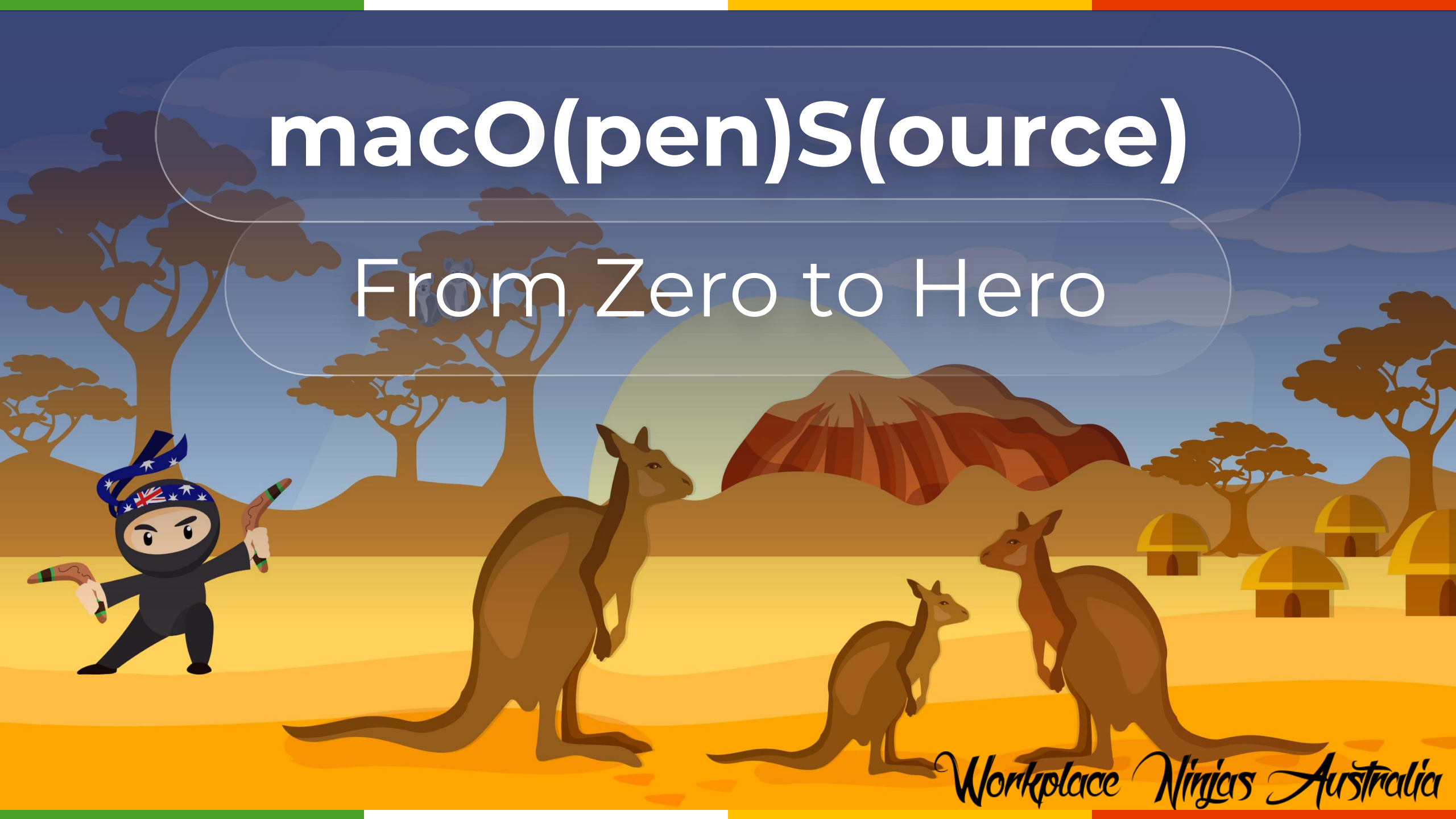
macO(pen)S(ource)

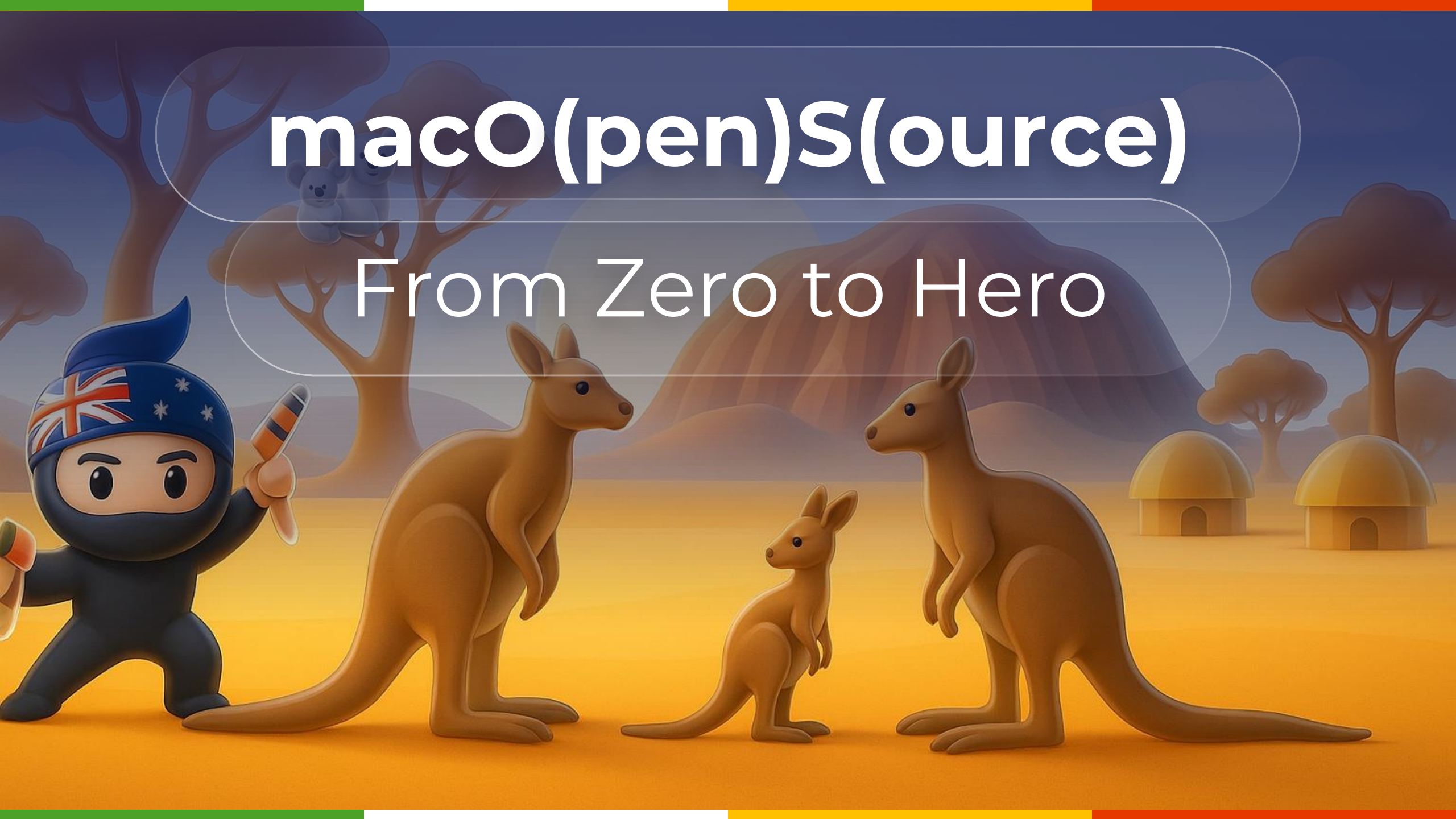
From Zero to Hero



Workplace Ninjas Australia

macO(pen)S(ource)

From Zero to Hero



Thank You Sponsors

glueck kanja

DEVICIE

nerdio

wpninjas.au

About Me

Joel Kino

From

- MSP Owner from Interconnekt
- Small MSP focusing on SMBs

Focus

- Modern Workplace Solutions
- Intune, Entra, Defender & M365

Certifications

- Lawyer
- Audio Engineer

Hobbies

- Music Production
- Drinking Whisky
- Geeking out!

Socials

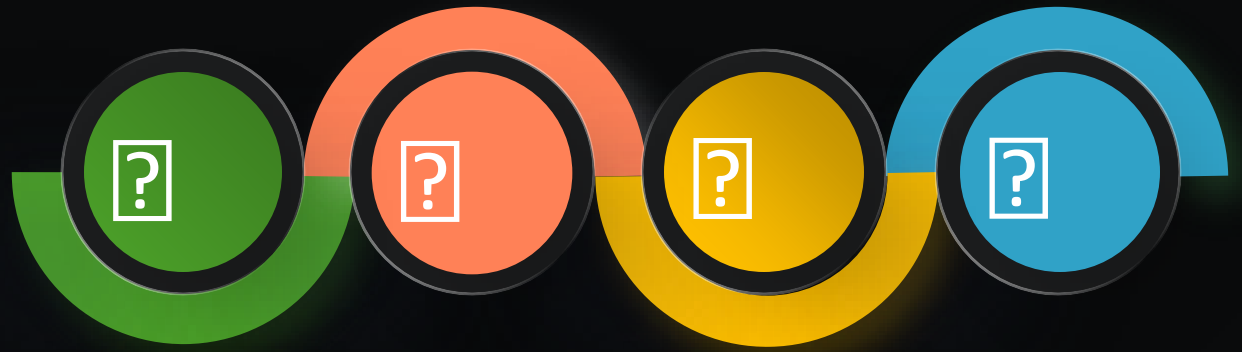
Contact

- joel@interconnekt.com.au
- github.com/joelkino

wpninjas.au

The Agenda

So, what are we trying to achieve today?



Foundation

Look at why Apple Business Manager is essential to managing macOS devices properly.

Configuration

Explore our options for creating, deploying and customizing our configurations.

Zero Touch

Use Open Source tooling to deploy apps, scripts to our devices with a user friendly zero touch provisioning tool.

Security

See how we can deploy and approve IT Tools like MDR and RMM Agents and allow users to Elevate to Admin

wpninjas.au

macOS Management

Then vs Now

wpninjas.au

My Journey to Mac Admin

The Love Begins

- Started using macOS over 20+ years ago as a Music Producer
- Loved the stability, design, and creative tools — Ableton & Logic Pro and the seamless hardware/software integration
- Became a Mac evangelist — everything just worked

Reality Check for the MSP

- Managing Macs in a corporate environment was painful
- Poor integration with Active Directory, Entra ID
- Limited management capabilities compared to Windows
- Felt like Macs were consumer-first, enterprise-last

macOS Management: Then vs Now

Item	Personal Device	Managed Device
Device Type	Personal	Supervised / Intune Managed
Intune Managed	No	Yes
Enrolment Methods	Can Be Onboarded To Intune Via Company Portal	Use DEP Or Apple Configurator To Onboard To ABM
Remote Support Tool	Manual Installation / Requires User Consent Of Permissions (Must Be Admin To Approve)	Manual Installation / Requires User Consent Of Permissions (Can Set Profile To Allow Standard User To Approve)
FileVault Encryption	User Controlled	Intune Settings Catalog
Settings Management	Scripts / RMM	Intune Settings Catalog
Defender Deployment	Manual Deployment Of Defender Via Onboarding Script	Intune, Script Or Installomator
Defender Settings	Manual Implementation Via Terminal Commands	Intune Endpoint Security Profile Or Settings Catalog
3rd Party Security Tools	Manual Deployment	Deploy App And Approve Kernel Extensions Via Intune
Local Admin Rights	First Account Local Admin	User Is Not Local Admin
OS Updates	No Control	Intune DDM Or Update Policy
M365 / Edge Updates	User Enables Auto-update	Set Auto-update Policy
App Deployment / Updates	No Control	Limited
LAPS	No	Yes
Platform SSO	No	Yes
Universal Print	Manual Install	Yes

A New Era for macOS Management

Over the past two years, macOS support in Intune has accelerated:

- Identity is simpler with **Platform SSO** and **federated authentication**.
- Updates go declarative **(DDM)**, giving admins more control and reliability.
- Admin overhead drops as the **Settings Catalog** evolves in **sync** with **Apple's YAML** definitions.
- Together, **Apple and Microsoft are meeting in the middle** — enabling modern, secure, and scalable macOS management.
- **Open-source fill the gaps** that Intune doesn't cover yet
- **macOS is finally enterprise-ready and MSP Friendly**

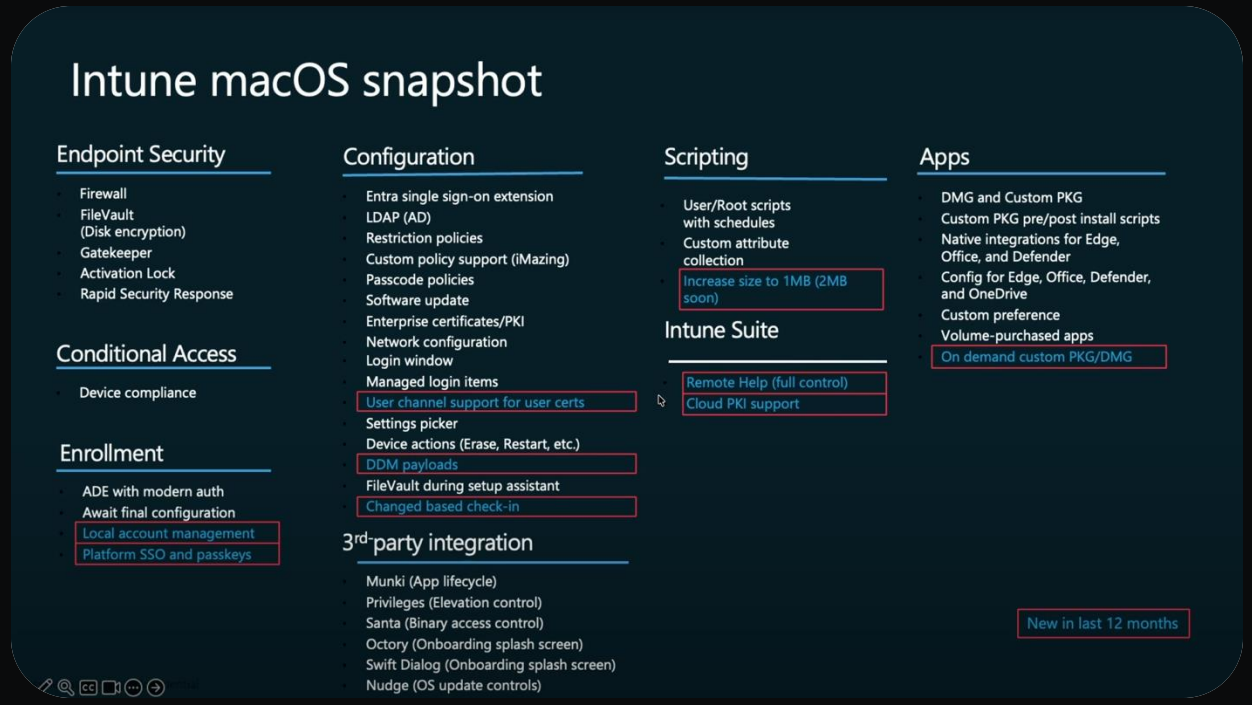
The *Glass* is (more than) Half Full

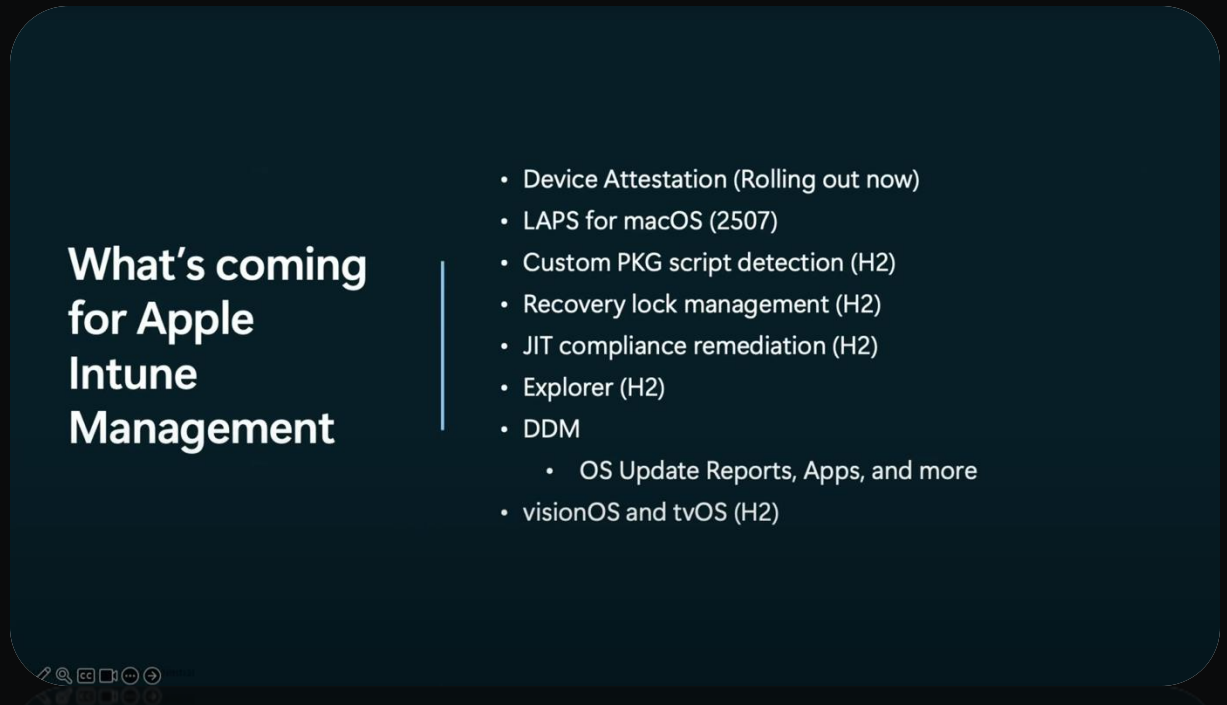
macOS Management Is Evolving & Intune is Growing Up

Feature	What It Enables	Why It Matters
Platform SSO	**Passwordless** login, password sync, smart card support, Kerberos SSO	Aligns macOS with cloud identity; fewer prompts, better CA posture
macOS LAPS*	**Randomized local admin password via ADE**; auto-rotate; fetch/rotate in Intune	Enhances device security and local admin control; caveat: first user gets secure token. ** Can only be done during ADE*
Declarative Device Management	Version-specific updates with deadlines; full update flow	Preferred over legacy MDM update policies for macOS 14+
Settings Catalog + Apple YAML	Tracks Apple's GitHub YAML; faster access to new payloads	Reduces reliance on brittle custom profiles; older templates deprecating
Universal Print on macOS	App deploy via ABM/MDM; user sign-in; add printers	Native support from macOS 14.6.1+

Intune macOS Feature Snapshot

Microsoft have been investing heavily in Intune's macOS Capabilities and continue to do so





[Managing macOS with Intune and Lessons Learned – Chris Kunze]

wpninjas.au

Laying the Foundation

wpninjas.au

Apple Business Manager

What is it?

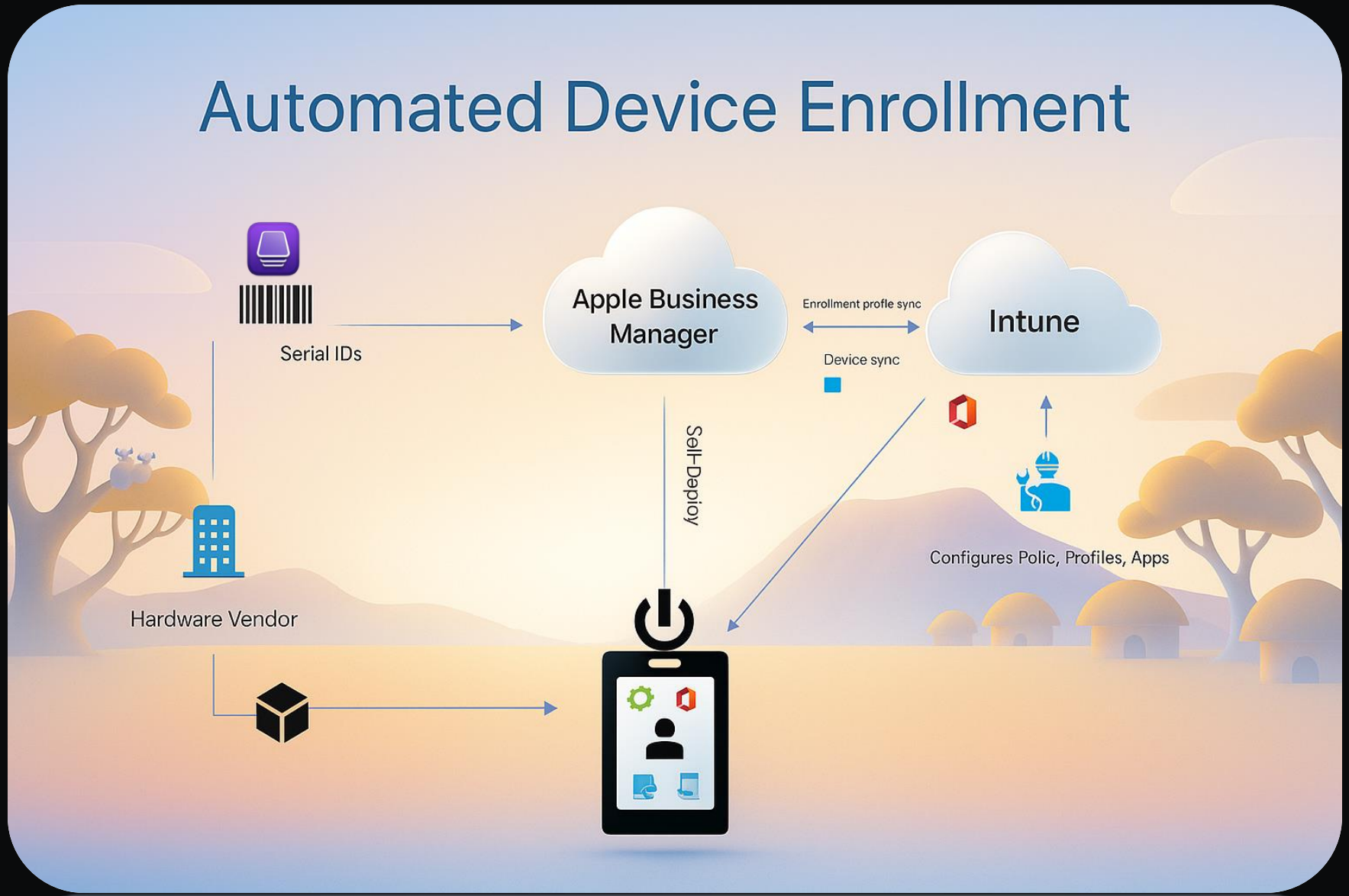
- Apple Business Manager (ABM) is a free service from Apple.
- Built to help organisations manage Apple devices, apps, and Apple IDs at scale.
- A must-have for any organisation deploying Apple hardware.

What does it do?

- Provides a centralised portal for:
  - Device deployment and assignment
  - Managing organisation-owned Apple IDs (can also federate with Entra ID)
  - Bulk app and content purchasing via Volume Purchase Program (VPP)
- Seamlessly integrates with MDM solutions for automated enrollment.

⚠️ **Note:** ABM is not an MDM itself — it works alongside your MDM (e.g., Intune) to enable full lifecycle management.

The Building Blocks for a Solid Architecture



Supervised vs Personal Devices

With Apple Business Manager

IT has more control when Apple devices are supervised.

- Configure accounts
- Configure global proxies
- Install, configure, and remove apps
- Require a complex passcode
- Enforce all restrictions
- Access inventory of all apps
- Remotely erase the entire device
- Manage software updates
- Remove system apps
- Modify the wallpaper
- Lock into a single app
- Bypass Activation Lock
- Force Wi-Fi on
- Place device in Lost Mode

Steps for Enrollment:

- Requires device is sync'd from ABM/ASM
- Assign Enrollment Profile
- Can choose with or without User Affinity
- Await Final Config
- Set Skip Keys
- Account creation

Without Apple Business Manager

MDM functions are limited on personal devices.

- Configure accounts
- Configure Per App VPN
- Install and configure apps
- Require a passcode
- Enforce certain restrictions
- Access inventory of work apps
- Remove work data only
- Access personal information
- Access inventory of personal apps
- Remove any personal data
- Collect any logs on the device
- Take over personal apps
- Require a complex passcode
- Remotely wipe the entire device
- Access device location

Steps for Enrollment:

- Go to https://aka.ms/EnrollMyMac to download and install Company Portal
- Launch Company Portal to enroll device

⚠ **Note:** Some configurations can only be applied for supervised devices, only devices from Apple Business Manager are supervised devices

Getting Started with Apple Business Manager

📒 **Note:** Everything you need is in this guide: Brilliantly Manage MacOS with Intune & Apple Business Manager

Tip and Tricks when Applying for an ABM Account:

✅ **Free service** from Apple for managing devices, apps, and Apple IDs

📝 **Requirements:**

- **DUNS Number** (available via credit reporting services: illion Express
- **Senior representative contact** for verification (needs to be an actual person, don't list generic email and phone numbers)

⏳ **Approval Timeline:**

- May take a few days — plan for this in your project schedule

ABM Admin Account Recommendations

⚠️ Why You Need At Least Two Admin Accounts ⚠️

✅ **Redundancy**: Ensures access if one account is locked out or unavailable.

🔐 **Security**: Helps maintain control during password resets or MFA issues.

🛠️ **Operational Continuity**: Critical for troubleshooting and maintaining federation.

Primary Admin with a non-federated domain

Alias for itsupport@customername.com distributes to MSP Helpdesk email. Uses fallback domain for DNS/federation issues.

Break Glass Admin using appleaccount.com

Secondary Admin. Uses Apple Account domain.

Name	Username	Email
IT ABM Admin	apple.abm@customername.onmicrosoft.com	apple.abm@customername.onmicrosoft.com
ABM BG Admin	apple.abm@customername.appleaccount.com	itsupport@customername.com

Other Security Considerations

- Store credentials securely (e.g., in a password manager) and note that ABM currently only supports MFA via phone (no TOTP, no Passkey)
- Multi-factor Authentication is via phone and is set up and confirmed by following: Two-factor authentication for Apple Account – Apple Support (AU)
- On the web: Go to account.apple.com and sign in to your Apple Account. Answer your security questions, then tap Continue. Tap Continue when you see a prompt to upgrade account security. Then tap Upgrade Account Security and follow the onscreen instructions.

Managed Apple Accounts

Why Verify & Lock Your Domain

- Prevents unauthorised Apple ID creation using your domain.
- Ensures all accounts are corporate-owned.
- Enables federated authentication (e.g., Microsoft 365).
- Simplifies integration with MDM and identity providers.
- Supports domain capture to convert existing Apple IDs to Managed Apple Accounts.

Why Verify & Lock Your Domain

- Enhanced security and control over Apple IDs.
- Streamlined device and account management.

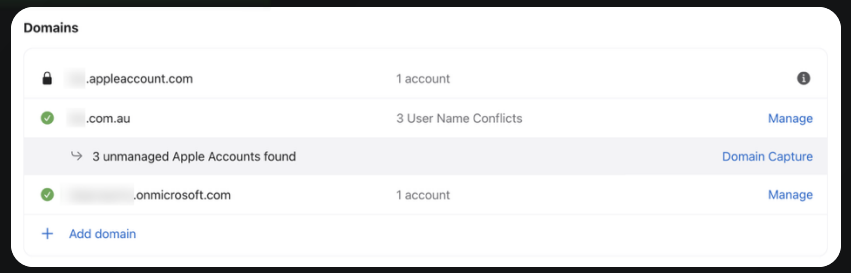
Managed Apple Accounts

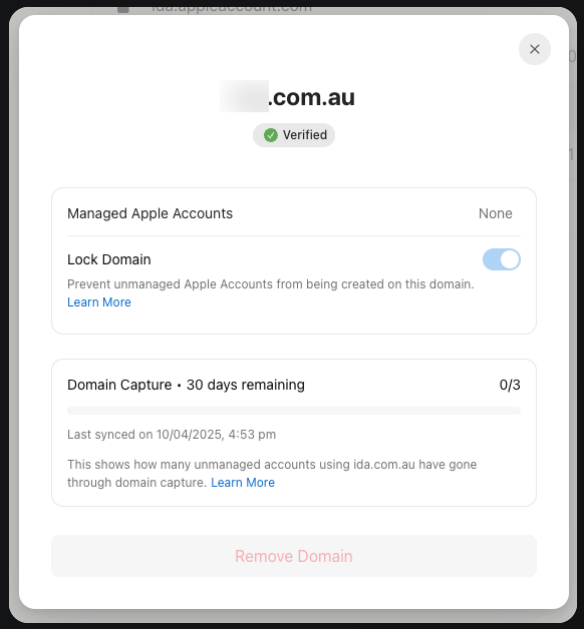
Capture A Domain

[Capture a domain in Apple Business Manager]

Once the domain is verified you will be notified if any unmanaged Apple Accounts were found:

- Liaise with users that they may receive a notification from Apple and to not take any action
- Assist users to migrate Apple ID to a personal account with a non-managed Domain.
- You can use your email security / exchange logs to search for who has received emails
- Use: [If you are asked to transfer your Apple Account or keep it as a personal account]

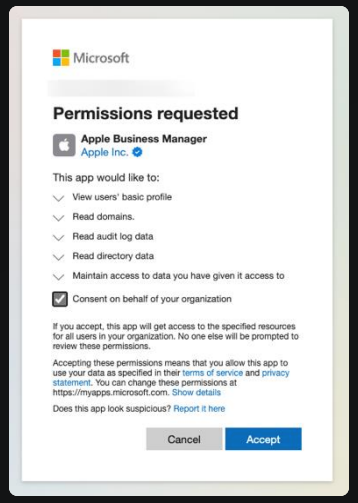




⚠ **Note:** If users do not take action within 30 days they may lose access to their account tied to that email address

The One Account to Rule Them All

Federate with Entra ID

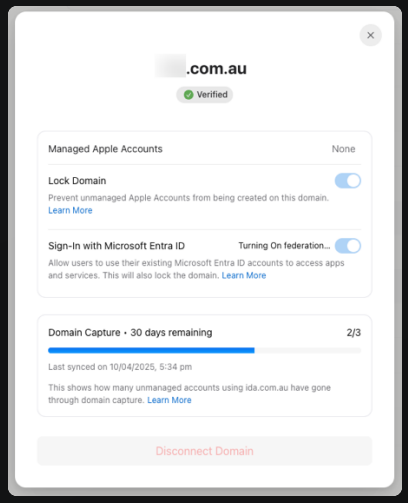


Allows **single sign-on (SSO)** for Apple services using **Microsoft Entra ID** instead of creating separate Apple IDs.

Benefits:

Sync users automatically:

- Accounts created in ABM from Entra ID.
- Managed Apple IDs match corporate email addresses.



[Intro to federated authentication with Apple Business Manager – Apple Support (AU)]

[Sync user accounts from Microsoft Entra ID to Apple Business Manager – Apple Support (AU)]

Integrating ABM with Intune

- Apple Business Manager (ABM) integrates with Microsoft Intune to streamline Apple device management.
- Enables automated enrolment (ADE), app distribution, and identity management for Apple devices.
- There are a few different integration points that must be set up and maintained.

Component	Purpose	Renewal	Notes
Apple MDM Push Certificate	Establishes trust between Apple and Intune for device management	Annually	Required for Intune to manage Apple devices
ADE Enrollment Token	Enables zero-touch deployment of Apple devices via ABM	Annually	Links ABM with Intune; required for ADE
VPP Token	Allows bulk purchase and assignment of apps without Apple ID	Annually	Enables app distribution to devices or users
Default MDM Assignment	Automatically assigns Intune as the MDM for newly added devices in ABM	Not applicable	Ensures enrollment and policy application

If the MDM Push Certificate expires, Intune loses the ability to communicate with Apple devices and you will need to wipe and re-enrol them for continued management

Hey Boo, it's Intune – I Got Chu

Intune has seriously levelled up its macOS game in the last few years...

💻 **Identity? Sorted.**

With Apple Business Manager, Entra ID, and Platform SSO, your Macs know who's boss.

⚙️ **Configuration? Getting There.**

Settings Catalog is catching up fast — just a few gaps, but we've got workarounds.

But Gaps Still Exist

🛡️ **Security? Locked Down.**

Defender, Conditional Access, and SmartScreen keep your endpoints squeaky clean.

🔐 **Local Admin? Who's That?**

macOS LAPS (for new builds) means no more shared admin passwords floating around.

wpninjas.au

Open Source

Secret Sauce for macOS Mastery

The Good, The Gaps and The Workarounds

The Power of Community

- The MacAdmins community has been solving macOS management challenges long before Intune was even in the game.
- From custom scripts to Open Source tools, MacAdmins have built solutions to fill gaps Apple and MDM vendors hadn't yet addressed.
- This community is active, collaborative, and incredibly resourceful, shares tools, workflows, and knowledge across Slack, GitHub, and conferences.

Why It Matters

- Many of the tools we rely on today, like iMazing Profile Editor, SAP Privileges were born out of real-world needs.
- MacAdmins have consistently pushed the boundaries of what's possible with macOS management.
- Their work ensures that even when commercial tools fall short, there's a workaround, a script, or a community-built solution ready to go.

Mind the Gap: Open Source to the Rescue

So, let's take a look at the gaps and how we can solve them with Open Source or Free Tools and Community Knowledge

Gap	Open-Source Solution
No Intune Baselines	OpenIntuneBaseline, CIPP
No Autopilot-like onboarding wizard	Create an Onboarding Wizard using Baseline
Limited app catalog, 3rd party app patching	Deploy apps using Installomator and scripts, used App Auto-Patch or IntuneBrew
PPPC & Configuration Profile creation	iMazing Profile Editor
Dock & UX customization	Custom scripts / configuration profiles
No Endpoint Privilege Management (EPM)	SAP Privileges2
Certificate Alerting for Intune/ABM	CIPP

📒 **Note:** There are many options, both free, open source and paid that can solve these gaps for you. These are just the ones I have chosen.

wpninjas.au

Intune Configuration

OpenIntuneBaseline

What gap does it plug?

- Community-driven security baseline for Intune
- Provides ready-to-deploy configuration templates for Windows and macOS.
- Aligns with industry frameworks like CIS, NCSC, and Microsoft best practices.
- Focused on security AND user experience—avoids breaking workflows.
- Continuously updated and tested in real-world environments, not just labs.
- Will save you 100's of hours of configuration time!

Which Legend made this?

- **James Robinson,Microsoft MVP** for Intune & Windows, from the UK and works at Threatscape
- Over **20 years in IT**, last 8 focused on Intune and modern management.
- Contributor to **CIS Benchmarks** and frequent speaker at **MMS** and **Workplace Ninja Summit**.
- Passionate about **sharing knowledge** and building community-driven solutions.

📒 **Note:** You can also deploy the OpenIntuneBaseline using the new OIB Deployer

CIPP - CyberDrain Improved Partner Portal

What gap does it plug?

Open-source platform for M365 multi-tenant built to solve common paint points:

- Multi-tenant chaos across Microsoft portals.
- Manage GDAP at scale
- Automated Offboarding Wizard.
- Manage Microsoft 365 Configuration using
- Has GitHub Integration with OpenIntuneBaseline

Which Legend made this?

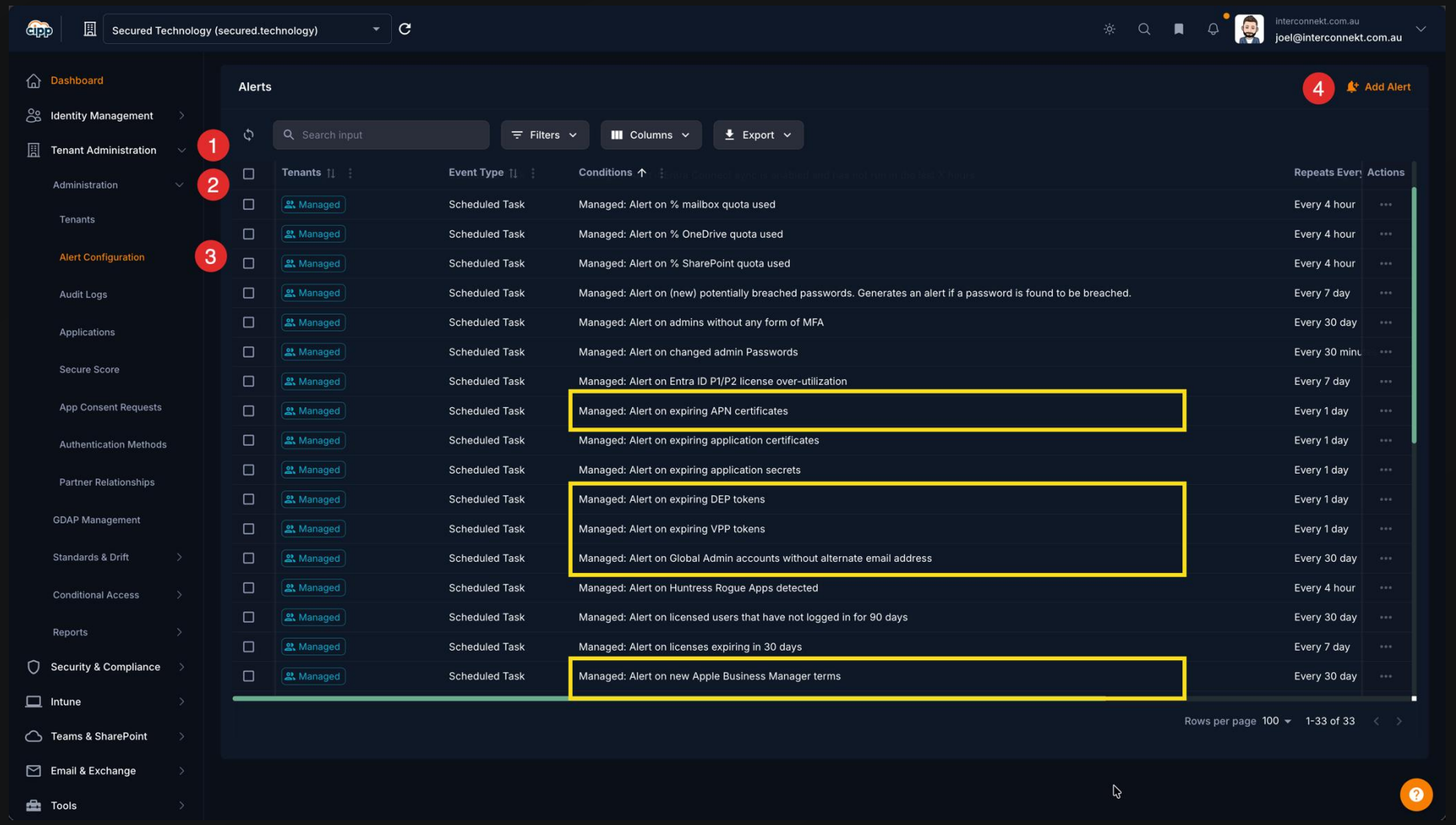
- Kelvin Tegelaar, Microsoft MVP in **Azure & M365 from the Netherlands**
- CTO at **Lime Networks B.V.** Founder of **CyberDrain.com and c**reator of **CIPP**
- 🪛 Super active in the community
- 🤝 Collaborates with many MSP Vendors

📒 **Other Options:**

- You can also deploy the OpenIntuneBaseline using the new OIB Deployer
- You could import the JSON Files from OIB Manually into Intune
- There are other Open Source options, such as the brand new TenuVault from **Uğur Koç** (from today's sponse Gluekkanja)
- Or paid options such as Devicie, Nerdio (both event sponsors) or infocer (which is what we also use at Interconnekt)

CIPP - CyberDrain Improved Partner Portal

What does it look like?



iMazing Profile Editor (v2): Build rock-solid Apple profiles—fast

What gap does it plug?

- A free profile authoring tool to create, edit, and sign Apple .mobileconfig profiles export to .plist.
- Sign and validate the profile for secure deployment.
- Export as .mobileconfig and push through your MDM or export to .plist.
- We will be revisiting this one a bit later as we use it to configure a few other things

Which Legend made this?

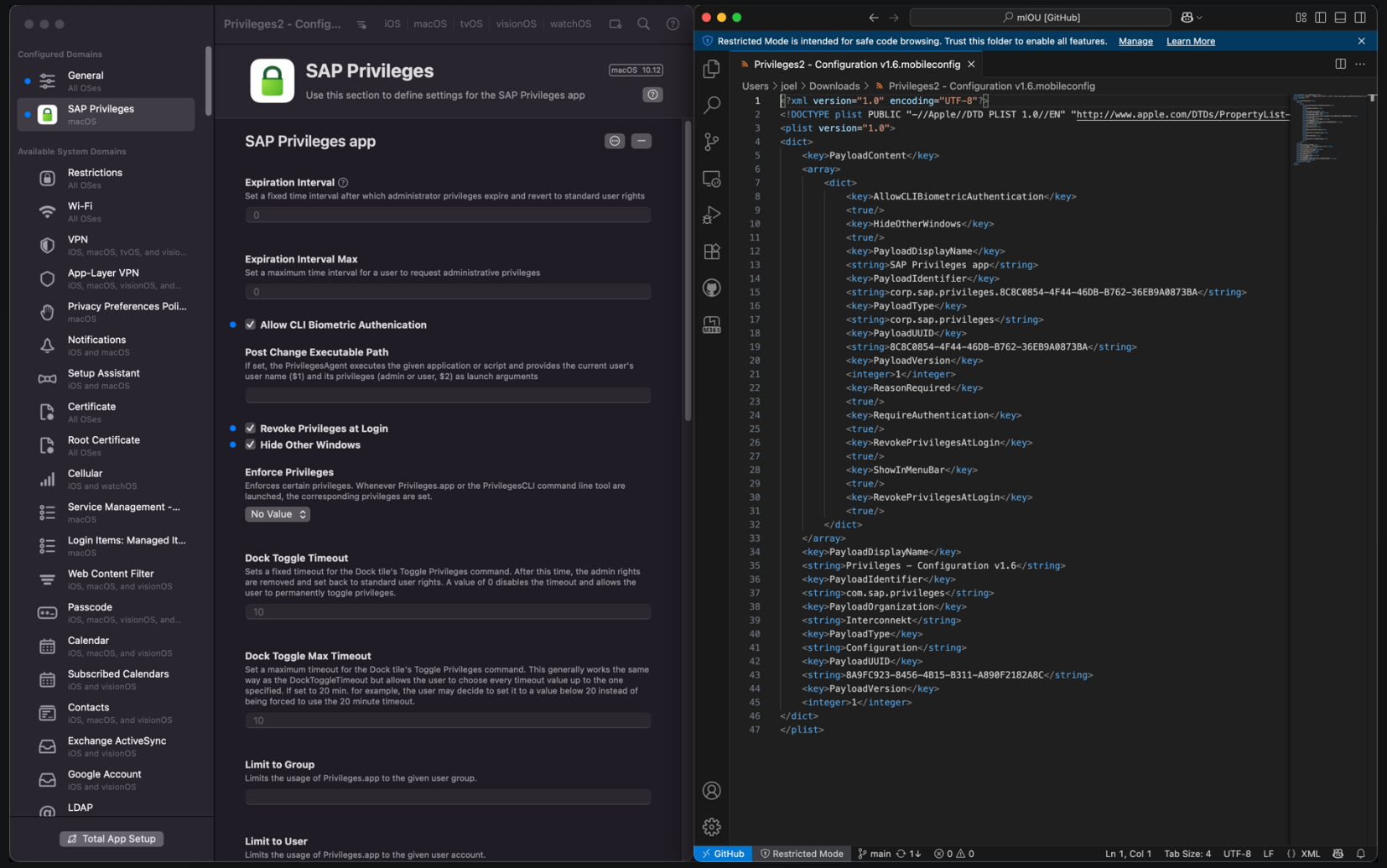
- So this one isn't Open Source and it isn't a community tool
- It was created by the fine folks at DigiDNA, who make iMazing and a whole lot of other tools.
- They are based in Geneva, Switzerland and have been making tools for Apple's platforms for decades.

Other Options:

- You can edit .mobileconfig and .plist files manually in a Code Editor like Visual Studio Code

iMazing Profile Editor (v2): Build rock-solid Apple profiles—fast

What does it look like?



wpninjas.au

Zero Touch Provisioning

Apple Configurator

What gap does it plug?

- Allows to scanning of new Apple Devices into Apple Business Manager from an iOS App for those who are not Apple Registered Resellers
- This ensures the device exists in ABM so it can be synced to Intune and go through the ADE enrolment flow

Which Legend made this?

- Apple made it. But it's free!
- Oh, but you need an iPhone to use it

Note: If you are an Authorised Apple Reseller you can also add devices to ABM using the Device Enrolment Program

swiftDialog: Modern macOS Dialog Utility

What gap does it plug?

- **Admin utility** for macOS 12+ written in **SwiftUI**.
- Displays **custom dialogs** for user notifications, onboarding, or input collection.
- Customizable appearance: colours, icons, banners, markdown, images, videos, and interactive elements (buttons, text fields, dropdowns).
- Supports timeouts, conditional logic, and real-time updates.
- It has spawned many other tools in the MacAdmins ecosystem, making it a foundation for modern workflows.

Which Legend made this?

- **Bart Reardon, Mac Admin & Developer**, active in the MacAdmins community and an Aussie! who works for the CSIRO in Canberra.
- Built swiftDialog to replace legacy tools like jamfHelper, DEPNotify with a **modern, flexible UI**.
- Maintains the project with contributions from the community.
- Active support via **#swiftdialog** channel on MacAdmins Slack.

Installomator: The One Installer Script to Rule Them All

What gap does it plug?

- Automates **installation and updating** of apps by downloading the latest versions directly from vendor sources.
- Supports **over 1000 application labels**
- Ideal for **“latest version” deployments** with minimal packaging overhead.
- Uses **labels** to identify apps.
- Verifies app authenticity via **Team ID** and notarization.
- Debug modes for safe testing.
- Active community on **MacAdmins Slack**.

Which Legend made this?

- **Armin Briegel, Mac Admin, Consultant, Author** of Scripting OS X – #! is not a curse word blog and https://macadmins.news/
- Founded Installomator to simplify **rapid deployment** of latest apps.
- Maintains project with a team including Erik Stam, Isaac Ordonez, Søren Theilgaard, Adam Codega, Trevor Sysock, Bart Reardon.

Note: Supports installation and updating of almost 1000 unique application which you can see here: Installomator/Labels.txt

Baseline

What gap does it plug?

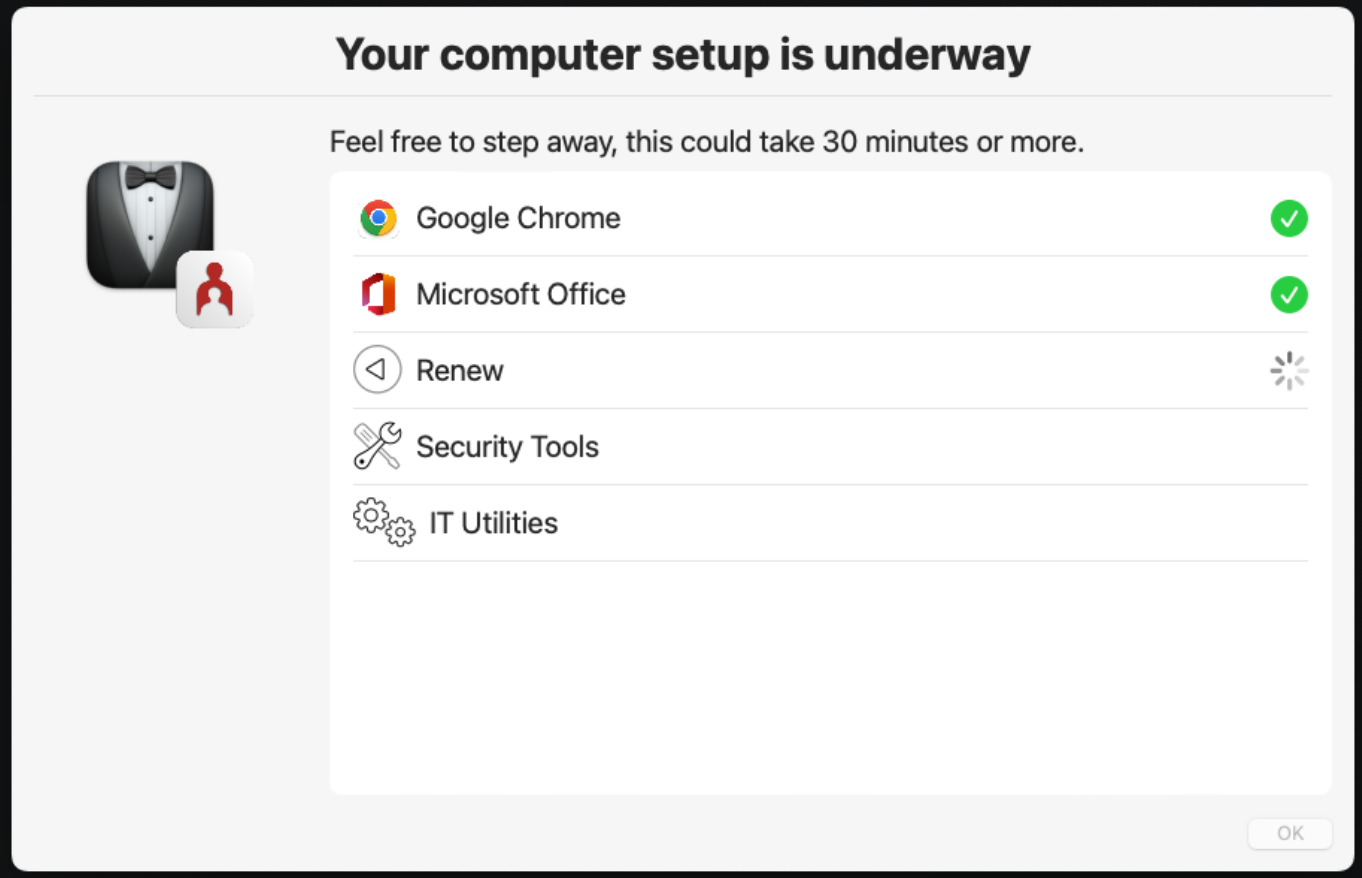
- **Open-source solution** for zero-touch or light-touch macOS deployment.
- Leverages **swiftDialog** for user-facing UI and **Installomator** for app installs.
- Driven by a **configuration file** (plist or mobileconfig) defining: **Packages**, **Scripts**, and **Installomator labels**.

Which Legend made this?

- **Trevor Sysock** – Director of MDM & Cloud Solutions, Second Son Consulting.
- Contributions from Bart Reardon (swiftDialog), Armin Briegel (Installomator), Søren Theilgaard, Adam Codega, and others.
- Active support via **#baseline** channel on MacAdmins Slack.

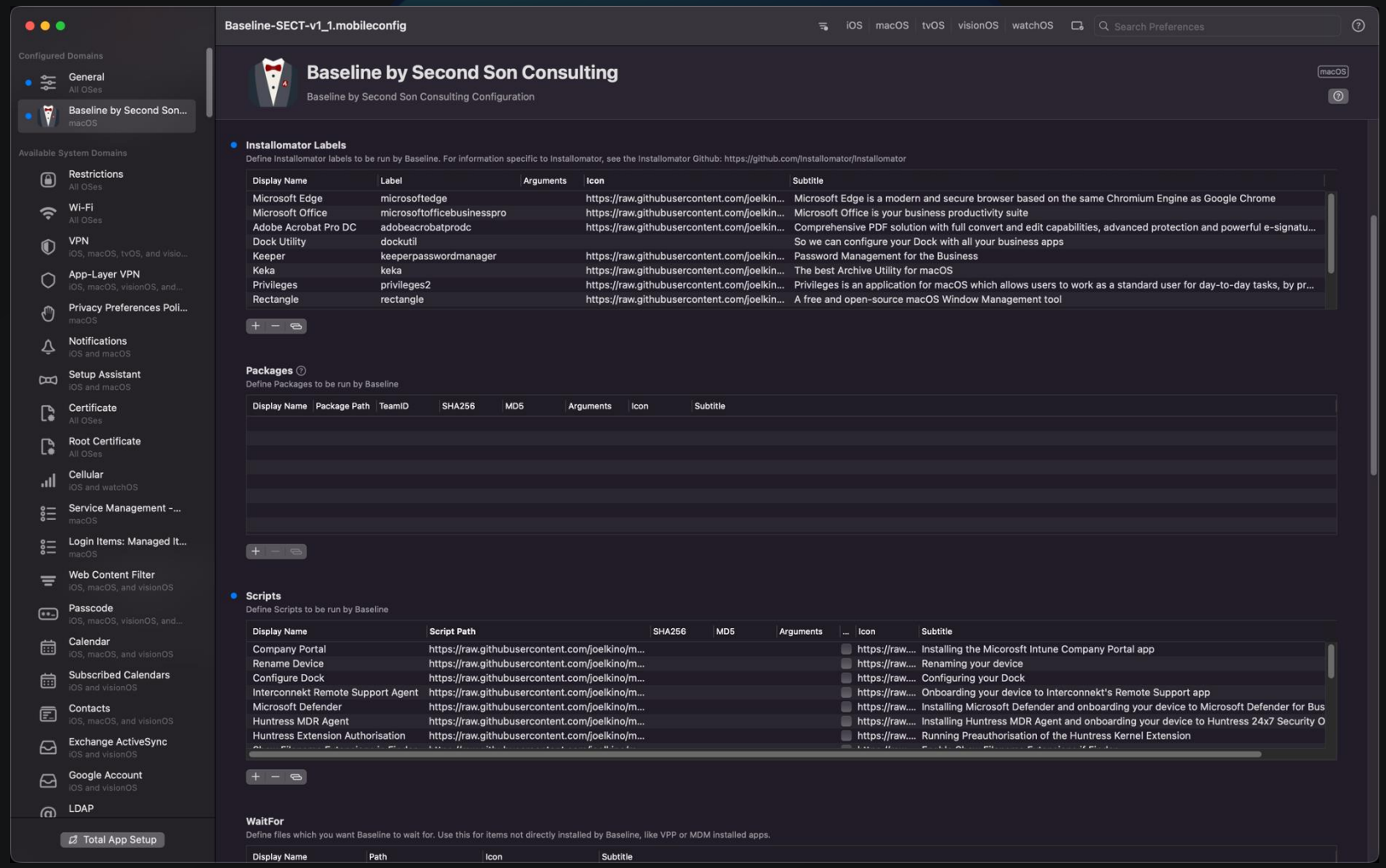
Baseline

What does it look like?



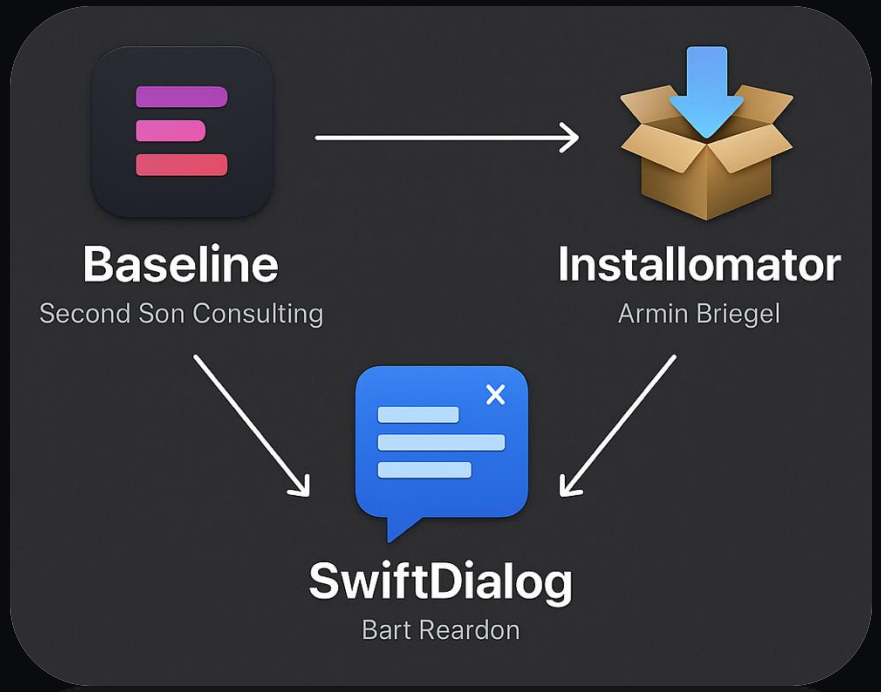
Baseline

What does it look like?



mIOU: macOS Intune Onboarding Utility

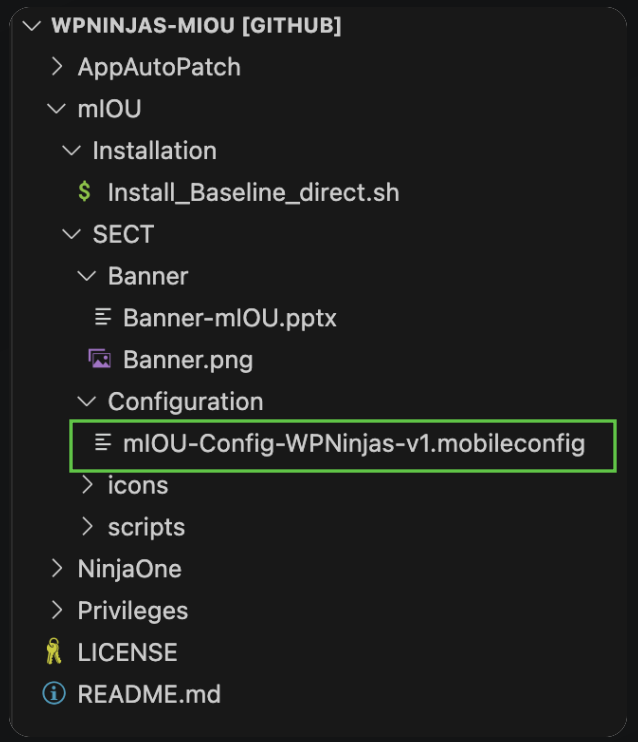
1. Create a .mobileconfig file using iMazing Profile editor and deploy it to your devices in Intune
2. Use the Bootstrap Bash Script so that new devices download and run Baseline with your desired configuration
3. Use script to Customize what apps are in the Dock

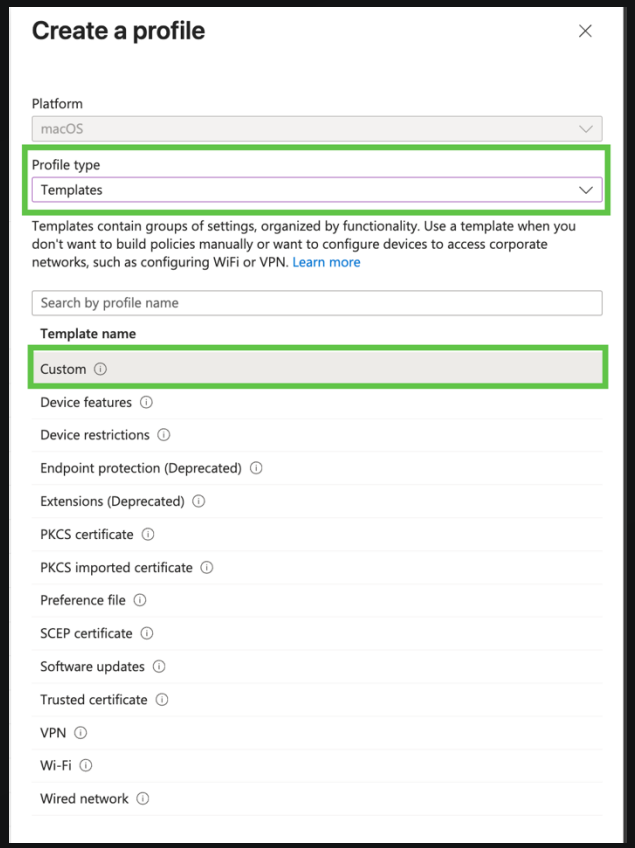


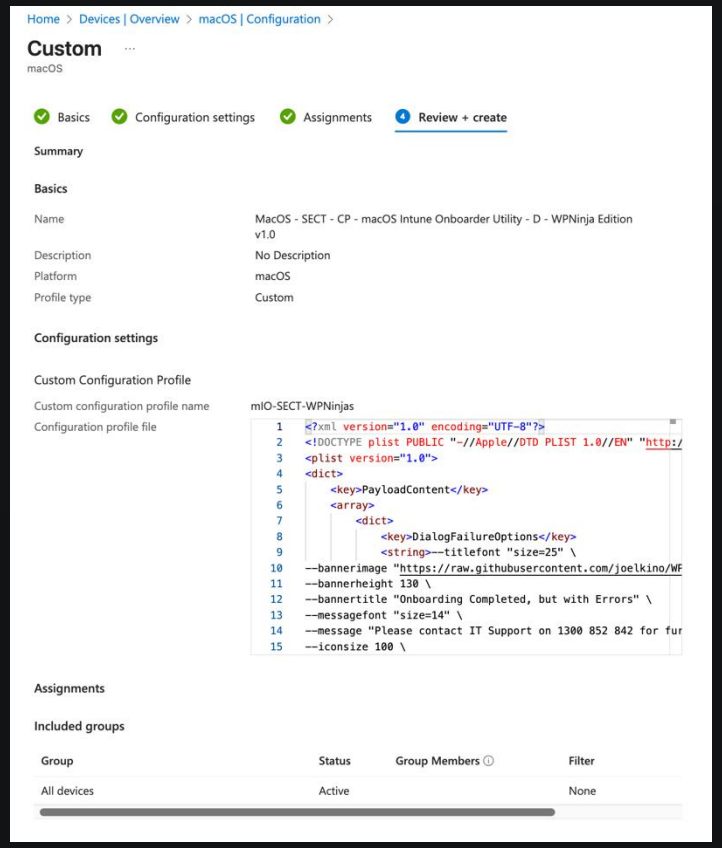
Note: You can test locally without having to reset the device, check the Baseline Wiki / Documentation for further info

mIOU: macOS Intune Onboarding Utility

- Upload your config to Intune as a Custom Template to the Device Chanel and assign to all devices



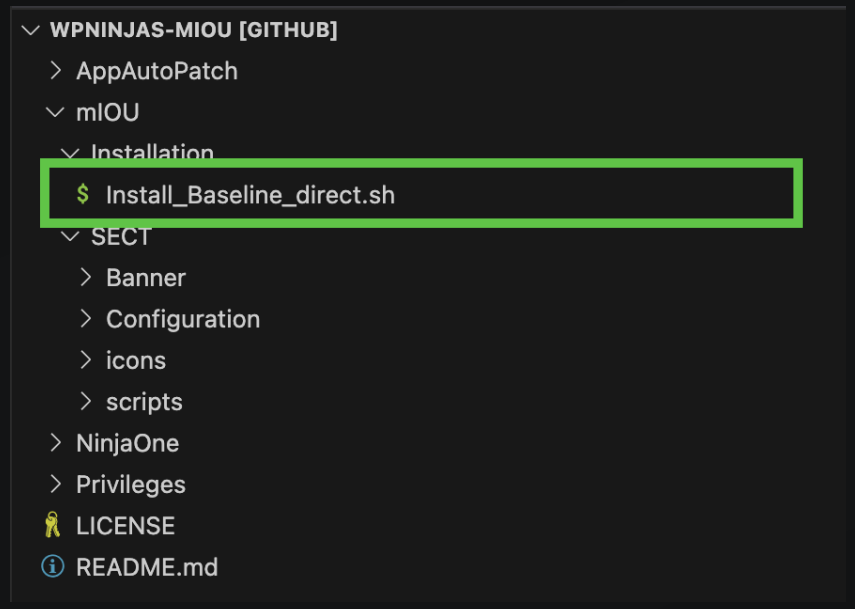


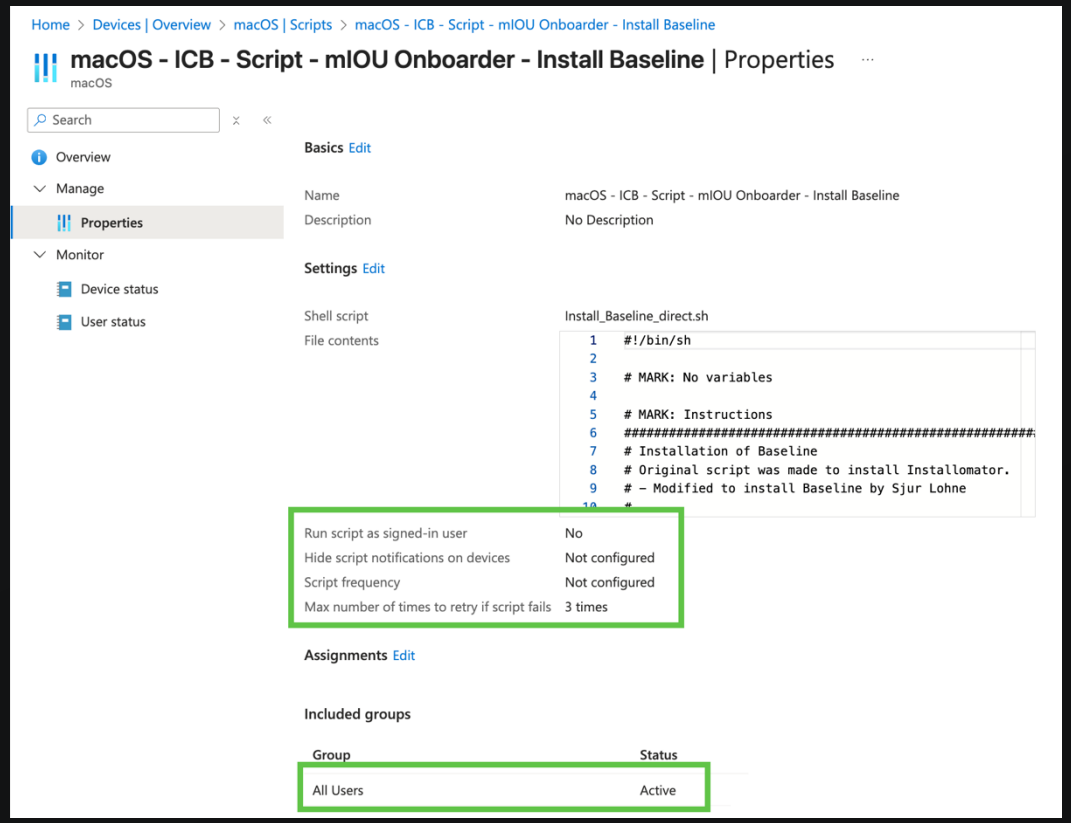


📒 **Note:** You can download these files from joelkino/WPNinjas-mIOU

mIOU: macOS Intune Onboarding Utility

- Upload the Install Baseline Script and Assign to All Users – ensure you use the same settings as here

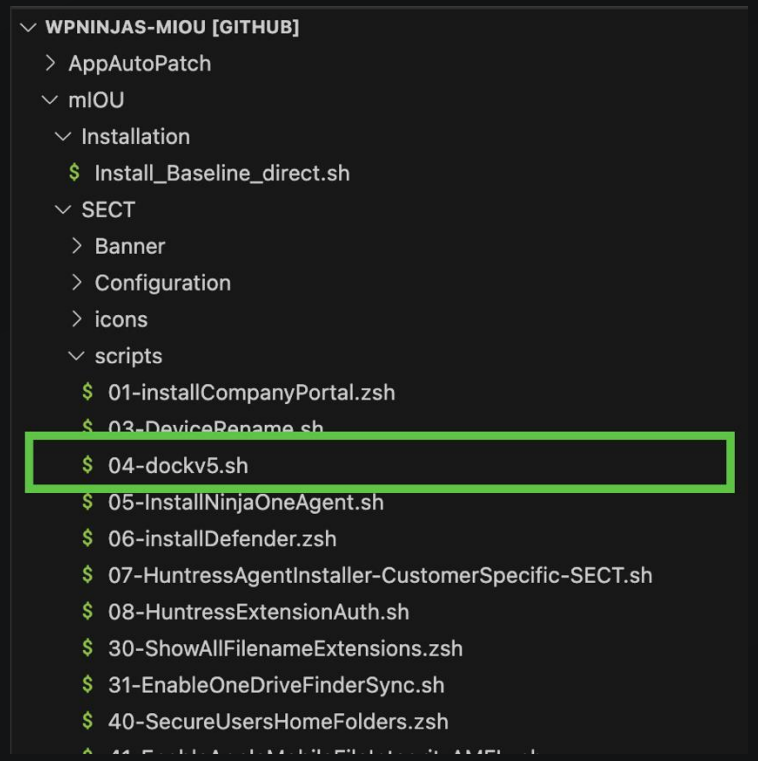


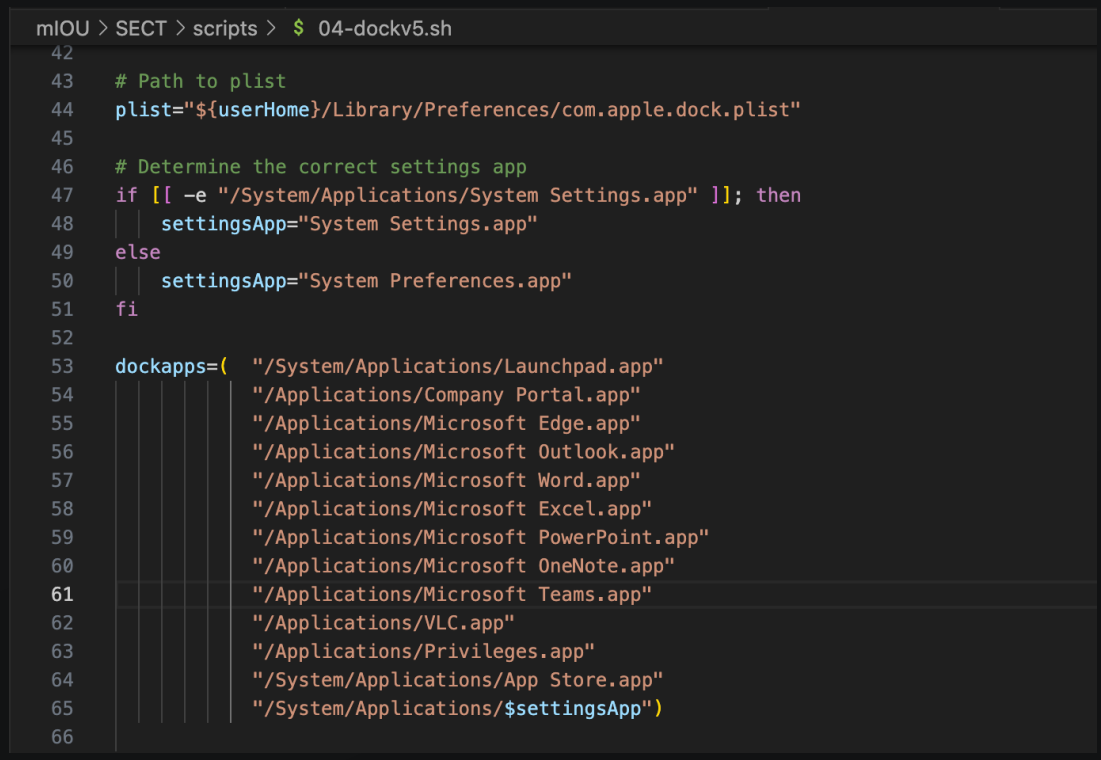


📒 **Note:** You can download these files from joelkino/WPNinjas-mIOU

mIOU: macOS Intune Onboarding Utility

- In the scripts folder, customize what Applications appear in the Dock using Visual Studio Code

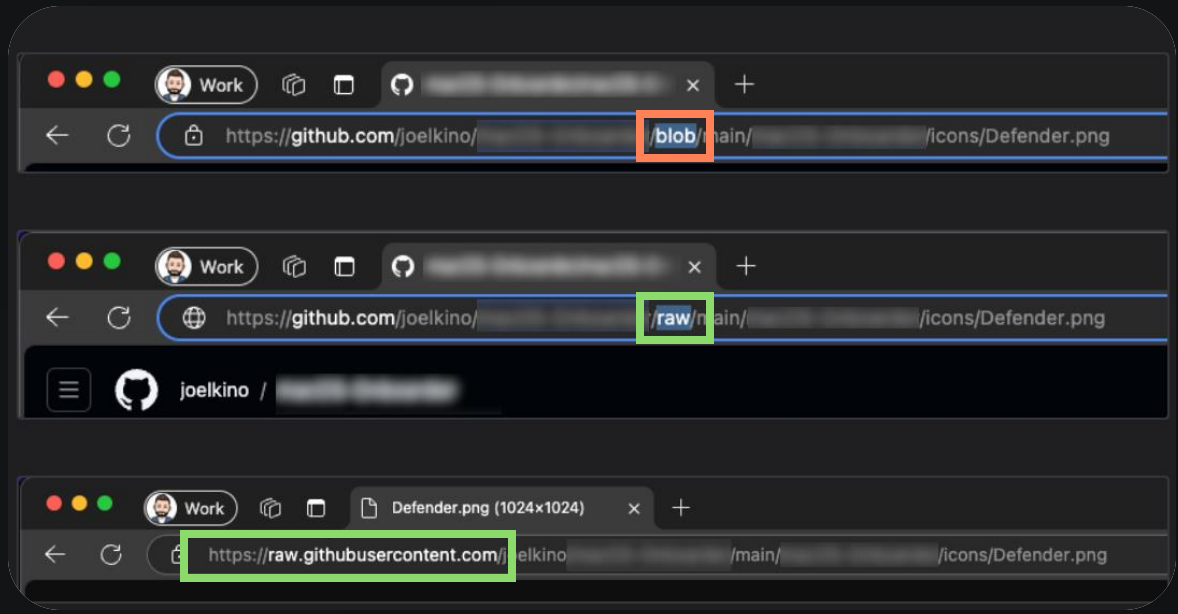




📒 **Note:** You can download these files from [joelkino/WPNinjas-mIOU]

Important Announcement about GitHub Links

- The repository ***must*** be **Public,** otherwise any links used will not be accessible
- You need to use the GitHub **RAW** link rather than the **Blob** links in your config
- To do this you can navigate to the resource in GitHub and the change the URL where is says blob change this to raw, then hit **Enter**
- You will be presented with a URL that starts with https://raw.githubusercontent.com –use these links and then it will work



⚠ **Note:**

- Just copying the link from your Browser's Address Bar will not work!
- Anything hosted in the GitHub will be publicly visible, so take care with what you include here!!

wpninjas.au

Security and Support

App Auto-Patch

What gap does it plug?

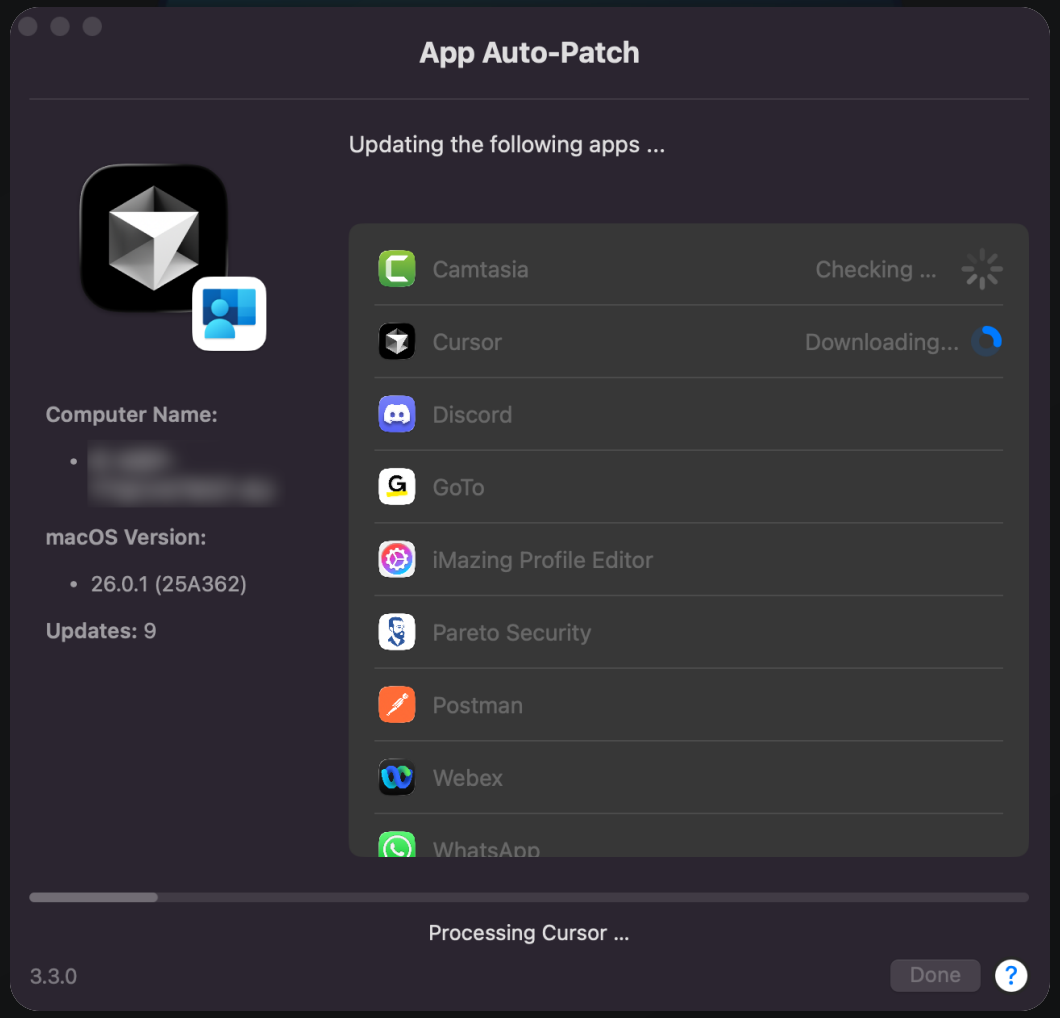
- **Open-source macOS patch management tool**.
- Automates **third-party app updates** using:
  - **Installomator** for app installs.
  - **swiftDialog** for user-friendly prompts.
- Originally inspired by **Patchomator**, now a standalone project.
- Keeps all your apps up to date
- You can exclude certain apps using a .mobileconfig Configuration Profule

Which Legend made this?

- **Rob Schroeder,** Mac Admin & Automation Advocate who built App Auto-Patch to simplify patching for macOS.
- **Community-first approach**:
  - Maintains project on GitHub under App-Auto-Patch org.
  - Active support via MacAdmins Slack (#app-auto-patch).
- **Tagline:** *"By MacAdmins, for MacAdmins—because patching shouldn't be painful."*

App Auto-Patch

What does it look like?



Privileges

What gap does it plug?

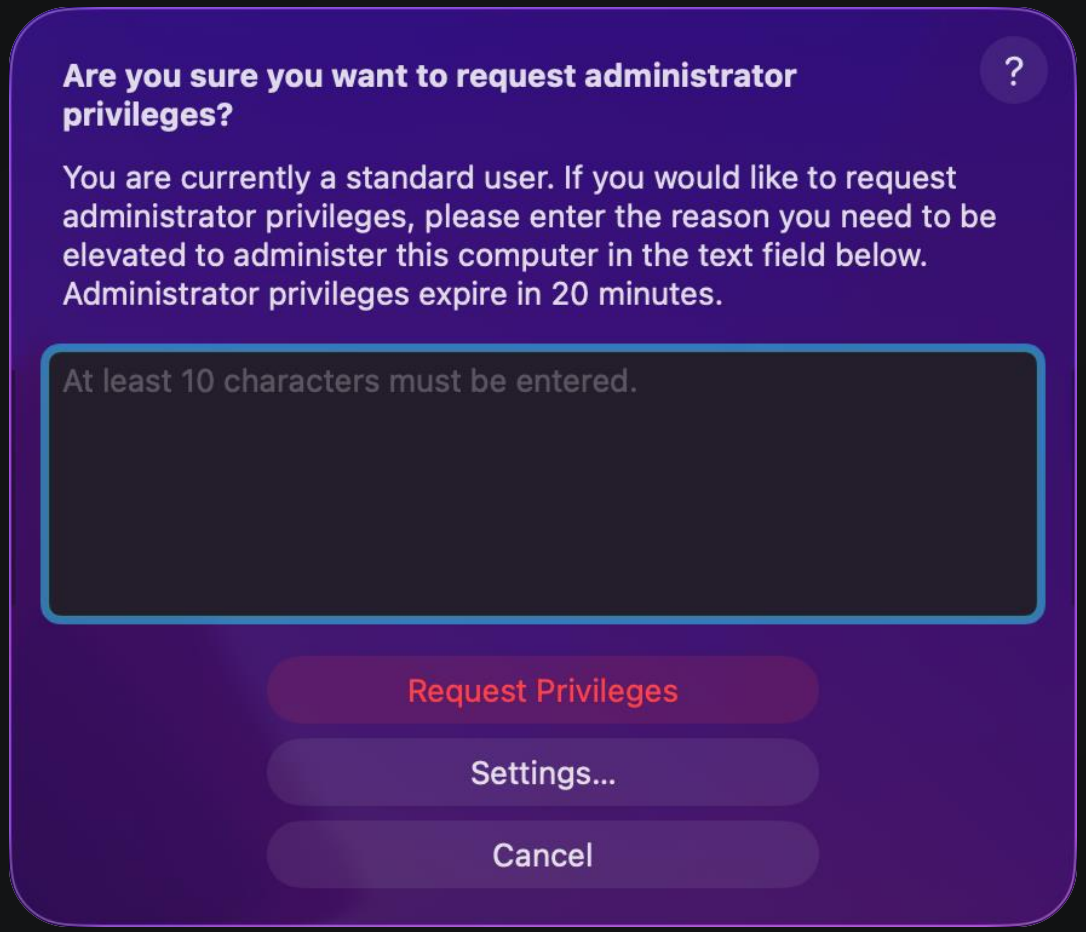
- **Revoke at login**: Force machines back to Standard User at sign-in;
- **Time Based Elevation**: Allow a user to be Admin for 10 minutes, then Revert to Standard User
- **Management via MDM profiles**: From v1.5+, manage app & CLI settings centrally (require reasons, set expiry, menu timer, etc.).

Which Legend made this?

- Originally developed by **Marc Thielemann**
- Part of SAP's commitment to **secure enterprise macOS deployments** by assisting Admins Enforce **least privilege** without sacrificing user productivity.
- Open-source under **Apache 2.0 license**.

Privileges

What does it look like?



wpninjas.au

Demo Time

wpninjas.au

The Community

For those looking to learn more

Resource	Description
Welcome to IntuneMacAdmins | IntuneMacAdmins	A community-driven platform offering guides, scripts, and best practices for managing macOS devices with Microsoft Intune. Focused on centralizing macOS-related Intune content and encouraging community contributions.
Intune - In Real Life	A blog by Microsoft MVP Somesh Pathak focusing on real-world Intune scenarios, macOS management, security hardening, and modern workplace strategies.
IntuneStuff	A resource hub and blog by Joery van den Bosch, Microsoft MVP, sharing Intune tips, Copilot integration insights, and modern workplace solutions.
All Things Cloud	A blog by Oktay Sari, Microsoft MVP, focusing on Microsoft Intune, macOS security, and endpoint management best practices, with deep dives into advanced configurations.
Ugur Koc - Microsoft MVP for Intune and Security Copilot	Ugur Koc's is an MVP from glueckkanja - one of today's sponsors. His site and resources on Intune, Security Copilot, and automation. Includes blogs, scripts, and tools for modern endpoint management and security.
SkipToTheEndpoint	A blog by Microsoft MVP James Robinson covering Intune, Windows, and modern management topics, including security baselines and cloud-native endpoint strategies.
https://macadmins.news/	A weekly curated newsletter by Armin Briegel summarizing Apple device management news, updates, and resources for Mac admins.
MacAdmins.org	A global Slack community for Apple device administrators with 50,000+ members. Offers channels for technical discussions & support for many of the Open Source tools mentioned in this presentation.
Microsoft MacAdmin LinkedIn Community	An official Microsoft-hosted LinkedIn group for IT pros managing Macs with Microsoft 365 and Intune. Provides a space to share experiences, best practices, and connect with peers.
Microsoft Intune Shell Samples	A GitHub repository maintained by Microsoft with sample shell scripts for macOS and Linux devices managed via Intune. Useful for extending management capabilities and automation.

📒 **Note:** If you are trying to record macOS Setup Assistant, please read this article Screen Recording Options - Dan K. Snelson

Thank you