< Previous Unit 6 of 9 Next >

✓ 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 >