Mac-nificent
How Platform SSO empowers security and usability

SCAN ME

CONNECT. COLLABORATE. CREATE

MC2MC

CONNECT

Arxus

PATCH MY PC

cegeka

AXXES_

INGRAM MICRO®

2Pint

veeam

TheCollective

Insight®

semperis

proximus NXT

ConXioN
The new style of IT

VirtualMetric

savaco
IT's about impact

evri

Thomas Naunheim

- Cyber Security Architect @glueckkanja AG
- Microsoft MVP
  (Identity & Access, Cloud Security)
- Co-Host „Cloud Inspires” Podcast
- Co-Organizer Azure Meetup Bonn and Cloud Identity Summit

Naunheim.cloud

ThomasNaunheim

Thomas_Live

Cloud-Architekt

ThomasNaunheim

cloud-architekt.net

Ugur Koc

- Cloud Architect @ glueckkanja AG
- Microsoft MVP for Intune
- Co-Organizer of WPNinja Germany
- ❤️ Graph API and Automation

I will spend 30 minutes coding to automate a task that would otherwise take 5 minutes of manual clicking in the Intune portal.

🦋 UgurKoc.De

𝕏 UgurKocDe

in UgurKocDe

▶ Ugur Koc

ugurkocde

🌐 UgurKoc.de

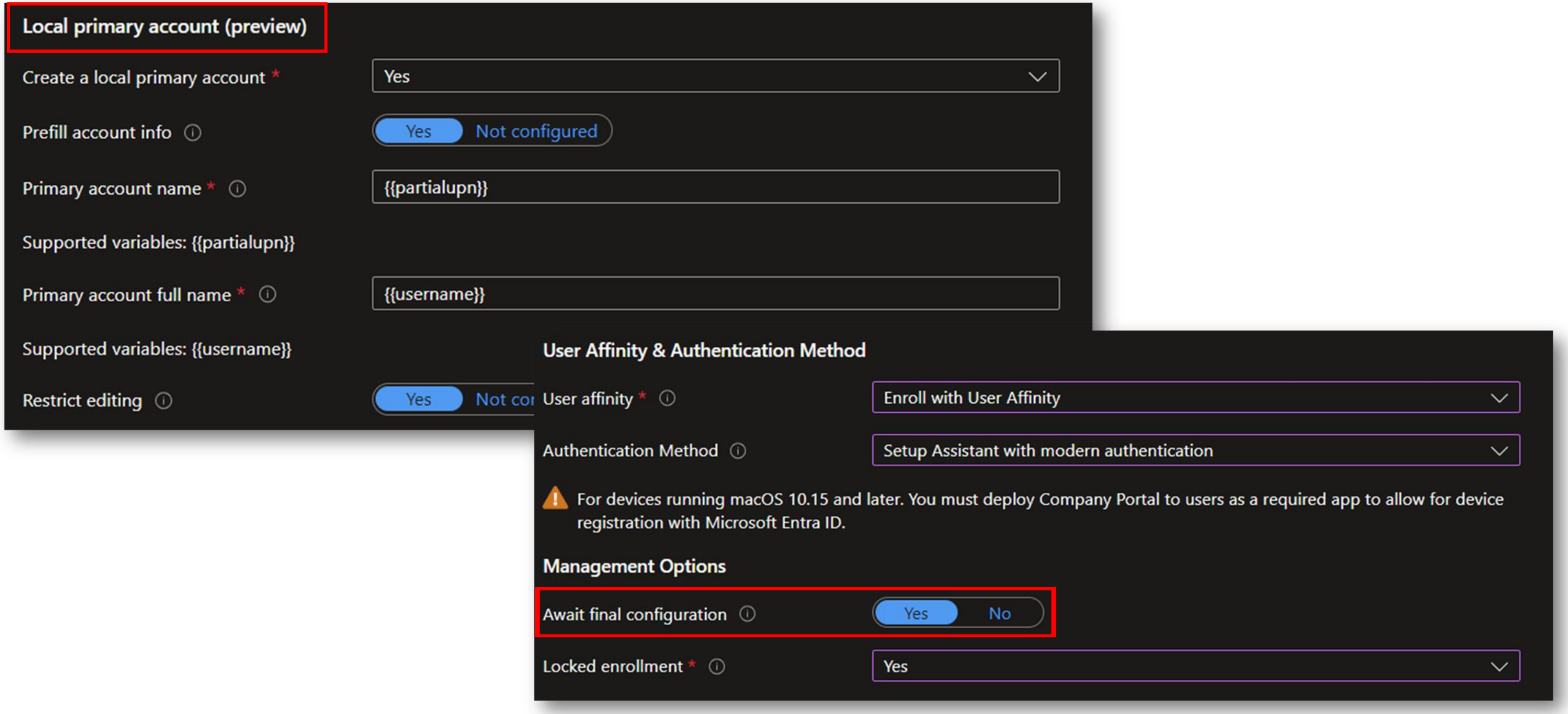
macOS & Intune – Where are we today?

CONNECT. COLLABORATE. CREATE

MC2MC

—CONNECT—

Enrollment



Local primary account (preview)

Create a local primary account * : Yes

Prefill account info ⓘ : [✓ Yes] Not configured

Primary account name * ⓘ : {{partialupn}}

Supported variables: {{partialupn}}

Primary account full name * ⓘ : {{username}}

Supported variables: {{username}}

Restrict editing ⓘ : [✓ Yes] Not cor

User Affinity & Authentication Method

User affinity * ⓘ : Enroll with User Affinity

Authentication Method ⓘ : Setup Assistant with modern authentication

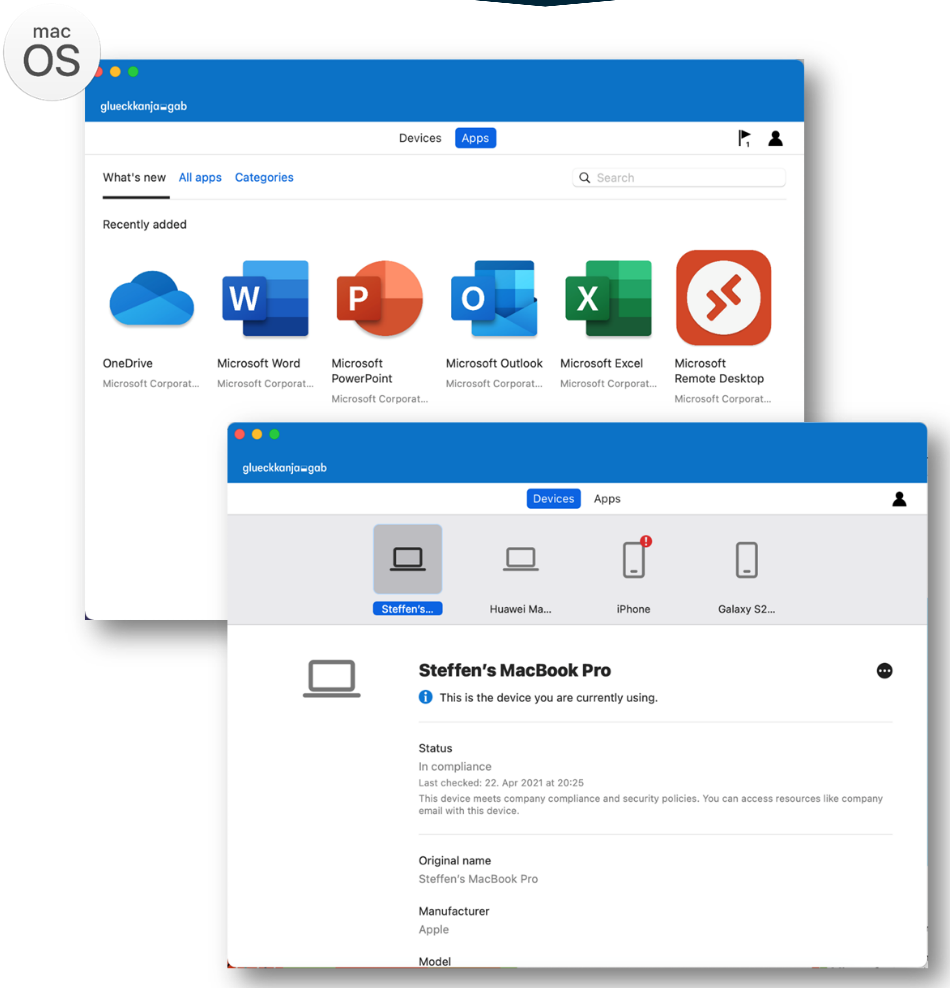
⚠ For devices running macOS 10.15 and later. You must deploy Company Portal to users as a required app to allow for device registration with Microsoft Entra ID.

Management Options

Await final configuration ⓘ : [✓ Yes] No

Locked enrollment * ⓘ : Yes

Company Portal



Steffen's MacBook Pro

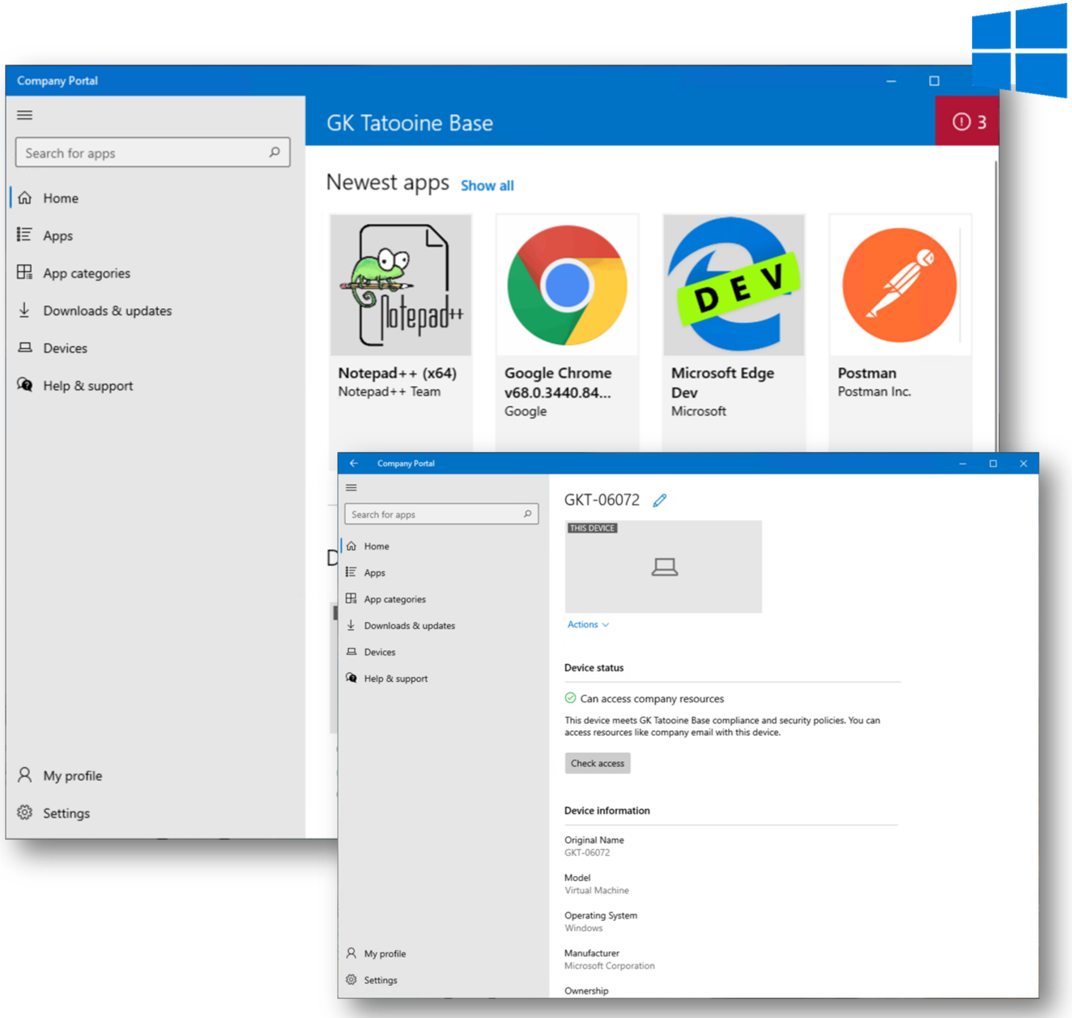
This is the device you are currently using.

Status
In compliance
Last checked: 22. Apr 2021 at 20:25
This device meets company compliance and security policies. You can access resources like company email with this device.

Original name
Steffen's MacBook Pro

Manufacturer
Apple

Model



GKT-06072

Device status

Can access company resources

This device meets GK Tatooine Base compliance and security policies. You can access resources like company email with this device.

Device information

Original Name
GKT-06072

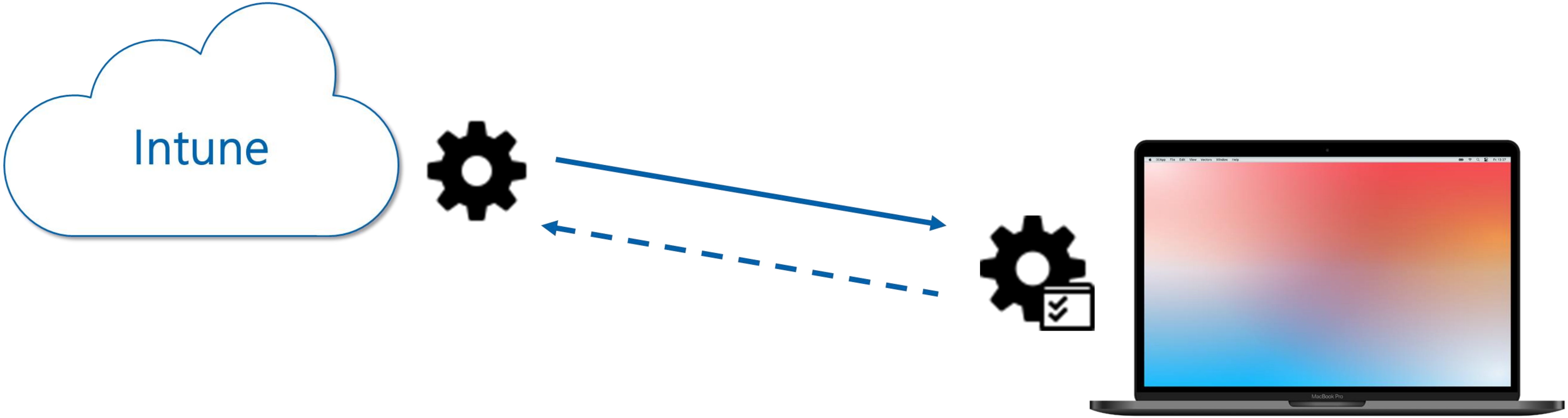
Model
Virtual Machine

Operating System
Windows

Manufacturer
Microsoft Corporation

Ownership

Declerative Device Management



Windows vs. macOS in Intune

I'm a PC.

Autopilot	Automated Device Enrollment
ESP	Not really (3rd Party)
Bitlocker	FileVault
LAPS/EPM	Not really (3rd Party)
TPM	?

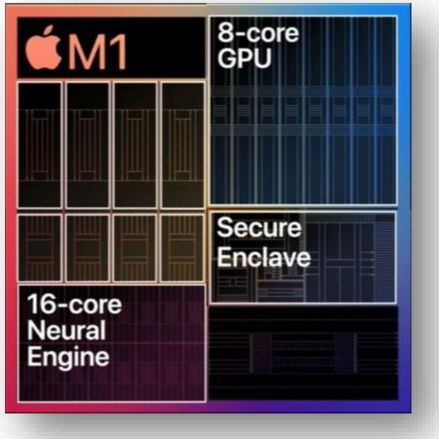
I'm a Mac.

Secure Enclave – dedicated subsystem

- Use Secure Enclave to protect a private key.
- Hardware-based key manager that's isolated from the main processor.
- You know a developer? Tell him to use Secure Enclave.

- Hardware requirements
  - Intel Mac computers with T1 or T2 Chip
  - All Mac computers with Apple silicon (M1, M2, M3 ...)
  - iPad, iPhone, HomePod, Apple TV
    - **Secure Enclave is the new default**

More about Secure Enclave:
https://support.apple.com/en-gb/guide/security/sec59b0b31ff/web



Windows vs. macOS in Intune

I'm a PC.

Autopilot	Automated Device Enrollment
ESP	Not really (3rd Party)
Bitlocker	FileVault
LAPS/EPM	Not really (3rd Party)
TPM	Secure Enclave
Windows Hello for Business	Platform Credential (Passkey)

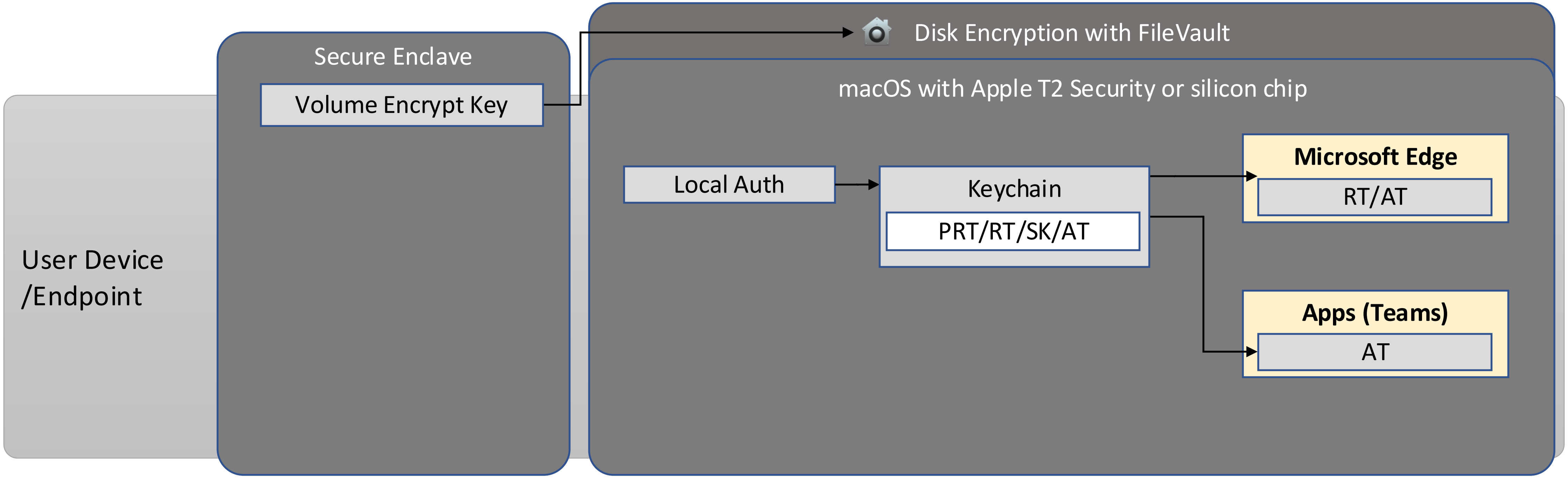
I'm a Mac.

Hot take-aways:

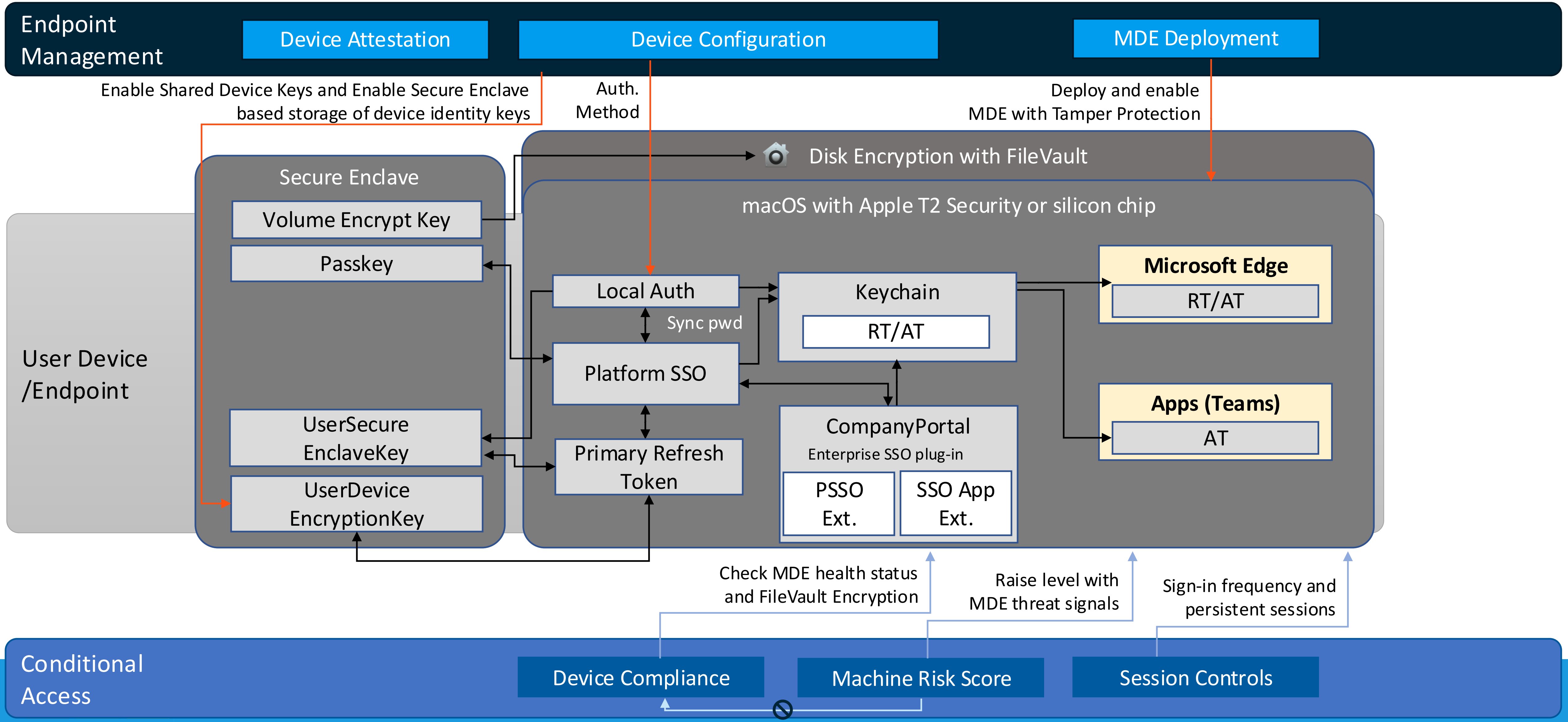
1. **macOS Management is very close to what we already know from Windows Management.**
2. **Before PSSO we had no Phishing Resistant Authentication**

How SSO works on macOS

macOS SSO on unmanaged devices



macOS SSO with Platform SSO



Endpoint Management

Device Attestation

Device Configuration

MDE Deployment

Enable Shared Device Keys and Enable Secure Enclave based storage of device identity keys

Auth. Method

Deploy and enable MDE with Tamper Protection

Disk Encryption with FileVault

User Device /Endpoint

Secure Enclave

Volume Encrypt Key

Passkey

UserSecure EnclaveKey

UserDevice EncryptionKey

macOS with Apple T2 Security or silicon chip

Local Auth

Sync pwd

Platform SSO

Primary Refresh Token

Keychain

RT/AT

CompanyPortal

Enterprise SSO plug-in

PSSO Ext.

SSO App Ext.

Microsoft Edge

RT/AT

Apps (Teams)

AT

Check MDE health status and FileVault Encryption

Raise level with MDE threat signals

Sign-in frequency and persistent sessions

Conditional Access

Device Compliance

Machine Risk Score

Session Controls

Summary of macOS + Entra SSO options

- SSO options on macOS with Microsoft Entra
  - Unmanaged device with Edge profile sign-in (Device Registration)
    → Allow SSO between selected Microsoft Apps (including Office 365)
  - Managed device with Intune and SSO extension (Device Registration)
    → SSO on Application-Level (requires MSAL)
  - Managed device with Intune and Platform SSO (Entra Join)
    → SSO on OS-Level and other integrations

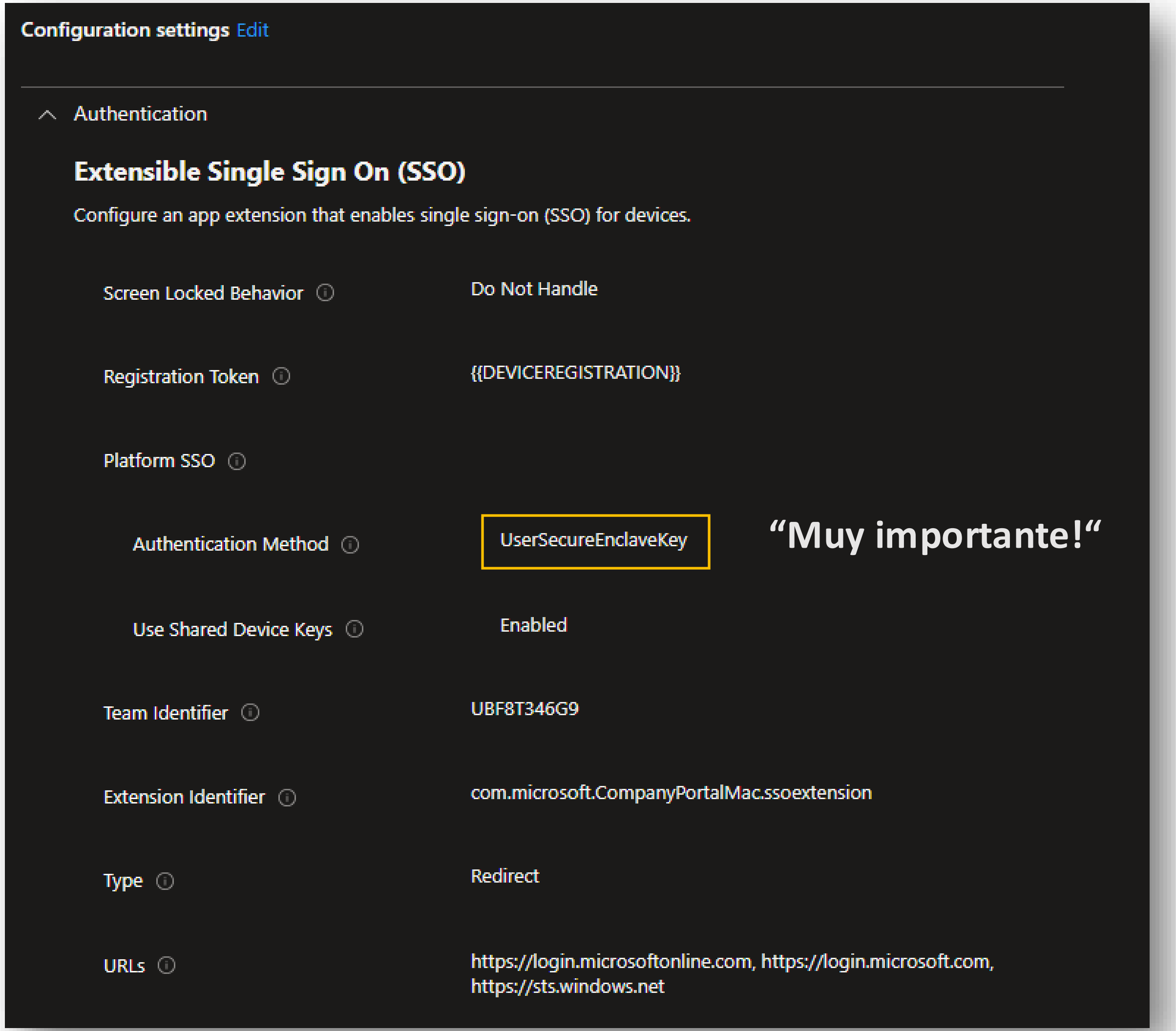
Configuration and User Experience of PSSO

CONNECT. COLLABORATE. CREATE

MC2MC

—CONNECT—

Configuration of PSSO



Configuration settings Edit

Authentication

Extensible Single Sign On (SSO)

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

Screen Locked Behavior	Do Not Handle
Registration Token	{{DEVICEREGISTRATION}}
Platform SSO	
Authentication Method	UserSecureEnclaveKey
Use Shared Device Keys	Enabled
Team Identifier	UBF8T346G9
Extension Identifier	com.microsoft.CompanyPortalMac.ssoextension
Type	Redirect
URLs	https://login.microsoftonline.com, https://login.microsoft.com, https://sts.windows.net

"Muy importante!"

Quick Start with these Settings

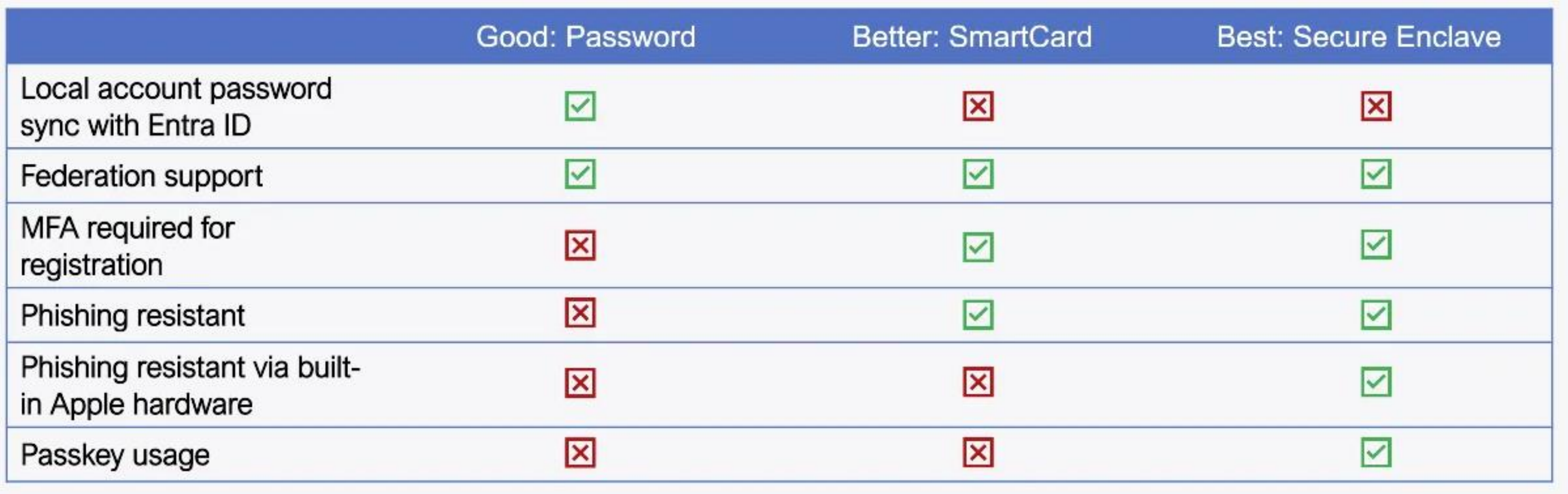
or …

Import Policy

Want more?

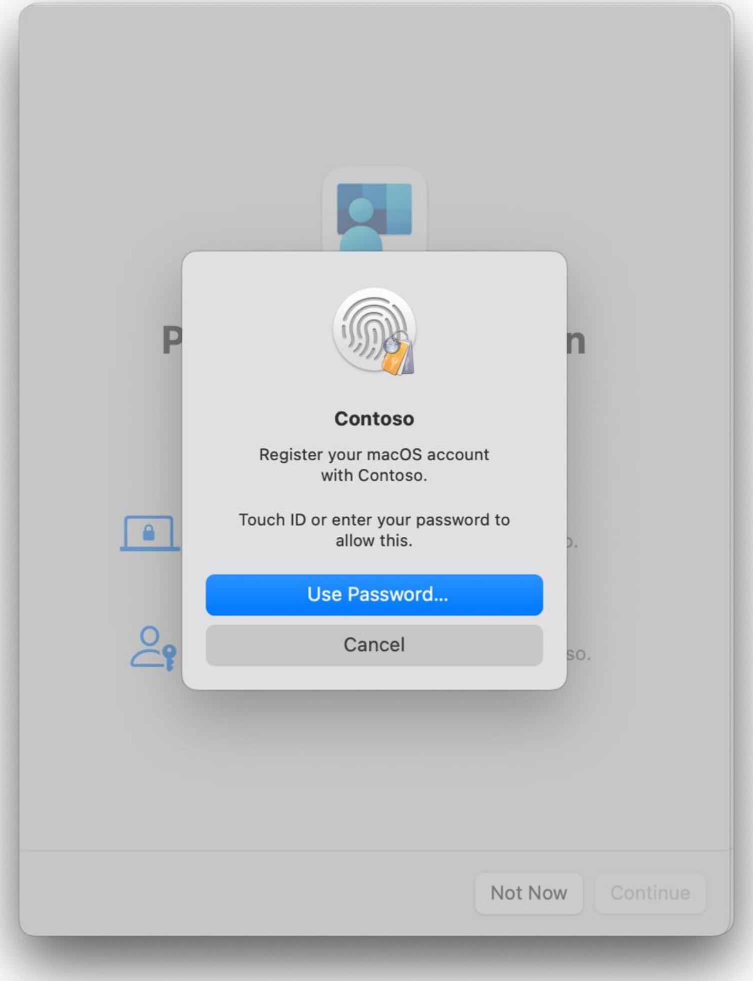
Visit ***IntuneMacAdmins.com***

Authentication options on macOS



	Good: Password	Better: SmartCard	Best: Secure Enclave
Local account password sync with Entra ID	☑	☒	☒
Federation support	☑	☑	☑
MFA required for registration	☒	☑	☑
Phishing resistant	☒	☑	☑
Phishing resistant via built-in Apple hardware	☒	☒	☑
Passkey usage	☒	☒	☑

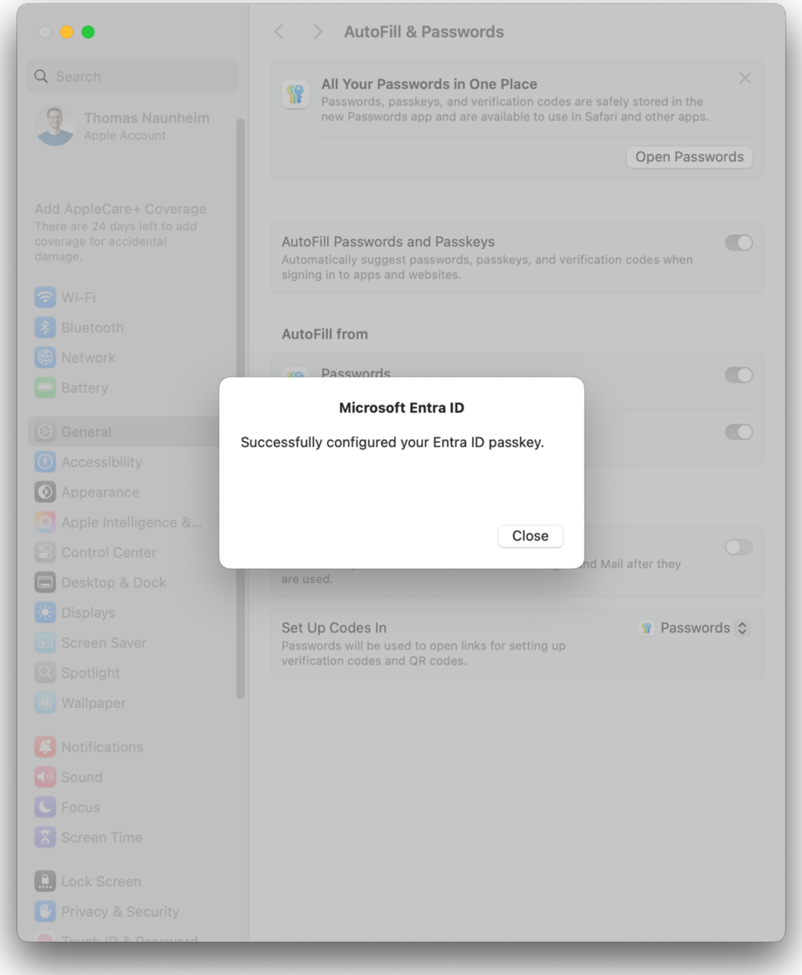
UX migration from SSO Ext. to PSSO



Contoso

Register your macOS account with Contoso.

Touch ID or enter your password to allow this.



Add AppleCare+ Coverage
There are 24 days left to add coverage for accidental damage.

All Your Passwords in One Place
Passwords, passkeys, and verification codes are safely stored in the new Passwords app and are available to use in Safari and other apps.

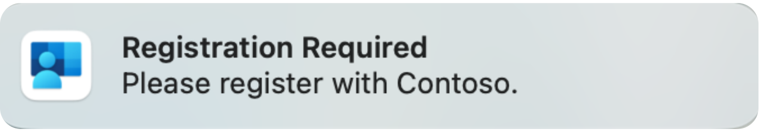
AutoFill Passwords and Passkeys
Automatically suggest passwords, passkeys, and verification codes when signing in to apps and websites.

...nd Mail after they are used.

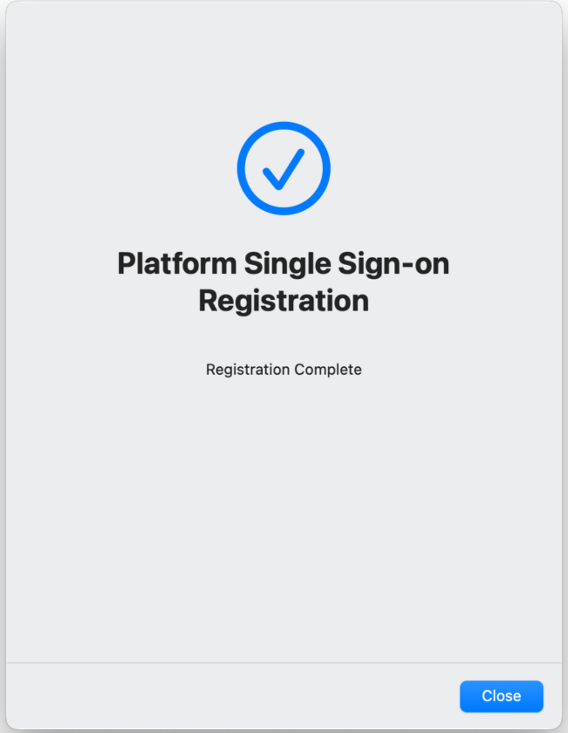
Set Up Codes In: Passwords
Passwords will be used to open links for setting up verification codes and QR codes.

Microsoft Entra ID

Successfully configured your Entra ID passkey.



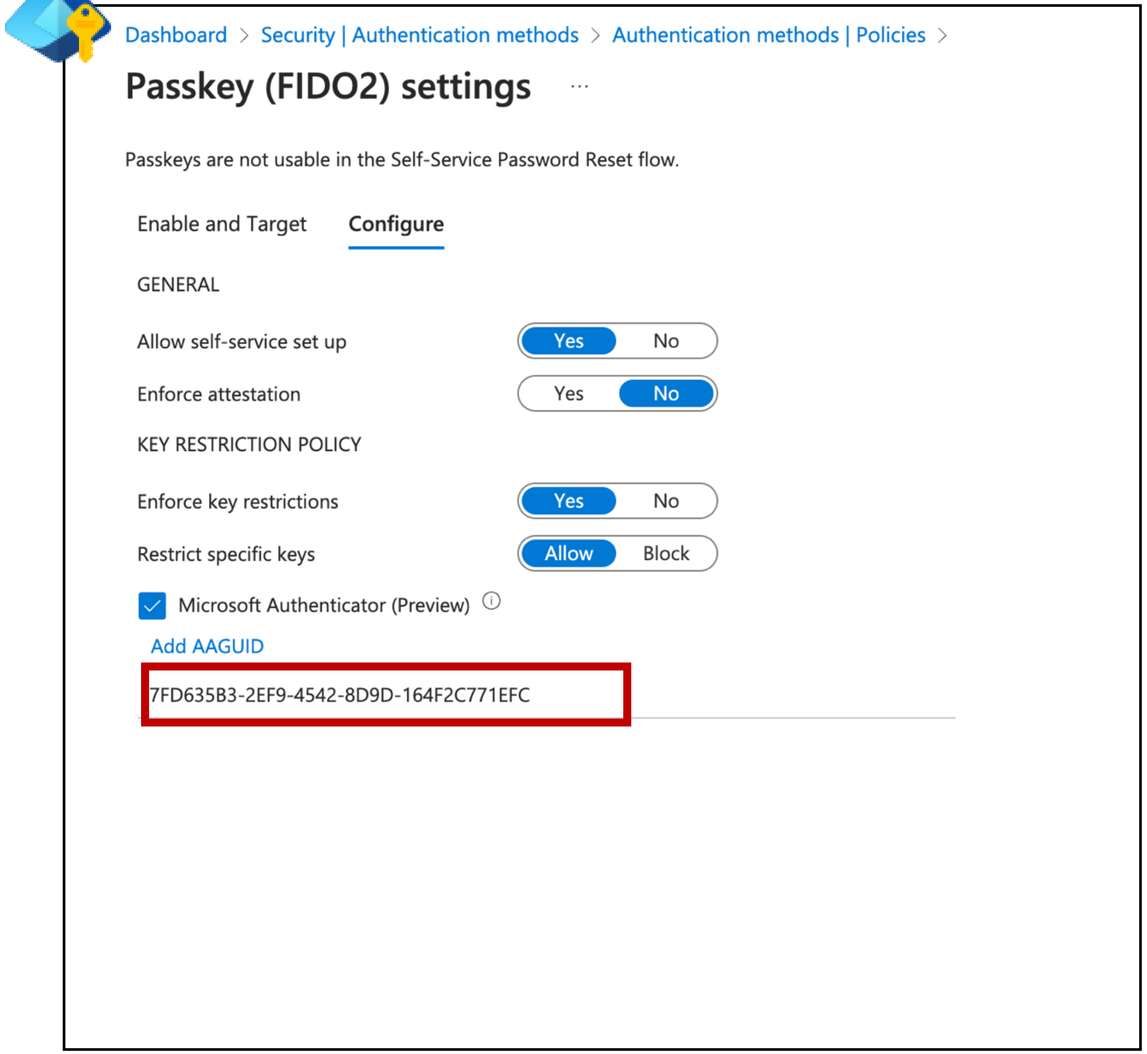
Registration Required
Please register with Contoso.



Platform Single Sign-on Registration

Registration Complete

macOS Platform credential



Dashboard > Security | Authentication methods > Authentication methods | Policies >

Passkey (FIDO2) settings ...

Passkeys are not usable in the Self-Service Password Reset flow.

Enable and Target | **Configure**

GENERAL

Allow self-service set up	[✓ Yes] No
Enforce attestation	Yes [✓ No]

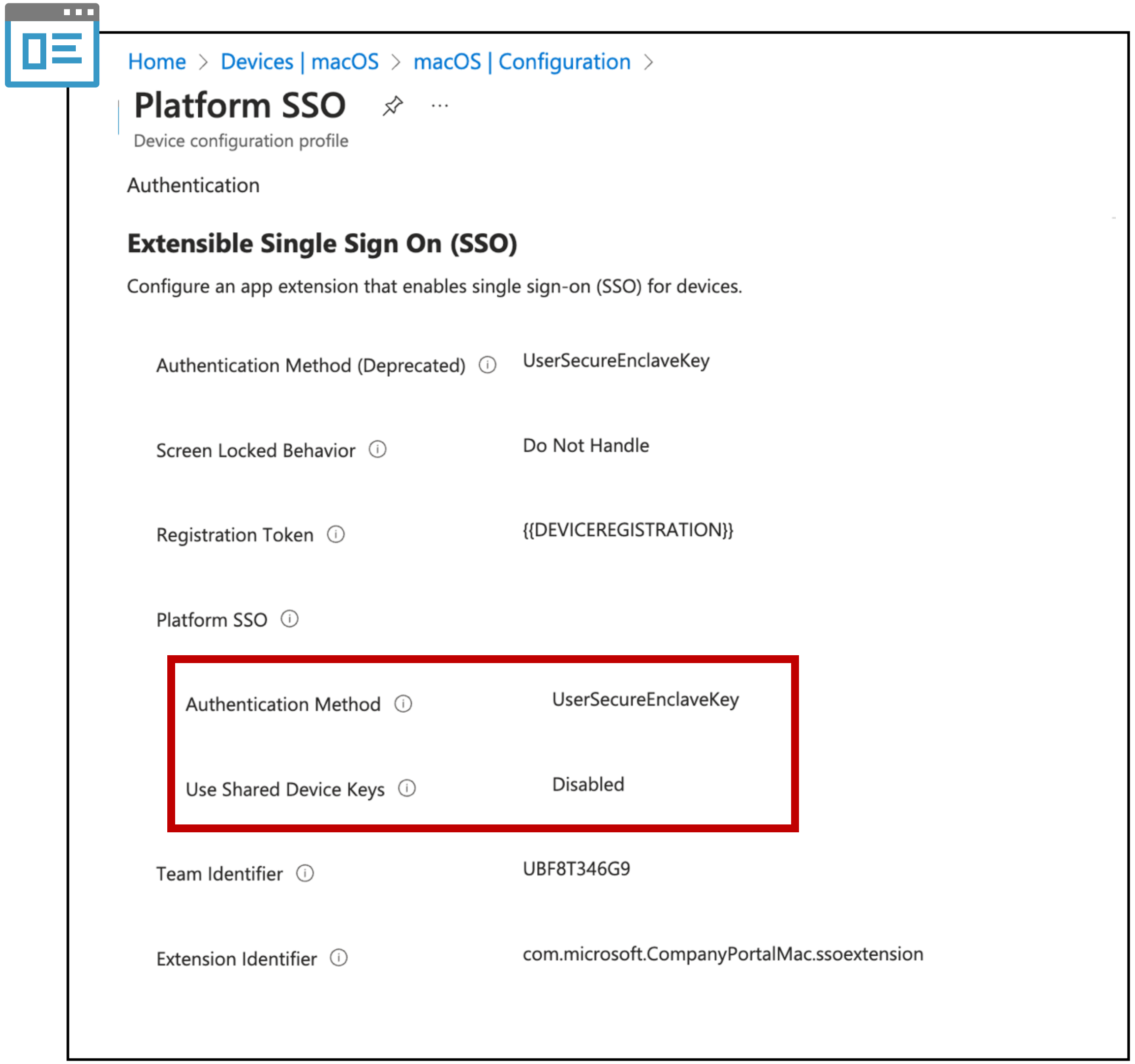
KEY RESTRICTION POLICY

Enforce key restrictions	[✓ Yes] No
Restrict specific keys	[✓ Allow] Block

☑ Microsoft Authenticator (Preview) ⓘ

Add AAGUID

7FD635B3-2EF9-4542-8D9D-164F2C771EFC



Home > Devices | macOS > macOS | Configuration >

Platform SSO ...

Device configuration profile

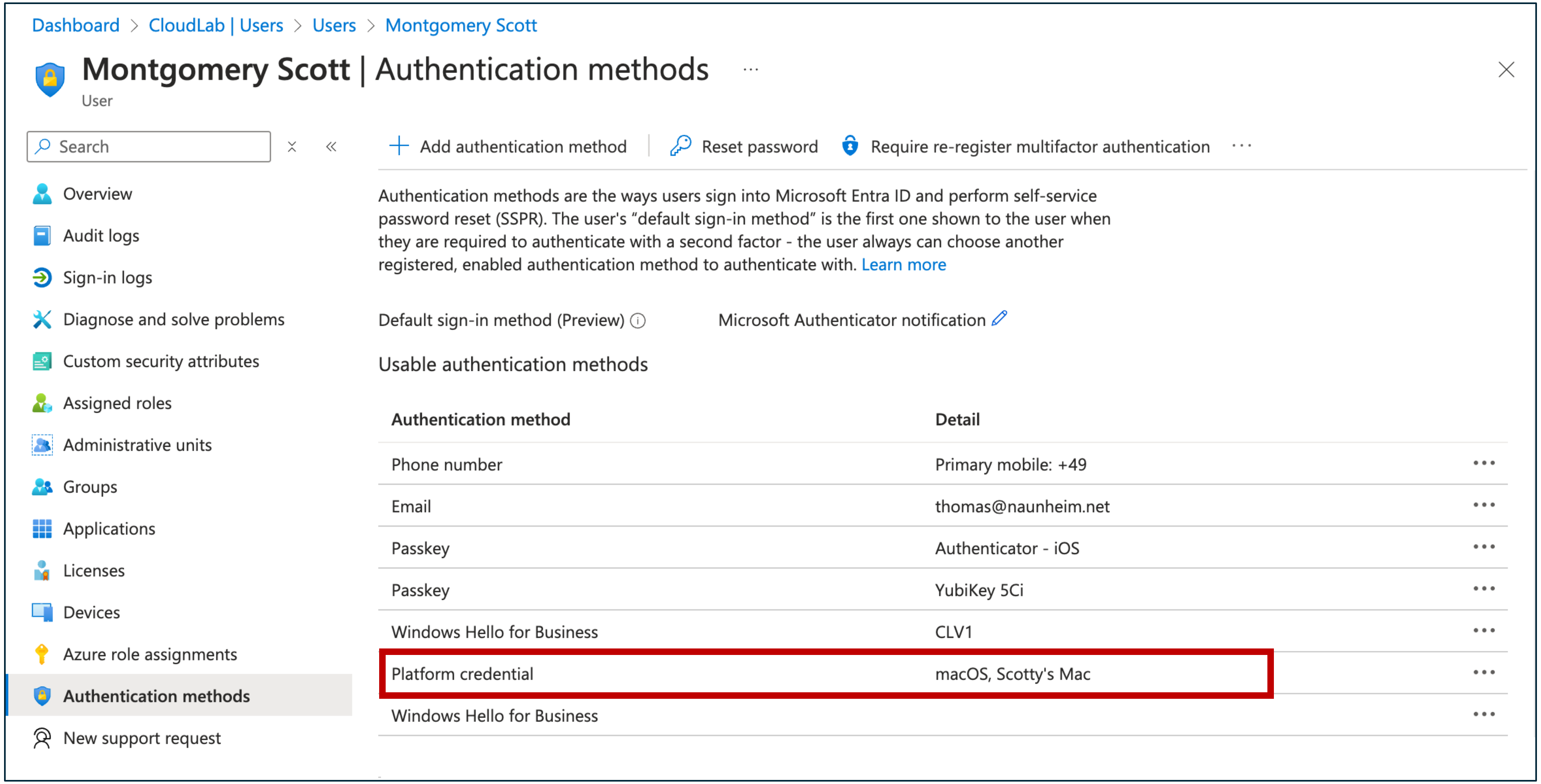
Authentication

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
Use Shared Device Keys ⓘ	Disabled
Team Identifier ⓘ	UBF8T346G9
Extension Identifier ⓘ	com.microsoft.CompanyPortalMac.ssoextension

macOS Platform credential



Dashboard > CloudLab | Users > Users > Montgomery Scott
Search
Overview
Audit logs
Sign-in logs
Diagnose and solve problems
Custom security attributes
Assigned roles
Administrative units
Groups
Applications
Licenses
Devices
Azure role assignments
Authentication methods
New support request
+ Add authentication method
Reset password
Require re-register multifactor authentication

Montgomery Scott | Authentication methods

User

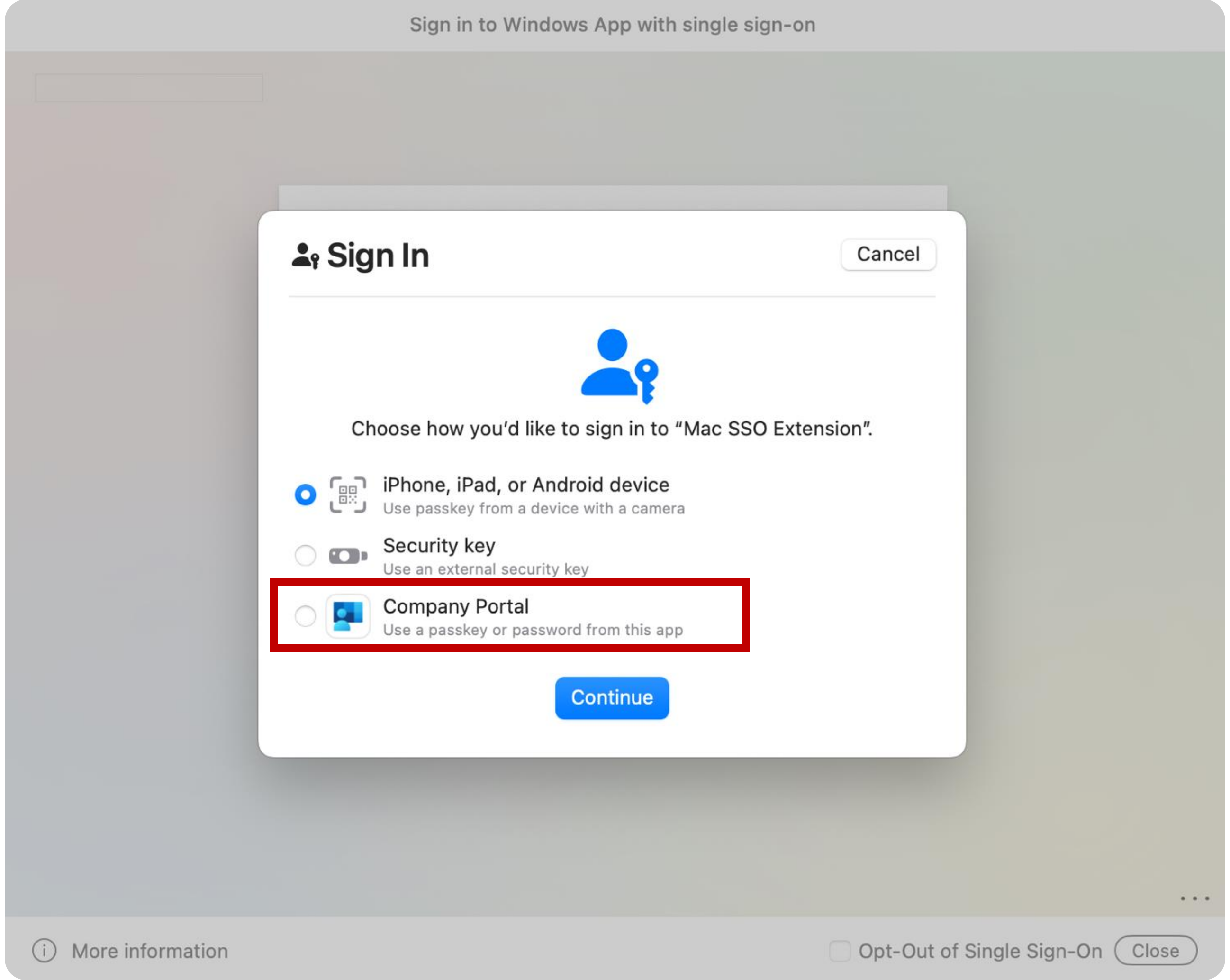
Authentication methods are the ways users sign into Microsoft Entra ID and perform self-service password reset (SSPR). The user's “default sign-in method” is the first one shown to the user when they are required to authenticate with a second factor - the user always can choose another registered, enabled authentication method to authenticate with. Learn more

Default sign-in method (Preview) ⓘ Microsoft Authenticator notification

Usable authentication methods

Authentication method	Detail
Phone number	Primary mobile: +49
Email	thomas@naunheim.net
Passkey	Authenticator - iOS
Passkey	YubiKey 5Ci
Windows Hello for Business	CLV1
Platform credential	macOS, Scotty's Mac
Windows Hello for Business	

macOS Platform credential



Sign in to Windows App with single sign-on

Sign In

Cancel

Choose how you'd like to sign in to "Mac SSO Extension".

● iPhone, iPad, or Android device
Use passkey from a device with a camera

○ Security key
Use an external security key

○ Company Portal
Use a passkey or password from this app

Continue

ⓘ More information

□ Opt-Out of Single Sign-On

Close

Benefits, limitations and security considerations

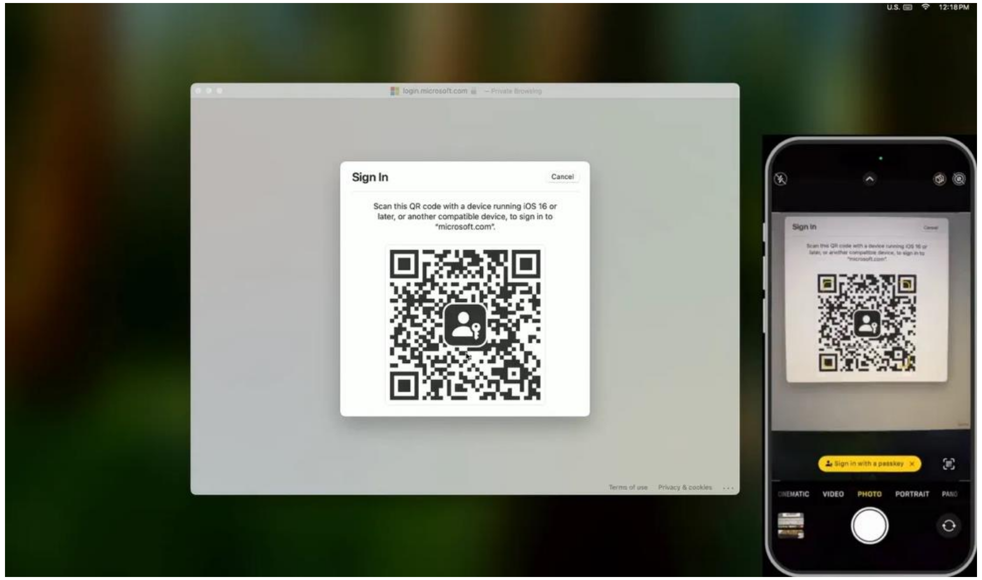
CONNECT. COLLABORATE. CREATE

MC2MC

CONNECT

UX limitations

- ~~No~~ Passkey support during MDM Enrollment ~~→ TAP~~



Sign In

Cancel

Scan this QR code with a device running iOS 16 or later, or another compatible device, to sign in to "microsoft.com".

- Password is still required after reboot (dependency to FileVault)
- The local account username isn't changed and stays as-is

UX benefits and limitations

- Secure Enclave vs. Password Sync
  - Better Security vs. Better User Experience

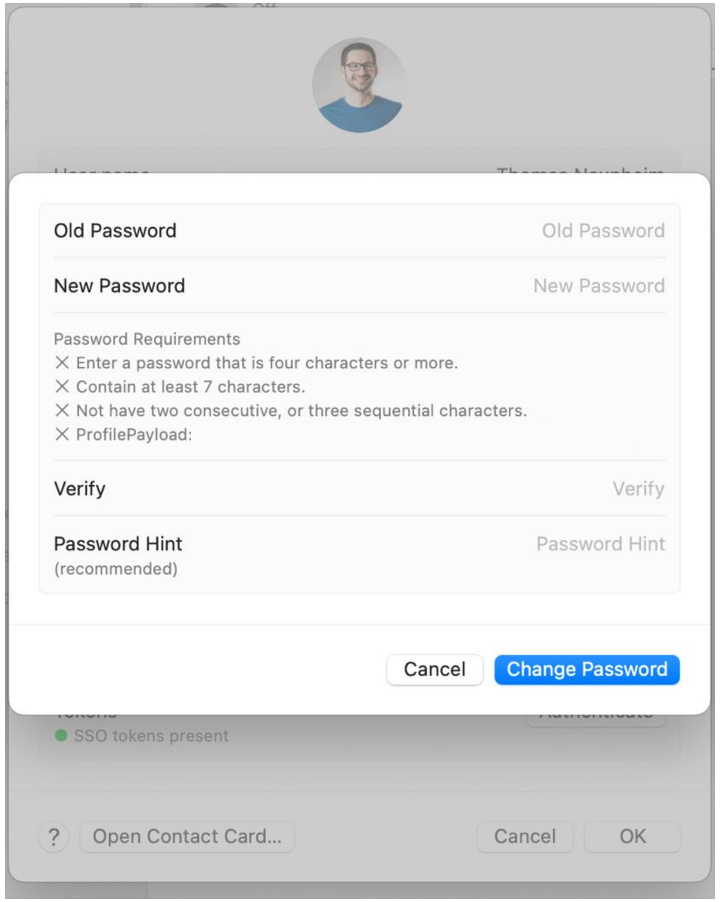
- Password Sync: Synchronized password between local macOS and Entra ID account

- Cloud Kerberos Tickets (VPN, Intranet use-cases)

- Secure Enclave: No Password Synchronization
  - This is what you need if you want to use Passkeys
  - Password Policy with PIN enforcement feels like WHfB

One more thing…

- Passcode instead of Password (WHfB PIN Experience)



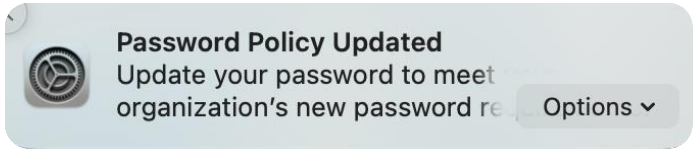
Old Password — Old Password

New Password — New Password

Password Requirements
✕ Enter a password that is four characters or more.
✕ Contain at least 7 characters.
✕ Not have two consecutive, or three sequential characters.
✕ ProfilePayload:

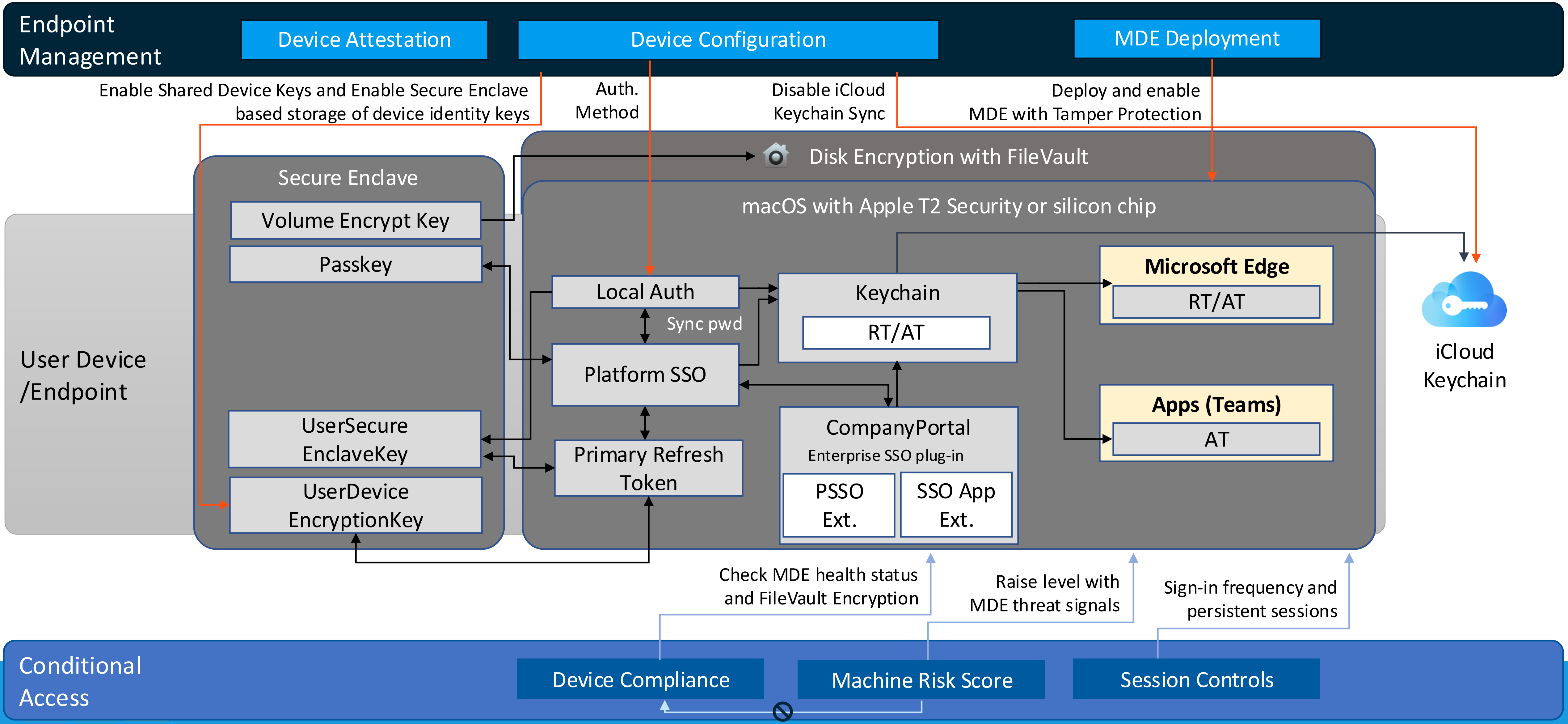
Verify — Verify

Password Hint (recommended) — Password Hint

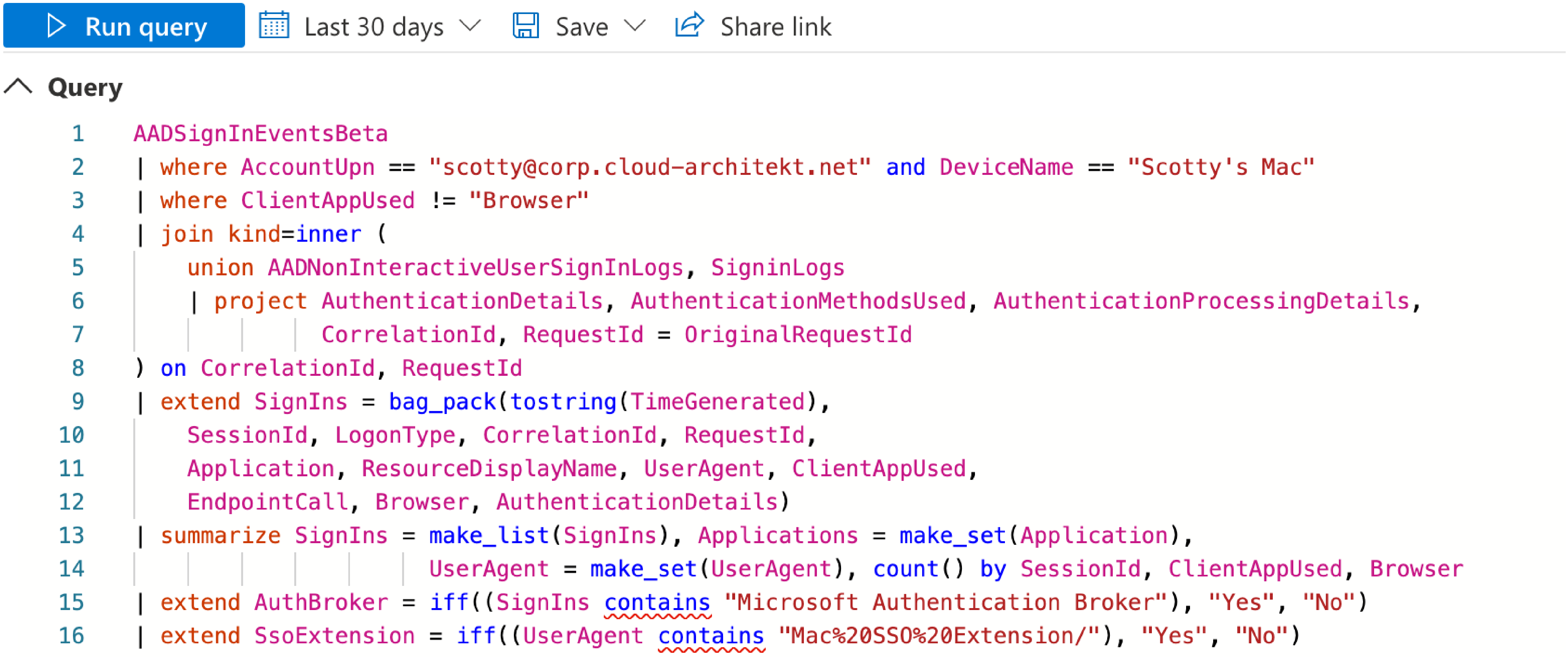


Password Policy Updated
Update your password to meet
organization's new password re

Access/Refresh Tokens in Keychain

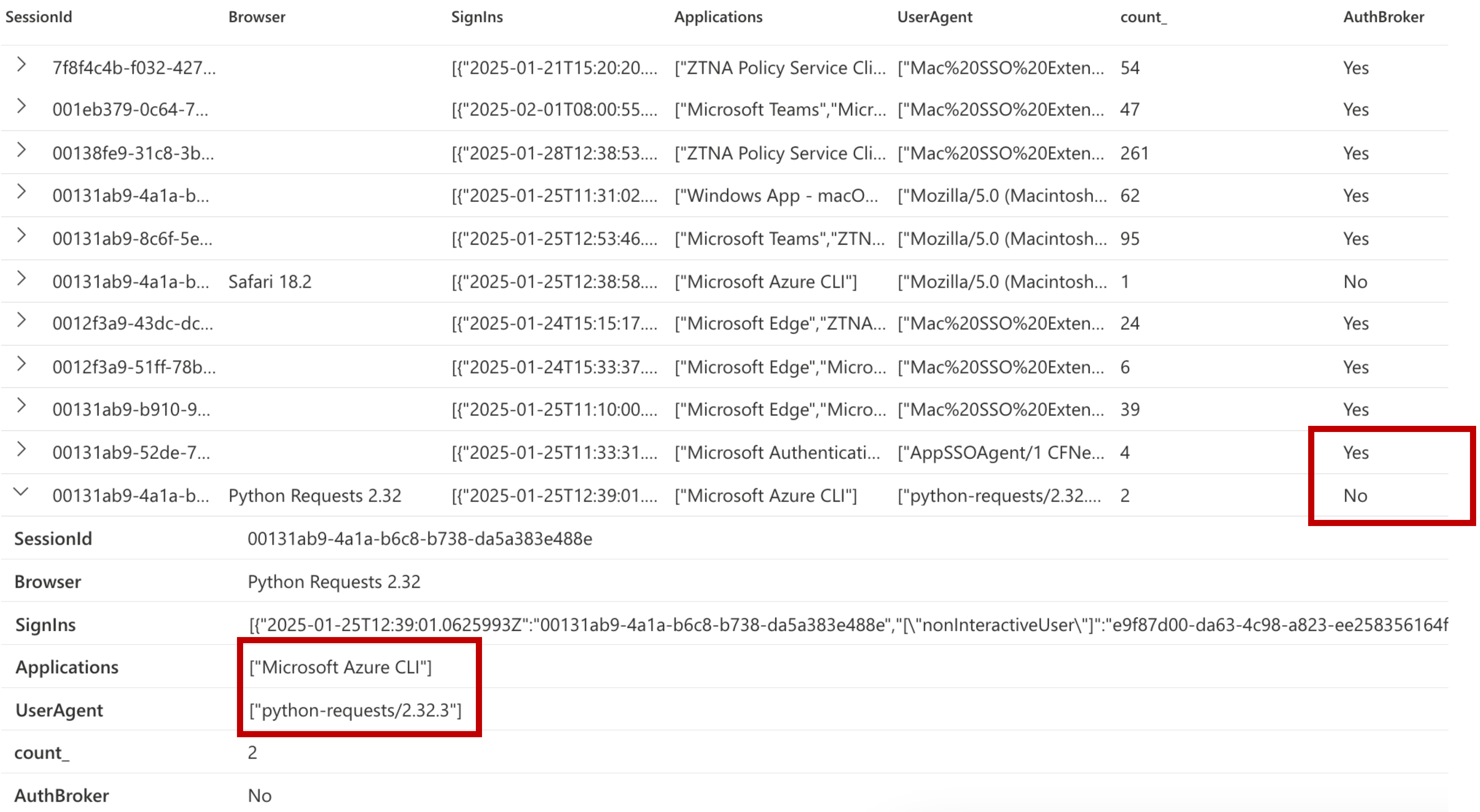


Platform SSO sign-ins vs. dedicated sessions



```
AADSignInEventsBeta
| where AccountUpn == "scotty@corp.cloud-architekt.net" and DeviceName == "Scotty's Mac"
| where ClientAppUsed != "Browser"
| join kind=inner (
    union AADNonInteractiveUserSignInLogs, SigninLogs
    | project AuthenticationDetails, AuthenticationMethodsUsed, AuthenticationProcessingDetails,
              CorrelationId, RequestId = OriginalRequestId
) on CorrelationId, RequestId
| extend SignIns = bag_pack(tostring(TimeGenerated),
    SessionId, LogonType, CorrelationId, RequestId,
    Application, ResourceDisplayName, UserAgent, ClientAppUsed,
    EndpointCall, Browser, AuthenticationDetails)
| summarize SignIns = make_list(SignIns), Applications = make_set(Application),
                      UserAgent = make_set(UserAgent), count() by SessionId, ClientAppUsed, Browser
| extend AuthBroker = iff((SignIns contains "Microsoft Authentication Broker"), "Yes", "No")
| extend SsoExtension = iff((UserAgent contains "Mac%20SSO%20Extension/"), "Yes", "No")
```

Platform SSO sign-ins vs. dedicated sessions



SessionId	Browser	SignIns	Applications	UserAgent	count_	AuthBroker
7f8f4c4b-f032-427...		[{"2025-01-21T15:20:20....	["ZTNA Policy Service Cli...	["Mac%20SSO%20Exten...	54	Yes
001eb379-0c64-7...		[{"2025-02-01T08:00:55....	["Microsoft Teams","Micr...	["Mac%20SSO%20Exten...	47	Yes
00138fe9-31c8-3b...		[{"2025-01-28T12:38:53....	["ZTNA Policy Service Cli...	["Mac%20SSO%20Exten...	261	Yes
00131ab9-4a1a-b...		[{"2025-01-25T11:31:02....	["Windows App - macO...	["Mozilla/5.0 (Macintosh...	62	Yes
00131ab9-8c6f-5e...		[{"2025-01-25T12:53:46....	["Microsoft Teams","ZTN...	["Mozilla/5.0 (Macintosh...	95	Yes
00131ab9-4a1a-b...	Safari 18.2	[{"2025-01-25T12:38:58....	["Microsoft Azure CLI"]	["Mozilla/5.0 (Macintosh...	1	No
0012f3a9-43dc-dc...		[{"2025-01-24T15:15:17....	["Microsoft Edge","ZTNA...	["Mac%20SSO%20Exten...	24	Yes
0012f3a9-51ff-78b...		[{"2025-01-24T15:33:37....	["Microsoft Edge","Micro...	["Mac%20SSO%20Exten...	6	Yes
00131ab9-b910-9...		[{"2025-01-25T11:10:00....	["Microsoft Edge","Micro...	["Mac%20SSO%20Exten...	39	Yes
00131ab9-52de-7...		[{"2025-01-25T11:33:31....	["Microsoft Authenticati...	["AppSSOAgent/1 CFNe...	4	Yes
00131ab9-4a1a-b...	Python Requests 2.32	[{"2025-01-25T12:39:01....	["Microsoft Azure CLI"]	["python-requests/2.32....	2	No

SessionId	00131ab9-4a1a-b6c8-b738-da5a383e488e
Browser	Python Requests 2.32
SignIns	[{"2025-01-25T12:39:01.0625993Z":"00131ab9-4a1a-b6c8-b738-da5a383e488e","[\"nonInteractiveUser\"]":"e9f87d00-da63-4c98-a823-ee258356164f
Applications	["Microsoft Azure CLI"]
UserAgent	["python-requests/2.32.3"]
count_	2
AuthBroker	No

Security considerations and limitations

- Applications are still caching their own tokens in Keychain
- Universal CAE in Global Secure Access is not supported on macOS
- Availability of Token Protection
  (announcement for Public Preview in 2025)
  - → Will mitigate some of the shown token replay scenarios from KeyChain
- Users can reset the local password via Apple ID,
  other local admin user or an admin recovery key
  → Breaks SSO trust to Entra, reconfiguration of PSSO required

Session feedback available in home feed of the app after the session

run
events

Thank you!

CONNECT. COLLABORATE. CREATE

MC2MC

CONNECT

CONNECT. COLLABORATE. CREATE

MC2MC

CONNECT