



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

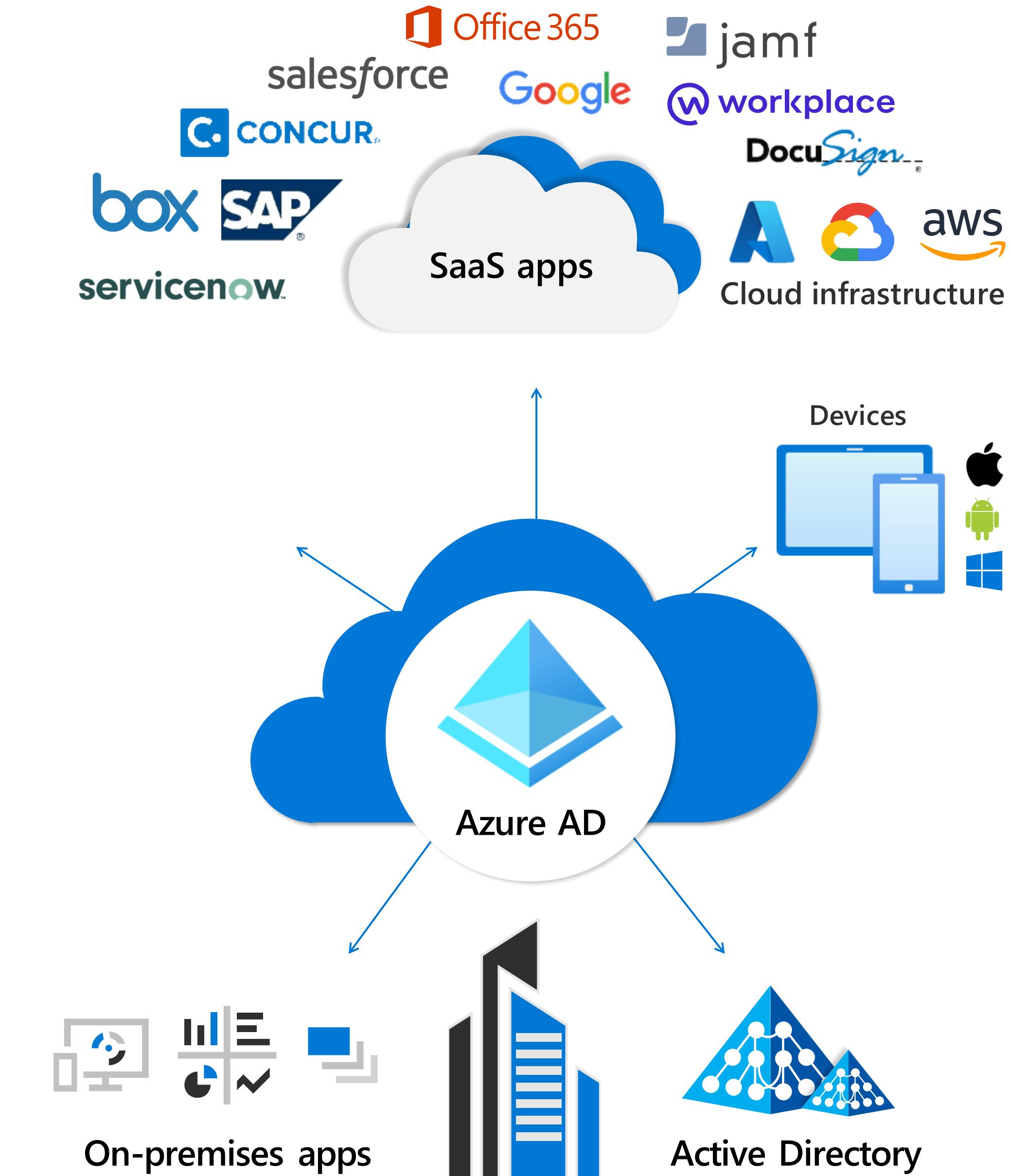
Troubleshooting Enterprise SSO

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



Amy 🍷❤️🥂
@amysw_sec

PSA... don't blindly accept
trying to log in to somethir

1:26 AM · Apr 13, 2021 · Twitter Web /

21 Retweets 4 Quote Tweets 19:

...

K. Reid Wightman

@ReverselCS

I kind of want to write an app that tracks how many hours per week I spend 2FA'ing into different collaboration systems.

7:15 AM · Apr 27, 2021 · TweetDeck

4 Retweets 65 Likes

...



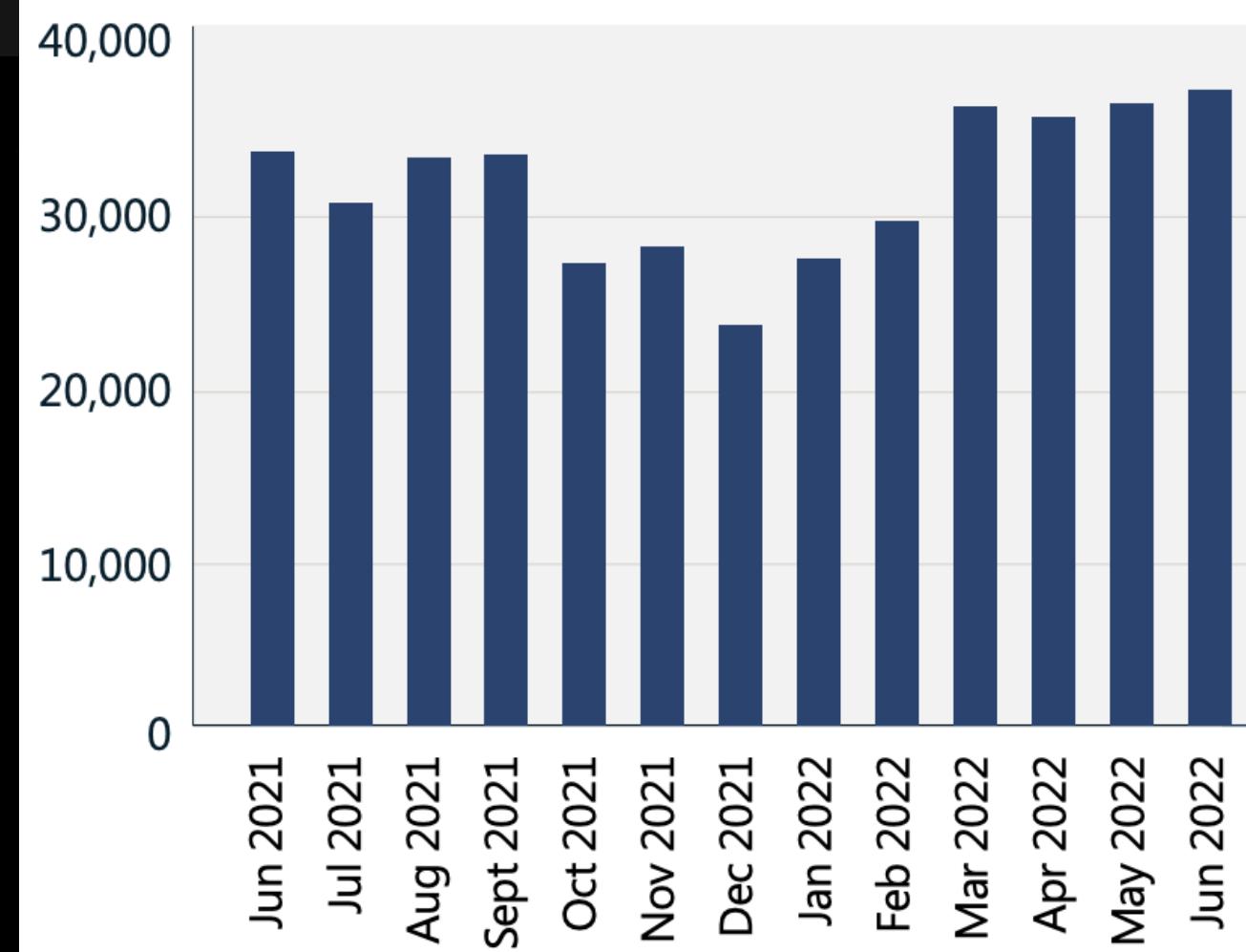
Reg
@RegGBlinker

Replying to @SchizoDuckie and @amysw_sec

Unfortunately, I found a company today who refreshes their users credentials every morning, so each morning their entire workforce gets a push notification to login, whether or not they've initiated access at that time. So,

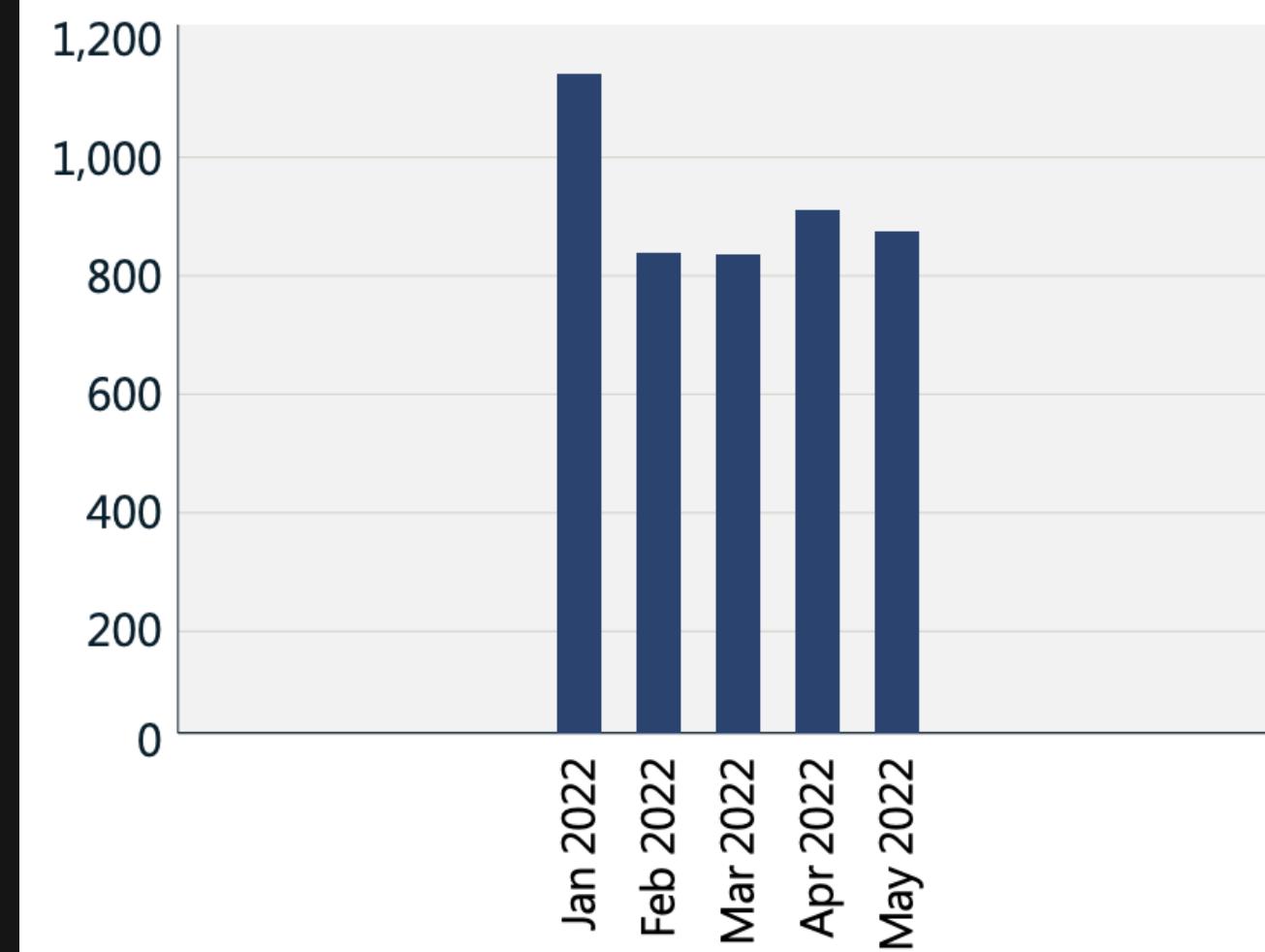
...

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



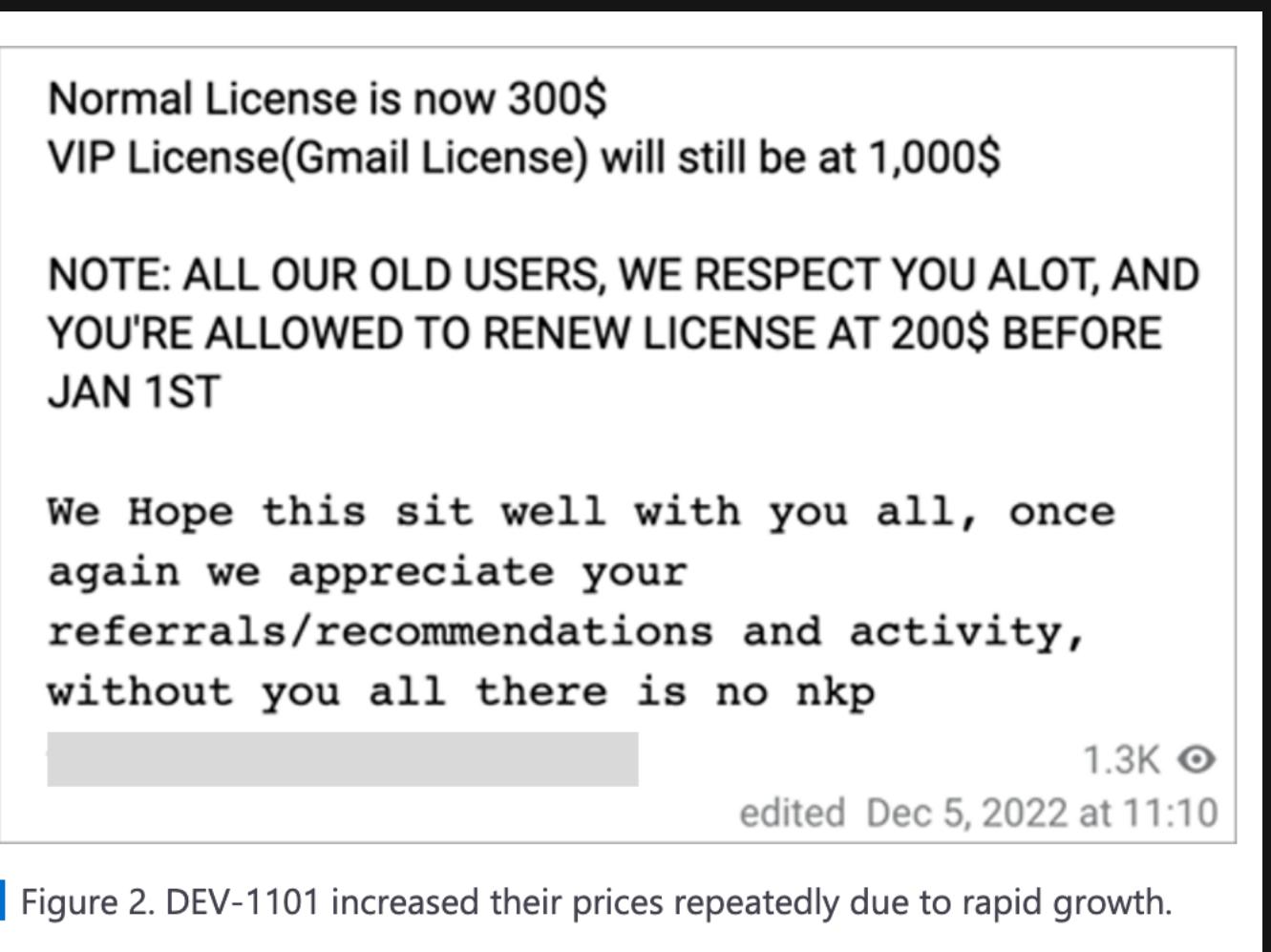
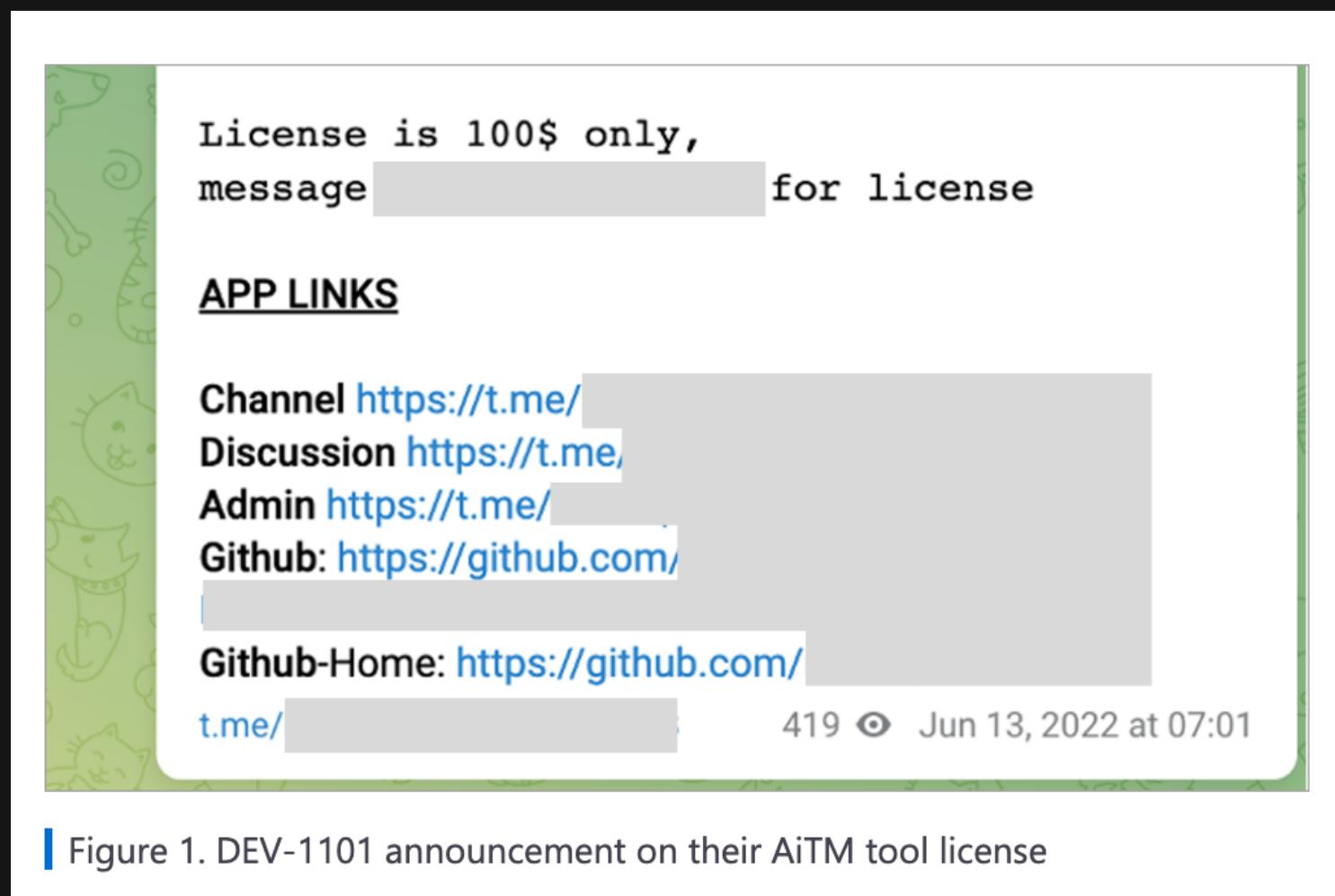
Date: April 2020

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

The screenshot shows a Microsoft Threat Intelligence blog post. The title is "DEV-1101 enables high-volume AiTM campaigns with open-source phishing kit". Below the title, it says "March 13, 2023 • 7 min read". The main content discusses the development of a high-volume AiTM tool. At the bottom, it says "Microsoft Threat Intelligence".



[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

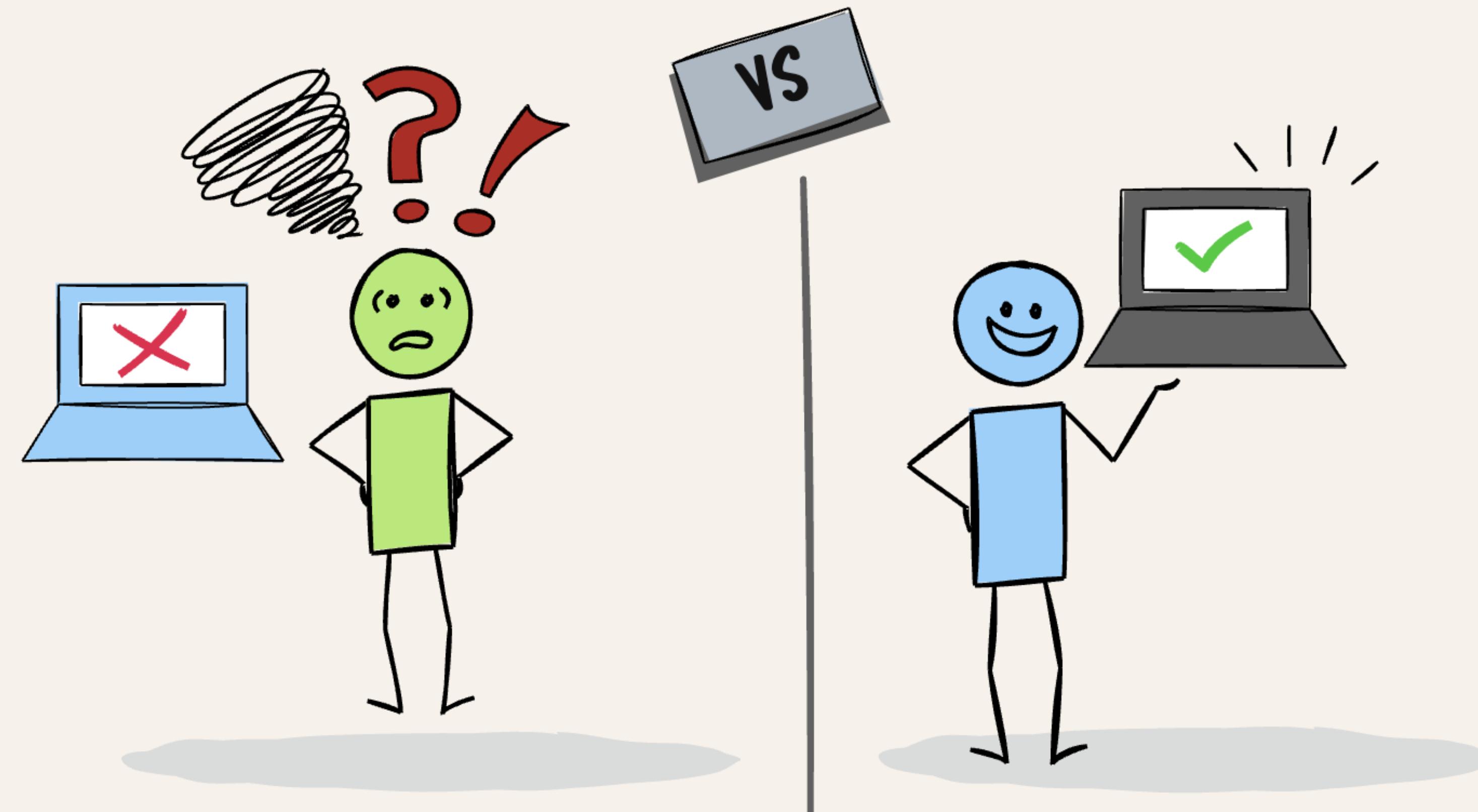
Single Sign On options

- 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...

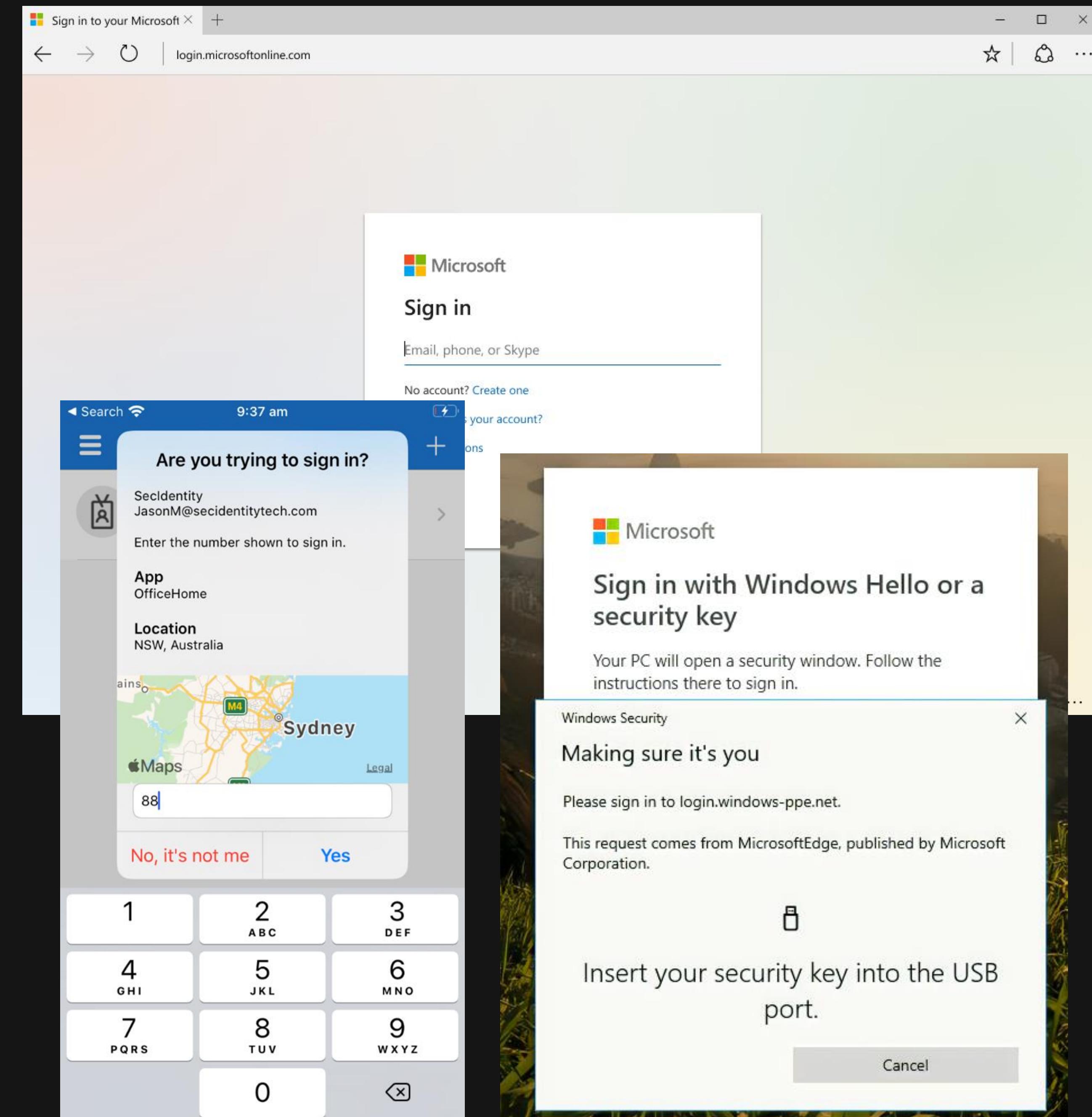
Kerberos SSO

Enterprise SSO

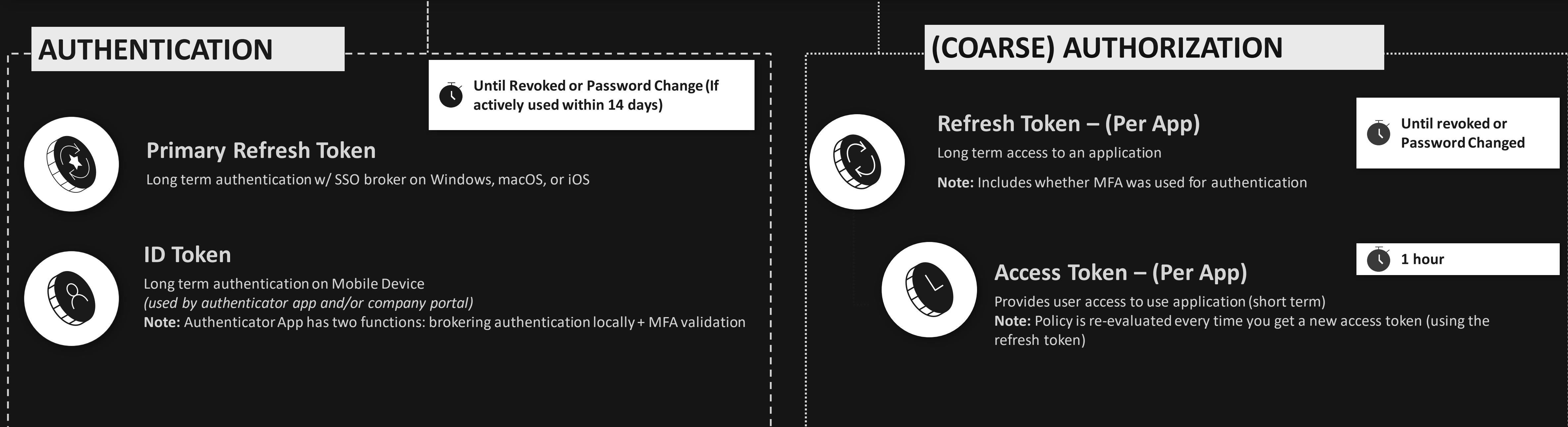
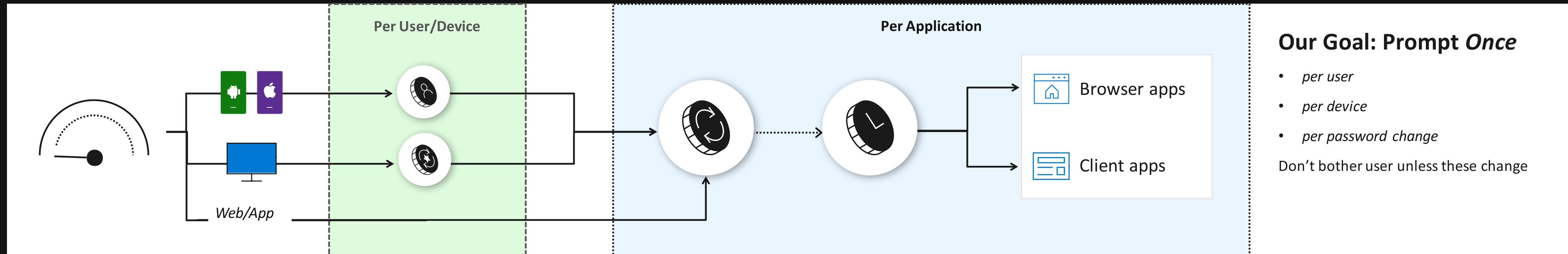


SSO – Modernize w/ Modern Auth

- 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



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

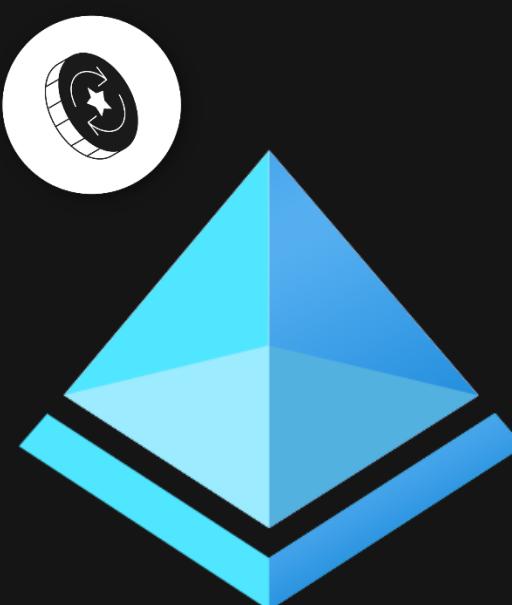
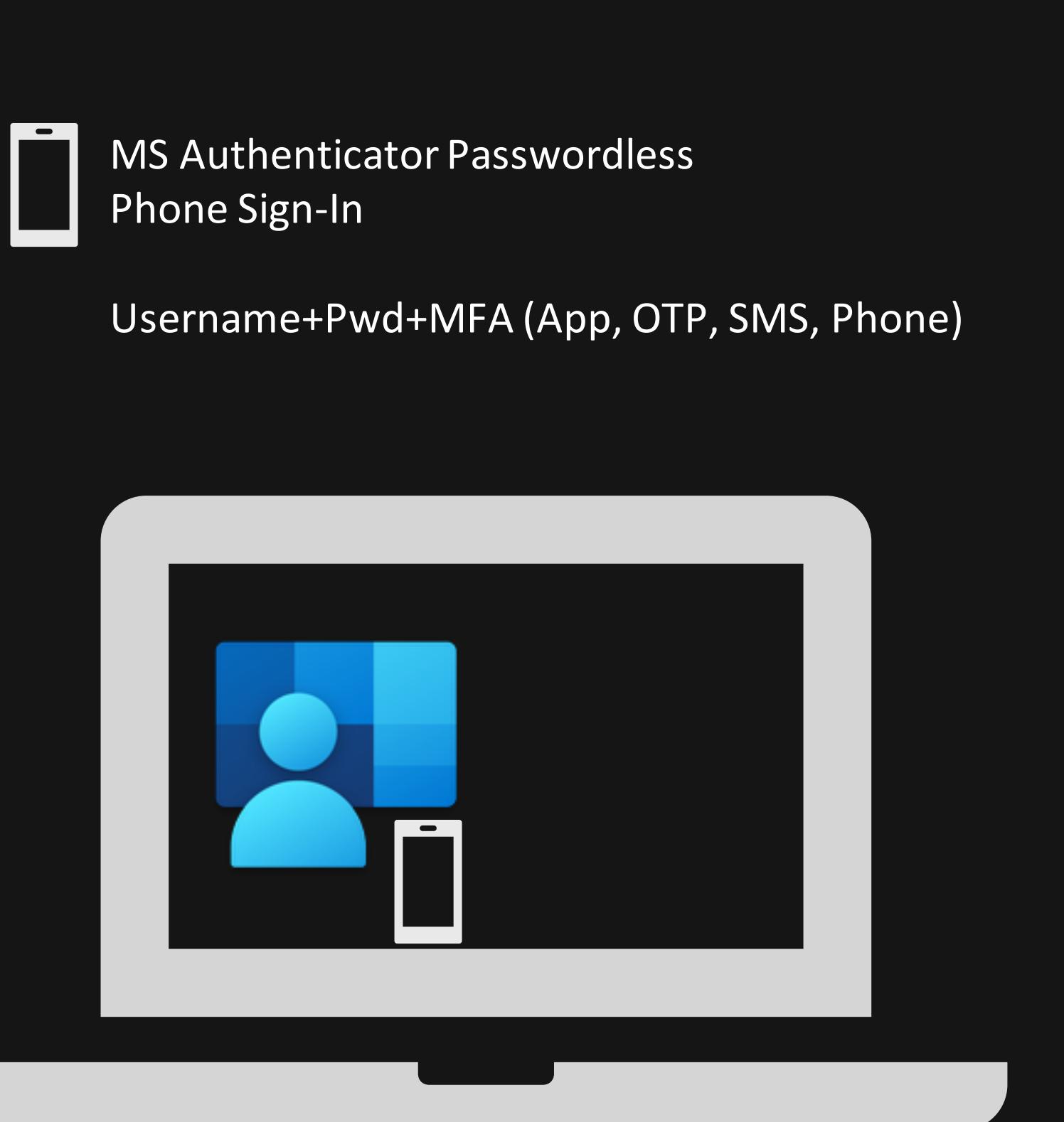
- The modern approach is to use an IDP, modern auth, and tokens
- SSO Extension is bundled in the Microsoft Company Portal

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

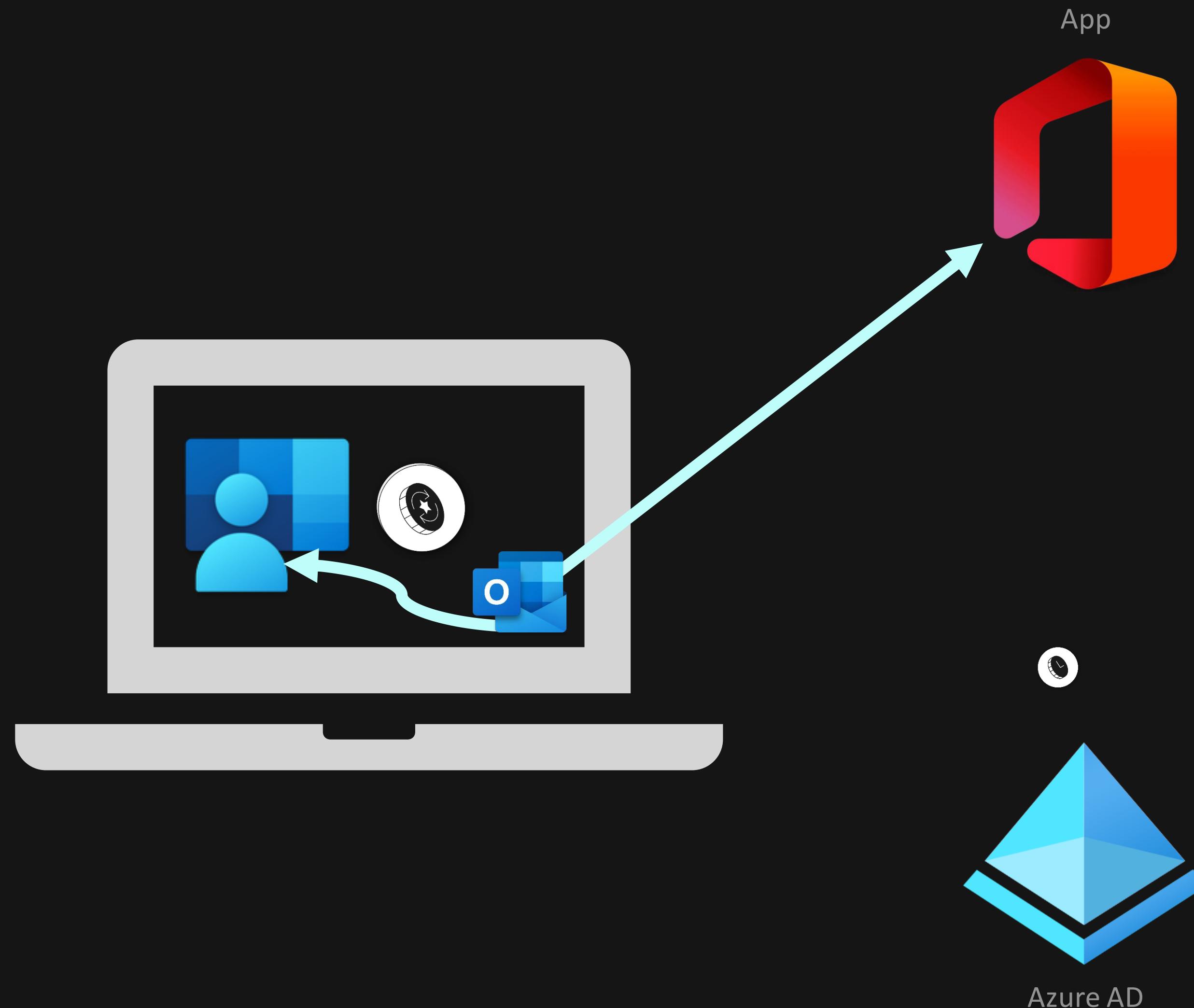


SSO with Microsoft Auth Library

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):

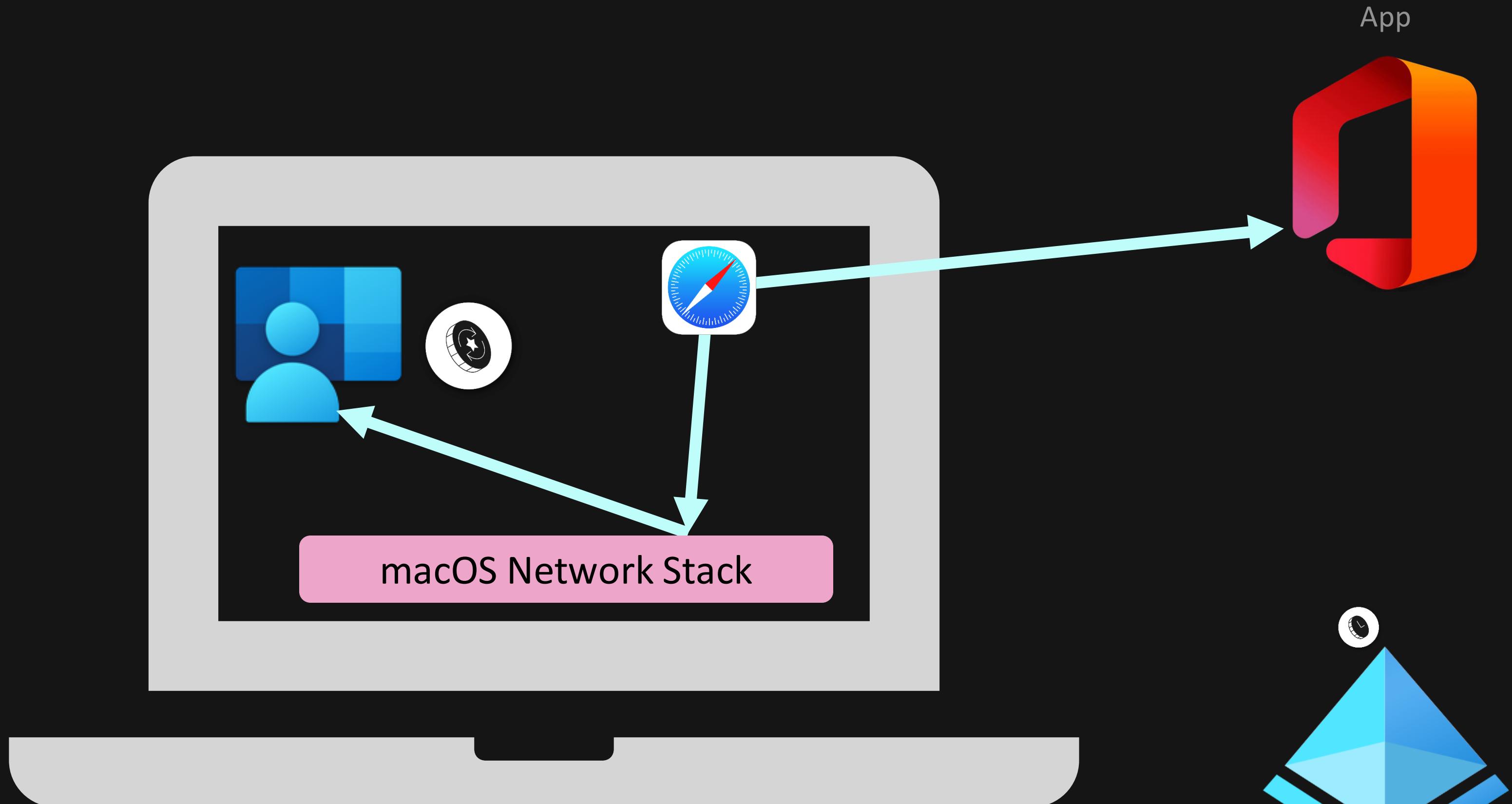
- App that uses MSAL talks to the SSO Extension directly, asks it to get a token
- AAD validates the PRT and returns the app-specific token
- The token is given to the client and the client sends the token to the app
- The user successfully accesses the app



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 < >

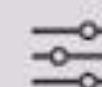


Search or enter website name



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 Document Media Other >

URL Contains login

Show: ⌘F New: ⌘N Remove: ⌘N Up: ⌘↑ Down: ⌘↓ On/Off: ⌘B Hide: ESC

ID	URL	Client	Method	Status	Code	Time
285	https://in.appcenter.ms	Proxyman	CONNECT	Completed	200	22:4
302	https://alive.github.com	Microsoft Edge Helper	CONNECT	Active		22:4
303	https://teams.events.data.microsoft.com	Microsoft Teams Helper	CONNECT	Active		22:4
304	https://in.appcenter.ms	Proxyman	CONNECT	Active		22:4
305	https://api.june.so	Screen Studio Helper	CONNECT	Active		22:4
306	https://config.teams.microsoft.com	Microsoft Teams Helper	CONNECT	Active		22:4

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

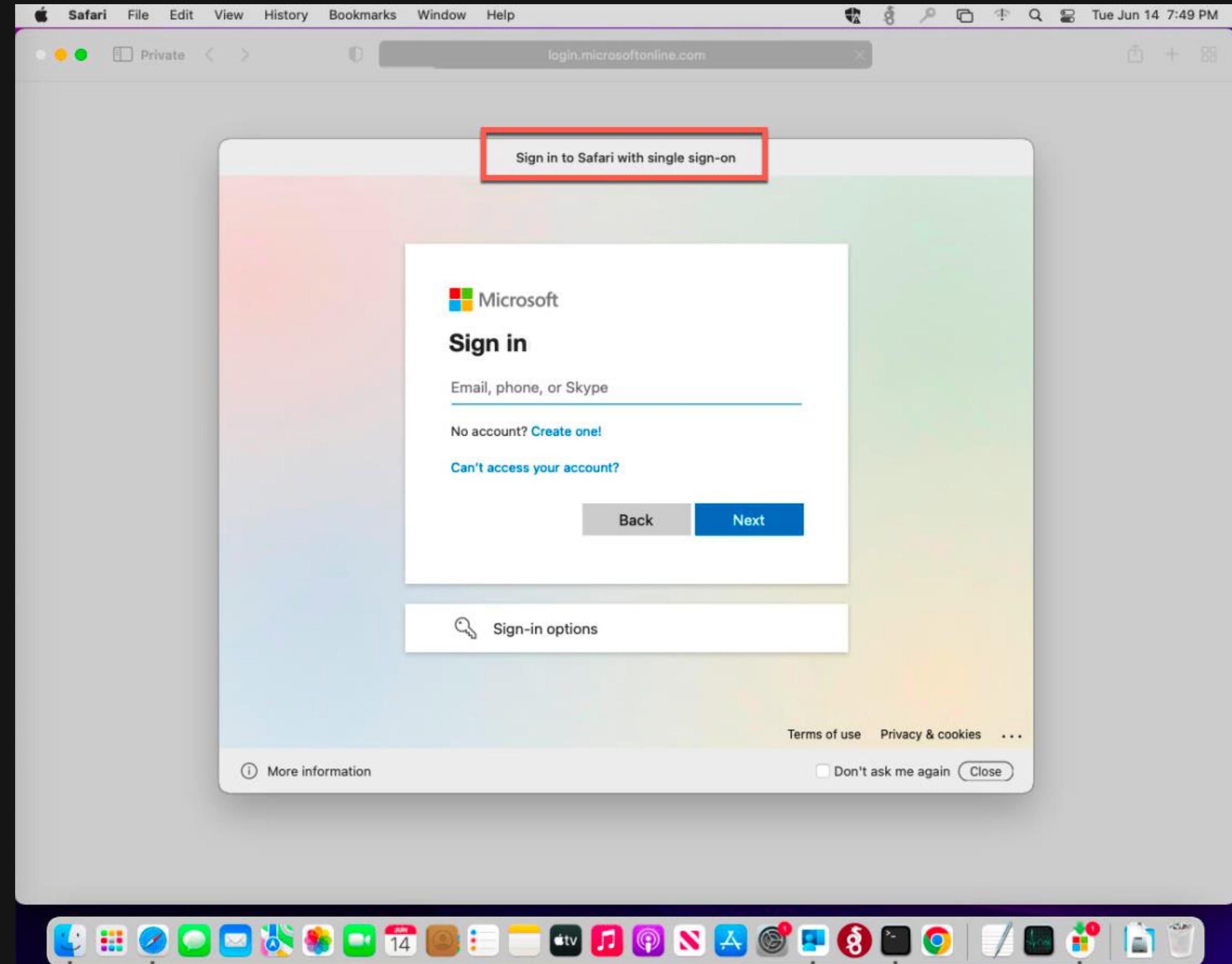
The screenshot shows the 'Computers : Configuration Profiles' screen. A new configuration profile for 'Azure AD SSO Extension for macOS' is being created. In the 'Single Sign-on Extensions' section, under 'Payload Type', 'Kerberos' is selected. Under 'Extension Identifier', the value 'com.microsoft.CompanyPortalMac.ssoextension' is entered. Under 'Team Identifier', the value 'UBF8T346G9' is entered. Under 'Sign-On Type', 'Redirect' is selected. At the bottom, there is a URL input field with the placeholder 'URLs'.

The screenshot shows the configuration profile details for 'Azure AD SSO Extension for macOS'. In the 'Single Sign-On Extensions' section, it shows 1 payload configured. The 'URLs' section lists several 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.de, https://login.microsoftonline.us, and https://login.usgovcloudapi.net. The 'Save' button is visible at the bottom right.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PLIST_1.0.dtd">
<plist version="1.0">
<dict>
    <key>AppPrefixAllowList</key>
    <string>com.microsoft.,com.apple.</string>
    <key>browser_sso_interaction_enabled</key>
    <integer>1</integer>
    <key>disable_explicit_app_prompt</key>
    <integer>1</integer>
</dict>
</plist>
```

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?

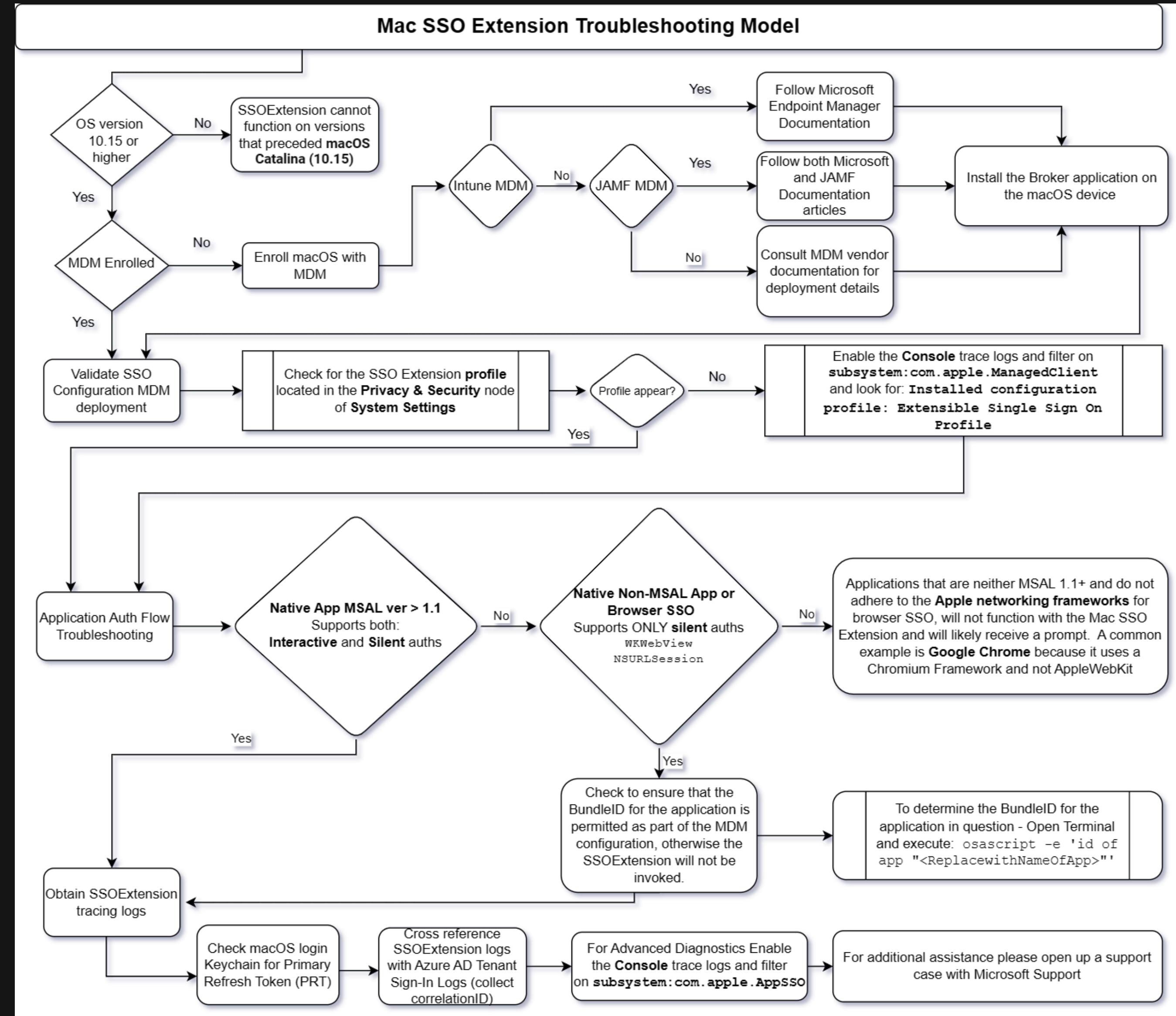
Prompting...why is it bad?

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

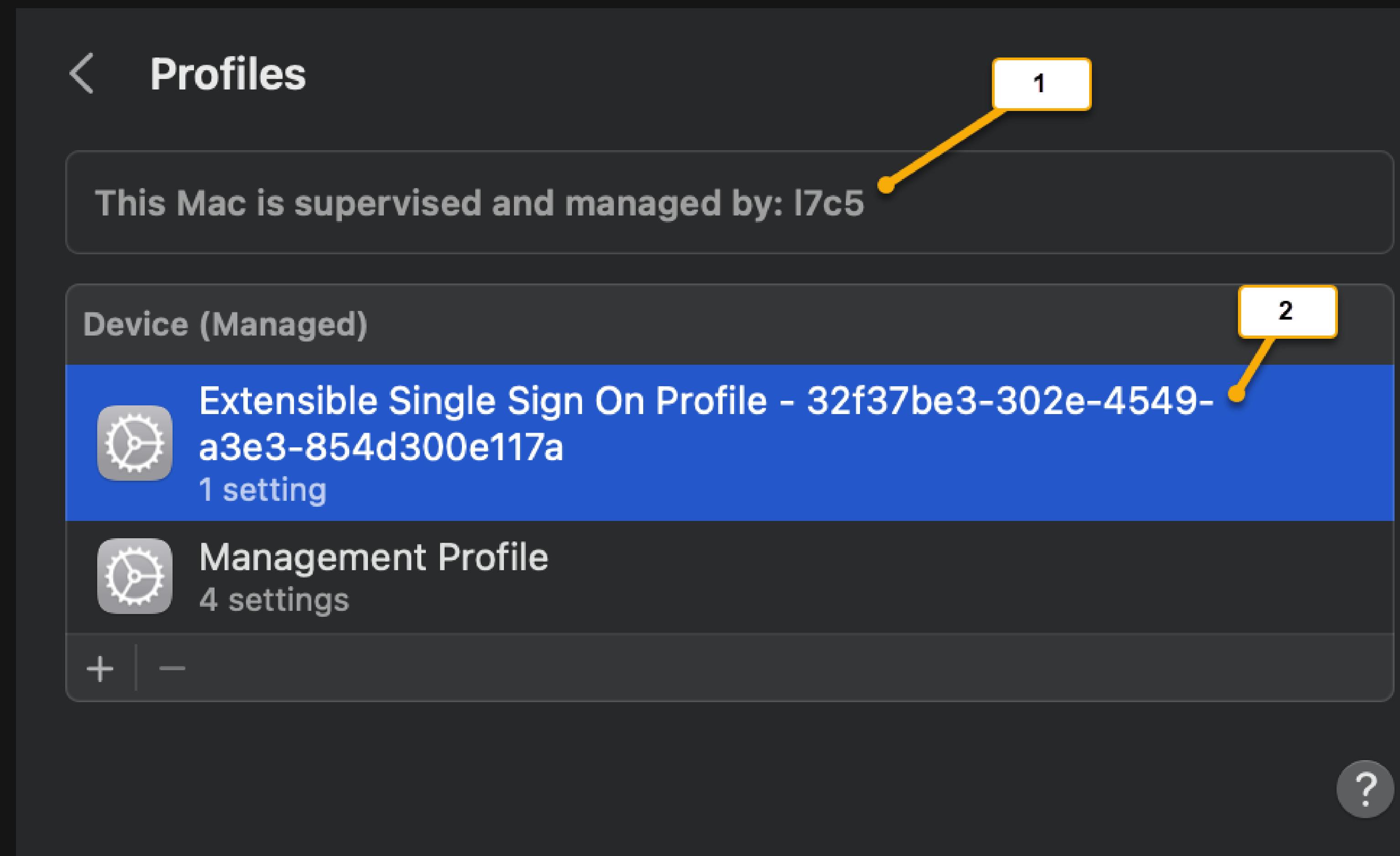
Deploying Enterprise SSO

Troubleshooting Enterprise SSO

Troubleshooting Enterprise SSO



Locate SSO extension MDM profile



Verify the extension configuration

Extensible Single Sign On Profile - 32f37be3-302e-4549-a3e3-854d300e117a
l7c5 Verified

Description The configuration profile enables your company's technical support to enforce security policies on your mobile device

Signed AppleConfigProfileSigning.manage.microsoft.com

Installed Dec 26, 2022 at 3:53 PM

Settings Single Sign On Extension

Details

Single Sign On Extension

Description Extensible Single Sign On Profile - 32f37be3-302e-4549-a3e3-854d300e117a

Extension com.microsoft.CompanyPortalMac.ssoextension (UBF8T346G9)

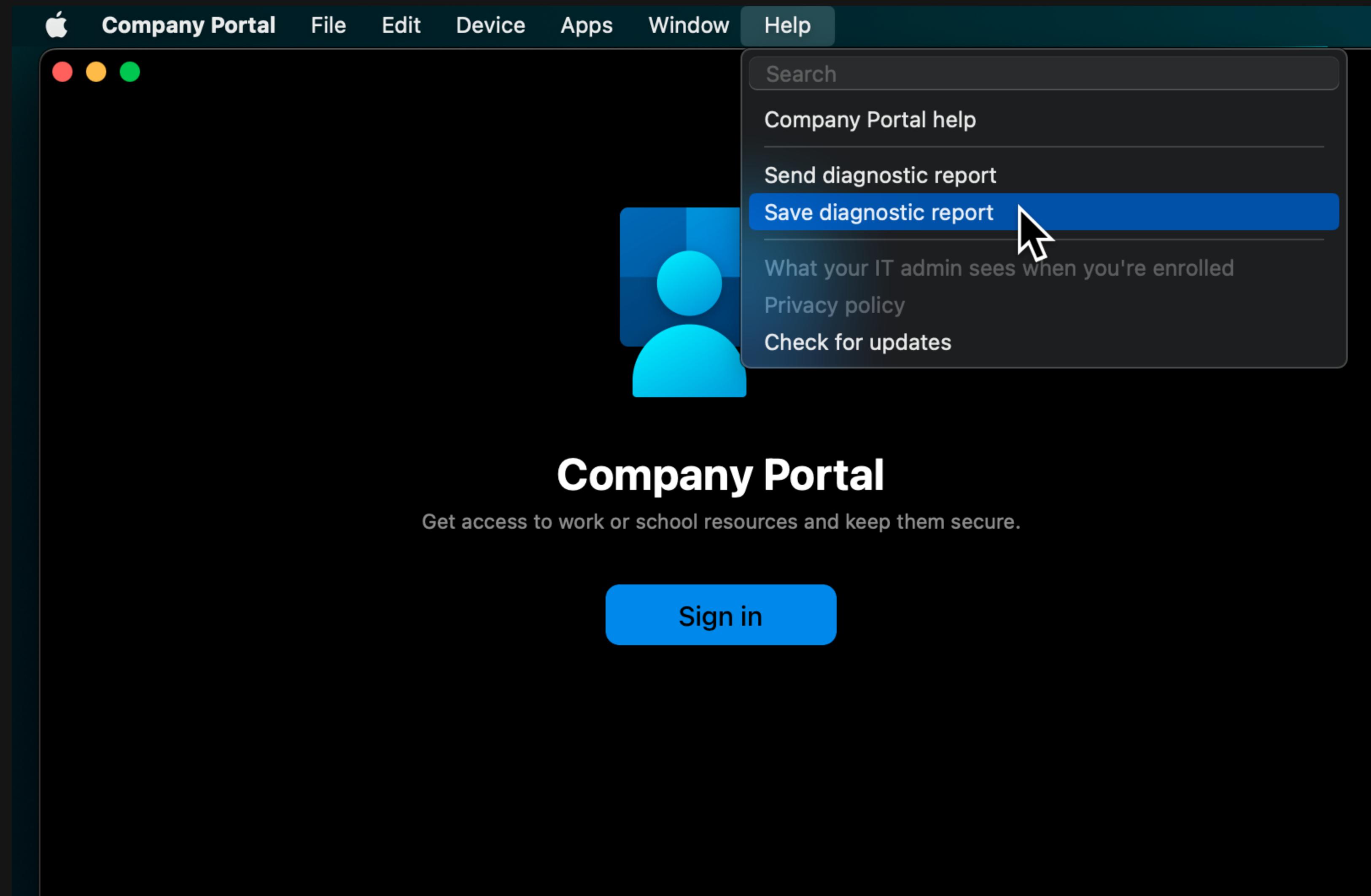
Type Redirect

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.de
https://login.microsoftonline.us

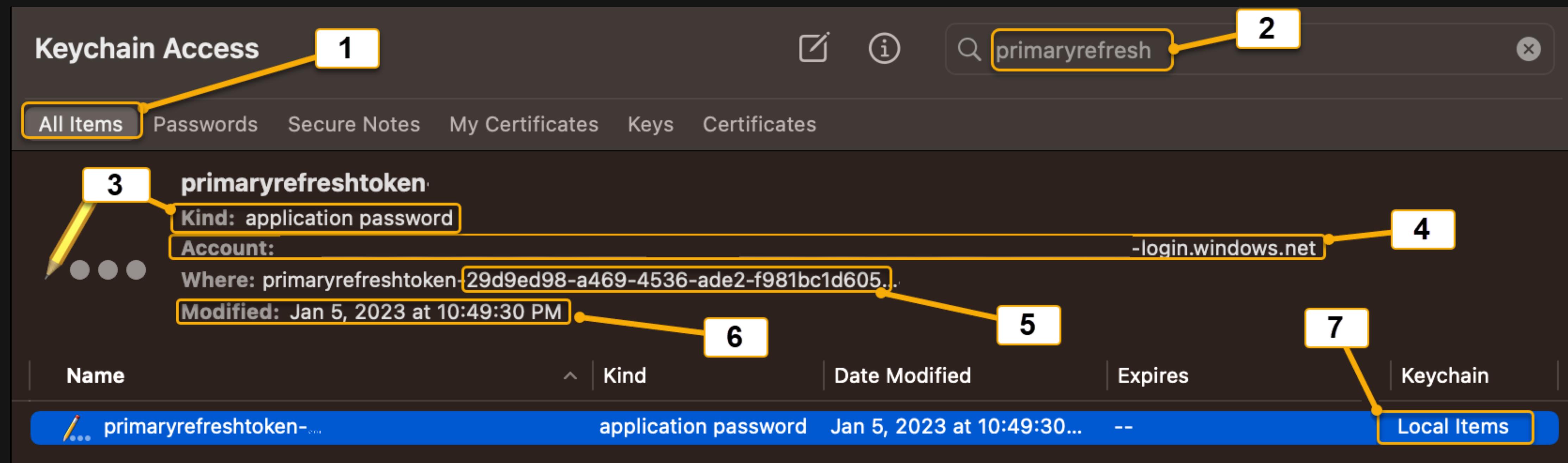
OK

- 1 Signed AppleConfigProfileSigning.manage.microsoft.com
- 2 Installed Dec 26, 2022 at 3:53 PM
- 3 Single Sign On Extension
- 4 com.microsoft.CompanyPortalMac.ssoextension
- 5 Redirect
- 6 https://login.microsoftonline.com
https://login.microsoft.com
https://sts.windows.net
https://login.partner.microsoftonline.cn
https://login.chinacloudapi.cn
https://login.microsoftonline.de
https://login.microsoftonline.us

Collect Enterprise SSO logs



Check keychain access for PRT



Troubleshooting Script

The screenshot shows a GitHub repository page for "AzureAD/Apple-SSO-Tools". The repository is public and contains one branch and no tags. The README.md file is open, displaying the following content:

Apple SSO Tools

The Apple SSO Tools repo is a collection of scripts for troubleshooting common issues with features such as the [Microsoft Enterprise SSO Extension Plugin](#).

For additional troubleshooting guidance please read the [Troubleshooting the Microsoft Enterprise SSO Extension plugin on Apple Devices](#)

SSOE Troubleshooter

The SSOE Troubleshooter is made up of 3 scripts written in zsh.

- 1.) SSOETroubleshoot.zsh - This is the main launching script.
- 2.) checkurls.sh - This is used to do network connectivity checks to the proper urls.
- 3.) featureflags.zsh - This is used to check common configuration settings pushed down from the MDM.

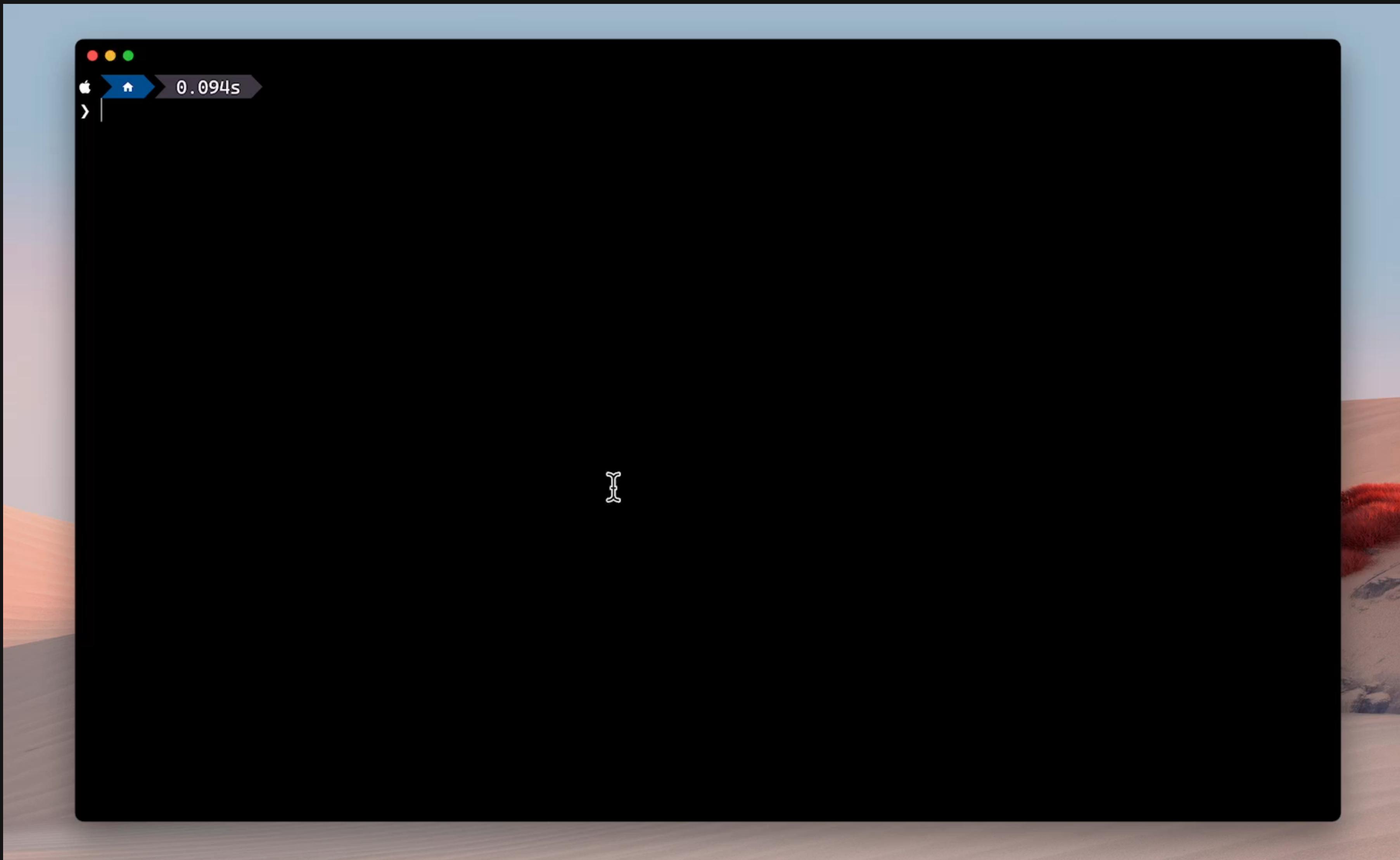
The repository has 1 fork and 6 stars. It includes links to the Readme, MIT license, Code of conduct, Security policy, and Report repository. Contributors listed are microsoftopensource and MarkMorow.

```
● ● ●
● Apple-SSO-Tools └─ main └─ 51.815s
> ./SSOETroubleshoot.zsh

Welcome to the macOS Enterprise SSO Troubleshooting Ulility

Please enter 1 to Check Network Connectivity
Please enter 2 to Check Configuration
Please enter q to quit
2
Executing featureflags.zsh script...
Feature Flag Name Value
browser_sso_interaction_enabled true
browser_sso_user_interaction_disabled false
disable_explicit_app_prompt_and_autologin true
SSOUIPromptDateKey Mon May 15 18:51:12 AEST 2023
bundleIdOfAppShowingUI com.apple.Safari
AppPrefixAllowList:PrefixElement com.adobe.
AppAllowList:AllowElement com.microsoft.Outlook
AppAllowList:AllowElement com.microsoft.teams
AppAllowList:AllowElement com.microsoft.edgemac
AppAllowList:AllowElement com.microsoft.Word
AppAllowList:AllowElement com.microsoft.onenote.mac
AppAllowList:AllowElement com.microsoft.OneDrive-Mac
AppAllowList:AllowElement com.microsoft.edgemac.local
AppAllowList:AllowElement com.microsoft.OneDrive
AppAllowList:AllowElement com.microsoft.Excel
AppAllowList:AllowElement com.microsoft.PowerPoint
AppAllowList:AllowElement com.microsoft.to-do-mac-dogfood
AppAllowList:AllowElement com.microsoft.to-do-mac
AppAllowList:AllowElement com.paloaltonetworks.GlobalProtect.client
```

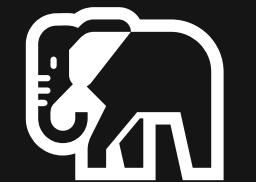
Troubleshooting Demo



Questions?

Thank You

 [@merill](https://twitter.com/merill)

 @merill@infosec.exchange

MacAdmins | [@merill](https://twitter.com/merill) | #microsoft-aad