

Migrating Existing MSO Cluster to Nexus Dashboard

- Overview, on page 1
- Prerequisites and Guidelines, on page 2
- Back Up Existing Cluster Configuration, on page 4
- Prepare New Cluster, on page 5
- Restore Configuration in the New Cluster, on page 8
- Upgrade Cloud Sites, on page 12
- Update NDO Infra Configuration for Cloud Sites, on page 14
- Resolve Configuration Drifts, on page 16

Overview

This release of Nexus Dashboard Orchestrator (previously known as Multi-Site Orchestrator) must be deployed as a service in Cisco Nexus Dashboard. The previously supported VMware ESX virtual appliance and Cisco Application Services Engine form factors are now deprecated.

The following sections describe how to migrate an earlier release of Cisco Multi-Site Orchestrator to Nexus Dashboard Orchestrator on Nexus Dashboard platform.

If your NDO cluster is already deployed in Nexus Dashboard, follow the steps described in Upgrading NDO Service in Nexus Dashboard instead.

Migration Workflow

The following list provides a high level overview of the migration process and the order of tasks you will need to perform.

1. Back up existing Multi-Site Orchestrator configuration and disconnect the existing Multi-Site Orchestrator cluster.

   If you deploy a brand new Nexus Dashboard cluster rather than upgrade an existing cluster, we recommend preserving the existing Multi-Site Orchestrator cluster until the new Nexus Dashboard Orchestrator service is deployed and configuration is restored.

2. Deploy a Nexus Dashboard cluster using physical, virtual, or cloud form factor.

   During new cluster deployment, you will also complete the following:

a. (Optional) Configure the Nexus Dashboard cluster with additional nodes if required for service co-hosting.

b. (Optional) Configure remote authentication servers in the Nexus Dashboard if required by your existing Multi-Site Orchestrator deployment.

c. On-board the APIC, Cloud APIC, or DCNM sites that you currently manage from the Multi-Site Orchestrator to the Nexus Dashboard.

Note When on-boarding the fabrics in the new cluster, you must use the same exact name for each fabric as in the original cluster.

d. Install the Nexus Dashboard Orchestrator service in the Nexus Dashboard.

3. Restore the configuration backup in the new NDO service installed in the Nexus Dashboard.
4. Upgrade cloud sites to Cloud APIC release 5.2(x) one site at a time.

   You will upgrade a site's Cloud APIC, then that site's CSRs, then repeat the procedure for each additional site.
5. Update Infra configuration settings in Nexus Dashboard Orchestrator.
6. Resolve any configuration drifts and redeploy those templates.

   Resolving configuration drifts may require importing objects from the on-boarded fabrics or deploying the configuration from the Orchestrator.

Prerequisites and Guidelines

Because the new platform is vastly different in how it implements clustering and infrastructure, site management, and user management, the migration process involves parallel deployment of a new Nexus Dashboard platform and manual transfer of the current configuration database from your existing Multi-Site Orchestrator (MSO) cluster.

Before you migrate your existing cluster to Nexus Dashboard:

- When upgrading an existing Nexus Dashboard Orchestrator release 3.2(1) or later, we recommend upgrading to release 3.7(2).
- We recommend that you first familiarize yourself with the Nexus Dashboard platform and overall deployment overview and guidelines described in the *Cisco Nexus Dashboard Deployment Guide* and the Deploying Nexus Dashboard Orchestrator chapter of this document.

Note Ensure that you have followed the Nexus Dashboard deployment prerequisites and guidelines (such as CPU, RAM, and disk requirements) for the cluster where you deploy your Nexus Dashboard Orchestrator. Specifically, if you have a virtual cluster, the CPU and RAM system requirements must be available with physical reservation.

- Ensure that your current Multi-Site Orchestrator cluster is healthy.

  You will create a backup of your existing configuration and then import it into the newly deployed NDO service in Nexus Dashboard.

  Ensure that the cluster is healthy and existing IPsec intersite connectivity between cloud and on-premises sites is up.

- Ensure that your on-premises sites are running Cisco APIC release 4.2(4) or later.

  Site management has moved from the Multi-Site Orchestrator UI to the Nexus Dashboard common site management, which supports releases 4.2(4) or later. Fabric upgrades are described in detail in *Cisco APIC Installation, Upgrade, and Downgrade Guide*

- Ensure that your cloud sites are running Cisco Cloud APIC release 5.1(1).

  Site management has moved from the Multi-Site Orchestrator UI to the Nexus Dashboard common site management, which supports on-boarding cloud site releases 5.1(1) or later. Fabric upgrades are described in detail in *Cisco APIC Installation, Upgrade, and Downgrade Guide*



Note However, you must not upgrade to Cloud APIC 5.2(1) release or later before Nexus Dashboard Orchestrator is migrated to this release. If your cloud sites are running Cloud APIC 4.x or 5.0(x) releases, you must upgrade to a Cloud APIC 5.1(x) release before following the instructions in this chapter.

- Ensure that there are no configuration drifts between the Orchestrator's configuration and what is actually deployed in the fabrics before you upgrade.



Note Any templates that have configuration changes that are not yet deployed to the sites may cause the upgrade to fail.

  More information on resolving configuration drifts is available in the "Schemas" chapter of the *Nexus Dashboard Orchestrator Configuration Guide* for your current release.

- Back up your existing Orchestrator configurations.

  Configuration backups are described in the "Backup and Restore" chapter of the *Nexus Dashboard Orchestrator Configuration Guide* for your release.

- Back up your existing fabrics' configurations.

  We recommend creating configuration backups of all fabrics managed by your Nexus Dashboard Orchestrator:

  - For more information on creating Cisco APIC configuration backups, see the "Management" chapter of the *Cisco APIC Basic Configuration Guide* for your release.
  - For more information on creating Cisco Cloud Network Controller configuration backups, see the "Configuring Cisco Cloud Network Controller Components" chapter of the *Cisco Cloud Network Controller for AWS User Guide* for your release.

- For more information on creating Cisco Nexus Dashboard Fabric Controller configuration backups, see the "Backup and Restore" chapter of the *Cisco NDFC Fabric Controller Configuration Guide* for your release.

- Once you upgrade to this release, downgrading to an earlier release is not supported.

  If you want to revert to an earlier release, you will need to re-install the NDO service and restore a configuration backup from that release.

Back Up Existing Cluster Configuration

The migration process includes creating a backup of current configuration from your existing Multi-Site Orchestrator cluster and then restoring that in the new Nexus Dashboard Orchestrator service running in Nexus Dashboard.

This section describes how to back up your existing cluster configuration.

Note Ensure that there are no configuration drifts between the Orchestrator's configuration and what is actually deployed in the fabrics before you upgrade. This includes any templates that are in edit mode and contain changes that have not been deployed to the fabrics yet. More information on resolving configuration drifts is available in the "Schemas" chapter of the *Nexus Dashboard Orchestrator Configuration Guide* for your current release.

Before you begin

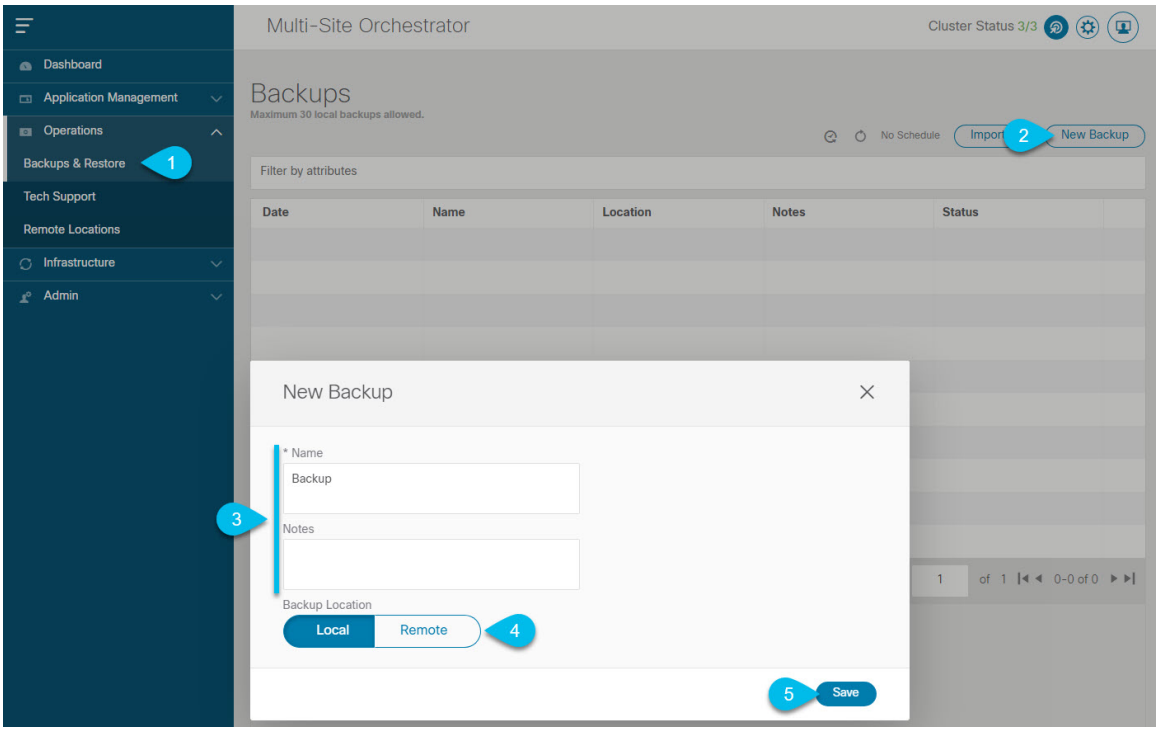
You must have the following completed:

- Familiarized yourself with the migration workflow order described in the Overview, on page 1
- Reviewed and completed general prerequisites described in Prerequisites and Guidelines, on page 2.

Procedure

Step 1 Log in to your existing Multi-Site 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) 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 (_).

d) Choose `Local` for the **Backup Location**.
e) Click **Save** to create the backup.

Step 3 Download the backup file from the existing Orchestrator.

If you created the backup using a remote location, you can skip this step.

In the main window, click the actions ( ) icon next to the backup and select **Download**. This will download the backup file to your system.

Prepare New Cluster

This section describes how to prepare a Nexus Dashboard cluster for installing the Nexus Dashboard Orchestrator service.

It includes choosing and deploying an appropriate form factor of Nexus Dashboard cluster and establishing network connectivity from the cluster to each site you plan to manage from the Nexus Dashboard Orchestrator.

Before you begin

You must have the following completed:

- Familiarized yourself with the migration workflow order described in the Overview, on page 1
- Reviewed and completed general prerequisites described in Prerequisites and Guidelines, on page 2.
- Existing configuration backed up as described in Back Up Existing Cluster Configuration, on page 4.

Procedure

Step 1 Deploy a Nexus Dashboard release 2.1.1e or later cluster and configure fabric connectivity.

How you deploy or upgrade to Nexus Dashboard depends on the deployment type of your existing cluster:

- If your existing Multi-Site Orchestrator is deployed directly in VMware ESX or in a **virtual** Cisco Application Services Engine cluster, you must deploy a brand new virtual or cloud Nexus Dashboard cluster as described in the *Cisco Nexus Dashboard Deployment Guide*.

  We also recommend completing the entire migration process before deleting the existing cluster.

- If you have an existing **physical** Cisco Application Services Engine cluster with Multi-Site Orchestrator service release 3.1(x), you must uninstall the existing service, then upgrade the cluster to Nexus Dashboard release 2.1.1e or later as described in the "Upgrading" chapter of the *Cisco Nexus Dashboard Deployment Guide*.
- If you have an existing **physical** Nexus Dashboard cluster with Nexus Dashboard Orchestrator service release 3.2(x), you can upgrade the cluster as described in the "Upgrading" chapter of the *Cisco Nexus Dashboard Deployment Guide* and then upgrade the Nexus Dashboard Orchestrator service as described in Upgrading Nexus Dashboard Orchestrator and skip the rest of this chapter.

  Note
  If you plan to add any Cloud APIC sites after the upgrade, ensure that they are running Cloud APIC release 5.2(1) or later.

Step 2 Ensure that your Nexus Dashboard cluster is appropriately scaled based on the fabric sizes and number of applications.

If you deployed a virtual or cloud form factor of the Nexus Dashboard, Nexus Dashboard Orchestrator is the only application supported and the base 3-node cluster is sufficient, so you can skip this step.

If you deployed a physical Nexus Dashboard cluster and Nexus Dashboard Orchestrator is the only application you plan to host, the base 3-node cluster is sufficient and you can skip this step.

However, if you deployed a physical Nexus Dashboard cluster and plan to co-host multiple applications, use the Cisco Nexus Dashboard Capacity Planning tool to determine the required cluster size for your specific use case. If you need to extend your cluster to support all required services, see the *Cisco Nexus Dashboard User Guide* for information on deploying additional worker nodes.

Step 3 Install the NDO service in your Nexus Dashboard.

This process is described in detail in the Deploying Nexus Dashboard Orchestrator chapter.

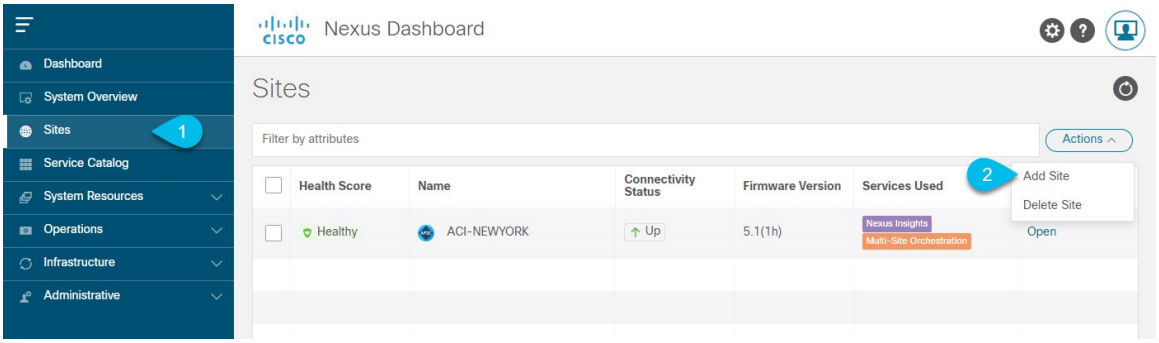
Step 4 On-board all sites to the Nexus Dashboard.

Site management has moved from the Multi-Site Orchestrator UI to the Nexus Dashboard common site management. As such, you must on-board the same sites using the same names that were assigned to the sites when on-boarded on the

original Multi-Site Orchestrator cluster to the Nexus Dashboard GUI before migrating your existing configuration to the new cluster, as described in Adding and Deleting Sites. If any site that exists in you current deployment is not present in Nexus Dashboard (or it exists with a different name), the configuration restore during migration will fail with a `Pre-restore check failed` error message.

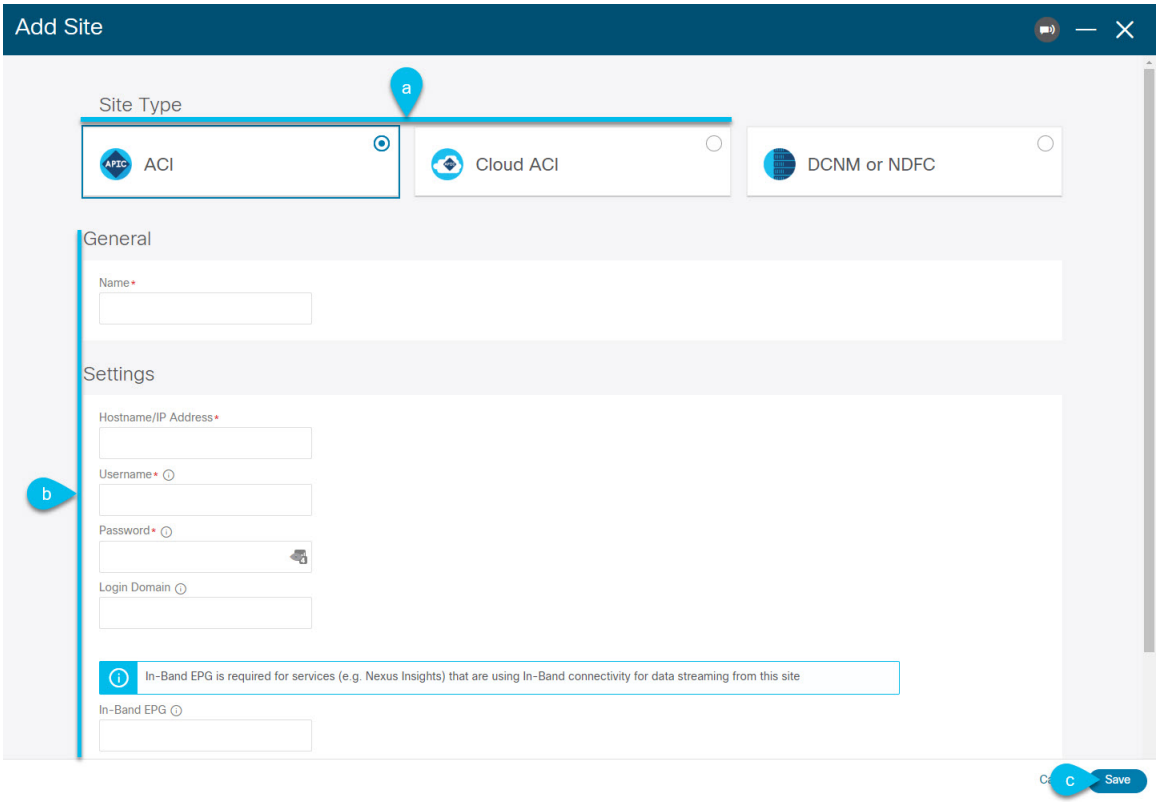
Note
After you add the sites to the Nexus Dashboard, you must not set them to `Managed` in the NDO service. The sites will be enabled for management automatically when you restore your configuration from backup.

Add a site:



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

If adding an ACI site, provide the following information:



a) For **Site Type**, select **ACI** or **Cloud ACI** depending on the type of ACI fabric you are adding.

b) Provide the controller information.

You need to provide the **Host Name/IP Address**, **User Name**, and **Password.** for the APIC controller currently managing your ACI fabrics. If NDO is the only application you plan to host, you can specify either the in-band or out-of-band address of the on-premises APIC; however, if you plan to host other applications, such as Nexus Insights, you must specify the in-band address.

Note
By default, the in-band or out-of-band address of the on-premises APIC that you use to on-board the fabric must be reachable from the Nexus Dashboard's data interface.

If you want to use the Nexus Dashboard's management interface for NDO traffic, you must configure a static route from the Nexus Dashboard cluster to the fabric's IP from the management interface. For more information, see the **Infrastructure Management** > **Cluster Configuration** chapter of the *Nexus Dashboard User Guide*.

For on-premises ACI sites managed by Cisco APIC, if you plan to use this site with Day-2 Operations applications such as Nexus Insights, you must also provide the **In-Band EPG** name used to connect the Nexus Dashboard to the fabric you are adding. Otherwise, if you will use this site with Nexus Dashboard Orchestrator only, you can leave this field blank.

c) Click **Add** to finish adding the site.

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

d) Repeat this step to add all the sites from your existing Multi-Site deployment.

Step 5 Add any remote authentication servers you had configured in your Multi-Site Orchestrator to the Nexus Dashboard.

User management has moved from the Multi-Site Orchestrator UI to the Nexus Dashboard common user management. As such, you must add the same remote users and authentication servers to the Nexus Dashboard, as described in the *Cisco Nexus Dashboard User Guide*.

Any local users you had previously configured directly in Multi-Site Orchestrator will be added into the Nexus Dashboard automatically when you import the existing configuration backup.

Step 6 Add any proxy configuration you had configured in your Multi-Site Orchestrator to the Nexus Dashboard.

Proxy configuration has moved from the Multi-Site Orchestrator UI to the Nexus Dashboard common cluster configuration. As such, you must add the proxy server to the Nexus Dashboard, as described in the *Cisco Nexus Dashboard User Guide*.

Any existing proxy configuration will not be migrated automatically and you must manually re-add it in Nexus Dashboard after the migration.

Restore Configuration in the New Cluster

This section describes how deploy and configure the new Nexus Dashboard cluster and the NDO service, which you will use to restore your previous configuration.

Before you begin

You must have the following completed:

- Existing configuration backed up as described in Back Up Existing Cluster Configuration, on page 4.

- Deployed Nexus Dashboard cluster and installed Nexus Dashboard Orchestrator service as described in Prepare New Cluster, on page 5.

Procedure

Step 1 Disconnect the existing Multi-Site Orchestrator cluster.

You must disconnect the existing Multi-Site Orchestrator cluster so it does not communicate with the sites during migration.

Note
We recommend preserving the existing Multi-Site Orchestrator cluster until the new cluster is deployed and configuration is restored.

Step 2 Ensure that the new Nexus dashboard cluster is up and running and the NDO service is installed.

The NDO service must be a fresh install with no configuration changes to the sites or policies.

Step 3 Log in to your Nexus Dashboard GUI.

Step 4 Ensure that all the sites are on-boarded to Nexus Dashboard.

When you restore the backup, NDO will validate that every site in the backup is present in the Nexus Dashboard with matching site name and type. If validation is unsuccessful, for example if a site is not on-boarded in Nexus Dashboard, configuration restore will fail and you will need to on-board the site before retrying, as described in the previous section.

Step 5 Open your new Nexus Dashboard Orchestrator service.

Step 6 Add remote location for configuration backups.

This release of Nexus Dashboard Orchestrator does not support configuration backups stored on the cluster's local disk. So before you can import the backup you saved before the migration, you need to configure a remote location in Nexus Dashboard Orchestrator to which you can then import your configuration backups.

a) From the left navigation pane, select **Operations** > **Remote Locations**.

b) In the top right of the main window, click **Add Remote Location**.

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

c) 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

d) 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.

e) 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/ndo`.

Note
The directory must already exist on the remote server.

f) Specify the port used to connect to the remote server.

By default, port is set to `22`.

g) 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.

h) Click **Save** to add the remote server.

Step 7 Import the backup file to your new Nexus Dashboard Orchestrator cluster.

a) From the left navigation pane, select **Operations** > **Backups & Restore**.
b) In the main pane, click **Upload**.
c) In the **Upload from file** window that opens, click **Select File** and choose the backup file you want to import.

This is the backup of your existing MSO configuration that you created and downloaded in previous section.

d) From the **Remote Location** dropdown menu, select the remote location.
e) (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.

f) 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, the files are stored only on the remote server and not directly on the cluster nodes.

Step 8 Restore the configuration.

a) In the main window, click the actions (**…**) icon next to the backup you created prior to the upgrade and select **Rollback to this backup**.

This opens the **Restore from this backup** warning dialog.

b) In the **Restore from this backup** dialog window, click **Restore** to confirm that you want to restore the backup you selected.

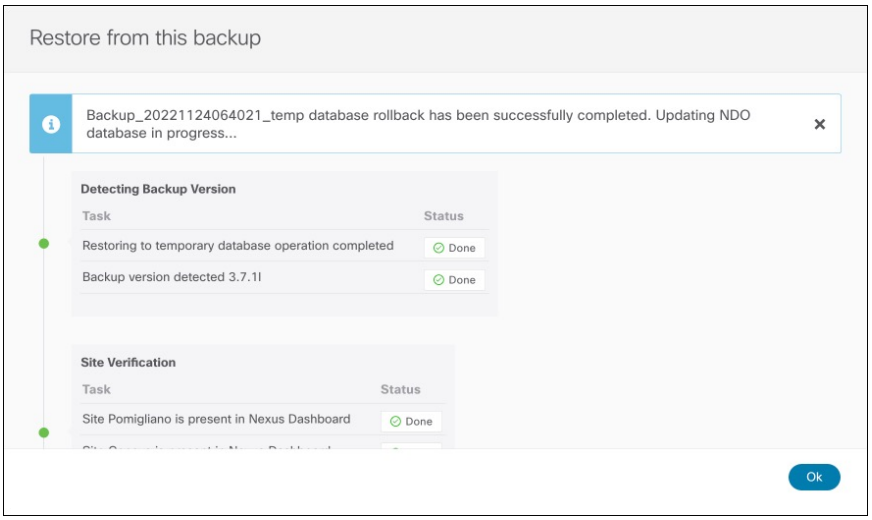
When the configuration is restored, any sites previously managed by Multi-Site Orchestrator and on-boarded to the Nexus Dashboard will be enabled for NDO management in the GUI. If the configuration backup contains sites that are not on-boarded to your Nexus Dashboard, backup restore will fail with a `Pre-restore check failed` error and you will need to repeat the procedure after on-boarding any missing sites.

Depending on the size of your configuration, the database rollback may take several minutes to complete.

c) After the database is restored, click **Ok** to proceed.

Release 3.7(2) added database optimization to the configuration rollback workflow, which is automatically triggered as the final stage of restoring configuration.

Simply click **Ok** to view the database update progress:

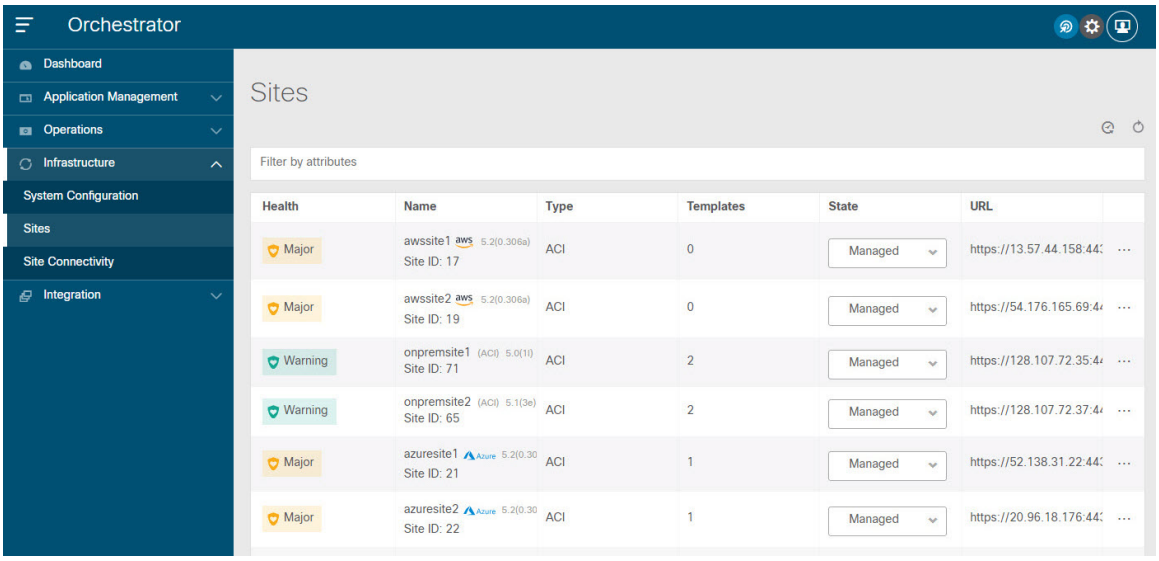


Step 9 Update the password.

Due to CSDL (Cisco Secure Development Lifecycle) requirements, you may be required to update the `admin` user password after configuration restore is completed.

Step 10 Verify that backup was restored successfully and all objects and configurations are present.

a) In the **Sites** page, verify that all sites are listed as `Managed`.



b) In the **Tenants** and **Schemas** pages, confirm that all tenants and schemas from your previous Multi-Site Orchestrator cluster are present.

c) Navigate to **Infrastructure** > **Site Connectivity** and confirm that intersite connectivity is intact.

In the main pane, click **Show Connectivity Status** next to each site and verify that the underlay and overlay connectivity is still successfully established.

d) In the main pane, click **Configure** to open **Fabric Connectivity Infra** screen and verify **External Subnet Pool** addresses.

You can view the external subnet pools by selecting **General Settings** > **IPsec Tunnel Subnet Pools** tab of the **Fabric Connectivity Infra** screen and verify that the External Subnet Pools previously configured in Cloud APIC have been imported from the cloud sites.

These subnets are used to address the IPsec tunnel interfaces and loopbacks of the Cloud Routers used for on-premises connectivity and had to be configured directly in the Cloud APIC in earlier Nexus Dashboard Orchestrator releases.

Note
You must not make any changes or deploy any configurations at this stage until the cloud sites are upgraded to Cloud APIC release 5.2(1) as described in following sections.

Upgrade Cloud Sites

After Nexus Dashboard Orchestrator is migrated to this release, you must upgrade any Cloud APIC sites managed by the NDO to release 5.2(1) or later. While existing intersite connectivity will remain intact, you will not be able to change or deploy any cloud site Infra configurations to sites running Cloud APIC releases prior to release 5.2(1).

Before you begin

You must have the following completed:

- Deployed Nexus Dashboard cluster and installed Nexus Dashboard Orchestrator service as described in Prepare New Cluster, on page 5.
- Existing configuration backup restored to the new cluster as described in Restore Configuration in the New Cluster, on page 8.

Procedure

Step 1 Upgrade cloud sites.

For each cloud site, you must upgrade its Cloud APIC and then its CSRs before proceed to upgrading the next site. After a site is upgraded and healthy, you can repeat the same steps to upgrade any additional sites.

a) Upgrade a site's Cloud APIC.

You can upgrade Cloud APIC as you typically would.

Note that after the Cloud APIC upgrade, any existing public IP tunnels will remain intact and intersite connectivity via public IPsec will not be interrupted .

b) Upgrade that site's CSR.

Starting with Cloud APIC release 5.2(1) , CSRs upgrade does not happen automatically as it used to in earlier releases, so you must manually trigger CSR upgrade after Cloud APIC is upgraded. You must upgrade the site's CSRs before moving on to upgrading the next site.

As you upgrade CSRs in each site, the following will occur:

- As each CSR is upgraded, its existing `/30` tunnels will be recreated and the traffic will continue to flow.
- Tunnel-management and all Infra configuration changes from Nexus Dashboard Orchestrator are disabled for as long as any of the cloud sites are still running any Cloud APIC or CSR releases prior to 5.2(1).
- If the last site you upgrade is an AWS cloud site, the following will occur for that site's CSRs only:
  - The last cloud site's tunnel endpoints will be deleted by Cloud APIC and NDO will delete the corresponding tunnels that use the endpoint
  - NDO will delete the tunnels originating from CSRs in the last cloud site
  - New `hcloudInterCloudSiteTunnel` MO will be created and Nexus Dashboard Orchestrator's tunnel management will allocate `/31` addresses for the new tunnels
  - The CSRs in this site and the CSRs in another cloud site peering with it will establish `/31` tunnels.

  If the last upgraded site is an Azure site, the same `/30` tunnel will be created on the CSRs and the above four bullet points are not relevant.

For any CSRs you add or any underlay configuration changes to existing CSRs after the migration process is completed, all new tunnels created by NDO will be `/31` tunnel.

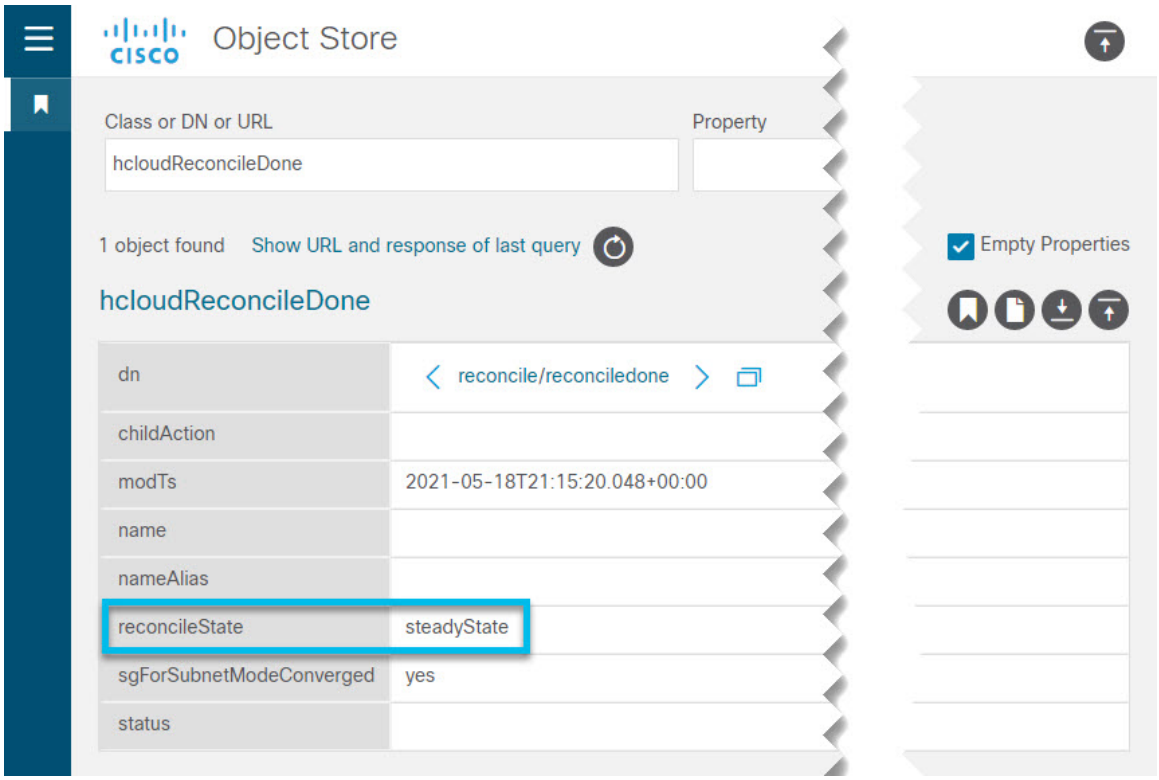
Note
If you do not see BGP sessions within 5 minutes of CSRs upgrade finishing and CSRs coming up, refresh the site's infra connectivity in the Nexus Dashboard Orchestrator **Infra Configuration** screen.

c) Repeat this step for each cloud site one at a time.

Step 2 Verify Cloud APIC and CSR upgrades have completed.

a) In each site's Cloud APIC, check that the `hcloudReconcileDone` MO shows `reconcileState=steadyState`.

You can check the MO by navigating to `https://<cloud-apic-ip>/visore.html` and searching for `hcloudReconcileDone` in the **Class or DN or URL** field.



b) In Nexus Dashboard Orchestrator, navigate to **Infrastructure** > **Site Connectivity** and confirm that intersite connectivity is intact.

In the main pane, click **Show Connectivity Status** next to each site and verify that connectivity is healthy in the `Overlay Status` and `Underlay Status` tabs.

c) In Nexus Dashboard Orchestrator's **Site Connectivity** page, click **Configure** and confirm that the External Subnet Pools previously configured in Cloud APIC have been imported and are present.

You can view the external subnet pools by selecting **General Settings** > **IPSec Tunnel Subnet Pools** tab of the **Fabric Connectivity Infra** screen.

d) In Nexus Dashboard Orchestrator's **Fabric Connectivity Infra** screen, select a cloud site, click the **Inter-Site Connectivity** tab in the right-hand sidebar, and confirm that underlay connectivity using public IPs is preserved for existing sites.

Update NDO Infra Configuration for Cloud Sites

In order to make subsequent changes to Infra configuration, you must first provide the following information immediately after the cloud sites are upgraded to Cloud APIC release 5.2(1):

- OSPF area ID
- IPN configuration

Note If you have no cloud sites, you can skip this section.

Before you begin

You must have the following completed:

- Deployed Nexus Dashboard cluster and installed Nexus Dashboard Orchestrator service as described in Prepare New Cluster, on page 5.
- Existing configuration backup restored to the new cluster as described in Restore Configuration in the New Cluster, on page 8.
- Upgraded cloud sites as described in Upgrade Cloud Sites, on page 12.

Procedure

Step 1 Log in to your new Nexus Dashboard Orchestrator.

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 the **OSPF Area ID** field.

This is OSPF area ID used by cloud sites for on-premises ISN peering, which you previously configured in the Cloud APIC for inter-site connectivity in earlier Nexus Dashboard Orchestrator releases.

Step 6 Add **IPN Devices** information.

a) Select the **IPN Devices** tab.
b) Click **Add IPN Device**.
c) Provide the **Name** and the **IP Address** of the on-premises IPN devices.

You must provide the IP addresses of the devices in your on-premises sites that are used as the tunnel peer address from the Cloud APIC's CSRs, not the IPN device's management IP address.

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 Update **Underlay Configuration** for inter-site connectivity between on-premises and cloud sites.

For each on-premises site that connects to cloud sites, you need to provide at least one IPN device IP address from the ones you added in the previous step, to which the Cloud APIC's CSRs establish a tunnel.

a) In the left pane, under **Sites**, select the on-premises site.
b) In the right **<*Site*> Settings** pane, select the **Underlay Configuration** tab.
c) Click **+Add IPN Device** to specify an IPN device.
d) From the dropdown, select one of the IPN devices you defined previously.

The IPN devices must be already defined in the **General Settings** > **IPN Devices** list, as described in the previous step.

Step 8 From the dropdown at the top of the screen, select **Deploy** to re-deploy the Infra configuration.

Resolve Configuration Drifts

In some cases you may run into a situation where the configuration actually deployed in the site's controller is different from the configuration defined 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.

After restoring an MSO backup configuration in NDO, some templates may show configuration drifts, which can occur for one of the following reasons:

- Nexus Dashboard Orchestrator added support for managing more objects' properties compared to the previous Multi-Site Orchestrator versions. As a result, the MSO configuration backup would not contain any information about or values for the new properties and NDO will assign default values to them. If you had modified those properties directly in APIC managed by MSO, the NDO templates containing those objects would show a drift.

Note Deploying any templates before resolving these drifts would push the configuration defined on the NDO templates and overwrite the non-default values defined in the fabrics' controllers.

- When migrating to NDO release 3.7(2) or later, enhancements have been introduced in the configuration rollback procedure to ensure that the content of the NDO database can be fully rebuilt based on the configuration information present in the backup file. This means that if some of the MSO templates were not fully deployed when the backup file was originally created (for example, left in the “edit” state), the NDO configuration for those templates would be based on that state and may differ from the configuration actually deployed on the fabrics' controllers resulting in a configuration drift.

Before you begin

You must have the following completed:

- Deployed Nexus Dashboard cluster and installed Nexus Dashboard Orchestrator service as described in Prepare New Cluster, on page 5.
- Existing configuration backup restored to the new cluster as described in Restore Configuration in the New Cluster, on page 8.
- Upgraded cloud sites as described in Upgrade Cloud Sites, on page 12.
- Updated Nexus Dashboard Orchestrator Infra configuration for the cloud sites as described in Update NDO Infra Configuration for Cloud Sites, on page 14.

Procedure

Step 1 Check for configuration drifts using the API.

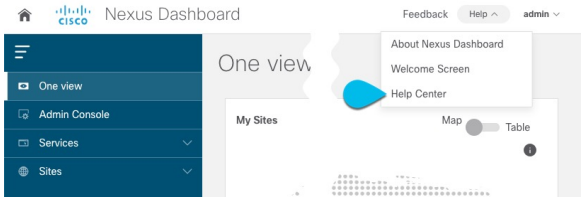
Beginning with release 3.7(2), you can generate a list of all templates that contain configuration drifts by using the `/api/v1/schemas/template-modified-policy-states` API call directly from your Nexus Dashboard Orchestrator's GUI as described in this step.

Alternatively, you can manually check every schema and template individually as described in the next step.

a) Ensure that you are logged in to you Orchestrator UI.

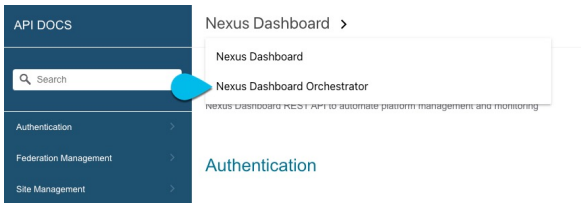
The API uses the authentication token from the Orchestrator UI login.

b) From the **Help** menu in the top right corner of the window, choose **Help Center**.



c) In the **Help Center**'s **Programming** tile, click **REST API**.

d) From the dropdown at the top of the page, select **Nexus Dashboard Orchestrator** to show NDO APIs.

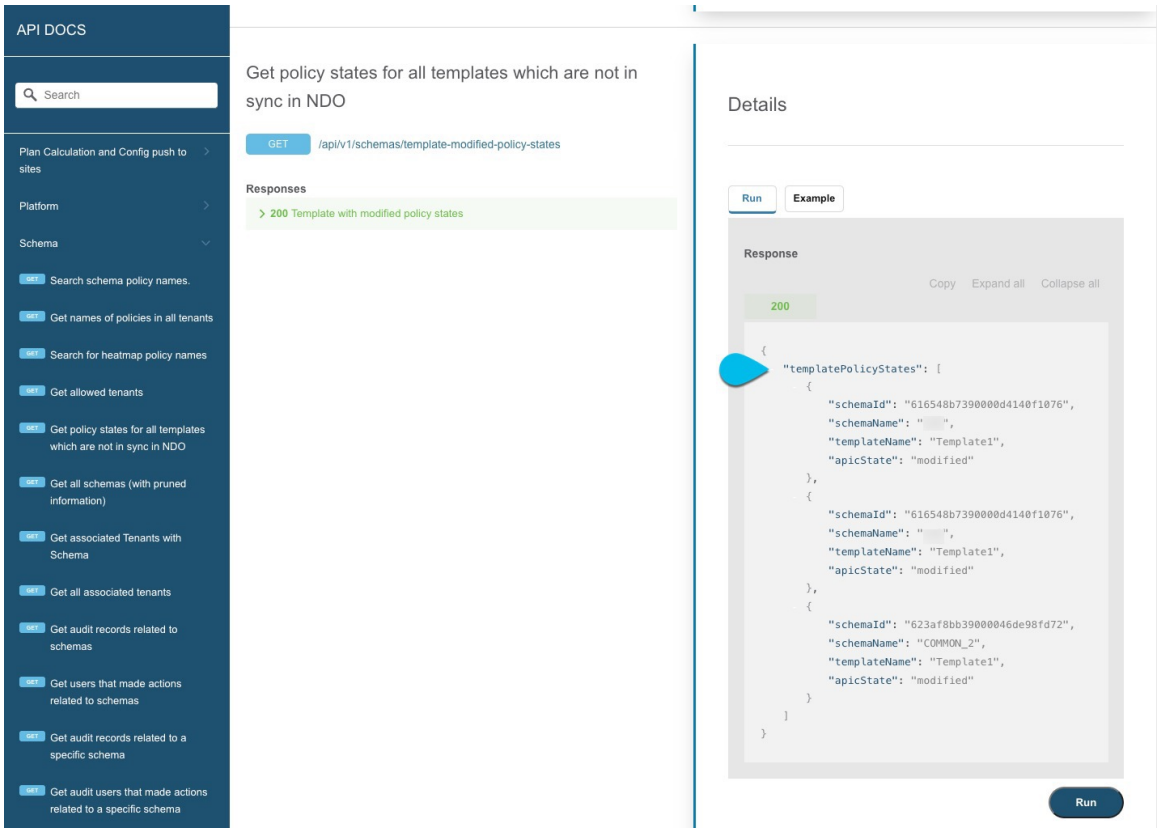


e) Scroll down to the `/api/v1/schemas/template-modified-policy-states` API and click **Run**.



Depending on the number of templates and the size of the configuration, this may take a few minutes, and the **Run** button will be grayed out during this process.

f) Note down all the templates returned by the API call.



Step 2 Check for configuration drifts using the GUI.

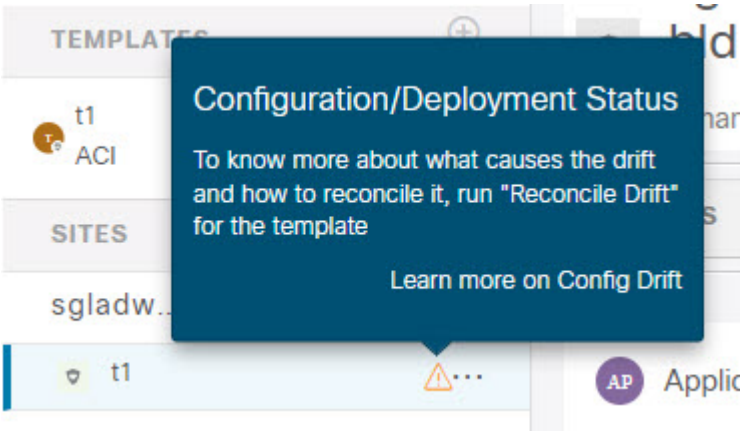
a) In your Nexus Dashboard Orchestrator, navigate to **Application Management** > **Schemas**.

b) Select the first schema and check its templates for configuration drifts.

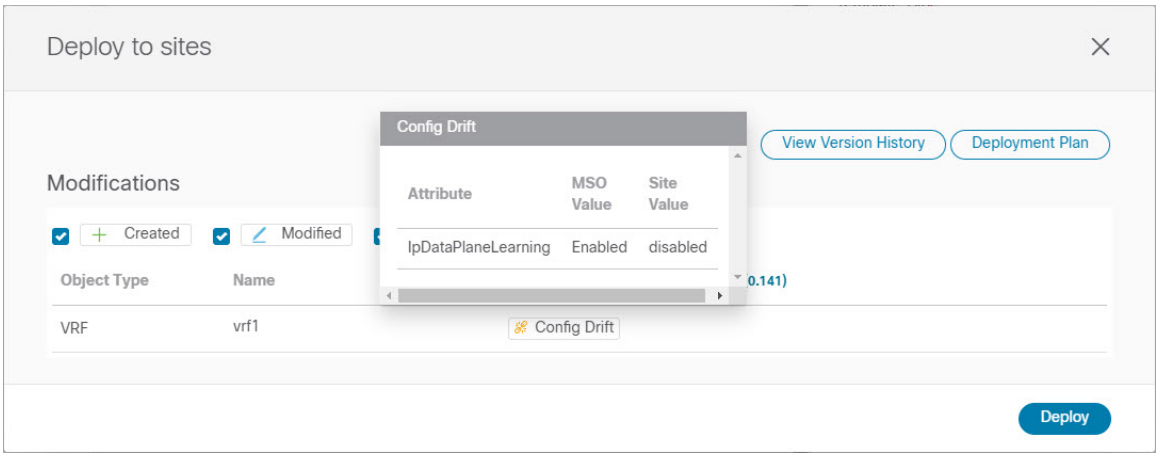
You will repeat the following steps for every schema and template in your deployment

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:



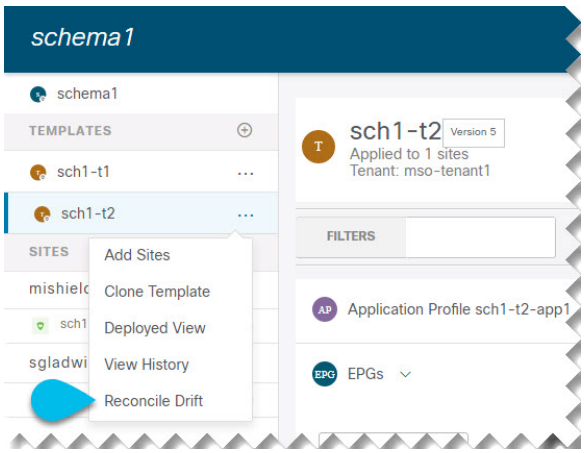
Step 3 For every template that contains a configuration drift, resolve the conflicts.

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.

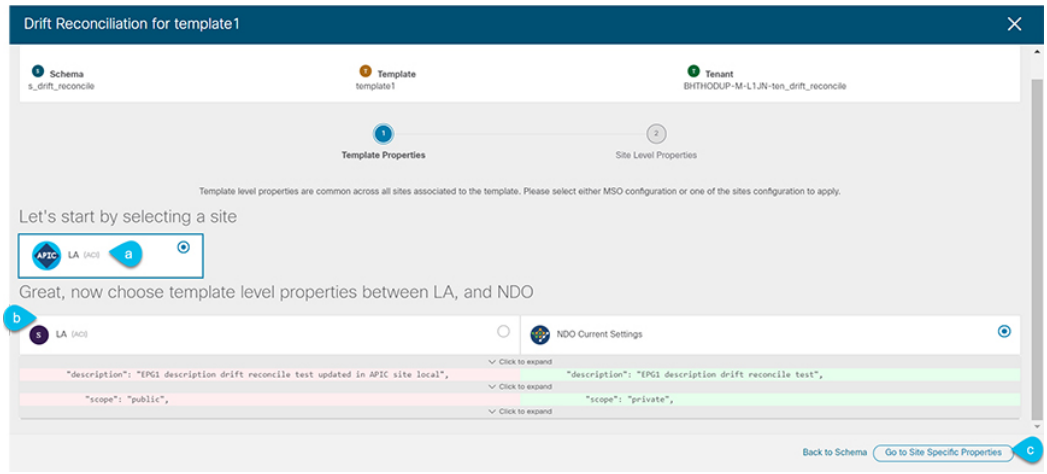
Deploying any templates at this point would push the values in the Orchestrator database and overwrite any existing settings in the fabrics.

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



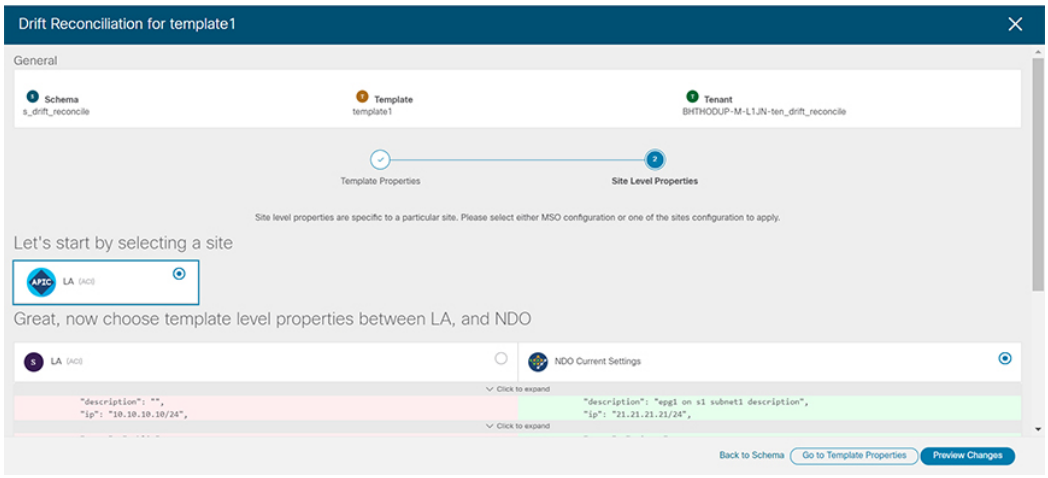
The **Drift Reconciliation** wizard opens.

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



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.



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.