jamf

Macs Factor:
The Risks and Rewards of Single Sign On

Sean Rabbitt

Sr Consulting Engineer,
Identity and Access Mgmt

PRESENTING TO

2024 MACADMINS CONFERENCE

Agenda

1 | Authentication Factors and Other Confusion

Passwords, and tokens, and biometrics, oh my!

2 | What the heck is "Single Sign On"?

There's only two identity providers in the world that support this thing, so I could understand your confusion.

3 | Hardening with factors and rules

Okta calls it one thing, and Microsoft calls it another thing. And now as an Apple admin, it's your thing.

4 | And then there's Platform Single Sign-On...

In which we supply a slide with the words "Don't Panic" in large friendly characters. Cake to follow.

jamf

“If you wish to make an apple pie from scratch, you must first invent the universe.”

Carl Sagan

COSMOS, C. 1980

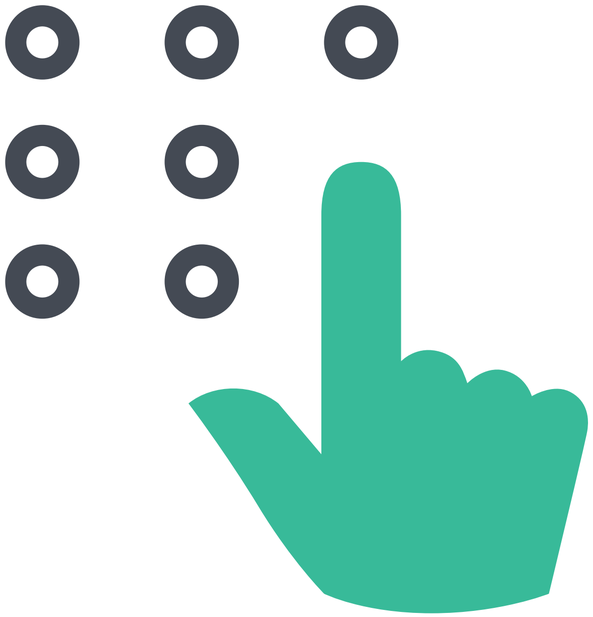
jamf

Authentication Factors or why don't you trust me

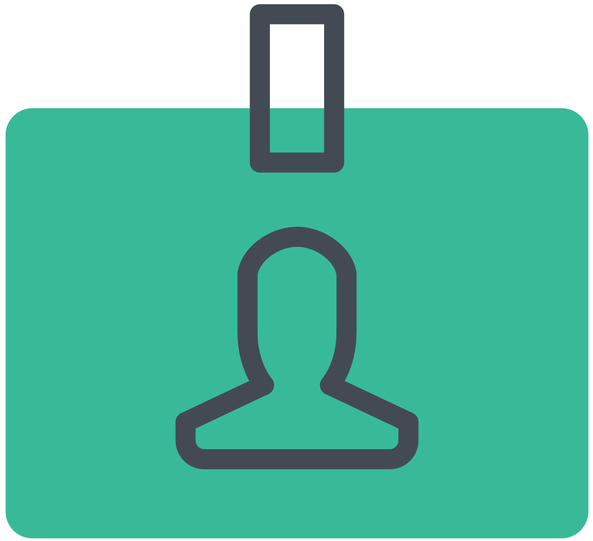
And what exactly do identity people have against jam bands from the 90's anyway?

jamf

Factor Types



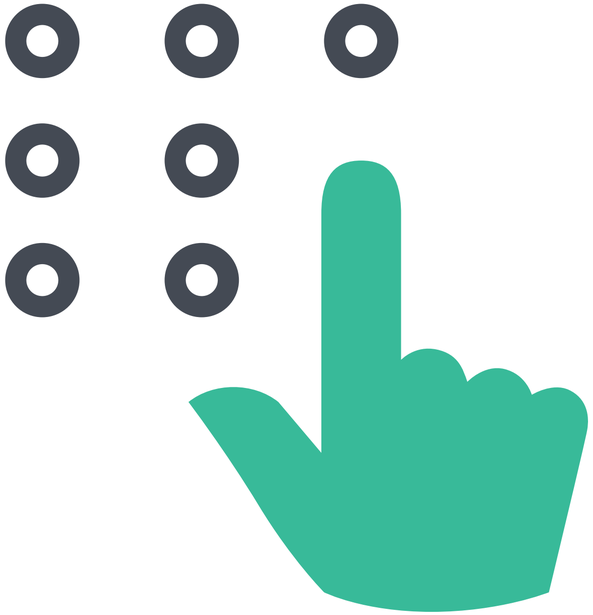
Knowledge



Possession

Biometric

jamf



Something you know

- PIN
- Password
- Mother's Maiden Name

Something you have

- PIV / SmartCard
- FIDO2 hardware token
- Some other device

Something you are

- TouchID / FaceID
- Fingerprint scanner
- Retinal scanner

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

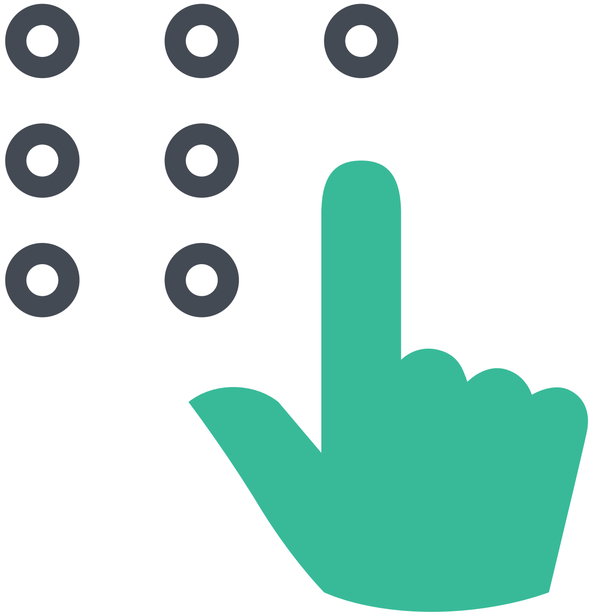
jamf

“Passcodes and passwords are essential to the security of Apple devices.”

Apple Platform Security guide

HTTPS://SUPPORT.APPLE.COM/GUIDE/SECURITY/FACE-ID-AND-TOUCH-ID-SECURITY-SEC067EB0C9E/1/WEB/1

jamf



Something you know

- PIN
- Password
- ~~Mother's Maiden Name~~

Something you have

- PIV / SmartCard
- ~~FIDO2 hardware token~~
- ~~Some other device~~

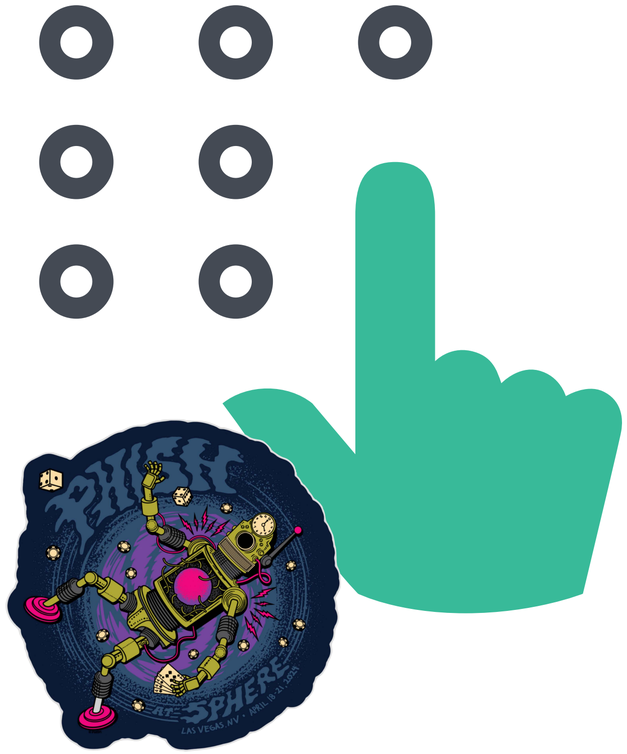
~~Something you are~~

- ~~TouchID / FaceID~~
- ~~Fingerprint scanner~~
- ~~Retinal scanner~~

jamf

jamf

drygoods.phish.com



jamf

jamf

“If **The Cloud** is just somebody else's server, **Passwordless** is just somebody else's hash.”

Sean Rabbitt

SR. CONSULTING ENGINEER, CIRCA 2022

jamf

Something you know

- PIN
- Password
- Mother's Maiden Name

Something you have

- PIV / SmartCard
- FIDO2 hardware token
- Some other device

Something you are

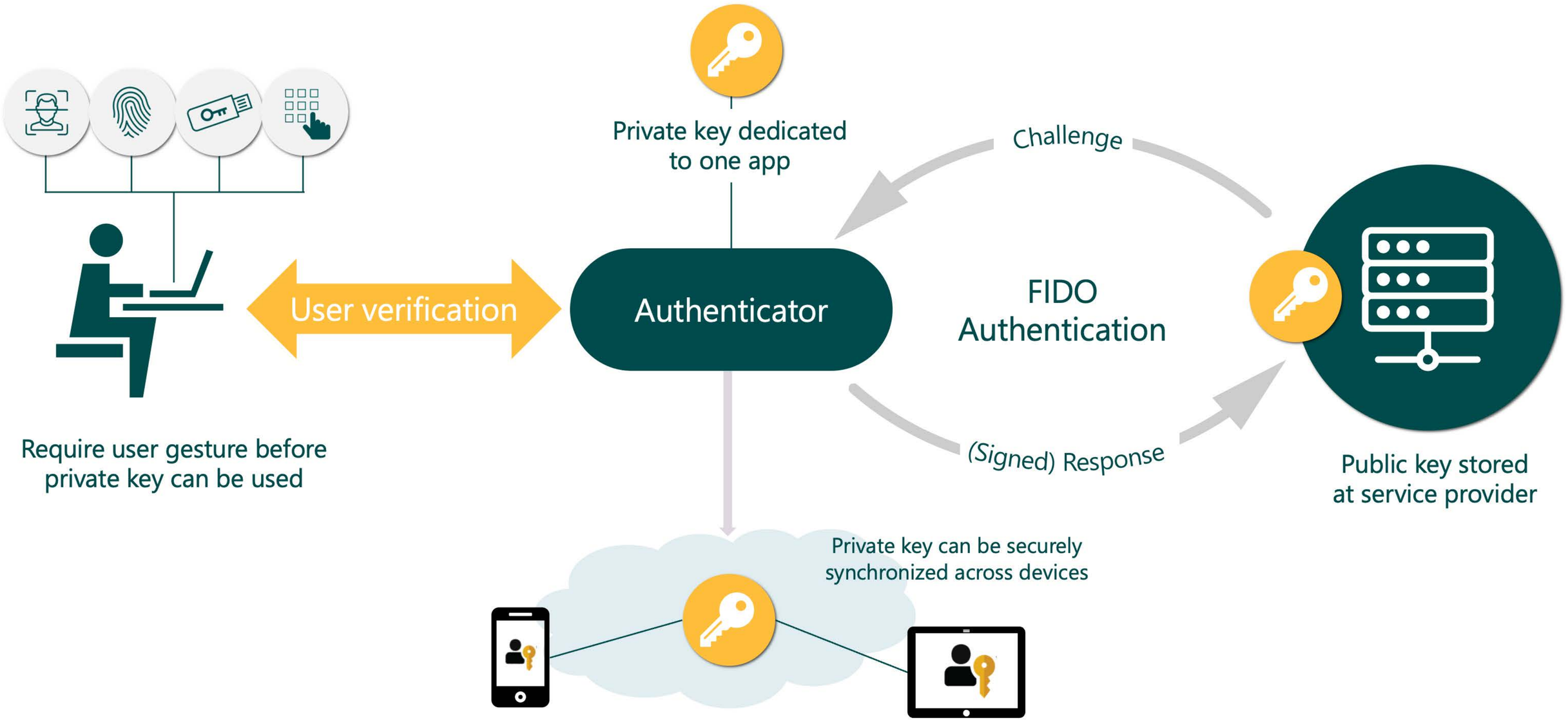
- TouchID / FaceID
- Fingerprint scanner
- Retinal scanner

“With Face ID or Touch ID turned off, when a device or account locks, the keys for the highest class of Data Protection—which are held in the Secure Enclave—are discarded. The files and keychain items in that class are inaccessible until the user unlocks the device or account by entering their **passcode or password**.”

Apple Platform Security guide

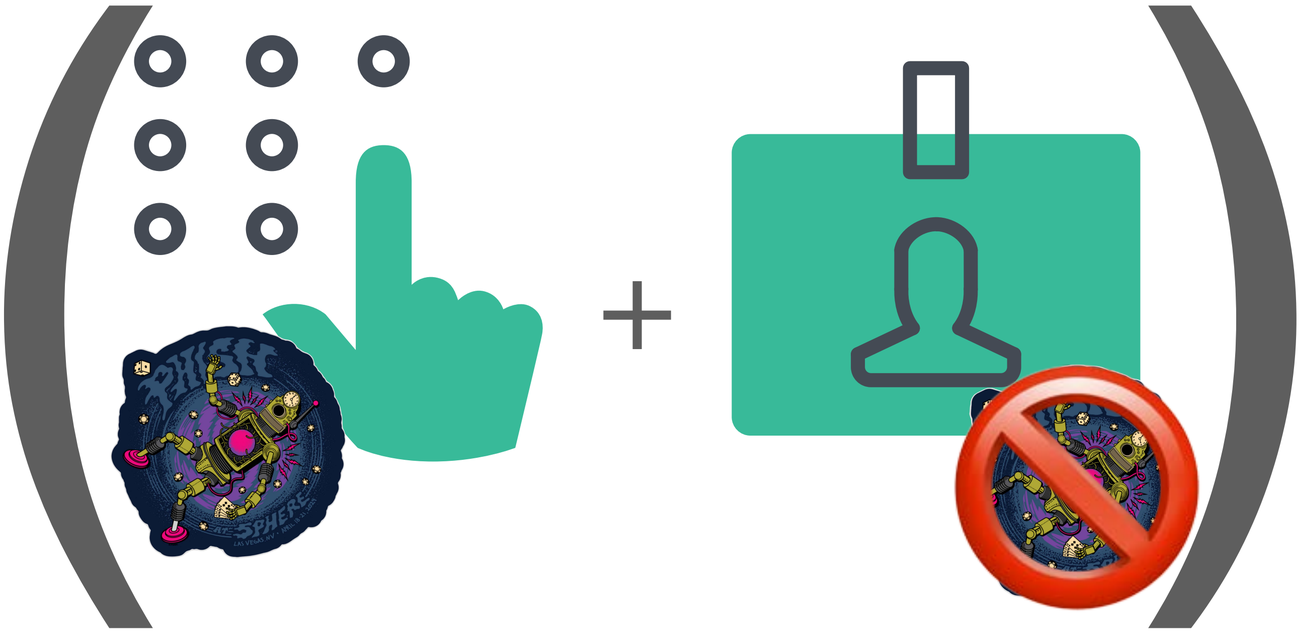
HTTPS://SUPPORT.APPLE.COM/GUIDE/SECURITY/USES-FOR-FACE-ID-AND-TOUCH-ID-SECC5227FF3C/1/WEB/1

jamf



jamf

jamf



+

x

- Knowledge based password reset procedures
- "Security" questions
- Untrained help desk
- SMS based factor resets
- Email based factor resets
- "My voice is my password. Verify me."

=

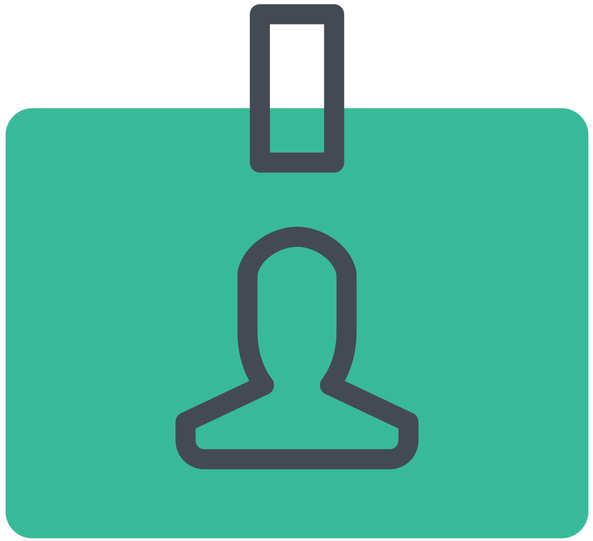
What the heck is
Single Sign On

You mean that thing where I type my user name and password 27 times a day?

jamf

Apple Extensible Single Sign On

Knowledge

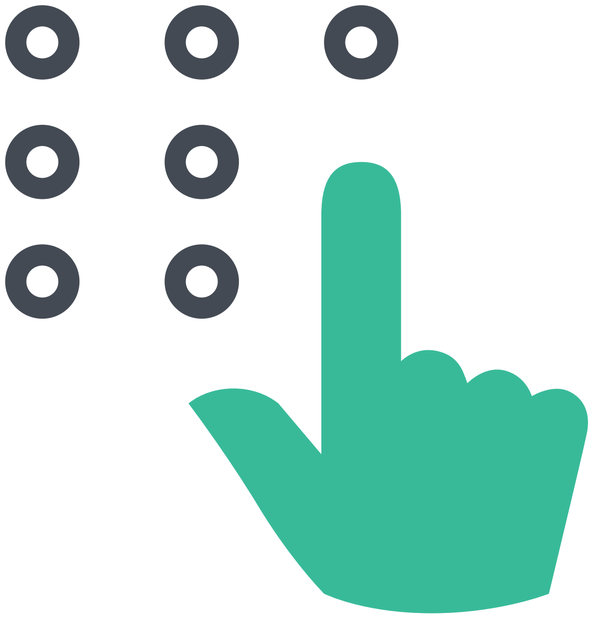


Possession

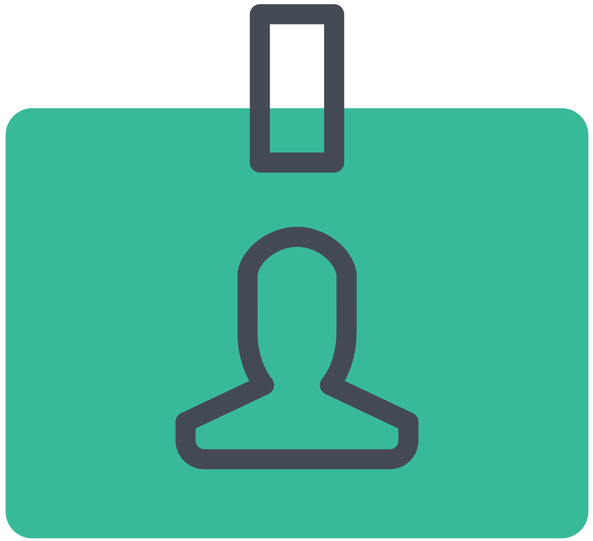
Biometric

jamf

Apple Extensible Single Sign On



Knowledge

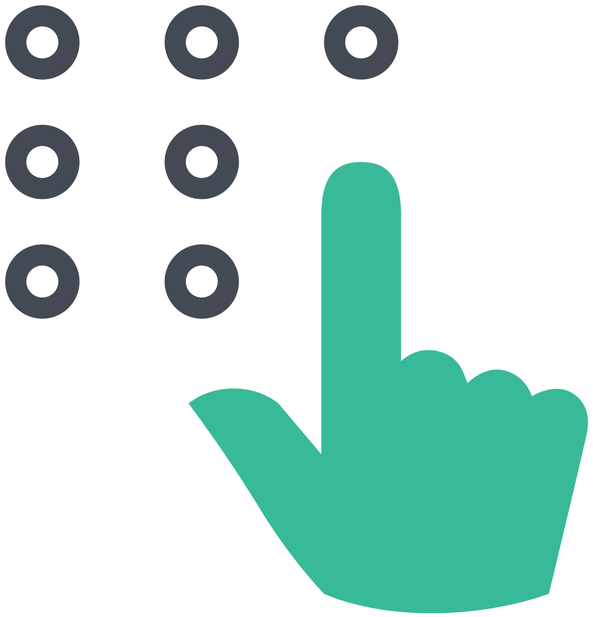


Possession

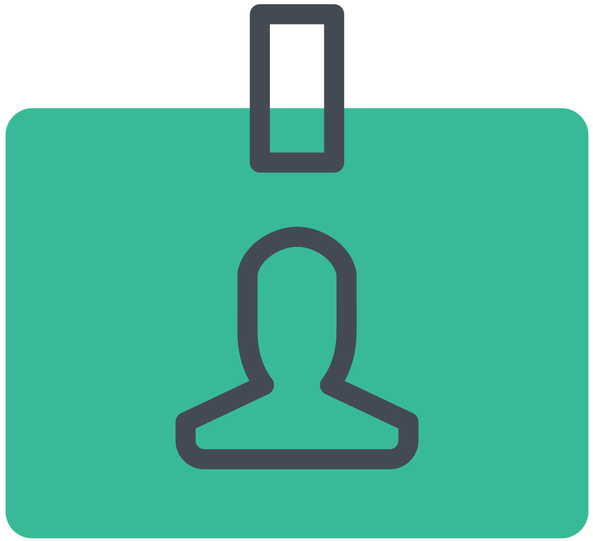
Biometric

jamf

Apple Extensible Single Sign On



Knowledge

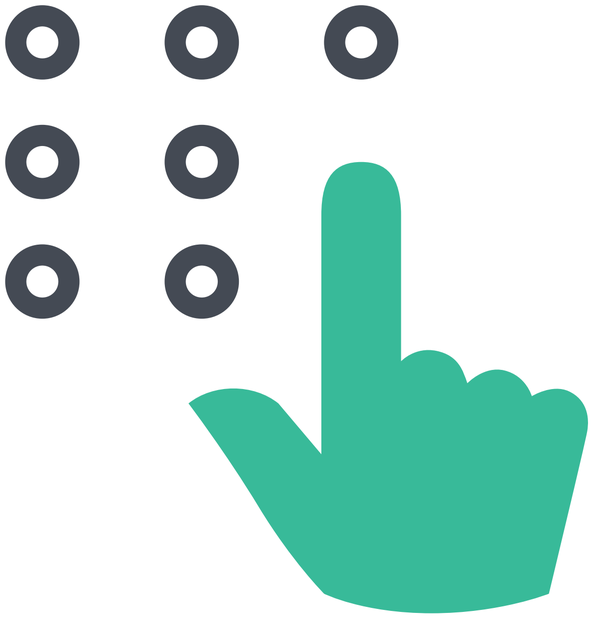


Possession

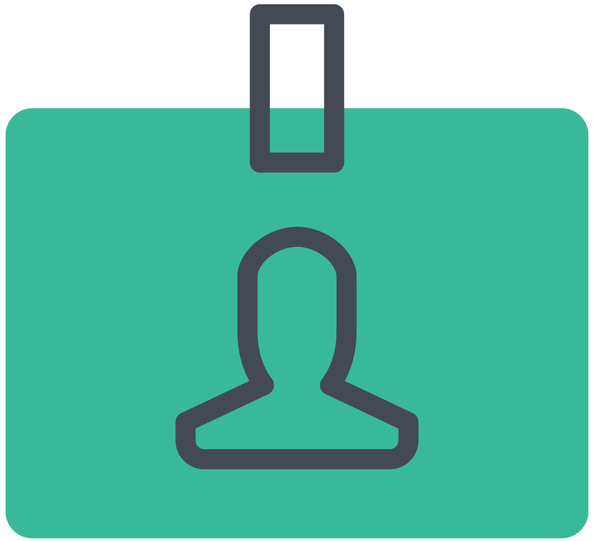
Biometric

jamf

Apple Extensible Single Sign On



Knowledge



Possession

Biometric

jamf

Use words more gooder

- Kerberos Single Sign-On
- Extensible Single Sign-On - SSOe

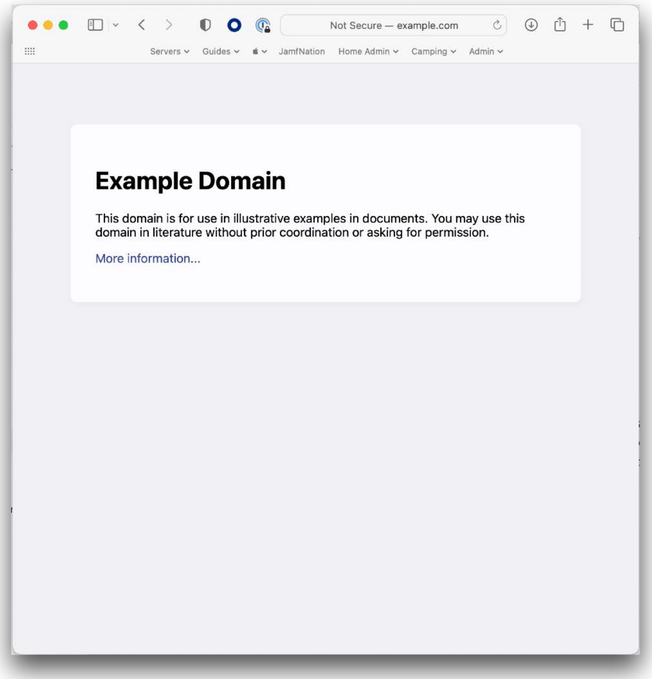
Use words more gooder

- Kerberos Single Sign-On
- Extensible Single Sign-On - SSOe
  - AuthenticationServices API - "credential"
  - URL interception method - "redirect"

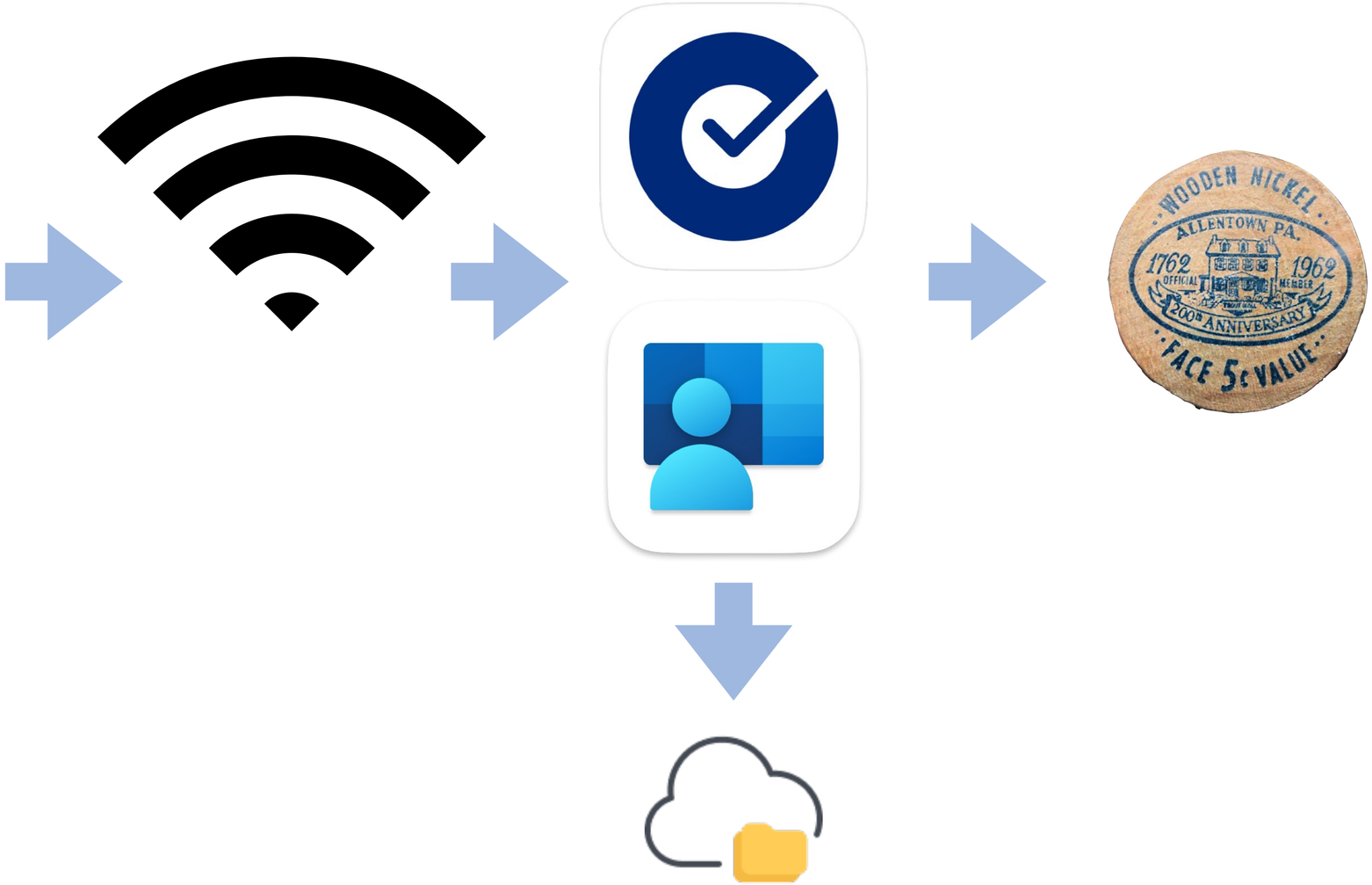
Use words more gooder

- Kerberos Single Sign-On
- Extensible Single Sign-On - SSOe
  - AuthenticationServices API - "credential"
  - URL interception method - "redirect"
- Enrollment Single Sign-On - "Enrollment SSO"
- Platform Single Sign-On - PSSOe

Extensible Single Sign-On

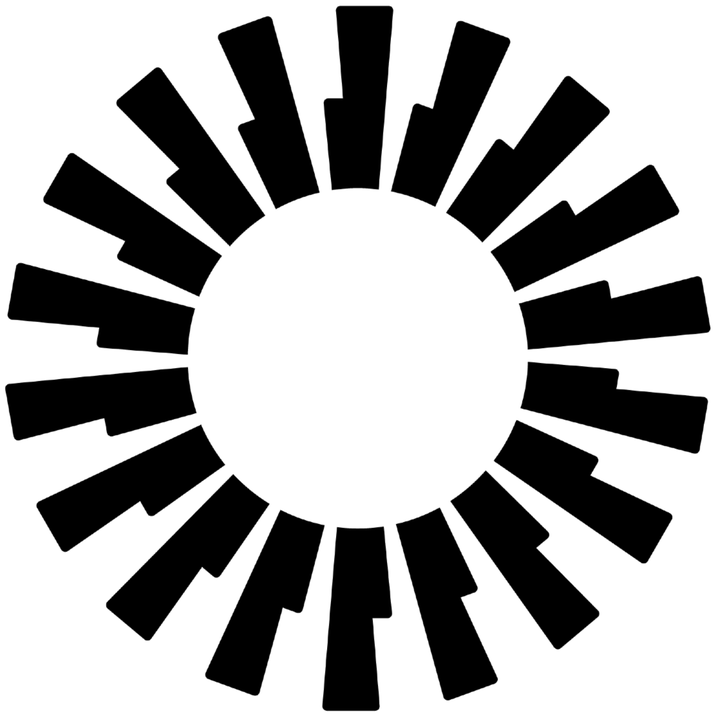


open https://example.com/login



jamf

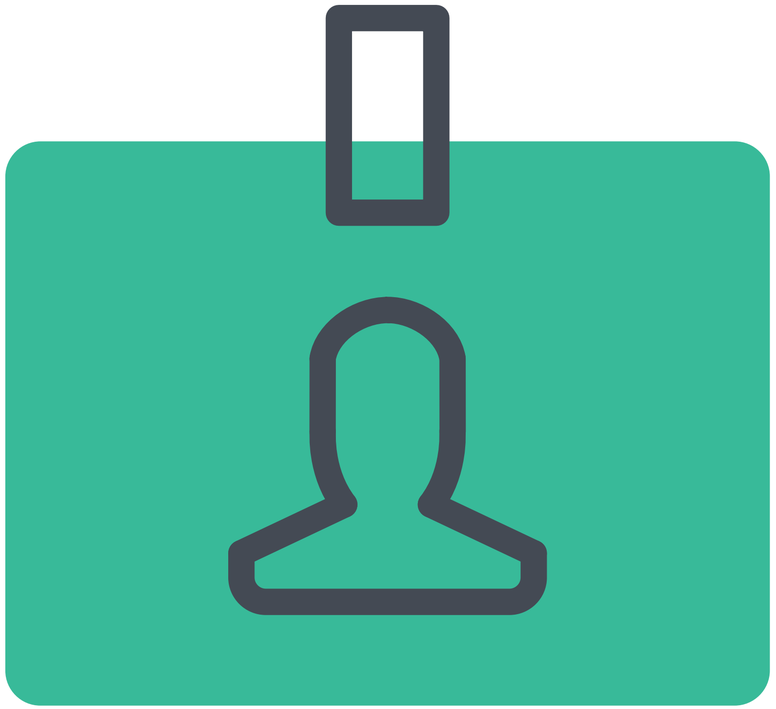
Microsoft Entra ID



Okta Identity Engine

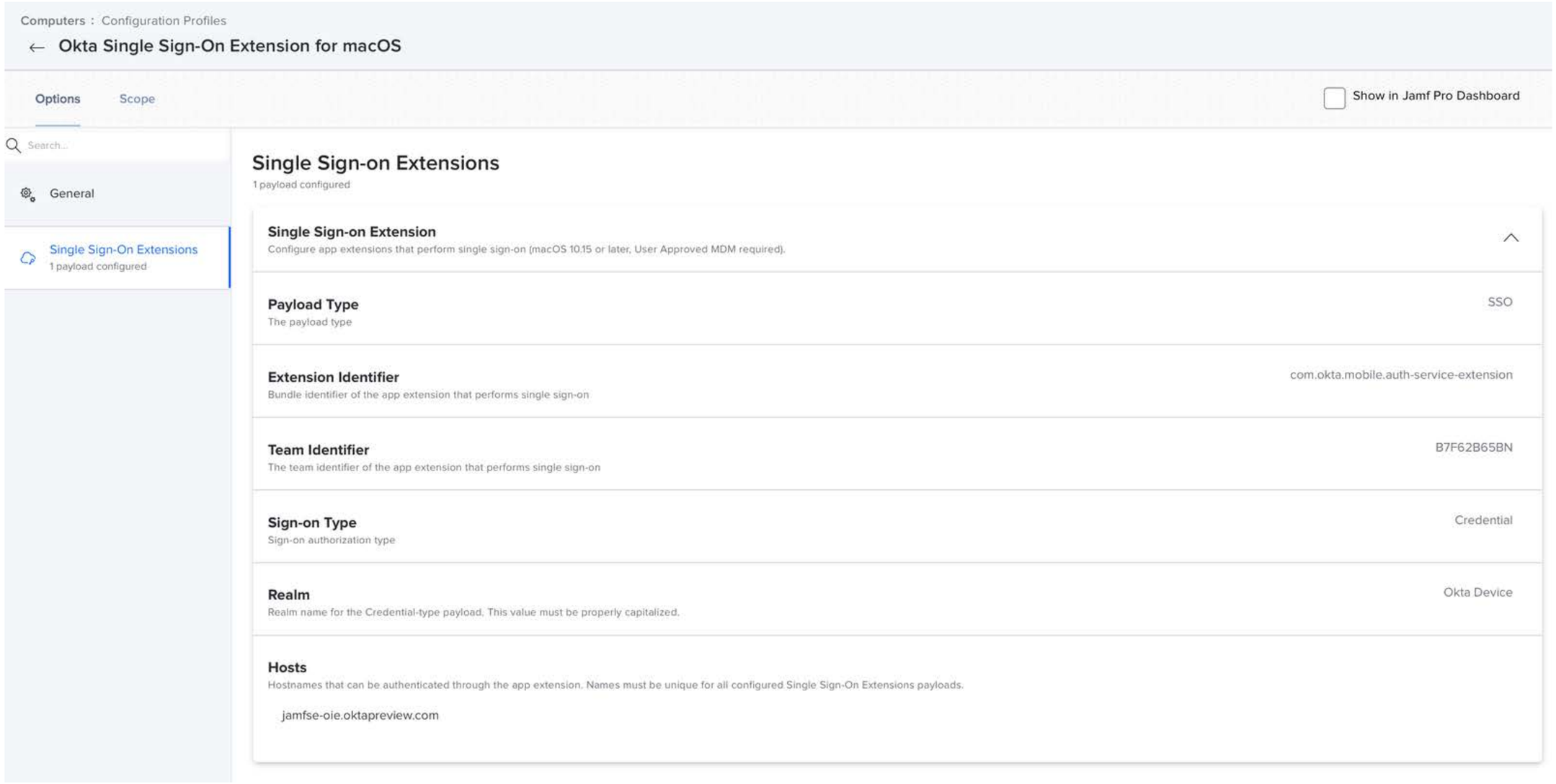
jamf

Single Sign On - A Possession Factor



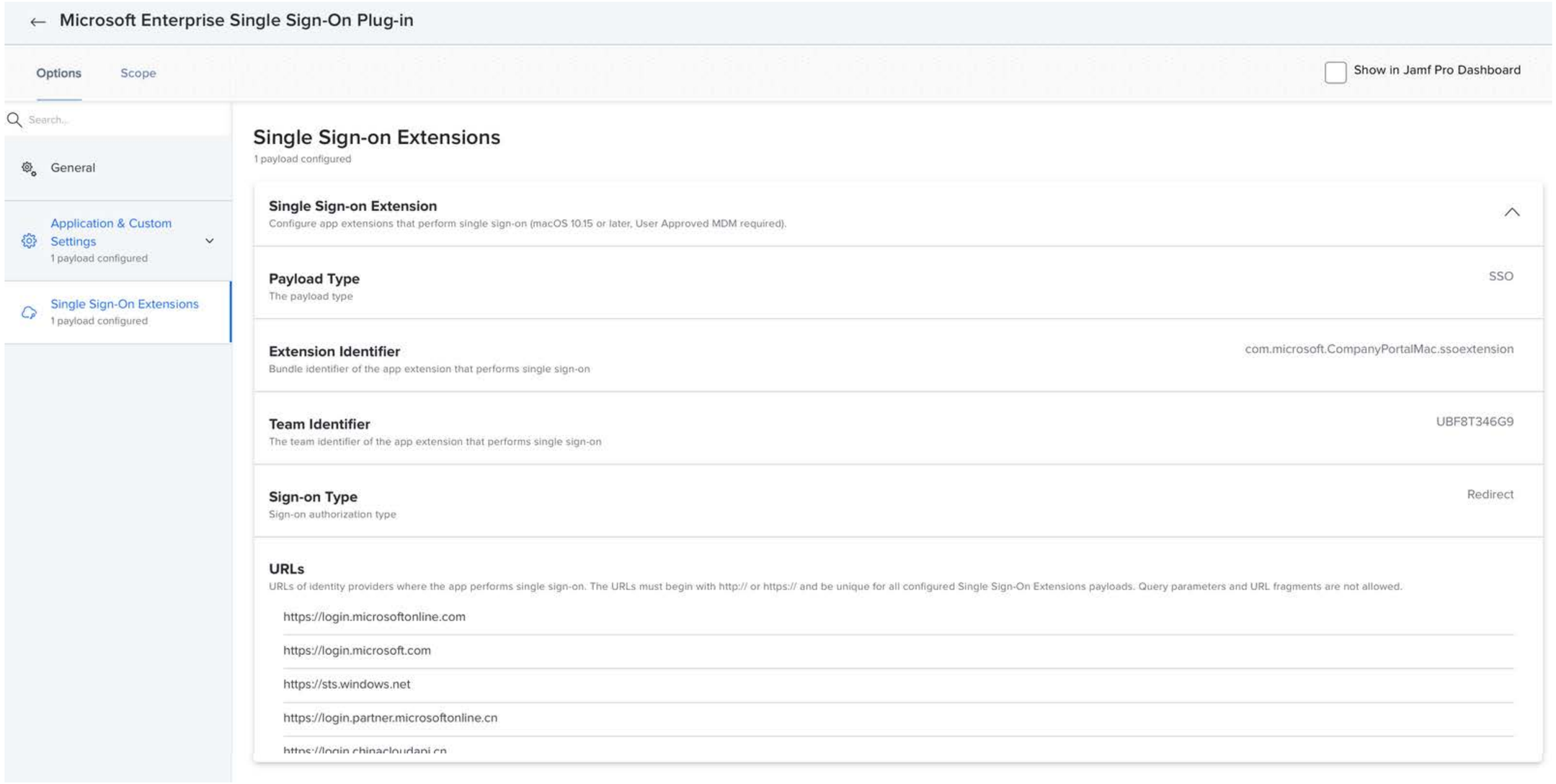
- It's on a managed device
- It's only active via an MDM installed profile
- Once it's active.... it's active
- Works in Private Browsing mode

Extensible Single Sign-On



jamf

Extensible Single Sign-On



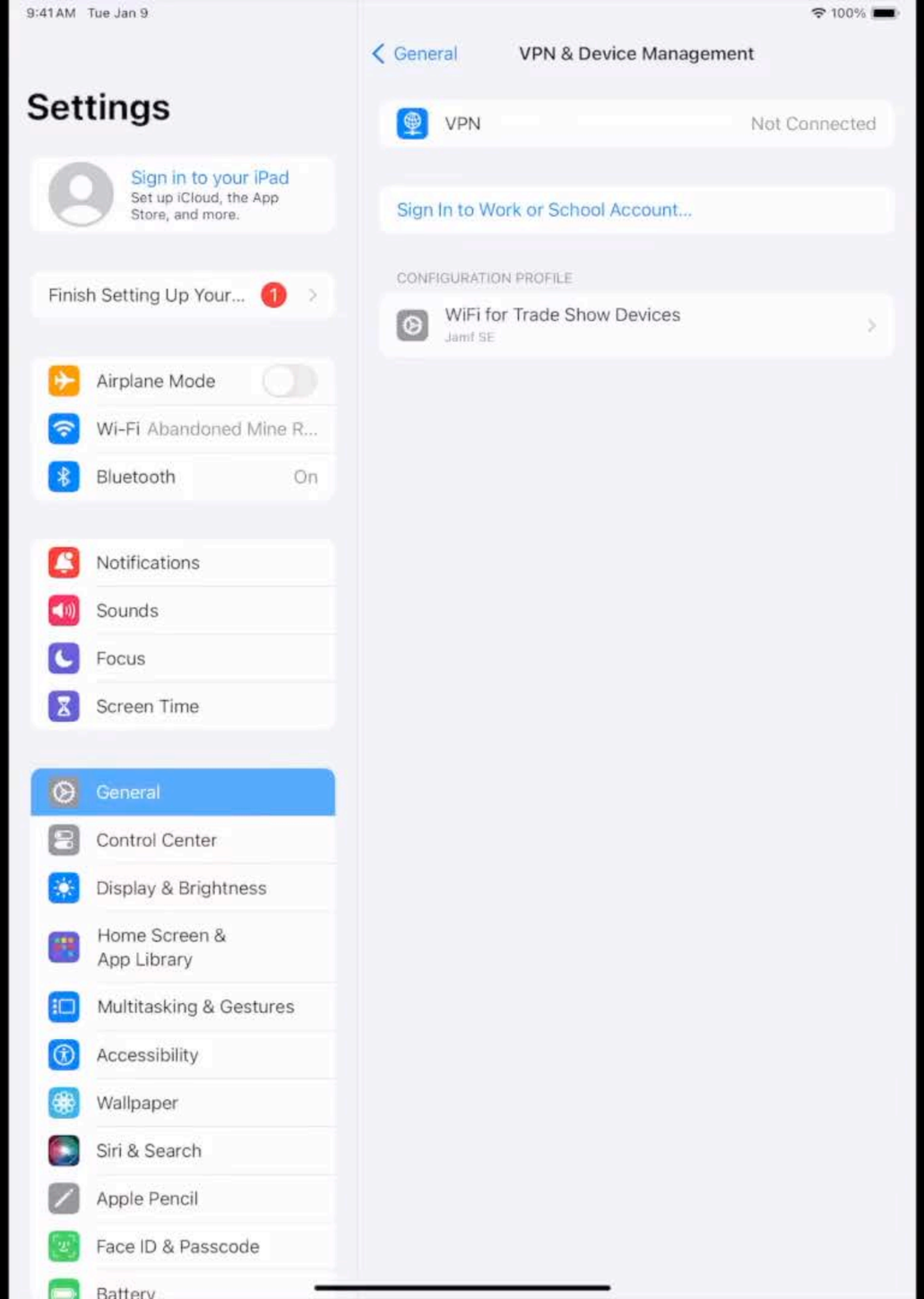
jamf

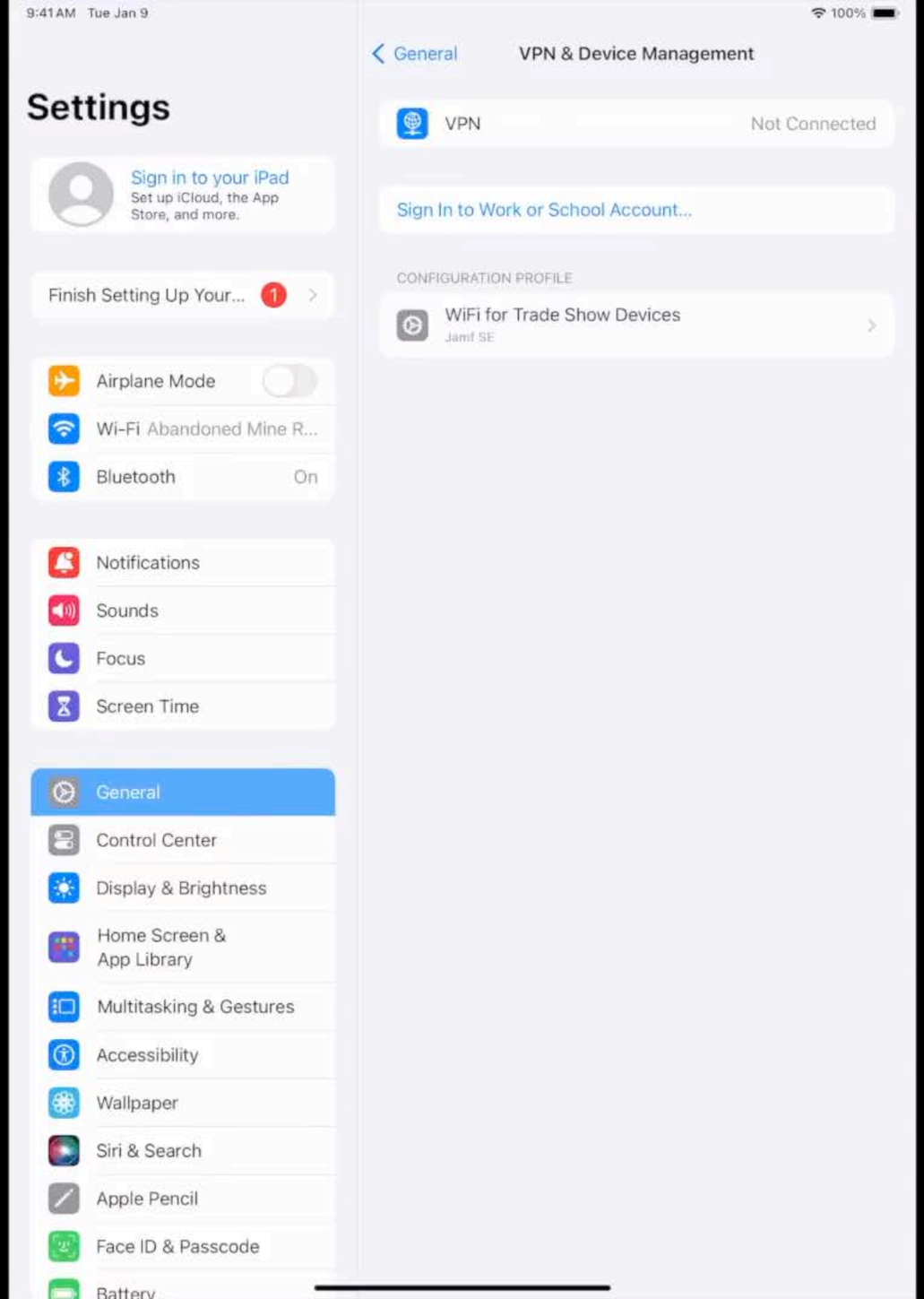

Finder
File
Edit
View
Go
Window
Help
Wed Jun 12 10:50 AM
JUN
12
tv

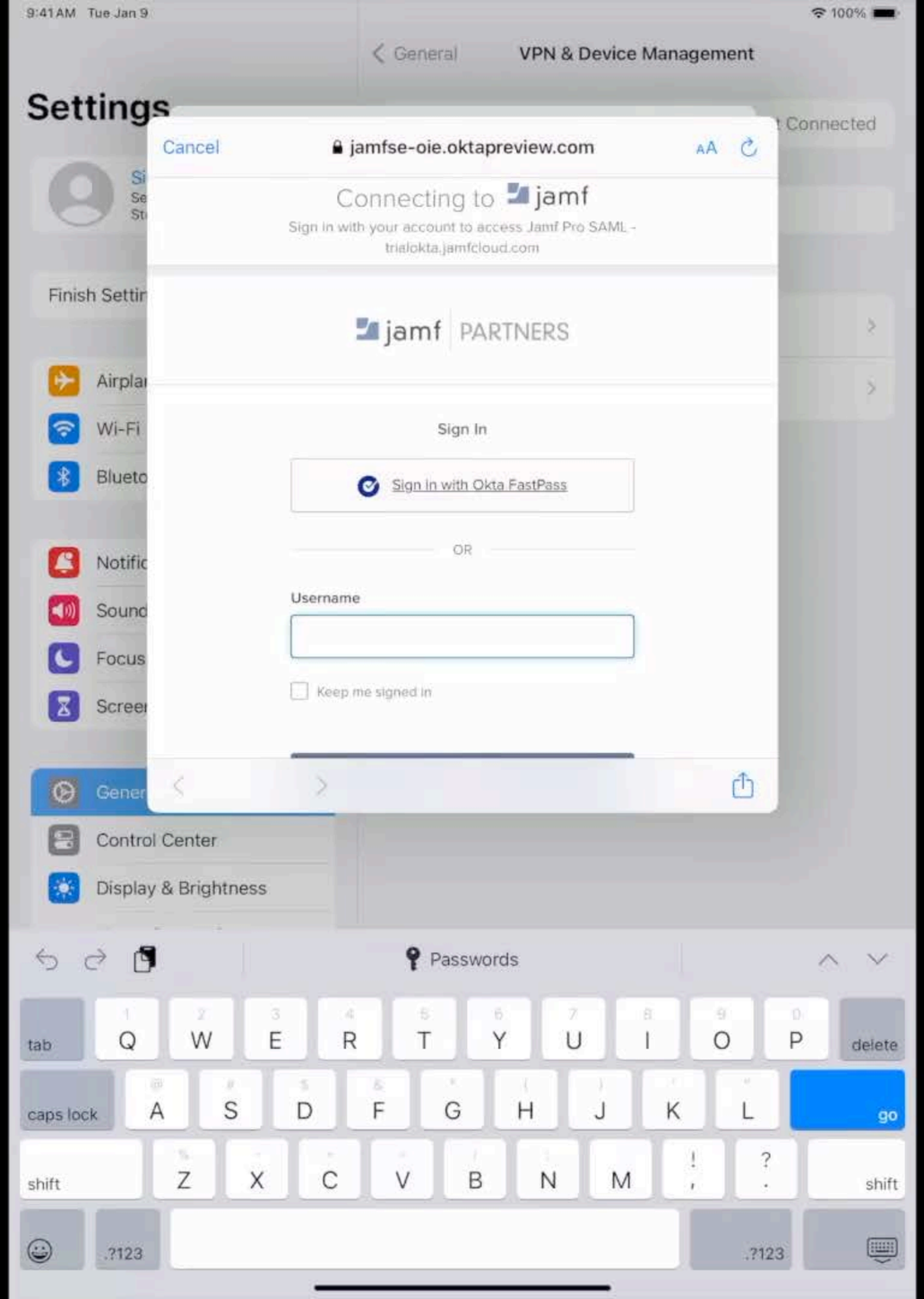

Finder
File
Edit
View
Go
Window
Help
Wed Jun 12 10:50 AM
JUN
12
tv

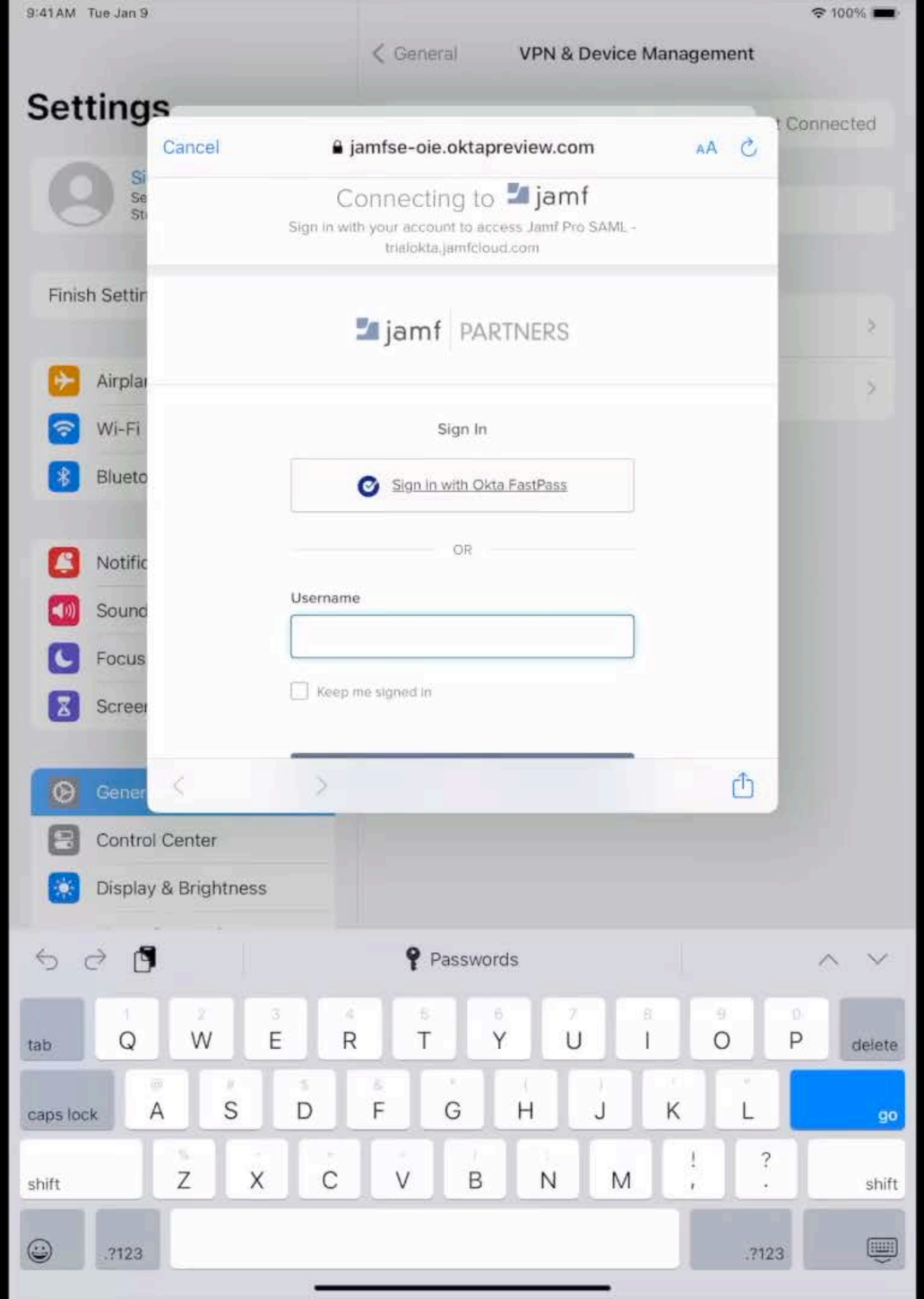

Safari File Edit View History Bookmarks Window Help
Wed Jun 12 10:59 AM
Jamf Connect
Complete multifactor authentication registration to increase device security.
JUN
12
tv

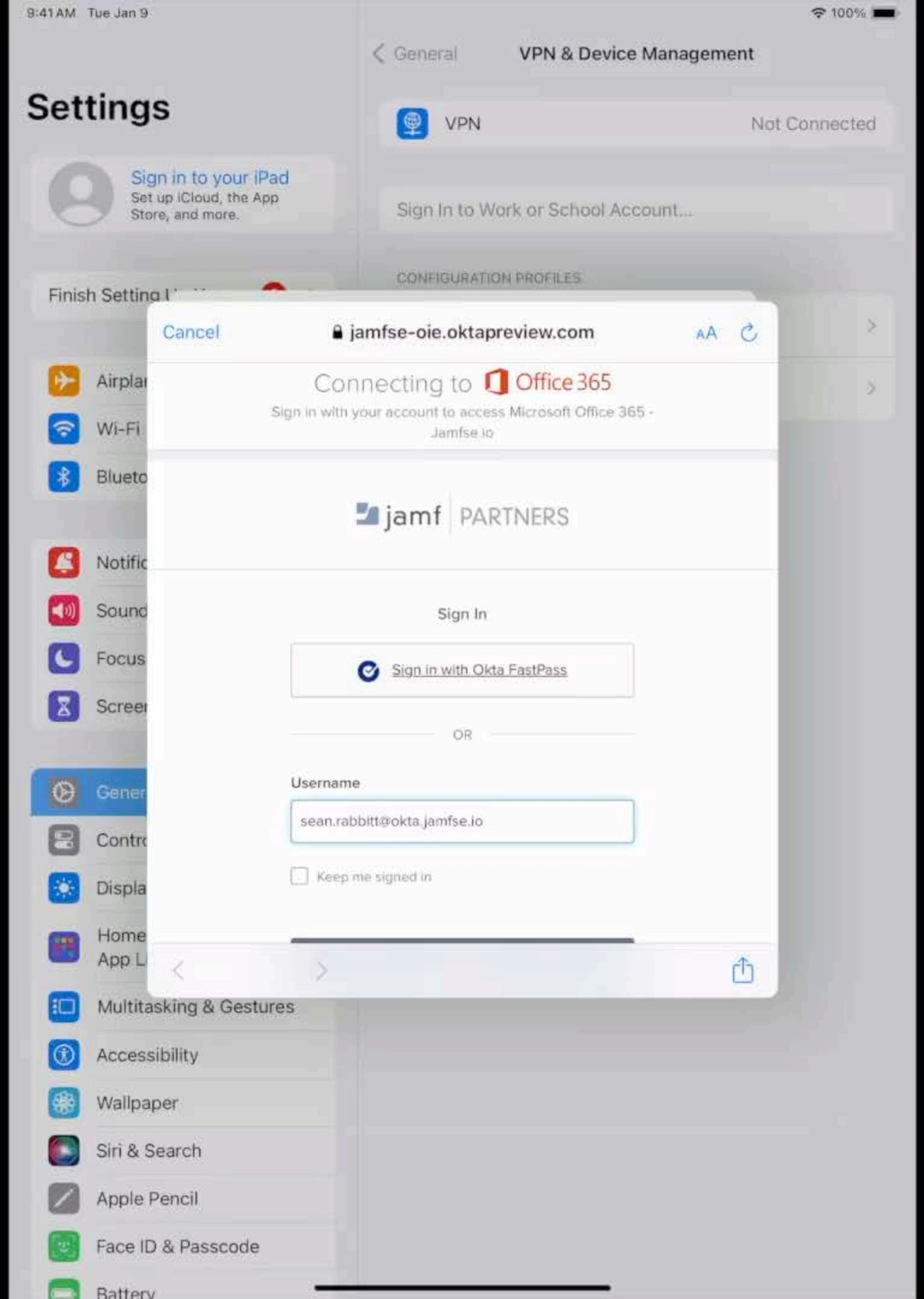

Safari File Edit View History Bookmarks Window Help
Wed Jun 12 10:59 AM
Jamf Connect
Complete multifactor authentication registration to increase device security.
JUN
12
tv

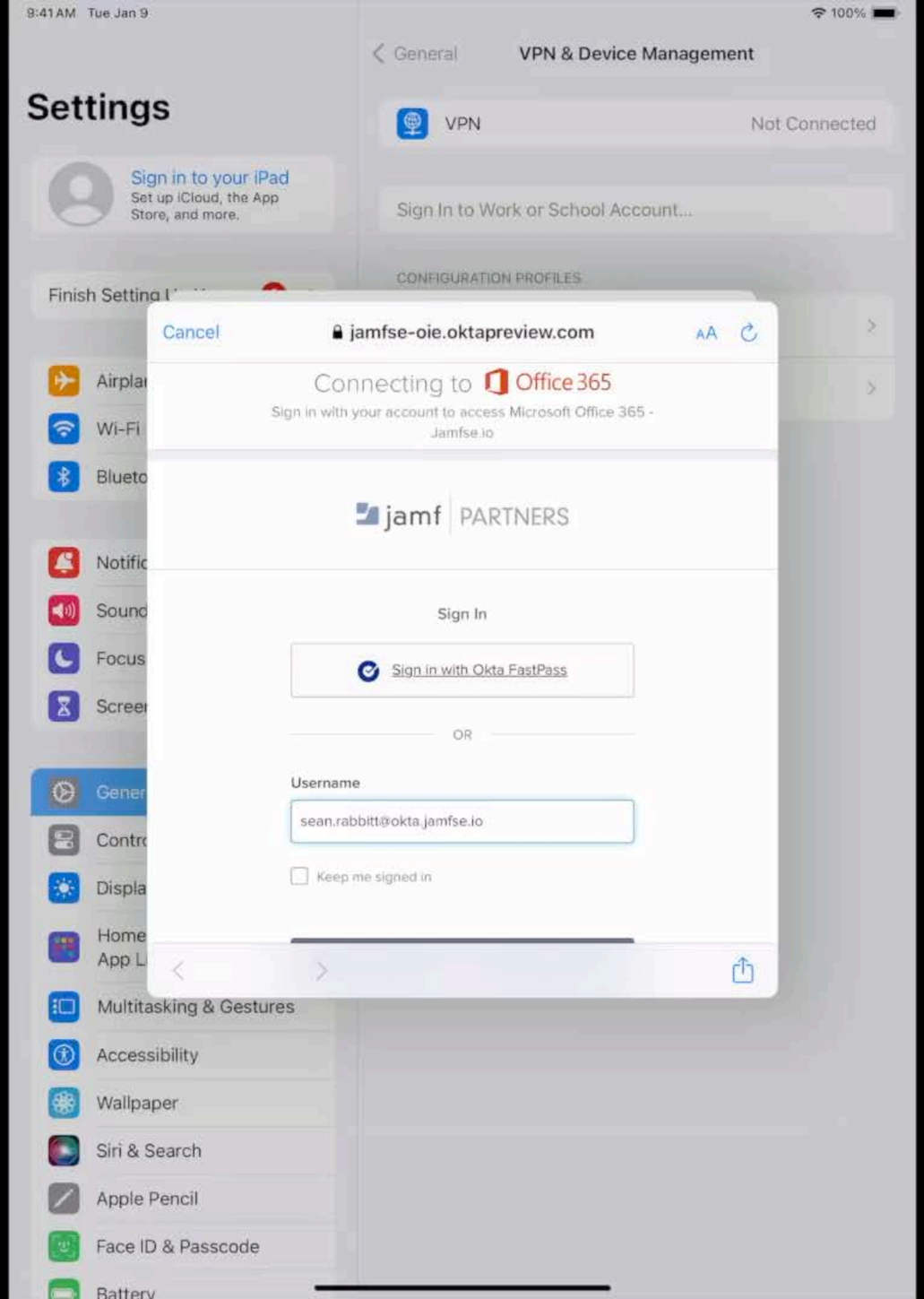

9:41 AM Tue Jan 9
100%
Settings
Sign in to your iPad
Set up iCloud, the App Store, and more.
Finish Setting Up Your... 1
Airplane Mode
Wi-Fi Abandoned Mine R...
Bluetooth On
Notifications
Sounds
Focus
Screen Time
General
Control Center
Display & Brightness
Home Screen & App Library
Multitasking & Gestures
Accessibility
Wallpaper
Siri & Search
Apple Pencil
Face ID & Passcode
Battery
General
VPN & Device Management
VPN Not Connected
Sign In to Work or School Account...
CONFIGURATION PROFILE
WiFi for Trade Show Devices
Jamf SE

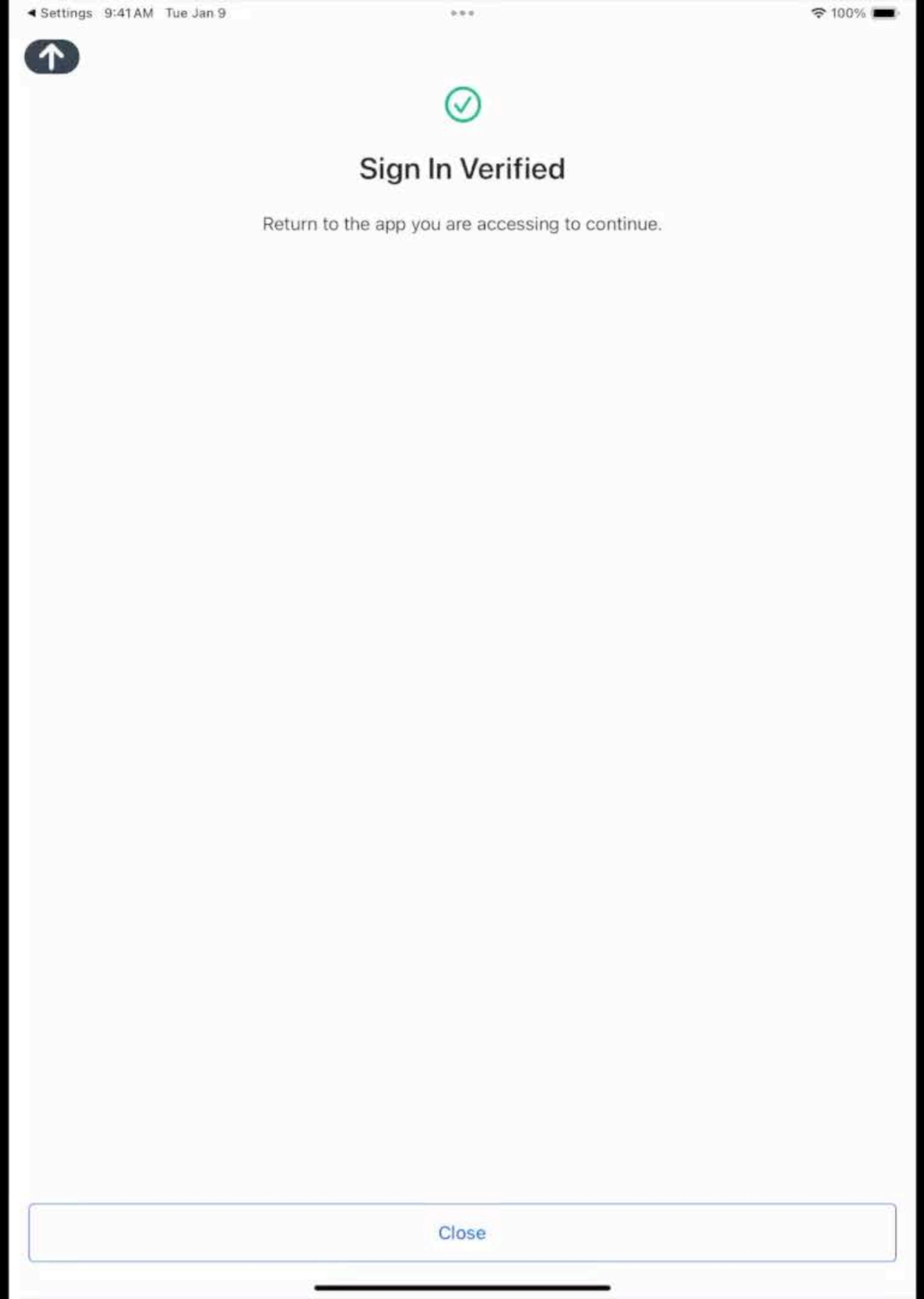

9:41 AM Tue Jan 9
100%
Settings
Sign in to your iPad
Set up iCloud, the App Store, and more.
Finish Setting Up Your... 1
Airplane Mode
Wi-Fi Abandoned Mine R...
Bluetooth On
Notifications
Sounds
Focus
Screen Time
General
Control Center
Display & Brightness
Home Screen & App Library
Multitasking & Gestures
Accessibility
Wallpaper
Siri & Search
Apple Pencil
Face ID & Passcode
Battery
General
VPN & Device Management
VPN Not Connected
Sign In to Work or School Account...
CONFIGURATION PROFILE
WiFi for Trade Show Devices
Jamf SE

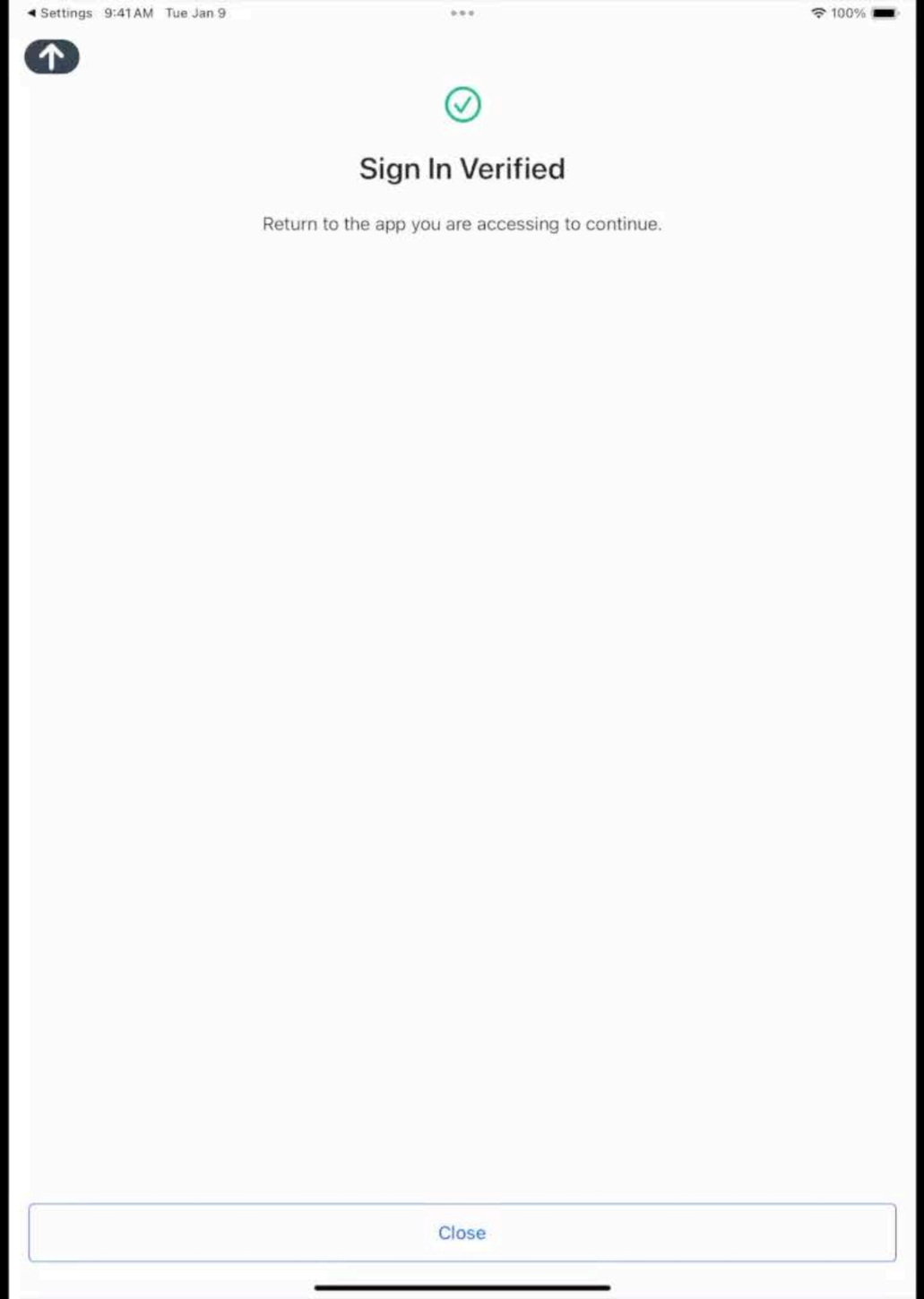

9:41 AM Tue Jan 9
100%
General
VPN & Device Management
Settings
Connected
Finish Settin
Airplan
Wi-Fi
Blueto
Notific
Sound
Focus
Screen
Gener
Control Center
Display & Brightness
Cancel
jamfse-oie.oktapreview.com
AA
Connecting to jamf
Sign in with your account to access Jamf Pro SAML - trialokta.jamfcloud.com
jamf PARTNERS
Sign In
Sign in with Okta FastPass
OR
Username
Keep me signed in
Passwords
tab
caps lock
shift
delete
go
.?123


9:41 AM Tue Jan 9
100%
General
VPN & Device Management
Settings
Connected
Finish Settin
Airplan
Wi-Fi
Blueto
Notific
Sound
Focus
Screen
Gener
Control Center
Display & Brightness
Cancel
jamfse-oie.oktapreview.com
AA
Connecting to jamf
Sign in with your account to access Jamf Pro SAML - trialokta.jamfcloud.com
jamf PARTNERS
Sign In
Sign in with Okta FastPass
OR
Username
Keep me signed in
Passwords
tab
caps lock
shift
delete
go
.?123

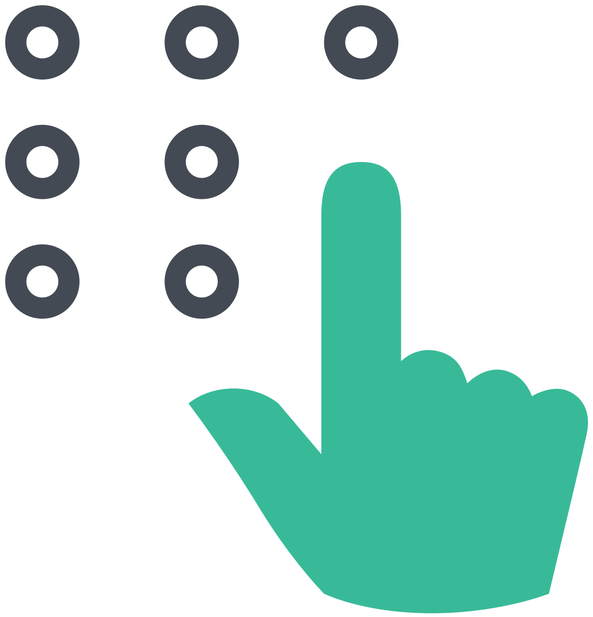

9:41 AM Tue Jan 9
100%
Settings
Sign in to your iPad
Set up iCloud, the App Store, and more.
Finish Setting
Airplan
Wi-Fi
Blueto
Notific
Sound
Focus
Scree
Gener
Contro
Displa
Home
App L
Multitasking & Gestures
Accessibility
Wallpaper
Siri & Search
Apple Pencil
Face ID & Passcode
Battery
General
VPN & Device Management
VPN
Not Connected
Sign In to Work or School Account...
CONFIGURATION PROFILES
Cancel
jamfse-oie.oktapreview.com
AA
Connecting to Office 365
Sign in with your account to access Microsoft Office 365 - Jamfse.io
jamf PARTNERS
Sign In
Sign in with Okta FastPass
OR
Username
sean.rabbitt@okta.jamfse.io
Keep me signed in


9:41 AM Tue Jan 9
100%
Settings
Sign in to your iPad
Set up iCloud, the App Store, and more.
Finish Setting
Airplan
Wi-Fi
Blueto
Notific
Sound
Focus
Scree
Gener
Contro
Displa
Home
App L
Multitasking & Gestures
Accessibility
Wallpaper
Siri & Search
Apple Pencil
Face ID & Passcode
Battery
General
VPN & Device Management
VPN
Not Connected
Sign In to Work or School Account...
CONFIGURATION PROFILES
Cancel
jamfse-oie.oktapreview.com
AA
Connecting to Office 365
Sign in with your account to access Microsoft Office 365 - Jamfse.io
jamf PARTNERS
Sign In
Sign in with Okta FastPass
OR
Username
sean.rabbitt@okta.jamfse.io
Keep me signed in

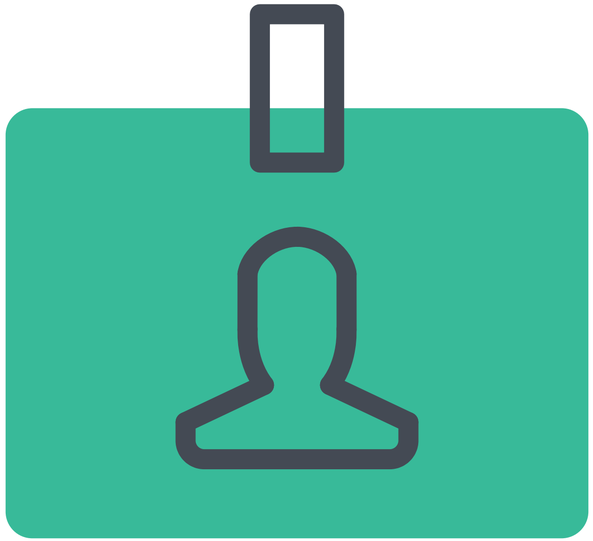

Settings 9:41 AM Tue Jan 9
100%
Sign In Verified
Return to the app you are accessing to continue.
Close


Settings 9:41 AM Tue Jan 9
100%
Sign In Verified
Return to the app you are accessing to continue.
Close

Apple Extensible Single Sign On



Knowledge

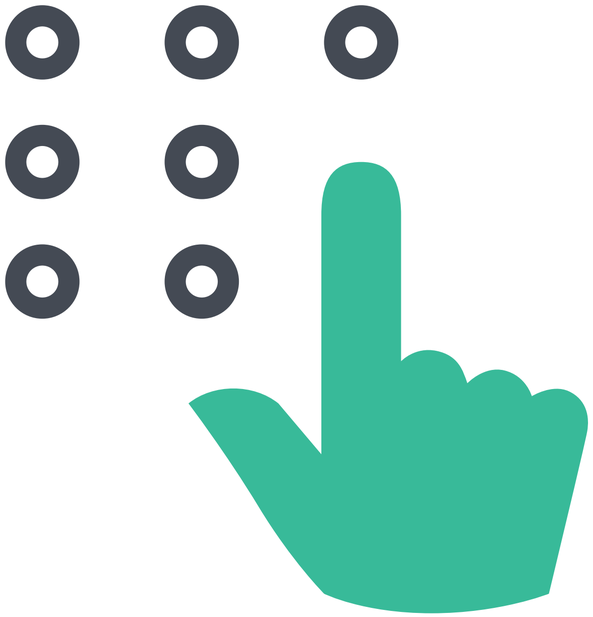


Possession

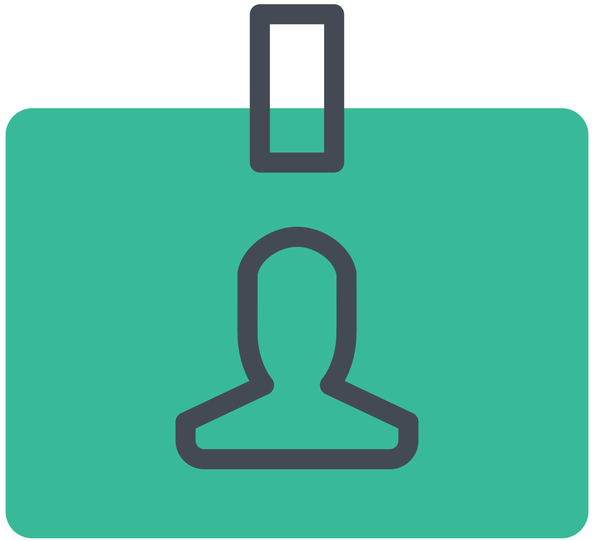
Biometric

jamf

Apple Extensible Single Sign On



Knowledge



Possession

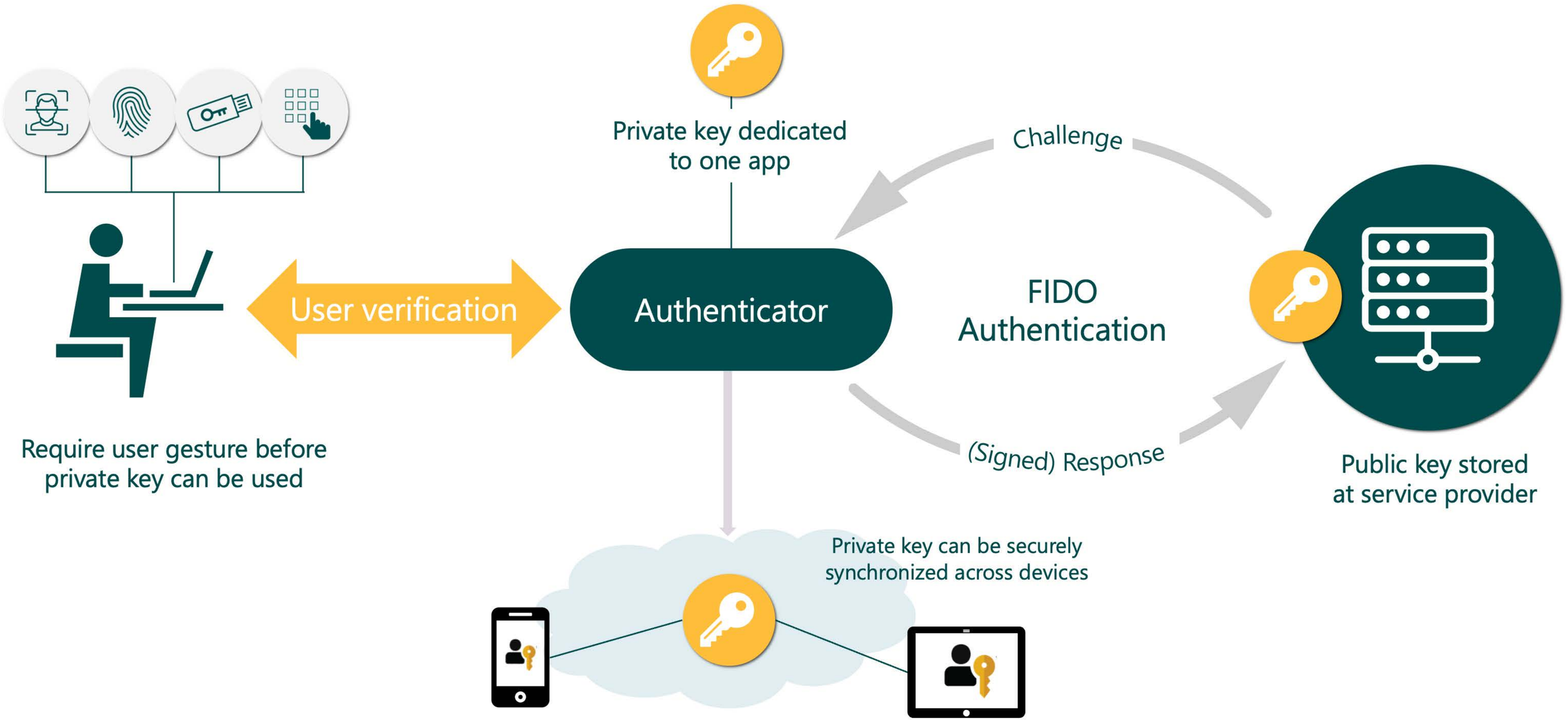
Biometric

jamf

=

With one major exception.....

jamf

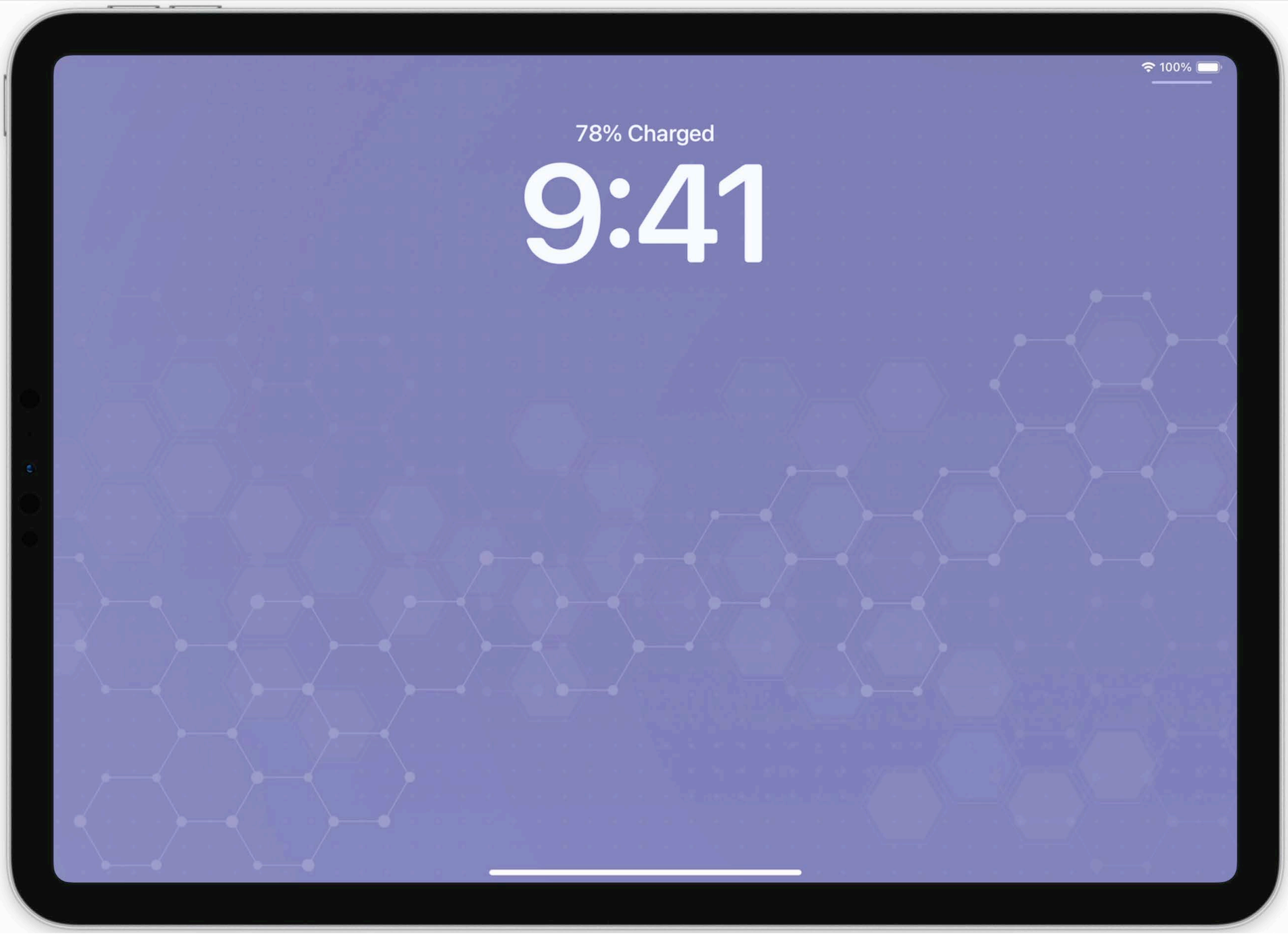


jamf

Require user gesture before private key can be used

jamf

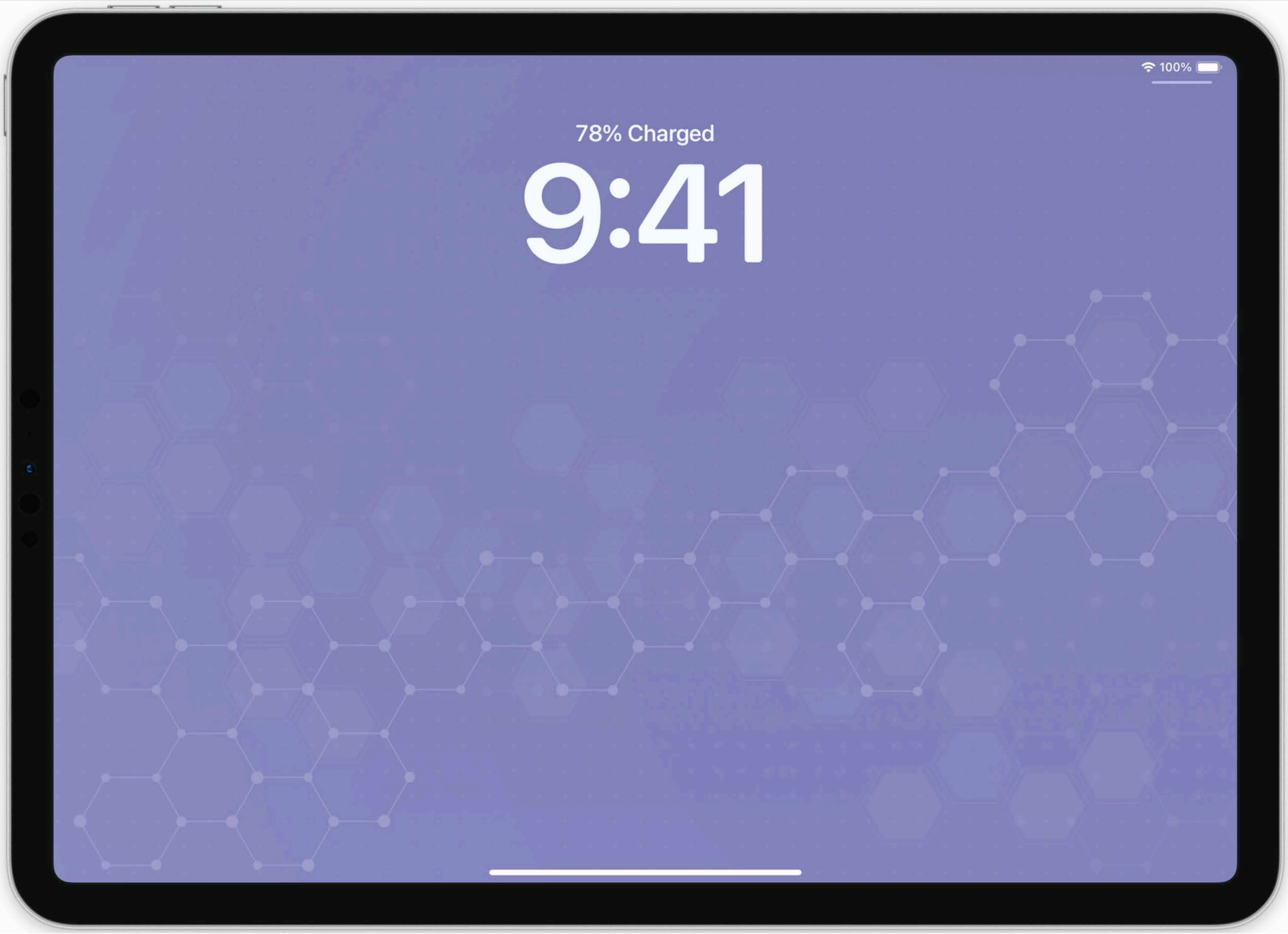
FIDO Seminar at RSAC: The State of Authentication 2024:the Global Progress Past Passwords
https://fidoalliance.org/content-presentations-fido-seminar-at-rsac-2024/



jamf

Bezel ❤️

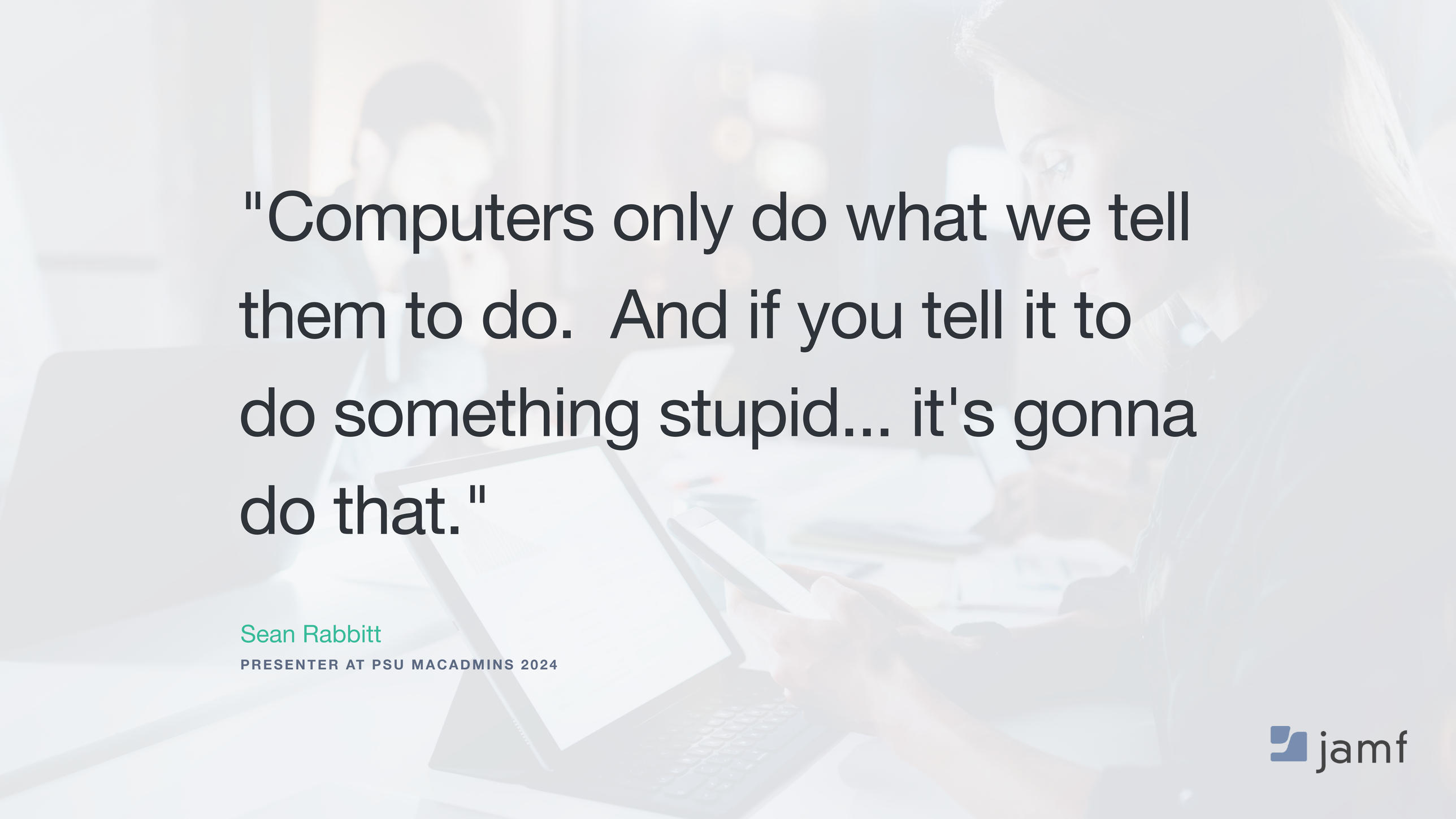
Sherlocked June 10, 2024



jamf

Bezel ❤️

Sherlocked June 10, 2024



"Computers only do what we tell them to do. And if you tell it to do something stupid... it's gonna do that."

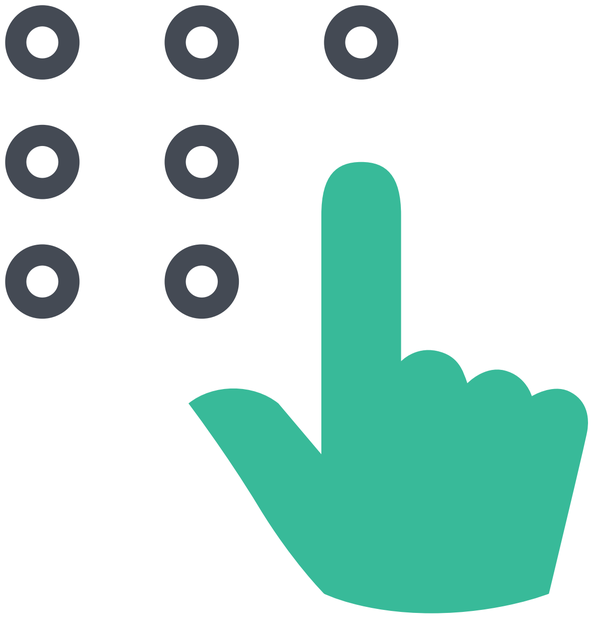
Sean Rabbitt

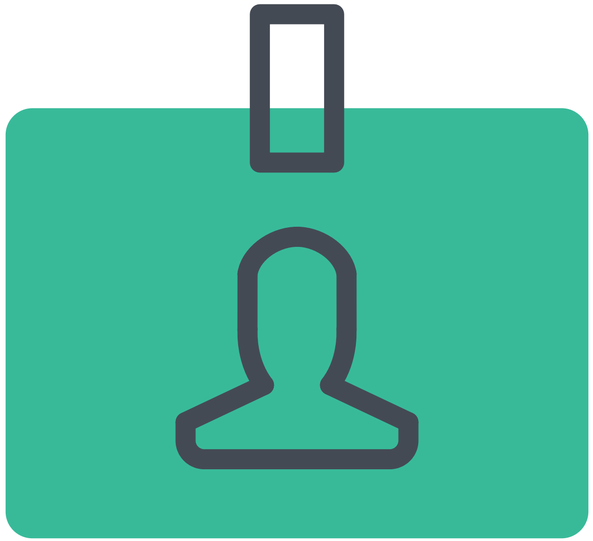
PRESENTER AT PSU MACADMINS 2024

jamf

Single Sign On does not have a mandatory requirement for **User Verification**

jamf

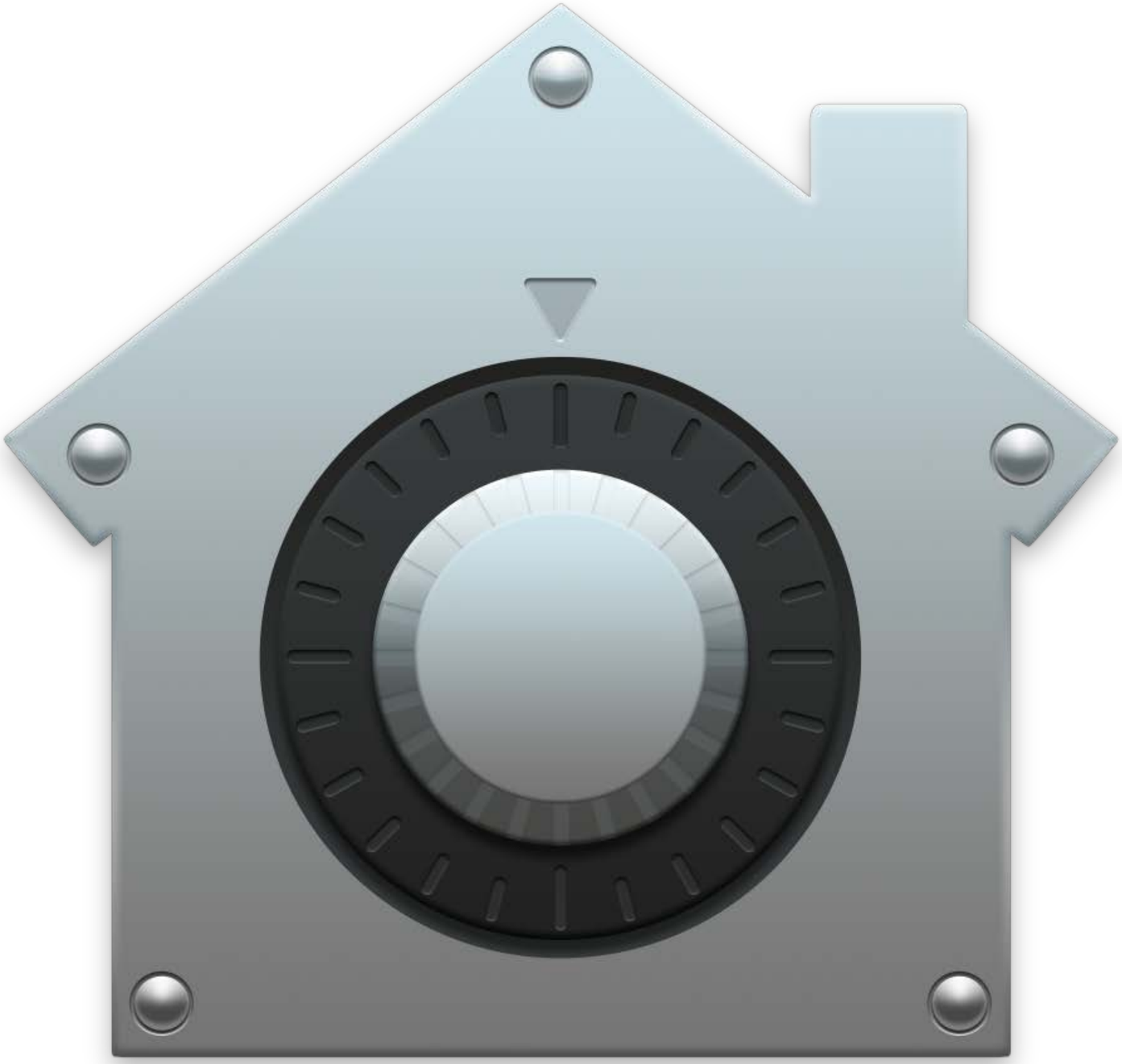




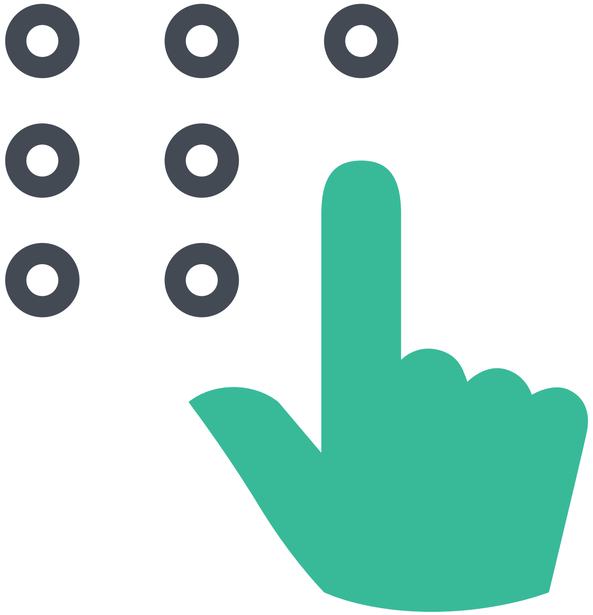
jamf

Hardening with authentication rules and additional factors

jamf



jamf



Something you know

- PIN
- Password
- ~~Mother's Maiden Name~~

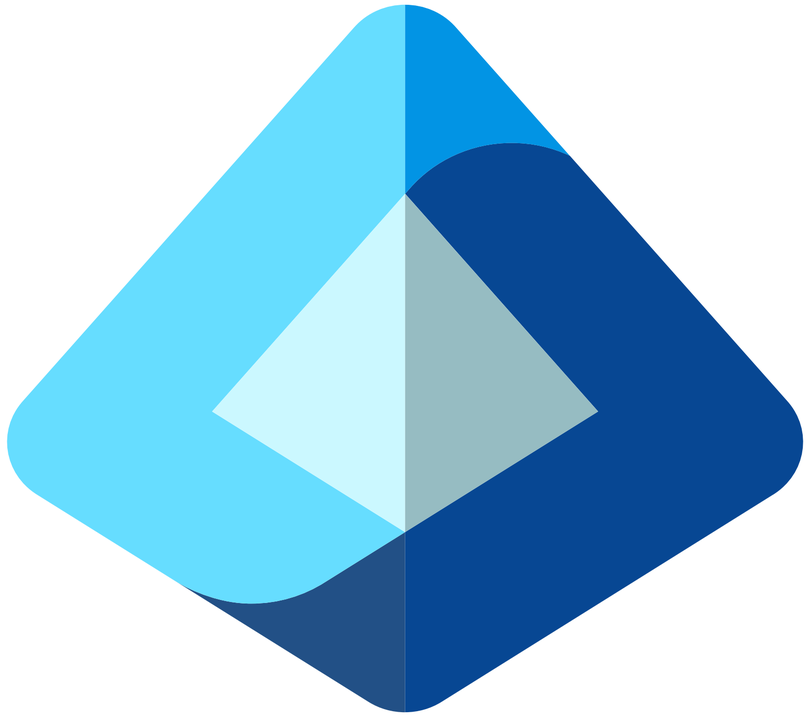
Something you have

- PIV / SmartCard
- ~~FIDO2 hardware token~~
- ~~Some other device~~

~~Something you are~~

- ~~TouchID / FaceID~~
- ~~Fingerprint scanner~~
- ~~Retinal scanner~~

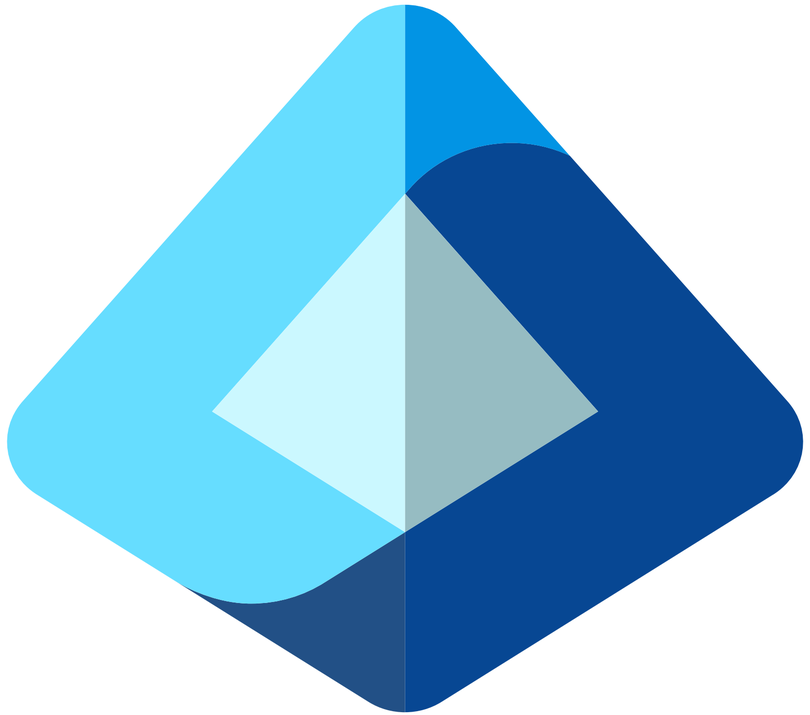
jamf



Microsoft Entra ID -> Security

- Enable authentication methods
  - FIDO2 key
  - Microsoft Authenticator
  - OAUTH tokens
  - Cert based
  - Passkey

jamf

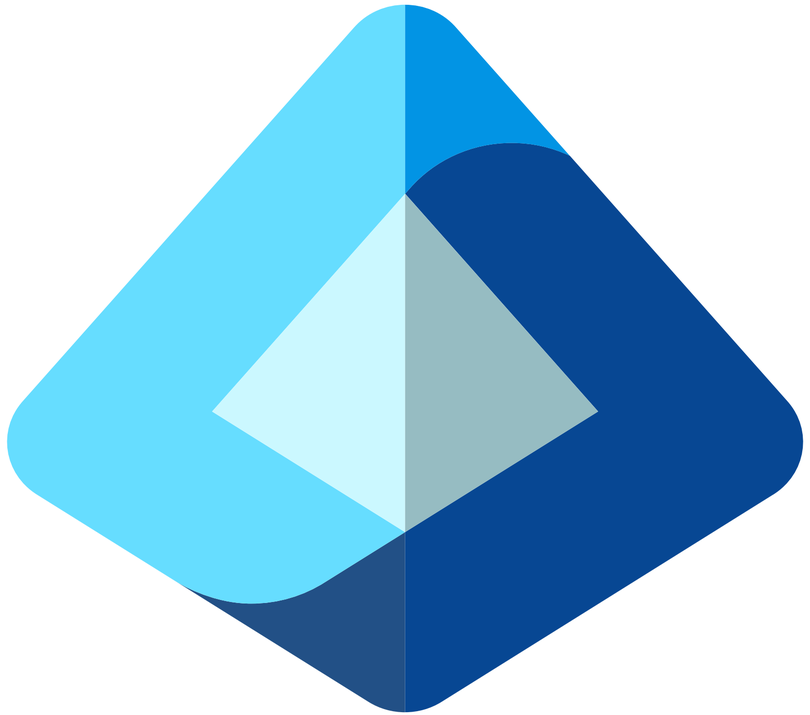


Microsoft Entra ID -> Security

- Enable authentication methods
  - FIDO2 key
  - Microsoft Authenticator
  - OAUTH tokens
  - Cert based
  - Passkey

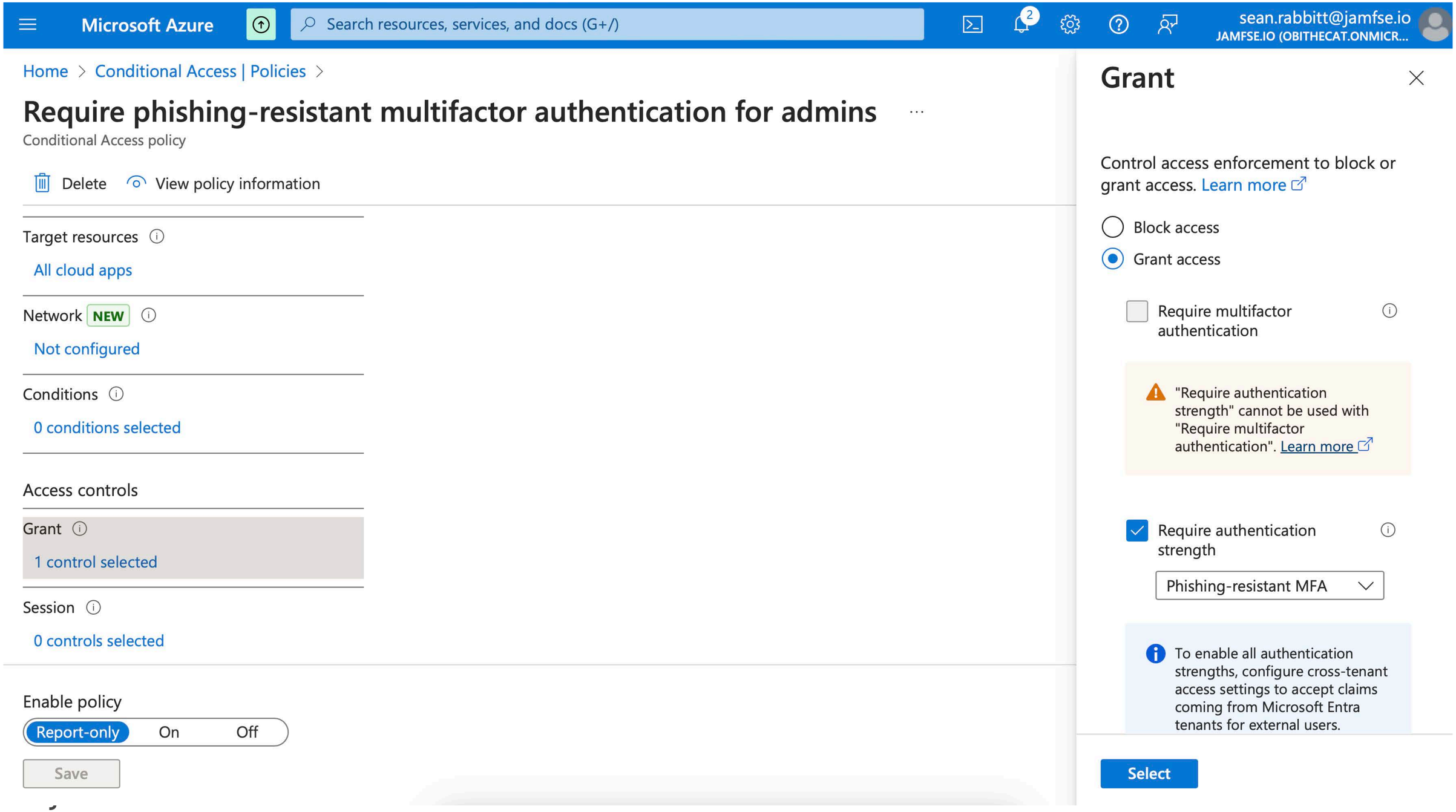
jamf

Microsoft Entra Conditional Access

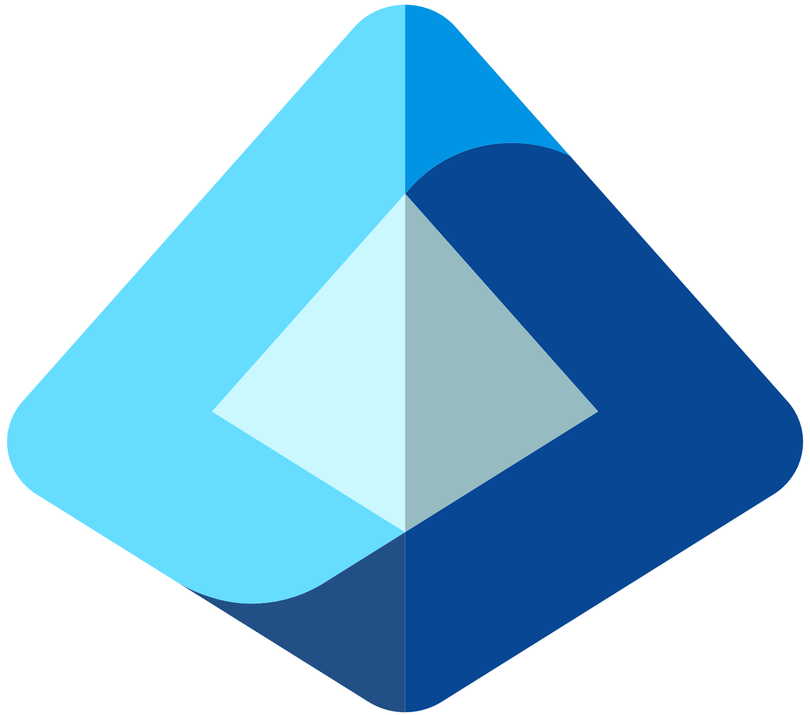


- Set requirement for multifactor OR
- Set requirement for non-phishable multifactor

jamf

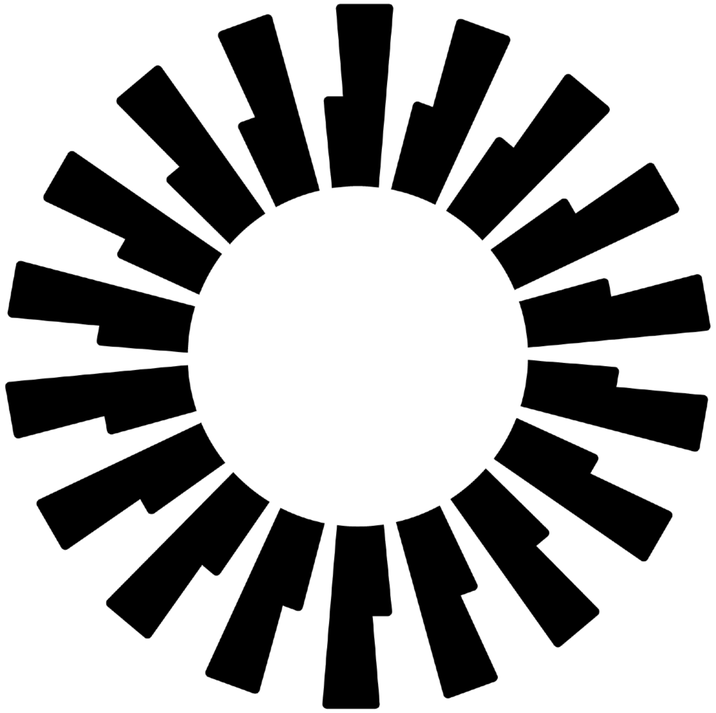

Microsoft Azure
Search resources, services, and docs (G+/)
sean.rabbitt@jamfse.io
JAMFSE.IO (OBITHECAT.ONMICR...
Home > Conditional Access | Policies >
Require phishing-resistant multifactor authentication for admins
Conditional Access policy
Delete
View policy information
Target resources
All cloud apps
Network NEW
Not configured
Conditions
0 conditions selected
Access controls
Grant
1 control selected
Session
0 controls selected
Enable policy
Report-only
On
Off
Save
Grant
Control access enforcement to block or grant access. Learn more
Block access
Grant access
Require multifactor authentication
"Require authentication strength" cannot be used with "Require multifactor authentication". Learn more
Require authentication strength
Phishing-resistant MFA
To enable all authentication strengths, configure cross-tenant access settings to accept claims coming from Microsoft Entra tenants for external users.
Select

Microsoft Entra - Issues



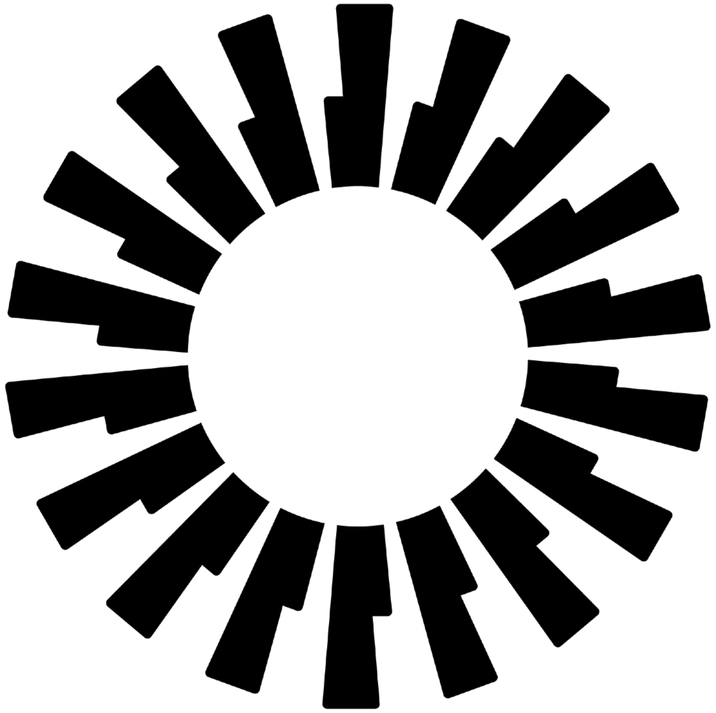
- "All cloud apps" may apply to unexpected resources and logins
- Additional devices needed for MFA
- Extensible SSOe is considered "non-phishable" method

Okta Identity Engine



- Security -> Global Session Policy
  - Establish user session with any factor used to meet requirements
  - MFA
    - Recommend set to "Not required"

Okta Identity Engine



Establish the user session with

- (•) Any factor used to meet the Authentication Policy requirements
- ( ) A password

An IdP claim will satisfy either of these options. The Authentication Policy determines the authentication requirement for a request.

Multifactor authentication (MFA) is

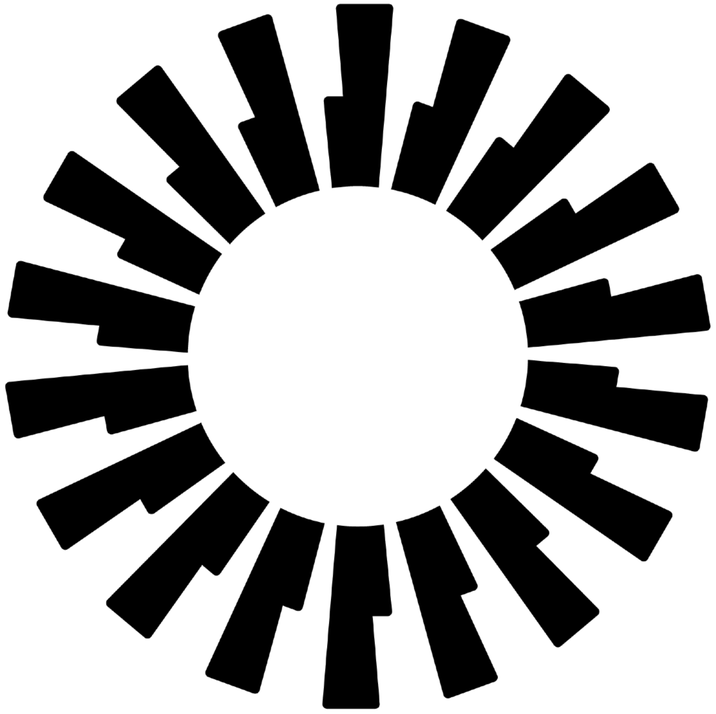
- (•) Not required
- ( ) Required

You can use the Authentication Policy to define multifactor requirements and characteristics of the allowed authenticators.

- Custom integrations that use the Okta Classic APIs are affected by this setting. Learn more
- Verify that multifactor authentication for your key applications is turned on. Learn more

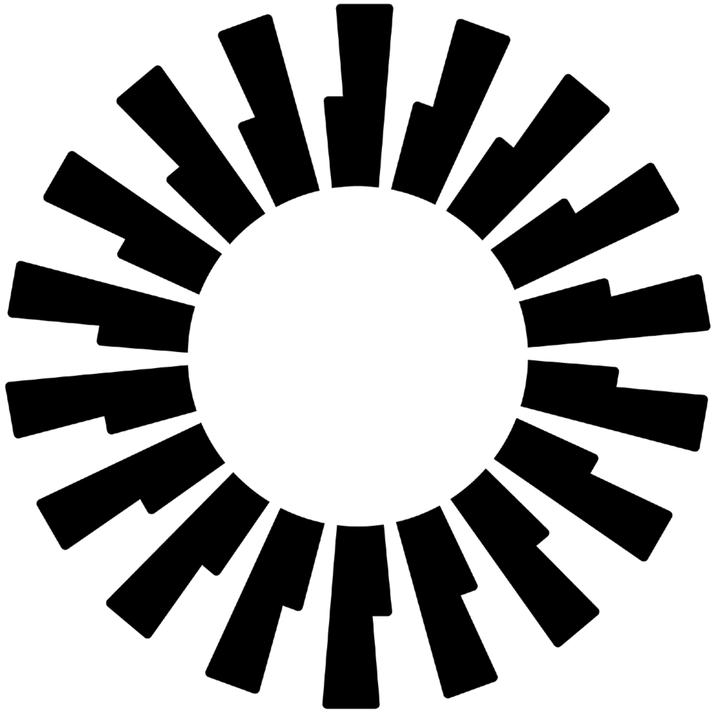
jamf

Okta Identity Engine



- Security -> Authentication policies
- User must authenticate with:
  - Any 1 factor, excluding password
  - Any 2 factors
  - Password + Another Factor
- Possession factor constraints are
  - Require user interaction
  - Require PIN or biometric verification

Okta Identity Engine



THEN

THEN Access is

- Denied
- Allowed after successful authentication

AND User must authenticate with

Any 1 factor type

AND Authentication methods

- Allow any method that can be used to meet the requirement
- Disallow specific authentication methods
- Allow specific authentication methods

Password ×

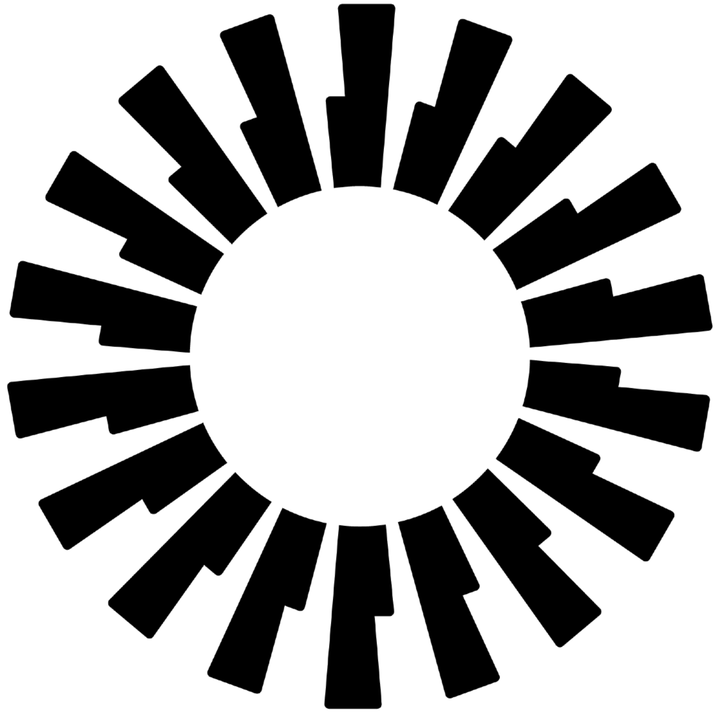
Remove

Your org's authenticators that satisfy this requirement:

1 factor type

Any TOTP Generator or Okta Verify - TOTP or Okta Verify - FastPass or Okta Verify - Push or FIDO2 (WebAuthn)

jamf



Okta Identity Engine

THEN

THEN Access is

- ○ Denied
- ◉ Allowed after successful authentication

AND User must authenticate with

Any 2 factor types

AND Possession factor constraints are

- ☐ Phishing resistant
- ☐ Hardware protected
- ☑ Require user interaction
  - ☑ Require PIN or biometric user verification

Learn more about possession factor constraints

AND Authentication methods

- ◉ Allow any method that can be used to meet the requirement
- ○ Disallow specific authentication methods
- ○ Allow specific authentication methods

Your org's authenticators that satisfy this requirement:

Knowledge / Biometric factor types

Okta Verify - FastPass[1] or Okta Verify - Push[1] or Password or FIDO2 (WebAuthn)[1]

AND

Additional factor types

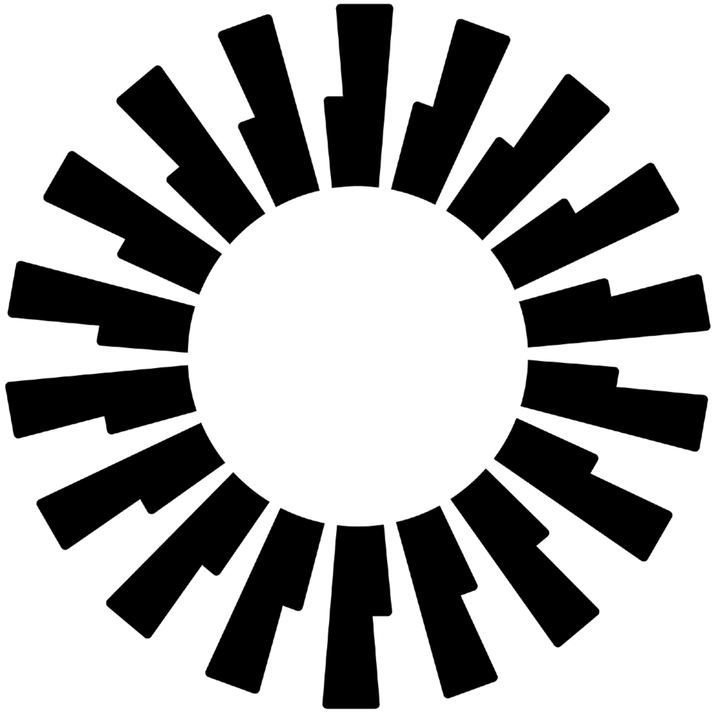
Okta Verify - FastPass[1] or Okta Verify - Push[1] or FIDO2 (WebAuthn)[1]

[1] *Authenticator that may satisfy multiple factor requirements*

Your org allows users to verify their identity with a knowledge factor (Password) before the possession factor. To change this, protect against password-based attacks in Security > General

jamf

Okta Identity Engine



THEN

THEN Access is

- ○ Denied
- ◉ Allowed after successful authentication

AND User must authenticate with

Password + Another factor

AND Possession factor constraints are

- ☐ Phishing resistant
- ☐ Hardware protected
- ☑ Require user interaction
  - ☑ Require PIN or biometric user verification

Learn more about possession factor constraints

AND Authentication methods

- ◉ Allow any method that can be used to meet the requirement
- ○ Disallow specific authentication methods
- ○ Allow specific authentication methods

Your org's authenticators that satisfy this requirement:

Password

AND

Additional factor types

Okta Verify - FastPass[1] or Okta Verify - Push[1] or FIDO2 (WebAuthn)[1]

Your org allows users to verify their identity with a knowledge factor (Password) before the possession factor. To change this, protect against password-based attacks in Security > General

jamf

Platform Single Sign-On

jamf

Platform Single Sign-On
and the authentication methods that love them

Password

- Local account password kept in sync with the cloud identity provider password
- Consistent FileVault password
- Updates password at macOS login screen, wake from screen saver

SmartCard

- Tie a PIV to your cloud identity provider account
- Physical key required - setup and infrastructure to support rollout
- Use the SmartCard to unlock FileVault on Macs with Apple Silicon processors

Secure Enclave Key

- Key used to authenticate to cloud identity provider stored in hardware bound Secure Element
- Still has a local UNIX password for account and FileVault
  - Enforce complexity via MDM configuration profile
- Local auth is Touch ID + PIN/ Passcode

jamf

Platform Single Sign-On
and the authentication methods that love them

Password

- Local account password kept in sync with the cloud identity provider password
- Consistent FileVault password
- Updates password at macOS login screen, wake from screen saver

SmartCard

- Tie a PIV to your cloud identity provider account
- Physical key required - setup and infrastructure to support rollout
- Use the SmartCard to unlock FileVault on Macs with Apple Silicon processors

Secure Enclave Key

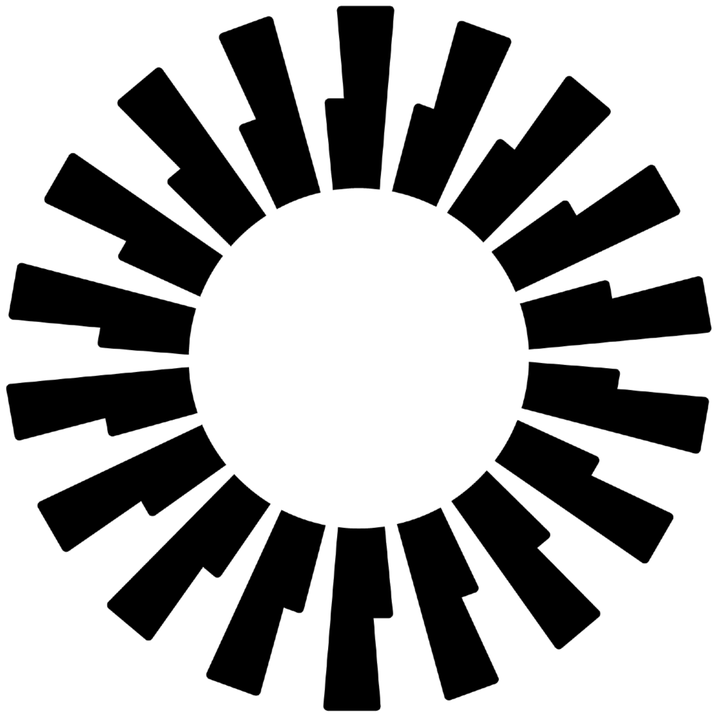
- Key used to authenticate to cloud identity provider stored in hardware bound Secure Element
- Still has a local UNIX password for account and FileVault
  - Enforce complexity via MDM configuration profile
- Local auth is Touch ID + PIN/ Passcode

jamf

Gratuitously cribbed from Microsoft
Go to Michael and Mark's session

Microsoft Entra ID

Uses "Redirect"



Okta Identity Engine

Uses "Credential" (for SSOe)

AND uses "Redirect" (for PSSOe)

We don’t talk about betas in public forums.

jamf

Platform Single Sign-on

To support highly secure macOS deployments that require authentication with the IdP, Platform Single Sign-on (Platform SSO) in macOS 15 is extended to:

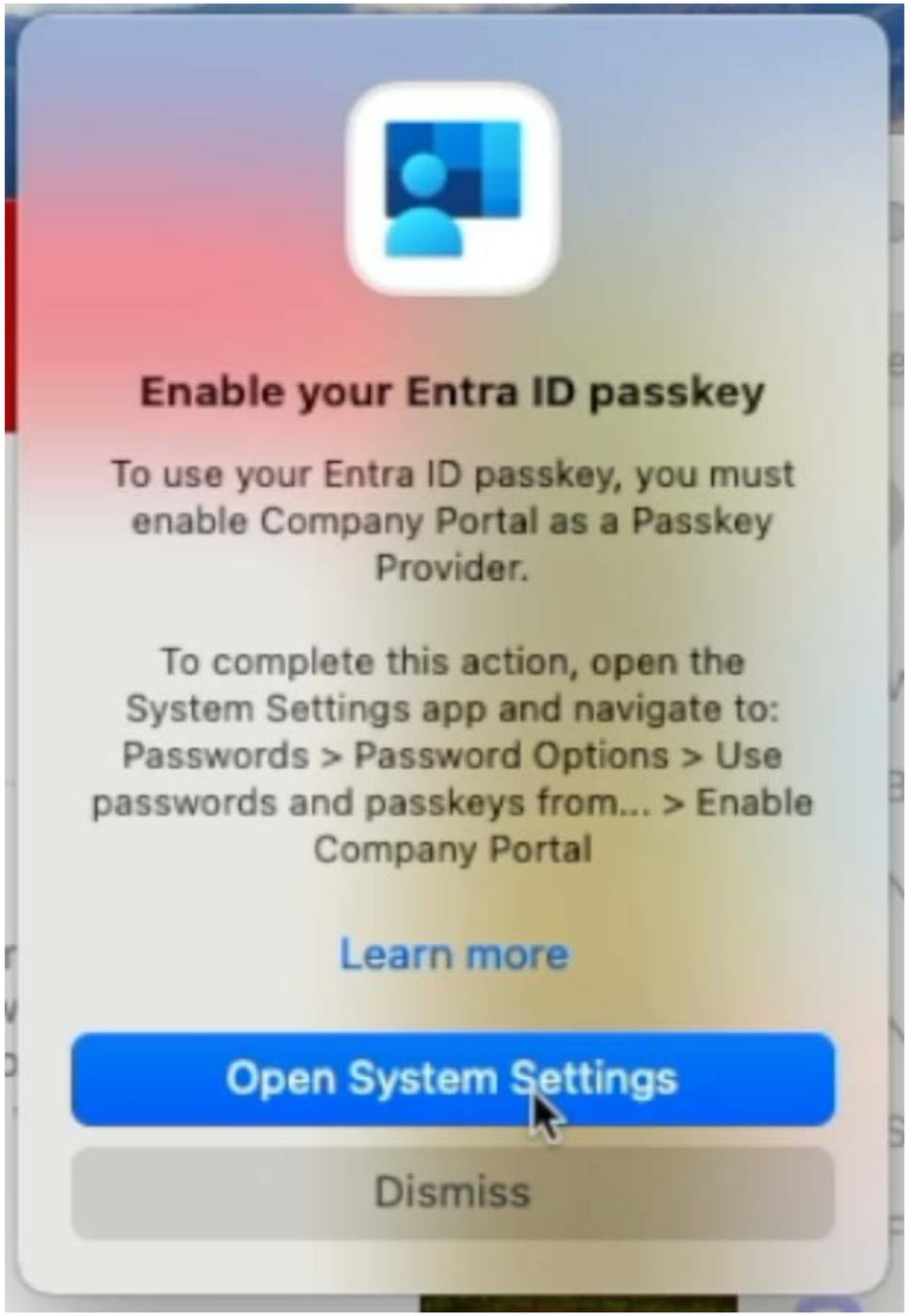
- Require IdP authentication across FileVault, the Lock Screen, and the login window, using a new policy option, `RequireAuthentication`
- Optionally configure Touch ID or Apple Watch to unlock the screen for ease of use when `RequireAuthentication` is enabled
- Configure offline and an authentication grace period, so that users can log in or unlock the screen when they're offline

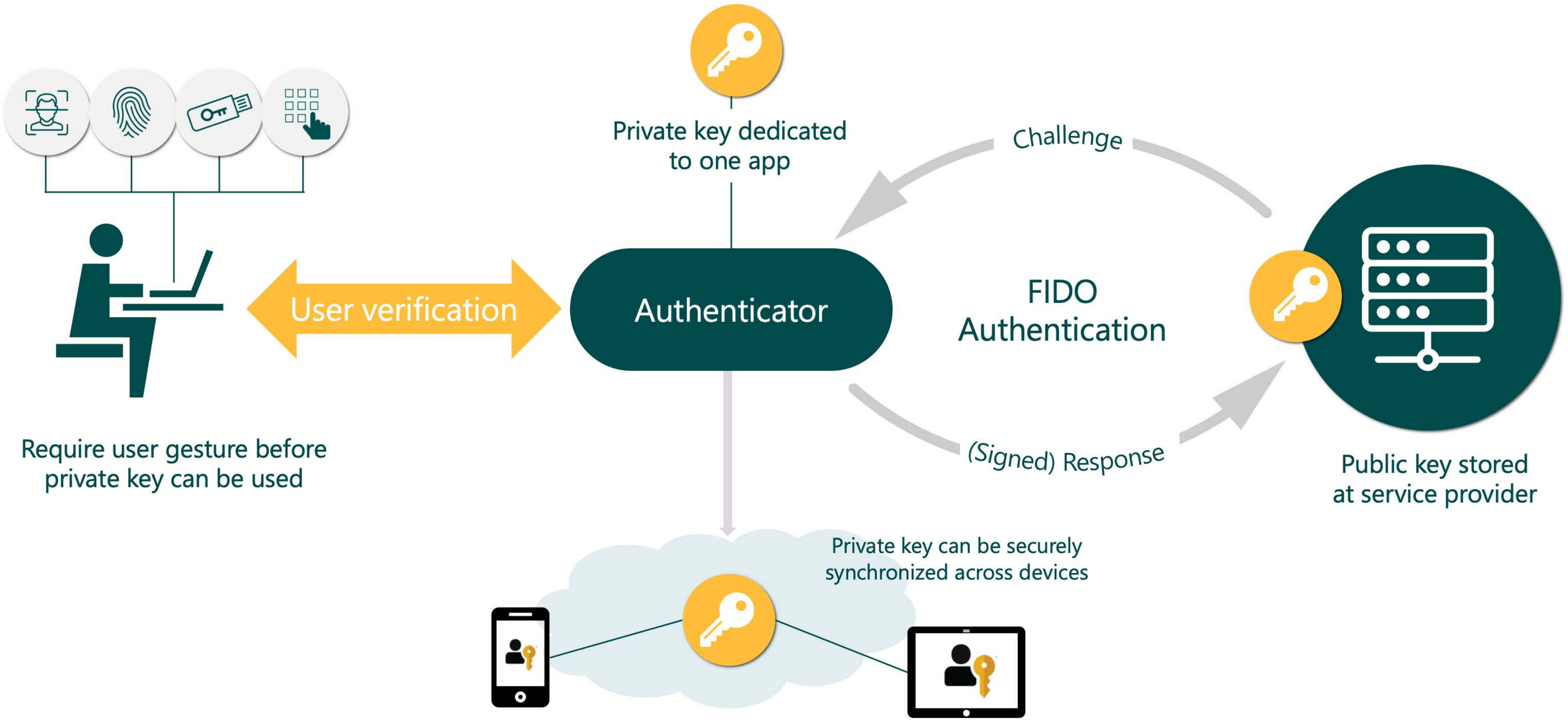
```
// Profile: com.apple.extensiblesso

<key>PlatformSSO</key>
<dict>
  <key>FileVaultPolicy</key>
  <array><string>AttemptAuthentication</string></array>
  <key>UnlockPolicy</key>
  <array>
    <string>RequireAuthentication</string>
    <string>AllowOfflineGracePeriod</string>
    <string>AllowTouchIDOrWatchForUnlock</string>
  </array>
  <key>LoginPolicy</key>
  <array/>
  <key>AuthenticationGracePeriod</key>
  <integer>604800</integer>
  <key>OfflineGracePeriod</key>
  <integer>604800</integer>
</dict>
```

Don't Panic

But do really go to Michael and Mark's session on PSSOe with Microsoft.

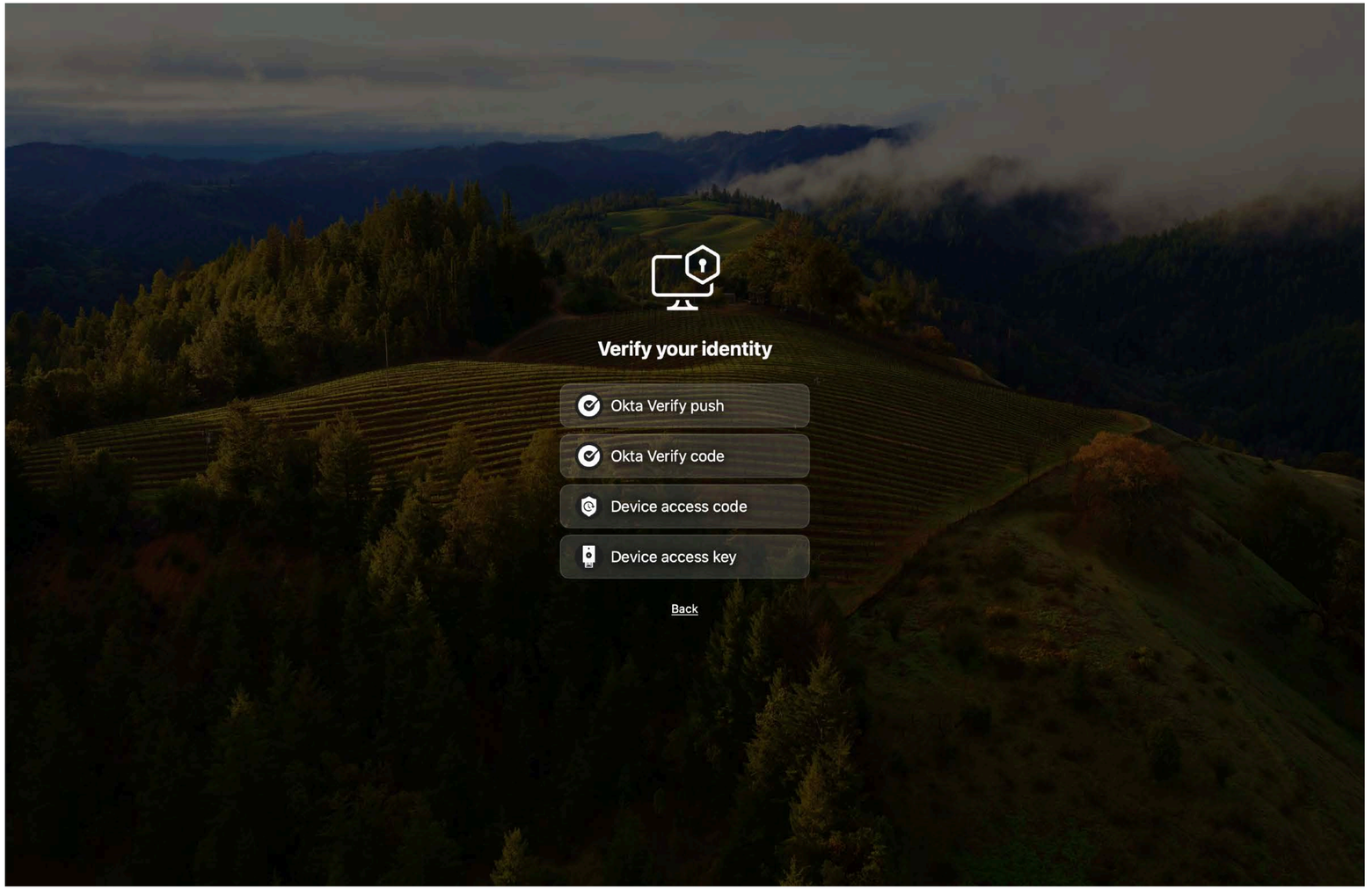
jamf


Enable your Entra ID passkey
To use your Entra ID passkey, you must enable Company Portal as a Passkey Provider.
To complete this action, open the System Settings app and navigate to: Passwords > Password Options > Use passwords and passkeys from... > Enable Company Portal
Learn more
Open System Settings
Dismiss

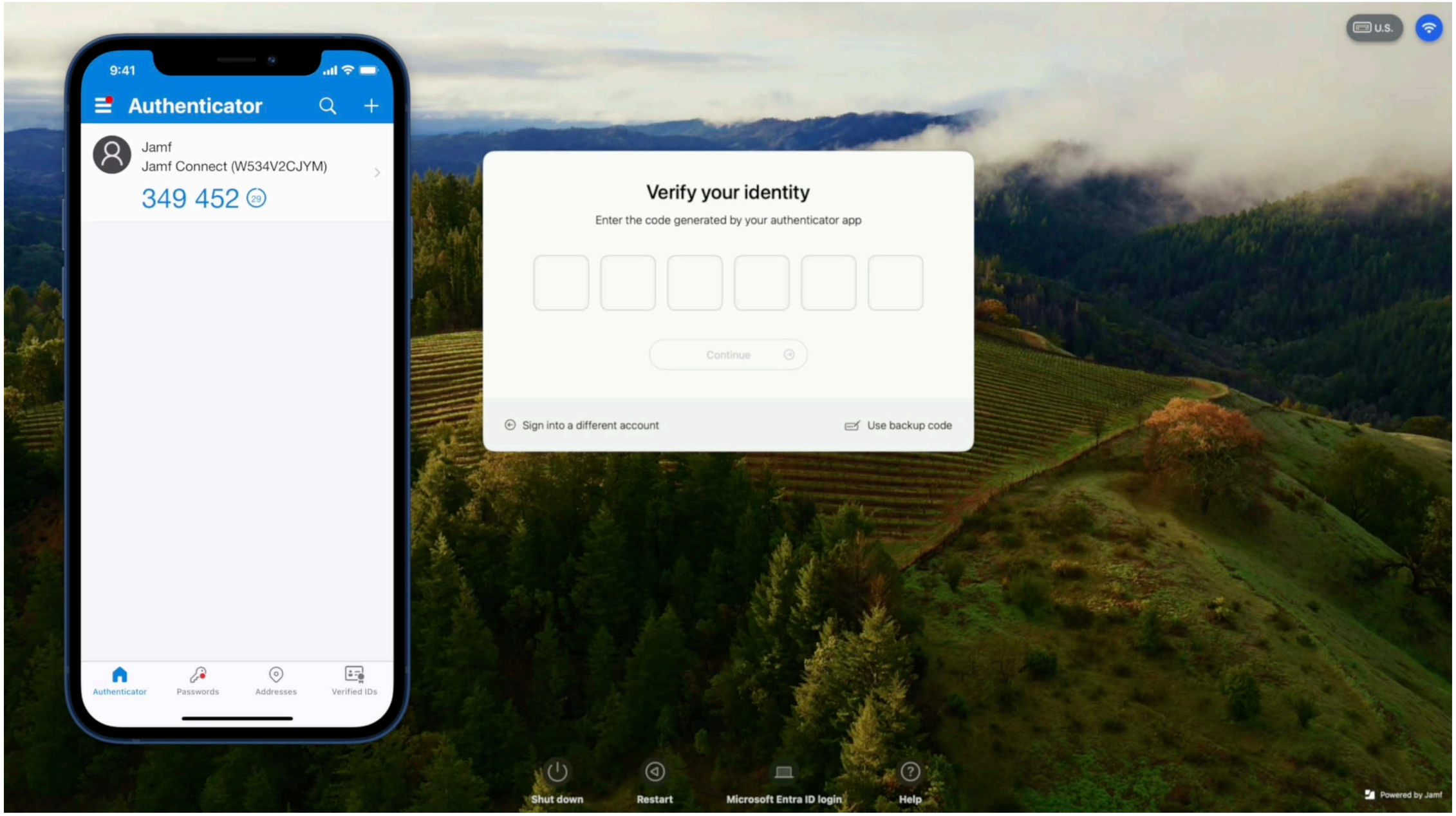


jamf

Okta Desktop MFA



jamf


9:41
Authenticator
Jamf
Jamf Connect (W534V2CJYM)
349 452
29
Authenticator
Passwords
Addresses
Verified IDs
U.S.
Verify your identity
Enter the code generated by your authenticator app
Continue
Sign into a different account
Use backup code
Shut down
Restart
Microsoft Entra ID login
Help
Powered by Jamf

jamf

One more thing....

jamf

ZTNA and killing network connections

jamf

ZTNA and killing network connections

Not valid before: 07-11-2024 09:00:00

Expires: 07-11-2024 10:45:00

jamf

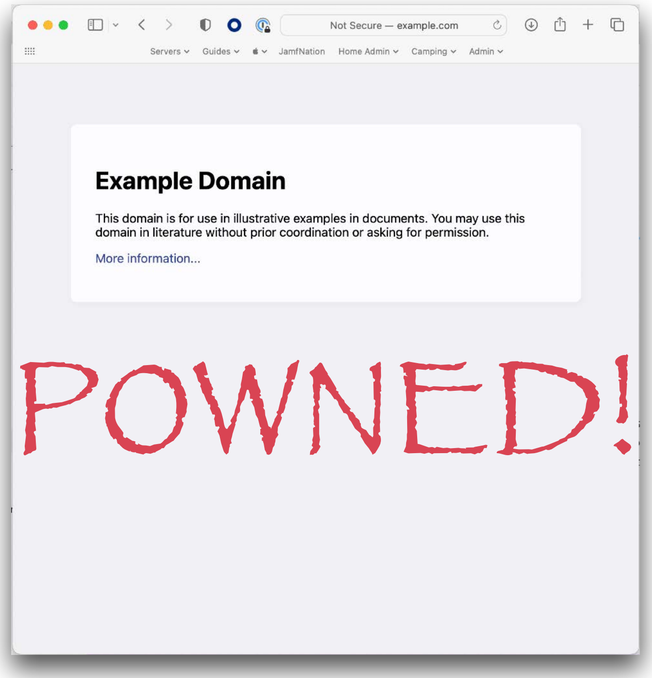
ZTNA and killing network connections

Not valid before: 07-11-2024 09:00:00

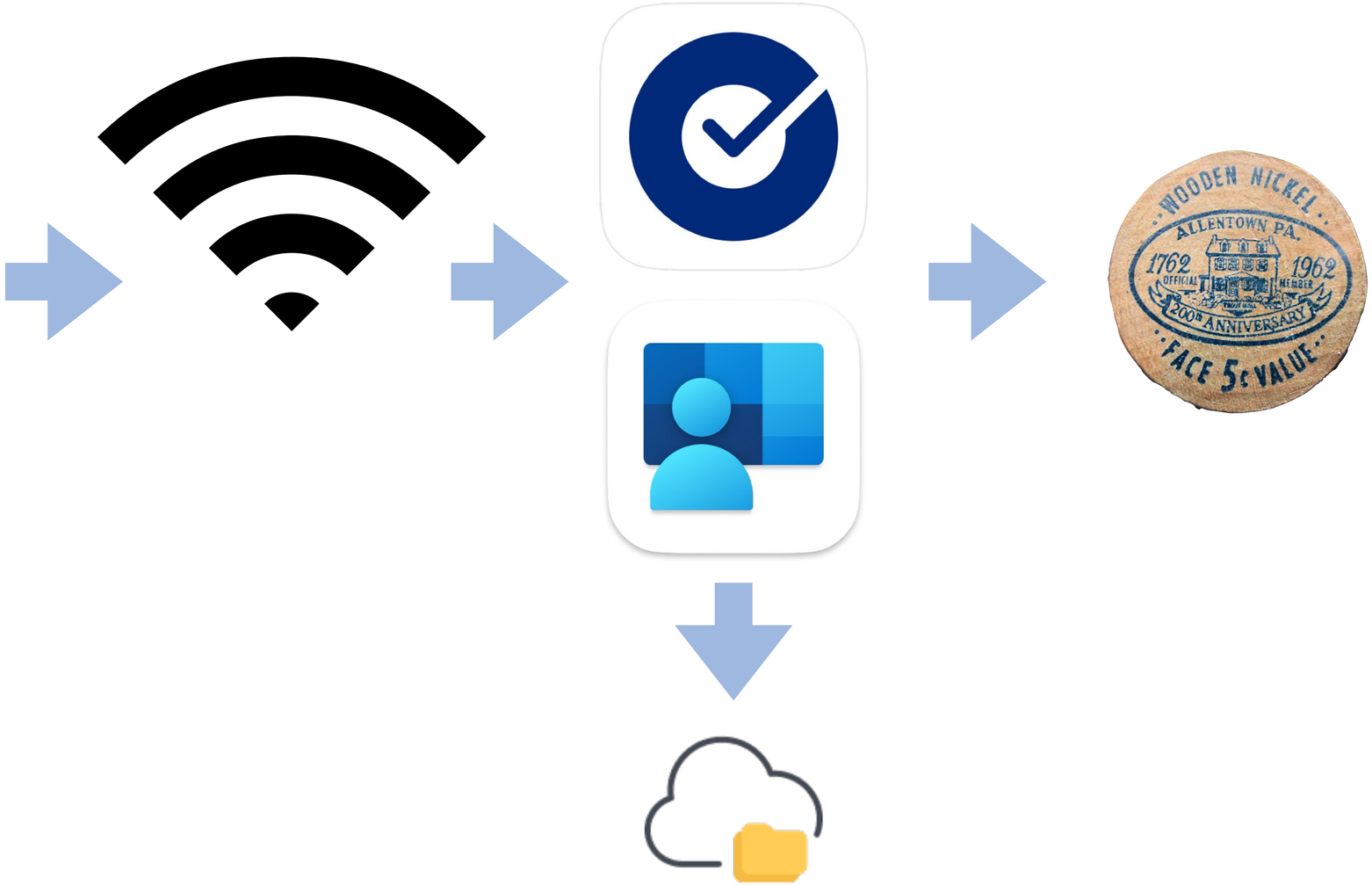
Expires: 07-11-2024 10:45:00

jamf

ZTNA and killing network connections



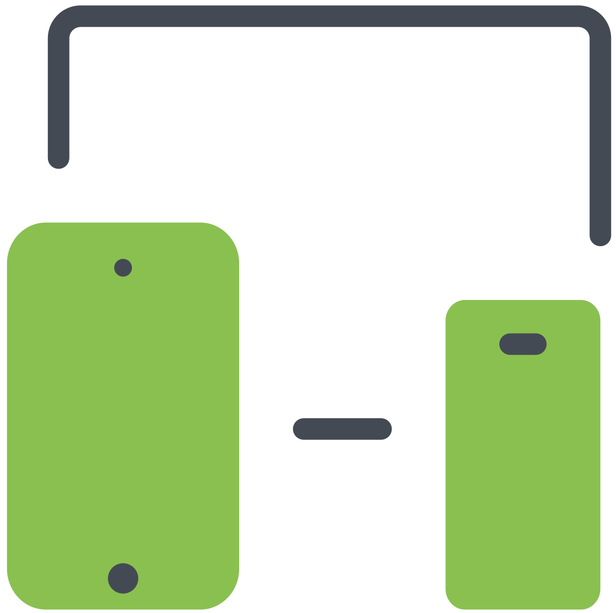
open https://example.com/login/p0wned

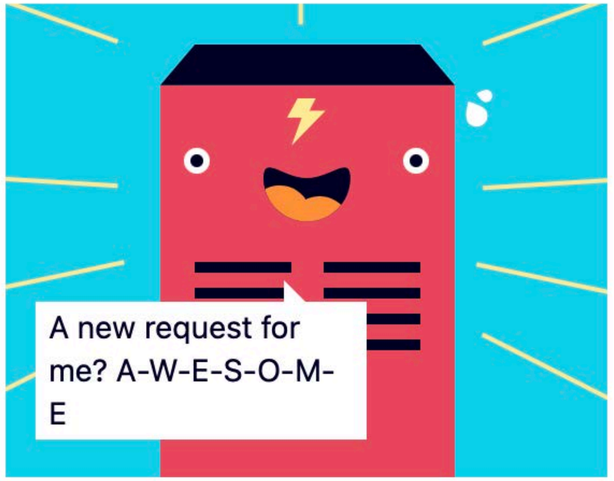


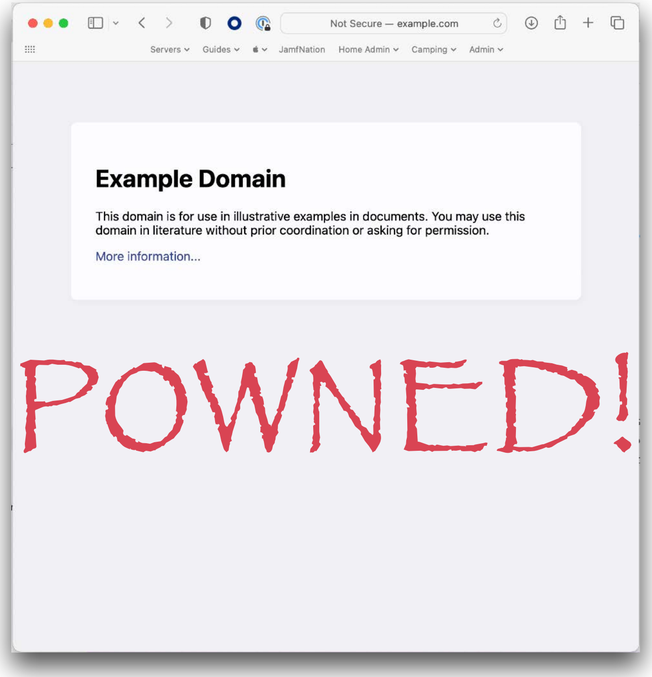
jamf

Public domain

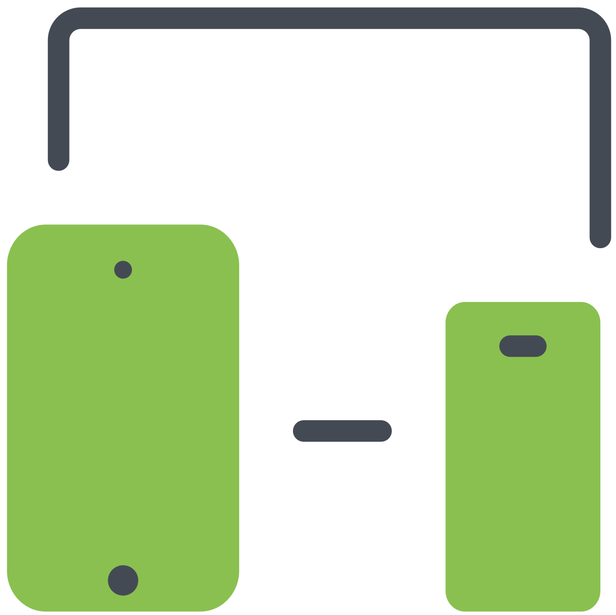
ZTNA and killing network connections





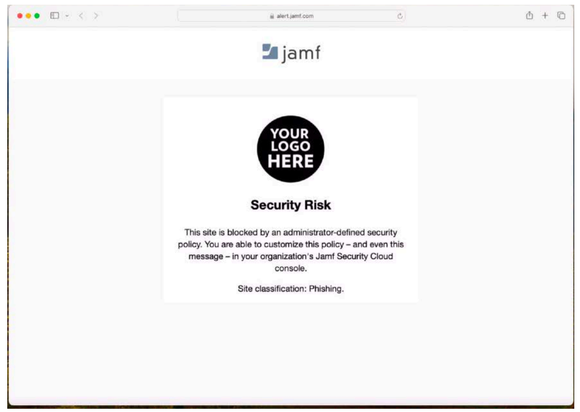


ZTNA and killing network connections



SSF Sender

"Device risk level set to HIGH"



CAEP signal receiver

Final Thoughts

And then there will be cake.

jamf

Final Thoughts

- SSOe is a possession factor, a *single* factor
- PSSOe is a possession factor too
- If you're accessing a resource, and the device itself is the factor, protect the device.

I'd like you to give the gift... of feedback. To Apple.

jamf

I'd  **the**
gift... c Apple.

jamf

feedbackassistant.apple.com

Use your Apple Business Manager or Apple School Manager managed Apple Account.
Switch to "Organization" mode.

jamf

feedbackassistant.apple.com

Use your Apple Business Manager or Apple School Manager managed Apple Account.
Switch to "Organization" mode.

"Basic authentication is no longer acceptable to decrypt our stored data at rest."

jamf

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

I'll be at Jamf's booth after this.

jamf

Thank you.

Special thanks to Doug Muth (Giza) for the Dead Simple QR Code Generator
https://httpbin.dmuth.org/qrcode/

jamf