# User Management



# User and Roles

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

- Power User—A power user can perform all the operations as an *admin* user.
- Site and Tenant Manager—A site and tenant manager can manage sites, tenants, and associations.
- Schema Manager—A schema manager can manage all schemas regardless of tenant associations.
- Schema Manager - Restricted —A restricted schema manager can manage schemas that contain at least one tenant to which the user is explicitly associated.
- User and Role Manager—A user and role manager can manage all the users, their roles, and passwords.

### Admin User

In the initial configuration script, the admin account is configured and the *admin* is the only user when the system starts. The initial password for the *admin* user is set by the system. You must change the *admin* password during the first log in.

- The *admin* user is assigned the role of a Power User.
- 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**.

# User Roles and Features

The following table lists the Cisco ACI Multi-Site features available with a user role.

***Table 1:***

| User Role | Multi-Site Features | Multi-Site av pair |
|---|---|---|
| Power User | • Dashboard<br>• Sites<br>• Schemas<br>• Tenants<br>• Users<br>• Troubleshooting Reports | shell:msc-roles=powerUser |
| Site and Tenant 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 Manager - Restricted | • Dashboard—Sites and Schema Health<br>• Schemas | shell:msc-roles=schemaEditor |
| User and Role Manager | • Users | shell:msc-roles=userManager |

# Guidelines and Limitations

- Users authentication and authorization can be local or external (using RADIUS or TACACS+). For more information about external authentication, see About External Authentication, on page 4.
- 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 features that the user may access.
- Users must be associated with tenants before they can use a tenant on a schema.

# Creating a User

**Procedure**

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

**Step 2** In the **Main menu**, click **Users**.

**Step 3** Click **ADD USER**.

**Step 4** In the **ADD USER** page, perform the following actions:

a) In the **USERNAME** field, enter the user name.

b) In the **PASSWORD** field, password.

The password must at least be six characters in length, and must contain at least one letter, one number, and a special character. Spaces and * are not allowed.

c) In the **CONFIRM PASSWORD** field, re-enter the password.

d) In the **FIRST NAME** field, enter the first name of the user.

e) In the **LAST NAME** field, enter the last name of the user.

f) In the **EMAIL ADDRESS** field, enter the email address of the user.

g) In the **PHONE NUMBER**field, enter the phone number of the user.

h) In the **ACCOUNT STATUS** field, choose the account status.

Only Active users are authenticated by Multi-Site.

**Step 5** Click the **User Role** button, to assign a role to a user.

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 may access. See User and Roles, on page 1 for more information.

**Step 6** Click **Submit**.

# Managing Users

**Procedure**

**Step 1** Cisco ACI Multi-Site.

**Step 2** In the **Main menu**, click **Users**.

**Step 3** Select a user and click **Actions** to perform the following actions.

a) From the **Actions** menu, choose **Delete** to delete a user.

You cannot delete an admin user.

b) From the **Actions** menu, choose **Edit** to edit a user.

An admin's user name, account status, and roles cannot be updated.

**Step 4** To update the password of a user, click **Welcome** *username*.

An admin user or a user associated with the user role **Power User** or **User and Role Manager** can update the password of an end user. On initial log in, an end user must update their password.

# Configuring External Authentication and Authorization

## About External Authentication

Starting in Cisco ACI Multi-Site Release 1.1(x), you can configure external authentication and authorization using RADIUS or TACACS+ for users.

As a Multi-Site administrator, you can configure:

- RADIUS or TACACS+ providers. It is recommended to set up at least 2 RADIUS or TACACS+ providers for redundancy.
- Login domains and associate them with providers.

  The default domain is the Local domain, for local authentication.
- Assign users to domains.

After you create domains, you can edit, deactivate, or delete them. You cannot delete the Local domain, but you can deactivate it.

Audit logs support external authentication and authorization.

## Guidelines for Configuring Users on RADIUS and TACACS+ Servers

To configure users for remote authentication, you must configure each user on the RADIUS and TACACS+ servers.

To configure a user, add the Cisco ACI Multi-Site attribute in the format `cisco-av-pair=shell:msc-roles=role1,role2`.

For example, `cisco-av-pair=shell:msc-roles=siteManager,schemaManager`.

Each role is one of the Multi-Site roles documented in User Roles and Features, on page 2.

## Creating a RADIUS or TACACS+ Provider

In Multi-Site, perform the following steps to add RADIUS or TACACS+ providers that perform user authentication and authorization.

### Procedure

**Step 1** Click **Admin** > **Providers**.

**Step 2** Click **ADD PROVIDER**.

**Step 3** Enter the host name or IP address of a RADIUS or TACACS+ server.

**Step 4** Enter a description of the provider.

**Step 5** Click **RADIUS** or **TACACS+**, as appropriate.

**Step 6** Enter the key in the **KEY** field and repeat it in the **CONFIRM KEY** field.

**Step 7** Optional. Click **Additional Settings** to change the default **PORT**, the authentication protocol (CHAP or PAP), **TIMEOUT (SEC)**, or **RETRIES (MAX 5 ALLOWED)**.

### What to do next

Repeat these steps to configure more providers.

## Creating a Login Domain

A login domain defines the authentication domain for a user. Login domains can be set to the Local, RADIUS, or TACACS+ authentication mechanisms. When accessing the system from the REST API or the GUI, Multi-Site enables the user to select the correct authentication domain.

For example, when using the REST API, the username is prefixed with a string so that the full login username looks as follows:

```
https://<host>:<port>/api/v1/auth/login
"username":"bob","password":"we1come!","domainId":"59d5b5978d0000d000909f65",
```

If accessing the system from the GUI, Multi-Site offers a drop-down list of domains for the user to select from. If no domain is specified, the Local domain is used to look up the username.

Perform the following steps in Multi-Site to configure a login domain.

### Procedure

**Step 1** Click **Admin** > **Domains**.

**Step 2** Click **ADD DOMAIN**.

**Step 3** Enter a domain name.

**Step 4** Enter a description of the domain.

**Step 5** In the **REALM** field, click **RADIUS** or **TACACS+** as appropriate.

**Step 6** Under the **Assign to providers** field, click a provider to assign the domain to one or more RADIUS or TACACS+ providers.

### What to do next

Repeat these steps to create more domains.

After they have been created, to edit, delete, or deactivate domains, click **Admin** > **Domains**. Right-click **Actions** on the domain, and choose **Edit**, **Delete**, or **Deactivate**.

You can't delete the Local domain, but you can deactivate it.

# Remote User Logon

When external authentication is enabled in Cisco ACI Multi-Site, you can log on to Multi-Site as follows:

### Procedure

**Step 1** Using a browser, enter the Multi-Site URL and enter your username.

**Step 2** Choose your assigned domain from the drop down list.

**Step 3** Enter the password you were assigned.

**Step 4** Click **Submit**.
If you are authorized and pass authentication, the Multi-Site GUI is displayed and you have privileges according to the roles assigned to you. The first time you log on, you must change your password.