Types of predefined security roles

The following predefined roles are available with a Power Apps environment. Unless otherwise noted, all the privileges have global scope.

ABOUT PREDEFINED SECURITY ROLES

Security role	Privileges	Description
Environment Maker	None	users who have this role can create new resources that are associated with an environment, including apps, connections, custom application programming interfaces (API's), gateways, and flows that use Power Automate. But these users can't access the data in an environment. To learn more about envrionments, see Announcing Power Apps environments.
System Administrator	Create, Read, Write, Delete, Customize	This role has full permission to customize or administer the environment, including creating, changing, and assigning security roles. Users who have this role can view all data in the environments. To learn more, see Privileges required for customization.
System Customizer	Create (self), Read (self), Write (self), Delete (self), Customizations	This role has full permission to customize the environment. But users who have this role can view rows only for environment tables that they create. To learn more, see Privileges required for customization.
Microsoft Dataverse User	Read, Create (self), Write (self), Delete (self)	Users who have this role can run an app in the environment and perform common tasks for the rows they own.
Delegate	Act on behalf of another user	This role lets code run as or impersonate another user. This role is typically used with another security role to provide access to rows. To learn more, see Impersonate another user.

Mark as completed

Like Dislike Report an issue