Azure AD Conditional Access

Policy Design Baseline

By: Daniel Chronlund, 2020 Version: 6

	BLOCK - Legacy Authentication	BLOCK - High-Risk Sign-Ins	BLOCK - Countries not Allowed	BLOCK - Explicitly Blocked Cloud Apps	GRANT - Terms of Use	GRANT - Browser Access	SESSION - Block Unmanaged Browser File Downloads	GRANT - Mobile Device Access	GRANT - Windows Device Access	GRANT - Mac Device Access	GRANT - Guest Access	BLOCK - Guest Access	BLOCK - Service Accounts
	This global policy blocks all connections from unsecure legacy protocols like ActiveSync, IMAP, PO3, etc.	This global policy blocks all high-risk authentications (requires Azure AD Premium P2).	This global policy blocks all connections from countries not in the Allowed countries whitelist.	This policy can be used to explicitly block certain cloud apps across the organization.	This global policy forces Terms of Use on all authentications.	General browser access policy that grants authentication from a browser on any device with MFA requirement.	Browsers on unmanaged devices can never download files and attachments from SharePoint Online and Exchange Online.	Grants access to managed mobile devices that are enrolled and compliant in Intune. An approved Microsoft app is required.	Grants access to managed Windows devices that are Hybrid Azure AD Joined (joined to on-prem AD and Azure AD).	Grants access to managed Mac devices that are Intune Compliant.	Approved apps that guest users can access (requires MFA).	Blocked apps that guest users can never access.	Block service accounts from untrested IP addresses. Service accounts can connect from allowed IP addresses without MFA requirement (only use service accounts as a last resort).
Include:													
	All Users	All Users	All Users	All Users	All Users	All Users	All Users	All Users	All Users	All Users	All Guests	All Guests	Service Accounts
Exclude:													
	Excluded from CA	Excluded from CA	Excluded from CA	Excluded from CA	Excluded from CA	Excluded from CA	Excluded from CA	Excluded from CA	Excluded from CA	Excluded from CA	Excluded from CA	Excluded from CA	Excluded from CA
						Service Accounts		Service Accounts	Service Accounts	Service Accounts			

Targeted Groups

Include:													
	All Users	All Users	All Users	All Users	All Users	All Users	All Users	All Users	All Users	All Users	All Guests	All Guests	Service Accounts
Exclude:													
	Excluded from CA	Excluded from CA	Excluded from CA	Excluded from CA	Excluded from CA	Excluded from CA	Excluded from CA	Excluded from CA	Excluded from CA	Excluded from CA	Excluded from CA	Excluded from CA	Excluded from CA
						Service Accounts		Service Accounts	Service Accounts	Service Accounts			

Targeted Apps

Include:													
	All Cloud Apps	All Cloud Apps	All Cloud Apps	None	All Cloud Apps	All Cloud Apps	Exchange Online	All Cloud Apps	All Cloud Apps	All Cloud Apps	Office 365	All Cloud Apps	All Cloud Apps
							SharePoint Online						
Exclude:													
	None	None	None	None	None	Intune Enrollment	None	Intune Enrollment	Intune Enrollment	Intune Enrollment	None	Office 365	None
						Intune		Intune	Intune	Intune			

Conditions

User risk													
High													
Medium													
Low													
Sign-in risk													
High		Yes											
Medium													
Low													
No risk													
Device platforms													
Include:													
Any device													
Android								Yes					
iOS								Yes					
Windows Phone								Yes					
Windows									Yes				
macOS										Yes			
Exclude:													
Android													
iOS													
Windows Phone													
Windows													
macOS													
Locations													
Include:													
Any location			Yes										Yes
All trusted locations													
Selected locations													
Exclude:													
All trusted locations													
Selected locations			Allowed countries										Service Account IP Addresses
Client apps													
Browser		Yes	Yes	Yes	Yes	Yes	Yes						Yes
Mobile apps and desktop clients (modern authentication)		Yes	Yes	Yes	Yes			Yes	Yes	Yes			Yes
Exchange ActiveSync clients (legacy client)	Yes												
Other clients (legacy client)	Yes												
Device state													
Exclude:													
Device Hybrid Azure AD joined							Yes						
Device marked as compliant							Yes						

Access Controls

Block access	Yes	Yes	Yes	Yes								Yes	Yes
Grant access					Yes	Yes		Yes	Yes	Yes	Yes		
Require multi-factor authentication						Yes		Yes	Yes	Yes	Yes		
Require device to be marked as compliant								Yes	Yes	Yes			
Require Hybrid Azure AD Joined device									Yes				
Require approved client app (iOS and Android only)								Yes					
Require app protection policy													
Require password change (requires MFA)													
Terms of Use					Yes								
Require all the selected controls								Yes	Yes	Yes			
Require one of the selected controls					Yes	Yes					Yes		
Use app enforced restrictions													
Enabling limited access with SharePoint Online							Yes						
Enabling limited access with Exchange Online							Yes						
Use Conditional Access App Control													
Sign-in frequency													
Persistent browser session													

Policy enabled	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes