

Managing MacOS in the enterprise - Intune's magic potion



Workplace Ninja Australia Tour



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>

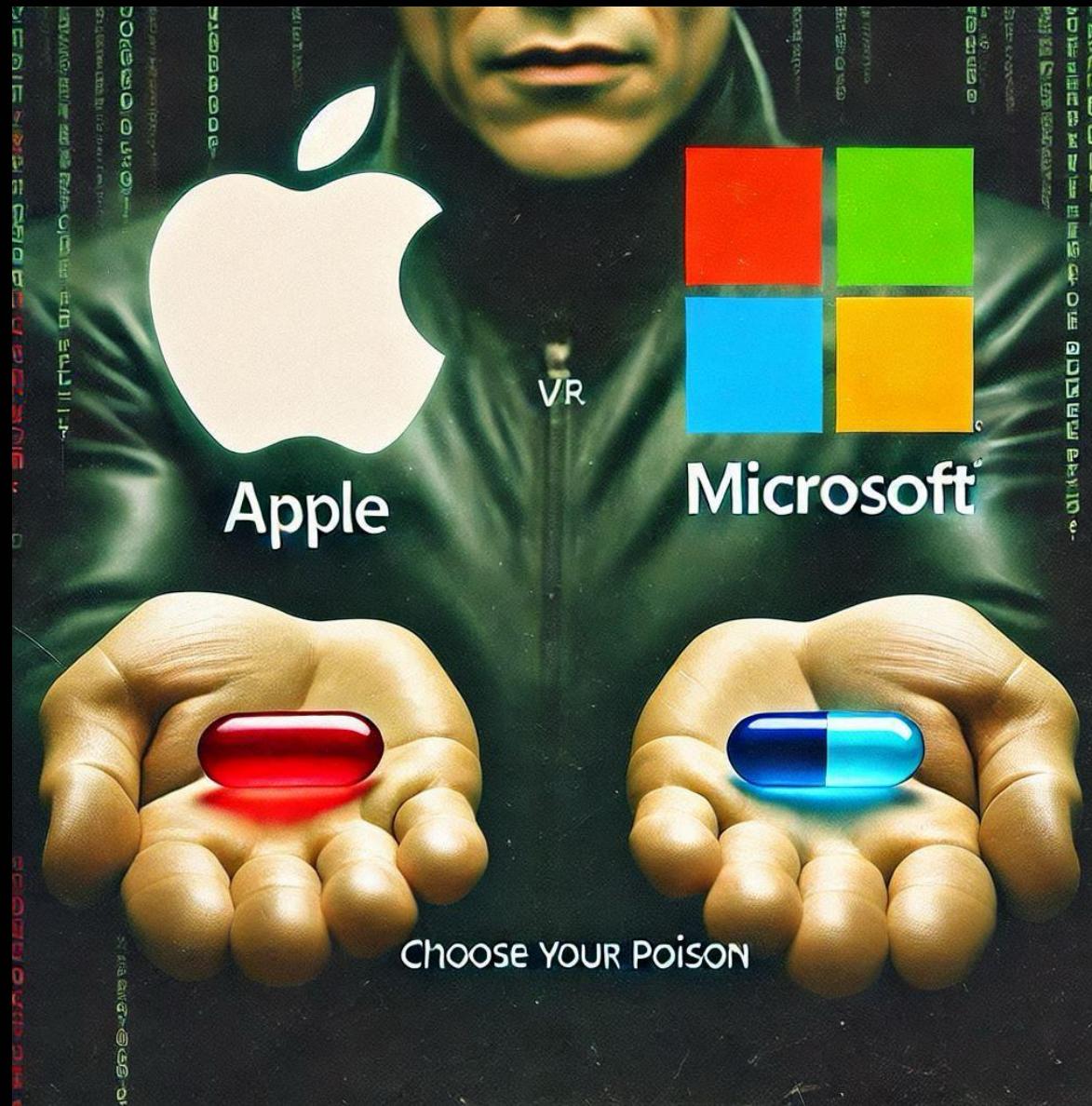
<https://www.linkedin.com/in/kennyBuntinx>



MacOS Management enrollment



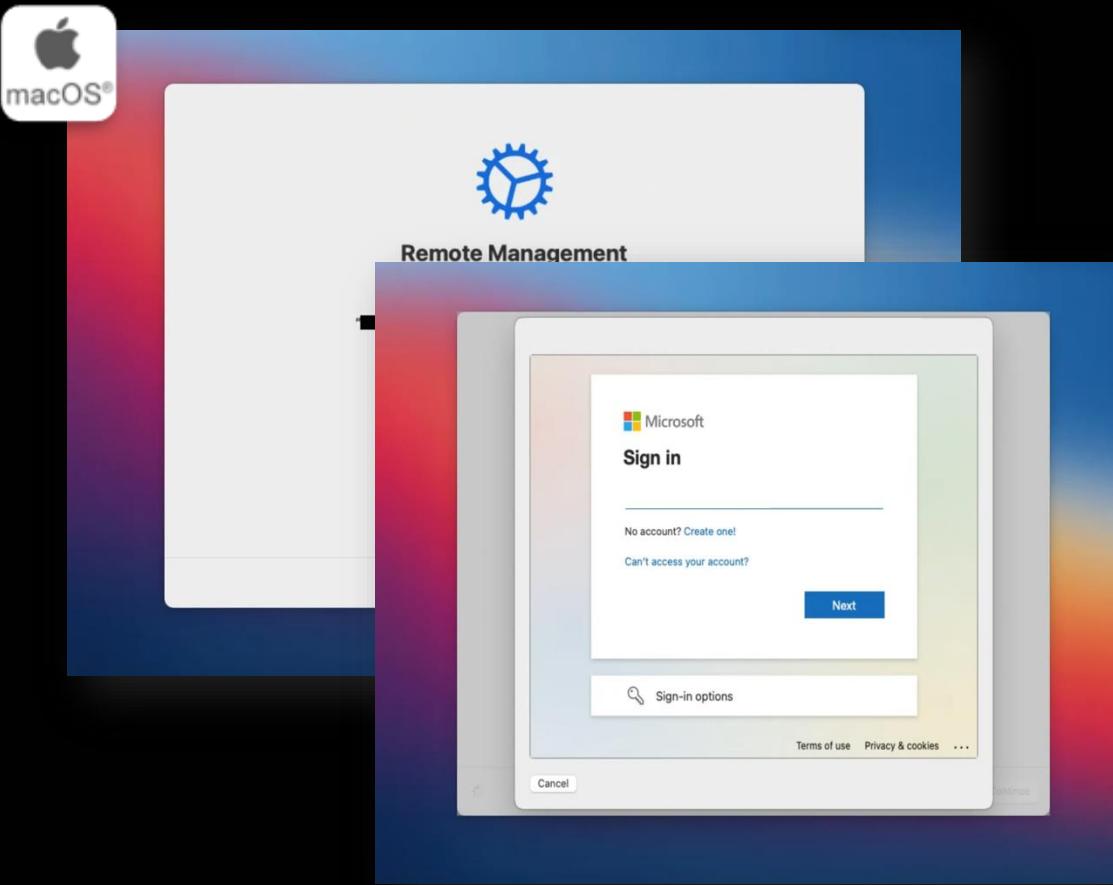
Enterprises today...



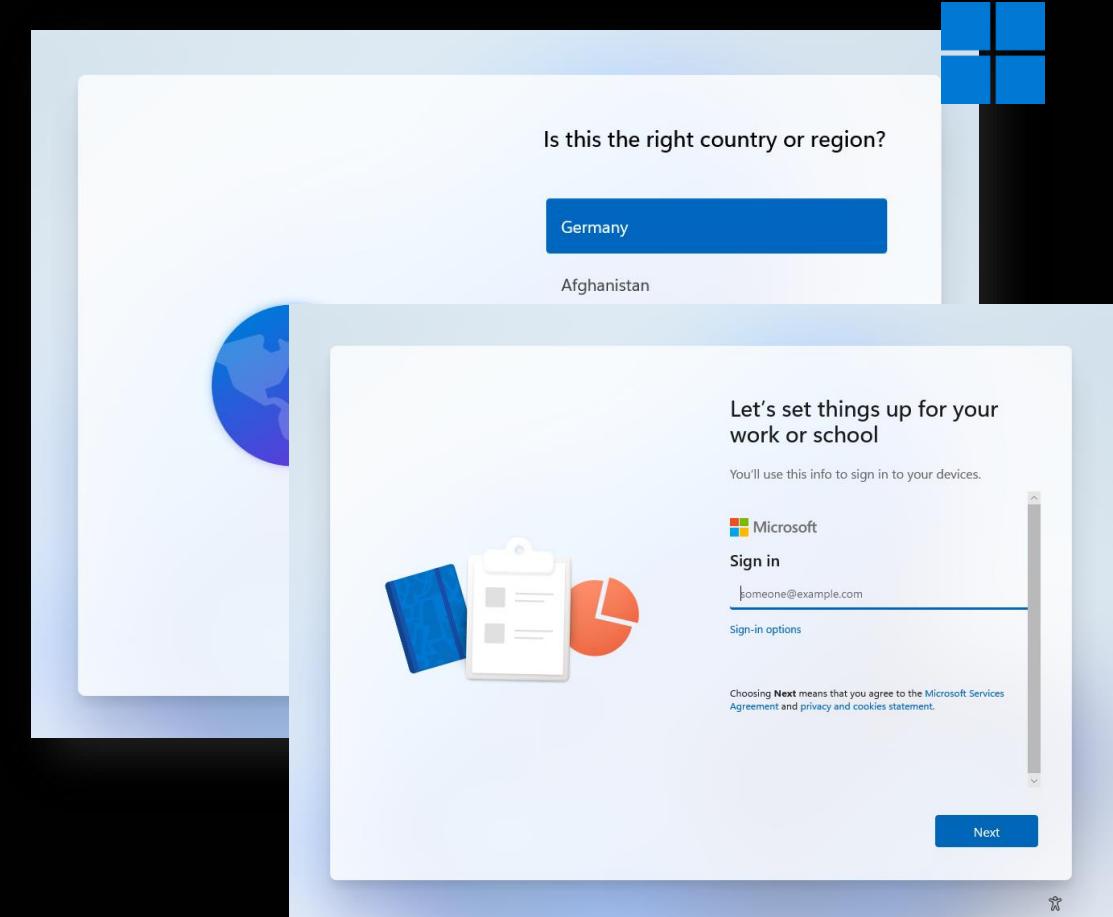


How to get started – ADE ...

MacOS - Automatic Device Enrollment (ADE)



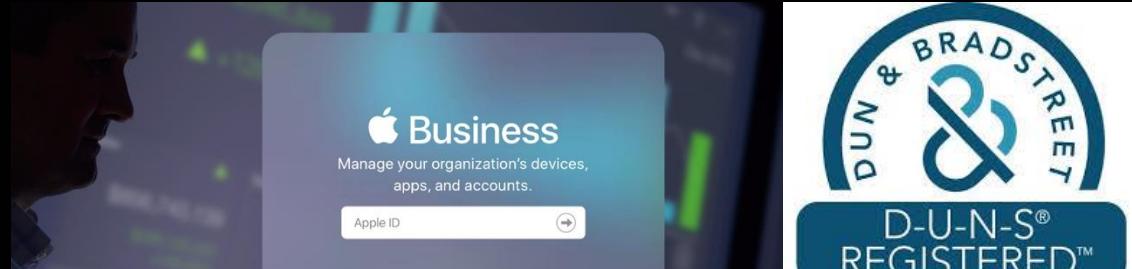
Windows - Autopilot





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.

B-Sure Intune
0 Devices

+ Add domain



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

FileVault Disk Encryption

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.

527F-3T8O-TXME-DOU3-ZK6C-QBG3

Write down the FileVault Recovery Key and keep it in a safe place so you don't lose access to your data.

Back Continue

Set Up Touch ID Later

Back Continue

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 *

Prefill account info ⓘ Yes Not configured

Primary account name * ⓘ

Supported variables: {{partialupn}}

Primary account full name * ⓘ

Supported variables: {{username}}

Restrict editing ⓘ Yes Not configured

Await final configuration required !!

08:18

Create a Computer Account

Fill out the following information to create your computer account.

Full name: 

Account name:
This will be the name of your home folder.

Password: verify

Hint:

Back Continue



Dynamic groups for ADE Enrollment Profile

wpnijas.au

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

Group

Save Discard Got feedback?

Overview Diagnose and solve problems 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. [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")
```

Edit

Application Delivery ?





Company portal Look & Feel

The screenshot shows the OB-V-US company portal interface running on macOS. The top navigation bar includes a circular icon for 'mac OS' and the 'OB-V-US' logo. Below the bar, there are tabs for 'Devices' (which is selected), 'Apps', and 'Support'. The main content area displays two devices: 'Kenny's MacBook Pro' (selected) and 'CPC-kbu-...'. The 'Kenny's MacBook Pro' card provides detailed information about the device, including its status ('In compliance'), last check time ('8 Dec 2024 at 12:49'), and ownership type ('Corporate'). Other details listed include manufacturer (Apple), model (MacBook Pro (14-inch, Nov 2023)), operating system (macOS), and a note about ownership type affecting what OB-V-US can see on the device.

The screenshot shows the OB-V-US company portal interface running on Windows. The top navigation bar includes a circular profile picture and the 'OB-V-US' logo. Below the bar, there are tabs for 'Home', 'Apps', 'Downloads & updates', 'Devices' (selected), and 'Help & support'. The main content area is titled 'Devices' and shows a section for 'THIS DEVICE' containing 'CPC-kbu-WDMVZ76' (checked 2 minutes ago) and a status message indicating it can access company resources. Below this is a section for 'Other devices' showing 'Kenny's MacBook Pro' (checked 3 minutes ago) with the same status message. At the bottom, there is a 'Settings' button.



Applications

Not all applications for MacBook are in VPP store !

The screenshot shows the OB-V-US application management interface on macOS. The sidebar includes sections for Business (Activity, Locations, Users, User Groups, Access Management, Devices, Assignment History), Apps and Books, and Custom Apps. The main area displays a list of available applications:

App Name	Developer	Type	Rating	Price
WhatsApp Messenger	WhatsApp Inc.	iOS and macOS App	★★★★★	€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 "Windows App" entry is highlighted with a blue background. To the right, a detailed view of the "Windows App" listing is shown, including a "Buy Licenses" section where users can assign locations, set price and quantity, and choose payment methods. The total cost is listed as €0.00. Below this, a "Manage Licenses" section shows the current usage and availability across different locations.

Applications



The screenshot shows the macOS App Store interface. On the left, there's a sidebar with a search bar, an 'Add' button, a 'Refresh' button, and a 'macOS apps' section. Below that is a list of installed applications: Adobe Acrobat Reader..., Apple Configurator, DisplayLink Login Scree..., DisplayLink Manager G..., F5Access, Firefox, Microsoft 365 Apps, Microsoft Edge, version 77 and later, Microsoft Defender for Endpoint, Web Application, macOS web clip, Other, Web link, Line-of-business app, macOS app (DMG), and macOS app (PKG). A red box highlights the 'macOS app (DMG)' option in the 'Line-of-business app' section of the 'Select app type' dialog box. A red arrow points from the bottom of the 'macOS app (DMG)' text towards the 'macOS app (PKG)' text.

- **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

wpnijas.au

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 files on a webserver.
- Possible to create a local MAU cache server (only if you have slow slow slow internet and need to upgrade your line)
- Includes the Microsoft Autoupdate (MAU) configured via plist to auto update and deployment of Office for testing to some users.

Disadvantages

- server infrastructure for caching.
- scripting skills.
- structure complexity.





Deploying Custom Apps the Ugur way

INTUNE BREW

macOS Apps in Intune 

Automates the entire workflow from downloading apps to uploading them to Intune, complete with proper metadata and logos.

▶ Download Now!

github.com/ugurkocde/IntuneBrew

 ugurkocde
  @ugurkocde
  BLOG www.ugurkoc.de

www.github.com/ugurkocde/IntuneBrew



IntuneBrew - Automated macOS Application Deployment via Microsoft Intune
Made by Ugur Koc with ❤️ and 🍷 | Version 0.2 Public Preview | Last updated: 2024-10-23

This is a preview version. If you have any feedback, please open an issue at <https://github.com/ugurkocde/intuneBrew/issues>. Thank you!

App ID, Tenant ID, or Certificate Thumbprint is missing or not set correctly.
Would you like to attempt a manual interactive connection? (y/n): y
Attempting manual interactive connection...
Successfully connected to Microsoft Graph using interactive sign-in.
All required permissions are present.

Available applications:

- adobe_acrobat_reader
- company_portal
- google_chrome
- keepassxc
- microsoft_teams
- mozilla_firefox
- parallels_desktop
- slack
- spotify
- windows_app
- zoom

Enter app names separated by commas:
all

App Name	Github Version	Intune Version	Status
Spotify	1.2.48-405		Up-to-date
Mozilla Firefox	131.0.3		Up-to-date
Windows App			Not in Intune
Zoom			Not in Intune
Company Portal			Not in Intune
Parallels Desktop			Not in Intune
Adobe Acrobat Reader	24.093.20112		Up-to-date
Microsoft Teams			Not in Intune
Slack	4.41.96		Up-to-date
Google Chrome	130.0.6723.70		Up-to-date
KeePassXC	2.7.9		Up-to-date

Found 5 new apps to upload. Do you want to continue? (y/n):

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

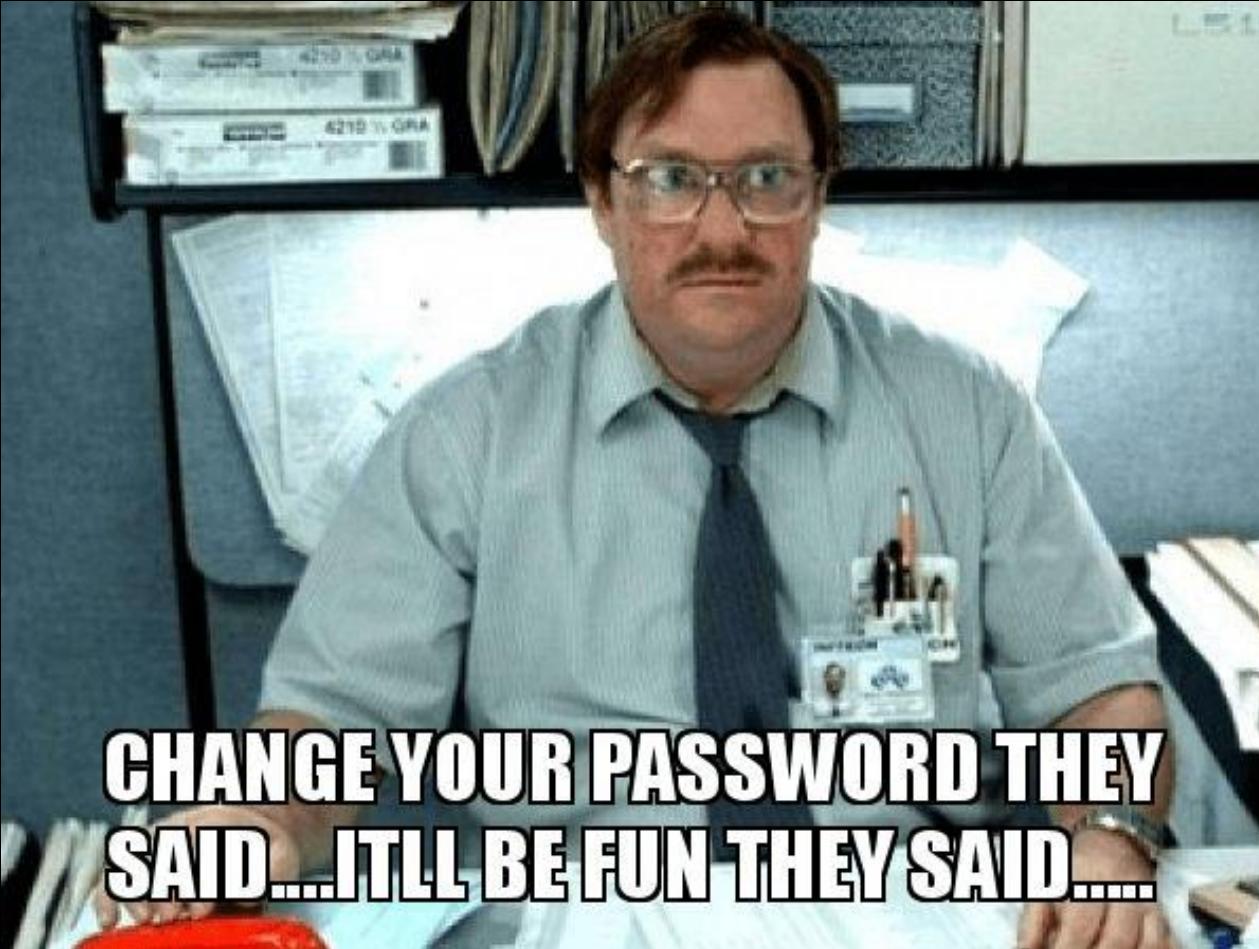


imgflip.com

JAKE-CLARK.TUMBLR



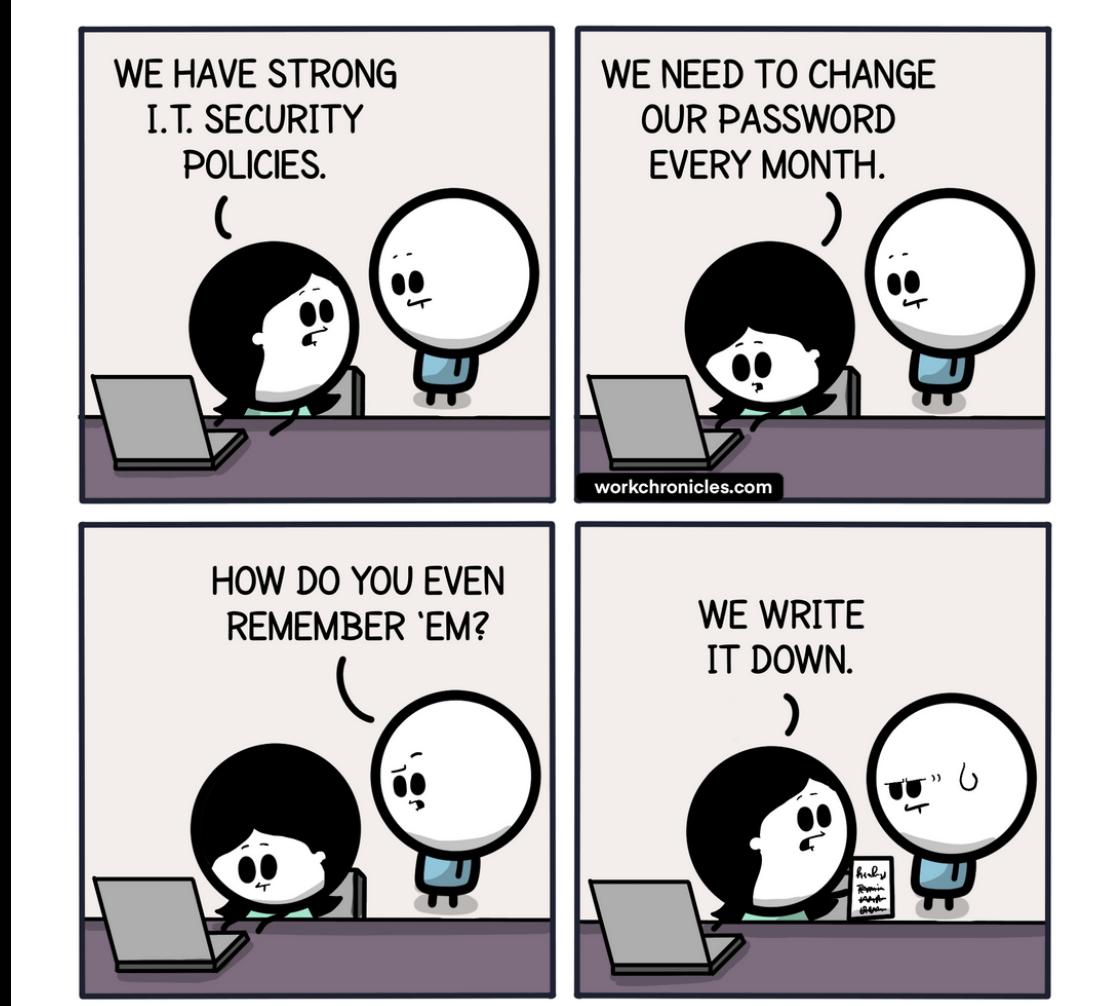
Password sync



- ♥ 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

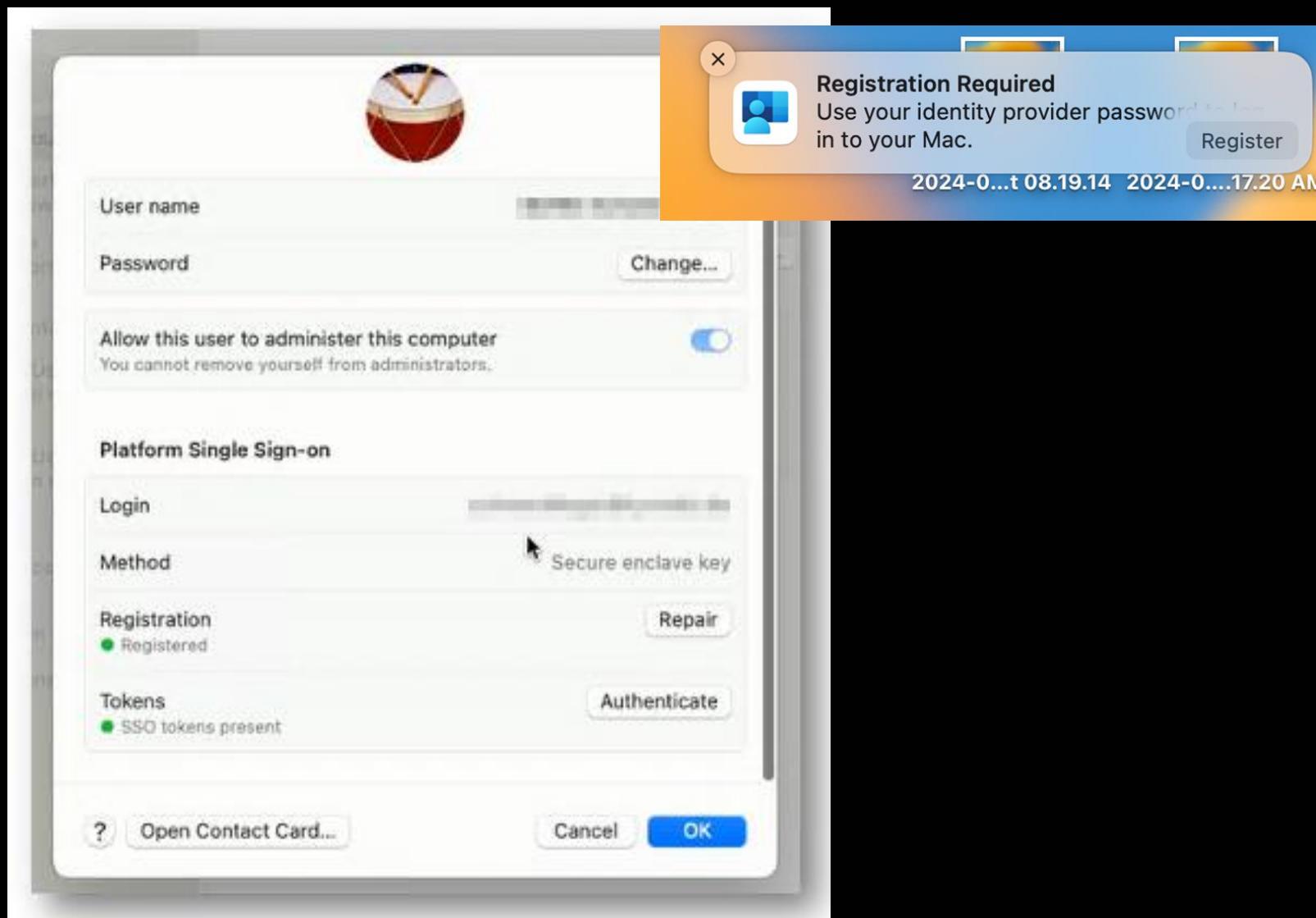
Secure Enclave



- ♥ 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

The screenshot shows the Mac OS X Keychain Access application. The left sidebar lists 'Default Keychains' (login, iCloud) and 'System Keychains' (System, System Roots). The main pane is titled 'Keychain Access' and shows a list of items under the 'All Items' tab. The top item is a selected 'primaryrefreshtoken' entry. Below it is a table of other items:

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-f981bc1d605e-- N...ZT14YWVkJMmM1YjY2YzkyYjFmMml3YTM5NGVmZDg3Nw	application password	Today, 19:45
primaryrefreshtoken-29d9ed98-a469-4536-ade2-f981bc1d605e-- NDRiOGNmNj...0M2i0ODMyZT14YWVkJMmM1YjY2YzkyYjFmMml3YTM5NGVmZDg3Nw	application password	Today, 20:28
primaryrefreshtoken-29d9ed98-a469-4536-ade2-f981bc1d605e-- N...kNGQwOGNjMmM1YjY2YzkyYjFmMml3YTM5NGVmZDg3Nw	application password	Today, 20:46
refreshtoken-00000000480728c5--	application password	Today, 20:49
refreshtoken-1--	application password	23 Sep 2024 at 16:19:54
jhhN2Y0M2NmE50DM4YTBrNjJhZjA2OTcymQ	application password	Today, 20:49
jhhN2Y0M2NmE50DM4YTBrNjJhZjA2OTcymQ	application password	Today, 21:33
jhhN2Y0M2NmE50DM4YTBrNjJhZjA2OTcymQ	application password	Today, 21:39
jhhN2Y0M2NmE50DM4YTBrNjJhZjA2OTcymQ	application password	Today, 20:46
jGnjMmM1YjY2YzkyYjFmMml3YTM5NGVmZDg3Nw	application password	23 Sep 2024 at 16:23:13
NjhhN2Y0M2NmE50DM4YTBrNjJhZjA2OTcymQ	application password	Today, 21:32
jGnjMmM1YjY2YzkyYjFmMml3YTM5NGVmZDg3Nw	application password	23 Sep 2024 at 16:23:30
ijhhN2Y0M2NmE50DM4YTBrNjJhZjA2OTcymQ	application password	3 Dec 2024 at 15:24:31
jhhN2Y0M2NmE50DM4YTBrNjJhZjA2OTcymQ	application password	Today, 20:40
NjhhN2Y0M2NmE50DM4YTBrNjJhZjA2OTcymQ	application password	Today, 05:41
NjhhN2Y0M2NmE50DM4YTBrNjJhZjA2OTcymQ	application password	Today, 20:29
NjhhN2Y0M2NmE50DM4YTBrNjJhZjA2OTcymQ	application password	23 Sep 2024 at 16:19:54
NjhhN2Y0M2NmE50DM4YTBrNjJhZjA2OTcymQ	application password	Today, 20:25
ijhhN2Y0M2NmE50DM4YTBrNjJhZjA2OTcymQ	application password	Today, 21:30
ijhhN2Y0M2NmE50DM4YTBrNjJhZjA2OTcymQ	application password	8 Oct 2024 at 11:53:48
ijhhN2Y0M2NmE50DM4YTBrNjJhZjA2OTcymQ	application password	Today, 21:33
ijhhN2Y0M2NmE50DM4YTBrNjJhZjA2OTcymQ	application password	Today, 21:39
ijhhN2Y0M2NmE50DM4YTBrNjJhZjA2OTcymQ	application password	Today, 20:46
NihhhN2Y0M2NmE50DM4YTBrNjJhZjA2OTcymQ	application password	Today, 21:09

The bottom of the window shows a checkbox for 'Allow Cloud Document Sync' which is set to 'False'.

efresh token
S Keychain

DS - Default - Device re
ice restriction



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

Description ⓘ Only numeric #WHfB

ANY ⓘ default

Regex ⓘ ^[0-9]+\$

Minimum Passcode Length ⓘ 7

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, which contains the value '^[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**

The screenshot shows the Microsoft Intune Settings Catalog interface for configuring Microsoft Edge settings on macOS. The main title is "Edit profile - macOS - Default - Edge - Profile and Sync - v3.0 - TF".

The left sidebar shows the navigation path: Configuration settings > Microsoft Edge > Browser sign-in settings.

The right pane displays the "Microsoft Edge" configuration settings:

- A message indicates "258 of 259 settings in this category are not configured".
- A setting titled "Set Microsoft Edge as default browser" is shown with a blue toggle switch labeled "Enabled". This setting is highlighted with a red border.
- Below it, another setting titled "Force users to sign-in to use the browser" is also highlighted with a red border.
- Other visible settings include "Force synchronization of browser data and do not show the sync consent prompt" which is set to "Enabled".

Improve security posture





Disk Encryption look & feel

wpninja.s.au



mac
OS

FileVault

Your organization has turned on FileVault for encrypting the data on your disk and requires you to store the recovery key in Microsoft Intune.

Turn on FileVault

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

This PC

Search This PC

New View Sort View ...

Pictures Music Videos Git

Devices and drives

Windows (C) 487 GB free of 952 GB

BitLocker Drive Encryption

Control Panel Home

BitLocker Drive Encryption

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

i For your security, some settings are managed by your system administrator.

Operating system drive

Windows (C:) BitLocker on

Suspend protection Back up your recovery key Turn off BitLocker



Recovery Key

The screenshot shows the OB-V-US mobile application interface. At the top, there is a navigation bar with tabs for Devices, Apps, and Support. Below the navigation bar, there are two device icons: "Kenny's M..." and "CPC-kbu...". A note 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
Device encryption	If available, the recovery key can be used to unlock this device. Get recovery key

The screenshot shows the OB-V-US website with a dark theme. At the top, there is a header with the logo "OB-V-US" and a navigation menu. Below the header, the breadcrumb navigation shows: Home \ Devices \ Kenny's MacBook Pro \ Get recovery key. The main content area has a heading: "FileVault Recovery Key for Kenny's MacBook Pro". A note below the heading states: "For security reasons, recovery key will be hidden from view after 5 minutes of inactivity". Below this, there is a text field containing the recovery key: "XACZ-X75P-WD6T-KLJB-C9F8-ZNHT". A "Copy" button is located next to the key.

LAPS for Mac





M365 Profile Photo Download and Sync for macOS ... ?

wpnijas.au

The screenshot shows the 'Users & Groups' section of the macOS System Preferences. On the left, a sidebar lists various system settings: General, Appearance, Accessibility, Control Centre, Siri & Spotlight, Privacy & Security, Desktop & Dock, Displays, Wallpaper, Screen Saver, Battery, Lock Screen, Touch ID & Password, Users & Groups (which is selected and highlighted in blue), Passwords, Internet Accounts, and Game Center. The main pane displays three user accounts: 'Admin Account' (Admin), 'Florent NOSARI' (Standard), and 'Guest User' (Off). Below the accounts are buttons for 'Add Group...' and 'Add User...'. Underneath the accounts, there are three configuration options: 'Automatically log in as' (set to Off), 'Allow network users to log in at login window' (with a toggle switch turned on and an 'Options...' button), and 'Network account server' (with an 'Edit...' button). A question mark icon is located in the bottom right corner of the main pane.

ts/macos-m365-picture/

Improve security posture



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

i 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 ..





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 EntralID 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
- 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 ?





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

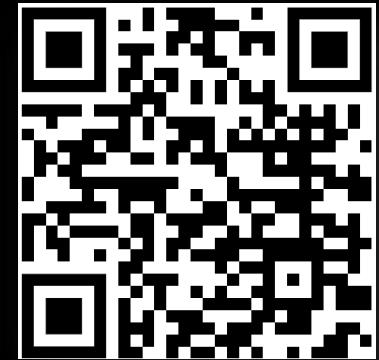
KFM is only supported by the **standalone OneDrive sync app** (e.g. contained in Microsoft 365 Apps package in Intune). The version from **macOS App Store** does not support KFM.

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.

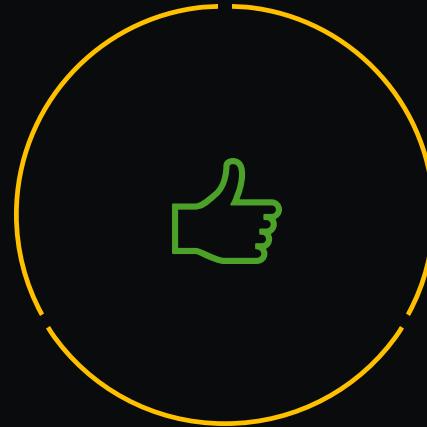


Community tools

GitHub Repo with scripts and information







Thank You



Workplace

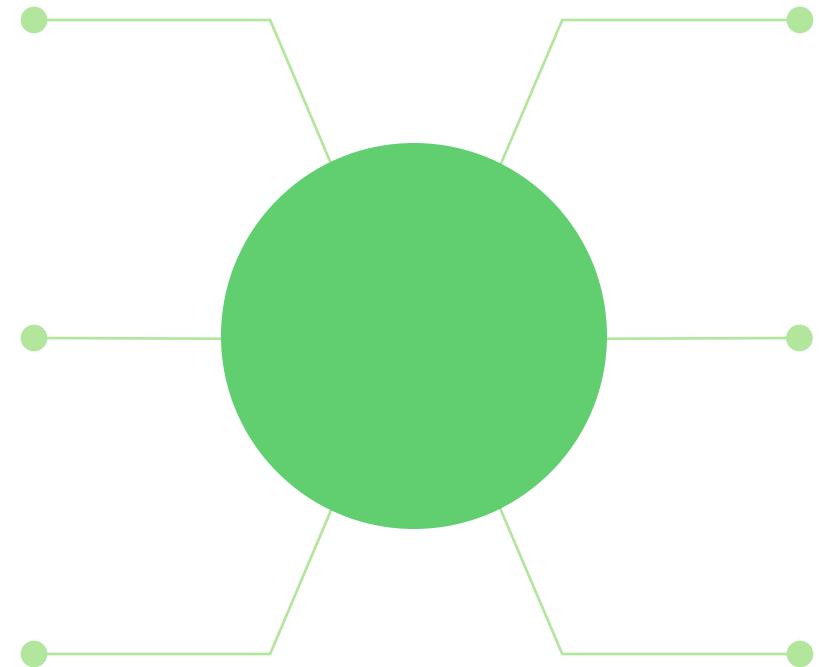


Workplace Ninja Australia Tour





About You

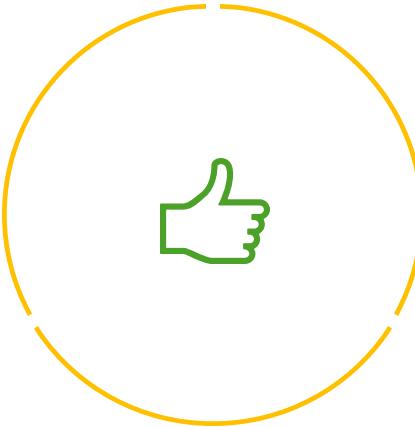












Thank You



Workplace Ninja Australia Tour