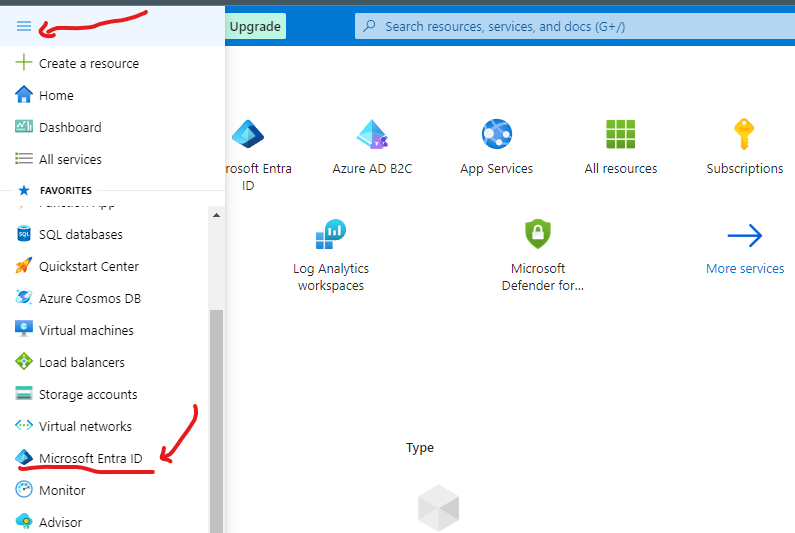
**Step 1: Login to Azure Portal**: Once your account is set up, log in to the Azure portal using your credentials.

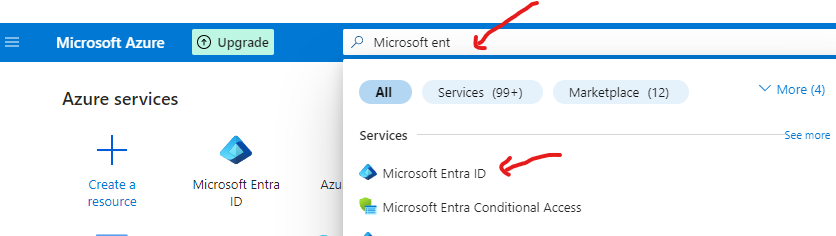
**Step 2: Create a New Azure Active Directory (AD) Tenant**

**Note***: Microsoft renamed* ***Azure Active Directory (Azure AD) to Microsoft Entra ID*** *to communicate the multi-cloud, multiplatform functionality of the products, alleviate confusion with Windows Server Active Directory, and unify the*[*Microsoft Entra*](https://learn.microsoft.com/en-us/entra)*product family.* (Microsoft, 03/05/2024)

1. **Navigate to Azure Active Directory/Microsoft Entra ID**:

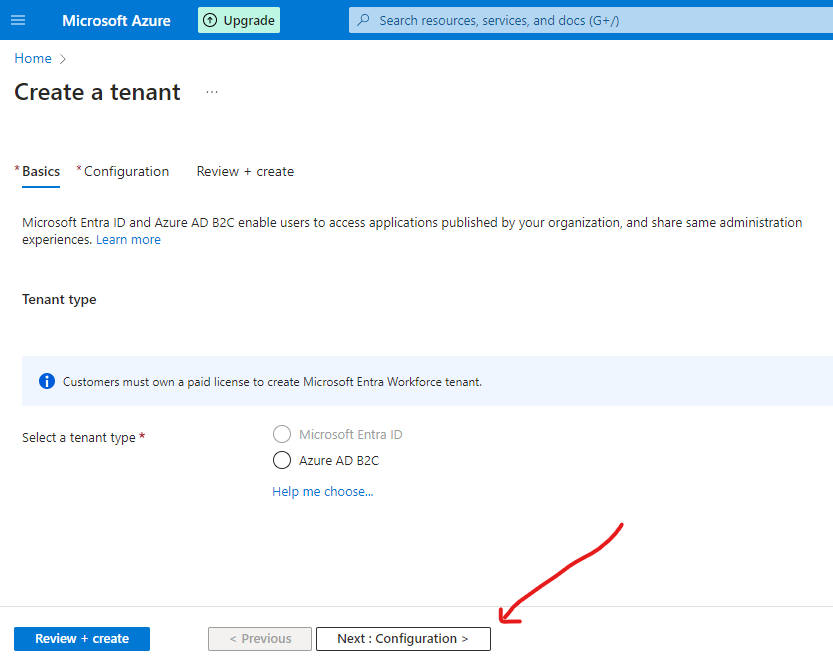
* Once logged into the Azure portal, select the **Menu** (three horizontal lines in the top-left corner) or the **Home** icon.
* In the sidebar, find and click on **Microsoft Entra ID**.



* Alternatively, In the Azure portal, search for "***Microsoft Entra ID***" in the search bar and select it from the results.

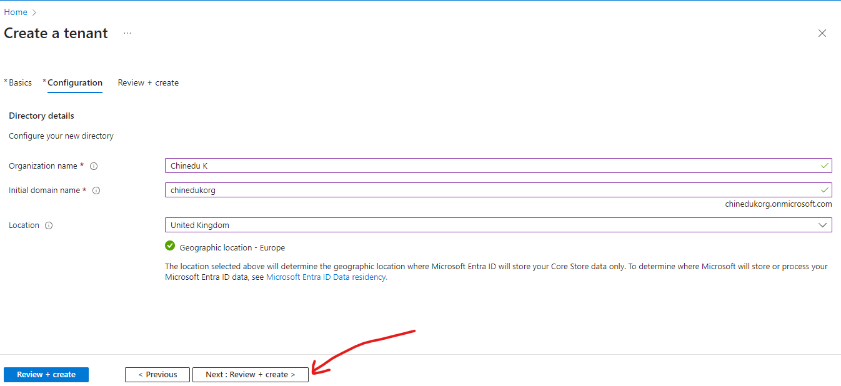
1. **Create a New Tenant**:

* In the Microsoft Entra ID pane, select **Create a tenant**.
* Choose **Azure Active Directory** (now part of Microsoft Entra) as the type.
* Click **Next: Configuration**.



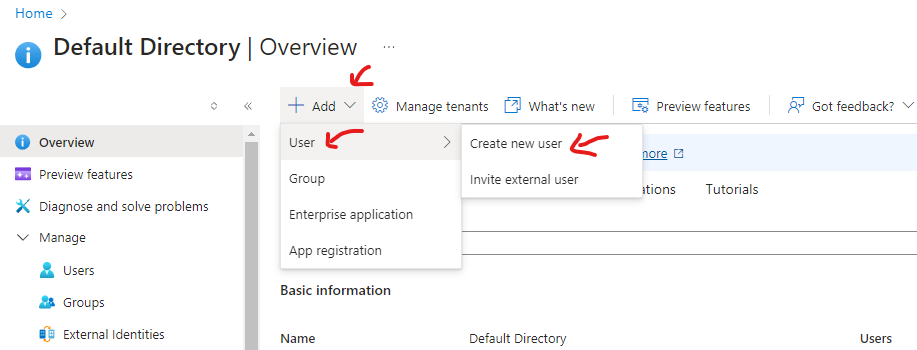
1. **Configure Your Tenant**:

* **Organization Name**: Enter a name for your directory.
* **Initial Domain Name**: Specify a domain name (e.g., "mycompany.onmicrosoft.com").
* **Country/Region**: Select the appropriate country.
* Click **Review + Create**, then click **Create**.
* Assign to **resource group**



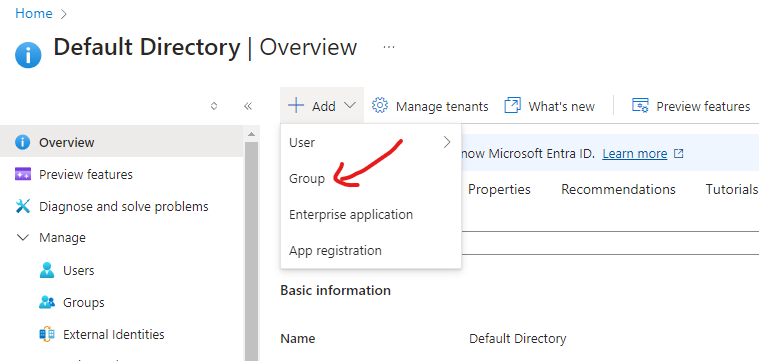
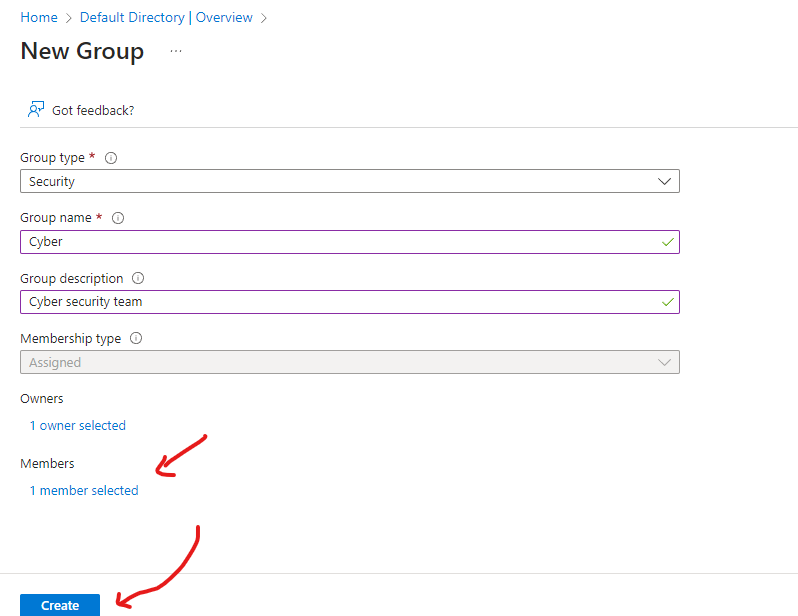
**Step 3: Manage Users and Groups**

1. **Add Users**:
   * In your Microsoft Entra ID tenant, go to **Users**.
   * Click **New user** and enter the required details, including username and password.
   * Click **Create**.



**Invite External Users (Guests) (OPTIONAL)**:

* For B2B collaboration, you can invite external users.
* Click **New user** > **Invite external user**.
* Provide the user’s email, configure their role, and send the invite.

1. **Create Groups**:
   * Go to **Groups**.
   * Click **New group**.
   * Choose the type (e.g., Security group), and enter a name and description.
   * Add members, then click **Create**.

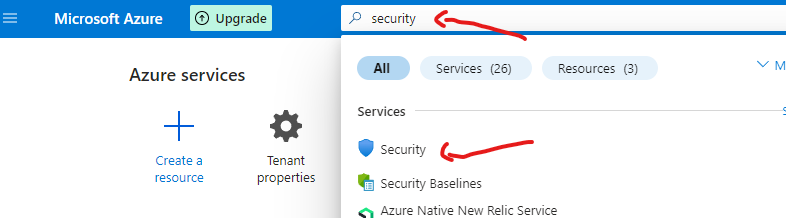
**Step 4: Integrate On-Premises AD with Azure AD (Optional)**

If you have an on-premises Active Directory and want to sync it with Azure AD:

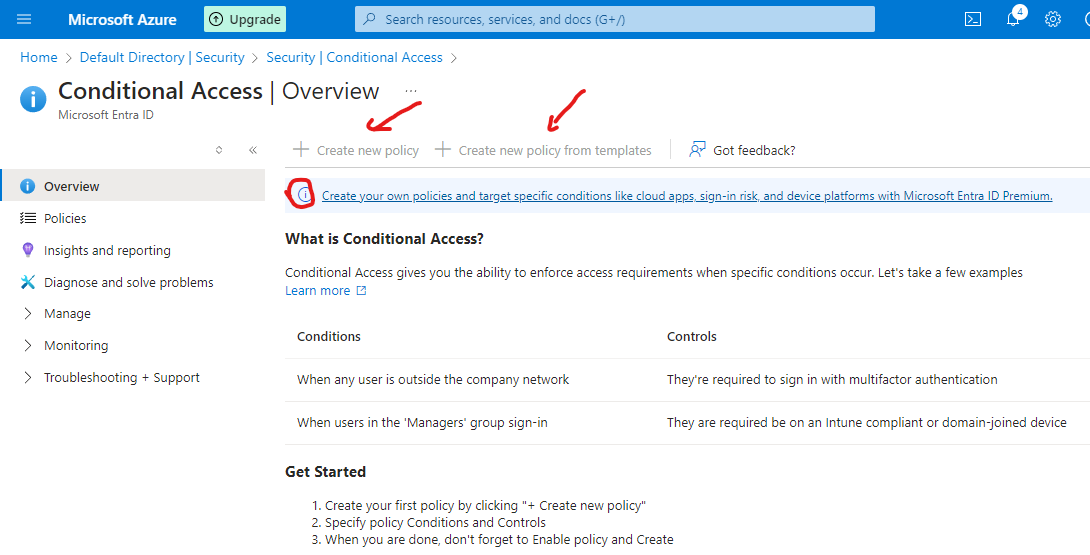
1. **Install Azure AD Connect**:
   * Download the Azure AD Connect tool from the Azure portal.
   * Install the tool on your on-premises server.
2. **Configure Azure AD Connect**:
   * During setup, choose the **Express Settings** for a simple configuration or **Customize** for more control.
   * Enter your Azure AD and on-premises AD credentials.
   * Configure synchronization options (e.g., Password Sync, Federation).
   * Finish the setup and start the initial sync.
3. **Verify Sync**:
   * After syncing, verify that users from on-premises AD are now visible in Azure AD under **Users**.

**Step 5: Configure Security Features**

1. **Set Up Multi-Factor Authentication (MFA)**:
   * In Microsoft Entra ID, go to **Security >Manage> Authentication methods**.
   * Enable and configure MFA settings as required.



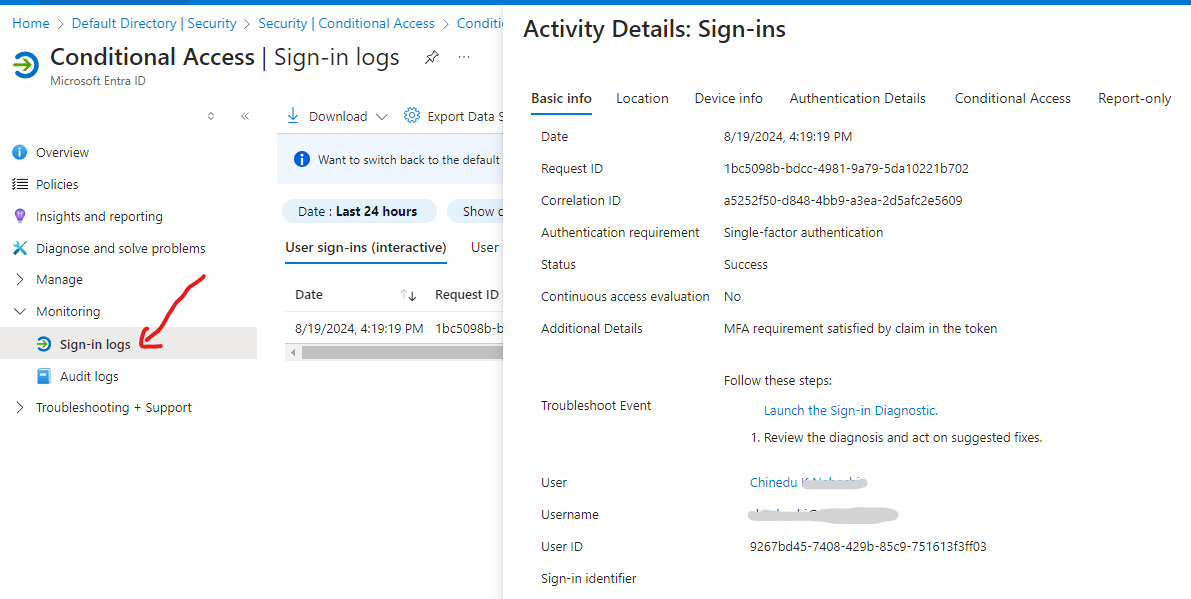
1. **Configure Conditional Access Policies**:
   * **Under Security > Protect > Conditional Access.**
   * Create policies based on conditions such as location, device compliance, etc.
   * Define controls like MFA, block access, or allow access with restrictions.



**6. Monitor and Audit Microsoft Entra ID**

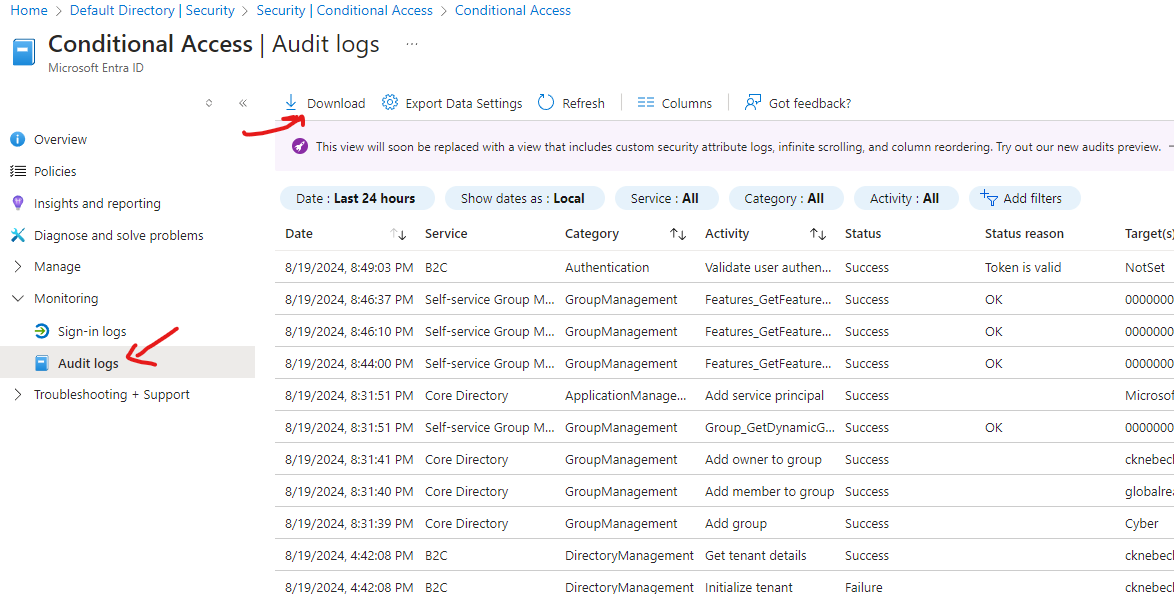
**A. Sign-In Monitoring**

1. **View Sign-In Logs**:
   * Go to **Monitoring > Sign-ins**.
   * Review detailed sign-in logs, including successful and failed sign-ins, MFA challenges, and suspicious activities.



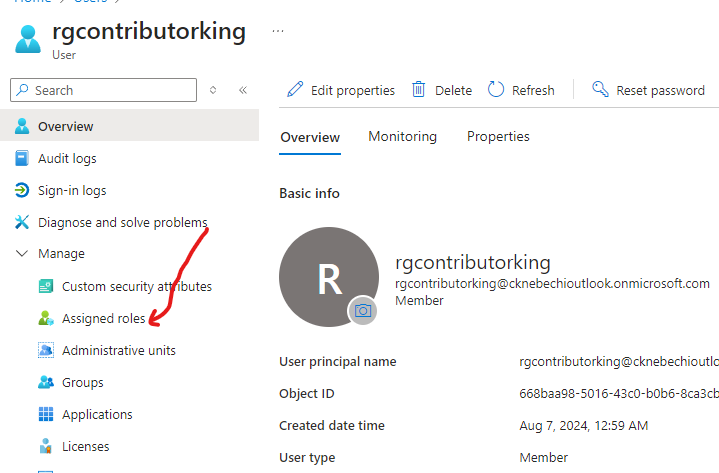
**B. Audit Logs**

1. **Access Audit Logs**:
   * Navigate to **Monitoring > Audit logs** to track changes within the Microsoft Entra ID environment.
   * This includes activities like user creation, group changes, and policy updates.
2. **Export Logs**:
   * Logs can be exported for compliance and further analysis.
   * Use Azure Monitor and Log Analytics for more advanced monitoring and alerting.

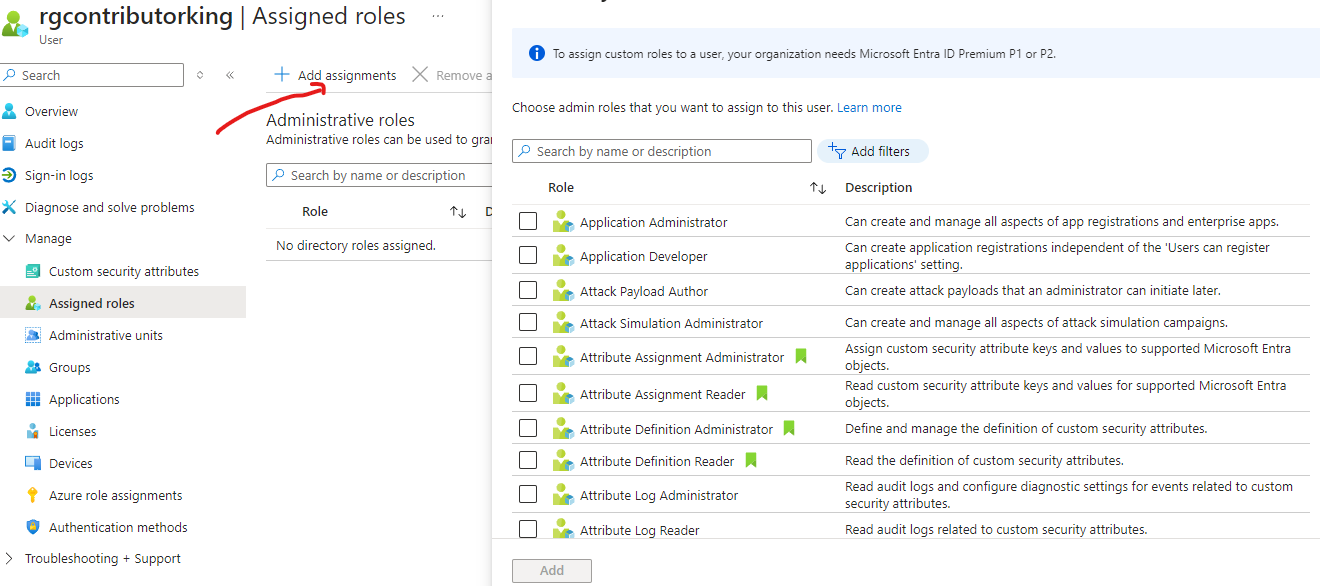


**Step 7: Assign Roles and Permissions**

1. **Assign Roles**:
   * In the **Users** section, select a user and go to **Roles and administrators**.



* + Assign appropriate roles like Global Administrator, User Administrator, etc.



**8: Stay Updated and Maintain Your Environment**

1. **Regular Updates**:
   * Staying informed about updates and new features in Microsoft Entra ID is paramount.
   * Regularly review and update security settings and policies.
2. **Training and Documentation**:
   * Explore Microsoft Learn for tutorials and best practices.
   * Utilise official documentation for detailed guidance on advanced configurations.

By following these steps, a robust identity and access management system set up with Microsoft Entra ID, ensuring organisation’s security and compliance needs are met while maintaining flexibility and scalability.