DIGITAL SURVIVAL
COMPANY

WORKPLACEDUDES

Meetup

macOS Security with Intune
From Basics to Bulletproof

Oktay Sari

27-02-2025

WORKPLACEDUDES

Focus

Microsoft Intune and all things Security

Hobbies

Hiking, Woodworking, RC planes & heli

Blog

https://allthingscloud.blog

You will never be ready, just start

Contact

@oktay_sari

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

Microsoft® Most Valuable Professional

RKPLACEDUDES

Agenda

01

macOS Security with Intune

- The basics
- The must haves
- Advanced security configurations
- Lessons learned & what to avoid

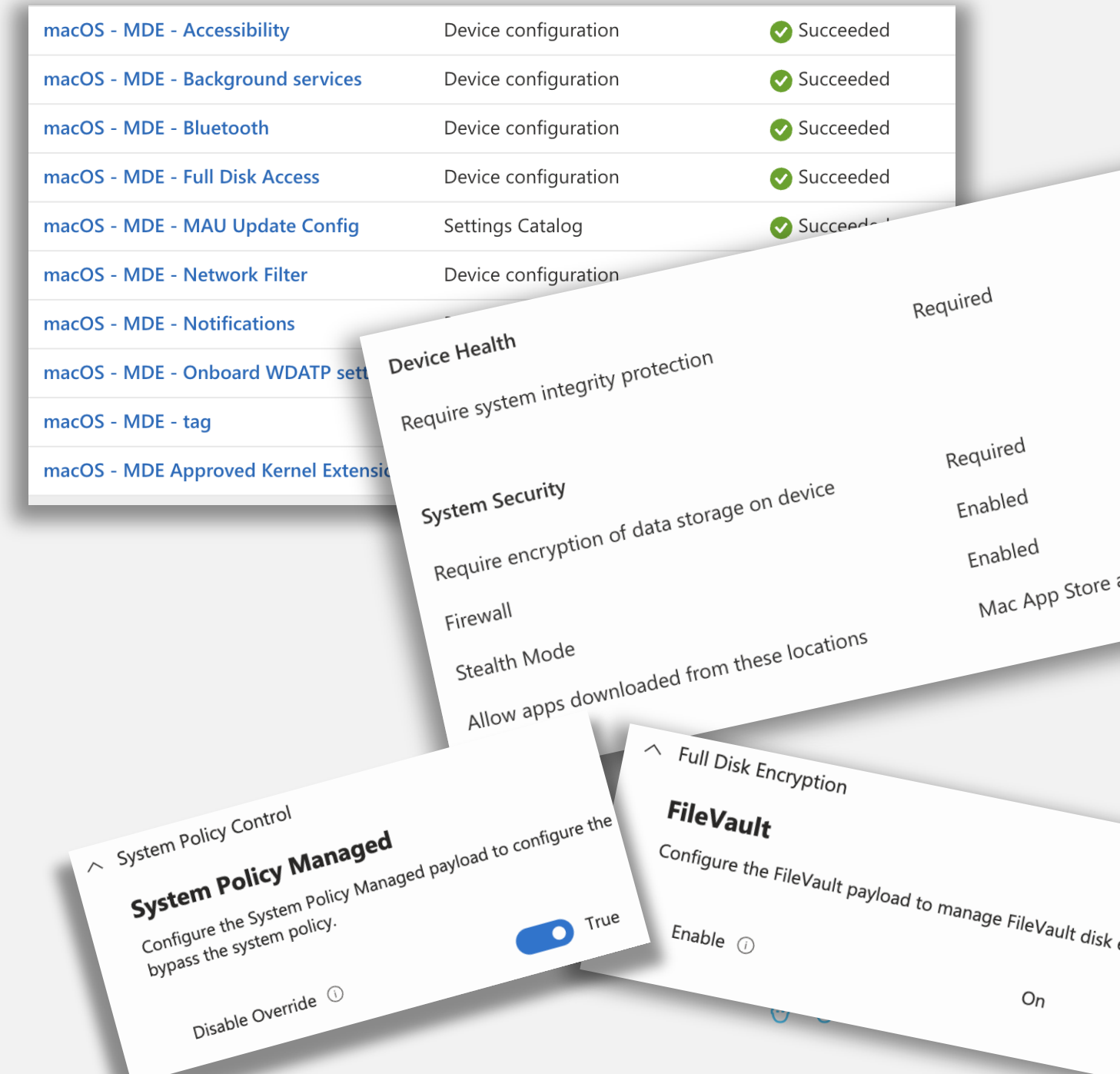
MacOS

Security
Best practices
from the field

WORKPLACEDUDES

The Basics

1. Compliance policies
2. Device restrictions and features
3. OS and Software Updates
4. Defender for Endpoint



The Must Haves

1. User and Accounts and Access
2. Disable Sharing options
3. Saving and Sharing Passwords
4. Cloud and storage

The Must Haves

1 User and Accounts and Access

- ❑ Disable password hints (login screen)
- ❑ ~~Disable show username and password window~~ (Wil break PSSO)
- ❑ Disable Guest accounts and remove guest Home folder
- ❑ Enable file name extensions

The Must Haves

2 Disable Sharing options

- ❑ Remote Apple Events
- ❑ Internet Sharing
- ❑ Screen Sharing (can have a negative impact)
- ❑ Printer Sharing
- ❑ Bluetooth Sharing
- ❑ SMB Sharing

The Must Haves

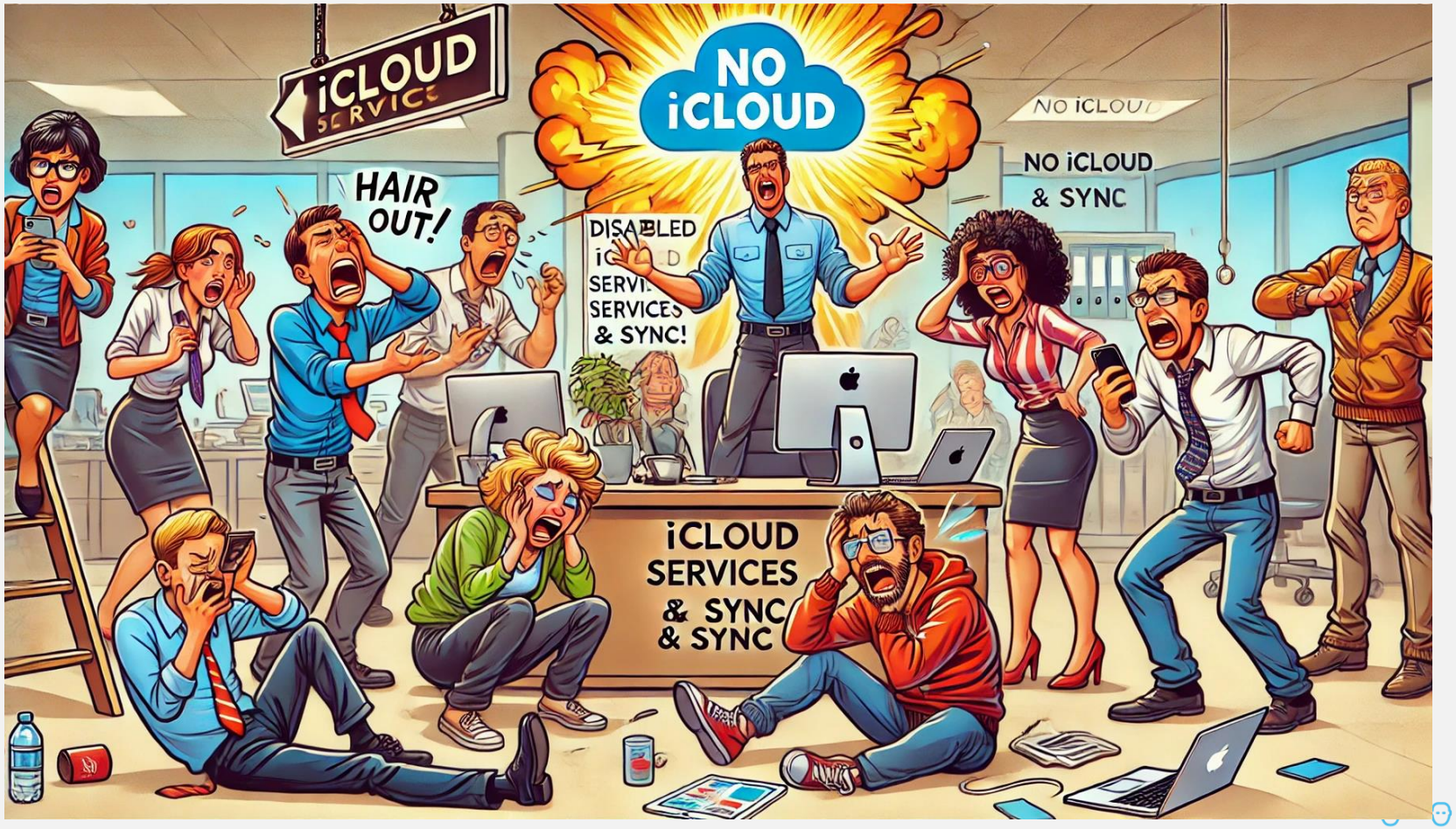
3 Disable Sharing and Saving Passwords

- ❑ ~~Disable Password Auto Fill~~ (Wil break PSSO)
- ❑ Disable Password Proximity Request
- ❑ Disable Password Sharing

If you want to drive everyone nuts...

4

Disable all iCloud services and syncs



Advanced Security configurations

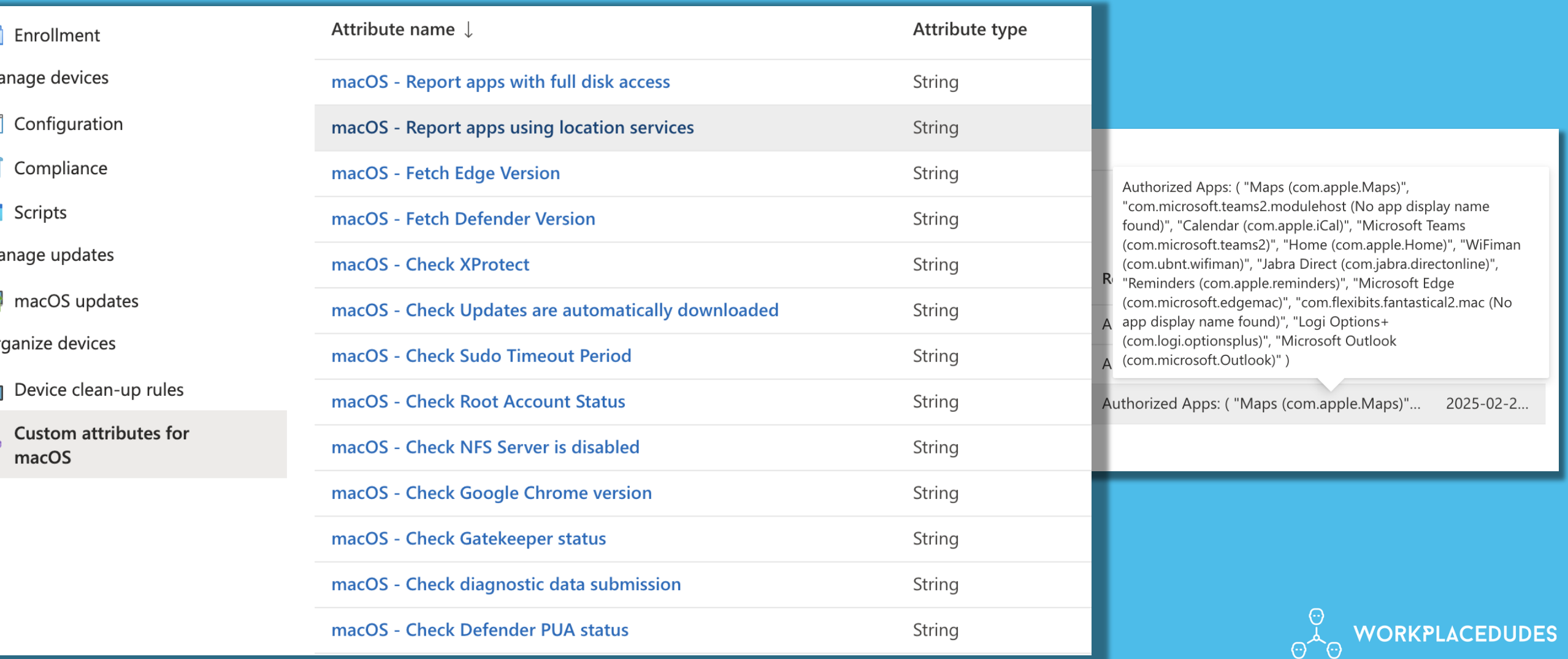
MacOS Scripts

	Platform	
- Set Login Window Banner	macOS	
ng - CIS_L2 - Set audit retention	macOS	Yes
Hardening - CIS_L2 - Set audit flags	macOS	Yes
Hardening - CIS_L2 - Enable Location Services Icon	macOS	Yes
Hardening - CIS_L2 - Configure Hide IP in Safari	macOS	Yes
Hardening - CIS_L2 - Audit apps with full disk acces:	macOS	Yes
Hardening - CIS_L2 - audit apps using location servi	macOS	Yes
Hardening - CIS_L1 - Show all filename extensions	macOS	Yes
Hardening - CIS_L1 - Set Sudo Timeout Period to Ze	macOS	Yes
Hardening - CIS_L1 - Secure User's Home Folders	macOS	Yes
Hardening - CIS_L1 - Install log retention 365	macOS	Yes
Hardening - CIS_L1 - Ensure Security Auditing Reten	macOS	No
Hardening - CIS_L1 - Enable Sudo Logging	macOS	Yes
ening - CIS_L1 - Enable Apple Mobile File Integ	macOS	Yes
IS_L1 - Disable Root	macOS	Ye
able Remote Login	macOS	
Server	macOS	

WORKPLACEDUDES

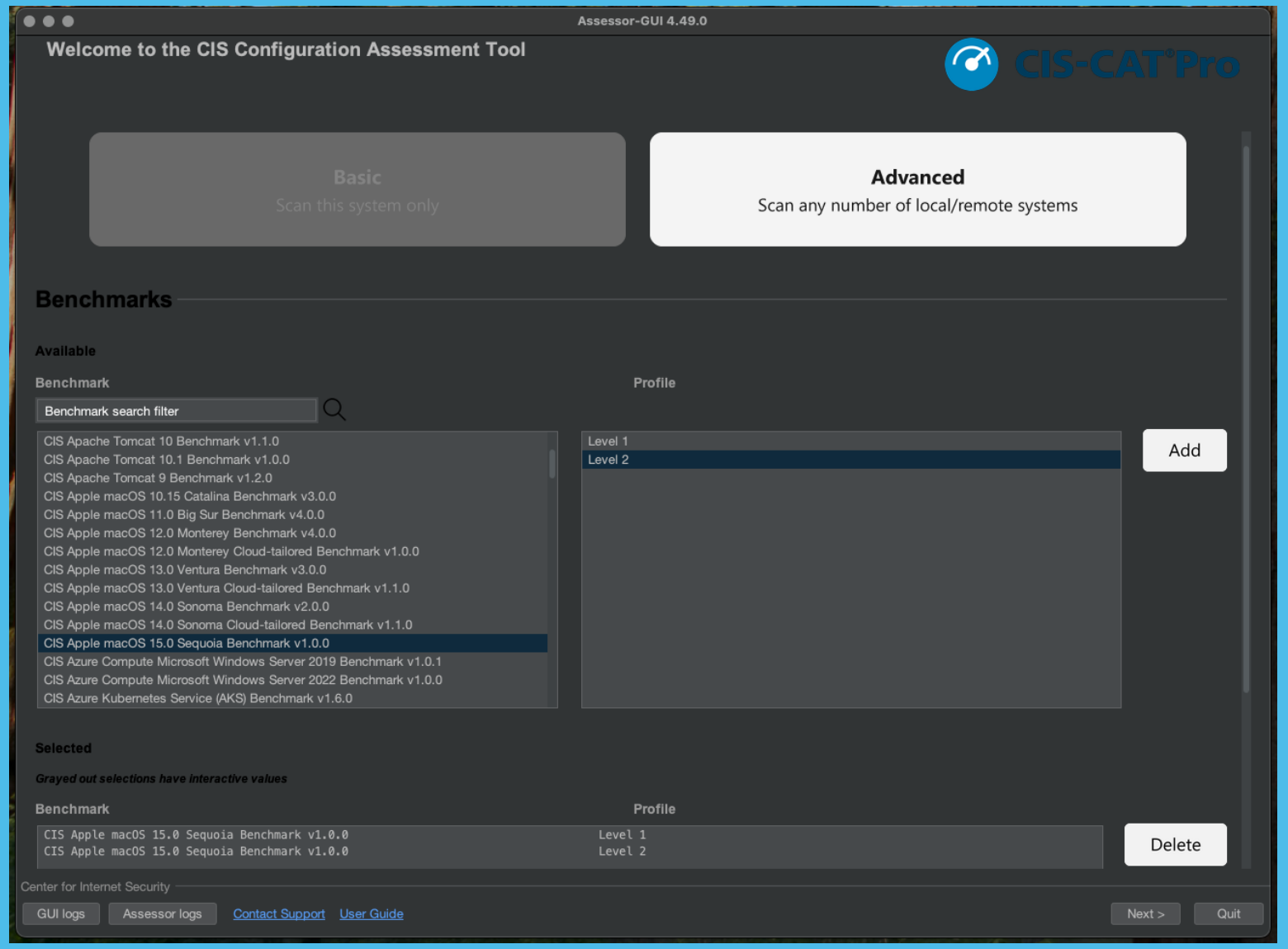
Settings Catalog & Custom Profiles

Custom attributes



WORKPLACEDUDES

CIS ASSESSOR

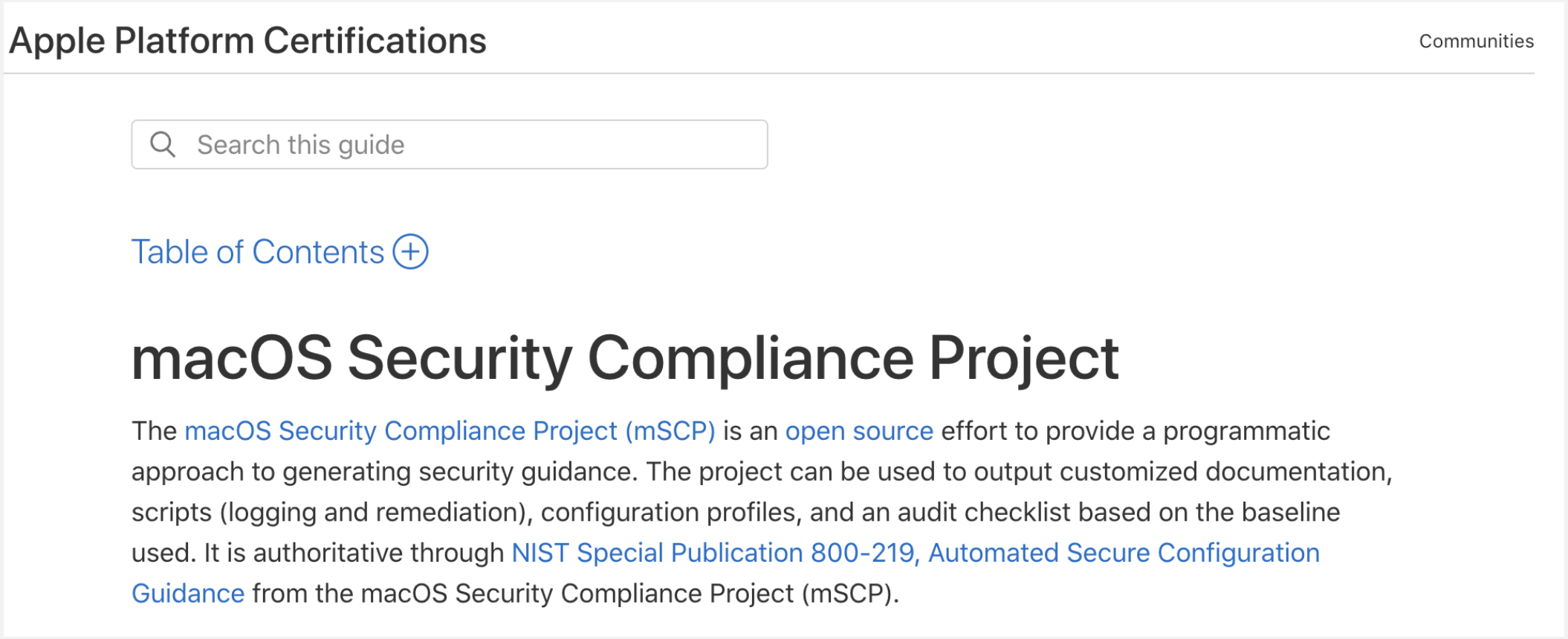


WORKPLACEDUDES

macOS Security Compliance

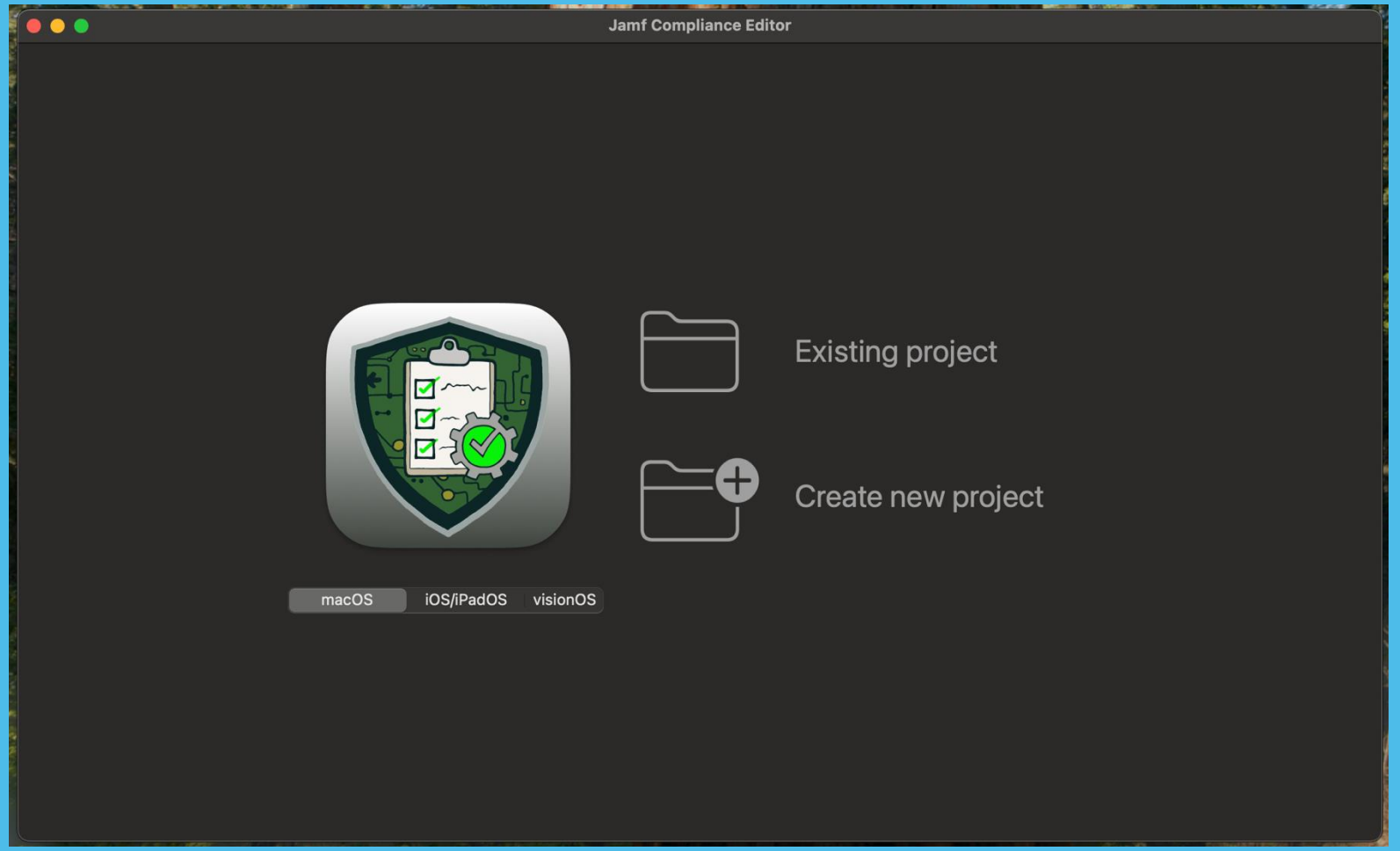
The macOS Security Compliance Project is an open source effort to provide a programmatic approach to generating security guidance

Source: https://github.com/usnistgov/macos_security

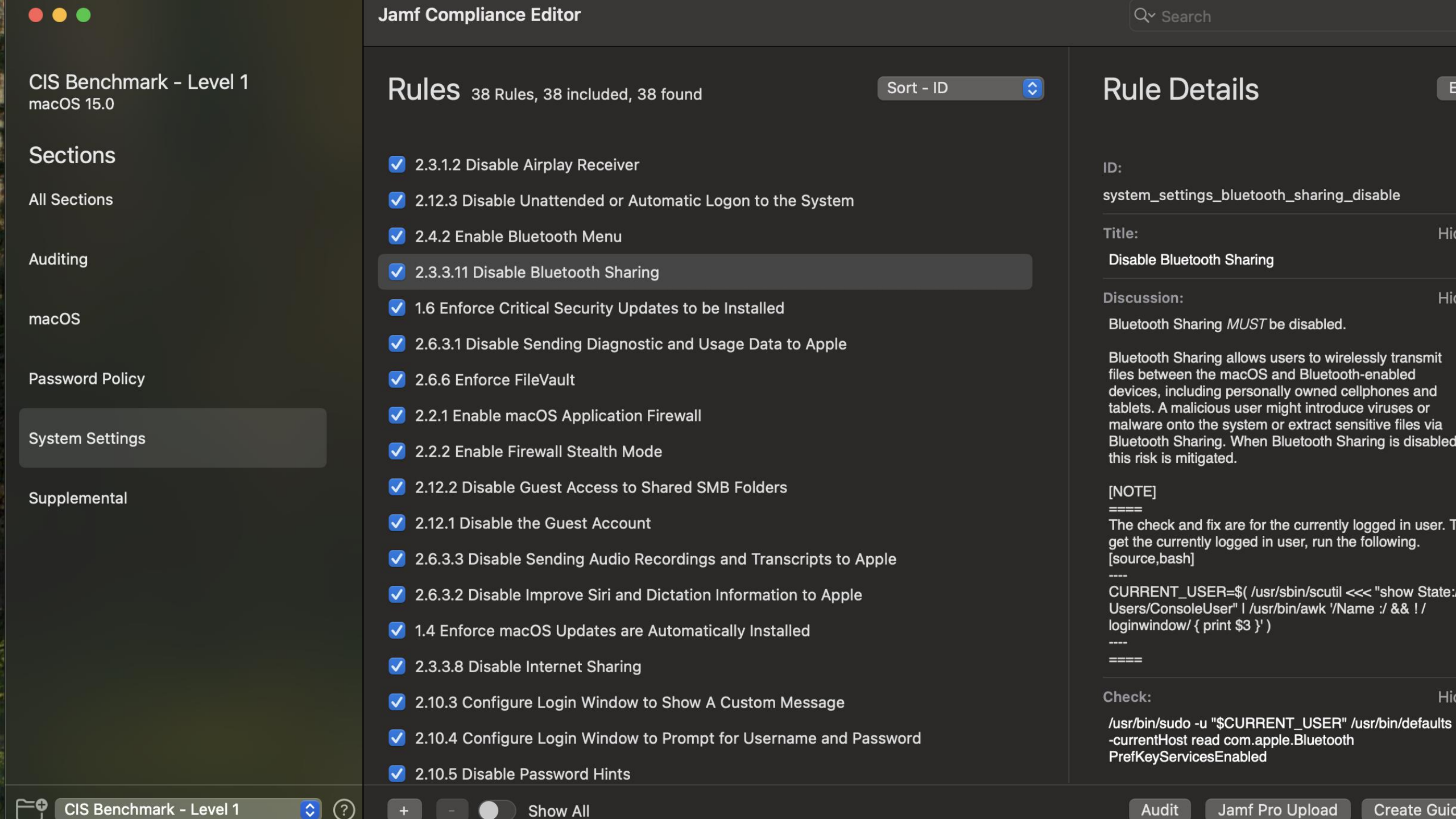


Source:https://support.apple.com/guide/certifications/macos-security-compliance-project-apc322685bb2/web

Jamf Compliance Editor



Source: https://github.com/Jamf-Concepts/jamf-compliance-editor/releases


Jamf Compliance Editor
Search
CIS Benchmark - Level 1
macOS 15.0
Sections
All Sections
Auditing
macOS
Password Policy
System Settings
Supplemental
Rules 38 Rules, 38 included, 38 found
Sort - ID
2.3.1.2 Disable Airplay Receiver
2.12.3 Disable Unattended or Automatic Logon to the System
2.4.2 Enable Bluetooth Menu
2.3.3.11 Disable Bluetooth Sharing
1.6 Enforce Critical Security Updates to be Installed
2.6.3.1 Disable Sending Diagnostic and Usage Data to Apple
2.6.6 Enforce FileVault
2.2.1 Enable macOS Application Firewall
2.2.2 Enable Firewall Stealth Mode
2.12.2 Disable Guest Access to Shared SMB Folders
2.12.1 Disable the Guest Account
2.6.3.3 Disable Sending Audio Recordings and Transcripts to Apple
2.6.3.2 Disable Improve Siri and Dictation Information to Apple
1.4 Enforce macOS Updates are Automatically Installed
2.3.3.8 Disable Internet Sharing
2.10.3 Configure Login Window to Show A Custom Message
2.10.4 Configure Login Window to Prompt for Username and Password
2.10.5 Disable Password Hints
Rule Details
ID:
system_settings_bluetooth_sharing_disable
Title:
Disable Bluetooth Sharing
Discussion:
Bluetooth Sharing MUST be disabled.
Bluetooth Sharing allows users to wirelessly transmit files between the macOS and Bluetooth-enabled devices, including personally owned cellphones and tablets. A malicious user might introduce viruses or malware onto the system or extract sensitive files via Bluetooth Sharing. When Bluetooth Sharing is disabled this risk is mitigated.
[NOTE]
====
The check and fix are for the currently logged in user. T
get the currently logged in user, run the following.
[source,bash]

CURRENT_USER=$(/usr/sbin/scutil <<< "show State:
Users/ConsoleUser" | /usr/bin/awk '/Name :/ && ! /
loginwindow/ { print $3 }')

====
Check:
/usr/bin/sudo -u "$CURRENT_USER" /usr/bin/defaults
-currentHost read com.apple.Bluetooth
PrefKeyServicesEnabled
CIS Benchmark - Level 1
Show All
Audit
Jamf Pro Upload

Compliance Audit

CIS Benchmark - Lev...
macOS 15.0
14/12/2024

Passed: 27 Failed: 64

Result: 29.67%

macOS	34	⚠
Disable Power Nap		✓
Ensure Warn When Visiting A Fraudulent Website in Safari Is Enabled		⚠
Disable Root Login		⚠
Enforce Enrollment in Mobile Device Management		✓
Must Use an Approved Antivirus Program		✓
Ensure No World Writable Files Exist in the System Folder		✓
Disable iPhone Mirroring		⚠
Disable Automatic Opening of Safe Files in Safari		⚠
Enable Authenticated Root		✓
Ensure Advertising Privacy Protection in Safari Is Enabled		⚠

Save Run

os_root_disable

Title

Disable Root Login

Result

0

Expected Result

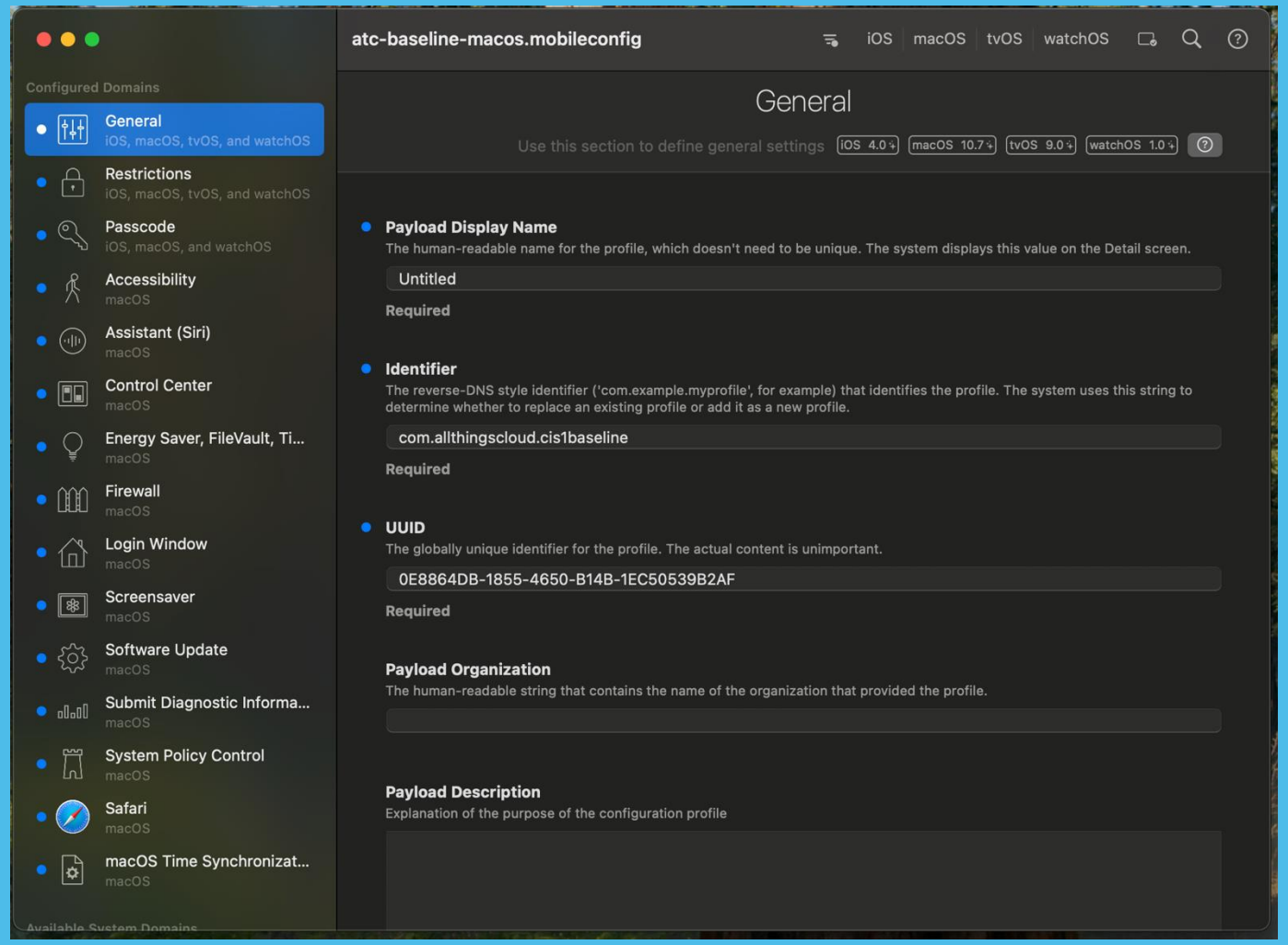
integer: 1

Description

To assure individual accountability a
unauthorized access, logging in as r
window _MUST_ be disabled.

The macOS system _MUST_ require
be authenticated with an individual a
prior to using a group authenticator,
administrator users _MUST_ never lo
root.

iMazing Profile Editor



Source: https://imazing.com/profile-editor

WORKPLACEDUDES

Common mistakes

Gatekeeper: Only configured with compliance policy!
You should **also configure restrictions** that do **not allow users to override Gatekeeper**

Platform SSO: Password sync?
Make sure your compliance policy (password settings) and configuration profiles (password settings) match!
Tip: Do not use compliance policies to enforce password settings. Instead, use configuration profile

Enrollment Profile: Await Final Configuration is not configured
You should **enable Await Final Configuration**

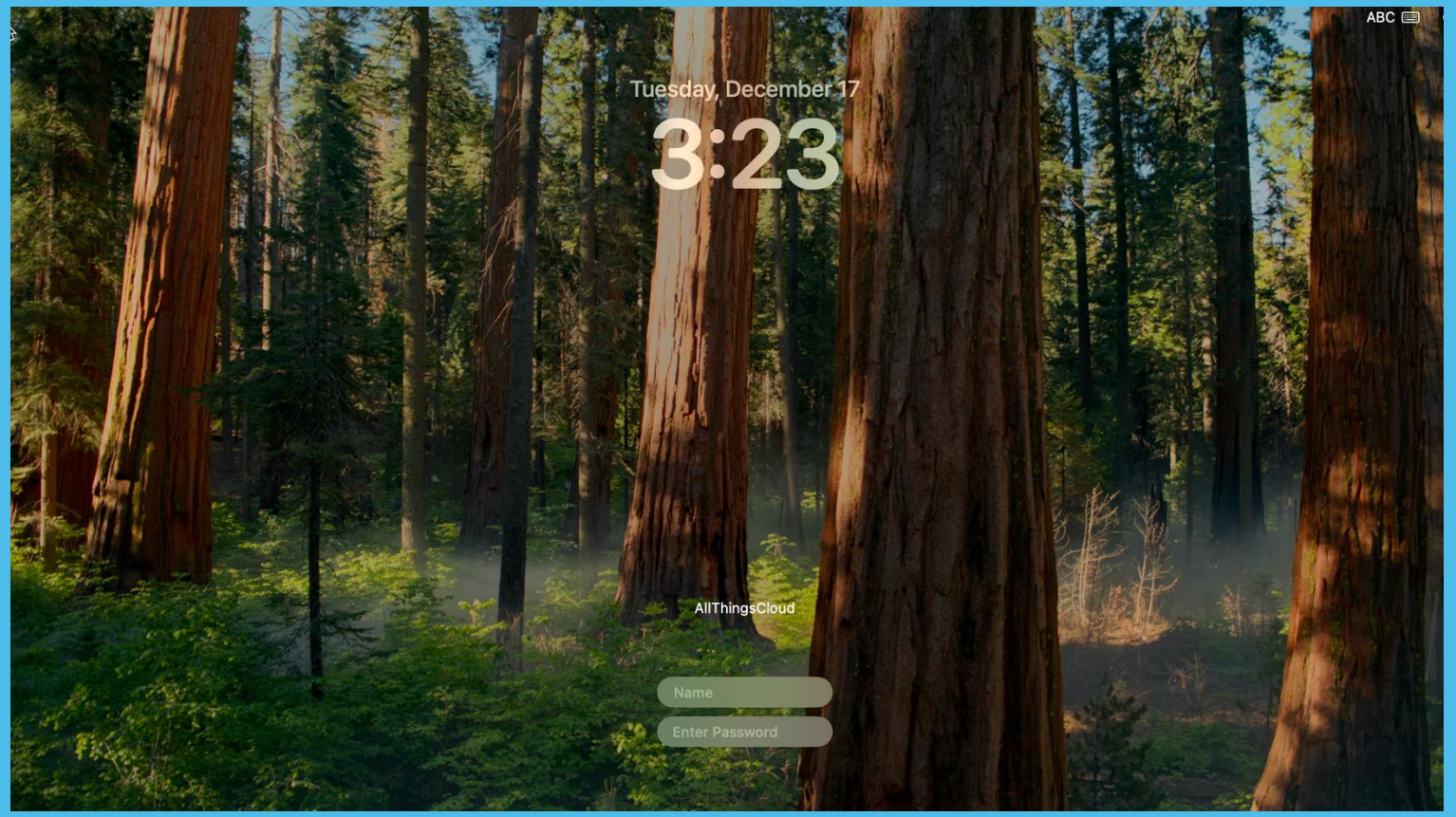
Human nature: We tend to finish to soon
You should take your time and don't rush things

Common mistakes

Login configuration: Do not show username config

You should inform users what to expect. They probably don't know their username!

IMPACT: When you do not show Username and Password, it will break PSSO



WORKPLACEDUDES

Common mistakes

Know what impact policies have:
Example: Ensure Wake for Network Access Is Disabled

This feature **allows the computer to take action when the user is not present** and the computer is in energy saving mode. This macOS feature is meant to **allow the computer to resume activity as needed regardless of physical security controls.**

This feature allows other users to be able to access your computer's shared resources, such as shared printers or Apple Music playlists, **even when your computer is in sleep mode.**

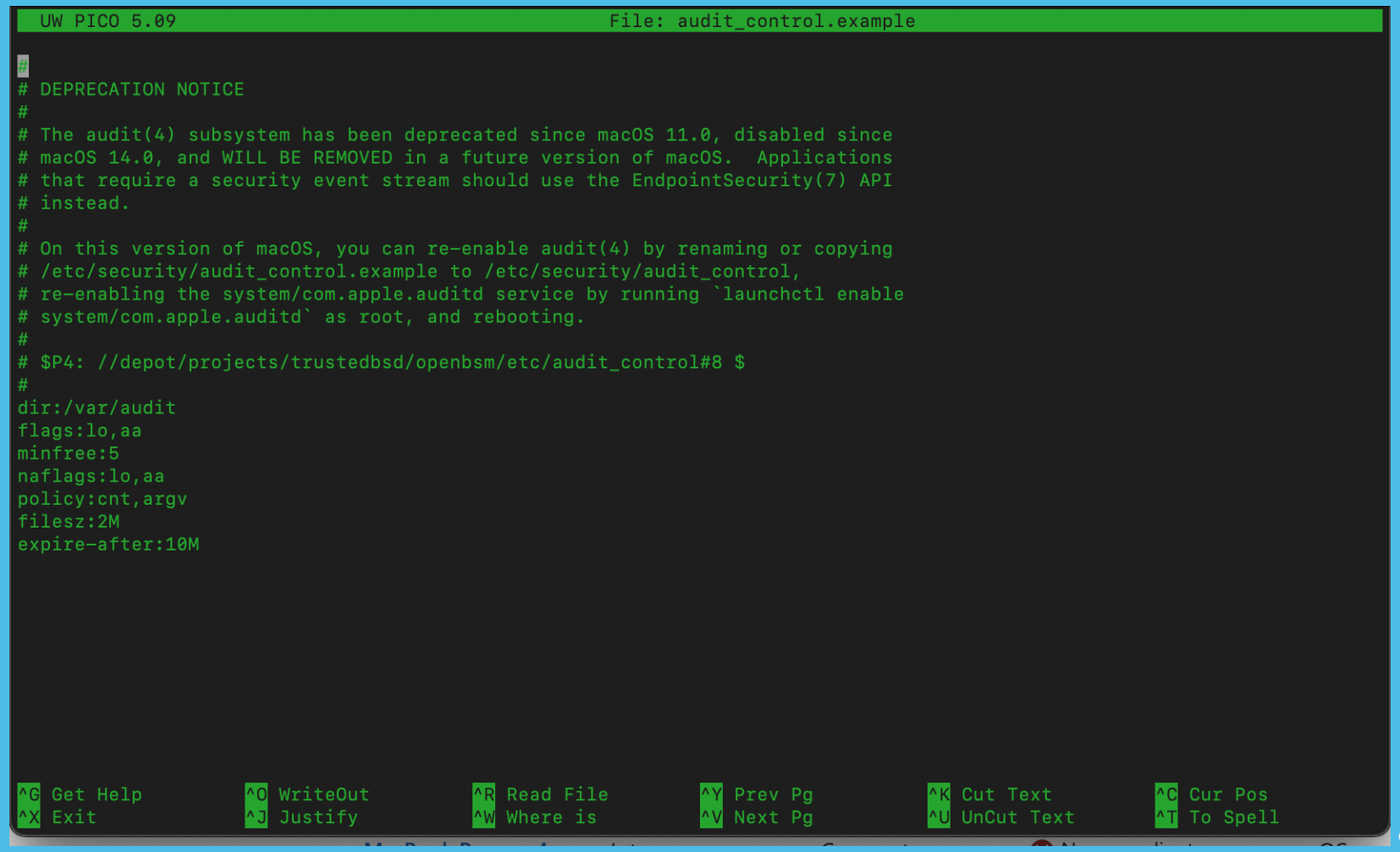
Rationale: Disabling this feature mitigates the risk of an attacker remotely waking the system and gaining access.

Impact: Management programs like **Apple Remote Desktop Administrator** use wake-on-LAN to connect with computers. If turned off, such management programs will not be able to wake a computer over the LAN. **If the wake-on-LAN feature is needed, do not turn off this feature.**

Turning off Wake for Network Access will also **not allow Find My to work when the computer is asleep**. It will also give this warning: **"You won't be able to locate, lock, or erase this Mac while it's asleep because Wake for network access is turned off."**

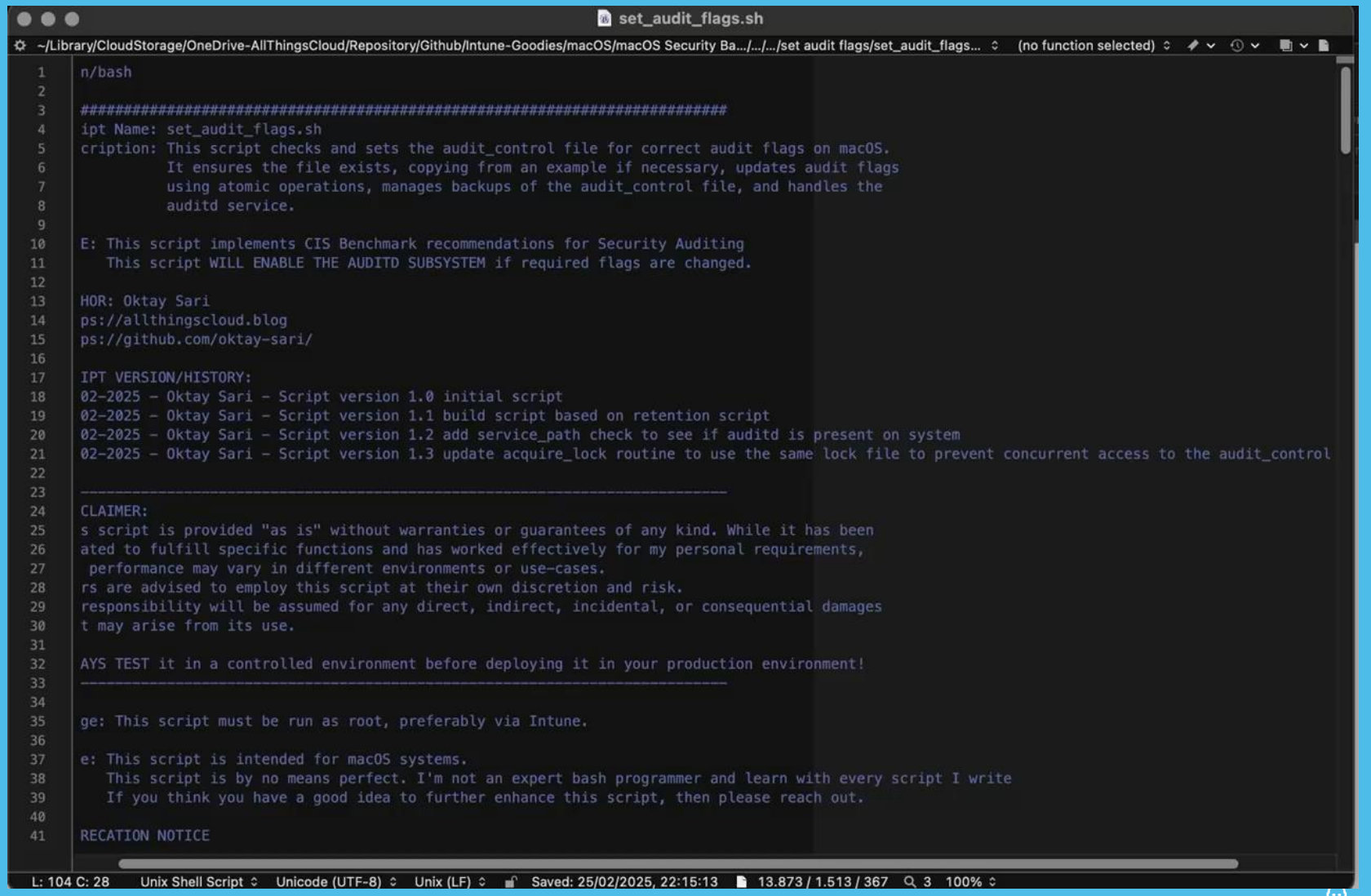
Common mistakes

How I Fort Knox'd Myself...



WORKPLACEDUDES

Lessons Learned



https://github.com/oktay-sari/Intune-Goodies

WORKPLACEDUDES

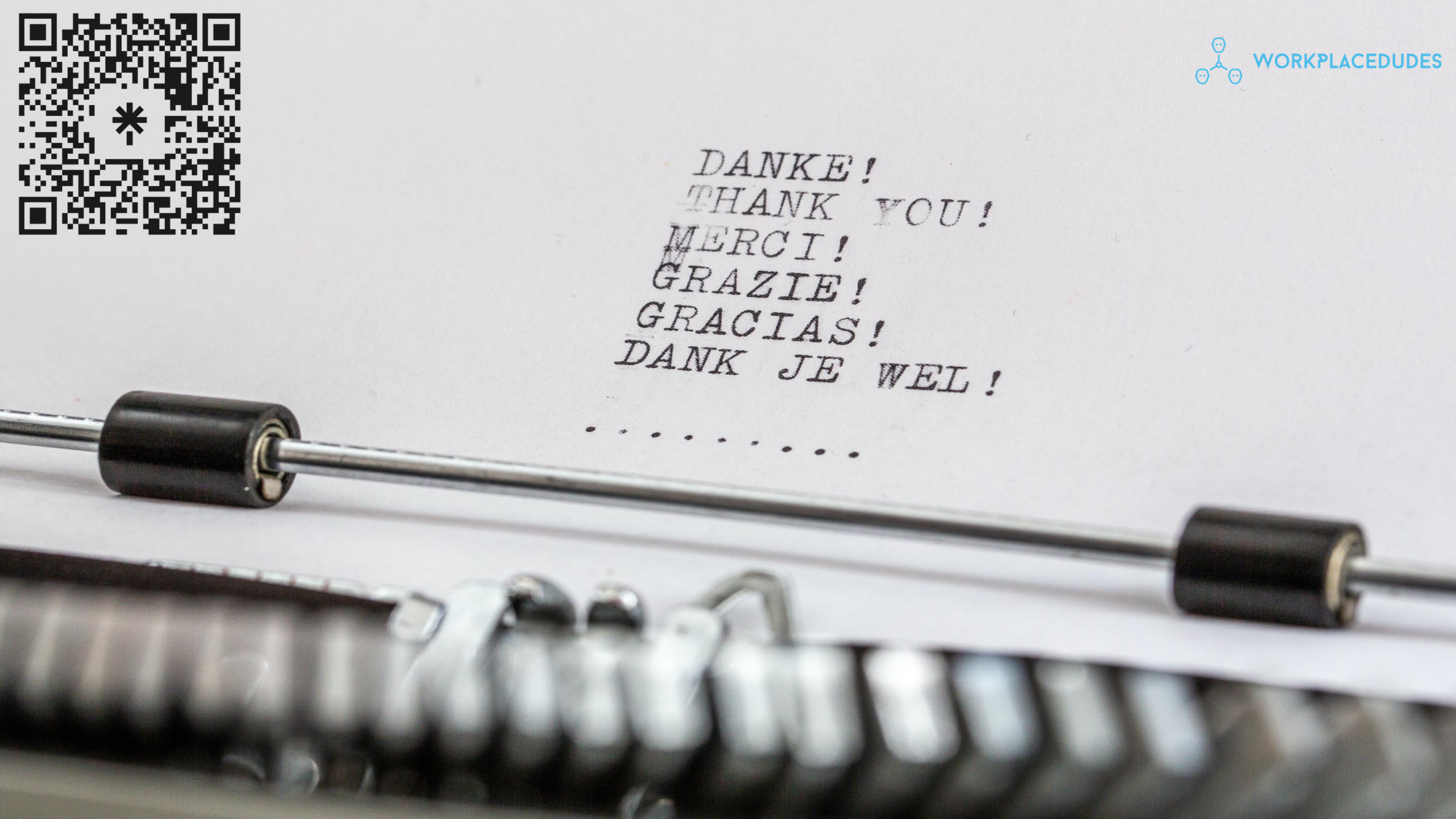
How to start?

Roadmap

Questions?

Resources

1. https://developer.apple.com/business/documentation/Configuration-Profile-Reference.pdf
2. https://en.wikipedia.org/wiki/MacOS_version_history
3. https://workbench.cisecurity.org/
4. https://github.com/oktay-sari/Intune-Goodies
5. https://trusted.jamf.com/docs/establishing-compliance-baselines
6. https://github.com/SkipToTheEndpoint/OpenIntuneBaseline
7. https://github.com/microsoft/shell-intune-samples/tree/master/macOS
8. https://github.com/Jamf-Concepts/jamf-compliance-editor/releases
9. https://www.linkedin.com/groups/13007354/ (Microsoft Mac Admins)
10. https://learn.microsoft.com/en-gb/mem/solutions/end-to-end-guides/macos-endpoints-get-started?tabs=esso
11. https://beta.apple.com/for-it


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