✓ 100 XP

Introduction

1 minute

Access to Azure resources is controlled through user accounts and identities that are defined in Azure Active Directory (Azure AD). Azure AD supports group accounts to help you organize user accounts for easier administration.

In this module, your company wants to take advantage of the user and group account features in Azure AD. You need to understand the concepts of user accounts and group accounts. You're looking for information about how to create, configure, and manage these accounts. Your organization needs support for bulk configuration of settings, group account organization, and managing accounts across multiple directories.

Learning objectives

In this module, you learn how to:

- Configure users accounts and user account properties.
- Create new user accounts.
- Import bulk user accounts with a template.
- Configure group accounts and assignment types.

Skills measured

The content in the module helps you prepare for Exam AZ-104: Microsoft Azure Administrator. The module concepts are covered in:

Manage identities and governance in Azure (15-20%)

- Manage Azure Active Directory objects
  - Create users and groups
  - Manage user and group properties
  - Manage device settings
  - Perform bulk user updates
  - Manage guest accounts

Prerequisites

None.

Next unit: Create user accounts

Continue ›

Create user accounts

3 minutes

Every user who wants access to Azure resources needs an Azure user account. A user account has all the information required to authenticate the user during the sign-in process. Azure Active Directory (Azure AD) supports three types of user accounts. The types indicate where the user is defined (in the cloud or on-premises), and whether the user is internal or external to your Azure AD organization.

Things to know about user accounts

The following table describes the user accounts supported in Azure AD. As you review these options, consider what types of user accounts suit your organization.

User account	Description
Cloud identity	A user account with a *cloud identity* is defined only in Azure AD. This type of user account includes administrator accounts and users who are managed as part of your organization. A cloud identity can be for user accounts defined in your Azure AD organization, and also for user accounts defined in an external Azure AD instance. When a cloud identity is removed from the primary directory, the user account is deleted.
Directory-synchronized identity	User accounts that have a *directory-synchronized identity* are defined in an on-premises Active Directory. A synchronization activity occurs via Azure AD Connect to bring these user accounts in to Azure. The source for these accounts is Windows Server Active Directory.
Guest user	*Guest user* accounts are defined outside Azure. Examples include user accounts from other cloud providers, and Microsoft accounts like an Xbox LIVE account. The source for guest user accounts is Invited user. Guest user accounts are useful when external vendors or contractors need access to your Azure resources.

Things to consider when choosing user accounts

- **Consider where users are defined**. Determine where your users are defined. Are all your users defined within your Azure AD organization, or are some users defined in external Azure AD instances? Do you have users who are external to your organization? It's common for businesses to support two or more account types in their infrastructure.

- **Consider support for external contributors**. Allow external contributors to access Azure resources in your organization by supporting the **Guest user** account type. When the external contributor no longer requires access, you can remove the user account and their access privileges.

- **Consider a combination of user accounts**. Implement the user account types that enable your organization to satisfy their business requirements. Support directory-synchronized identity user accounts for users defined in Windows Server Active Directory. Support cloud identities for users defined in your internal Azure AD structure or for user defined in an external Azure AD instance.

Next unit: Manage user accounts

Continue >

✓ 100 XP

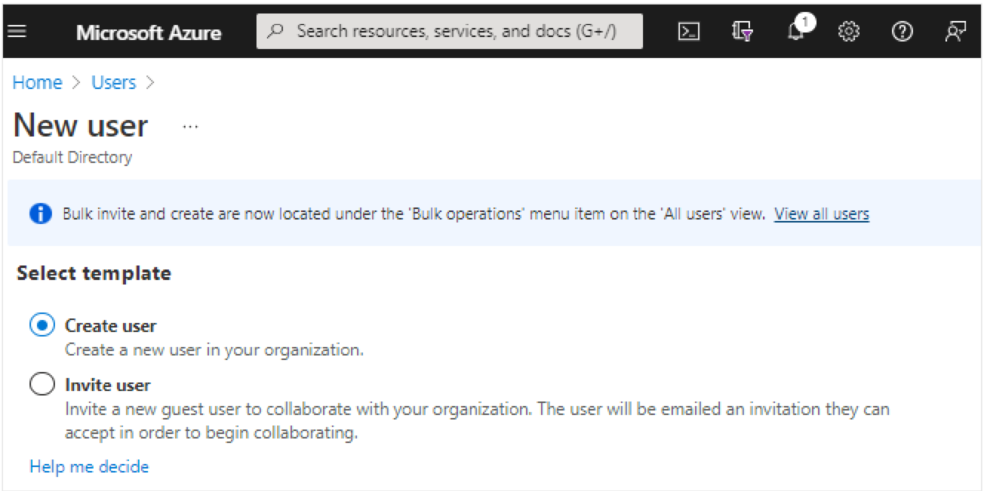
Manage user accounts

3 minutes

There are several ways to add cloud identity user accounts in Azure Active Directory (Azure AD). A common approach is by using the Azure portal. User accounts can also be added to Azure AD through Microsoft 365 Admin Center, Microsoft Intune admin console, and the Azure CLI.

Things to know about cloud identity accounts

Let's review how cloud identity user accounts are defined in Azure AD. Here's an example of the new **User** page in the Azure portal. The administrator can **Create** a user within the organization or **Invite** a guest user to provide access to organization resources:



New user ...

Default Directory

Bulk invite and create are now located under the 'Bulk operations' menu item on the 'All users' view. View all users

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

- A new user account must have a display name and an associated user account name. An example display name is `Aran Sawyer-Miller` and the associated user account name could be `asawmill@contoso.com`.
- Information and settings that describe a user are stored in the user account profile.
- The profile can have other settings like a user's job title, and their contact email address.
- A user with Global administrator or User administrator privileges can preset profile data in user accounts, such as the main phone number for the company.
- Non-admin users can set some of their own profile data, but they can't change their display name or account name.

Things to consider when managing cloud identity accounts

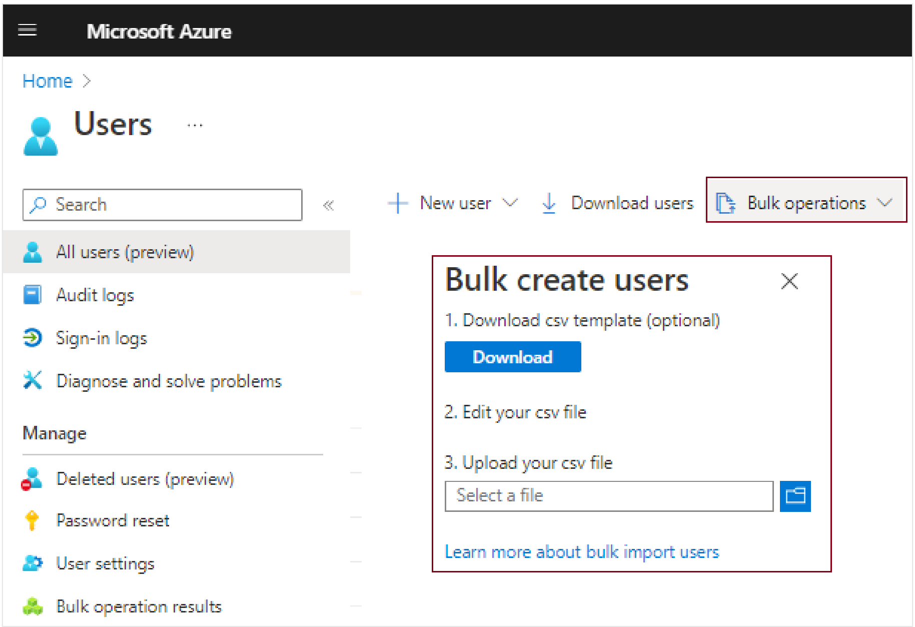
There are several points to consider about managing user accounts. As you review this list, consider how you can add cloud identity user accounts for your organization.

- **Consider user profile data**. Allow users to set their profile information for their accounts, as needed. User profile data, including the user's picture, job, and contact information is optional. You can also supply certain profile settings for each user based on your organization's requirements.
- **Consider restore options for deleted accounts**. Include restore scenarios in your account management plan. Restore operations for a deleted account are available up to 30 days after an account is removed. After 30 days, a deleted user account can't be restored.
- **Consider gathered account data**. Collect sign-in and audit log information for user accounts. Azure AD lets you gather this data to help you analyze and improve your infrastructure.

common approach for these operations is to use the Azure portal. Azure PowerShell can be used for bulk upload of user accounts.

Things to know about bulk account operations

Let's examine some characteristics of bulk operations in the Azure portal. Here's an example that shows the **Bulk create user** option for new user accounts in Azure AD:



Bulk create users

1. Download csv template (optional)

2. Edit your csv file

3. Upload your csv file

- Only Global administrators or User administrators have privileges to create and delete user accounts in the Azure portal.
- To complete bulk create or delete operations, the admin fills out a comma-separated values (CSV) template of the data for the user accounts.
- Bulk operation templates can be downloaded from the Azure AD portal.
- Bulk lists of user accounts can be downloaded.

Things to consider when creating user accounts

Here are some design considerations for creating and deleting user accounts. Think about what user account conventions and processes might be required by your organization.

- **Consider naming conventions**. Establish or implement a naming convention for your user accounts. Apply conventions to user account names, display names, and user aliases for consistency across the organization. Conventions for names and aliases can simplify the bulk create process by reducing areas of uniqueness in the CSV file. A convention for user names could begin with the user's last name followed by a period, and end with the user's first name, as in `Sawyer-Miller.Aran@contoso.com`.
- **Consider using initial passwords**. Implement a convention for the initial password of a newly created user. Design a system to notify new users about their passwords in a secure way. You might generate a random password and email it to the new user or their manager.
- **Consider strategies for minimizing errors**. View and address any errors, by downloading the results file on the **Bulk operation results** page in the Azure portal. The results file contains the reason for each error. An error might be a user account that's already been created or an account that's duplicated. Generally, it's easier to upload and troubleshoot smaller groups of user accounts.

Next unit: Create group accounts

✓ 100 XP

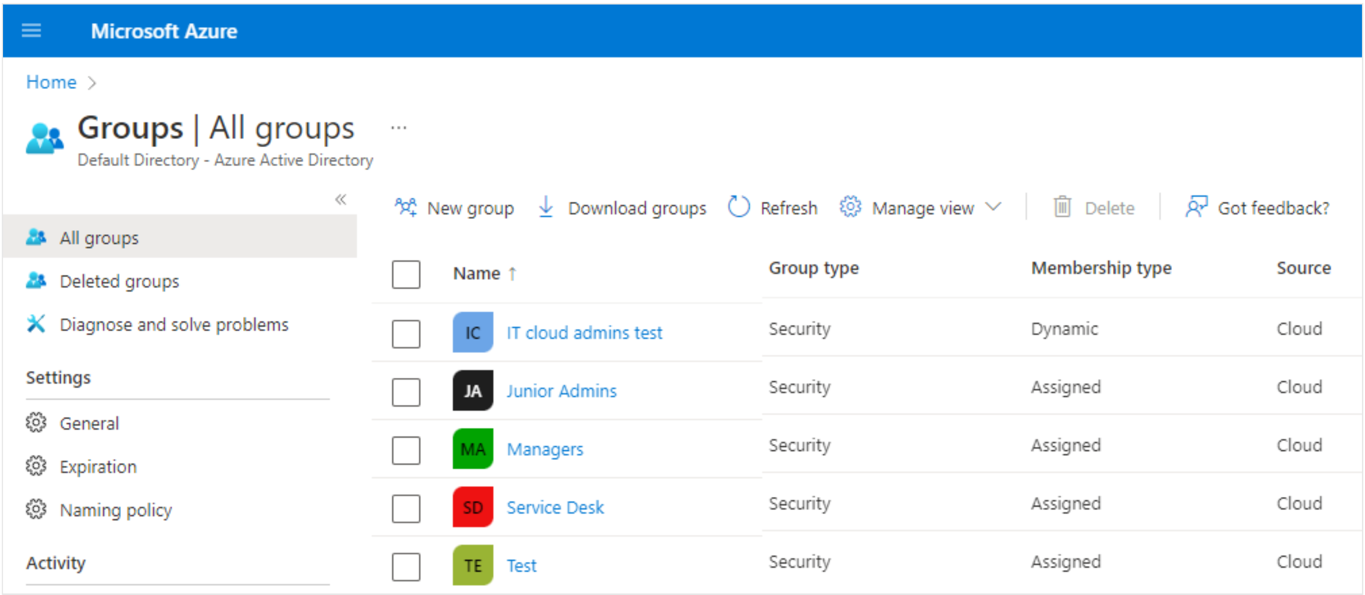
Create group accounts

3 minutes

Azure Active Directory (Azure AD) allows your organization to define two different types of group accounts. **Security groups** are used to manage member and computer access to shared resources for a group of users. You can create a security group for a specific security policy and apply the same permissions to all members of a group. **Microsoft 365 groups** provide collaboration opportunities. Group members have access to a shared mailbox, calendar, files, SharePoint site, and more.

Things to know about creating group accounts

Review the following characteristics of group accounts in Azure AD. The following screenshot shows a list of groups in the Azure portal:



□	Name ↑	Group type	Membership type	Source
□	IC IT cloud admins test	Security	Dynamic	Cloud
□	JA Junior Admins	Security	Assigned	Cloud
□	MA Managers	Security	Assigned	Cloud
□	SD Service Desk	Security	Assigned	Cloud
□	TE Test	Security	Assigned	Cloud

- Use security groups to set permissions for all group members at the same time, rather than adding permissions to each member individually.
- Add Microsoft 365 groups to enable group access for guest users outside your Azure AD organization.
- Security groups can be implemented only by an Azure AD administrator.
- Normal users and Azure AD admins can both use Microsoft 365 groups.

Things to consider when adding group members

When you add members to a group, there are different ways you can assign member access rights. As you read through these options, consider which groups are needed to support your organization, and what access rights should be applied to group members.

Access rights	Description
Assigned	Add specific users as members of a group, where each user can have unique permissions.
Dynamic user	Use dynamic membership rules to automatically add and remove group members. When member attributes change, Azure reviews the dynamic group rules for the directory. If the member attributes meet the rule requirements, the
Access rights	**Description**

	member is added to the group. If the member attributes no longer meet the rule requirements, the member is removed.
Dynamic device	(*Security groups only*) Apply dynamic group rules to automatically add and remove devices in security groups. When device attributes change, Azure reviews the dynamic group rules for the directory. If the device attributes meet the rule requirements, the device is added to the security group. If the device attributes no longer meet the rule requirements, the device is removed.

Next unit: Create administrative units

Continue >

How are we doing? ☆ ☆ ☆ ☆ ☆

✓ 100 XP ▶

Create administrative units

3 minutes

As you design your strategy for managing identities and governance in Azure, planning for comprehensive management of your Azure Active Directory (Azure AD) infrastructure is critical. It can be useful to restrict administrative scope by using administrative units for your organization. The division of roles and responsibilities is especially helpful for organizations that have many independent divisions.

Consider the management tasks for a large university that's composed of several different schools like Business, Engineering, and Medicine. The university has administrative offices, academic buildings, social buildings, and student dormitories. For security purposes, each business office has its own internal network for resources like servers, printers, and fax machines. Each academic building is connected to the university network, so both instructors and students can access their accounts. The network is also available to students and deans in the dormitories and social buildings. Across the university, guest users require access to the internet via the university network.

The university has a team of IT admins who work together to control resource access, manage users, and set policies for the school. Some admins have greater privileges than others depending on the scope of their responsibilities. A central authority is needed to plan, manage, and oversee the complete structure. In this scenario, you can assign administrative units to make it easier to manage the organization.

Things to think about administrative units

Consider how a central admin role can use administrative units to support the Engineering department in our scenario:

- Create a role that has administrative permissions for only Azure AD users in the Engineering department administrative unit.
- Create an administrative unit for the Engineering department.
- Populate the administrative unit with only the Engineering department students, staff, and resources.
- Add the Engineering department IT team to the role, along with its scope.

Things to consider when working with administrative units

Think about how you can implement administrative units in your organization. Here are some considerations:

- **Consider management tools**. Review your options for managing AUs. You can use the Azure portal, PowerShell cmdlets and scripts, or Microsoft Graph.
- **Consider role requirements in the Azure portal**. Plan your strategy for administrative units according to role privileges. In the Azure portal, only the Global Administrator or Privileged Role Administrator users can manage AUs.
- **Consider scope of administrative units**. Recognize that the scope of an administrative unit applies only to *management* permissions. Members and admins of an administrative unit can exercise their default *user* permissions to browse other users, groups, or resources outside of their administrative unit.

Next unit: Interactive lab simulation

Continue ›

✓ 100 XP

Interactive lab simulation

30 minutes

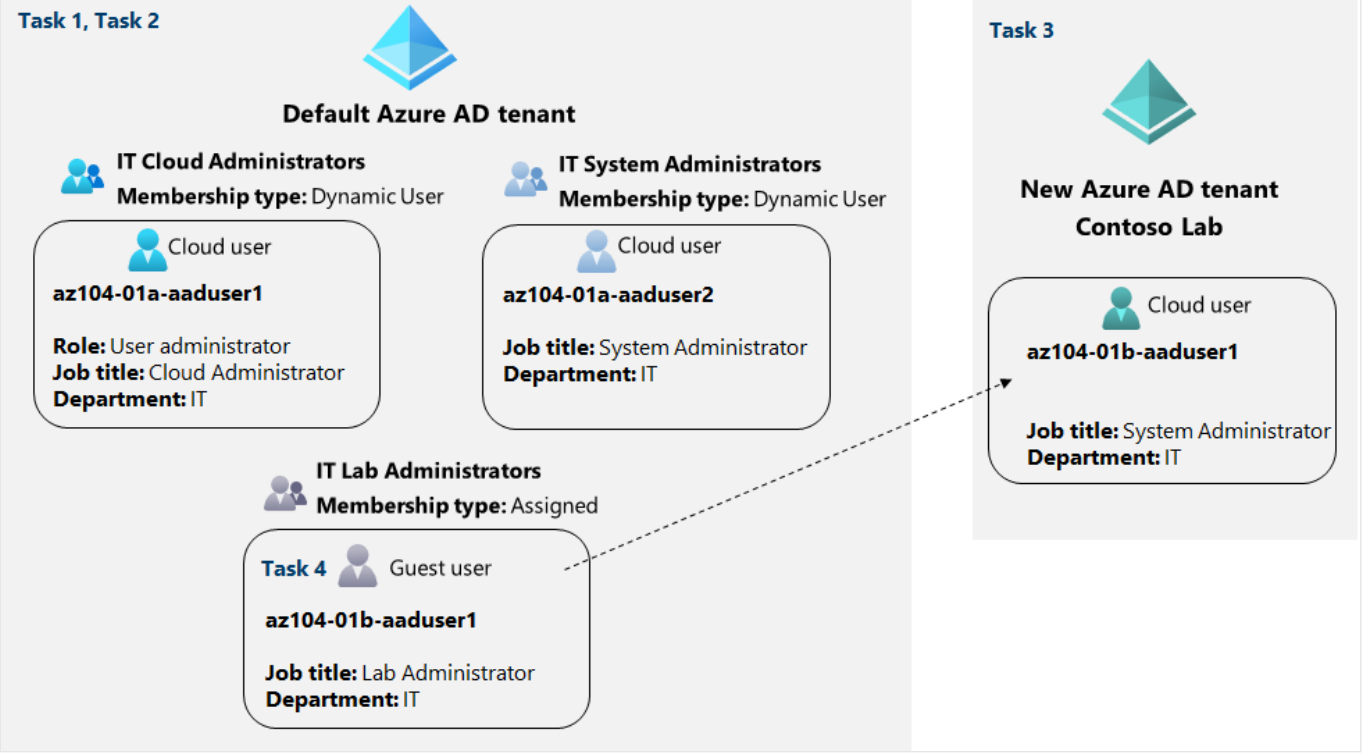
Lab scenario

Your organization will be using Azure AD authentication. You've been tasked with provisioning the required user and group accounts. Membership of the groups should be updated automatically based on the user job titles. You also need to invite guest users from another tenant. These guest users should have only limited permissions to resources in your subscription.

Your organization has these specific requirements:

- Any user with the Cloud Administrator job title should be assigned to the IT Cloud Administrator group.
- Any user with the System Administrator job title should be assigned to the IT System Administrator group.
- Any user that is a member of the IT Cloud Administrator group or the IT System Administrator group should be assigned to the IT Lab Administrator group.
- A System Administrator in another Active Directory tenant should be invited as guest user with limited permissions.

Architecture diagram



Objectives

- **Task 1**: Create and configure Azure AD users.
  - User **AZ104-01a-aaduser1** will be a Cloud Administrator assigned the User Administrator role.
  - User **AZ104-01a-aaduser2** will be a System Administrator.
- **Task 2**: Create AD groups with assigned and dynamic membership.
  - The **IT Cloud Administrator** group should include any user with the Cloud Administrator job title.
  - The **IT System Administrator** group should include any user with the System Administrator job title.

  - The **IT Lab Administrator** group should include any user in the IT Cloud Administrator group or the IT System Administrator group.
- **Task 3**: Create an Azure Active Directory (AD) tenant. This tenant will be used to demonstrate guest users.
- **Task 4**: Manage Azure AD guest users.
  - In the new Azure AD tenant create a System Administrator user, **az104-01b-aaduser1**.
  - Invite the new user as a guest user to your subscription.

ⓘ Note

Click on the thumbnail image to start the lab simulation. When you're done, be sure to return to this page so you can continue learning.

Microsoft Azure
Interactive Lab Simulation:
Manage Azure Active Directory identities
From AZ-104: Microsoft Azure Administrator

Next unit: Knowledge check

Continue >

How are we doing? ☆ ☆ ☆ ☆ ☆

200 XP

Knowledge check

3 minutes

Your company has decided to implement the user and group account features of Azure Active Directory (Azure AD) in their identity and governance strategy. You need to explain the types of accounts, roles, and assignments to the planning team, and guide them in their strategy.

Answer the following questions

Choose the best response for each of the questions below. Then select **Check your answers**.

1. What type of user account allows an external organization to access your resources? *

○ A Contributor user account for each member of the team.

○ An administrator account for each member of the team.

○ A guest user account for each member of the external team.

2. What kind of group account can you create so you can apply the same permissions to all group members? *

○ Security group

○ Azure AD bulk group

○ Microsoft 365 group

3. Which Azure AD role enables a user to manage all groups in your Teams tenants, and also assign other admin roles? *

○ Global administrator

○ Security administrator

○ User administrator

Check your answers

How are we doing? ☆ ☆ ☆ ☆ ☆

Summary and resources

1 minute

Azure Administrators must be familiar with configuring user and group accounts in Azure Active Directory.

In this module, you learned that every user who wants access to Azure resources needs an Azure user account. Azure AD supports access to your organization's resources by assigning access rights to users and groups. You discovered how user and group accounts are created in Azure AD. You explored how to configure and manage user and group accounts, including bulk configuration. You reviewed how your organization can support group account organization, and manage accounts across multiple directories.

Learn more with Azure documentation

- Discover the fundamentals of Azure Active Directory.
- Read about Azure built-in roles.
- Manage your resources with Azure custom roles.

Learn more with self-paced training

- Explore how to create users and groups in Azure AD.

Learn more with optional hands-on exercises

- Manage users and groups in Azure AD (sandbox).

Module incomplete:

Go back to finish >

How are we doing? ☆ ☆ ☆ ☆ ☆