

Entra ID --- macOS Platform SSO



Agenda

- **macOS and Identity – how did we get here**
- What problems still exist for identity on macOS
- What is Platform SSO and how does it work with Entra ID
- Deployment Guidance
- Troubleshooting
- Go-Dos
- Q&A

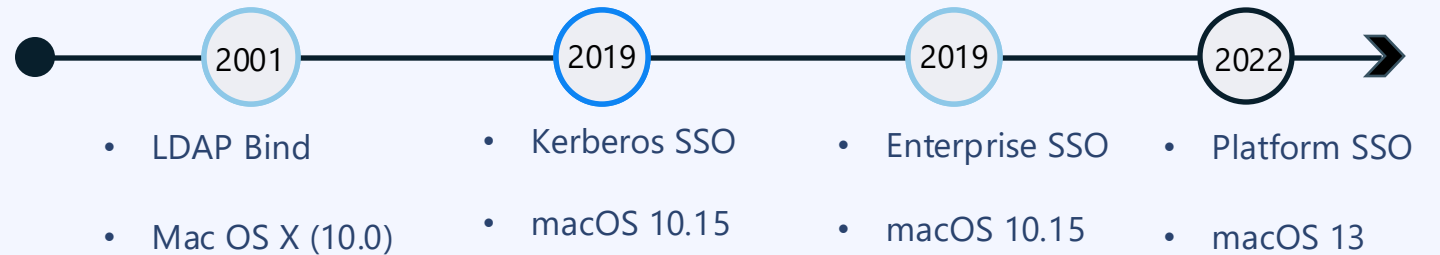


History of enterprise identity options on macOS

Native options from Apple, all still exist and are supported

3rd party options also exist that can do password sync with an IDP or render web browsers on the Mac login screen:

- Jamf Connect
- Xcreds
- Etc.



Agenda

- macOS and Identity – how did we get here
- **What problems still exist for identity on macOS**
- What is Platform SSO and how does it work with Entra ID
- Deployment Guidance
- Troubleshooting
- Go-Dos
- Q&A



Where are the gaps?

Nothing outlined so far represents a great way to manage Mac local identities, credentials, or provide SSO everywhere:

- Local creds must be managed locally, via on-premises AD, MDM, or via 3rd party tools
- Multiple tools used for SSO to on-premises and cloud resources
- On-premises dependencies cause bad user experiences
- No modern phishing-resistant options

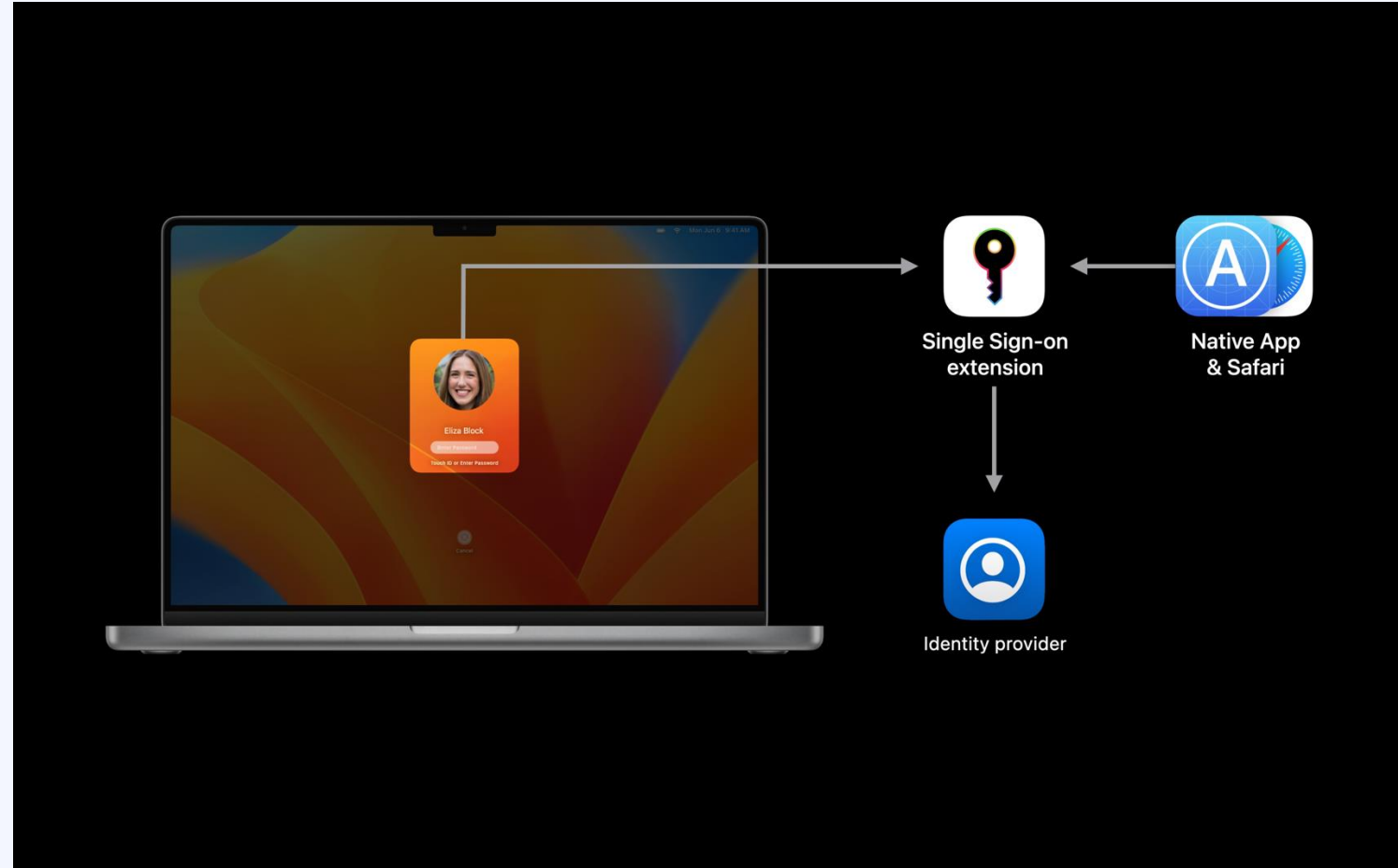
Agenda

- macOS and Identity – how did we get here
- What problems still exist for identity on macOS
- **What is Platform SSO and how does it work with Entra ID**
- Deployment Guidance
- Troubleshooting
- Go-Dos
- Q&A



Platform SSO

- Framework built by Apple into macOS
- Local credential managed by combo of MDM and plugin created by an Identity Provider
- Replacement for binding to directory services
- Multiple Authentication Methods supported by Apple, up to IDPs to support them too

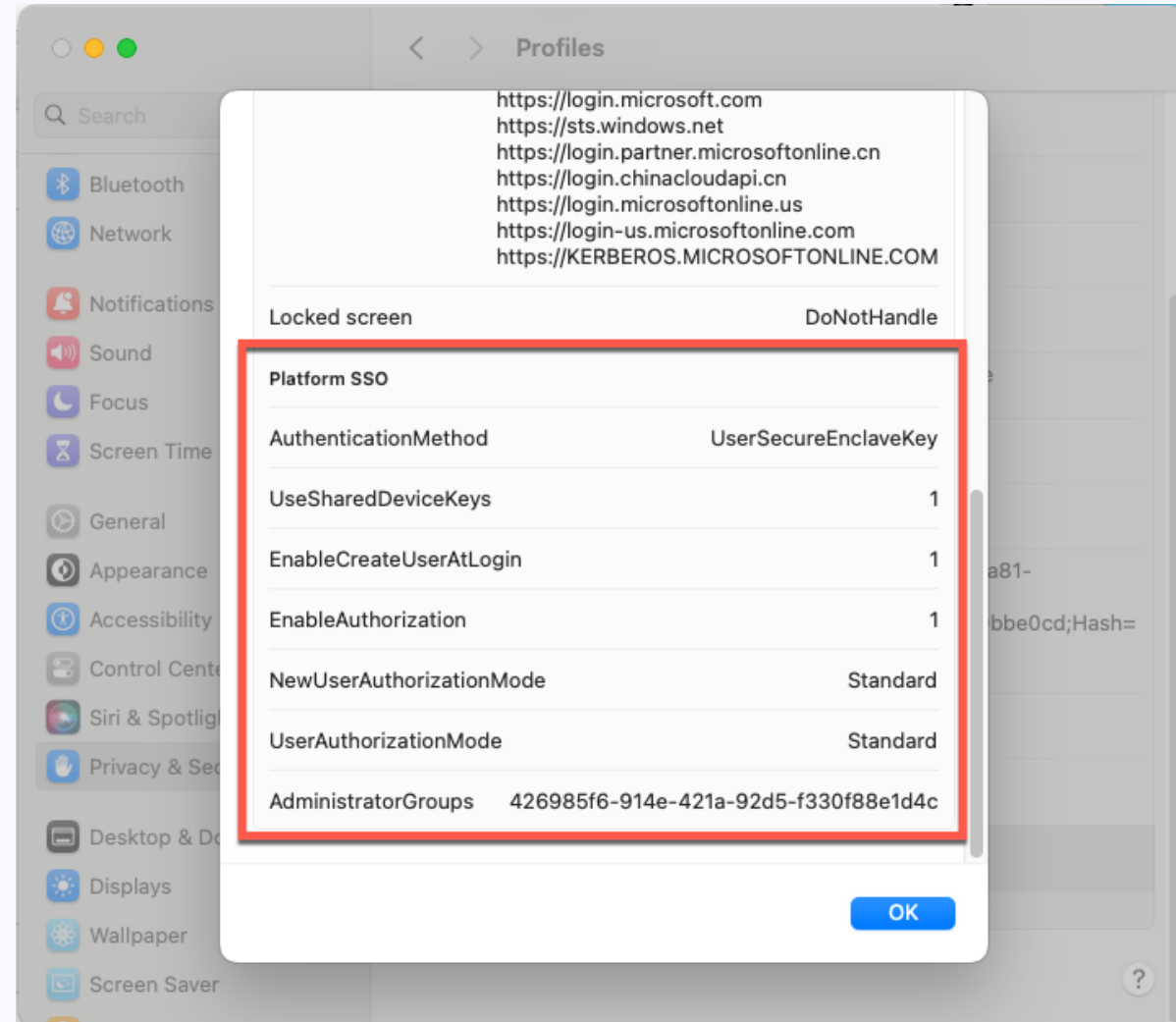


3 Authentication Methods Support by Platform SSO

	Good: Password	Better: SmartCard	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	✗	✗	✓

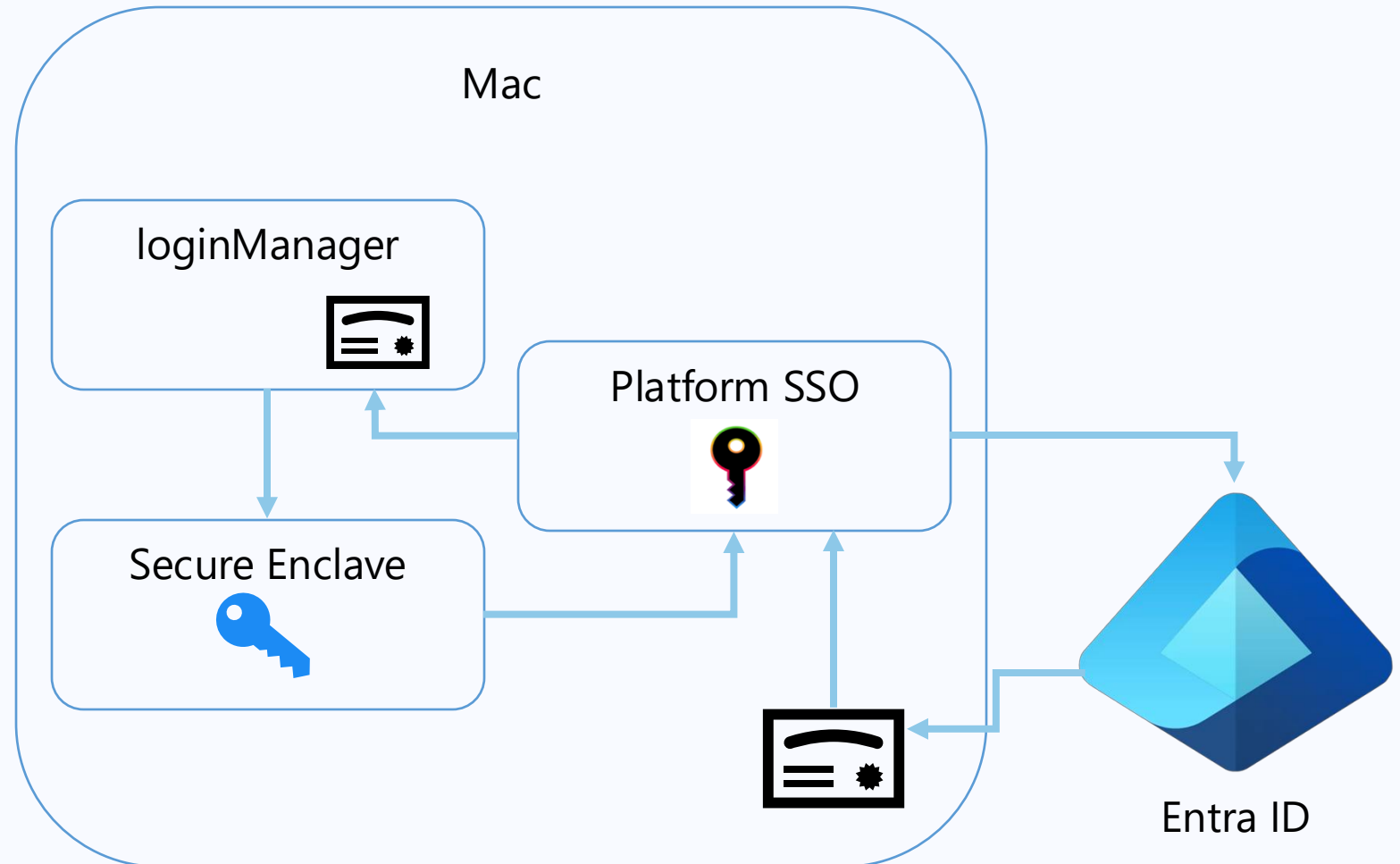
How does the Entra ID implementation of PSSO work?

1. Install the Intune Company Portal app
2. MDM policy pushed down



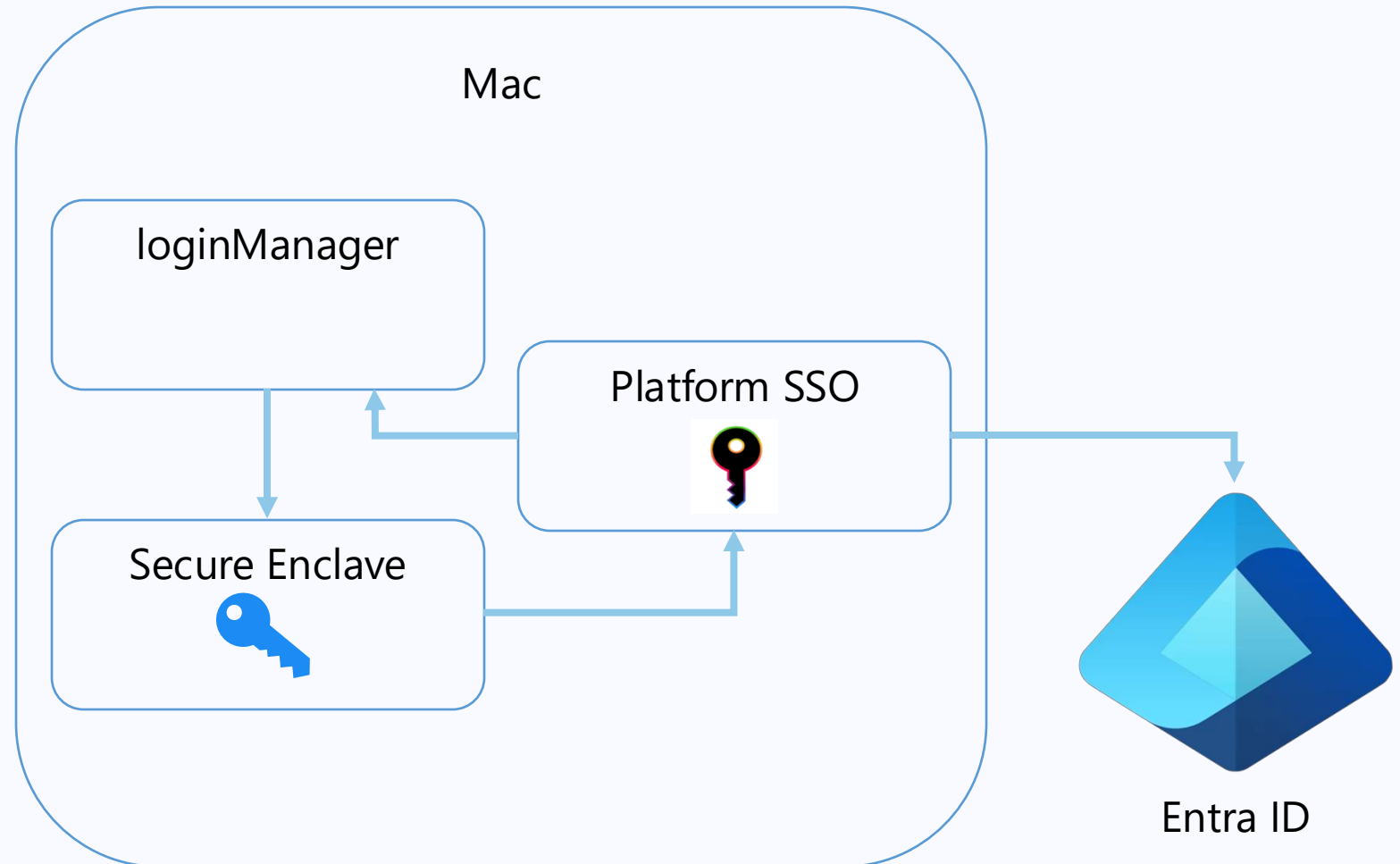
How does the Entra ID implementation of PSSO work?

1. Install the Intune Company Portal app
2. MDM policy pushed down
3. Device Registration – secure device artifacts stored in the secure enclave and accessible only via the SSO Extension



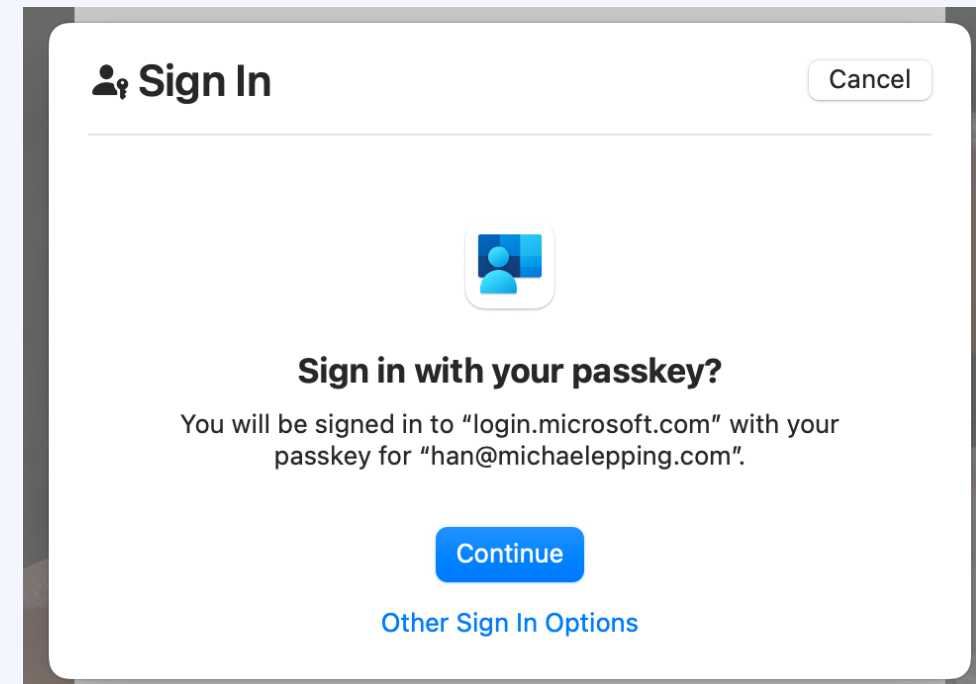
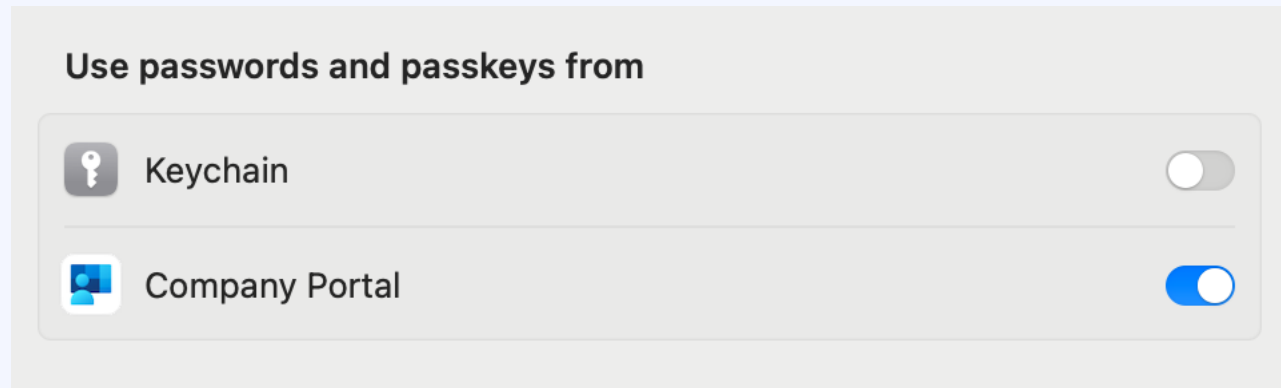
How does the Entra ID implementation of PSSO work?

1. Install the Intune Company Portal app
2. MDM policy pushed down
3. Device Registration – secure, artifacts stored in the secure enclave and accessible only via the SSO Extension
4. User Registration – SE method results in cloud credential equivalent to WHFB key. Also useable as a passkey for re-auth scenarios.



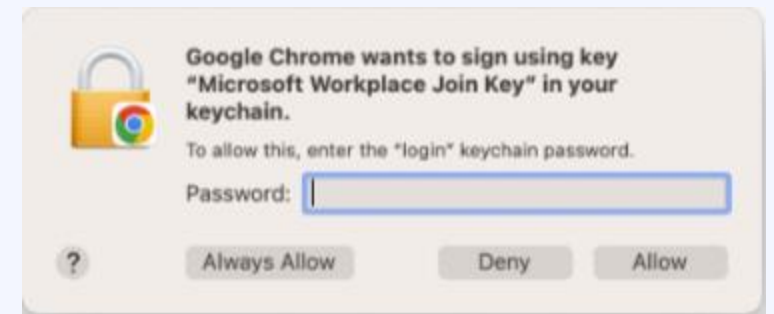
Platform SSO Details

- SSO with Entra ID is based off Primary Refresh Tokens, no changes there – refreshed every 4 hours
- Passkey flow allows users to do phishing-resistant interactive authentication with Entra ID
 - Smartcard also an option for phishing-resistance, but requires much more hardware and infrastructure



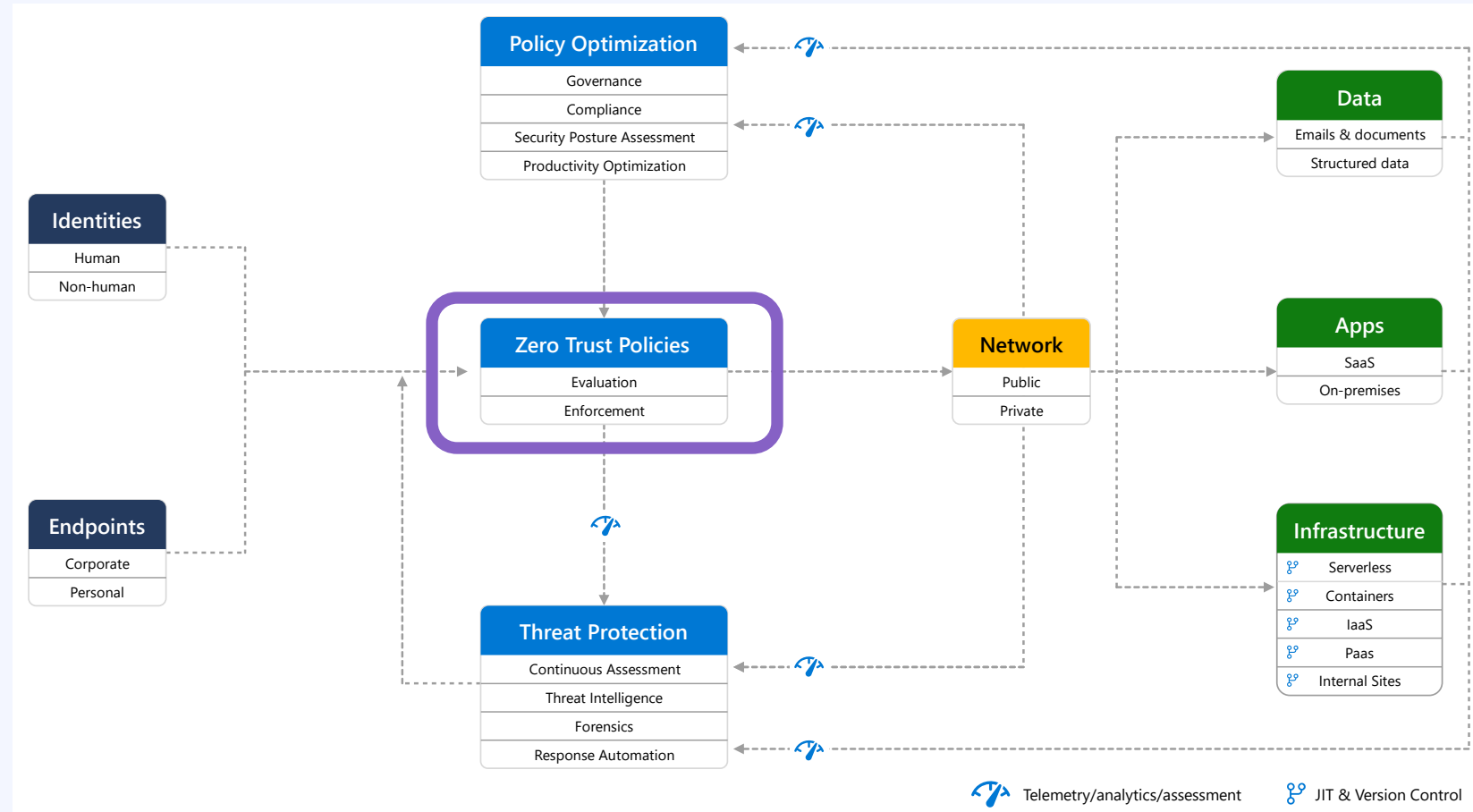
Platform SSO Details

- SSO with Entra ID is based off Primary Refresh Tokens, no changes there – refreshed every 4 hours
- Passkey flow allows users to do phishing-resistant interactive authentication with Entra ID
 - Smartcard also an option for phishing-resistance, but requires much more hardware and infrastructure
- Device cert can only be used by the SSO Extension – apps that don't talk to the SSO Extension can no longer satisfy device-based Conditional Access policies
 - Chrome is the big one, we're making a browser extension to help Chrome talk to the SSO Extension
 - Chrome extension will bring SSO to Chrome for the first time!
 - Let us know about other apps where you run into the same issue



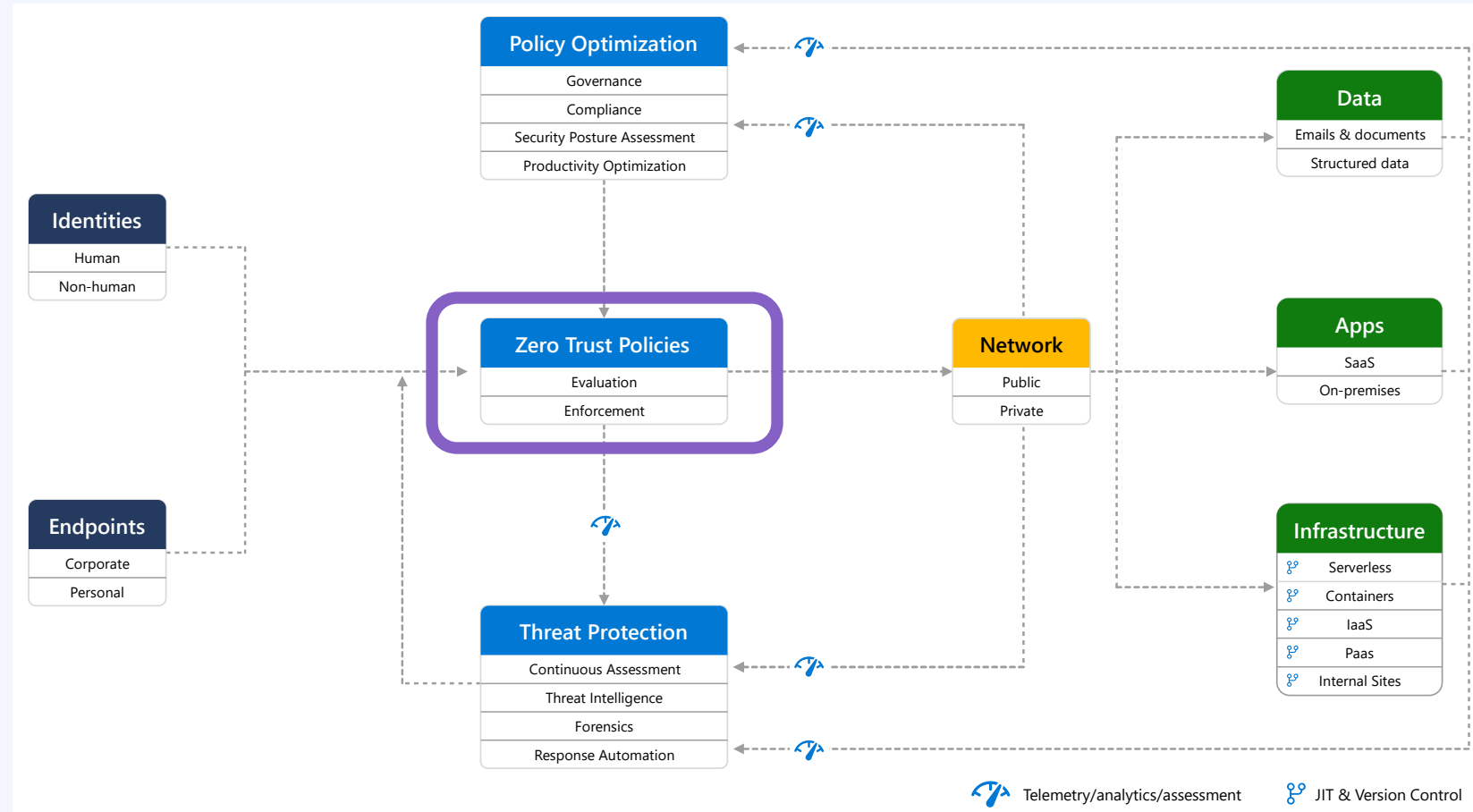
Where is MFA Evaluated and Enforced?

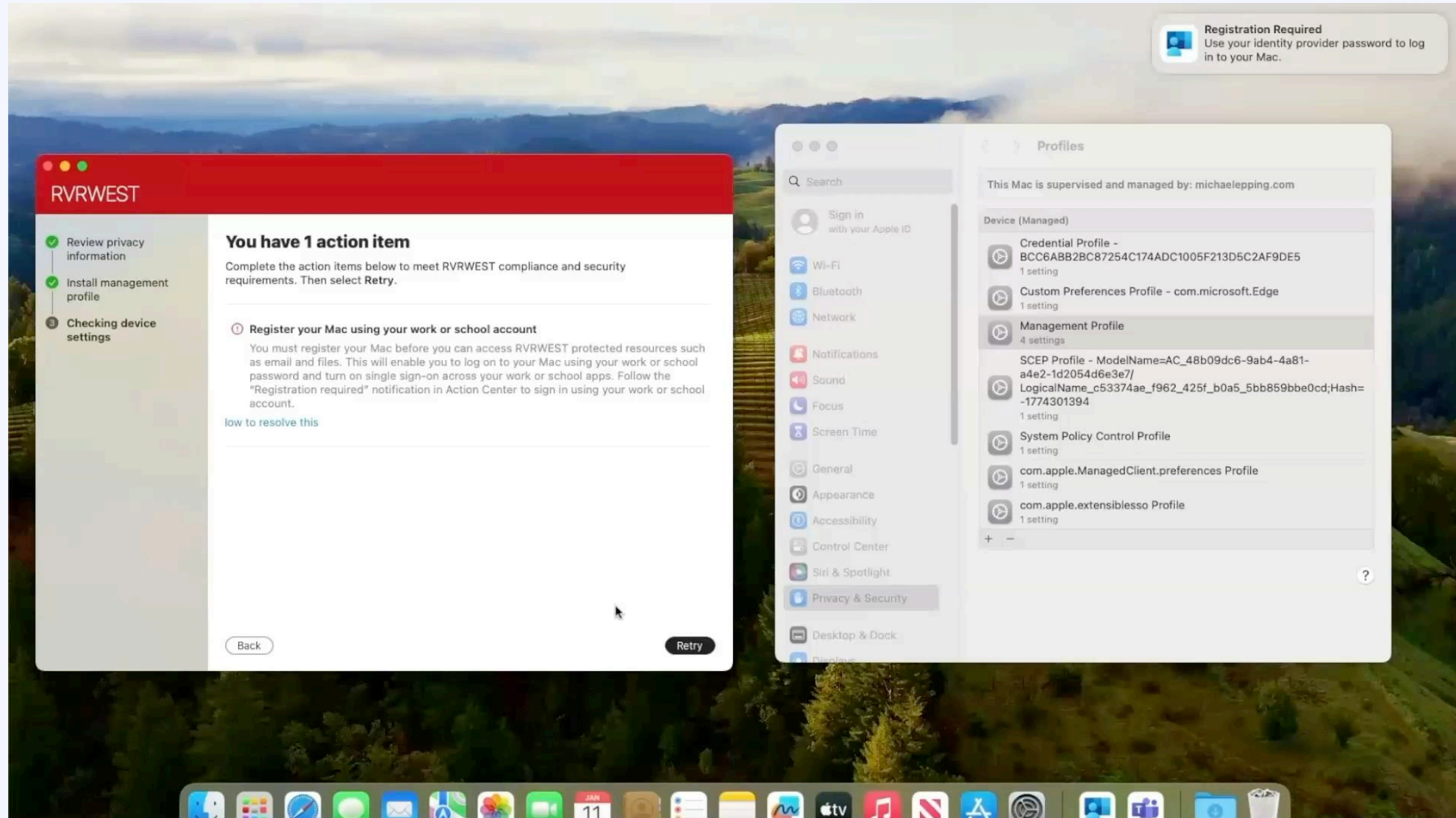
- MFA is about protecting access to resources
 - Cloud Apps
 - APIs
 - Sensitive Data
 - Networks
- Enforced at a Policy Decision Point (see NIST SP 800-207)



Where is MFA Evaluated and Enforced?

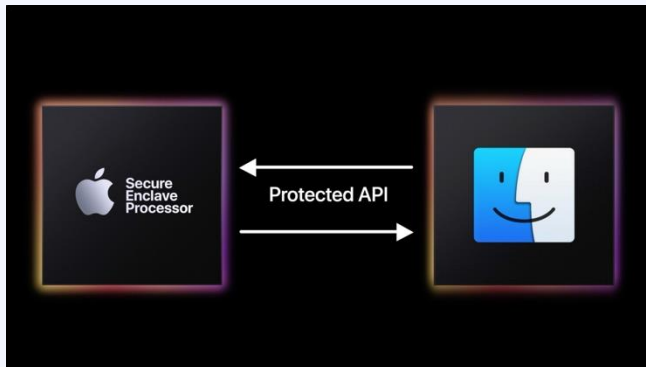
- Enforced at a Policy Decision Point (see NIST SP 800-207)
 - Just like WHFB, Secure Enclave auth to Entra ID always checks:
 - Can the credential only be used from the device it was issued to? (Something You Have)
 - And requires one of these two:
 - Did the user have to provide a memorized secret PIN/Passcode? (Something You Know)
 - Did the user have to provide a biometric? (Something You Are)
 - If all requirements are satisfied then the Policy Decision Point views that auth as "strong auth" / multifactor



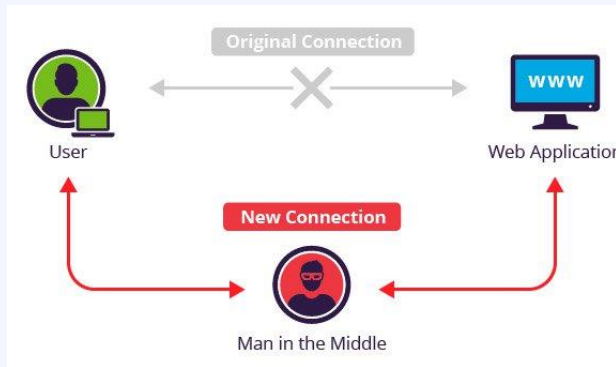


Why are PINs better than Passwords?

PINs are tied to a device –
useless without the device



PINs are local to the device –
not transmitted to a server



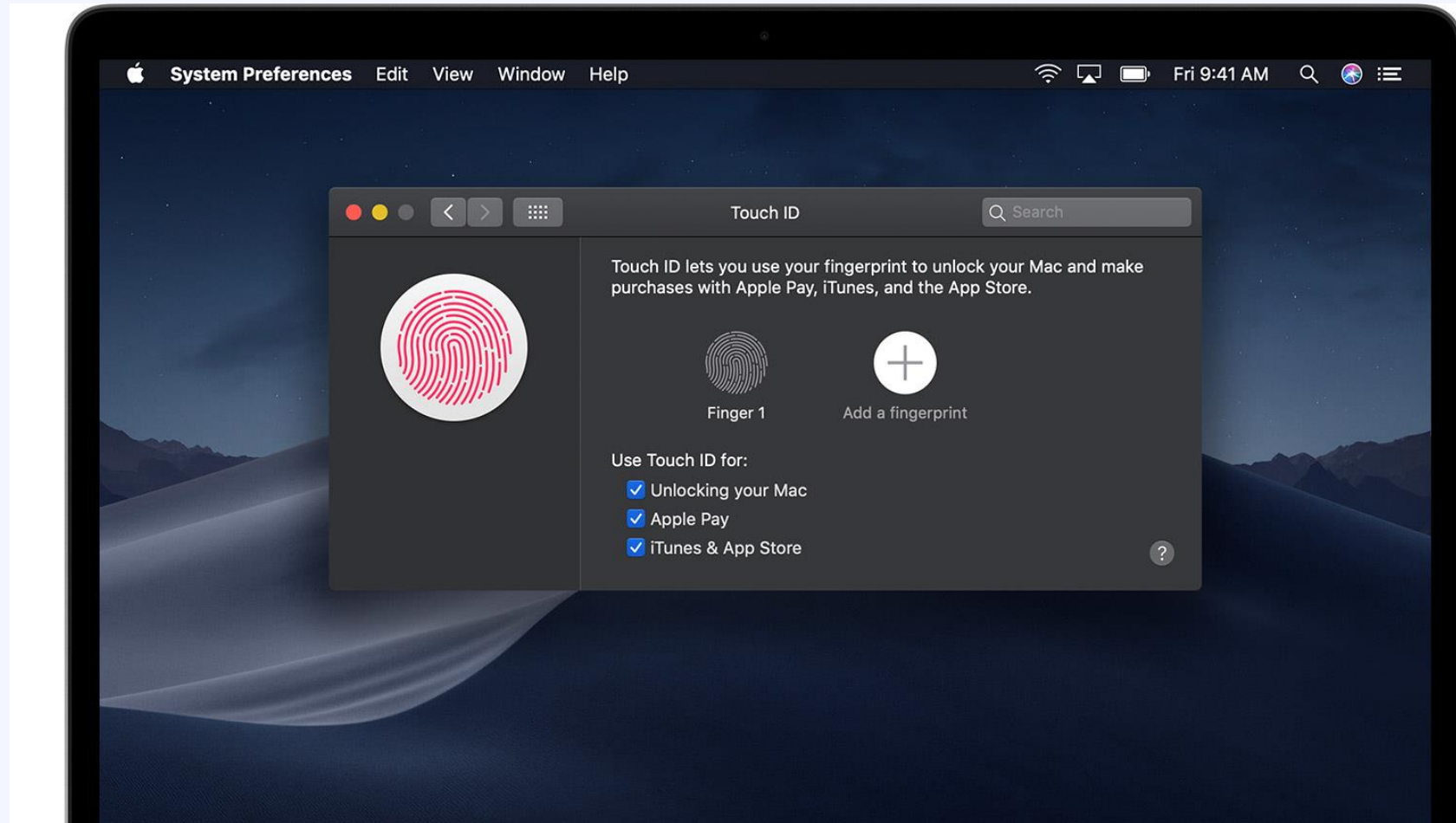
PINs are backed by hardware



Secure Enclave and MFA

When you deploy the Secure Enclave PSSO option you are setting up a multi-factor authenticator for your users when authenticating to Entra ID:

- PIN/Local Passcode =
Something you have +
something you know
- TouchID = Something you have
+ something you are



Agenda

- macOS and Identity – how did we get here
- What problems still exist for identity on macOS
- What is Platform SSO and how does it work with Entra ID
- **Deployment Guidance**
- Troubleshooting
- Go-Dos
- Q&A



Deployment Guidance

1. Update to macOS Sonoma

Sonoma vs. Ventura

Feature	Ventura (macOS 13)	Sonoma (macOS 14)
Secure Enclave	✓	✓
Password Sync	✓	✓
Federated IDP Support	✓	✓
Smartcards	✗	✓
User enrollment and registration UX in System Settings	✗	✓
Local Account Creation using IDP	✗	✓
Admin authentication without local user account	✗	✓
Admin Groups	✗	✓
Authorization Groups	✗	✓
Kerberos SSO	✗	✓

Deployment Guidance

1. Update to macOS Sonoma
2. Deploy Platform SSO via MDM with recommended config options

Recommended MDM Settings

Recommended Configuration:

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

Sample file: <https://aka.ms/psso-sample>

```
12 <key>PayloadContent</key>
13 <dict>
14   <key>ExtensionData</key>
15   <dict>
16     <key>AppPrefixAllowList</key>
17     <string>com.microsoft.,com.apple.,com.jamf.,com.jamfsoftware.</string>
18     <key>browser_sso_interaction_enabled</key>
19     <integer>1</integer>
20     <key>disable_explicit_app_prompt</key>
21     <integer>1</integer>
22   </dict>
23   <key>ExtensionIdentifier</key>
24   <string>com.microsoft.CompanyPortalMac.ssoextension</string>
25   <key>PlatformSSO</key>
26   <dict>
27     <key>AuthenticationMethod</key>
28     <string>UserSecureEnclaveKey</string>
29     <key>EnableAuthorization</key>
30     <true/>
31     <key>EnableCreateUserAtLogin</key>
32     <true/>
33     <key>NewUserAuthorizationMode</key>
34     <string>Admin</string>
35     <key>TokenToUserMapping</key>
36     <dict>
37       <key>AccountName</key>
38       <string>preferred_username</string>
39       <key>FullName</key>
40       <string>name</string>
41     </dict>
42     <key>UseSharedDeviceKeys</key>
43     <true/>
44     <key>UserAuthorizationMode</key>
45     <string>Admin</string>
46   </dict>
47   <key>RegistrationToken</key>
48   <string>*****</string>
49   <key>ScreenLockedBehavior</key>
50   <string>DoNotHandle</string>
51   <key>TeamIdentifier</key>
52   <string>UBF8T346G9</string>
53   <key>Type</key>
54   <string>Redirect</string>
55   <key>URLs</key>
56   <array>
57     <string>https://login.microsoftonline.com</string>
58     <string>https://login.microsoft.com</string>
59     <string>https://sts.windows.net</string>
60     <string>https://login.partner.microsoftonline.cn</string>
61     <string>https://login.chinacloudapi.cn</string>
62     <string>https://login.microsoftonline.us</string>
63     <string>https://login-us.microsoftonline.com</string>
64   </array>
65 </dict>
66 <key>PayloadDisplayName</key>
67 <string>Configuration Profile</string>
68 <key>PayloadIdentifier</key>
69 <string>com.apple.extensiblesso.266d3a49-3785-4ede-afc6-127d0ab501fc.payload</string>
70 <key>PayloadOrganization</key>
71 <string>Woodgrove</string>
72 <key>PayloadType</key>
73 <string>com.apple.extensiblesso</string>
74 <key>PayloadUUID</key>
75 <string>1c8b424e-c8a7-9fa7-6c4d5580273b</string>
76 <key>PayloadVersion</key>
77 <integer>1</integer>
78 </dict>
```

Recommended MDM Settings

Recommended Configuration:

- Enable Secure Enclave-based passwordless
- Shared Device Keys is pre-req for many other features
- Enable Shared Device Keys right away, changing it later requires user re-registration
- Push same profile to both Ventura and Sonoma

Key	Value
Authentication Method (Deprecated)	UserSecureEnclaveKey
Authentication Method	UserSecureEnclaveKey
Enable Authorization	Enabled
Enable Create User At Login	Enabled
New User Authorization Mode	User/Admin
Use Shared Device Keys	Enabled
User Authorization Mode	User/Admin
Registration Token	{{DEVICEREGISTRATION}}
Authorization Groups	Multiple Options – Coming Later

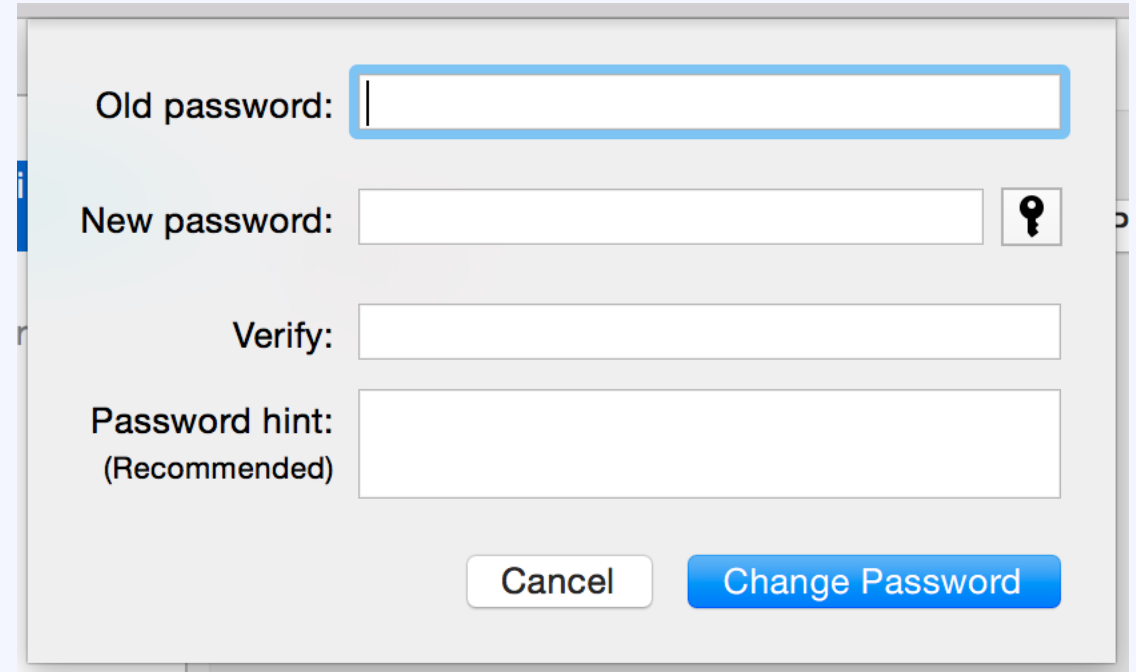
Deployment Guidance

1. Update to macOS Sonoma
2. Deploy Platform SSO via MDM with recommended config options
3. Update MDM password policy profiles

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

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

Use a Trusted Platform Module (TPM): ⓘ	<div><div>Required</div><div>Preferred</div></div>
Minimum PIN length: * ⓘ	<div>4 ✓</div>
Maximum PIN length: * ⓘ	<div>127 ✓</div>
Lowercase letters in PIN: ⓘ	<div>Allowed ▼</div>
Uppercase letters in PIN: ⓘ	<div>Allowed ▼</div>
Special characters in PIN: ⓘ	<div>Allowed ▼</div>
PIN expiration (days): ⓘ	<div>Never ▼</div>
Remember PIN history: ⓘ	<div>No ▼</div>
Allow biometric authentication: ⓘ	<div><div>Yes</div><div>No</div></div>

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

Use a Trusted Platform Module (TPM): ⓘ	<div><div>Required</div><div>Preferred</div></div>
Minimum PIN length: * ⓘ	<div>6</div>
Maximum PIN length: * ⓘ	<div>127</div>
Lowercase letters in PIN: ⓘ	<div>Allowed</div>
Uppercase letters in PIN: ⓘ	<div>Allowed</div>
Special characters in PIN: ⓘ	<div>Allowed</div>
PIN expiration (days): ⓘ	<div>Never</div>
Remember PIN history: ⓘ	<div>No</div>
Allow biometric authentication: ⓘ	<div><div>Yes</div><div>No</div></div>



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 * ⓘ	<input type="text" value="2"/> ✓	⊖
Require Alphanumeric Passcode ⓘ	<input checked="" type="checkbox"/> True	⊖
PIN History * ⓘ	<input type="text" value="5"/> ✓	⊖
Max PIN Age In Days * ⓘ	<input type="text" value="90"/> ✓	⊖
↻		
Min Length * ⓘ	<input type="text" value="8"/> ✓	⊖
Force PIN ⓘ	<input checked="" type="checkbox"/> True	⊖
Allow Simple Passcode ⓘ	<input type="checkbox"/> False	⊖

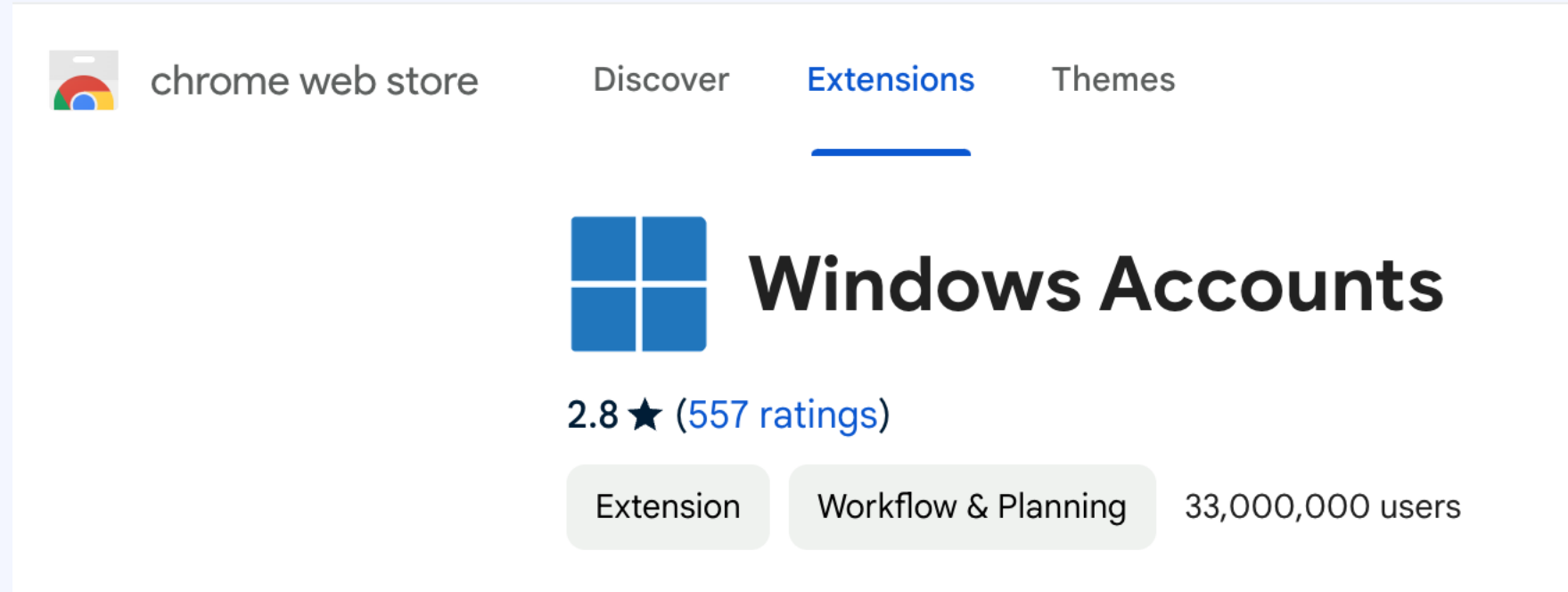
Deployment Guidance

1. Update to macOS Sonoma
2. Deploy Platform SSO via MDM with recommended config options
3. Update MDM password policy configuration/compliance profiles
4. Deploy the Chrome extension

Chrome Extension


Two ways for apps to do device-based Conditional Access:

1. Use the Microsoft SSO broker
2. ~~Access the device cert in the keychain directly~~
 - This one is going away with PSSO!
 - The device cert will now be bound to the Secure Enclave



The screenshot shows the Chrome Web Store interface. At the top, there's a navigation bar with the Chrome Web Store logo, 'Discover', 'Extensions' (which is underlined), and 'Themes'. Below this, the 'Windows Accounts' extension is featured. It has a blue square icon with a white 'W'. The title 'Windows Accounts' is in large, bold black text. Below the title, it shows a rating of '2.8 ★ (557 ratings)'. At the bottom of the extension card, there are two tabs: 'Extension' and 'Workflow & Planning', with '33,000,000 users' listed to the right.

chrome web store Discover **Extensions** Themes

 **Windows Accounts**

2.8 ★ (557 ratings)

Extension Workflow & Planning 33,000,000 users

Deployment Guidance

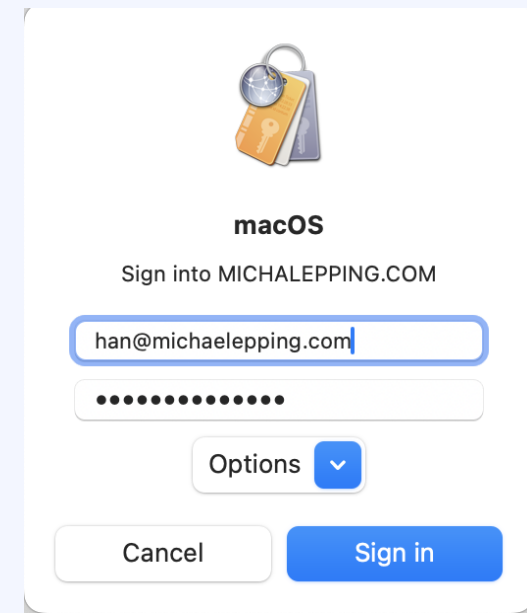
1. Update to macOS Sonoma
2. Deploy Platform SSO via MDM with recommended config options
3. Update MDM password policy configuration/compliance profiles
4. Deploy the Chrome extension
5. Deploy Kerberos SSO using Platform SSO

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/>
```

```
<key>Hosts</key>
<array>
    <string>michaelepping.com</string>
    <string>*.michaelepping.com</string>
</array>
```



Agenda

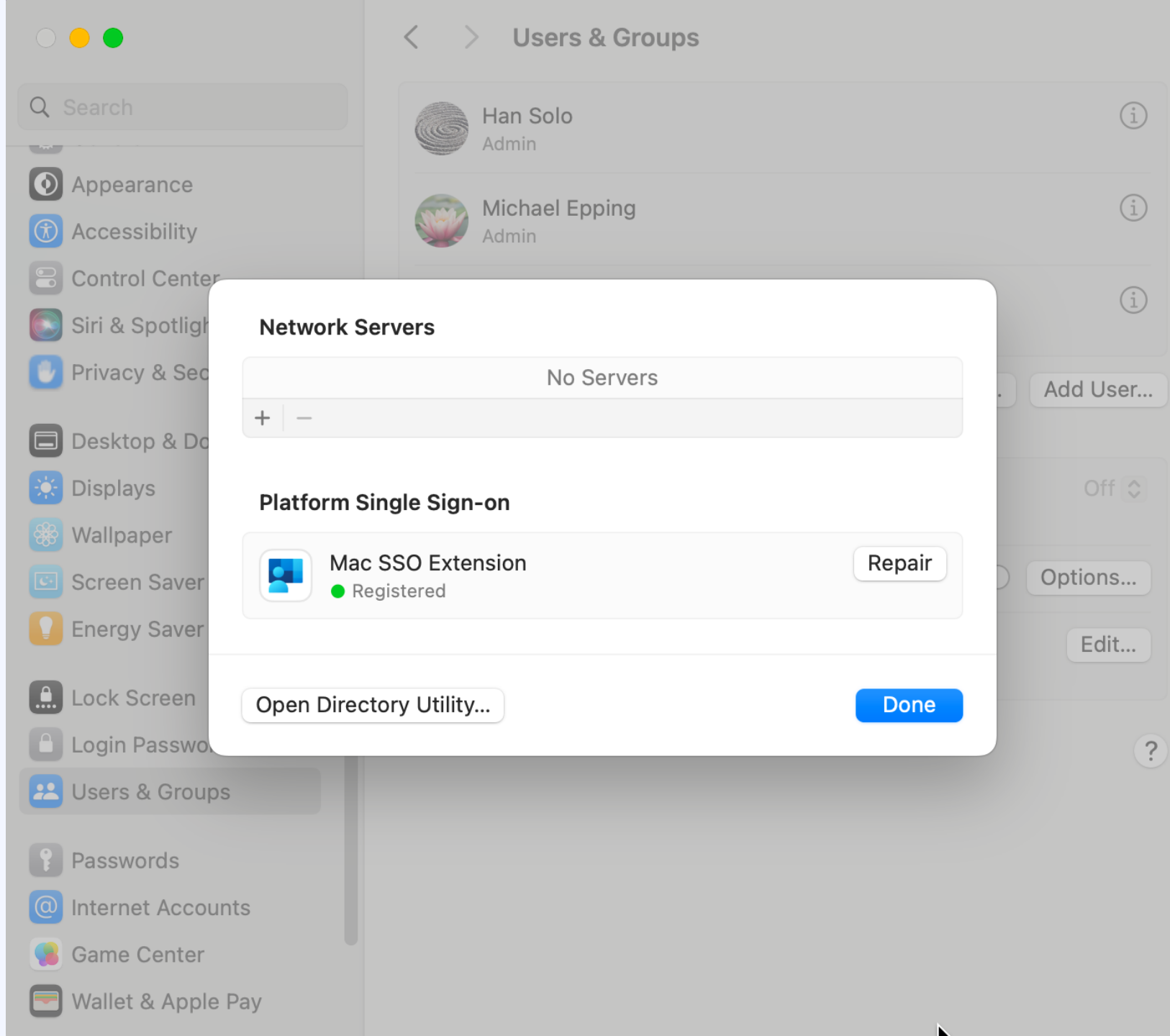
- macOS and Identity – how did we get here
- What problems still exist for identity on macOS
- What is Platform SSO and how does it work with Entra ID
- Deployment Guidance
- **Troubleshooting**
- Go-Dos
- Q&A



Validate PSSO and User Status

On Sonoma:

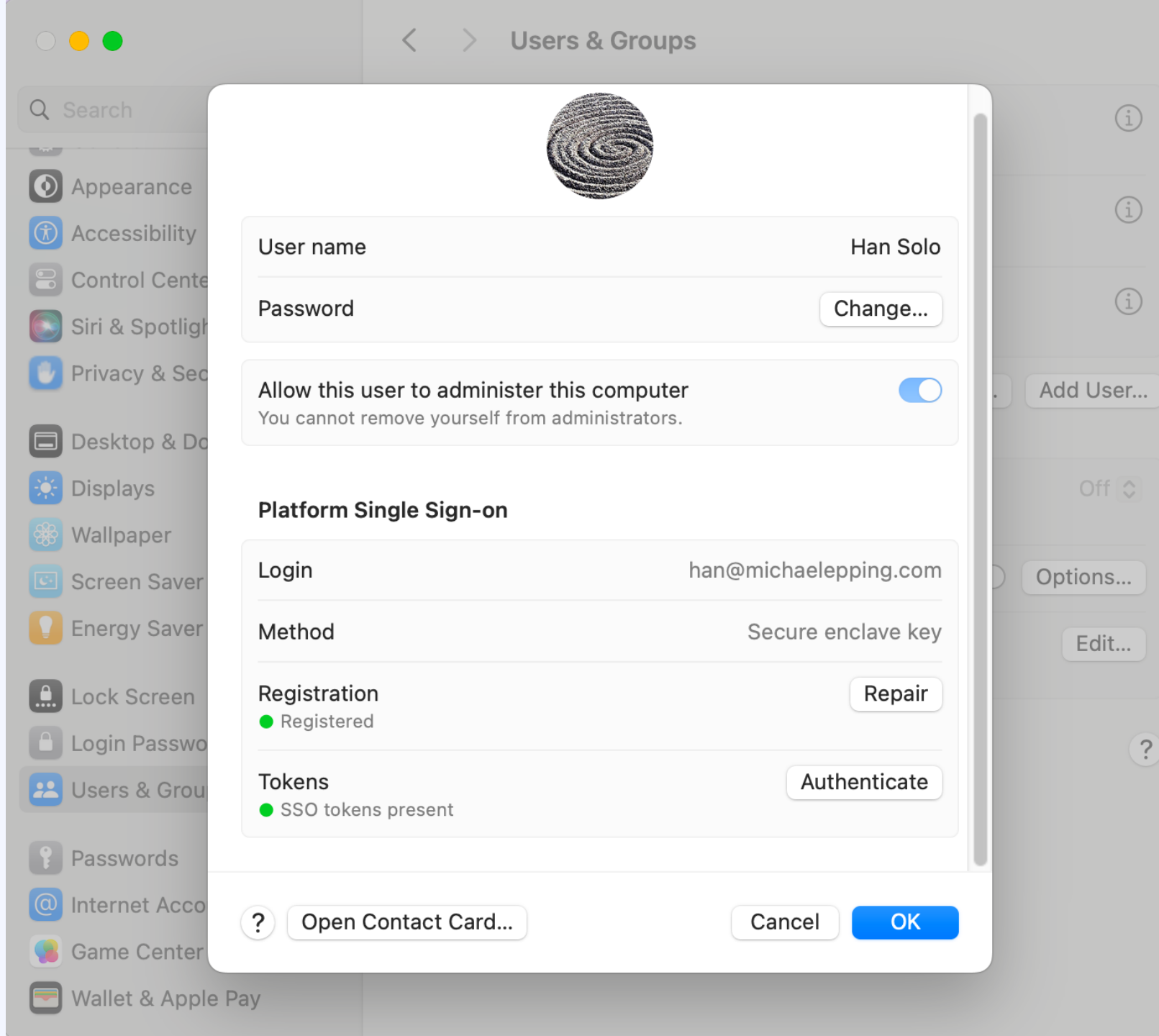
- Go to System Settings -> Users & Groups
- Check Network account server



Validate PSSO and User Status

On Sonoma:

- Go to System Settings -> Users & Groups
- Check Network account server
- Check user profile PSSO status



Validate PSSO and User Status

On Ventura or Sonoma:

- Check the status via CLI by running:
 - `app-sso platform -s`

```
han — -zsh — 97x41

  "clientNameKeyName" : "cn",
  "encryptionKeyTypeKeyName" : "keyType",
  "messageBufferKeyName" : "messageBuffer",
  "realmKeyName" : "realm",
  "serviceNameKeyName" : "sn",
  "sessionKeyKeyName" : "clientKey",
  "ticketKeyPath" : "tgt_cloud"
}
],
"nonceResponseKeypath" : "Nonce",
"previousRefreshTokenClaimName" : "previous_refresh_token",
"refreshEndpointURL" : "https://login.microsoftonline.com/0348ff6f-154e-41c2-b1b7-60743cb165dc/oauth2/v2.0/token",
"serverNonceClaimName" : "request_nonce",
"tokenEndpointURL" : "https://login.microsoftonline.com/0348ff6f-154e-41c2-b1b7-60743cb165dc/oauth2/v2.0/token",
"uniqueIdentifierClaimName" : "oid"
}

User Configuration:
{
  "_sepKeyData" : "dFWsbkr8vWJGysP2qppg6xdfejhD2loBpa9g1905lZk=",
  "created" : "2024-03-06T18:22:54Z",
  "lastLoginDate" : "2024-02-27T18:31:50Z",
  "loginType" : "POLoginTypeUserSecureEnclaveKey (2)",
  "state" : "POUserStateNormal (0)",
  "uniqueIdentifier" : "DBDED2F5-5DB1-4B0A-9900-749A...",
  "userLoginConfiguration" : {
    "created" : "2024-03-06T18:22:54Z",
    "loginUserName" : "***@michaelepping.com"
  },
  "version" : 1
}

SSO Tokens:
Received:
2024-03-06T18:13:47Z
Expiration:
2024-03-20T18:13:46Z (Not Expired)

han@Hans-Virtual-Machine ~ %
```

Validate PSSO and User Status

On Ventura or Sonoma:

- Check particular properties:
 - SSO Tokens Expiration
 - extensionIdentifier
 - Device -> Registration Completed
 - kerberosTicketMappings (if using PSSO for Kerberos)

```
SSO Tokens:  
Received:  
2024-03-06T18:13:47Z  
Expiration:  
2024-03-20T18:13:46Z (Not Expired)
```

```
"whshjlokfJTYg1yxMED9yqDB12EB1SSnY2rUwvEJYxvmy8Q01sSAytnsu1th2mby3qY",  
"extensionIdentifier" : "com.microsoft.CompanyPortalMac.ssoextension",  
"loginFrequency" : 44800
```

```
"protocolVersion" : 0,  
"registrationCompleted" : true,  
"sdkVersionString" : 14
```

```
},  
"kerberosTicketMappings" : [  
  {  
    "clientNameKeyName" : "cn",  
    "encryptionKeyTypeKeyName" : "keyType",  
    "messageBufferKeyName" : "messageBuffer",  
    "realmKeyName" : "realm",  
    "serviceNameKeyName" : "sn",  
    "sessionKeyKeyName" : "clientKey",  
    "ticketKeyPath" : "tgt_ad"  
  },  
  {  
    "clientNameKeyName" : "cn",  
    "encryptionKeyTypeKeyName" : "keyType",  
    "messageBufferKeyName" : "messageBuffer",  
    "realmKeyName" : "realm",  
    "serviceNameKeyName" : "sn",  
    "sessionKeyKeyName" : "clientKey",  
    "ticketKeyPath" : "tgt_cloud"  
  }  
],
```


Microsoft SSO Extension Troubleshooting Guide

- For SSO-related issues, use our Troubleshooting Guide:
 - aka.ms/AppleSSOTSG
 - Helps with complex troubleshooting, like:
 - Gathering logs
 - Validating TLS inspection settings
 - Checking configuration parameters
 - Understanding how the SSO Extension works
- Added instructions for removing PSSO

Agenda

- macOS and Identity – how did we get here
- What problems still exist for identity on macOS
- What is Platform SSO and how does it work with Entra ID
- Deployment Guidance
- Troubleshooting
- **Go-Dos**
- Q&A



Go-Dos

1. Strengthen your environment

- Deploy phishing-resistant credentials
- Enforce phishing-resistant auth methods with Conditional Access Authentication Strengths

2. Get your enterprise ecosystem integrated

- Get apps integrated with Entra ID
- Use governance tools to govern access to apps integrated with Entra ID
- Deploy the Chrome browser extension
- Integrate Apple Business Manager with Entra ID

Go-Dos

4. Talk to your vendors

- Some feature requests should go to Apple, not Microsoft. File feedbacks/radars with Apple
- Get desktop apps integrated with the SSO brokers – might require you to talk to the app vendor or your developers

5. Don't forget about iOS!

- Deploy phishing resistant creds (FIDO keys, Smartcards, Passkeys soon)
- Deploy the Microsoft Enterprise SSO Extension to your iOS devices

6. Deploy all the best features for your Mac users, they'll appreciate it:

- Automated Device Enrollment
- Secure Enclave phishing-resistant auth with Platform SSO
- SSO enabled everywhere using Entra ID Platform SSO and Kerberos
- Device Compliance health checking and Conditional Access policies

Agenda

- macOS and Identity – how did we get here
- What problems still exist for identity on macOS
- What is Platform SSO and how does it work with Entra ID
- Deployment Guidance
- Troubleshooting
- Go-Dos
- **Q&A**



Pre-Staged Questions

- Using MDM to deploy the profile, is the first user on setup assistant a PSSO user?
- What happens if the user account is disabled in Entra ID?
- How does MFA work when the computer is offline?
- Does it work with FileVault? What happens when the user's password changes?
- Do I need an Entra ID App Registration?
- Do I need a special O365 configuration for it to work with SSO?

Pre-Staged Questions

- How does it work with Jamf Connect?
- How do I configure it with Jamf Pro?
- Why and how did you come out with multiple options? What were those known challenges which brought introduction to these options?
- Is there any migration workflow from migrating from initial Jamf Pro Device Compliance configuration to Platform SSO ?

Thank You!

