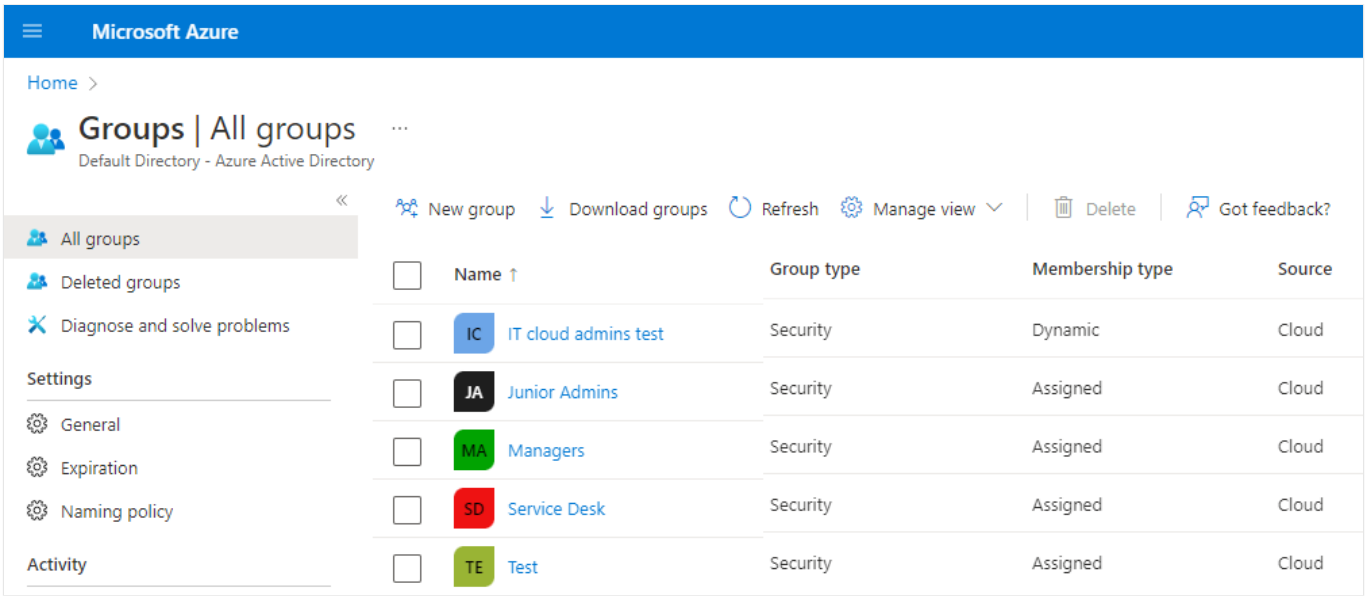
Create group accounts

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:



- 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? ☆ ☆ ☆ ☆ ☆