Cisco Multi-Site Orchestrator Deployment Guide, Release 3.2(x)

First Published: 2020-11-25

Last Modified: 2020-12-22

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.

CONTENTS

CHAPTER 1

New and Changed Information

New and Changed Information

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

Table 1: Latest Updates

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

CHAPTER 2

Deploying Multi-Site Orchestrator

Deployment Overview

Beginning with Release 3.2(1), you must deploy the Cisco Multi-Site Orchestrator (MSO) as an application in Cisco Nexus Dashboard.

Cisco Nexus Dashboard is a central management console for multiple data center sites and a common platform for hosting Cisco data center applications. Nexus Dashboard provides a common platform and modern technology stack for these micro-services-based applications, simplifying the life cycle management of the different modern applications and reducing the operational overhead to run and maintain those applications. Cisco Nexus Dashboard supports the Cisco Day-2 Operations apps, which provide real time analytics, visibility, and assurance for policy and infrastructure, and the Cisco Multi-Site Orchestrator app, which provides a single pane of glass view into managing multiple Cisco ACI and Cisco DCNM fabrics.

Each Nexus Dashboard cluster consists of 3 `master` nodes. In addition, you can add up to 4 additional `worker` nodes to enable horizontal scaling and up to 2 `standby` nodes for easy cluster recovery in case of a master node failure.

For detailed information about Nexus Dashboard cluster initial deployment and configuration, see Cisco Nexus Dashboard Deployment Guide.

For more information about using Nexus Dashboard, such as adding sites and users, see the Cisco Nexus Dashboard User Guide.

This document describes initial installation requirements and procedures for the Multi-Site Orchestrator application. Detailed configuration and use case information is available from the Cisco Multi-Site Configuration Guide for Cisco ACI or Cisco Multi-Site Configuration Guide for Cisco DCNM, depending on the type of fabrics you plan to manage.

Prerequisites and Guidelines

Nexus Dashboard

You must have Cisco Nexus Dashboard deployed and fabric connectivity configured, as described in Cisco Nexus Dashboard Deployment Guide.

This release of Cisco Multi-Site Orchestrator is supported on Nexus Dashboard physical appliance clusters only. The following table summarizes the Nexus Dashboard requirements for Cisco Multi-Site Orchestrator.

Orchestrator Version	Requirements
Release 3.2(1) and later	Cisco Nexus Dashboard, Release 2.0.1 The Nexus Dashboard cluster must be deployed as a physical appliance.

Nexus Dashboard Networks

When first configuring Nexus Dashboard, you will need to provide two IP addresses for the two Nexus Dashboard interfaces—one connected to the Data Network and the other to the Management Network. The data network is used for the nodes' clustering and Cisco fabrics traffic. The management network is used to connect to the Cisco Nexus Dashboard GUI, CLI, or API.

The two interfaces can be in the same or different subnets. In addition, each network's interfaces across different nodes in the cluster can also be in different subnets.

Connectivity between the nodes is required on both networks with the round trip time (RTT) not exceeding 150ms for Multi-Site Orchestrator. Other application running in the same Nexus Dashboard cluster may have lower RTT requirements, so we recommend consulting the Nexus Dashboard User Guide or the specific application's documentation.

When Multi-Site Orchestrator app is deployed in Nexus Dashboard, it uses each of the two networks for different purposes as shown in the following table:

MSO Traffic Type	Nexus Dashboard Network
Any traffic to and from: • Cisco APIC • Cisco DCNM • Any other remote devices or controllers	Data network
Intra-cluster communication	Data network
Audit log streaming (Splunk/syslog)	Management network
Remote backup	Management network

Nexus Dashboard Cluster Sizing

Nexus Dashboard supports co-hosting of applications. Depending on the type and number of applications you choose to run, you may be required to deploy additional worker nodes in your cluster. For cluster sizing information and recommended number of nodes based on specific use cases, see the Cisco Nexus Dashboard Capacity Planning tool.

If you plan to host other applications in addition to the Multi-Site Orchestrator, ensure that you deploy and configure additional Nexus Dashboard nodes based on the cluster sizing tool recommendation, as described in the Cisco Nexus Dashboard User Guide, which is also available directly from the Nexus Dashboard GUI.

Network Time Protocol (NTP)

Multi-Site Orchestrator uses NTP for clock synchronization, so you must have an NTP server configured in your environment.

Installing Multi-Site Orchestrator Application Using App Store

This section describes how to install Cisco Multi-Site Orchestrator application in an existing Cisco Nexus Dashboard cluster.

Before you begin

- Ensure that you meet the requirements and guidelines described in Prerequisites and Guidelines, on page 4.
- The Cisco DC App Center must be reachable from the Nexus Dashboard via the Management Network directly or using a proxy configuration. Nexus Dashboard proxy configuration is described in the Nexus Dashboard User Guide.

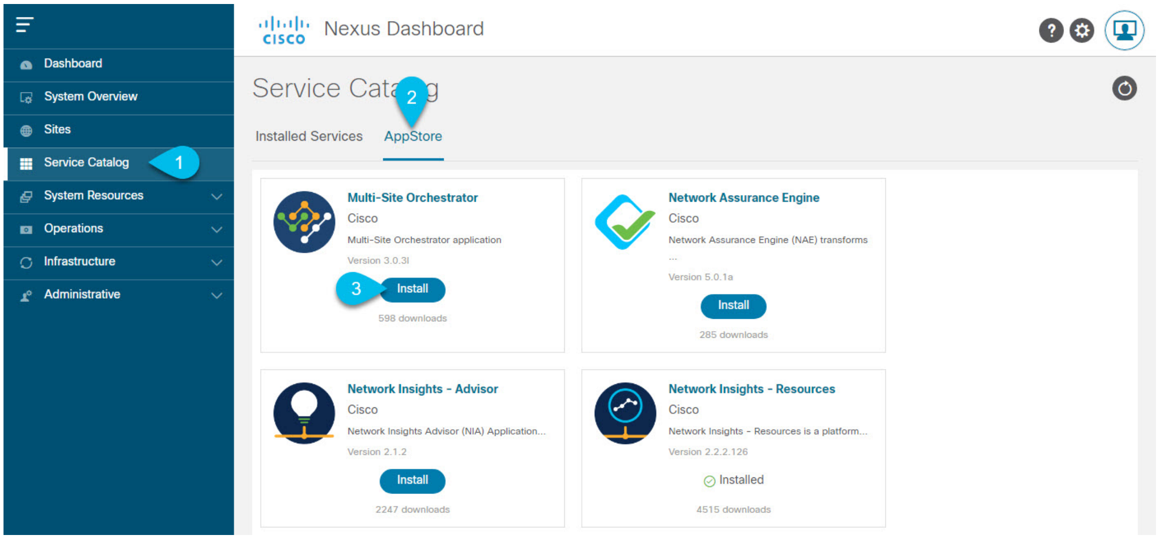
  If you are unable to establish the connection to the DC App Center, skip this section and follow the steps described in Installing Multi-Site Orchestrator Application Manually, on page 6.
- The App Store allows you to install the latest version of the application only.

  If you want to install an earlier version, you will need to download the application image and manually upload it to the Nexus Dashboard, as described in Installing Multi-Site Orchestrator Application Manually, on page 6.

  Note Nexus Dashboard supports MSO Release 3.2(1) or later only. If you want to install a version prior to Release 3.2(1), see the Multi-Site Orchestrator Installation Guide specific to that release for the available deployment options and procedures.

Step 1 Log in to the Nexus Dashboard GUI

Step 2 Navigate to the App Store and choose Multi-Site Orchestrator app.



a) From the left navigation menu, select Service Catalog.
b) Select the App Store tab.
c) In the Multi-Site Orchestrator tile, click Install.

Step 3 In the License Agreement window that opens, click Agree and Download.

Step 4 Wait for the application to be downloaded to the Nexus Dashboard and deployed.

It may take up to 30 minutes for the application to replicate to all nodes and all services to fully deploy.

Step 5 Enable the app.

After installation is complete, the application will remain in the `Disabled` state by default and you must enable it.

To enable the app, click the ... menu on the app and select Enable.

Step 6 Launch the app.

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

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

Installing Multi-Site Orchestrator Application Manually

This section describes how to manually upload and install Cisco Multi-Site Orchestrator application in an existing Cisco Nexus Dashboard cluster.

Before you begin

- Ensure that you meet the requirements and guidelines described in Prerequisites and Guidelines, on page 4.

Step 1 Download the Cisco Multi-Site Orchestrator application.

a) Browse to the Multi-Site Orchestrator page on DC App Center:

https://dcappcenter.cisco.com/nexus-dashboard-orchestrator.html

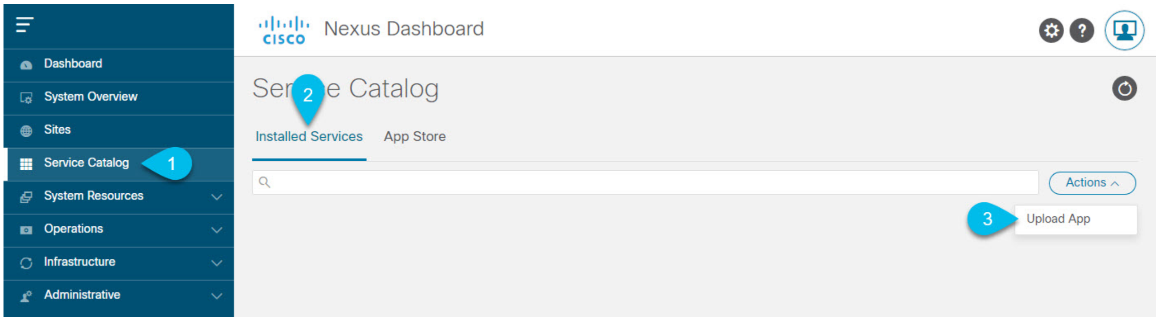
b) From the Version drop-down, choose the version you want to install and click Download.

c) Click Agree and download to accept the license agreement and download the image.

Step 2 Log in to your Cisco Nexus Dashboard dashboard.

When deploying an app, you need to install it in only one of the Nexus Dashboard nodes, the application will be replicated to the other nodes in the cluster automatically. So you can log in to any one of your Nexus Dashboard nodes using its management IP address.

Step 3 Upload the app image.

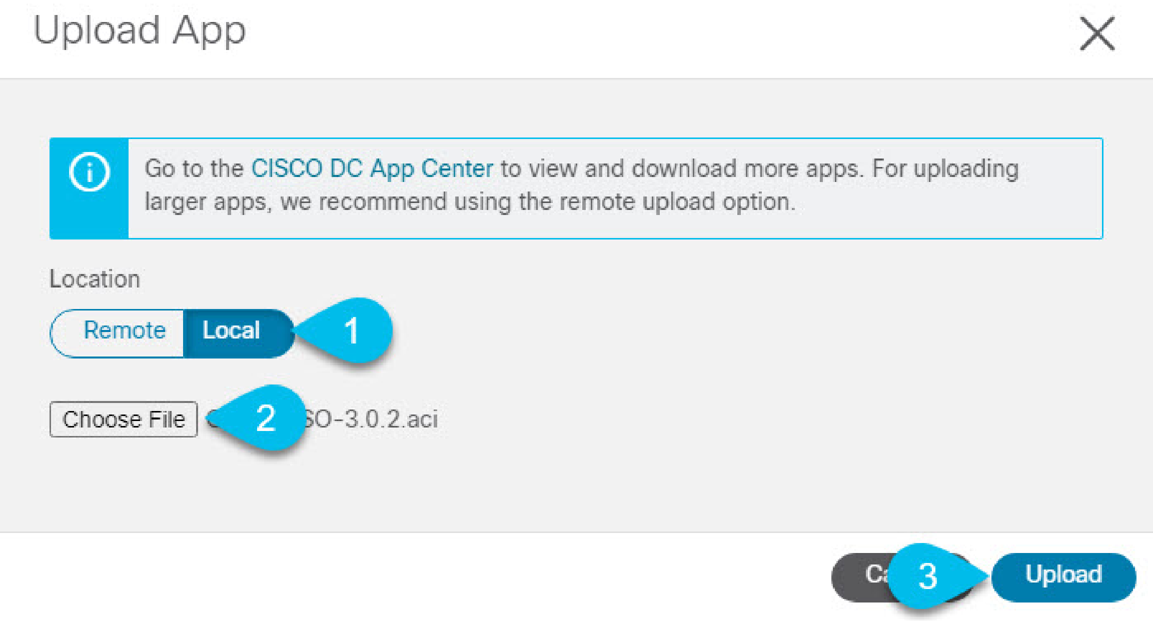


a) In the left navigation bar, click Service Catalog.

b) Select the Installed Services tab.

c) In the top right of the main pane, select Actions > Upload App.

Step 4 Upload the image file to the Nexus Dashboard cluster.


Upload App

Go to the CISCO DC App Center to view and download more apps. For uploading larger apps, we recommend using the remote upload option.

a) Choose the location of the image.

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

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

b) Choose the file.

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

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

c) Click Upload to add the app to the cluster.

Step 5 Wait for the application to be downloaded to the Nexus Dashboard and deployed.

It may take up to 30 minutes for the application to replicate to all nodes and all services to fully deploy.

Step 6 Enable the app.

After installation is complete, the application will remain in the `Disabled` state by default and you must enable it.

To enable the app, click the ... menu on the app and select Enable.

Step 7 Launch the app.

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

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

PART I

Day-0 Operations for ACI Fabrics

CHAPTER 3

Configuring Cisco ACI Sites

Pod Profile and Policy Group

In each site's APIC, you must have one POD profile with a POD policy group. If you site does not have a POD policy group you must create one.

Procedure

	Command or Action	Purpose
Step 1	Log in to the site's Cisco APIC GUI.	
Step 2	Check that the POD profile contains a POD policy group.	Navigate to Fabric > Fabric Policies > Pods > Profiles > Pod Profile default.
Step 3	If necessary, create a POD policy group.	
Step 4	Assign the new POD policy group to the default POD profile.	

Configuring Fabric Access Policies for All APIC Sites

Before your APIC fabrics can be added to and managed by the Multi-Site Orchestrator, there is a number of fabric-specific access policies that you must configure on each site.

Configuring Fabric Access Global Policies

This section describes the global fabric access policy configurations that must be created for each APIC site before it can be added to and managed by the Multi-Site Orchestrator.

Step 1 Log in directly to the site's APIC GUI.

Step 2 From the main navigation menu, select Fabric > Access Policies.

You must configure a number of fabric policies before the site can be added to the Multi-Site Orchestrator. From the APIC's perspective, this is something you do just like you would if you were connecting a bare-metal host, where you would configure domains, AEPs, policy groups, and interface selectors; you must configure the same options for connecting the spine switch interfaces to the inter-site network for all the sites that will be part of the same Multi-Site domain.

Step 3 Specify the VLAN pool.

The first thing you configure is the VLAN pool. We use Layer 3 sub-interfaces tagging traffic with VLAN-4 to connect the spine switches to the inter-site network.

a) In the left navigation tree, browse to Pools > VLAN.
b) Right-click the VLAN category and choose Create VLAN Pool.

In the Create VLAN Pool window, specify the following:

- For the Name field, specify the name for the VLAN pool, for example `msite`.
- For Allocation Mode, specify `Static Allocation`.
- And for the Encap Blocks, specify just the single VLAN 4. You can specify a single VLAN by entering the same number in both Range fields.

Step 4 Configure Attachable Access Entity Profiles (AEP).

a) In the left navigation tree, browse to Global Policies > Attachable Access Entity Profiles.
b) Right-click the Attachable Access Entity Profiles category and choose Create Attachable Access Entity Profiles.

In the Create Attachable Access Entity Profiles window, specify the name for the AEP, for example `msite-aep`.

c) Click Next and Submit

No additional changes, such as interfaces, are required.

Step 5 Configure domain.

The domain you configure is what you will select from the Multi-Site Orchestrator when adding this site.

a) In the left navigation tree, browse to Physical and External Domains > External Routed Domains.
b) Right-click the External Routed Domains category and choose Create Layer 3 Domain.

In the Create Layer 3 Domain window, specify the following:

- For the Name field, specify the name the domain, for example `msite-l3`.
- For Associated Attachable Entity Profile, select the AEP you created in Step 4.
- For the VLAN Pool, select the VLAN pool you created in Step 3.

c) Click Submit.

No additional changes, such as security domains, are required.

What to do next

After you have configured the global access policies, you must still add interfaces policies as described in #unique_14.

Configuring Fabric Access Interface Policies

This section describes the fabric access interface configurations that must be done for the Multi-Site Orchestrator on each APIC site.

Before you begin

You must have configured the global fabric access policies, such as VLAN Pool, AEP, and domain, in the site's APIC, as described in #unique_16.

Step 1 Log in directly to the site's APIC GUI.

Step 2 From the main navigation menu, select Fabric > Access Policies.

In addition to the VLAN, AEP, and domain you have configured in previous section, you must also create the interface policies for the fabric's spine switch interfaces that connect to the Inter-Site Network (ISN).

Step 3 Configure a spine policy group.

a) In the left navigation tree, browse to Interface Policies > Policy Groups > Spine Policy Groups.

This is similar to how you would add a bare-metal server, except instead of a Leaf Policy Group, you are creating a Spine Policy Group.

b) Right-click the Spine Policy Groups category and choose Create Spine Access Port Policy Group.

In the Create Spine Access Port Policy Group window, specify the following:

- For the Name field, specify the name for the policy group, for example `Spine1-PolGrp`.
- For the Link Level Policy field, specify the link policy used between your spine switch and the ISN.
- For CDP Policy, choose whether you want to enable CDP.
- For the Attached Entity Profile, select the AEP you have configured in previous section, for example `msite-aep`.

c) Click Submit.

No additional changes, such as security domains, are required.

Step 4 Configure a spine profile.

a) In the left navigation tree, browse to Interface Policies > Profiles > Spine Profiles.

b) Right-click the Spine Profiles category and choose Create Spine Interface Profile.

In the Create Spine Interface Profile window, specify the following:

- For the Name field, specify the name for the profile, for example `Spine1-ISN`.
- For Interface Selectors, click the + sign to add the port on the spine switch that connects to the ISN. Then in the Create Spine Access Port Selector window, provide the following:
  - For the Name field, specify the name for the port selector, for example `Spine1-ISN`.

- For the Interface IDs, specify the switch port that connects to the ISN, for example `5/32`.
- For the Interface Policy Group, choose the policy group you created in the previous step, for example `Spine1-PolGrp`.

Then click OK to save the port selector.

c) Click Submit to save the spine interface profile.

Step 5 Configure a spine switch selector policy.

a) In the left navigation tree, browse to Switch Policies > Profiles > Spine Profiles.
b) Right-click the Spine Profiles category and choose Create Spine Profile.

   In the Create Spine Profile window, specify the following:

   - For the Name field, specify the name for the profile, for example `Spine1`.
   - For Spine Selectors, click the +to add the spine and provide the following:
     - For the Name field, specify the name for the selector, for example `Spine1`.
     - For the Blocks field, specify the spine node, for example `201`.

c) Click Update to save the selector.
d) Click Next to proceed to the next screen.
e) Select the interface profile you have created in the previous step

   For example `Spine1-ISN`.

f) Click Finish to save the spine profile.

Configuring Sites That Contain Remote Leaf Switches

Starting with Release 2.1(2), the Multi-Site architecture supports APIC sites with Remote Leaf switches. The following sections describe guidelines, limitations, and configuration steps required to allow Multi-Site Orchestrator to manage these sites.

Remote Leaf Guidelines and Limitations

If you want to add an APIC site with a Remote Leaf to be managed by the Multi-Site Orchestrator, the following restrictions apply:

- You must upgrade your Cisco APIC to Release 4.2(4) or later.
- Only physical Remote Leaf switches are supported in this release
- Only -EX and -FX or later switches are supported as Remote Leaf switches for use with Multi-Site
- Remote Leaf is not supported with back-to-back connected sites without IPN switches
- Remote Leaf switches in one site cannot use another site's L3Out

- Stretching a bridge domain between one site and a Remote Leaf in another site is not supported

You must also perform the following tasks before the site can be added to and managed by the Multi-Site Orchestrator:

- You must enable Remote Leaf direct communication and configure routable subnets directly in the site's APIC, as described in the following sections.
- You must add the routable IP addresses of Cisco APIC nodes in the DHCP-Relay configuration applied on the interfaces of the Layer 3 routers connecting to the Remote Leaf switches.

  The routable IP address of each APIC node is listed in the Routable IP field of the System > Controllers > <controller-name> screen of the APIC GUI.

Configuring Routable Subnets for Remote Leaf Switches

Before you can add a site that contains one or more Remote Leaf switches to the Multi-Site Orchestrator, you must configure routable subnets for the pod with which the Remote Leaf nodes are associated.

Step 1 Log in directly to the site's APIC GUI.

Step 2 From the menu bar, select Fabric > Inventory.

Step 3 In the Navigation pane, click Pod Fabric Setup Policy.

Step 4 In the main pane, double-click the pod where you want to configure the subnets.

Step 5 In the Routable Subnets area, click the + sign to add a subnet.

Step 6 Enter the IP and Reserve Address Count, set the state to `Active` or `Inactive`, then click Update to save the subnet.

When configuring routable subnets, you must provide a netmask between `/22` and `/29`.

Step 7 Click Submit to save the configuration.

Enabling Direct Communication for Remote Leaf Switches

Before you can add a site that contains one or more Remote Leaf switches to the Multi-Site Orchestrator, you must configure direct remote leaf communication for that site. Additional information about remote leaf direct communication feature is available in the Cisco APIC Layer 3 Networking Configuration Guide. This section outlines the steps and guidelines specific to the integration with Multi-Site.

Note Once you enable Remote Leaf switch direct communication, the switches will function in the new mode only

Step 1 Log in directly to the site's APIC.

Step 2 Enable direct traffic forwarding for Remote Leaf switches.

a) From the menu bar, navigate to System > System Settings.

b) From the left side bar, select Fabric Wide Setting.

c) Check the Enable Remote Leaf Direct Traffic Forwarding checkbox.

Note You cannot disable this option after you enable it.

d) Click Submit to save the changes.

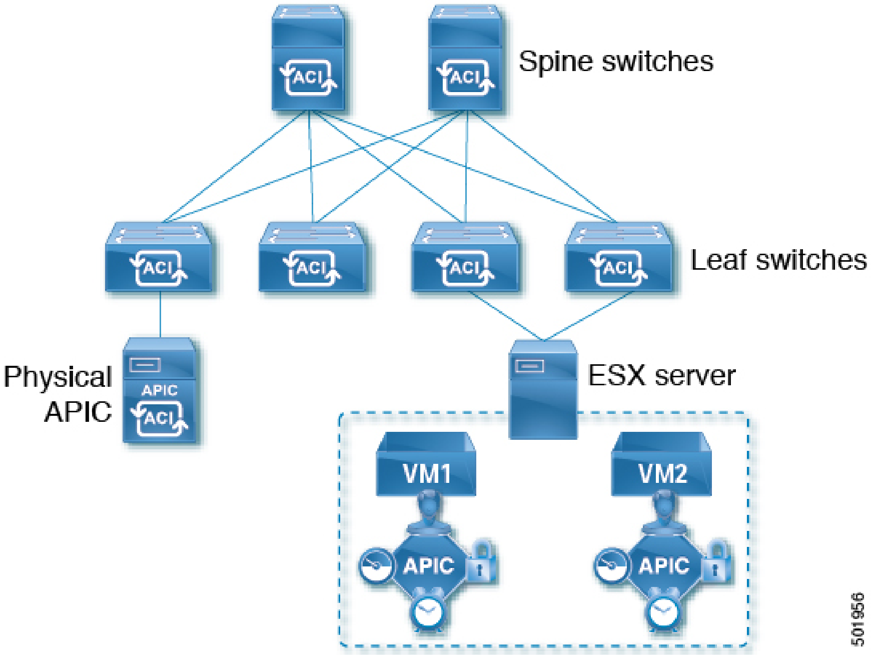
Cisco Mini ACI Fabrics

Cisco Multi-Site supports Cisco Mini ACI fabrics as typical on-premises sites without requiring any additional configuration. This section provides brief overview of Mini ACI fabrics, detailed info on deploying and configuring this type of fabrics is available in Cisco Mini ACI Fabric and Virtual APICs.

Cisco ACI, Release 4.0(1) introduced Mini ACI Fabric for small scale deployment. Mini ACI fabric works with Cisco APIC cluster consisting of one physical APIC and two virtual APICs (vAPIC) running in virtual machines. This reduces the physical footprint and cost of the APIC cluster, allowing ACI fabric to be deployed in scenarios with limited rack space or initial budget, such as a colocation facility or a single-room data center, where a full-scale ACI installations may not be practical due to physical footprint or initial cost.

The following diagram shows an example of a mini Cisco ACI fabric with a physical APIC and two virtual APICs (vAPICs):

Figure 1: Cisco Mini ACI Fabric



CHAPTER 4

Adding and Deleting Sites

Cisco MSO and APIC Interoperability Support

Cisco Multi-Site Orchestrator (MSO) does not require a specific version of APIC to be running in all sites. The APIC clusters in each site as well as the MSO itself can be upgraded independently of each other and run in mixed operation mode as long as each fabric is running APIC, Release 3.2(6) or later. As such, we recommend that you always upgrade to the latest release of the Multi-Site Orchestrator.

However, keep in mind that if you upgrade the MSO before upgrading the APIC clusters in one or more sites, some of the new MSO features may not yet be supported by an earlier APIC release. In that case a check is performed on each template to ensure that every configured option is supported by the target sites.

The check is performed when you save a template or deploy a template. If the template is already assigned to a site, any unsupported configuration options will not be saved; if the template is not yet assigned, you will be able to assign it to a site, but not be able to save or deploy the schema if it contains configuration unsupported by that site.

In case an unsupported configuration is detected, an error message will show, for example: `This APIC site version` *`<site-version>`* `is not supported by MSO. The minimum version required for this` *`<feature>`* `is` *`<required-version>`* `or above.`

The following table lists the features and the minimum required APIC release for each one:

Note While some of the following features are supported on earlier Cisco APIC releases, Release 4.2(4) is the earliest release that can be on-boarded to the Nexus Dashboard and managed by this release of Multi-Site Orchestrator.

Feature	Minimum APIC Version
ACI Multi-Pod Support	Release 4.2(4)
Service Graphs (L4-L7 Services)	Release 4.2(4)

Feature	Minimum APIC Version
External EPGs	Release 4.2(4)
ACI Virtual Edge VMM Support	Release 4.2(4)
DHCP Support	Release 4.2(4)
Consistency Checker	Release 4.2(4)
vzAny	Release 4.2(4)
Host Based Routing	Release 4.2(4)
CloudSec Encryption	Release 4.2(4)
Layer 3 Multicast	Release 4.2(4)
MD5 Authentication for OSPF	Release 4.2(4)
EPG Preferred Group	Release 4.2(4)
Intersite L3Out	Release 4.2(4)

Adding Cisco APIC Sites

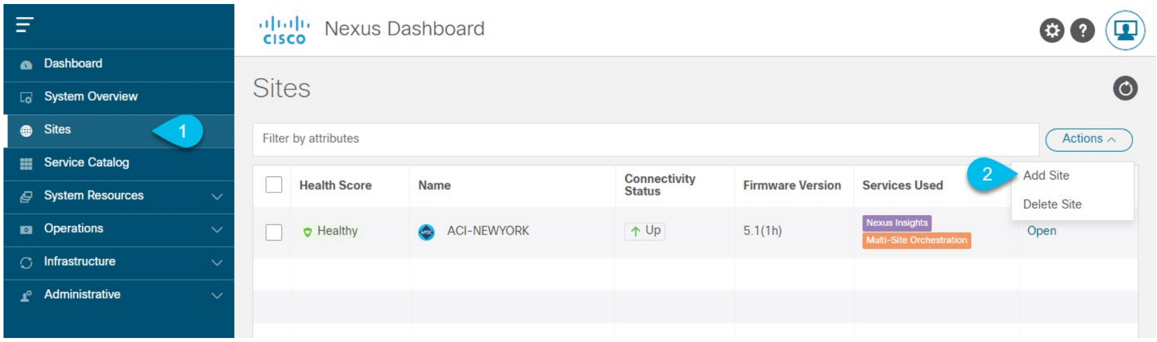
This section describes how to add a Cisco APIC site using the Nexus Dashboard GUI and then enable that site to be managed by Multi-Site Orchestrator.

Before you begin

- You must have completed the site-specific configurations in each site's APIC, as described in previous sections in this chapter.
- You must ensure that the site(s) you are adding are running Cisco APIC, Release 4.2(4) or later.

Step 1 Log in to the Nexus Dashboard GUI

Step 2 Add a new site.

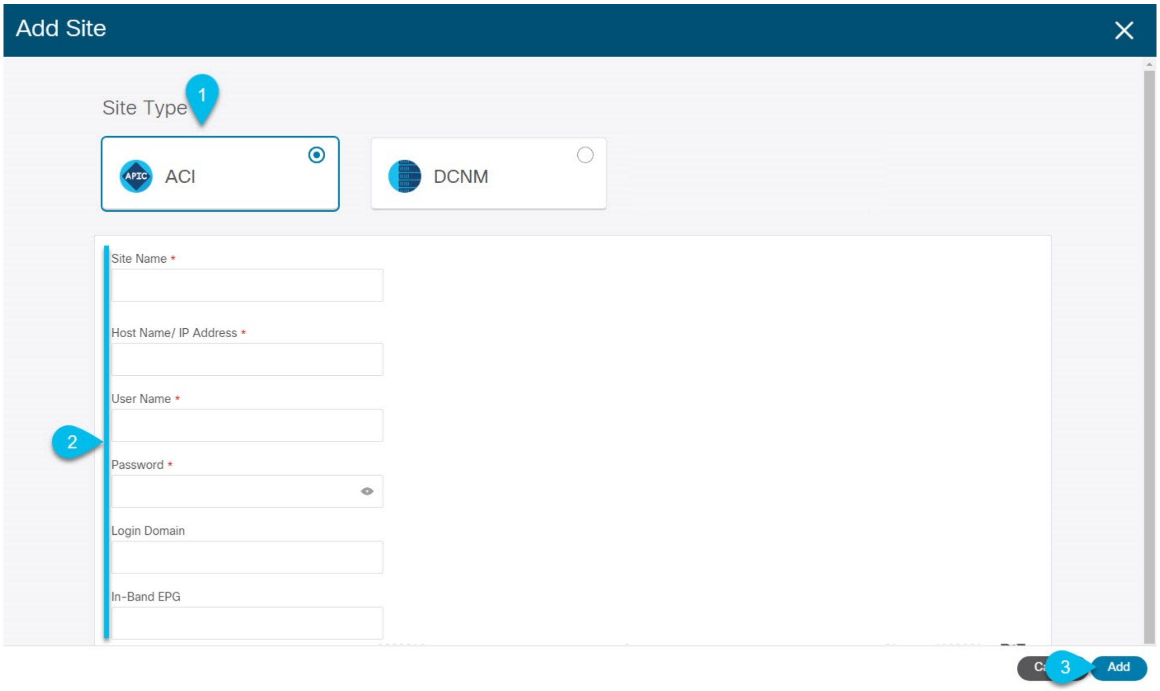


Health Score	Name	Connectivity Status	Firmware Version	Services Used	
Healthy	ACI-NEWYORK	Up	5.1(1h)	Nexus Insights Multi-Site Orchestration	Open

a) From the left navigation menu, select Sites.

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

Step 3 Provide site information.



a) For Site Type, select ACI.

b) Provide the APIC 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 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 Multi-Site Orchestrator only, you can leave this field blank.

c) Click Add to finish adding the site.

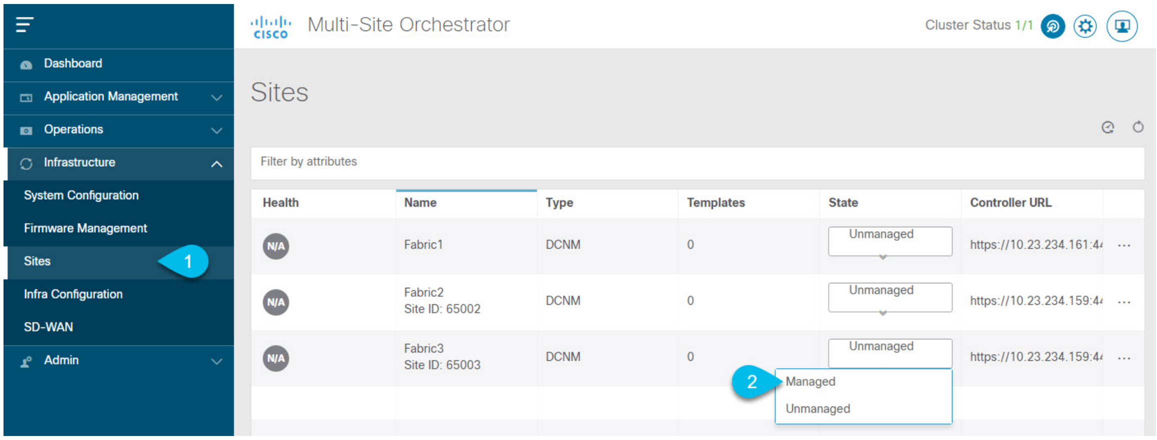
At this time, the sites will be available in the Nexus Dashboard, but you still need to enable them for Multi-Site Orchestrator management as described in the following steps.

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

Step 5 From the Nexus Dashboard's Service Catalog, open the Multi-Site Orchestrator application.

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

Step 6 In the Multi-Site Orchestrator GUI, enable the sites.



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

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

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

Removing Sites

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

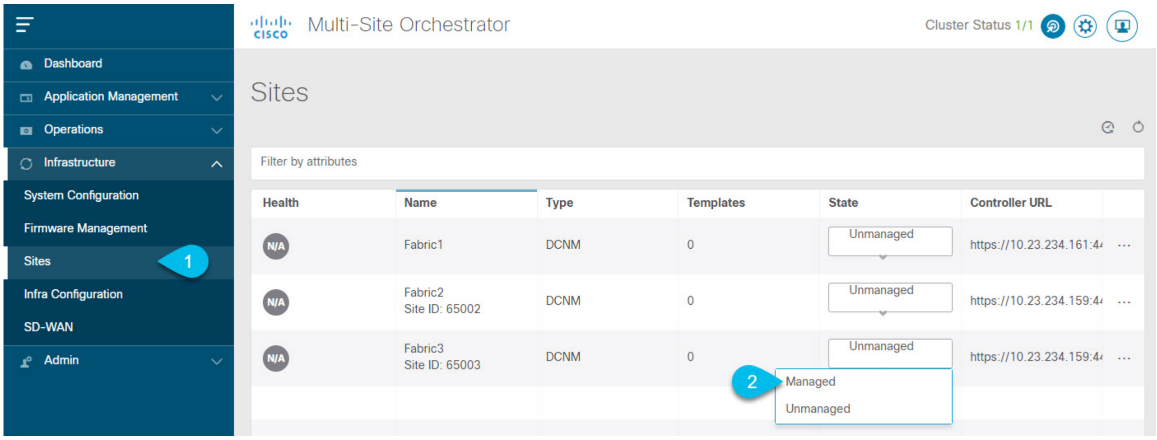
Before you begin

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

Step 1 Open the Multi-Site Orchestrator GUI.

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

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



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

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

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

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

Cross Launch to Fabric Controllers

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

You can cross launch into the specific site controller's GUI from the MSO's 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 your Nexus Dashboard and the fabric are configured for remote user authentication, you will be logged in automatically into the fabric's controller using the same log in information as the Nexus Dashboard user.

CHAPTER 5

Configuring Infra for Cisco ACI Sites

Prerequisites and Guidelines

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

Before you proceed with Infra configuration, you must have configured and added the sites as described in previous sections, which includes:

- Configuring each site's fabric access policies.
- Configuring direct communication and routable subnets for sites with remote leaf switches.

In addition, keep in mind the following:

- Any infrastructure changes such as adding and removing spine switches or spine node ID changes require a Multi-Site Orchestrator fabric connectivity information refresh described in the Refreshing Site Connectivity Information, on page 24 as part of the general Infra configuration procedures.
- The Overlay Unicast TEP, Overlay Multicast TEP, and BGP-EVPN Router-IDs IP addresses assigned on the Orchestrator should not be taken from the address space of the original fabric's `Infra` TEP pool or from the `0.x.x.x` range.

Configuring Infra: General Settings

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

Step 1 Log in to the Cisco Multi-Site Orchestrator GUI.

Step 2 In the left navigation menu, select Infrastructure > Infra Configuration.

Step 3 In the main pane, click Configure Infra.

Step 4 In the left sidebar, select General Settings.

Step 5 Configure control plane BGP.

a) From the BGP Peering Type dropdown, choose either `full-mesh` or `route-reflector`.

   The `route-reflector` option is effective only when all sites are part of the same BGP Autonomous System (AS).

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

   We recommend keeping the default value.

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

   We recommend keeping the default value.

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

   We recommend keeping the default value.

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

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

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

Refreshing Site Connectivity Information

Any infrastructure changes, such as adding and removing spines or changing spine node IDs, require a Multi-Site fabric connectivity site refresh. This section describes how to pull up-to-date connectivity information directly from each site's APIC.

Step 1 Log in to the Cisco Multi-Site Orchestrator GUI.

Step 2 In the Main menu, select Infrastructure > Infra Configuration.

Step 3 In the top right of the main Infra Configuration view, click the Configure Infra button.

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

Step 5 In the main window, click the Reload Site Data button to pull fabric information from the APIC.

Step 6 (Optional) In the Confirmation dialog, check the box if you want to remove configuration for decommissioned spine switch nodes.

If you choose to enable this checkbox, all configuration info for any currently decommissioned spine 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 APIC.

Configuring Infra: On-Premises Site Settings

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

Step 1 Log in to the Cisco Multi-Site Orchestrator GUI.

Step 2 In the left navigation menu, select Infrastructure > Infra Configuration.

Step 3 In the main pane, click Configure Infra.

Step 4 In the left pane, under Sites, select a specific on-premises site.

Step 5 In the right ***<Site>*** Settings pane, enable the Multi-Site knob to manage the site from the Orchestrator.

Step 6 (Optional) Enable the CloudSec Encryption knob encryption for the site.

CloudSec Encryption provides inter-site traffic encryption. The "Infrastructure Management" chapter in the Cisco Multi-Site Configuration Guide covers this feature in detail.

Step 7 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 spine switches that are part of the same fabric, regardless of whether it is a single pod or multi-pod fabric.

Step 8 Specify the BGP Autonomous System Number.

Step 9 Specify the BGP Password.

Step 10 Specify the OSPF Area ID.

When configuring the Multi-Site infra OSPF details, we recommend that you use OSPF Area `0`. If you use an Area ID other than `0`, in the next step configure it as a `regular` OSPF area type and not a `stub` area type.

Step 11 Select the OSPF Area Type from the dropdown menu.

The OSPF area type can be one of the following:

- `nssa`
- `regular`
- `stub`

Step 12 Select the external routed domain from the dropdown menu.

Choose an external router domain that you have created in the Cisco APIC GUI.

Step 13 Configure OSPF settings for the site.

You can either click an existing policy (for example, `msc-ospf-policy-default`) to modify it or click +Add Policy to add a new OSPF policy. Then in the Add/Update Policy window, specify the following:

- In the Policy Name field, enter the policy name.
- In the Network Type field, choose either `broadcast`, `point-to-point`, or `unspecified`.

  The default is `broadcast`.
- In the Priority field, enter the priority number.

  The default is `1`.

- In the Cost of Interface field, enter the cost of interface.

  The default is `0`.

- From the Interface Controls dropdown menu, choose one of the following:
  - advertise-subnet
  - bfd
  - mtu-ignore
  - passive-participation

- In the Hello Interval (Seconds) field, enter the hello interval in seconds.

  The default is `10`.

- In the Dead Interval (Seconds) field, enter the dead interval in seconds.

  The default is `40`.

- In the Retransmit Interval (Seconds) field, enter the retransmit interval in seconds.

  The default is `5`.

- In the Transmit Delay (Seconds) field, enter the transmit delay in seconds.

  The default is `1`.

Step 14 (Optional) Configure SR-MPLS settings for the site.

If the site is connected via an MPLS network, enable the SR-MPLS Connectivity knob and provide the Segment Routing global block (SRGB) range.

The Segment Routing Global Block (SRGB) is the range of label values reserved for Segment Routing (SR) in the Label Switching Database (LSD). These values are assigned as segment identifiers (SIDs) to SR-enabled nodes and have global significance throughout the domain.

The default range is `16000-23999`.

If you enable MPLS connectivity for the site, you will need to configure additional settings as described in the "Sites Connected via SR-MPLS" chapter of the Cisco Multi-Site Configuration Guide for ACI Fabrics.

Configuring Infra: Pod Settings

This section describes how to configure pod-specific settings in each site.

Step 1 Log in to the Cisco Multi-Site Orchestrator GUI.

Step 2 In the Main menu, click Sites.

Step 3 In the Sites view, click Configure Infra.

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

Step 5 In the main window, select a pod.

Step 6 In the right POD Properties pane, add the Overlay Unicast TEP for the POD.

This IP address is deployed on all spine switches that are part of the same pod and used for intersite known unicast traffic.

Step 7 Click +Add TEP Pool to add a routable TEP pool.

The routable TEP pools are used for public IP addresses for inter-site connectivity.

Step 8 Repeat the procedure for every pod in the site.

Configuring Infra: Spine Switches

This section describes how to configure spine switches in each site for Cisco Multi-Site.

Step 1 Log in to the Cisco Multi-Site Orchestrator GUI.

Step 2 In the Main menu, click Sites.

Step 3 In the Sites view, click Configure Infra.

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

Step 5 In the main window, select a spine switch within a pod.

Step 6 In the right ***<Spine>*** Settings pane, click +Add Port.

Step 7 In the Add Port window, enter the following information:

- In the Ethernet Port ID field, enter the port ID, for example `1/29`.
- In the IP Address field, enter the IP address/netmask.

  MSO creates a sub-interface with VLAN 4 with the specified IP ADDRESS under the specified PORT.
- In the MTU field, enter the MTU. You can specify either `inherit` or a value between `576` and `9000`.

  MTU of the spine port should match MTU on IPN side.
- In the OSPF Policy field, choose the OSPF policy for the switch that you have configured in Configuring Infra: On-Premises Site Settings, on page 25.

  OSPF settings in the OSPF policy you choose should match on IPN side.
- For OSPF Authentication, you can pick either `none` or one of the following:
  - `MD5`
  - `Simple`

Step 8 Enable BGP Peering knob.

In a single Pod fabric with more than two spine switches, BGP peering should only be enabled on a pair (for redundancy) of spine switches called BGP Speakers. All other spine switches should have BGP peering disabled and will function as BGP Forwarders.

In a Multi-Pod fabric BGP peering should only be enabled on a couple of BGP speaker spine switches, each deployed in a different Pod. All other spines switches should have BGP peering disabled and function as BGP forwarders.

Step 9 In the BGP-EVPN Router-ID field, provide the IP address used for BGP-eVPN session between sites.

Step 10 Repeat the procedure for every spine switch.

Deploying Infra Configuration

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

In the top right of the main pane, click Deploy to deploy the configuration.

PART II

Day-0 Operations for DCNM Fabrics

CHAPTER 6

Adding and Deleting Sites

Adding Cisco DCNM Sites

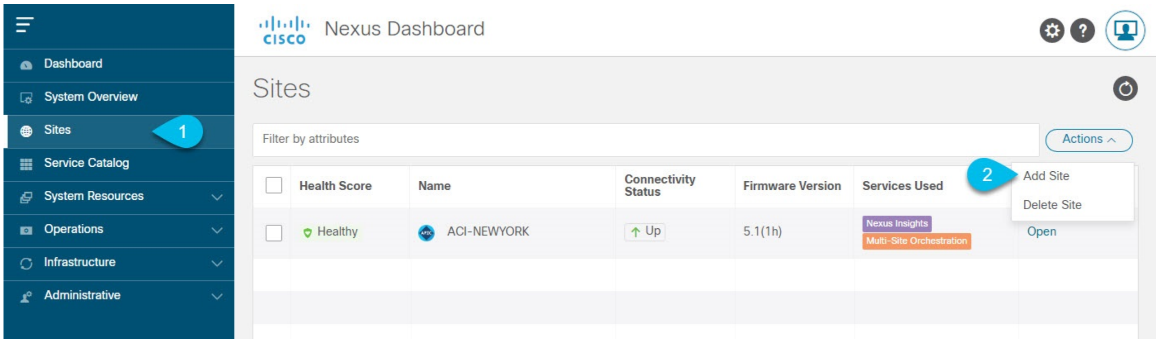
This section describes how to add a DCNM site using the Nexus Dashboard GUI and then enable that site to be managed by Multi-Site Orchestrator.

Before you begin

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

Step 1 Log in to the Nexus Dashboard GUI

Step 2 Add a new site.

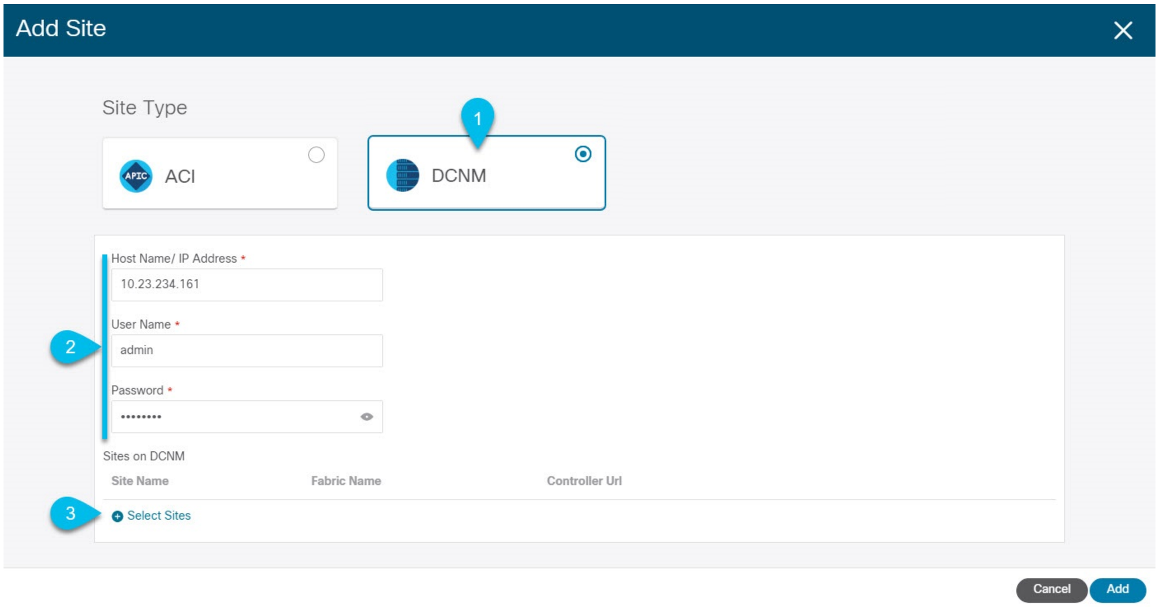


□	Health Score	Name	Connectivity Status	Firmware Version	Services Used	
□	Healthy	ACI-NEWYORK	Up	5.1(1h)	Nexus Insights Multi-Site Orchestration	Open

a) From the left navigation menu, select Sites.

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

Step 3 Provide site information.



Add Site

Site Type

○ ACI

● DCNM

Host Name/ IP Address *

10.23.234.161

User Name *

admin

Password *

••••••••

Sites on DCNM

Site Name	Fabric Name	Controller Url

Select Sites

a) For Site Type, select DCNM.

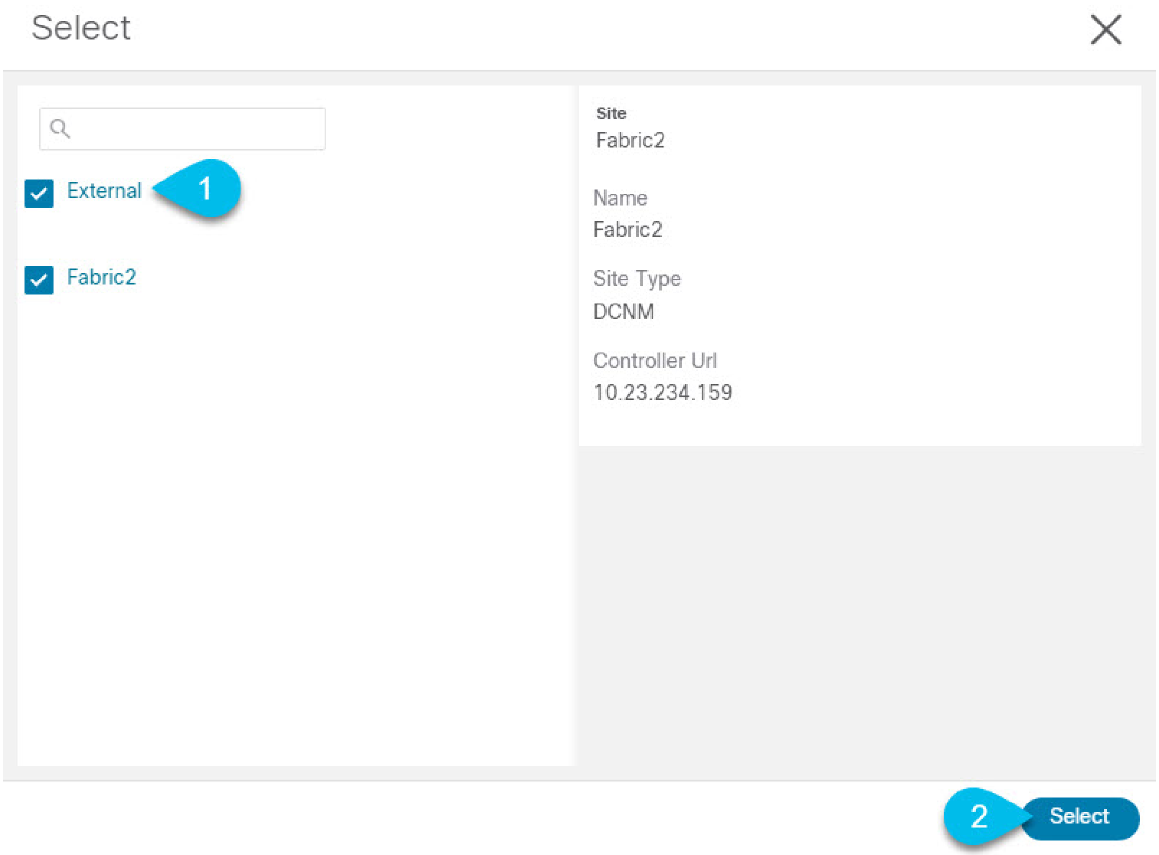
b) Provide the DCNM controller information.

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

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

The fabric selection window will open.

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



Site
Fabric2

Name
Fabric2

Site Type
DCNM

Controller Url
10.23.234.159

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

b) Click Select.

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

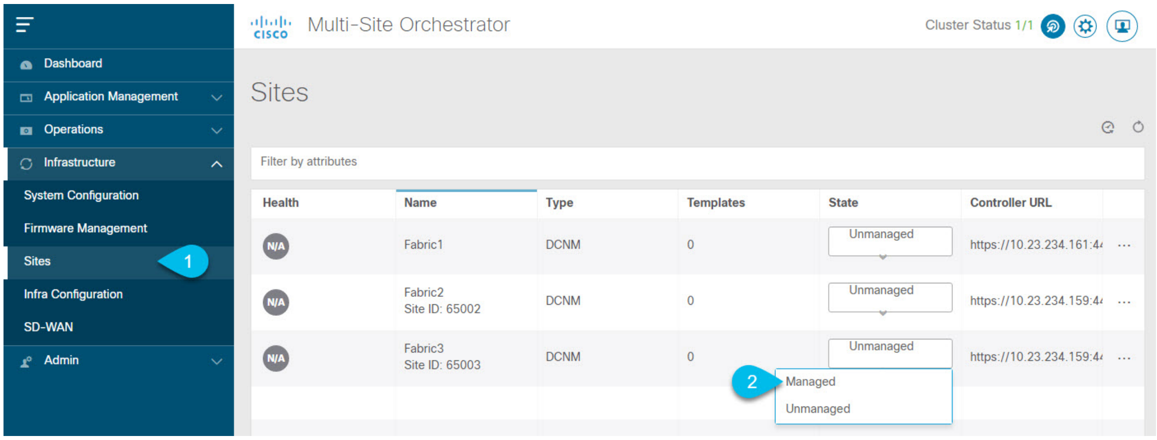
At this time, the sites will be available in the Nexus Dashboard, but you still need to enable them for Multi-Site Orchestrator management as described in the folowing steps.

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

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

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

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



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

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

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

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

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

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

Removing Sites

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

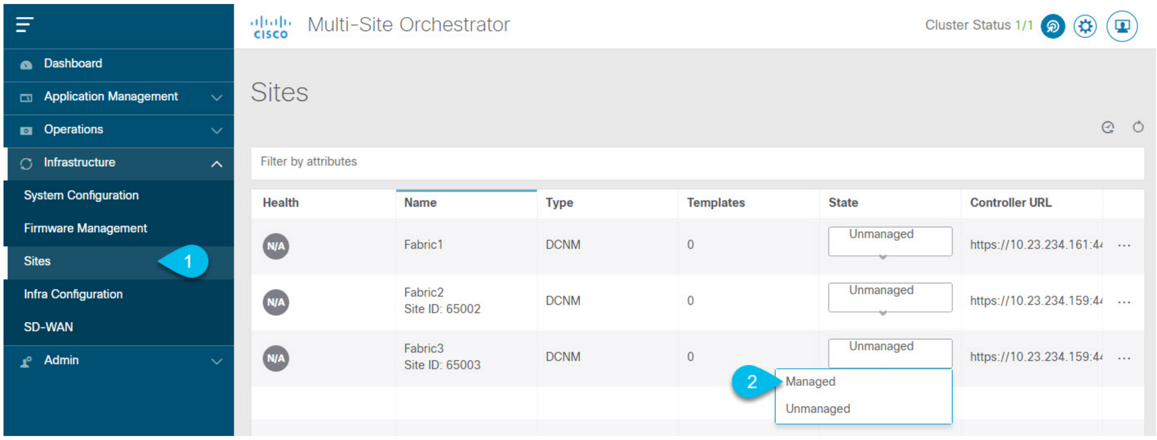
Before you begin

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

Step 1 Open the Multi-Site Orchestrator GUI.

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

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



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

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

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

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

Cross Launch to Fabric Controllers

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

You can cross launch into the specific site controller's GUI from the MSO's 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 your Nexus Dashboard and the fabric are configured for remote user authentication, you will be logged in automatically into the fabric's controller using the same log in information as the Nexus Dashboard user.

CHAPTER 7

Configuring Infra for Cisco DCNM Sites

Prerequisites and Guidelines

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

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

In addition, keep in mind the following:

- Adding or removing border gateway switches requires a Multi-Site Orchestrator fabric connectivity information refresh described in the Refreshing Site Connectivity Information, on page 38 as part of the general Infra configuration procedures.

Configuring Infra: General Settings

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

Step 1 Log in to the Cisco Multi-Site Orchestrator GUI.

Step 2 In the left navigation menu, select Infrastructure > Infra Configuration.

Step 3 In the main pane, click Configure Infra.

Step 4 In the left sidebar, select General Settings.

Step 5 Configure control plane BGP.

a) Choose BGP Peering Type.

- `full-mesh`—All border gateway switches in each site will establish peer connectivity with remote sites' border gateway switches.

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

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

In the Add Route Server window that opens:

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

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

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

We recommend keeping the default value.

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

We recommend keeping the default value.

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

We recommend keeping the default value.

d) Choose whether you want to turn on the Graceful Helper option.
e) In the Maximum AS Limit field, enter the maximum AS limit.
f) In the BGP TTL Between Peers field, enter the BGP TTL between peers.

Step 6 Configure DCNM settings.

a) Provide the L2 VXLAN VNI Range.
b) Provide the L3 VXLAN VNI Range.
c) Provide the Multi-Site Routing Loopback IP Range.

This field is used to auto-populate the Multi-Site TEP field for each fabric, which is described in Configuring Infra: DCNM Site Settings, on page 39.

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

d) Provide the Anycast Gateway MAC.

Refreshing Site Connectivity Information

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

Step 1 Log in to the Cisco Multi-Site Orchestrator GUI.

Step 2 In the left navigation menu, select Infrastructure > Infra Configuration.

Step 3 In the main pane, click Configure Infra.

Step 4 In the left sidebar, under Sites, select a specific site.

Step 5 In the main window, click the Refresh button to pull fabric information from the controller.

Step 6 (Optional) In the Confirmation dialog, check the box if you want to remove configuration for decommissioned border gateway switches.

If you choose to enable this checkbox, all configuration info for any currently decommissioned border gateway switches will be removed from the database.

Step 7 Finally, click Yes to confirm and load the connectivity information.

This will discover any new or removed spines and all site-related fabric connectivity will be re-imported from the site's controller.

Configuring Infra: DCNM Site Settings

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

Step 1 Log in to the Cisco Multi-Site Orchestrator GUI.

Step 2 In the left navigation menu, select Infrastructure > Infra Configuration.

Step 3 In the main pane, click Configure Infra.

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

Step 5 In the right ***<Site>*** Settings sidebar, specify the Multi-Site TEP.

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

Note If the site you are configuring is part of the DCNM Multi-Site Domain (MDS), this field will be pre-populated with the information imported from DCNM. In this case, changing the value and re-deploying the infra configuration, will impact traffic between the sites that are part of the MDS.

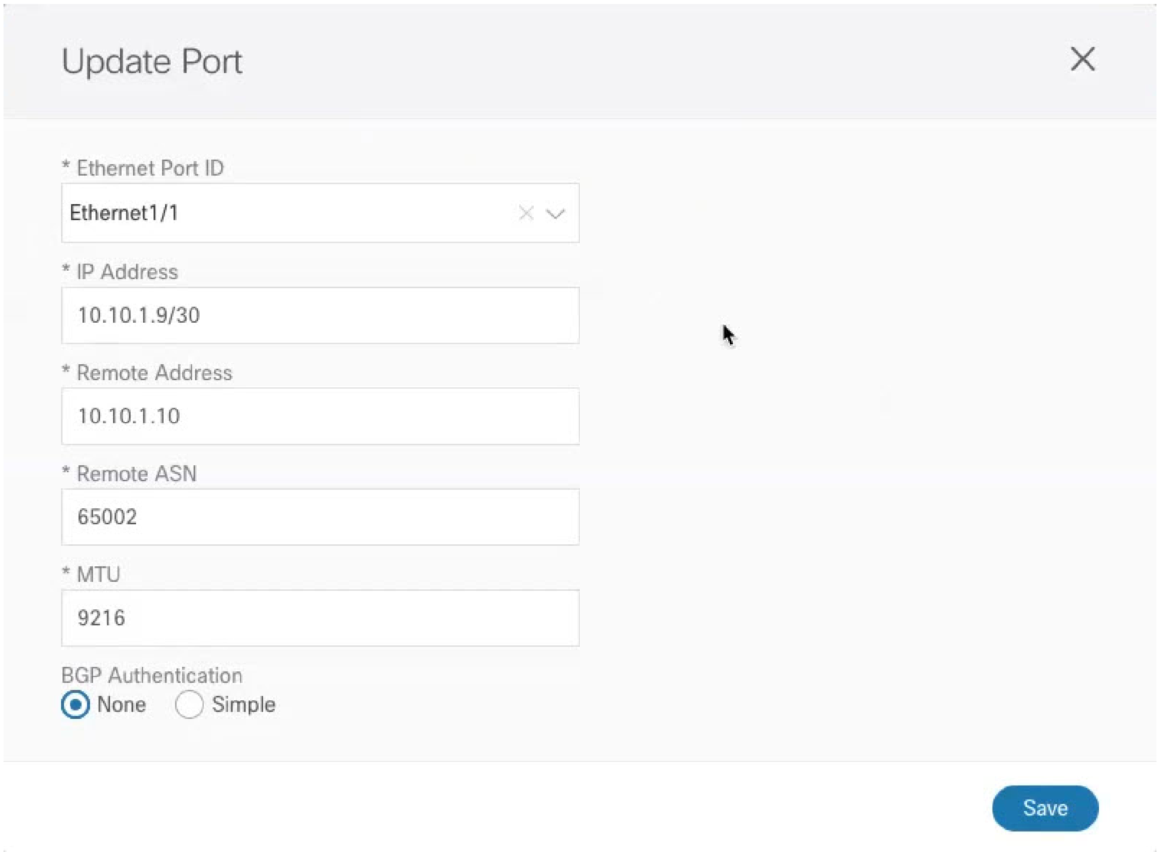
You can choose to Auto Allocate this field, which will allocate the next available address from the Multi-Site Routing Loopback IP Range you defined in previous section.

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

Step 7 In the right ***<border-gateway>*** setting sidebar, specify the Control Plane TEP and Data Plane TEP.

Step 8 Click Add Port to configure the port that connects to the IPN.

Note This release does not support importing the port configuration from the DCNM. If the site you are configuring is already part of the DCNM Multi-Site Domain (MDS), you must use the same values that are already configured in DCNM.


Update Port

* Ethernet Port ID
Ethernet1/1

* IP Address
10.10.1.9/30

* Remote Address
10.10.1.10

* Remote ASN
65002

* MTU
9216

BGP Authentication
● None ○ Simple

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

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

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

  You can specify either `inherit` or a value between `576` and `9000`.
- For BGP Authentication, you can pick either `None` or `Simple` (MD5).

  If you select `Simple`, you must also provide the Authentication Key.

Deploying Infra Configuration

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

Before you begin

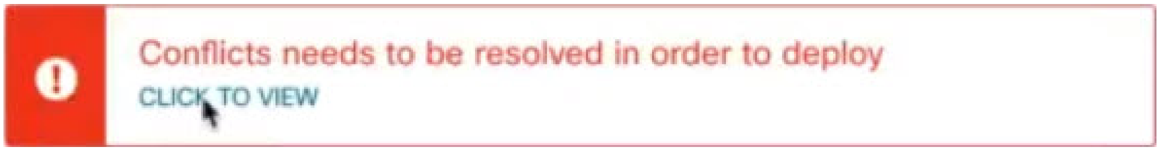
You must have the general and site-specific infra configurations completed as described in previous sections of this chapter.

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

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

In case of configuration conflicts:

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

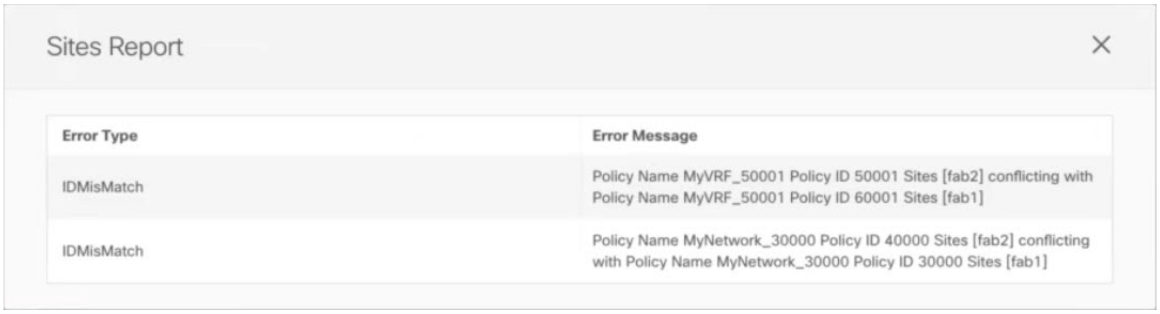


Conflicts needs to be resolved in order to deploy

CLICK TO VIEW

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 MSO, as described in Removing Sites, on page 20.

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

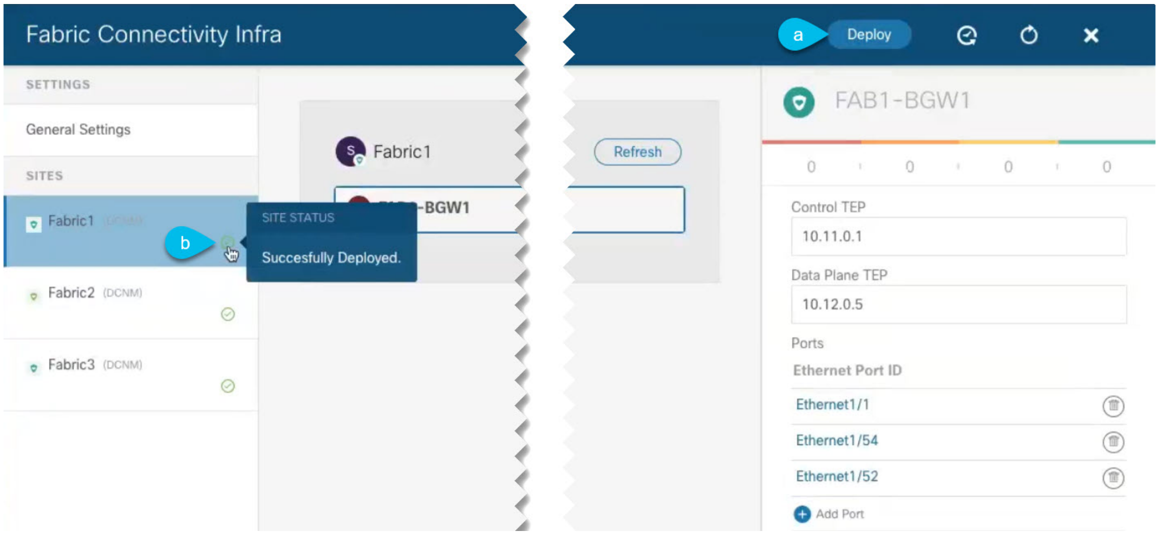
e) Resolve the existing configuration conflicts.

f) Manage the site again, as described in Adding Cisco DCNM Sites, on page 31.

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

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

Step 2 Deploy configuration.



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

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

b) Wait for configuration to be deployed.

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

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

PART III

Upgrading or Downgrading Multi-Site Orchestrator Application

CHAPTER 8

Upgrading or Downgrading MSO Application

Overview

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

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

Prerequisites and Guidelines

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

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

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

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

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

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

    - Using the Nexus Dashboard's App Store, as described in Upgrading MSO Application Using Cisco App Store, on page 46.

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

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

    - By manually uploading the new app image, as described in this section, as described in Upgrading Multi-Site Orchestrator Application Manually, on page 48.

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

- The downgrade workflow is similar to the manual upgrade process and is described in Downgrading MSO Application, on page 50.

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

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

Upgrading MSO Application Using Cisco App Store

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

Before you begin

- Ensure that you have completed the prerequisites described in Prerequisites and Guidelines, on page 45.

- Ensure that Cisco DC App Center is reachable from the Nexus Dashboard via the Management Network directly or using a proxy configuration.

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

Step 1 Log in to your Nexus Dashboard..

Step 2 From the left navigation menu, select Service Catalog.

Step 3 Upgrade the application using the App Store.

a) In the Service Catalog screen, select the App Store tab.

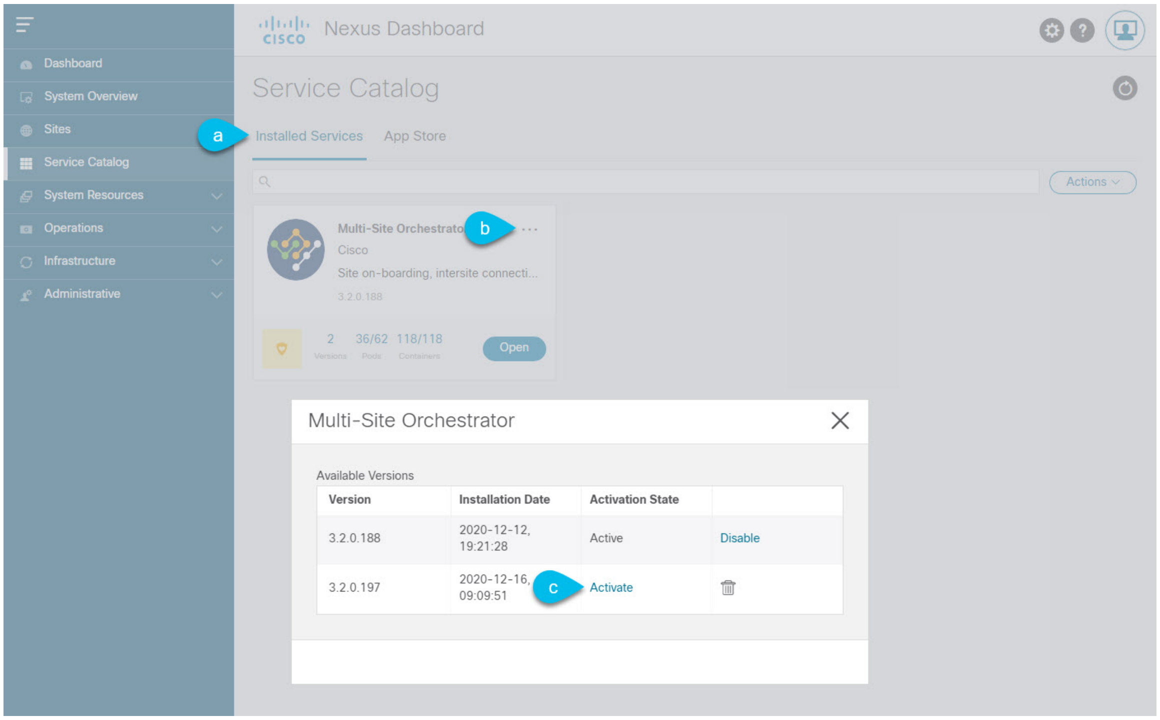
b) In the Multi-Site Orchestrator tile, click Upgrade.

c) In the License Agreement window that opens, click Agree and Download.

Step 4 Wait for the new image to initialize.

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

Step 5 Activate the new image.



Multi-Site Orchestrator

Available Versions

Version	Installation Date	Activation State	
3.2.0.188	2020-12-12, 19:21:28	Active	Disable
3.2.0.197	2020-12-16, 09:09:51	Activate	

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

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

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

Step 6 (Optional) Delete the old application image.

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

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

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

Step 7 Launch the app.

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

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

Upgrading Multi-Site Orchestrator Application Manually

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

Before you begin

- Ensure that you have completed the prerequisites described in Prerequisites and Guidelines, on page 45.

Step 1 Download the target release image.

a) Browse to the Multi-Site Orchestrator page on DC App Center:

https://dcappcenter.cisco.com/nexus-dashboard-orchestrator.html

b) From the Version drop-down, choose the version you want to install and click Download.

c) Click Agree and download to accept the license agreement and download the image.

Step 2 Log in to your Nexus Dashboard..

Step 3 Upload the image to your Nexus Dashboard.

a) From the left navigation menu, select Service Catalog.

b) In the Nexus Dashboard's Service Catalog screen, select the Installed Services tab.

c) From the Actions menu in the top right of main pane, select Upload App.

d) In the Upload App window, choose the location of the image

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

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

e) Choose the file.

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

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

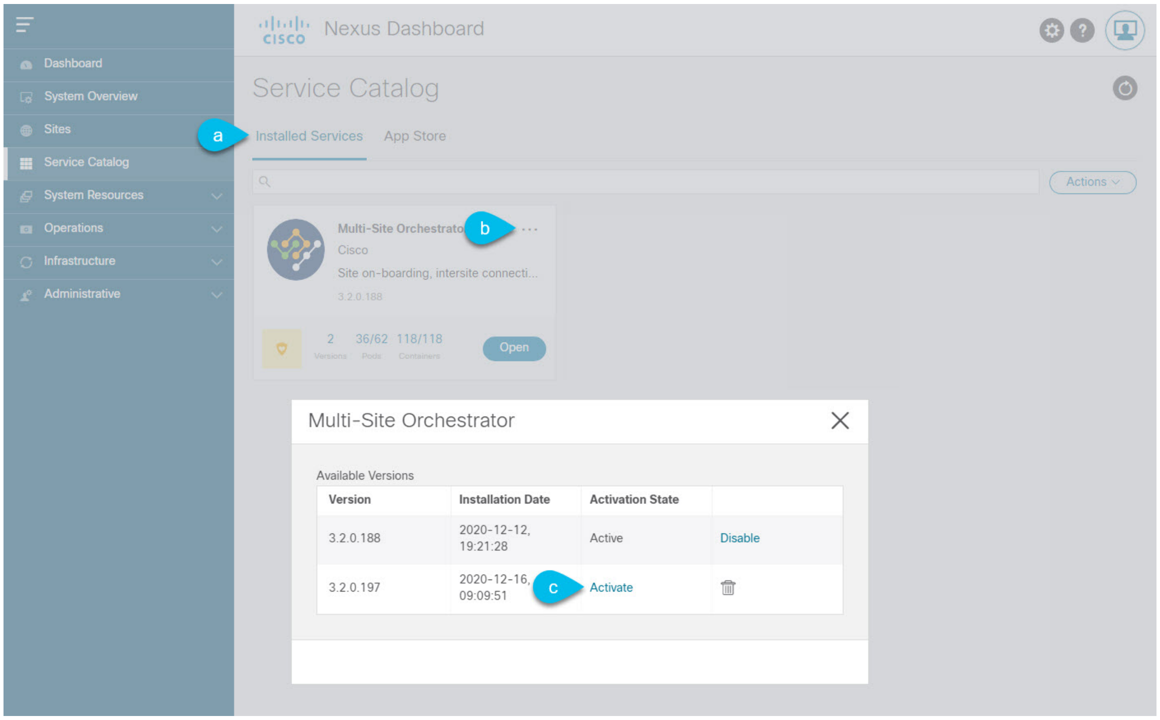
f) Click Upload to add the app to the cluster.

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

Step 4 Wait for the new image to initialize.

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

Step 5 Activate the new image.



Multi-Site Orchestrator

Available Versions

Version	Installation Date	Activation State	
3.2.0.188	2020-12-12, 19:21:28	Active	Disable
3.2.0.197	2020-12-16, 09:09:51	Activate	🗑

a) In the Service Catalog screen, select the Installed Services tab.

b) In the top right of the Multi-Site Orchestrator tile, click the menu (. . .) and choose Available Versions.

c) In the available versions window, click Activate next to the new image.

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

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

Step 6 (Optional) Delete the old application image.

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

a) In the Service Catalog screen, select the Installed Services tab.

b) In the top right of the Multi-Site Orchestrator tile, click the menu (. . .) and choose Available Versions.

c) In the available versions window, click the delete icon next to the image you want to delete.

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

Step 7 Launch the app.

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

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

Downgrading MSO Application

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

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

Before you begin

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

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

- Ensure that you have completed the prerequisites described in Prerequisites and Guidelines, on page 45

Step 1 Download the target release image.

a) Browse to the Multi-Site Orchestrator application DC App Center page: https://dcappcenter.cisco.com/multi-site-orchestrator.html.

b) From the Version dropdown, choose the version you want to install and click Download.

c) Accept the license agreement and download the image.

Step 2 Log in to your Nexus Dashboard..

Step 3 Upload the image to your Nexus Dashboard.

a) From the left navigation menu, select Service Catalog.

b) In the Nexus Dashboard's Service Catalog screen, select the Installed Services tab.

c) From the Actions menu in the top right of main pane, select Upload App.

d) In the Upload App window, choose the location of the image

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

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

e) Choose the file.

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

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

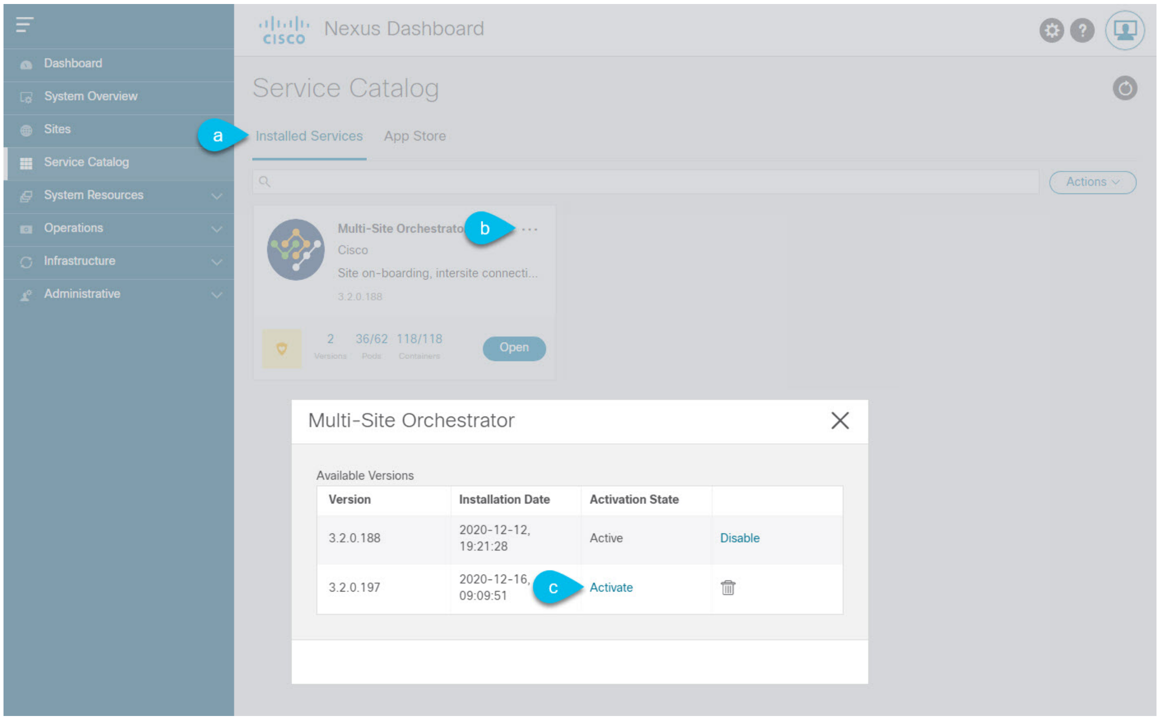
f) Click Upload to add the app to the cluster.

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

Step 4 Wait for the new image to initialize.

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

Step 5 Activate the new image.



Multi-Site Orchestrator

Available Versions

Version	Installation Date	Activation State	
3.2.0.188	2020-12-12, 19:21:28	Active	Disable
3.2.0.197	2020-12-16, 09:09:51	Activate	🗑

a) In the Service Catalog screen, select the Installed Services tab.

b) In the top right of the Multi-Site Orchestrator tile, click the menu (. . .) and choose Available Versions.

c) In the available versions window, click Activate next to the new image.

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

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

Step 6 (Optional) Delete the old application image.

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

a) In the Service Catalog screen, select the Installed Services tab.

b) In the top right of the Multi-Site Orchestrator tile, click the menu (. . .) and choose Available Versions.

c) In the available versions window, click the delete icon next to the image you want to delete.

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

Step 7 Launch the app.

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

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

CHAPTER 9

Migrating Existing Cluster to Nexus Dashboard

Migrating Existing Cluster to Nexus Dashboard

Starting with Release 3.2(1), Multi-Site Orchestrator must be deployed as an application in Cisco Nexus Dashboard. The previously supported VMware ESX virtual appliance and Cisco Application Services Engine form factors are now deprecated.

The following subsections describe how to migrate an existing Cisco Multi-Site Orchestrator that is deployed in VMware ESX VMs or Cisco Application Services Engine to the Cisco Nexus Dashboard.

If your MSO cluster is already deployed in Nexus Dashboard, follow the steps described in Overview, on page 45 instead.

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:

- 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 Multi-Site Orchestrator, on page 3 chapter of this document.
- Ensure that your current MSO cluster is healthy.

  You will use it to create a backup of your configuration, which you will then import into the newly deployed MSO application in Nexus Dashboard.
- Ensure that you have upgraded your fabrics to Cisco APIC, Release 4.2(4) or later.

Site management has moved from the MSO UI to the Nexus Dashboard common site management, which supports releases 4.2(6) or later. Fabric upgrades are described in detail in Cisco APIC Installation, Upgrade, and Downgrade Guide

- Deploy a fresh Nexus Dashboard cluster and configure fabric connectivity as described in Cisco Nexus Dashboard Deployment Guide.

  If you have an existing Application Services Engine cluster with MSO application that you plan to upgrade to Nexus Dashboard, you must first disable and uninstall the MSO application running on it. Then you can upgrade the cluster to Nexus Dashboard as described in Cisco Nexus Dashboard Deployment Guide

- Install the MSO application in your Nexus Dashboard as described in Deploying Multi-Site Orchestrator, on page 3.

  If you plan to co-host multiple applications on the same Nexus Dashboard cluster, you must ensure that the cluster size is appropriately scaled based on the fabric sizes and number of applications. The Cisco Nexus Dashboard Capacity Planning tool can provide you with the required cluster size for your specific use case. If you need to extend your cluster to support the addition of MSO application, see the Cisco Nexus Dashboard User Guide for information on deploying additional worker nodes.

- Ensure that all the sites you want to manage from your MSO application are on-boarded in the Nexus Dashboard.

  Site management has moved from the MSO UI to the Nexus Dashboard common site management. As such, you must on-board the same sites using the same names to the Nexus Dashboard GUI before migrating your existing configuration to the new cluster, as described in Adding and Deleting Sites, on page 17. If sites that exist in the backup are not present in Nexus Dashboard, the restore 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 MSO application. The sites will be enabled for management automatically when you restore your configuration from backup.

- Ensure that all remote users you had configured in MSO are added to the Nexus Dashboard.

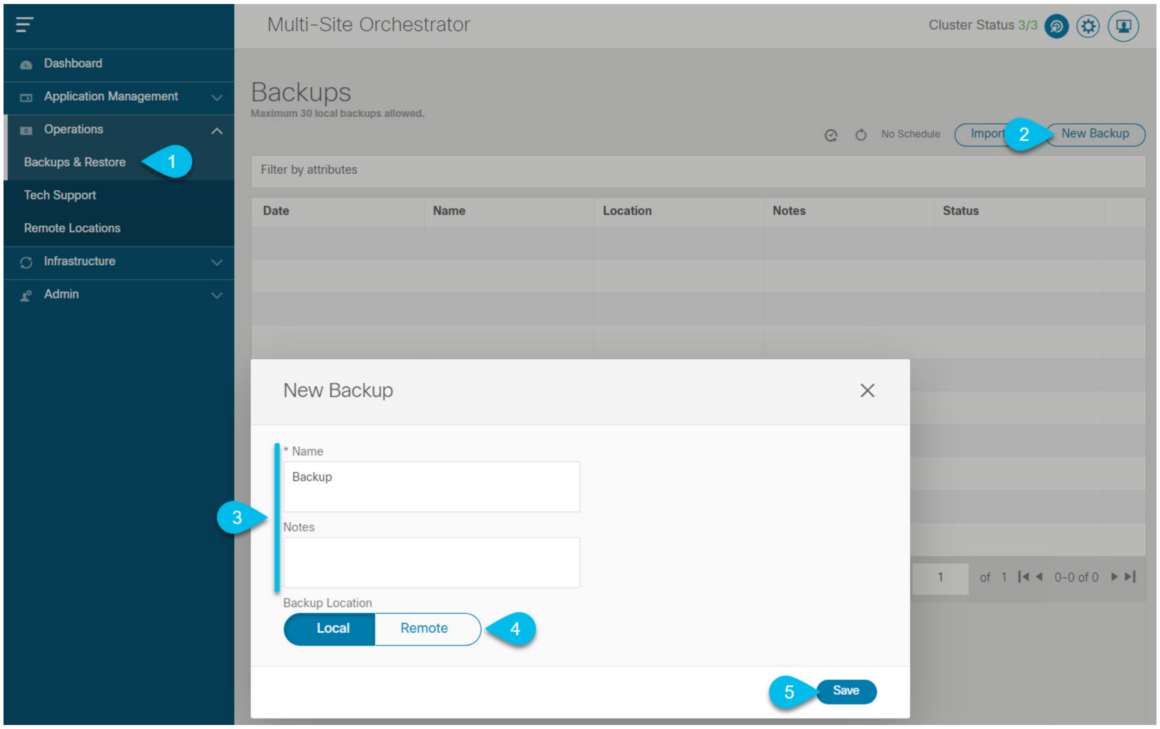
  User management has moved from the MSO UI to the Nexus Dashboard common user management. As such, you must add the same remote users and authentication servers to the Nexus Dashboard, as described in the Cisco Nexus Dashboard User Guide.

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

Back Up Existing Cluster Configuration

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

Step 1 Backup existing deployment configuration.



a) Log in to your existing Multi-Site Orchestrator.

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

c) In the main window, click New Backup.

A New Backup window opens.

d) 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 (_).

e) Choose the Backup Location.

You can save the backup file locally on the Orchestrator nodes or export it to a remote location. Note that if you choose to back up to a remote location, the remote location must already be configured in your MSO.

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

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

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

f) Click Save to create the backup.

Step 2 Copy 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.

Deploy New Cluster and Restore Configuration

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

Step 1 Disconnect the existing Multi-Site Orchestrator cluster.

We recommend preserving the existing MSO 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 MSO application is installed.

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

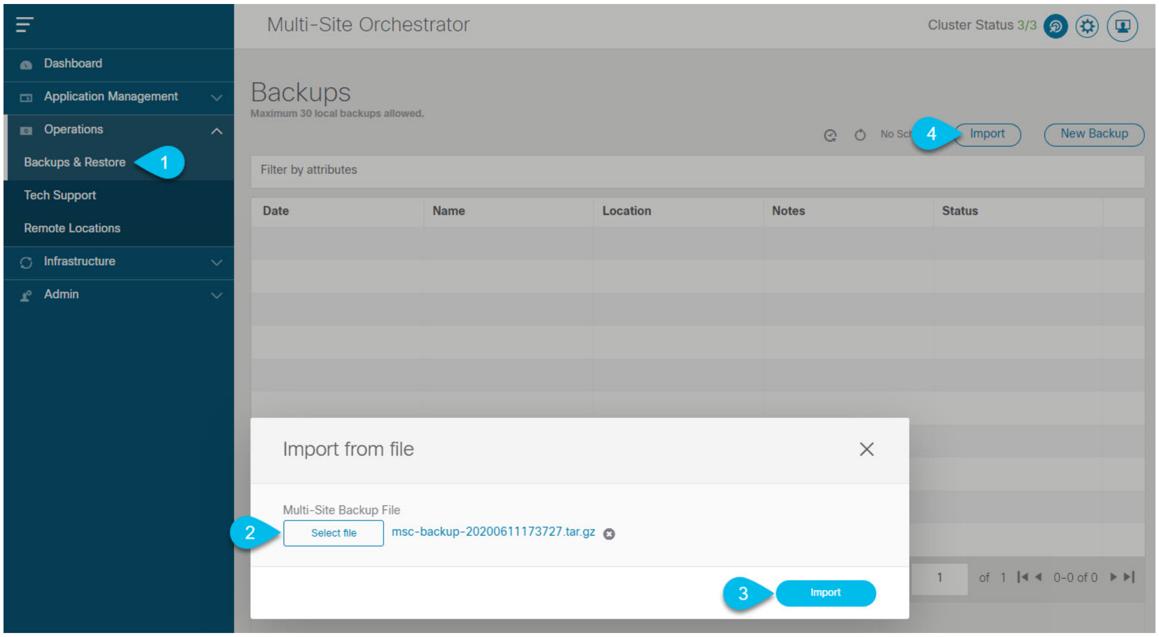
Step 3 Log in to your Nexus Dashboard GUI.

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

When you restore the backup, MSO 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. On-boarding sites is described in Adding and Deleting Sites, on page 17.

Step 5 Import the backup file to your new Orchestrator cluster deployed on the Nexus Dashboard.

If you saved the backup locally, simply import the file:



a) Open your new Multi-Site Orchestrator application.
b) From the left navigation pane, select Operations > Backups & Restore.
c) In the main window, click Import.
d) In the Import from file window that opens, click Select File and choose the backup file you want to import.

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

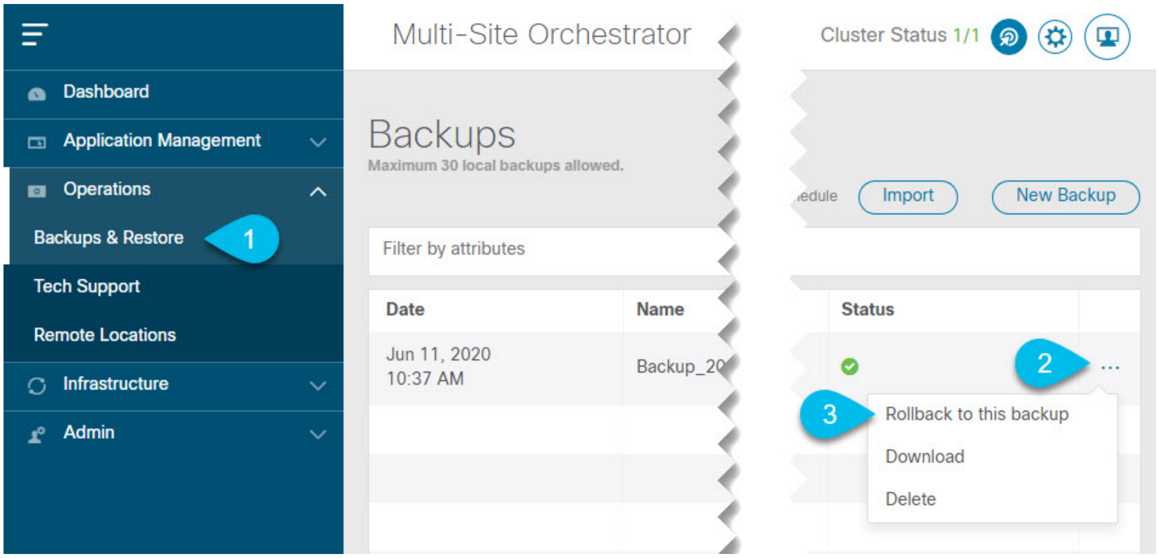
If you saved the backup to a remote location, add the remote location to the new Multi-Site Orchestrator:

a) Open your new Multi-Site Orchestrator application.
b) From the left navigation pane, select Admin > Remote Locations.
c) In the top right of the main window, click Add Remote Location.

   An Add New Remote Location screen appears.

d) Provide the same information for the remote location that you used in your old Orchestrator.
e) Click Save to add the remote server.

Step 6 Restore the configuration.



Date	Name	Status
Jun 11, 2020 10:37 AM	Backup_20	✓

a) From the left navigation menu, select Admin > Backups.
b) In the main window, click the actions (⋮) icon next to the backup you want to restore and select Rollback to this backup.
c) Click Yes to confirm that you want to restore the backup you selected.

   When the configuration is restored, any sites previously managed by MSO and on-boarded to the Nexus Dashboard will be enabled for MSO 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.

   After the configuration is imported and restored, a number of services will be restarted.