



Cisco Multi-Site Configuration Guide for DCNM Fabrics, Release 3.2(x)

First Published: 2020-11-25

Last Modified: 2021-04-05

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS REFERENCED IN THIS DOCUMENTATION ARE SUBJECT TO CHANGE WITHOUT NOTICE. EXCEPT AS MAY OTHERWISE BE AGREED BY CISCO IN WRITING, ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS DOCUMENTATION ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED.

The Cisco End User License Agreement and any supplemental license terms govern your use of any Cisco software, including this product documentation, and are located at: <http://www.cisco.com/go/softwareterms>. Cisco product warranty information is available at <http://www.cisco.com/go/warranty>. US Federal Communications Commission Notices are found here <http://www.cisco.com/c/en/us/products/us-fcc-notice.html>.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any products and features described herein as in development or available at a future date remain in varying stages of development and will be offered on a when-and if-available basis. Any such product or feature roadmaps are subject to change at the sole discretion of Cisco and Cisco will have no liability for delay in the delivery or failure to deliver any products or feature roadmap items that may be set forth in this document.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

The documentation set for this product strives to use bias-free language. For the purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com go trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2020 Cisco Systems, Inc. All rights reserved.



CONTENTS

| | | |
|------------------|------------------------------------|----------|
| CHAPTER 1 | New and Changed Information | 1 |
| | New and Changed Information | 1 |

| | | |
|------------------|---------------------------------------|----------|
| CHAPTER 2 | GUI Overview | 3 |
| | Overview | 3 |
| | Dashboard | 4 |
| | Application Management > Tenants Page | 4 |
| | Application Management > Schemas Page | 6 |
| | Infrastructure > Sites Page | 6 |

| | | |
|------------------|------------------------------------|----------|
| CHAPTER 3 | Adding and Deleting Sites | 9 |
| | Adding Cisco DCNM Sites | 9 |
| | Removing Sites | 12 |
| | Cross Launch to Fabric Controllers | 13 |

| | | |
|------------------|---|-----------|
| CHAPTER 4 | Configuring Infra for Cisco DCNM Sites | 15 |
| | Prerequisites and Guidelines | 15 |
| | Configuring Infra: General Settings | 15 |
| | Refreshing Site Connectivity Information | 16 |
| | Configuring Infra: DCNM Site Settings | 17 |
| | Deploying Infra Configuration | 18 |

| | | |
|------------------|----------------------------------|-----------|
| CHAPTER 5 | Fabric Management | 21 |
| | Tenants | 21 |
| | Schemas and Templates | 22 |
| | Concurrent Configuration Updates | 23 |

- Creating Schemas and Templates 25
 - Importing Schema Elements From DCNM Sites 26
 - Creating VRFs 27
 - Creating Networks 28
- Deploying Templates 31
- Schema Overview and Deployment Visualizer 31

PART I **Operations 35**

CHAPTER 6 **System Configuration 37**

- System Configuration Settings 37
- System Alias and Banner 37
- Login Attempts and Lockout Time 38

CHAPTER 7 **Audit Logs 39**

- Audit Logs 39

CHAPTER 8 **Backup and Restore 41**

- Configuration Backup and Restore 41
- Backup and Restore Guidelines 41
- Remote Backups 42
 - Configuring a Remote Location for Backups 43
 - Moving Existing Backups to a Remote Location 44
- Creating Backups 44
- Restoring Backups 45
- Downloading Backups 46
- Importing Backups 46

CHAPTER 9 **Tech Support 47**

- Tech Support and System Logs 47
- Downloading System Logs 47
- Streaming System Logs to External Analyzer 48

CHAPTER 10 **Upgrading or Downgrading MSO Application 53**

| | |
|---|----|
| Overview | 53 |
| Prerequisites and Guidelines | 53 |
| Upgrading MSO Application Using Cisco App Store | 54 |
| Upgrading MSO Application Manually | 56 |
| Downgrading MSO Application | 58 |

PART II**Features and Use Cases 61**

CHAPTER 11**Brownfield Import of VRFs and Networks 63**

| | |
|---|----|
| Overview | 63 |
| Prerequisites | 64 |
| Create Schema and Templates for Importing Configuration | 65 |
| Importing Schema Elements From DCNM Sites | 66 |
| Deploying Template and Making Changes | 68 |



CHAPTER 1

New and Changed Information

- [New and Changed Information](#), on page 1

New and Changed Information

The following table provides an overview of the significant changes to the organization and features in this guide from the release the guide was first published to the current release. The table does not provide an exhaustive list of all changes made to the guide.

Table 1: Latest Updates

| Release | New Feature or Update | Where Documented |
|---------|---------------------------------|------------------|
| 3.2(1) | First release of this document. | -- |



CHAPTER 2

GUI Overview

- [Overview](#), on page 3
- [Dashboard](#), on page 4
- [Application Management > Tenants Page](#), on page 4
- [Application Management > Schemas Page](#), on page 6
- [Infrastructure > Sites Page](#), on page 6

Overview

The Multi-Site Orchestrator (MSO) GUI is a browser-based graphical interface for configuring and monitoring your Cisco APIC, Cloud APIC, and DCNM deployments.

The GUI is arranged according to function. For example, the **Dashboard** page contains an overview of your fabrics and their health, the **Sites** page provides information on each site and allows you to add sites, the **Schemas** page allows you to create and configure schemas, and so on. The functionality of each MSO GUI page is described in the following sections.

The top of each page shows the controller status indicating how many controllers are operational, the **Get Started** menu icon, the **Settings** icon, and the **User** icon.

The **Get Started** menu provides easy access to a number of common tasks you may want to perform, such as adding sites or schemas, configuring specific policies, or performing administrative tasks.

The **Settings** icon allows you to access overview information about your Multi-Site Orchestrator, such as the currently running version, what's new in the current release, API documentation, and system status:

- The **About MSO** link displays information about the version of the Multi-Site Orchestrator currently installed.
- The **What's New in This Release** link displays a short summary of the new features in your release, as well as links to the rest of the Multi-Site Orchestrator documentation.
- The **API Docs** link gives you access to the set of Swagger API object and method references. Using the Swagger API is described in more detail in the *Cisco Multi-Site REST API Configuration Guide*.
- The **System Status** link provides you with the status and health of all running services that are used by the MSO.

The **User** icon allows you to view information about the currently logged in user, preferences and bookmarks. It also allows you to log out of the Orchestrator GUI.



Note Starting with Release 3.2(1), user management has moved to the common user and authentication management in the Nexus Dashboard where your MSO application is running.

- The **Preferences** link allows you to change a few GUI options.
- The **Bookmarks** link opens the list of all the bookmarked schemas you save while using the Orchestrator. You can bookmark a schema by clicking the bookmark icon in the top right corner of the screen while viewing or editing the schema.

When working with fabric objects, a **Display Name** field is used throughout the Orchestrator's GUI whenever the objects are shown. You can specify a display name when creating the objects, however due to object naming requirements on the site controllers, any invalid characters are removed and the resulting **Internal Name** is used when pushing the objects to sites. The **Internal Name** that will be used when creating the tenant is typically displayed below the **Display Name** text box.

Dashboard

The Multi-Site Orchestrator dashboard displays the list of all sites in addition to their current functionality and health.

The **Dashboard** has the following functional areas:

- **Site Name:** Displays the name, type, and release version for each site.
- **Fault Severity:** The fault status columns list the number of faults per site according to their severity:
 - **Critical** (red)
 - **Major** (orange)
 - **Minor** (yellow)
 - **Warning** (green)

Application Management > Tenants Page

The Multi-Site **Tenants** page lists all of the tenants that comprise your implementation.

The table on the **Tenants** page displays the following:

- **Tenant Name**
- **Assigned to Sites**
- **Assigned to Users**
- **Assigned to Schemas**
- **Actions**

The features and functionality on this page include the following:

- **Name:** click a tenant name to access the **Tenant Details** settings page. On the **Tenant Details** page you can edit or update the following sections:
 - **General Settings:** change the Display Name and Description as required.
 - **Associated Sites:** view the sites associated with the subject tenant.
 - **Associated Users:** view the users associated with the subject tenant - you can associate a user with the subject tenant by checking the empty box next to the user name.
- **Associated Schemas:** click the **Associated Schema** listing to view the schemas associated with the subject tenant.
- **Actions:** click the **Actions** listing to edit the subject tenant's details sites or to create a new network mapping.



Note You can delete the Tenant object by selecting **Delete** on the **Actions** drop down menu.

- **Add Tenant:** click **Add Tenant** button to add an existing tenant to your implementation. On the proceeding Tenant Details page, you can add the tenant name, description, security domain, and associated users.

Audit Logs

Click the **Audit Log** icon next to the **Add Schema** tab to list the log details for the Schemas page. The **Audit Logs: Tenant List** page is displayed.

The table on the page displays the following details:

- **Date**
- **Action**
- **Details**
- **User**

Click the **Most Recent** tab to select the audit logs during a particular time period. For example, when you select the range from November 10, 2019 to February 14, 2020 and click **Apply**, the audit log details for this time period are displayed on the **Audit Logs** page.

Click the **Filter** icon next to the **Most Recent** tab to filter the log details using the following criteria:

- **User:** Select one username or all users and click **Apply** to filter the log details using the username.
- **Action:** Select the action, for example, created, updated, or deleted, and click **Apply** to filter the log details according to the action.

For more information, see the [Tenants, on page 21](#) chapter.

Application Management > Schemas Page

The **Schemas** page lists all schemas that are associated with your deployment.

Use the magnifying glass and associated field to search for a specific schema. Use schemas to configure or import tenant policies, such as VRFs and networks.

The Schemas table shows the following information:

- **Name:** click the schema name to view or update the settings for the subject schema.
- **Templates:** displays the name of the template that is used for the schema. A template is a set of configuration objects and their properties that you deploy all at once to one or more sites
- **Tenants:** displays the name of the tenant that is used for the subject schema.
- **Actions:** click the **Action** field with the associated schema to either edit or delete the subject schema.

You can use the **Add Schema** button to add a new schema, which is described in more details in later sections of this document.

Audit Logs

Click the **Audit Log** icon next to the **Add Schema** tab to list the log details for the Schemas page. The **Audit Logs: Schemas List** page is displayed.

The table on the page displays the following details:

- **Date**
- **Action**
- **Details**
- **User**

Click the **Most Recent** tab to select the audit logs during a particular time period. For example, when you select the range from November 10, 2019 to December 14, 2020 and click **Apply**, the audit log details for this time period are displayed on the **Audit Logs** page.

Click the **Filter** icon next to the **Most Recent** tab to filter the log details using the following criteria:

- **User:** Select one username or all users and click **Apply** to filter the log details using the username.
- **Action:** Select the action, for example, created, updated, or deleted, and click **Apply** to filter the log details according to the action.

Infrastructure > Sites Page

The MSO **Infrastructure > Sites** page displays all of the sites in your implementation, for example:

Figure 1: Multi-Site Sites Page

| Health | Name | Type | Templates | State | Controller URL |
|--------------------------------------|----------------------------|------|-----------|---------|--|
| ✔ | Fabric-2 Site ID: 65002 | DCNM | 1 | Managed | https://172.25.74.139:443/... ... |
| ✔ | Fabric-3 Site ID: 65003 | DCNM | 3 | Managed | https://172.25.74.139:443/... ... |
| ✔ | Fabric-1 Site ID: 65001 | DCNM | 1 | Managed | https://172.25.74.137:443/... ... |

The **Sites** page includes the following:

- Site **Health** indicates the status of the site's overall health according to the following color coded identifiers:
 - **Critical** (red)
 - **Major** (orange)
 - **Minor** (yellow)
 - **Warning** (green)
- Site **Name** shows the display name of the site as you defined it when adding the site.
- Site **Type** displays the fabric type, for example `ACI` or `DCNM`.
- The **Templates** column indicates the number of templates associated with the site.
- The **State** column indicates whether or not this particular fabric is managed by MSO.

You add and manage sites and their properties in the Nexus Dashboard GUI. The MSO **Sites** page displays all the sites available in the Nexus Dashboard GUI and allows you to define which specific sites you want to be managed by the MSO.
- The **Controller URL** column displays the in-band IP address of the site's controller.
- The actions menu (...) allows you to import the site's tenants (ACI fabrics only) or open the site's controller UI.

If you click a specific site, a right **Properties** sidebar opens and you can view additional information about the site.



CHAPTER 3

Adding and Deleting Sites

- [Adding Cisco DCNM Sites, on page 9](#)
- [Removing Sites, on page 12](#)
- [Cross Launch to Fabric Controllers, on page 13](#)

Adding Cisco DCNM Sites

This section describes how to add a DCNM site using the Nexus Dashboard GUI and then enable that site to be managed by Multi-Site Orchestrator.

Before you begin

- You must ensure that the site(s) you are adding are running Cisco DCNM, Release 11.5(1) or later.

Step 1 Log in to the Nexus Dashboard GUI

Step 2 Add a new site.

| <input type="checkbox"/> | Health Score | Name | Connectivity Status | Firmware Version | Services Used | Actions |
|--------------------------|--------------|-------------|---------------------|------------------|--|---------------------------------|
| <input type="checkbox"/> | Healthy | ACI-NEWYORK | Up | 5.1(1h) | Nexus Insights Multi-Site Orchestration | Add Site Delete Site Open |

- From the left navigation menu, select **Sites**.
- In the top right of the main pane, select **Actions** > **Add Site**.

Step 3 Provide site information.

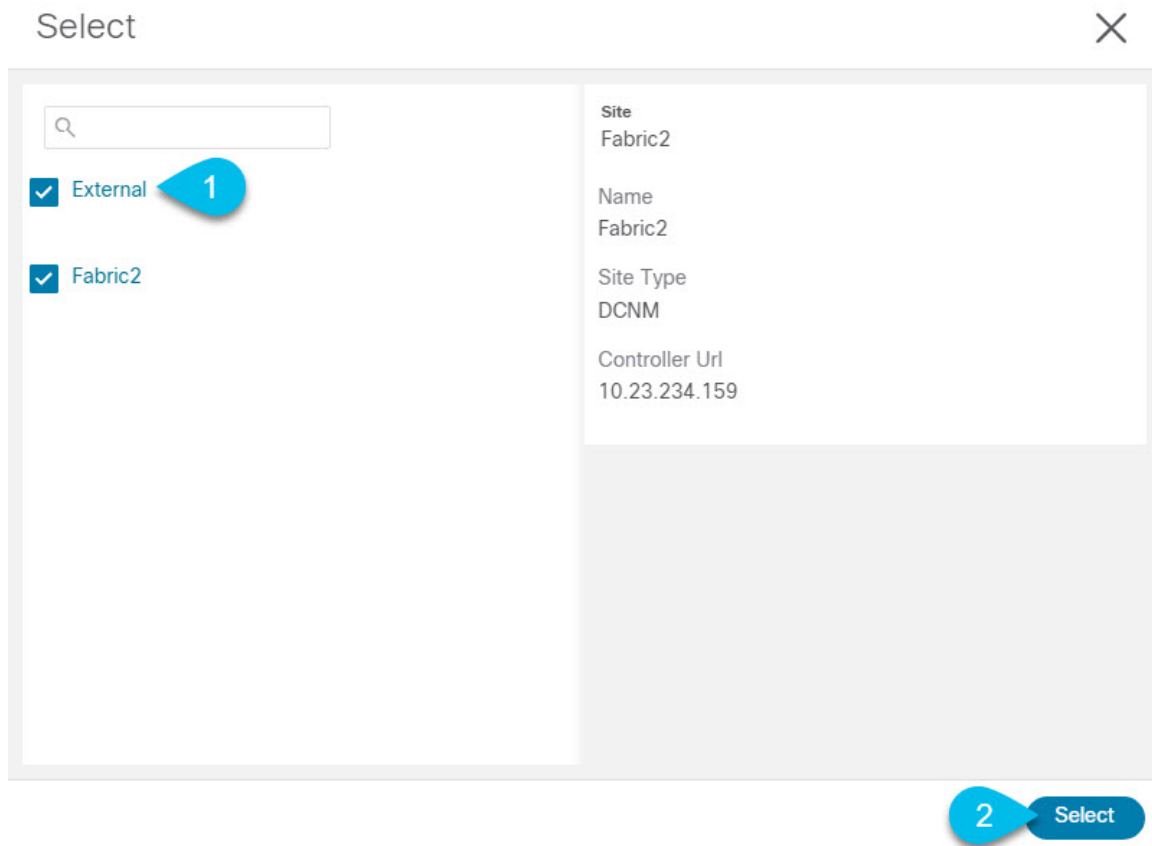
The screenshot shows the 'Add Site' configuration window. The 'Site Type' section has two radio buttons: 'ACI' and 'DCNM'. The 'DCNM' option is selected, indicated by a blue callout '1'. Below this, there are three input fields: 'Host Name/ IP Address' containing '10.23.234.161', 'User Name' containing 'admin', and 'Password' containing masked characters. A blue callout '2' points to the 'User Name' field. Below these fields is a section titled 'Sites on DCNM' with columns for 'Site Name', 'Fabric Name', and 'Controller Url'. A 'Select Sites' button is located below this section, indicated by a blue callout '3'. At the bottom right of the window are 'Cancel' and 'Add' buttons.

- a) For **Site Type**, select **DCNM**.
- b) Provide the DCNM controller information.

You need to provide the **Host Name/IP Address** of the in-band (eth2) interface, **User Name**, and **Password**. for the DCNM controller currently managing your DCNM fabrics.

- c) Click **Select Sites** to select the specific fabrics managed by the DCNM controller.
The fabric selection window will open.

Step 4 Select the fabrics you want to add to the Nexus Dashboard.



- a) Check one or more fabrics that you want to be available to the applications running in your Nexus Dashboard.
- b) Click **Select**.

Step 5 In the **Add Site** window, click **Add** to finish adding the sites.

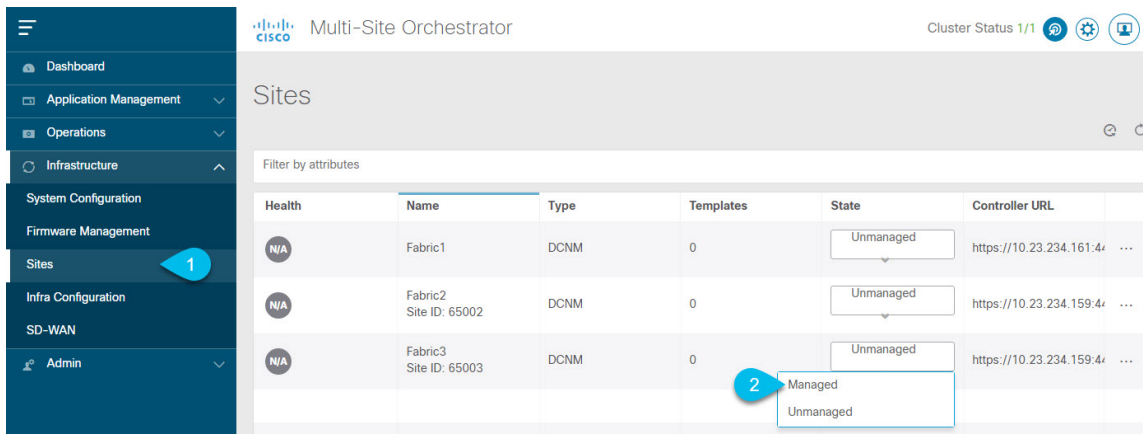
At this time, the sites will be available in the Nexus Dashboard, but you still need to enable them for Multi-Site Orchestrator management as described in the following steps.

Step 6 Repeat the previous steps for any additional DCNM controllers.

Step 7 From the Nexus Dashboard's **Service Catalog**, open the Multi-Site Orchestrator application.

You will be automatically logged in using the Nexus Dashboard user's credentials.

Step 8 In the Multi-Site Orchestrator GUI, enable the sites.



- a) From the left navigation menu, select **Infrastructure** > **Sites**.
- b) In the main pane, change the **State** from `Unmanaged` to `Managed` for each fabric that you want the MSO to manage.

If the fabric you are managing is part of a DCNM Multi-Site Domain (MSD), it will have a **Site ID** already associated with it. In this case, simply changing the **State** to `Managed` will manage the fabric.

However, if the fabric is not part of a DCNM MSD, you will also be prompted to provide a **Fabric ID** for the site when you change its state to `Managed`.

Note If you want to manage both kinds of fabrics, those that are part of an existing MSD and those that are not, you must on-board the MSD fabrics first, followed by any standalone fabrics.

Removing Sites

This section describes how to disable site management for one or more sites using the Multi-Site Orchestrator GUI. The sites will remain present in the Nexus Dashboard.

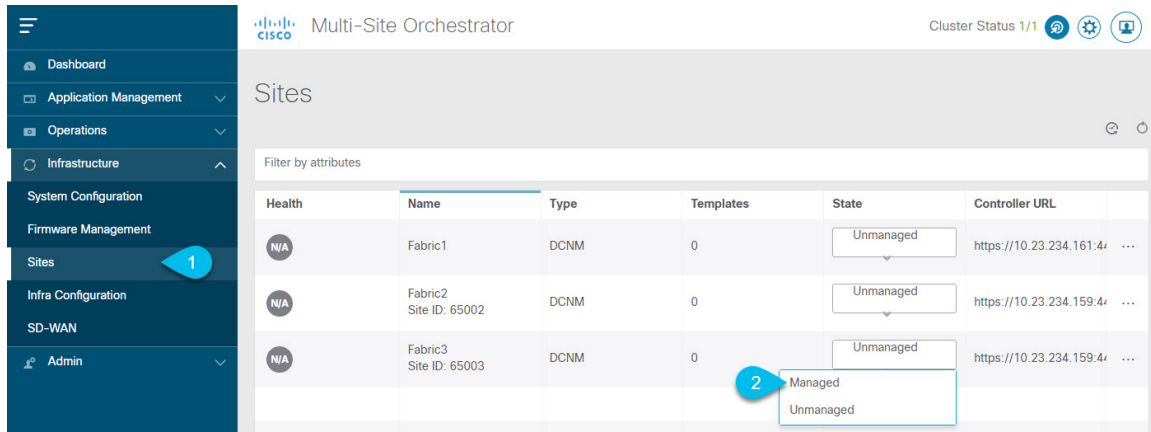
Before you begin

You must ensure that all templates associated with the site you want to remove are not deployed.

Step 1 Open the Multi-Site Orchestrator GUI.

You can open the MSO application from the Nexus Dashboard's **Service Catalog**. You will be automatically logged in using the Nexus Dashboard user's credentials.

Step 2 In the Multi-Site Orchestrator GUI, disable the sites.



- From the left navigation menu, select **Infrastructure** > **Sites**.
- In the main pane, change the **State** from *Managed* to *Unmanaged* for each fabric that you want the MSO to stop managing.

Note If the site is associated with one or more deployed templates, you will not be able to change its state to *Unmanaged* until you undeploy those templates.

Cross Launch to Fabric Controllers

Multi-Site Orchestrator currently supports a number of configuration options for each type of fabrics. For many additional configuration options, you may need to log in directly into the fabric's controller.

You can cross launch into the specific site controller's GUI from the MSO's **Infrastructure** > **Sites** screen by selecting the actions (...) menu next to the site and clicking **Open in user interface**. Note that cross-launch works with out-of-band (OOB) management IP of the fabric.

If your Nexus Dashboard and the fabric are configured for remote user authentication, you will be logged in automatically into the fabric's controller using the same log in information as the Nexus Dashboard user.



CHAPTER 4

Configuring Infra for Cisco DCNM Sites

- [Prerequisites and Guidelines, on page 15](#)
- [Configuring Infra: General Settings, on page 15](#)
- [Refreshing Site Connectivity Information, on page 16](#)
- [Configuring Infra: DCNM Site Settings, on page 17](#)
- [Deploying Infra Configuration, on page 18](#)

Prerequisites and Guidelines

The following sections describe the steps necessary to configure the general as well as site-specific fabric Infra settings.

Before you proceed with Infra configuration, you must have added the sites as described in previous sections.

In addition, keep in mind the following:

- Adding or removing border gateway switches requires a Multi-Site Orchestrator fabric connectivity information refresh described in the [Refreshing Site Connectivity Information, on page 16](#) as part of the general Infra configuration procedures.

Configuring Infra: General Settings

This section describes how to configure general Infra settings for all the sites.

- Step 1** Log in to the Cisco Multi-Site Orchestrator GUI.
- Step 2** In the left navigation menu, select **Infrastructure** > **Infra Configuration**.
- Step 3** In the main pane, click **Configure Infra**.
- Step 4** In the left sidebar, select **General Settings**.
- Step 5** Configure control plane BGP.
 - a) Choose **BGP Peering Type**.
 - `full-mesh`—All border gateway switches in each site will establish peer connectivity with remote sites' border gateway switches.

- `route-server`—The route-server option allows you to specify one or more control-plane nodes to which each site establishes MP-BGP EVPN sessions. The route-server nodes perform a function similar to traditional BGP route-reflectors, but for EBGP (and not iBGP) sessions. The use of route-server nodes avoids creating MP-BGP EVPN full mesh adjacencies between all the VXLAN EVPN sites managed by MSO.

b) If you set the **BGP Peering Type** to `route-server`, click **+Add Route Server** to add one or more route servers.

In the **Add Route Server** window that opens:

- From the **Site** dropdown, select the site you want to connect to the route server.
- The **ASN** field will be auto-populated with the site's ASN.
- From the **Core Router Device** dropdown, select the route server to which you want to connect.
- From the **Interface** dropdown, select the interface on the core router device.

You can add up to 4 route servers. If you add multiple route servers, every site will establish MP-BGP EVPAN adjacencies to every route server.

a) In the **Keepalive Interval (Seconds)** field, enter the keep alive interval seconds.

We recommend keeping the default value.

b) In the **Hold Interval (Seconds)** field, enter the hold interval seconds.

We recommend keeping the default value.

c) In the **Stale Interval (Seconds)** field, enter stale interval seconds.

We recommend keeping the default value.

d) Choose whether you want to turn on the **Graceful Helper** option.

e) In the **Maximum AS Limit** field, enter the maximum AS limit.

f) In the **BGP TTL Between Peers** field, enter the BGP TTL between peers.

Step 6 Configure DCNM settings.

a) Provide the **L2 VXLAN VNI Range**.

b) Provide the **L3 VXLAN VNI Range**.

c) Provide the **Multi-Site Routing Loopback IP Range**.

This field is used to auto-populate the **Multi-Site TEP** field for each fabric, which is described in [Configuring Infra: DCNM Site Settings, on page 17](#).

For sites that were previously part of a Multi-Site Domain (MSD) in DCNM, this field will be pre-populated with the previously defined value.

d) Provide the **Anycast Gateway MAC**.

Refreshing Site Connectivity Information

Infrastructure changes, such as adding and removing border gateway switches, require a Multi-Site Orchestrator fabric connectivity refresh. This section describes how to pull up-to-date connectivity information directly from each site's controller.

-
- Step 1** Log in to the Cisco Multi-Site Orchestrator GUI.
- Step 2** In the left navigation menu, select **Infrastructure > Infra Configuration**.
- Step 3** In the main pane, click **Configure Infra**.
- Step 4** In the left sidebar, under **Sites**, select a specific site.
- Step 5** In the main window, click the **Refresh** button to pull fabric information from the controller.
- Step 6** (Optional) In the **Confirmation** dialog, check the box if you want to remove configuration for decommissioned border gateway switches.
- If you choose to enable this checkbox, all configuration info for any currently decommissioned border gateway switches will be removed from the database.
- Step 7** Finally, click **Yes** to confirm and load the connectivity information.
- This will discover any new or removed spines and all site-related fabric connectivity will be re-imported from the site's controller.
-

Configuring Infra: DCNM Site Settings

This section describes how to configure site-specific Infra settings for on-premises sites.

- Step 1** Log in to the Cisco Multi-Site Orchestrator GUI.
- Step 2** In the left navigation menu, select **Infrastructure > Infra Configuration**.
- Step 3** In the main pane, click **Configure Infra**.
- Step 4** In the left pane, under **Sites**, select a specific DCNM.
- Step 5** In the right **<Site> Settings** sidebar, specify the **Multi-Site TEP**.
- This address is used for the inter-site L2 BUM and L3 multicast traffic. This IP address is deployed on all border gateway switches that are part of the same fabric.
- Note** If the site you are configuring is part of the DCNM Multi-Site Domain (MDS), this field will be pre-populated with the information imported from DCNM. In this case, changing the value and re-deploying the infra configuration, will impact traffic between the sites that are part of the MDS.
- You can choose to **Auto Allocate** this field, which will allocate the next available address from the **Multi-Site Routing Loopback IP Range** you defined in previous section.
- Step 6** Within the **<fabric-name>** tile, select the border gateway.
- Step 7** In the right **<border-gateway>** setting sidebar, specify the **Control Plane TEP** and **Data Plane TEP**.
- Step 8** Click **Add Port** to configure the port that connects to the IPN.
- Note** This release does not support importing the port configuration from the DCNM. If the site you are configuring is already part of the DCNM Multi-Site Domain (MDS), you must use the same values that are already configured in DCNM.

Update Port ✕

* Ethernet Port ID
Ethernet1/1 ✕ ▾

* IP Address
10.10.1.9/30

* Remote Address
10.10.1.10

* Remote ASN
65002

* MTU
9216

BGP Authentication
 None Simple

[Save](#)

Provide the following information specific to your deployment for the port that connects this border gateway to a core switch or another border gateway:

- From the **Ethernet Port ID** dropdown, select the port that connects to the IPN.
- In the **IP Address** field, enter the IP address and netmask.
- In the **Remote Address** field, provide the IP address of the remote device to which the port is connected.
- In the **Remote ASN** field, provide the remote site's ID.
- In the **MTU** field, enter the port's MTU.

MTU of the spine port should match MTU on IPN side.

You can specify either `inherit` or a value between 576 and 9000.

- For **BGP Authentication**, you can pick either `None` or `Simple` (MD5).
If you select `Simple`, you must also provide the **Authentication Key**.

Deploying Infra Configuration

This section describes how to deploy the Infra configuration to each DCNM site.

Before you begin

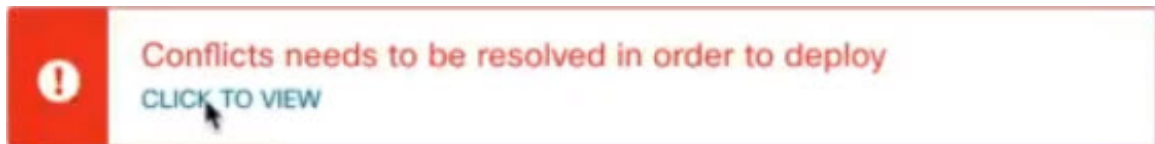
You must have the general and site-specific infra configurations completed as described in previous sections of this chapter.

Step 1 Ensure that there are no configuration conflicts or resolve them if necessary.

The **Deploy** button will be disabled and a warning will be displayed if there are any configuration conflicts from the already configured settings in each site. For example, if a VRF or network with the same name exists in multiple sites but uses different VNI in each site.

In case of configuration conflicts:

- a) Click **Click to View** link in the conflict notification pop-up.



- b) Note down the specific configurations that are causing the conflicts.

For example, in the following report, there are ID mismatches between VRFs and networks in `fab1` and `fab2` sites.

| Error Type | Error Message |
|------------|--|
| IDMismatch | Policy Name MyVRF_50001 Policy ID 50001 Sites [fab2] conflicting with Policy Name MyVRF_50001 Policy ID 60001 Sites [fab1] |
| IDMismatch | Policy Name MyNetwork_30000 Policy ID 40000 Sites [fab2] conflicting with Policy Name MyNetwork_30000 Policy ID 30000 Sites [fab1] |

- c) Click the **X** button to close the report, then exit Infra configuration screen.
- d) Unmanage the site in MSO, as described in [Removing Sites, on page 12](#).

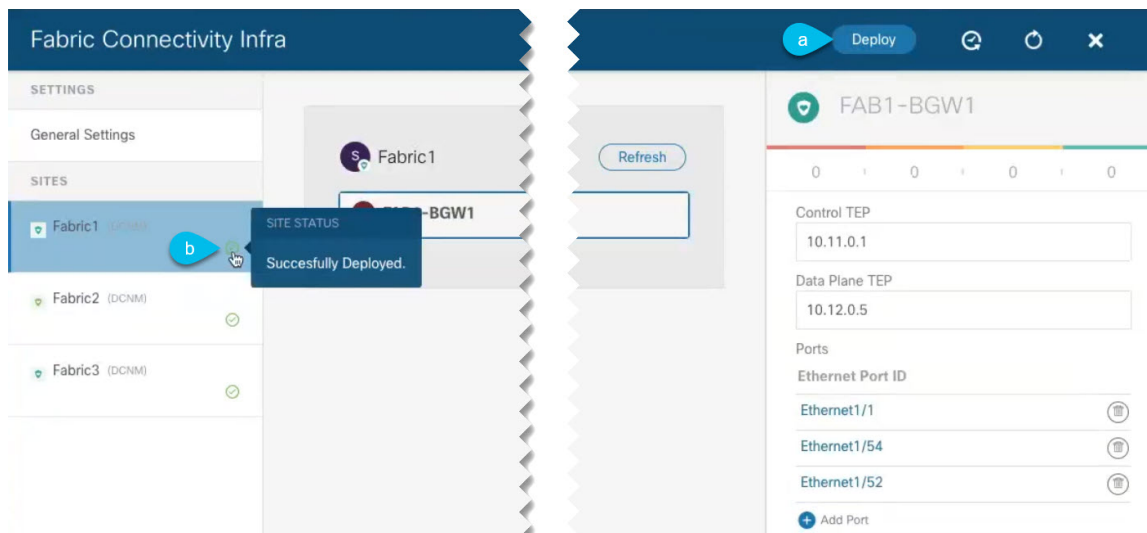
You do not need to remove the site from the Nexus Dashboard, simply unmanage it in MSO GUI.

- e) Resolve the existing configuration conflicts.
- f) Manage the site again, as described in [Adding Cisco DCNM Sites, on page 9](#).

Since the site is already added in Nexus Dashboard, simply enable it for management in MSO.

- g) Verify that all conflicts are resolved and the **Deploy** button is available.

Step 2 Deploy configuration.



- a) In the top right of the **Fabric Connectivity Infra** screen, choose the appropriate **Deploy** option to deploy the configuration.

If you are configuring only DCNM sites, simply click **Deploy** to deploy the Infra configuration.

- b) Wait for configuration to be deployed.

When you deploy infra configuration, MSO will signal the DCNM to configure the underlay and the EVPN overlay between the border gateways.

When configuration is successfully deployed, you will see a green checkmark next to the site in the **Fabric Connectivity Infra** screen:



CHAPTER 5

Fabric Management

- [Tenants, on page 21](#)
- [Schemas and Templates, on page 22](#)
- [Concurrent Configuration Updates, on page 23](#)
- [Creating Schemas and Templates, on page 25](#)
- [Deploying Templates, on page 31](#)
- [Schema Overview and Deployment Visualizer, on page 31](#)

Tenants

A tenant is a logical container for application policies that enable an administrator to exercise domain-based access control. A tenant represents a unit of isolation from a policy perspective, but it does not represent a private network. Tenants can represent a customer in a service provider setting, an organization or domain in an enterprise setting, or just a convenient grouping of policies.

To manage tenants, you must have either `Power User or Site` and `Tenant Manager` read-write role.

Three tenants are pre-configured for you:

- `common`—A special tenant with the purpose of providing "common" services to other tenants in ACI fabrics. Global reuse is a core principle in the common tenant. Some examples of common services include shared L3Outs, DNS, DHCP, Active Directory, and shared private networks or bridge domains.
- `dcnm-default-tn`—A special tenant with the purpose of providing configuration for Cisco DCNM fabrics.
- `infra`—The Infrastructure tenant that is used for all internal fabric communications, such as tunnels and policy deployment. This includes switch to switch and switch to APIC communications. The `infra` tenant does not get exposed to the user space (tenants) and it has its own private network space and bridge domains. Fabric discovery, image management, and DHCP for fabric functions are all handled within this tenant.

When using Multi-Site Orchestrator to manage Cisco DCNM fabrics, you will use the default `dcnm-default-tn` that is preconfigured for you and allows you to create and manage the following objects:

- VRFs
- Networks

Schemas and Templates

A schema is a collection of templates, which are used for defining networking configuration, with each template assigned to a specific tenant. A template is a set of configuration objects and their properties that you deploy all at once to one or more sites. There are multiple approaches you can take when it comes to creating schema and template configurations specific to your deployment use case. The following sections describe a few simple design directions you can take when deciding how to define the schemas, templates, and policies in your Multi-Site environment.

Keep in mind that when designing schemas, you must consider the supported scalability limits for the number of schemas, templates, and objects per schema. Detailed information on verified scalability limits is available in the [Cisco Multi-Site Verified Scalability Guides](#) for your release.

Single Schema Deployment

The simplest schema design approach is a single schema deployment. You can create a single schema with all VRFs and Networks in that schema. You can then create a single application profile or multiple application profiles within the templates and deploy it to one or more sites.

This simplest approach to Multi-Site schema creation is to create all objects within the same schema and template. However, the supported number of schemas or templates per schema scalability limit may make this approach unsuitable for large scale deployments, which could exceed those limits.

Multiple Schemas Based On Object Relationships

When configuring multiple schemas with shared object references, it is important to be careful when making changes to those objects. For instance, making changes to or deleting a shared networking object can impact applications in one or more sites. Because of that, you may choose to create a template around each individual site that contains only the objects used by that site and its applications. And create different templates containing the shared objects.

For example, you can use the following templates for a configuration that you plan to deploy to 3 different sites:

- Site 1 template
- Site 2 template
- Site 3 template
- Site 1 and 2 shared template
- Site 1 and 3 shared template
- Site 2 and 3 shared template
- All shared template

Similarly, rather than separating objects based on which site they are deployed to, you can also choose to create schemas and templates based on individual applications instead. This would allow you to easily identify each application profile and map them to schemas and sites as well as easily configure each application as local or stretched across sites.

However, as this could quickly exceed the templates per schema limit (listed in the [Verified Scalability Guide](#) for your release), you would have to create additional schemas to accommodate the multiple combinations.

While this creates additional complexity with multiple additional schemas and templates, it provides true separation of objects based on site or application.

Template Design

In this release, we recommend creating separate templates for VRFs and Networks within each schema and then deploying the VRF templates first, followed by the templates that contain Networks. This way any VRFs required by the networks will be already created when you push Network configuration to the sites.

Similarly, when undeploying multiple networks and VRFs, we recommend undeploying the Networks template first, followed by the VRF templates. This will ensure that when VRFs are undeployed, there will be no conflicts with any existing Networks still using them.

Concurrent Configuration Updates

The Multi-Site Orchestrator GUI will ensure that any concurrent updates on the same site or schema object cannot unintentionally overwrite each other. If you attempt to make changes to a site or schema that was updated by another user since you opened it, the GUI will reject any subsequent changes you try to make and present a warning requesting you to refresh the object before making additional changes:



However, the default REST API functionality was left unchanged in order to preserve backward compatibility with existing applications. In other words, while the UI is always enabled for this protection, you must explicitly enable it for your API calls for MSO to keep track of configuration changes.



Note When enabling this feature, note the following:

- This release supports detection of conflicting configuration changes for Site and Schema objects only.
- Only `PUT` and `PATCH` API calls support the version check feature.
- If you do not explicitly enable the version check parameter in your API calls, MSO will not track any updates internally. And as a result, any configuration updates can be potentially overwritten by both subsequent API calls or GUI users.

To enable the configuration version check, you can pass the `enableVersionCheck=true` parameter to the API call by appending it to the end of the API endpoint you are using, for example:

```
https://<mso-ip-address>/mso/api/v1/schemas/<schema-id>?enableVersionCheck=true
```

Example

We will use a simple example of updating the display name of a template in a schema to show how to use the version check attribute with `PUT` or `PATCH` calls.

First, you would `GET` the schema you want to modify, which will return the current latest version of the schema in the call's response:

```

{
  "id": "601acfed38000070a4ee9ec0",
  "displayName": "Schema1",
  "description": "",
  "templates": [
    {
      "name": "Template1",
      "displayName": "current name",
      [...]
    }
  ],
  "_updateVersion": 12,
  "sites": [...]
}

```

Then you can modify the schema in one of two ways appending `enableVersionCheck=true` to the request URL:



Note You must ensure that the value of the `"_updateVersion"` field in the payload is the same as the value you got in the original schema.

- Using the `PUT` API with the entire updated schema as payload:

```

PUT /v1/schemas/601acfed38000070a4ee9ec0?enableVersionCheck=true
{
  "id": "601acfed38000070a4ee9ec0",
  "displayName": "Schema1",
  "description": "",
  "templates": [
    {
      "name": "Template1",
      "displayName": "new name",
      [...]
    }
  ],
  "_updateVersion": 12,
  "sites": [...]
}

```

- Using any of the `PATCH` API operations to make a specific change to one of the objects in the schema:

```

PATCH /v1/schemas/601acfed38000070a4ee9ec0?enableVersionCheck=true
[
  {
    "op": "replace",
    "path": "/templates/Template1/displayName",
    "value": "new name",
    "_updateVersion": 12
  }
]

```

When the request is made, the API will increment the current schema version by 1 (from 12 to 13) and attempt to create the new version of the schema. If the new version does not yet exist, the operation will succeed and the schema will be updated; if another API call (with `enableVersionCheck` enabled) or the UI have modified the schema in the meantime, the operation fails and the API call will return the following response:

```

{
  "code": 400,
  "message": "Update failed, object version in the DB has changed, refresh your client"
}

```

```
and retry"
}
```

Creating Schemas and Templates

Before you begin

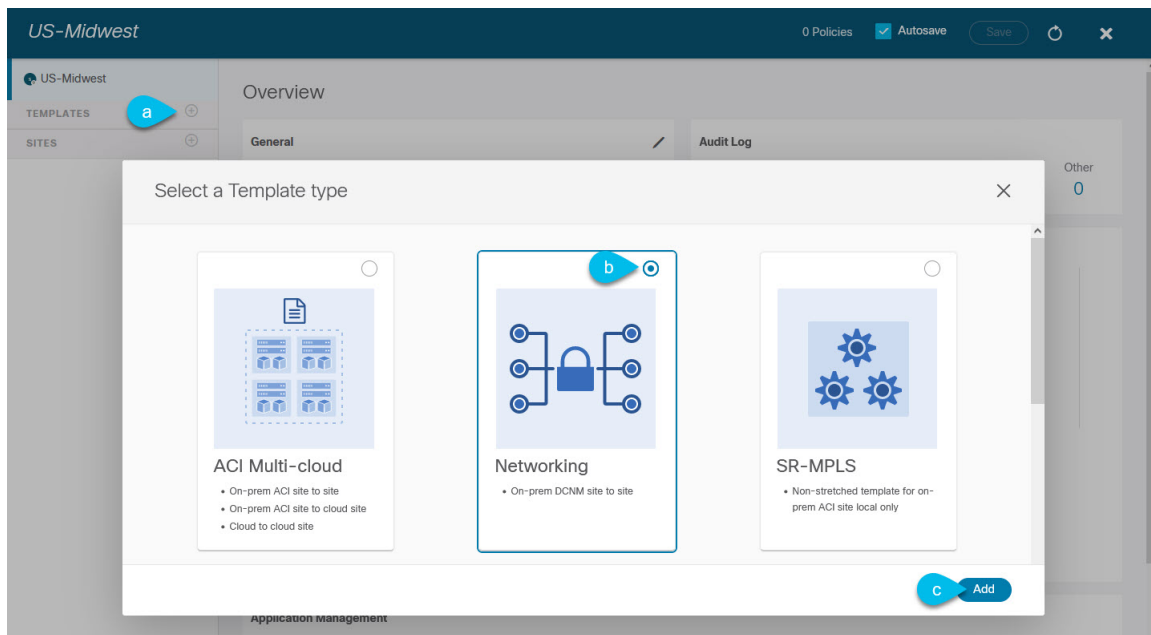
- You must have an administrative user account with full read/write privileges.
- You must have a tenant user account with read/write tenant policy privileges.

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

Step 2 Create a new schema.

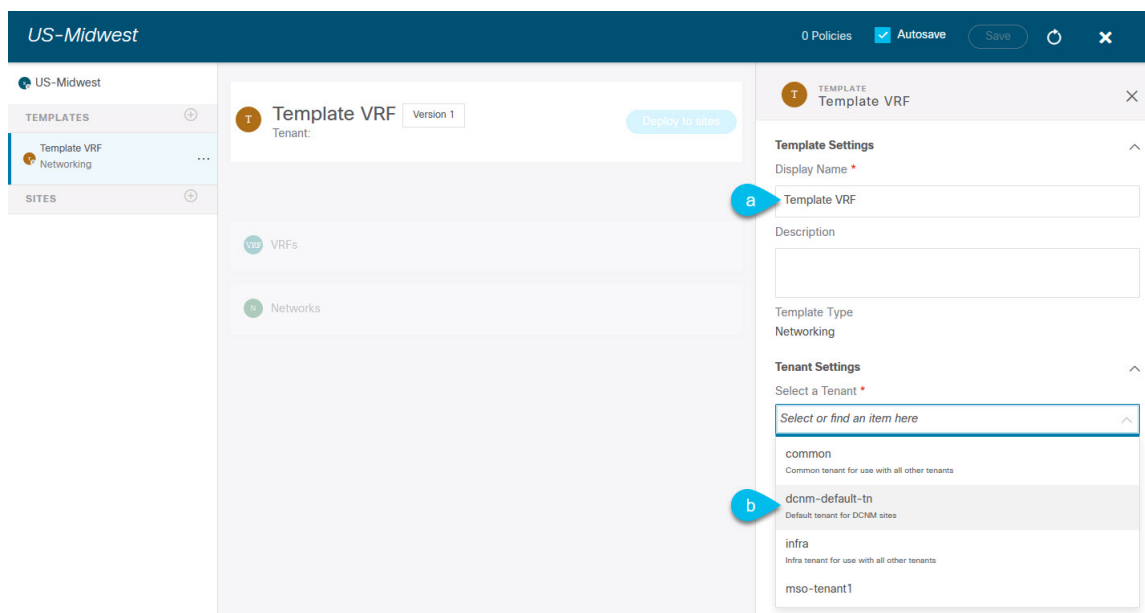
- From the left navigation pane, choose **Application Management > Schemas**.
- On the Schemas page, click **Add Schema**.
- In the schema creation dialog, provide the **Name** and optional description for the schema.
By default, the new schema is empty, so you need to add one or more templates.

Step 3 Create a template.



- In the left sidebar under **Templates**, click the + sign to add a new template.
- In the **Select a Template type** window, choose **Networking** for the template type.
- Click **Add** to create the template.

Step 4 Provide the name and the tenant for the template.



- a) In the right sidebar, specify the **Display Name** for the template.
- b) From the **Select a Tenant** dropdown, select the `dcnm-default-tn` tenant.

Keep in mind, the user account you're using to create a new schema must be associated with the tenant you are trying to add to it, otherwise the tenant will not be available in the drop-down menu.

Step 5 Assign the templates to sites.

You deploy one template at a time, so you need to associate the template with at least one site where you want to deploy the configuration.

- a) In the left pane, click the + icon next to Sites
- b) In the **Add Sites** window, check the checkbox next to the sites where you want to deploy the template.
- c) From the **Assign to Template** dropdown next to each site, select one or more templates.

While you deploy one template at a time to every site with which it is associated, you can associate multiple templates to a site at once.

- d) Click **Save**.

Importing Schema Elements From DCNM Sites

You can create new objects and push them out to one or more sites or you can import existing site-local objects and manage them using the Multi-Site Orchestrator. This section describes how to import one or more existing objects, while creating new objects is described later on in this document.

Step 1 Open the **Schema** where you want to import objects.

Step 2 In the left sidebar, select the **Template** where you want to import objects.

Step 3 In the main pane click the **Import** button and select the **Site** from which you want to import.

Step 4 In the **Import from** <site-name> window that opens, select one or more objects.

Note The names of the objects imported into the Multi-Site Orchestrator must be unique across all sites. Importing different objects with duplicate names will cause a schema validation error and the import to fail. If you want to import objects that have the same name, you must first rename them.

Creating VRFs

This section describes how to create a VRF.

Before you begin

You must have the schema and template created and a tenant assigned to the template, as described in [Creating Schemas and Templates, on page 25](#).

Step 1 Select the schema and template where you want to create VRF.

Step 2 In the schema edit view, choose **Create Object** > **VRF**.

Step 3 In the properties pane on the right, provide **Display Name** for the VRF.

Step 4 Configure the **DCNM Properties** for the VRF.

a) (Optional) Provide the **VRF ID**.

You can choose to specify the VNI of the VRF or leave the field empty and the VNI will be automatically allocated by the MSO from the ranges you specified in [Configuring Infra: General Settings, on page 15](#).

b) From the **VRF Profile** dropdown, select the VRF profile.

You can assign the `Default_VRF_Universal` profile or choose any available VRF Profile that had been previously created in DCNM. Any profiles created in DCNM are automatically imported into the MSO and are available for selection here.

c) From the **VRF Extension Profile** dropdown, select the extension profile.

You can assign the `Default_VRF_Extension_Universal` profile or choose any available VRF Extension Profile that had been previously created in the DCNM. Any profiles created in DCNM are automatically imported into the MSO and are available for selection here.

d) Provide the **Loopback Routing Tag**.

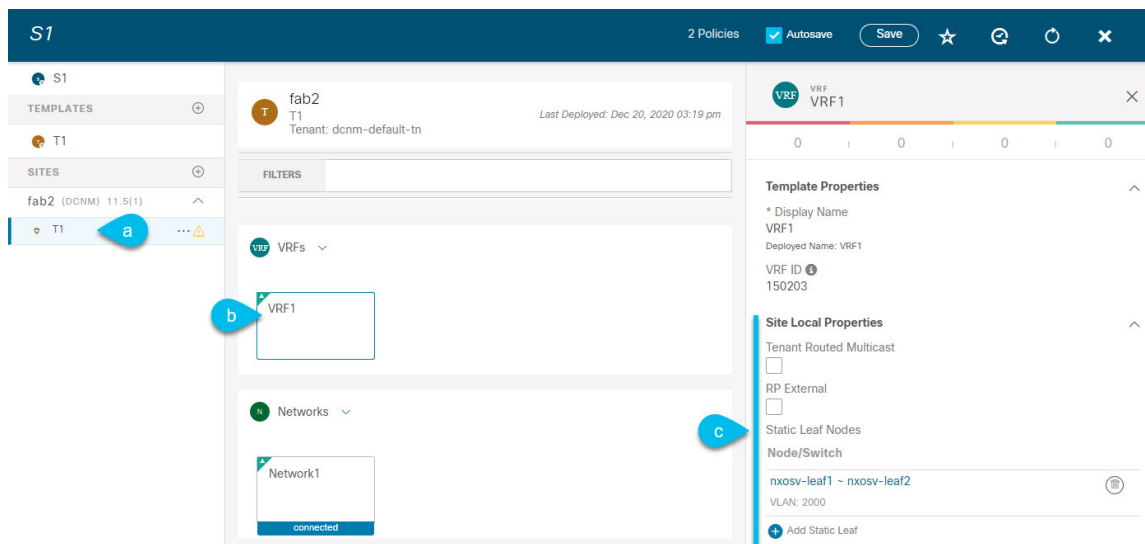
If a VLAN is associated with multiple subnets, then this tag is associated with the IP prefix of each subnet. Note that this routing tag is associated with overlay network creation too.

e) Provide the **Redistribute Direct Route Map**.

Specifies the route map name for redistribution of routes in the VRF.

Step 5 Configure the VRF's site-local properties.

In addition to the network's general properties that apply to every site where the VRF is deployed, you can configure site-specific properties for this VRF individually for each site.



- In the left sidebar under **SITES**, select the template where the network is defined.
- In the main pane, select the network.
- In the right **Properties** sidebar, provide the site-specific settings.

You can configure the following site-local properties:

- Enable **Tenant Routed Multicast**—Tenant Routed Multicast (TRM) enables multicast forwarding on the VXLAN fabric that uses a BGP-based EVPN control plane. TRM provides multi-tenancy aware multicast forwarding between senders and receivers within the same or different subnets local or across VTEPs. If you enable TRM, you must also provide the **RP Address** and **Overlay Multicast Group**.
- Enable **RP External** if the Rendezvous Point (RP) is external to the fabric.
- Click **Add Static Leaf** to select one or more leaf switches where the VRF will be configured.

In the **Add Static Leaf** window that opens, choose the leaf node and provide the VLAN ID for the VRF.

Creating Networks

This section describes how to configure a DCNM network from Multi-Site Orchestrator.

Before you begin

- You must have the schema and template created and a tenant assigned to the template, as described in [Creating Schemas and Templates, on page 25](#).
- You must have the VRF created as described in [Creating VRFs, on page 27](#)

- Step 1** Select the schema and template where you want to create the application profile.
- Step 2** In the schema edit view, choose **Create Object > Network**.

Step 3 In the properties pane on the right, provide **Display Name** for the network.

Step 4 (Optional) Provide the **Network ID**.

You can choose to specify the network ID or leave the field empty and the ID will be automatically allocated by the MSO when you save the schema.

Step 5 Choose whether or not this is a **Layer2 Only** network.

Step 6 From the **Virtual Routing & Forwarding** dropdown, select the VRF you created for this network.

This option will be unavailable if you enabled **Layer2 Only**.

Step 7 From the **Network Profile** dropdown, select the network profile.

You can assign the `Default_Network_Universal` profile or choose any available Network Profile that had been previously created in DCNM. Any profiles created in DCNM are automatically imported into the MSO and are available for selection here.

Step 8 From the **Network Extension Profile** dropdown, select the network extension profile.

You can assign the `Default_Network_Extension_Universal` profile or choose any available Network Extension Profile that had been previously created in the DCNM. Any profiles created in DCNM are automatically imported into the MSO and are available for selection here.

Step 9 Provide the **VLAN ID** for the network.

Step 10 Provide the **VLAN Name**.

Step 11 Add one or more **Subnets**.

This option will be unavailable if you enabled **Layer2 Only**.

a) Click **+Add Subnet**.

An **Add Subnet** window opens.

b) Click **+Add Gateway IP** and enter the subnet's **Gateway IP** address.

You can configure up to four gateway IPs.

c) Choose `Primary` for the first gateway you add.

d) Click the checkmark to save the gateway information.

e) Repeat the previous substeps to provide additional gateways.

f) Click **Add** to finish adding the subnet.

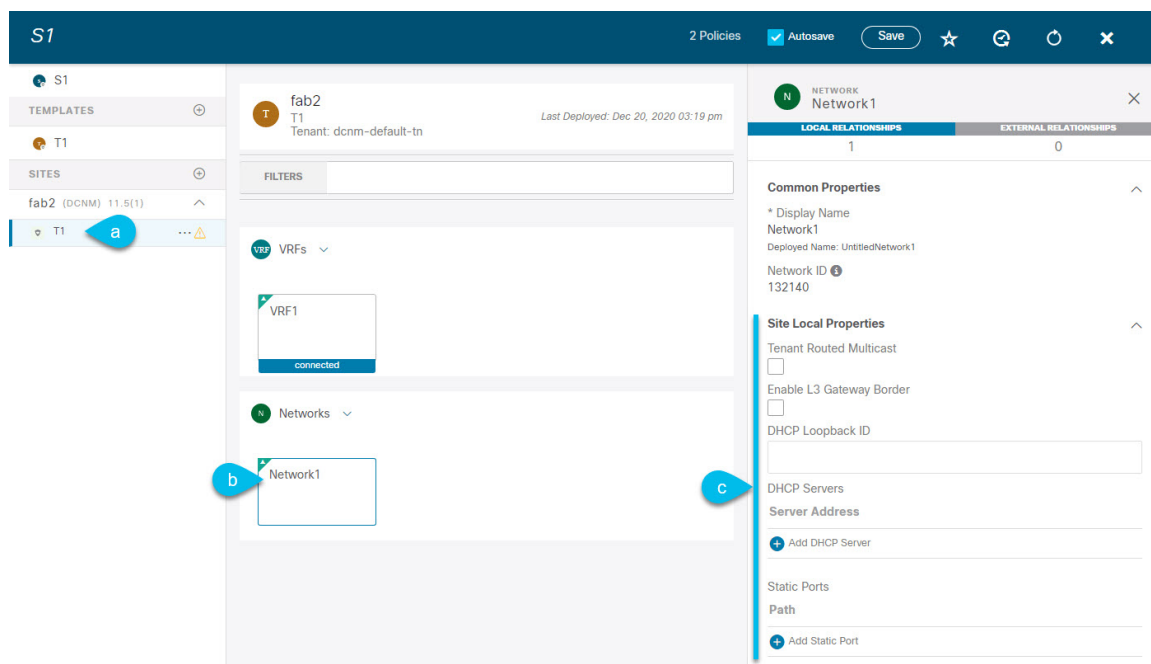
Step 12 Choose whether you want to **Suppress ARP**.

Step 13 Provide the **MTU** for this network.

Step 14 Provide the **Routing Tag**.

Step 15 Configure the network's site-local properties.

In addition to the network's general properties that apply to every site where the network is deployed, you can configure site-specific properties for this network individually for each site.



- In the left sidebar under **SITES**, select the template where the VRF is defined.
- In the main pane, select the VRF.
- In the right **Properties** sidebar, provide the site-specific settings.

You can configure the following site-local properties:

- Enable **Tenant Routed Multicast**—Tenant Routed Multicast (TRM) enables multicast forwarding on the VXLAN fabric that uses a BGP-based EVPN control plane. TRM provides multi-tenancy aware multicast forwarding between senders and receivers within the same or different subnets local or across VTEPs.
- Check **Enable L3 Gateway Border** to enable Layer 3 SVI on the border gateways to allow connecting dual-attached hosts to it.
- Provide the **DHCP Loopback ID**.

The value must be in the 0-1023 range.

- Click **+Add DHCP Server** to add one or more DHCP relay servers.

In the **Add DHCP Server** window that opens, provide the IP address of the DHCP relay and the VRF to which it belongs.

- Click **+Add Static Port** to add one or more ports to which the network's VLAN will be attached.

In the **Add Static Port** window that opens, select the leaf switch that contains the port, provide the VLAN ID, and finally click **Add Port** to specify one or more ports for the network.

Note that if you want to add multiple static ports from different leaf switches, you will need to repeat the process for each leaf switch separately.

Deploying Templates

This section describes how to deploy new or updated configuration to DCNM fabrics.

Before you begin

You must have the schema, template, and any objects you want to deploy to sites already created, as described in previous sections of this document.

Step 1 Navigate to the schema that contains one or more templates that you want to deploy.

Step 2 Assign the templates to sites.

If you have already assigned the templates to sites, skip this step.

You deploy one template at a time, so you need to associate the template with at least one site where you want to deploy the configuration.

- a) In the left pane, click the + icon next to Sites
- b) In the **Add Sites** window, check the checkbox next to the sites where you want to deploy the template.
- c) From the **Assign to Template** dropdown next to each site, select one or more templates.

While you deploy one template at a time to every site with which it is associated, you can associate multiple templates to a site at once.

- d) Click **Save**.

Step 3 In the left sidebar, select the template you want to deploy.

Step 4 In the top right of the template edit view, click **Deploy to sites**.

The **Deploy to Sites** window opens that shows the summary of the objects to be deployed.

Step 5 Click **Deploy** to deploy the template.

- If this is the first time you are deploying this template or you have made changes to a previously deployed template, the **Deploy to Sites** summary will show the configuration difference that will be deployed to sites.

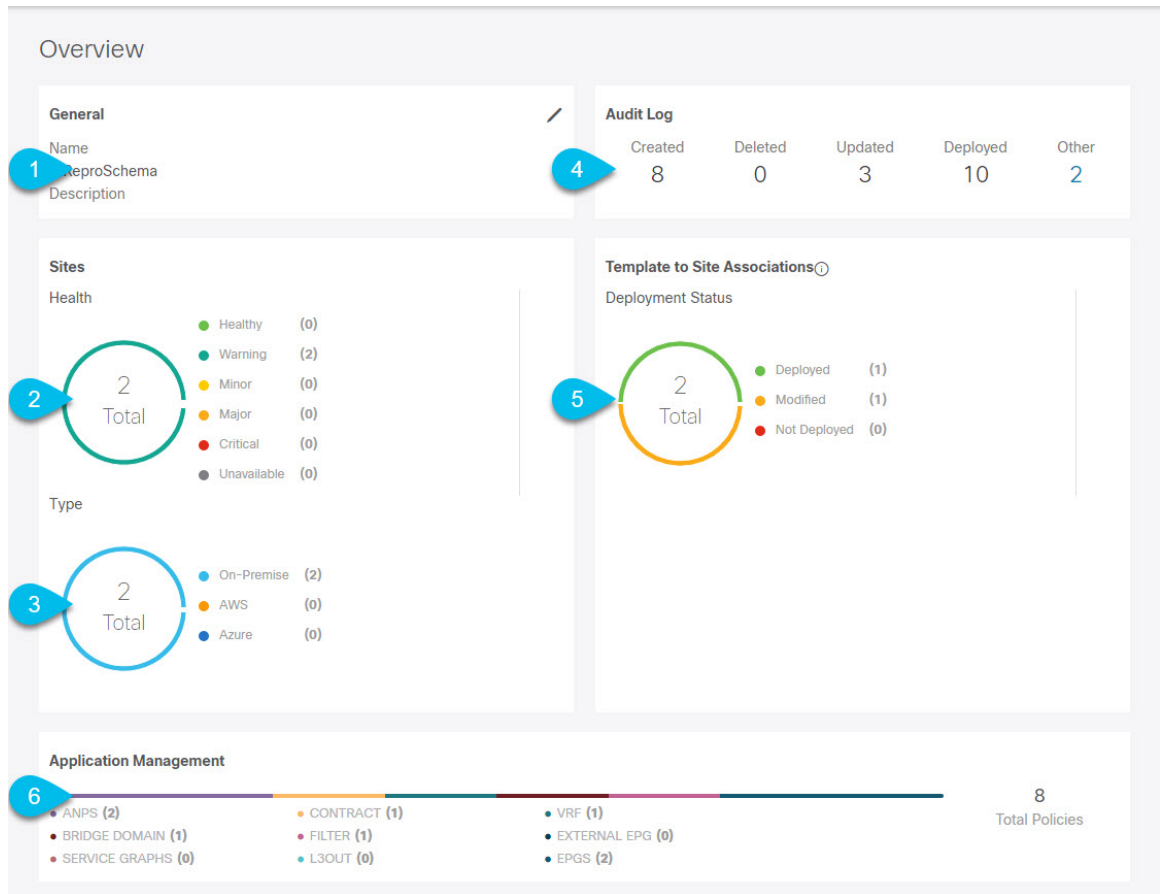
Note You can filter the view using the `Created`, `Modified`, and `Deleted` checkboxes for informational purposes, but keep in mind that all of the changes are still deployed when you click **Deploy**.

- If you have previously deployed this template but made no changes to it since, the **Deploy to Sites** summary will allow you to re-deploy the entire template only the `Full Template` option and you can simply click **Deploy** to re-deploy the entire template.

Schema Overview and Deployment Visualizer

When you open a schema with one or more objects defined and deployed to one or more fabrics, the schema **Overview** page will provide you with a summary of the deployment.

Figure 2: Schema Overview

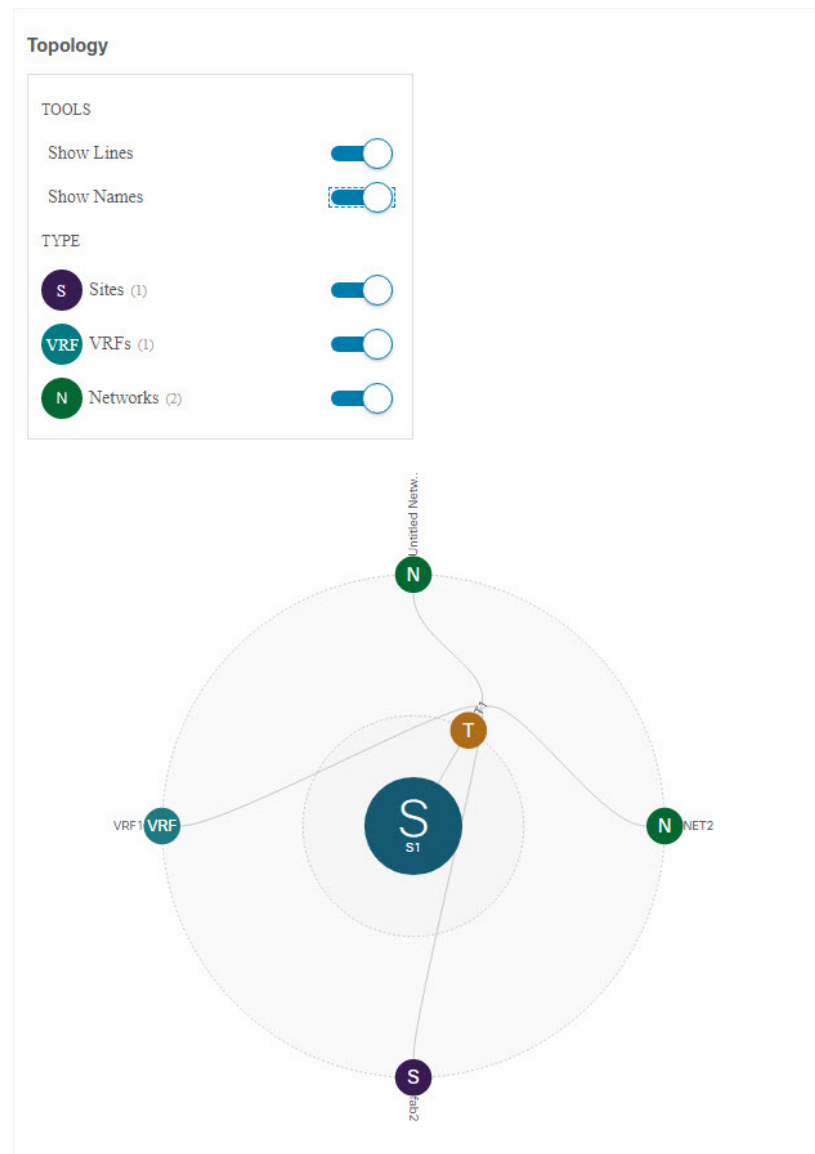


The following details are provided on this page:

- 1. General**—Provides general information of the schema, such as the name and description.
- 2. Audit Log**—Provides an audit log summary of the actions performed on the schema.
- 3. Sites > Health**—Provides the number of sites associated with the templates in this schema, sorted by the site's health status.
- 4. Sites > Type**—Provides the number of sites associated with the templates in this schema, sorted by the site's type.
- 5. Template to Site Associations > Deployment Status**—Provides the number of templates in this schema that are associated with one or more sites and their deployment status.
- 6. Application Management**—Provides a summary of individual objects contained by the templates in this schema.

The **Topology** tile allows you to create a topology visualizer by selecting one or more objects to be displayed by the diagram as shown in the following figure.

Figure 3: Deployment Visualizer



1. **Configuration Options**—Allows you to choose which policy objects to display in the topology diagram below.
2. **Topology Diagram**—Provides visual representation of the policies configured in all of the Schema's templates that are assigned to sites.

You can choose which objects you want to display using the **Configuration Options** above.

You can also mouse over an objects to highlight all of its dependencies.



PART I

Operations

- [System Configuration, on page 37](#)
- [Audit Logs, on page 39](#)
- [Backup and Restore, on page 41](#)
- [Tech Support, on page 47](#)
- [Upgrading or Downgrading MSO Application, on page 53](#)



CHAPTER 6

System Configuration

- [System Configuration Settings](#), on page 37
- [System Alias and Banner](#), on page 37
- [Login Attempts and Lockout Time](#), on page 38

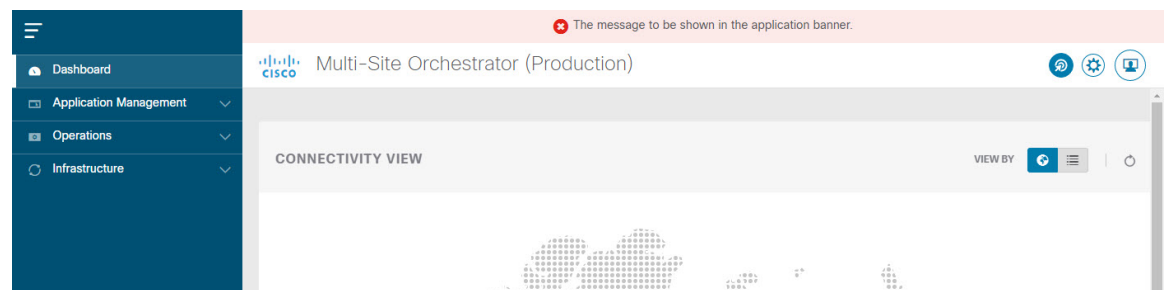
System Configuration Settings

There is a number of global system settings that are available under **Admin > System Configuration**, which you can configure for your Multi-Site Orchestrator as described in the following sections.

System Alias and Banner

This section describes how to configure an alias for your Multi-Site Orchestrator as well as enable a custom GUI-wide banner to be displayed at the top of your screen, as shown in the following figure.

Figure 4: System Banner Display



- Step 1** Log in to your Orchestrator.
- Step 2** From the left navigation pane, select **Admin > System Configuration**.
- Step 3** Click the **Edit** icon to the right of the **System Alias & Banners** area.
This opens the **System Alias & Banners** settings window.
- Step 4** In the **Alias** field, specify the system alias.
- Step 5** Choose whether you want to enable the GUI banner.

- Step 6** If you enable the banner, you must provide the message that will be displayed on it.
- Step 7** If you enable the banner, you must choose the severity, or color, for the banner.
- Step 8** Click **Save** to save the changes.
-

Login Attempts and Lockout Time

When the Orchestrator detects a significant number of failed consecutive login attempts, the user is locked out of the system to prevent unauthorized access. You can configure how failed log in attempts are treated, for example the number of failed attempts before lockout and the length of the lockout.



Note This feature is enabled by default when you first install or upgrade to Release 2.2(1) or later.

- Step 1** Log in to your Orchestrator.
- Step 2** From the left navigation pane, select **Admin > System Configuration**.
- Step 3** Click the **Edit** icon to the right of the **Fail Attempts & Lockout Time** area.
This opens the **Fail Attempts & Lockout Time** settings window.
- Step 4** From the **Fail Attempt Settings** dropdown, select the number of attempts before the user is locked out.
- Step 5** From the **Lockout Time (Minutes)** dropdown, select the length of the lockout.
This specifies the base lockout duration once it's triggered. The timer is extended up to three times exponentially with every additional consecutive login failure.
- Step 6** Click **Save** to save the changes.
-



CHAPTER 7

Audit Logs

- [Audit Logs, on page 39](#)

Audit Logs

Multi-Site Orchestrator system logging is automatically enabled when you first deploy the Orchestrator cluster and captures the events and faults that occur in the environment.

You can view the Multi-Site Orchestrator logs directly in the GUI by selecting **Operations > Audit Logs** from the main navigation menu.

From the **Audit 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, 2019 to November 17, 2019 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*) 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.



CHAPTER 8

Backup and Restore

- [Configuration Backup and Restore, on page 41](#)
- [Backup and Restore Guidelines, on page 41](#)
- [Remote Backups, on page 42](#)
- [Creating Backups, on page 44](#)
- [Restoring Backups, on page 45](#)
- [Downloading Backups, on page 46](#)
- [Importing Backups, on page 46](#)

Configuration Backup and Restore

You can create backups of your Multi-Site Orchestrator configuration that can facilitate in recovering 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 Multi-Site Orchestrator nodes.



Note Restoring a backup action restores the database on the Multi-Site Orchestrator, but it does not make any changes to the controller 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 Multi-Site Orchestrator and each site's controller. For information on specific configuration mismatch scenarios and backup restore procedures related to each one, see [Backup and Restore Guidelines, on page 41](#)

Backup and Restore Guidelines

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

- Importing and restoring backups created from later releases is not supported.
For example, if you downgrade your Multi-Site Orchestrator to an earlier release, you cannot restore a backup of the configuration created on a later release.
- Restoring configuration backups created on releases prior to Release 3.2(1) is supported as a one-time step during cluster migration to Nexus Dashboard.

Subsequent restore of backups from VMware ESX or Application Services Engine deployments are not supported.

- 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 controller 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 Multi-Site Orchestrator and the 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 45](#).

Sites, Objects, or Policies Created, Modified, or Deleted Since Backup

If any configuration changes took place between the time when the configuration backup was created and the time it is being restored, consider the following:

- Restoring a backup will not modify any objects, policies, or configurations on the sites. Any new objects or policies created and deployed since the backup will remain deployed. You will need to manually remove these after restoring the backup to avoid any stale configurations.

Alternatively, you can choose to undeploy all policies first, which will avoid any potential stale objects after the configuration is restored from backup. However, this would cause a disruption in traffic or services defined by those policies.

- The steps required to restore a configuration backup are described in [Restoring Backups, on page 45](#).
- If the configuration backup you restored was saved before it was deployed to the sites, it will be restored in the `undeployed` state and you can simply deploy it to the 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 configurations will exist in the sites yet. In this case, in order for the configuration to be properly pushed to each site, you will need to re-deploy it to sync the Multi-Site Orchestrator's configuration with the sites.
- If sites that were managed when the backup was created are no longer present in the Nexus Dashboard, the restore will fail.
- If sites' status since the backup has changed (`managed` vs `unmanaged`) but the sites are still present in the Nexus Dashboard, the status will be restored to what it was at the time of backup.

Remote Backups

Multi-Site Orchestrator is deployed as an application in Nexus Dashboard. When you first deploy the cluster, any backups you create are saved to a default location which is located on each node's local disk.

While the backups are available on any one node and can be viewed using the MSO GUI, we recommend exporting all backups to a remote location outside the Nexus Dashboard nodes.

You can configure a remote SCP or SFTP location using the MSO GUI and then exporting the backup files there as described in the following sections.



Note When you create a configuration backup and export it to a remote server, the files are first created on the Orchestrators' local drives, then uploaded to the remote location, and finally deleted from the local storage. There is a limit on the local backups disk space usage, which if reached can prevent remote backups from being created.

Configuring a Remote Location for Backups

This section describes how to configure a remote location in Multi-Site Orchestrator to which you can then export your configuration backups.

Step 1 Log in to your Multi-Site Orchestrator.

Step 2 From the left navigation pane, select **Operations > Remote Locations**.

Step 3 In the top right of the main window, click **Add Remote Location**.

An **Add New Remote Location** screen appears.

Step 4 Provide the name for the location and an optional description.

Two protocols are currently supported for remote export of configuration backups:

- SCP
- SFTP

Note SCP is supported for non-Windows servers only. If your remote location is a Windows server, you must use the SFTP protocol

Step 5 Specify the host name or IP address of the remote server.

Based on your **Protocol** selection, the server you specify must allow SCP or SFTP connections.

Step 6 Provide the full path to a directory on the remote server where you will save the backups.

The path must start with a slash (/) characters and must not contain periods (.) or backslashes (\). For example, */backups/multisite*.

Note The directory must already exist on the remote server.

Step 7 Specify the port used to connect to the remote server.

By default, port is set to 22.

Step 8 Specify the authentication type used when connecting to the remote server.

You can configure one of the following two authentication methods:

- `Password`—provide the username and password used to log in to the remote server.
- `SSH Private Files`—provide the username and the SSH Key/Passphrase pair used to log in to the remote server.

Step 9 Click **Save** to add the remote server.

Moving Existing Backups to a Remote Location

This section describes how to move an existing configuration backup you have created in the Multi-Site Orchestrator GUI from the nodes' local drives to a remote location.

Before you begin

You must have completed the following:

- Created a configuration backup as described in [Creating Backups, on page 44](#).
 - Added a remote location for exporting backups as described in [Configuring a Remote Location for Backups, on page 43](#).
-

Step 1 Log in to your Multi-Site Orchestrator.

Step 2 From the left navigation pane, select **Operations > Backups & Restore**.

Step 3 Locate the backup you want to export, then click the actions (...) icon next to it, then click **Move to remote location**.
A **Move Backup To Remote Location** window opens.

Step 4 From the **Remote Location** dropdown menu, select the remote location.

Step 5 (Optional) Update the remote location path.

The target directory on the remote server, which you configured when creating the remote backup location, will be displayed in the **Remote Path** field.

You can choose to append additional subdirectories to the path. However, the directories must be under the default configured path and must have been already created on the remote server.

Creating Backups

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

Before you begin

If you want to create the backup using a remote location, you must first add the remote location as described in [Configuring a Remote Location for Backups, on page 43](#).

Step 1 Log in to your Multi-Site Orchestrator.

Step 2 Create a new backup.

- a) From the left navigation pane, select **Operations > Backups & Restore**.
- b) In the main window, click **New Backup**.

A **New Backup** window opens.

Step 3 Provide backup information.

- a) Provide the **Name** and optional **Notes** for the backup.

The name can contain up to 10 alphanumeric characters, but no spaces or underscores (_).

- b) Choose the **Backup Location**.

You can save the backup file locally on the Orchestrator nodes or export it to a remote location.

If you want to save the backup file locally, choose **Local**.

Otherwise, if you want to save the backup file to a remote location, choose **Remote** and provide the following:

- From the **Remote Location** dropdown menu, select the remote location.

The remote location must be already created as described in [Configuring a Remote Location for Backups](#), on page 43.

- In the **Remote Path**, either leave the default target directory or you can choose to append additional subdirectories to the path. However, the directories must be under the default configured path and must have been already created on the remote server.

- c) 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 controller databases on each site. Therefore, after you restore the Multi-Site Orchestrator database, you must also re-deploy any existing schemas to avoid potentially mismatching policies between the Multi-Site Orchestrator and sites.

For information on specific configuration mismatch scenarios and recommended restore procedures related to each one, see [Backup and Restore Guidelines](#), on page 41.

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 41.

Step 3 From the left navigation menu, select **Operations > Backups & Restore**.

Step 4 In the main window, click the actions (...) icon 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.

Note If your Multi-Site Orchestrator cluster is deployed in Application Services Engine, multiple services are restarted during the configuration restore process. As a result, you may notice an up to 5 minute delay before the restored configuration is properly reflected in the MSO GUI.

Step 6 If necessary, redeploy the configuration.

We recommend you perform this step to sync the restored configuration with the sites. Additional context is available in [Backup and Restore Guidelines, on page 41](#).

Downloading Backups

This section describes how to download your 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 **Operations > Backups & Restore**.

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

This will download the backup file in `msc-backups-<timestamp>.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 **Operations > Backups & Restore**.

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.



CHAPTER 9

Tech Support

- [Tech Support and System Logs](#), on page 47
- [Downloading System Logs](#), on page 47
- [Streaming System Logs to External Analyzer](#), on page 48

Tech Support and System Logs

Multi-Site Orchestrator system logging is automatically enabled when you first deploy the Orchestrator cluster and captures the events and faults that occur in the environment.

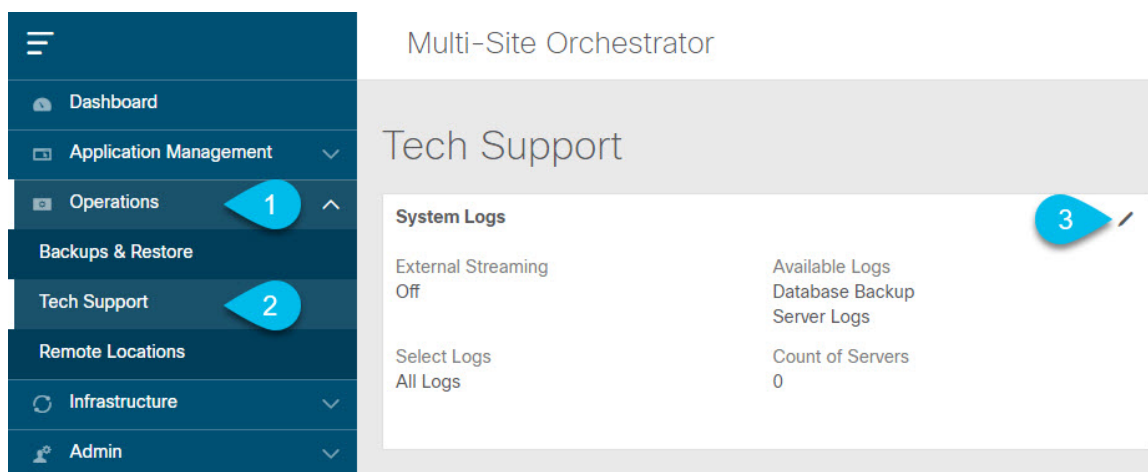
You can choose to download the logs at any time or stream them to an external log analyzer, such as Splunk, if you want to use additional tools to quickly parse, view, and respond to important events without a delay.

Downloading System 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 Multi-Site Orchestrator.

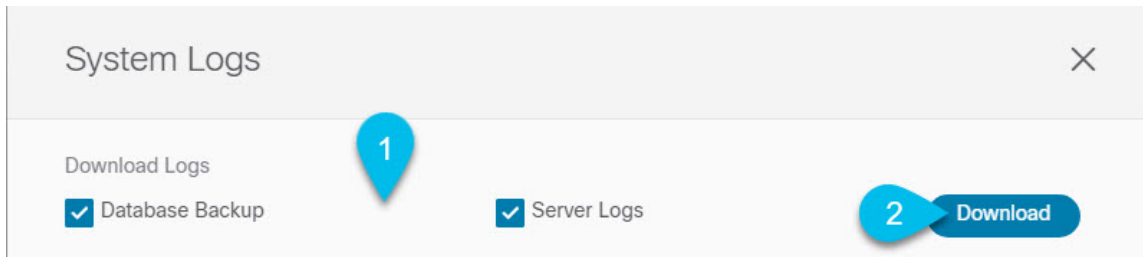
Step 1 Log in to your Multi-Site Orchestrator GUI.

Step 2 Open the **System Logs** screen.



- a) In the main menu, select **Operations > Tech Support**.
- b) In the top right corner of the **System Logs** frame, click the edit button.

Step 3 Download the logs.



- a) Select which logs you want to download.
- b) Click the **Download** button.

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

Streaming System Logs to External Analyzer

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-Site Orchestrator to stream its logs to an external analyzer tool, such as Splunk or syslog.

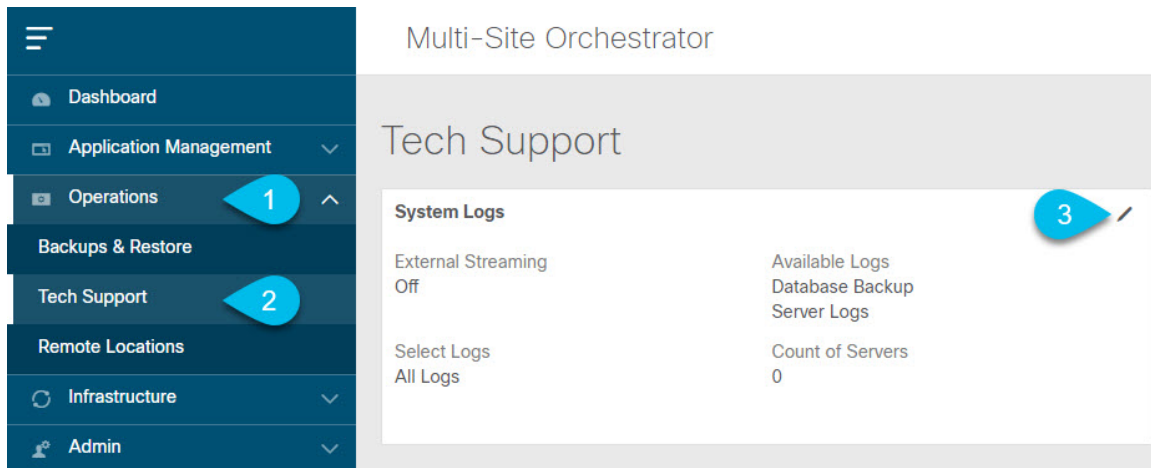
Before you begin

- This release supports only Splunk and `syslog` as external log analyzer.
- This release supports `syslog` only for Multi-Site Orchestrator in Application Services Engine deployments.
- This release supports up to 5 external servers.
- If using Splunk, set up and configure the log analyzer service provider.
For detailed instructions on how to configure an external log analyzer, consult its documentation.
- If using Splunk, 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**.

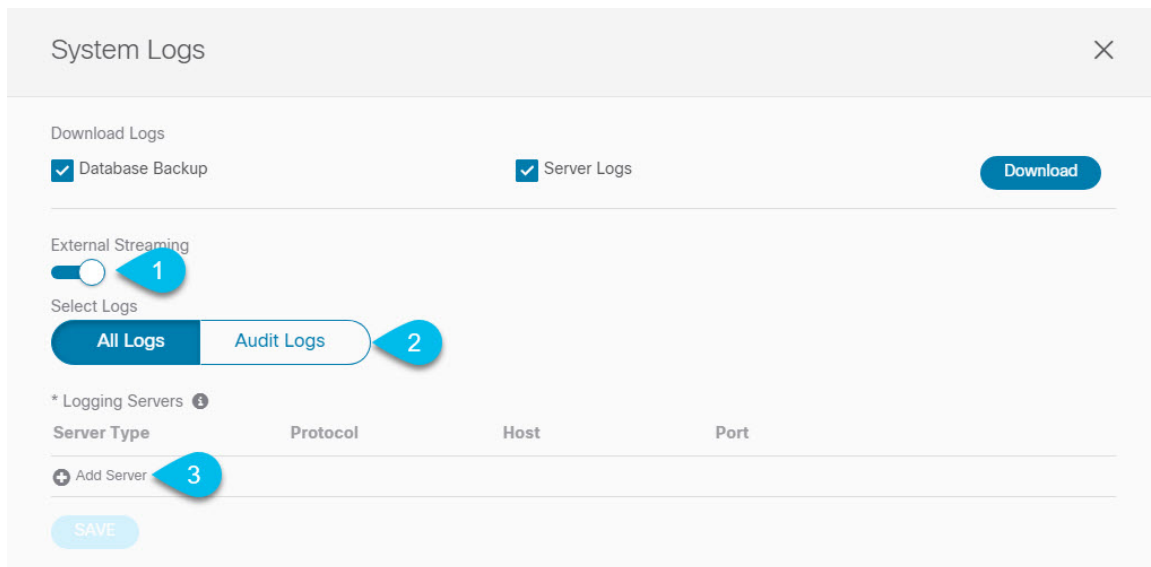
Step 1 Log in to your Multi-Site Orchestrator GUI.

Step 2 Open the **System Logs** screen.



- In the main menu, select **Operations > Tech Support**.
- In the top right corner of the **System Logs** frame, click the edit button.

Step 3 In the **System Logs** window, enable external streaming and add a server.



- Enable the **External Streaming** knob.
- Choose whether you want to stream **All Logs** or just the **Audit Logs**.
- Click **Add Server** to add an external log analyzer server.

Step 4 Add a Splunk server.

If you do not plan to use Splunk service, skip this step.

The screenshot shows a configuration form for adding a Splunk server. The form includes the following fields and options:

- Select Service:** A dropdown menu with "splunk" selected. A blue callout bubble with the number "1" points to the dropdown arrow.
- Protocol:** Two radio buttons, "HTTP" (selected) and "HTTPS". A blue callout bubble with the number "2" points to the "HTTPS" button.
- * Host:** A text input field containing "10.30.11.69". A vertical blue line is positioned to the right of this field, with a blue callout bubble with the number "3" pointing to it.
- * Port:** A text input field containing "8088".
- * Token:** A text input field containing "2824ec94-fbce-4111-954f-e8df0c9cfcb5".
- Confirmation:** A checkmark icon and a close icon are located in the top right corner. A blue callout bubble with the number "4" points to the checkmark icon.

- Choose `splunk` for the server type.
- Choose the protocol.
- Provide the server name or IP address, port, and the authentication token you obtained from the Splunk service.

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**.

- Click the checkmark icon to finish adding the server.

Step 5

Add a `syslog` server.

If you do not plan to use `syslog`, skip this step.

The screenshot shows a configuration form for adding a syslog server. The form includes the following fields and options:

- Select Service:** A dropdown menu with "syslog" selected. A blue callout bubble with the number "1" points to the dropdown arrow.
- Protocol:** Two radio buttons, "TCP" (selected) and "UDP". A blue callout bubble with the number "2" points to the "UDP" button.
- * Host:** A text input field containing "10.195.223.220". A vertical blue line is positioned to the right of this field, with a blue callout bubble with the number "3" pointing to it.
- * Port:** A text input field containing "514".
- Severity:** A dropdown menu with "Warning" selected. A blue callout bubble with the number "4" points to the checkmark icon in the top right corner.

- Choose `syslog` for the server type.

- b) Choose the protocol.
- c) Provide the server name or IP address, port number, and the severity level of the log messages to stream.
- d) Click the checkmark icon to finish adding the server.

Step 6 Repeat the steps if you want to add multiple servers.

This release supports up to 5 external servers.

Step 7 Click **Save** to save the changes.

System Logs ×

Download Logs

Database Backup Server Logs Download

External Streaming

Select Logs

All Logs Audit Logs

* Logging Servers ⓘ

| Server Type | Protocol | Host | Port | |
|-------------|----------|----------------|------|---|
| splunk | http | 10.30.11.69 | 8088 | ✖ |
| syslog | tcp | 10.195.223.220 | 514 | ✖ |

+ Add Server

SAVE



CHAPTER 10

Upgrading or Downgrading MSO Application

- [Overview, on page 53](#)
- [Prerequisites and Guidelines, on page 53](#)
- [Upgrading MSO Application Using Cisco App Store, on page 54](#)
- [Upgrading MSO Application Manually, on page 56](#)
- [Downgrading MSO Application, on page 58](#)

Overview

The following sections describe how to upgrade or downgrade Cisco Multi-Site Orchestrator, Release 3.2(1) or later that is deployed in Cisco Nexus Dashboard.

If you are running an earlier release deployed in VMware ESX VMs or Cisco Application Services Engine, you must deploy a brand new cluster and then transfer the configuration from your existing cluster, as described in the "Migrating Existing Cluster to Nexus Dashboard" chapter of the [Multi-Site Orchestrator Deployment Guide](#).

Prerequisites and Guidelines

Before you upgrade or downgrade your Cisco Multi-Site Orchestrator cluster:

- Stateful upgrades from releases prior to Release 3.2(1) are not supported and you would need to re-deploy the cluster and restore existing configuration backup.
- Ensure that your current Nexus Dashboard cluster is healthy.

You can check the Nexus Dashboard cluster health in one of two ways:

- By logging into your Nexus Dashboard GUI and verifying system status in the **System Overview** page.
- By logging into any one of the nodes directly as `rescue-user` and running the following command:

```
# acs health
All components are healthy
```

- Ensure that your current Cisco Multi-Site Orchestrator is running properly.
- You can upgrade the MSO application in one of two ways:

- Using the Nexus Dashboard's App Store, as described in [Upgrading MSO Application Using Cisco App Store, on page 54](#).

In this case, the Cisco DC App Center must be reachable from the Nexus Dashboard via the Management Network directly or using a proxy configuration. Nexus Dashboard proxy configuration is described in the *Nexus Dashboard User Guide*.

Note that the App Store allows you to upgrade to the latest available version of the application only.

- By manually uploading the new app image, as described in this section, as described in [Upgrading MSO Application Manually, on page 56](#).

You can use this approach if you are unable to establish the connection to the DC App Center or if you want to upgrade to a version of the application that is not the latest available release.

- The downgrade workflow is similar to the manual upgrade process and is described in [Downgrading MSO Application, on page 58](#).

- Downgrading to releases prior to Release 3.2(1) is not supported.

If you want to downgrade to an earlier release, you must deploy a new Multi-Site Orchestrator cluster on a platform supported by that release, then restore the older configuration backup. Restoring backups created on Release 3.2(1) or later to an older MSO cluster is not supported.

Upgrading MSO Application Using Cisco App Store

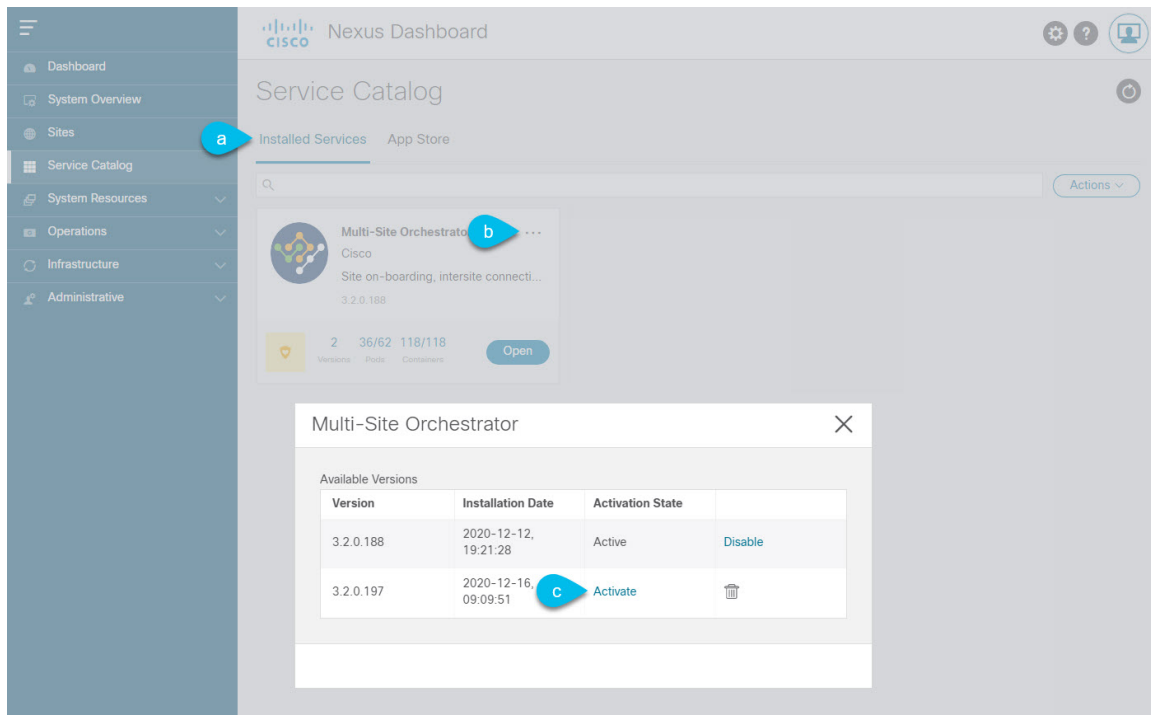
This section describes how to upgrade Cisco Multi-Site Orchestrator, Release 3.2(1) or later.

Before you begin

- Ensure that you have completed the prerequisites described in [Prerequisites and Guidelines, on page 53](#).
- Ensure that Cisco DC App Center is reachable from the Nexus Dashboard via the Management Network directly or using a proxy configuration.

Nexus Dashboard proxy configuration is described in the *Nexus Dashboard User Guide*

-
- Step 1** Log in to your Nexus Dashboard..
- Step 2** From the left navigation menu, select **Service Catalog**.
- Step 3** Upgrade the application using the App Store.
- a) In the **Service Catalog** screen, select the **App Store** tab.
 - b) In the **Multi-Site Orchestrator** tile, click **Upgrade**.
 - c) In the License Agreement window that opens, click **Agree and Download**.
- Step 4** Wait for the new image to initialize.
- It may take up to 20 minutes for the new application image to become available.
- Step 5** Activate the new image.



- In the **Service Catalog** screen, select the **Installed Services** tab.
- In the top right of the Multi-Site Orchestrator tile, click the menu (. . .) and choose **Available Versions**.
- In the available versions window, click **Activate** next to the new image.

Note Do not **Disable** the currently running image before activating the new image. The image activation process will recognize the currently running image and perform the upgrade workflows necessary for the currently running app version.

It may take up to 20 additional minutes for all the application services to start and the GUI to become available. The page will automatically reload when the process is completed.

Step 6 (Optional) Delete the old application image.

You can choose to retain the old application version in case you ever want to downgrade. Or you can delete it as described in this step.

- In the **Service Catalog** screen, select the **Installed Services** tab.
- In the top right of the Multi-Site Orchestrator tile, click the menu (. . .) and choose **Available Versions**.
- In the available versions window, click the delete icon next to the image you want to delete.

It may take up to 20 additional minutes for all the application services to start and the GUI to become available. The page will automatically reload when the process is completed.

Step 7 Launch the app.

To launch the app, simply click **Open** on the application tile in the Nexus Dashboard's **Service Catalog** page.

The single sign-on (SSO) feature allows you to log in to the application using the same credentials as you used for the Nexus Dashboard.

Upgrading MSO Application Manually

This section describes how to upgrade Cisco Multi-Site Orchestrator, Release 3.2(1) or later.

Before you begin

- Ensure that you have completed the prerequisites described in [Prerequisites and Guidelines, on page 53](#).

Step 1 Download the target release image.

- a) Browse to the Multi-Site Orchestrator application DC App Center page: <https://dcappcenter.cisco.com/multi-site-orchestrator.html>.
- b) From the **Version** dropdown, choose the version you want to install and click **Download**.
- c) Accept the license agreement and download the image.

Step 2 Log in to your Nexus Dashboard..

Step 3 Upload the image to your Nexus Dashboard.

- a) From the left navigation menu, select **Service Catalog**.
- b) In the Nexus Dashboard's **Service Catalog** screen, select the **Installed Services** tab.
- c) From the **Actions** menu in the top right of main pane, select **Upload App**.
- d) In the **Upload App** window, choose the location of the image

If you downloaded the application image to your system, choose **Local**.

If you are hosting the image on a server, choose **Remote**.

- e) Choose the file.

If you chose **Local** in the previous substep, click **Select File** and select the app image you downloaded.

If you chose **Remote**, provide the full URL to the image file, for example

```
http://<ip-address>:<port>/<full-path>/cisco-mso-<version>.aci.
```

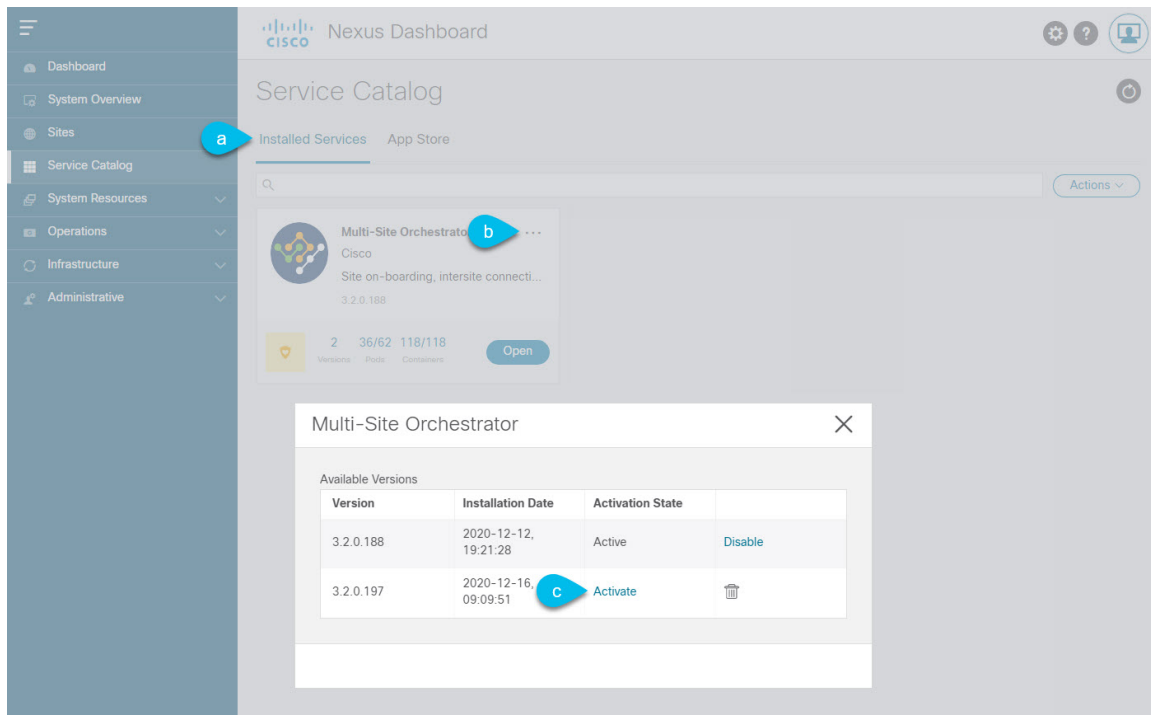
- f) Click **Upload** to add the app to the cluster.

A new tile will appear with the upload progress bar. Once the image upload is completed, the Nexus Dashboard will recognize the new image as an existing application and add it as a new version.

Step 4 Wait for the new image to initialize.

It may take up to 20 minutes for the new application image to become available.

Step 5 Activate the new image.



- In the **Service Catalog** screen, select the **Installed Services** tab.
- In the top right of the Multi-Site Orchestrator tile, click the menu (. . .) and choose **Available Versions**.
- In the available versions window, click **Activate** next to the new image.

Note Do not **Disable** the currently running image before activating the new image. The image activation process will recognize the currently running image and perform the upgrade workflows necessary for the currently running app version.

It may take up to 20 additional minutes for all the application services to start and the GUI to become available. The page will automatically reload when the process is completed.

Step 6 (Optional) Delete the old application image.

You can choose to retain the old application version in case you ever want to downgrade. Or you can delete it as described in this step.

- In the **Service Catalog** screen, select the **Installed Services** tab.
- In the top right of the Multi-Site Orchestrator tile, click the menu (. . .) and choose **Available Versions**.
- In the available versions window, click the delete icon next to the image you want to delete.

It may take up to 20 additional minutes for all the application services to start and the GUI to become available. The page will automatically reload when the process is completed.

Step 7 Launch the app.

To launch the app, simply click **Open** on the application tile in the Nexus Dashboard's **Service Catalog** page.

The single sign-on (SSO) feature allows you to log in to the application using the same credentials as you used for the Nexus Dashboard.

Downgrading MSO Application

This section describes how to downgrade Cisco Multi-Site Orchestrator, Release 3.2(1) or later.

The downgrade workflow is similar to the upgrade workflow and involves uploading the target release image and switching the currently running app version to the new image as described below.

Before you begin

- Downgrading to releases prior to Release 3.2(1) is not supported.

If you want to downgrade to an earlier release, you must deploy a new Multi-Site Orchestrator cluster on a platform supported by that release, then restore the older configuration backup. Restoring backups created on Release 3.2(1) or later to an older MSO cluster is not supported.

- Ensure that you have completed the prerequisites described in [Prerequisites and Guidelines, on page 53](#)

Step 1 Download the target release image.

- a) Browse to the Multi-Site Orchestrator application DC App Center page: <https://dcappcenter.cisco.com/multi-site-orchestrator.html>.
- b) From the **Version** dropdown, choose the version you want to install and click **Download**.
- c) Accept the license agreement and download the image.

Step 2 Log in to your Nexus Dashboard..

Step 3 Upload the image to your Nexus Dashboard.

- a) From the left navigation menu, select **Service Catalog**.
- b) In the Nexus Dashboard's **Service Catalog** screen, select the **Installed Services** tab.
- c) From the **Actions** menu in the top right of main pane, select **Upload App**.
- d) In the **Upload App** window, choose the location of the image

If you downloaded the application image to your system, choose **Local**.

If you are hosting the image on a server, choose **Remote**.

- e) Choose the file.

If you chose **Local** in the previous substep, click **Select File** and select the app image you downloaded.

If you chose **Remote**, provide the full URL to the image file, for example
`http://<ip-address>:<port>/<full-path>/cisco-mso-<version>.aci.`

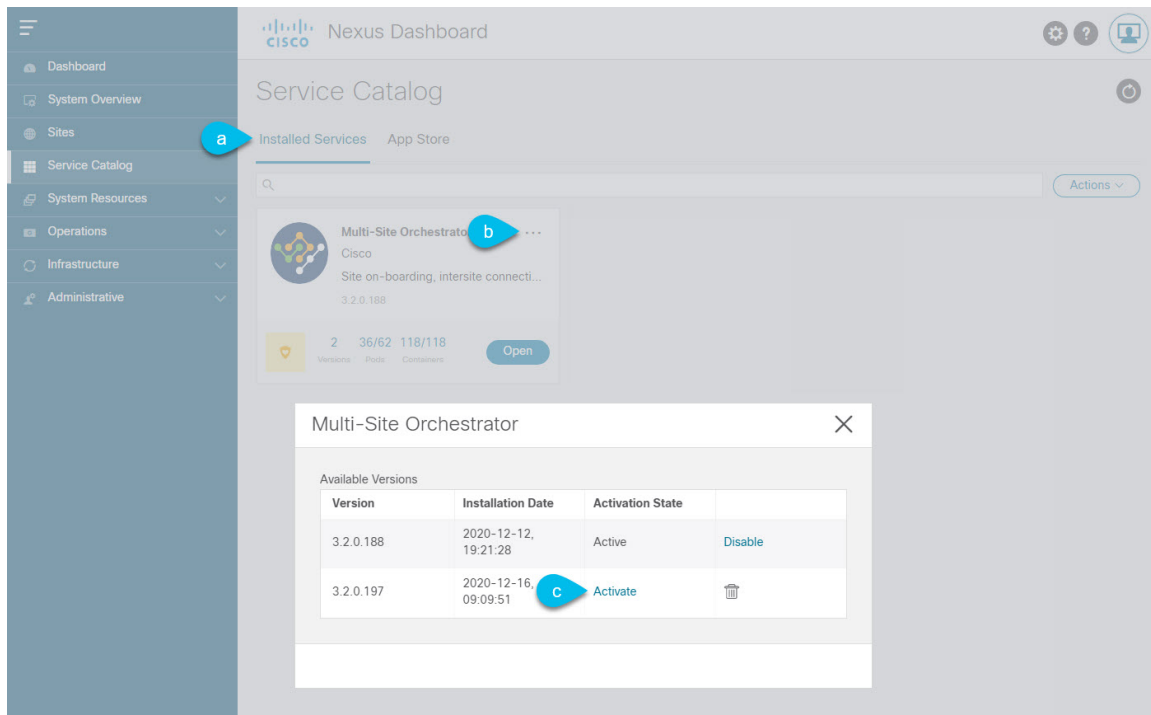
- f) Click **Upload** to add the app to the cluster.

A new tile will appear with the upload progress bar. Once the image upload is completed, the Nexus Dashboard will recognize the new image as an existing application and add it as a new version.

Step 4 Wait for the new image to initialize.

It may take up to 20 minutes for the new application image to become available.

Step 5 Activate the new image.



- In the **Service Catalog** screen, select the **Installed Services** tab.
- In the top right of the Multi-Site Orchestrator tile, click the menu (. . .) and choose **Available Versions**.
- In the available versions window, click **Activate** next to the new image.

Note Do not **Disable** the currently running image before activating the new image. The image activation process will recognize the currently running image and perform the downgrade workflows necessary for the currently running app version.

It may take up to 20 additional minutes for all the application services to start and the GUI to become available. The page will automatically reload when the process is completed.

Step 6 (Optional) Delete the old application image.

You can choose to retain the old application version in case you ever want to downgrade. Or you can delete it as described in this step.

- In the **Service Catalog** screen, select the **Installed Services** tab.
- In the top right of the Multi-Site Orchestrator tile, click the menu (. . .) and choose **Available Versions**.
- In the available versions window, click the delete icon next to the image you want to delete.

It may take up to 20 additional minutes for all the application services to start and the GUI to become available. The page will automatically reload when the process is completed.

Step 7 Launch the app.

To launch the app, simply click **Open** on the application tile in the Nexus Dashboard's **Service Catalog** page.

The single sign-on (SSO) feature allows you to log in to the application using the same credentials as you used for the Nexus Dashboard.



PART II

Features and Use Cases

- [Brownfield Import of VRFs and Networks, on page 63](#)



CHAPTER 11

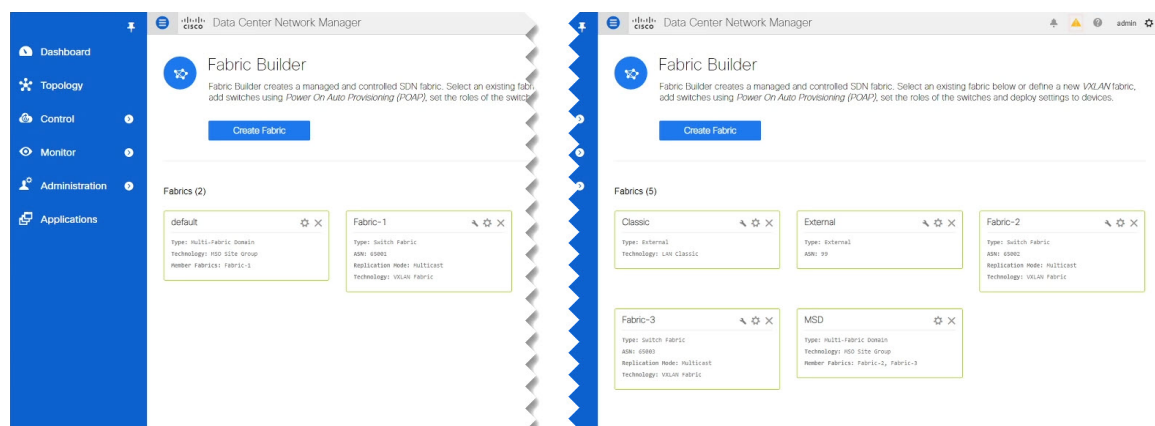
Brownfield Import of VRFs and Networks

- [Overview, on page 63](#)
- [Prerequisites, on page 64](#)
- [Create Schema and Templates for Importing Configuration, on page 65](#)
- [Importing Schema Elements From DCNM Sites, on page 66](#)
- [Deploying Template and Making Changes, on page 68](#)

Overview

The following sections describe the brownfield import use case scenario which will allow you to import existing DCNM fabric configurations, including fabrics that are part of a Multi-Site Domain (MSD), and to stretch those configurations across multiple greenfield or brownfield fabrics from a single location using Multi-Site Orchestrator. The same use case is demonstrated in the [Cisco DCNM VRF and Network Configuration using Multi-Site Orchestrator](#) video demo.

The examples in this chapter will use two different DCNM controllers where `Fabric-1` from the first DCNM is a single fabric, while `Fabric-2` and `Fabric-3` are part of an MSD and are managed by the second DCNM:



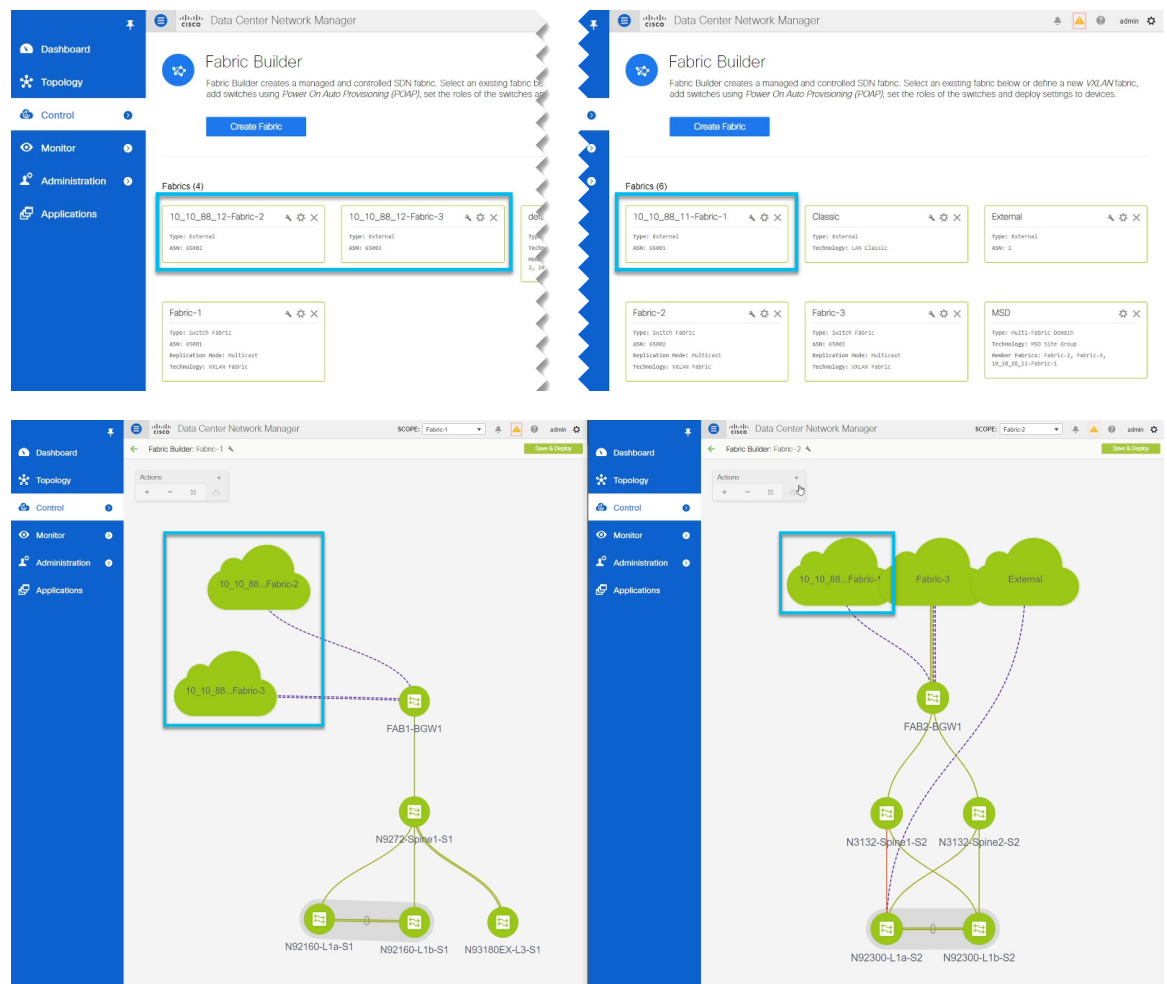
The following sections will detail how to import existing configuration, then stretch it from one fabric to another managed by different DCNMs, as well as how to deploy brand new VRFs and networks.

Prerequisites

Before you can import and manage VRFs and networks from the existing DCNM fabrics in your environment, you must have the following:

- Nexus Dashboard cluster deployed and the Multi-Site Orchestrator application installed, as described in [Cisco Nexus Dashboard Deployment Guide](#) and [Cisco Multi-Site Orchestrator Deployment Guide](#).
- Existing DCNM fabrics on-boarded in the Nexus Dashboard and enabled for management in the Multi-Site Orchestrator GUI, as described in [Adding and Deleting Sites, on page 9](#).
- Have the inter-site infrastructure configured and deployed, as described in [Configuring Infra for Cisco DCNM Sites, on page 15](#).

Expanding on the example fabrics show in the "Overview" section above, after you configure the Infra settings for all fabrics, you will see the inter-site connectivity deployed to each DCNM:



Create Schema and Templates for Importing Configuration

This section describes how to create a schema and template where you will import existing and then create new configurations.

Before you begin

- You must have reviewed and completed the prerequisites described in [Prerequisites](#), on page 64.

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

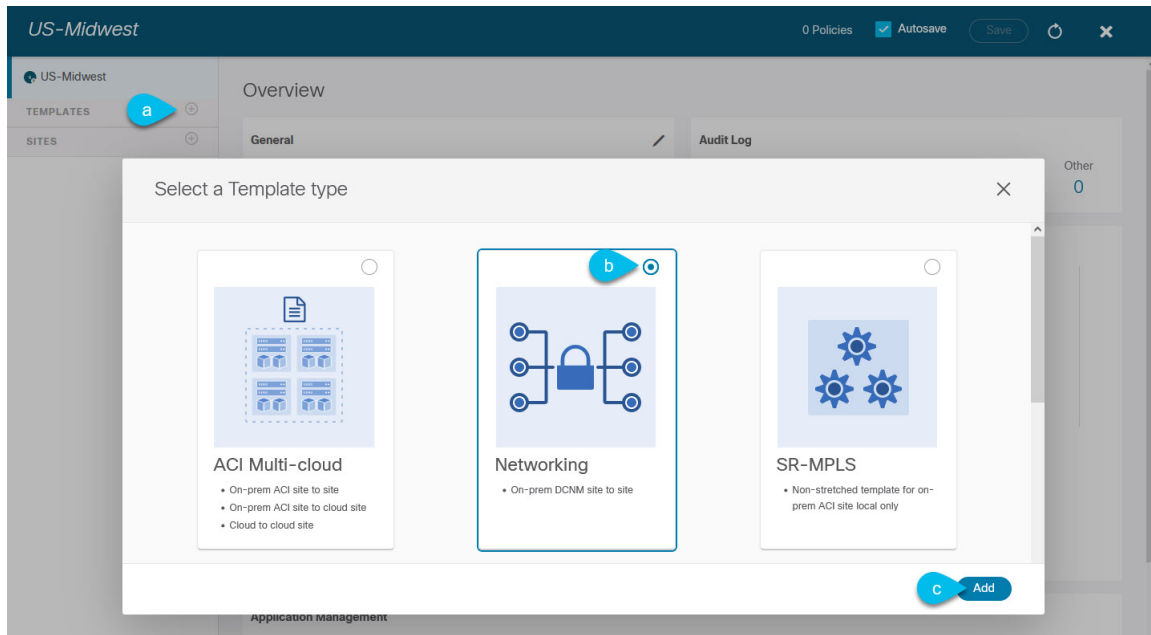
Step 2 Create a new schema.

- From the left navigation pane, choose **Application Management > Schemas**.
- On the Schemas page, click **Add Schema**.
- In the schema creation dialog, provide the **Name** and optional description for the schema.

By default, the new schema is empty, so you need to add one or more templates.

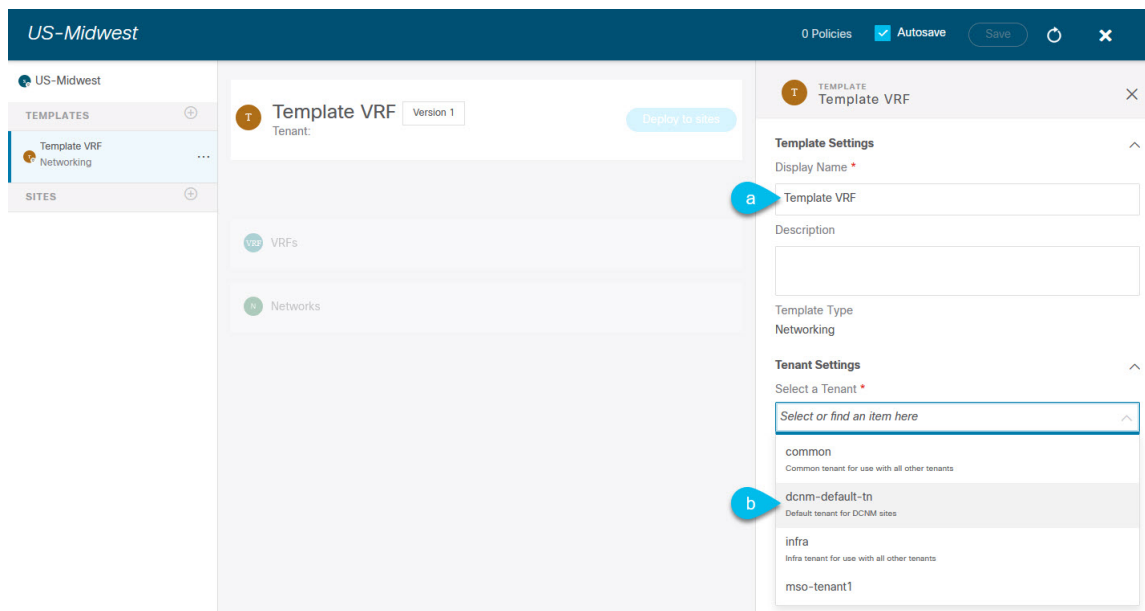
Step 3 Create a template.

We recommend creating two separate templates: one for the VRFs and one for Networks. The following two steps will describe how to create a template.



- In the left sidebar under **Templates**, click the + sign to add a new template.
- In the **Select a Template type** window, choose **Networking** for the template type.
- Click **Add** to create the template.

Step 4 Provide the name and the tenant for the template.



- a) In the right sidebar, specify the **Display Name** for the template.
- b) From the **Select a Tenant** dropdown, select the `dcnm-default-tn` tenant.

This tenant is created in MSO by default specifically for defining objects and configurations for DCNM sites

Step 5 Repeat the pervious two steps to create a second template.

In this release, we recommend creating separate templates for VRFs and Networks within each schema and then deploying the VRF templates first, followed by the templates that contain Networks. This way any VRFs required by the networks will be already created when you push Network configuration to the sites.

Similarly, when undeploying multiple networks and VRFs, we recommend undeploying the Networks template first, followed by the VRF templates. This will ensure that when VRFs are undeployed, there will be no conflicts with any existing Networks still using them.

Step 6 In the top right corner of the schema view, click **Save** to save the schema and template.

You must save the schema and template you created before you can import configuration.

Importing Schema Elements From DCNM Sites

This section describes how to import configuration from existing fabrics.

Before you begin

- You must have associated the template with the existing fabrics as described in the previous section.

Step 1 In the main pane click the **Import** button and select the **Site** from which you want to import.

You can import from one fabric at a time, so you will repeat these steps for each fabric.

Step 2 In the **Import from <site-name>** window that opens, select one or more VRFs.

a) In the import screen, you can select all or some of the existing objects.

In the example above, we import `ENG-11` and `CORP-11` networks from `Fabric-2` which is part of the MSD.

Note The names of the objects imported into the Multi-Site Orchestrator must be unique across all sites. Importing different objects with duplicate names will cause a schema validation error and the import to fail. If you want to import objects that have the same name, you must first rename them.

b) Ensure that the **Include Relations** box is unchecked.

You will import the VRFs separately into the second template.

c) Click **Import** to import the objects.

Step 3 Repeat the steps to import Networks from other fabrics.

If you select the template under the site from which you imported (`Fabric-2` in this example), the networks will have switch and port configuration already created as they were imported from that site. However, if you select the template under a different fabric (`Fabric-3`), where the same networks also exist, the switch configuration will be empty.

To get the interface configuration for the networks we imported, we import the same networks again from the other fabric.

Step 4 Select the second template and repeat previous two steps to import all required VRFs.

As best practice, you will use one of the templates to import the VRF configuration from your sites and the other template to import the Network configuration.

Deploying Template and Making Changes

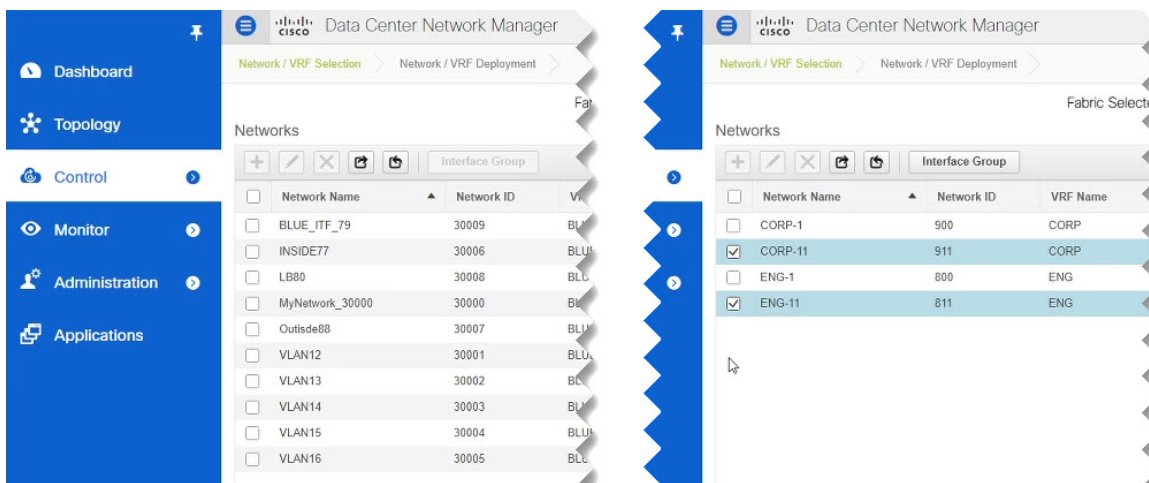
This section describes how to deploy the imported configuration to the site where it doesn't yet exist.

Before you begin

You must have the configuration imported as described in the previous section.

Step 1 In the left sidebar, select the template you want to deploy.

Following the same example, you can use the DCNM UI to verify that the networks and VRFs you have imported from Fabric-2 and Fabric-3 do not yet exist in Fabric-1.



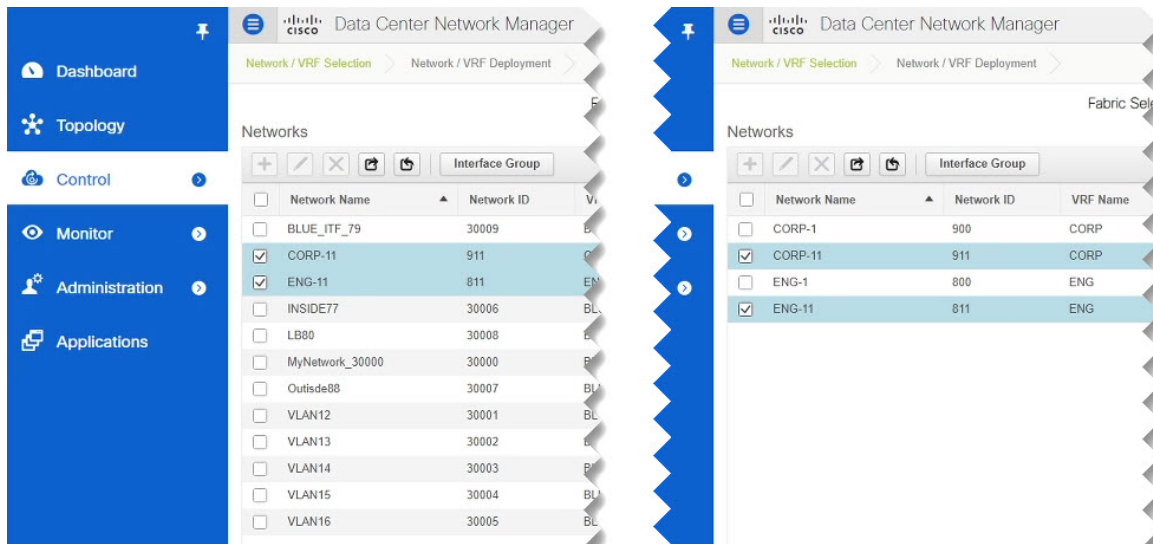
Step 2 In the top right of the template edit view, click **Deploy to sites**.

The **Deploy to Sites** window opens that shows the summary of the objects to be deployed.

Step 3 Click **Deploy** to deploy the template.

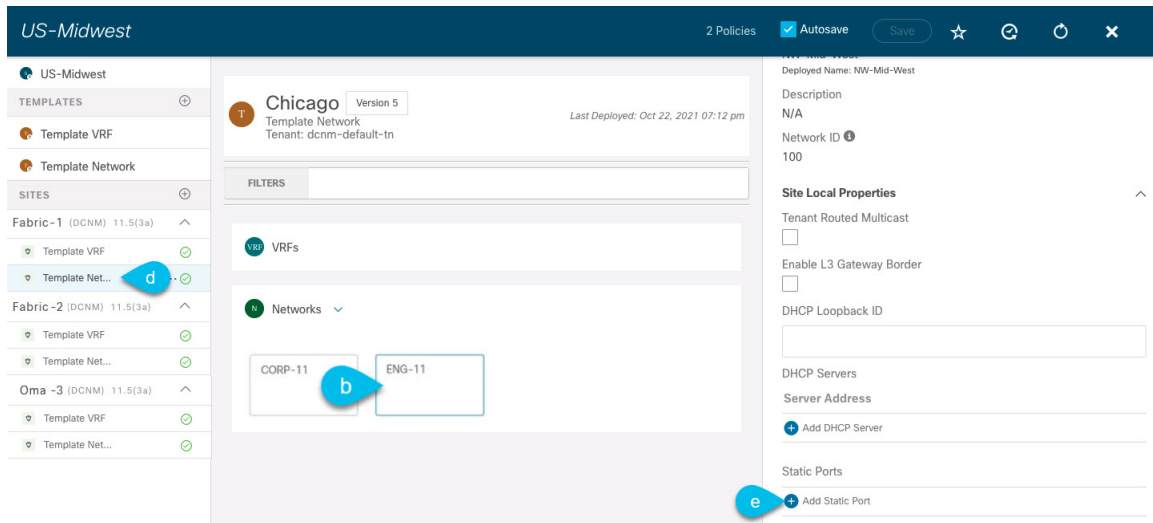
Since this is the first time you are deploying this template, the **Deploy to Sites** summary will show the configuration difference that will be deployed to sites.

It may take a few minutes for the configuration to get deployed. After you see a confirmation message in the MSO GUI, you can verify that the configuration was deployed using the DCNM UI:



Step 4 Assign switch ports to the new network.

We have verified that the network you imported from Fabric-2 and Fabric-3 was deployed to Fabric-1, we need to assign one or more switch ports to it for Fabric-1.



- a) Select the template under Fabric-1.
- b) Select the Network we deployed.
- c) In the right sidebar, click **Add Static Ports**.

In the **Add Static Port** window that opens, select the switch and the port to which you want to assign the network's VLAN. Then click **Save**.

Step 5 Save and redeploy the template with the new configuration changes.

You can once again verify the change by navigating back to the DCNM GUI and refreshing the Networks page. The status of the network will go from NA to In Progress to Deployed.

