Administrative Operations

Viewing Site Status

You can use the Multi-Site Orchestrator GUI's **Dashboard** view to see each site's status, number and types of faults, and schema health.

In the **SITE STATUS** panel, the following fields are displayed on the dashboard:

- **SITE NAME**
- **CRITICAL** Alarms
- **MAJOR** Alarms
- **MINOR** Alarms
- **WARNING** Alarms

Viewing Schema Health

Using the schema health functionality in the Multi-Site Orchestrator GUI dashboard, you can view the health of the individual schemas that are associated with different sites. In the **Schema Details** window, you can view the policy types that are associated with each site.

You can perform the following tasks using the **SCHEMA HEALTH** chart in the GUI:

- View the aggregated health score of the entire Multi-Site fabric and all APICs
- View the aggregated fault counts and the fault types for each schema in the **Schema Details** window

- View the health of the inter-site schemas
- View the health of the multi-sites nodes and their components
- View the health of the connected APICs and ACI clusters

You can view the schema health in the GUI using the following different formats:

- Hovering on an Individual Cell: Each cell in the **SCHEMA HEALTH** chart represents the health of the schema. If the cell is color coded as Green and if you hover on the cell, it displays the application health score of the schema.
- Clicking in the Cell: If you click the individual cell in the table, it provides the additional schema details for the template and the faults with the associated with each policy type, for example, ANP, EPG, Contract, VRF, and BD.

  The faults and warnings are displayed in the columns to the right side of each policy. This functionality is used to collect the details and get more information on the issues causing low health.
- Viewing the Health Score Slider: The health score slider at the top of the page provides capabilities to filter the schemas by the minimum or maximum health score. A range in the slider can be adjusted to view the schemas that match the heath score range. For example, you can adjust the health score to display the schemas matching the health score between 0 to 30 range.
- Using the Search Functionality: The search functionality in the schema health view provides the capabilities to find a schema or a policy based on the keywords that are typed in the search area. When the keywords are typed in the search area, only schemas that contain the keywords are displayed. The results are based on the matching keywords as part of the schema name, template name, or any of the contained policies within that schema.

Viewing Faults for Individual Sites

This section describes how to display the faults for the individual sites using the Multi-Site GUI.

Step 1 Log in to Multi-Site Orchestrator GUI.

Step 2 In the **Main Menu**, click **Sites**.

Step 3 In the **Sites list** page, click **CONFIGURE INFRA**.

Step 4 In the **Fabric Connectivity Infra** page, click the appropriate site in the **Master List**. For example, click site1.

The site details with the associated pods and the spines are displayed in the GUI.

The total number of the faults and the fault types, for example, Critical, Major, Minor, and Warning faults are displayed at the top of the panel. Clicking on each fault type displays the fault details with the individual codes and their explanations.

System Logs

You can view the Multi-Site Orchestrator logs by selecting **Admin** > **Logs** from the main navigation menu.

From the **Logs** page, you can click the **Most Recent** field to select a specific time period for which you want to see the logs. For example, when you select the range from November 14, 2017 to November 17, 2017 and click **Apply**, the audit log details for this time period are displayed on the **Audit Logs** page.

You can also click the **Filter** icon to filter the log details using the following criteria:

- **User**: Select this option to filter the audit logs by the user type, then click **Apply** to apply the filter.
- **Type**: Select this option to filter the audit logs by the policy types, for example, site, user, template, application profile, bridge domain, EPG, external EPG, filter, VRF, BGP config, contract, OSPF policy, pod, node, port, domain, provider, RADIUS, TACACS+ and click **Apply**.
- **Action**: Select this option to filter the audit logs by an action. The available actions are Created, Updated, Deleted, Added, Removed, Associated, Disassociated, Deployed, Undeployed, Downloaded, Uploaded, Restored, Logged in, Logged Out, Login Failed. Select an action and click **Apply** to filter the log details according to the action.

Generating Troubleshooting Report and Logs

This section describes how to generate a troubleshooting report and infrastructure logs file for all the schemas, sites, tenants, and users that are managed by Cisco ACI Multi-Site Orchestrator.

Step 1 Log in to your Multi-Site Orchestrator GUI.

Step 2 In the top right corner, click the **Options** icon and select **System Logs**.

Step 3 Check the logs you want to download.

Check the **Database Backup** to download a backup of the Orchestrator database.

Check the **Server Logs** to download the Orchestrator logs.

Step 4 Click **DOWNLOAD**.

An archive of the selected items will be downloaded to your system. The report contains the following information:

- All schemas in JSON format
- All sites definitions in JSON format
- All tenants definitions in JSON format
- All users definitions in JSON format
- All logs of the containers in the `infra_logs.txt` file

Enabling Log Streaming to an External Log Analyzer

Cisco ACI Multi-Site Orchestrator allows you to send the Orchestrator logs to an external log analyzer tool in real time. By streaming any events as they are generated, you can use the additional tools to quickly parse, view, and respond to important events without a delay.

This section describes how to enable Multi-SiteOrchestrator to stream its logs to an external analyzer tool, such as Splunk.

Before you begin

- Set up and configure the log analyzer service provider.

  For detailed instructions on how to configure an external log analyzer, consult its documentation.

  Note This release of Cisco ACI Multi-Site Orchestrator only supports Splunk as the service provider.

- Obtain an authentication token for the service provider.

  Obtaining an authentication token for Splunk service is detailed in the Splunk documentation, but in short, you can get the authentication token by logging into the Splunk server, selecting **Settings** > **Data Inputs** > **HTTP Event Collector**, and clicking **New Token**.

Step 1 Log in to your Multi-Site Orchestrator GUI.

Step 2 In the top right corner, click the **Options** icon and select **System Logs**.

Step 3 In the **System Logs** window that opens, enable the **EXTERNAL STREAMING** knob.

Step 4 Select which logs you want to stream.

You can select either all logs or audit logs only.

Step 5 From the **SELECT SERVICE** dropdown menu, select the log analyzer service.

This release of Cisco ACI Multi-Site Orchestrator supports only Splunk as the service provider.

Step 6 Choose the **PROTOCOL** for the traffic.

Select **UNSECURE** for HTTP or **SECURE** for HTTPS.

Step 7 Provide the service's information.

In the **HOST** field, enter the host's IP address.

In the **PORT** field, enter the host's port number.

In the **TOKEN** field, enter the authentication token you obtain from the service provider.

Step 8 For each Multi-Site Orchestrator node, provide the node's root password.

Note This is the `root` user password of each Orchestrator node, not the password you use to log in to the Orchestrator GUI.

Step 9 Click **OK** to save the changes.

Configuration Backup and Restore

You can create backups of your Multi-Site Orchestrator configuration that can facilitate in recovery from Orchestrator failures or cluster restarts. We recommend creating a backup of the configuration before every

upgrade or downgrade of your Orchestrator and after every configuration change or deployment. We also recommend exporting the backups to an external storage outside of the Orchestrator nodes' VMs.

Note Restoring a backup action restores the database on the Multi-Site Orchestrator, but it does not make any changes to the APIC databases on each site. Therefore, after you restore the Orchestrator database, you must also re-deploy any existing schemas to avoid potentially mismatching policies between the Orchestrator and APIC sites. For information on specific configuration mismatch scenarios and backup restore procedures related to each one, see Backup and Restore Guidelines, on page 6

Storing the Backups on NFS Shares

Cisco ACI Multi-Site is deployed as a 3-node cluster. When you first deploy the cluster, there are no network shares (NFS) mounted on the nodes and the backups are saved directly to each node's local disk in the `/opt/cisco/msc/backups/` directory.

While the backups are available on any one node and can be viewed using the Orchestrator GUI, we recommend mounting a network file system share to store the backups outside the Orchestrator VMs, as described in Adding an NFS Share to Store Backups, on page 5.

Adding an NFS Share to Store Backups

This section describes how to add an NFS share to the Multi-Site Orchestrator VMs to store configuration backups.

Before you begin

Step 1 Log in directly to your Multi-Site Orchestrator node's VM as the `root` user.

Step 2 Mount the NFS share.

The following command mounts the shared NFS directory to the default Orchestrator backups folder so all future backups are automatically stored to an external storage outside the Orchestrator VMs.

Note If you have any existing backups in this default directory that you want to save, you must manually move them to a different location before mounting the NFS share. After the share is mounted, any existing files in the mount directory will be hidden from view.

```
# mount <nfs-server-ip>:/<nfs-share-path> /opt/cisco/msc/backups/
```

Step 3 Repeat steps 1 through 2 on each Orchestrator VM.

Because each Orchestrator node can create and store its own backup files, you must mount the same NFS share on all nodes.

Step 4 Update the Docker backup services.

You must run the following Docker update command for the newly mounted file system to be usable by the Orchestrator services. However, since the command updates the services across the cluster, you only need to do this once after mounting the shares on each node.

```
# docker service update msc_backupservice --force
```

What to do next

If at any point you want to remove the NFS share and go back to storing the backups locally on each VM, simply unmount the directory on each node and run the `docker service update msc_backupservice --force` command again.

Backup and Restore Guidelines

When saving and restoring configuration backups, the following guidelines apply:

- When saving a backup, the configuration is saved in the same state in which it was deployed. When restoring a backup, any policies that were deployed will show as "deployed", while any policies that were not deployed will remain in the "undeployed" state.
- Restoring a backup action restores the database on the Multi-Site Orchestrator, but it does not make any changes to the APIC databases on each site. As such, certain precautions and steps must be taken when restoring a previous configuration to avoid potentially mismatching policies between the Orchestrator and the APIC sites, as described below.

No Configuration Changes Since Backup

If there have been no policy changes between when the backup was created and when it is being restored, no additional considerations are required and you can simply restore the configuration as described in Restoring Backups, on page 7.

New Objects or Policies Configured Since Backup

If additional policy objects have been added between the time when the configuration backup was created and the time it is being restored, we recommend performing the following actions:

- Before restoring the configuration, undeploy any policies currently deployed to the APIC sites. This action will clean up all policy objects in each APIC site, which will avoid any potential stale objects after the configuration is restored from backup.

  Note Keep in mind, undeploying the configuration policies will cause a disruption in traffic or services defined by the policies.

- Restore the backup, as described in Restoring Backups, on page 7.
- Re-deploy all the required policies to the APIC sites. This action will deploy fresh configuration to every APIC site.

  However, keep in mind the following possible scenarios after configuration is restored from backup:

  - If the configuration backup you restored was saved before it was deployed to the APIC sites, it will be restored in the "undeployed" state and you can simply deploy it to the APIC sites as necessary.

- If the configuration backup you restored was saved when the configuration was already deployed, it will be restored in the "deployed" state, even though none of the policies will exist in the APIC sites yet. In this case, in order for the configuration to be properly pushed to each site, you will need to make a minor configuration change and re-deploy it to sync the Orchestrator's configuration with the APIC sites.

Objects or Policies Removed or Modified Since Backup

If no additional objects have been added between the time when the configuration backup was created and the time it is being restore, but some objects have been modified or deleted, we recommend performing the following actions:

- Restore the backup, as described in Restoring Backups, on page 7.
- If the configuration backup you restored was saved before it was deployed to the APIC sites, it will be restored in the "undeployed" state and you can simply deploy it to the APIC sites as necessary.

  However, if the configuration backup you restored was saved when the configuration was already deployed, it will be restored in the "deployed" state. In this case you will need to make a minor configuration change and re-deploy it to sync the Orchestrator's configuration, along with any deleted or modified objects, with the APIC sites.

Creating Backups

This section describes how to create a new backup of your Multi-Site Orchestrator configuration.

Before you begin

Step 1 Log in to your Multi-Site Orchestrator GUI.

Step 2 From the left navigation menu, select **Admin** > **Backups**.

Step 3 In the main window, click **New Backup**.

Step 4 In the **New Backup** window that opens, provide the backup details.

In the **Name** field, enter the name for the backup. The name can contain up to 10 alphanumeric characters and no spaces or underscores.

In the **Notes** field, enter any additional information to describe the backup.

Step 5 Click **SAVE** to create the backup.

Restoring Backups

This section describes how to restore a Multi-Site Orchestrator configuration to a previous state.

Before you begin

Restoring a backup action restores the database on the Multi-Site Orchestrator, but it does not make any changes to the APIC databases on each site. Therefore, after you restore the Orchestrator database, you must

also re-deploy any existing schemas to avoid potentially mismatching policies between the Orchestrator and APIC sites.

For information on specific configuration mismatch scenarios and recommended restore procedures related to each one, see Backup and Restore Guidelines, on page 6.

Step 1 Log in to your Multi-Site Orchestrator GUI.

Step 2 If necessary, undeploy existing policies.

We recommend you perform this step if new objects or policies were added to the configuration between when the backup was created and current configuration. Additional context is available in Backup and Restore Guidelines, on page 6.

Step 3 From the left navigation menu, select **Admin** > **Backups**.

Step 4 In the main window, click the **...** actions menu next to the backup you want to restore and select **Rollback to this backup**.

If the version of the selected backup is different from the running Multi-Site version, the rollback could cause a removal of the features that are not present in the backup version.

Step 5 Click **Yes** to confirm that you want to restore the backup you selected.

If you click **Yes**, the system terminates the current session and the user is logged out.

Step 6 If necessary, redeploy the configuration.

We recommend you perform this step to sync the restored configuration with the APIC sites. Additional context is available in Backup and Restore Guidelines, on page 6.

Downloading Backups

This section describes how to download you backup from the Multi-Site Orchestrator.

Before you begin

Step 1 Log in to your Multi-Site Orchestrator GUI.

Step 2 From the left navigation menu, select **Admin** > **Backups**.

Step 3 In the main window, click the **...** actions menu next to the backup you want to download and select **Download**.

This will download the backup file in `.tar.gz` format to your system. You can then extract the file to view its contents.

Importing Backups

This section describes how to import an existing backup into your Multi-Site Orchestrator.

Before you begin

Step 1 Log in to your Multi-Site Orchestrator GUI.

Step 2 From the left navigation menu, select **Admin** > **Backups**.

Step 3 In the main window, click **Import**.

Step 4 In the **Import from file** window that opens, click **Select File** and choose the backup file you want to import.

Importing a backup will add it to the list of the backups displayed the **Backups** page.

Configuring Custom SSL Certificates

Cisco ACI Multi-Site Orchestrator OVA contains a self-signed SSL certificate that is stored in `/data/msc/secrets` directory on each node during the Orchestrator installation. By default, the Orchestrator GUI uses this certificate for its HTTPS connections.

While you could previously update these certificates by logging directly into an Orchestrator node server and changing its web server (`nginx`) configuration, starting with Cisco ACI Multi-Site Orchestrator Release 2.1(1), you can use the GUI to easily add or update custom certificates to be used for the Orchestrator's GUI connection.

When adding custom certificates, you can use one of the following two options:

- **Self-Signed Certificate** provide you with the ability to create your own public and private keys to be used by the Orchestrator's GUI.
- **CA-Issued Certificate** allows you to use a certificate provided by an existing Certificate Authority (CA) along with its keys.

You can add multiple CAs and Keyrings containing the public/private key combinations in the GUI, however only a single keyring can be active at any given time and used to secure the communication between the Orchestrator GUI and your browser.

Adding Custom Certificate Authority

You can add a custom Certificate Authority (CA) to be used for verifying the public key provided by the Orchestrator for HTTPS traffic encryption.

This section describes how to add and configure a custom CA in Multi-SiteOrchestrator GUI. Configuring keyrings and keys is described in the next section.

Step 1 Log in to your Multi-Site Orchestrator GUI.

Step 2 From the left navigation menu, select **Admin** > **Security**.

Step 3 In the main window, select the **Certificate Authority** tab and click **Add Certificate Authority**.

Step 4 In the **Add Certificate Authority** window that opens, provide the CA details.

In the **Name** field, enter the CA name.

In the **Description** field, enter the CA description.

In the **Certificate Chain** field, enter the CA's certificate chain. You must include both, intermediate and root, certificates. The intermediate certificate must be entered first, followed by the root certificate.

Step 5 Click **SAVE** to save the changes.

Adding Custom Keyring

You can add a custom keyring containing a public and prviate encryption keys to be used for Orchestrator GUI HTTPS traffic encryption.

This section describes how to add a custom keyring. For instructions on adding a Certificate Authority (CA) that can be used to verify the public key in this keyring, see the previous section.

Step 1 Log in to your Multi-Site Orchestrator GUI.

Step 2 From the left-hand navigation menu, select **Admin** > **Security**.

Step 3 In the main window, select the **Key Rings** tab and click **ADD KEY RING**.

Step 4 In the **Create Key Ring** window that opens, provide the key ring details.

From the **SELECT CERTIFICATE AUTHORITY** dropdown menu, select the certificate authority that will contain the key ring.

In the **NAME** field, enter the key ring name.

In the **KEY RING DESCRIPTION** field, enter the key ring description.

In the **PUBLIC KEY** field, enter the ring's public key.

In the **PRIVATE KEY** field, enter the ring's private key

Step 5 Click **SAVE** to save the changes.

Activating Custom Keyring

After you add a keyring, as described in previous section, you need to activate it as the default keyring.

Step 1 Log in to your Multi-Site Orchestrator GUI.

Step 2 From the left-hand navigation menu, select **Admin** > **Security**.

Step 3 In the main window, select the **Key Rings** tab.

Step 4 In the main window, click the **...** icon next to the keyring you want to activate and choose **Make Keyring Active**.

Step 5 Click **ACTIVATE** to activate the keyring.

Activating a key will log you out of the Multi-Site Orchestrator GUI. When the login page is loaded, it will use the new certificate and key.

Custom Certificates Troubleshooting

The following sections describe how to resolve common issues when using custom SSL certificates with Multi-Site Orchestrator.

Unable to Load the Orchestrator GUI

If you are unable to load the Orchestrator GUI page after installing and activating a custom certificate, it is possible that the certificates were not copied correctly to each Orchestrator node. You can resolve this issue by recovering the default certificates and then repeating the new certificate installation procedure again.

To recover the default Orchestrator certificates:

1. Log in to each Orchestrator node directly.
2. Change into the certificates directory:

   ```
   # cd /data/msc/secrets
   ```

3. Replace the msc.key and msc.cert files with msc.key_backup and msc.cert_backup files respectively.

   ```
   # cp msc.key_backup msc.key
   # cp msc.cert_backup msc.cert
   ```

4. Restart the Orchestrator GUI service

   ```
   # docker service update msc_ui --force
   ```

5. Re-install and activate the new certificates as described in previous sections.

Adding a New Orchestrator Node to the Cluster

If you add a new node to you Multi-Site Orchestrator cluster:

1. Log in to the Orchestrator GUI.
2. Re-activate the key you are using as described in previous sections.

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.

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.

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

Starting with Release 2.1(1) you can add one or more LDAP servers as external authentication servers for authenticating Cisco ACI Multi-Site Orchestrator users.

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** and **BIND DN** values for the LDAP server..

Step 8 Enter the **KEY** and confirm it in the **CONFIRM KEY** field.

Step 9 (Optional). Configure additional settings.

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

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

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

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

d) You can specify the filter used.

The default LDAP filter is `(cn=$userid)`.

For Microsoft, the LDAP filter should be `(sAMAccountName=$userid)`.

e) You can specify the authentication type.

The authentication type can be:

- **CISCO-AVPAIR** – for authorization based on individual user's attribute.
- **LDAP GROUP MAP RULES** - for authorization based on the user's group membership.

f) You can specify the attribute value and one or more user groups.

If **CISCO-AVPAIR** is selected for authentication type, the attribute value is an attribute assigned to individual users, for example `ciscoAVPair`.

If **LDAP GROUP MAP RULES** is selected for authentication type, the attribute value is group membership, for example `memberOf` and a list of groups.

g) If you select **LDAP GROUP MAP RULES** for authentication type, you must also provide one or more groups to which the LDAP user belongs.

In the **LDAP GROUP MAP RULES** list, click the **+** sign.

In the **Add New Group Map Rule** window that opens, provide the group details, such as **Name**, **Description**, **Group DN**, and **Roles**. You can add multiple roles for the same group map rule.

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 13 or Adding LDAP as Authentication Provider, on page 13.

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 In the main window, click **ADD LOGIN DOMAIN**.

Step 4 Enter the domain's name.

Step 5 (Optional) Enter a description for the domain.

Step 6 Select **REALM** type to specify the authentication provider.

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

Step 7 Assign the login domain to one or more providers.

Mark the checkbox next to one or more providers' names to assign the domain.

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 15.

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 14.

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:

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.

Managing Scope of Schema and Template Deployment

Cisco ACI Multi-Site schemas and templates contain the policies and scope of what you intend to deploy to each site.

In order to ensure correct policy deployment and operation, we recommend that you add each schema and template to the sites incrementally and confirm the desired operation and performance.