< Previous Unit 4 of 8 ∨ Next >

✓ 100 XP

Understand user security roles and security role defaults

6 minutes

Roles are groups of permissions that you can assign to a user to grant them access and various capabilities and functionality like read, delete, or edit of records in an entity within an environment. Roles are granular and can be assigned to one or many entities in an environment. Roles can also control certain actions like the ability to create a custom entity or option sets. Additionally, users are associated with one or many roles, and associating a user with a role gives them access to data and functionality that is specified within that role.

User security roles are either:

- Standard and created with every instance of Microsoft Dataverse.
- Custom and created by an administrator.

This unit examines each type of security role.

Default user security roles

When you create a new instance of Dataverse in an environment, a database is created with standard entities and several default security roles are created. The following predefined roles are available every time you create a Dataverse environment by using the Power Apps portal. Unless otherwise noted, all the privileges have global scope.

Dataverse includes several default roles with different access levels to standard entities and actions. The default standard roles are listed in the following table.

Security role	Database privileges*	Description

Security role	Database privileges*	Description
Environment Admin	Create, Read, Write, Delete, Customizations, Security Roles	The Environment Admin role can perform all administrative actions on an environment, including the following: • Add or remove a user from either the Environment Admin or Environment Maker role. • Provision a Dataverse database for the environment. After a database is provisioned, the System Customizer role should also be assigned to an Environment Admin to give them access to the environment's data. • View and manage all resources created within an environment. • Set data loss prevention policies.
Environment Maker	Customizations	Can create new resources associated with an environment, including apps, connections, custom APIs, gateways, and flows using Microsoft Power Automate. However, this role doesn't have any privileges to access data within an environment. More information: Environments overview
System Administrator	Create, Read, Write, Delete, Customizations, Security Roles	Has full permission to customize or administer the environment, including creating, modifying, and assigning security roles. Can view all data in the environment. More information: Privileges required for customization
System Customizer	Create (self), Read (self), Write (self), Delete (self), Customizations	Has full permission to customize the environment. However, users with this role can only view records for environment entities that they create. More information: Privileges required for customization
Basic User	Read (self), Create (self), Write (self), Delete (self)	Can run an app within the environment and perform common tasks for the records that they own. Note that this only applies to non-custom entities.
Delegate	Act on behalf of another user	Allows code to *impersonate*, or run as another user. Typically used with another security role to allow access to records. More information: Impersonate another user

Security role	Database privileges*	Description
Support User	Read Customizations, Read Business Management settings	Has full Read permission to customization and business management settings to allow Support staff to troubleshoot environment configuration issues. Does not have access to core records.

*The scope of these privileges is global, unless specified otherwise.

ⓘ Note

- Environment Maker and Environment Admin are the only predefined roles for environments that have no Dataverse database.
- The Environment Makerrole can create resources within an environment, including apps, connections, custom connectors, gateways, and flows using Power Automate. Environment makers can also distribute the apps they build in an environment to other users in your organization. They can share the app with individual users, security groups, or all users in the organization. More information: **Share an app in Power Apps**
- For users who make apps that connect to the database and need to create or update entities and security roles, you need to assign the System Customizer role in addition to the Environment Maker role. This is necessary because the Environment Maker role doesn't have privileges on the environment's data.
- If the environment has a Dataverse database, a user must be assigned the System Administrator role instead of the Environment Admin role for full admin privileges, as described in the preceding table.

Tip

Add the System Customizer role to a user if you want them to be able to create new entities.

When you add a user to an environment in Dataverse, the user is automatically assigned to the following:

- Security user roles - Basic User

- Environment roles - Environment Maker

Next unit: Create a custom role

Continue >