Recommended Conditional Access Policy Design

Alex Fields, ITProMentor.com; Updated 7/15/2019

	Recommended for all Businesses							Sensitive Businesses			
	Block foreign countries	Block guest access	Require MFA - untrusted devices and locations	Block legacy protocols	Block Exchange ActiveSync	Require compliant PCs	Require managed apps on mobile devices	Require compliant PCs and mobile devices	Block web downloads on unmanaged devices	Always require MFA	Require MFA for Guests
Assignments											
Users and groups											
Include	All users	All guests	All users	All users	All users	All users	All users	All users	All users	All users	All guests
Exclude	Exclude from CA	Exclude from CA	Exclude from CA	Exclude from CA	Exclude from CA	Exclude from CA	Exclude from CA	Exclude from CA	Exclude from CA	Exclude from CA	Exclude from CA
Cloud apps											
Include		All cloud apps	All cloud apps	All cloud apps	Exchange Online	All cloud apps	All cloud apps	All cloud apps	Exchange Online SharePoint Online	All cloud apps	All cloud apps
Exclude		SharePoint Online Teams				Intune Enrollment		Intune Enrollment			
Conditions											
Sign-in risk (Azure AD Premium P2)											
High											
Medium											
Low											
No risk											
Device platforms											
Android							X				
iOS							X				
Windows Phone											
Windows						X					
macOS						X					
Locations											
Include	All locations										
Exclude	Allowed Countries		Trusted locations								
Client apps											
Browser									X		
Mobile apps and desktop clients				X	X	X	X	X			
Modern authentication clients						X	X	X			
Exchange ActiveSync clients					X						
Other clients				X							
Device State											
Exclude											
Device Hybrid Azure AD joined	X		X						X		
Device marked as compliant	X		X						X		
Access controls											
Block access	X	X		X	X						
Grant access			X			X	X	X		X	X
Require MFA			X							X	X
Require device to be marked as compliant						X		X			
Require Hybrid Azure AD Joined device											
Require approved client app							X				
Require one of the selected controls			X			X	X	X		X	X
Require all of the selected controls											
Session											
Use app enforced restrictions									X		
Use Conditional access app control											
Sign-in frequency											
Persistent browser session											