User Roles

User Roles in Cisco Defense Orchestrator

There are a variety of user roles in Cisco Defense Orchestrator (CDO): Read-Only, Edit-Only, Deploy-only, Admin, and Super Admin. User roles are configured for each user on each tenant. If a CDO user has access to more than one tenant, they may have the same user ID but different roles on different tenants. A user may have a read-only role on one tenant and a Super Admin role on another. When the interface or the documentation refers to a Read-only user, an Admin user, or a Super Admin user we are describing that user's permission level on a particular tenant.

Roles in Multicloud Defense

Roles play an important part of what a user is allowed to do when accessing the Multicloud Defense tenant through the Multicloud Defense portal. A role is a privilege that grants the user a set of permissions.

There are three available roles:

- Super Admin (admin_super) .
- Edit-only Admin (admin_rw).
- Read-only Admin (admin_read-only) .

There are two permission definitions:

- Modify - Read, write, edit, and delete.
- Read - Read-only.

The permissions for each setting associated with each role are outlined in the following table:

Setting	Super Admin(admin_super)	Edit-Only (admin_rw)	Read-Only (admin_read-only)
Management			
Users	Modify	Modify (except Super Admin)	Read

Setting	Super Admin(admin_super)	Edit-Only (admin_rw)	Read-Only (admin_read-only)
MFA Enable / Disable	Modify	Modify (except Super Admin)	Read
Reset MFA	Modify	Modify (except Super Admin)	Read
API Keys	Modify	Modify	Read
Roles	Read	Read	Read
Account > Application Tags	Modify	Modify	Read
Account > Email Domains	Modify	Read	Read
System	Read	Read	Read
Metering	Read	Read	Read
Alert Profiles			
Services	Modify	Modify	Read
Alert	Modify	Modify	Read

Only one (1) user within a Multicloud Defense tenant can be assigned the super admin role. This user is seen as the **owner** of the account and is synonymous with the owner of an AWS account or a linux root account. All other users should be assigned a read/write admin or read-only admin role.

The super admin role is assigned by Multicloud Defense and is granted to the first user created when the Multicloud Defense tenant is created. If any changes are required to a super admin user, please contact Multicloud Defense Support.