Authentication

External Authentication

You can configure external user authentication and authorization using RADIUS, TACACS+, and LDAP servers.

As a Multi-Site Orchestrator administrator, you can:

- Add one or more external authentication providers.

  It is recommended to set up at least 2 authentication providers for redundancy.

- Create 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 External Authentication Servers

When configuring external authentication servers for Multi-Site Orchestrator user authentication:

- You must configure each user on the remote authentication servers.
- For both local and external authentication, the username supports a maximum length of 20 characters.
- For each user, you must add a custom attribute-value (AV) pair, specifying the use roles assigned to that user. The roles are documented in Users, Roles, and Permissions.

  When specifying the roles, use the following format:

  ```
  cisco-av-pair=shell:msc-roles=role1,role2
  ```

  For example:

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

- Starting with Release 2.1(2), each of the user roles 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.

  The AV pair string format differs when configuring a read-only or a combination of read-write and read-only roles for a specific user. In the following example, the read-write roles are separated from the read-only roles using the slash (/) character, while the individual roles are separated by the pipe (|) character:

  `cisco-av-pair=shell:msc-roles=writeRole1|writeRole2/readRole1|readRole2`

  The following example illustrates how to assign the Schema Manager and User Manager roles to a user, while still allowing them to see objects visible to the Site Manager users:

  `shell:msc-roles=schemaManager|userManager/siteManager`

  If you want to configure only either the read-only or read-write permissions for a user, you must still include the slash (/) character. The following examples show how to set just the read-write or read-only access to the objects available to Site Manager role.

  - Read-only: `shell:msc-roles=/siteManager`
  - Read-write: `shell:msc-roles=siteManager/`

Note While either the old (comma-separated) or the new (pipes and a slash) format is supported, you cannot mix them when configuring a single user. Mixed or incorrectly formatted AV strings are not parsed and the user roles are not configured.

- 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.
- For LDAP configurations, we recommend using **`CiscoAVPair`** as the attribute string. If, for any reason, you are unable to use an Object ID `1.3.6.1.4.1.9.22.1`, an additional Object IDs `1.3.6.1.4.1.9.2742.1-5` can also be used in the LDAP server.

Configuring Remote Authentication Server for Orchestrator Users

When configuring the remote authentication server for Multi-Site Orchestrator users, you must add a custom attribute-value (AV) pair, specifying the user roles assigned to them.

Detailed information about available user roles and their permissions is available in Users, Roles, and Permissions. But in short, the following user role strings are supported in AV pairs: `powerUser`, `siteManager`, `schemaManager`, `schemaEditor`, and `userManager`.

The AV pair string format differs when configuring a read-write role, read-only role, or a combination of read-write and read-only roles for a specific user. A typical string includes the domain, followed by the

read-write roles separated from the read-only roles using the slash (/) character; individual roles are separated by the pipe (|) character:

`shell:domains=<domain>/<writeRole1>|<writeRole2>/<readRole1>|<readRole2>`

Note In this release, only the `msoall` domain is supported and is required for consistency with the APIC AV pair format in order to support the single sign-on (SSO) feature. The `msoall` domain is the equivalent of the `all` domain on the APIC.

For example, the following string illustrates how to assign the Schema Manager and User Manager roles to a user, while still allowing them to see objects visible to the Site Manager users:

`shell:domains=msoall/schemaManager|userManager/siteManager`

If you want to use a single AV pair string for both MSO and APIC roles, you can combine them as follows:

`shell:domains=all/admin/,msoall/schemaManager|userManager/siteManager`

If you want to configure only the read-only or only read-write permissions for a user, you must still include the slash (/) character. The following examples show how to set just the read-write or read-only access to the objects available to Site Manager role:

- Read-only: `shell:domains=msoall//siteManager`
- Read-write: `shell:domains=msoall/siteManager/`

AV Pair String in Release 3.0(1) and Earlier

Starting with Release 3.0(2), the AV pair format was updated to match the format used by the Cisco APIC in order to support the single sing-on (SSO) feature.

Prior releases did not include the domain value but followed a similar format, for example:

`shell:msc-roles=writeRole1|writeRole2/readRole1|readRole2`

Note While Release 3.0(2) and later are backward compatible with the older AV pair formats, the SSO feature will not work until you update the AV pair string to the new format. If you ever downgrade to a release that does not support the new format, the users defined using the format will not be able to log in.

In addition, you cannot mix the old and the new format for the AV pairs them when configuring a single user. Mixed or incorrectly formatted AV strings are not parsed and the user roles are not configured.

Adding RADIUS or TACACS+ as Authentication Provider

This section describes how to add one or more RADIUS or TACACS+ servers as external authentication servers for authenticating Cisco ACI Multi-Site Orchestrator users.

Procedure

Step 1 Log in to your Cisco ACI Multi-Site Orchestrator as the `admin` user using the Local domain.

Step 2 From the left-hand navigation pane, select **Admin** > **Providers**.

Step 3 In the main window, click **ADD PROVIDER**.

Step 4 Enter the host name or IP address of the external authentication server.

Step 5 (Optional) Enter a description for the provider you are adding.

Step 6 Select **RADIUS** or **TACACS+** for the provider type you are adding.

Step 7 Enter the **KEY** and confirm it in the **CONFIRM KEY** field.

Step 8 (Optional). Configure additional settings.

a) Expand **Additional Settings** for more settings.

b) You can specify the port used to connect to the authentication server.

The default port is `1812` for **RADIUS** and `49` for **TACACS+**.

c) You can specify the protocol used.

You can choose between **PAP** or **CHAP** protocols.

d) You can specify the timeout and number of attempts for connecting to the authentication server.

Adding LDAP as Authentication Provider

This section describes how to add one or more LDAP servers as external authentication servers for Cisco ACI Multi-Site Orchestrator users.

Procedure

Step 1 Log in to your Cisco ACI Multi-Site Orchestrator as the `admin` user using the Local domain.

Step 2 From the left-hand navigation pane, select **Admin** > **Providers**.

Step 3 In the main window, click **Add Provider**.

Step 4 Enter the host name or IP address of the external authentication server.

Step 5 (Optional) Enter a description for the provider you are adding.

Step 6 Select **LDAP** for the provider type you are adding.

Step 7 Enter the **Base DN**, **Bind DN**, and the **Key** values for the LDAP server.

The Base DN and Bind DN depend on how your LDAP server is configured. You can get the Base DN and Bind DN values from the distinguished name of the user created on the LDAP server.

Base DN is the point from which the server will search for users. For example, `DC=mso,DC=local`.

Bind DN is the credentials used to authenticate against the server. For example, `CN=admin, CN=Users,DC=mso,DC=local`.

Bind DN comes with a key, which you can provide in the next field.

Step 8 (Optional) Enable SSL for LDAP communication.

a) Check the **Enable SSL** checkbox.

b) Select the certificate you want to use.

c) Select the validation level.

Permissive: Accept a certificate signed by any certificate authority (CA) and use it for encryption.

Restrictive: Verify the entire certificate chain before using it.

Step 9 (Optional). Configure additional settings.

a) Click **Additional Settings** to expand.

b) Specify the port used to connect to the LDAP server.

The default port for **LDAP** is `389`.

c) Specify the timeout and number of attempts for connecting to the authentication server.

d) Specify the filter used.

The filter value depends on the LDAP server configuration. The default LDAP filter is `(cn=username)`. However, if you're using a Microsoft LDAP server, set the filter to `(sAMAccountName={username})` instead.

e) Specify the authentication type.

The authentication type can be:

- **Cisco-AVPair** – uses an attribute-value (AV) pair to configure authorization based on individual user's role. When using this method, set the **Attribute** field to `ciscoAVPair`.

  You must also configure each user individually in your LDAP server using the AV pair string in the following format:

  - Release 2.1(2) and later:

    `cisco-av-pair=shell:msc-roles=writeRole1|writeRole2/readRole1|readRole2`

  - Release 2.1(1) and earlier:

    `cisco-av-pair=shell:msc-roles=role1,role2`

  For additional information, see Guidelines for Configuring External Authentication Servers, on page 1.

- **LDAP Group Map Rules** - use an LDAP server group to configure authorization based on the users' group membership. When using this method, set the **Attribute** field to `memberOf`, then click **+LDAP Group Map Rules** to specify the group membership.

  In the **New Group Map Rule**, specify the group DN (for example, `CN=group1,OU=msc-ou,DC=msc,DC=local`) and the user roles to be assigned to that group. You can add multiple roles for the same group map rule. Detailed descriptions of each user role are available in Users, Roles, and Permissions.

Creating Login Domains

A login domain defines the authentication domain for a user. Login domains can be set to the Local, RADIUS, TACACS+, or LDAP authentication mechanisms.

When you are logging in to the Cisco ACI Multi-Site Orchestrator using the GUI, the login screen 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.

When you are logging in to the Cisco ACI Multi-Site Orchestrator using the REST API, the login domain is provided along with the login information in the `POST` message, for example:

```
{
    "username":"bob",
```

```
    "password":"We1come2msc!",
    "domainId":"59d5b5978d0000d000909f65"
}
```

To create a login domain using the Cisco ACI Multi-Site Orchestrator GUI:

Before you begin

You must have added one or more authentication providers as described in Adding RADIUS or TACACS+ as Authentication Provider, on page 3 or Adding LDAP as Authentication Provider, on page 4.

Procedure

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

Step 2 Navigate to **Admin** > **Authentication**.

Step 3 In the main window, select the **Login Domains** tab.

Step 4 Click **Add Login Domain**.

Step 5 Enter the domain's name.

Step 6 (Optional) Enter a description for the domain.

Step 7 In the **Realm** selection, specify the authentication provider.

You must have an external authentication provider added before creating a login domain.

Step 8 Assign providers to the login domain.

You can choose multiple providers for the domain to enable redundancy in case one of the providers experiences an issue.

If you select more than one provider, ensure that each provider has a unique **Priority** value. When multiple providers are available, they are used in order of priority when authenticating users.

What to do next

After you create one or more login domains, you can edit, delete, or deactivate them as described in Editing, Deleting, or Deactivating Login Domains, on page 6.

Editing, Deleting, or Deactivating Login Domains

After you have created one or more login domains, you can use the instruction described in this section to edit, delete, or deactivate them. You cannot delete the Local domain, but you can deactivate it.

Before you begin

You must have created one or more Login domains as described in Creating Login Domains, on page 5.

Procedure

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

Step 2 From the left-hand navigation pane, select **Admin** > **Login Domains**.

Step 3 Click the **...** menu next to the login domain you want to edit.

You can choose to **Edit** the domain information, **Deactivate** the domain so that it cannot be used, or **Set as default** so it is automatically selected when logging in using GUI.

Remote User Logon

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

Procedure

Step 1 Using a browser, navigate to the Multi-Site URL.

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

Step 3 Enter your username and password.

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

Single Sign-On (SSO) Across APIC Sites

Beginning with Release 3.0(2), Cisco ACI Multi-Site supports single sign-on (SSO) capability between the Multi-Site Orchestrator and each site's Cisco APIC.

When you configure remote authentication for the MSO and APIC users, you can cross-launch into individual sites' APIC GUI directly from the MSO GUI without being prompted to log in at the APIC level.

SSO Guidelines and Limitations

When using the single sign-on feature, the following restriction apply:

- Your Multi-Site Orchestrator must be running Release 3.0(2) or later.
- Your Multi-Site Orchestrator must be deployed in Cisco Application Services Engine.

  Older Docker deployments using in vCenter or OVA do not support SSO.
- The APIC sites must be running Cisco APIC, Release 5.0(2) or later.

  If you cross-launch into an APIC running an earlier version, you will be prompted to log in.
- Your Multi-Site Orchestrator must be configured for remote user authentication.

  Remote authentication is described in External Authentication, on page 1.

Launching APIC GUI

This section describes how to cross-launch into an APIC GUI from your Multi-Site Orchestrator utilizing single sign-on.

Before you begin

You must have:

- Configured Cisco Multi-Site Orchestrator and Cisco APIC users and roles in your authentication provider server, as described in External Authentication, on page 1.

  In your AV pair string, you must include roles for both MSO and APIC.

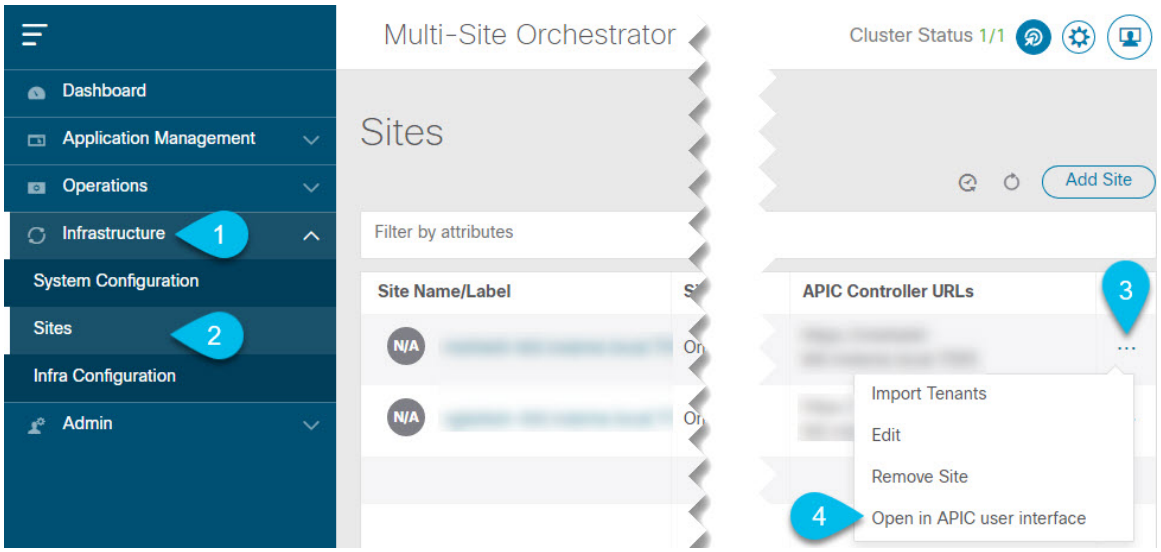
- Added the remote authentication provider to your Multi-Site Orchestrator, as described in External Authentication, on page 1.

Procedure

Step 1 Log in to your Cisco Multi-Site Orchestrator GUI as a remote user.

Single sign-on is not supported for local MSO users.

Step 2 Launch APIC GUI from the **Sites** page.



a) Navigate to **Infrastructure** > **Sites**.

b) Click the **Actions** menu next to the site you want to launch.

You must select a site running APIC Release 5.0(2) or later.

c) Click **Open in APIC user interface**.

A new tab will open and you will be automatically logged in to the APIC GUI using the same user as you used to log in to the MSO.

Step 3 Alternatively, launch APIC GUI from a **Schema** page.

a) Navigate to **Application Management** > **Schemas**.
b) Select a schema.
c) In the left sidebar, select one of the sites in the schema.
d) Click the **Actions** menu next to the site you want to launch.

   You must select a site running APIC Release 5.0(2) or later.

e) Click **Open APIC**.

A new tab will open and you will be automatically logged in to the APIC GUI using the same user as you used to log in to the MSO.

Once the APIC GUI is loaded via cross-launch from Multi-Site Orchestrator, logging out of MSO will not logout from the APIC.