



# Managing your Mac in the enterprise – Intune's magic potion



# Thank you sponsors!

liquidware™



W2Pint



CONSULTEQ

PROXSYS\*

O  
Daalmans  
consulting

Secure At Work

Technical Partners

Gold



# Agenda



## MacOS Management

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 “Kim Heyrman”

Endpoint Management

## Focus



Antwerp (Belgium)

## From

[www.obvus.be/blog](http://www.obvus.be/blog)

## My Blog



## Certifications

M365 , security and a pinch of AVD ..

## Hobbies

Gym, Gaming and football

## Contact

@kimmiez\_h



/in/kimmiez



Let's make **IT OB·V·US**  
> [www.obvus.be](http://www.obvus.be)





# 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](http://www.obvus.be/blog)



## Certifications



Former 14 year



## Hobbies

Beer, Cars & BBQ

## Contact

KBU@obvus.be

<https://twitter.com/kennybuntinx>

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

Let's make **IT OB-V-US**  
> [www.obvus.be](http://www.obvus.be)

# MacOS Management enrollment

How to get started compared to Windows endpoints





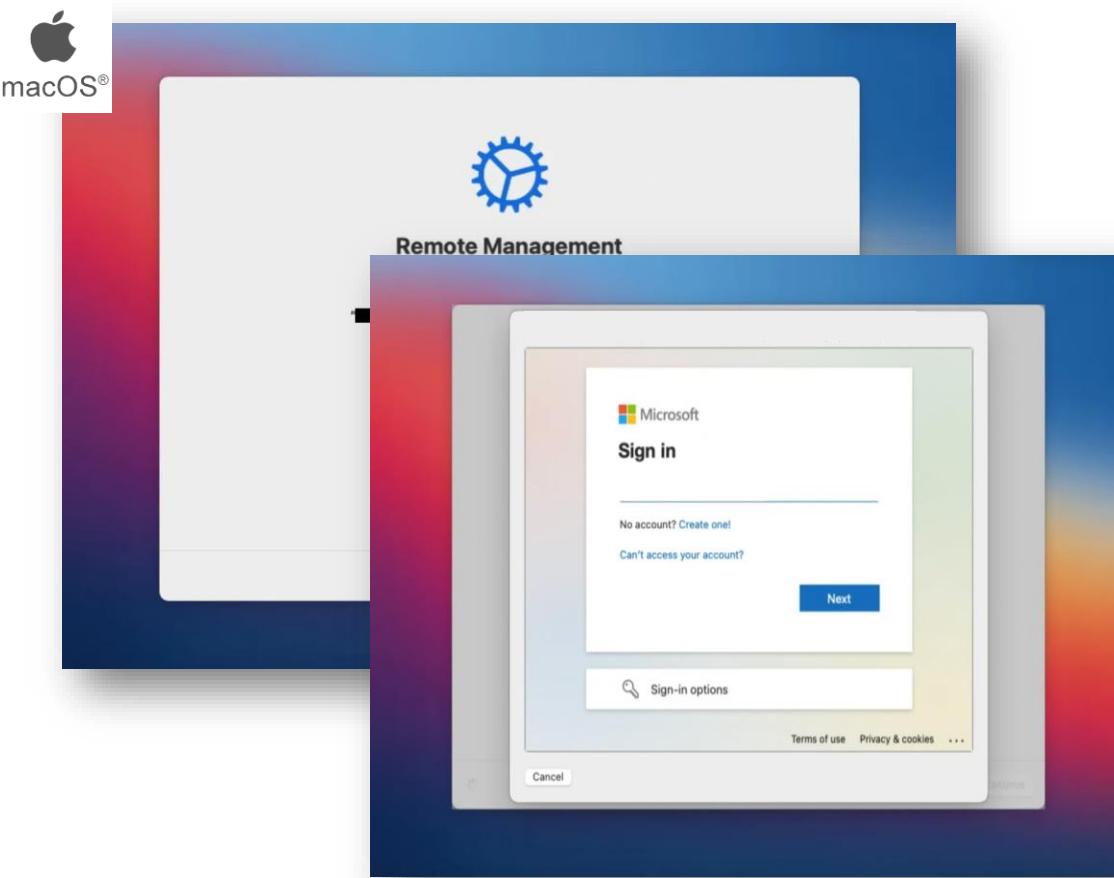
# Enterprises today...



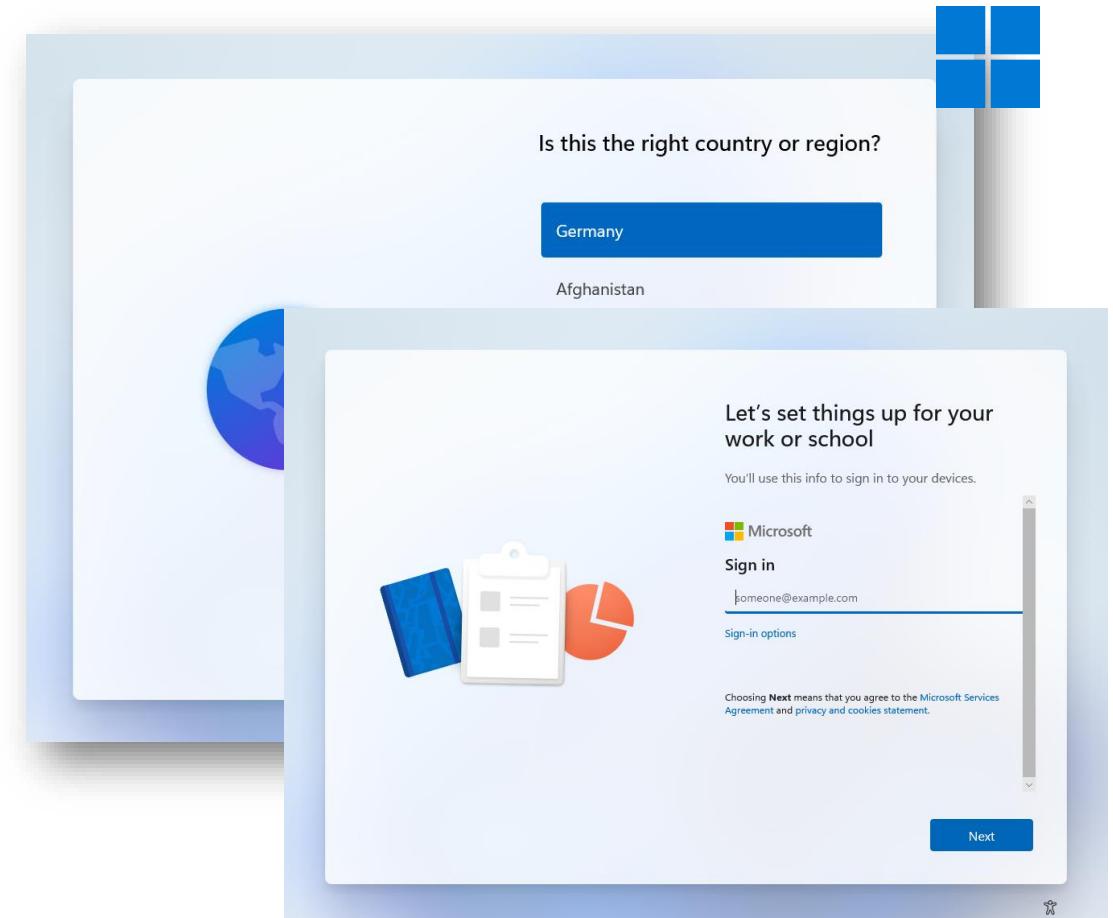


# How to get started – ADE ...

MacOS - Automatic Device Enrollment (ADE)



Windows - Autopilot





# How to get started with ADE

- **Automatic Device Enrollment (ADE)**

- Apple Business Manager
  - Link your Domain (like your Microsoft tenant)
  - To domain or not to domain capture ....



## 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.
  - **After enrollment Company Portal is required and user needs to sign in if**
    - users need access to CA protected resources
    - To complete Microsoft Entra registration

**Business**

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

**Managed Apple Accounts**

Supports Modern Authentication against Entra ID

Preview - Feature for User Creation

User sign in and directory sync

Custom identity providers sync to devices and services by using an existing user directory from an Identity Provider. Learn more

Get Started

**Note:**

- 2000 ADE tokens per tenant
- 1000 ADE profiles per tenant (a bit overkill 😊)
- 200k devices per token
- 3k devices are synced per minute

**Domains**

- b-sure.appleaccount.com
- b-sure.eu

7 unmanaged Apple Accounts found

Add domain

B-Sure Intune

0 Devices

Domain Capture



# 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](#)

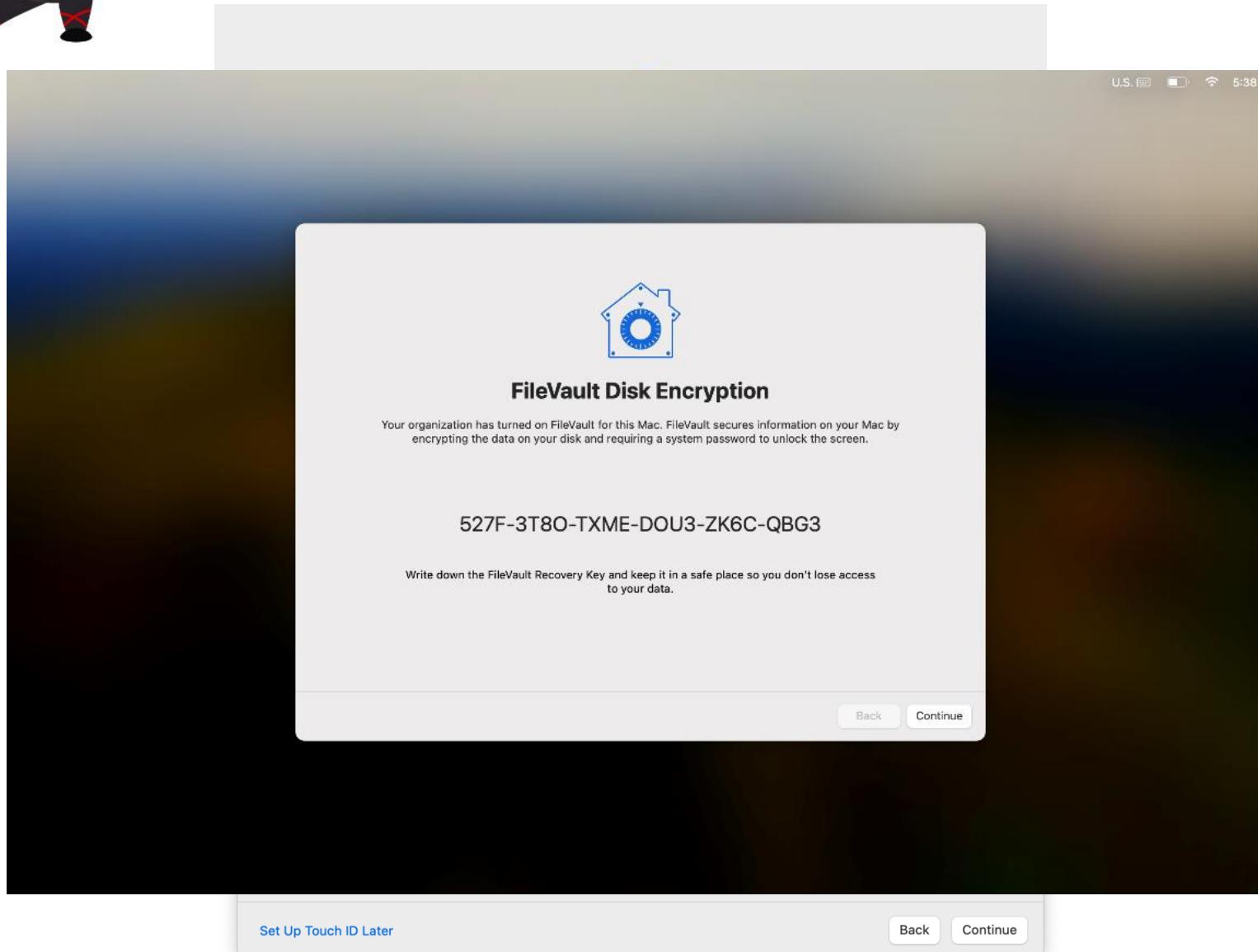
### Management Options

Await final configuration [Yes](#)

Locked enrollment [Yes](#)



# Enrollment Profile for ADE



A screenshot of a Mac OS X setup screen titled "FileVault Disk Encryption". It shows a blue house icon with a circular dial. Below it, the text "FileVault Disk Encryption" is displayed. A message states: "Your organization has turned on FileVault for this Mac. FileVault secures information on your Mac by encrypting the data on your disk and requiring a system password to unlock the screen." A unique recovery key is shown: "527F-3T8O-TXME-DOU3-ZK6C-QBG3". A note below says: "Write down the FileVault Recovery Key and keep it in a safe place so you don't lose access to your data." At the bottom are "Back" and "Continue" buttons. A green bar at the bottom left contains the text "Set Up Touch ID Later".

## 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}}

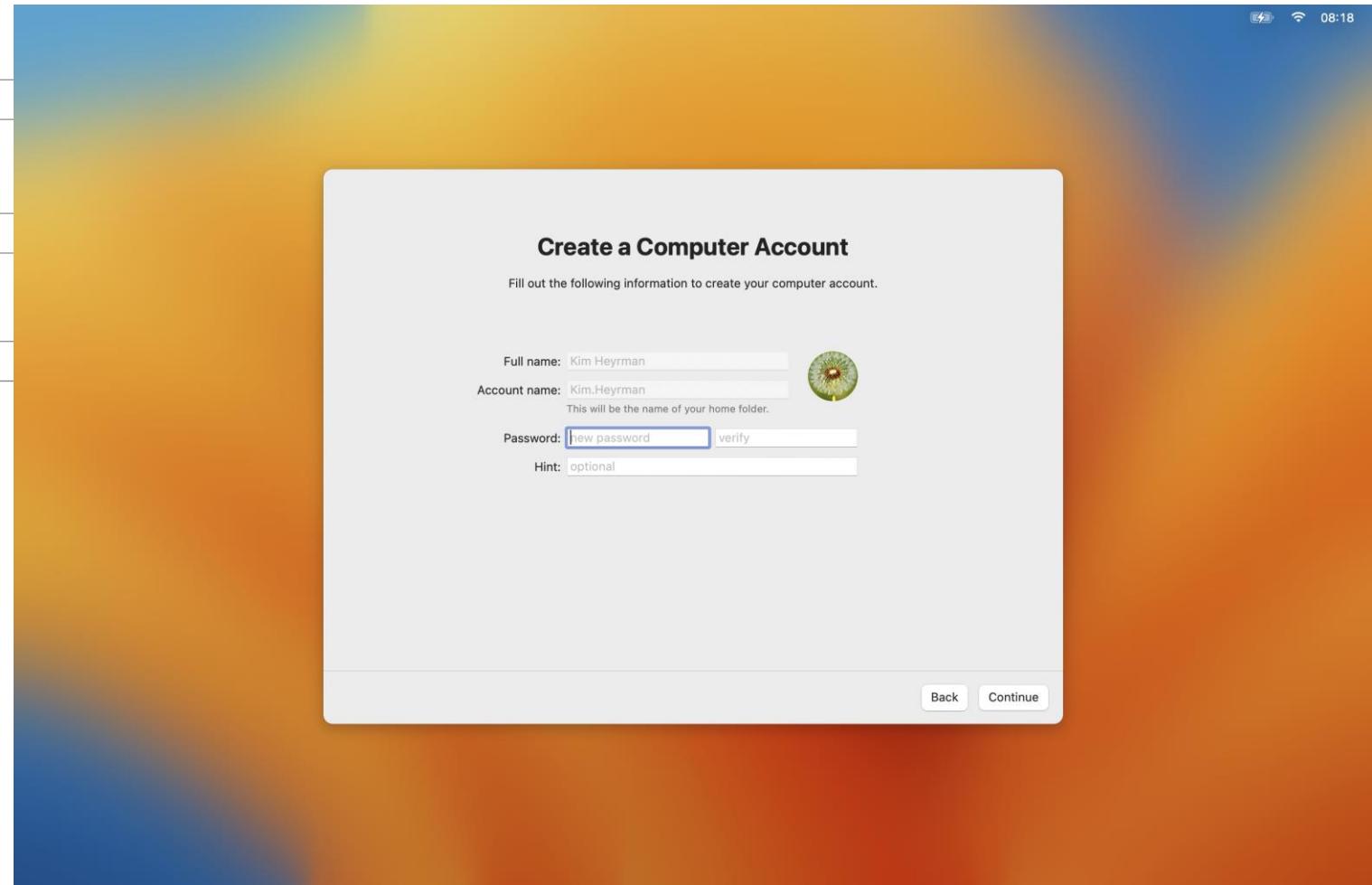
Supported variables: {{username}}

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

Home > Groups | All groups > OBVUS - CFG - MacOS - DDG - ADE enrolled

OBVUS - CFG - MacOS - DDG - ADE enrolled | Dynamic membership rules X

Group

Save Discard Got feedback?

i Overview X Diagnose and solve problems

v Manage

- Properties
- Members
- Owners
- Roles and administrators
- Administrative units
- Group memberships
- Applications
- Licenses

Configure Rules Validate Rules

You can use the rule builder or rule syntax text box to create or edit a dynamic membership rule. i [Learn more](#)

And/Or	Property	Operator	Value
	enrollmentProfileName	Equals	OB-V-US - Automated MacOS Enrollment

+ Add expression

**Rule syntax**

```
(device.enrollmentProfileName -eq "OB-V-US - Automated MacOS Enrollment")
```

o Edit



# Company portal Look & Feel

## Company Portal

The screenshot shows the Company Portal interface for a Mac device. At the top, there's a circular icon for 'mac OS' and the 'OB-V-US' logo. Below the header, there are tabs for 'Devices', 'Apps', and 'Support'. The main content area displays two devices: 'Kenny's MacBook Pro' (selected) and 'CPC-kbu-WDMVZ76'. The 'Kenny's MacBook Pro' card provides detailed information:

- Status:** In compliance. Last checked: 8 Dec 2024 at 12:49. This device meets company compliance and security policies.
- Original name:** Kenny's MacBook Pro
- Manufacturer:** Apple
- Model:** MacBook Pro (14-inch, Nov 2023)
- Operating system:** macOS
- Ownership type:** Corporate. Ownership type affects what OB-V-US can see on your device.

A blue 'Learn more' button is at the bottom right of the card.

The screenshot shows the 'Devices' page from the Company portal. The left sidebar includes links for Home, Apps, Downloads & updates, Devices (which is selected), and Help & support. The main content area is titled 'Devices' and contains sections for 'THIS DEVICE' and 'Other devices'.

**THIS DEVICE:** CPC-kbu-WDMVZ76 (Checked 2 minutes ago). It has a green checkmark indicating it can access company resources.

**Other devices:** Kenny's MacBook Pro (Checked 3 minutes ago). It also has a green checkmark indicating it can access company resources.

At the bottom right of the main content area, there's a 'Settings' button.

# Application Delivery ?

How to deploy applications to your MacBook compared to Windows endpoints





# Applications

Not all applications for MacBook are in VPP store !

## Apps

The screenshot shows the 'OB-V-US' Apple Business Manager interface. On the left, there's a sidebar with various management sections like 'Business', 'Activity', 'Locations', 'Users', 'User Groups', 'Access Management', 'Devices', 'Assignment History', 'Apps and Books' (which is selected), and 'Custom Apps'. The main area displays a search bar and a list of apps. The 'Windows App' by Microsoft Corporation is highlighted with a blue background. Other visible apps include WhatsApp Messenger, Microsoft OneDrive, Signal - Private Messenger, Microsoft Outlook, Apple Configurator, and Universal Print.

Sort By				7 Total
	WhatsApp Messenger	WhatsApp Inc.	iOS and macOS	★★★★★ €0.00
	Microsoft OneDrive	Microsoft Corporation	iOS App	★★★★★ €0.00
	Signal - Private Messenger	Signal Messenger, LLC	iOS App	★★★★★ €0.00
	Microsoft Outlook	Microsoft Corporation	iOS App	★★★★★ €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

The screenshot shows the VPP store interface. In the center, there's a card for the 'Windows App' by Microsoft Corporation, which is described as a 'macOS App' and 'Device Assignable'. Below this, there's a 'Buy Licenses' section with fields for 'Assign to' (Choose a Location), 'Price' (€0.00), 'Quantity' (0), and 'Payment Method' (None). A 'Get' button is at the bottom right. To the right, there's a grid of other app cards, including 'Kleos for Outlook' by Wolters Kluwer, 'To Do: s &...' by Microsoft Corporation, 'Microsoft Whiteboard' by Microsoft Corporation, and 'VCare - Belgium e-ID...' by V-Care®.

### Buy Licenses

Assign to: Choose a Location

Price: €0.00   Quantity: 0   Payment Method: None

Total Cost: €0.00   Get

### Manage Licenses

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



# Applications

## Package deployment

The screenshot shows the Microsoft Intune Company portal interface. On the left, there's a sidebar with a 'macOS' icon and a search bar. Below the search bar, 'macOS apps' is selected. The main area lists various macOS applications like Adobe Acrobat Reader, Apple Configurator, etc. On the right, a modal window titled 'Select app type' is open, showing a dropdown menu with options: 'Select app type', 'Microsoft 365 Apps', 'macOS', 'Microsoft Edge, version 77 and later', 'Web Application', 'Other', 'Line-of-business app', 'macOS app (DMG)', and 'macOS app (PKG)'. The 'macOS app (DMG)' option is highlighted with a yellow box and a red arrow pointing to it.

- 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.
  - preinstall 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 individual apps.
- Possible to cache the initial installation on a webserver.
- Possible to create a local MAU cache for updates. (only if you have slow slow connection and no \$\$\$ to upgrade your line)
- Includes the Microsoft Autoupdate feature which can be configured via plist to automatically download insider builds of Office for testing to some users.

### Disadvantages



server infrastructure for caching.

IT management skills.

Structure complexity.

# Improve your security posture

Platform SSO, Local Account Management and Software updates





# 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
- Enabled through MDM Profile



# Options

- **Secure Enclave**

- cryptographic key in Secure Enclave used for SSO with Entra ID
- comparable to Windows Hello
- 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

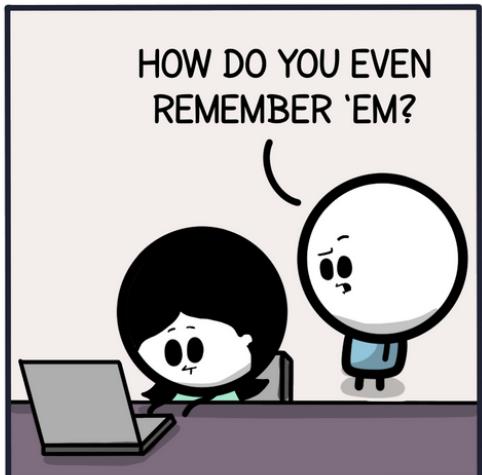


imgflip.com

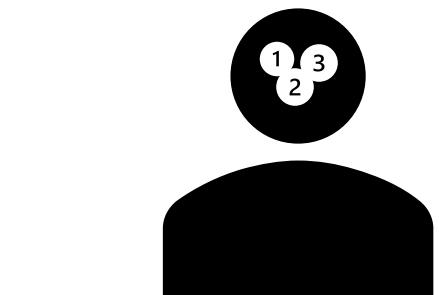
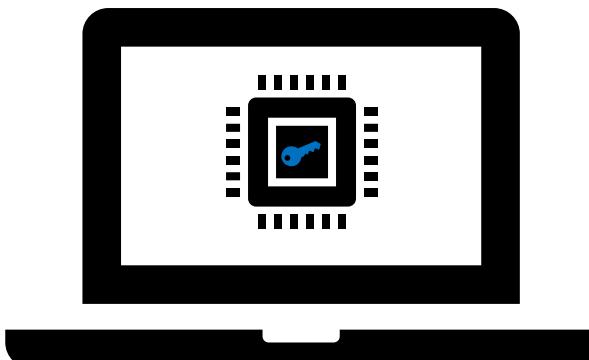
JAKE-CLARK.TUMBLR



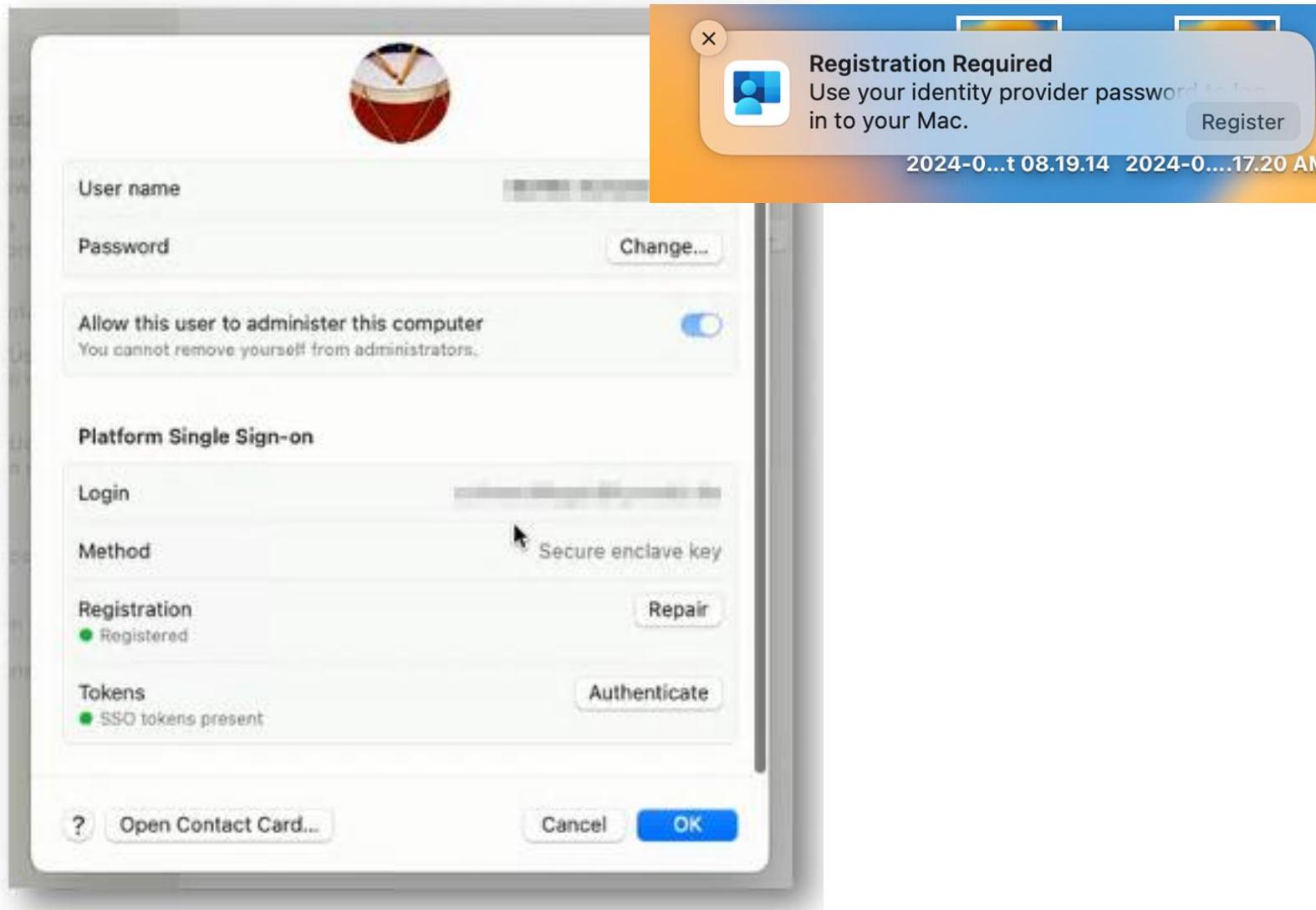
# Secure Enclave



- ♥ like Windows Hello
  - ♥ Touch ID possible
  - ♥ Hardware-bound cryptographic keys like TPM on Windows
  - ♥ Phishing resistant
  - ♥ SSO
  - ♥ passkey support
- 
- !
  - !
  - !
- !
  - !
  - !
- !
  - !
  - !
- !
  - !
  - !

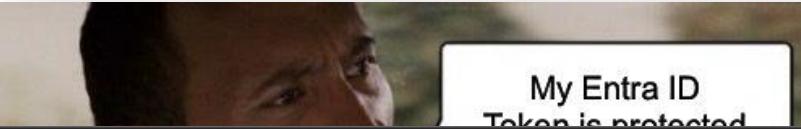


# Secure Enclave





# Secure Enclave



Keychain Access

All Items Passwords Secure Notes My Certificates Keys Certificates

primaryrefreshtoken-29d9ed98-a469-4536-ade2-f981bc1d605e--|N...ZTI4YWVvkNGQwOGNjMmM1YjY2YzkyYjFmMml3YTM5NGVmZDg3Nw

Kind: application password  
Account: e886fb6-a039-42b2-86a6-e2119dfd11a6.9dbb1daa-1942-4484-a034-c68de94c2d2f-login.windows.net  
Where: primaryrefreshtoken-29d9ed98-a469-4536-ade2-f981bc1d605e--|NDRiOGNmNj...0M2l0ODMyZTI4YWVvkNGQwOGNjMmM1YjY2YzkyYjFmMml3YTM5NGVmZDg3Nw  
Modified: Today, 19:45

Name	Kind	Date Modified
/ com.apple.account.Exchange.oauth-refresh-token	application password	8 Nov 2021 at 12:30:14
/ com.apple.account.Exchange.oauth-refresh-token	application password	8 Nov 2021 at 12:30:14
/ cura	application password	Yesterday, 10:40
/ primaryrefreshtoken-29d9ed98-a469-4536-ade2-f981b...kNGQwOGNjMmM1YjY2YzkyYjFmMml3YTM5NGVmZDg3Nw	application password	Today, 19:45
/ primaryrefreshtoken-29d9ed98-a469-4536-ade2-f981b...kNGQwOGNjMmM1YjY2YzkyYjFmMml3YTM5NGVmZDg3Nw	application password	Today, 20:28
/ primaryrefreshtoken-29d9ed98-a469-4536-ade2-f981b...kNGQwOGNjMmM1YjY2YzkyYjFmMml3YTM5NGVmZDg3Nw	application password	Today, 20:46
/ refreshoken-0000000480728c5--	application password	Today, 20:49
/ refreshoken-1--	application password	23 Sep 2024 at 16:19:54
primaryrefreshtoken-29d9ed98-a469-4536-ade2-f981bc1d605e-- N...	application password	Today, 20:49
jhhN2Y0M2M2NmE50DM4YTBrnJhJzA2OTcyMQ	application password	Today, 21:33
jhhN2Y0M2M2NmE50DM4YTBrnJhJzA2OTcyMQ	application password	Today, 21:39
jhhN2Y0M2M2NmE50DM4YTBrnJhJzA2OTcyMQ	application password	Today, 20:46
IGNjMmM1YjY2YzkyYjFmMml3YTM5NGVmZDg3Nw	application password	23 Sep 2024 at 16:23:13
NjhN2Y0M2M2NmE50DM4YTBrnJhJzA2OTcyMQ	application password	Today, 21:32
IGNjMmM1YjY2YzkyYjFmMml3YTM5NGVmZDg3Nw	application password	23 Sep 2024 at 16:23:30
ljjhN2Y0M2M2NmE50DM4YTBrnJhJzA2OTcyMQ	application password	3 Dec 2024 at 15:24:31
jhhN2Y0M2M2NmE50DM4YTBrnJhJzA2OTcyMQ	application password	Today, 20:40
NjhN2Y0M2M2NmE50DM4YTBrnJhJzA2OTcyMQ	application password	Today, 05:41
NjhN2Y0M2M2NmE50DM4YTBrnJhJzA2OTcyMQ	application password	Today, 20:29
NjhN2Y0M2M2NmE50DM4YTBrnJhJzA2OTcyMQ	application password	23 Sep 2024 at 16:19:54
NjhN2Y0M2M2NmE50DM4YTBrnJhJzA2OTcyMQ	application password	Today, 20:25
ijhhN2Y0M2M2NmE50DM4YTBrnJhJzA2OTcyMQ	application password	Today, 21:30
ijhhN2Y0M2M2NmE50DM4YTBrnJhJzA2OTcyMQ	application password	8 Oct 2024 at 11:53:48
ijhhN2Y0M2M2NmE50DM4YTBrnJhJzA2OTcyMQ	application password	Today, 21:33
ijhhN2Y0M2M2NmE50DM4YTBrnJhJzA2OTcyMQ	application password	Today, 21:39
ijhhN2Y0M2M2NmE50DM4YTBrnJhJzA2OTcyMQ	application password	Today, 20:46
NjhN2Y0M2M2NmE50DM4YTBrnJhJzA2OTcyMQ	application password	Today, 21:09

Attributes Access Control

Access for this item cannot be edited.

Access group for this item:

Name: UBF8T346G9.com.microsoft.identity.ssoextension

use and replay of Azure AD refresh token from Microsoft Edge in macOS Keychain

macOS | Configuration > macOS - Default - Device restriction

macOS - Default - Device restriction

Sync Sync (i) False

Sync Sync (i) False

Sync Sync (i) False

Sync Sync (i) False



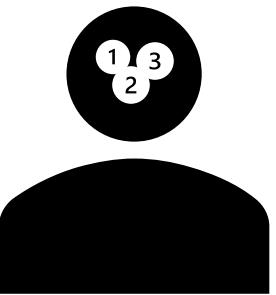
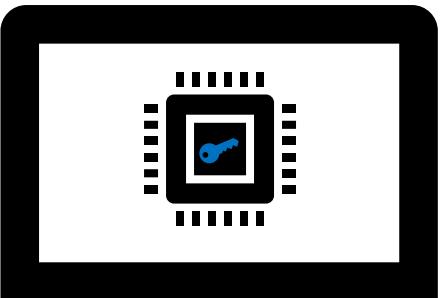
# Password sync



- ♥ 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



# Comparison as reference



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



# 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

Description ⓘ Only numeric #WHfB

Automatic Device Lock ⓘ 10

Failed Attempts Reset In Minutes ⓘ 10

Description ⓘ ANY ⓘ default

Minimum Passcode Length ⓘ 7

Regex ⓘ ^[0-9]+\$

Change At Next Auth ⓘ Enabled

Require Passcode on Device ⓘ True

Maximum Grace Period ⓘ 0

A magnifying glass icon is positioned over the "Custom Regex" field, highlighting the regular expression `^[0-9]+$`.



# Deploying SSO for Microsoft 365 Apps

New settings available with  
Intune 2408 + 2409 for macOS

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 ⓘ {{mail}} Ⓢ

Microsoft Outlook Remove subcategory

22 of 24 settings in this subcategory are not configured

Enable New Outlook ⓘ  New Outlook only Ⓢ Ⓢ

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



# 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**

Edit profile - macOS - Default - Edge - Profile and Sync - v3.0 - TF ...

Settings catalog

① Configuration settings ② Review + save

+ Add settings ⓘ

^ Microsoft Edge

258 of 259 settings in this category are not configured

Set Microsoft Edge as default browser ⓘ  Enabled

Remove category ⓧ

^ Microsoft Edge

257 of 259 settings in this category are not configured

Browser sign-in settings ⓘ Force users to sign-in to use the browser ⌄

Force synchronization of browser data and do not show the sync consent prompt ⓘ  Enabled

⊖

⊖

⊖

A screenshot of the Microsoft Intune Settings Catalog interface. The main title is "Edit profile - macOS - Default - Edge - Profile and Sync - v3.0 - TF ...". Below it is a "Settings catalog" section. On the left, there are two buttons: "Configuration settings" (marked with a blue circle and the number 1) and "Review + save" (marked with a blue circle and the number 2). Below these are links for "+ Add settings" and a help icon. A "Microsoft Edge" category is expanded, showing a message "258 of 259 settings in this category are not configured". Inside this category, a setting "Set Microsoft Edge as default browser" is shown with a status of "Enabled" and a blue toggle switch. This setting is highlighted with a red rectangular box. Below this, another "Microsoft Edge" category is expanded, showing a message "257 of 259 settings in this category are not configured". It contains a "Browser sign-in settings" section, which includes a dropdown menu set to "Force users to sign-in to use the browser" and a link "Force users to sign-in to use the browser". This entire "Browser sign-in settings" section is also highlighted with a red rectangular box.

# Improve security posture

FileVault & Local Admin





# Disk Encryption look & feel

## Disk encryption

mac OS

The screenshot shows the macOS System Preferences window for "FileVault". The "FileVault" section is open, displaying the following configuration:

- Defer**: Enabled (highlighted with a red border)
- Recovery Key Rotation In Months**: 3 months
- Enable**: On
- Show Recovery Key**: Enabled
- Force Enable In Setup Assistant**: True (highlighted with a red border)

**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

The screenshot shows the Windows Control Panel under "System and Security" with the "BitLocker Drive Encryption" link selected. The "Operating system drive" section shows "Windows (C): BitLocker on".

**BitLocker Drive Encryption**

Help protect your files and folders from unauthorized access by protecting your drives with BitLocker.

**Operating system drive**

Windows (C): BitLocker on

- Suspend protection
- Back up your recovery key
- Turn off BitLocker



# Recovery Key

Disk encryption



The screenshot shows the OB-V-US Devices interface. At the top, there are three tabs: Devices (which is selected), Apps, and Support. Below the tabs, there are two device icons: "Kenny's M..." and "CPC-kbu-...". A message below the icons states: "This device meets company compliance and security policies. You can access resources like company email with this device." The main content area displays the following device details:

- Original name:** Kenny's MacBook Pro
- Manufacturer:** Apple
- Model:** MacBook Pro (14-inch, Nov 2023)
- Operating system:** macOS
- Ownership type:** Corporate  
Ownership type affects what OB-V-US can see on your device.  
[Learn more](#)
- Device category:** OB-V-US Device

At the bottom of the page, there is a section titled "Device encryption" with the sub-instruction: "If available, the recovery key can be used to unlock this device." Below this, there is a blue link: "Get recovery key". This entire section is highlighted with a red rectangular border.



[Home](#) \ [Devices](#) \ [Kenny's MacBook Pro](#) \ Get recovery key

## FileVault Recovery Key for Kenny's MacBook Pro

For security reasons, recovery key will be hidden from view after 5 minutes of inactivity

Enter this 24-digit code into the FileVault recovery screen on your computer.

XACZ-X75P-WD6T-KLJB-C9F8-ZNHT

[Copy](#)



# LAPS for Mac

Get ready

It's coming



# Improve security posture

DDM - Software updates





# Introduction





# Software Updates

## Declarative Device Management (DDM)

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

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



**Restarting Your Computer**  
Your computer needs to restart to install updates.



**Managed Update**  
An update to macOS 14.4 is overdue. You can install it now or it will be installed automatically Today, 09:39.

macOS Sonoma +

[Remove category](#)

[Remove subcategory](#)

## Create profile

macOS - Settings catalog

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 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

macOS Sequoia +

[Remove subcategory](#)

# Lessons Learned ..

Common real-world macOS experiences





# 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 EntralD Object like Windows
- Reset of device mandatory

trying to remember the password I just reset and made 60 seconds ago





# Lessons learned

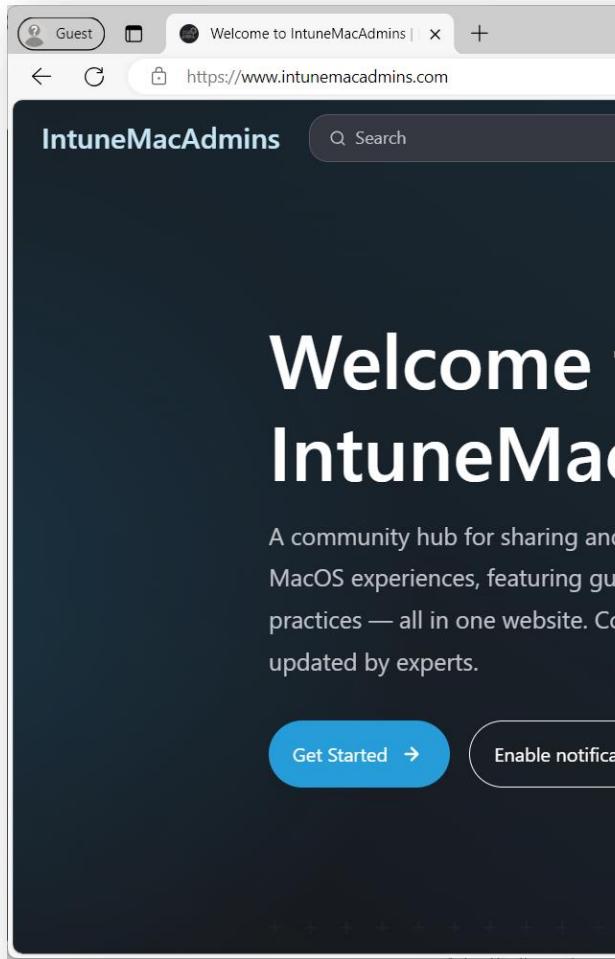
---

- If you do password sync → Keep note of your Password Complexity policies
- Make sure that per-user-MFA is not enabled if you want to setup PSSO
- 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
- You will need an extra tool like Intune Suite Remote Control ,TeamViewer or other as there is no built-in remote-control client
- When you need to hand back an end-of-lease device
  - Foresee an ADE release scenario
- If you buy an existing MacBook and want to add it to ADE
  - manually add it to ADE with Apple configurator – but be aware the first 30 days end user could step out

# Community Tools ?

Share and learn from real-world macOS experiences

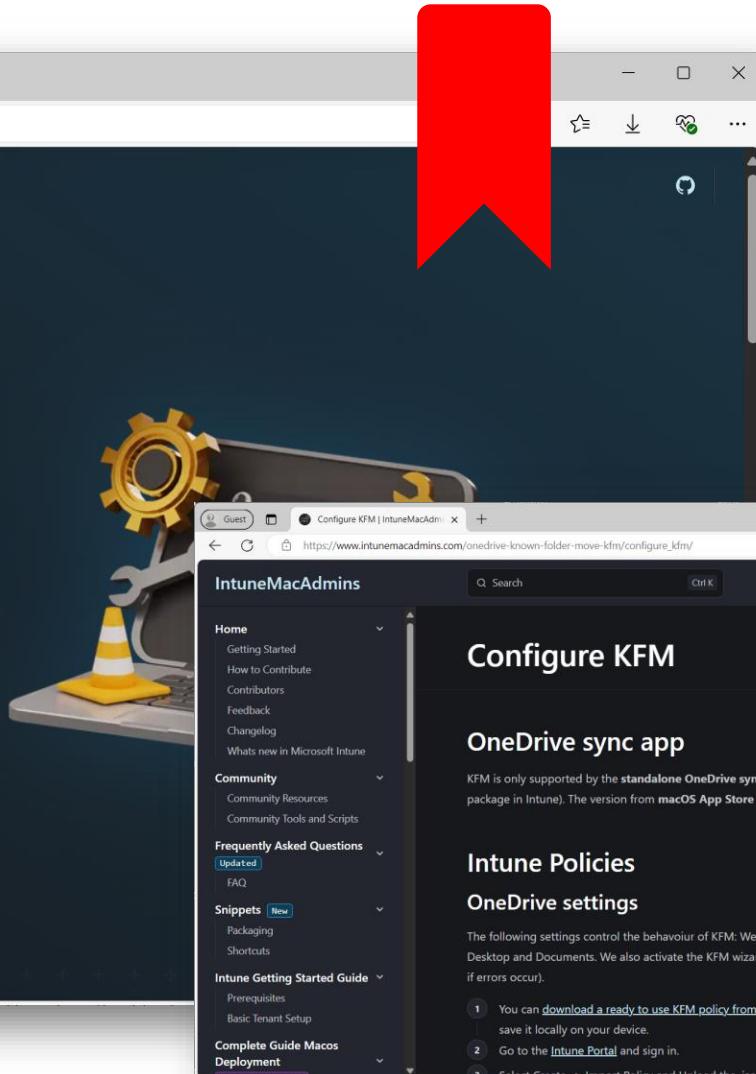




Welcome to IntuneMacAdmins

A community hub for sharing and learning from real-world MacOS experiences, featuring guides, scripts, tools, and best practices — all in one website. Continuously improved and updated by experts.

[Get Started →](#) [Enable notifications for new content](#) [View on GitHub](#)



Configure KFM

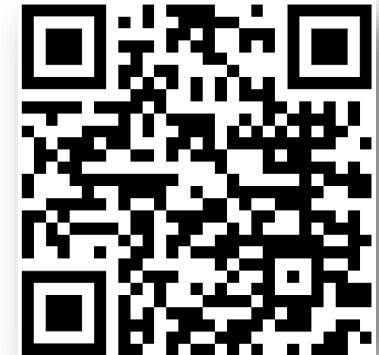
OneDrive sync app

Intune Policies

OneDrive settings

The following settings control the behaviour of KFM: We are forcing KFM and enable it silently for Desktop and Documents. We also activate the KFM wizard to prompt users for activation (e.g.: kicks in if errors occur).

- 1 You can [download a ready to use KFM policy from here](#). Right click and select "Save as ..." to save it locally on your device.
- 2 Go to the [Intune Portal](#) and sign in.
- 3 Select Create >> Import Policy and Upload the .json file that you have downloaded earlier.





## Community tools

GitHub Repo with scripts and information

