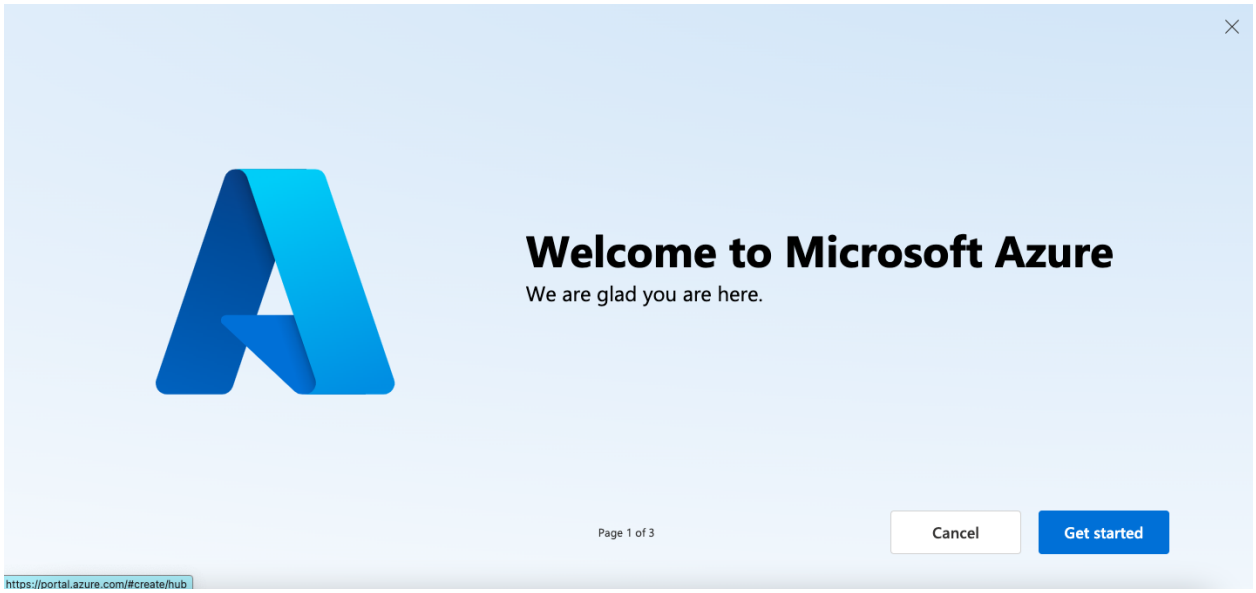
Privileged Identity Management

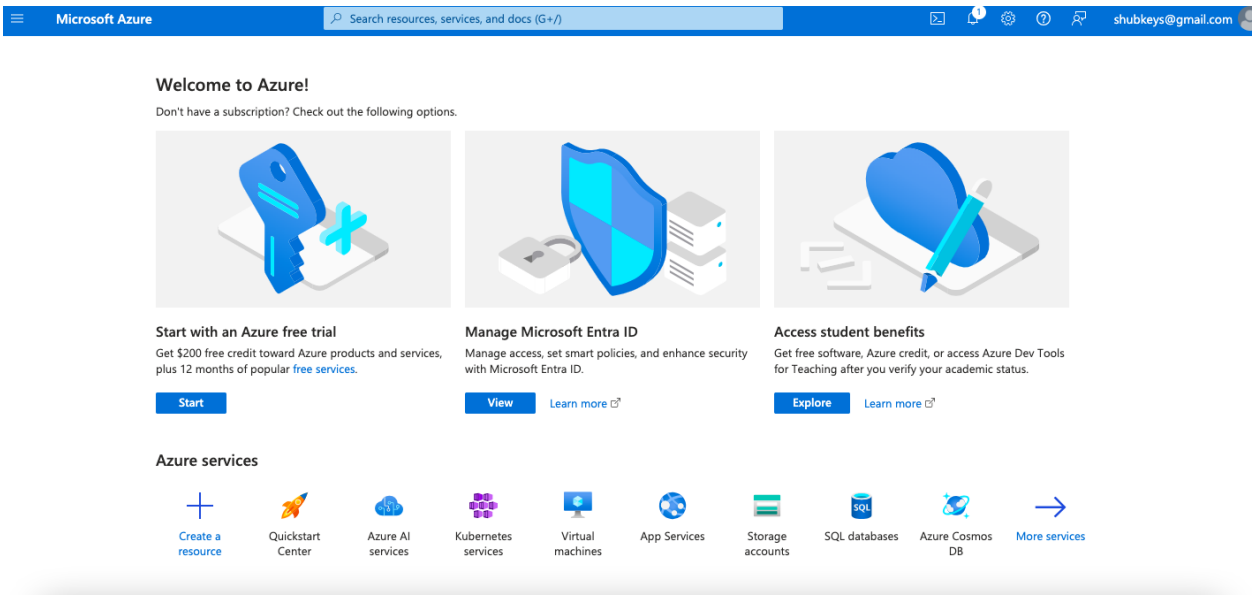
1.1. Verify Azure AD Premium P2 Licenses

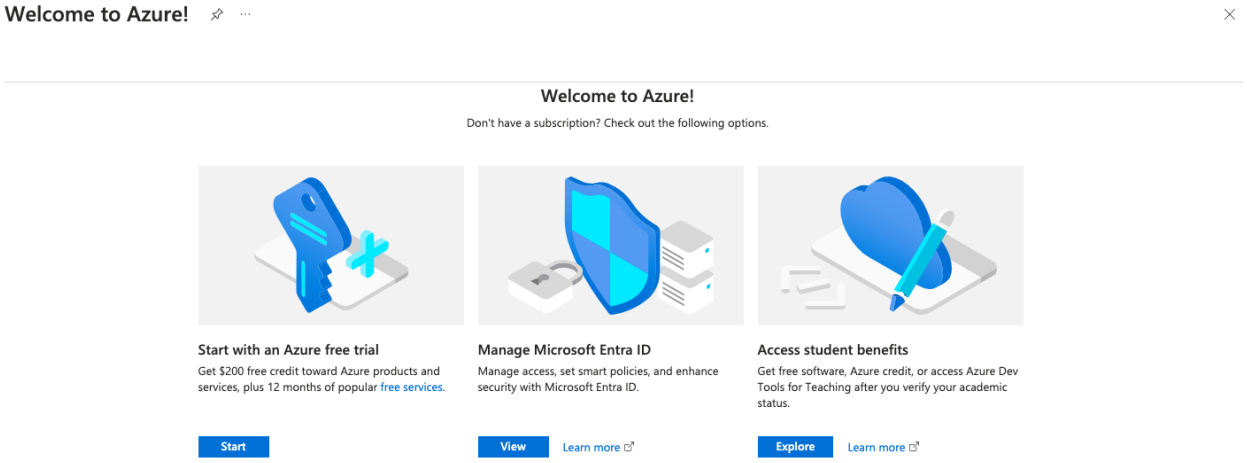
1. Sign into the Azure portal: [Azure Portal](https://portal.azure.com)
2. Navigate to Azure Active Directory:
   - In the left-hand navigation pane, select "Azure Active Directory".
3. Check Licenses:
   - Under "Manage", select "Licenses".
   - Click on "All products" to view all your subscriptions.
   - Ensure that the "Azure AD Premium P2" license is listed.
   - If not, acquire the necessary licenses from Microsoft or your licensing provider.
4. Assign Licenses:
   - Still under "Licenses", select "Assign".
   - Choose the users who need PIM access.
   - Click on "Assign" to allocate the licenses.

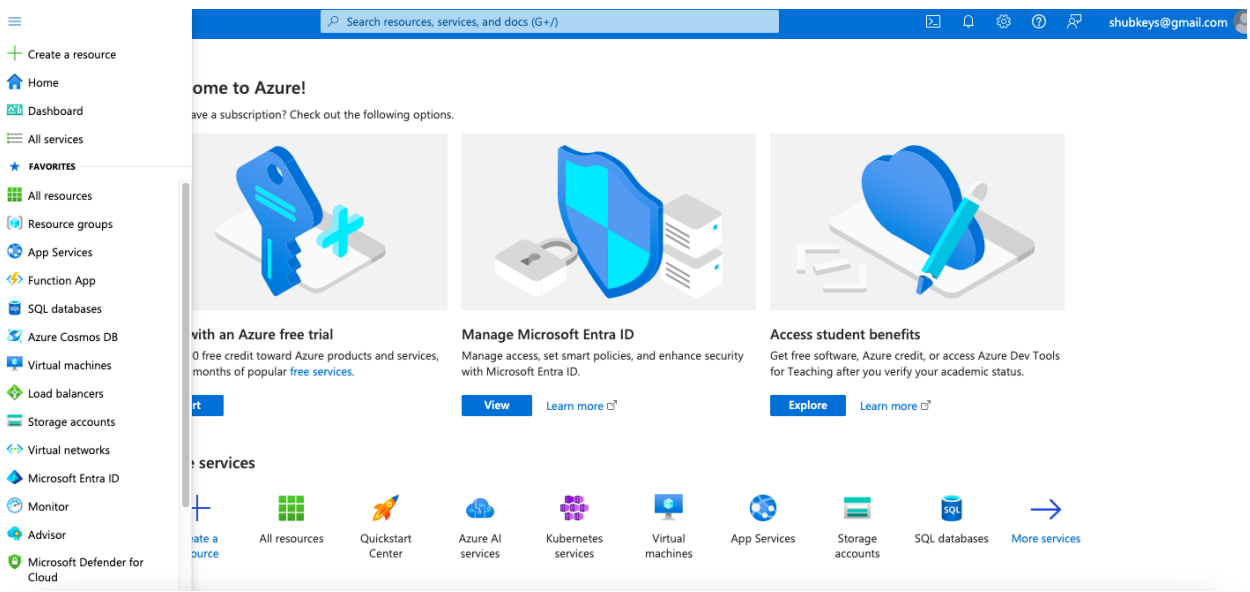
1.2. Assign Administrative Roles

1. Navigate to Roles and Administrators:
   - In Azure AD, under "Manage", select "Roles and administrators".
2. Assign Roles:
   - Select the role you need to assign (e.g., "Global Administrator" or "Privileged Role Administrator").
   - Click on the role name to open its settings.
   - Click on "Assignments" and then "Add assignment".
   - Search for and select the user(s) you want to assign the role to.
   - Click "Add" to complete the assignment.




Microsoft Azure
Search resources, services, and docs (G+/)
shubkeys@gmail.com
Welcome to Azure!
Don't have a subscription? Check out the following options.
Start with an Azure free trial
Get $200 free credit toward Azure products and services, plus 12 months of popular free services.
Start
Manage Microsoft Entra ID
Manage access, set smart policies, and enhance security with Microsoft Entra ID.
View
Learn more
Access student benefits
Get free software, Azure credit, or access Azure Dev Tools for Teaching after you verify your academic status.
Explore
Learn more
Azure services
Create a resource
Quickstart Center
Azure AI services
Kubernetes services
Virtual machines
App Services
Storage accounts
SQL databases
Azure Cosmos DB
More services


Welcome to Azure!
Welcome to Azure!
Don't have a subscription? Check out the following options.
Start with an Azure free trial
Get $200 free credit toward Azure products and services, plus 12 months of popular free services.
Start
Manage Microsoft Entra ID
Manage access, set smart policies, and enhance security with Microsoft Entra ID.
View
Learn more
Access student benefits
Get free software, Azure credit, or access Azure Dev Tools for Teaching after you verify your academic status.
Explore
Learn more


Search resources, services, and docs (G+/)
shubkeys@gmail.com
Create a resource
Home
Dashboard
All services
FAVORITES
All resources
Resource groups
App Services
Function App
SQL databases
Azure Cosmos DB
Virtual machines
Load balancers
Storage accounts
Virtual networks
Microsoft Entra ID
Monitor
Advisor
Microsoft Defender for Cloud
ome to Azure!
ave a subscription? Check out the following options.
vith an Azure free trial
0 free credit toward Azure products and services,
months of popular free services.
Manage Microsoft Entra ID
Manage access, set smart policies, and enhance security with Microsoft Entra ID.
View
Learn more
Access student benefits
Get free software, Azure credit, or access Azure Dev Tools for Teaching after you verify your academic status.
Explore
Learn more
services
All resources
Quickstart Center
Azure AI services
Kubernetes services
Virtual machines
App Services
Storage accounts
SQL databases
More services

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

2.1. Enable Just-In-Time Access

1. Navigate to Privileged Identity Management:
   - In the Azure portal, go to "Azure AD" and then select "Privileged Identity Management".
2. Select Role Management:
   - Choose either "Azure AD roles" or "Azure resources" based on your needs.
3. Enable JIT for Roles:
   - Click on "Manage" and then "Roles".
   - Select the role you want to configure for JIT.
   - Click on "Settings".
   - Under "Assignment type", ensure "Eligible" is selected.
   - Configure the settings to require activation, such as multi-factor authentication (MFA) and approval.

2.2. Set Activation Duration

1. Configure Activation Settings:
   - In the role settings, find the "Activation" section.
   - Set the "Maximum activation duration (hours)" to the desired time limit (e.g., 4 hours).
   - Save the changes.

3. Configure Azure Roles in PIM, Including Settings and Assignments

3.1. Navigate to PIM

1. Access Privileged Identity Management:
   - Go to "Azure AD" -> "Privileged Identity Management".

3.2. Select Azure AD Roles

1. Manage Roles:
   - In PIM, select "Azure AD roles".
   - Click on "Manage" -> "Roles".

3.3. Configure Role Settings

1. Select and Configure Role:
   - Choose a role (e.g., "Global Administrator").
   - Click on the role to open its settings.
2. Set Activation Requirements:
   - Under "Settings", configure:
     - Require MFA: Ensure Multi-Factor Authentication is enabled.
     - Justification: Require a reason for activation.
     - Approval: Configure who needs to approve the activation.

3. Set Activation Duration:
   - Define how long the role remains active upon activation.

3.4. Assign Roles

1. Assign Users:
   - Under "Assignments", click "Add assignment".
   - Choose the users to assign the role to.
   - Select the assignment type: "Eligible" or "Active".
   - Click "Add" to finalize.

4. Configure Azure Resources in PIM, Including Settings and Assignments

4.1. Select Azure Resources

1. Manage Resources:
   - In PIM, select "Azure resources".
   - Choose the subscription or resource group to manage.

4.2. Configure Resource Role Settings

1. Select Resource Role:
   - Click on a role (e.g., "Owner") to open its settings.
2. Set Activation Requirements:
   - Under "Settings", configure:
     - Require MFA: Ensure Multi-Factor Authentication is required.
     - Justification: Require a reason for activation.
     - Approval: Set up the approval process.
3. Set Activation Duration:
   - Define the duration the role can be active (e.g., 2 hours).

4.3. Assign Resource Roles

1. Assign Users to Roles:
   - Under "Assignments", click "Add assignment".
   - Select the users and define the assignment type: "Eligible" or "Active".
   - Click "Add" to complete.

5. Configure Privileged Access Groups

5.1. Navigate to Groups in PIM

1. Access Groups:
   - In Azure AD, go to "Groups".
   - Select "Privileged access groups".

5.2. Create and Configure Group

1. Create Group:
   - Click "New group".
   - Provide a name and description for the group.
   - Select "Assigned" as the group type.
   - Under "Privileged access", enable "Azure AD roles can be assigned to the group".
2. Configure Group Settings:
   - Set the group settings to manage privileged access roles.
   - Define the roles (e.g., Owner, Contributor) to be assigned to the group.

5.3. Assign Members to Groups

1. Add Members:
   - Go to the group's "Members" section.
   - Click "Add members".
   - Select users to be added to the group.
   - Define eligibility and activation settings for these users.

6. Set Up PIM Requests and Approval Process

6.1. Configure Approval Workflow

1. Access Approval Settings:
   - In PIM, go to "Azure AD roles" or "Azure resources".
   - Click on "Approval" settings.
2. Define Approvers:
   - Specify the approvers for role activation requests.
   - Ensure approvers have the appropriate permissions.

6.2. Set Up Access Requests

1. Request Access:
   - Users go to "Azure AD" -> "PIM".
   - They select the role or resource they need access to.
   - Submit a request with justification.
2. Approval Process:
   - Approvers receive a notification of the request.
   - Approvers review the request and approve or deny it.

7. Analyze PIM Audit History and Reports

7.1. Access PIM Audit Logs

1. View Audit History:
   - In PIM, go to "Audit history".

- Review logs of role activations, assignments, and approvals.

7.2. Generate Reports

1. Generate Compliance Reports:
  - In the audit history, generate reports based on specific criteria (e.g., time range, user activity).
  - Export reports for compliance and review.

8. Create and Manage Break-Glass Accounts

8.1. Create Break-Glass Accounts

1. Set Up Emergency Accounts:
  - Create dedicated break-glass accounts in Azure AD.
  - Assign high-level privileges (e.g., Global Administrator).
  - Use strong, unique passwords and store them securely (e.g., in a password vault).

8.2. Monitor and Review

1. Regular Reviews:
  - Periodically review the usage and access of break-glass accounts.
  - Implement alerts for any login attempts to these accounts.

9. Explore Eligible and Active Roles

9.1. View Eligible Roles

1. Check Eligible Assignments:
  - In PIM, go to "Assignments".
  - View roles where users have eligible status and can activate the role when needed.

9.2. Manage Active Roles

1. Check Active Assignments:
  - In PIM, view roles currently active.
  - Ensure activations comply with policies.

10. Set the Time Limit of the Roles

10.1. Configure Role Duration

1. Set Activation Time Limit:
  - In PIM, select the role settings.
  - Set the "Maximum activation duration (hours)" to a specific limit (e.g., 1 hour, 4 hours).
  - Save the settings to enforce the time limit.

Access Request and Approval Workflow

Detailed Workflow Process:

1. User Requests Owner Role

1. Submit Role Request:
   - User navigates to "Azure AD" -> "PIM".
   - Selects the subscription and requests the "Owner" role.
   - Provides justification for the request.
   - Submits the request.

2. Approval Process

1. Approve Request:
   - Approver receives a notification of the request.
   - Reviews the request details and justification.
   - Approves or denies the request.
   - User is notified of the decision.

3. User Requests Group Assignment

1. Submit Group Request:
   - User requests to join a privileged access group.
   - Provides justification and submits the request.
2. Approval and Assignment:
   - Approver reviews and approves the group request.
   - User is assigned the "Contributor" role on the subscription upon approval.