Editing Campus VXLAN Fabric Settings, Release 4.1.1

Table of Contents

New and changed information

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

Release Version	Feature	Description
Nexus Dashboard 4.1.1	Improved navigation and workflow when editing Campus VXLAN fabric settings	Beginning with Nexus Dashboard 4.1.1, Nexus Dashboard enhanced the navigation and workflow when editing Campus VXLAN fabric settings.
Nexus Dashboard 4.1.1	Support for southbound loop detection	With this release, Nexus Dashboard supports southbound loop detection for leaf, border-leaf, and border-gateway devices. When you edit fabric settings, you can enable southbound loop detection for detecting and mitigating loops in VXLAN EVPN fabrics. This feature is supported when editing the Data Center VXLAN EVPN (for fabrics with iBGP and eBGP overlay routing protocols). For more information, see Fabric Management > Advanced.

About Campus VXLAN EVPN fabric

Nexus Dashboard supports Campus VXLAN EVPN fabric type to automate and manage Enterprise Campus VXLAN BGP EVPN networks based on Catalyst 9000 series switches. Optionally, administrators can integrate a Nexus 9000 switch with Border Gateway functionality to interconnect with remote Data Centers and Campus for VXLAN EVPN multi-fabric Layer 2 and Layer 3 extensions.

This document describes how to create a Campus VXLAN EVPN fabric with Cisco Catalyst 9000 series switches and Nexus 9000 series switches using the **Campus VXLAN EVPN** fabric template. This fabric supports OSPF as the underlay protocol and BGP EVPN as the overlay protocol. Using this fabric template, Nexus Dashboard manages all the configurations of a VXLAN EVPN fabric consisting of Cisco Catalyst 9000 IOS XE and Nexus 9000 NX-OS switches. Backing up and restoring this fabric is similar to **Data Center VXLAN EVPN** backup and restore.

Nexus Dashboard provides support for the following features with Campus VXLAN EVPN fabrics:

- Tenant Routed Multicast (TRM)
- Zero-Touch Provisioning (ZTP) on Cisco Catalyst switches through Plug and Play (PnP)
- Deploying Campus VXLAN EVPN fabric as a child fabric in VXLAN EVPN Multi-Site.

Guidelines for configuring Campus VXLAN EVPN fabrics

- Out-of-band management is required for Campus VXLAN EVPN fabric types.
- Provides support for EVPN VXLAN Distributed Anycast Gateway when each SVI is configured with the same Anycast Gateway MAC.
- Provides support for Cisco Catalyst switches with Stackwise or Stackwise Virtual.
- Provides support for spine, leaf, and border roles on Cisco Catalyst switches. Whereas, Cisco Nexus 9000 series switches support border gateway, border gateway spine and border gateway super spine roles.
- Does not support Brownfield deployments.
- Does not support IPv6 underlay and Anycast RP.
- Does not support ISIS, ingress replication, unnumbered intra-fabric link, and 4 bytes BGP ASN.
- Does not support breakout interfaces on Cisco IOS XE switches.

For information about configuration compliance, see the section "Configuration Compliance in External Fabrics" in Editing External Fabric Settings.

Editing Campus VXLAN fabric settings

A **Campus VXLAN** fabric is a type of fabric that is used for a VXLAN EVPN campus deployment with Catalyst 9000 and Nexus 9000 switches as border gateways.

When you first create a Campus VXLAN fabric using the procedures provided in Creating LAN and ACI Fabrics and Fabric Groups, the standard workflow allows you to create a fabric using the bare minimum settings so that you are able to create a fabric quickly and easily. Use the procedures in this article to make more detailed configurations for your campus VXLAN fabric.

Perform the following steps to create the Campus VXLAN EVPN fabric for Cisco Catalyst 9000 series switches and Nexus 9000 series switches:

1. Navigate to the main **Fabrics** page:

   Manage > Fabrics

2. Locate the Campus VXLAN fabric that you want to edit.

   Campus VXLAN fabrics are shown with **Campus VXLAN EVPN** in the **Type** column.

3. Click the circle next to the Campus VXLAN fabric that you want to edit to select that fabric, then click **Actions > Edit Fabric Settings**.

   The **Edit *fabric_name* Settings** page appears.

4. Click the appropriate tab to edit these settings for the fabric:
   - General
   - Fabric Management
   - Telemetry (if the **Telemetry** feature is enabled for the fabric)

General

Use the information in this section to edit the settings on the **General** page for your campus VXLAN fabric.

The fields on this **Edit Fabric Settings > General** page are the same fields that appeared on the **3. Settings** page when you first created this Campus VXLAN fabric, with the same configurations that you provided when you created this fabric. Edit these already-configured settings if necessary, or click another tab to leave these settings unchanged.

Change the general parameters that you configured previously for the Campus VXLAN fabric, if necessary.

Fabric type	Description
Name	The name for the fabric. This field is not editable.
Type	The fabric type for this fabric. This field is not editable.
Location	Choose the location for the fabric.
BGP ASN for Spines	Enter the BGP autonomous system number (ASN) for the fabric's spine switches.
License tier	Choose the licensing tier for the fabric: • **Essentials** • **Advantage** • **Premier** Click on the information icon (i) next to License tier to see what functionality is enabled for each license tier.
Security domain	Choose the security domain for the fabric.

Fabric Management

Use the information in this section to edit the settings on the **Fabric Management** page for your Campus VXLAN fabric. The tabs and their fields on the page are explained in these sections. The fabric-level parameters are included in these tabs.

- General Parameters
- Replication
- Protocols
- Advanced
- Resources
- Bootstrap
- Configuration Backup
- Border Gateway

General Parameters

The **General Parameters** tab is displayed by default. The fields in this tab are described in the following table.

Field	Description
Underlay Subnet IP Mask	Specifies the subnet mask for the fabric interface IP addresses.
Link-State Routing Protocol	Specifies the supported routing protocol which is OSPF.

Field	Description
Route-Reflectors	The number of spine switches that are used as route reflectors for transporting BGP traffic. Choose option 2 or 4 from the drop-down list. The default value is 2. To deploy spine devices as RRs, Nexus Dashboard sorts the spine devices based on their serial numbers and designates two or four spine devices as RRs. If you add more spine devices, existing RR configuration won't change. Increasing the count - You can increase the route reflectors from two to four at any point in time. Configurations are automatically generated on the other two spine devices designated as RRs. Decreasing the count - When you reduce four route reflectors to two, remove the required route reflector devices from the fabric. Follow these steps to reduce the count from 4 to 2. 1. Change the value in the drop-down list to 2. 2. Identify the spine switches designated as route reflectors. An instance of the **rr_state** policy is applied on the spine switch if it's a route reflector. 3. Delete the spine devices that are not required from the fabric. If you delete existing RR devices, the next available spine switch is selected as the replacement RR. 4. Click **Deploy Config** in the fabric topology window. You can preselect RRs and RPs before performing the first **Save & Deploy** operation.
Anycast Gateway MAC	Specifies the shared MAC address for the leaf switches.
Enable Performance Monitoring	Enables performance monitoring on the switches. Ensure that you do not clear interface counters from the Command Line Interface of the switches. Clearing interface counters can cause the Performance Monitor to display incorrect data for traffic utilization. If you must clear the counters and the switch has both clear counters and clear counters snmp commands (not all switches have the clear counters snmp command), ensure that you run both the main and the SNMP commands simultaneously. For example, you must run the clear counters interface ethernet slot/port command followed by the clear counters interface ethernet slot/port snmp command. This can lead to a one time spike.

What's next: Complete the configurations in another tab if necessary or click **Save** when you have completed the necessary configurations for this fabric.

Replication

The fields in the **Replication** tab are described in the following table. All the fields are automatically populated based on Cisco-recommended best practice configurations, but you can update the fields if needed.

Field	Description
Replication Mode	Specifies the mode of replication used in the fabric for BUM (Broadcast, Unknown Unicast, Multicast) traffic. **Multicast** is selected by default.
Multicast Group Subnet	Specifies the IP address prefix used for multicast communication. A unique IP address is allocated from this group for each overlay network. The replication mode change is not allowed if a policy template instance is created for the current mode. For example, if a multicast related policy is created and deployed, you cannot change the mode to Ingress.
Enable Tenant Routed Multicast (TRM)	Enables Tenant Routed Multicast (TRM) that allows overlay multicast traffic support over EVPN/MVPN in the VXLAN EVPN fabric.
Rendezvous-Points	Specifies the number of spine switches acting as rendezvous points.
Underlay RP Loopback Id	Specifies the loopback ID used for the RP, for multicast protocol peering purposes in the fabric underlay. The default is 254.

What's next: Complete the configurations in another tab if necessary or click **Save** when you have completed the necessary configurations for this fabric.

Protocols

The fields in the **Protocols** tab are described in the following table. All the fields are automatically populated based on Cisco-recommended best practice configurations, but you can update the fields if needed.

Field	Description
Underlay Routing Loopback Id	Specifies the loopback interface ID. By default, value 0 is populated as loopback0 that is normally used for fabric underlay IGP peering purposes.
Underlay VTEP Loopback Id	Specifies the loopback interface ID. By default, value 1 is populated as loopback1 used as the VTEP address.
OSPF Process Id	Specifies the OSPF process tag.
OSPF Area Id	Specifies the OSPF unique 32-bit area ID denoted in dotted decimal format.

What's next: Complete the configurations in another tab if necessary or click **Save** when you have completed the necessary configurations for this fabric.

Advanced

The fields in the **Advanced** tab are described in the following table. All the fields are automatically populated based on Cisco-recommended best practice configurations, but you can update the fields

if needed.

Field	Description
VRF Template	Specifies the VRF template for creating VRFs. By default, the system uses the pre-defined **Default_VRF_Universal** template for overlay configuration for leaf switches.
Network Template	Specifies the network template for creating networks. By default, the system uses the pre-defined **Default_Network_Universal** template for leaf switches.
VRF Extension Template	Specifies the VRF extension template for enabling VRF extension to other fabrics. By default, the system uses the pre-defined **Default_VRF_Extension_Universal** template for border switches.
Network Extension Template	Specifies the network extension template for extending the network to other fabrics. By default, the system uses the pre-defined **Default_Network_Extension_Universal** template for border switches.
Intra Fabric Interface MTU	Specifies the MTU for the intra fabric interface. The value must be an even number. The valid values range from 576 to 9216. This is a mandatory field.
Layer 2 Host Interface MTU	Specifies the MTU for the layer 2 host interface. This value must be an even number. The valid values range from 1500 to 9216. The default MTU for both fabric interface and host interface is 9198. The default MTU for IOS XE is 1500.
IOS XE System MTU	Specifies the MTU for an IOS XE device. This value must be an even number. The valid values range from 1500 to 9198.
Enable Tenant DHCP	Check the check box to enable DHCP and associated configurations globally on all the switches in the fabric. This is a prerequisite for supporting DHCP for overlay networks that are part of the tenant VRFs.  Ensure that **Enable Tenant DHCP** is enabled before enabling DHCP-related parameters in the overlay profiles.
VTP Mode	By default, the VTP mode is **Off**. **Transparent** mode allows you to relay all VTP protocol packets that it receives on a trunk port to all other trunk ports.
Enable NDFC as Trap Host	Allows you to configure Nexus Dashboard as an SNMP trap destination.

Field	Description
Enable Overlay Template Conversion	Allows you to convert all the existing VRFs and networks to use the default templates. In existing deployments using the **IOS_XE_VRF** and **IOS_XE_Network** templates, enabling this field converts the templates to use the **Default_VRF_Universal**, **Default_Network_Universal**, **Default_VRF_Extension_Universal** and **Default_Network_Extension_Universal** templates after performing a **Recalculate and deploy**. When adding child fabrics to a VXLAN fabric group, a Campus VXLAN EVPN fabric does not allow you to add fabrics that are configured with **IOS_XE_VRF** and **IOS_XE_Network** as the templates for existing VRFs and networks. Enable the **Enable Overlay Template Conversion** field to convert the existing VRFs and networks using **IOS_XE_VRF** and **IOS_XE_Network** templates to the **Default_VRF** and **Default_Network** templates.
Leaf Freeform Config	Configures additional CLIs for all the Cisco Catalyst leaf switches in the fabric.
Spine Freeform Config	Configures additional CLIs for all the Cisco Catalyst spine switches in the fabric.
Intra-fabric Links Additional Config	Configures additional CLIs for all the intra fabric links.

What's next: Complete the configurations in another tab if necessary or click **Save** when you have completed the necessary configurations for this fabric.

Resources

The fields in the **Resources** tab are described in the following table. Most of the fields are automatically populated based on Cisco-recommended best practice configurations, but you can update the fields if needed.

Field	Description
Underlay Routing Loopback IP Range	Specifies the loopback IPv4 addresses for protocol peering.
Underlay VTEP Loopback IP Range	Specifies the loopback IP address range for VTEPs.
Underlay RP Loopback IP Range	Specifies anycast or phantom RP IP address range.
Underlay Subnet IP Range	Specifies the IP addresses for underlay P2P routing traffic between interfaces.
Layer 2 VXLAN VNI Range	Specify the VXLAN VNI IDs for the fabric.
Layer 3 VXLAN VNI Range	Specify the VXLAN VNI IDs for the fabric.

Field	Description
Network VLAN Range	VLAN range for the per switch overlay network (min:2, max:4094).
VRF VLAN Range	VLAN range for the per switch overlay Layer 3 VRF (min:2, max:4094).
Subinterface Dot1q Range	Specifies the subinterface range when L3 sub-interfaces are used.
VRF Lite Deployment	Specifies the VRF Lite method for extending inter-fabric connections. The **VRF Lite Subnet IP Range** field specifies resources reserved for IP address used for VRF Lite when VRF Lite IFCs are auto-created. If you select **Back2Back&ToExternal**, then VRF Lite IFCs are auto-created.
Auto Deploy for Peer	This check box is applicable for VRF Lite deployment. When you select this checkbox, auto-created VRF Lite IFCs will have the **Auto Generate Configuration for Peer** field in the **VRF Lite** tab set, if the peer is a Cisco device. To access VRF Lite IFC configuration, navigate to the **Links** tab, select the link, and then choose **Actions > Edit**. You can check or uncheck the check box when the **VRF Lite Deployment** field is not set to **Manual**. This configuration only affects the new auto-created IFCs and does not affect the existing IFCs. You can edit an auto-created IFC and check or uncheck the **Auto Generate Configuration for Peer** field. This setting takes priority always.
Auto Deploy Default VRF	When you select this check box, the **Auto Generate Configuration on default VRF** field is automatically enabled for auto-created VRF Lite IFCs. You can check or uncheck this check box when the VRF Lite Deployment field is not set to **Manual**. The **Auto Generate Configuration on default VRF** field when set, automatically configures the physical interface for the border device, and establishes an eBGP connection between the border device and the edge device or another border device in a different VXLAN EVPN fabric.
Auto Deploy Default VRF for Peer	When you select this check box, the **Auto Generate Configuration for NX-OS Peer on default VRF** field is automatically enabled for auto-created VRF Lite IFCs. You can check or uncheck this check box when the VRF Lite Deployment field is not set to **Manual**. The **Auto Generate Configuration for NX-OS Peer on default VRF field** when set, automatically configures the physical interface and the eBGP commands for the peer NX-OS and IOS XE switches.  To access the **Auto Generate Configuration on default VRF** and **Auto Generate Configuration for NX-OS Peer on default VRF** fields for an IFC link, navigate to the **Links** tab, select the link and choose **Actions > Edit**.
Redistribute BGP Route-map Name	Route Map used to redistribute BGP routes to IGP in default VRF for auto-created VRF Lite IFC links.

Field	Description
VRF Lite Subnet IP Range	These fields are prefilled with the DCI subnet details. Update the fields as needed. The values shown on the page are automatically generated. If you want to update the IP address ranges, VXLAN Layer 2/Layer 3 network ID ranges or the VRF/network VLAN ranges, ensure that each fabric has its own unique range and is distinct from any underlay range to avoid possible duplication. You should only update one range of values at a time. If you want to update more than one range of values, do it in separate instances. For example, if you want to update Layer 2 and Layer 3 ranges, you should do the following. 1. Update the Layer 2 range and click **Save**. 2. Click the **Edit Fabric** option again, update the Layer 3 range, and click **Save**.
VRF Lite Subnet Mask	
Auto Allocation of Unique IP on VRF Extension over VRF Lite IFC	When enabled, IP prefix allocated to the VRF Lite IFC is not reused on VRF extension over VRF Lite IFC. Instead, unique IP Subnet is allocated for each VRF extension over VRF Lite IFC.
Per VRF Per VTEP Loopback Auto-Provisioning	Enables you to auto provision a loopback on a VTEP on VRF attachment. 1. Enable the **Per VTEP Loopback Auto-Provisioning** option. 2. Save the fabric settings. 3. Perform a **Recalculate and deploy** operation. 4. Navigate to **VRF Attachments**. 5. If certain VRFs are already attached, click **Actions > Quick attach**. This generates the new loopback in the VRF.  If VRF extensions are already enabled and configured, for example, VRF Lite on a border device, prior to enabling the fabric setting, you need to access the respective VRF attachment and the border device to reattach the VRF extension again. For example, VRF Corp is attached on Border-1 and extended to an external domain using VRF Lite. In this situation, when you perform a **Quick attach** to provision the new loopback in the VRF, the original VRF-Lite extension gets detached. You can then select the VRF attachment, edit, and re-attach the VRF-Lite extension and then deploy all the relevant configurations.
Per VRF Per VTEP IP Pool for Loopbacks	Indicates the prefix pool to assign IP addresses to loopbacks on VTEPs on a per VRF basis.

What's next: Complete the configurations in another tab if necessary or click **Save** when you have completed the necessary configurations for this fabric.

Bootstrap

The fields in the **Bootstrap** tab are described in the following table. Most of the fields are automatically populated based on Cisco-recommended best practice configurations, but you can update the fields if needed.

Field	Description
Enable Bootstrap	Check this check box to enable the bootstrap feature. Bootstrap allows easy day-0 import and bring-up of new devices into an existing fabric. Bootstrap leverages POAP for NX-OS and PnP for IOS XE. For NX-OS switches, POAP will not work if you have set **Bootstrap Script Download Protocol** (in the **Server Settings** for LAN) as **https**.
Enable Local DHCP Server	Select this check box to initiate enabling of automatic IP address assignment through a local DHCP server. When you select this check box, the **DHCP Scope Start Address** and **DHCP Scope End Address** fields become editable. If you want to configure a remote or external DHCP server for automatic IP address assignment, enter details about the external DHCP server in the **Switch Mgmt Default Gateway** and **Switch Mgmt IP Subnet Prefix** fields.
DHCP Version	Select DHCPv4 or DHCPv6 from this drop-down list. When you select DHCPv4, the **Switch Mgmt IPv6 Subnet Prefix** field is disabled. If you select DHCPv6, the **Switch Mgmt IP Subnet Prefix** is disabled. Cisco Nexus 9000 and 3000 Series Switches support IPv6 POAP only when switches are either Layer-2 adjacent (eth1 or out-of-band subnet must be a /64) or they are L3 adjacent residing in some IPv6 /64 subnet. Subnet prefixes other than /64 are not supported.
Domain name	Specifies the domain name of the DHCP server.
DHCP Scope Start Address and **DHCP Scope End Address**	Specifies the first and the last IP addresses of the IP address range to be used for the switch out of band POAP.
Switch Mgmt Default Gateway	Specifies the default gateway for the management VRF on the switch.

Field	Description
Switch Mgmt IP Subnet Prefix	Specifies the prefix for the management interface on the switch. The prefix should be between 8 and 30. *DHCP scope and management default gateway IP address specification*: If you specify the management default gateway IP address 10.0.1.1 and subnet mask 24, ensure that the DHCP scope is within the specified subnet, between 10.0.1.2 and 10.0.1.254.
Switch Mgmt IPv6 Subnet Prefix	Specifies the IPv6 prefix for the Mgmt0 interface on the switch. The prefix should be between 64 and 126. This field is editable if you enable IPv6 for DHCP.
Bootstrap Freeform Config (IOS-XE)	(Optional) Enter additional commands for IOS XE switches, as needed. For example, if you require some additional configurations to be pushed to the device and be available post device bootstrap, they can be captured in this field, to save the desired intent. After the devices boot up, they will contain the configuration defined in the **Bootstrap Freeform Config** field. Copy-paste the running-config to a **freeform config** field with correct indentation, as seen in the running configuration on the IOS XE switches. The freeform config must match the running config. For more information, see Enabling Freeform Configurations on Fabric Switches.
Bootstrap Freeform Config (NXOS)	(Optional) Enter additional commands for NX-OS switches, as needed. For example, if you require some additional configurations to be pushed to the device and be available post device bootstrap, they can be captured in this field, to save the desired intent. After the devices boot up, they will contain the configuration defined in the **Bootstrap Freeform Config** field. Copy-paste the running-config to a **freeform config** field with correct indentation, as seen in the running configuration on the NX-OS switches. The freeform config must match the running config. For more information, see Enabling Freeform Configurations on Fabric Switches.
DHCPv4 Multi Subnet Scope	Specifies the field to enter one subnet scope per line. This field is editable after you check the **Enable Local DHCP Server** check box. The format of the scope should be defined as: **DHCP Scope Start Address, DHCP Scope End Address, Switch Management Default Gateway, Switch Management Subnet Prefix** For example: 10.6.0.2, 10.6.0.9, 10.6.0.1, 24

What's next: Complete the configurations in another tab if necessary or click **Save** when you have completed the necessary configurations for this fabric.

Configuration Backup

The fields in the **Configuration Backup** tab is described in the following table. Most of the fields are automatically populated based on Cisco-recommended best practice configurations, but you can update the fields, if needed.

Field	Description
Hourly Fabric Backup	Select the check box to enable an hourly backup of fabric configurations and the intent. The hourly backups are triggered during the first 10 minutes of the hour.
Scheduled Fabric Backup	Check the check box to enable a daily backup. This backup tracks changes in running configurations on the fabric devices that are not tracked by configuration compliance.
Scheduled Time	Specify the scheduled backup time in a 24-hour format. This field is enabled if you check the **Scheduled Fabric Backup** check box. Select both the check boxes to enable both back up processes. The backup process is initiated after you click **Save**. The scheduled backups are triggered exactly at the time you specify with a delay of up to two minutes. The scheduled backups are triggered regardless of the configuration deployment status. The number of fabric backups that are retained on Nexus Dashboard is decided by the **Admin > System Settings > Server Settings > LAN Fabric > Maximum Backups per Fabric** option. The number of archived files that are retained is set in the **# Number of archived files per device to be retained:** field on the **Server Properties** page. Note: To trigger an immediate backup, do the following: 1. Choose **Overview > Topology**. 2. Click within the specific fabric box. The fabric topology screen comes up. 3. Right-click on a switch within the fabric, then select **Preview Config**. 4. On the **Preview Config** page for this fabric, click **Re-Sync All**. You can also initiate the fabric backup on the fabric topology page. Click **Backup Now** in the **Actions** pane.

What's next: Complete the configurations in another tab if necessary or click **Save** when you have completed the necessary configurations for this fabric.

Border Gateway

The **Border Gateway** tab is applicable only to Cisco Nexus 9000 switches. The fields in the tab are described in the following table. Most of the fields are automatically populated based on Cisco-

recommended best practice configurations, but you can update the fields if needed.

Field	Description
Site Id	Specifies the ID for this fabric when you are moving this fabric within a VXLAN EVPN Multi-Site. The site ID is mandatory for a member fabric to be a part of a VXLAN EVPN Multi-Site. Each member fabric of a VXLAN EVPN Multi-Site has a unique site ID for identification.
Anycast Border Gateway advertise-pip	Advertises Anycast Border Gateway PIP as VTEP.
Enable L3VNI w/o VLAN	Enables the Layer 3 VNI without VLAN option. The setting at this fabric-level field affects the related field at the VRF level. For more information, see: • Layer 3 VNI without VLAN • The "Creating a VRF" section in About Fabric Overview for LAN Operational Mode Setups
vPC Peer Link VLAN Range	Specifies the VLAN range used for the vPC peer link SVI. The vPC fields become active only if the switch role is border gateway. Valid entries: 2-4094.
Make vPC Peer Link VLAN as Native VLAN	Enables vPC peer link VLAN as Native VLAN.
vPC Peer Keep Alive option	Allows you to configure routed links between vPC peers using management or loopback interfaces. To use IP addresses assigned to the management port and the management VRF, choose **management**. To use IP addresses assigned to loopback interfaces and a non-management VRF, choose underlay routing loopback with IPv6 address for PKA. Both the options are supported for IPv6 underlay.
vPC Auto Recovery Time (In Seconds)	Specifies the vPC auto recovery time-out period in seconds.
vPC Delay Restore Time (In Seconds)	Specifies the vPC delay restore period in seconds.
vPC Peer Link Port Channel ID	Specifies the Port Channel ID for a vPC Peer Link. By default, the value in this field is 500.
vPC IPv6 ND Synchronize	Enables IPv6 Neighbor Discovery synchronization between vPC switches. The check box is enabled by default.
vPC advertise-pip	Select the check box to enable the Advertise PIP feature. You can enable the advertise PIP feature also on a specific vPC.
vPC Domain Id Range	Specifies the vPC Domain Id range to use for new pairings.
Enable NX-API	Enables NX-API on HTTPS. This check box is checked by default.
NX-API HTTPS Port Number	Specifies the port on which NX-API is enabled. By default, NX-API is enabled on HTTPS port 443.

Field	Description
Enable HTTP NX-API	Enables NX-API to use HTTP connections. This option is enabled by default. However, it is recommended to use HTTPs for secure communication.
NX-API HTTP Port Number	Specifies the port on which NX-API is enabled. By default, NX-API is enabled on HTTP port 80.
Enable TCAM Allocation	Automatically generates TCAM commands for VXLAN and vPC Fabric Peering, when enabled.
Nexus Border Gateway Freeform Config	Allows you to configure additional CLIs for all the border gateway switches.
Nexus Intra-fabric Links Additional Config	Allows you to configure additional CLIs for all the intra fabric links.
Greenfield Cleanup Option	Enables cleaning up the switches imported into Nexus Dashboard with Preserve-Config=No, without a switch reload. This option is typically recommended only for the fabric environments with Cisco Nexus 9000v switches to improve the switch clean-up time.

What's next: Complete the configurations in another tabs if necessary or click **Save** when you have completed the necessary configurations for this fabric.

Telemetry

The telemetry feature in Nexus Dashboard allows you to collect, manage, and monitor real-time telemetry data from your Nexus Dashboard. This data provides valuable insights into the performance and health of your network infrastructure, enabling you to troubleshoot proactively and optimize operations. When you enable telemetry, you gain enhanced visibility into network operations and efficiently manage your fabrics.

Follow these steps to enable telemetry for a specific fabric.

1. Navigate to the **Fabrics** page.

   Go to **Manage > Fabrics**.

2. Choose the fabric for which you want to enable telemetry.
3. From the **Actions** drop-down list, choose **Edit fabric settings**.

   The **Edit *fabric-name* settings** page displays.

   You can also access the **Edit *fabric-name* settings** page for a fabric from the **Fabric Overview** page. In the **Fabric Overview** page, click the **Actions** drop-down list and choose **Edit fabric settings**.

4. In the **Edit *fabric-name* settings** page, click the **General** tab.
5. Under the **Enabled features** section, check the **Telemetry** check box.
6. Click **Save**.

   Navigate back to the **Edit *fabric-name* settings** page. The **Telemetry** tab displays.

   NOTE: The **Telemetry** tab appears only when you enable the **Telemetry** option under the **General** tab in the **Edit *fabric-name* settings** page.

The **Telemetry** tab includes these options.

- **Configuration**—allows you to manage telemetry settings and parameters.
- **NAS**—provides Network Analytics Service (NAS) features for advanced insights.

Edit configuration settings

The **Configuration** tab includes these settings.

- **General**—allows you to enable analysis.

  You can enable these settings.

  - **Enable assurance analysis**—enables you to collect of telemetry data from devices to ensure network reliability and performance.
  - **Enable Microburst sensitivity** - allows you to monitor traffic to detect unexpected data bursts

within a very small time window (microseconds). Choose the sensitivity type from the **Microburst Sensitivity Level** drop-down list. The options are **High sensitivity**, **Medium sensitivity**, and **Low sensitivity**.

The **Enable Microburst sensitivity** option is available only for ACI fabrics.

- **Flow collection modes**—allows you to choose the mode for telemetry data collection. Modes include **NetFlow**, **sFlow**, and **Flow Telemetry**.

  For more information see: Flow collection and Configure flows.

- **Flow collection rules**—allows you to define rules for monitoring specific subnets or endpoints. These rules are pushed to the relevant devices, enabling detailed telemetry data collection.

  For more information, see Flow collection.

Edit NAS settings

Nexus Dashboard allows you to export captured flow records to a remote NAS device using the Network File System (NFS) protocol. Nexus Dashboard defines the directory structure on NAS where the flow records are exported.

You can choose between the two export modes.

- **Full**—exports the complete data for each flow record.
- **Base**—exports only the essential 5-tuple data for each flow record.

Nexus Dashboard needs both read and write permissions on the NAS to perform the export successfully. If Nexus Dashboard cannot write to the NAS, it will generate an alert to notify you of the issue.

Disable Telemetry

You can uncheck the **Telemetry** check box on your fabric's **Edit Fabric Settings > General >** page to disable the telemetry feature for your fabric. Disabling telemetry puts the telemetry feature in a transition phase and eventually the telemetry feature is disabled.

In certain situations, the disable telemetry workflow can fail, and you may see the **Force disable telemetry** option on your fabric's **Edit Fabric Settings** page.

If you disable the telemetry option using the instructions provided in [Perform force disable telemetry] on your fabric, Nexus Dashboard acknowledges the user intent to disable telemetry feature for your fabric, ignoring any failures.

The Nexus Dashboard **Force disable telemetry** allows you to perform a force disable action for the telemetry configuration on your fabric. This action is recommended when the telemetry disable workflow has failed and you need to disable the telemetry feature on your fabric.

Using the **Force disable telemetry** feature may leave switches in your fabric with stale telemetry configurations. You must manually clean up these stale

configurations on the switches before re-enabling telemetry on your fabric.

Perform force disable telemetry on your fabric

Follow these steps to perform a force disable telemetry on your fabric.

1. (Optional) Before triggering a force disable of telemetry configuration, resolve any telemetry configuration anomalies flagged on the fabric.
2. On the **Edit Fabric Settings** page of your fabric, a banner appears to alert you that telemetry cannot be disabled gracefully, and a **Force Disable** option is provided with the alert message.
3. Disable telemetry from the Nexus Dashboard UI using one of these options.
   a. Click the **Force disable** option in the banner that appears at the top of your fabric's **Edit Fabric Settings** page to disable telemetry for your fabric gracefully.
   b. Navigate to your fabric's **Overview** page and click the **Actions** drop-down list to choose **Telemetry > Force disable telemetry** option.

      Once the force disable action is executed, the **Telemetry** configuration appears as disabled in **Edit Fabric Settings > General > Enabled features > Telemetry** area, that is, the **Telemetry** check box is unchecked.
4. Clean up any stale telemetry configurations from the fabric before re-enabling telemetry on Nexus Dashboard.

NAS

You can export flow records captured by Nexus Dashboard on a remote Network Attached Storage (NAS) with NFS.

Nexus Dashboard defines the directory structure on NAS where the flow records are exported.

You can export the flow records in Base or Full mode. In Base mode, only 5-tuple data for the flow record is exported. In Full mode the entire data for the flow record is exported.

Nexus Dashboard requires read and write permission to NAS in order to export the flow record. A system issue is raised if Nexus Dashboard fails to write to NAS.

Guidelines and limitations for network attached storage

- In order for Nexus Dashboard to export the flow records to an external storage, the Network Attached Storage added to Nexus Dashboard must be exclusive for Nexus Dashboard.
- Network Attached Storage with Network File System (NFS) version 3 must be added to Nexus Dashboard.
- Flow Telemetry and Netflow records can be exported.
- Export of FTE is not supported.
- Average Network Attached Storage requirements for 2 years of data storage at 20k flows per sec:
  - Base Mode: 500 TB data

- Full Mode: 2.8 PB data

- If there is not enough disk space, new records will not be exported and an anomaly is generated.

Add network attached storage to export flow records

The workflow to add Network Attached Storage (NAS) to export flow records includes the following steps:

1. Add NAS to Nexus Dashboard.
2. Add the onboarded NAS to Nexus Dashboard to enable export of flow records.

Add NAS to Nexus Dashboard

Follow these steps to add NAS to Nexus Dashboard.

1. Navigate to **Admin** > **System Settings** > **General**.
2. In the **Remote storage** area, click **Edit**.
3. Click **Add Remote Storage Locations**.
4. Complete the following fields to add NAS to Nexus Dashboard.
   a. Enter the name of the Network Attached Storage and a description, if desired.
   b. In the **Remote storage location type** field, click **NAS Storage**.
   c. In the **Type** field, choose **Read Write**.

      Nexus Dashboard requires read and write permission to export the flow record to NAS. A system issue is raised if Nexus Dashboard fails to write to NAS.

   d. In the **Hostname** field, enter the IP address of the Network Attached Storage.
   e. In the **Port** field, enter the port number of the Network Attached Storage.
   f. In the **Export path** field, enter the export path.

      Using the export path, Nexus Dashboard creates the directory structure in NAS for exporting the flow records.

   g. In the **Alert threshold** field, enter the alert threshold time.

      Alert threshold is used to send an alert when the NAS is used beyond a certain limit.

   h. In the **Limit (Mi/Gi)** field, enter the storage limit in Mi/Gi.
   i. Click **Save**.

Add the onboarded NAS to Nexus Dashboard

Follow these steps to add the onboarded NAS to Nexus Dashboard.

1. Navigate to the Fabrics page:

   Manage > Fabrics

2. Choose the fabric with the telemetry feature enabled.
3. Choose **Actions > Edit Fabric Settings**.
4. Click **Telemetry**.
5. Click the **NAS** tab in the **Telemetry** window.
6. Make the necessary configurations in the **General settings** area.
   a. Enter the name in the **Name** field.
   b. In the **NAS server** field, choose the NAS server added to Nexus Dashboard from the drop-down list.
7. In the **Collection settings** area, choose the flow from the **Flows** drop-down list.
   - In Base mode, only 5-tuple data for the flow record is exported.
   - In Full mode, the entire data for the flow record is exported.
8. Click **Save**.

The traffic from the flows displayed in the **Flows** page is exported as a JSON file to the external NAS in the following directory hierarchy.

```
└── NDI-<VERSION>-FLOW-JSON/
    └── fabricName=<fabricName>/
        └── year=2022/
            ├── month=01/
            │   └── date=01/
            │       ├── hour=01/
            │       │   ├── 52170795-0b94-481c-800a-c47f0fa41fac.json
            │       │   └── fa92c70c-96fc-4e32-ac76-324bdd5139d4.json
            │       └── hour=23/
            │           ├── 737f4292-bf29-4630-bdd9-ccb80885ddc1.json
            │           └── 68b434d9-0957-4fe4-be01-e0688cb4336d.json
            └── month=02/
                └── date=20/
                    ├── hour=10/
                    │   ├── e05ce8fb-88af-45db-8c52-4b00e1841b16.json
                    │   └── 6fd2b652-dfe1-430e-905a-020abd399e3e.json
                    └── hour=23/
                        ├── eeb6784a-33a0-4ae3-b13e-db4db93fe48b.json
                        └── b289c75e-a709-4284-a018-b38ab101d90f.json
```

Navigate to **Analyze** > **Flows** to view the flows that will be exported.

Each flow record is written as a line delimited JSON.

JSON output file format for a flow record in base mode

{" fabricName" :" myapic" ," terminalTs" :1688537547433," originTs" :1688537530376," srcIp" :" 2000:201:1:1::1" ," dstIp" :" 2000:201:1:1::3" ," srcPort" :1231," dstPort" :1232," ingressVrf" :" vrf1" ," egressVrf" :" vrf1" ," ingressTenant" :" FSV1" ," egressTenant" :" FSV1" ," protocol" :" U

DP" }

{" fabricName" :" myapic" ," terminalTs" :1688537547378," originTs" :1688537530377," srcIp" :" 201.1.1.127" ," dstIp" :" 201.1.1.1" ," srcPort" :0," dstPort" :0," ingressVrf" :" vrf1" ," egressVrf " :" " ," ingressTenant" :" FSV2" ," egressTenant" :" " ," protocol" :" ANY-HOST" }

JSON output file format for a flow record in full mode

{" fabricName" :" myapic" ," terminalTs" :1688538023562," originTs" :1688538010527," srcIp" :" 201.1.1.121" ," dstIp" :" 201.1.1.127" ," srcPort" :0," dstPort" :0," ingressVrf" :" vrf1" ," egress Vrf" :" vrf1" ," ingressTenant" :" FSV2" ," egressTenant" :" FSV2" ," protocol" :" ANY-HOST" ," srcEpg" :" ext-epg" ," dstEpg" :" ext-epg1" ," latencyMax" :0," ingressVif" :" eth1/15" ," ingressVni" :0," latency" :0," ingressNodes" :" Leaf1-2" ," ingressVlan" :0," ingressByteCount" :104681600," ingressPktCount" :817825," ingressBurst" :0," ingressBurstMax" :34768," egressNodes" :" Leaf1-2" ," egressVif" :" po4" ," egressVni" :0," egressVlan" :0," egressByteCount" :104681600," egressPktCount" :817825," egressBurst" :0," egressBurstMax" :34768," dropPktCount" :0," dropByteCount" :0," dropCode " :" " ," dropScore" :0," moveScore" :0," latencyScore" :0," burstScore" :0," anomalyScore" :0," hashCollision" :false," dropNodes" :" []" ," nodeNames" :" [\" Leaf1-2\"]" ," nodeIngressVifs" :" [\" Leaf1-2,eth1/15\"]" ," nodeEgressVifs" :" [\" Leaf1-2,po4\"]“ ," srcMoveCount" :0," dstMoveCount" :0," moveCount" :0," prexmit" :0," rtoOutside" :false," events" :" [[\\\" 1688538010527,Leaf1-2,0,3,1,no,no,eth1/15,,po4,po4,,,,,0,64,0,,,,,,,,\\\"]]" }

Flow collection

Understanding flow telemetry

Flow telemetry allows users to see the path taken by different flows in detail. It also allows you to identify the EPG and VRF instance of the source and destination. You can see the switches in the flow with the help of flow table exports from the nodes. The flow path is generated by stitching together all the exports in order of the flow.

You can configure the Flow Telemetry rule for the following interface types:

- VRF instances
- Physical interfaces
- Port channel interfaces
- Routed sub-interfaces (Cisco ACI fabric)
- SVIs (Cisco ACI fabric)

In a Cisco ACI fabric, if you want to configure routed sub-interfaces from the UI, select L3 Out.

> In an NX-OS fabric, physical or port channel flow rules are supported only on routed interfaces.

Flow telemetry monitors the flow for each fabric separately, as there is no stitching across the fabrics in a fabric group. Therefore, flow telemetry is for individual flows. For example, if there are two fabrics (fabric A and fabric B) within a fabric group, and traffic is flowing between the two fabrics, they will be displayed as two separate flows. One flow will originate from Fabric A and display where the flow exits. And the other flow from Fabric B will display where it enters and where it exits.

Flow telemetry guidelines and limitations

- All flows are monitored as a consolidated view in a unified pipeline for Cisco ACI and NX-OS fabrics, and the flows are aggregated under the same umbrella.
- Even if a particular node (for example, a third-party switch) is not supported for Flow Telemetry, Nexus Dashboard will use LLDP information from the previous and next nodes in the path to identify the switch name and the ingress and egress interfaces.
- Nexus Dashboard supports Kafka export for Flow anomalies. However, Kafka export is not currently supported for Flow Event anomalies.

Flow telemetry guidelines and limitations for NX-OS fabrics

- Ensure that you have configured NTP and enabled PTP in Nexus Dashboard. See Cisco Nexus Dashboard Deployment Guide and Precision Time Protocol (PTP) for Cisco Nexus Dashboard Insights for more information. You are responsible for configuring the switches with external NTP servers.
- In the **Edit Flow** page, you can enable all three telemetry types. sFlow is most restrictive, Netflow has some more capability, and Flow Telemetry has the most capability. We recommend that you enable Flow Telemetry if it is available for your configuration. If Flow Telemetry is not available, then use Netflow. If Netflow is not available, use sFlow.
- If there are multiple Nexus Dashboard clusters onboarded to Nexus Dashboard, partial paths will be generated for each fabric.
- If you manually configure the fabric to use with Nexus Dashboard and Flow Telemetry support, the Flows Exporter port changes from 30000 to 5640. To prevent a breakage of the Flows Exporter, adjust the automation.
- Nexus Dashboard supports Kafka export for Flow anomalies. However, Kafka export is not currently supported for Flow Event anomalies.
- Flow telemetry is supported in -FX3 platform switches for the following NX-OS versions:
  - 9.3(7) and later
  - 10.1(2) and later
  - Flow telemetry is not supported in -FX3 platform switches for NX-OS version 10.1(1).
- Interface based Flow Telemetry is only supported on modular chassis with -FX land -GX line cards on physical ports and port-channels rules.
- If interface-based Flow Telemetry is pushed from Nexus Dashboard for **Classic LAN** and **External Connectivity Network** fabrics, perform the following steps:
  - Choose the fabric.

    - Choose **Policies** > **Action** > **Add policy** > **Select all** > **Choose template** > host_port_resync and click **Save**.
    - In the Fabric Overview page, choose **Actions** > **Recalculate and deploy**.
- For VXLAN fabrics, interface-based Flow Telemetry is not supported on switch links between spine switch and leaf switch.
- If you want to use the default VRF instance for flow telemetry, you must create the VRF instance with a name of " default" in lowercase. Do not enter the name with any capital letters.
- Flow telemetry is not supported in classic LAN topologies with 2-level VPC access layers.
- If you want to enable Flow Telemetry, ensure that there are no pre-existing Netflow configurations on the switches. If there are any pre-existing configurations, the switch configuration may fail.

  To enable Flow Telemetry without configuration issues, follow these steps:

    - Ensure that there are no pre-existing Netflow configurations on the switches. If such configurations exist, enabling Flow Telemetry might result in a system anomaly with an error message stating invalid command match IP source address.
    - If you encounter the error, disable Flow Telemetry.
    - Remove any existing Netflow configurations from the switches.
    - Re-enable Flow Telemetry.
    - For some flows, latency information is not available, which could happen due to latency issues. In these cases, latency information will be reported as 0.

Flow telemetry rules guidelines and limitations for NX-OS fabrics

- If you configure an interface rule (physical or port channel) on a subnet, it can monitor only incoming traffic. It cannot monitor outgoing traffic on the configured interface rule.
- If a configured port channel that contains two physical ports, only the port channel rule is applicable. Even if you configure physical interface rules on the port, only port channel rule takes precedence.
- For NX-OS release 10.3(2) and earlier, if a flow rule are configured on an interface, then global flow rules are not matched.
- For NX-OS release 10.3(3) and later, a flow rule configured on an interface is matched first and then the global flow rules are matched.

Configure flows

Configure flow collection modes

Follow these steps to configure flow collection modes.

1. Navigate to **Admin** > **System Settings** > **Flow collection**.
2. In the **Flow collection mode** area, choose **Flow telemetry**.

Enabling Flow Telemetry automatically activates Flow Telemetry Events. Whenever a compatible event takes place, an anomaly will be generated, and the What's the impact? section in the **Anomaly** page will display the associated flows. You can

> manually configure a Flow Telemetry rule to acquire comprehensive end-to-end information about the troublesome flow.

Configure flow collection rules in an NX-OS fabric

Follow these steps to configure flow collection rules in an NX-OS fabric.

1. Navigate to the **Telemetry** window for your fabric.
   a. Navigate to the main **Fabrics** page:

      Manage > Fabrics

   b. In the table showing all of the Nexus Dashboard fabrics that you have already created, locate the LAN or IPFM fabric where you want to configure telemetry settings.
   c. Single-click on that fabric.

      The **Overview** page for that fabric appears.

   d. Click **Actions > Edit Fabric Settings**.

      The **Edit *fabric_name* Settings** window appears.

   e. Verify that the **Telemetry** option is enabled in the **Enabled features** area.

      The Telemetry tab doesn't become available unless the **Telemetry** option is enabled in the **Enabled features** area.

   f. Click the **Telemetry** tab to access the telemetry settings for this fabric.
2. Click the **Flow collection** tab in the **Telemetry** window.
3. In the **Mode** area, click **Flow telemetry**.
4. In the **Flow collections rules** area, determine what sort of flow collection rule that you want to add.
   - VRF
   - Physical interface
   - Port channel

VRF

To add a VRF rule:

1. Click the **VRF** tab.

   A table with already-configured VRF flow collection rules is displayed.

   For any VRF flow collection rule in this table, click the ellipsis (...), then click **Edit rule** to edit that rule or **Delete rule** to delete it.

2. Add a new rule by clicking **Create flow collection rule**.
   a. In the **General** area, complete the following:

i. Enter the name of the rule in the **Rule Name** field.

ii. The VRF field is disabled. The flow rule applies to all the VRF instances.

iii. In the **Flow Properties** area, select the protocol for which you intend to monitor the flow traffic.

iv. Enter the source and destination IP addresses. Enter the source and destination port.

v. Click **Save**.

Physical interface

To add a physical interface rule:

1. Click the **Physical interface** tab.

   A table with already-configured physical interface flow collection rules is displayed.

   For any physical interface flow collection rule in this table, click the ellipsis (...), then click **Edit rule** to edit that rule or **Delete rule** to delete it.

2. Add a new rule by clicking **Create flow collection rule**.
   a. In the **General** area, complete the following:
      i. Enter the name of the rule in the **Rule Name** field.
      ii. Check the **Enabled** check box to enable the status. If you enable the status, the rule will take effect. Otherwise, the rule will be removed from the switches.
      iii. In the **Flow Properties** area, select the protocol for which you intend to monitor the flow traffic.
      iv. Enter the source and destination IP addresses. Enter the source and destination port.
      v. In the **Interface List** area, click **Select a Node**. Use the search box to select a node.
      vi. From the drop-down list, select an interface. You can add more than one row (node+interface combination) by clicking **Add Interfaces**. However, within the rule, a node can appear only once. Configuration is rejected if more than one node is added.
      vii. Click **Save**.

Port channel

To add a port channel rule:

1. Click the **Port channel** tab.

   A table with already-configured port channel flow collection rules is displayed.

   For any port channel flow collection rule in this table, click the ellipsis (...), then click **Edit rule** to edit that rule or **Delete rule** to delete it.

2. Add a new rule by clicking **Create flow collection rule**.
   a. In the **General** area, enter the name of the rule in the **Rule Name** field.
      i. Select the **Enabled** check box to enable the status. If you enable the status, the rule will take effect. Otherwise, the rule will be removed from the switches.

ii. In the **Flow Properties** area, select the protocol for which you intend to monitor the flow traffic.

iii. Enter the source and destination IP addresses. Enter the source and destination port.

iv. From the drop-down list, select an interface. You can add more than one row (node+interface combination) by clicking **Add Interfaces**. However, within the rule, a node can appear only once. Configuration is rejected if more than one node is added.

v. Click **Save**.

3. Click **Done**.

Monitor the subnet for flow telemetry

In the following example, the configured rule for a flow monitors the specific subnet provided. The rule is pushed to the fabric which pushes it to the switches. So, when the switch sees traffic coming from a source IP or the destination IP, and if it matches the subnet, the information is captured in the TCAM and exported to the Nexus Dashboard service. If there are 4 nodes (A, B, C, D), and the traffic moves from A > B > C > D, the rules are enabled on all 4 nodes and the information is captured by all the 4 nodes. Nexus Dashboard stitches the flows together. Data such as the number of drops and the number of packets, anomalies in the flow, and the flow path are aggregated for the 4 nodes.

Follow these steps to monitor the subnet for flow telemetry.

1. Navigate to **Manage** > **Fabric**.
2. Choose a fabric.
3. Verify that your **Fabrics** and the **Snapshot** values are appropriate. The default snapshot value is 15 minutes. Your choice will monitor all the flows in the chosen fabric or snapshot fabric.
4. Navigate to **Connectivity** > **Flows** to view a summary of all the flows that are being captured based on the snapshot that you chose.

The related anomaly score, record time, the nodes sending the flow telemetry, flow type, ingress and egress nodes, and additional details are displayed in a table format. If you click a specific flow in the table, specific details are displayed in the sidebar for the particular flow telemetry. In the sidebar, if you click the Details icon, the details are displayed in a larger page. In this page, in addition to other details, the **Path Summary** is also displayed with specifics related to source and destination. If there are flows in the reverse direction, that will also be visible in this location.

For a bi-directional flow, there is an option to choose to reverse the flow and see the path summary displayed. If there are any packet drops that generate a flow event, they can be viewed in the Anomaly dashboard.

Understanding Netflow

Netflow is an industry standard where Cisco routers monitor and collect network traffic on an interface. Netflow version 9 is supported.

Netflow enables the network administrator to determine information such as source, destination, class of service, and causes of congestion. Netflow is configured on the interface to monitor every packet on the interface and provide telemetry data. You cannot filter on Netflow.

Netflow in Nexus series switches is based on intercepting the packet processing pipeline to capture summary information of network traffic.

The components of a flow monitoring setup are as follows:

- Exporter: Aggregates packets into flows and exports flow records towards one or more collectors
- Collector: Reception, storage, and pre-processing of flow data received from a flow exporter
- Analysis: Used for traffic profiling or network intrusion
- The following interfaces are supported for Netflow:

Supported interfaces for Netflow

Interfaces	5 Tuple	Nodes	Ingress	Egress	Path	Comments
Routed Interface/Port Channel	Yes	Yes	Yes	No	Yes	Ingress node is shown in path
Sub Interface/Logical (Switch Virtual Interface)	Yes	Yes	No	No	No	No

In an NX-OS fabric, port channel support is available if you monitor only the host-facing interfaces.

Understanding Netflow types

You can use these Netflow types.

Full Netflow

With Full Netflow, all packets on the configured interfaces are captured into flow records in a flow table. Flows are sent to the supervisor module. Records are aggregated over configurable intervals and exported to the collector. Except in the case of aliasing (multiple flows hashing to the same entry in the flow table), all flows can be monitored regardless of their packet rate.

Nexus 9000 Series switches with the Fabric Controller type as well as switches in a Cisco ACI fabric support Full Netflow.

Sampled Netflow

With Sampled Netflow, packets on configured interfaces are time sampled. Flows are sent to the supervisor or a network processor for aggregation. Aggregated flow records are exported at configured intervals. The probability of a record for a flow being captured depends on the sampling frequency and packet rate of the flow relative to other flows on the same interface.

Nexus 7000 and Nexus 7700 Series switches with F/M line cards and the Fabric Controller type, support Sampled Netflow.

Netflow guidelines and limitations

- In Cisco Nexus 9000 series switches, Netflow supports a small subset of the published export fields in the RFC.
- Netflow is captured only on the ingress port of a flow as only the ingress switch exports the flow. Netflow cannot be captured on fabric ports.
- You must configure persistent IP addresses under the cluster configuration, including 7 IP addresses in the same subnet as the data network.

Netflow guidelines and limitations for Cisco ACI fabrics

- We recommend that you enable Flow Telemetry. If that is not available for your configuration, use Netflow. However, you can determine which mode of flow to use based upon your fabric configuration.
- Enabling both Flow Telemetry and Netflow is not supported.
- After you enable Netflow, you must obtain the Netflow collector IP address and configure Cisco APIC with the collector IP address. See Cisco APIC and NetFlow.

  To obtain the Netflow collector IP address, navigate to **Admin** > **System Settings** > **Flow collection**. In the **Flow Collection per Fabric** table, click **View** in the **Collector List** column.

- The Netflow and sFlow flow collection modes do not support any anomaly.

Netflow guidelines and limitations for NX-OS fabrics

- In the **Edit Flow** page, you can enable all three modes. Choose the best possible mode for a product. sFlow is the most restrictive, Netflow has more capabilities, and Flow Telemetry has the most capabilities. We recommend that you enable Flow Telemetry if it is available for your configuration. If Flow Telemetry is not available, then use Netflow. If Netflow is not available, use sFlow.
- In Nexus 7000 and Nexus 9000 Series switches, only the ingress host-facing interface configured for Netflow are supported (either in VXLAN or Classic LAN).
- The Netflow supported fabrics are Classic and VXLAN. VXLAN is not supported on fabric ports.
- Netflow configurations will not be pushed. However, if a fabric is managed, the software sensors will be pushed.
- If you manually configure the fabric to use with Nexus Dashboard and Netflow support, the Flows Exporter port changes from 30000 to 5640. To prevent a breakage of the Flows Exporter, adjust the automation.

- To configure Netflow on fabric switches, see the **Configuring Netflow** section in the Cisco Nexus 9000 Series NX-OS System Management Configuration Guide.

Configure Netflow

Follow these steps to configure Netflow.

1. Navigate to the **Telemetry** page for your LAN or IPFM fabric.
2. Click the **Flow collection** tab on the **Telemetry** page.
3. In the **Mode** area, make the following choices:
    - Choose **Netflow**.
    - Choose **Flow Telemetry**.
4. Click **Save**.

Understanding sFlow

sFlow is an industry standard technology traffic in data networks containing switches and routers. Nexus Dashboard supports sFlow version 5 on Cisco Nexus 3000 series switches.

sFlow provides the visibility to enable performance optimization, an accounting and billing for usage, and defense against security threats.

The following interfaces are supported for sFlow:

Supported interfaces for sFlow

Interfaces	5 Tuple	Nodes	Ingress	Egress	Path	Comments
Routed Interface	Yes	Yes	Yes	Yes	Yes	Ingress node is shown in path

Guidelines and limitations for sFlow

- Nexus Dashboard supports sFlow with Cisco Nexus 3000 series switches.
- It is recommended to enable Flow Telemetry if it is available for your configuration. If it is not available for your configuration, use Netflow. If Netflow, is not available for your configuration, then use sFlow.
- For sFlow, Nexus Dashboard requires the configuration of persistent IPs under cluster configuration, and 6 IPs in the same subnet as the data network are required.
- sFlow configurations will not be pushed. However, if a fabric is managed, the software sensors will be pushed.
- If you manually configure the fabric to use with Nexus Dashboard and sFlow support, the Flows Exporter port changes from 30000 to 5640. To prevent a breakage of the Flows Exporter, adjust the automation.
- Nexus Dashboard does not support sFlow in the following Cisco Nexus 3000 Series switches:
  - Cisco Nexus 3600-R Platform Switch (N3K-C3636C-R)
  - Cisco Nexus 3600-R Platform Switch (N3K-C36180YC-R)
  - Cisco Nexus 3100 Platform Switch (N3K-C3132C-Z)
- Nexus Dashboard does not support sFlow in the following Cisco Nexus 9000 Series fabric modules:
  - Cisco Nexus 9508-R fabric module (N9K-C9508-FM-R)
  - Cisco Nexus 9504-R fabric module (N9K-C9504-FM-R)
- To configure sFlow on fabric switches, see the **Configuring sFlow** section in the Cisco Nexus 9000 Series NX-OS System Management Configuration Guide.

Configure sFlow telemetry

Prerequisites

Follow these steps to configure sFlow telemetry.

1. Navigate to the **Telemetry** page for your LAN or IPFM fabric.
2. Click the **Flow collection** tab on the **Telemetry** page.
3. In the **Mode** area, make the following choices:
    - Choose **sFlow**.
    - Choose **Flow Telemetry**.
4. Click **Save**.

External streaming

The **External streaming** tab in Nexus Dashboard allows you export data that Nexus Dashboard collects over Kafka, email, and syslog. Nexus Dashboard generates data such as advisories, anomalies, audit logs, faults, statistical data, and risk and conformance reports. When you configure a Kafka broker, Nexus Dashboard writes all data to a topic. By default, the Nexus Dashboard collects export data every 30 seconds or at a less frequent interval.

For ACI fabrics, you can also collect data for specific resources (CPU, memory, and interface utilization) every 10 seconds from the leaf and spine switches using a separate data pipeline. To export this data, select the **Usage** option under **Collection Type** in the **Message bus** export settings. Additionally, CPU and memory data is collected for the controllers.

Nexus Dashboard does not store the collected data in Elasticsearch; instead, it exports the data directly to your repository or data lake using a Kafka broker for consumption. By using the Kafka export functionality, you can then export this data to your Kafka broker and push it into your data lake for further use.

You can configure an email scheduler to define the type of data and the frequency at which you want to receive information via email. You can also export anomaly records to an external syslog server. To do this, select the **Syslog** option under the **External Streaming** tab.

Configure external streaming settings

Follow these steps to configure external streaming settings.

1. Navigate to the **Fabrics** page.

   Go to **Manage > Fabrics**.

2. Choose the fabric for which you configure streaming settings.
3. From the **Actions** drop-down list, choose **Edit fabric settings**.

   The **Edit *fabric-name* settings** page displays.

   You can also access the **Edit *fabric-name* settings** page for a fabric from the **Fabric Overview** page. In the **Fabric Overview** page, click the **Actions** drop-down list and choose **Edit fabric settings**.

4. In the **Edit *fabric-name* settings** page, click the **External streaming** tab.

   You can view these options.

   - Email
   - Message bus
   - Syslog

Guidelines and limitations

- Intersight connectivity is required to receive the reports by email.
- You can configure up to five emails per day for periodic job configurations.
- A maximum of six exporters is supported for export across all types of exporters including email, message bus, and syslog. You must provide unique names for each export.
- The scale for Kafka exports is increased to support up to 20 exporters per cluster. However, statistics selection is limited to any six exporters.
- Before configuring your Kafka export, you must add the external Kafka IP address as a known route in your Nexus Dashboard cluster configuration and verify that Nexus Dashboard can reach the external Kafka IP address over the network.
- The anomalies in Kafka and email messages include categories such as Resources, Environmental, Statistics, Endpoints, Flows, and Bugs.
- Export data is not supported for snapshot fabrics.
- You must provide unique names for each exporter, and they may not be repeated between Kafka export for **Alerts and Events** and Kafka export for **Usage**.
- Nexus Dashboard supports Kafka export for flow anomalies. However, Kafka export is not currently supported for flow Event anomalies.

Guidelines and limitations in NX-OS fabrics

- Remove all configurations in the *Message Bus Configuration* and *Email* page before you disable Software Telemetry on any fabric and remove the fabric from Nexus Dashboard.

Email

The email scheduler feature in Nexus Dashboard automates the distribution of summarized data collected from Nexus Dashboard. It allows customization of selection of email recipients, choice of email format, scheduling frequency settings, and configuring the types of alerts and reports.

To configure email at the system settings level, see [Add email configuration].

Follow these steps to configure an email scheduler.

1. Navigate to the **Fabrics** page.

   Go to **Manage > Fabrics**.

2. Choose the fabric for which you configure streaming settings.
3. From the **Actions** drop-down list, choose **Edit fabric settings**.

   The **Edit *fabric-name* settings** page displays.

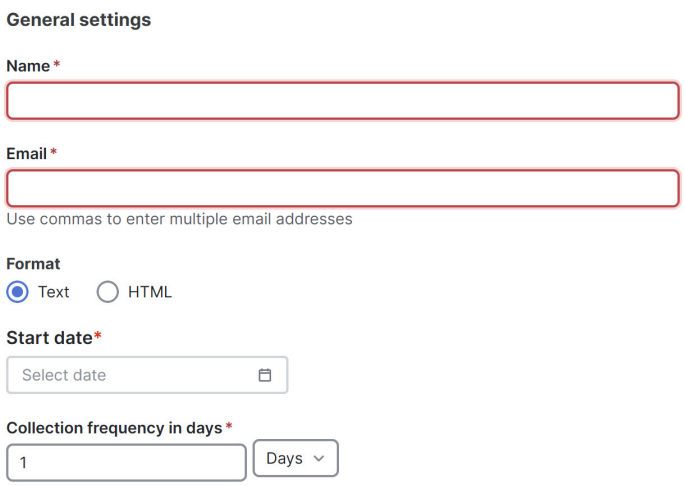
4. In the **Edit *fabric-name* settings** page, click the **External streaming** tab.
5. Click the **Email** tab.
6. Review the information provided in the **Email** tab for already-configured email configurations.

The following details display under **Email** tab.

Field	Description
Name	The name of the email configuration.
Email	The email addresses used in the email configuration.
Start time	The start date used in the email configuration.
Frequency	The frequency in days or weeks set in the email configuration.
Anomalies	The severity level for anomalies and advisories set in the email configuration.
Advisories	
Risk and conformance reports	The status of the overall inventory for a fabric, including software release, hardware platform, and a combination of software and hardware conformance.

To add a new email configuration, click **Add email** in the **Email** page.

1. Follow these steps to configure **General** Settings.
   a. In the **Name** field, enter the name of the email scheduler.
   b. In the **Email** field, enter one or more email addresses separated by commas.
   c. In the **Format** field, choose **Text** or **HTML** email format.
   d. In the **Start date** field, choose the start date when the scheduler should begin sending emails.
   e. In the **Collection frequency in days** field, specify how often the summary is sent, you can choose days or weeks.



2. Follow these steps to configure **Collection Settings**.
   a. In the **Mode** field, choose one of the following modes.
      - **Basic**—displays the severity levels for anomalies and advisories.
      - **Advanced**—displays the categories and severity levels for anomalies and advisories.
   b. Check the **Only include active alerts in email** check box, to include only active anomaly alerts.
   c. Under **Anomalies** choose the categories and severity levels for the anomalies.

d. Under **Advisories** choose the categories and severity levels for the advisories.

e. Under **Risk and Conformance Reports**, choose from the following options.

- Software
- Hardware

3. Click **Save**.

   The **Email** area displays the configured email schedulers.

You will receive an email about the scheduled job on the provided *Start Date* and at the time provided in the **Collection frequency in days** field. The subsequent emails follow after *Collect Every* frequency expires. If the provided time is in the past, Nexus Dashboard will send you an email immediately and trigger the next email after the duration from the provided start time expires.

Message bus

Add Kafka broker configuration

Follow these steps to configure the message bus and add kafka broker.

1. Configure the message bus at the **System Settings** level.
   a. Navigate to **Admin** > **System Settings** > **General**.
   b. In the **Message bus configuration** area, click **Edit**.

      The **Message bus configuration** dialog box opens.

   c. Click **Add message bus configuration**.

      The **Add message bus configuration** dialog box opens.

   d. In the **Name** field, enter a name for the configuration.
   e. In the **Hostname/IP address** and **Port** fields, enter the IP address of the message bus consumer and the port that is listening on the message bus consumer.

f. In the **Topic name** field, enter the name of the Kafka topic to which Nexus Dashboard must send the messages.

g. In the **Mode** field, choose the security mode.

The supported modes are **Unsecured**, **Secured SSL** and **SASLPLAIN**. The default value is **Unsecured**.

- For **Unsecured**, no other configurations are needed.
- For **Secured SSL**, fill out the following field:

Client certification name—The System Certificate name configured at the Certificate Management level. The CA certificate and System Certificate (which includes Client certificate and Client key) are added at the Certificate Management level.

Refer to Step 2 for step-by-step instructions on managing certificates. Navigate to **Admin** > **Certificate Management** to manage the following certificates:

- **CA Certificate**—The CA certificate used for signing consumer certificate, which will be stored in the trust-store so that Nexus Dashboard can trust the consumer.
- **Client Certificate**—The CA signed certificate for Nexus Dashboard. The certificate is signed by the same CA, and the same CA certificate will be in the truststore of the consumer. This will be stored in Nexus Dashboard's Kafka keystore that is used for exporting.
- **Client Key**—A private key for the Kafka producer, which is Nexus Dashboard in this case. This will be stored in Nexus Dashboard's Kafka keystore that is used for exporting.

- For **SASLPLAIN**, fill out these fields:

- **Username**—The username for the SASL/PLAIN authentication.
- **Password**—The password for the SASL/PLAIN authentication.

h. Click **Save**

2. Add CA certificates and System certificates at the **Certificate Management level**.

a. Navigate to **Admin** > **Certificate Management**.

b. In the **Certificate management** page, click the **CA Certificates** tab, then click **Add CA certificate**.

The fields in the **CA Certificates** tab are described in the following table.

Field	Description
Certificate name	The name of the CA certificate.
Certificate details	The details of the CA certificate.
Attached to	The CA signed certificate attached to Nexus Dashboard.
Expires on	The Expiry date and time of the CA certificate.

Field	Description
Last updated time	The last updated time of the CA certificate.

c. In the **Certificate management** page, click the **System certificates** tab, then click **Add system certificate** to add Client Certificate and Client key. Note that the Client certificate and Client key should have same names except extensions as .cer/.crt/.pem for Client certificate and .key for Client key.

You must add a valid CA Certificate before adding the corresponding System Certificate.

The fields in the **System Certificates** tab are described in the following table.

Field	Description
Certificate name	The name of the Client certificate.
Certificate details	The details of the Client certificate.
Attached to	The feature to which the system certificate is attached to, in this case, the message bus.
Expires on	The Expiry date and time of the CA certificate.
Last updated time	The last updated time of the CA certificate.

To configure message bus, the System Certificate should be attached to message bus feature.

To attach a System Certificate to the message bus feature:

a. Choose the System Certificate that you want to use and click the ellipses (...) on that row.

b. Choose **Manage Feature Attachments** from the drop-down list.

The **Manage Feature Attachments** dialog box opens.

c. In the **Features** field, choose **messageBus**.

d. Click **Save**.

For more information on CA certificates, see Managing Certificates in your Nexus Dashboard.

Configure Kafka exports in fabric settings

1. Navigate to the **External streaming** page for your fabric.

   a. Navigate to the **Fabrics** page.

   Go to **Manage > Fabrics**.

   b. Choose the fabric for which you configure streaming settings.

   c. From the **Actions** drop-down list, choose **Edit fabric settings**.

   The **Edit *fabric-name* settings** page displays.

d. In the **Edit *fabric-name* settings** page, click the **External streaming** tab.

e. Click the **Message bus** tab.

2. Review the information provided in the **Message bus** tab for already-configured message bus configurations, or click **Add message bus** to add a new message bus configuration.

   Skip to Step 3 if you are adding a message bus.

   The fields in the **Message bus** tab are described in the following table.

Field	Description
Message bus stream	The name of the message bus stream configuration.
Collection type	The collection type used by the message bus stream.
Mode	The mode used by the message bus stream.
Anomalies	The severity level for anomalies and advisories set in the message bus stream configuration.
Advisories	
Statistics	The statistics that were configured for the message bus stream.
Faults	The severity level for faults set in the message bus stream configuration.
Audit Logs	The audit logs that were configured for the message bus stream.

3. To configure a new message bus stream, in the **Message bus** page, click **Add message bus**.
4. In the **Message bus stream** field, choose the message bus stream that you want to edit.
5. In the **Collection Type** area, choose the appropriate collection type.

   Depending on the **Collection Type** that you choose, the options displayed in this area will change.

   - **Alerts and events**: This is the default setting. Continue to Step 7, if you choose **Alerts and events**.
   - **Usage**: In the **Collection settings** area, under **Data**, the Resources, and Statistics for the collection settings are displayed. By default, the data for CPU, Memory, and Interface Utilization are collected and exported. You cannot choose to export a subset of these resources.

     Usage is applicable only for ACI Fabrics. This option is disabled for other fabrics.

6. Click **Save**. The configured message bus streams are displayed in the **Message bus** area. This configuration now sends immediate notification when the selected anomalies or advisories occur.
7. If you choose **Alerts and events** as the **Collection Type**, in the **Mode** area, choose either **Basic** or **Advanced**.

   The configurations that are available in each collection settings section might vary, depending on the mode that you set.

8. Determine which area you want to configure for the message bus stream.

   The following areas appear in the page:

- Anomalies
- Advisories
- Statistics
- Faults
- Audit Logs

After you complete the configurations on this page, click **Save**. Nexus Dashboard displays the configured message bus streams in the **Message bus** area. This configuration now sends immediate notification when the selected anomalies or advisories occur.

Anomalies

- If you chose **Basic** in the **Mode** area, choose one or more of the following severity levels for anomaly statistics that you want to configure for the message bus stream:
  - Critical
  - Major
  - Warning
  - Minor

  Or click **Select all** to select all available statistics for the message bus stream.
- If you chose **Advanced** in the **Mode** area:
  - Choose one or more of the following categories for anomaly statistics that you want to configure for the message bus stream:
    - Active Bugs
    - Capacity
    - Compliance
    - Configuration
    - Connectivity
    - Hardware
    - Integrations
    - System
  - Choose one or more of the following severity levels for anomaly statistics that you want to configure for the message bus stream:
    - Critical
    - Major
    - Warning
    - Minor

    Or click **Select all** to select all available categories and statistics for the message bus stream.

  For more information on anomaly levels, see Detecting Anomalies and Identifying Advisories in Your Nexus Dashboard.

Advisories

- If you chose **Basic** in the **Mode** area, choose one or more of the following severity levels for advisory statistics that you want to configure for the message bus stream:
    - Critical
    - Major
    - Warning
    - Minor

  Or click **Select all** to select all available statistics for the message bus stream.
- If you chose **Advanced** in the **Mode** area:
    - Choose one or more of the following categories for advisory statistics that you want to configure for the message bus stream:
        - Best Practices
        - Field Notices
        - HW end-of-life
        - SW end-of-life
        - PSIRT
    - Choose one or more of the following severity levels for advisory statistics that you want to configure for the message bus stream:
        - Critical
        - Major
        - Warning
        - Minor

      Or click **Select all** to select all available categories and statistics for the message bus stream.

  For more information on advisory levels, see Detecting Anomalies and Identifying Advisories in Your Nexus Dashboard.

Statistics

There are no differences in the settings in the **Statistics** area when you choose **Basic** or **Advanced** in the **Mode** area.

Choose one or more of the following categories for statistics that you want to configure for the message bus stream:

- Interfaces
- Protocol
- Resource Allocation
- Environmental
- Endpoints

Faults

There are no differences in the settings in the **Faults** area when you choose **Basic** or **Advanced** in the **Mode** area.

Choose one or more of the following severity levels for fault statistics that you want to configure for the message bus stream:

- Critical
- Major
- Minor
- Warning
- Info

Audit Logs

There are no differences in the settings in the **Audit Logs** area when you choose **Basic** or **Advanced** in the **Mode** area.

Choose one or more of the following categories for audit logs that you want to configure for the message bus stream:

- Creation
- Deletion
- Modification

Syslog

Nexus Dashboard supports the export of anomalies in syslog format. You can use the syslog configuration feature to develop network monitoring and analytics applications on top of Nexus Dashboard, integrate with the syslog server to get alerts, and build customized dashboards and visualizations.

After you choose the fabric where you want to configure the syslog exporter and set up the syslog export configuration, Nexus Dashboard establishes a connection with the syslog server and sends data to the syslog server.

Nexus Dashboard exports anomaly records to the syslog server. With syslog support, you can export anomalies to your third-party tools even if you do not use Kafka.

Guidelines and limitations for syslog

If the syslog server is not operational at a certain time, messages generated during that downtime will not be received by a server after the server becomes operational.

Add syslog server configuration

Follow these steps to add syslog server configuration.

1. Navigate to **Admin > System Settings > General**.
2. In the **Remote streaming servers** area, click **Edit**.

   The **Remote streaming servers** page displays.
3. Click **Add server**.

   The **Add server** page displays.
4. Choose the **Service** as **Syslog**.
5. Choose the **Protocol**.

   You have these options.

   - TCP
   - UDP
6. In the **Name** field, provide the name for the syslog server.
7. In the **Hostname/IP address** field, provide the hostname or IP address of the syslog server.
8. In the **Port** field, specify the port number used by the syslog server.
9. If you want to enable secure communication, check the **TLS** check box.

Before you enable **TLS** you must upload the CA certificate for the syslog destination host to Nexus Dashboard. For more information see, Upload a CA certificate.

Configure syslog to enable exporting anomalies data to a syslog server

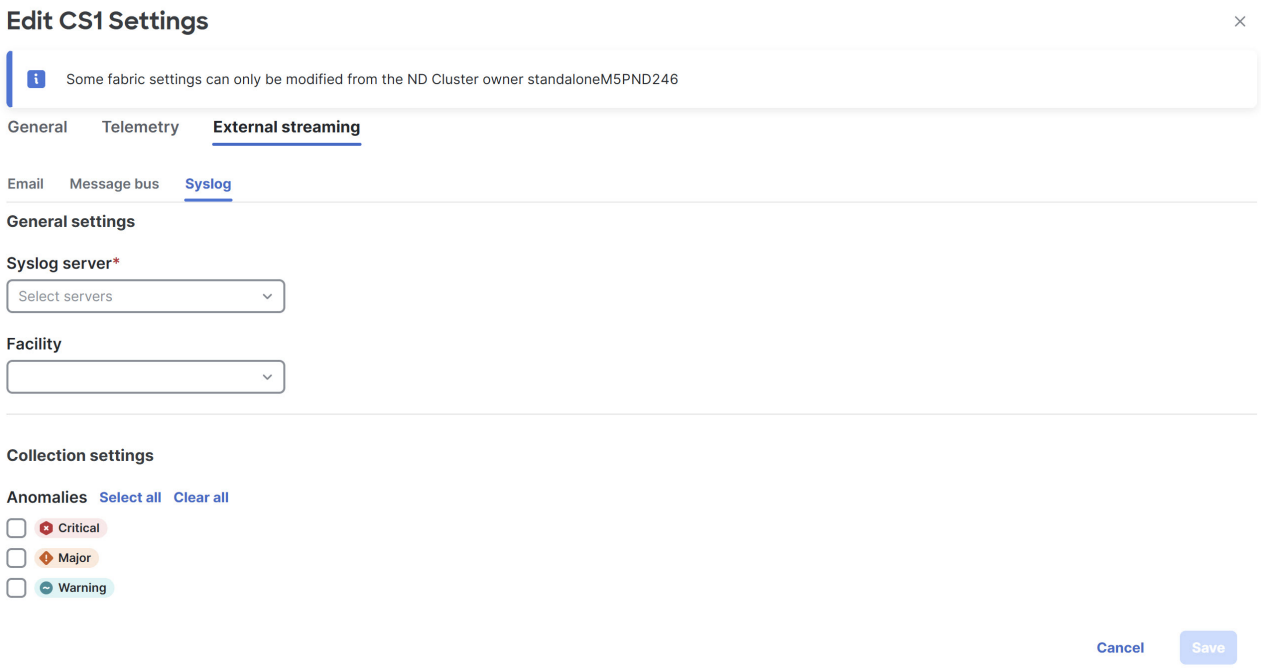
Follow these steps to configure syslog to enable exporting anomalies data to a syslog server.

1. Navigate to the **Fabrics** page.

   Go to **Manage > Fabrics**.
2. Choose the fabric for which you configure streaming settings.
3. From the **Actions** drop-down list, choose **Edit fabric settings**.

   The **Edit *fabric-name* settings** page displays.
4. In the **Edit *fabric-name* settings** page, click the **External streaming** tab.
5. Click the **Syslog** tab.

   The following details display under **Syslog** tab.



6. Make the necessary configurations in the **General settings** area.
   a. In the **Syslog server** drop down list, choose a syslog server.

      The **Syslog server** drop down list displays the syslog servers that you added in the **System Settings** level. For more information, see Add syslog server configuration.

   b. In the **Facility** field, from the drop-down list, choose the appropriate facility string.

      A facility code is used to specify the type of system that is logging the message. For this feature, the **local0-local7** keywords for locally used facility are supported.
7. In the **Collection settings** area, choose the desired severity options.

   The options available are **Critical**, **Major**, and **Warning**.
8. Click **Save**.

Upload a CA certificate

Follow these steps to upload a CA certificate for syslog server **TLS**.

1. Navigate to **Admin** > **Certificate Management**.
2. In the **Certificate management** page, click the **CA certificates** tab, then click **Add CA certificate**.

   You can upload multiple files at a single instance.
3. Browse your local directory and choose the certificate-key pair to upload.

   You can upload certificates with the .pem/.cer/.crt/ file extensions.
4. Click **Save** to upload the selected files to Nexus Dashboard.

   A successful upload message appears. The uploaded certificates are listed in the table.

Additional settings

The following sections provide information for additional settings that might be necessary when editing the settings for a campus VXLAN fabric.

Layer 3 VNI without VLAN

Following is the upper-level process to enable the Layer 3 VNI without VLAN feature in a fabric:

1. (Optional) When configuring a new fabric, check the **Enable L3VNI w/o VLAN** field to enable the Layer 3 VNI without VLAN feature at the fabric level. The setting at this fabric-level field affects the related field at the VRF level, as described below.
2. When creating or editing a VRF, check the **Enable L3VNI w/o VLAN** field to enable the Layer 3 VNI without VLAN feature at the VRF level. The default setting for this field varies depending on the following factors:
    - For existing VRFs, the default setting is disabled (the **Enable L3VNI w/o VLAN** box is unchecked).
    - For newly-created VRFs, the default setting is inherited from the fabric settings, as described above.
    - This field is a per-VXLAN fabric variable. For VRFs that are created from a VXLAN EVPN Multi-Site fabric, the value of this field is inherited from the fabric setting in the child fabric. You can edit the VRF in the child fabric to change the value, if desired.

      See the "Create a VRF" section in Working with Segmentation and Security for Your Nexus Dashboard VXLAN Fabric for more information.

The VRF attachment (new or edited) then uses the new Layer 3 VNI without VLAN mode if the following conditions are met:

- The **Enable L3VNI w/o VLAN** is enabled at the VRF level
- The switch supports this feature and the switch is running on the correct release (see Guidelines and limitations for Layer 3 VNI without VLAN)

The VLAN is ignored in the VRF attachment when these conditions are met.

Guidelines and limitations for Layer 3 VNI without VLAN

Following are the guidelines and limitations for the Layer 3 without VLAN feature:

- The Layer 3 VNI without VLAN feature is supported on the -EX, -FX, and -GX versions of the Nexus 9000 switches. When you enable this feature at the VRF level, the feature setting on the VRF will be ignored on switch models that do not support this feature.
- When used in a Campus VXLAN EVPN fabric, this feature is only supported on Cisco Nexus 9000 series switches in that type of fabric. This feature is not supported on Cisco Catalyst 9000 series switches in the Campus VXLAN EVPN fabric; those switches require VLANs for Layer 3 VNI configurations.
- This feature is supported on switches running on NX-OS release 10.3.1 or later. If you enable this feature at the VRF level, the feature setting on the VRF is ignored on switches running an NX-OS

image earlier than 10.3.1.

- When you perform a brownfield import in a Data Center VXLAN EVPN fabric, if one switch configuration is set with the **Enable L3VNI w/o VLAN** configuration at the VRF level, then you should also configure this same setting for the rest of the switches in the same fabric that are associated with this VRF, if the switch models and images support this feature.

Configuring automatic generation of BGP neighbor description

You can enable auto generation of a BGP neighbor description on BGP sessions between route reflectors and Virtual Tunnel Endpoints (VTEPs), border gateways, and border gateways and a route server. Nexus Dashboard added the **Generate BGP EVPN Neighbor Description** option on the **Edit Fabric Settings** page. Once enabled, Nexus Dashboard generates CLIs for a BGP neighbor description, including the host name of the neighbor. Nexus Dashboard stores the BGP neighbor description in a **bgp_neighbor_desc** policy. You can edit the policy with a different description.

You can also configure automatic generation of a BGP neighbor description between border gateways in a VXLAN fabric group.

Guidelines and limitations for automatic generation of a BGP neighbor description

- In brownfield deployments, the neighbor description on the switch is honored.
- For greenfield deployments, the default for this option is on.
- For fabrics upgraded from a previous release, this option is turned off during an upgrade.
- In a VXLAN fabric group, if you enable the **BGP Neighbor Description on Multi-Site Overlay IFC** option, Nexus Dashboard auto fills the BGP neighbor description in an auto generated multi-fabric overlay inter-fabric link (IFC). You can add a description in the manually created overlay IFC. You can also edit the BGP description field in existing IFCs.
- Auto generation of a BGP neighbor description between a route reflector and a VTEP does not include an eBGP fabric that does not have a route reflector.

How to configure automatic generation of a BGP neighbor description

Follow these steps to configure automatic generation of a BGP neighbor description.

1. On the **Manage > Fabrics** page, choose the Data Center VXLAN EVPN or the Campus VXLAN EVPN fabric that you want to edit.
2. From the **Actions** drop-down list, choose **Edit fabric settings**.
3. Navigate to the **Fabric Management > Protocols** page in the BGP section.
4. Check the **Generate BGP EVPN Neighbor Description** option.
5. Click **Save**.
6. Perform a **Recalculate and deploy** operation after saving the fabric setting to deploy the configuration to the switches.

How to configure automatic generation of a BGP neighbor description between border gateways in a VXLAN fabric group

Follow these steps to configure automatic generation of a BGP neighbor description between border gateways or between a border gateway and a route server in a VXLAN fabric group.

1. Create a VXLAN fabric group. For more information, see Creating LAN and ACI Fabrics and Fabric Groups.

   When creating a VXLAN fabric group, navigate to the **DCI** tab, and check the **BGP Neighbor Description on Multi-Site Overlay IFC** option.

2. On the **Manage > Fabrics** page, choose the fabric that you want to add to the fabric group.
3. From the **Actions** drop-down list, choose **Move Fabric into MSD**.
4. On the **Manage > Fabrics** page, choose the VXLAN fabric group for which you want to edit.

   The **Edit *fabric-name* Settings** page displays.

5. Navigate to the **DCI** tab.
6. Ensure that the **Multi-Site Overlay IFC Deployment Method** field displays **directPeering** or **routeServer** as the drop-down option.
7. Add another fabric to the VXLAN fabric group.
8. Click **Save**.
9. Perform a **Recalculate and deploy** operation after saving the fabric settings to deploy the configuration to the switches.

   Nexus Dashboard auto generates the inter-fabric link sessions between the border gateways in the VXLAN fabric group that you created.

Adding Cisco Catalyst 9000 series switches and Nexus 9000 series switches to a Campus VXLAN EVPN fabric

Cisco Catalyst 9000 series switches and Nexus 9000 series switches are discovered using SSH. Before adding the switches to the fabric, it is necessary that you configure the switches for SSH discovery as described in **Before You begin**.

Choose one of the following navigation paths to add switches to the fabric:

- Choose **Manage > Fabrics**. Select the required Campus VXLAN EVPN fabric from the list and choose **Actions > Add Switches**.
- Choose **Manage > Fabrics**. Select the required Campus VXLAN EVPN fabric from the list. Go to the **Switches** tab and then choose **Actions > Add Switches**.
- Choose **Manage > Inventory > Switches** and then choose **Actions > Add Switches**. Click **Choose Fabric**, choose the required Campus VXLAN EVPN fabric, and then click **Select**.

Before you begin

- Set the default credentials for the device in the **LAN Credentials Management** window if not already set. To navigate to the **LAN Credentials Management** page from Nexus Dashboard,

choose **Admin > Switch Credentials > LAN Credentials Management**.

- For StackWise and StackWise Virtual switches, configure the StackWise/StackWise Virtual settings before adding them to the fabric.
- Run the following SSH commands on the Cisco Catalyst 9000 switch console:

```
switch (config)# hostname <hostname>
switch (config)# ip domain name <domain_name>switch (config)# crypto key generate rsa
switch (config)# ip ssh time-out 90
switch (config)# ip ssh version 2
switch (config)# line vty 1 4
switch (config-line)# transport input ssh
switch (config)# username admin privilege 15 secret <password>
switch (config)# aaa new-model
switch (config)# aaa authentication login default local
switch (config)# aaa authorization exec default local none
```

Enter values for the following fields:

Field	Description
Seed IP	Enter the IP address of the switch in one of the following formats - "2.2.2.20" or "10.10.10.40-60" or "2.2.2.20, 2.2.2.21". You can import more than one switch by providing the IP address range. The switches must be properly cabled and reachable from Nexus Dashboard.
Authentication Protocol	Choose the authentication protocol from the drop-down list.
Device Type	Choose **IOS XE** or **NX-OS** from the drop-down list. If you select **IOS XE**, the **CAT9K** radio button appears which is selected by default.
Username	Enter the username for the switch.
Password	Enter the password for the switch.
Set as individual device write credential	Check the checkbox to set the discovery/read credentials as LAN/write credentials for individual devices.

You can change the Discover and LAN credentials only after discovering the switch.

Perform the following steps to add switches to a Campus VXLAN EVPN fabric:

1. Click **Discover Switches**.

The switch details are populated.

Nexus Dashboard supports the import of Cisco Catalyst 9500 switches running in StackWise Virtual. The StackWise Virtual configuration to form a pair of Cisco Catalyst 9500 Switches into a virtual switch has to be in place before the import.

For more information on how to configure StackWise Virtual, see the Configuring Cisco StackWise Virtual chapter in the *High Availability Configuration Guide (Catalyst 9500 Switches)* for the required release.

2. Check the check boxes next to the switches you want to import.

   You can import only switches with the **manageable** status.

   Note that the existing configuration on the switches will be erased after adding the switches to the Campus VXLAN EVPN fabric.

3. Click **Add Switches**.

   The switch discovery process is initiated, and the discovery status is updated under the **Discovery Status** column in the **Switches** tab.

4. (Optional) View the details of the device.

   After the discovery of the device, the discovery status changes to **ok** in green.

What to do next:

1. Set the appropriate role. The supported roles are:

Cisco Catalyst 9000 series switches	Nexus 9000 series switches
Leaf	Border gateway
Spine	Border gateway spine
Border	Border gateway super spine

   To set the role, choose the switch and choose **Actions > Set role**. Choose a role and click **Select**.

   After discovering the switches, Nexus Dashboard usually assigns **Leaf** as the default role for Cisco Catalyst 9000 series switches and border gateway for Nexus 9000 series switches.

   Optionally, you can form a VPC pair if there are Cisco Nexus 9000 switches with a border gateway role in the fabric.

   After setting the switch role, if the switch credentials and the default credentials do not match, the **Discovery Status** or the **Mode** column for the switches displays an error. In such case, set the LAN credentials for the switch. For more information, see the section "LAN Credentials Management" in Managing Your Device Credentials.

2. Recalculate the configurations and deploy the configurations to the switches. Proceed to the next section for the steps to perform recalculate and deploy.

Recalculating and deploying configurations

To recalculate and deploy the configurations to the switch(es) in the Campus VXLAN EVPN fabric, perform the following steps to recalculate configurations:

Before you begin:

Set the role of the switch(es) in the fabric.

1. In Nexus Dashboard, navigate to **Manage > Fabrics**.
2. Click the fabric name to open the **Fabric Overview** page.
3. Choose **Actions > Recalculate and deploy**.

   Recalculation of configurations starts on the switch(es).

Creating VRFs in Campus VXLAN EVPN Fabric

Perform the following steps to create tenant VRFs in a Campus VXLAN EVPN fabric:

1. In Nexus Dashboard, choose **Manage > Fabrics**.
2. From the list of available fabrics, double-click the Campus VXLAN EVPN fabric that you have created in the previous step.

   The **Fabric Overview** page appears.

3. Navigate to the **VRFs** tab and choose **Actions > Create**.

   The **Create VRF** window appears.

4. Enter the required details in the mandatory fields. Some of the fields are autopopulated with default values. You can make changes, as required.
   - **VRF Name** - Accept the default value or enter a name for VRF. The VRF name should not contain any white spaces or special characters except underscore (_), hyphen (-), and colon (:).
   - **VRF ID** - Accept the default or enter an ID for the VRF.
   - **VLAN ID** - Specifies the corresponding tenant VLAN ID for the network. Enter an ID for the VLAN. If you want to propose a new VLAN for the network, click **Propose Vlan**.
   - **VRF Template** - Accept the default autopopulated template or choose another template from the list.

     The default template is the template name specified in the **VRF Template** field in the **Advanced** tab on the **Create Fabric** window.

   - **VRF Extension Template** - Accept the default autopopulated template or choose another template from the list.

     The default template is the template name specified in the **VRF Extension Template** field in the **Advanced** tab on the **Create Fabric** window.

5. Configure the following fields under **General Parameters**, as needed.

- **VRF VLAN Name** - Enter the VLAN name for the VRF.
- **VRF Description** - Enter a description for the VRF.
- **VRF Interface Description**- Enter a description for the VRF interface.

6. Click the **Advanced** tab to optionally specify the advanced profile settings.

   Some of the fields in the **Advanced** tab are mentioned here. For more information about configuring the fields in the **Advanced** tab, see "Creating VRF" section in the About Fabric Overview for LAN Operational Mode Setups.

   - **VRF Interface MTU** - Specifies VRF interface MTU.
   - **Loopback Routing Tag** - If a VLAN is associated with multiple subnets, then this tag is associated with the IP prefix of each subnet. Note that this routing tag is associated with overlay network creation also.
   - **Redistribute Direct Route Map** - Specifies the redistribute direct route map name.
   - **Max BGP Paths** - Specifies the maximum BGP paths. The valid value range is 1-64 for NX-OS and 1-32 for IOS XE.
   - **Max iBGP Paths** - Specifies the maximum iBGP paths. The valid value range is 1-64 for NX-OS and 1-32 for IOS XE.
   - **Advertise Host Routes** - Check the check box to control advertisement of /32 and /128 routes to Edge routers.
   - **Advertise Default Route** - Check the check box to control advertisement of default route internally.
   - **Config Static 0/0 Route** - Check the check box to control configuration of static default route.

7. Click **Create** to create the VRF or click **Cancel** to discard the VRF.

   A message appears indicating that the VRF is created.

   The new VRF appears on the **VRFs** tab. The status displays **NA** as the VRF is created but not yet deployed. Now that the VRF is created, you can create and deploy networks on the devices in the fabric.

What to do next

1. Attach the VRF.
2. Create a loopback interface and select the **VRF_LITE** extension.

Attaching VRFs to switches in Campus VXLAN EVPN fabrics

Follow these steps to attach the VRFs and VRF Lite extensions to the switches in the Campus VXLAN EVPN fabric:

1. On the **VRFs** tab in the **Fabric Overview** window, double-click the VRF that you created in the previous section.

   The **VRF Attachments** page opens.

2. Go to the **VRF Attachments** tab and choose the VRF corresponding to the switch by checking the check box next to it.
3. Choose **Actions > Edit**.

   The **Extension** page opens.
4. Toggle the knob to **Attach** and click **Save**.

Similarly, you can create a loopback interface, and select the **VRF_LITE** extension.

For more information about attaching and detaching VRFs, see the section "VRF Attachments" in About Fabric Overview for LAN Operational Mode Setups.

What to do next

Deploy the configurations as follows:

1. Click **Actions** in **Fabric Overview**.
2. Choose **Deploy config to switches**.
3. Click **Deploy** after the configuration preview is complete.
4. Click **Close** after the deployment is complete.

Creating and deploying networks in Campus VXLAN EVPN fabrics

The next step is to create and deploy networks in Campus VXLAN EVPN fabrics.

Creating networks for Campus VXLAN EVPN fabrics

Follow these steps to create a network for a Campus VXLAN EVPN fabric:

1. In Nexus Dashboard, choose **Manage > Fabrics**.
2. From the list of available fabrics, click the Campus VXLAN EVPN fabric that you have created in the previous step.

   The **Fabric Overview** page appears.
3. Navigate to the **Networks** tab and choose **Actions > Create**.

   The **Create Network** page appears.
4. Enter the required details in the mandatory fields. Some of the fields are autopopulated with default values. You can make changes, as required.

   The fields in the **Create Network** page are:

Field	Description
Network Name	Specifies the name of the network. The network name should not contain any white spaces or special characters except underscore (_) and hyphen (-).

Field	Description
Layer 2 Only	Enables you to create a Layer 2 only network.
VRF Name	Allows you to select the VRF that you have created for the fabric. When no VRF is created, this field appears as blank. If you want to create a new VRF, click **Create VRF**. The VRF name should not contain any white spaces or special characters except underscore (_), hyphen (-), and colon (:).
VLAN ID	Specifies the corresponding tenant VLAN ID for the network. If you want to propose a new VLAN for the network, click **Propose VLAN**.
Network Template	Auto-populates the universal template. This is only applicable for leaf switches.
Network Extension Template	Auto-populates the universal extension template. This allows you to extend this network to another fabric. The VRF Lite extension is supported. The template is applicable for border leaf switches.
Generate Multicast IP	If you want to generate a new multicast group address and override the default value, click **Generate Multicast IP**.

5. Configure the following fields in the **General Parameters** tab:

If the network is a non-Layer 2 network, then it is mandatory to provide the gateway IP address.

Field	Description
IPv4 Gateway/NetMask	Specifies the IPv4 address with subnet. Specify the anycast gateway IP address for transporting the L3 traffic from a server belonging to MyNetwork_30000 and a server from another virtual network. The anycast gateway IP address is the same for MyNetwork_30000 on all switches of the fabric that have a network.  If the same IP address is configured in the **IPv4 Gateway** and **IPv4 Secondary GW1** or **IPv4 Secondary GW2** fields of the network template, Nexus Dashboard does not show an error, and you will be able to save this configuration. However, after the network configuration is pushed to the switch, it would result in a failure as the configuration is not allowed by the switch.
IPv6 Gateway/Prefix List	Specifies one or more IPv6 addresses with subnets.
Vlan Name	Enter a name for the VLAN.
Interface Description	Enter a description for the interface. This interface is a switch virtual interface (SVI).
IPv4 Secondary GW1	Enter the gateway IP address for the additional subnet.

Field	Description
IPv4 Secondary GW2	Enter the gateway IP address for the additional subnet.
IPv4 Secondary GW3	Enter the gateway IP address for the additional subnet.
IPv4 Secondary GW4	Enter the gateway IP address for the additional subnet.

6. Configure the following fields in the **Advanced** tab.

Field	Description
Multicast Group Address	The multicast IP address for the network is auto-populated. Multicast group address is a per fabric instance variable and remains the same for all networks by default. * Configure DHCP relay server fields as follows: a. Under **DHCP Relay Server Information**, choose **Actions > Add**. b. Enter the DHCP relay IP address of the first DHCP server in the **Server 1 V4 Address** field. c. Enter the DHCP server VRF ID in the **Server VRF** field. d. Click **Save**.  You can configure up to 16 DCHP servers.
Loopback ID for DHCP Relay interface (Min:0, Max:1023)	Enter the loopback ID for DHCP relay interface.
IPv4 TRM Enable	Check the checkbox to enable TRM with IPv4. For more information, see Editing Data Center VXLAN EVPN Fabric Settings.
IPv6 TRM enable	Check the check box to enable TRM with IPv6. For more information, see Editing Data Center VXLAN EVPN Fabric Settings.
L2 VNI Route-Target Both Enable	Check the check box to enable automatic importing and exporting of route targets for all L2 virtual networks. This is applicable only for Cisco Nexus 9000 switches.
Interface Vlan Netflow Monitor	Specifies the Netflow monitor specified for Layer 3 record for the VLAN interface. This is applicable only if Layer 2 Record is not enabled in the Netflow Record for the fabric. This is applicable only for Cisco Nexus 9000 switches.
Vlan Netflow Monitor	Enter the Netflow monitor name defined in the fabric setting for Layer 3 Netflow Record. This is applicable only for Cisco Nexus 9000 switches.
Enable L3 Gateway on Border	Check the check box to enable a Layer 3 gateway on the border switches.

7. Click **Create**.

A message appears indicating that the network is created. The new network appears on the

Networks page that comes up.

The **Status** appears as **NA** since the network is created but not yet deployed on the switches. Now that the network is created, you can create more networks if needed and deploy the networks on the devices in the fabric.

Attaching networks in a Campus VXLAN EVPN fabric

To attach a network in a Campus VXLAN EVPN fabric from Nexus Dashboard, perform the following steps:

1. In Nexus Dashboard, choose **Manage > Fabrics**.
2. From the list of available fabrics, click the Campus VXLAN EVPN fabric.

   The **Fabric Overview** page appears.
3. Navigate to the **Networks** tab and click the network that you created in the previous section to open the **Network Attachments** page.
4. On the **Network attachments** tab, select the required network and choose **Actions > Edit**.

   The **Edit Network Attachment** page opens.
5. Use the toggle switch to enable **Attach** and then click **Save**.

Deploying networks in Campus VXLAN EVPN fabrics

To attach networks in a Campus VXLAN EVPN fabric from Nexus Dashboard, perform the following steps:

1. In Nexus Dashboard, choose **Manage > Fabrics**.
2. From the list of available fabrics, double-click the Campus VXLAN EVPN fabric.

   The **Fabric Overview** page appears.
3. Navigate to the **Switches** tab, select the switches and choose **Actions > Deploy**.
4. Click **Deploy All** after the configuration preview is complete.
5. Click **Close** after the deployment is complete.

Creating DCI links for switches in Campus VXLAN EVPN fabrics

You can create a VRF-Lite IFC between a Cisco Catalyst 9000 series switch or a Cisco Nexus 9000 switch with a border role in a Campus VXLAN EVPN fabric, and another switch in a different fabric. The other switch can be a Cisco Nexus 9000 switch in an External fabric, LAN Classic fabric, or Campus VXLAN EVPN fabric. It can also be a Catalyst 9000 switch in an External Fabric or a Campus VXLAN EVPN fabric. The link can be created only from a Campus VXLAN EVPN fabric. The other switch can be an External, Classic LAN, Campus VXLAN EVPN, or a Data Center VXLAN EVPN fabric. The link can be created only from the Campus VXLAN EVPN fabric.

For more information, see the section "Links" in About Fabric Overview for LAN Operational Mode

Setups and Templates.

When creating DCI links for a Campus VXLAN EVPN fabric, auto-deploy is supported only if the destination device is a Cisco Nexus 9000 switch.

Follow these steps for creating links for a Campus VXLAN EVPN fabric:

1. Navigate to the **Links** tab in the fabric overview.

   The list of previously created links is displayed. The list contains intra-fabric links, which are between switches within a fabric, and inter-fabric links, which are between border switches in this fabric and switches in other fabrics.

2. Choose **Actions > Create**.

   The **Create Link** page appears. By default, the **Intra-Fabric** option is chosen as the link type.

3. From the **Link Type** drop-down box, choose **Inter-Fabric**.
4. From the **Link Sub-Type** drop-down list, choose **VRF_LITE**.
5. In the **Link Template** field, ensure **ext_fabric_setup** template is auto populated for VRF_LITE IFC.

   The templates are autopopulated with corresponding pre-packaged default templates that are based on your selection. The template to use for **VRF_LITE** IFC is **ext_fabric_setup**.

6. From the **Source Fabric** drop-down list, choose the campus VXLAN EVPN fabric.
7. From the **Destination Fabric** drop-down list, choose a destination fabric.
8. Choose the **Source Device** and Ethernet interface that connects to the destination device.
9. Choose the **Destination Device** and Ethernet interface that connects to the source device.
10. Enter values in other fields, as required. For more information about configuring the fields in the **Default VRF** tab, see VRF Lite
11. Click **Save**.

    Instead of the **Create** option, you can also use **Edit** to create VRF-Lite IFC(s) using the existing inter-fabric link(s). Choose the **VRF_Lite** link subtype. By default, if you select **Edit**, then the data for the fields **Link-Type**, **Source Fabric**, **Destination Fabric**, **Source Device**, **Destination Device**, **Source Interface** and **Destination Interface** are auto-populated in the **Edit Link** window.

    Choose **VRF_LITE** as the link sub-type and **ext_fabric_setup** template for VRF_LITE IFC. To complete the procedure, repeat step 4 to step 10 mentioned above.

First Published: 2025-01-31
Last Modified: 2025-01-31