

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>



# 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

macOS - MDE - Accessibility Device configuration ✓ Succeeded

macOS - MDE - Background services Device configuration ✓ Succeeded

macOS - MDE - Bluetooth Device configuration ✓ Succeeded

macOS - MDE - Full Disk Access Device configuration ✓ Succeeded

macOS - MDE - MAU Update Config Settings Catalog ✓ Succeeded

macOS - MDE - Network Filter Device configuration ✓ Succeeded

macOS - MDE - Notifications

macOS - MDE - Onboard WDATP settings

macOS - MDE - tag

macOS - MDE Approved Kernel Extensions

Device Health  
Require system integrity protection Required

System Security  
Require encryption of data storage on device Enabled

Firewall  
Stealth Mode  
Allow apps downloaded from these locations Enabled

Mac App Store Apps

System Policy Control  
**System Policy Managed**  
Configure the System Policy Managed payload to configure the bypass the system policy.  
True  
Disable Override

Full Disk Encryption  
**FileVault**  
Configure the FileVault payload to manage FileVault disk On

# 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 (Will 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

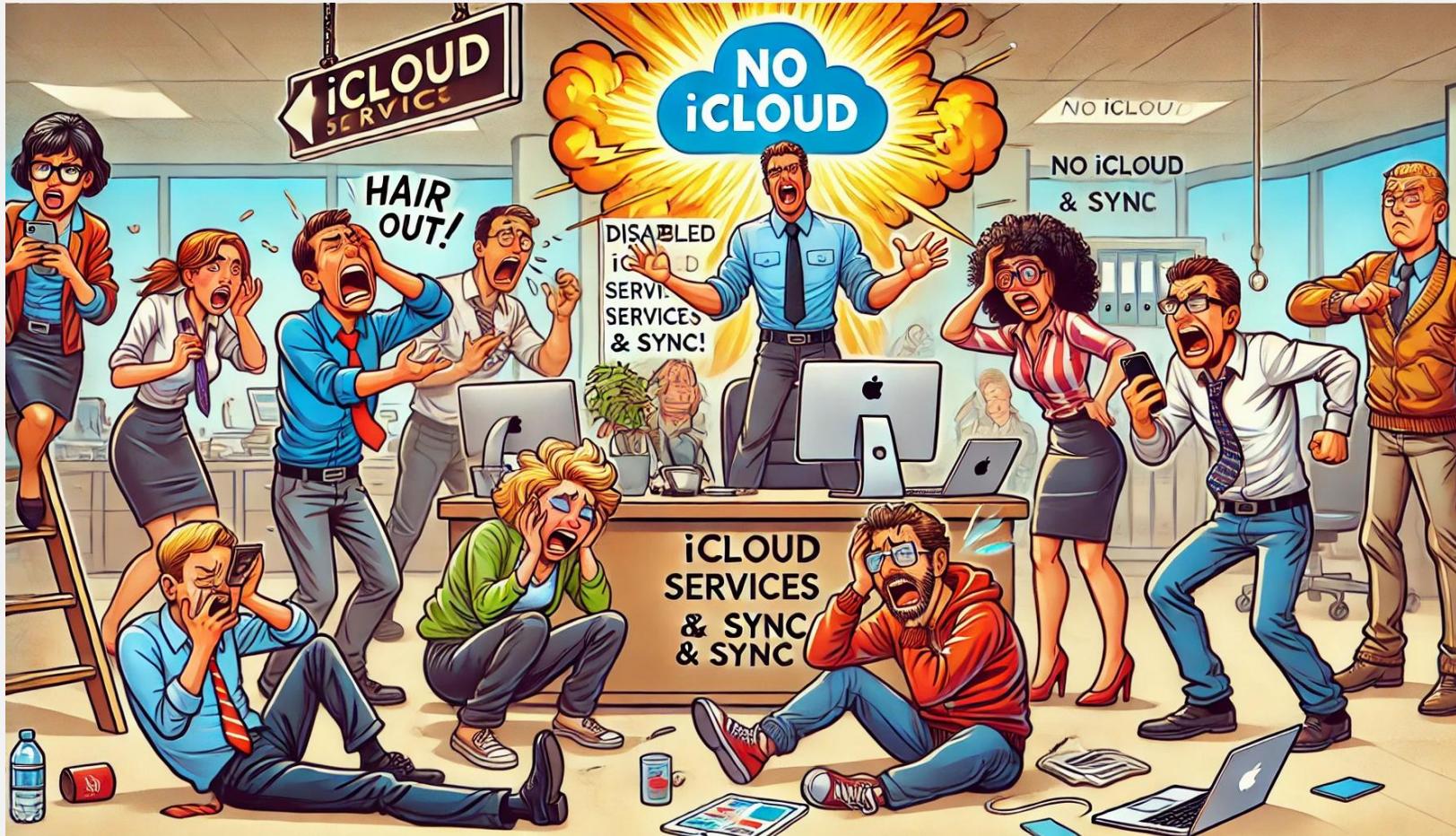
## Disable Sharing and Saving Passwords

- Disable Password Auto Fill (will 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	
Hardening - CIS_L2 - Set Login Window Banner	macOS	
Hardening - 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 access	macOS	Yes
Hardening - CIS_L2 - audit apps using location service	macOS	Yes
Hardening - CIS_L1 - Show all filename extensions	macOS	Yes
Hardening - CIS_L1 - Set Sudo Timeout Period to Zero	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 Retention	macOS	No
Hardening - CIS_L1 - Enable Sudo Logging	macOS	Yes
Hardening - CIS_L1 - Enable Apple Mobile File Integration	macOS	Yes
Hardening - CIS_L1 - Disable Root	macOS	Yes
Hardening - CIS_L1 - Disable Remote Login	macOS	
Hardening - CIS_L1 - Disable SSH Server	macOS	



WORKPLACEDUDES

# Settings Catalog & Custom Profiles

macOS - Hardening - CIS\_L2 - Secure Hot Corners

macOS - Hardening - CIS\_L2 - Power settings

macOS - Hardening - CIS\_L2 - Notifications and Focus

macOS - Hardening - CIS\_L2 - Disable Siri completely

macOS - Hardening - CIS\_L2 - Disable iCloud Document and Desktop Sync

macOS - Hardening - CIS\_L2 - Disable Content Caching

macOS - Hardening - CIS\_L2 - Baseline Security Configuration

macOS - Hardening - CIS\_L1 - TimeServer

macOS - Hardening - CIS\_L1 - Terminal Full Disk Access

macOS - Hardening - CIS\_L1 - Software update

macOS - Hardening - CIS\_L1 - Show Wifi and Bluetooth status

macOS - Hardening - CIS\_L1 - Screensaver password

Hardening - CIS\_L1 - Safari Security and Privacy

Hardening - CIS\_L1 - Privacy Restrictions

CIS\_L1 - Login Window configuration

REPLACED UDES

# Custom attributes

- Enrollment
- Manage devices
- Configuration
- Compliance
- Scripts
- Manage updates
- macOS updates
- Organize devices
- Device clean-up rules
- Custom attributes for macOS

Attribute name ↓	Attribute type
macOS - Report apps with full disk access	String
macOS - Report apps using location services	String
macOS - Fetch Edge Version	String
macOS - Fetch Defender Version	String
macOS - Check XProtect	String
macOS - Check Updates are automatically downloaded	String
macOS - Check Sudo Timeout Period	String
macOS - Check Root Account Status	String
macOS - Check NFS Server is disabled	String
macOS - Check Google Chrome version	String
macOS - Check Gatekeeper status	String
macOS - Check diagnostic data submission	String
macOS - Check Defender PUA status	String

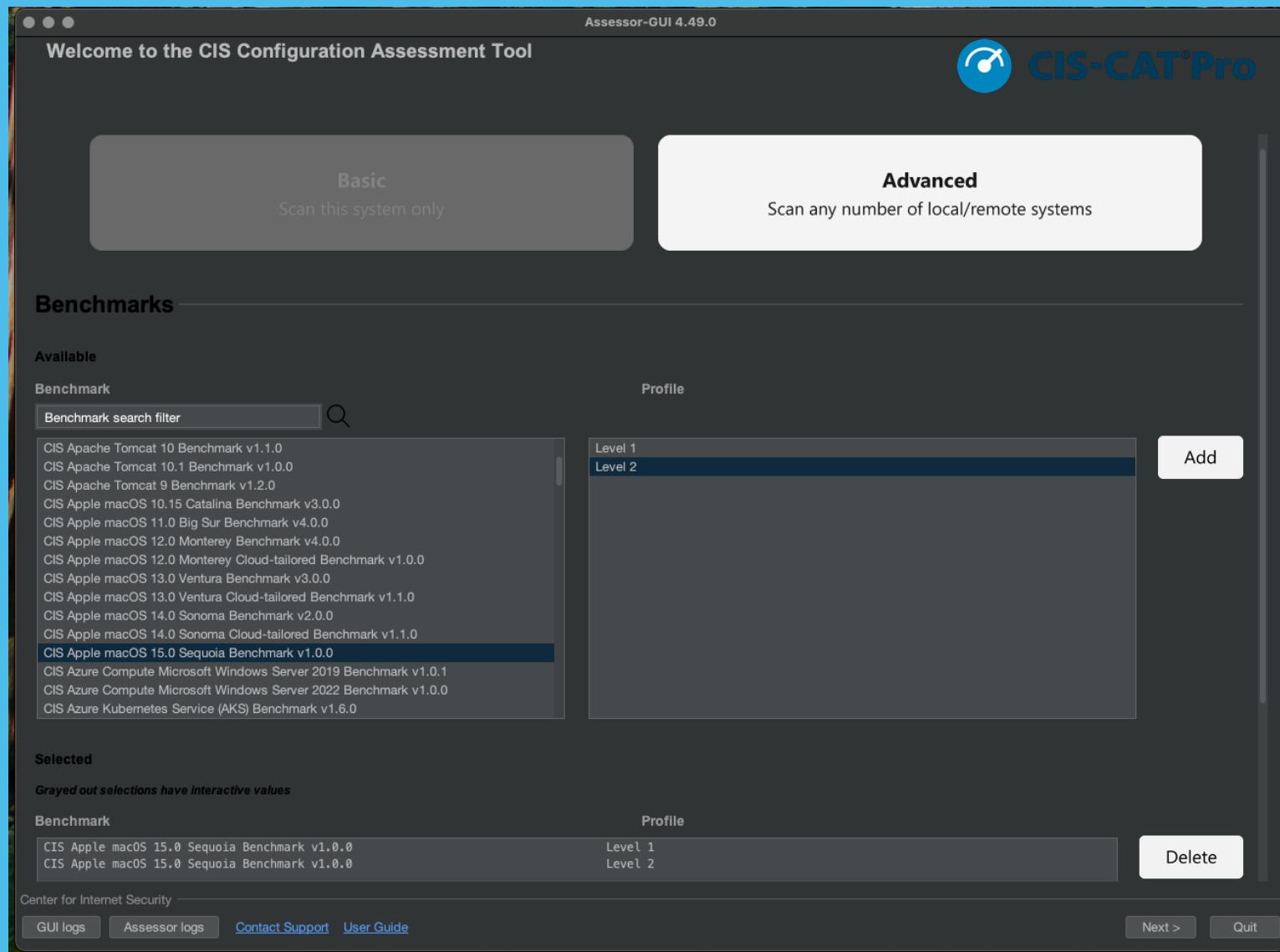
Authorized Apps: ( "Maps (com.appleMaps)", "com.microsoft.teams2.modulehost (No app display name found)", "Calendar (com.apple.iCal)", "Microsoft Teams (com.microsoft.teams2)", "Home (com.apple.Home)", "WiFiman (com.ubnt.wifiman)", "Jabra Direct (com.jabra.directonline)", "Reminders (com.apple.reminders)", "Microsoft Edge (com.microsoft.edgemac)", "com.flexibits.fantastical2.mac (No app display name found)", "Logi Options+ (com.logi.optionsplus)", "Microsoft Outlook (com.microsoft.Outlook)" )

Authorized Apps: ( "Maps (com.appleMaps)" ... 2025-02-2...



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](https://github.com/usnistgov/macOS_security)

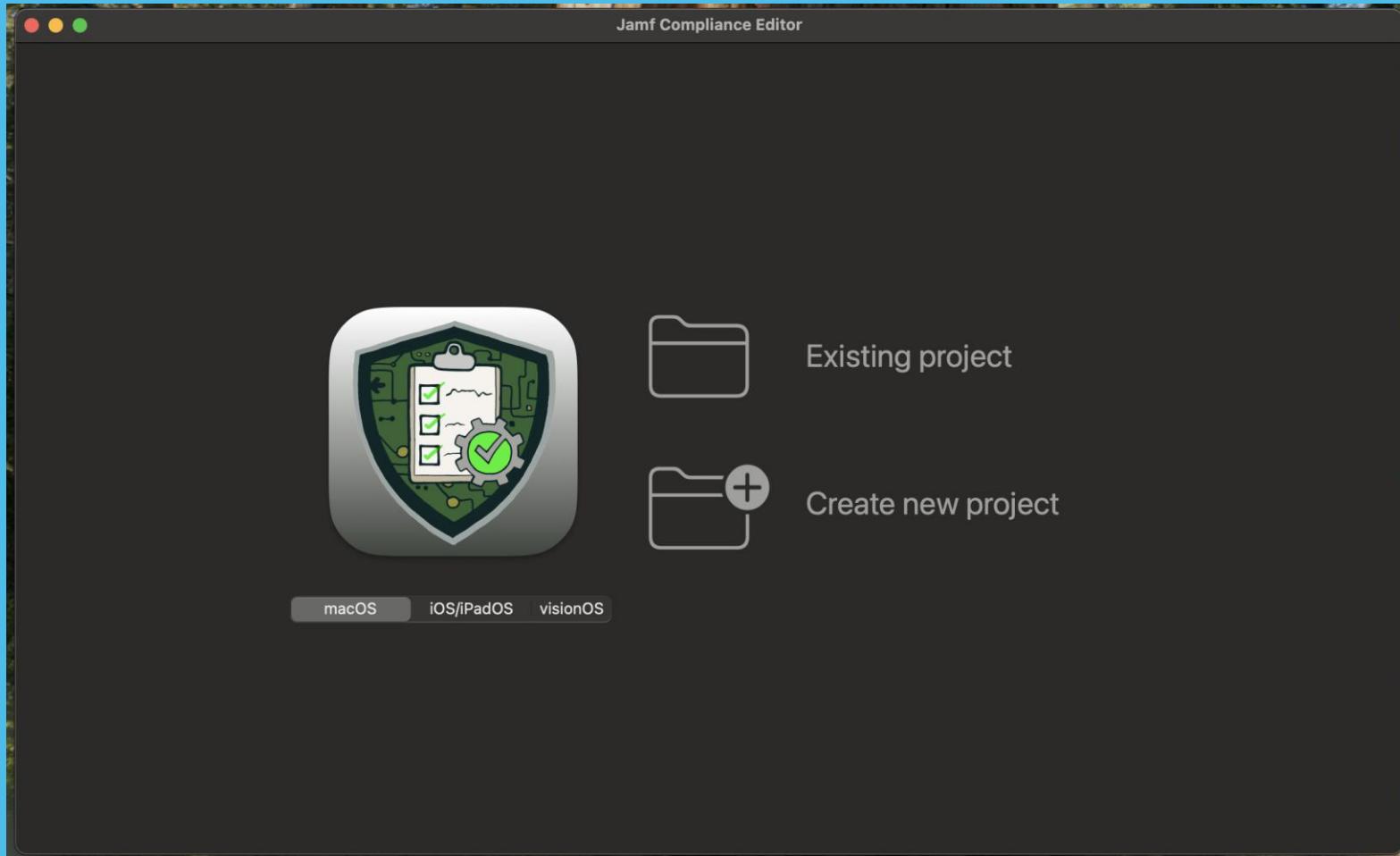
 Search this guide

[Table of Contents !\[\]\(3cf084882489248c66b41ee5d191c91e\_img.jpg\)](#)

# macOS Security Compliance Project

The [macOS Security Compliance Project \(mSCP\)](#) is an [open source](#) effort to provide a programmatic approach to generating security guidance. The project can be used to output customized documentation, scripts (logging and remediation), configuration profiles, and an audit checklist based on the baseline used. It is authoritative through [NIST Special Publication 800-219, Automated Secure Configuration Guidance](#) from the macOS Security Compliance Project (mSCP).

# Jamf Compliance Editor



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

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. To 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.BluetoothPrefKeyServicesEnabled
```



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

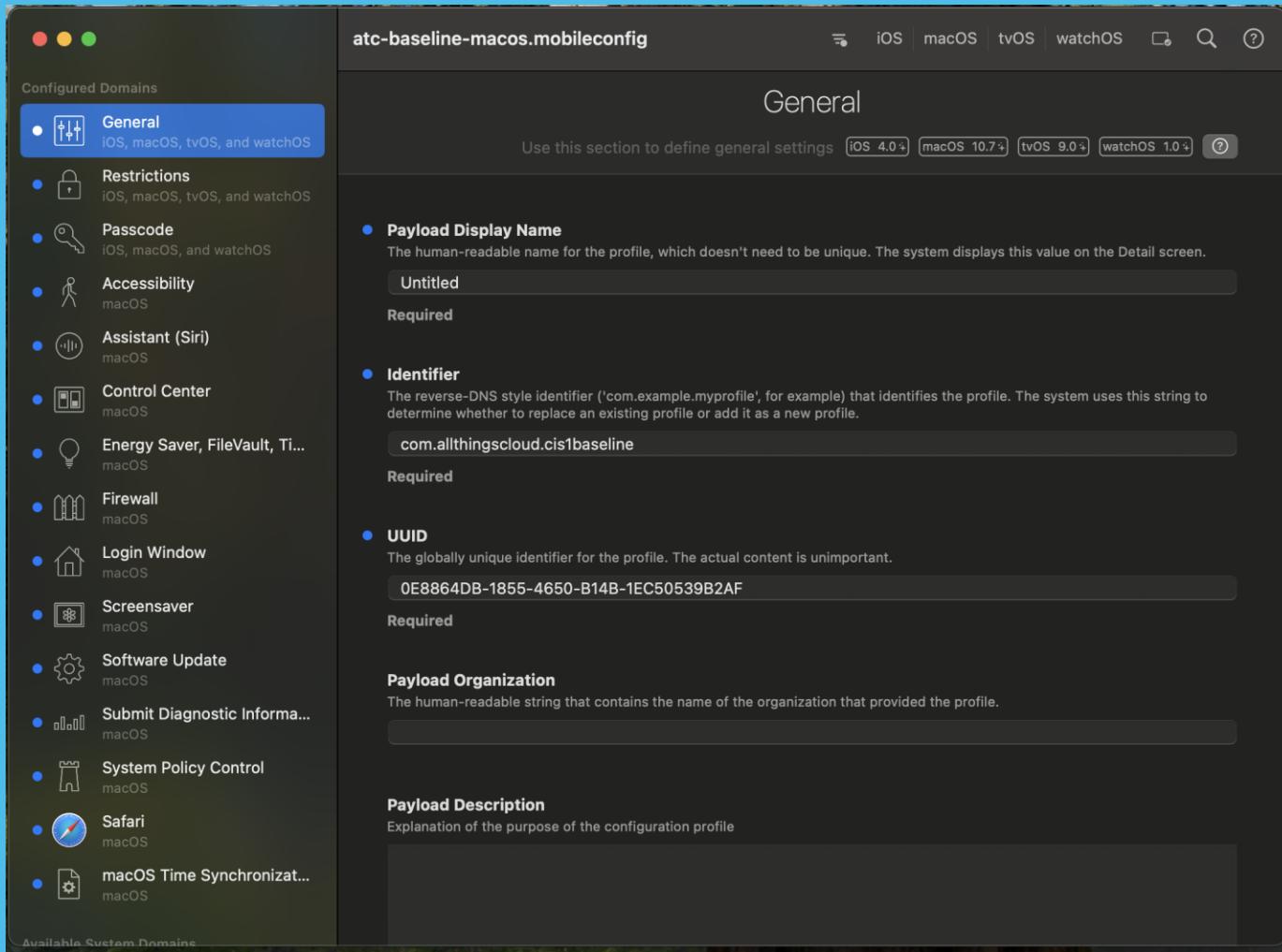
integer: 1

Description

To assure individual accountability and prevent unauthorized access, logging in as root \_MUST\_ be disabled.

The macOS system \_MUST\_ require authentication with an individual password prior to using a group authenticator, and administrator users \_MUST\_ never log in as 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 too soon

You should take your time and don't rush things



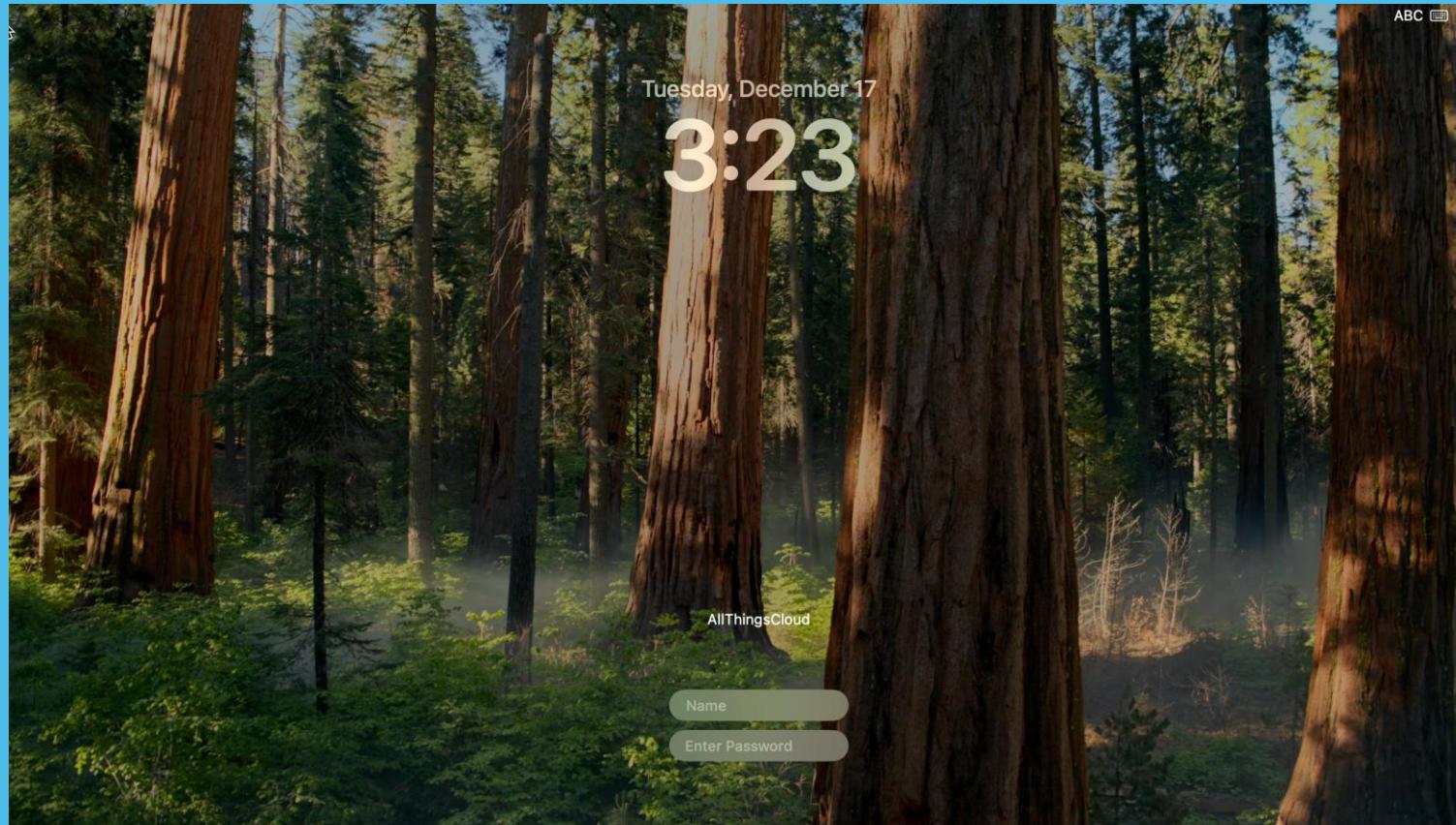
WORKPLACEDUDES

# 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...

```
UW PICO 5.09                               File: audit_control.example

#
# DEPRECATION NOTICE
#
# The audit(4) subsystem has been deprecated since macOS 11.0, disabled since
# macOS 14.0, and WILL BE REMOVED in a future version of macOS. Applications
# that require a security event stream should use the EndpointSecurity(7) API
# instead.
#
# On this version of macOS, you can re-enable audit(4) by renaming or copying
# /etc/security/audit_control.example to /etc/security/audit_control,
# re-enabling the system/com.apple.auditd service by running `launchctl enable
# system/com.apple.auditd` as root, and rebooting.
#
# $P4: //depot/projects/trustedbsd/openbsm/etc/audit_control#8 $
#
dir:/var/audit
flags:lo,aa
minfree:5
naflags:lo,aa
policy:cnt,argv
filesz:2M
expire-after:10M
```

^G Get Help  
^X Exit

^O WriteOut  
^J Justify

^R Read File  
^W Where is

^Y Prev Pg  
^V Next Pg

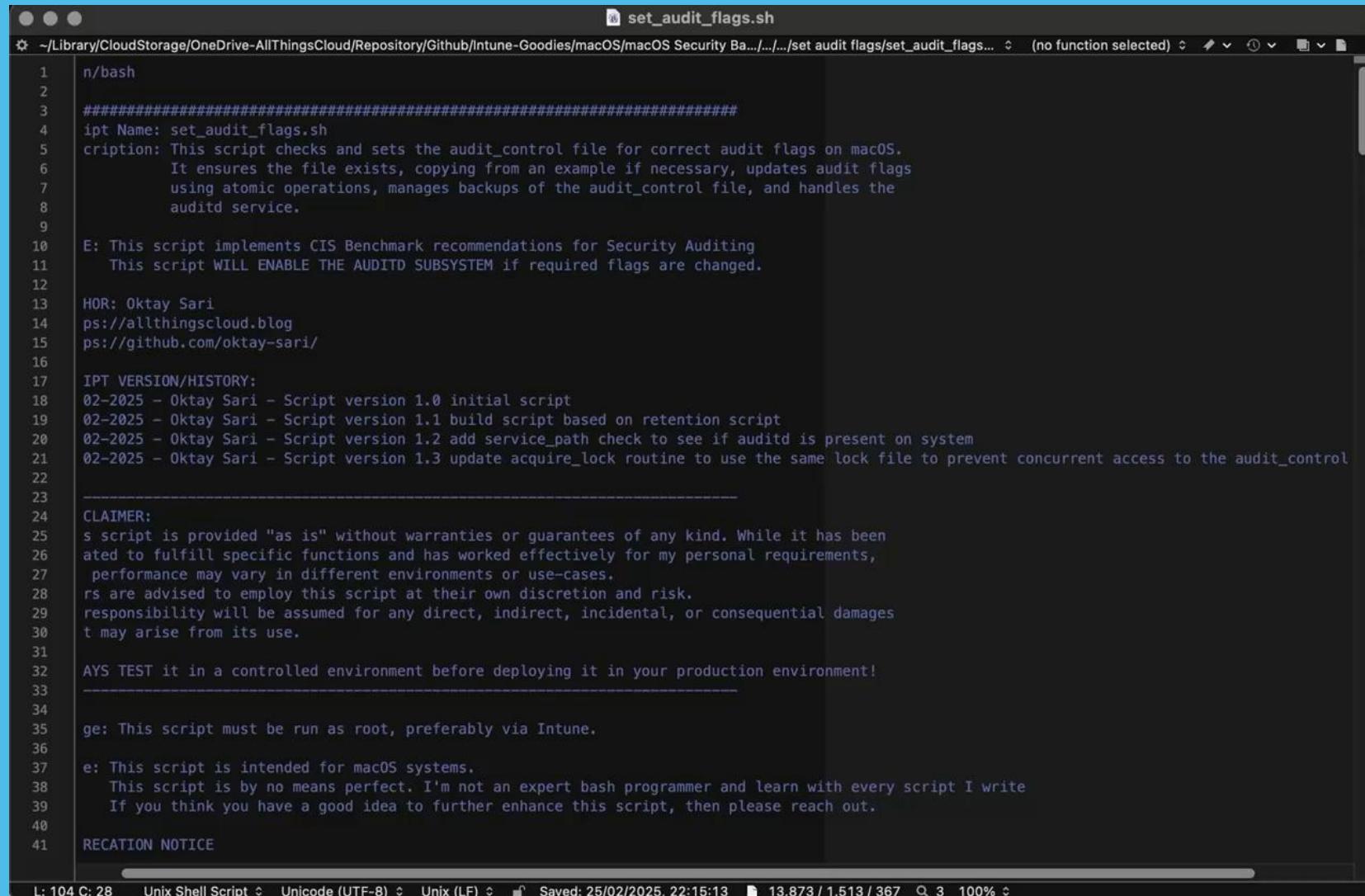
^K Cut Text  
^U UnCut Text

^C Cur Pos  
^T To Spell



WORKPLACEDUDES

# Lessons Learned



The screenshot shows a terminal window with the title bar "set\_audit\_flags.sh". The path in the title bar is "/Library/CloudStorage/OneDrive-AllThingsCloud/Repository/Github/Intune-Goodies/macOS/macOS Security Ba.../.../set audit flags/set\_audit\_flags...". The status bar at the bottom shows "L: 104 C: 28 Unix Shell Script ◊ Unicode (UTF-8) ◊ Unix (LF) ◊ Saved: 25/02/2025, 22:15:13 13.873 / 1.513 / 367 ⌂ 3 100% ◊". The script content is as follows:

```
1 n/bash
2
3 #####
4 #!/bin/bash
5 # Description: This script checks and sets the audit_control file for correct audit flags on macOS.
6 # It ensures the file exists, copying from an example if necessary, updates audit flags
7 # using atomic operations, manages backups of the audit_control file, and handles the
8 # auditd service.
9
10 E: This script implements CIS Benchmark recommendations for Security Auditing
11     This script WILL ENABLE THE AUDITD SUBSYSTEM if required flags are changed.
12
13 HOR: Oktay Sari
14 ps://allthingscloud.blog
15 ps://github.com/oktay-sari/
16
17 IPT VERSION/HISTORY:
18 02-2025 - Oktay Sari - Script version 1.0 initial script
19 02-2025 - Oktay Sari - Script version 1.1 build script based on retention script
20 02-2025 - Oktay Sari - Script version 1.2 add service_path check to see if auditd is present on system
21 02-2025 - Oktay Sari - Script version 1.3 update acquire_lock routine to use the same lock file to prevent concurrent access to the audit_control
22
23
24 CLAIMER:
25 This script is provided "as is" without warranties or guarantees of any kind. While it has been
26 created to fulfill specific functions and has worked effectively for my personal requirements,
27 performance may vary in different environments or use-cases.
28 Users are advised to employ this script at their own discretion and risk.
29 No responsibility will be assumed for any direct, indirect, incidental, or consequential damages
30 that may arise from its use.
31
32 AYS TEST it in a controlled environment before deploying it in your production environment!
33
34
35 ge: This script must be run as root, preferably via Intune.
36
37 e: This script is intended for macOS systems.
38     This script is by no means perfect. I'm not an expert bash programmer and learn with every script I write
39     If you think you have a good idea to further enhance this script, then please reach out.
40
41 RECAUTION NOTICE
```

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

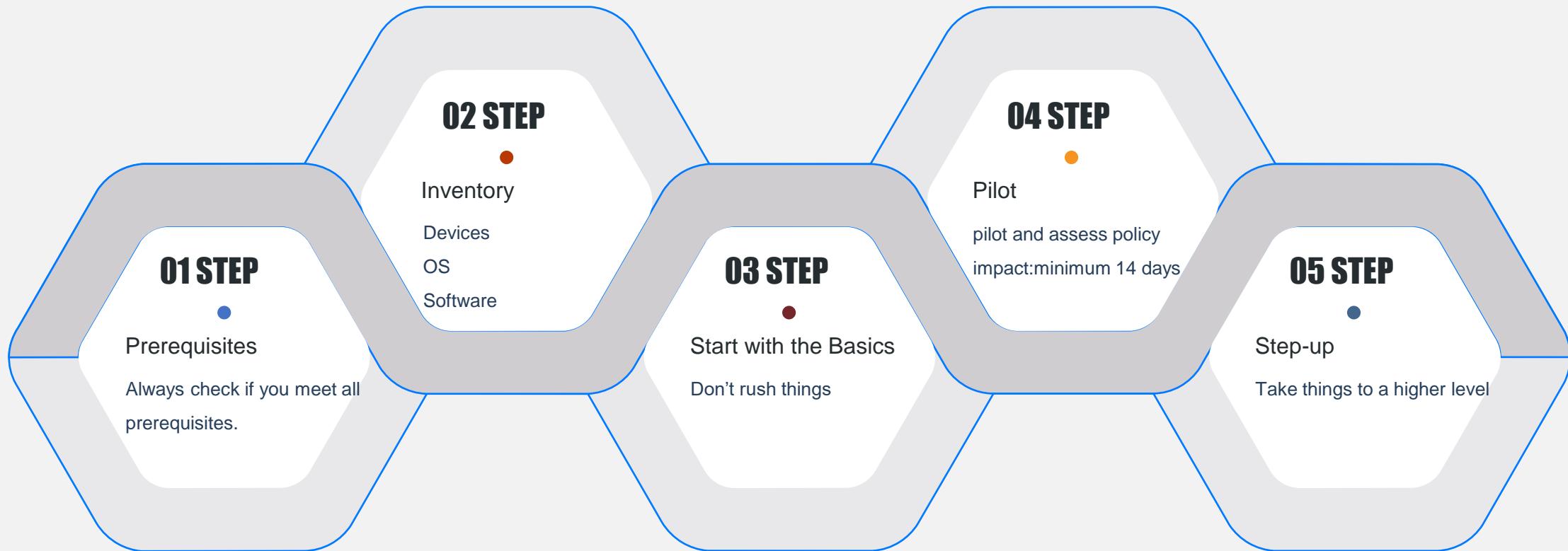


WORKPLACE DUDES

# How to start?



REPLACEDUDES



# Questions?



# Resources

1. <https://developer.apple.com/business/documentation/Configuration-Profile-Reference.pdf>
2. [https://en.wikipedia.org/wiki/MacOS\\_version\\_history](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!

.....