jamf

Managing user identity on Macs

Sean Rabbitt

Sr Consulting Engineer,
Identity and Access Mgmt

PRESENTING TO

2023 MACADMINS CONFERENCE

Agenda

1 | Background and history of macOS

I promise not to bore you with stories of how I used to work at Data General and DG/UX

2 | Local User Accounts

How to deal with them, command line fun times, and why we're stuck with them forever. (Spoiler: FileVault)

3 | On-Premises and Cloud Directories

Where Sean goes on a rant about binding, the alternatives, and cloud identity provider management

4 | The Future: Platform Single Sign-On

With a whole bunch of speculation because after 4 years, we barely have normal Single Sign-On

jamf

A short history lesson

History

By ComputerGeek7066 - Own work, CC BY-SA 4.0, https://commons.wikimedia.org/w/index.php?curid=80616265

jamf

History

macOS
is
UNIX

By ComputerGeek7066 - Own work, CC BY-SA 4.0, https://commons.wikimedia.org/w/index.php?curid=80616265

jamf

macOS is **UNIX**

Local Accounts and Groups

Short Name
Real Name
UID
Primary Group
Home Directory

Hierarchical File Structure

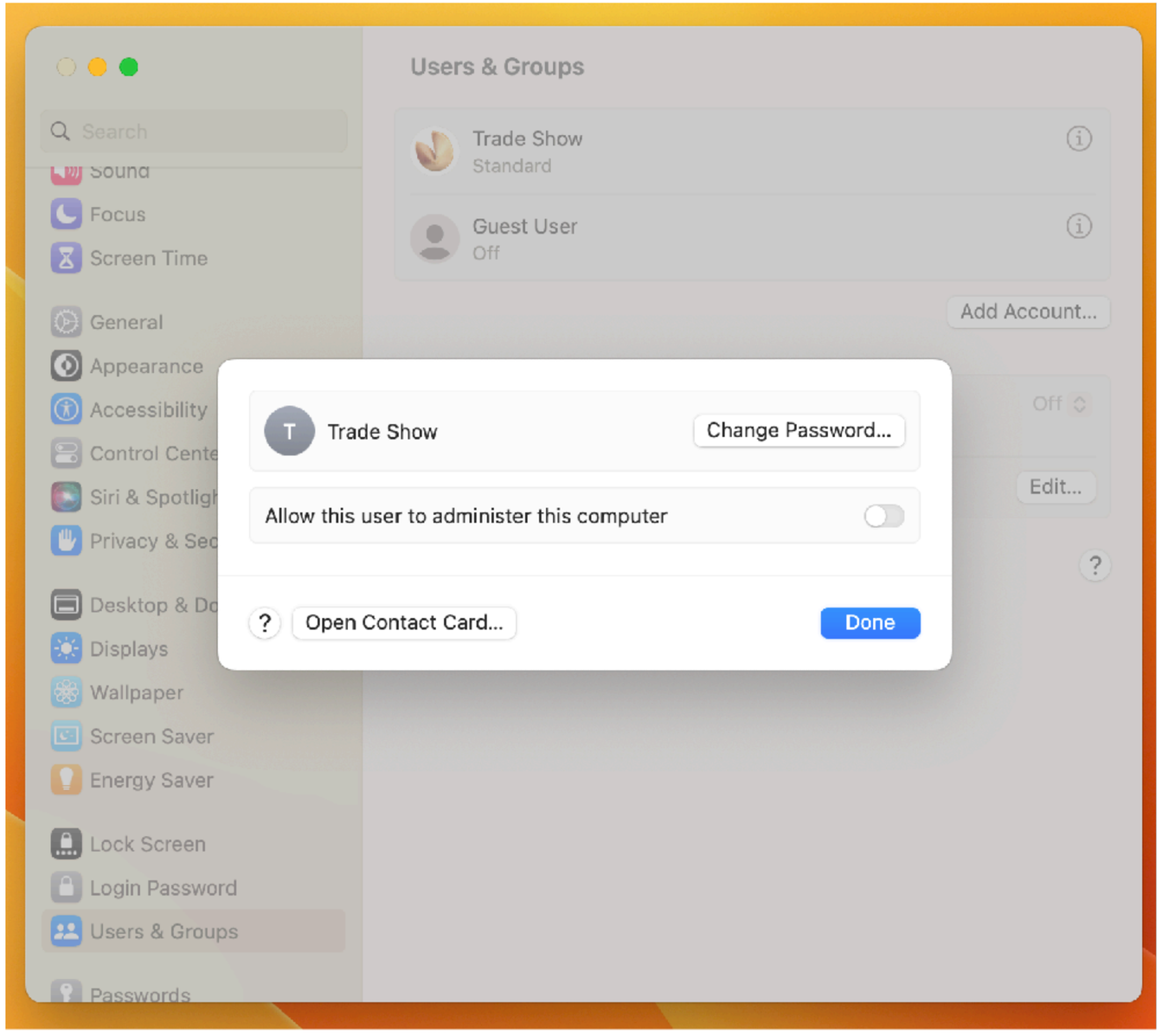
File Owner
Group Owner
Read / Write / Execute
Other Apple Specific Magic

Basic Privilege Access Management (PAM)

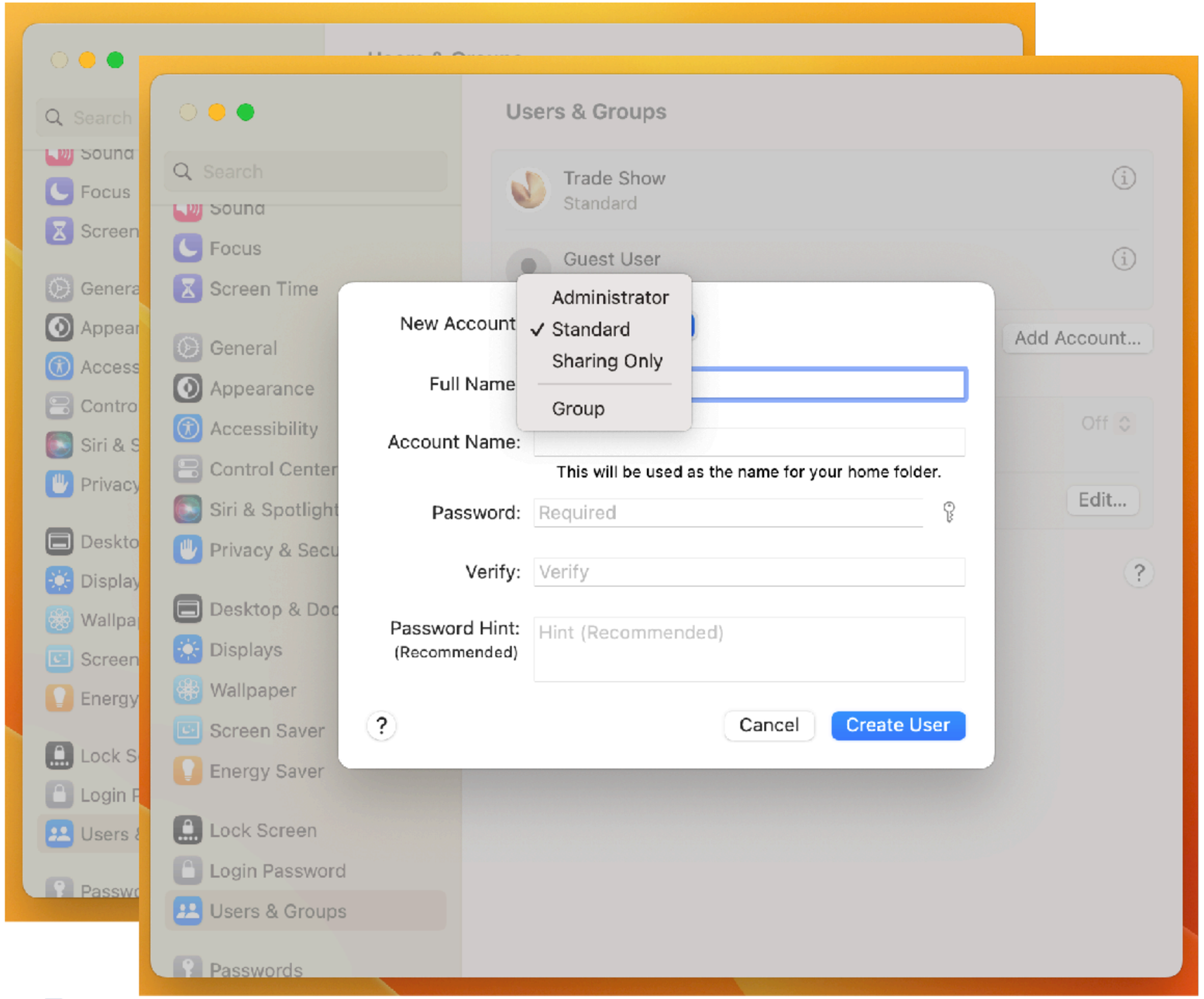
Administrator User
Standard User
Guest User
Sharing Only User

jamf

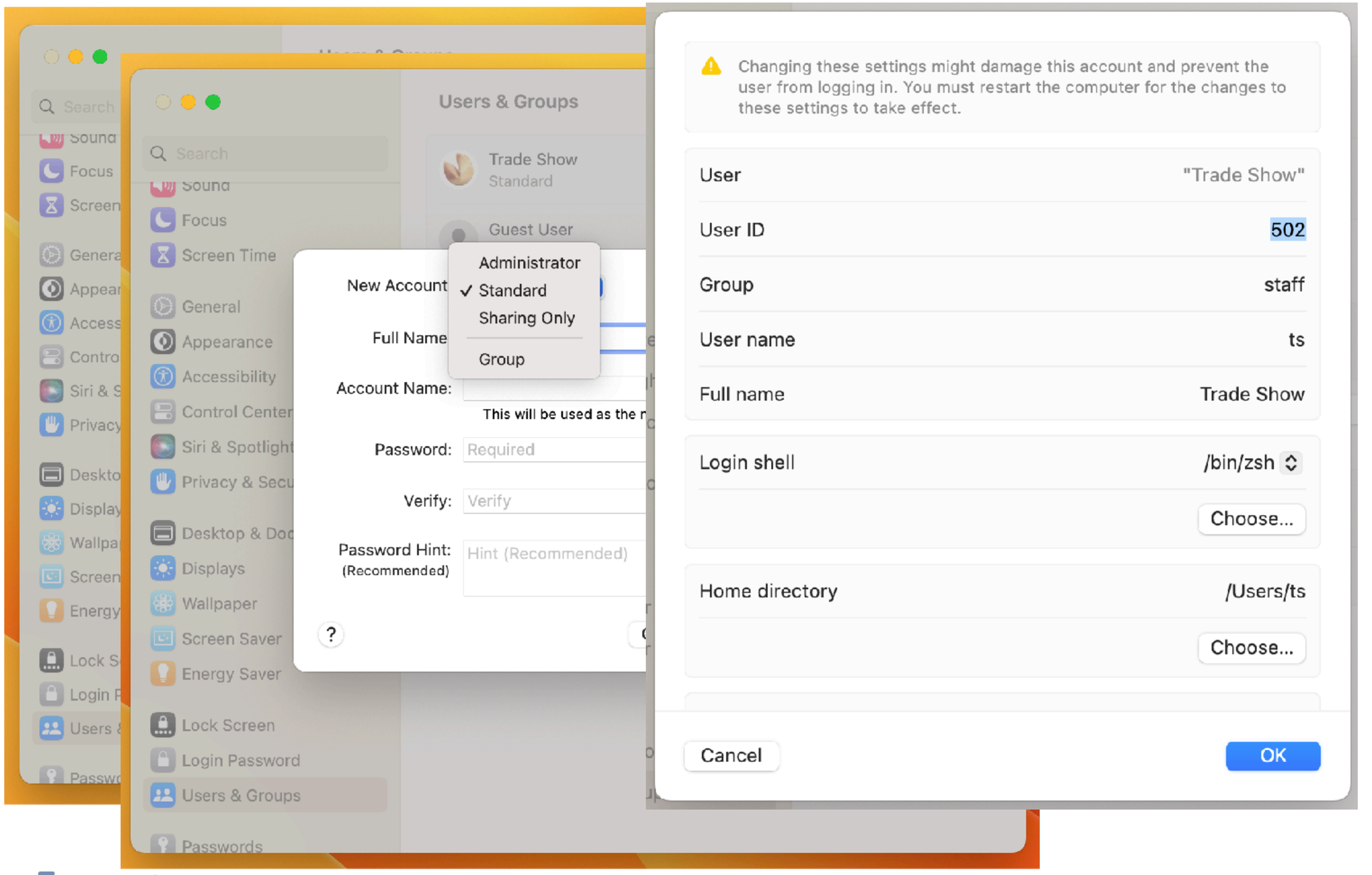
Local User Accounts


Users & Groups
Search
Sound
Focus
Screen Time
General
Appearance
Accessibility
Control Cente
Siri & Spotligh
Privacy & Sec
Desktop & Do
Displays
Wallpaper
Screen Saver
Energy Saver
Lock Screen
Login Password
Users & Groups
Passwords
Trade Show
Standard
Guest User
Off
Add Account...
Off
Edit...
T
Trade Show
Change Password...
Allow this user to administer this computer
Open Contact Card...
Done

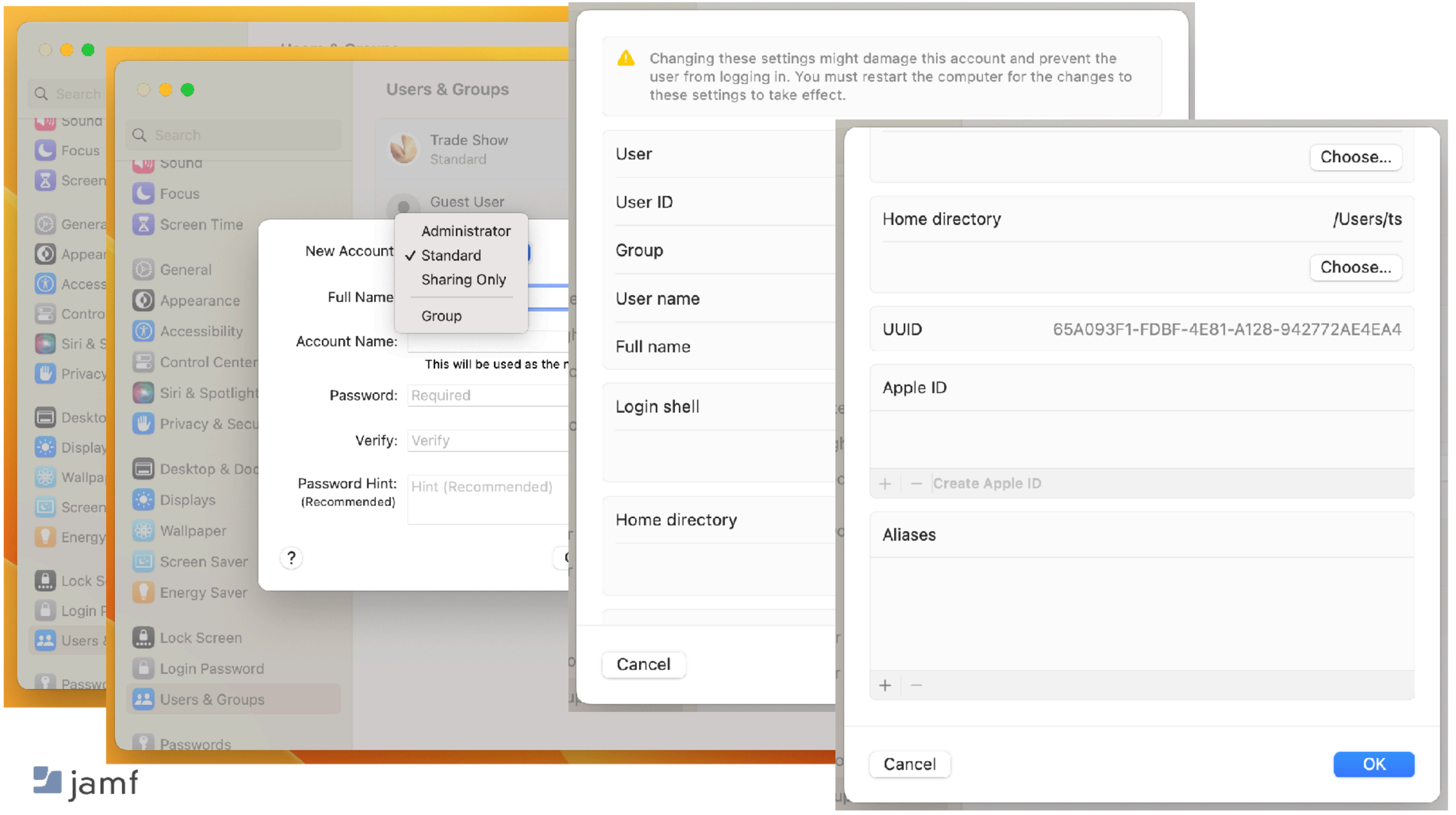
jamf


Users & Groups
Search
Trade Show
Standard
Guest User
Add Account...
Off
Edit...
New Account
Administrator
Standard
Sharing Only
Group
Full Name
Account Name:
This will be used as the name for your home folder.
Password:
Required
Verify:
Verify
Password Hint:
(Recommended)
Hint (Recommended)
Cancel
Create User
General
Appearance
Accessibility
Control Center
Siri & Spotlight
Privacy & Secu
Desktop & Doc
Displays
Wallpaper
Screen Saver
Energy Saver
Lock Screen
Login Password
Users & Groups
Passwords
Focus
Screen Time

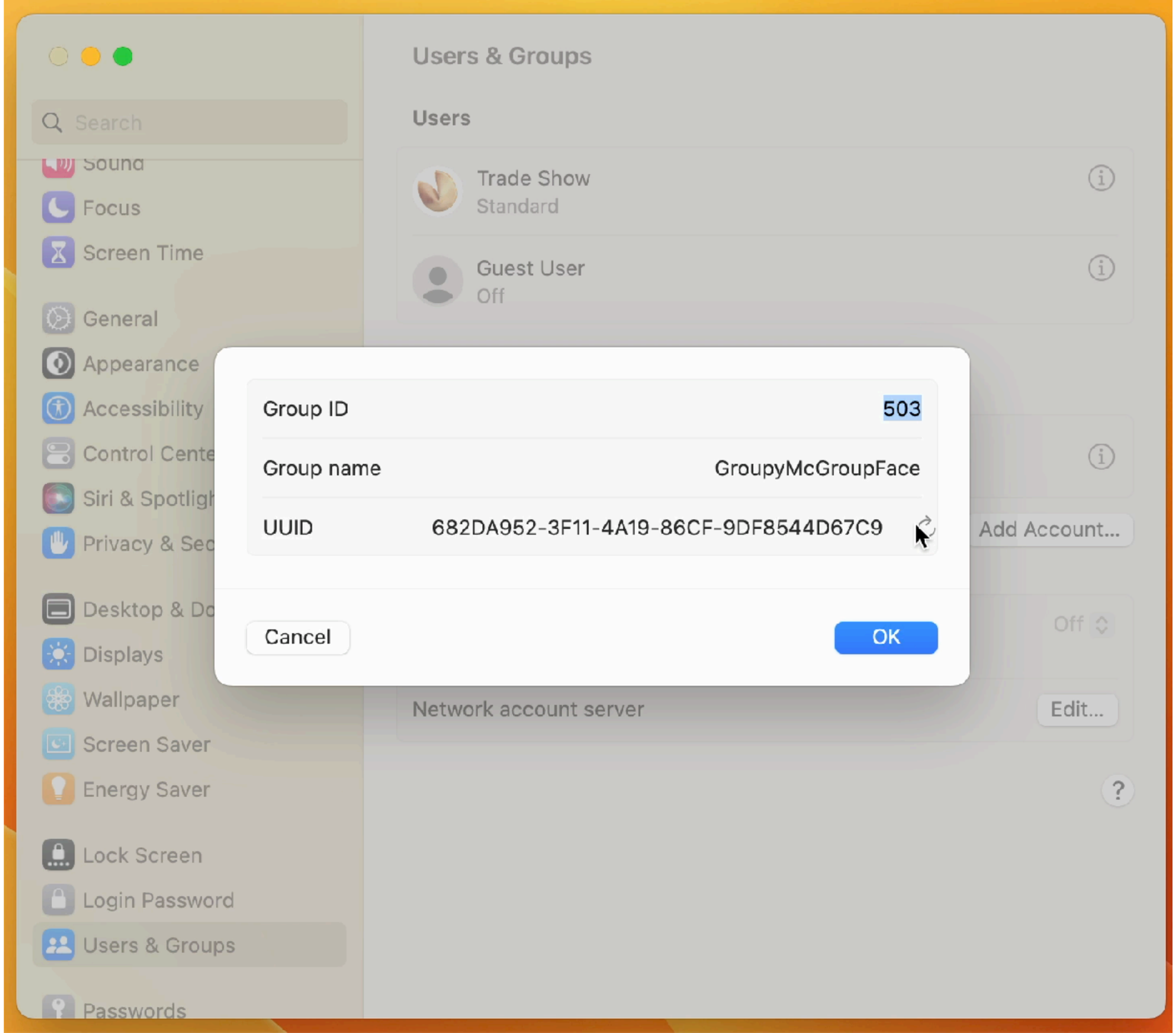
jamf


Users & Groups
Trade Show
Standard
Guest User
Search
Sound
Focus
Screen Time
General
Appearance
Accessibility
Control Center
Siri & Spotlight
Privacy & Secu
Desktop & Doc
Displays
Wallpaper
Screen Saver
Energy Saver
Lock Screen
Login Password
Users & Groups
Passwords
New Account
Administrator
Standard
Sharing Only
Group
Full Name
Account Name:
This will be used as the n
Password:
Required
Verify:
Verify
Password Hint:
(Recommended)
Hint (Recommended)
?
Changing these settings might damage this account and prevent the user from logging in. You must restart the computer for the changes to these settings to take effect.
User
"Trade Show"
User ID
502
Group
staff
User name
ts
Full name
Trade Show
Login shell
/bin/zsh
Choose...
Home directory
/Users/ts
Choose...
Cancel
OK

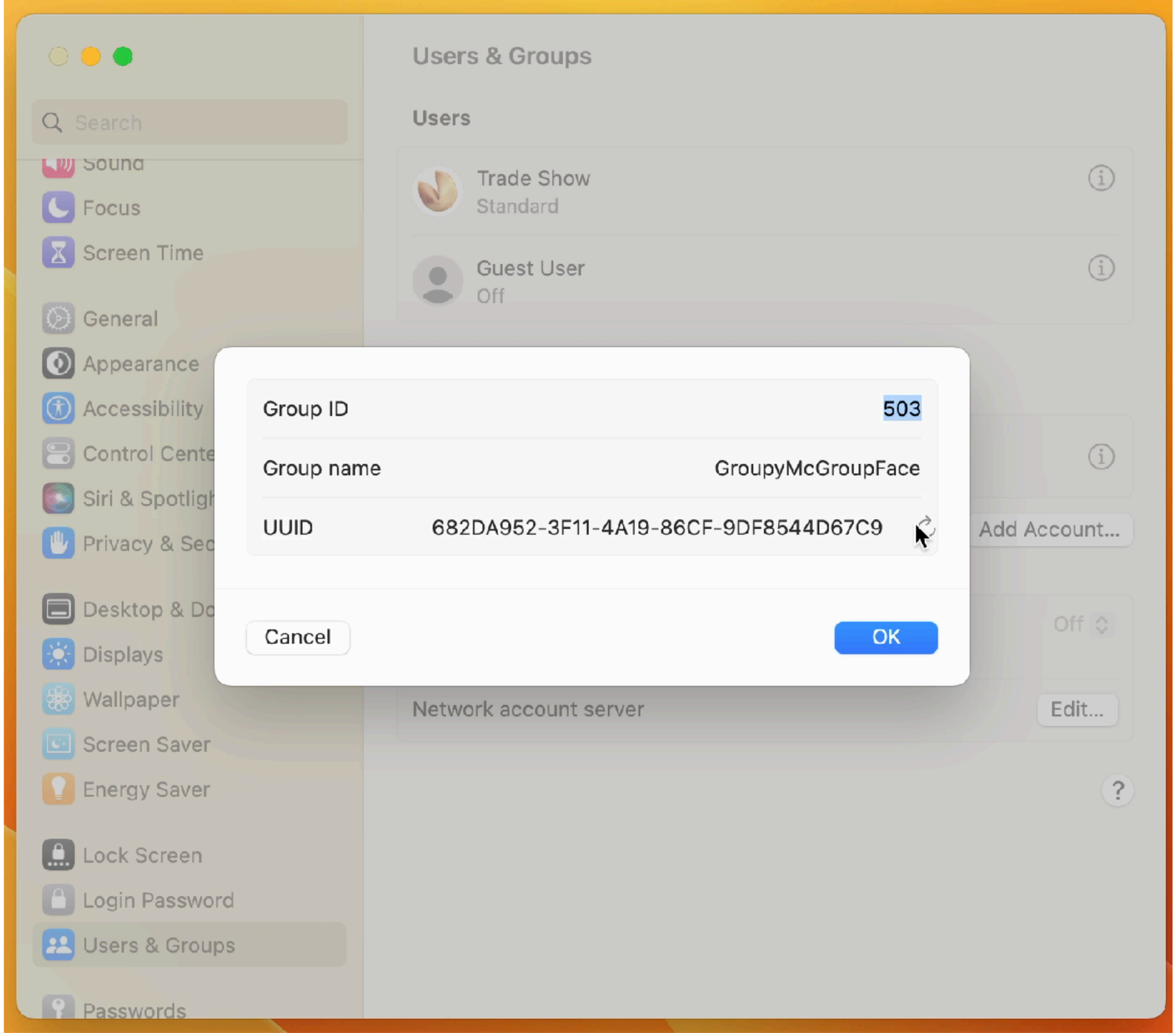
jamf


Users & Groups
Search
Trade Show
Standard
Guest User
Administrator
Standard
Sharing Only
Group
New Account
Full Name
Account Name:
This will be used as the n
Password:
Required
Verify:
Verify
Password Hint:
(Recommended)
Hint (Recommended)
General
Appearance
Accessibility
Control Center
Siri & Spotlight
Privacy & Secu
Desktop & Doc
Displays
Wallpaper
Screen Saver
Energy Saver
Lock Screen
Login Password
Users & Groups
Passwords
Changing these settings might damage this account and prevent the user from logging in. You must restart the computer for the changes to these settings to take effect.
User
User ID
Group
User name
Full name
Login shell
Home directory
Cancel
Choose...
Home directory
/Users/ts
Choose...
UUID
65A093F1-FDBF-4E81-A128-942772AE4EA4
Apple ID
Create Apple ID
Aliases
Cancel
OK

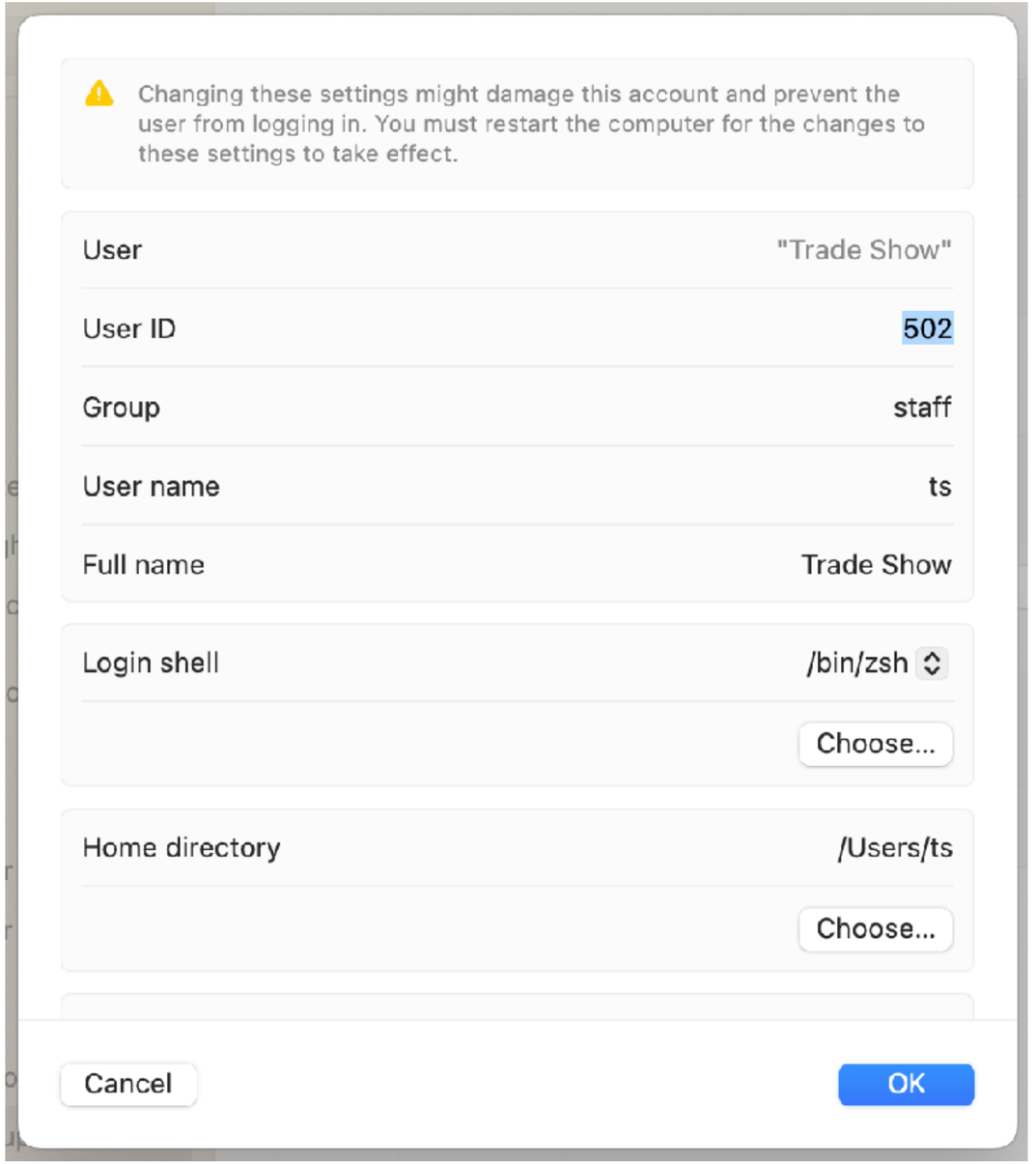
jamf

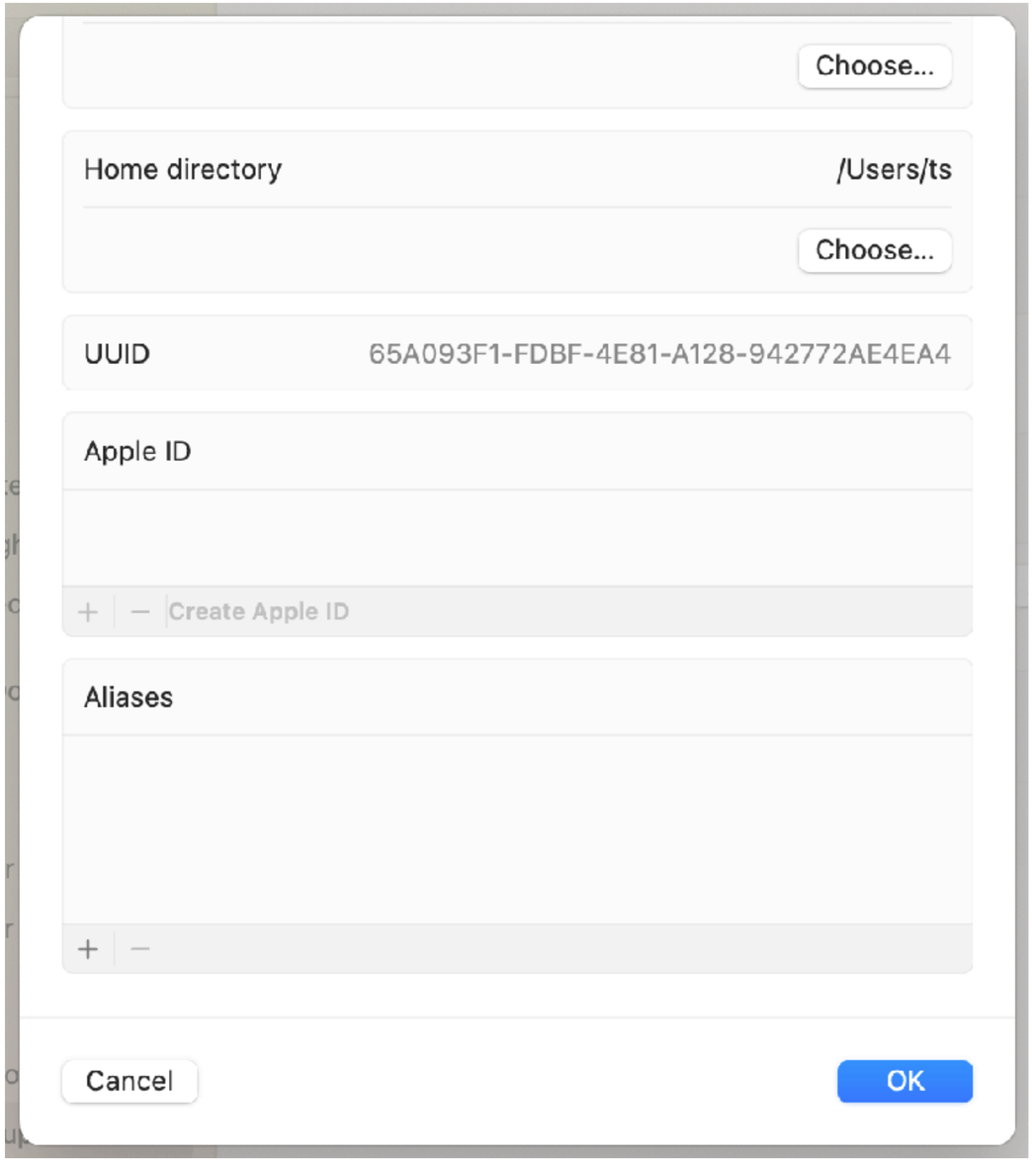

Users & Groups
Users
Search
Sound
Focus
Screen Time
General
Appearance
Accessibility
Control Cente
Siri & Spotligh
Privacy & Sec
Desktop & Do
Displays
Wallpaper
Screen Saver
Energy Saver
Lock Screen
Login Password
Users & Groups
Passwords
Trade Show
Standard
Guest User
Off
Group ID
503
Group name
GroupyMcGroupFace
UUID
682DA952-3F11-4A19-86CF-9DF8544D67C9
Cancel
OK
Add Account...
Off
Network account server
Edit...

jamf

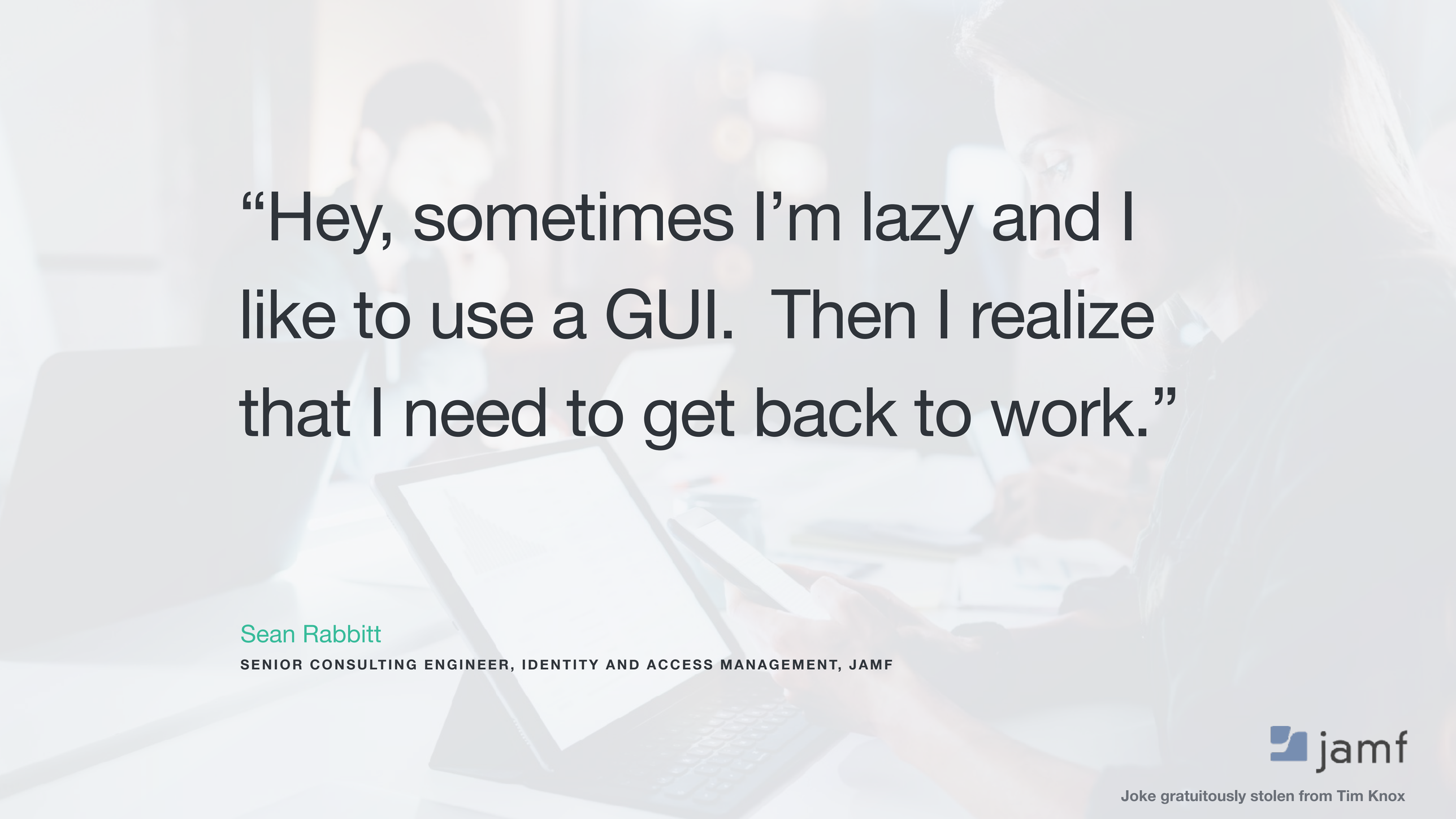

Users & Groups
Users
Search
Sound
Focus
Screen Time
General
Appearance
Accessibility
Control Cente
Siri & Spotligh
Privacy & Sec
Desktop & Do
Displays
Wallpaper
Screen Saver
Energy Saver
Lock Screen
Login Password
Users & Groups
Passwords
Trade Show
Standard
Guest User
Off
Group ID
503
Group name
GroupyMcGroupFace
UUID
682DA952-3F11-4A19-86CF-9DF8544D67C9
Cancel
OK
Add Account...
Off
Network account server
Edit...

jamf


Changing these settings might damage this account and prevent the user from logging in. You must restart the computer for the changes to these settings to take effect.
User
"Trade Show"
User ID
502
Group
staff
User name
ts
Full name
Trade Show
Login shell
/bin/zsh
Choose...
Home directory
/Users/ts
Choose...
Cancel
OK


Choose...
Home directory
/Users/ts
Choose...
UUID
65A093F1-FDBF-4E81-A128-942772AE4EA4
Apple ID
Create Apple ID
Aliases
Cancel
OK

jamf



“Hey, sometimes I’m lazy and I like to use a GUI. Then I realize that I need to get back to work.”

Sean Rabbitt

SENIOR CONSULTING ENGINEER, IDENTITY AND ACCESS MANAGEMENT, JAMF

jamf

Joke gratuitously stolen from Tim Knox

To Thine Own Self Be True, or who am i, really?

```
whoami
```

```
echo $USER
```

```
loggedInUser=$(stat -f %Su /dev/console)
echo "$loggedInUser"
```

```
loggedInUser=$( scutil <<< "show State:/Users/ConsoleUser" \
  | awk '/Name :/ && ! /loginwindow/ { print $3 }' )
echo "$loggedInUser"
```

jamf

* Armin Briegel rocks.

dscl

dscl

```
dscl . read /Users/$user
```

jamf

dscl

```
dscl . read /Users/$user
```

jamf

dscl

```
dscl . read /Users/$user
```

jamf

dscl

```
dscl . read /Users/$user
```

```
NFSHomeDirectory: /Users/ts
Password: *********
PrimaryGroupID: 20
RealName:
 Trade Show
RecordName: ts
RecordType: dsRecTypeStandard:Users
UniqueID: 502
UserShell: /bin/zsh
```

jamf

dscl

Individual Keys

```
dscl . read /Users/$user AuthenticationAuthority
```

jamf

dscl

Individual Keys

```
dscl . read /Users/$user AuthenticationAuthority
```

```
~ % dscl . read /Users/$user accountPolicyData

dsAttrTypeNative:accountPolicyData:
 <?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
 <key>creationTime</key>
 <real>1672773068.921921</real>
 <key>failedLoginCount</key>
 <integer>0</integer>
 <key>failedLoginTimestamp</key>
 <integer>0</integer>
 <key>passwordLastSetTime</key>
 <real>1682003884.02179</real>
</dict>
</plist>
```

dscl

Individual Keys

```
dscl . read /Users/$user AuthenticationAuthority
```

```
dscl . -readpl /Users/$user accountPolicyData creationTime
```

```
dscl . -readpl /Users/$user accountPolicyData failedLoginTimestamp
```

Dump the whole record to XML for further munging

```
dscl -plist . read /Users/$user
```

Append a record with stuff

```
dscl . -append /Users/$user Comment "User is a menace."
```

Remove keys from a record

```
dscl . delete /Users/$user Comment
```

dscl

```
dscl . read /Users/$user
```

```
dsAttrTypeNative:_writers_AvatarRepresentation: ts
dsAttrTypeNative:_writers_hint: ts
dsAttrTypeNative:_writers_jpegphoto: ts
dsAttrTypeNative:_writers_passwd: ts
dsAttrTypeNative:_writers_picture: ts
dsAttrTypeNative:_writers_unlockOptions: ts
dsAttrTypeNative:_writers_UserCertificate: ts
dsAttrTypeNative:accountPolicyData:
 <?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DT
<plist version="1.0">
<dict>
        <key>creationTime</key>
        <real>1687821212.484699</real>
        <key>failedLoginCount</key>
        <integer>0</integer>
        <key>failedLoginTimestamp</key>
        <integer>0</integer>
        <key>passwordLastSetTime</key>
        <real>1687821212.507021</real>
</dict>
</plist>

dsAttrTypeNative:AvatarRepresentation:
dsAttrTypeNative:record_daemon_version: 8780000
dsAttrTypeNative:unlockOptions: 0
AppleMetaNodeLocation: /Local/Default
AuthenticationAuthority: ;SecureToken; ;ShadowHash;HASHLIST:<SALTED-SHA512-PB
LKDC:SHA1.8DCD22811DA43DBA95A290C16E6FAF928CE94D09;
GeneratedUID: 65A093F1-FDBF-4E81-A128-942772AE4EA4
NetworkSignIn:
 2023-06-26 23:13:32 +0000
NetworkUser: ts@jamfse.io
NFSHomeDirectory: /Users/ts
OIDCProvider: Azure
Password: ********
Picture:
 /Library/User Pictures/Fun/Fortune Cookie.heic
PrimaryGroupID: 20
RealName:
 Trade Show
RecordName: ts
RecordType: dsRecTypeStandard:Users
UniqueID: 502
UserShell: /bin/zsh
```

jamf

dseditgroup

It says “edit” in the name so that must be all it does, right?

```
dseditgroup -o read admin
```

```
dsAttrTypeStandard:GroupMembership -
                root
                jamfManagement
dsAttrTypeStandard:GeneratedUID -
                ABCDEFAB-CDEF-ABCD-EFAB-CDEF00000050
dsAttrTypeStandard:RecordName -
                admin
                BUILTIN\Administrators
dsAttrTypeStandard:AppleMetaNodeLocation -
                /Local/Default
dsAttrTypeStandard:GroupMembers -
                FFFFEEEE-DDDD-CCCC-BBBB-AAAA00000000
                2C651619-AB7D-4E29-90B5-D1C817E06D24
dsAttrTypeStandard:RecordType -
                dsRecTypeStandard:Groups
dsAttrTypeStandard:SMBSID -
                S-1-5-32-544
dsAttrTypeStandard:PrimaryGroupID -
                80
dsAttrTypeStandard:RealName -
                Administrators
dsAttrTypeStandard:Password -
                *
```

List all local groups

```
dscacheutil -q group
```

jamf

dseditgroup

It says “edit” in the name so that must be all it does, right?

```
dseditgroup -o read admin
```

Check if an individual user is an admin or not

```
dseditgroup -m "$user" -o checkmember admin
```

```
yes sean.rabbitt is a member of admin
no ts is NOT a member of admin
```

dseditgroup

It says “edit” in the name so that must be all it does, right?

```
dseditgroup -o read admin
```

Check if an individual user is an admin or not

```
dseditgroup -m "$user" -o checkmember admin
```

```
yes sean.rabbitt is a member of admin
no ts is NOT a member of admin
```

```
echo "Demoting $elevateThisUser to standard account"
/usr/sbin/dseditgroup -o edit -d "$elevateThisUser" -t user admin
echo "Elevating $elevateThisUser to admin account"
/usr/sbin/dseditgroup -o edit -a "$elevateThisUser" -t user admin
```

Changing a user's local password

Or, why do I need four different ways to accomplish the same thing?

```
dscl . -passwd /Users/$user [new_password | old_password new_password]
```

```
passwd
```

```
pwpolicy -a authenticator -u user -setpassword newpassword
```

```
sysadminctl -newPassword <new password> -oldPassword <old password> [-passwordHint <password hint>]
```

```
sysadminctl -resetPasswordFor <local user name>
 -newPassword <new password>
 [-passwordHint <password hint>]
 (interactive] || -adminUser <administrator user name> -adminPassword <administrator password>)
```

jamf

sysadminctl

The command line tool that gets jammed full of stuff when nobody knows where else to put it.

- User - Create / Delete
- Password - Set / Force Reset
- FileVault secure token - Enable / Disable / Status
- Auto-login - Enable / Disable / Status
- Guest accounts - Enable / Disable / Status
- Samba (SMB) or Apple Filing Protocol (AFP) guest access - Enable / Disable / Status

sysadminctl

The command line tool that gets jammed full of stuff when nobody knows where else to put it.

- User - Create / Delete
- Password - Set / Force Reset
- FileVault secure token - Enable / Disable / Status
- Auto-login - Enable / Disable / Status
- Guest accounts - Enable / Disable / Status
- Samba (SMB) or Apple Filing Protocol (AFP) guest access - Enable / Disable / Status
- Automatic Time (?!?) - Enable / Disable / Status (but not which NTP server, thats in /etc/ntp.conf)
- File System encryption - Status
- Screen Lock - Status OR disable / seconds to enable with local admin password required

pwpolicy

Wait, it does more than reset passwords?

```
pwpolicy -a authenticator -u user -setpassword newpassword
```

Disable a local user from logging in

```
pwpolicy -u user -disableuser
```

```
pwpolicy -u user -enableuser
```

Do something terrible and set a local account policy manually

```
pwpolicy -u user -setpolicy "minChars=4 maxFailedLoginAttempts=3"
```

Clear account policies (aka set it back to 4 character minimum requirement)

```
pwpolicy -clearaccountpolicies
```

pwpolicy

Wait, it does more than reset passwords?

```
pwpolicy -a authenticator -u user -setpassword newpassword
```

Disable a local user from logging in

```
pwpolicy -u user -disableuser
```

```
pwpolicy -u user -enableuser
```

Do something terrible and set a local account policy manually

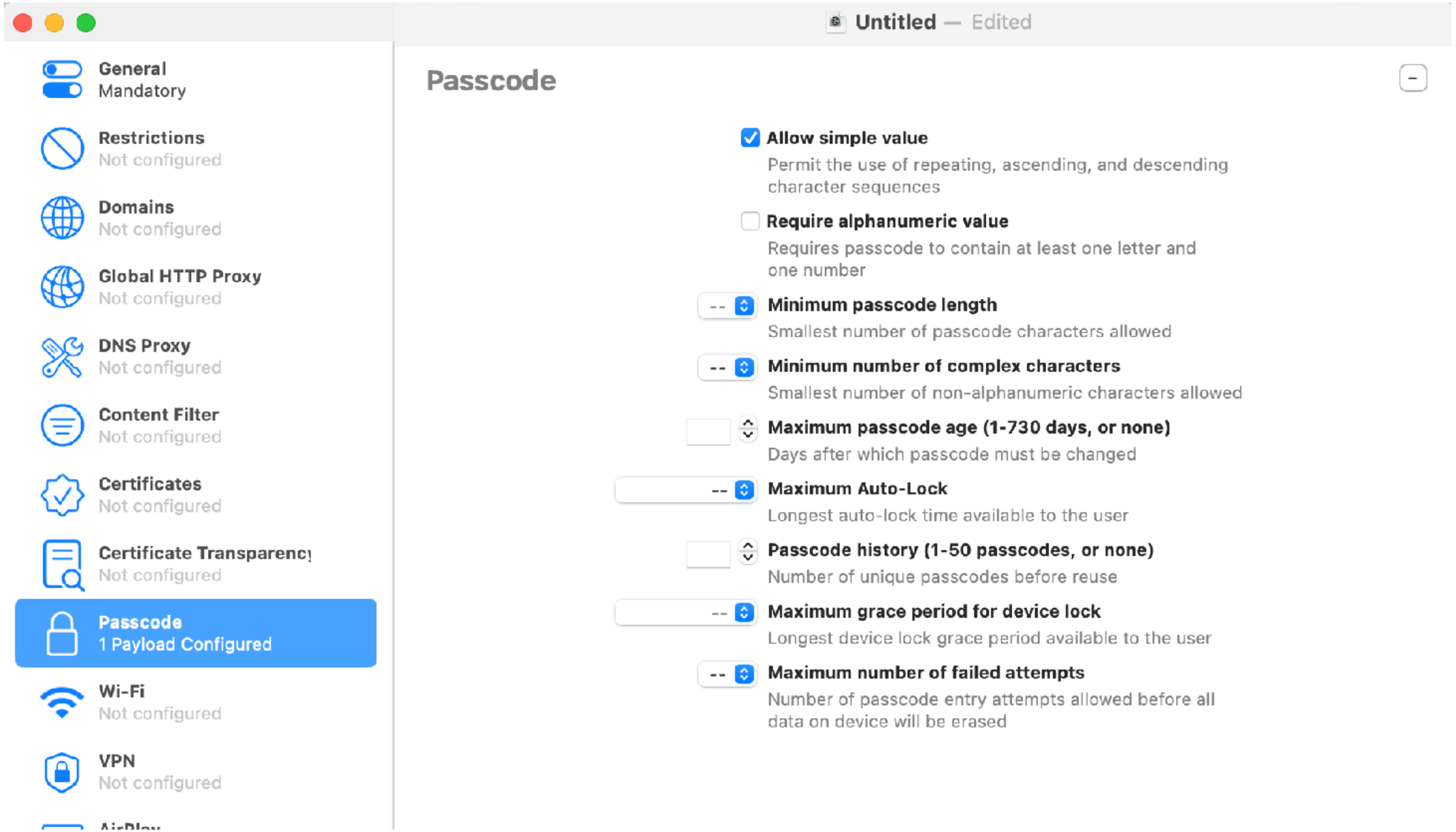
```
pwpolicy -u user -setpolicy "minChars=4 maxFailedLoginAttempts=3"
```

Clear account policies (aka set it back to 4 character minimum requirement)

```
pwpolicy -clearaccountpolicies
```

*

Pushing settings via MDM…

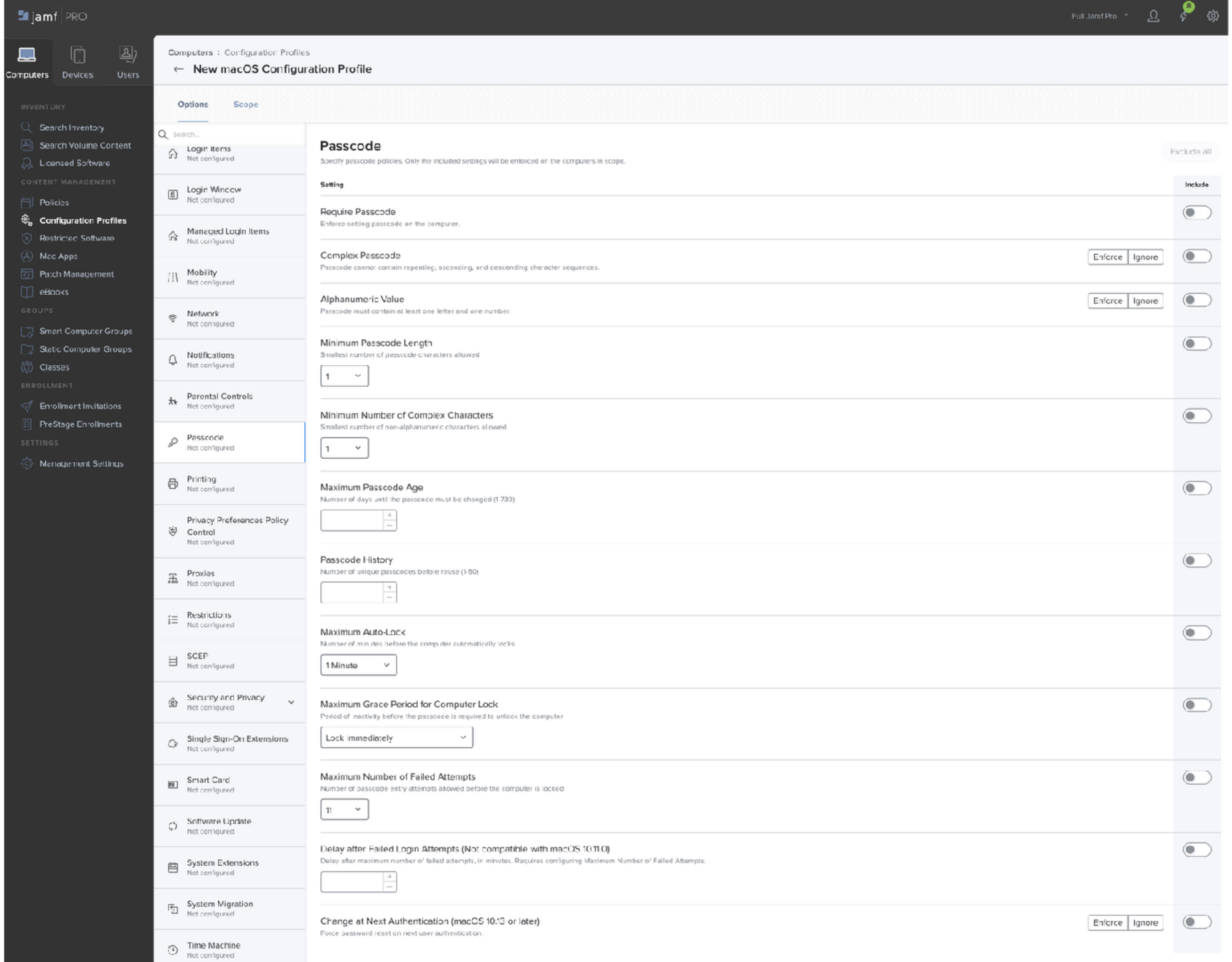


jamf

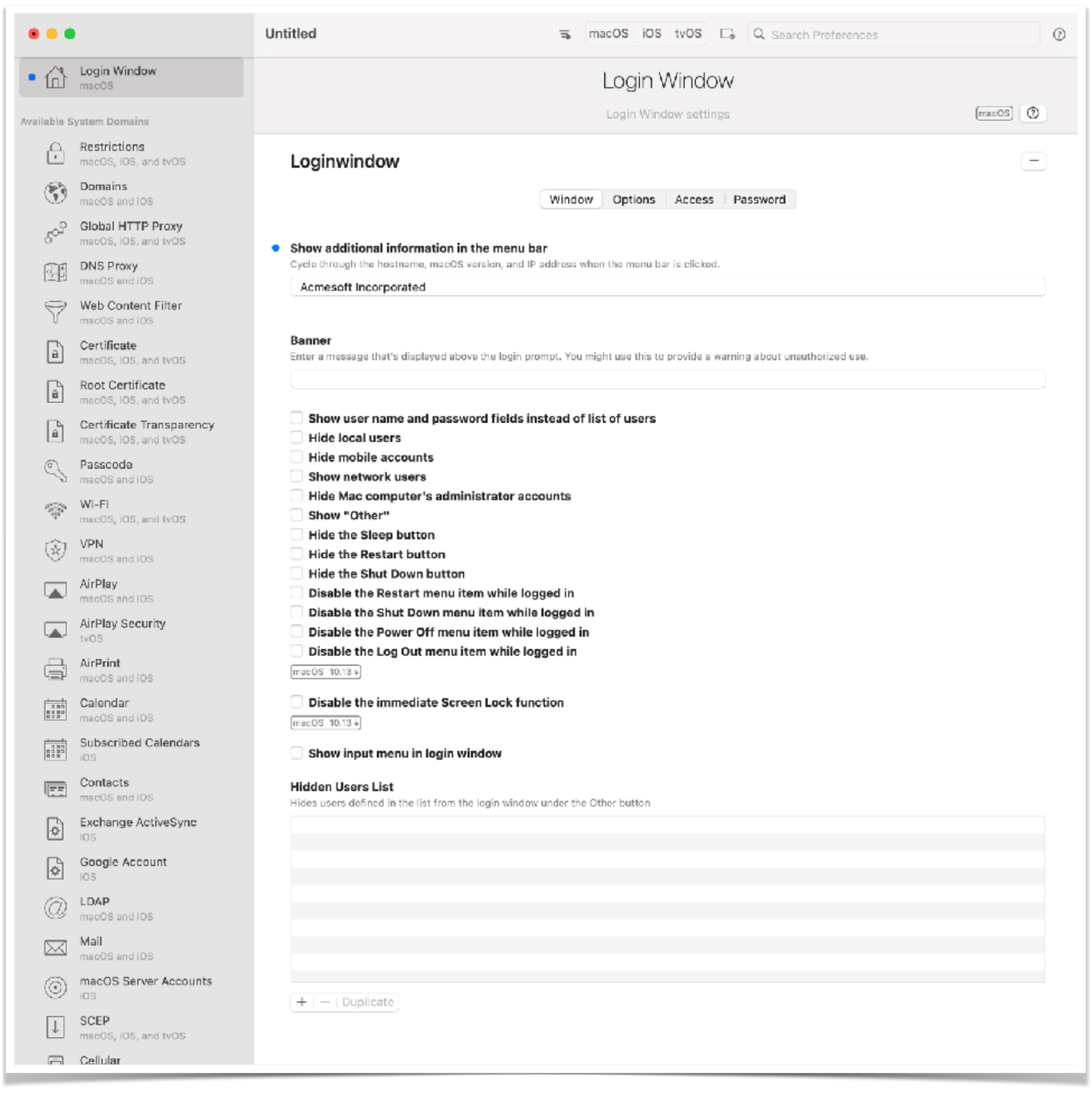
Pushing settings via MDM…

Unscoping or removing a profile does not remove the password policy from the device.

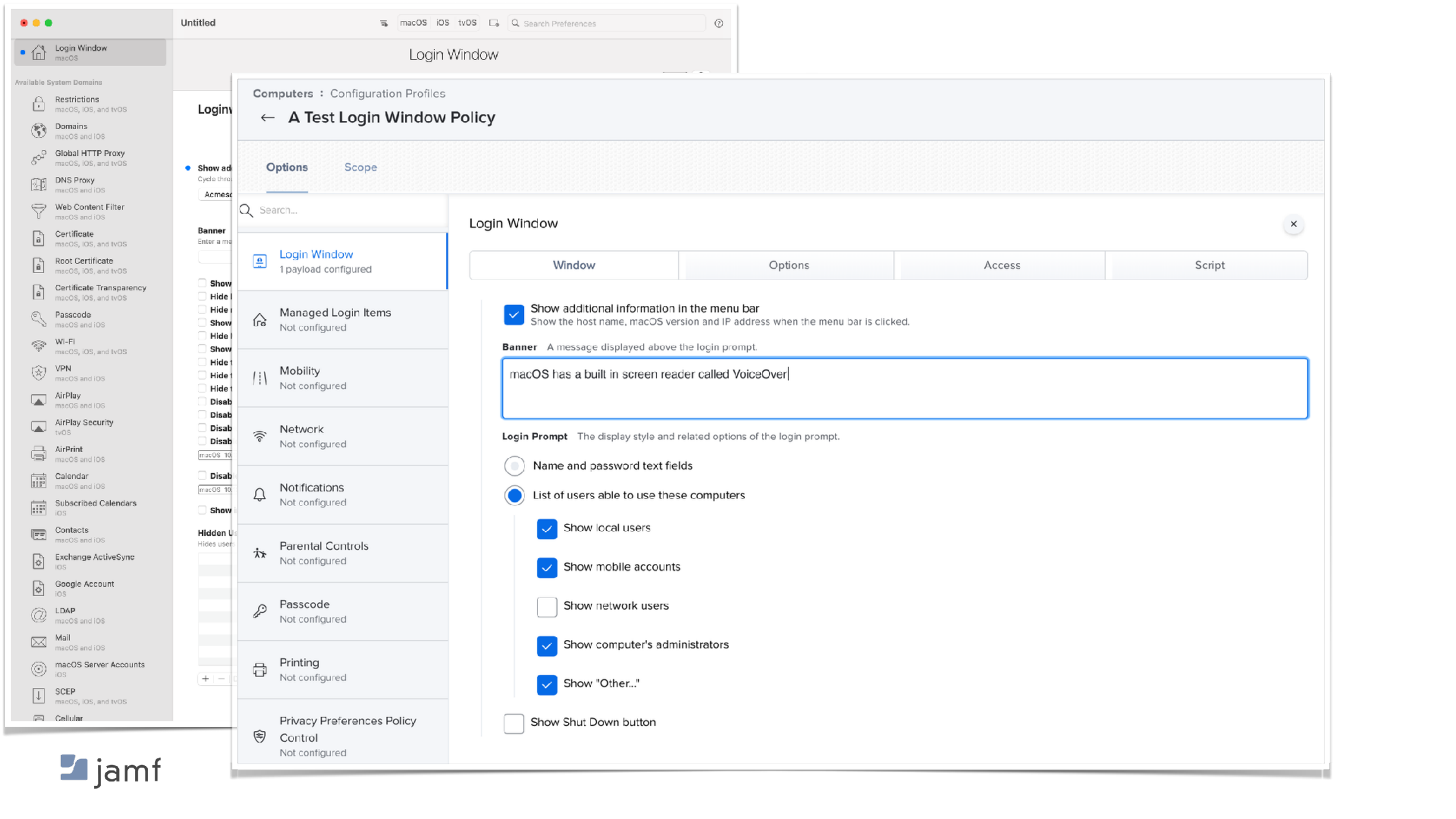
```
pwpolicy -clearaccountpolicies
```


jamf PRO
Full Jamf Pro
Computers
Devices
Users
INVENTORY
Search Inventory
Search Volume Content
Licensed Software
CONTENT MANAGEMENT
Policies
Configuration Profiles
Restricted Software
Mac Apps
Patch Management
eBooks
GROUPS
Smart Computer Groups
Static Computer Groups
Classes
ENROLLMENT
Enrollment Invitations
PreStage Enrollments
SETTINGS
Management Settings
Computers : Configuration Profiles
New macOS Configuration Profile
Options
Scope
Search...
Login Items
Not configured
Login Window
Not configured
Managed Login Items
Not configured
Mobility
Not configured
Network
Not configured
Notifications
Not configured
Parental Controls
Not configured
Passcode
Not configured
Printing
Not configured
Privacy Preferences Policy Control
Not configured
Proxies
Not configured
Restrictions
Not configured
SCEP
Not configured
Security and Privacy
Not configured
Single Sign-On Extensions
Not configured
Smart Card
Not configured
Software Update
Not configured
System Extensions
Not configured
System Migration
Not configured
Time Machine
Not configured
Passcode
Specify passcode policies. Only the included settings will be enforced on the computers in scope.
Exclude all
Setting
Include
Require Passcode
Enforce setting passcode on the computer.
Complex Passcode
Passcode cannot contain repeating, ascending, and descending character sequences.
Enforce
Ignore
Alphanumeric Value
Passcode must contain at least one letter and one number.
Enforce
Ignore
Minimum Passcode Length
Smallest number of passcode characters allowed
1
Minimum Number of Complex Characters
Smallest number of non-alphanumeric characters allowed
1
Maximum Passcode Age
Number of days until the passcode must be changed (1-730)
Passcode History
Number of unique passcodes before reuse (1-50)
Maximum Auto-Lock
Number of minutes before the computer automatically locks
1 Minute
Maximum Grace Period for Computer Lock
Period of inactivity before the passcode is required to unlock the computer
Lock immediately
Maximum Number of Failed Attempts
Number of passcode entry attempts allowed before the computer is locked
11
Delay after Failed Login Attempts (Not compatible with macOS 10.11.0)
Delay after maximum number of failed attempts, in minutes. Requires configuring Maximum Number of Failed Attempts.
Change at Next Authentication (macOS 10.13 or later)
Force password reset on next user authentication.
Enforce
Ignore

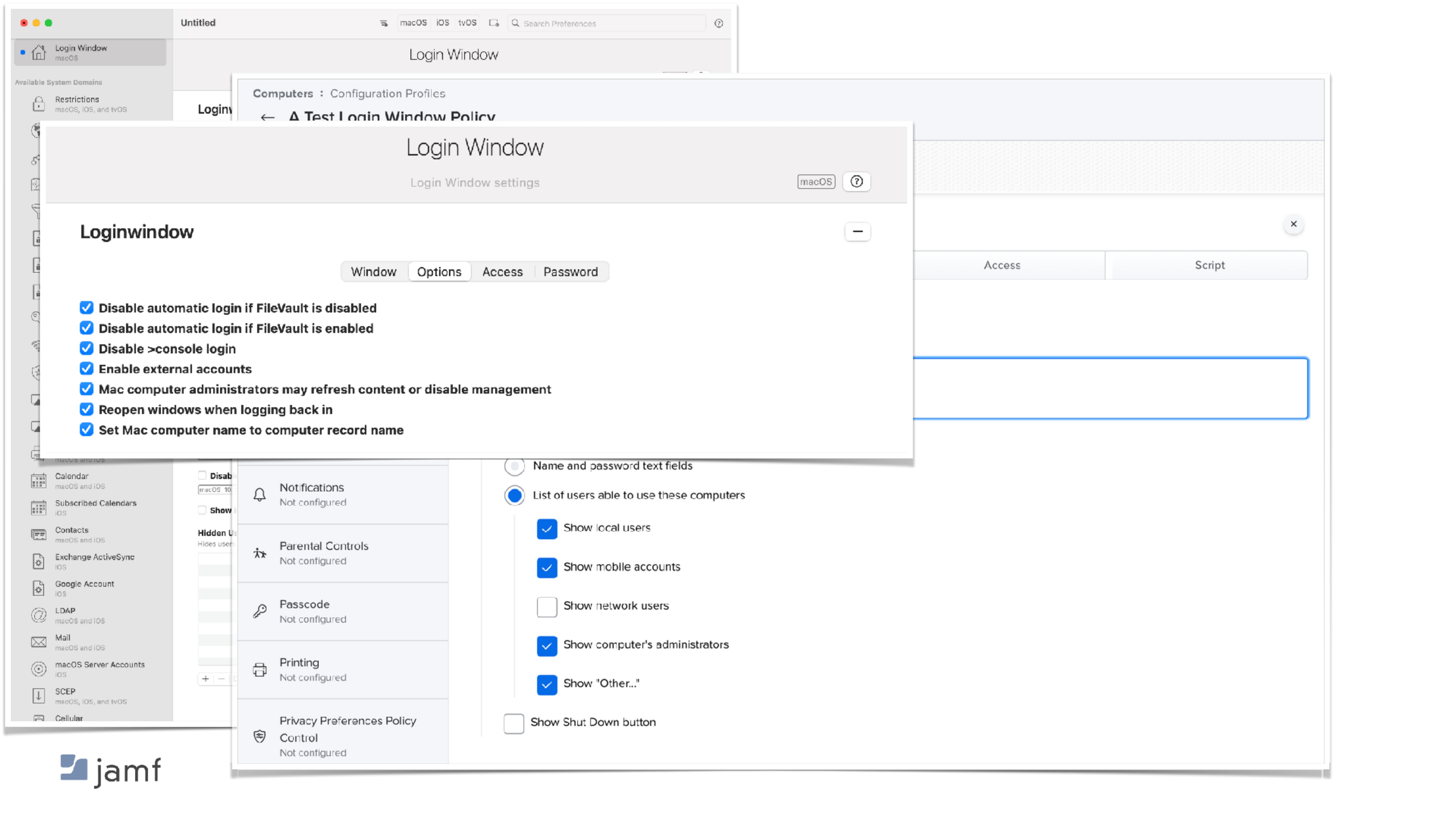
jamf


Untitled
macOS iOS tvOS
Search Preferences
Login Window
macOS
Available System Domains
Restrictions
macOS, iOS, and tvOS
Domains
macOS and iOS
Global HTTP Proxy
macOS, iOS, and tvOS
DNS Proxy
macOS and iOS
Web Content Filter
macOS and iOS
Certificate
macOS, iOS, and tvOS
Root Certificate
macOS, iOS, and tvOS
Certificate Transparency
macOS, iOS, and tvOS
Passcode
macOS and iOS
Wi-Fi
macOS, iOS, and tvOS
VPN
macOS and iOS
AirPlay
macOS and iOS
AirPlay Security
tvOS
AirPrint
macOS and iOS
Calendar
macOS and iOS
Subscribed Calendars
iOS
Contacts
macOS and iOS
Exchange ActiveSync
iOS
Google Account
iOS
LDAP
macOS and iOS
Mail
macOS and iOS
macOS Server Accounts
iOS
SCEP
macOS, iOS, and tvOS
Cellular
Login Window
Login Window settings
macOS
Loginwindow
Window
Options
Access
Password
Show additional information in the menu bar
Cycle through the hostname, macOS version, and IP address when the menu bar is clicked.
Acmesoft Incorporated
Banner
Enter a message that's displayed above the login prompt. You might use this to provide a warning about unauthorized use.
Show user name and password fields instead of list of users
Hide local users
Hide mobile accounts
Show network users
Hide Mac computer's administrator accounts
Show "Other"
Hide the Sleep button
Hide the Restart button
Hide the Shut Down button
Disable the Restart menu item while logged in
Disable the Shut Down menu item while logged in
Disable the Power Off menu item while logged in
Disable the Log Out menu item while logged in
macOS 10.13+
Disable the immediate Screen Lock function
macOS 10.13+
Show input menu in login window
Hidden Users List
Hides users defined in the list from the login window under the Other button
Duplicate

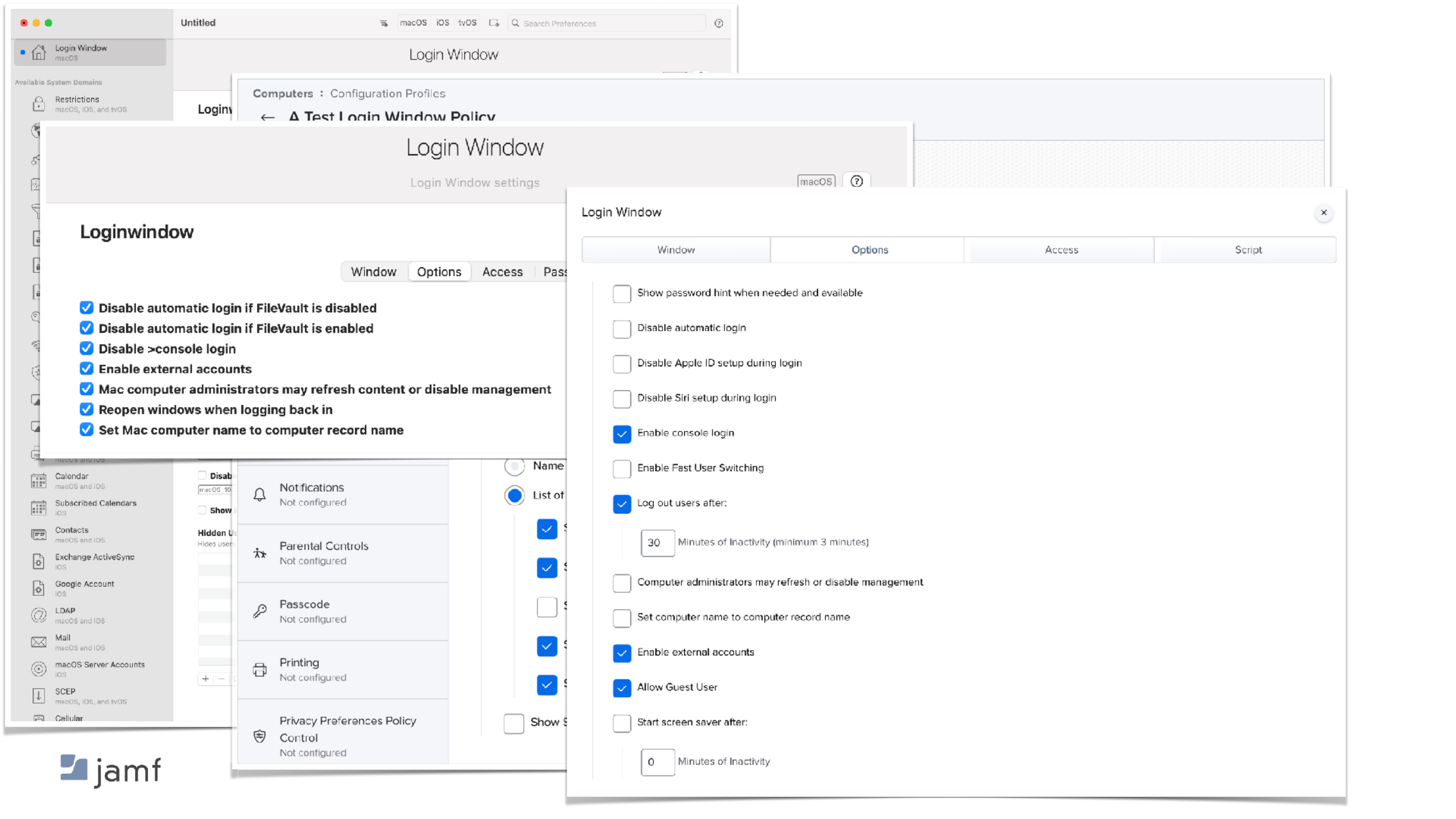
jamf


Untitled
macOS iOS tvOS
Search Preferences
Login Window
macOS
Available System Domains
Restrictions
macOS, iOS, and tvOS
Domains
macOS and iOS
Global HTTP Proxy
macOS, iOS, and tvOS
DNS Proxy
macOS and iOS
Web Content Filter
macOS and iOS
Certificate
macOS, iOS, and tvOS
Root Certificate
macOS, iOS, and tvOS
Certificate Transparency
macOS, iOS, and tvOS
Passcode
macOS and iOS
Wi-Fi
macOS, iOS, and tvOS
VPN
macOS and iOS
AirPlay
macOS and iOS
AirPlay Security
tvOS
AirPrint
macOS and iOS
Calendar
macOS and iOS
Subscribed Calendars
iOS
Contacts
macOS and iOS
Exchange ActiveSync
iOS
Google Account
iOS
LDAP
macOS and iOS
Mail
macOS and iOS
macOS Server Accounts
iOS
SCEP
macOS, iOS, and tvOS
Cellular
Computers : Configuration Profiles
A Test Login Window Policy
Options
Scope
Search...
Login Window
1 payload configured
Managed Login Items
Not configured
Mobility
Not configured
Network
Not configured
Notifications
Not configured
Parental Controls
Not configured
Passcode
Not configured
Printing
Not configured
Privacy Preferences Policy Control
Not configured
Login Window
Window
Options
Access
Script
Show additional information in the menu bar
Show the host name, macOS version and IP address when the menu bar is clicked.
Banner A message displayed above the login prompt.
macOS has a built in screen reader called VoiceOver
Login Prompt The display style and related options of the login prompt.
Name and password text fields
List of users able to use these computers
Show local users
Show mobile accounts
Show network users
Show computer's administrators
Show "Other..."
Show Shut Down button

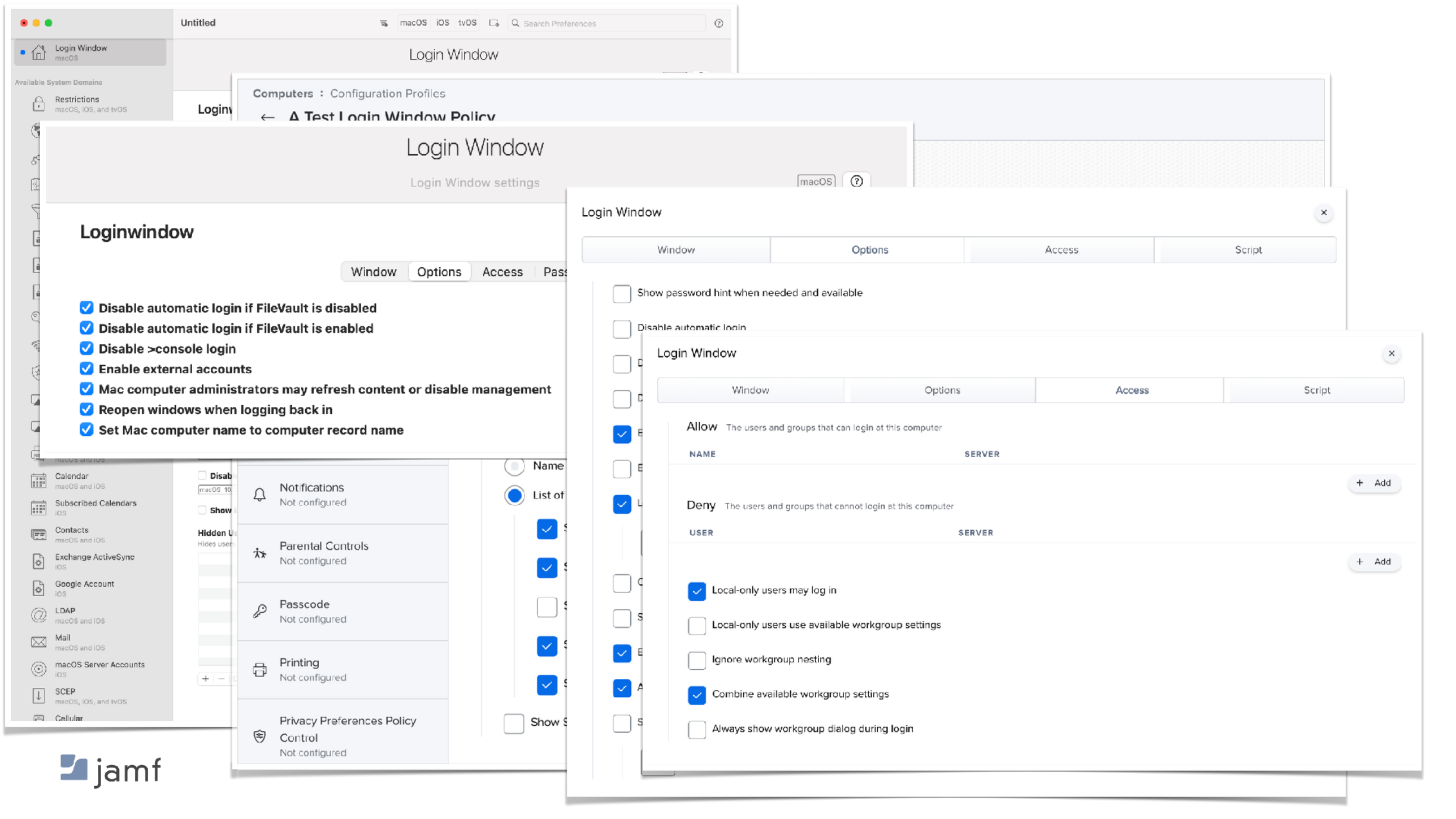
jamf


Untitled
macOS iOS tvOS
Search Preferences
Login Window
macOS
Available System Domains
Restrictions
macOS, iOS, and tvOS
Computers : Configuration Profiles
Login Window
Login Window settings
macOS
Loginwindow
Window Options Access Password
Disable automatic login if FileVault is disabled
Disable automatic login if FileVault is enabled
Disable >console login
Enable external accounts
Mac computer administrators may refresh content or disable management
Reopen windows when logging back in
Set Mac computer name to computer record name
Access
Script
Calendar
macOS and iOS
Subscribed Calendars
iOS
Contacts
macOS and iOS
Exchange ActiveSync
iOS
Google Account
iOS
LDAP
macOS and iOS
Mail
macOS and iOS
macOS Server Accounts
iOS
SCEP
macOS, iOS, and tvOS
Cellular
Notifications
Not configured
Parental Controls
Not configured
Passcode
Not configured
Printing
Not configured
Privacy Preferences Policy Control
Not configured
Name and password text fields
List of users able to use these computers
Show local users
Show mobile accounts
Show network users
Show computer's administrators
Show "Other..."
Show Shut Down button

jamf


Untitled
macOS iOS tvOS
Search Preferences
Login Window
macOS
Available System Domains
Restrictions
macOS, iOS, and tvOS
Computers : Configuration Profiles
Login Window
Login Window settings
macOS
Loginwindow
Window
Options
Access
Disable automatic login if FileVault is disabled
Disable automatic login if FileVault is enabled
Disable >console login
Enable external accounts
Mac computer administrators may refresh content or disable management
Reopen windows when logging back in
Set Mac computer name to computer record name
Login Window
Window
Options
Access
Script
Show password hint when needed and available
Disable automatic login
Disable Apple ID setup during login
Disable Siri setup during login
Enable console login
Enable Fast User Switching
Log out users after:
30
Minutes of Inactivity (minimum 3 minutes)
Computer administrators may refresh or disable management
Set computer name to computer record name
Enable external accounts
Allow Guest User
Start screen saver after:
0
Minutes of Inactivity
Notifications
Not configured
Parental Controls
Not configured
Passcode
Not configured
Printing
Not configured
Privacy Preferences Policy Control
Not configured
Calendar
Subscribed Calendars
Contacts
Exchange ActiveSync
Google Account
LDAP
Mail
macOS Server Accounts
SCEP
Cellular

jamf


Untitled
macOS iOS tvOS
Search Preferences
Login Window
macOS
Available System Domains
Restrictions
macOS, iOS, and tvOS
Computers : Configuration Profiles
Login Window
Login Window settings
macOS
Loginwindow
Window
Options
Access
Pass
Disable automatic login if FileVault is disabled
Disable automatic login if FileVault is enabled
Disable >console login
Enable external accounts
Mac computer administrators may refresh content or disable management
Reopen windows when logging back in
Set Mac computer name to computer record name
Notifications
Not configured
Parental Controls
Not configured
Passcode
Not configured
Printing
Not configured
Privacy Preferences Policy Control
Not configured
Calendar
macOS and iOS
Subscribed Calendars
iOS
Contacts
macOS and iOS
Exchange ActiveSync
iOS
Google Account
iOS
LDAP
macOS and iOS
Mail
macOS and iOS
macOS Server Accounts
iOS
SCEP
macOS, iOS, and tvOS
Cellular
Name
List of
Show
Login Window
Window
Options
Access
Script
Show password hint when needed and available
Disable automatic login
Login Window
Window
Options
Access
Script
Allow
The users and groups that can login at this computer
NAME
SERVER
Add
Deny
The users and groups that cannot login at this computer
USER
SERVER
Add
Local-only users may log in
Local-only users use available workgroup settings
Ignore workgroup nesting
Combine available workgroup settings
Always show workgroup dialog during login

jamf

Restrictions

Use this section to configure restrictions on a device. macOS iOS tvOS

Restrictions

General | AirDrop | AirPlay | AirPrint | Apps | Classroom | iCloud | Media | Passwords / Unlock | Siri | Updates

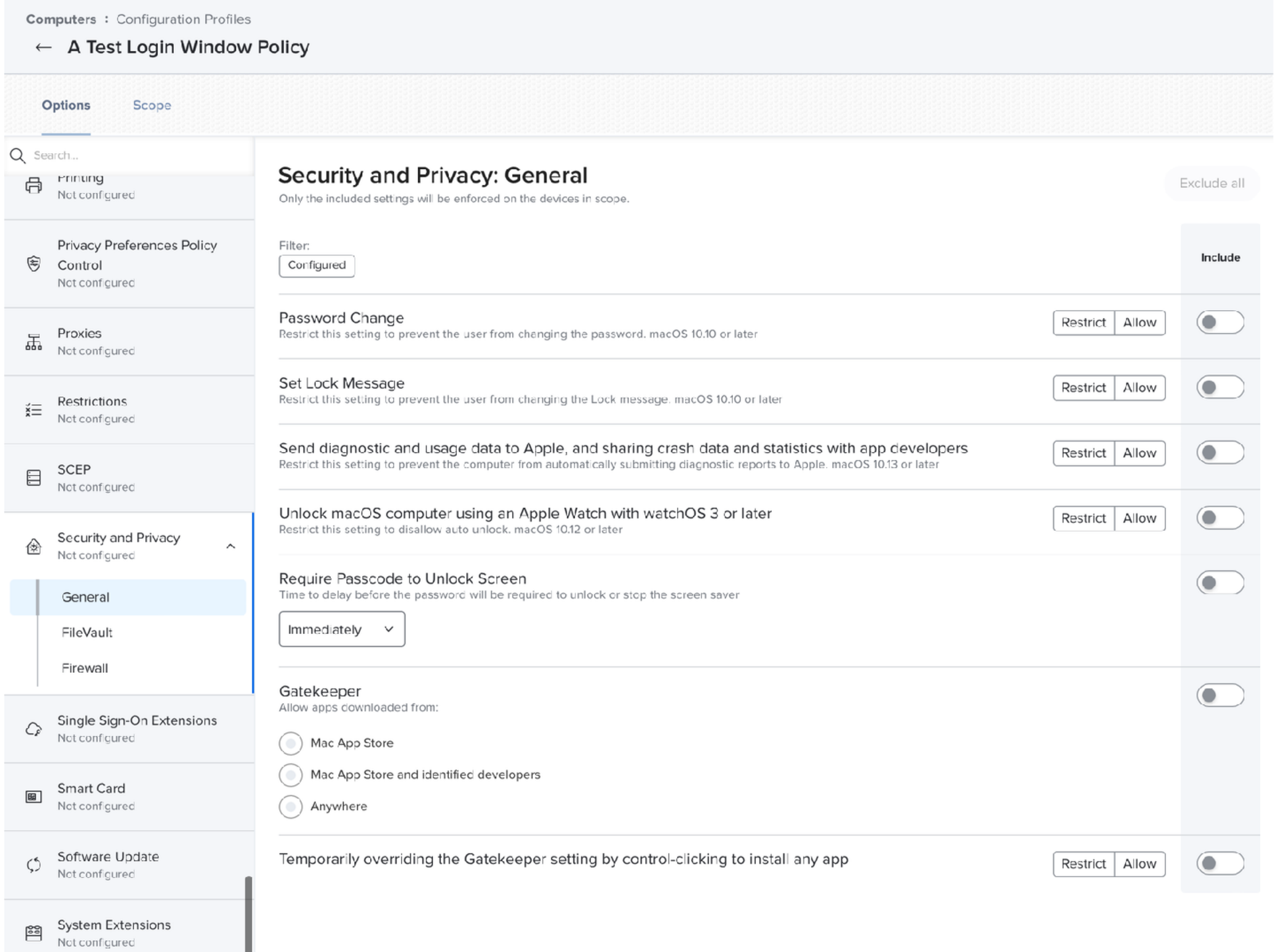
- [x] **Allow modifying passcode**
  Supervised only iOS 9.0+
  - [x] **Allow modifying Touch ID / Face ID**
    Supervised only iOS 9.0+
- [x] **Allow Touch ID / Face ID to unlock device**
  macOS 10.12.4+ iOS 7.0+
- [x] **Allow password autofill**
  Supervised only macOS 10.14+ iOS 12.0+
- [x] **Allow Apple Watch to auto unlock device**
  macOS 10.12+ iOS 14.5+
- [x] **Allow proximity based password sharing requests**
  Supervised only macOS 10.14+ iOS 12.0+ tvOS 12.0+
- [x] **Allow password sharing**
  Supervised only macOS 10.14+ iOS 12.0+

Enforced Fingerprint Timeout
Period of time in seconds after which the device will require entry of password or passcode to unlock.

macOS 12.0+ iOS 15.0+

- [x] **Allow Automatic Screen Saver**
  tvOS 15.4+

jamf


Computers : Configuration Profiles
A Test Login Window Policy
Options
Scope
Search...
Printing
Not configured
Privacy Preferences Policy Control
Not configured
Proxies
Not configured
Restrictions
Not configured
SCEP
Not configured
Security and Privacy
Not configured
General
FileVault
Firewall
Single Sign-On Extensions
Not configured
Smart Card
Not configured
Software Update
Not configured
System Extensions
Not configured
Security and Privacy: General
Only the included settings will be enforced on the devices in scope.
Exclude all
Filter:
Configured
Include
Password Change
Restrict this setting to prevent the user from changing the password. macOS 10.10 or later
Restrict
Allow
Set Lock Message
Restrict this setting to prevent the user from changing the Lock message. macOS 10.10 or later
Restrict
Allow
Send diagnostic and usage data to Apple, and sharing crash data and statistics with app developers
Restrict this setting to prevent the computer from automatically submitting diagnostic reports to Apple. macOS 10.13 or later
Restrict
Allow
Unlock macOS computer using an Apple Watch with watchOS 3 or later
Restrict this setting to disallow auto unlock. macOS 10.12 or later
Restrict
Allow
Require Passcode to Unlock Screen
Time to delay before the password will be required to unlock or stop the screen saver
Immediately
Gatekeeper
Allow apps downloaded from:
Mac App Store
Mac App Store and identified developers
Anywhere
Temporarily overriding the Gatekeeper setting by control-clicking to install any app
Restrict
Allow

jamf

Local User Accounts - Section Summary

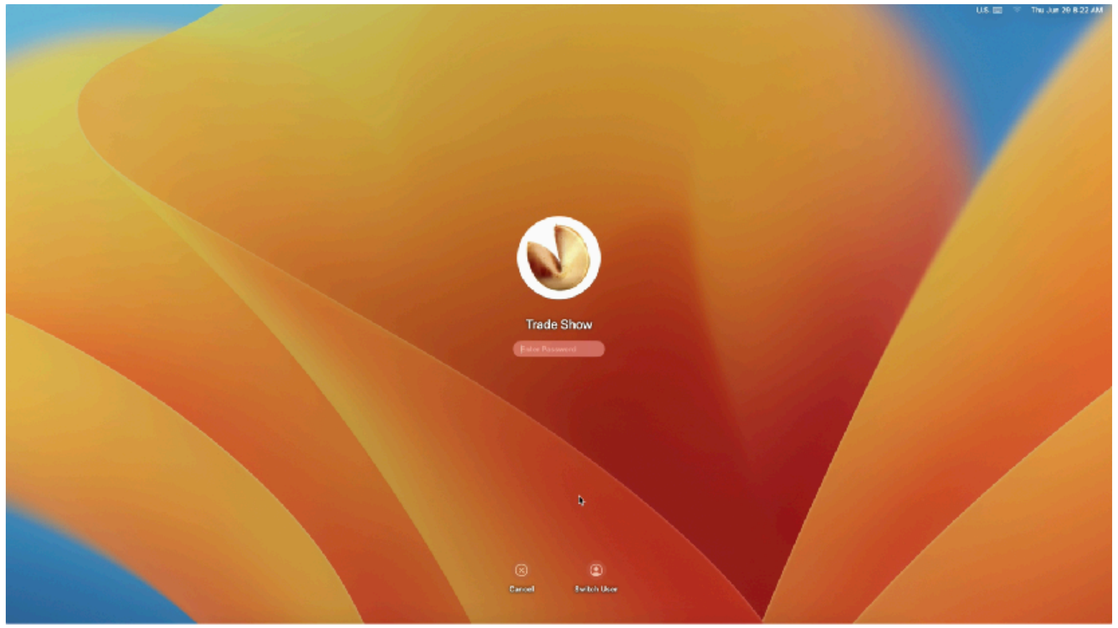
- macOS is UNIX
- Useful commands
  - `dscl`
  - `dseditgroup`
  - `passwd`
  - `pwpolicy`
  - `sysadminctl`

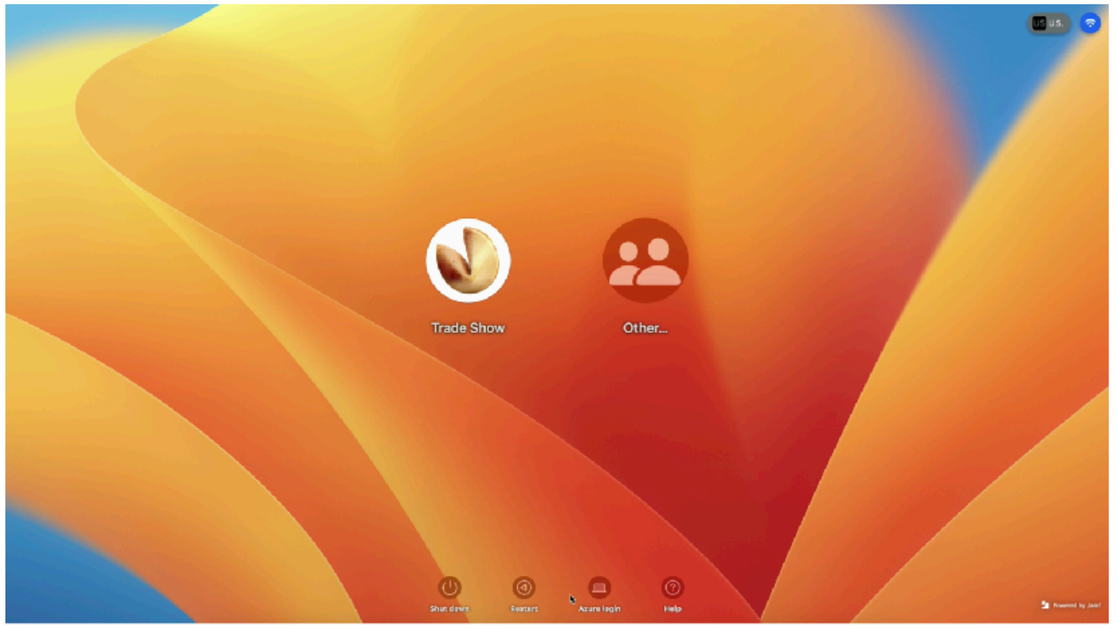
- Unscoping a config profile donna undo a `pwpolicy` applied to machine

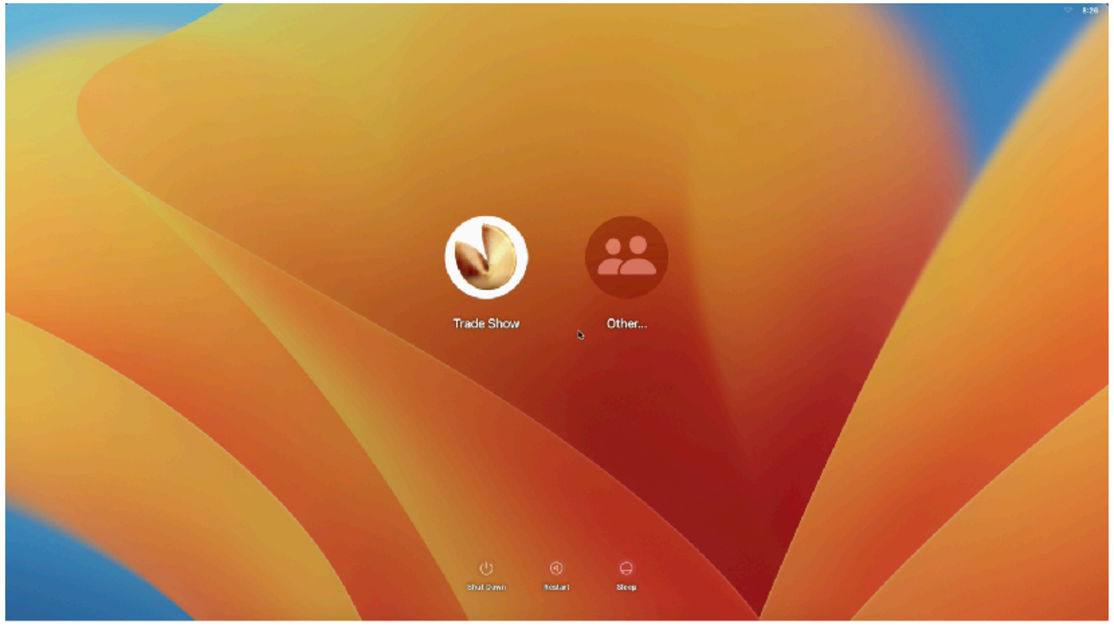
- There are a billion config profile keys spread across a billion payloads

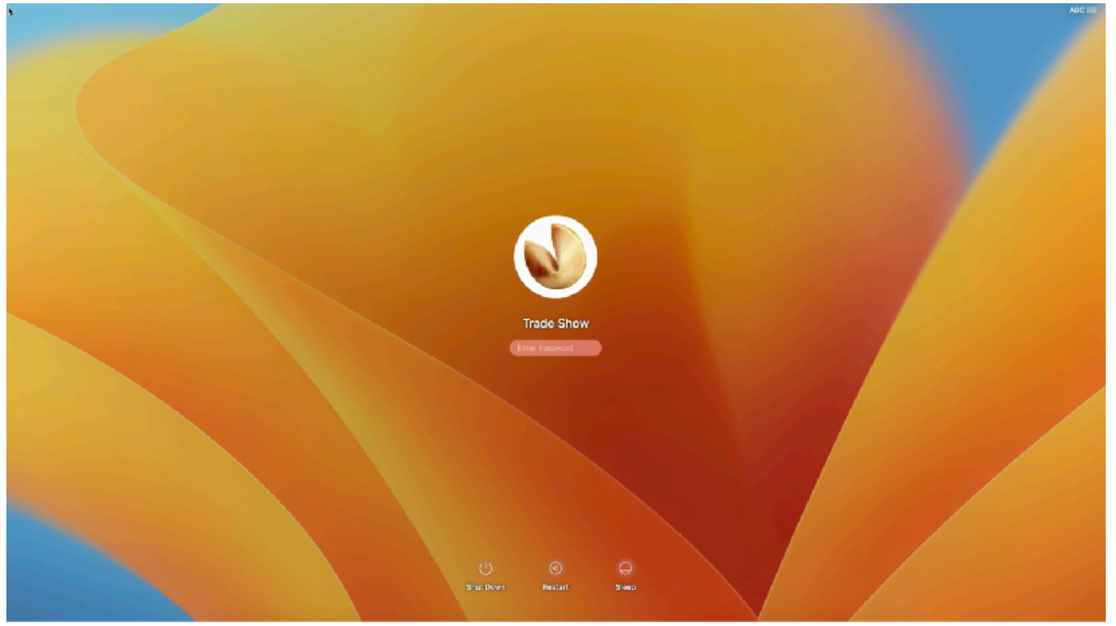
And now for something completely different.

jamf

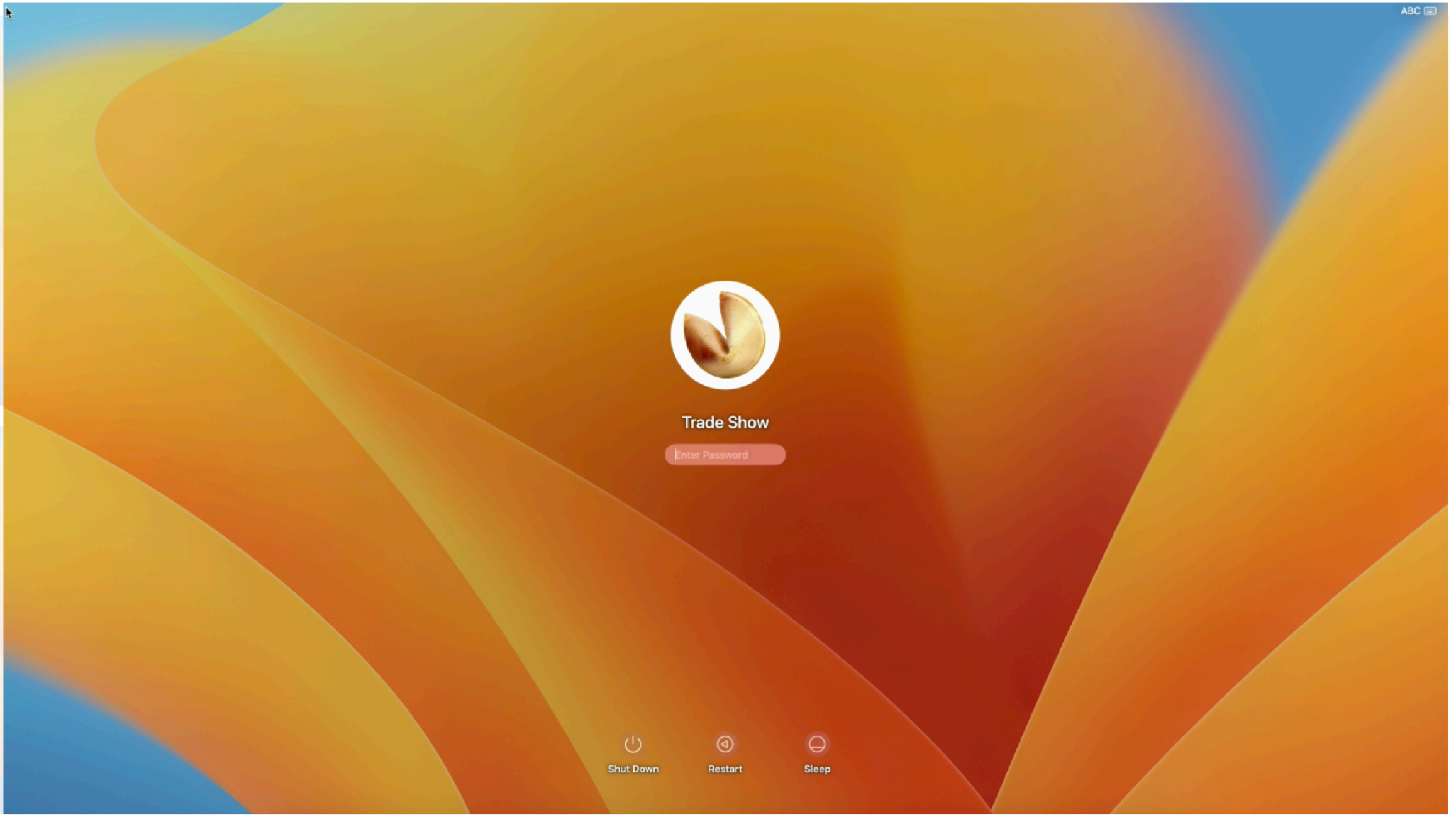

Trade Show
Cancel
Switch User


Trade Show
Other...
Shut down
Restart
Azure login
Help

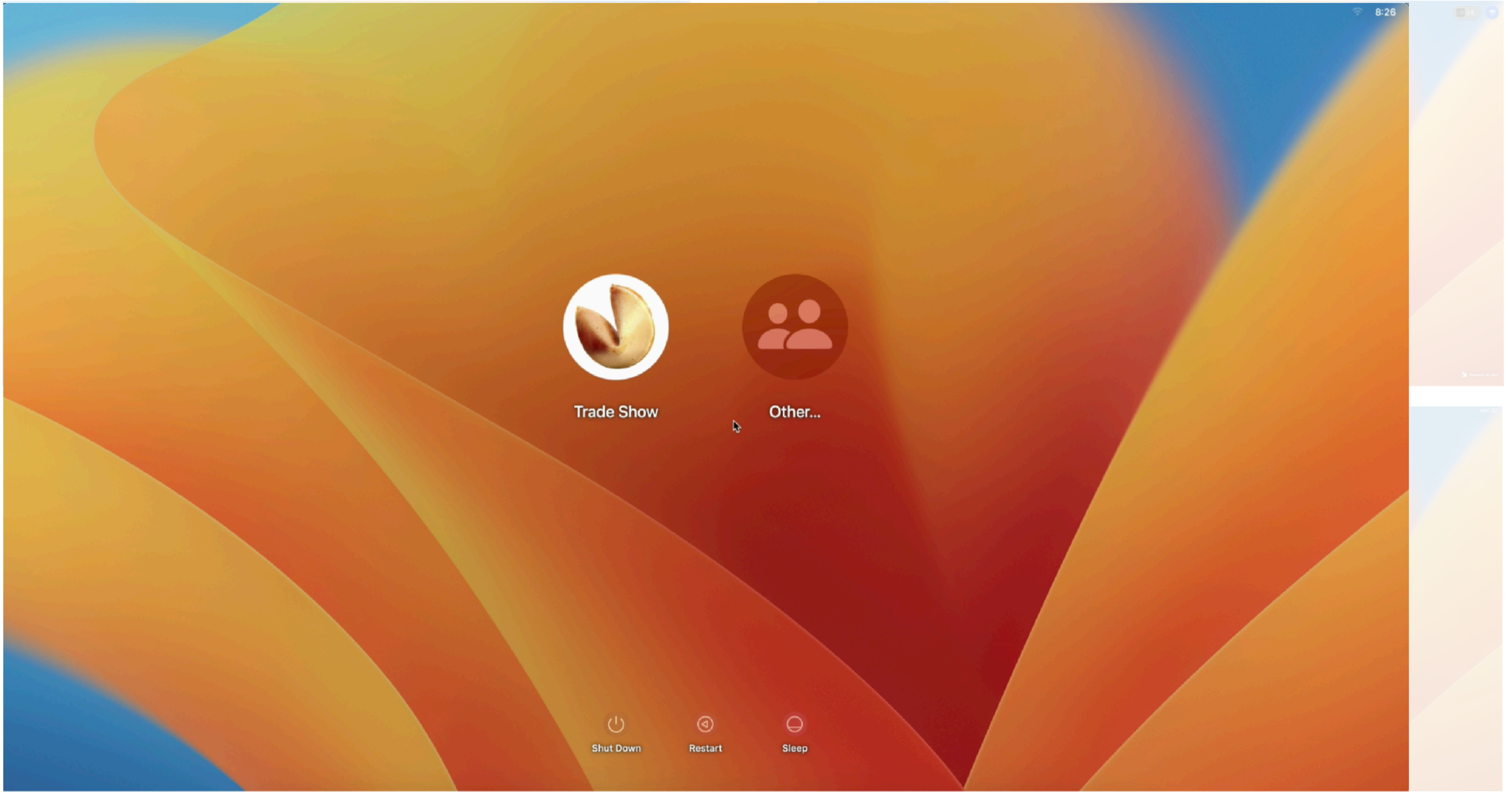

Trade Show
Other...
Shut Down
Restart
Sleep


Trade Show
Shut Down
Restart
Sleep

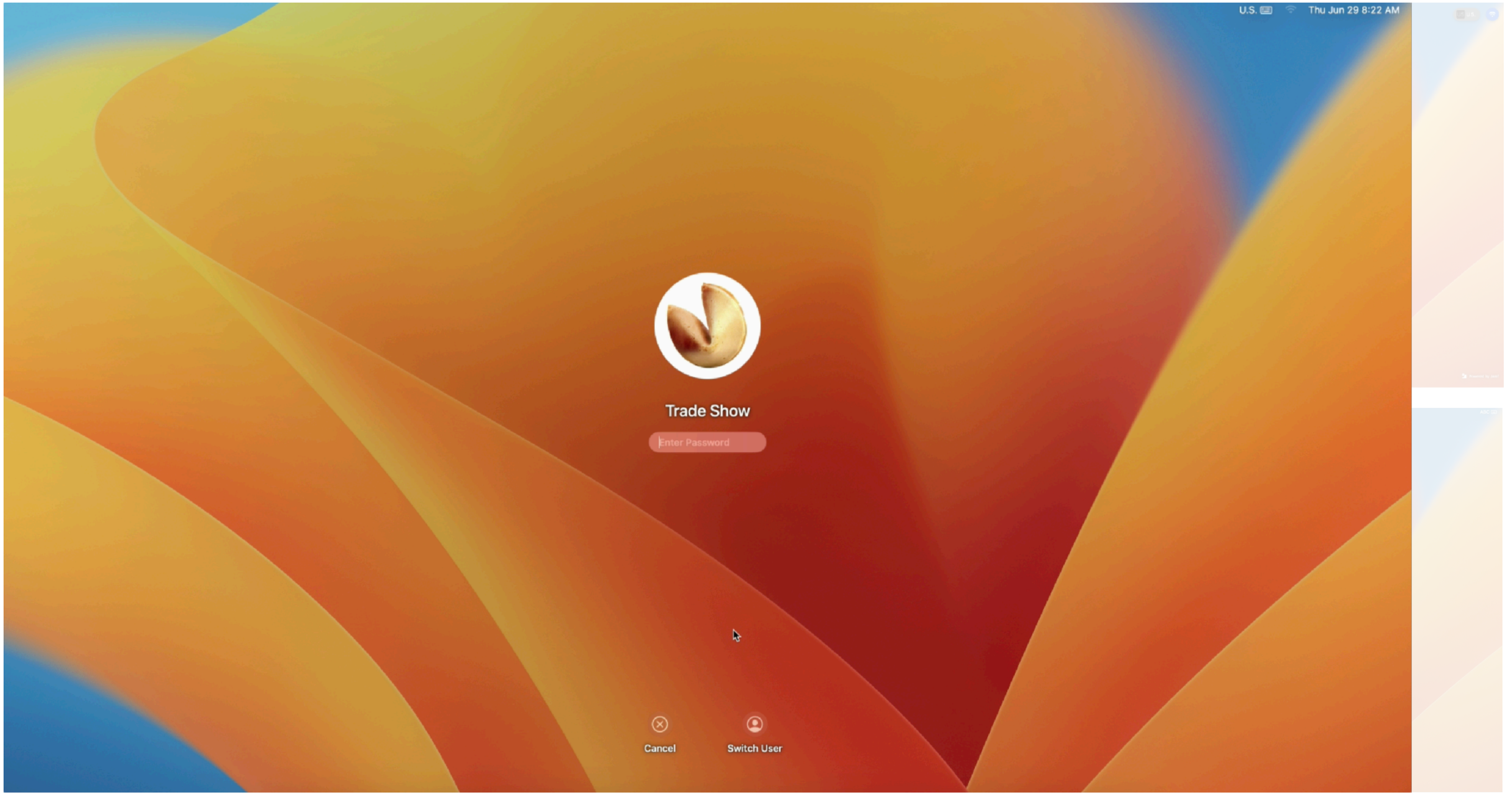
jamf



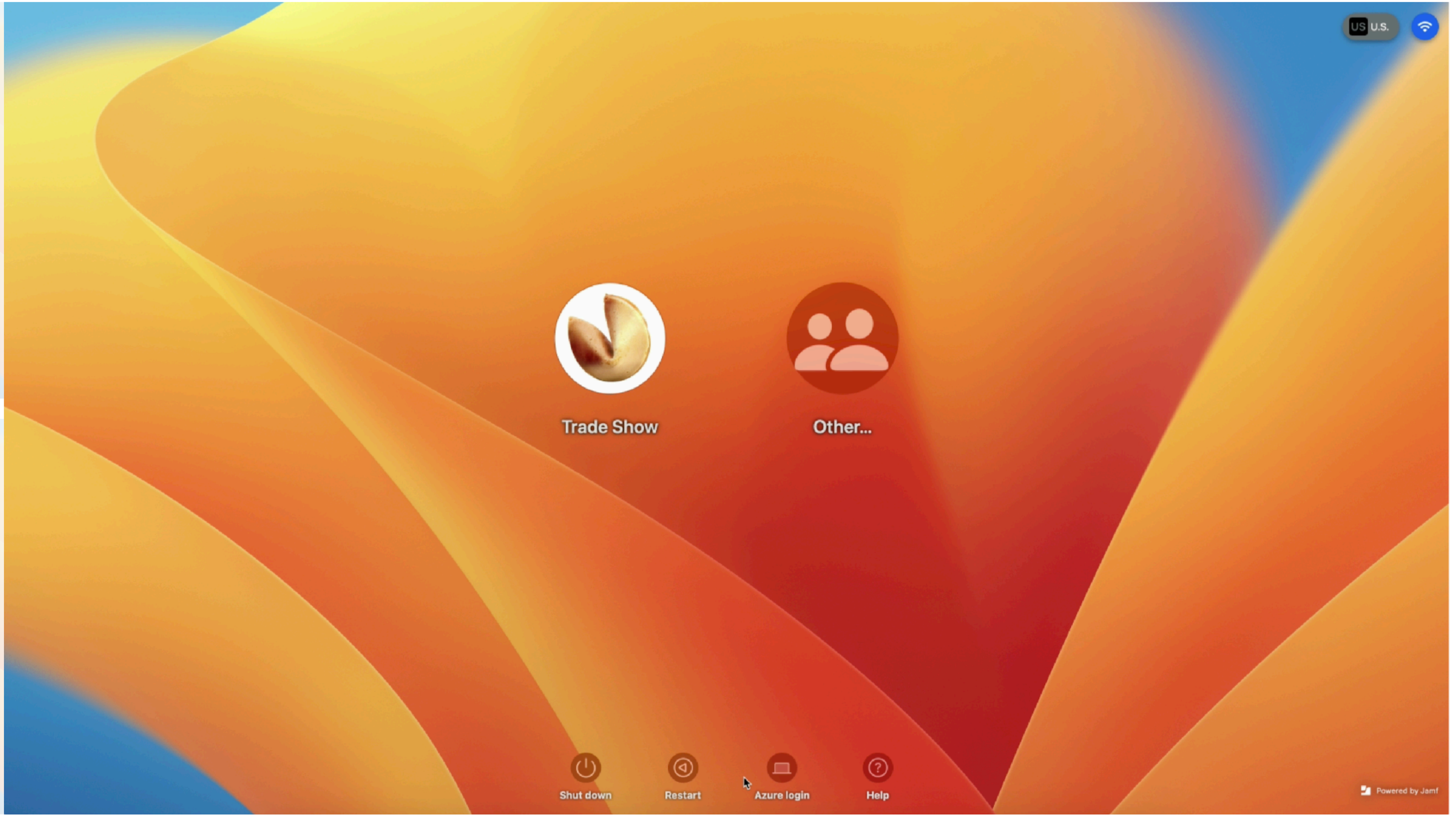
jamf



jamf

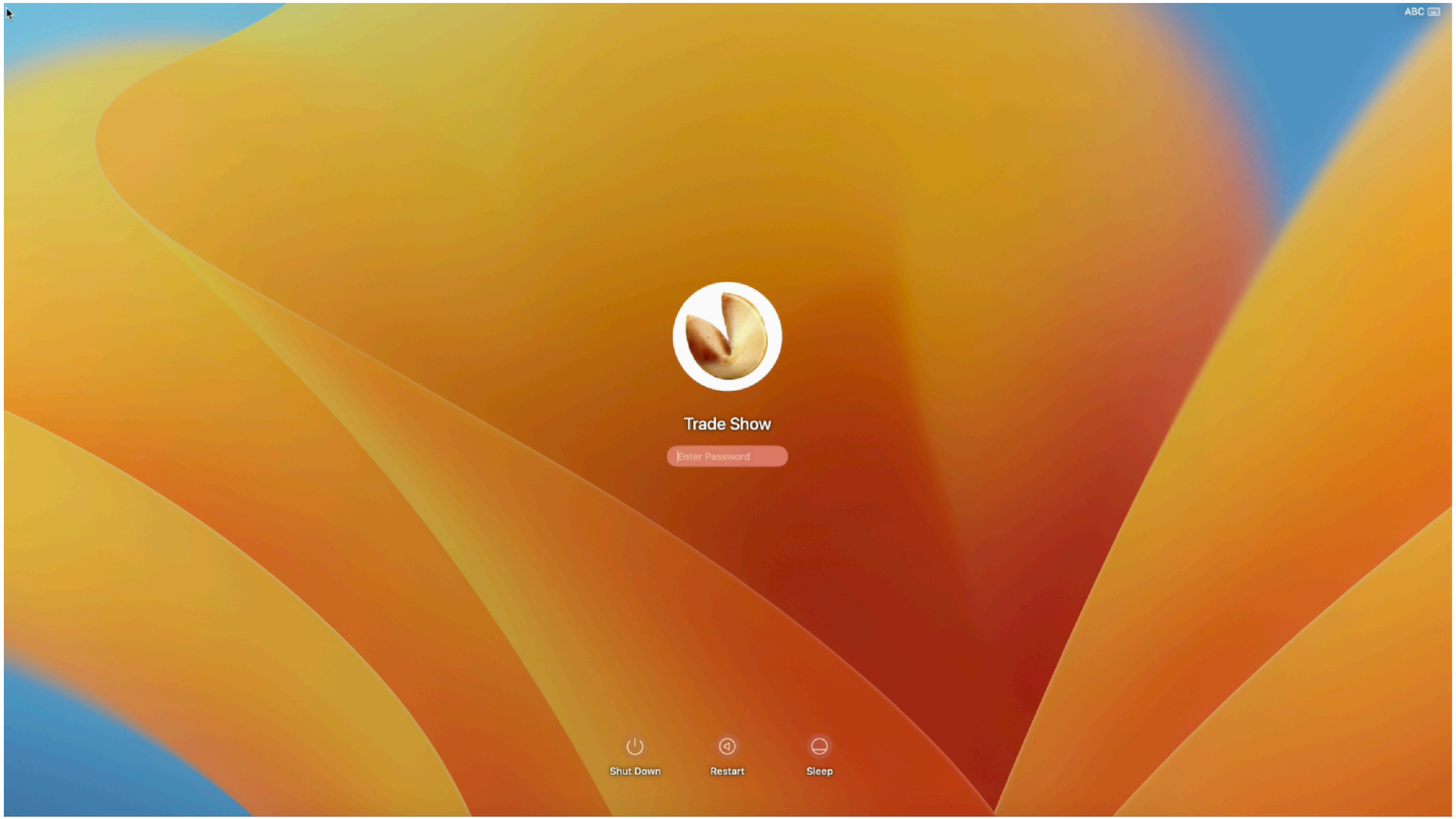

U.S.
Thu Jun 29 8:22 AM
Trade Show
Enter Password
Cancel
Switch User

jamf


US U.S.
Trade Show
Other...
Shut down
Restart
Azure login
Help
Powered by Jamf

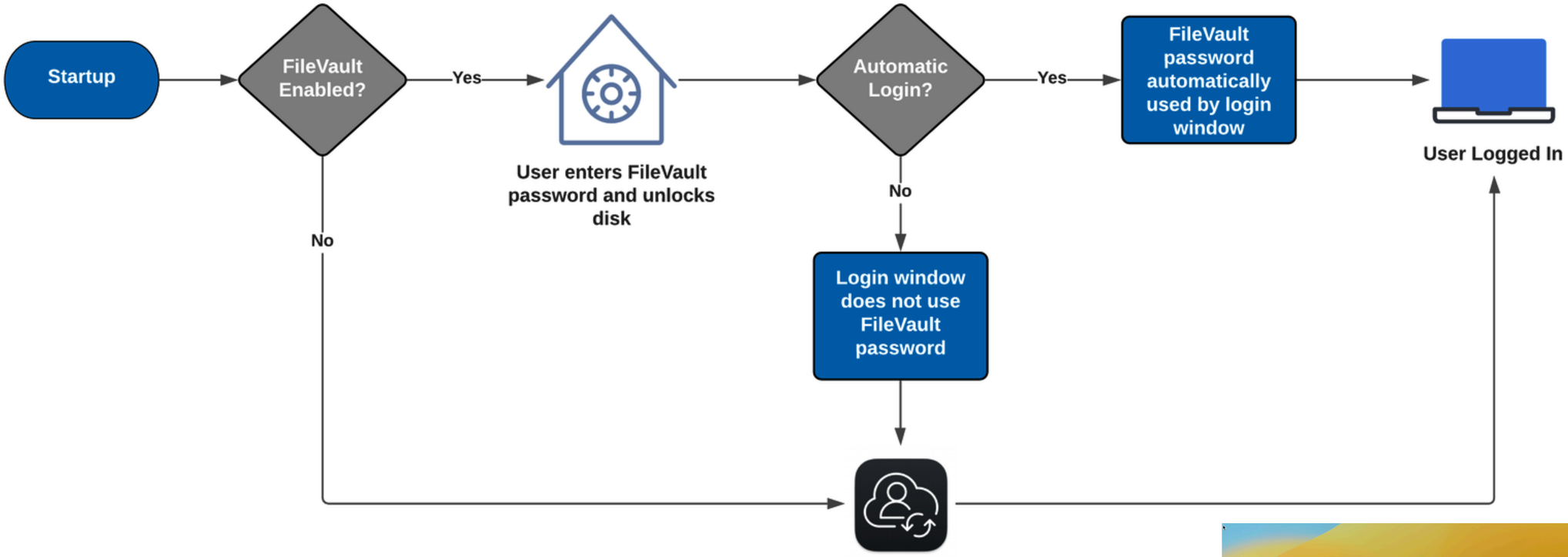
jamf

FileVault, or why you will have a local user account forever

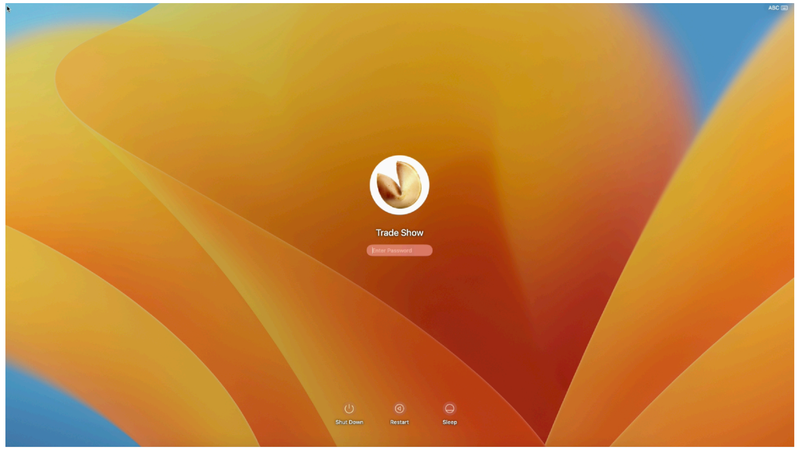


jamf

FileVault, or why you will have a local user account forever



User logs in with
macOS login window, or however
it's been modified by someone



jamf

HCS Technology Group - Resync FileVault Passwords

https://hcsonline.com/support/blog/entry/how-to-fix-out-of-sync-filevault-password

jamf

https://httpbin.dmuth.org/qrcode/

Apple - Resetting a local user password

https://support.apple.com/en-us/HT202860

jamf

https://httpbin.dmuth.org/qrcode/

Apple - Resetting a local user password

Option 3: Reset using your recovery key

1. Click the option to reset using your recovery key.
2. Enter your FileVault recovery key. It's the long string of letters and numbers you received when you turned on FileVault and chose to create a recovery key instead of allowing your iCloud account (Apple ID) to unlock your disk.
3. Enter your new password information, then click Reset Password.

https://support.apple.com/en-us/HT202860

jamf

On-Premises and **Cloud** Directory Services

jamf

<!—content warning—>
<rant>

jamf

On-Premises Directory - Binding your Mac to AD

- Centralized account management
  - Unified password complexity policies
  - Common credentials for all on-premises services

jamf

https://support.apple.com/guide/directory-utility/integrate-active-directory-diru39a25fa2/6.3/mac/13.0

On-Premises Directory - Binding your Mac to AD

- Centralized account management
  - Unified password complexity policies
  - Common credentials for all on-premises services
- User and Machine based certificates
  - Key Distribution Server (KDS) on prem
  - Kerberos ticket for accessing resources

jamf

https://support.apple.com/guide/directory-utility/integrate-active-directory-diru39a25fa2/6.3/mac/13.0

On-Premises Directory - Binding your Mac to AD

- Centralized account management
  - Unified password complexity policies
  - Common credentials for all on-premises services
- User and Machine based certificates
  - Key Distribution Server (KDS) on prem
  - Kerberos ticket for accessing resources
- Mount and traverse DFS namespace
  - Automatic mounting of underlying SMB shares

jamf

https://support.apple.com/guide/directory-utility/integrate-active-directory-diru39a25fa2/6.3/mac/13.0

On-Premises Directory - Binding your Mac to AD

- All users are “Network” accounts

jamf

On-Premises Directory - Binding your Mac to AD

- All users are “Network” accounts
- Some users can be “Mobile” accounts

jamf

On-Premises Directory - Binding your Mac to AD

- All users are “Network” accounts
- Some users can be “Mobile” accounts
- But everyone is still also a local account, so….

On-Premises Directory - Binding your Mac to AD

- All users are “Network” accounts
- Some users can be “Mobile” accounts
- But everyone is still also a local account, so….

This will be a problem for you,
guaranteed,
every time.

On-Premises Directory - Binding your Mac to AD

```
dscl . list /Users OriginalNodeName
```

On-Premises Directory - Binding your Mac to AD

```
dscl . list /Users OriginalNodeName
```

```
dscl . read /Users/$USER AuthenticationAuthority
```

jamf

On-Premises Directory - Binding your Mac to AD

```
dscl . list /Users OriginalNodeName
```

```
dscl . read /Users/$USER AuthenticationAuthority
```

A Mobile account is just a local user account where the password happens to be the same… until it’s not.

On-Premises Directory - Binding your Mac to AD

https://developer.apple.com/videos/play/wwdc2021/10130/

https://developer.apple.com/videos/play/wwdc2022/10045/

https://developer.apple.com/videos/play/wwdc2020/10639/

jamf

On-Premises Directory - Binding your Mac to AD

DO NOT BIND MACS TO A DIRECTORY.

https://developer.apple.com/videos/play/wwdc2021/10130/

https://developer.apple.com/videos/play/wwdc2022/10045/

https://developer.apple.com/videos/play/wwdc2020/10639/

jamf

</rant>

jamf

On-Premises Directory - Alternatives

- Kerberos Single Sign-On Extension *
  - Built into the operating system, no companion app needed
  - Configured and deployed with MDM config profiles
  - Supported by AppleCare

jamf

* Artist formerly known as Apple Enterprise Connect

On-Premises Directory - Alternatives

- Kerberos Single Sign-On Extension *
  - Built into the operating system, no companion app needed
  - Configured and deployed with MDM config profiles
  - Supported by AppleCare
- NoMAD
  - Uses a partner application
  - Offers additional features that are customizable
  - Open Source - Free as in Beer - Community support

jamf

* Artist formerly known as Apple Enterprise Connect

On-Premises Directory - Alternatives

“Your password is…”

“My password is…”

On-Premises Directory - Alternatives

“Your password is…”

“I’m gonna make my password be…”

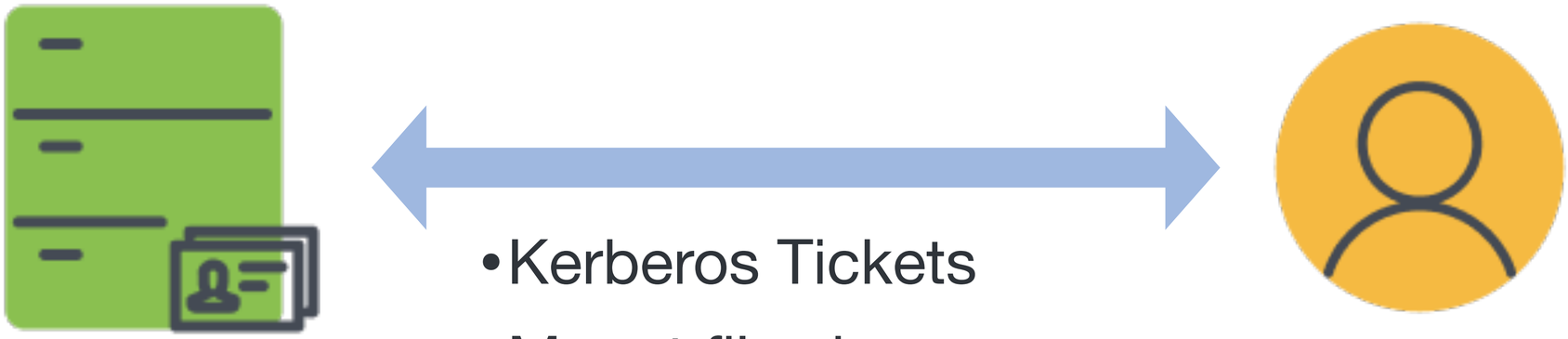
jamf

On-Premises Directory - Alternatives

“Your password is…”

“My password was…”

On-Premises Directory - Alternatives



- Kerberos Tickets
- Mount file shares
- Home directory
- Ongoing password sync

On-Premises Directory - Alternatives

- Make user account with Setup Assistant
  - “MDM managed user”

On-Premises Directory - Alternatives

- Make user account with Setup Assistant
  - “MDM managed user”
- Make users with NoLoAD
- Make users with MDM or terminal
  - No user level config profiles

On-Premises Directory - Alternatives

- Make user account with Setup Assistant
  - “MDM managed user”
- Make users with NoLoAD
- Make users with MDM or terminal
  - No user level config profiles

Sean rants about MDM managed users

jamf

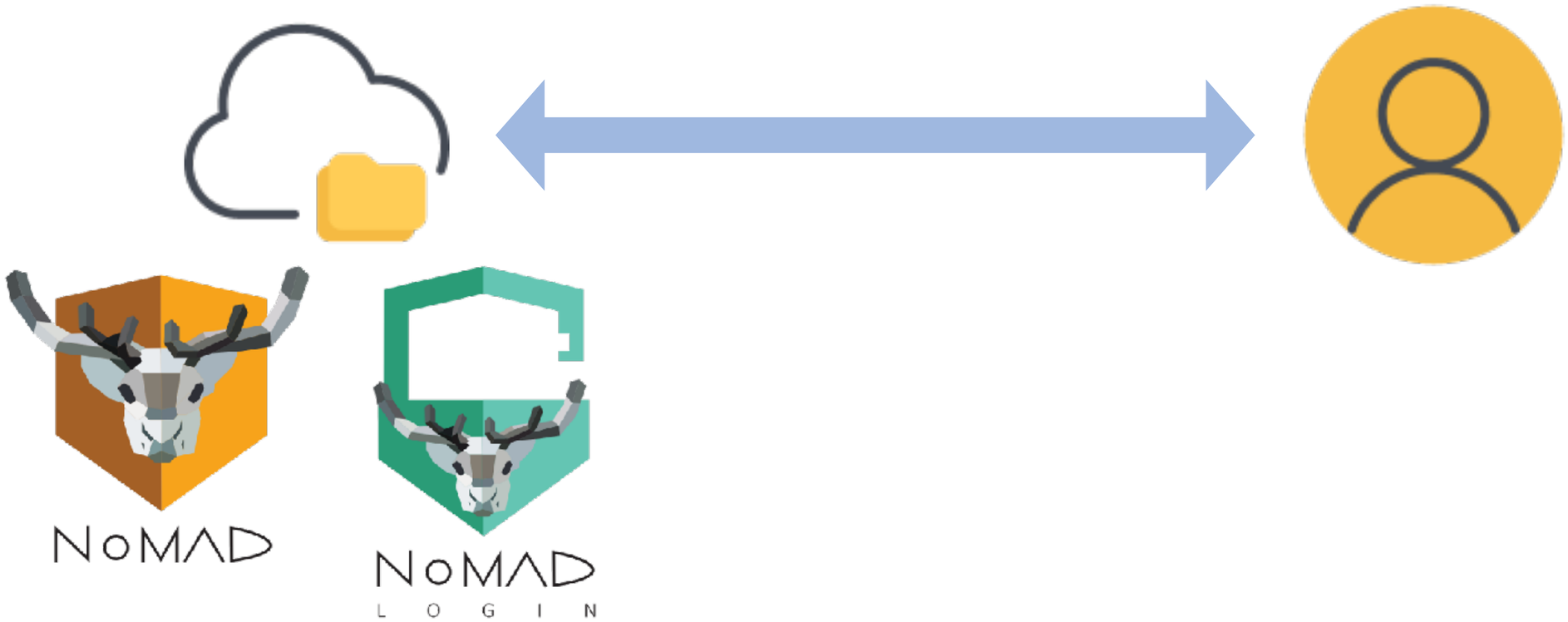
~~On-Premises~~ and **Cloud** Directory Services

jamf

Cloud Directory

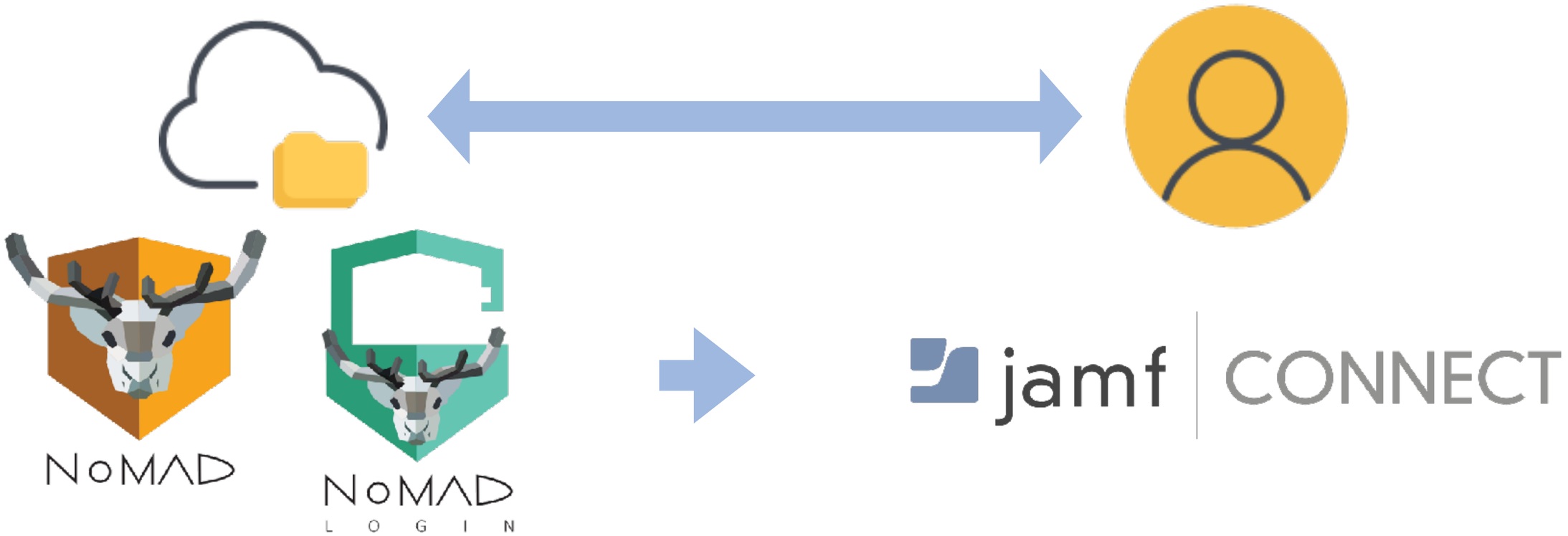
jamf

Cloud Directory



jamf

Cloud Directory



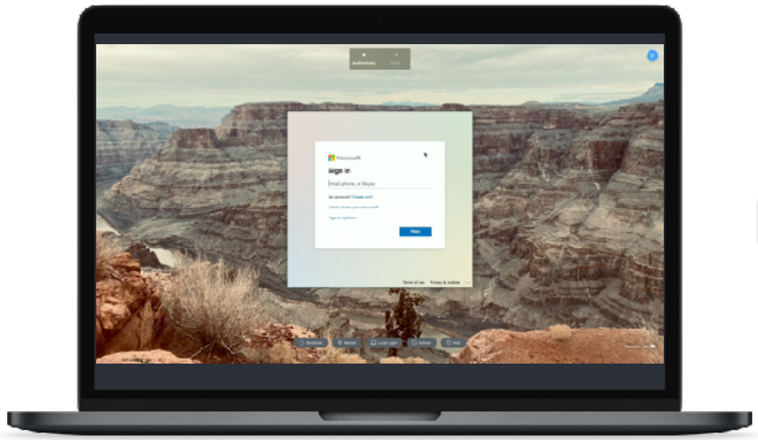
Cloud Directory

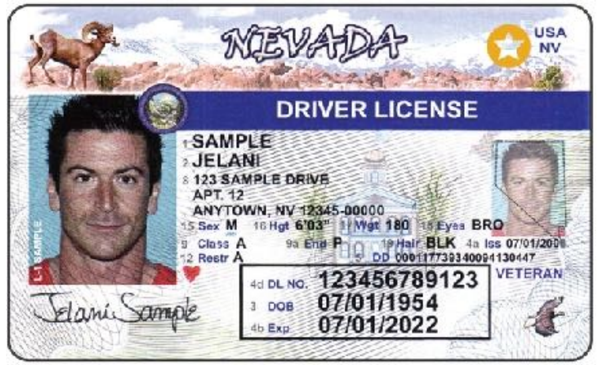
- Jamf Connect
- XCreds
- Mosyle Auth
- Kandji Passport

Cloud Directory

jamf

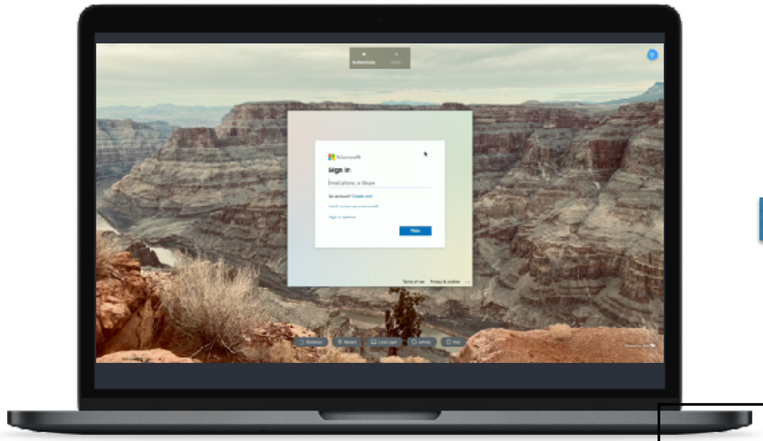
Cloud Directory

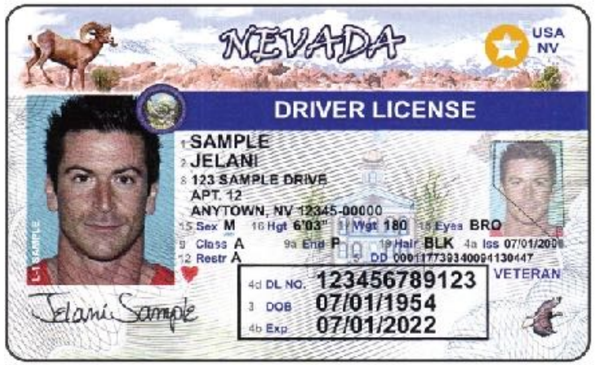




jamf

Cloud Directory



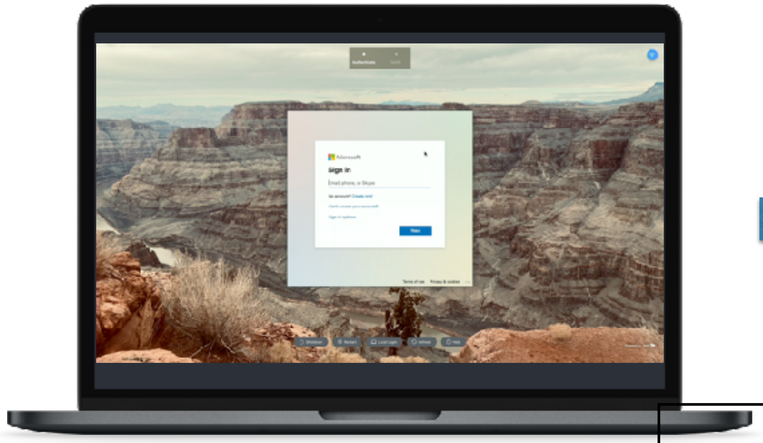


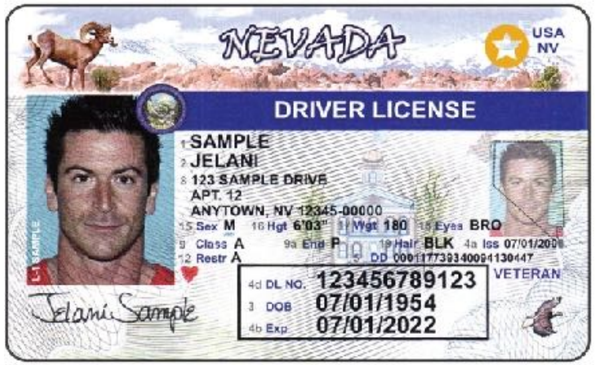

```
<saml2:AttributeStatement xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
  <saml2:Attribute Name="http://schemas.xmlsoap.org/claims/Group"
                   NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
    <saml2:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
                          xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
                          xsi:type="xs:string">macadmin</saml2:AttributeValue>
    <saml2:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
                          xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
                          xsi:type="xs:string">System Engineers</saml2:AttributeValue>
  </saml2:Attribute>
  <saml2:Attribute Name="RealName"
                   NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
    <saml2:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
                          xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
                          xsi:type="xs:string">Sean Rabbitt</saml2:AttributeValue>
  </saml2:Attribute>
  <saml2:Attribute Name="UserName"
                   NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
    <saml2:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
                          xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
                          xsi:type="xs:string">sean.rabbitt</saml2:AttributeValue>
  </saml2:Attribute>
  <saml2:Attribute Name="ShoeSize"
                   NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
    <saml2:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
                          xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
                          xsi:type="xs:string">10.5 Wide</saml2:AttributeValue>
  </saml2:Attribute>
</saml2:AttributeStatement>
```

jamf

* SAML token stunt double used

Cloud Directory






```
<saml2:AttributeStatement xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
  <saml2:Attribute Name="http://schemas.xmlsoap.org/claims/Group"
                   NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
    <saml2:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
                          xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
                          xsi:type="xs:string">macadmin</saml2:AttributeValue>
                    Value xmlns:xs="http://www.w3.org/2001/XMLSchema"
                          xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
                          xsi:type="xs:string">System Engineers</saml2:AttributeValue>
  </saml2:Attribute>
  <saml2:Attribute Name="RealName"
                   NameFormat="urn:oasis:names:tc:SAML:2.0:attrna
    <saml2:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLS
                          xmlns:xsi="http://www.w3.org/2001/XM
                          xsi:type="xs:string">Sean Rabbitt</
  </saml2:Attribute>
  <saml2:Attribute Name="UserName"
                   NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
    <saml2:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema
                          xmlns:xsi="http://www.w3.org/2001/XMLS
                          xsi:type="xs:string">sean.rabbitt</
  </saml2:Attribute>
  <saml2:Attribute Name="ShoeSize"
                   NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
    <saml2:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
                          xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
                          xsi:type="xs:string">10.5 Wide</saml2:AttributeValue>
  </saml2:Attribute>
</saml2:AttributeStatement>
```

Groups

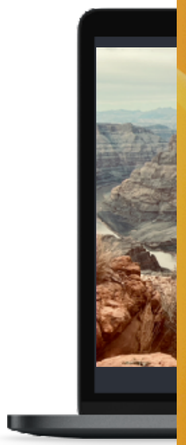
User's "real name"

A user name

jamf

* SAML token stunt double used

Clou



jamf

Search

Sound

Focus

Screen Time

General

Appearance

Accessibility

Control Center

Siri & Spotlight

Privacy & Secu

Desktop & Doc

Displays

Wallpaper

Screen Saver

Energy Saver

Lock Screen

Login Password

Trade Show
Standard

Guest User

Add Account...

Off

Edit...

New Account

Administrator
✓ Standard
Sharing Only
Group

Full Name

Account Name:

This will be used as the name for your home folder.

Password: Required

Verify: Verify

Password Hint:
(Recommended)

Hint (Recommended)

Cancel

Create User

unt double used

Cloud Directory

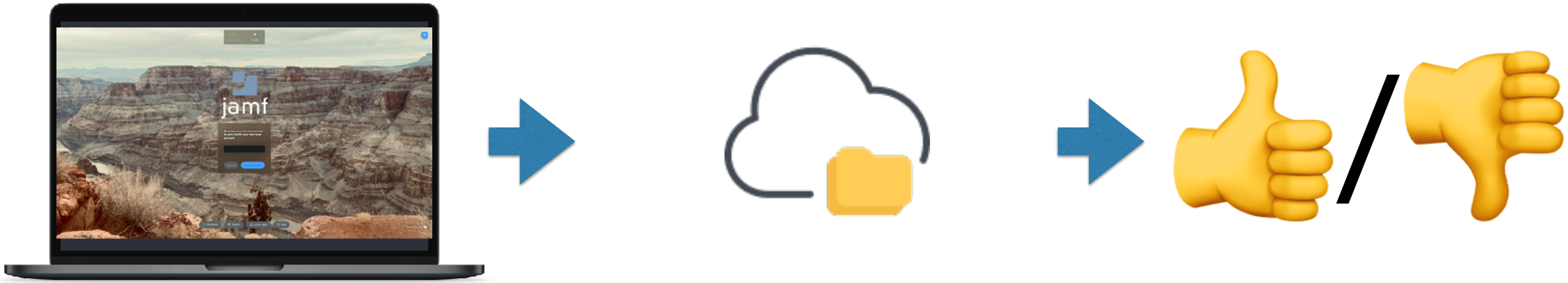
But wait, didn’t you forget something?

jamf

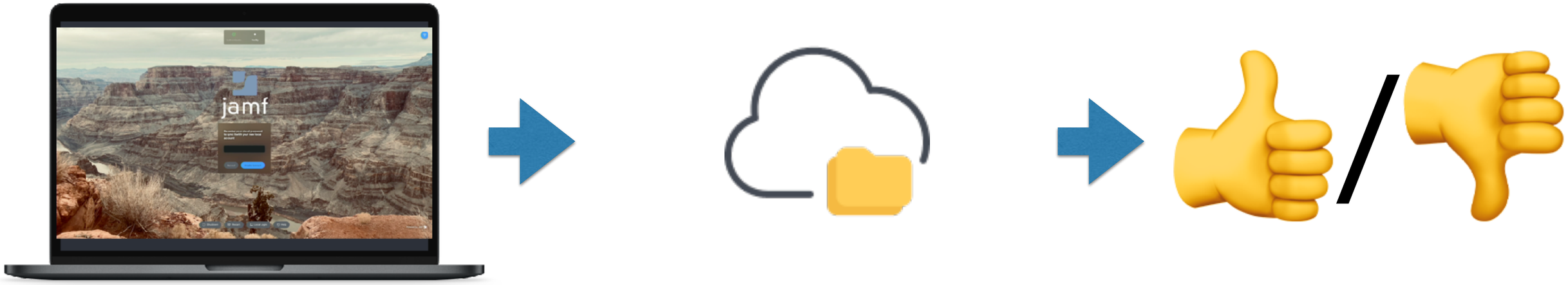
Cloud Directory

jamf

Cloud Directory



Cloud Directory

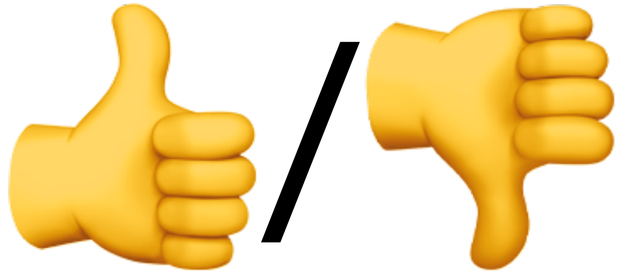


Resource Owner Password Grant

or

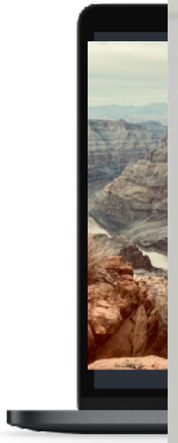
ROPG

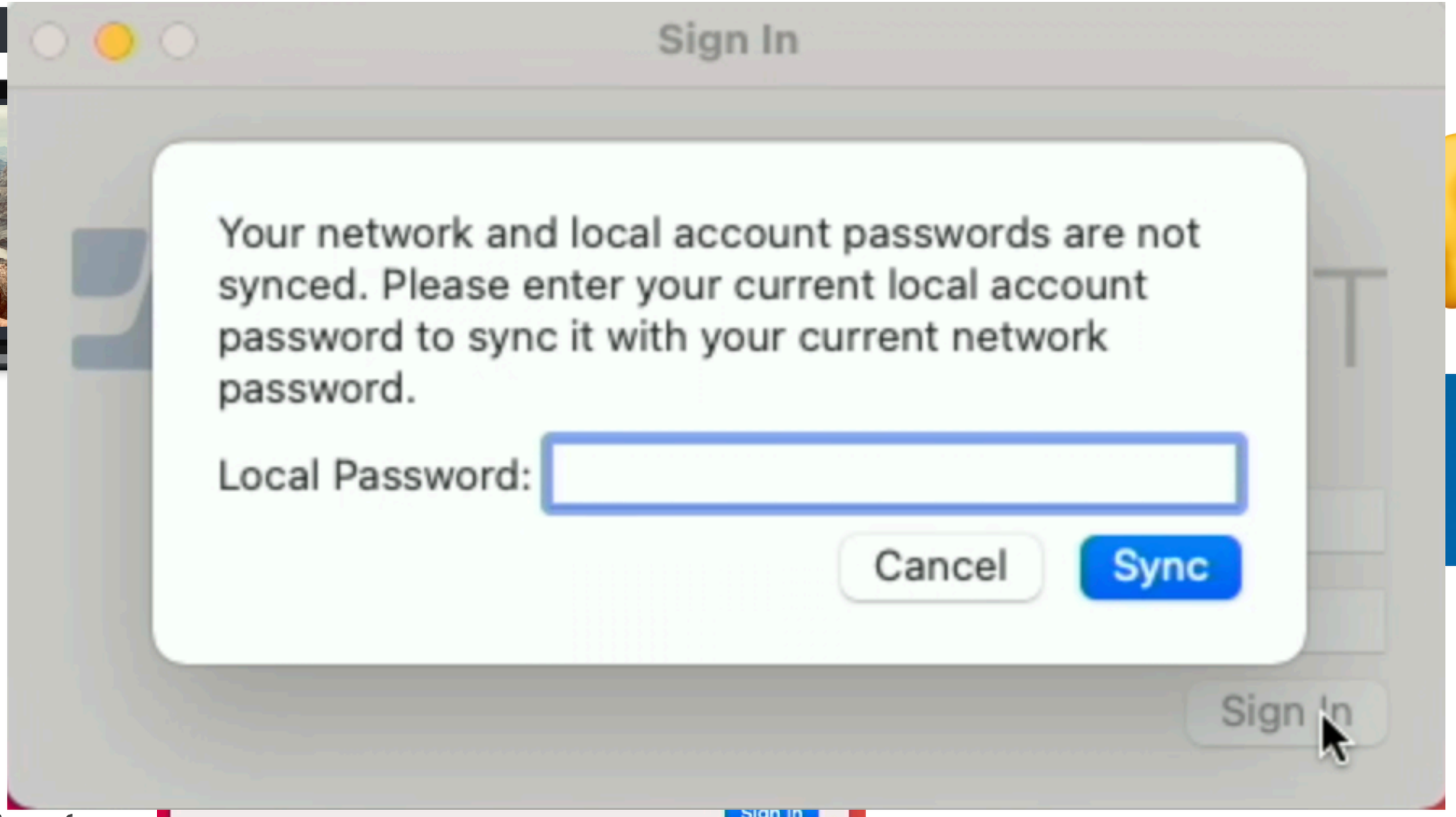
Cloud Directory



jamf

Cl

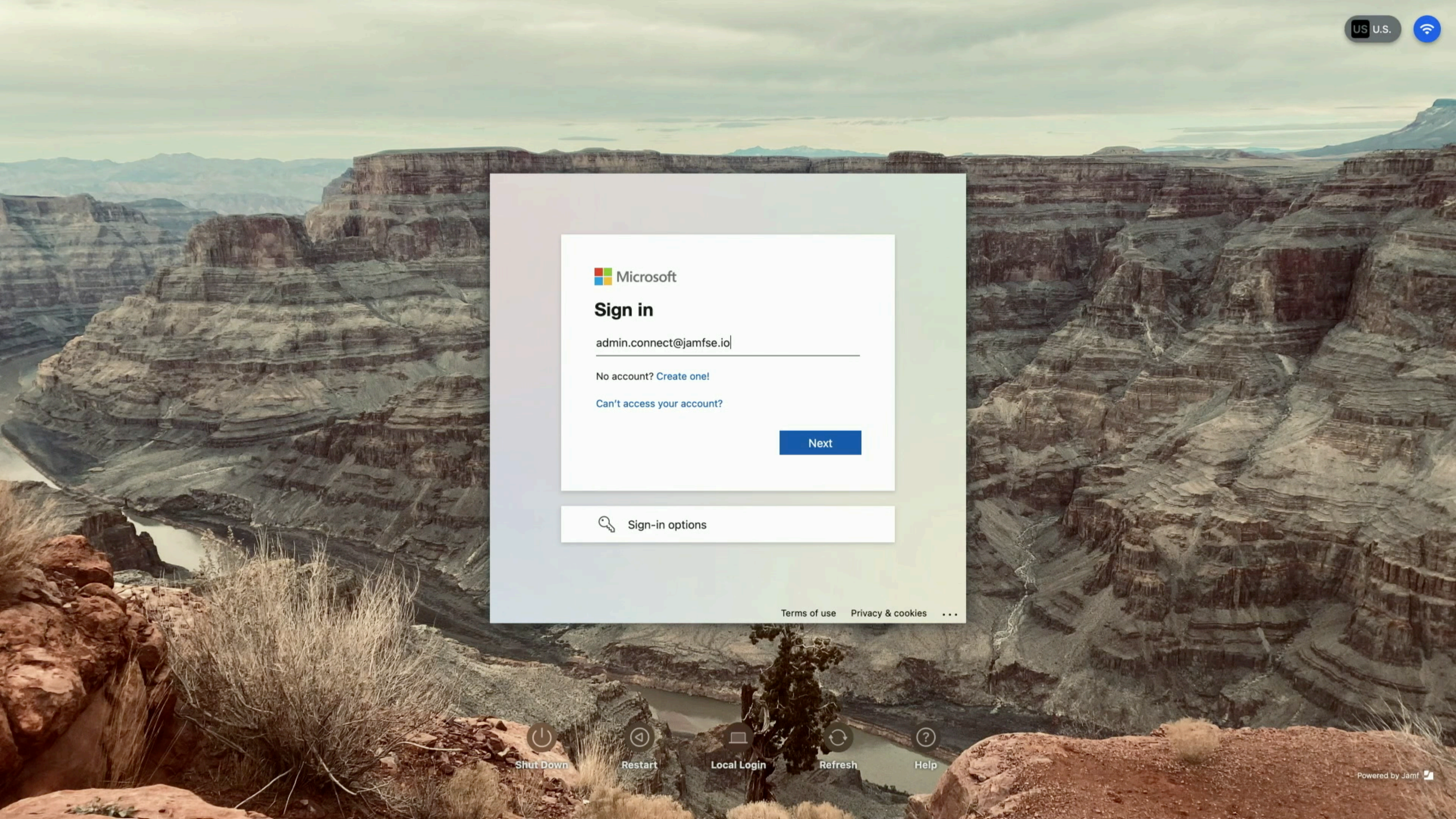


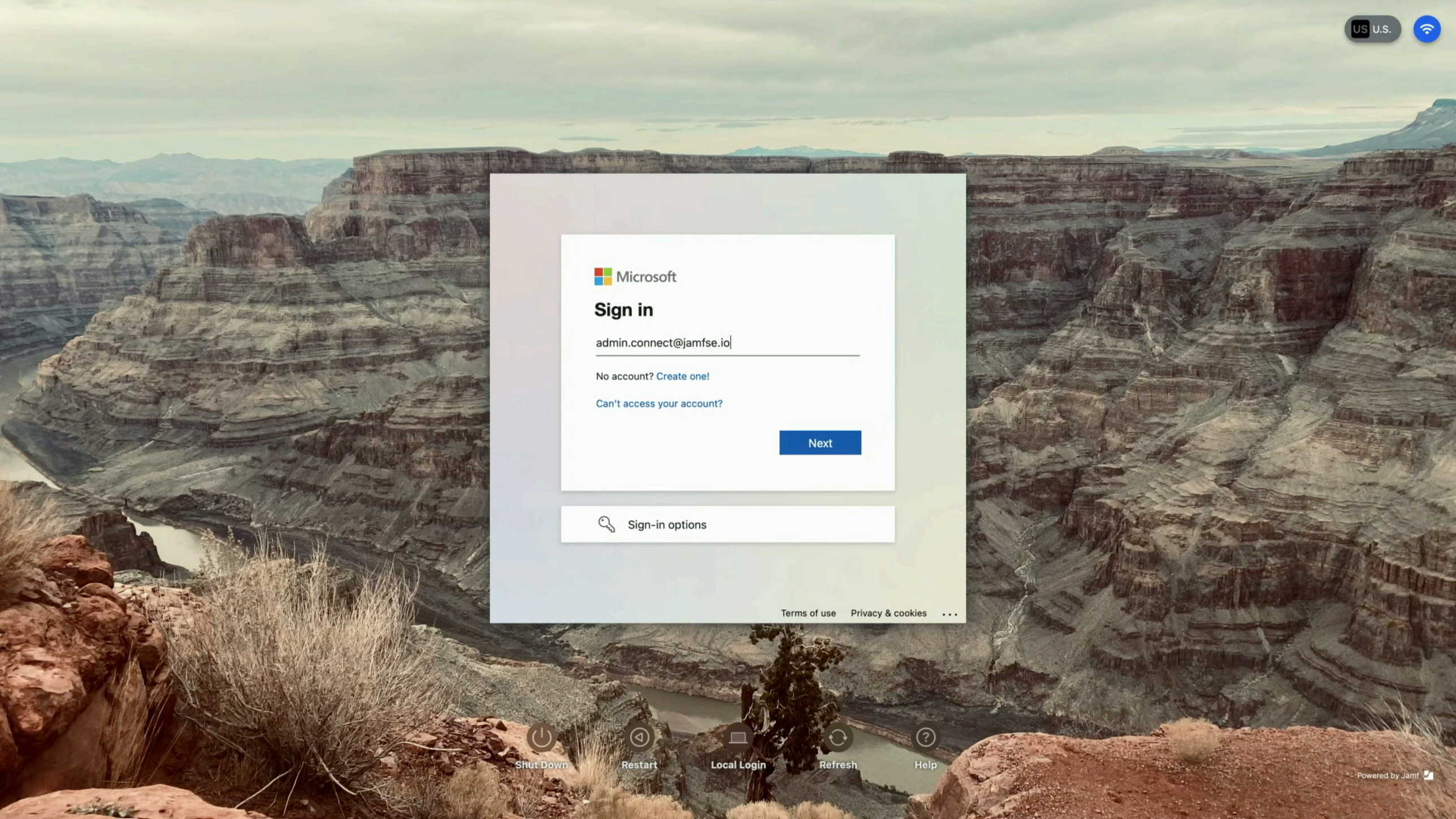

Sign In
Your network and local account passwords are not synced. Please enter your current local account password to sync it with your current network password.
Local Password:
Cancel
Sync
Sign In

jamf

Cloud Directory

- Local account with a “password nag”
  - FileVault and Keychain password kept in sync
  - Grab Kerberos tickets without a bind
  - Mount file shares, home directories, etc.
- Login window could…
  - Force network login
  - Force network login unless no network found
  - Allow or default to local logins


US U.S.
Microsoft
Sign in
admin.connect@jamfse.io
No account? Create one!
Can't access your account?
Next
Sign-in options
Terms of use
Privacy & cookies
...
Shut Down
Restart
Local Login
Refresh
Help
Powered by Jamf


US U.S.
Microsoft
Sign in
admin.connect@jamfse.io
No account? Create one!
Can't access your account?
Next
Sign-in options
Terms of use
Privacy & cookies
...
Shut Down
Restart
Local Login
Refresh
Help
Powered by Jamf


Finder
File
Edit
View
Go
Window
Help
Thu Jun 29 2:52 PM
JUN
29
tv

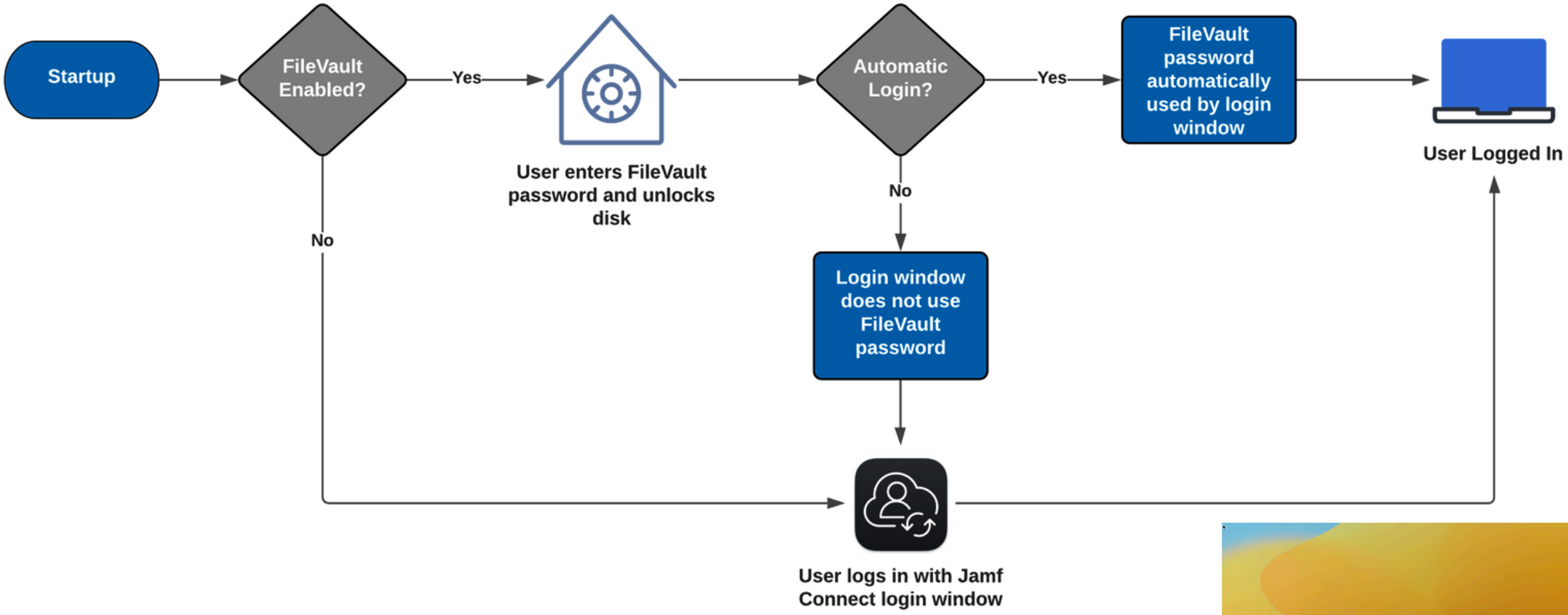

Finder
File
Edit
View
Go
Window
Help
Thu Jun 29 2:52 PM
JUN
29
tv

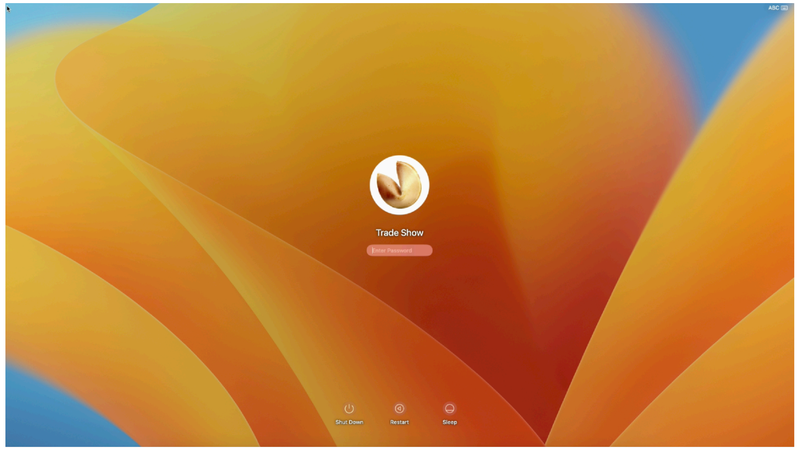
Cloud Directory

Sample Uses

- Login and Menu Bar
- Just Login
  - Kiosk / Lab / Shared Desk
  - Ephemeral accounts, deleted after X time
- Just Menu Bar
  - Ongoing password sync, 1:1 machines

Cloud Directory and FileVault, or “war never changes”





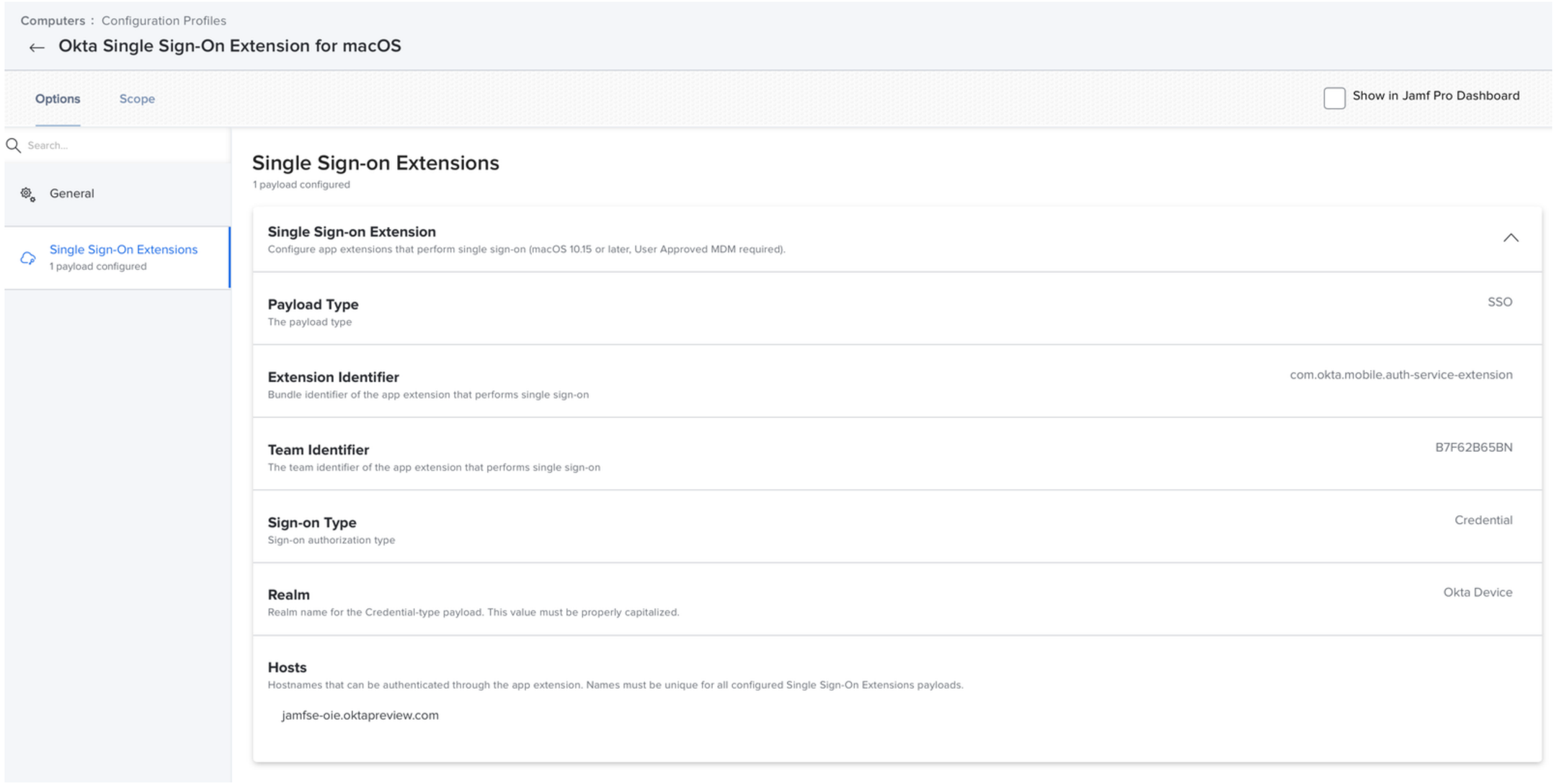
jamf

The Future:
Platform Single Sign-On

Or, rampant speculation because ain’t nobody has released this to the public yet

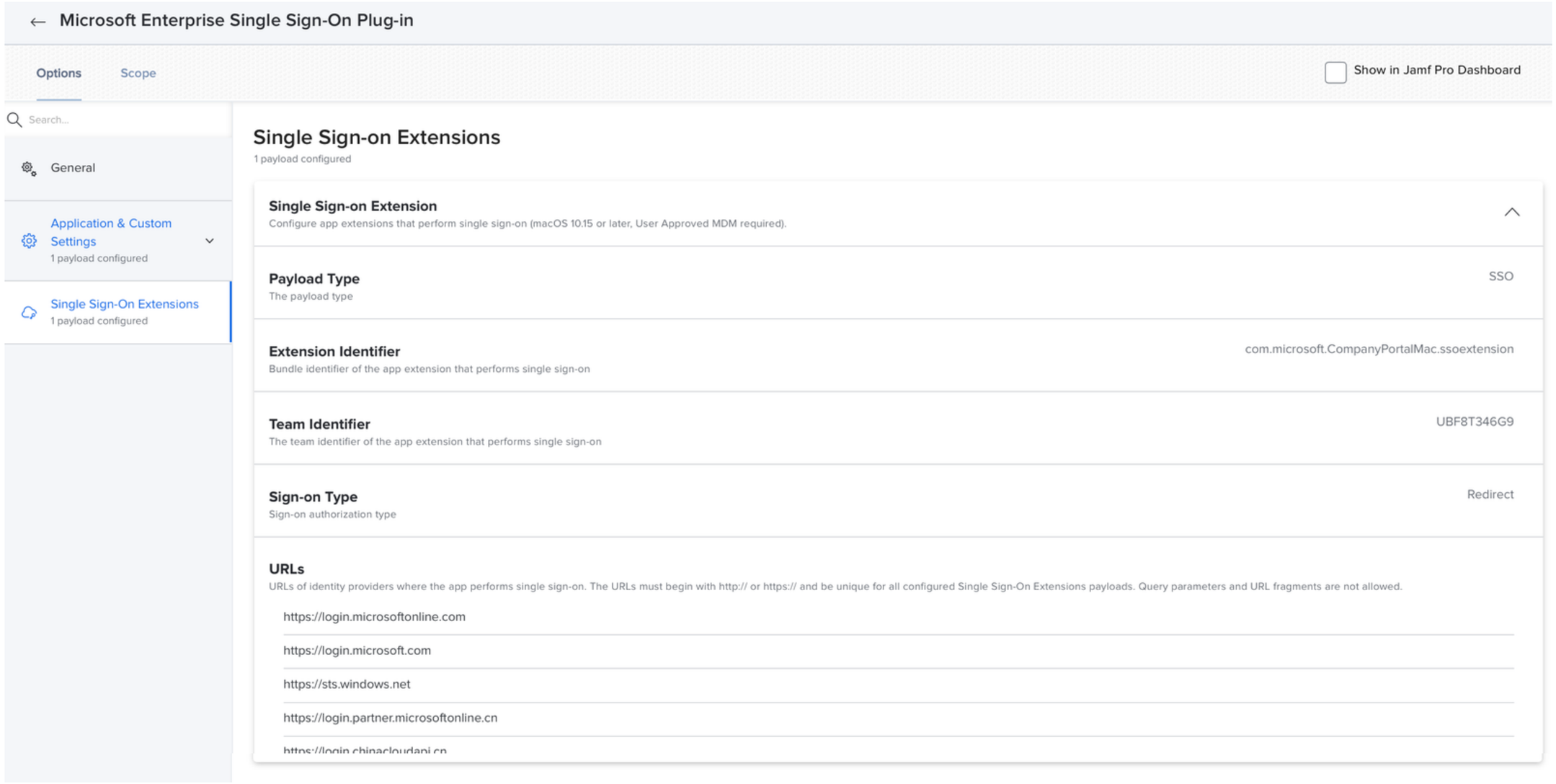
jamf

Single Sign-On Extension for Enterprise



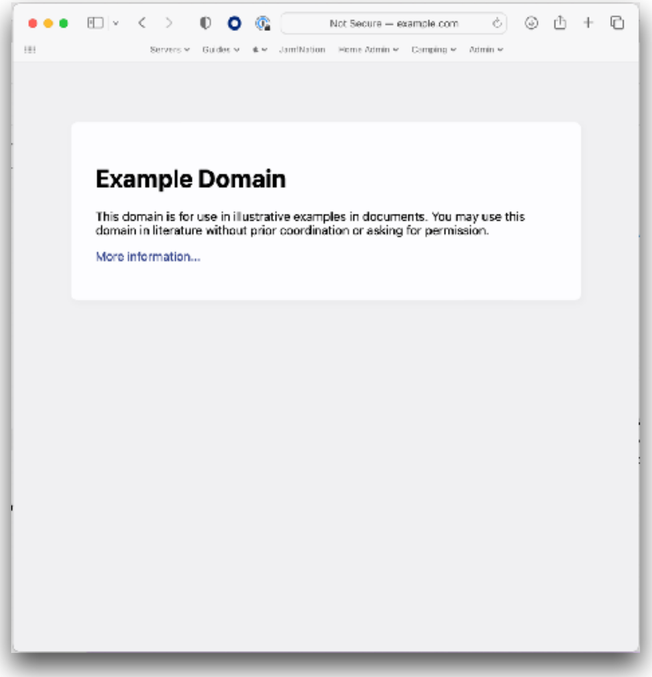
jamf

Single Sign-On Extension for Enterprise

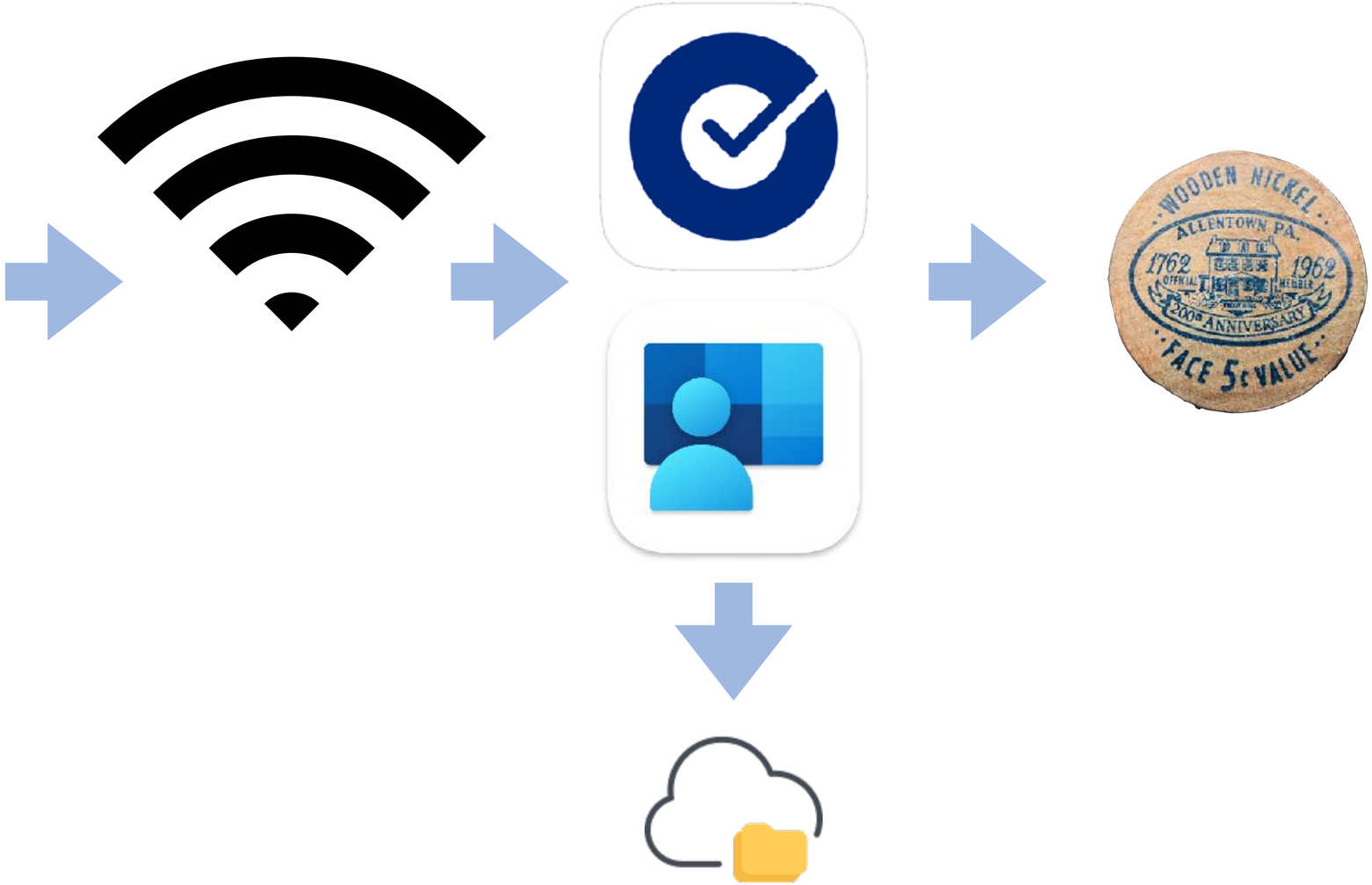


jamf

Single Sign-On Extension for Enterprise

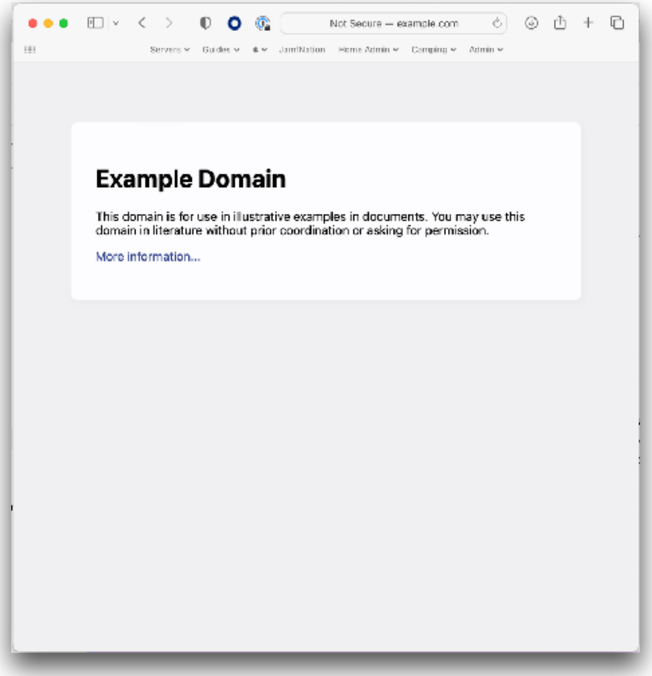


open https://example.com/login

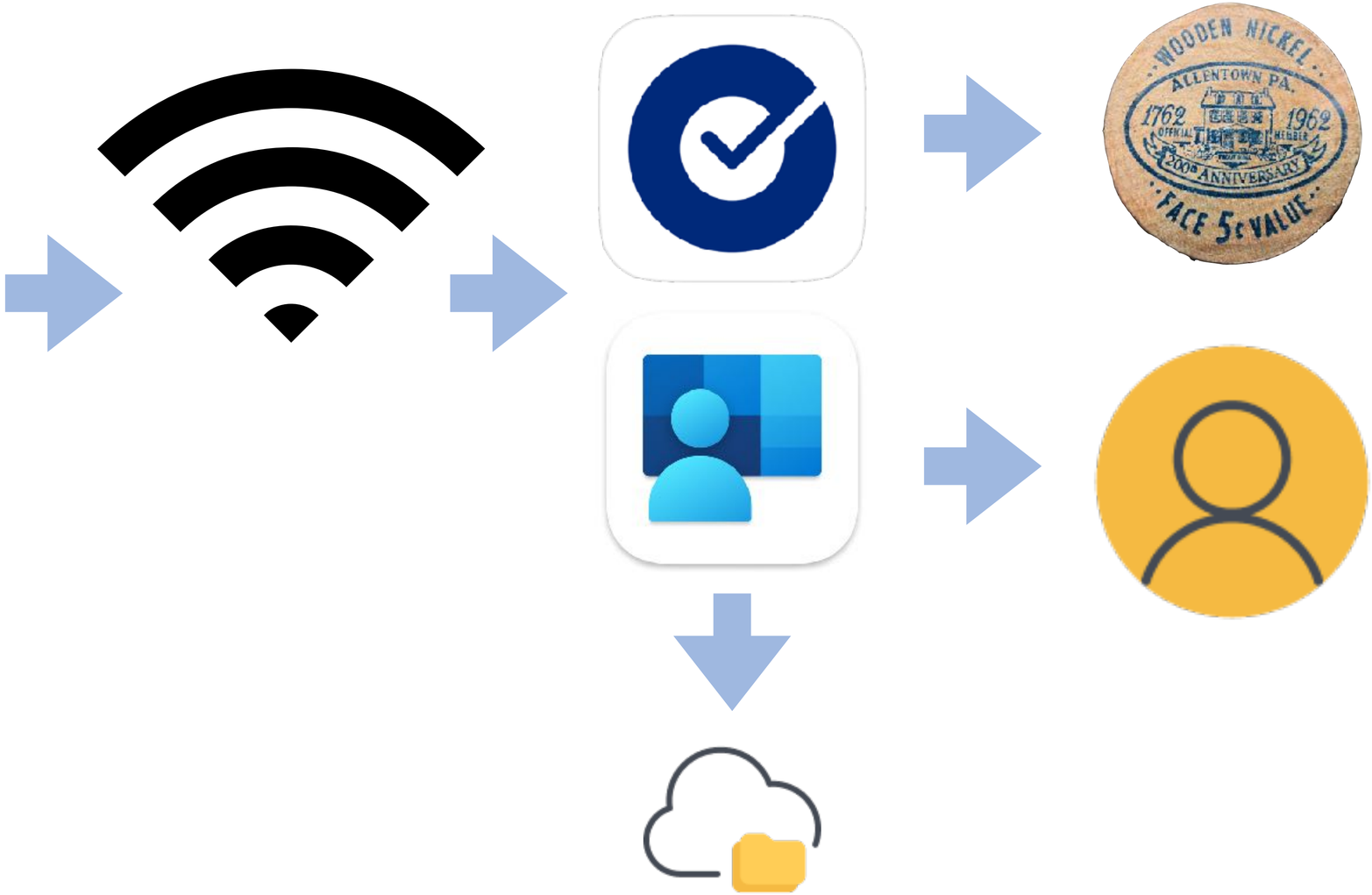


jamf

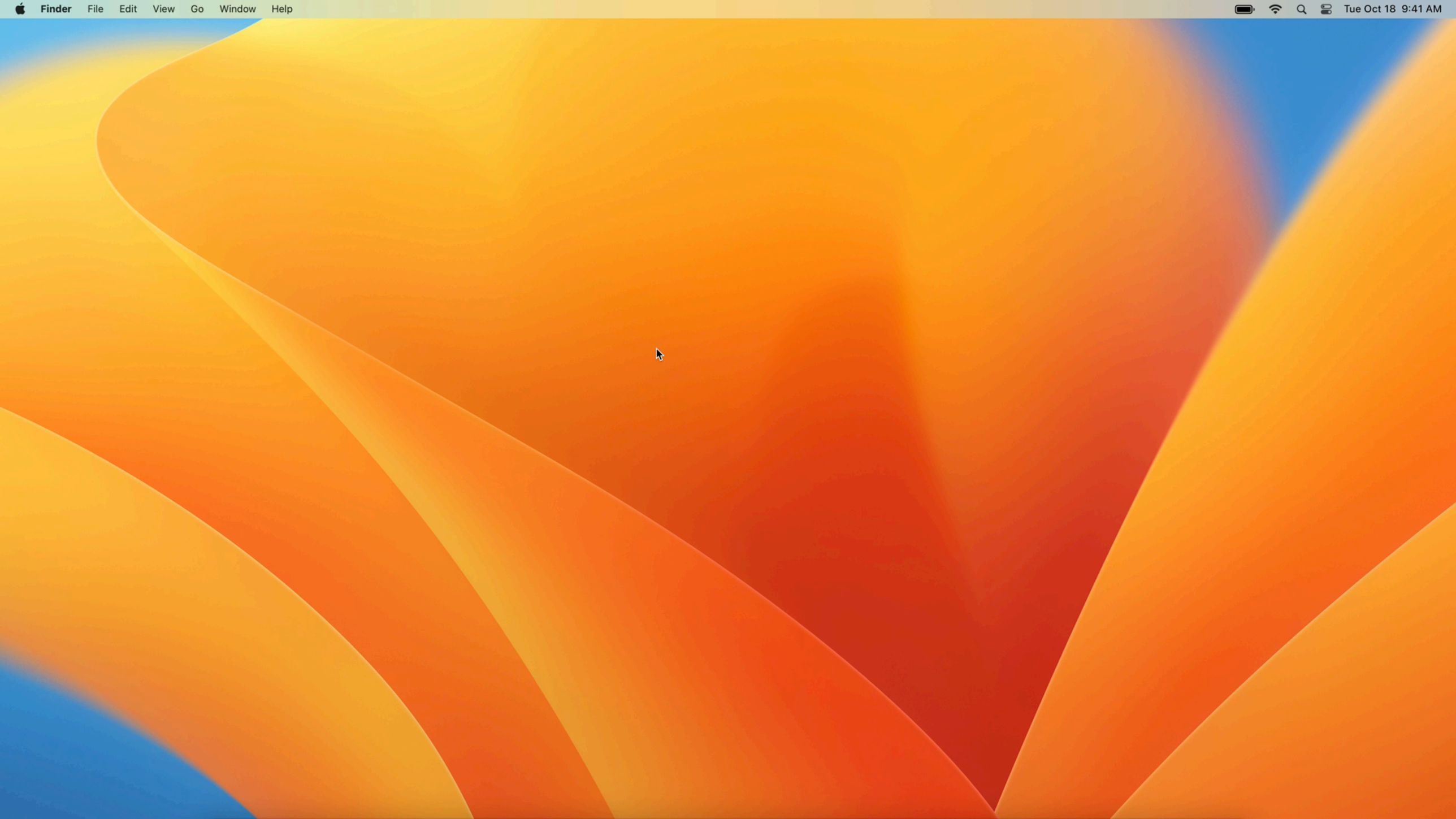
Platform Single Sign-On Extension

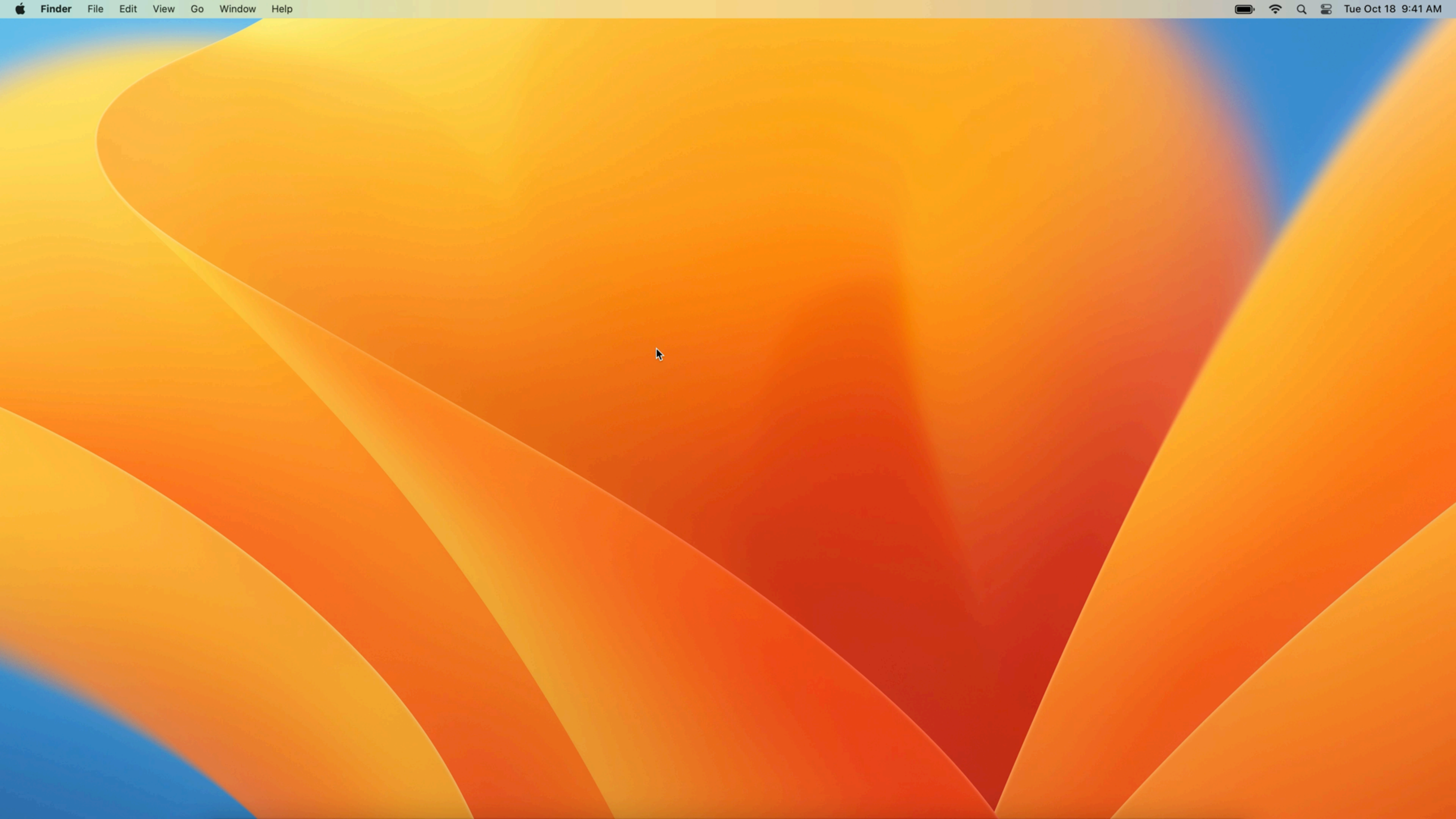


open https://example.com/login



jamf


Finder
File
Edit
View
Go
Window
Help
Tue Oct 18 9:41 AM


Finder
File
Edit
View
Go
Window
Help
Tue Oct 18 9:41 AM

Platform Single Sign On - as of macOS Ventura

Feature	Platform Single Sign On	Jamf Connect & Others
Works at login window		✅
Makes local user account		✅
Admin / Standard rights management		✅
Works in Zero Touch Enrollment flow		✅
Can enforce network only logins		✅
Can enforce MFA for offline auth		✅ (Depends on tool used)
Keeps local account in sync with IdP	✅	✅
Kerberos support	✅ (with Kerberos SSOe)	✅
Automatically logs in to cloud IdP gated apps	✅	
Screensaver Unlock	?	

jamf

We don’t talk about betas in public forums.

But it’s not really beta…

https://appleseed.apple.com
https://beta.apple.com/it

Platform Single Sign On - as of macOS Sonoma

Feature	Platform Single Sign On	Jamf Connect & Others
Works at login window	✅	✅
Makes local user account	✅ (After first admin account created)	✅
Admin / Standard rights management	✅	✅
Works in Zero Touch Enrollment flow	🤷‍♀️	✅
Can enforce network only logins		✅
Can enforce MFA for offline auth		✅ (Jamf Connect only)
Keeps local account in sync with IdP	✅	✅
Kerberos support	✅ (with Kerberos SSOe)	✅
Automatically logs in to cloud IdP gated apps	✅	
Screensaver Unlock	✅	
PIV / SmartCard Support	✅	

jamf

Platform Single Sign On - as of macOS Sonoma

Authentication Scenarios:

- Password - Local account password sync with the IdP
- Password with WS-Trust - IdP doesn’t know password - SAML token auth
- User Secure Enclave Key - Auth to IdP without a password - still local password
- SmartCard - Auth with cert on PIV - local password maybe?

Platform Single Sign On - as of macOS Sonoma

Authentication Scenarios:

- Password - Local account password sync with the IdP
- Password with WS-Trust - IdP doesn’t know password - SAML token auth
- User Secure Enclave Key - Auth to IdP without a password - still local password
- SmartCard - Auth with cert on PIV - local password maybe?

Group Membership:

- Pass up to 100 IdP based groups to local macOS device
- Local UNIX group membership determines admin/standard/sudo rights

Platform Single Sign On - as of macOS Sonoma

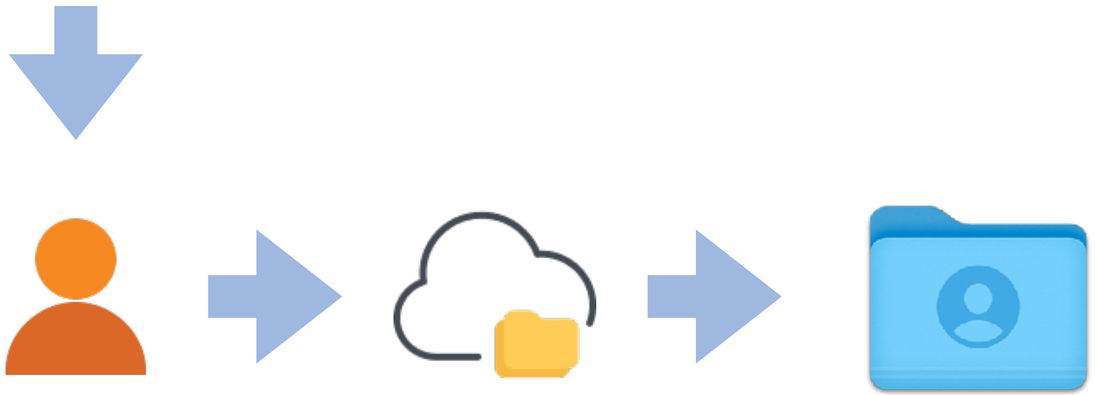
Shared Device Registration

jamf

Platform Single Sign On - as of macOS Sonoma

Shared Device Registration

User Registration



Final thoughts :

Local User Accounts

Network Accounts

Cloud Identity Accounts

Platform Single Sign-On

jamf

Final Thoughts

- macOS is UNIX
- FileVault gonna FileVault
- Tying to a directory introduces challenges
- Challenges can be overcome
- Let’s see what happens with PSSOe in the future
- macOS is still UNIX

https://github.com/sean-rabbitt
for slides

See you at the Jamf booth!

jamf


Thank you.
jamf