



# Jamf and Microsoft Entra ID Conditional Access



© copyright 2002–2023 Jamf





# 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?



- Formerly known as Azure Active Directory
- Part of Microsoft Entra



# What is Microsoft Entra ID?



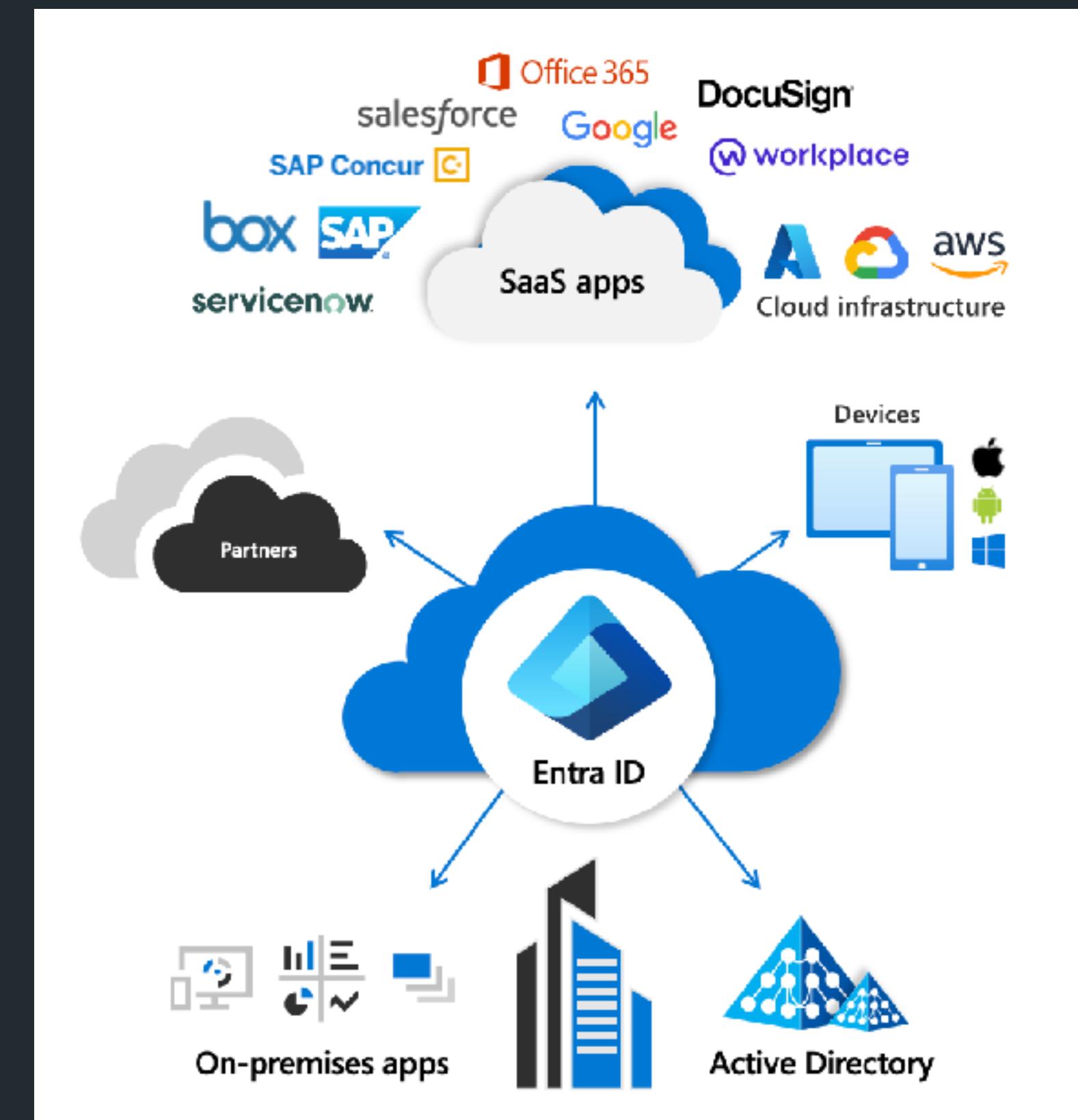
- Formerly known as Azure Active Directory
- Part of Microsoft Entra
- Full blown IDaaS



# What is Microsoft Entra ID?

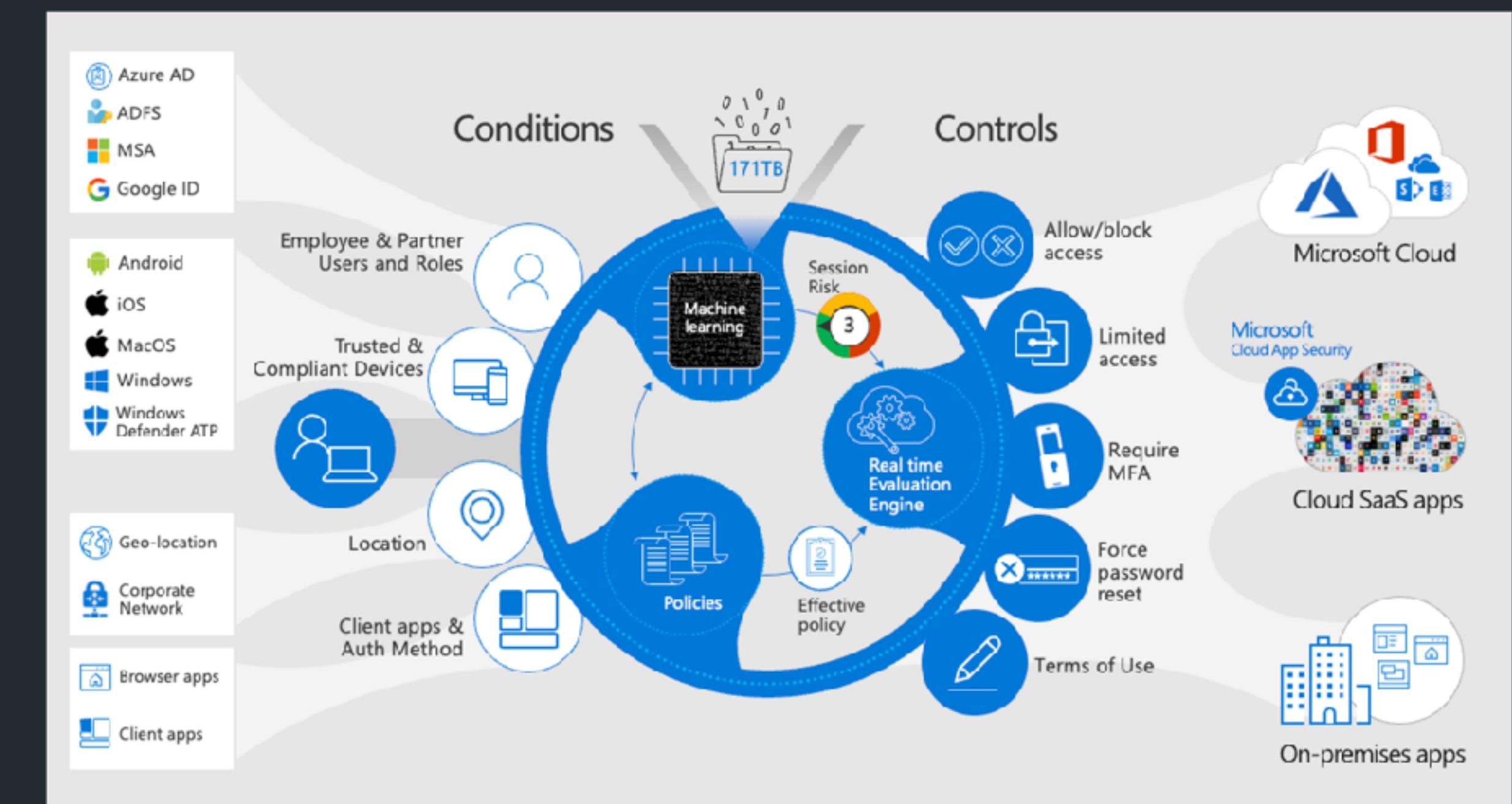


- Formerly known as Azure Active Directory
- Part of Microsoft Entra
- Full blown IDaaS
- Rich set of features
  - SSO, Provisioning
  - Governance, Passwordless
  - Conditional Access



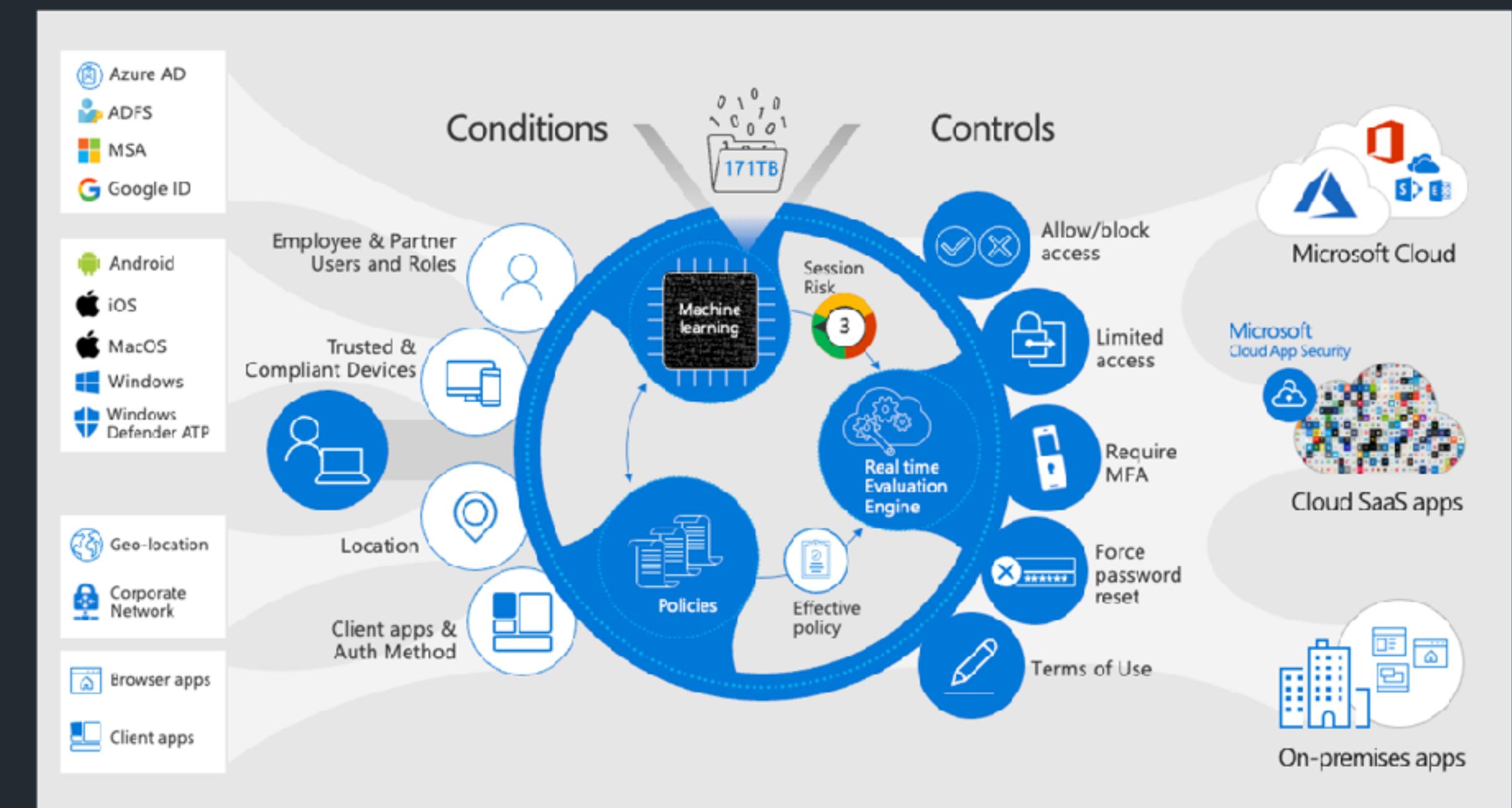
# Conditional Access Reminder

- Zero-trust engine



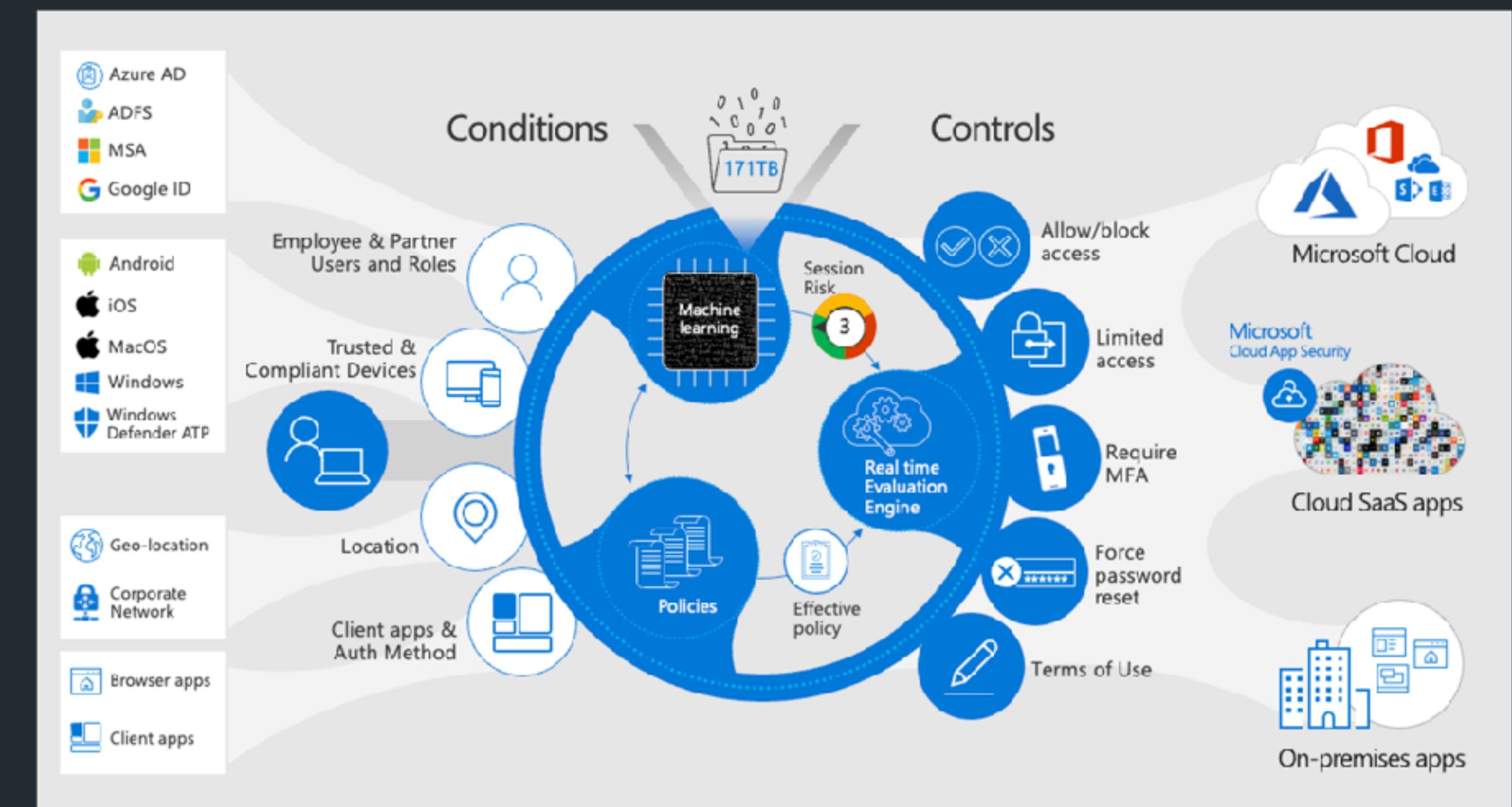
# Conditional Access Reminder

- Zero-trust engine
- CA understands user's activity
  - User Location
  - User Risk
  - App Requirements
  - State of Device (Critical!)



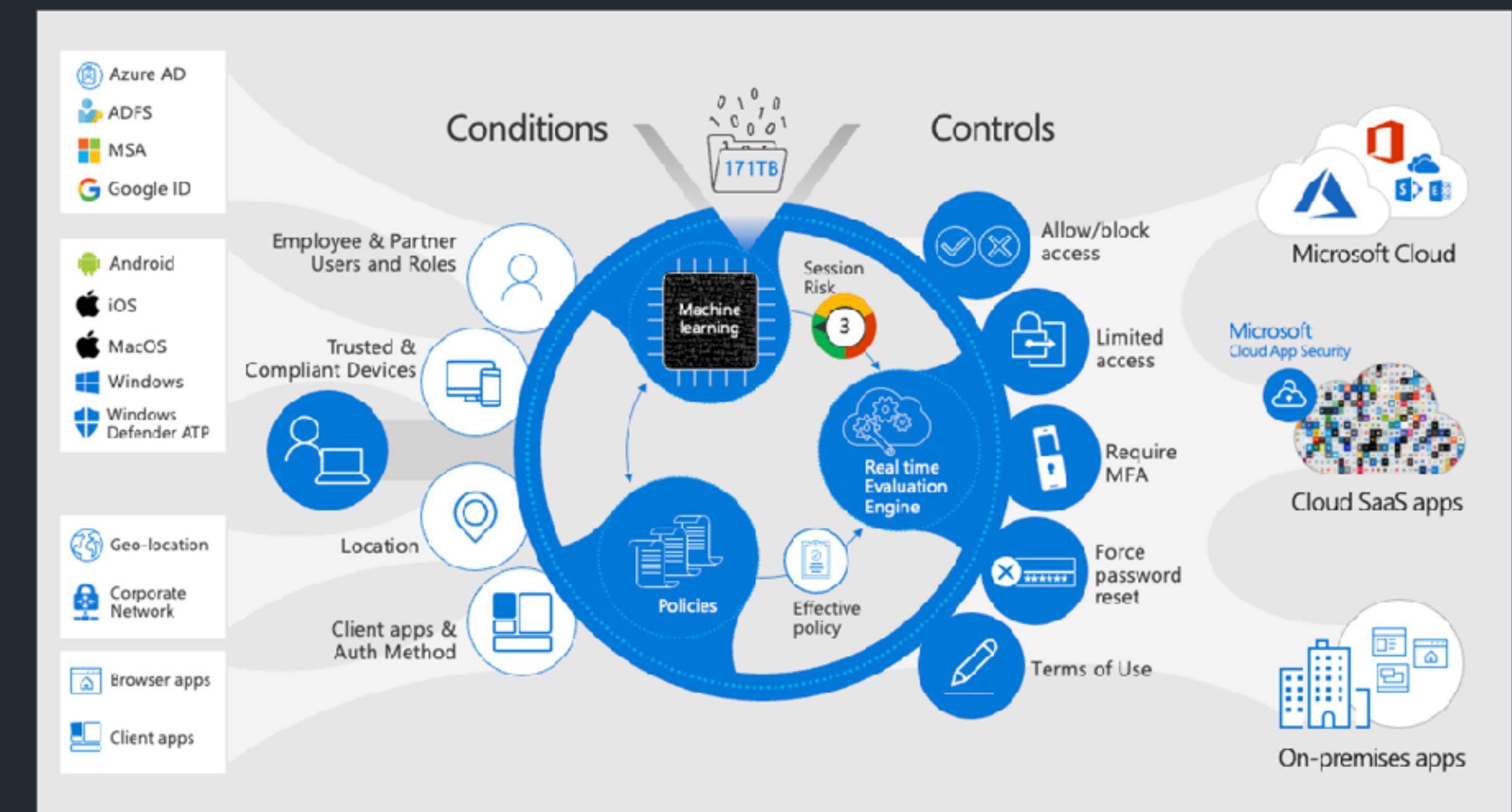
# Conditional Access Reminder

- Zero-trust engine
- CA understands user's activity
  - User Location
  - User Risk
  - App Requirements
  - State of Device (Critical!)
- Applies to “Cloud Apps”



# 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



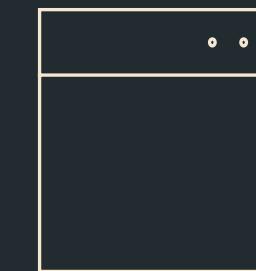
### **Web services**

APIs



# What are cloud apps?

## Cloud Apps **ARE**



### Web sites

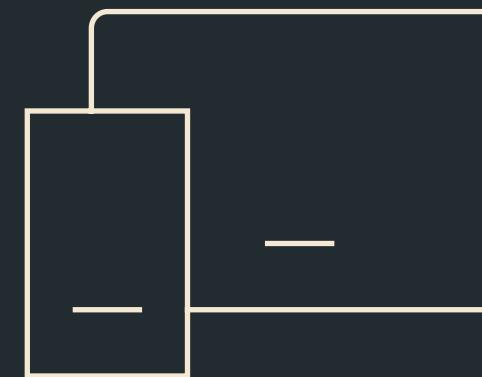
OpenID Connect / OAuth 2.0  
confidential clients  
SAML



### Web services

APIs

## Cloud Apps **ARE NOT**



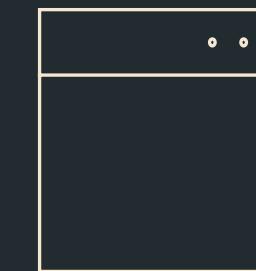
### Mobile or desktop apps

OpenID Connect / OAuth 2.0 native clients



# 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



# Conditional Access Evaluation Phases

- All CA policies are ANDed together
- Is Policy in scope of the request



# Conditional Access Evaluation Phases

- All CA policies are ANDed together
- Is Policy in scope of the request
- Block controls satisfied first



# 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



# 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  
    }  
  }  
}
```





© copyright 2002-2023 Jamf



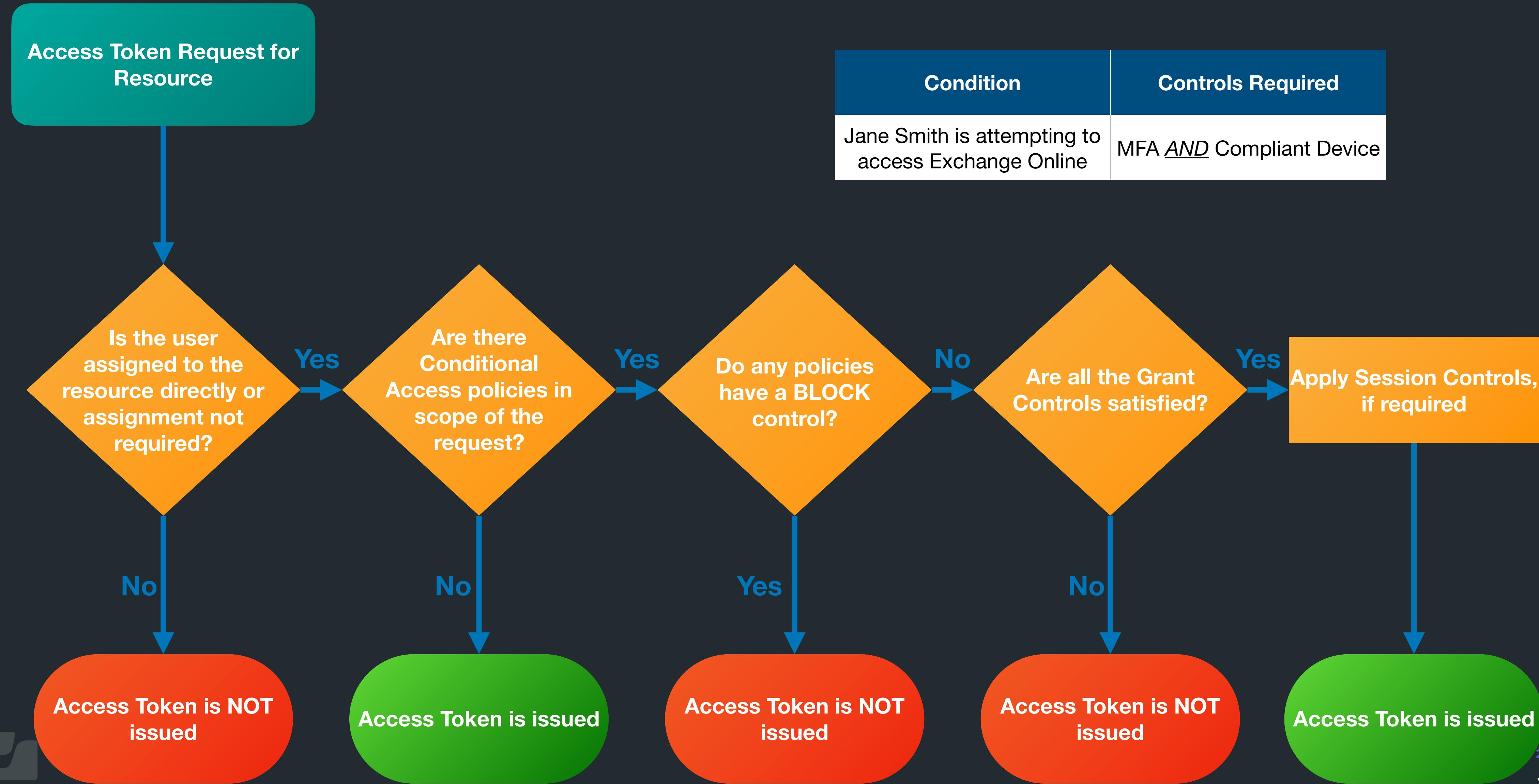
Policy Number	When <i>this</i> happens	Then do <i>this</i>
1	An access attempt is made: <ul style="list-style-type: none"><li>- To Exchange Online</li><li>- By Jane Smith</li></ul>	Grant access with: <ul style="list-style-type: none"><li>- MFA</li></ul>
2	An access attempt is made: <ul style="list-style-type: none"><li>- To Exchange Online</li><li>- By Jane Smith</li></ul>	Grant Access with: <ul style="list-style-type: none"><li>- Compliant Device</li></ul>



Policy Number	When <i>this</i> happens	Then do <i>this</i>
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 <u>AND</u> Compliant Device

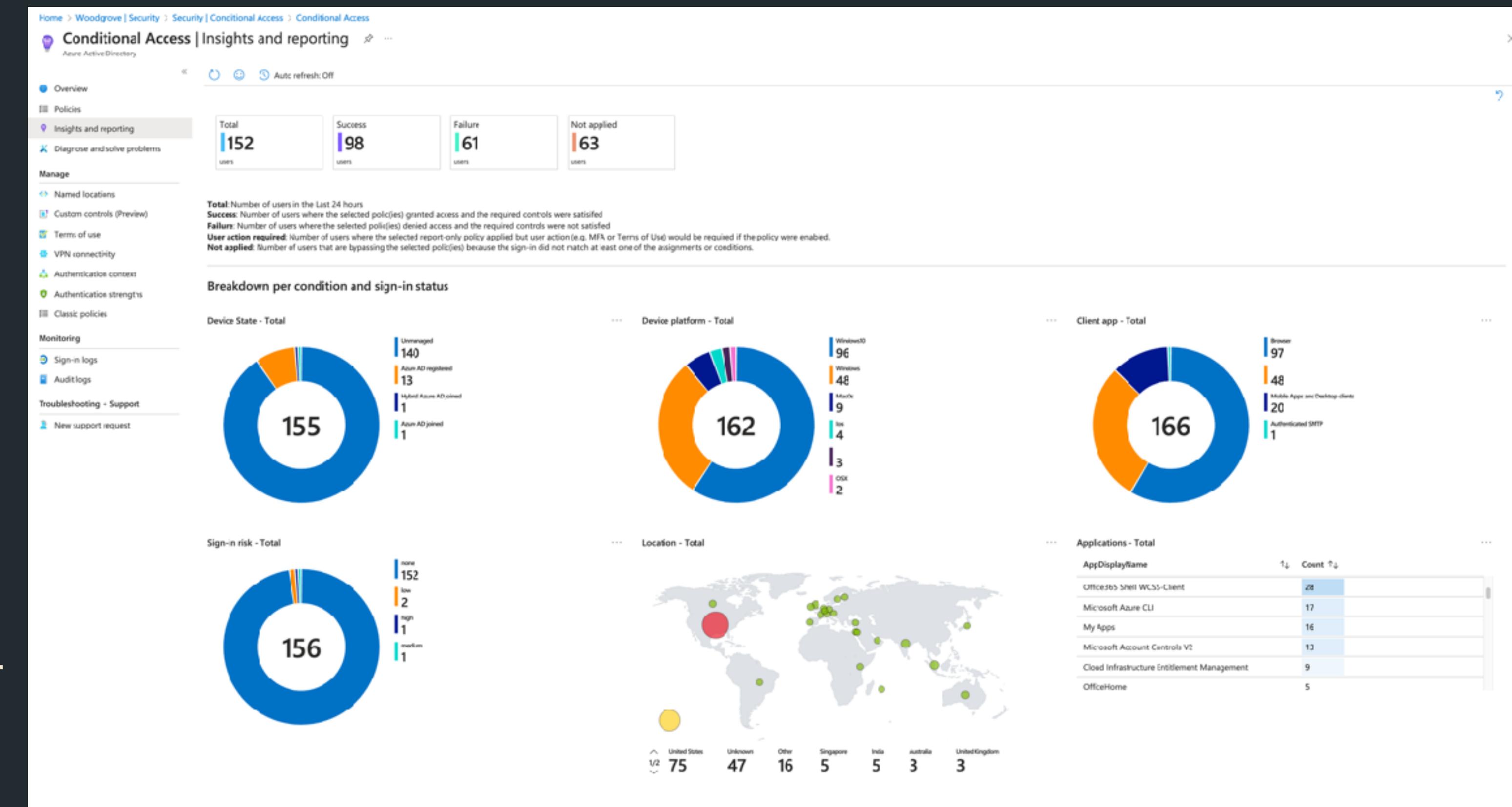




# Conditional Access Insights and Reporting

Understand the impact of CA Policies over time in your org

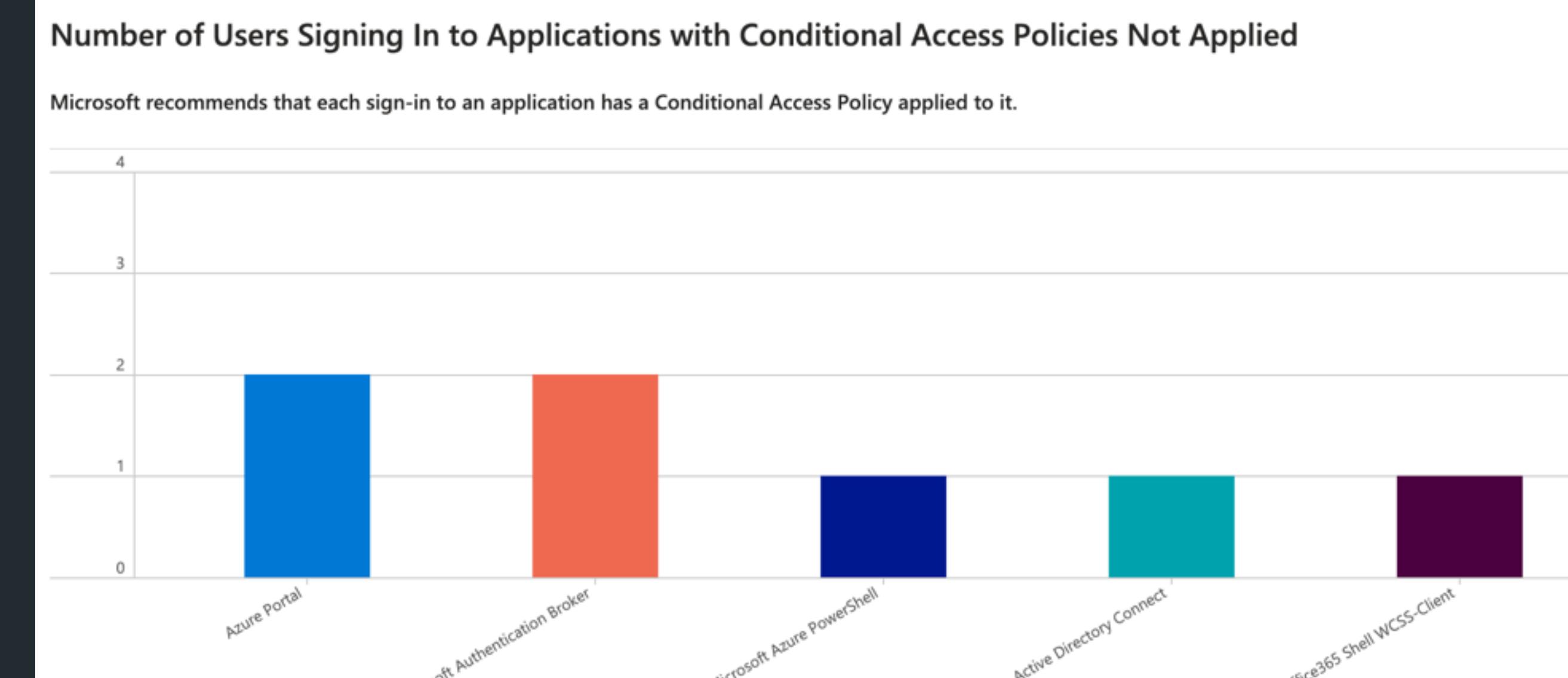
[aka.ms/CAInsights](https://aka.ms/CAInsights)



# 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](https://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, phishing-resistant credentials)



# Common CA Policies

- Requiring strong authentication (MFA, phish-resistant credentials)
- Blocking legacy auth



# Common CA Policies

- Requiring strong authentication (MFA, phish-resistant credentials)
- Blocking legacy auth
- Blocking access by country location



# Common CA Policies

- Requiring strong authentication (MFA, phishing-resistant credentials)
- Blocking legacy auth
- Blocking access by country location
- Require compliant or hybrid join device

**Filter for devices**

Configure a filter to apply policy to specific devices. [Learn more](#)

Configure [?](#) Yes No

Devices matching the rule:

Include filtered devices in policy  
 Exclude filtered devices from policy

You can use the rule builder or rule syntax text box to create or edit the filter rule.

And/Or	Property	Operator	Value
	isCompliant	Equals	True

+ Add expression

Rule syntax [?](#)

```
device.isCompliant -eq True
```



# Common CA Policies

- Requiring strong authentication (MFA, phishing-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

**Filter for devices**

Configure a filter to apply policy to specific devices. [Learn more](#)

Configure [?](#)

Yes  No

Devices matching the rule:  
 Include filtered devices in policy  
 Exclude filtered devices from policy

You can use the rule builder or rule syntax text box to create or edit the filter rule.

And/Or	Property	Operator	Value
	isCompliant	Equals	True

+ Add expression

Rule syntax [?](#)

```
device.isCompliant -eq True
```

**Session**

Control access based on session controls to enable limited experiences within specific cloud applications. [Learn more](#)

Use app enforced restrictions [?](#)

This control only works with supported apps. Currently, Office 365, Exchange Online, and SharePoint Online are the only cloud apps that support app enforced restrictions. Click here to learn more.

Use Conditional Access App Control [?](#)

Sign-in frequency [?](#)

Periodic reauthentication

2

Hours



# Common CA Policies

- Requiring strong authentication (MFA, phishing-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 policies to “All Apps”

**Filter for devices**

Configure a filter to apply policy to specific devices. [Learn more](#)

Configure [?](#)

Yes  No

Devices matching the rule:  
 Include filtered devices in policy  
 Exclude filtered devices from policy

You can use the rule builder or rule syntax text box to create or edit the filter rule.

And/Or	Property	Operator	Value
	isCompliant	Equals	True

+ Add expression

Rule syntax [?](#)

```
device.isCompliant -eq True
```

**Session**

Control access based on session controls to enable limited experiences within specific cloud applications. [Learn more](#)

Use app enforced restrictions [?](#)

This control only works with supported apps. Currently, Office 365, Exchange Online, and SharePoint Online are the only cloud apps that support app enforced restrictions. Click here to learn more.

Sign-in frequency [?](#)

Periodic reauthentication

2

Hours



# Common Issues



# Common Issues

- Confusion Around CA Policy Applying



# Common Issues

- Confusion Around CA Policy Applying
- Frequent Authentication Prompts



# Common Issues

- Confusion Around CA Policy Applying
- Frequent Authentication Prompts
- Compliant Device Check Fail



# Common Issues

- Confusion Around CA Policy Applying
- Frequent Authentication Prompts
- Compliant Device Check Fail
- Device Registration Failures



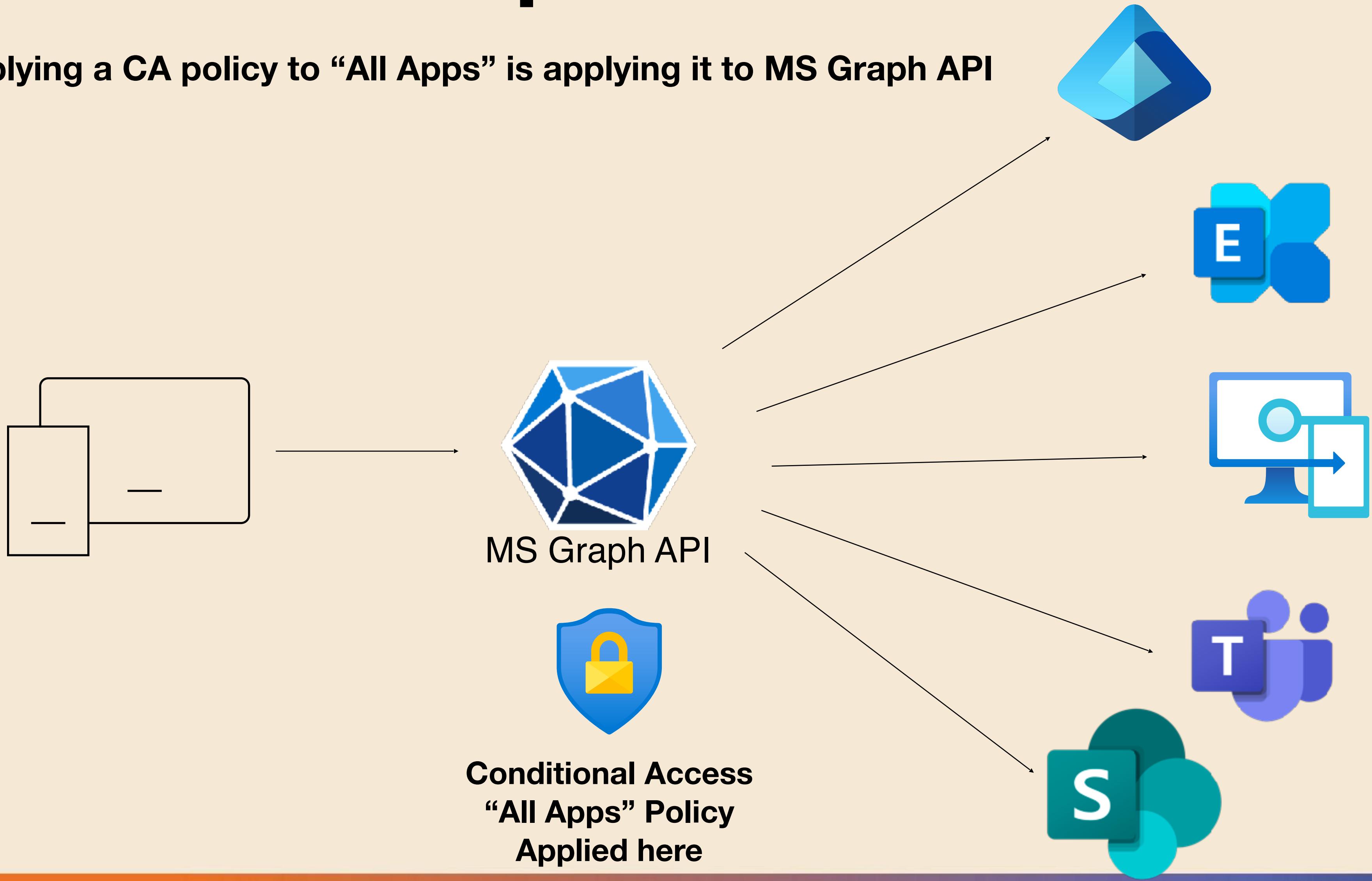
# Common Issues

- Confusion Around CA Policy Applying
- Frequent Authentication Prompts
- Compliant Device Check Fail
- Device Registration Failures
- Jamf Connect and Conditional Access w/ MFA



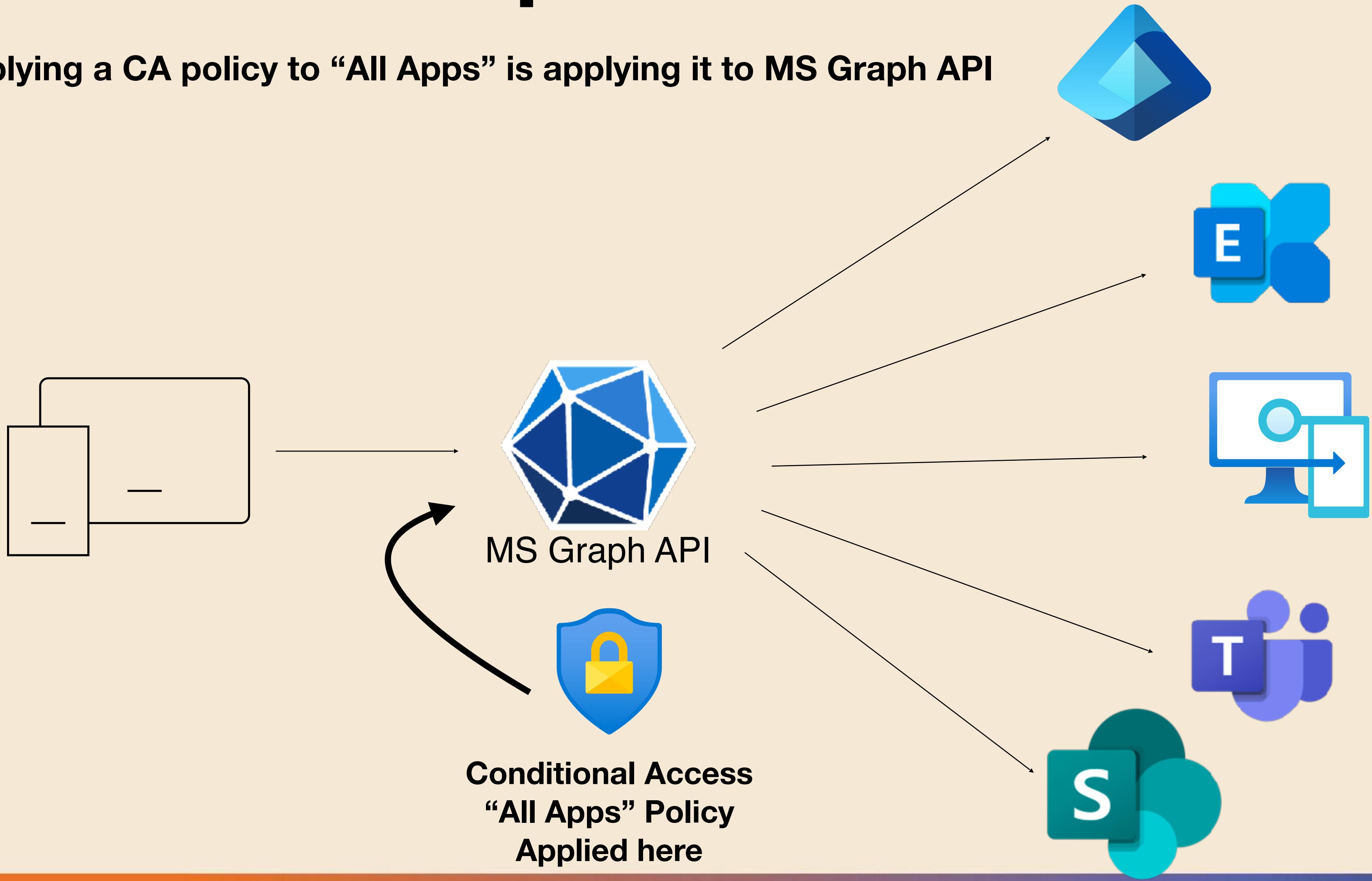
# Microsoft Graph API

- Applying a CA policy to “All Apps” is applying it to MS Graph API



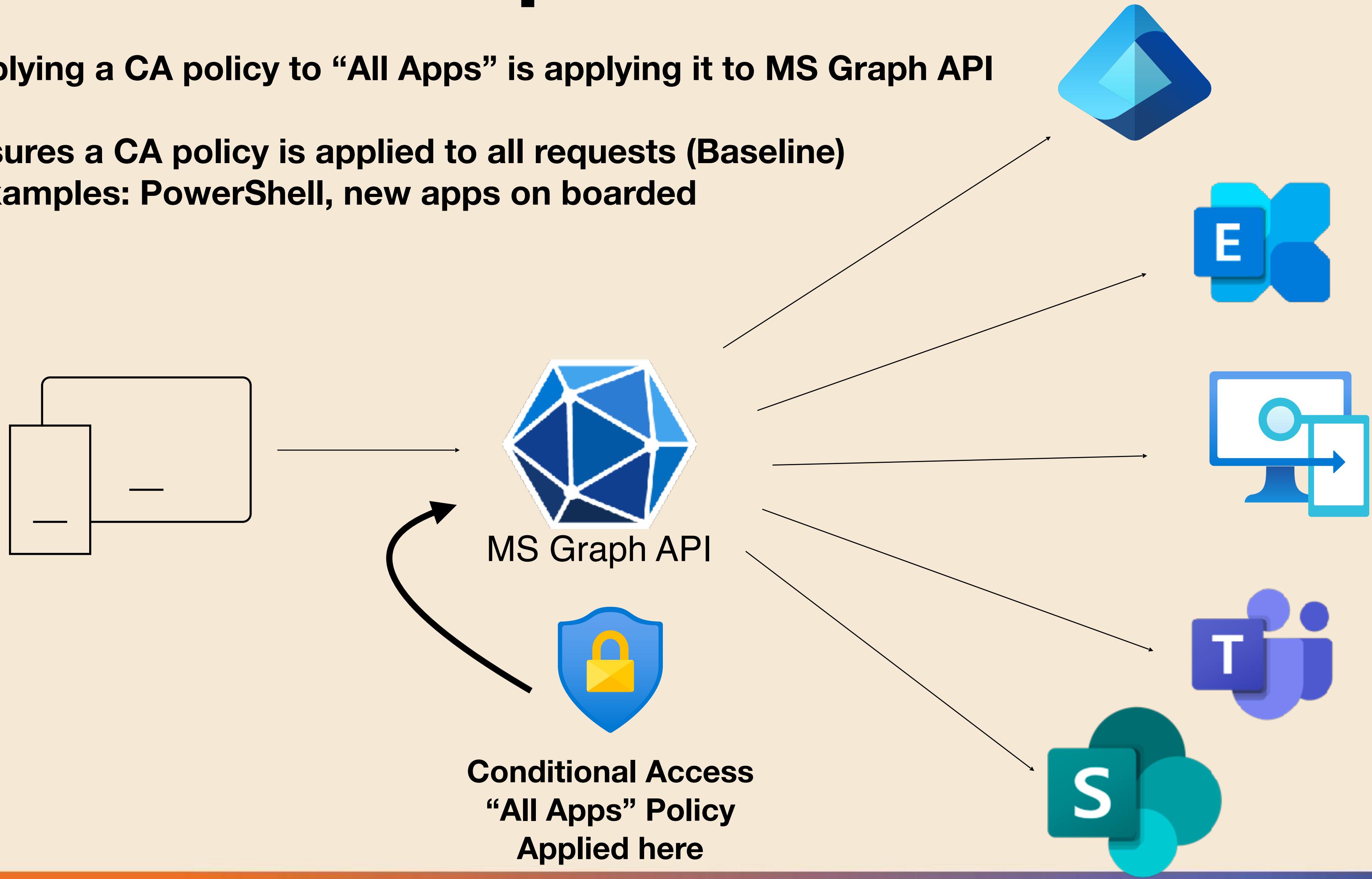
# Microsoft Graph API

- Applying a CA policy to “All Apps” is applying it to MS Graph API



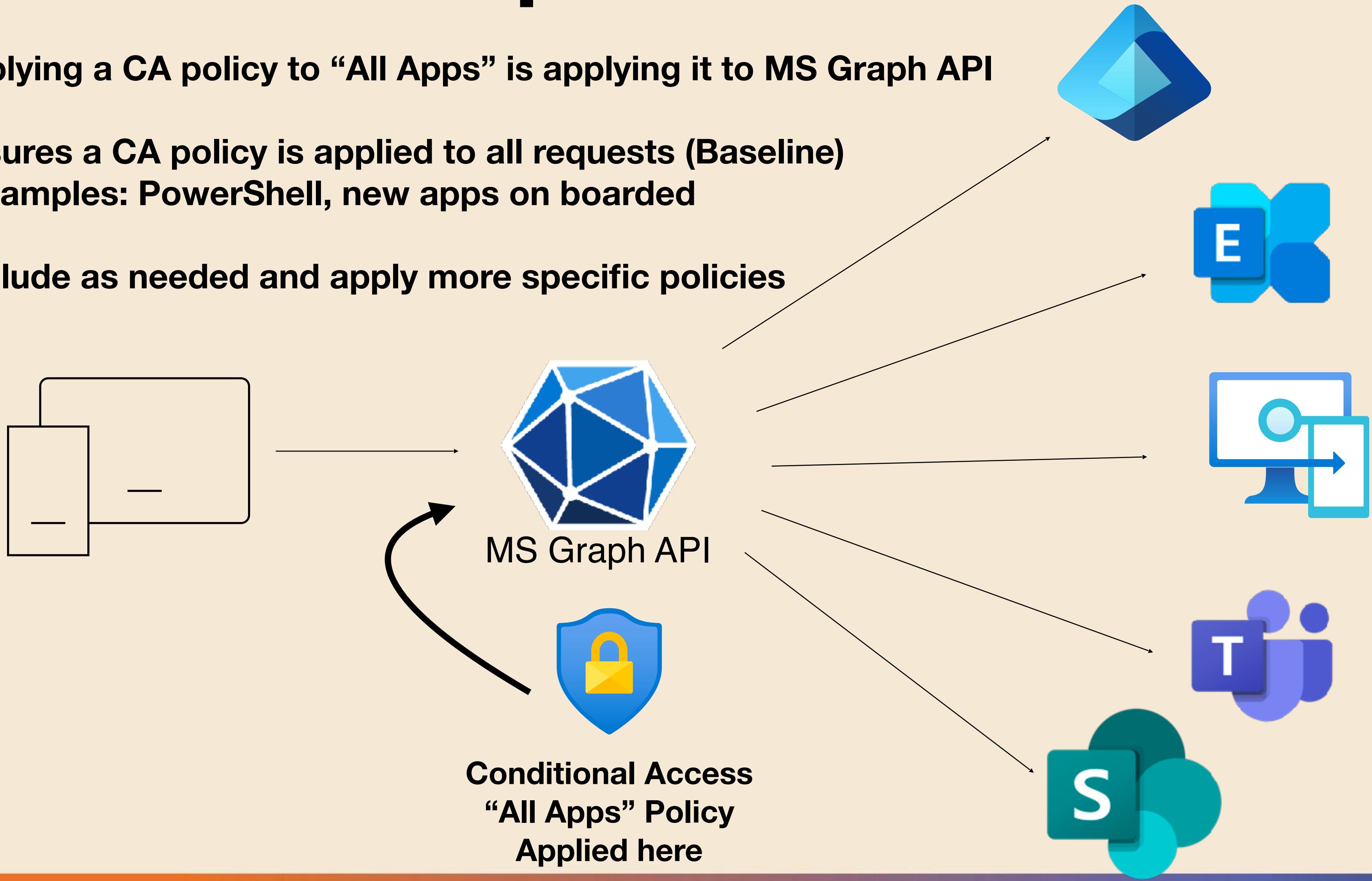
# Microsoft Graph API

- 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



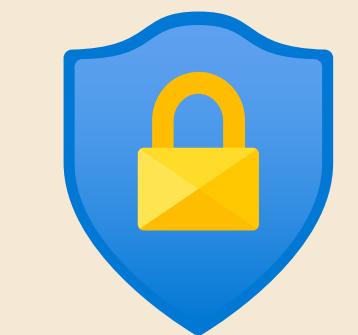
# Microsoft Graph API

- 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



Conditional Access  
“All Apps” Policy  
Applied here

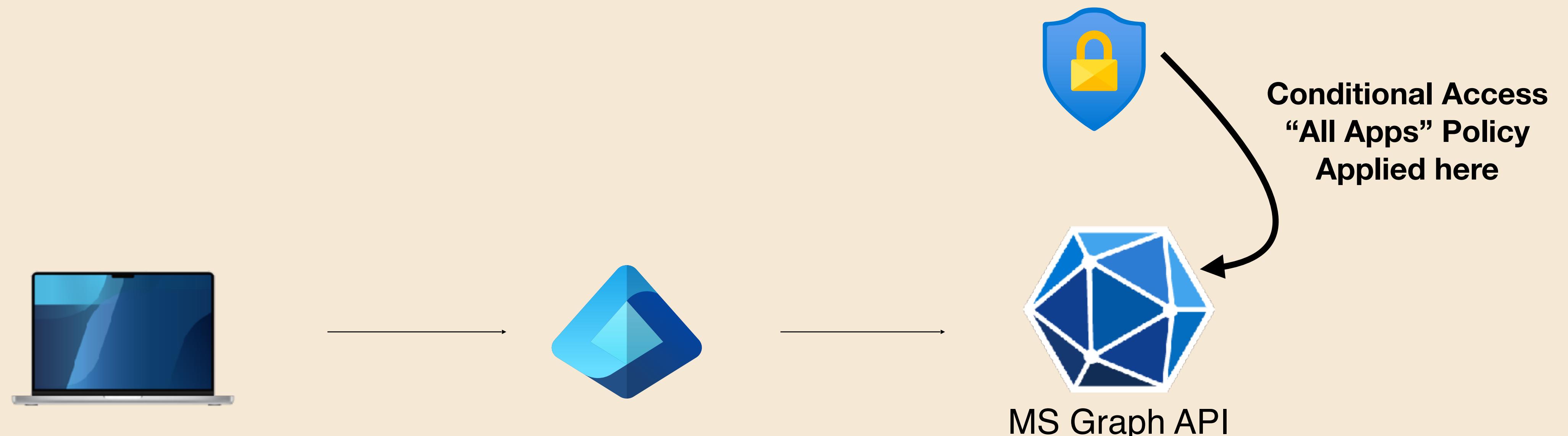


MS Graph API



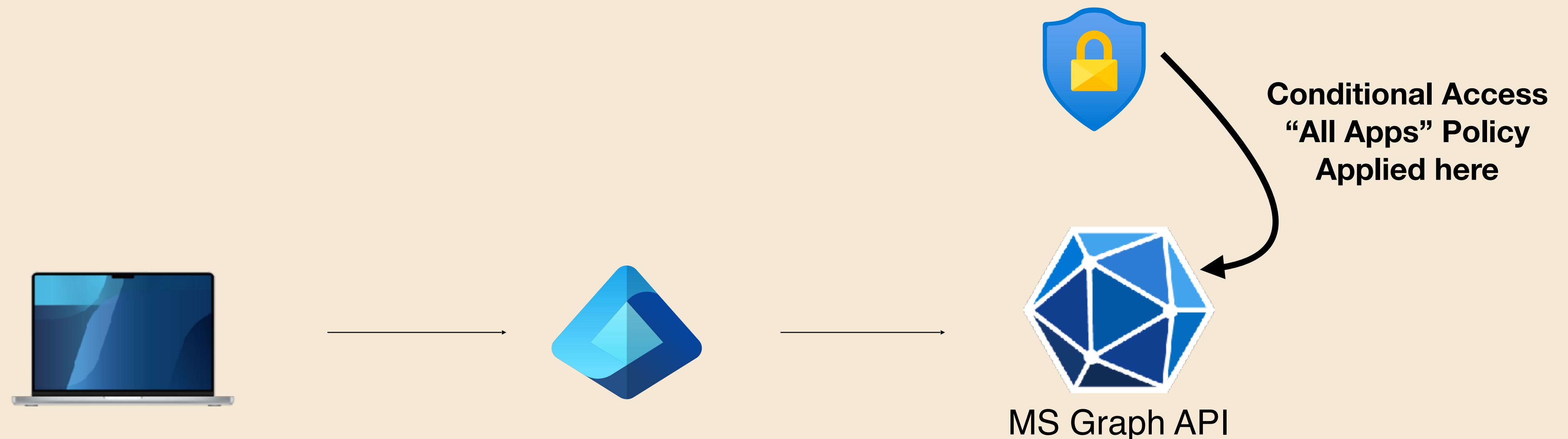
# All Apps Policy Challenges

- CA policy to “All Apps” Require MFA



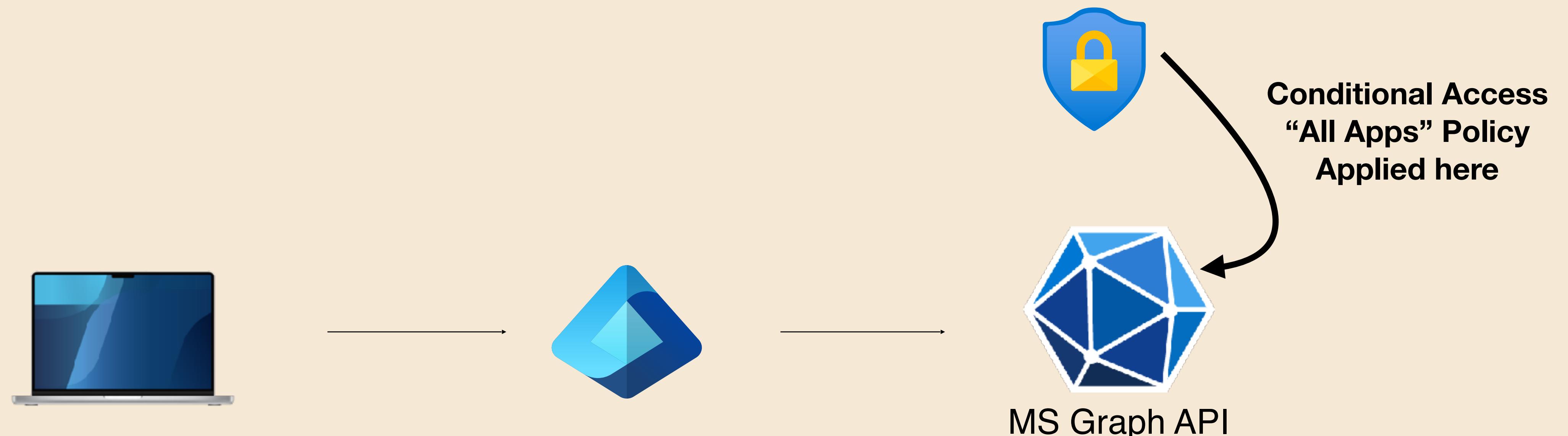
# All Apps Policy Challenges

- CA policy to “All Apps” Require MFA
- You have an ROPG/ROPC OAuth flow (no web UI)



# 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



# 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



MS Graph API



Conditional Access  
“All Apps” Policy  
Applied here



# 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



MS Graph API



Conditional Access  
“All Apps” Policy  
Applied here



# Agenda

Conditional Access Recap

Common Deployments & Issues

**Jamf Pro & Conditional Access**

Jamf Connect & Conditional Access

Go Do's!



# Device Compliance



macOS



iOS  
iPadOS



**Microsoft Entra ID**  
**(formerly Azure AD)**



# Device Compliance



macOS



iOS  
iPadOS



Rules



**Microsoft Entra ID**  
**(formerly Azure AD)**



# Device Compliance



macOS



iOS  
iPadOS



## Rules

OS Updated

Password Policy

Full Disk Encryption



**Microsoft Entra ID**  
**(formerly Azure AD)**



# Device Compliance



macOS



iOS  
iPadOS



## Rules



OS Updated



Password Policy



Full Disk Encryption



**Microsoft Entra ID**  
**(formerly Azure AD)**



# Device Compliance



macOS



iOS  
iPadOS



## Rules



CIS/NIST Compliant



Obtained Entra Device ID



Apps Updated



**Microsoft Entra ID**  
**(formerly Azure AD)**



# Device Compliance



macOS



iOS  
iPadOS



**Microsoft Entra ID**  
**(formerly Azure AD)**



# Device Compliance



**Microsoft Entra ID  
(formerly Azure AD)**

macOS



iOS  
iPadOS



# Device Compliance



**Microsoft Entra ID  
(formerly Azure AD)**

macOS



iOS  
iPadOS



Compliant



# Microsoft Conditional Access

jamf | PRO



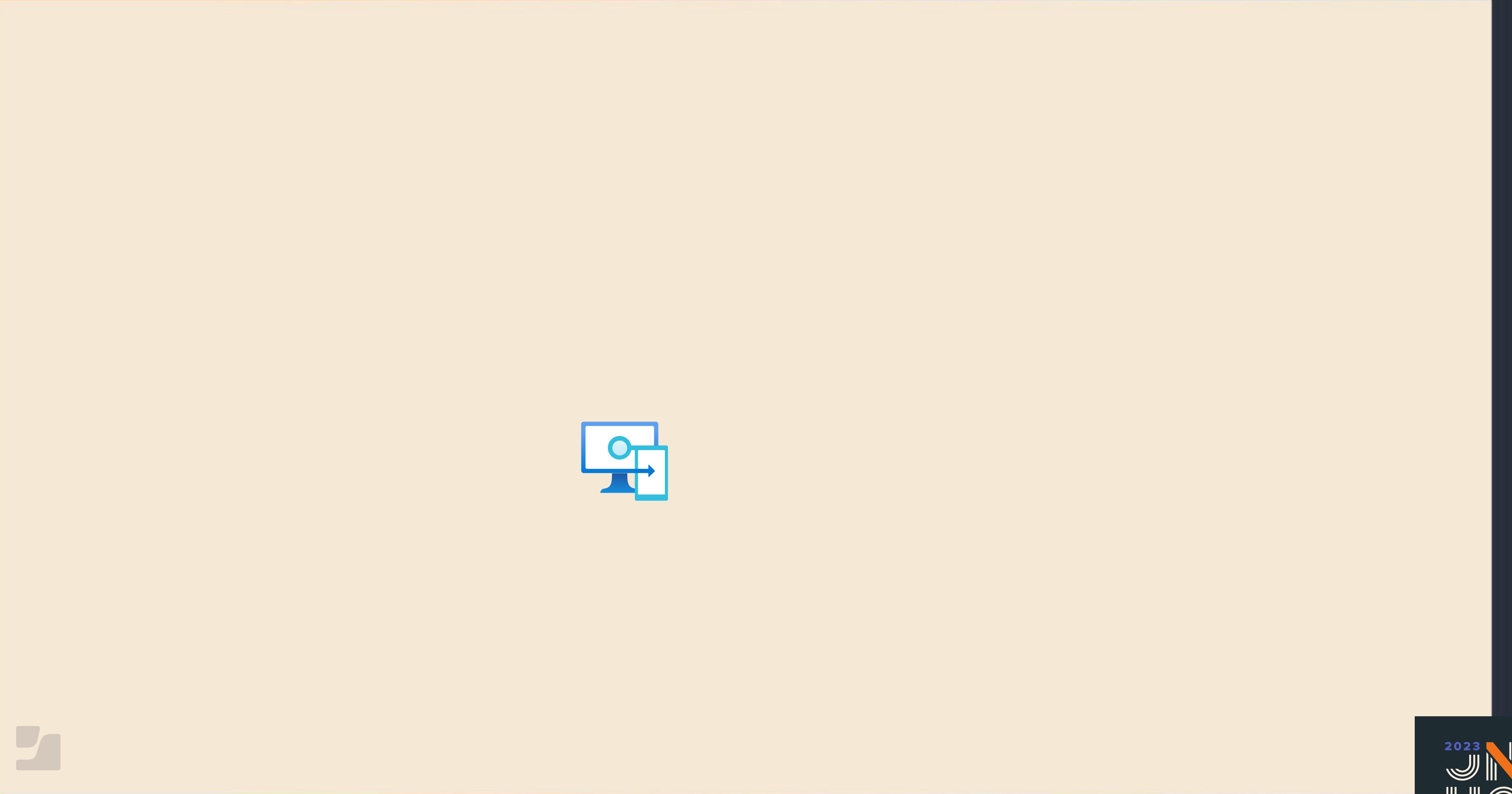
**Microsoft Entra ID  
(formerly Azure AD)**

macOS



iOS  
iPadOS





© copyright 2002-2023 Jamf

2023  
**JAMF**  
UNIVERSE

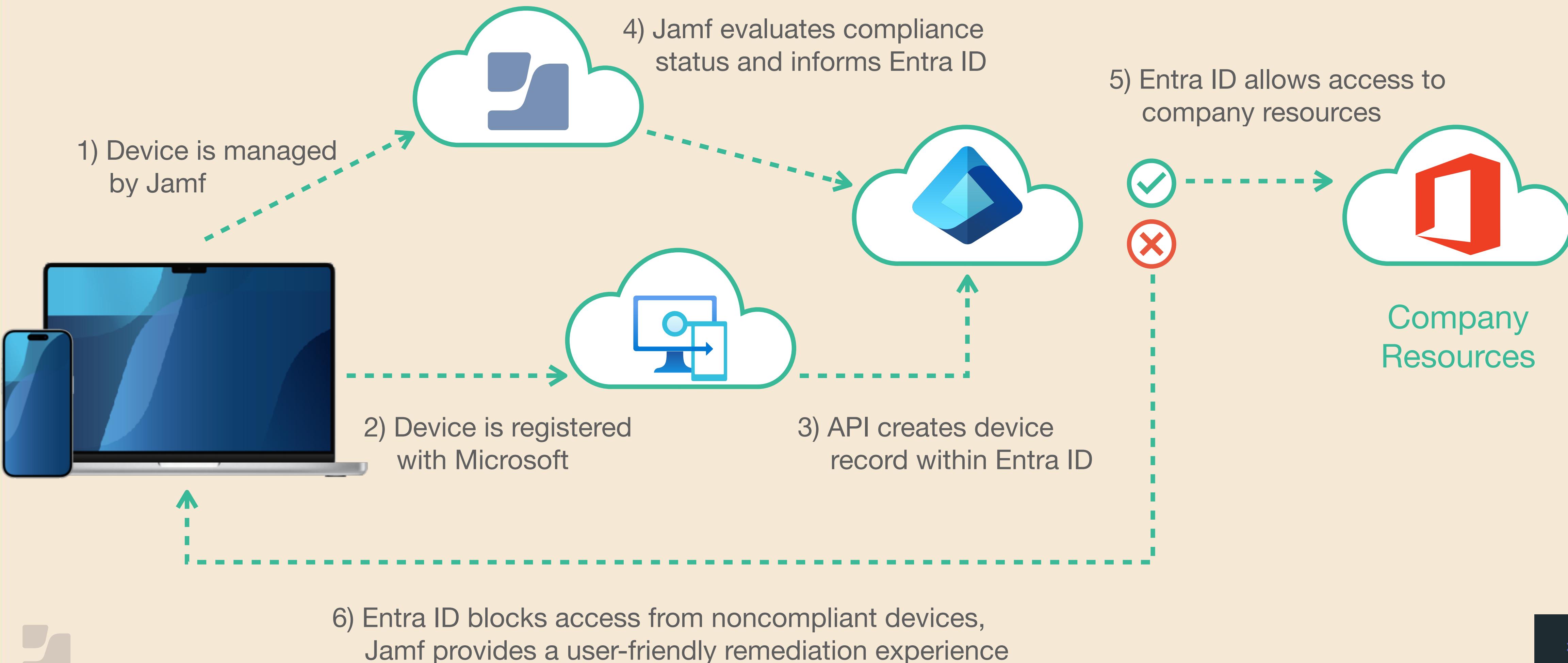
# Device Compliance

with Jamf and Microsoft



# 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](https://learn.jamf.com/search/device-compliance)  
Search: Device Compliance



# Jamf Pro Setup

Mobile Devices : Smart Device Groups

← Microsoft Conditional Access - Registration Eligible

Mobile Device Group Criteria Automated Management Reports

**Display Name** Display name for the smart mobile device group  
Microsoft Conditional Access - Registration Eligible

Send email notification on membership change  
When group members work

**Site** Site to add the smart mobile device group  
None

Mobile Devices : Smart Device Groups

← Microsoft Conditional Access - Registration Eligible

Mobile Device Group Criteria Automated Management Reports

AND/OR	CRITERIA	OPERATOR	VALUE	
	App Identifier	is	com.microsoft.azureauthenticat	<input type="button" value="Delete"/>
and	App Identifier	is	com.jamfsoftware.selfservice	<input type="button" value="Delete"/>
<input type="button" value="Add"/>				



# Jamf Pro Setup

Mobile Devices : Smart Device Groups

← Microsoft Conditional Access - Compliant

Mobile Device Group Criteria Automated Management Reports

**Display Name** Display name for the smart mobile device group

Microsoft Conditional Access - Compliant

Send email notifications When group membership changes

**Site** Site to add the smart mobile devices

None

Mobile Devices : Smart Device Groups

← Microsoft Conditional Access - Compliant

Mobile Device Group Criteria Automated Management Reports

AND/OR	CRITERIA	OPERATOR	VALUE	⋮	⋮	Delete
	Passcode Compliance	is	Compliant	⋮	⋮	Delete
and	App Name	does not have	Onion Browser	⋮	⋮	Delete
and	iOS Version	greater than or equal	16.6	⋮	⋮	Delete

+ Add

# Jamf Pro Setup

Computers : Smart Computer Groups

← Microsoft Conditional Access - Register

---

Computer Group      Criteria      Reports

---

Send email  
When group n

**Site** Site to add the

None

Computers : Smart Computer Groups

← Microsoft Conditional Access - Register

Computer Group Criteria Reports

AND/OR	CRITERIA	OPERATOR	VALUE		
	Application Title	is	Company Portal.app	...	<input type="button" value="Delete"/>
<input type="button" value="Add"/>					

# Jamf Pro Setup

Computers : Smart Computer Groups

← Microsoft Conditional Access - Compliant

Computer Group	Criteria	Reports				
AND/OR	CRITERIA	OPERATOR	VALUE	...	⋮	Delete
	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

CIS Benchmark - Level 1  
macOS 13.0

Sections

- All Sections
- Auditing
- macOS
- Password Policy
- System Settings
- Supplemental

Rules 85 Rules, 85 included, 85 found Sort - ID

- 3.5 Configure Audit Log Files to Not Contain Access Control List
- 3.5 Configure Audit Log Folder to Not Contain Access Control Li
- 3.1 Enable Security Auditing
- 3.5 Configure Audit\_Control to Not Contain Access Control Lists
- 3.5 Configure Audit\_Control Group to Wheel
- 3.5 Configure Audit\_Control Owner to Mode 440 or Less Permis
- 3.5 Configure Audit\_Control Owner to Root
- 3.5 Configure Audit Log Files Group to Wheel
- 3.5 Configure Audit Log Files to Mode 440 or Less Permissive
- 3.5 Configure Audit Log Files to be Owned by Root
- 3.5 Configure Audit Log Folders Group to Wheel
- 3.5 Configure Audit Log Folders to be Owned by Root
- 3.5 Configure Audit Log Folders to Mode 700 or Less Permissive
- 3.4 Configure Audit Retention to \$ODV
- 2.3.1.1 Disable AirDrop
- 5.1.4 Enable Authenticated Root
- 1.6 Enforce Installation of XProtect Remediator and Gatekeeper

+

Search

Rule Details

ID: os\_airdrop\_disable

Title: Show

Discussion: Show

Check: Show

Result: Show

Fix: Show

References: Show

Tags: Show

Mobileconfig:  Hide

com.apple.applicationaccess:  
allowAirDrop: false

CIS Benchmark - Level 1

Show All

Jamf Pro Upload Create Guidance



[trusted.jamf.com](https://trusted.jamf.com)

# Jamf Pro Setup

Computers : Configuration Profiles

← Microsoft Enterprise Single Sign-On Plug-in

Options Scope  Show in Jamf Pro Dashboard

Search... General

Application & Custom Settings 1 payload configured

Upload

Single Sign-On Extensions 1 payload configured

**Single Sign-on Extension**  
Configure app extensions that perform single sign-on (macOS 10.15 or later, User Approved MDM required).

**Payload Type** SSO  
The payload type

**Extension Identifier** com.microsoft.CompanyPortalMac.ssoextension

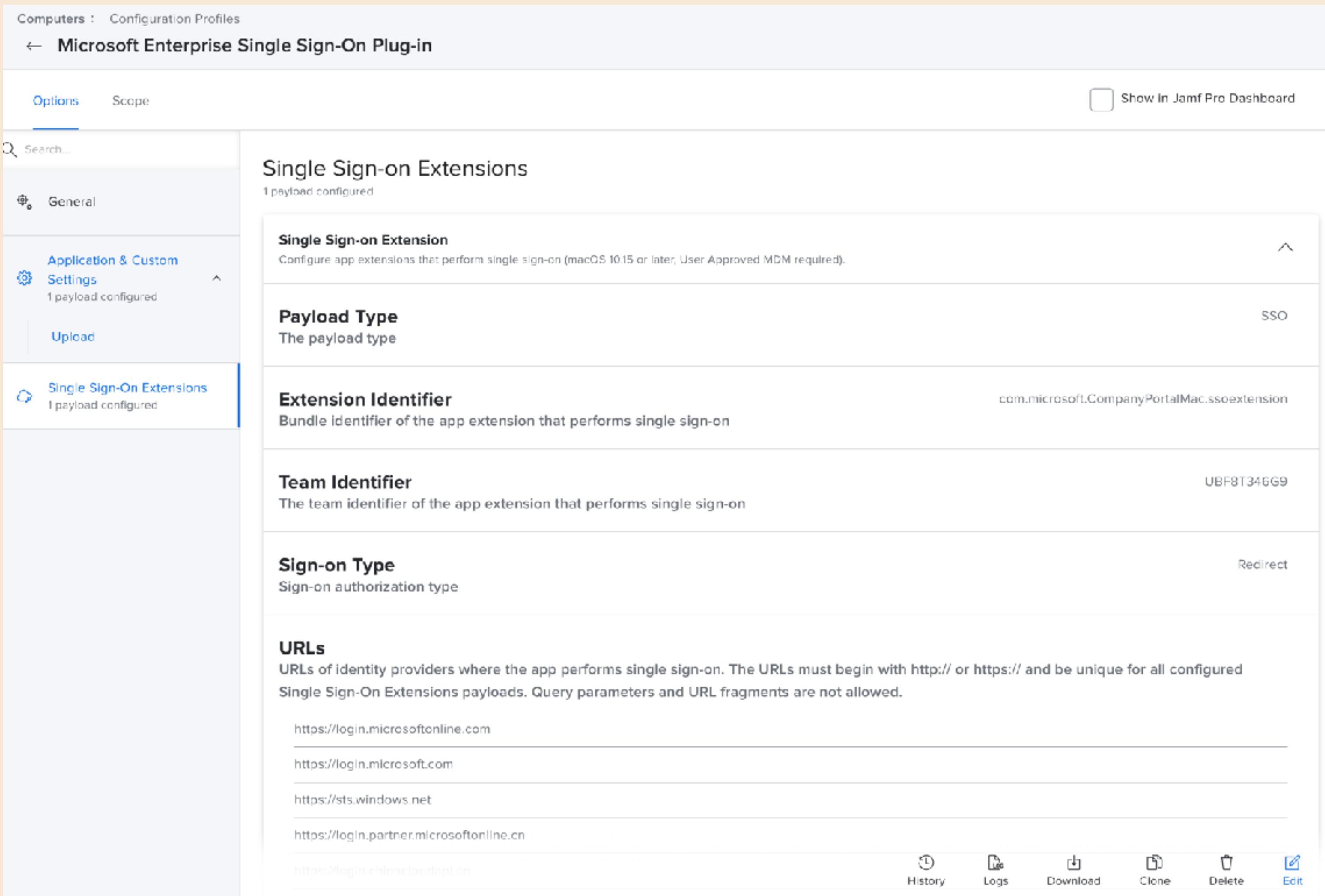
**Team Identifier** UBF8T346G9  
The team identifier of the app extension that performs single sign-on

**Sign-on Type** Redirect  
Sign-on authorization type

**URLs**  
URLs of identity providers where the app performs single sign-on. The URLs must begin with http:// or https:// and be unique for all configured Single Sign-On Extensions payloads. Query parameters and URL fragments are not allowed.

https://login.microsoftonline.com  
https://login.microsoft.com  
https://sts.windows.net  
https://login.partner.microsoftonline.cn  
https://login.chinacloudcdn.cn

History Logs Download Clone Delete Edit



[jamf.it/entraSSOe](https://jamf.it/entraSSOe)



<https://jamf.it/entrassoe-ios>

# Jamf Pro Setup

**Jamf Pro Settings ->  
Global ->  
Device Compliance**

Settings : Global  
[← Device Compliance](#)

**Configuration status**  
Use the switch to enable or disable the connection.

**Platform** Select platform type to configure.

macOS

**Compliance Group** Smart computer group Jamf Pro will use to calculate device compliance.  
Microsoft Conditional Access - Compliant

**Applicable Group** Smart group containing all computers Jamf Pro uses to send a compliance status to Microsoft Intune. This also makes the Register button available in Self Service.  
Microsoft Conditional Access - Register

iOS and iPadOS

**Compliance Group** Smart device group Jamf Pro will use to calculate device compliance.  
Microsoft Conditional Access - Compliant

**Applicable Group** Smart group containing all devices Jamf Pro uses to send a compliance status to Microsoft Intune. This also makes the Register button available in Self Service.  
Microsoft Conditional Access - Registration Eligible

**Allowed Duration Of Inactivity** Number of days after a device's last check in with Jamf Pro before the device is marked as "Unspecified" in Azure AD.  
120

Required

**Landing Page For Devices Not Recognized By Microsoft Azure** Webpage where users are redirected to if their device is not registered with Azure AD or not enrolled with Jamf Pro.

Default Jamf Pro Device Registration page

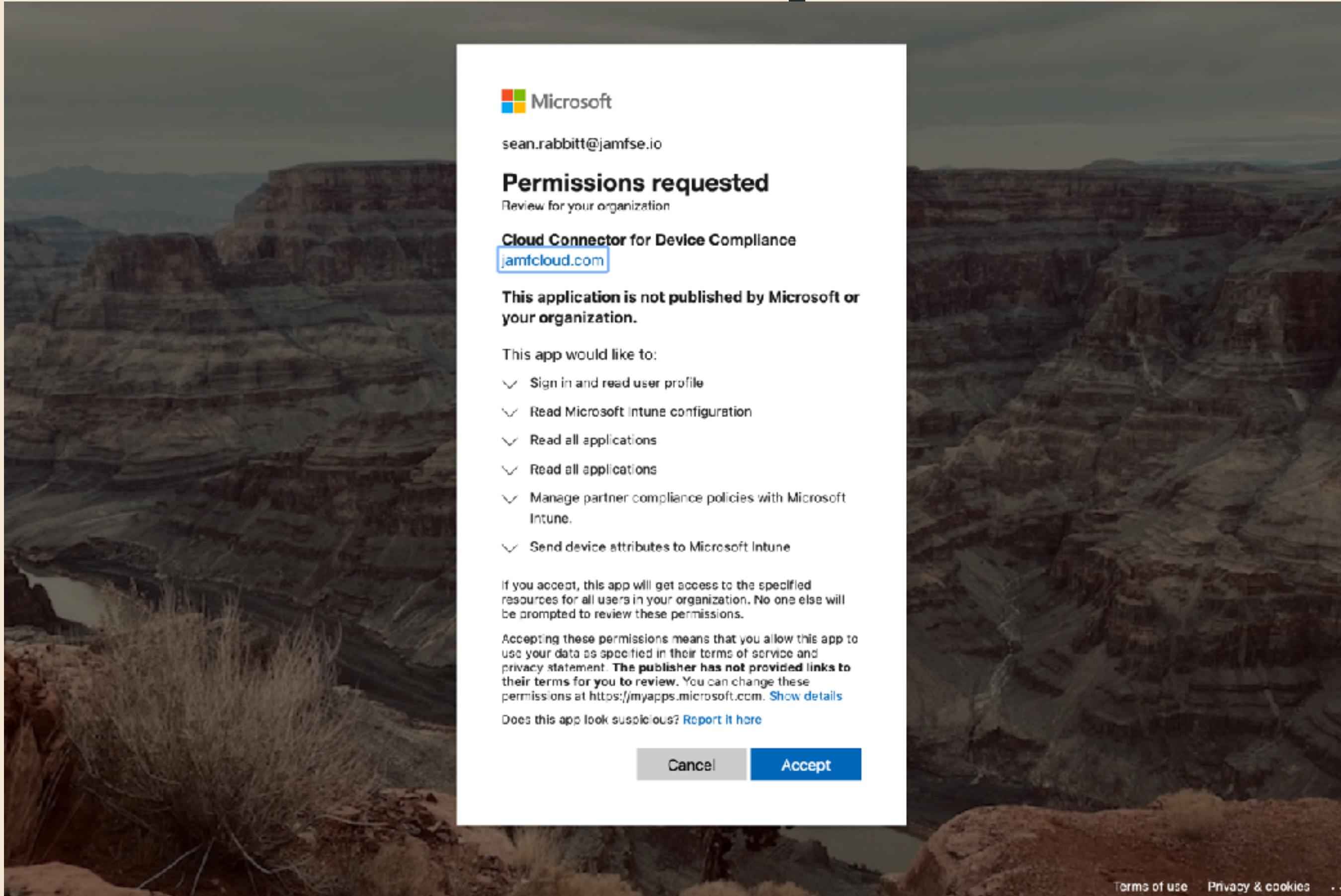
Access Denied page

Custom URL:

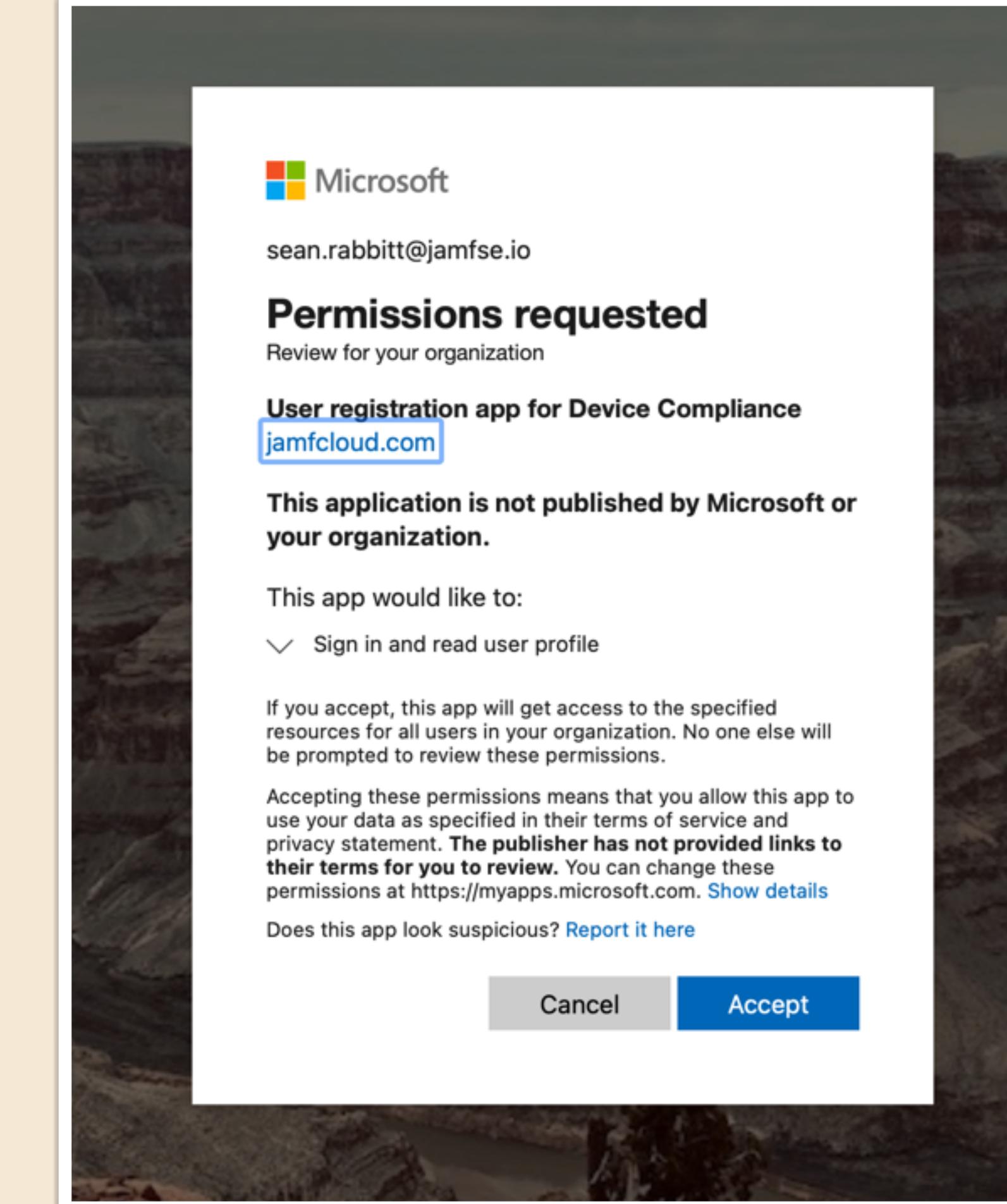
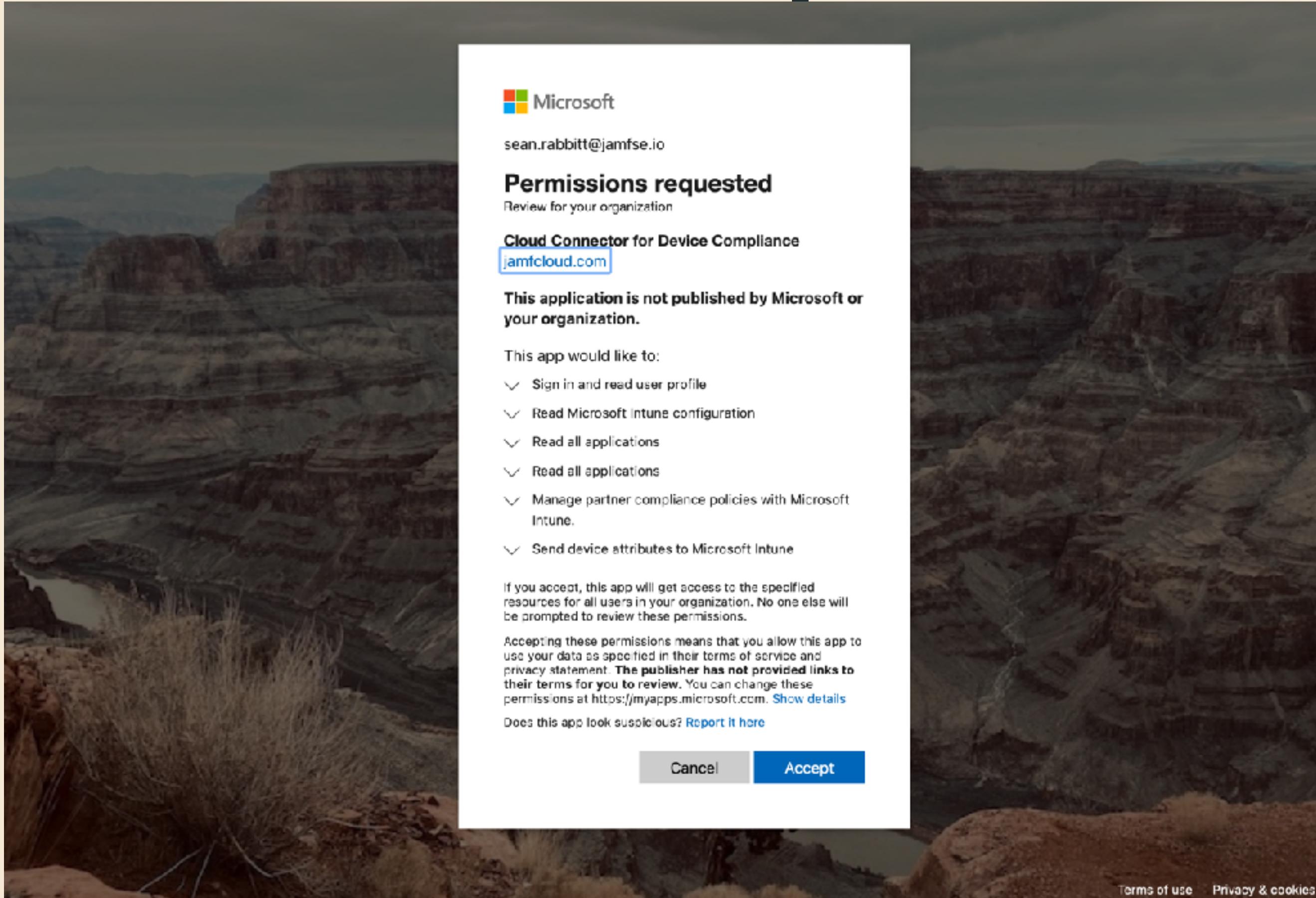
**Registration Page Name** Descriptive name of the enrollment page option for redirection from Microsoft unregistered CA block. This will display to end users to pick. Name could relate to division or organization for each Jamf Pro listed.



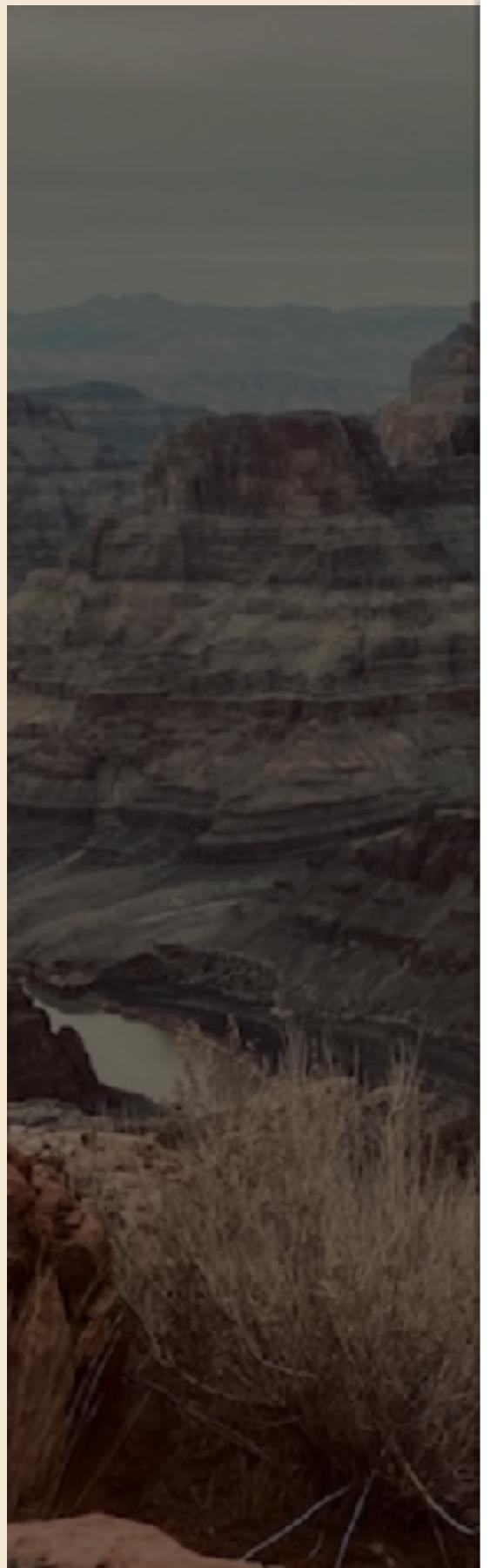
# Jamf Pro Setup



# Jamf Pro Setup



# 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



- [Home](#)
- [Dashboard](#)
- [All services](#)
- [Devices](#)
- [Apps](#)
- [Endpoint security](#)
- [Reports](#)
- [Users](#)
- [Groups](#)
- [Tenant administration](#)
- [Troubleshooting + support](#)

## Connectors and tokens | Partner compliance management



Search

[+ Add compliance partner](#)[Refresh](#)

### Windows

[Windows enterprise certificate](#)[Microsoft Endpoint Configuration Manager](#)[Windows 365 Citrix connector](#)[Windows data](#)

### Apple

[Apple VPP Tokens](#)

### Android and Chrome OS

[Managed Google Play](#)[Chrome Enterprise \(preview\)](#)[Firmware over-the-air update \(preview\)](#)

### Cross platform

[Microsoft Defender for Endpoint](#)[Mobile Threat Defense](#)[Partner device management](#)[Partner compliance management](#)[TeamViewer connector](#)[ServiceNow connector](#)[Certificate connectors](#)

Intune compliance evaluates partner-managed devices in your organization. Set up the connection here.

A device must comply with the highest priority partner assigned to its user. Intune is the default compliance partner and has the lowest priority and cannot be edited or deleted.

[Find out more about connecting compliance partners to Intune.](#)

## Android

Priority	Partner	Assigned	Partner status	Last Successful Sync	Action
Default	Intune	N/A	N/A	N/A	

## iOS

Priority	Partner	Assigned	Partner status	Last Successful Sync	Action
1	Jamf Device Compliant	Yes	Active	7/28/2023, 11:24:41 AM	
Default	Intune	N/A	N/A	N/A	

## macOS

Priority	Partner	Assigned	Partner status	Last Successful Sync	Action
1	Jamf Device Compliant	Yes	Active	7/28/2023, 11:24:41 AM	
Default	Intune	N/A	N/A	N/A	

# Jamf Pro Setup

Settings : Global

← Device Compliance

Configuration status

Use the switch to enable or disable the connection.



 Connection verification status: Success



# Jamf Pro Setup

Computers : Policies

← Register Device with Microsoft

Options Scope Self Service User Interaction

Scripts 0 Scripts

Printers 0 Printers

Disk Encryption Not Configured

Dock Items 0 Dock Items

Local Accounts 0 Accounts

Management Accounts Not Configured

Directory Bindings 0 Bindings

EFI Password Not Configured

Restart Options Not Configured

Maintenance Not Configured

Files and Processes Configured

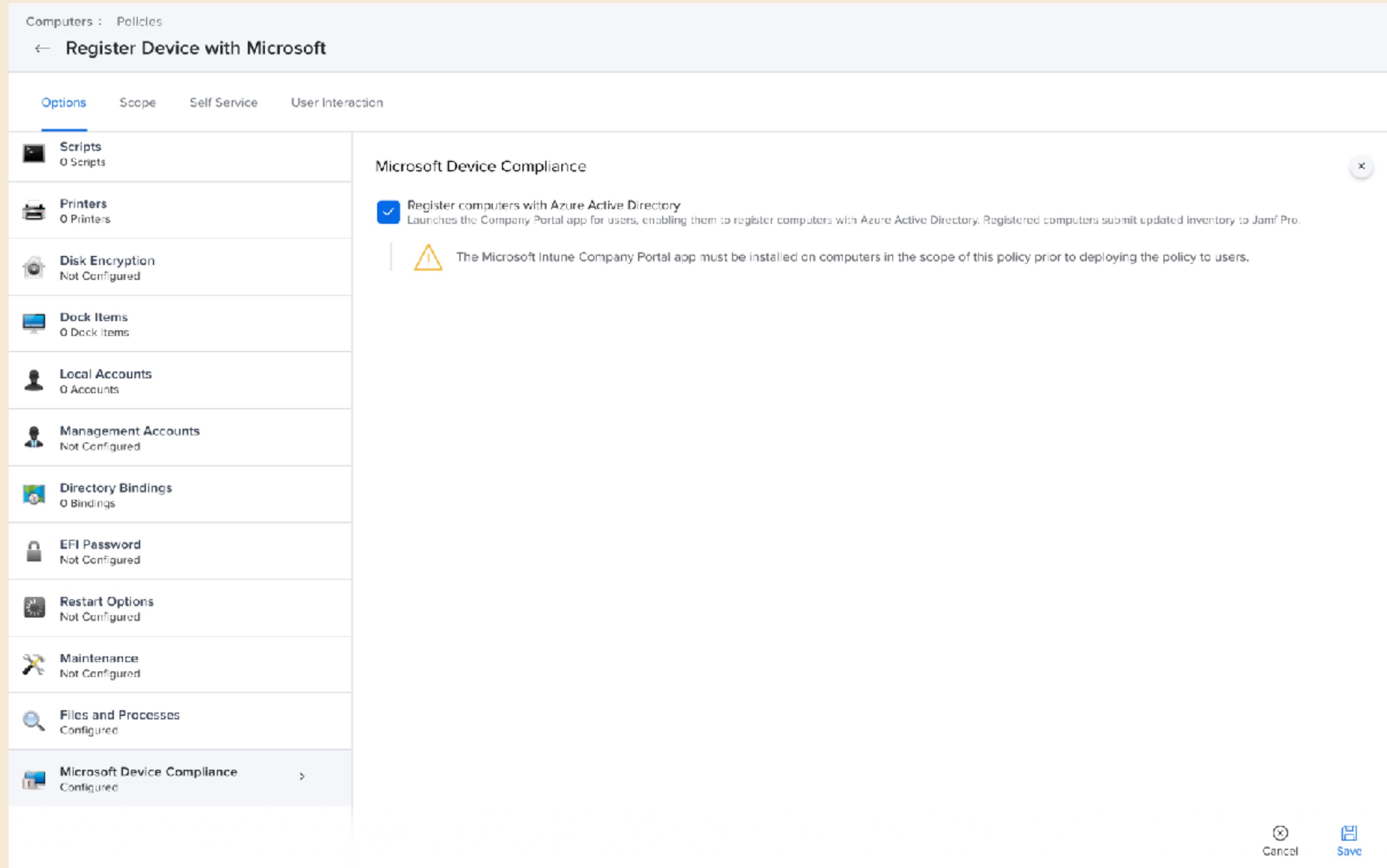
Microsoft Device Compliance > Configured

Microsoft Device Compliance

Register computers with Azure Active Directory  
Launches the Company Portal app for users, enabling them to register computers with Azure Active Directory. Registered computers submit updated inventory to Jamf Pro.

 The Microsoft Intune Company Portal app must be installed on computers in the scope of this policy prior to deploying the policy to users.

(x) Cancel Save



# Jamf Pro Setup

The screenshot shows the Jamf Pro web interface for managing app deployments. The left sidebar navigation includes: Computers, Devices, User, Inventory (Search Inventory, Search Volume Content, Licensed Software), Content Management (Policies, Configuration Profiles, Software Updates, Restricted Software, Mac Apps, Patch Management, eBooks), Groups (Smart Computer Groups, Static Computer Groups, Classes), Enrollment (Enrollment Invitations, PreStage Enrollments), and Settings (Management Settings). The main content area is titled "Microsoft Intune Company Portal Deployment". It displays the following configuration details:

- Display Name:** Microsoft Intune Company Portal
- Site:** None
- Category:** Compliance
- Target Group:** Microsoft Conditional Access - Register
- Distribution Method:** Install automatically
- Configuration profiles for additional settings:** A checked checkbox for "Install supporting configuration profiles" with a note: "Automatically install supporting configuration profiles during deployment of this App Installer. Jamf recommends enabling this option." A tooltip indicates: "Jamf Pro will automatically install configuration profiles with all required settings to successfully deploy this App Installer. These profiles cannot be previewed or removed." A "More information" link is also present.
- App Installer metadata:**

Application name	Media source URL	Installer package hash
Microsoft Intune Company Portal	<a href="https://go.microsoft.com/fwlink/?LinkId=869555">https://go.microsoft.com/fwlink/?LinkId=869555</a>	3b2a62612a6a5afe4b7c5299eee2f6bf

At the bottom right, there are buttons for History, Delete, and Edit. The top right corner shows a notification icon with a red '1' and a gear icon.

# Jamf Pro Setup

Mobile Devices : Mobile Device Apps  
← Microsoft Authenticator

**General** Scope Managed Distribution App Configuration

**Display Name** Display name for the app  
Microsoft Authenticator

Enabled

**Site** Site to add the app to  
None

**Category** Category to add the app to  
Microsoft

**Short Version** Short Version of the app  
6.712

**Bundle Identifier** Bundle identifier for the app  
com.microsoft.azureauthenticator

Free  
App is free

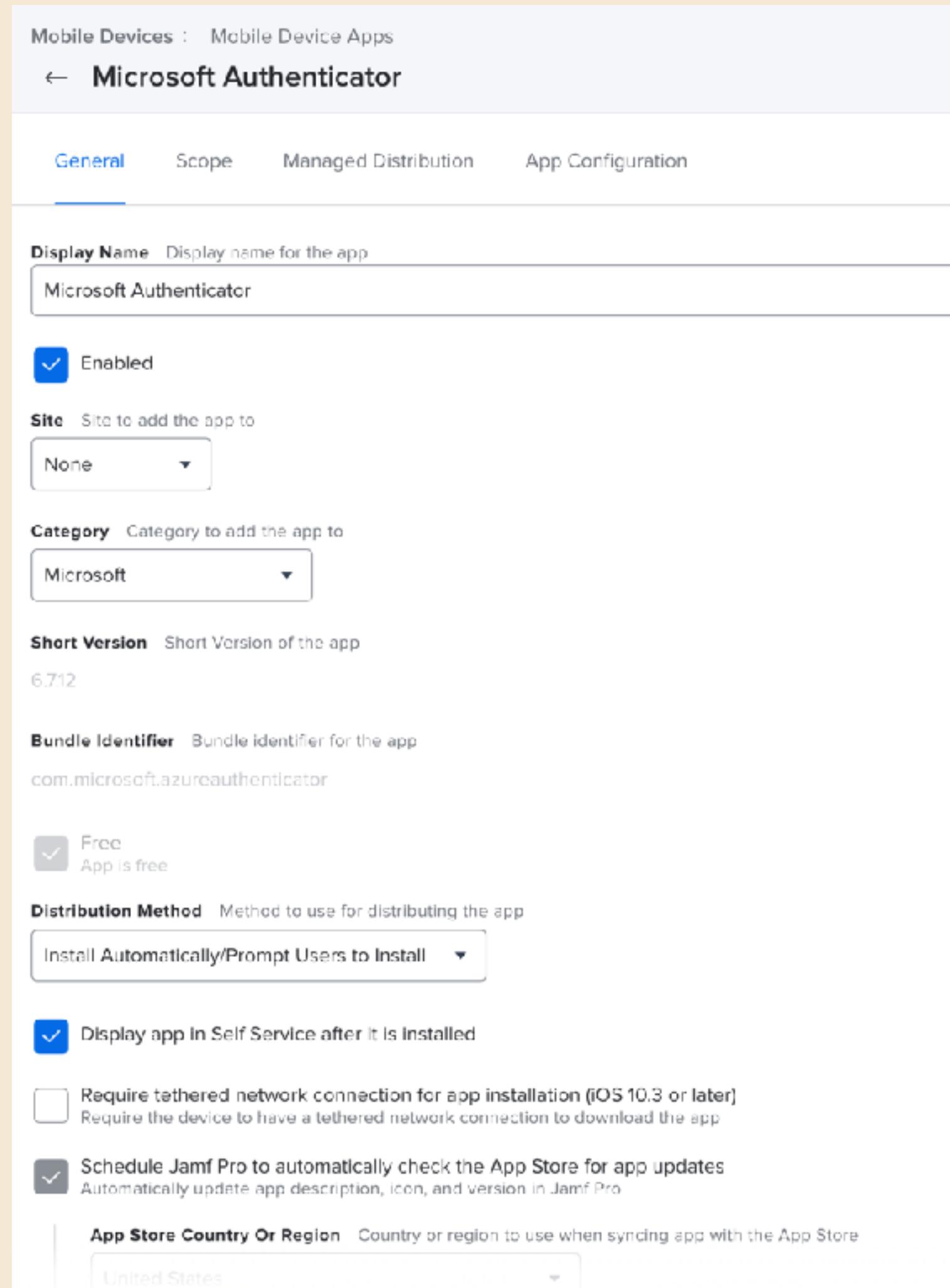
**Distribution Method** Method to use for distributing the app  
Install Automatically/Prompt Users to Install

Display app in Self Service after it is Installed

Require tethered network connection for app installation (iOS 10.3 or later)  
Require the device to have a tethered network connection to download the app

Schedule Jamf Pro to automatically check the App Store for app updates  
Automatically update app description, icon, and version in Jamf Pro

**App Store Country Or Region** Country or region to use when syncing app with the App Store  
United States







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

The screenshot shows the 'Device Compliance' section of the Self Service application. It features two main items: 'Firewall (Turn On)' with an 'Enable' button and 'Register Device with Microsoft' with a 'Re-Register' button. The background of the application window has a blurred orange and yellow gradient.



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

The screenshot shows the 'Device Compliance' section of the Self Service application. It features two main items: 'Firewall (Turn On)' with an 'Enable' button and 'Register Device with Microsoft' with a 'Re-Register' button. The background of the application window has a blurred orange and yellow gradient.



[Home >](#) [Devices | All devices >](#)

## H2WGW2C9Q6NV | Properties

jamfse.io - Azure Active Directory

 [Manage](#)  [Enable](#)  [Disable](#)  [Delete](#)  [Got feedback?](#)

### Manage

 [Properties](#) [Roles and administrators](#) [Administrative Units](#)

Name	H2WGW2C9Q6NV
Device ID	a9289152-10f0-4b0a-8786-aab96ebf7e06
Object ID	d69bde9e-4625-4453-99aa-51ffeba3e354
Enabled	Yes
OS	MacOS
Version	13.5.0
Join Type	Azure AD registered
Owner	User Microsoft
User principal name	user.microsoft@jamfse.io
MDM	Microsoft Intune
Compliant	Yes
Registered	7/31/2023, 9:36:03 AM
Activity	7/31/2023, 9:36:03 AM
Groups	None
Extension Attributes	No Extension Attributes



# Agenda

Conditional Access Recap

Common Deployments & Issues

Jamf Pro & Conditional Access

**Jamf Connect & Conditional Access**

Go Do's!

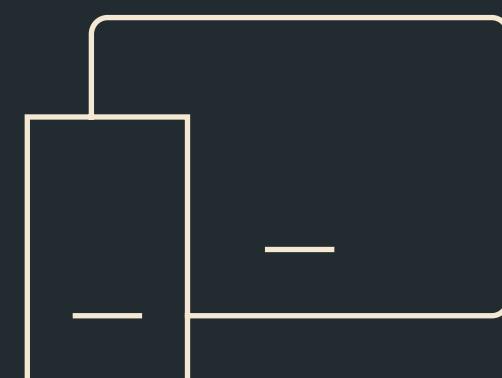


# Remember when we said Conditional Access applies to Cloud Apps?



# Remember when we said Conditional Access applies to Cloud Apps?

Cloud Apps **ARE NOT**



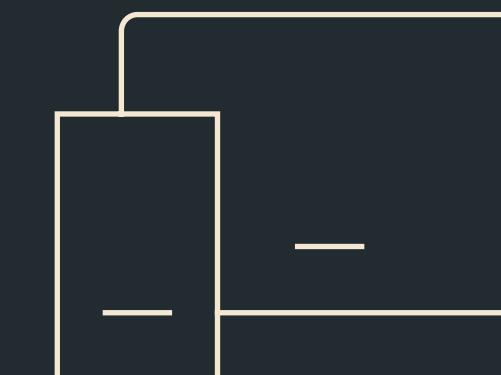
Mobile or desktop apps

OpenID Connect / OAuth 2.0 native clients



# 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!



# Remember when we said Conditional Access applies to Cloud Apps?

Jamf Connect is one of these!



Cloud Apps **ARE NOT**

Mobile or desktop apps

OpenID Connect / OAuth 2.0 native clients

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



# Remember when we said Conditional Access applies to Cloud Apps?

Jamf Connect is one of these!



Cloud Apps **ARE NOT**

Mobile or desktop apps

OpenID Connect / OAuth 2.0 native clients

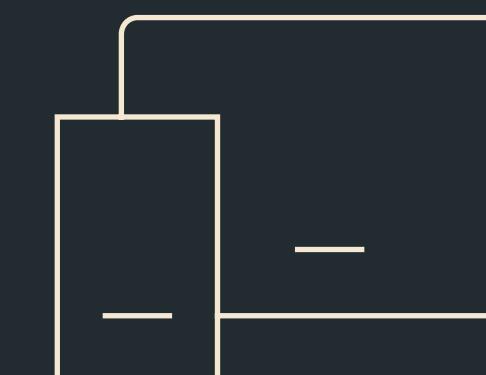
**Reminder: CA is applied to the RESOURCE**  
**Ex: You apply it to Exchange Online, NOT Outlook**

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



# Remember when we said Conditional Access applies to Cloud Apps?

Jamf Connect is one of these!



Cloud Apps **ARE NOT**

Mobile or desktop apps

OpenID Connect / OAuth 2.0 native clients

**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:



# But which API?

There's a few options:

API	Pros	Cons
Azure AD Graph API	Been around forever	Support is ending!



# 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



# 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



# 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!

Microsoft Graph API

Custom API



# Custom API...why?



# 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



# 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?

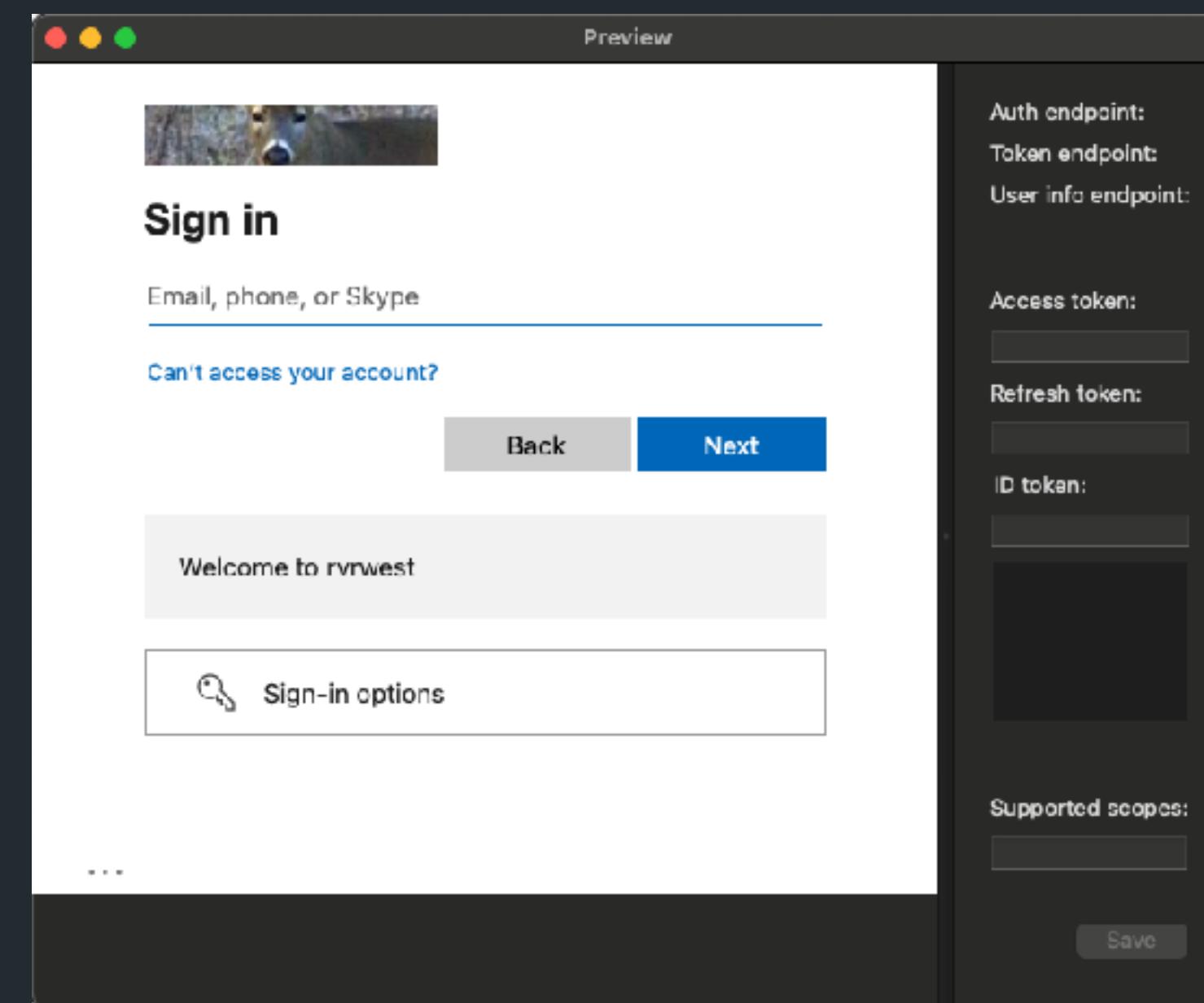
OIDC (Auth Code)

ROPG/ROPC



# Custom API...why?

OIDC (Auth Code)



ROPG/ROPC



# Registering a Custom API in Entra ID

The screenshot shows the Microsoft Entra ID interface. On the left, there is a navigation sidebar with the following items:

- Home
- Favorites
- Identity
  - Overview
  - Users
  - Groups
  - Devices
- Applications
  - Enterprise applications
  - App registrations
- Roles & admins

A red arrow points from the top of the sidebar towards the 'App registrations' item. Another red arrow points from the bottom of the sidebar towards the 'App registrations' item.

The main content area is titled 'App registrations' and shows the following details:

- Header buttons: New registration, Endpoints, Troubleshooting, Refresh
- Information banner: Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory B2B feature updates. Applications will need to be upgraded to Microsoft App registrations.
- Filter tabs: All applications, **Owned applications**, Deleted applications
- Search bar: Start typing a display name or application (client) ID to filter these applications
- Count: 90 applications found
- Sort by: Display name ↑
- List of applications:
  - AP Access Package Custom Extension Workflows
  - AA API App 01

# Registering a Custom API in Entra ID

The screenshot shows the Microsoft Entra ID interface. On the left, there's a navigation sidebar with various links: Home, Favorites, Identity, Overview, Users, Groups, Devices, Applications, Enterprise applications, App registrations, and Roles & admins. The 'Enterprise applications' link has a red arrow pointing to it from below. The 'App registrations' link under 'Enterprise applications' also has a red arrow pointing to it from the left. The main content area is titled 'App registrations' and shows a message about feature deprecation. It has tabs for 'All applications', 'Owned applications' (which is selected), and 'Deleted applications'. A search bar says 'Start typing a display name or application (client) ID to filter these'. Below, it says '90 applications found' and lists two items: 'Access Package Custom Extension Workflows' (AP) and 'API App 01' (AA).

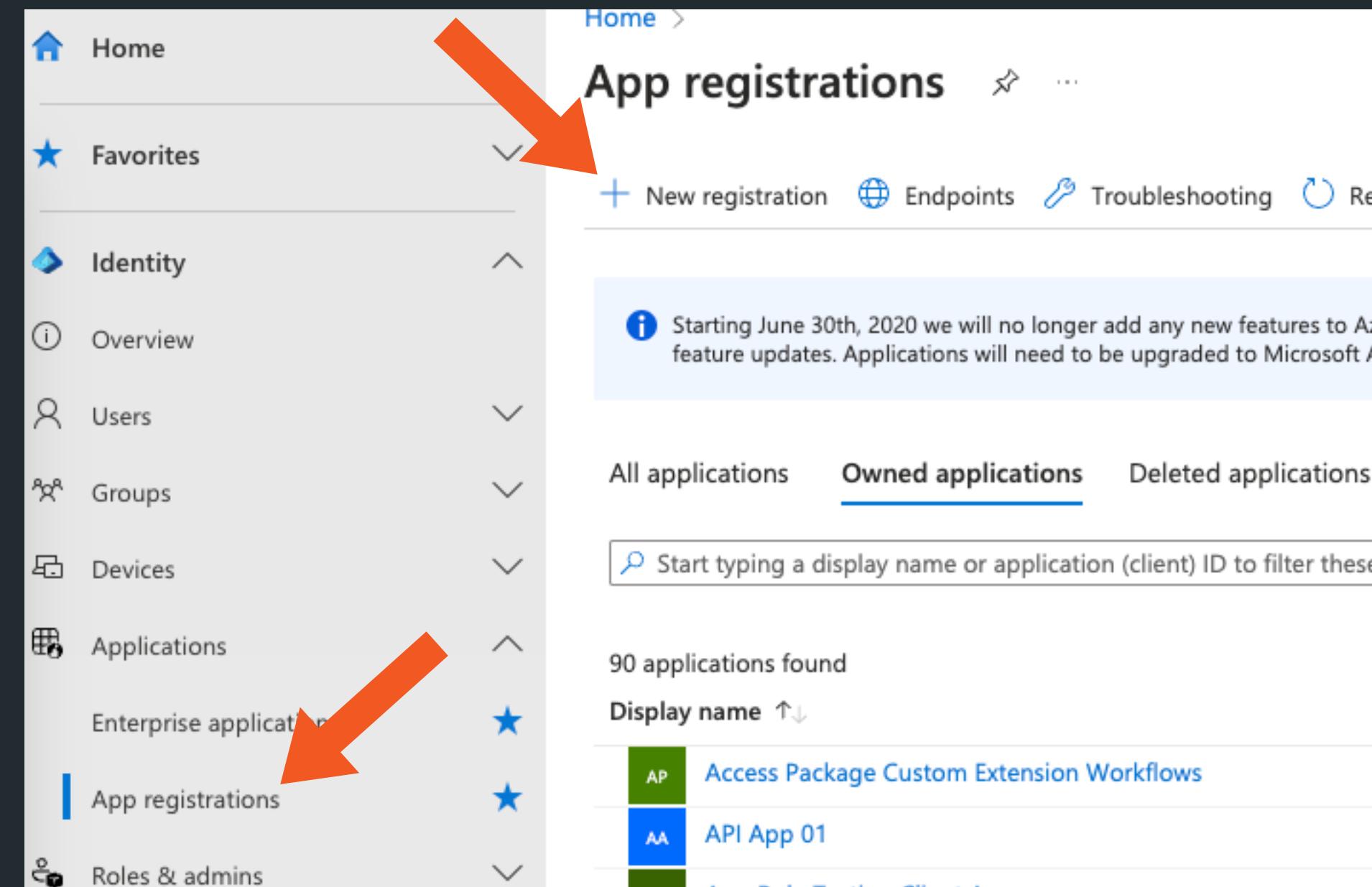
**There's still a few issues we need to solve**

## Common Customer Requirements:

- 1. Require MFA in web UI on lock screen**



# Registering a Custom API in Entra ID



The screenshot shows the Microsoft Entra ID interface. On the left, there's a navigation sidebar with icons for Home, Favorites, Identity, Overview, Users, Groups, Devices, Applications, Enterprise applications, App registrations, and Roles & admins. The 'App registrations' item is highlighted with a blue selection bar. In the main content area, the title 'App registrations' is at the top, followed by a 'New registration' button, 'Endpoints', 'Troubleshooting', and a refresh icon. A message box states: 'Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory B2B feature updates. Applications will need to be upgraded to Microsoft Entra ID.' Below this, tabs for 'All applications', 'Owned applications' (which is selected and underlined), and 'Deleted applications' are shown. A search bar says 'Start typing a display name or application (client) ID to filter these'. It shows 90 applications found, with a 'Display name' column header and two entries: 'Access Package Custom Extension Workflows' (AP) and 'API App 01' (AA).

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



# Registering a Custom API in Entra ID

The screenshot shows the Microsoft Entra ID portal. On the left, there's a navigation sidebar with icons for Home, Favorites, Identity, Overview, Users, Groups, Devices, Applications, Enterprise applications, App registrations, and Roles & admins. The 'App registrations' link is highlighted with a red arrow. The main content area is titled 'App registrations' and shows a message about feature updates. It has tabs for All applications, Owned applications (which is selected), and Deleted applications. A search bar says 'Start typing a display name or application (client) ID to filter these'. Below it, it says '90 applications found' and lists two items: 'Access Package Custom Extension Workflows' (AP) and 'API App 01' (AA).

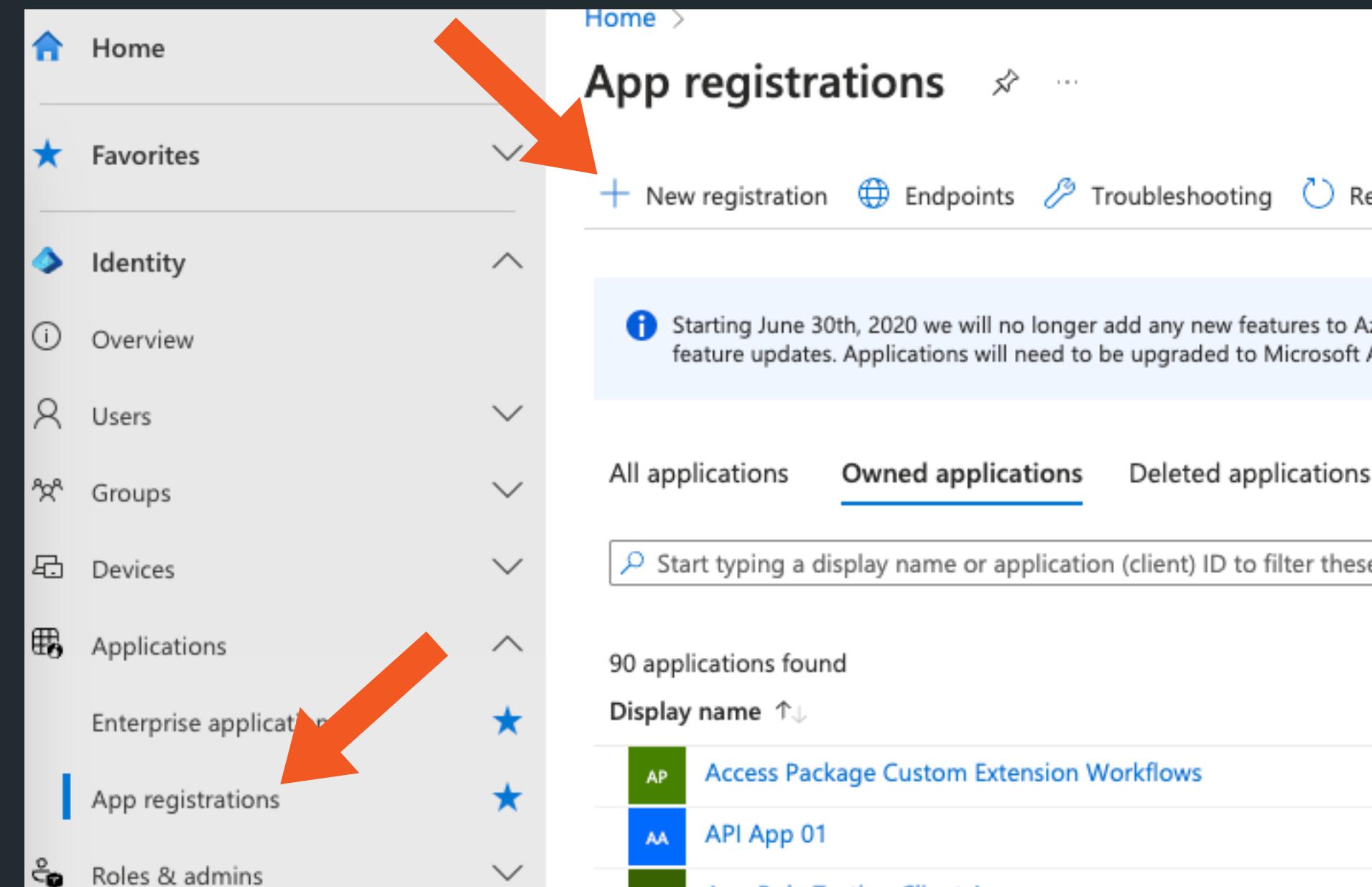
There's still a few issues we need to solve

## 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**



# Registering a Custom API in Entra ID



The screenshot shows the Microsoft Entra ID interface. On the left, there's a sidebar with various navigation items: Home, Favorites, Identity, Overview, Users, Groups, Devices, Applications, Enterprise applications, App registrations, and Roles & admins. The 'App registrations' item is highlighted with a blue background and has a red arrow pointing to it from the bottom-left. At the top, there's a header with 'Home >' and the title 'App registrations'. Below the header, there are buttons for 'New registration', 'Endpoints', 'Troubleshooting', and 'Refresh'. A message box states: 'Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory B2B feature updates. Applications will need to be upgraded to Microsoft Entra ID.' There are tabs for 'All applications', 'Owned applications' (which is selected and underlined in blue), and 'Deleted applications'. A search bar says 'Start typing a display name or application (client) ID to filter these'. Below the search bar, it says '90 applications found' and lists two entries: 'Access Package Custom Extension Workflows' (AP) and 'API App 01' (AA). The 'API App 01' entry has a red arrow pointing to it from the top-right.

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



Conditional Access “All Apps”  
MFA Policy Applied here



 jamf | CONNECT  
Cloud App  
Registered in Entra ID

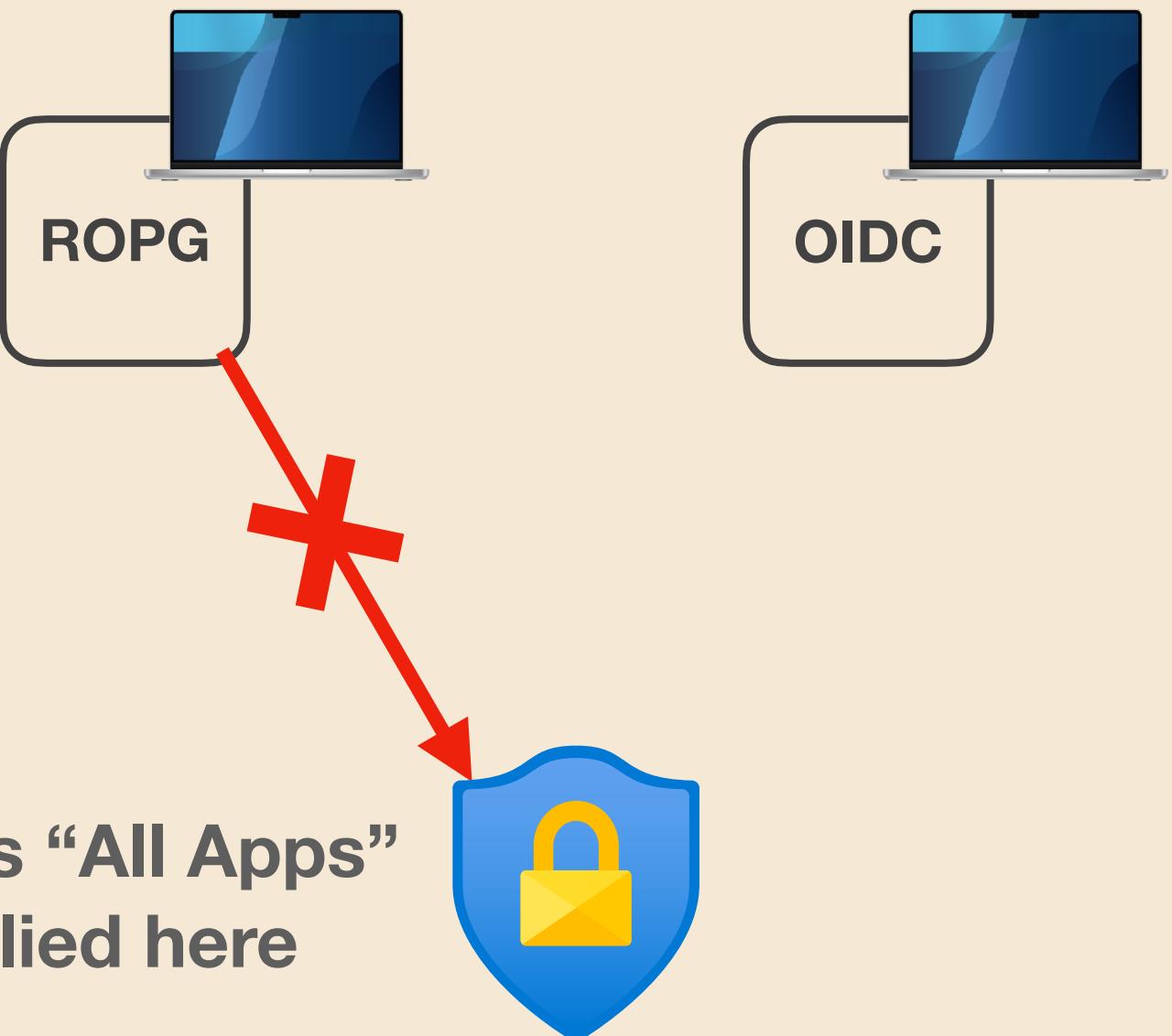


MS Graph API



# Problem 1: MFA Policies

Blocked by MFA Requirement  
Shows as failed sign-in in Entra ID



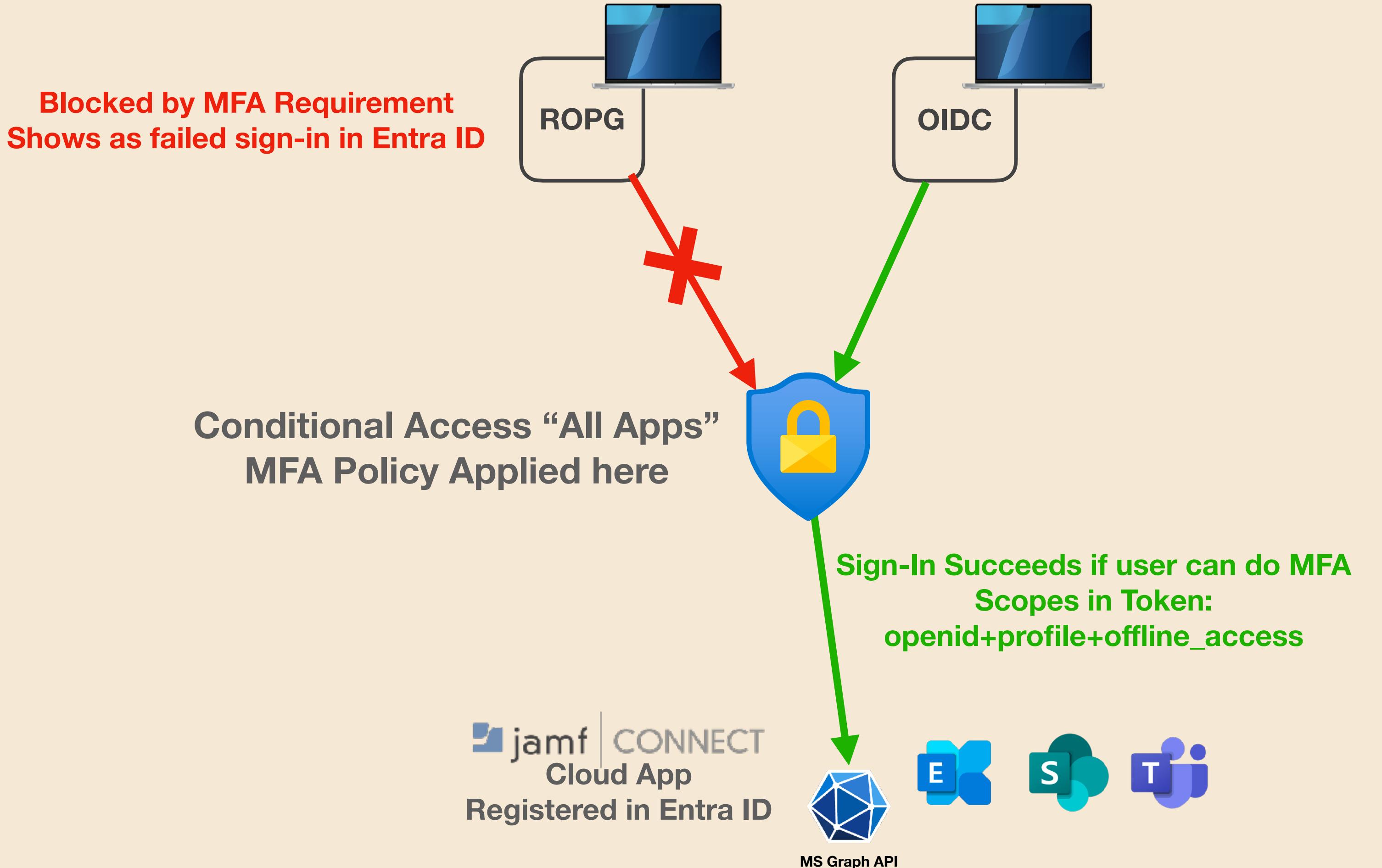
jamf | CONNECT  
Cloud App  
Registered in Entra ID



MS Graph API



# Problem 1: MFA Policies



# Problem 2: Compliant Device Policies



Conditional Access “All Apps”  
MFA Policy Applied here



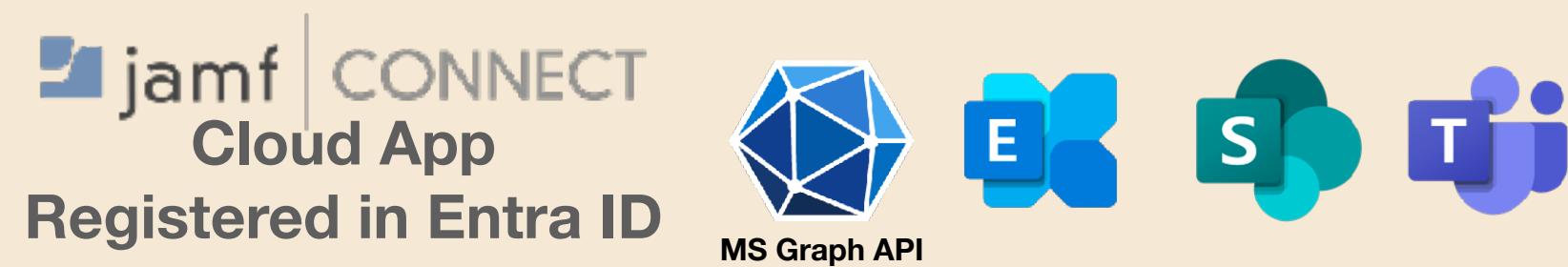
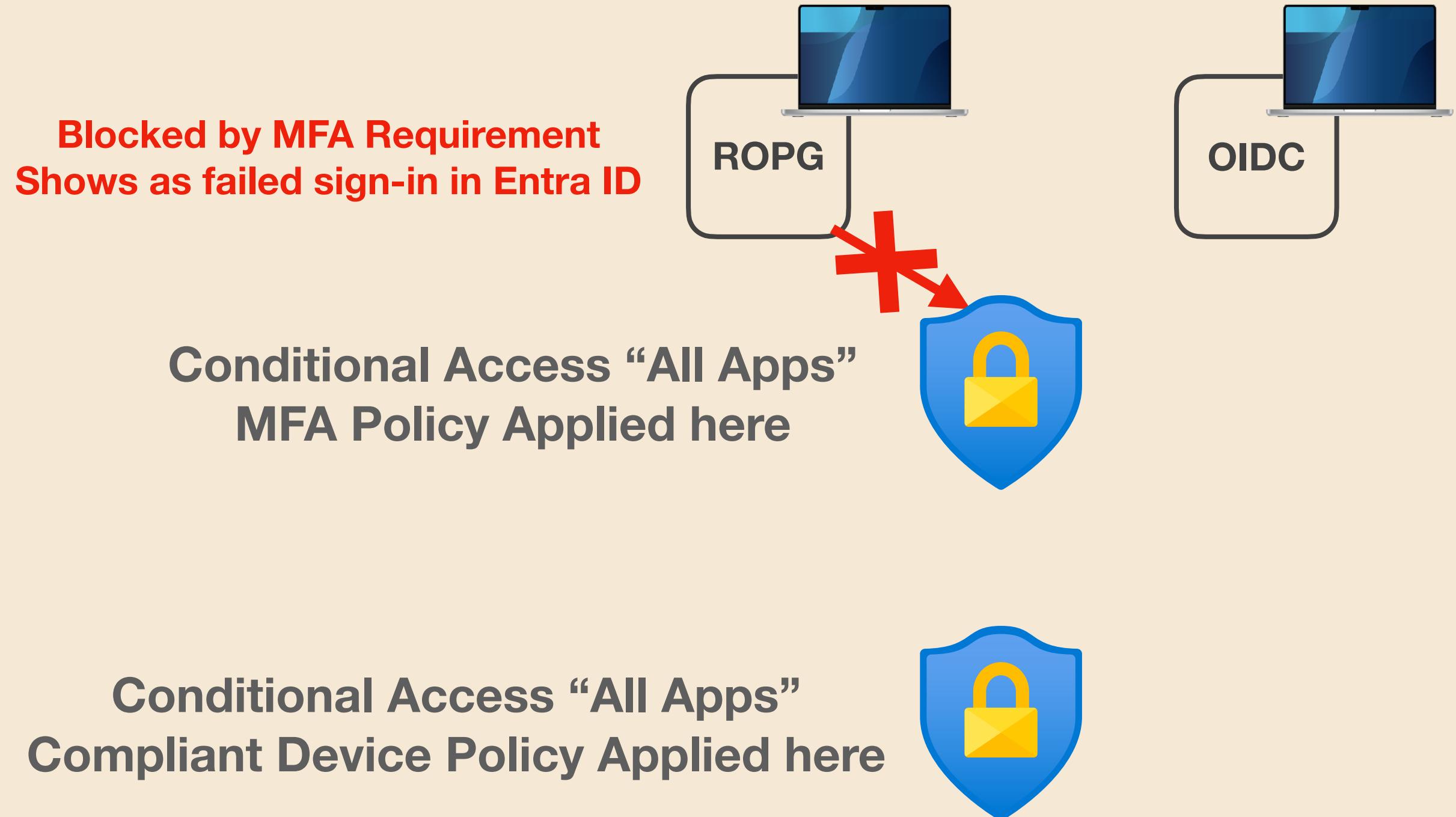
Conditional Access “All Apps”  
Compliant Device Policy Applied here



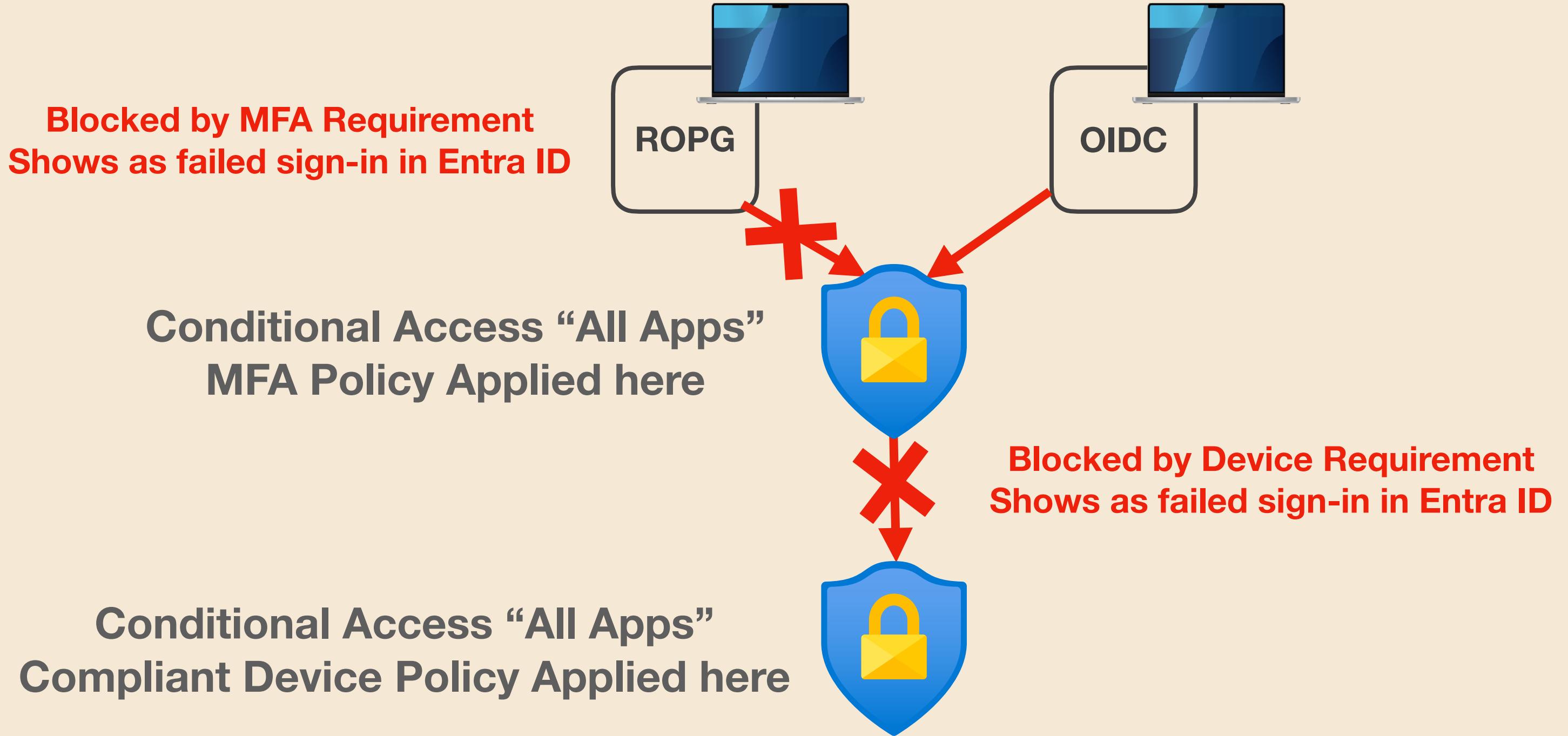
 jamf | CONNECT  
Cloud App  
Registered in Entra ID



# Problem 2: Compliant Device Policies



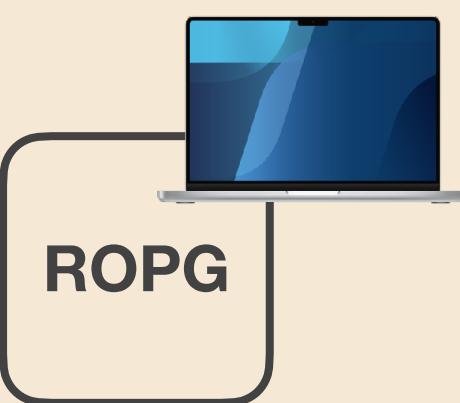
# Problem 2: Compliant Device Policies



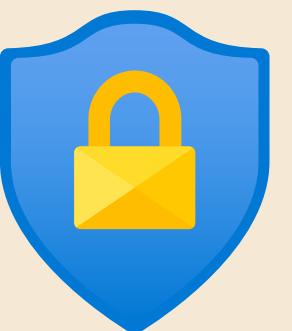
 **jamf** | CONNECT  
Cloud App  
Registered in Entra ID



# Problem 3: Exclusions



Conditional Access “All Apps”  
MFA Policy Applied here



Conditional Access “All Apps”  
Compliant Device Policy Applied here

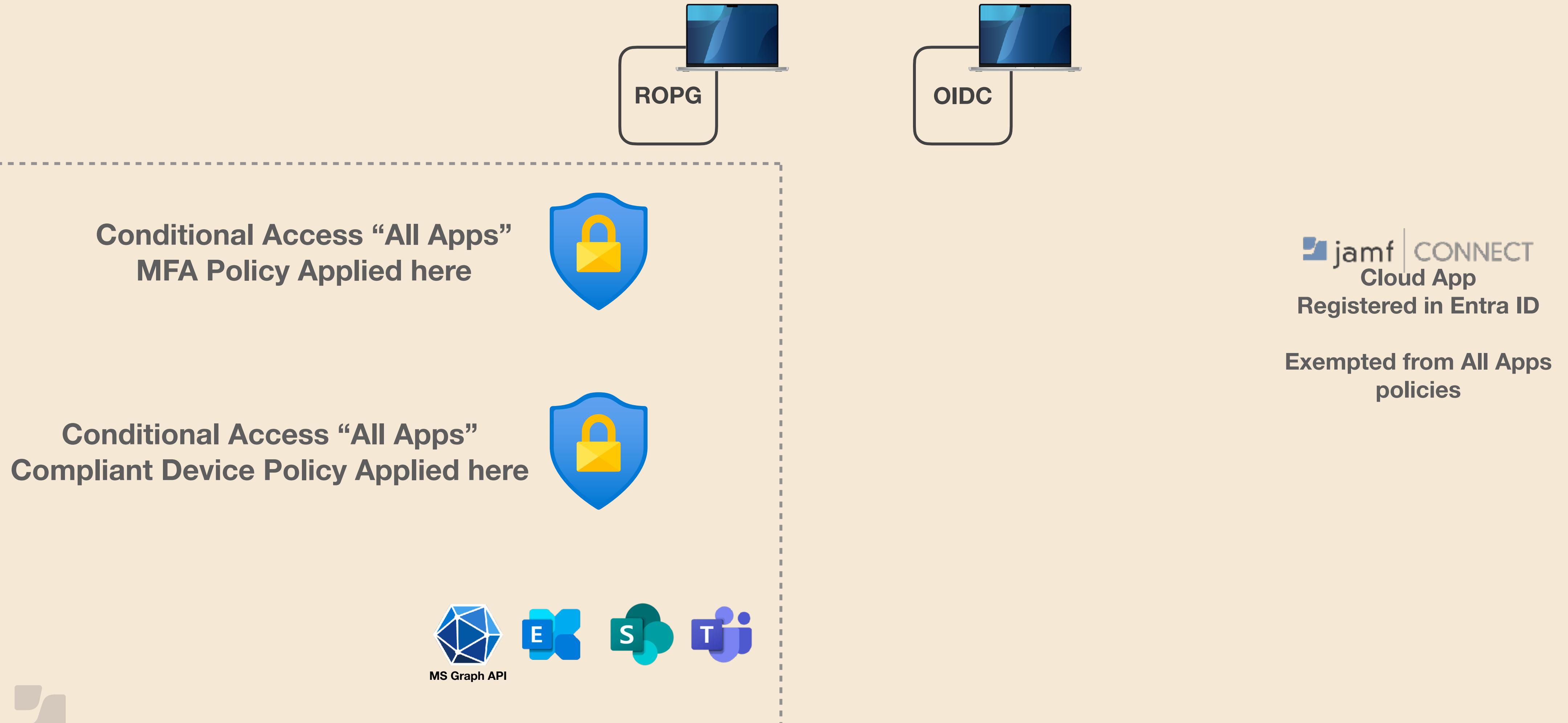


jamf CONNECT  
Cloud App  
Registered in Entra ID

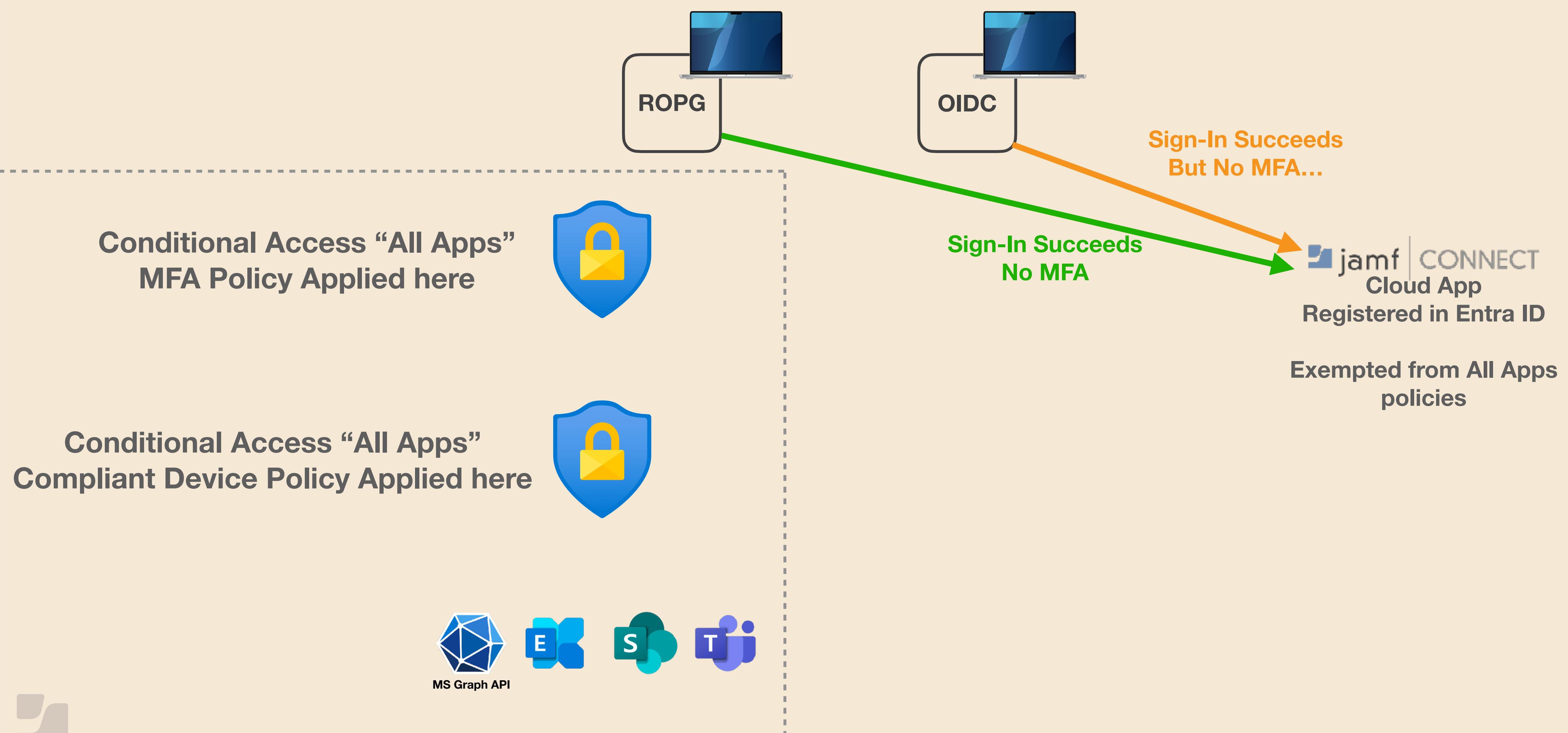
Exempted from All Apps  
policies



# Problem 3: Exclusions



# Problem 3: Exclusions





© copyright 2002-2023 Jamf



# What now?

## How do we meet all 3 requirements?



# What now?

How do we meet all 3 requirements?

We need more than one custom App and API!

[aka.ms/JC\\_CA](https://aka.ms/JC_CA)



# Solution



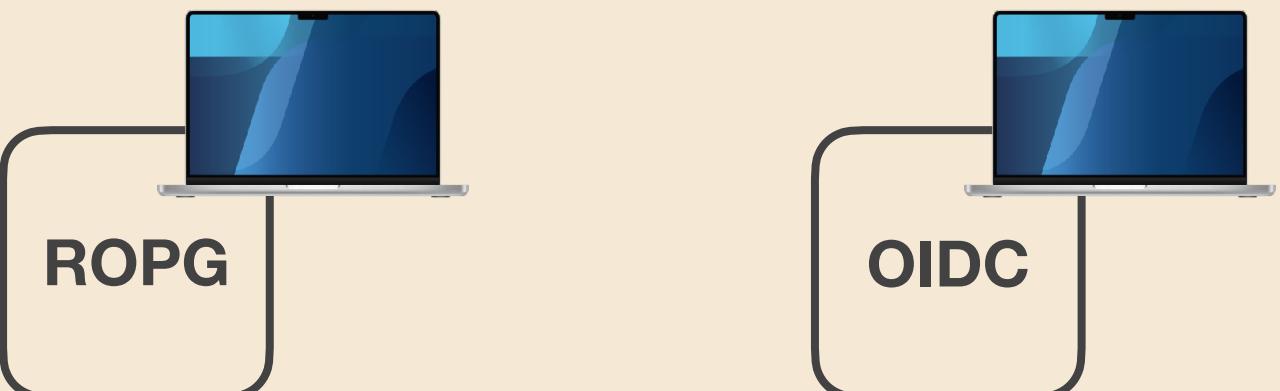
# Solution

jamf CONNECT

ROPG Cloud App

Registered in Entra ID

Exempted from All Apps policies



Conditional Access “All Apps”  
MFA Policy Applied here



jamf CONNECT

API Cloud App

Registered in Entra ID

Subject to All Apps MFA  
Policies

Conditional Access “All Apps”  
Compliant Device Policy Applied here



jamf CONNECT

OIDC Cloud App

Registered in Entra ID

Exempted from All Apps policies

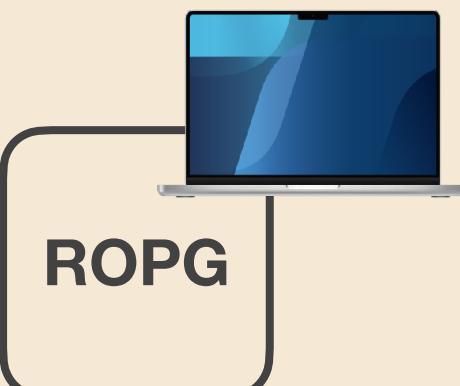
# Solution



ROPG Cloud App  
Registered in Entra ID

Exempted from All Apps policies

Sign-In Succeeds  
No MFA



Conditional Access “All Apps”  
MFA Policy Applied here



API Cloud App  
Registered in Entra ID

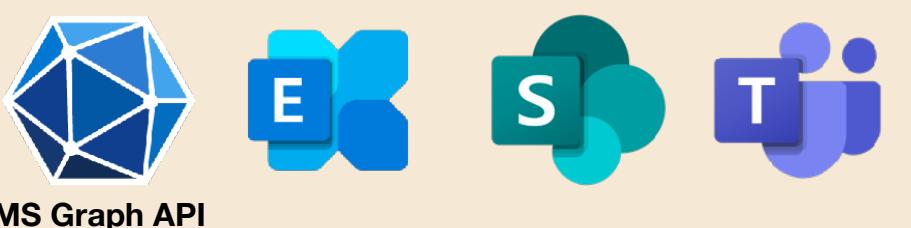
Subject to All Apps MFA Policies

Conditional Access “All Apps”  
Compliant Device Policy Applied here



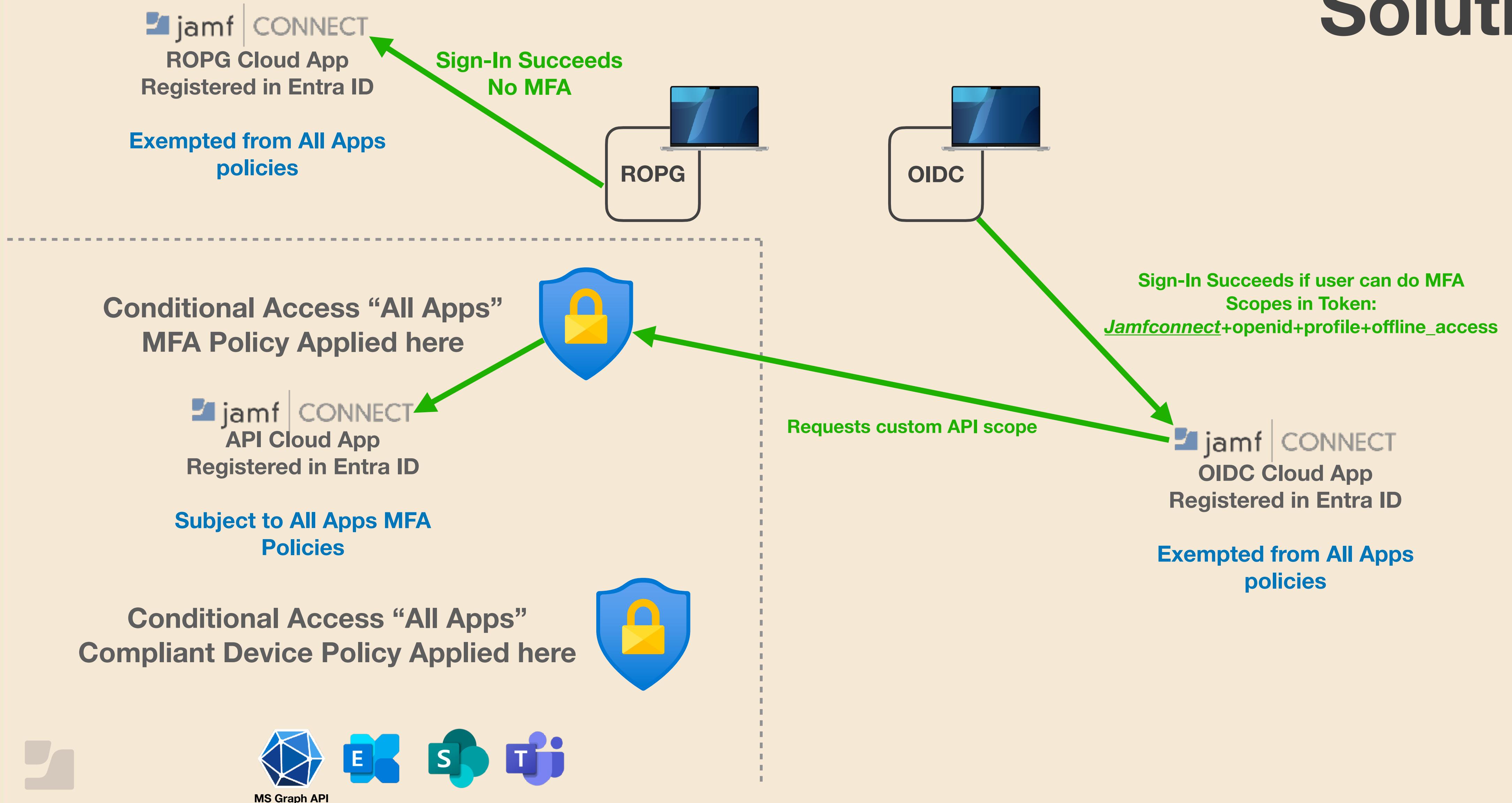
OIDC Cloud App  
Registered in Entra ID

Exempted from All Apps policies



MS Graph API

# Solution



# Solution: Entra ID App Config

Display name ↑↓		Application (client) ID
JC	Jamf Connect - API	8d289493-ebc0-4425-bb18-6f6e7adce4c
JC	Jamf Connect - OIDC	153fb010-cf53-4a2a-8a20-1a1a1a1a1a1a
JC	Jamf Connect - ROPC	0233f8ac-8040-4a00-8000-000000000000

Home > App registrations > Jamf Connect - API

## Jamf Connect - API | Expose an API

Search Got feedback?

Application ID URI : `api://8d289493-ebc0-4425-bb18-6f6e7adce4c` Edit

Scopes defined by this API

Define custom scopes to restrict access to data and functionality protected by the API. An application that requires access to parts of this API can request that a user or admin consent to one or more of these.

Adding a scope here creates only delegated permissions. If you are looking to create application-only scopes, use 'App roles' and define app roles assignable to application type. [Go to App roles](#).

+ Add a scope

Scopes	Who can consent	Admin consent display name	User consent display name	State
<code>api://8d289493-ebc0-4425-bb18-6f6e7adce4c/jamfc...</code>	Admins and users	Read user information		Enabled

Authorized client applications

Authorizing a client application indicates that this API trusts the application and users should not be asked to consent when the client calls this API.

Manage

- Branding & properties
- Authentication
- Certificates & secrets
- Token configuration
- API permissions
- Expose an API**
- App roles
- Owners
- Roles and administrators
- Manifest



# Solution: Entra ID App Config

The screenshot displays three separate pages from the Microsoft Entra ID portal:

- Top Left:** A list of applications found, showing three entries: "Jamf Connect - API", "Jamf Connect - OIDC", and "Jamf Connect - ROPC".
- Middle Left:** The "Jamf Connect - API | Expose an API" configuration page. It shows the application ID URI as "api://8d289493-ebc0-4425-b...". Under "Manage", the "API permissions" section is highlighted with a yellow background. The "Expose an API" option is also highlighted with a yellow background.
- Right:** The "Jamf Connect - OIDC | API permissions" configuration page. It shows the "jamfconnect" permission under "Microsoft Graph (1)". The "User.Read" scope is listed with a "Delegated" type and a "Read user information" description. The "Admin consent required" column shows "No", and the "Status" column shows "Granted for michaelepping.com".

Two red arrows point upwards from the highlighted sections in the left-hand navigation menus towards the top navigation bar of the middle-right page, indicating the relationship between the configurations.



# Solution: Entra ID App Tagging

Jamf Connect - ROPC | Custom security attributes (preview)

Enterprise Application

Overview Deployment Plan Diagnose and solve problems

Manage Properties Owners Roles and administrators Users and groups Single sign-on Provisioning Custom security attributes (preview)

Save Discard Add assignment Remove assignment Got feedback?

Search attribute names or values Add filters

Attribute set	Attribute name	Attribute description	Data type	Multi-valued	Assigned values
AppFilters	caExemption		String	No	CAExempt



# Solution: Entra ID App Tagging

aka.ms/JC\_CSA

[https://aka.ms/JC\\_CAFilters](https://aka.ms/JC_CAFilters)

The screenshot shows the Jamf Connect - ROPC | Custom security attributes (preview) page. The left sidebar lists various management options, with 'Custom security attributes (preview)' highlighted by a red arrow. The main area displays a table for managing custom security attributes. One row is selected, showing the attribute name 'caExemption'. A red arrow points to this attribute name. Another red arrow points to the 'Assigned values' column, which contains the value 'CAExempt'. The table columns are: Attribute set, Attribute name, Attribute description, Data type, Multi-valued, and Assigned values.

Attribute set	Attribute name	Attribute description	Data type	Multi-valued	Assigned values
AppFilters	caExemption		String	No	CAExempt



# Solution: Entra ID App Tagging

The screenshot shows the configuration of a Conditional Access policy named "Require Compliant Device for All Apps". The policy is set to apply to "Cloud apps" using the "Exclude" option. It targets "All users" and "All cloud apps". The "Edit filter (Preview)" section shows a single condition labeled "Configured". There are no excluded cloud apps.

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Name \*  
Require Compliant Device for All Apps ✓

Assignments

Users or workload identities ⓘ  
All users

Target resources ⓘ  
All cloud apps

Conditions ⓘ  
1 condition selected

Access controls

Grant ⓘ  
1 control selected

Session ⓘ  
0 controls selected

Control access based on all or specific network access traffic, cloud apps or actions. [Learn more](#)

Select what this policy applies to  
Cloud apps

Include Exclude

Select the cloud apps to exempt from the policy

Edit filter (Preview)  
Configured

Select excluded cloud apps  
None



# Solution: Entra ID App Tagging

The screenshot shows the Microsoft Conditional Access policy configuration interface. A modal window titled "Edit filter (Preview)" is open, overlaid on the main policy configuration screen.

**Main Policy Configuration (Left):**

- Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)
- Name **Require Compliant Device for All Apps** (highlighted with a purple border)
- Assignments:
  - Users or workload identities: All users
  - Target resources: All cloud apps (highlighted with a red arrow)
- Conditions: 1 condition selected
- Access controls: Grant 1 control selected
- Session: 0 controls selected

**Edit filter (Preview) Modal (Right):**

Control access based on all or specific network access traffic, cloud apps or actions. [Learn more](#)

Select what this policy applies to: Cloud apps

Include **Exclude** (highlighted with a red arrow)

Select the cloud apps to exempt from the policy

**Edit filter (Preview)**

Configured Yes (highlighted with a red arrow)

Select excluded cloud apps: None

Using custom security attributes you can use the rule builder or rule syntax text box to create or edit the filter rules. In the preview, only attributes of type String are supported. Attributes of type Integer or Boolean will not be shown. [Learn more](#)

And/Or	Attribute	Operator	Value
	AppFilters_caExemption	Equals	CAExempt

+ Add expression

Rule syntax: `CustomSecurityAttribute.AppFilters_caExemption -eq "CAExempt"`



# Solution: Entra ID App Tagging

Edit filter (Preview)

Configure ⓘ  
 Yes  No

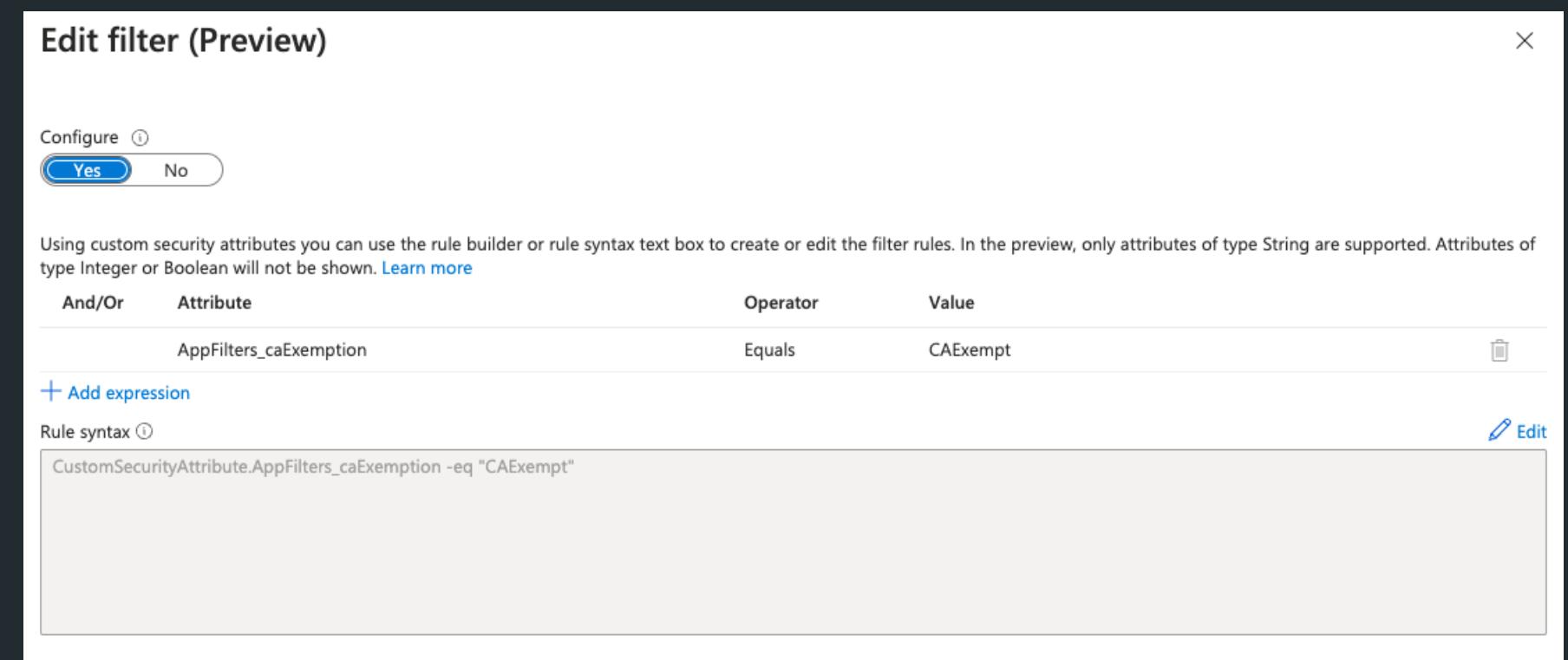
Using custom security attributes you can use the rule builder or rule syntax text box to create or edit the filter rules. In the preview, only attributes of type String are supported. Attributes of type Integer or Boolean will not be shown. [Learn more](#)

And/Or	Attribute	Operator	Value
	AppFilters_caExemption	Equals	CAExempt

+ Add expression

Rule syntax ⓘ  
CustomSecurityAttribute.AppFilters\_caExemption -eq "CAExempt"

Edit



# Solution: Entra ID App Tagging

Edit filter (Preview)

Configure ⓘ  
 Yes  No

Using custom security attributes you can use the rule builder or rule syntax text box to create or edit the filter rules. In the preview, only attributes of type String are supported. Attributes of type Integer or Boolean will not be shown. [Learn more](#)

And/Or	Attribute	Operator	Value
	AppFilters_caExemption	Equals	CAExempt

+ Add expression

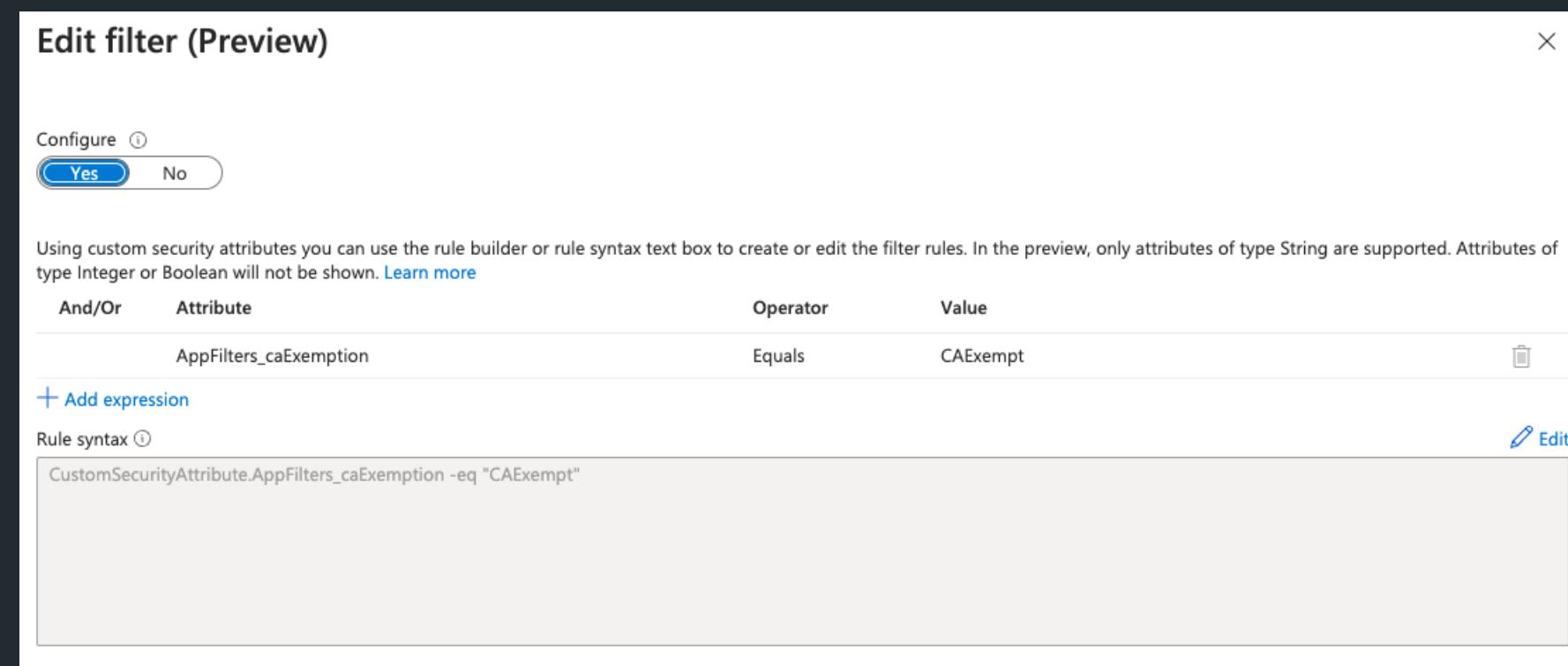
Rule syntax ⓘ

```
CustomSecurityAttribute.AppFilters_caExemption -eq "CAExempt"
```

Why are we doing this with tags?



# Solution: Entra ID App Tagging



Configure ⓘ

Yes  No

Using custom security attributes you can use the rule builder or rule syntax text box to create or edit the filter rules. In the preview, only attributes of type String are supported. Attributes of type Integer or Boolean will not be shown. [Learn more](#)

And/Or	Attribute	Operator	Value
	AppFilters_caExemption	Equals	CAExempt

+ Add expression

Rule syntax ⓘ

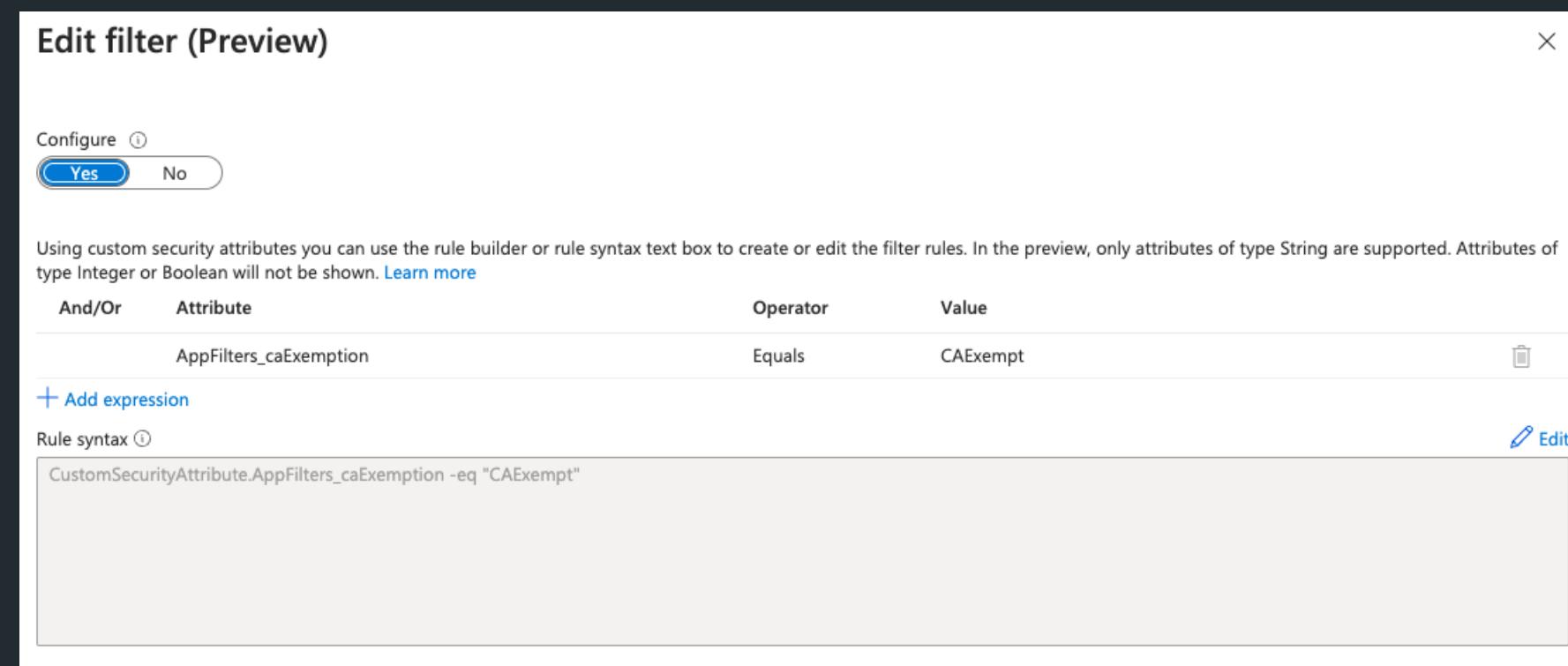
```
CustomSecurityAttribute.AppFilters_caExemption -eq "CAExempt"
```

## Why are we doing this with tags?

- Normally, ROPG apps and other public clients cannot be explicitly included or excluded from Conditional Access policies



# Solution: Entra ID App Tagging



Configure ⓘ

Yes  No

Using custom security attributes you can use the rule builder or rule syntax text box to create or edit the filter rules. In the preview, only attributes of type String are supported. Attributes of type Integer or Boolean will not be shown. [Learn more](#)

And/Or	Attribute	Operator	Value
	AppFilters_caExemption	Equals	CAExempt

+ Add expression

Rule syntax ⓘ

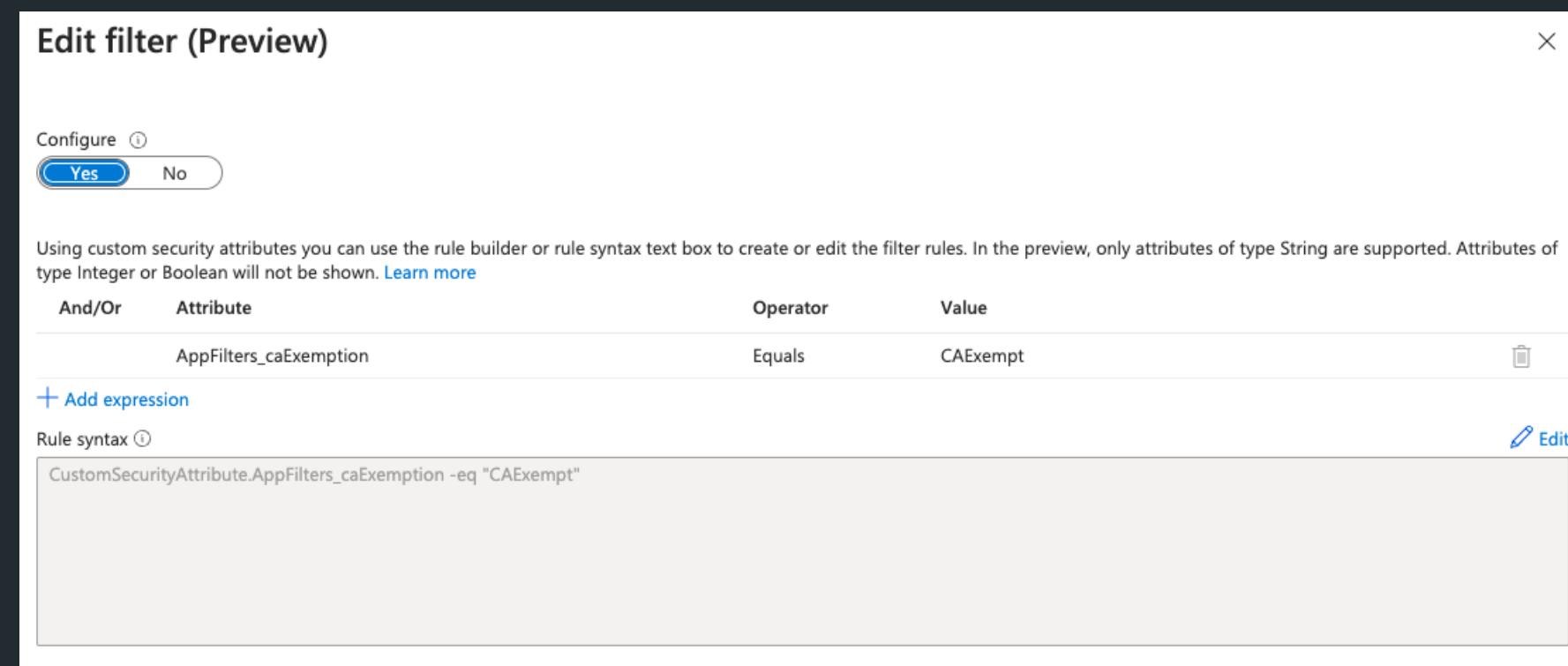
```
CustomSecurityAttribute.AppFilters_caExemption -eq "CAExempt"
```

## 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



# Solution: Entra ID App Tagging



The screenshot shows the 'Edit filter (Preview)' dialog box. At the top, there's a 'Configure' section with 'Yes' (selected) and 'No' buttons. Below that, a note states: 'Using custom security attributes you can use the rule builder or rule syntax text box to create or edit the filter rules. In the preview, only attributes of type String are supported. Attributes of type Integer or Boolean will not be shown. [Learn more](#)'.

And/Or	Attribute	Operator	Value
	AppFilters_caExemption	Equals	CAExempt

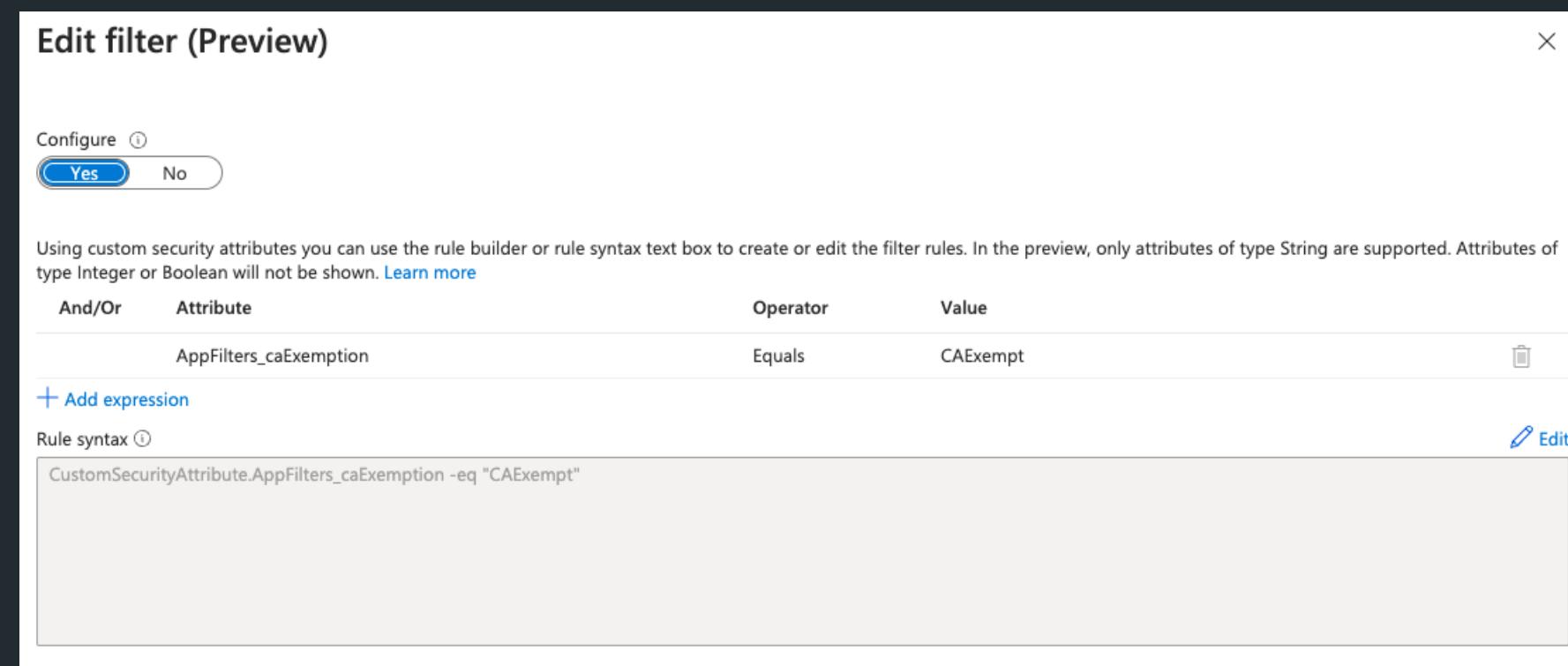
Below the table, there's a '+ Add expression' button and a 'Rule syntax' section containing the PowerShell-like rule: 'CustomSecurityAttribute.AppFilters\_caExemption -eq "CAExempt"'.

## 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!



# Solution: Entra ID App Tagging



The screenshot shows the 'Edit filter (Preview)' dialog box. At the top, there's a 'Configure' button with 'Yes' selected. Below it, a note states: 'Using custom security attributes you can use the rule builder or rule syntax text box to create or edit the filter rules. In the preview, only attributes of type String are supported. Attributes of type Integer or Boolean will not be shown. [Learn more](#)'.

And/Or	Attribute	Operator	Value
	AppFilters_caExemption	Equals	CAExempt

Below the table, there's a '+ Add expression' button and a 'Rule syntax' section containing the PowerShell-like command: 'CustomSecurityAttribute.AppFilters\_caExemption -eq "CAExempt"'.

## 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



# Go-Dos

- Understand your CA policies, make sure Apple users are IN SCOPE



# Go-Dos

- Understand your CA policies, make sure Apple users are IN SCOPE
- Remember, everyone should be doing device compliance



# 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



# 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



# 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



# 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](https://aka.ms/PSSO4MAC)





Thank you for  
listening!

