
Creating and Managing Users and Groups in Microsoft Entra ID

In this guide, we'll walk through how to create users and groups in Microsoft Entra ID (formerly Azure Active Directory), as well as manage their properties effectively.

Step 1: Access Users in Microsoft Entra ID

- Sign in to the **Azure Portal**.
- Navigate to **Microsoft Entra ID** (Azure Active Directory).
- Click on **Users** in the left-hand menu.
- Here you can see a list of all existing users in your tenant.

Step 2: Creating a New User

1. Click **+ New user** > **Create new user**.
2. Fill in the required information:
    - **User principal name (UPN):** Enter the user's sign-in name, for example, `akreddy.demouser@yourdomain.com`.
    - **Display name:** Enter a friendly name for the user, e.g., "Akreddy Demo User."
3. Choose whether to auto-generate a password or specify a password manually.
4. The account will be enabled by default upon creation.
5. Click **Create**.

Step 3: Managing User Properties

After creating the user, you can further configure their details by selecting the user from the list and updating the following sections:

- **Profile:**
    - First name, last name.
    - User type: Select **Member** for internal users or **Guest** for external users (e.g., users with personal emails like Gmail or corporate emails from other organizations).
- **Job Info:**
    - Job title, department, company name, employee ID, employee type — typically used in Outlook and other Microsoft services.
- **Contact Info:**
    - Phone number, email, address.
- **Parental Controls:**
    - Set age group and consent details for minors.
- **Settings:**
    - **Usage location:** Important for licensing and multi-factor authentication policies.
- **Group Memberships:**
    - Add the user to one or more groups for easier access management.
- **Roles:**
    - Assign Azure AD roles by clicking **Add role assignment** and selecting the appropriate roles for the user.

Step 4: Assigning Roles to Users

- Go to the user's **Assigned roles** tab.
- Click **Add assignment**, then choose from roles like **Global Administrator**, **User Administrator**, or **Security Reader**.
- Assign the appropriate role and save.

Step 5: Managing Group Memberships

- Within a user's profile, go to **Groups** > **Add memberships**.
- Select the groups to which the user should belong, e.g., "Finance Group."
- Click **Select** to add the user to those groups.

Step 6: Creating and Managing Groups

1. Navigate to **Groups** in Microsoft Entra ID.
2. Click **+ New group**.
3. Choose the **Group type**:
    - **Security group:** Used for access control and permissions.
    - **Microsoft 365 group:** Used for collaboration, email, and shared resources.
4. Enter the **Group name** and optionally a **Description**.
5. Set **Membership type**:
    - **Assigned:** Manually add members.
    - **Dynamic User/Device:** Members are added based on rules or attributes.

6. Assign **Owners** who can manage the group membership.
7. Add members to the group (e.g., the newly created user).
8. Click **Create** to finalize.

Step 7: Additional User Management Features

- **Applications:** Assign enterprise applications and configure single sign-on (SSO) for the user.
- **Licenses:** Assign Microsoft 365 or other product licenses directly to the user.
- **Devices:** Review devices enrolled or registered by the user.
- **Azure Role Assignments:** View or assign roles related to Azure subscriptions or resources.

Summary

- Creating users and groups in Microsoft Entra ID allows streamlined identity and access management.
- Users can be internal members or guests with external identities.
- Groups help organize users for easier permission management.
- Assigning roles and licenses to users ensures they have appropriate access to resources.
- Regularly review user and group properties to keep your directory secure and organized.
