Unconditionally Conditional

Strong authentication in Microsoft Entra ID (formerly Azure AD)

Don Mallory

whoami

- 30 years in IT, mostly for critical infrastructure
- Healthcare security professional
- Volunteer:
    - Healthcare Infosec Group - Moderator
    - C3X - Builder & Mentor (2018-2020)
    - Hak4Kidz Toronto (2019)
    - B&W Photography Lead (since 2007)

Disclaimer

The thoughts and opinions shared throughout this presentation are mine alone and not those of, past, present, or future employers

Agenda

- Trust & Zero Trust
- Devices & Apps
- Conditional access policies & components
- Model for strong authentication
- Troubleshooting
- Other things that tie in
- Licensing
- Resources & links
- Conclusions

You don’t need to take screenshots or photos

Assumptions

- Authentication is only one part of your defence strategy
- Authentication does not only apply to users
  - Identity applies to devices, applications, services, users
  - Authentication is verification of identity
- Authorization will be mentioned, but not covered in detail

- We will not cover:
  - Everything
    - There will always be more
    - Embrace the rate of change
  - Pricing - that’s between you and your sales rep
  - How long will it take to implement - talk to your CAB

What is trust?

- NIST SP800-161 - A belief that an entity meets certain expectations and therefore, can be relied upon.
- (n) Assured reliance on the character, ability, strength, or truth of someone or something
- (vt) To hope or expect confidently

What is zero trust?

a principle-based **model** designed within a cybersecurity strategy that **enforces** a **data-centric** approach to **continuously treat everything** as an **unknown** - whether a human or a machine, to ensure trustworthy behaviour

This is still all about trust

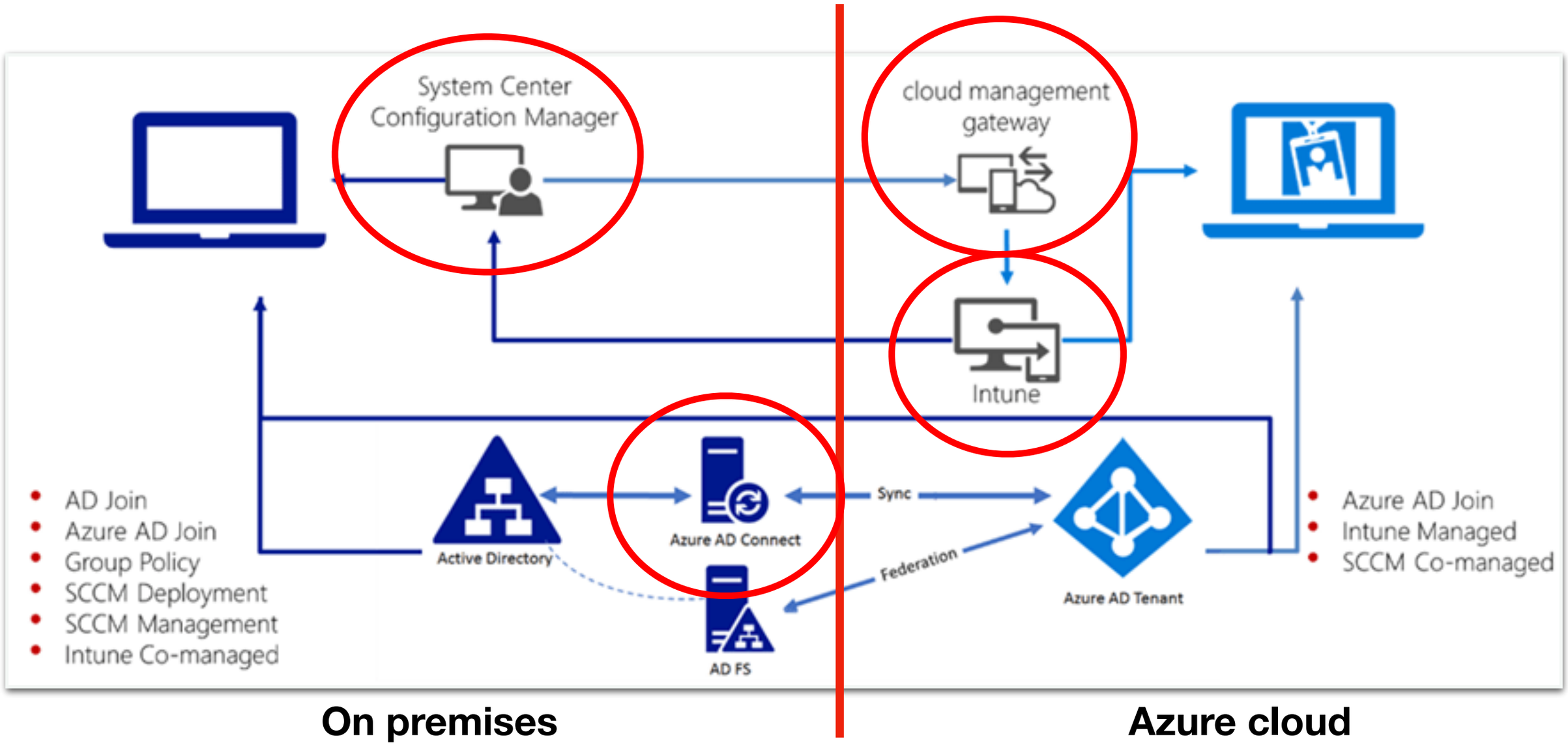
Why should we care?

- Traditional thinking:
  - The physical network boundary is the edge.
  - A firewall will save us!

- Cloud posture:
  - The data is the edge.
  - The client is just a conduit to the data.
  - Authentication is the gateway to your data.

Regulatory, legal, and moral obligation to protect the data of your staff and clients.

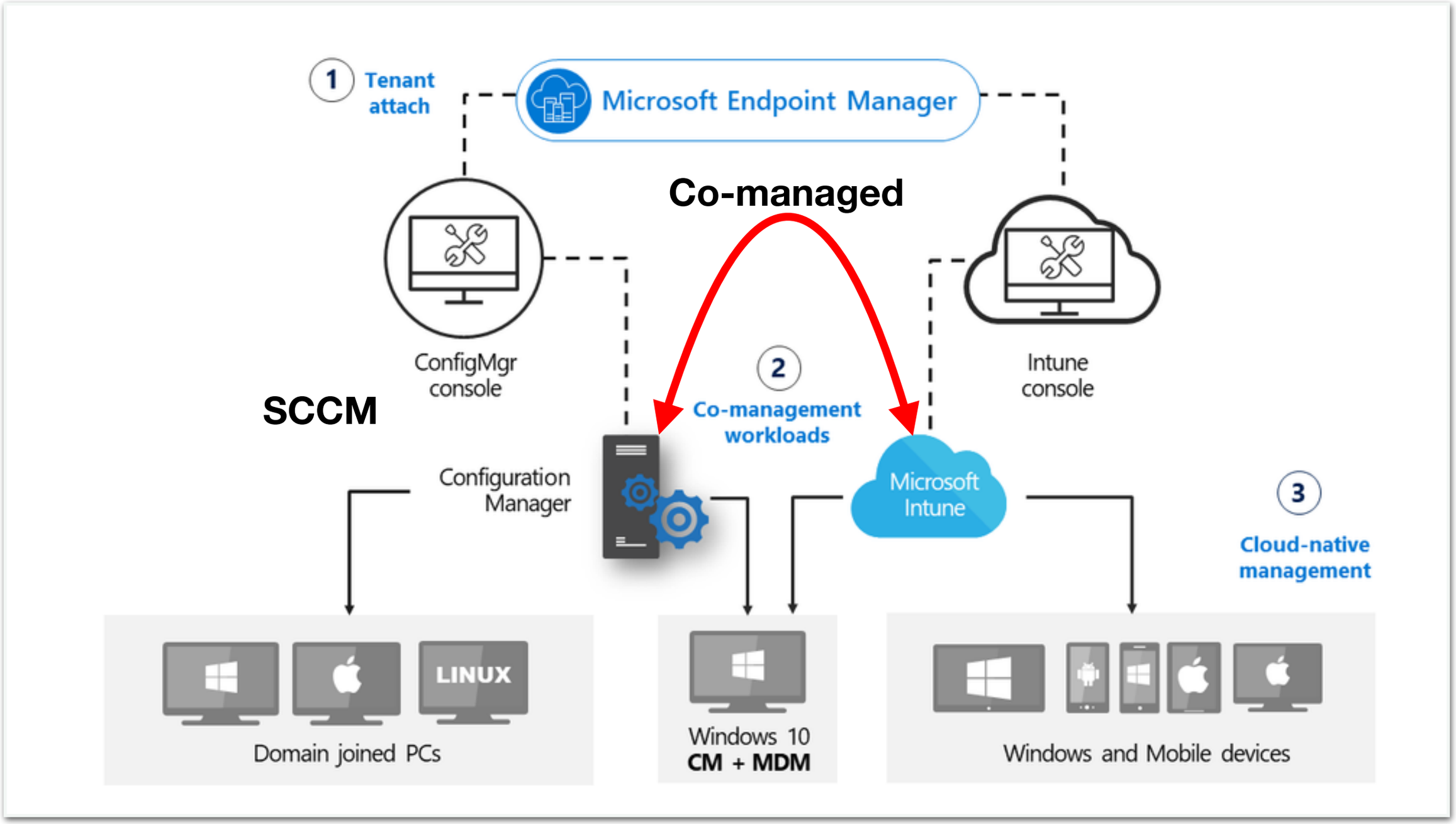
Hybrid management architecture



Note: Microsoft recently renamed “Azure AD”, to “Entra ID”
“Azure joined” = “Entra joined”

https://learn.microsoft.com/en-us/mem/configmgr/core/clients/manage/cmg/overview

Start with devices



AD joined → **Hybrid joined** ← **Azure / Entra joined**

https://learn.microsoft.com/en-us/azure/active-directory/devices/

MDM vs MAM

MDM

- Device focused
- Device config policies
- Device compliance policies
- Device encryption

- Device wipe
- App push
- OS & App updates
- App visibility / limits
- Best for Org owned devices

MAM

- Application focused
- App config policies
- App compliance policies
- App containerization & encryption
- App data wipe
- Users download apps from app store
- Can be layered on top of MDM
- Best for BYOD

https://learn.microsoft.com/en-us/mem/intune/fundamentals/manage-devices
https://learn.microsoft.com/en-us/mem/intune/fundamentals/manage-apps

MDM policies (1)

Home > Devices | Compliance > M365_iOS >

iOS compliance policy

iOS/iPadOS

1 Compliance settings 2 Review + save

Email

Email

Unable to set up email on the device — Require | Not configured

Device Health

Jailbroken devices — Block | Not configured

Require the device to be at or under the Device Threat Level — Not configured

Device Properties

Operating System Version

Minimum OS version — 16.6

Maximum OS version — Not configured

Minimum OS build version — Not configured

Maximum OS build version — Not configured

Microsoft Defender for Endpoint

Microsoft Defender for Endpoint rules

Require the device to be at or under the machine risk score: — Not configured

System Security

iOS compliance policy

iOS/iPadOS

System Security

All enrollment types

These settings work for devices that were enrolled in Intune through device enrollment or user enrollment, and for devices enrolled using Apple School Manager or Apple Business Manager with automated device enrollment (formerly DEP).

Requiring a password automatically enforces a non-simple, 6-digit PIN requirement on all user enrolled devices, regardless of what you configure for those settings.

Password

Require a password to unlock mobile devices — Require | Not configured

Device enrollment and automated device enrollment

These settings work for devices that were enrolled in Intune through device enrollment, and for devices enrolled using Apple School Manager or Apple Business Manager with automated device enrollment (formerly DEP).

Simple passwords — Block | Not configured

Minimum password length — 6

Required password type — Numeric

Number of non-alphanumeric characters in password — Not configured

Maximum minutes after screen lock before password is required — Immediately

Maximum minutes of inactivity until screen locks — 5 minutes

Password expiration (days) — Enter number of days (1-730)

Number of previous passwords to prevent reuse — Enter a number (1-24)

https://learn.microsoft.com/en-us/mem/intune/protect/device-compliance-get-started#compliance-policy-settings
https://learn.microsoft.com/en-us/mem/intune/protect/compliance-policy-create-ios

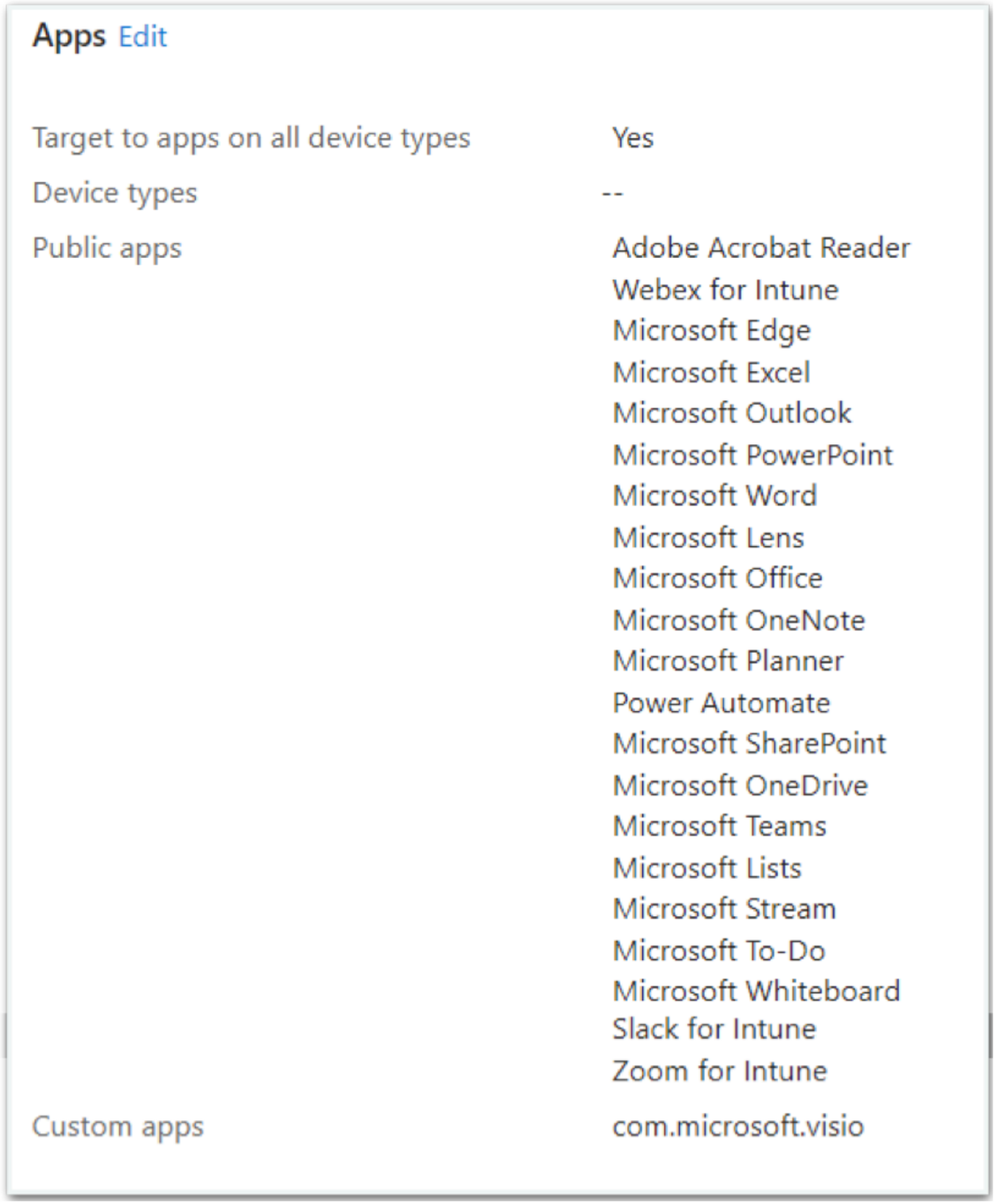
MDM policies (2)

Actions for noncompliance Edit

Action	Schedule	Message template	Additional recipients (via email)
Mark device noncompliant	Immediately		None selected
Send push notification to end user	Immediately		None selected
Send email to end user	Immediately	Selected	1 Selected
Send email to end user	10 Days	Selected	1 Selected
Remotely lock the noncompliant device	15 Days		None selected
Add device to retire list	30 Days		None selected

https://learn.microsoft.com/en-us/mem/intune/protect/actions-for-noncompliance

MAM policies (1)



- Protected apps run in a container
- Not all apps are protected equally
- Notice special app versions
- Data outside the container is managed by MDM for enrolled devices

https://learn.microsoft.com/en-us/mem/intune/apps/apps-supported-intune-apps

MAM policies (2)

Home > Apps | App protection policies > Intune App Protection | Properties >

Edit policy

M365_IOS_Protection

Data Transfer

Backup org data to iTunes and iCloud backups	Allow / **Block**
Send org data to other apps	Policy managed apps with Open-In/Share filtering
Select apps to exempt	Select
Select universal links to exempt	Select
Select managed universal links	Select
Save copies of org data	Allow / **Block**
Allow user to save copies to selected services	OneDrive for Business
Transfer telecommunication data to	Any dialer app
Dialer App URL Scheme	
Receive data from other apps	Policy managed apps
Open data into Org documents	**Allow** / Block
Allow users to open data from selected services	4 selected
Restrict cut, copy, and paste between other apps	Policy managed apps with paste in
Cut and copy character limit for any app *	0
Third party keyboards	Allow / **Block**

⚠ Keyboard restrictions will apply to all areas of an app. Personal accounts for apps that support multiple identities will be affected by this restriction. Learn more.

Encryption

Encrypt org data	**Require** / Not required

Functionality

Sync policy managed app data with native apps or add-ins	Allow / **Block**
Printing org data	Allow / **Block**
Restrict web content transfer with other apps	Any app
Unmanaged browser protocol	
Org data notifications	Allow

Home > Apps | App protection policies > Intune App Protection | Properties >

Edit policy

M365_IOS_Protection

1 Access requirements 2 Review + save

Configure the PIN and credential requirements that users must meet to access apps in a work context.

PIN for access	**Require** / Not required
PIN type	**Numeric** / Passcode
Simple PIN	**Allow** / Block
Select minimum PIN length	6
Touch ID instead of PIN for access (iOS 8+/iPadOS)	**Allow** / Block
Override biometrics with PIN after timeout	Require / **Not required**
Timeout (minutes of inactivity)	0
Face ID instead of PIN for access (iOS 11+/iPadOS)	**Allow** / Block
PIN reset after number of days	Yes / **No**
Number of days	0
App PIN when device PIN is set	Require / **Not required**
Work or school account credentials for access	Require / **Not required**
Recheck the access requirements after (minutes of inactivity) *	7200

MAM policies (3)

Home > Apps | App protection policies > Intune App Protection | Properties >

Edit policy

M365_Android_Protection

1 Conditional launch 2 Review + save

Set the sign-in security requirements for your access protection policy. Select a **Setting** and enter the **Value** that users must meet to sign in to your company app. Then select the **Action** you want to take if users do not meet your requirements. In some cases, multiple actions can be configured for a single setting. Learn more about conditional launch actions.

App conditions

Setting	Value	Action
Max PIN attempts	5	Reset PIN
Offline grace period	4320	Block access (minutes)
Offline grace period	90	Wipe data (days)
Disabled account		Block access
Select one		

Device conditions

Configure the following conditional launch settings for device based conditions through your app protection policy.

Similar device based settings can be configured for enrolled devices. Learn more about configuring device compliance settings for enrolled devices.

Setting	Value	Action
Jailbroken/rooted devices		Block access
Min OS version	12.0	Warn
Min OS version	11.0	Block access
SafetyNet device attestation	Basic integrity and certified devices	Block access
Select one		

Home > Apps | App protection policies > Intune App Protection | Properties >

Edit policy

Test_Outlook_Protection_iOS

App conditions

Setting	Value	Action
Max PIN attempts	5	Reset PIN
Offline grace period	720	Block access (minutes)
Offline grace period	90	Wipe data (days)
Disabled account		Wipe data
Select one		

Device conditions

Configure the following conditional launch settings for device based conditions through your app protection policy.

Similar device based settings can be configured for enrolled devices. Learn more about configuring device compliance settings for enrolled devices.

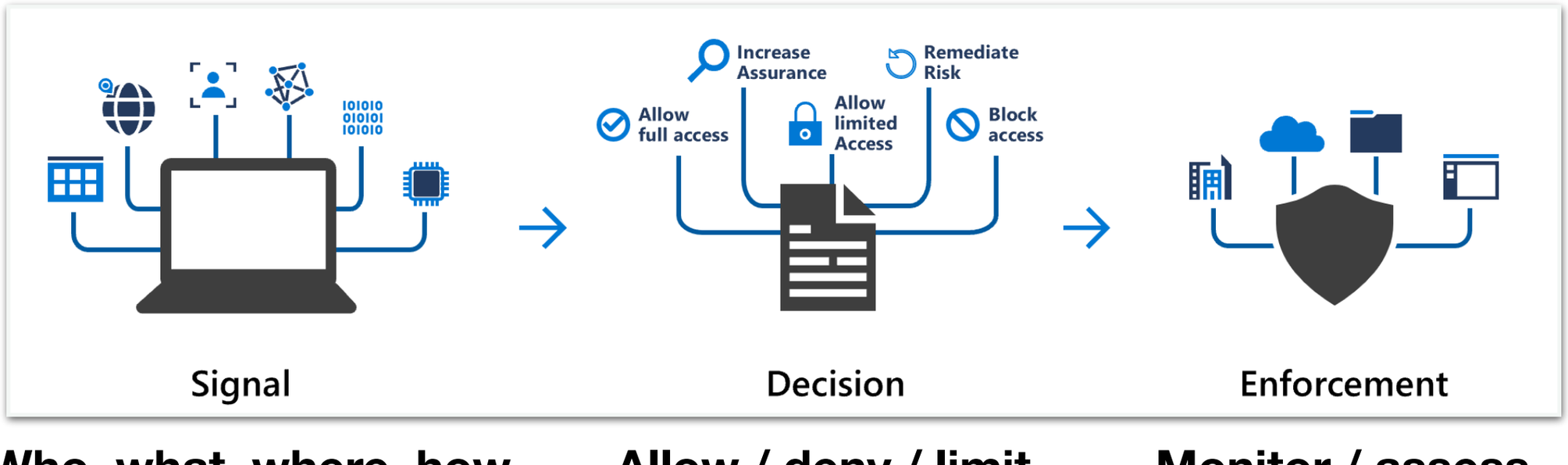
Setting	Value	Action
Jailbroken/rooted devices		Block access
Min OS version	16.6.1	Warn
Min OS version	16.4	Block access
Min OS version	16.3	Wipe data

https://learn.microsoft.com/en-us/mem/intune/fundamentals/deployment-guide-enrollment-mamwe

Some of Intune’s Limitations

- Privacy / troubleshooting of MAM compliance.
- Policy reports / compliance are inconsistent
  - Best report is per feature non-compliance
- ConfigMgr policy mgmt is going away in Q1 2024
- Hybrid joined and co-managed is tricky and takes time
  - Make sure GPO and ADFS are operating properly
  - Work closely with your SCCM team
  - ConfigMgr client must be up to date and pushed
  - CMG has a cost if you push apps from on prem to remote users
- Policy filters are an art
- iOS & Mac - Device Enrolment Program (DEP) required for best management

Conditional access

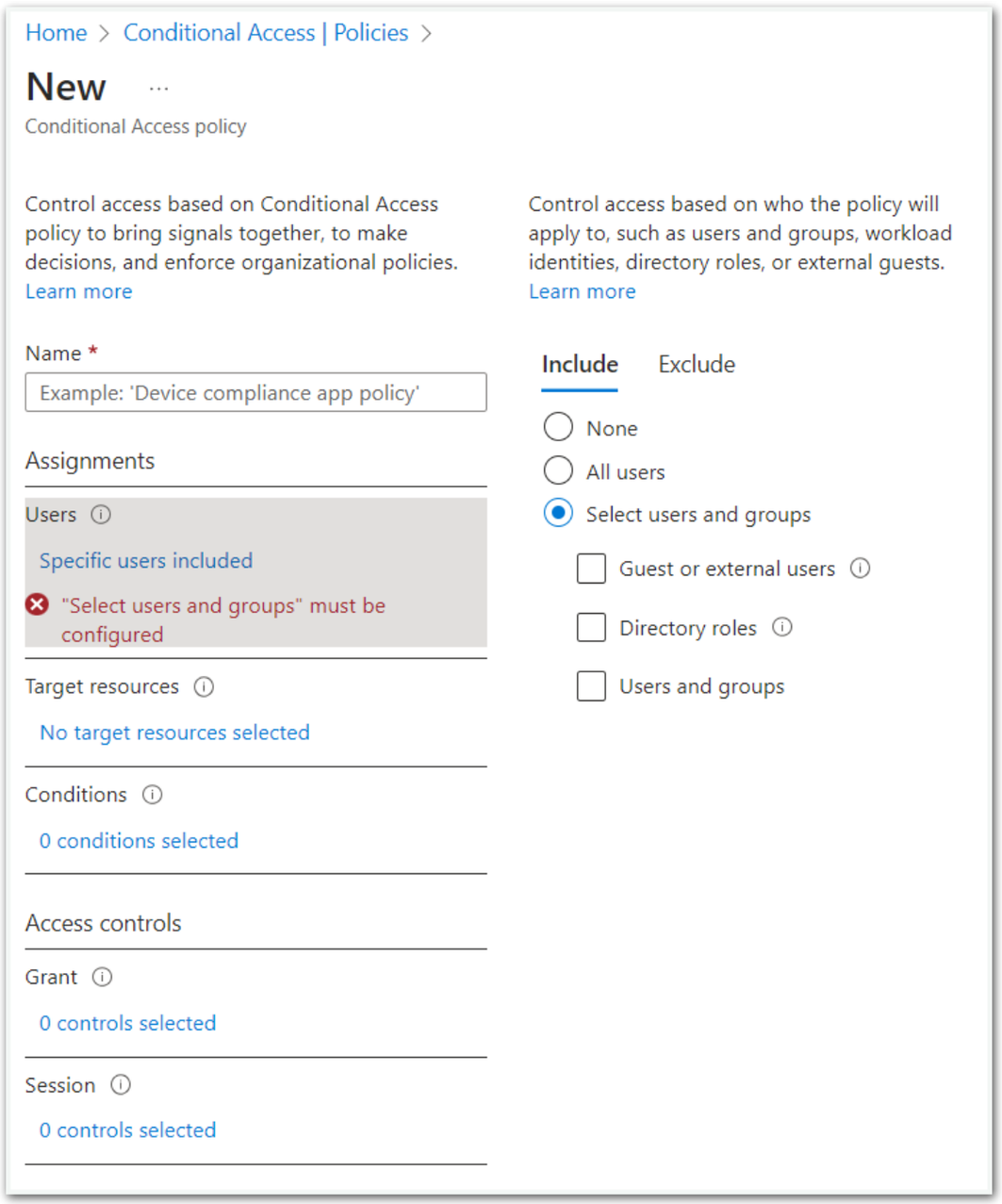


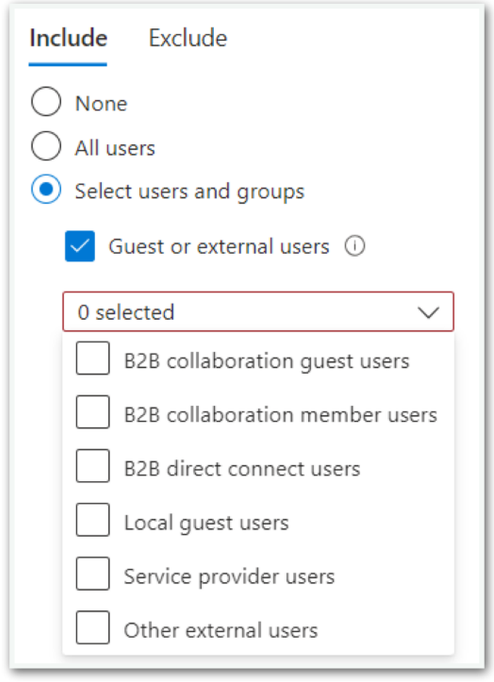
- Conditional Access allows you to layer controls around your data based on signals that you define.
  - Central to a data centric security strategy.

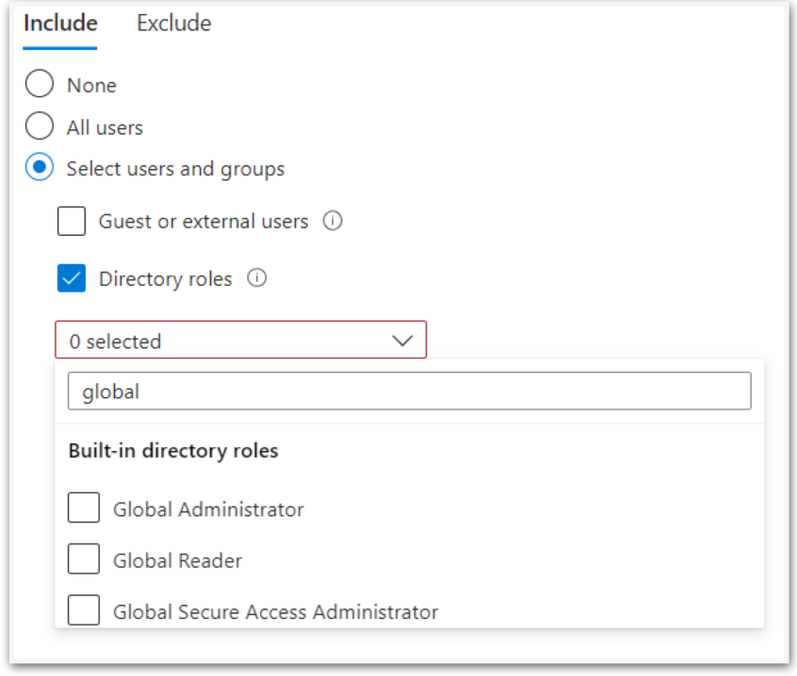
- “Just-in-time” evaluation to ensure that the person who is seeking access to content is authorized to access the content.

https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/overview

CA Policies - Users

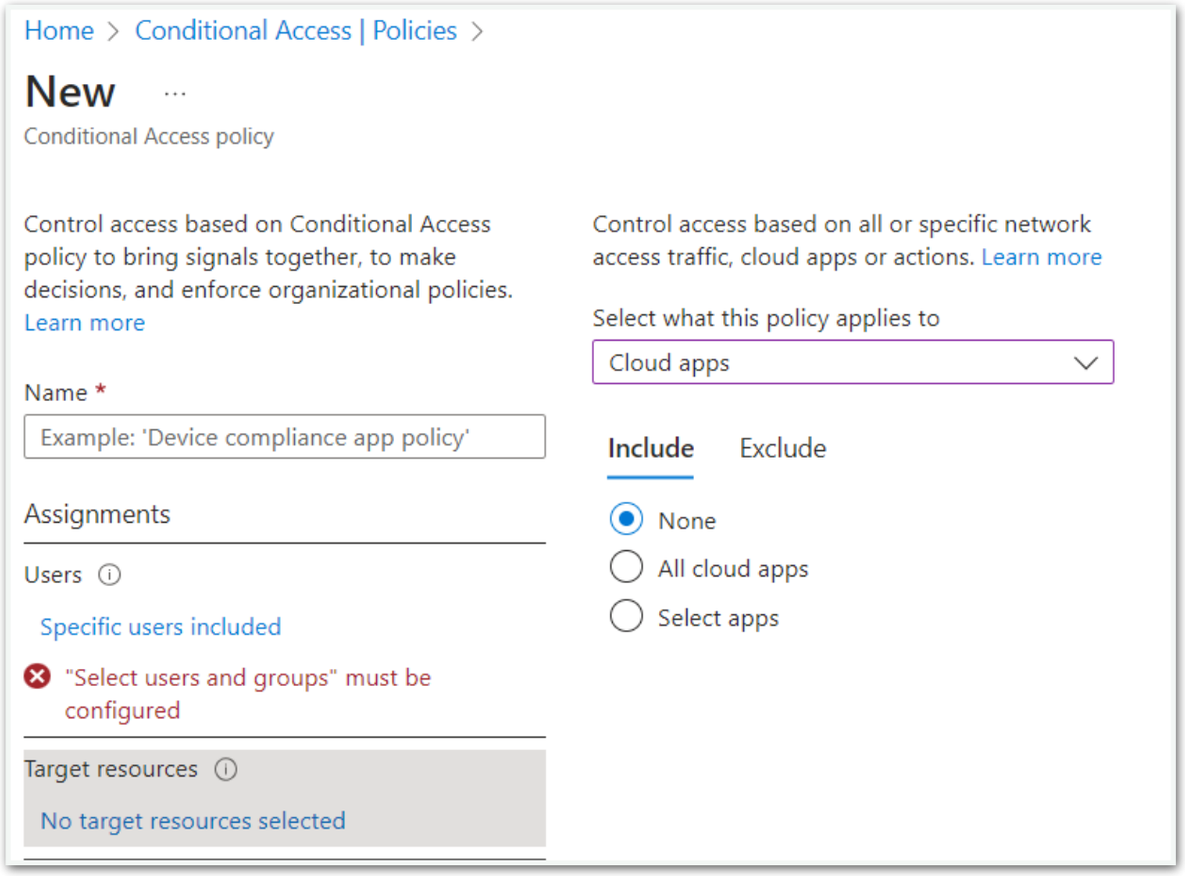


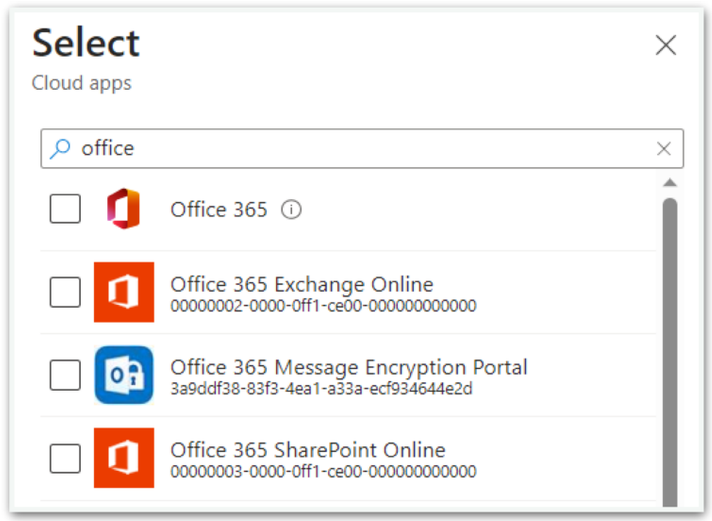


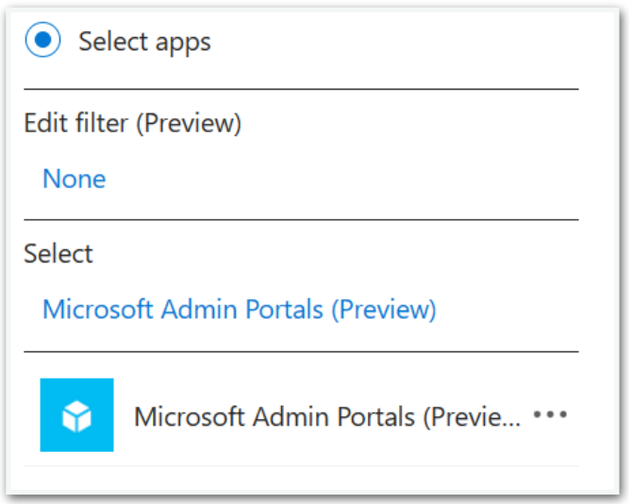


https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-users-groups

CA Policies - Target Resource - Apps

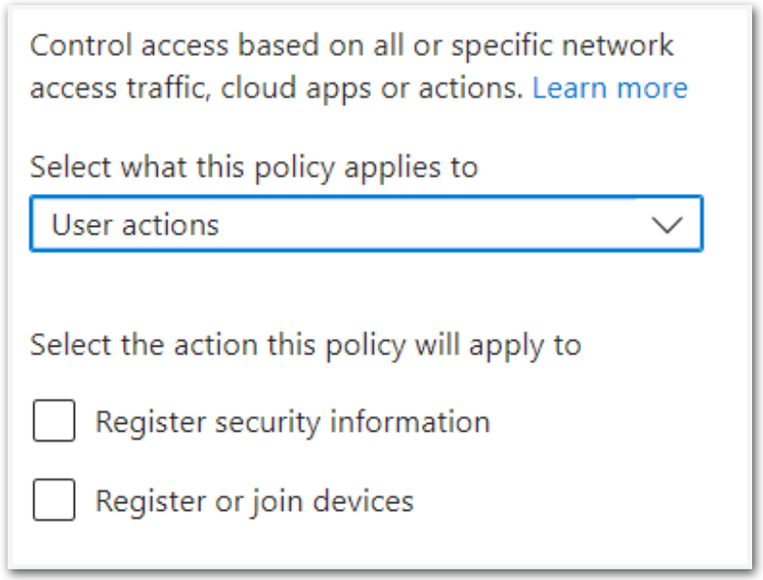


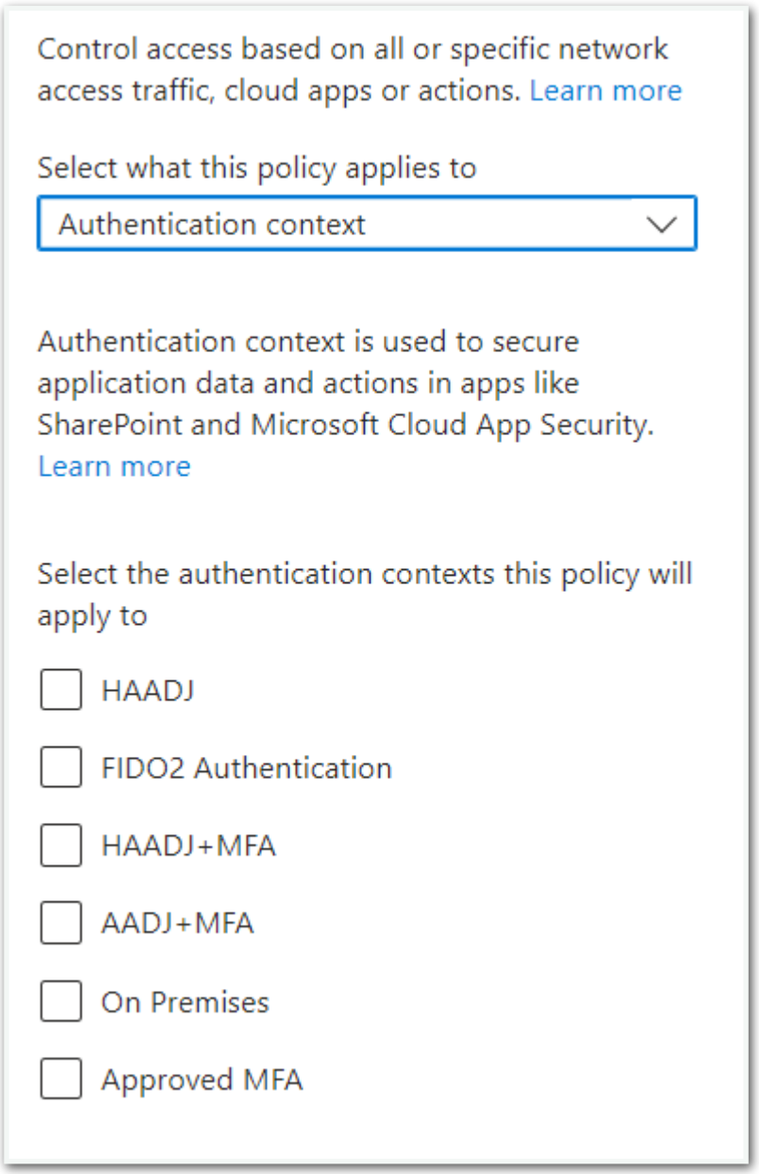


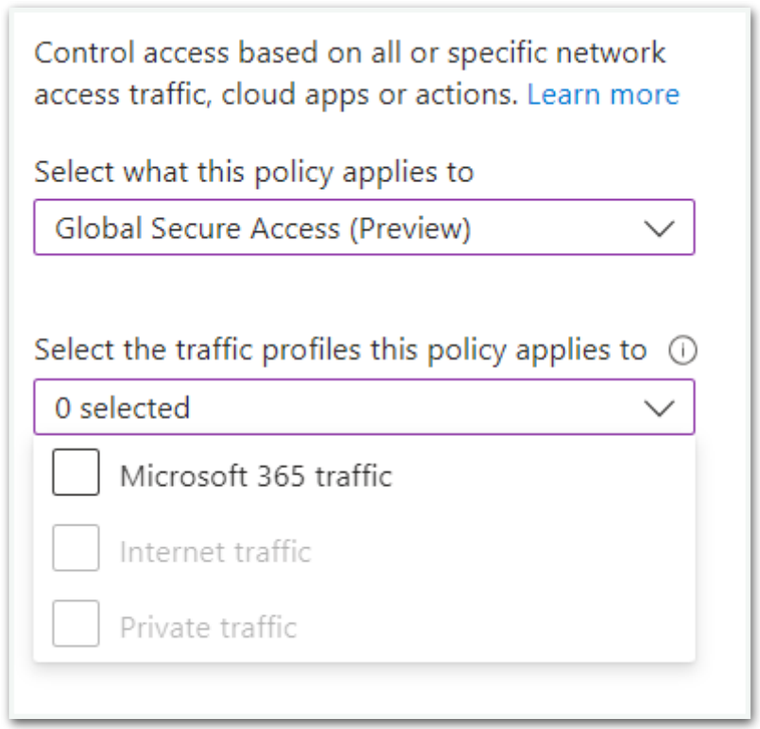


https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-cloud-apps
https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-cloud-apps#microsoft-cloud-applications

CA Policies - Target Resource - Actions







https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-cloud-apps

CA Policies - Conditions

Control access based on signals from conditions like risk, device platform, location, client apps, or device state. Learn more

User risk
Not configured

Sign-in risk
Not configured

Device platforms
Not configured

Locations
Not configured

Client apps
Not configured

Filter for devices
Not configured

User risk

Configure
Yes No

Configure user risk levels needed for policy to be enforced

- [ ] High
- [ ] Medium
- [ ] Low

Sign-in risk

Control user access to respond to specific sign-in risk levels. Learn more

Configure
Yes No

Sign-in risk level is generated based on all real-time risk detections.

Select the sign-in risk level this policy will apply to

- [ ] High
- [ ] Medium
- [ ] Low
- [ ] No risk

Device platforms

Apply policy to selected device platforms. Learn more

Configure
Yes No

Include Exclude

- ( ) Any device
- ( ) Select device platforms
  - [ ] Android
  - [ ] iOS
  - [ ] Windows Phone
  - [ ] Windows
  - [ ] macOS
  - [ ] Linux

Client apps

Control user access to target specific client applications not using modern authentication. Learn more

Configure
Yes No

Select the client apps this policy will apply to

Modern authentication clients

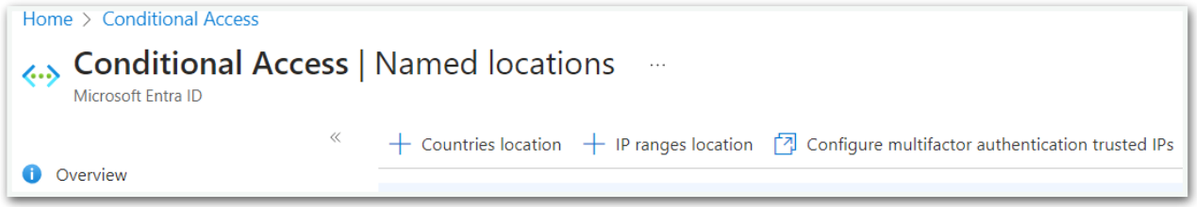
- [ ] Browser
- [ ] Mobile apps and desktop clients

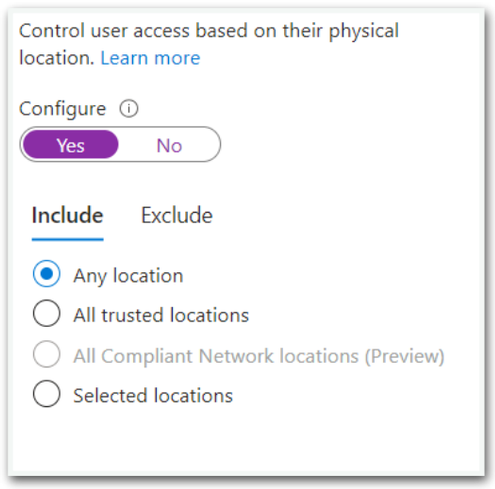
Legacy authentication clients

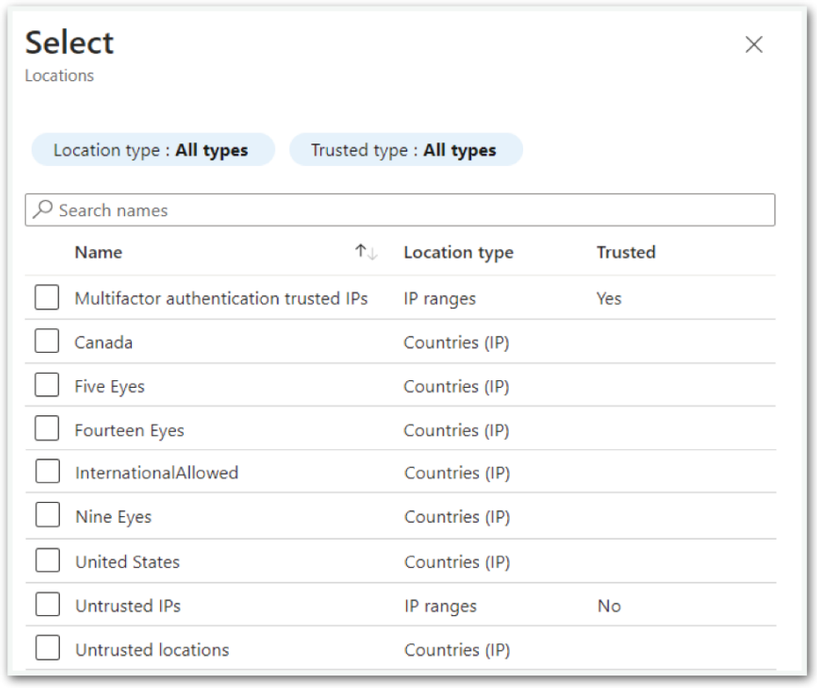
- [ ] Exchange ActiveSync clients
- [ ] Other clients

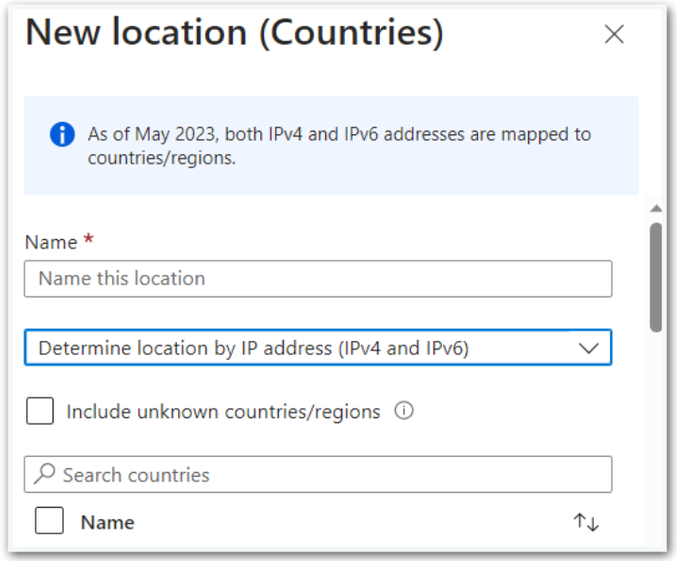
https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-conditions

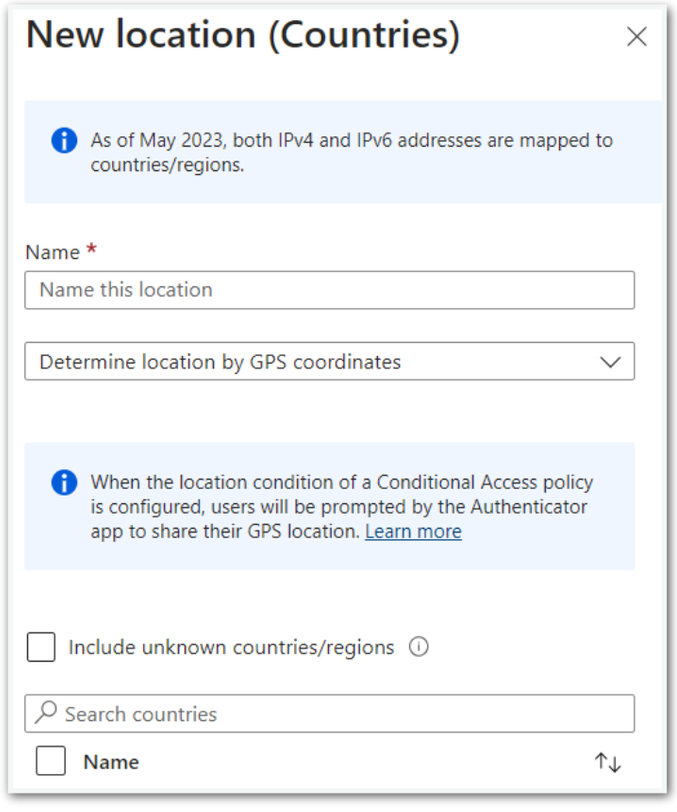
CA Policies - Conditions - Locations











https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition

CA Policies - Conditions - Device Filters

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
	trustType	Equals	Micros
Or	TrustType	Equals	Hybri
And	deviceOwnership	Equals	Comp
And	isCompliant	Equals	True

+ Add expression

Rule syntax ⓘ

```
device.trustType -eq "AzureAD" -or device.trustType -eq "ServerAD" -and device.d
-eq True
```

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
	<Choose a property>	<Choose an ope...	<Pick a property and operator first>

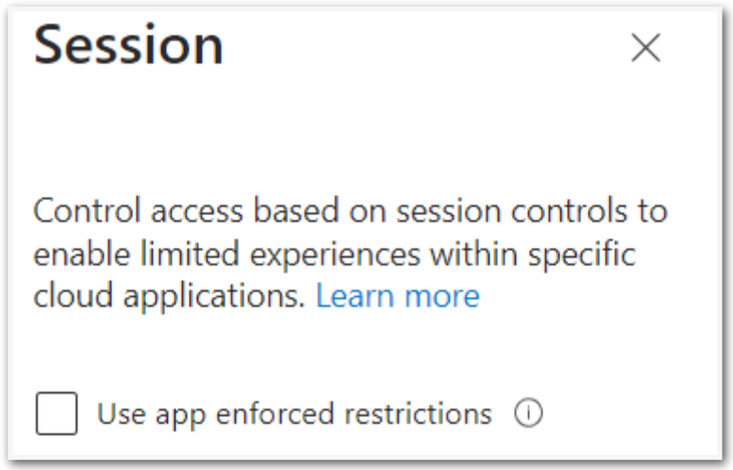
+ Add expression

Rule syntax ⓘ Apply

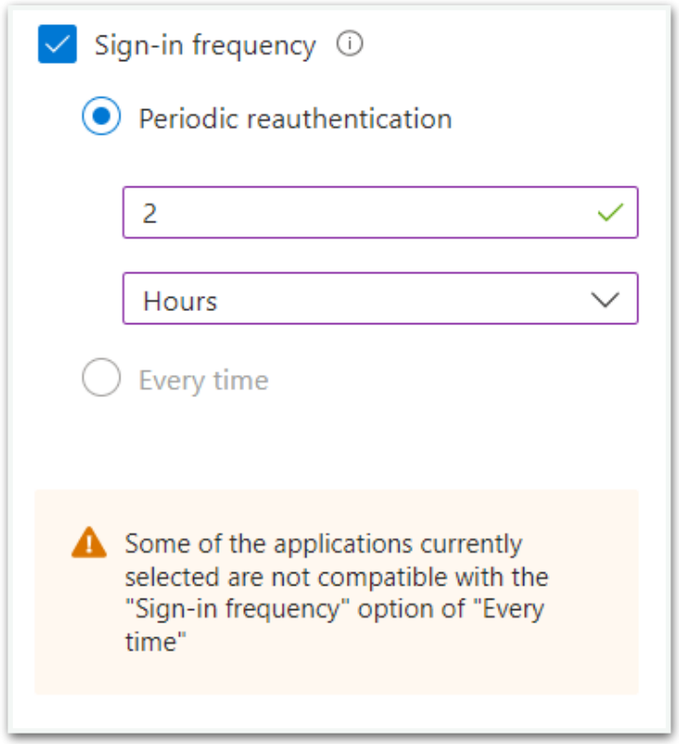
```
( device.trustType -eq "AzureAD" -or device.trustType -eq "ServerAD" ) -and device.deviceOwnership -eq "Company" -and
device.isCompliant -eq True
```

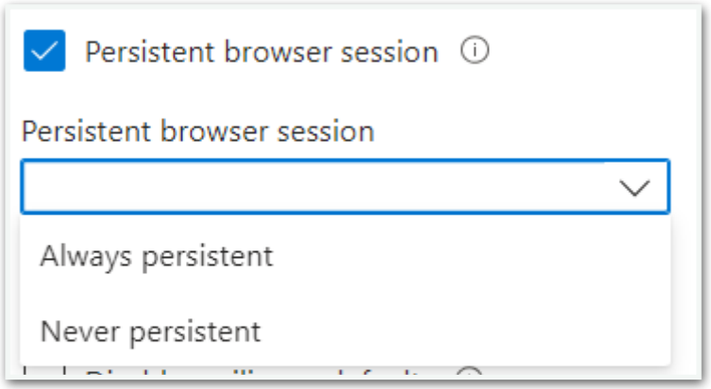
https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/concept-condition-filters-for-devices

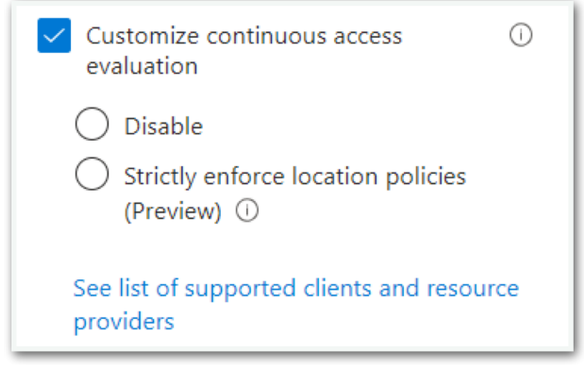
CA Policies - Session Controls

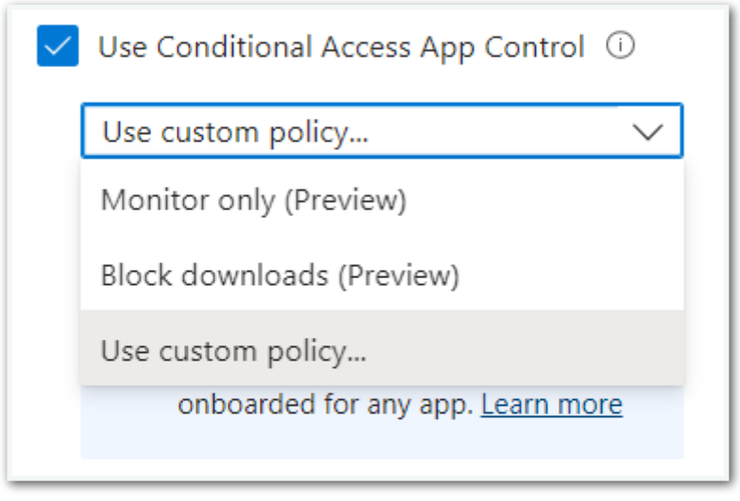


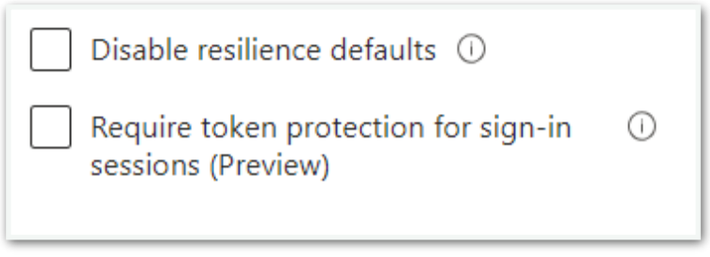
Only supports O365, EXO, SPO





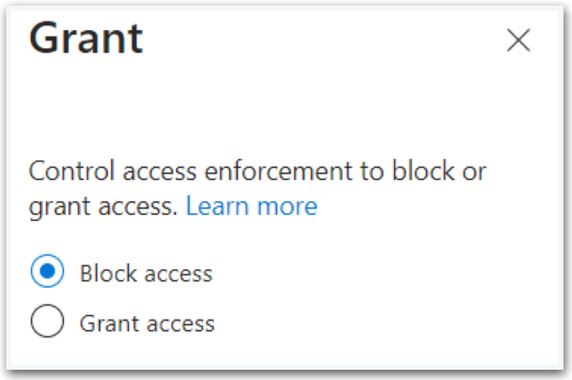


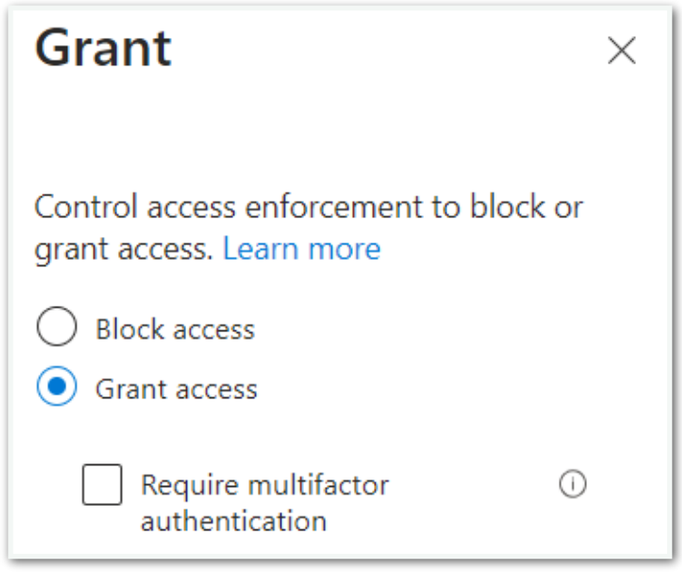


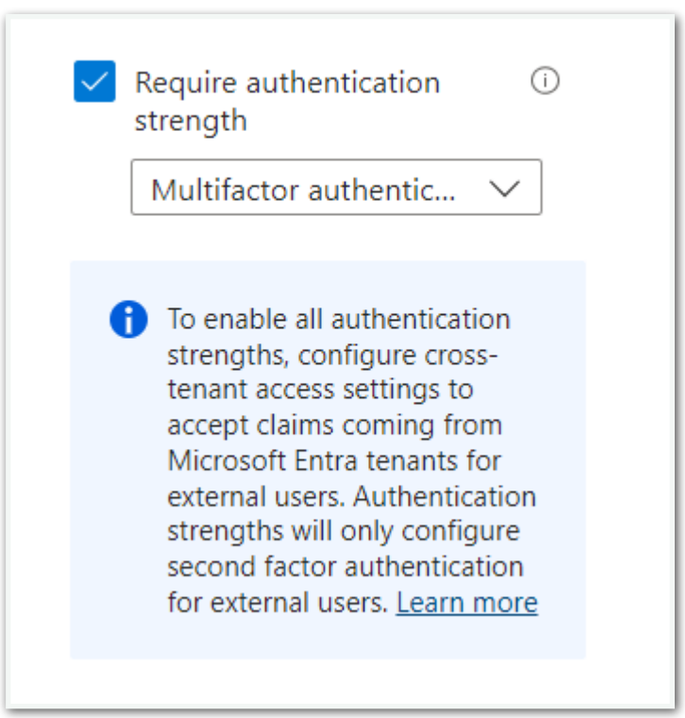


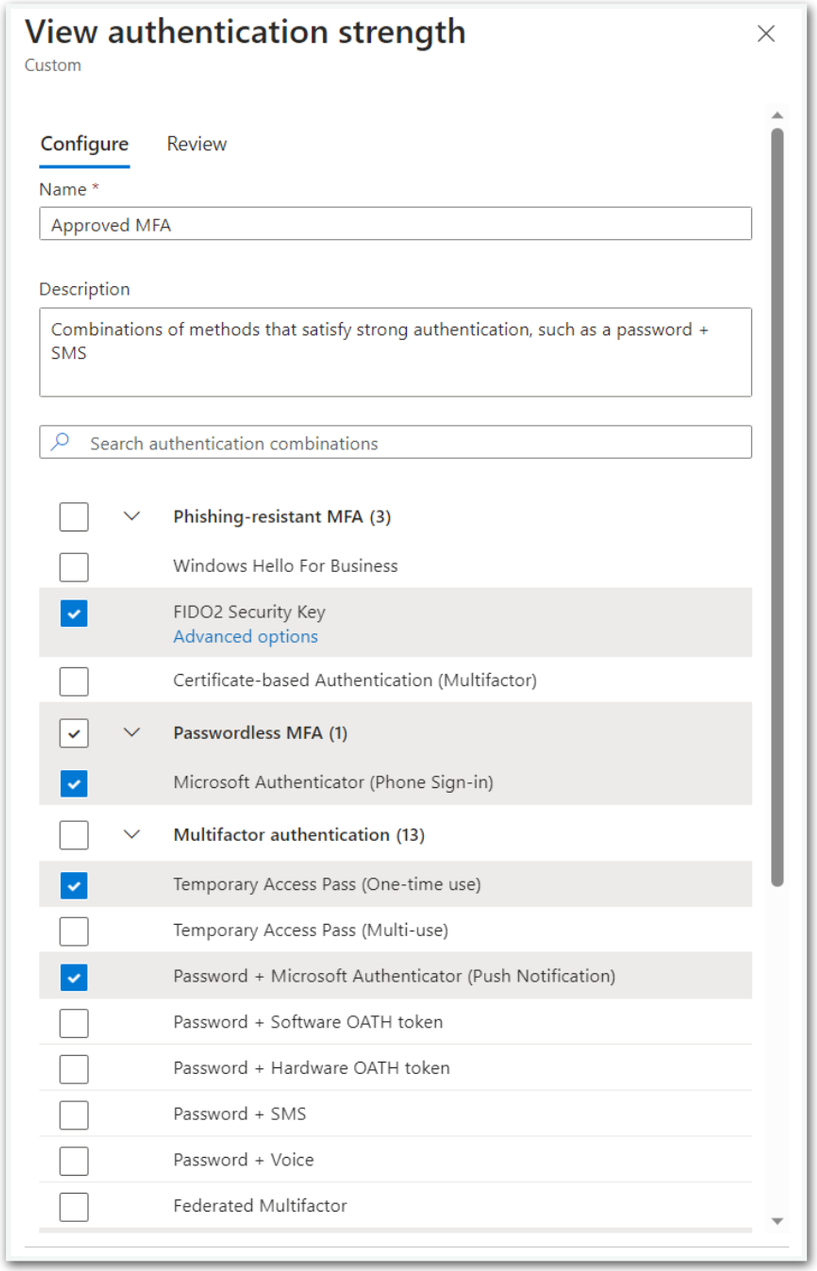
https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-session
https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/concept-continuous-access-evaluation
https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/concept-token-protection

CA Policies - Controls - Block/Grant



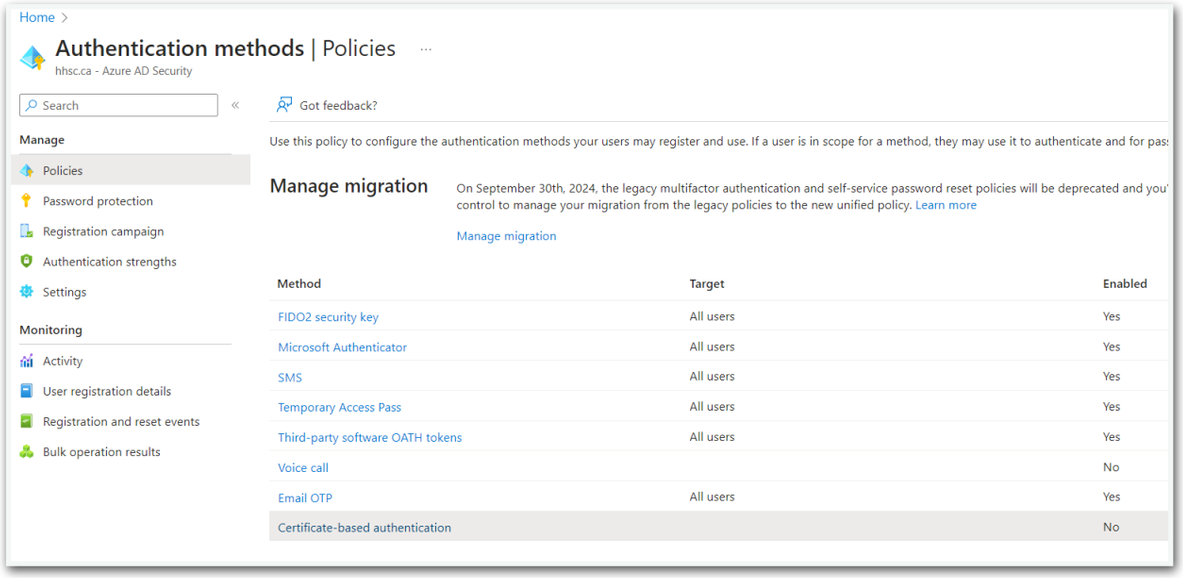


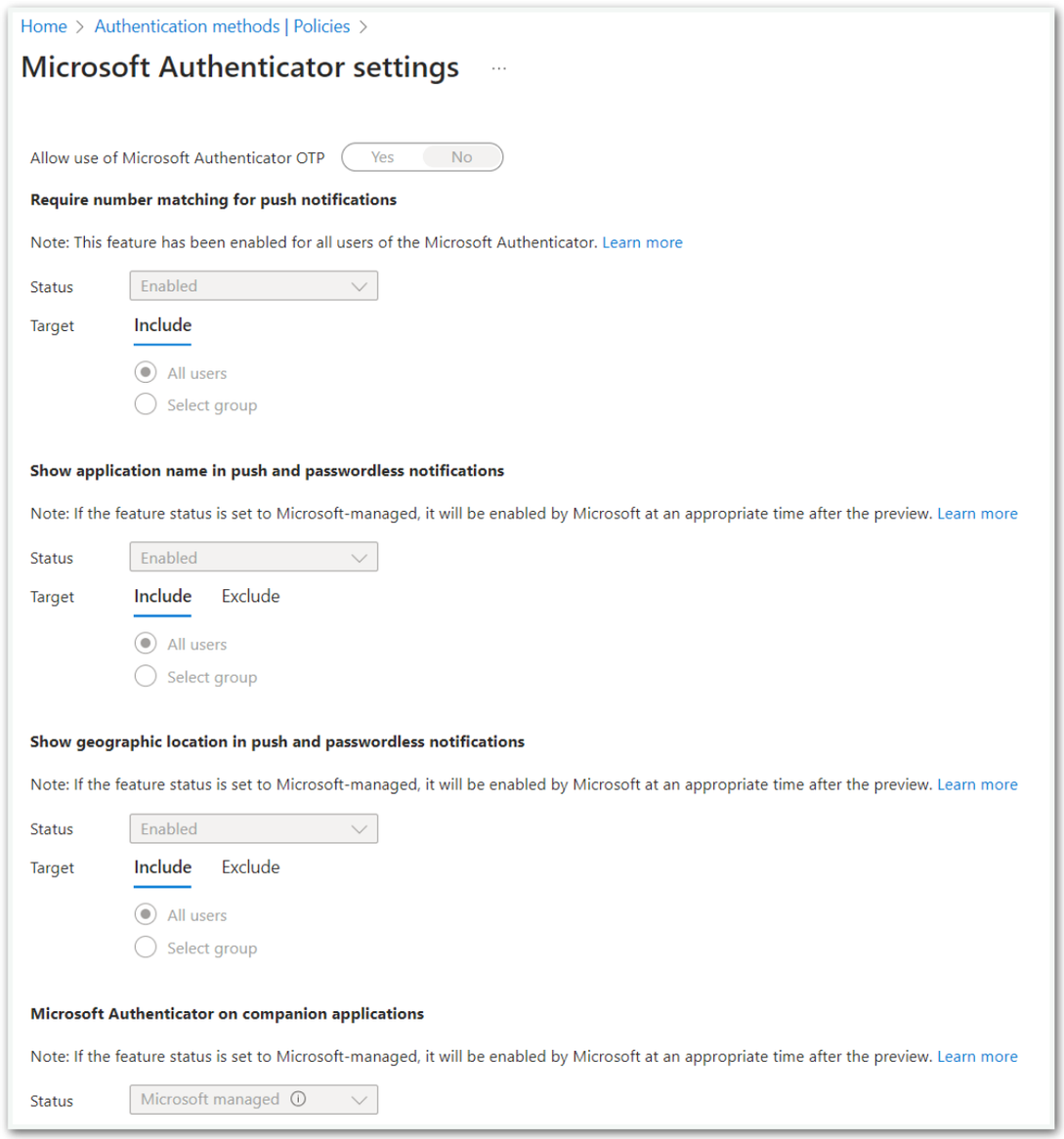


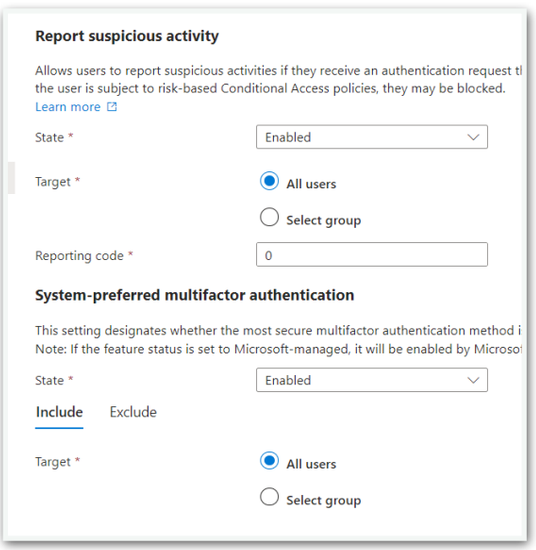


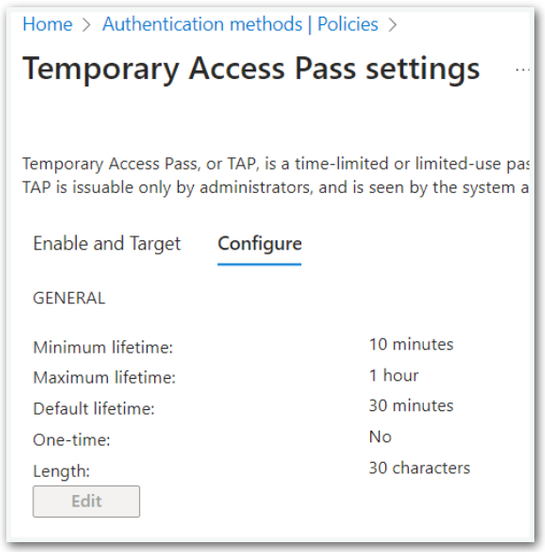
https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-grant

Sidebar - Authentication Methods



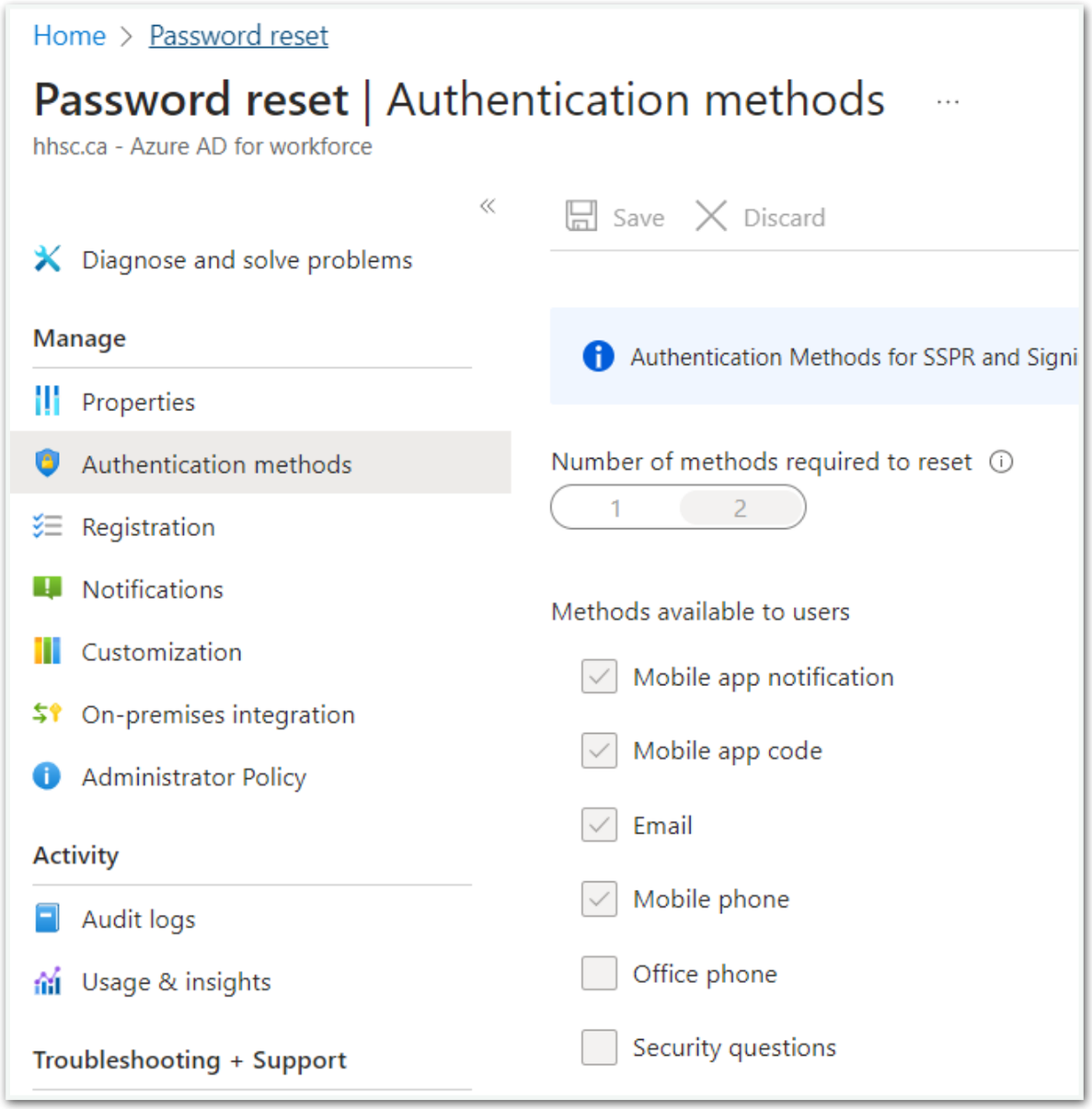




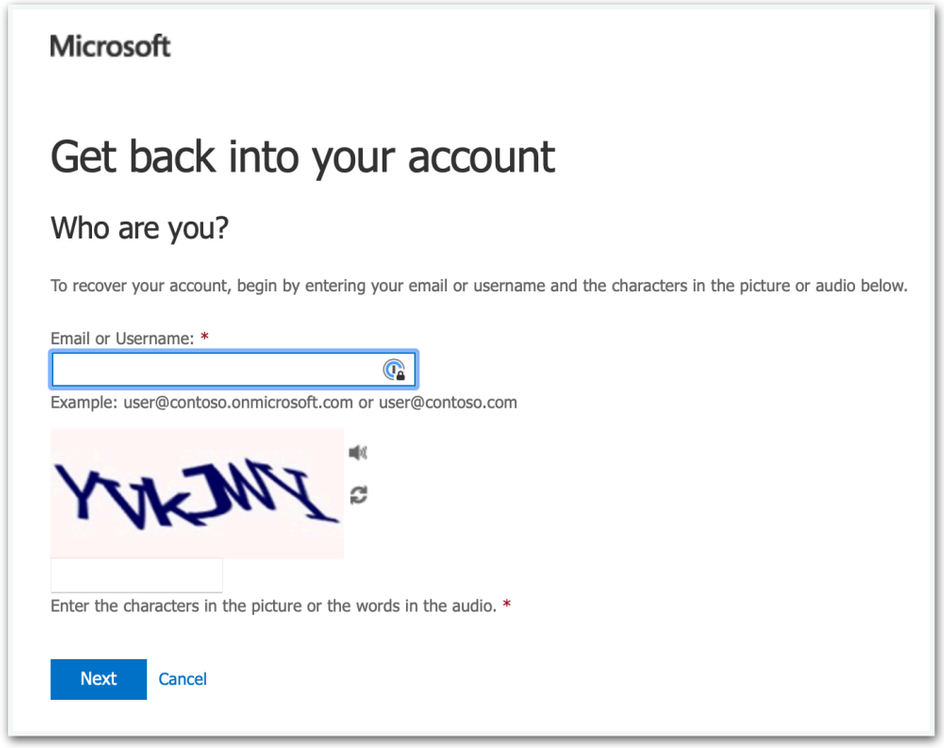


https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-methods

Sidebar - Self-Service Password Reset



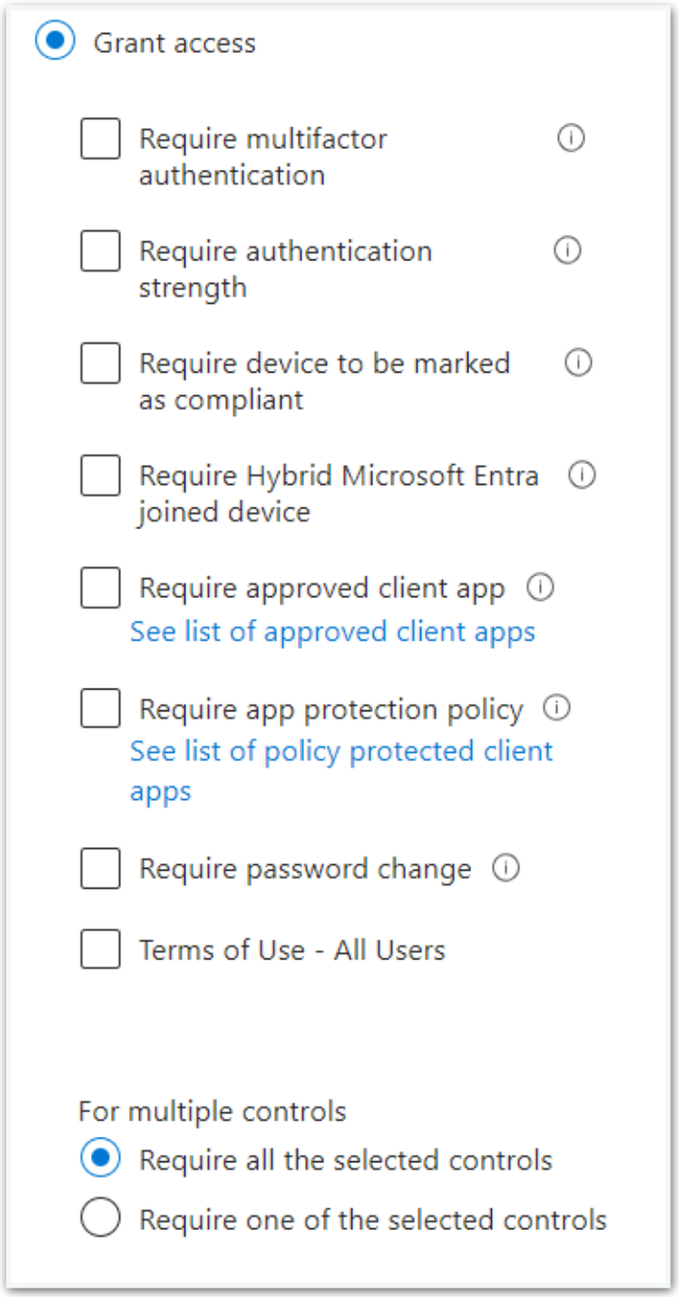
https://aka.ms/sspr



- AD write-back must be enabled on your AD (MIM) Sync server
- This also enables password strength verification, and stores hashed hashes in the US

https://learn.microsoft.com/en-us/microsoft-identity-manager/working-with-self-service-password-reset
https://learn.microsoft.com/en-us/azure/active-directory/hybrid/connect/how-to-connect-password-hash-synchronization#how-password-hash-synchronization-works

CA Policies - Controls - Grant



- Deprecated controls:
  - Require mulitfactor auth
  - Require approved client app
- Device compliance = MDM
  - Requires Entra join
- App protection policy = MAM
- Terms of Use

https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-grant

CA Policies - Limitations

Register or join devices

Only "Require multifactor authentication" can be used in policies created for the "Register or join devices" user action. Learn more

Persistent browser session

Persistent browser session

Persistent browser session only works correctly when All cloud apps is selected. Please change your cloud apps selection. Learn more

Use Conditional Access App Control

Block downloads (Preview)

This control works instantly for featured apps and can be self onboarded for any app. Learn more

Sign-in frequency

Periodic reauthentication

0

Select units

Every time

Some of the applications currently selected are not compatible with the "Sign-in frequency" option of "Every time"

Require password change

"Require password change" can only be used when policy is assigned to "All cloud apps". Learn more

Require token protection for sign-in sessions (Preview)

The control "Require token protection for sign-in sessions" only works with supported devices and applications (Exchange Online and SharePoint). Unsupported devices and client applications will be blocked. Learn more

Use Conditional Access App Control

Use custom policy...

Custom policies need to be configured in Cloud App Security portal. This control works instantly for featured apps and can be self onboarded for any app. Learn more

Sign-in frequency

Periodic reauthentication

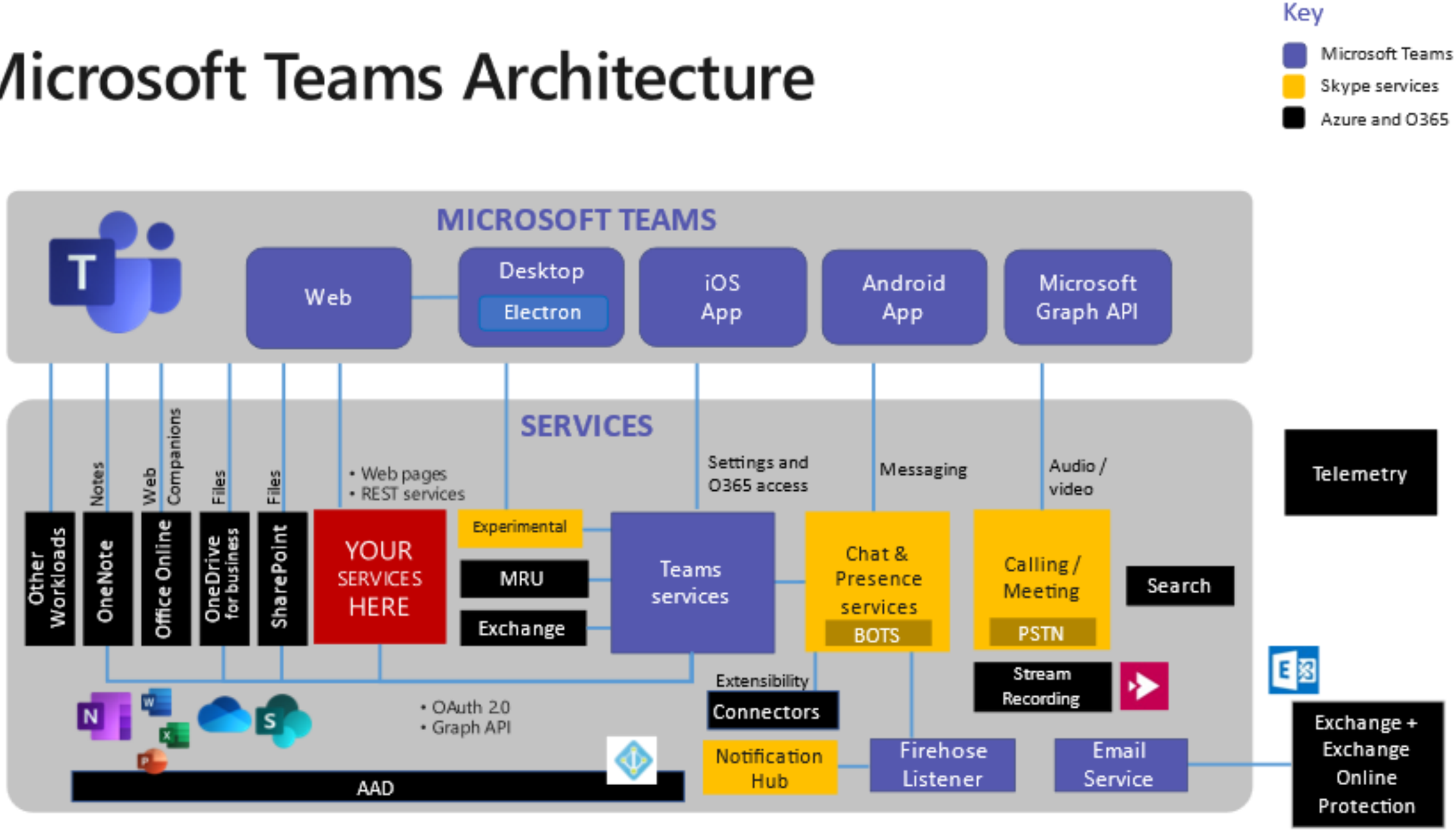
Every time

Require approved client app

See list of approved client apps

You should no longer use "Require approved client app", as we will soon stop updating it. Learn more

Microsoft Teams Architecture



https://devblogs.microsoft.com/microsoft365dev/microsoft-teams-development-all-you-need-to-know/

CA Policies - Deployment

Require compliant or hybrid Azure AD joined device for admins

Require privileged administrators to only access resources when using a compliant or hybrid Azure AD joined device.
Learn more

View | Download JSON file

Block access for unknown or unsupported device platform

Users will be blocked from accessing company resources when the device type is unknown or unsupported.
Learn more

View | Download JSON file

No persistent browser session

Protect user access on unmanaged devices by preventing browser sessions from remaining signed in after the browser is closed and setting a sign-in frequency to 1 hour.
Learn more

View | Download JSON file

Require approved client apps or app protection policies

To prevent data loss, organizations can restrict access to approved modern auth client apps with Intune app protection policies.
Learn more

View | Download JSON file

Require compliant or hybrid Azure AD joined device or multifactor authentication for all users

Protect access to company resources by requiring users to use a managed device or perform multifactor authentication.
Learn more

View | Download JSON file

Use application enforced restrictions for O365 apps

Block or limit access to O365 apps, including SharePoint Online, OneDrive, and Exchange Online content. This policy requires SharePoint admin center configuration.
Learn more

View | Download JSON file

Require phishing-resistant multifactor authentication for admins

Require phishing-resistant multifactor authentication for privileged administrative accounts to reduce risk of compromise and phishing attacks. This policy requires admins to have at least one phishing resistant authentication method registered.
Learn more

View | Download JSON file

Require multifactor authentication for Microsoft admin portals (Preview)

Use this template to protect sign-ins to admin portals if you are unable to use the "Require MFA for admins" template.
(Preview)
Learn more

View | Download JSON file

Show less

https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-policy-common?tabs=secure-foundation#conditional-access-templates
https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-apis
https://github.com/Azure-Samples/azure-ad-conditional-access-apis/tree/main/01-configure/powershell

Is everybody with me so far?

Putting it all together

- Exclusion vs Inclusion
  - Very important for block and layered policies
- Wide policies work well for session settings
- Narrow policies
  - Ease of troubleshooting
  - Target specific issues
- OS specific policies
  - What is your typical user base?
  - If it shouldn’t be there, don’t allow it
- Browser only vs App policies
  - Some settings don't work on one or the other.
  - Consider where your users will be working
- Trusted vs untrusted devices, locations, user types
- Interesting special cases
  - Device enrolment, security info registration, admin users
  - Things that should never happen, but seem to all the time.

Define some locations

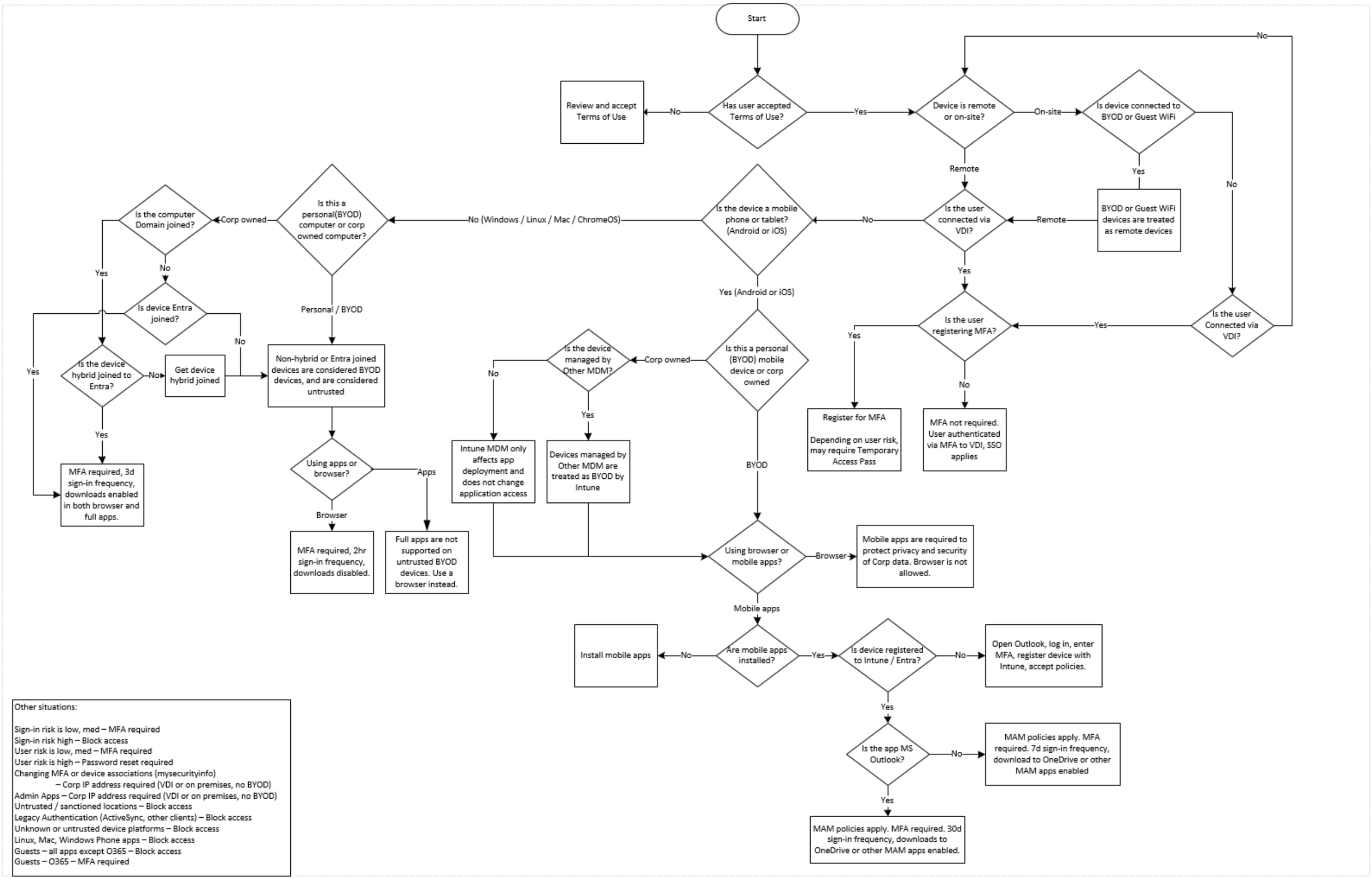
Name	Address range	Country
Corp	192.168.0.0/16, 172.16.0.0/12, 10.0.0.0/8	
PAW	192.168.42.0/24	
Canada		Canada
US		US
Five Eyes		Canada, US, UK, Australia, New Zealand
Nine Eyes		Five Eyes + Denmark, France, Netherlands, Norway
Fourteen Eyes		Nine Eyes + Belgium, Germany, Italy, Spain, Sweden
Untrusted (IP)	IOC list	
Untrusted (Geo)		Start with gc.ca sanction list
Allowed International		Fourteen Eyes + other approved countries

- Corp - Internal network range
- PAW - Privileged Access Workstations - Admin network
- Regional locations as appropriate
- Untrusted IPs - IOCs, blocked network ranges, etc.
- Untrusted Geo - Canadian gov sanctioned countries list
- Allowed International - Approved locations

Blueprint for strong authentiction

Policy Name	State	Users		Cloud Apps or Actions		Conditions						Grant		Session	Notes
		Included	Excluded	Included	Excluded	User Risk	Sign-in Risk	Device Platforms	Locations	Client apps	Filter for devices	Block	Grant		
Allow International Connectivity	On	CA_Allow_International		All cloud apps					Include Any Exclude Corp, InternationalAllowed			Block			
Allow Guest O365	On	All Guests or external users		Office 365				Include Android, iOS, Windows, macOS, Linux		Browser			Require auth strength: Corp Approved MFA	Use Conditional Access App Control: Block downloads Sign-in frequency: 2h Disable resilience defaults	
Block Guest Global Apps (excl O365)	On	All Guests or external users		All cloud apps	Office 365					Browser Mobile apps and desktop clients Exchange ActiveSync clients Other clients		Block			
Block High Risk Admin tools (excl PAW)	On	All Users	BreakGlass Admin	Azure AD Identity Governance - Entitlement Management Azure AD Identity Governance Insights Azure Advanced Threat Protection Azure Analysis Services Azure DevOps Azure Key Vault Azure Linux VM Sign-In Azure Monitor Control Service Azure SQL Database Azure Storage Microsoft Azure Management Microsoft Admin Portals					Include Any Exclude PAW			Block			
Block Legacy Auth	On	All Users		All cloud apps						Legacy Auth: Exchange ActiveSync Other Clients		Block			
Block Linux Apps	On	All Users		All cloud apps				Linux	Include Any	Mobile apps and desktop clients		Block			
Block Mac Apps	On	All Users		All cloud apps				Mac	Include Any	Mobile apps and desktop clients		Block			
Block Mobile Browser block EXO SPO	On	All Users	CA_MobileBrowser_Exclude	Office 365 Office 365 Exchange Online Office 365 Sharepoint Online				Android iOS Windows Phone	Include Any	Browser		Block			
Block Security Registration Restrictions Off Prem	On	All Users	CA_SecInfoReg_Limits_Exclude	Register security information					Include Any Exclude Corp			Block			
Block Security Registration Restrictions - Exclude	On	CA_SecInfoReg_Limits_Exclude	BreakGlass Admin	Register security information					Include Any Exclude Corp, Canada			Block			
Block unknown or unsupported device platform	On	All Users	BreakGlass Admin	All cloud apps				Include All Exclude Android, iOS, Windows Phone, Windows, macOS, Linux				Block			
Block untrusted locations (exclude)	On	All Users	CA_InternationalAllowed	All cloud apps					Include Any Exclude Corp, Canada			Block			
Block untrusted locations (include)	On	All Users		All cloud apps					Include Untrusted locations Exclude Corp, US, Canada, Fourteen Eyes, InternationalAllowed			Block			
Block Windows Apps Unmanaged	On	All Users	CA_Unmanaged_WinApps_Exclude	All cloud apps	VPN App Prod VPN App Test			Windows	Include Any Exclude Corp	Mobile apps and desktop clients	Exclude device.isCompliant -eq True and device.deviceOwnership -eq "Company" -and (device.trustType -eq "AzureAD" -or device.trustType -eq "ServerAD")	Block			
Block Windows Phone Apps	On	All Users		All cloud apps				Windows Phone	Include Any	Mobile apps and desktop clients		Block			
Grant MFA for VPN	On	VPN_Prod_Users VPN_Test_Users		VPN App Prod VPN App Test									Require auth strength: Corp Approved MFA	Sign-in frequency: 12h	Device compliance assessed via VPN client, VPN profiles per contractor group with least privilege
Grant Off Prem All Users (Mac/Linux Browser Untrusted)	On	All Users		All cloud apps				macOS, Linux	Include Any Exclude Corp	Browser			Require auth strength: Corp Approved MFA	Use Conditional Access App Control: Block downloads Sign-in frequency: 4 hours Disable resilience defaults	
Grant Off Prem All Users (MFA non-MAM Mobile Apps)	On	All Users		All cloud apps	Office 365 Microsoft Intune Microsoft Intune Enrollment Microsoft Teams Shifts Office 365 Exchange Online Office 365 Sharepoint Online Project Online			Android iOS	Include Any	Mobile apps and desktop clients			Require auth strength: Corp Approved MFA Require device to be marked as compliant	Use Conditional Access App Control: Monitor Sign-in frequency: 7d Disable resilience defaults	
Grant Off Prem All Users (Mobile Apps)	On	All Users		Office 365 Microsoft Teams Shifts Project Online	Office 365 Exchange Online			Android iOS	Include Any	Mobile apps and desktop clients			Require auth strength: Corp Approved MFA Require app protection policy	Sign-in frequency: 7d	
Grant Off Prem All Users (Mobile Browser Exclude)	On	CA_MobileBrowser_Exclude		All cloud apps				Android iOS	Include Any	Browser			Require auth strength: Corp Approved MFA	Use Conditional Access App Control: Block downloads Sign-in frequency: 2h Disable resilience defaults	
Grant Off Prem All Users (Mobile Outlook Only)	On	All Users		Office 365 Exchange Online				Android iOS	Include Any	Mobile apps and desktop clients			Require auth strength: Corp Approved MFA Require approved client app Require app protection policy	Sign-in frequency: 30d Use app enforced restrictions	
Grant Off Prem All Users (Windows Browser AADJ)	On	All Users		All cloud apps				Windows	Include Any Exclude Corp	Browser	Include device.isCompliant -eq True -and device.deviceOwnership -eq "Company" -and device.trustType -eq "AzureAD"		Require auth strength: Corp Approved MFA Require device to be marked as compliant	Use Conditional Access App Control: Monitor only Sign-in frequency: 3d Disable resilience defaults	
Grant Off Prem All Users (Windows Browser HAADJ)	On	All Users		All cloud apps				Windows	Include Any Exclude Corp	Browser	Inlcude device.isCompliant -eq True -and device.deviceOwnership -eq "Company" -and device.trustType -eq "ServerAD"		Require auth strength: Corp Approved MFA Require device to be marked as compliant Require Hybrid Azure AD joined device	Use Conditional Access App Control: Monitor only Sign-in frequency: 3d Disable resilience defaults	
Grant Off Prem All Users (Windows Browser Untrusted)	On	All Users		All cloud apps				Windows	Include Any Exclude Corp	Browser	Exclude device.isCompliant -eq True and device.deviceOwnership -eq "Company" -and (device.trustType -eq "AzureAD" -or device.trustType -eq "ServerAD")		Require auth strength: Corp Approved MFA	Use Conditional Access App Control: Block downloads Sign-in frequency: 2h Disable resilience defaults	
Grant Off Prem All Users (Windows Apps AADJ)	On	All Users		All cloud apps				Windows	Include Any Exclude Corp	Mobile apps and desktop clients	Include device.isCompliant -eq True -and device.deviceOwnership -eq "Company" -and device.trustType -eq "AzureAD"		Require auth strength: Corp Approved MFA Require device to be marked as compliant	Sign-in frequency: 3d Disable resilience defaults	
Grant Off Prem All Users (Windows Apps HAADJ)	On	All Users		All cloud apps				Windows	Include Any Exclude Corp	Mobile apps and desktop clients	Inlcude device.isCompliant -eq True -and device.deviceOwnership -eq "Company" -and device.trustType -eq "ServerAD"		Require auth strength: Corp Approved MFA Require device to be marked as compliant Require Hybrid Azure AD joined device	Use Conditional Access App Control: Monitor only Sign-in frequency: 7d Disable resilience defaults	
Grant Off Prem (Windows Apps Unmanaged Exclude)	On	CA_Unmanaged_WinApps_Exclude		All cloud apps	VPN App Prod VPN App Test			Windows	Include Any Exclude Corp	Mobile apps and desktop clients	Exclude device.isCompliant -eq True and device.deviceOwnership -eq "Company" -and (device.trustType -eq "AzureAD" -or device.trustType -eq "ServerAD")		Require auth strength: Corp Approved MFA	Sign-in frequency: 2h	
Grant On Prem All Users (Windows Apps)	On	All Users	BreakGlass Admin	All cloud apps				Windows	Include Corp	Mobile apps and desktop clients			Grant	Sign-in frequency: 7d	Apply compliance via SCCM
Grant On Prem All Users (Windows Browser)	On	All Users	On-Prem Directory Sync Service Account BreakGlass Admin	All cloud apps				Windows	Include Corp	Browser			Grant	Sign-in frequency: 7d Disable resilience defaults	Apply compliance via SCCM
Session Admin MFA+SignIn Freq	On	Include all admin roles	On-Prem Directory Sync Service Account BreakGlass Admin	All cloud apps									Require auth strength: Corp Approved MFA	Sign-in frequency: 12h Persisent browser session: Never	
Session Disable Browser Persistence	On	All Users	BreakGlass Admin	All cloud apps					Include Any	Browser			Grant	Persistent browser session: Never Disable resilience defaults	
Session Limit Downloads	On	All Users	BreakGlass Admin	Office 365 Microsoft Teams Shifts Project Online				Include Any Exclude Android, iOS	Include Any Exclude Corp		Exclude device.isCompliant -eq True and device.deviceOwnership -eq "Company" -and (device.trustType -eq "AzureAD" -or device.trustType -eq "ServerAD")		Grant	Use Conditional Access App Control: Block downloads	
Session MDM Enrollment	On	Allow_MDM_Enrollment		Register or join devices					Include Corp				Require auth strength: Corp Approved MFA		
Sign In Risk - High - Block	On	All Users	On-Prem Directory Sync Service Account BreakGlass Admin	All cloud apps			High		Include Any Exclude Corp			Block			
Sign In Risk - Medium - MFA	On	All Users	On-Prem Directory Sync Service Account BreakGlass Admin	All cloud apps			Medium		Include Any Exclude Corp				Require auth strength: Corp Approved MFA		
Sign In Risk - Low - MFA	On	All Users	On-Prem Directory Sync Service Account BreakGlass Admin	All cloud apps			Low		Include Any Exclude Corp				Require auth strength: Corp Approved MFA		
Terms of Use	On	All Users	On-Prem Directory Sync Service Account BreakGlass Admin	All cloud apps						Mobile apps and desktop clients Browser			Terms of Use		
User Risk - High - ChangePW	On	All Users	On-Prem Directory Sync Service Account BreakGlass Admin	All cloud apps		High			Include Any Exclude Corp				Require auth strength: Corp Approved MFA Require password change		
User Risk - Medium - MFA	On	All Users	On-Prem Directory Sync Service Account BreakGlass Admin	All cloud apps		Medium			Include Any Exclude Corp				Require auth strength: Corp Approved MFA		
User Risk - Low - MFA	On	All Users	On-Prem Directory Sync Service Account BreakGlass Admin	All cloud apps		Low			Include Any Exclude Corp				Require auth strength: Corp Approved MFA		

Authentication policy flow diagram



Things to block

- Block Guest Global Apps (excluding O365)
- Block High Risk Admin tools (excluding PAW)
- Block Legacy Auth
- Block Linux Apps
- Block Mac Apps
- Block Windows Phone Apps
- Block Windows Apps Unmanaged
- Block Mobile Browser block EXO SPO
- Block Security Registration Restrictions Off Prem
- Block unknown or unsupported device platform
- Block untrusted locations (exclude) - All except allowed
- Block untrusted locations (include) - Untrusted

Session, TOU, and risk policies

- Session Admin MFA+Sign In Freq
- Session Disable Browser Persistence
- Session Limit Downloads
- Session MDM Enrolment

- Terms of Use

- Sign In Risk
  - High - Block
  - Medium - MFA
  - Low - MFA

- User Risk
  - High - ChangePW
  - Medium - MFA
  - Low - MFA

Allow policies

- On Premises
  - Grant On Prem All Users (Windows Apps)
  - Grant On Prem All Users (Windows Browser)

- Allow International Connectivity
- Allow Guest O365
- Grant MFA for VPN

Off premises allow policies

- Grant Off Prem All Users
  - Untrusted devices
    - Mobile Apps
    - Mobile Outlook Only
    - MFA non-MAM Mobile Apps
    - Mac/Linux Browser Untrusted
    - Windows Browser Untrusted

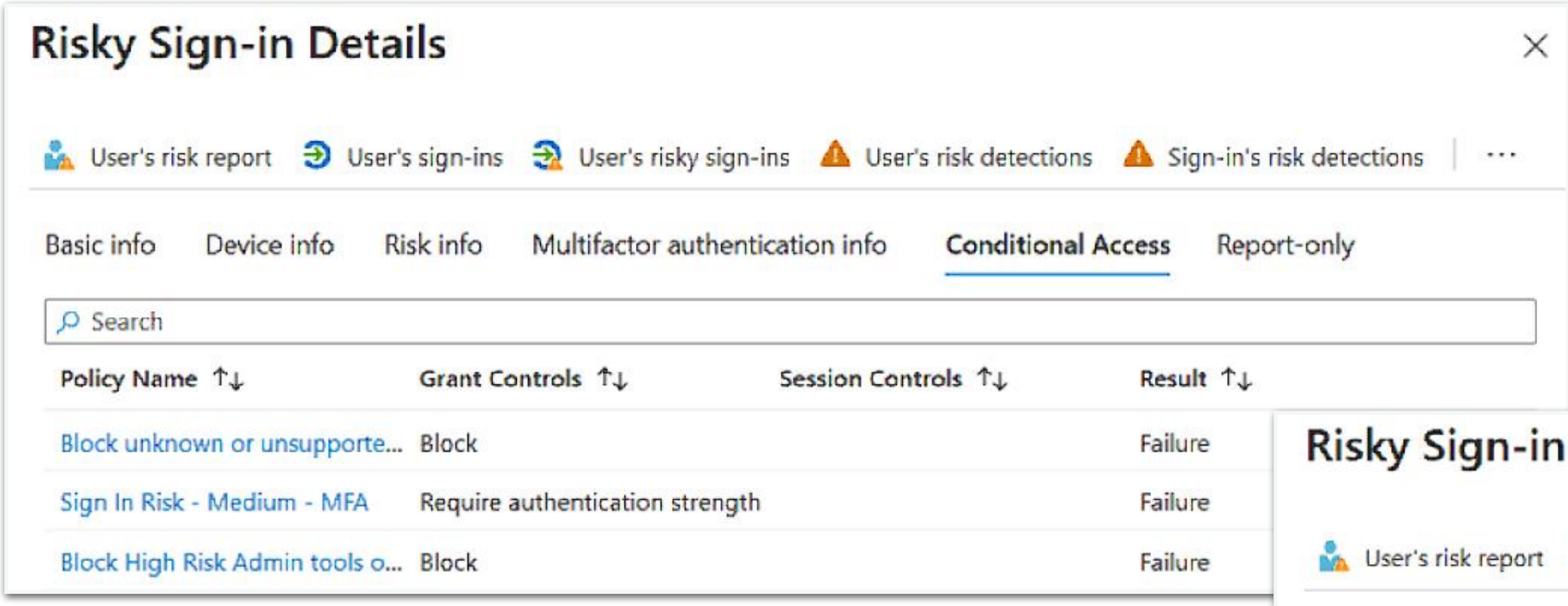
- Trusted devices:
  - Windows Browser AADJ
  - Windows Browser HAADJ
  - Windows Apps AADJ
  - Windows Apps HAADJ

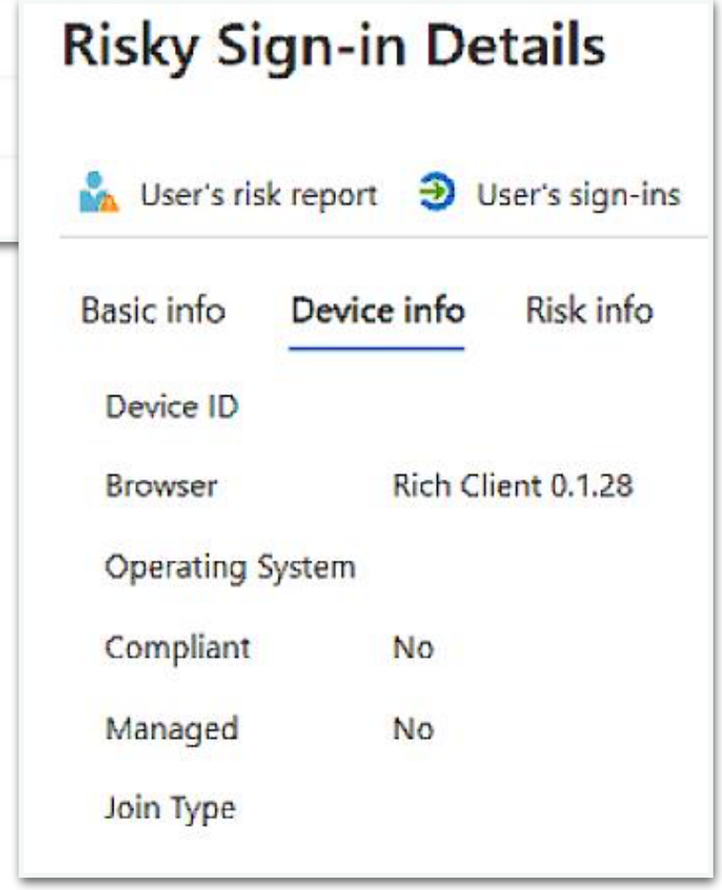
Exclude policies

- Block Security Registration Restrictions - Exclude
- Grant Off Prem All Users (Mobile Browser Exclude)
- Grant Off Prem (Windows Apps Unmanaged Exclude)

- Testing, testing, testing…

Example Risky Sign-in

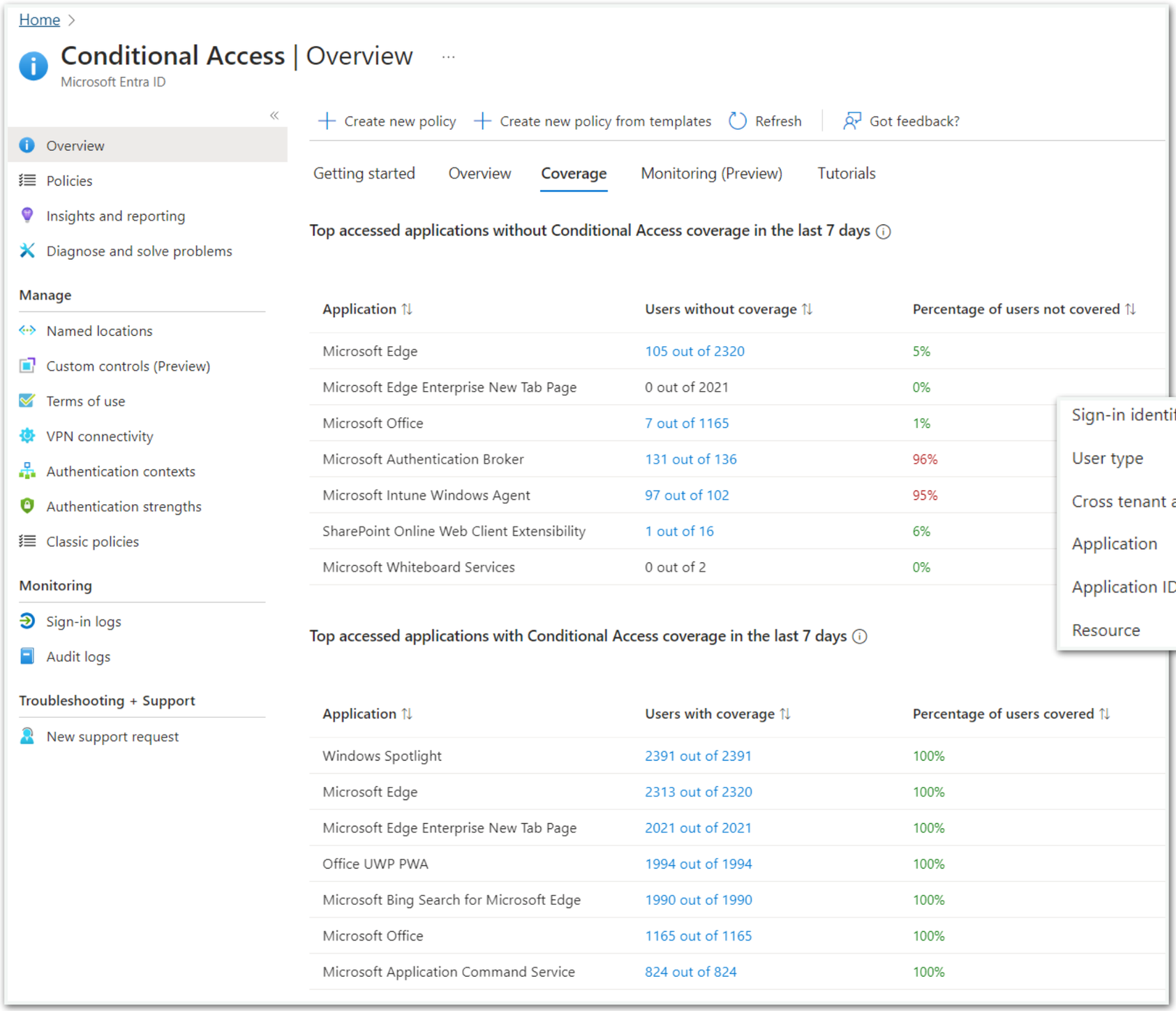




- 1st hit - Block unknown or unsupported platform
  - No operating system
- 2nd hit - Sign In Risk - Medium
  - Identified by Microsoft *after* rule above
- 3rd hit - Block high risk admin tools
  - Attempted use of Azure CLI via “Rich Client”

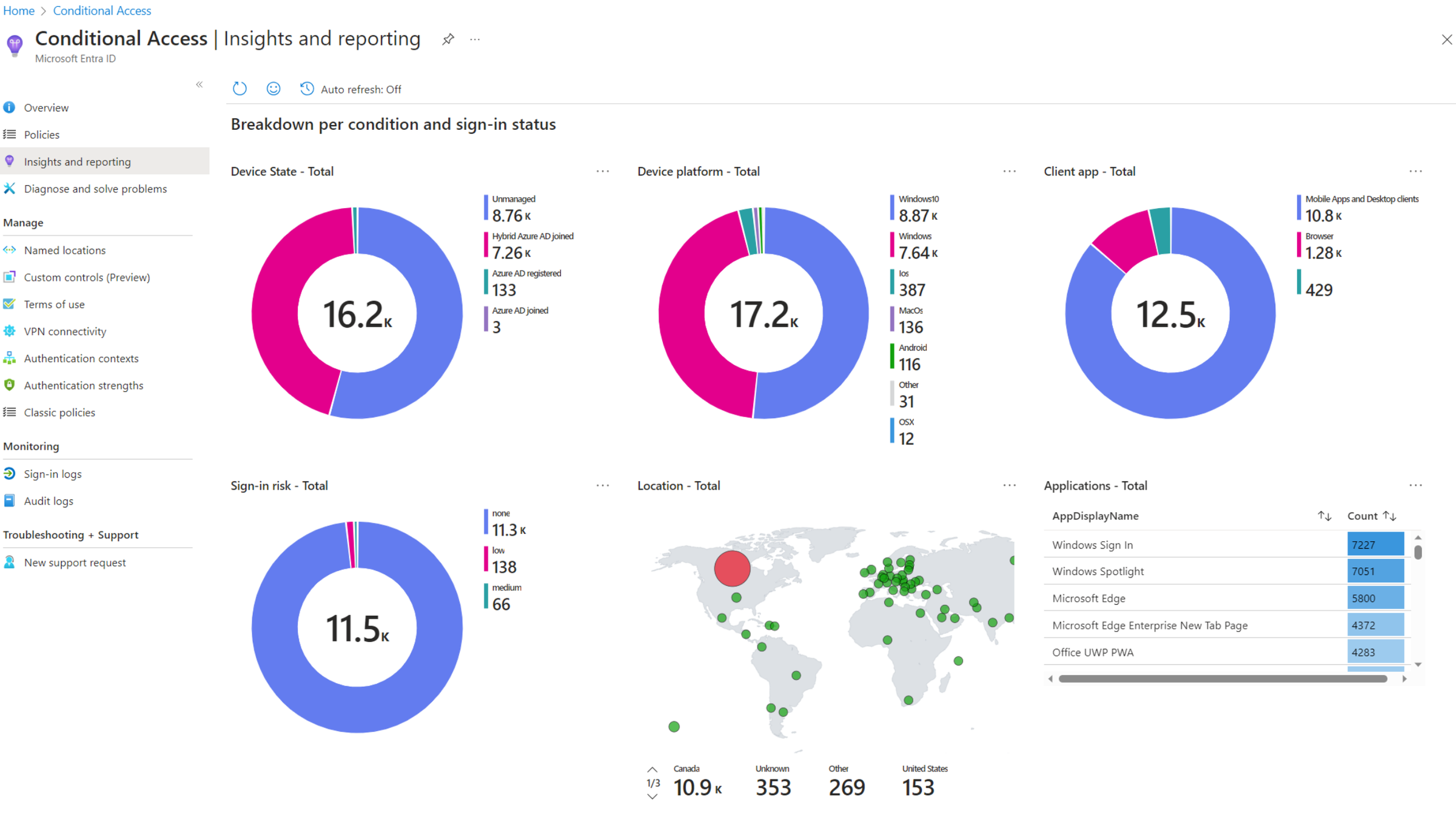
But wait, there’s more

Troubleshooting - Coverage

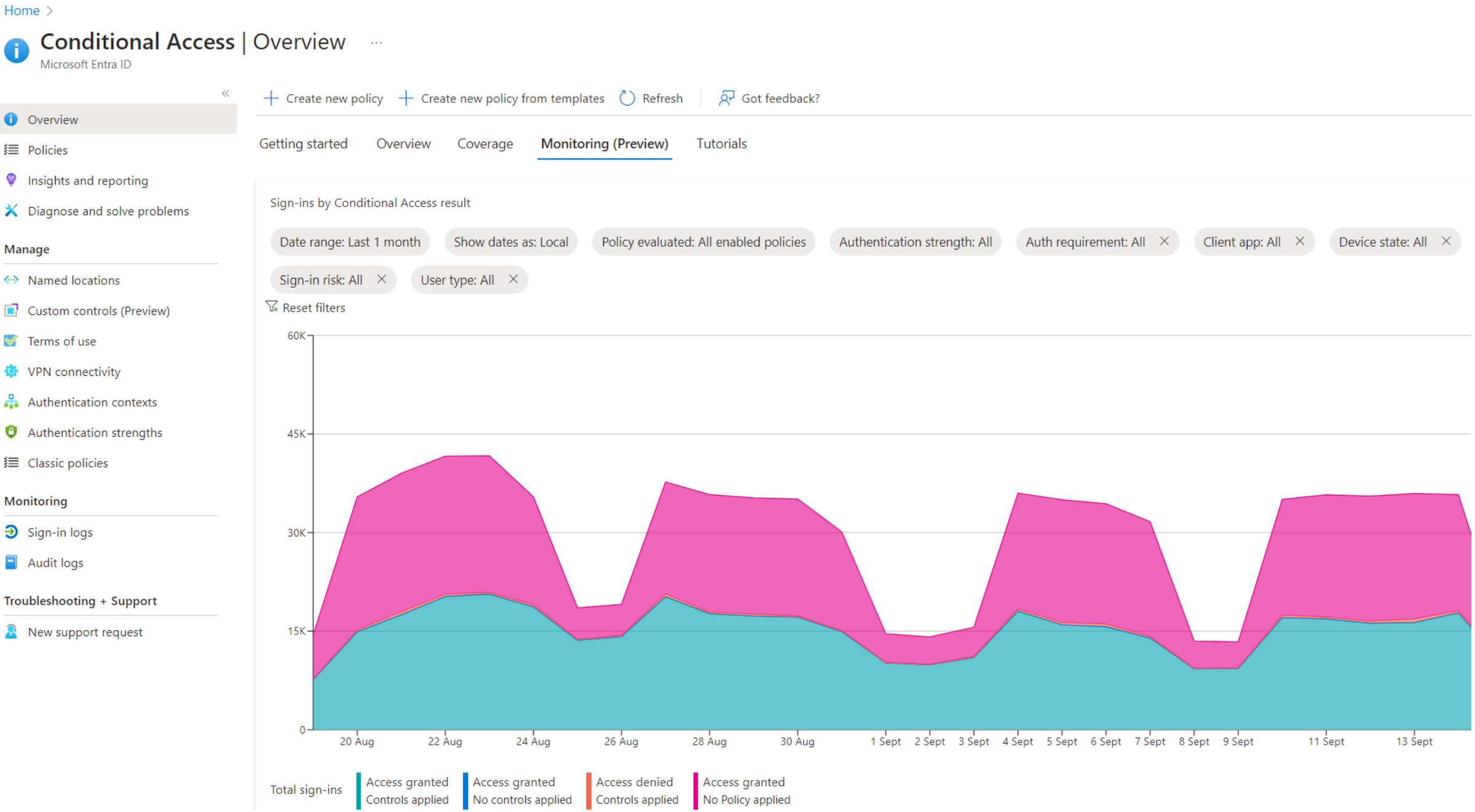


https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/troubleshoot-conditional-access

Troubleshooting - Insights

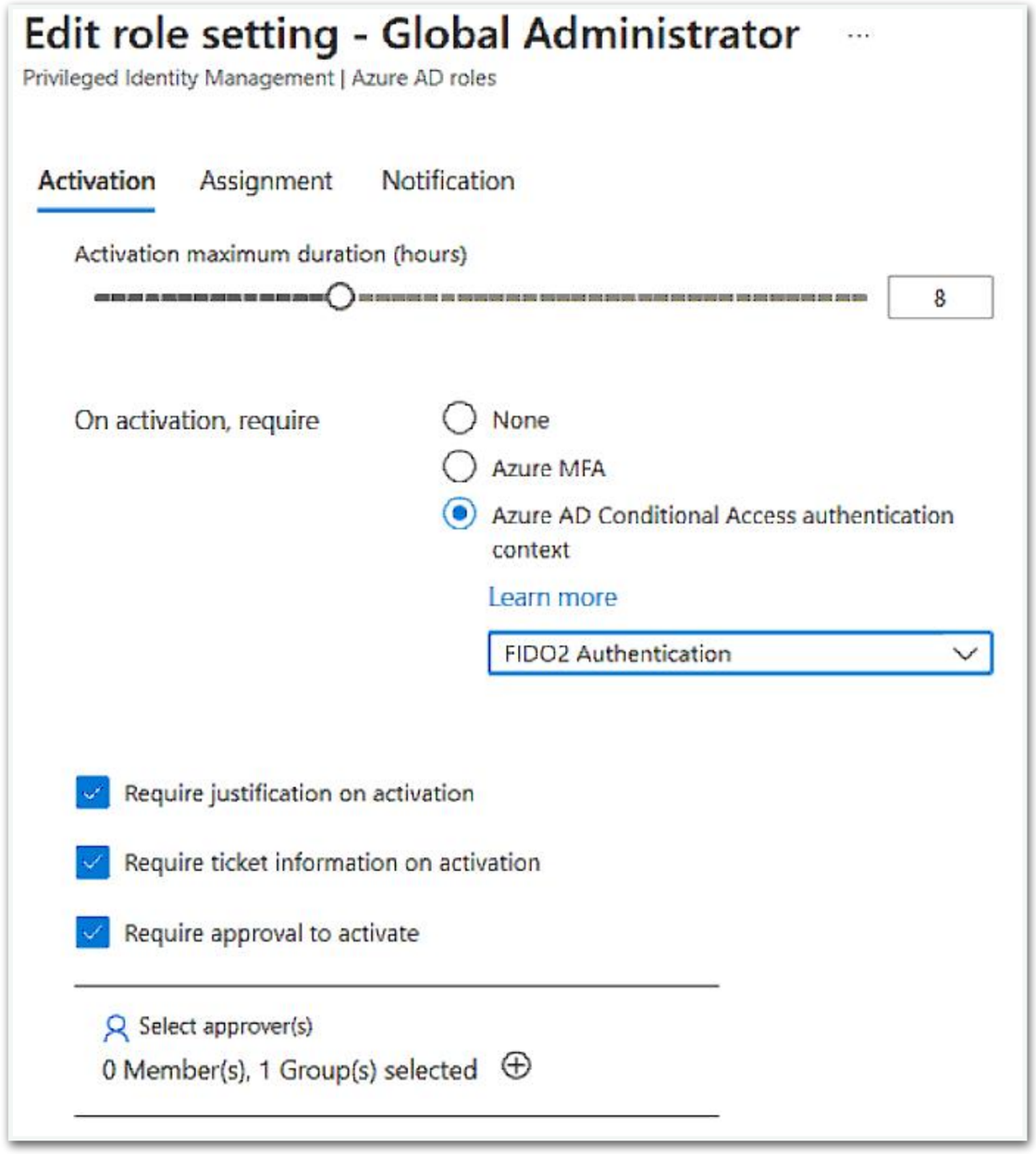


Troubleshooting - Monitoring



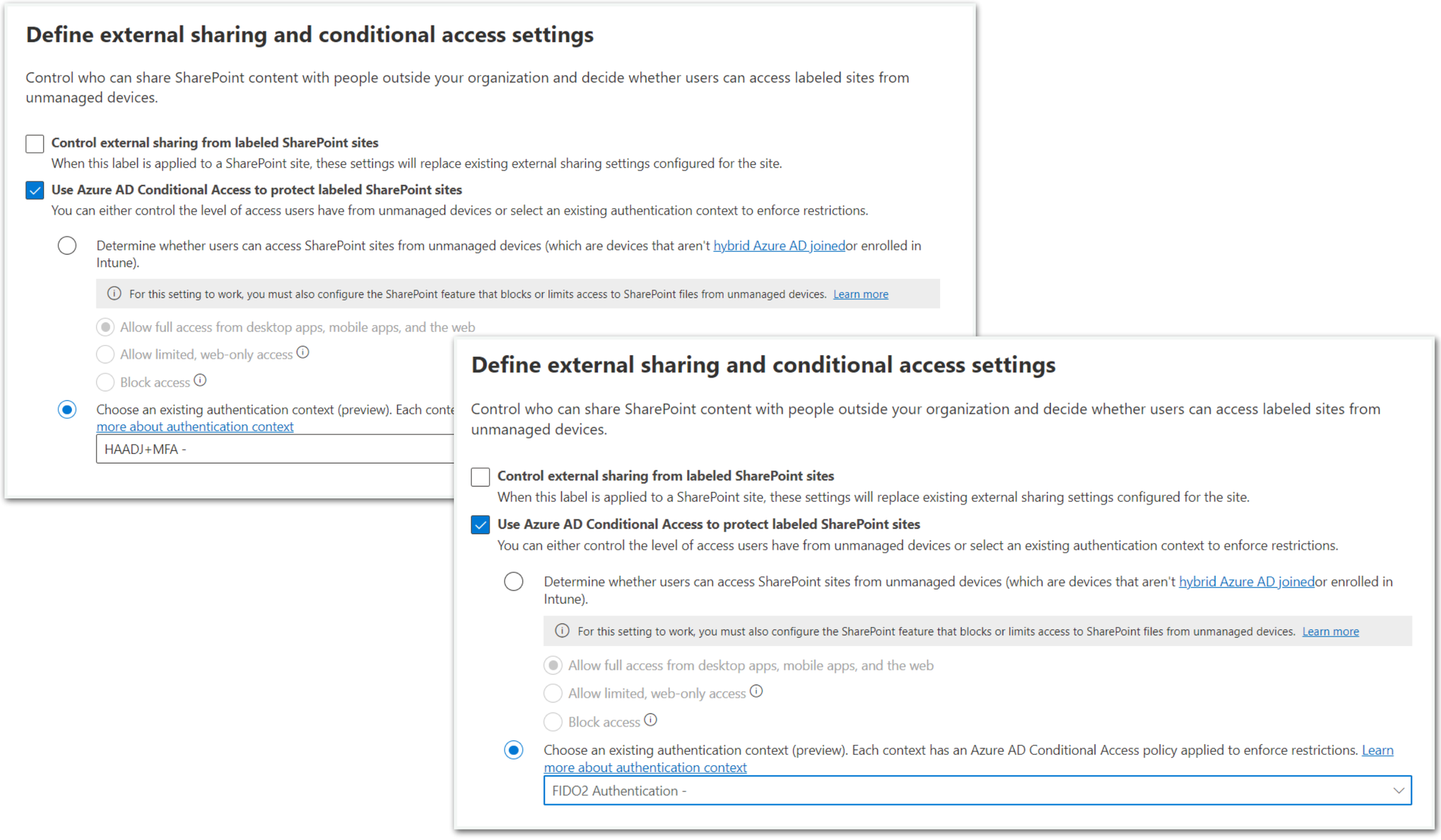
Authentication contexts and PIM

- Authentication contexts define allowed circumstances.
- PIM allows for role escalation within these limits
- e.g:
  - Must be on a specific network (PAW)
  - Must use FIDO2 auth
  - Must have an approved purpose.



https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-cloud-apps
https://learn.microsoft.com/en-us/azure/active-directory/develop/developer-guide-conditional-access-authentication-context
https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/

Sensitivity Labels



https://learn.microsoft.com/en-us/purview/what-the-dlp-policy-templates-include

Data Loss Prevention

Start with a template or create a custom policy

Choose an industry regulation to see the DLP policy templates you can use to protect that info or create a custom policy start
you need to protect labeled content, you'll be able to choose labels later. Learn more about DLP policy templates

Check out our new enhanced policy templates. These enhanced templates extend several of the original templates by also detecting named entities (such as f
physical addresses). Just look for the templates labeled 'Enhanced' to start protecting even more personal data.

Search for specific templates | Canada

Categories

- Financial
- Medical and health
- Privacy
- Custom

Templates

- Canada Health Information Act (HIA)
- Canada Personal Health Information Act (PHIA) - Manitoba
- Canada Personal Health Act (PHIPA) - Ontario

Canada Personal Health Act (PHIPA)

Helps detect the presence of informati
Canada Personal Health Information P
(PHIPA) for Ontario, including data like
numbers and health information.

Protect this information:

- Canada Passport Number
- Canada Social Insurance Numbe
- Canada Health Service Number

Choose locations to apply the policy

We'll apply the policy to data that's stored in the locations you choose.

If your role group permissions are restricted to a specific set of users or groups, you'll only be able to apply this policy to those users or groups. Learn more about role group permissions. View role groups

Protecting sensitive info in on-premises repositories (SharePoint sites and file shares) is now in preview. Note that there are prerequisite steps needed to support this new capability. Learn more about the prerequisites

Location	Scope	
Exchange email	All distribution groups	Edit
SharePoint sites	All sites	Edit
OneDrive accounts	All accounts and groups	Edit
Teams chat and channel messages	All accounts or distribution groups	Edit
Devices	All users or groups	Edit
Cloud Apps	All instances	Edit
es	All repositories	Edit
	Turn on location to scope	

Protection actions

We'll automatically create detailed activity reports so you can review the content that matches this policy. What else do you want to do?

When content matches the policy conditions, show policy tips to users and send them an email notification

Tips appear to users in their apps (like Outlook, OneDrive, and SharePoint) and help them learn how to use sensitiv
default tip or customize it to your liking. Learn more about notifications and tips

Customize the tip and email

Detect when a specific amount of sensitive info is being shared at one time

At least 10 or more instances of the same sensitive info type

Send incident reports in email

By default, you and your global admin will automatically receive the email. Incident reports are supported onl
OneDrive, and Teams.

Choose what to include in the report and who receives it

Send alerts if any of the DLP rules match

By default, you and any global admins will automatically be alerted if a DLP rule is matched.

Customize alert configuration

Restrict access or encrypt the content in Microsoft 365 locations

Info to protect

This policy will protect content that matches these conditions. Review them and make any necessary changes. For example, you can edit the conditions to detect additional sensitive info or content that has specific sensitivity or retention labels applied.

Content contains any of these sensitive info types:
Canada Passport Number
Canada Social Insurance Number
Canada Health Service Number
Canada Personal Health Identification Number (PHIN)

Edit

Detect when this content is shared from Microsoft 365:

- With people outside my organization
- Only with people inside my organization

User's risk level for Adaptive Protection is

Risk levels for Adaptive Protection are defined in insider risk management. They determine how risky a user's activity is and can be based on conditions such as how many exfiltration activities they performed or whether their activity generated a high severity insider risk alert. If insider risk management detects that a user matched the risk level condition, the DLP policy will enforce any actions you configure below. Learn more about risk levels for Adaptive Protection

Select one or more risk levels

https://learn.microsoft.com/en-us/purview/dlp-policy-reference#rules

What about licensing?

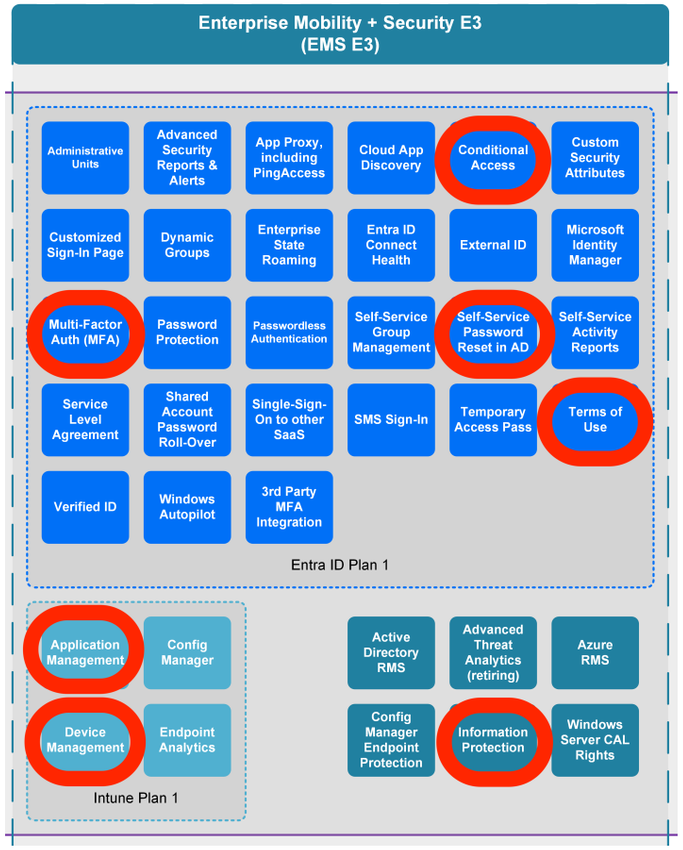
- Entra ID P1 includes:
  - Conditional Access
  - MFA
  - Self-Service Password Reset (SSPR)
  - Terms of Use

- Intune P1 inclues:
  - Device management
  - Device compliance (MDM)
  - App Protection (MAM)

- Both are part of M365 Enterprise + Mobility F3/A3/E3
  - Which also includes Information Protection (Sensitivity Labels, DLP)
    - Parts are in O365 F3/A3/E3 and F5/A5/E5 Compliance

- PIM is part of Entra ID P2, which is part of F5/A5/E5 Security

- Everything is in M365 F5/A5/E5



https://m365maps.com/files/Microsoft-365-Enterprise-Landscape.htm

Microsoft 365 Enterprise

July 2023

m365maps.com

Office 365 E3

- Activity Reports
- Adoption Score
- Alert Policies
- Audit Conferencing (free add-on)
- Audit (standard)
- Basic Mobility & Security
- Bookings
- Briefing Email
- Compliance Manager
- Content Search
- Data Loss Prevention
- Delve
- eDiscovery (standard)
- Entra ID for Office 365
- Exchange Online Plan 2
- Exchange Online Protection
- InfoPath App
- Information Protection for M365
- Kaizala Pro (retiring)
- Live Events
- Message Encryption (basic)
- Microsoft 365 Apps for Enterprise
- Microsoft 365 Mobile App
- Microsoft Dataverse for Teams
- Microsoft Forms
- Microsoft Lists
- Microsoft Search
- Microsoft Teams
- Microsoft To Do
- Microsoft Whiteboard
- Office for the Web (incl Visio)
- OneDrive for Business Plan 2
- Planner
- Power Apps for Office 365
- Power Automate for Office 365
- Power Virtual Agents for Teams
- Productivity Server CAL
- Project & Roadmap View Access
- Retention Labels
- Retention Policies
- Secure Score
- SharePoint Online Plan 2
- Stream for Office 365
- Sway
- Viva Connections
- Viva Engage
- Viva Insights - Personal (basic)
- Viva Learning (basic)
- Webinars

Enterprise Mobility + Security E3 (EMS E3)

- Administrative Units
- Advanced Security Reports & Alerts
- App Proxy, including PingAccess
- Cloud App Discovery
- Conditional Access
- Custom Security Attributes
- Customized Sign-In Page
- Dynamic Groups
- Enterprise State Roaming
- Entra ID Connect Health
- External ID
- Microsoft Identity Manager
- Multi-Factor Auth (MFA)
- Password Protection
- Passwordless Authentication
- Self-Service Group Management
- Self-Service Password Reset in AD
- Self-Service Activity Reports
- Service Level Agreement
- Shared Account Password Roll-Over
- Single-Sign-On to other SaaS
- SMS Sign-In
- Temporary Access Pass
- Terms of Use
- Verified ID
- Windows Autopilot
- 3rd Party MFA Integration

Entra ID Plan 1

- Application Management
- Config Manager
- Device Management
- Endpoint Analytics

Intune Plan 1

- Active Directory RMS
- Advanced Threat Analytics (retiring)
- Azure RMS
- Config Manager Endpoint Protection
- Information Protection
- Windows Server CAL Rights

Windows Enterprise E3

- Always On VPN
- Application Control
- Application Guard
- AppLocker
- App Assure
- Assigned Access
- Attack Surface Reduction
- BitLocker
- BitLocker to Go
- BranchCache
- Cortana
- Credential Guard
- Custom Logon
- Custom Shell
- Defender Antivirus
- DirectAccess
- Domain Join
- Edge for Business
- Entra ID Join
- Keyboard Filter
- LAPS
- Long Term Servicing Channel
- Manage by MDM
- MDOP (retiring)
- Persistent Memory
- Power Automate Attended Desktop Flows
- Resilient File System (ReFS)
- SMB Direct
- Unbranded Boot
- Unified Write Filter
- Universal Print
- Windows Autopatch
- Windows Conditional Access
- Windows Firewall
- Windows Hello for Business
- Windows Information Protection (retiring)
- Windows Update for Business
- Windows Virtualization Rights
- 36 months support for Windows 11

Microsoft 365 E3

Microsoft 365 E5 Step-up

Microsoft 365 E5 Step-up

Microsoft 365 E5 Compliance

- Audio Conferencing (full)
- Graph Connector Index Quota (500 per user)
- Office 365 Cloud App Security
- Power BI Pro
- Skype for Business Plus CAL
- Teams Phone
- Viva Insights - Personal (premium)

eDiscovery & Audit

- 3x Premium & Custom Compliance Templates
- Audit (premium)
- eDiscovery (premium)

Insider Risk Management

- Insider Risk Management
- 3x Premium & Custom Compliance Templates
- Comm Compliance
- Customer Lockbox
- Information Barriers
- Privileged Access Management

Information Protection & Governance

- Endpoint DLP
- Trainable Classifiers
- 3x Premium & Custom Compliance Templates
- Customer Key
- Data Lifecycle Management
- Double Key Encryption
- Exact Data Match
- Message Encryption (advanced)
- Records Management
- Rules-Based Classification (Office 365)
- Teams Data Loss Prevention
- Teams DLP & Export Graph API
- Rules-Based Classification (Client & Scanner)
- App Governance
- Defender for Cloud Apps

Microsoft 365 E5 Compliance

Microsoft 365 E5 Security

- Application Guard for Office
- Safe Documents
- Sentinel Benefit
- Advanced Anti-Phishing
- Exchange Online Protection
- Real-Time Reports
- Safe Attachments
- Safe Links

Defender for Office 365 Plan 1

- Attack Simulation Training
- Automated Investigation & Response
- Campaign Views
- Compromised User Detection
- Threat Explorer
- Threat Trackers

Defender for Office 365 Plan 2

- Access Reviews
- Entitlement Management
- ID Protection
- MFA Registration Policy
- Privileged Identity Management
- Risk-Based Conditional Access

Entra ID Plan 2 Step-up

- App Governance
- Defender for Cloud Apps
- Defender for Identity
- Advanced Hunting
- Automated Investigations
- Defender for Cloud Apps Integration
- Endpoint Attack Notifications
- Endpoint Detection & Response
- Evaluation Lab
- MIP Integration
- Threat Analytics
- Vulnerability Management (core)
- 6-Months Searchable Data

Defender for Endpoint Plan 2 Step-up

Microsoft 365 E5 Security

Microsoft 365 E5 Step-up

Office 365 E5 Step-up

Enterprise Mobility + Security E5 Step-up (EMS E5)

Windows Enterprise E5 Step-up

Microsoft 365 Enterprise Benefits

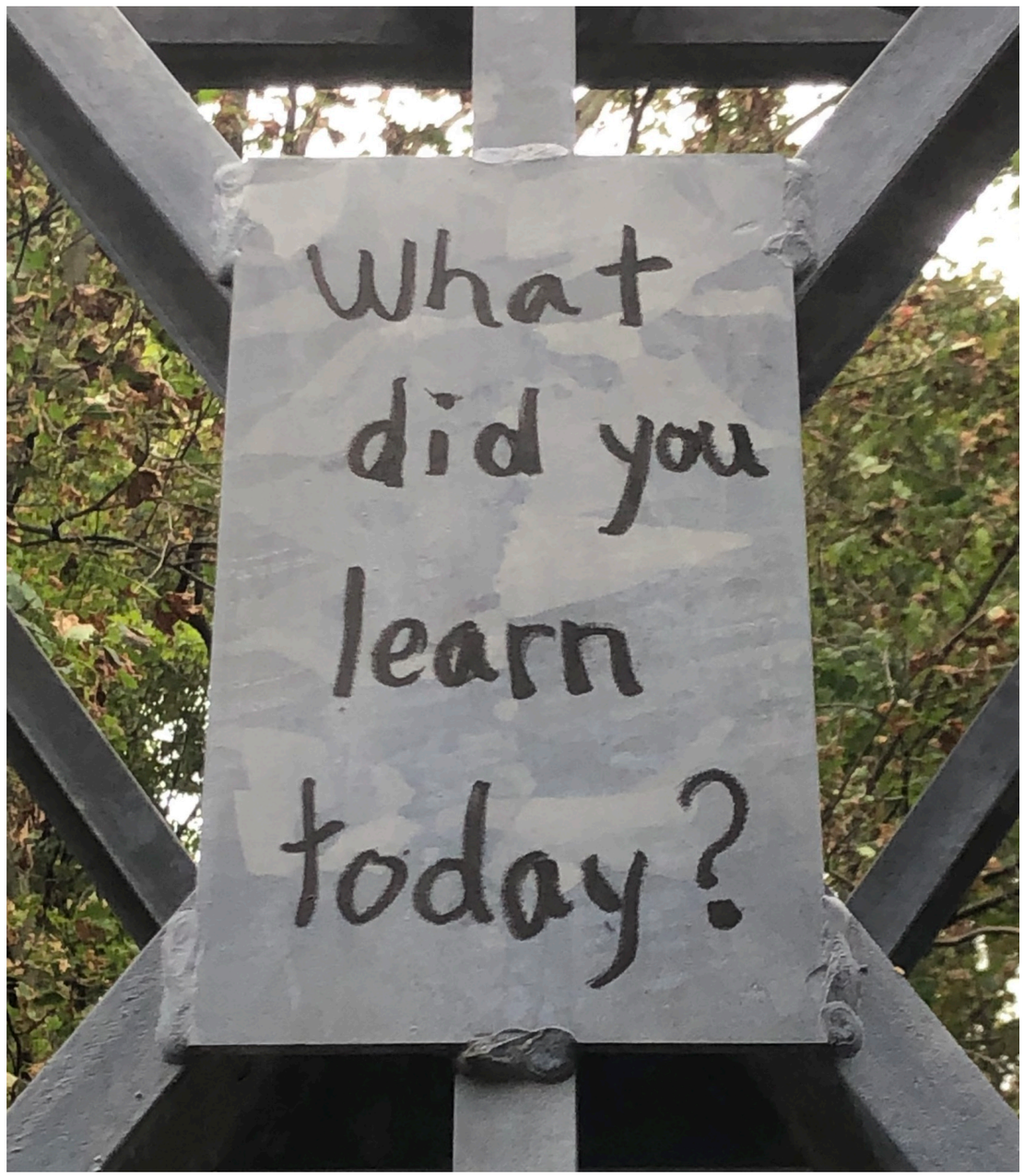
FastTrack — FastTrack helps customers deploy Microsoft 365. Customers with 150+ eligible licenses can use FastTrack at no additional cost for the life of their subscription.

Office Professional Plus — One traditional Office Professional Plus device install for each existing Software Assurance (SA) user, and new users up to the number of existing From SA users.

Office Servers — Install SharePoint, Exchange, and Skype for Business Server, on dedicated hardware (not multi-tenant), for use by Microsoft 365 E3 & E5 licensed users. Excludes CSP/MCA.

Conclusions

- Authentication starts with:
  - Devices
  - Clients
  - Apps
- Devices
  - Hybrid join for hybrid orgs
  - Entra join for cloud-native
  - Registering is only for BYOD mobile devices
- Require compliance
- MDM for devices, but layer MAM for applications
- User authentication methods matter
- Things often change, review at least quarterly
- Licenses are important
- So are your logs



Resources & Links

M365Maps - Enterprise Landscape
https://m365maps.com/files/Microsoft-365-Enterprise-Landscape.htm

Australian Government - Digital Transformation Authority - Protected Utility Blueprint
https://desktop.gov.au/blueprint/

CISA Secure Cloud Business Applications (SCuBA) Project
https://www.cisa.gov/resources-tools/services/secure-cloud-business-applications-scuba-project

Conditional Access Session Lifetimes
https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-session-lifetime

Resilience Overview
https://learn.microsoft.com/en-us/azure/active-directory/architecture/resilience-overview

Co-Management for existing CM clients
https://learn.microsoft.com/en-us/mem/configmgr/comanage/tutorial-co-manage-clients

Co-Management for new internet based devices
https://learn.microsoft.com/en-us/mem/configmgr/comanage/tutorial-co-manage-new-devices

Intune Compliance policy – Windows
https://learn.microsoft.com/en-us/mem/intune/protect/compliance-policy-create-windows

Intune Windows update compliance workbook
https://msendpointmgr.com/2021/11/26/windows-update-compliance-workbook-community-edition/

Intune Data collection
https://learn.microsoft.com/en-us/mem/intune/protect/privacy-data-collect

Questions?

Thank you

Contact Info:

singleusermode@infosec.exchange
don - Hackfest Discord
nixuser23@gmail.com