Microsoft Security

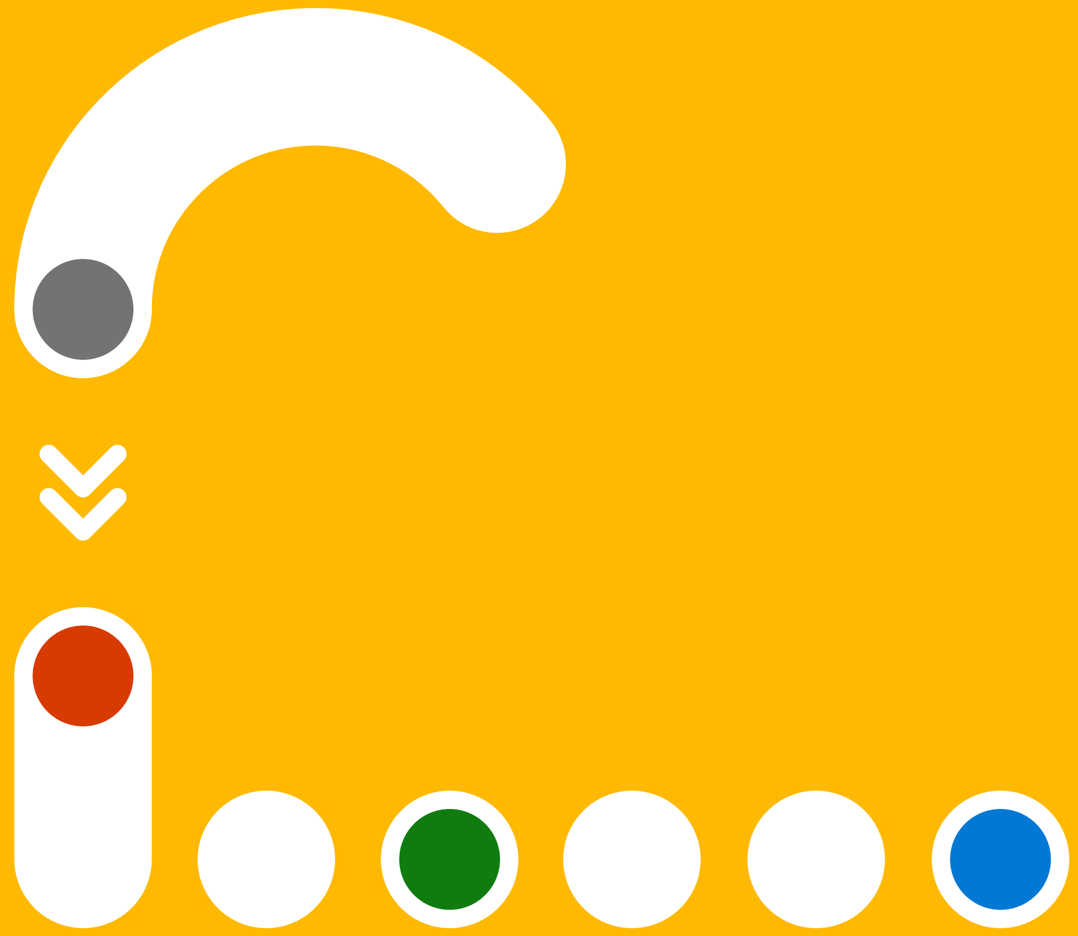
Microsoft Enterprise SSO Extension – What's New

Michael Epping
Senior Product Manager –
Microsoft Security CxE

Agenda

- What is Microsoft Entra
- Microsoft Enterprise SSO Extension General Availability
- Partner Integrations
- What’s Next
- Go Dos

What is Microsoft Entra



Microsoft Entra Product Family

Identity & access management

- Microsoft Entra ID
- Microsoft Entra ID Governance
- Microsoft Entra External ID

New Identity categories

- Microsoft Entra Verified ID
- Microsoft Entra Permissions Management
- Microsoft Entra Workload ID

Network Access

- Microsoft Entra Internet Access
- Microsoft Entra Private Access

Microsoft Enterprise SSO Extension General Availability

General Availability

- “When is it going GA” - this was the top question we received for years
- GA = April 10th, 2023
- Deployment guide: https://aka.ms/AppleSSO-Intune

macOS GA

- Usage has grown greatly since GA
  - Still lots of room for improvement
- Lots of bugs fixed both before and after GA
- Working with MDMs like Intune and Jamf to consider deploying SSO Extension by default

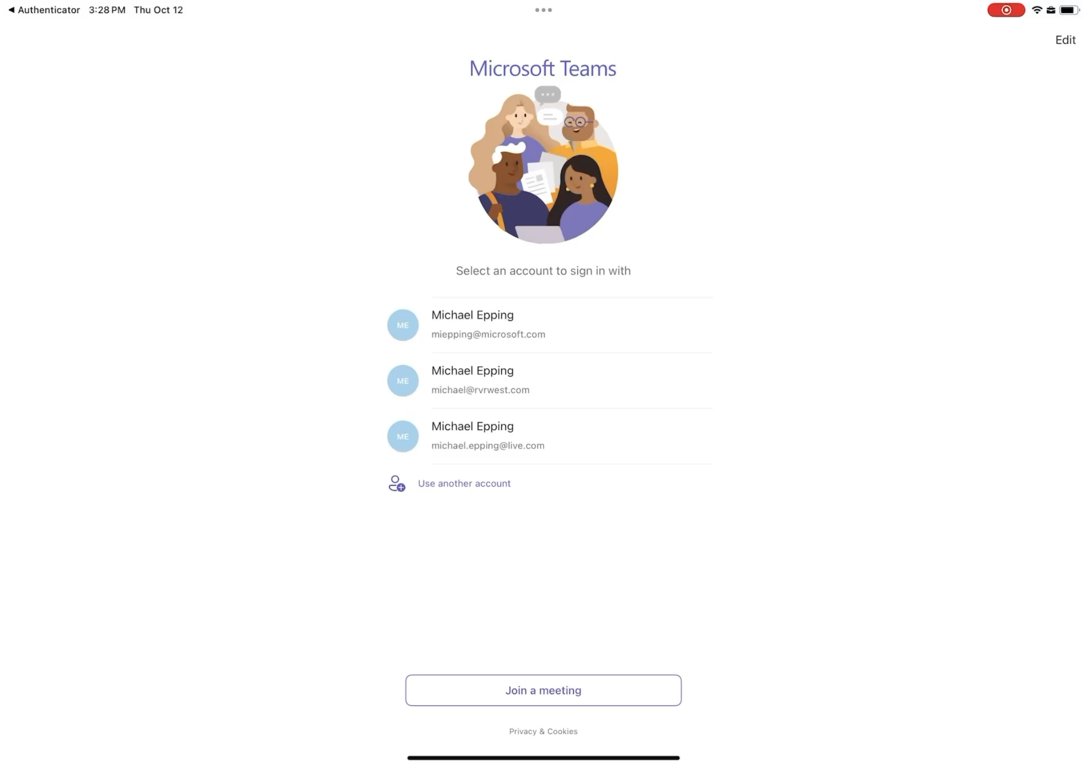
Private Browsing Enabled

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.

Safari does not keep cross-site tracker statistics in Private Browsing.

iOS GA

- Growth has been much slower on iOS
- Why…?
- Theory:
  - SSO for mobile apps is less broken on iOS for *some* organizations
  - Users use fewer web apps on iOS compared to macOS
- How does SSO work on iOS?
  1. Authenticator App without SSO Extension present



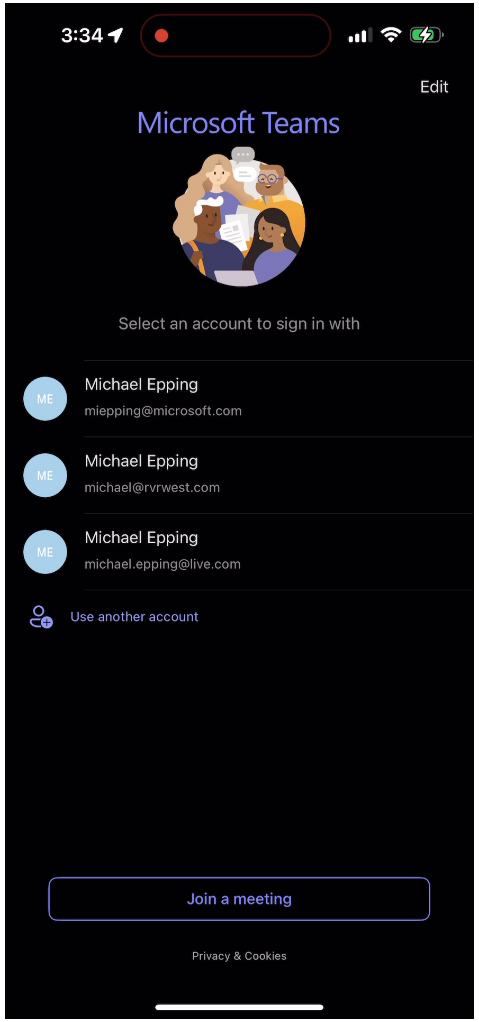
Microsoft Teams

Select an account to sign in with

- Michael Epping
  miepping@microsoft.com
- Michael Epping
  michael@rvrwest.com
- Michael Epping
  michael.epping@live.com
- Use another account

iOS GA

- Growth has been much slower on iOS
- Why…?
- Theory:
  - SSO for mobile apps is less broken on iOS for *some* organizations
  - Users use fewer web apps on iOS compared to macOS
- How does SSO work on iOS?
  1. Authenticator App without SSO Extension present
  2. SSO Extension present



3:34

Edit

Microsoft Teams

Select an account to sign in with

ME Michael Epping
miepping@microsoft.com

ME Michael Epping
michael@rvrwest.com

ME Michael Epping
michael.epping@live.com

Use another account

Join a meeting

Privacy & Cookies

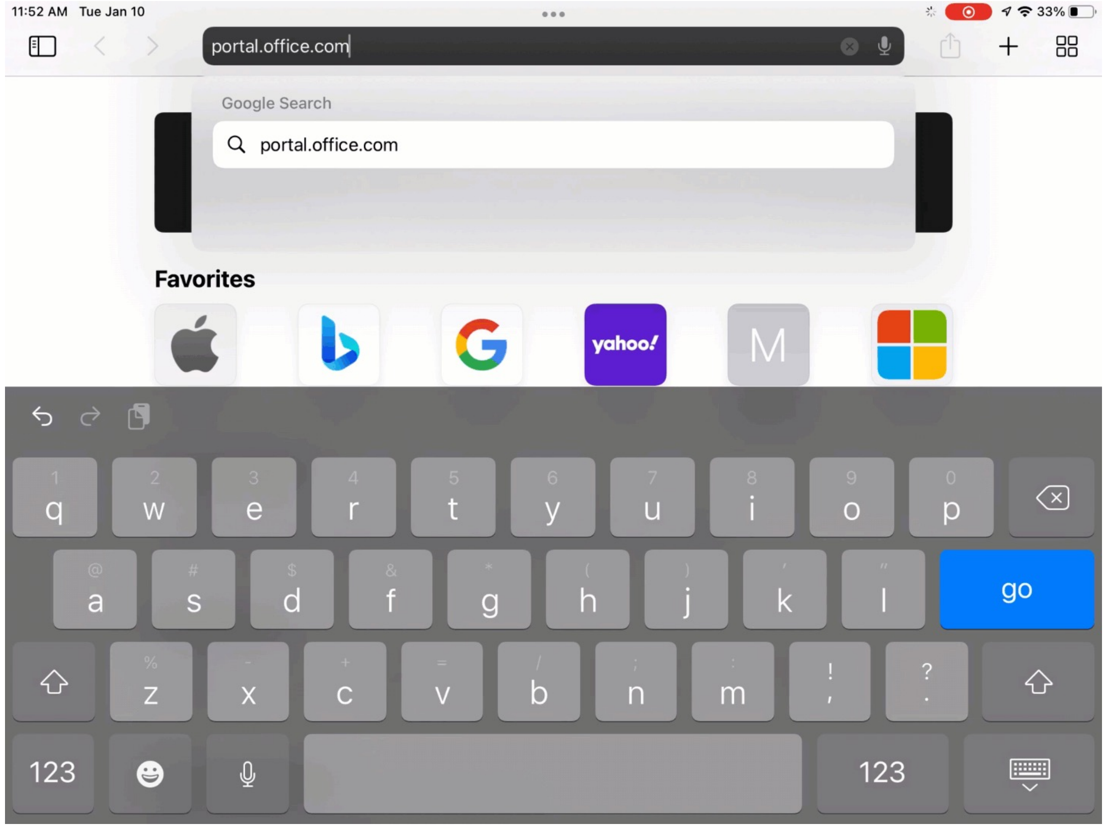
iOS GA

- Growth has been much slower on iOS
- Why…?
- Theory:
  - SSO for mobile apps is less broken on iOS for *some* organizations
  - Users use fewer web apps on iOS compared to macOS
- How does SSO work on iOS?
  1. Authenticator App without SSO Extension present
  2. SSO Extension present

- Users on iOS have better user experiences without the SSO Extension, fewer web apps, and more BYOD
- Orgs are under less pressure to fix user experience on iOS because its already better

iOS GA

- Deploy the SSO Extension for iOS anyways!
  - Premier user experience
  - Future features will require it, such as token binding



11:52 AM Tue Jan 10

33%

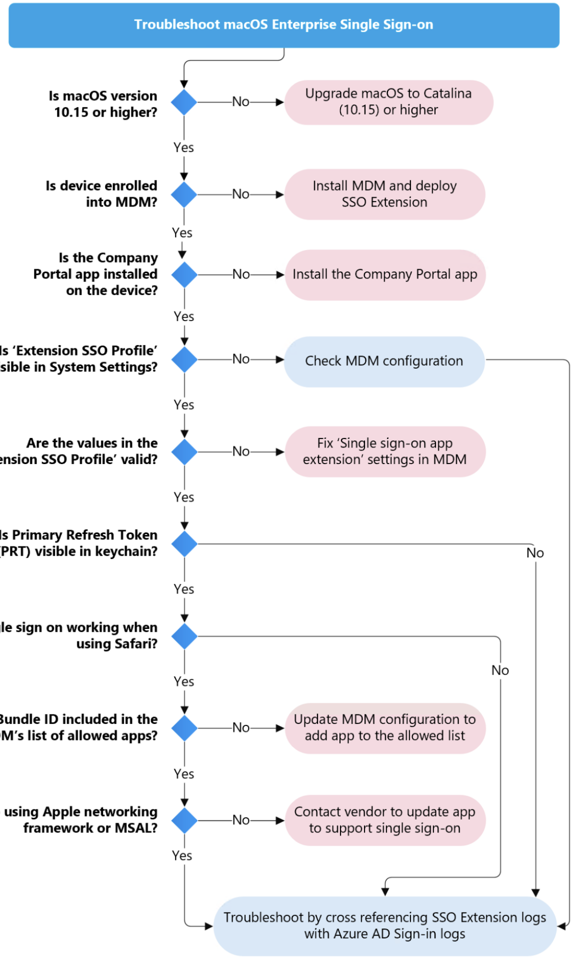
portal.office.com

Google Search

portal.office.com

Favorites

SSO Extension Troubleshooting Guide



Troubleshoot macOS Enterprise Single Sign-on

Is macOS version 10.15 or higher? — No → Upgrade macOS to Catalina (10.15) or higher

Yes

Is device enrolled into MDM? — No → Install MDM and deploy SSO Extension

Yes

Is the Company Portal app installed on the device? — No → Install the Company Portal app

Yes

Is 'Extension SSO Profile' visible in System Settings? — No → Check MDM configuration

Yes

Are the values in the 'Extension SSO Profile' valid? — No → Fix 'Single sign-on app extension' settings in MDM

Yes

Is Primary Refresh Token (PRT) visible in keychain? — No

Yes

Is single sign on working when using Safari? — No

Yes

Is app's Bundle ID included in the MDM's list of allowed apps? — No → Update MDM configuration to add app to the allowed list

Yes

Is app using Apple networking framework or MSAL? — No → Contact vendor to update app to support single sign-on

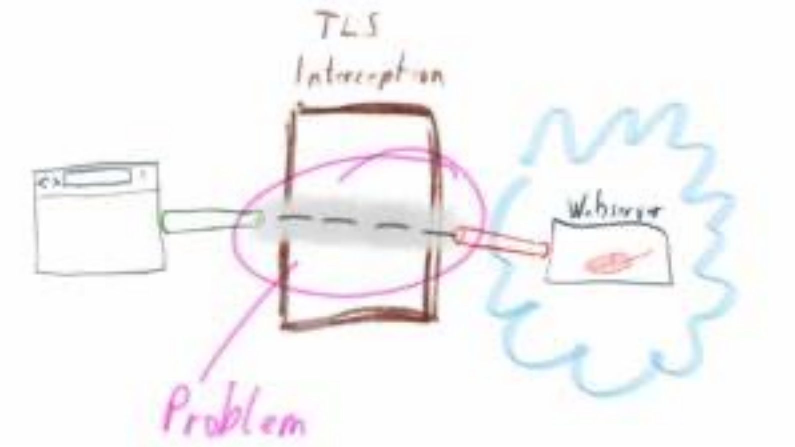
Yes

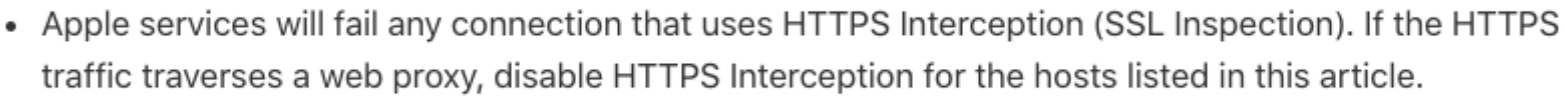
Troubleshoot by cross referencing SSO Extension logs with Azure AD Sign-in logs

- Helps you understand the inner workings of the SSO Extension and its logs
- Solve common issues without calling support
- Support is still there if you need it, of course

TLS Inspection

- This is the most common support issue by a *huge* margin
- Certain Apple hosts must be exempted from any TLS inspection/interception for SSO to work:
  - app-site-association.cdn-apple.com
  - app-site-association.networking.apple

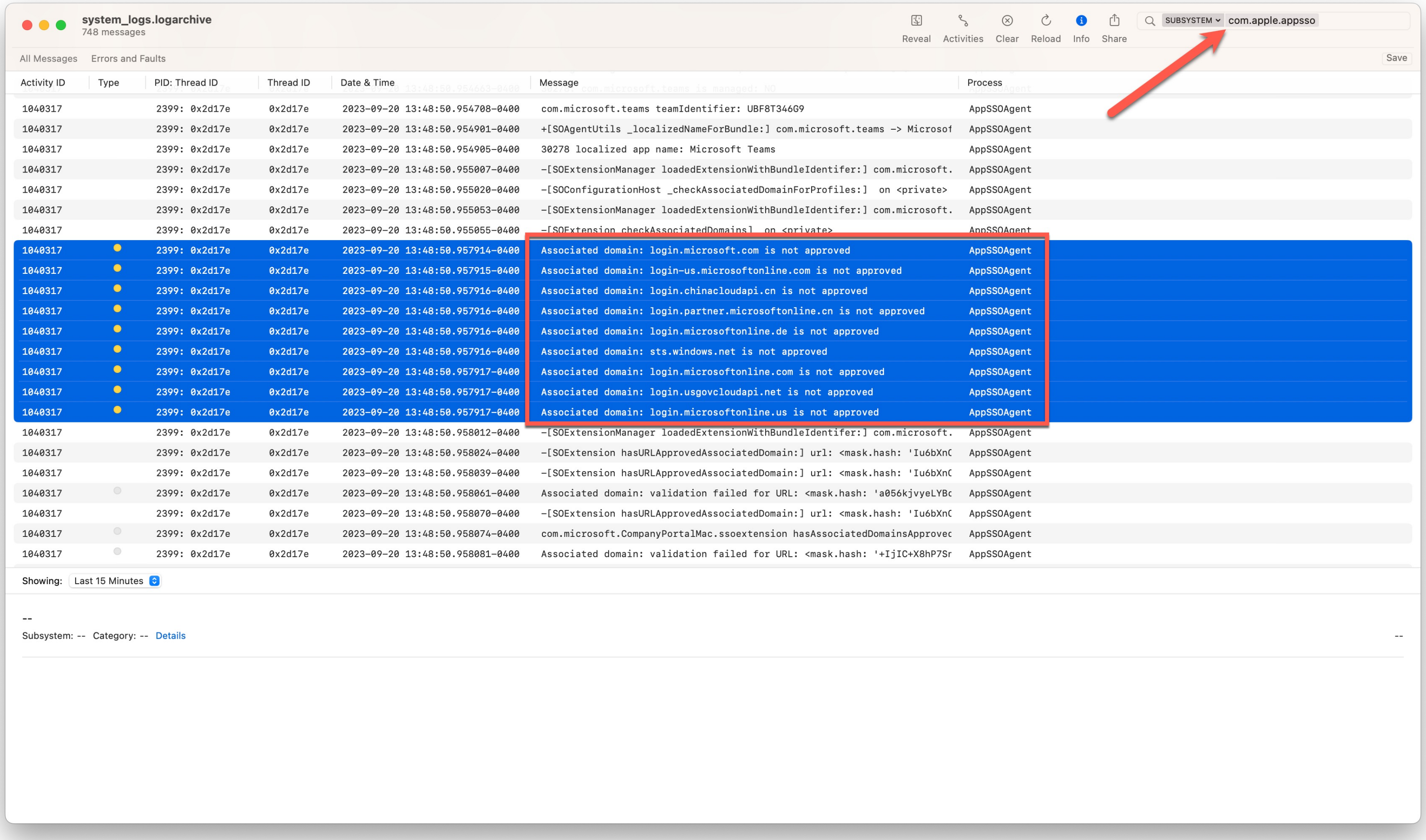




- Apple services will fail any connection that uses HTTPS Interception (SSL Inspection). If the HTTPS traffic traverses a web proxy, disable HTTPS Interception for the hosts listed in this article.

https://support.apple.com/en-us/HT210060

Finding TLS Inspection - sysdiagnose



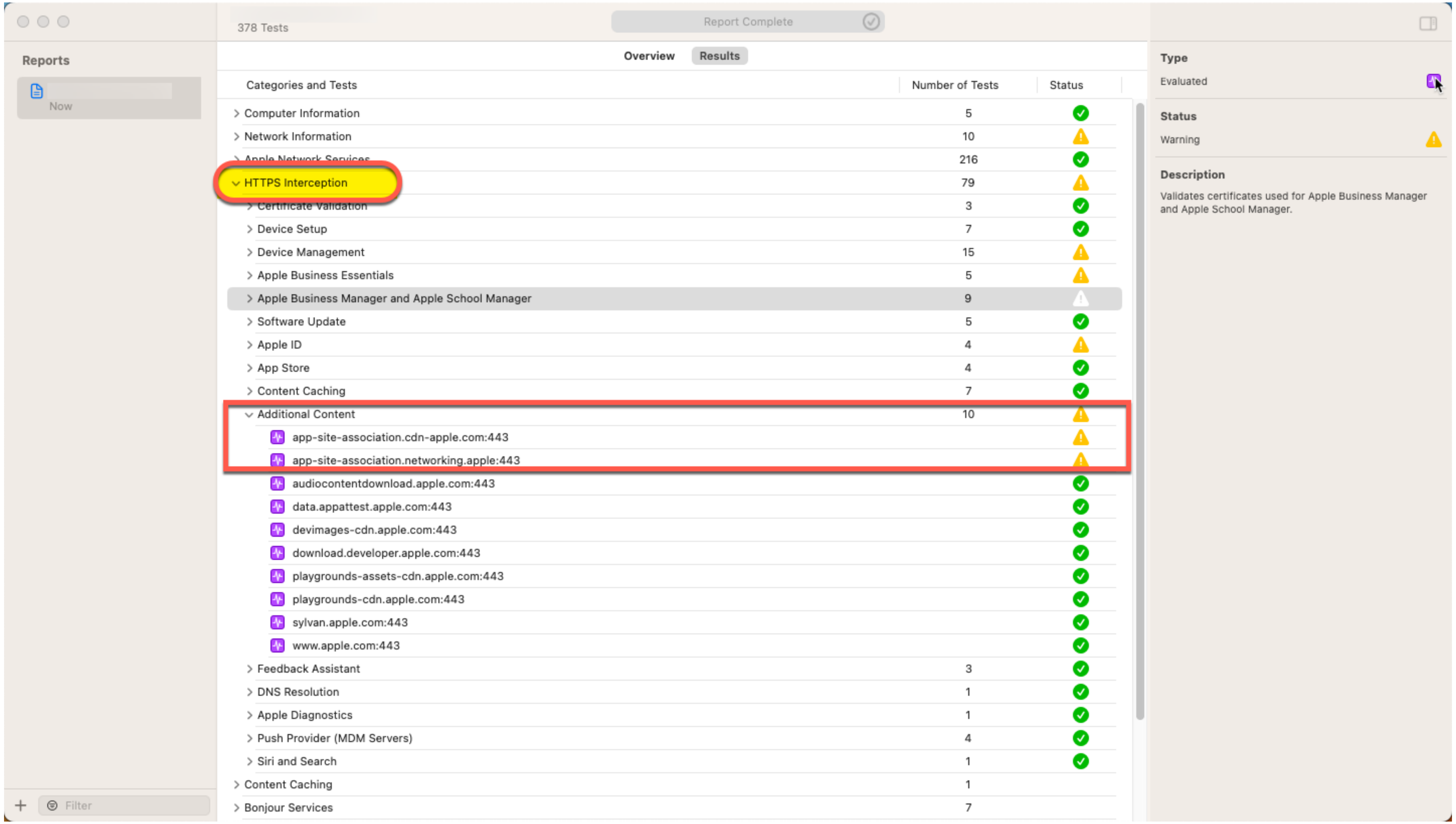
```
Activity ID  Type  PID: Thread ID   Thread ID  Date & Time                          Message                                                                Process
1040317            2399: 0x2d17e    0x2d17e    2023-09-20 13:48:50.954708-0400      com.microsoft.teams teamIdentifier: UBF8T346G9                         AppSSOAgent
1040317            2399: 0x2d17e    0x2d17e    2023-09-20 13:48:50.954901-0400      +[SOAgentUtils _localizedNameForBundle:] com.microsoft.teams -> Microsof AppSSOAgent
1040317            2399: 0x2d17e    0x2d17e    2023-09-20 13:48:50.954905-0400      30278 localized app name: Microsoft Teams                              AppSSOAgent
1040317            2399: 0x2d17e    0x2d17e    2023-09-20 13:48:50.955007-0400      -[SOExtensionManager loadedExtensionWithBundleIdentifer:] com.microsoft. AppSSOAgent
1040317            2399: 0x2d17e    0x2d17e    2023-09-20 13:48:50.955020-0400      -[SOConfigurationHost _checkAssociatedDomainForProfiles:]  on <private> AppSSOAgent
1040317            2399: 0x2d17e    0x2d17e    2023-09-20 13:48:50.955053-0400      -[SOExtensionManager loadedExtensionWithBundleIdentifer:] com.microsoft. AppSSOAgent
1040317            2399: 0x2d17e    0x2d17e    2023-09-20 13:48:50.955055-0400      -[SOExtension checkAssociatedDomains]  on <private>                    AppSSOAgent
1040317      ●     2399: 0x2d17e    0x2d17e    2023-09-20 13:48:50.957914-0400      Associated domain: login.microsoft.com is not approved                 AppSSOAgent
1040317      ●     2399: 0x2d17e    0x2d17e    2023-09-20 13:48:50.957915-0400      Associated domain: login-us.microsoftonline.com is not approved        AppSSOAgent
1040317      ●     2399: 0x2d17e    0x2d17e    2023-09-20 13:48:50.957916-0400      Associated domain: login.chinacloudapi.cn is not approved              AppSSOAgent
1040317      ●     2399: 0x2d17e    0x2d17e    2023-09-20 13:48:50.957916-0400      Associated domain: login.partner.microsoftonline.cn is not approved    AppSSOAgent
1040317      ●     2399: 0x2d17e    0x2d17e    2023-09-20 13:48:50.957916-0400      Associated domain: login.microsoftonline.de is not approved            AppSSOAgent
1040317      ●     2399: 0x2d17e    0x2d17e    2023-09-20 13:48:50.957916-0400      Associated domain: sts.windows.net is not approved                     AppSSOAgent
1040317      ●     2399: 0x2d17e    0x2d17e    2023-09-20 13:48:50.957917-0400      Associated domain: login.microsoftonline.com is not approved           AppSSOAgent
1040317      ●     2399: 0x2d17e    0x2d17e    2023-09-20 13:48:50.957917-0400      Associated domain: login.usgovcloudapi.net is not approved             AppSSOAgent
1040317      ●     2399: 0x2d17e    0x2d17e    2023-09-20 13:48:50.957917-0400      Associated domain: login.microsoftonline.us is not approved            AppSSOAgent
1040317            2399: 0x2d17e    0x2d17e    2023-09-20 13:48:50.958012-0400      -[SOExtensionManager loadedExtensionWithBundleIdentifer:] com.microsoft. AppSSOAgent
1040317            2399: 0x2d17e    0x2d17e    2023-09-20 13:48:50.958024-0400      -[SOExtension hasURLApprovedAssociatedDomain:] url: <mask.hash: 'Iu6bXn( AppSSOAgent
1040317            2399: 0x2d17e    0x2d17e    2023-09-20 13:48:50.958039-0400      -[SOExtension hasURLApprovedAssociatedDomain:] url: <mask.hash: 'Iu6bXn( AppSSOAgent
1040317      ○     2399: 0x2d17e    0x2d17e    2023-09-20 13:48:50.958061-0400      Associated domain: validation failed for URL: <mask.hash: 'a056kjvyeLYBc AppSSOAgent
1040317            2399: 0x2d17e    0x2d17e    2023-09-20 13:48:50.958070-0400      -[SOExtension hasURLApprovedAssociatedDomain:] url: <mask.hash: 'Iu6bXn( AppSSOAgent
1040317      ○     2399: 0x2d17e    0x2d17e    2023-09-20 13:48:50.958074-0400      com.microsoft.CompanyPortalMac.ssoextension hasAssociatedDomainsApprovec AppSSOAgent
1040317      ○     2399: 0x2d17e    0x2d17e    2023-09-20 13:48:50.958081-0400      Associated domain: validation failed for URL: <mask.hash: '+IjIC+X8hP7Sr AppSSOAgent
```

Showing: Last 15 Minutes

--

Subsystem: -- Category: -- Details --

Finding TLS Inspection - Mac Evaluation Utility



Reports

[redacted]
Now

378 Tests

Report Complete

Overview | Results

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	✓
› Push Provider (MDM Servers)	4	✓
› Siri and Search	1	✓
› Content Caching	1	
› Bonjour Services	7	

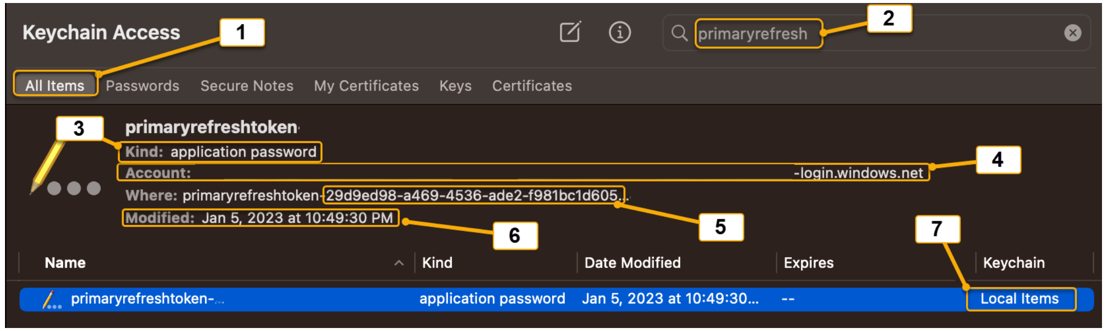
Type
Evaluated

Status
Warning ⚠

Description
Validates certificates used for Apple Business Manager and Apple School Manager.

Other Troubleshooting Steps

- Check for the existence of the Primary Refresh Token
  - Note: the PRT will no longer appear in the keychain in the future w/ some PSSO configurations



primaryrefreshtoken

Kind: application password

Account: -login.windows.net

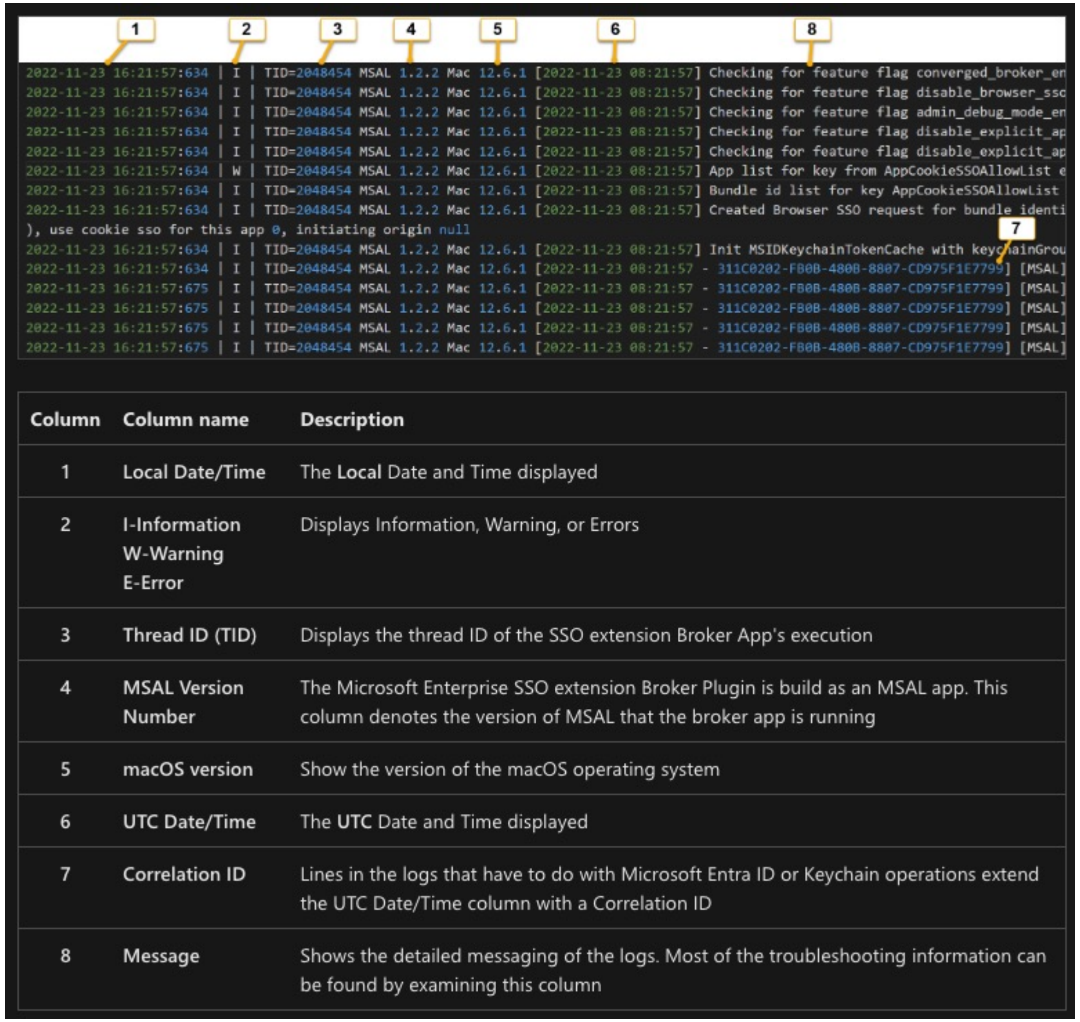
Where: primaryrefreshtoken-29d9ed98-a469-4536-ade2-f981bc1d605...

Modified: Jan 5, 2023 at 10:49:30 PM

Name	Kind	Date Modified	Expires	Keychain
primaryrefreshtoken-...	application password	Jan 5, 2023 at 10:49:30...	--	Local Items

Other Troubleshooting Steps

- Check for the existence of the Primary Refresh Token
  - Note: the PRT will no longer appear in the keychain in the future w/ some PSSO configurations
- Check the SSO Extension logs



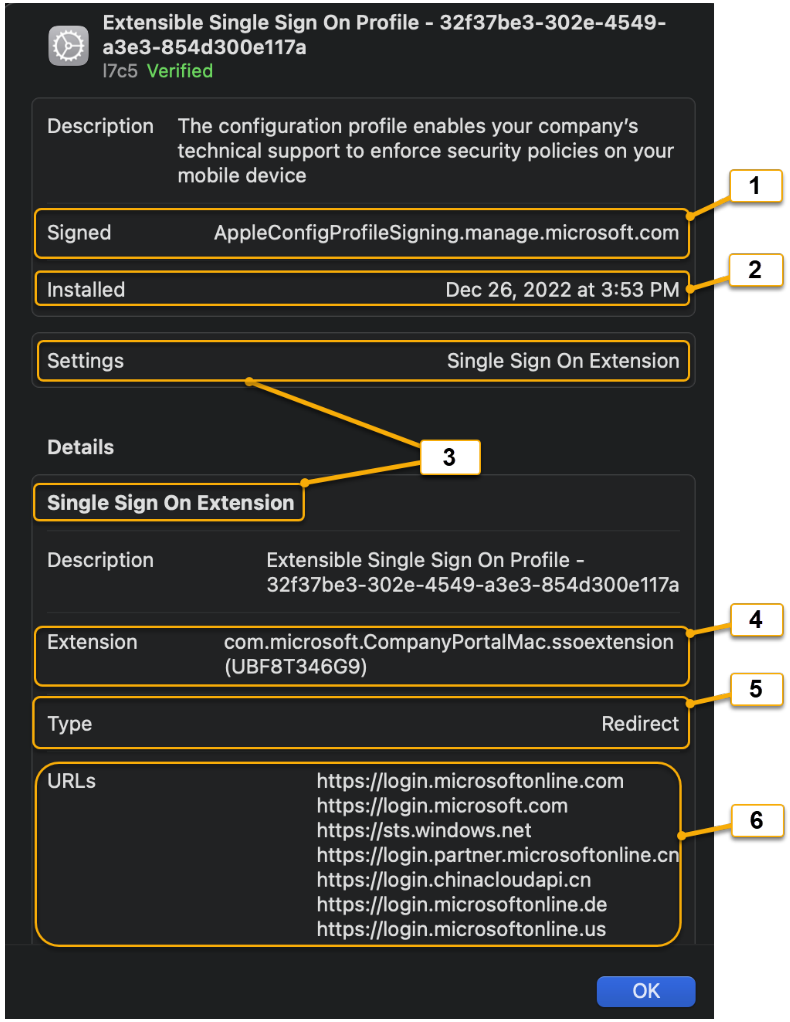
```
2022-11-23 16:21:57:634 | I | TID=2048454 MSAL 1.2.2 Mac 12.6.1 [2022-11-23 08:21:57] Checking for feature flag converged_broker_en
2022-11-23 16:21:57:634 | I | TID=2048454 MSAL 1.2.2 Mac 12.6.1 [2022-11-23 08:21:57] Checking for feature flag disable_browser_ssc
2022-11-23 16:21:57:634 | I | TID=2048454 MSAL 1.2.2 Mac 12.6.1 [2022-11-23 08:21:57] Checking for feature flag admin_debug_mode_en
2022-11-23 16:21:57:634 | I | TID=2048454 MSAL 1.2.2 Mac 12.6.1 [2022-11-23 08:21:57] Checking for feature flag disable_explicit_ap
2022-11-23 16:21:57:634 | I | TID=2048454 MSAL 1.2.2 Mac 12.6.1 [2022-11-23 08:21:57] Checking for feature flag disable_explicit_ap
2022-11-23 16:21:57:634 | W | TID=2048454 MSAL 1.2.2 Mac 12.6.1 [2022-11-23 08:21:57] App list for key from AppCookieSSOAllowList e
2022-11-23 16:21:57:634 | I | TID=2048454 MSAL 1.2.2 Mac 12.6.1 [2022-11-23 08:21:57] Bundle id list for key AppCookieSSOAllowList
2022-11-23 16:21:57:634 | I | TID=2048454 MSAL 1.2.2 Mac 12.6.1 [2022-11-23 08:21:57] Created Browser SSO request for bundle identi
), use cookie sso for this app 0, initiating origin null
2022-11-23 16:21:57:634 | I | TID=2048454 MSAL 1.2.2 Mac 12.6.1 [2022-11-23 08:21:57] Init MSIDKeychainTokenCache with keychainGrou
2022-11-23 16:21:57:634 | I | TID=2048454 MSAL 1.2.2 Mac 12.6.1 [2022-11-23 08:21:57 - 311C0202-FB0B-480B-8807-CD975F1E7799] [MSAL]
2022-11-23 16:21:57:675 | I | TID=2048454 MSAL 1.2.2 Mac 12.6.1 [2022-11-23 08:21:57 - 311C0202-FB0B-480B-8807-CD975F1E7799] [MSAL]
2022-11-23 16:21:57:675 | I | TID=2048454 MSAL 1.2.2 Mac 12.6.1 [2022-11-23 08:21:57 - 311C0202-FB0B-480B-8807-CD975F1E7799] [MSAL]
2022-11-23 16:21:57:675 | I | TID=2048454 MSAL 1.2.2 Mac 12.6.1 [2022-11-23 08:21:57 - 311C0202-FB0B-480B-8807-CD975F1E7799] [MSAL]
2022-11-23 16:21:57:675 | I | TID=2048454 MSAL 1.2.2 Mac 12.6.1 [2022-11-23 08:21:57 - 311C0202-FB0B-480B-8807-CD975F1E7799] [MSAL]
```

Column	Column name	Description
1	Local Date/Time	The Local Date and Time displayed
2	I-Information W-Warning E-Error	Displays Information, Warning, or Errors
3	Thread ID (TID)	Displays the thread ID of the SSO extension Broker App's execution
4	MSAL Version Number	The Microsoft Enterprise SSO extension Broker Plugin is build as an MSAL app. This column denotes the version of MSAL that the broker app is running
5	macOS version	Show the version of the macOS operating system
6	UTC Date/Time	The UTC Date and Time displayed
7	Correlation ID	Lines in the logs that have to do with Microsoft Entra ID or Keychain operations extend the UTC Date/Time column with a Correlation ID
8	Message	Shows the detailed messaging of the logs. Most of the troubleshooting information can be found by examining this column

```
tail -F ~/Library/Containers/com.microsoft.CompanyPortalMac.ssoextension/Data/Library/Caches/Logs/Microsoft/SSOExtension/*
```

Other Troubleshooting Steps

- Check for the existence of the Primary Refresh Token
  - Note: the PRT will no longer appear in the keychain in the future w/ some PSSO configurations
- Check the SSO Extension logs
- Validate the SSO Extension profile exists on the local client



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

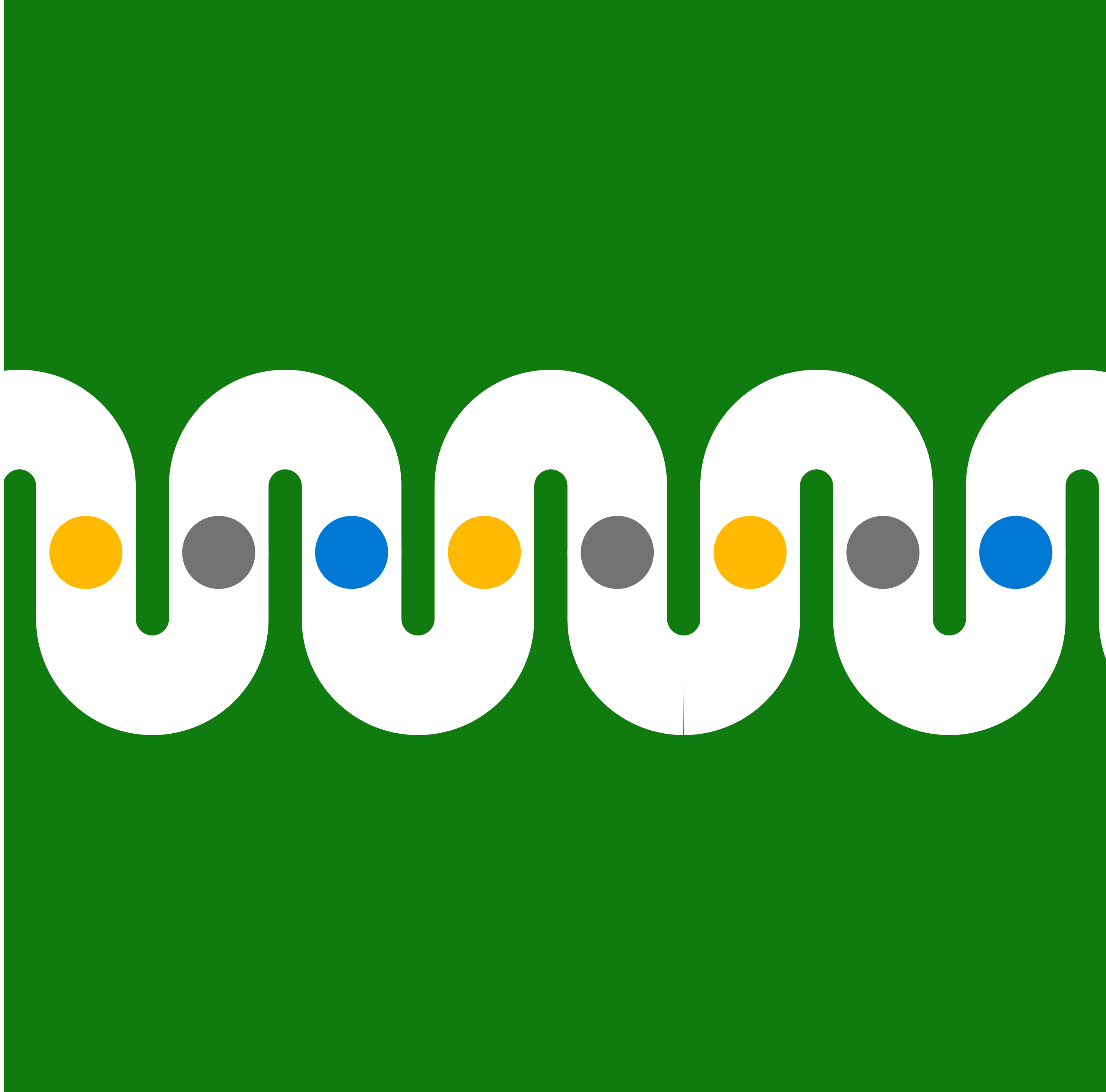
Description Extensible Single Sign On Profile - 32f37be3-302e-4549-a3e3-854d300e117a

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

Partner Integrations



Partner Improvements

- We've worked with Jamf and VMWare to greatly improve the user experience with their MDMs and ESSO

Partner Improvements

- We’ve worked with Jamf and VMWare to greatly improve the user experience with their MDMs and ESSO
- Also worked with Jamf to improve other things, like Jamf Connect integration with Conditional Access
  - See our joint session with Sean Rabbitt from JNUC 2023

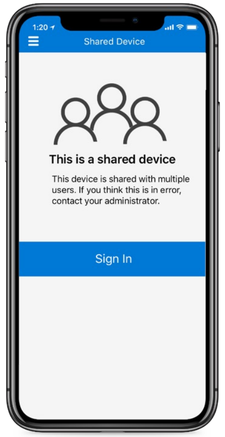
What’s Next

Platform SSO

- Public Preview coming soon
- Requires Ventura, but many improvements in Sonoma
- Password sync option
- Secure Enclave-based authentication option (equivalent to Windows Hello for Business)
- Smart Card option (Sonoma only)

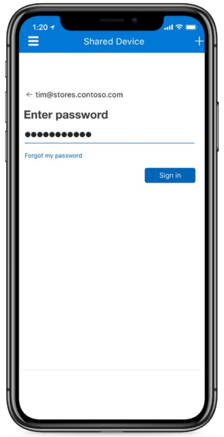
https://aka.ms/PSSO4MAC

Shared Device Mode



This is a shared device

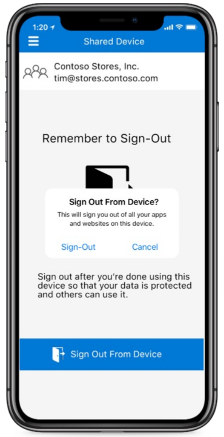
This device is shared with multiple users. If you think this is in error, contact your administrator.



← tim@stores.contoso.com

Enter password

●●●●●●●●●●●



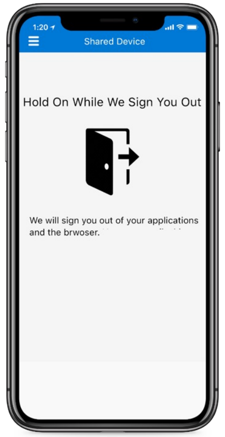
Contoso Stores, Inc.
tim@stores.contoso.com

Remember to Sign-Out

Sign Out From Device?

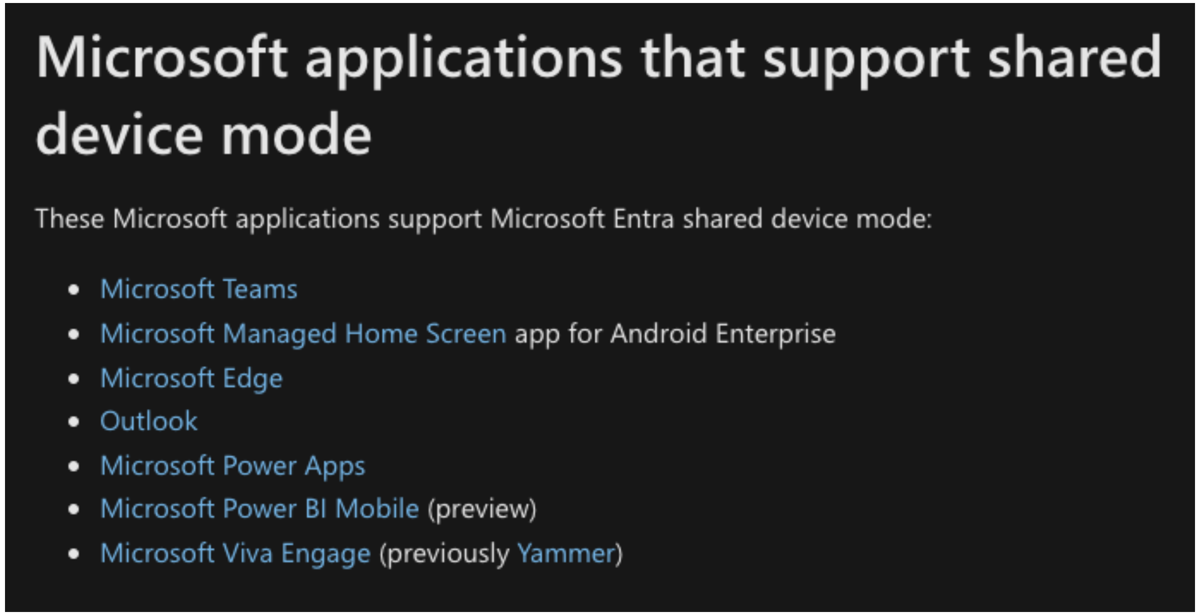
This will sign you out of all your apps and websites on this device.

Sign out after you're done using this device so that your data is protected and others can use it.



Hold On While We Sign You Out

We will sign you out of your applications and the brwoser.



Microsoft applications that support shared device mode

These Microsoft applications support Microsoft Entra shared device mode:

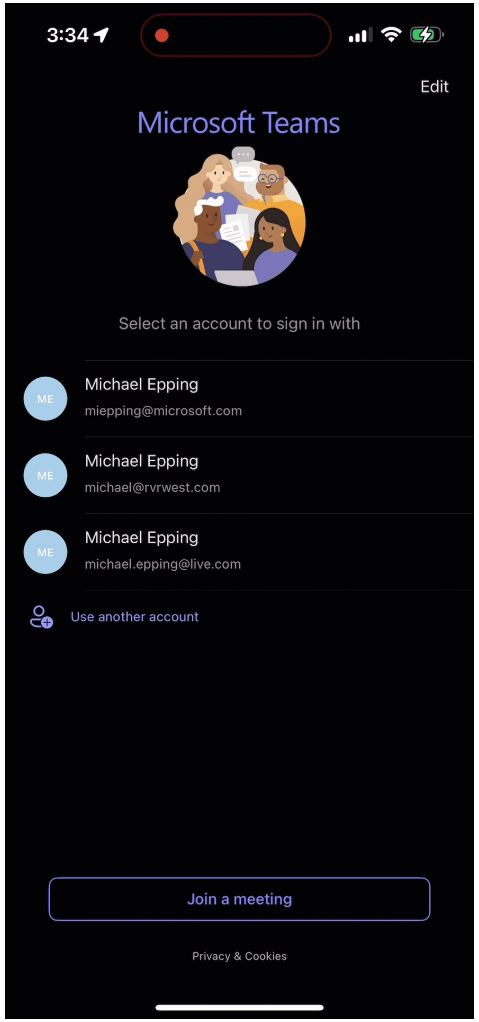
- Microsoft Teams
- Microsoft Managed Home Screen app for Android Enterprise
- Microsoft Edge
- Outlook
- Microsoft Power Apps
- Microsoft Power BI Mobile (preview)
- Microsoft Viva Engage (previously Yammer)

- SDM is GA for Android
- iOS GA is coming soon
  - 3rd party MDM support will come shortly after GA
- Same set of Microsoft apps will be supported for iOS and Android
- 3rd party apps will be supported, preferably will use MSAL
- What types of sign-in methods do you want for FLW workers?

Go Dos

Go Dos

- Deploy the SSO Extension
  - Don’t forget about iOS!
- Use the SSO Extension to improve your MDM integration with Microsoft
- Get devices upgraded to Sonoma if you want PSSO
- Watch our JNUC session if you use Jamf products and Conditional Access



Microsoft Teams

Select an account to sign in with

Michael Epping
miepping@microsoft.com

Michael Epping
michael@rvrwest.com

Michael Epping
michael.epping@live.com

Microsoft Security

Thank you

Microsoft Security