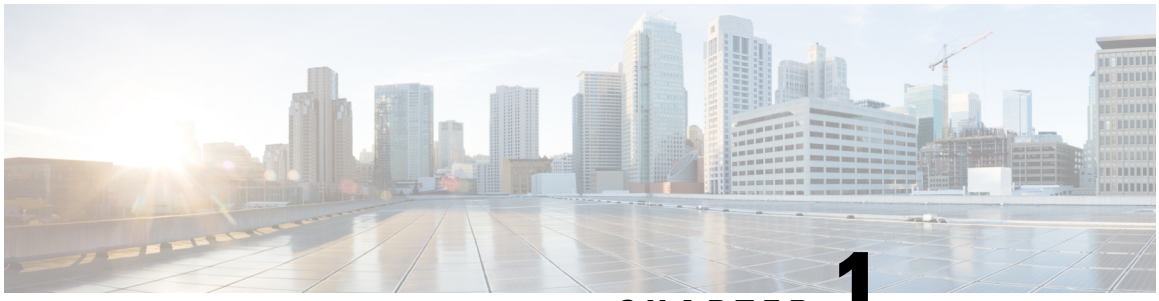
Cisco Nexus Dashboard Orchestrator Configuration Guide for DCNM Fabrics, Release 3.5(x)

First Published: 2021-09-09

Last Modified: 2021-10-15

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

CONTENTS



CHAPTER 1

New and Changed Information

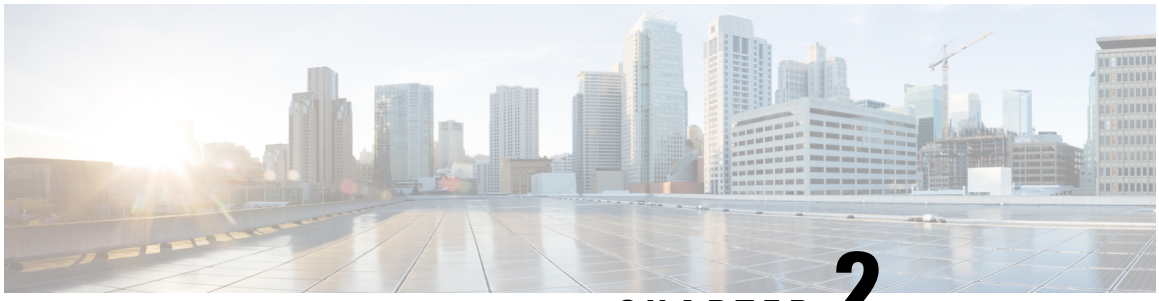
New and Changed Information

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
3.5(2)	Support for custom route targets on VRFs.	Creating VRFs, on page 27.
3.5(1)	First release of this document.	--

New and Changed Information



CHAPTER 2

GUI Overview

Overview

The Nexus Dashboard Orchestrator (NDO) 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 NDO 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 Nexus Dashboard Orchestrator, such as the currently running version, what's new in the current release, API documentation, and system status:

- The **About NDO** link displays information about the version of the Nexus Dashboard 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 Nexus Dashboard 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 NDO.

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 NDO service 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 Nexus Dashboard 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.

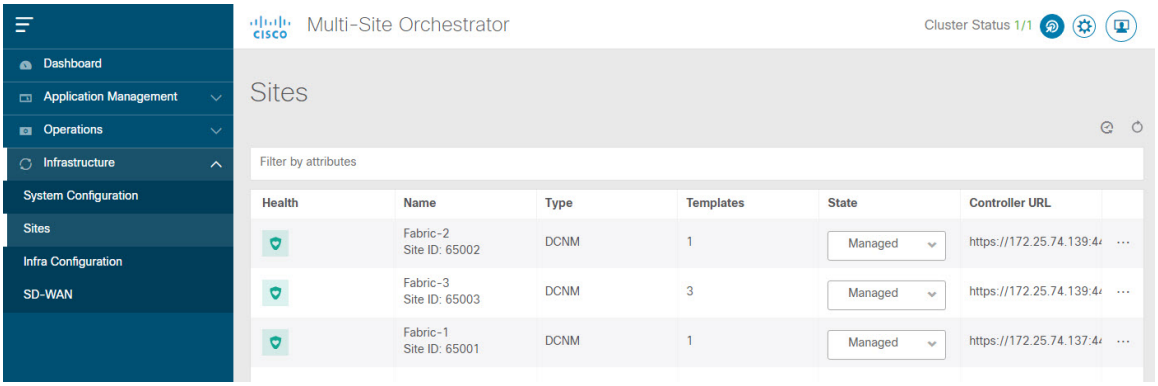
Click the **Filter** icon next to the **Most Recent** tab to filter the log details using the following criteria:

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

Figure 1: Multi-Site Sites Page

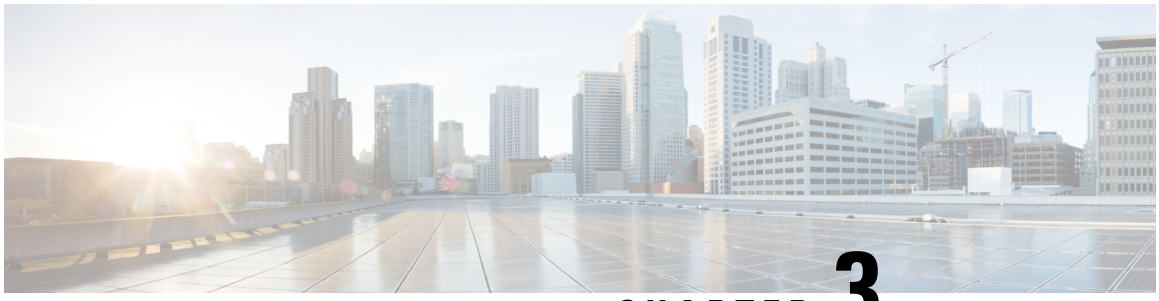


The **Sites** page includes the following:

- 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 NDO.

  You add and manage sites and their properties in the Nexus Dashboard GUI. The NDO **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 NDO.
- 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

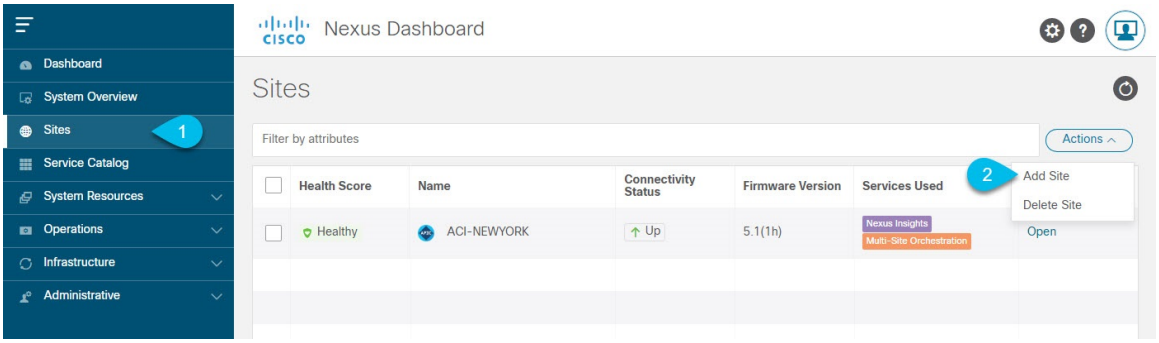
This section describes how to add a DCNM site using the Nexus Dashboard GUI and then enable that site to be managed by Nexus Dashboard Orchestrator.

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

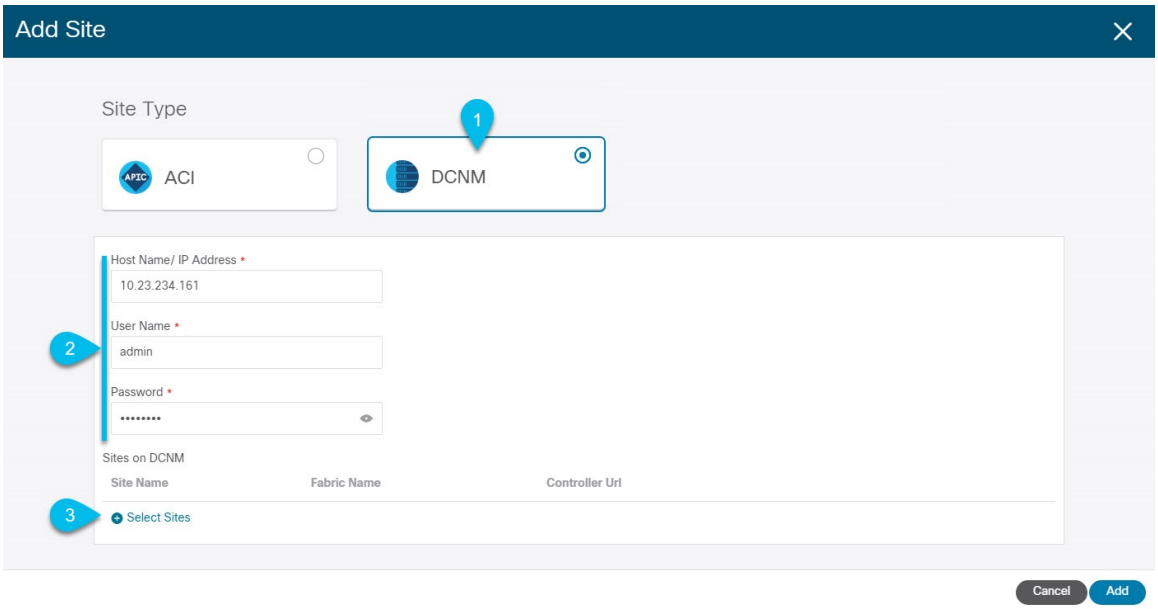
Step 2 Add a new site.



a) From the left navigation menu, select **Sites**.

b) In the top right of the main pane, select **Actions** > **Add Site**.

Step 3 Provide site information.



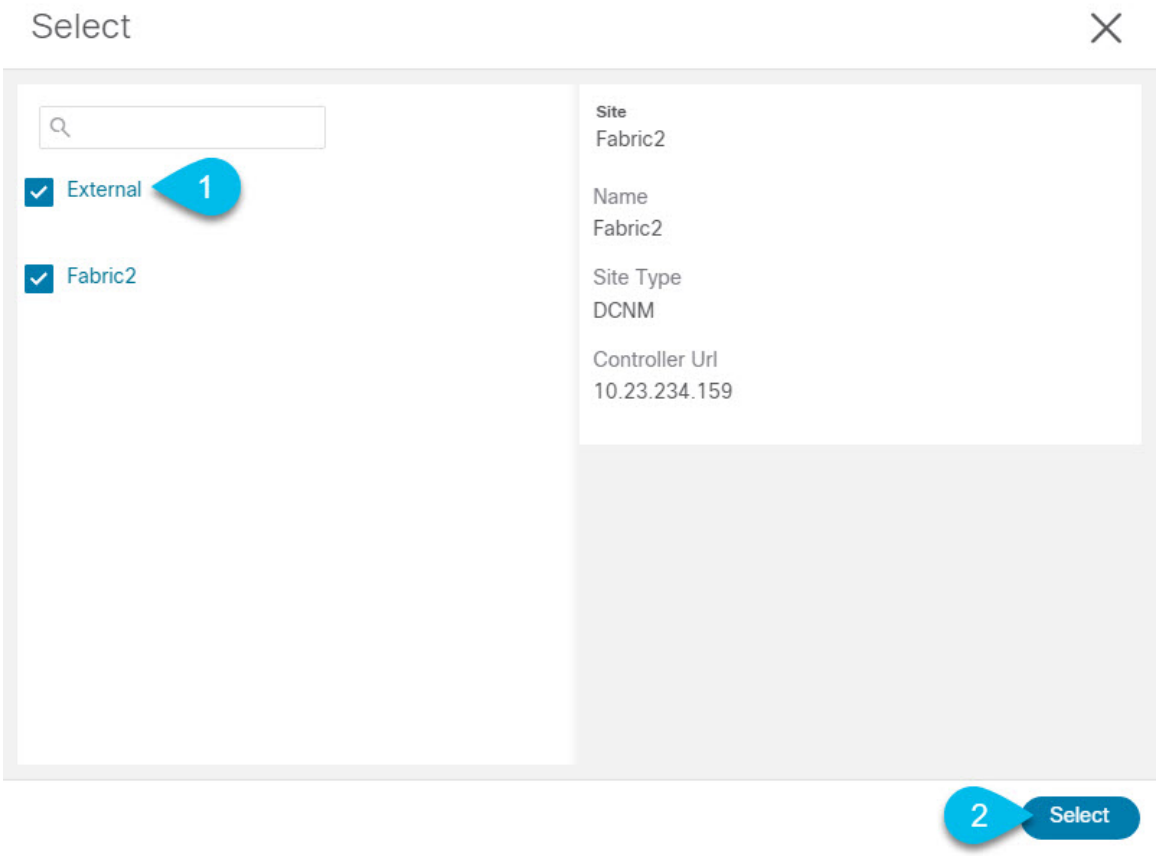
a) For **Site Type**, select **DCNM**.
b) Provide the DCNM controller information.

   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.

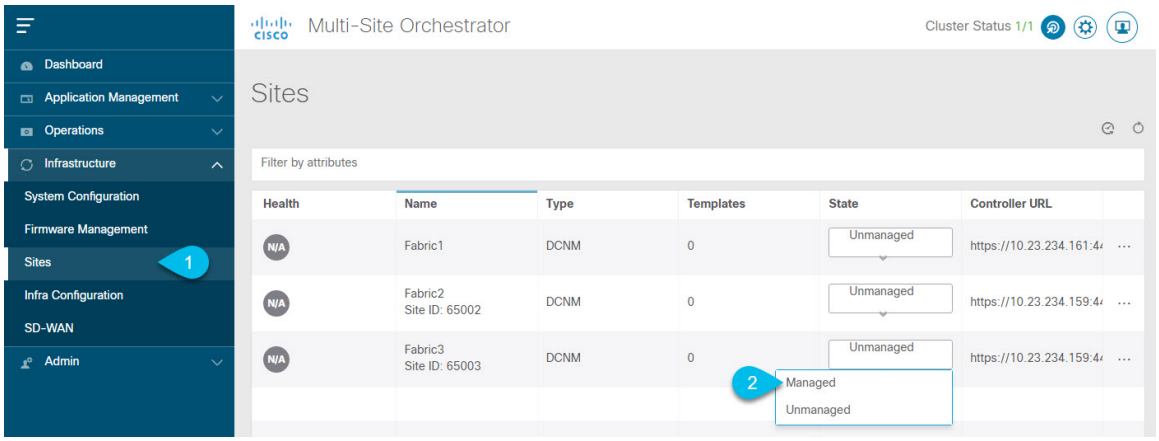
At this time, the sites will be available in the Nexus Dashboard, but you still need to enable them for Nexus Dashboard Orchestrator management as described in the folowing steps.

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

Step 7 From the Nexus Dashboard's **Service Catalog**, open the Nexus Dashboard Orchestrator service.

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

Step 8 In the Nexus Dashboard Orchestrator GUI, manage 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 NDO 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 Nexus Dashboard 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 Nexus Dashboard Orchestrator GUI.

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

Step 2 Remove the site's underlay configuration.

a) From the left navigation menu, select **Infrastructure** > **Infra Configuration**.
b) In the main pane, click **Configure Infra**.
c) In the left sidebar, select the site you want to unmanage.
d) In right bar, under **Overlay Configuration** tab, disable the **Multi-Site** knob.
e) In the right sidebar, select the **Underlay Configuration** tab.
f) Remove all underlay configurations from the site.
g) Click **Deploy** to deploy underlay and overlay configuration changes to the site.

Step 3 In the Nexus Dashboard Orchestrator GUI, disable the sites.

a) From the left navigation menu, select **Infrastructure** > **Sites**.

b) In the main pane, change the **State** from `Managed` to `Unmanaged` for each fabric that you want the NDO 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.

Step 4 Delete the site from Nexus Dashboard.

If you no longer want to manage this site or use it with any other applications, you can delete the site from the Nexus Dashboard as well.

Note Note that the site must not be currently in use by any of the applications installed in your Nexus Dashboard cluster.

a) From the left navigation menu of the Nexus Dashboard GUI, select **Sites**.

b) Select one or more sites you want to delete.

c) In the top right of the main pane, select **Actions** > **Delete Site**.

d) Provide the site's login information and click **OK**.

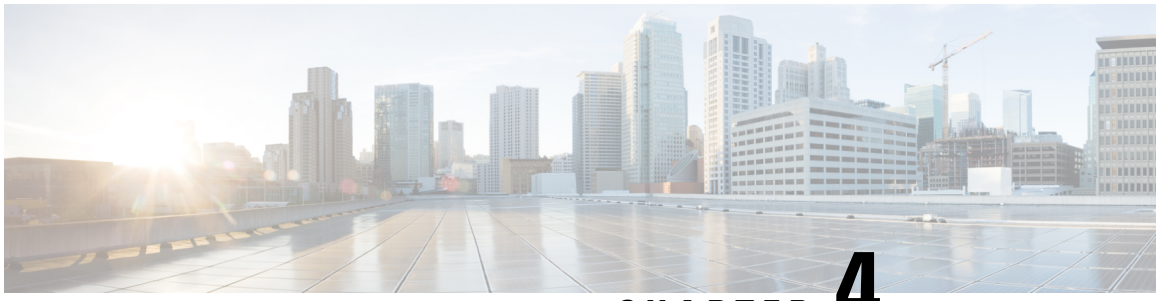
The site will be removed from the Nexus Dashboard.

Cross Launch to Fabric Controllers

Nexus Dashboard 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 NDO's **Infrastucture** > **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 the same user is configured in Nexus Dashboard and the fabric, you will be logged in automatically into the fabric's controller using the same log in information as the Nexus Dashboard user. For consistency, we recommend configuring remote authentication with common users across Nexus Dashboard and the fabrics.



CHAPTER 4

Configuring Infra for Cisco DCNM Sites

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 Nexus Dashboard 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 Nexus Dashboard 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 Configuration**.

a) Select the **Control Plane BGP** tab.

b) 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 NDO.

c) 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.

d) Leave the **Keepalive Interval (Seconds)**, **Hold Interval (Seconds)**, **Stale Interval (Seconds)**, **Graceful Helper**, **Maximum AS Limit**, and **BGP TTL Between Peers** fields at default values as they are relevant for Cisco ACI fabrics only.

e) Skip the **OSPF Area ID** and **External Subnet Pool** fields at default values as they are relevant for Cisco Cloud ACI fabrics only.

Step 6 Skip the **IPN Devices** tab settings.

The settings under the **IPN Devices** tab are for Cisco ACI inter-site connectivity between on-premises APIC and Cloud APIC sites. You can skip these settings when managing Cisco DCNM sites only.

Step 7 Configure **DCNM Settings**.

a) Select the **DCNM Settings** tab.

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

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

d) 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.

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

Refreshing Site Connectivity Information

Infrastructure changes, such as adding and removing border gateway switches, require a Nexus Dashboard 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 Nexus Dashboard 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 Nexus Dashboard 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 VIP**.

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.

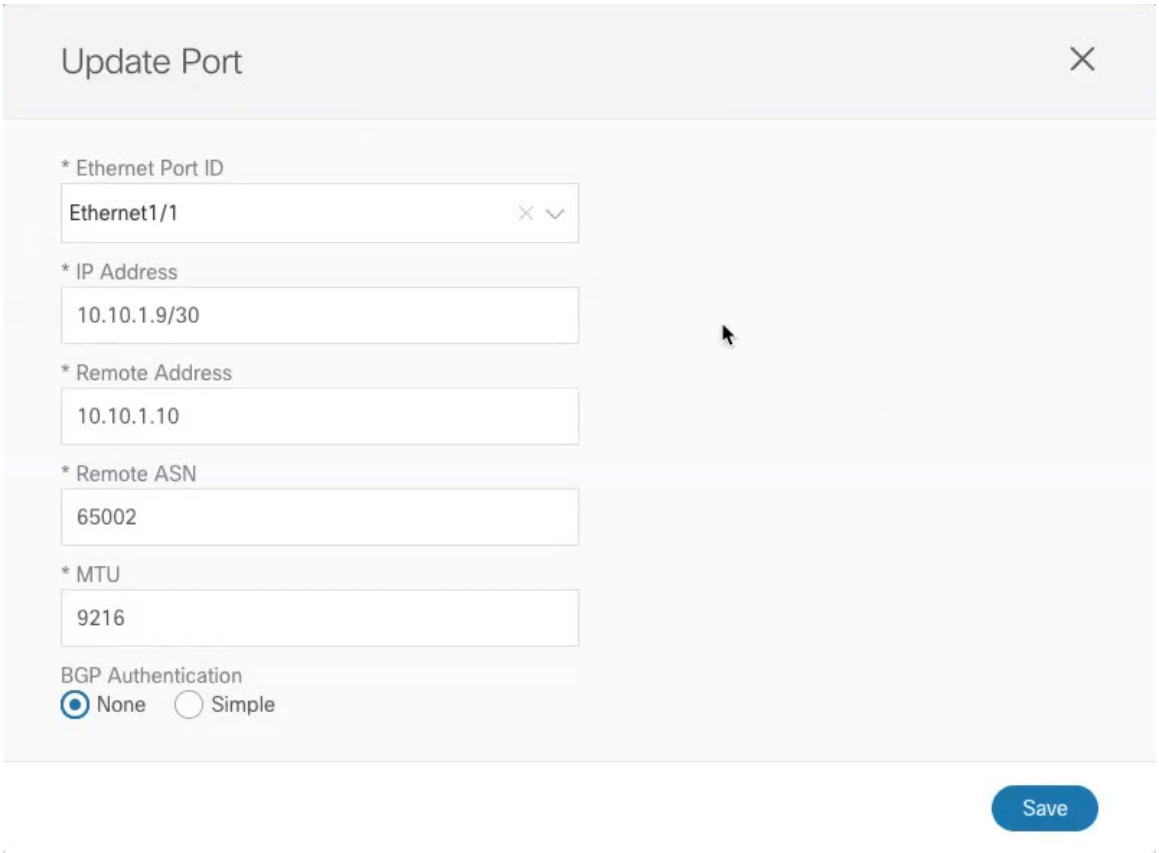
Step 6 Within the **<fabric-name>** tile, select the border gateway.

Step 7 In the right **<*border-gateway*>** setting sidebar, specify the **BGP-EVPN ROUTER-ID** and **BGW PIP**.

For border gateways that are part of a vPC domain, you must also specify a **VPC VIP**

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.



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

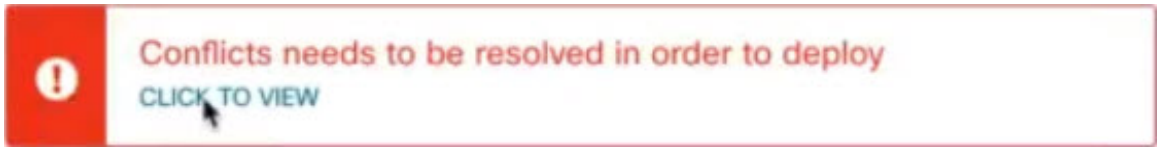
You must have the general and site-specific infra configurations completed as described in previous sections of this chapter.

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.

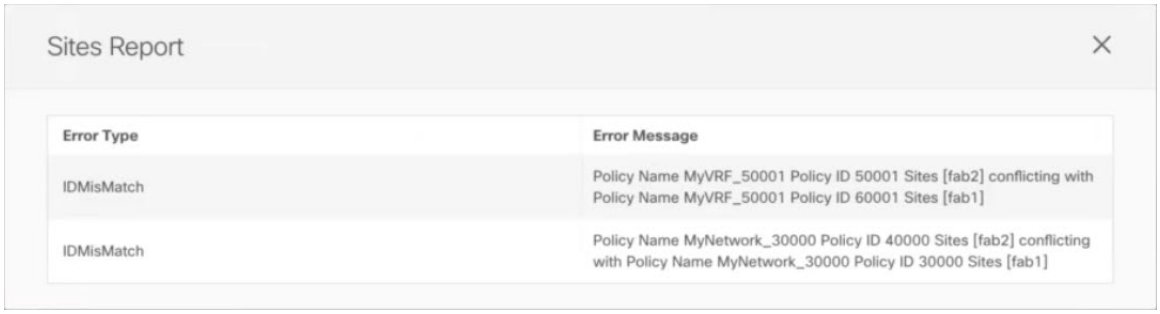
In case of configuration conflicts:

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.



c) Click the **X** button to close the report, then exit Infra configuration screen.

d) Unmanage the site in NDO, as described in Removing Sites, on page 12.

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

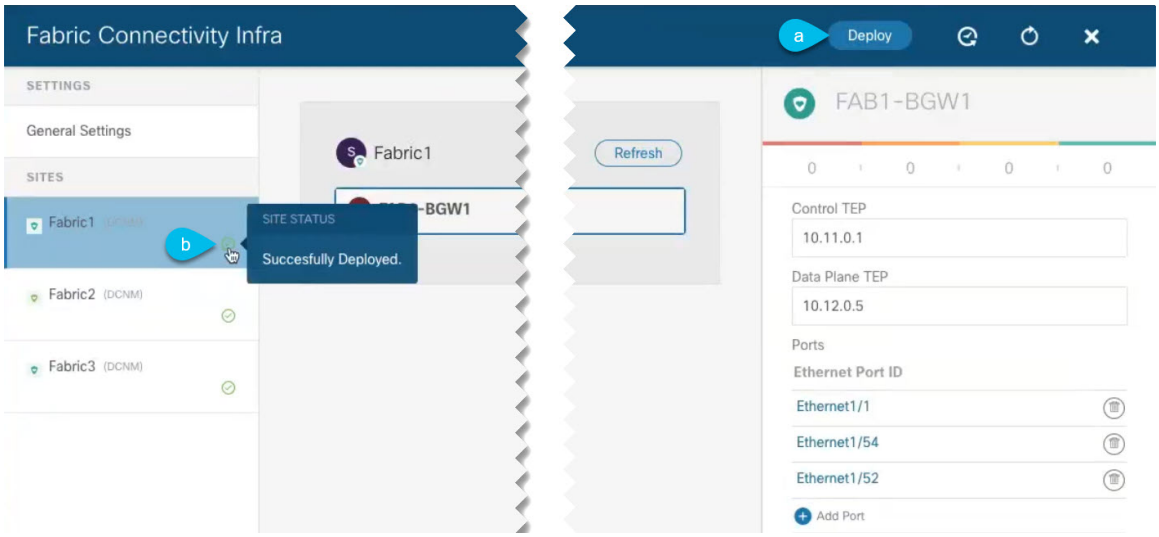
e) Resolve the existing configuration conflicts.

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 NDO.

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

Step 2 Deploy configuration.



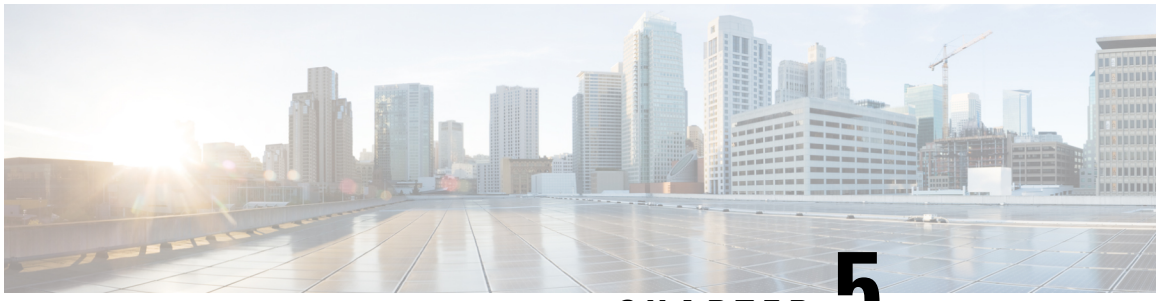
a) In the top right of the **Fabric Connectivity Infra** screen, choose the appropriate **Deploy** option to deploy the configuration.

   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, NDO 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

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 Nexus Dashboard 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 Nexus Dashboard 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 template 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; refreshing the template will lose any edits you made up to that point and you will have to make those changes again:

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 NDO 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, NDO 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.

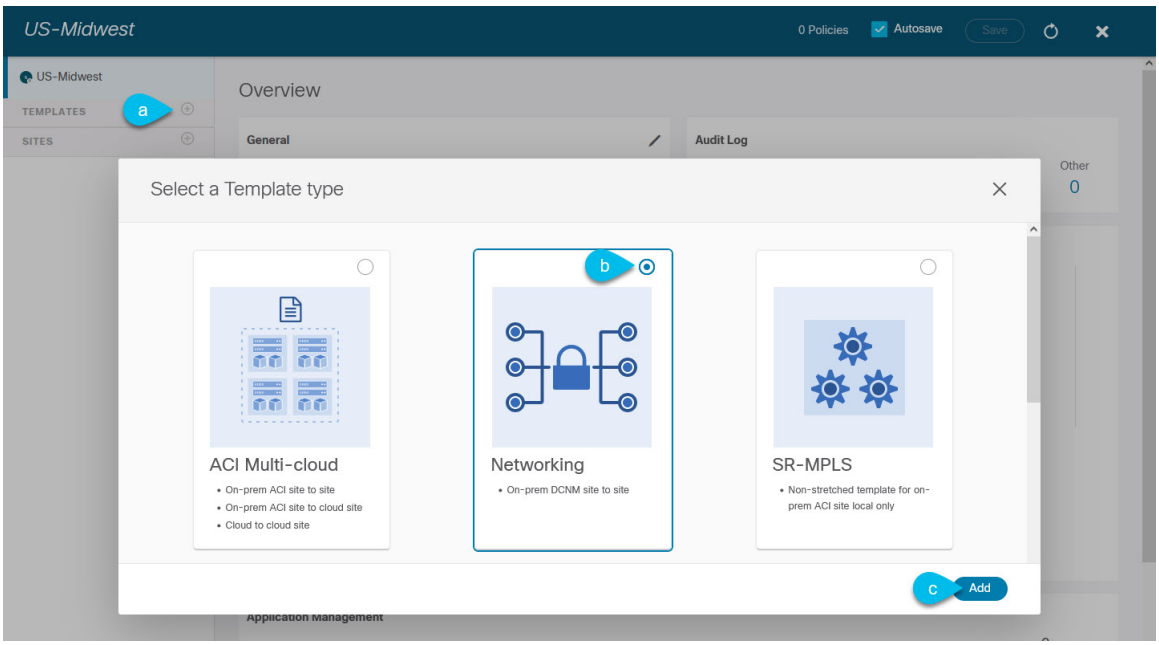
Step 1 Log in to your Nexus Dashboard Orchestrator GUI.

Step 2 Create a new schema.

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

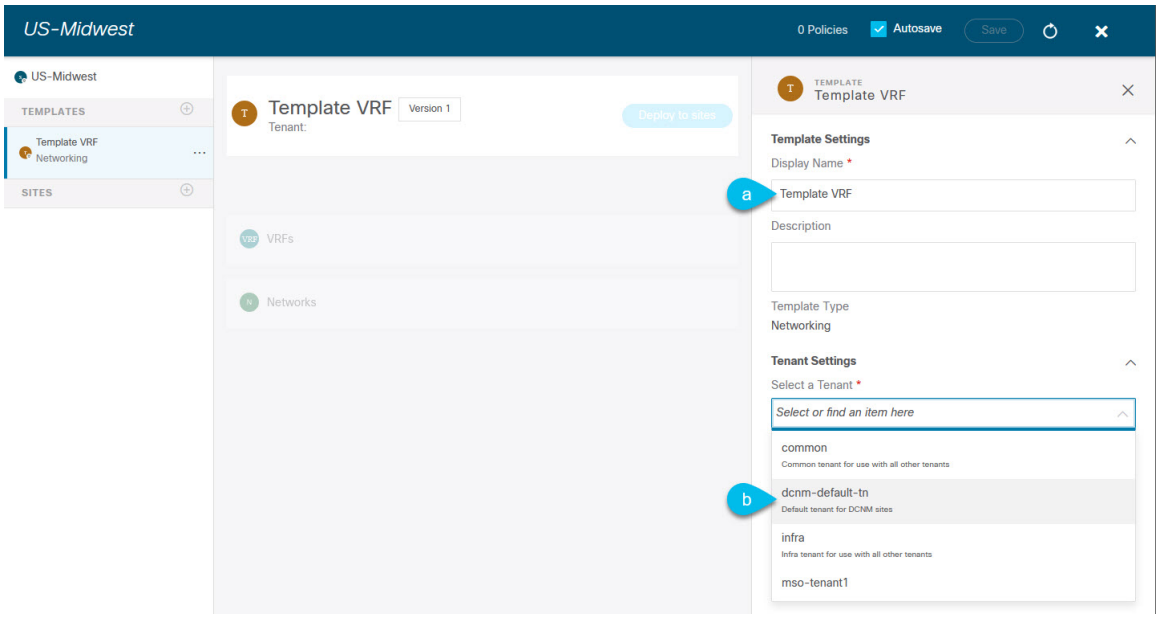
By default, the new schema is empty, so you need to add one or more templates.

Step 3 Create a template.



a) In the left sidebar under **Templates**, click the + sign to add a new template.
b) In the **Select a Template type** window, choose **Networking** for the template type.
c) 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 Nexus Dashboard 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 Nexus Dashboard 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 NDO 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 NDO 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 NDO 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.

f) (Optional) Check **Disable RT Auto-Generate** to disable automatic generation of route targets.

Note This feature is supported in Nexus Dashboard Orchestrator, Release 3.5(2) and later.

By default when this option is unchecked, the route targets (RTs) are generated by the switches and you can choose to generate custom RTs in addition to the existing auto-generated ones.If you enable this option, the automatic generation of RTs will be disabled and you can use only the custom RTs.

g) (Optional) Provide any custom route targets.

Note This feature is supported in Nexus Dashboard, Release 3.5(2) and later.

To provide custom RTs, enter one or more values for the following fields:

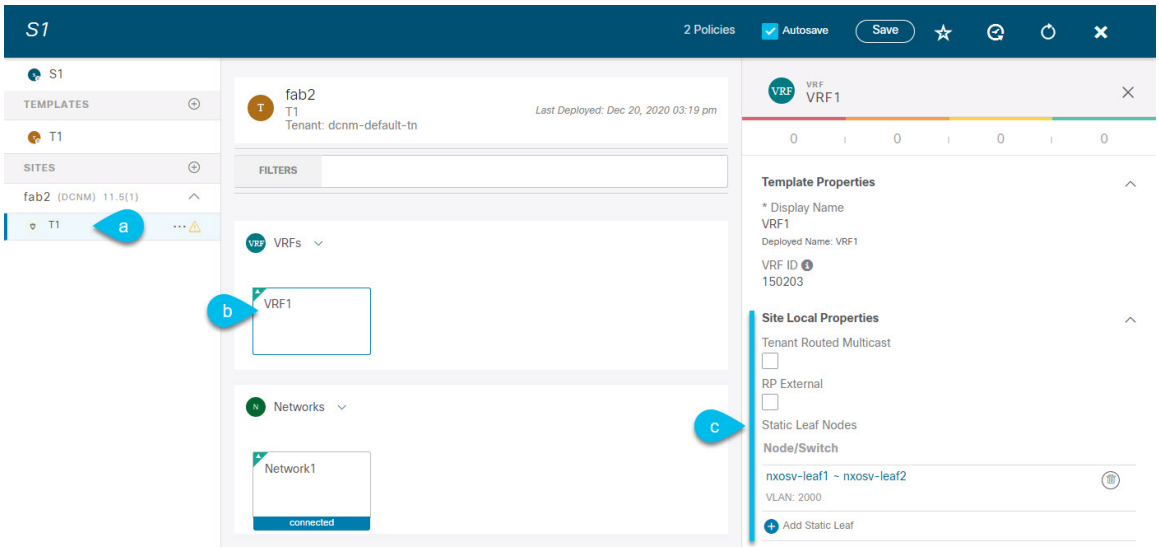
- **Import**—for VPN routes import
- **Export**—for VPN routes export
- **Import EVPN**—for EVPN routes import
- **Export EVPN**—for EVPN routes export

You must enter a valid value, for example `12.2.3.4:2200`. As you type in a value, the UI will validate it and once the format is correct, you will see a `Create "<value>"` option in the dropdown.

You can provide up to 10 custom route target values in total.

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.



a) In the left sidebar under **SITES**, select the template where the network is defined.
b) In the main pane, select the network.
c) 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 Nexus Dashboard 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 NDO 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 NDO 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 NDO 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.

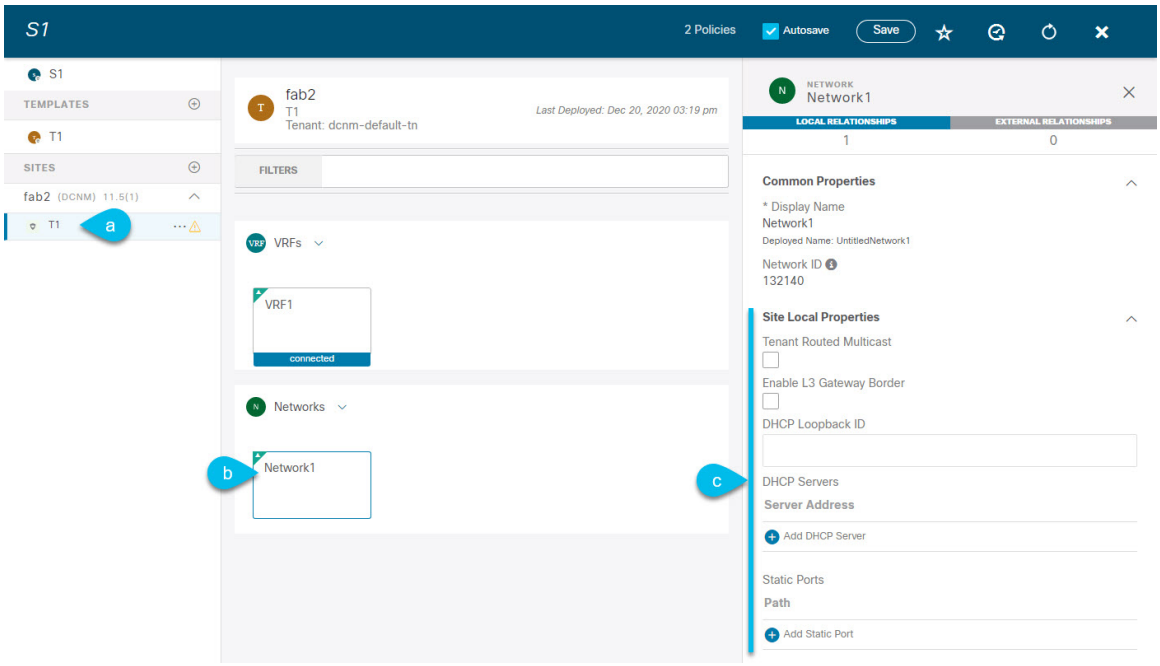
Step 12 Choose whether you want to **Suppress ARP**.

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.



a) In the left sidebar under **SITES**, select the template where the VRF is defined.
b) In the main pane, select the VRF.
c) 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.

Template Versioning

Release 3.4(1) adds support for template versioning. A new version of the template is created every time it is saved. From within the NDO UI, you can view the history of all configuration changes for any template along with information about who made the changes and when. You can also compare any of the previous versions to the current version.

New versions are created at the template level, not schema level, which allows you to configure, compare, and roll back each template individually.

Tagging Templates

At any point you can choose to tag the current version of the template as "golden", for example for future references to indicate a version that was reviewed, approved, and deployed with a fully validated configuration.

Step 1 Log in to your Nexus Dashboard Orchestrator GUI.

Step 2 From the left navigation menu, select **Application Management** > **Schemas**.

Step 3 Click the schema that contains the template you want to view.

Step 4 In the Schema view, select the template you want to review.

Step 5 From the template's actions (**...**) menu, select **Set as Golden**.

If the template is already tagged, the option will change to **Remove Golden** and allows you to remove the tag from the current version.

Any version that was tagged will be indicated by a star icon in the template's version history screen.

Viewing History and Comparing Previous Versions

This section describes how to view previous versions for a template and compare them to the current version.

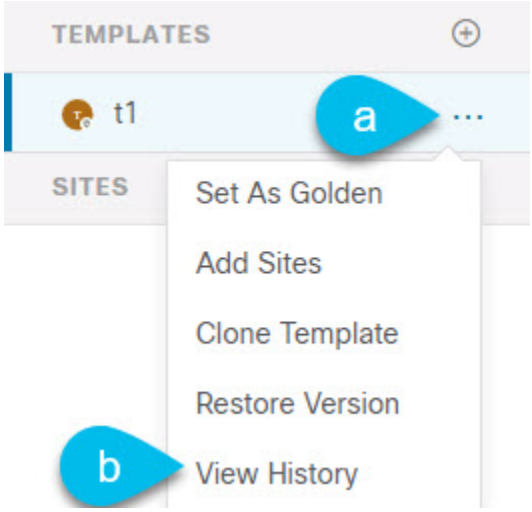
Step 1 Log in to your Nexus Dashboard Orchestrator GUI.

Step 2 From the left navigation menu, select **Application Management** > **Schemas**.

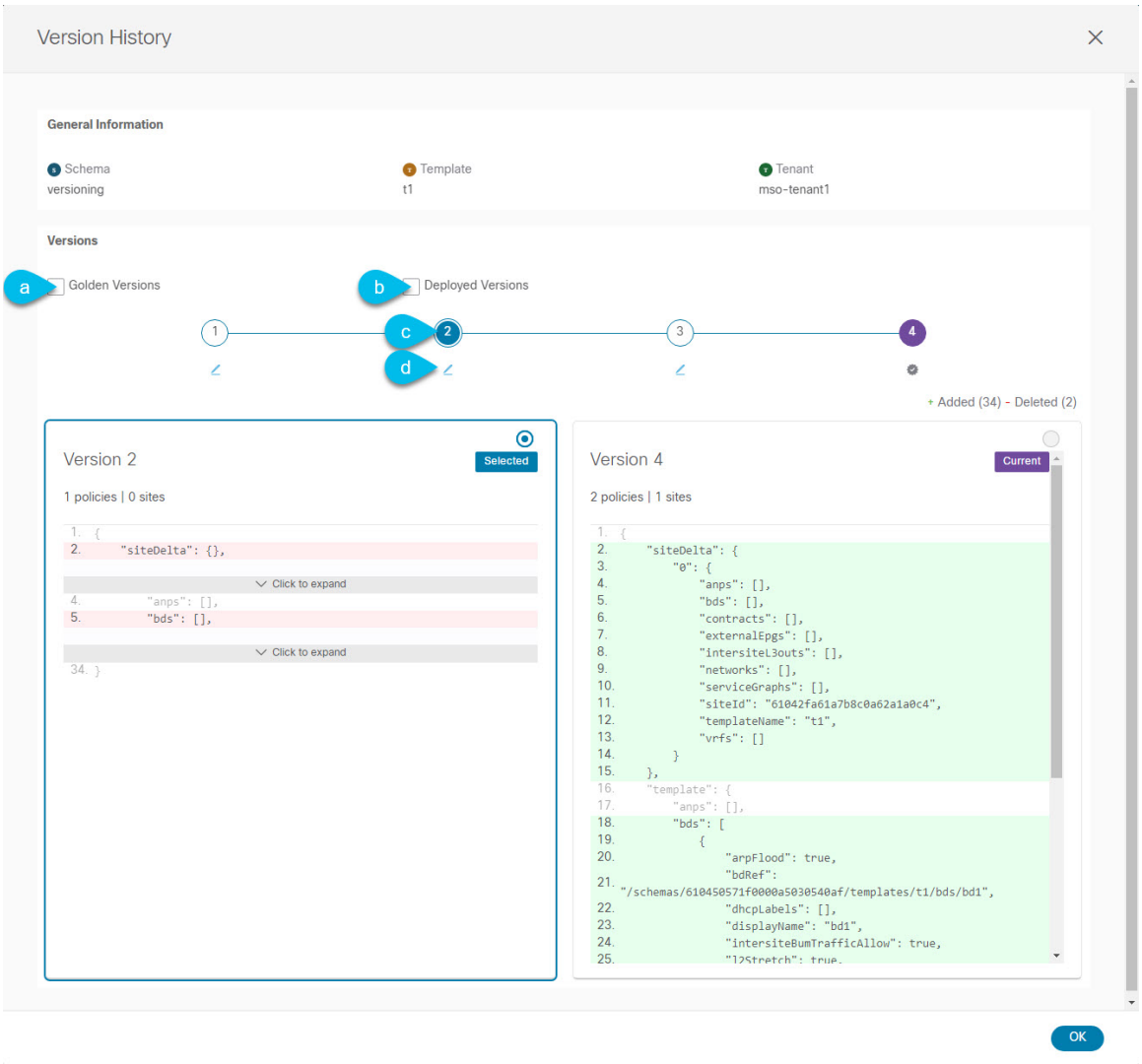
Step 3 Click the schema that contains the template you want to view.

Step 4 In the Schema view, select the template you want to review.

Step 5 From the template's actions (**...**) menu, select **View History**.



Step 6 In the **Version History** window, make the appropriate selections.



a) Enable the **Golden Versions** checkbox to filter the list of previous versions to display only the versions of this template that had been marked as `Golden`.

   Tagging a template as "Golden" is described in Tagging Templates, on page 31.

b) Enable the **Deployed Versions** checkbox to filter the list of previous versions to display only the versions of this template that had been deployed to sites.

   A new template version is created every time the template is changed and the schema is saved. You can choose to only show the versions of the template that were actually deployed to sites at some point.

c) Click on a specific version to compare it to the current version.

   The version you select is always compared to the current version of the template. Even if you filter the list using the **Golden Versions** or **Deployed Versions** filters, the current version will always be displayed even if it was never deployed or tagged as golden.

d) Mouse over the **Edit** icon to see information about who created the version and when.

Step 7 Click **OK** to close the version history window.

Reverting Template to Earlier Version

This section describes how to restore a previous version of the template. When reverting a template, the following rules apply:

- If the target version references objects that are no longer present, restore operation will not be allowed.
- If the target version references sites that are no longer managed by NDO, restore operation will not be allowed.
- If the current version is deployed to one or more sites to which the target version was not deployed, restore operation will not be allowed.

  You must first undeploy the current version from those sites before reverting the template.
- If the target version was deployed to one or more sites to which the current version is not deployed, restore operation is allowed.

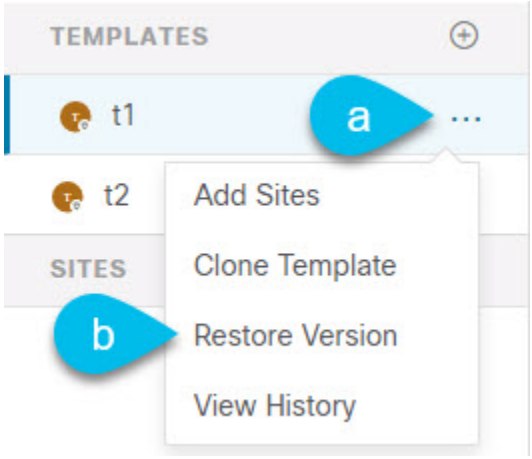
Step 1 Log in to your Nexus Dashboard Orchestrator GUI.

Step 2 From the left navigation menu, select **Application Management** > **Schemas**.

Step 3 Click the schema that contains the template you want to view.

Step 4 In the Schema view, select the template you want to review.

Step 5 From the **Actions** menu, select **Restore Version**.



Step 6 In the **Restore Version** window, select one of the earlier versions to which you want to restore.

You can filter the list of versions using the **Golden Versions** and **Deployed Versions** checkboxes.

When you select a version, you can compare the template configuration of that version to the current version of the template.

Step 7 Click **Restore** to restore the selected version.

When you restore a previous version, a new version of the template is created with the same configuration as the version you selected in the previous step.

For example, if the latest template version is `3` and you restore version `2`, then version `4` is created that is identical to the version `2` configuration. You can verify the restore by browsing to the template version history and comparing the current latest version to the version you had selected during restore, which should be identical.

If template review and approval (change control) is disabled and your account has the correct privileges to deploy templates, you can deploy the version to which you reverted as described in Deploying Templates, on page 38.

However, if change control is enabled, then:

- If you revert to a version that had been previously deployed and your account has the correct privileges to deploy templates, you can immediately deploy the template.
- If you revert to a version that had not been previously deployed or your account does not have the correct privileges to deploy templates, you will need to request template approval before the reverted version can be deployed.

  Additional information about review and approval process is available in the Template Review and Approval, on page 35 sections.

Template Review and Approval

Release 3.4(1) adds support for template review and approval (change control) workflow which allows you to set up designated roles for template designers, reviewers and approvers, and template deployers to ensure that the configuration deployments go through a validation process.

From within the NDO UI, a template designer can request review on the template they create. Then reviewers can view the history of all configuration changes for the template along with information about who made the changes and when, at which point they can approve or deny the current version of the template. If the template configuration is denied, the template designer can make any required changes and re-request review; if the template is approved, it can be deployed to the sites by a user with `Deployer` role. Finally, the deployer themselves can deny deployment of an approved template and restart the review process from the beginning.

The workflow is done at the template level, not schema level, which allows you to configure, review, and approve each template individually.

Note Because the review and approval workflow depends on user roles that are defined in Nexus Dashboard, you must be running Nexus Dashboard release 2.1(1) or later to use this feature. If you deployed your Nexus Dashboard Orchestrator in Nexus Dashboard release 2.0.2, the review and approval feature will be disabled until you upgrade your platform.

Enabling Template Approval Requirement

Before you can use the review and approval workflow for template configuration and deployment, you must enable the feature in the Nexus Dashboard Orchestrator's system settings.

Step 1 Log in to your Nexus Dashboard Orchestrator GUI.

Step 2 From the left navigation menu, select **Infrastructure** > **System Configuration**.

Step 3 On the **Change Control** tile, click the **Edit** icon.

Step 4 In the **Change Control** window, check the **Change Control Workflow** checkbox to enable the feature.

Step 5 In the **Approvers** field, enter the number of unique approvals required before the templates can be deployed.

Step 6 Click **Save** to save the changes.

Create Users with Required Roles

Before you can use the review and approval workflow for template configuration and deployment, you must create the users with the necessary privileges in the Nexus Dashboard where the NDO service is deployed.

Step 1 Log in to your Nexus Dashboard GUI.

Users cannot be created or edited in the NDO GUI, you must log in directly to the Nexus Dashboard cluster where the service is deployed.

Step 2 From the left navigation menu, select **Administrative** > **Users**.

Step 3 Create the required users.

The workflow depends on three distinct user roles: template designer, approver, and deployer. You can assign each role to a different user or combine the roles for the same user; users with `admin` privileges can perform all 3 actions.

Detailed information about configuring users and their privileges for local or remote Nexus Dashboard users is described in the Nexus Dashboard User Guide.

You must have at least as many unique users with `Approver` role as the minimum number of approvals required, which you configured in Enabling Template Approval Requirement, on page 35.

Note If you disable the **Change Control Workflow** feature, any `Approver` and `Deployer` users will have read-only access to the Nexus Dashboard Orchestrator.

Requesting Template Review and Approval

This section describes how to request template review and approval.

Before you begin

You must have:

- Enabled the global settings for approval requirement, as described in Enabling Template Approval Requirement, on page 35.
- Created or updated users in Nexus Dashboard with `approver` and `deployer` roles, as described in Create Users with Required Roles, on page 36.

- Created a template with one or more policy configurations and assigned it to one or more sites.

Step 1 Log in to your Nexus Dashboard Orchestrator GUI as a user with `Tenant Manager`, `Site Manager`, or `admin` role.

Step 2 From the left navigation menu, select **Application Management** > **Schemas**.

Step 3 Click the schema that contains the template for which you want to request approval.

Step 4 In the schema view, select the template.

Step 5 In the main pane, click **Send for Approval**.

Note that the **Send for Approval** button will not be available in the following cases:

- The global change control option is not enabled
- The template has no policy configurations or is not assigned to any sites
- Your user does not have the right permissions to edit templates
- The template has already been sent for approval
- The template was denied by the approver user

Reviewing and Approving Templates

This section describes how to request template review and approval.

Before you begin

You must have:

- Enabled the global settings for approval requirement, as described in Enabling Template Approval Requirement, on page 35.
- Created or updated users in Nexus Dashboard with `approver` and `deployer` roles, as described in Create Users with Required Roles, on page 36.
- Created a template with one or more policy configurations and assigned it to one or more sites.
- Had the template approval requested by a schema editor, as described in Requesting Template Review and Approval, on page 36.

Step 1 Log in to your Nexus Dashboard Orchestrator GUI as a user with `Approver` or `admin` role.

Step 2 From the left navigation menu, select **Application Management** > **Schemas**.

Step 3 Click the schema that contains the template you want to review and approve.

Step 4 In the schema view, select the template.

Step 5 In the main pane, click **Approve**.

If you have already approved or denied the template, you will not see the option until the template designer makes changes and re-sends the template for review again.

Step 6 In the **Approving template** window, review the template and click **Approve**.

The approval screen will display all the changes which the template would deploy to the sites.

You can click **View Version History** to view the complete version history and incremental changes made between versions. Additional information about version history is available in Viewing History and Comparing Previous Versions, on page 31.

You can also click **Deployment Plan** to see a visualization and an XML of the configuration that would be deployed from this template. The functionality of the "Deployment Plan" view is similar to the "Deployed View" for already-deployed templates, which is described in Viewing Currently Deployed Configuration, on page 39.

What to do next

After the template is reviewed and approved by the required number of approvers, you can deploy the template as described in Deploying Templates, on page 38.

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.

Viewing Currently Deployed Configuration

You can view all objects currently deployed to sites from a specific template. Even though any given template can be deployed, undeployed, updated, and re-deployed any number of times, this feature will show only the final state that resulted from all of those actions. For example, if `Template1` contains only `VRF1` object and is deployed to `Site1`, the API will return only `VRF1` for the template; if you then add `VRF2` and redeploy, the API will return both objects, `VRF1` and `VRF2`, from this point on.

This information comes from the Orchestrator database, so it does not account for any potential configuration drifts caused by changes done directly in the site's controller.

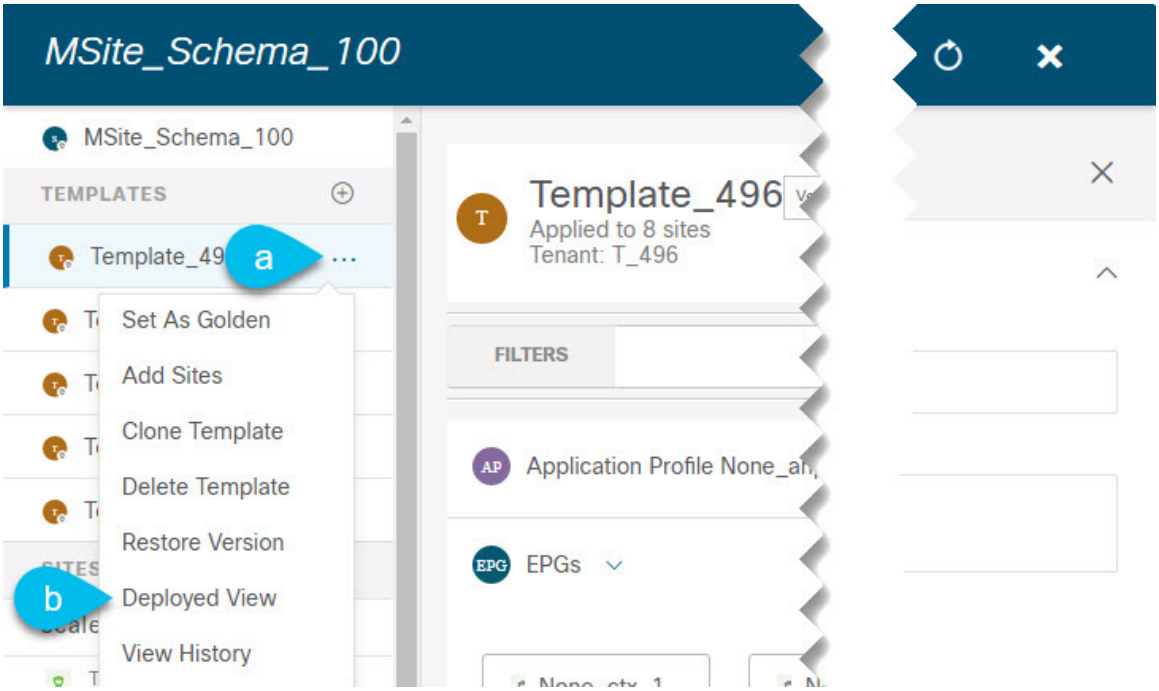
Step 1 Log in to your Nexus Dashboard Orchestrator GUI.

Step 2 From the left navigation menu, select **Application Management** > **Schemas**.

Step 3 Click the schema that contains the template you want to view.

Step 4 In the left sidebar, select the template.

Step 5 Open the **Deployed View** for the template.



a) Click the **Actions** menu next to the template's name.
b) Click **Deployed View**.

Step 6 In the **Deployed View** screen, select the site for which you want to view the information.

You will see a graphical representation of the template configuration comparison between what's already deployed to the site and what's defined in the template.

a) The color-coded legend indicates which objects would be created, deleted, or modified if you were to deploy the template at this time.

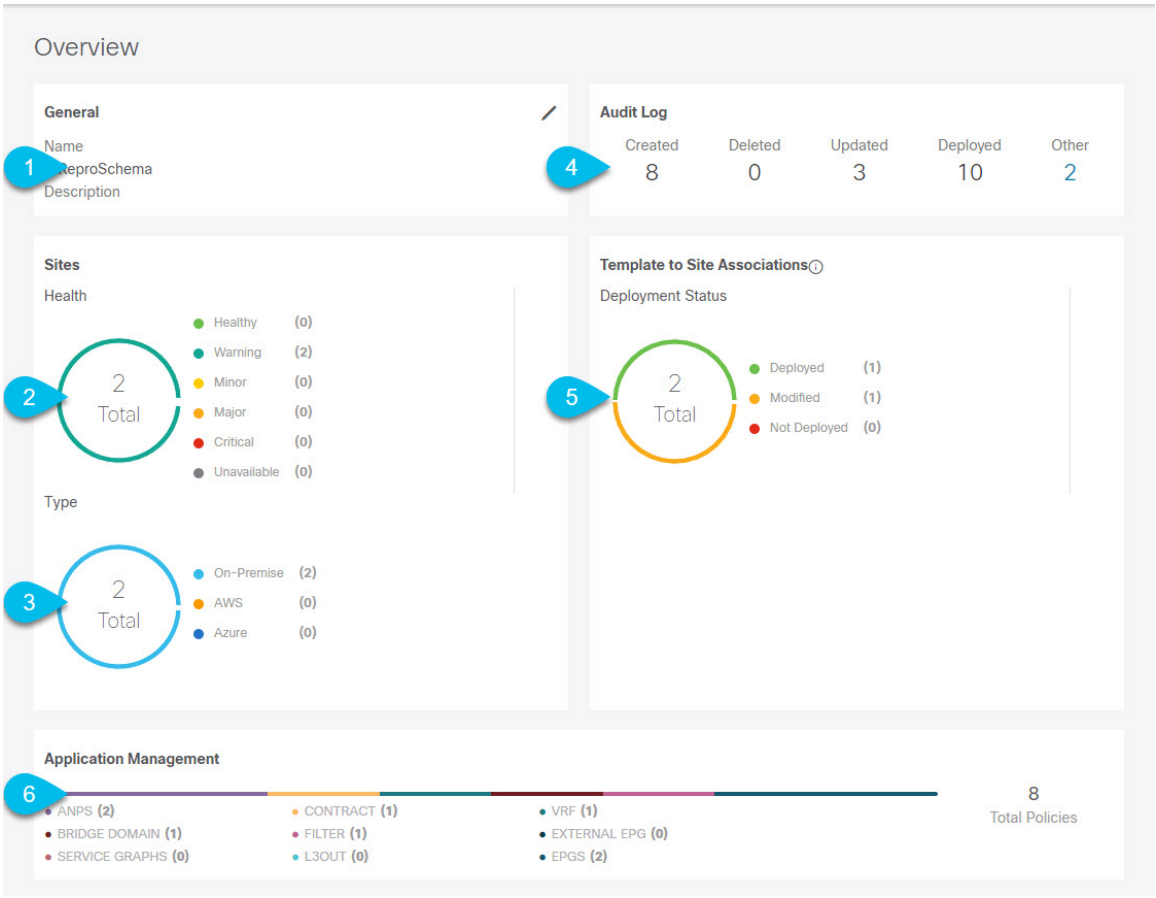
   If the latest version of the template is already deployed, the view will not contain any color-coded objects and will simply display the currently deployed configuration.

b) You can click on a site name to show configuration for that specific site.
c) You can click **View XML/JSON** to see the XML config of all the objects that are deployed to the selected site.

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

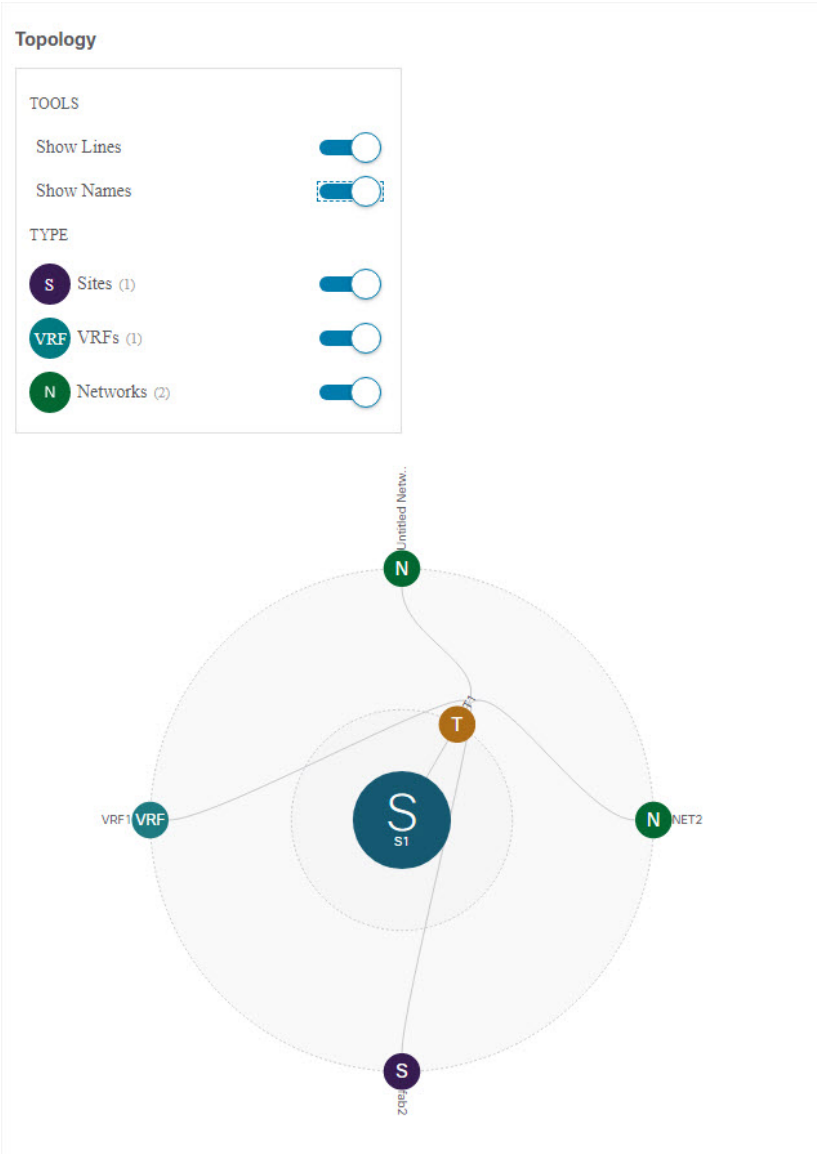


The following details are provided on this page:

1. **General**—Provides general information of the schema, such the name and description.
2. **Audit Log**—Provides 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



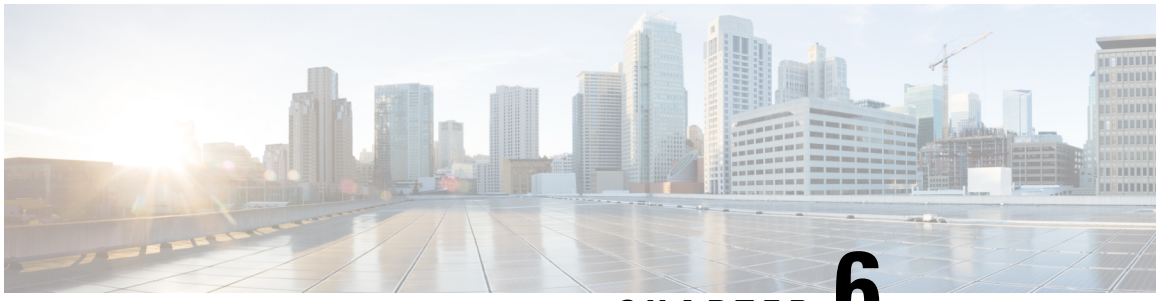
1. **Configuration Options**—Allows you to choose which policy objects to display in the topology diagram below.
2. **Topology Diagram**—Provides visual representation of the policies configured in all of the Schema's templates that are assigned to sites.

   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



CHAPTER 6

System Configuration

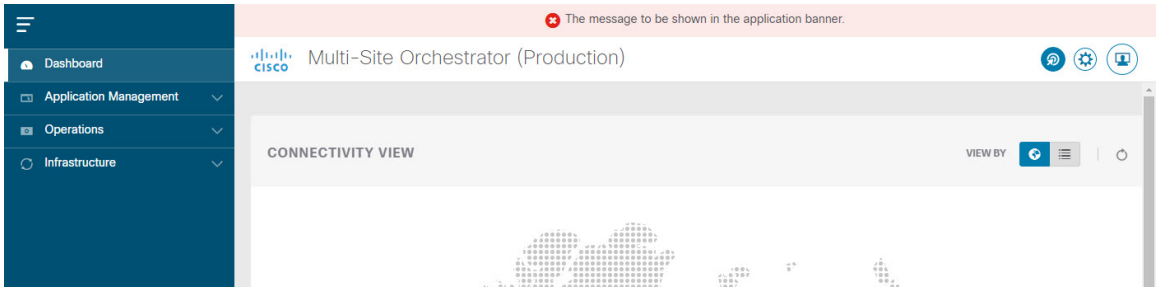
System Configuration Settings

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 Nexus Dashboard 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.

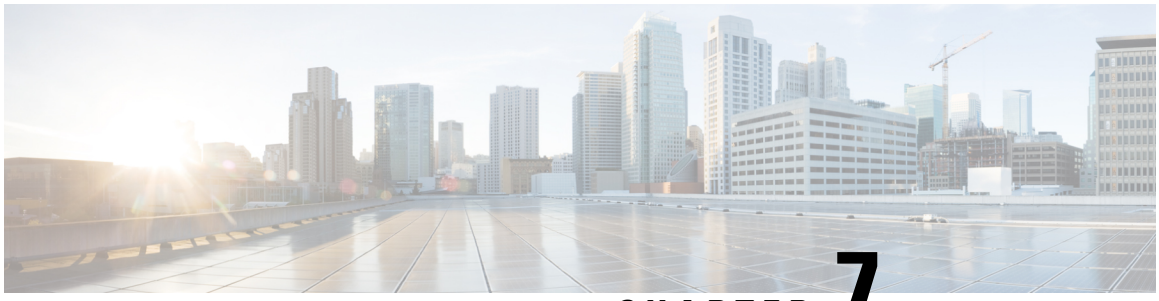
This opens the **Fail Attempts & Lockout Time** settings window.

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

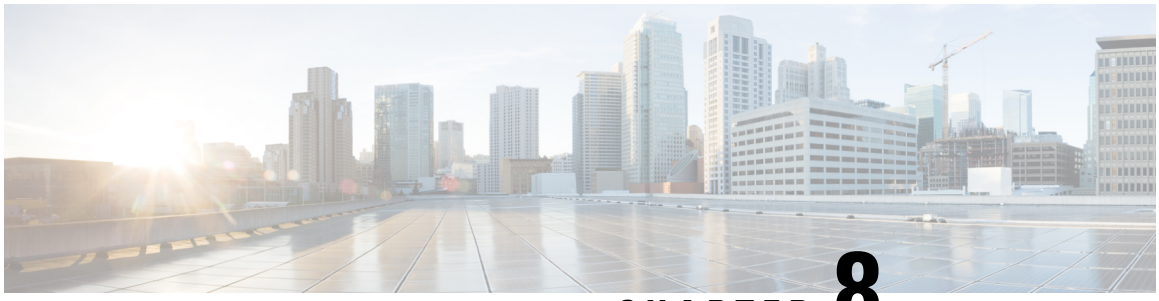
Nexus Dashboard Orchestrator system logging is automatically enabled when you first deploy the Orchestrator cluster and captures the events and faults that occur in the environment.

You can view the Nexus Dashboard 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

You can create backups of your Nexus Dashboard 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. The backups are always created on a remote server (not Nexus Dashboard cluster), which is defined in the Nexus Dashboard Orchestrator as described in the following sections.

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 Nexus Dashboard 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 Multi-Site Orchestrator releases in VMware ESX or Application Services Engine deployments is 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 Nexus Dashboard Orchestrator, but it does not make any changes to the controller (such as APIC, Cloud APIC, or DCNM) 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 Nexus Dashboard Orchestrator and each site's controller.
- Backups must be created on a remote location.

  Prior to release 3.4(1), when you first deployed the cluster, any backups you created were saved to a default location on each node's local disk with an option to configure a remote location outside the Orchestrator cluster and relocate the backups there.

  Starting with release 3.4(1), the local disk option has been deprecated and all backups must be created on a remote location outside the Nexus Dashboard cluster. You can configure a remote SCP or SFTP location using the NDO GUI and then exporting the backup files there as described in the following sections.

  When you first upgrade from release 3.3(1) or earlier to release 3.4(1) or later, you will be able to download previously-created local backups as described in Downloading and Importing Older Local Backups, on page 51. You can then re-import those backups into the Nexus Dashboard Orchestrator using a remote location.

  Note Local backups cannot be restored.

- When you create a configuration backup and export it to a remote server, the files are first created on the Orchestrator's local drives, then uploaded to the remote location, and finally deleted from the local storage. If there is not enough local disk space, the backup will fail.
- If you have a backup scheduler enabled to take local backups before upgrading to Release 3.4(1) or later, it will be disabled after the upgrade.

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 54.

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 54.

- 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 Nexus Dashboard 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.

Downloading and Importing Older Local Backups

Releases prior to 3.4(1) supported creation of configuration backups on the Orchestrator's local disk. We recommend downloading any local backups before upgrading to release 3.4(1) or later. However, the local backups will still be available for download after the upgrade.

While you can download the old backups after the upgrade, you cannot restore them directly in the UI. This section describes how to download any such backups from the Orchestrator GUI to your local machine and then re-import them back into the Nexus Dashboard Orchestrator GUI this time using a remote location.

Before you begin

You must have completed the following:

- Upgraded from release 3.3(1) or earlier to release 3.4(1) or later, where local backups are no longer supported.
- Added a remote location for backups as described in Configuring a Remote Location for Backups, on page 52.

Step 1 Log in to your Nexus Dashboard 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 to your system.

Step 4 Delete the backup you downloaded in the Nexus Dashboard Orchestrator GUI.

If you try to re-import the backup without deleting the existing local backup from previous version, the upload will fail as there is already a backup file with the same name.

To delete the backup you just downloaded, click the actions (**...**) menu next to the backup and select **Delete**.

Step 5 Import the backup to a remote location.

Simply re-upload the backup file you just downloaded back into the Nexus Dashboard Orchestrator but using a remote location, as described in Uploading Backups, on page 53.

Configuring a Remote Location for Backups

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

Step 1 Log in to your Nexus Dashboard 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 remote 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.

Uploading Backups

This section describes how to upload an existing configuration backup you have previously downloaded and import it into one of the remote locations configured in your Nexus Dashboard Orchestrator.

Before you begin

You must have completed the following:

- Created and downloaded a configuration backup as described in Creating Backups, on page 53 and Downloading Backups, on page 55.

  If your backup is already on a remote location, for example if it was created on release 3.4(1) or later, you can download it to your local machine and upload it to a different remote location.

- Added a remote location for backups as described in Configuring a Remote Location for Backups, on page 52.

Step 1 Log in to your Nexus Dashboard Orchestrator.

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

Step 3 In the main pane, click **Upload**.

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

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

Step 5 From the **Remote Location** dropdown menu, select the remote location.

Step 6 (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.

Step 7 Click **Upload** to import the file.

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

Note that even though the backups are shown on the NDO UI, they are located on the remote servers only.

Creating Backups

This section describes how to create a new backup of your Nexus Dashboard Orchestrator configuration.

Before you begin

You must first add the remote location as described in Configuring a Remote Location for Backups, on page 52.

Step 1 Log in to your Nexus Dashboard 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) From the **Remote Location** dropdown, select the remote location you have configured for backups.

c) In the **Remote Path**, either leave the default target directory or append additional subdirectories to the path.

Note that the directories must be under the default configured path and must have been already created on the remote server.

d) Click **Save** to create the backup.

Restoring Backups

This section describes how to restore a Nexus Dashboard Orchestrator configuration to a previous state.

Before you begin

Restoring a backup action restores the database on the Nexus Dashboard Orchestrator, but it does not make any changes to the controller databases on each site. Therefore, after you restore the Nexus Dashboard Orchestrator database, you must also re-deploy any existing schemas to avoid potentially mismatching policies between the Nexus Dashboard 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 49.

Step 1 Log in to your Nexus Dashboard 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 49.

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 Nexus Dashboard Orchestrator 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 Multiple services are restarted during the configuration restore process. As a result, you may notice an up to 10 minute delay before the restored configuration is properly reflected in the NDO 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 49.

Downloading Backups

This section describes how to download the backup from the Nexus Dashboard Orchestrator.

Before you begin

Step 1 Log in to your Nexus Dashboard 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.

Backup Scheduler

This section describes how to enable or disable the backup scheduler, which will perform complete configuration backup at regular intervals.

Before you begin

You must have already added a remote location for backups as described in Configuring a Remote Location for Backups, on page 52.

Step 1 Log in to your Nexus Dashboard Orchestrator GUI.

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

Step 3 In the top right of the main pane, click **Scheduler**.

The **Backup Scheduler Settings** window will open.

Step 4 Set up backup scheduler.

a) Check the **Enable Scheduler** checkbox.
b) In the **Select Starting Date** field, provide the day when you want the scheduler to start.
c) In the **Select Time** fields, provide the time of day when you want the scheduler to start.
d) From the **Select Frequency** dropdown, choose how often the backup should be performed
e) From the **Remote Location** dropdown, select the location where the backups will be saved.

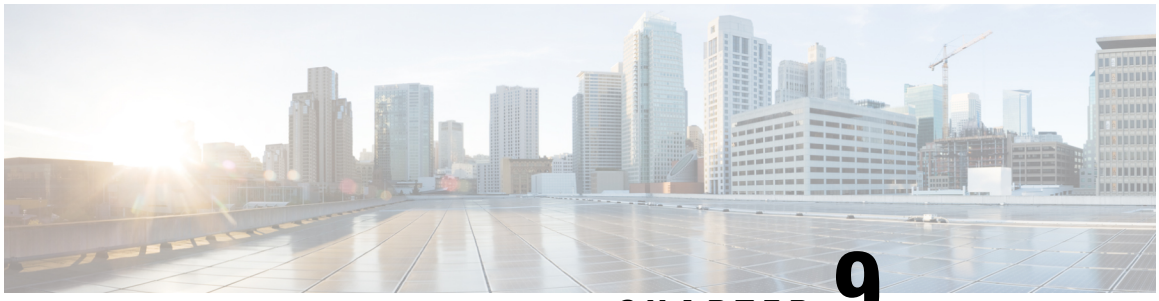
f) (Optional) In the **Remote Path** field, update the path on the remote location where the backups will be saved.

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.

g) Click **OK** to finish.

Step 5 If you want to disable the backup scheduler, simply uncheck the **Enable Scheduler**checkbox in the above step.



CHAPTER 9

Tech Support

Tech Support and System Logs

Nexus Dashboard 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.

Starting with Release 3.3(1), the tech support logs are split into two parts:

- Original database backup files containing the same information as in prior releases
- JSON-based database backup for ease of readability

Within each backup archive, you will find the following contents:

- `x.x.x.x`—one or more files in *x.x.x.x* format for container logs available at the time of the backup.
- `msc-backup-<date>_temp`—Original database backup containing the same information as previous releases.
- `msc-db-json-<date>_temp`—Backup contents in JSON format.

  For example:

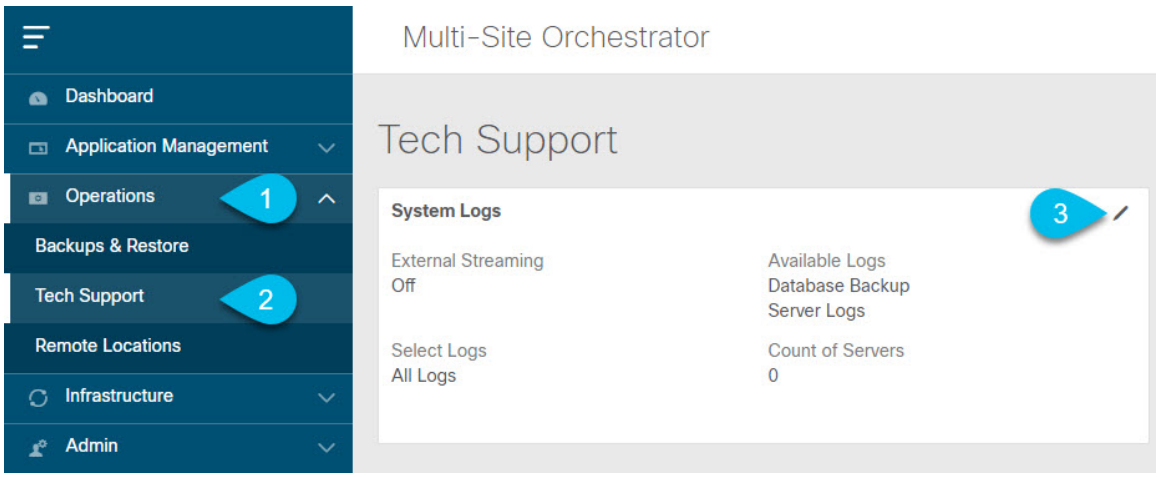
```
msc_anpEpgRels.json
msc_anpExtEpgRels.json
msc_asyncExecutionStatus.json
msc_audit.json
msc_backup-versions.json
msc_backupRecords.json
msc_ca-cert.json
msc_cloudSecStatus.json
msc_consistency.json
...
```

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 Nexus Dashboard Orchestrator.

Step 1 Log in to your Nexus Dashboard 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 Click **Download** download the logs.

An archive will be downloaded to your system. Containing all the information as described in the first section of this chapter.

Streaming System Logs to External Analyzer

Nexus Dashboard 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 Nexus Dashboard 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 Nexus Dashboard 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.

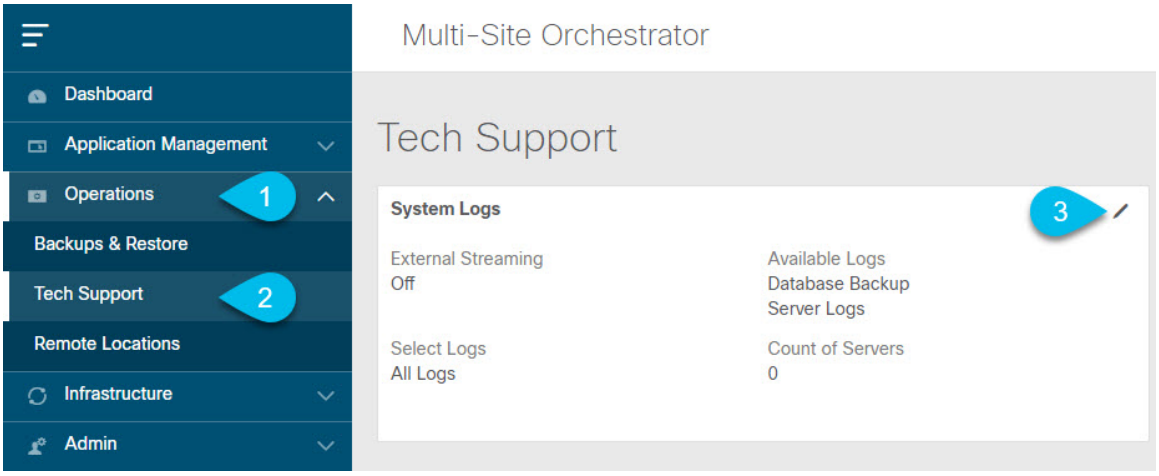
  For detailed instructions on how to configure an external log analyzer, consult its documentation.

- 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 Nexus Dashboard 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 In the **System Logs** window, enable external streaming and add a server.

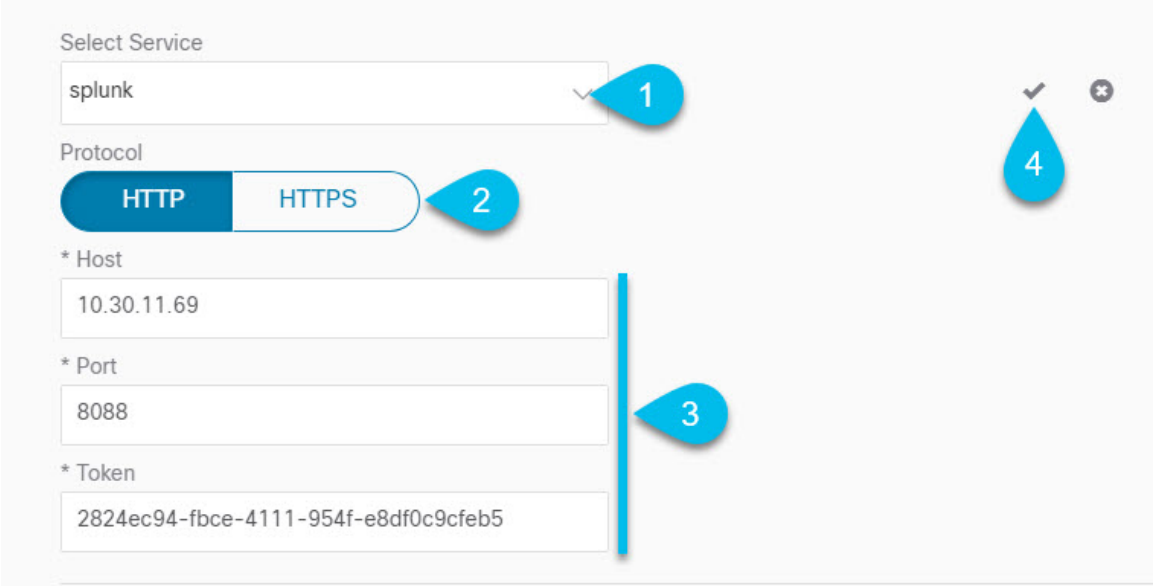
a) Enable the **External Streaming** knob.

b) Choose whether you want to stream **All Logs** or just the **Audit Logs**.

c) 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.



a) Choose `Splunk` for the server type.

b) Choose the protocol.

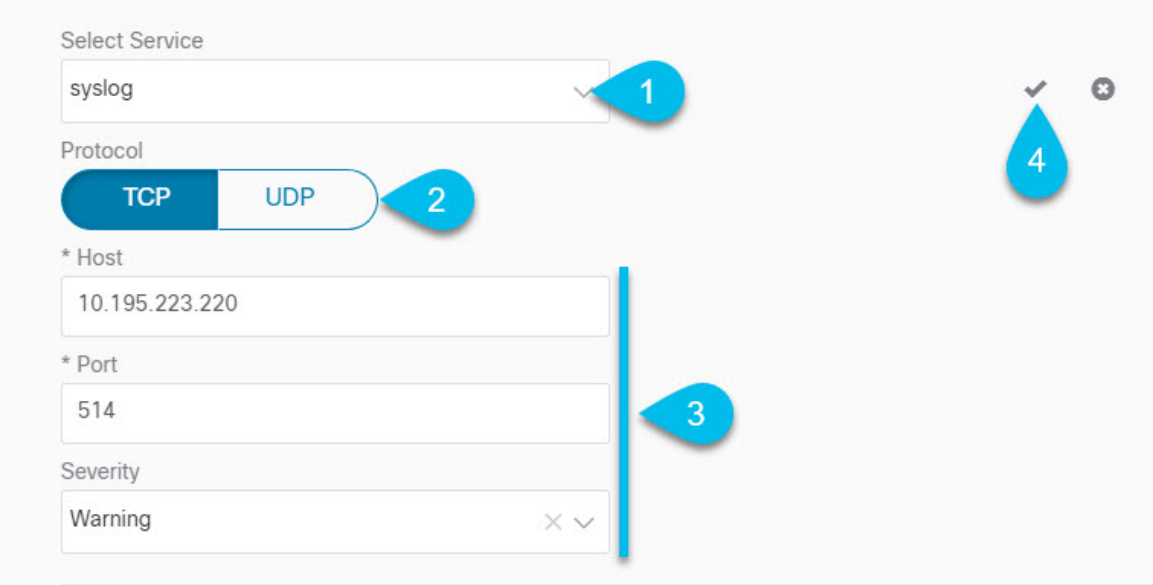
c) Provide the server name or IP address, port, and the authentication token you obtained from the Splunk service.

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**.

d) 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.

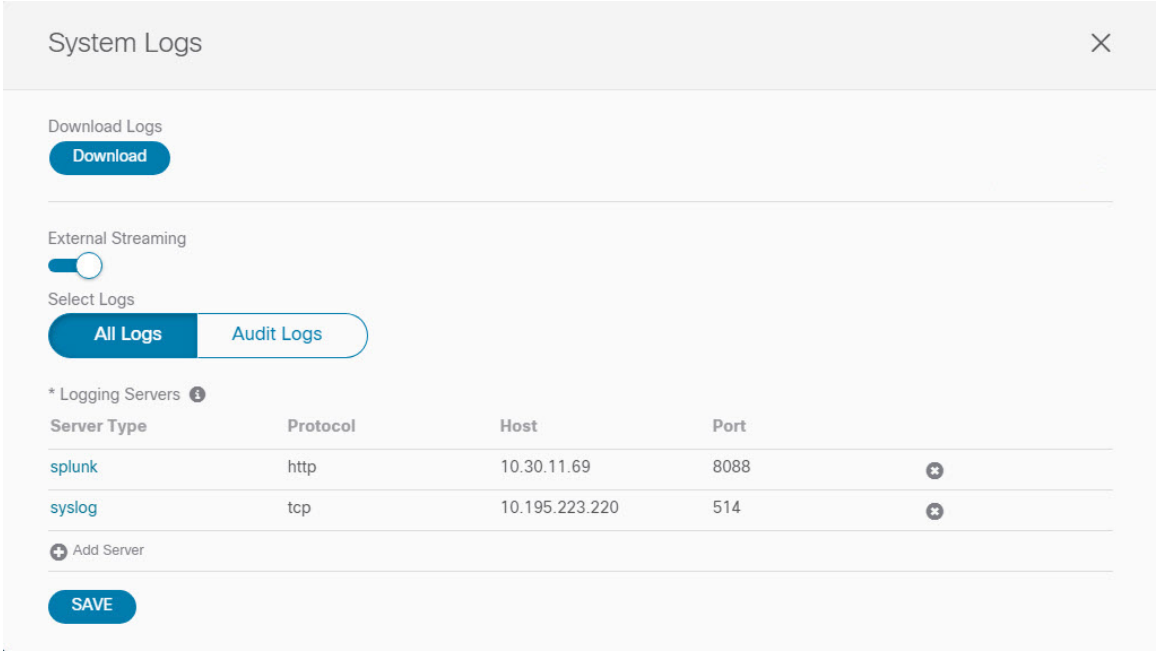


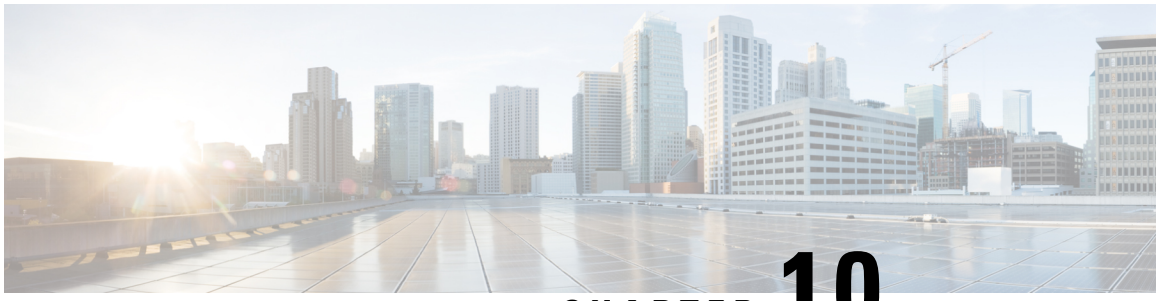
a) Choose `syslog` for the server type.
b) Choose the protocol.
c) Provide the server name or IP address, port number, and the severity level of the log messages to stream.
d) Click the checkmark icon to finish adding the server.

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.





CHAPTER 10

Upgrading or Downgrading NDO Service

Overview

The following sections describe how to upgrade or downgrade Cisco Nexus Dashboard 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 *Nexus Dashboard Orchestrator Deployment Guide*.

Prerequisites and Guidelines

Before you upgrade or downgrade your Cisco Nexus Dashboard Orchestrator cluster:

- Stateful upgrades from releases prior to Release 3.2(1) are not supported.

  If you are upgrading from an earlier release, skip the rest of this chapter and follow the instructions described in the "Migrating Existing Cluster to Nexus Dashboard" section of the *Nexus Dashboard Orchestrator Deployment Guide*.

- Ensure that your current Nexus Dashboard cluster is healthy.

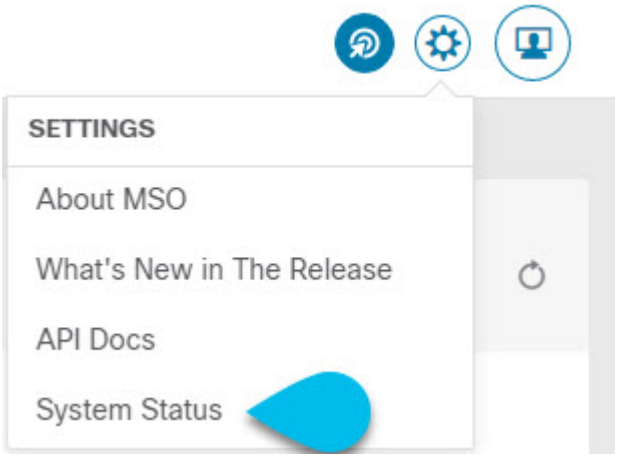
  You can check the Nexus Dashboard cluster health in one of two ways:

  - 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:

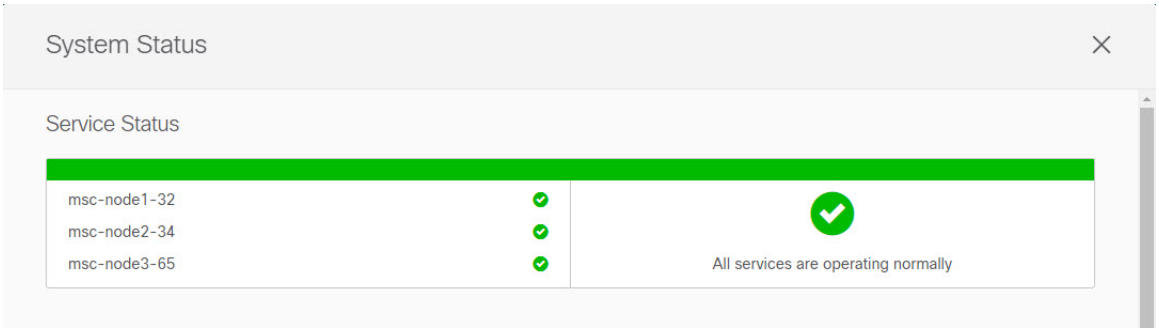
    ```
    # acs health
    All components are healthy
    ```

- Ensure that your current Cisco Nexus Dashboard Orchestrator is running properly.

You can check the status of you Nexus Dashboard Orchestrator service by navigating to **Settings** > **System Status**:



Then ensure that the status of all nodes and services is healthy:



- You can upgrade the NDO service in one of two ways:
  - Using the Nexus Dashboard's App Store, as described in Upgrading NDO Service Using Cisco App Store, on page 65.

    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 The App Store allows you to upgrade to the latest available version of the service only. In other words, if release 3.4(1) is available, you cannot use the App Store to upgrade to release 3.3(1) and must use the manual upgrade process as described below.

  - By manually uploading the new app image, as described in Upgrading NDO Service Manually, on page 67.

    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.

- If you plan to add and manage new Cloud APIC sites after you upgrade your Nexus Dashboard Orchestrator to release 3.3(1) or later, you must ensure that they are running Cloud APIC release 5.2(1) or later.

  On-boarding and managing Cloud APIC sites running earlier releases is not support in Nexus Dashboard Orchestrator 3.3(1).

- Downgrading to releases prior to release 3.3(1) is not supported.

  If you want to downgrade to an earlier release, you must deploy a new Nexus Dashboard Orchestrator cluster on a platform supported by the earlier release, then restore the older configuration backup. Restoring backups created on Release 3.3(1) or later to an older NDO cluster is not supported.

  If you downgrade to an earlier release of Nexus Dashboard Orchestrator, you must also downgrade all Cloud APIC sites to a release prior to Release 5.2(1).

Upgrading NDO Service Using Cisco App Store

This section describes how to upgrade Cisco Nexus Dashboard Orchestrator, Release 3.2(1) or later.

Before you begin

- Ensure that you have completed the prerequisites described in Prerequisites and Guidelines, on page 63.
- 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**.

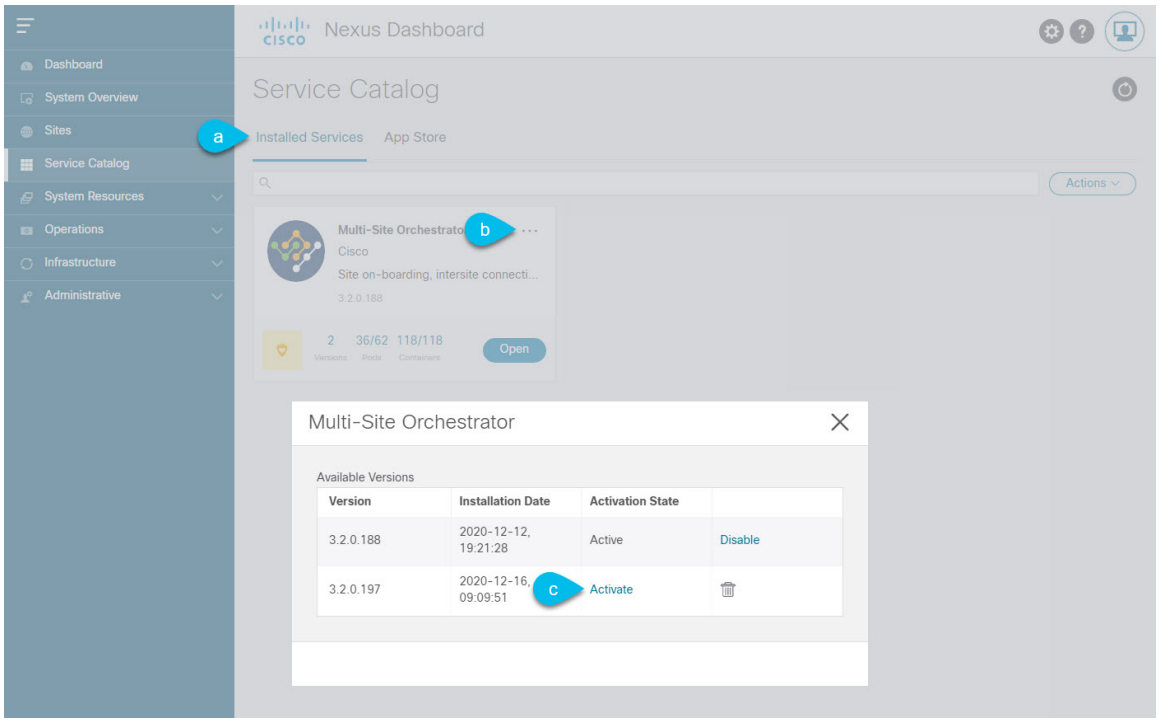
Step 3 Upgrade the application using the App Store.

a) In the **Service Catalog** screen, select the **App Store** tab.
b) In the **Nexus Dashboard 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.



a) In the **Service Catalog** screen, select the **Installed Services** tab.
b) In the top right of the Nexus Dashboard Orchestrator tile, click the menu (. . .) and choose **Available Versions**.
c) 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.

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

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 NDO Service Manually

This section describes how to upgrade Cisco Nexus Dashboard Orchestrator, Release 3.2(1) or later.

Before you begin

- Ensure that you have completed the prerequisites described in Prerequisites and Guidelines, on page 63.

Step 1 Download the target release image.

a) Browse to the Nexus Dashboard Orchestrator service 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`.

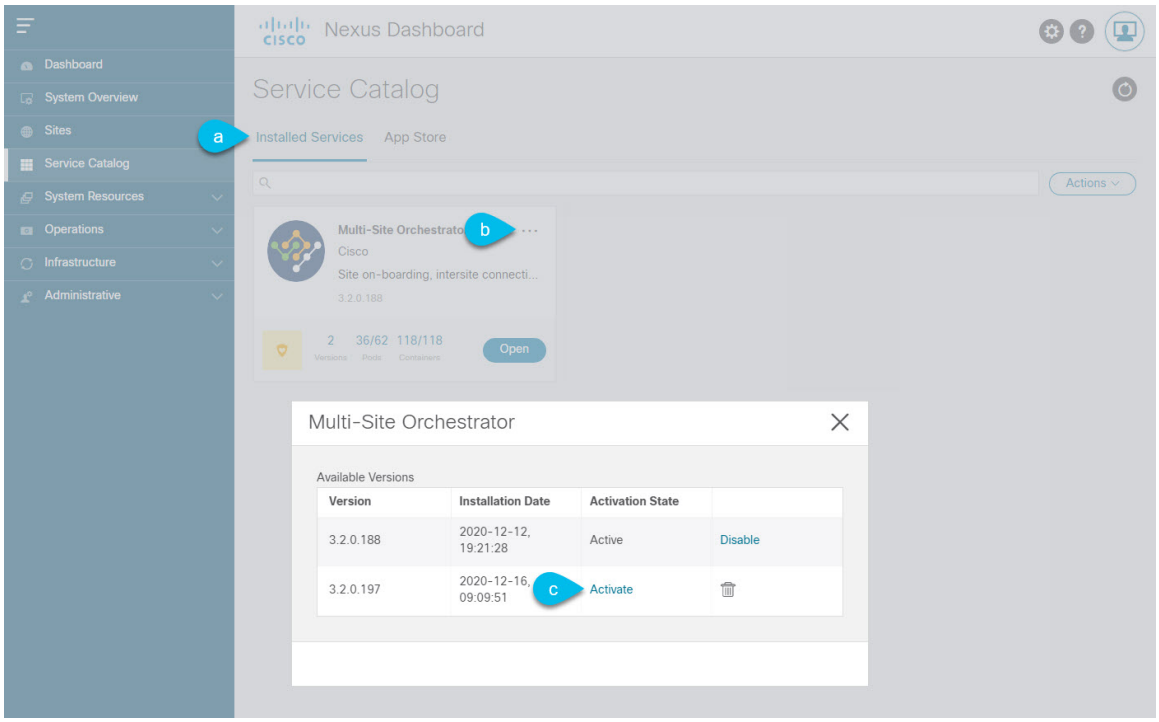
f) Click **Upload** to add the app to the cluster.

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.



a) In the **Service Catalog** screen, select the **Installed Services** tab.
b) In the top right of the Nexus Dashboard Orchestrator tile, click the menu (. . .) and choose **Available Versions**.
c) 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.

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

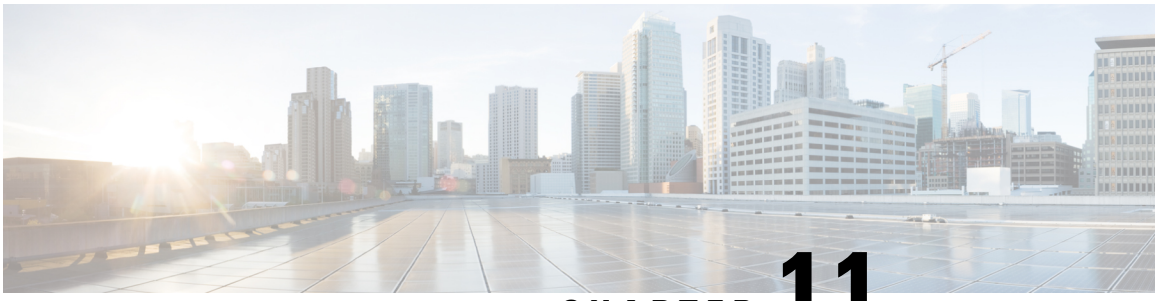
Step 7 Launch the app.

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



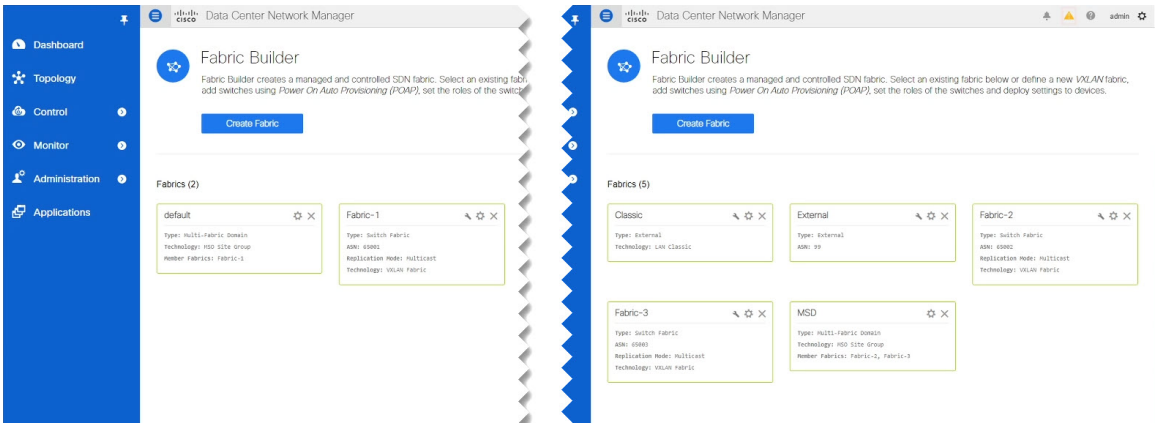
CHAPTER 11

Brownfield Import of VRFs and Networks

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 Nexus Dashboard Orchestrator. The same use case is demonstrated in the *Cisco DCNM VRF and Network Configuration using Nexus Dashboard 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:



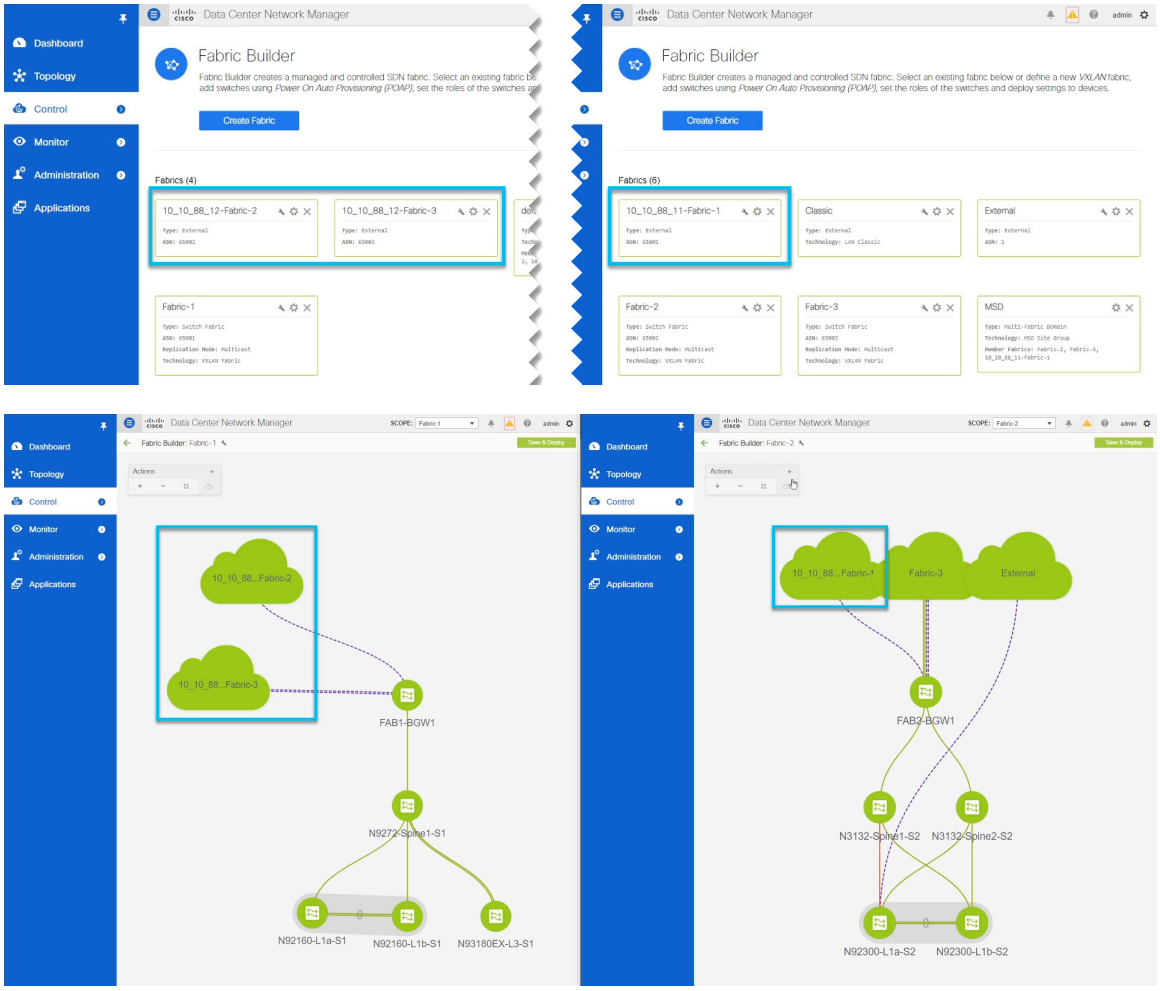
The following sections will detail how to import existing configuration, then stretch it from one fabric to another managed by different DCNMs, as well as how to deploy brand new VRFs and networks.

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 Nexus Dashboard Orchestrator service installed, as described in *Cisco Nexus Dashboard Deployment Guide* and *Cisco Nexus Dashboard Orchestrator Deployment Guide*.
- Existing DCNM fabrics on-boarded in the Nexus Dashboard and enabled for management in the Nexus Dashboard 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 72.

Step 1 Log in to your Nexus Dashboard Orchestrator GUI.

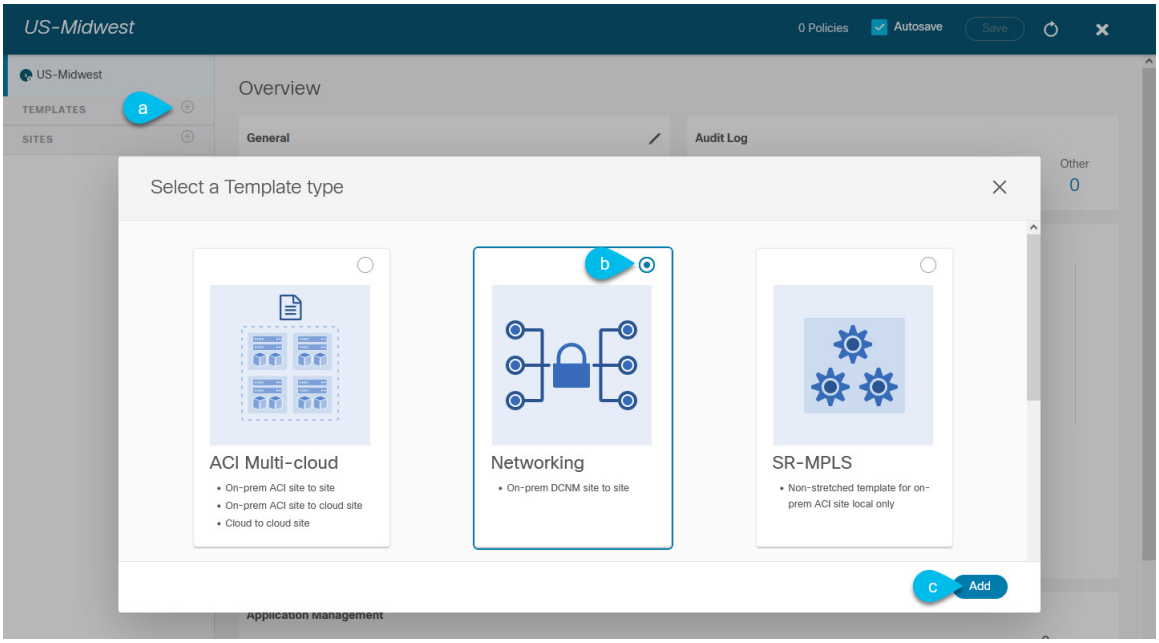
Step 2 Create a new schema.

a) From the left navigation pane, choose **Application Management** > **Schemas**.
b) On the Schemas page, click **Add Schema**.
c) 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.

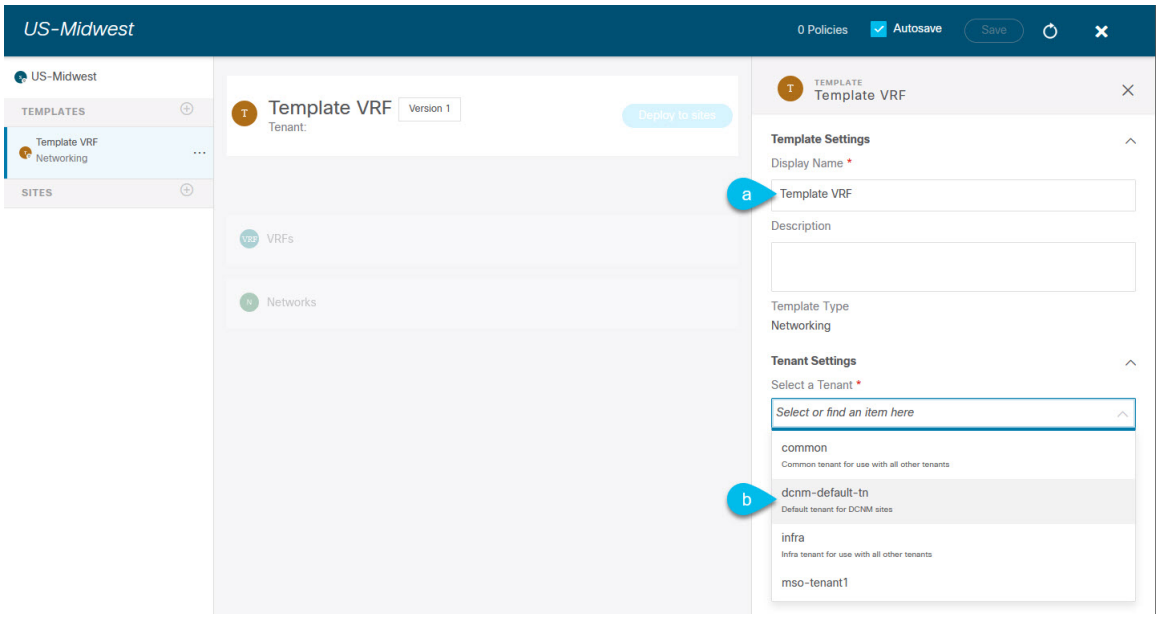
Step 3 Create a template.

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



a) In the left sidebar under **Templates**, click the + sign to add a new template.
b) In the **Select a Template type** window, choose **Networking** for the template type.
c) 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 NDO 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.

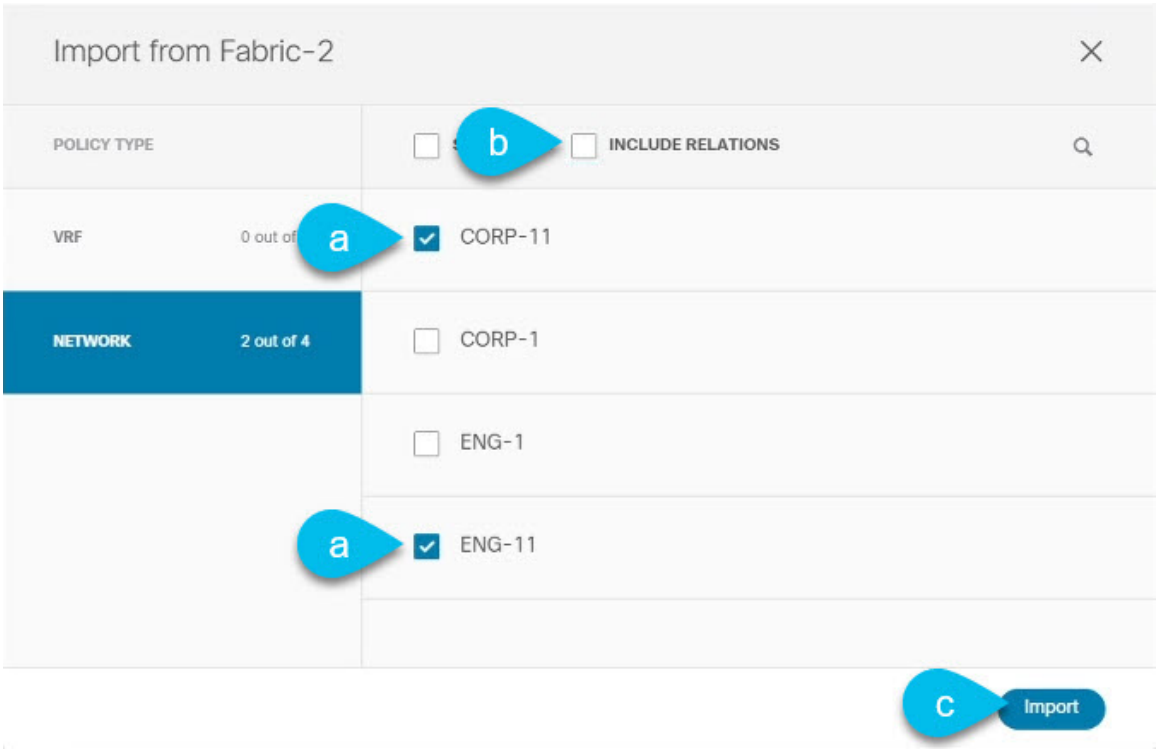
Before you begin

- 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 tese 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 Nexus Dashboard 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) Esnure 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

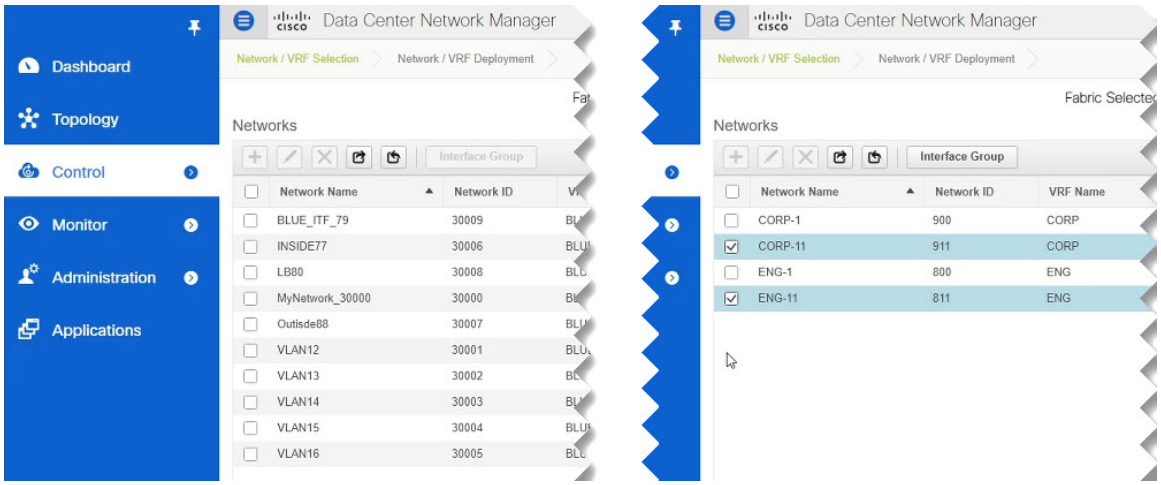
This section describes how to deploy the imported configuration to the site where it doesn't yet exist.

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`.



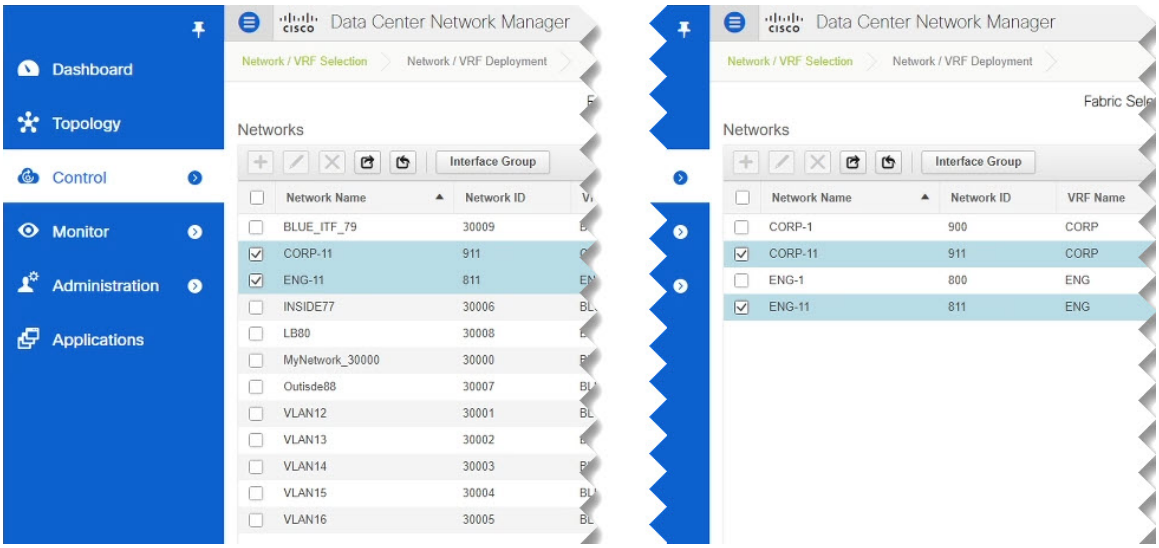
Step 2 In the top right of the template edit view, click **Deploy to sites**.

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

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

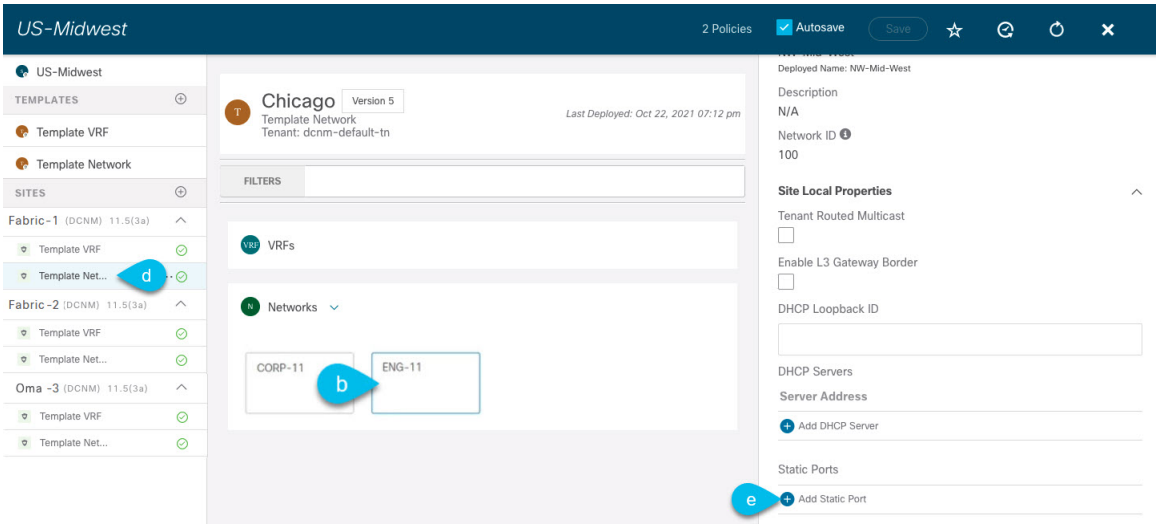
Since this is the first time you are deploying this template, the **Deploy to Sites** summary will show the configuration difference that will be deployed to sites.

It may take a few minutes for the configuration to get deployed. After you see a confirmation message in the NDO 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`.