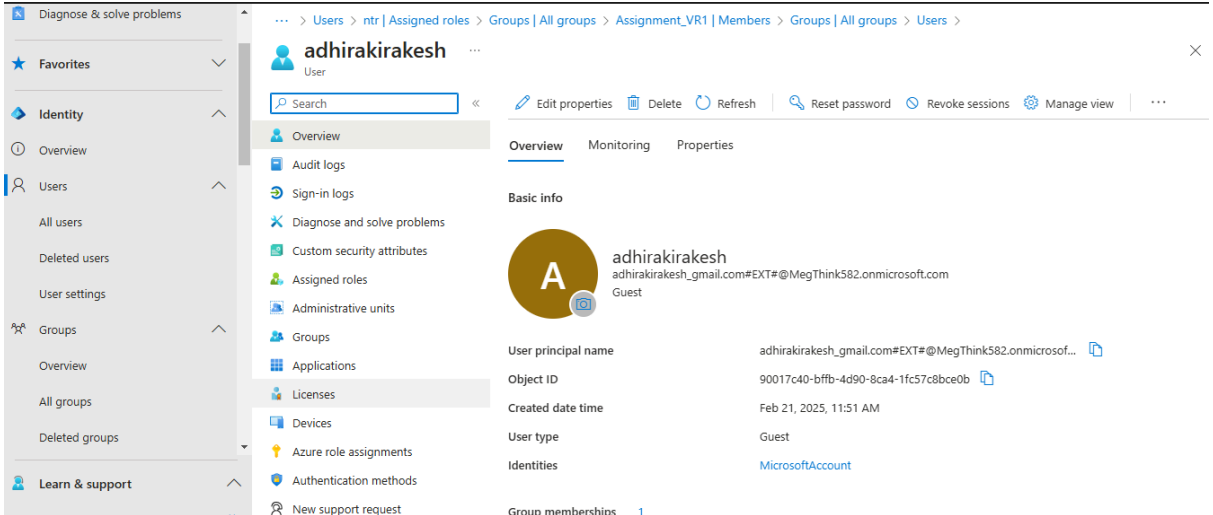


## Blocking PowerShell for Guest User and Internal Member:-

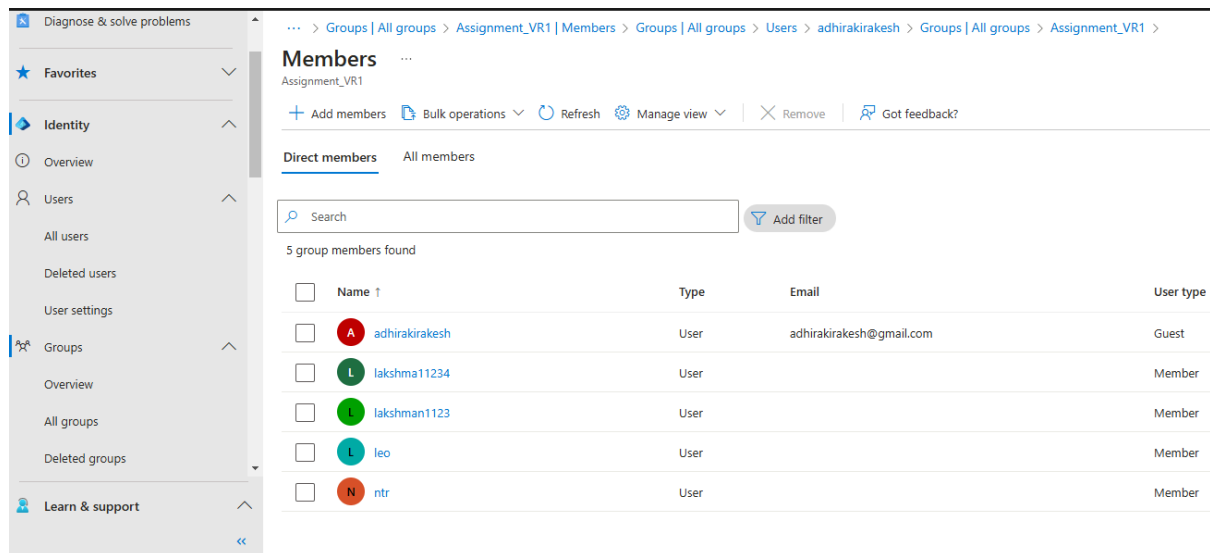
1. Login to EntraID.
2. Create a Group in EntraID
3. Invite a guest user to entraid

4.



The screenshot displays the Microsoft Entra ID management console. On the left, a navigation pane shows categories like 'Identity', 'Users', 'Groups', and 'Learn & support'. The main area shows the user profile for 'adhirakirakesh', who is a 'Guest' user. The profile includes a search bar, action buttons (Edit properties, Delete, Refresh, Reset password, Revoke sessions, Manage view), and tabs for Overview, Monitoring, and Properties. The 'Overview' tab is active, showing basic information: User principal name (adhirakirakesh\_gmail.com#EXT#@MegThink582.onmicrosoft.com), Object ID (90017c40-bffb-4d90-8ca4-1fc57c8bce0b), Created date time (Feb 21, 2025, 11:51 AM), User type (Guest), and Identities (MicrosoftAccount). A 'Group memberships' section at the bottom indicates 1 membership.

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.



Diagnose & solve problems

... > Groups | All groups > Assignment\_VR1 | Members > Groups | All groups > Users > adhirakirakesh > Groups | All groups > Assignment\_VR1 >

### Members






Assignment\_VR1

+ Add members Bulk operations Refresh Manage view Remove Got feedback?

Direct members All members

Search Add filter

5 group members found

<input type="checkbox"/>	Name ↑	Type	Email	User type
<input type="checkbox"/>	 adhirakirakesh	User	adhirakirakesh@gmail.com	Guest
<input type="checkbox"/>	 lakshma11234	User		Member
<input type="checkbox"/>	 lakshman1123	User		Member
<input type="checkbox"/>	 leo	User		Member
<input type="checkbox"/>	 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.

The screenshot shows the Microsoft Entra admin center interface. The left sidebar contains navigation links: Home, What's new, Diagnose & solve problems, Favorites, Identity, Protection, Identity Protection, Conditional Access, Authentication methods, Password reset, Custom security attributes, Risky activities, and Learn & support. The main content area is titled 'New' and 'Conditional Access | Policies'. It includes a description: 'Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. Learn more'. Below this are input fields for 'Name' (with an example: 'Device compliance app policy'), 'Assignments' (Users: 0 users and groups selected), 'Target resources' (No target resources selected), and 'Network' (NEW, Not configured). At the bottom, there is an 'Enable policy' section with a 'Report-only' button and 'On'/'Off' radio buttons, and a 'Create' button.

14.

The screenshot shows the Microsoft Entra admin center interface. The left sidebar is the same as in the previous screenshot. The main content area is titled 'Block legacy authentication\_Assignment\_VR' and 'Conditional Access policy'. It includes links for 'Delete', 'View policy information', and 'Learn more'. Below these are input fields for 'Name' (Block legacy authentication\_Assignment\_VR), 'Assignments' (Users: Specific users included and specific users excluded), 'Target resources' (4 resources included), and 'Network' (NEW, Not configured). At the bottom, there is an 'Enable policy' section with a 'Report-only' button, 'On'/'Off' radio buttons, and a 'Save' button.

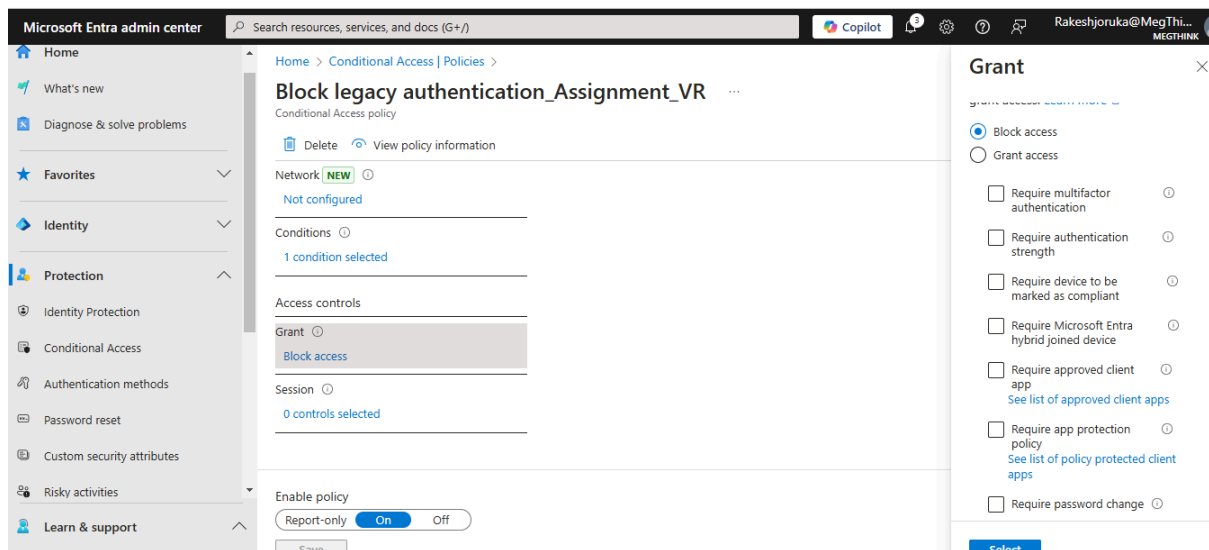
15.

The screenshot shows the Microsoft Entra admin center interface. The left sidebar contains navigation links: Home, What's new, Diagnose & solve problems, Favorites, Identity, Protection, Identity Protection, Conditional Access, Authentication methods, Password reset, Custom security attributes, Risky activities, and Learn & support. The main content area is titled 'Block legacy authentication\_Assignment\_VR' and is categorized as a 'Conditional Access policy'. It includes options to 'Delete' or 'View policy information'. The 'Assignments' section shows 'Users' with a link to 'Specific users included and specific users excluded'. The 'Target resources' section shows '4 resources included'. The 'Network' section shows 'NEW' and 'Not configured'. The 'Conditions' section shows '1 condition selected'. On the right, there are radio buttons for 'None', 'All users', and 'Select users and groups' (which is selected). Below these are checkboxes for 'Guest or external users' (checked), 'Specify external Microsoft Entra organizations' (with 'All' selected), 'Directory roles' (unchecked), and 'Users and groups' (checked). At the bottom, there is an 'Enable policy' section with 'Report-only' set to 'On' and a 'Save' button.

16.

This screenshot shows the same Microsoft Entra admin center interface as the previous one, but with more detailed configuration visible. The 'Target resources' section shows '4 resources included'. The 'Network' section shows 'NEW' and 'Not configured'. The 'Conditions' section shows '1 condition selected'. The 'Access controls' section shows 'Grant' with 'Block access' selected. The 'Enable policy' section shows 'Report-only' set to 'On' and a 'Save' button. On the right, there are radio buttons for 'All resources (formerly "All cloud apps")' and 'Select resources' (which is selected). Below these are links for 'Edit filter' (None) and 'Select' (Microsoft Graph Command Line Tools and 3 more). A list of selected resources is shown, including 'Office 365' and 'Azure Credential Configuratio...'.

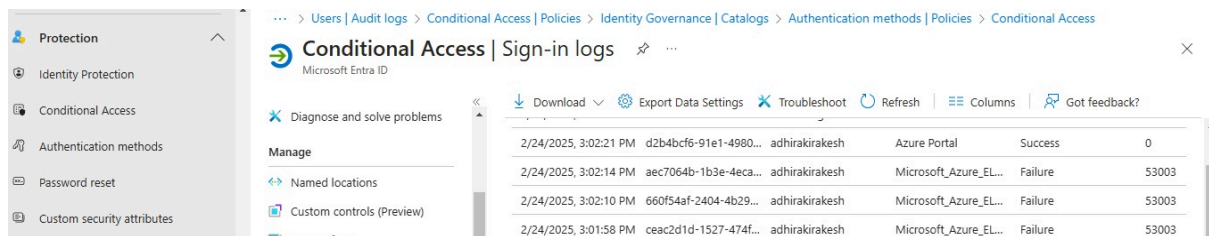
17.



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.



entra.microsoft.com/#view/Microsoft\_AAD\_ConditionalAccess/ConditionalAccessBlade/~:/signInLogs/fromNav/

Microsoft Entra admin center

Search resources, services, and docs (G+)

Copilot

RakeshJoruka@MegThi... MEGTHINK (MEGTHINKS82.ONM...)

Relaunch to update

Protection

- Identity Protection
- Conditional Access
- Authentication methods
- Password reset
- Custom security attributes
- Risky activities
- Show more

Identity Governance

- Dashboard
- Entitlement management
- Access reviews

Learn & support

- Troubleshooting + Support
- New support request

Users | Audit logs > Conditional Access

Conditional Access

Microsoft Entra ID

- Diagnose and solve problems
- Manage
  - Named locations
  - Custom controls (Preview)
  - Terms of use
  - VPN connectivity
  - Authentication contexts
  - Authentication strengths
  - Classic policies
- Monitoring
  - Sign-in logs
  - Audit logs
- Troubleshooting + Support
- New support request

### 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: <a href="#">Launch the Sign-in Diagnostic.</a> 1. Review the diagnosis and act on suggested fixes.
User	adhirakirakesh
Username	adhirakirakesh@gmail.com

entra.microsoft.com/#view/Microsoft\_AAD\_ConditionalAccess/ConditionalAccessBlade/~:/signInLogs/fromNav/

Microsoft Entra admin center

Search resources, services, and docs (G+)

Copilot

RakeshJoruka@MegThi... MEGTHINK (MEGTHINKS82.ONM...)

Relaunch to update

Protection

- Identity Protection
- Conditional Access
- Authentication methods
- Password reset
- Custom security attributes
- Risky activities
- Show more

Identity Governance

- Dashboard
- Entitlement management
- Access reviews

Learn & support

- Troubleshooting + Support
- New support request

Users | Audit logs > Conditional Access

Conditional Access

Microsoft Entra ID

- Diagnose and solve problems
- Manage
  - Named locations
  - Custom controls (Preview)
  - Terms of use
  - VPN connectivity
  - Authentication contexts
  - Authentication strengths
  - Classic policies
- Monitoring
  - Sign-in logs
  - Audit logs
- Troubleshooting + Support
- New support request

### 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_ELMAAdmin
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	

entra.microsoft.com/#view/Microsoft\_AAD\_ConditionalAccess/ConditionalAccessBlade/~:/signInLogs/fromNav/

Microsoft Entra admin center

Search resources, services, and docs (G+)

Copilot

RakeshJoruka@MegThi... MEGTHINK (MEGTHINKS82.ONM...)

Relaunch to update

Protection

- Identity Protection
- Conditional Access
- Authentication methods
- Password reset
- Custom security attributes
- Risky activities
- Show more

Identity Governance

- Dashboard
- Entitlement management
- Access reviews

Learn & support

- Troubleshooting + Support
- New support request

Users | Audit logs > Conditional Access

Conditional Access

Microsoft Entra ID

- Diagnose and solve problems
- Manage
  - Named locations
  - Custom controls (Preview)
  - Terms of use
  - VPN connectivity
  - Authentication contexts
  - Authentication strengths
  - Classic policies
- Monitoring
  - Sign-in logs
  - Audit logs
- Troubleshooting + Support
- New support request

### Conditional Access Policy details

Previous Next

Policy: Block legacy authentication COPY

Policy state: Enabled

Result: Not Applied

Assignments

User	adhirakirakesh	Matched
Resource	Microsoft_Azure_ELMAAdmin	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 :-

