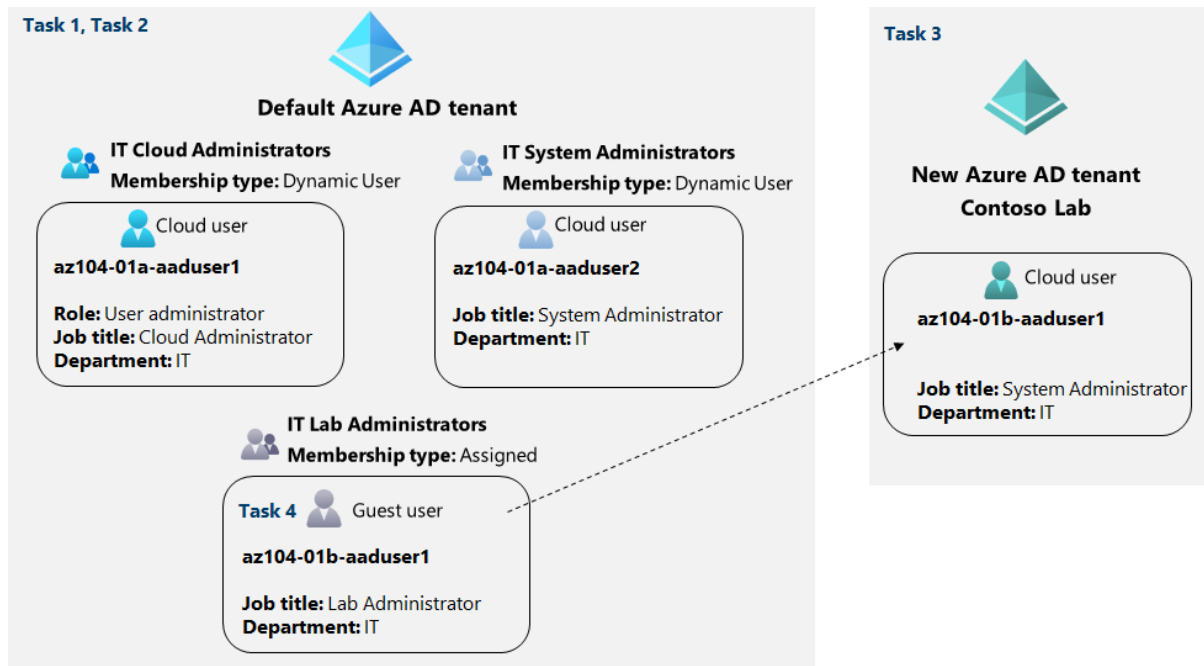


Lab 01 - Manage Azure Active Directory Identities

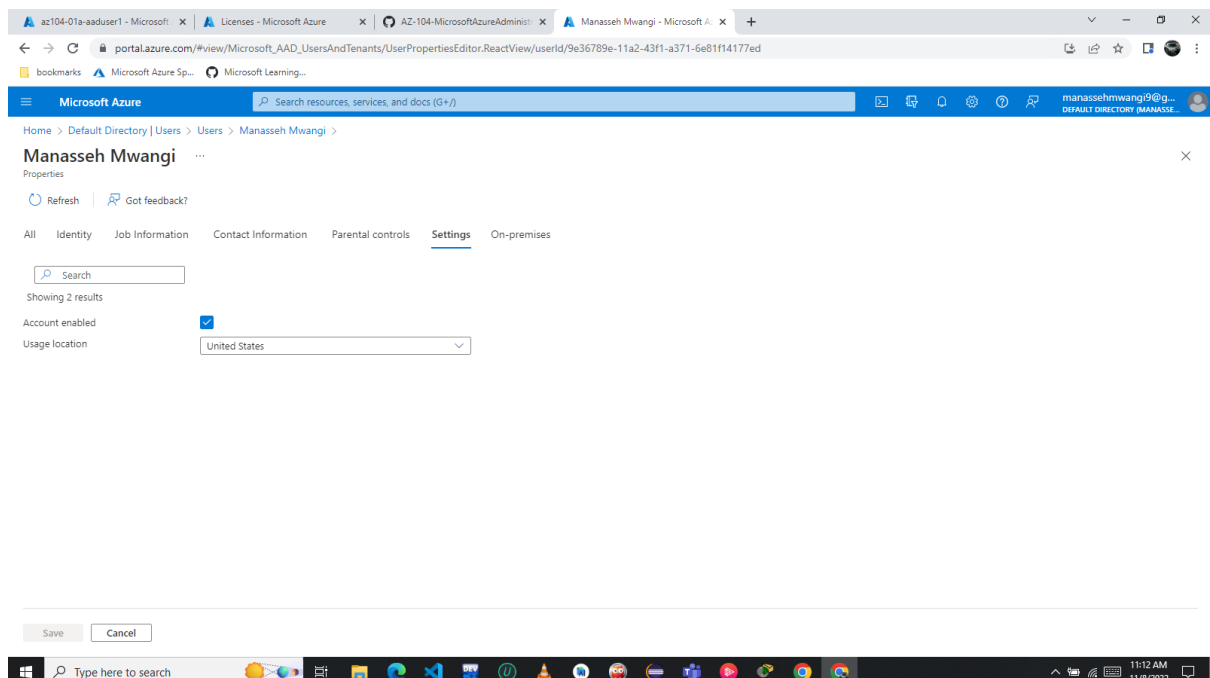
Architecture diagram



Task 1: Create and configure Azure AD users

Set **Usage location** to **United States** and click **save** to apply the change.

This is necessary in order to assign an Azure AD Premium P2 license to your user account later in this lab.



Create a new user with the following settings **az104-01a-aaduser1**, Provide a secure password, United States, Cloud Administrator & IT

Microsoft Azure

Home > Default Directory | Users > Users > New user

Identity

User name * The domain name I need isn't shown here

Name *

First name

Last name

Password

☒ Auto-generate password
☐ Let me create the password

Initial password

☐ Show Password

Groups and roles

Groups 0 groups selected

Create

In the list of users, click the newly created user account to display its blade.

Review the options available in the **Manage** section and note that you can identify the Azure AD roles assigned to the user account as well as the user account's permissions to Azure resources.

assign the **User administrator** role to **az104-01a-aaduser1**

Microsoft Azure

Home > Default Directory | Users > Users > az104-01a-aaduser1

az104-01a-aaduser1 | Assigned roles

Search + Add assignments X Remove assignments Refresh Got feedback?

Overview
Audit logs
Sign-in logs
Diagnose and solve problems

Manage

Custom security attributes (preview)
Assigned roles
Administrative units
Groups
Applications
Licenses
Devices
Azure role assignments
Authentication methods
Troubleshooting + Support
New support request

Administrative roles

Administrative roles can be used to grant access to Azure AD and other Microsoft services. [Learn more](#)

Search by name or description Add filters

Role	Description	Resource Name	Resource Type	Assignment Path	Type
<input type="checkbox"/> User administrator	Can manage all aspects of users and groups, including resetting pass...	Directory	Organization	Direct	Built-in

While this user account can access the Azure Active Directory tenant, it does not have any access to Azure resources. This is expected, since such access would need to be granted explicitly by using Azure Role-Based Access Control.

Create a new user with the following settings **az104-01a-aaduser2**, Provide a secure password, **United States, System Administrator & IT**

The screenshot shows the 'User Properties' page for 'az104-01a-aaduser2' in the Microsoft Azure portal. The user is a 'Member' created on 2022-11-08T07:59:54Z. The user principal name is 'az104-01a-aaduser2@manassehwmwangi9@gmail.onmicros...'. The job title is 'System Administrator'. A 'Cloud Network Security Tr...' window is visible in the bottom right corner.

Property	Value
Display name	az104-01a-aaduser2
First name	
Last name	
User principal name	az104-01a-aaduser2@manassehwmwangi9@gmail.onmicros...
Object ID	2c5e5f8e-2383-4b44-be1d-693b2c7f01ce
User type	Member
Creation type	
Created date time	2022-11-08T07:59:54Z
Last password change date time	2022-11-08T07:59:54Z
External user state	
External user state change date time	
Sign in sessions valid from date time	2022-11-08T07:59:54Z
Authorization info	Edit Certificate user IDs
Job title	System Administrator

Task 2: Create Azure AD groups with assigned and dynamic membership

Azure AD Premium P1 or P2 licenses are required in order to implement dynamic groups.

The screenshot shows the 'Licenses | All products' page in the Microsoft Azure portal. The page displays a table of licenses for 'Azure Active Directory Premium P2'. The table has columns for Name, Total, Assigned, Available, and Expiring soon.

Name	Total	Assigned	Available	Expiring soon
Azure Active Directory Premium P2	100	3	97	0

From the **Licenses - All products** blade, select the **Azure Active Directory Premium P2** entry, and assign all license options of Azure AD Premium P2 to your user account and the two newly created user accounts.

The screenshot shows the Microsoft Azure portal interface. The main page is the 'Assign license' blade, which is currently empty, showing 'No users and groups assigned yet'. A modal titled 'Add users and groups' is open on the right. It contains a search bar and a list of users and groups. The 'Selected items' section shows three items: 'az104-01a-aaduser1', 'az104-01a-aaduser2', and 'Manasseh Mwangi'. Each item has a 'Remove' button. The 'Select' button at the bottom of the modal is highlighted.

create a new group with the following settings: **Security, IT Cloud Administrators, Contoso IT cloud administrators & Dynamic User**

The screenshot shows the Microsoft Azure portal interface. The main page is the 'New Group' blade. It contains the following settings:

- Group type: Security
- Group name: IT Cloud Administrators
- Group description: Contoso IT cloud administrators
- Azure AD roles can be assigned to the group: No
- Membership type: Dynamic User
- Owners: No owners selected
- Dynamic user members: Add dynamic query

The 'Create' button at the bottom is highlighted.

On the **Configure Rules** tab of the **Dynamic membership rules** blade, create a new rule with the following settings:

The screenshot shows the 'Configure Rules' tab in the Azure portal. The rule is configured with the following settings:

And/Or	Property	Operator	Value
	jobTitle	Equals	Cloud Administrator

Below the rule builder, the 'Rule syntax' section shows the generated rule: `[user.jobTitle -eq "Cloud Administrator"]`.

Back on the **Groups - All groups** blade of the Azure AD tenant, click the **+ New group** button and create a new group with the following settings: **Security, IT System Administrators, Contoso IT system administrators & Dynamic User**

The screenshot shows the 'New Group' blade in the Azure portal. The group is configured with the following settings:

- Group type: Security
- Group name: IT System Administrators
- Group description: Contoso IT system administrators
- Azure AD roles can be assigned to the group: No
- Membership type: Dynamic User

The 'Owners' section shows 'No owners selected' and the 'Dynamic user members' section shows 'Add dynamic query'.

On the **Configure Rules** tab of the **Dynamic membership rules** blade, create a new rule with the following settings:

Home > Default Directory | Groups > Groups | All groups > New Group >

Dynamic membership rules

Save Discard Got feedback?

Configure Rules Validate Rules (Preview)

You can use the rule builder or rule syntax text box to create or edit a dynamic membership rule. [Learn more](#)

And/Or	Property	Operator	Value
<input type="button" value="And/Or"/>	<input type="text" value="jobTitle"/>	<input type="text" value="Equals"/>	<input type="text" value="System Administrator"/>

[+ Add expression](#) [+ Get custom extension properties](#)

Rule syntax [Edit](#)

```
(user.jobTitle -eq "System Administrator")
```

Click on the **Groups - All groups** blade of the Azure AD tenant, click the **+ New group** button, and create a new group with the following settings: **Security, IT Lab Administrators, Contoso IT Lab administrators & Assigned**

Home > Default Directory | Groups > Groups | All groups >

New Group

Got feedback?

Group type *

Group name *

Group description

Azure AD roles can be assigned to the group ☐ ☒

Membership type

Owners
No owners selected

Members
No members selected

Create

Add members

Search

- ☒ IT Cloud Administrators Selected
- ☒ IT Lab Administrators
- ☒ IT System Administrators Selected

Selected items

- ☒ IT Cloud Administrators [Remove](#)
- ☒ IT System Administrators [Remove](#)

Select

Click **No members selected**. **Add members** blade, search and select the **IT Cloud Administrators** and **IT System Administrators** groups

Click the entry representing the **IT Cloud Administrators** group and, on then display its **members** blade. Verify that the **az104-01a-aaduser1** appears in the list of group members.

The screenshot shows the Microsoft Azure portal interface. The breadcrumb navigation is: Home > Default Directory | Groups > Groups | All groups > IT Cloud Administrators. The page title is 'IT Cloud Administrators | Members'. The left sidebar shows the 'Members' blade selected under the 'Manage' section. The main content area displays a table of direct members.

Name	Type	Email	User type
az104-01a-aaduser1	User		Member

Click the entry representing the **IT System Administrators** group and, on then display its **Members** blade. Verify that the **az104-01a-aaduser2** appears in the list of group members.

The screenshot shows the Microsoft Azure portal interface. The breadcrumb navigation is: Home > Default Directory | Groups > Groups | All groups > IT System Administrators. The page title is 'IT System Administrators | Members'. The left sidebar shows the 'Members' blade selected under the 'Manage' section. The main content area displays a table of direct members.

Name	Type	Email	User type
az104-01a-aaduser2	User		Member
az104-01b-aaduser1	User		Member

Task 3: Create an Azure Active Directory (AD) tenant

In this task, you will create a new Azure AD tenant.

The screenshot shows the Microsoft Azure portal interface. The main pane displays the 'Manage tenants' section for the 'Default Directory' tenant. It lists three tenants:

Organization name	Domain name	Tenant type
Contoso Lab	adlab104cns.onmicrosoft.com	Azure Active Directory
Default Directory (Default)	manassehmgwangi@gmail.onmicrosoft.com	Azure Active Directory
United States International University (USIU)	usiu.ac.ke	Azure Active Directory

The right-hand pane shows 'Tenant details' for the 'Default Directory' tenant. It includes a 'My profile' section with fields for Name, Object ID, and Your role in this tenant. The 'Tenant information' section shows the Organization name as 'Contoso Lab' and the Tenant ID as '5867c962-9dd3-414d-9752-030b555...'. The 'Subscription state' indicates that an Azure subscription is required to continue receiving SLA support for External Identities. The 'Objects' section shows counts for Users (2), Groups (0), Applications (0), and Devices (0).

Task 4: Manage Azure AD guest users.

In this task, you will create Azure AD guest users and grant them access to resources in an Azure subscription.

Create a new user with the following settings (leave others with their defaults): **az104-01b-aaduser1**, Provide a secure password, System Administrator & IT

The screenshot shows the Microsoft Azure portal interface for the 'Users' section. The 'All users (preview)' section is active, displaying a table with two users:

Display name	User principal name	User type	On-premises sy...	Identities	Company name	Creation type
az104-01b-aaduser1	az104-01b-aaduser1_man...	Guest	No	adlab104cns.onmicrosoft.com		Invitation
Manasseh Mwangi	manassehmgwangi@gmail...	Member	No	MicrosoftAccount		

Invite a new guest user with the following settings (leave others with their defaults): **az104-01b-aaduser1, United States, Lab Administrator & IT**

Microsoft Azure

Home > Contoso Lab > Users > Users

New user

Contoso Lab

Got feedback?

Select template

☐ Create user
Create a new user in your organization.

☒ Invite user
Invite a new guest user to collaborate with your organization. The user will be emailed an invitation they can accept in order to begin collaborating.
[Help me decide](#)

Identity

Name

Email address

First name

Last name

Personal message

[Invite](#)

Add membership and add the guest user account to the **IT Lab Administrators** group.

Microsoft Azure

Home > Default Directory > Users > Users > az104-01b-aaduser1

az104-01b-aaduser1 | Groups

User

Search + Add memberships Remove memberships Refresh Columns Got feedback?

Search groups Add filters

	Name	Object Id	Group Type	Membership Type	Email	Source
<input type="checkbox"/>	IT Lab Administrators	9a99b25b-aa09-4d0e-90d4-a395...	Security	Assigned		Cloud
<input type="checkbox"/>	IT System Administrators	f684159c-ef26-4eb1-aa91-43c6b...	Security	Dynamic		Cloud

Manage

- Custom security attributes (preview)
- Assigned roles
- Administrative units
- Groups**
- Applications
- Licenses
- Devices
- Azure role assignments
- Authentication methods

Troubleshooting + Support

- New support request

Task 5: Clean up resources

Proceed by then selecting **Licensed Users**. Select the user accounts **az104-01a-aaduser1** and **az104-01a-aaduser2** to which you assigned licenses in this lab, click **Remove license**, and, when prompted to confirm, click **Yes**.

The screenshot shows the 'Licensed users' page in the Azure Active Directory Premium P2 portal. The page title is 'Azure Active Directory Premium P2 | Licensed users'. The left sidebar shows 'General' with 'Licensed users' selected. The main area has a search bar and a table of users. The table has columns for 'Name', 'User Name', and 'State'. Two users are selected with checkboxes: 'az104-01a-aaduser1' and 'az104-01a-aaduser2'. A notification on the right says 'Assignments removed' and '2 license assignments have been removed.'

Name	User Name	State
<input checked="" type="checkbox"/> az104-01a-aaduser1	az104-01a-aaduser1@manassehmgwangi9gmail.onmicrosoft.com	Active
<input checked="" type="checkbox"/> az104-01a-aaduser2	az104-01a-aaduser2@manassehmgwangi9gmail.onmicrosoft.com	Active
<input type="checkbox"/> Manasseh Mwangi	manassehmgwangi9_gmail.com#EXT#@manassehmgwangi9gmail.com	Active

Delete tenant 'Contoso Lab' blade and click **Refresh**, click **Delete**.

The screenshot shows the 'Delete tenant 'Contoso Lab'' page in the Azure Active Directory Premium P2 portal. The page title is 'Delete tenant 'Contoso Lab?'. The left sidebar shows 'Troubleshoot' and 'Refresh'. The main area has a table of resources and their status. All resources are marked as 'Successfully deleted'. A notification on the right says 'Successfully deleted tenant' and 'Successfully deleted tenant Contoso Lab.'

Resource	Status	Required action
Users	Successfully deleted	--
LinkedIn application	Successfully deleted	--
App registrations	Successfully deleted	--
Enterprise applications	Successfully deleted	--
License-based subscriptions	Successfully deleted	--
Microsoft Azure subscriptions	Successfully deleted	--
Self-service sign up products	Successfully deleted	--
Azure AD Domain Services	Successfully deleted	--
Multi-Factor Authentication	Successfully deleted	--
Identity providers	Successfully deleted	--