**Lab 01 - Manage Microsoft Entra ID Identities**

**Lab introduction**

This is the first in a series of labs for Azure Administrators. In this lab, you learn about users and groups. Users and groups are the basic building blocks for an identity solution.

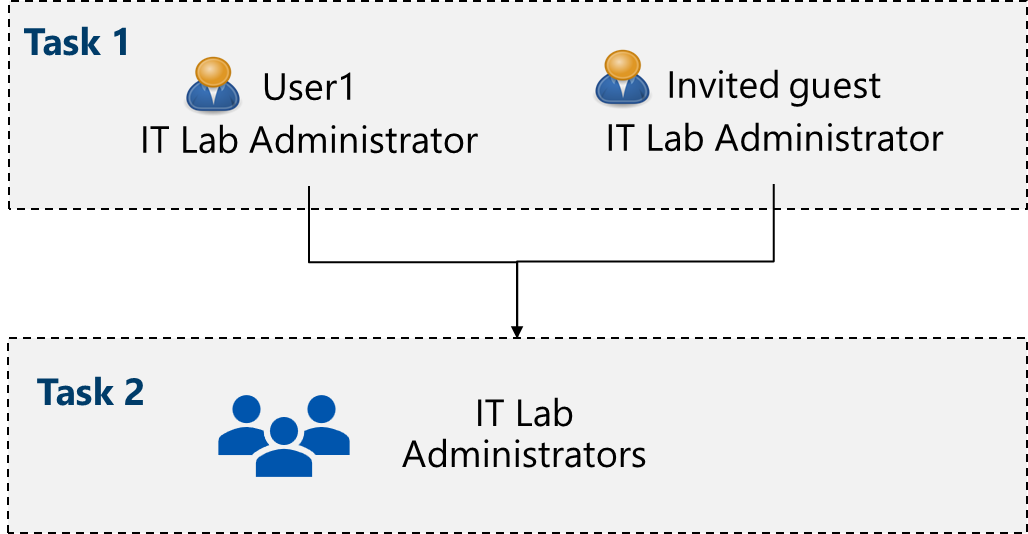
This lab requires an Azure subscription. Your subscription type may affect the availability of features in this lab. You may change the region, but the steps are written using **East US**.

**Estimated timing: 30 minutes**

**Lab scenario**

Your organization is building a new lab environment for pre-production testing of apps and services. A few engineers are being hired to manage the lab environment, including the virtual machines. To allow the engineers to authenticate by using Microsoft Entra ID, you have been tasked with provisioning users and groups. To minimize administrative overhead, membership of the groups should be updated automatically based on job titles.

**Architecture diagram**

[](https://github.com/MicrosoftLearning/AZ-104-MicrosoftAzureAdministrator/blob/master/Instructions/media/az104-lab01-architecture.png)

**Job skills**

* Task 1: Create and configure user accounts.
* Task 2: Create groups and add members.

**Task 1: Create and configure user accounts**

In this task, you will create and configure user accounts. User accounts will store user data such as name, department, location, and contact information.

1. Sign in to the **Azure portal** - https://portal.azure.com.
2. To proceed to the portal, select **Cancel** on the **Welcome to Azure** splash screen.

**Note:** The Azure portal is used in all the labs. If you are new to the Azure, search for and select Quickstart Center. Take a few minutes to watch the **Getting started in the Azure portal** video. Even if you have used the portal before, you will find a few tips and tricks on navigating and customizing the interface.

1. Search for and select Microsoft Entra ID. Microsoft Entra ID is Azure's cloud-based identity and access management solution. Take a few minutes to familiarize yourself with some of the features listed in the left pane.
2. Select the **Overview** blade and then the **Manage tenants** tab.

**Did you know?** A tenant is a specific instance of Microsoft Entra ID containing accounts and groups. Depending on your situation, you can create more tenants and **Switch** between them.

1. Return to the **Entra ID** page by pressing back in the browser or selecting the option in the breadcrumb menu.
2. Select **Licenses**. From here you can purchase a license, manage the licenses you have, and assign licenses to users and groups. Select **Licensed features** to see what is available.

**Create a new user**

1. Select **Users**, then in the **New user** drop-down select **Create new user**.
2. Create a new user with the following settings (leave others with their defaults). On the **Properties** tab notice all the different types of information that can be included in the user account.

| **Setting** | **Value** |
| --- | --- |
| User principal name | az104-user1 |
| Display name | az104-user1 |
| Auto-generate password | **checked** |
| Account enabled | **checked** |
| Job title (Properties tab) | IT Lab Administrator |
| Department (Properties tab) | IT |
| Usage location (Properties tab) | **United States** |

1. Once you have finished reviewing, select **Review + create** and then **Create**.
2. Refresh the page and confirm your new user was created.

**Invite an external user**

1. In the **New user** drop-down select **Invite an external user**.

| **Setting** | **Value** |
| --- | --- |
| Email | your email address |
| Display name | your name |
| Send invite message | **check the box** |
| Message | Welcome to Azure and our group project |

1. Move to the **Properties** tab. Complete the basic information, including these fields.

| **Setting** | **Value** |
| --- | --- |
| Job title | IT Lab Administrator |
| Department | IT |
| Usage location (Properties tab) | **United States** |

1. Select **Review + invite**, and then **Invite**.
2. **Refresh** the page and confirm the invited user was created. You should receive the invitation email shortly.

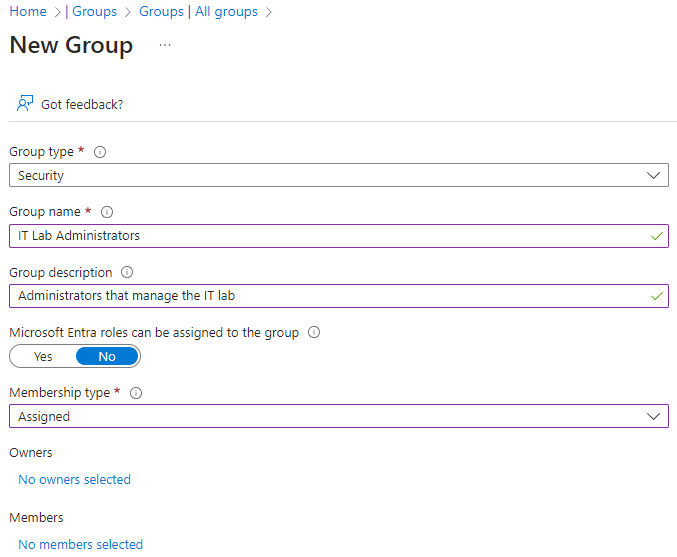
**Note:** It is unlikely you will be creating user accounts individually. Do you know how your organization plans to create and manage user accounts?

**Task 2: Create groups and add members**

In this task, you create a group account. Group accounts can include user accounts or devices. These are two basic ways members are assigned to groups: Statically and Dynamically. Static groups require administrators to add and remove members manually. Dynamic groups update automatically based on the properties of a user account or device. For example, job title.

1. In the Azure portal, search for and select Microsoft Entra ID. In the **Manage** blade, select **Groups**.
2. Take a minute to familiarize yourself with the group settings in the left pane.
   * **Expiration** lets you configure a group lifetime in days. After that time the group must be renewed by the owner.
   * **Naming policy** lets you configure blocked words and add a prefix or suffix to group names.
3. In the **All groups** blade, select **+ New group** and create a new group.

| **Setting** | **Value** |
| --- | --- |
| Group type | **Security** |
| Group name | IT Lab Administrators |
| Group description | Administrators that manage the IT lab |
| Membership type | **Assigned** |

1. **Note**: An Entra ID Premium P1 or P2 license is required for dynamic membership. If other **Membership types** are available, the options will show up in the drop-down.
2. [](https://github.com/MicrosoftLearning/AZ-104-MicrosoftAzureAdministrator/blob/master/Instructions/media/az104-lab01-create-assigned-group.png)
3. Select **No owners selected**.
4. In the **Add owners** page, search for and **select** yourself (shown in the top right corner) as the owner. Notice you can have more than one owner.
5. Select **No members selected**.
6. In the **Add members** pane, search for and **select** the **az104-user1** and the **guest user** you invited. Add both of the users to the group.
7. Select **Create** to deploy the group.
8. **Refresh** the page and ensure your group was created.
9. Select the new group and review the **Members** and **Owners** information.

**Note:** You may be managing a large number of groups. Does your organization have a plan for creating groups and adding members?

**Extend your learning with Copilot**

Copilot can assist you in learning how to use the Azure scripting tools. Copilot can also assist in areas not covered in the lab or where you need more information. Open an Edge browser and choose Copilot (top right) or navigate to *copilot.microsoft.com*. Take a few minutes to try these prompts.

* What are the Azure PowerShell and CLI commands to create a security group called IT Admins? Provide the official command reference page.
* Provide a step-by-step strategy for managing users and groups in Microsoft Entra ID.
* What are the steps in the Azure portal to bulk create users and groups?
* Provide a comparison table of internal and external Microsoft Entra ID user accounts.

**Learn more with self-paced training**

* [Understand Microsoft Entra ID](https://learn.microsoft.com/training/modules/understand-azure-active-directory/). Compare Microsoft Entra ID to Active Directory DS, learn about Microsoft Entra ID P1 and P2, and explore Microsoft Entra Domain Services for managing domain-joined devices and apps in the cloud.
* [Create Azure users and groups in Microsoft Entra ID](https://learn.microsoft.com/training/modules/create-users-and-groups-in-azure-active-directory/). Create users in Microsoft Entra ID. Understand different types of groups. Create a group and add members. Manage business-to-business guest accounts.
* [Allow users to reset their password with Microsoft Entra self-service password reset](https://learn.microsoft.com/training/modules/allow-users-reset-their-password/). Evaluate self-service password reset to allow users in your organization to reset their passwords or unlock their accounts. Set up, configure, and test self-service password reset.

**Key takeaways**

Congratulations on completing the lab. Here are some main takeaways for this lab:

* A tenant represents your organization and helps you to manage a specific instance of Microsoft cloud services for your internal and external users.
* Microsoft Entra ID has user and guest accounts. Each account has a level of access specific to the scope of work expected to be done.
* Groups combine together related users or devices. There are two types of groups including Security and Microsoft 365.
* Group membership can be statically or dynamically assigned.