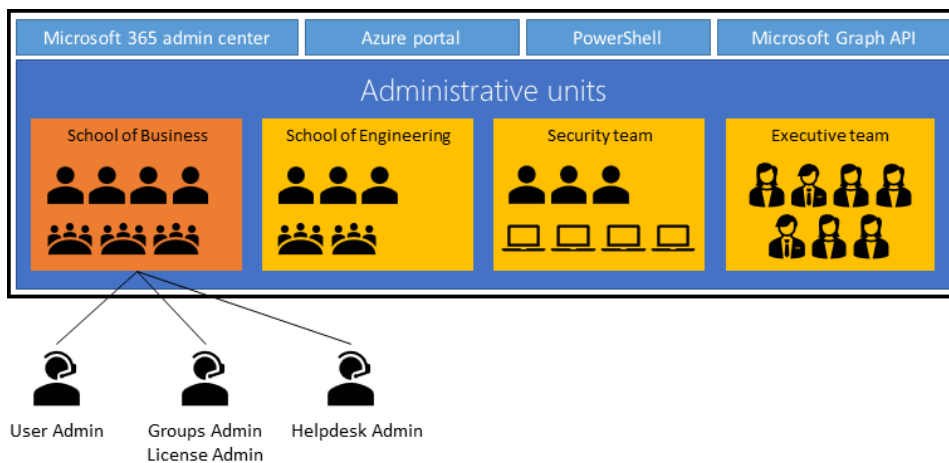


AZ-104 Azure Identity - Creating Administrative Units

Administrative Units for Entra ID

An administrative unit is a Microsoft Entra resource that can be a container for other Microsoft Entra resources. An administrative unit can contain only users, groups, or devices.



Constraints

- Administrative units can't be nested.
- Administrative units are currently not available in Microsoft Entra ID Governance.

Groups

Adding a group to an administrative unit brings the group itself into the management scope of the administrative unit, but **not** the members of the group. In other words, an administrator scoped to the administrative unit can manage properties of the group, such as group name or membership, but they cannot manage properties of the users or devices within that group (unless those users and devices are separately added as members of the administrative unit).

For example, a User Administrator scoped to an administrative unit that contains a group can and can't do the following:

Permissions	Can do
Manage the name of the group	<input type="checkbox"/>
Manage the membership of the group	<input type="checkbox"/>
Manage the user properties for individual members of the group	<input type="checkbox"/>
Manage the user authentication methods of individual members of the group	<input type="checkbox"/>
Reset the passwords of individual members of the group	<input type="checkbox"/>

Plan the organization

Plan the organization and evaluate its needs to determine the value that administrative units can provide for managing identities like groups and users.

Create and Administrative Unit

Create an administrative unit to logically divide the organization and allow for scoping.

Home >

Default Directory | Overview

Microsoft Entra ID

- Overview
- Preview features
- Diagnose and solve problems
- Manage
 - Users
 - Groups
 - External Identities
 - Roles and administrators
 - Administrative units
 - Delegated admin partners
 - Enterprise applications
 - Devices
 - App registrations
 - Identity Governance
 - Application proxy
 - Custom security attributes
 - Licenses

+ Add Manage tenants What's new Preview features Got feedback?

Azure Active Directory is now Microsoft Entra ID. [Learn more](#)

Overview Monitoring Properties Recommendations Tutorials

Search your tenant

Basic information

Name	Default Directory	Users	4
Tenant ID	bd5269da-06cb-4962-bbc1-d3d58a129ec9	Groups	1
Primary domain	csrgzzoutlook.onmicrosoft.com	Applications	0
License	Microsoft Entra ID Free	Devices	0

Alerts



Microsoft Entra Connect v1 Retirement

All version 1.x builds of Microsoft Entra Connect (formerly AAD Connect) will soon stop working between October 2023 – March 2024. You must move to Cloud Sync or Microsoft Entra Connect v2.x.

[Learn more](#)



Azure AD is now Microsoft Entra ID

Microsoft Entra ID is the new name for Azure Active Directory. No action is required from you.

[Learn more](#)

Home > Default Directory

Default Directory | Administrative units

Microsoft Entra ID

- Overview
- Preview features
- Diagnose and solve problems
- Manage
 - Users

Learn more + Add Delete Refresh Preview features Got feedback?

Search administrative units Add filters

Name	Description	Restricted management	Membership type
MX		No	Assigned



MX | Properties (Preview) ...

Default Directory - Microsoft Entra ID

Save Discard

Manage

Properties (Preview)

Users

Groups

Devices

Roles and administrators

Activity

Bulk operation results

Display name *

Description

Membership type * ⓘ

Object ID

Restricted management administrative unit ⓘ

Yes No

- Purpose of administrative units: An Azure AD resource for providing a container for Azure AD Objects.
- Benefits of Administrative units: Allow you to control the scope of your administrative users.

Revision #3

Created 15 February 2024 20:21:24 by Cesar Gzz

Updated 15 February 2024 21:02:41 by Cesar Gzz