



AllThingsCloud

SIMPLIFY

INTUNE | SECURITY | M365 | AZURE

OLD WAYS
WONT OPEN
NEW
DOORS

**macOS Security with Intune;
From Basics to Bulletproof**

You will never be ready, just start

Oktay Sari

Modern Workplace Consultant



Focus

Microsoft Intune and all things Security

Hobbies

Hiking, Woodworking, RC planes & heli

My Blog

<https://allthingscloud.blog>

Awards



Contact

 [@oktay_sari](https://twitter.com/oktay_sari)

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



You will never be ready, just start



Focus

Microsoft Intune and all things **Security**

Hobbies

Hiking, Woodworking, RC planes & heli

My Blog

<https://allthingscloud.blog>

Awards



Contact

 [@oktay_sari](https://twitter.com/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

Start with

The Basics



The Basics

1

Compliance policies

2

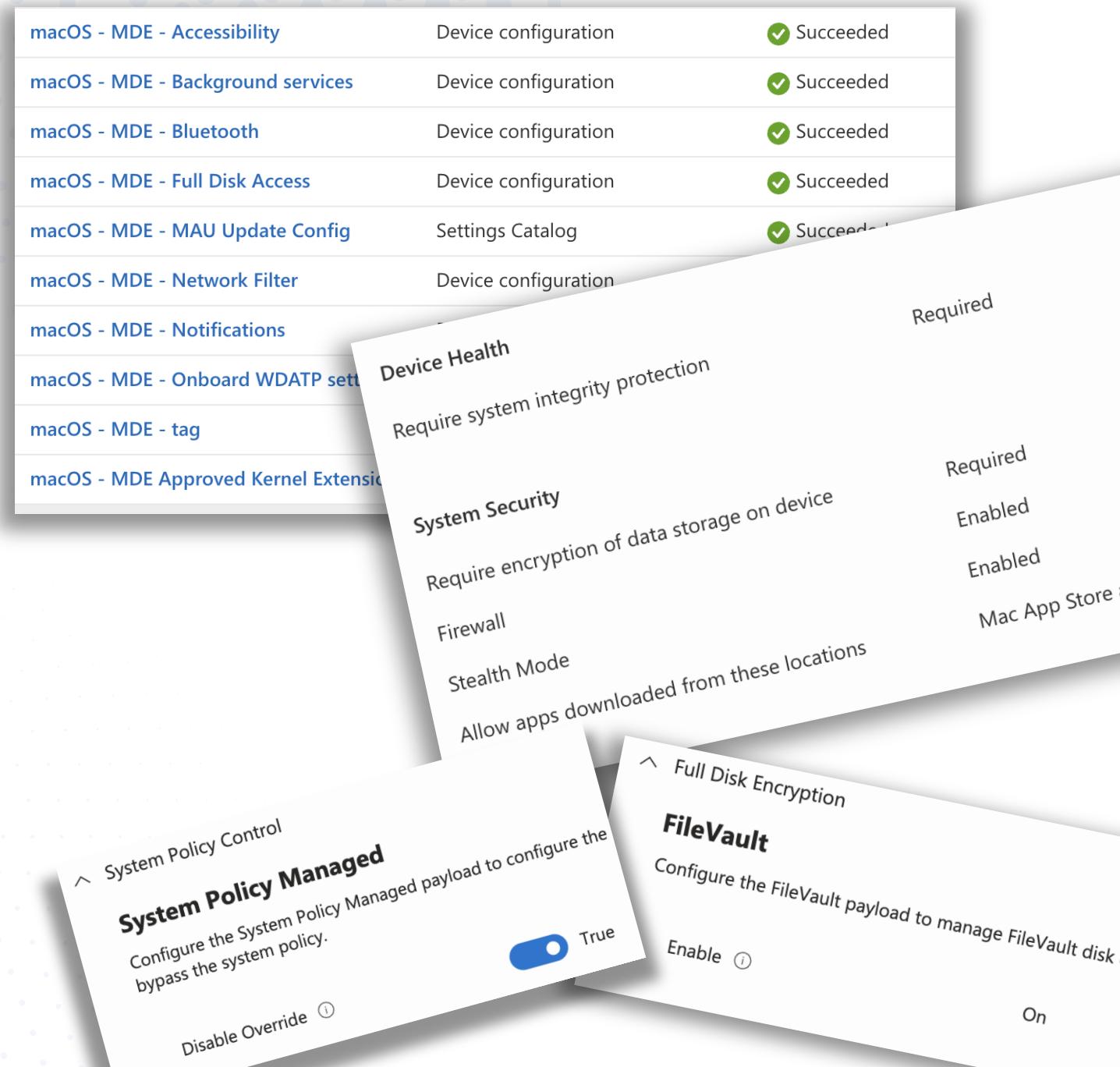
Device restrictions and features

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

System Security
Require encryption of data storage on device

FileVault
Configure the FileVault payload to manage FileVault disk

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

The Must Haves



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)**
- Always show username and password window (vs list all users)**
- 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

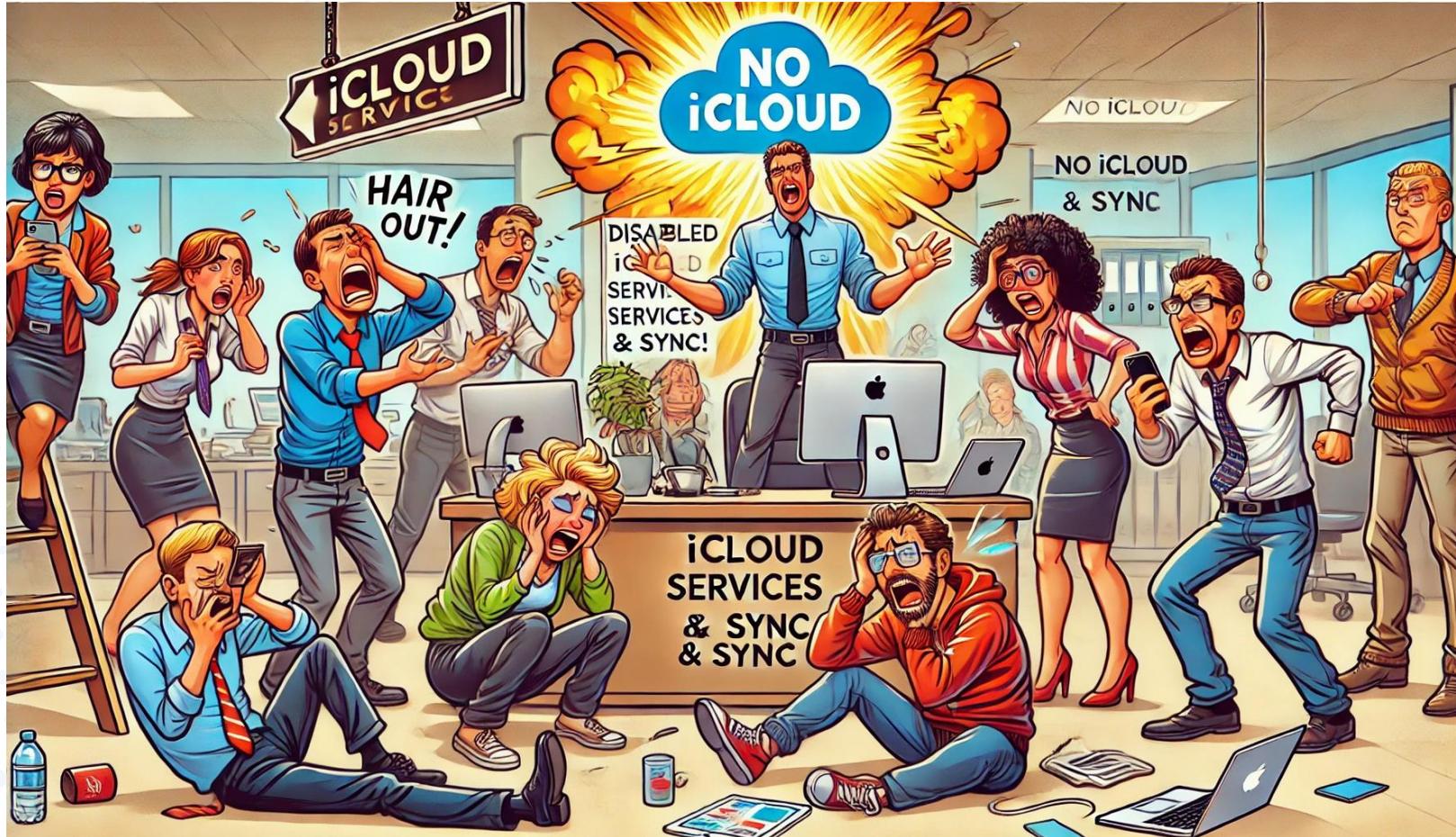
Disable Sharing and Saving Passwords

- Disable Password Auto Fill**
- Disable Password Proximity Request**
- Disable Password Sharing**

If you want to drive everyone nuts...

4

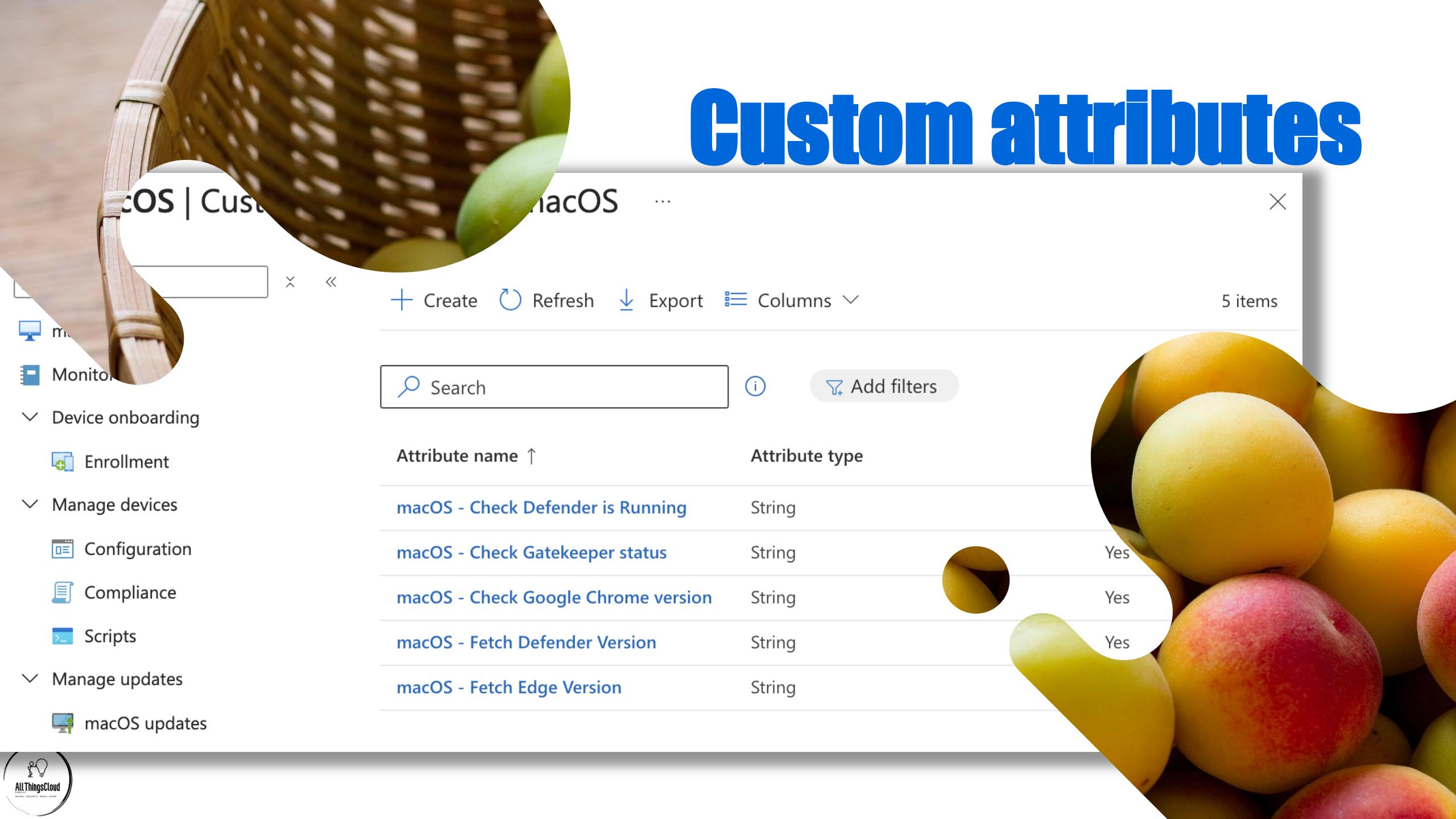
Disable all iCloud services and syncs



Advanced Security configurations



Custom attributes



A collage of images illustrating custom attributes. The central image is a screenshot of a macOS search interface titled 'macOS | Custom attributes'. It shows a list of five items with columns for 'Attribute name' and 'Attribute type'. The items are:

Attribute name	Attribute type
macOS - Check Defender is Running	String
macOS - Check Gatekeeper status	String
macOS - Check Google Chrome version	String
macOS - Fetch Defender Version	String
macOS - Fetch Edge Version	String

On the left, a sidebar shows navigation options like 'macOS', 'Monitoring', 'Device onboarding', 'Enrollment', 'Manage devices', 'Configuration', 'Compliance', 'Scripts', 'Manage updates', and 'macOS updates'. The right side of the collage features a close-up of ripe peaches.

MacOS Scripts



A screenshot of a software interface for managing MacOS scripts. The left sidebar shows navigation options: Devices, Configuration, Compliance, Scripts (selected), Manage updates, and Organize devices. The main area displays a table of scripts with columns for Script name, Platform, and Assigned. The table lists 12 scripts, all of which are assigned to the 'Yes' category. The scripts are: Rename MacOS, macOS - Hardening - CIS_lvl1 - Show all filename extensions, macOS - Hardening - CIS_lvl1 - Secure User's Home Folders, macOS - Hardening - CIS_lvl1 - Enable Apple Mobile File Integrity, macOS - Hardening - CIS_lvl1 - Disable NFS Server, macOS - Hardening - CIS_lvl1 - Disable HTTP Server, macOS - Hardening - CIS_lvl1 - Disable Guest Access to Shared Fo, macOS - Hardening - CIS_lvl1 - Disable File Sharing, macOS - Hardening - CIS_lvl1 - Delete Guest Home Folder, macOS - Hardening - CIS_lvl1 - Controlled Audit records, macOS - Hardening - CIS_lvl1 - Administrator Account Restriction:, and macOS - Hardening - CIS_lvl1 - Admin Password for system wide s.

Script name ↓	Platform	Assigned
Rename MacOS	macOS	Yes
macOS - Hardening - CIS_lvl1 - Show all filename extensions	macOS	Yes
macOS - Hardening - CIS_lvl1 - Secure User's Home Folders	macOS	Yes
macOS - Hardening - CIS_lvl1 - Enable Apple Mobile File Integrity	macOS	Yes
macOS - Hardening - CIS_lvl1 - Disable NFS Server	macOS	Yes
macOS - Hardening - CIS_lvl1 - Disable HTTP Server	macOS	Yes
macOS - Hardening - CIS_lvl1 - Disable Guest Access to Shared Fo	macOS	Yes
macOS - Hardening - CIS_lvl1 - Disable File Sharing	macOS	Yes
macOS - Hardening - CIS_lvl1 - Delete Guest Home Folder	macOS	Yes
macOS - Hardening - CIS_lvl1 - Controlled Audit records	macOS	Yes
macOS - Hardening - CIS_lvl1 - Administrator Account Restriction:	macOS	Yes
macOS - Hardening - CIS_lvl1 - Admin Password for system wide s	macOS	Yes



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

Apple Platform Certifications

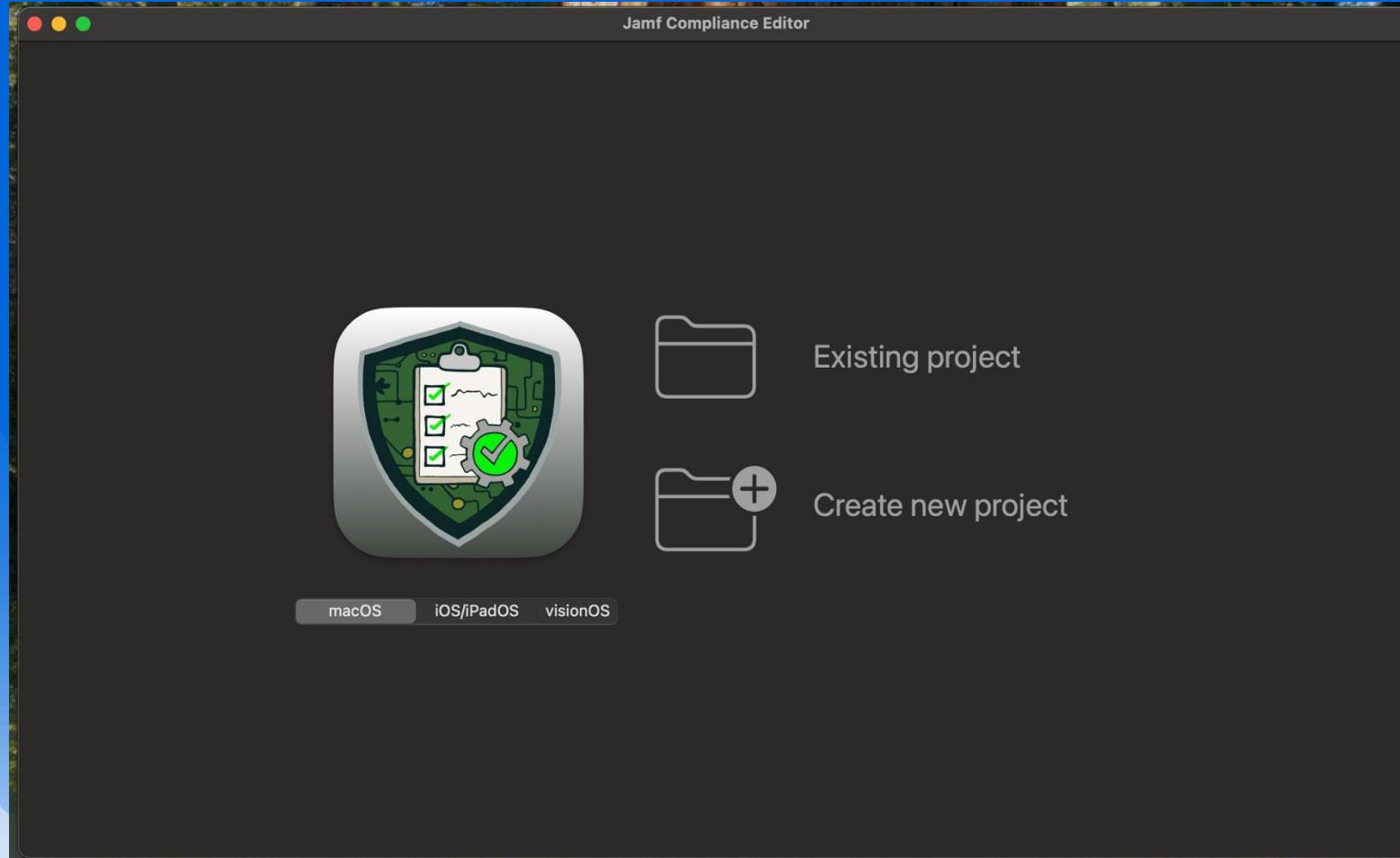
[Communities](#) Search this guide[Table of Contents !\[\]\(dfc59eaff22f8544bedb238cca58d143_img.jpg\)](#)

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).

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>



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]

====

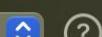
```
CURRENT_USER=$( /usr/sbin/scutil <<< "show State:Users/ConsoleUser" | /usr/bin/awk '/Name :/ && !/loginwindow/ { print $3 }' )
```

====

====

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 account prior to using a group authenticator, and administrator users _MUST_ never log in as root.

Source: <https://beta.apple.com/for-it>



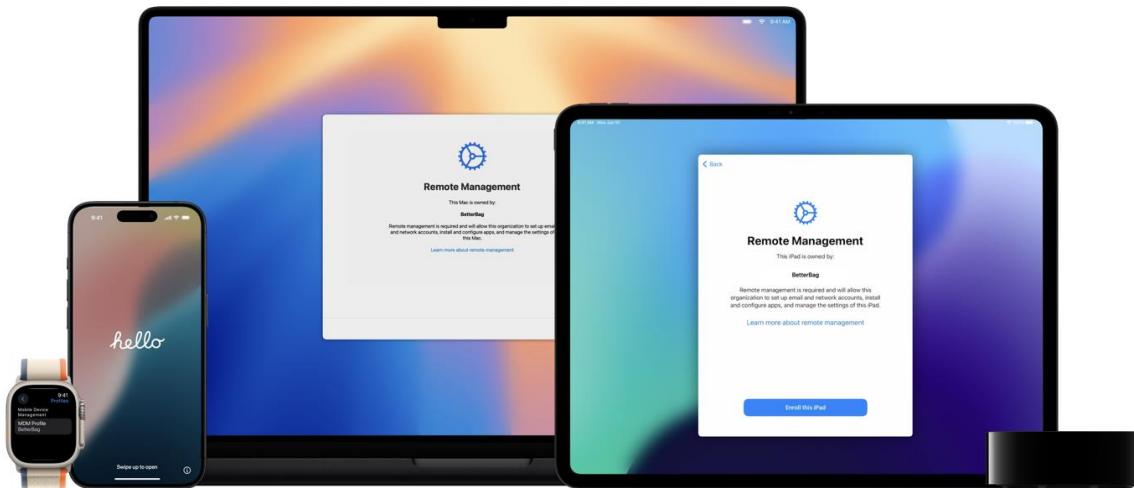
Mac Evaluation Utility

Version
4.6.4

Released
November 22, 2024

[Mac Evaluation Utility 4.6.4 Release Notes](#)

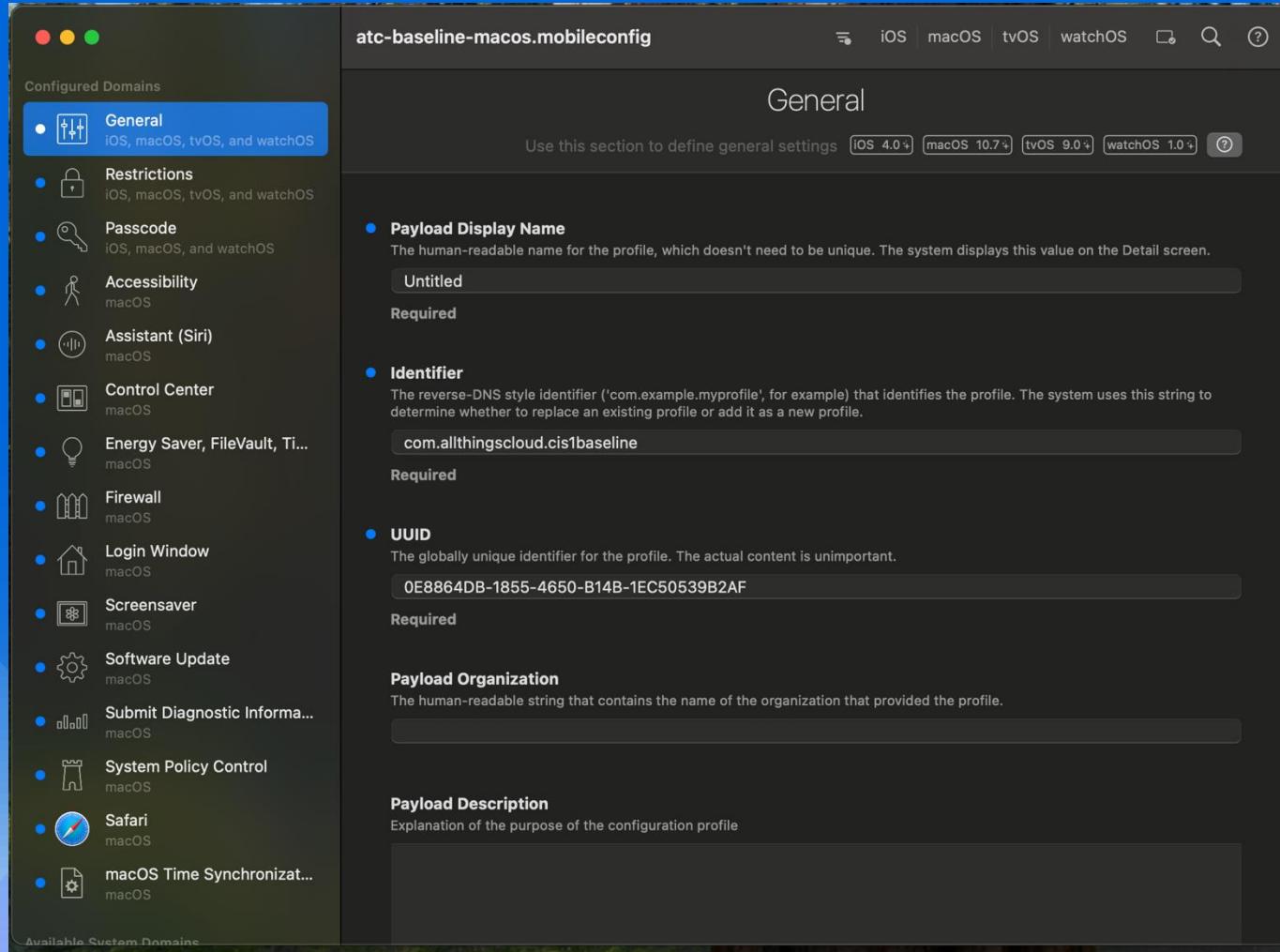
[Mac Evaluation Utility 4.6.4](#)



AppleSeed for IT

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

iMazing Profile Editor



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

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**

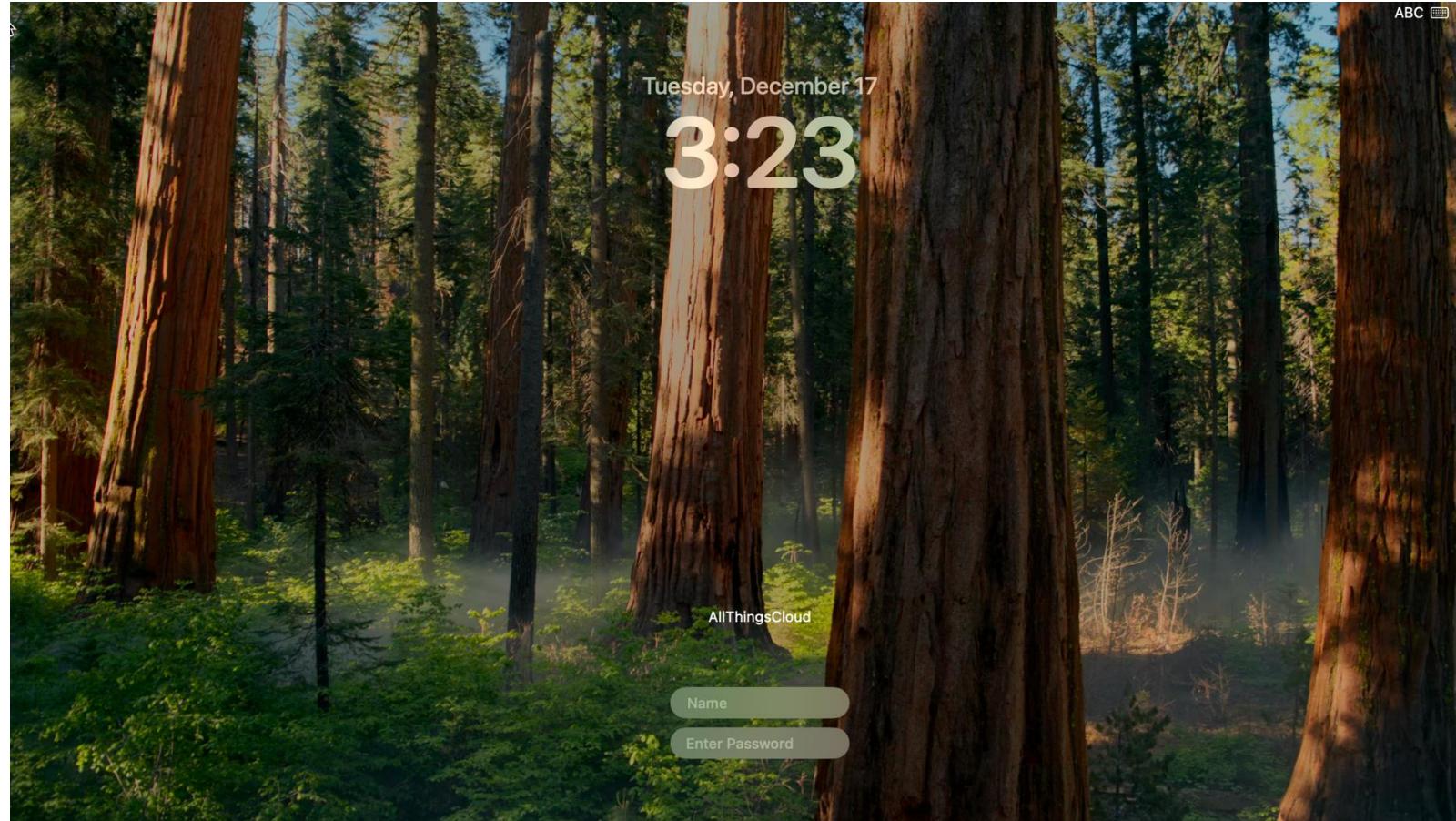
Human nature: We tend to finish to soon

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!



Common mistakes

Know what impact policies have:

Example: Ensure Wake for Network Access Is Disabled

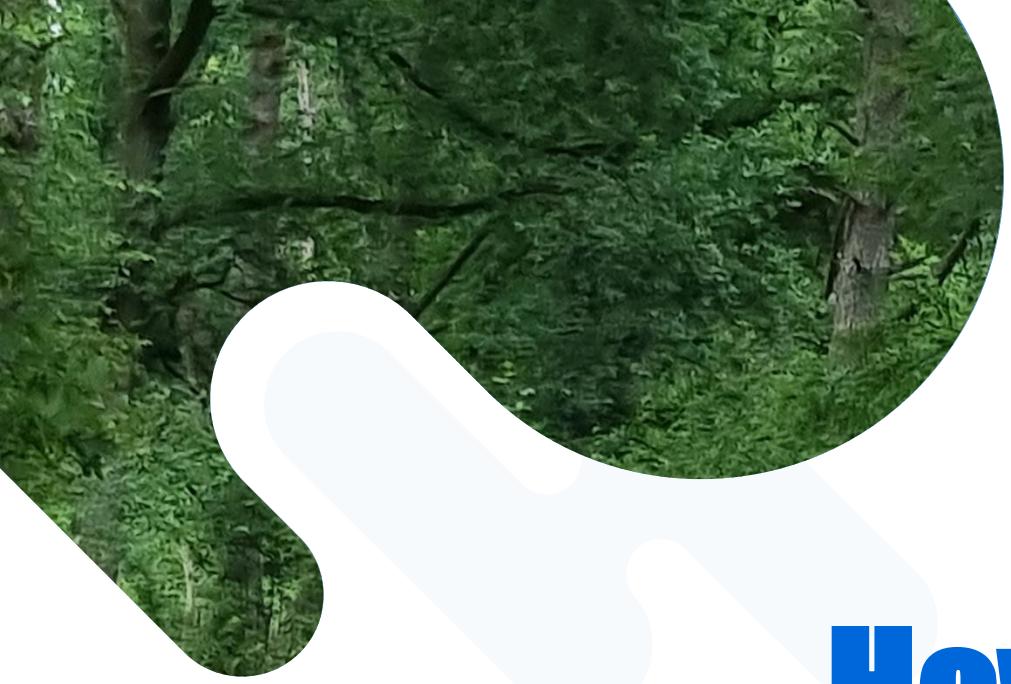
This feature **allows the computer to take action when the user is not present** and the computer is in energy saving mode. This macOS feature is meant to **allow the computer to resume activity as needed regardless of physical security controls**.

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."**

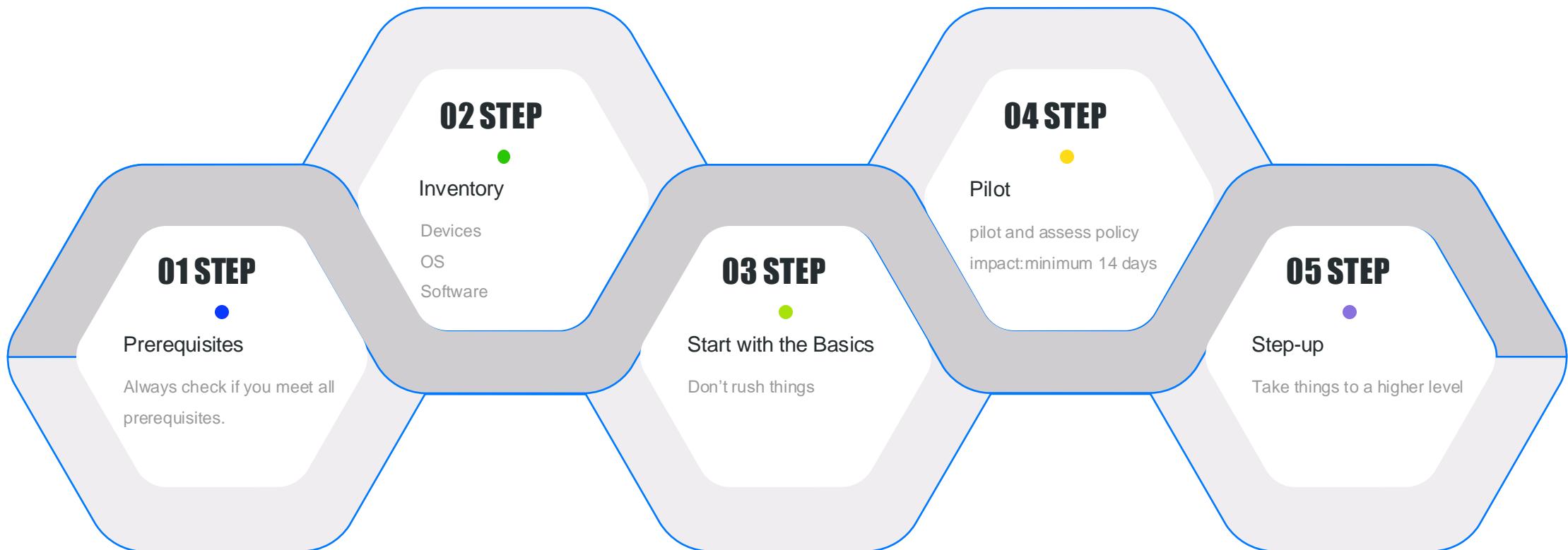


How to start?



Roadmap

Cloud



Questions?





Thank You



AllThingsCloud

SIMPPLY

INTUNE | SECURITY | M365 | AZURE

Happy holidays
&
have a great 2025!



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://www.tenable.com/audits/CIS_Apple_macOS_15.0_Sequoia_v1.0.0_L2
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>