Recommended Conditional Access												
Policy Design	Recommended for all Businesses							Sensitive Businesses				
Alex Fields, ITProMentor.com; Updated 8/15/2019												
Alex rielus, ir rioliientoi com, opuateu 8/13/2019			Require MFA -					Require				81.1
			untrusted				Require managed	compliant PCs	downloads on			Block
	Block foreign	Block guest	devices and	Block legacy	Block Exchange	Require	apps on mobile	and mobile	unmanaged	Always require	Require MFA for	unsupported
	countries	access	locations	protocols	ActiveSync	compliant PCs	devices	devices	devices	MFA	Guests	device platforms
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	All users
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	Exclude from CA
Claudanna												
Cloud apps Include	All cloud apps	All cloud apps	All cloud apps	All cloud apps	Exchange Online	Exchange Online	All cloud apps	Exchange Online	Exchange Online	All cloud apps	All cloud apps	All cloud apps
include	All cloud apps	All cloud apps	All cloud apps	All cloud apps	Excitatige Offilite	SharePoint Online	All cloud apps	SharePoint Online	SharePoint Online	All cloud apps	All cloud apps	All cloud apps
Exclude		SharePoint Online				Sharerount Online		Shareronic Online	Shareroint Online			
		Teams										
Conditions												
Sign-in risk (Azure AD Premium P2)												
High												
Medium												
Low												
No risk												
Device platforms												
Include						macOS	iOS					Any device
						Windows	Android					
Exclude												Supported devices
Locations												
Include	All locations											
include	Airiocations											
Exclude	Allowed Countries		Trusted locations									
Client apps												
Browser									Х			
Mobile apps and desktop clients				х	x	x	х	Х				
Modern authentication clients						Х	Х	Х				
Exchange ActiveSync clients					Х							
Other clients				Х								
Device State												
Exclude	х		V						х			
Device Hybrid Azure AD joined Device marked as compliant	X		x x						X			
Device marked as compilant	^		_ ^						^			
Access controls]
Block access	Х	x		X	X							X
Grant access			х			х	х	Х		Х	х	
Require MFA			x							X	X	
Require device to be marked as compliant						Х		Х				
Require Hybrid Azure AD Joined device												
Require approved client app							Х					
Require one of the selected controls			х			Х	X	Х		Х	Х	
Require all of the selected controls												
Session												
Use app enforced restrictions									Х			
Use Conditional access app control												
Sign-in frequency Persistent browser session												