Unconditionally Conditional

Strong authentication in Microsoft Entra ID (formerly Azure AD)

Don Mallory

BSidesTO - Oct 21, 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
- Example risky sign in
- 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 ~~hope~~ trust

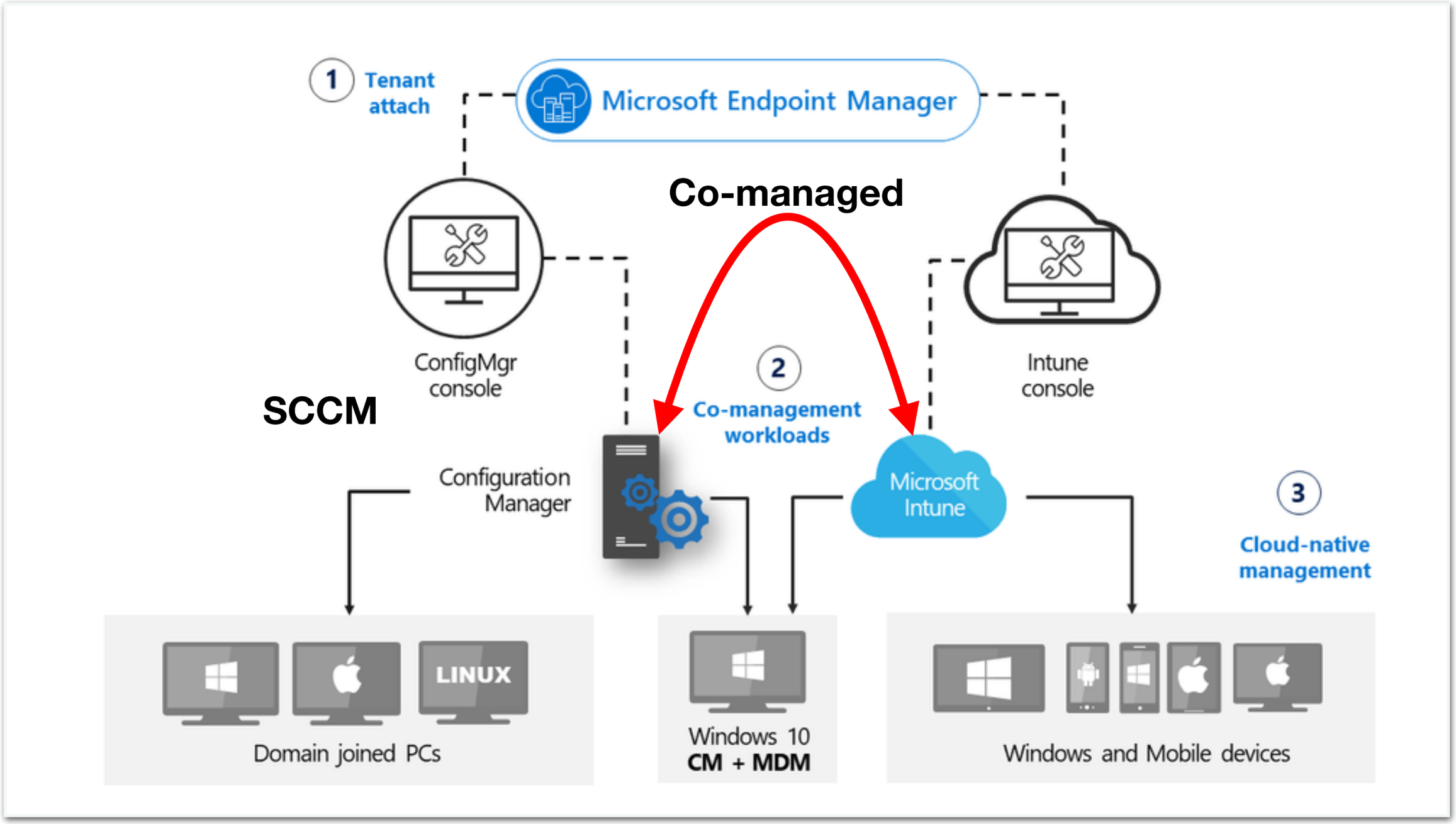
Why should we care?

- 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.

Start with devices



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

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

Device vs App Management

MDM

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

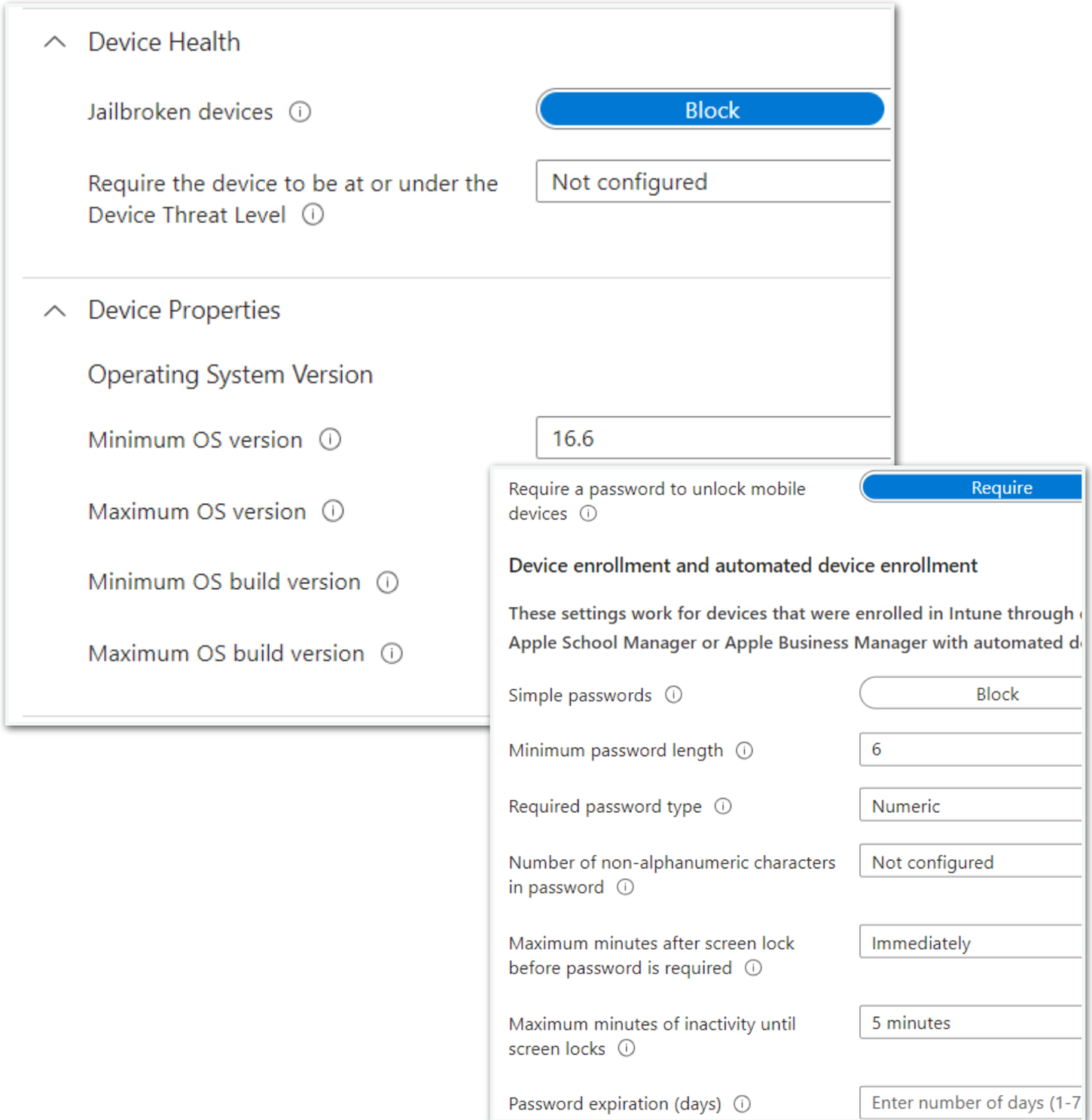
- Device wipe
- App push
- OS & App updates
- App visibility / limits
- Best for Org owned devices

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

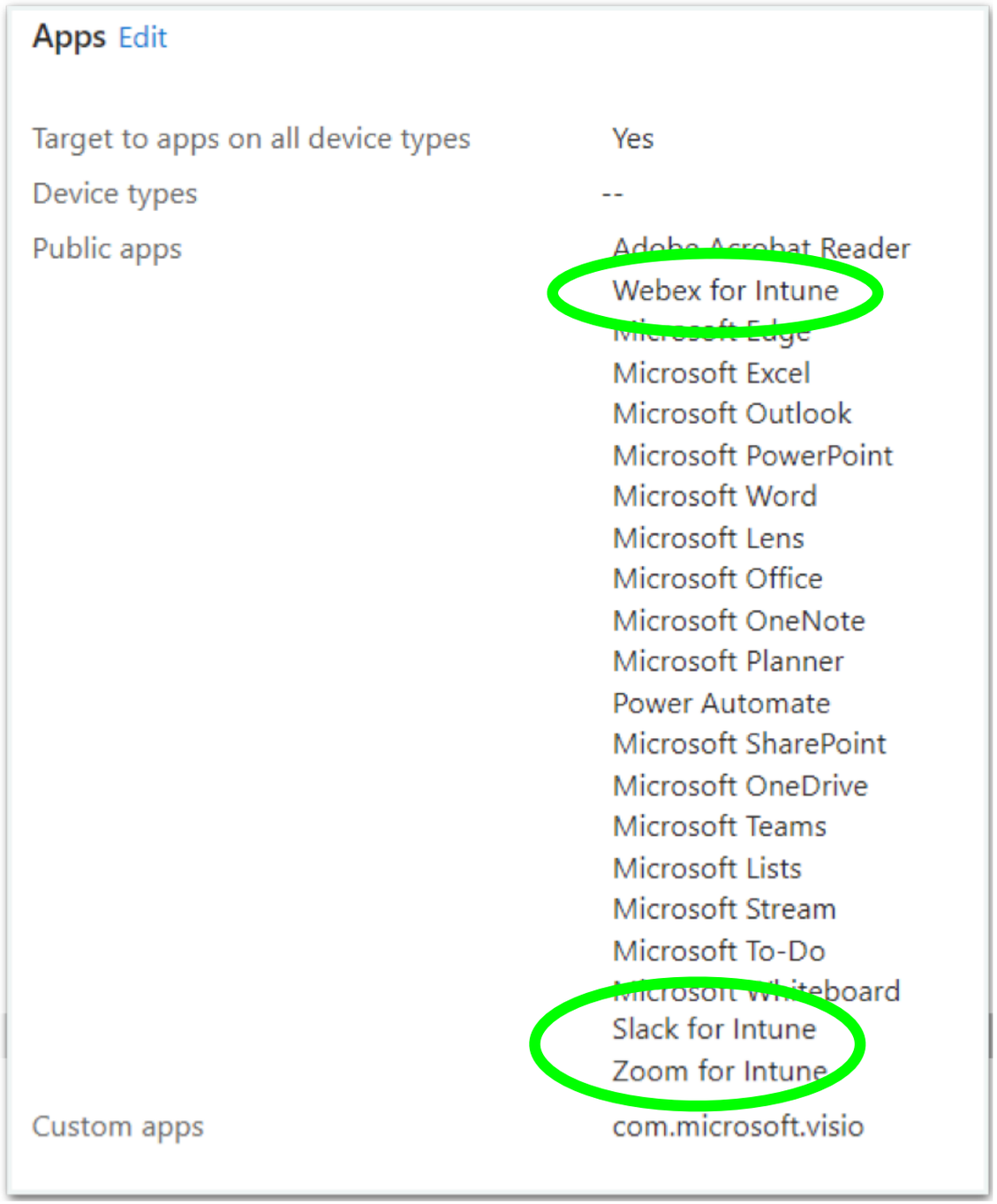
MDM policies



- Different policies for:
  - iOS
  - Android
  - Windows
  - macOS
- Applies to:
  - Jailbreaking
  - OS versions & builds
  - Password/PIN policies
  - Device Encryption
  - Restricted apps
  - Firewalls
  - Anti-malware
- Expects that:
  - Configuration policies will apply first

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

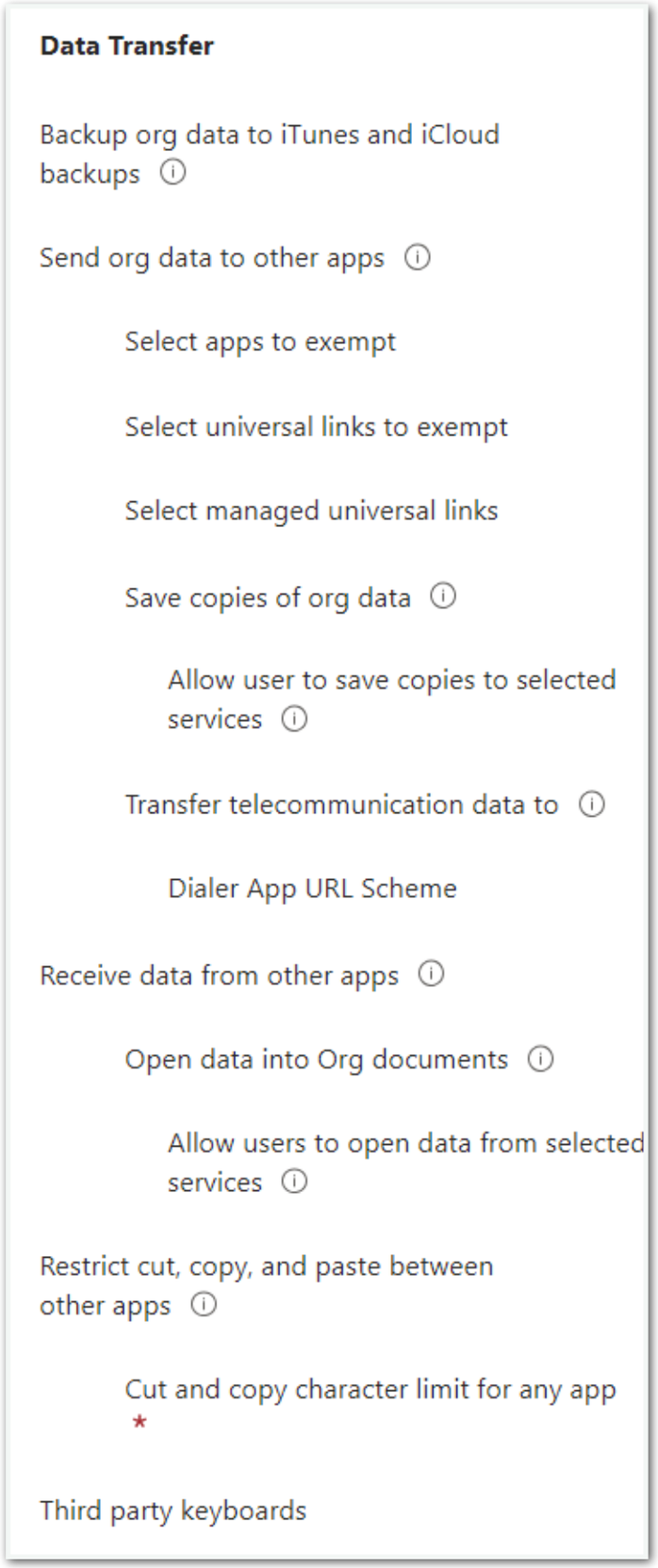
MAM policies - Apps

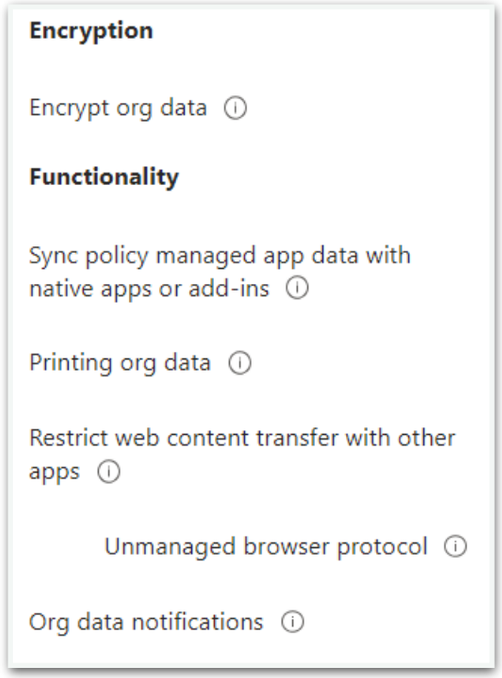


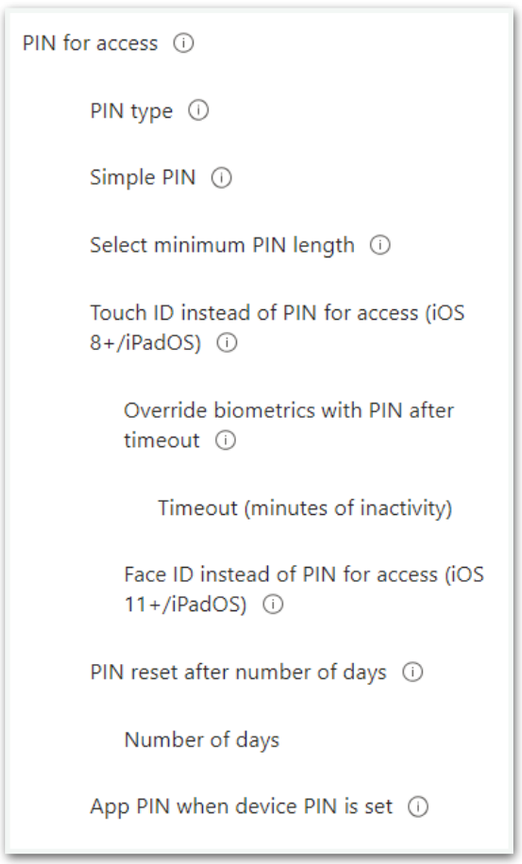
- Protected apps run in a container
- Notice special app versions
- Data outside the container is managed by MDM for enrolled devices

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

MAM policies

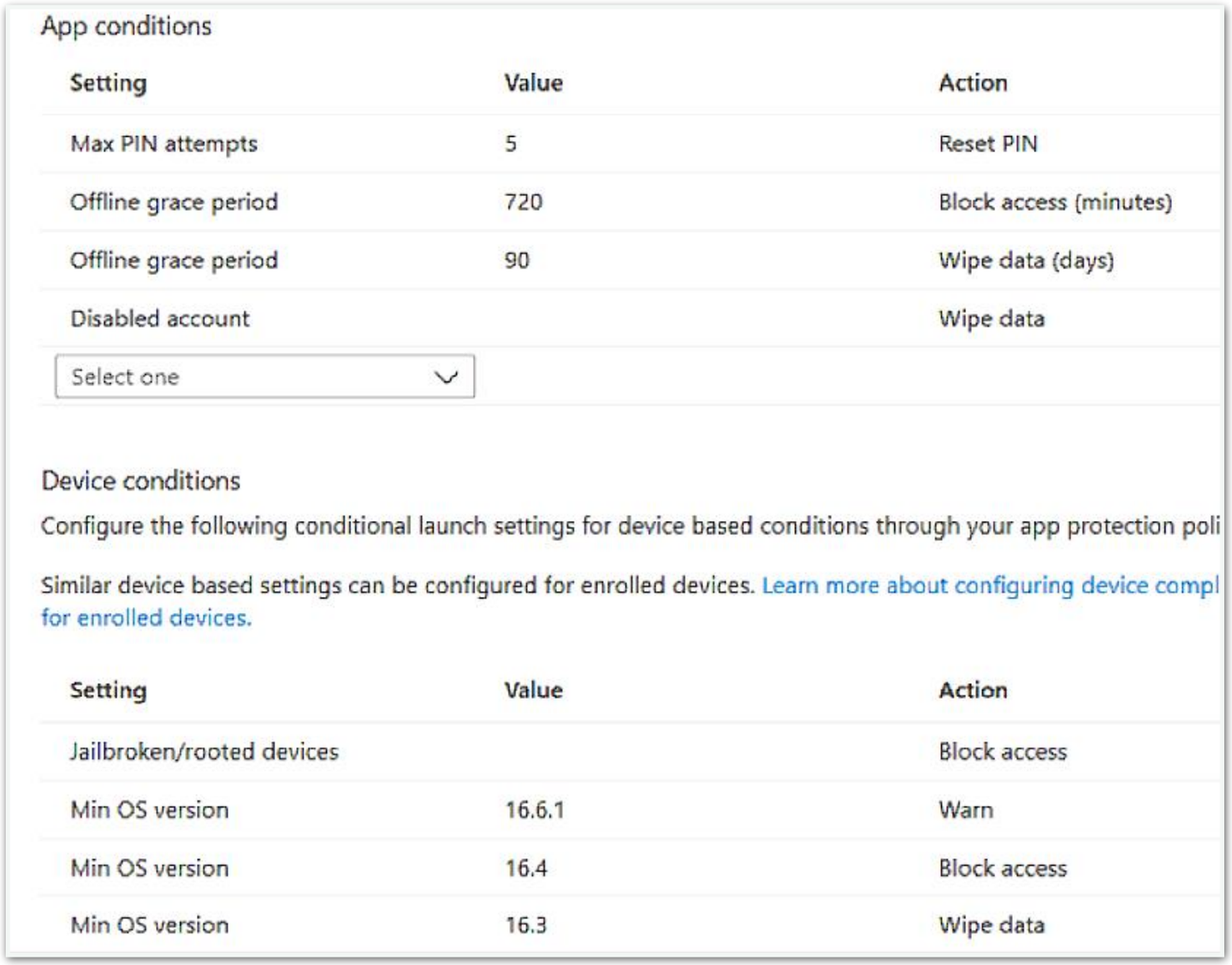






- Org data in the container
- Deny:
  - Backup org data to iTunes/iCloud/ GoogleDrive
  - Copying data out of container apps
  - Syncing org data to native apps
  - Printing
  - 3rd party keyboards
  - Unencrypted data
- Allow
  - Saving to OneDrive, it’s in the container
  - Numeric PIN
  - Biometrics
- Do not:
  - Block notifications
  - Force PIN reset based on time

MAM policies - Conditions



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 poli

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

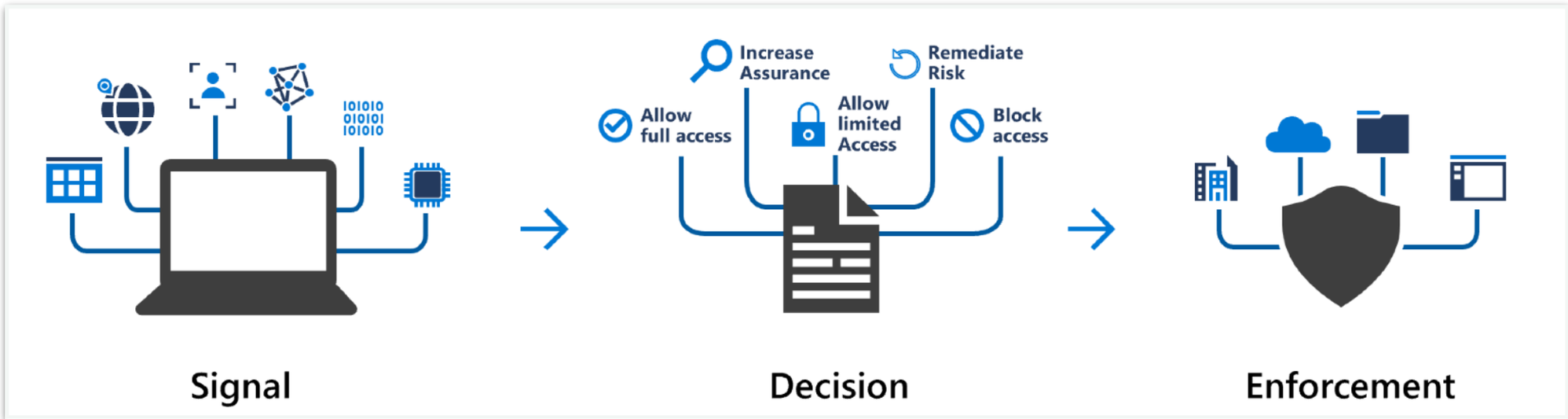
- Settings:
  - Max PIN attempts
  - Office grace period
  - Disabled account
- Conditions:
  - Jailbroken
  - Min OS version
  - SafetyNet Attest (Android only)

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
- 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.

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

Is everybody with me so far?

Putting it all together

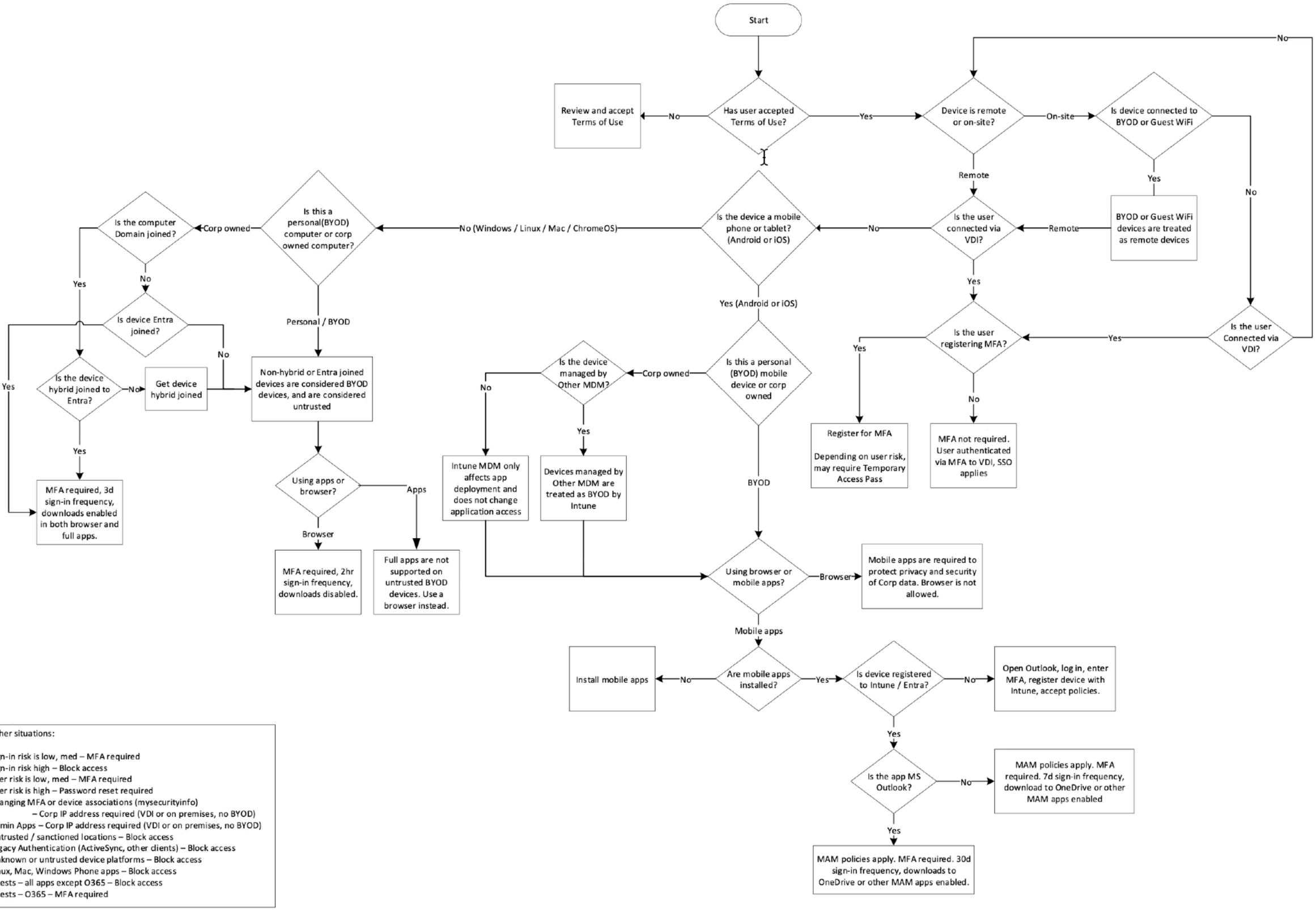
- The closer you are to the data, the more trust you will require
- The less trust in your device, location, or auth, greater friction is applied
- Exclusion vs Inclusion
  - Very important for block and layered policies
- Wide policies work well for session settings
- Narrow policies
  - Ease of troubleshooting
  - 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

Authentication policy flow diagram

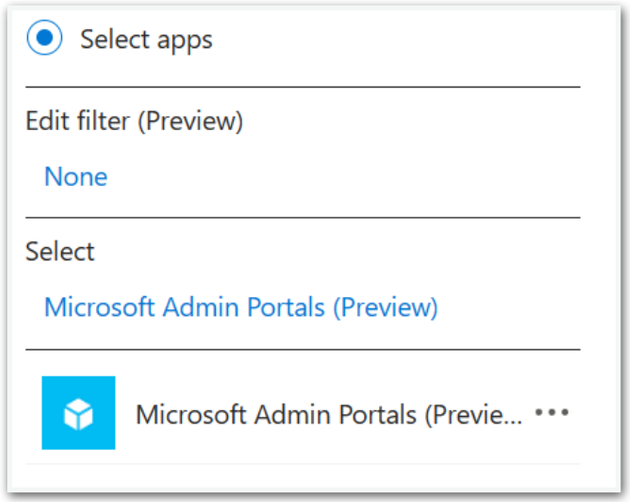


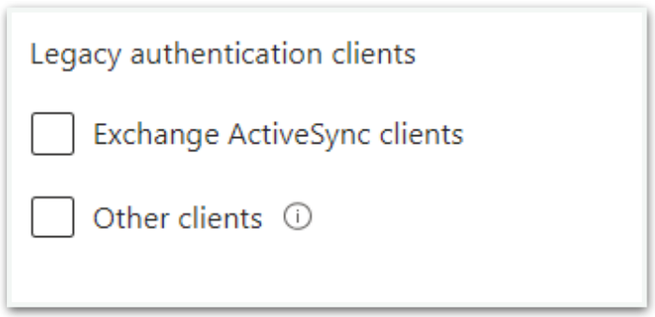
Other situations:

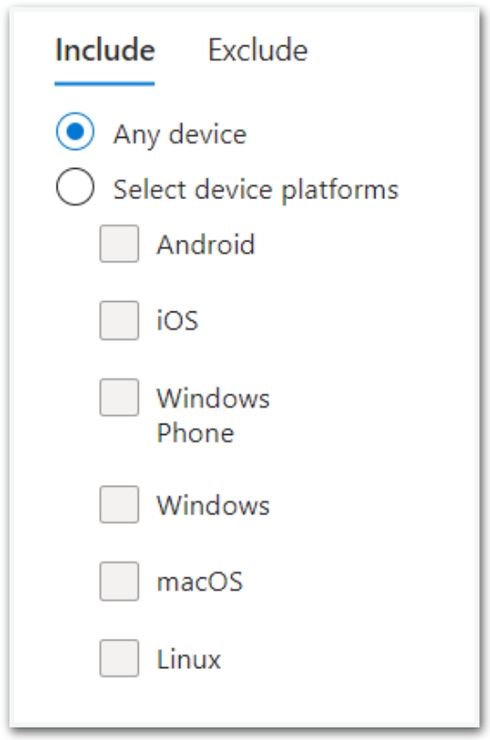
Sign-in risk is low, med – MFA required
Sign-in risk high – Block access
User risk is low, med – MFA required
User risk is high – Password reset required
Changing MFA or device associations (mysecurityinfo)
– Corp IP address required (VDI or on premises, no BYOD)
Admin Apps – Corp IP address required (VDI or on premises, no BYOD)
Untrusted / sanctioned locations – Block access
Legacy Authentication (ActiveSync, other clients) – Block access
Unknown or untrusted device platforms – Block access
Linux, Mac, Windows Phone apps – Block access
Guests – all apps except O365 – Block access
Guests – O365 – MFA required

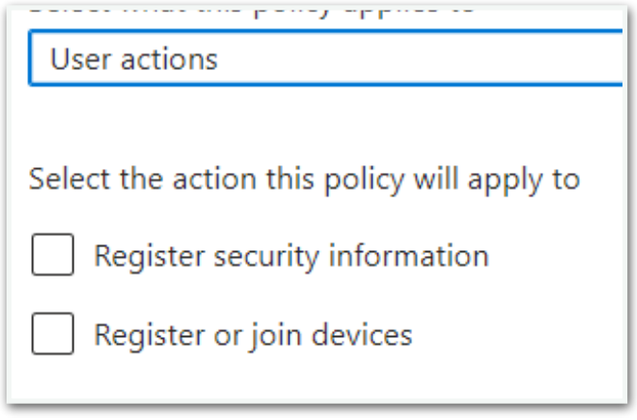
Things to block

- 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









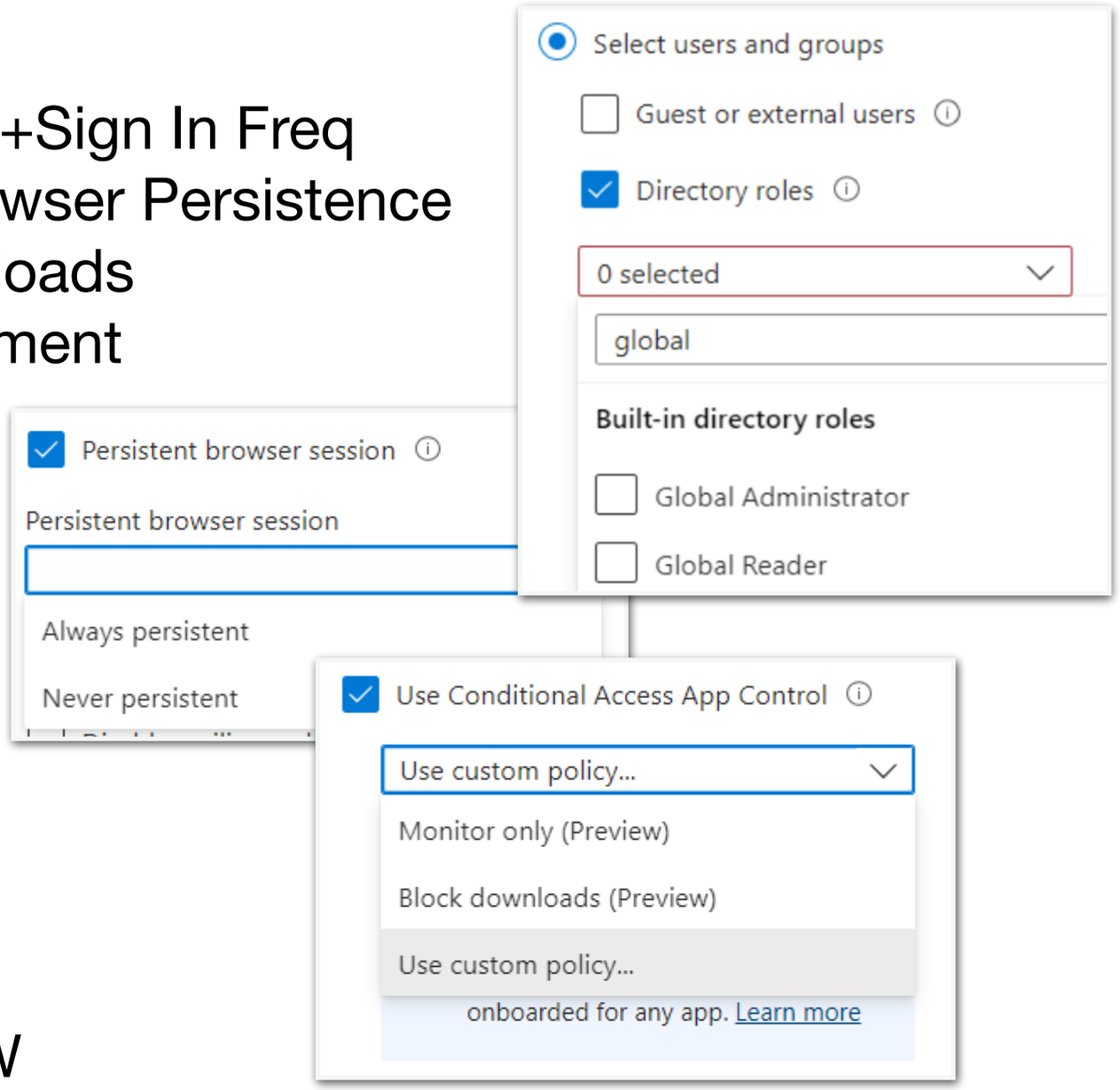
Session, TOU, and risk policies

- 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

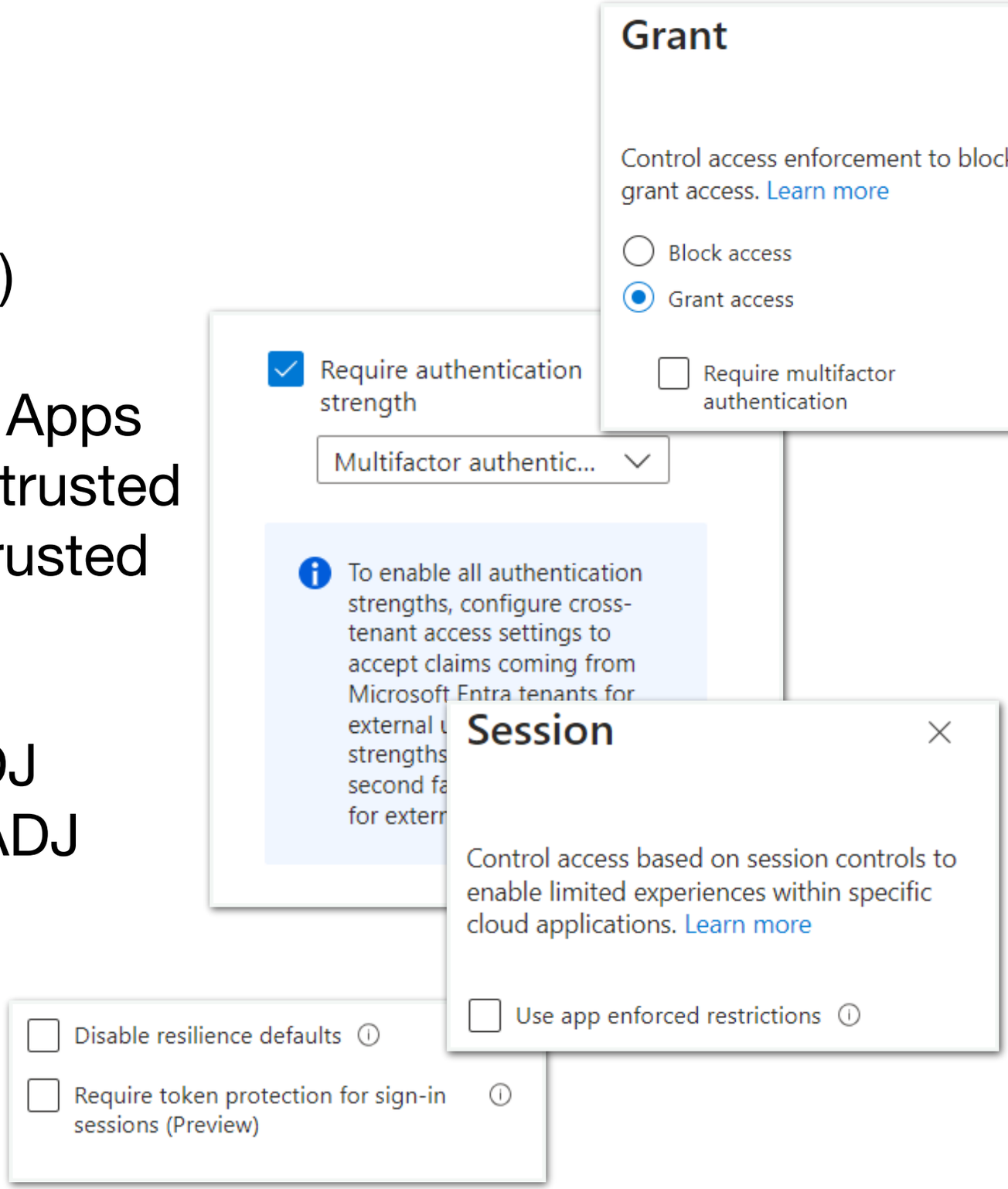
- On Premises
  - Grant On Prem All Users (Windows Apps)
  - Grant On Prem All Users (Windows Browser)

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

Off premises allow policies

- Grant Off Prem All Users
  - Untrusted devices
    - Mobile Apps (excl EXO)
    - 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

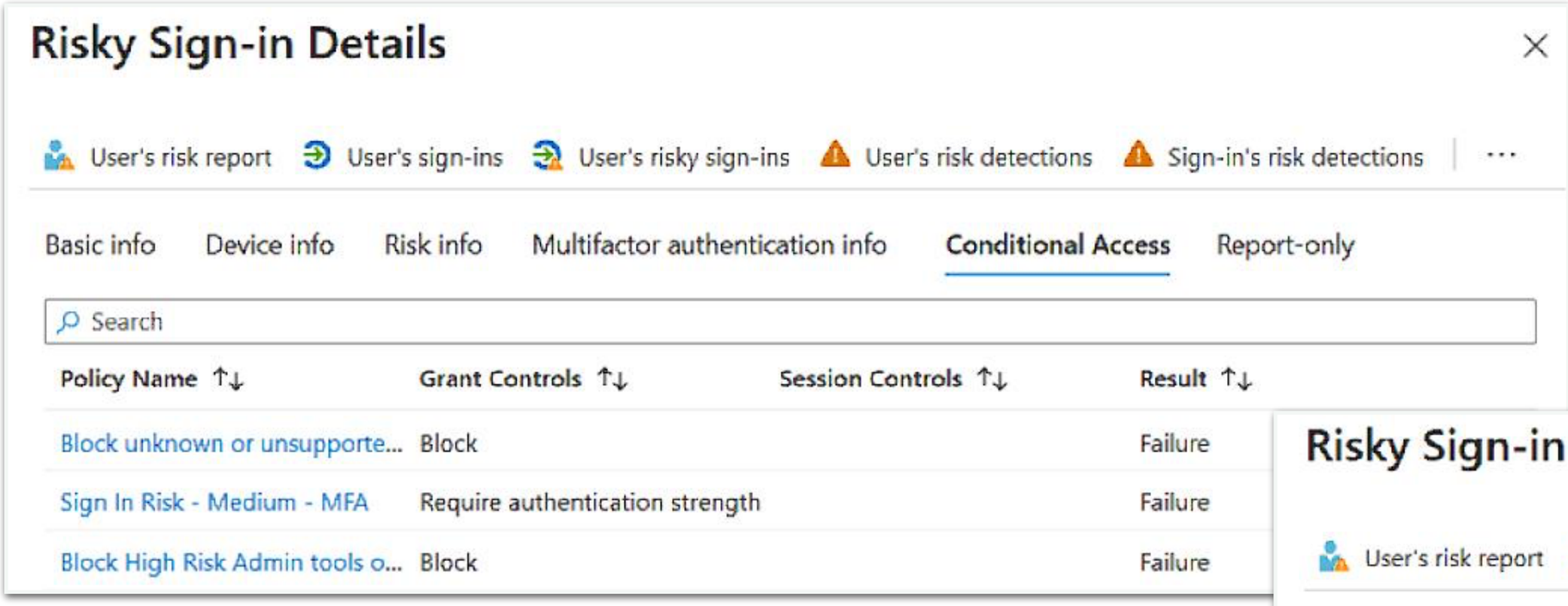
- Block Security Registration Restrictions - Exclude

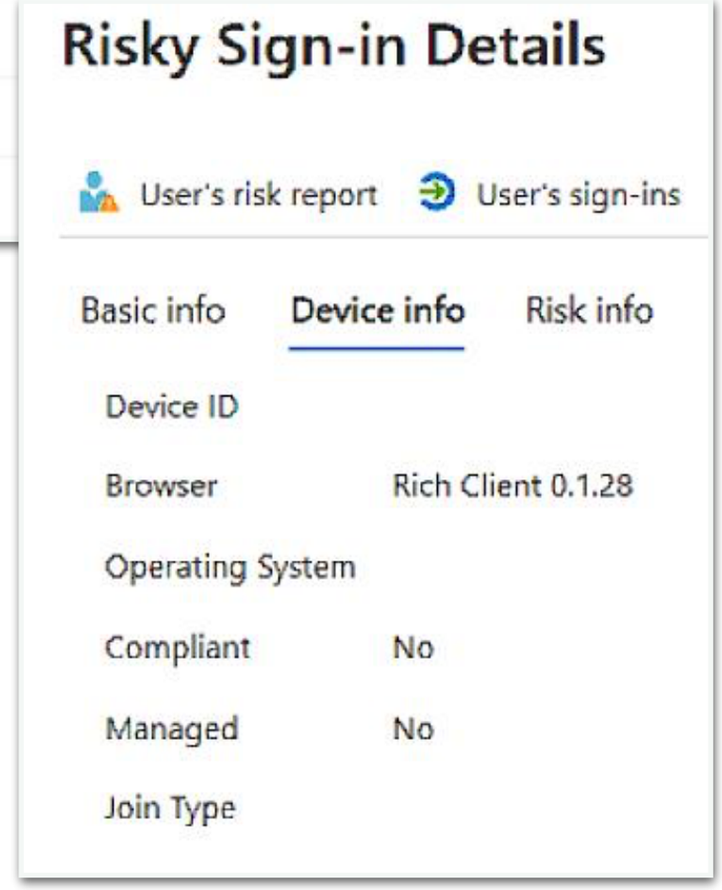
- Other Examples:
  - Grant Off Prem All Users (Mobile Browser Exclude)
  - Grant Off Prem (Windows Apps Unmanaged Exclude)

- Testing, testing, testing…

- Break glass account

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”

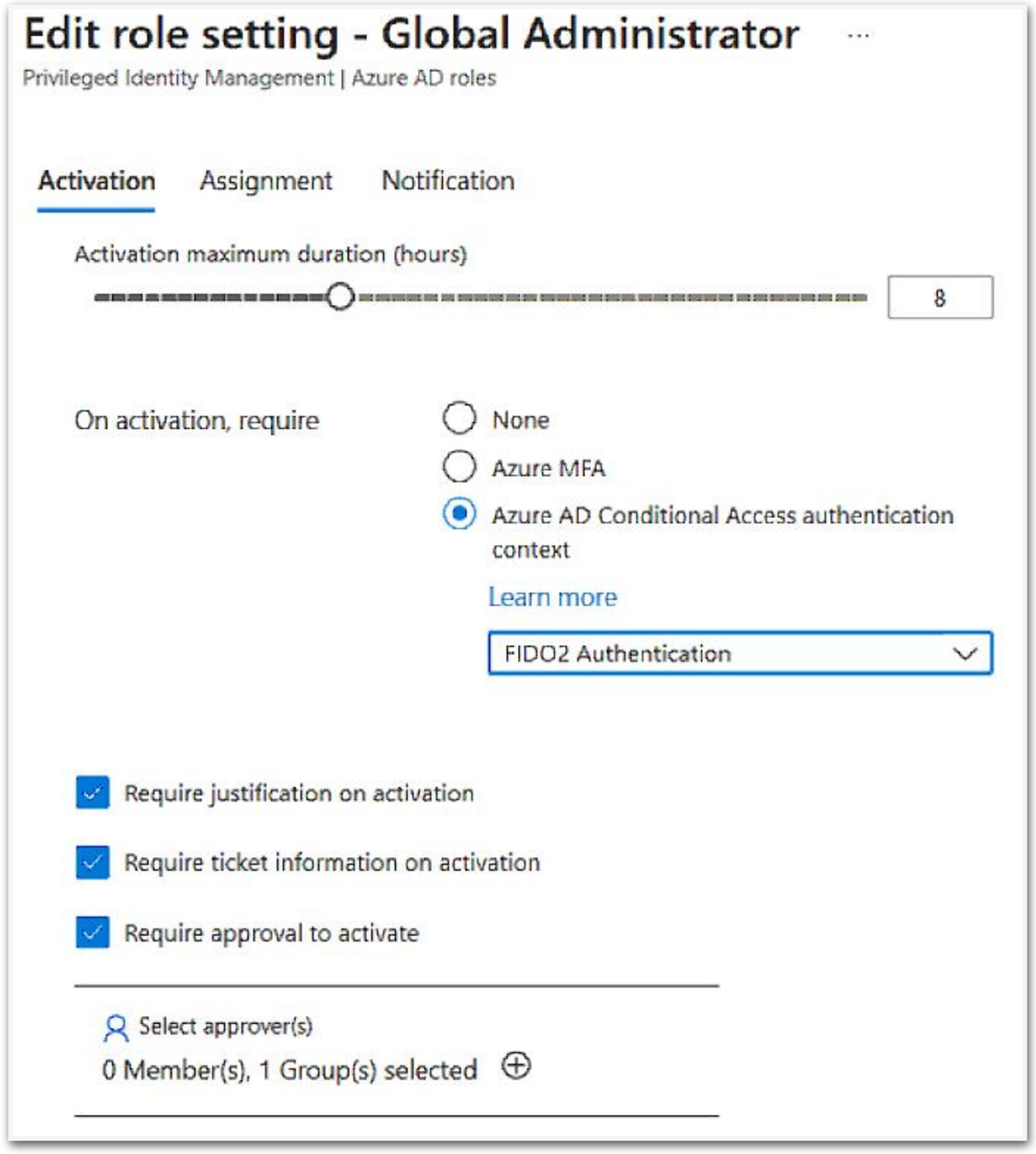
Blueprint for strong authentiction

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		

But wait, there’s more

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

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 joinedor enrolled in Intune).

ⓘ 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

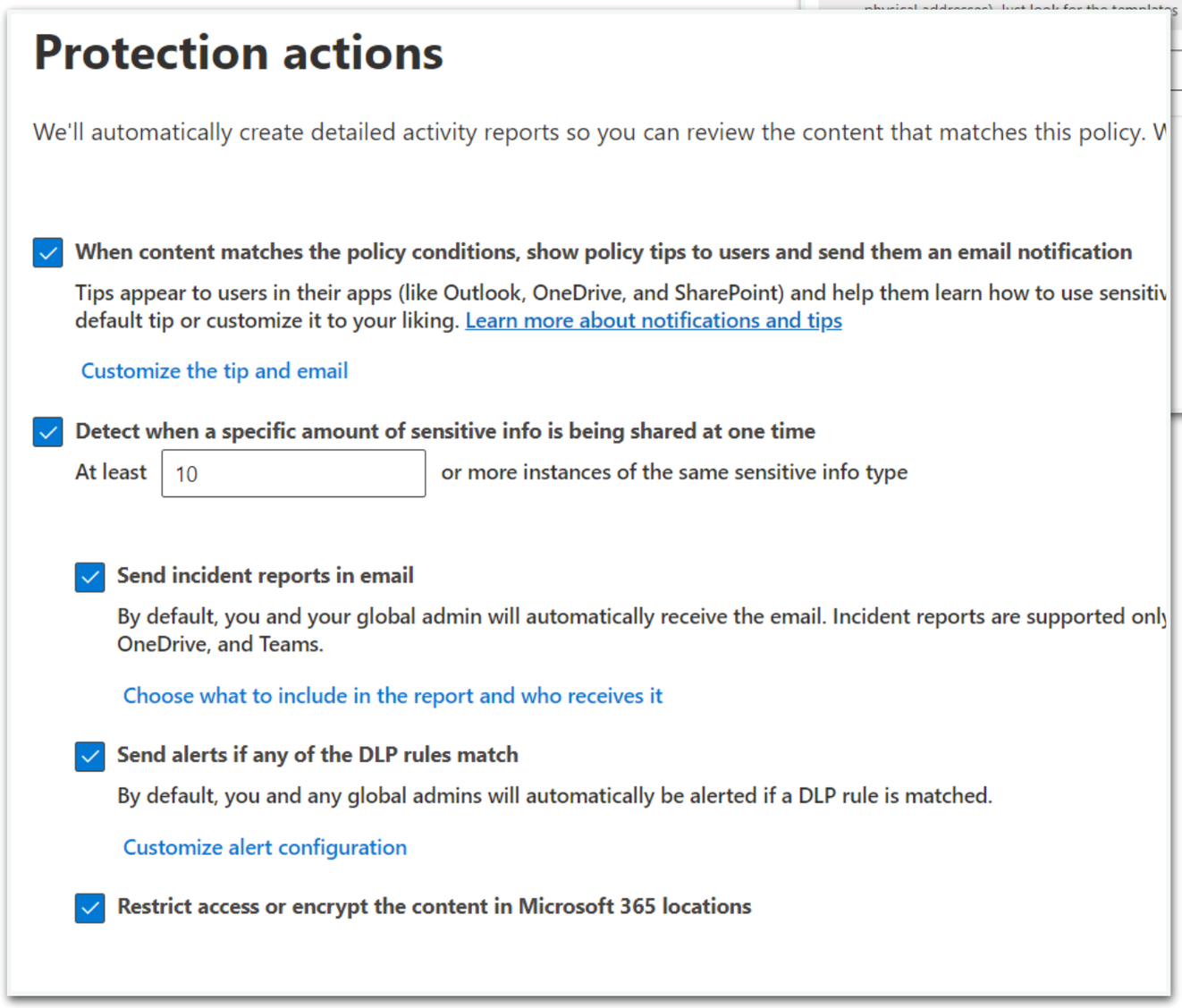
- ◉ Allow full access from desktop apps, mobile apps, and the web
- ○ Allow limited, web-only access ⓘ
- ○ Block access ⓘ

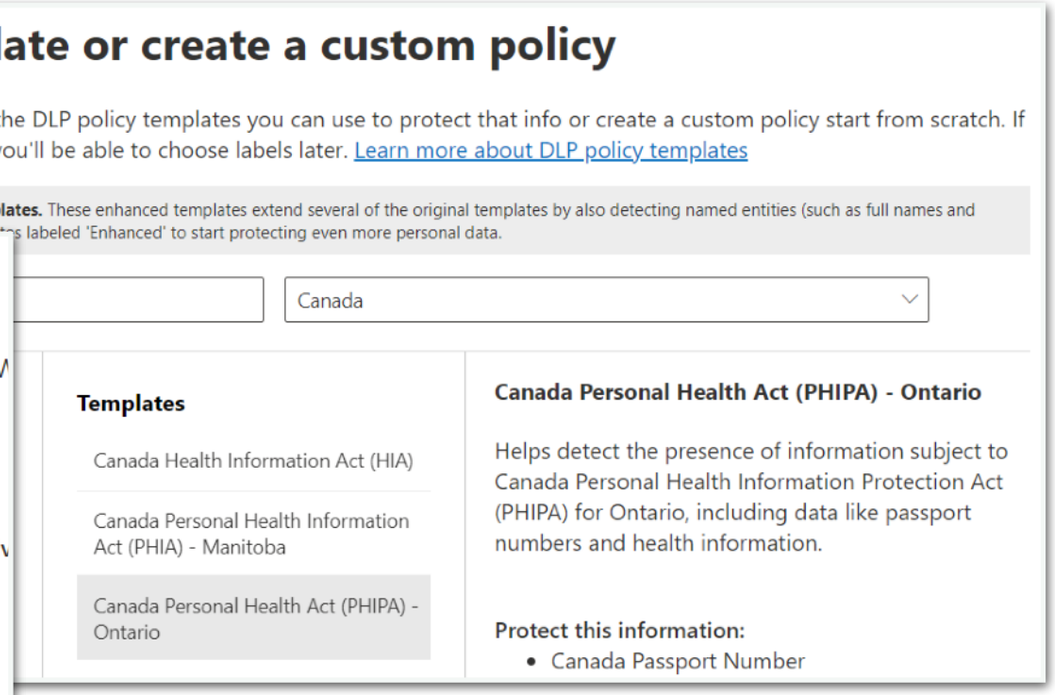
◉ Choose an existing authentication context (preview). Each context has an Azure AD Conditional Access policy applied to enforce restrictions. Learn more about authentication context

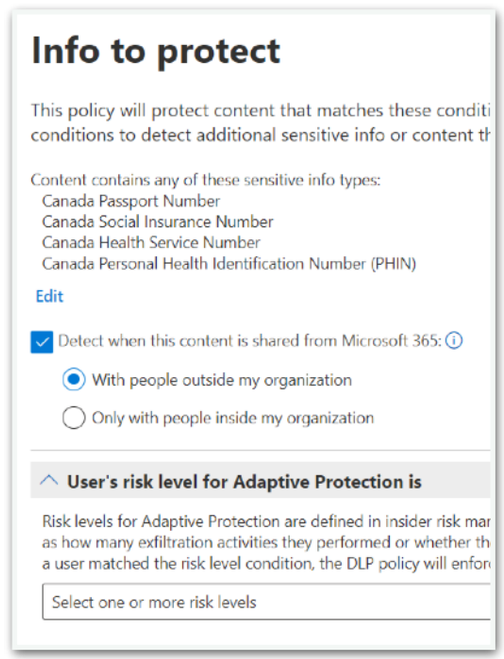
HAADJ+MFA -

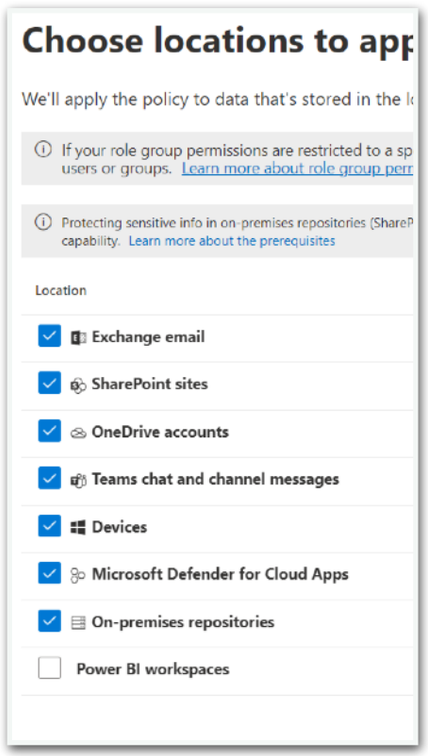
https://learn.microsoft.com/en-us/purview/what-the-dlp-policy-templates-include

Data Loss Prevention







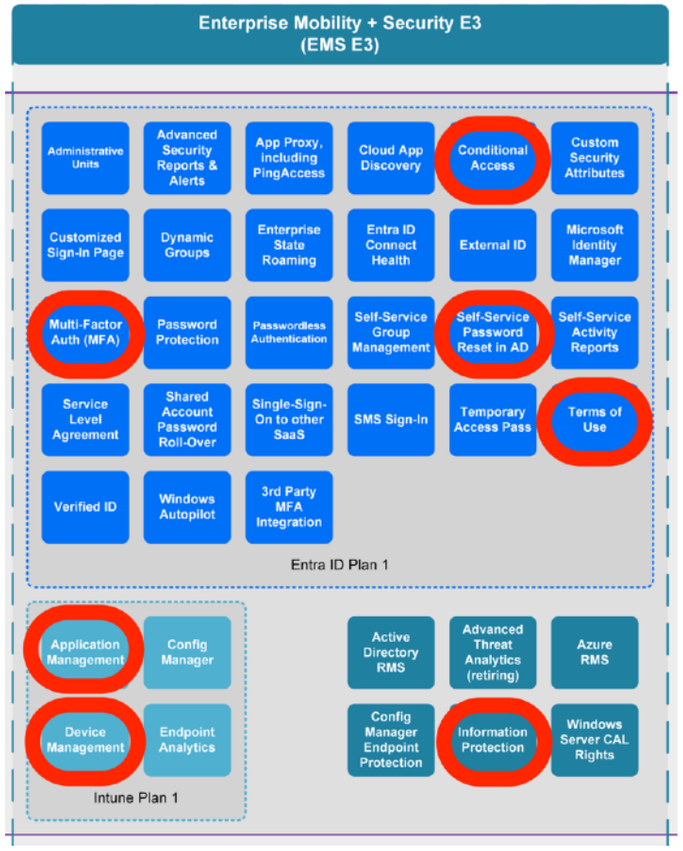


https://learn.microsoft.com/en-us/purview/dlp-policy-reference#rules

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

- Block at First Sight
- Centralized Management
- Cross-Platform Support
- Defender for Cloud Apps Integration
- Enhanced ASR
- Manual Response Actions
- Mobile Threat Defence
- Next Gen Protection
- Tamper Protection
- Web Content Filtering

Defender for Endpoint Plan 1

Microsoft 365 E5 Step-up

- 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)

Microsoft 365 E5 Compliance

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 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

Office 365 E5 Step-up

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

Windows Enterprise E5 Step-up

Microsoft 365 Enterprise Benefits

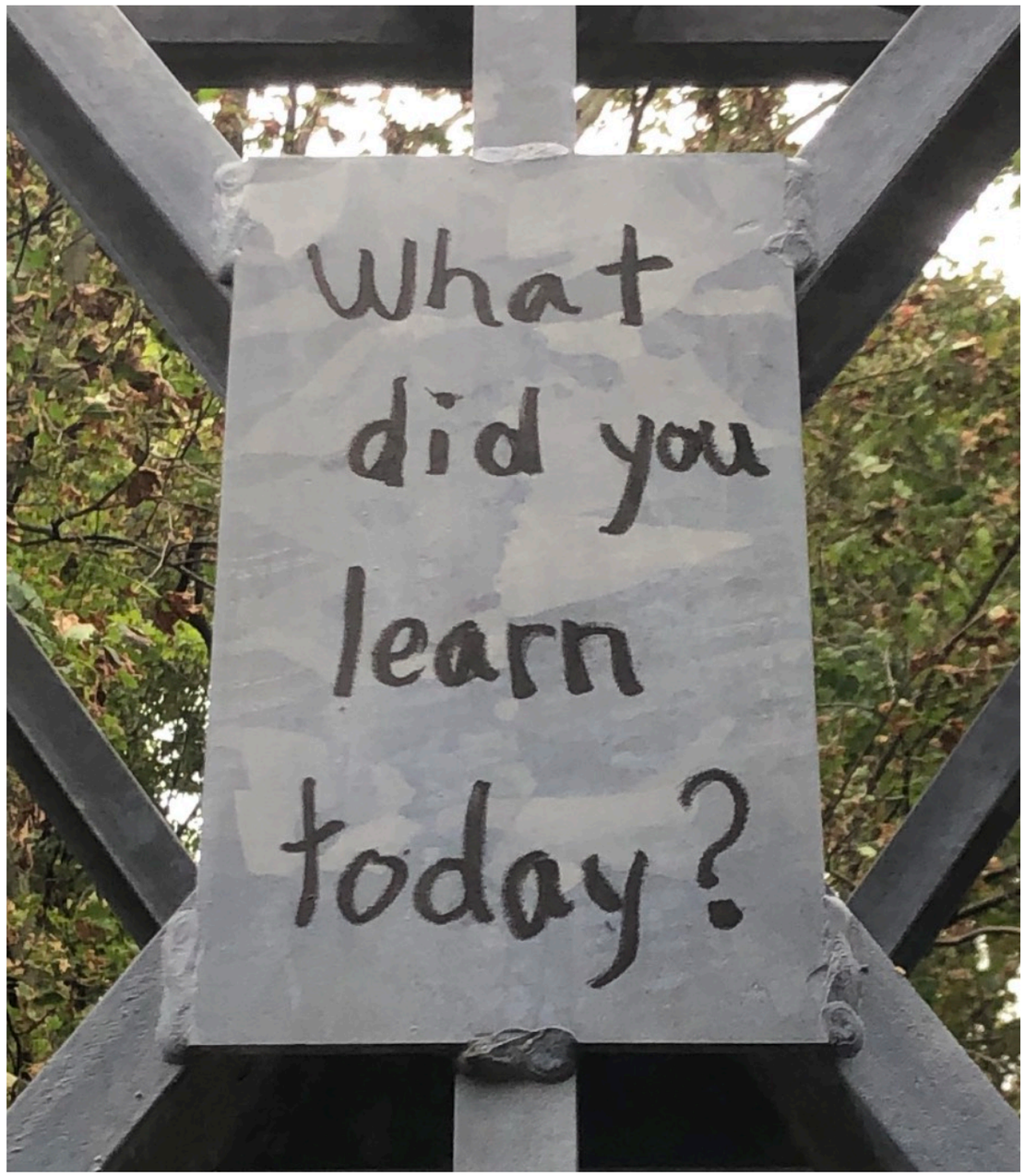
FastTrack — FastTrack helps customers deploy Microsoft 365. Customers with 150+ eligible licenses can use FastTrack at no additional cost for the life of their subscription.

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
nixuser23@gmail.com

Do not contact me on LinkedIn unless you talk to me first.

This QR code is safe

https://github.com/nixy23/bsidesto2023