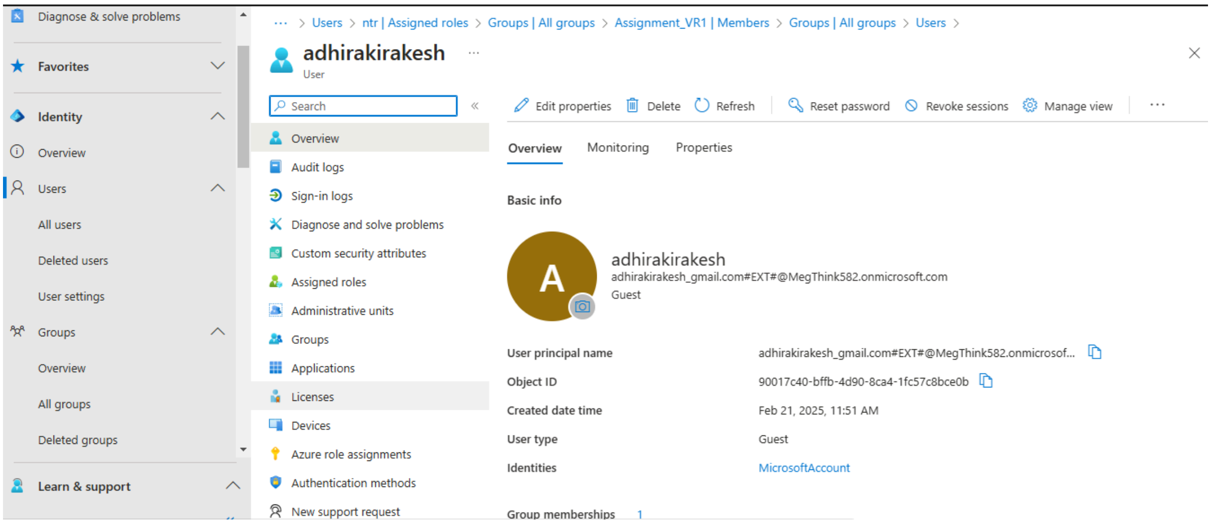
Blocking PowerShell for Guest User and Internal Member:-

1. Login to EntraID.
2. Create a Group in EntraID
3. Invite a guest user to entraid

4.



adhirakirakesh
adhirakirakesh_gmail.com#EXT#@MegThink582.onmicrosoft.com
Guest

User principal name adhirakirakesh_gmail.com#EXT#@MegThink582.onmicrosof...

Object ID 90017c40-bffb-4d90-8ca4-1fc57c8bce0b

Created date time Feb 21, 2025, 11:51 AM

User type Guest

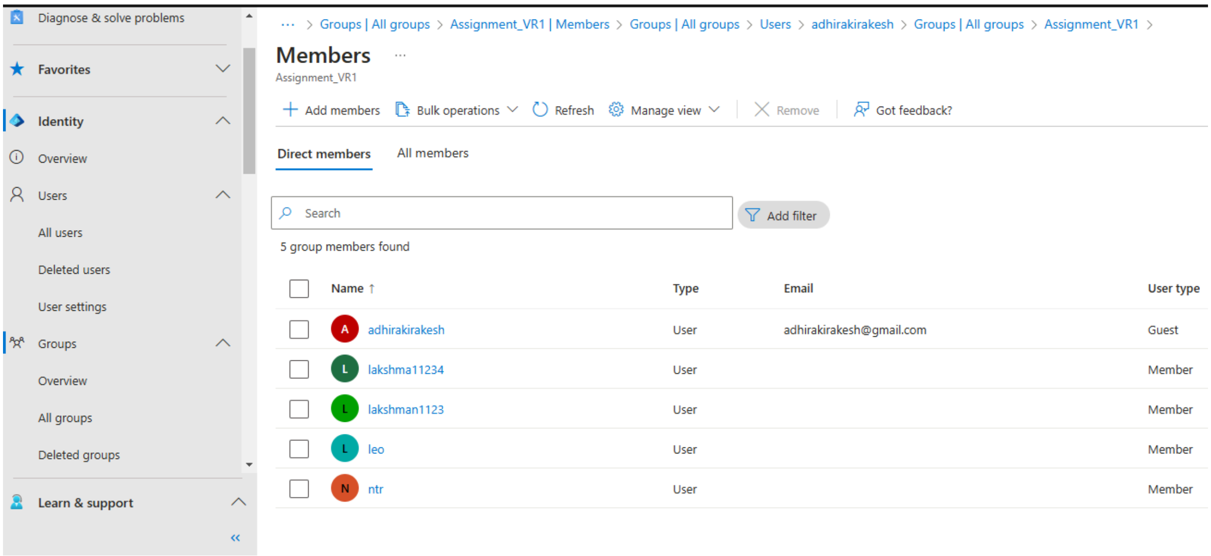
Identities MicrosoftAccount

Group memberships 1

5. Login to the guest user through username and password

6. Create a one user in entraid tenant i.e: Internal member.

7. Add internal member and guest user in to one group.



Members

Assignment_VR1

5 group members found

	Name ↑	Type	Email	User type
□	A adhirakirakesh	User	adhirakirakesh@gmail.com	Guest
□	L lakshma11234	User		Member
□	L lakshman1123	User		Member
□	L leo	User		Member
□	N ntr	User		Member

8. Now goto identity protection and click on conditional access policy.

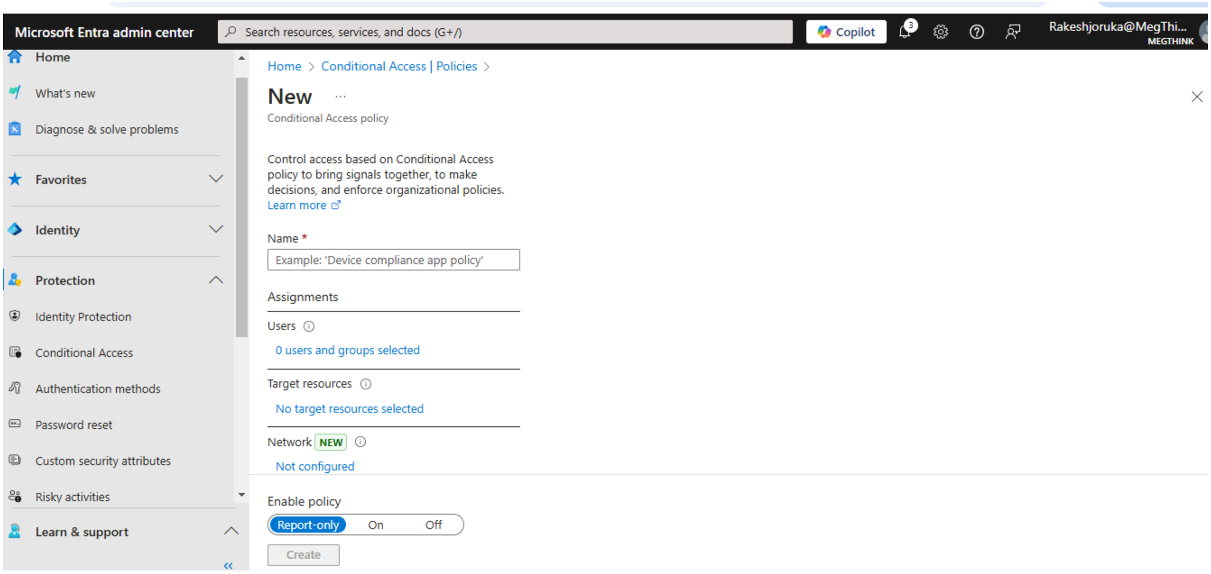
9. Go to policies in left side of your dash board.

10.click on new policies.

11.Give name and select users and groups in users

12. In target resources select cloud apps and select applications (that users needed).

13.



New ···

Conditional Access policy

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies.
Learn more

Name *
Example: 'Device compliance app policy'

Assignments

Users ⓘ
0 users and groups selected

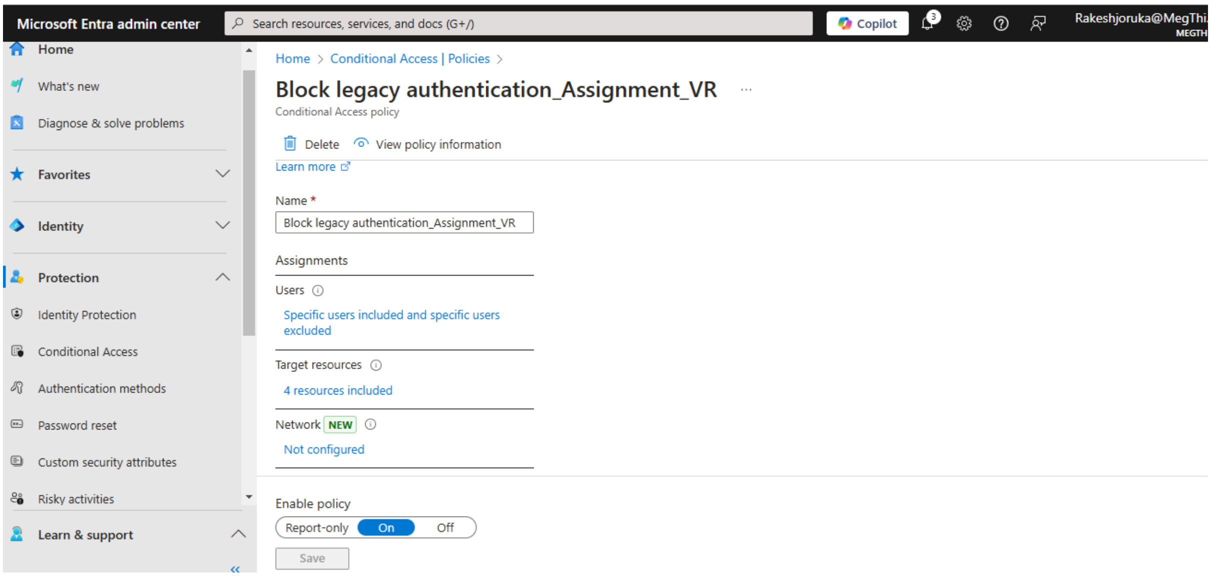
Target resources ⓘ
No target resources selected

Network NEW ⓘ
Not configured

Enable policy
[✓ Report-only] On Off

Create

14.



Block legacy authentication_Assignment_VR ···

Conditional Access policy

Delete   View policy information

Learn more

Name *
Block legacy authentication_Assignment_VR

Assignments

Users ⓘ
Specific users included and specific users excluded

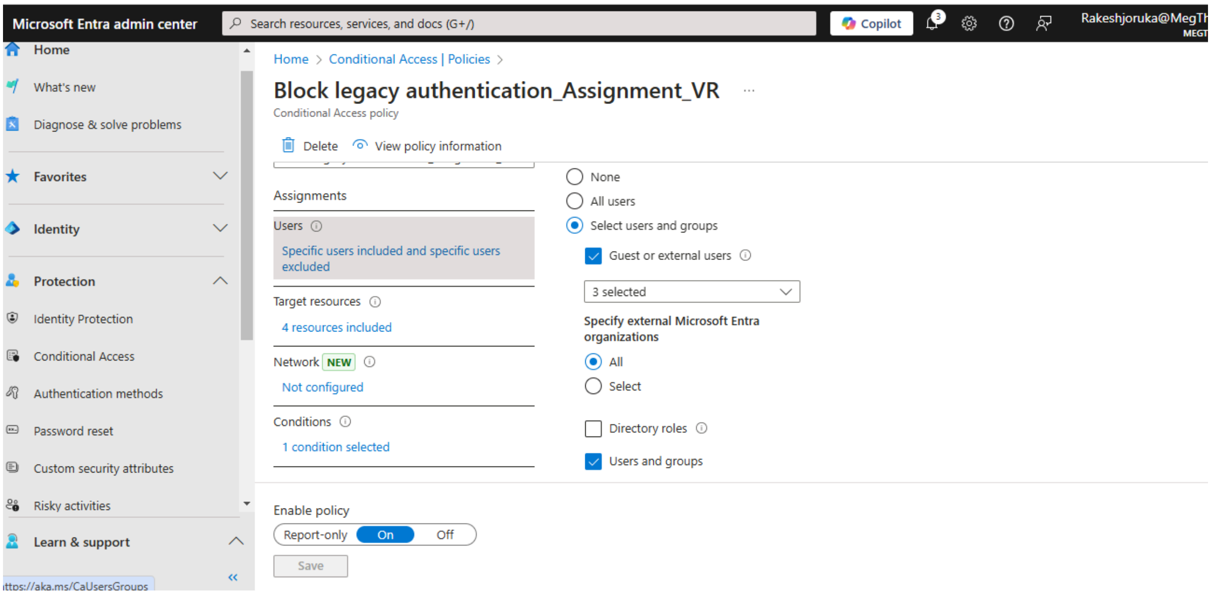
Target resources ⓘ
4 resources included

Network NEW ⓘ
Not configured

Enable policy
Report-only [✓ On] Off

Save

15.



Block legacy authentication_Assignment_VR

Conditional Access policy

Assignments

Users ⓘ
Specific users included and specific users excluded

Target resources ⓘ
4 resources included

Network NEW ⓘ
Not configured

Conditions ⓘ
1 condition selected

○ None
○ All users
● Select users and groups
☑ Guest or external users ⓘ
3 selected

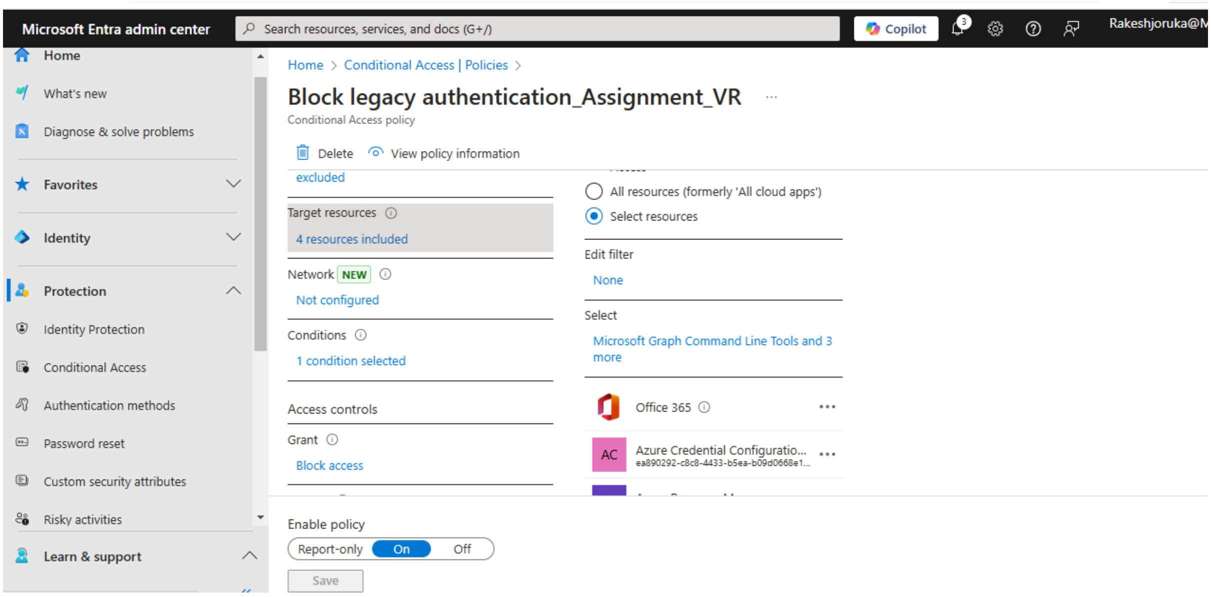
Specify external Microsoft Entra organizations
● All
○ Select

□ Directory roles ⓘ
☑ Users and groups

Enable policy
Report-only [✓ On] Off

Save

16.



Block legacy authentication_Assignment_VR

Conditional Access policy

excluded

Target resources ⓘ
4 resources included

Network NEW ⓘ
Not configured

Conditions ⓘ
1 condition selected

Access controls

Grant ⓘ
Block access

○ All resources (formerly 'All cloud apps')
● Select resources

Edit filter
None

Select
Microsoft Graph Command Line Tools and 3 more

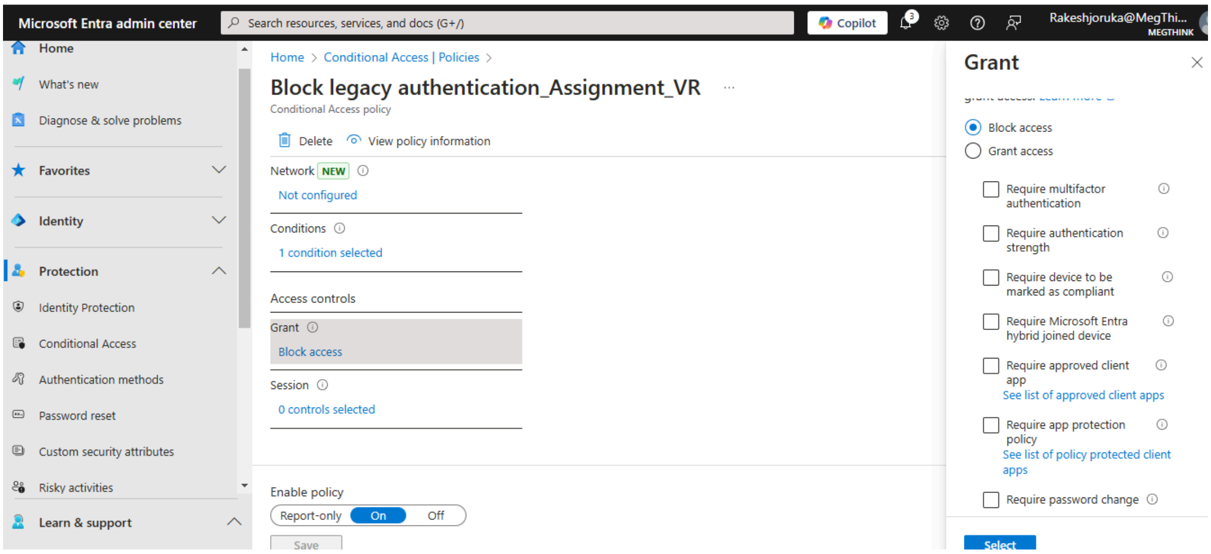
Office 365 ⓘ

AC Azure Credential Configuratio...
ea890292-c8c8-4433-b5ea-b09d0668e1...

Enable policy
Report-only [✓ On] Off

Save

17.



Block legacy authentication_Assignment_VR

Conditional Access policy

Network NEW
Not configured

Conditions
1 condition selected

Access controls

Grant
Block access

Session
0 controls selected

Enable policy
Report-only [✓ On] Off

Grant

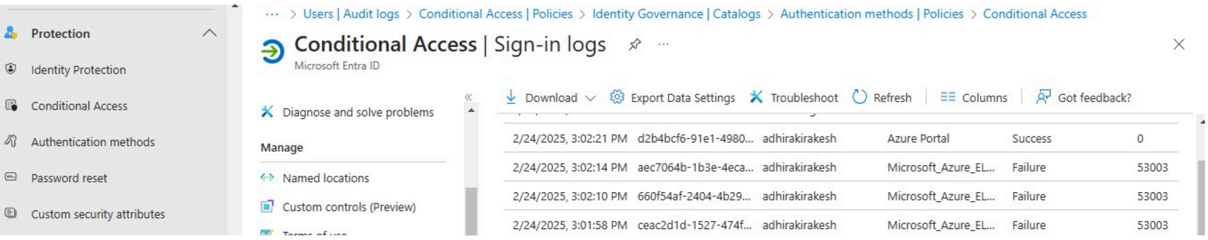
● Block access
○ Grant access

□ Require multifactor authentication
□ Require authentication strength
□ Require device to be marked as compliant
□ Require Microsoft Entra hybrid joined device
□ Require approved client app
See list of approved client apps
□ Require app protection policy
See list of policy protected client apps
□ Require password change

18.now select enable policy to on.

19.click on save.

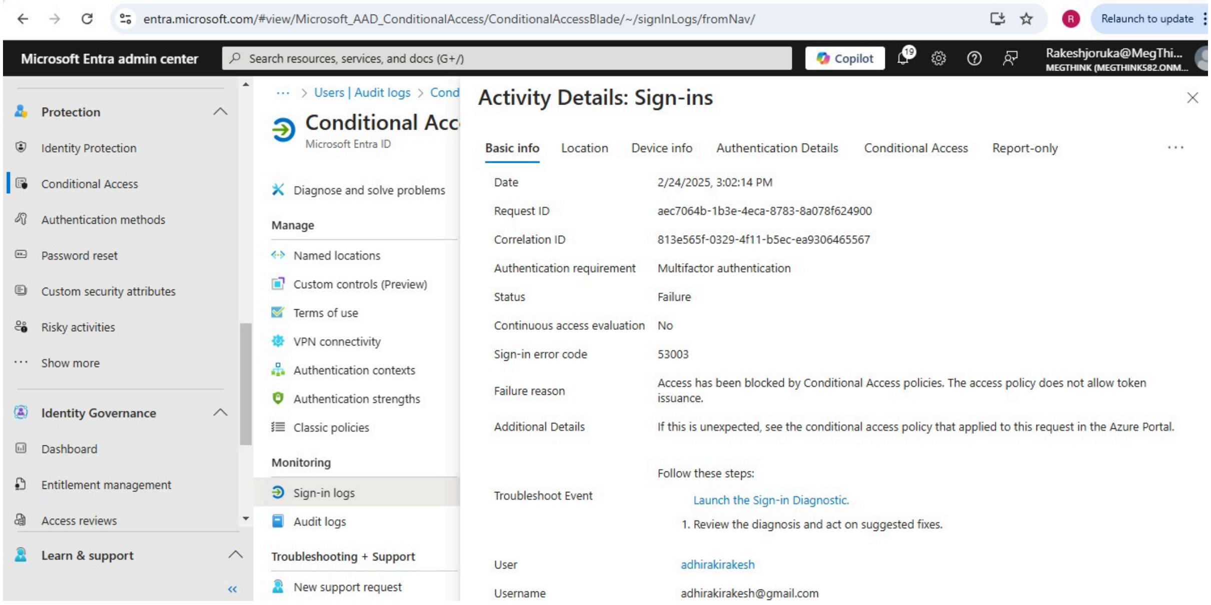
20.Now you can run powershell command i.e; connect-mggraph.It will say authentication error in powershell.


Protection
Identity Protection
Conditional Access
Authentication methods
Password reset
Custom security attributes
... > Users | Audit logs > Conditional Access | Policies > Identity Governance | Catalogs > Authentication methods | Policies > Conditional Access
Diagnose and solve problems
Manage
Named locations
Custom controls (Preview)
Download
Export Data Settings
Troubleshoot
Refresh
Columns
Got feedback?

Conditional Access | Sign-in logs

Microsoft Entra ID

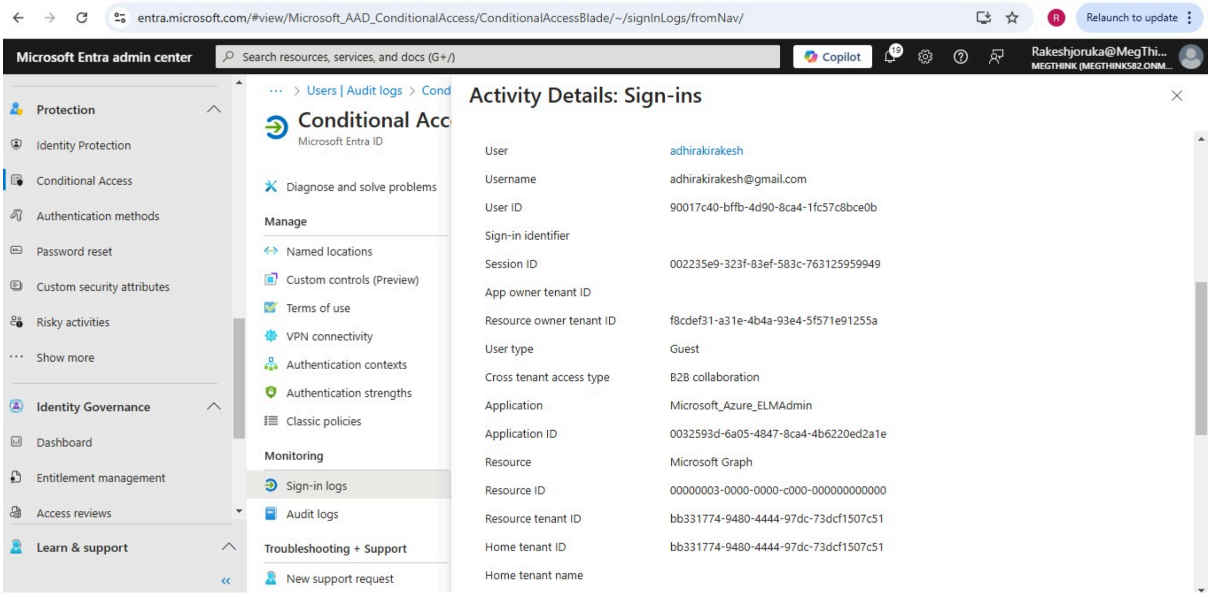
2/24/2025, 3:02:21 PM	d2b4bcf6-91e1-4980...	adhirakirakesh	Azure Portal	Success	0
2/24/2025, 3:02:14 PM	aec7064b-1b3e-4eca...	adhirakirakesh	Microsoft_Azure_EL...	Failure	53003
2/24/2025, 3:02:10 PM	660f54af-2404-4b29...	adhirakirakesh	Microsoft_Azure_EL...	Failure	53003
2/24/2025, 3:01:58 PM	ceac2d1d-1527-474f...	adhirakirakesh	Microsoft_Azure_EL...	Failure	53003



Activity Details: Sign-ins

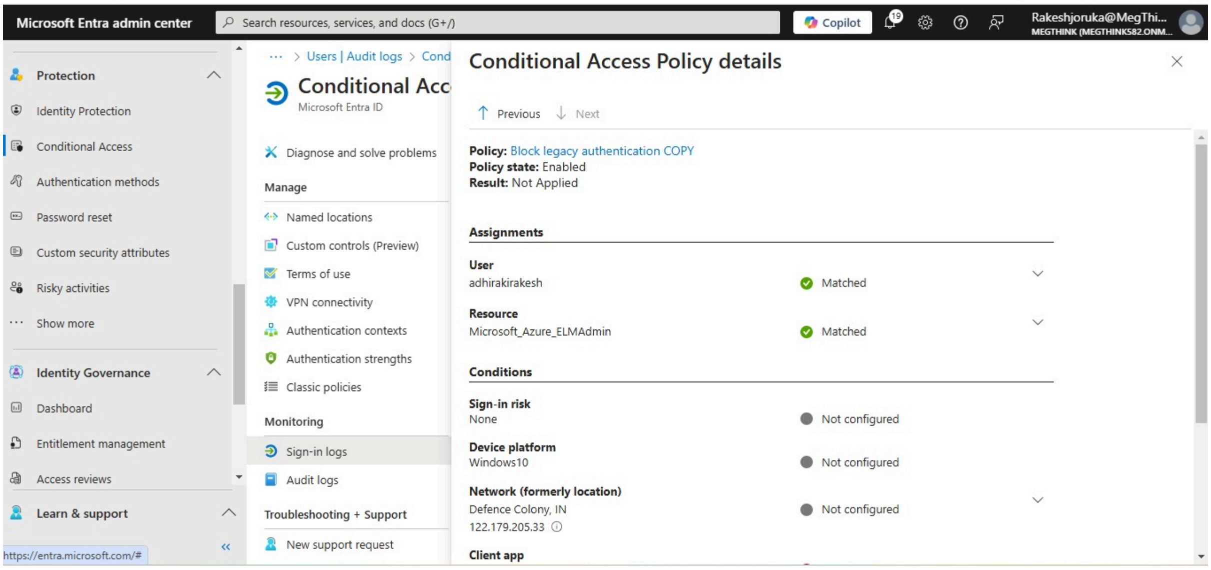
Basic info | Location | Device info | Authentication Details | Conditional Access | Report-only

Date	2/24/2025, 3:02:14 PM
Request ID	aec7064b-1b3e-4eca-8783-8a078f624900
Correlation ID	813e565f-0329-4f11-b5ec-ea9306465567
Authentication requirement	Multifactor authentication
Status	Failure
Continuous access evaluation	No
Sign-in error code	53003
Failure reason	Access has been blocked by Conditional Access policies. The access policy does not allow token issuance.
Additional Details	If this is unexpected, see the conditional access policy that applied to this request in the Azure Portal.
Troubleshoot Event	Follow these steps: Launch the Sign-in Diagnostic. 1. Review the diagnosis and act on suggested fixes.
User	adhirakirakesh
Username	adhirakirakesh@gmail.com



Activity Details: Sign-ins

User	adhirakirakesh
Username	adhirakirakesh@gmail.com
User ID	90017c40-bffb-4d90-8ca4-1fc57c8bce0b
Sign-in identifier	
Session ID	002235e9-323f-83ef-583c-763125959949
App owner tenant ID	
Resource owner tenant ID	f8cdef31-a31e-4b4a-93e4-5f571e91255a
User type	Guest
Cross tenant access type	B2B collaboration
Application	Microsoft_Azure_ELMAdmin
Application ID	0032593d-6a05-4847-8ca4-4b6220ed2a1e
Resource	Microsoft Graph
Resource ID	00000003-0000-0000-c000-000000000000
Resource tenant ID	bb331774-9480-4444-97dc-73dcf1507c51
Home tenant ID	bb331774-9480-4444-97dc-73dcf1507c51
Home tenant name	



Conditional Access Policy details

Policy: Block legacy authentication COPY
Policy state: Enabled
Result: Not Applied

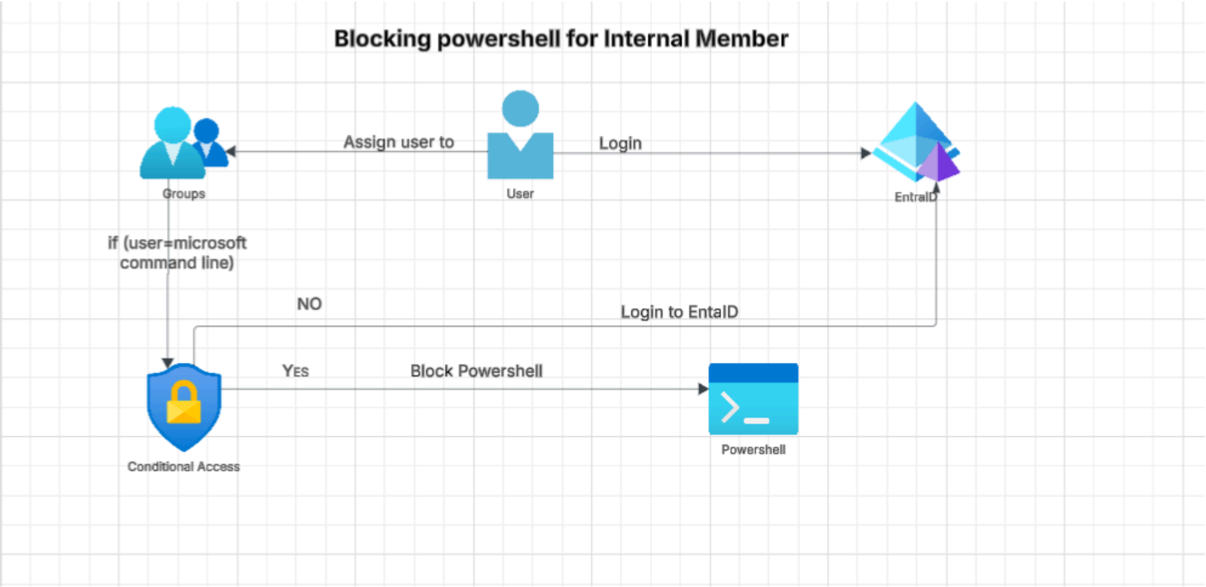
Assignments

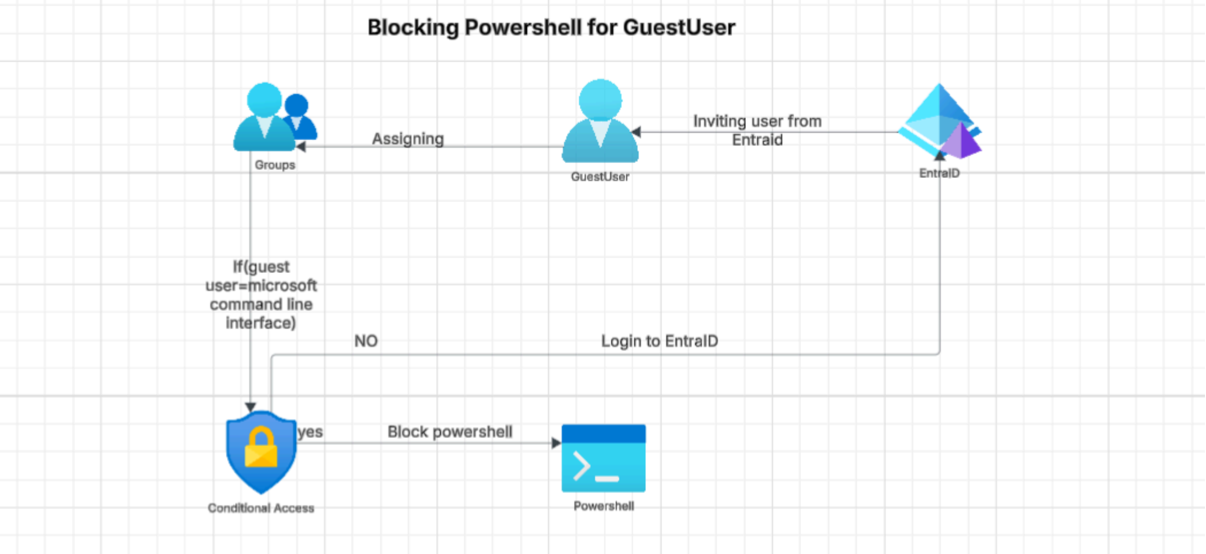
User adhirakirakesh	✓ Matched
Resource Microsoft_Azure_ELMAdmin	✓ Matched

Conditions

Sign-in risk None	● Not configured
Device platform Windows10	● Not configured
Network (formerly location) Defence Colony, IN 122.179.205.33	● Not configured
Client app	

UML DIAGRAMS :-




Blocking Powershell for GuestUser
Groups
Assigning
GuestUser
Inviting user from Entraid
EntraID
If(guest user=microsoft command line interface)
NO
Login to EntraID
yes
Block powershell
Conditional Access
Powershell