Microsoft

DEVICIE

# Managing MacOS in the enterprise - Intune's magic potion

# Agenda

- **How to get started compared to Windows endpoints**
  Improve your security posture
- **Platform SSO, Local Account Management, FileVault & Software Updates**
  Lessons Learned …
- **Because we learned it the hard way …**
  Community tools you say?
- **Are there any ?**
  Conclusion
- **Recap of key takeaways, Q&A**

# About “Kenny Buntinx”



## Focus

Modern Workplace Consultant

Co-founder OB-V-US

Co-organizer at Workplace Ninja Summit

## From

Be(er)lgium

## My Blog

www.obvus.be/blog

## Certifications

Former

14 year

## Hobbies

Travel, Beer, Cars & BBQ


## Contact

KBU@obvus.be

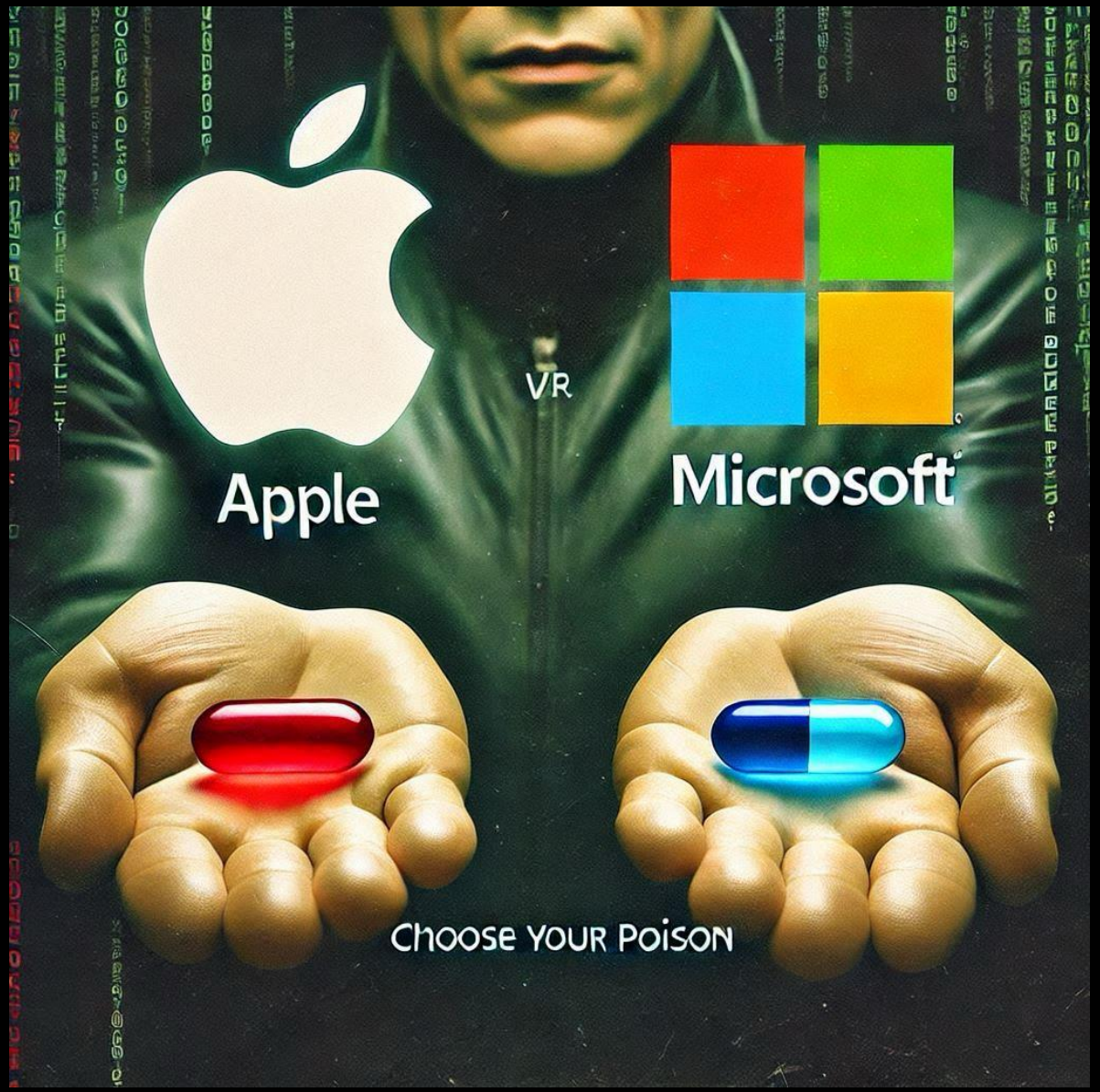
https://twitter.com/kennybuntinx

https://www.linkedin.com/in/kennyBuntinx

# MacOS Management enrollment

# Enterprises today…

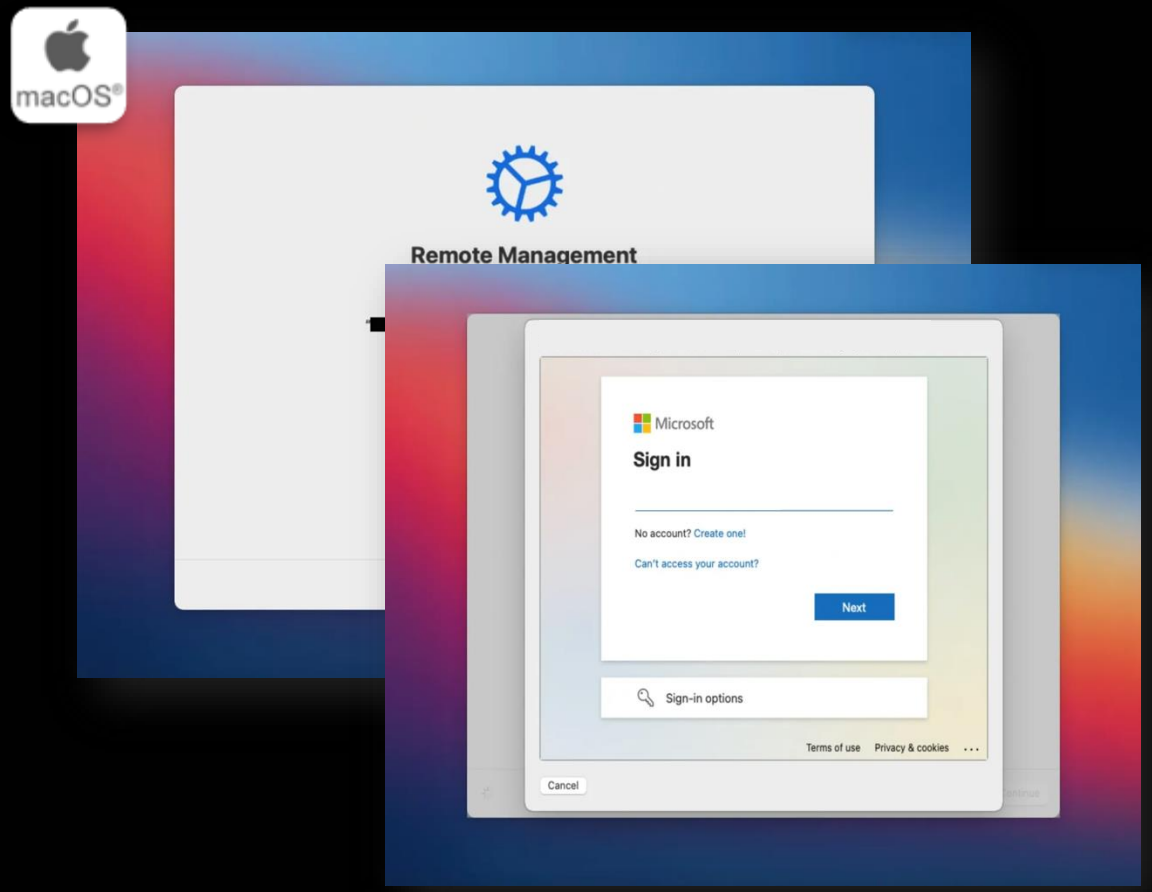




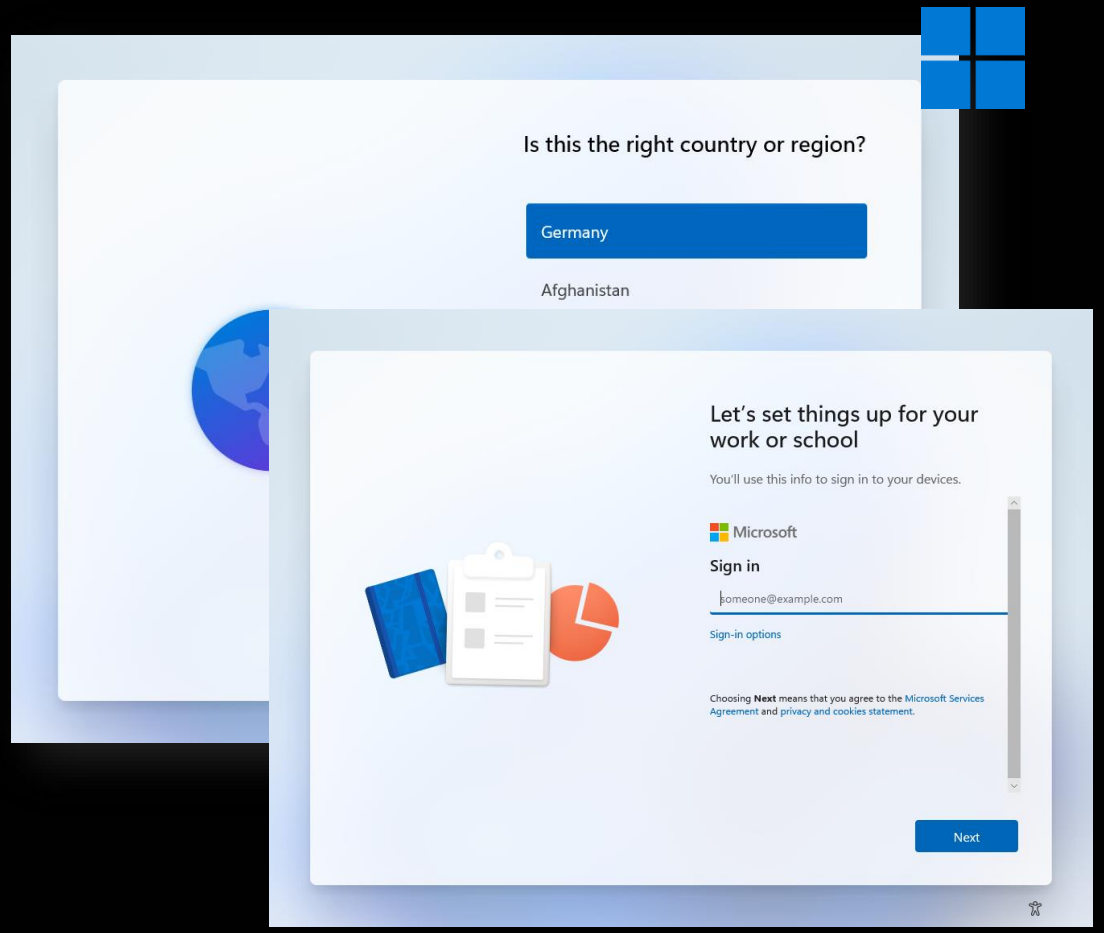
# How to get started – ADE …



## MacOS - Automatic Device Enrollment (ADE)




## Windows - Autopilot



# How to get started with ADE



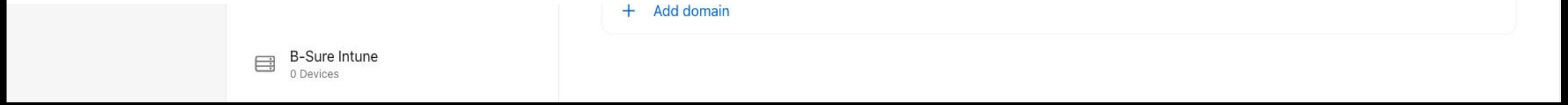
- **Automatic Device Enrollment (ADE)**
  - Apple Business Manager


## Domain capture process

After the domain capture process starts, personal Apple Accounts using that domain are notified in an email and in a notification on any device signed into the account. For notifications, the device must use iOS 18, iPadOS 18, macOS 15.1, visionOS 2.0, or later.

The email and notification present two options to the user:

- Choose a new primary email address to continue using their personal Apple Account.
- Transfer the personal Apple Account and its data to the organization, which then converts it into a Managed Apple Account.



# Enrollment Profile for ADE



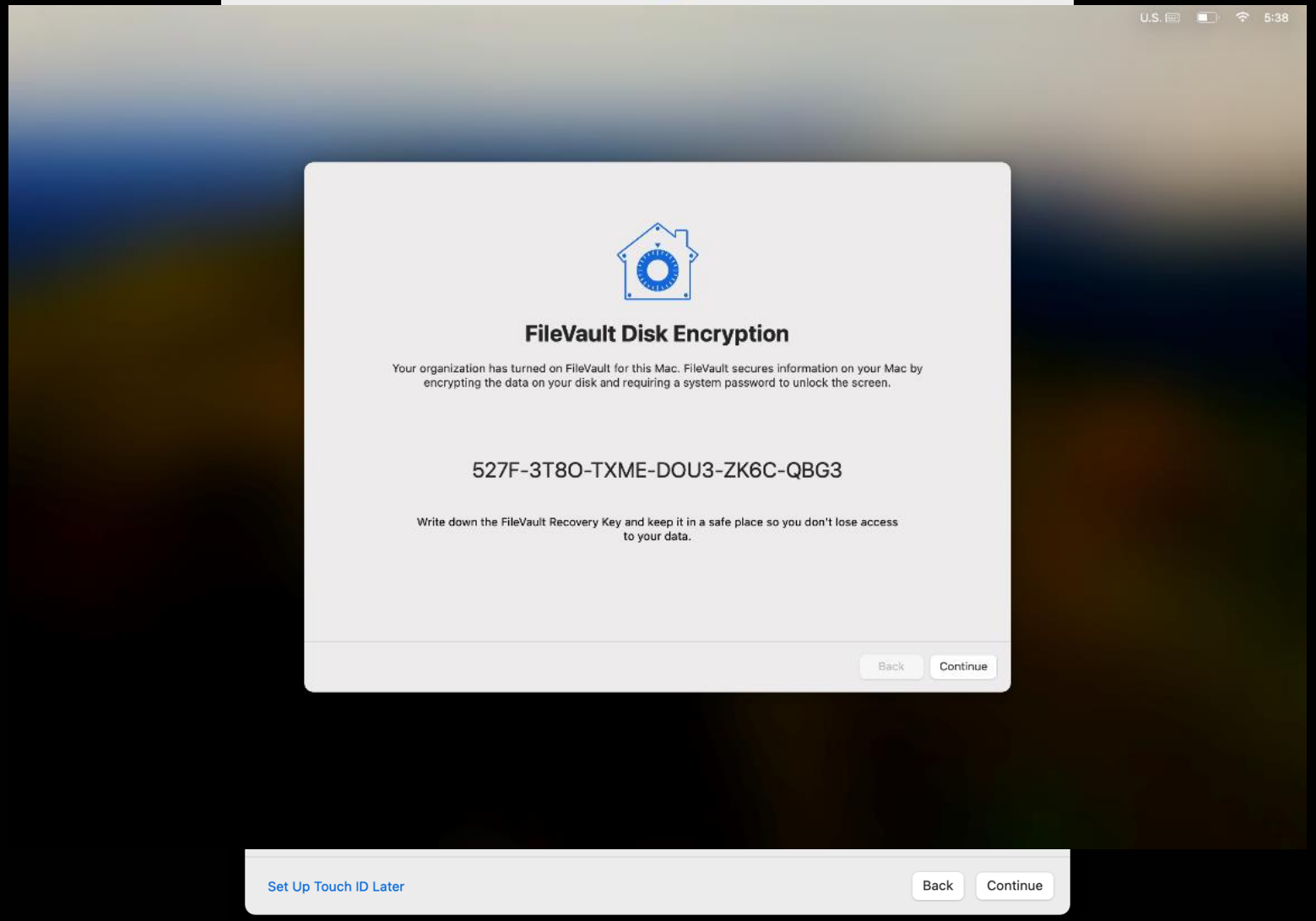
**Create a more secure onboarding experience by guaranteeing that the Mac is configured before releasing to the user.**

**Management Settings** Edit

| | |
|---|---|
| User Affinity & Authentication Method | |
| User affinity | Enroll with User Affinity |
| Authentication Method | Setup Assistant with modern authentication |
| Management Options | |
| Await final configuration | Yes |
| Locked enrollment | Yes |

# Enrollment Profile for ADE

wpninjas.au




**Setup Assistant** Edit

| | |
|---|---|
| Department | OBVUS |
| Department Phone | 69696969 |
| Setup Assistant Screens | |
| Location Services | Show |
| Restore | Hide |
| Apple ID | Hide |
| Terms and conditions | Hide |
| Touch ID and Face ID | Show |
| Apple Pay | Hide |
| Siri | Show |
| Diagnostics Data | Hide |
| FileVault | Show |
| iCloud Diagnostics | Show |
| iCloud Storage | Hide |
| Display Tone | Hide |
| Appearance | Show |
| Registration | Hide |
| Screen Time | Hide |
| Privacy | Hide |
| Accessibility | Hide |
| Auto unlock with Apple Watch | Hide |
| Lockdown mode | Show |
| Wallpaper | Show |
| Terms of Address | Hide |
| Intelligence | Show |

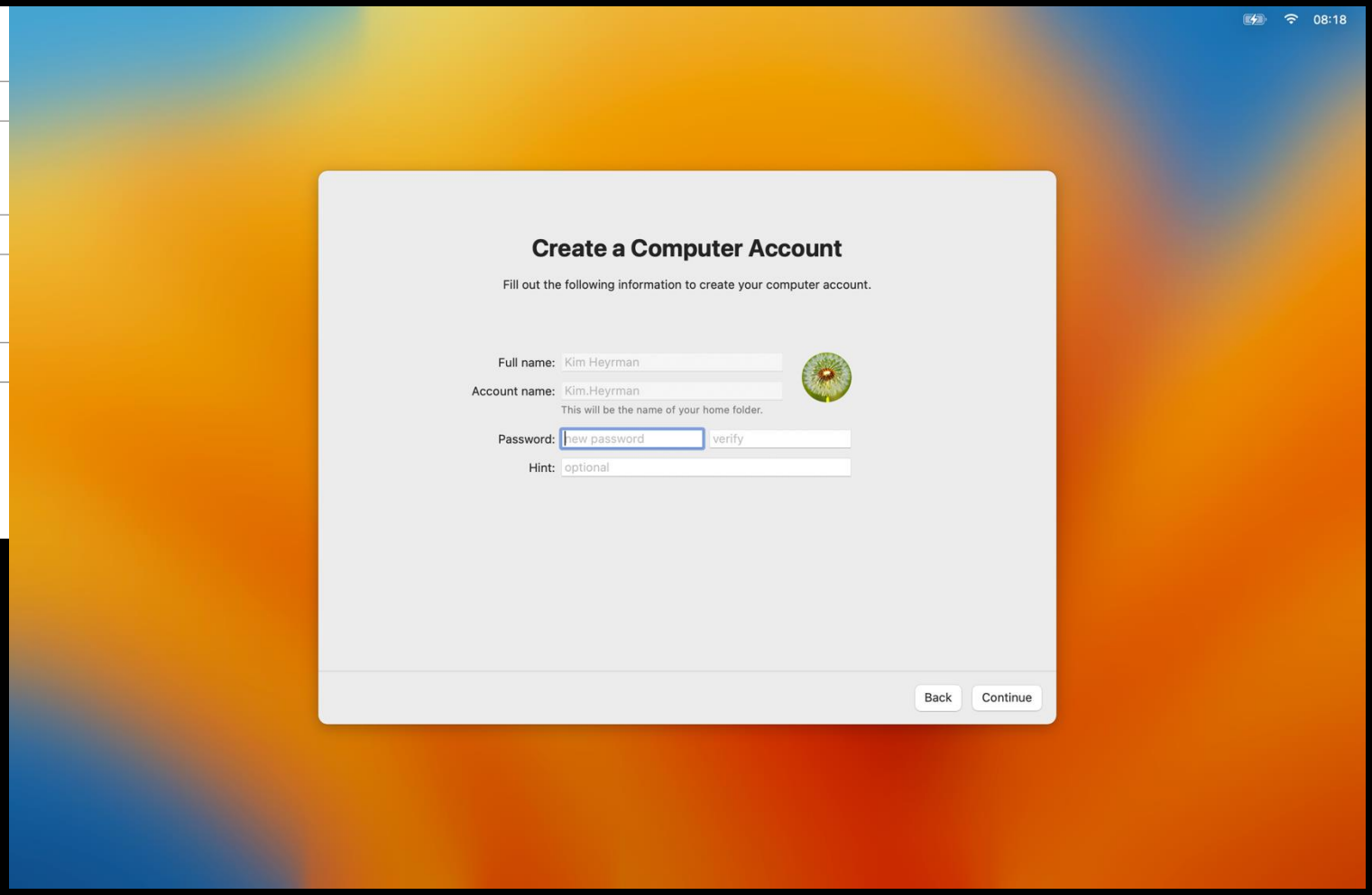
# Enrollment Profile for ADE



Create and configure local admin and primary account on ADE enrolled Macs

**Local primary account (preview)**

| | |
|---|---|
| Create a local primary account * | Yes |
| Prefill account info ⓘ | Yes / Not configured |
| Primary account name * ⓘ | {{partialupn}} |
| Supported variables: {{partialupn}} | |
| Primary account full name * ⓘ | {{username}} |
| Supported variables: {{username}} | |
| Restrict editing ⓘ | Yes / Not configured |



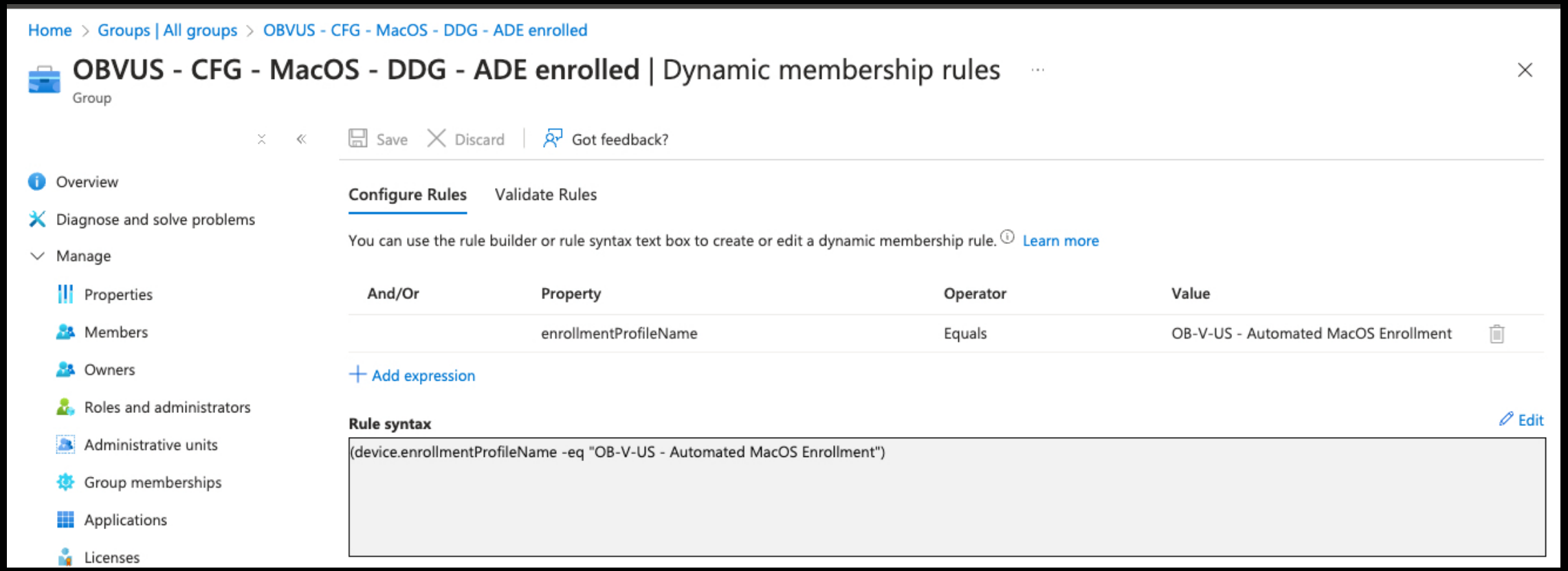

**Await final configuration required !!**

# Dynamic groups for ADE Enrollment Profile



**Create a naming logic in your different Enrollment Profiles :**

- **Create Dynamic Device groups based on EnrollmentProfileName to target different configuration baselines**

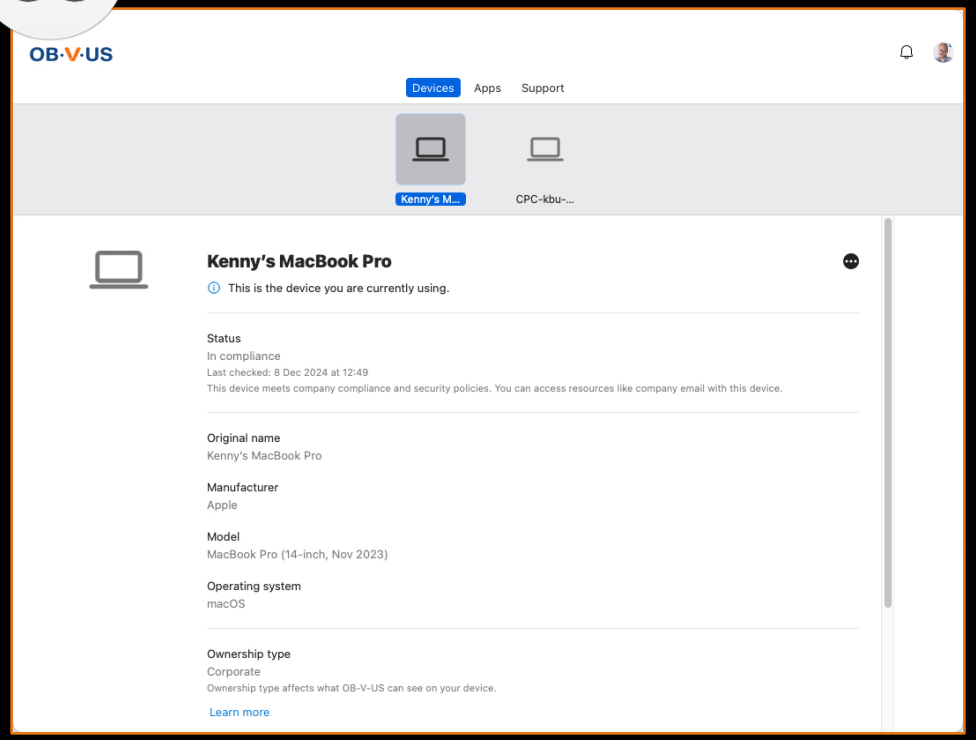


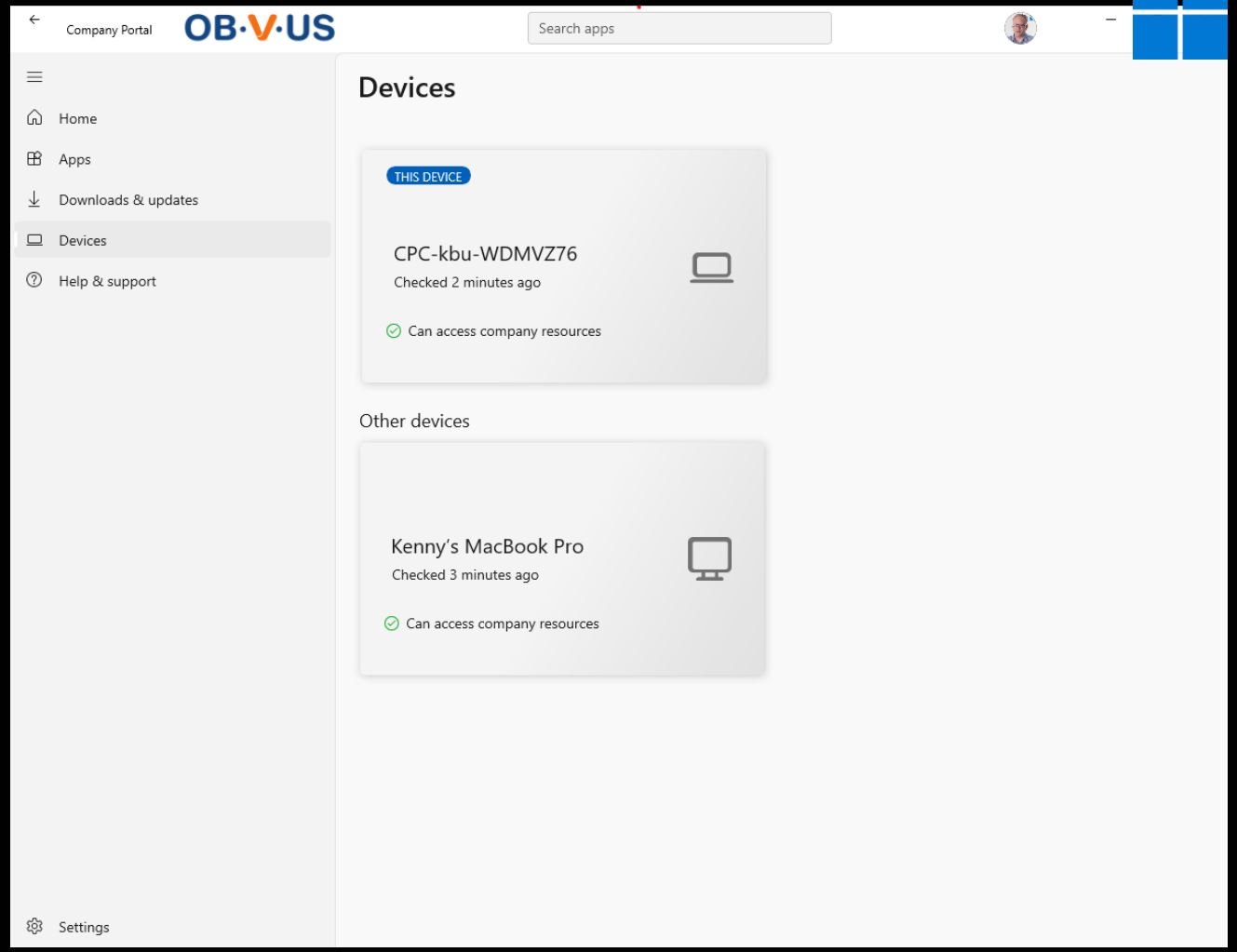
# Application Delivery ?

# Company portal Look & Feel

wpninjas.au

mac OS



# Applications



## Not all applications for MacBook are in VPP store !

mac OS

OB·V·US

What's new | All apps | Categories

Recently added

Universal Print
Microsoft Corporat...

WhatsApp Messenger
WhatsApp Inc.

Business

- Activity
- Locations
- Users
- User Groups
- Access Management
- Devices
- Assignment History
- Apps and Books
- Custom Apps

Search content by Name, Keyword, ISBN, or URL

Sort By | 7 Total

**WhatsApp Messenger**
WhatsApp Inc. · iOS and macOS
★★★★½ €0.00

**Microsoft OneDrive**
Microsoft Corporation · iOS App
★★★★½ €0.00

**Signal - Private Messenger**
Signal Messenger, LLC · iOS App
★★★★½ €0.00

**Microsoft Outlook**
Microsoft Corporation · iOS App
★★★★½ €0.00

**Apple Configurator**
Apple · macOS App
☆☆☆☆☆ €0.00

**Windows App**
Microsoft Corporation · macOS App
☆☆☆☆☆ €0.00

**Universal Print**
Microsoft Corporation · macOS App
☆☆☆☆☆ €0.00

**Windows App**
Microsoft Corporation · macOS App
Device Assignable
View Details ↗

### Buy Licenses

Assign to
Choose a Location

| Price | Quantity | Payment Method |
|---|---|---|
| €0.00 | 0 | None |

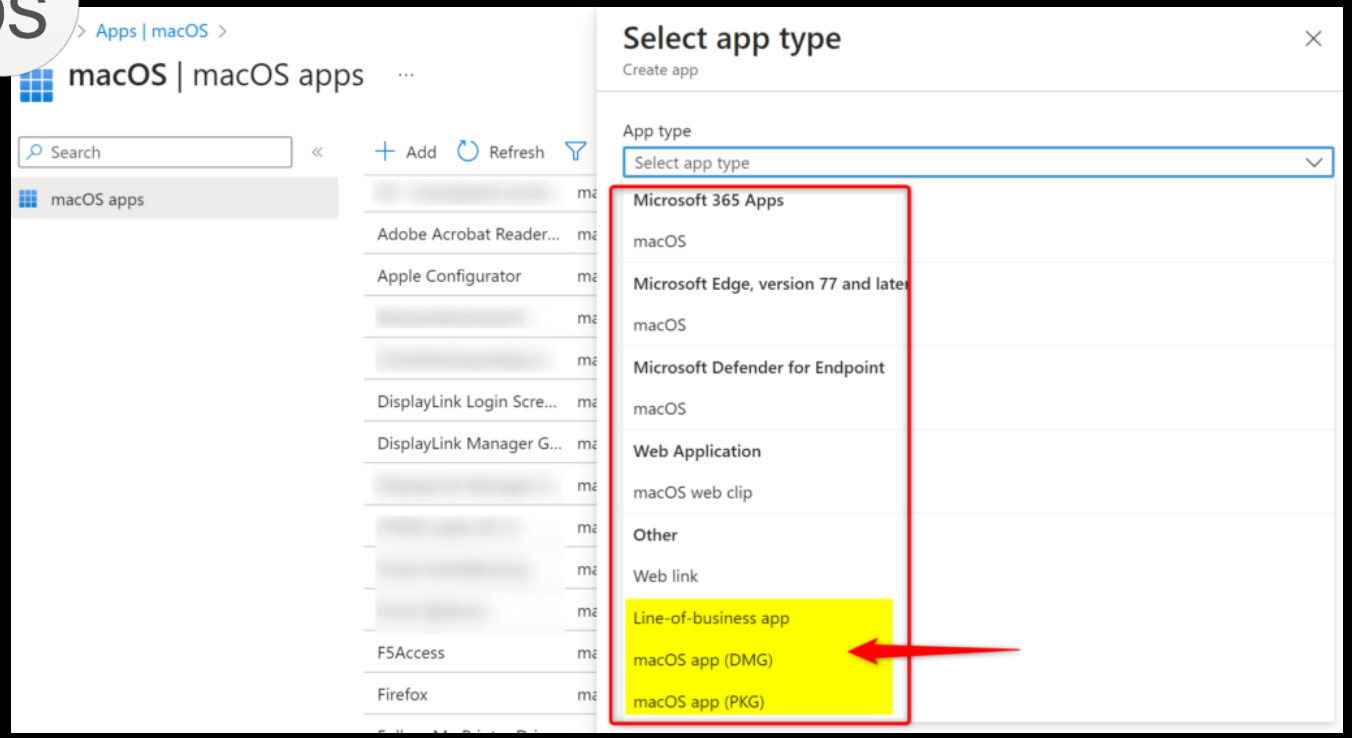
Total Cost €0.00 | Get

### Manage Licenses

| Location | In Use | Available |
|---|---|---|
| Ob-V-Us NV | 2 | 998 |
| **Total** | **2** | **998** |

# Applications






- **DMG files** are disk images that provide a simpler, drag-and-drop installation experience when installed manually.
  - Full disk access permission is required to update or delete DMG apps
- **PKG files** are installer packages native to macOS, essential for applications that need a structured installation process.
  - **Pre- or a Post-install** script for complex customization.
  - The PKG file must successfully run using the installer command in Terminal
- **MacOS LOB apps (Legacy way)**
  - need to have a logo in order to be displayed in the Company portal App
  - LOB apps need to be signed

# Deploying Microsoft 365 Apps for Mac



## Option 1: Mac App Store via Volume Purchase Program (VPP)

### Advantages

• It makes use of Apple's content caching, which can greatly improve deployment efficiency (Note: Intune can also be used to configure your content caches)

• It's possible to deploy the individual apps.

• It's easy to configure if you already have Apple Business Manager.

• You can configure the apps to uninstall on unenrollment.

• You can send an uninstall command to remove unwanted apps.

### Disadvantages

• Teams is not yet in the Mac App Store (could be deployed via scripting agent)

• You cannot control which update channel to use.

• When OneDrive is deployed via VPP it will have a different bundleID than if it was installed via a standalone installer.

- VPP: com.microsoft.OneDrive-mac
- CDN: com.microsoft.OneDrive

• Updates via this approach can be unpredictable, especially if apps are permanently open.

# Deploying Microsoft 365 Apps for Mac



## Option 2: Deploying Microsoft 365 Apps for Mac via the Microsoft Content Delivery Network

### Advantages

- It's easy to deploy. This mechanism is supported natively by Microsoft Intune. It is as simple as checking a box and providing a group of users to deploy it to.
- It includes the Microsoft Autoupdate (MAU) tool, which can be configured via plist to auto update and deploy insider builds of Office for testing to some users.
- It's possible to create a local MAU cache server for updates.

### Disadvantages

- The initial download size (1.8GB) is large.

# Deploying Microsoft 365 Apps for Mac



## Option 3: Deploying Microsoft 365 Apps for Mac via the Intune Scripting Agent for Mac

### Advantages

- Fastest install time.
- Additional logging.
- Can deploy either entire suite or individua
- Possible to cache the initial installation file webserver.
- Possible to create a local MAU cache serve (only if you have slow slow slow internet an upgrade your line)
- Includes the Microsoft Autoupdate (MAU) configured via plist to auto update and depl of Office for testing to some users.

### Disadvantages

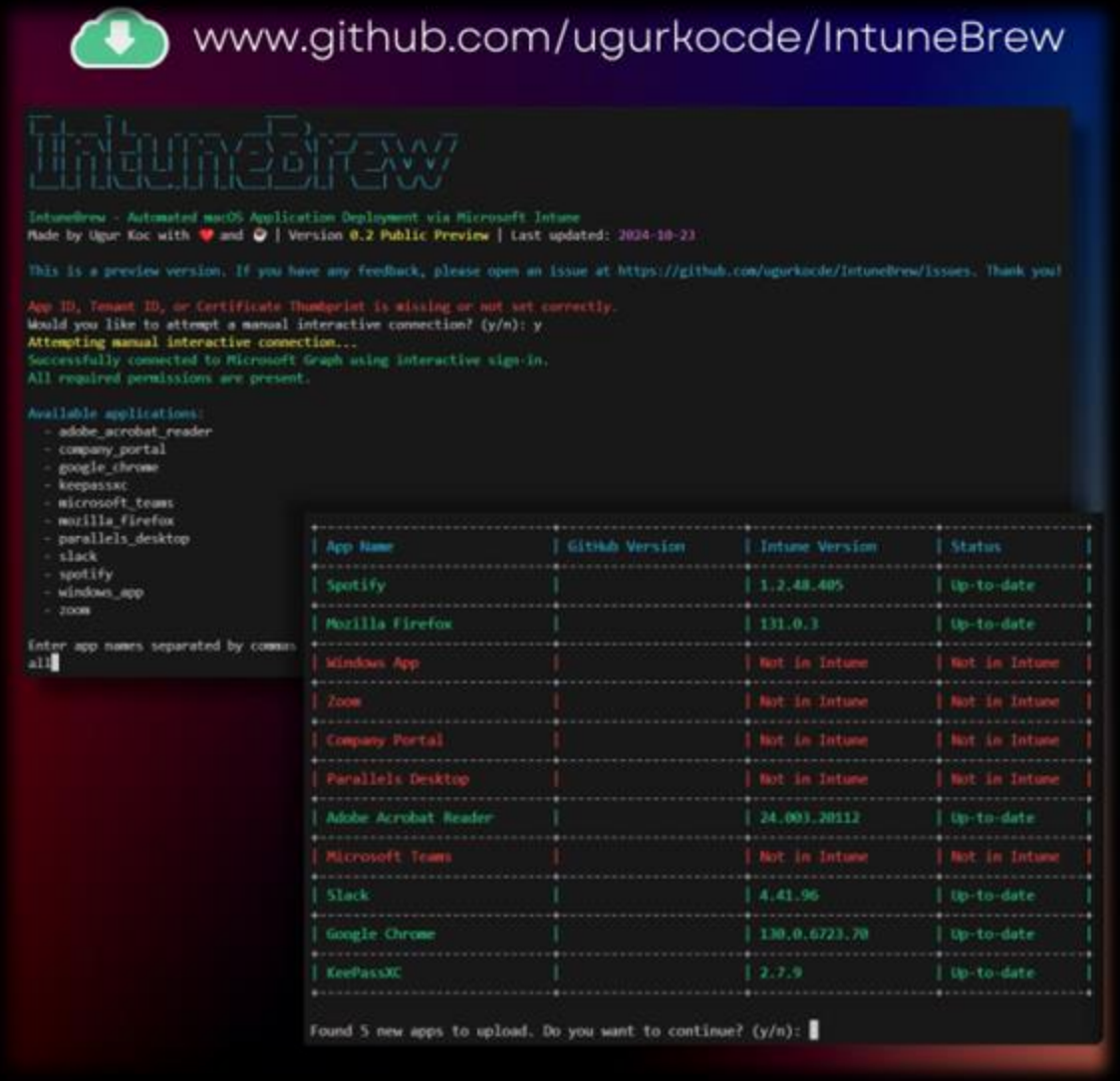
server infrastructure for caching.

ing skills.

cture complexity.

# Deploying Custom Apps the Ugur way



# Improve your security posture

# What do you mean with SSO ?



- Apple's enterprise single sign-on feature, supported since macOS 13.x
- Provide SSO – even for applications not supporting Microsoft Authentication Library (MSAL)
- Platform SSO = enhancement to SSO plugin
  - Depending on choice, allows logging in with Entra ID Password
- Key benefit: hardware-bound device record in Entra ID
- It gets enabled through MDM Profile



# Options

- **Secure Enclave**
  - cryptographic key in Secure Enclave used for SSO with Entra ID
  - comparable to Windows Hello 4 Business
  - but sign in still with local account and password
- **Smart Cards**
  - sign in with external smart card and SSO
- **Password sync**
  - local account password is in sync with Entra ID

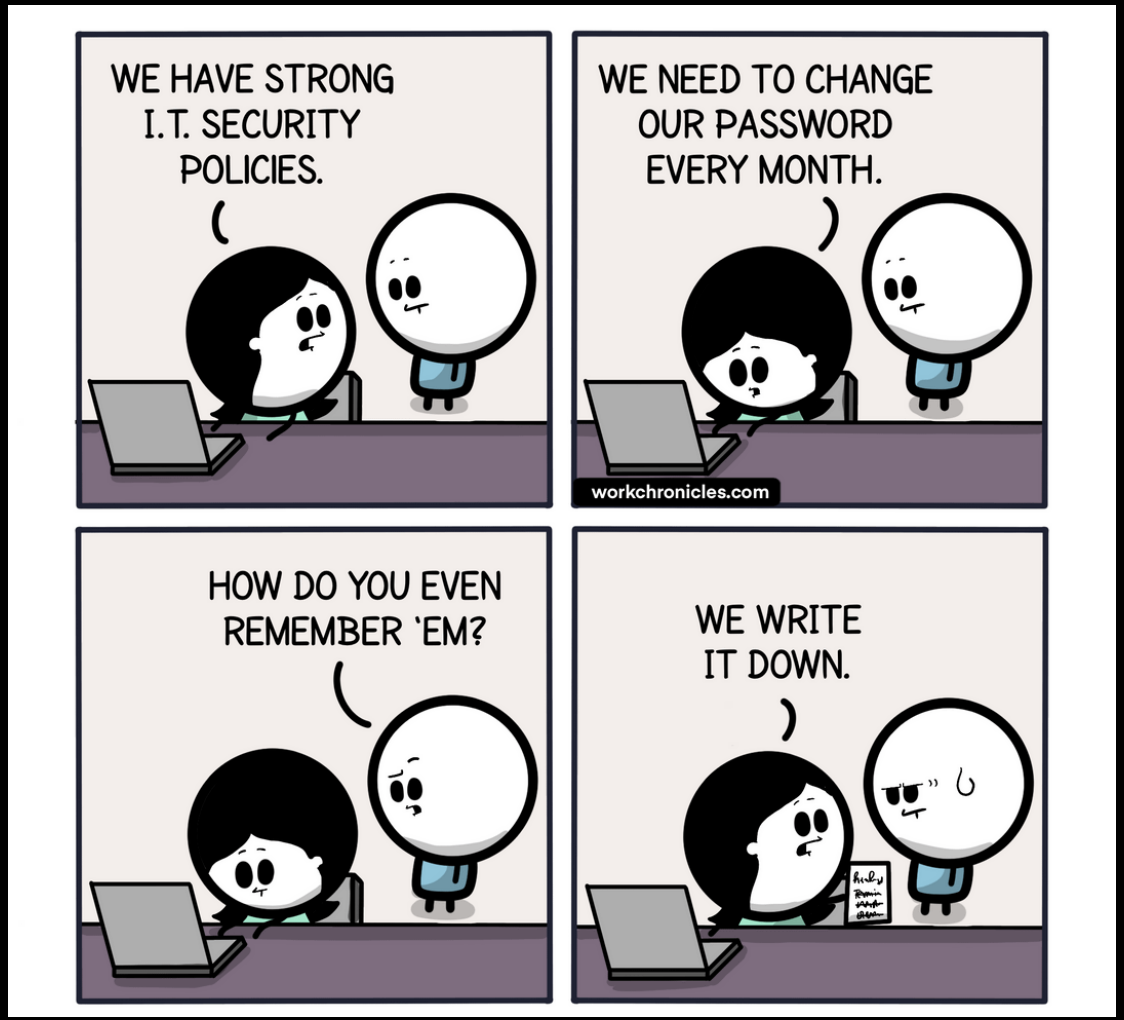
# Password sync


- ❤️ user-friendly – one central password
- ❤️ Touch ID possible
- ❤️ SSO

- 😱 Secure enclave not used (instead: keychain for tokens)
- 😱 not phishing resistant / no Zero Trust
- 😱 not password-less
- 😱 local password still existing for FileVault

# Secure Enclave



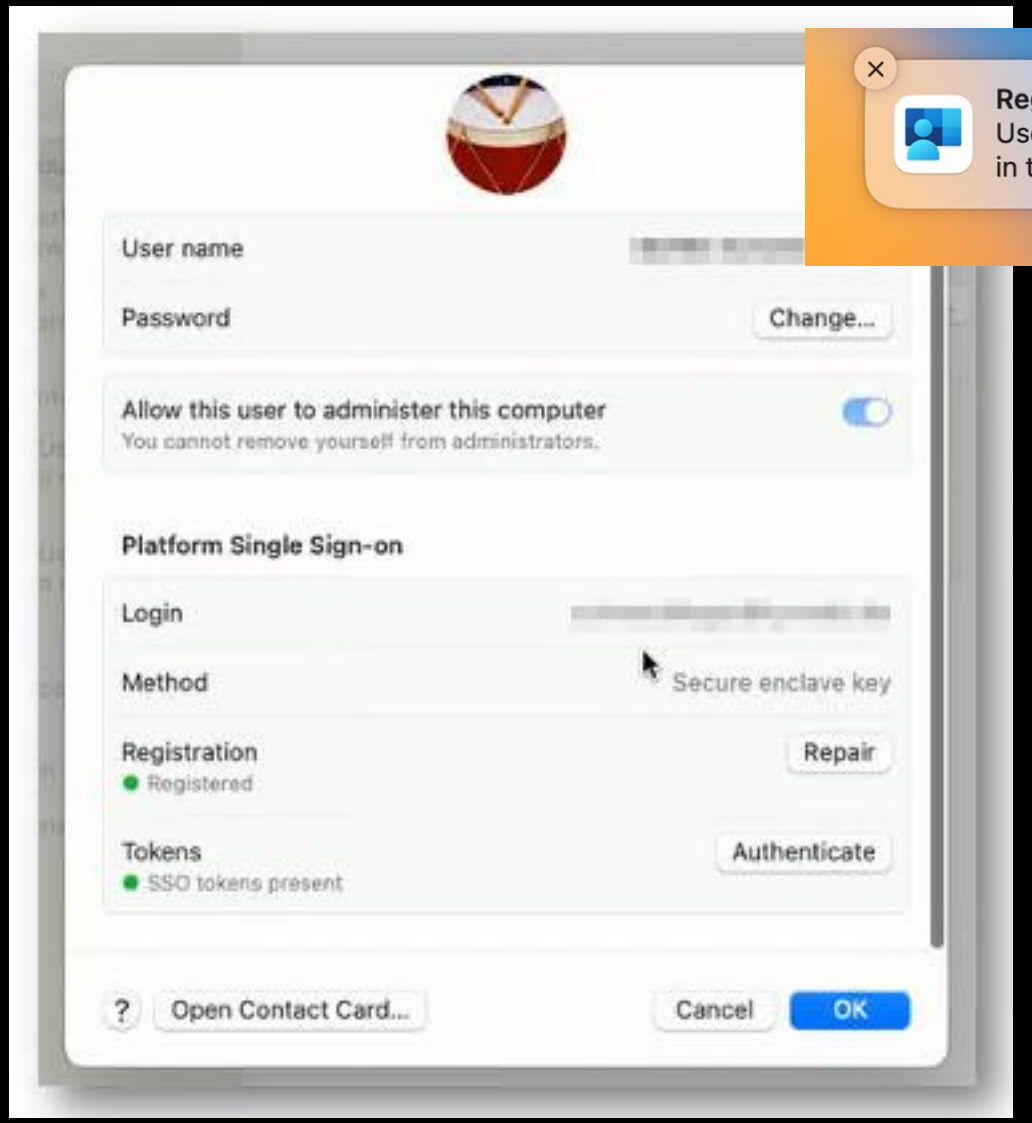


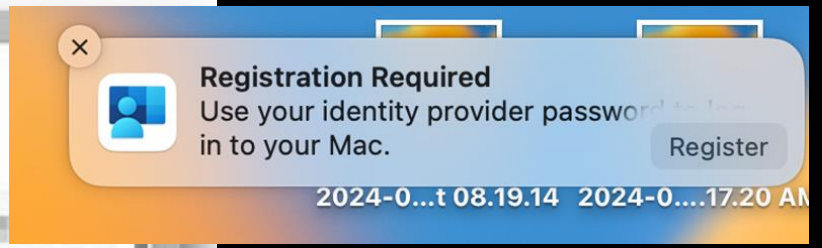

- ❤️‍🩹 like Windows Hello 4 Business
- ❤️‍🩹 Touch ID possible
- ❤️‍🩹 Hardware-bound cryptographic keys like TPM on Windows
- ❤️‍🩹 Phishing resistant
- ❤️‍🩹 SSO
- ❤️‍🩹 passkey support

- 😱 Password still required (after reboot) or 24h biometric
- 😱 Password different than Entra ID
- 😱 no easy recovery of local password (no alternatives)

# Secure Enclave

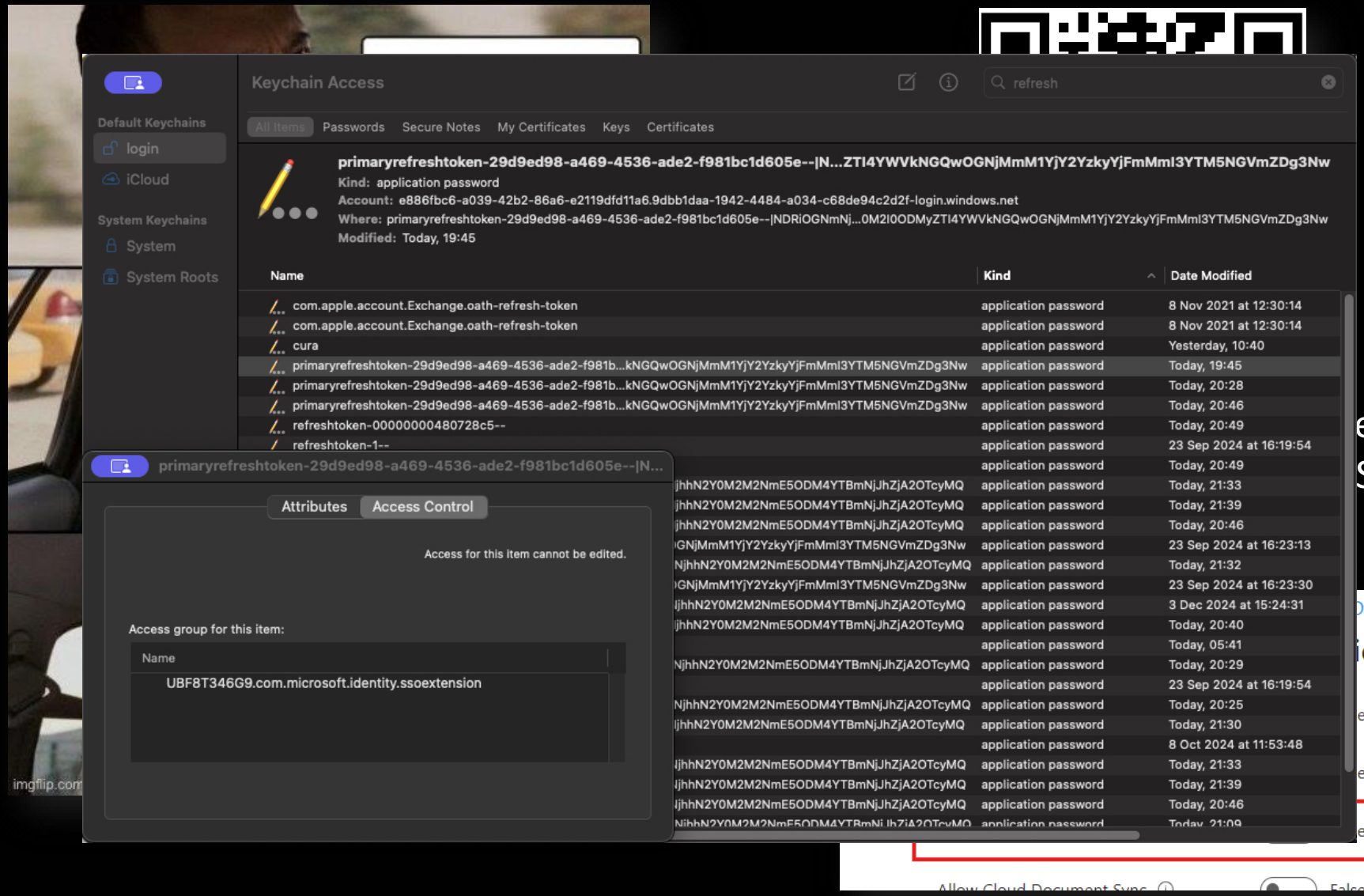




# Password Sync / Security Enclave






efresh token
S Keychain

# Comparison as reference



| Feature | Secure Enclave | 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 14.x + | ✅ | ✅ |
| Optionally, allow new users to log in with Entra ID credentials (macOS 14.x +) | ✅ | ✅ |

Configure Platform SSO for macOS devices | Microsoft Learn

# Best practices



- use Secure Enclave
- caution: no in-place migration from Password Sync to Secure Enclave possible
- numeric PIN instead of password


macOS - Default - Passcode - With Change At Sign-In - v3.0

Device configuration profile

Delete

**Passcode**

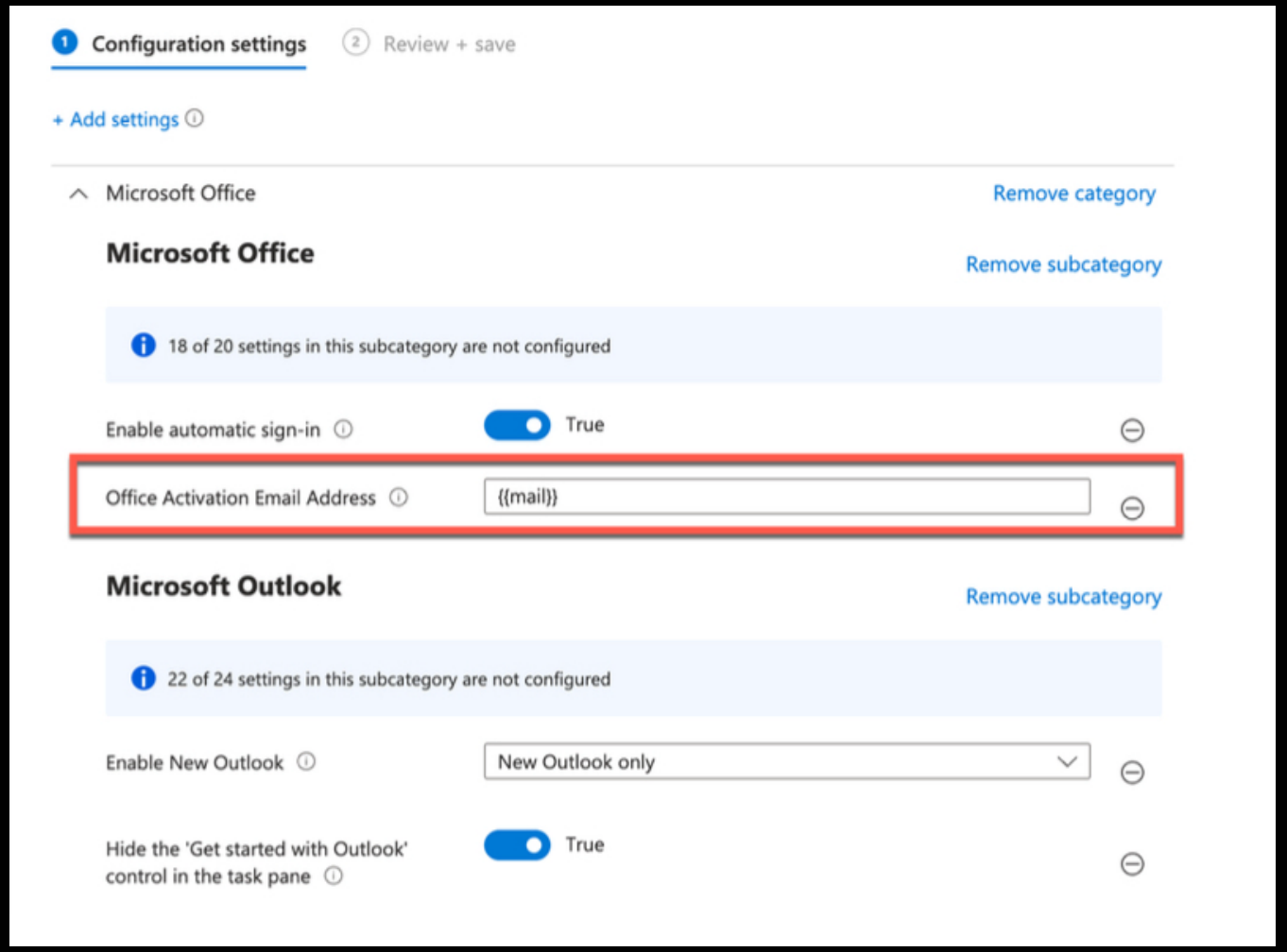
| | |
|---|---|
| Require Complex Passcode | True |
| Custom Regex | |
| Description | Only numeric #WHfB |
| ANY | default |
| Regex | [0-9]+$ |
| Maximum Number of Failed Attempts | 10 |
| Automatic Device Lock | 10 |
| Failed Attempts Reset In Minutes | 10 |
| Minimum Passcode Length | 7 |
| Change At Next Auth | Enabled |
| Require Passcode on Device | True |
| Maximum Grace Period | 0 |


| | |
|---|---|
| Description | Only numeric #WHfB |
| ANY | default |
| Regex | ^[0-9]+$ |

# Deploying SSO for Microsoft 365 Apps



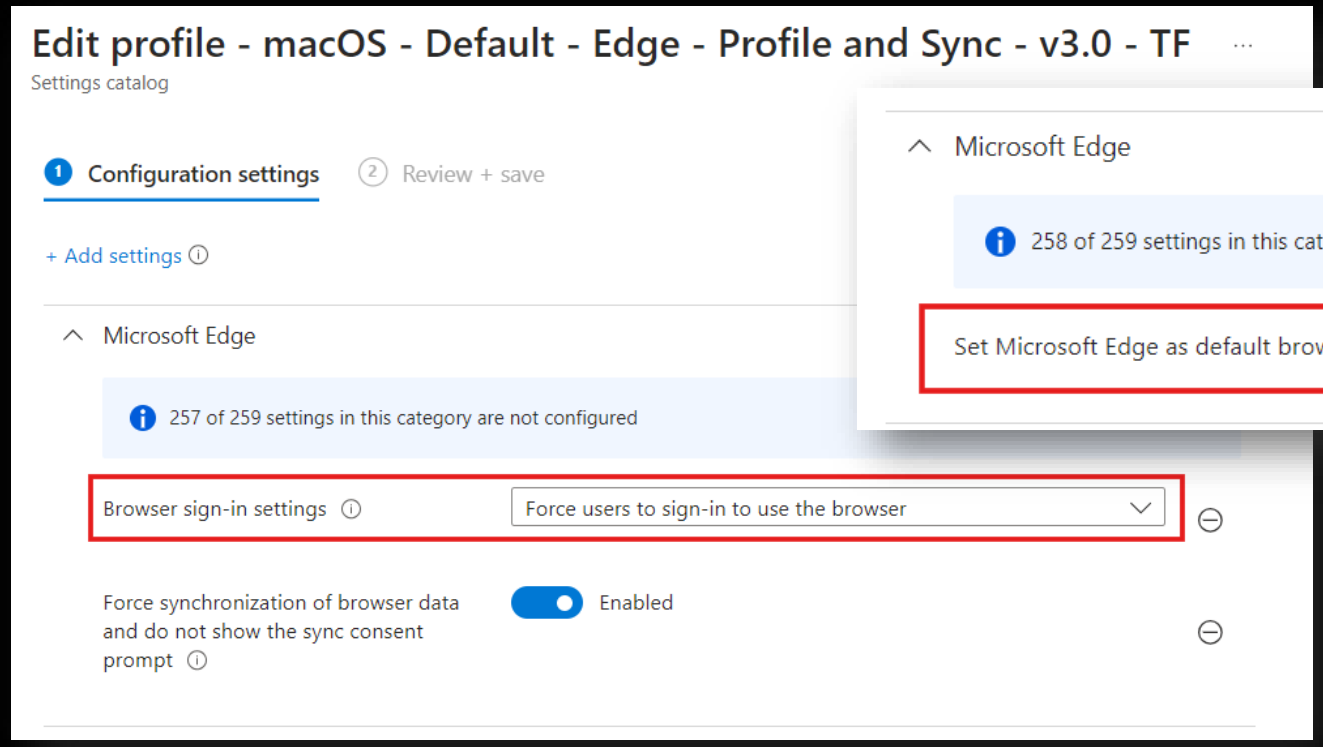
**New settings available with Intune 2408 + 2409 for macOS**

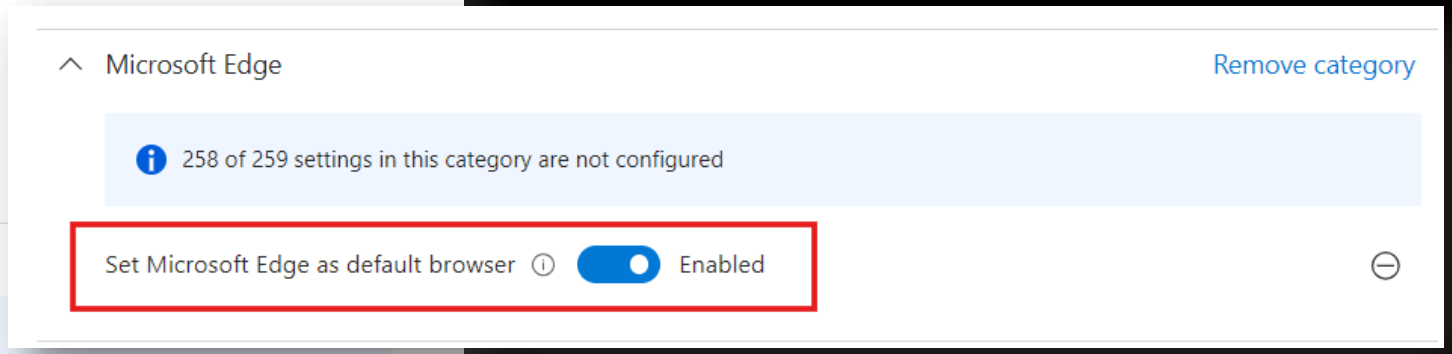


# Deploying SSO for Microsoft Edge



- **force login** to allow SSO to Entra ID authenticated websites
- **enable browser sync** for favorites etc.
- set as **default browser**



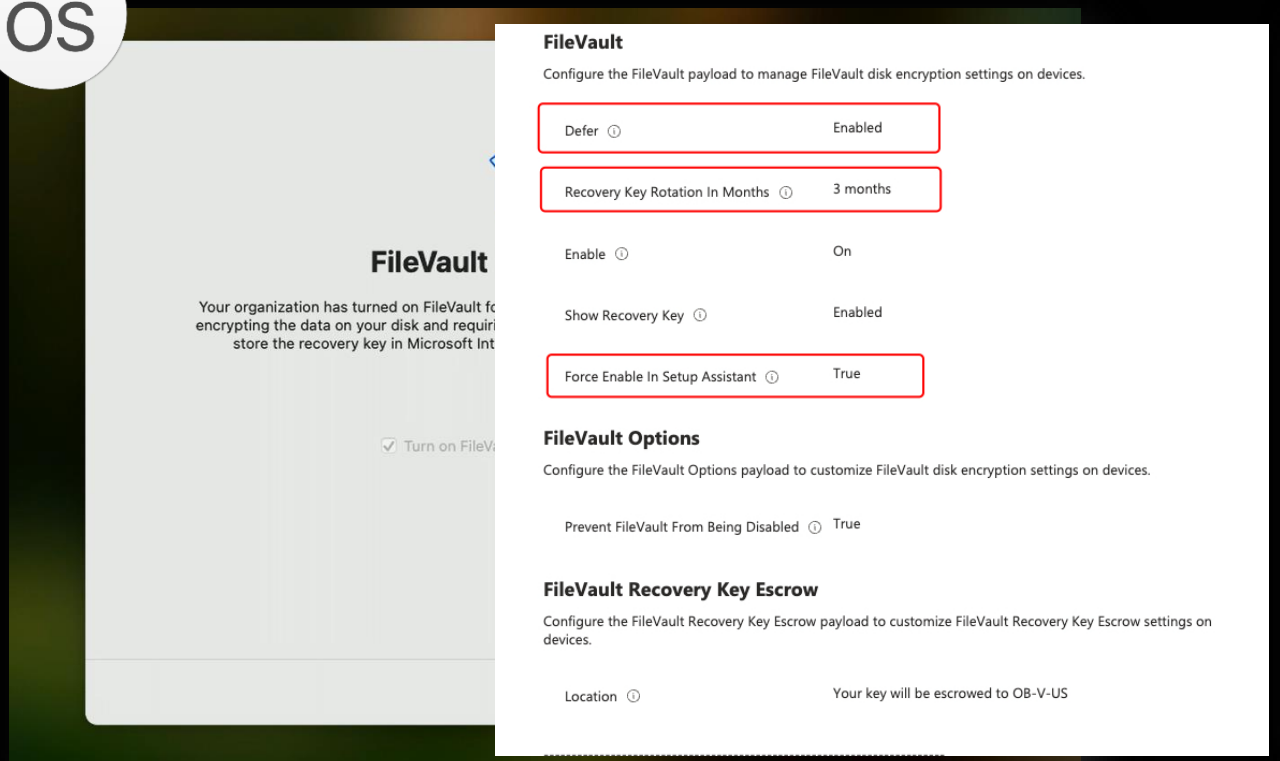



# Improve security posture

# Disk Encryption look & feel

wpninjas.au

mac OS




**FileVault**

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

| | |
|---|---|
| Defer | Enabled |
| Recovery Key Rotation In Months | 3 months |
| Enable | On |
| Show Recovery Key | Enabled |
| Force Enable In Setup Assistant | True |

**FileVault Options**

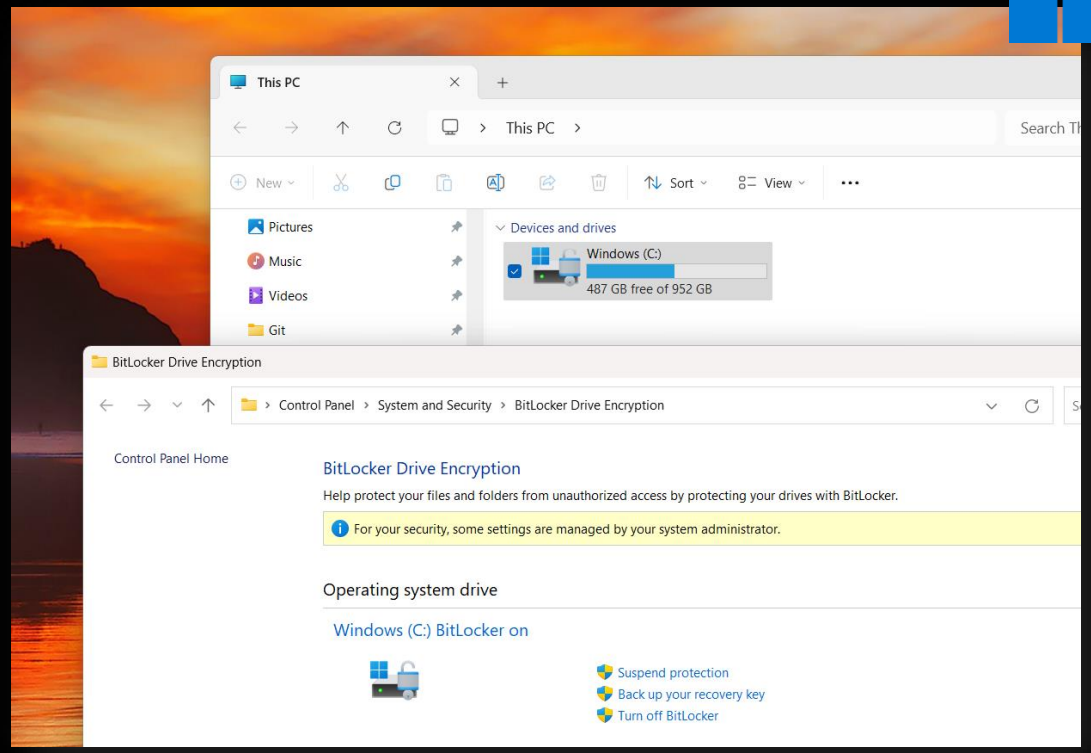
Configure the FileVault Options payload to customize FileVault disk encryption settings on devices.

| | |
|---|---|
| Prevent FileVault From Being Disabled | True |

**FileVault Recovery Key Escrow**

Configure the FileVault Recovery Key Escrow payload to customize FileVault Recovery Key Escrow settings on devices.

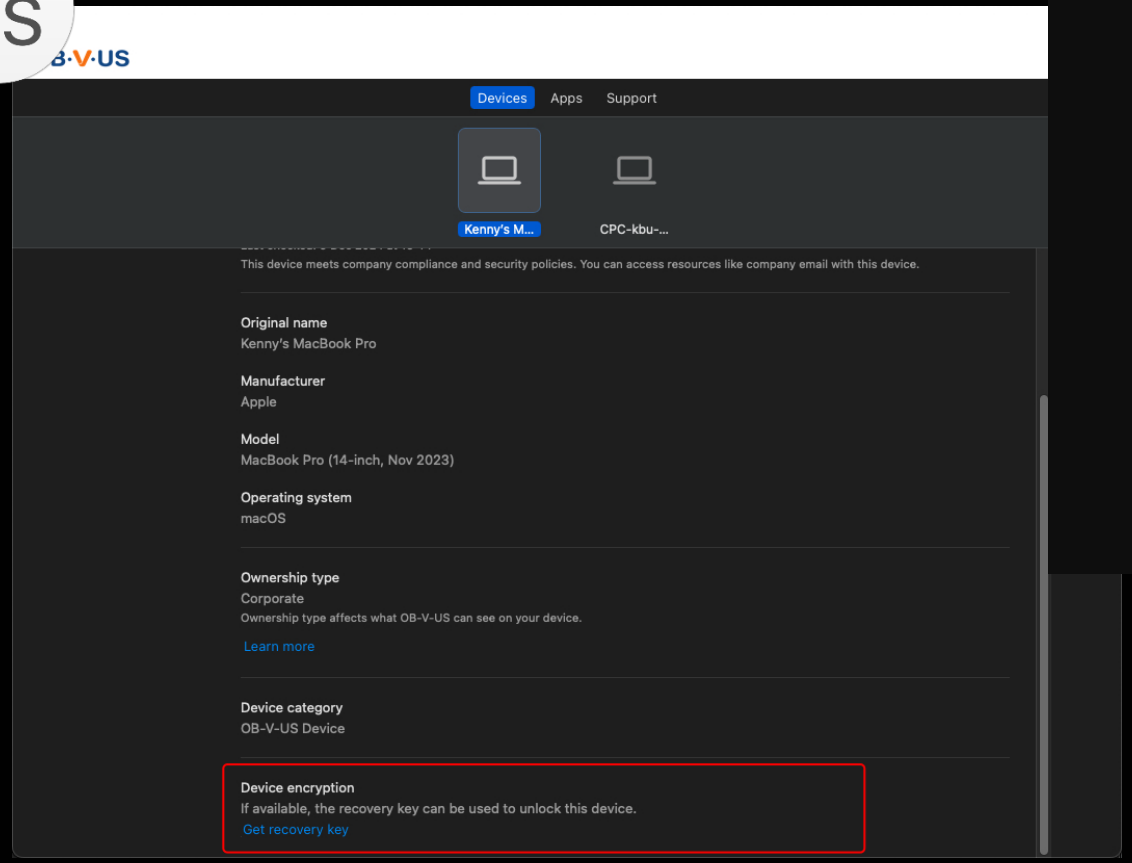
| | |
|---|---|
| Location | Your key will be escrowed to OB-V-US |

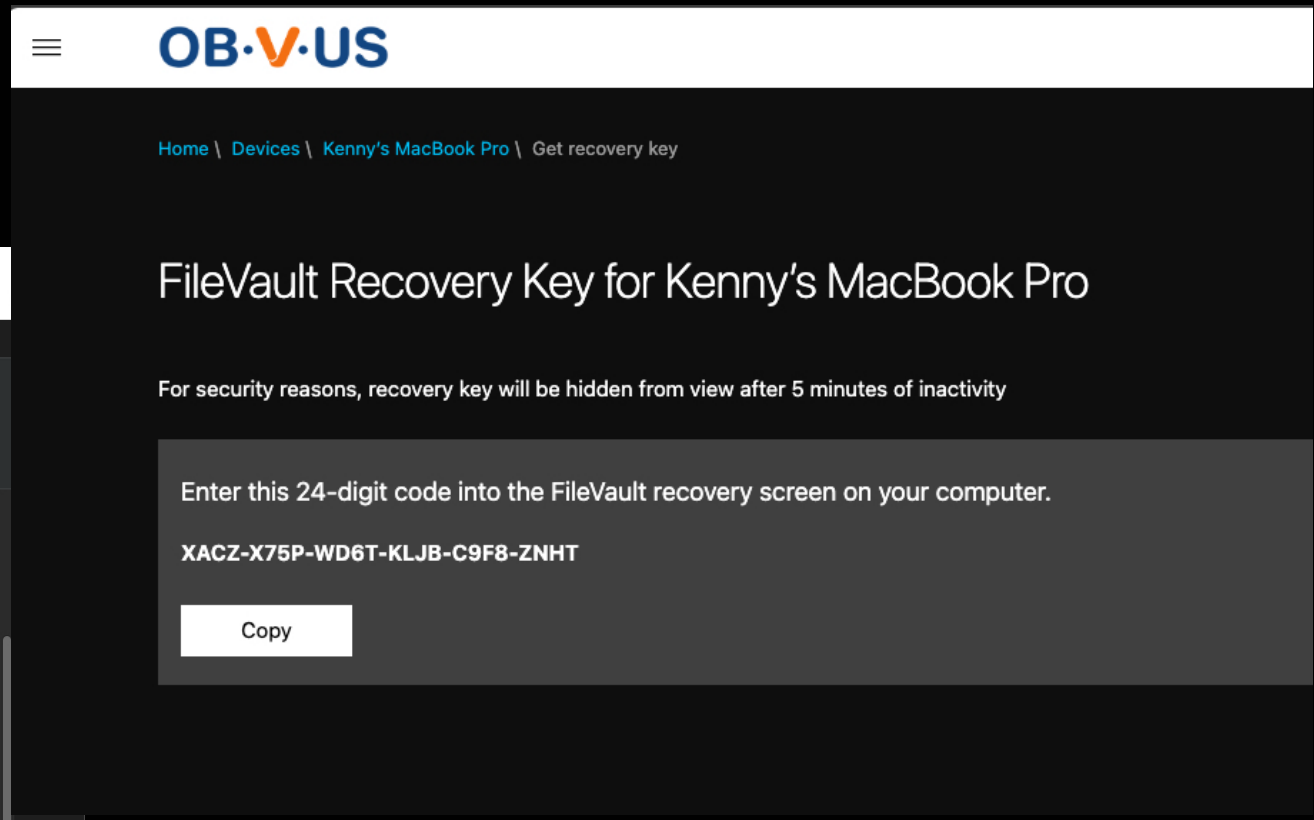


# Recovery Key

wpninjas.au

mac OS



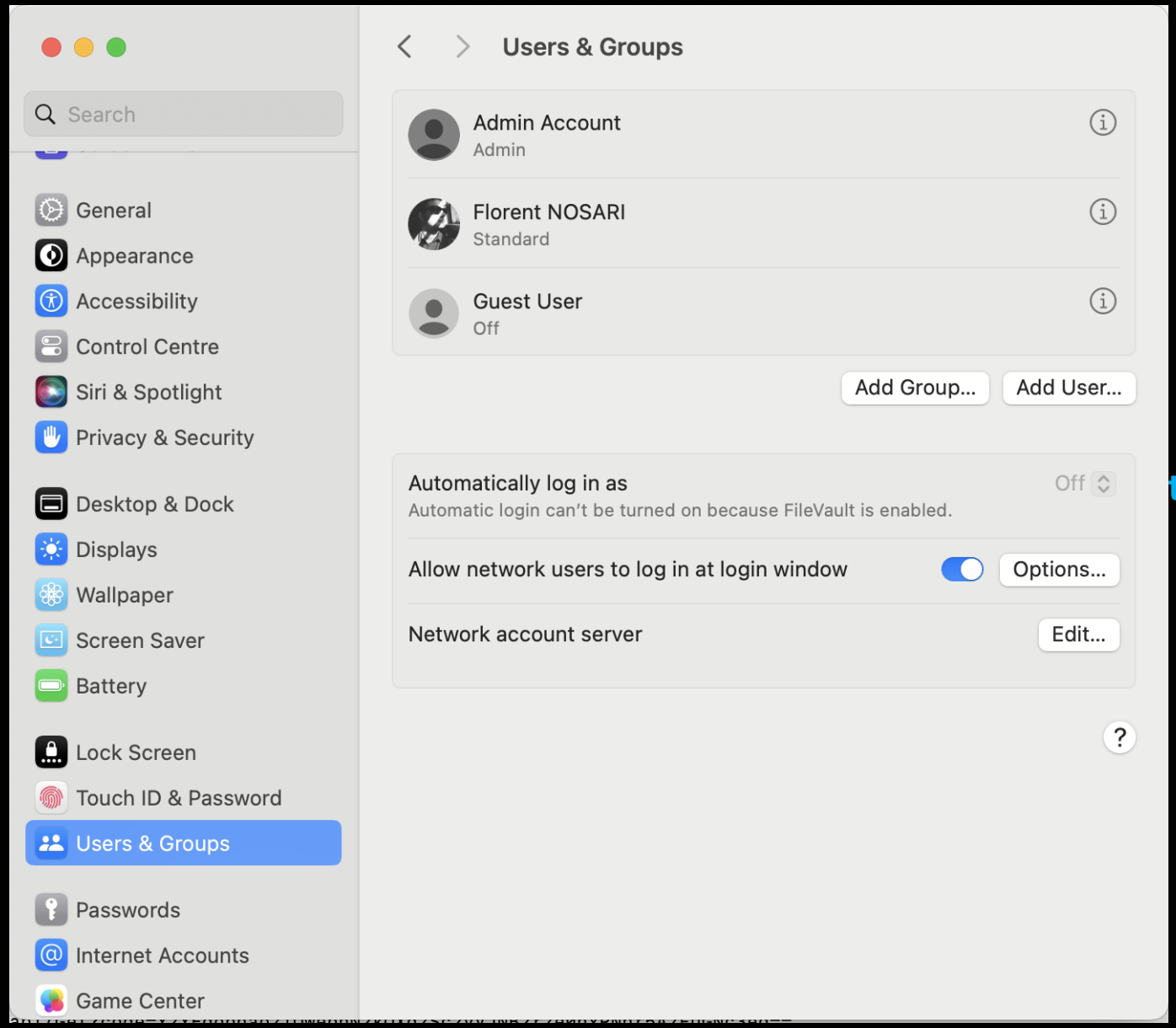



# LAPS for Mac




# M365 Profile Photo Download and Sync for macOS … ?

wpninjas.au




ts/macos-m365-picture/

# Improve security posture

# Introduction



# Software Updates

wpninjas.au

macOS Sonoma +

Declarative Device Management (DDM) 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

2 of 4 settings in this subcategory are not configured

Target Date Time (UTC) * 15/08/2024 3:00 PM

Target OS Version * 14.6.1


macOS Sequoia +

Create profile
macOS - Settings catalog

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

**Software Update Settings** Remove subcategory

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

# Lessons Learned ..

# Software Updates – Ring Principle



- Create Dynamic Groups for rings

**Rule syntax**

```
(device.deviceManagementAppId -ne null) and (device.deviceOSType -eq "MacMDM") and (device.deviceOwnership -eq "Company") and ((device.deviceId -startsWith "0") or (device.deviceId -startsWith "1") or (device.deviceId -startsWith "a"))
```

- Office Example

Microsoft AutoUpdate (MAU)

Configure the Microsoft AutoUpdate preferences to control the update process for Microsoft applications on devices.

| | |
|---|---|
| Days before forced updates | 2 |
| Deferred updates (Deprecated) | Defer 3 days |

# Lessons Learned



- User forgot their password
- ServiceDesk deleted Intune Computer object
- Bye Bye FileVault key because not synced in EntraID Object like Windows
- Reset of device mandatory

# Lessons learned

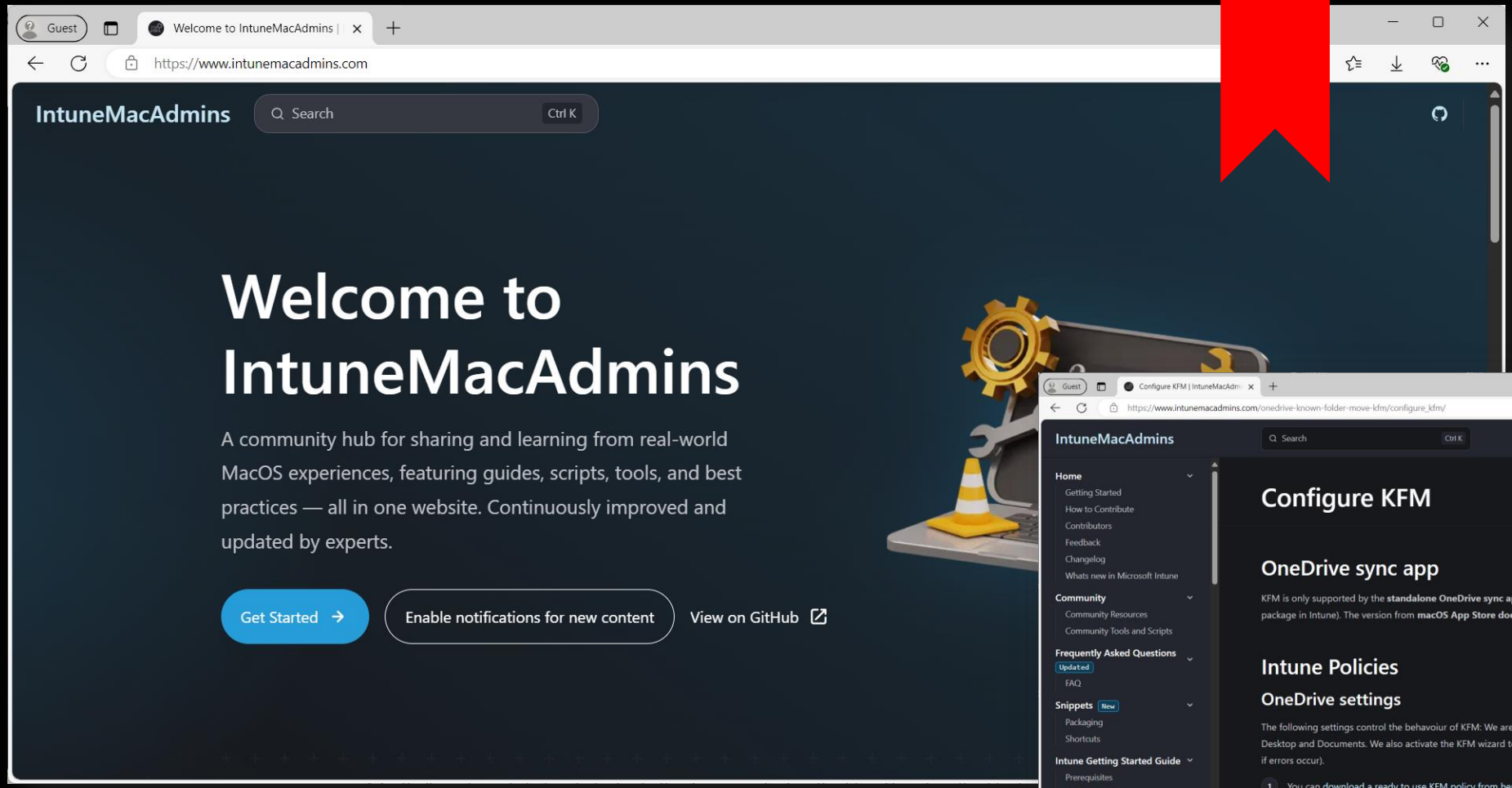


- If you do password sync –> Keep note of your Password Complexity policies
- If you still require SSO on non-Microsoft apps, add this to the Platform SSO policy
  - You can't have 2 SSO policies targeted on the same device → error
- No Built-in remote tool → You need a tool like Intune Suite Remote Control
- Release from ADE for end-of-lease device
- An existing MacBook and you want to add it to ADE
  - Use Apple configurator – but be aware the first 30 days end user could step out

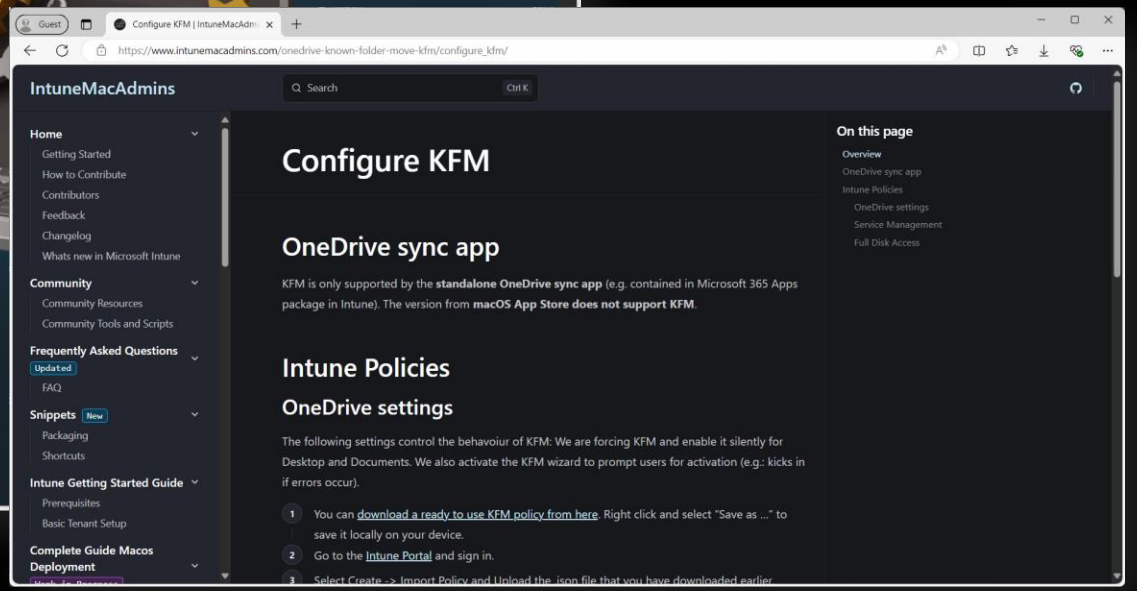
# Community Tools ?

# IntuneMacAdmins.com

wpninjas.au





# Community tools



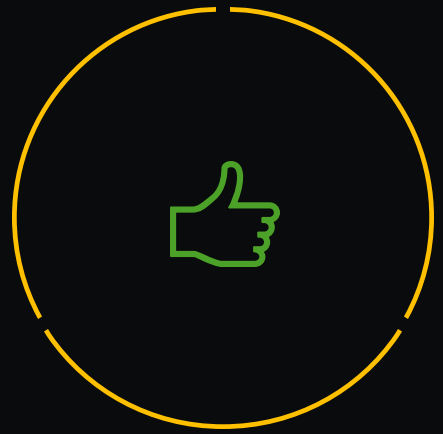
## GitHub Repo with scripts and information

GitHub



Microsoft

DEVICIE



# Thank You

Workplace


Microsoft
DEVICIE
Workplace Ninja Australia Tour

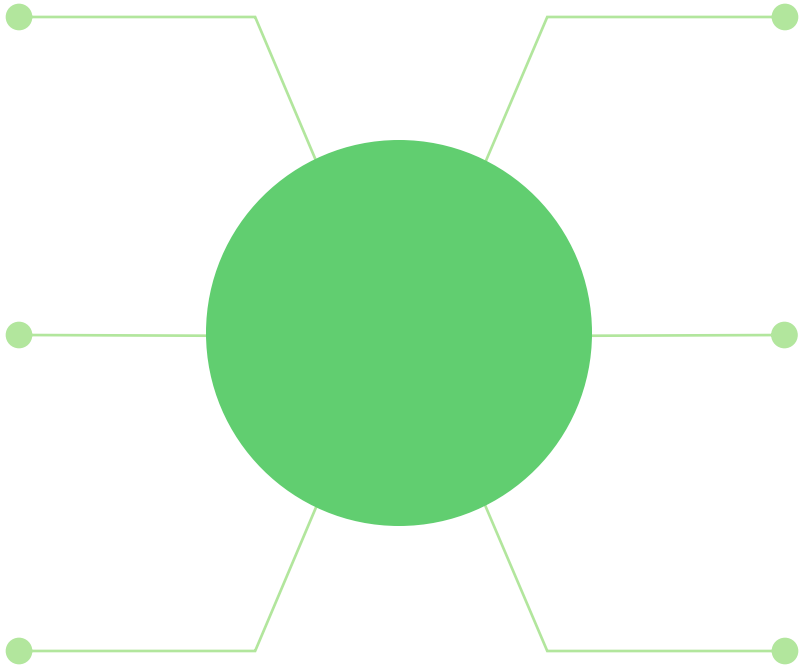


Microsoft

DEVICIE

# About You





# Thank You