

Unconditionally Conditional

**Strong authentication in Microsoft Entra ID
(formerly Azure AD)**

Don Mallory
Hackfest - Oct 13, 2023

whoami

- 30 years in IT, mostly for critical infrastructure
- Healthcare security professional
- CISSP, GSEC, GCED, GCIH
- 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

No need to take photos
Wait for the **last** QR code



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

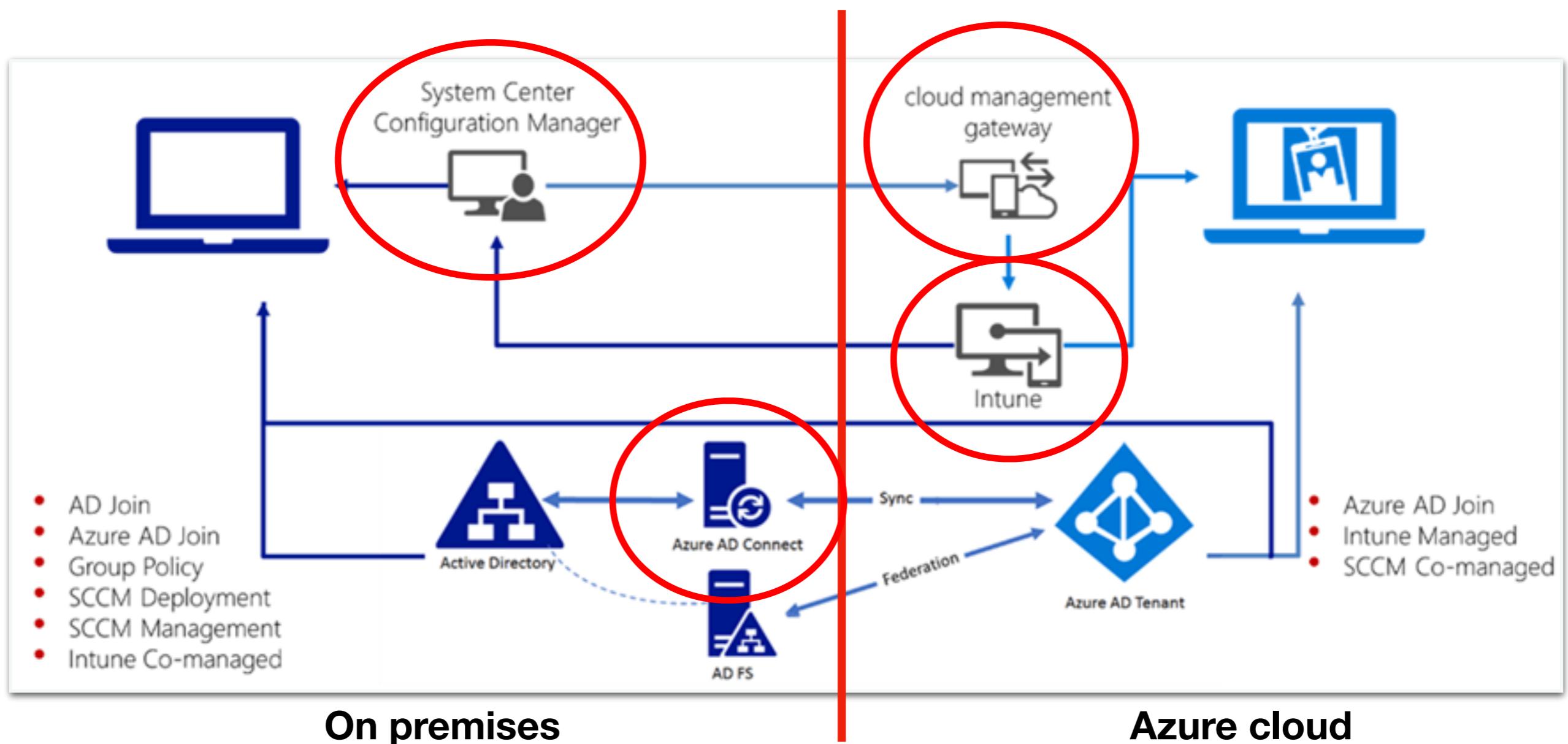
This is still all about trust

Why should we care?

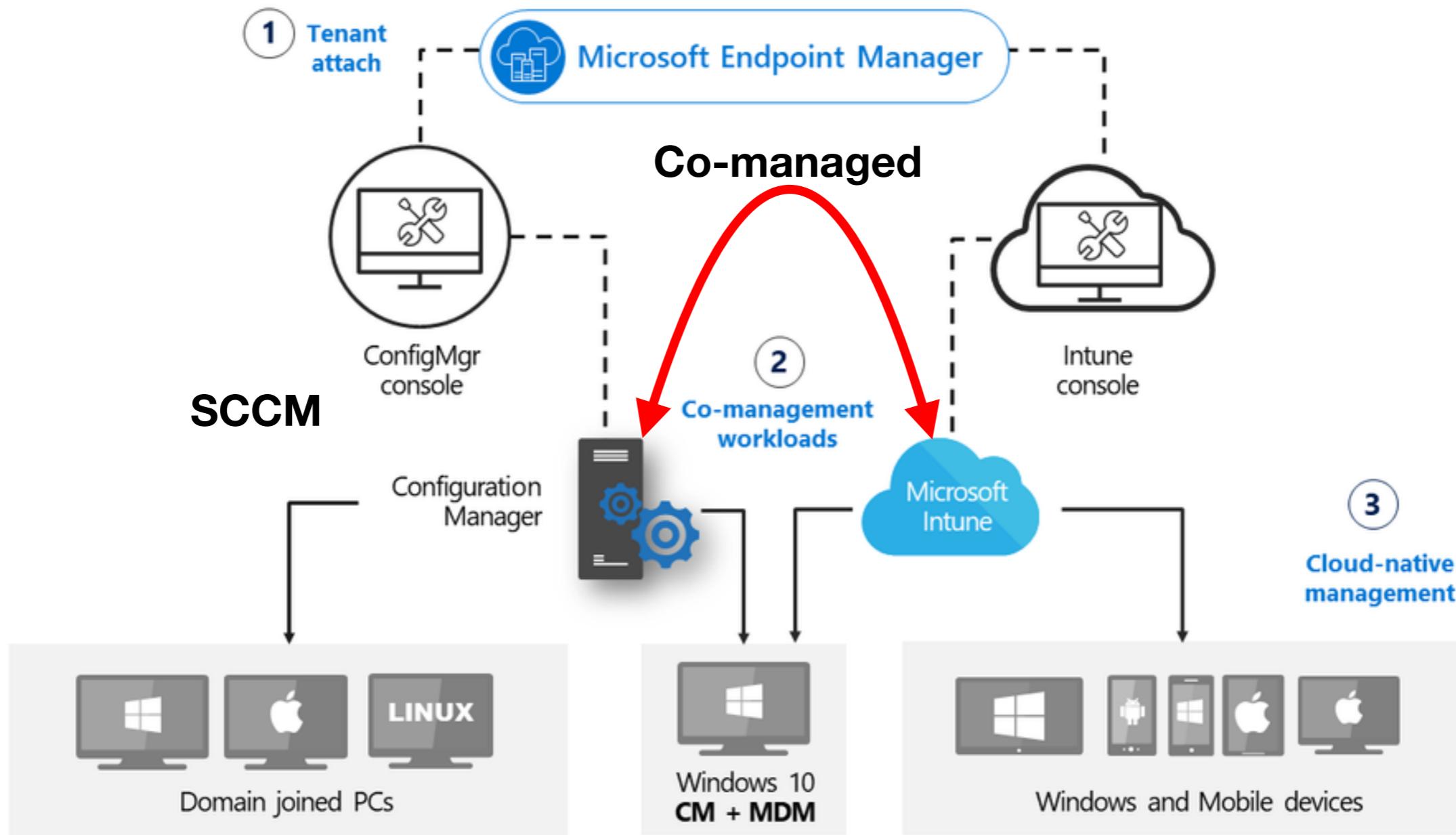
- Traditional thinking:
 - The physical network boundary is the edge.
 - A firewall will save us!
- Cloud posture:
 - The data is the edge.
 - The client is just a conduit to the data.
 - Authentication is the gateway to your data.

**Legal, regulatory, and moral obligation to protect
the data of your staff and clients.**

Hybrid management architecture



Start with 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

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**

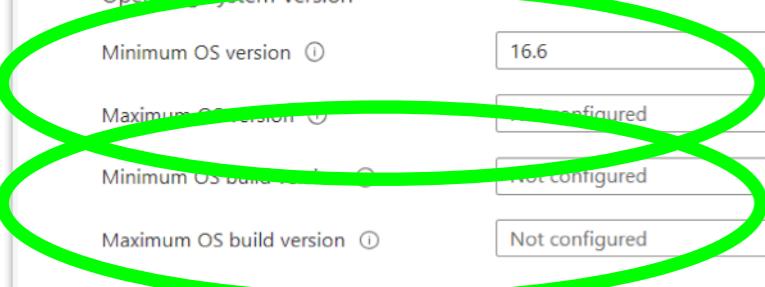
Maximum OS build version ⓘ **Not configured**

^ 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

MAM policies (1)

Apps [Edit](#)

Target to apps on all device types Yes

Device types --

Public apps

Custom apps

- Adobe Acrobat Reader
- Webex for Intune
- Microsoft Edge
- Microsoft Excel
- Microsoft Outlook
- Microsoft PowerPoint
- Microsoft Word
- Microsoft Lens
- Microsoft Office
- Microsoft OneNote
- Microsoft Planner
- Power Automate
- Microsoft SharePoint
- Microsoft OneDrive
- Microsoft Teams
- Microsoft Lists
- Microsoft Stream
- Microsoft To-Do
- Microsoft Whiteboard
- Slack for Intune
- Zoom for Intune
- com.microsoft.visio

- 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



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 ⓘ
- Send org data to other apps ⓘ
- Select apps to exempt
- Select universal links to exempt
- Select managed universal links
- Save copies of org data ⓘ
- Allow user to save copies to selected services ⓘ
- Transfer telecommunication data to ⓘ
- Dialer App URL Scheme
- Receive data from other apps ⓘ
- Open data into Org documents ⓘ
- Allow users to open data from selected services ⓘ
- Restrict cut, copy, and paste between other apps ⓘ
- Cut and copy character limit for any app *
- Third party keyboards

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

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 ⓘ
- PIN type ⓘ
- Simple PIN ⓘ
- Select minimum PIN length ⓘ
- Touch ID instead of PIN for access (iOS 8+/iPadOS) ⓘ
- Override biometrics with PIN after timeout ⓘ
- Timeout (minutes of inactivity)
- Face ID instead of PIN for access (iOS 11+/iPadOS) ⓘ
- PIN reset after number of days ⓘ
- Number of days
- App PIN when device PIN is set ⓘ
- Work or school account credentials for access ⓘ
- Recheck the access requirements after (minutes of inactivity) * ⓘ

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.

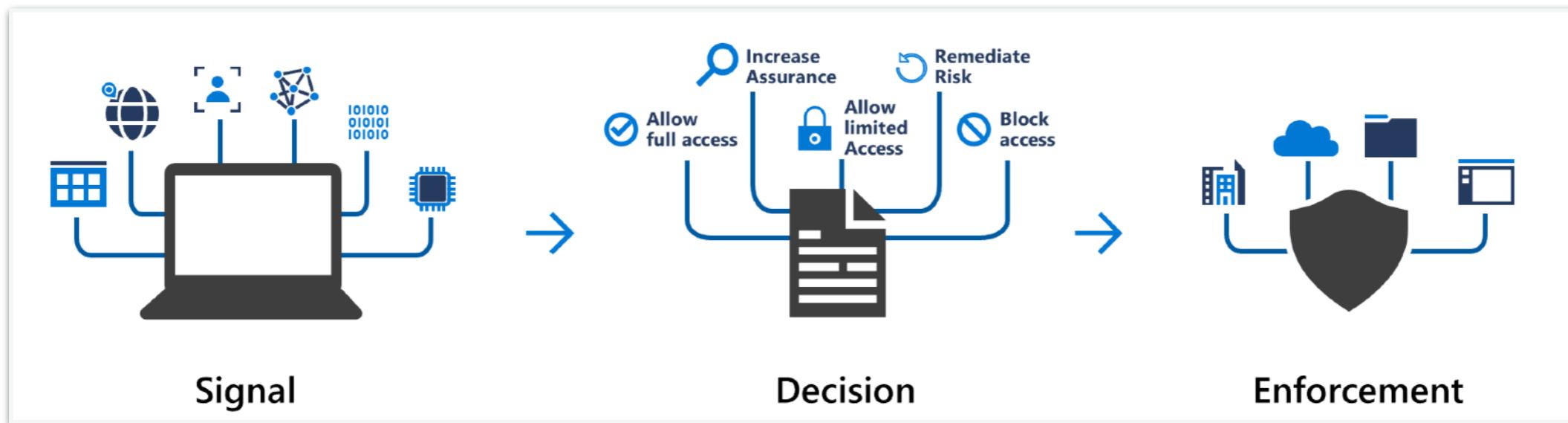
Similar device based settings can be configured for enrolled devices. [Learn more about configuring device compliance settings for enrolled devices.](#)

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	...

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
- Config policies are required before compliance on Mac

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.

CA Policies - Users

Home > Conditional Access | Policies >

New ...

Conditional Access policy

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

Name *
Example: 'Device compliance app policy'

Assignments

Users ⓘ
Specific users included
✗ "Select users and groups" must be configured

Target resources ⓘ
No target resources selected

Conditions ⓘ
0 conditions selected

Access controls

Grant ⓘ
0 controls selected

Session ⓘ
0 controls selected

Include Exclude

None
 All users
 Select users and groups

Guest or external users ⓘ

0 selected

B2B collaboration guest users
 B2B collaboration member users
 B2B direct connect users
 Local guest users
 Service provider users
 Other external users

Include Exclude

None
 All users
 Select users and groups

Guest or external users ⓘ
 Directory roles ⓘ

0 selected

global

Built-in directory roles

Global Administrator
 Global Reader
 Global Secure Access Administrator

- Exclusions:
 - Always exclude your “break glass” admin account, or the account you are performing changes with to avoid lockout
 - Plan exclusion groups for testing

CA Policies - Target Resource - Apps

Home > Conditional Access | Policies >

New ...

Conditional Access policy

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

Name *

Assignments

Users ⓘ

Specific users included

✖ "Select users and groups" must be configured

Target resources ⓘ

No target resources selected

Select what this policy applies to

Cloud apps

Include Exclude

None

All cloud apps

Select apps

Select

Cloud apps

Search bar: office

<input type="checkbox"/>	Office 365 ⓘ
<input type="checkbox"/>	Office 365 Exchange Online 0000002-0000-0ff1-ce00-000000000000
<input type="checkbox"/>	Office 365 Message Encryption Portal 3a9ddf38-83f3-4ea1-a33a-ecf934644e2d
<input type="checkbox"/>	Office 365 SharePoint Online 0000003-0000-0ff1-ce00-000000000000

Select apps

Edit filter (Preview)
None

Select
[Microsoft Admin Portals \(Preview\)](#)

 Microsoft Admin Portals (Previe... ***

<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

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

Select what this policy applies to

User actions

Select the action this policy will apply to

Register security information

Register or join devices

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

Select what this policy applies to

Authentication context

Authentication context is used to secure application data and actions in apps like SharePoint and Microsoft Cloud App Security. [Learn more](#)

Select the authentication contexts this policy will apply to

HAADJ

FIDO2 Authentication

HAADJ+MFA

AADJ+MFA

On Premises

Approved MFA

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

Select what this policy applies to

Global Secure Access (Preview)

Select the traffic profiles this policy applies to ⓘ

0 selected

Microsoft 365 traffic

Internet traffic

Private traffic

CA Policies - Conditions

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

User risk [\(i\)](#)
[Not configured](#)

Sign-in risk [\(i\)](#)
[Not configured](#)

Device platforms [\(i\)](#)
[Not configured](#)

Locations [\(i\)](#)
[Not configured](#)

Client apps [\(i\)](#)
[Not configured](#)

Filter for devices [\(i\)](#)
[Not configured](#)

User risk

Configure [\(i\)](#)
[Yes](#) [No](#)

Configure user risk levels needed for policy to be enforced

High
 Medium
 Low

Device platforms

Apply policy to selected device platforms. [Learn more](#)

Configure [\(i\)](#)
[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 [\(i\)](#)
[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 [\(i\)](#)

Sign-in risk

Control user access to respond to specific sign-in risk levels. [Learn more](#)

Configure [\(i\)](#)
[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

CA Policies - Conditions - Locations

The screenshot illustrates the Microsoft Conditional Access Named locations interface, specifically focusing on location conditions.

Conditional Access | Named locations (Overview):

- Control user access based on their physical location. [Learn more](#)
- Configure [Yes](#) or [No](#)
- Include [Any location](#) (selected), [All trusted locations](#), [All Compliant Network locations \(Preview\)](#), or [Selected locations](#).

Select Locations:

- Location type: All types
- Trusted type: All types
- Search names:

Name	Location type	Trusted
<input type="checkbox"/> Multifactor authentication trusted IPs	IP ranges	Yes
<input type="checkbox"/> Canada	Countries (IP)	
<input type="checkbox"/> Five Eyes	Countries (IP)	
<input type="checkbox"/> Fourteen Eyes	Countries (IP)	
<input type="checkbox"/> InternationalAllowed	Countries (IP)	
<input type="checkbox"/> Nine Eyes	Countries (IP)	
<input type="checkbox"/> United States	Countries (IP)	
<input type="checkbox"/> Untrusted IPs	IP ranges	No
<input type="checkbox"/> Untrusted locations	Countries (IP)	

New location (Countries):

- As of May 2023, both IPv4 and IPv6 addresses are mapped to countries/regions.
- Name *****: Name this location
- Determine location by IP address (IPv4 and IPv6) [▼](#)
- Include unknown countries/regions [i](#)
- Search countries
- Name [↑↓](#)

New location (Countries):

- As of May 2023, both IPv4 and IPv6 addresses are mapped to countries/regions.
- Name *****: Name this location
- Determine location by GPS coordinates [▼](#)
- Include unknown countries/regions [i](#)
- Search countries
- Name [↑↓](#)

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
Or	trustType	Equals	Microsoft Entra
And	deviceOwnership	Equals	Company
And	isCompliant	Equals	True

+ Add expression

Rule syntax ⓘ

```
device.trustType -eq "AzureAD" -or device.trustType -eq "ServerAD" -and device.deviceOwnership -eq "Company" -and device.isCompliant -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 operator>	<Pick a property and operator first>

+ Add expression

Rule syntax ⓘ

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

Apply

CA Policies - Session Controls

The screenshot shows the 'Session' configuration page for Conditional Access. It includes sections for 'Sign-in frequency', 'Persistent browser session', 'Customize continuous access evaluation', and other optional settings.

Session

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

Use app enforced restrictions ⓘ

Only supports O365, EXO, SPO

Use Conditional Access App Control ⓘ

Use custom policy...

Monitor only (Preview)

Block downloads (Preview)

Use custom policy...
 onboarded for any app. [Learn more](#)

Sign-in frequency ⓘ

Periodic reauthentication

2 Hours

Every time

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

Persistent browser session ⓘ

Persistent browser session

Always persistent

Never persistent

Customize continuous access evaluation ⓘ

Disable

Strictly enforce location policies (Preview) ⓘ

[See list of supported clients and resource providers](#)

Disable resilience defaults ⓘ

Require token protection for sign-in sessions (Preview) ⓘ

<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

The image displays three screenshots of Conditional Access (CA) policy controls:

- Grant (Left):** A simple interface for choosing access enforcement. It shows "Control access enforcement to block or grant access." with two options: "Block access" (radio button selected) and "Grant access".
- Grant (Middle):** Similar to the first, but includes a checkbox for "Require multifactor authentication". The "Grant access" option is selected. A tooltip message states: "To enable all authentication strengths, configure cross-tenant access settings to accept claims coming from Microsoft Entra tenants for external users. Authentication strengths will only configure second factor authentication for external users.".
- View authentication strength (Right):** A detailed list of authentication methods. The "Configure" tab is selected. It shows a table of methods, each with a checkbox and a dropdown arrow:

Method	Status
Phishing-resistant MFA (3)	unchecked
Windows Hello For Business	unchecked
FIDO2 Security Key	checked
Advanced options	dropdown arrow
Certificate-based Authentication (Multifactor)	unchecked
Passwordless MFA (1)	checked
Microsoft Authenticator (Phone Sign-in)	checked
Multifactor authentication (13)	unchecked
Temporary Access Pass (One-time use)	checked
Temporary Access Pass (Multi-use)	unchecked
Password + Microsoft Authenticator (Push Notification)	checked
Password + Software OATH token	unchecked
Password + Hardware OATH token	unchecked
Password + SMS	unchecked
Password + Voice	unchecked
Federated Multifactor	unchecked

Sidebar - Authentication Methods

The screenshot displays four windows from the Azure AD Authentication methods Policies interface:

- Manage migration:** Shows a table mapping legacy authentication methods to new ones. Most methods map to "All users" and are enabled.
- Report suspicious activity:** Settings for reporting suspicious activity. State is set to Enabled, Target is All users, Reporting code is 0, and System-preferred multifactor authentication is also set to Enabled.
- Temporary Access Pass settings:** Configure TAP settings. General options include Minimum lifetime (10 minutes), Maximum lifetime (1 hour), Default lifetime (30 minutes), One-time (No), and Length (30 characters).
- Microsoft Authenticator settings:** Configuration for Microsoft Authenticator OTP. It includes sections for push notifications, geographic location, and companion applications. Status for most features is set to Enabled, while Microsoft Authenticator on companion applications is Microsoft managed.

Sidebar - Self-Service Password Reset

The screenshot shows the 'Password reset | Authentication methods' page in the Azure AD for workforce portal. The left sidebar has sections like 'Diagnose and solve problems', 'Manage' (Properties, Authentication methods, Registration, Notifications, Customization, On-premises integration, Administrator Policy), 'Activity' (Audit logs, Usage & insights), and 'Troubleshooting + Support'. The main area shows 'Authentication Methods for SSPR and Sign-in' with a requirement of 'Number of methods required to reset: 2'. It lists available methods: Mobile app notification (checked), Mobile app code (checked), Email (checked), Mobile phone (checked), Office phone (unchecked), and Security questions (unchecked).

<https://aka.ms/sspr>

The screenshot shows the Microsoft self-service password reset page at <https://aka.ms/sspr>. It asks 'Who are you?' and provides a text input field for 'Email or Username' with an example. Below it is a CAPTCHA image showing the text 'YVkJMV' and a text input field for 'Enter the characters in the picture or the words in the audio.' There are 'Next' and 'Cancel' buttons at the bottom.

- 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

Grant access

Require multifactor authentication ⓘ

Require authentication strength ⓘ

Require device to be marked as compliant ⓘ

Require Hybrid Microsoft Entra joined device ⓘ

Require approved client app ⓘ
[See list of approved client apps](#)

Require app protection policy ⓘ
[See list of policy protected client apps](#)

Require password change ⓘ

Terms of Use - All Users

For multiple controls

Require all the selected controls

Require one of the selected controls

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

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) ▾

i 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)

i 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... ▾

i 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

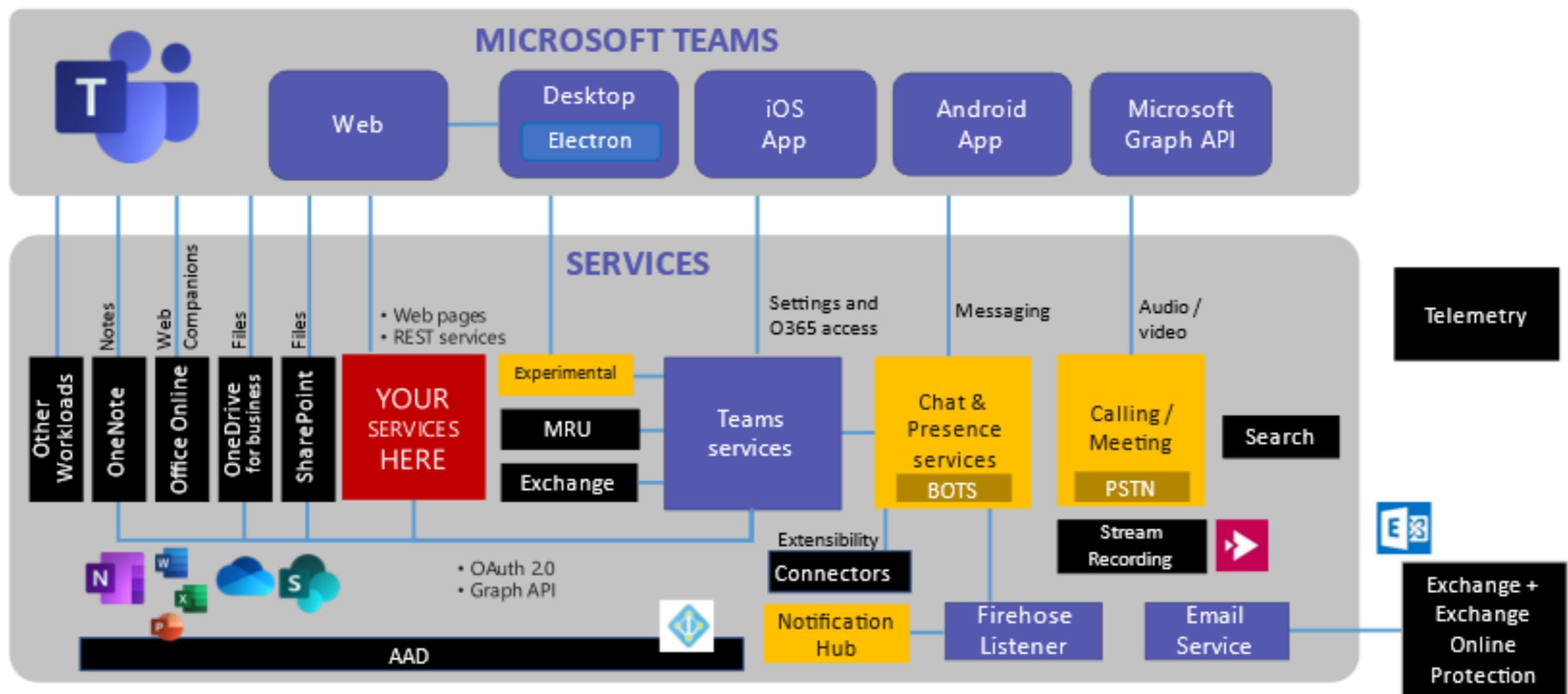
[See list of approved client apps](#)

⚠ You should no longer use "Require approved client app", as we will soon stop updating it. [Learn more](#)

Key

- Microsoft Teams
- Skype services
- Azure and O365

Microsoft Teams Architecture



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

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

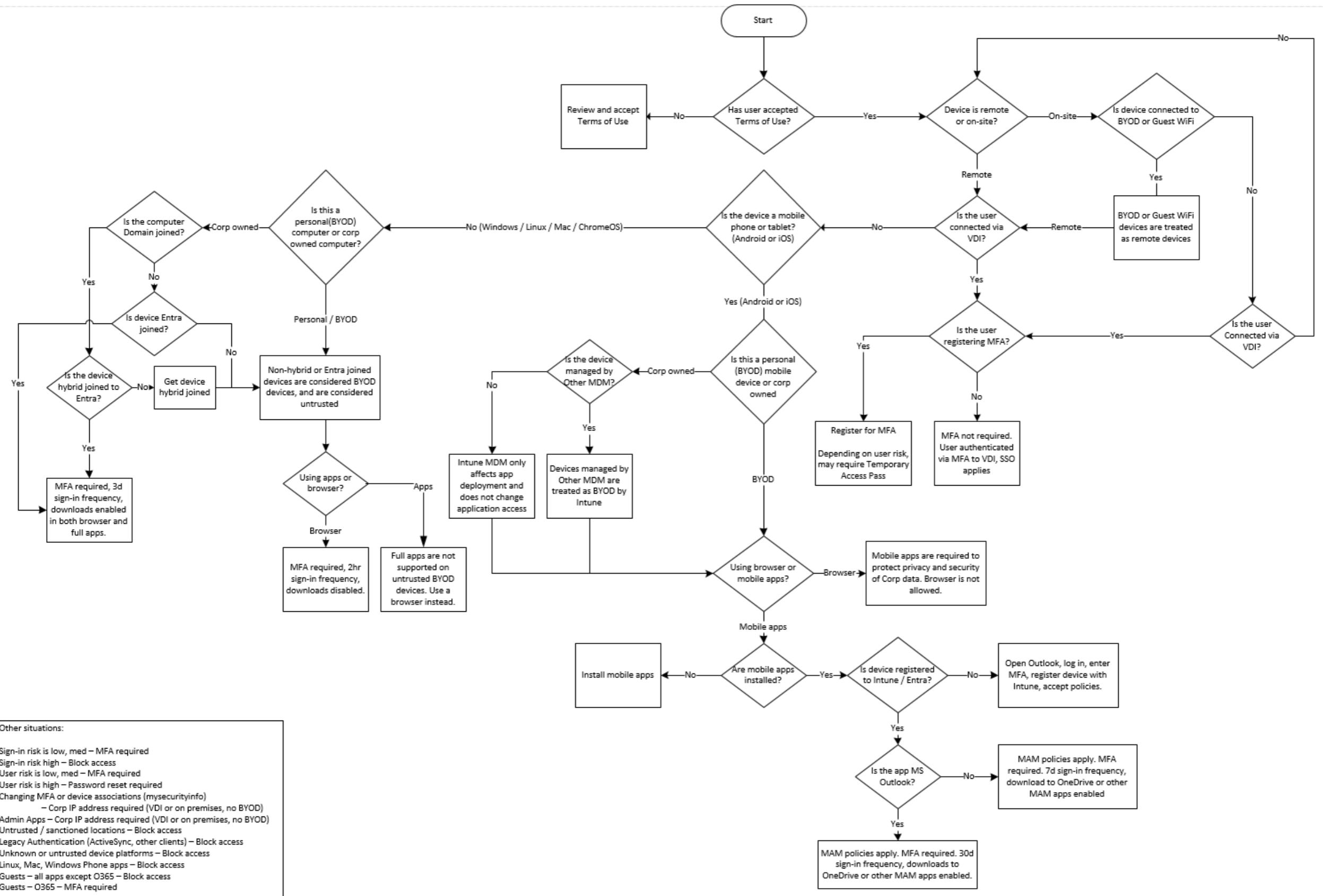
Name	Address range	Country
Corp	192.168.0.0/16, 172.16.0.0/12, 10.0.0.0/8	
PAW	192.168.42.0/24	
Canada		Canada
US		US
Five Eyes		Canada, US, UK, Australia, New Zealand
Nine Eyes		Five Eyes + Denmark, France, Netherlands, Norway
Fourteen Eyes		Nine Eyes + Belgium, Germany, Italy, Spain, Sweden
Untrusted (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 authentication

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					Require auth strength: Corp Approved MFA	Use Conditional Access App Control: Block downloads Sign-in frequency: 2h	Disable resilience defaults
Block Guest Global Apps (exc 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 (exc PAW)	On	All Users	BreakGlass Admin	Azure AD Identity Governance - Enrollment 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	All cloud apps				Include Any Exclude PAW			Block			
Block Legacy Auth	On	All Users		All cloud apps					Legacy Auth: Exchange ActiveSync 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	Office 365			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				macOS, Linux	Include Any Exclude Corp	Browser			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					Include Any Exclude Corp	Mobile apps and desktop clients			Require auth strength: Corp Approved MFA	Use Conditional Access App Control: Block downloads Sign-in frequency: Never	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	Use Conditional Access App Control: Monitor Sign-in frequency: 7d	Require device to be marked as compliant 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	Sign-in frequency: 30d	Use app enforced restrictions
Grant Off Prem All Users (Windows Browser AADI)	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	Use Conditional Access App Control: Monitor only Sign-in frequency: 3d	Disable resilience defaults
Grant Off Prem All Users (Windows Browser HAIDI)	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 "ServerAD"		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 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 AADI)	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	Sign-in frequency: 3d	Disable resilience defaults
Grant Off Prem All Users (Windows Apps HAIDI)	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 "ServerAD"		Require auth strength: Corp Approved MFA Require device to be marked as compliant	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	Exclude device.isCompliant -eq True and device.deviceOwnership -eq "Company" -and [device.trustType -eq "AzureAD" -or device.trustType -eq "ServerAD"]		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	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	Persistent browser session: Never
Session Disable Browser Persistence	On	All Users	BreakGlass Admin	All cloud apps					Include Any	Browser			Grant	Persistent browser session: Never	
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						
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	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

Risky Sign-in Details

User's risk report User's sign-ins User's risky sign-ins User's risk detections Sign-in's risk detections ...

Basic info Device info Risk info Multifactor authentication info **Conditional Access** Report-only

Policy Name ↑↓	Grant Controls ↑↓	Session Controls ↑↓	Result ↑↓
Block unknown or unsupported platform	Block		Failure
Sign In Risk - Medium - MFA	Require authentication strength		Failure
Block High Risk Admin tools	Block		Failure

Risky Sign-in Details

User's risk report User's sign-ins

Basic info **Device info** Risk info

Device ID	
Browser	Rich Client 0.1.28
Operating System	
Compliant	No
Managed	No
Join Type	

- 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

Home >

Conditional Access | Overview Microsoft Entra ID

[Create new policy](#) [Create new policy from templates](#) [Refresh](#) [Got feedback?](#)

[Overview](#) [Getting started](#) [Overview](#) [Coverage](#) [Monitoring \(Preview\)](#) [Tutorials](#)

Top accessed applications without Conditional Access coverage in the last 7 days ⓘ

Application ↑	Users without coverage ↑	Percentage of users not covered ↑
Microsoft Edge	105 out of 2320	5%
Microsoft Edge Enterprise New Tab Page	0 out of 2021	0%
Microsoft Office	7 out of 1165	1%
Microsoft Authentication Broker	131 out of 136	96%
Microsoft Intune Windows Agent	97 out of 102	95%
SharePoint Online Web Client Extensibility	1 out of 16	6%
Microsoft Whiteboard Services	0 out of 2	0%

Sign-in identifier

User type	Guest
Cross tenant access type	B2B collaboration
Application	SharePoint Online Web Client Extensibility
Application ID	
Resource	Office 365 SharePoint Online

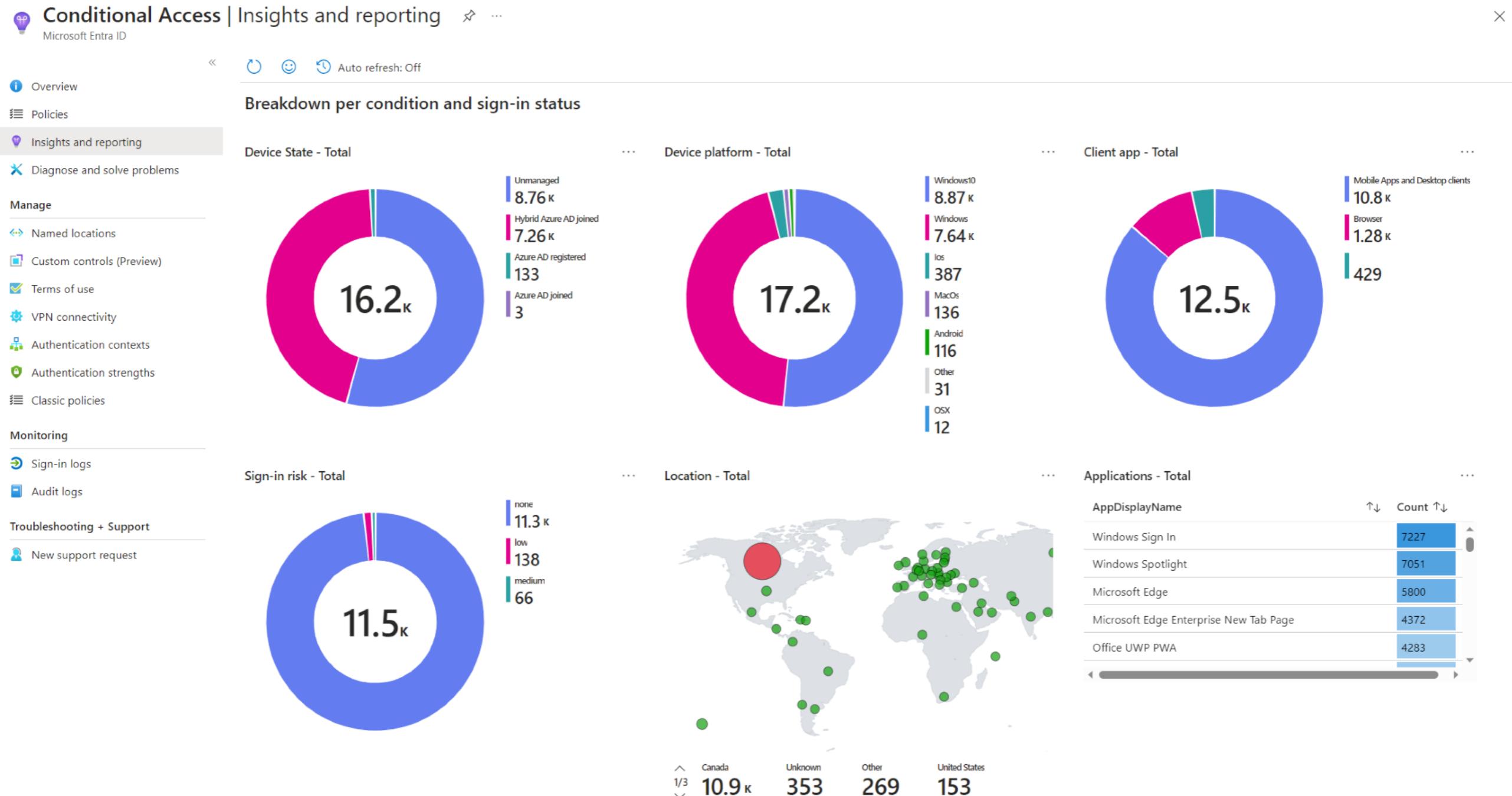
Top accessed applications with Conditional Access coverage in the last 7 days ⓘ

Application ↑	Users with coverage ↑	Percentage of users covered ↑
Windows Spotlight	2391 out of 2391	100%
Microsoft Edge	2313 out of 2320	100%
Microsoft Edge Enterprise New Tab Page	2021 out of 2021	100%
Office UWP PWA	1994 out of 1994	100%
Microsoft Bing Search for Microsoft Edge	1990 out of 1990	100%
Microsoft Office	1165 out of 1165	100%
Microsoft Application Command Service	824 out of 824	100%

New support request

Troubleshooting - Insights

Home > Conditional Access

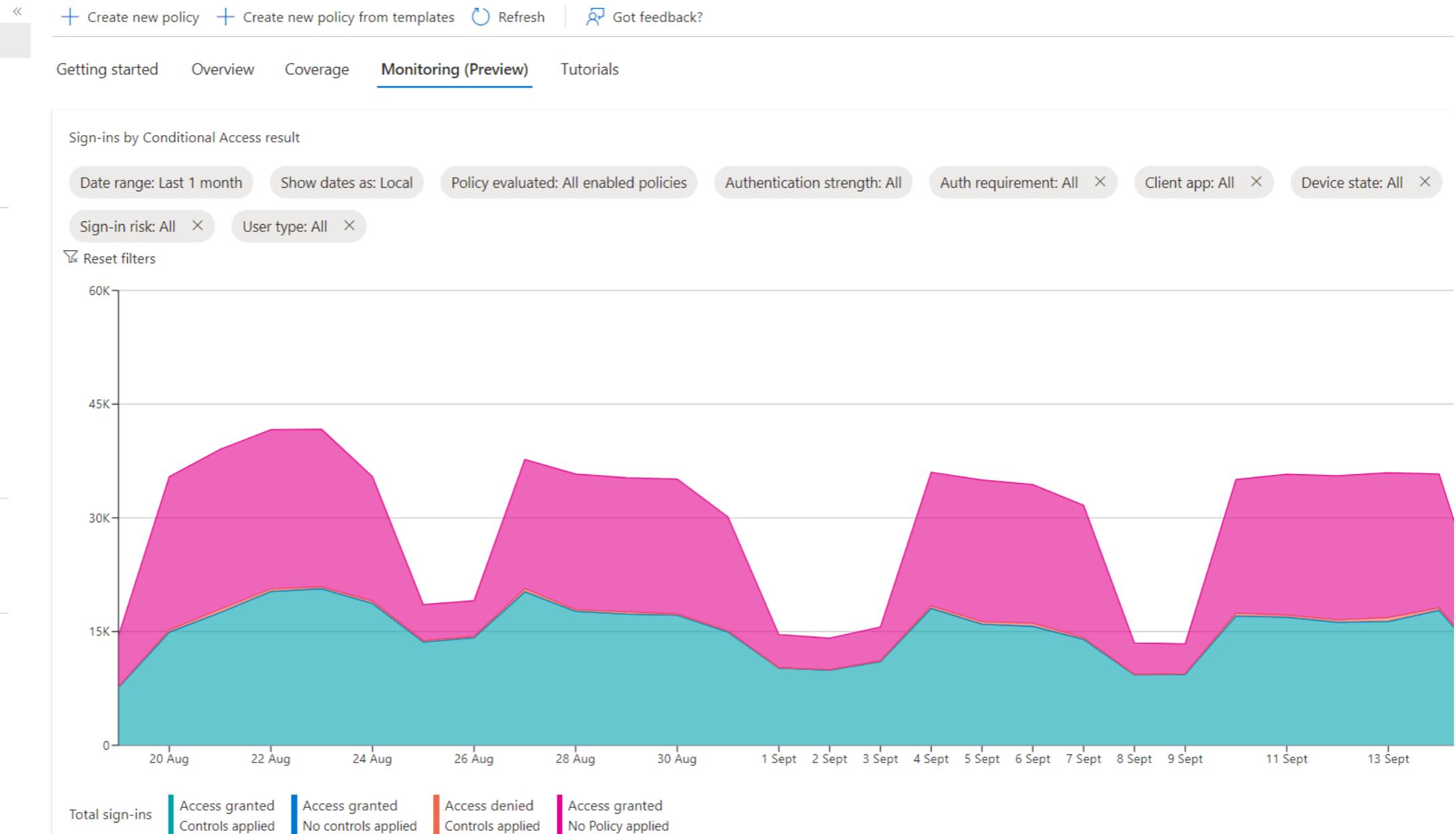


Troubleshooting - Monitoring

Home >

Conditional Access | Overview

Microsoft Entra ID



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.

Edit role setting - Global Administrator ...

Privileged Identity Management | Azure AD roles

Activation Assignment Notification

Activation maximum duration (hours)

----- 8 -----

On activation, require

None
 Azure MFA
 Azure AD Conditional Access authentication context

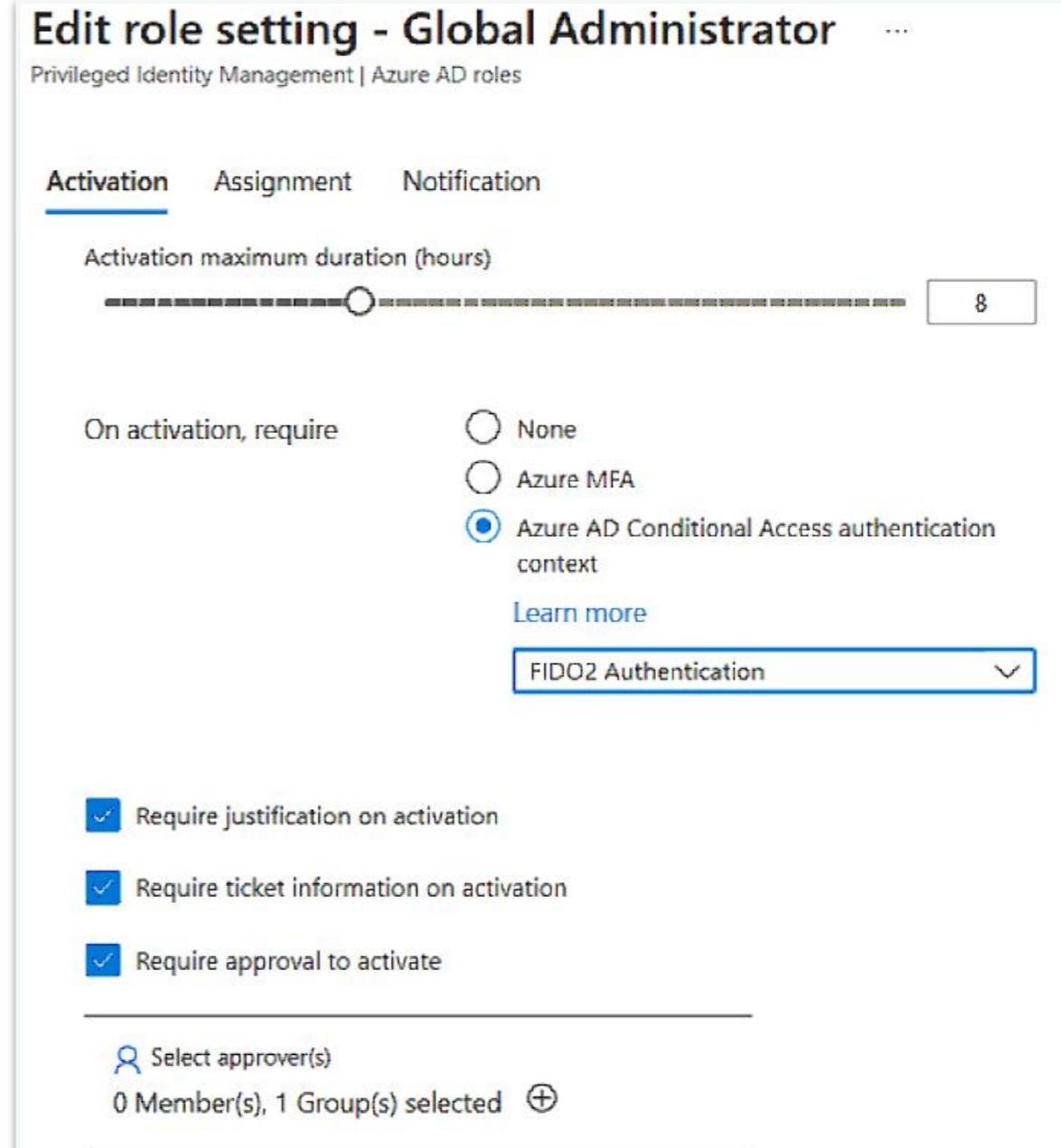
[Learn more](#)

FIDO2 Authentication

Require justification on activation
 Require ticket information on activation
 Require approval to activate

Select approver(s)

0 Member(s), 1 Group(s) selected [+](#)



Sensitivity Labels

Define external sharing and conditional access settings

Control who can share SharePoint content with people outside your organization and decide whether users can access labeled sites from unmanaged devices.

Control external sharing from labeled SharePoint sites

When this label is applied to a SharePoint site, these settings will replace existing external sharing settings configured for the site.

Use Azure AD Conditional Access to protect labeled SharePoint sites

You can either control the level of access users have from unmanaged devices or select an existing authentication context to enforce restrictions.

- Determine whether users can access SharePoint sites from unmanaged devices (which are devices that aren't [hybrid Azure AD joined](#) or enrolled in Intune).

(i) For this setting to work, you must also configure the SharePoint feature that blocks or limits access to SharePoint files from unmanaged devices. [Learn more](#)

- Allow full access from desktop apps, mobile apps, and the web

- Allow limited, web-only access (i)

- Block access (i)

- Choose an existing authentication context (preview). Each context has an Azure AD Conditional Access policy applied to enforce restrictions. [Learn more about authentication context](#)

HAADJ+MFA -

Define external sharing and conditional access settings

Control who can share SharePoint content with people outside your organization and decide whether users can access labeled sites from unmanaged devices.

Control external sharing from labeled SharePoint sites

When this label is applied to a SharePoint site, these settings will replace existing external sharing settings configured for the site.

Use Azure AD Conditional Access to protect labeled SharePoint sites

You can either control the level of access users have from unmanaged devices or select an existing authentication context to enforce restrictions.

- Determine whether users can access SharePoint sites from unmanaged devices (which are devices that aren't [hybrid Azure AD joined](#) or enrolled in Intune).

(i) For this setting to work, you must also configure the SharePoint feature that blocks or limits access to SharePoint files from unmanaged devices. [Learn more](#)

- Allow full access from desktop apps, mobile apps, and the web

- Allow limited, web-only access (i)

- Block access (i)

- Choose an existing authentication context (preview). Each context has an Azure AD Conditional Access policy applied to enforce restrictions. [Learn more about authentication context](#)

FIDO2 Authentication -

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 physical addresses). Just look for the templates labeled 'Enhanced' to start protecting even more personal data.

Categories	Templates
Financial	Canada Health Information Act (HIA)
Medical and health	Canada Personal Health Information Act (PHIA) - Manitoba
Privacy	Canada Personal Health Act (PHIPA) - Ontario
Custom	

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 sensitive 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 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 only on 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

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	
<input checked="" type="checkbox"/> Exchange email	All distribution groups	Edit
<input checked="" type="checkbox"/> SharePoint sites	All sites	Edit
<input checked="" type="checkbox"/> OneDrive accounts	All accounts and groups	Edit
<input checked="" type="checkbox"/> Teams chat and channel messages	All accounts or distribution groups	Edit
<input checked="" type="checkbox"/> Devices	All users or groups	Edit
<input type="checkbox"/> Cloud Apps	All instances	Edit
<input type="checkbox"/> File shares	All repositories	Edit

[Turn on location to scope](#)

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: i

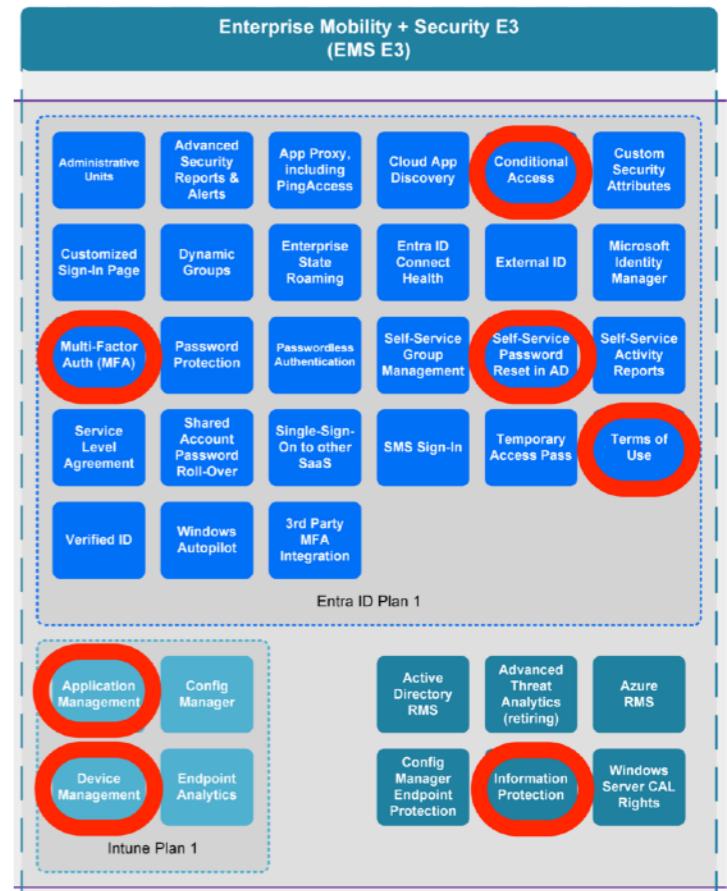
- With people outside my organization
 Only with people inside my organization

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](#)

What about licensing?

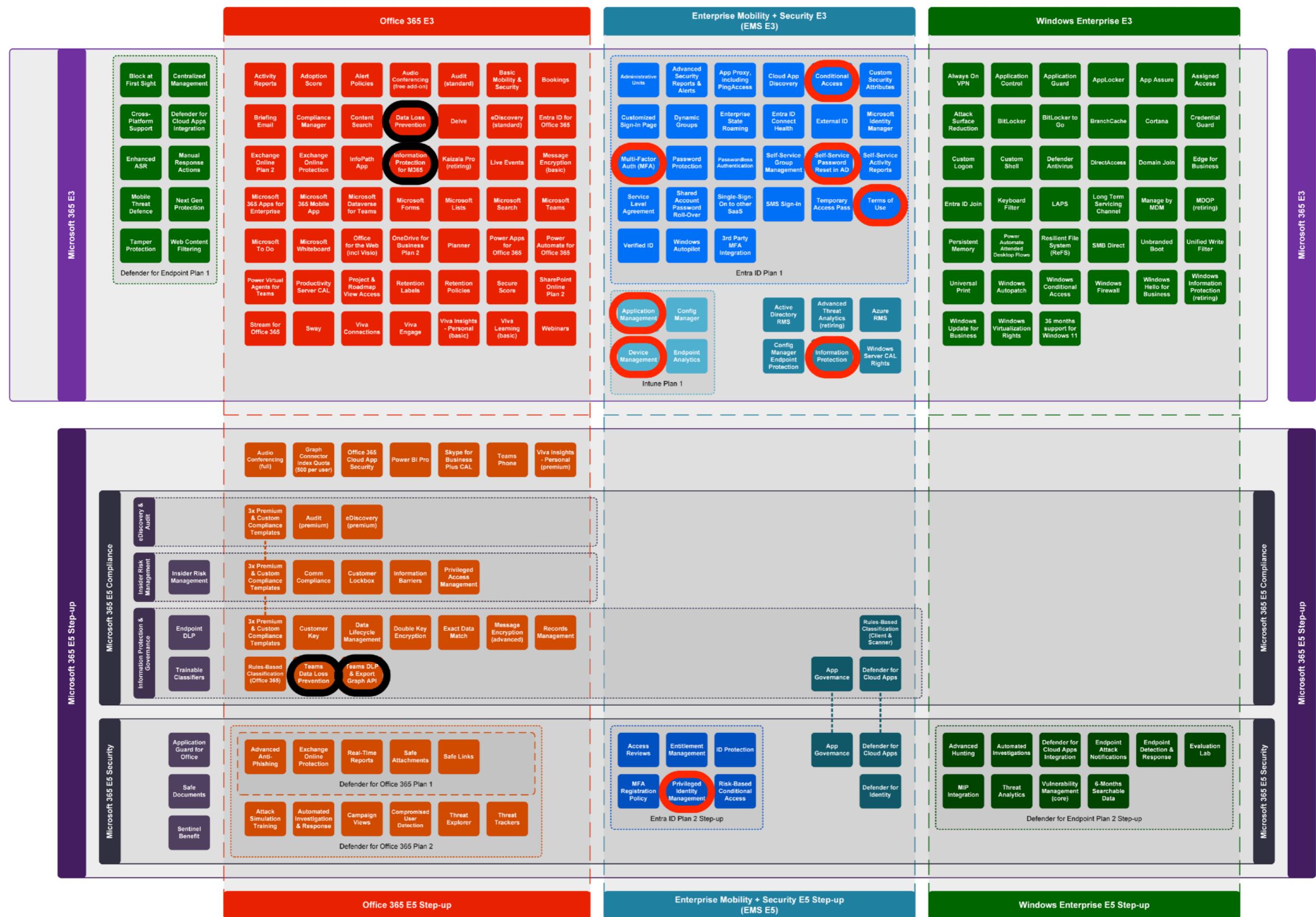
- Entra ID P1 includes:
 - Conditional Access
 - MFA
 - Self-Service Password Reset (SSPR)
 - Terms of Use
- Intune P1 includes:
 - Device management
 - Device compliance (MDM)
 - App Protection (MAM)
- Both are part of M365 Enterprise + Mobility F3/A3/E3
 - Which also includes Information Protection (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



Microsoft 365 Enterprise

July 2023

m365maps.com



Microsoft 365 Enterprise Benefits



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



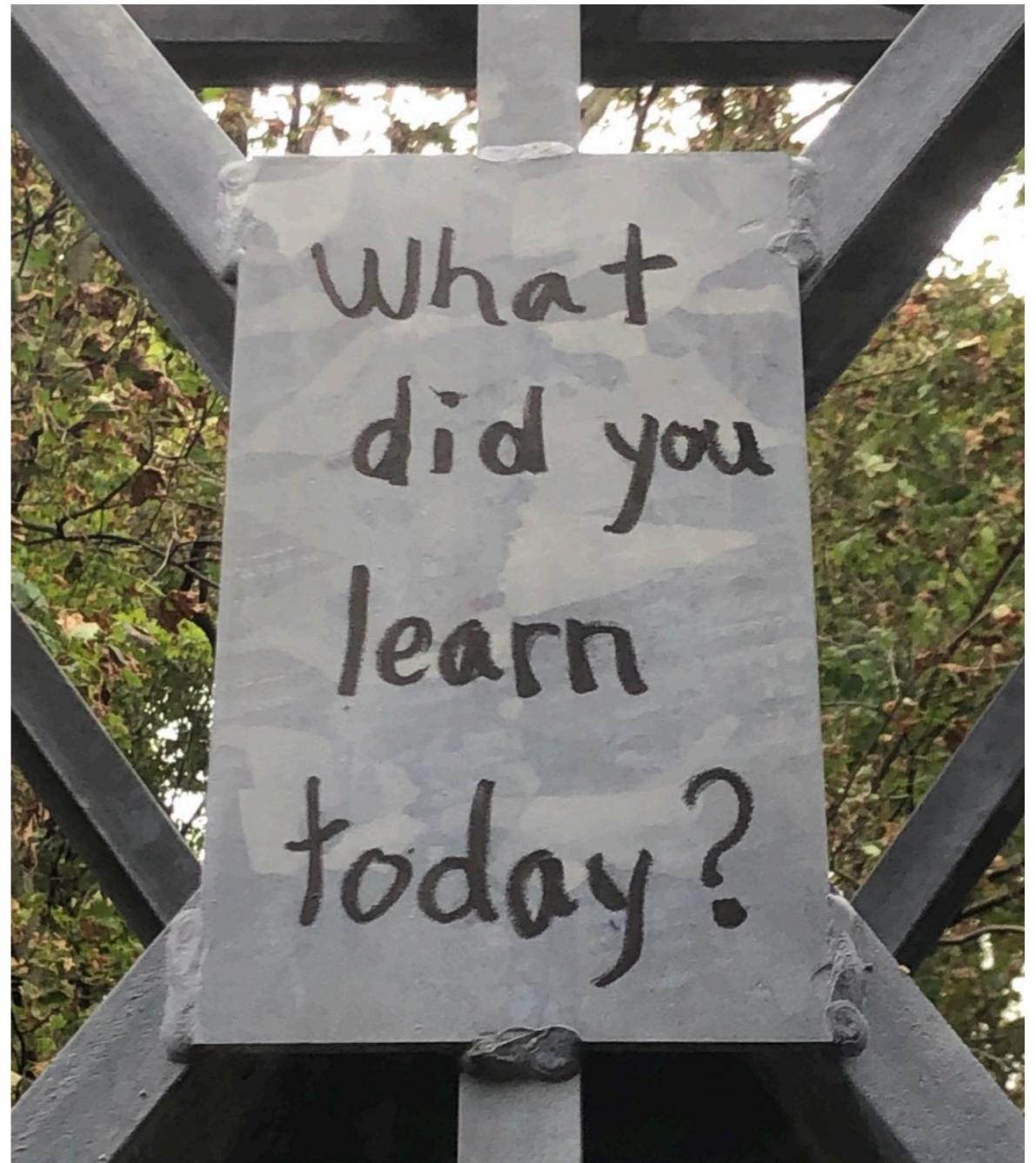
One traditional Office Professional Plus device install for each existing Software Assurance (SA) user, and new users up to the number of existing SA users.



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?



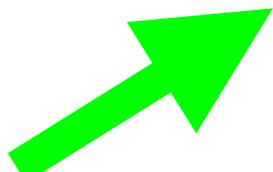
Thank you

Contact Info:

singleusermode@infosec.exchange

don - Hackfest Discord

nixuser23@gmail.com



This QR
code is safe

<https://github.com/nixy23/hackfest2023>



