard User OS Updates	Allowed
Automatic Actions	
Download	Allowed
Deferrals	
Minor Period In Days	1

Declarative Software Updates

Just say yes

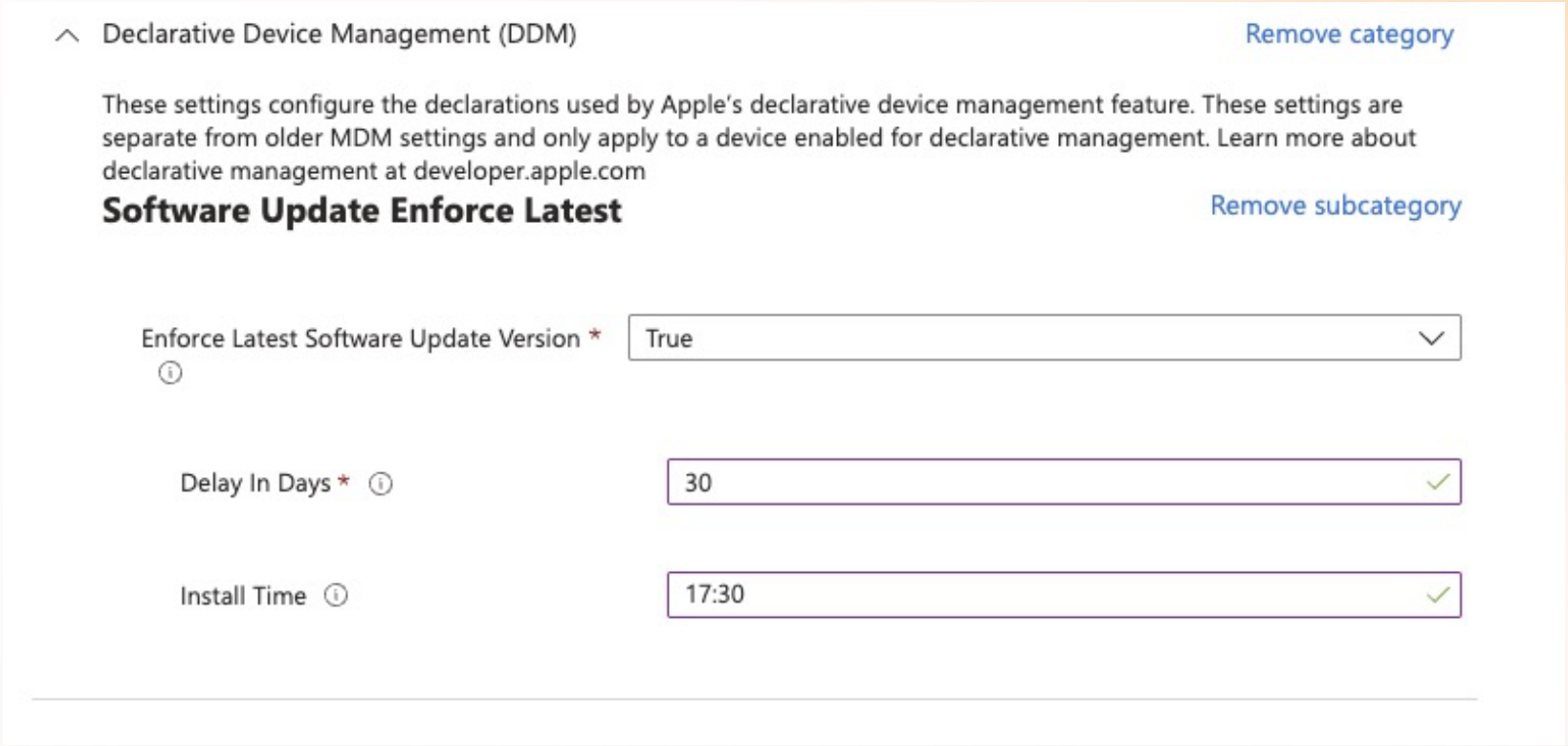
Delay is based on Apple released date

Major OS update are the last version

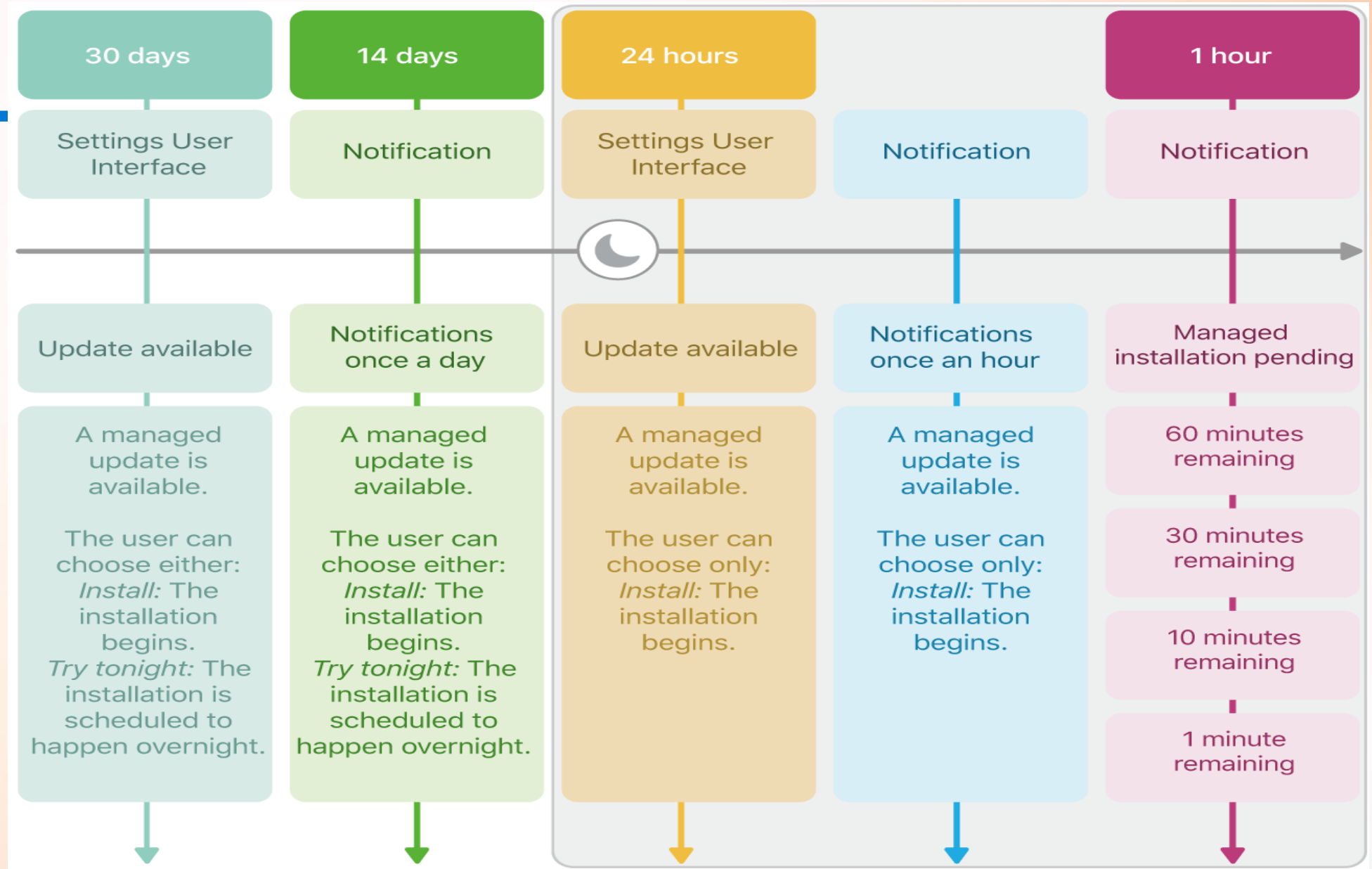
It is a profile, so rings of update are possible

Install time in 24h format

Local time of the device



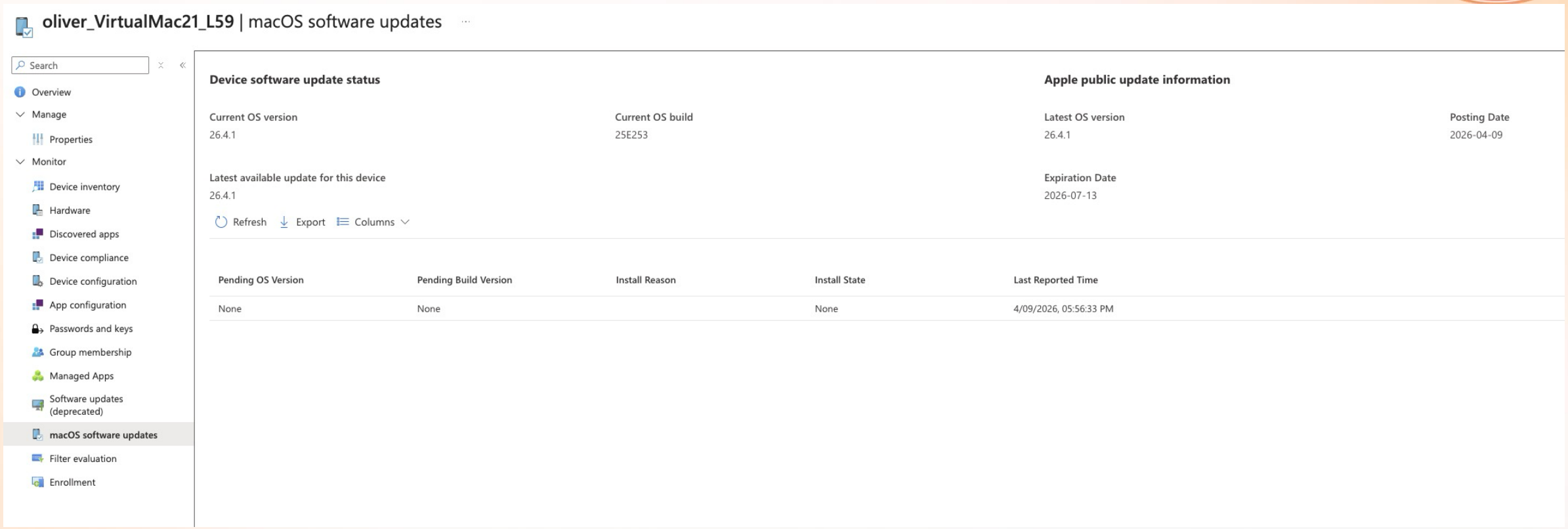
Microsoft


30 days
14 days
24 hours
1 hour
Settings User Interface
Notification
Settings User Interface
Notification
Notification
Update available
Notifications once a day
Update available
Notifications once an hour
Managed installation pending
A managed update is available.
The user can choose either: *Install:* The installation begins. *Try tonight:* The installation is scheduled to happen overnight.
A managed update is available.
The user can choose either: *Install:* The installation begins. *Try tonight:* The installation is scheduled to happen overnight.
A managed update is available.
The user can choose only: *Install:* The installation begins.
A managed update is available.
The user can choose only: *Install:* The installation begins.
60 minutes remaining
30 minutes remaining
10 minutes remaining
1 minute remaining


MODERN
ENDPOINT
MANAGEMENT
SUMMIT
2026

Microsoft

Declarative Software Updates Report



How to monitor MDM/DDM check-ins


```
/usr/bin/log show --info --predicate 'process == "mdmclient" AND composedMessage
CONTAINS "Processing server request: DeclarativeManagement for"' --last 24h
```

tony — -zsh — 217×57

```
tony@tony_VirtualMac21_NN1 ~ % /usr/bin/log show --info --predicate 'process == "mdmclient" AND composedMessage CONTAINS "Processing server request: DeclarativeManagement for"' --last 24h

Filtering the log data using "process == "mdmclient" AND composedMessage CONTAINS "Processing server request: DeclarativeManagement for""
Skipping debug messages, pass --debug to include.
Timestamp                       Thread     Type        Activity             PID    TTL
2025-09-14 17:35:49.948599+0200 0xa75      Default     0x0                  460    7    mdmclient: [com.apple.ManagedClient:MDMDaemon] [*] [0:MDMDaemon:<0xa75>] Processing server request: DeclarativeManagement for: <D
evice> (A27F5726-570A-4075-ACED-7CDFDE884343) PowerNap: no
2025-09-14 18:07:24.812672+0200 0xce0      Default     0x0                  648    7    mdmclient: [com.apple.ManagedClient:MDMDaemon] [*] [0:MDMDaemon:<0xce0>] Processing server request: DeclarativeManagement for: <D
evice> (27E8B6F2-AA22-4E5F-84C5-1E67CB16247C) PowerNap: no
2025-09-14 22:05:48.651404+0200 0x163db    Default     0x0                  31664  7    mdmclient: [com.apple.ManagedClient:MDMDaemon] [*] [0:MDMDaemon:<0x163db>] Processing server request: DeclarativeManagement for:
<Device> (98176440-D51C-4CFF-9D58-0C6ED1617B40) PowerNap: no
2025-09-14 23:43:12.430886+0200 0x1c47f    Default     0x0                  38560  7    mdmclient: [com.apple.ManagedClient:MDMDaemon] [*] [0:MDMDaemon:<0x1c47f>] Processing server request: DeclarativeManagement for:
<Device> (C8FC5A3A-BAF2-4935-9B9D-EE469289FE10) PowerNap: no
2025-09-14 23:43:20.227292+0200 0x1c47f    Default     0x0                  38560  7    mdmclient: [com.apple.ManagedClient:MDMDaemon] [*] [0:MDMDaemon:<0x1c47f>] Processing server request: DeclarativeManagement for:
<Device> (5890A396-41CD-4F9E-BC6F-CB9CD4F6F621) PowerNap: no
2025-09-15 01:55:28.279735+0200 0x25850    Default     0x0                  50452  7    mdmclient: [com.apple.ManagedClient:MDMDaemon] [*] [0:MDMDaemon:<0x25850>] Processing server request: DeclarativeManagement for:
<Device> (B0C81EC2-6516-43A2-85C5-9D2E38D59297) PowerNap: no
2025-09-15 05:52:57.704299+0200 0x356ca    Default     0x0                  69772  7    mdmclient: [com.apple.ManagedClient:MDMDaemon] [*] [0:MDMDaemon:<0x356ca>] Processing server request: DeclarativeManagement for:
<Device> (5850C9B5-8769-49F1-A0AA-DFFDF7CD99E9) PowerNap: no
2025-09-15 07:43:46.215384+0200 0x3d55e    Default     0x0                  79807  7    mdmclient: [com.apple.ManagedClient:MDMDaemon] [*] [0:MDMDaemon:<0x3d55e>] Processing server request: DeclarativeManagement for:
<Device> (18F16EAC-2E1D-4F98-B1D7-287B5220BF2C) PowerNap: no
2025-09-15 07:43:54.657590+0200 0x3d55e    Default     0x0                  79807  7    mdmclient: [com.apple.ManagedClient:MDMDaemon] [*] [0:MDMDaemon:<0x3d55e>] Processing server request: DeclarativeManagement for:
<Device> (DDB5F08B-E48F-4E56-BA0D-538057B40332) PowerNap: no
2025-09-15 09:42:22.385484+0200 0x45328    Default     0x0                  89329  7    mdmclient: [com.apple.ManagedClient:MDMDaemon] [*] [0:MDMDaemon:<0x45328>] Processing server request: DeclarativeManagement for:
<Device> (5CC9D96A-925D-4DC6-AF8C-BF19EEBA1F4B) PowerNap: no
2025-09-15 11:11:35.732815+0200 0x4b2ea    Default     0x0                  96161  7    mdmclient: [com.apple.ManagedClient:MDMAgent] [*] [501:MDMAgent:<0x4b2ea>] Processing server request: DeclarativeManagement for:
<User: 501> (662B706F-8D53-45B1-81EC-62A78744273F) PowerNap: no
2025-09-15 11:11:57.876923+0200 0x4bbd3    Default     0x0                  96161  7    mdmclient: [com.apple.ManagedClient:MDMAgent] [*] [501:MDMAgent:<0x4bbd3>] Processing server request: DeclarativeManagement for:
<User: 501> (45B2CA61-E94B-4CCF-8868-817CD275616C) PowerNap: no
2025-09-15 16:14:16.782206+0200 0xf8a      Default     0x0                  607    7    mdmclient: [com.apple.ManagedClient:MDMAgent] [*] [501:MDMAgent:<0xf8a>] Processing server request: DeclarativeManagement for: <U
ser: 501> (4EC3EC34-9F1C-4CC9-A48B-94306898E972) PowerNap: no
2025-09-15 16:14:24.896343+0200 0xf8a      Default     0x0                  607    7    mdmclient: [com.apple.ManagedClient:MDMAgent] [*] [501:MDMAgent:<0xf8a>] Processing server request: DeclarativeManagement for: <U
ser: 501> (4B582817-1F3A-4CD2-A9F6-3F7C525AAD1E) PowerNap: no
-------------------------------------------------------------------------------------------------------------------
Log      - Default:         14, Info:               0, Debug:            0, Error:          0, Fault:          0
Activity - Create:           0, Transition:         0, Actions:          0
tony@tony_VirtualMac21_NN1 ~ %
```

Demo


Microsoft Intune admin center
macOS | Configuration
Policies
Create
Refresh
Export
Columns
ddm
Add filters
Policy name
Platform
Policy type
Last modified
Scope tag
macOS | DDM update Sequoia 15.6.1
macOS | DDM Beta testing Tahoe 26
macOS | DDM update Sequoia 15.5
macOS | DDM update Sequoia 15.3.1
macOS | DDM update Sequoia 15.2
macOS | DDM update Sequoia 15.1.1
Settings catalog
Default

Intune Agent check-ins

- Outside the normal MDM/DDM channel check-ins
- Supports Intune Agent (PKG/DMG apps and Shell Scripts)
- Current check-in schedule
  - Every 15 minutes for the first hour after enrollment
  - Every 8 hours after the first hour
  - Note: this is currently being addressed to improve Intune Agent performance
- Log can be found at */Library/Logs/Microsoft/Intune*
- New blog published

Support tip: Troubleshooting Microsoft Intune management agent on macOS

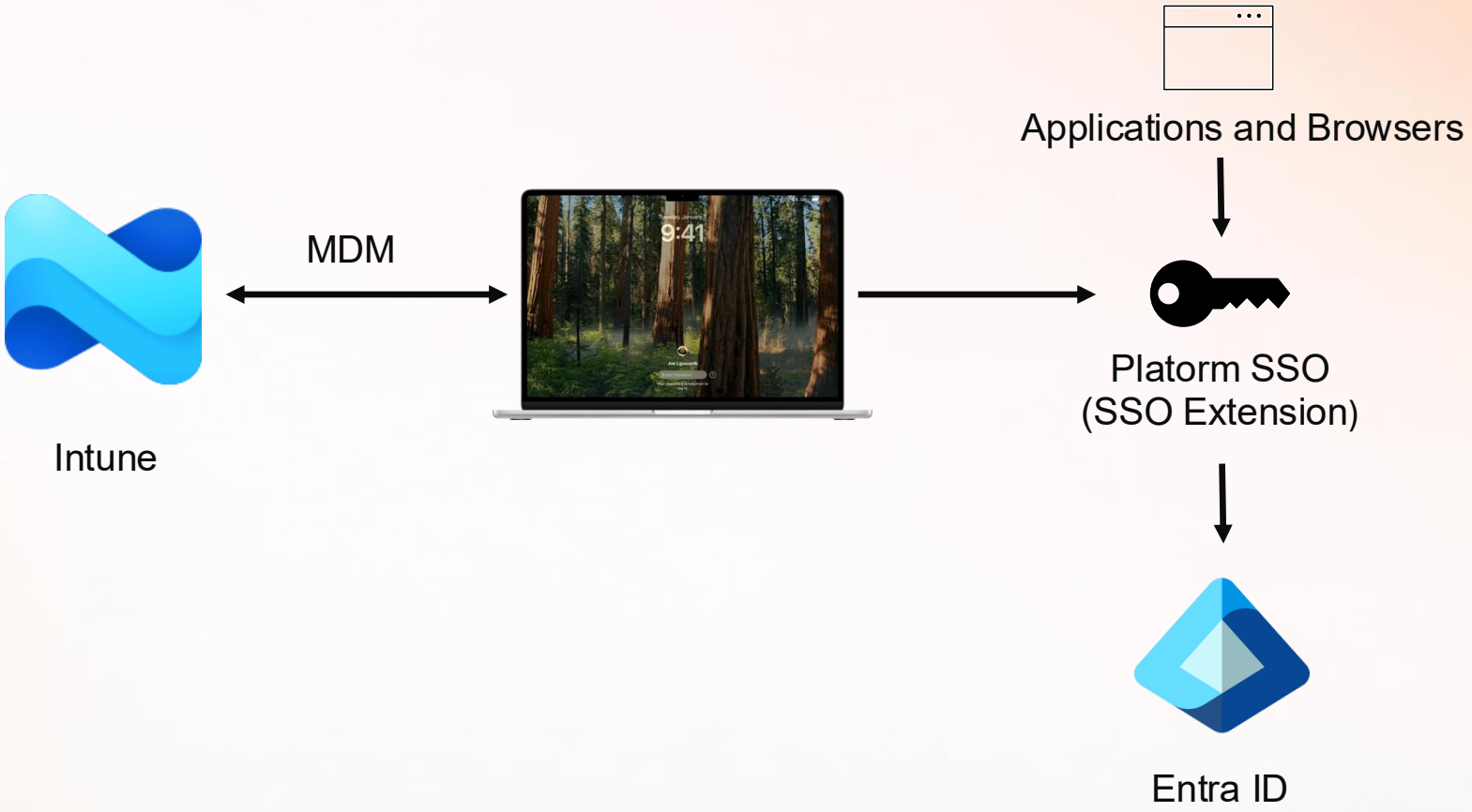
https://techcommunity.microsoft.com/blog/intunecustomersuccess/support-tip-troubleshooting-microsoft-intune-management-agent-on-macos/4431810

Microsoft

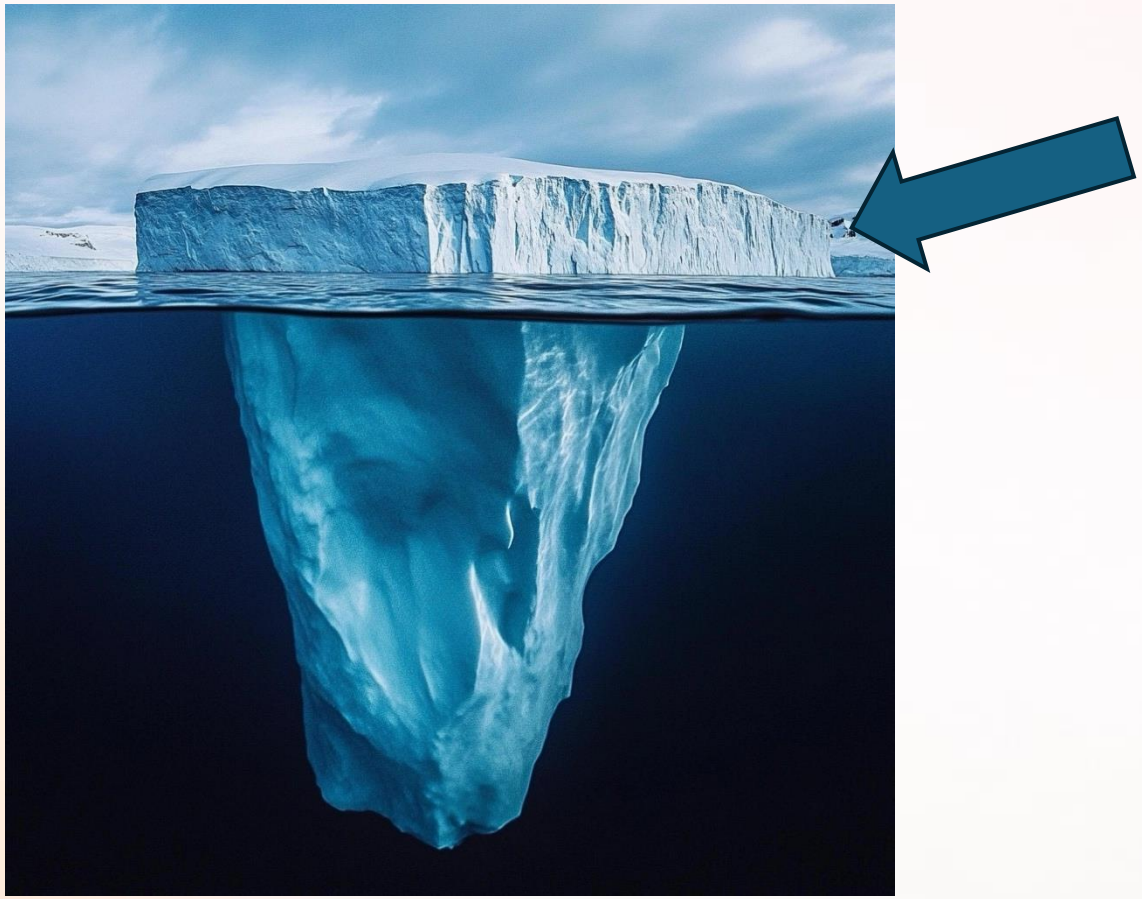
Agenda

- **macOS management**
  Roadmap, migration,Copilot
- **Security, Standard user**
  Recovery lock, LAPS,DDM
- **Platform SSO**
  Simple or not
- **Tools for next steps**

Platform SSO

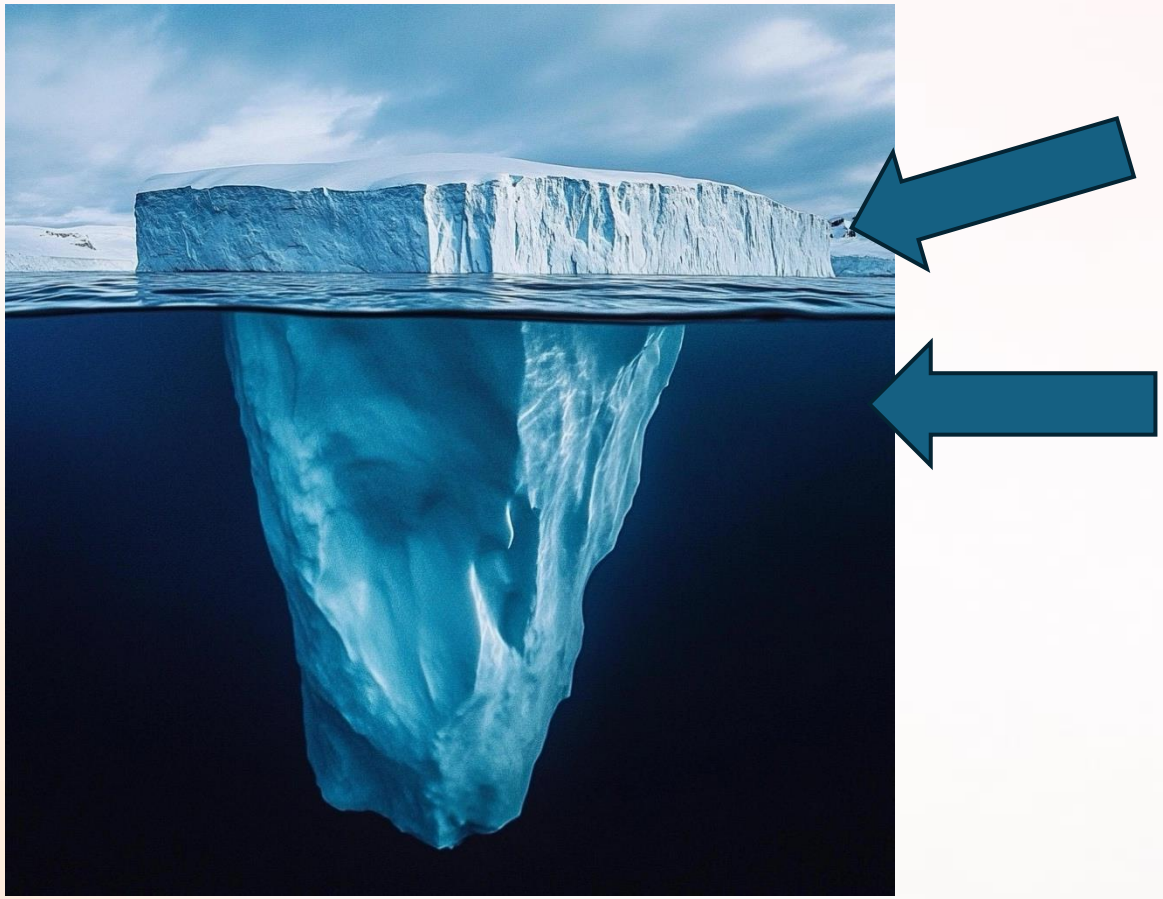


Platform SSO: Swiss knife of macOS authentication



Allows logging on to your Mac using Entra ID password.

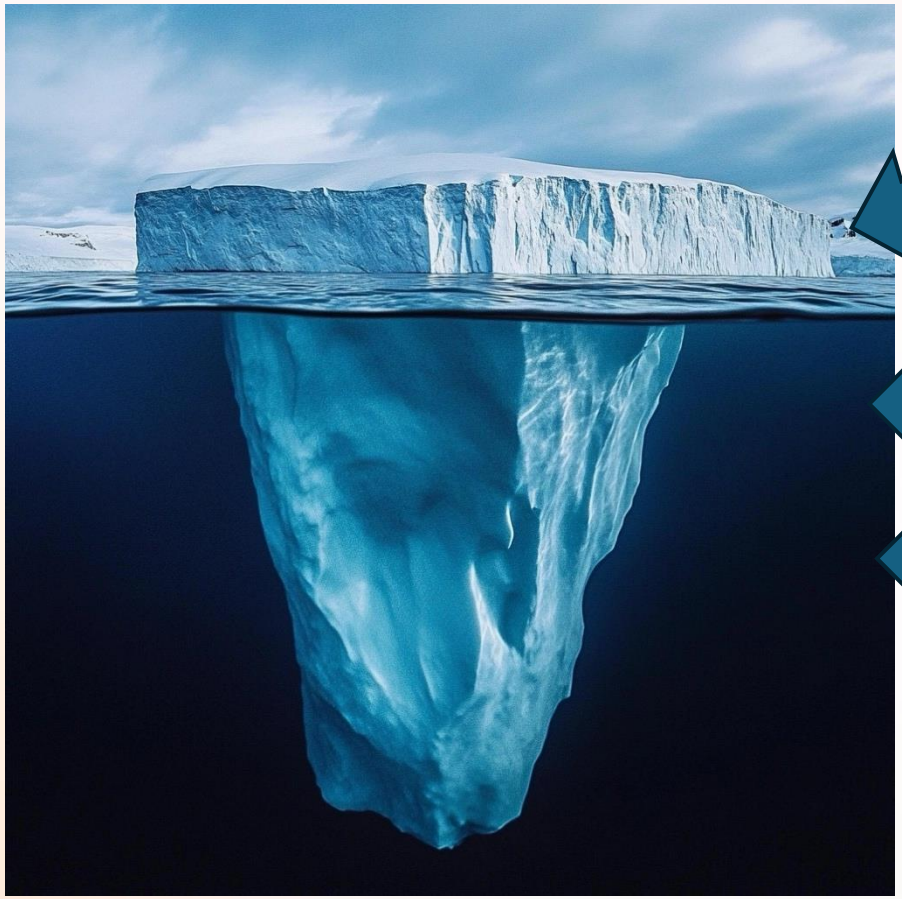
Platform SSO: Swiss knife of macOS authentication



Allows logging on to your Mac using Entra ID password.

Secure the access with Secure enclave

Platform SSO: Swiss knife of macOS authentication

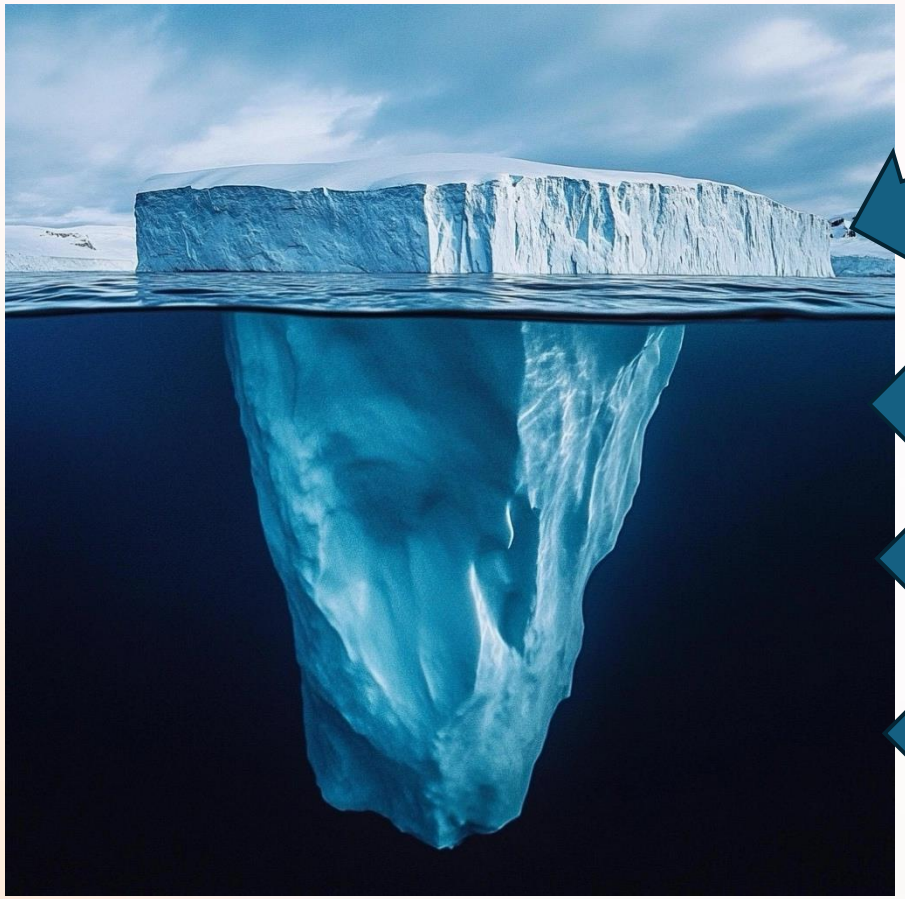


Allows logging on to your Mac using Entra ID password.

Secure the access with Secure enclave

Any users from the enterprise can log

Platform SSO: Swiss knife of macOS authentication



Allows logging on to your Mac using Entra ID password.

Secure the access with Secure enclave

Any users from the enterprise can log

Set user as Standard / Admin

Decide the authentication method

Secure Enclave

Phishing resistant

A secure key protected by the Secure Enclave is used for authentication with Entra ID.

- Analogous to WHfB on macOS
- Local authentication using a passcode, password, or TouchID
- In web browsers, this PRT key can be used as an access key using the WebAuthN APIs
- MFA required for configuration, use of the Temporary Access Pass (TAP) possible
- Can be used as passkey

Smart card

Phishing resistant

Uses an external smart card to authenticate with Entra ID.

- Useful for highly secure customers with existing investments in smart card technology
- The username of the local account remains unchanged.
- Requires MFA for configuration
- TouchID supported for unlock

Password

Not phishing resistant

The local account password is used to authenticate to Entra ID and is kept in sync.

- The username remains unchanged.
- Fewer passwords for users and administrators to remember/manage.
- MFA not required (*not recommended)*
- TouchID supported for unlock

Better Good

PSSO per OS version

	Sonoma	Sequoia	Tahoe
Password Sync	☑	☑	☑
Secure Enclave	☑	☑	☑
Smartcard support	☑	☑	☑
Admin or Standard user	☑	☑	☑
Enable Entra ID user creation at login	☑	☑	☑
Kerberos Support	☑	☑	☑
FileVault Entra ID validation	☒	☑	☑
Non-Platform SSO Accounts	☒	☑	☑
Run during setup assistant	☒	☒	☑*
Synchronize Entra ID Photo	☒	☒	☑*

https://aka.ms/macOSPSSO

List is not complete, only main topics

* Will be supported by Intune soon

Platform SSO: FileVault unlock Sequoia (Psync)

Platform SSO

Authentication Method	Password
Enable Create User At Login	Enabled
FileVault Policy	AttemptAuthentication
New User Authorization Mode	Standard
Unlock Policy	AttemptAuthentication, AllowTouchIDOrWatchForUnlock
Use Shared Device Keys	Enabled
User Authorization Mode	Admin

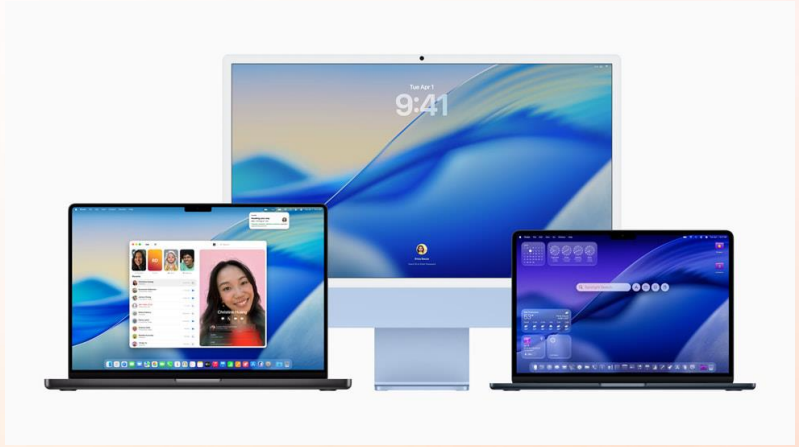
Simplified Platform SSO

- Platform SSO during the Setup Assistant
- 2 ways of using it : 403 and Await config mode
- macOS Tahoe 26.1 as the minimum version (bug fix)
- SSO broker must be on the device → Company Portal
- Need PSSO configuration

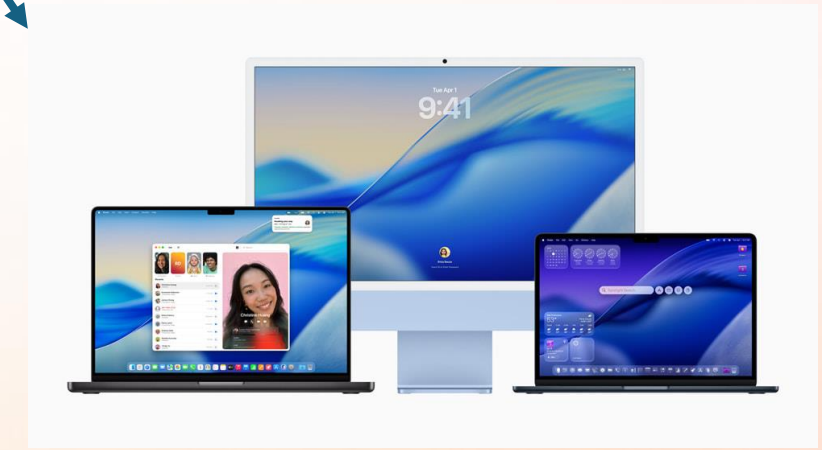
403 mode

- User goes through PSSO registration before MDM enrollment
- 403 request = stop don’t go there but coming with result
  - Package (any package to install before enrollment)
  - json configuration (config profile)
  - Auth url (optional)

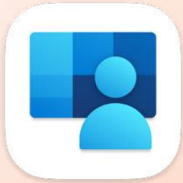
Business



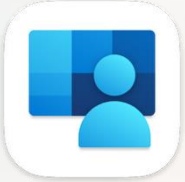
url

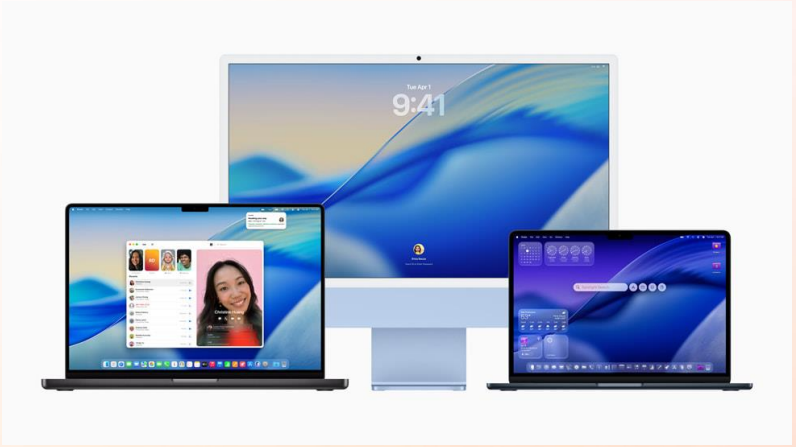


403 -> pkg + JSON + auth URL

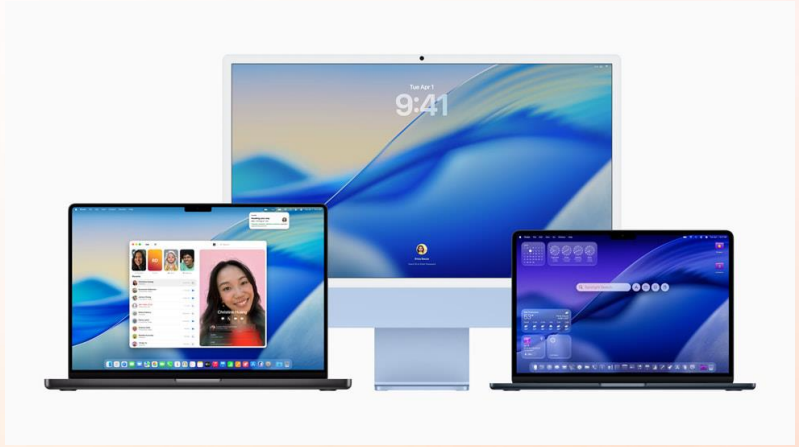


Pkg + JSON + auth URL



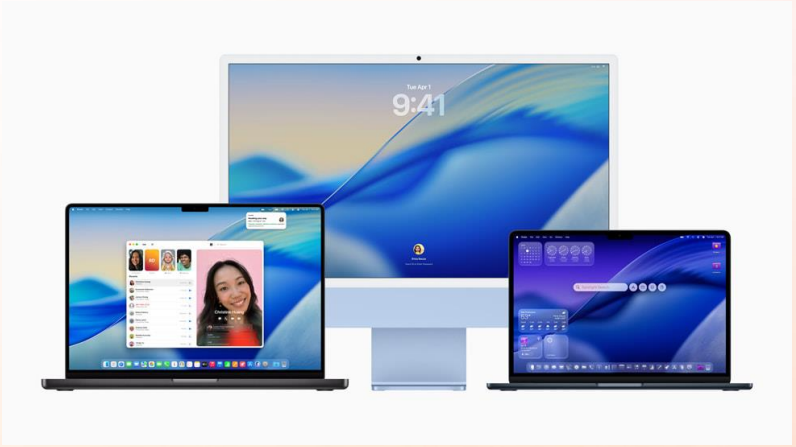


PSSO registration



Token

Enrollment



User Journey with 403 Mode

PSSO

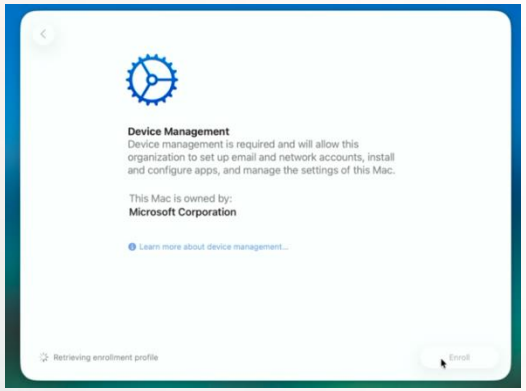
Auth

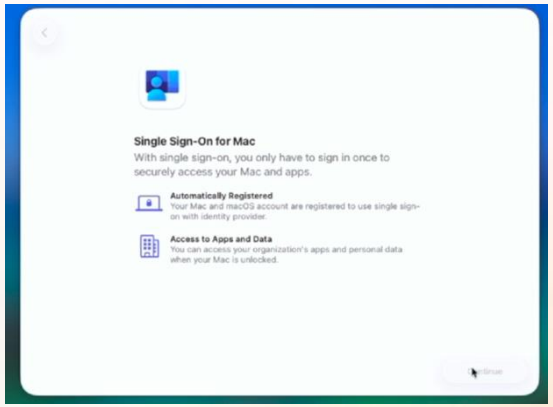
Await Config

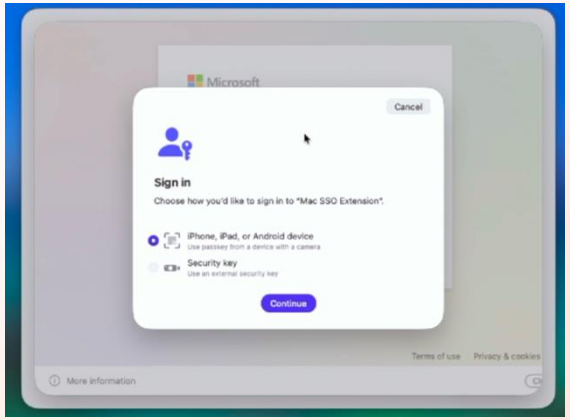
User setup

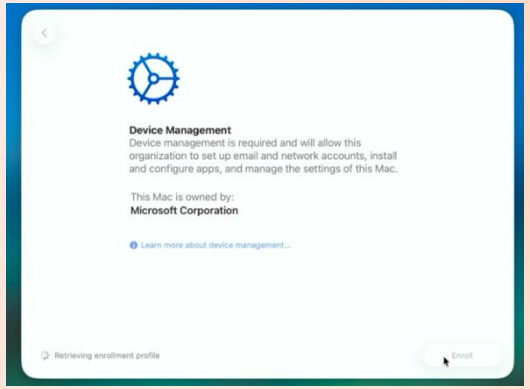
Location TID

Welcome Screen









Await config mode

- Same enrollment as now
- PSSO configuration is processed during the SA, after the MDM config, before the user configuration
- Company portal must be installed before the PSSO

User Journey with await config Mode

Modern Auth

Await Config

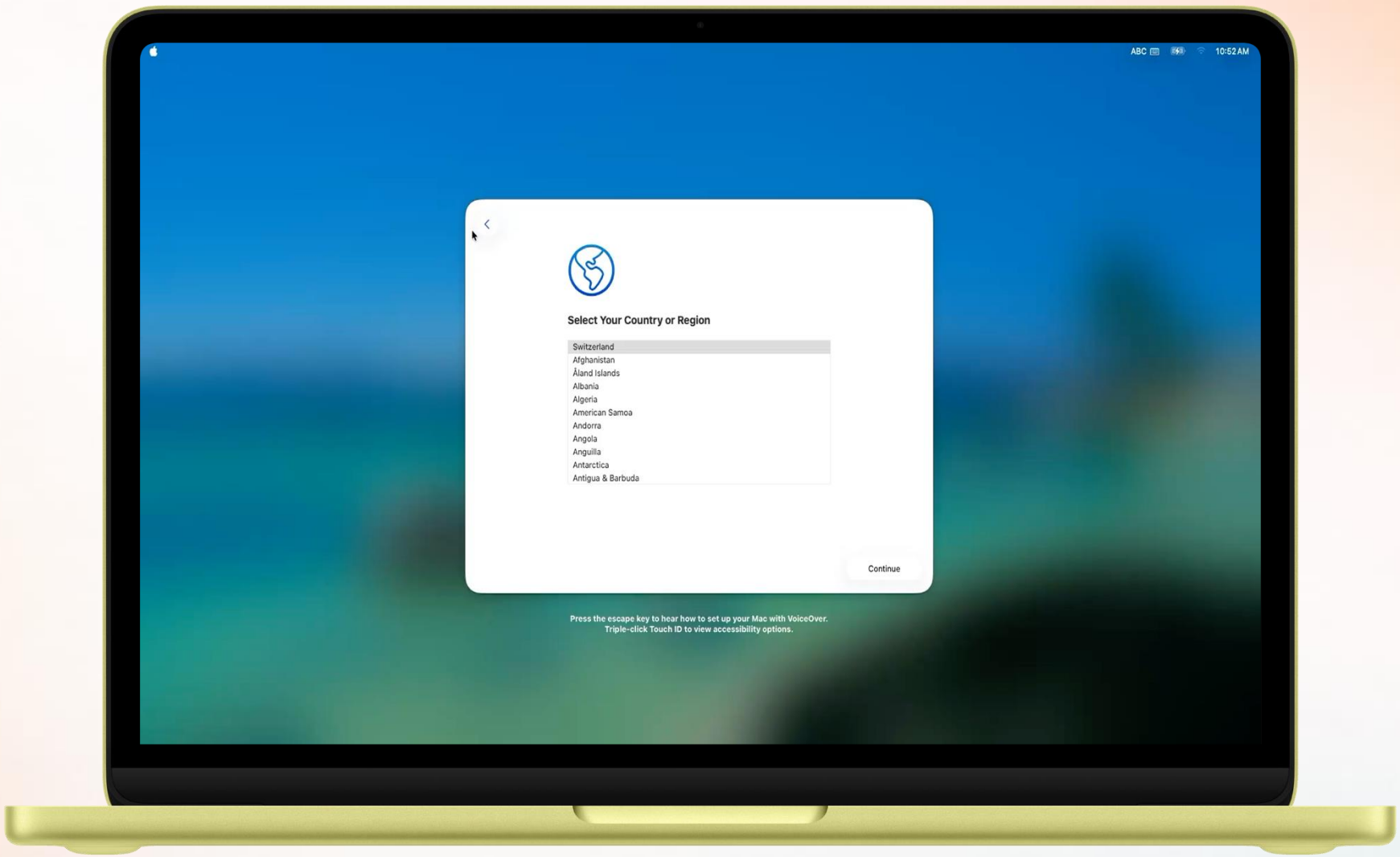
PSSO & Auth

User setup

Location TID

Welcome Screen

PSSO Psync Enrollment



Agenda

- **macOS management**
  Roadmap, migration,Copilot
- **Security, Standard user**
  Recovery lock, LAPS,DDM
- **Platform SSO**
  Simple or not
- **Tools for next steps**

Open-Source tools we love

Applications	Links	Descriptions
Munki	https://github.com/munki/munki	Application lifecycle management tool
Privileges	https://github.com/SAP/macOS-enterprise-privileges	User elevation control for macOS
Santa	https://github.com/northpolesec/santa	Binary execution control (allow/block)
Octory	https://www.octory.io	Customized onboarding splash screen
SwiftDialog	https://github.com/swiftDialog/swiftDialog	admin utility that presents custom dialogs, displays informative messages or can be used as a form to request user input.

And More...

New Open-Source tools we love

Applications	Links	Descriptions
Intune Uploader	https://github.com/almenscorner/intune-uploader	Creating & updating apps & payloads in Intune, leveraging AutoPkg
Intune Brew	https://www.intunebrew.com/ https://www.youtube.com/watch?v=7NEs-EnvmII	A PowerShell-based tool that automates the process of uploading and managing macOS applications(>1200) in Intune, with metadata and logos.
IntuneManagement	https://github.com/Micke-K/IntuneManagement/blob/master/README.md	A GraphAPI alternate console **with PowerShell and WPF UI**
Intune logs reader	https://intuneirl.com	A macOS tool for reading and analyzing Intune MDM logs with real-time monitoring capabilities.
macOS Security Compliance	https://github.com/usnistgov/macos_security	Programmatic approach to generating security guidance

intune-my-macs

Intune macOS configuration.

One script. Five minutes.

Open-source starter kit from the Intune CxE team. Production-ready policies, compliance baselines, apps, and scripts — aligned to Apple's Mac Evaluation Utility.

WHAT GETS DEPLOYED

Security Policies

FileVault · Firewall · Gatekeeper · Restrictions · Login Window · Screensaver lock

Compliance & System

DDM passcode · Software update · NTP · Power management · macOS version baseline

Apps & Onboarding

Company Portal · M365 defaults · Remote Help · Swift Dialog onboarding

Scripts & Inventory

Device rename · Dock config · Escrow Buddy · Custom attributes for reporting

Defender for Endpoint

Optional MDE onboarding · System extensions · Privacy preferences · all automated

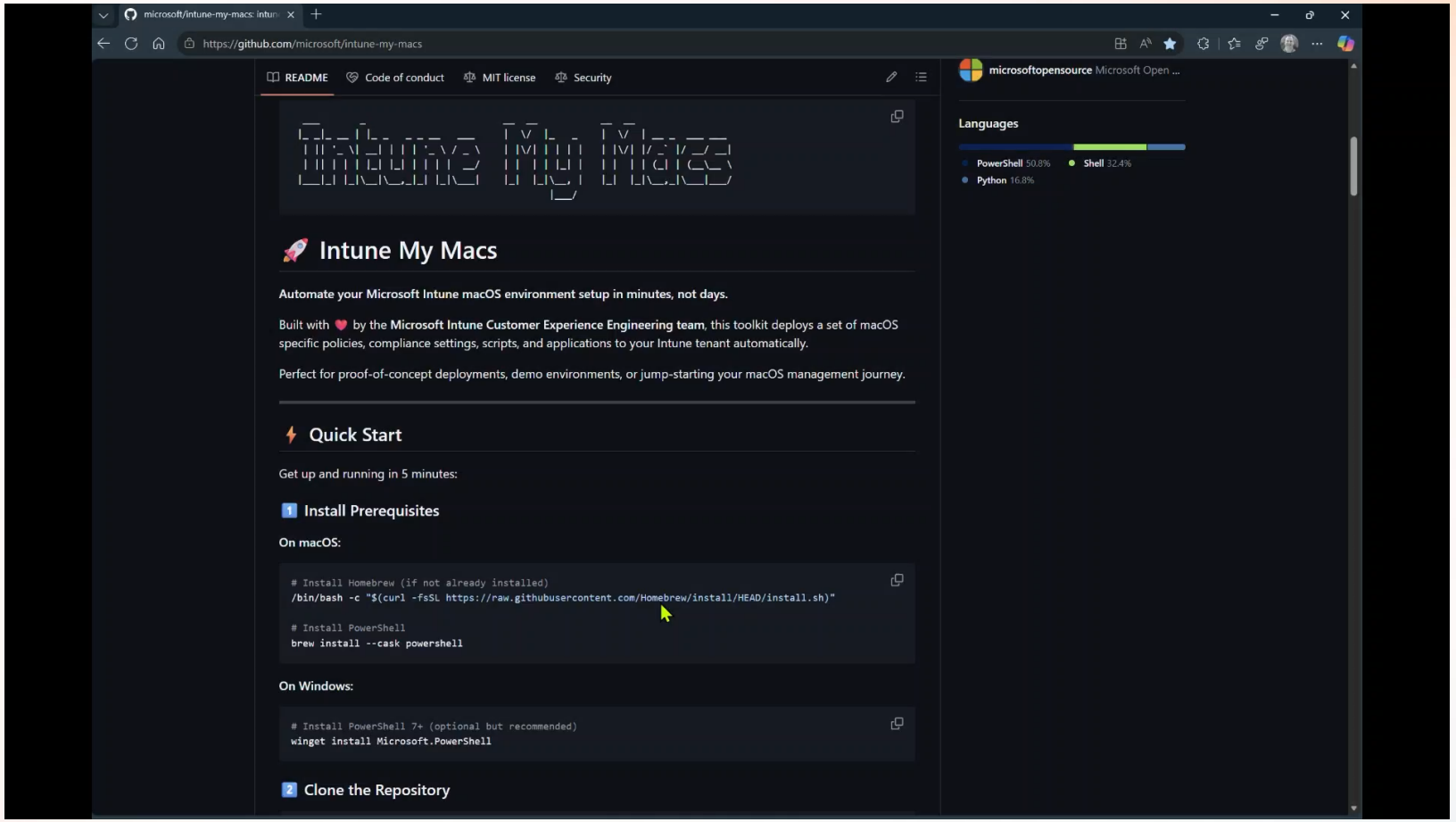
Day-2 Tools

Policy export · Conflict detection · Auto-generated documentation

GET STARTED Dry-run by default · --apply to commit · --remove-all to clean up

```
git clone https://github.com/microsoft/intune-my-macs.git && pwsh ./mainScript.ps1
```

/* Start Managing macOS with Intune*/



https://aka.ms/intunemacpoc

/* The Microsoft Mac Admins Community! */

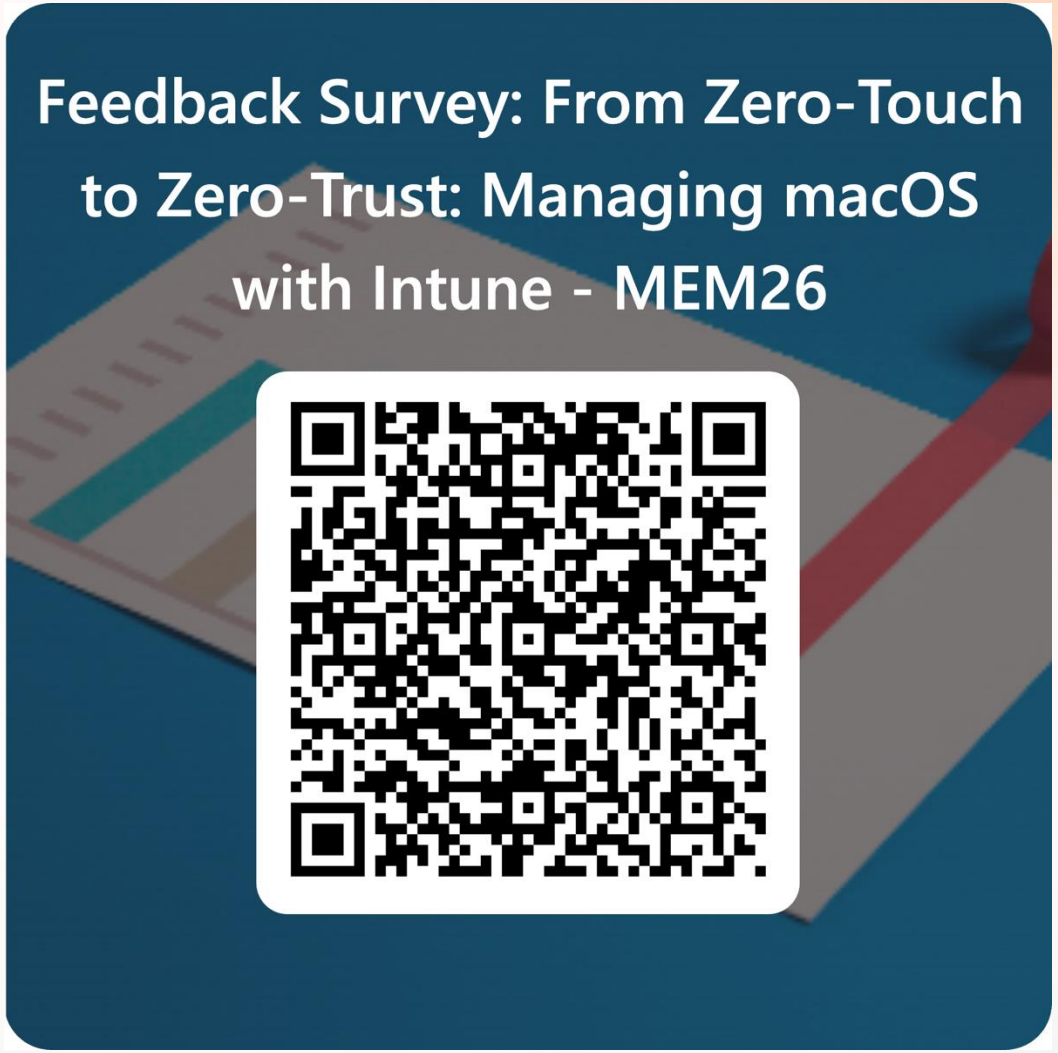
ENDPOINT MANAGEMENT SUMMIT 2026

LinkedIn

aka.ms/MacAdmins

You can join it with just one click

Thanks!


Feedback Survey: From Zero-Touch to Zero-Trust: Managing macOS with Intune - MEM26