2023 JNUC

AUSTIN, TX

Jamf and Microsoft Entra ID Conditional Access

Microsoft

Michael Epping

Microsoft

Mark Morowczynski

Microsoft

Sean Rabbitt

Jamf

Agenda

Conditional Access Recap

Common Deployments & Issues

Jamf Pro & Conditional Access

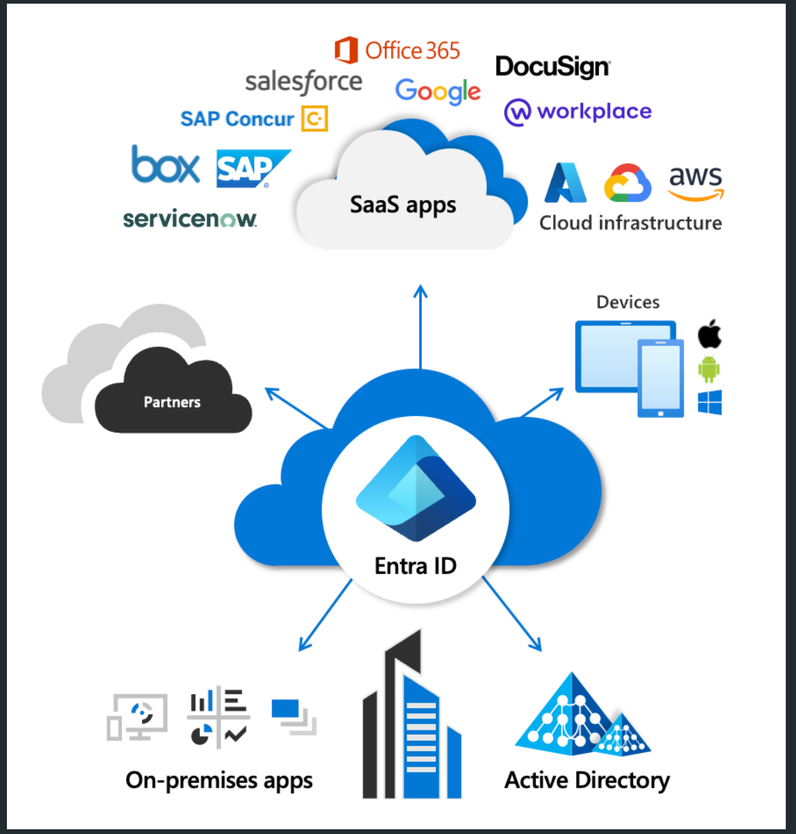
Jamf Connect & Conditional Access

Go Do’s!

What is Microsoft Entra ID?

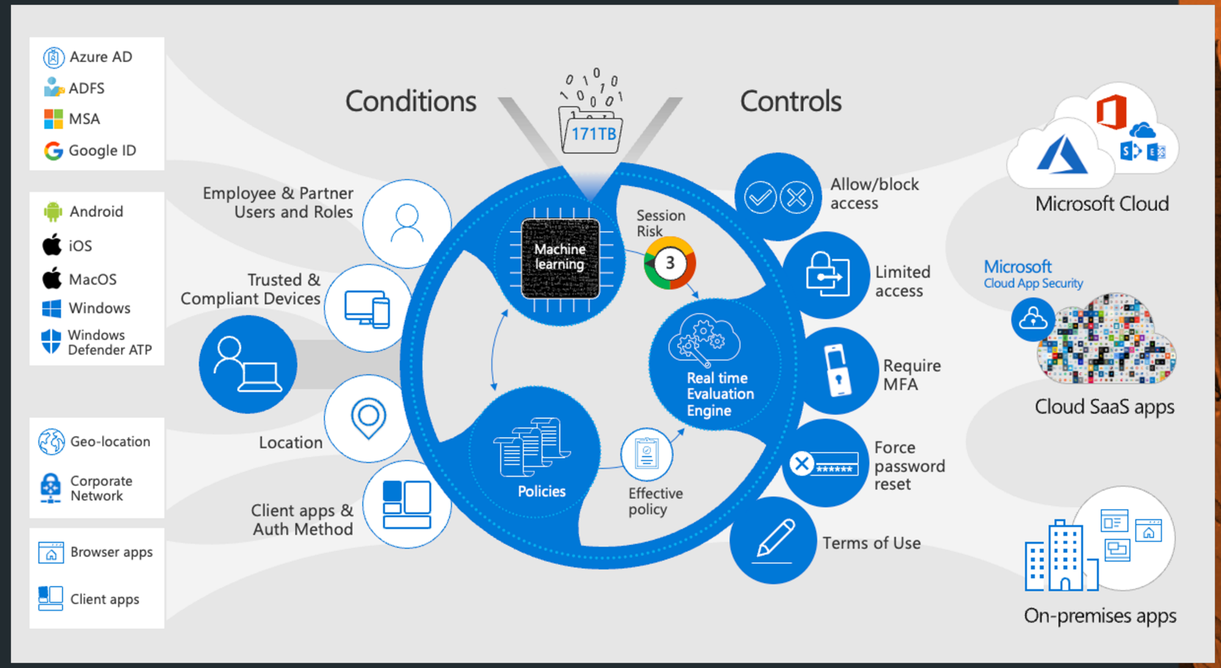
Microsoft

- Formerly known as Azure Active Directory
- Part of Microsoft Entra
- Full blown IDaaS
- Rich set of features
  - SSO, Provisioning
  - Governance, Passwordless
  - Conditional Access



Conditional Access Reminder

- Zero-trust engine
- CA understands user's activity
  - User Location
  - User Risk
  - App Requirements
  - State of Device (Critical!)
- Applies to "Cloud Apps"
- Goal: CA policy in scope for every request



What are cloud apps?

Cloud Apps ARE

Web sites
OpenID Connect / OAuth 2.0
confidential clients
SAML

Web services
APIs

Cloud Apps ARE NOT

Mobile or desktop apps
OpenID Connect / OAuth 2.0 native clients

Conditional Access is applied to the RESOURCE
Ex: You apply it to Exchange Online, NOT Outlook

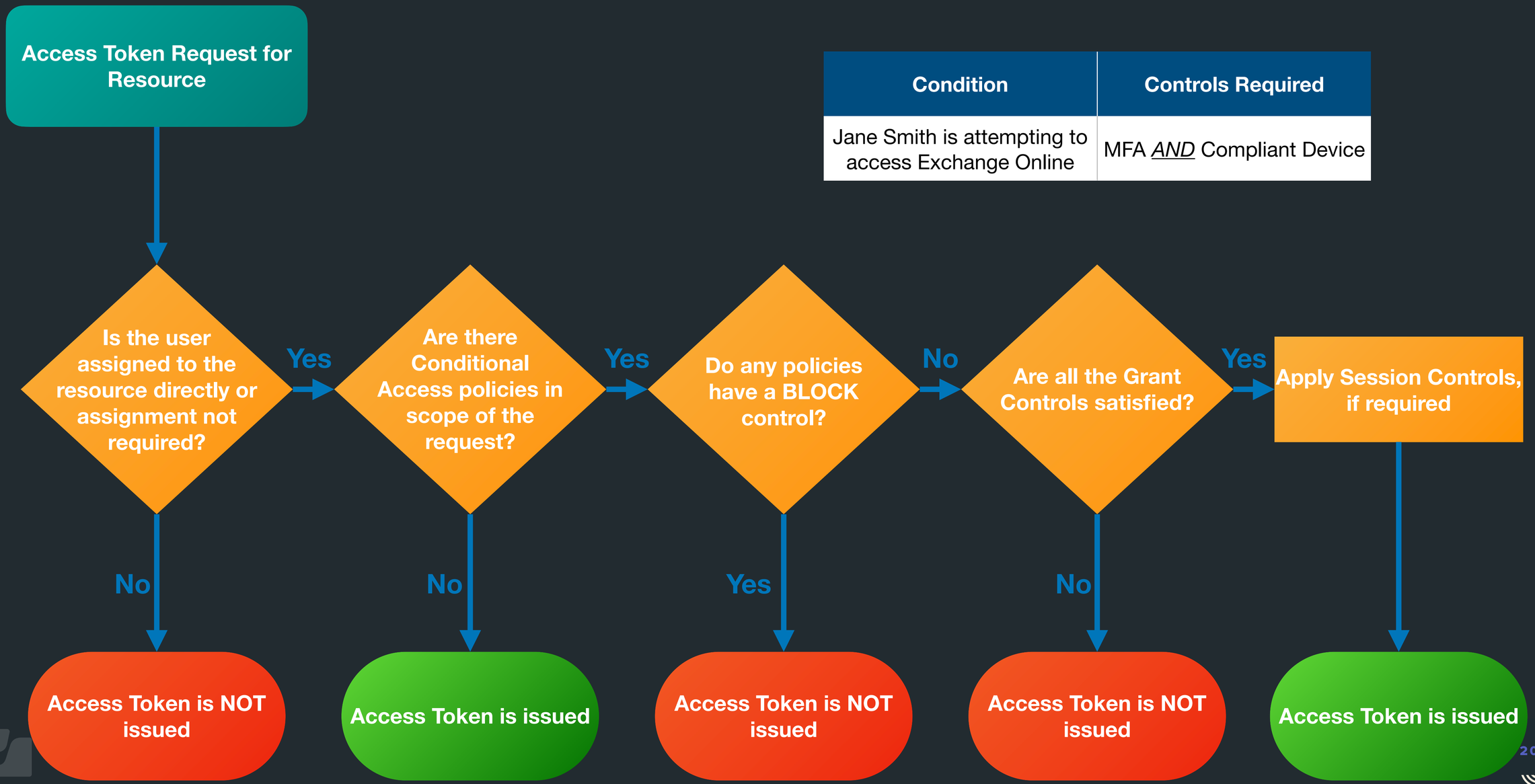
Conditional Access Evaluation Phases

- All CA policies are ANDed together
- Is Policy in scope of the request
- Block controls satisfied first
- Grant controls applied in order
  - Risk
  - MFA
  - Device
  - Approved client app/app protection
- Tries to satisfy policy without user interaction
  - Example: Control MFA or device compliant. If device is NOT compliant, will THEN prompt for MFA


```
{
  "userDisplayName": "Michael Epping",
  "appDisplayName": "Azure Portal",
  "ipAddress": "97.113.39.216",
  "clientAppUsed": "Browser",
  "conditionalAccessStatus": "success",
  "riskDetail": "none",
  "riskLevelAggregated": "none",
  "riskLevelDuringSignIn": "none",
  "riskState": "none",
  "resourceDisplayName": "Windows Azure Service Management API",
  "deviceDetail": {
    "deviceId": "",
    "displayName": "",
    "operatingSystem": "MacOs",
    "browser": "Edge 102.0.1245",
    "isCompliant": false,
    "isManaged": false,
    "trustType": ""
  },
  "location": {
    "city": "Seattle",
    "state": "Washington",
    "countryOrRegion": "US",
    "geoCoordinates": {
      "altitude": null,
      "latitude": 47.61837,
      "longitude": -122.3142
    }
  }
}
```

Policy Number	When *this* happens	Then do *this*
1	An access attempt is made: - To Exchange Online - By Jane Smith	Grant access with: - MFA
2	An access attempt is made: - To Exchange Online - By Jane Smith	Grant Access with: - Compliant Device

Condition	Controls Required
Jane Smith is attempting to access Exchange Online	MFA *AND* Compliant Device

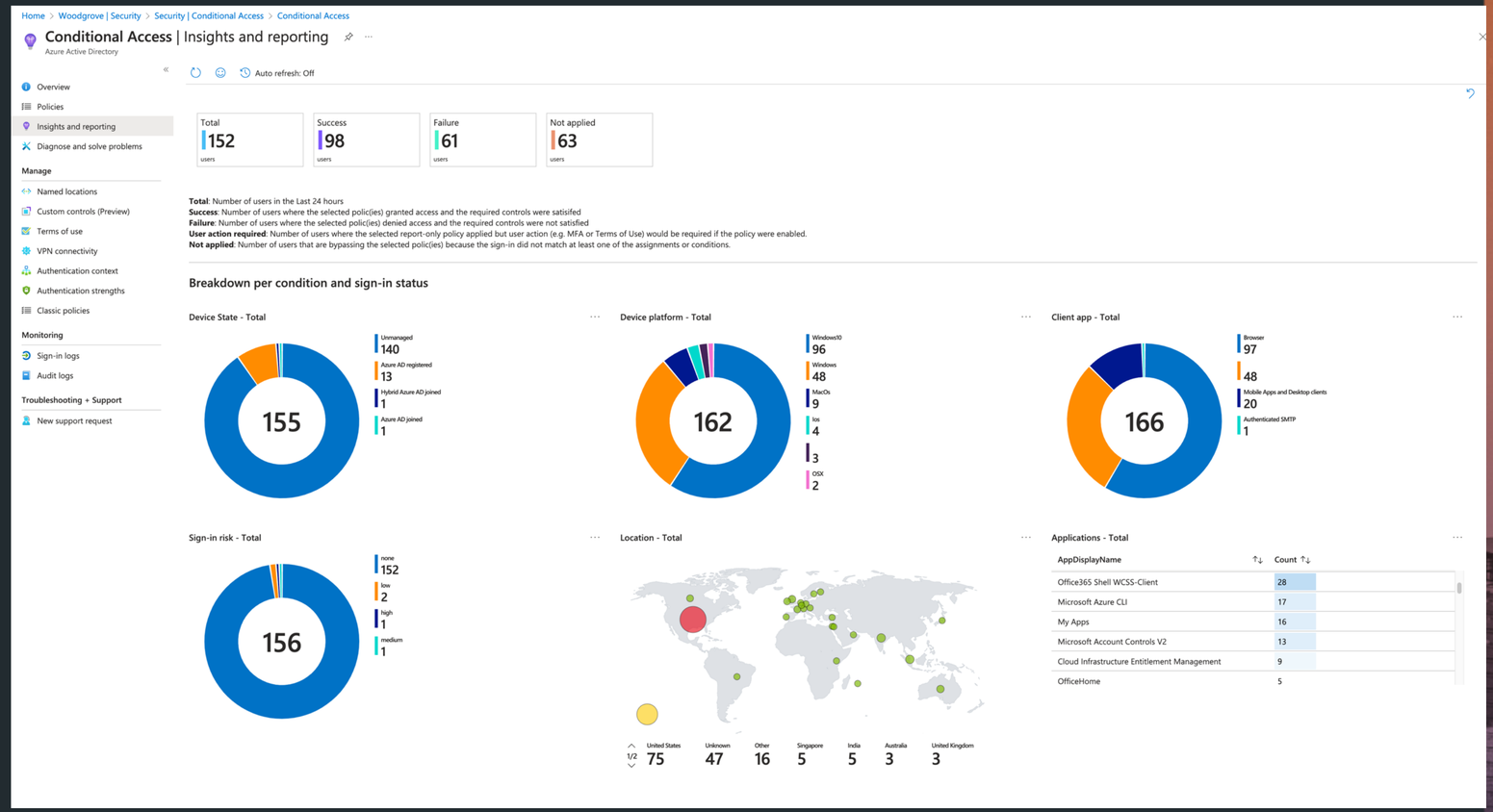


Condition	Controls Required
Jane Smith is attempting to access Exchange Online	MFA *AND* Compliant Device

Conditional Access Insights and Reporting

Understand the impact of CA Policies over time in your org

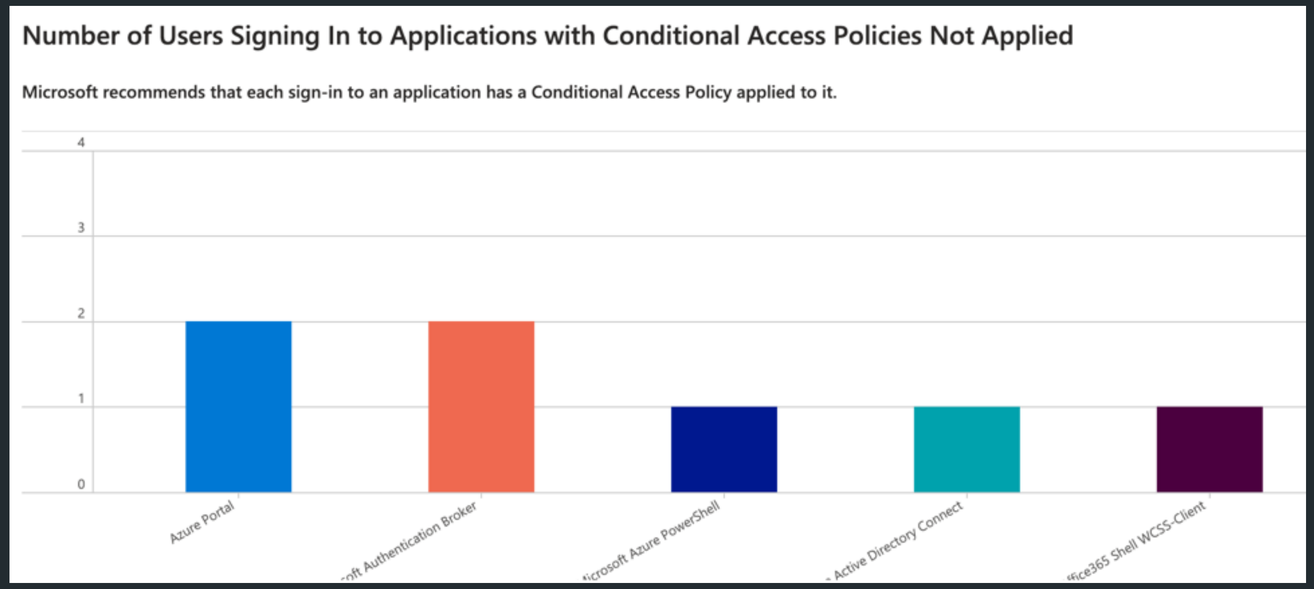
aka.ms/CAInsights



Conditional Access Gap Analyzer Workbook

- Legacy Auth Sign-Ins
- Apps with No CA Policies Applied
- High Risk Sign-In with no CA
- Sign-Ins by location/ Named Locations with no CA Policy (Includes IPv6)
- KQL based!

aka.ms/CAGapAnalyzer



Agenda

Conditional Access Recap

Common Deployments & Issues

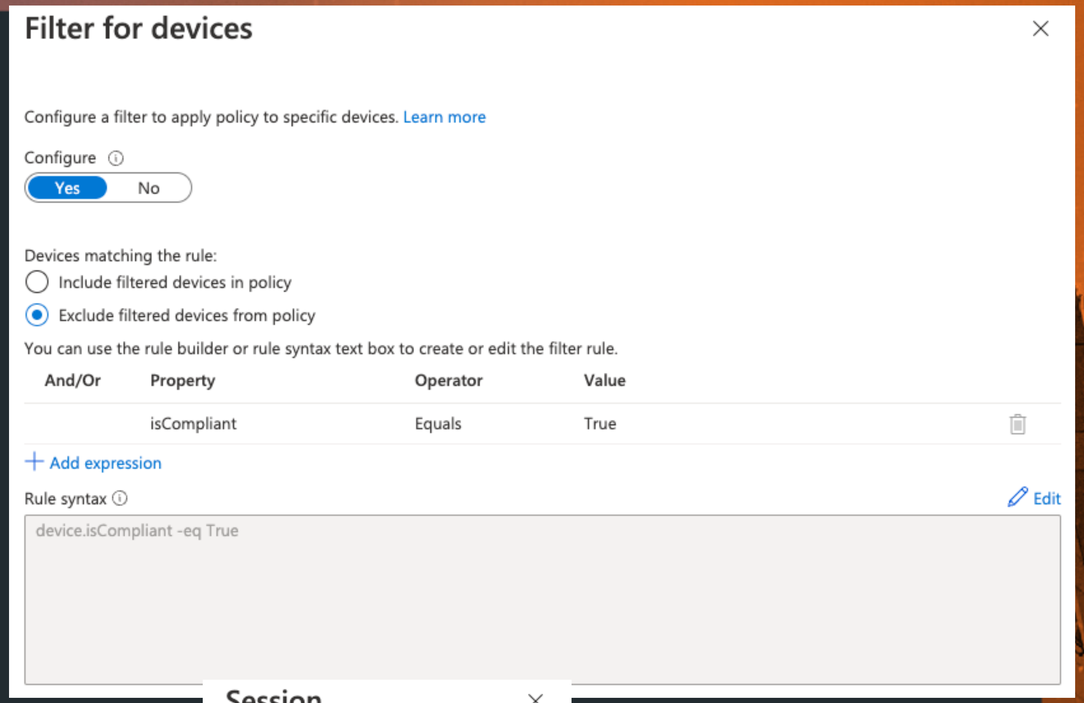
Jamf Pro & Conditional Access

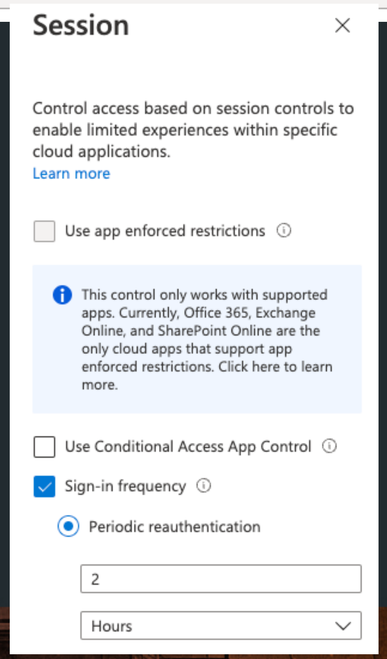
Jamf Connect & Conditional Access

Go Do’s!

Common CA Policies

- Requiring strong authentication (MFA, phish-resistant credentials)
- Blocking legacy auth
- Blocking access by country location
- Require compliant or hybrid join device
- Stricter Controls for non-corp managed devices (is this macOS in your environment?)
  - Sign-In Frequency to 2 hours for everything not filtered out
- Applying polices to “All Apps”



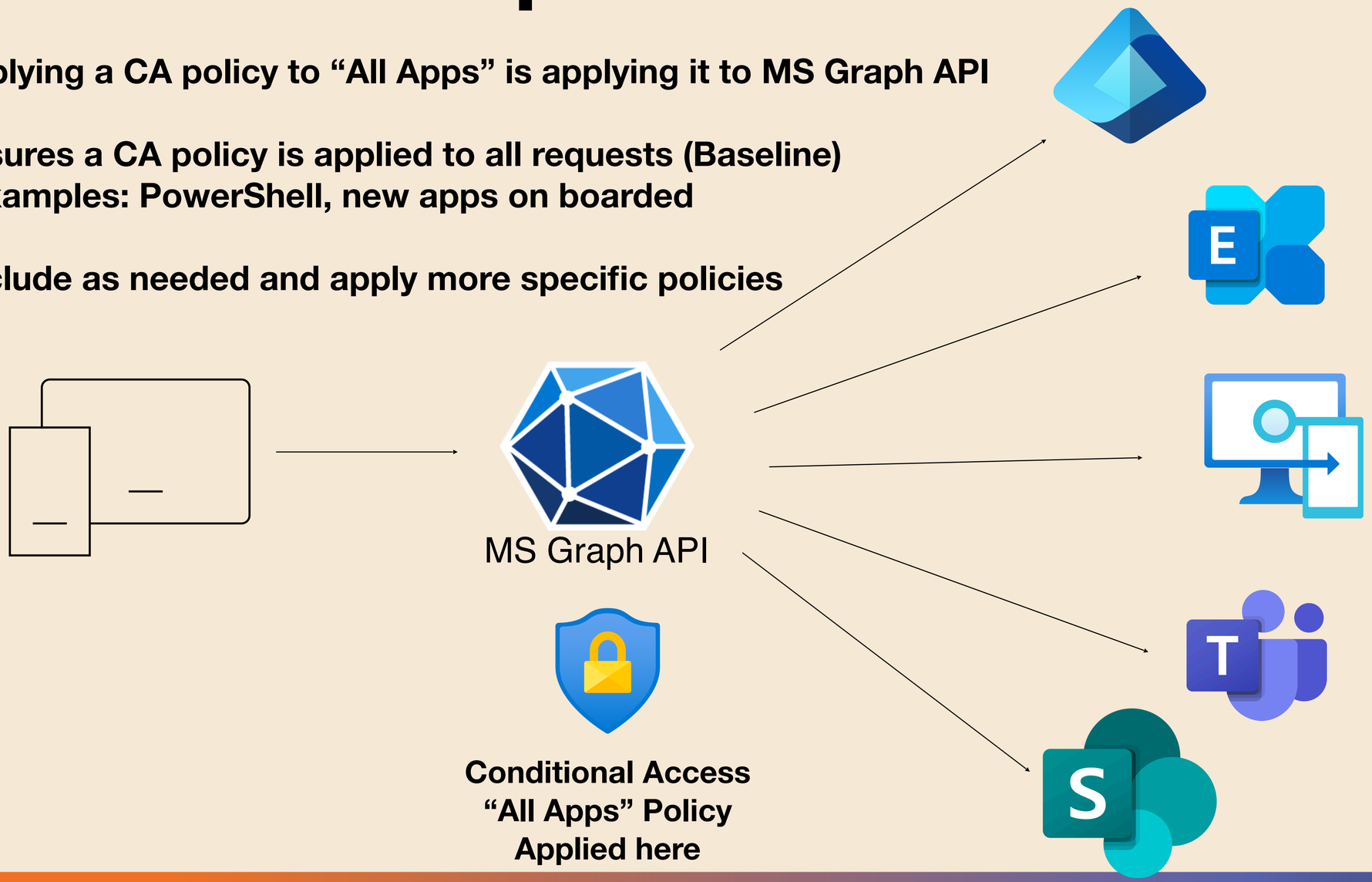


Common Issues

Device Registration Failures
Frequent Authentication Prompts
Compliant Device Check Fail
Confusion around which policy did what
Jamf Connect and Conditional Access w/ MFA

Microsoft Graph API

- Applying a CA policy to “All Apps” is applying it to MS Graph API
- Ensures a CA policy is applied to all requests (Baseline)
  - Examples: PowerShell, new apps on boarded
- Exclude as needed and apply more specific policies



All Apps Policy Challenges

- CA policy to “All Apps” Require MFA
- You have an ROPG/ROPC OAuth flow (no web UI)
- Valid username/password, no UI for MFA challenge response
- Sign-In Log errors
- Increased ‘User Risk’ level in Entra ID Protection

Agenda

Conditional Access Recap

Common Deployments & Issues

Jamf Pro & Conditional Access

Jamf Connect & Conditional Access

Go Do’s!

Device Compliance

jamf | PRO

Microsoft Entra ID
(formerly Azure AD)

macOS

iOS
iPadOS

Rules

- ✅ OS Updated / CIS/NIST Compliant
- ✅ Password Policy / Obtained Entra Device ID
- ✅ Full Disk Encryption / Apps Updated

✅ **Compliant**

Microsoft Conditional Access

jamf | PRO

Microsoft Entra ID
(formerly Azure AD)

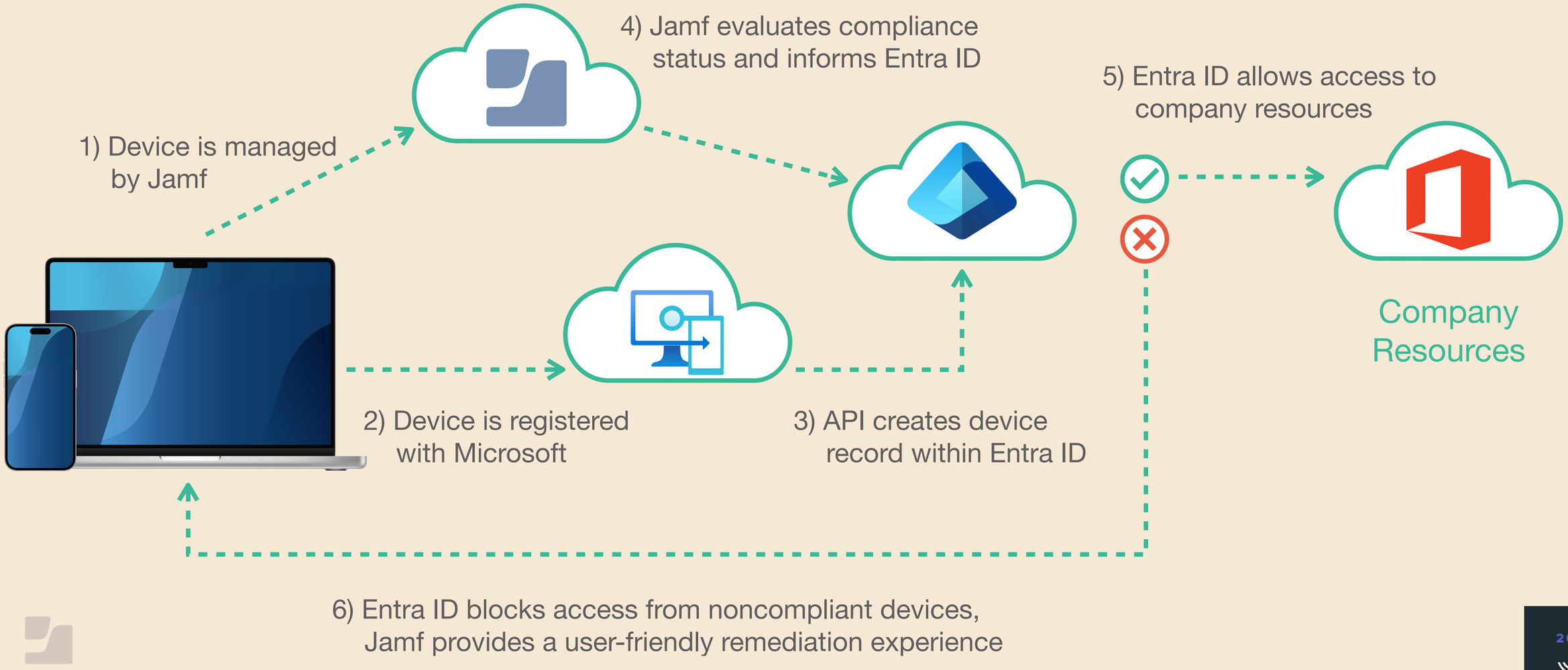
macOS 

iOS
iPadOS 

Compliant

Device Compliance

with Jamf and Microsoft



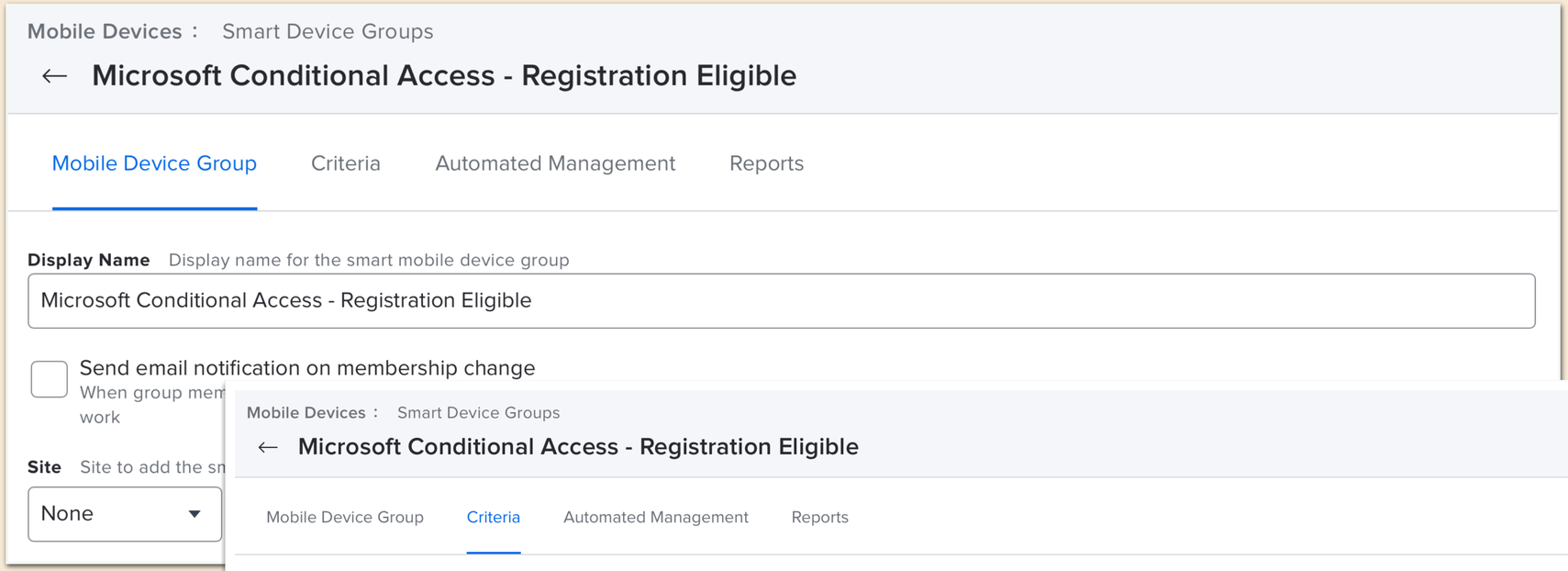
Jamf Pro Setup

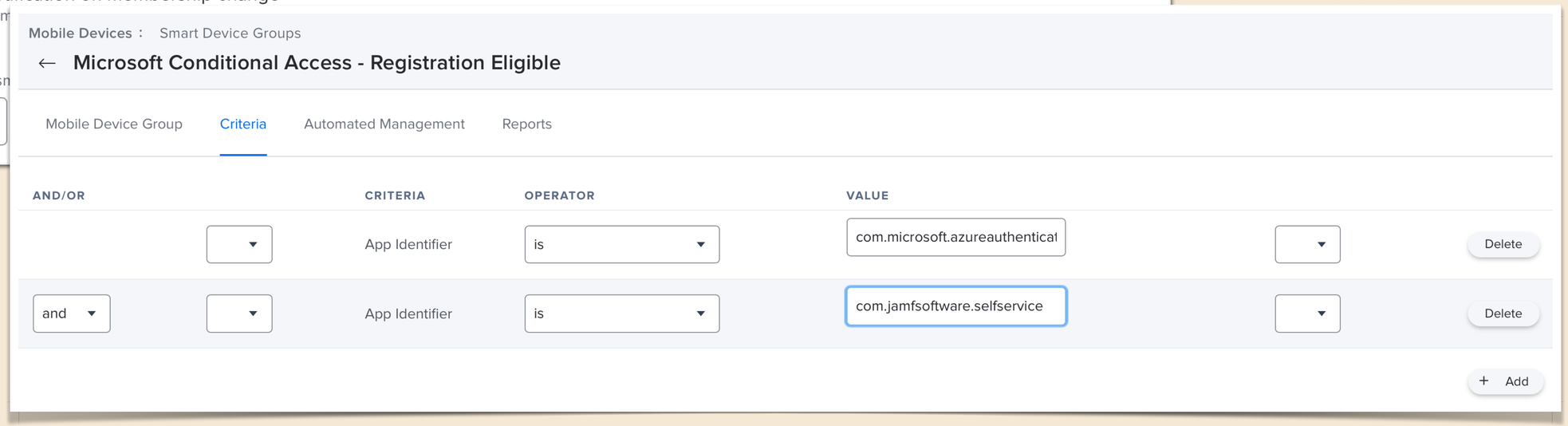
Prerequisites:

- Jamf Pro - 10.43 or greater - cloud hosted
- Microsoft Intune administrator
- VPP licenses for Microsoft Authenticator app
- Microsoft Company Portal app

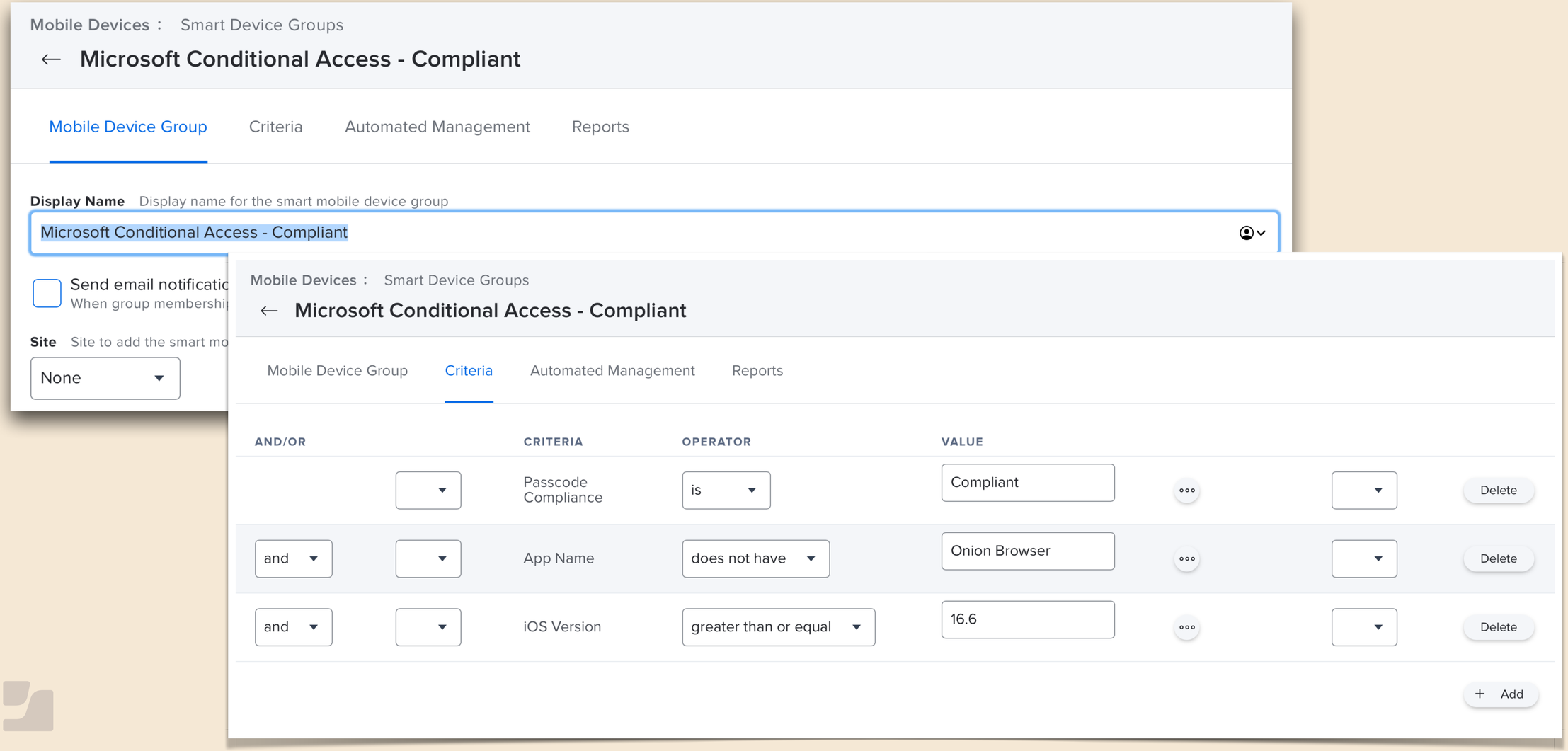
learn.jamf.com
Search: Device Compliance

Jamf Pro Setup

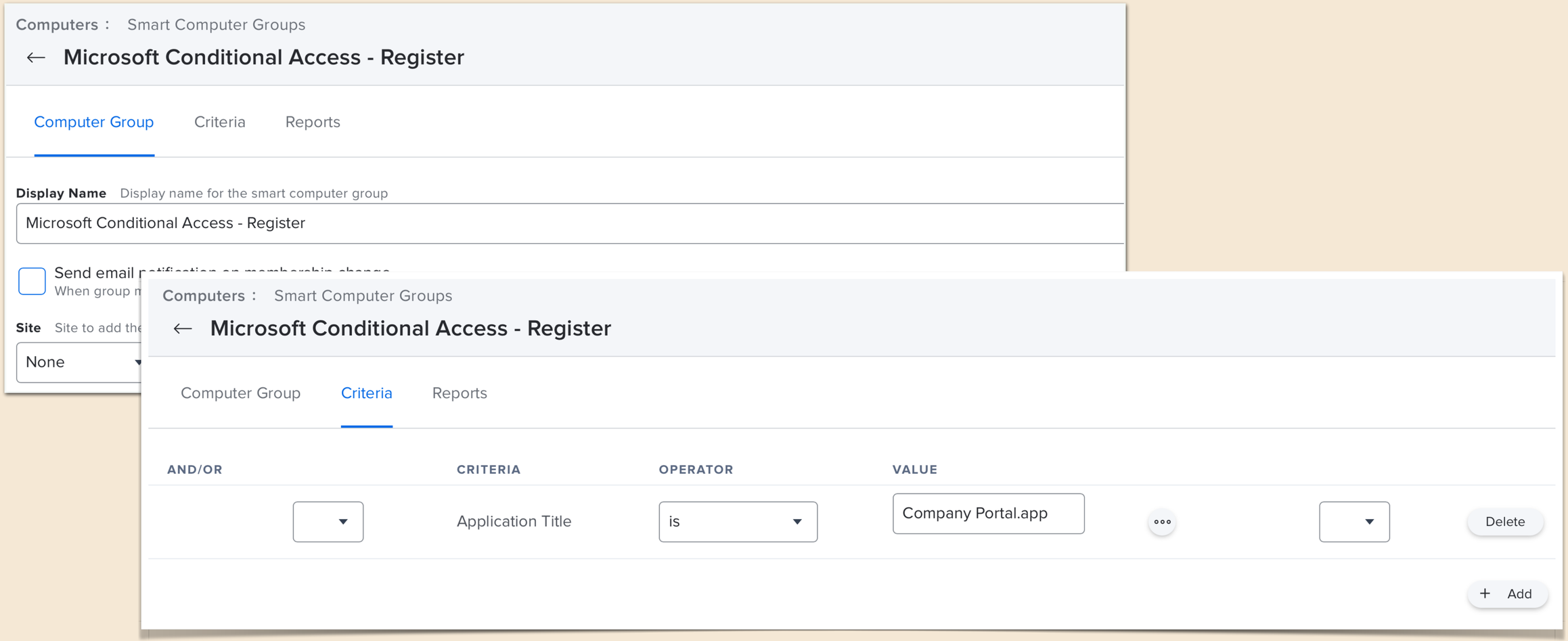




Jamf Pro Setup



Jamf Pro Setup



Jamf Pro Setup

Computers : Smart Computer Groups

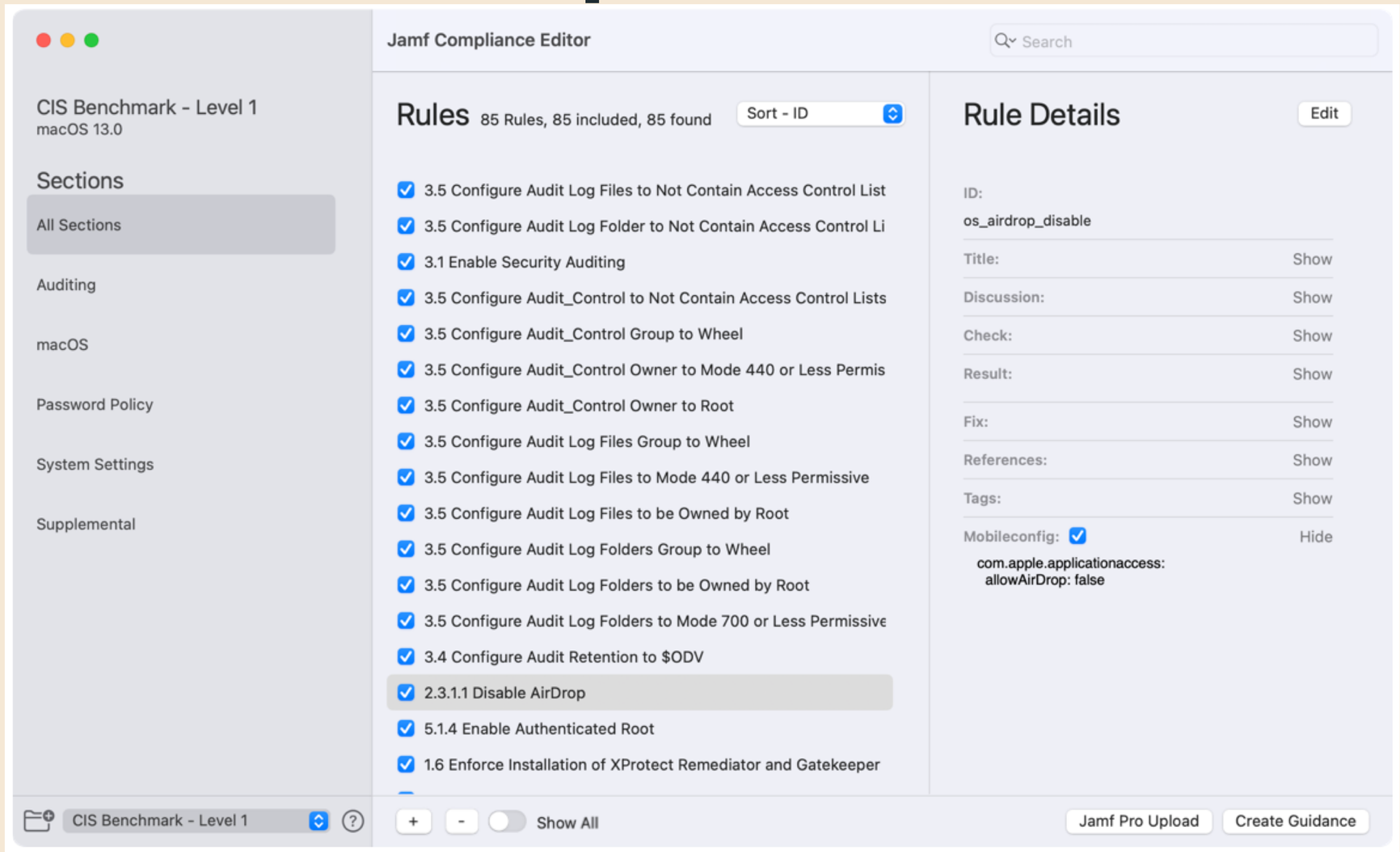
← Microsoft Conditional Access - Compliant

Computer Group | Criteria | Reports

AND/OR		CRITERIA	OPERATOR	VALUE			
		FileVault 2 Partition Encryption State	is	Encrypted	•••		Delete
anc		Jamf Protect: Installation	is	Installed			Delete
anc		Application Title	is	Company Portal.app	•••		Delete
anc		Computer Group	not member of	Jamf Protect: HIGH	•••		Delete

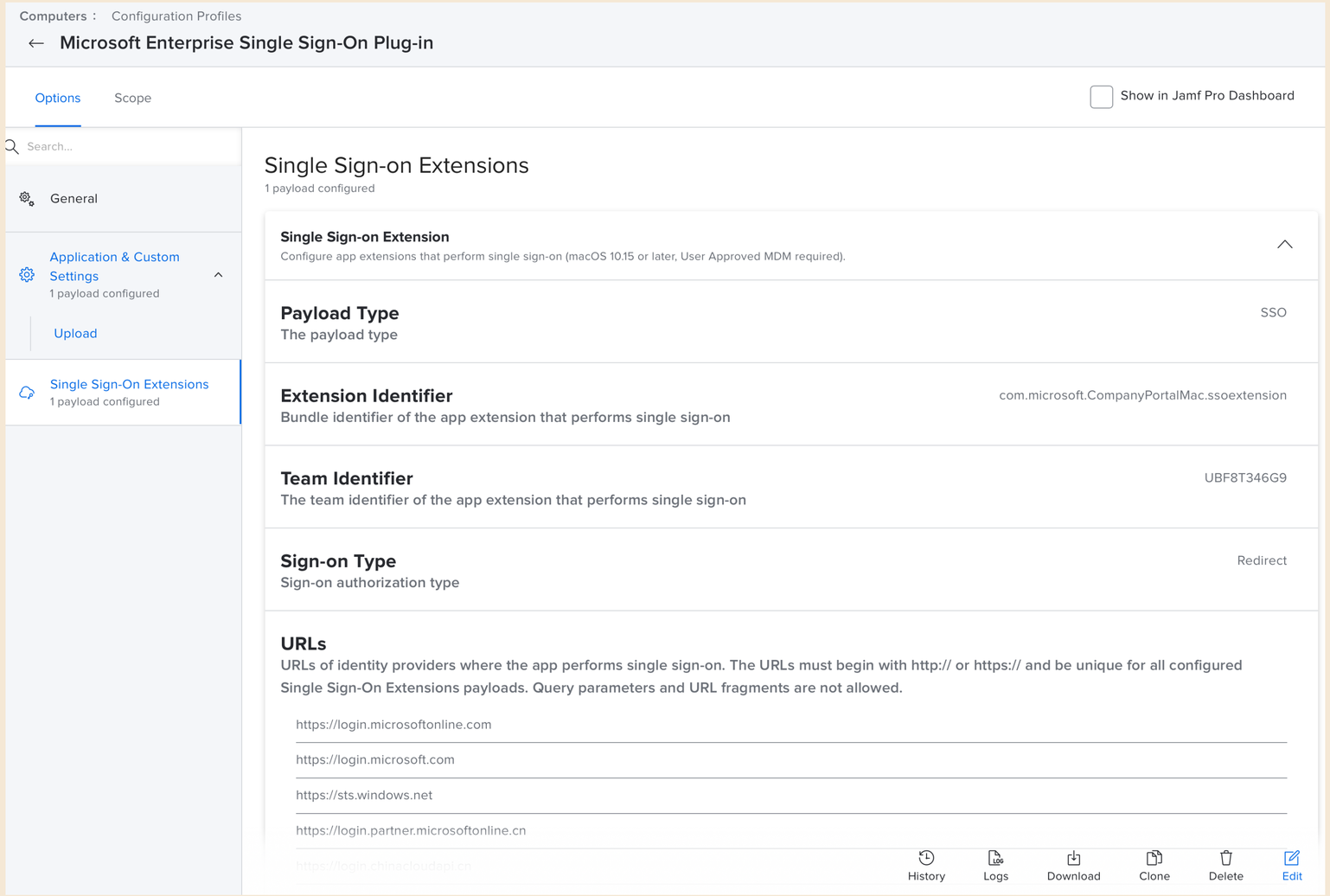
+ Add

Jamf Pro Setup



trusted.jamf.com

Jamf Pro Setup

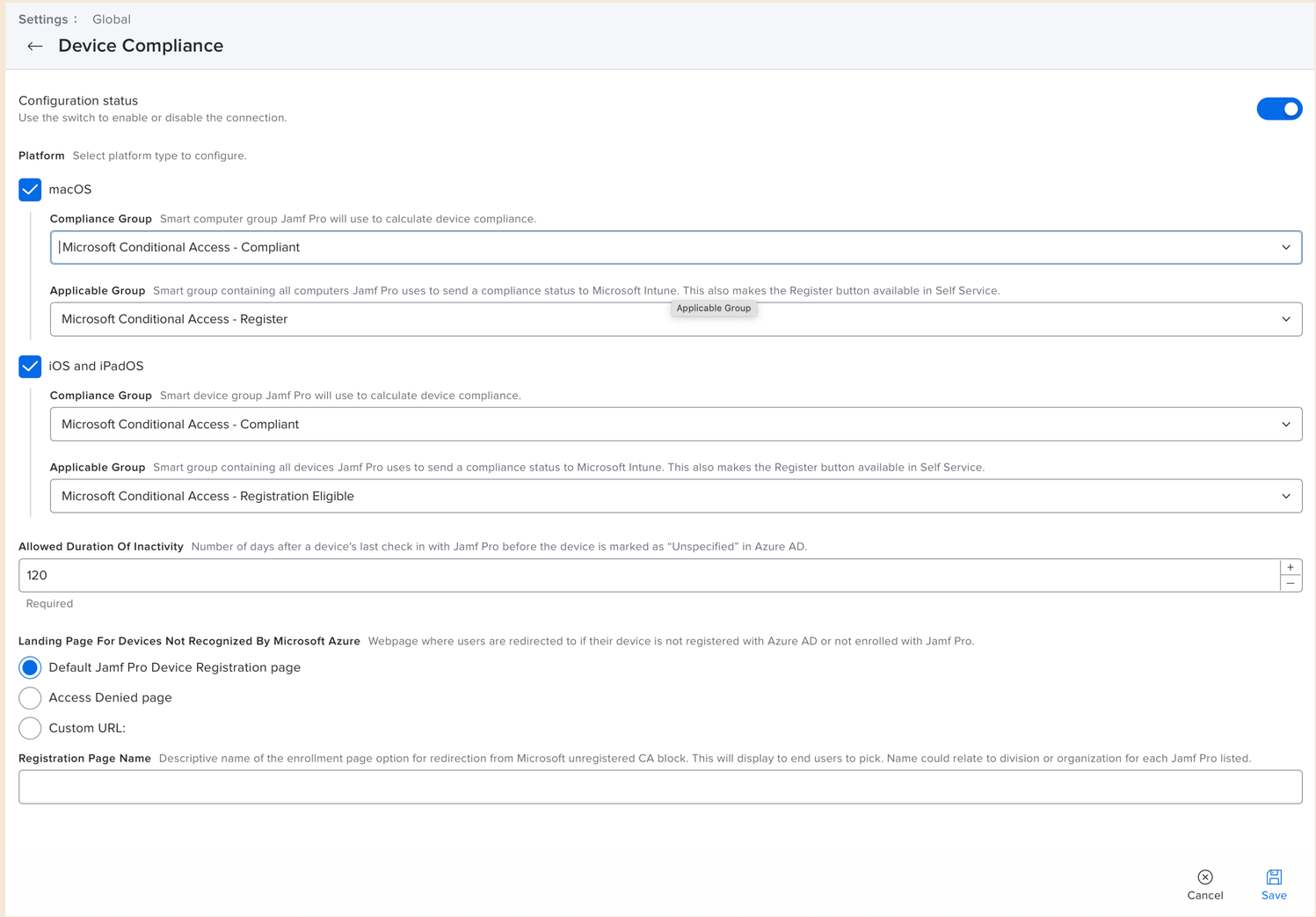


jamf.it/entraSSOe

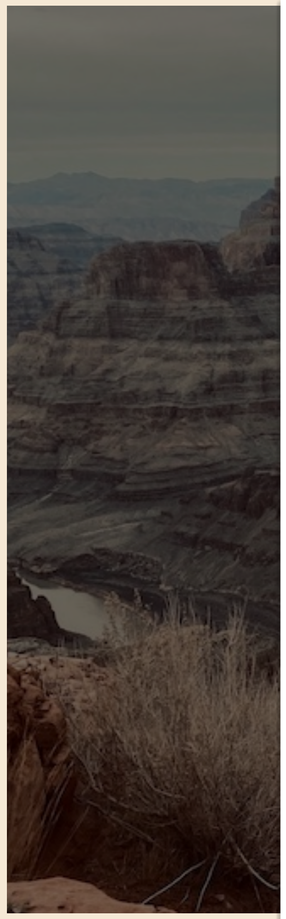
https://jamf.it/entrassoe-ios

Jamf Pro Setup

Jamf Pro Settings ->
Global ->
Device Compliance



Jamf Pro Setup



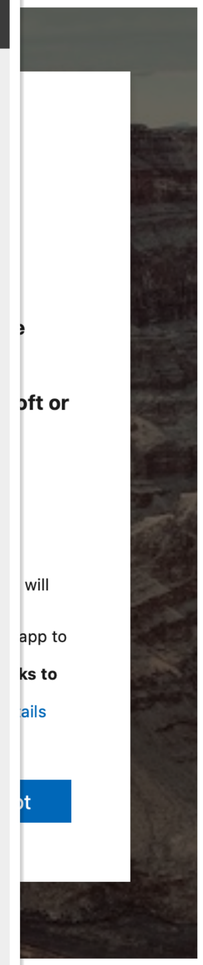
jamf | PRO

Configure Compliance Partner

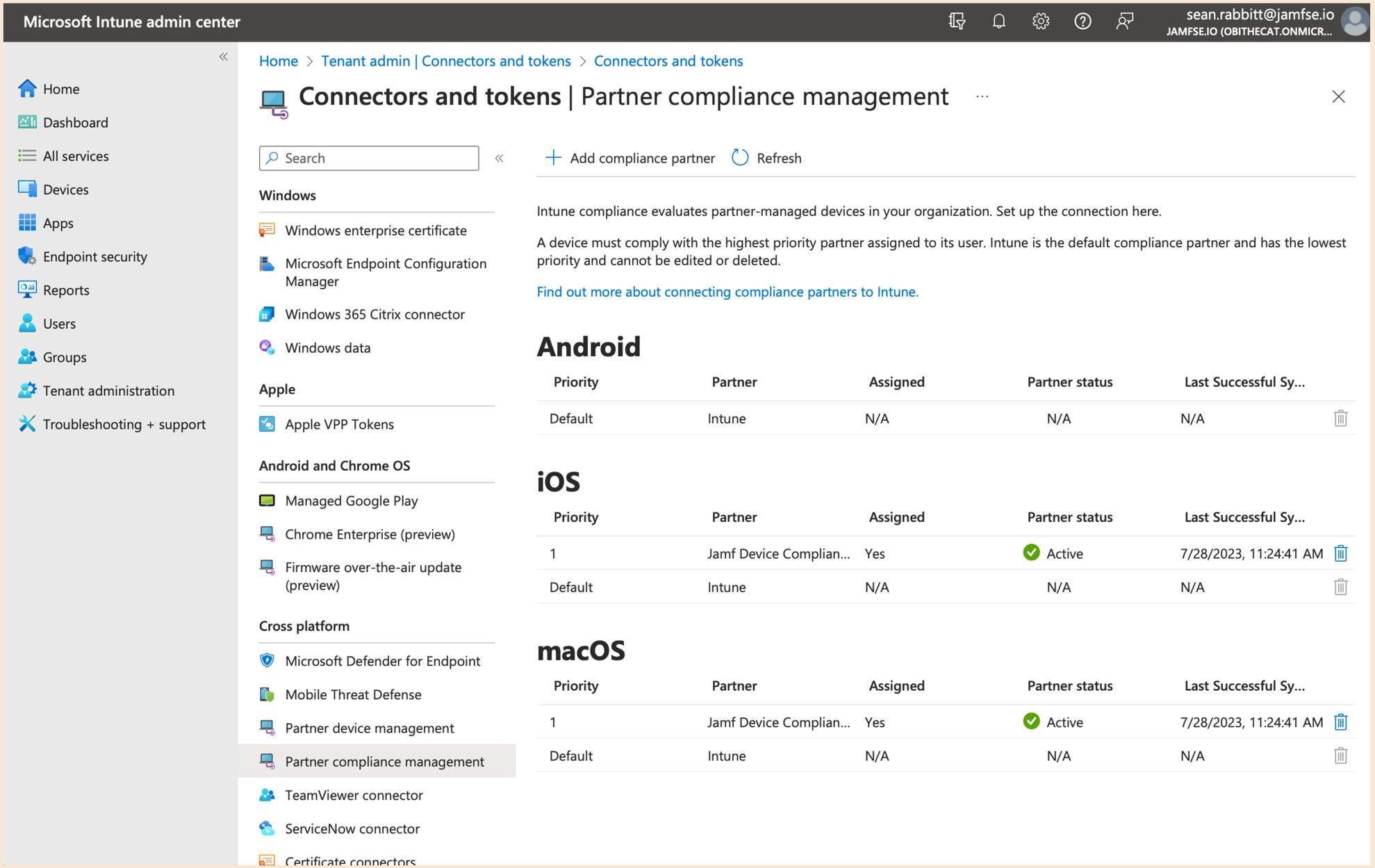
You must add Jamf as a compliance partner in Microsoft Azure before continuing. When adding the compliance partner, assign it to the AAD groups you wish to use to calculate device compliance and select your platform type.

Open Microsoft Endpoint Manager

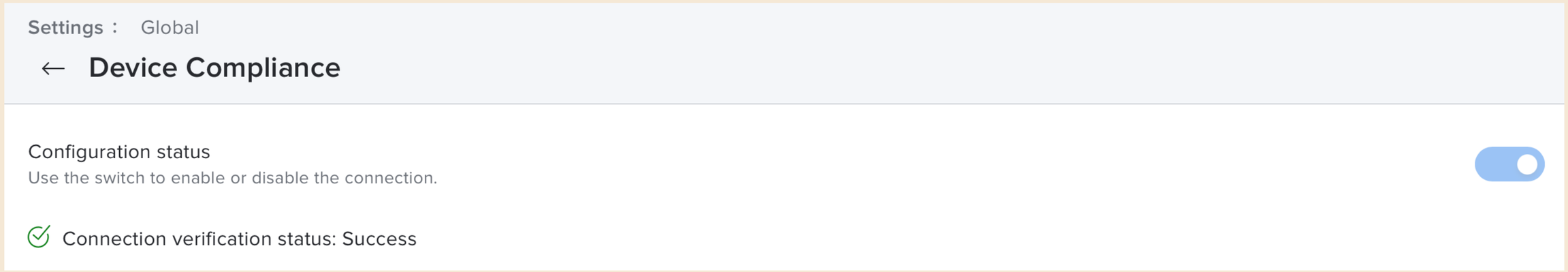
Cancel Confirm



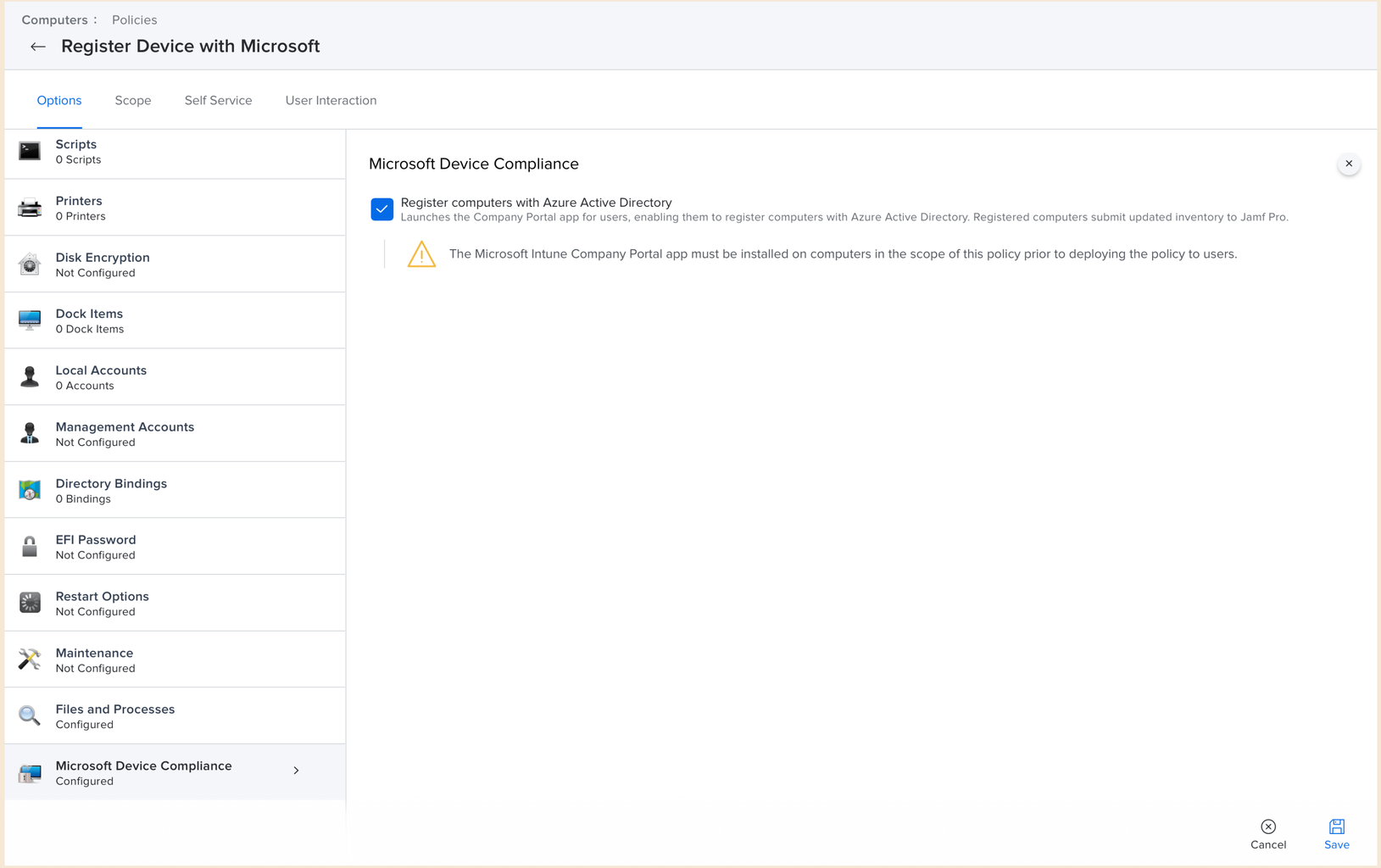
2023 JNUC



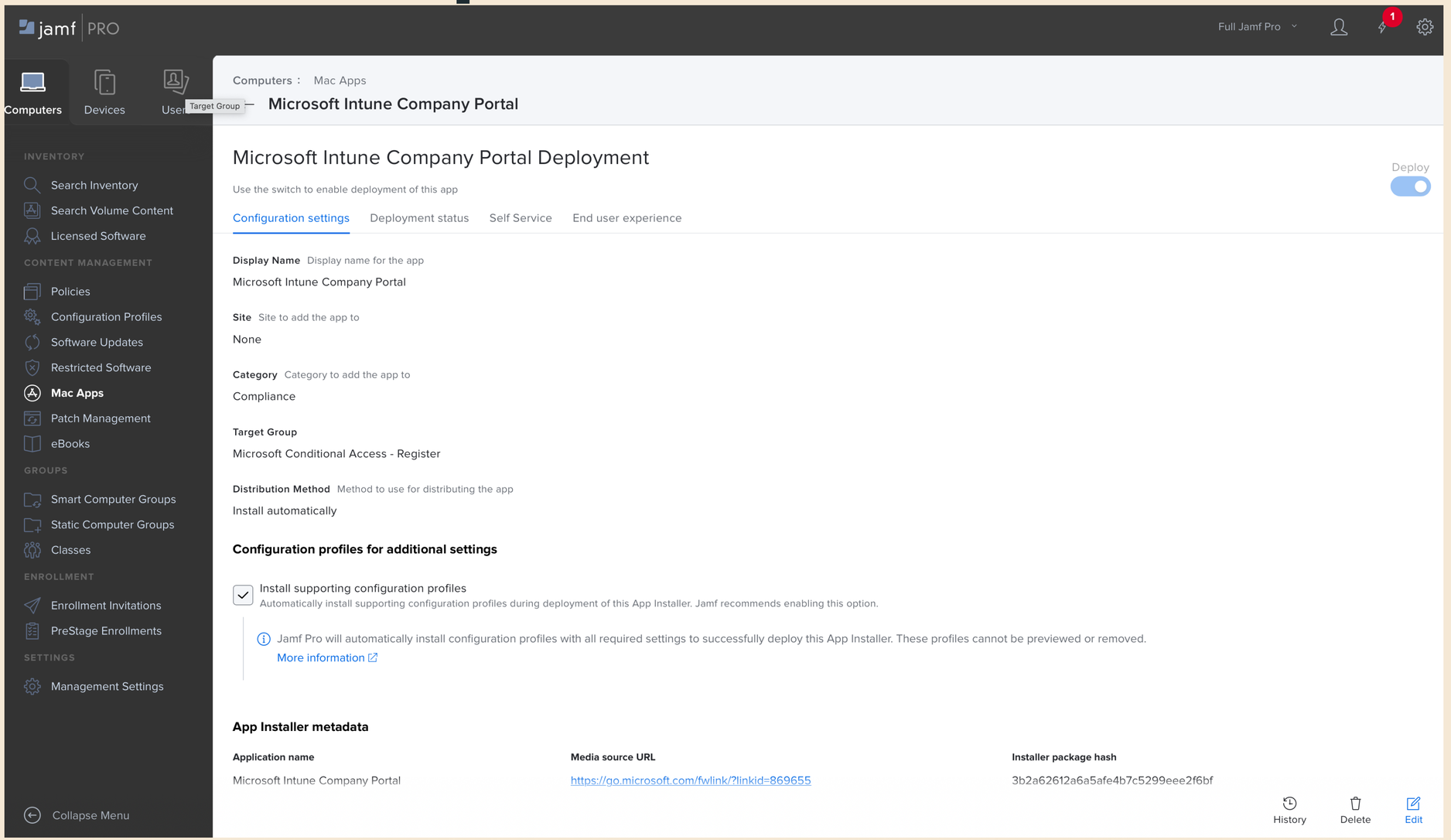
Jamf Pro Setup



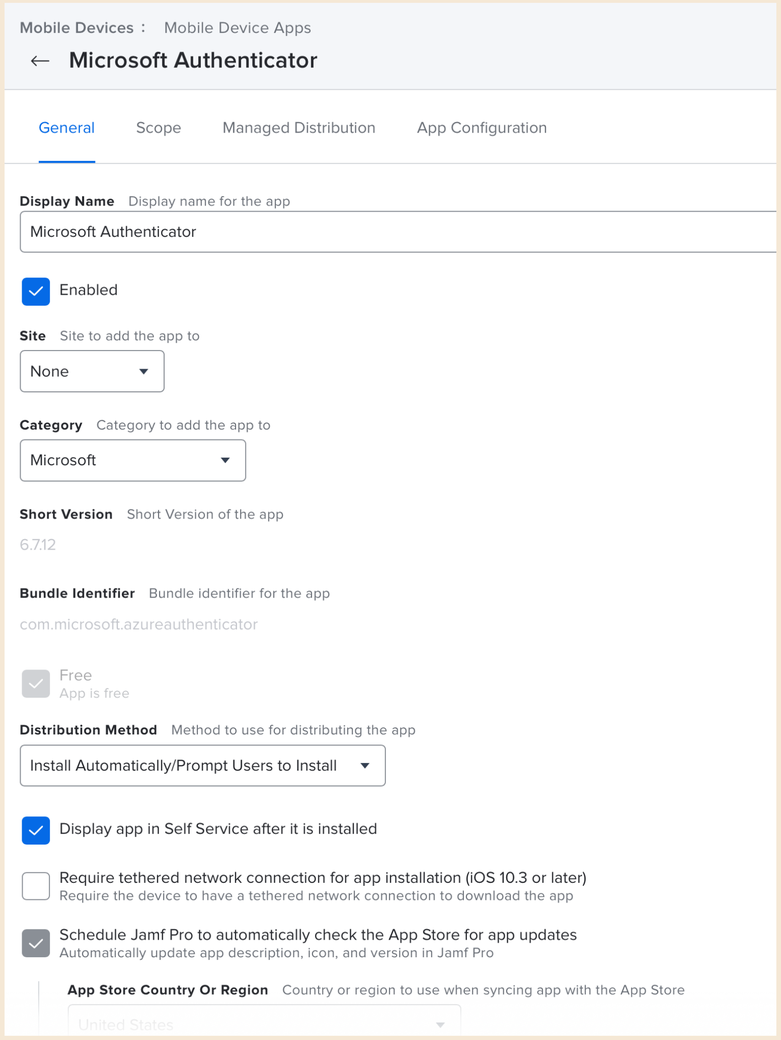
Jamf Pro Setup



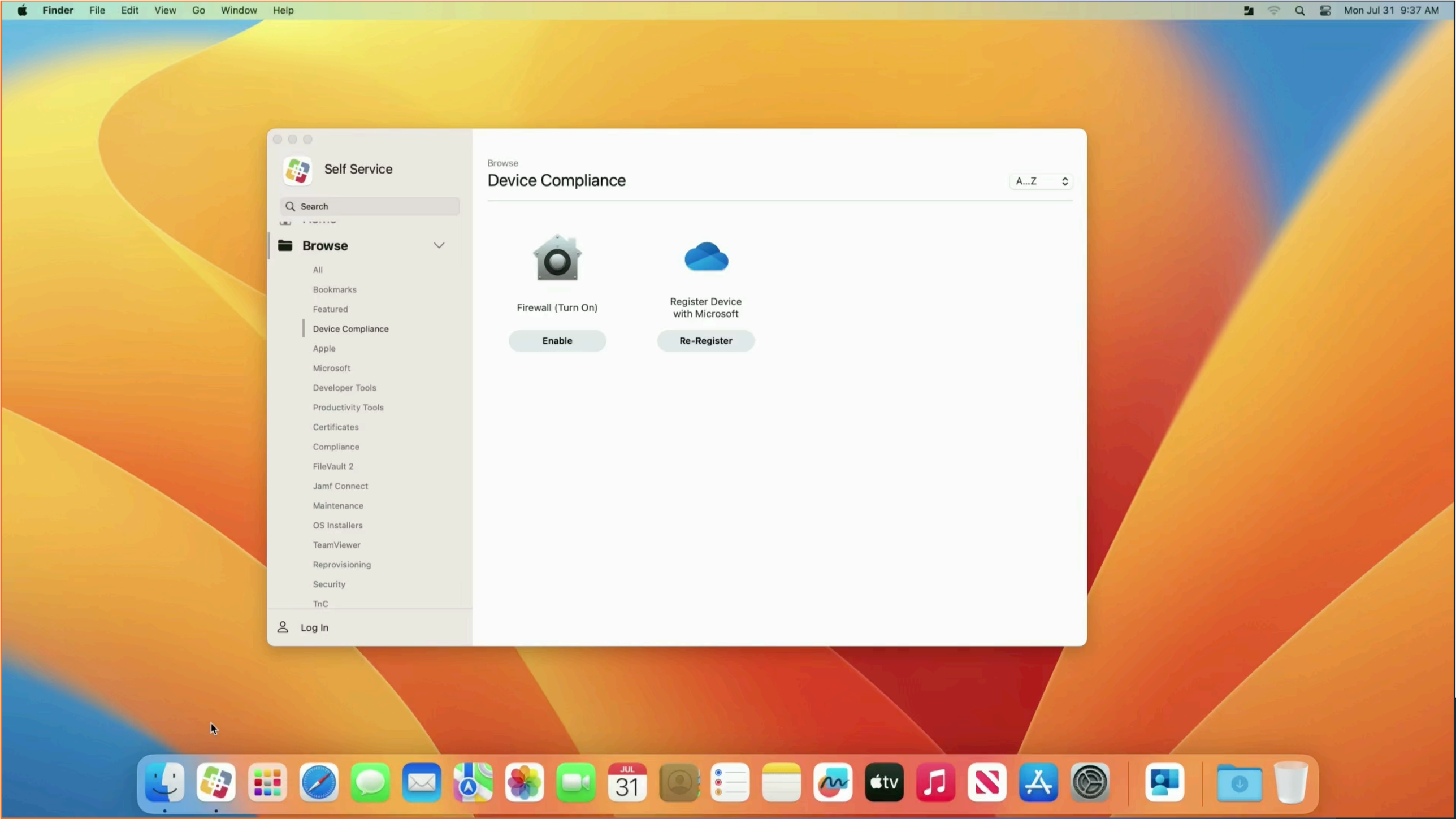
Jamf Pro Setup

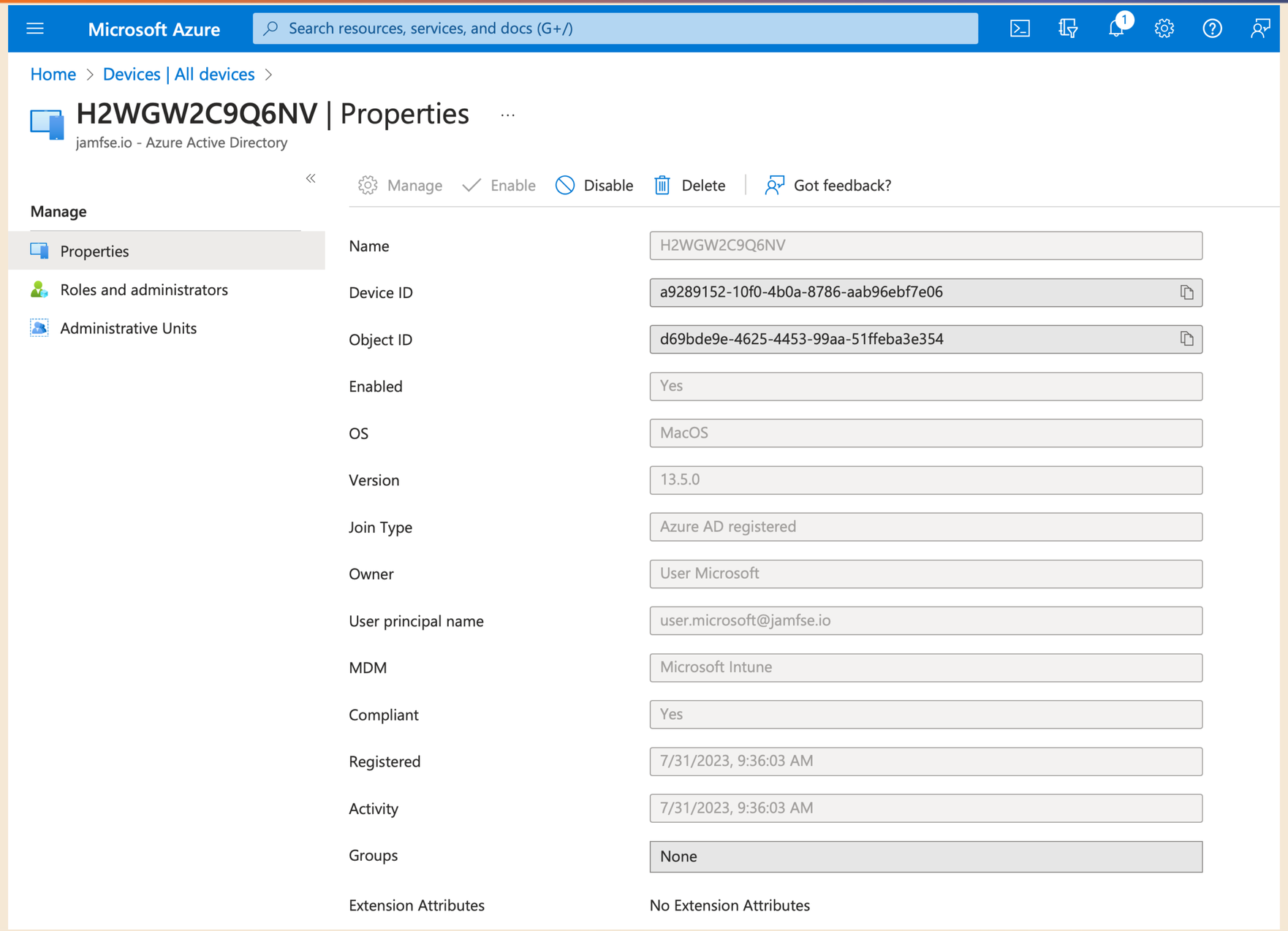


Jamf Pro Setup




Finder
File
Edit
View
Go
Window
Help
Mon Jul 31 9:35 AM
JUL
31
tv


Finder File Edit View Go Window Help
Mon Jul 31 9:37 AM
Self Service
Search
Browse
All
Bookmarks
Featured
Device Compliance
Apple
Microsoft
Developer Tools
Productivity Tools
Certificates
Compliance
FileVault 2
Jamf Connect
Maintenance
OS Installers
TeamViewer
Reprovisioning
Security
TnC
Log In
Browse
Device Compliance
A...Z
Firewall (Turn On)
Enable
Register Device with Microsoft
Re-Register
JUL
31



Agenda

Conditional Access Recap
Common Deployments & Issues
Jamf Pro & Conditional Access
Jamf Connect & Conditional Access
Go Do’s!

Remember when we said Conditional Access applies to Cloud Apps?

Cloud Apps ARE NOT

Mobile or desktop apps
OpenID Connect / OAuth 2.0 native clients

Jamf Connect is one of these!

Reminder: CA is applied to the RESOURCE
Ex: You apply it to Exchange Online, NOT Outlook

So…how do you trigger things like MFA when using Jamf Connect?

You call some other API!

But which API?

There’s a few options:

API	Pros	Cons
Azure AD Graph API	Been around forever	Support is ending!
Microsoft Graph API	Fully supported	Cannot be excluded from All Apps Conditional Access policies
Custom API	Maximum flexibility, can exempt from Conditional Access policies	More configuration work for admins

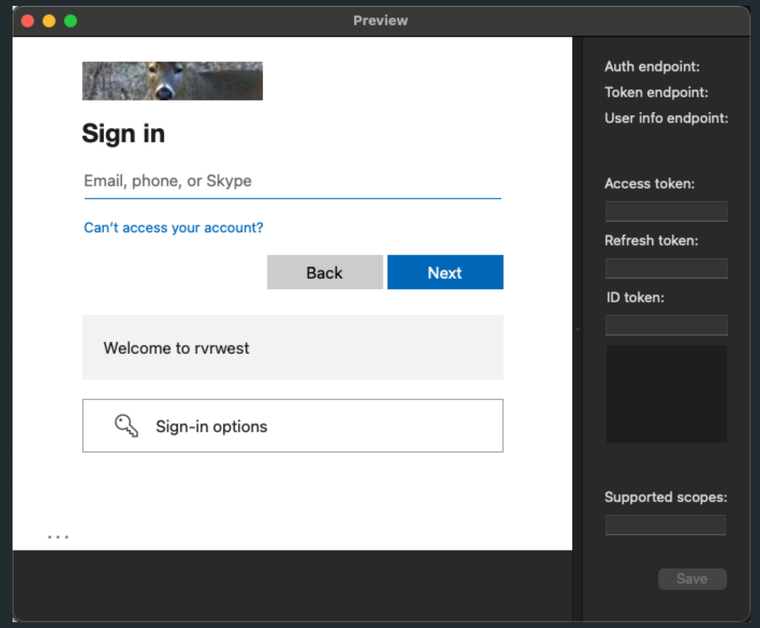
Use this one!

Custom API…why?

- Jamf Connect actually has 2 flows for talking to Entra ID:
  - OIDC
    - Used for interactive web login - any time you see the Entra ID login page
  - ROPG/ROPC
    - Used for non-interactive password checking in the background

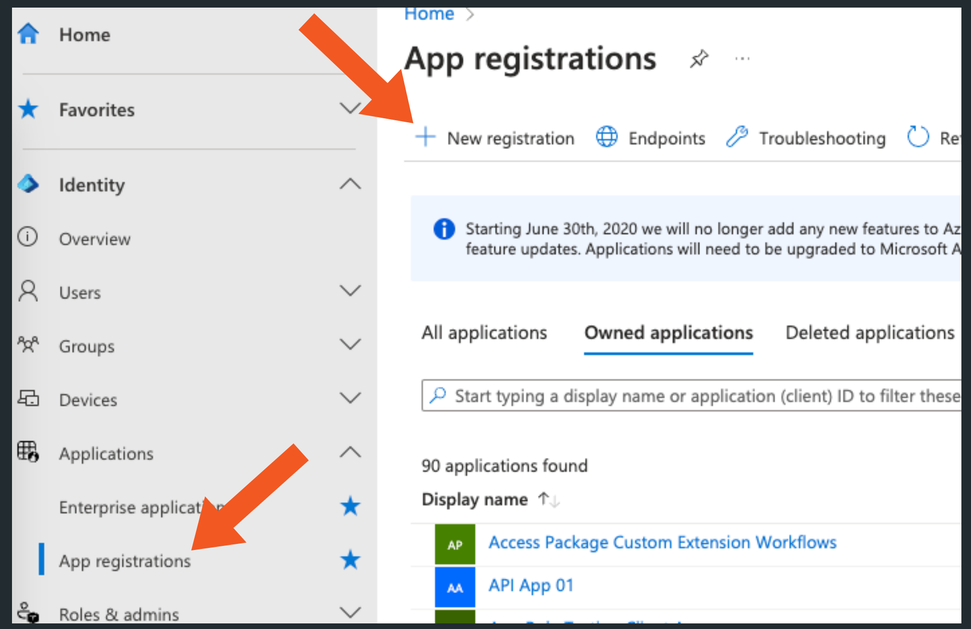
Custom API…why?

OIDC (Auth Code)



ROPG/ROPC

Registering a Custom API in Entra ID

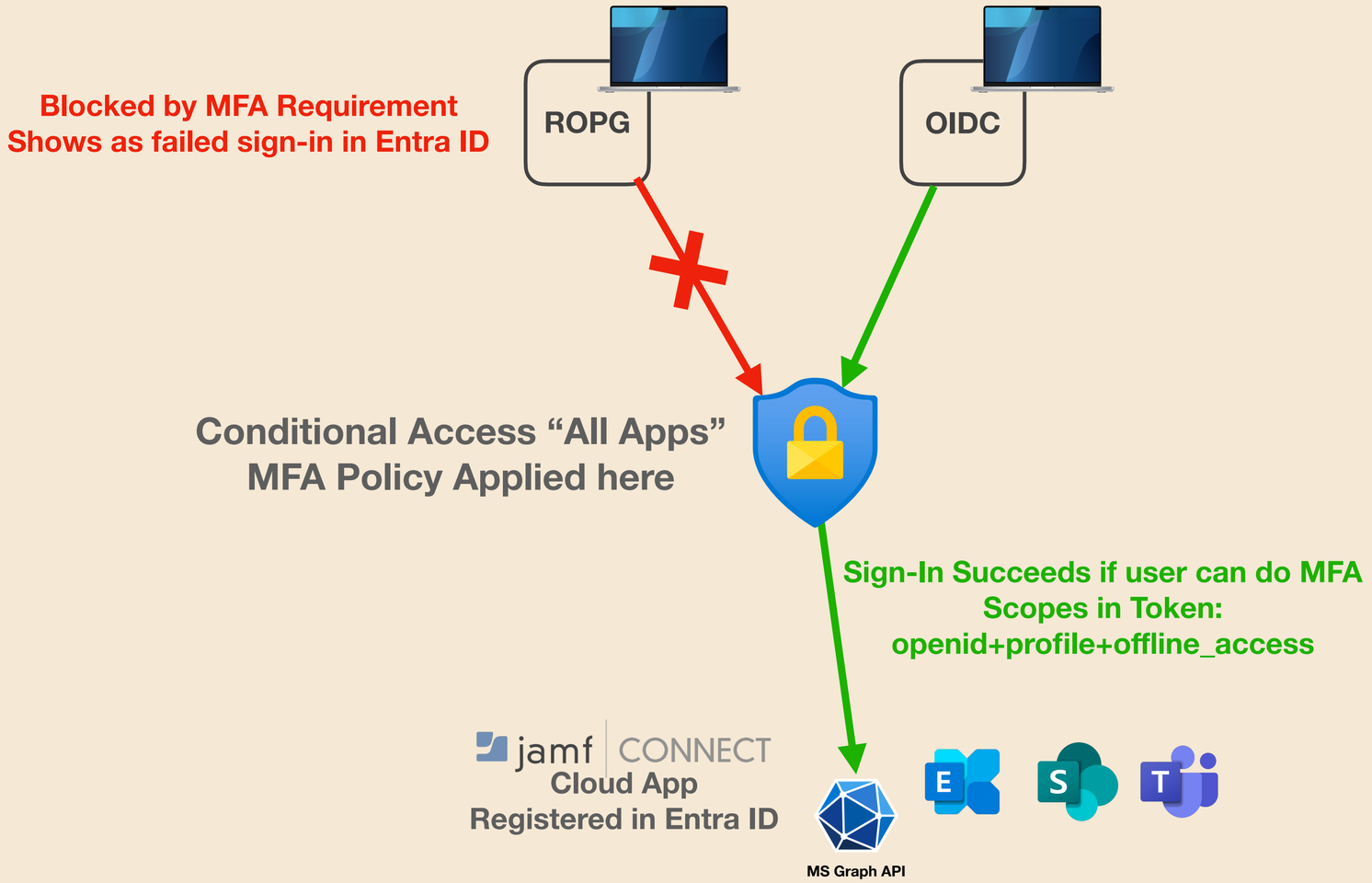


There's still a few issues we need to solve

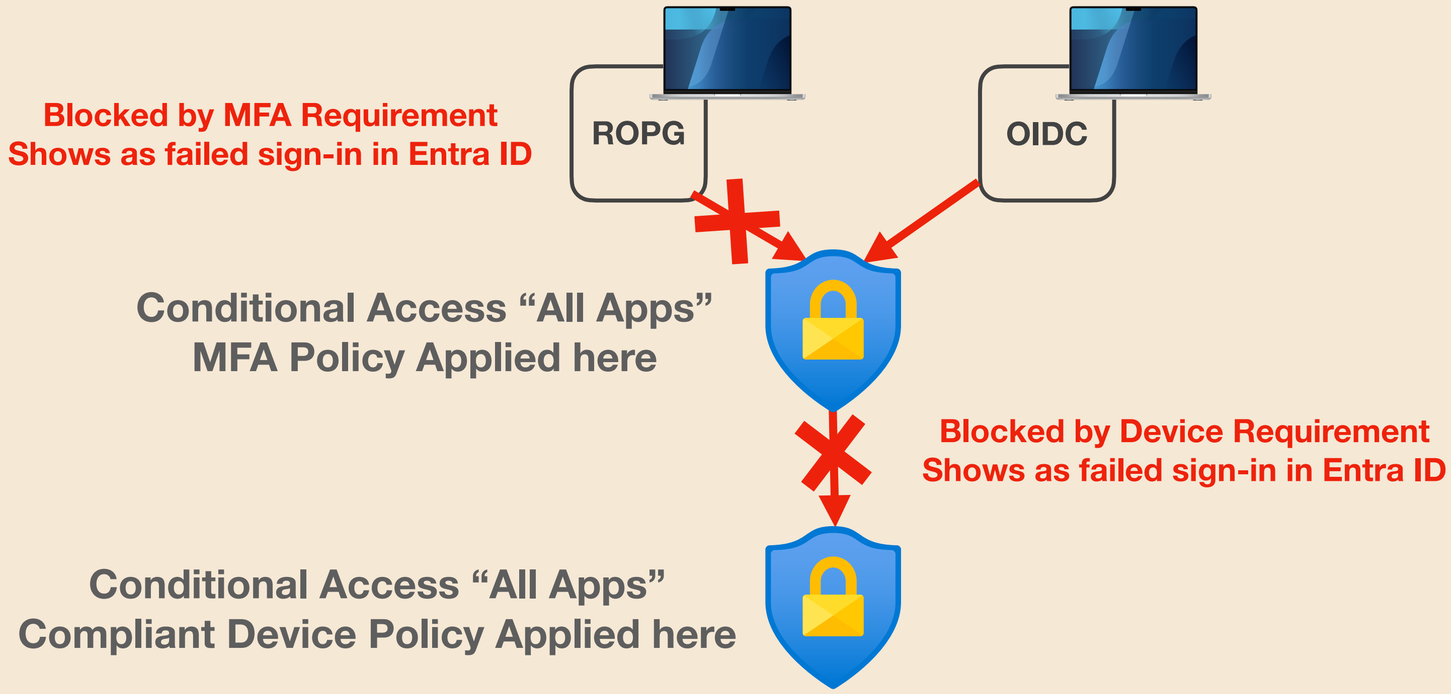
Common Customer Requirements:

1. Require MFA in web UI on lock screen
2. Jamf Connect ROPG checks passwords in the background
3. ROPG background password checks get a successful sign-in event returned in Entra ID logs
4. Mac users have similar security posture as Windows users

Problem 1: MFA Policies



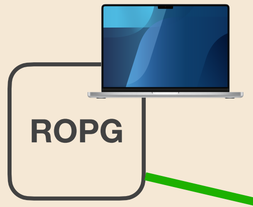
Problem 2: Compliant Device Policies

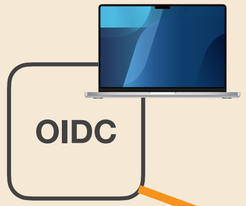


jamf | CONNECT
Cloud App
Registered in Entra ID

MS Graph API

Problem 3: Exclusions





Sign-In Succeeds
But No MFA…

Sign-In Succeeds
No MFA

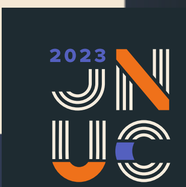
jamf CONNECT
Cloud App
Registered in Entra ID

Exempted from All Apps
policies

Conditional Access “All Apps”
MFA Policy Applied here

Conditional Access “All Apps”
Compliant Device Policy Applied here

MS Graph API



What now?

How do we meet all 3 requirements?

We need more than one custom App and API!

aka.ms/JC_CA

Solution

jamf CONNECT
ROPG Cloud App
Registered in Entra ID

Exempted from All Apps policies

Sign-In Succeeds
No MFA

ROPG

OIDC

Sign-In Succeeds if user can do MFA
Scopes in Token:
Jamfconnect+openid+profile+offline_access

Conditional Access “All Apps”
MFA Policy Applied here

jamf CONNECT
API Cloud App
Registered in Entra ID

Subject to All Apps MFA Policies

Requests custom API scope

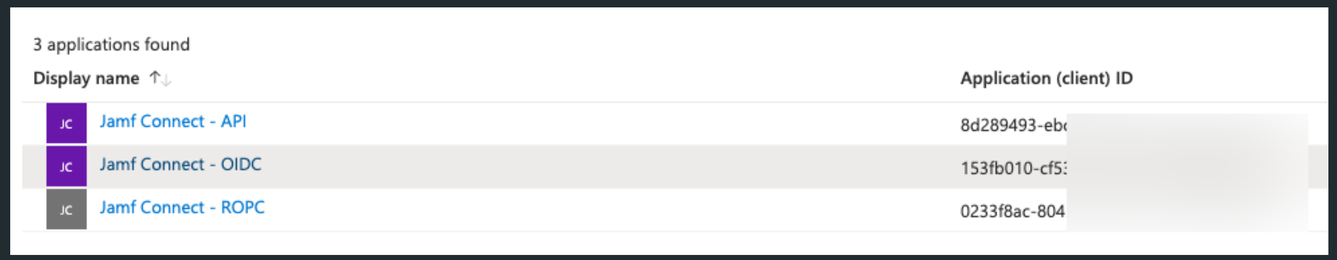
jamf CONNECT
OIDC Cloud App
Registered in Entra ID

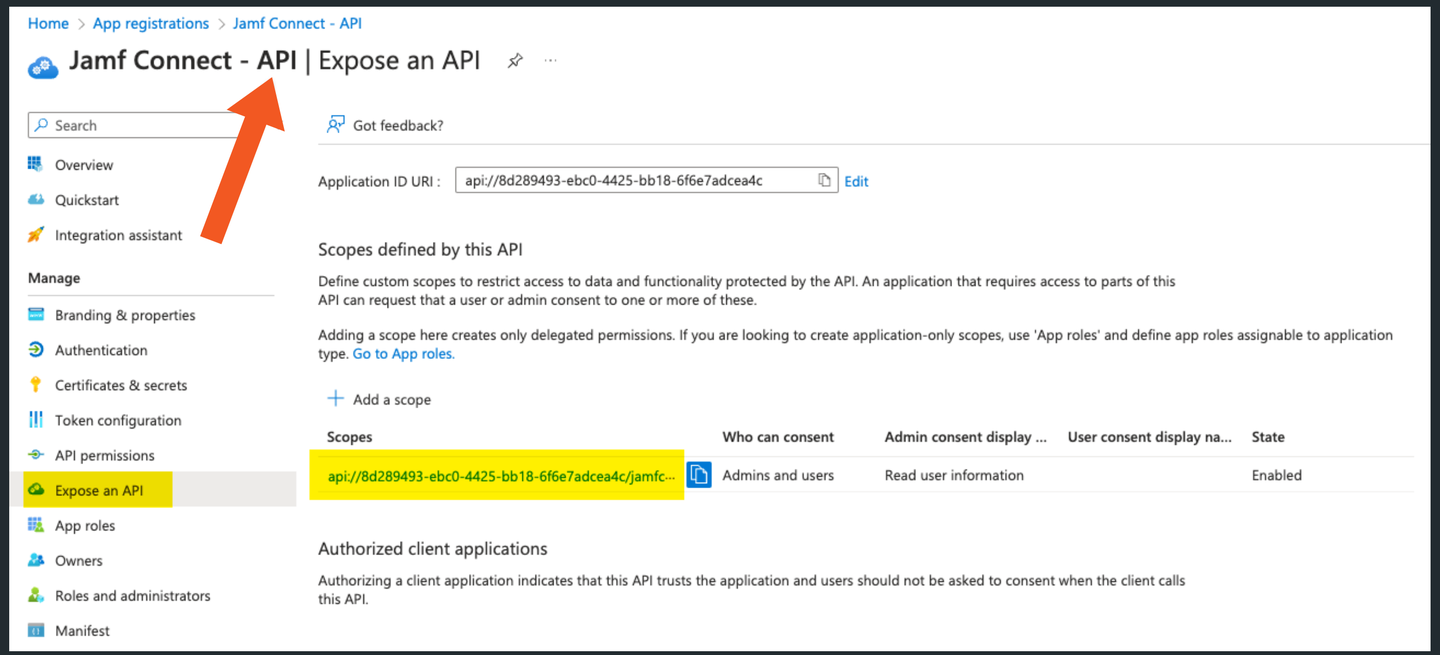
Exempted from All Apps policies

Conditional Access “All Apps”
Compliant Device Policy Applied here

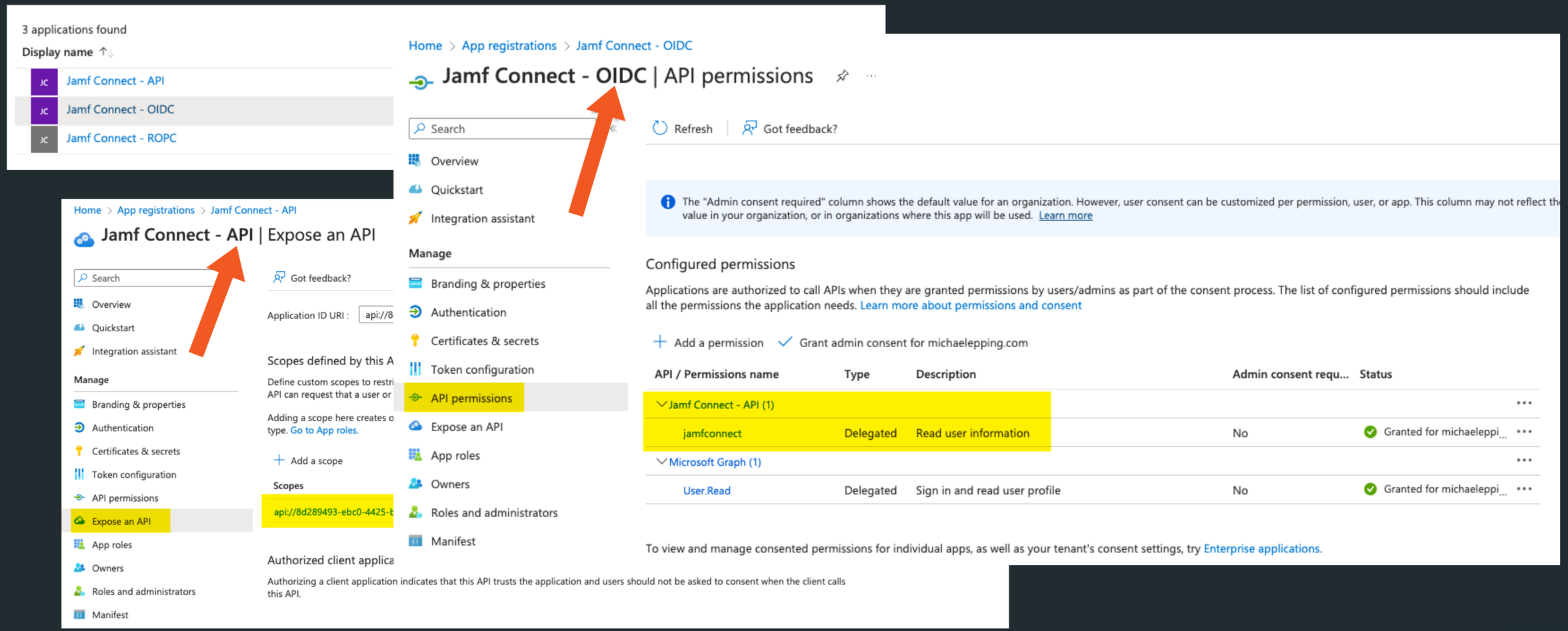
MS Graph API

Solution: Entra ID App Config





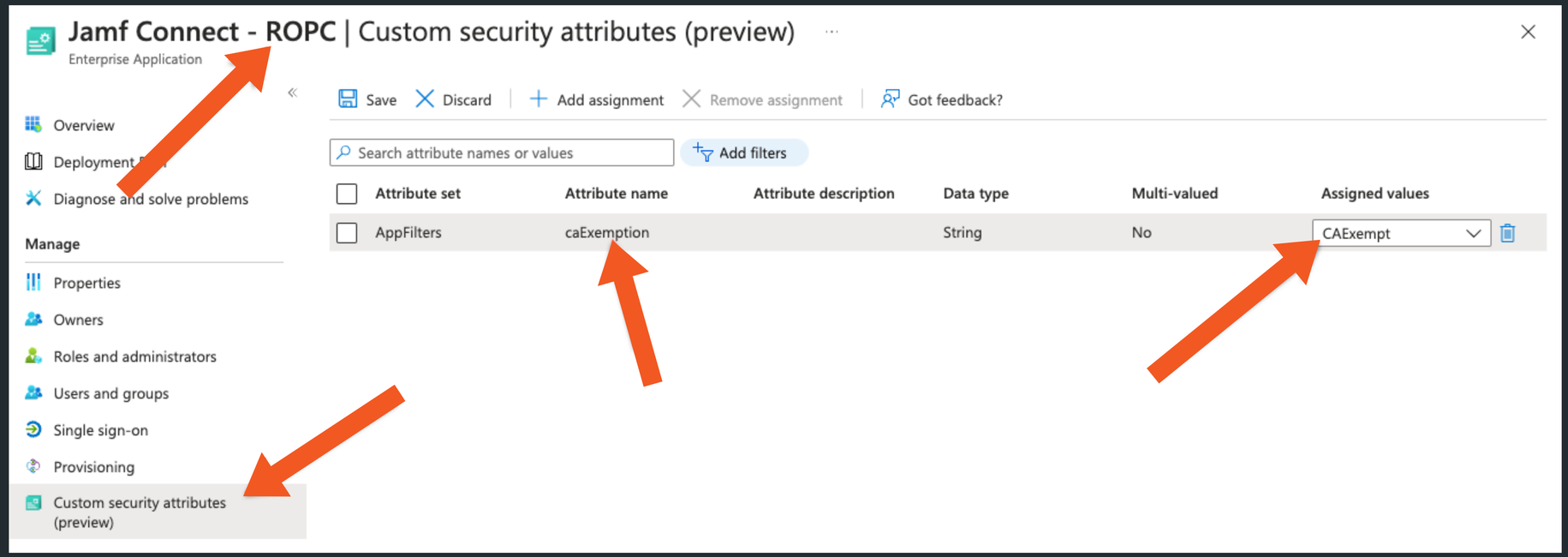
Solution: Entra ID App Config



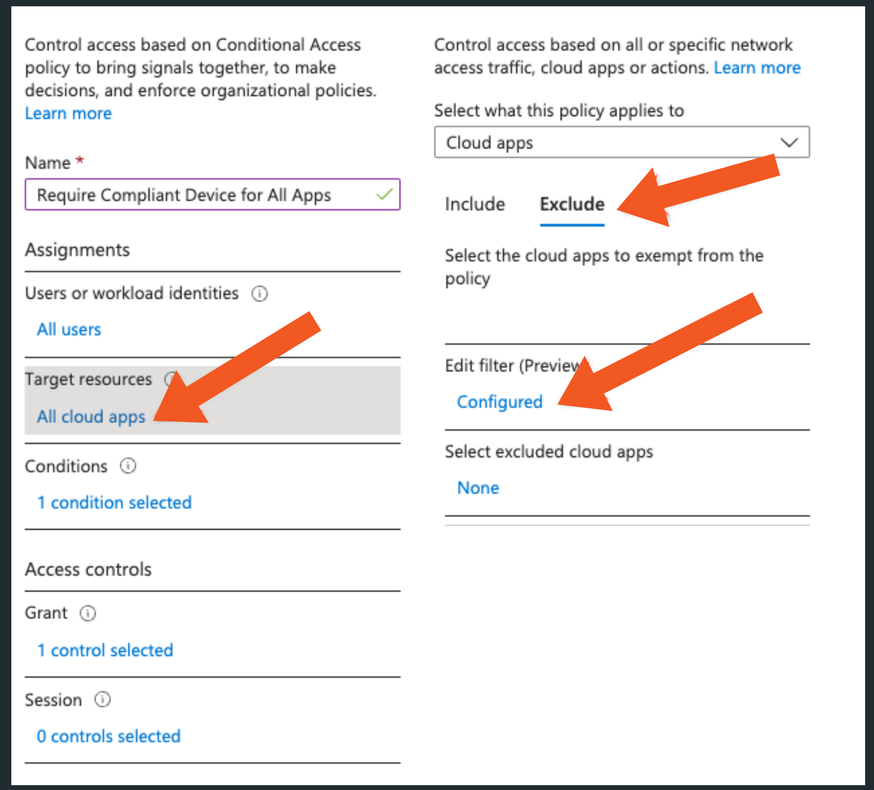
Solution: Entra ID App Tagging

aka.ms/JC_CSA

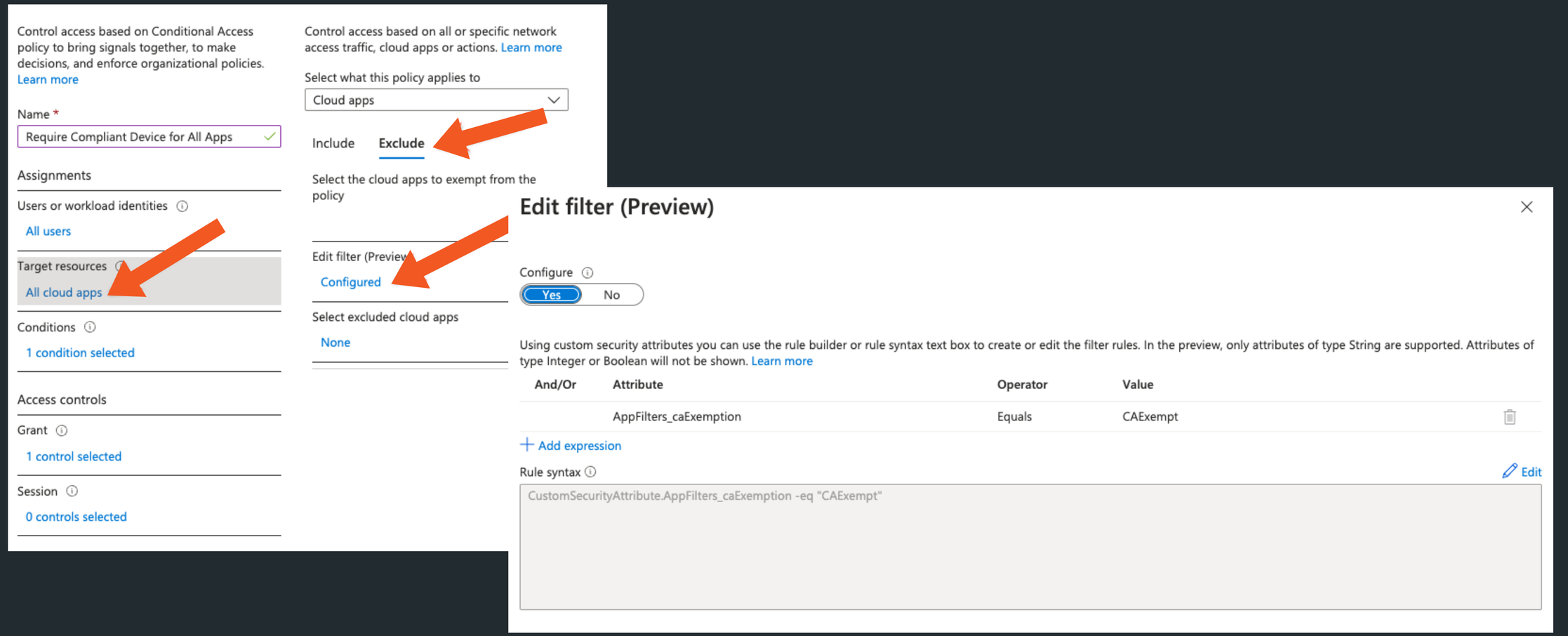
https://aka.ms/JC_CAFilters



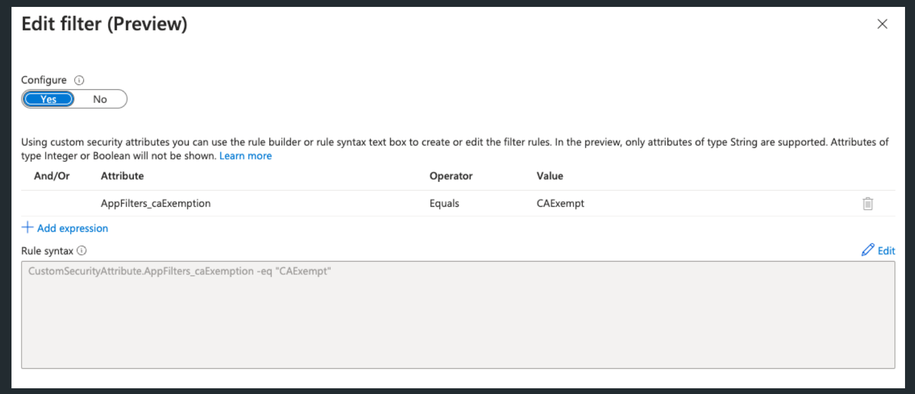
Solution: Entra ID App Tagging



Solution: Entra ID App Tagging



Solution: Entra ID App Tagging



Why are we doing this with tags?

- Normally, ROPG apps and other public clients cannot be explicitly included or excluded from Conditional Access policies
- Tags provide a workaround
- Use with caution!
  - For example, don’t try to exempt Microsoft Graph from All Apps policies, this is untested and unsupported

Agenda

Conditional Access Recap
Common Deployments & Issues
Jamf Pro & Conditional Access
Jamf Connect & Conditional Access
Go Do’s!

Go-Dos

- Understand your CA policies, make sure Apple users are IN SCOPE
- Remember, everyone should be doing device compliance
- Move to the new Jamf Pro Device Compliance flow
- Deploy the Enterprise SSO Extension everywhere you can
- Move to the new Jamf Connect Entra ID integration pattern
- Hit us up on Slack / social media

By the way…

- Platform SSO is almost ready for Public Preview
  - Intune supported right away
  - Jamf and other MDMs coming soon
- Check out the blog post here
- If you haven't *already* done the following, you should start *now*:
  - Make sure users are registered for an Entra ID MFA method, preferably Microsoft Authenticator
- Get upgraded to at least Ventura, Sonoma if possible

aka.ms/PSSO4MAC

Thank you for listening!