

## Unlocking Security: Microsoft Entra ID Policy Deployment

**Prepared By** 

Md. Rishad Istiak Sachcha

Md. Oliullah



#### Contents

Introduction to Entra ID
Benefits:3
Features:3
Task-01: Location Based Access Policy4
Scenario-01:4
Policy-01:4
Task-02: Device Based Access Policy
Scenario-02:6
Policy-02:
Task-03: Client App Based Access Policy7
Scenario-03:7
Policy-03:7
Task-04: Terms Based Access Policy9
Scenario-04:9
Policy-04:9
Task-05: Multifactor Authentication Registration Policy
Scenario-05:
Policy-05:12



#### Introduction to Entra ID

Microsoft Entra ID is a cloud-based identity and access management (IAM) solution that helps organizations secure and manage identities for hybrid and multi-cloud environments. It provides a unified identity management experience for users, applications, and devices, and it helps organizations to protect their data and resources from unauthorized access.

#### Benefits:

There are many benefits to using Microsoft Entra ID, including:

- **Improved security**: Microsoft Entra ID helps to protect organizations from unauthorized access by providing strong authentication and authorization capabilities.
- Increased efficiency: Microsoft Entra ID helps to streamline identity management tasks, such as user provisioning and deprovisioning.
- **Reduced costs:** Microsoft Entra ID can help to reduce costs by eliminating the need for on-premises IAM infrastructure.

#### Features:

Microsoft Entra ID offers a wide range of features, including:

- User management: Create, manage, and delete user accounts.
- Application management: Integrate applications with Microsoft Entra ID to control user access.
- Device management: Manage devices that access Microsoft Entra ID-protected resources.
- Access control: Control who can access what resources.
- **Reporting and auditing:** Monitor and audit user activity.

## **SM2RT**

#### Task-01: Location Based Access Policy

#### Scenario-01:

Recently Smart Digital Bank is facing different identity related attacks like spamming, bruteforce attack etc. The security team has informed that the attacks are coming from Bangladesh region. So We have to Block access from Bangladesh region. In this case we have blocked access from Bangladesh for our most critical user Nipa.

#### Policy-01:

First of all we will have to select the location. We can select location in two ways – 1. Geolocation 2. Ip address. Here we have selected Bangladesh region according to geolocation.

⊳ e □	🐃 ent	tra.microsoft.com/#view/Microsoft_AAD_Co	nditionalAccess/ConditionalA	ccessBlade/~/NamedLocations/	fromNav/Identity	<b>1</b>	• • •
icrosoft Entra admin center	ר א Se	earch resources, services, and docs (G+/)			G 🖓 🛛	रू <b>0</b> %	engineeroliullah@mq17 MSFT (MQ17.ONMICROSOFT.COM)
App registrations	*	Home > Conditional Access					
Roles & admins	$\sim$	Conditional Access	Named location:	S			×
Billing	$\sim$	~	+ Countries location +	IP ranges location 🛛 Configu	re multifactor authe	ntication trusted IP	s 🕐 Refresh 🛛 …
Settings	$\sim$	Overview					
Protection	~	I Policies	<ul> <li>To go back to the old vie tab.</li> </ul>	w, click here or use Preview features (	to turn off the enhanc	ed named locations (	list experience and refresh the
Identity Protection		<ul> <li>Insights and reporting</li> <li>X Diagnose and solve problems</li> </ul>	Named locations are used by policies. Named Locations that	Microsoft Entra security reports to at are marked Trusted or configure	o reduce false positiv d in Conditional Acc	ves and by Microsof cess Policies cannot	ft Entra Conditional Access be deleted. Learn more [2]
Conditional Access		Manage	Search by name				
Security Center		↔ Named locations	Location type: All types	Trusted type: All types 🛛 🛣 Res	set filters		
Identity Secure Score		Custom controls (Preview)	4 named locations found				
Multifactor authentication		S Terms of use	Name	Location type	Trusted	Conditional Acc	ess policies
Authentication methods		<ul> <li>VPN connectivity</li> <li>Authentication contexts</li> </ul>	BD	Countries (		Policy-01	
Password reset		O Authentication strengths	india	IP ranges	Yes	Not configured i	in any policy yet
Custom security attributes		i Classic policies					
	-	Monitoring	norway	Countries (		Not configured i	in any policy yet
Learn & support	^	Sign-in logs	smart ip	IP ranges	Yes	Policy-01	
	~	Audit logs		-			

Then from conditional access we have created a new policy policy-01 for the user Nipa. We have selected the target app Office365 & under condition, we have blocked access from Bangladesh region that we created earlier.



Policy-01 ··· Conditional Access policy	
Delete O View policy information	
Policy-01	]
Assignments	
Users 🛈	-
Specific users included	
Target resources (i)	-
1 app included	
Conditions	-
1 condition selected	
Access controls	-
Grant ①	-
Block access	

After creating the policy, we have tried to login to O365 as the user Nipa & our access is blocked which means our policy is working successfully.





#### Task-02: Device Based Access Policy

Scenario-02: Humayra- an employee of Smart Digital Bank. She is a user of Microsoft 365. Recently Smart Digital Bank has created a policy that M365 will only be accessible from Linux & Mac device. So they have to update their policy at Entra Conditional Access.

#### Policy-02:

We have selected the user Humayra first. For Microsoft admin portal, we have blocked access from other devices excluding Linux & Mac.

Policy-02 Conditional Access policy		
Delete View policy information		
Learn more 🖒		
Name *		
Policy-02		
Assignments		
Users 🕕		
Specific users included		
Target resources 🛈		
1 app included		
Conditions ①		
1 condition selected		
Access controls		
Access controls		
Enable policy		
Report-only On Off		

We tried to access to the account of humayra from windows-10 device & it didn't allow us to enter.

## **SM2RT**



#### Task-03: Client App Based Access Policy

#### Scenario-03:

Smart Digital Bank wanted that some of their users shouldn't browse O365 from browser rather they should use app. They already applied the policy. But the new employee Apon wasn't under the policy. He must have to use app to use O365 service & smart need to create that policy immediately.

#### Policy-03:

For the user Apon, we have created a conditional access policy where we have blocked O365 app access from the client app – "Browser"



🗠 en	tra.microsoft.com/#view/Microsoft_AAD_ConditionalAccess/PolicyBlade/policyId/1a2bc067-23fd-48e1-bb
و م	earch resources, services, and docs (G+/)
~	Home > Conditional Access   Policies >
Ť	Policy-03
$\sim$	Conditional Access policy
$\sim$	📋 Delete 💿 View policy information
$\sim$	decisions, and enforce organizational policies. Learn more 🗹
^	Name *
	Policy-03
	Assignments
	Users ①
	Specific users included
	Target resources ①
	1 app included
	Conditions ①
	1 condition selected
-	Enable policy
^	Report-only On Off
«	Save

Here we tried to access the account of apon from browser & our policy has successfully restricted access from browser.

## **SM2**RT



apon@mq17.onmicrosoft.com

## You cannot access this right now

Your sign-in was successful but does not meet the criteria to access this resource. For example, you might be signing in from a browser, app, or location that is restricted by your admin.

Sign out and sign in with a different account

More details

#### Task-04: Terms Based Access Policy

Scenario-04: Mr. Tanjil is an employee of Smart Digital Bank. Recently a Microsoft Entra ID user account has been created for him. But when he will login first time, he will have to accept the terms & conditions. Otherwise his access will be limited or denied.

#### Policy-04:

At first we have created a pdf file of Terms & Conditions. We have gone to the following path Conditional access  $\rightarrow$  Manage  $\rightarrow$  Terms of Use & have uploaded our file & created Term-01.



N	licrosoft Entra admin center	R	Search resources, services, and docs (G+/)			G 🖓 🎯 (	<b>ଡ</b> ନ୍ମ	engineeroliullah@ MSFT (MQ17.0NMICRO	omq17 soft.com
50 8	Devices Applications	> >	Home > Conditional Access Conditional Access Microsoft Entra ID	<b>s</b>   Terms of use	\$				×
°.	Roles & admins	×	<ol> <li>Overview</li> </ol>	K + New terms ⊘ Ed	lit terms 📋 Delete terms 🖳 Vie	ew audit logs 📳 View se	elected aud	lit logs 🕴 🔊 Got fee	dback?
1	Settings	~	<ul><li>Policies</li><li>Insights and reporting</li></ul>	Name Term-01		↑↓ Current Accepted 0	$\uparrow_{\downarrow}$	Current Declined	¢↓
A	Protection Identity Protection	^	<ul> <li>Diagnose and solve problems</li> <li>Manage</li> </ul>						
	Conditional Access		Named locations     Custom controls (Preview)						
	Security Center		Terms of use						
	Multifactor authentication		Authentication contexts						
	Authentication methods		<ul> <li>Authentication strengths</li> <li>Classic policies</li> </ul>						

Then we have gone to the conditional access policy, added the user Tanjil & selected the Term-O1 under allow access

*	Favorites	~ ^	Home > Conditional Access   Policies >
			Policy-04
٩	Identity	~	Conditional Access policy
i	Overview		Delete O View policy information
8	Users	$\sim$	Assignments
ĥXª	Groups	$\sim$	Users 🕜
£	Devices	$\sim$	
₿,	Applications	$\sim$	1 app included
ී	Roles & admins	$\sim$	Conditions ①
£.	Billing	$\sim$	0 conditions selected
ŝ	Settings	$\sim$	Access controls
8	Protection	$\sim$	Grant ()
٢	Identity governance	$\sim$	Session ()
ą	External Identities	~ -	Enable policy
2	Learn & support	^	Report-only On Off
			Save

Now we can see when the user logged in his account, a new page with terms & conditions have come out. The user must have to accept it to access the resources.



C 🖞 https://account.activedirectory.windowsazure.com/TermsOfUse#/termsOfUse/conditionalAccess/consent/2

Micro	coff
IVIICIO	son

 $\rightarrow$ 

of use.

### MSFT Terms of Use

In order to access MSFT resource(s), you must read the Terms of Use.

t&c Please click Accept to confirm that you have read and understood the terms of use.

Decline Accept

Here we can see that the user declined and failed to access the resources.

$\langle$	Https://account.activedirectory.windowsazure.com/TermsOfUse#/termsOfUse/conditionalAccess/consent/declined	A	☆	CD	ເ∕≡	Ē	~	
	Microsoft							
	Access Restricted							
	You do not have access because you have declined the MSFT terms of use. If you later wish to access the app you will need to sign in	to the	e app i	again and	accep	t the te	rms	

#### Task-05: Multifactor Authentication Registration Policy

Scenario-05: Recently authentication related attacks like bruteforce, password spraying etc has increased. Some of the employees has already become victim of this attack. Smart Digital Bank is concerned about this issue. So Smart Digital Bank have decided to deploy multifactor authentication policy to a certain group of users. Tulin is one of them.



#### Policy-05:

Before applying the multifactor authentication policy, we have created a group called "MultiAuth" & have assigned user Tulin in the group. We can put all the users who requires multifactor authentication in this group.

Micro	soft Entra admin center $P$ Search	resources, services, and docs (G+/)		G 🖓 🕸 (	P R engineeroliullah@mq17 MSFT (MQ17.0NMICROSOFT.COM)
▲ 8~8	Home > Groups   All groups >				
£0	● MultiAuth 🖈 … <sub>Group</sub>				×
€6	«	📋 Delete 🛛 🖗 Got feedback?			
0	Overview				A
	× Diagnose and solve problems	MultiAuth			
۲	Manage	IVI			
eĵe	Properties				
	2 Members	Membership type	Assigned		
	🎒 Owners	Source	Cloud	D	
2.	🍰 Roles and administrators	-		6	
	Administrative units	Type	MICROSOTT 365	U.	
۲	Group memberships	Object Id	54658eb9-f294-4d94-a04a-05ae3c6eaa77	D	
4	🎝 Assigned roles	Created at	11/19/2023, 11:27:26 AM	D	
~	Applications	Email	MultiAuth@mq17.onmicrosoft.com	D	
	🔓 Licenses				
-	Azure role assignments				
2	Activity	Direct members		A all is	
>>	Privileged Identity	I lotal 🐴 1 Us	er(s) are () Group(s)	U Other(s)	

Then we have selected the Multifactor authentication registration policy from Identity Protection. We have added the group - "MultiAuth-01" in this policy & enabled this policy.

A	Here & Hertity Bestertion		MSFT (MQ17.ONMICROSOFT.COM)
	Identity Protection	Multifactor authentication registration policy	×
× × × ×	<ul> <li>➢ Search 《</li> <li>Dashboard (Preview)</li> <li>Overview</li> <li>Tutorials</li> <li>X Diagnose and solve problems</li> <li>Protect</li> <li>User risk policy</li> <li>Sign-in risk policy</li> <li>Multifactor authentication</li> </ul>	Policy Name       Include       Exclude         Multifactor authentication registration policy       Select the users and groups to include         ▲ Users       1 group included       O       All users         Controls       Selected users and groups       Selected users and groups         Provide the user of th	ude in this
	Report Risky users	<ol> <li>Multifactor authentication registration policy only affects cloud-based Azure multifactor authentication server it will not be affected.</li> </ol>	authentication. If you have multifactor
thods -	<ul> <li>Risky workload identities</li> <li>Risky sign-ins</li> </ul>	Policy enforcement (Enabled) Disabled	



Here we can see that even after submitting the username & password, it's not letting us to enter. Rather it's asking for more information.

Microsoft	
tulin@mq17.onmic	crosoft.com
More inforr	nation required
Your organization i your account secur	needs more information to kee e
You have 14 days u	intil this is required.
Use a different acc	ount
Learn more	



When will clicked next to go forward it's asking to authenticate using Microsoft Authenticator App. We can connect with the app by scanning the QR code & verify with a two digit code. Only after completing these two steps, a user can access the service.

	Keep your account secure Your organization requires you to set up the following methods of proving who you are.
Micr	osoft Authenticator
9	Start by getting the app On your phone, install the Microsoft Authenticator app. Download now After you install the Microsoft Authenticator app on your device, choose "Next"
	I want to use a different authenticator app
I want to	set up a different method



# Thank You