

Cisco Nexus Dashboard Insights Getting Started, Release 6.5.x - For Cisco ACI

Table of Contents

New and Changed Information . . . 2
Cisco Nexus Dashboard Insights Setup . . . 3
- Meet Nexus Dashboard Insights . . . 3
- Initial Setup . . . 4
- Add Fabrics . . . 4
- Fabric Analysis . . . 8
- Assurance Analysis . . . 8
- Assurance analysis guidelines and limitations . . . 8
- On-Demand Analysis . . . 9
- Enable Assurance Analysis . . . 9
- Policy-Based Redirect Service Chain Assurance . . . 10
- Microburst . . . 11
- About Device Connector . . . 12
- Metadata Support . . . 12
- Usage guidelines and limitations . . . 13

Configure Flows . . . 15
- Flow Telemetry . . . 15
- Flow Telemetry Guidelines and Limitations . . . 15
- Configure Flows . . . 16
- Monitoring the Subnet for Flow Telemetry . . . 19
- Netflow . . . 20
- Netflow Types . . . 20
- Netflow Guidelines and Limitations . . . 20
- Configure Netflow . . . 21

Export Data . . . 22
- Export Data . . . 22
- Configure the Kafka exporter for the Alerts and Events collection type . . . 23
- Configure Kafka exporter for the Usage collection type . . . 23
- Configure Email . . . 24
- Syslog . . . 26
- Configure Syslog . . . 26
- Export Flow Records To Network Attached Storage . . . 29
- Guidelines and Limitations . . . 29
- Add Network Attached Storage to Export Flow Records . . . 29

System Settings . . . 34
- System issues . . . 34
- System Status . . . 34
- Import and Export of Configurations . . . 36
- Guidelines and Limitations . . . 37
- Exporting a Configuration . . . 37
- Importing a Configuration . . . 38

Copyright 39

First Published: 2024-06-28

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

New and Changed Information

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

New Features and Changed Behavior in the Cisco Nexus Dashboard Insights

Feature	Description	Release	Where Documented
Policy-based redirect assurance anomaly	The anomaly, Service Chain Redirect Policy Violation, is added for policy-based redirect (PBR) assurance. This anomaly is generated when one or more redirect zoning rules for contract and service graph instances are missing or do not match the Cisco APIC configuration. As a result, traffic will not be redirected as expected for the contract and service graph instance.	6.5.1	PBR Anomalies
Nexus Dashboard Insights backup and restore	The Nexus Dashboard Insights 6.5.1 release introduces the unified backup and restore functionality at the Cisco Nexus Dashboard level, which backs up configuration information not only for Nexus Dashboard, but also for any services (such as Nexus Dashboard Insights) running in that Nexus Dashboard.	6.5.1	Nexus Dashboard Insights backup and restore
Terminology change	The term " sites" is renamed to " fabrics" .	6.5.1	Entire document

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

Cisco Nexus Dashboard Insights Setup

Meet Nexus Dashboard Insights

Cisco Nexus Dashboard Insights (Nexus Dashboard Insights) is a single-pane-of-glass console that streamlines data center network operations and management.

Nexus Dashboard Insights consists of the following components:

- **Overview**: Provides basic information about your fabric and Nexus Dashboard Insights.
  - **Global View**: Provides a bird's-eye view of your global network infrastructure.
  - **Journey: Getting Started**: Helps you to set up your fabrics in Nexus Dashboard Insights and provides an overview of some of the key features. The **What's New** tab provides you with information about updates and new features in the platform.
  - **Topology**: Visualizes interconnectivity of the switches in Nexus Dashboard Insights and their connected components, such as devices and endpoints.
  - **Custom Dashboards**: Enables you to create dashboards to which you can pin pages that you use frequently. These pages appear as widgets in the dashboard, which you can click to go to those pages easily.
- Manage: Provides a deeper look into your network infrastructure and its operations.
  - Fabrics: Fabrics are on-premises network regions that consist of a group of switches and other networking devices that provide connectivity for your applications and endpoints.
  - Inventory: Displays information about your switches and controllers.
  - Rules: Enables you to manage your fabric's anomalies and advisories configuration.
  - Software Management: Allows you to easily manage the software running on all your devices from a single place, install updates, and perform pre and post-update analysis.
- Analyze: Allows you to go back in time and let analytics help you understand historical network patterns.
  - Anomalies: Allows you to proactively detect different types of anomalies across the network, analyze the anomalies, and identify remediation methods.
  - Advisories: Provides recommendations to keep your network under support and running in optimal conditions.
- Analysis Hub: Enables you to analyze and troubleshoot your network with advanced analytics tools optimized for you to gain valuable insights into the performance and health of your network.
  - Sustainability: Explore your fabric's energy usage, cost, and emissions.
  - Conformance: Keep track of your hardware and software life cycles.
  - Compliance: Monitor your fabric's compliance with custom anomaly rules.
  - Connectivity Analysis: Analyze flows from one endpoint to another.
  - Delta Analysis: Compare configurations and differences in your fabrics between two points in time.
  - Pre-Change Analysis: View the potential impact of configuration changes.
  - Log Collector: Collect and analyze logs from you devices

    - Policy CAM: Monitor your network's policies.
    - Traffic Analytics: Monitor your network's latency, congestion, and drops.
    - Bug Scan: Learn more about active and potential bugs affecting your network.
- Admin:
    - Integrations: Allows you to add integrations such as AppDynamics, vCenter, DNS, and Nexus Dashboard Orchestrator.
    - Configuration Import/Export: Enables you to import and export the configurations in Nexus Dashboard Insights.

Initial Setup

The following workflow will guide you through the configurations required for the initial setup. After you add a fabric, you can enable or configure the relevant features. You do not have to follow a sequential order to proceed with these tasks. You can perform or enable the tasks in any order.

- Add Fabrics. See Add Fabrics.
- Fabric Analysis. See Fabric Analysis.
- Configure Flows. See Configure Flows.
- Enable Microburst. See Microburst.
- Export Data. See Export Data.
- System Status. See System Status.

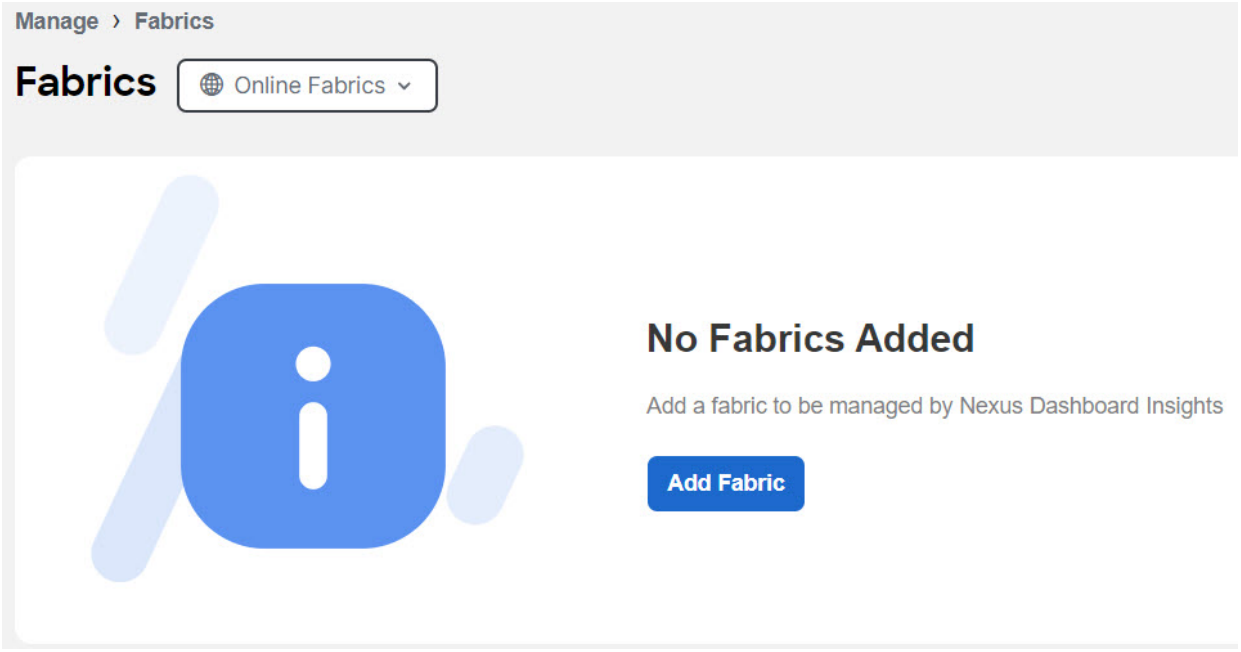
Add Fabrics

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

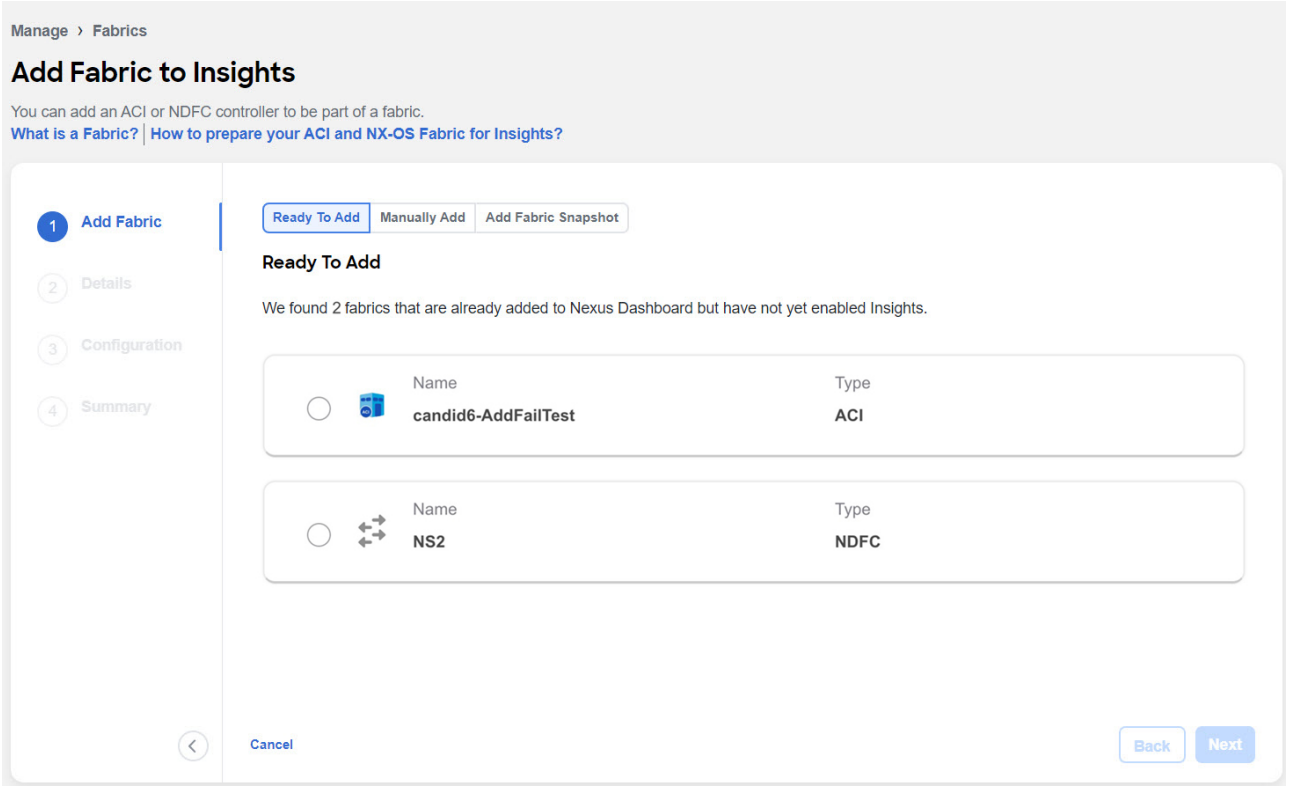
- Online Fabrics
    - Enable the fabric that has already been added to Nexus Dashboard. Fabrics added to the Nexus Dashboard are not enabled in the services by default, so you will need to explicitly enable them directly from Nexus Dashboard Insights.
    - Add a fabric to Nexus Dashboard and then enable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

Add an Online Fabric

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



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



4. Complete the following fields for **Ready to Add**.
   a. Select the fabric.
   b. Click **Next**.
   c. Select the fabric location from the map to identify the fabric on Nexus Dashboard.
   d. Click **Next**.
   e. Select the in-band EPG from the drop-down list. For Nexus Dashboard Insights, in-band EPG is used for connectivity between Nexus Dashboard and the fabric.

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

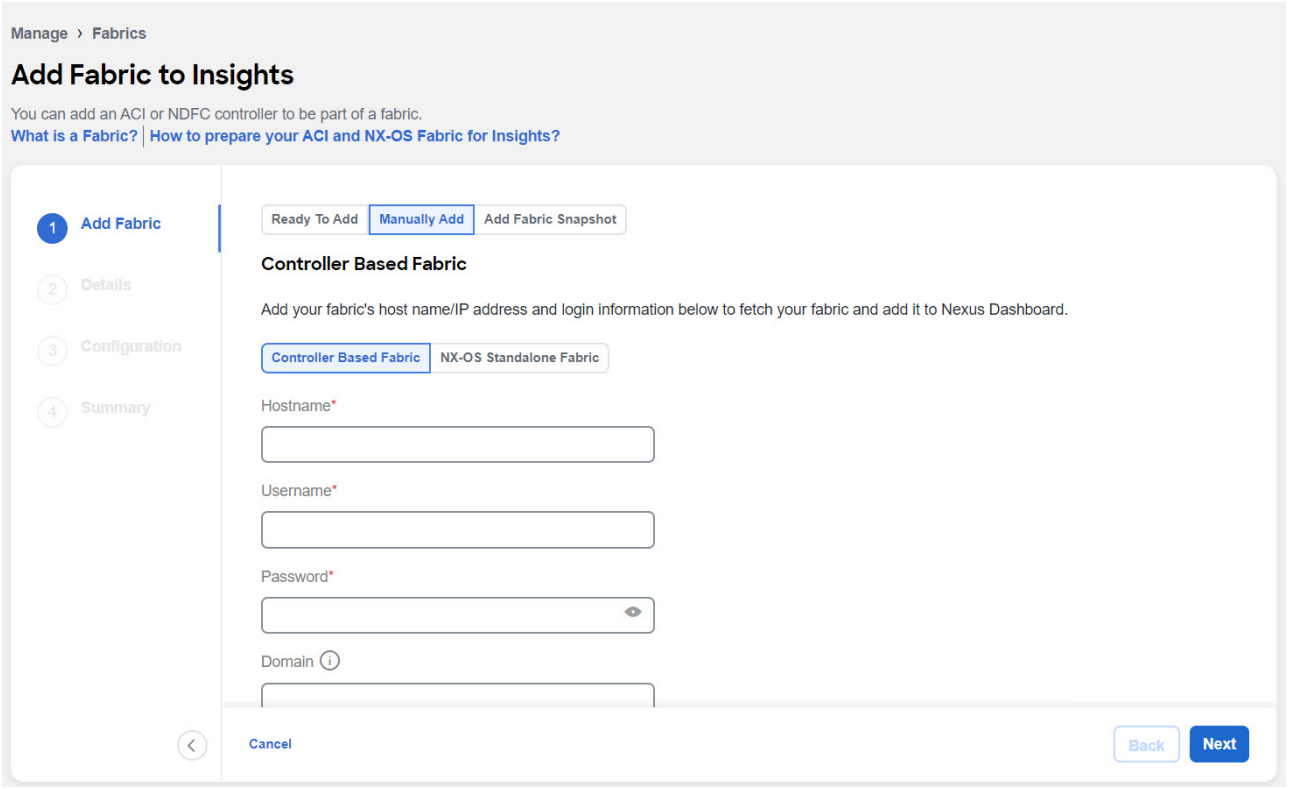
> IPv6 is only supported for Cisco APIC release 6.0(3) and later.

g. Click **Next**.

h. Verify the configuration.

i. Click **Submit**.

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



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

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

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

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

d. Click **Next**.

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

f. Select the fabric location from the map to identify the fabric on Nexus Dashboard.

g. Click **Next**.

h. Select the in-band EPG from the drop-down list. For Nexus Dashboard Insights, in-band EPG is used for connectivity between Nexus Dashboard and the fabric.

i. Use toggle to select IPv4 or IPv6 to onboard the fabric. Based on this setting, Nexus Dashboard Insights will configure its collector to receive telemetry from this fabric. This setting

should match your fabrics IP address configuration.

> IPv6 is only supported for Cisco APIC release 6.0(3) and later.

j. Enter the username and password.

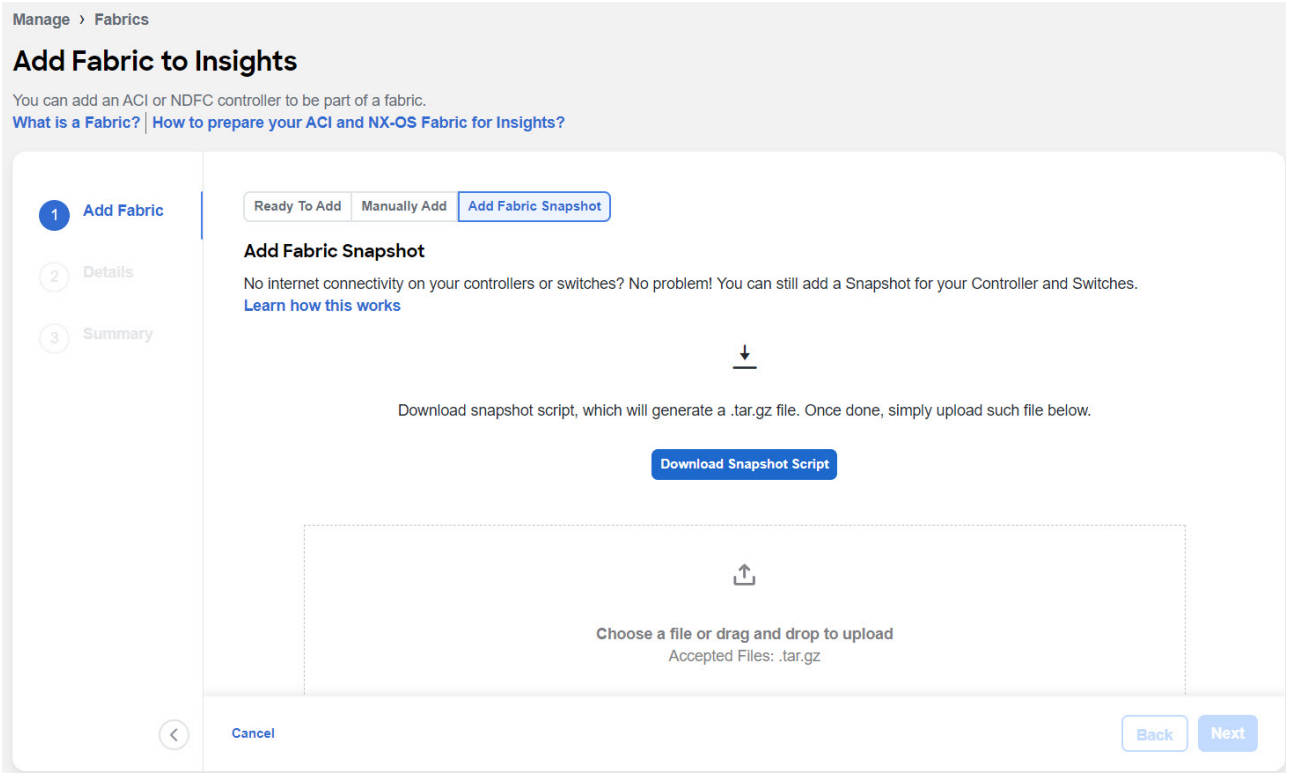
k. Click **Next**.

l. Verify the configuration.

m. Click **Submit**.

Add a Snapshot Fabric

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



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

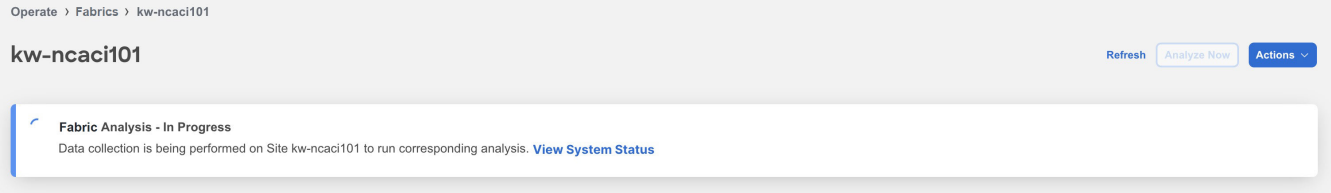
> The collection script requires that you have Python3 installed on your system.

6. Upload the file in Nexus Dashboard Insights and click **Next**
7. Enter the fabric name to identify the fabric on Nexus Dashboard.
8. Select the fabric location from the map to identify the fabric on Nexus Dashboard.
9. Click **Next**.

10. Verify the configuration.
11. Click **Submit**.

Fabric Analysis

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



Click System Status to view the status. See System Status.

During fabric analysis, Telemetry Collection, Assurance Analysis, and Bug Scan analysis is carried out automatically. See Assurance Analysis and Bug Scan in Analysis Hub.

Assurance Analysis

Assurance analysis involves collecting data from fabrics, running the analysis to create a model with the collected data, and generating the results.

- Assurance analysis provides assurance in real time. During assurance analysis for online fabrics, the data collection, model generation, and results generation are carried out simultaneously. The collected data is analyzed immediately after collection followed by result generation. This is repeated after a fixed time interval or as specified by the user. For online fabrics, assurance analysis is performed automatically every 2 hours. The schedule is determined by the fabric size and scale. For larger fabrics, assurance analysis is performed automatically every 3-4 hours.
- For snapshot fabrics, a one-time assurance is provided. This assurance analysis allows you to decouple the data collection stage from the analysis stage. The data is collected using a Python script and the collected data is then uploaded to Nexus Dashboard Insights to provide a one-time assurance. The collected data can also be analyzed at a later time. It enables the user to collect the data during change management windows and then perform the analysis.

Assurance analysis guidelines and limitations

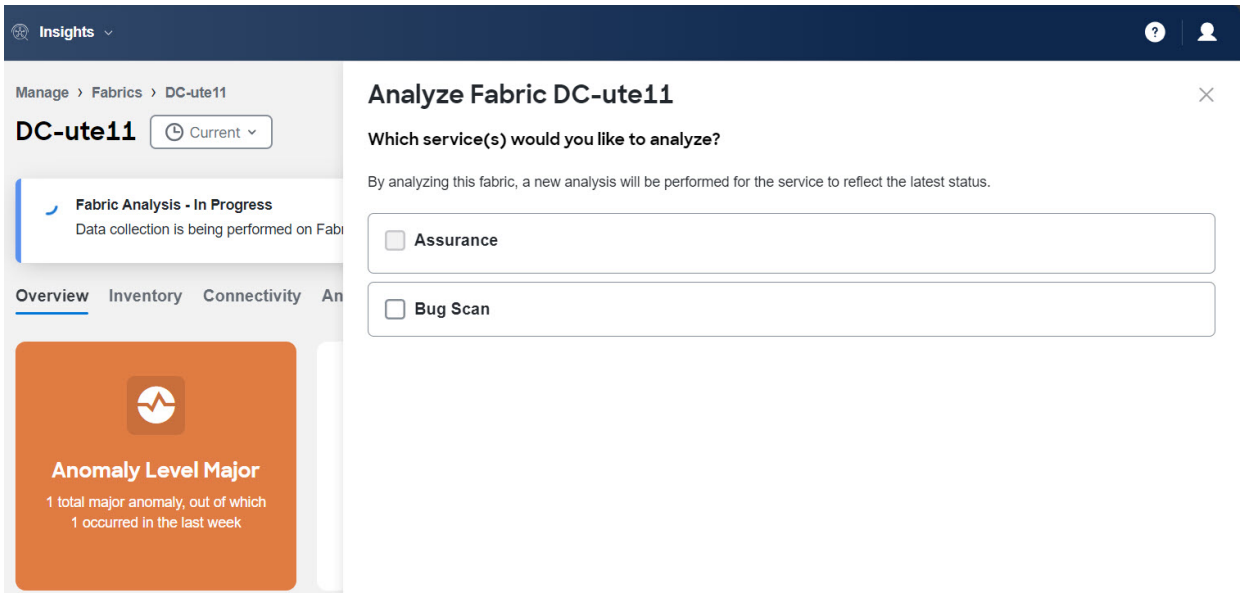
- If you take the assurance analysis from a fabric and export the raw data set to upload a file to a Snapshot fabric, assurance analysis for the snapshot fabric will only generate assurance related anomalies.
- Currently, if you begin an assurance analysis for a snapshot fabric, you can simultaneously continue to run the assurance analysis for online fabrics that are already in progress. They will all run without any disruption to the behavior.
- Anomaly Rules and Compliance Rules are valid in assurance analysis for snapshot fabrics.

On-Demand Analysis

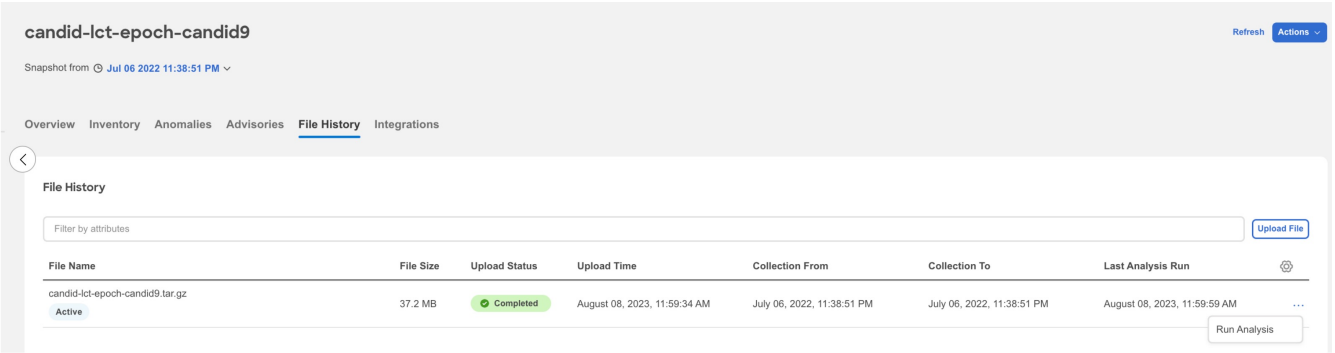
For online fabrics, assurance analysis is performed automatically, but you can also choose to request one at any time. This may be useful in cases where you resolve one or more issues in a fabric and would like Nexus Dashboard Insights to poll the latest Anomalies and Advisories information without waiting for the next automatic run.

Similarly, you can also run an on-demand analysis for Bug Scan to reflect the latest status.

1. Navigate to **Manage** > **Fabrics**.
2. Choose Online or Snapshot fabrics from the drop-down list.
3. For an online fabric, click the fabric name to view the details.
    a. Click **Analyze Now**.
    b. Choose the service. For Bug Scan, select the switches and click **Run Now**.



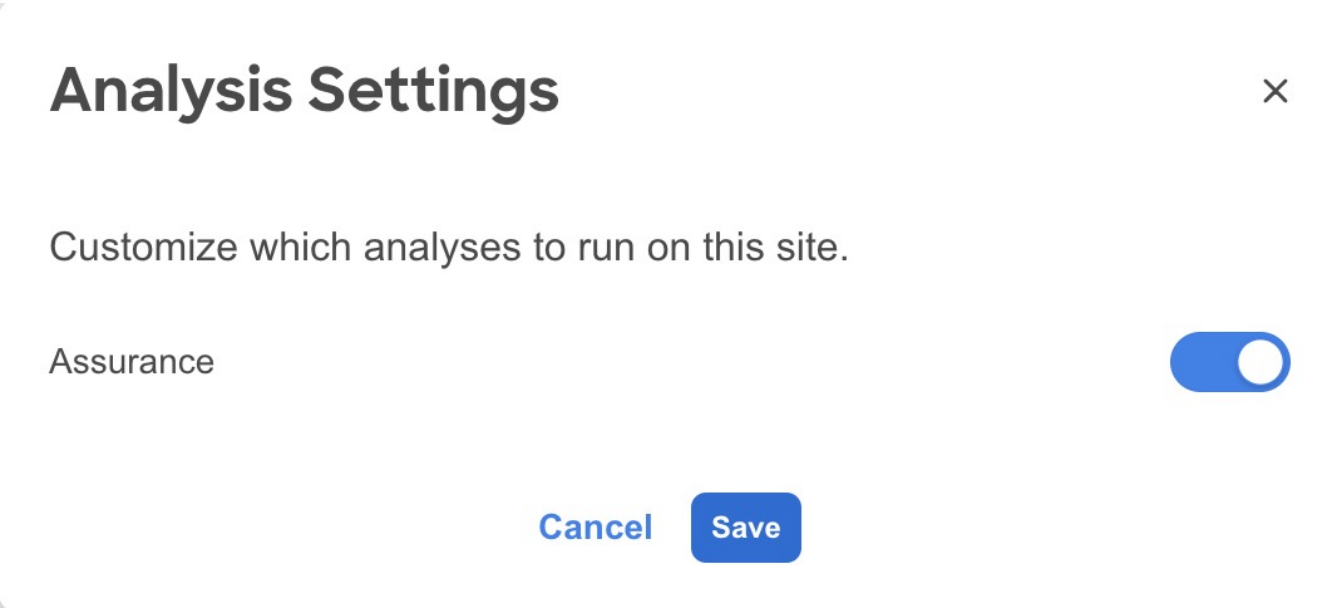
4. For snapshot fabric, click the fabric name to view the details.
5. Click **File History**.
6. In the **File History** table, click the ellipsis icon and choose **Run Analysis**.



Enable Assurance Analysis

You can also enable or disable the automatically scheduled assurance analysis job.

1. Navigate to **Manage** > **Fabrics**.
2. Choose Online fabric from the drop-down list.
3. Click the fabric name to view the details.
4. From the Actions menu, choose **System Status**.
5. From the Actions menu, choose **Analyze Settings**.
6. Use toggle to enable or disable scheduled assurance analysis job.
7. Click **Save**.



Policy-Based Redirect Service Chain Assurance

With policy-based redirect (PBR) support, the Nexus Dashboard Insights assurance engine checks for inconsistencies with device cluster, device selection policy, deployment of vPC nodes, and device cluster deployment for unmanaged single nodes in the GoTo mode.

Nexus Dashboard Insights assures PBR service graphs. If all conditions listed below are met, there will be no false positive anomalies. However, if any of the conditions are not met, then PBR service graphs are not assured and they may result in false positives.

- A service graph template must have route redirect enabled.
- Only a single service node is supported and the service node must be in the GoTo mode **Function Type** under the **Function Node** properties.
- The direct connect option for service graphs is not supported, therefore you must set the value to **False**.
- The set of provider/consumer bridge domains must not overlap with the set of shadow EPG bridge domains. Additionally, every shadow EPG must have its own bridge domain.
- The provider EPG and the consumer EPG must be one of the following types: an L3Out EPG, an application EPG, or a vzAny EPG.
- In a transit routing case with a PBR contract, the provider L3Out and consumer L3Out must be different L3Outs. PBR destinations in an L3Out is not supported.
- There must be a single service graph per contract, and the service graph must be bidirectional.

- There must be no filters set on the function node connectors under the service graph template.
- Only one service graph per contract is supported.
- Subnets on logical interface contexts are not supported.
- The backup PBR policy feature (introduced in Cisco APIC release 4.2(1)) is not supported.
- If you use the threshold-redir command, you must set the threshold down action to permit.
- Filters from a contract for a PBR service graph template is not supported.

PBR Anomalies

In Nexus Dashboard Insights release 6.5.1, the anomaly, Service Chain Redirect Policy Violation is added for PBR assurance.

The following checks are performed before the Service Chain Redirect Policy Violation is generated:

- If one or more zoning rules contracts are missing or do not match the APIC configurations.
- If redirect destination or redirect destination group which is used by deployed PBR graph is in disabled state.

As a result, traffic will not be redirected as expected for the contract and graph instance.

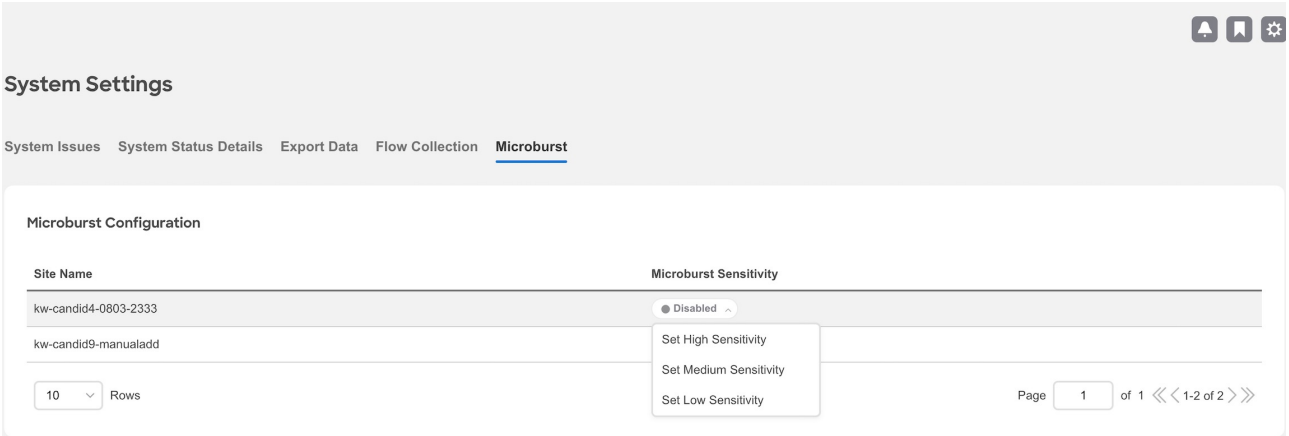


If IP-SLA policy or health group is not enabled in the PBR redirect policy, the anomaly Service Chain Redirect Policy Violation will not be generated even if the redirect destination is not reachable. In this case, the anomaly PBR Redirect Destination Learning Error will be generated.

Microburst

In Nexus Dashboard Insights, to configure Microburst, perform the following actions:

1. Navigate to **Admin** > **System Settings** > **Microburst**.
2. In the **Microburst Configuration** area, select the fabric and click the drop-down menu for **Microburst Sensitivity**. The default value is **Disable**. Choose the value appropriate that you want to configure. The other values are **Set High Sensitivity**, **Set Medium Sensitivity**, and **Set Low Sensitivity**.



Based on the percentage of threshold, a microburst is either low, high, or medium. The

percentage of threshold is inverse to sensitivity. When the number of microbursts are greater than 100 on a particular interface, an anomaly is raised. Nexus Dashboard Insights collects the microburst data for the selected fabrics. Microburst anomalies are raised on the interface of the node.

This table provides the microburst thresholds.

Sensitivity	Up threshold	Down threshold
Low	75%	50%
Medium	50%	25%
High	25%	5%

To Learn More,

- See Micro-Burst Monitoring for details.
- See Supported Platforms for details.
- See Inventory to view microburst information on Nexus Dashboard Insights.

About Device Connector

Data center apps and services such as the Cisco Nexus Dashboard Insights service is connected to the Cisco Intersight cloud portal through a Device Connector that is embedded in the management controller of the Cisco Nexus Dashboard platform.

See Cisco Nexus Dashboard Operations for Configuring the Device Connector and Claiming a Device.

For connectivity requirements, see Network Connectivity Requirements.

Metadata Support

Nexus Dashboard Insights uses metadata bundles to detect new bugs, Security Advisories, Field Notices, and End of Life Notices.

Navigate to **Admin > System Settings > Metadata** to view the metadata version.

- In the **General** area, the **Metadata Version** is displayed.
- In the **Update Metadata Version** area, you can upload metadata for air-gapped environments.

Metadata support for air-gapped environment

Nexus Dashboard Insights now supports Metadata support for air-gapped environments. With Metadata support for air-gapped environments, you can periodically upload the latest Metadata to Nexus Dashboard Insights in a secure and trusted way when Nexus Dashboard Insights is not connected to Cisco Secure Cloud.

You can download the metadata file from Intersight PVAPP portal and upload it to Nexus Dashboard Insights to get decrypted updates on exposure to Bugs, Security Advisories, Defects, Field Notices, and End of Life Notices.

Update Metadata version using air-gapped mechanism

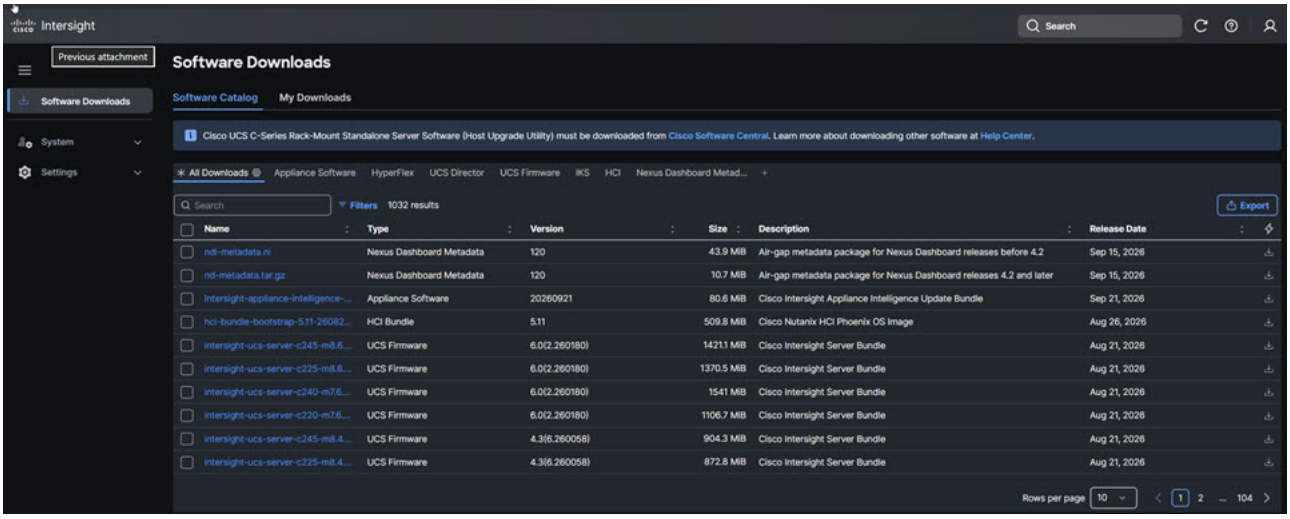
Nexus Dashboard Insights also provides an option to upload an encrypted metadata package downloaded from Cisco Intersight for air-gapped deployments. You can use the air-gapped mechanism to manually upload your metadata file when Cisco Intersight is not available.

Follow these steps to upload metadata using the air-gapped mechanism.

1. Create an Intersight PVAPP account. You can create your Intersight PVAPP account at https://intersight.com/pvapp. You will be prompted to set up an account name. You can use 'NexusDashboard-Metadata' or a similar name to easily identify it from other Intersight accounts you may already have.

   This step is only required for initial setup of your PVAPP account; you can skip this step for future metadata download access.

2. Login to Cisco Intersight.com account using the 'NexusDashboard-Metadata' account you created in the previous step or use an existing account.
3. Click the **All Downloads** tab on the **Software Download** page. The **Software Download** page displays multiple software versions including entries for versions prior to Nexus Dashboard Insights 4.2.1 release and forNexus Dashboard Insights 4.2.1 and later releases.



4. Choose the version that applies to your cluster version and click the download icon next to the latest metadata file available.
5. Wait for the download to complete.
6. In the Nexus Dashboard Insights user interface, navigate to the **Admin > System Settings > Metadata** page.
7. Upload the downloaded metadata file in the **Update metadata version** field.

Usage guidelines and limitations

These general usage guidelines and limitations apply for Cisco Nexus Dashboard Insights:

- You cannot downgrade Nexus Dashboard Insights.
- After modifying a bridge domain or VRF instance for an EPG, the flow analytics does not work as

expected momentarily.

- In a multi-cluster setup, remote cluster system anomalies are not displayed in the local cluster. You must log in to the remote cluster to view that system's anomalies.
- Nexus Dashboard Insights creates a user in the Cisco APIC called cisco_SN_NI. This user is used when Nexus Dashboard Insights needs to make any changes or query any information from the Cisco APIC. In the Cisco APIC GUI, navigate to **System > History > Audit Logs**. The cisco_SN_NI user is displayed in the **User** column.

Configure Flows

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 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:

- VRFs
- Physical Interfaces
- Port Channel Interfaces
- Routed Sub-Interfaces
- SVIs



If you want to configure Routed Sub-Interfaces from the UI, select L3 Out.

Flow telemetry monitors the flow for each fabric separately, as there is no stitching across the fabrics in a fabrics group. Therefore, flow telemetry is for individual flows. For example, if there are two fabrics (fabric A and fabric B) within a fabrics 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

- Ensure that you have configured NTP and enabled PTP on Cisco APIC. See Cisco Nexus Dashboard Insights Deployment Guide and Precision Time Protocol (PTP) for Cisco Nexus Dashboard Insights for more information.
- All flows are monitored as a consolidated view in a unified pipeline for fabric types ACI and DCNM/NDFC, 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, Cisco Nexus Dashboard Insights will use LLDP information from the previous and next nodes in the path to identify the switch name and the ingress and egress interfaces.
- The toggle buttons can be enabled for Flow Telemetry and Netflow by the user if desired. It is recommended that you enable either one of the options.
- Nexus Dashboard supports Kafka export for Flow anomalies. However, Kafka export is not currently supported for Flow Event anomalies.
- Flow telemetry including Flow Telemetry Events supports the following:
  - 20,000 unique flows/s [physical standard]
  - 10,000 unique flows/s [physical small]
  - 2,500 unique flows/s [vND]
- In case of Nexus Dashboard cluster being connected to an ACI fabric directly via an EPG:

- Make sure you do not have any native or leaked default routes in the mgmt:inb vrf.
- Make sure Nexus Dashboard data network subnet is different from ACI fabric inband subnet.

- The following Cisco Nexus 9000 ACI-Mode Switches versions are not supported with Nexus Dashboard Insights Flow Telemetry:
  - 14.2(4i)
  - 14.2(4k)
  - 15.0(1k)

  If you enable Flow Collection for a fabric that contains 1 or more unsupported switches, the status of Flow is displayed as **Disabled**. After you upgrade the switches to a supported version, the the status of Flow is displayed as **Enabled**.

- Interface based Flow Telemetry is only supported on leaf switches and is not supported on spine switches.
- The following Cisco Nexus 9000 ACI-Mode Switches versions are supported with Nexus Dashboard Insights for interface based Flow Telemetry:
  - Cisco APIC release 6.0(3) and later
  - Cisco ACI Switch release 16.0(3) and later



Interface based Flow Telemetry is a beta feature on Cisco NX-OS release 16.0(2).

- SVIs are not supported for telemetry streaming to Nexus Dashboard Insights.

Flow Telemetry Rules guidelines and limitations:

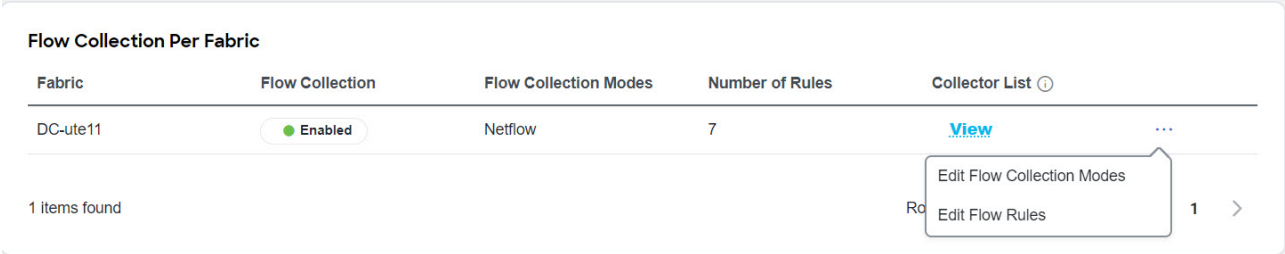
- The node can operate either in the VRF mode or interface mode. If the rule is configured in physical/port-channel/L3out/SVI, then the node operates in interface mode. If both VRF and interface rules are configured, interface rules take preference and take effect, the VRF rule will not take effect. Let's consider a scenario where multiple VRF rules are configured on a node, and you configure an interface rule. In that case, all the rules in the node are converted to interface rules and only the interface rules will be active on that node. If you remove the interface rules from that node, the rules will be converted back to VRF mode.
- If you configure an interface rule (physical/portchannel/L3out/SVI)on a subnet, it can monitor only incoming traffic. It can't monitor outgoing traffic on the configured 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.
- The maximum number of logical interfaces (including the combined total of physical interface, port channels, L3Out, and SVI) that you can configure on a node is 63.
- You can configure up to 500 rules on a node.

Configure Flows

Configure Flow Collection Modes

Procedure

1. Navigate to **Admin** > **System Settings** > **Flow Collection**.
2. In the **Flow Collection Mode** area, select **Flow Telemetry**.
3. In the **Flow Collection per Fabric** table, select the fabric and click the ellipsis icon.
4. Click **Edit Flow Collection Modes**.



5. In the **Edit Flow Collection Mode** page, select **Flow Telemetry** to enable Flow Telemetry. All the flows are disabled by default.
6. Click **Save**.

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

Procedure

1. Navigate to **Admin** > **System Settings** > **Flow Collection**.
2. In the **Flow Collection Mode** area, select **Flow Telemetry**.
3. In the **Flow Collection per Fabric** table, select the fabric and click the ellipsis icon.
4. Click **Edit Flow Rules**.
5. To add a VRF rule, click VRF tab and perform the following:
   a. From the **Actions** drop-down menu, select **Create New Rule**.
   b. In the **General** area, complete the following:
      i. Enter the name of the rule in the **Rule Name** field.
      ii. Select the tenant from the **Tenant** drop-down list.
      iii. Select the VRF from the **VRF** drop-down list.
      iv. In the **Subnets** area, enter the subnet on which you intend to monitor the flow traffic. If you have endpoints that are under the same endpoint groups, then you can provide a rule to monitor the subnet.
      v. Click **Add Subnet**.
6. To add a physical interfaces rule, click **Physical Interfaces** tab and perform the following:

a. From the **Actions** drop-down menu select **Create New Rule**.

b. 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. 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.

iv. In the **Subnets** area, enter the subnet on which you want to monitor the flow traffic.

v. Click **Add Subnet**.

c. Click **Save**.

7. To add a port channel rule, click **Port Channel** tab and perform the following:

a. From the **Actions** drop-down menu, select **Create New Rule**.

b. In the **General** area, complete the following:

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

ii. 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.

iii. 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.

iv. In the **Subnets** area, enter the subnet on which you want to monitor the flow traffic.

v. Click **Add Subnet**.

c. Click **Save**.

8. To add a L3Out rule, click **L3Out** tab and perform the following:

a. From the **Actions** drop-down menu, select **Create New Rule**.

b. In the **General** area, complete the following:

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

ii. 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.

iii. From the respective drop-down list, select a tenant, L3Out, encapsulation, and interface.



If L3Out is not configured on the node, you cannot select any items from the drop-down list and you cannot configure the flow rule.



For L3Out based interface rule you can select Sub-Interface type L3Out from the L3Out drop-down menu. To configure other L3Out rules such as Port Channel, SVI, and Physical Interface, click the respective tab.

iv. In the **Subnets** area, enter the subnet on which you want to monitor the flow traffic.

v. Click **Add Subnet**.

vi. Click **Save**.

9. To add an SVI rule, click **SVI** tab and perform the following:
   a. From the **Actions** drop-down menu, select **Create New Rule**.
   b. In the **General** area, complete the following:
      i. Enter the name of the rule in the **Rule Name** field.
      ii. 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.
      iii. From the respective drop-down list, select a tenant, L3Out, and encapsulation.
      iv. In the **Subnets** area, enter the subnet on which you want to monitor the flow traffic.
      v. Click **Add Subnet**.
   c. Click **Save**.
10. Click **Done**

Monitoring the Subnet for Flow Telemetry

For Flow Telemetry, you monitor the subnet as follows.

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 Cisco Nexus Dashboard Insights 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. Cisco Nexus Dashboard Insights 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.

1. Navigate to **Operate** > **Fabric**.
2. Select a fabric.
3. Verify that your **Fabrics** and the **Snapshot** values are appropriate. The default snapshot value is 15 minutes. Your selection 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 selected.

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.

Netflow

Netflow is an industry standard where Cisco routers monitor and collect network traffic on an interface. Starting with Cisco Nexus Dashboard Insights release 6.0, 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

Netflow Types

Currently, Full Netflow type is supported with Cisco Nexus Dashboard Insights.

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.

Netflow Guidelines and Limitations

- For Cisco Nexus Dashboard Insights with the ACI type, 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 for a Cisco ACI fabric.
- Netflow, in Cisco Nexus 9000 series switches, 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.
- For Netflow, Cisco Nexus Dashboard requires the configuration of persistent IP addresses under cluster configuration, and 7 IP addresses in the same subnet as the data network are required.
- After you enable Netflow in Nexus Dashboard Insights, 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.

Configure Netflow

Configure Netflow as follows.

1. Navigate to **Admin** > **System Settings** > **Flow Collection**.
2. In the **Flow Collection Mode** area, select **Flow Telemetry**.
3. In the **Flow Collection per Fabric** table, select the fabric and click the ellipsis icon.
4. Click **Edit Flow Collection Modes**.
5. In the **Edit Flow Collection Mode** page, select **Netflow**. All the flows are disabled by default. The sFlow button will remain grayed out as it is not supported for ACI type.
6. Click **Save**.

Export Data

Export Data

The **Export Data** feature enables you to export the data collected by Nexus Dashboard Insights over Kafka and Email. Nexus Dashboard Insights produces data such as advisories, anomalies, audit logs, faults, statistical data, risk and conformance reports. When you import a Kafka broker, all the data is written as a topic. By default, the export data is collected every 30 seconds or at a less frequent duration.

Starting with Nexus Dashboard Insights release 6.0.2, data can *also* be collected for specific resources (for CPU, memory, and interface utilization) every 10 seconds from the leaf and spine switches using a separate data pipeline. Additionally, CPU and memory data is collected for the controllers. The collected data is not stored in Elasticsearch by Nexus Dashboard Insights, but it is directly exported and pushed to your repository for consumption. Using the Kafka Export functionality, this data can then be exported to your Kafka Broker so that you can consume the data and push it into your data lake.

Additionally, you can configure an email scheduler to specify the data and the frequency with which you want to receive the information in an email.

Cisco Intersight is used for email notifications. See About Device Connector for more information.

Guidelines and Limitations for Export Data

- You can configure up to 5 emails per day for periodic job configurations.
- Intersight connectivity is required to receive the reports via email.
- Before configuring your Kafka Export, you must add the external Kafka IP address as a known route in your Nexus Dashboard cluster configuration.
- The following categories will be included for Anomalies in the Kafka and Email messages: Resources, Environmental, Statistics, Endpoints, Flows, Bugs.
- The following categories will not be included for Anomalies in the Kafka and Email messages: Security, Forwarding, Change Analysis, Compliance, System.
- Export data is not supported for Snapshot fabrics.
- A maximum of 5 exporters for Kafka Export for **Usage** will be supported in addition to the currently supported 5 Kafka exporters for **Alerts and Events**.
- You must provide unique names for each export, and they may not be repeated between Kafka Export for **Alerts and Events** and Kafka Export for **Usage**.
- You can configure separate Kafka Export sessions with each of the options: **Alerts and Events** and **Usage**.
- Nexus Dashboard supports Kafka export for Flow anomalies. However, Kafka export is not currently supported for Flow Event anomalies.

Configure the Kafka exporter for the Alerts and Events collection type

Follow these steps to configure the Kafka exporter for the Alerts and Events collection type.

1. Navigate to **Admin** > **System Settings** > **Export Data**.
2. In the **Message Bus Configuration** area, click **Add New** and perform the following tasks.
   a. In the **Add New Message Bus Configuration** page, **Credentials** area, **Fabric Name** field, select the appropriate fabric.
   b. In the **IP Address** and **Port** fields, enter the appropriate IP address and port.
   c. In the **Mode** field, select the security mode. The supported modes are **Unsecured**, **Secured SSL**, and **SASLPLAIN**. The default value is **Unsecured**.

      For **Secured SSL**, fill out these fields:

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

   d. In the **Collection Type** area, choose **Alerts and Events**.
   e. In the **Collection Settings** area, select the Basic or Advanced mode. The Kafka export details for the anomalies and advisories are displayed.
3. In the **Collection Settings** area for each category, choose the severity level for anomalies and advisories.
4. Click **Save**.

This configuration sends immediate notification when the selected anomalies or advisories occur. To configure an email scheduler, see the procedure Configure Email.

Configure Kafka exporter for the Usage collection type

Follow these steps to configure Kafka exporter for the Usage collection type.

1. Navigate to **Admin** > **System Settings** > **Export Data**.
2. In the **Message Bus Configuration** area, click **Add New** and perform the following tasks.

a. In the **Add New Message Bus Configuration** page, **Credentials** area, **Fabric Name** field, select the appropriate fabric.

b. In the **IP Address** and **Port** fields, enter the appropriate IP address and port.

c. In the **Mode** field, select the security mode. The supported modes are **Unsecured**, **Secured SSL**, and **SASLPLAIN**. The default value is **Unsecured**.

For **Secured SSL**, fill out these fields:

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

d. In the **Collection Type** area, choose **Usage**. The default value is **Alerts and Events**. Depending upon the Collection Type you choose, the options displayed in this area will change.

3. In the **Collection Settings** area, under **Data**, the **Category** and **Resources** for the collection settings are displayed.

   By default, the data for CPU, Memory, and Interface Utilization will be collected and exported. You cannot choose to export a subset of these resources.

4. Click **Save**.

The Kafka Export for Usage is enabled.

Configure Email

Use the following procedure to configure an email scheduler that sends the summary of the data collected from Nexus Dashboard Insights:

1. Navigate to **Admin** > **System Settings** > **Export Data**.
2. In the **Email** area, click **Add New**, and perform the following actions:
   a. In the **General Settings** area, in the **Fabric Name** field, choose the fabric name.
   b. In the **Name** field, enter the name.
   c. In the **Email** field, enter the email address. For multiple email addresses, use commas as separators.
   d. In the **Format** field, choose Text or HTML format for email.

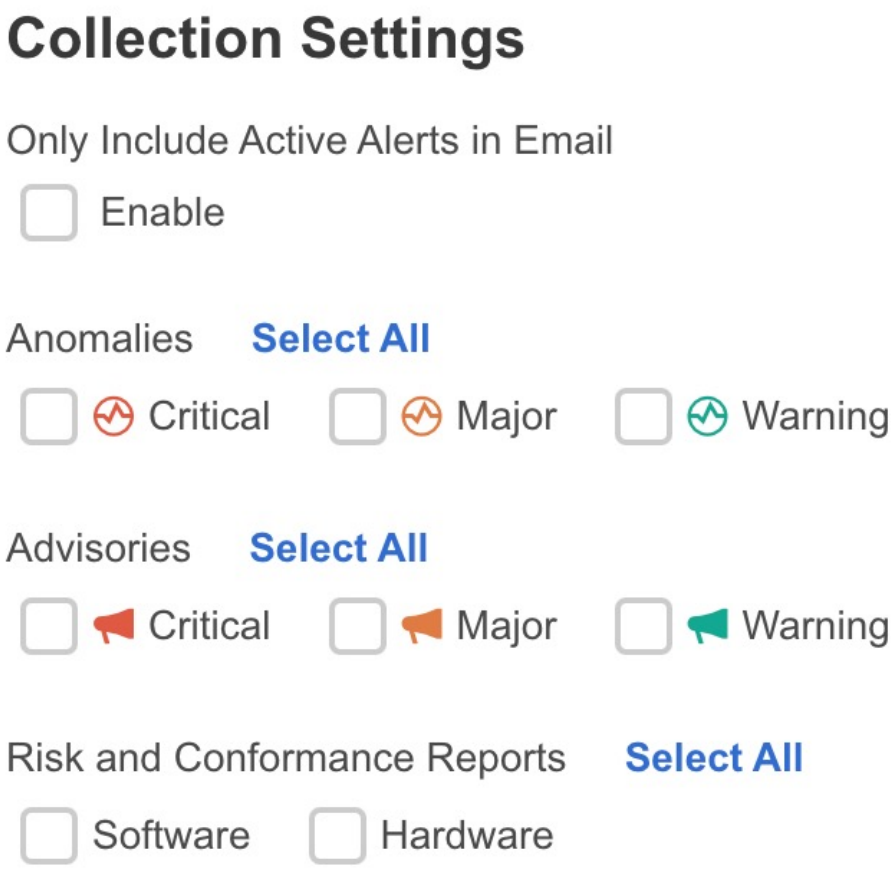
e. In the **Start Date** field, enter the start date.

f. In the **Collect Every** field, specify the frequency in days or weeks.

g. In the **Mode** field, select Basic or Advanced.

In the Basic mode, the severity for anomalies, advisories, and faults are displayed in the **Collection Settings** area. In the Advanced mode, the categories and severity for anomalies and advisories, are displayed in the **Collection Settings** area.

3. In the **Collection Settings** area for each category select the severity level for anomalies and advisories. Select all that apply. For **Active Alerts** select the enable or disable options. For **Conformance Reports**, select **Software** for software release, **Hardware** for hardware platform, and both for combination of software and hardware conformance.



4. Click **Save**. The configured email schedulers are displayed in the **Email** area.

You will receive an email about the scheduled job on the provided *Start Date* and at the time provided in *Collect Every*. The subsequent emails follow after *Collect Every* frequency expires. If the time provided is in the past, you will receive an email immediately and the next email is triggered after the expiry of the duration from the start time provided.

5. (Optional) In the edit area, perform the following steps:

a. Click ✎ to edit an email scheduler.

b. Click the  to delete an email scheduler.

Syslog

Starting from release 6.1.1, Nexus Dashboard Insights supports the export of anomalies and advisories in syslog format. You can use this feature to develop network monitoring and analytics applications on top of Nexus Dashboard Insights, 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 you set up the configuration for syslog export, Nexus Dashboard Insights will establish a connection with the syslog server and send the data to the syslog server.

Nexus Dashboard Insights will read the anomalies and advisories from the Kafka message bus and then export this data to the syslog server. With syslog support, even if you do not use Kafka, you will be able to export anomalies to your third-party tools.

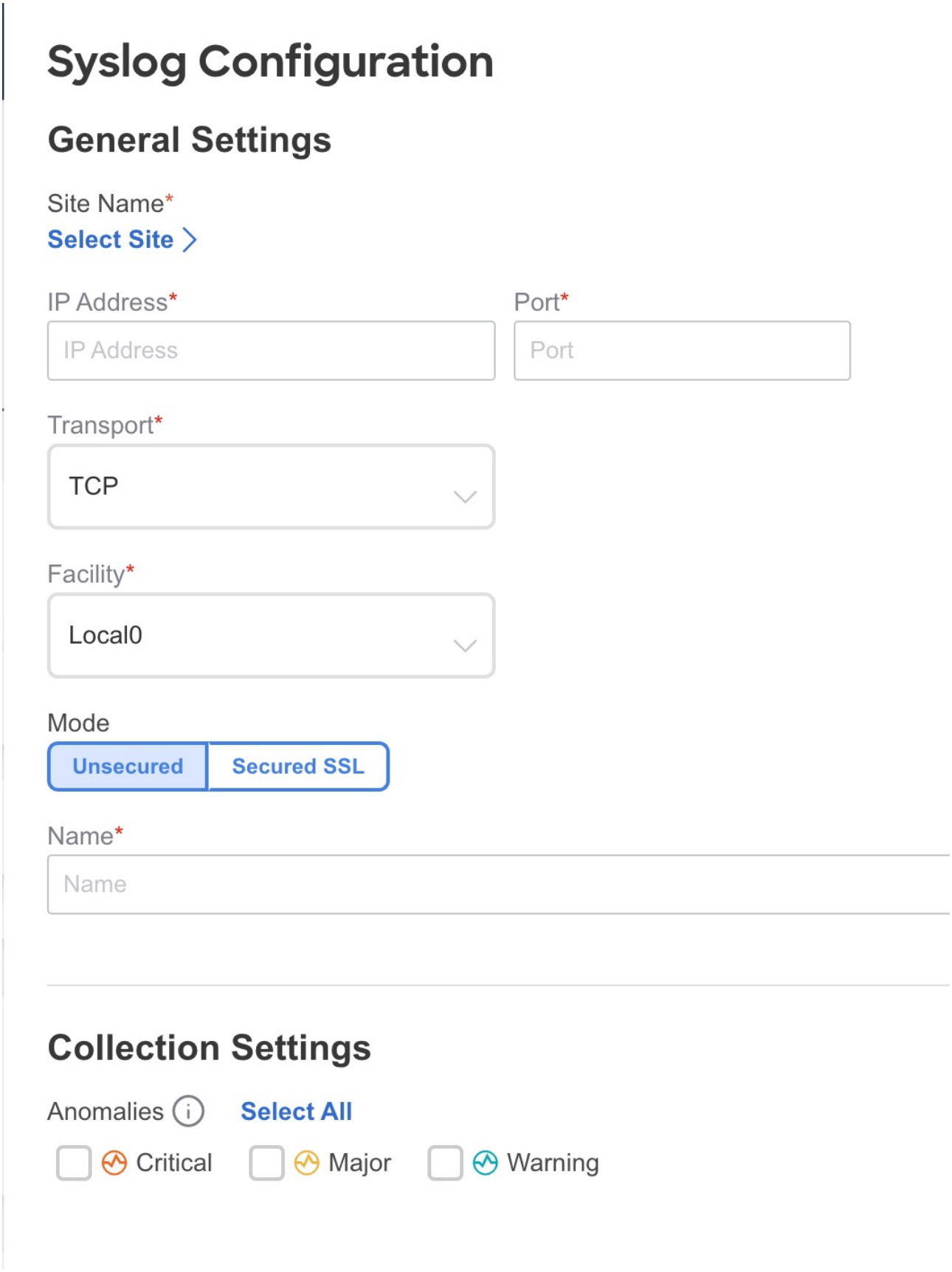
Guidelines and Limitations for Syslog

- 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.
- Nexus Dashboard Insights supports a maximum number of 5 syslog exporter configuration across fabrics.

Configure Syslog

Use the following procedure to configure syslog to enable exporting anomalies and advisories data to a syslog server:

1. Navigate to **Admin** > **System Settings** > **Export Data**.
2. In the **Syslog** field, click **Add New**.
3. In the **Syslog Configuration** dialog box, in the **Credentials** area, perform the following actions:



a. In the **Fabric Name** field, click **Select Fabric** and choose the fabric name.

b. In the **IP Address** and **Port** fields, enter the IP address and port details.

c. In the **Transport** field, from the drop-down list, choose the appropriate option. The choices are **TCP**, **UDP**, and **SSL**.

d. 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.

4. In the **Mode** field, click the toggle button to choose between **Unsecured** and **Secured SSL**.

   If you choose Secured SSL, you will be required to provide a server CA certificate.

5. In the **Configuration** area, enter a unique name for the syslog configuration for export.
6. In the **Collection Settings** area select the desired severity options.

   The options available are **Critical**, **Error**, **Warning**, and **Info**. **Major** and **Minor** anomalies and advisories in Nexus Dashboard Insights are mapped to **Error**.

7. Click **Save**.

Export Flow Records To Network Attached Storage

Starting from Nexus Dashboard Insights Release 6.3.1, you can export flow records captured by Nexus Dashboard Insights on a remote Network Attached Storage (NAS) with NFS.

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

Guidelines and Limitations

- In order for Nexus Dashboard Insights to export the flow records to an external storage, the Network Attached Storage added to Nexus Dashboard must be exclusive for Nexus Dashboard Insights.
- Network Attached Storage with Network File System (NFS) version 3 must be added to Nexus Dashboard.
- Flow Telemetry, Netflow, and sflow (only for NDFC fabrics) 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 on Nexus Dashboard to Nexus Dashboard Insights to enable export of flow records.

Add NAS to Nexus Dashboard

1. In Nexus Dashboard's Admin Console, navigate to **Admin** > **System Settings** > **Network-Attached Storage**.
2. Click **Edit**.
3. Click **Add Network-Attached Storage**.
4. Complete the following fields for **Add Network-Attached Storage**.
   a. Select **Read Write** Type. Nexus Dashboard Insights requires read and write permission to export the flow record to NAS. A system issue is raised if Nexus Dashboard Insights fails to

write to NAS.

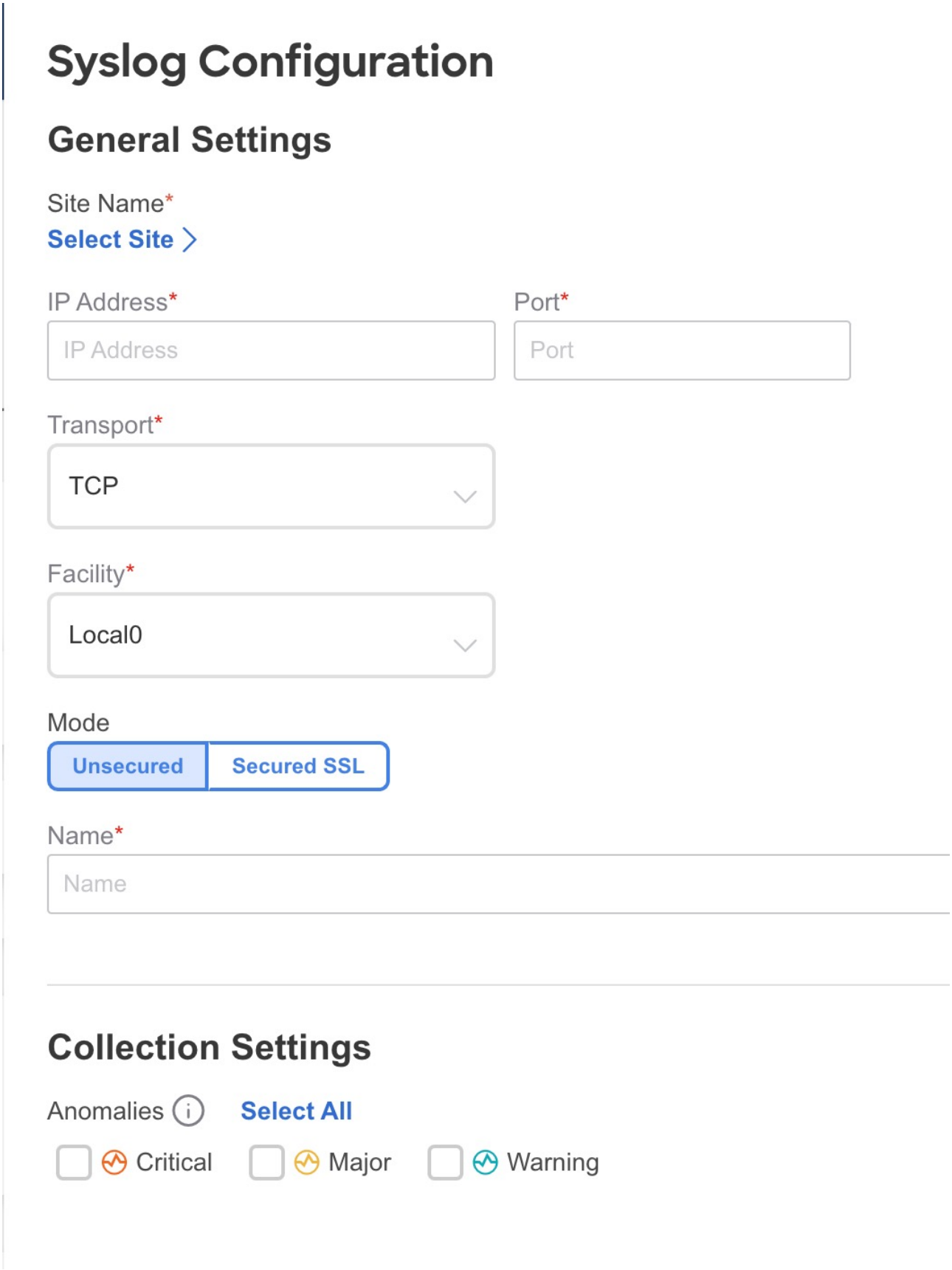


In Nexus Dashboard Insights, navigate to **Admin** > **System Settings** > **System Issues** to view the system issue.

a. Enter the name of the Network Attached Storage.
b. Enter the IP address of the Network Attached Storage.
c. Enter the port number of the Network Attached Storage.
d. Enter the export path. Using the export path, Nexus Dashboard Insights creates the directory structure in NAS for exporting the flow records.
e. Enter the alert threshold time. Alert threshold is used to send an alert when the NAS is used beyond a certain limit.
f. Enter the storage limit in Mi/Gi.
g. Click **Save**.

Add the onboarded NAS to Nexus Dashboard Insights

1. In Nexus Dashboard Insights, navigate to **Admin** > **System Settings** > **Export Data**.
2. In the Network-Attached storage area, click **Add New**.
3. Complete the following fields for **NAS Configuration**.



a. Enter the name.

b. Select the NAS server added to Nexus Dashboard from the drop-down list.

c. Click **Select Fabric** to select a fabric. You can only select one fabric at a time.

d. Select the Collection Settings for the flow from the 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.

e. Click **Save**.

4. 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.

5. 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" :" UDP" }

{" 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" ," egressVrf" :" 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,,,,,,,,\\\"]]" }

System Settings

System issues

System issues are problems that may affect the Nexus Dashboard Insights directly and they are raised for system related issues such as connectivity issues, status upgrade, onboarding configurations. The categories for system include Connectivity system issue and Collection system issue.

- A Connectivity system issue is raised when there is a failure in fabric connectivity or any connectivity issues related to Nexus Dashboard Insights.
- A Collection system issue is raised when there is a failure in enabling telemetry configuration.

View system issues

1. Navigate to **Admin** > **System Settings** > **System Issues**.
2. Use the search bar to filter the system issues. The **System Issues** table displays the filtered system issues.
3. Click a system issue to view the additional details such as What's wrong?, What's the impact?, and How do I fix it?.

System Status

The System Status page displays the collection status for your fabric for the last hour.

Nexus Dashboard Insights processes your fabrics telemetry and displays the status for the following jobs or services.

- Fabric
- Node
- Assurance
- Capacity
- Hardware Resources
- Statistics
- Endpoints
- Bug Scan
- Best Practices
- Telemetry Configuration Status

View System Status

1. Navigate to **Admin** > **System Settings** > **System Status Details**.

OR

1. Navigate to **Manage** > **Fabrics**
2. Select a fabric.
3. In the Fabrics page, from the Actions drop-down menu, select **System Status**.



In **Endpoints** column of the status table, a value of "No Data" can indicate there were no changes in the endpoint count in the last hour. This value does not necessarily indicate that there is an issue.

Import and Export of Configurations

The import and export of configurations feature enables you import and export the following configurations in Nexus Dashboard Insights:

- Flow Collection Mode
- Flow Telemetry
- Microburst
- Anomaly Rules
- Compliance
- Export Settings
- Email
- Message Bus Configurations
- Syslog
- Network Attached Storage (NAS)
- Flow Rules
- User Preferences
- Integrations



Only an administrator can manage all operations for configuration import and export.

User Preferences refers to the custom dashboards and bookmarks information. ND User Preference will not be included.

Nexus Dashboard Insights backup and restore

The Nexus Dashboard Insights 6.5.1 release introduces the unified backup and restore functionality at the Cisco Nexus Dashboard level, which backs up configuration information not only for Nexus Dashboard, but also for any services (such as Nexus Dashboard Insights) running in that Nexus Dashboard.

Even though you will use the unified backup and restore feature to back up and restore configurations at the Nexus Dashboard level, the existing import and export of configurations process at the Nexus Dashboard Insights level will continue to be available to back up and restore Nexus Dashboard Insights deployments. This is necessary for situations where you might want to restore Nexus Dashboard Insights backups from releases prior to the Nexus Dashboard Insights 6.5.1 release.

For example:

- If you backed up a configuration from the Nexus Dashboard Insights release 6.5.1 or later and you want to restore from that backup, you would use the new unified backup and restore functionality, as described in Unified Backup and Restore for Nexus Dashboard and Services.
- However, if you backed up a configuration from an Nexus Dashboard Insights release prior to 6.5.1 and you want to restore from that backup, you would use the import and export of configurations process at the Nexus Dashboard Insights level to restore that backup.

Guidelines and Limitations

- You must be an administrator user to import or export a configuration.
- Snapshot fabrics are not supported.
- Running more than one import job simultaneously could yield unpredictable results and is not supported. Perform only one import job at a time.
- Importing a configuration appends the existing configuration in Nexus Dashboard Insights.
- Importing a configuration does not affect existing anomalies, and existing assurance analyses. Existing anomalies continue to exist after importing a configuration.
- The online fabric must be onboarded on Nexus Dashboard Insights first with the same name as that in the exported configuration tar.gz file before importing all the configuration.
- Only the configurations local to Nexus Dashboard cluster is exported, and the configurations of remote Nexus Dashboard cluster is not exported.
- **Export Settings** import will fail if Nexus Dashboard Insights is not connected to Cisco Intersight. Nexus Dashboard Insights must be connected to Cisco Intersight before importing **Export Settings**.
- Import of any secured configuration that have certificates or passwords is not supported.
- The following behaviors are observed when configurations are exported from releases prior to Nexus Dashboard Insights release 6.3.1:
  - Import of Anomaly Rules with categories and severities that are deprecated in Nexus Dashboard Insights release 6.3.1 are not supported.
  - Export of fast kafka in Message Bus configuration is not supported.
- When you import an exported APIC configuration to APIC, some of the Nexus Dashboard Insights features may not work as expected due to key mismatch. You must delete the fabric from Nexus Dashboard's Admin Console as well as Nexus Dashboard Insights and then add the fabric using the same fabric name.

Exporting a Configuration

1. Navigate to **Admin** > **Configuration Import/Export**.
2. Click **Create Configuration Import/Export**.
3. In the **Create Configuration Import/Export** page, click **Export**.
4. Click **Start**. All the configurations available in Nexus Dashboard Insights are exported. All the existing configurations on the host, which includes, Fabrics, Alert Rules, Compliance, Export Settings, Flow Rules, Integrations, and User Preferences are exported. The **Configuration Import/Export** table displays information of the exported files such as status, type, start time, last update time, and content.
5. Click the ellipsis icon and choose **Download** after the export job status has moved to **Completed**. The exported configuration is downloaded as a compressed file.
6. Click the ellipsis icon and choose **Delete** to delete the configuration.

Importing a Configuration

1. Navigate to **Admin** > **Configuration Import/Export**.
2. Click **Create Configuration Import/Export**.
3. In the **Create Configuration Import/Export** page, click **Import**.
4. Select the downloaded compressed tar.gz configuration file and click **Start**. The import job details are displayed in the **Configuration Import/Export** table.
5. Click the ellipsis icon and choose **Apply** once the import job status has moved to **Validated**.
6. Select the configurations to import and click **Apply** The **Configuration Import/Export** table displays the details of the imported configuration.



When the status of the import job status is Partially Failed, some of the configurations would be added and some would be skipped due to failures. To view the reasons for the failure hover the mouse over the status column.

Copyright

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

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

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

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

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

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

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

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

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