

Manage & Secure your macOS devices w/ Intune

Fabian Rodriguez
IT Analyst @ Recast Software



Agenda:

Management and Security

Management

- Enrollment (Autopilotish, Local Primary Account, Await Config)
- Application Deployments (DMG, PKG management)
- Platform SSO

Security

- Filevault Encryption (Encryption during setup assistant)
- Microsoft Defender for Endpoint (Configuration kind of)
- Software Updates (Declarative Device Management)

Autopilotish for macOS

Ecommerce (Apple Store)

Device info goes to Apple Business Manager

Sync device to Microsoft Intune Server

Assign enrollment profile inside of Intune Enrollment program tokens

User logins

- Home
- Dashboard
- All services
- Devices
- Apps
- Endpoint security
- Reports
- Users
- Groups
- Tenant administration
- Troubleshooting + support

Home > Devices | Overview > macOS | Enrollment > Enrollment program tokens > Intune MDM Server | Profiles > macOS Production Profile | Properties >

Edit profile

macOS

1 Management Settings 2 Review + save

Define enrollment and management settings for your macOS devices. [Learn more](#)

User Affinity & Authentication Method

User affinity * ⓘ

Enroll with User Affinity

Authentication Method ⓘ

Setup Assistant with modern authentication



For devices running macOS 10.15 and later. You must deploy Company Portal to users as a required app to allow for device registration with Microsoft Entra ID.

Management Options

Await final configuration ⓘ

Yes No

Locked enrollment * ⓘ

Yes

Create profile ...

macOS

- ✓ Basics
- ✓ Management Settings
- ✓ Setup Assistant
- 4 Account Settings**
- 5 Review + create

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 *

Yes

Prefill account info **i**

Yes Not configured

Primary account name **i**

{{partialupn}}

Supported variables: {{partialupn}}

Primary account full name **i**

{{username}}

Supported variables: {{username}}

Restrict editing **i**

Yes Not configured

- Home
- Dashboard
- All services
- Devices
- Apps
- Endpoint security
- Reports
- Users
- Groups
- Tenant administration
- Troubleshooting + support

Home > Devices | Overview > macOS | Enrollment > Enrollment program tokens > Intune MDM Server

Intune MDM Server | Profiles

Enrollment program tokens

Search

+ Create profile ▾ ⚙ Set default profile

Overview

Manage

Devices

Profiles

Set default enrollment profile

Select the enrollment profile to set as default profile. Set a default profile for iOS/iPadOS and macOS if you will be enrolling those platforms.

iOS/iPadOS Enrollment Profile

iOS

macOS Enrollment Profile

macOS Production Profile

OK

Cancel

FileVault Encryption (Setup Assistant)

Like BitLocker

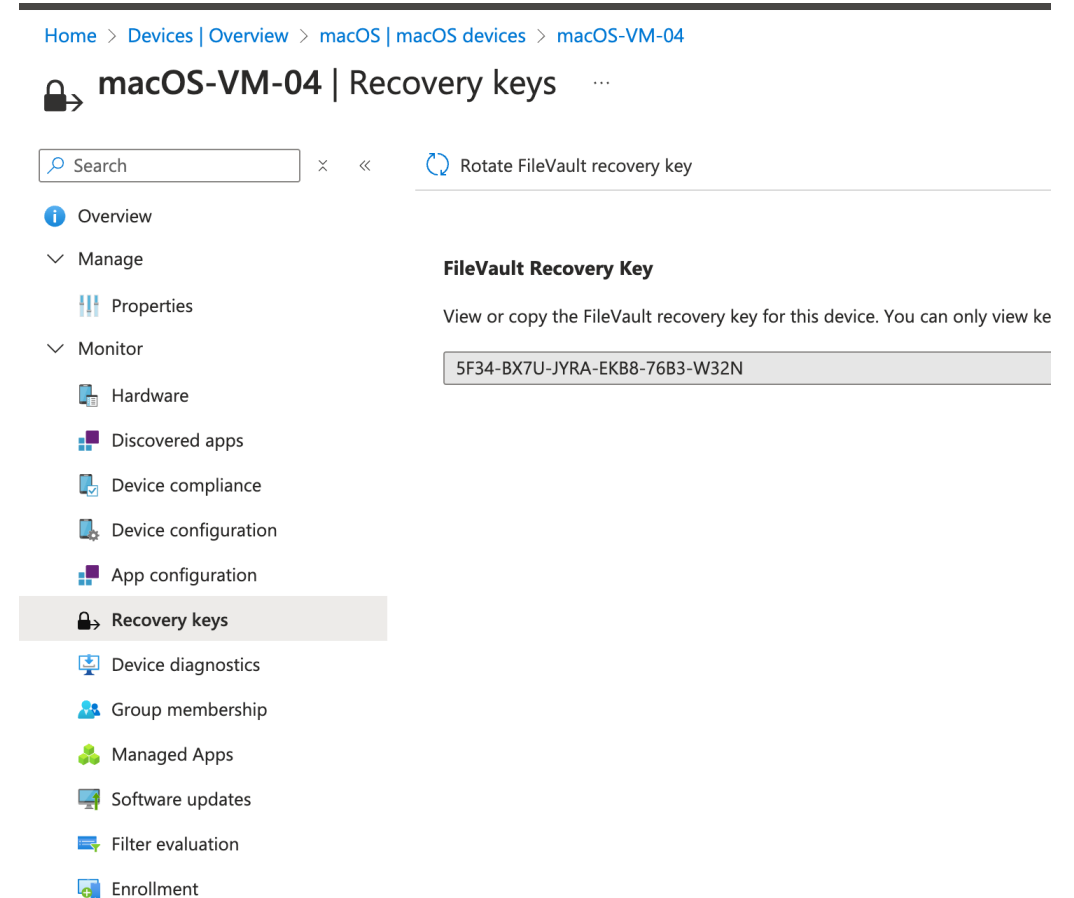
Enforce during user onboarding

Where else can I setup FileVault Encryption? Endpoint Security Policy or Settings Catalog policy.

Optional: Block end users from disabling FileVault

Show me the recovery keys

- **End User:** Can retrieve personal recovery keys from Company Portal Website (portal.manage.microsoft.com), iOS/iPadOS Company Portal, Android Company Portal.
- **IT Admins:** Inside of Microsoft Intune and we can also rotate the keys.



Create a Computer Account

Fill out the following information to create your computer account.

Full name: Fabian Rodriguez

Account name: fabianr

This will be the name of your home folder.

Password: ••••••••

Verify

Hint: optional

Back

Continue

Application Deployments

Intune agent channel apps

macOS DMG app

An admin has to upload a DMG file from local when creating a new app policy in admin portal. The .app under the DMG file will be copied to the Application folder to install on the device.

Recommended usage scenario: You need to deploy a disk image that contains one or more applications in .app format to be installed to the Applications folder.

Note that all apps are unmanaged and won't be uninstalled when the MDM profile is removed.

Find more details in: [Add a macOS DMG app to Microsoft Intune](#) .

macOS PKG app

An admin has to upload a PKG file from local when creating a new app policy in the admin center. Complex PKGs are also supported by this deployment type.

Complex PKG: A complex PKG refers to a type of package file used primarily in macOS environments that includes more intricate configurations and requirements compared to standard PKG files. These packages often contain multiple components, scripts, and dependencies that need to be managed during the installation process.

Recommended usage scenario:

1. You need to deploy a PKG with advanced controls for pre-install or post-install scripts.
2. You need to deploy a PKG containing only scripts and no app payload.
3. You need to deploy a PKG that the macOS LOB app workflow cannot install.
4. You need to deploy a PKG that is not signed by an Apple Developer ID installer certificate.

Pre-install and post-install scripts are available for apps installed via Intune agent.

Note that all apps are unmanaged and won't be uninstalled when the MDM profile is removed.

Find more details in: [Add an unmanaged macOS PKG app to Microsoft Intune](#) .

Platform SSO



FRAMEWORK BUILT
BY APPLE



CONNECTS YOUR
MAC TO YOUR IDP




AVAILABLE ON
MACOS 13+

What do we need?

Requirements

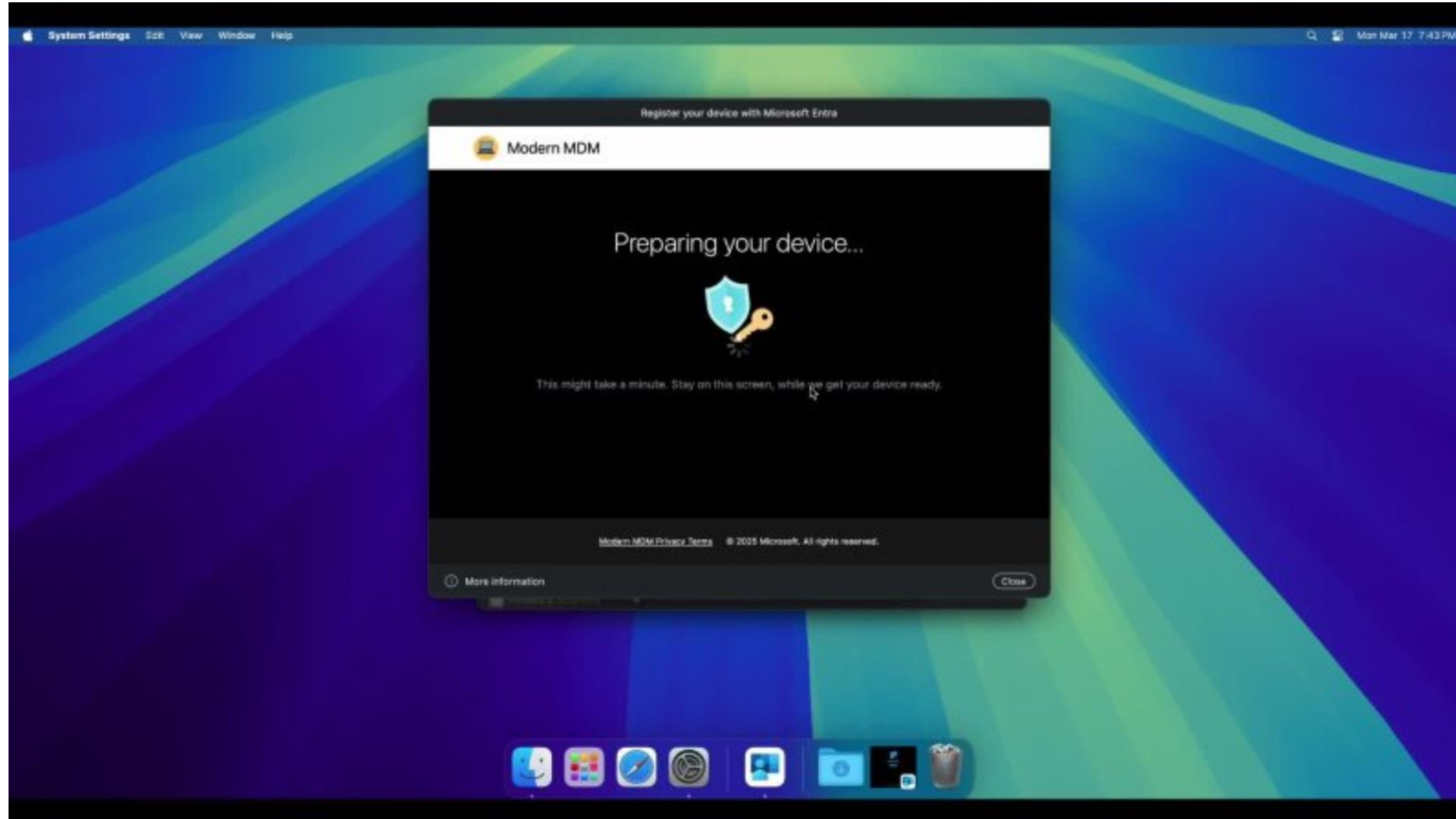
To deploy Platform SSO for macOS, you need to meet the following minimum requirements.

- A recommended minimum version of macOS 14 Sonoma. While macOS 13 Ventura is supported, we strongly recommend using macOS 14 Sonoma for the best experience.
- [Microsoft Authenticator](#) 
- Microsoft Intune [Company Portal app](#) version 5.2404.0 or later installed. This version is required before users are targeted for PSSO.

[Expand table](#)

Feature	Secure Enclave	Smart Card	Password
Passwordless (phishing resistant)	✓	✓	✗
TouchID supported for unlock	✓	✓	✓
Can be used as passkey	✓	✗	✗
MFA mandatory for setup	✓	✓	✗
Multifactor authentication (MFA) is always recommended			
Local Mac password synced with Entra ID	✗	✗	✓
Supported on macOS 13.x +	✓	✗	✓
Supported on macOS 14.x +	✓	✓	✓
Optionally, allow new users to log in with Entra ID credentials (macOS 14.x +)	✓	✓	✓

Platform SSO Configuration & Demo



Microsoft Defender for Endpoint (macOS)

- **What is Microsoft Defender for Endpoint?**

Microsoft Defender for Endpoint is an enterprise endpoint security platform designed to help enterprise networks prevent, detect, investigate, and respond to advanced threats.

It's available for macOS devices and you can deploy with Microsoft Intune

What is Declarative Device Management?

■ ■

Declarative device management is an update to the existing protocol for device management that can be used in combination with the existing MDM protocol capabilities. It allows the device to asynchronously apply settings and report status back to the MDM solution without constant polling. This is ideal for performance and scalability.

- Available on macOS 14.0 and later

Currently Available inside of Intune

Settings picker

Use commas "," among search terms to lookup settings by their keywords

Browse by category

- > App Management
 - App Store
- > Authentication
- ▼ Declarative Device Management (DDM)
 - Disk Management
 - Math Settings
 - Passcode
 - Safari Extension Settings
 - Software Update
 - Software Update Settings

Setting name

Select a category to show settings

Configure DDM & Demo

Intune macOS capabilities: Recent updates



Coming soon....

Intune macOS capabilities: Coming soon

User channel support for resource access profiles – In product today

Sidecar Enhancements – CY24 Q4-CY25 Q1

LAPS – CY25 H2

macOS Recovery lock management – CY25 H1

Managed device attestation with ACME – CY25 H1

Custom app detection – CY25 Q2

Platform SSO (General Availability) – CY25 Q3

JIT compliance remediation – CY25 H1

Thanks Again!

Sponsor: Zerotouch.ai

Speakers: Steve Weiner, Andrew Johnson & Matt Roy, Fabian Rodriguez

Discord: TCSMUG



Next User Group Meetings:

4/10/2025 @ 4:30pm (mini mms series with Steve Jesok, Matthew Teegarden, maybe Scott Erickson)

5/21/2025 @ TBD

