Manage app and resource access by using Azure Active Directory groups

3 minutes

You want to give the all developers within your organization the same access. You also want to manage who is part of the developers group and who isn't.

Azure Active Directory (Azure AD) helps you to manage your cloud-based apps, on-premises apps, and resources by using your organization's groups. Your resources can be part of the Azure AD organization, like permissions to manage objects through roles. Or your resources can be external to the organization, like software as a service (SaaS) apps, Azure services, SharePoint sites, and on-premises resources.

Access management in Azure AD

- **Azure AD roles**: Use Azure AD roles to manage Azure AD-related resources like users, groups, billing, licensing, application registration, and more.
- **Role-based access control (RBAC) for Azure resources**: Use RBAC roles to manage access to Azure resources like virtual machines, SQL databases, or storage. For example, you could assign an RBAC role to a user to manage and delete SQL databases in a specific resource group or subscription.

Access rights through single user or group assignment

Azure AD helps you provide access rights to a single user or to an entire group of users. You can assign a set of access permissions to all the members of the group. Access permissions range from full access to the ability to create or remove resources.

There are different ways you can assign access rights:

- **Direct assignment**: Assign a user the required access rights by directly assigning a role that has those access rights.

- **Group assignment**: Assign a group the required access rights, and members of the group will inherit those rights.
- **Rule-based assignment**: Use rules to determine a group membership based on user or device properties. For a user account or device's group membership to be valid, the user or device must meet the rules. If the rules aren't met, the user account or device's group membership is no longer valid. The rules can be simple. You can select prewritten rules or write your own advanced rules.

In the next unit, we'll assign users to an Azure AD group and use rule-based assignment to automatically manage their group membership.

Next unit: Exercise - Assign users to Azure Active Directory groups

Continue >

How are we doing? ☆ ☆ ☆ ☆ ☆