Microsoft

Delighting your users with a seamless and secure Microsoft 365 experience

Merill Fernando
Principal Product Manager, Microsoft Security

Quick show of hands…

How many of you use Microsoft 365 (Outlook or Teams or OneDrive)?

How many of you use Azure Active Directory?

How many of you have heard of Enterprise SSO?

How many of you have deployed Enterprise SSO?

Agenda

What is Azure Active Directory?

Prompting…why is it bad?

Enterprise Single Sign On (SSO) - How does it work?

Deploying Enterprise SSO

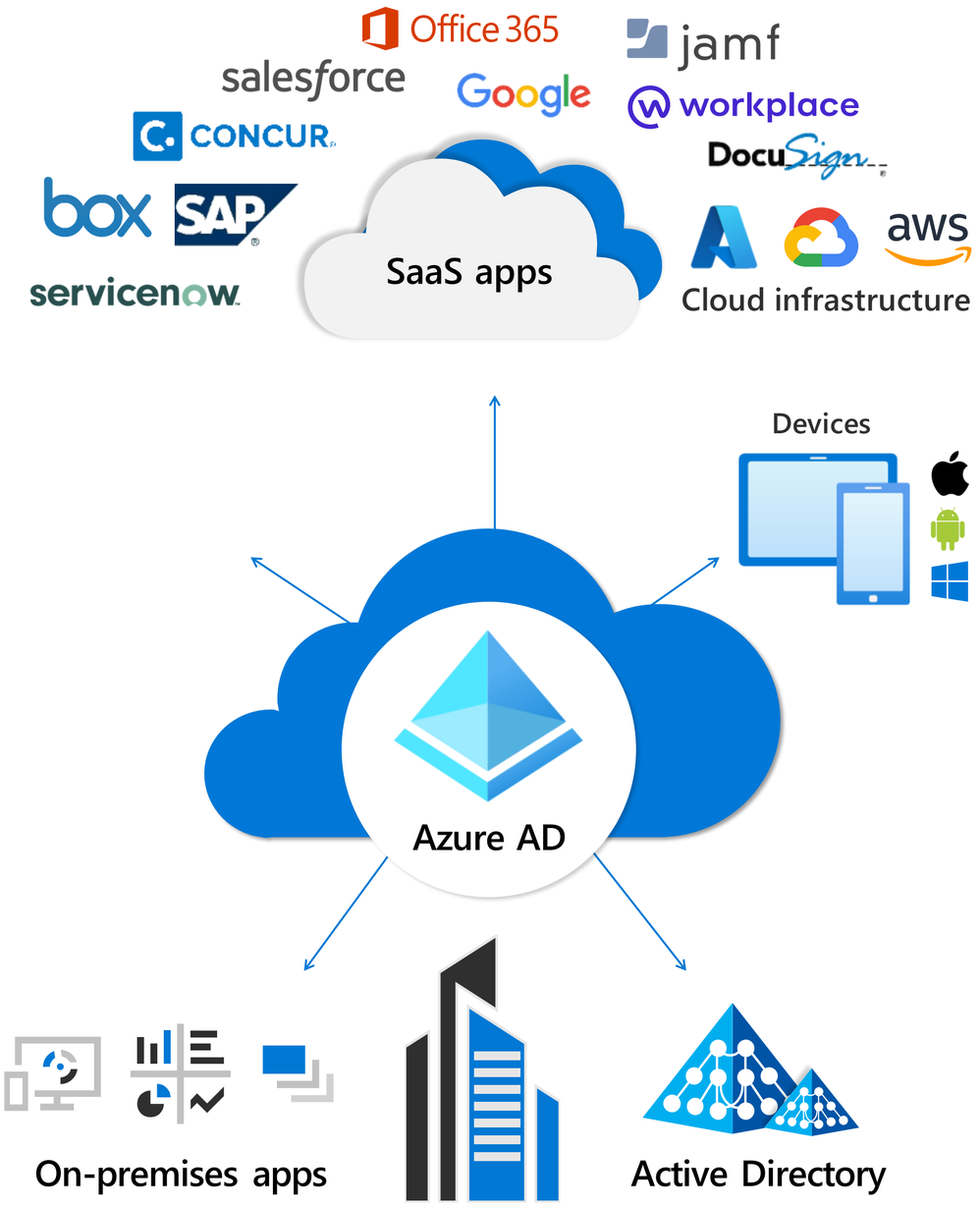
Troubleshooting Enterprise SSO

Azure Active Directory

Azure Active Directory is a cloud based IDaaS solution, not an IDP for just Office 365/Azure

Resources are moving to the cloud, devices are proliferating, users are outside the office

Identity needs to be the new control plane, rather than the network perimeter



Agenda

What is Azure AD?

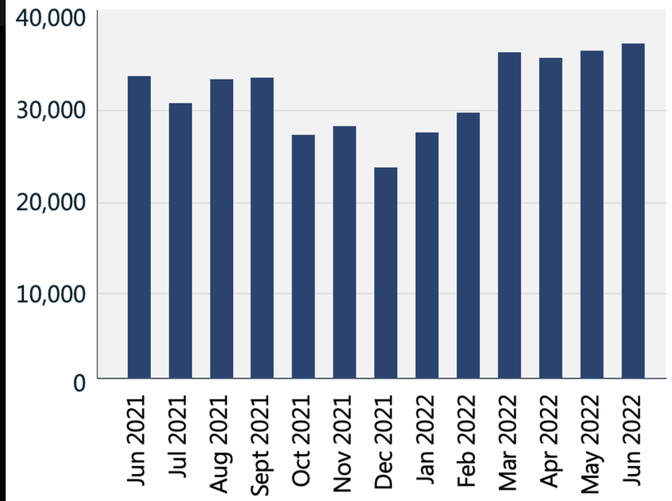
Prompting…why is it bad?

Enterprise Single Sign On (SSO) - How does it work?

Deploying Enterprise SSO

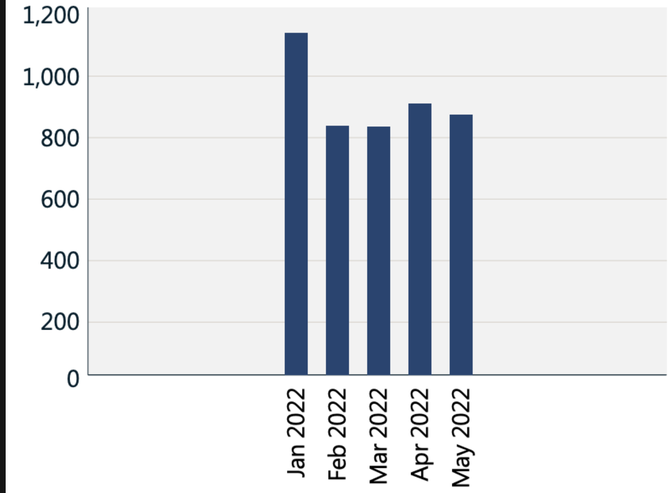
Troubleshooting Enterprise SSO

Estimated instances of MFA fatigue attacks



Source: Azure AD Identity Protection.

Detected instances of phishing followed by man-in-the-middle attacks



Source: Microsoft Defender for Cloud Apps.

Recent phishing attacks that made the news

CyberSecurity Connect

services.

It is believed that the entry point that caused the cyber attack on the private health insurer was when a person with high-level access within Medibank's systems had their credentials stolen by a hacker. The information was then sold on a Russian-language cyber crime forum, according to a report from *The Guardian* that attributed the information to a source who was not authorised to speak publicly.

UpGuard

8. Australian Parliament House Data Breach

AUSTRALIAN PARLIAMENT HOUSE

Date: February 2019

Impact: Multiple political party networks - Liberal, Labor, and the Nationals.

The cybercriminals used phishing methods to steal employee credentials and gain entry into the government's network. This precursor attack took place on an infected external website that a small number of parliament staff visited.

6. Service NSW Data Breach

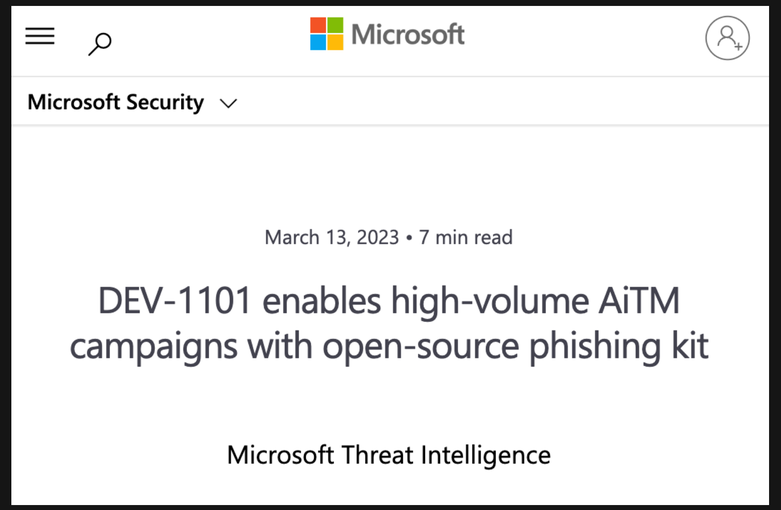
Service NSW

Date: April 2020

Impact: 104,000 people

47 Service NSW staff email accounts were hacked through a series of phishing attacks. This led to 5 million documents being accessed, 10 percent of which contains sensitive data impacting 104,000 people.

High volume AiTM phishing kits



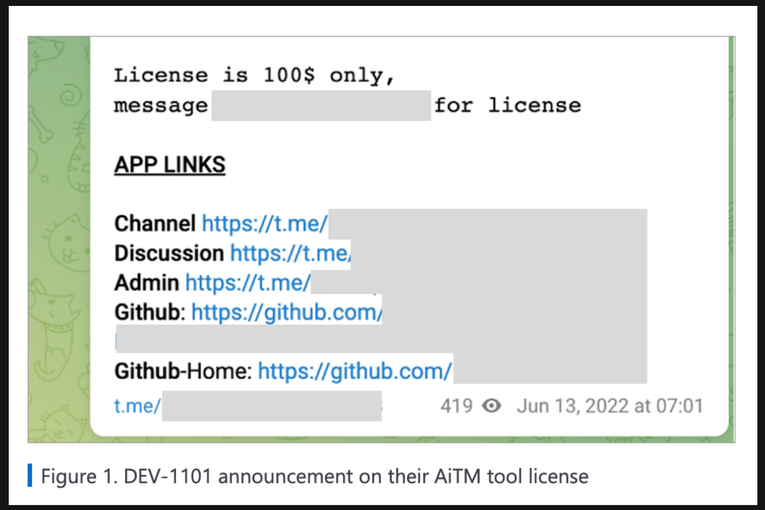


Figure 1. DEV-1101 announcement on their AiTM tool license

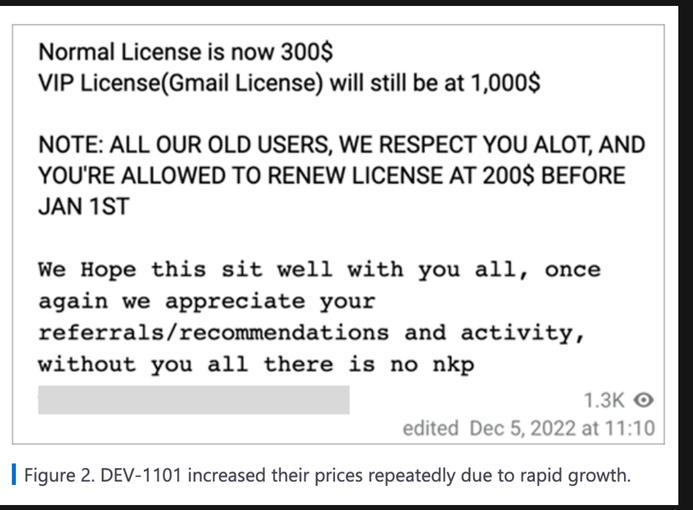


Figure 2. DEV-1101 increased their prices repeatedly due to rapid growth.

DEV-1101 enables high-volume AiTM campaigns with open-source phishing kit

Why Prompting is Bad

- Over-prompting leads to compromise
  - Users learn bad behaviors, like blindly approving MFA requests
- Prompts impact productivity, especially on platforms without SSO
- Prompting is especially common on macOS, which does not do SSO with Azure AD out of the box
- Should strive to improve user experience AND security
  - Prompt when *needed*, such as new device, new location, change in risk, etc.
  - Passwordless makes prompting less impactful when it IS needed

Prompts are bad

Agenda

What is Azure AD?

Prompting…why is it bad?

Enterprise Single Sign On (SSO) - How does it work?

Deploying Enterprise SSO

Troubleshooting Enterprise SSO

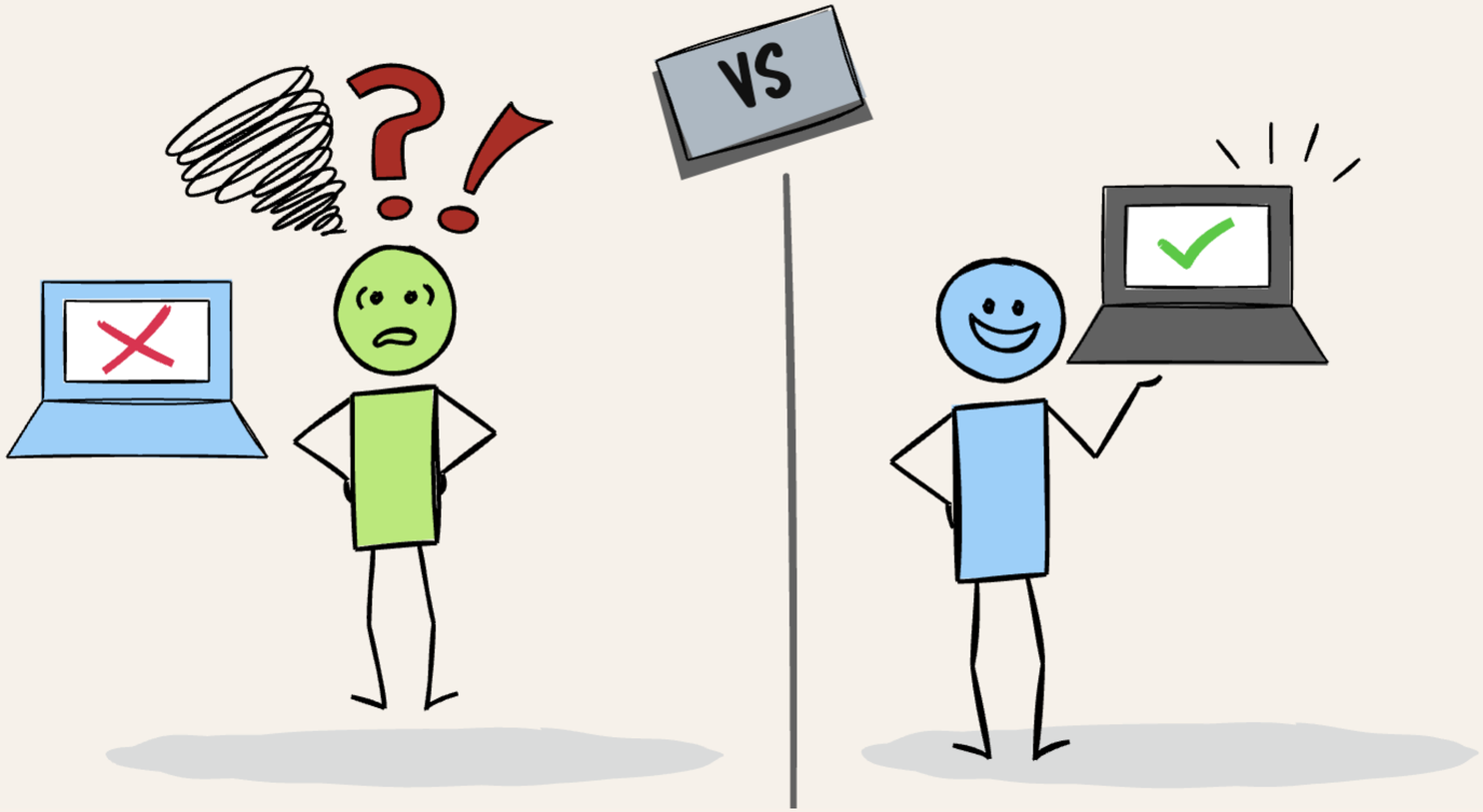
Single Sign On options

- macOS can provide SSO in a few different ways:
  - Kerberos, via BIND to an LDAP directory, commonly on-premises Active Directory
    - Apple is actively telling customers to move away from this
  - Kerberos, via Apple's Kerberos SSO Extension
    - Must be deployed through MDM
    - Still designed for on-premises directory services, not really designed for the cloud
  - Modern Auth (tokens), via IDP vendor-provided plug-ins for Apple's Extensible Enterprise SSO Framework
    - IDP vendor…that's me!
    - Must be deployed through MDM
    - Two types:
      - Credential
      - Redirect – Azure AD's option is this type

Single Sign On over the internet...

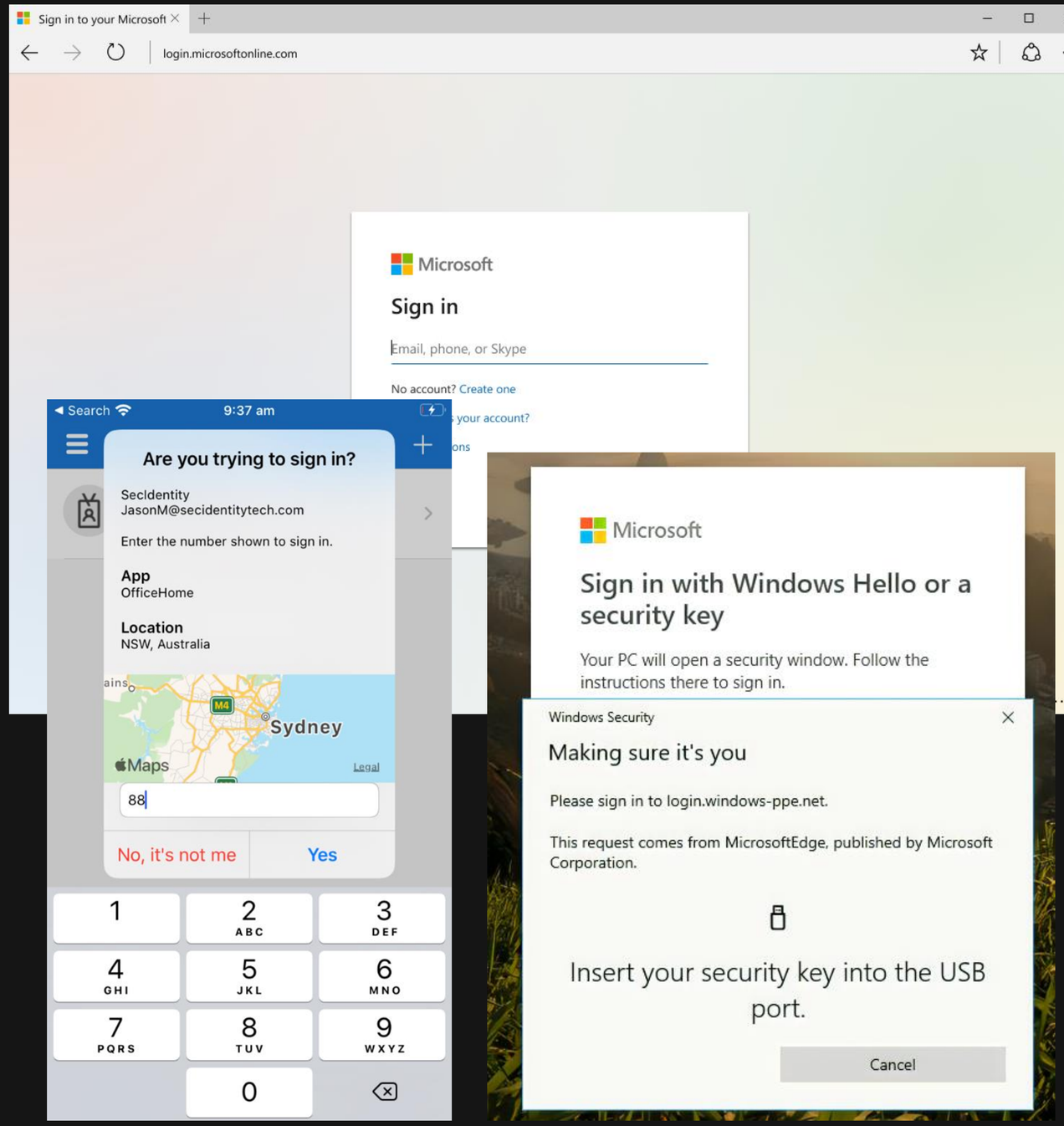
Kerberos SSO

Enterprise SSO

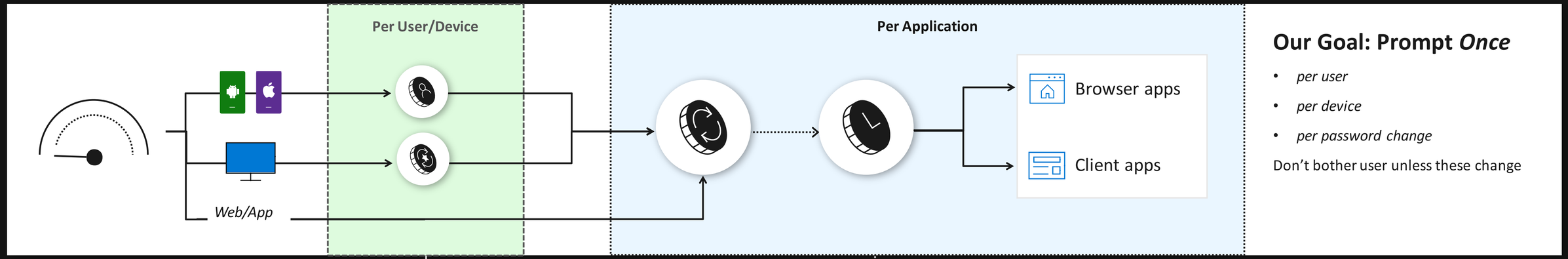


SSO – Modernize w/ Modern Auth

- The future is Modern Auth!
  - SAML – good
  - OpenID Connect and OAuth 2 - better!
- The key advantage of Modern Auth is that it is web-based
  - The flexibility of web technology gives us many security options:
    - Challenge for certificates
    - Many forms of MFA (FIDO, Auth apps, Smartcards, SMS codes, etc.)
    - Direct traffic through proxied sessions to block downloads
    - And much more!



Microsoft’s ‘prompt’ goal



Our Goal: Prompt *Once*

- *per user*
- *per device*
- *per password change*

Don’t bother user unless these change

AUTHENTICATION

Until Revoked or Password Change (If actively used within 14 days)

Primary Refresh Token

Long term authentication w/ SSO broker on Windows, macOS, or iOS

ID Token

Long term authentication on Mobile Device
(used by authenticator app and/or company portal)
Note: Authenticator App has two functions: brokering authentication locally + MFA validation

(COARSE) AUTHORIZATION

Refresh Token – (Per App)

Long term access to an application

Note: Includes whether MFA was used for authentication

Until revoked or Password Changed

Access Token – (Per App)

Provides user access to use application (short term)
Note: Policy is re-evaluated every time you get a new access token (using the refresh token)

1 hour

SSO – Modernize w/ Modern Auth

- Here’s what you need for Modern Auth and SSO on Apple Platforms:
  - IDP that supports SAML and/or OpenID Connect
    - Azure AD is Microsoft’s cloud IDP, but there are plenty of others on the market
  - Apps integrated with the IDP
  - IDP Vendor must create an SSO Extension plugin
  - Macs under MDM management

SSO – Modernize w/ IDP Vendor SSO Extensions

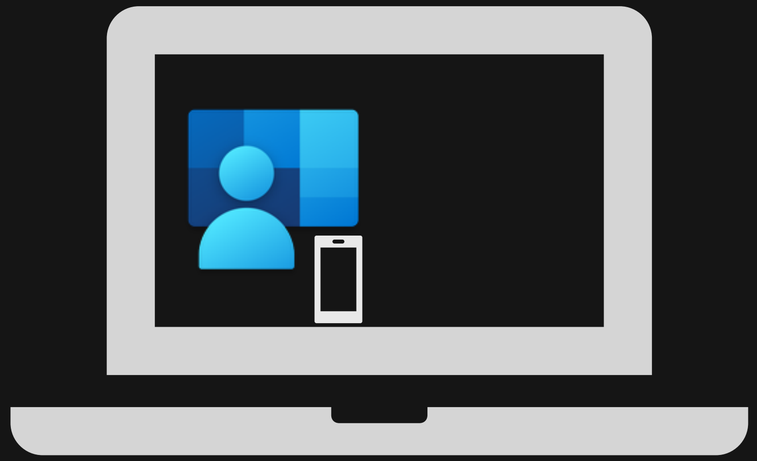
- The *modern* approach is to use an IDP, modern auth, and tokens
- SSO Extension is bundled in the Microsoft Company Portal

1) User authenticates to Azure AD in the SSO Extension window – this can be in Company Portal or another app, such as Safari
    - Azure AD supports many more credential types than AD does
2) Azure AD SSO Extension acquires a Primary Refresh Token (PRT) from Azure AD after the user signs in, stores it in the keychain
    - PRTs are good for a rolling 14 day window, constantly refreshed when the user uses the Mac

MS Authenticator Passwordless Phone Sign-In

Username+Pwd+MFA (App, OTP, SMS, Phone)

App



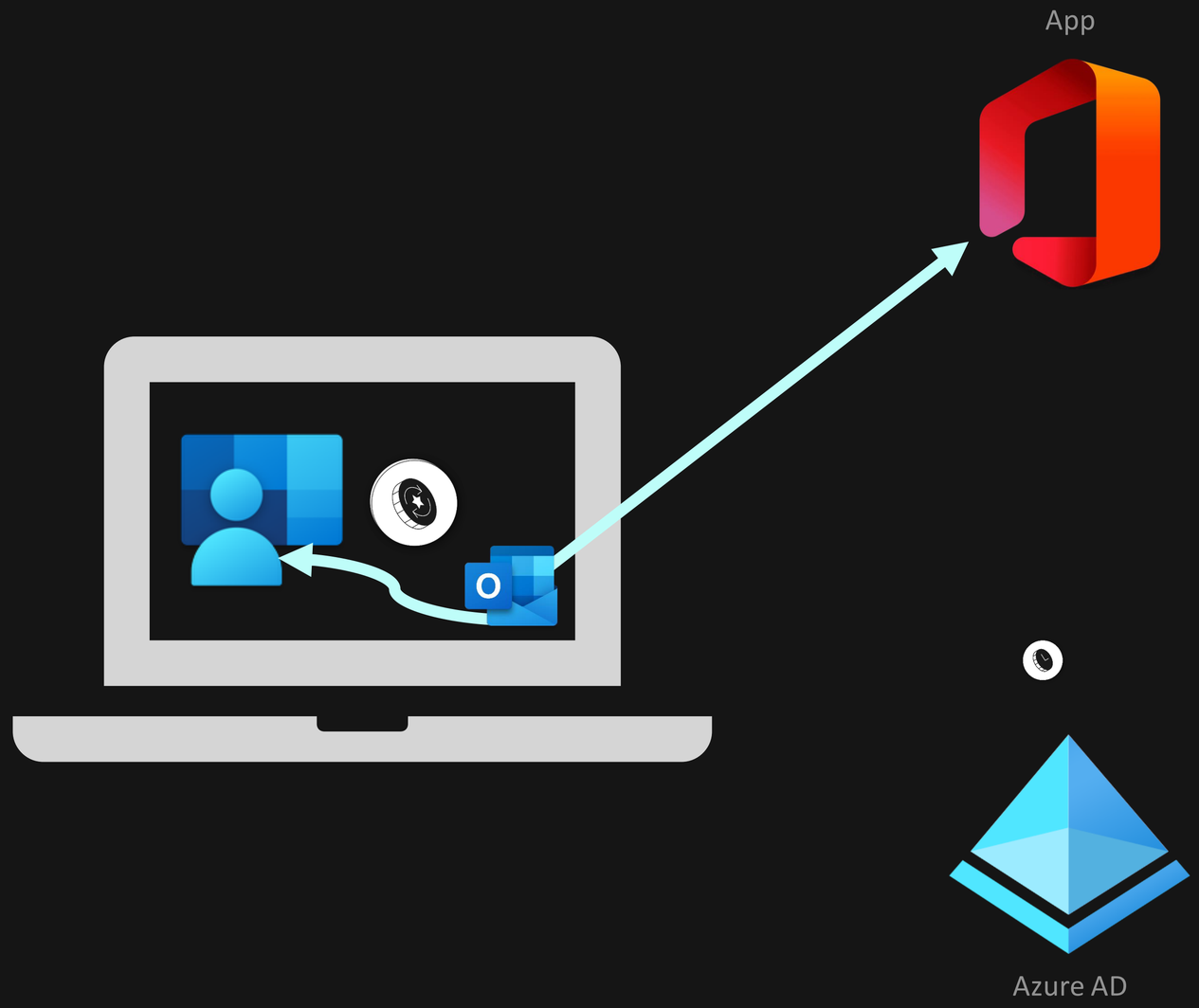
Azure AD

SSO with Microsoft Auth Library

Let’s look at the out of the box SSO experience for Microsoft & MSAL apps.

We’ll start with the MSAL flow (MSAL is Microsoft Authentication Library, our auth library provided to make app integration with Azure AD easy):

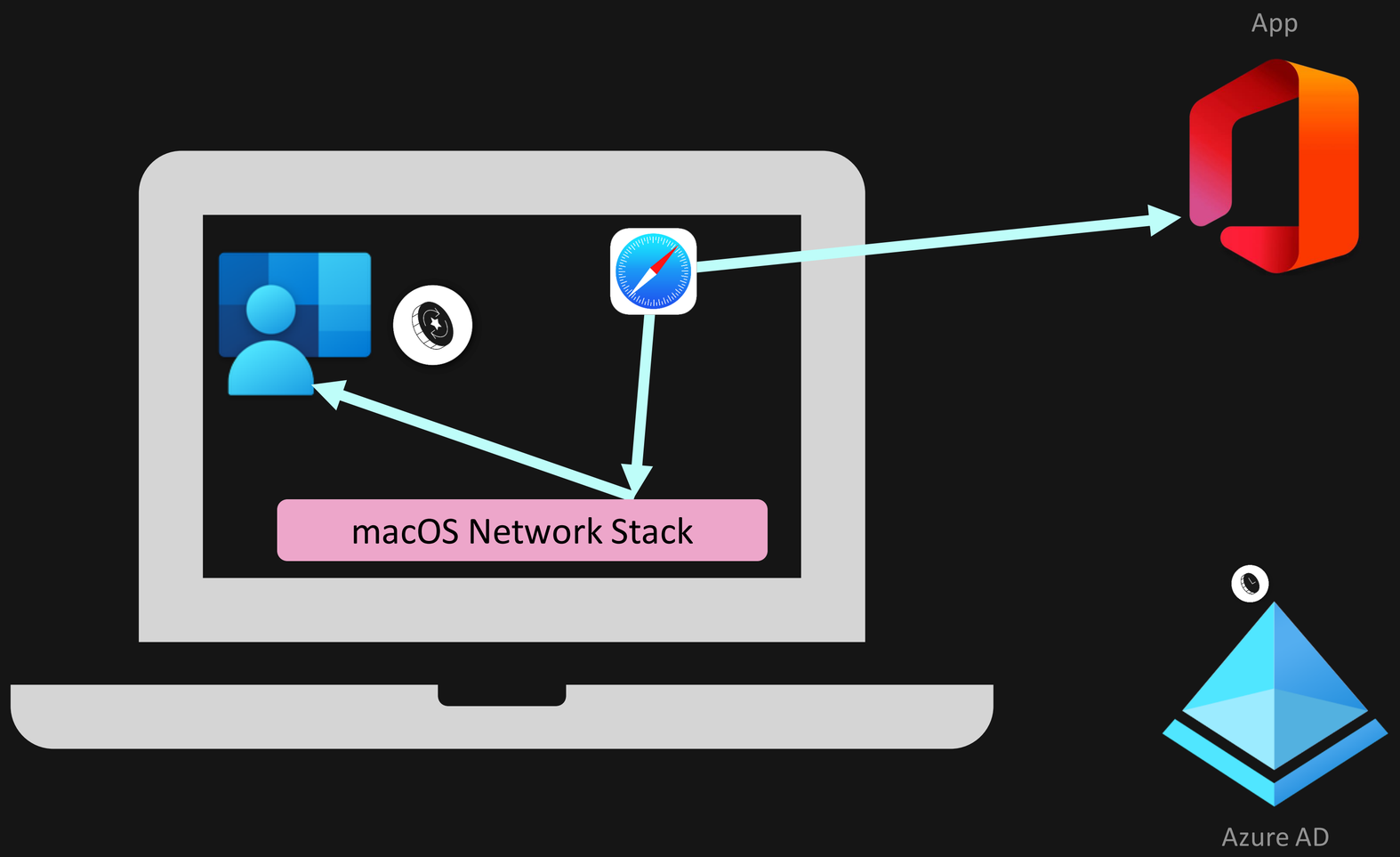
- App that uses MSAL talks to the SSO Extension directly, asks it to get a token
- AAD validates the PRT and returns the app-specific token
- The token is given to the client and the client sends the token to the app
- The user successfully accesses the app



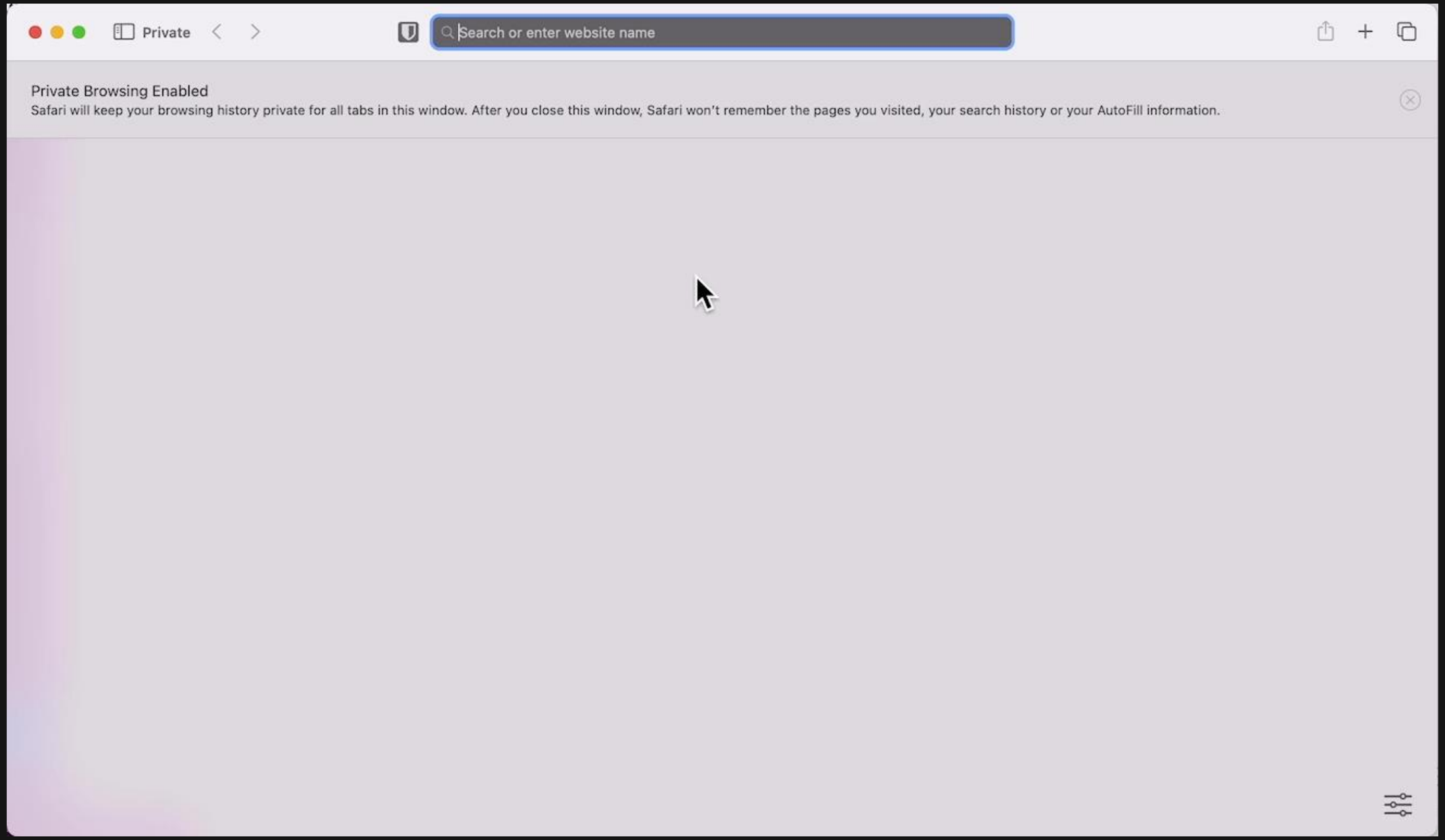
Enterprise SSO Redirect flow

Now let’s look at the redirect flow:

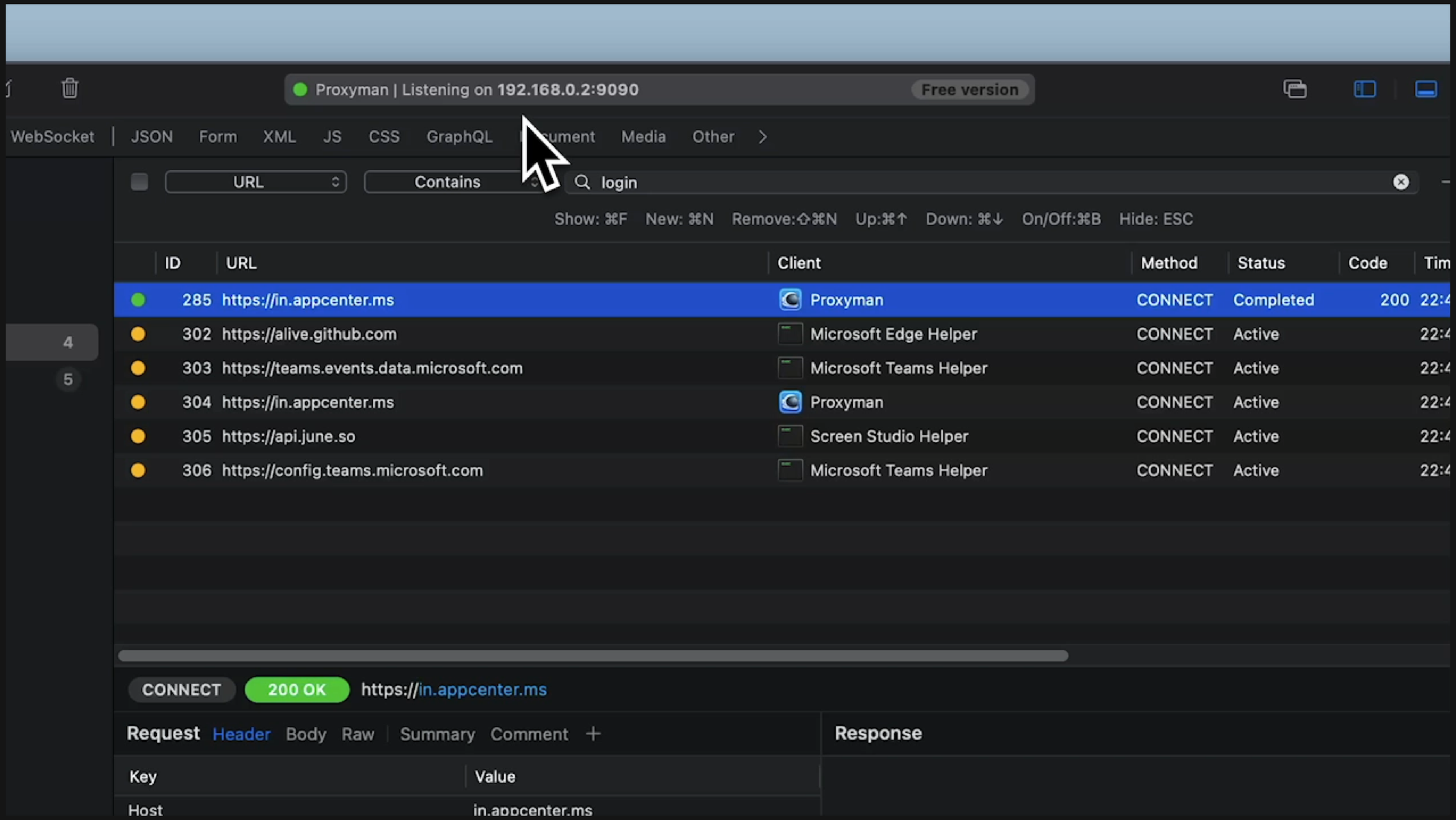
- User tries to log into app, is told to get a token from Azure AD
- App that doesn’t use MSAL tries to go to an Azure AD URL…the macOS Network Stack intercepts the traffic and redirects it to the SSO Extension
- SSO Extension uses its PRT to request a token
- AAD validates the PRT and returns the app-specific token
- The token is given to the client and the client sends the token to the app
- The user successfully accesses the app



Demo


Private
Search or enter website name
Private Browsing Enabled
Safari will keep your browsing history private for all tabs in this window. After you close this window, Safari won't remember the pages you visited, your search history or your AutoFill information.

That’s it! 


Proxyman | Listening on 192.168.0.2:9090
Free version
WebSocket | JSON Form XML JS CSS GraphQL Media Other
URL
Contains
login
Show: ⌘F New: ⌘N Remove:⇧⌘N Up:⌘↑ Down: ⌘↓ On/Off:⌘B Hide: ESC
ID URL Client Method Status Code
285 https://in.appcenter.ms Proxyman CONNECT Completed 200
302 https://alive.github.com Microsoft Edge Helper CONNECT Active
303 https://teams.events.data.microsoft.com Microsoft Teams Helper CONNECT Active
304 https://in.appcenter.ms Proxyman CONNECT Active
305 https://api.june.so Screen Studio Helper CONNECT Active
306 https://config.teams.microsoft.com Microsoft Teams Helper CONNECT Active
CONNECT
200 OK
https://in.appcenter.ms
Request Header Body Raw Summary Comment
Response
Key
Value
Host
in.appcenter.ms

Agenda

What is Azure AD?

Prompting…why is it bad?

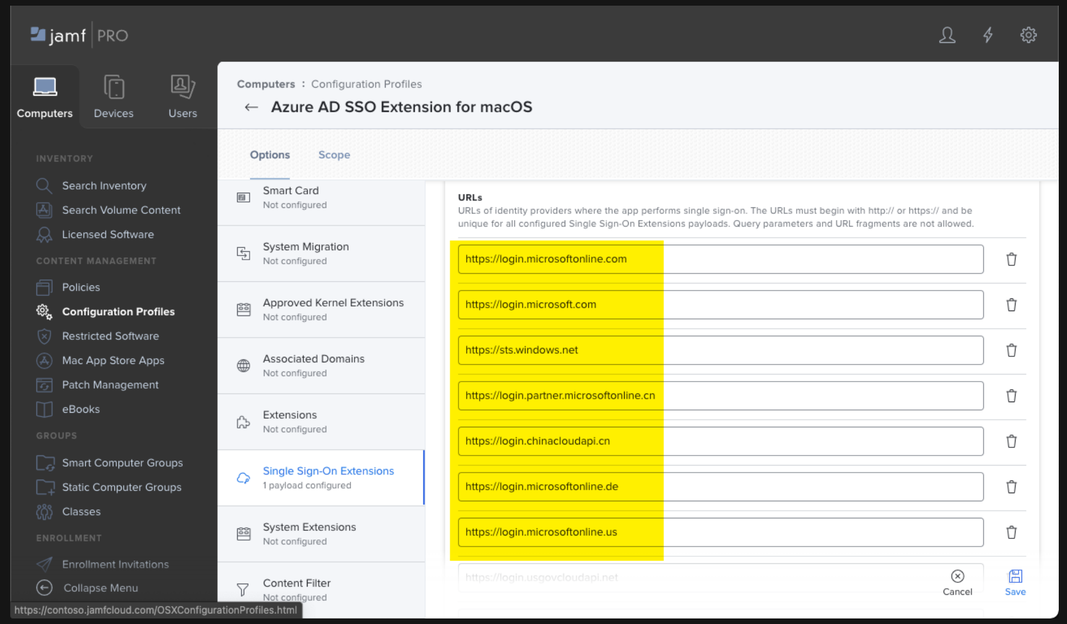
Enterprise Single Sign On (SSO) - How does it work?

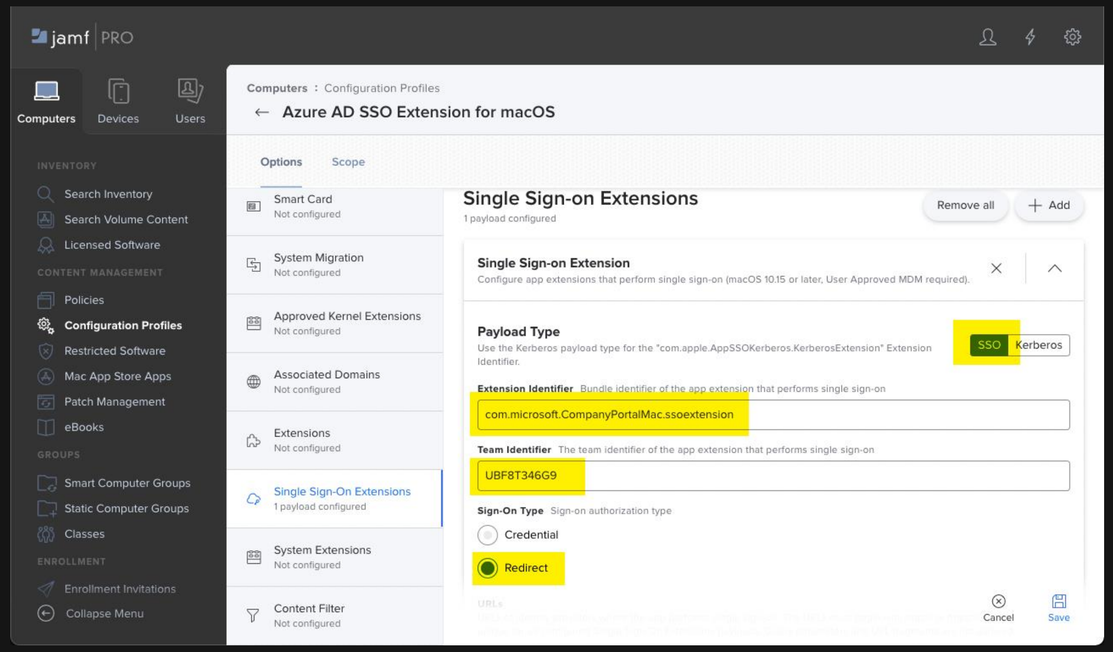
Deploying Enterprise SSO

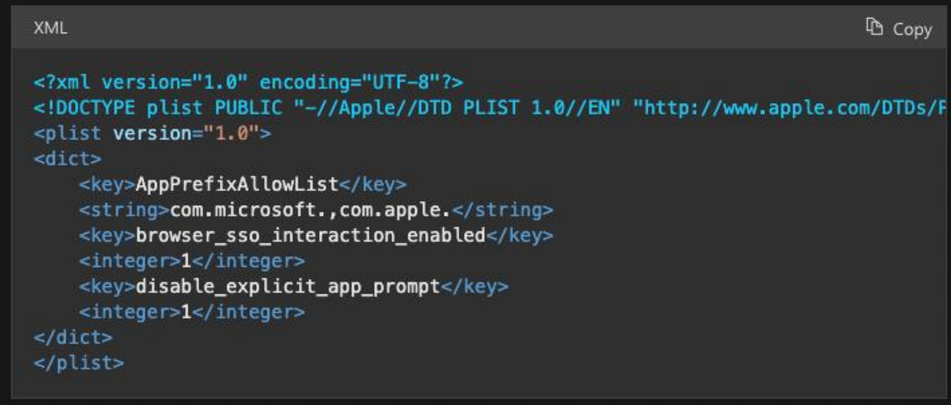
Troubleshooting Enterprise SSO

Deploying Enterprise SSO with Jamf Pro

- Redirect SSO Extension Profiles *must* be deployed via MDM:
  - Jamf Pro config is quite straightforward with a PLIST file



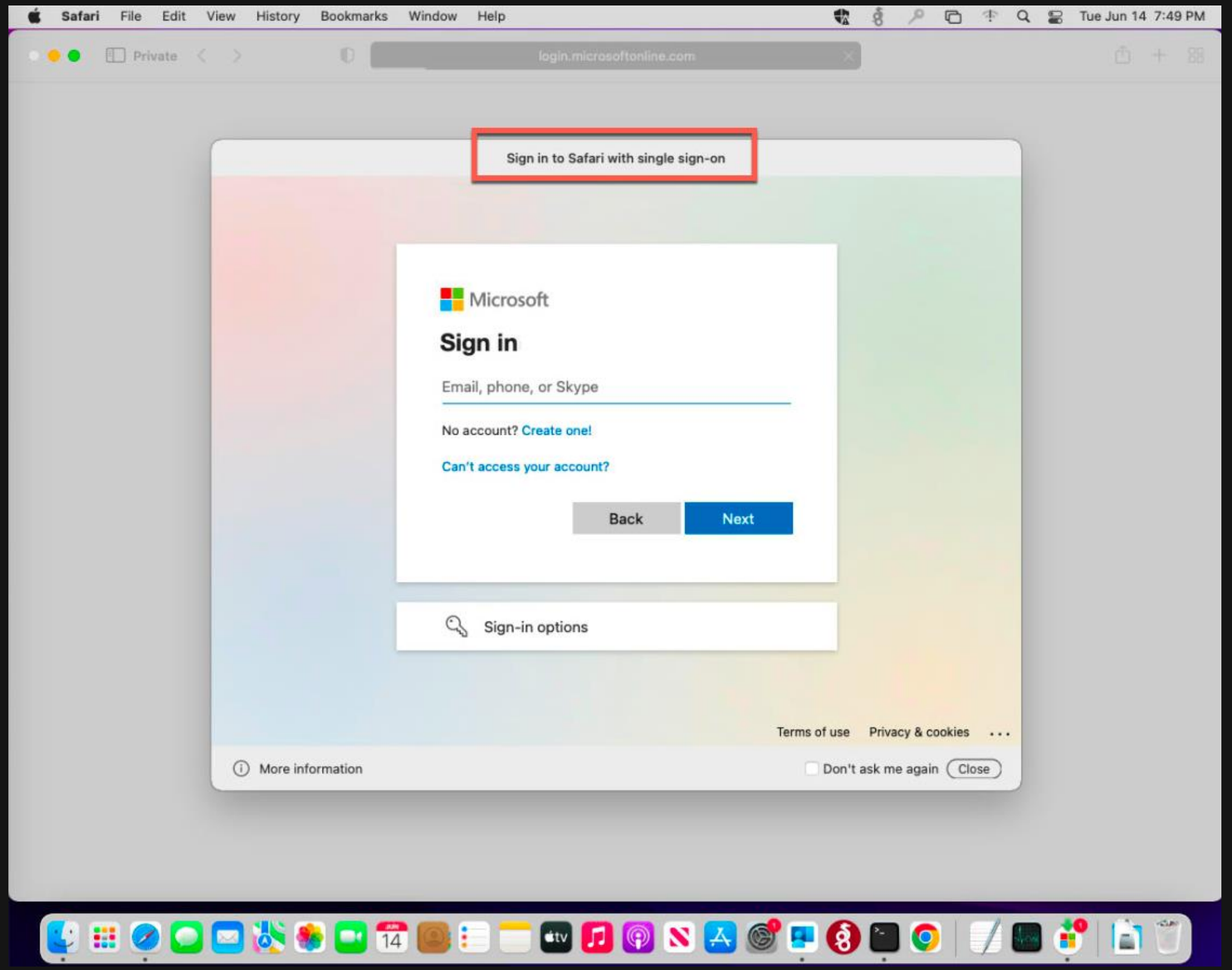




aka.ms/AppleSSO-JamfPro

Modernize w/ IDP Vendor SSO Extensions

- *Can configure settings so users never need to open Company Portal*
  - Company Portal must always be installed, but users don’t need to open it if you follow recommended config



Some things to keep in mind

There’s a few limitations/caveats/warnings:

- Apps must use MSAL or Apple’s system frameworks for network requests
  - This means that some apps don’t work…the SSO Extension is unaware of them and they don’t use Apple’s network stack
  - Chrome and Firefox are the primary examples
  - Talk to your app vendors about the need to support SSO extensions! They should want their apps to work, Apple is only making SSO extensions more important as time goes on
- No support for FIDO keys as a passwordless auth method in the SSO Extension window
  - Authenticator App Phone Sign-In passwordless mode works well

Agenda

What is Azure AD?

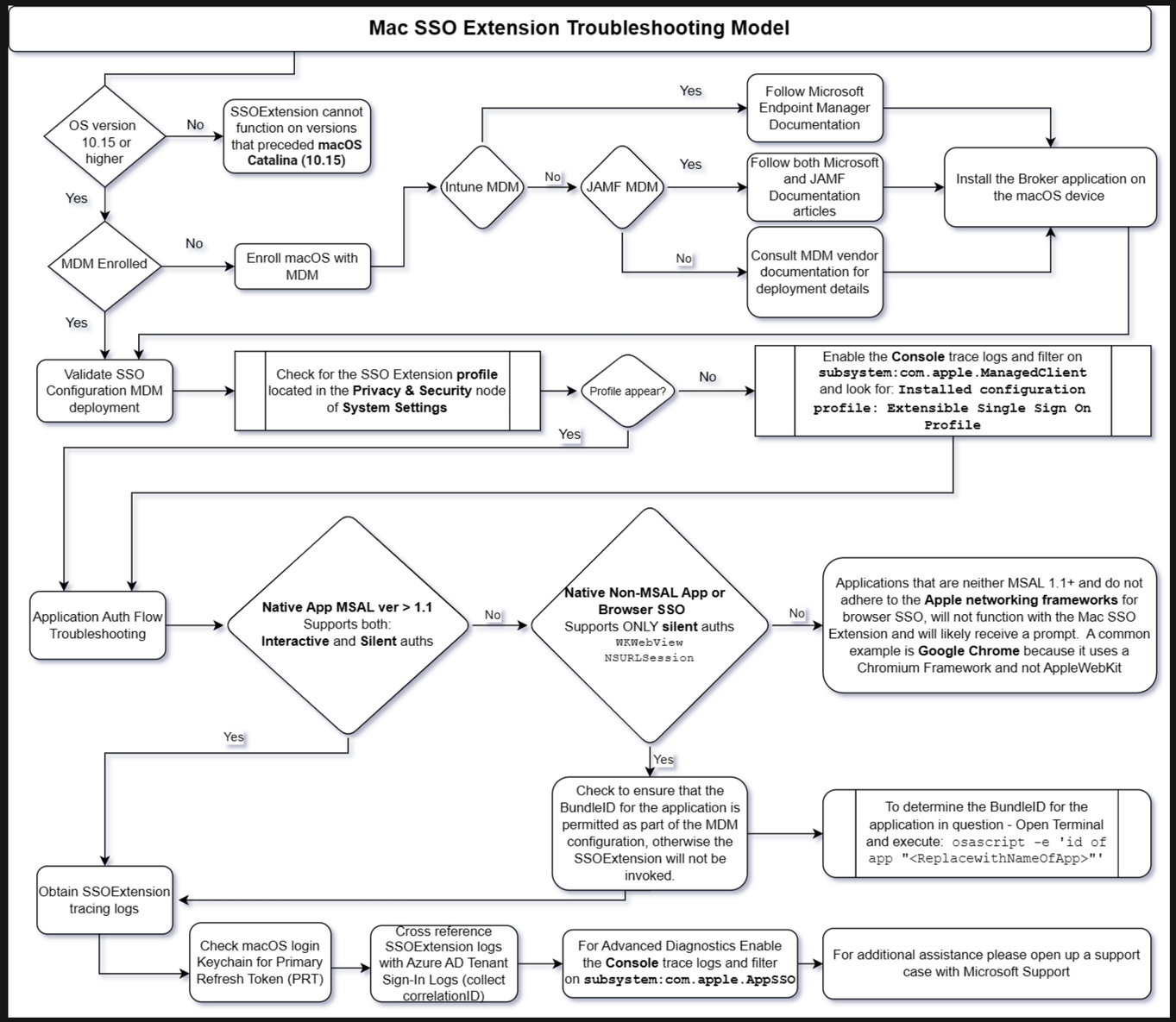
Prompting…why is it bad?

Enterprise Single Sign On (SSO) - How does it work?

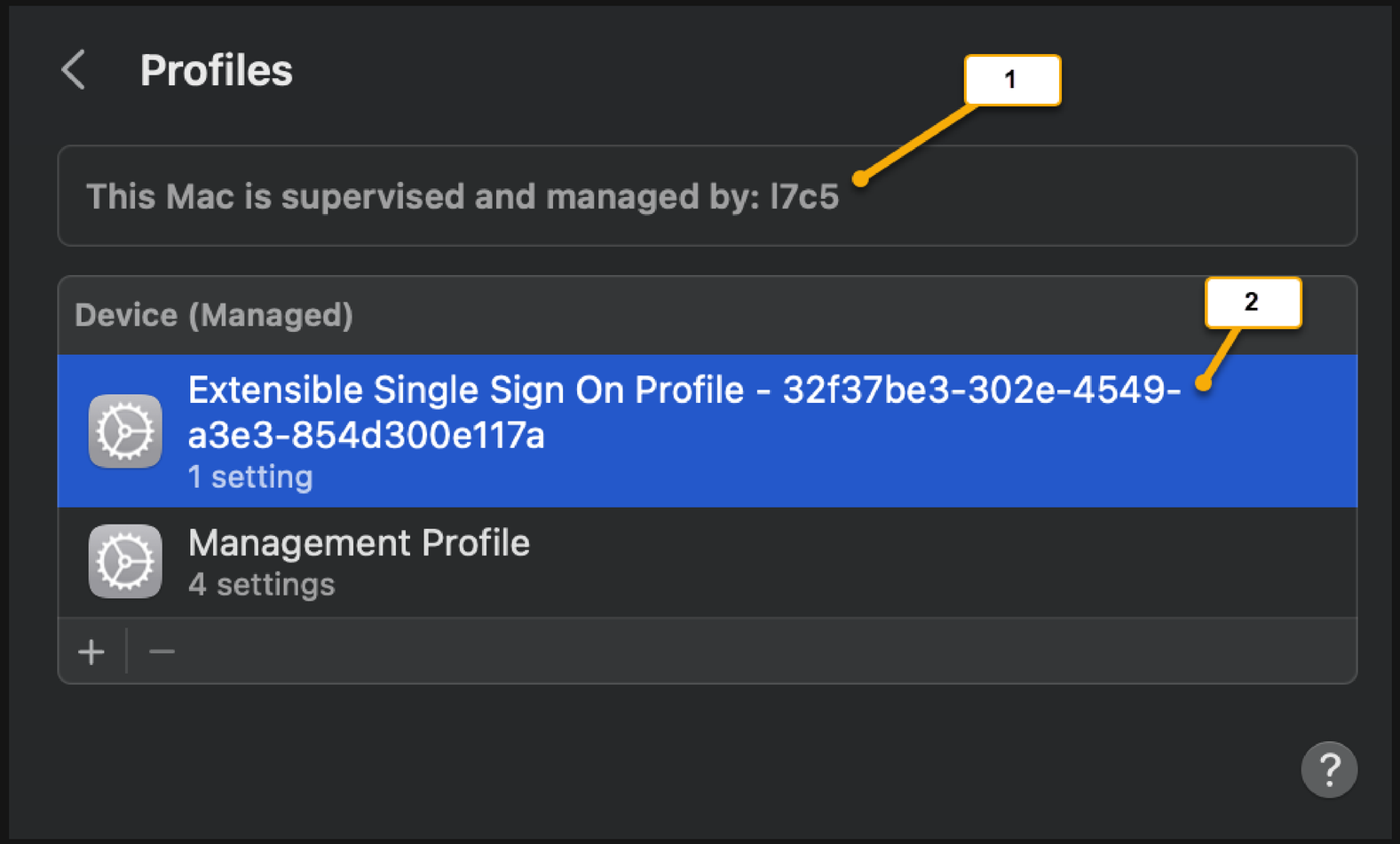
Deploying Enterprise SSO

Troubleshooting Enterprise SSO

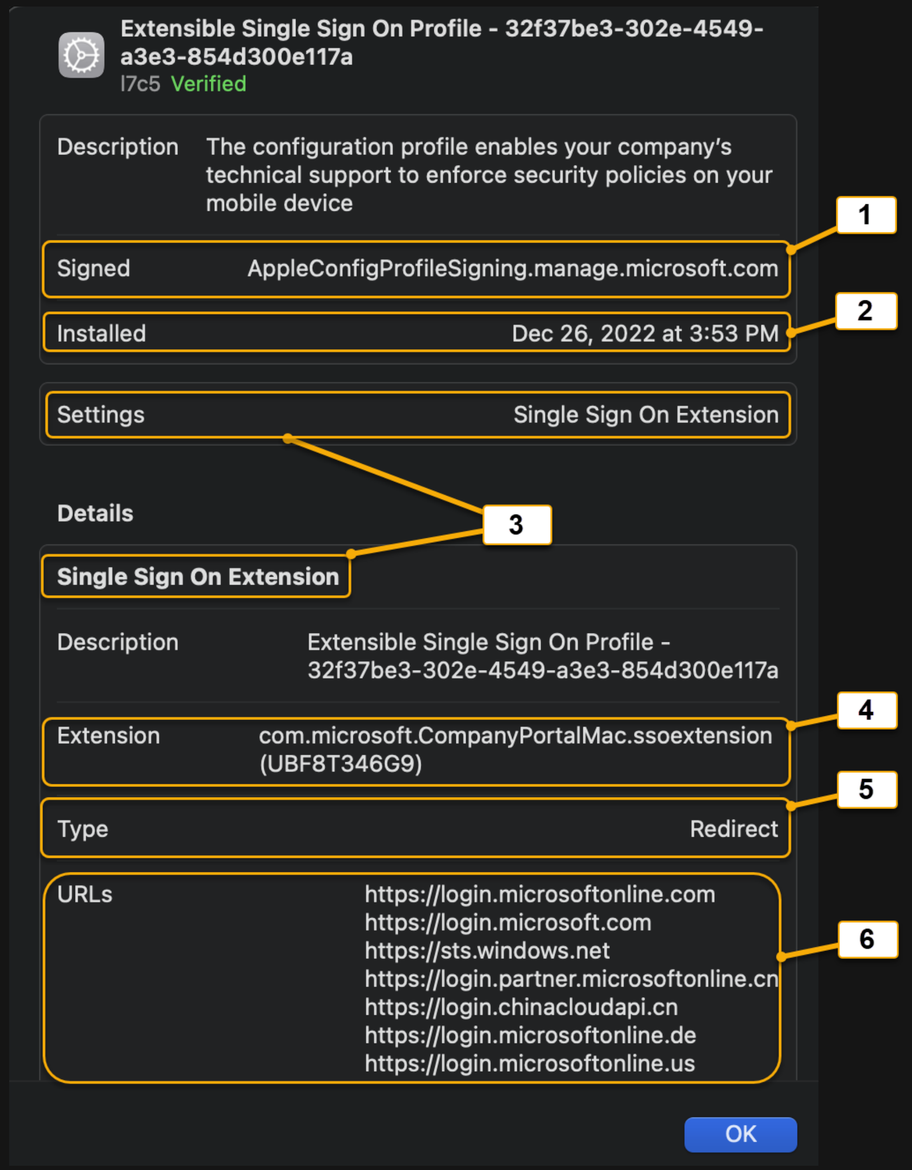
Troubleshooting Enterprise SSO



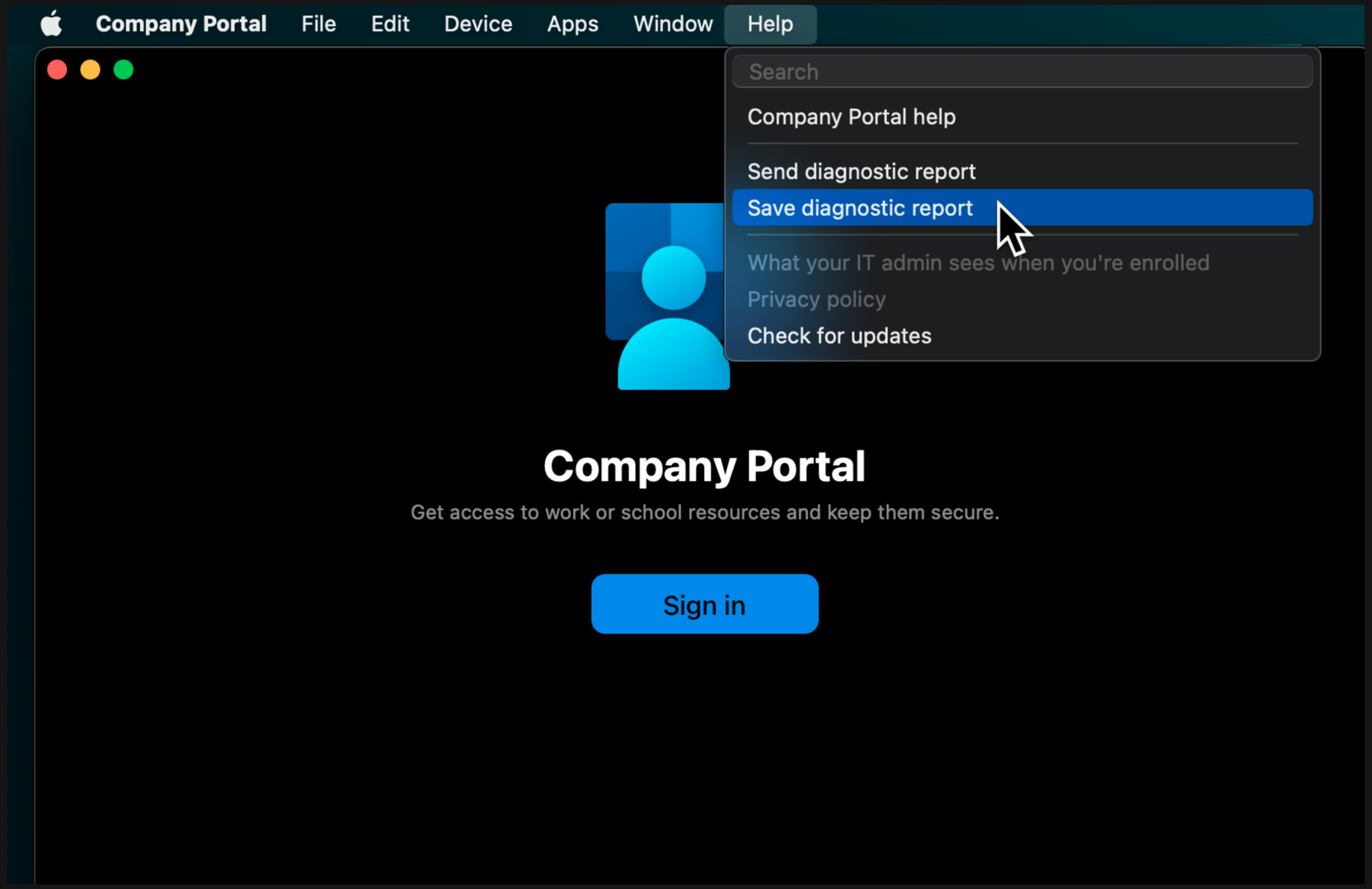
Locate SSO extension MDM profile



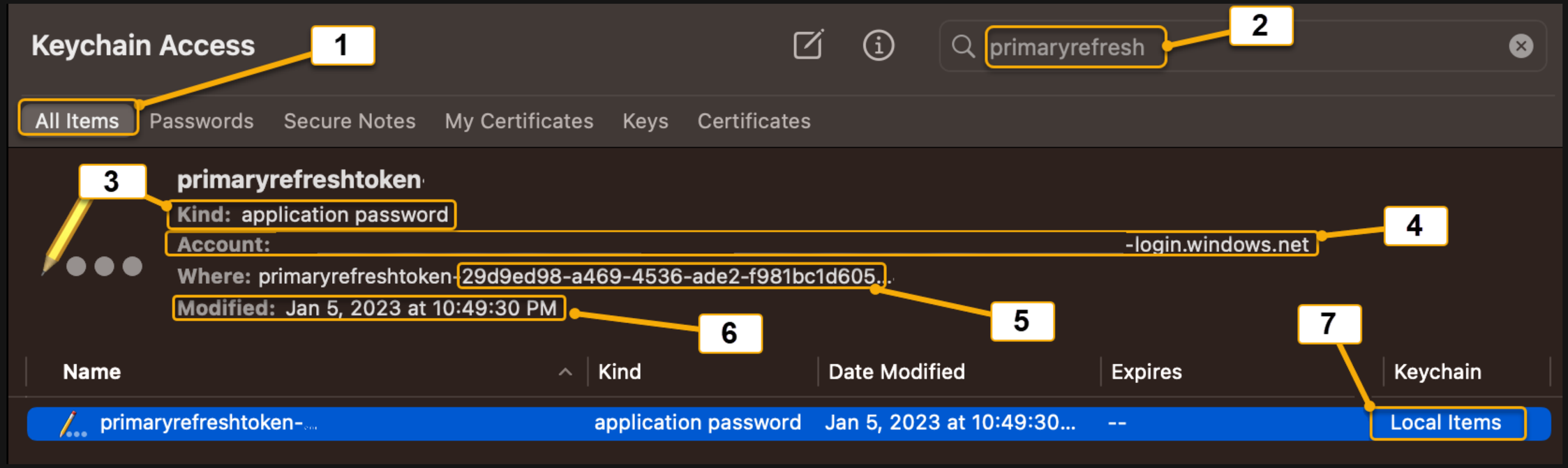
Verify the extension configuration



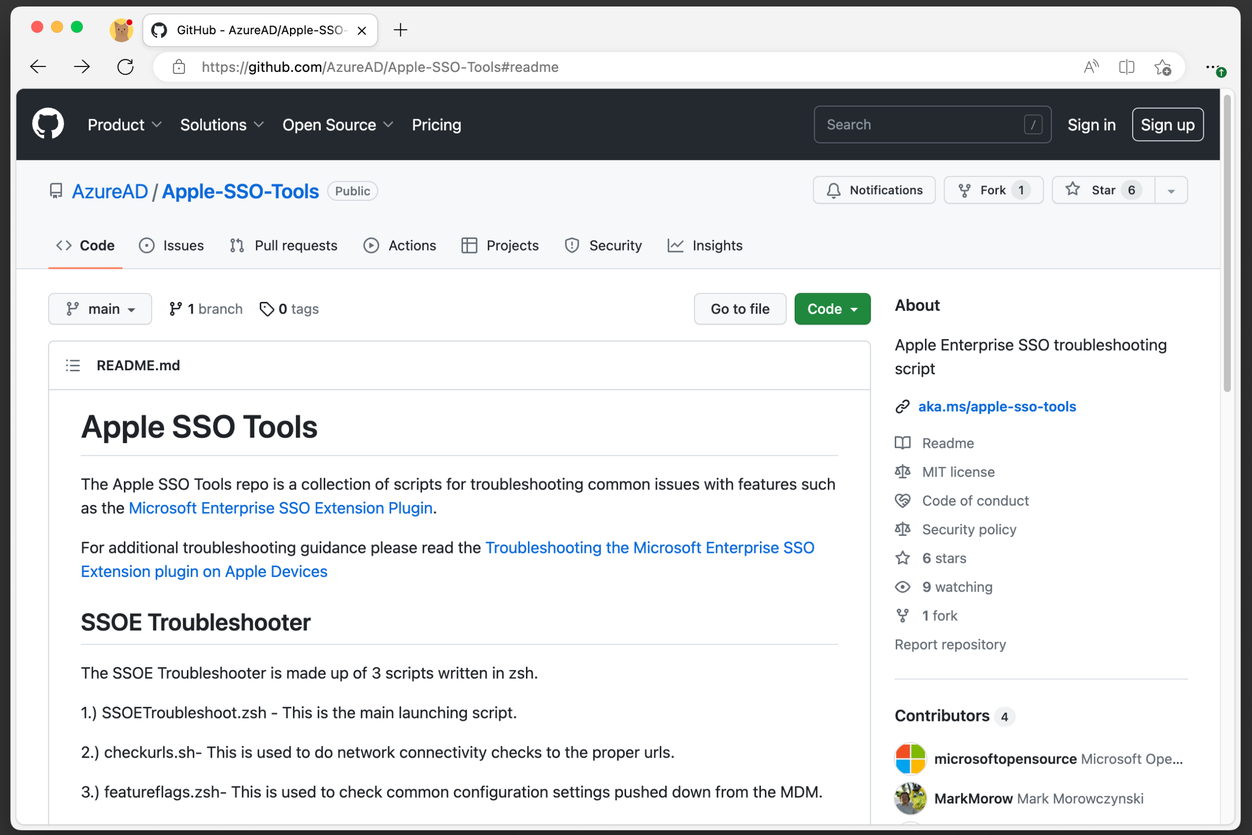
Collect Enterprise SSO logs

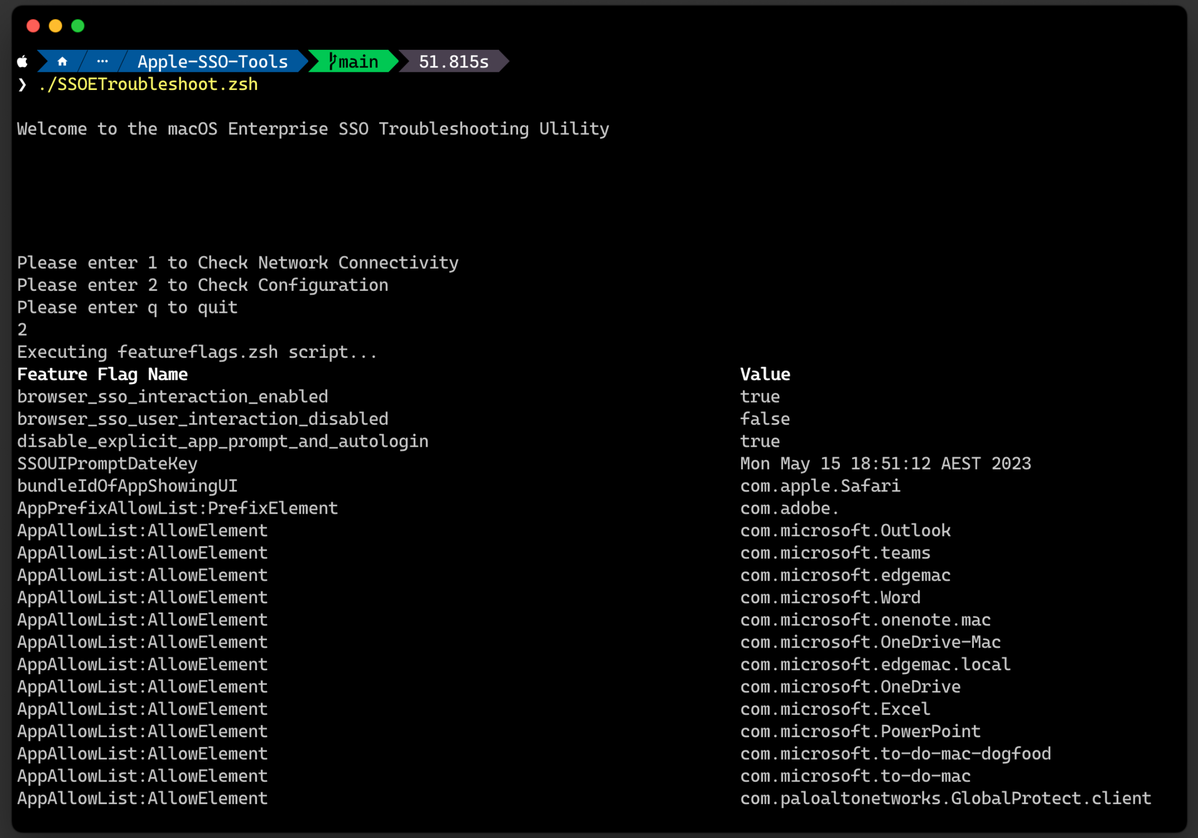


Check keychain access for PRT



Troubleshooting Script





aka.ms/apple-sso-tools

Troubleshooting Demo

Questions?

Thank You

 @merill

 @merill@infosec.exchange

MacAdmins | @merill | #microsoft-aad