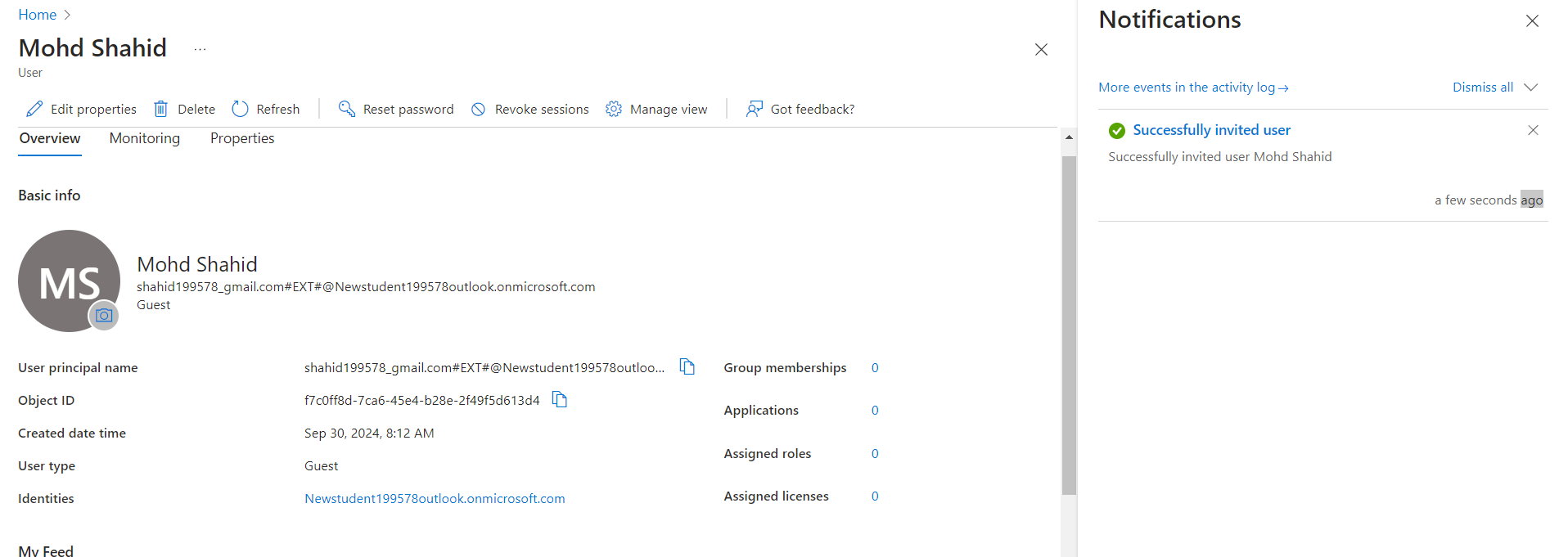
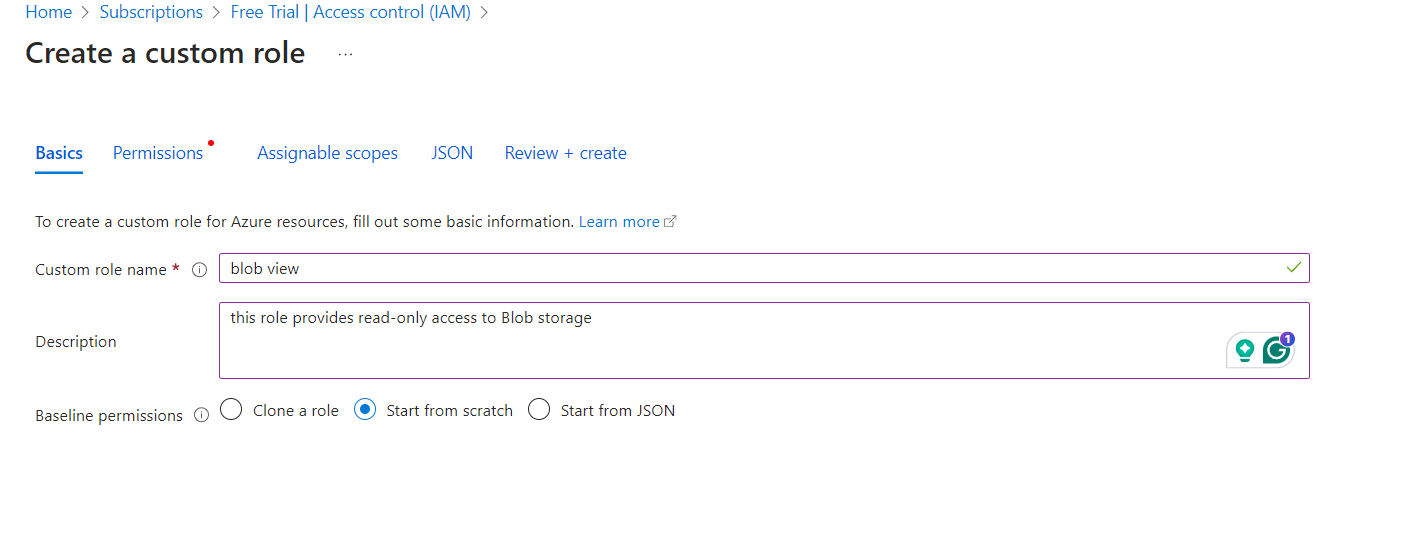
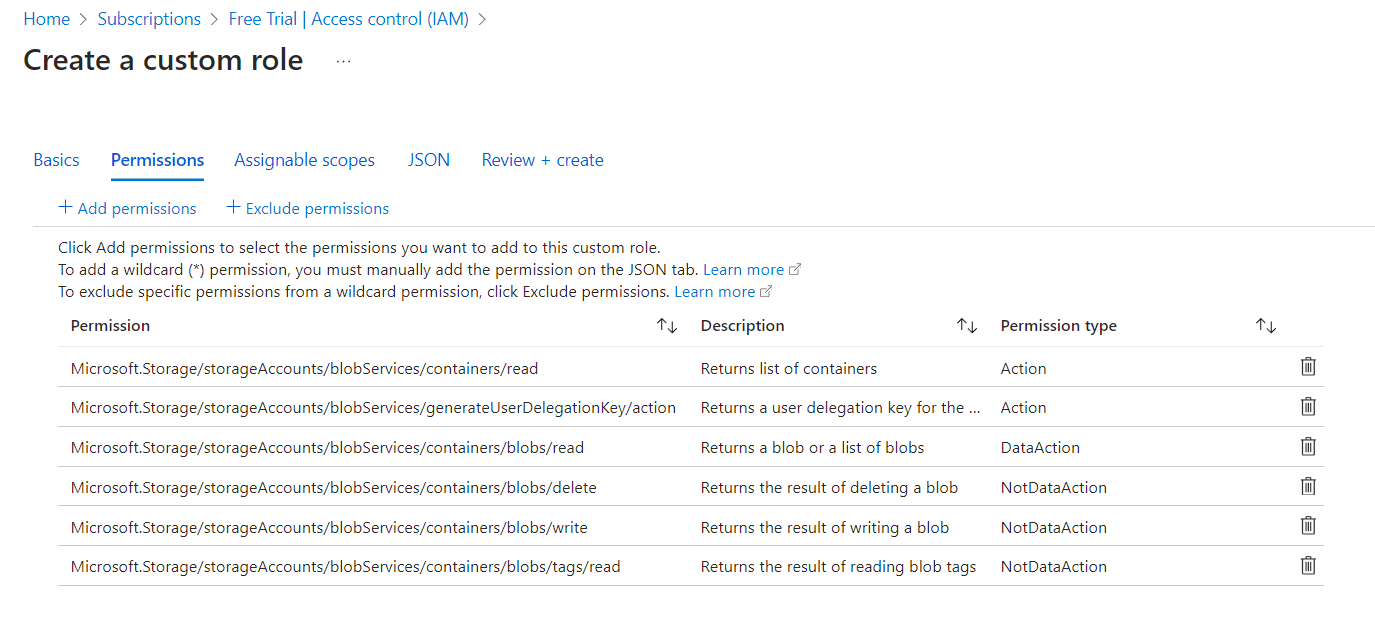
**Task 1: Add External Partners as Users in Azure Active Directory and Grant Read-Only Access to Azure Blob**

1. **Log in to the** [**Azure Portal**](https://portal.azure.com/).
2. In the left-hand menu, select **Azure Active Directory**.
3. Click on **Users** and then **+ New guest user**.
4. Enter the email address of the external partner and add a personal message if needed. Click **Invite**.

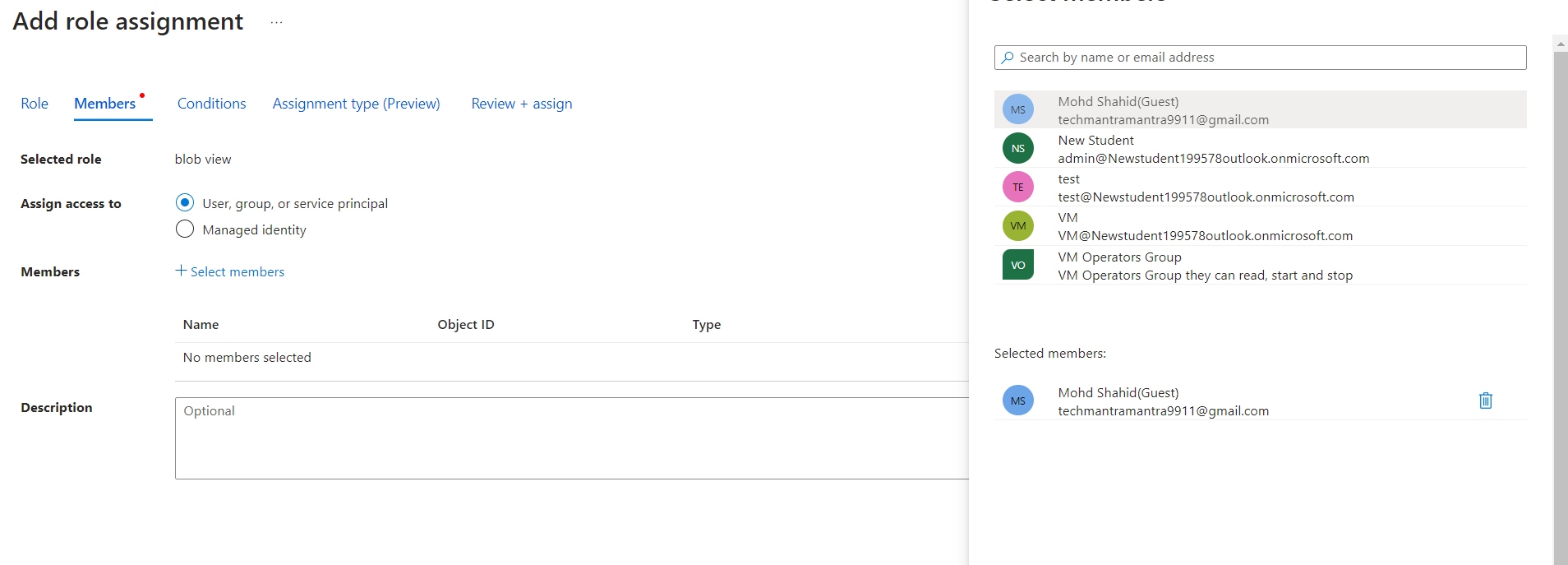


1. After the user accepts the invitation, go to the **Subscriptions** or **Resource Groups** where the Azure Blob Storage resides.
2. Click on **Access control (IAM)**.
3. Click on **+ Add**, then select **Add role assignment**.
4. In the **Role** dropdown, select **Storage Blob Data Reader** (this role provides read-only access to Blob storage).





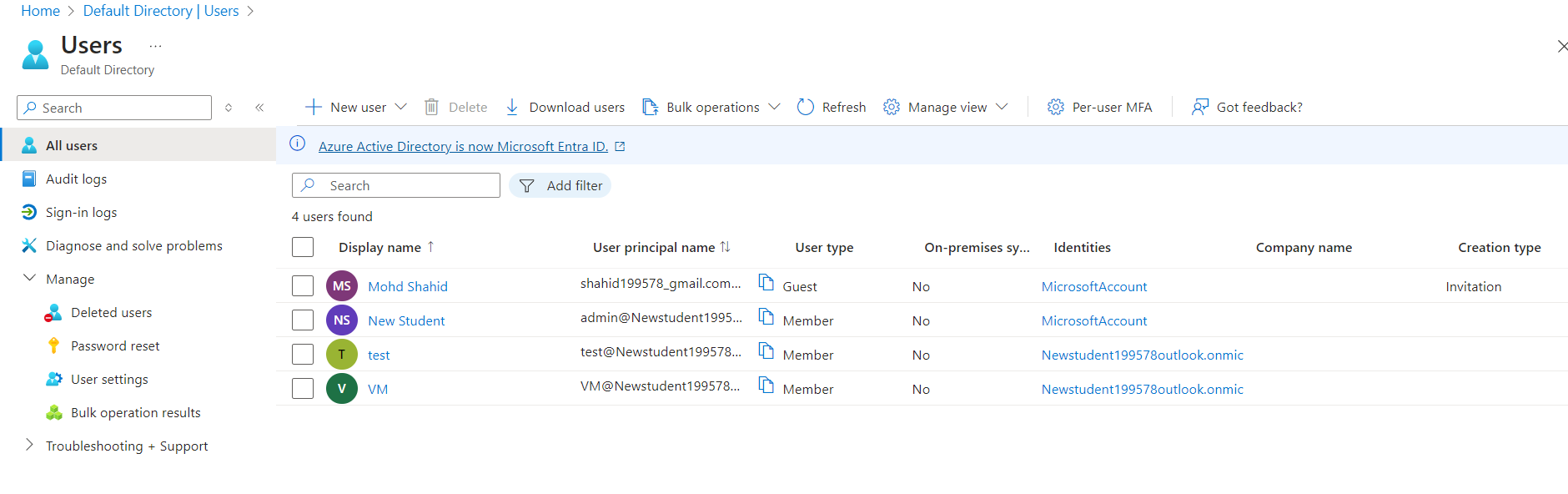
1. In the **Assign access to** dropdown, select **User, group, or service principal**.

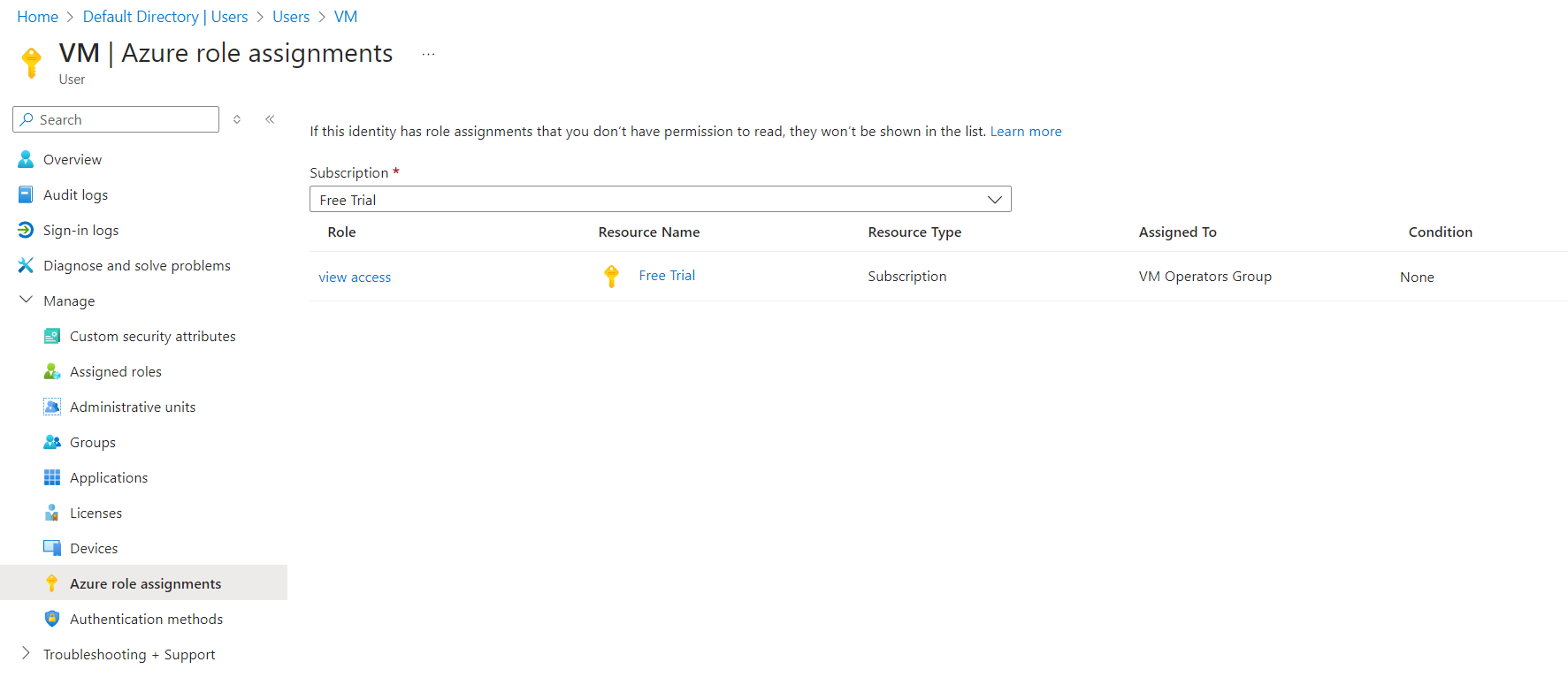


1. Search for and select the external partner's user account, then click **Save**.

**Task 2: Create Users for Internal Employees in Custom Azure Active Directory Domain**

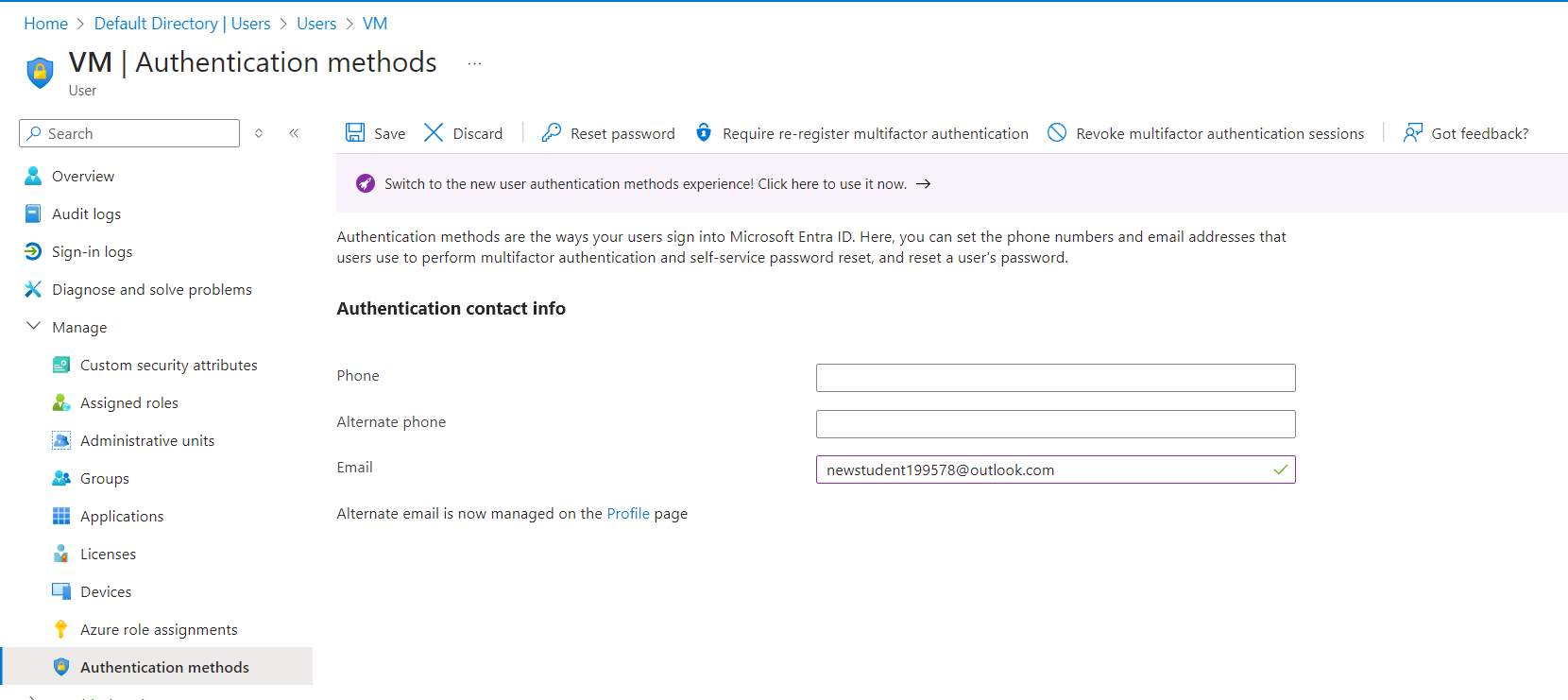
1. **Log in to the Azure Portal**.
2. Navigate to **Azure Active Directory**.
3. Click on **Users** and then **+ New user**.
4. Fill in the details for the internal employee:
   * **User name**: Choose a username in the format of your custom domain (VM).
   * **Name**: Enter the full name of the employee.
   * **Password**: Generate or set a password for the user.
5. Click **Create** to create the user.

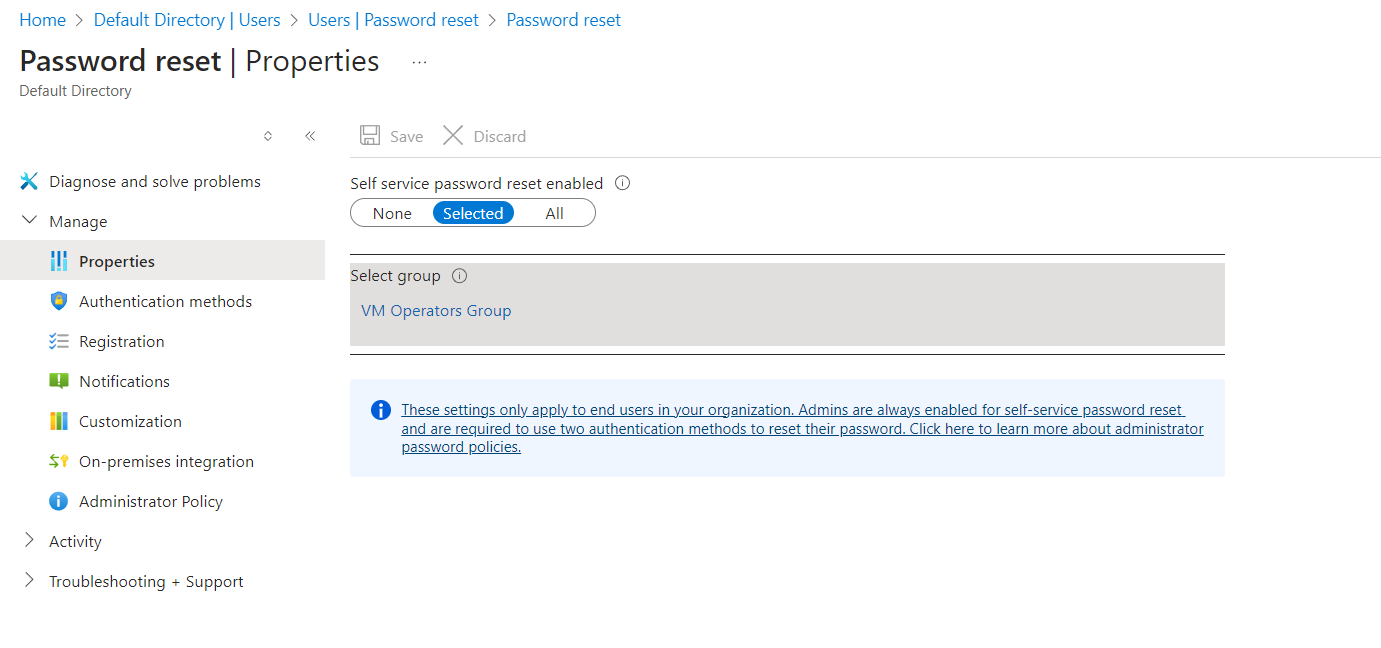


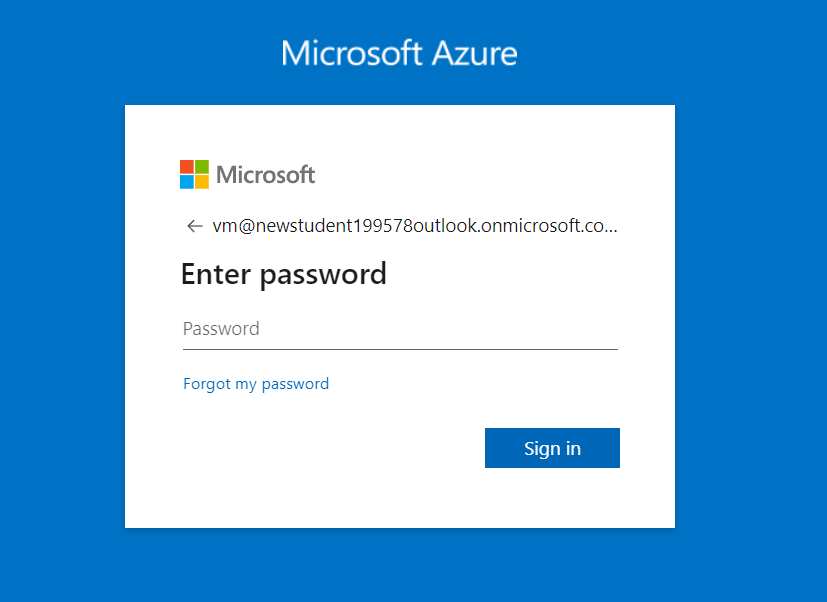


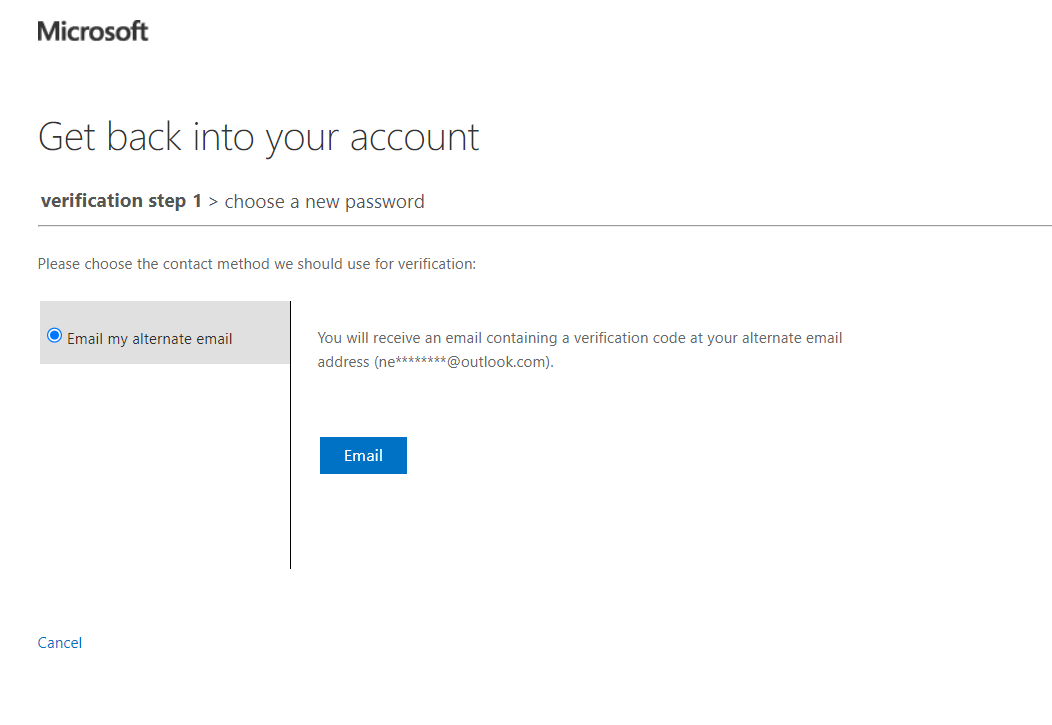
**Task 3: Set Up Password Reset for Users Without Help Desk Support**

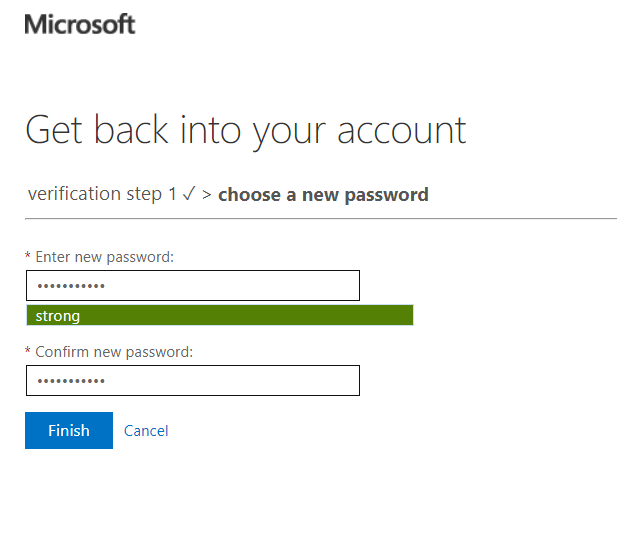
1. **Log in to the Azure Portal**.
2. Navigate to **Microsoft Entra ID**.
3. Select **Users** and then click on **User settings**.
4. Under **Password reset**, enable the option for **All users** or specific groups as required.
5. Choose the **Authentication methods** you want to allow for password resets, such as **Email** or **Mobile app verification**.
6. Set up the **Registration** for users to ensure they provide the necessary information for password resets.
7. Click **Save** to apply the settings.

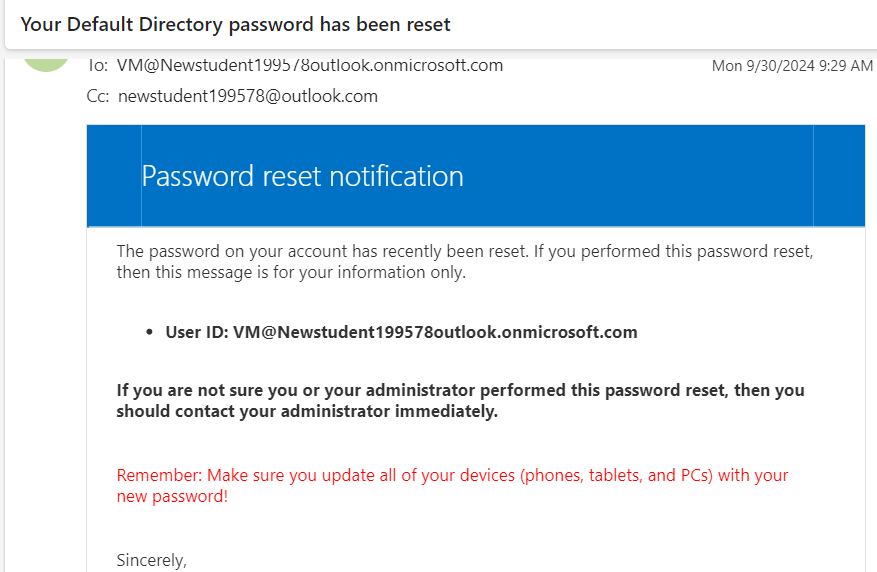












**Task 4: Set Up MFA for External Partners**

1. **Log in to the Azure Portal**.
2. Navigate to **Azure Active Directory**.
3. Click on **Users**, then select **Multi-Factor Authentication**.
4. On the MFA settings page, find the external partner’s user account.
5. Enable Multi-Factor Authentication for that user. You can set up various verification methods such as:
   * **SMS**
6. Inform the external partner to complete the MFA setup by following the instructions they receive.

