

Streamlining macOS operations - Empowering efficiency with Microsoft Intune



MacSysAdmin 2024

Marc Nahum

Senior Program Manager

[linkedin.com/in/marc-nahum](https://www.linkedin.com/in/marc-nahum)





Agenda

Key takeaways:

- macOS devices can be managed the same way as other devices in the enterprise.
- Intune keep your Apple devices secured

● What is Intune and where are we?

Past, current and future roadmap

● Onboarding

Await final config, FileVault, ect...

● Device Configuration

Direct Import, Zero Day, DDM



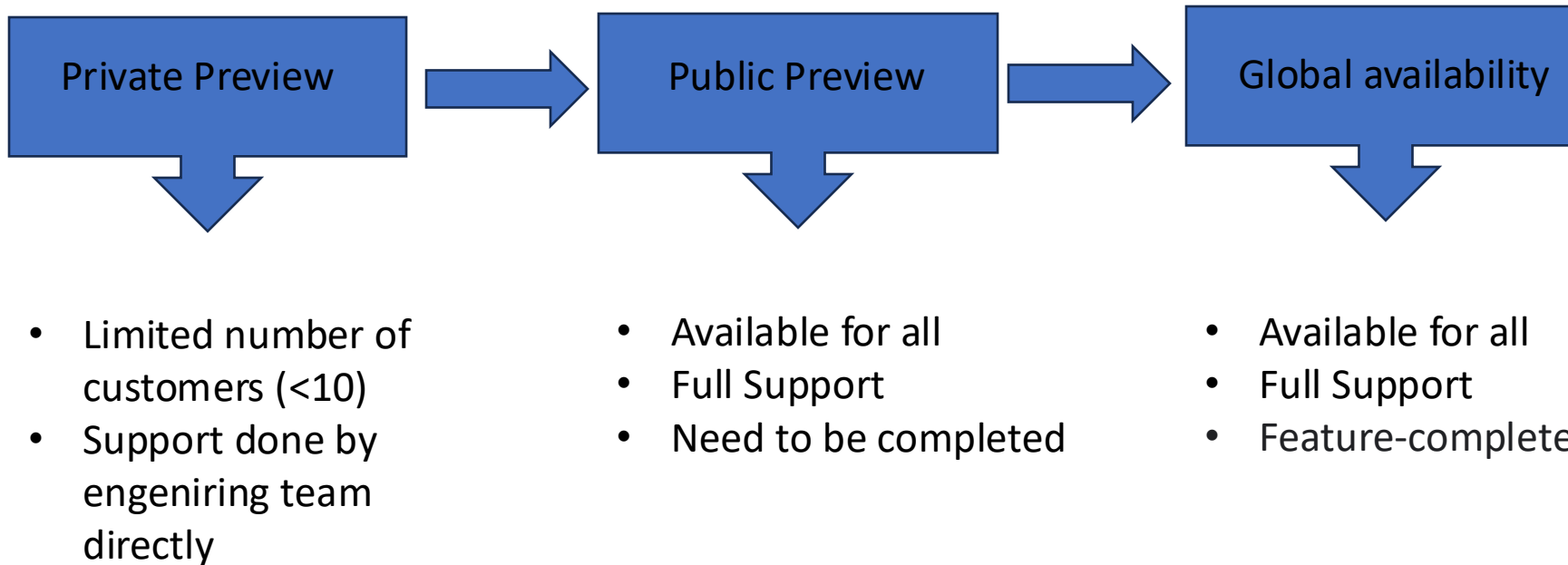
● Platform SSO

A Swiss knife or an Iceberg?

● Applications & Suite

Flexible App and Remote Help

Terminology





Intune macOS snapshot

Endpoint Security

- Firewall
- FileVault (Disk encryption)
- Gatekeeper
- Activation Lock
- Rapid Security Response

Conditional Access

- Device compliance

Enrollment

- ADE with modern auth
- Local account management
- Await final configuration
- Platform SSO and passkeys

Configuration

- Entra single sign-on extension
- LDAP (AD)
- Restriction policies
- Custom policy support (iMazing)
- Passcode policies
- Software update
- Enterprise certificates/PKI
- Network configuration/ Proxy server
- Login window
- Managed login items
- Content caching
- Settings picker
- Device actions (Erase, Restart, etc.)
- DDM software update
- FileVault during setup assistant

3rd party integration

- Munki (App lifecycle)
- Privileges (Elevation control)
- Santa (Binary access control)
- Octory (Onboarding splash screen)
- Nudge (OS update controls)

Scripting

- User/Root scripts with schedules
- Custom attribute collection

Intune Suite

- Remote Help with full control
- Cloud PKI support

Apps

- DMG, PKG support & Available assignment
- Custom PKG pre/post install scripts
- Native integrations for Edge, Office, and Defender
- Config for Edge, Office, Defender, and OneDrive
- Custom preference
- Volume-purchased apps

Coming soon

- Custom app detection
- User channel support for resource access profiles
- Recovery lock management
- JIT compliance remediation
- Default hardware-bound Entra registration

 New in last 12 months

Intune is the only needed solution for macOS management.



Agenda

● What is Intune and where are we?

Past, current and future roadmap

● Onboarding

Await final config, FileVault, ect...

● Device Configuration

Direct Import, Zero Day, DDM

Platform SSO

A Swiss knife or an Iceberg?

● Applications & Suite

Flexible App and Remote Help



Await configuration after Automated Device Enrollment

Create a more secure onboarding experience by guaranteeing that the Mac is configured before releasing to the user.

User remains within Setup Assistant experience until first device check-in completes.

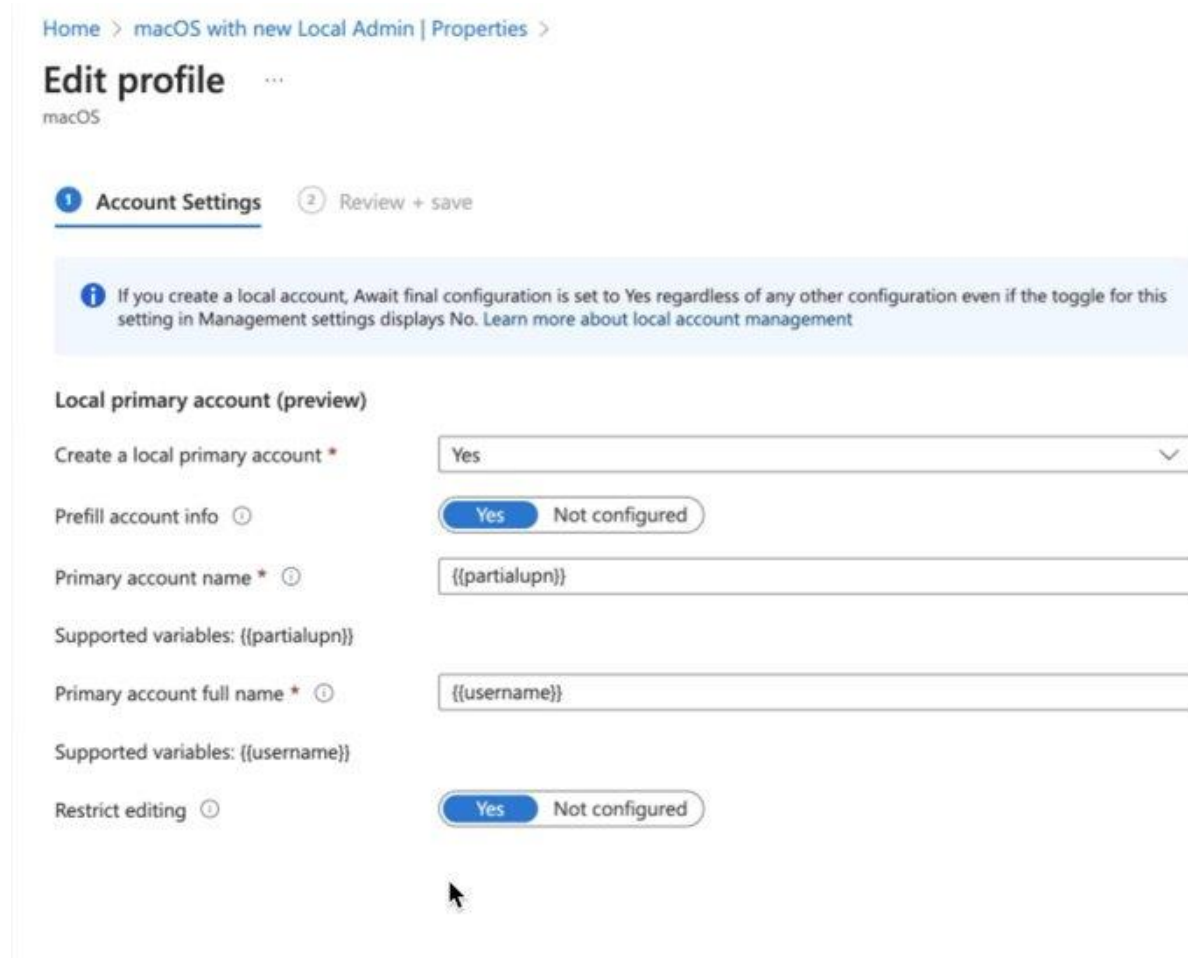
The screenshot shows the Microsoft Intune admin center interface for creating a macOS profile. The breadcrumb trail is: Home > Devices | macOS > macOS | macOS enrollment > Enrollment program tokens > Woodgrove.ms | Profiles >. The page title is "Create profile" for macOS. The progress indicator shows five steps: 1. Basics (checked), 2. Management Settings (active), 3. Setup Assistant, 4. Account Settings, and 5. Review + create. Below the progress indicator, there is a description: "Define enrollment and management settings for your macOS devices. [Learn more.](#)". The "User Affinity & Authentication Method" section includes a "User affinity" dropdown menu set to "Select an option". The "Management Options" section is highlighted with a blue box and contains a toggle for "Await final configuration" which is currently set to "Yes". Below this, there is a "Locked enrollment" dropdown menu also set to "Select an option".

Local Account management

- Create and configure local admin and primary account on ADE enrolled Macs
- Admin account Azure AD LAPS integration for Mac.

Coming in 2 parts:

- Configure and restrict editing
- Set standard and create management admin account
- LAPS for macOS (2025)



Home > macOS with new Local Admin | Properties >

Edit profile

macOS

1 Account Settings 2 Review + save

i If you create a local account, Await final configuration is set to Yes regardless of any other configuration even if the toggle for this setting in Management settings displays No. [Learn more about local account management](#)

Local primary account (preview)

Create a local primary account *

Prefill account info ⓘ Yes Not configured

Primary account name * ⓘ

Supported variables: {{partialupn}}

Primary account full name * ⓘ

Supported variables: {{username}}

Restrict editing ⓘ Yes Not configured

FileVault during Setup Assistant

Starting macOS 14, you can enforce FileVault encryption within Setup Assistant before the user can access company resources.

FileVault

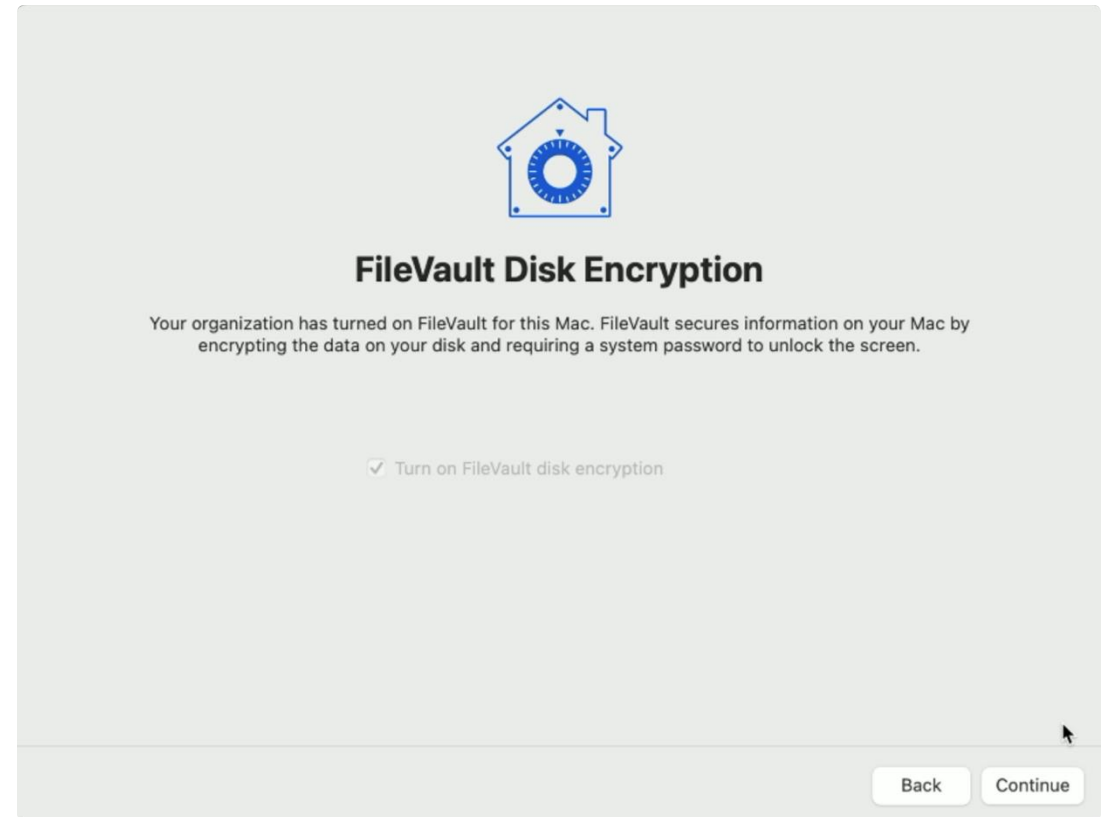
Configure the FileVault payload to manage FileVault disk encryption settings on devices.

Defer ⓘ	Enabled
Enable ⓘ	On
Force Enable In Setup Assistant ⓘ	True

FileVault Options

Configure the FileVault Options payload to customize FileVault disk encryption settings on devices.

Prevent FileVault From Being Disabled ⓘ	True
---	------



Managed device attestation with ACME

Strongest proof of hardware-bound (secure enclave) device identity that is attested to by Apple.

Managed Macs can provide the trusted attestation to prove device identity to servers.

Initiated via MDM, it protects the Intune enrollment cert against device spoofing.

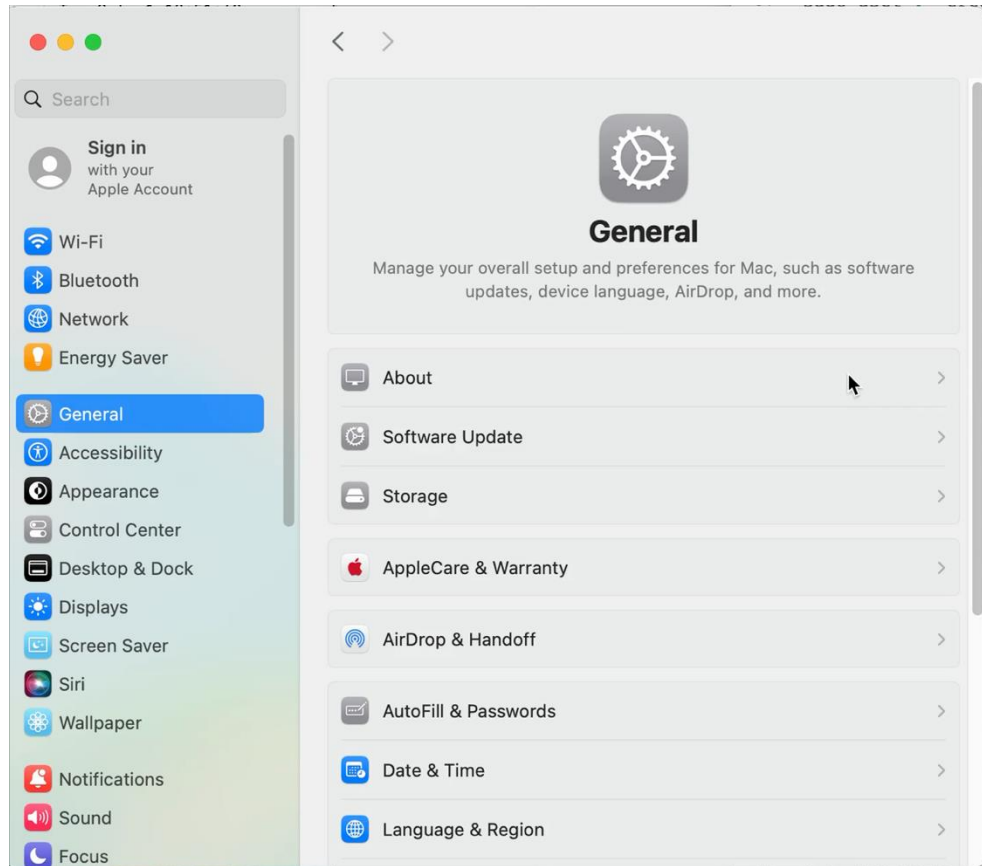
Currently in private preview.

Sequoia only



Joel Slide's

Intune not InTune!



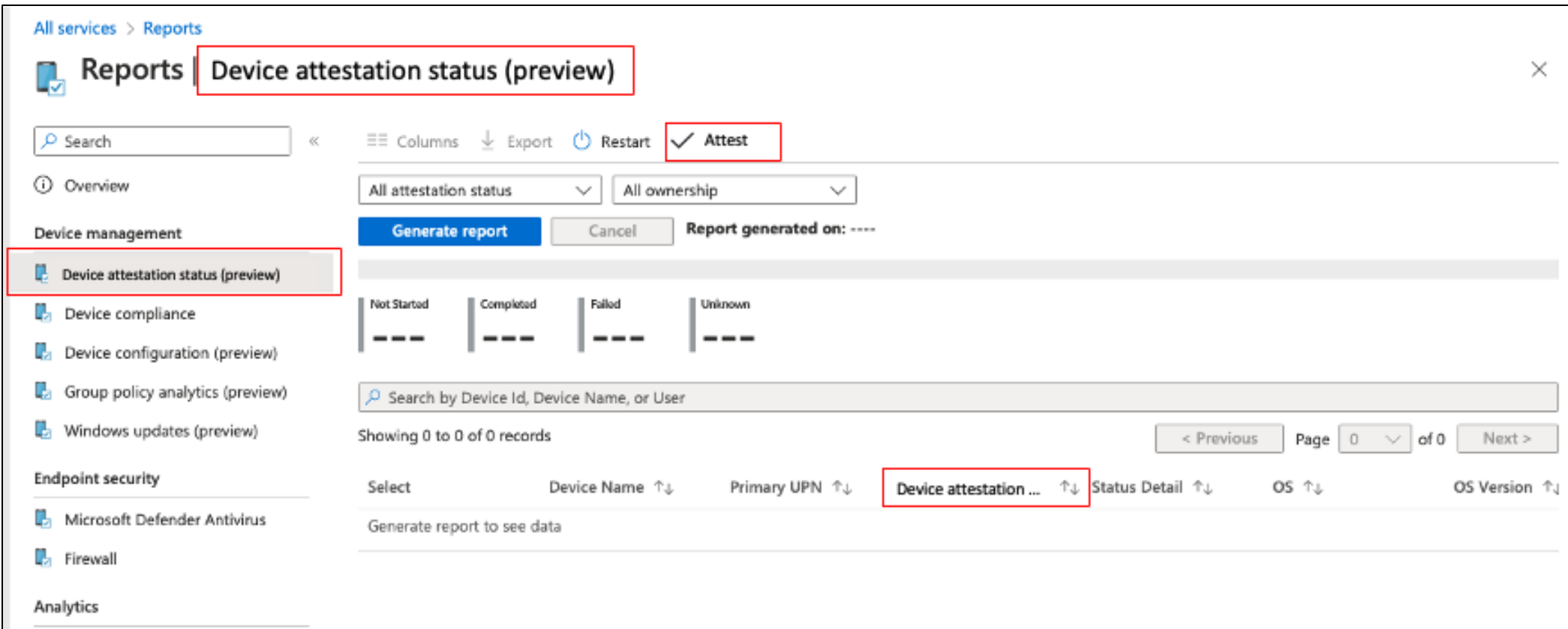
Every device check-in which is every 8 hours, the device will try to connect to Intune and that's where Intune will check if the certificate is valid or not.

- if its not valid - we fail the check-in
- if its valid - we proceed with the check-in

if the device fails to check-in after XX days ; the device will be out of compliance after XX days as set by admin. once the device is out of compliance, the user will lose their access to resources.

Note: The ACME cert is valid for 1 year, and between 6 months and 1 year, we attempt renewal to give one more year of validity to it.

- Reports > Device attestation status
- Cross platform – Attested Windows and iOS/iPadOS and macOS devices show up here



All services > Reports

Reports | Device attestation status (preview)

Search

Columns Export Restart **Attest**

All attestation status All ownership

Generate report Cancel Report generated on: ----

Not Started Completed Failed Unknown

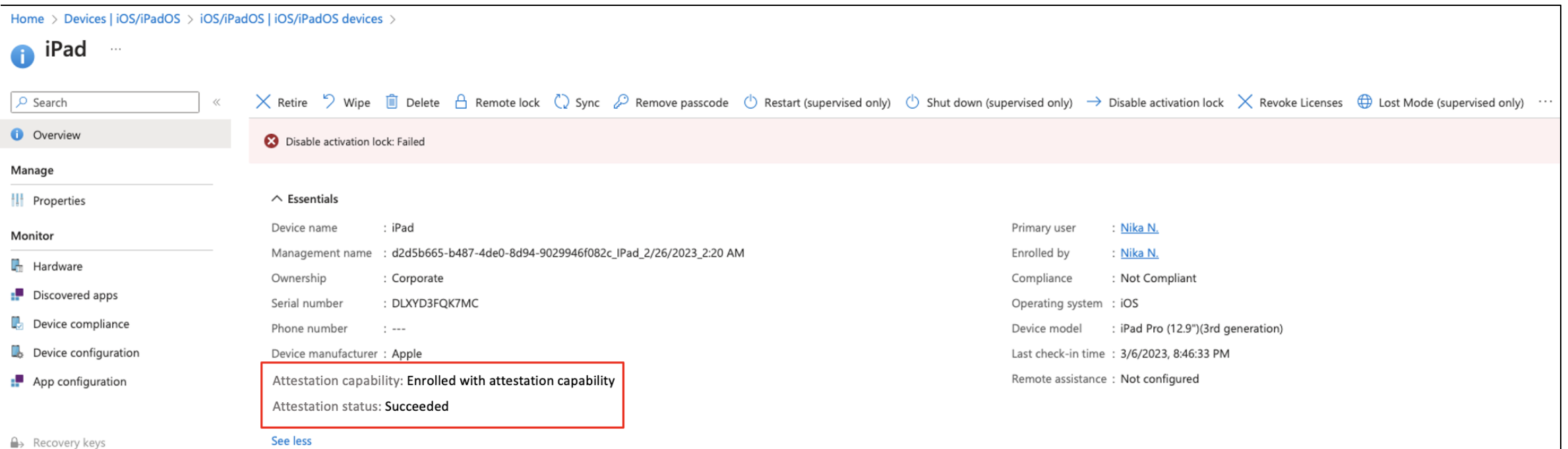
Search by Device Id, Device Name, or User

Showing 0 to 0 of 0 records < Previous Page 0 of 0 Next >

Select	Device Name ↑↓	Primary UPN ↑↓	Device attestation ... ↑↓	Status Detail ↑↓	OS ↑↓	OS Version ↑↓
Generate report to see data						

- Devices > iOS/iPadOS (or macOS) > choose a device > Overview > See more > **Attestation capability** and **Attestation status**
- **Attestation capability**
 - Enrolled with attestation capability
 - Enrolled without attestation capability * (Mac VMs / Shared iPads)

- **Attestation status**
 - Not tried
 - Failed
 - Succeeded
 - Not supported due to hardware
 - Not supported due to OS
 - Incomplete data from device
 - Attestation not offered



Home > Devices | iOS/iPadOS > iOS/iPadOS | iOS/iPadOS devices >

iPad ...

Search

Retire Wipe Delete Remote lock Sync Remove passcode Restart (supervised only) Shut down (supervised only) Disable activation lock Revoke Licenses Lost Mode (supervised only)

Disable activation lock: Failed

Manage

Properties

Monitor

Hardware

Discovered apps

Device compliance

Device configuration

App configuration

Recovery keys

Essentials

Device name	: iPad	Primary user	: Nika N.
Management name	: d2d5b665-b487-4de0-8d94-9029946f082c_iPad_2/26/2023_2:20 AM	Enrolled by	: Nika N.
Ownership	: Corporate	Compliance	: Not Compliant
Serial number	: DLXYD3FQK7MC	Operating system	: iOS
Phone number	: ---	Device model	: iPad Pro (12.9")(3rd generation)
Device manufacturer	: Apple	Last check-in time	: 3/6/2023, 8:46:33 PM
Attestation capability	: Enrolled with attestation capability	Remote assistance	: Not configured
Attestation status	: Succeeded		

[See less](#)



Admin console – Enrollment restriction & filter

Edit rule syntax



You can create or edit rules directly by editing the syntax in the box below. Note that changes made here may not be reflected in the rule builder.

```
(device.isDeviceAttested -eq "False")
```

Edit rule syntax



You can create or edit rules directly by editing the syntax in the box below. Note that changes made here may not be reflected in the rule builder.

```
(device.isDeviceAttested -eq "True")
```

Home > Devices | Enroll devices > Enroll devices | Enrollment device platform restrictions >

Create restriction

Device type restriction

- ✓ Basics
- ✓ Platform settings
- ✓ Scope tags
- ④ Assignments
- ⑤ Review + create

Specify the platform configuration restrictions that must be met for a device to enroll. Use compliance policies to restrict devices after enrollment. Define versions as major.minor.build. Version restrictions only apply to devices enrolled with the Company Portal. Intune classifies devices as personally-owned by default. Additional action is required to classify devices as corporate-owned. [Learn more.](#)

MDM

Allow **Block**

Allow min/max range:

Min Max

Personally owned devices

Allow Block

Create restriction

Device type restriction

- ✓ Basics
- ✓ Platform settings
- ✓ Scope tags
- ④ Assignments
- ⑤ Review + create

Included groups

Add groups Add all users

Groups	Group Members ①	Filter	Filter mode	Edit filter	Remove
All users		isDeviceAttested	Include	Edit filter	Remove



Agenda

● What is Intune and where are we?

Past, current and future roadmap

● Onboarding

Await final config, FileVault, ect...

● Device Configuration

Direct Import, Zero Day, DDM

🔒 Platform SSO

A Swiss knife or an Iceberg?

● Applications & Suite

Flexible App and Remote Help



```

title: Disk Management:Settings
description: Use this configuration to install disk management settings on the device.
payload:
  declarationtype: com.apple.configuration.diskmanagement.settings
  supportedOS:
    iOS:
      introduced: n/a
    macOS:
      introduced: '15.0'
      allowed-enrollments:
        - supervised
        - local
      allowed-scopes:
        - system

```

```

- key: ExternalStorage
  title: External Storage
  type: <string>
  presence: optional
  rangelist:
    - Allowed
    - ReadOnly
    - Disallowed

```

1. Apple YAML

```

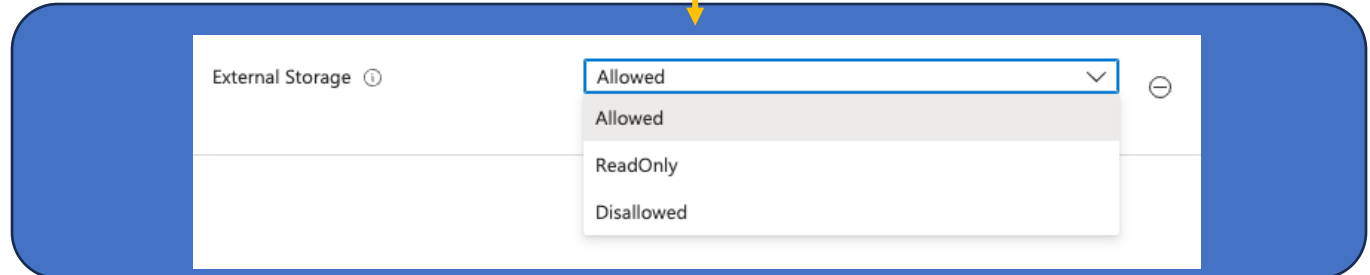
{Name": "com.apple.configuration.diskmanagement.settings",
  "Applicability":
    "VersionApplicabilities": [
      {
        "InternalVersionRange": "[15.0,)",
        "DeviceType": 4,
        "Constraints": 0
      }
    ],
  "FriendlyName": "External Storage",
  "Description": "Specifies the mount policy for external storage:
  "OptionValue": {
    "OptionType": "String",
    "Value": "Allowed"
  },
  "OptionValue": {
    "OptionType": "String",
    "Value": "ReadOnly"
  },
  "OptionValue": {
    "OptionType": "String",
    "Value": "Disallowed"
  },

```

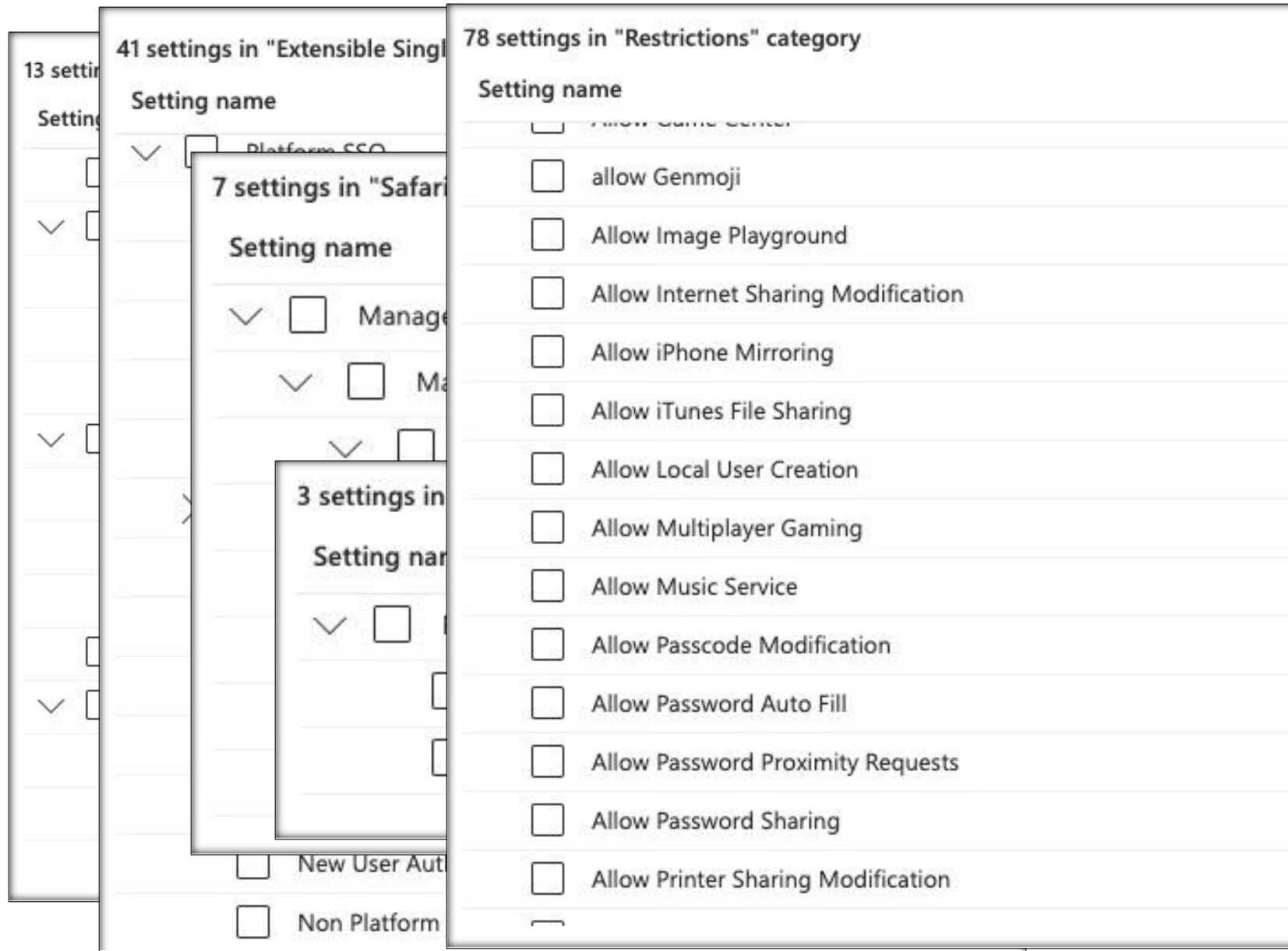
2. Processed JSON understood by Apple Settings Catalog



Settings Catalog



New features, zero day support



The image shows a screenshot of the Windows Settings application with several windows open, illustrating the 'New features, zero day support' theme. The windows display various settings categories:

- 41 settings in "Extensible Single..."**: Shows settings like "Platform SSO".
- 7 settings in "Safari..."**: Shows settings like "Manage...", "Ma...", and "3 settings in...".
- 78 settings in "Restrictions" category**: Lists various system restrictions such as "allow Genmoji", "Allow Image Playground", "Allow Internet Sharing Modification", "Allow iPhone Mirroring", "Allow iTunes File Sharing", "Allow Local User Creation", "Allow Multiplayer Gaming", "Allow Music Service", "Allow Passcode Modification", "Allow Password Auto Fill", "Allow Password Proximity Requests", "Allow Password Sharing", and "Allow Printer Sharing Modification".



aka.ms/AppleDayZero
aka.ms/Intune/Apple-Intelligence

Settings Catalog inc. Variables



- Before Settings Catalog, new features would take 2 sprints (8 weeks)
- Last year's day zero work for Sonoma took 3 days before we could begin testing. Less than 24h for Sequoia
- Now the process is automated. Once approved, New payloads go for immediate testing.
- We can even use variables in the payloads from Entra ID.

1 Configuration settings 2 Review + save

+ Add settings ⓘ

^ Microsoft Office Remove category

Microsoft Office Remove subcategory

ⓘ 18 of 20 settings in this subcategory are not configured

Enable automatic sign-in ⓘ True ⓘ

Office Activation Email Address ⓘ ⓘ

Microsoft Outlook Remove subcategory

ⓘ 22 of 24 settings in this subcategory are not configured

Enable New Outlook ⓘ ⓘ

Hide the 'Get started with Outlook' control in the task pane ⓘ True ⓘ

Declarative device management

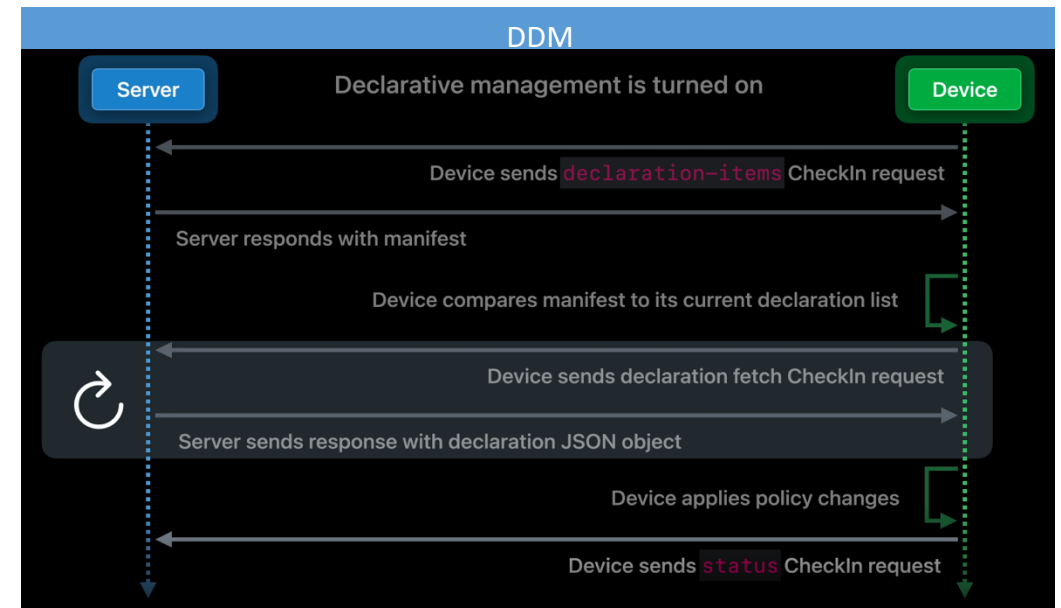
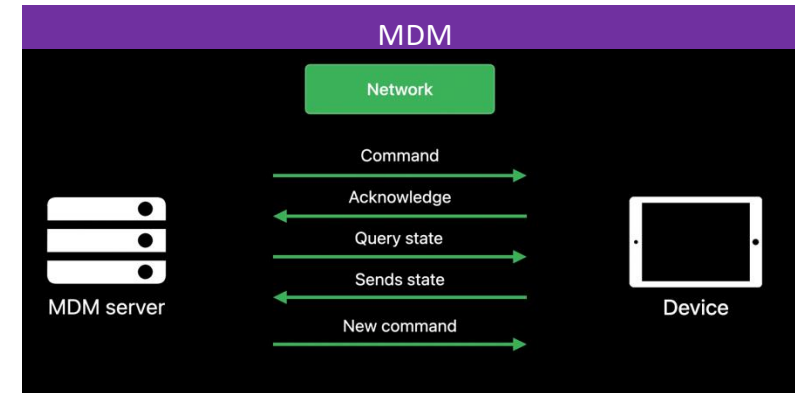
DDM is a new paradigm that can coexist with MDM.

MDM is imperative and reactive.

- Multiple round trips between Intune and devices
- SW update based on 4 commands, not scalable

DDM is declarative and proactive.

- Admin configures desired state
- Device applies policy to itself
- Rich, async status updates



Declarative Software Updates



New DDM configuration for software update enforcement!

Specify OS/build to install by an exact time

Only Version and date are mandatory



Do not use Sequoia settings in Sonoma

Create profile ... ×
macOS - Settings catalog

✓ Basics **2 Configuration settings** ③ Scope tags ④ Assignments ...

[+ Add settings](#) ⓘ

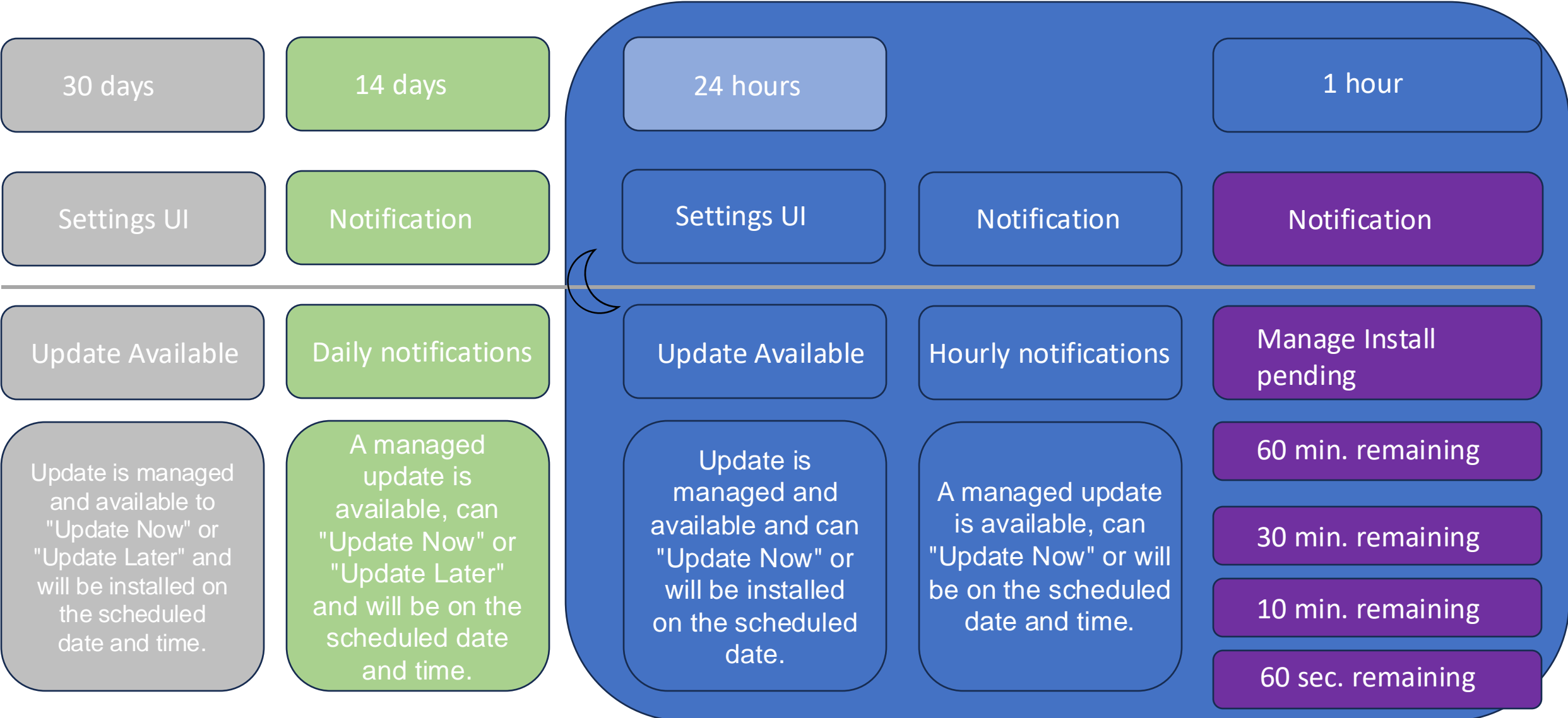
^ Declarative Device Management (preview) [Remove category](#)

These settings configure the declarations used by Apple's declarative device management feature. These settings are separate from older MDM settings and only apply to a device enabled for declarative management. Learn more about declarative management at developer.apple.com

Software Update [Remove subcategory](#)

Details URL ⓘ	<input type="text" value="https://support.apple.com/en-us/HT213895"/> ✓ ⊖
Target Build Version ⓘ	<input type="text" value="23B81"/> ✓ ⊖
Target Local Date Time * ⓘ	<input type="text" value="12/15/2023"/> <input type="text" value="12:00 AM"/>
Target OS Version ⓘ	<input type="text" value="14.1.1"/> ✓

Declarative Software Updates



DDM Settings

[Remove subcategory](#)

Declarative Device Management

These settings configure the declarative management at developer. These settings separate from older MDM settings and declarative management at developer.

Disk Management

Restrictions

External Storage ⓘ

Network Storage ⓘ

Declarative Device Management (DDM)

These settings configure the declarative management at developer. These settings separate from older MDM settings and declarative management at developer.

Passcode

i 10 of 17 settings in this subcategory

Passcode Reuse Limit * ⓘ

Minimum Passcode Length * ⓘ

Maximum Passcode Age In Days *

Minimum Complex Characters * ⓘ

Maximum Number of Failed Attempts ⓘ

Maximum Grace Period * ⓘ

Failed Attempts Reset In Minutes * ⓘ

Declarative Management

These settings separate from declarative management at developer.

Software

Details URL

Target Build

Target Data

Target OS

Software Update Settings

Allow Standard User OS Updates ⓘ Allowed ⓘ

Automatic Actions

Download ⓘ

Allowed ⓘ

Install OS Updates ⓘ

Allowed ⓘ

Install Security Update ⓘ

Allowed ⓘ

Deferrals

Major Period In Days * ⓘ

0 ⓘ

Minor Period In Days * ⓘ

0 ⓘ

System Period In Days * ⓘ

0 ⓘ

Notifications ⓘ

Enabled ⓘ

Rapid Security Response

Enable ⓘ

Enabled ⓘ

Certificate deployment in user keychain

- Admin can choose which keychain (device/user) resource access profile or certs are delivered to.
- By default, device keychain will be used.
- Scope: SCEP, PKCS, WiFi, VPN, Wired network, trusted (root) cert profiles.

✓ Basics 2 Configuration settings 3 Assignments 4 Review + create

Deployment channel * ⓘ

Device channel
Device channel
User channel



Agenda

- **What is Intune and where are we?**

Past, current and future roadmap

- **Onboarding**

Await final config, FileVault, ect...

- **Device Configuration**

Direct Import, Zero Day, DDM

-  **Platform SSO**

A Swiss knife or an Iceberg?

- **Applications & Suite**

Flexible App and Remote Help



Platform SSO: Swiss knife of macOS authentication



Allows logging on to your Mac using Entra ID password.

Platform SSO Breakdown

Home > Devices | macOS > macOS | Configuration profiles > Platform SSO config >

Edit profile - Platform SSO config

Settings catalog

1 Configuration settings 2 Review + save

+ Add settings ⓘ

Authentication Remove category

Extensible Single Sign On (SSO) Remove subcategory

Configure an app extension that enables single sign-on (SSO) for devices.

i 24 of 35 settings in this subcategory are not configured

Authentication Method (Deprecated) ⓘ Password ⊖

Registration Token ⓘ {{(DEVICEREGISTRATION)}} ⊖

Platform SSO ⊖

Authentication Method ⓘ Password ⊖

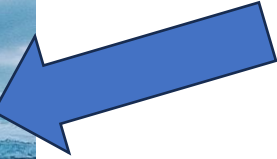
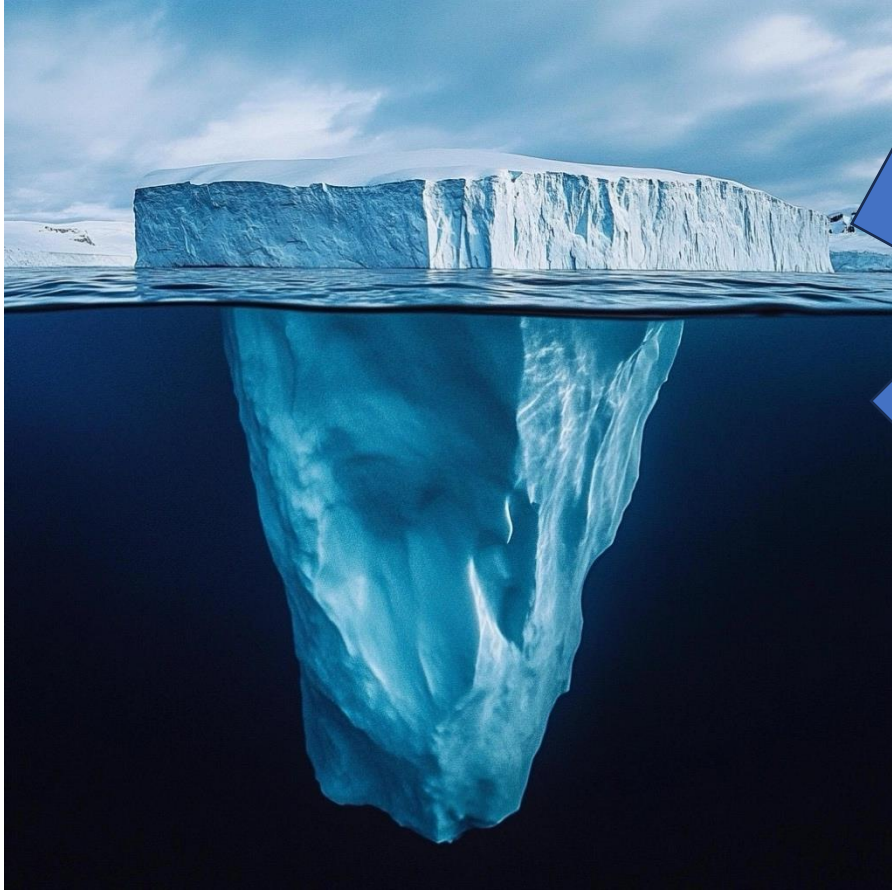
Applies to macOS 13.x



Applies to macOS 14.x and later



Platform SSO: Swiss knife of macOS authentication



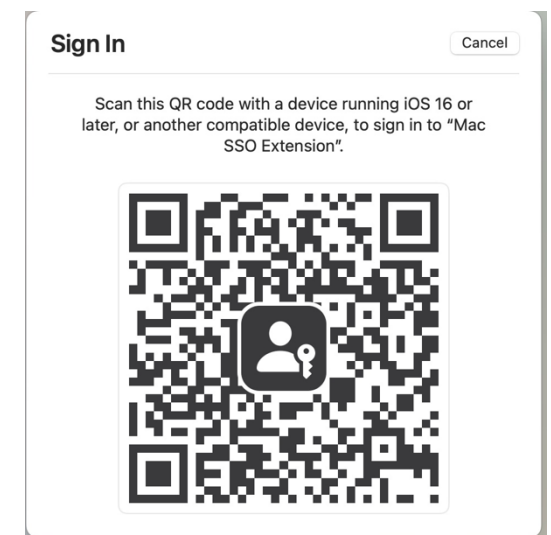
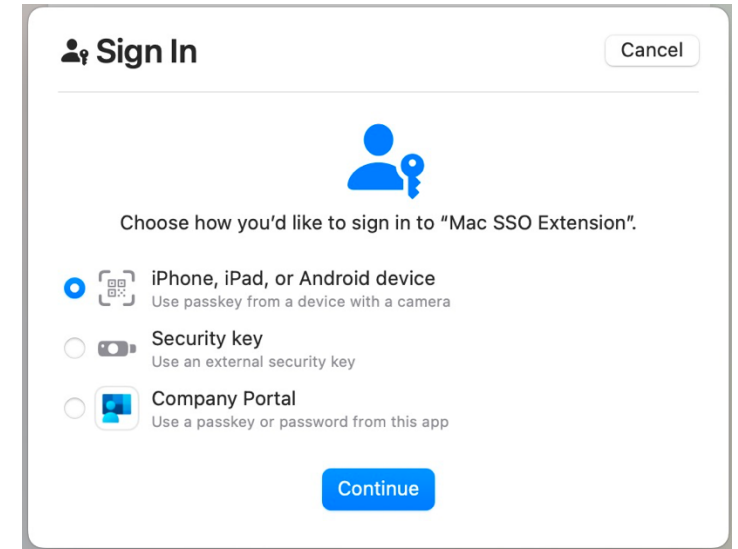
Allows logging on to your Mac using Entra ID password.



Secure the access with Secure enclave

Platform SSO Breakdown

- Secure Enclave is working with:
- Password
- Yubikey
- Passkey

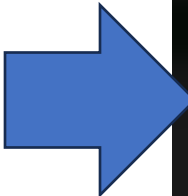


Platform SSO Breakdown

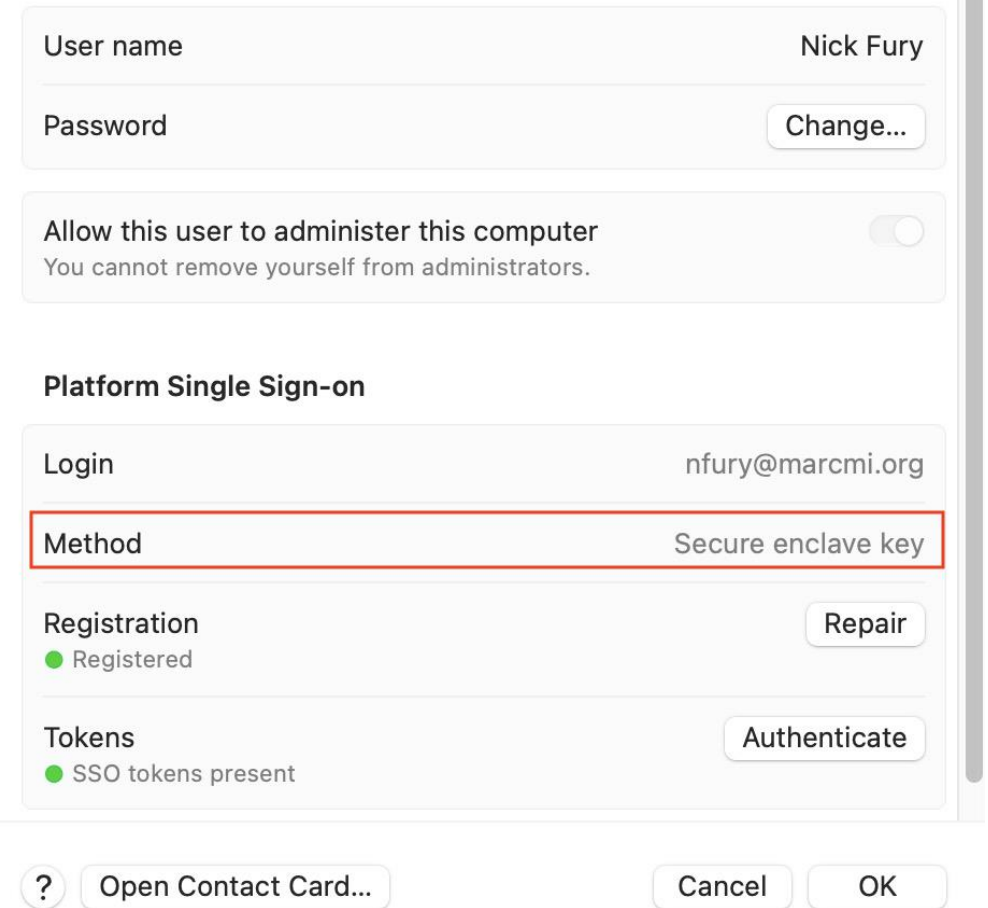


Secure enclave storage is an alternative

- No Password synchronisation with the local account
- Secure the cloud & the token
- App-sso platform –s



```
User Configuration:
{
  "_sepKeyData" : "qz7yHHod8Feq1Cs+v4IdoGrK4X06UoZXvwR2fTRSsL4="
  "created" : "2023-10-02T19:35:13Z",
  "lastLoginDate" : "2023-10-02T19:34:51Z",
  "loginType" : "POLoginTypeUserSecureEnclaveKey (2)",
  "state" : "POUserStateNormal (0)",
  "uniqueIdentifier" : "EE312758-E195-405D-8D39-D432559DCE3D",
  "userLoginConfiguration" : {
    "created" : "2023-10-02T19:35:13Z",
    "loginUserName" : "v***e@lab6523.onmicrosoft.com"
  },
  "version" : 1
}
```



User name: Nick Fury

Password: [Redacted] [Change...](#)

Allow this user to administer this computer
 You cannot remove yourself from administrators.

Platform Single Sign-on

Login: nfury@marcmi.org

Method: Secure enclave key

Registration: Registered [Repair](#)

Tokens: SSO tokens present [Authenticate](#)

[Open Contact Card...](#) [Cancel](#) [OK](#)

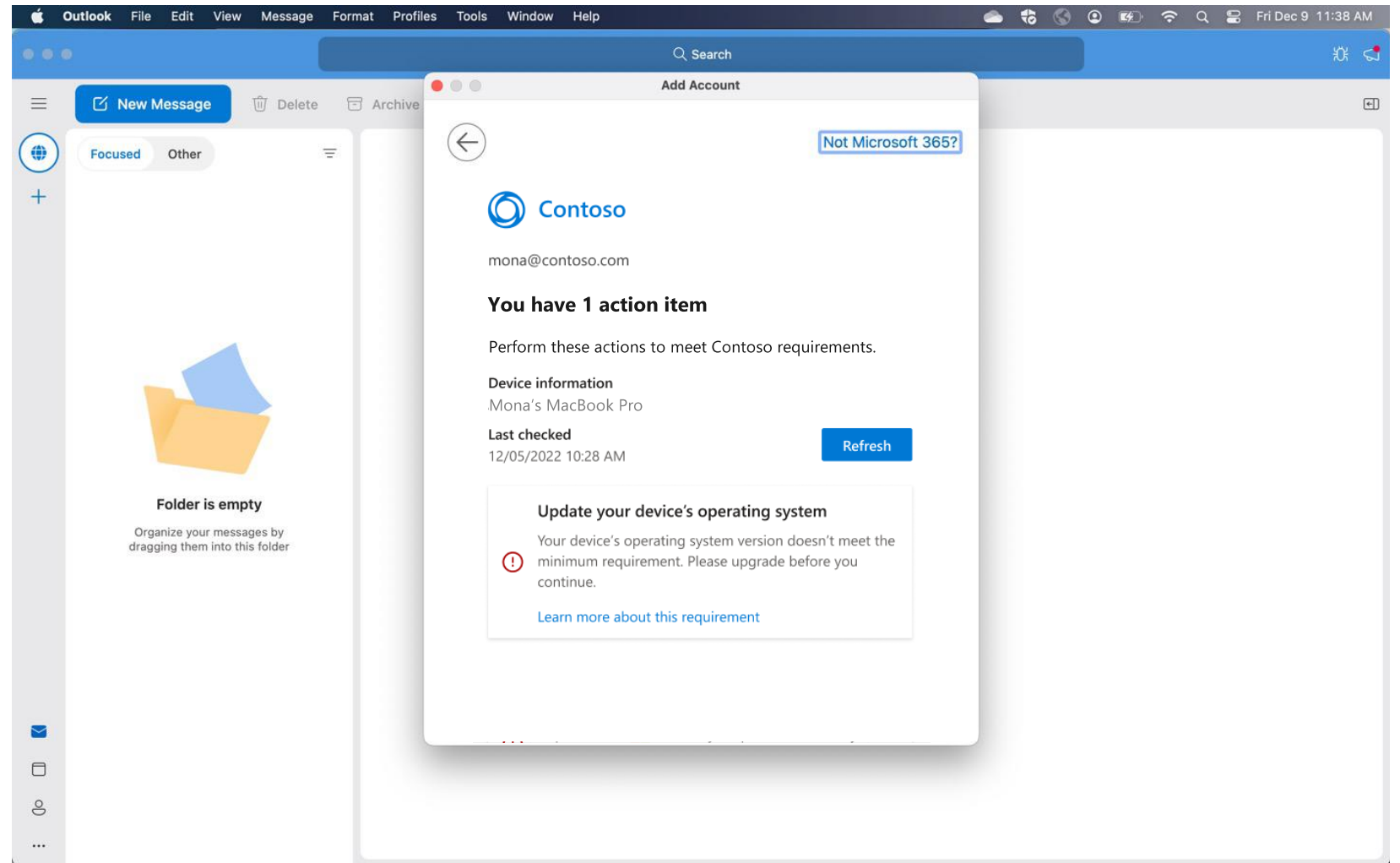
Platform SSO Breakdown (JIT Included)



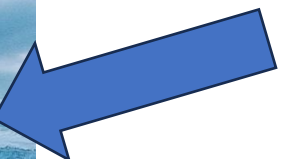
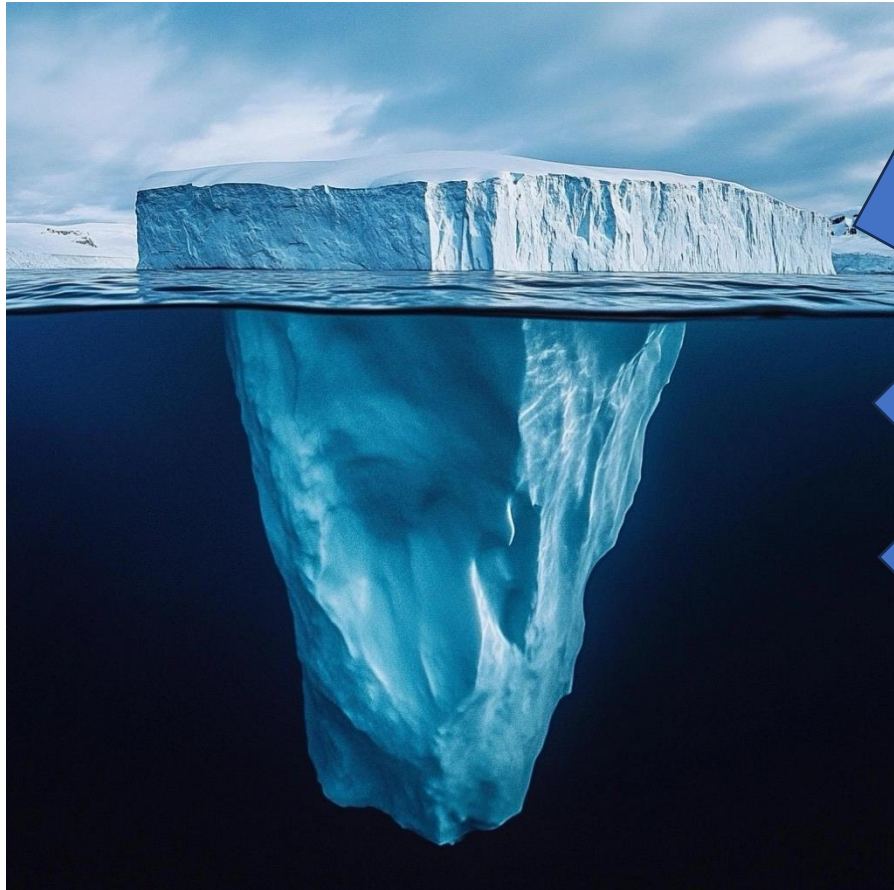
Noncompliance
detection and
remediation experience
from within protected
apps.

Company Portal app is
not required!

Based on AAD SSO ext,
any app using MSAL can
benefit.



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

- New features in Platform SSO public preview:
 - Smartcard as an authentication method.
 - Enable Entra ID user creation at login.
 - Kerberos support.
 - Standard/admin privilege management.
- Coming later:
 - Granular privilege management using admin-configurable authorization mode.

Authentication Method ⓘ

SmartCard

Password

UserSecureEnclaveKey

SmartCard

Enable Create User At Login ⓘ

Enabled

New User Authorization Mode ⓘ

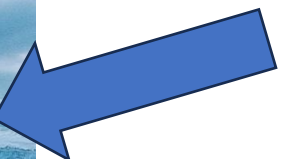
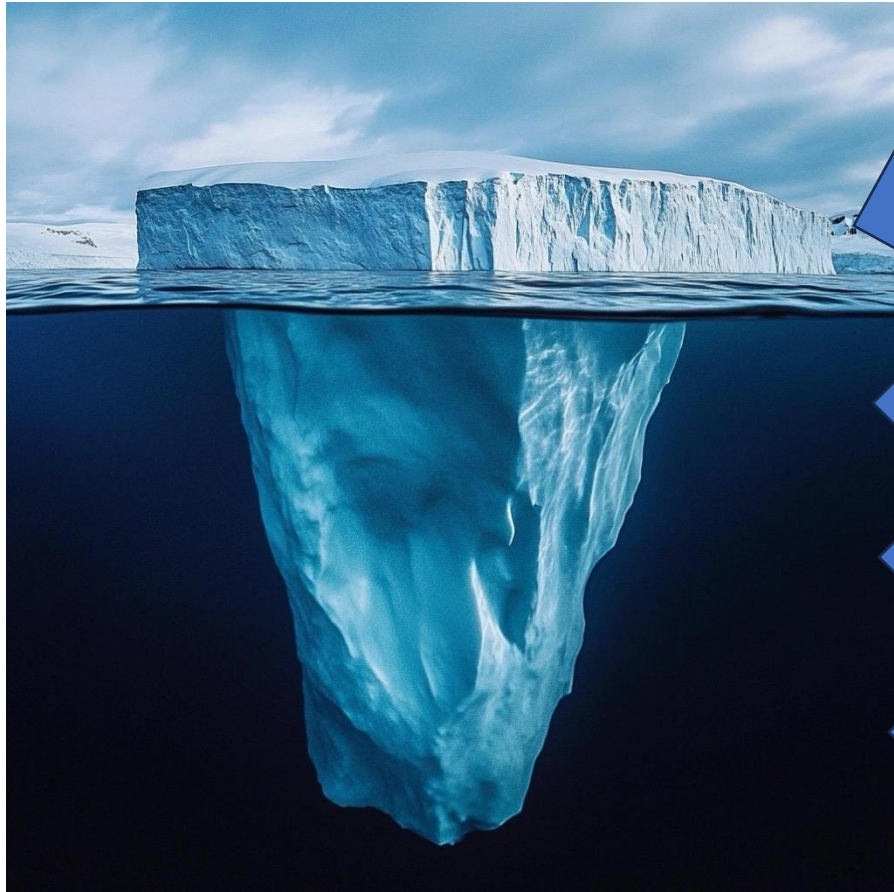
Standard

Standard

Admin

Groups

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

Platform SSO: Swiss knife of macOS authentication



?

Password Synchronization


Your previous macOS password is required to enable offline log in.


You can proceed with the current Microsoft Entra password, but previous Keychain and protected data will no longer be accessible.

Enter Previous Password

Use Microsoft Entra Password

Cancel

?




Do you want to use the "Microsoft Entra" password?

Your macOS password will be replaced. The previous Keychain and protected data will no longer be accessible.

Cancel

Change

Cancel



Account Updated

Your password has been synchronized with your Microsoft Entra account.



Agenda

● What is Intune and where are we?

Past, current and future roadmap

● Onboarding

Await final config, FileVault, ect...

● Device Configuration

Direct Import, Zero Day, DDM

🔒 Platform SSO

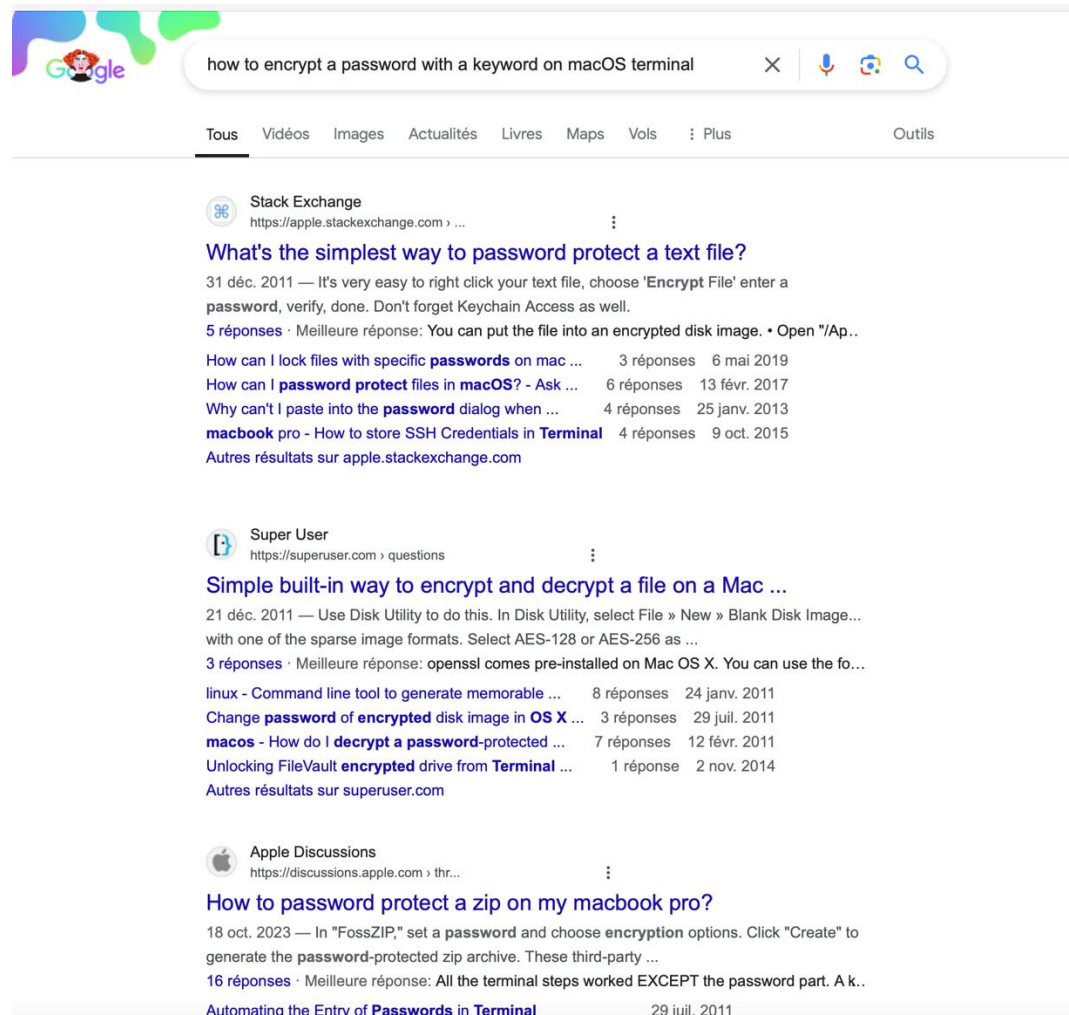
A Swiss knife or an Iceberg?

● Applications & Suite

Flexible App and Remote Help



Admin: "I want a local admin account, with an encrypted password, and have my service desk be able to unencrypt it"



The screenshot shows a Google search interface with the query "how to encrypt a password with a keyword on macOS terminal". The search results are displayed in a list format, showing the source, title, and a brief description of each result.

- Stack Exchange** (https://apple.stackexchange.com):
 - What's the simplest way to password protect a text file?**
31 déc. 2011 — It's very easy to right click your text file, choose 'Encrypt File' enter a password, verify, done. Don't forget Keychain Access as well.
5 réponses · Meilleure réponse: You can put the file into an encrypted disk image. • Open "Ap...
 - How can I lock files with specific passwords on mac ... 3 réponses 6 mai 2019
 - How can I password protect files in macOS? - Ask ... 6 réponses 13 févr. 2017
 - Why can't I paste into the password dialog when ... 4 réponses 25 janv. 2013
 - macbook pro - How to store SSH Credentials in Terminal 4 réponses 9 oct. 2015
- Super User** (https://superuser.com > questions):
 - Simple built-in way to encrypt and decrypt a file on a Mac ...**
21 déc. 2011 — Use Disk Utility to do this. In Disk Utility, select File » New » Blank Disk Image... with one of the sparse image formats. Select AES-128 or AES-256 as ...
3 réponses · Meilleure réponse: openssl comes pre-installed on Mac OS X. You can use the fo...
 - linux - Command line tool to generate memorable ... 8 réponses 24 janv. 2011
 - Change password of encrypted disk image in OS X ... 3 réponses 29 juil. 2011
 - macos - How do I decrypt a password-protected ... 7 réponses 12 févr. 2011
 - Unlocking FileVault encrypted drive from Terminal ... 1 réponse 2 nov. 2014
- Apple Discussions** (https://discussions.apple.com > thr...):
 - How to password protect a zip on my macbook pro?**
18 oct. 2023 — In "FossZIP," set a password and choose encryption options. Click "Create" to generate the password-protected zip archive. These third-party ...
16 réponses · Meilleure réponse: All the terminal steps worked EXCEPT the password part. A k...
 - Automating the Entry of Passwords in Terminal 29 juil. 2011

Admin: "I want a local admin account, with an encrypted password, and have my service desk be able to unencrypt it"

The screenshot shows a Microsoft Bing search page with the following elements:

- Search Bar:** Contains the query "how to encrypt a password with a keyword on macOS terminal".
- Navigation:** Includes "SEARCH", "COPILOT", "IMAGES", "VIDEOS", "MAPS", "NEWS", "SHOPPING", "MORE", and "TOOLS".
- Results:**
 - Super User:** A link to "Simple built-in way to encrypt and decrypt a file on a Mac via ..." with a snippet of terminal commands: `openssl enc -aes-256-cbc -salt -in file.txt -out file.enc`.
 - iMore:** A link to "How to create and password protect a zip file on macOS" with a snippet: "It's always a good time to protect your important files. Today, securing your private data is essential. Here's how you can create a ...".
 - Videos:** A section titled "Videos of How to Encrypt a Password With a Keyword on macOS T..." containing:
 - "Make Password Protected Pen Drive" (11,8K views, May 3, 2019).
 - "How To Enter Password Into Terminal On A Mac" (92,5K views, Apr 29, 2022).
 - "How to Encrypt a File" (partial view).
- AI Assistant:** A panel on the right provides a step-by-step guide:
 - Open Terminal:** Search for "Terminal" in Spotlight or Applications > Utilities > Terminal.
 - Navigate to the Directory:** Use the `cd` command to navigate to the file's location.
- Advertisement:** A blue banner for "Encryption Software for Mac" with sub-sections: "What is the best encryption software for Mac?" and "Which encryption software is best for XTS-AES 128-bit device encryption?".

More with Microsoft Copilot



Admin: "I want a local admin account, with an encrypted password, and have my service desk be able to unencrypt it"



Copilot

The screenshot shows the Microsoft Copilot interface in a notebook. The user asks: "Do you know how you encrypt a password with a key word on macOS Terminal?". Copilot responds with a step-by-step guide:

- Open Terminal:** You can find it in Applications > Utilities > Terminal.
- Encrypt the Password:** Use the following command to encrypt your password. Replace `your_password` with the password you want to encrypt and `your_keyword` with the keyword you want to use for encryption.

```
echo -n "your_password" | openssl enc -aes-256-cbc -a -salt -pass pass:your_keyword
```

This command uses the AES-256-CBC encryption method. The `-a` flag ensures the output is base64 encoded, making it easier to handle.

- Decrypt the Password:** To decrypt the password, use the following command. Replace `encrypted_password` with the encrypted password you got from the previous step and `your_keyword` with the keyword you used for encryption.

More with Microsoft Copilot



Admin: "I want a local admin account, with an encrypted password, and have my service desk be able to unencrypt it"



Copilot

The screenshot shows the Microsoft Copilot interface in a browser window. The user asks: "Do you know how you encrypt a password with a key word on macOS Terminal?". Copilot responds with a step-by-step guide:

- Open Terminal:** You can find it in Applications > Utilities > Terminal.
- Encrypt the Password:** Use the following command to encrypt your password. Replace `your_password` with the password you want to encrypt and `your_keyword` with the keyword you want to use for encryption.

```
echo -n "your_password" | openssl enc -aes-256-cbc -a -salt -pass pass:your_keyword
```

This command uses the AES-256-CBC encryption method. The `-a` flag ensures the output is base64 encoded, making it easier to handle.

- Decrypt the Password:** To decrypt the password, use the following command. Replace `encrypted_password` with the encrypted password you got from the previous step and `your_keyword` with the keyword you used for encryption.



Agenda

- **What is Intune and where are we?**

Past, current and future roadmap

- **Onboarding**

Await final config, FileVault, ect...

- **Device Configuration**

Direct Import, Zero Day, DDM

- **Platform SSO**

A Swiss knife or an Iceberg?

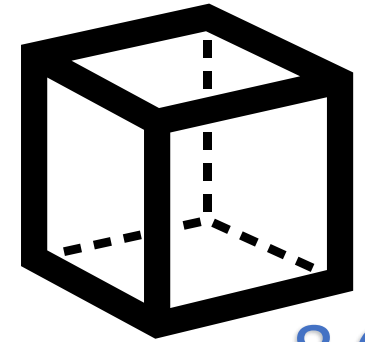
- **Applications & Suite**

Flexible App



macOS app management

Fundamental improvements & broad support for Mac app-types



8 Go

Managed apps

Flat PKGs installed using MDM.

Simplified app upload.

Intune app wrapping tool is no longer needed.

Will take advantage of DDM improvements.

Purchased and custom apps are also supported.

DMG apps

Most common Mac apps.

Easy to create with macOS Disk Utility.

Intune supports DMGs containing one or more apps (not .zip).

Deployed using Intune agent.

Expanded app size to 8GB.

“Available” assignment type

Flexible PKG installers

Great for deploying unsigned, component, or custom (non-flat) packages.

Uses built-in installer command.

Pre and post install scripts

Deployed using Intune agent.

Expanded app size to 8GB.

“Available” assignment type

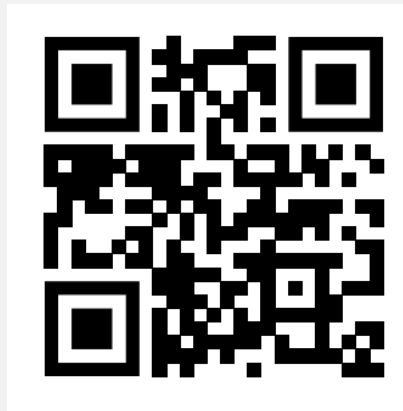
/* Microsoft Mac Admins Community */



LinkedIn

aka.ms/MacAdmins

You can join it with just one click



Thankyou!

