Microsoft Entra ID User and Group Management Lab

Duration: 30 minutes
Difficulty: Beginner
Prerequisites: Azure subscription with Global Administrator or User Administrator role

Lab Overview

In this lab, you'll learn to create and manage users and groups in Microsoft Entra ID (formerly Azure Active Directory), assign roles, and configure basic security settings.

Part 1: Access Microsoft Entra ID (5 minutes)

Step 1: Sign in to Azure Portal

1. Navigate to https://portal.azure.com
2. Sign in with your Azure credentials
3. In the search bar at the top, type **"Microsoft Entra ID"**
4. Click on **Microsoft Entra ID** from the results

Step 2: Explore the Overview

- Take a moment to review the dashboard
- Note your tenant name and domain (e.g., yourcompany.onmicrosoft.com)
- Observe the overview statistics (users, groups, applications)

Part 2: Create Individual Users (8 minutes)

Step 3: Create Your First User

1. In the left navigation pane, click **Users**
2. Click **+ New user** at the top
3. Select **Create new user**
4. Fill in the following details:
    - **User principal name:** john.doe (domain will auto-populate)
    - **Display name:** John Doe
    - **Password:** Check "Auto-generate password"
    - Copy the password shown (you'll need this later)
    - Check **Show password** to view it
5. Under **Settings:**
    - **Usage location:** Select your country

6. Click **Review + create**
7. Click **Create**

Step 4: Create Additional Users

Repeat Step 3 to create two more users:

User 2:

- Username: jane.smith
- Display name: Jane Smith
- Save the auto-generated password

User 3:

- Username: bob.johnson
- Display name: Bob Johnson
- Save the auto-generated password

Step 5: View User Properties

1. Click on **John Doe** from the users list
2. Explore the different sections:
    - Profile information
    - Assigned roles
    - Groups
    - Licenses

Part 3: Create and Configure Groups (10 minutes)

Step 6: Create a Security Group

1. Go back to **Microsoft Entra ID** home
2. Click **Groups** in the left navigation
3. Click **+ New group**
4. Configure the group:
    - **Group type:** Security
    - **Group name:** IT Department
    - **Group description:** Members of the IT Department
    - **Membership type:** Assigned
5. Click **No members selected** under Members

6. Search and select **John Doe** and **Jane Smith**
7. Click **Select**
8. Click **Create**

Step 7: Create a Microsoft 365 Group

1. Click **+ New group** again
2. Configure the group:
    - **Group type:** Microsoft 365
    - **Group name:** Marketing Team
    - **Group description:** Marketing department collaboration group
    - **Membership type:** Assigned
3. Add **Bob Johnson** as a member
4. Click **Create**

Step 8: Add Owners to Groups

1. Click on the **IT Department** group
2. Click **Owners** in the left menu
3. Click **+ Add owners**
4. Select **John Doe**
5. Click **Select**

Part 4: Assign Roles and Permissions (5 minutes)

Step 9: Assign Administrative Role

1. Go back to **Users**
2. Click on **John Doe**
3. Click **Assigned roles** in the left menu
4. Click **+ Add assignments**
5. Search for **User Administrator**
6. Select it and click **Add**
7. Verify the role appears in the list

Step 10: Verify Group Membership

1. Go to **Groups**
2. Click on **IT Department**

3. Click **Members** to verify John and Jane are listed
4. Note the total member count

Part 5: Test and Validate (2 minutes)

Step 11: Test User Sign-in

1. Open a new **private/incognito browser window**
2. Go to https://portal.azure.com
3. Sign in as **john.doe@yourdomain.onmicrosoft.com**
4. Use the password you saved earlier
5. You'll be prompted to change the password
6. Set a new password and complete sign-in
7. Verify you can see the Azure portal

Step 12: Verify User Access

- As John Doe, try to navigate to Microsoft Entra ID
- Due to the User Administrator role, John should be able to view and manage users
- Try viewing the user list to confirm

Part 6: Cleanup and Review (Optional)

Step 13: Review What You Created

Go to Microsoft Entra ID and verify:

- **3 users created:** John Doe, Jane Smith, Bob Johnson
- **2 groups created:** IT Department, Marketing Team
- **1 role assigned:** User Administrator to John Doe

Cleanup Instructions (Optional)

If this is a test environment, you can clean up resources:

1. **Delete Users:**
    - Go to Users > Select each user > Delete
2. **Delete Groups:**
    - Go to Groups > Select each group > Delete
3. **Remove Role Assignments:**
    - Not necessary if users are deleted, but can be done via Users > [User] > Assigned