

# Forward-Looking Statement Disclaimer

This presentation may contain forward-looking statements under applicable securities laws. All statements other than statements of historical facts are forward-looking statement. Forward-looking statements are based on information available to Jamf at the time they are made and provide Jamf's current expectations and projections about its financial condition, results, plans, objectives, future performance and business. You can identify forward-looking statements by the fact that they do not relate strictly to historical or current facts. Forward-looking statements may include words such as "anticipate", "estimate", "project", "plan", "intend", "believe", "may", "will", "should", "can have", "likely" and other terms of similar meaning in connection with any discussion of timing or nature of future operating or financial performance or other events.

All statements we make about our estimated and projected costs, expenses, cash flows, growth rates and financial results are forward-looking statements. In addition, our plans and objectives for future operations, growth initiatives, product plans and product strategies are forward-looking statements.

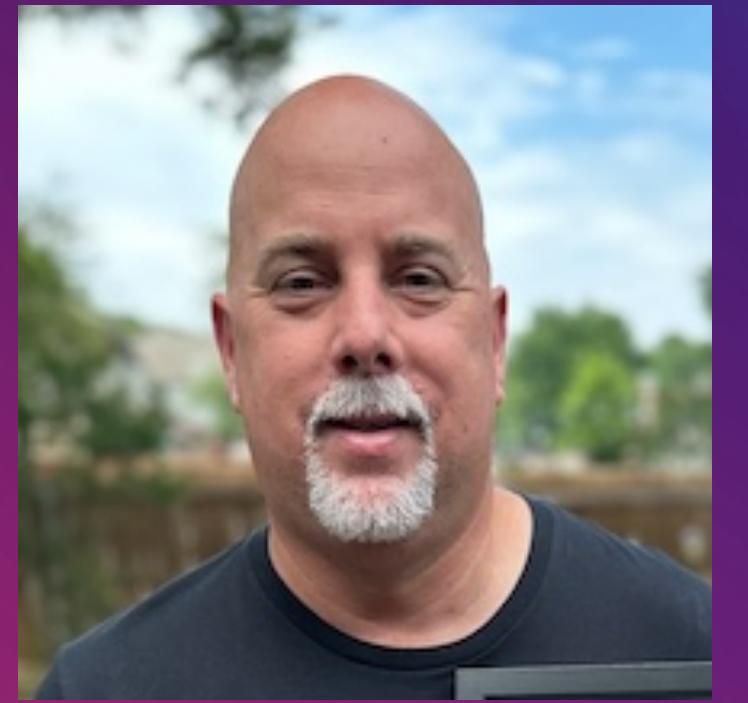
There are various factors, risks and uncertainties that may cause Jamf's actual results to differ materially from those that we expected in any forward-looking statements. These factors and risks are set forth in the documents Jamf files with U.S. Securities and Exchange Commission (SEC). These documents are publicly available on the SEC's website at [www.sec.gov](http://www.sec.gov) or on Jamf's website at [ir.jamf.com](http://ir.jamf.com).

Forward-looking statements are not guarantees of future performance and you should not place undue reliance on them. Jamf is under no obligation to update any forward-looking statements made in this presentation, except as required by law.





# Extension Attributes: A year in the life of an admin



# Steve Wood

Jamf



# Lee Collik

Jamf





# Remember Jill?





“ Remember, hacking is more than just a crime. It's a survival trait. “

- Razor

# Software Update Compliance

?

<b>Required OS Version:</b>	14.6.2
Actively Exploited CVEs:	False
Current OS Version:	14.6.1
Hours Remaining To Update:	6
Deferred Count:	2

Your device requires a security update  
A friendly reminder from your local IT team

Your device will restart during this update  
Updates can take around 30 minutes to complete

**Update Device**

**Important Notes**

A fully up-to-date device is required to ensure that IT can accurately protect your device.

If you do not update your device, you may lose access to some items necessary for your day-to-day tasks.

To begin the update, simply click on the **Update Device** button and follow the provided steps.

Defer



# Software Update Compliance

```
#!/bin/sh

osProductVersion=$( /usr/bin/sw_vers -productVersion )

case "${osProductVersion}" in

10*)
    echo "<result>N/A; macOS ${osProductVersion}</result>"
;;
11* | 12* | 13* | 14*)
    loggedInUser=$( /bin/echo "show State:/Users/ConsoleUser" | /usr/sbin/scutil | /usr/bin/awk '/Name :/ { print $3 }' )
    requiredOS=$( /usr/bin/defaults read /Users/"${loggedInUser}"/Library/Preferences/com.github.macadmins.Nudge.plist requiredMinimumOSVersion )
    logEntries=$( /usr/bin/grep com.github.macadmins.Nudge /private/var/log/Nudge.log | /usr/bin/tail -5 | /usr/bin/awk '{ split($2, split_time, "."); $2 = split_time[1]; print }' | /usr/bin/cut -d ' ' -f -2,6- )
;;
esac
```

<https://github.com/dan-snelson/Nudge-Post-install/blob/main/EA-Nudge-Logs.sh>



# Software Update Compliance

Nudge Log:

Required OS: 14.6.1

2024-08-19 09:00:00 Assessed Model ID found in SOFA Entry: true

2024-08-19 09:00:00 enforceMinorUpdates: true

2024-08-19 09:00:00 Current operating system (14.6.1) is greater than or equal to required operating system (14.6.1)

2024-08-19 09:00:00 Device is fully updated

2024-08-19 09:00:00 Nudge is terminating due to condition met

Nudge Log:

Required OS: 14.6.2

2024-09-24 09:04:05 Nudge is currently the frontmostApplication

2024-09-24 09:05:05 Nudge is currently the frontmostApplication

2024-09-24 09:05:09 Defaulting actionButtonPath to /System/Library/CoreServices/Software  
Update.app.

2024-09-24 09:05:09 User clicked updateDevice

2024-09-24 09:05:09 Attempting to remove forced blur



# Jamf Compliance Editor





# Jamf Compliance Editor

Compliance - 1. Version:

org.cis\_lvl2.audit.plist

```
#!/bin/bash

result=$(/bin/ls -l /Library/Preferences | /usr/bin/grep "org.*.audit.plist" | /usr/bin/awk '{print $NF}')

if [[ ! -z "$result" ]]; then
    count=$(echo "$result" | /usr/bin/wc -l | /usr/bin/xargs)
    if [[ "$count" != 1 ]]; then
        result="Multiple Baselines Set"
    fi
else result="No Baseline Set"
fi
echo "<result>$result</result>"
```



# Jamf Compliance Editor

Compliance - 2. Failed Results Count: 0

```
#!/bin/bash

audit=$(ls -l /Library/Preferences | /usr/bin/grep 'org.*.audit.plist' | /usr/bin/awk
'{print $NF}')
EXEMPT_RULES=()
FAILED_RULES=()

if [[ ! -z "$audit" ]]; then

    count=$(echo "$audit" | /usr/bin/wc -l | /usr/bin/xargs)
    if [[ "$count" == 1 ]]; then

        # Get the Exemptions
        exemptfile="/Library/Managed Preferences/${audit}"
        if [[ ! -e "$exemptfile" ]]; then
```



# Jamf Compliance Editor

Compliance - 3. Failed Result List:

**system\_settings\_siri\_listen\_disable**

```
#!/bin/bash

audit=$(/bin/ls -l /Library/Preferences | /usr/bin/grep 'org.*.audit.plist' | /usr/bin/
awk '{print $NF}')
FAILED_RULES=()
if [[ ! -z "$audit" ]]; then

    count=$(echo "$audit" | /usr/bin/wc -l | /usr/bin/xargs)
    if [[ "$count" == 1 ]]; then
        auditfile="/Library/Preferences/${audit}"

        rules=$((/usr/libexec/PlistBuddy -c "print :" "${auditfile}" | /usr/bin/awk '/
Dict/ { print $1 }'))
    else
        for rule in ${rules[*]}; do
```



# Jamf Compliance Editor

Compliance - 4. Exemptions:

`system_settings_siri_listen_disable`

```
#!/bin/bash

audit=$(/bin/ls -l /Library/Preferences | /usr/bin/grep 'org.*.audit.plist' | /usr/bin/awk
'{print $NF}')
EXEMPT_RULES=()

if [[ ! -z "$audit" ]]; then

    count=$(echo "$audit" | /usr/bin/wc -l | /usr/bin/xargs)
    if [[ "$count" == 1 ]]; then
        auditfile="/Library/Managed Preferences/${audit}"
        if [[ ! -e "$auditfile" ]];then
            auditfile="/Library/Preferences/${audit}"
        fi

        rules=($(/usr/libexec/PlistBuddy -c "print :" "${auditfile}" | /usr/bin/awk '/Dict/ {
```



# Jamf Compliance Editor

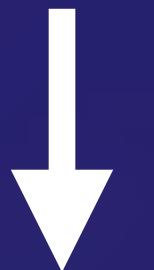
Compliance - 1. Version:	<code>org.cis_lvl2.audit.plist</code>
Compliance - 2. Failed Results Count:	0
Compliance - 3. Failed Result List:	<code>system_settings_siri_listen_disable</code>
Compliance - 4. Exemptions:	<code>system_settings_siri_listen_disable</code>



# Device Compliance

JNUC24 - Device Compliance  
Registration Status:

Not Registered for user home /var/setup



JNUC24 - Device Compliance  
Registration Status:

WPJ Key present, JamfAAD PLIST missing from user home: /Users/leeg



JNUC24 - Device Compliance  
Registration Status:

Registered



# Device Compliance Status

```
#!/bin/bash
#Written by Ben Whitis - 08/11/2022
#Updated 11/29/2023 - use dscl to identify user home directory for scenarios
where loggedInUser is an alias

#get user
loggedInUser=$( scutil <<< "show State:/Users/ConsoleUser" | awk '/Name :/
&& ! /loginwindow/ { print $3 }' )
#get user home directory
userHome=$(dscl . read "/Users/$loggedInUser" NFSHomeDirectory | awk -F ' '
'{print $2}')
#check if wpj private key is present
WPJKey=$(security dump "$userHome/Library/Keychains/login.keychain-db" | grep
MS-ORGANIZATION-ACCESS)
if [ ! -z "$WPJKey" ]
...

```

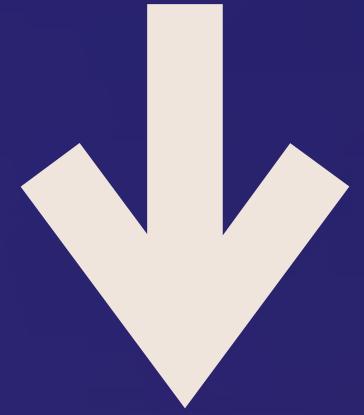
[https://github.com/benwhitis/Jamf\\_Conditional\\_Access/blob/main/EA\\_registrationStatus](https://github.com/benwhitis/Jamf_Conditional_Access/blob/main/EA_registrationStatus)



# PSSOe Status

JNUC24 - PSSO Enabled:

Not Registered



JNUC24 - PSSO Enabled:

leeg@geekygordo.com



# PSSOe Status

```
#!/bin/bash

currentUser=$(ls -l /dev/console | awk '/ / { print $3 }')
entraUPN=$(dscl . read /Users/"$currentUser"
dsAttrTypeStandard:AltSecurityIdentities | awk -F'SSO:' '/PlatformSSO/
{print $2}')

if [ [ -z $entraUPN ]]; then
    echo "<result>Not Registered</result>"
else
    echo "<result>$entraUPN</result>"
fi
```



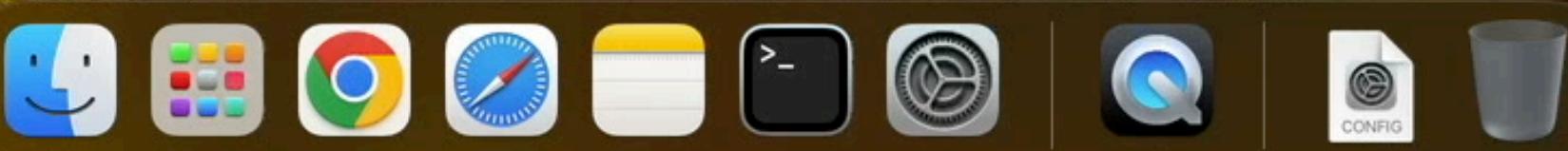
# Device Compliance and PSSOe

JNUC24 - Device Compliance Registration Status:	Registered
JNUC24 - Find Battery Status:	OK
JNUC24 - Last Startup Date:	2024-08-01 13:49:36
JNUC24 - Nudge Logs:	Required OS:
JNUC24 - PSSO Enabled:	leeg@geekygordo.com



# Privilege Elevation Management





© copyright 2024 Jamf

JNUC  
2024

# Privilege Elevation Management

Jamf Connect - Privilege Elevation

Audit Log:

2024-08-12 08:52:51 User user elevated to admin for stated reason: Other: Hello JNUC 2024  
2024-08-12 08:56:31 User user elevated to admin for stated reason: Production  
2024-08-12 08:59:00 User user elevated to admin for stated reason: Testing

```
#!/bin/zsh

# Path to the log file
log_file="/Library/Logs/JamfConnect/UserElevationReasons.log"

# Check if the log file exists
if [ ! -f "$log_file" ]; then
    # If the log file doesn't exist, output a specific message for the extension attribute
    echo "<result>No Jamf Connect privilege elevations</result>"
    exit 0

https://community.jamf.com/t5/jamf-connect/jamf-connect-2-33-0-admin-elevation-extension-attribute/m-p/313300
```



# Computer Uptime

Uptime (Days):

6

```
#!/bin/bash

# Commands required by this script
declare -x awk="/usr/bin/awk"
declare -x sysctl="/usr/sbin/sysctl"
declare -x perl="/usr/bin/perl"

declare -xi DAY=86400
declare -xi EPOCH=$(perl -e "print time")
declare -xi UPTIME=$(sysctl kern.boottime |
    awk -F' [= ,]' '/sec/{print $6;exit}' )

declare -xi DIFF=$((EPOCH - $UPTIME))
```

<https://gist.github.com/acidprime/2046271>



# Remote Desktop Status

JNUC24 - Remote Desktop Status: **Remote Desktop Enabled**

```
#!/bin/bash

launchctl="/bin/launchctl"

# Check to see if Remote Desktop is on
remoteDesktopOn=$(($launchctl list com.apple.screensharing > /dev/null 2>&1; /bin/echo $?))

if [[ $remoteDesktopOn == "0" ]]; then
    echo "<result>Remote Desktop Enabled</result>"
else
    echo "<result>Remote Desktop Disabled</result>"
fi
```



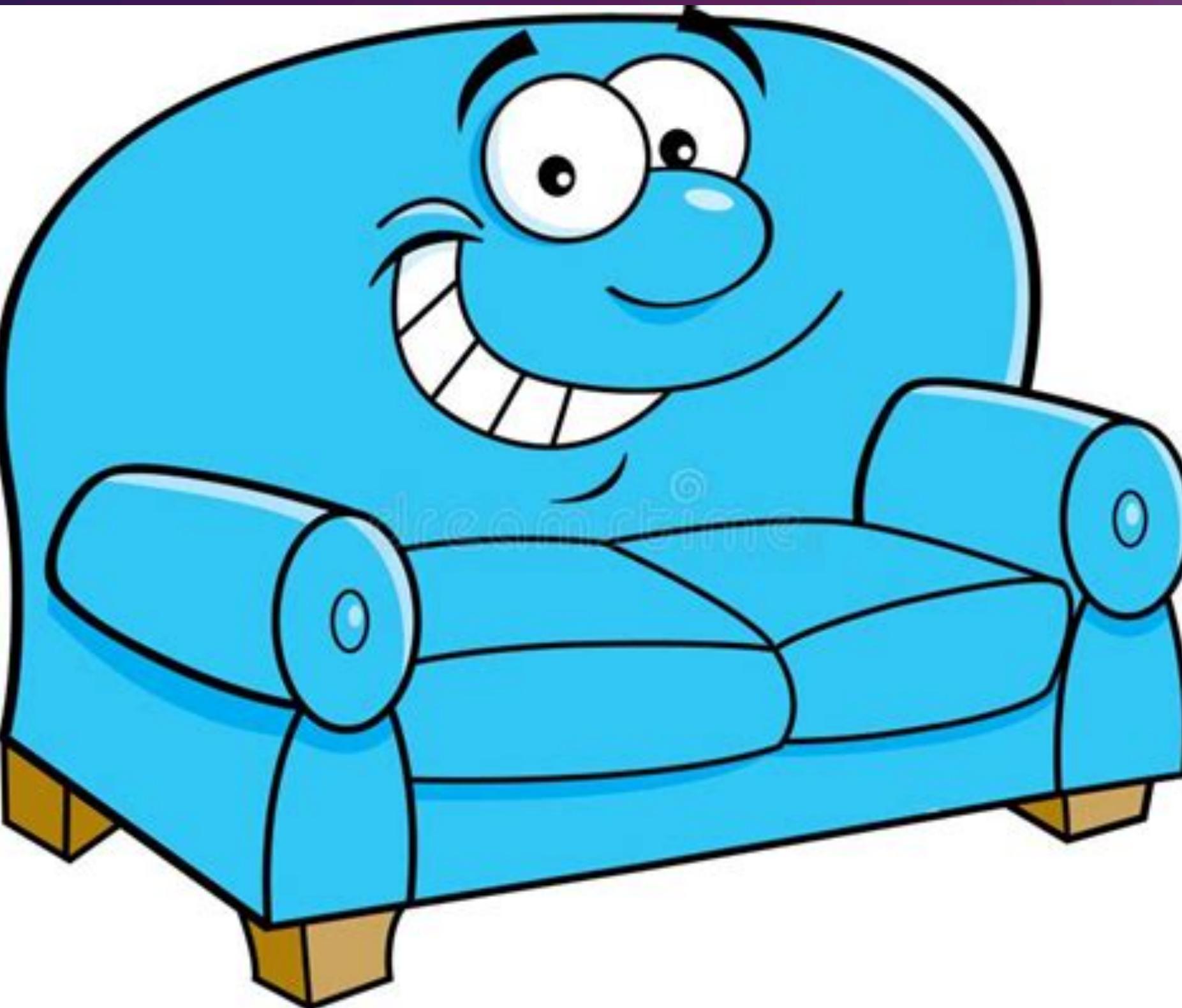
# Remote Login Status

JNUC24 - Remote Login: **On**

```
#!/bin/bash  
  
echo "<result>$(/usr/sbin/systemsetup -getremotelogin | awk '{print $3}')</result>"
```

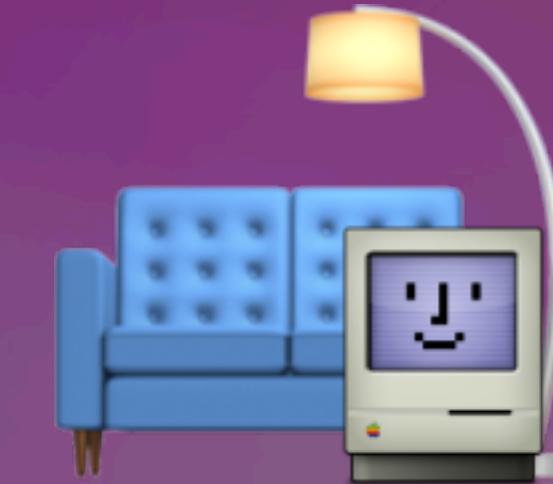


# SOFA



# SOFA

Simple  
Organized  
Feed for  
Apple Software Updates



<https://github.com/macadmins/sofa>

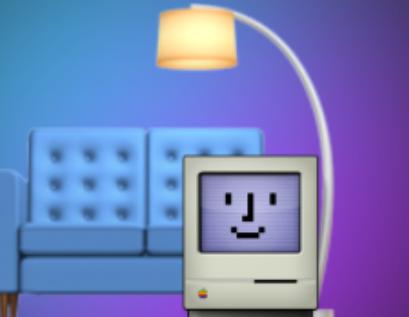


# SOFA

SOFA - by MAOS

Home Sequoia Sonoma Ventura Monterey iOS 17 iOS 16 Use Cases ...

## SOFA - Simple Organized Feed for Apple Software Updates



SOFA supports MacAdmins by efficiently tracking and surfacing information on updates for macOS and iOS.

Sonoma 14 Ventura 13 Monterey 12 iOS 17 iOS 16

---

### macOS feed file

[View macOS Data Feed JSON](#)

Last Check: 2024-08-02T19:01:57+00:00Z

Update Hash: f4c49816f57d3c3f42569c9bcc7ed37f0cdc45a6528f7ff1f11209b66ed52358

---

### iOS feed file

[View iOS Data Feed JSON](#)

Last Check: 2024-08-02T19:02:14+00:00Z

Update Hash: fc0030b8e3ea575c24fc03546e6dd949c7c960ae89603e3b0142871bbbfa0c6d

---

### Debug Info

You fetched this data at: 2024-08-02T19:47:52.958Z

Time since last macOS feed file timestamp: 0 days, 0 hours, 45 minutes ago

<https://sofa.macadmins.io/>



# SOFA

SOFA - by MAOS

Home Sequoia Sonoma Ventura Monterey iOS 17 iOS 16 Use Cases ...

On this page >

## macOS Sonoma 14 Current Version (N-0)

**RECOMMENDED RELEASE FOR MOST UP-TO-DATE SECURITY**

This is the latest version of macOS that receives the most up-to-date security patches and updates, making it the recommended choice to protect your devices.

### Latest Release Info



<b>Latest macOS Sonoma 14</b>	<b>Latest XProtect</b>
OS Version: Sonoma 14	XProtect Framework: 140
Product Version: 14.6	Plugin Service: 74
Build: 23G80	Release Date: July 23, 2024
Release Date: July 28, 2024	Time Since Release: 11 days, 21 hours
Days Since Release: 6	XProtect Config Data: 5270
Installer Package: <a href="#">Download</a>	Plist Release Date: July 23, 2024
Current IPSW file: <a href="#">Download</a>	Time Since Plist Release: 11 days, 21 hours

### Essential Apple Resources

[What's new for enterprise in macOS Sonoma](#)  
[What's new in the updates for macOS Sonoma](#)



# SOFA

SOFA - by MAOS

Home Sequoia Sonoma Ventura Monterey iOS 17 iOS 16 Use Cases ...

On this page >

## Security Information

**macOS Sonoma 14.6**

Release Date: July 28, 2024 ▲

macOS Sonoma 14.6

Security Info: <https://support.apple.com/kb/HT214119>

Vulnerabilities Addressed: 69

Actively Exploited Vulnerabilities (KEV):

CVEs: [CVE-2024-40804](#), [CVE-2023-38709](#), [CVE-2024-24795](#), [CVE-2024-27316](#),  
[CVE-2024-40783](#), [CVE-2024-40774](#), [CVE-2024-40814](#), [CVE-2024-40775](#), [CVE-2024-27877](#), [CVE-2024-27878](#), [CVE-2024-40799](#), [CVE-2024-27873](#), [CVE-2024-2004](#), [CVE-2024-2379](#), [CVE-2024-2398](#), [CVE-2024-2466](#), [CVE-2024-40827](#), [CVE-2024-40815](#), [CVE-2024-40795](#), [CVE-2023-6277](#), [CVE-2023-52356](#), [CVE-2024-40806](#), [CVE-2024-40777](#), [CVE-2024-40784](#), [CVE-2024-27863](#), [CVE-2024-40816](#), [CVE-2024-40788](#), [CVE-2024-40803](#), [CVE-2024-40805](#), [CVE-2024-40832](#), [CVE-2024-40796](#), [CVE-2024-6387](#), [CVE-2024-40781](#), [CVE-2024-40802](#), [CVE-2024-40823](#), [CVE-2024-27882](#), [CVE-2024-27883](#), [CVE-2024-40778](#), [CVE-2024-40800](#), [CVE-2023-27952](#), [CVE-2024-40817](#), [CVE-2024-40824](#), [CVE-2024-27871](#), [CVE-2024-27881](#), [CVE-2024-40821](#), [CVE-2024-40798](#), [CVE-2024-27872](#), [CVE-2024-27862](#), [CVE-2024-40833](#), [CVE-2024-40835](#), [CVE-2024-40836](#), [CVE-2024-40807](#), [CVE-2024-40834](#), [CVE-2024-40809](#), [CVE-2024-40812](#), [CVE-2024-40787](#), [CVE-2024-40793](#), [CVE-2024-40818](#), [CVE-2024-40822](#), [CVE-2024-40828](#), [CVE-2024-40811](#), [CVE-2024-40776](#), [CVE-2024-40782](#), [CVE-2024-40779](#), [CVE-2024-40780](#), [CVE-2024-40785](#), [CVE-2024-40789](#), [CVE-2024-4558](#), [CVE-2024-40794](#)

Days to Prev. Release: 77

**macOS Sonoma 14.5**

Release Date: May 12, 2024 ▲



# SOFA Statuses



JNUC24 - SOFA - macOS Compatibility: **Pass**

JNUC24 - SOFA - macOS Version  
Check: **Fail**

JNUC24 - SOFA - XProtect Version: **Pass**

JNUC24 - SOFA macOS CVE: **CVEs:69 ActiveExploits:0**



# SOFA Statuses



Computers : Smart Computer Groups

## ← Active CVE Exploits

Computer Group

Criteria

Reports

AND/OR

CRITERIA

OPERATOR

VALUE

▼

JNUC24 - SOFA  
macOS CVE

matches regex

ActiveExploits:[1-9]



# SOFA Statuses

Computers : Smart Computer Groups

← Active CVE Exploits

Computer Group Criteria Reports

Display Name  
Display name for the smart computer group

Active CVE Exploits

Send email notification on membership change  
When group membership changes, send an email notification to Jamf Pro users with e

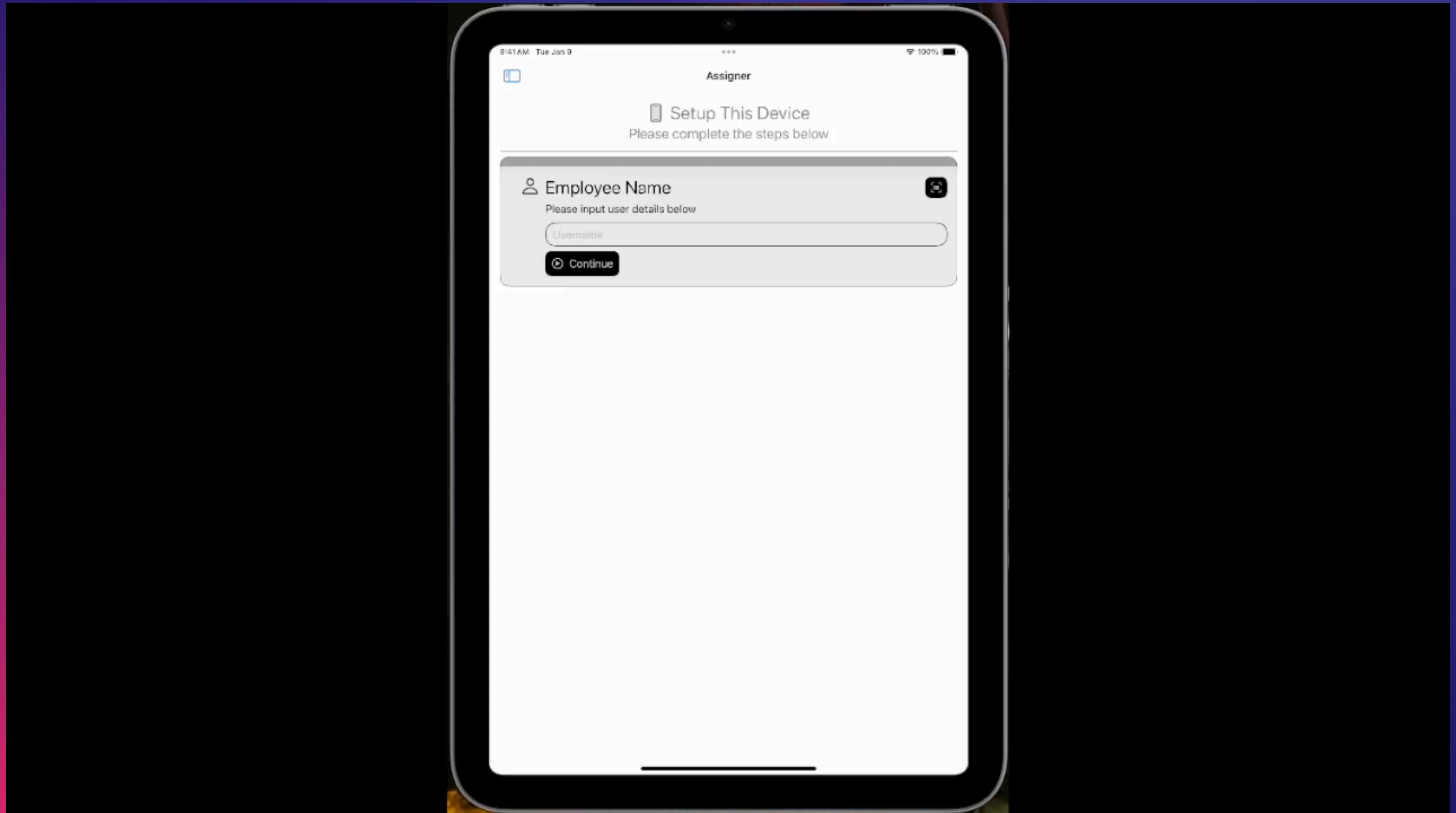
Site  
Site to add the smart computer group to

None ▾



# Mobile Assist and Return to Service





## Extension Attributes

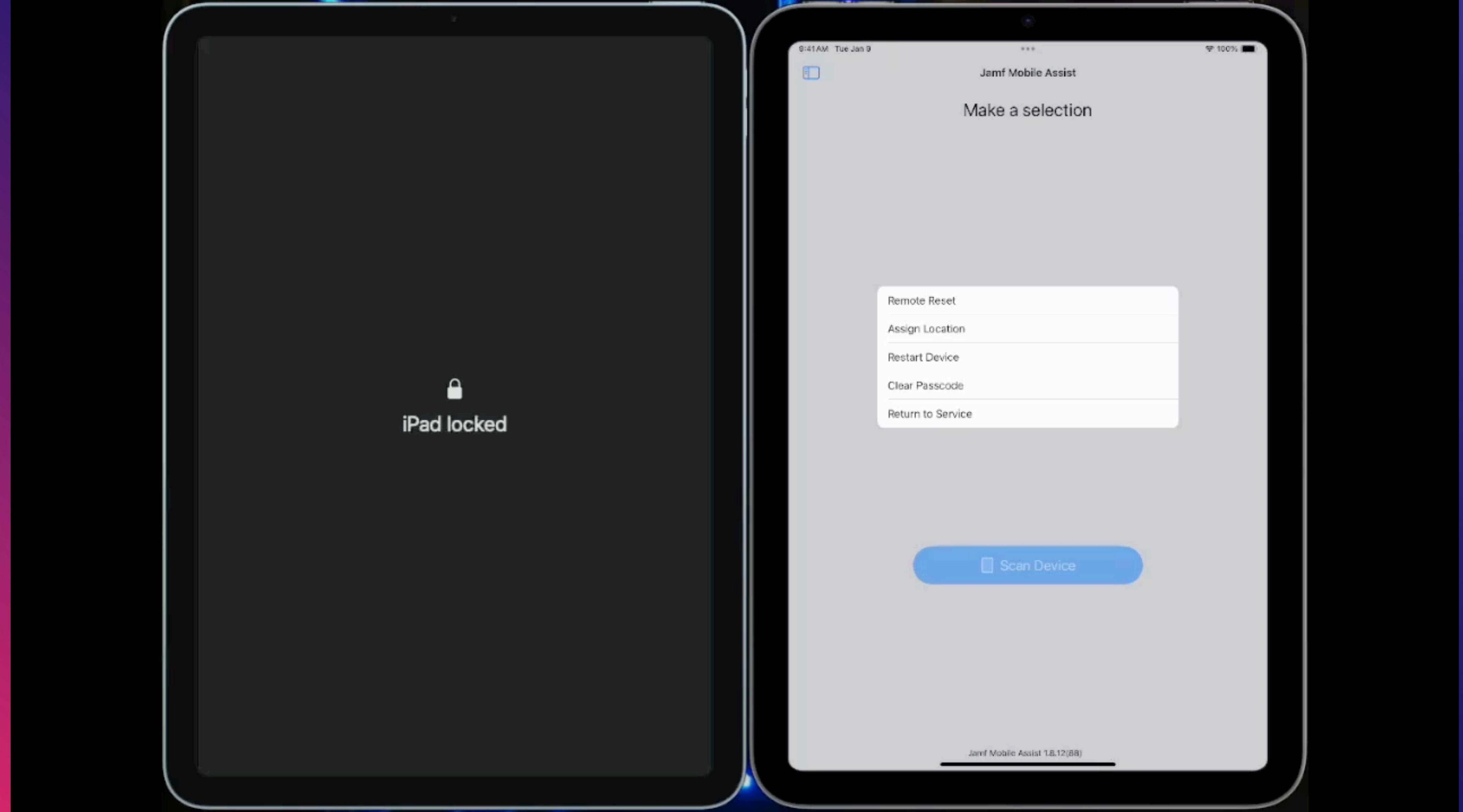
Country (Directory Attribute): **US**

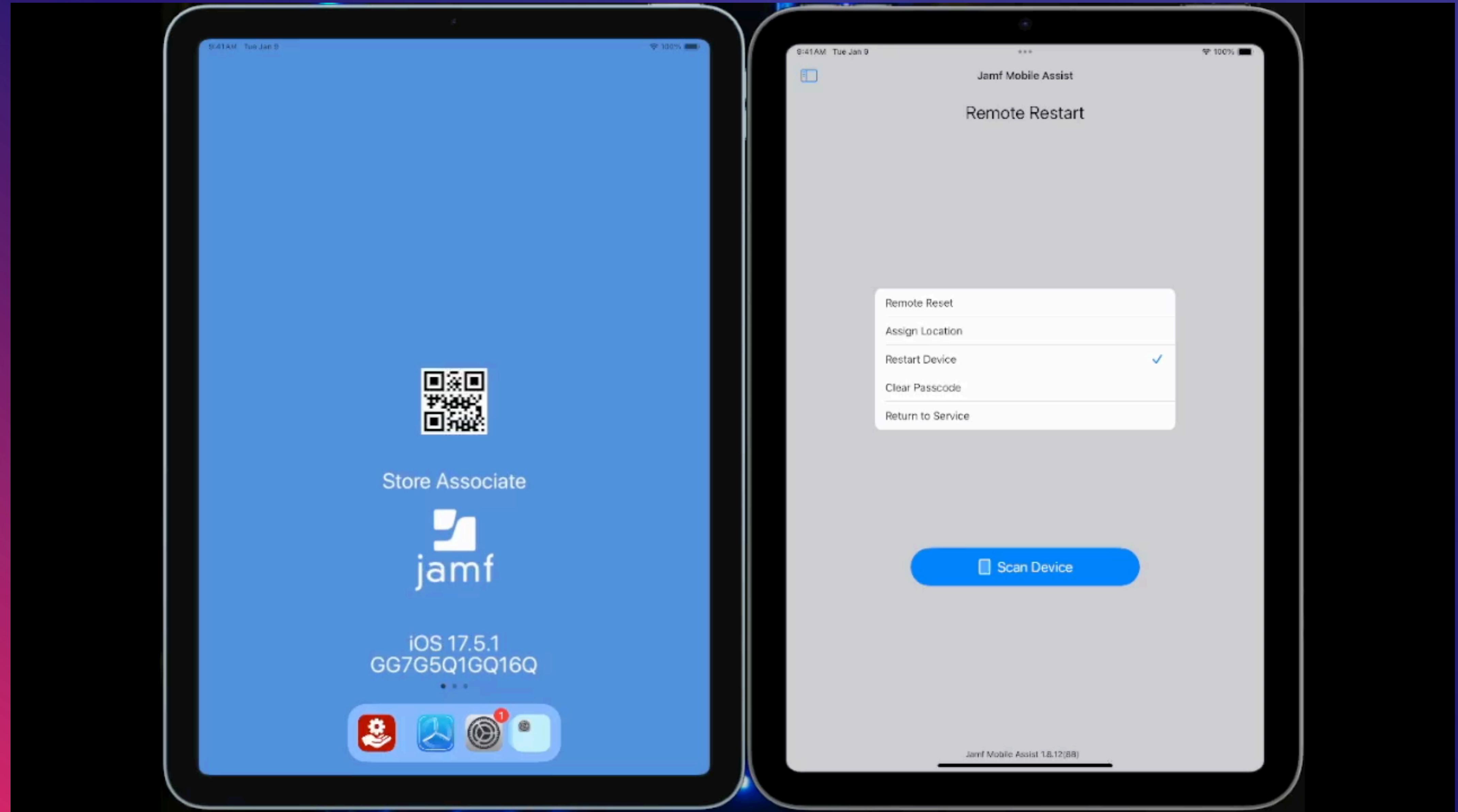
Role: **Store Associate**

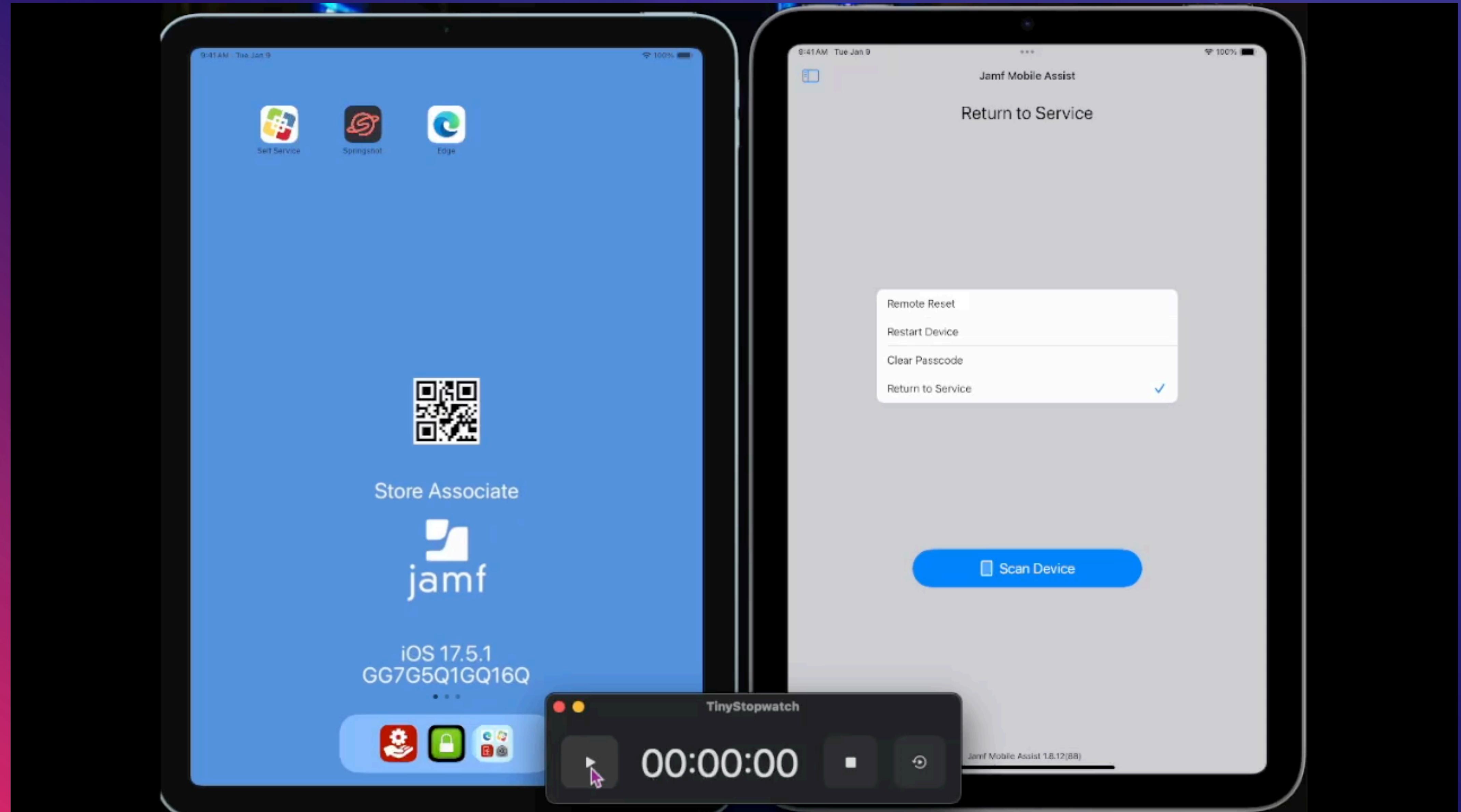
Store: **Store 1**

Store City (Directory Attribute): **Austin**









Pro

Full Jamf Pro ▾

Devices

Inventory Management History

← JMA-LQ56MFQF3G

Extension Attributes

Country (Directory Attribute):

Return to Service:

Role:

Store:

Store City (Directory Attribute):

History Delete

General JMA-LQ56MFQF3G

Hardware iPad mini 6th generation (Wi-Fi)

User and Location

Purchasing

Security Data protection is not enabled

Extension Attributes

Apps 7 Apps

Managed eBooks 0 Managed eBooks

Network

iBeacon Regions 0 Beacon Regions

Inventory Search Inventory

Search Volume Content

Content Management Configuration Profiles

Software Updates Provisioning Profiles

Personal Device Profiles

Mobile Device Apps

eBooks

Groups

Smart Device Groups

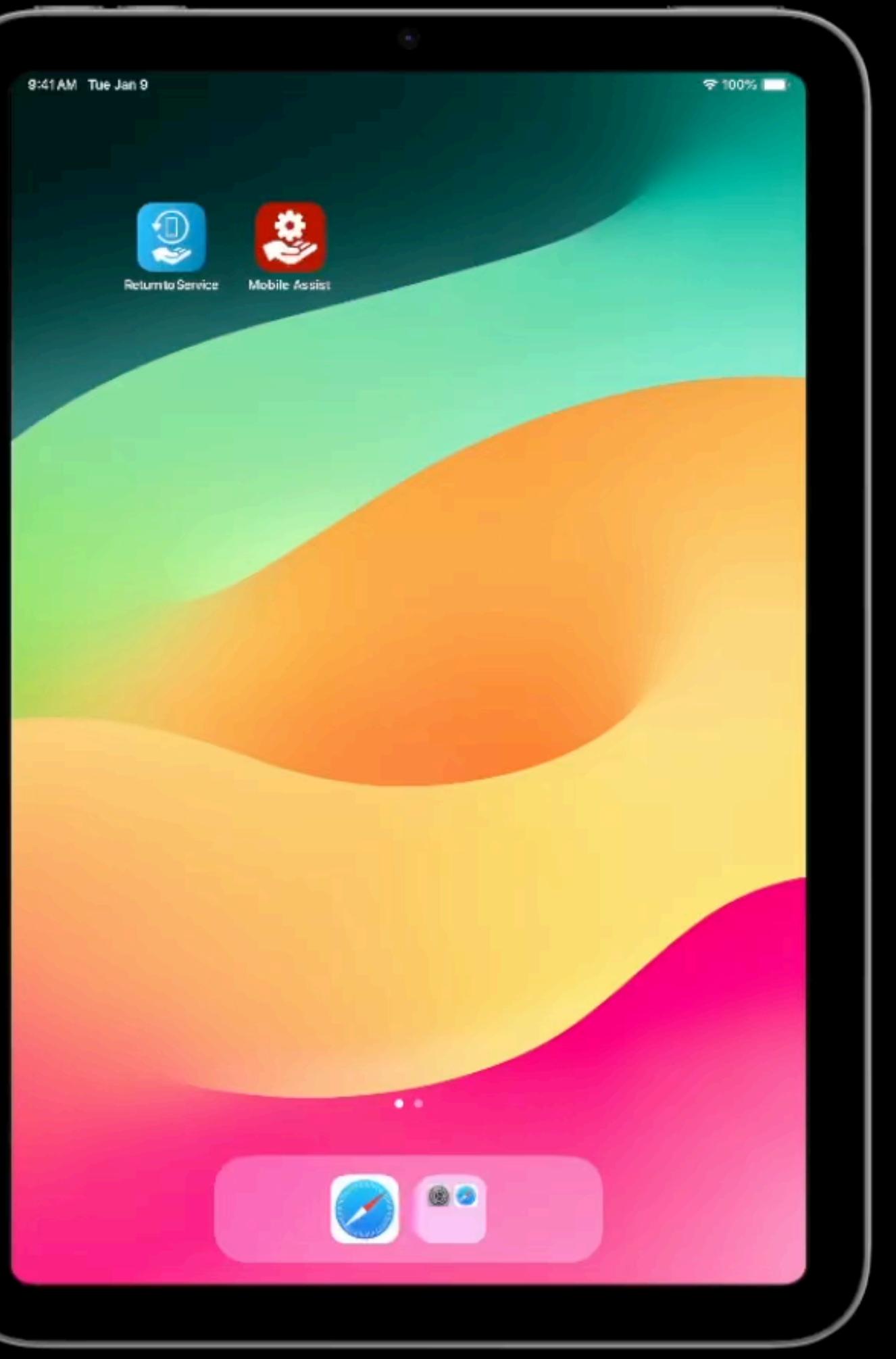
Static Device Groups

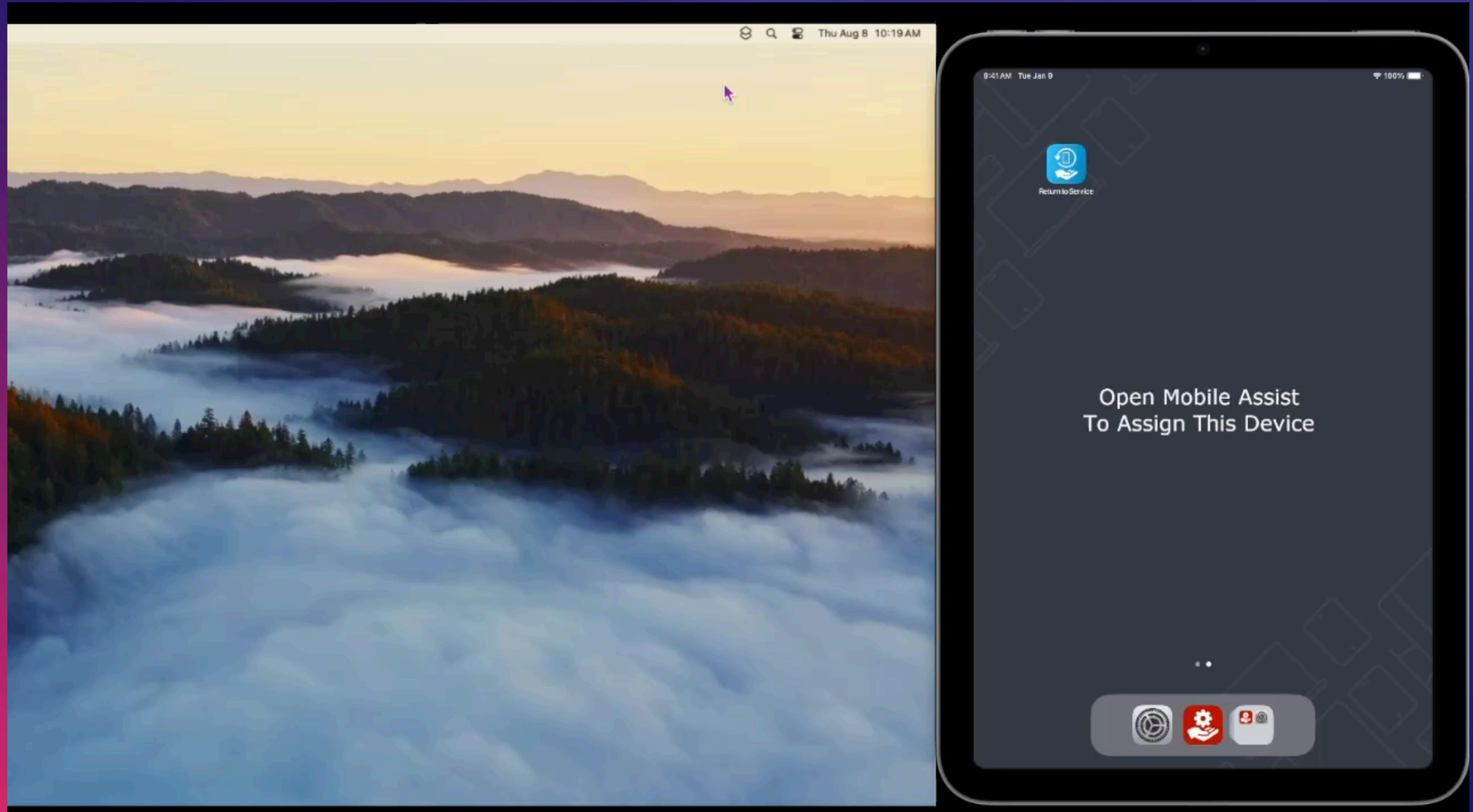
Classes

Enrollment Enrollment Profiles

Enrollment Invitations

PreStage Enrollments





<https://trusted.jamf.com/concepts/docs/jamf-actions>

JNUC  
2024

# References



**Do you dare scan the QR code?**

<https://github.com/stevewood-tx/JNUC2024>



# References

<https://github.com/dan-snelson/Nudge-Post-install/blob/main/EA-Nudge-Logs.sh>

<https://trusted.jamf.com/docs/establishing-compliance-baselines>

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

[https://github.com/benwhitis/Jamf\\_Conditional\\_Access/blob/main/EA\\_registrationStatus](https://github.com/benwhitis/Jamf_Conditional_Access/blob/main/EA_registrationStatus)

<https://community.jamf.com/t5/jamf-connect/jamf-connect-2-33-0-admin-elevation-extension-attribute/m-p/313300>

<https://gist.github.com/acidprime/2046271>

<https://github.com/stevewood-tx/JNUC2024>



# References

<https://github.com/macadmins/sofa>

<https://sofa.macadmins.io/>

<https://github.com/macadmins/sofa/tree/main/tool-scripts>

<https://marketplace.jamf.com/details/jamf-mobile-assist>

<https://marketplace.jamf.com/details/return-to-service-app>

<https://trusted.jamf.com/concepts/docs/jamf-actions>





**Thank you!**

