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 Enrolment	On	Allow_MDM_Enrolment		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		

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