# User Management



# Users, Roles, and Permissions

The Cisco ACI Multi-Site Orchestrator allows access according to a user's role defined by role-based access control (RBAC). Roles are used in both local and external authentication. The following user roles are available in Cisco ACI Multi-Site Orchestrator.

- Power User—A role that allows the user to perform all the operations.
- Site Manager—A role that allows the user to manage sites, tenants, and associations between them.
- Schema Manager—A role that allows the user to manage all schemas regardless of their tenant associations.
- Schema Editor—A role that allows the user to manage schemas that contain at least one tenant to which the user is explicitly associated.
- User Manager—A role that allows the user to manage all the users, their roles, and passwords.

Each role above is associated with a set of permissions, which in turn are used to show relevant and hide irrelevant elements from the user's view of the Orchestrator GUI. For example, the User Manager role has only the user-related permissions associated with it and as such the user with that role will only see **Users** and **Admin** tabs in the GUI.

### User Roles and Permissions

The following table lists the Cisco ACI Multi-Site permissions allowed with each available user role. The `Attribute-Value (AV)` column specifies the user configuration string required when configuring an external authentication server for use with the Multi-Site Orchestrator. External authentication is covered in more detail in the *Administrative Operations* chapter.

*Table 1: User Roles*

| User Role | Permissions | Attribute-Value (AV) Pair |
|---|---|---|
| Power User | • Dashboard<br>• Sites<br>• Schemas<br>• Tenants<br>• Users<br>• Troubleshooting Reports | `shell:msc-roles=powerUser` |
| Site Manager | • Dashboard—Sites<br>• Sites<br>• Tenants | `shell:msc-roles=siteManager` |
| Schema Manager | • Dashboard—Sites and Schema Health<br>• Schemas | `shell:msc-roles=schemaManager` |
| Schema Editor | • Dashboard—Sites and Schema Health<br>• Schemas | `shell:msc-roles=schemaEditor` |
| User Manager | • Users | `shell:msc-roles=userManager` |

### Admin User

In the initial configuration script, a default `admin` user account is configured and is the only user account available when the system starts. The initial password for the *admin* user is set by the system and you are prompted to change it after the first log in.

- The `admin` user's default password is `We1come2msc!`
- The `admin` user is assigned the Power User role.
- Use the `admin` user to creating other users and perform all other Day-0 configurations.
- The account status of the *admin* user cannot be set to **Inactive**.

### Read-Only Access

Each of the user roles above can be assigned in read-only mode. When read-only permissions are granted, the user can view any fabric objects available to that role just like before, but they cannot make any changes to those objects.

# Guidelines for User Management

- Users authentication and authorization can be local or external. For external authentication, you can use RADIUS, TACACS+, or LDAP servers. For more information about external authentication, see External Authentication in the *Administrative Operations* chapter.
- For both local and external authentication, the username supports a maximum length of 20 characters.
- For both local and external authentication, you must associate at least one role with every user. A user may be associated with more than one role. Associating a user to multiple roles offers a combination of objects that the user may access.
- Users must be associated with tenants before they can use a tenant or a schema.
- Starting with Release 2.1(2), users can be assigned roles in read-only mode. When read-only permissions are granted, the user can view any fabric objects available to that role just like before, but they cannot make any changes to those objects.

  If you configure any read-only user roles and then downgrade your Multi-Site Orchestrator to an earlier version, which does not support read-only permissions, those roles will be removed from all users. This also means that any user that has **only** the read-only roles will have no roles assigned to them and be deleted. A Power User or User Manager will need to recreate the users and re-assign them new read-write roles.

# Adding a User

This section describes how to create a Multi-Site Orchestrator user.

**Step 1** Log in to Cisco ACI Multi-Site Orchestrator.

**Step 2** From the main menu, select **Users**.

**Step 3** In the top right of the main window pane, click **Add User**.

**Step 4** In the **Add User** page, specify the following:

a) In the **Username** field, enter the new user's username.

b) In the **Password** and **Confirm Password** fields, provide the user's password.

The password must:

- Be at least 12 characters in length
- Contain at least one letter
- Contain at least one number
- Contain at least one special character apart from * and spaces

c) In the **First Name** field, enter the first name of the user.

d) In the **Last Name** field, enter the last name of the user.

e) In the **Email Address** field, enter the email address of the user.

f) (Optional) In the **Phone Number** field, enter the phone number of the user.

g) In the **Account Status** field, choose the account status.

You can set users to either `Active` or `Inactive` status. Only active users can log in to the Multi-Site Orchestrator.

**Step 5** In the **User Roles** list, assign one or more user roles for the new user you are adding.

You must associate at least one role with every user. A user may be associated with more than one role. Associating a user to multiple roles offers a combination of features that the user can access.

Each of the available roles can be configured in read-only mode. When a user is assigned a read-only role, they can view any fabric objects available to that role, but cannot make any changes to those objects

**Step 6** Click **Save**.

# Managing Users

This section describes how to edit or delete existing users.

**Step 1** Log in to Cisco ACI Multi-Site Orchestrator.

**Step 2** If you want to update your own password...

a) Click the **User** icon in the top right of the screen.
b) Select **Reset Password**

**Step 3** If you want to delete a user...

a) From the main menu, select **Users**.
b) Click the actions icon next to the user's name and select **Delete**.

You cannot delete the default `admin` user.

**Step 4** If you want to edit an existing user and their permissions...

a) From the main menu, select **Users**.
b) Click the actions icon next to the user's name and select **Edit**.

You cannot change the default `admin` user's name, account status, and roles.

The default `admin` user or a user associated with the **Power User** or **User Manager** roles can update the passwords for other users. On initial log in, the user will be prompted to update their own password.