



Assigning an Azure AD built-in Role

Azure AD built-in roles are a set of predefined roles that provide granular access to various Azure AD resources and functionalities. These roles are designed to facilitate access management and delegation of administrative tasks within Azure AD. Here are some key points about Azure AD built-in roles:

1. **Predefined Permissions:** Each built-in role comes with a set of permissions that define what actions a user assigned to that role can perform within Azure AD.
2. **Granular Access Control:** Azure AD built-in roles offer granular access control, allowing administrators to assign specific roles to users based on their responsibilities and the tasks they need to perform.
3. **Common Scenarios:** Built-in roles cater to common administrative scenarios, such as user management, application management, password management, and role management.
4. **Scope of Permissions:** Some built-in roles have permissions that are limited to specific scopes, such as management of users within a single directory or across multiple directories.
5. **Hierarchy of Roles:** Azure AD built-in roles follow a hierarchical structure, with roles at different levels of privilege. For example, the "Global Administrator" role has the highest level of privilege and encompasses permissions across the entire Azure AD tenant, while other roles may have more limited scopes.
6. **Role-Based Access Control (RBAC):** Azure AD built-in roles are part of the Role-Based Access Control (RBAC) model, which allows organizations to manage access to Azure resources based on assigned roles.

In this lab, we're showcasing how to assign Azure AD built-in roles to user accounts within the Azure AD environment. The end goal is to delegate specific administrative tasks to users by granting them appropriate permissions defined by these built-in roles. By assigning roles such as User Administrator, we empower users to perform tasks like creating new user accounts, thus streamlining administrative processes and enhancing efficiency in managing Azure AD resources. Ultimately, this exercise aims to demonstrate effective access management and delegation of administrative responsibilities within Azure AD.



To begin with the Lab:

1. In this lab we are going to assign our demo user an Azure AD built-in role.
2. For that you should navigate to Microsoft Entra ID from your Azure Admin Account.
3. Then open users, from all users you need to open the demo user and then expand the Manage section. There you have to choose assigned roles.
4. Here you will see that currently you have zero roles assigned to it.

demouser1 | Assigned roles

User

Search X < + Add assignments X Remove assignments Refresh Got feedback?

Overview Audit logs Sign-in logs Diagnose and solve problems Manage Custom security attributes Assigned roles

Administrative roles

Administrative roles can be used to grant access to Microsoft Entra ID and other Microsoft services. [Learn more](#)

Search by name or description Add filters

Role ↑↓	Description	Resource Name ↑↓
No directory roles assigned.		

5. But if you check in Azure role assignments, you will see that you have a reader role assigned here.
6. This role is associated with RBAC (role-based access control).

Home > demouser1

demouser1 | Azure role assignments

User

Search X < If this identity has role assignments that you don't have permission to read, they won't be shown in the list. [Learn more](#)

Subscription * Azure Pass - Sponsorship

Role	Resource Name	Resource Type	Assigned To
Reader	demo-entra-RG	Resource Group	demouser1

Overview Audit logs Sign-in logs Diagnose and solve problems Manage Custom security attributes Assigned roles Administrative units Groups Applications Licenses Devices Azure role assignments Authentication methods Troubleshooting + Support New support request

7. But when you are in assigned roles then it is known as Azure AD roles.
8. Now come back to assigned roles and click on add assignments.

+ Add assignments X Remove assignments Refresh Got feedback?

Administrative roles

Administrative roles can be used to grant access to Microsoft Entra ID and other Microsoft services. [Learn more](#)

Search by name or description Add filters

Role ↑↓	Description	Resource Name ↑↓	Resource Type ↑↓	Assignment Path ↑↓	Type
No directory roles assigned.					

9. Then you need to search user administrator role and choose it accordingly.

Choose admin roles that you want to assign to this user. [Learn more](#)

Role	Description
<input type="checkbox"/>  Extended Directory User Administrator	Manage all aspects of external user profiles in the extended directory for Teams.
<input checked="" type="checkbox"/>  User Administrator	Can manage all aspects of users and groups, including resetting passwords for limited admins.

10. After some time you'll be able to see the role in place.

+ Add assignments X Remove assignments ⏪ Refresh | Got feedback?

Administrative roles
Administrative roles can be used to grant access to Microsoft Entra ID and other Microsoft services. [Learn more](#)

Role	Description	Resource Name	Resource Type	Assignment Path	Type
<input type="checkbox"/>  User Administrator	Can manage all aspects of users and groups, including resetting passwords for limited admins.	Directory	Organization	Direct	Built-in

11. Now if you login with your demo user then go to Microsoft Entra then go to users.

Microsoft Azure

Home > Default Directory | Overview

Azure Active Directory is now Microsoft Entra ID. Learn more

Overview Monitoring Properties Recommendations Tutorials

Basic information

Name	Default Directory	Users	8
Tenant ID	30aa9099-b1e3-4652-abe8-06318e4b8029	Groups	3
Primary domain	pulkitkumar2711@gmail.onmicrosoft.com	Applications	2
License	Microsoft Entra ID Free	Devices	2

Alerts

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](#)

Upcoming MFA Server deprecation
Please migrate from MFA Server to Microsoft Entra Multi-Factor Authentication by September 2024 to avoid any service impact.
[Learn more](#)

12. Now you can see that you have the ability to create a new user from your demo user.

The screenshot shows the 'Users' page in Microsoft Entra ID. On the left, there's a sidebar with links: 'All users', 'Audit logs', 'Sign-in logs', and 'Diagnose and solve problems'. On the right, there's a main content area with a search bar and navigation buttons ('New user', 'Download users', etc.). A dropdown menu is open over the 'New user' button, showing two options: 'Create new user' (with the sub-instruction 'Create a new internal user in your organization') and 'Invite external user' (with the sub-instruction 'Invite an external user to collaborate with your organization').

13. Below you can also see that we have logged in with our demo user 2 account and it does not have the ability to create a new user because we haven't assigned roles to this user yet.

This screenshot shows the 'Users' page in Microsoft Azure. The interface is similar to the one above, with a sidebar and a main content area. A dropdown menu is open over the 'New user' button, showing the same two options: 'Create new user' and 'Invite external user'. The 'Create new user' option has the sub-instruction 'Create a new internal user in your organization'. The 'User principal name' field is partially filled with 'er'.

14. Plus, from your default directory of your admin account if you choose roles and administrators.

Home >

i Default Directory | Overview

The screenshot shows the Microsoft Azure AD Default Directory Overview page. On the left, there's a sidebar with various links: Overview (selected), Preview features, Diagnose and solve problems, Manage (with sub-links for Users, Groups, External Identities), and Roles and administrators (which is highlighted with a red box). The main content area has sections for Basic information (Name, Tenant ID), and a search bar.

15. From here also you can directly attach an Azure AD role to user.

The screenshot shows the 'Roles and administrators | All roles' page in Microsoft Azure AD. It displays a list of roles, with 'user administrator' selected. The page includes a sidebar with links for All roles, Protected actions, Diagnose and solve problems, Activity, and Troubleshooting + Support. A filter bar at the top allows searching for roles and applying filters. Below the filter bar, there's a note about creating custom roles. The main table lists roles with columns for Role, Description, Privileged, Ass., and Type. The 'user administrator' row is highlighted.

Role	Description	Privileged	Ass.	Type
Extended Directory User Administrator	Manage all aspects of external user profiles in the extended directory for Teams.	0	Built-in	
User Administrator	Can manage all aspects of users and groups, including resetting passwords for limited admins.	1	Built-in	