Prepared by: Nandini Goyal
Intern at Celebal Technologies
Department: Cloud Infra & Security

Date: 21 July 2025

Project Report

Privileged Identity Management (PIM)

Table of Contents

1. Introduction to Azure PIM

Theory

Azure Privileged Identity Management (PIM) is a critical security feature within Microsoft Entra (formerly Azure Active Directory) designed to manage, control, and monitor privileged access across Azure AD, Azure resources, and other Microsoft services. PIM enhances security by reducing standing privileges through just-in-time (JIT) access, enforcing approval workflows, maintaining detailed audit trails, and providing alerts for privileged operations. This minimises the risk of unauthorised access, ensures compliance with regulatory standards, and reduces the attack surface for organisations.

PIM is particularly valuable in environments where multiple administrators or users require elevated permissions to perform specific tasks. Instead of granting permanent access, PIM allows organisations to assign temporary, time-bound roles that are activated only when needed. This approach aligns with the principle of least privilege, a cornerstone of modern cybersecurity practices.

Key Features of Azure PIM

- **Just-In-Time Access**: Temporary role activation to reduce exposure.
- **Approval Workflows**: Require approvals for role activation to enhance oversight.
- **Audit Trails**: Comprehensive logs for tracking privileged activities.
- **Role-Based Access Control (RBAC)**: Fine-grained control over Azure AD and Azure resources.
- **Privileged Access Groups**: Manage roles through security groups for scalability.
- **Break-Glass Accounts**: Emergency accounts for critical access scenarios.

Why Use PIM?

Organisations face increasing threats from insider attacks, compromised credentials, and external breaches. PIM addresses these challenges by:

- Limiting the duration of privileged access.
- Requiring justification and approval for role activations.
- Providing visibility into who has access and when.

- Supporting compliance with standards like GDPR, HIPAA, and ISO 27001.

Practical Applications

PIM is used in various scenarios, such as:

- Granting temporary administrative access for IT maintenance tasks.
- Managing access for third-party vendors or contractors.
- Ensuring compliance with regulatory requirements through audit logs.
- Securing access to critical Azure resources like virtual machines or databases.

2. Setup Prerequisites for Roles and Licenses

Theory

Before implementing PIM, organisations must ensure they meet the necessary prerequisites, including licensing, administrative roles, and permissions. Proper setup ensures PIM functions correctly and aligns with organisational security policies.

2.1 Azure AD Premium Licensing

PIM requires an **Azure AD Premium P2** license (or equivalent, such as Microsoft 365 E5 or Enterprise Mobility + Security E5). This license enables advanced PIM features like JIT access and approval workflows.

Practical Steps

1. **Verify License Status**:
    - Navigate to **Azure Portal > Microsoft Entra ID > Licenses > All products**.
    - Confirm that "Azure AD Premium P2" is active and assigned to relevant users.
    - Assign licenses to users who will manage or use PIM.

2. **License Assignment**:
    - Go to **Microsoft Entra ID > Licenses > Licensed users**.
    - Add users to the Azure AD Premium P2 license group.
    - Verify license activation in the user's profile.

2.2 Admin Roles

To configure PIM, users must have the **Global Administrator** role or equivalent permissions. For Azure resource-level PIM, **Owner** or **User Access Administrator** permissions are required at the subscription or resource group level.

Practical Steps

1. **Check Role Assignments**:
   - Navigate to **Microsoft Entra ID > Roles and administrators**.
   - Verify that the user configuring PIM has the Global Administrator role.
2. **Assign Additional Roles**:
   - If needed, assign roles like **Privileged Role Administrator** to manage PIM settings without full Global Administrator access.

2.3 Additional Prerequisites

- **Multi-Factor Authentication (MFA)**: Enable MFA for all users with privileged roles to enhance security.
- **Azure Subscription**: Ensure an active Azure subscription is linked to the tenant for resource-level PIM.
- **Network Access**: Verify that users have access to the Azure Portal (no restrictive Conditional Access policies blocking PIM).

Best Practices

- Regularly audit license assignments to ensure compliance.
- Use dynamic groups for automatic license assignment.
- Document all role assignments for accountability.

3. Explore Just-In-Time (JIT) Access

Theory

Just-In-Time (JIT) access is a core feature of PIM that grants temporary elevated permissions only when needed. This reduces the risk of standing privileges, which can be exploited if credentials are compromised.

3.1 Benefits of JIT Access

- **Reduced Attack Surface**: Limits the time window for potential misuse.
- **Granular Control**: Specifies exact roles and durations.
- **Auditability**: Tracks all activation requests and actions.
- **Compliance**: Aligns with zero-trust security models.

3.2 JIT Access Workflow

1. **Role Eligibility**: Users are assigned as “eligible” for a role instead of having permanent access.
2. **Activation Request**: Users request activation through the Azure Portal or PIM dashboard.
3. **Approval (if required)**: Designated approvers review and approve/deny the request.
4. **Time-Bound Access**: The role is active for a specified duration (e.g., 1–8 hours).
5. **Deactivation**: Access is automatically revoked after the duration expires.

3.3 Common Use Cases

- **IT Maintenance**: Temporary access to manage servers or databases.
- **Audits**: Grant auditors read-only access for a specific period.
- **Vendor Access**: Provide contractors with limited-time access to specific resources.

Practical Steps

1. **Access PIM Dashboard**:
   - Go to **Microsoft Entra ID > Privileged Identity Management > Azure AD roles**.
2. **Activate a Role**:
   - Select an eligible role from the “My roles” section.
   - Click **Activate**, provide a justification, and set the duration.
3. **Monitor Activation**:
   - Check the status in the “Active roles” tab.

Best Practices

- Limit activation durations to the minimum required.

- Require MFA for all role activations.
- Regularly review eligible roles to remove unused assignments.

4. Configure Azure Roles in PIM

Theory

Configuring Azure AD roles in PIM involves assigning users as eligible for roles, setting activation conditions, and defining approval workflows. This ensures that only authorized users can access privileged roles under controlled conditions.

4.1 Assigning Roles

Assigning roles in PIM makes users eligible to activate specific Azure AD roles when needed.

Practical Steps

1. **Navigate to PIM**:
   - Go to **Microsoft Entra ID > PIM > Azure AD roles > Assignments**.
2. **Add Assignment**:
   - Click **Add assignments**, select a role (e.g., Global Administrator), and choose a user or group.
   - Set the assignment type to “Eligible” or “Active.”
3. **Confirm Assignment**:
   - Verify the assignment in the “Assignments” tab.

4.2 Role Settings Configuration

Role settings define the conditions for role activation, such as duration, MFA, and approval requirements.

Practical Steps

1. **Edit Role Settings**:
   - Go to **PIM > Azure AD roles > Roles > Settings**.
   - Select a role and click **Edit**.
2. **Configure Settings**:

- **Activation Maximum Duration**: Set the maximum time a role can be active (e.g., 8 hours).
- **Require MFA**: Enable MFA for activation.
- **Require Justification**: Mandate a reason for activation.
- **Require Approval**: Specify approvers or groups for activation requests.

3. **Save Changes**:
   - Apply and verify settings in the PIM dashboard.

4.3 Best Practices for Role Management

- Use the least privileged role for tasks (e.g., User Administrator instead of Global Administrator).
- Regularly review role assignments to remove unnecessary access.
- Document all role configurations for audit purposes.

5. Configure Azure Resources in PIM

Theory

PIM extends privileged access management to Azure resources, including subscriptions, resource groups, and individual resources like virtual machines or storage accounts. This allows organisations to control access at a granular level.

5.1 Subscription-Level Configuration

Manage access to entire Azure subscriptions using PIM.

Practical Steps

1. **Access PIM for Resources**:
   - Navigate to **PIM > Azure resources**.
   - Select a subscription from the list.
2. **View Roles**:
   - Click **Roles** to see available roles (e.g., Owner, Contributor).
3. **Assign Roles**:
   - Add eligible users or groups for specific roles.

5.2 Resource Group-Level Configuration

Control access to resource groups to limit the scope of permissions.

Practical Steps

1. **Select Resource Group**:
   - In **PIM > Azure resources**, choose a resource group.
2. **Assign Roles**:
   - Click **Roles > Add assignment**, select a role, and assign it to a user or group.
3. **Verify Assignment**:
   - Check the assignment in the “Assignments” tab.

5.3 Resource-Level Configuration

For fine-grained control, configure PIM for individual resources like VMs or databases.

Practical Steps

1. **Navigate to Resource**:
   - In **PIM > Azure resources**, select a specific resource (e.g., a virtual machine).
2. **Assign Roles**:
   - Add eligible users for roles like “Virtual Machine Contributor.”
3. **Set Conditions**:
   - Configure activation settings similar to Azure AD roles.

5.4 Troubleshooting Resource Access

- **Issue**: User cannot activate a role.
- **Solution**: Verify the user is assigned as eligible and has the correct license.
- **Issue**: Resource not visible in PIM.
- **Solution**: Ensure the subscription is registered for PIM management.

6. Configure Privileged Access Groups

Theory

Privileged Access Groups are security groups that can be assigned roles, allowing scalable role management. Users added to these groups become eligible for role activation.

6.1 Creating Privileged Access Groups

Practical Steps

1. **Create a Group**:
   - Go to **Microsoft Entra ID > Groups > New group**.
   - Select **Security** as the group type.
2. **Enable Role Assignment**:
   - Under **Group settings**, enable "Azure AD roles can be assigned to the group."
3. **Add Members**:
   - Add users or nested groups to the privileged access group.

6.2 Managing Group Membership

- Use dynamic groups for automatic membership based on user attributes.
- Regularly audit group members to ensure only authorized users are included.

6.3 Group-Based Role Assignment

1. **Assign Roles to Group**:
   - In **PIM > Azure AD roles > Assignments**, select the group and assign a role.
2. **Configure Activation**:
   - Set activation conditions like MFA or approval.

7. Set up PIM Requests and Approval Process

Theory

PIM's approval workflows ensure that role activations are reviewed by designated approvers, adding an extra layer of security.

7.1 Configuring Approval Workflows

Practical Steps

1. **Access Role Settings**:
    - Go to **PIM > Azure AD roles > Roles > Settings**.
2. **Enable Approval**:
    - Select a role and enable "Require approval to activate."
3. **Add Approvers**:
    - Specify users or groups as approvers.

7.2 Managing Approvers

- Use security groups for approvers to simplify management.
- Rotate approvers periodically to prevent privilege creep.

7.3 Automating Approval Processes

- Integrate with **Azure Logic Apps** for automated approval notifications.
- Use **Microsoft Teams** or email for approval alerts.

8. Analyse PIM Audit History and Reports

Theory

PIM provides detailed audit logs to track role activations, assignments, and approval activities, supporting compliance and security monitoring.

8.1 Accessing Audit Logs

Practical Steps

1. **Navigate to Audit History**:
    - Go to **PIM > Audit history**.
2. **Filter Logs**:
    - Filter by user, role, time range, or action (e.g., activation, assignment).
3. **Export Logs**:
    - Download logs for external analysis or compliance reporting.

8.2 Generating Reports

- Use **Azure Monitor** to create custom reports on PIM activities.
- Schedule recurring reports for compliance reviews.

8.3 Compliance and Governance

- Map PIM audit logs to compliance frameworks (e.g., GDPR, SOC 2).
- Retain logs for the required retention period (e.g., 7 years for some regulations).

9. Create and Manage Break-Glass Accounts

Theory

Break-glass accounts are emergency accounts with permanent privileged access, used only in critical situations. They are excluded from PIM to ensure availability but must be tightly controlled.

9.1 Setting Up Break-Glass Accounts

Practical Steps

1. **Create Account**:
   - In **Microsoft Entra ID > Users**, create a dedicated user (e.g., “breakglassadmin”).
   - Assign the **Global Administrator** role permanently.
2. **Secure Account**:
   - Enable MFA and store credentials in a secure vault (e.g., Azure Key Vault).
3. **Exclude from PIM**:
   - Ensure the account is not managed by PIM to guarantee emergency access.

9.2 Monitoring Break-Glass Usage

- Configure **Azure Monitor** alerts for break-glass account activity.
- Log all access attempts in a secure audit trail.

9.3 Security Best Practices

- Limit the number of break-glass accounts (typically 2–3).
- Store credentials in a physical or digital vault with restricted access.

- Review usage monthly to detect unauthorized access.

10. Explore Eligible and Active Roles

Theory

PIM distinguishes between **Eligible** roles (requiring activation) and **Active** roles (persistent access). Eligible roles align with JIT access, while active roles are used sparingly for critical functions.

10.1 Understanding Role Types

- **Eligible Roles**: Users must activate the role, subject to approval and time limits.
- **Active Roles**: Users have constant access without activation.

10.2 Managing Role Assignments

Practical Steps

1. **View Assignments**:
   - Go to **PIM > Azure AD roles > Assignments**.
2. **Toggle Role Type**:
   - Switch between "Eligible" and "Active" when assigning roles.
3. **Review Assignments**:
   - Regularly audit to ensure only necessary roles are active.

10.3 Role Activation Scenarios

- **Scenario 1**: A sysadmin activates the "Contributor" role to deploy resources.
- **Scenario 2**: An auditor activates a "Reader" role for a compliance review.

11. Set Role Time Limits

Theory

Setting time limits for role activations ensures that privileges are revoked automatically, reducing the risk of prolonged access.

11.1 Configuring Time Limits

Practical Steps

1. **Edit Role Settings**:
   - Go to **PIM > Azure AD roles > Roles > Settings**.
   - Select a role and set the **Activation Maximum Duration** (e.g., 4 hours).
2. **Apply Policy**:
   - Save and verify the policy in the PIM dashboard.

11.2 Enforcing Time-Based Policies

- Use short durations for sensitive roles (e.g., 1–2 hours for Global Administrator).
- Notify users before role expiration to prevent disruptions.

11.3 Handling Expirations

- Configure alerts for role expirations using **Azure Monitor**.
- Allow users to request extensions if needed, subject to approval.

12. Advanced PIM Features

12.1 Integration with Azure Monitor

- Create alerts for unusual PIM activities (e.g., frequent role activations).
- Use **Log Analytics** to analyze PIM logs in depth.

12.2 Conditional Access Integration

- Combine PIM with **Conditional Access** policies to enforce location or device-based restrictions.
- Example: Require activation only from corporate networks.

12.3 Automation with PowerShell

Use PowerShell to automate PIM tasks, such as role assignments or audit log exports.

Example PowerShell Script

```
Connect-AzureAD

# Assign a user as eligible for a role
```

```
$role = Get-AzureADDirectoryRole | Where-Object {$_.DisplayName -eq "Global Administrator"}
$user = Get-AzureADUser -ObjectId "user@contoso.com"
Add-AzureADDirectoryRoleMember -ObjectId $role.ObjectId -RefObjectId $user.ObjectId
```

13. Case Studies

13.1 Enterprise Deployment Example

A multinational corporation implemented PIM to secure access to its Azure subscriptions. By using JIT access and approval workflows, they reduced unauthorised access incidents by 60%.

13.2 Small Business Use Case

A small business used PIM to grant temporary access to a contractor for database management. The contractor activated the “Contributor” role for 2 hours, completing the task without permanent access.

13.3 Compliance-Driven Implementation

A healthcare organisation used PIM to meet HIPAA requirements by enforcing MFA, approvals, and audit logging for all privileged roles.

14. Troubleshooting

14.1 Common Issues and Solutions

- **Issue**: User cannot activate a role.
- **Solution**: Verify the user is assigned as eligible and has the correct license.
- **Issue**: Resource not visible in PIM.
- **Solution**: Ensure the subscription is registered for PIM management.

14.2 Specific Issues Encountered with Student Azure Plan

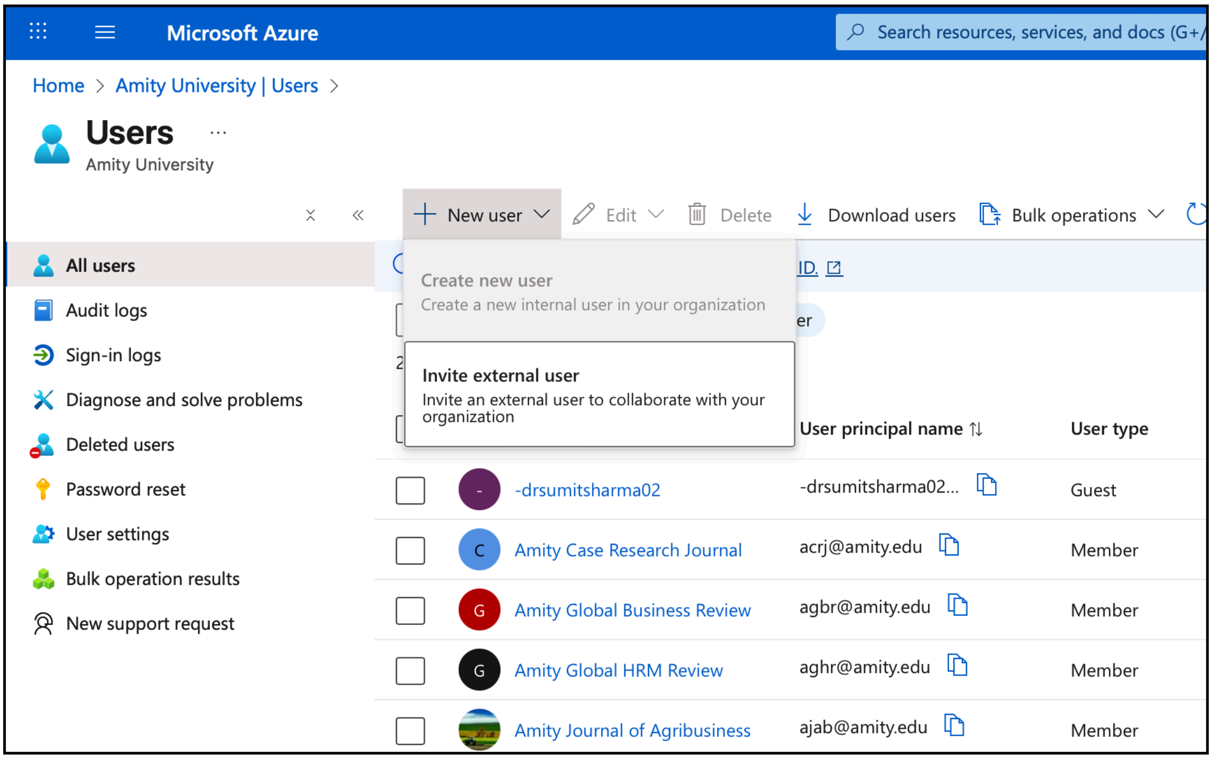
During the implementation of Azure PIM, specific challenges were encountered when attempting to assign roles under a student Azure plan subscription. Below are the issues faced, their potential causes, and recommended solutions:

Issue 1: Unable to Create a New User (Option Disabled)

- **Description**: When attempting to create a new user in **Microsoft Entra ID > Users > New user**, the option to create a user was disabled or greyed out.

- **Potential Causes**:
  1. **Limited Permissions**: The account used may lack the necessary permissions, such as **User Administrator** or **Global Administrator**, to create users.
  2. **Student Plan Restrictions**: Azure for Students subscriptions often have limitations, such as restricted access to certain Microsoft Entra ID features or user management capabilities.
  3. **Tenant Configuration**: The tenant may have policies (e.g., Conditional Access or role-based restrictions) that disable user creation for certain accounts.

- **Solutions**:
  1. **Verify Permissions**:
     - Ensure the account has **Global Administrator** or **User Administrator** privileges. Navigate to **Microsoft Entra ID > Roles and administrators** to check.
     - If permissions are missing, contact the tenant administrator to grant the necessary roles.
  2. **Check Subscription Type**:
     - Confirm the subscription is an Azure for Students plan, which may restrict user creation. Consider upgrading to a pay-as-you-go or enterprise subscription for full functionality.
  3. **Use an Existing User**:
     - If user creation is disabled, try assigning roles to an existing user in the tenant.
  4. **Contact Azure Support**:
     - If the issue persists, open a support ticket via the Azure Portal to clarify restrictions specific to the student plan.



	User principal name	User type
-drsumitsharma02	-drsumitsharma02...	Guest
Amity Case Research Journal	acrj@amity.edu	Member
Amity Global Business Review	agbr@amity.edu	Member
Amity Global HRM Review	aghr@amity.edu	Member
Amity Journal of Agribusiness	ajab@amity.edu	Member

Figure 14.2.1: Disabled “New user” option in Microsoft Entra ID.

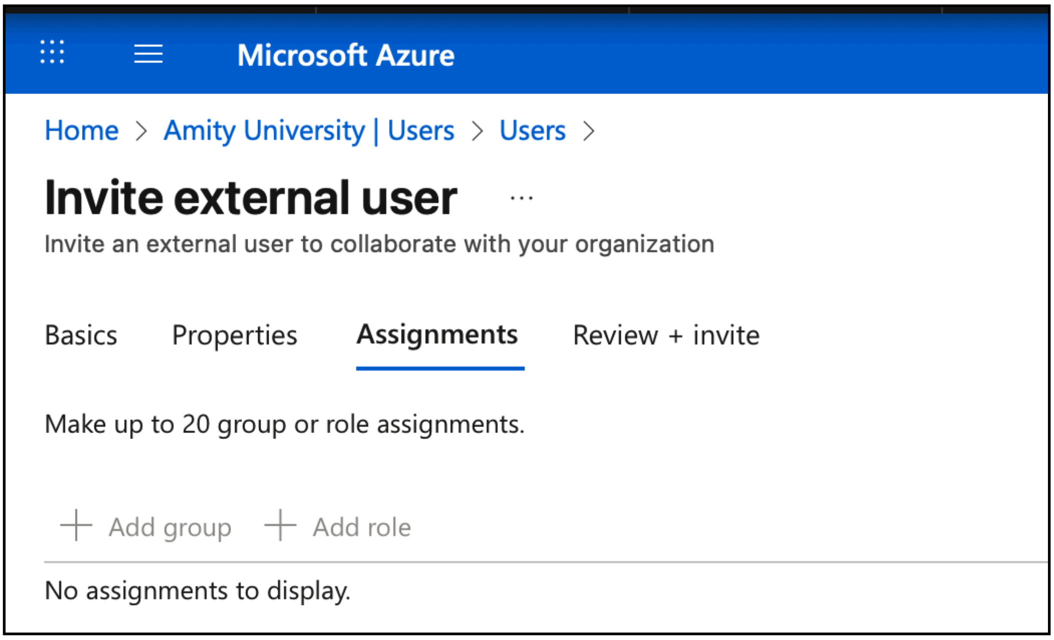
Issue 2: Unable to Assign Roles After Inviting a User (Option Disabled)

- **Description**: After attempting to invite a guest user via **Microsoft Entra ID > Users > New guest user**, the option to assign a role in PIM was disabled or greyed out.

- **Potential Causes**:
  1. **Guest User Limitations**: Guest users may not be eligible for certain roles in PIM due to tenant restrictions or subscription limitations.
  2. **PIM Configuration**: The role assignment feature may not be fully enabled for the subscription or tenant.
  3. **License Requirements**: The invited user may not have an Azure AD Premium P2 license assigned, which is required for PIM role assignments.

- **Solutions**:
  1. **Assign Licenses**:
     - Navigate to **Microsoft Entra ID > Licenses > All products** and assign an Azure AD Premium P2 license to the guest user.

2. **Enable Role Assignability**:
   - Ensure the role is configured for PIM management. Go to **PIM > Azure AD roles > Roles** and verify the role is listed.
3. **Use Internal Users**:
   - If guest users face restrictions, try assigning roles to internal users within the tenant.
4. **Check Tenant Policies**:
   - Review **Microsoft Entra ID > User settings** to ensure guest user invitations are enabled and not restricted by policies.



Microsoft Azure

Home > Amity University | Users > Users >

Invite external user ...

Invite an external user to collaborate with your organization

Basics Properties Assignments Review + invite

Make up to 20 group or role assignments.

+ Add group + Add role

No assignments to display.

Figure 14.2.2: Disabled role assignment option for an invited user.

Issue 3: No Roles Available for Assignment to a Group in Student Azure Plan

- **Description**: After creating a new security group and adding members, no roles were available to assign to the group in **PIM > Azure AD roles > Assignments** under the student Azure plan subscription.

- **Potential Causes**:

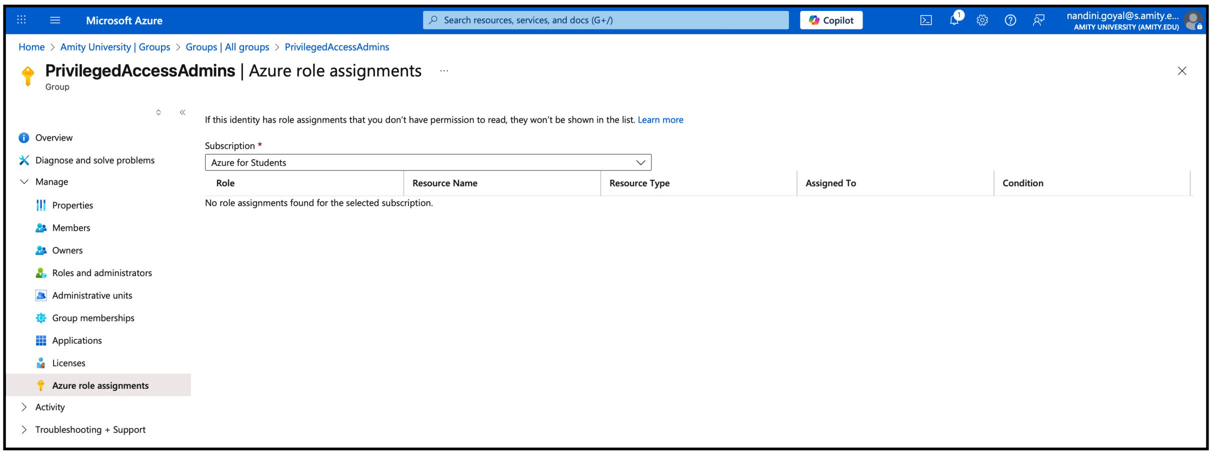
1. **Student Plan Limitations**: Azure for Students subscriptions may not support assigning roles to groups in PIM due to restricted RBAC capabilities.

2. **PIM Not Enabled for Subscription**: The subscription may not be fully onboarded to PIM for Azure resources or Azure AD roles.
3. **Role Scope Issues**: The roles may not be available at the subscription level used in the student plan.

- **Solutions**:

1. **Verify PIM Enablement**:
   - Go to **PIM > Azure resources** and ensure the subscription is listed and enabled for PIM. If not, select the subscription and click **Enable PIM**.
   - For Azure AD roles, ensure PIM is enabled in **Microsoft Entra ID > PIM > Azure AD roles**.
2. **Check Subscription Type**:
   - Confirm that the Azure for Students subscription supports PIM group-based role assignments. If not, consider using a different subscription type or assigning roles directly to users.

3. **Use Azure AD Roles**:
   - Instead of resource-level roles, try assigning Azure AD roles (e.g., User Administrator) to the group, as these may be less restricted.
4. **Contact Azure Support**:
   - Open a support ticket to clarify whether the student plan supports group-based role assignments in PIM. Provide details about the subscription and the specific roles attempted.
5. **Workaround with Individual Users**:
   - Assign roles directly to individual users instead of groups until the limitation is resolved.


Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
nandini.goyal@s.amity.e...
AMITY UNIVERSITY (AMITY.EDU)
Home > Amity University | Groups > Groups | All groups > PrivilegedAccessAdmins
Overview
Diagnose and solve problems
Manage
Properties
Members
Owners
Roles and administrators
Administrative units
Group memberships
Applications
Licenses
Azure role assignments
Activity
Troubleshooting + Support

PrivilegedAccessAdmins | Azure role assignments

Group

If this identity has role assignments that you don't have permission to read, they won't be shown in the list. Learn more

Subscription *

Azure for Students

Role	Resource Name	Resource Type	Assigned To	Condition

No role assignments found for the selected subscription.

Figure 14.2.3: No roles available for group assignment in PIM.

15. Conclusion

Azure Privileged Identity Management is a powerful tool for securing privileged access in Azure environments. By implementing JIT access, approval workflows, and audit logging, organisations can reduce security risks, ensure compliance, and maintain operational efficiency. Regular reviews, automation, and adherence to best practices will maximise PIM’s effectiveness.

16. References

- Azure PIM Documentation – Microsoft Learn
- Azure AD Premium Licensing
- Video: Azure PIM Full Tutorial – YouTube
- Microsoft Entra ID Governance