

Deploying Platform SSO with Entra ID

Best Practices



Presenters



Michael Epping

Product Manager, Microsoft



Mark Morowczynski

Product Manager, Microsoft

Platform SSO Fundamentals

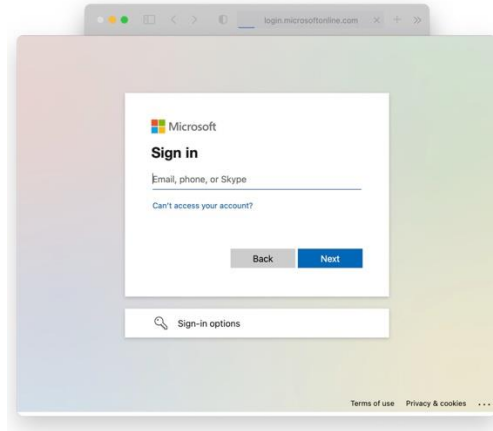
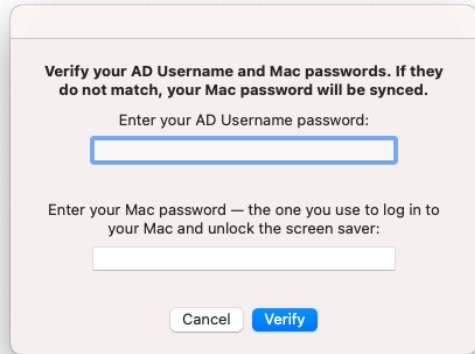
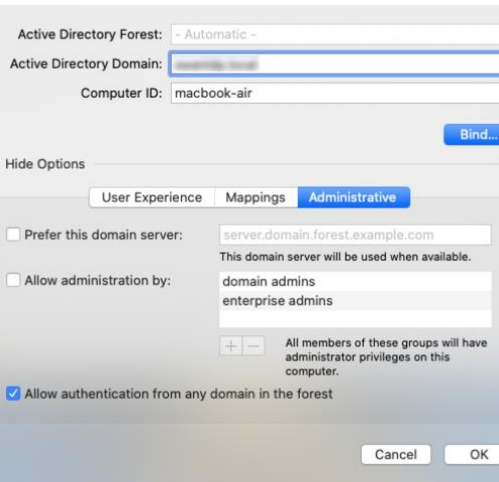
Deployment Best Practices

Authentication Strengths Feedback

Go Do's!



History of Enterprise Identity Options on macOS



LDAP Bind
2001
Mac OS X (10.0)

Kerberos SSO
2019
macOS 10.15

Enterprise SSO
2019
macOS 10.15

3rd Party
(Jamf Connect,
XCreds, etc.)

Platform SSO
2022
macOS 13+

Quick Poll

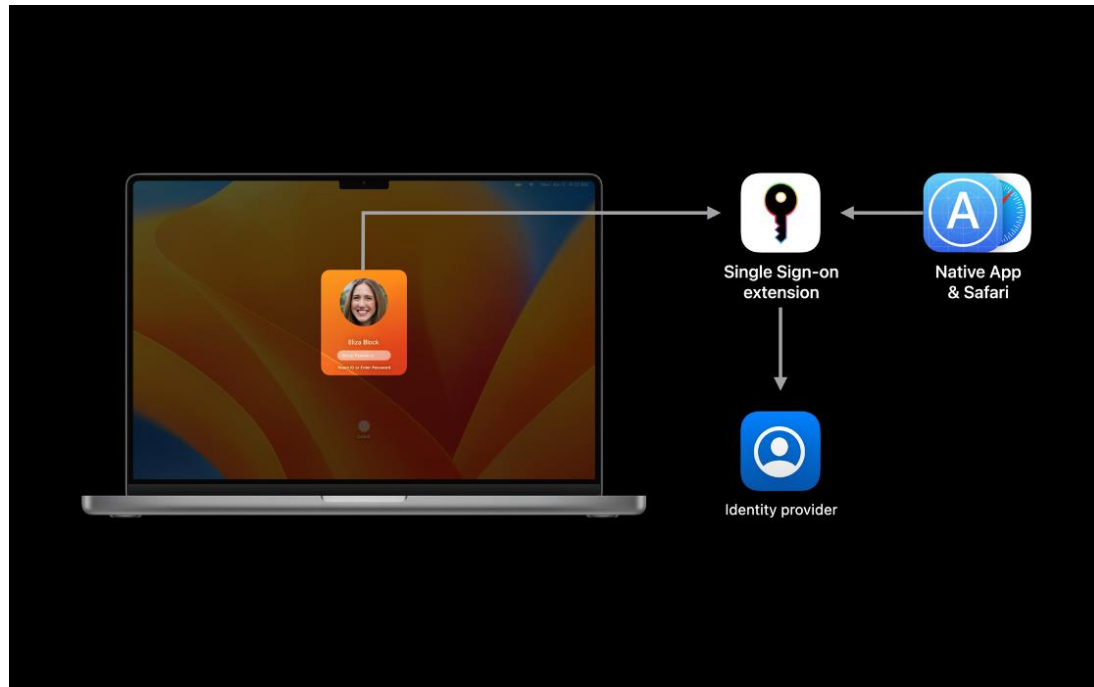
Show of hands, how many of you have deployed the Microsoft Enterprise SSO Extension?

Where are the gaps?

Nothing outlined so far provides a native way to manage local identities without on-premises AD

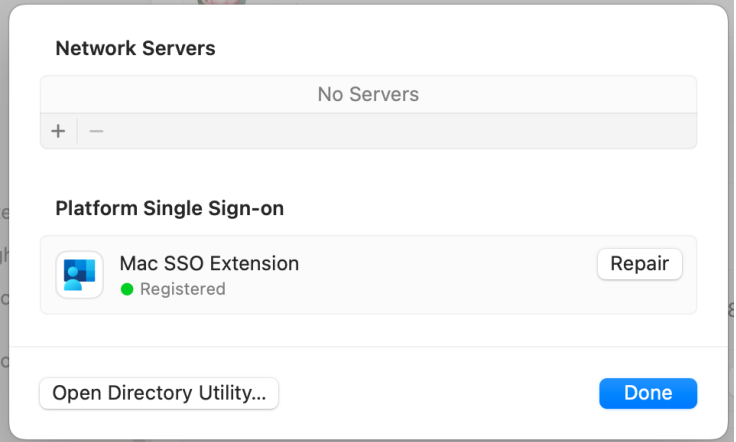
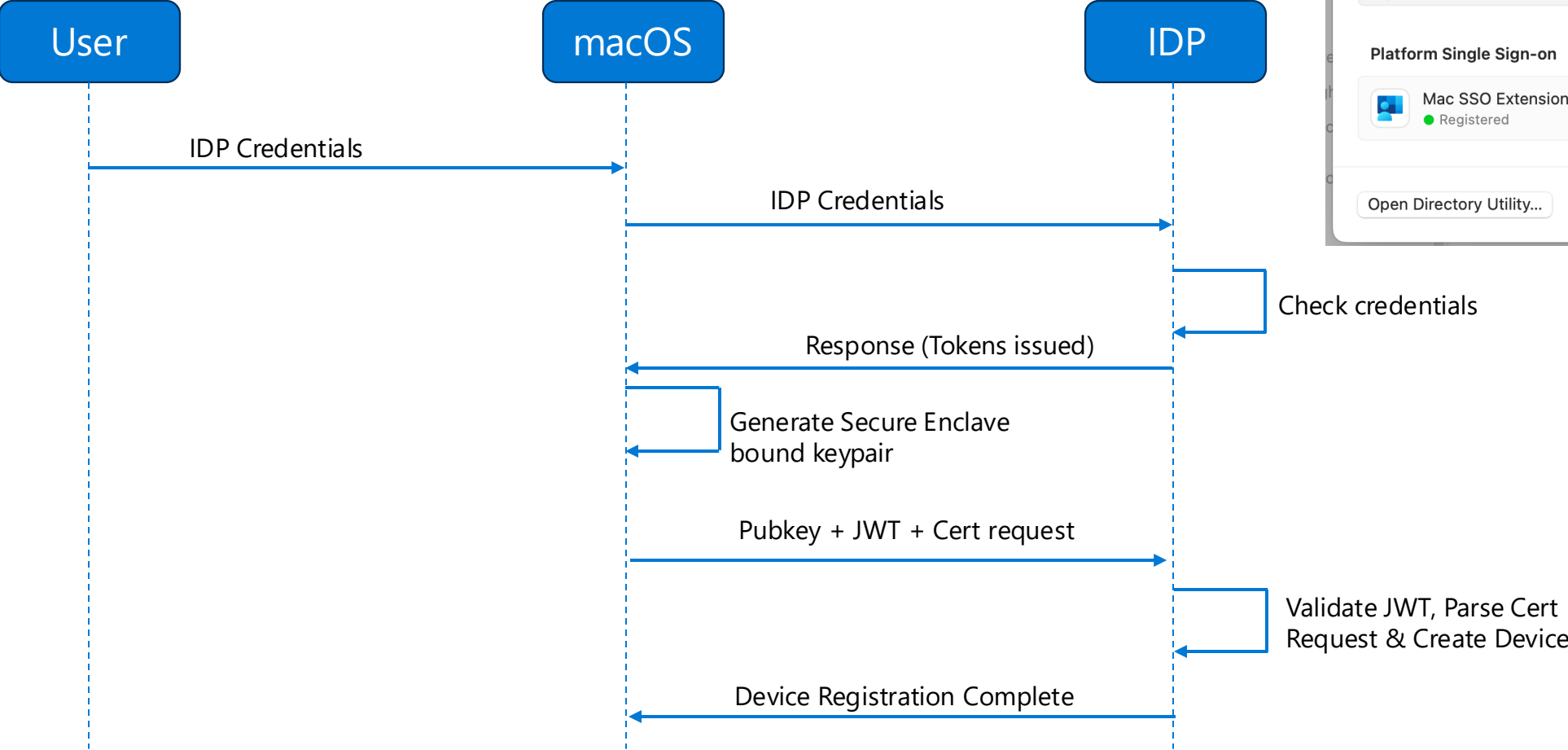
- Local creds, on-premises AD, MDM, or 3rd party tools
- On-premises dependencies
- Multiple tools used for SSO
- No phishing-resistance

Platform SSO



- Framework built by Apple
- Local account credential managed by combo of MDM and IDP vendor plugin
- Replacement for AD join
- Multiple auth methods

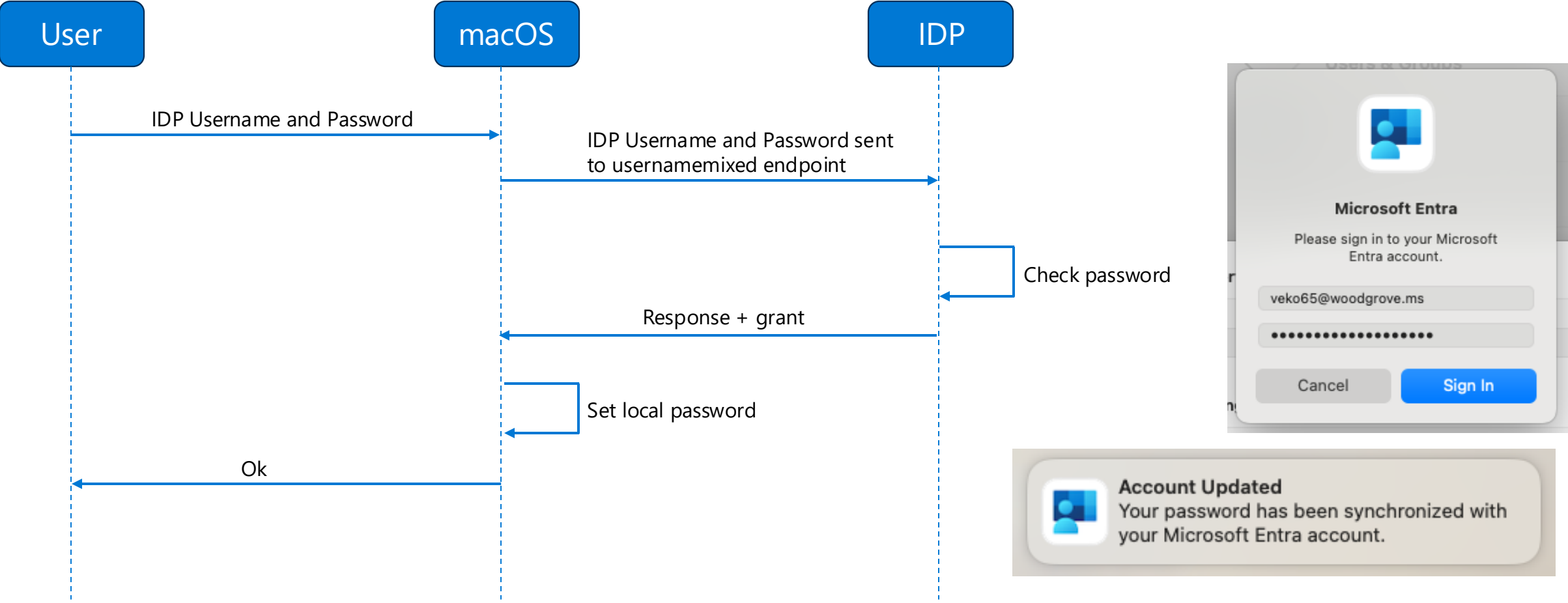
Step 1: Device Registration



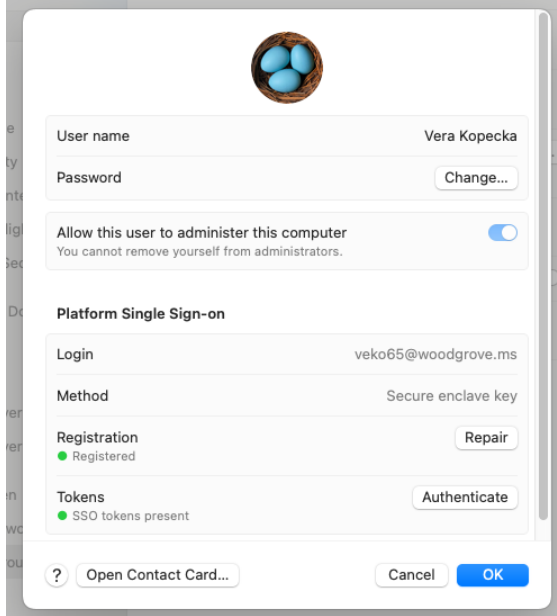
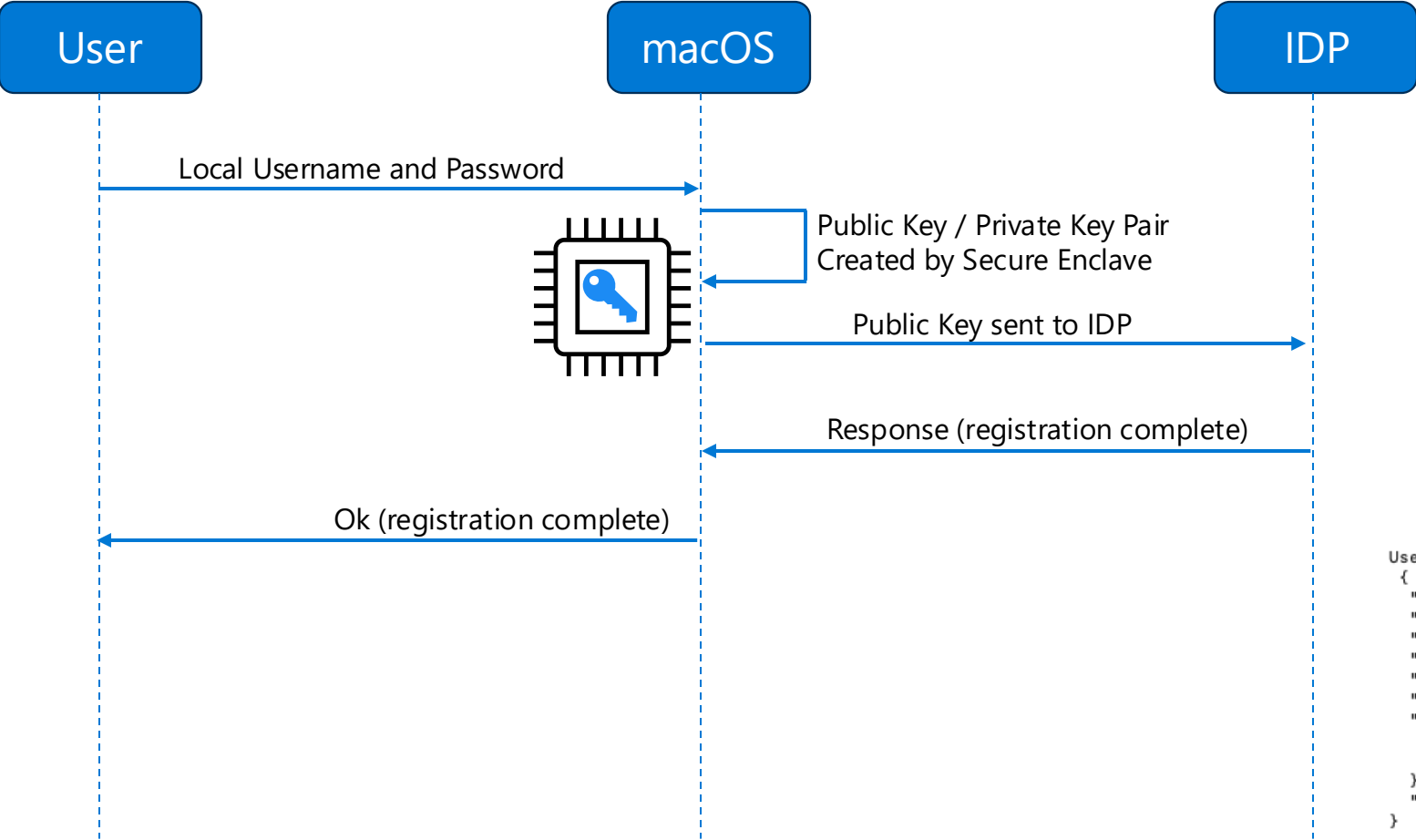
3 Authentication Methods Support by Platform SSO

| | Good: Password | Better: Smart Card | Best: Secure Enclave Key |
|------------------------------------------------|-------------------------------------|--------------------|-------------------------------------------------------|
| Local Account Password Sync w/ Entra ID | ✓ | ✗ | ✗ |
| Federation Support | ✓ via WS-Trust (same as Windows) | ✓ | ✓ |
| MFA Required for Registration | ✗ | ✓ | ✓ |
| Phishing Resistant | ✗ | ✓ | ✓ |
| Phishing Resistant via Built-In Apple Hardware | ✗ | ✗ | ✓ via same protocols as Windows Hello for Business |
| Can be used as a passkey | ✗ | ✗ | ✓ |

Step 2: User Registration - Password Sync Flow

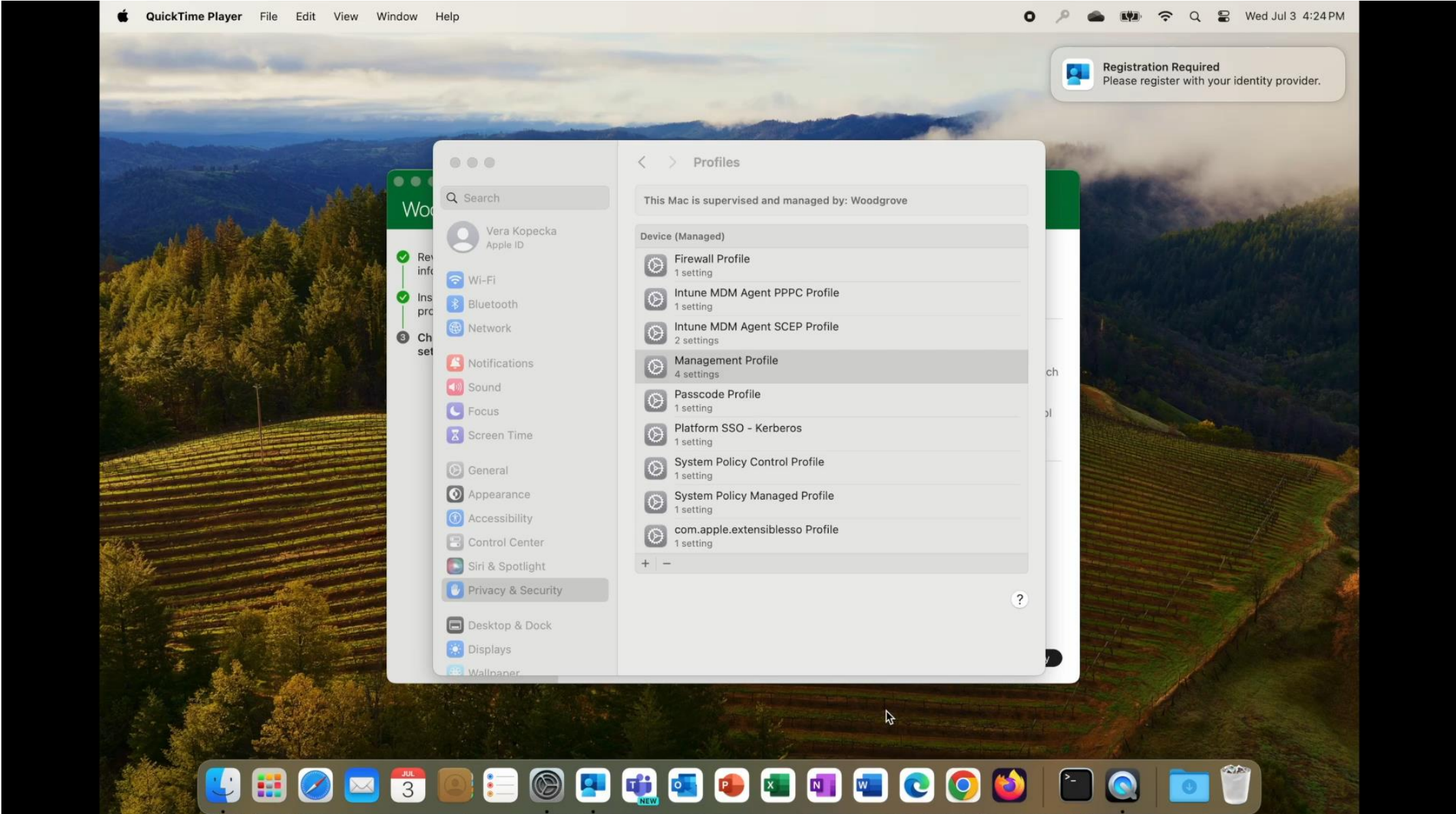


Step 2: User Registration - Secure Enclave Key Flow

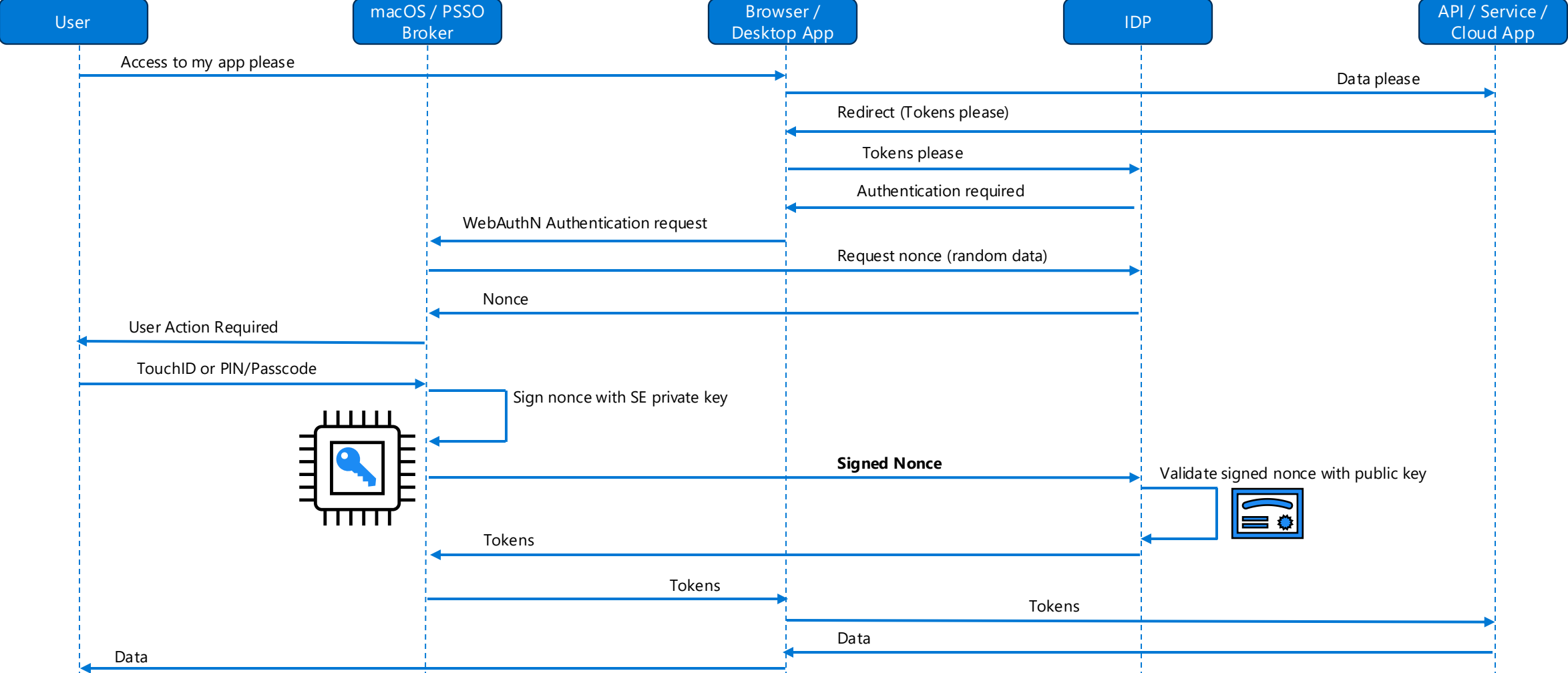


```
User Configuration:
{
  "_sepKeyData" : "cpRyk+90gI1JM06zFpYVUqbx+3R85P+BdWi91ERTKZE=",
  "created" : "2024-07-03T21:30:42Z",
  "lastLoginDate" : "2024-07-03T21:29:49Z",
  "loginType" : "POLoginTypeUserSecureEnclaveKey (2)",
  "state" : "POUserStateNormal (0)",
  "uniqueIdentifier" : "4251CE01-07A2-40B5-A267-BCC3667A96A6",
  "userLoginConfiguration" : {
    "created" : "2024-07-03T21:30:42Z",
    "loginUserName" : "v***@woodgrove.ms"
  },
  "version" : 1
}
```

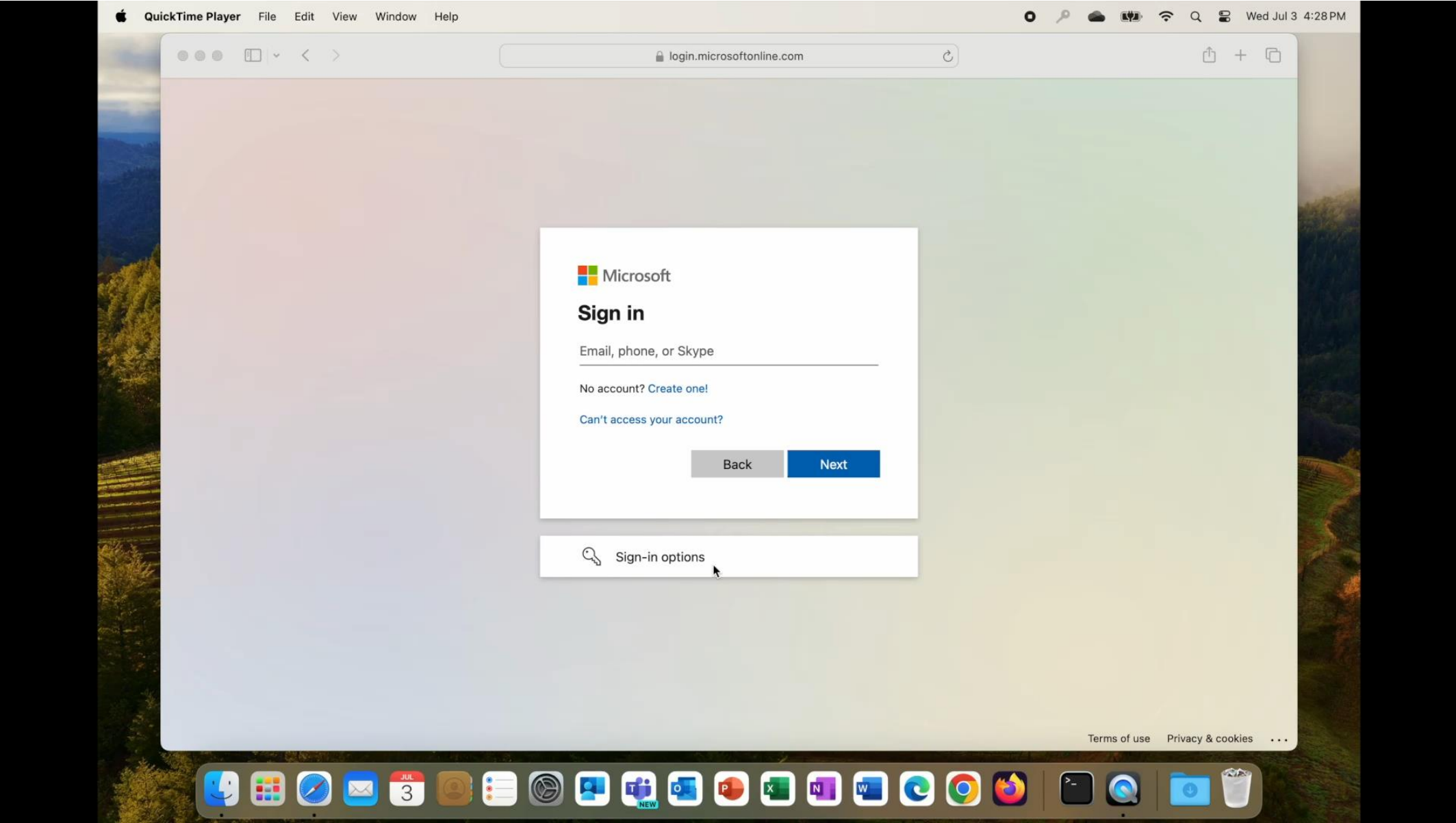
Secure Enclave Key Registration Experience



Secure Enclave Key Interactive Authentication Flow



Secure Enclave Key Authentication Experience



Sonoma vs. Ventura

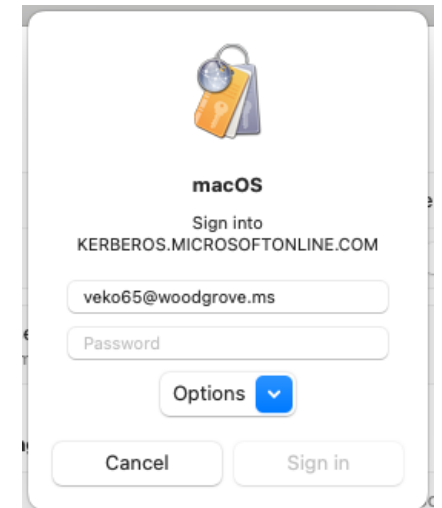
| Feature | Ventura (macOS 13) | Sonoma (macOS 14) |
|--------------------------------------------------------|--------------------|-------------------|
| Secure Enclave | ✓ | ✓ |
| Password Sync | ✓ | ✓ |
| Smart Cards | ✗ | ✓ |
| User enrollment and registration UX in System Settings | ✗ | ✓ |
| Local Account Creation using IDP | ✗ | ✓ |
| Admin authentication without local user account | ✗ | ✓ |
| Kerberos SSO | ✗ | ✓ |

Kerberos SSO via Platform SSO

- Leverages the Apple Kerberos SSO extension
- Simplifies delivery of SSO to one tool
- Requires custom configuration profile (see docs)
- User experience similar to Apple Kerberos SSO, easier deployment

```
<key>ExtensionData</key>
<dict>
  <key>allowPasswordChange</key>
  <true/>
  <key>allowPlatformSSOAuthFallback</key>
  <true/>
  <key>performKerberosOnly</key>
  <true/>
  <key>pwReqComplexity</key>
  <true/>
  <key>syncLocalPassword</key>
  <true/>
  <key>usePlatformSSOTGT</key>
  <true/>
</dict>
```

```
<key>Hosts</key>
<array>
  <string>woodgrove.net</string>
  <string>*.woodgrove.net</string>
</array>
```

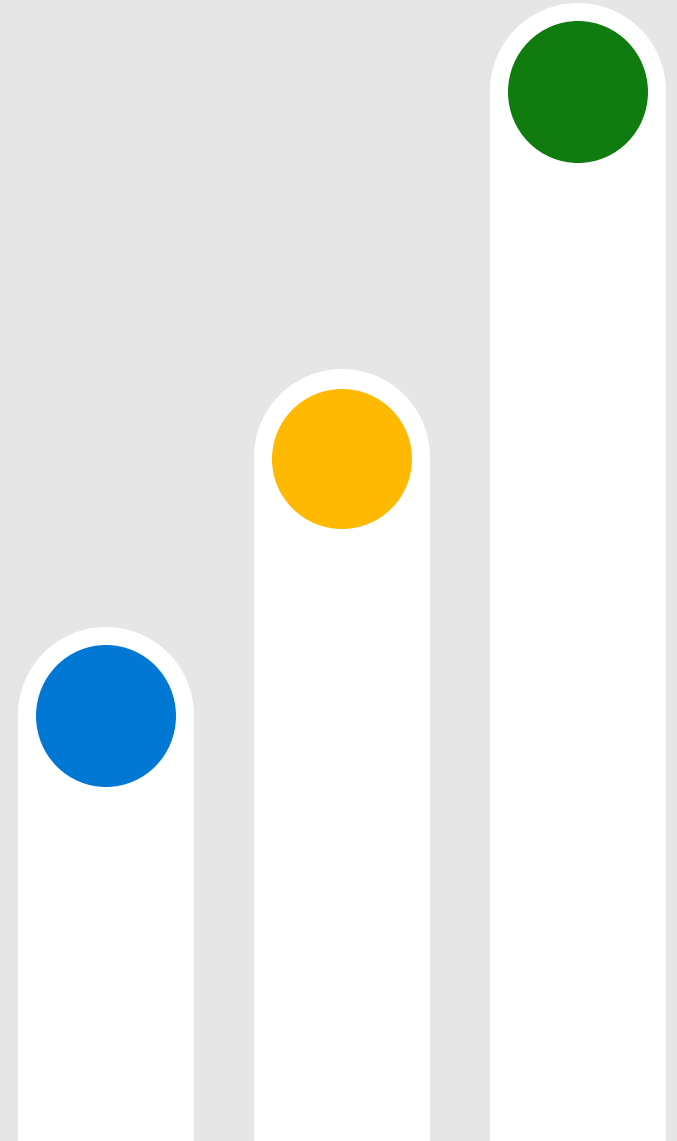


Platform SSO Fundamentals

Deployment Best Practices

Authentication Strengths Feedback

Go Do's!



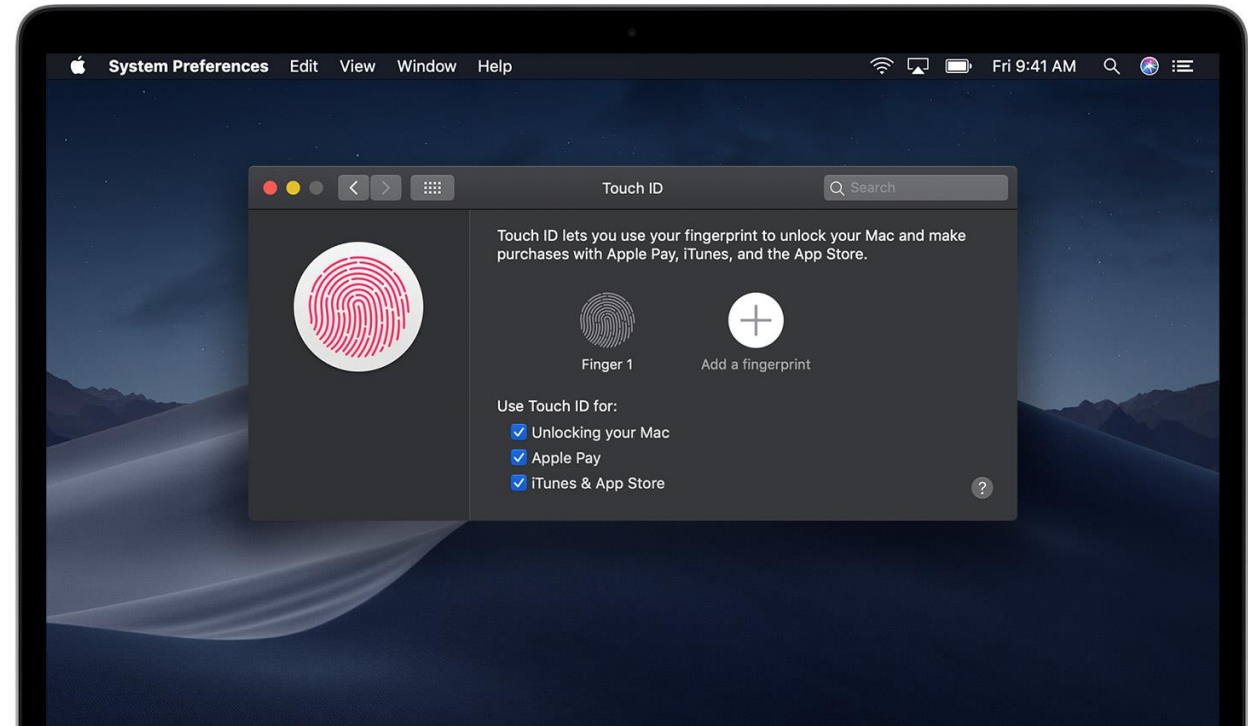
Best Practices

1. Deploy Secure Enclave Key

Secure Enclave and MFA

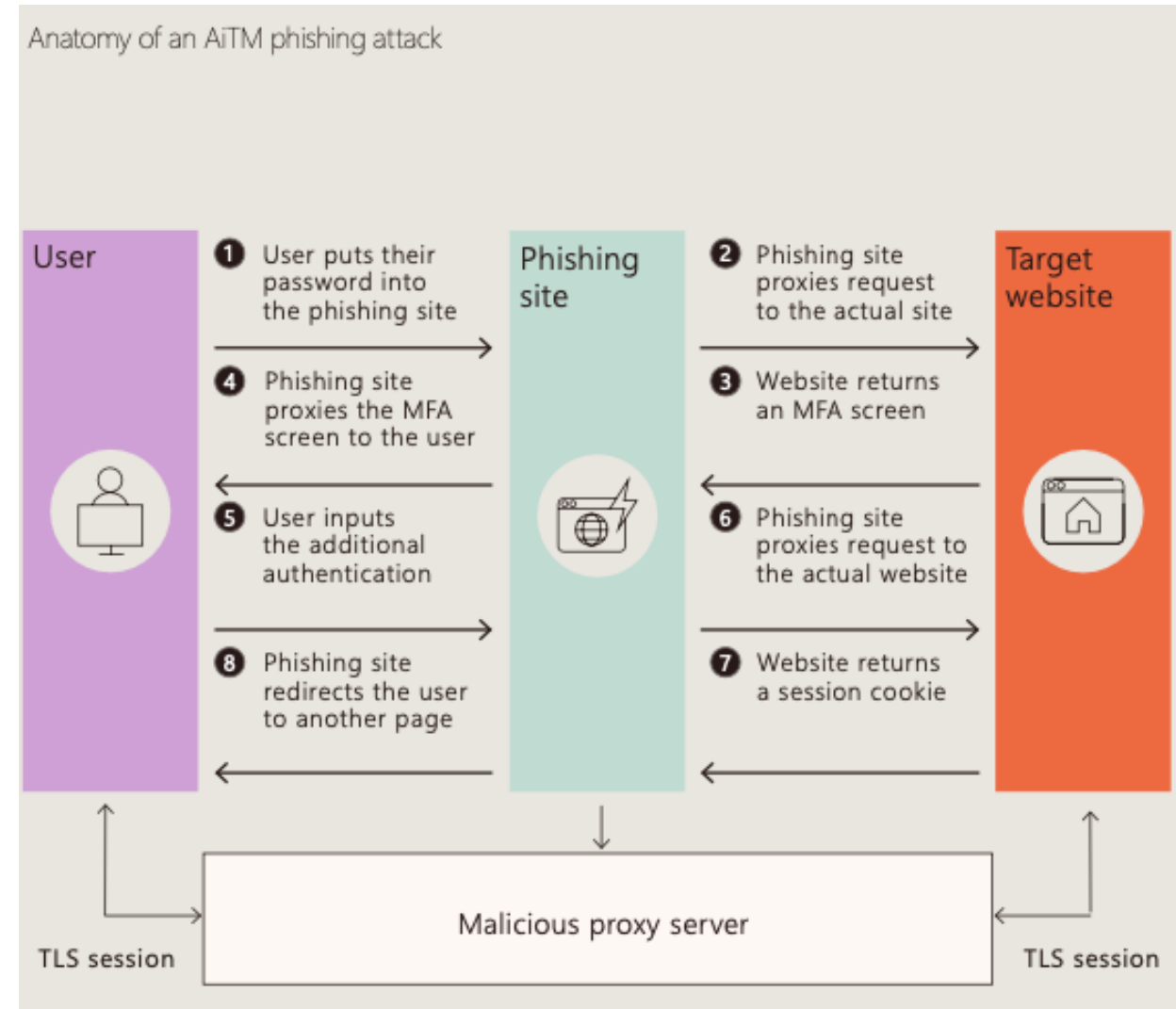
Secure Enclave PSSO = Phishing Resistant MFA credential

- PIN/Local Passcode =
Something you have +
something you know
- TouchID = Something you have
+ something you are
- You'll satisfy MFA Conditional
Access Policies



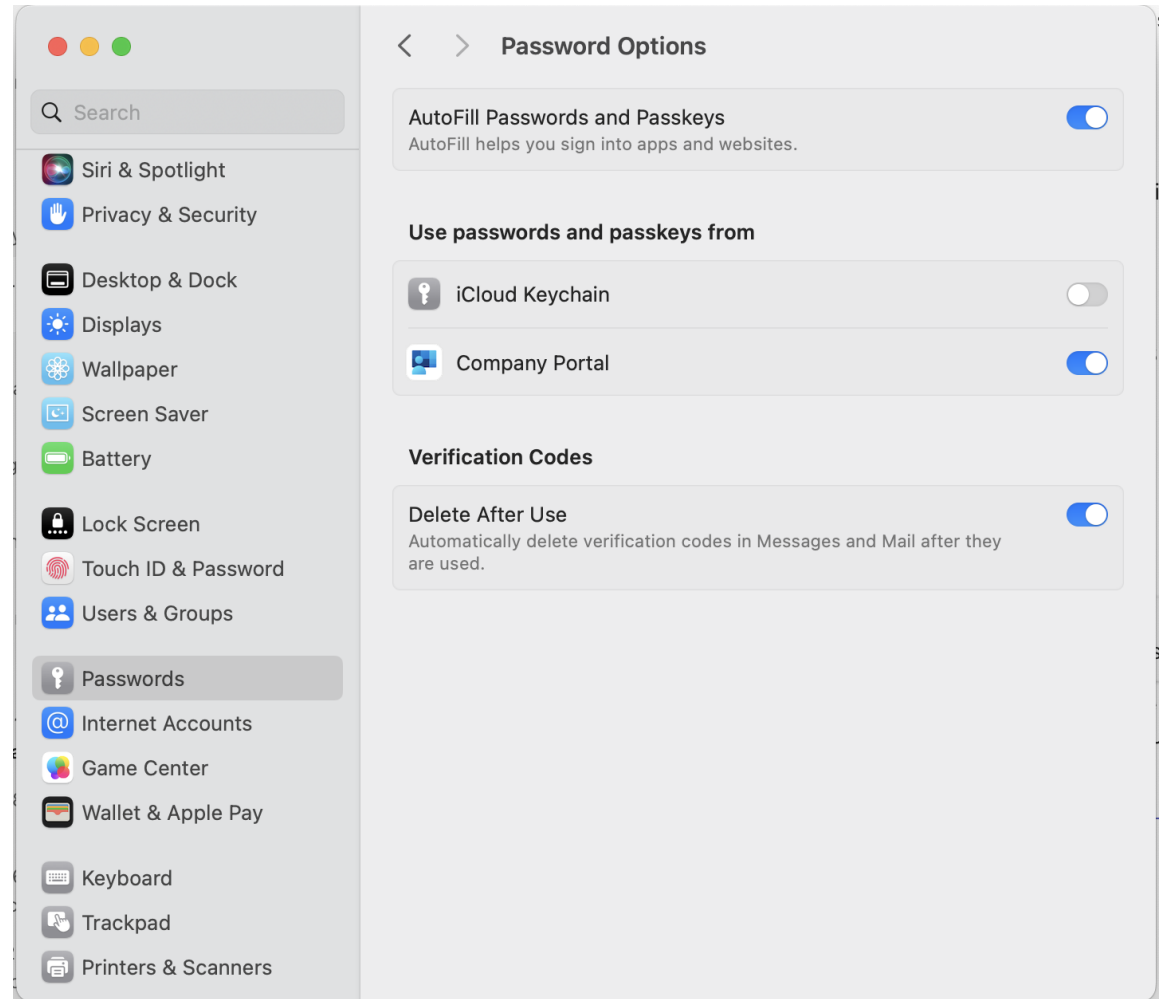
Why Phishing Resistant is Critical?

- Defenses erode over time
- MFA is the bare minimum... today



Why Phishing Resistant is Critical?

- Defenses erode over time
- MFA is the bare minimum... today
- Understand FIDO2/CTAP2/WebAuthN-
<https://aka.ms/PSU2024FIDO2>
- Then really shift focus to endpoint (token theft, malware, updates, physical device theft)



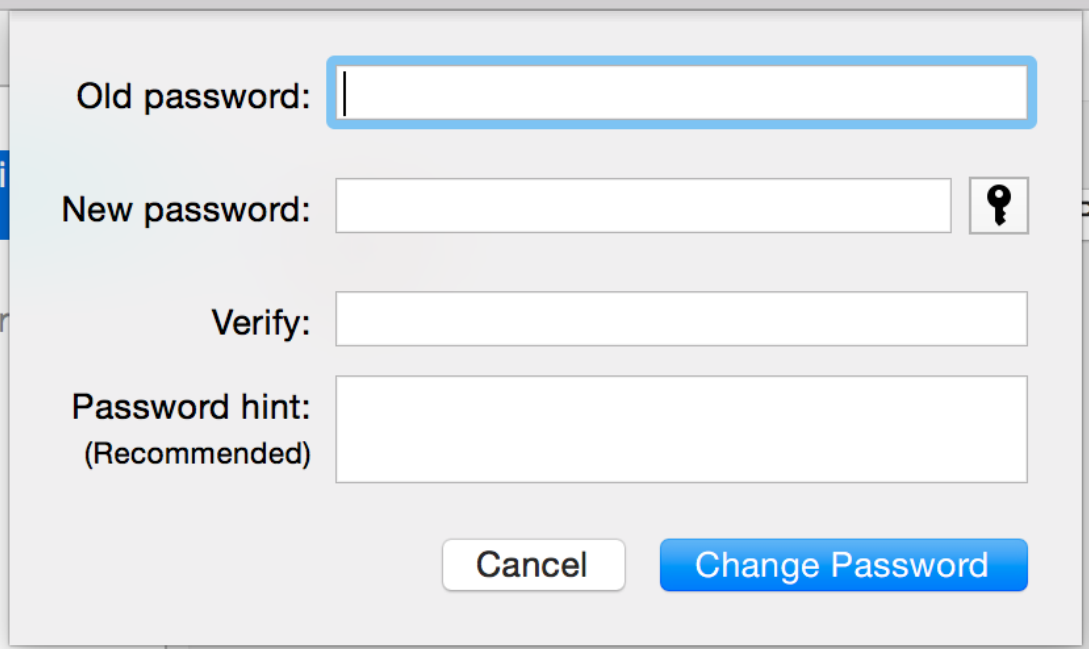
Best Practices

1. Deploy Secure Enclave Key
2. Align password management for macOS

MDM Password Policy Considerations


Password policies set via MDM can conflict with Platform SSO

- Secure Enclave – overly complex password policies or frequent rotation requirements will cause user experience issues
- Password Sync – MDM password policies that don't match Entra ID / Active Directory password settings will conflict



A screenshot of a password change dialog box. The dialog has a light gray background and a white border. It contains four input fields: 'Old password:', 'New password:', 'Verify:', and 'Password hint: (Recommended)'. The 'Old password:' field is highlighted with a blue border. The 'New password:' field has a key icon to its right. At the bottom, there are two buttons: 'Cancel' and 'Change Password'.

Old password:

New password: 

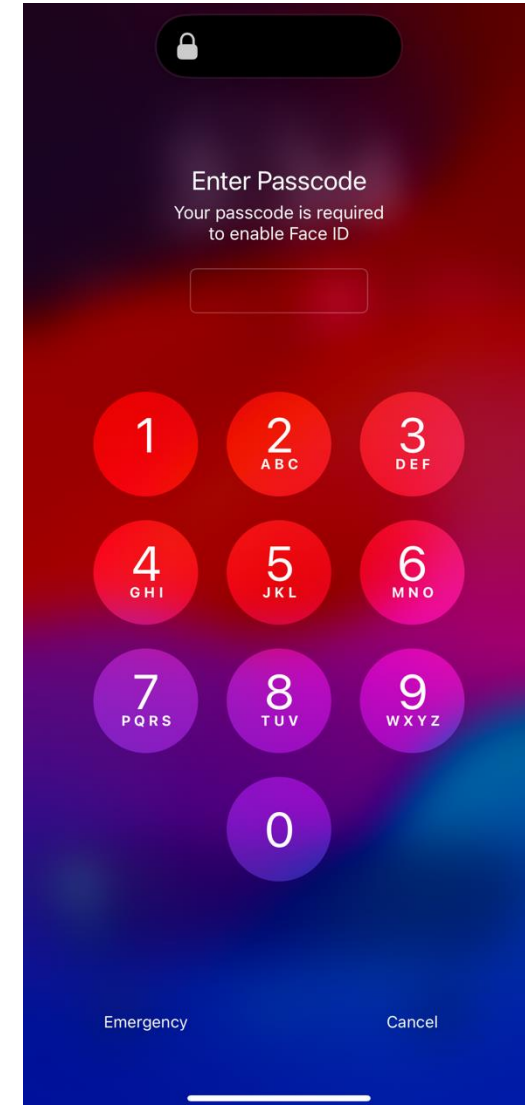
Verify:

Password hint:
(Recommended)

MDM Password Policy Considerations

Secure Enclave Guidance:

- Align requirements with the rules your organization use to manage Windows Hello for Business PINs
- Default WHFB PIN rules:
 - 4 characters
 - Numeric-only Allowed
 - No expiration
 - Biometric Allowed
- Recommended PIN rules:
 - 6-8 characters
 - Numeric-only Allowed
 - No expiration
 - Biometric Allowed



MDM Password Policy Considerations

Secure Enclave Guidance:

- Align requirements with the rules your organization use to manage Windows Hello for Business PINs
- Default WHFB PIN rules:
 - 4 characters
 - Numeric-only Allowed
 - No expiration
 - Biometric Allowed
- Recommended PIN rules:
 - 6-8 characters
 - Numeric-only Allowed
 - No expiration
 - Biometric Allowed

Declarative Device Management (DDM)

[Remove category](#)

These settings configure the declarations used by Apple's declarative device management feature. These settings are separate from older MDM settings and only apply to a device enabled for declarative management. Learn more about declarative management at developer.apple.com

Passcode

[Remove subcategory](#)

i 3 of 7 settings in this subcategory are not configured

- | | | |
|------------------------------|------------------------------------------|---|
| Maximum Grace Period * ⓘ | <input type="text" value="0"/> | ⊖ |
| Minimum Passcode Length * ⓘ | <input type="text" value="6"/> | ⊖ |
| Require Complex Passcode ⓘ | <input type="checkbox"/> False | ⊖ |
| Require Passcode on Device ⓘ | <input checked="" type="checkbox"/> True | ⊖ |

Restrictions

[Remove category](#)

Configure the Restrictions payload to enable or disable features on devices. These configurations can be used prevent users from accessing a specific app, service or function on enrolled devices. For example, a restriction can be added that prevents an iPhone or iPad from using AirPrint. Another restriction can be added to prevent the sharing of passwords over AirDrop on an iPhone, iPad and Mac. Certain restrictions on an iPhone may be mirrored on a paired Apple Watch.

i 73 of 74 settings in this category are not configured

- | | | |
|--------------------------------|------------------------------------------|---|
| Allow Fingerprint For Unlock ⓘ | <input checked="" type="checkbox"/> True | ⊖ |
|--------------------------------|------------------------------------------|---|

MDM Password Policy Considerations

Password Sync Guidance:

- Remove MDM password policies altogether, let PSSO Password Sync take control
- At minimum, make sure MDM password policy has same requirements as Entra ID / Active Directory

| Account Policies/Password Policy | |
|--------------------------------------------|------------------------|
| Policy | Setting |
| Enforce password history | 5 passwords remembered |
| Maximum password age | 90 days |
| Minimum password age | 30 days |
| Minimum password length | 8 characters |
| Password must meet complexity requirements | Enabled |

Passcode

[Remove subcategory](#)

Configure the Passcode payload to specify whether a password or passcode is required to access and use an enrolled device. When the configuration profile is installed, users are asked to enter a password or passcode that meets the policies you specify. Otherwise, the profile won't be installed. When the Passcode payload is installed on an iPhone or iPad, users have 60 minutes to enter a passcode. If users don't do so within that time frame, the payload forces them to enter a passcode using the specified settings. If you use device policies and Exchange passcode policies, the two sets of policies are merged and the strictest settings are enforced.

i 11 of 17 settings in this subcategory are not configured

- Min Complex Characters * ✓
- Require Alphanumeric Passcode True
- PIN History * ✓
- Max PIN Age In Days * ✓
- Min Length * ✓
- Force PIN True
- Allow Simple Passcode False

Best Practices

1. Deploy Secure Enclave Key
2. Align password management for macOS
3. Enable Recommended MDM configs

Recommended MDM Settings

Recommended Configuration:

- All other configuration options can be the same as previous Enterprise SSO profiles
- Replace eSSO profile, don't create conflicting eSSO and PSSO profiles

Extensible Single Sign On (SSO)

Configure an app extension that enables single sign-on (SSO) for devices.

| | |
|--------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Authentication Method (Deprecated) ⓘ | UserSecureEnclaveKey |
| Screen Locked Behavior ⓘ | Do Not Handle |
| Registration Token ⓘ | {{(DEVICEREGISTRATION)}} |
| Platform SSO ⓘ | |
| Authentication Method ⓘ | UserSecureEnclaveKey |
| Enable Authorization ⓘ | Enabled |
| Enable Create User At Login ⓘ | Enabled |
| New User Authorization Mode ⓘ | Standard |
| Use Shared Device Keys ⓘ | Enabled |
| User Authorization Mode ⓘ | Standard |
| Team Identifier ⓘ | UBF8T346G9 |
| Extension Identifier ⓘ | com.microsoft.CompanyPortalMac.ssoextension |
| Type ⓘ | Redirect |
| URLs ⓘ | https://login.microsoftonline.com , https://login.microsoft.com , https://sts.windows.net , https://login.partner.microsoftonline.cn , https://login.chinacloudapi.cn , https://login.microsoftonline.us , https://login-us.microsoftonline.com , |

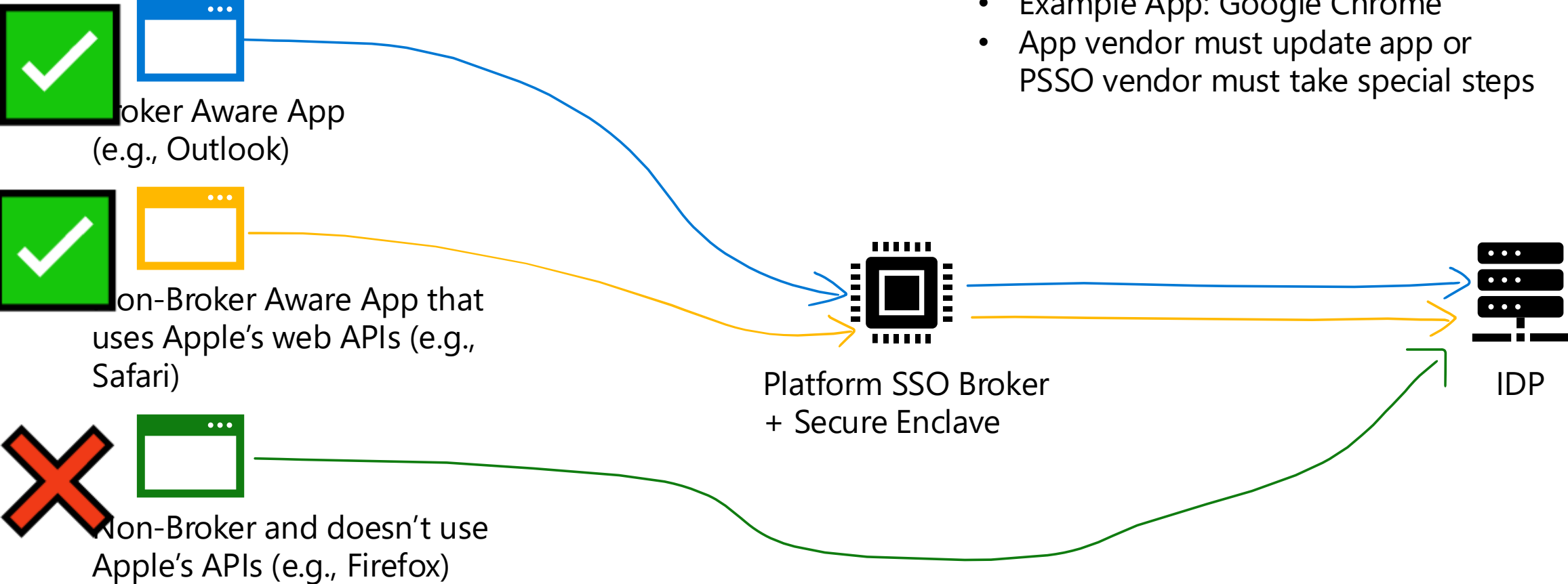
MDM Config Best Practices Round Up

- Start with the *recommended* and *documented* Platform SSO settings
 - Especially Shared Device Keys
 - Iterate from there
- Deploy Kerberos settings as part of your Platform SSO configuration
- Make sure to bring over your Microsoft Enterprise SSO Extension settings
- Align MDM password policy settings with org requirements
 - Work with Security and Identity teams to align across OSes

Best Practices

1. Deploy Secure Enclave Key
2. Align password management for macOS
3. Enable Recommended MDM configs
4. Understand impact of hardware-bound device identity

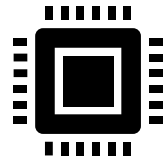
Authentication Flows



- No access to any key material controlled by Platform SSO
- Example App: Google Chrome
- App vendor must update app or PSSO vendor must take special steps

Device-Bound Cert Impact on MDMs

macOS Device



Platform SSO Broker
+ Secure Enclave



macOS Keychain



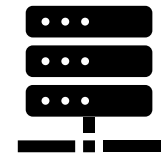
MDM Client



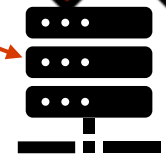
1. Check Device Cert in Keychain for
Device ID

2. Report Device Info to MDM
Server w/ Device Identifier

Microsoft Compliance API

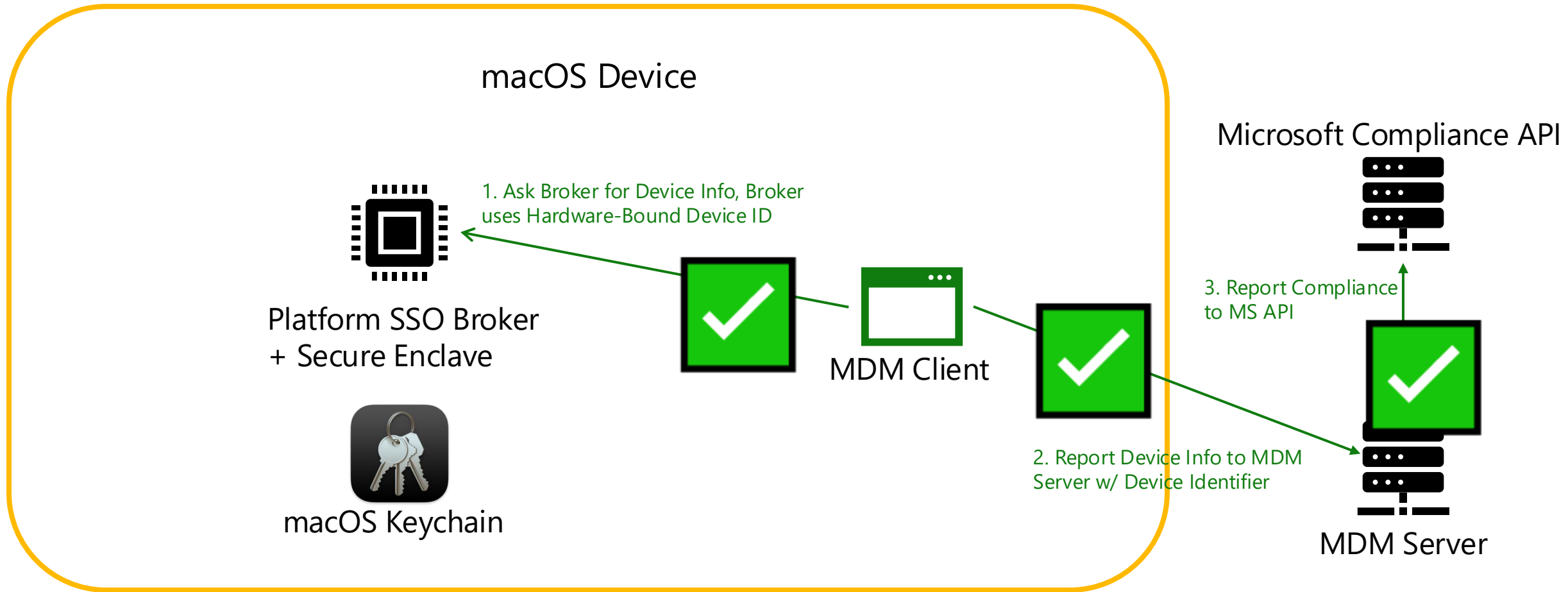


3. Report Compliance
to MS API



MDM Server

Device-Bound Cert Impact on MDMs



Requirement: MDM Vendors must make updates to their clients to use the broker instead of the Keychain for 3rd Party Compliance Integration w/ Microsoft

Best Practices

1. Deploy Secure Enclave Key
2. Align password management for macOS
3. Enable Recommended MDM configs
4. Understand hardware-bound device identity impacts
5. Follow Apple's TLS Guidance

TLS Inspection and Apple's SSO Framework

- TLS Inspection is not allowed for specific Apple URLs:
 - app-site-association.cdn-apple.com
 - app-site-association.networking.apple
- Top cause of support cases we see for macOS SSO, SSO will be completely broken
- Work with your network teams to exempt these URLs, or preferably these wildcards:
 - *.cdn-apple.com
 - *.networking.apple

TLS Inspection and Apple's SSO Framework

- Trust but Verify – check if TLS Inspection is occurring on your Macs:
 - Use Mac Evaluation Utility from AppleSeed for IT

The screenshot displays the 'report01' results in the Mac Evaluation Utility. The 'Results' tab is active, showing a table of categories and tests. The 'HTTPS Interception' category is highlighted, and the 'Additional Content' section is expanded to show individual tests. A warning icon is present next to the 'app-site-association.cdn-apple.com:443' test. The right-hand pane shows the 'Status' as 'Warning' and the 'Observation' text.

| Categories and Tests | Number of Tests | Status |
|---------------------------------------------------|-----------------|--------|
| > Computer Information | 5 | ✓ |
| > Network Information | 10 | ⚠ |
| > Apple Network Services | 216 | ✓ |
| ▼ HTTPS Interception | 79 | ⚠ |
| > Certificate Validation | 3 | ⚠ |
| > Device Setup | 7 | ⚠ |
| > Device Management | 15 | ⚠ |
| > Apple Business Essentials | 5 | ⚠ |
| > Apple Business Manager and Apple School Manager | 9 | ⚠ |
| > Software Update | 5 | ⚠ |
| > Apple ID | 4 | ⚠ |
| > App Store | 4 | ⚠ |
| > Content Caching | 7 | ⚠ |
| ▼ Additional Content | 10 | ⚠ |
| 🔍 app-site-association.cdn-apple.com:443 | | ⚠ |
| 🔍 app-site-association.networking.apple:443 | | ⚠ |
| 🔍 audiocontentdownload.apple.com:443 | | ⚠ |
| 🔍 data.appattest.apple.com:443 | | ⚠ |
| 🔍 devimages-cdn.apple.com:443 | | ⚠ |
| 🔍 download.developer.apple.com:443 | | ⚠ |
| 🔍 playgrounds-assets-cdn.apple.com:443 | | ⚠ |
| 🔍 playgrounds-cdn.apple.com:443 | | ⚠ |
| 🔍 sylvan.apple.com:443 | | ⚠ |
| 🔍 www.apple.com:443 | | ⚠ |
| > Feedback Assistant | 3 | ⚠ |
| > DNS Resolution | 1 | ⚠ |
| > Apple Diagnostics | 1 | ⚠ |

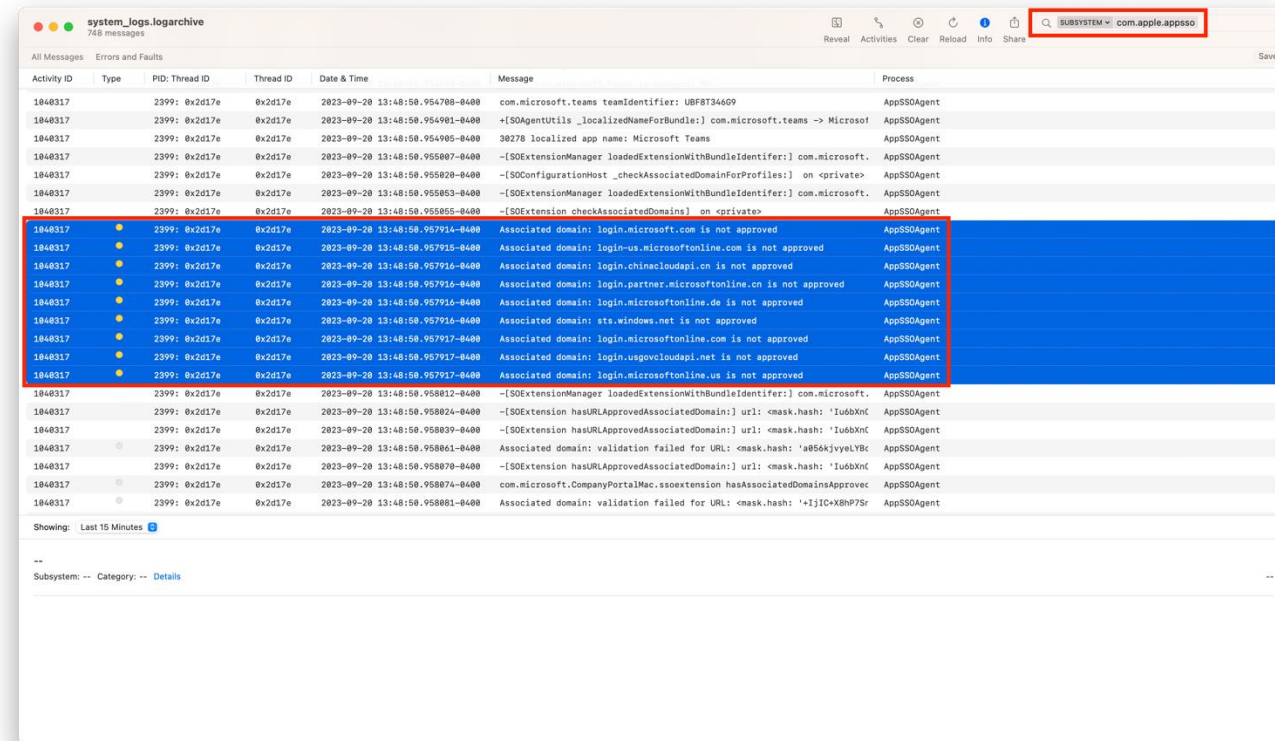
Status: Warning

Observation: app-site-association.cdn-apple.com:443 — Certificate isn't trusted by built-in anchor certs (("Charles Proxy CA (2 Nov 2023, Michaels-MacBook-Pro-2.local)" certificate is not trusted))

Description: HTTPS Interception app-site-association.cdn-apple.com:443

TLS Inspection and Apple's SSO Framework

- Trust but Verify – check if TLS Inspection is occurring on your Macs:
 - Use Mac Evaluation Utility from AppleSeed for IT
- Can also check with sysdiagnose:
 - `sudo sysdiagnose -f ~/Desktop/`
 - Open the `system_logs.logarchive` file.
 - Search for `com.apple.appsso` and change the filter to SUBSYSTEM



Best Practices

1. Deploy Secure Enclave Key
2. Align password management for macOS
3. Enable Recommended MDM configs
4. Understand hardware-bound device identity impacts
5. Follow Apple's TLS Guidance
6. Use the Troubleshooting Guides

Troubleshooting Guides

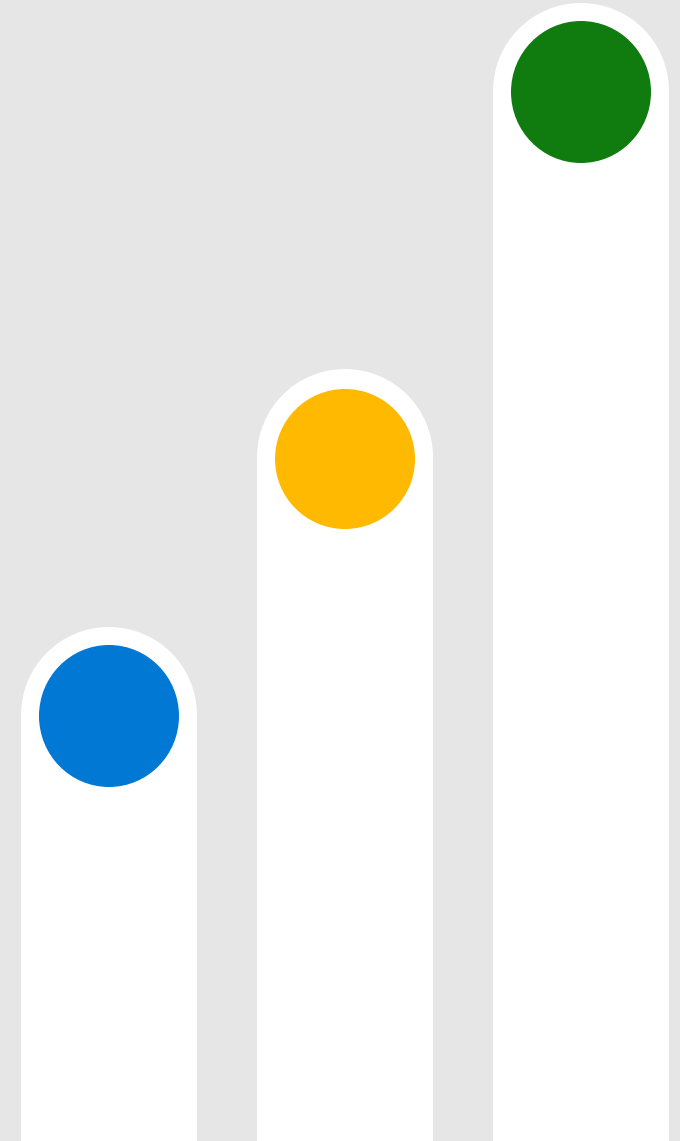
- “PSSO isn’t working. Has anyone seen this before?”...YES!
 - Have we seen your specific issue before? Maybe
- Leverage the troubleshooting guides
 - Enterprise SSO: aka.ms/AppleSSOTSG
 - Platform SSO: aka.ms/PSSOTSG
- Be SPECIFIC
 - Which credential? Password/Smart Card/Secure Enclave
 - Which OS? Ventura/Sonoma/Sequoia
 - Which MDM? Intune/Jamf/etc.
 - Does that MDM support this?
 - Where do you differ from the recommended config?
 - What do the guides lead you to believe the issue is?
 - Do you have a support case open?

Platform SSO Fundamentals

Deployment Best Practices

Authentication Strengths Feedback

Go Do's!



Auth Strengths Option 1

View Authentication Strength ×

- Pros

- Quicker time to PSSO General Availability (already works this way in Public Preview)

- Cons

- Lack of per-OS granularity between Windows and macOS
- Microsoft may still make changes in the future and split the “overloaded authentication flow”
 - May or may not require administrator action

Name

Phishing-resistant MFA

Type

Built-in

Description

Include authentication methods that are phishing-resistant like Passkeys (FIDO2) and Windows Hello for Business

Authentication Flows

Windows Hello For Business / **macOS SE Key**

OR

Passkeys (FIDO2)

OR

Certificate-based Authentication (Multifactor)

Auth Strengths Option 2

View Authentication Strength



- Pros
 - Better per-OS granularity
 - Future-proof, no changes required down the road
- Cons
 - Longer time to PSSO
 - General Availability

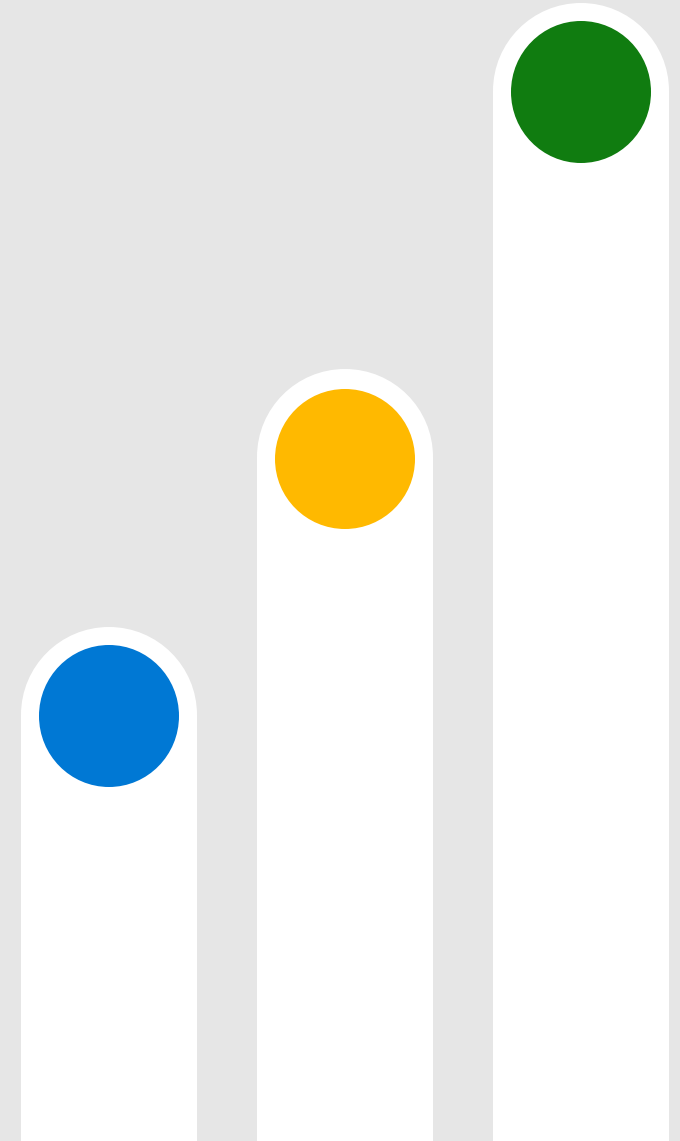
| | |
|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Name | Phishing-resistant MFA |
| Type | Built-in |
| Description | Include authentication methods that are phishing-resistant like Passkeys (FIDO2) and Windows Hello for Business |
| Authentication Flows | Windows Hello For Business OR Passkeys (FIDO2) OR Certificate-based Authentication (Multifactor) OR macOS SE Key |

Platform SSO Fundamentals

Deployment Best Practices

Authentication Strengths Feedback

Go Do's!



Go Do's!

- Understand how PSSO works and you meet the pre-reqs
- Deploy Secure Enclave whenever possible
- Align your password management policy
- Understand hardware-bound device identity impacts, deploy Chrome extension if needed
- Prepare to enforce with Conditional Access Authentication Strengths
- Continue to provide feedback to Microsoft, Apple, and your MDM provider
 - We try to watch the #Microsoft-entra channel on MacAdmins Slack and Microsoft Mac Admins on LinkedIn (aka.ms/MacAdmins)



Q&A

<https://bit.ly/psumac-2024-39>

