NEXXT

WORKPLACEDUDES

Meetup

Mastering MacOS Management with Microsoft Intune;

Tips, Tricks, and Treats

Oktay Sari

08-02-2024

WORKPLACEDUDES

About “Oktay Sari”

Focus

Family man,

Microsoft Intune and all things security

Awards

Microsoft® Most Valuable Professional

From

Netherlands

Hobbies

Hiking, woodworking,

Whisky, Rum, Craft Bear & BBQ

My Blog

https://allthingscloud.blog

Contact

@oktay_sari

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

WORKPLACEDUDES

Agenda

- Apple Business Manager (just quickly…)
  - Why ABM?
  - Onboard, Connect, Configure
- Device Configuration
  - (Platform) SSO
  - Local Account Management
  - Declaritive Device Management (DDM)
  - Rapid Security Response (RSS)
  - App Deployment
- TIPS, Tricks and Treats
  - PLIST and MobileConfig files
  - PLISTWATCH
  - Imazing Profile Editor
  - AppleSeed for IT
  - MacAdmins

Apple Business Manager

ABM; Your Work BFF

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

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

Source: https://www.apple.com/business/docs/site/Mac_Deployment_Overview.pdf

Intune is NOT (yet) the Holy Grail when it comes to managing macOS

But it has come a long way….

ABM & Intune; Match made in heaven??

- **STEP 1: Swiping Right on ABM to Enroll…**
  - https://business.apple.com/signup/

You see? Enrolling in ABM is as easy as setting up a dating profile…

ABM & Intune; Match made in heaven??

- **STEP 2: The Courtship - Intune Meets ABM**

  Play matchmaker! Grant Microsoft permission to introduce your user and/or device info to Apple…

ABM & Intune; Match made in heaven??

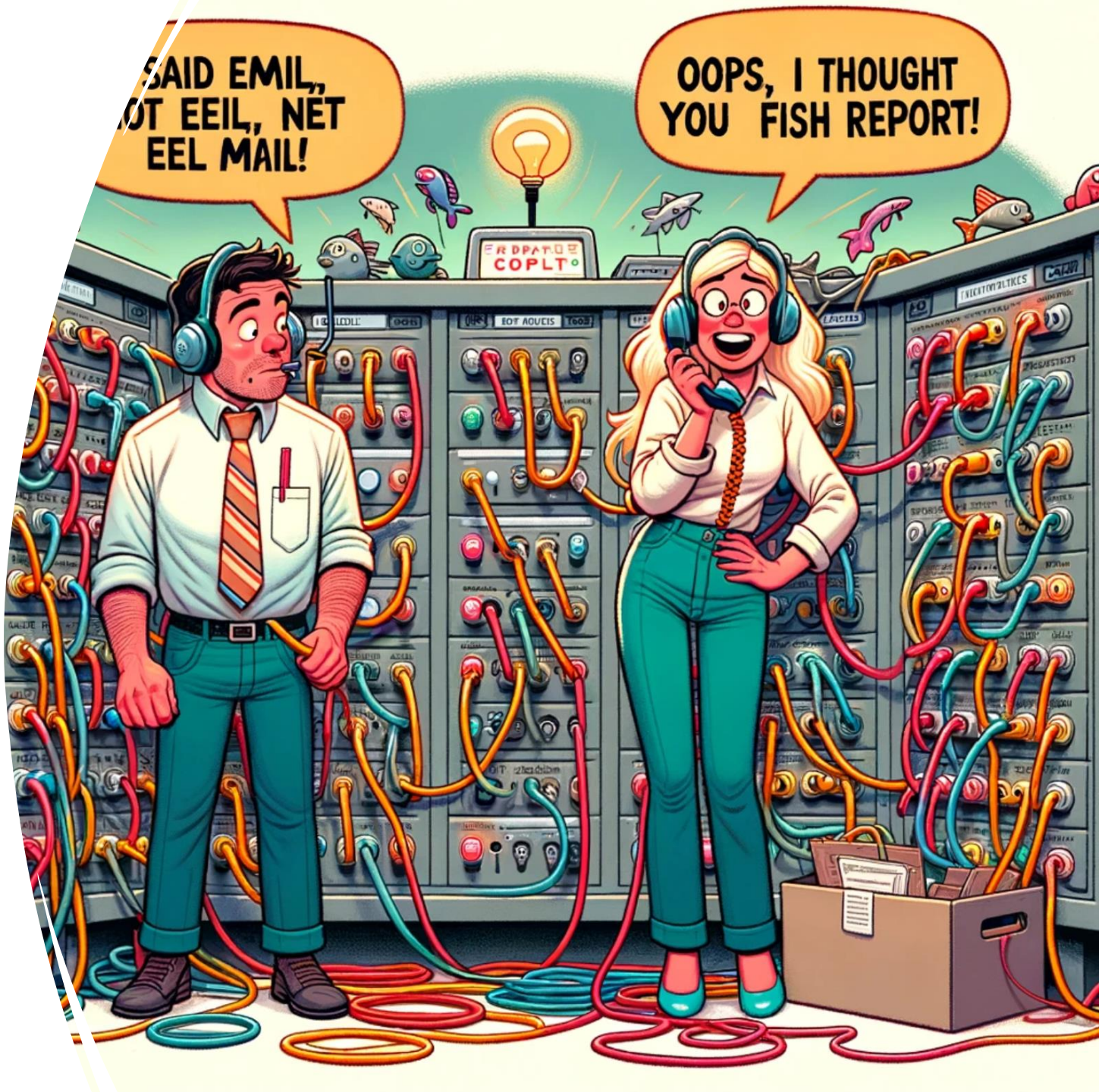
- **STEP 2: The Courtship - Intune Meets ABM**

  Create that Apple PUSH Notification Certificate -- think of it as the engagement ring. Remember, no personal accounts here!

ABM & Intune; Match made in heaven??

- **STEP 2: The Courtship - Intune Meets ABM**

  Configure the Push Certificate; This is where you make sure the communication lines are open and clear. Just like home!



ABM & Intune; Match made in heaven??

- **STEP 2: The Courtship - Intune Meets ABM**

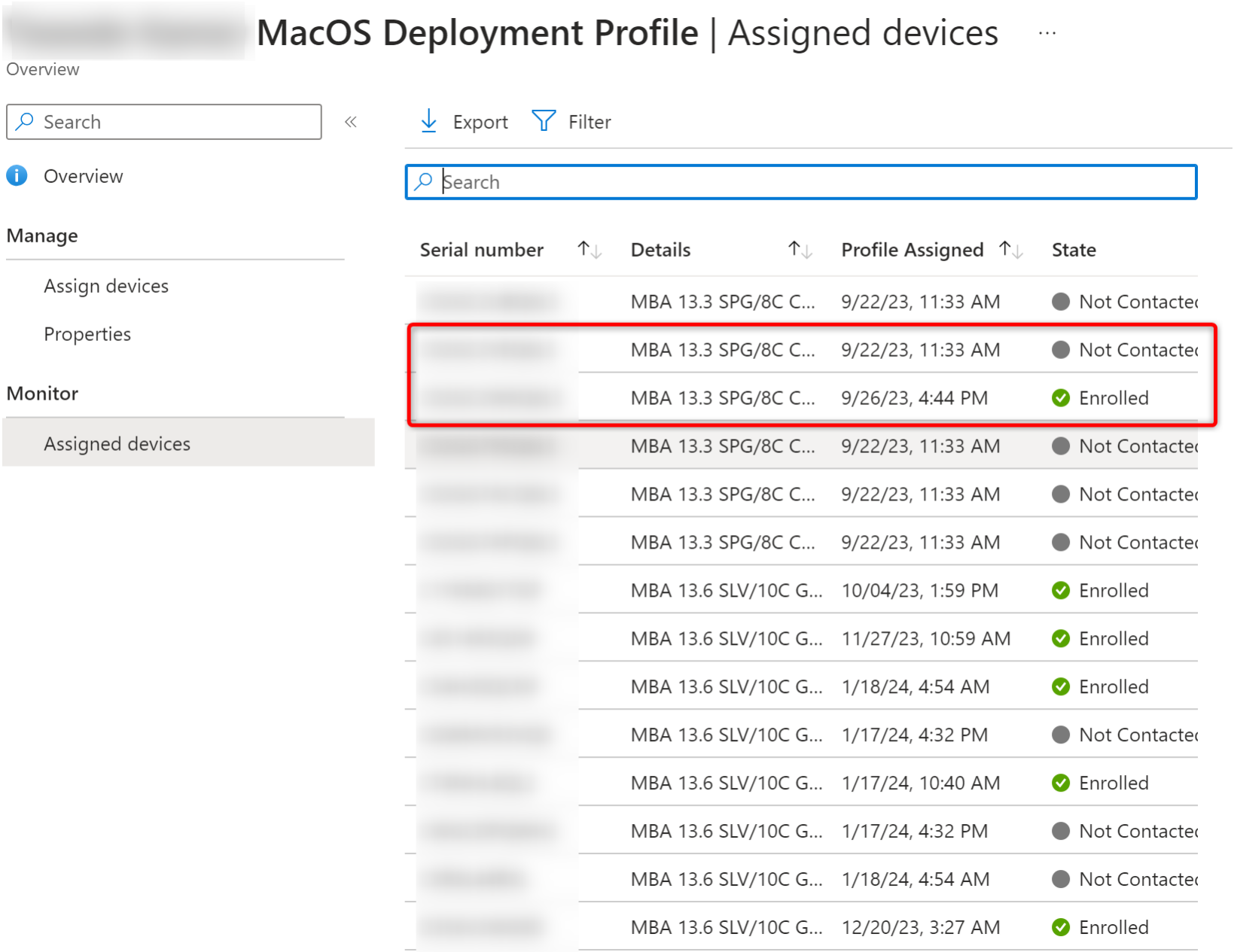
- Crafting the Apple **Enrollment Program Token** is like planning the perfect honeymoon. Get it right, and it's smooth sailing…

ABM & Intune; Match made in heaven??

- **STEP 2: The Courtship - Intune Meets ABM**

  Finally, assigning devices to the **Enrollment Program Token Profile** is like sending out the invites to the exclusive party. Make sure every device knows where it's going

Assigned devices



Device Configuration

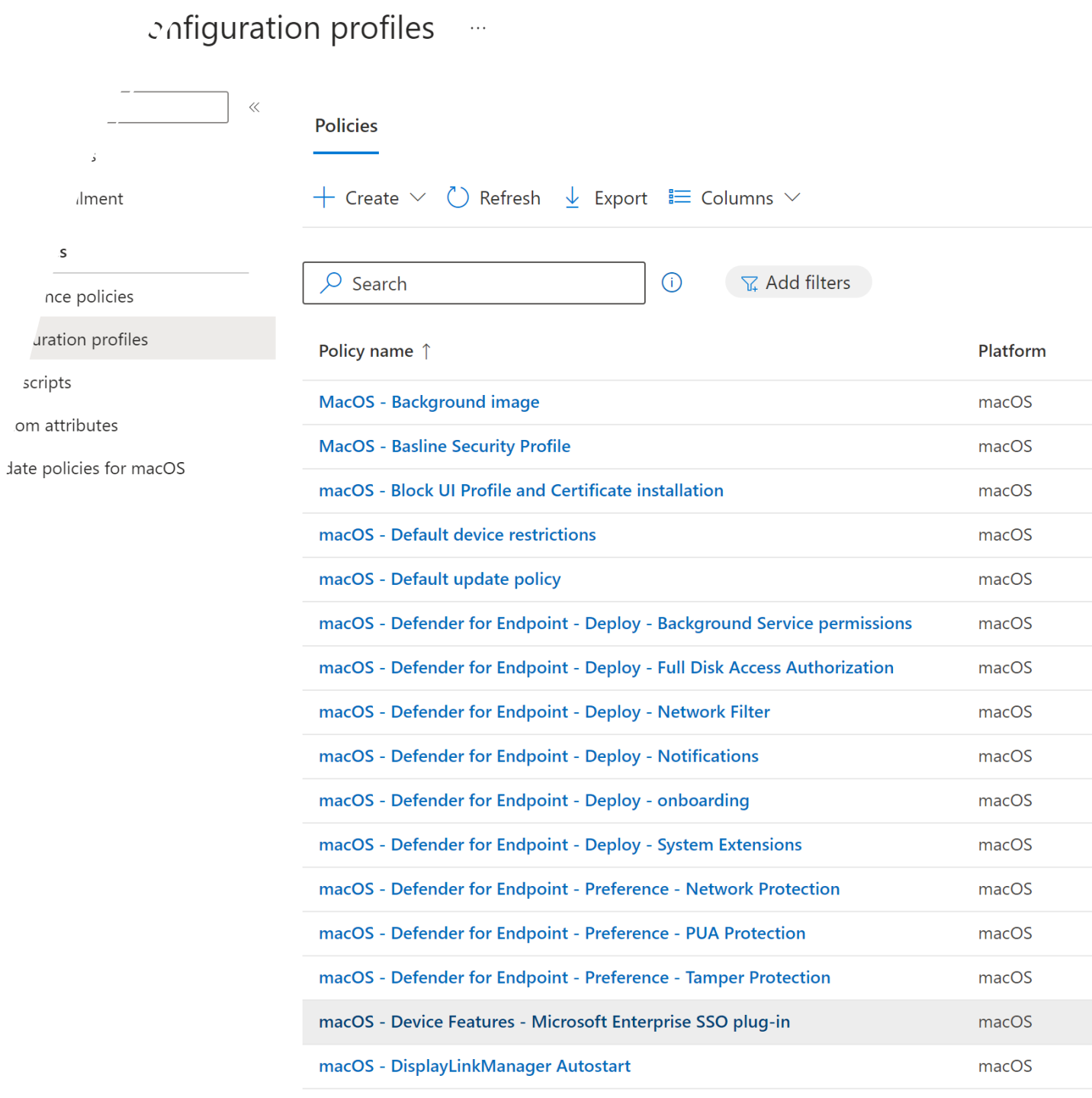
It’s like this…

Configuring macOS with Intune can sometimes leave even the most tech-savvy professionals nibbling on their pencils.

Hang in there –

You’ll crack the code…once you swap your Windows for a macOS!

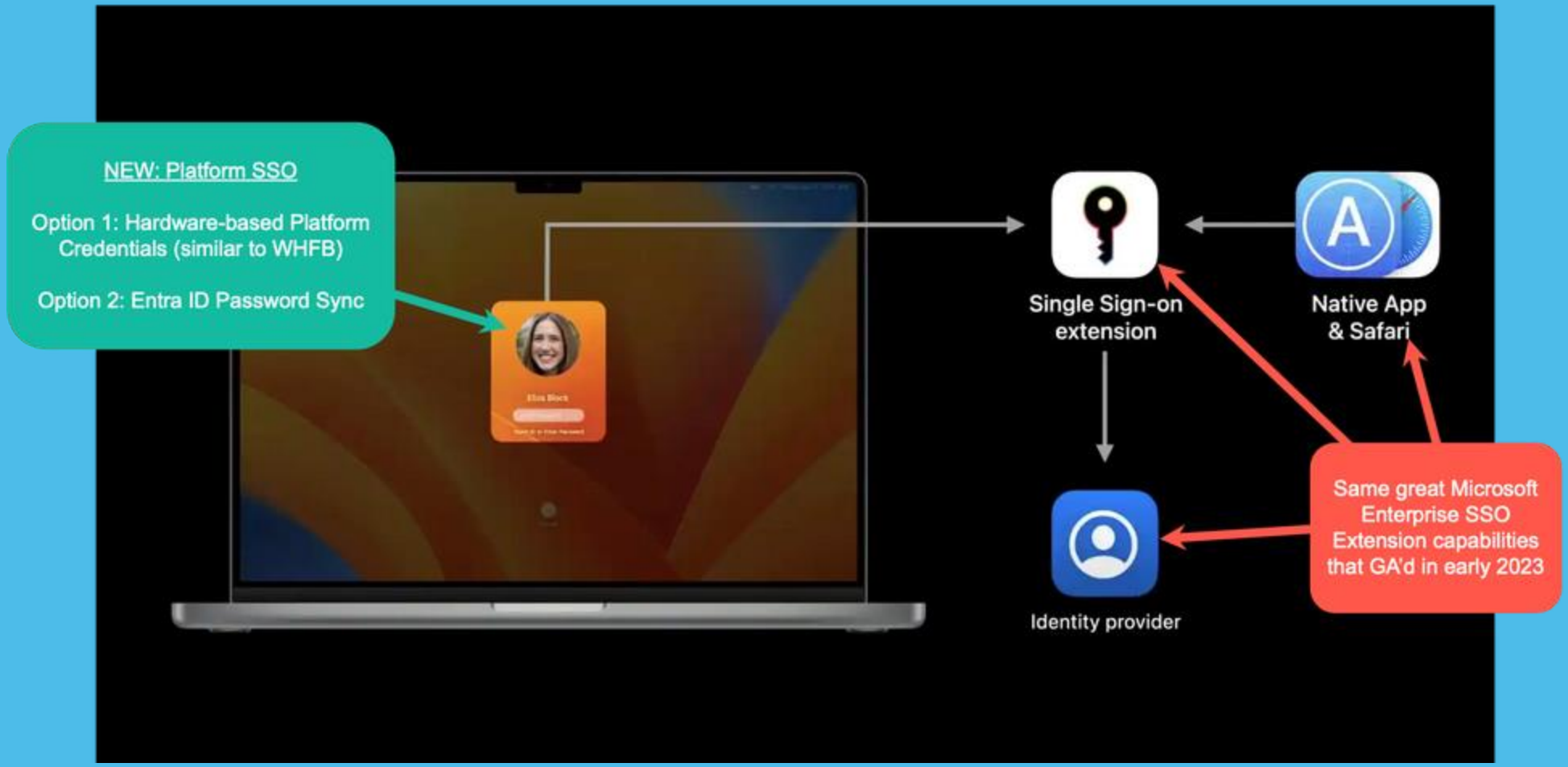
MacOS Configuration Profiles



Platform SSO

What’s the buzz…"Single Sign-On: because your team's memory space is better used for remembering lunch orders, not passwords

Platform SSO



Platform SSO

Why is it important? This is what normally happens

- Remote Management (sign in with Entra ID)
- Local user account creation (local admin / no pw sync)
- Company Portal App Sign in

Platform SSO

Prerequisites for enabling Platform SSO:

- The preview version of the Company Portal app
- SSO extension and Platform SSO configuration profiles in Intune.
- MacOS devices are enrolled in Intune.

Supported OS Versions

- MacOS Ventura (13) and newer.

Local Account Management

Local Account Management

Coming soon? Maybe this half?;

- Developing support for the local administrator account and local primary account creation during macOS ADE (automated device enrollment).

- The plan is to enable you to customize the local administrator settings within new and existing macOS enrollment profiles for devices enrolling with user-device affinity.

Source: https://techcommunity.microsoft.com/t5/microsoft-intune-blog/10-ways-microsoft-intune-improves-apple-device-management/ba-p/3766718

Enterprise SSO plug-in

Device features

macOS

Login window

Single sign-on app extension

Configure an app extension that enables single sign-on (SSO) for devices running macOS 10.15 or later.

User approved and automated device enrollment

These settings work for devices that were enrolled in Intune with user approval, and for devices enrolled using Apple School Manager or Apple Business Manager with automated device enrollment (formerly DEP). This includes all supervised devices.

SSO app extension type: Microsoft Entra ID

App bundle IDs

App bundle ID
com.example.app

Additional configuration

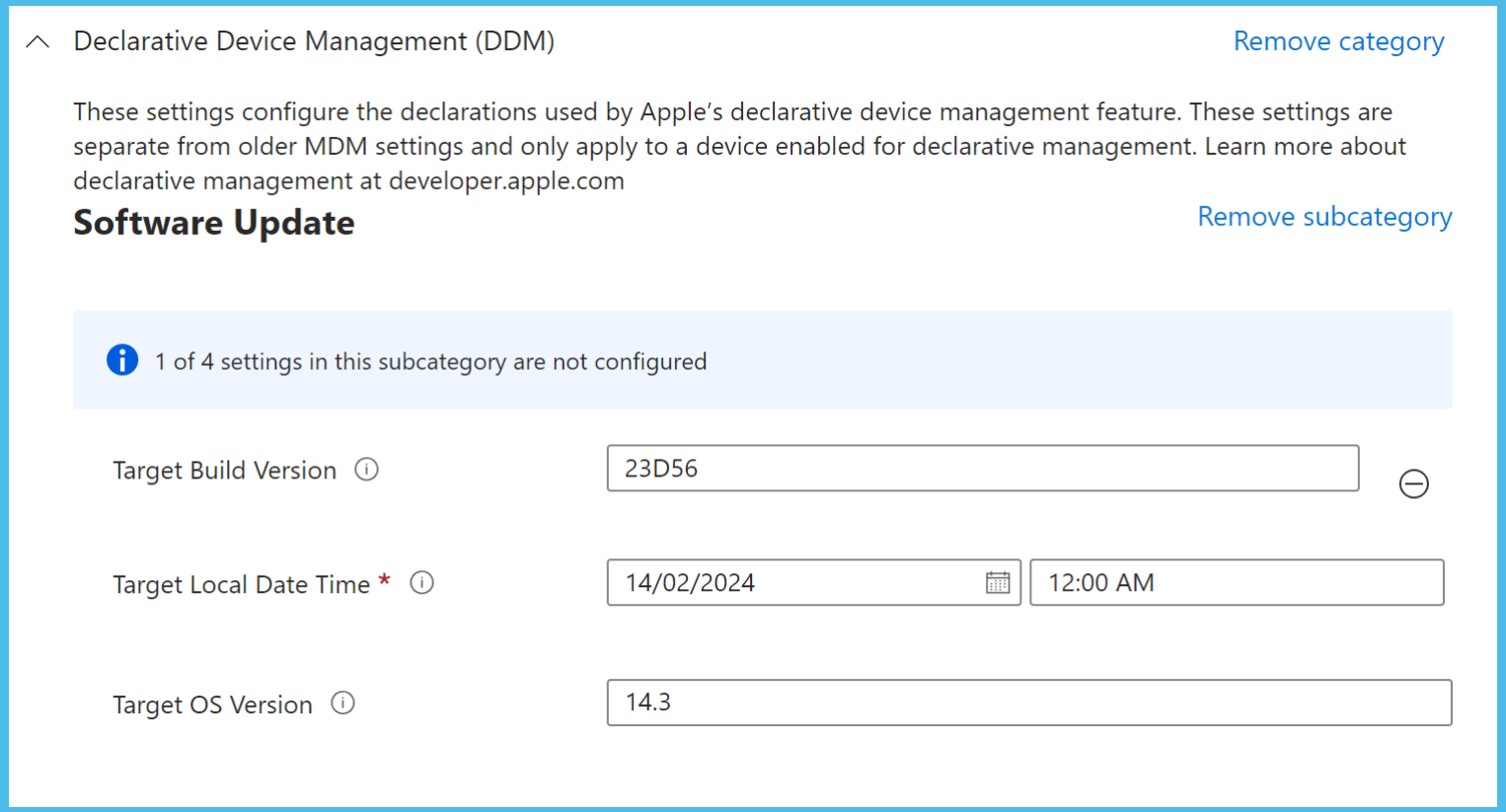
Key	Type	Value
browser_sso_interaction_enabled	Integer	1
disable_explicit_app_prompt	Integer	1
AppPrefixAllowList	String	com.microsoft. ,com.apple.
Enable_SSO_On_All_ManagedA...	Integer	1
Not configured	Not configured	Not configured

Enterprise SSO

DDM

Declarative Device Management is like having a smart assistant for your devices. You tell it what the **end state** should look like, and voilà! It figures out the 'hows' faster than you can say 'automate my tasks, please…

DDM



Rapid Security Response

Rapid Security Responses are a new type of software release for iPhone, iPad, and Mac. They deliver important security improvements between software updates—for example, improvements to the Safari web browser, the WebKit framework stack, or other critical system libraries. They may also be used to mitigate some security issues more quickly, such as issues that might have been exploited or reported to exist "in the wild."

RSS

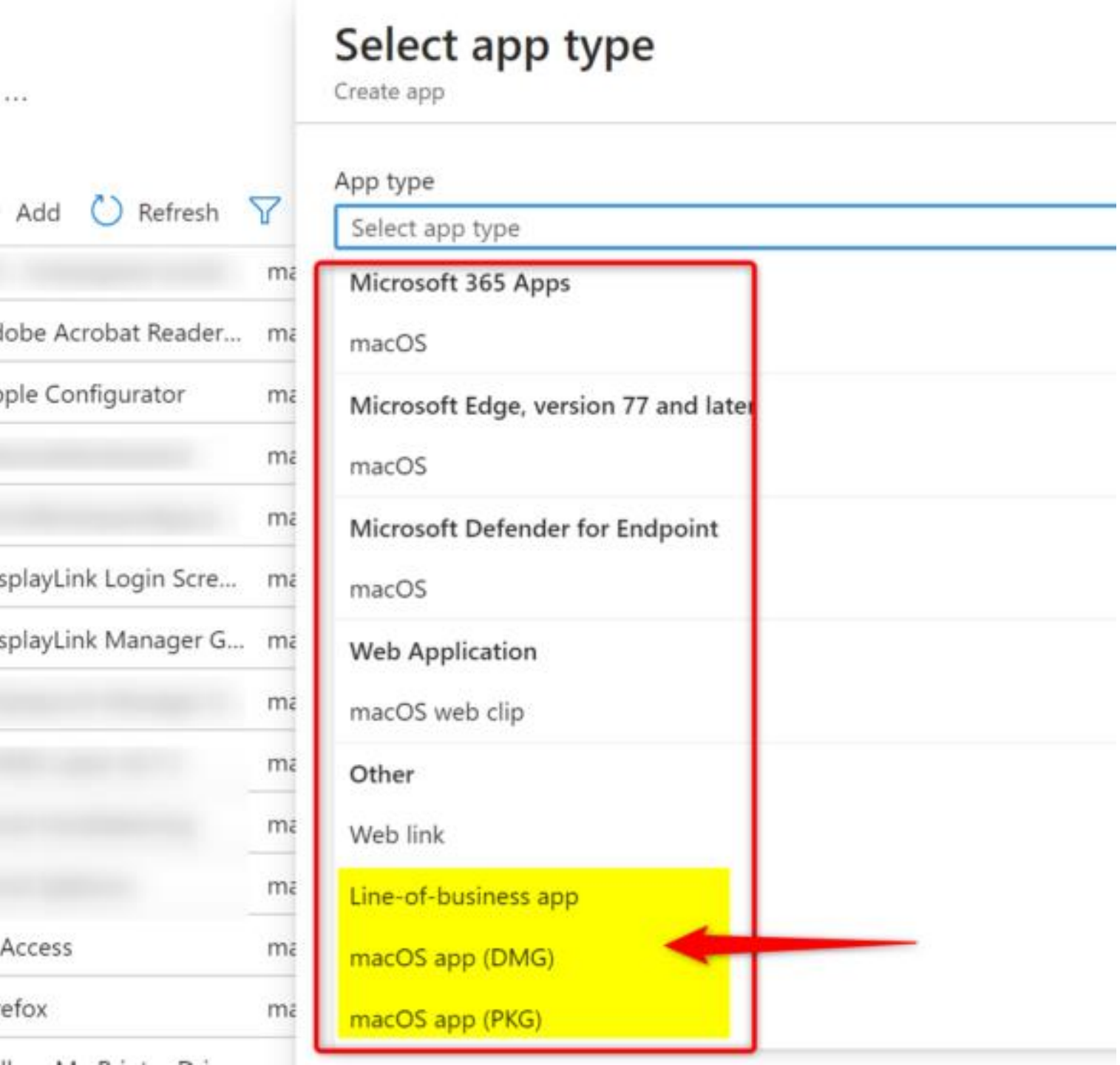
Configuration settings Edit

Restrictions

Configure the Restrictions payload to enable or disable features on devices. These configurations can be used prevent users from accessing a specific app, service or function on enrolled devices. For example, a restriction can be added that prevents an iPhone or iPad from using AirPrint. Another restriction can be added to prevent the sharing of passwords over AirDrop on an iPhone, iPad and Mac. Certain restrictions on an iPhone may be mirrored on a paired Apple Watch.

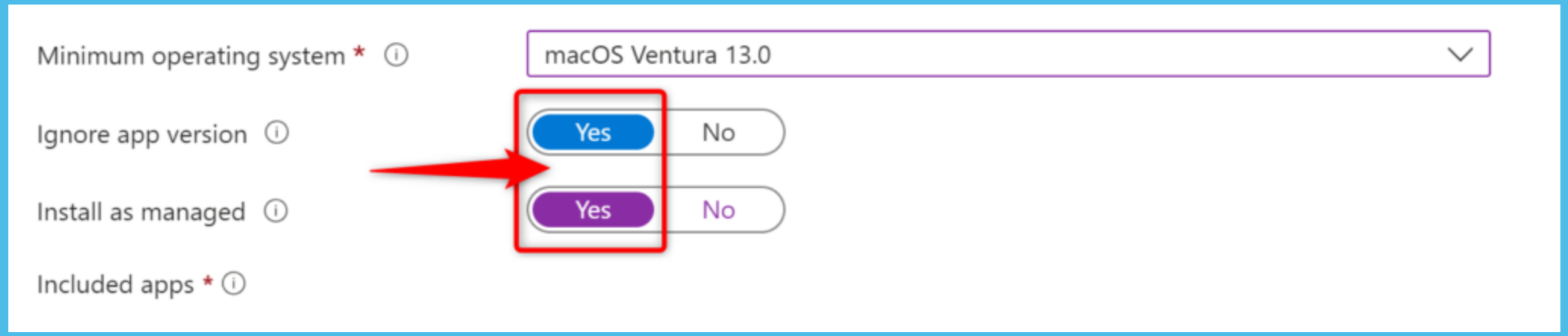
Allow Rapid Security Response Removal ⓘ	False
Allow Rapid Security Response Installation ⓘ	True

App Deployment



App deployment

LOB (Managed Apps)



NEED TO KNOW:

You can wave goodbye to the app with the ‘uninstall assignment type’ on devices that support this feature.

When you decide to pull the plug on the MDM profile (remove it), it’s like a clean sweep – every managed app, along with its data, gets whisked away from the device

PKG (Unmanaged Apps)

NEED TO KNOW:

Apps deployed by both the PKG and DMG deployment methods are considered unmanaged. When it comes to assigning apps using the PKG deployment method, think of it as a one-way street.

The only option you've got is the "**Required**" assignment type. The "**Available for enrolled devices**" and "**uninstall**" options? They're like those elusive ice cream flavors that aren't on the menu right now.

DMG (Unmanaged Apps)

NEED TO KNOW:

When deploying DMG apps, you have both the "**Required**" assignment type and the "**uninstall**" options in your toolkit. The "**Available for enrolled devices**" is not available for DMG apps.

Managed vs Unmanaged?

“ To install an app as managed, you have to deploy it via the macOS MDM stack, which means it has to meet those strict requirements. Lots of PKGs can never meet the requirements to be deployed via MDM and for those or custom PKGs (lots of security agents, VPN's etc) we must deploy via agent instead.

The tradeoff really is that you get much more flexibility from deploying as unmanaged, but you lose some of the lifecycle controls. We're hoping to try and add these to the unmanaged side too over the year.”

Ignore App Version

NEED TO KNOW:

Ignore App version setting	App install status on Device	App Deployment action
YES	App is NOT found	Deploy the app
	App is installed: Other version	Do not deploy
NO	App is NOT found	Deploy the app
	App is installed: Other version	Deploy the app

Tips, Trics and Treats

PLIST & MobileConfig

WORKPLACEDUDES

PLIST

NEED TO KNOW:

.plist (Property List) files are fundamental components of macOS, storing application preferences and configuration settings. Intune leverages PLIST files to provide granular control over macOS devices by enabling administrators to modify these files directly.

PLIST

- **Purpose:**
  - Plist files are used to store settings and configuration data for applications and system components.
- **Format:**
  - Plist files can be in XML format or a binary format. They can be edited with a text editor, property list editor, or with command-line tools like defaults.

- **Scope:**
  - Plists are often specific to an application or system component and are used to store settings and preferences for that particular element. They can be scoped at system and user level. You are configuring only one payload. For example; com.apple.dock.plist
- **Examples:**
  - Application settings, system preferences.

.Mobileconfig

- **Purpose:**
  - Mobileconfig files are also used to configure settings, but more like actual configuration profiles in macOS and iOS.
- **Format:**
  - Mobileconfig files are essentially plist files but formatted specifically for profile management. It's a proprietary format that is similar to XML. They can be signed and encrypted.

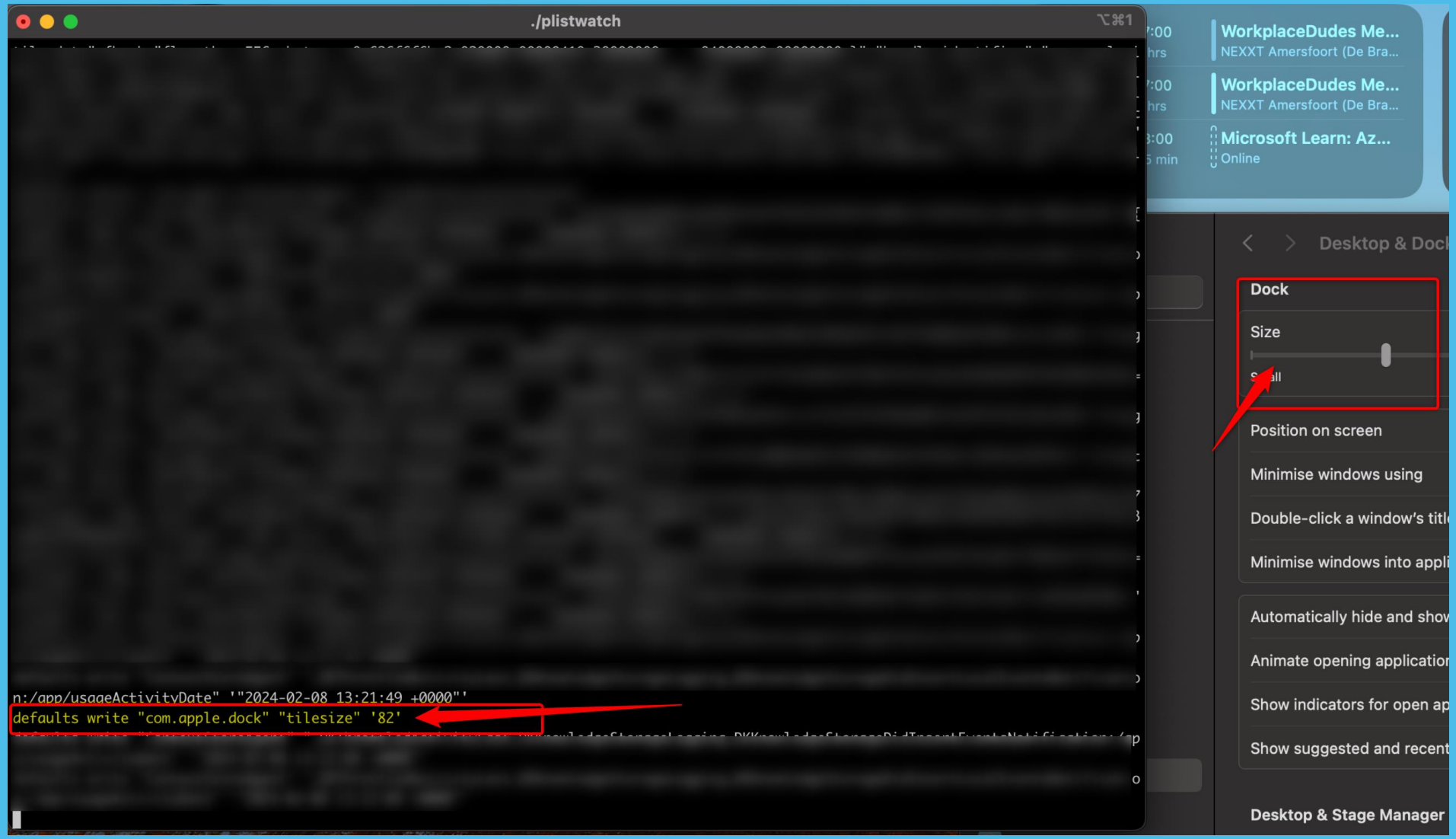
- **Scope:**
  - These files have a broader scope compared to plist files and are used for managing and deploying device-wide settings and configurations. A configuration profile can have more than one payload
- **Examples:**
  - Configuration profiles containing Wi-Fi settings, VPN configurations, email settings, security policies, restrictions, certificates, etc.

PLISTWATCH

PlistWatch monitors real-time changes to plist files on your system. It outputs a defaults command to recreate that change.

WORKPLACEDUDES

PLISTWATCH



https://github.com/catilac/plistwatch

WORKPLACEDUDES

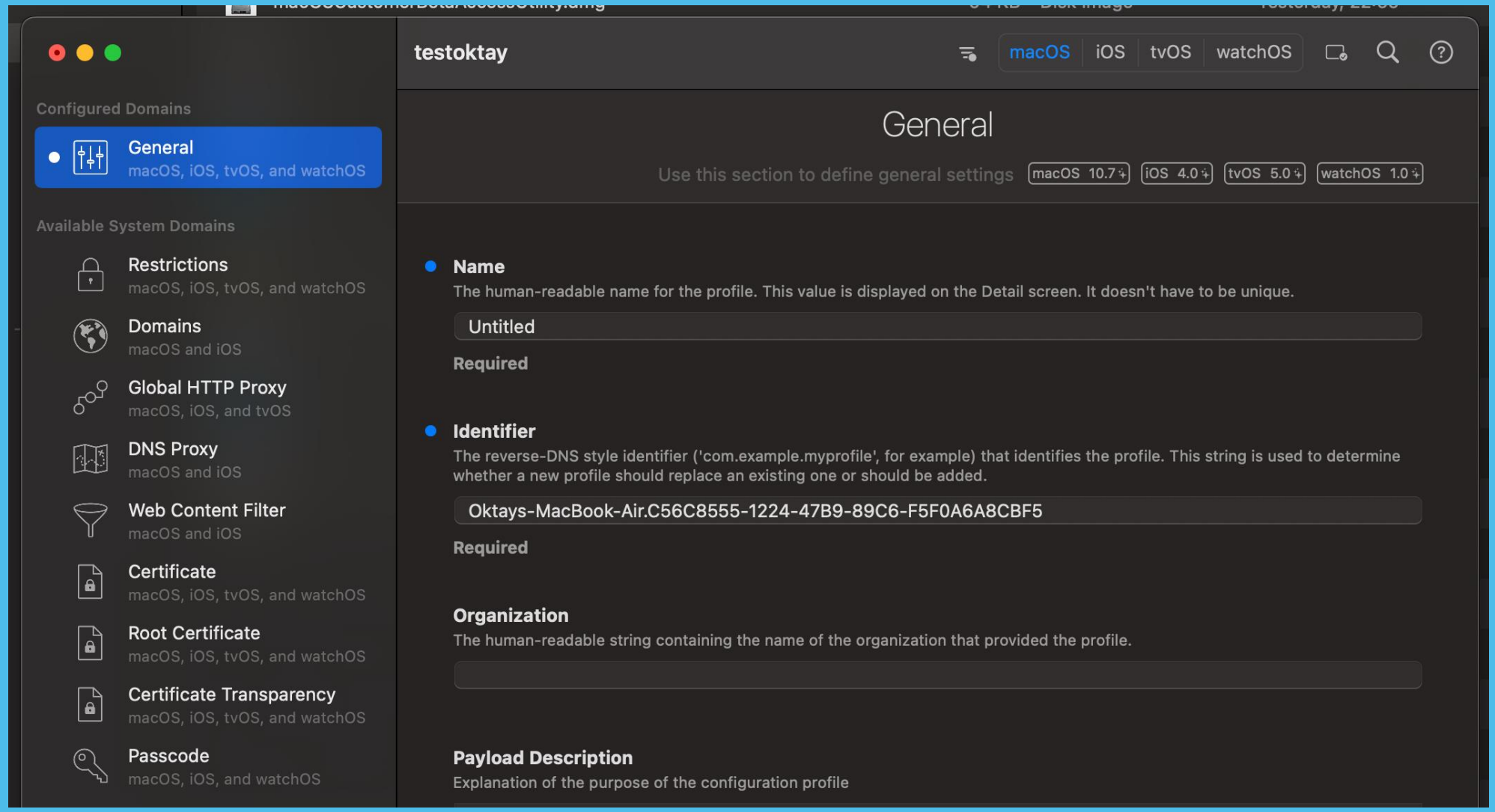
iMazing Profile Editor

Create, Edit, and Sign Apple Configuration Profiles

A free app to easily define settings that are ready to be deployed locally or via MDM to fleets of iPhones, iPads, Macs, and other Apple devices

WORKPLACEDUDES

iMazing Profile Editor



https://imazing.com/profile-editor

WORKPLACEDUDES

Appleseed for IT

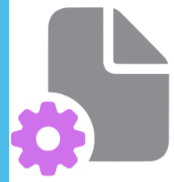
AppleSeed for IT

AppleSeed for IT

AppleSeed for IT provides IT professionals and technology managers an opportunity to evaluate prerelease software in your unique work environments. Test against your IT infrastructure, corporate network and with mission critical apps to make sure you are ready to support employees, staff, and students with the latest Apple software.

https://beta.apple.com/it

AppleSeed for IT



Configuration Profiles

Exchange Mail and Calendar Sync Diagnostic Profile (2023)

Cryptographic Message Syntax (CMS) Diagnostic Profile

iOS Webclip for Beta Enrollment

iOS and iPadOS 17 AppleSeed Profile

macOS Beta Access Utility

tvOS 17 AppleSeed Profile

Test Plans & Documentation

2023 Shortcuts Automation with Apple Configurator Test Plan

macOS Testing Template

2023 Exchange Test Plan

Platform SSO developer documentation v2.0

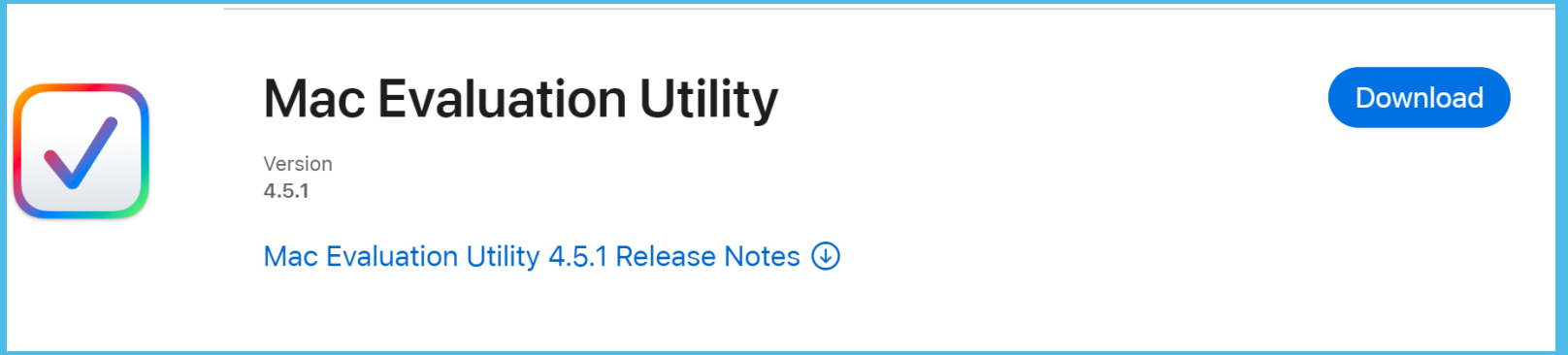
2023 Declarative Management: Software Update Enforcement Test Plan

Identity Provider developer documentation

https://beta.apple.com/it

WORKPLACEDUDES

AppleSeed for IT



Ensure your Mac is ready for work

Mac Evaluation Utility evaluates your organization's ability to deploy Mac computers. The app checks the network to help verify that critical hosts and services are reachable for essential services like Automated Device Enrollment and software updates.

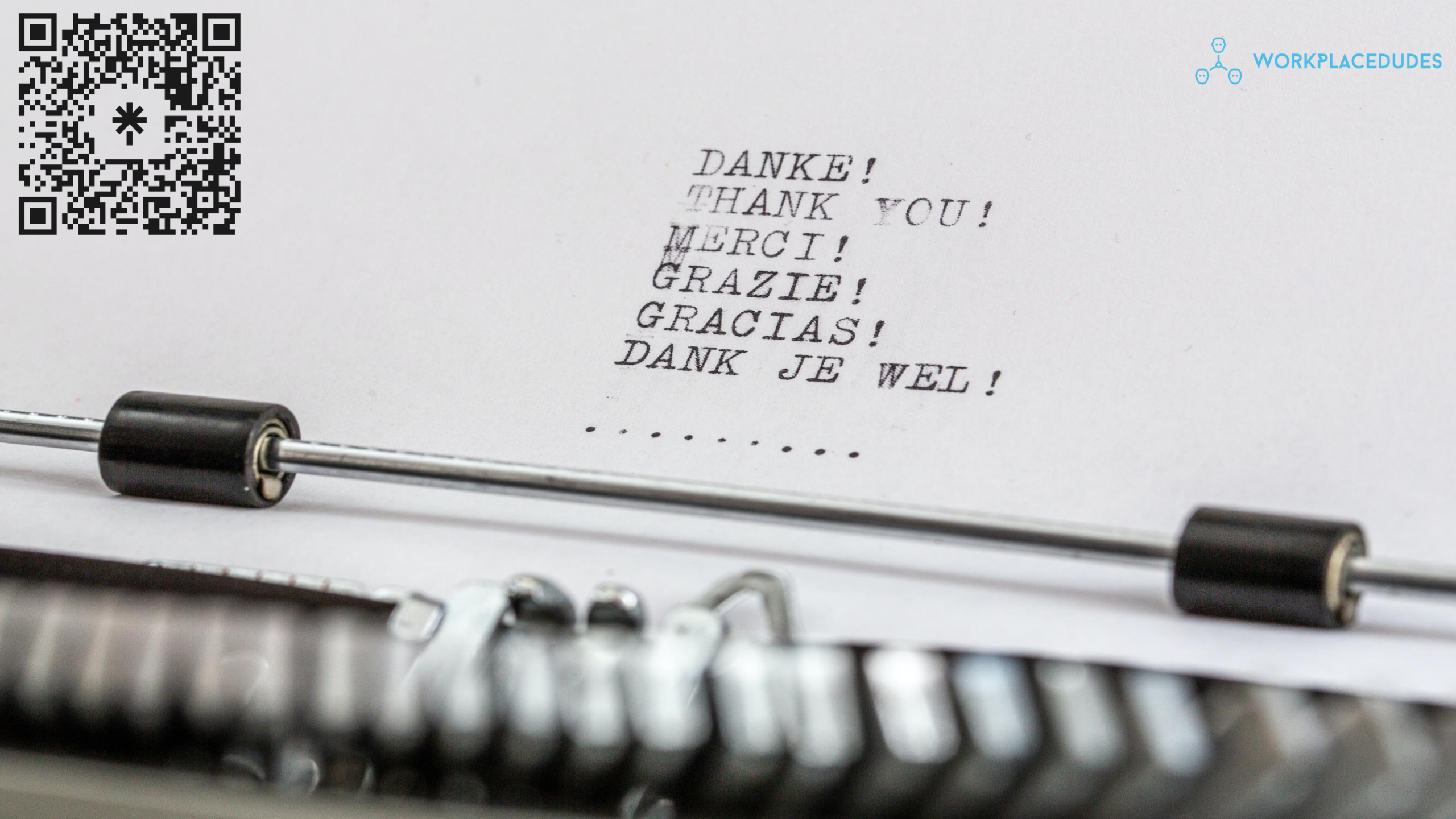
It also examines the device's management configuration to help make sure you're aligned with best practices. The results can be shared with colleagues to help you build a plan to succeed at deploying Mac computers at scale.

https://beta.apple.com/it

WORKPLACEDUDES

macAdmins

https://aka.ms/MacAdmins


DANKE!
THANK YOU!
MERCI!
GRAZIE!
GRACIAS!
DANK JE WEL!
.....