



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"?

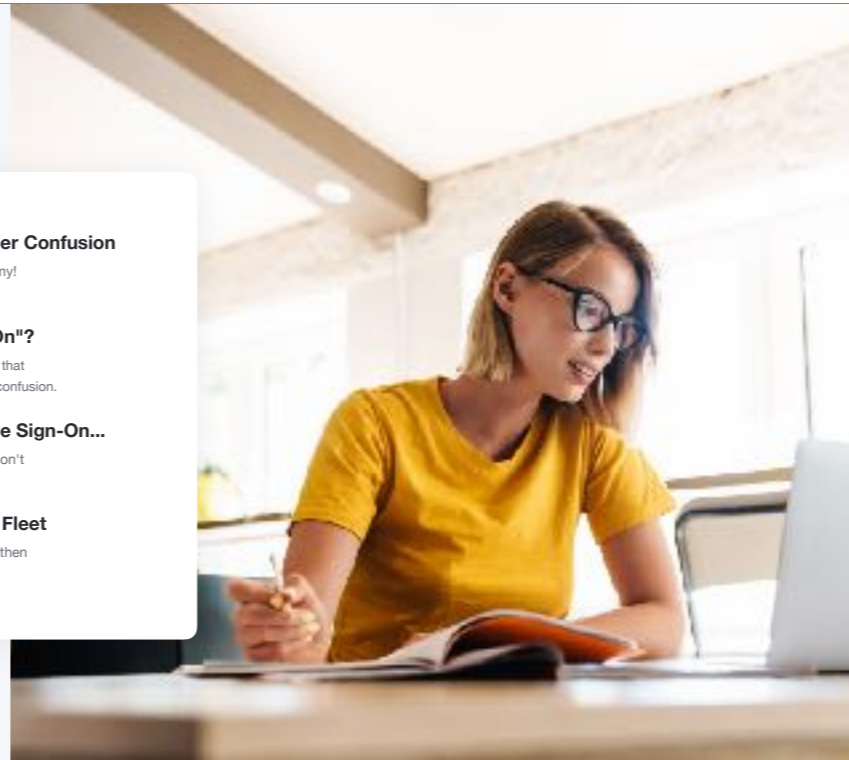
There's only two identity providers in the world that support this thing, so I could understand your confusion.


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

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

4 | Three Steps to Hardening Your Fleet

Physical, Cloud, and Network security. And then there will be cake.





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

Carl Sagan
COSMOS, C. 1980

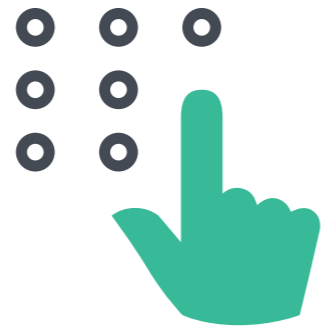


Authentication Factors or why don't you trust me

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



Factor Types



Knowledge



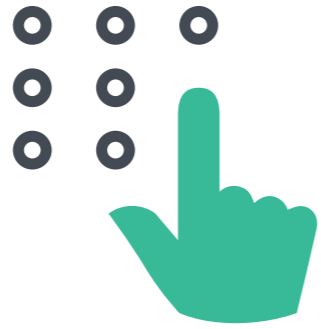
Possession



Biometric



Something you know
Something you have
Something you are



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



Something you know
Something you have
Something you are

History

macOS is UNIX



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

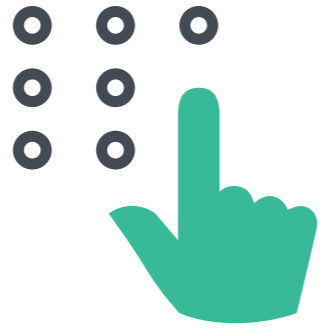
Pdp-7 (build) macOS is Unix

“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](https://support.apple.com/guide/security/face-id-and-touch-id-security-sec067eb0c9e/1/web/1)





Something you know

- PIN
- Password
- Mother's Maiden Name



Something you have

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



Something you are

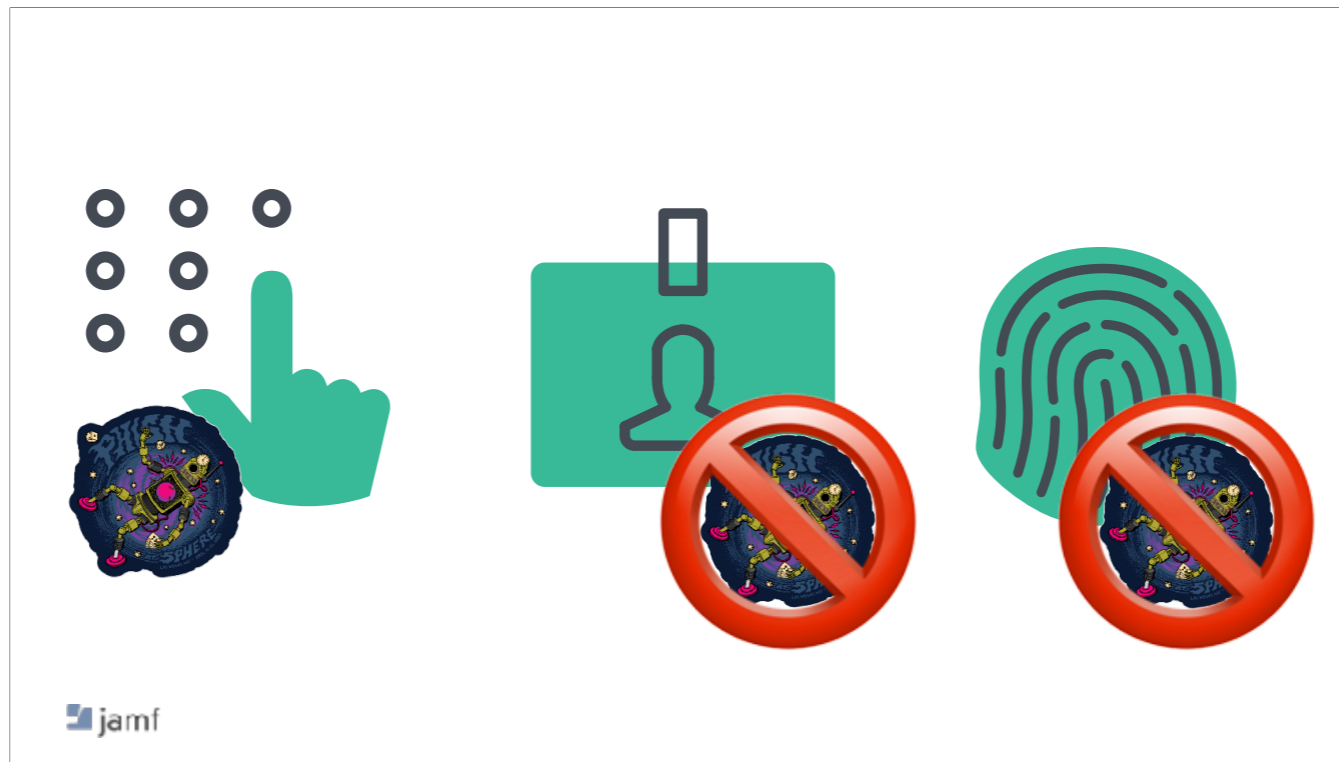
- TouchID / FaceID
- Fingerprint scanner
- Retinal scanner



Something you know
Something you have
Something you are




Khan C. Smith - phreak



Something you know - phishable
Something you have - stealable
Something you are - kinda hard to remove



Additive nature of phish



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

Sean Rabbitt
SR. CONSULTING ENGINEER, CIRCA 2022



anytime someone says "passwordless" they just mean a possession or a biometric factor
possession factor is just a certificate exchange
biometric is just a hash derived from the randomness of yourself

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

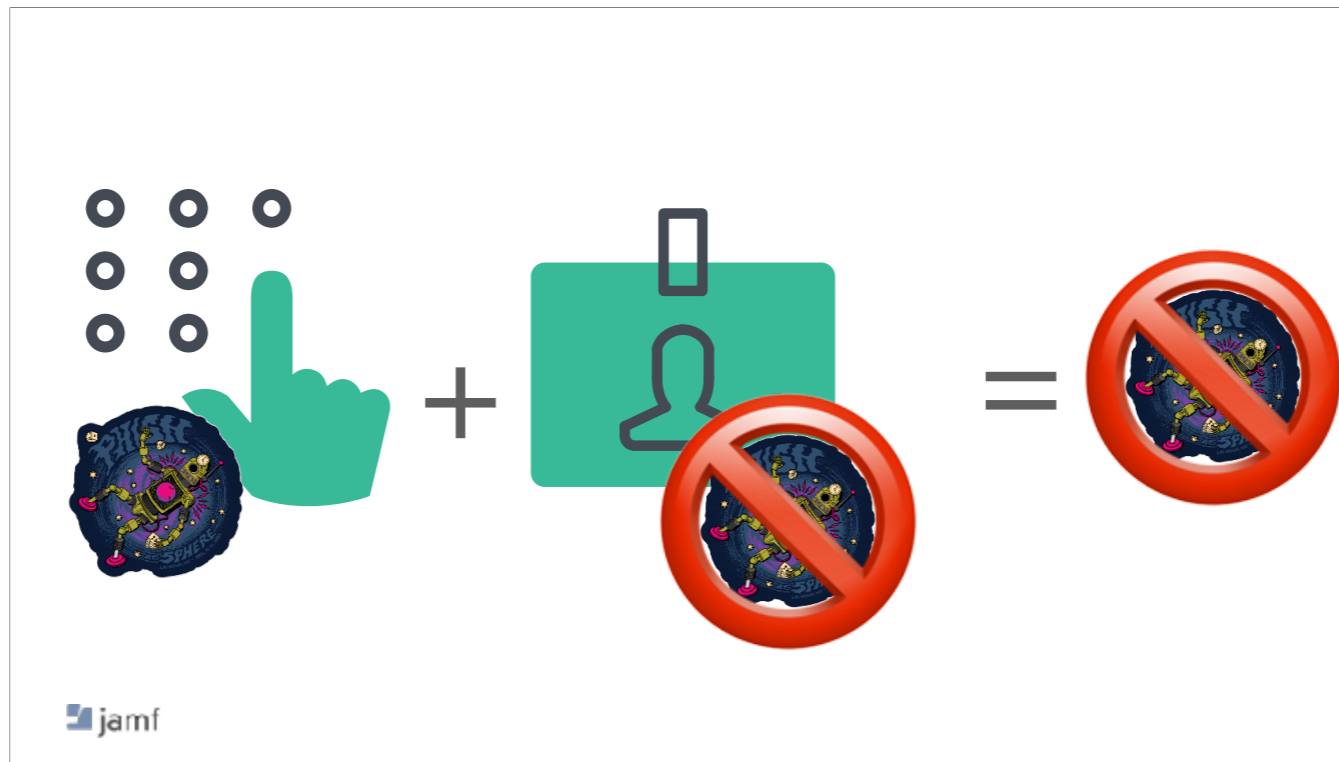
touchid and faceid are the biometric combined with unique hardware identifiers of the currently logged in user. also used by a pam. also an unlock from screen saver is not an authentication. blame apple - and why is it not available at login? [next slide]

“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.**”

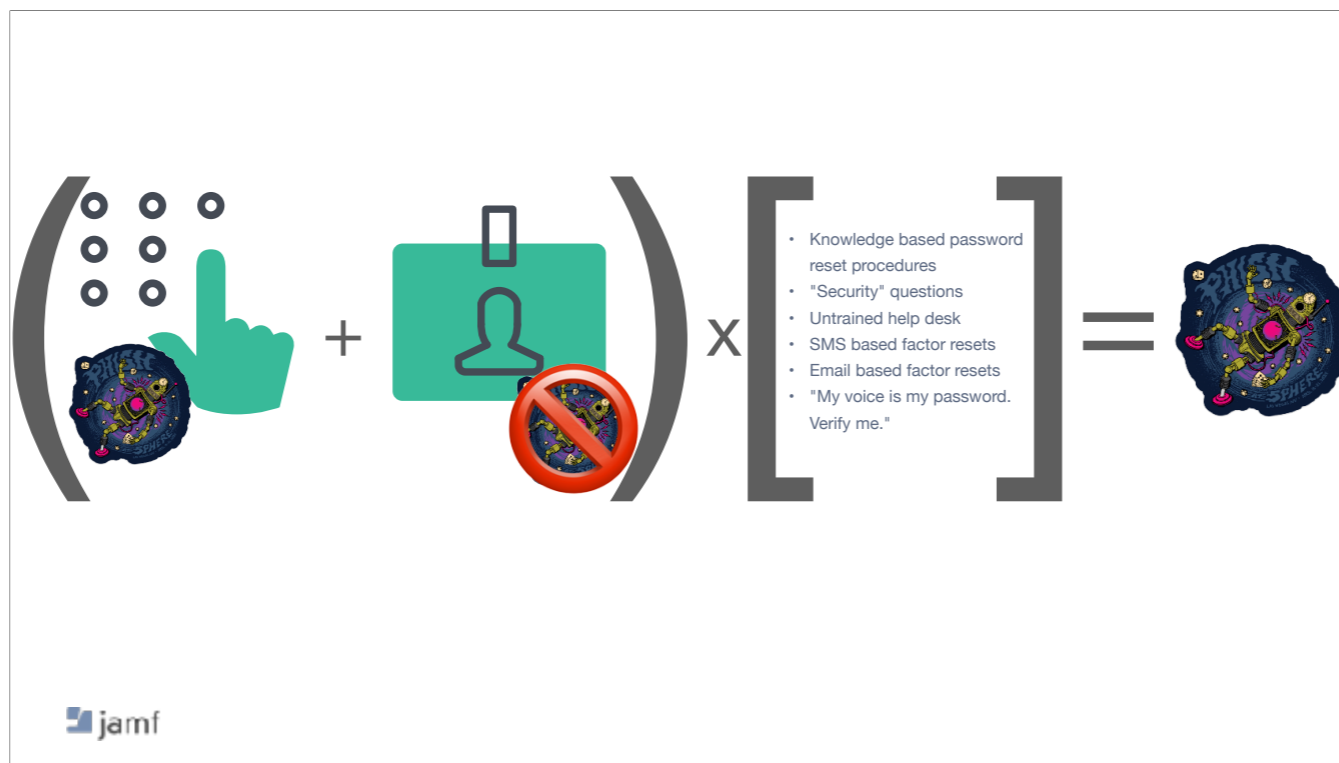
[Apple Platform Security guide](#)

[HTTPS://SUPPORT.APPLE.COM/GUIDE/SECURITY/USES-FOR-FACE-ID-AND-TOUCH-ID-SECC5227FF3C/1/WEB/1](https://support.apple.com/guide/security/uses-for-face-id-and-touch-id-secc5227ff3c/1/web/1)





The horrible truth of password security and password reset procedure



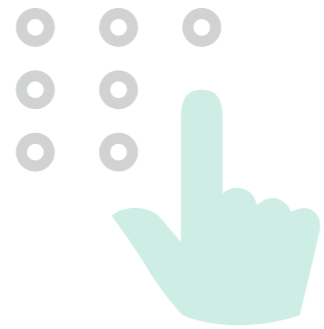
The horrible truth of password security and password reset procedure

What the heck is Single Sign On

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



Apple Extensible Single Sign On



Knowledge



Possession

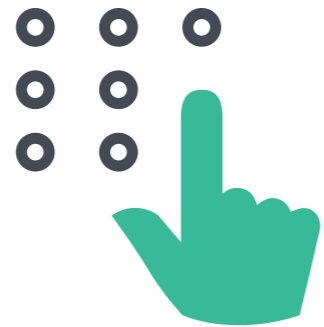


Biometric



Single Sign On is possession based factor

Apple Extensible Single Sign On



Knowledge



Possession

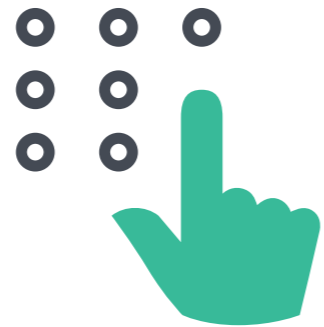


Biometric



Access to the possession based factor is tied to a knowledge factor - unlocking macOS session, FileVault, or turning on iOS/iPadOS/VisionOS device

Apple Extensible Single Sign On



Knowledge



Possession



Biometric



Spoilers - while there's biometrics on these devices, it is NOT a requirement of the SSOe specification to use biometrics

Use words more gooder

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

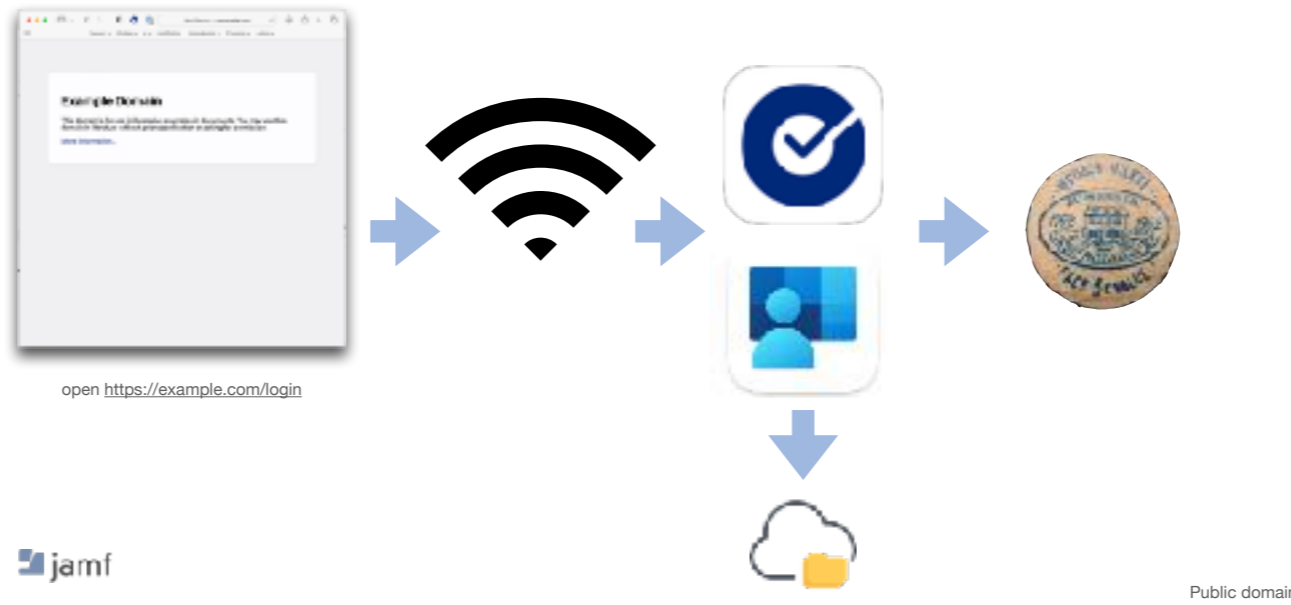
Use words more gooder

- 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



- Companion application with entitlements granted by Apple
 - network layer intercepts authentication requests
 - SAML
 - OAuth
 - Open ID Connect 2.0 (OIDC)
 - Specialized authentication requests depending on identity provider (MSAL)
 - Redirects authentication requests to the companion application
 - Companion app requests a Primary Refresh Token (PRT) which is then used to obtain other tokens for other applications. PRT stored in user's keychain
- Discuss when this was introduced (macOS Catalina 10.15 - 4 years ago)



Microsoft Entra ID



Okta Identity Engine

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

Microsoft Enterprise Single Sign-On Plugin

Settings | About Show or Hide My Data

11 | **Single Sign-On Extensions**

12 | **Single Sign-On Extensions**

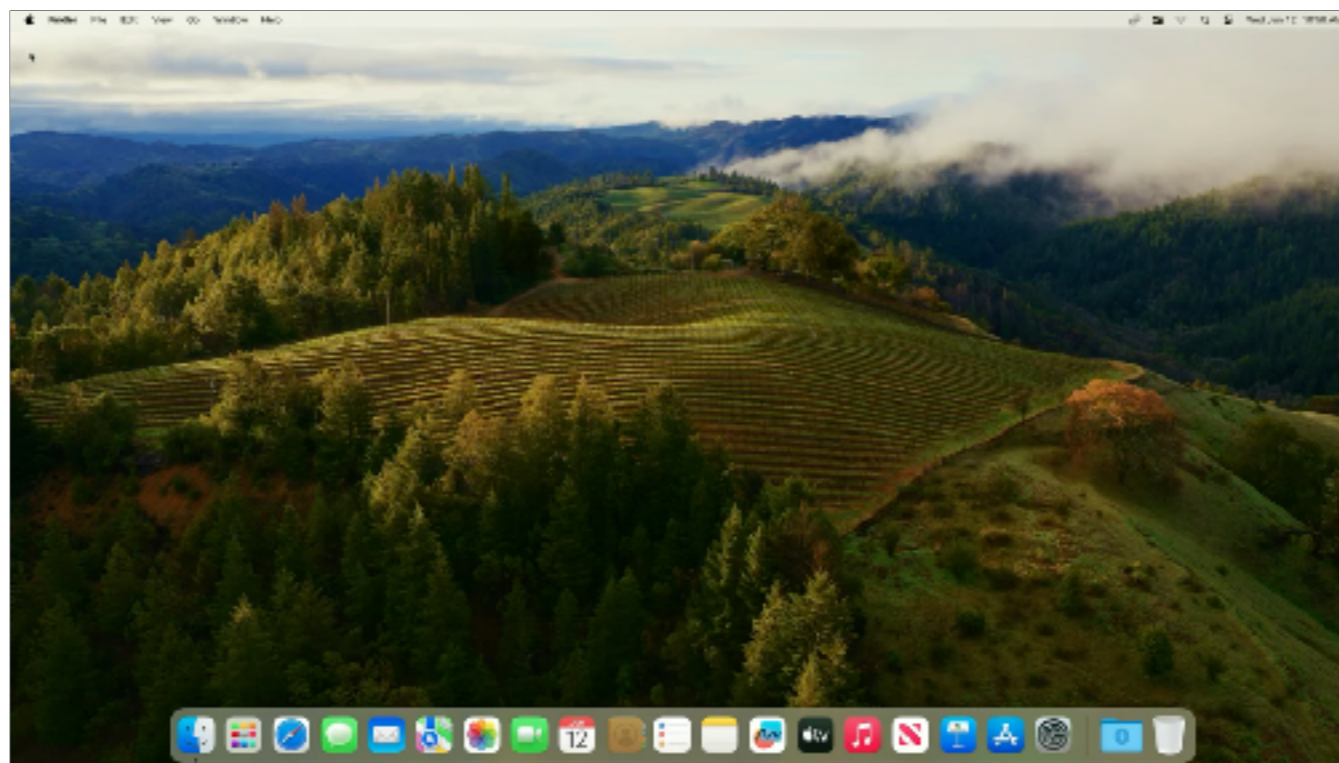
Single Sign-On Extension	Created Time
Extension Identifier	1/1/2016 12:00:00 AM
Team Identifier	1/1/2016 12:00:00 AM
System Type	Native

APIs

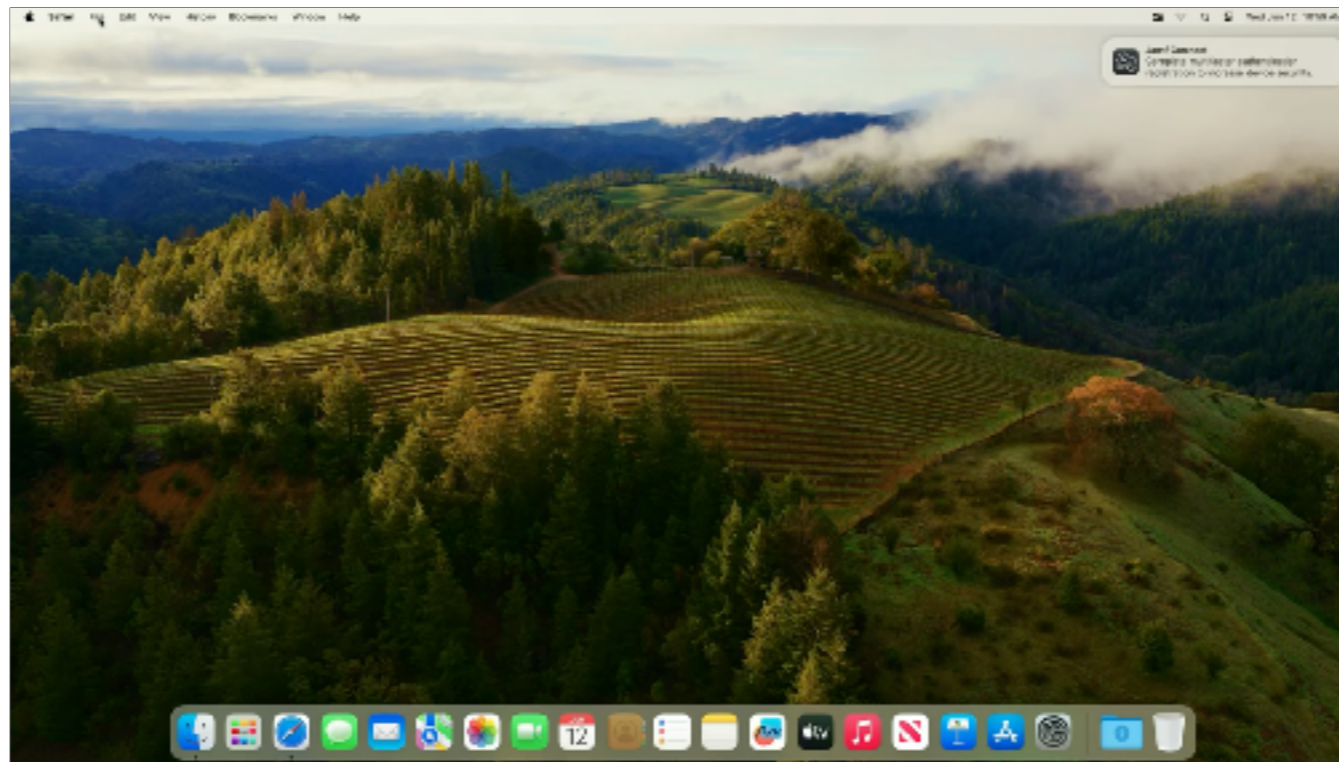
APIs are used to extend the capabilities of the Single Sign-On plugin. The APIs are implemented by the plugin and are unique for all installed Single Sign-On Extension plugins. Some attributes are fully managed by the system.

API Name	API Identifier
API Name	API Identifier
API Name	API Identifier
API Name	API Identifier
API Name	API Identifier

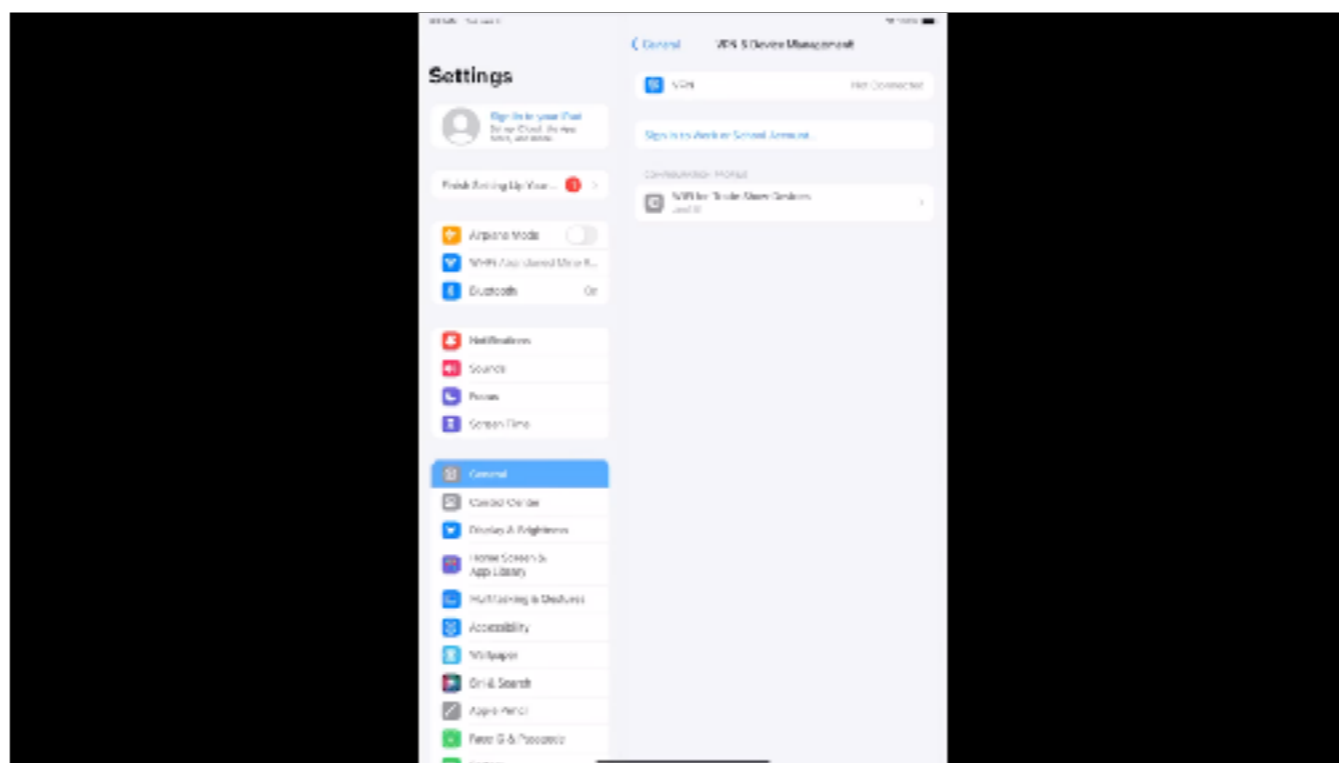




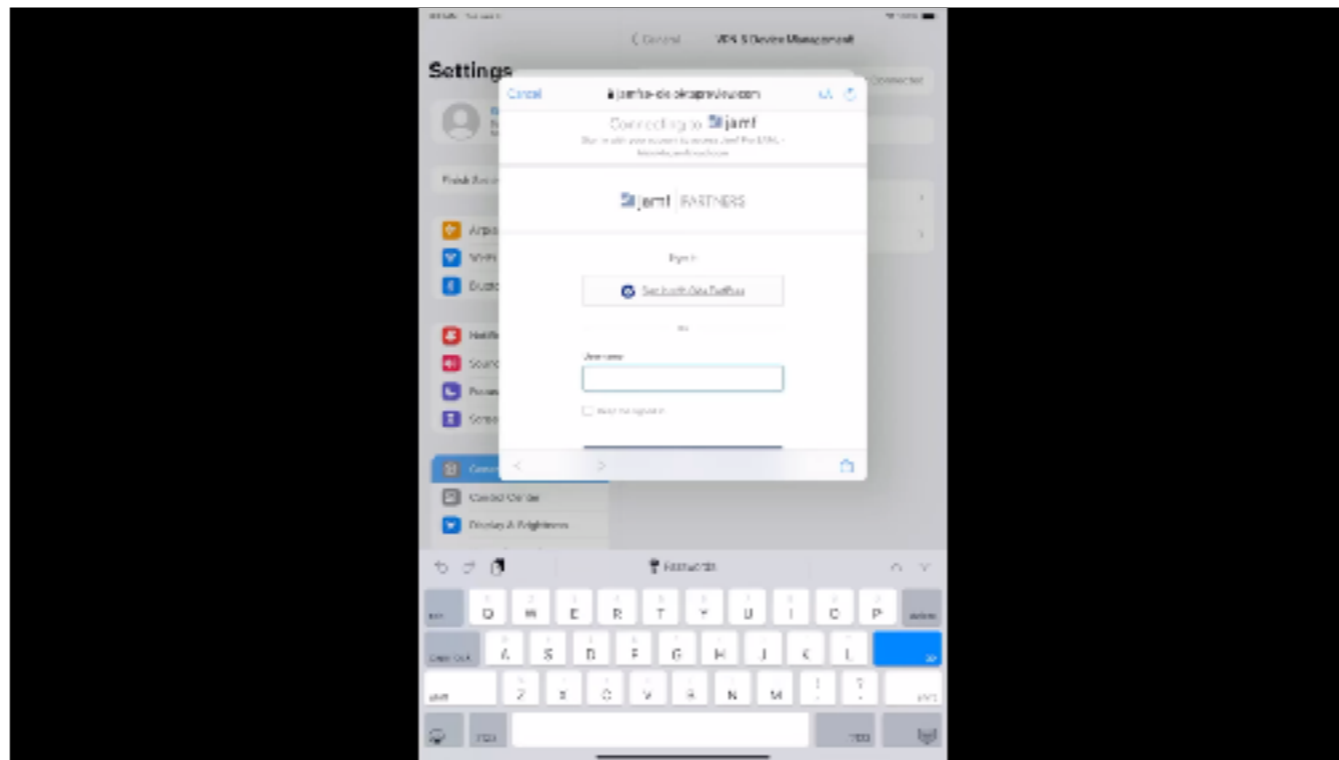
0:45 video - first time login to "prime" SSOe



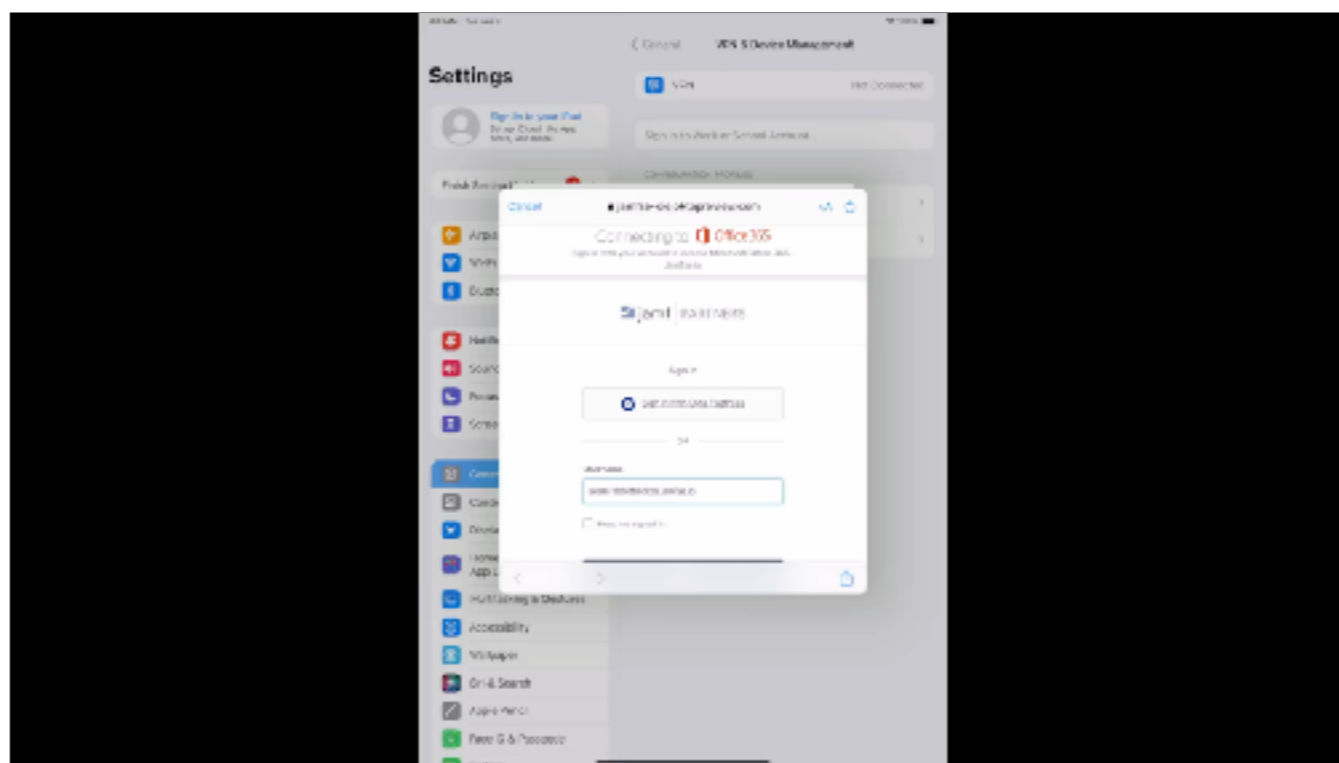
01:07 video Subsequent logins -



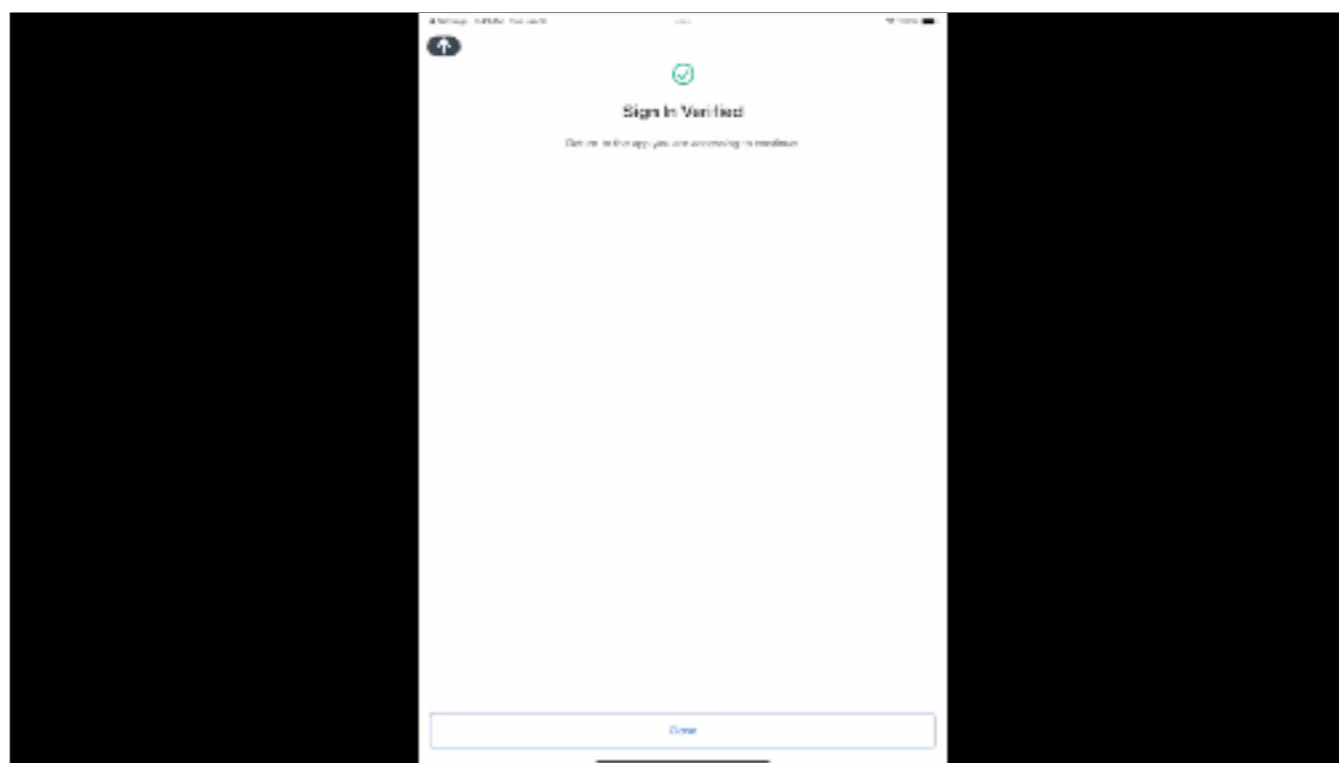
0:45 - log in, download okta verify magically, we're prompted to log in



0:25 -

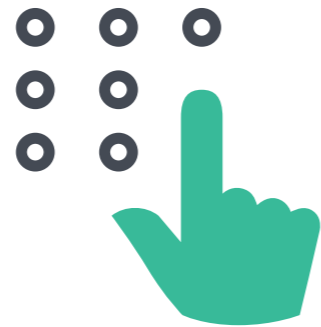


1:08 - So what we did is log in. What we were supposed to do was hit the Sign in with Okta Fast Pass
Fast Pass registration - ends at end of fast pass



1:16 - Fast pass, see settings in profiles, see that we are registered with Okta Verify, log into a webpage with okta gate, ssoe works

Apple Extensible Single Sign On



Knowledge



Possession



Biometric



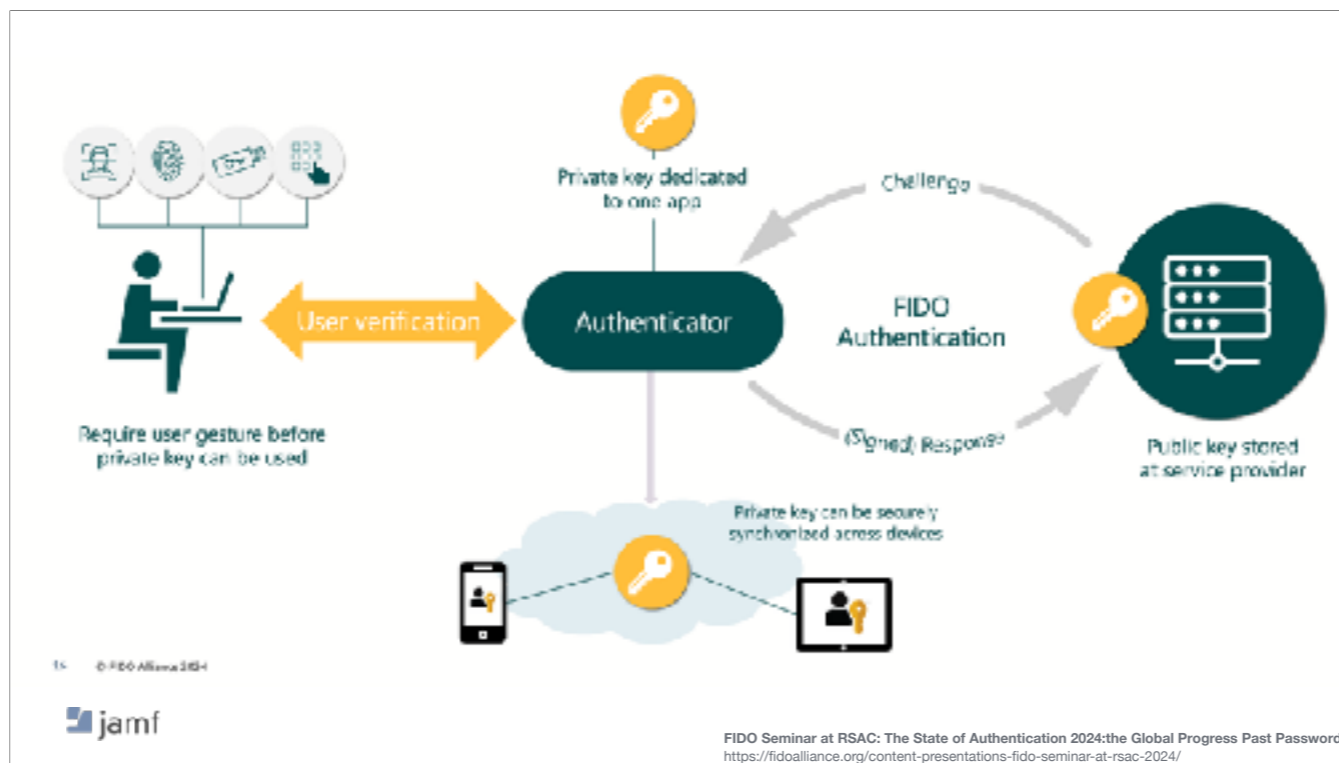
Spoilers - while there's biometrics on these devices, it is NOT a requirement of the SSOe specification to use biometrics (Oh, and even if it did - what's the bypass for biometrics if say you're wearing a mask?)



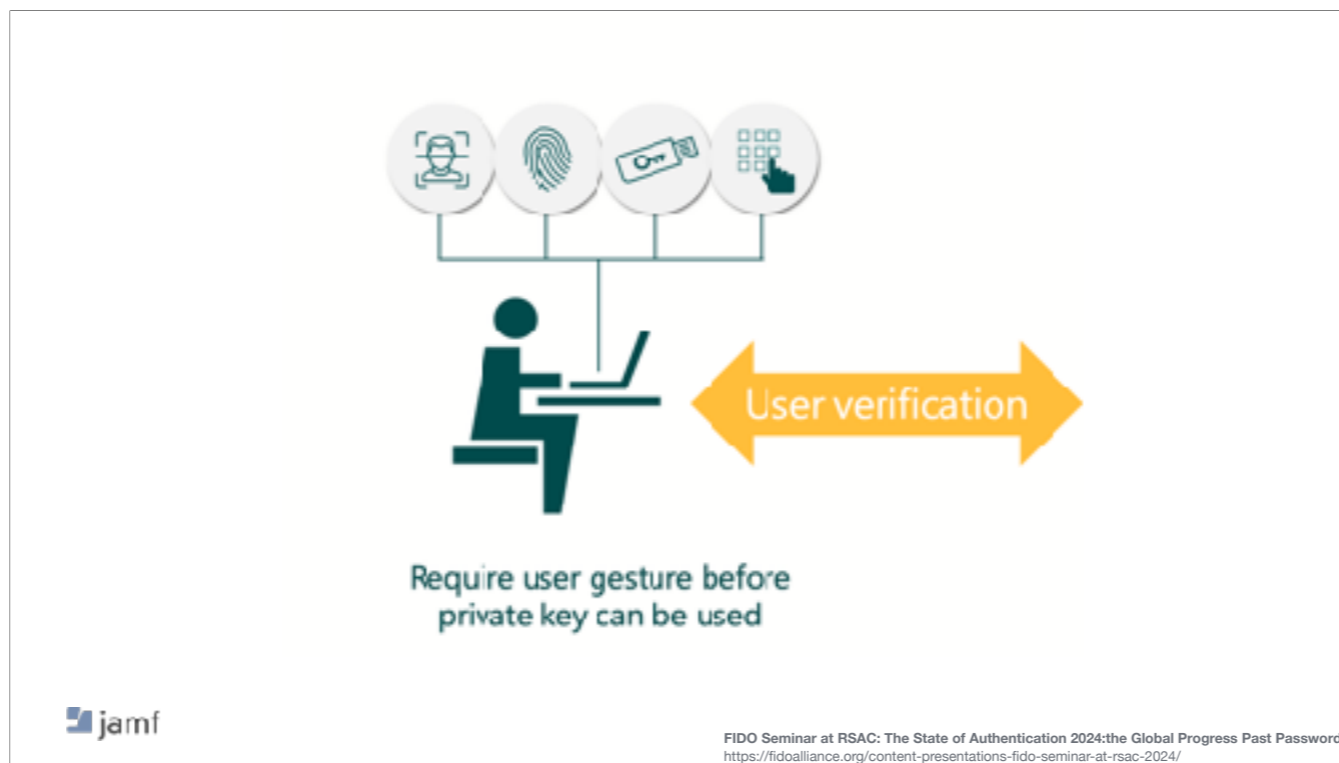
=



With one major exception.....

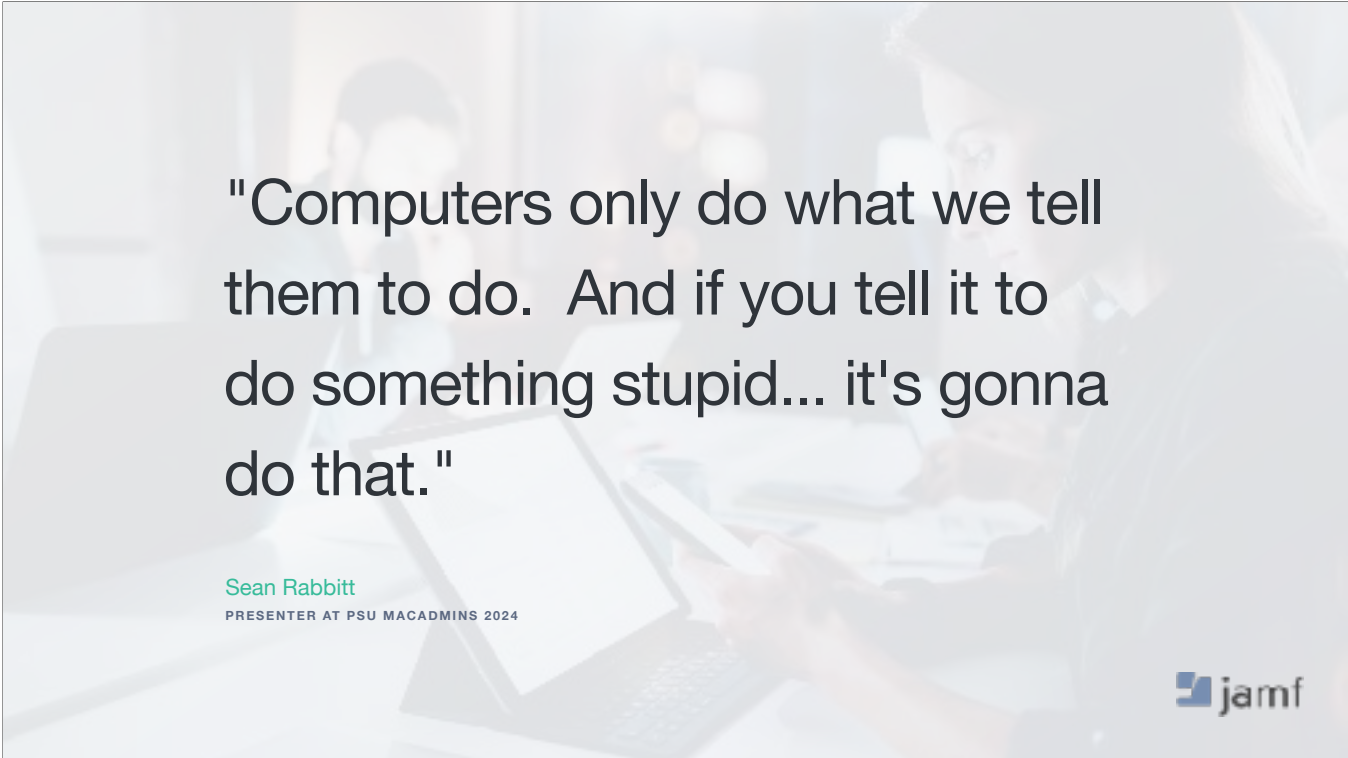


FIDO2 and passkeys - a possession factor with a required user interaction



FIDO2 standard says you need interaction. But remember, the MS didn't require it.





"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

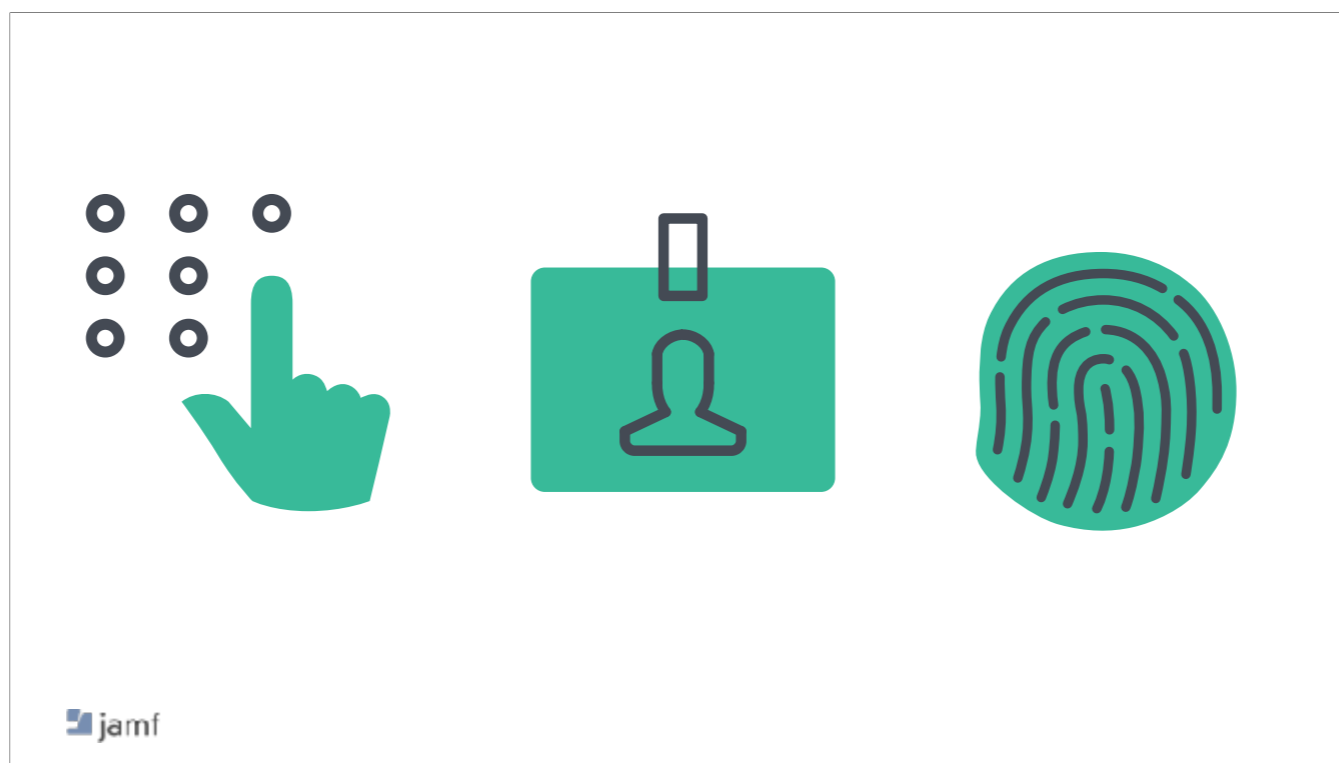




Single Sign On does not have a mandatory requirement for **User Verification**



Who is this guy in the photo? How did he get my iPhone?



So obviously if we want to bring any sort of security into this, we'll need to introduce another factor to using SSOE

Platform Single Sign-On



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



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

Password - wstrust join like windows

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



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

"Advanced Data Protection" - why is phishing and shoulder surfing such a big issue

Extensible Single Sign-On

Microsoft Enterprise Single Sign-On Plugin

Settings Show Show or Hide My, Don't Show

Home Settings

Single Sign-On Extensions

Single Sign-on Extensions

EXTENSION IDENTIFIER

Single Sign-on Extension
EXTENSION IDENTIFIER TO IDENTIFY THE EXTENSION TO THE SYSTEM AND TO THE USER.

Name
EXTENSION NAME

Extension Identifier
EXTENSION IDENTIFIER OF THE EXTENSION TO IDENTIFY THE EXTENSION.

Team Identifier
TEAM IDENTIFIER OF THE EXTENSION TO IDENTIFY THE EXTENSION.

Extension Type
EXTENSION TYPE

Name
Name of the extension to identify the extension. The Name must be unique for all installed Single Sign-On Extensions. Some extensions may have a Name that is not allowed.

- com.jamf.plugins.single-sign-on
- com.jamf.plugins.single-sign-on
- com.jamf.plugins.single-sign-on
- com.jamf.plugins.single-sign-on
- com.jamf.plugins.single-sign-on



Remember how we talked about redirect and payloads and config - redirect vs credential



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.**



(build)

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



this is an error in the documentation. `RequireAuthentication` does not work at the FileVault screen. Discuss these new features and network availability.

```
// 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.



Hardening with authentication
rules and additional factors





 jamf

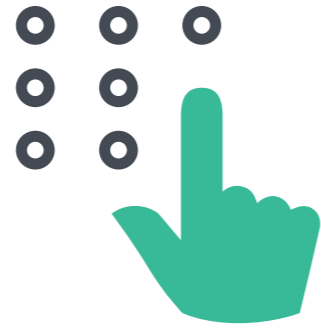
- Block It
- Chock It
- Lock It



We're going to do the same to protect our assets. Physical security, cloud security, and network security. Trusted Access

Physical Device Security





Something you know

- PIN
- Password
- Mother's Maiden Name



Something you have

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

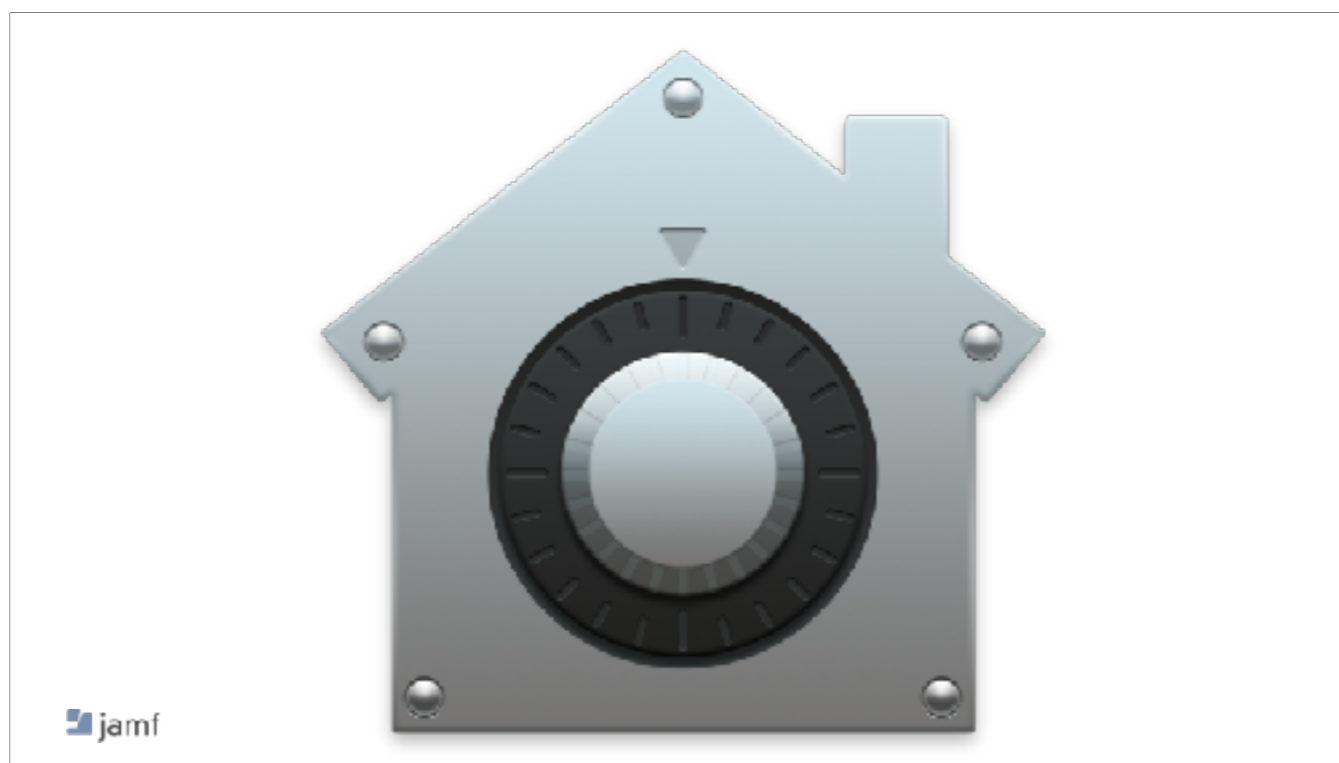


Something you are

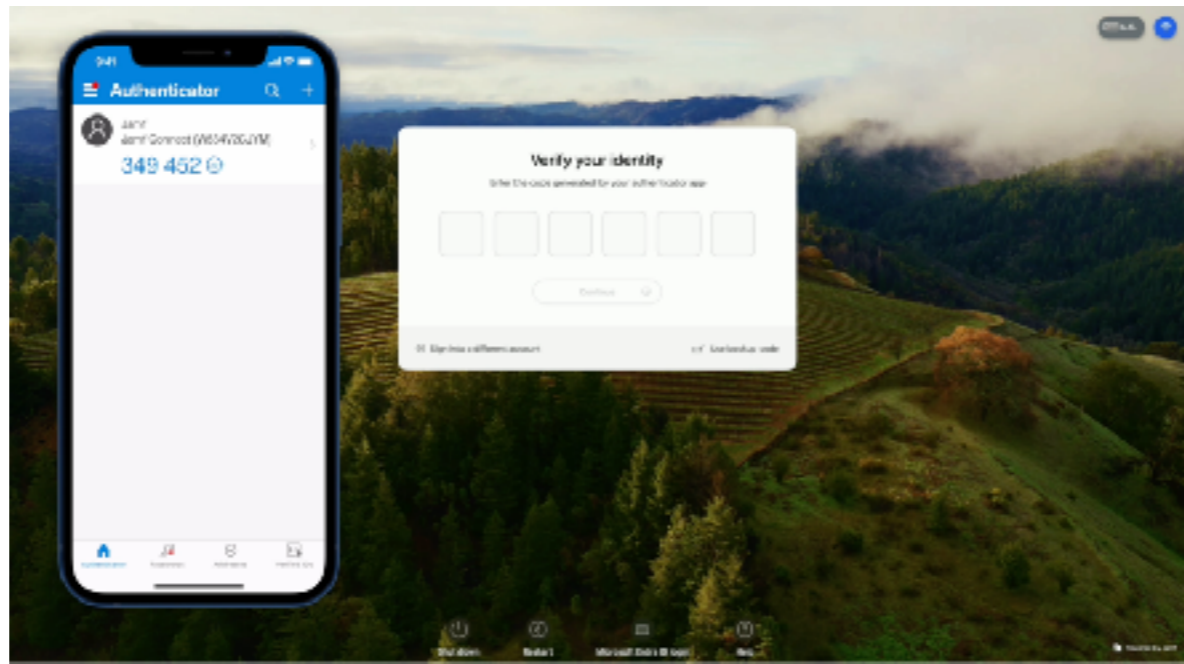
- TouchID / FaceID
- Fingerprint scanner
- Retinal scanner



Remember, password is still phishable or shoulder surfable. see also people stealing iPhones at bars.
"Advanced Data Protection" - talk about this later too - why is phishing and shoulder surfing such a big issue

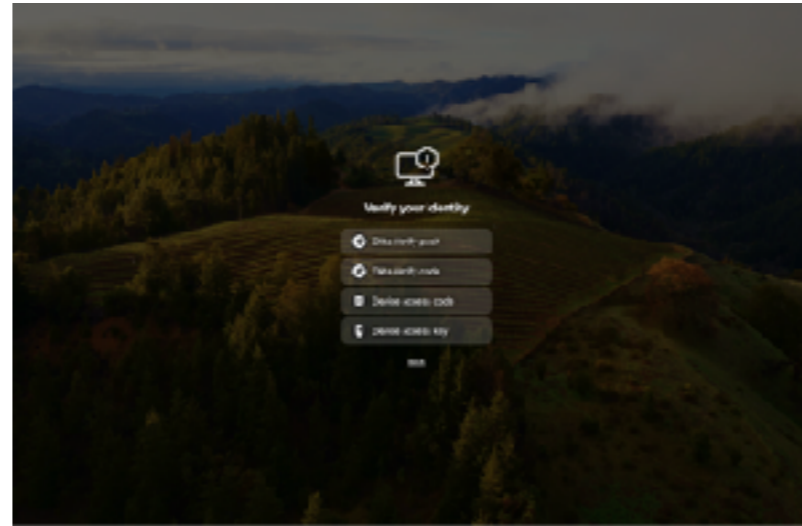


first obvious thing - enable filevault. turn on password minimums. enforce with config profiles. make passcodes not optional on byo



jamf

Okta Desktop MFA



Lock your users out of their computers in even more new and interesting ways with FIDO2 key at "login" screen.



Enable your Entra ID passkey

To use your Entra ID passkey, you must enable Company Portal as a Passkey Provider.

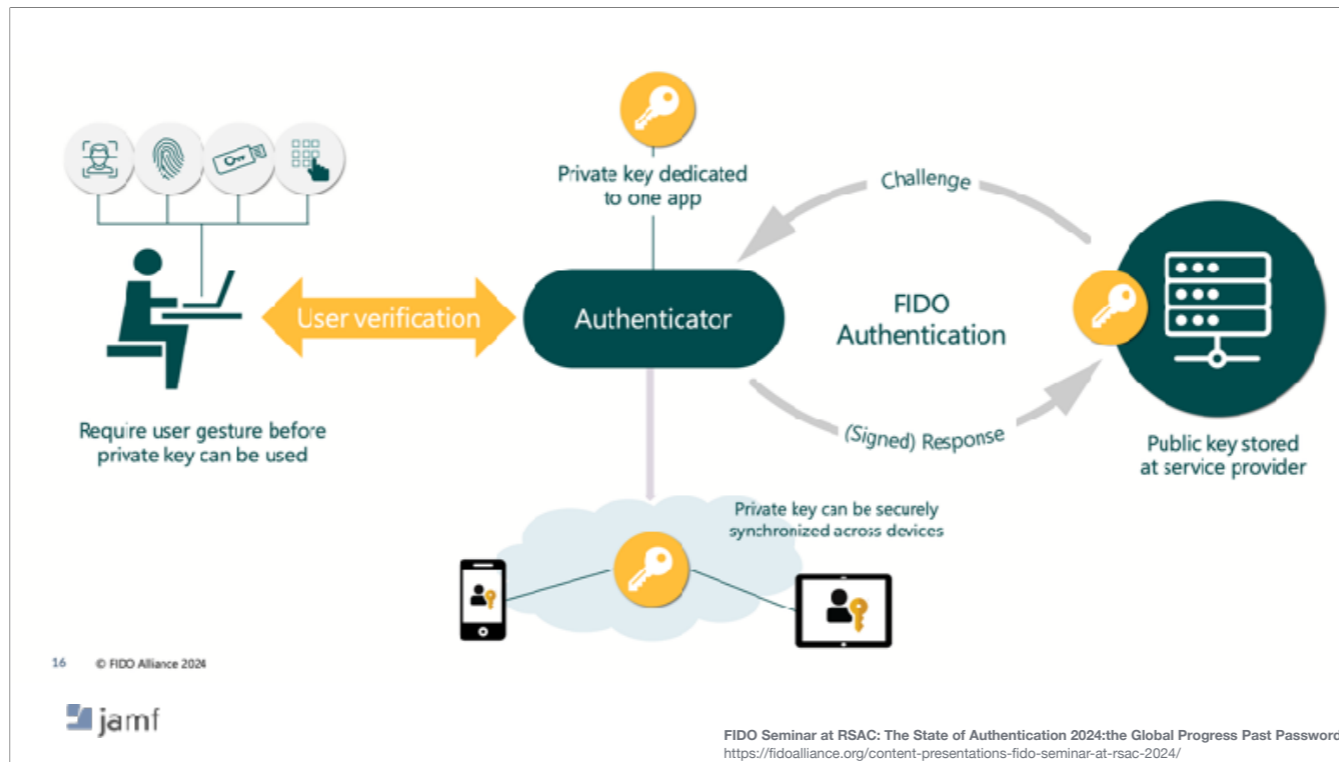
To complete this action, open the System Settings app and navigate to: Passwords > Password Options > Use passwords and passkeys from... > Enable Company Portal

[Learn more](#)

[Open System Settings](#)

Dismiss





FIDO2 and passkeys - a possession factor with a required user interaction

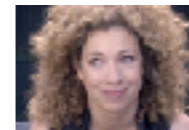
Cloud Security



Microsoft Entra ID -> Security



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



 jamf

<https://learn.microsoft.com/en-us/entra/identity/authentication/concept-authentication-passwordless#platform-credential-for-macos>

Microsoft Entra Conditional Access



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



<https://learn.microsoft.com/en-us/entra/identity/authentication/concept-authentication-passwordless#platform-credential-for-macos>

Microsoft Azure Search resources, services, and docs (G+)

Home > Conditional Access | Policies >

Require phishing-resistant multifactor authentication for admins

Conditional Access policy

Delete View policy information

Target resources

All cloud apps

Network: **K1M**
Not configured

Conditions

0 conditions selected

Access controls

Grant: **1 control selected**

Block: **0 controls selected**

Enable policy

Recommended 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

i To enable all authentication strength, configure conditional access settings to accept claims coming from Microsoft, then enable 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



<https://learn.microsoft.com/en-us/entra/identity/authentication/concept-authentication-passwordless#platform-credential-for-macos>

Okta Identity Engine



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



But Sean, you just said to require MFA....

Okta Identity Engine



Establish the user session with

Multifactor authentication (MFA) is

Any factor used to meet the Authentication Policy requirements

A password

An MFA claim will satisfy either of these options. The [Authentication Policy](#) determines the authentication requirement for a request.

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](#)



But Sean, you just said to require MFA....



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



because authentication policy takes over

Okta Identity Engine



T-10H

THIS: Assess to

AND: User must authenticate with

AND: Authentication methods

- Denied
- Allowed after successful authentication

Any 1 factor type

- Allow any method that can be used to meet its requirements
- Disallow specific authentication methods
- Allow specific authentication methods

Password X

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 FIDO (WebAuthn)



1 factor that doesn't allow password...



Okta Identity Engine

OKTA

RECI Access to

RECI Use most authenticators with

RECI Possessor factor constraints

RECI Authentication methods

Denied

Allow after successful authentication

Any 2 factor types

Phishing resistant

Hardware protection

Require user interaction

Require PIN or biometric user verification

Learn more about [possessor factor constraints](#)

Allow any method that can be used to meet the requirement

Show specific authentication methods

Show specific authentication methods

Your org's authenticators that satisfy this requirement

Knowledge (Biometric) factor types

Okta Verify - FaceView™ or Okta Verify - Face™ or Password or MFA (WebAuthn)


AND

Additional factor types

Okta Verify - Password™ or Okta Verify - Pass™ or MFA (WebAuthn)


*Authenticators 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, visit [Okta Admin Console](#) in [Security > General](#)



any two factors (including password) - but you can't reuse factors

Okta Identity Engine



THEN

Denied

Allowed after success/authentication

password + another factor

MFA required

Hardware presence

Require user interaction

Require PIN or biometric user verification

Learn more about [possession factor constraints](#)

Allow any method that can be used to meet the requirement

Exclude specific authentication methods

Allow specific authentication methods

View each authentication method category


password

MFA

Additional factor types

Okta Verify - Push (SMS) | Okta Verify - Push (Voice) | FIDO (Security Key)

For sig users, users to verify their identity with a knowledge factor (password) before the possession factor. To change this, visit: [admin:password-based access in Security > General](#)



or password plus another non-phishable factor that "Require user interaction" and "require pin or biometric"

Network Security



ZTNA and killing network connections



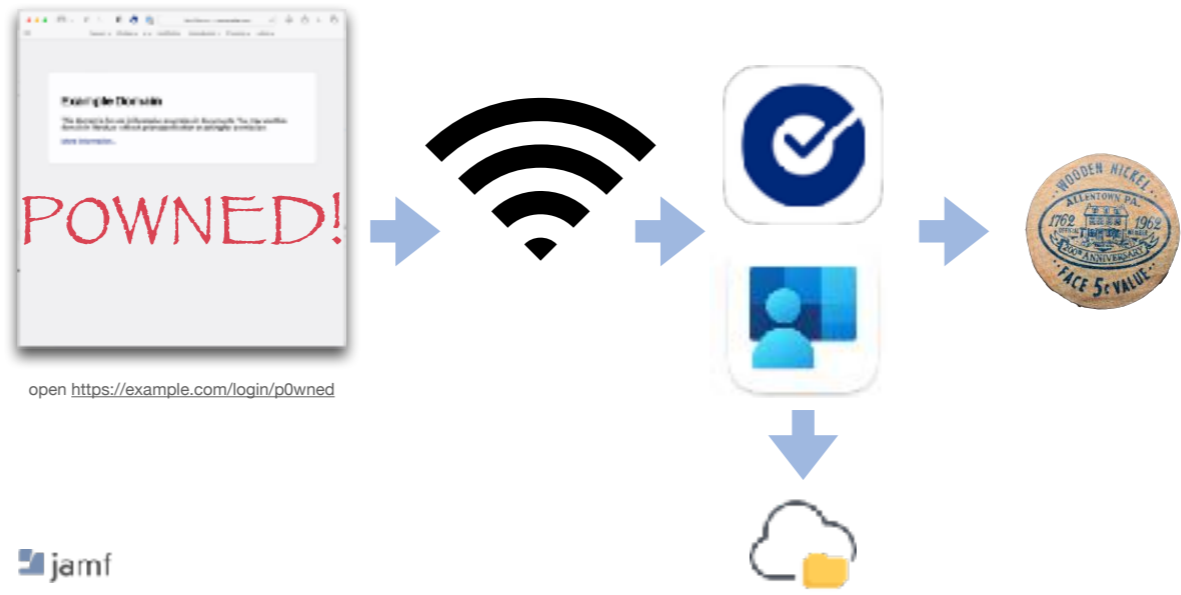
Not valid before: 07-11-2024 09:00:00

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



talk about token, bouncer at the club, [build] expiration, [build] refresh token

ZTNA and killing network connections

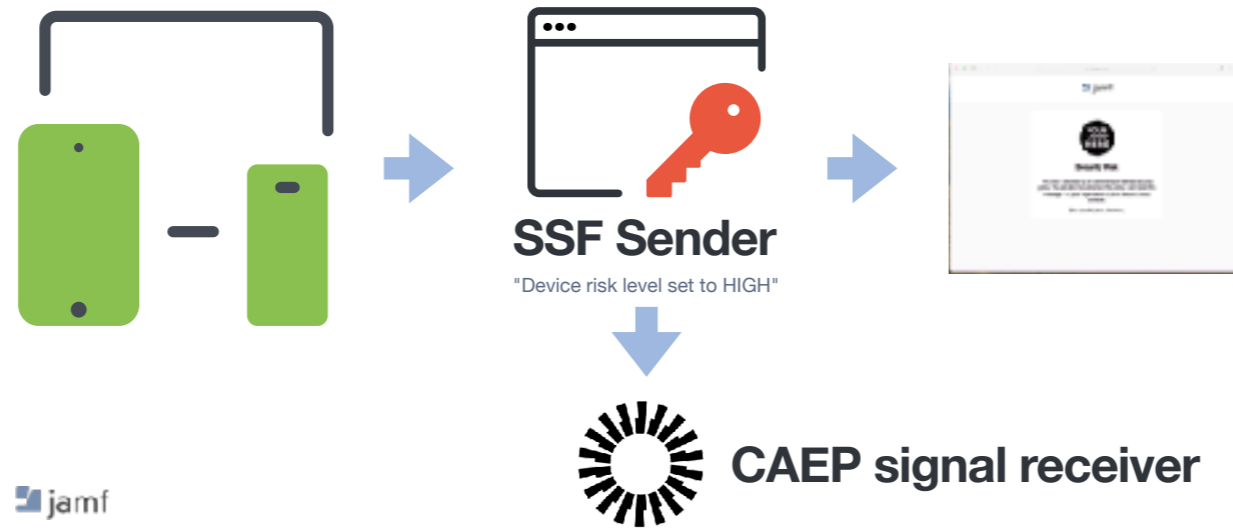


what happens when machine compromised? token generating machine. without user interaction. papyrus cursed font

ZTNA and killing network connections



ZTNA and killing network connections



Final Thoughts

And then there will be cake.



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 to give the
gift... of the
Apple.



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."**



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

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



Thank you.



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

