

Cisco Nexus Dashboard Insights Fabrics, Release 6.5.x - For Cisco NDFC or Standalone NX-OS

Table of Contents

New and Changed Information . . . 2
Fabrics . . . 3
- Fabrics . . . 3
- Prerequisites . . . 5
- Guidelines and Limitations . . . 6
- Add fabrics . . . 6
- Add an online NDFC fabric . . . 7
- Add an online NX-OS fabric without a controller (standalone NX-OS fabric) . . . 11
- Add a snapshot fabric . . . 16
- Fabric Details . . . 17
- Multicast Routes . . . 20
- Working with Fabrics . . . 22
- Troubleshooting telemetry configuration issues . . . 23

Copyright . . . 28

First Published: 2024-06-28

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

New and Changed Information

The following table provides an overview of the significant changes up to the current release. The table does not provide an exhaustive list of all changes or the new features up to this release.

New Features and Changed Behavior in the Cisco Nexus Dashboard Insights

Feature	Description	Release	Where Documented
Multicast routing analytics support for VXLAN fabrics	You can now use multicast routing analytics with VXLAN fabrics.	6.5.1	Guidelines and limitations for multicast routes
Out-of-band management connection support for telemetry streaming	When you add a fabric, you can now use an out-of-band management connection support for telemetry streaming. In previous releases, you could only use in-band management.	6.5.1	Fabric connection types
Terminology change	The term " sites" is renamed to " fabrics" .	6.5.1	Entire document

This document is available from your Cisco Nexus Dashboard Insights GUI as well as online at www.cisco.com. For the latest version of this document, visit Cisco Nexus Dashboard Insights Documentation.

Fabrics

Fabrics

Fabrics are on-premises network regions that consist of a group of switches and other networking devices that provide connectivity for your applications and endpoints. You can split fabrics into different availability zones, such as pods, that are analyzed and managed by Nexus Dashboard Insights.

Types of on-premises fabrics

- Online fabrics: Multiple Nexus switches running ACI or NX-OS that can be represented by a controller such as Cisco APIC or NDFC and connected to Nexus Dashboard Insights to continuously stream telemetry. Types of online fabrics include:
  - ACI: Multiple Nexus switches with Cisco ACI and represented by a Cisco APIC.
  - NDFC: Multiple Nexus switches with Cisco NX-OS and represented by a Cisco NDFC.
  - NX-OS: A group of Cisco Nexus 9000 switches running NX-OS without a controller.
- Snapshot fabrics: Controller-based fabrics, that are referenced by a snapshot, for use in one-time analysis or demonstrations. They may or may not be connected to Nexus Dashboard Insights over the network.

To learn about how to prepare fabrics for onboarding, see Add fabrics.

An NDFC fabric comprises a fabric running NX-OS that is either fully managed or only monitored by NDFC. All of the switches in the fabric can be analyzed as a part of the fabric. With a NX-OS based fabric, the fabric could be a NDFC managed fabric or it could be configured using other means such as CLI, Ansible, or any other configuration automation mechanism. For fabrics not using NDFC for configuration management, NDFC must be installed and the fabric must be discovered in read-only or monitor mode. Nexus Dashboard Insights uses NDFC for topology discovery and to identify the role of the switch in the fabric.

An NX-OS fabric comprises Nexus 9000 switches that run NX-OS without a controller and is connected to Nexus Dashboard.

Once your fabric is onboarded and fully prepared, Nexus Dashboard Insights will start the fabric analysis to collect data from your fabric and display the fabric information in the **Fabrics** page. See Fabric Details. From there, you can view your fabric's general information, inventory, L2 and L3 connectivity, endpoints, anomalies and advisories and more! To learn more see Fabric Details.

Fabric connection types

When you add a fabric, you can use either an in-band management or out-of-band management connection for telemetry streaming. You specify the connection type in the GUI with the **Telemetry Streaming Network** property.

With out-of-band management, NDFC and standalone NX-OS fabrics use the out-of-band management IP addresses of the switches.

Advantages of in-band management

In-band management supports Flow Telemetry and increased bandwidth for telemetry streaming.

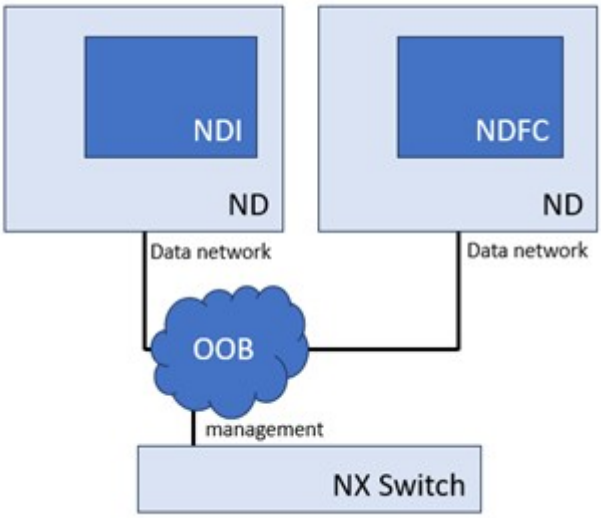
Advantages of out-of-band management

Most fabrics already have out-of-band management set up. In such a case, using this connection type does not require any additional connection configuration.

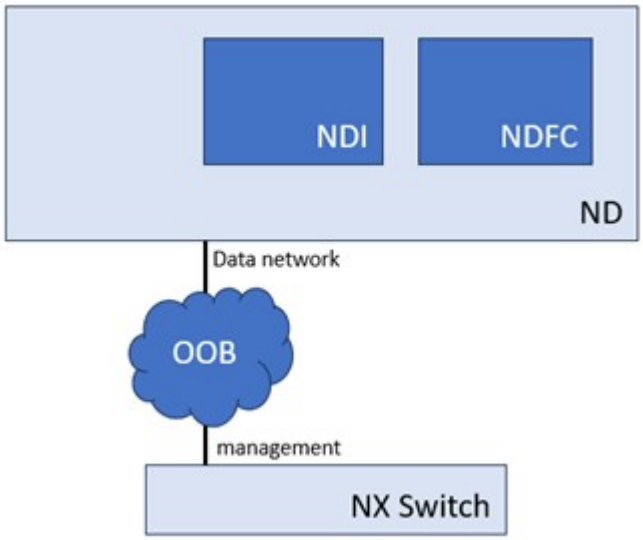
Supported out-of-band management fabric topologies

Nexus Dashboard Insights supports these out-of-band management fabric topologies:

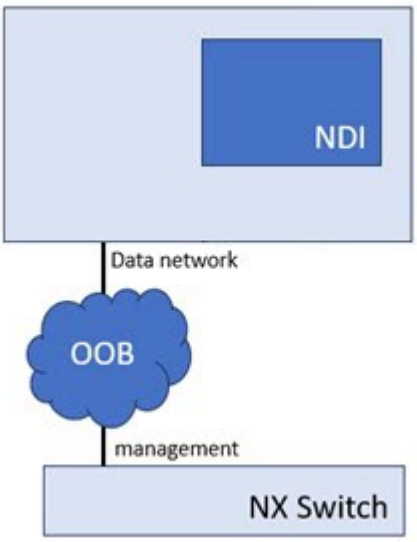
- Nexus Dashboard Insights is in a different cluster than NDFC



- Nexus Dashboard Insights is in the same cluster as NDFC



- Nexus Dashboard Insights is in a standalone NX-OS fabric



Guidelines and limitations for the connection types

Observe these guidelines and limitations for the connection types:

- You can set the connection type only when you add the fabric. You cannot change the type after you added the fabric. To change the connection type, you must remove the fabric then re-add it.
- For out-of-band management, the Nexus Dashboard Insights data network must have reachability to the management addresses of the switches.
- Out-of-band management is not supported with Flow Telemetry.
- If you use out-of-band management with Traffic Analytics, flow troubleshooting is disabled.

Prerequisites

- You have configured DNS on the fabric.
- You have configured NTP on the fabric.
- You have configured PTP on the fabric.
- For in-band management, configure the Nexus switch in-band port address on the loopback interface and the address should be reachable to the Nexus Dashboard data network. For out-of-band management, this is optional.
- For out-of-band management, the Nexus Dashboard Insights data network must have reachability to the management addresses of the switches.
- If the switches are controlled by NDFC and they are discovered using the out-of-band management interface, then the Nexus Dashboard data interface should have routed connectivity to those switches.
- You have configured Fabric connectivity in Cisco Nexus Dashboard's Admin Console. See Cisco Nexus Dashboard Platform Overview.
- You have the supported software version for your fabric. See Nexus Dashboard and Services Compatibility Matrix.
- For snapshot fabrics, you have Python3 installed on your system.
- To onboard an NX-OS fabric without a controller:

    - You must enable NX-OS Discovery in Nexus Dashboard.
    - You must enable CDP or LLDP in Nexus switches.
- You must enable the NX-API feature on all Cisco NX-OS switches at the CLI prompt before onboarding the fabric in Nexus Dashboard Insights by using the following command:

```
switch(config)# feature nxapi
```

Guidelines and Limitations

- You cannot onboard a Cisco NDFC fabric with remote authentication using the **Manually Add** option in Nexus Dashboard Insights. You must first add the NDFC fabric with remote authentication in Nexus Dashboard's Admin Console. You can then onboard the NDFC fabric using the **Ready to Add** option in NDI.
- Switch name or Host name should be unique across all the fabrics discovered in Nexus Dashboard Insights.
- SVI interfaces are not displayed for Cisco NX-OS switches.
- Connectivity Analysis is not supported with externally-onboarded NDFC fabrics.

Guidelines and Limitations for NX-OS Fabrics without a Controller (Standalone NX-OS Fabrics)

- Interface flow rules in the context of Flow Telemetry are not supported.
- Onboarding a snapshot fabric is not supported.
- Onboarding NX-OS fabrics without a controller is supported on Cisco NX-OS release 9.3(10) and later.
- Onboarding an online NX-OS fabric without a controller is only supported on a physical Nexus Dashboard cluster. Onboarding an online NX-OS fabric without a controller is not supported on a virtual Nexus Dashboard cluster.
- Only Nexus Dashboard Insights deployment mode is supported to onboard NX-OS Standalone fabrics. The following deployment modes are not supported and you cannot enable NX-OS discovery for onboarding NX-OS Standalone fabrics:
    - Nexus Dashboard Insights and NDFC
    - Nexus Dashboard Insights and Nexus Dashboard Orchestrator
- Onboarding NX-OS fabrics without a controller is supported only on the Cisco Nexus 9000 product families.
- Both default and non-default VRF instances are supported. The VRF instance should be used for non-tenant purposes and should not be associated with tenant traffic. The VRF instance need to be part of underlay and not overlay.

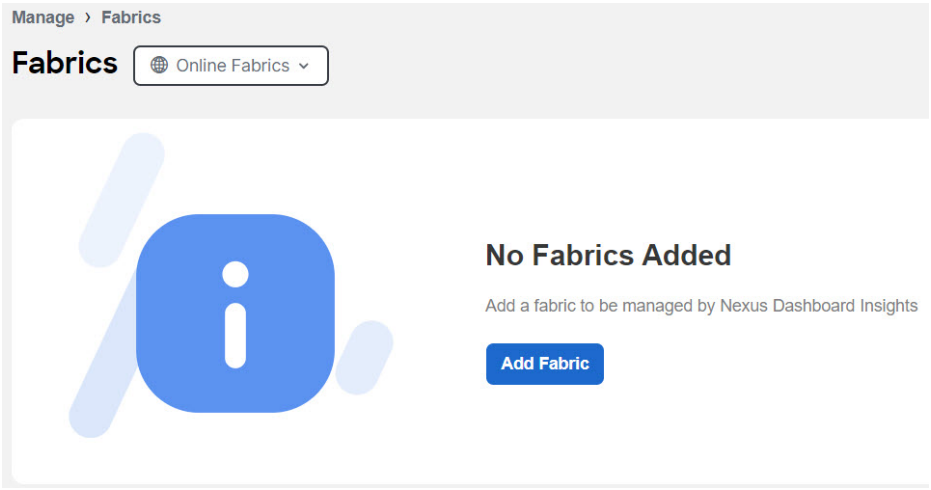
Add fabrics

You can add a fabric to Nexus Dashboard Insights using the following methods:

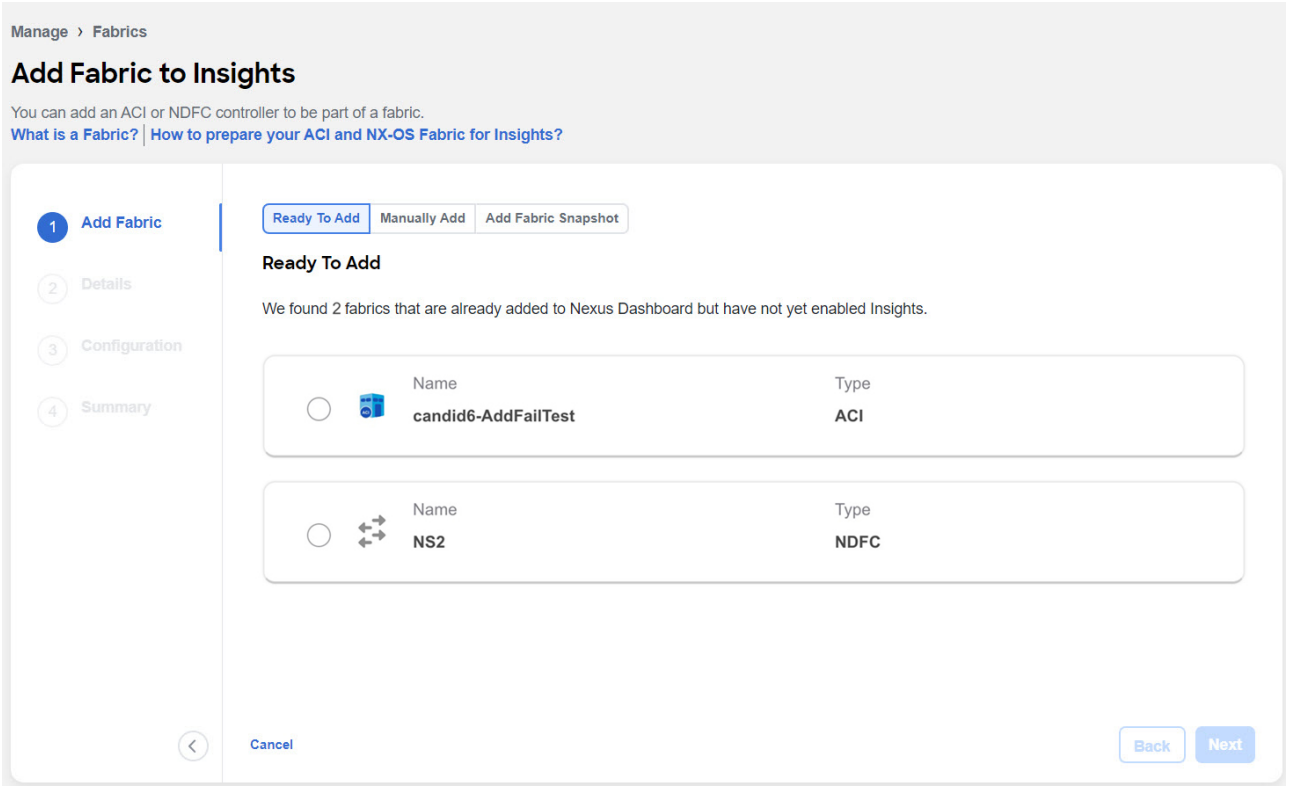
- Online fabrics
  - Enable the fabric that has already been added to Nexus Dashboard. Fabrics added to the Nexus Dashboard are not enabled in the services by default, so you will need to explicitly enable them directly from Nexus Dashboard Insights.
  - Add a fabric directly to Nexus Dashboard Insights.
- Snapshot fabrics
  - Add a snapshot fabric.

Add an online NDFC fabric

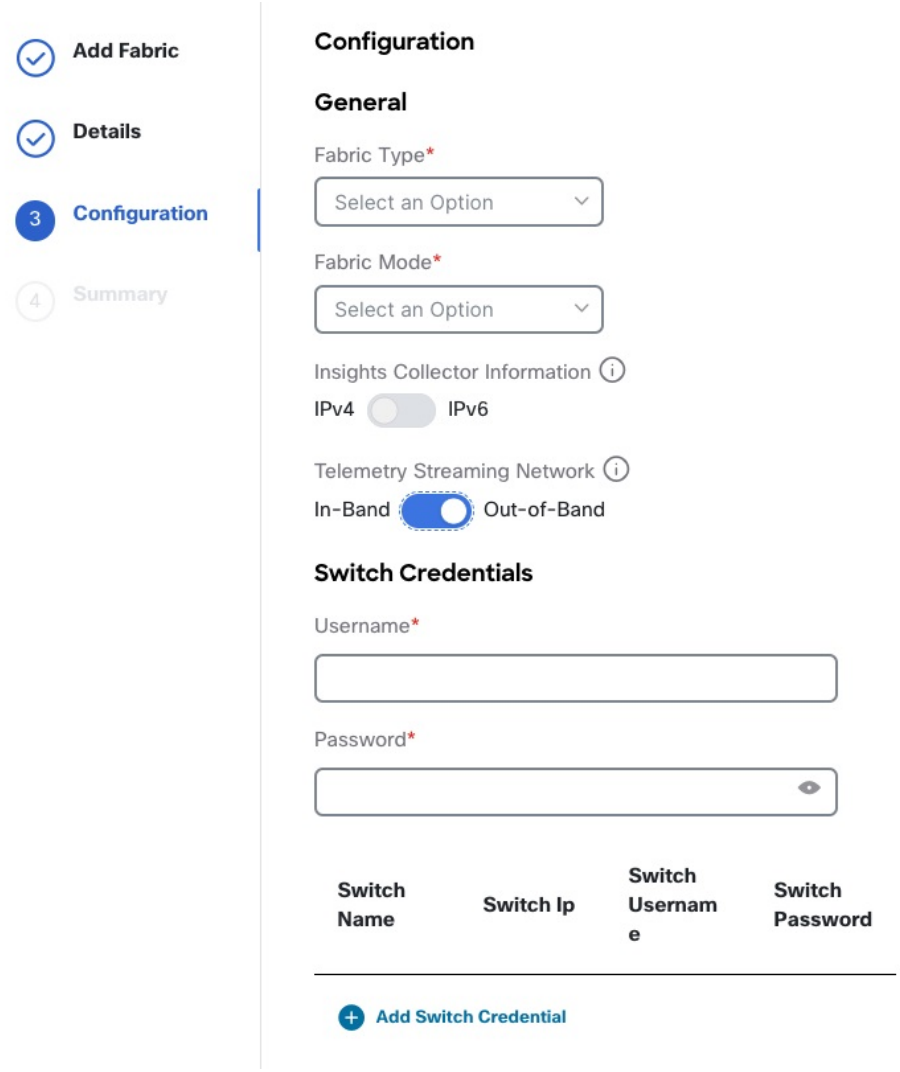
1. Navigate to **Manage** > **Fabrics**.
2. Click **Add Fabric**.
   a. If you are adding a fabric in Nexus Dashboard Insights for the very first time, you will receive the following message. Click **Add Fabric** to proceed.



3. To enable a fabric that has been already added to Nexus Dashboard, choose **Ready to Add**. The fabrics added to Nexus Dashboard are displayed. To add a fabric to Nexus Dashboard, see Cisco Nexus Dashboard Fabrics Management.



4. Complete the following fields for **Ready to Add**.
    a. Choose the NDFC fabric.
    b. Click **Next**.
    c. Click **See on map** and click the fabric location on the map to identify the fabric in the Admin Console.
    d. Click **Next**.



e. In the **User Name** and **Password** field for Switch Credentials, provide the login credentials for a LAN user with admin privileges on the switch you are adding.

f. For **Insights Collector Configuration**, use the toggle to choose IPv4 or IPv6 to onboard the fabric. Based on this setting, Nexus Dashboard Insights will configure its collector to receive telemetry from this fabric. This setting should match your fabrics IP address configuration.

g. For **Telemetry Streaming Network**, use the toggle to choose in-band management or out-of-band management.

h. For in-band management, in the **VRF** field, enter the VRF instance instance name associated with the loopback interfaces. This is the VRF instance instance that provides connectivity to the Nexus Dashboard in-band IP addresses.

> Both default and non-default VRF instances are supported. The VRF instance should be used for non-tenant purposes and should not be associated with tenant traffic.

i. For in-band management, in the **Loopback** field, enter the loopback configured on the switches that provide connectivity to the Nexus Dashboard in-band IP address.

j. Click **Add Switch Credentials** to add switches to the list and specify their credentials only if the switch credentials do not match the default credentials provided above.

   i. In the **Switch Name** field, enter the name for the switch.

ii. In the **Switch IP** field, enter the IP address for the switch.

iii. In the **Switch Username** field, enter the username for the switch.

iv. In the **Switch Password** field, enter the password.

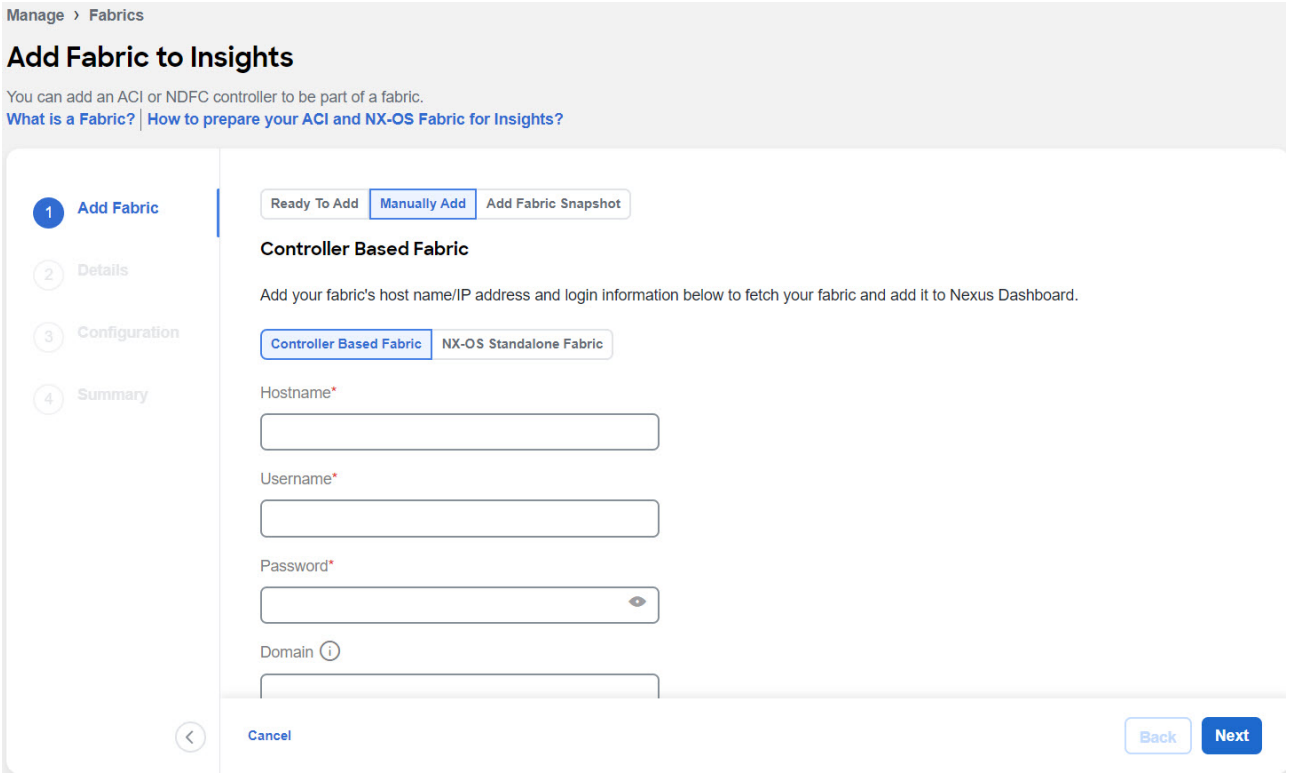
k. Check the check mark to complete to add your entries, and add additional switches as appropriate.

l. Click **Next**.

m. Verify the configuration.

n. Click **Save**.

5. To add a fabric to Nexus Dashboard and then enable the fabric using Nexus Dashboard Insights, choose **Manually Add**.



6. Complete the following fields for **Manually Add**.

a. Choose **Controller Based Fabric**.

b. In the **Hostname** field, enter the IP address used to communicate with the fabric's controller.

c. In the **User Name** and **Password** field, provide the login credentials for a user with admin privileges on the fabric you are adding.

d. In the **Domain** field, enter the controller login domain name.

e. Click **Next**.

f. Enter the fabric name to identify the fabric on Nexus Dashboard.

g. Choose the fabric location from the map to identify the fabric on Nexus Dashboard.

h. Click **Next**.

i. From the **Fabric Type** drop-down list, choose the fabric type. The options are **Classic** or **VXLAN**. Enhanced Classic LAN is not supported for NDFC fabrics.

j. From the **Fabric Mode** drop-down menu, choose the fabric mode. The options are **Managed**

or **Monitored**. In Managed mode, Nexus Dashboard Insights will deploy telemetry configuration to all switches in the fabric. In monitored mode, Nexus Dashboard Insights will not deploy telemetry configuration to all switches in the fabric.

k. For **Insights Collector Configuration**, use the toggle to choose IPv4 or IPv6 to onboard the fabric. Based on this setting, Nexus Dashboard Insights will configure its collector to receive telemetry from this fabric. This setting should match your fabrics IP address configuration.

l. In the **Loopback** field, enter the loopback configured on the switches that provide connectivity to the Nexus Dashboard in-band IP address.

m. In the **VRF** field, enter the VRF instance instance name associated with the loopback interfaces. This is the VRF instance instance that provides connectivity to the Nexus Dashboard in-band IP addresses.



Both default and non-default VRF instances are supported. The VRF instance should be used for non-tenant purposes and should not be associated with tenant traffic.

n. In the **User Name** and **Password** field for Switch Credentials, provide the login credentials for a LAN user with admin privileges on the switch you are adding.

o. Click **Add Switch Credentials** to add switches to the list and specify their credentials only if the switch credentials do not match the default credentials provided above.

   i. In the **Switch Name** field, enter the name for the switch.

   ii. In the **Switch IP** field, enter the IP address for the switch.

   iii. In the **Switch Username** field, enter the username for the switch.

   iv. In the **Switch Password** field, enter the password.

p. Check the check mark to complete to add your entries, and add additional switches as appropriate.

q. Click **Next**.

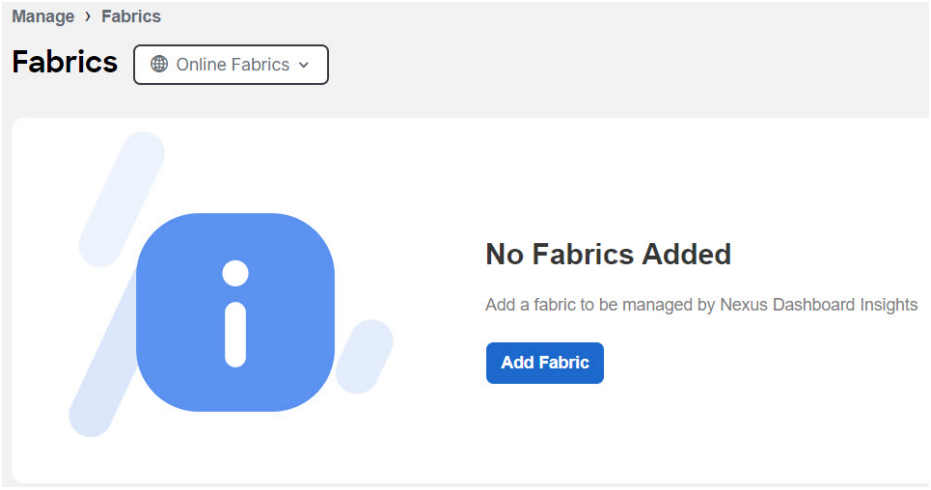
r. Verify the configuration.

s. Click **Submit**.

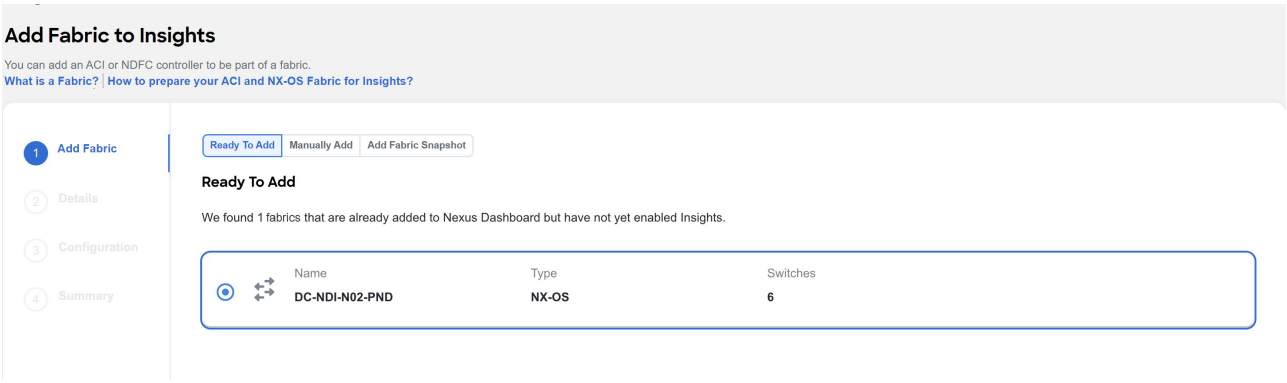
Add an online NX-OS fabric without a controller (standalone NX-OS fabric)

1. Navigate to **Manage** > **Fabrics**.
2. Click **Add Fabric**.

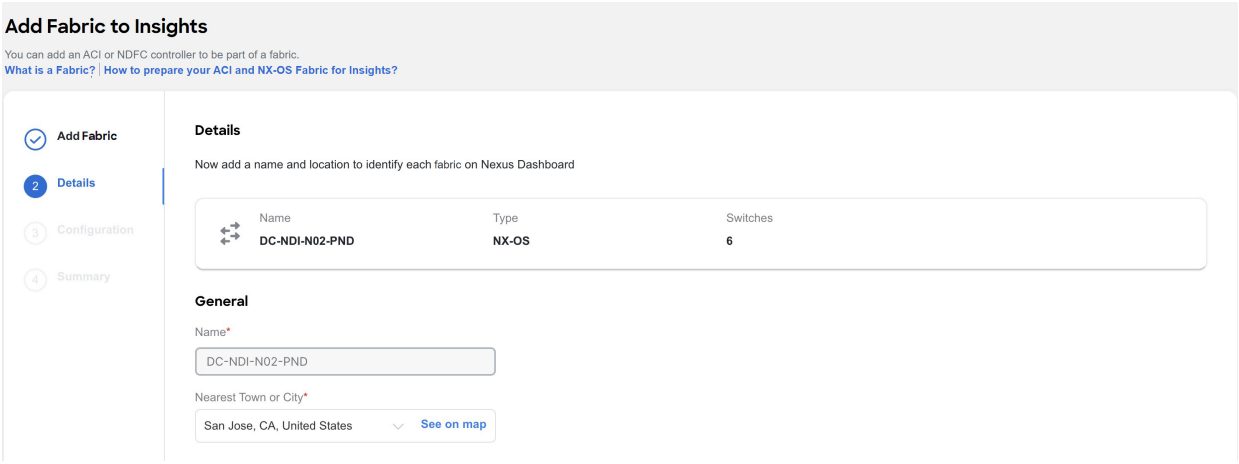
   a. If you are adding a fabric in Nexus Dashboard Insights for the very first time, you will receive the following message. Click **Add Fabric** to proceed.



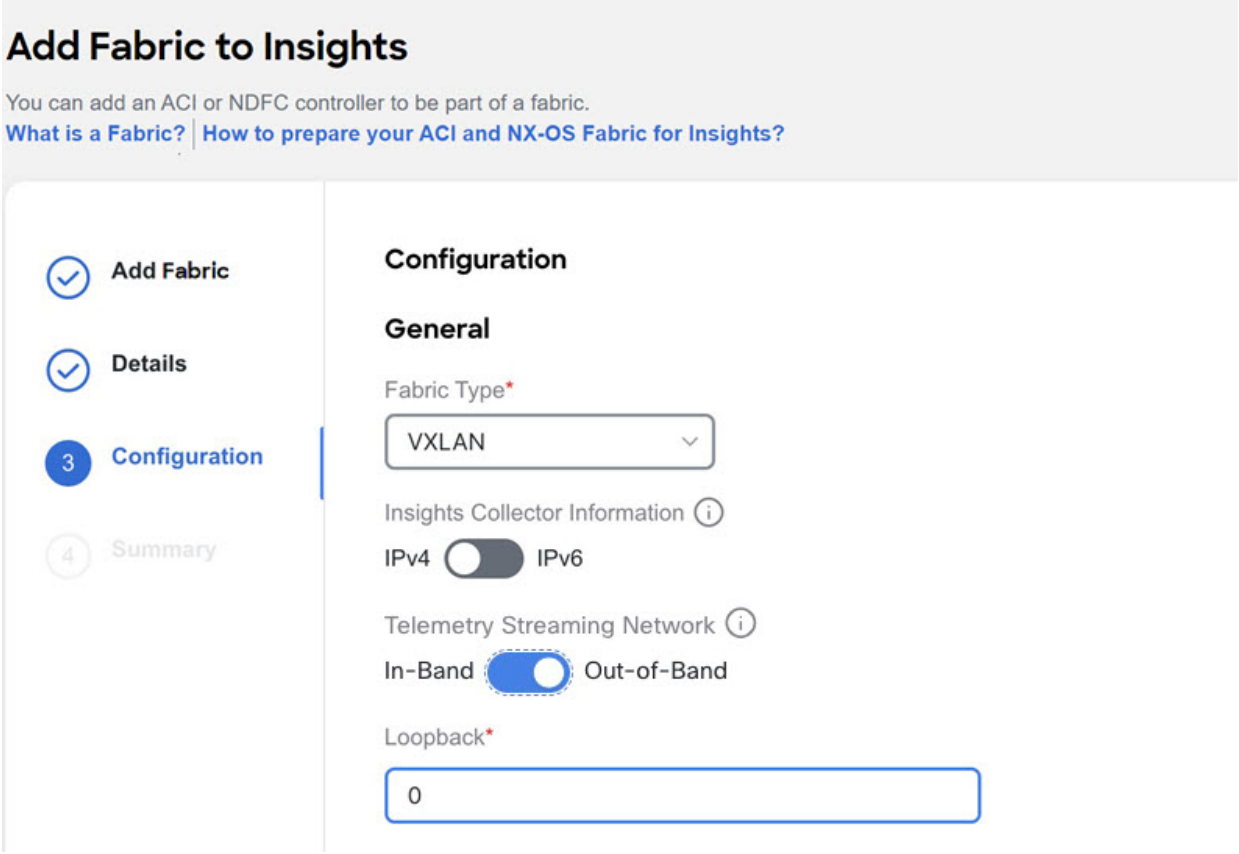
3. To enable a fabric that has been already added to Nexus Dashboard, choose **Ready to Add**. The fabrics added to Nexus Dashboard are displayed. To add a fabric to Nexus Dashboard, see Cisco Nexus Dashboard Fabrics Management.
4. Complete the following fields for **Ready to Add**.



a. Choose the NX-OS fabric.
b. Click **Next**.
c. Choose the fabric location from the map to identify the fabric on Nexus Dashboard.



d. Click **Next**.



e. From the **Fabric Type** drop-down menu, choose the fabric type. The options are **Classic** or **VXLAN**.

f. For **Insights Collector Configuration**, use the toggle to choose IPv4 or IPv6 to onboard the fabric. Based on this setting, Nexus Dashboard Insights will configure its collector to receive telemetry from this fabric. This setting should match your fabrics IP address configuration.

g. For **Telemetry Streaming Network**, use the toggle to choose in-band management or out-of-band management.

h. For in-band management, in the **VRF** field, enter the VRF instance instance name associated with the loopback interfaces. This is the VRF instance instance that provides connectivity to the Nexus Dashboard in-band IP addresses.

> Both default and non-default VRF instances are supported. The VRF instance should be used for non-tenant purposes and should not be associated with tenant traffic.

i. For in-band management, in the **Loopback** field, enter the loopback configured on the switches that provide connectivity to the Nexus Dashboard in-band IP address.

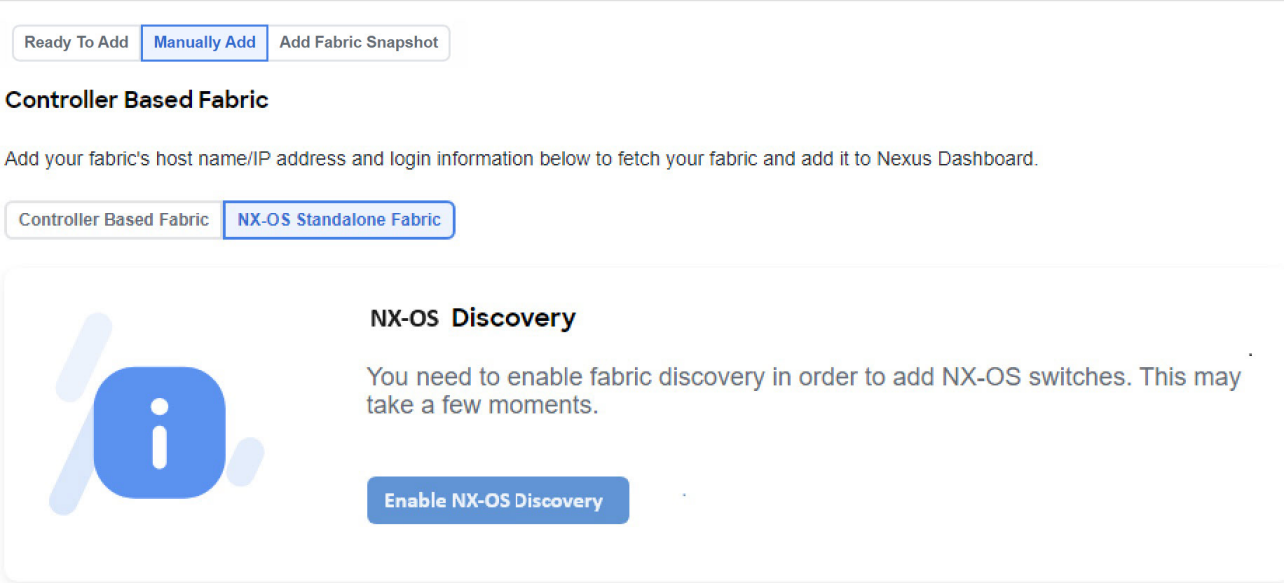
j. Click **Next**.

k. Verify the configuration.

l. Click **Submit**.

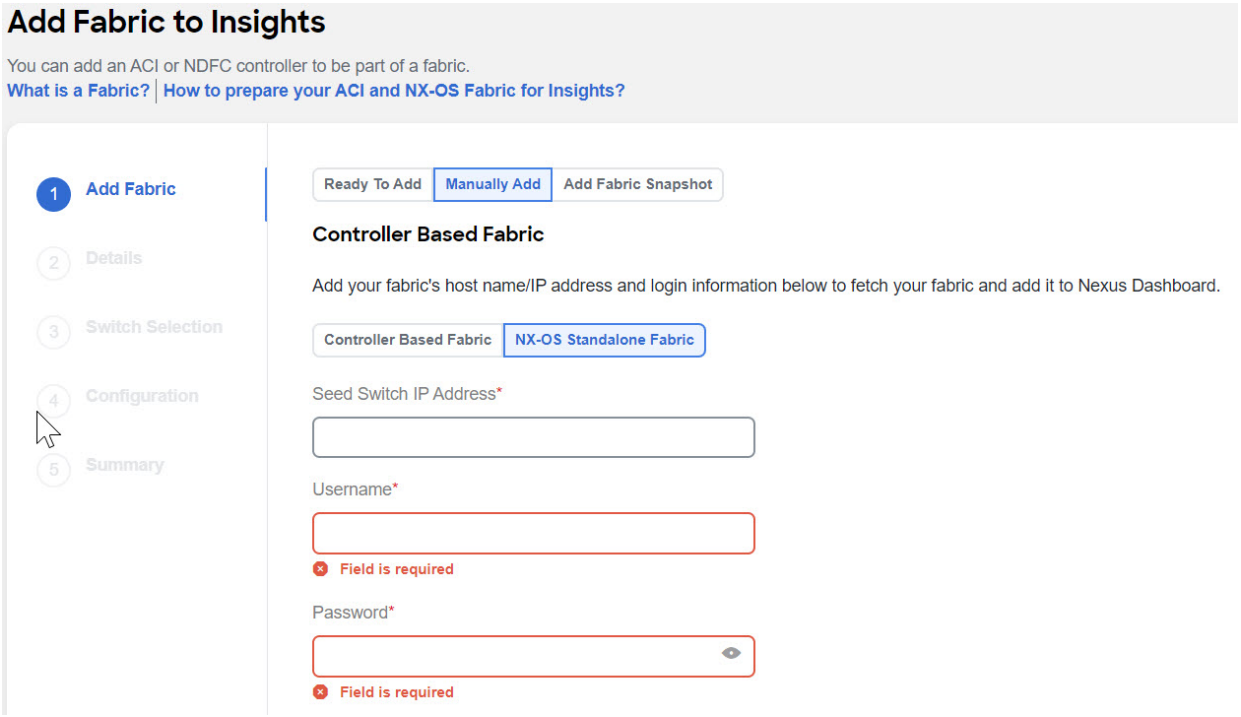
5. To add a fabric to Nexus Dashboard and then enable the fabric using Nexus Dashboard Insights, choose **Manually Add**.

6. Complete the following fields for **Manually Add**.



a. Choose **NX-OS Standalone Fabric**.

b. Click **Enable NX-OS Discovery** to enable NX-OS Discovery in Nexus Dashboard's Admin Console.

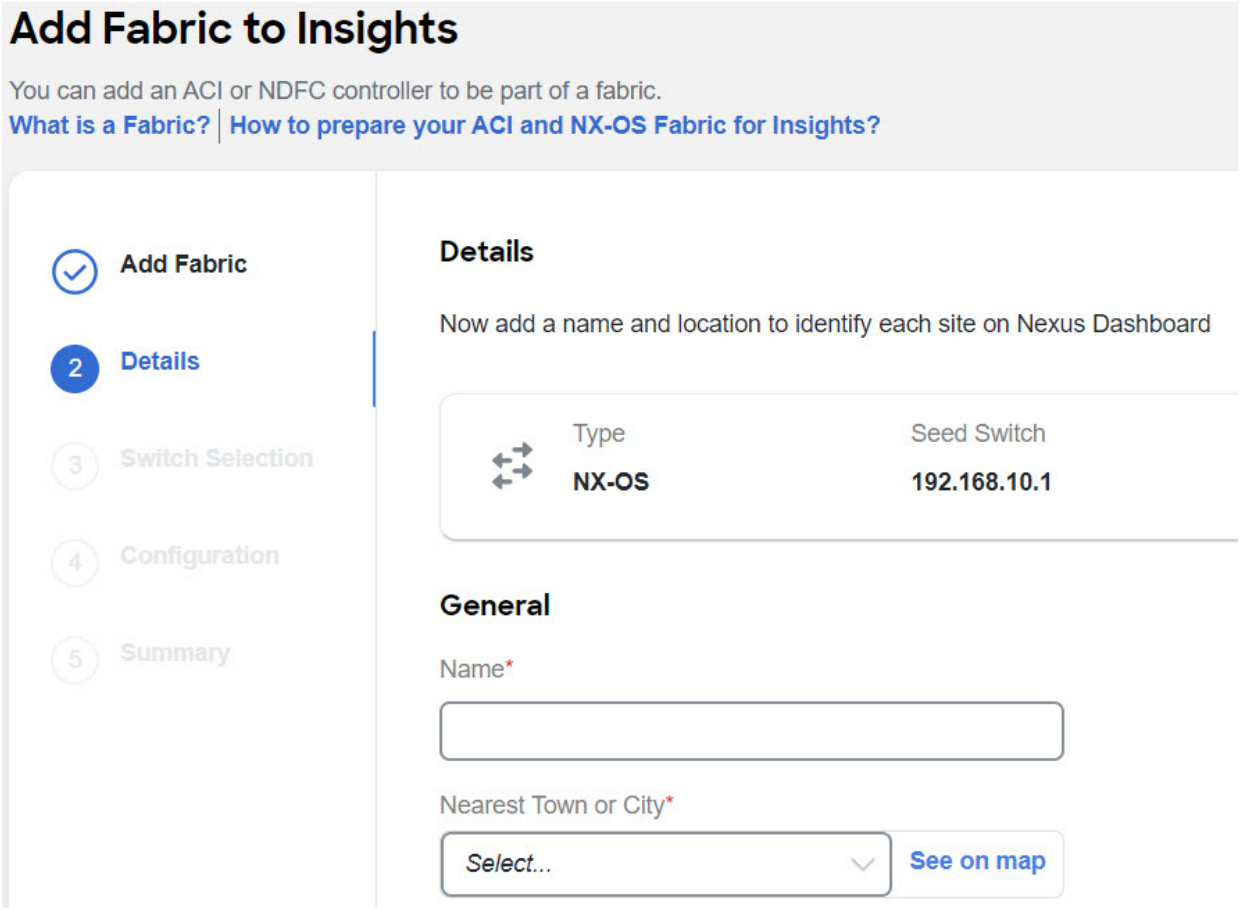


c. In the **Seed Switch IP Address** field, enter the IP address of the seed switch management interface.

d. In the **User Name** and **Password** field, provide the login credentials for a user with admin privileges on the switch you are adding.

e. From the **Authentication Protocol** drop-down list, choose the protocol.

f. Click **Next**.

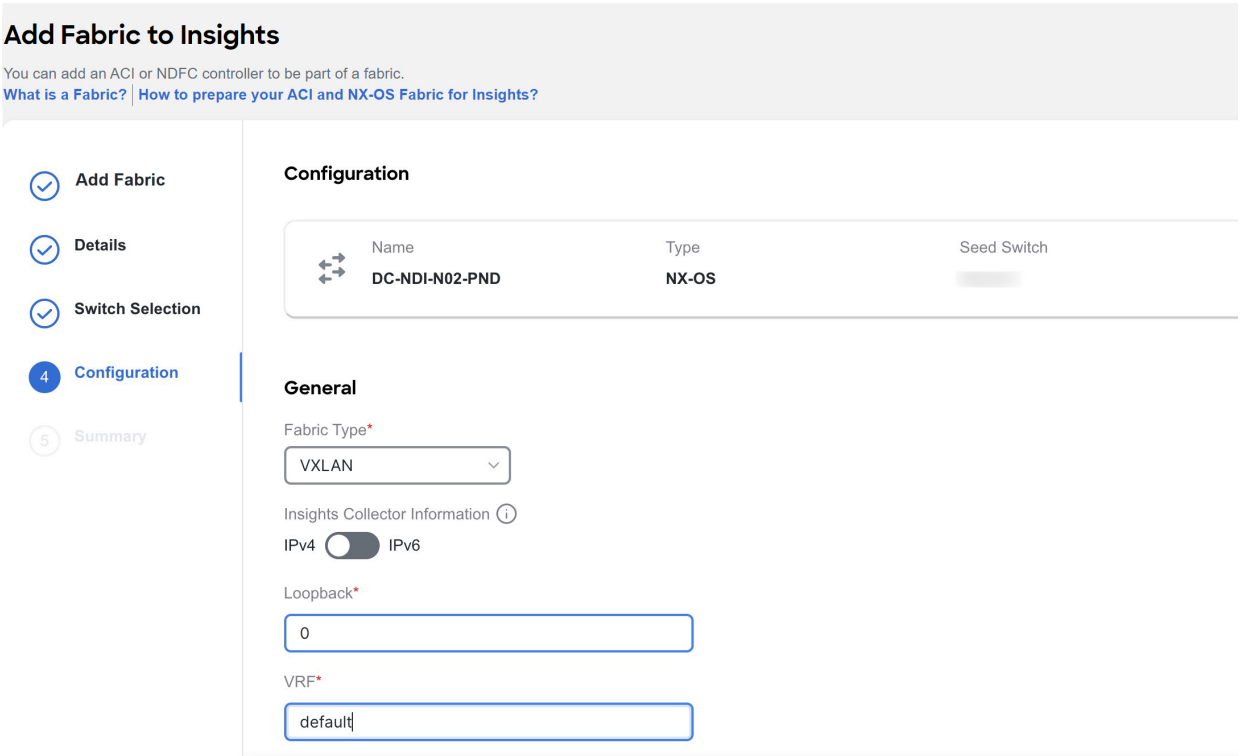


g. Enter the NX-OS fabric name to identify the fabric on Nexus Dashboard.

h. Choose the NX-OS fabric location from the map to identify the fabric on Nexus Dashboard.

i. Choose the switches to be added to the fabric.

j. Click **Next**.



k. From the **Fabric Type** drop-down menu, choose the fabric type. The options are **Classic** or

VXLAN.

l. For **Insights Collector Configuration**, use the toggle to choose IPv4 or IPv6 to onboard the fabric. Based on this setting, Nexus Dashboard Insights will configure its collector to receive telemetry from this fabric. This setting should match your fabrics IP address configuration.

m. In the **Loopback** field, enter the loopback configured on the switches that provide connectivity to the Nexus Dashboard in-band IP address.

n. In the **VRF** field, enter the VRF instance name associated with the loopback interfaces. This is the VRF instance that provides connectivity to the Nexus Dashboard in-band IP addresses.



Both default and non-default VRF instances are supported. The VRF instance should be used for non-tenant purposes and should not be associated with tenant traffic.

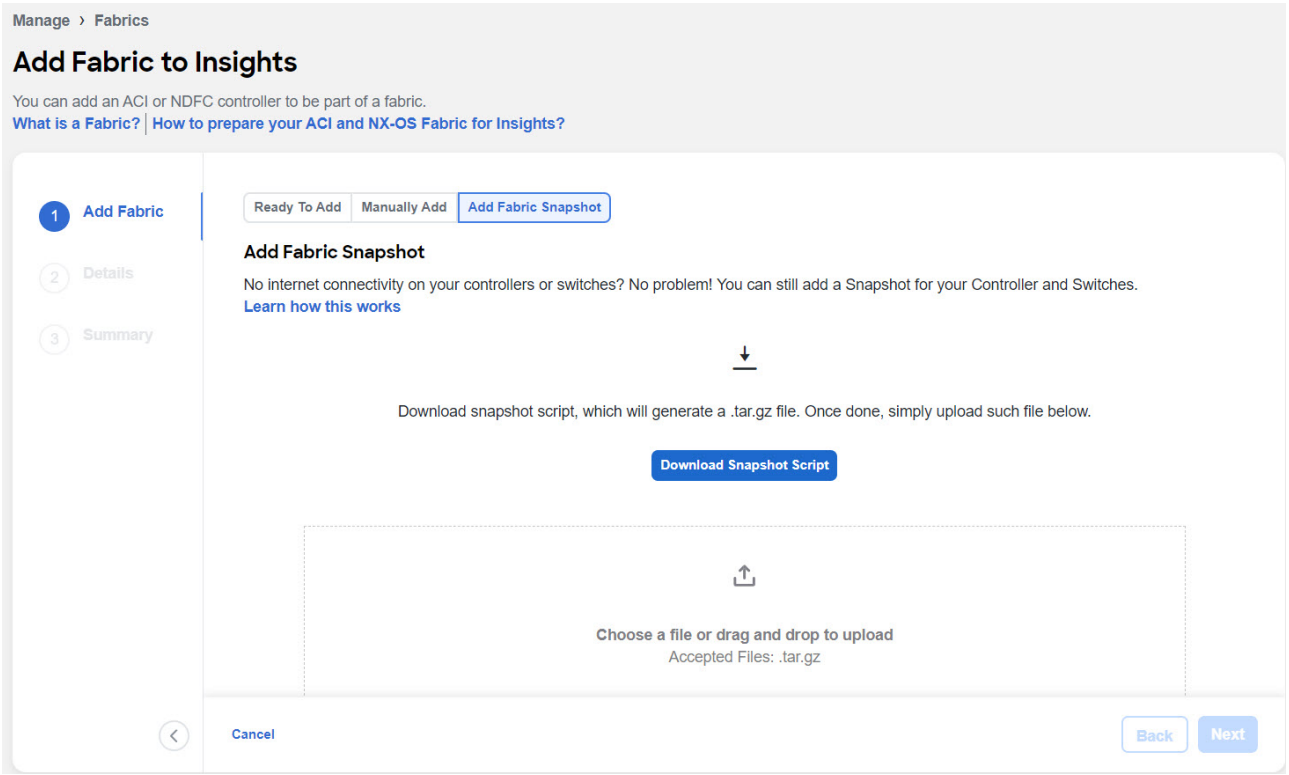
o. Click **Next**.

p. Verify the configuration.

q. Click **Submit**.

Add a snapshot fabric

1. Navigate to **Manage** > **Fabrics**.
2. Click **Add Fabric**.
3. To add a snapshot fabric, choose **Add Fabric Snapshot**.

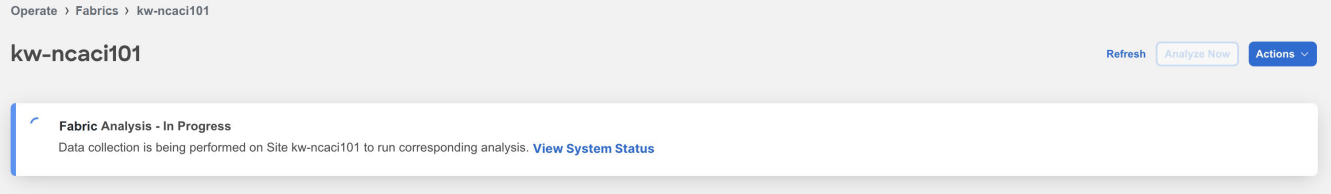


4. Click **Download Snapshot Script** to download the data-collectors.tar.gz to your machine.
5. Extract the file you downloaded and run the data collection script. Follow the instructions provided in the readme.md file. After the script is completed successfully, the data is collected in a <filename>.tar.gz file.

The collection script requires that you have Python3 installed on your system.

6. Upload the file in Nexus Dashboard Insights and click **Next**.
7. Enter the fabric name to identify the fabric on Nexus Dashboard.
8. Choose the fabric location from the map to identify the fabric on Nexus Dashboard.
9. Click **Next**.
10. Verify the configuration.
11. Click **Submit**.

After your fabric is onboarded and fully prepared, Nexus Dashboard Insights will start the analysis to collect data from your fabric and display the fabric information in the **Fabrics** page. See Fabric Details. The Fabric Analysis banner displays the progress of the analysis. The time to run the analysis depends on the size of the fabric.



Fabric Details

In Nexus Dashboard Insights, **Global View** provides bird's eye view of your global network infrastructure for all your fabrics. The Fabrics page provides the details for an individual fabric.

Fabric Details in Global View

After you add the first fabric, **Global View** gives you a bird's eye view of your global network infrastructure for all your fabrics, their locations, and the key health metrics.

Navigate to **Overview** > **Global View**.

The map visually shows the physical location and total number of your fabrics in each continent, and their names. Click a fabric to jump directly to the details for that fabric, or scroll down to the Fabrics area to navigate to your fabric. You can also use the the zoom control icons in the page to change your view of the map.

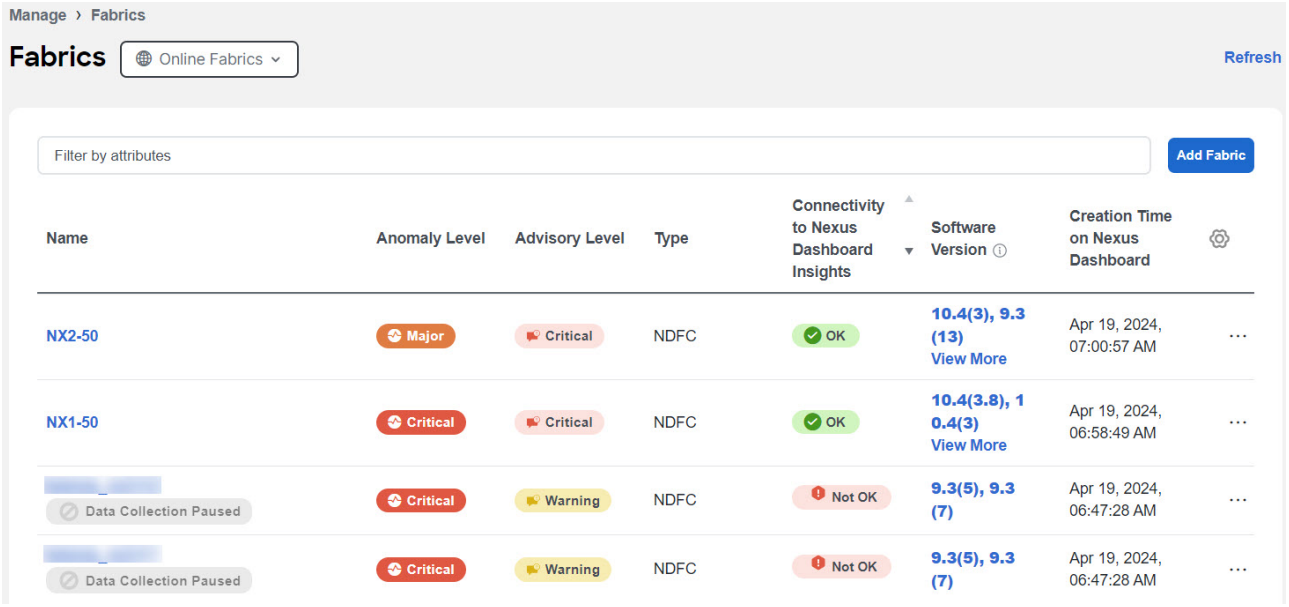
See an at-a-glance summary for each individual fabric in the Fabrics area. It includes their anomaly and advisory health levels, fabric-external traffic with total data transferred, and connectivity data for endpoints and Layer 3 neighbors. To learn about fabrics in Global View, see Journey and Global View.

Individual Fabric Details

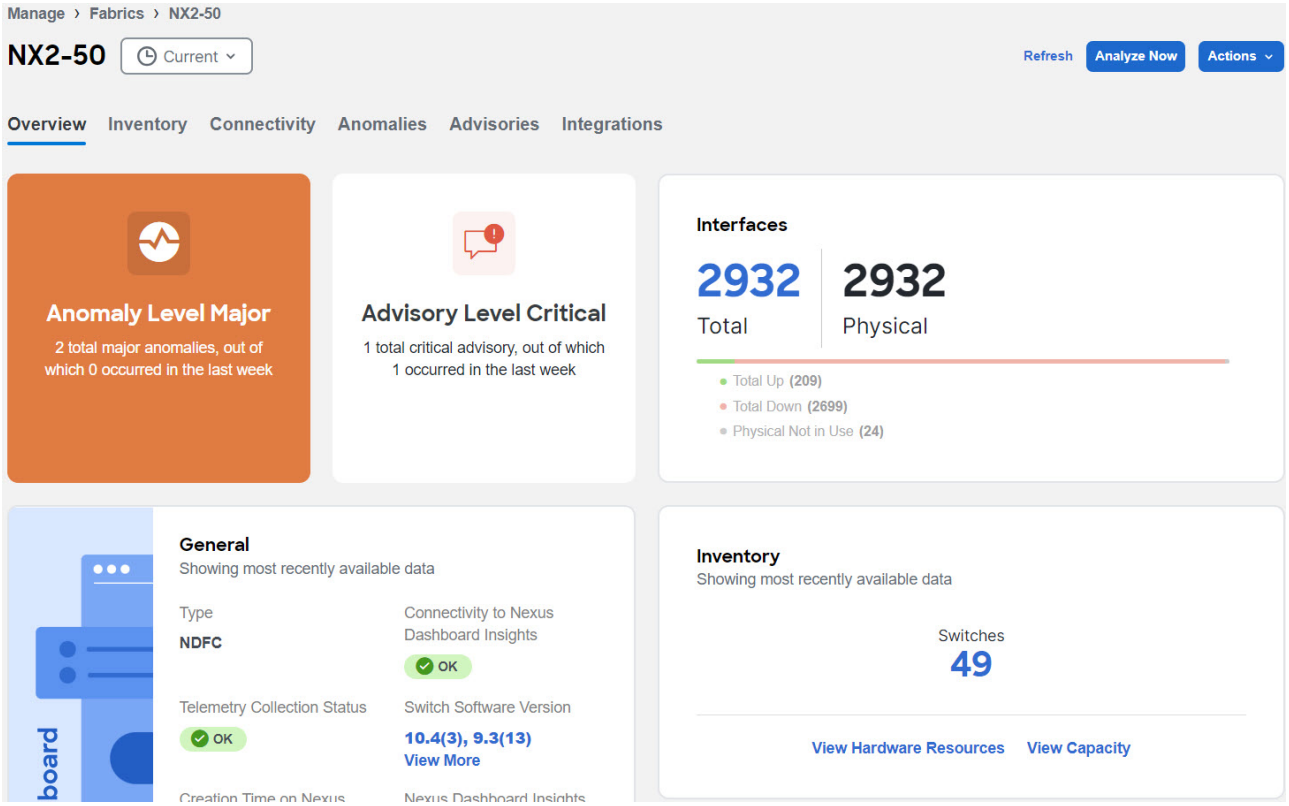
In the Fabrics page, you can dive into the details for an individual fabric, switch, or interface, with a comprehensive dashboard, simple topology, per-device summaries and more. You can also manage anomalies and advisories at a fabric level.

1. Navigate to **Manage** > **Fabrics**.
2. Choose Online or Snapshot fabrics from the drop-down list.

3. Use the search bar to filter the fabrics. The Fabrics table, displays the fabric type, connectivity status, anomaly and advisory level, onboarding time.



4. Click the fabric name to view details for your fabric. From the Time Selection drop-down menu choose the time. All sections will show data based on time selection and data availability. By default, the current time is selected.
5. Click **Overview**.



   a. In the The **Anomaly** and **Advisory** area you can view the status of your anomaly and advisory levels, and a list of your top anomaly and advisory categories.

      i. Click **Anomaly** to view the level, category, and count for your anomalies for the fabric.

      ii. Click the anomaly name to view additional details.

iii. Click **Advisory** to view the level, category, and count for your advisories for the fabric.

iv. Click the advisory name to view additional details.

b. The **General** area shows you the type of fabric, the software version used, the connectivity status to Nexus Dashboard, conformance status, onboarding time, telemetry status, and Traffic Analytics status. You can see Traffic Analytics status if you have enabled Traffic Analytics in **Flow Collection**. See Traffic Analytics. In the General area hover on the software version and click **View Bugs** to view the active and susceptible bugs for that fabric. See Getting Started.

   Telemetry collection status provides insights into the health and performance of the switches and devices in your network. The different telemetry collection statuses at the fabric level include:

   i. **OK** – This status indicates that the telemetry data streaming from all the switches to Nexus Dashboard Insights is functioning correctly. This is the desired state, as it ensures comprehensive monitoring and visibility into the network's performance.

   ii. **Not OK** – This status indicates the telemetry data streaming from all the switches to Nexus Dashboard Insights is not functioning correctly. This could be as a result of various problems such as network outages, misconfigurations, or hardware failures.

   iii. **Partial OK** – This status indicates that telemetry data streaming from all the switches to Nexus Dashboard Insights is not functioning correctly from some of the switches but it is functioning correctly from others. This suggests an inconsistent or partial telemetry data flow within the network which could be caused by various factors, such as switch-specific issues or misconfigurations on some switches.

c. In the **Analytics Summary** area, you can see an overview of the multiple analytics collected from across the fabric. It displays the status for conformance, congestion score, sustainability and traffic analytics. For Inventory you can view only congestion score under **Analytics Summary**.

d. In the **External Traffic** area, you can see the External Traffic that the fabric has sent and received in the last 7 days. The donut helps view the how much traffic is sent and received by the fabric. Click the information icon to view more information about what External Traffic is and how it can be measured for the different types of fabrics.

e. In the **Interfaces** area, you can see the summary of the interfaces for the fabric. Click **Total** to view additional details such as Anomaly Level, Admin Status, Operational Status, and Interface Type. Click the interface name to view additional details.

f. In the **Connectivity** area, you can view details about your endpoints, and L3 neighbors.

g. In the **Inventory** area, you can view the summary of the controllers and switches for the fabric.

   i. Click **View Hardware Resources** to view the hardware resources for the fabric. Click and choose a resource from the **Top Devices By** drop-down list to see a graph for that resource. In the table that follows, see the resource usage by switch. Click the switch name to view additional details.

   ii. Click **View Capacity** to view the different resources with their maximum capacity and current usage. Fabric Summary shows you the trends for the week, as well as the capacity by resource for the entire fabric. You see the number of resources used out of the total available capacity for each resource in this fabric (for example, Bridge Domains 2829 of 15000). The percentage indicates the percentage of resource used. The Switch Summary displays the capacity breakout of resources by switch. The graph shows you the timeline

for the parameter that you have chosen from the **Top Switches By** drop-down list. In the table, click Operational Resources, Configuration Resources, or Hardware Resources, to see the capacity and usage for each switch in the fabric.

6. Click **Inventory** to view the the controllers and switches information for the fabric. To learn more, see Inventory.
7. Click **Connectivity** to view the details of interfaces, endpoints, L3 neighbors, vPC Domains, flows for the fabric. To learn more, see Inventory. You can also view Multicast Route details for a fabric. See Multicast Routes.
8. Click **Anomalies** to view all the anomalies for the fabric. To learn more, see Anomalies and Advisories.
9. Click **Advisories** to view all the advisories for the fabric. To learn more, see Anomalies and Advisories.
10. Click **Integrations** to view all the integrations associated with the fabric. To learn more, see Integrations.
11. Click **File History** to view he history of files that are attached to the snapshot fabric. It shows the file name, the file size, when the file was uploaded, upload status, and when the last analysis was run.

    File History is displayed only for snapshot fabrics.

    a. For the currently active snapshot, which is the latest file that you uploaded, you can click **Run Analysis** to run the same snapshot analysis again. This can be useful when additional features are added and you want to re-run an analysis so that the additional features are included in your analysis.

    b. You can also upload a snapshot file for the same fabric at a different time interval. Click **Upload File** to upload the file and then click **Run Analysis** to run the snapshot analysis.

Multicast Routes

In the multicast dashboard, you can view the following multicast route information for an NDFC fabric:

- Top groups by traffic
- Top groups by receivers

Prerequisites for multicast routes

Execute the following commands on the Nexus switch:

```
switch(config)# hardware profile multicast flex-stats-enable

switch(config)# multicast flow-path export

switch(config)# copy running-config startup-config

switch(config)# reload
```

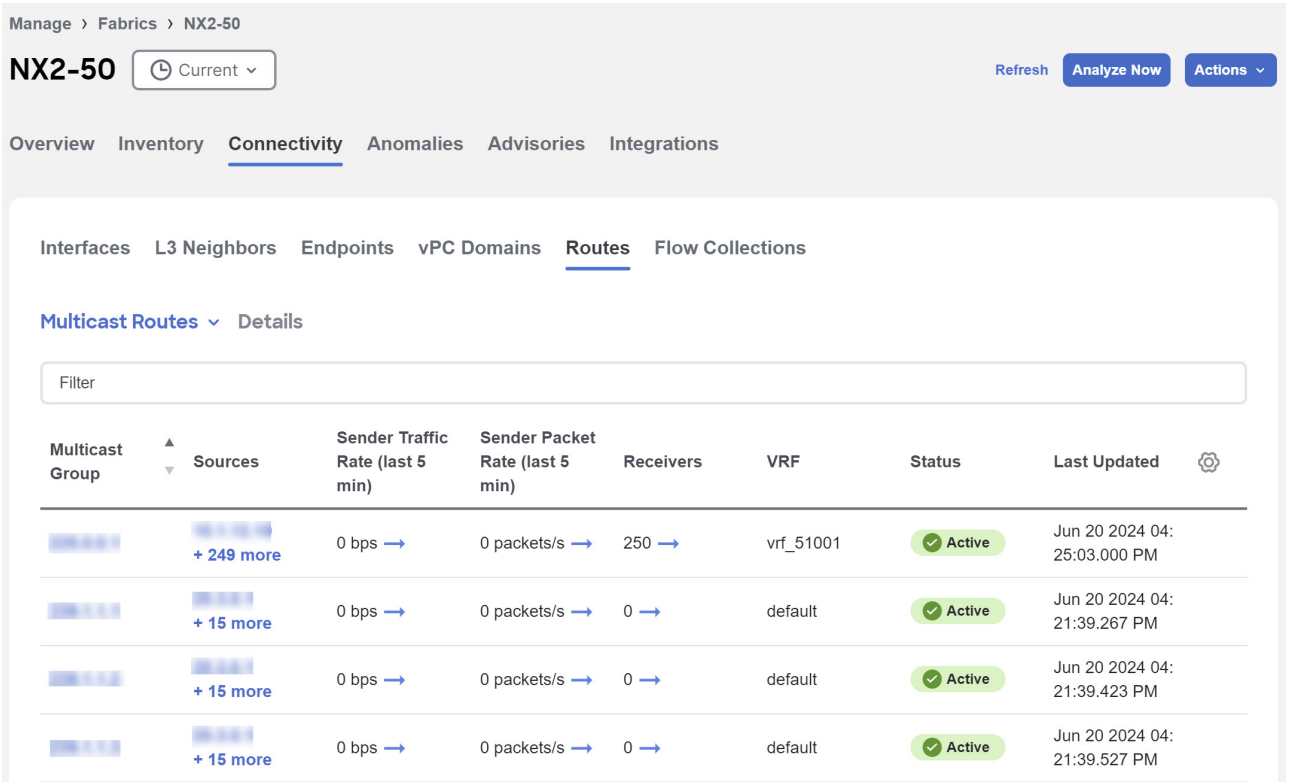
You must execute the commands copy running-config startup-config and reload for the changes to take effect.

Guidelines and limitations for multicast routes

- Multicast routing analytics is supported on Cisco NX-OS release 10.4(1)F and later for VXLAN and 10.3(3)F and later for classic LAN.
- Multicast routing analytics is supported for Classic VLAN and VXLAN fabrics.
- Multicast routing analytics is only supported for IPv4 addresses.
- Supported scale limits per fabric: 2000 multicast groups, 16000 S,G entries, 8K routed interfaces.
- When First Hop Router for multicast or the multicast source is configured outside the fabric, multicast routes are not displayed in the GUI.

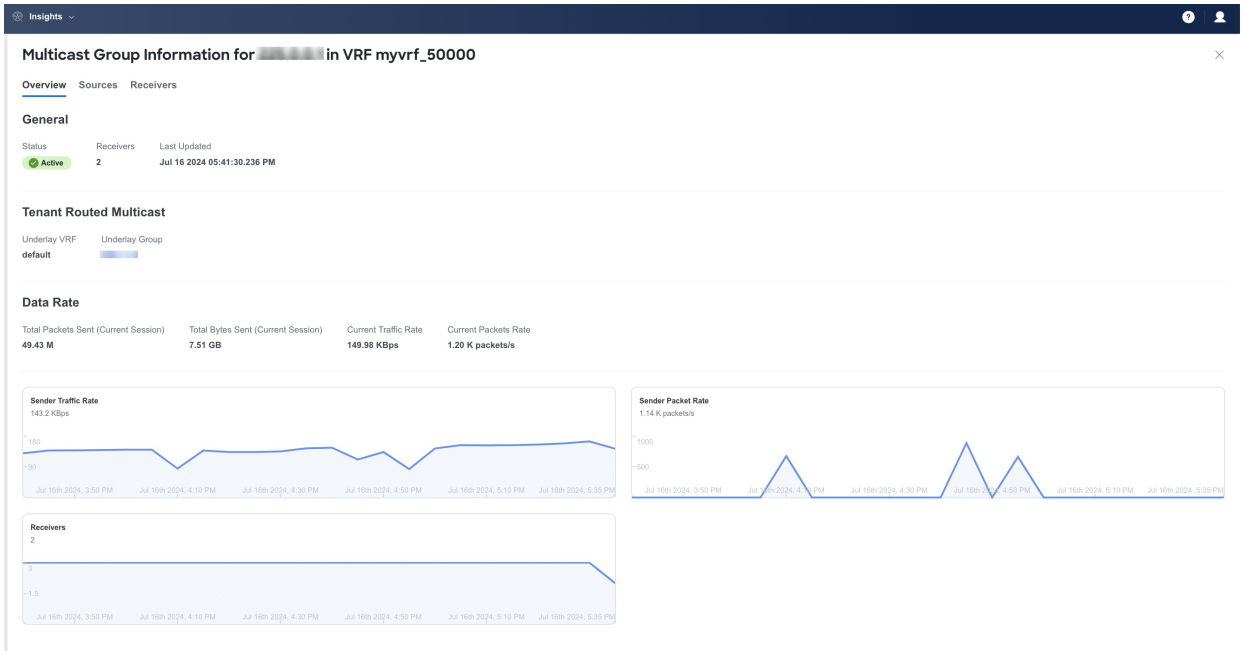
View multicast routes

1. Navigate to **Manage** > **Fabrics**.
2. Choose **Online Fabrics** or **Snapshot Fabrics** from the drop-down list.
3. Click the fabric name to view the fabric details.
4. Choose **Connectivity** > **Routes**.
5. In the **Details** drop-down menu, choose **Multicast Routes**.
6. In the Multicast page, you can view the information such as multicast groups, sources sending to this group, sending rate per source, number of receivers for this group, and VRF instances.

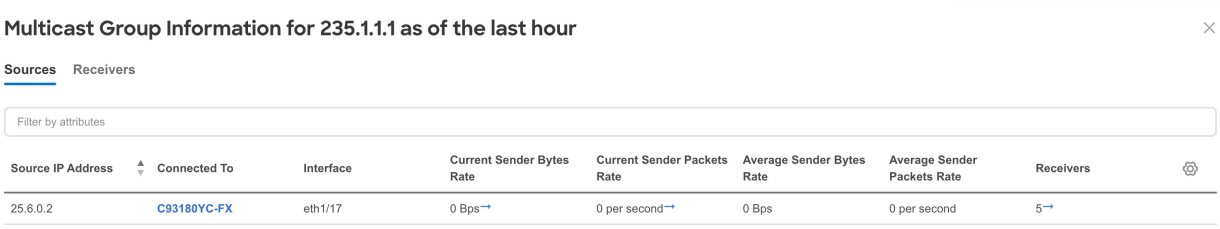


7. Click a multicast group to view additional information for sources and receivers.
   a. Click **Overview** to view information such as multicast underlay group information for all tenant routed multicast sources, and trend graphs showing the sender traffic rate, sender packet

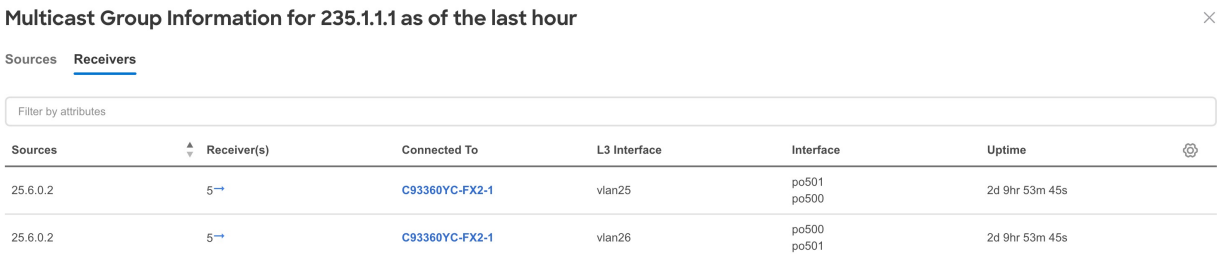
rate, and number of receivers. The **Overview** displays by default.



b. Click **Sources** to view information such as source IP address, switch name, and interface.



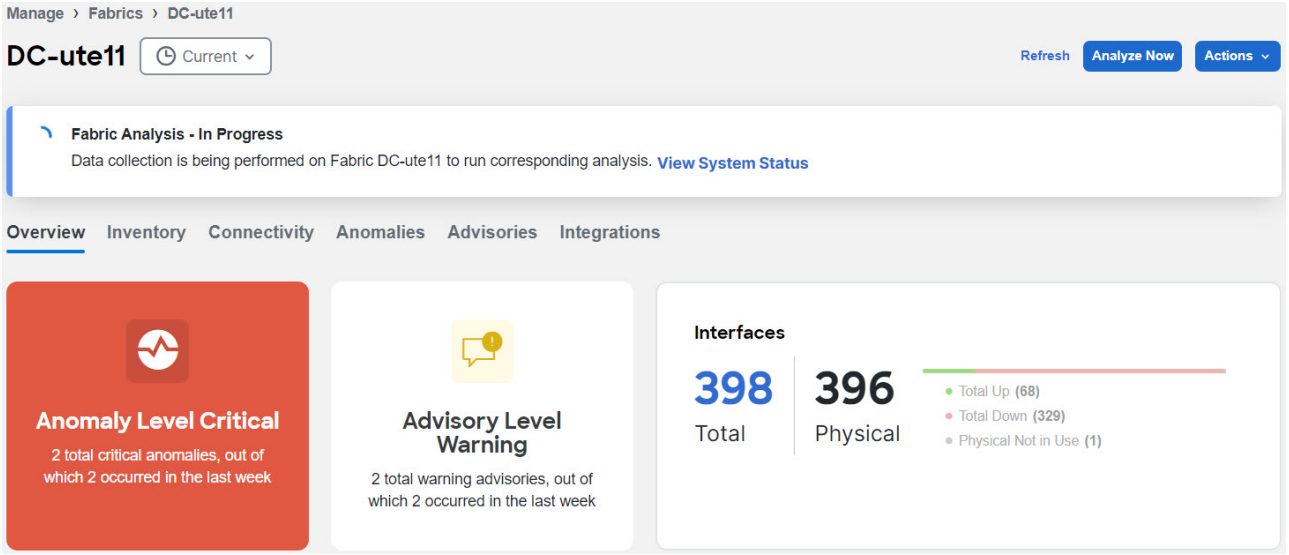
c. Click **Receivers** to view information such as switch name,receiver count, uptime, and L3 interface.



8. Click a **Sources** entry to view the list of all source IP addresses for that multicast group.
   a. Click one of the source IP addresses in the list to view additional information about that source.

Working with Fabrics

1. Navigate to **Manage** > **Fabrics**.
2. To add a fabric, click **Add Fabric**. See Add fabrics.
3. Choose Online or Snapshot fabrics from the drop-down list.
4. Click the fabric name to view the Fabric Details.



5. From the Actions drop-down menu, choose **Edit Fabric** to edit the fabric details. After you update the information, click **Save**.
6. From the Actions drop-down menu, choose **View in Topology** to view the topology for the fabric.
7. From the Actions drop-down menu, choose **System Status** to view the status of the data analysis for your fabric. See Getting Started.
8. To delete a fabric from Nexus Dashboard Insights, perform the following steps:
    a. From the Actions drop-down menu, choose **Pause Telemetry Collection** to pause data collection.
    b. From the Actions drop-down menu, choose **Remove from Insights** to remove the fabric. The fabric is removed from Nexus Dashboard Insights only and not from Nexus Dashboard's Admin Console.
9. From the Actions drop-down menu, choose **Resume Telemetry Collection** to resume data collection.
10. Click **Analyze Now** to perform an on-demand analysis. Choose the service such as Assurance, Bug Scan, or Best Practices and click **Run Now**. See Getting Started.

Troubleshooting telemetry configuration issues

The Nexus Dashboard Insights telemetry configurations can fail on the switches for various reasons. These sections describe some of the common scenarios.

Common configuration issues with standalone NX-OS fabrics

The table provides common configuration issues and solutions with standalone NX-OS fabrics.

Common configuration issues and solutions with standalone NX-OS fabrics

Issue	Solution
If you already enabled feature analytics on the switches, the Traffic Analytics configuration from Nexus Dashboard Insights will fail because you cannot enable feature netflow when feature analytics is enabled. Nexus Dashboard Insights raises a system anomaly that contains the following string: Delivery failed with message: Netflow feature cannot be enabled while analytics feature is enabled	1. Remove the switch from the fabric. 2. Remove feature analytics from the switch. 3. Add the switch to the fabric. 4. Verify that the anomaly was cleared.
If you already enabled feature netflow on the switches, Nexus Dashboard Insights will not allow Flow Telemetry to be enabled on switches that have an NX-OS release earlier than 10.3(3).	1. Remove the switch from the fabric. 2. Disable feature netflow and remove all associated Netflow configurations. 3. Add the switch to the fabric.
If you added a switch with a stale flow exporter configuration to the fabric, the Flow Telemetry configuration from Nexus Dashboard Insights can fail due to conflicting exporter destination IP address configurations. Nexus Dashboard Insights raises a system anomaly that contains the following string: Delivery failed with message: Cannot delete destination address of an exporter attached to the monitor. Remove the exporter from the monitor to delete	1. Remove the switch from the fabric. 2. Remove feature analytics from the switch. 3. Add the switch to the fabric. 4. Verify that the anomaly was cleared.

Issue	Solution
Nexus Dashboard Insights configurations are saved to the startup configuration by periodically using the " copy running-config startup-config" command on a switch. If you reboot the switch after you deployed the Nexus Dashboard Insights configuration but before the copy operation is run, the configuration will be lost, which can result in inconsistencies in the configuration. The worst case time period for this issue to happen is about 2 hours.	• If the configuration was lost because you enabled Nexus Dashboard Insights for the first time, you can recover the configuration by manually deploying the Nexus Dashboard Insights configuration on the switch. • If the configuration was lost during a Flow Telemetry-to-Traffic Analytics change or a similar operation, the rebooted switch will have the old Flow Telemetry configuration whereas Nexus Dashboard will have the Traffic Analytics configuration. Clean up the Flow Telemetry configuration, then manually deploy the Nexus Dashboard Insights configuration on the switch. In either case, these steps get the configuration that you must deploy: 1. In the Nexus Dashboard Insights GUI, go to **Admin > System Settings > System Status Details**. 2. In the table, find the switch, scroll to the far right of the table, click the ellipsis, and choose **Expected Configuration**. Another solution is to pause telemetry on the fabric, then resume telemetry.
If the switches and Nexus Dashboard become out of sync due to out-of-band configuration changes on the switches, this can result in subsequent configuration failures. Nexus Dashboard detects the switches as out of sync as part of their scheduled CC runs once every 24 hours. You can also trigger a CC run manually using **Resync Insights Configuration** from Nexus Dashboard. Nexus Dashboard Insights raises a system anomaly that contains the following string: switch's configs are out of sync	Avoid any manual configuration changes that can result in a configuration conflict. In the case of a conflict, remove all telemetry-related configurations from the switches, then re-add the necessary configurations. Follow these steps to get the configurations that you must re-add: 1. In the Nexus Dashboard Insights GUI, go to **Admin > System Settings > System Status Details**. 2. In the table, find the switch, scroll to the far right of the table, click the ellipsis, and choose **Expected Configuration**. Removing feature telemetry and feature analytics also removes all configurations under these features, including user configurations. You must manually re-add the user configurations after you restore the Nexus Dashboard Insights telemetry configurations.

Issue	Solution
When operating in monitored mode, the Nexus Dashboard Insights does not automatically deploy telemetry configurations to all switches within the fabric. Instead, you must manually apply the necessary configurations using CLI or APIs. The Nexus Dashboard Fabric Controller shows the required configuration within the Nexus Dashboard Insights setup screen.	You must manually re-add the user configurations and execute the CLI commands to deploy telemetry configurations. Follow these steps to get the configurations that you must re-add: 1. In the Nexus Dashboard Insights GUI, go to **Admin > System Settings > System Status Details**. 2. In the table, find the switch, scroll to the far right of the table, click the ellipsis, and choose **Expected Configuration**.
When you add a switch in monitored mode, you may not see all endpoints or interfaces due to connectivity issues of the switch. You can resolve by executing the CLI commands.	Make sure that the telemetry configuration is applied as expected. You can do this by navigating to the Nexus Dashboard Insights and checking **Expected Configuration** under the **System Status Details** section (see the previous row). Once the configuration is confirmed execute the following commands to initiate a synchronization of the switch telemetry with Nexus Dashboard Insights: - telemetry trigger subscription 500 - telemetry trigger subscription 501

Common configuration issues with Cisco NDFC-managed fabrics

The table provides common configuration issues and solutions with Cisco NDFC-managed fabrics.

Common configuration issues and solutions with Cisco NDFC-managed fabrics

Issue	Solution
If you already enabled feature analytics on the switches, the Traffic Analytics configuration from Nexus Dashboard Insights will fail because you cannot enable feature netflow when feature analytics is enabled.	1. Delete the the Flow Telemetry feature configurations from the switches: a. Remove the intents from NDFC. b. Trigger recalculate and deploy. 2. Trigger the Traffic Analytics configuration push from Nexus Dashboard Insights.
If you already have the Netflow configuration on NDFC, either from the Netflow configuration from the NDFC fabric settings or from the switch free-form templates, Nexus Dashboard Insights will not allow Flow Telemetry to be enabled on switches that have an NX-OS release earlier than 10.3(3).	1. Remove the Netflow configuration from NDFC. 2. Trigger recalculate and deploy. 3. Trigger the Flow Telemetry push from Nexus Dashboard Insights.

Common configuration issues with all fabrics

The table provides common configuration issues and solutions with all fabrics.

Common configuration issues and solutions with all fabrics

Issue	Solution
If there are connectivity issues between the switches and Nexus Dashboard, deploying a configuration can fail.	1. Restore the connectivity. 2. Retry the configuration.

Copyright

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

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

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

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2017-2025 Cisco Systems, Inc. All rights reserved.