Step-by-Step Guide – Integrating RedOrange Application with Microsoft Entra ID (Azure AD) for SAML Single Sign-On and Automated User Provisioning

1. Understand the prerequisites

Before starting, ensure the following:

- You have access to Microsoft Entra ID (formerly Azure Active Directory) with one of these roles:
    - Cloud Application Administrator
    - Application Administrator
    - Global Administrator
- You have admin-level access to the RedOrange Application with permissions to configure Identity Providers and user provisioning settings.

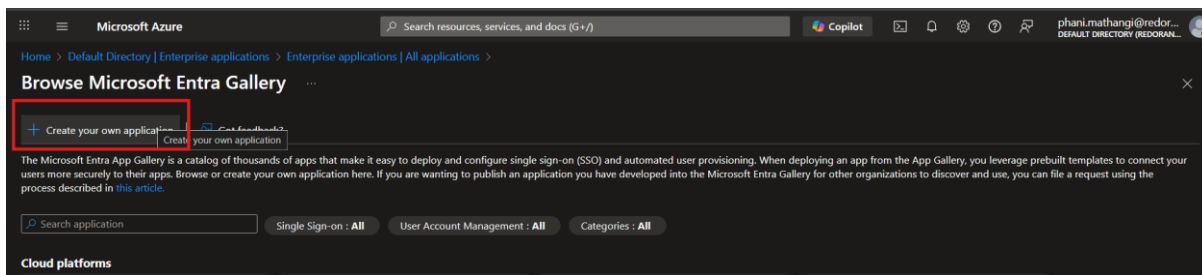## 2. Register the RedOrange Application in Microsoft Entra ID

- Sign in to the [Azure Portal](#).
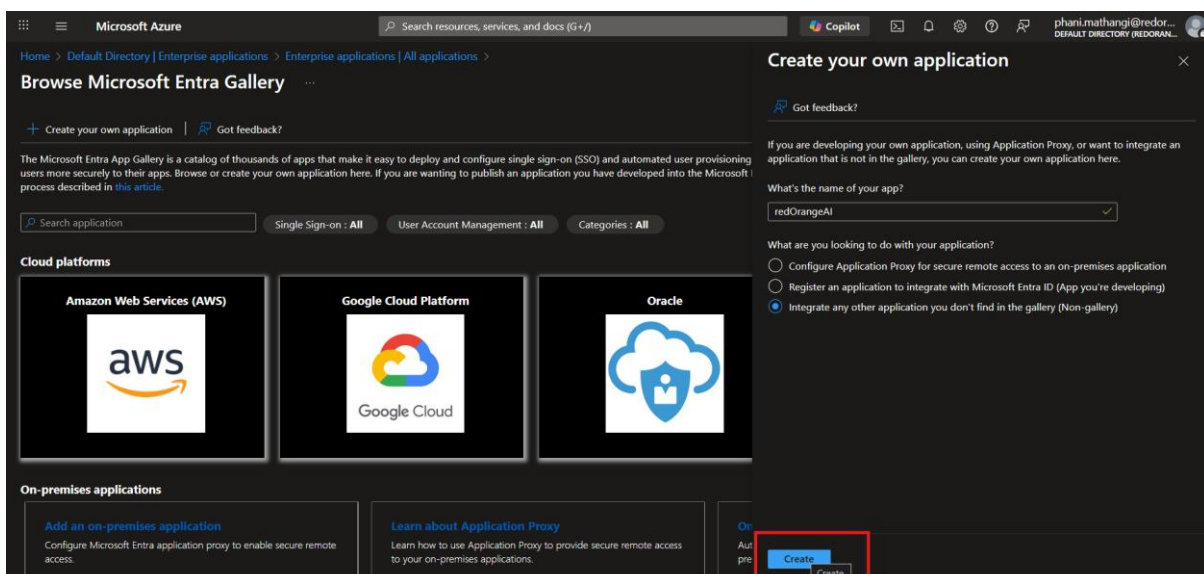- Navigate to Microsoft Entra ID > Enterprise Applications.
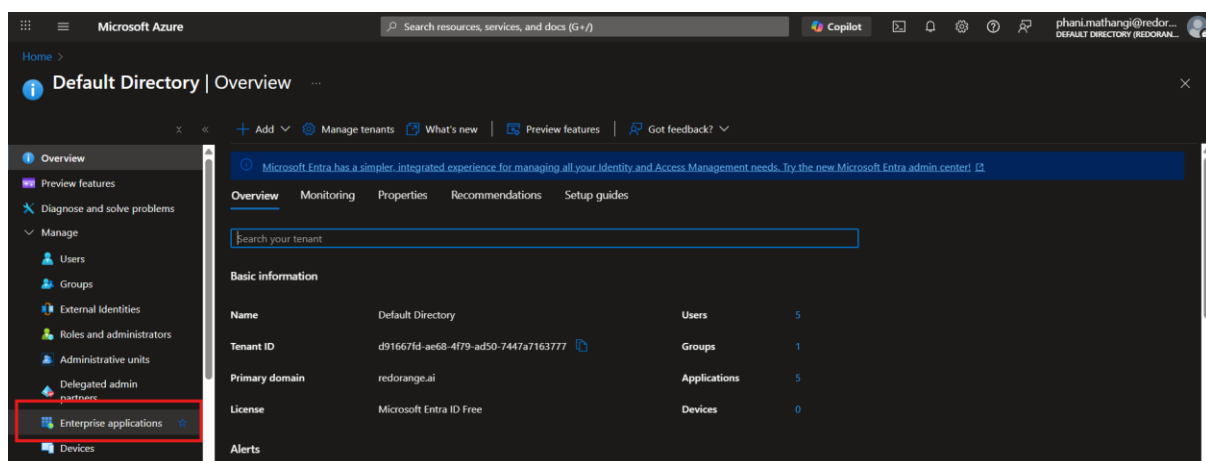
- Click + New application.
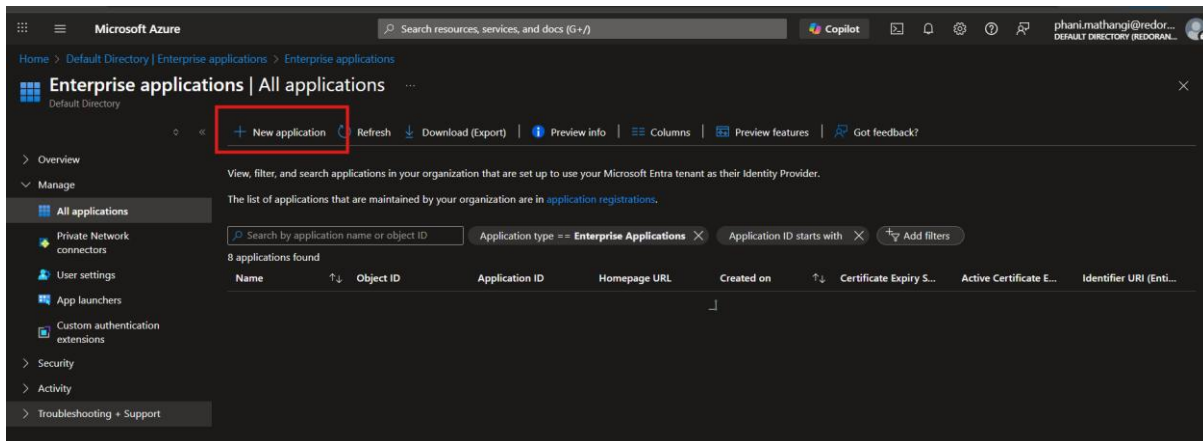
- Select Create your own application (usually at the top-right).

- Enter the name redOrangeAI (or your preferred name).

- Choose **Integrate any other application you don't find in the gallery (Non-gallery)** and click **Create**.
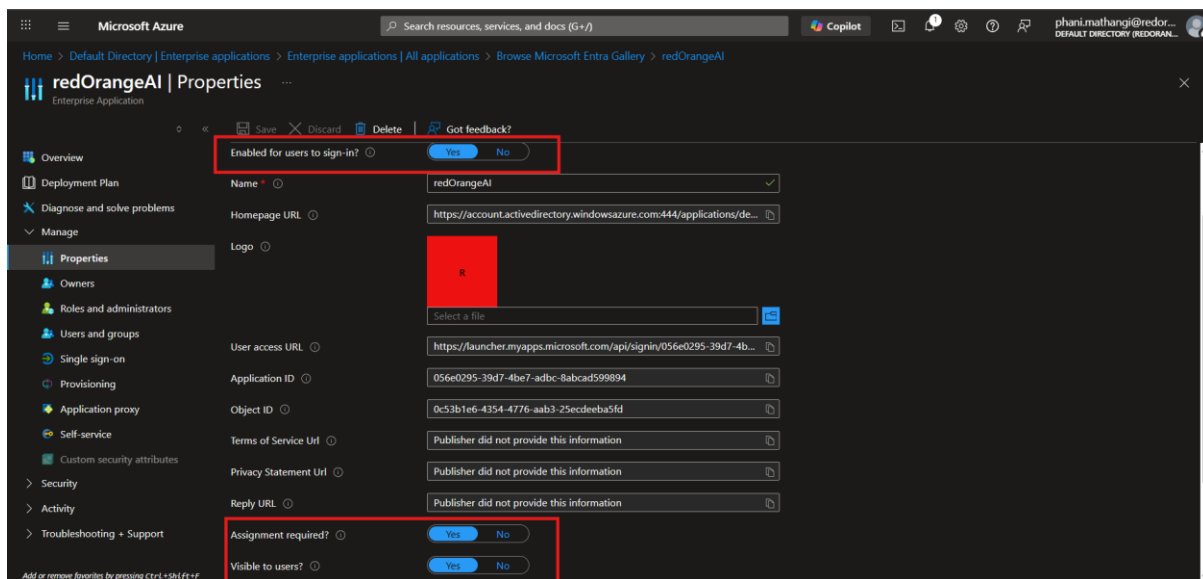
3. Configure Application Properties

- After the application is created, open it and go to **Properties**.
- Verify or set the following:

    Enabled for users to sign-in: Yes

    Assignment required: Yes (recommended for controlled access)
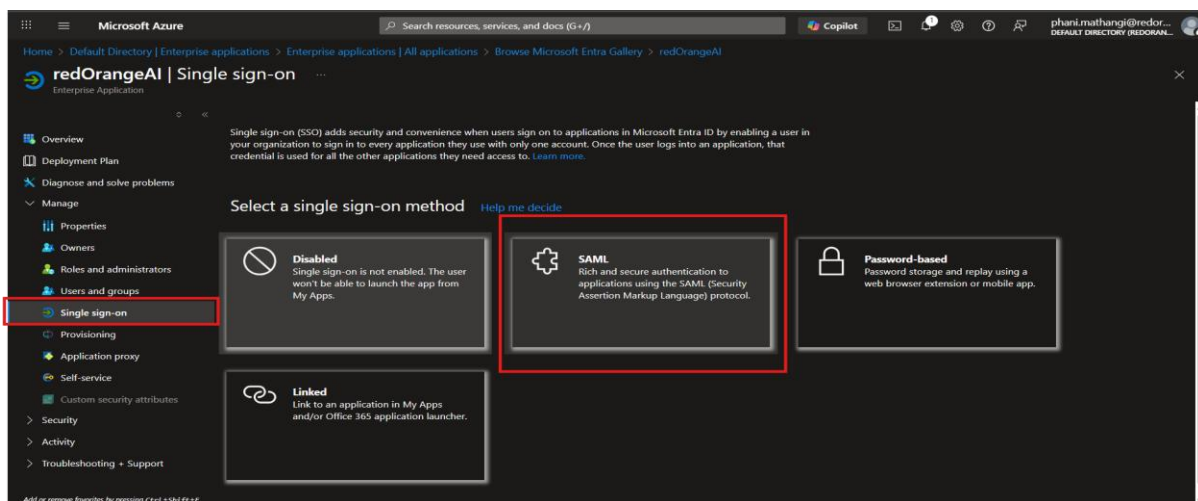
    Visible to users: Yes

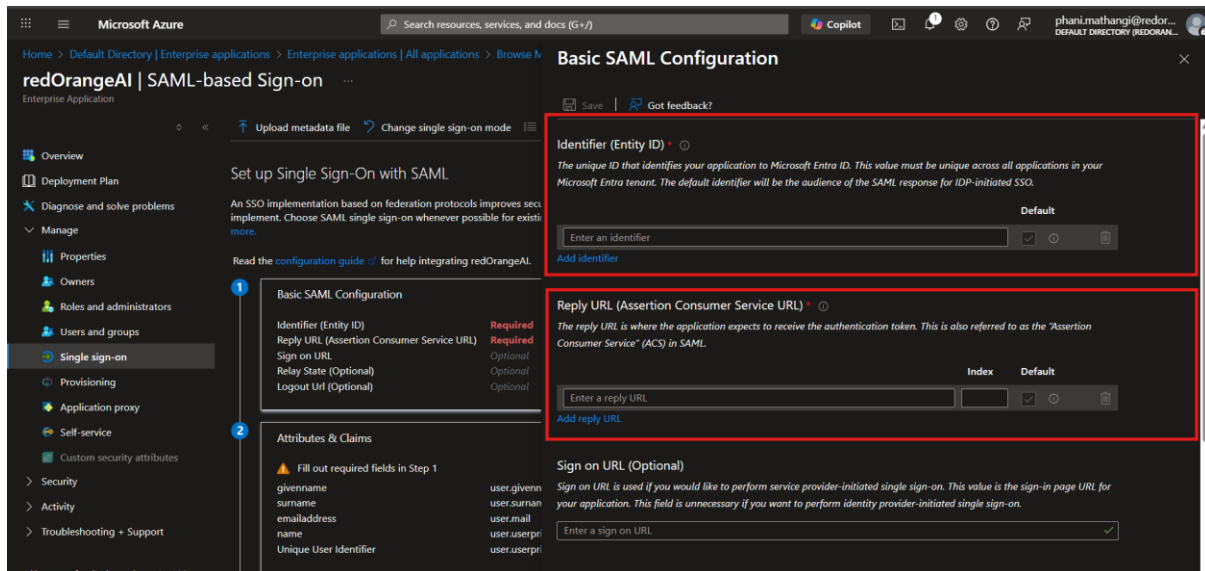- Save changes if you modify any settings.

4. Configure SAML Single Sign-On (SSO)

- In the RedOrangeAI enterprise application, select **Single sign-on** from the left menu.
- Choose **SAML** as the single sign-on method.

Once you navigate you can view **"Entity ID"** and **"Reply URL (Assertion Consumer Service URL)"**


Now, log in to your **RedOrange Application**:

- Navigate to **Settings** > **Security** > **Identity Providers**.

- Select **Azure AD** and click **Connect**.

- A popup will display the **Entity ID** and **Assertion Consumer Service (ACS) URL** for SAML authentication.

- Copy these two URLs.
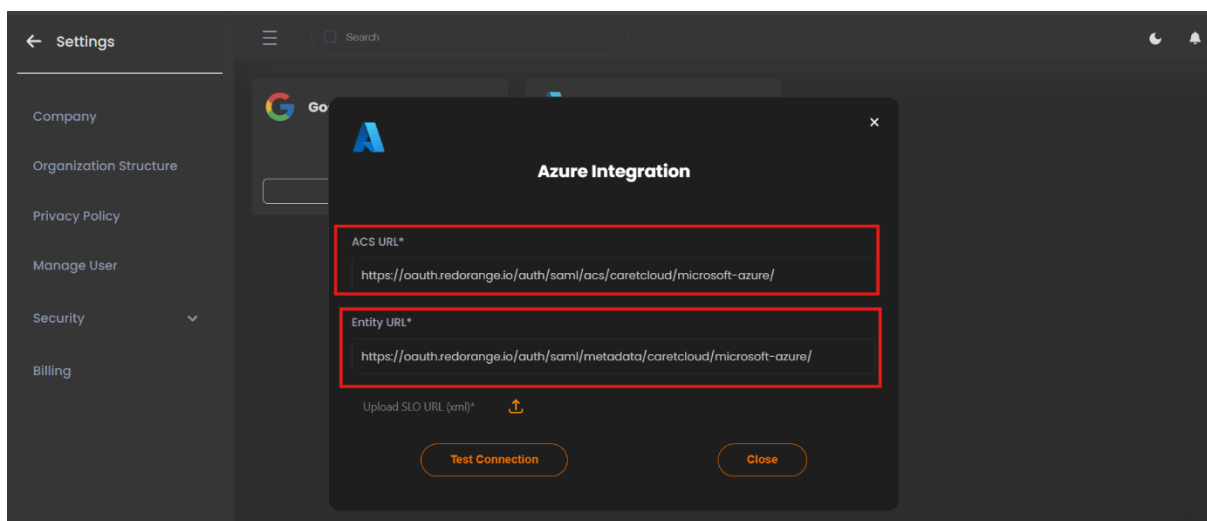
Return to the Azure Portal, in the SAML configuration section of your enterprise application:

- Paste the **Entity ID** from RedOrange into **Identifier (Entity ID)**.

- Paste the **ACS URL** from RedOrange into **Reply URL (Assertion Consumer Service URL)**.

- Save the configuration.
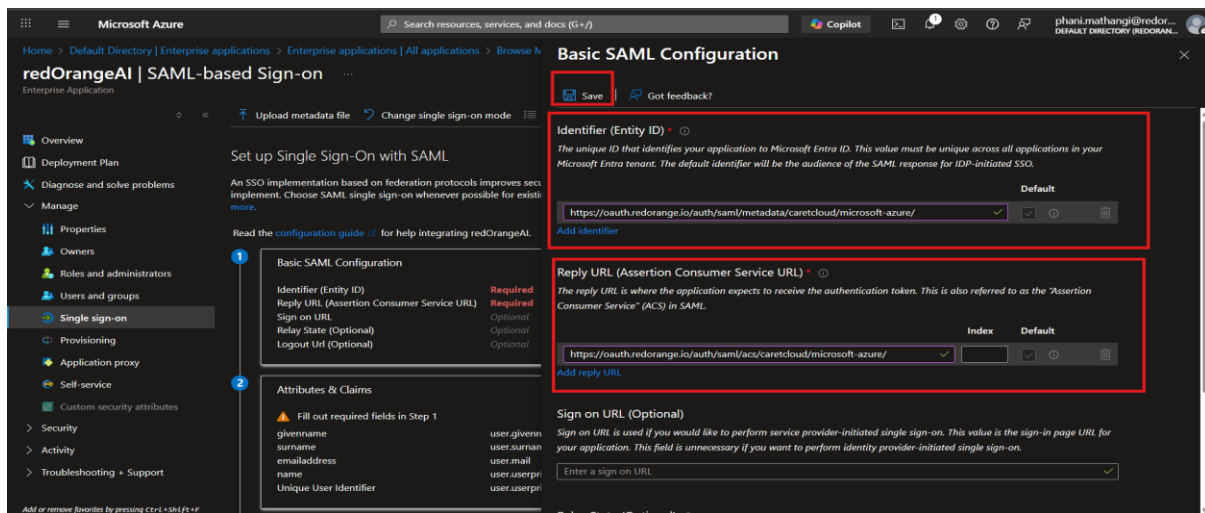
- Download the **Federation Metadata XML** from the **SAML Certificates** section in Azure.
- Upload this XML file in RedOrange under **Upload Federation Metadata XML** to complete the trust setup.
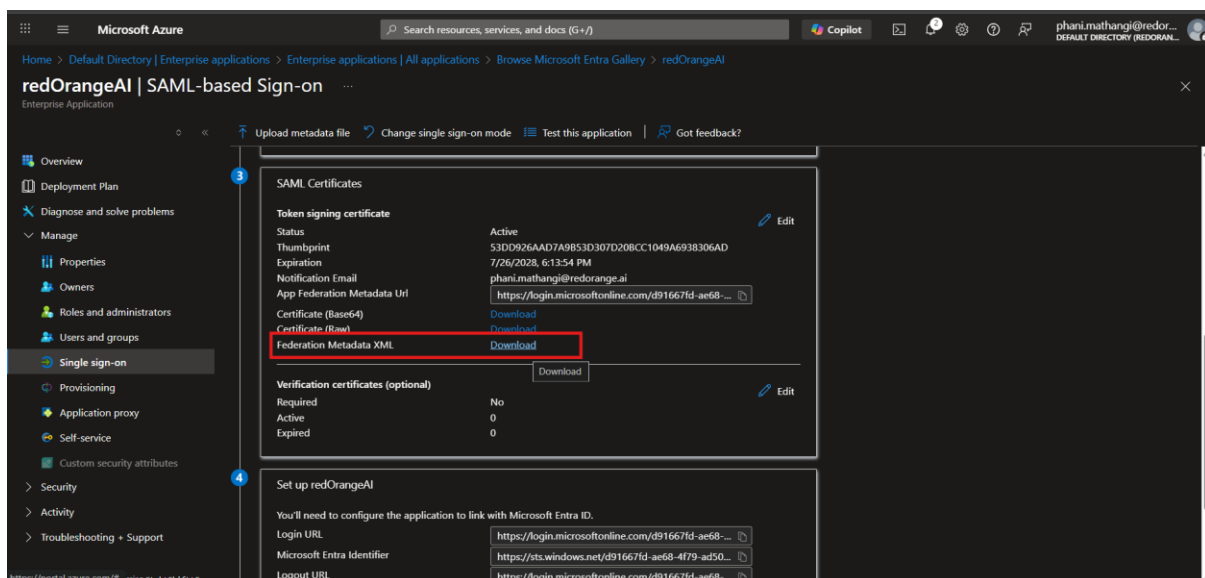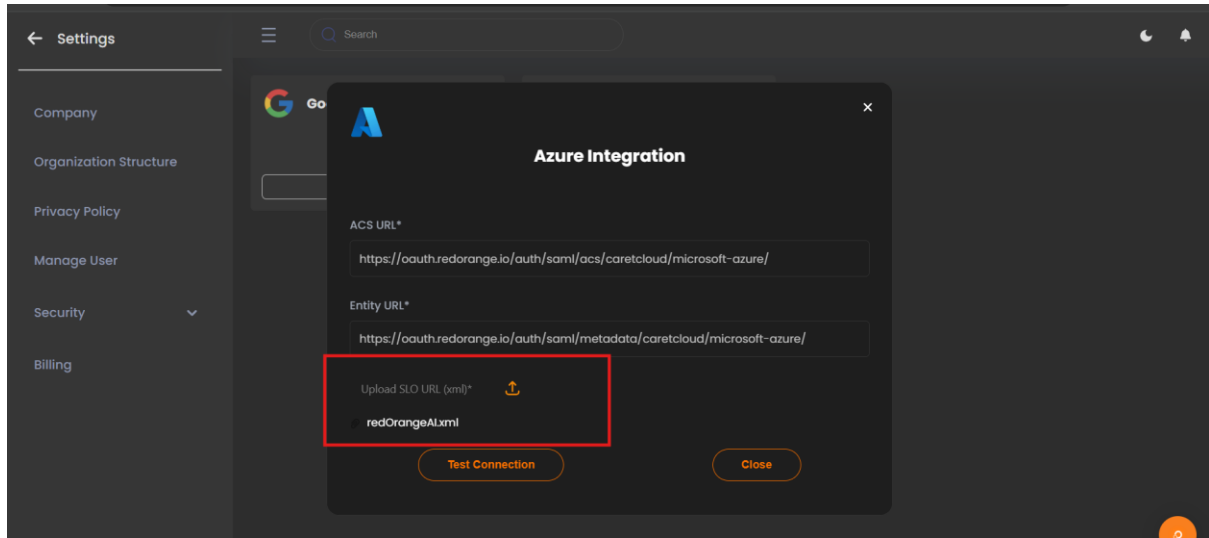
If You choose to provision the users to redOrange Application **Manually** You can proceed to click on Test Connection

Note: If you choose to proceed with **Automated User Provisioning** follow the next steps (Step -5) without clicking on test connection button
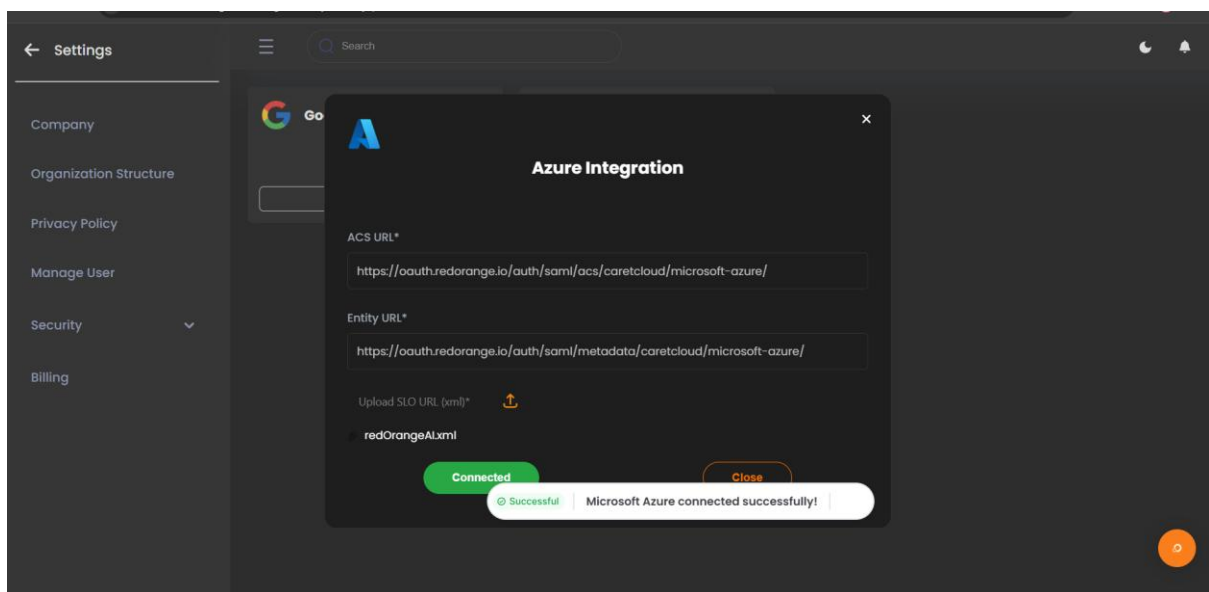

Now you can assign the user and groups to the created Enterprise Application and those users can login into redOrange Application through single sign on make sure the assigned users are manually created in redOrange Application.
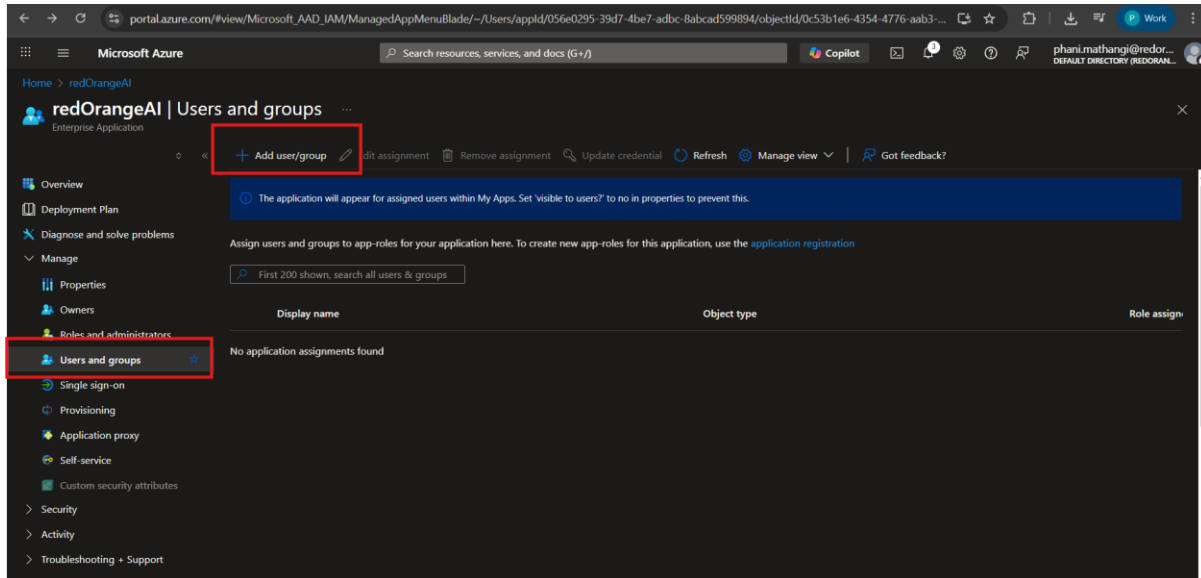
5. Configure automated user provisioning

a. Enable Provisioning in RedOrange

- In your RedOrange Application, after uploading the Federation Metadata XML, enable the **Active Directory Sync** option.

- This will provide you with:

 - **Tenant URL**

  - **Secret Token**
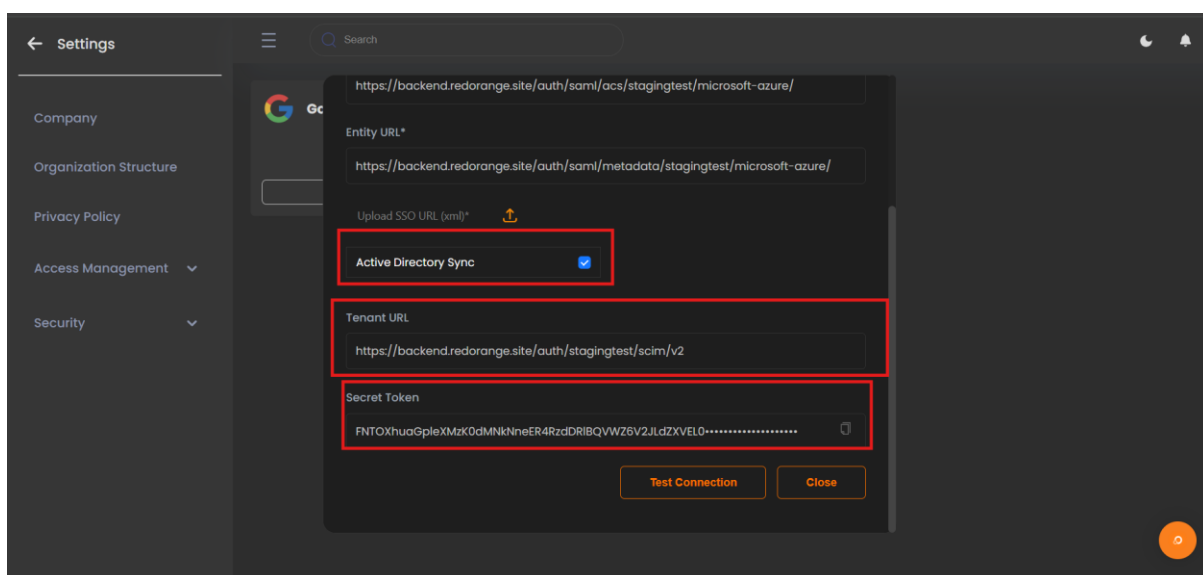
b. Configure Provisioning in Azure

1. Return to the **redOrangeAI** application in Azure Portal.

2. Select **Provisioning** from the left menu.

3. Click **Manage provisioning**.

4. Set **Provisioning Mode** to **Automatic**.
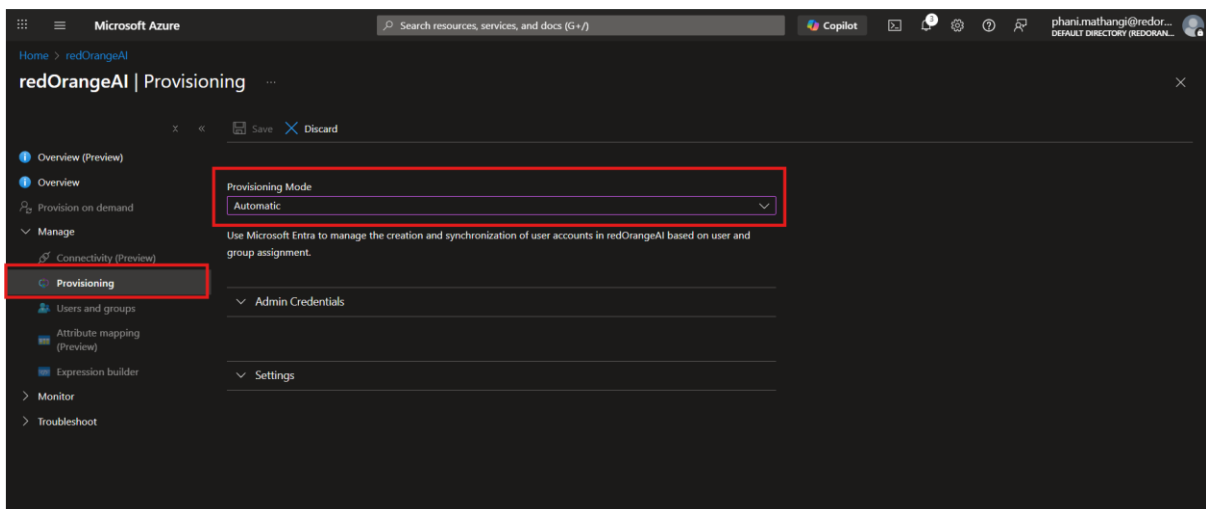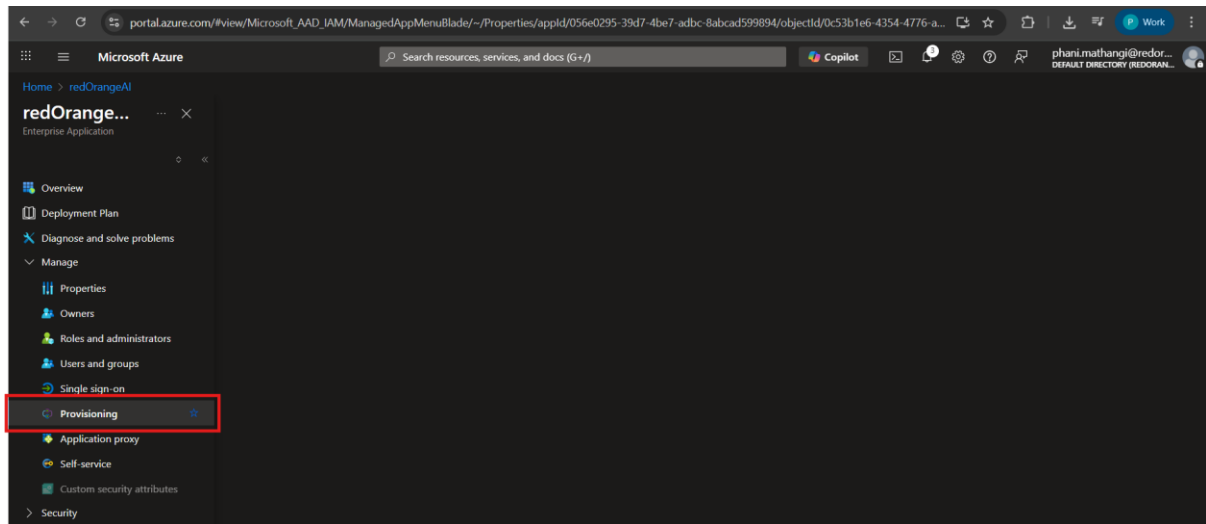
5. Under **Admin Credentials**, enter the **Tenant URL** and **Secret Token** obtained from RedOrange.
6. Click **Test Connection**. You should see **Test connection successful**.
7. Click **Save** to apply the provisioning configuration.
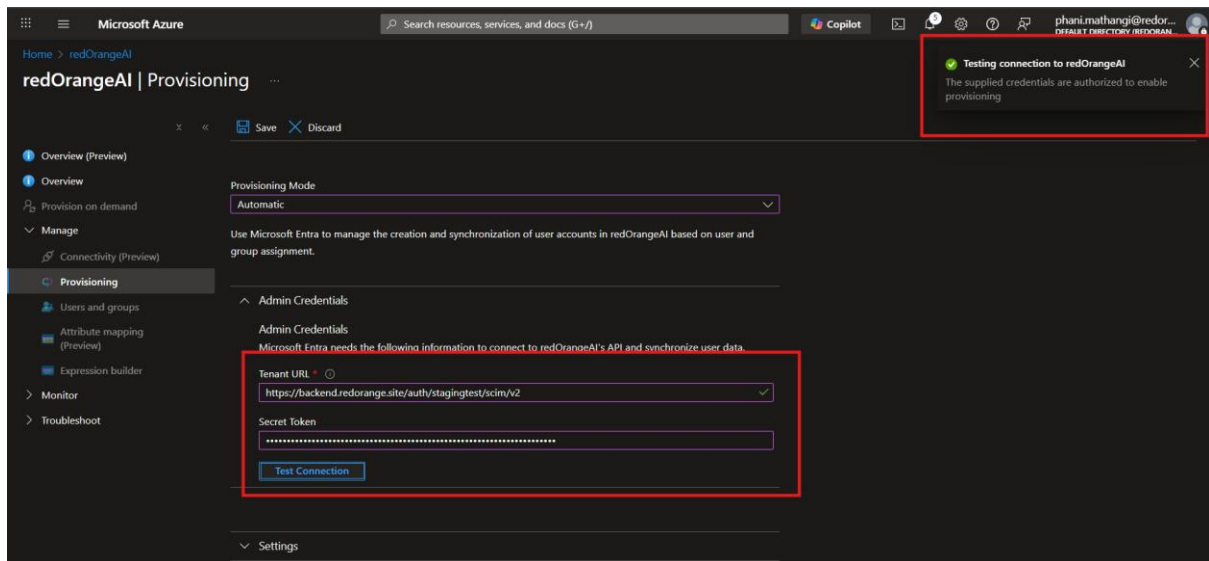
c. Define Provisioning Scope

1. In **Provisioning** settings, locate the **Scope** dropdown.

2. Select one of the following based on your access control preference:

   ○ **Sync only assigned users and groups** (Recommended):
   Only users and groups explicitly assigned to the RedOrangeAI app in Azure will be provisioned (created/updated/deactivated) in RedOrange. This option gives granular control and security.

   ○ **Sync all users and groups:**
   All users and groups in your Azure AD tenant will be provisioned to RedOrange automatically, suitable for apps requiring company-wide access.
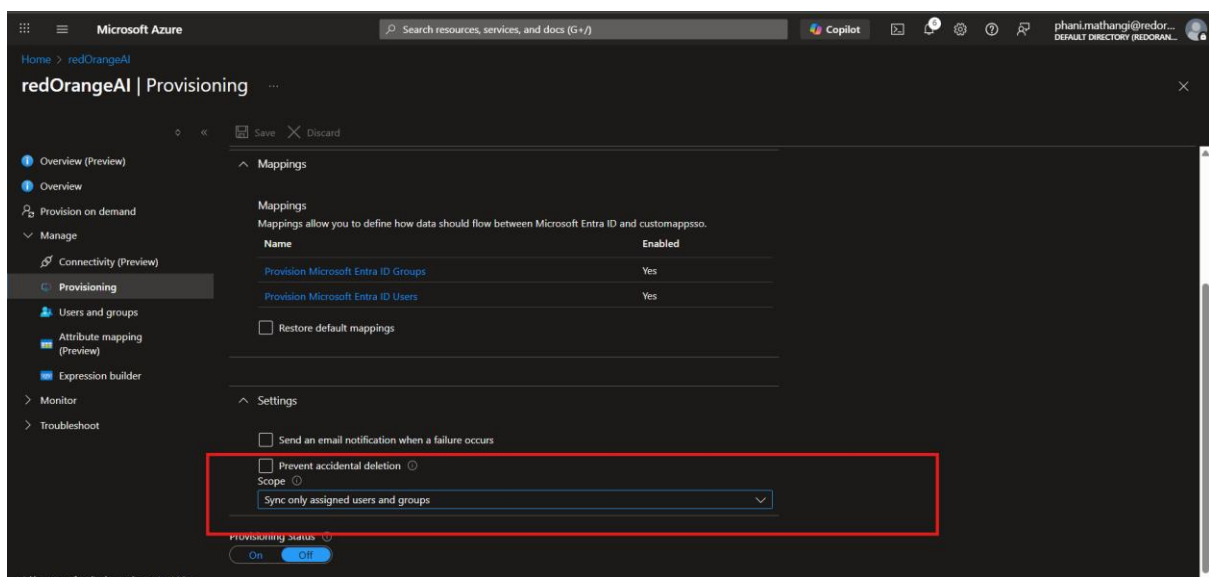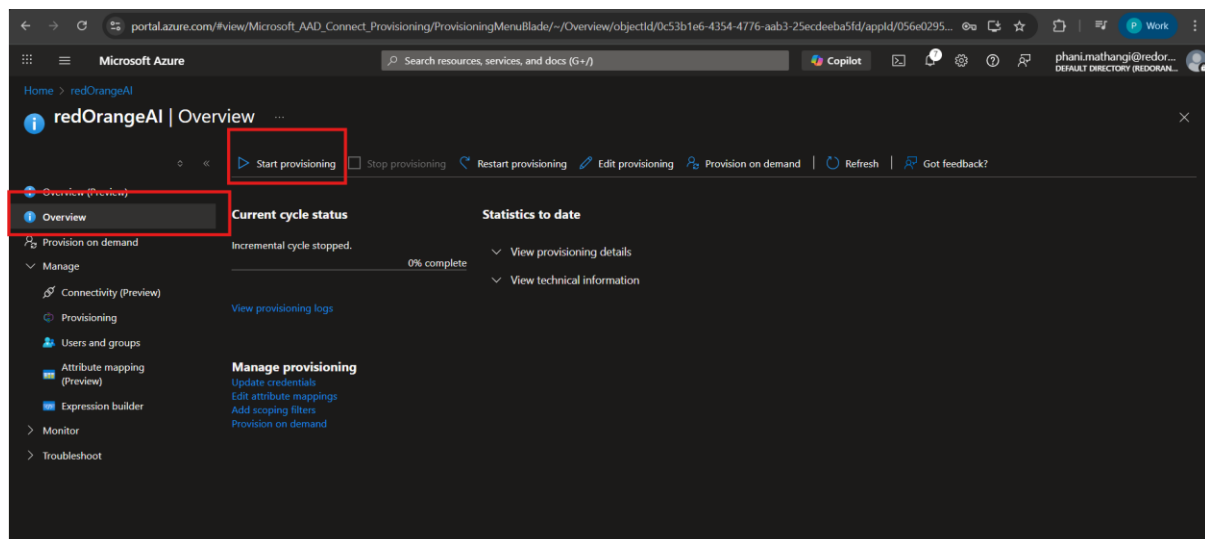
d. Assign Users and Groups in Azure

1. In the enterprise application, go to **Users and groups**.

2. Add the users and groups who should have access to RedOrange.
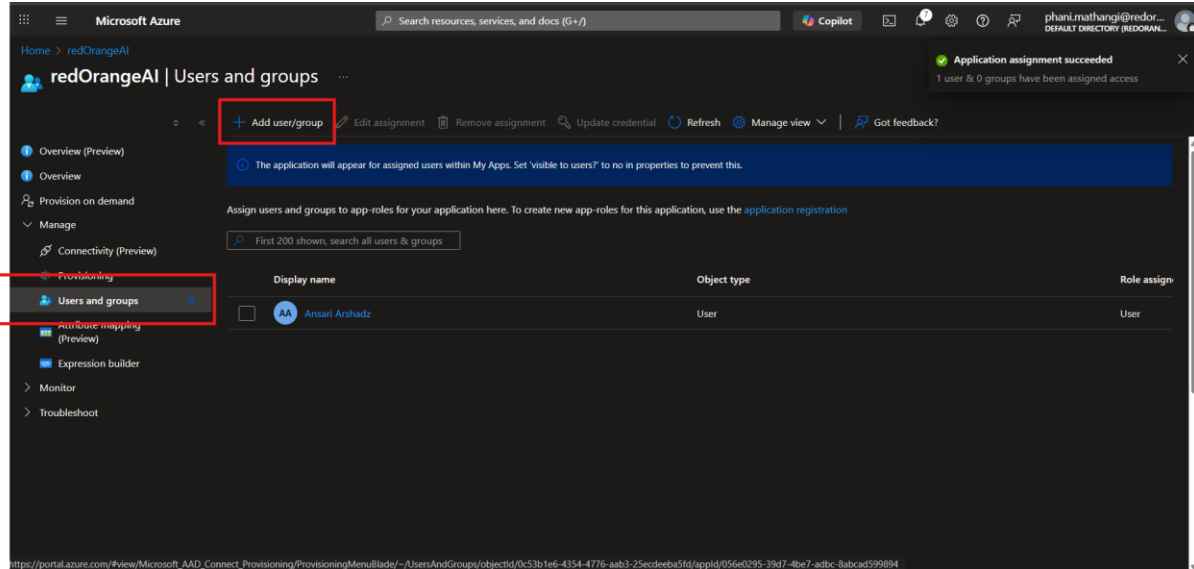
e. Start Provisioning

1. Navigate to **Overview** in the **Provisioning** section.

2. Click **Start provisioning**.

3. The provisioning service will run every 40 minutes by default, syncing user changes to RedOrange.

4. Users will be provisioned with the default role **Standard User** in RedOrange, which can be updated later inside the app.

Note: Provisioning will run automatically for every 40 mins it will check if any new users added to the created Enterprise Application or not
Users added may not be added immediately as it will check in the next cycle (after 40 mins)

If you want the users to provison on demand you can select the option provison on demand and add the users instantly
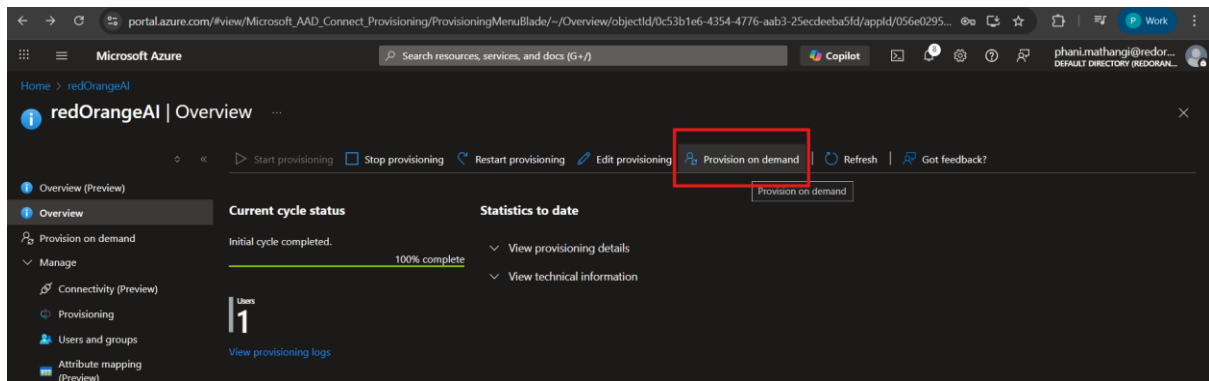
6. Additional Notes and Troubleshooting

- Ensure that **user assignments** in Azure match the users you expect to provision.

- If the test connection fails during provisioning setup, verify the **Tenant URL** and **Secret Token** values and network connectivity.

- Keep your Federation Metadata XML updated in RedOrange if you make any changes in Azure AD SAML configuration.

- For SAML issues, verify that the Entity ID and Reply URL exactly match in both Azure and RedOrange configurations.

7. Support

If you encounter any issues or need assistance, please contact:
support@redorange.ai