
🧪 Microsoft Entra ID – Demo

🎯 Goal of Demo

By the end of this demo, you will:

- Create a user and a group in Microsoft Entra ID
- Assign RBAC roles to that group
- Enforce MFA using Conditional Access
- Validate access controls

🧵 Scenario (AZ-104 style)

> You are an Azure Administrator. Your company hires a team of developers who need Contributor access to a specific Resource Group. To secure their access, you must enforce MFA.

🛠️ Step-by-Step Demo

🔹 Step 1: Create a User in Microsoft Entra ID

📍 **Portal:**

1. Go to https://entra.microsoft.com
2. Navigate to **Users** → **+ New user**

3. Fill in:
    - **Username**: dev1@yourdomain.onmicrosoft.com
    - **Name**: Dev User 1
    - **Password**: Auto-generated or custom
4. Click **Create**

📍 **CLI:**

```
az ad user create \
  --display-name "Dev User 1" \
  --user-principal-name "dev1@yourdomain.onmicrosoft.com" \
  --password "StrongP@ssword123" \
  --force-change-password-next-login true
```

🔹 Step 2: Create a Security Group

📍 **Portal:**

1. Go to **Groups** → **+ New group**
2. **Group type**: Security
3. **Group name**: DevTeam
4. Add **Dev User 1** as a member
5. Click **Create**

📍 **CLI:**

```
az ad group create \
  --display-name "DevTeam" \
  --mail-nickname "devteam"
```

To add the user:

```
az ad group member add \
  --group "DevTeam" \
```

```
--member-id "<user-object-id>"
```

🔹 Step 3: Assign RBAC Role to Group on a Resource Group

Let's say the Resource Group is named `Dev-Resources`.

📍 **Portal:**

1. Go to **Resource groups** → **Dev-Resources**
2. Click **Access control (IAM)** → **+ Add role assignment**
3. Role: **Contributor**
4. Assign access to: **User, group, or service principal**
5. Select: **DevTeam**
6. Click **Save**

📍 **CLI:**

```
az role assignment create \
  --assignee "<group-object-id>" \
  --role "Contributor" \
  --scope "/subscriptions/<sub-id>/resourceGroups/Dev-Resources"
```

🔹 Step 4: Create a Conditional Access Policy to Require MFA

📍 **Portal:**

1. Go to **Microsoft Entra Admin Center**
2. Navigate to **Protection** → **Conditional Access**
3. Click **+ New policy**
4. **Name**: "MFA for DevTeam"
5. **Assignments**:

- **Users**: Select the **DevTeam** group
- **Cloud apps**: All cloud apps

6. **Conditions**: (optional) — leave default or customize (e.g., exclude trusted locations)
7. **Grant**:
   - Select **Require multi-factor authentication**
8. Click **On** → **Create**

✅ Now, any user in the DevTeam group must complete MFA when accessing Azure resources.

🔹 Step 5: Test the Setup (Optional in Lab)

1. Log in as **dev1@yourdomain.onmicrosoft.com**
2. Try accessing Azure Portal
3. You'll be prompted to **set up MFA**
4. Try accessing **Dev-Resources** → Should have **Contributor** access

---

🎓 Exam Relevance

Task	AZ-104 Skill
Create Users & Groups	✅ Manage Entra ID identities
Assign RBAC roles	✅ Control access using RBAC
Enforce MFA	✅ Configure Conditional Access
Hybrid Identity (if needed)	🔄 Covered separately

📝 Bonus Tips for Demos

- Use **Azure Cloud Shell** (Bash or PowerShell) for CLI commands
- Show users the **“My Sign-ins”** page for reviewing login attempts: https://mysignins.microsoft.com
- Always demo **RBAC using groups** to show real-world, scalable IAM practice
- Enable **Azure AD Premium P1** in a test tenant if you want full Conditional Access features

---