Cisco Nexus Dashboard Orchestrator Configuration Guide for NDFC Fabrics, Release 4.0(x)

First Published: 2022-06-27

Last Modified: 2023-11-07

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

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

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

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

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

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

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

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

CONTENTS

CHAPTER 1 **New and Changed Information** 1

New and Changed Information 1

CHAPTER 2 **Adding and Deleting Sites** 3

Adding Cisco NDFC Sites 3

Removing Sites 5

Cross Launch to Fabric Controllers 6

CHAPTER 3 **Configuring Infra for Cisco NDFC Sites** 7

Prerequisites and Guidelines 7

Configuring Infra: General Settings 7

Refreshing Site Connectivity Information 10

Configuring Infra: NDFC Site-Specific Settings 10

Deploying Infra Configuration 12

CHAPTER 4 **Fabric Management** 15

Tenants Overview 15

Add Users to NDFC Tenant 16

Schemas and Templates 17

Concurrent Configuration Updates 18

Creating Schemas and Templates 20

Importing Schema Elements From NDFC Sites 22

Creating VRFs 22

Creating Networks 24

Bulk Update of Template Objects 26

Template Versioning 28

Tagging Templates 29
Viewing History and Comparing Previous Versions 29
Reverting Template to Earlier Version 31
Template Review and Approval 32
Enabling Template Approval Requirement 32
Create Users with Required Roles 32
Requesting Template Review and Approval 33
Reviewing and Approving Templates 34
Deploying Templates 34
Disassociating Template from Sites 36
Configuration Drifts 36
Reconciling Configuration Drifts 38
Viewing Currently Deployed Configuration 40
Schema Overview and Deployment Visualizer 41

PART I Operations and Infrastructure 45

CHAPTER 5 Audit Logs 47
Audit Logs 47

CHAPTER 6 Backup and Restore 49
Configuration Backup and Restore 49
Configuration Backup and Restore Guidelines 49
Downloading and Importing Older Local Backups 51
Configuring Remote Locations for Backups 52
Importing Backups to Remote Location 53
Creating Backups 53
Restoring Backups 54
Exporting (Downloading) Backups 58
Backup Scheduler 59

CHAPTER 7 Tech Support 61
Tech Support and System Logs 61
Downloading System Logs 62

Streaming System Logs to External Analyzer 62

CHAPTER 8 **System Configuration** 67

System Configuration Settings 67

System Alias and Banner 67

PART II **Features and Use Cases** 69

CHAPTER 9 **Brownfield Import of VRFs and Networks** 71

Overview 71

Prerequisites 72

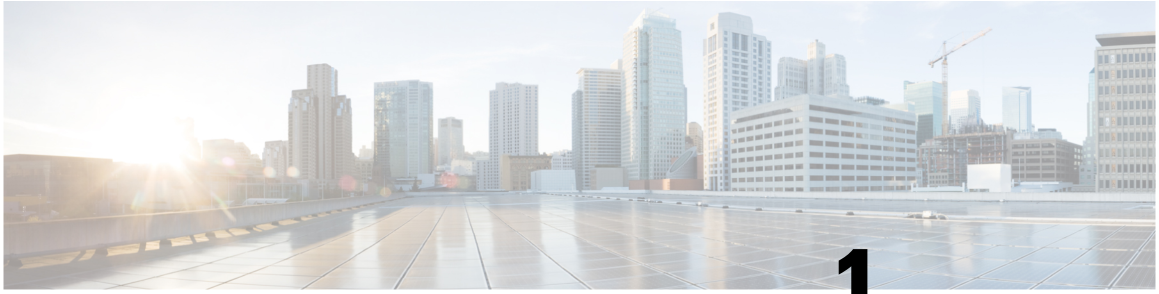
Create Schema and Templates for Importing Configuration 73

Importing Schema Elements From NDFC Sites 74

Deploying Template and Making Changes 76

CHAPTER 10 **Integration with Cloud Network Controller** 79

Overview 79



CHAPTER 1

New and Changed Information

- New and Changed Information, on page 1

New and Changed Information

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

Table 1: Latest Updates

Release	New Feature or Update	Where Documented
3.7(1)	First release of this document.	--

CHAPTER 2

Adding and Deleting Sites

- Adding Cisco NDFC Sites, on page 3
- Removing Sites, on page 5
- Cross Launch to Fabric Controllers, on page 6

Adding Cisco NDFC Sites

This section describes how to add a NDFC 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 NDFC, Release 11.5(1) or later.

Step 1 Log in to your Nexus Dashboard and open the **Admin Console**.

Step 2 From the left navigation menu, choose **Sites** and click **Add Site**..

Step 3 Provide site information.

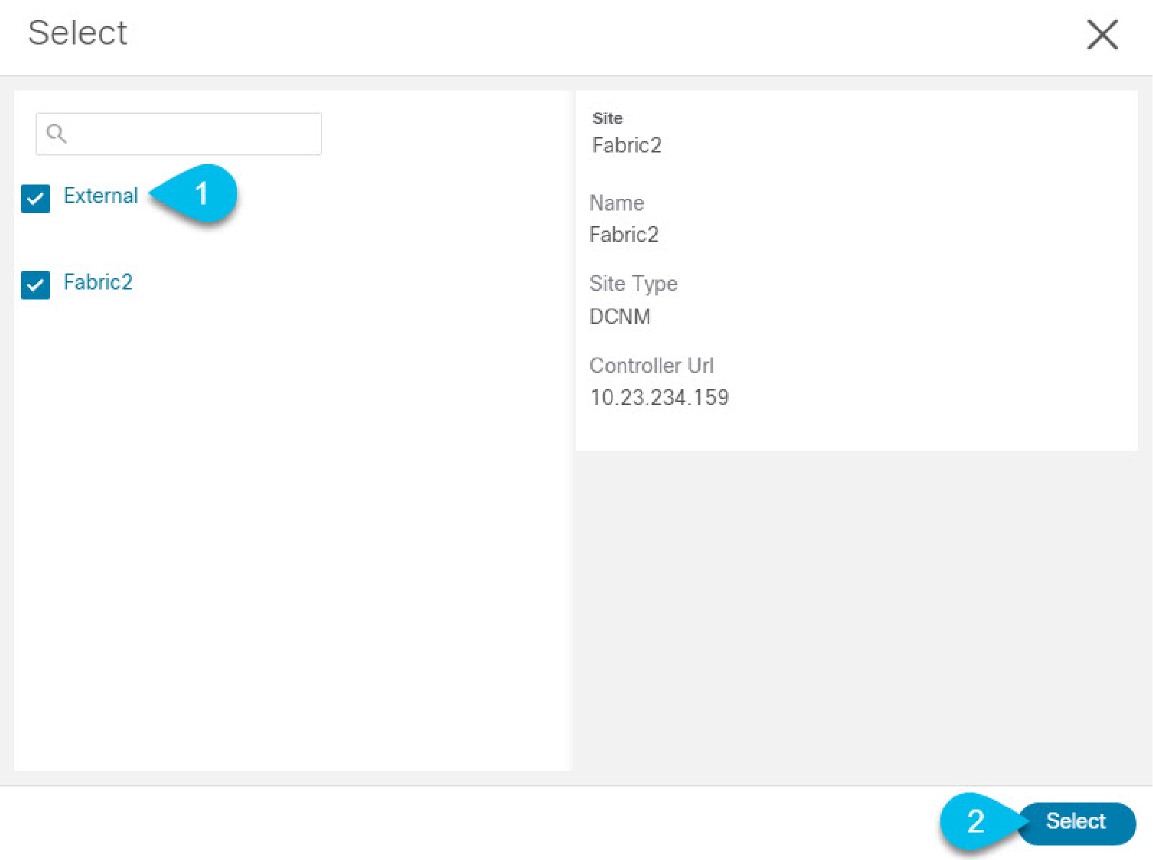
a) For **Site Type**, select **NDFC or NDFC**.

b) Provide the NDFC controller information.

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

c) Click **Select Sites** to select the specific fabrics managed by the controller.

In the fabric selection window that opens, select the fabrics you want to add to the Nexus Dashboard and click **Select**:



Site
Fabric2

Name
Fabric2

Site Type
DCNM

Controller Url
10.23.234.159

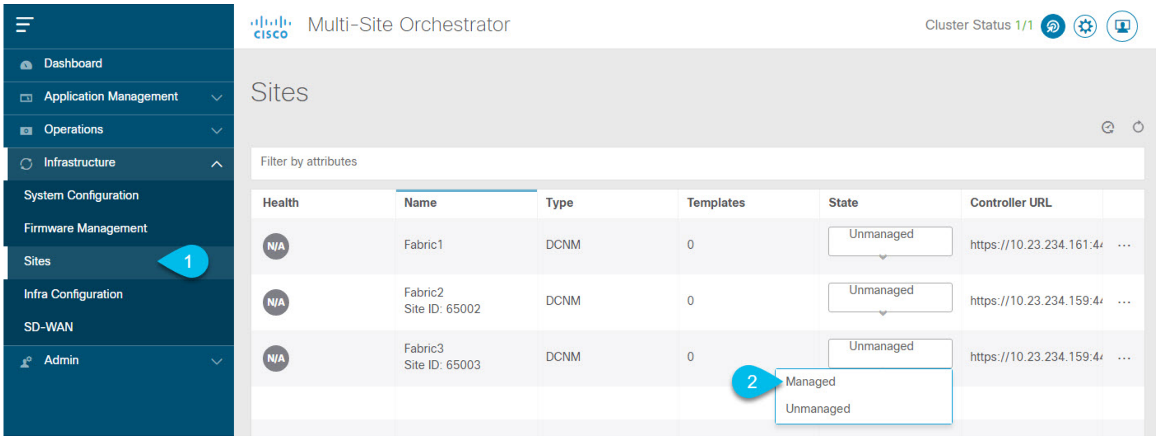
d) Click **Add Security Domains** to select one or more security domains that will have access to this site.

Step 4 Repeat the previous steps for any additional NDFC sites.

Step 5 From the Nexus Dashboard's **Service Catalog** page, open the Nexus Dashboard Orchestrator service.

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

Step 6 In the Nexus Dashboard Orchestrator GUI, manage the sites.



Health	Name	Type	Templates	State	Controller URL
N/A	Fabric1	DCNM	0	Unmanaged	https://10.23.234.161:4ɩ
N/A	Fabric2 Site ID: 65002	DCNM	0	Unmanaged	https://10.23.234.159:4ɩ
N/A	Fabric3 Site ID: 65003	DCNM	0	Unmanaged	https://10.23.234.159:4ɩ

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 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 an 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 from all templates.

You must remove the site from all templates with which it is associated before you can unmanaged the site and remove it from your Nexus Dashboard.

a) Navigate to **Application Management** > **Schemas**.
b) Click a schema that contains one or more templates associated with the site.
c) In the left sidebar's **Sites** area, select a template associated with the site, click the options menu (**...**) next to the template, and choose **Undeploy Template**.

This will remove configurations that were deployed using this template to this site.

Note For non-stretched templates, you can choose to preserve the configuration by selecting **Dissociate Template** instead of **Undeploy Template**, but you must undeploy any stretched templates.

d) Repeat this step for all templates associated with the site that you want to unmanage in this and all other schemas.

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 the site that you want to unmanage.

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, as described in the previous step.

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 services installed in your Nexus Dashboard cluster.

a) In the top navigation bar, click the **Home** icon to return to the Nexus Dashboard GUI.
b) From the left navigation menu of the Nexus Dashboard GUI, select **Sites**.
c) Select one or more sites you want to delete.
d) In the top right of the main pane, select **Actions** > **Delete Site**.
e) 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 3

Configuring Infra for Cisco NDFC Sites

- Prerequisites and Guidelines, on page 7
- Configuring Infra: General Settings, on page 7
- Refreshing Site Connectivity Information, on page 10
- Configuring Infra: NDFC Site-Specific Settings, on page 10
- Deploying Infra Configuration, on page 12

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 10 as part of the general Infra configuration procedures.

Configuring Infra: General Settings

This section describes how to configure general Infra settings for your NDFC sites that are onboarded and managed by Nexus Dashboard Orchestrator.

Step 1 Log in to your Nexus Dashboard and open the Nexus Dashboard Orchestrator service.

Step 2 In the left navigation menu, select **Infrastructure** > **Site Connectivity**.

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

Step 4 In the left sidebar, select **General Settings**.

Step 5 Provide **Control Plane Configuration**.

a) Select the **Control Plane Configuration** 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 Cloud Network Controller fabrics only.

Step 6 Provide the **On Premises IPSec Devices** information.

If your inter-site connectivity between on-premises and cloud sites is using private connection and you will not enable IPSec, you can skip this step. For connectivity over public Internet, IPSec is always enabled and you must provide the information in this step.

When you configure inter-site underlay connectivity between on-premises and cloud sites as described in later sections, you will need to select an on-premises IPN device which will establish connectivity to the cloud CSRs. These IPN devices must first be defined here before they are available in the on-premises site configuration screen.

a) Select the **On Premises IPSec Devices** tab.

b) Click **+Add On-Premises IPSec Device**.

c) Choose whether the device is **Unmanaged** or **Managed** and provide the device information.

This defines whether or not the device is directly managed by NDFC:

- For **Unmanaged** IPN devices, simply provide the **Name** and the **IP Address** of the device.

  The IP address you provide will be used as the tunnel peer address from the cloud CSRs, not the IPN device's management IP address.

- For **Managed** IPN devices, choose the NDFC **Site** that contains the device and then the **Device** from that site.

  Then choose the **Interface** on the device that is facing the Internet and provide the **Next Hop** IP address, which is the IP address of the gateway that is connecting to the Internet.

d) Click the check mark icon to save the device information.

e) Repeat this step for any additional IPN devices you want to add.

Step 7 Provide the **IPSec Tunnel Subnet Pools** information.

There are two types of subnet pools that you can provide here:

- **External Subnet Pool**—used for connectivity between cloud site CSRs and other sites (cloud or on-premises).

  These are large global subnet pools that are managed by Nexus Dashboard Orchestrator. The Orchestrator, creates smaller subnets from these pools and allocates them to sites to be used for inter-site IPsec tunnels and external connectivity IPsec tunnels.

  You must provide at least one external subnet pool if you want to enable external connectivity from one or more of your cloud sites.

- **Site-Specific Subnet Pool**—used for connectivity between cloud site CSRs and external devices.

  These subnets can be defined when the external connectivity IPsec tunnels must be in a specific range. For example, where a specific subnet is already being used to allocate IP addresses to the external router and you want to continue using those subnets for IPsec tunnels for NDO and cloud sites. These subnets are not managed by the Orchestrator and each subnet is assigned to a site in its entirety to be used locally for external connectivity IPsec tunnels.

  If you do not provide any named subnet pools but still configure connectivity between cloud site's CSRs and external devices, the external subnet pool will be used for IP allocation. .

Note The minimum mask length for both subnet pools is `/24`.

To add one or more **External Subnet Pools**:

a) Select the **IPSec Tunnel Subnet Pools** tab.

b) In the **External Subnet Pool** area, click **+Add IP Address** to add one or more external subnet pools.

   This subnet will be used to address the IPsec tunnel interfaces and loopbacks of the Cloud Routers used for on-premises connectivity, which you previously configured in the Cloud Network Controller for inter-site connectivity in earlier Nexus Dashboard Orchestrator releases.

   The subnets must not overlap with other on-premises TEP pools, should not begin with `0.x.x.x` or `0.0.x.x`, and should have a network mask between `/16` and `/24`, for example `30.29.0.0/16`.

c) Click the check mark icon to save the subnet information.

d) Repeat these substeps for any additional subnet pools you want to add.

To add one or more **Site-Specific Subnet Pools**:

a) Select the **IPSec Tunnel Subnet Pools** tab.

b) In the **Site-Specific Subnet Pools** area, click **+Add IP Address** to add one or more external subnet pools.

   The **Add Named Subnet Pool** dialogue will open.

c) Provide the subnet **Name**.

   You will be able to use the subnet pool's name to choose the pool from which to allocate the IP addresses later on.

d) Click **+Add IP Address** to add one or more subnet pools.

   The subnets must have a network mask between `/16` and `/24`and not begin with `0.x.x.x` or `0.0.x.x`, for example `30.29.0.0/16`.

e) Click the check mark icon to save the subnet information.

   Repeat the steps if you want to add multiple subnets to the same named subnet pool.

f) Click **Save** to save the named subnet pool.

g) Repeat these substeps for any additional named subnet pools you want to add.

Step 8 Configure **NDFC Settings**.

a) Select the **NDFC 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: NDFC Site-Specific Settings, on page 10.

For sites that were previously part of a Multi-Site Domain (MSD) in NDFC, 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** > **Site Connectivity**.

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

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: NDFC Site-Specific Settings

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

Step 1 Log in to your Nexus Dashboard and open the Nexus Dashboard Orchestrator service.

Step 2 In the left navigation menu, select **Infrastructure** > **Site Connectivity**.

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

Step 4 In the left pane, under **Sites**, select a specific NDFC.

Step 5 In the right **<*Site*> Settings** sidebar, specify the **Overlay Multicast TEP**.

This address is used for the inter-site L2 BUM and L3 multicast traffic. This IP address is deployed on all border gateway switches that are part of the same fabric.

Note If the site you are configuring is part of the NDFC Multi-Site Domain (MDS), this field will be pre-populated with the information imported from NDFC. 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.

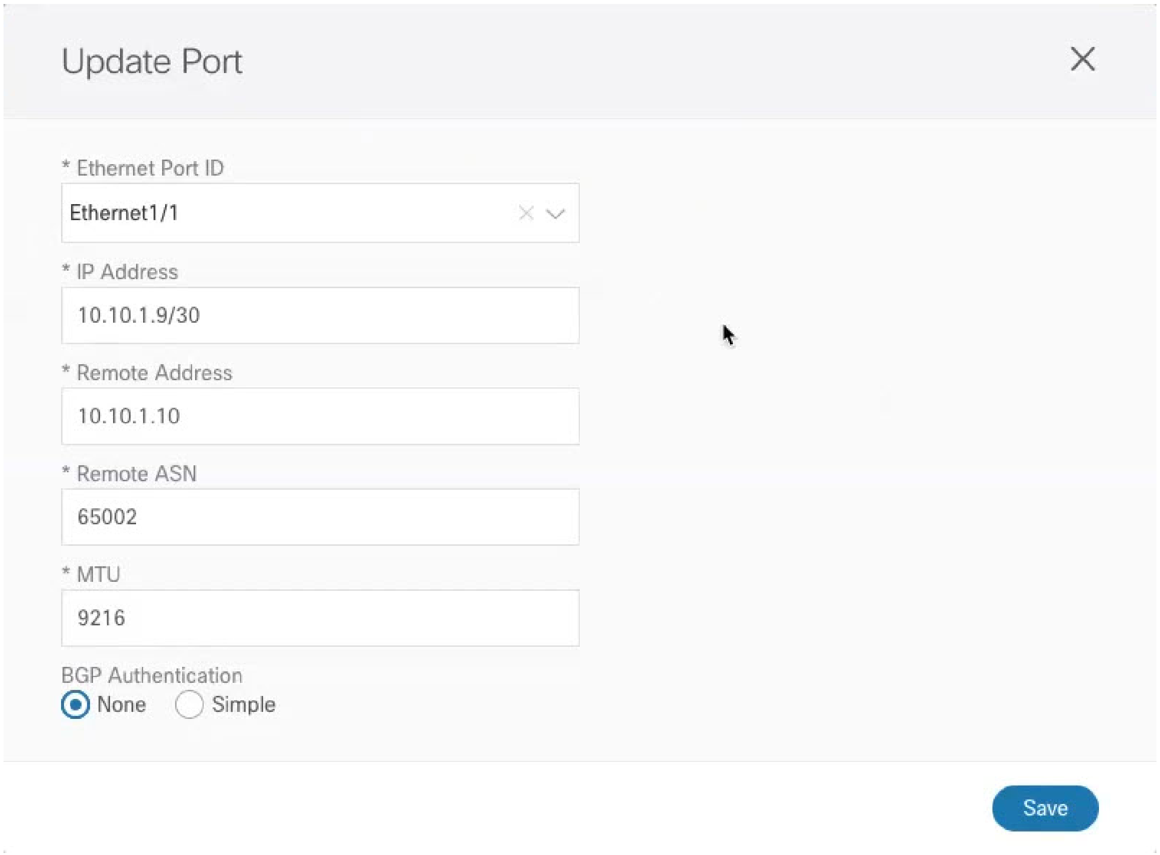
Step 6 Within the **<fabric-name>** tile, select the border gateway.

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 NDFC. If the site you are configuring is already part of the NDFC Multi-Site Domain (MDS), you must use the same values that are already configured in NDFC.



Update Port

* Ethernet Port ID: Ethernet1/1

* IP Address: 10.10.1.9/30

* Remote Address: 10.10.1.10

* Remote ASN: 65002

* MTU: 9216

BGP Authentication: ● None ○ Simple

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 NDFC site.

Before you begin

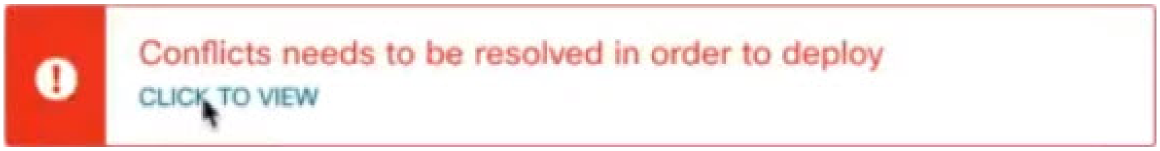
You must have the general and site-specific infra configurations completed as described in previous sections of this chapter.

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:

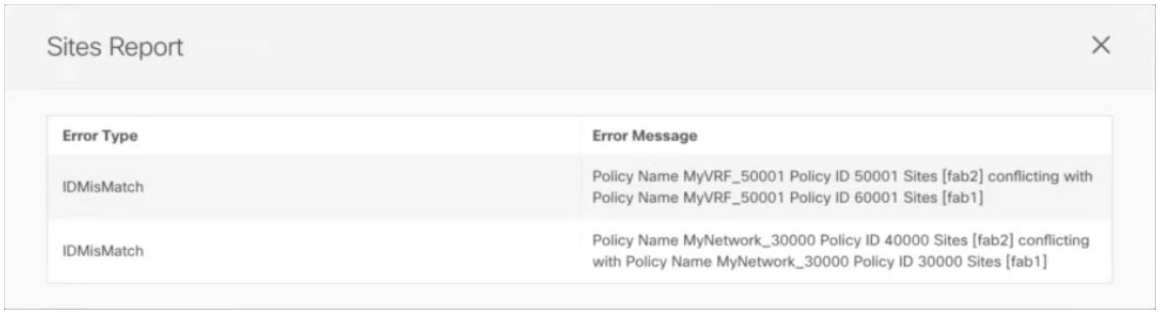
a) Click **Click to View** link in the conflict notification pop-up.



Conflicts needs to be resolved in order to deploy

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.



Sites Report

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

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

d) Unmanage the site in NDO, as described in Removing Sites, on page 5.

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

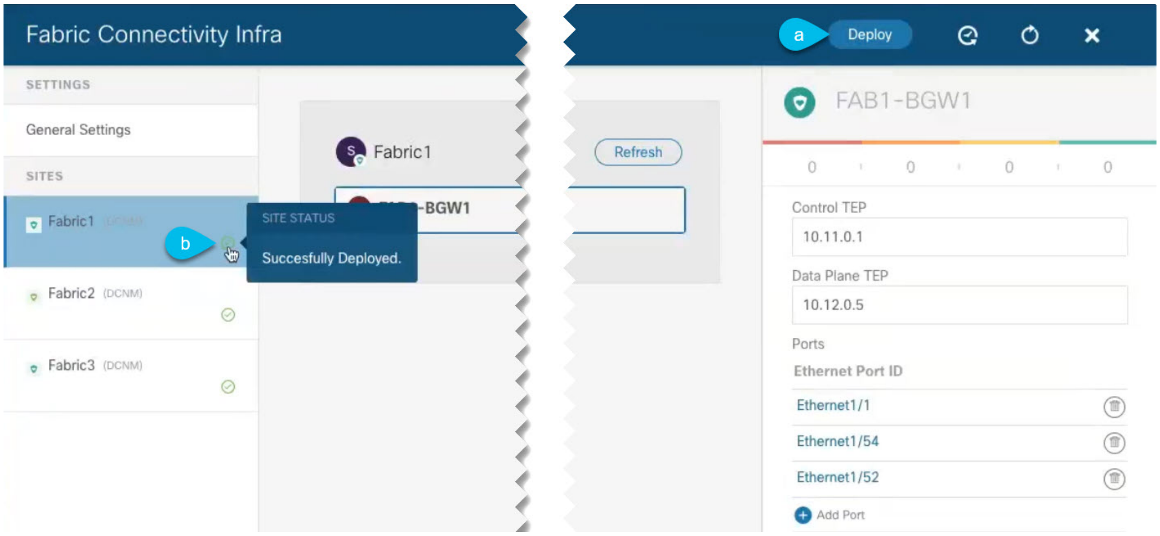
e) Resolve the existing configuration conflicts.

f) Manage the site again, as described in Adding Cisco NDFC Sites, on page 3.

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.



SITE STATUS

Succesfully Deployed.

Control TEP: 10.11.0.1

Data Plane TEP: 10.12.0.5

Ports

Ethernet Port ID
Ethernet1/1
Ethernet1/54
Ethernet1/52

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 NDFC 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 NDFC 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 4

Fabric Management

- Tenants Overview, on page 15
- Schemas and Templates, on page 17
- Concurrent Configuration Updates, on page 18
- Creating Schemas and Templates, on page 20
- Bulk Update of Template Objects , on page 26
- Template Versioning, on page 28
- Template Review and Approval, on page 32
- Deploying Templates, on page 34
- Disassociating Template from Sites, on page 36
- Configuration Drifts, on page 36
- Viewing Currently Deployed Configuration, on page 40
- Schema Overview and Deployment Visualizer, on page 41

Tenants Overview

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.

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

Three default 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 NDFC fabrics.

  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

- `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 NDFC fabrics, you will always use the default `dcnm-default-tn` tenant.

Tenant Policies Templates

This section provides a number of tenant templates that are supported for on-premises ACI fabrics managed by Cisco APIC. For additional information, see the *Cisco Nexus Dashbaord Orchestrator Configuration Guide for ACI Fabrics*.

Add Users to NDFC Tenant

This section describes how to add users to the existing default `dcnm-default-tn` tenant which you will use when creating schema templates for your NDFC configurations.

Before you begin

You must have a user with either `Power User` or `Site Manager` read-write role to manage tenants.

Step 1 Log in to your Nexus Dashboard and open the Nexus Dashboard Orchestrator service.

Step 2 Select the `dcnm-default-tn` tenant.

a) From the left navigation pane, choose **Application Management** > **Tenants**.

b) In the main pane, click `dcnm-default-tn` tenant name.

The **Update Tenant** screen opens.

Step 3 Provide tenant details.

The tenant's **Display Name** is used throughout the Orchestrator's GUI whenever the tenant is shown. However, due to object naming requirements on the APIC, any invalid characters are removed and the resulting **Internal Name** is used when pushing the tenant to sites. The **Internal Name** that will be used when creating the tenant is displayed below the **Display Name** textbox.

Note You can change the **Display Name** of the tenant at any time, but the **Internal Name** cannot be changed after the tenant is created.

a) In the **Associated Sites** section, check all the sites you want to associate with this tenant.

Only the selected sites will be available for any templates using this tenant.

b) In the **Associated Users** section, select the Nexus Dashboard Orchestrator users that are allowed to access the tenant.

Only the selected users will be able to use this tenant when creating templates.

Step 4 Click **Save** to finish adding the tenant.

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.

Template Types

There are 3 types of templates available in Nexus Dashboard Orchestrator, each designed for a specific purpose:

- **ACI Multi-Cloud**—Templates used for Cisco ACI on-premises and cloud sites, which allow template and object stretching between multiple sites. This template supports two deployment types:
  - `Multi-Site` - The template can be associated to a single site (site-local policies) or to multiple sites (stretched policies) and the option should be selected for Multi-Site Network (ISN) or VXLAN intersite communication.
  - `Autonomous` - The template can be associated to one or more sites that are operated independently and are not connected through an Inter-Site Network (no intersite VXLAN communication).

  This guide described Nexus Dashboard Orchestrator configurations for on-premises Cisco NDFC fabrics. For information on working with Cisco ACI sites, see the *Cisco Nexus Dashboard Orchestrator Configuration Guide for ACI Fabrics* instead.

- **NDFC**—Templates designed for Cisco Nexus Dashboard Fabric Controller (formerly Data Center Network Manager) sites.

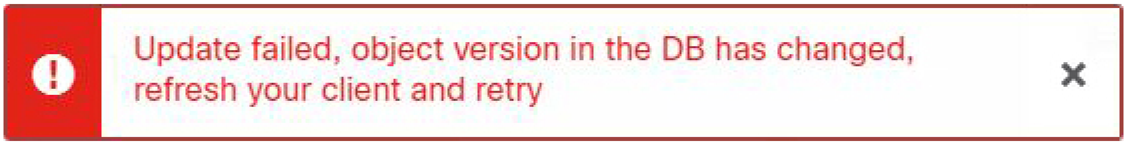
  The following sections focus primarily on this type of template.

- **Cloud Local**—Templates designed for specific Cloud Network Controller use cases, such as Google Cloud site connectivity, and cannot be stretched between multiple sites.

  This guide described Nexus Dashboard Orchestrator configurations for on-premises Cisco NDFC fabrics. For information on working with Cloud Network Controller fabrics, see the Nexus Dashboard Orchestrator use case library instead.

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:



Update failed, object version in the DB has changed, refresh your client and retry

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 the user accounts which you will use to create and modify schemas already associated with the Tenant that those schemas will use, as described in Add Users to NDFC Tenant, on page 16

Step 1 Log in to your Nexus Dashboard and open the Nexus Dashboard Orchestrator service.

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 and click **Add**.

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

Step 3 Create a template.

a) In the schema page, click **View** > **Overview** and choose **Add New Template**.

b) In the **Select a Template type** window, choose `NDFC` and click **Add**.

- **ACI Multi-Cloud**—Templates used for Cisco ACI on-premises and cloud sites, which allow template and object stretching between multiple sites. This template supports two deployment types:

  - `Multi-Site` - The template can be associated to a single site (site-local policies) or to multiple sites (stretched policies) and the option should be selected for Multi-Site Network (ISN) or VXLAN intersite communication.
  - `Autonomous` - The template can be associated to one or more sites that are operated independently and are not connected through an Inter-Site Network (no intersite VXLAN communication).

  This guide described Nexus Dashboard Orchestrator configurations for on-premises Cisco NDFC fabrics. For information on working with Cisco ACI sites, see the *Cisco Nexus Dashboard Orchestrator Configuration Guide for ACI Fabrics* instead.

- **NDFC**—Templates designed for Cisco Nexus Dashboard Fabric Controller (formerly Data Center Network Manager) sites.

  The following sections focus primarily on this type of template.

- **Cloud Local**—Templates designed for specific Cloud Network Controller use cases, such as Google Cloud site connectivity, and cannot be stretched between multiple sites.

  This guide described Nexus Dashboard Orchestrator configurations for on-premises Cisco NDFC fabrics. For information on working with Cloud Network Controller fabrics, see the Nexus Dashboard Orchestrator use case library instead.

c) In the right sidebar, provide the **Display Name** for the template.

d) (Optional) Provide a **Description**.

e) From the **Select a Tenant** dropdown, select the `dcnm-default-tn` tenant.

f) In the template view page, click **Save**.

You must save the template after this initial configuration for additional options (such as site association) to become available.

g) Repeat this step to create any additional templates.

For more information on schema and template design, see Schemas and Templates, on page 17.

Step 4 Assign the templates to sites.

You deploy fabric configuration by deploying one template at a time to one or more sites. So you need to associate the template with at least one site where you want to deploy the configuration.

a) In the template view page, click **Actions** and choose **Sites Association**.

b) In the **Add Sites to <template>** dialog, select one or more sites where you want to deploy the template and click **Ok**.

What to do next

After you have created a schema and one or more templates, you can proceed with editing the templates as described in the following sections of this document based on your specific use cases. After you finish defining configurations, you can deploy the templates as described in Deploying Templates, on page 34.

Importing Schema Elements From NDFC 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 20.

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

Step 2 Create a VRF.

a) In the schema edit view, choose **Create Object** > **VRF**.

b) In the properties pane on the right, provide **Display Name** for the VRF.

c) (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 7.

d) 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 NDFC. Any profiles created in NDFC are automatically imported into the NDO and are available for selection here.

e) 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 NDFC. Any profiles created in NDFC are automatically imported into the NDO and are available for selection here.

f) 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.

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

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

h) (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.

i) (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 3 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) From the **Template Properties** dropdown, select the site with which this template is associated..
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 NDFC 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 20.
- You must have the VRF created as described in Creating VRFs, on page 22

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

Step 2 Create a Network.

a) In the template edit view, choose **Create Object** > **Network**.

b) In the properties pane on the right, provide **Display Name** for the network.

c) (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.

d) Choose whether or not this is a **Layer2 Only** network.

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

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

f) 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 NDFC. Any profiles created in NDFC are automatically imported into the NDO and are available for selection here.

g) 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 NDFC. Any profiles created in NDFC are automatically imported into the NDO and are available for selection here.

h) Provide the **VLAN ID** for the network.

i) Provide the **VLAN Name**.

j) Add one or more **Subnets**.

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

1. Click **+Add Subnet**.

An **Add Subnet** window opens.

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

   You can configure up to four gateway IPs.

3. Choose `Primary` for the first gateway you add.

4. lick the checkmark to save the gateway information.

5. Repeat the previous substeps to provide additional gateways.

6. Click **Add** to finish adding the subnet.

k) Choose whether you want to **Suppress ARP**.
l) Provide the **MTU** for this network.
m) Provide the **Routing Tag**.

Step 3 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.

Bulk Update of Template Objects

The bulk update feature allows you to update multiple properties on multiple different objects of the same type within a template at once. When using this workflow, all selected objects must be of the same type otherwise the update feature won't work. For example, in the case of Cisco NDFC you cannot choose to update a VRF and Network simultaneously.

You can use "Select" on a type of object then update the properties of those objects. If the selected objects already have different property values configured on them, the update will overwrite those properties with the values you provide.

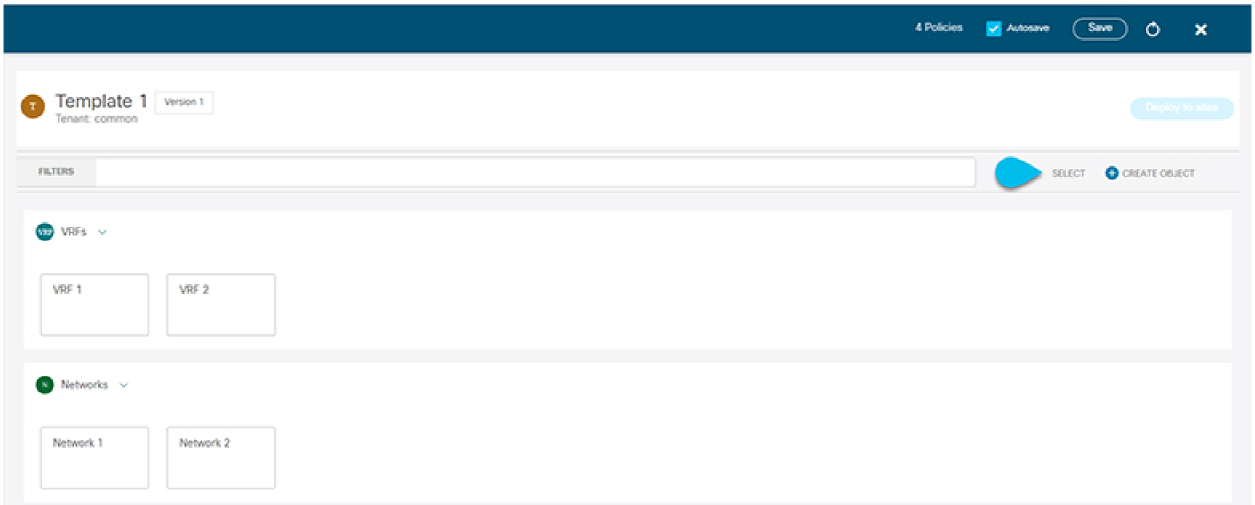
Note This feature is supported for Cisco APIC and Cisco NDFC fabrics only; it is not supported for Cisco Cloud Network Controller sites.

The following example will walk you through the process.

Step 1 Navigate to the schema and template that contains the objects you want to update.

Step 2 The following figure shows all the objects belonging to a single template.

Choose "Select". It will allow you select multiple objects at once.

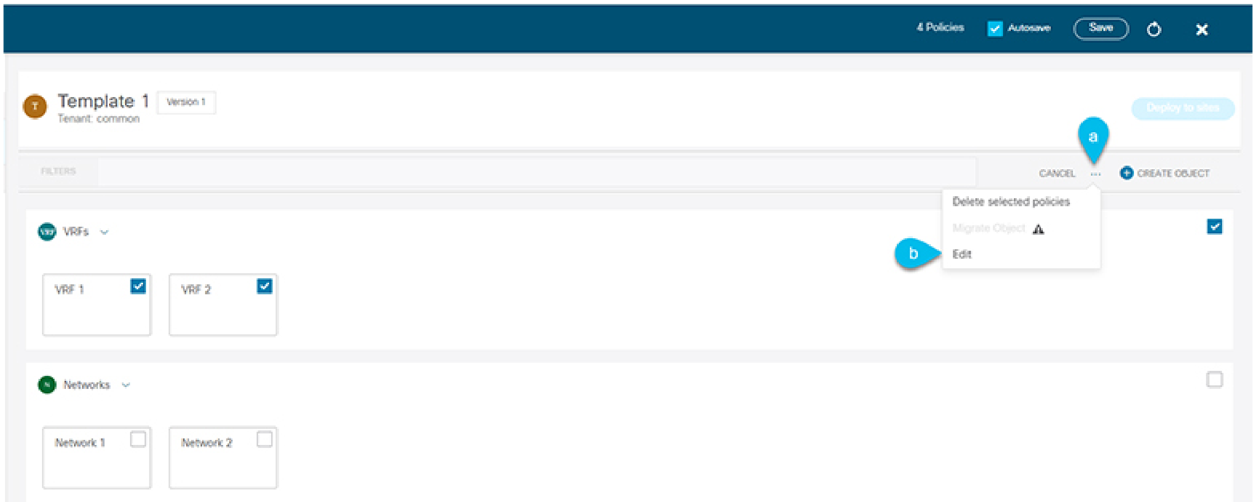


Step 3 After selecting all the objects that you want to update.

a) Choose "…" right next to the cancel option.

b) From the dropdown Choose "Edit".

If you choose objects of different type, you won't see the Edit option in the dropdown.

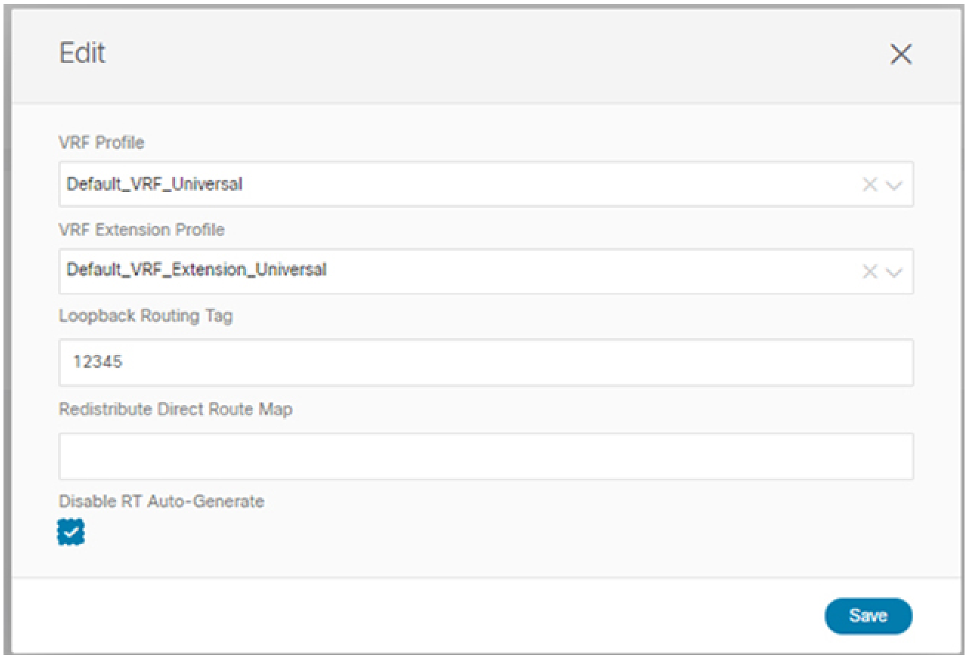


Step 4 After choosing “Edit”, a pop-up will show up.

You can update the following properties based on the type of objects you selected.

a. **VRF**: VRF Profile, VRF Extension Profile, Loopback Routing Tag, Redistribute Direct Route Map, Disable RT Auto-Generate.

b. **Network**: Layer2 Only, Network Profile, Network Extension Profile.


Edit

VRF Profile: Default_VRF_Universal

VRF Extension Profile: Default_VRF_Extension_Universal

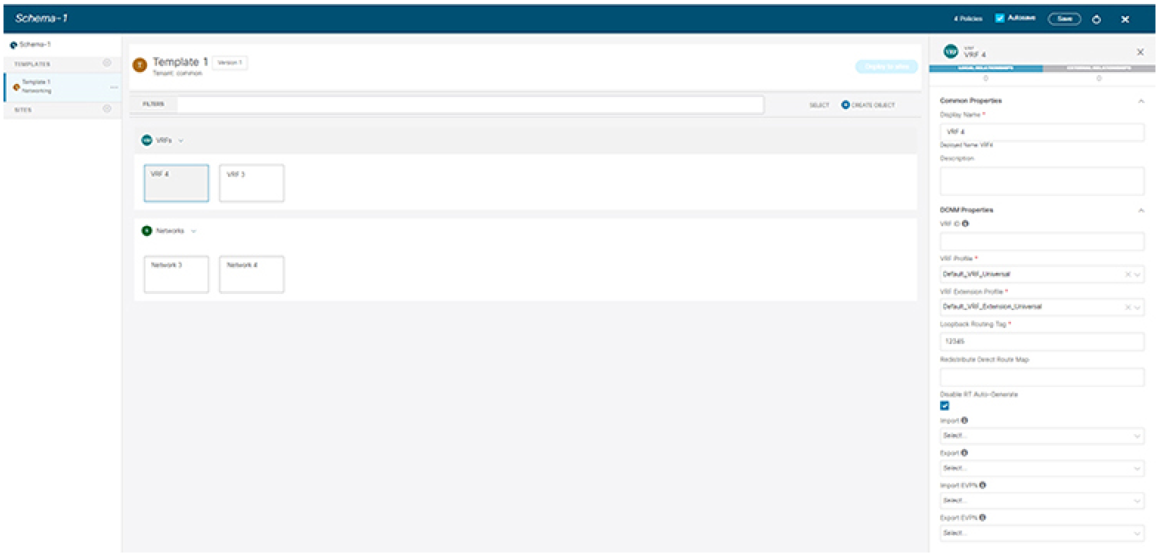
Loopback Routing Tag: 12345

Redistribute Direct Route Map:

Disable RT Auto-Generate: ☑

Step 5 Choose “Save”, it will implement the updates you've made.

Step 6 As you save the updates, you can see the changes you made.



Common Properties

Display Name *: VRF 4

Deployed Name: VRF4

Description:

DCNM Properties

VRF ID:

VRF Profile *: Default_VRF_Universal

VRF Extension Profile *: Default_VRF_Extension_Universal

Loopback Routing Tag *: 12345

Redistribute Direct Route Map:

Disable RT Auto-Generate: ☑

Import: Select...

Export: Select...

Import EVPN: Select...

Export EVPN: Select...

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.

Template versions are created and maintained according to the following rules:

- All template versions are either `Deployed` or `Intermediate`.

  `Deployed`—versions of the template that have been deployed to sites.

  `Intermediate`—versions of the template that have been modified and saved, but not deployed to sites.

- A maximum of 20 `Deployed` and 20 `Intermediate` versions per template can be stored at any given time.

- When a new `Intermediate` version is created that would exceed the 20 version limit, the earliest existing `Intermediate` version is deleted.

- When a template is deployed and a new `Deployed` version is created, all `Intermediate` versions are deleted. If the new `Deployed` version exceeds the 20 version limit, the earliest existing `Deployed` version is deleted.

- Tagging a version `Golden` does not affect the number of stored template versions.

- A template that is tagged `Golden` cannot be deleted.

  You must untag the template first before you can delete it.

- When a template is modified and saved or deployed, any versions that exceed the 20 `Deployed` and 20 `Intermediate` scale are removed according to the above rules.

- When upgrading from a release prior to 4.0(1) to release 4.0(1) or later, only the latest versions of templates are preserved.

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.

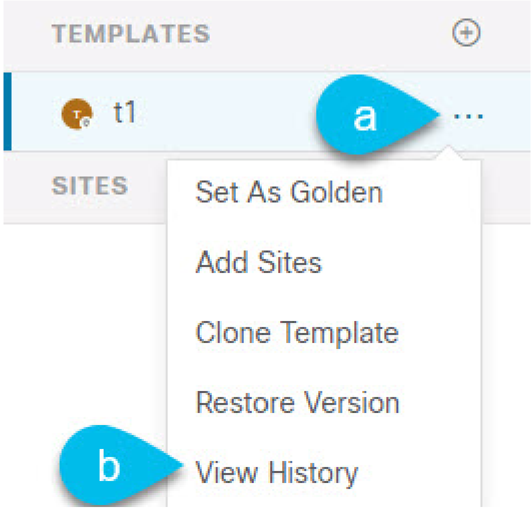
Step 1 Log in to your Nexus Dashboard Orchestrator GUI.

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

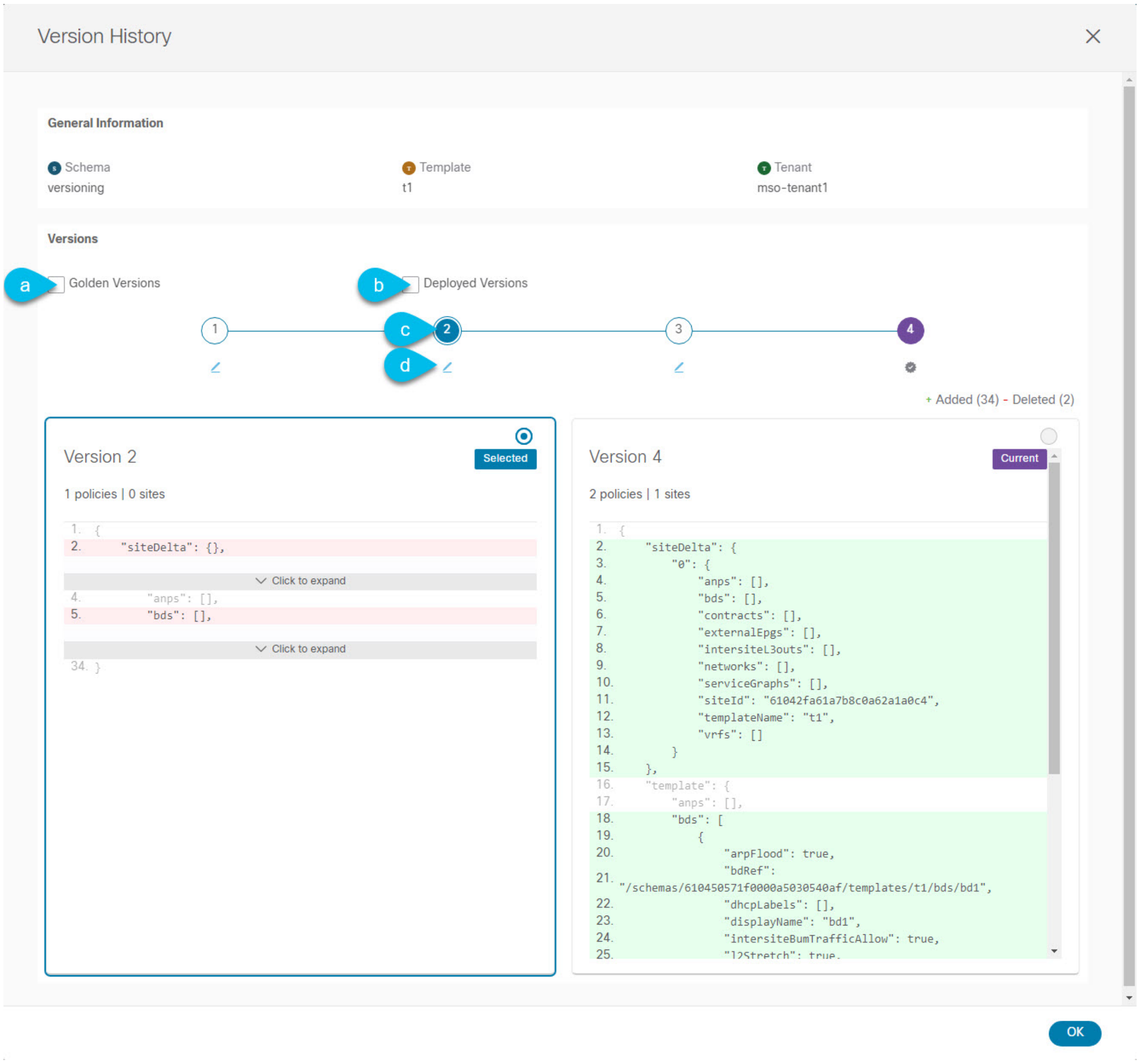
Step 3 Click the schema that contains the template you want to view.

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.



Version History

General Information

Schema: versioning
Template: t1
Tenant: mso-tenant1

Versions

□ Golden Versions
□ Deployed Versions

+ Added (34) - Deleted (2)

Version 2 — Selected

1 policies | 0 sites

```
{
    "siteDelta": {},
        "anps": [],
        "bds": [],
}
```

Version 4 — Current

2 policies | 1 sites

```
{
    "siteDelta": {
        "0": {
            "anps": [],
            "bds": [],
            "contracts": [],
            "externalEpgs": [],
            "intersiteL3outs": [],
            "networks": [],
            "serviceGraphs": [],
            "siteId": "61042fa61a7b8c0a62a1a0c4",
            "templateName": "t1",
            "vrfs": []
        }
    },
    "template": {
        "anps": [],
        "bds": [
            {
                "arpFlood": true,
                "bdRef":
"/schemas/610450571f0000a5030540af/templates/t1/bds/bd1",
                "dhcpLabels": [],
                "displayName": "bd1",
                "intersiteBumTrafficAllow": true,
                "l2Stretch": true,
```

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 29.

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 **Rollback**.

Step 6 In the **Rollback** 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.

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 32 sections.

Template Review and Approval

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.

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 32.

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 32.
- Created or updated users in Nexus Dashboard with `approver` and `deployer` roles, as described in Create Users with Required Roles, on page 32.
- 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 32.
- Created or updated users in Nexus Dashboard with `approver` and `deployer` roles, as described in Create Users with Required Roles, on page 32.
- 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 33.

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 29.

You can also click **Deployment Plan** to see a visualization and a JSON 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 40.

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 34.

Deploying Templates

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

Before you begin

- You must have the schema, template, and any objects you want to deploy to sites already created and the templates assigned to one or more sites, as described in previous sections of this document.
- If template review and approval is enabled, the template must also be already approved by the required number of approvers as described in Template Review and Approval, on page 32.

Step 1 Navigate to the schema that contains the template that you want to deploy.

Step 2 From the **View** dropdown menu, select the template you want to deploy.

Step 3 In the template view, click **Deploy to sites**.

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

Step 4 If you have made changes to your template, review the **Deployment Plan** to verify the new configuration.

If you have previously deployed this template but made no changes to it since, the **Deploy** summary will indicate that there are no changes and you can choose to re-deploy the entire template. In this case, you can skip this step.

The **Deploy to sites** window will show you a summary of the configuration differences that will be deployed to sites.

You can also 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**.

Here you can also choose to:

- **View Version History**, which shows 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 29.
- Check the **Deployment Plan** to see a visualization and an XML payload of the configuration that will be deployed from this template.

  This feature provides better visibility into configuration changes that the Orchestrator will provision to the different fabrics that are part of your Multi-Site domain after you make a change to the template and deploy it to one or more sites.

  Unlike earlier releases of the Nexus Dashboard Orchestrator, which still provided a list of specific changes made to the template and site configuration, the Deployment Plan provides full visibility into all the objects that the deployment of the template would provision across the different fabrics. For example, depending on what change you make, shadow objects may be created in multiple sites even if the specific change is applied to only a single site.

  Note We recommend verifying your changes using the Deployment Plan as described in this step before deploying the template. The visual representation of the configuration changes can help you reduce potential errors from deploying unintended configuration changes.

a) Click the **Deployment Plan** button.

b) Verify your changes in the first listed site.

c) Repeat the previous substep to verify the changes in other sites

d) (Optional) Click **View Payload** to see the XML payload for each site.

In addition to the visual representation of the new and modified objects, you can also choose to **View Payload** for the changes in each site.

e) After you are done verifying the changes, click the `x` icon to close the **Deployment Plan** screen.

Step 5 In the **Deploy to sites** window, click **Deploy** to deploy the template.

Disassociating Template from Sites

You can choose to disassociate a template from a site without undeploying it. This allows you to preserve any configuration deployed to the site from NDO while removing the template-site association in the schema. The managed object and policy ownership is transferred from NDO to the site's controller.

Before you begin

- The template and its configuration must already be deployed to a site.
- The template must be deployed to a single site only and not stretched across sites.
- The objects defined in the template must not be deployed as shadow objects in other sites.

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 disassociate.

Step 4 In the Schema view, select the template under the specific site from which you want to disassociate it.

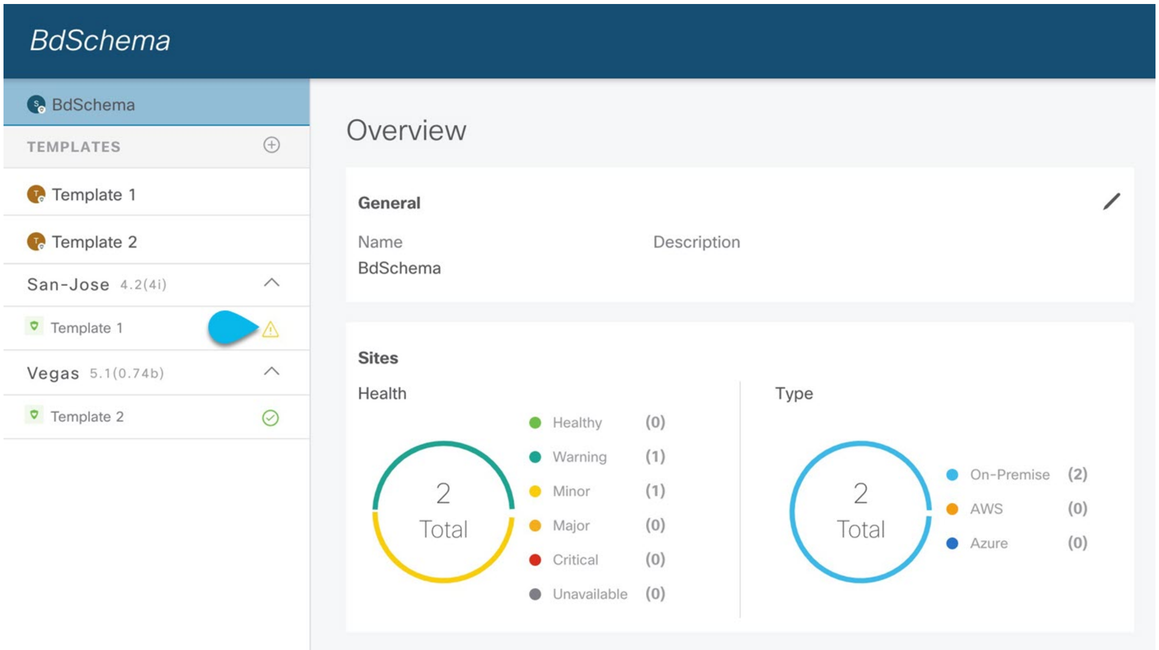
Step 5 From the **Actions** menu, select **Disassociate Template**.

Step 6 In the confirmation window, click **Confirm Action**.

Configuration Drifts

Occasionally, you may run into a situation where the configuration actually deployed in a NDFC domain is different from the configuration defined for that domain in the Nexus Dashboard Orchestrator. These configuration discrepancies are referred to as **Configuration Drifts** and are indicated by a yellow warning sign next to the template name in the schema view as shown in the following figure:

Figure 1:



Configuration drifts can manifest due to a number of different reasons. Specific steps required to resolve a configuration drift depends on its cause. Most common scenarios and their resolutions are outlined below:

- **Configuration is modified in NDO**—when you modify a template in NDO GUI, it will show as configuration drift until you deploy the changes to the sites.

  To resolve this type of configuration drift, either deploy the template to apply the changes to the sites or revert the changes in the schema.

- **Configuration is modified directly in the site's controller**—while the objects deployed from NDO are indicated by a warning icon and text in the site's NDFC, an admin user can still make changes to them causing the configuration drift.

- **NDO configuration is restored from backup**—restoring configuration from a backup in NDO restores only the objects and their state as they were when the backup was created, it does not automatically re-deploy the restored configuration. As such, if there were changes made to the configuration and deployed on NDFC since the backup was created, restoring the backup would create a configuration drift.

- **NDO configuration is restored from a backup created on an older release**—if the newer release added support for object properties which were not supported by the earlier release, these properties may cause configuration drift warning. Typically, this happens if the new properties were modified directly in the site's NDFC GUI and the values are different from the defaults assumed by the Nexus Dashboard Orchestrator

- **NDO is upgraded from an earlier release**—this scenario is similar to the previous one where if new object properties are added in the new release, existing configuration may indicate a drift.

  We recommend running the "Reconcile Drift" workflow for the template, to have more visibility into the causes of the drift and be able to reconcile it. This recommendation applies to all the drift scenarios previously described in this section. For more information on the drift reconciliation workflow, see the "Reconciling Configuration Drifts" section below.

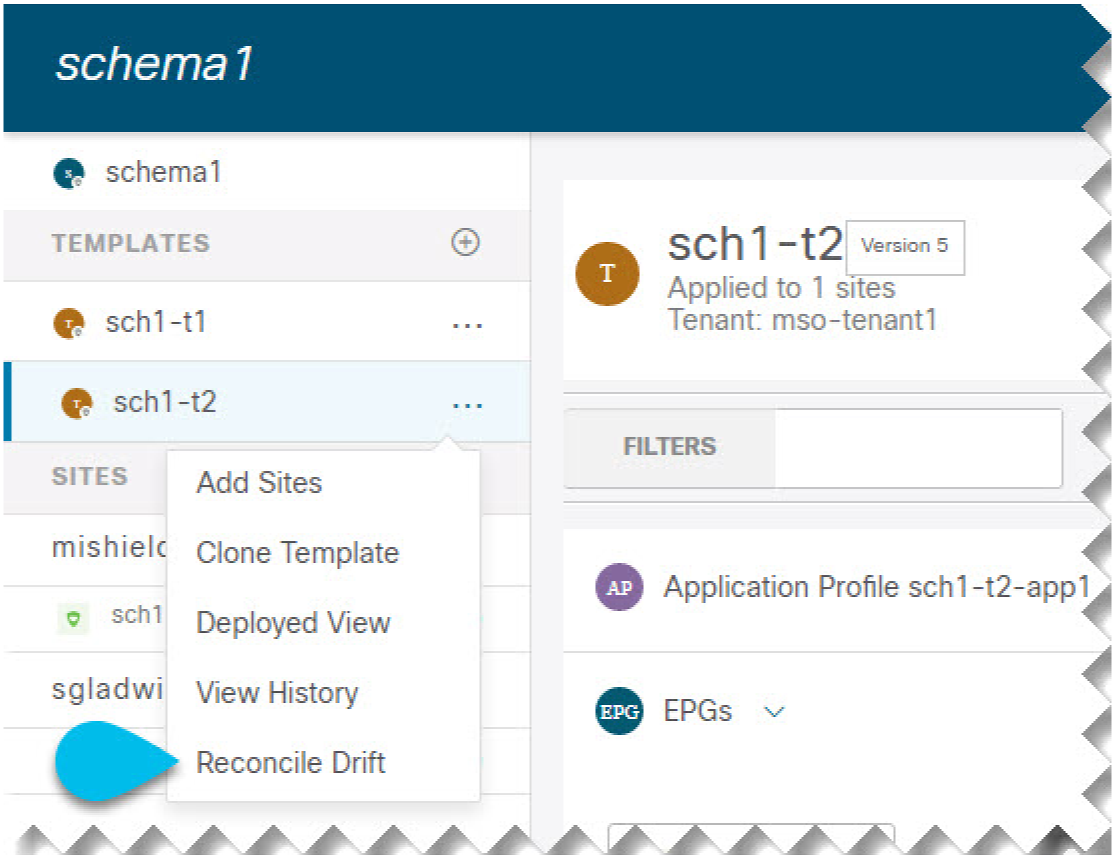
Reconciling Configuration Drifts

NDO release 3.6(1) introduced support for a drift reconciliation workflow that can be run to compare the template configuration defined on Nexus Dashboard Orchestrator and the configuration rendered in the NDFC controllers of the sites part of the Multi-Site domain. This allows to provide more visibility into what causes the configuration drift (i.e. changes that have been made on Nexus Dashboard Orchestrator or on NDFC directly) and give the user the choice on how to reconcile the drift, as described in the steps below.

Note If you do not want the configurations you chose, you can close the schema and re-open. This will show the original configurations. You can re-trigger "Reconcile Drift" flow again if needed. The schema will get saved only after you choose Save or Deploy button.

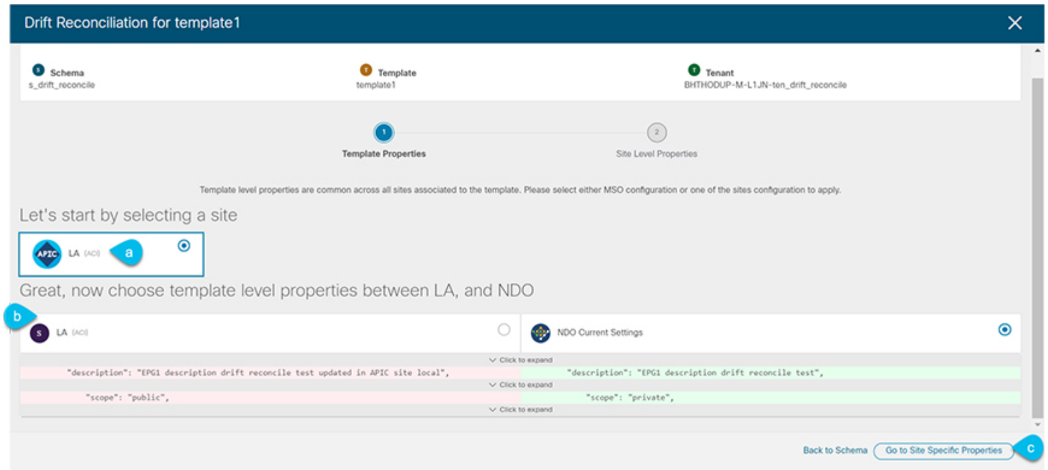
Step 1 Navigate to the schema that contains the template you want to check for configuration drifts.

Step 2 From the template's **Actions** menu, select **Reconcile Drift**.



The **Drift Reconciliation** wizard opens.

Step 3 In the **Drift Reconciliation** screen, compare the template-level configurations for each site and choose the one you want.



Template level properties are common across all sites associated to the template. Please select either MSO configuration or one of the sites configuration to apply.

Let's start by selecting a site

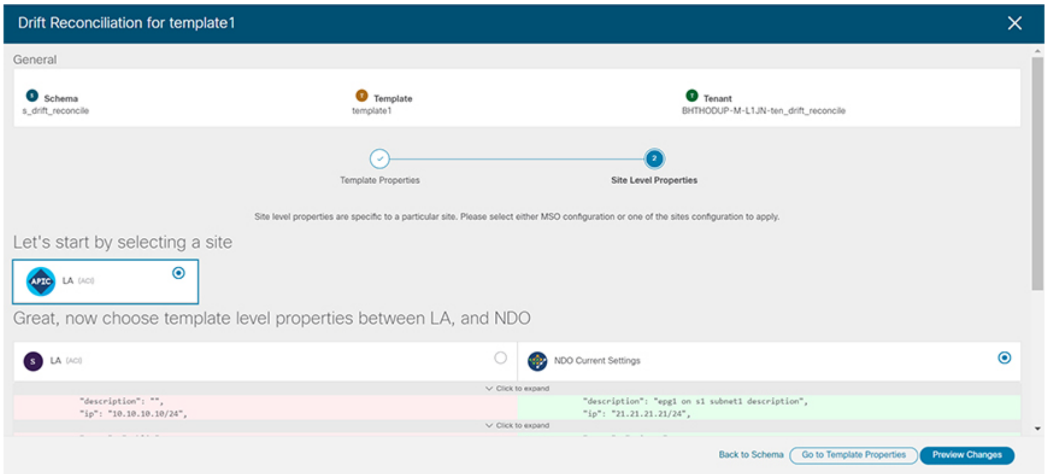
Great, now choose template level properties between LA, and NDO

```
"description": "EPG1 description drift reconcile test updated in APIC site local",
"scope": "public",
```

```
"description": "EPG1 description drift reconcile test",
"scope": "private",
```

Template-level properties are common across all sites associated to the template. You can compare the template level properties defined on Nexus Dashboard Orchestrator with the configuration rendered in each site and decide what should become the new configuration in the Nexus Dashboard Orchestrator template. Selecting the site configuration will modify those properties in the existing Nexus Dashboard Orchestrator template, whereas selecting the Nexus Dashboard Orchestrator configuration will keep the existing Nexus Dashboard Orchestrator template settings as is

Step 4 Click **Go to Site Specific Properties** to switch to site-level configuration.



Site level properties are specific to a particular site. Please select either MSO configuration or one of the sites configuration to apply.

Let's start by selecting a site

Great, now choose template level properties between LA, and NDO

```
"description": "",
"ip": "10.10.10.10/24",
```

```
"description": "epg1 on s1 subnet1 description",
"ip": "21.21.21.21/24",
```

You can choose a site to compare that specific site's configuration. Unlike template-level configurations, you can choose either the Nexus Dashboard Orchestrator-defined or actual existing configurations for each site individually to be retained as the template's site-local properties for that site.

Even though in most scenarios you will make the same choice for both template-level and site-level configuration, the drift reconciliation wizard allows you to choose the configuration defined in the site's controller at the "Template Properties" level and the configuration defined in Nexus Dashboard Orchestrator at the "Site Local Properties" level or vice versa.

Step 5 Click **Preview Changes** to verify your choices.

The preview will display full template configuration adjusted based on the choices picked in the **Drift Reconciliation** wizard. You can then click **Deploy to sites** to deploy the configuration and reconcile the drift for that 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.

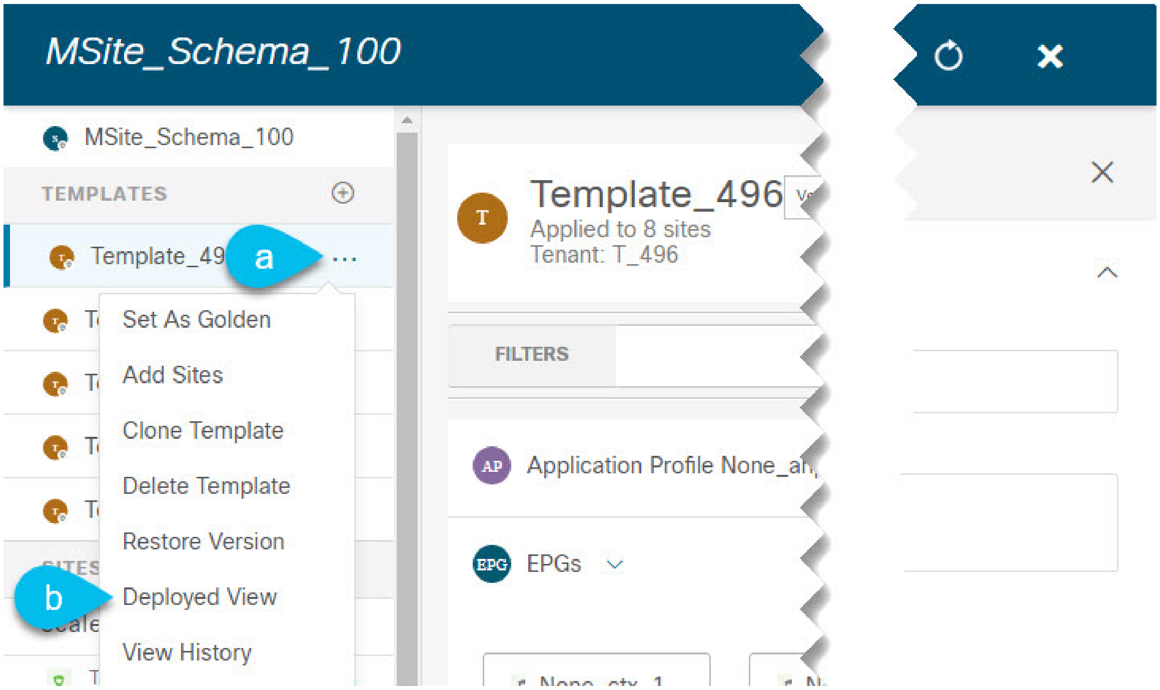
Step 1 Log in to your Nexus Dashboard Orchestrator GUI.

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.

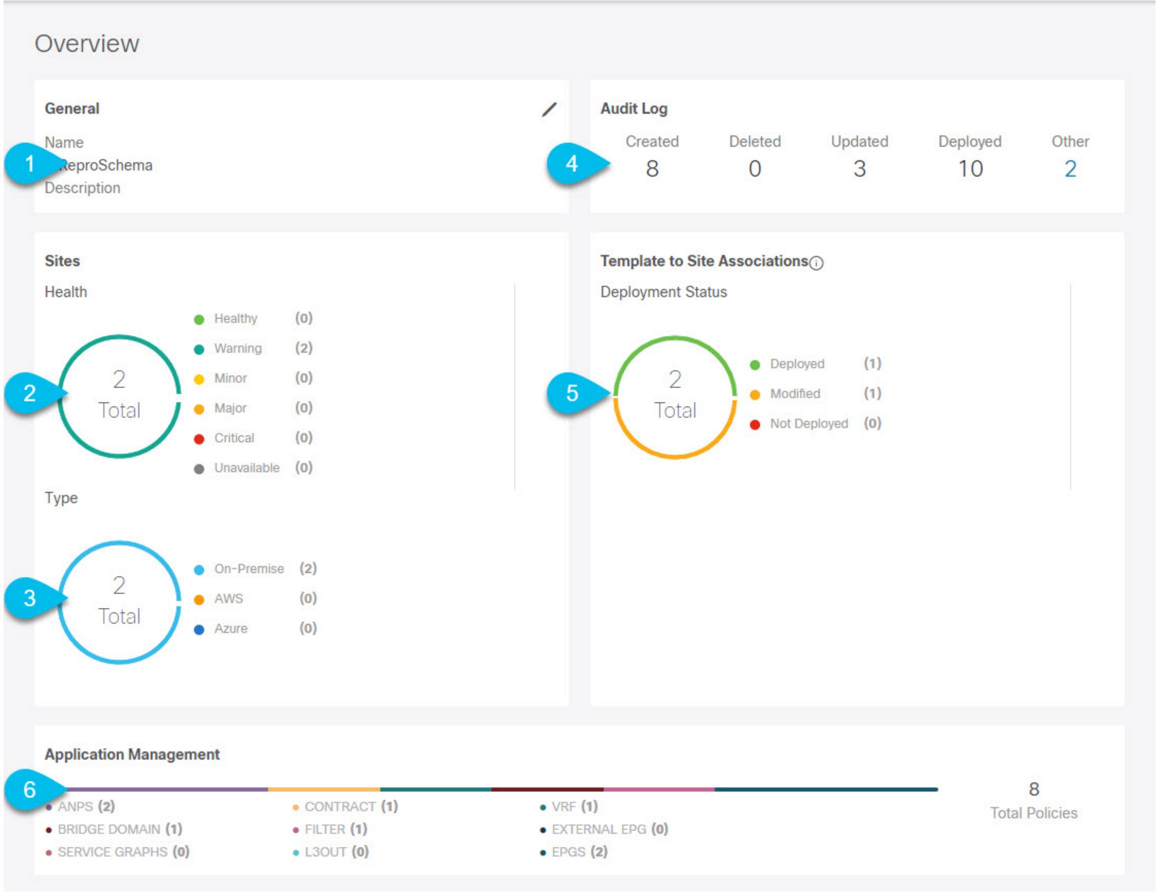
b) You can click on a site name to show configuration for that specific site.

c) You can click **View JSON** to see the 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



Overview

General

Name
ReproSchema
Description

Audit Log

Created	Deleted	Updated	Deployed	Other
8	0	3	10	2

Sites

Health

2 Total

● Healthy	(0)
● Warning	(2)
● Minor	(0)
● Major	(0)
● Critical	(0)
● Unavailable	(0)

Type

2 Total

● On-Premise	(2)
● AWS	(0)
● Azure	(0)

Template to Site Associations ⓘ

Deployment Status

2 Total

● Deployed	(1)
● Modified	(1)
● Not Deployed	(0)

Application Management

● ANPS (2)	● CONTRACT (1)	● VRF (1)
● BRIDGE DOMAIN (1)	● FILTER (1)	● EXTERNAL EPG (0)
● SERVICE GRAPHS (0)	● L3OUT (0)	● EPGS (2)

8
Total Policies

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.

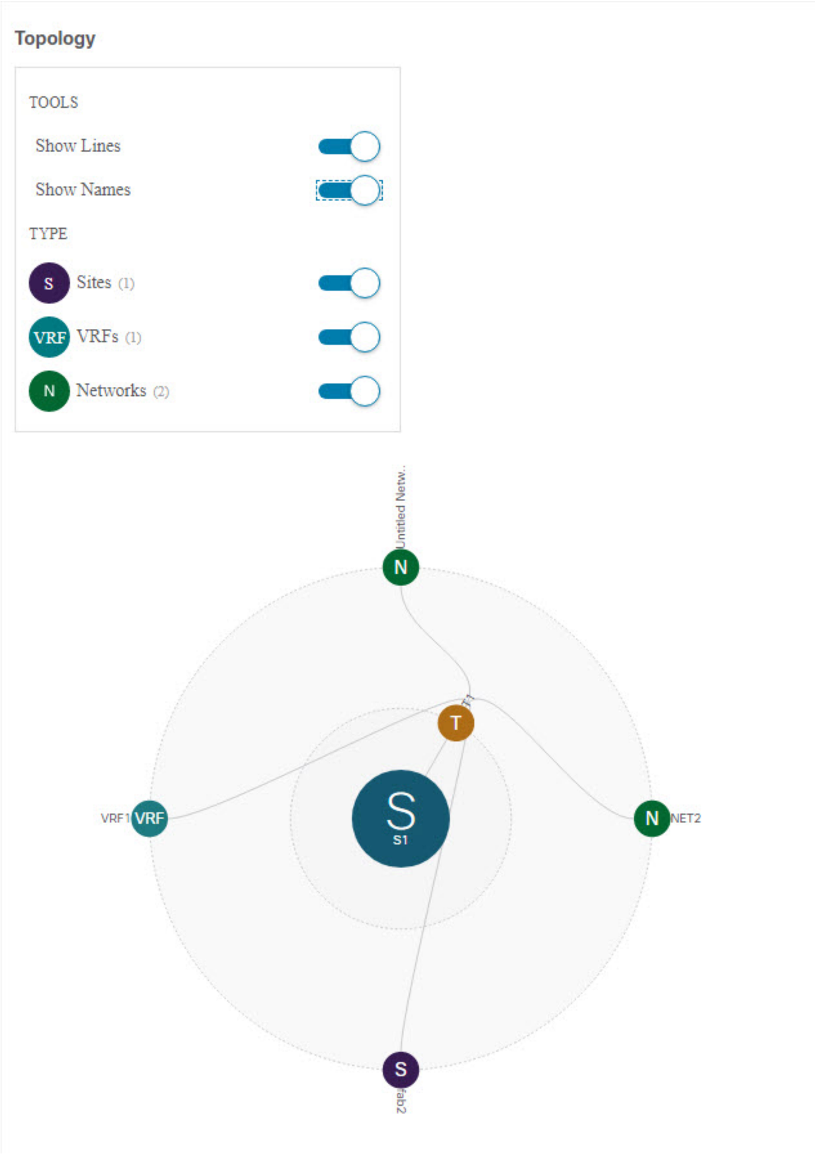
4. **Sites** > **Type**—Provides the number of sites associated with the templates in this schema sorted by the site's type.

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



Topology

TOOLS

Show Lines

Show Names

TYPE

Sites (1)

VRFs (1)

Networks (2)

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 and Infrastructure

- Audit Logs, on page 47
- Backup and Restore, on page 49
- Tech Support, on page 61
- System Configuration, on page 67

CHAPTER 5

Audit Logs

- Audit Logs, on page 47

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 6

Backup and Restore

- Configuration Backup and Restore, on page 49
- Configuration Backup and Restore Guidelines, on page 49
- Configuring Remote Locations for Backups, on page 52
- Importing Backups to Remote Location, on page 53
- Creating Backups, on page 53
- Restoring Backups, on page 54
- Exporting (Downloading) Backups, on page 58
- Backup Scheduler, on page 59

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.

Configuration Backup and Restore Guidelines

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.

When creating 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 4.0(1) is supported only during the initial upgrade to this release.

If you want to upgrade from a release prior to release 4.0(1) to this release, see the "Upgrading NDO Service in Nexus Dashboard" chapter in the *Cisco Nexus Dashboard Orchestrator Deployment Guide*.

- 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 Network Controller, or NDFC) databases on each site.

  We recommend that after you restore the Orchestrator database you resolve any configuration drifts that may appear in the templates, as described in "Configuration Drifts" section of this guide, and then re-deploy the existing templates to avoid potentially mismatching policies between the Nexus Dashboard Orchestrator and each site's controller.

- When you create a configuration backup, 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 4.0(1) or later, it will be disabled after the upgrade.

  After the upgrade, you will need to re-add any remote locations you had set up and then re-enable backup scheduler.

- Deleting a backup using the UI also deletes the backup files from the remote location.

When restoring configuration backups, the following guidelines apply:

- 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.

- 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.

    We recommend that after you restore the Orchestrator database you resolve any configuration drifts that may appear in the templates, as described in "Configuration Drifts" section of this guide, and then re-deploy the existing templates to avoid potentially mismatching policies between the Nexus Dashboard Orchestrator and each site's controller.

    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, resolve any configuration drifts that may appear in the templates, as described in "Configuration Drifts" section of this guide and re-deploy the templates 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 Remote Locations 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 Importing Backups to Remote Location, on page 53.

Configuring Remote Locations 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 and open the Nexus Dashboard Orchestrator service.

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.

Importing Backups to Remote Location

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 Exporting (Downloading) Backups, on page 58.

  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 Remote Locations 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 Remote Locations for Backups, on page 52.

Step 1 Log in to your Nexus Dashboard Orchestrator.

Step 2 Backup existing deployment configuration.

a) From the left navigation pane, select **Operations** > **Backups & Restore**.

b) In the main window, click **New Backup**.

A **New Backup** window opens.

c) Provide the backup information.

- In the **Name** field, provide the name for the backup file.

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

- From the **Remote Location** drop-down, select a remote location you have configured for storing backups.

- (Optional) In the **Remote Path**, provide the specific directory on the remote server where to save the backup.

  The directory you specify must already exist.

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

- You must have configured a remote location for storing your NDO backups, as described in Configuring Remote Locations for Backups, on page 52.

- Ensure that the backup you want to restore is on the remote location server or import the backup into the remote location, as described in Importing Backups to Remote Location, on page 53.

Note 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 Network Controller, or NDFC) databases on each site.

We recommend that after you restore the Orchestrator database you resolve any configuration drifts that may appear in the templates, as described in "Configuration Drifts" section of this guide, and then re-deploy the existing templates to avoid potentially mismatching policies between the Nexus Dashboard Orchestrator and each site's controller.

For information on specific configuration mismatch scenarios and recommended restore procedures related to each one, see Configuration 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 Configuration 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.

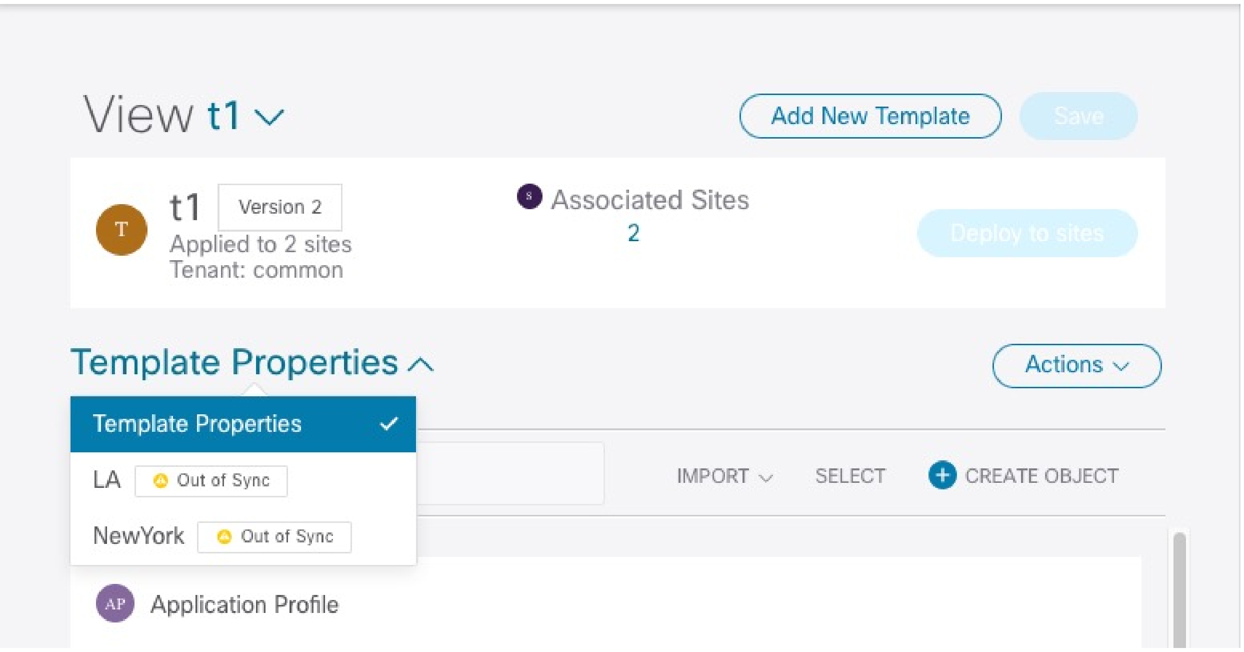
Note Multiple services are restarted during the configuration restore process. As a result, you may notice an up to 10 minute delay before the restored configuration is properly reflected in the NDO GUI.

Step 6 Check if any templates contain configuration drifts.

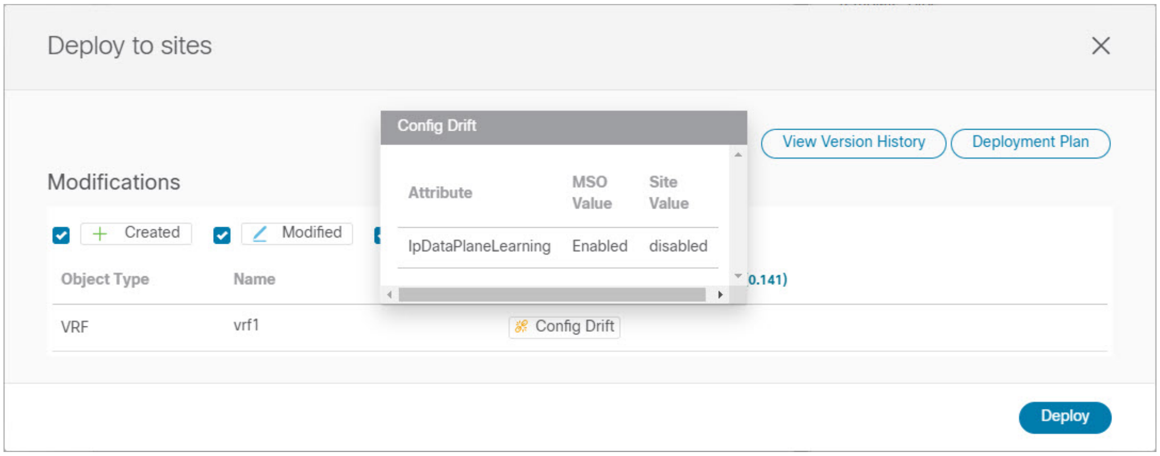
You will repeat the following steps for every schema and template in your deployment

You can check for configuration drifts in one of the following two ways:

- Check the template deployment status icon for each site to which the template is assigned:



- Select the template and click **Deploy to sites** to bring up the configuration comparison screen to check which objects contain configuration drifts:



Attribute	MSO Value	Site Value
IpDataPlaneLearning	Enabled	disabled

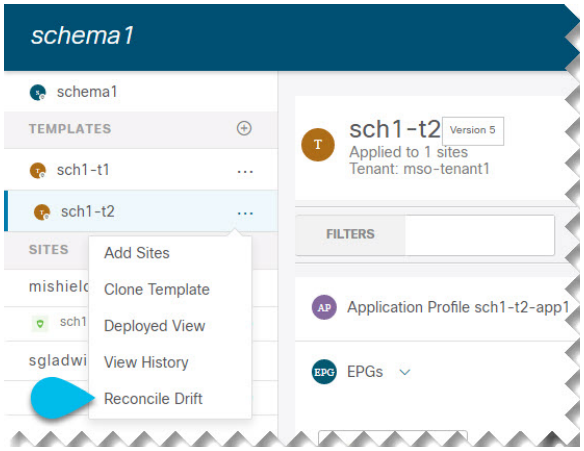
Step 7 If any template contains a configuration drift, resolve the conflicts.

For more information about configuration drifts, check the "Configuration Drifts" chapter in the *Cisco Nexus Dashboard Orchestrator Configuration Guide for ACI Fabrics*.

a) Close the template deployment dialog to return to the Schema view.

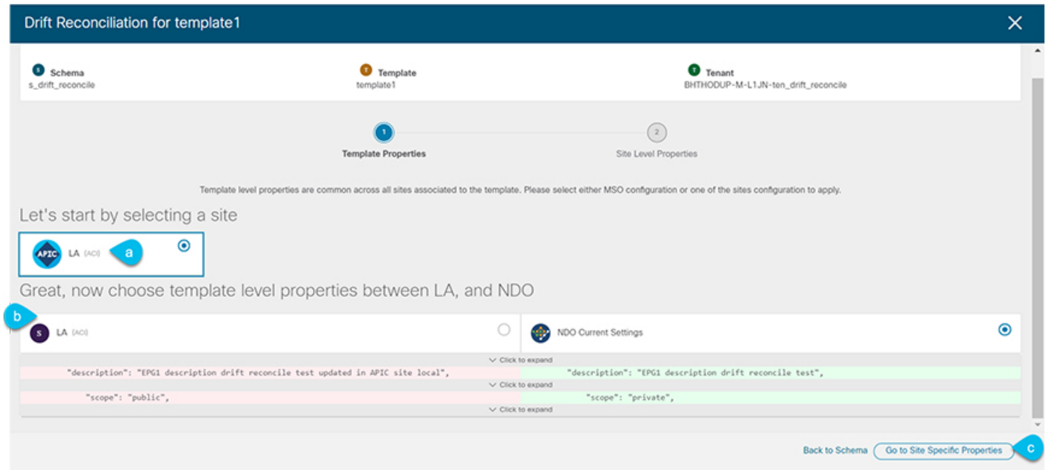
Deploying any templates at this point would push the values in the Orchestrator database and overwrite any existing settings in the fabrics.

b) From the template's **Actions** menu, select **Reconcile Drift**.



The **Drift Reconciliation** wizard opens.

c) In the **Drift Reconciliation** screen, compare the template-level configurations for each site and choose the one you want.



Drift Reconciliation for template1

Schema: s_drift_reconcile
Template: template1
Tenant: BHTHODUP-M-L1JN-ten_drift_reconcile

1 Template Properties — 2 Site Level Properties

Template level properties are common across all sites associated to the template. Please select either MSO configuration or one of the sites configuration to apply.

Let's start by selecting a site

LA (ACI) ●

Great, now choose template level properties between LA, and NDO

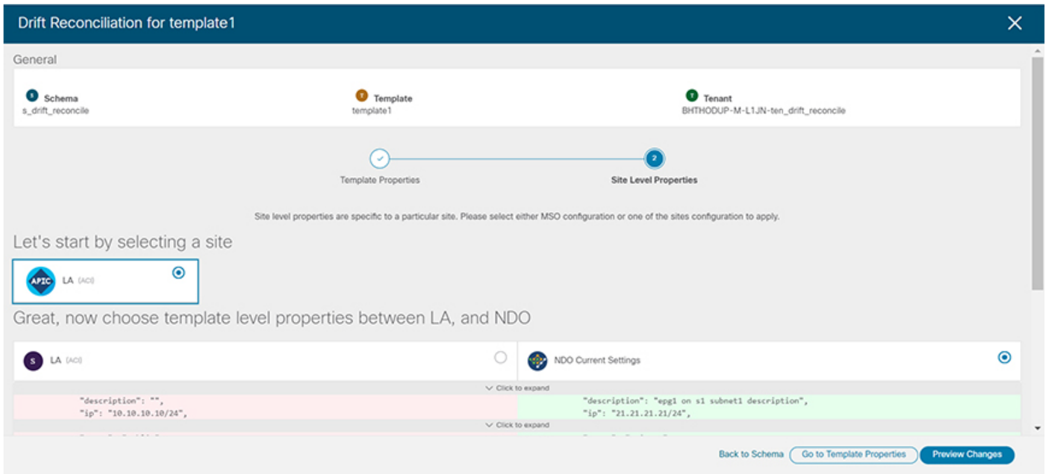
○ LA (ACI) | ● NDO Current Settings

```
        "description": "EPG1 description drift reconcile test updated in APIC site local",
            "scope": "public",
```

```
        "description": "EPG1 description drift reconcile test",
            "scope": "private",
```

Template-level properties are common across all sites associated to the template. You can compare the template level properties defined on Nexus Dashboard Orchestrator with the configuration rendered in each site and decide what should become the new configuration in the Nexus Dashboard Orchestrator template. Selecting the site configuration will modify those properties in the existing Nexus Dashboard Orchestrator template, whereas selecting the Nexus Dashboard Orchestrator configuration will keep the existing Nexus Dashboard Orchestrator template settings as is

d) Click **Go to Site Specific Properties** to switch to site-level configuration.



Drift Reconciliation for template1

General

Schema: s_drift_reconcile
Template: template1
Tenant: BHTHODUP-M-L1JN-ten_drift_reconcile

✓ Template Properties — 2 Site Level Properties

Site level properties are specific to a particular site. Please select either MSO configuration or one of the sites configuration to apply.

Let's start by selecting a site

LA (ACI) ●

Great, now choose template level properties between LA, and NDO

○ LA (ACI) | ● NDO Current Settings

```
            "description": "",
            "ip": "10.10.10.10/24",
```

```
            "description": "epg1 on s1 subnet1 description",
            "ip": "21.21.21.21/24",
```

You can choose a site to compare that specific site's configuration. Unlike template-level configurations, you can choose either the Nexus Dashboard Orchestrator-defined or actual existing configurations for each site individually to be retained as the template's site-local properties for that site.

Even though in most scenarios you will make the same choice for both template-level and site-level configuration, the drift reconciliation wizard allows you to choose the configuration defined in the site's controller at the "Template Properties" level and the configuration defined in Nexus Dashboard Orchestrator at the "Site Local Properties" level or vice versa.

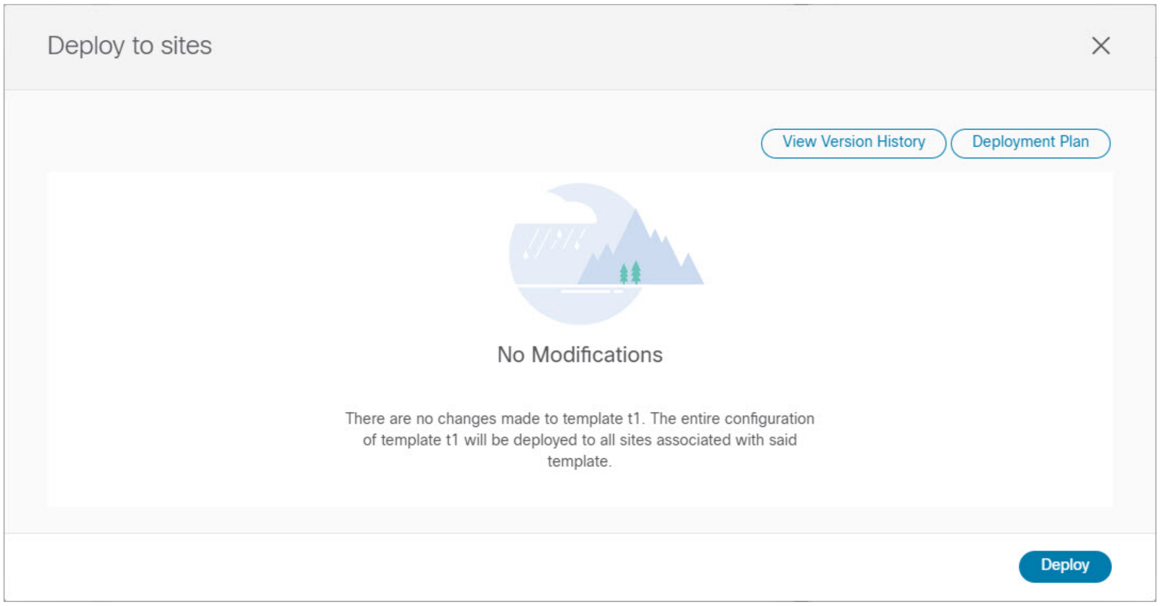
e) Click **Preview Changes** to verify your choices.

The preview will display full template configuration adjusted based on the choices picked in the **Drift Reconciliation** wizard. You can then click **Deploy to sites** to deploy the configuration and reconcile the drift for that template.

Step 8 After all configuration drifts are resolved and there are no changes shown in the **Deploy to sites** dialog for the template, perform full redeployment of the template.

Note Due to database transformations in Release 3.7(1), you must perform a full redeployment of each template.

Ensure that the **Deploy to sites** dialog contains no changes as shown in the following figure, then click **Deploy** to redeploy complete configuration:



Deploy to sites

No Modifications

There are no changes made to template t1. The entire configuration of template t1 will be deployed to all sites associated with said template.

Step 9 Repeat the above steps for every schema and template in your Nexus Dashboard Orchestrator.

Step 10 Check audit logs to verify that all templates have been re-deployed.

You can view the audit logs in the **Operations** tab.

Audit Logs page and confirm that all templates show as `Redeployed` to ensure that full re-deployment successfully completed.

Exporting (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 Remote Locations 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 7

Tech Support

- Tech Support and System Logs, on page 61
- Downloading System Logs, on page 62
- Streaming System Logs to External Analyzer, on page 62

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:

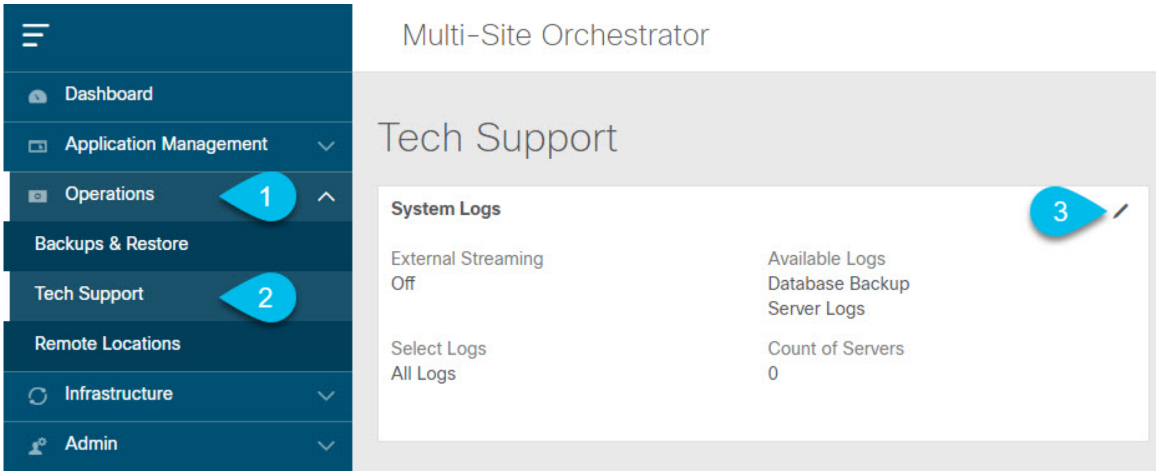
  ```
  msc_anpEpgRels.json
  msc_anpExtEpgRels.json
  msc_asyncExecutionStatus.json
  msc_audit.json
  msc_backup-versions.json
  msc_backupRecords.json
  msc_ca-cert.json
  msc_cloudSecStatus.json
  msc_consistency.json
  ...
  ```

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 Nexus Dashboard deployments.
- This release supports up to 5 external servers.

- If using Splunk, set up and configure the log analyzer service provider.

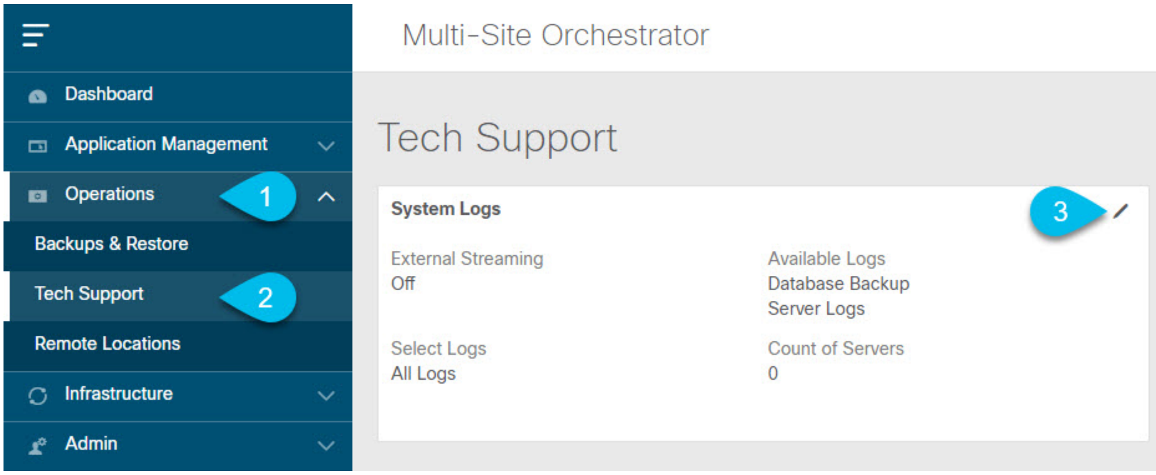
  For detailed instructions on how to configure an external log analyzer, consult its documentation.

- 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.

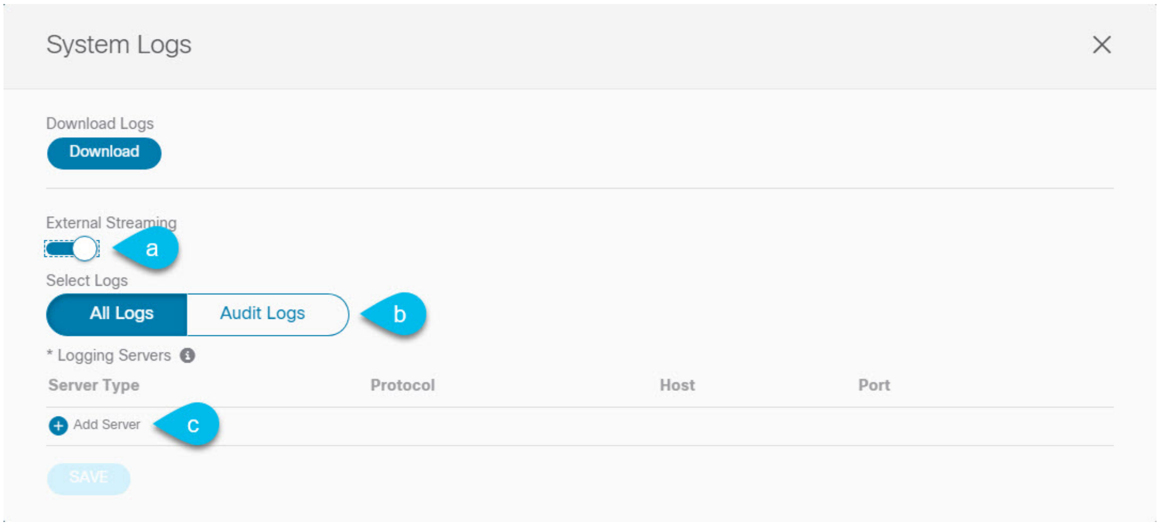


External Streaming: Off
Available Logs: Database Backup, Server Logs
Select Logs: All Logs
Count of Servers: 0

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.



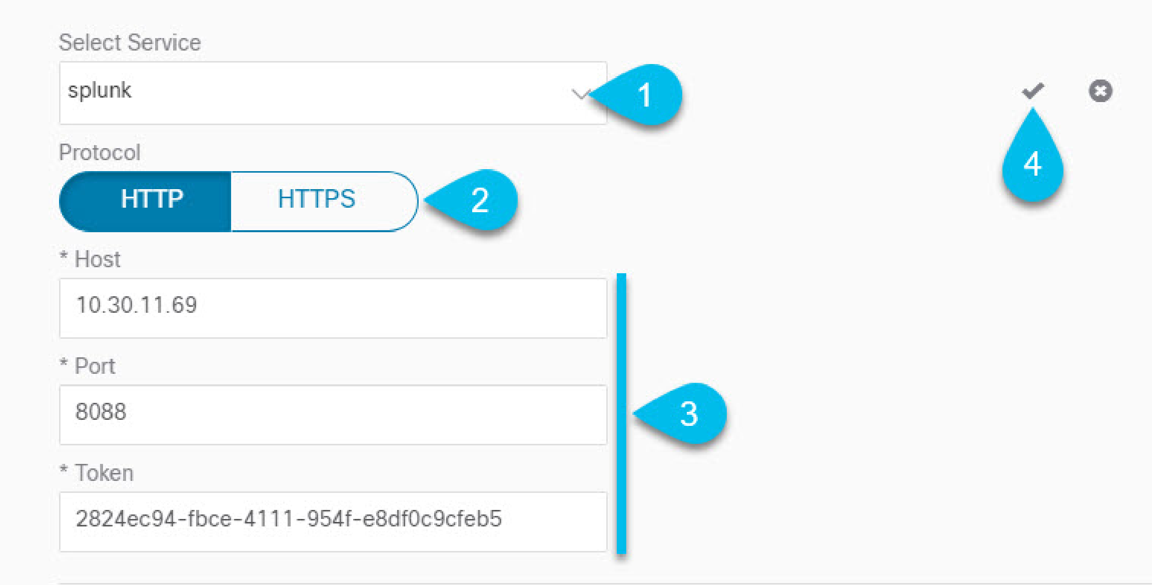
a) Enable the **External Streaming** knob.

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.



Select Service: splunk

Protocol: HTTP / HTTPS

* Host: 10.30.11.69

* Port: 8088

* Token: 2824ec94-fbce-4111-954f-e8df0c9cfeb5

a) Choose `splunk` for the server type.

b) Choose the protocol.

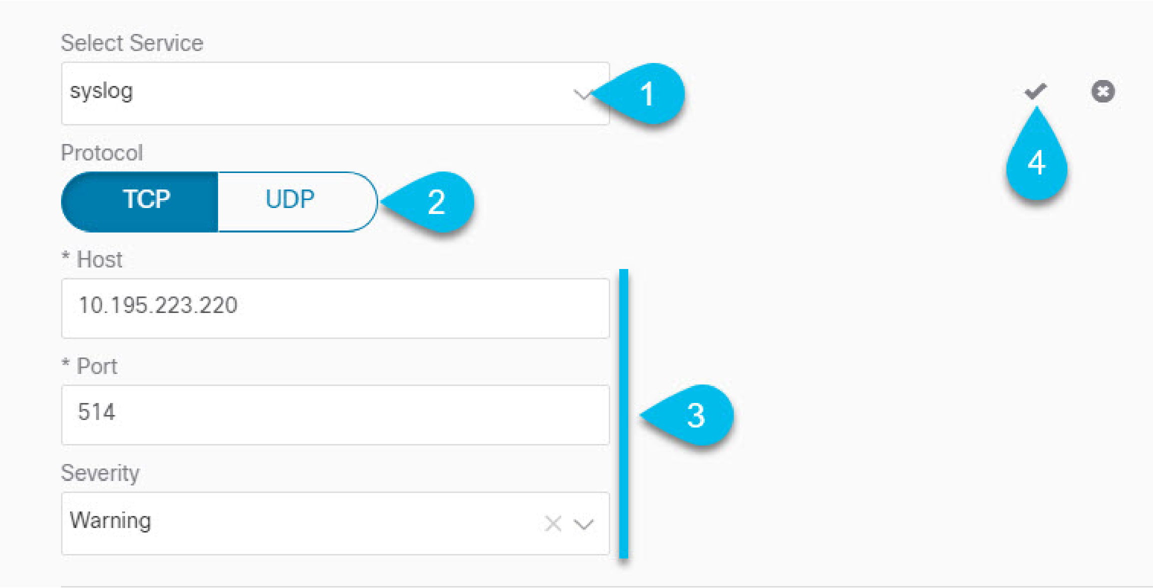
c) Provide the server name or IP address, port, and the authentication token you obtained from the Splunk service.

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.



Select Service: syslog

Protocol: TCP | UDP

* Host: 10.195.223.220

* Port: 514

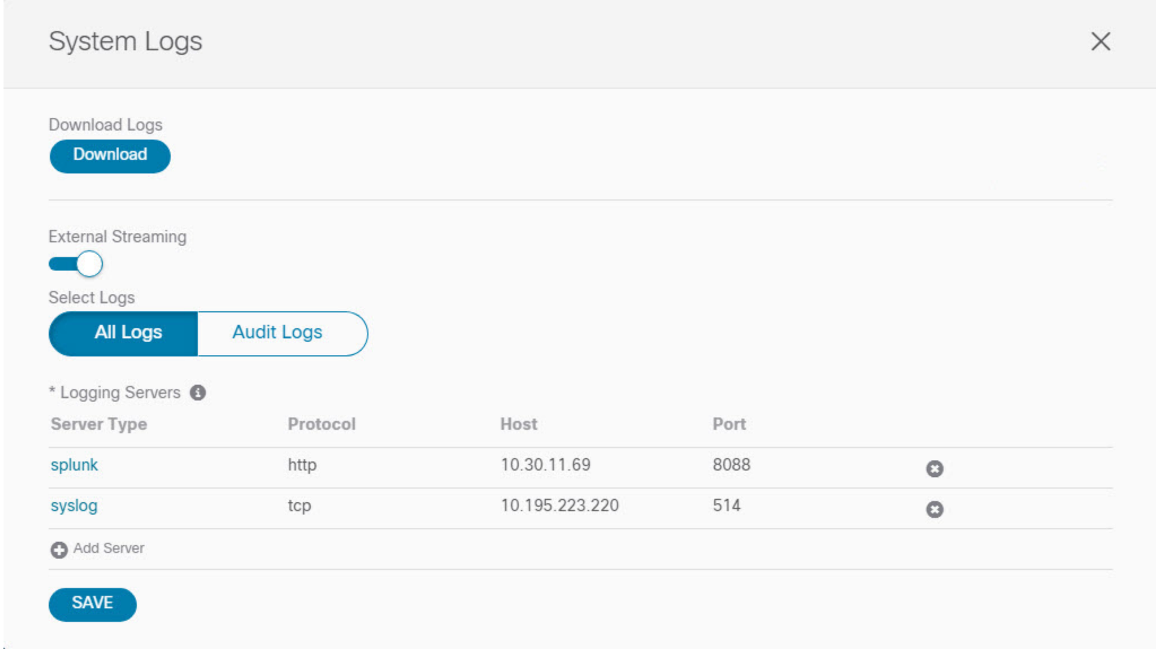
Severity: Warning

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.



System Logs

Download Logs

External Streaming

Select Logs: All Logs | Audit Logs

* Logging Servers

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

CHAPTER 8

System Configuration

- System Configuration Settings, on page 67
- System Alias and Banner, on page 67

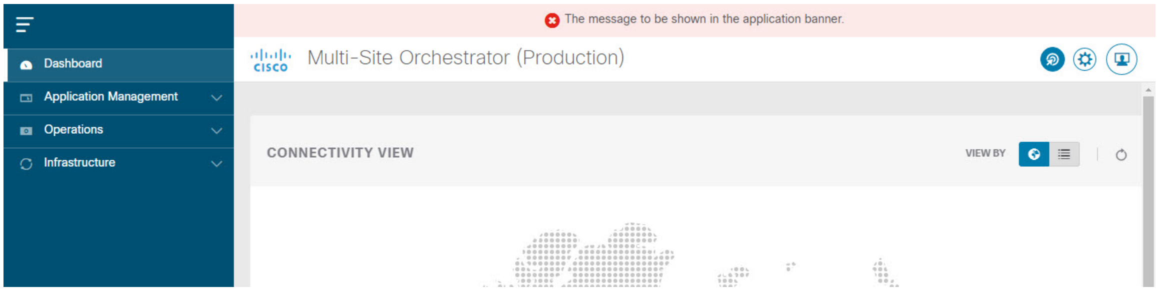
System Configuration Settings

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



The message to be shown in the application banner.

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.

PART II

Features and Use Cases

- Brownfield Import of VRFs and Networks, on page 71
- Integration with Cloud Network Controller, on page 79

CHAPTER 9

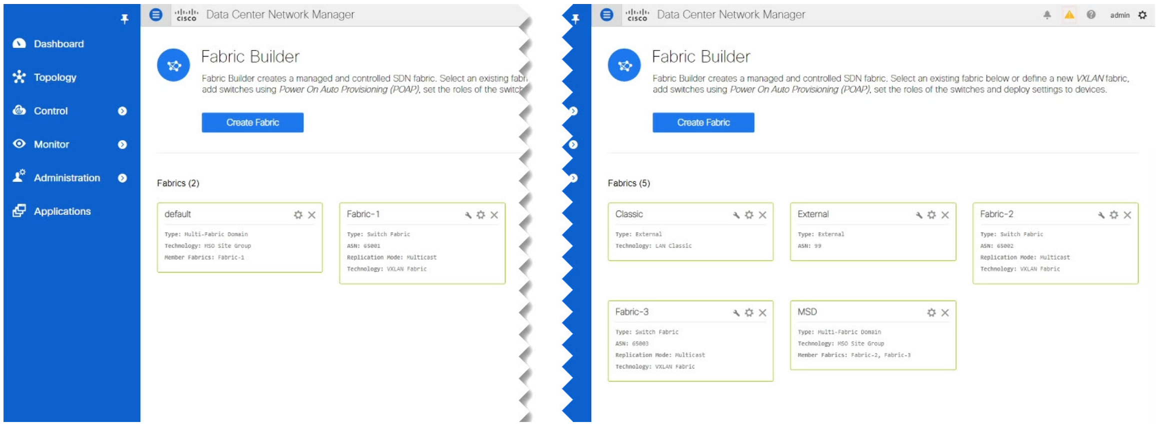
Brownfield Import of VRFs and Networks

- Overview, on page 71
- Prerequisites, on page 72
- Create Schema and Templates for Importing Configuration, on page 73
- Importing Schema Elements From NDFC Sites, on page 74
- Deploying Template and Making Changes, on page 76

Overview

The following sections describe the brownfield import use case scenario which will allow you to import existing NDFC 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 NDFC VRF and Network Configuration using Nexus Dashboard Orchestrator* video demo.

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



Fabric Builder

Fabric Builder creates a managed and controlled SDN fabric. Select an existing fabric below or define a new *VXLAN* fabric, add switches using *Power On Auto Provisioning (POAP)*, set the roles of the switches and deploy settings to devices.

Fabrics (2)

default
Type: Multi-Fabric Domain
Technology: MSO Site Group
Member Fabrics: Fabric-1

Fabric-1
Type: Switch Fabric
ASN: 65001
Replication Mode: Multicast
Technology: VXLAN Fabric

Fabrics (5)

Classic
Type: External
Technology: LAN Classic

External
Type: External
ASN: 99

Fabric-2
Type: Switch Fabric
ASN: 65002
Replication Mode: Multicast
Technology: VXLAN Fabric

Fabric-3
Type: Switch Fabric
ASN: 65003
Replication Mode: Multicast
Technology: VXLAN Fabric

MSD
Type: Multi-Fabric Domain
Technology: MSO Site Group
Member Fabrics: Fabric-2, Fabric-3

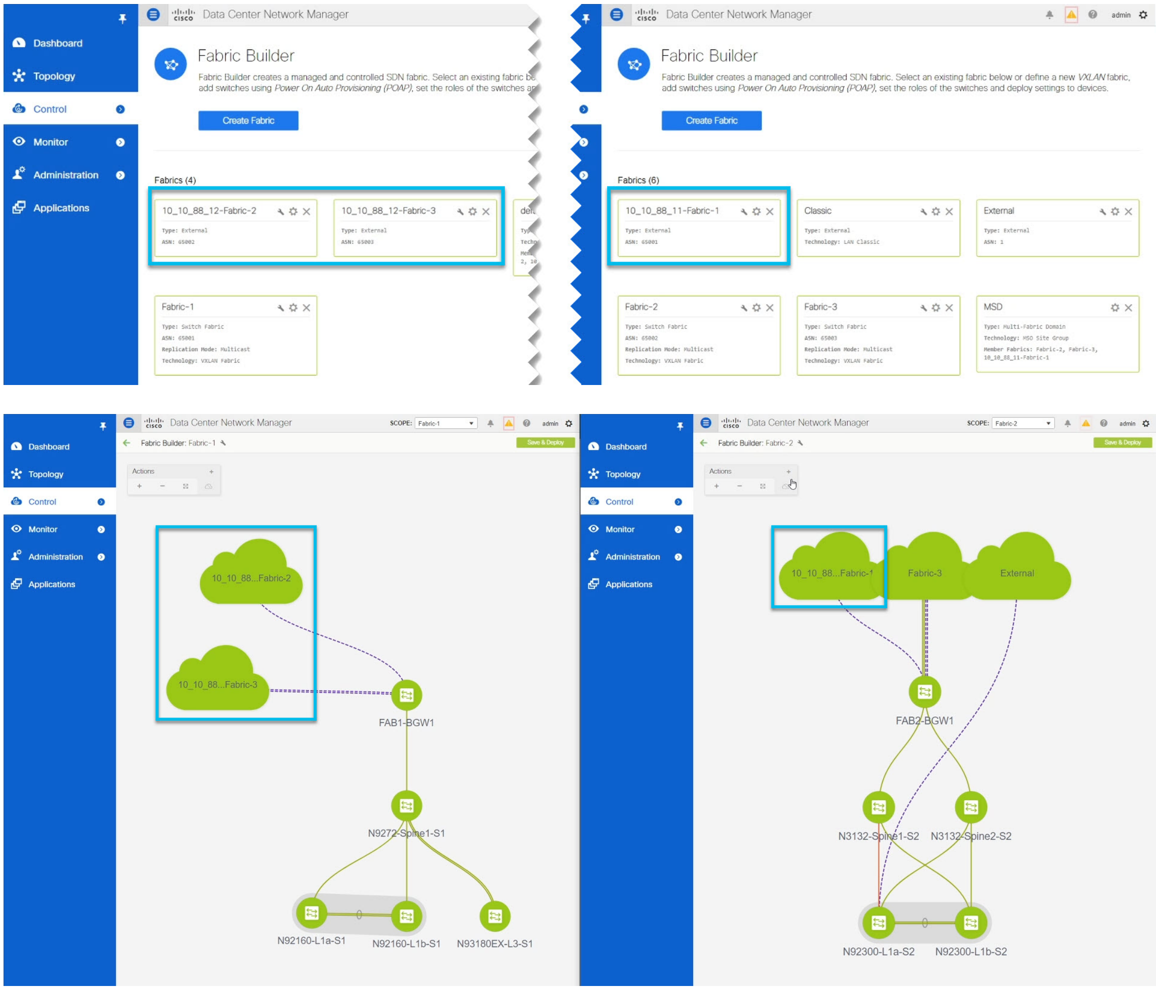
The following sections will detail how to import existing configuration, then stretch it from one fabric to another managed by different NDFCs, as well as how to deploy brand new VRFs and networks.

Prerequisites

Before you can import and manage VRFs and networks from the existing NDFC 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 NDFC 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 3.
- Have the inter-site infrastructure configured and deployed, as described in Configuring Infra for Cisco NDFC Sites, on page 7.

  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 NDFC:



Data Center Network Manager

Fabric Builder

Fabric Builder creates a managed and controlled SDN fabric. Select an existing fabric below or define a new *VXLAN* fabric, add switches using *Power On Auto Provisioning (POAP)*, set the roles of the switches and deploy settings to devices.

Create Fabric

Fabrics (4)

10_10_88_12-Fabric-2
Type: External
ASN: 65002

10_10_88_12-Fabric-3
Type: External
ASN: 65003

Fabric-1
Type: Switch Fabric
ASN: 65001
Replication Mode: Multicast
Technology: VXLAN Fabric

Fabrics (6)

10_10_88_11-Fabric-1
Type: External
ASN: 65001

Classic
Type: External
Technology: LAN Classic

External
Type: External
ASN: 1

Fabric-2
Type: Switch Fabric
ASN: 65002
Replication Mode: Multicast
Technology: VXLAN Fabric

Fabric-3
Type: Switch Fabric
ASN: 65003
Replication Mode: Multicast
Technology: VXLAN Fabric

MSD
Type: Multi-Fabric Domain
Technology: MSD Site Group
Member Fabrics: Fabric-2, Fabric-3, 10_10_88_11-Fabric-1

SCOPE: Fabric-1
Fabric Builder: Fabric-1

SCOPE: Fabric-2
Fabric Builder: Fabric-2

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**.

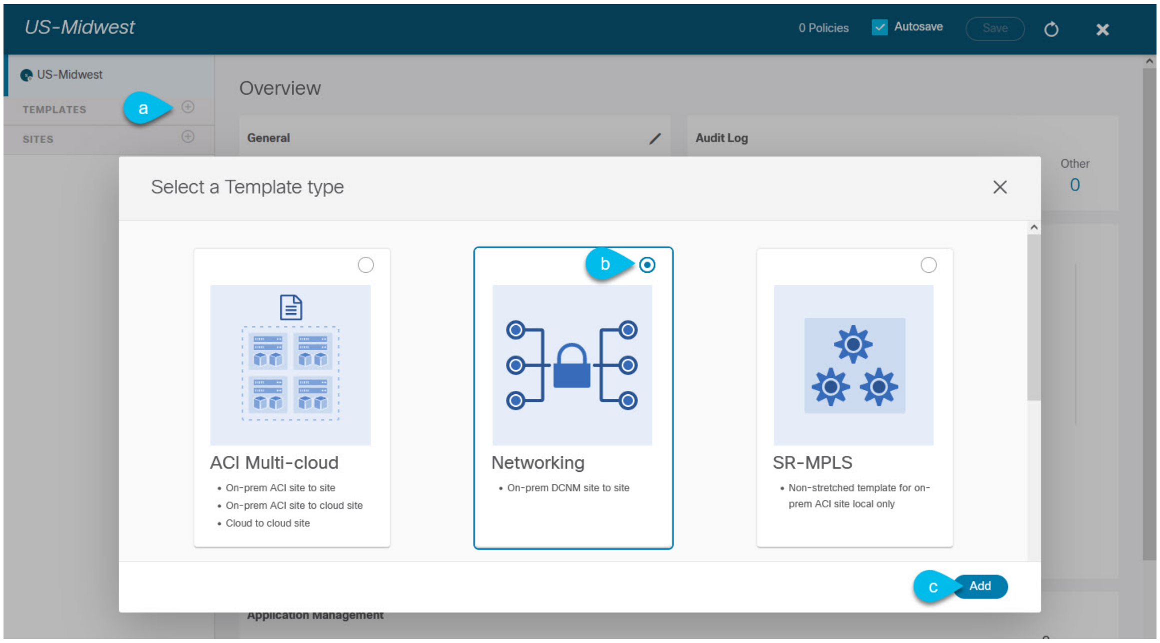
b) On the Schemas page, click **Add Schema**.

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.

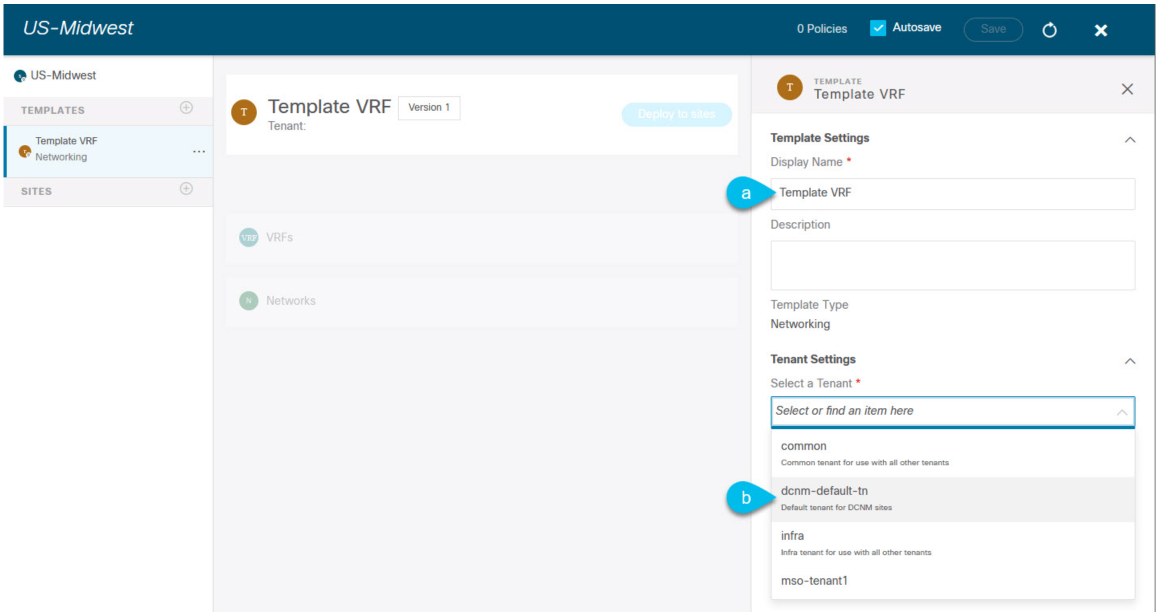


a) In the left sidebar under **Templates**, click the + sign to add a new template.

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.



Display Name * Template VRF

Template Type Networking

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 NDFC 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 NDFC Sites

This section describes how to import configuration from existing fabrics.

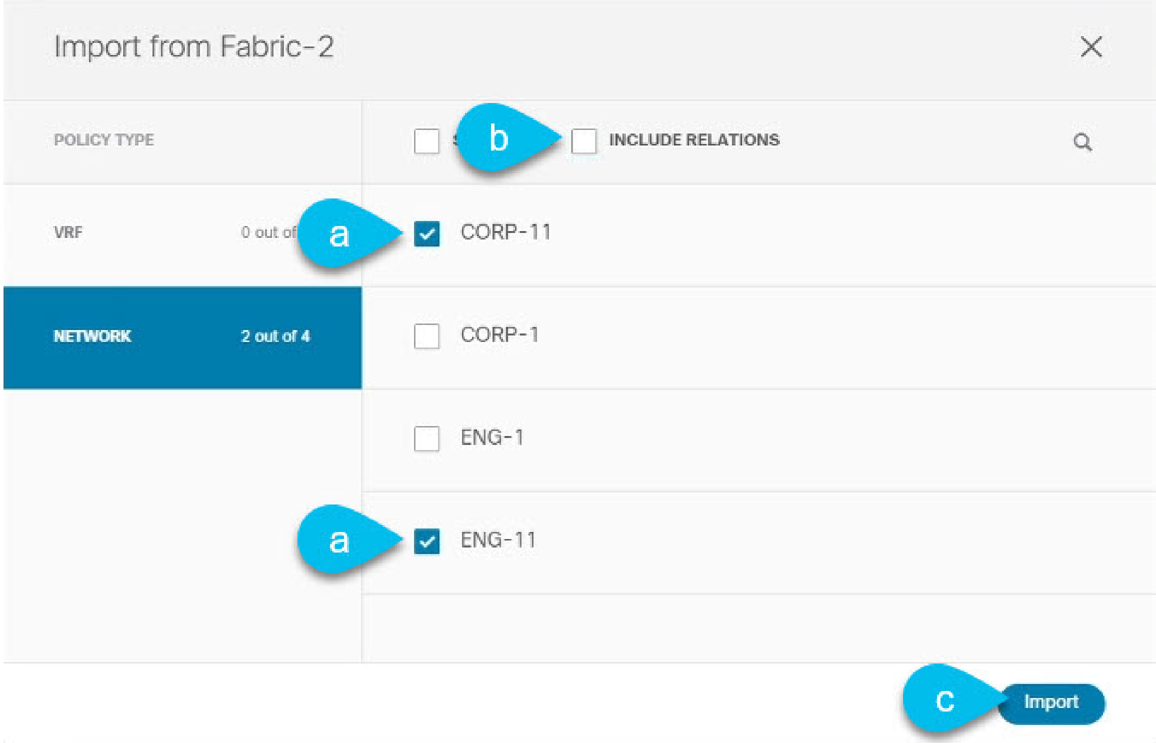
Before you begin

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

You will import the VRFs separately into the second template.

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

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

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

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

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

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

Deploying Template and Making Changes

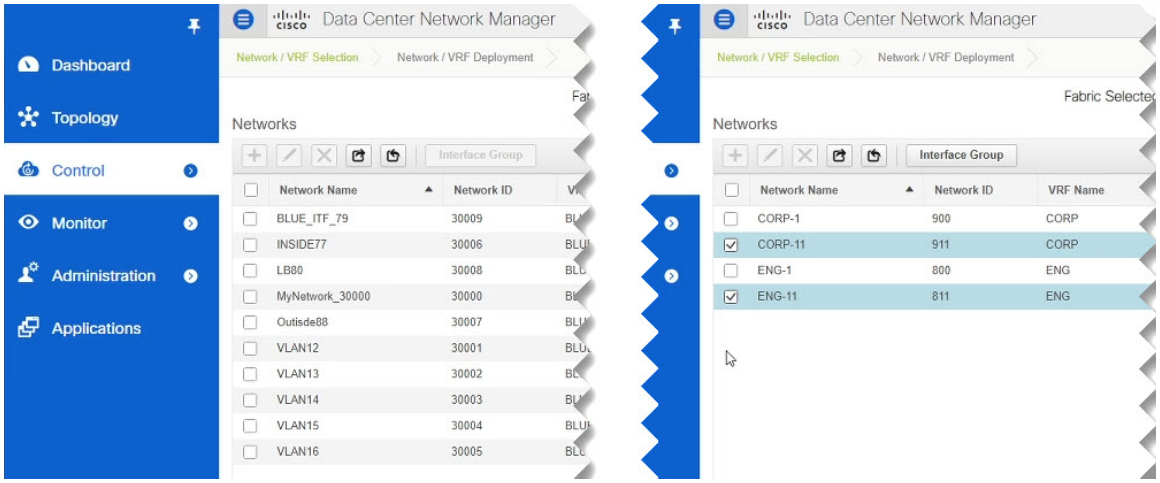
This section describes how to deploy the imported configuration to the site where it doesn't yet exist.

Before you begin

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

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

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



☐	Network Name ▲	Network ID	Vi
☐	BLUE_ITF_79	30009	BL
☐	INSIDE77	30006	BLU
☐	LB80	30008	BLL
☐	MyNetwork_30000	30000	BL
☐	Outisde88	30007	BLU
☐	VLAN12	30001	BLU
☐	VLAN13	30002	BL
☐	VLAN14	30003	BL
☐	VLAN15	30004	BLU
☐	VLAN16	30005	BLL

☐	Network Name ▲	Network ID	VRF Name
☐	CORP-1	900	CORP
☑	CORP-11	911	CORP
☐	ENG-1	800	ENG
☑	ENG-11	811	ENG

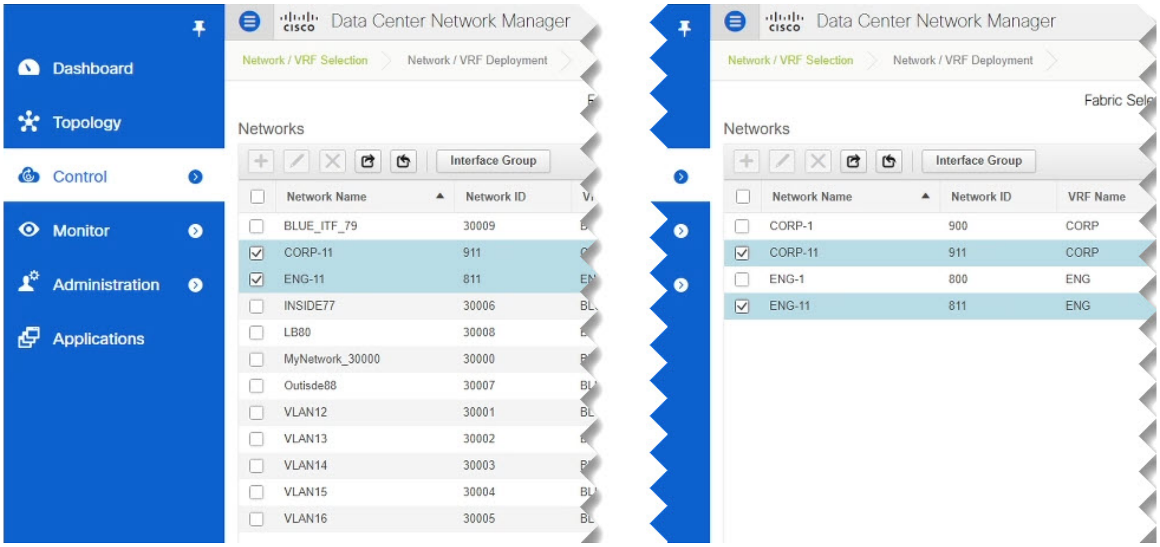
Step 2 In the top right of the template edit view, click **Deploy to sites**.

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 NDFC UI:



Networks

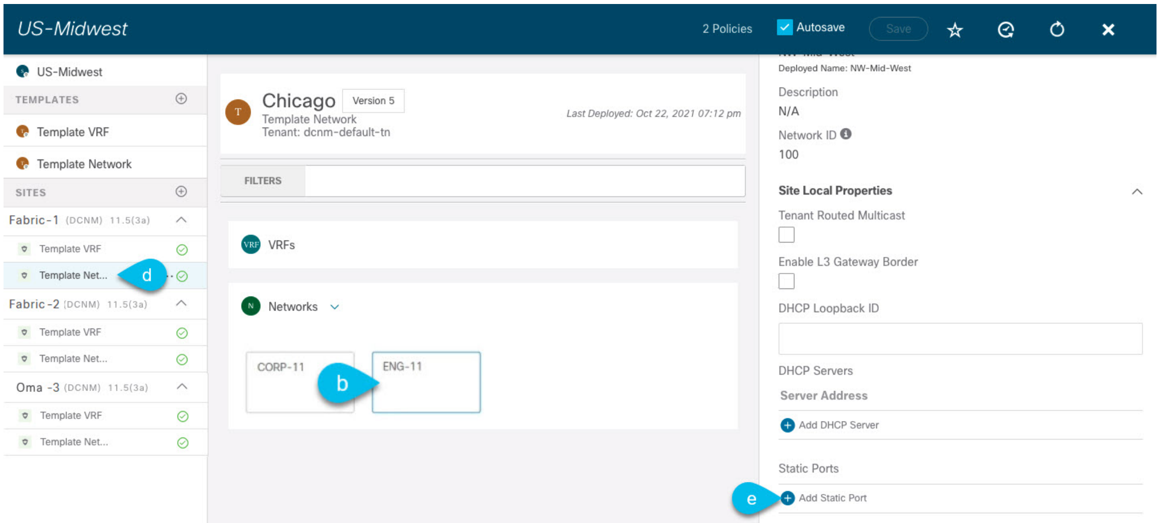
Network Name	Network ID
BLUE_ITF_79	30009
☑ CORP-11	911
☑ ENG-11	811
INSIDE77	30006
LB80	30008
MyNetwork_30000	30000
Outisde88	30007
VLAN12	30001
VLAN13	30002
VLAN14	30003
VLAN15	30004
VLAN16	30005

Networks

Network Name	Network ID	VRF Name
CORP-1	900	CORP
☑ CORP-11	911	CORP
ENG-1	800	ENG
☑ ENG-11	811	ENG

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`.



Deployed Name: NW-Mid-West

Description
N/A

Network ID
100

Site Local Properties

Tenant Routed Multicast □

Enable L3 Gateway Border □

DHCP Loopback ID

DHCP Servers

Server Address

Static Ports

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 NDFC GUI and refreshing the Networks page. The status of the network will go from `NA` to `In Progress` to `Deployed`.

CHAPTER 10

Integration with Cloud Network Controller

- Overview, on page 79

Overview

The Cisco Nexus Dashboard Orchestrator (NDO) based Hybrid Cloud solution offers seamless connectivity between on-premises and cloud networks. This solution uses NDFC to manage on-premises VXLAN-based fabric and on-premises Cisco Catalyst 8000Vs, while cloud sites (AWS or Microsoft Azure) are managed by the Cisco Cloud Network Controller (CNC). NDO is used to orchestrate connectivity between on-premises and cloud sites, and between two or more cloud sites. VXLAN is used to build overlay tunnels between the sites.

For detailed description of this use case, supported topologies, and configuration steps, see the *Hybrid Cloud Connectivity Deployment for Cisco NX-OS* document.