Using Cisco Network Insights Advisor

This chapter contains the following sections:

- Using the Cisco NIA Application, on page 1

Using the Cisco NIA Application

Each Cisco device known to the Cisco NIA application is analyzed to help be more proactive about issues and anomalies in the network. Use the dashboard in the Cisco NIA application to view relevant information and select specific items to view details.

Main Dashboard

The Cisco NIA application main dashboard provides immediate access to a high-level view of the advisories, notices, issues and TAC Assist logs applicable to your network, schedule and configure bug scan, and compliance check jobs.

Property	Description
Total Controllers	Displays the total number of controllers in your network.
Total Switches	Displays the total number of switches in your network.
[Critical | Moderate | Healthy] Devices	Displays the total number of devices determined to be in one of the following categories: • Critical Devices • Moderate Devices • Healthy Devices Device counts in the higher category (Critical is highest) appear in the displayed count. If no devices are currently in the Critical category, then the device count of the Moderate category is displayed. If no issues are detected in any device, then the device count of the Healthy category is displayed.
Advisories	Displays the total number of advisories delivered for software and hardware in your network.

Property	Description
Issues By Severity	Displays the total number of issues (anomalies, bugs, and PSIRTs) delivered for software and hardware in your network.
Notices	Displays the total number of notices delivered for devices in your network.
TAC Assist	Displays the total number of TAC assist logs currently being collected or finished being collected.
Jobs	Provides access to configure and schedule bug scan, compliance check, and flow state validation jobs that run across the fabric.

Advisories Dashboard

The Advisories dashboard displays three levels of advisory severity for switch hardware and software in your network. It categorizes by severity and identifies software versions and hardware platforms to which the advisories apply.

Advisories are delivered based on the detection of relevant field notices, PSIRTs, bugs, software, hardware, and hardening violations. NIA considers this information and recommends:

- Software or hardware upgrades to address bugs, PSIRTs, and field notices
- Contacting the Technical Assistance Center (TAC)
- Measuring a software upgrade impact (disruptive/non-disruptive)
- Compliance configurations
- Advisory Report
- Software Upgrade Path and Upgrade Impact

Property	Description
Critical Advisories	Displays the number of critical advisories that are applicable to devices in your network.
Severe Advisories	Displays the number of severe advisories that are applicable to devices in your network.
Moderate Advisories	Displays the number of moderate advisories that are applicable to devices in your network.
Advisory Type by Devices	Displays the advisory types and the number of affected devices in your network for each.
Advisories Affecting (Version, Platforms)	Displays the number of advisories affecting software versions or hardware platforms.

Browse Advisories

View, sort, and filter advisories through the Browse Advisories work pane.

Advisory Report

You can view and download a Advisory Report as an Excel file from the top right corner of the **Browse Advisories** work pane. Each advisory has a tab in the Excel file that lets you view the notices, issues, advisories, and anomaly details for devices in the fabric. You can download the advisory report to your local machine and share the report for hardware upgrade recommendations.

Filters

You can refine the displayed advisory information by using the following filters:

- Operators - display advisories using an operator. Valid operators are:
  - = = - display advisories with an exact match.
- Severity - display advisories only for a specific severity. Valid severities are:
  - Critical - Returns matches for critical advisories.
  - Severe - Returns matches for severe advisories.
  - Moderate - Returns matches for moderate advisories.
- Type - display advisories only for a specific type. Valid types are:
  - S/W Ver. - Returns matches for advisories for a specific software version. This filter must be followed by a valid software version.
  - Field Notice - Returns matches for advisories for a specific field notice.
  - H/W - Returns matches for advisories for a specific hardware version. This filter must be followed by a valid hardware version.
  - Compliance - Returns matches for advisories for compliance notices.
  - TAC - Returns matches for advisories for TAC notices.

Property	Description
Advisories Chart	Displays the advisory chart for all advisories or only for the filtered severity or type.

Property	Description
Advisories List	Displays a list of all advisories or only for the filtered severity or type. Column labels are: • Severity • Last Updated Time • Type • Title: Click the link in the **Title** column to view details about the advisory. **Note** **CALLTAC**: The Call TAC advisory encompasses all the issues not addressed by the current advisories in the system. The user can contact Cisco Technical Assistance Center (TAC) to get these issues resolved with the help of a TAC expert. A user can also choose to collect the logs for the bug scan job for which this advisory was issued to help TAC, or trigger a fresh TAC Assist job for other types of call TAC advisories to collect logs for TAC experts to review. • Devices Affected

Software Upgrade Path and Upgrade Impact

When attempting to upgrade to a recommended software version, Cisco NIA app suggests an upgrade path and helps to determine the potential impact of the upgrade to the first-hop. The upgrade impact checks for NX-OS version and configuration compatibility. BIOS compatibility is not checked.

The upgrade paths table displays the various upgrade paths and the associated devices affected, non-disruptive and disruptive count.

The upgrade impact table indicates if the upgrade to the first-hop will be disruptive or non-disruptive.

Note The **feature scp-server** command should be enabled on the devices for the upgrade impact check to function.

Software upgrade recommendations typically appear in the Advisories list after a bug scan is completed. To initiate an upgrade impact, follow these steps:

1. In the navigation pane, click the browse view icon next to the **Advisories** option.

2. In the advisories list table, locate the software upgrade recommendation identified by the S/W Ver. in the **Type** column.

3. Click the software version in the **Title** column and then click **Software Version** in the title column.

The **Advisories Detail** dialog appears.

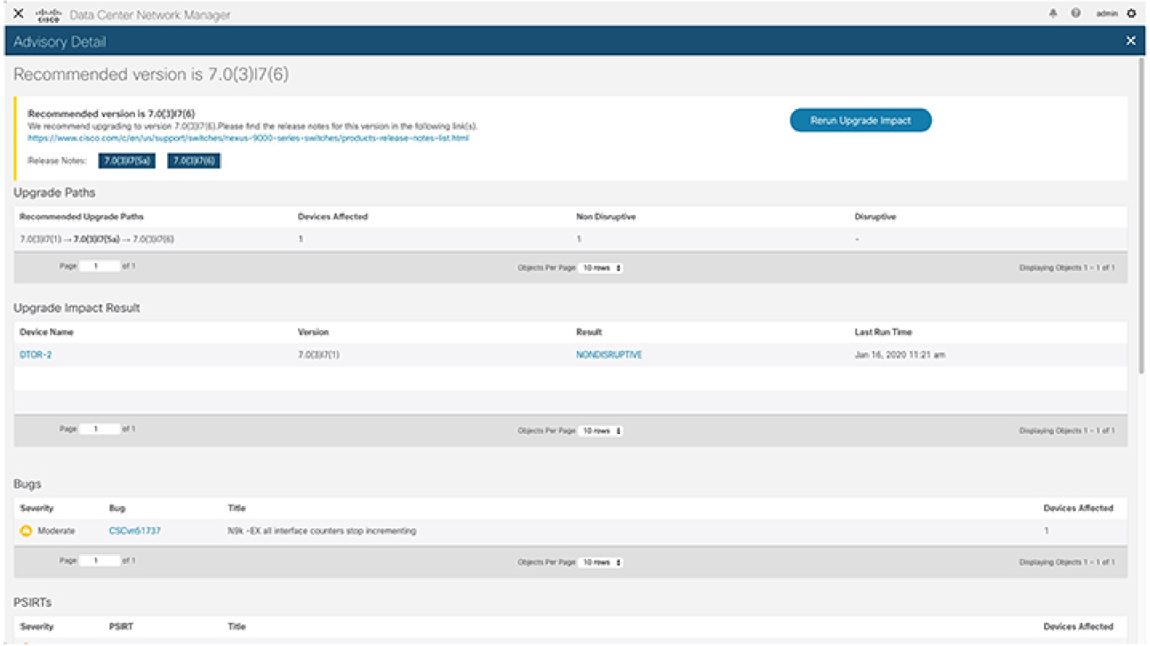
4. Click **Upgrade Impact** and then click **Run Upgrade Impact** on the **Confirm Action** dialog.

A note appears in the **Advisory Details** dialog stating that the "Upgrade Impact is currently running". In the **Upgrade Impact Results** table, the devices that could be impacted by the upgrade are listed and the **Result** column indicates that the impact process is "PENDING". Once the upgrade impact begins, the **Result** column changes to "RUNNING".

In the **Upgrade Paths** table, the **Non Disruptive** and **Disruptive** columns reflect the count for non-disruptive and disruptive types of upgrades of the **Recommended Upgrade Paths**.

Once complete, the upgrade impact result can be one of the following:

- **NON-DISRUPTIVE**: Devices can likely be upgraded to the new suggested software version without disrupting the network.
- **DISRUPTIVE**: Devices can be upgraded to the new suggested software version but with disruption, described by the reason on the result dialog.
- **FAIL**: A technical error occurred, described by the reason on the result dialog.



Recommended version is 7.0(3)I7(6)

Recommended version is 7.0(3)I7(6)
We recommend upgrading to version 7.0(3)I7(6).Please find the release notes for this version in the following link(s).
https://www.cisco.com/c/en/us/support/switches/nexus-9000-series-switches/products-release-notes-list.html

Release Notes: 7.0(3)I7(5a) 7.0(3)I7(6)

Upgrade Paths

Recommended Upgrade Paths	Devices Affected	Non Disruptive	Disruptive
7.0(3)I7(1) → **7.0(3)I7(5a)** → 7.0(3)I7(6)	1	1	-

Page 1 of 1 Objects Per Page 10 rows Displaying Objects 1 - 1 of 1

Upgrade Impact Result

Device Name	Version	Result	Last Run Time
DTOR-2	7.0(3)I7(1)	NONDISRUPTIVE	Jan 16, 2020 11:21 am

Page 1 of 1 Objects Per Page 10 rows Displaying Objects 1 - 1 of 1

Bugs

Severity	Bug	Title	Devices Affected
Moderate	CSCvn51737	N9k -EX all interface counters stop incrementing	1

Page 1 of 1 Objects Per Page 10 rows Displaying Objects 1 - 1 of 1

PSIRTs

Severity	PSIRT	Title	Devices Affected

Notices Dashboard

The Notices dashboard displays field notices such as end-of-life notices for specific switch hardware and software in your network. It categorizes notices by severity and identifies software versions and hardware platforms to which the notices apply.

Property	Description
Critical Notices	Displays the number of critical notices that are applicable to devices in your network.
Severe Notices	Displays the number of severe notices that are applicable to devices in your network.
Moderate Notices	Displays the number of moderate notices that are applicable to devices in your network.

Property	Description
Notices Chart (by notice type)	Displays the notice types and the number of affected devices in your network for each.
Notices Affecting (Versions, Platforms)	Displays the number of notices affecting software versions or hardware platforms.

Browse Notices

View, sort, and filter notices through the Browse Notices work pane.

Filters

You can refine the displayed notice information by using the following filters:

- Operators - display notices using an operator. Valid operators are:
  - = = - display notices with an exact match.
- Severity - display notices only for a specific severity. Valid severity's are:
  - Critical - Returns matches for critical notices.
  - Severe - Returns matches for severe notices.
  - Moderate - Returns matches for moderate notices.
- Type - display notices only for a specific type. Valid types are:
  - S/W Ver. - Returns matches for notices for a specific software version. This filter must be followed by a valid software version.
  - Field Notice - Returns matches for notices for a specific field notice.
  - PSIRT - Returns matches for notices for a specific PSIRT.
  - EOL H/W - Returns matches for notices for a specific hardware end-of-life.
  - EOL S/W - Returns matches for notices for a specific software end-of-life.

Property	Description
Notices Chart	Displays the notice chart for all noitces or only for the filtered severity or type.
Notices List	Displays a list of all notices or only for the filtered severity or type. Click the link in the **Title** column to view details about the notice.

Issues Dashboard

Issues are divided into these components:

- Anomalies - Compliance check violations
- Bugs - Known bugs that are automated and have show tech with matching signatures

- PSIRTs - Product Security Incident Response Team notices

Anomalies Dashboard

The Anomalies dashboard displays three levels of anomaly severity for switch hardware and software in your network. It categorizes by severity and identifies software versions and hardware platforms to which the anomalies apply.

Property	Description
Critical Anomalies	Displays the number of critical anomalies that are applicable to devices in your network.
Severe Anomalies	Displays the number of severe anomalies that are applicable to devices in your network.
Moderate Anomalies	Displays the number of moderate anomalies that are applicable to devices in your network.
Anomaly Severity by Devices (chart)	Displays the anomaly types and the number of affected devices in your network for each.
Anomalies Affecting (Versions, Platforms)	Displays the number of anomalies affecting software versions or hardware platforms.

Browse Anomalies

View, sort, and filter anomalies through the Browse Anomalies work pane.

Filters

You can refine the displayed anomaly information by using the following filters:

- Operators - display anomalies using an operator. Valid operators are:
  - = = - display anomalies with an exact match.
- Severity - display anomalies only for a specific severity. Valid severities are:
  - Critical - Returns matches for critical anomalies.
  - Severe - Returns matches for severe anomalies.
  - Moderate - Returns matches for moderate anomalies.
- Type - display anomalies only for a specific type. Valid types are:
  - Compliance - Returns matches for anomalies for a specific compliance mandate or requirement.

Property	Description
Anomalies Chart	Displays the anomaly chart for all anomalies or only for the filtered severity or type.
Anomalies List	Displays a list of all anomalies or only for the filtered severity or type.

Bugs Dashboard

The Bugs dashboard displays three levels of known bug severity for switch hardware and software in your network. It categorizes by severity and identifies software versions and hardware platforms to which the bugs apply.

Property	Description
Critical Bugs	Displays the number of critical bugs that are applicable to devices in your network.
Severe Bugs	Displays the number of severe bugs that are applicable to devices in your network.
Moderate Bugs	Displays the number of moderate bugs that are applicable to devices in your network.
Bug Severity by Devices (chart)	Displays the bug types and the number of affected devices in your network for each.
Bugs Affecting (Versions, Platforms)	Displays the number of bugs affecting software versions or hardware platforms.

Browse Bugs

View, sort, and filter bugs through the Browse Bugs work pane.

Filters

You can refine the displayed bug information by using the following filters:

- Operators - display bugs using an operator. Valid operators are:
  - = = - display bugs with an exact match.
- Severity - display bugs only for a specific severity. Valid severity's are:
  - Critical - Returns matches for critical bugs.
  - Severe - Returns matches for severe bugs.
  - Moderate - Returns matches for moderate bugs.

Property	Description
Bugs Chart	Displays the bug chart for all bugs or only for the filtered severity.
Bugs List	Displays a list of all bugs or only for the filtered severity.

PSIRTs Dashboard

The PSIRTs dashboard displays three levels of known PSIRT severity for switch hardware and software in your network. It categorizes by severity and identifies software versions and hardware platforms to which the PSIRTs apply.

Property	Description
Critical PSIRTs	Displays the number of critical PSIRTs that are applicable to devices in your network.

Property	Description
Severe PSIRTs	Displays the number of severe PSIRTs that are applicable to devices in your network.
Moderate PSIRTs	Displays the number of moderate PSIRTs that are applicable to devices in your network.
PSIRT Severity by Devices (chart)	Displays the PSIRT types and the number of affected devices in your network for each.
PSIRTs Affecting (Versions, Platforms)	Displays the number of PSIRTs affecting software versions or hardware platforms.

Browse PSIRTs

View, sort, and filter PSIRTs through the Browse PSIRTs work pane.

Filters

You can refine the displayed PSIRT information by using the following filters:

- Operators - display PSIRTs using an operator. Valid operators are:
  - = = - display PSIRTs with an exact match.
- Severity - display PSIRTs only for a specific severity. Valid severity's are:
  - Critical - Returns matches for critical PSIRTs.
  - Severe - Returns matches for severe PSIRTs.
  - Moderate - Returns matches for moderate PSIRTs.

Property	Description
PSIRTs Chart	Displays the PSIRT chart for all PSIRTs or only for the filtered severity.
PSIRTs List	Displays a list of all PSIRTs or only for the filtered severity.

Devices Dashboard

The Devices dashboard displays issues affecting devices in your network. It also identifies devices by software versions and hardware platforms.

Property	Description
Device Issues	Displays the number of devices that have reached **End of Maintenance** date for hardware and software. This also shows the number of devices currently running a version of software that is different from the Cisco Recommended Version. Click **Recommended Version Info** for more details.
Device by (chart)	Displays the different versions of software and types of hardware detected.

Property	Description
Top Devices by Maintenance Score	Displays the top six devices in critical order based on the maintenance score. The maintenance score is derived from notices and issues seen for each device according to criteria in the table below. Click on any device in this category to reveal additional details.

Maintenance Score

The following table identifies the criteria used to calculate the maintenance score displayed in the Devices dashboard and Browse Devices table.

Issue	Critical (Red)	Severe/Moderate/Low (Amber)	None (Green)
End of Maintenance Support	Less than 365 days to the end of support date	Between 365 days and 730 days to the end of support date	Greater than 730 days to the end of support date
Bugs	Any severity 1 and/or severity 2 bugs	Other than severity 1 or severity 2 bugs	No (0) bugs
Field Notices	Any applicable field notice	N/A	No applicable field notices
Compliance Failure	More than 2 compliance failures	One to two compliance failures	No (0) compliance failures
PSIRTs	Any severity 1 and/or severity 2 PSIRTs	Other than severity 1 or severity 2 PSIRTs	No (0) PSIRTs

New Device: This indicates that the device is new and no jobs have run for it.

Browse Devices

View, sort, and filter devices through the Browse Devices work pane.

Filters

You can refine the displayed device information by using the following filters:

- Operators - display devices using an operator. Valid operators are:
  - = = - display devices with an exact match.
  - contains - display device names or platform identifiers containing entered text or symbols. This operator must be followed by text and/or symbols.
  - != - display devices that are not equal to the entered text or symbols. This operator must be followed by text and/or symbols.
- Platform - display devices that are a specific type defined by the platform ID.
- Device Name - display devices that are specifically named.

- Version - displays devices based on the software version running on them.

Property	Description
Devices Chart	Displays the Devices chart for all devices or only for the filtered device name or platform product ID.
Devices List	Displays a list of all devices or only for the filtered device name or platform product ID. Click a name in the **Device Name** field to display the details for that device.

TAC Assist Dashboard

The TAC Assist dashboard has the Connected TAC Assist feature, which lets the user collect and upload the logs for devices in your network to Cisco Intersight cloud. It also enables Cisco TAC to trigger on-demand collection of logs for specified user devices and pull the logs from cloud.

The Connected TAC Assist has two modes:

- User initiated - The user collects the logs for specified devices and then the user uploads the collected logs to Cisco cloud.
- TAC triggered - Cisco TAC triggers on-demand collection of logs for specified devices and pulls the logs from Cisco cloud.

User Initiated Upload to Cloud

This section contains the steps required for you to upload the logs to cloud and Cisco TAC pulls the logs from Cisco cloud.

Before you begin

Before you upload the collected logs to cloud, make sure the fabric is conneced to Cisco Intersight cloud. See Configuring the Intersight Device Connector for details.

Step 1 Click **TAC Assist** in the Cisco DCNM navigation pane.

Step 2 Click **Begin** to initiate the log collection process.

The Collect Logs dialog appears.

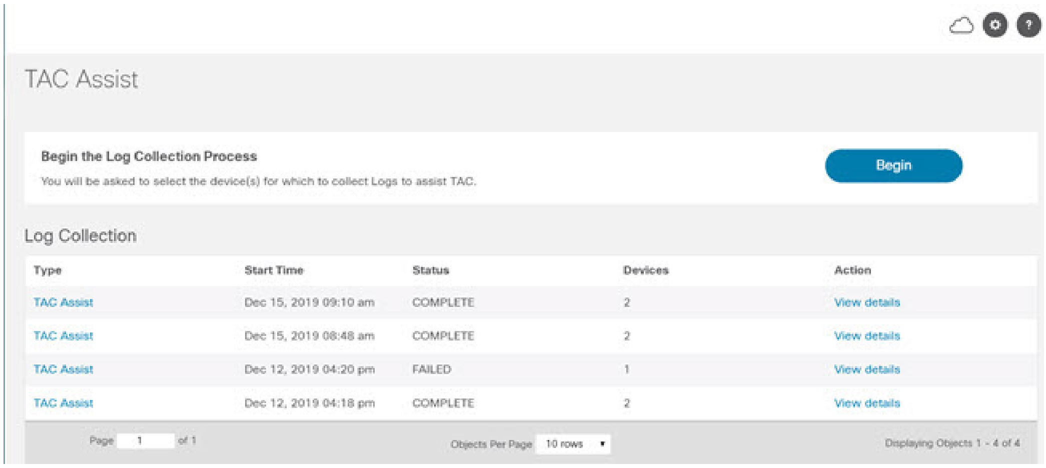
Step 3 To display specific devices in the list, use the filter utility:

- Operators - display devices using an operator. Valid operators are:
  - = = - display devices with an exact match. This operator must be followed by text and/or symbols that are the exact software version, product ID, device name, or assigned IP address of the device.
  - contains - display device names or platform identifiers containing entered text or symbols. This operator must be followed by text and/or symbols.
- Version - display devices that are running a specific software version.

- Platform - display devices that are a specific type defined by the platform ID.
- Device Name - display devices that are specifically named.
- IP Address - display devices that are assigned a specific IP address.

Step 4 From the **Collect Logs** page check the checkbox next to the device for which you want to collect logs. If you want to choose all of the devices in the list, check the checkbox next to the **Device Name** column.

The **Log Collection** section displays the new job triggered for TAC Assist.



TAC Assist

Begin the Log Collection Process

You will be asked to select the device(s) for which to collect Logs to assist TAC.

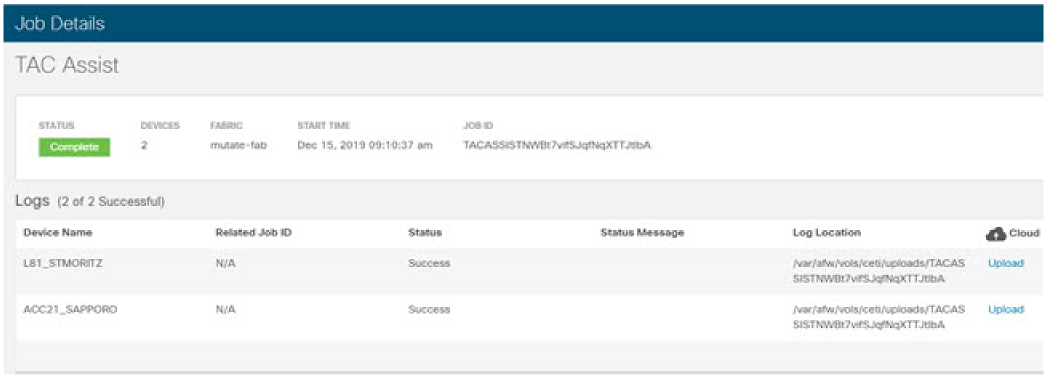
Log Collection

Type	Start Time	Status	Devices	Action
TAC Assist	Dec 15, 2019 09:10 am	COMPLETE	2	View details
TAC Assist	Dec 15, 2019 08:48 am	COMPLETE	2	View details
TAC Assist	Dec 12, 2019 04:20 pm	FAILED	1	View details
TAC Assist	Dec 12, 2019 04:18 pm	COMPLETE	2	View details

Page 1 of 1 Objects Per Page 10 rows Displaying Objects 1 - 4 of 4

Step 5 Click **View Details** from the list of logs to display the **Job Details** page.

All information about TAC Assist job including, status, devices, fabric, start time, job id, device name, log location, and cloud upload appear in the work pane.



Job Details

TAC Assist

STATUS	DEVICES	FABRIC	START TIME	JOB ID
Complete	2	mutate-fab	Dec 15, 2019 09:10:37 am	TACASSISTNWBt7vifSJqfNqXTTJtlbA

Logs (2 of 2 Successful)

Device Name	Related Job ID	Status	Status Message	Log Location	Cloud
L81_STMORITZ	N/A	Success		/var/afw/vols/ceti/uploads/TACASSISTNWBt7vifSJqfNqXTTJtlbA	Upload
ACC21_SAPPORO	N/A	Success		/var/afw/vols/ceti/uploads/TACASSISTNWBt7vifSJqfNqXTTJtlbA	Upload

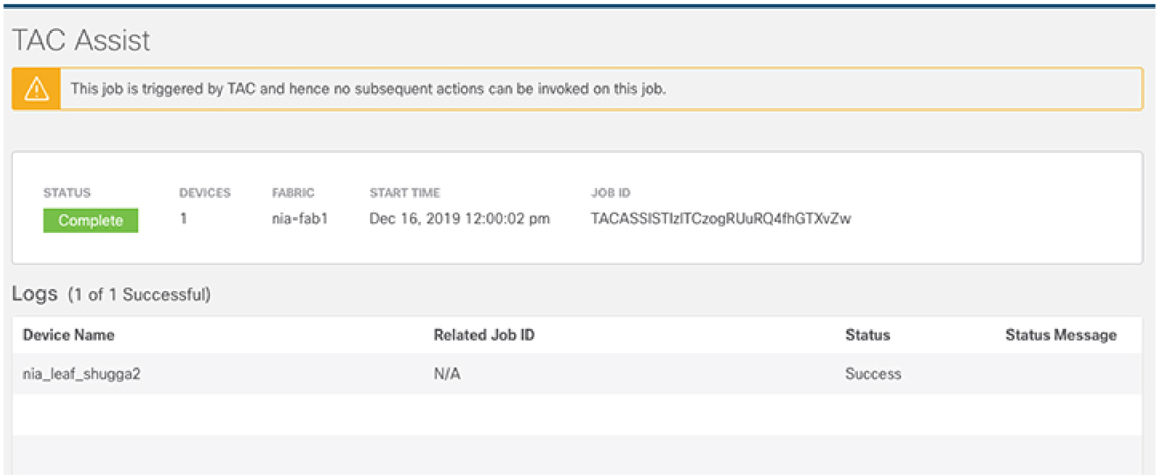
Step 6 Click **Upload** to upload the collected logs to Cisco Intersight Cloud.

The **Cloud** status shows **Complete** when the upload of collected logs to Cisco Intersight Cloud is complete.

TAC Initiated Pull from Cloud

The Connected TAC Assist also enables Cisco TAC to trigger on-demand collecion of logs for specified user devices and pulls the logs from cloud.

Click **View Details** from list of logs to display the job details page.



TAC Assist

⚠ This job is triggered by TAC and hence no subsequent actions can be invoked on this job.

STATUS	DEVICES	FABRIC	START TIME	JOB ID
Complete	1	nia-fab1	Dec 16, 2019 12:00:02 pm	TACASSISTIzITCzogRUuRQ4fhGTXvZw

Logs (1 of 1 Successful)

Device Name	Related Job ID	Status	Status Message
nia_leaf_shugga2	N/A	Success	

The **View Details** page shows a message that the job is triggered by TAC and hence no subsequent actions can be invoked on this job.

Jobs Dashboard

The Jobs dashboard provides access to configure and schedule bug scan and compliance check jobs that run for a specific fabric. The flow state validator gathers information about flow related issues.

Fabric

The Fabric Job provides access to configure and schedule bug scan and compliance check jobs that run for a specific fabric.

1. Click **Fabric** > ⚙ icon on the left navigation pane to schedule a log collection fabric job for bug scan and compliance check for the selected fabrics.

   The Fabric Job Configuration page appears.

2. Click **Configure** to schedule a on-demand bug scan or compliance check job for the selected fabric.

   Choose the scheduled job time and date and click **Apply**.

3. Click the browse view icon on the left navigation pane to view the scheduled jobs for the selected fabric and time range from the **Fabric Job List** page.

   To display specific devices in the list, use the filter utility:

   - Operators - display devices using an operator. Valid operators are:
     - == - display devices with an exact match. This operator must be followed by text and/or symbols that are the exact time, summary, start time, status, devices, and action for the fabric.
     - contains - display device names or platform identifiers containing entered text or symbols. This operator must be followed by text and/or symbols.
   - Status - display devices with a specific status.

- Summary - display devices that have a specific summary.

The **Bug Scan**: User can schedule or run an on-demand Bug-scan on their network. Cisco NIA app collects technical support information from all the devices and runs them against known set of signatures, and then flags the corresponding defects. Cisco NIA app also generates an advisory for the customer. For further details, see Advisories from Advisories Dashboard, on page 2.

The **Compliance Check**: User can schedule or run an on-demand Compliance Check on their network. Cisco NIA app collects technical support information from the selected devices and runs them against known set of signatures and, then flags the defects that are not compliant. Cisco NIA app also generates an anomaly list for the customer. For further details, see Anomalies from Issues Dashboard, on page 6 and view anomaly details.

Global

The Global Job provides access to configure and schedule flow state validator jobs that run across the network.

Flow State Validator

Flow state validator is a micro-service launched through Cisco NIA, used for tracing end-to-end forwarding path for a given flow and narrowing down the offending device on its path.

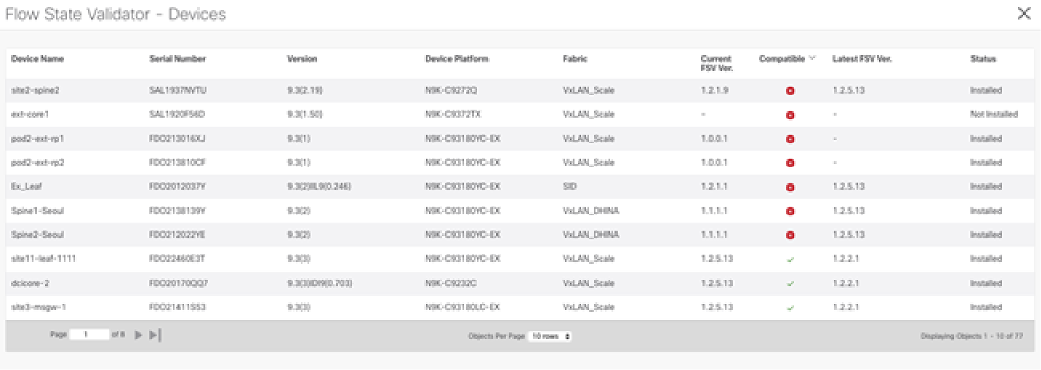
The flow state validator detects and isolates offending nodes in the network for a given flow and includes the following functionalities.

- Traces all possible forwarding paths for a given flow across source to destination endpoints.
- Identifies the offending device with issue, resulting in the flow drop.
- Helps troubleshoot to narrow down the root cause of the issue, including running forwarding path checks, software and hardware states programming consistencies through consistency-checkers, and further details related to packets walkthrough.

The Cisco NIA agent is a RPM based application service, which is pre-installed on the Cisco NX-OS. The Cisco NIA agent gets the path for a specific flow. The flow validator uses the path returned from the agent and goes to the next hop running flow validation job.

Click **Global** > ⚙ icon on the left navigation pane to schedule a global job that gathers information about your network across all fabrics. It allows you to enter flow details.

The **Global Job Configuration** page appears. The **Global Job Configuration** page lists the number of devices compatible with flow state validator.



Flow State Validator - Devices

Device Name	Serial Number	Version	Device Platform	Fabric	Current FSV Ver.	Compatible	Latest FSV Ver.	Status
site2-spine2	SAL1937NVTU	9.3(2.19)	N9K-C9272Q	VxLAN_Scale	1.2.1.9	⊗	1.2.5.13	Installed
ext-core1	SAL1920F56D	9.3(1.50)	N9K-C9372TX	VxLAN_Scale	-	⊗	-	Not Installed
pod2-ext-rp1	FDO213016XJ	9.3(1)	N9K-C93180YC-EX	VxLAN_Scale	1.0.0.1	⊗	-	Installed
pod2-ext-rp2	FDO213810CF	9.3(1)	N9K-C93180YC-EX	VxLAN_Scale	1.0.0.1	⊗	-	Installed
Ex_Leaf	FDO2012037Y	9.3(2)IIL9(0.246)	N9K-C93180YC-EX	SID	1.2.1.1	⊗	1.2.5.13	Installed
Spine1-Seoul	FDO2138139Y	9.3(2)	N9K-C93180YC-EX	VxLAN_DHINA	1.1.1.1	⊗	1.2.5.13	Installed
Spine2-Seoul	FDO2122022YE	9.3(2)	N9K-C93180YC-EX	VxLAN_DHINA	1.1.1.1	⊗	1.2.5.13	Installed
site11-leaf-1111	FDO22460E3T	9.3(3)	N9K-C93180YC-EX	VxLAN_Scale	1.2.5.13	✓	1.2.2.1	Installed
dcicore-2	FDO20170QQ7	9.3(3)IDI9(0.703)	N9K-C9232C	VxLAN_Scale	1.2.5.13	✓	1.2.2.1	Installed
site3-msgw-1	FDO21411S53	9.3(3)	N9K-C93180LC-EX	VxLAN_Scale	1.2.5.13	✓	1.2.2.1	Installed

Page 1 of 8 Objects Per Page 10 rows Displaying Objects 1 - 10 of 77

- Click **View Devices** to view granular information about the devices such as device name, serial number, device platform, fabric, minimum and maximum flow state validator version.
- Click **Update** to trigger a latest Cisco NIA agent RPM install for all the devices that are compatible with flow state validator to the latest version.

Start Flow State Validator

Use this procedure to schedule a flow state validator job for all the devices compatible with flow state validator.

Step 1 Choose **Jobs** > **Global Configuration** from the left navigation pane.

Step 2 On the Global Job Configuration page choose the **VXLAN** or **Classic LAN** installation mode.

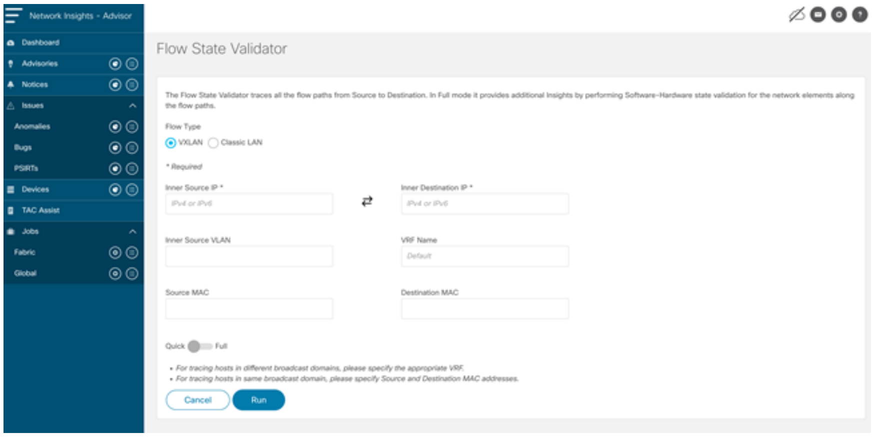
Step 3 Enter the required fields and optinal fields to configure the flow state validator job.

Flow State Validator Job	Input Fields
Classic Lan - L3 routed flow	Mandatory: Source IP address, Destination IP address, and VRF name (if non-default). Optional: All the other fields such as Source MAC address, Destination MAC address, and Source VLAN.
VXLAN – L2 VNI switched flow	Mandatory: Source IP address, Destination IP address, Destination MAC address, and Source MAC address. Optional: All the other fields on the UI.
VXLAN – L3 VNI routed flow	Mandatory: Source IP address, Destination IP address, and VRF name. Optional: All the other fields such as Source MAC address, Destination MAC address, and Source VLAN.

Step 4 Toggle between **Quick** or **Full** IP address checks in the network.

The **Quick** validator traces the network path using L2, L3, and VXLAN CLI for a specific flow to detect and isolate the offending nodes that result in the flow drop.

The **Full** validator runs consistency checker between software and hardware for programming consistencies. It also traces the network path using L2, L3, and VXLAN CLI for a specific flow.



Flow State Validator

The Flow State Validator traces all the flow paths from Source to Destination. In Full mode it provides additional insights by performing Software-Hardware state validation for the network elements along the flow paths.

Flow Type

● VXLAN ○ Classic LAN

** Required*

Inner Source IP *: IPv4 or IPv6 ⇄ Inner Destination IP *: IPv4 or IPv6

Inner Source VLAN

VRF Name: Default

Source MAC

Destination MAC

Quick — Full

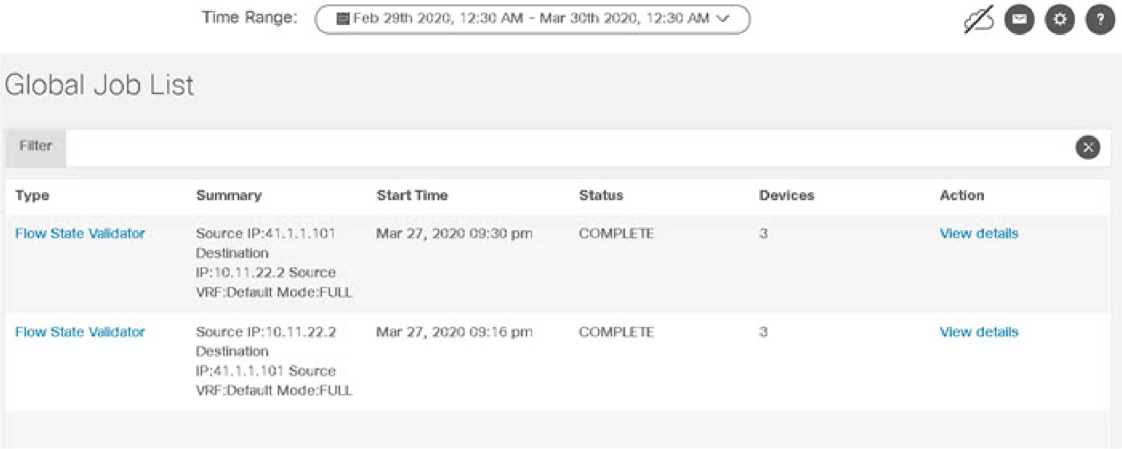
- *For tracing hosts in different broadcast domains, please specify the appropriate VRF.*
- *For tracing hosts in same broadcast domain, please specify Source and Destination MAC addresses.*

Cancel Run

Step 5 Click **Run** to run the flow state validator job.

View Flow State Validator

To view the **Global Job Configuration** page, click the settings icon from the left navigation pane. This page shows the current running flow state validator jobs.



Time Range: Feb 29th 2020, 12:30 AM - Mar 30th 2020, 12:30 AM

Global Job List

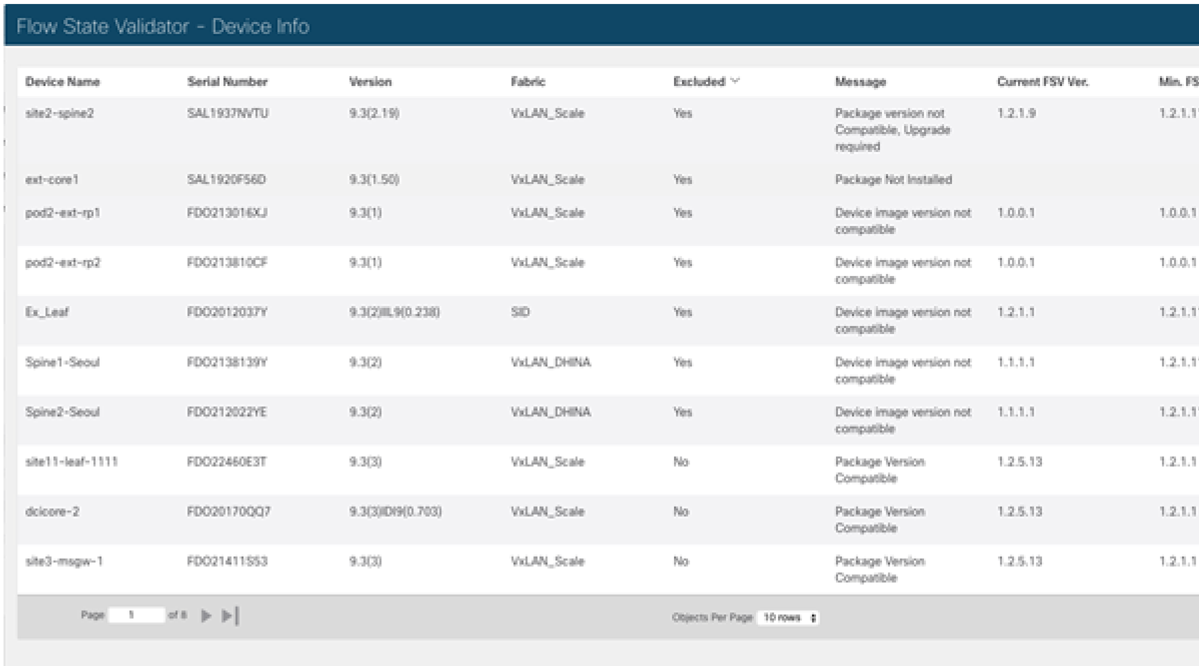
Filter

Type	Summary	Start Time	Status	Devices	Action
Flow State Validator	Source IP:41.1.1.101 Destination IP:10.11.22.2 Source VRF:Default Mode:FULL	Mar 27, 2020 09:30 pm	COMPLETE	3	View details
Flow State Validator	Source IP:10.11.22.2 Destination IP:41.1.1.101 Source VRF:Default Mode:FULL	Mar 27, 2020 09:16 pm	COMPLETE	3	View details

The flow state validator job details page consists of the following sections.

- Configuration Summary: Provides information for the validator job such as start time, SIP, DIP, devices, etc. The number of devices on this page indicates the total number of devices flow state validator was initiated.

  Click **Device Count** to view details about the devices that were part of that validator job. This can be used to debug and ascertain why a certain device was not part of the validator job.



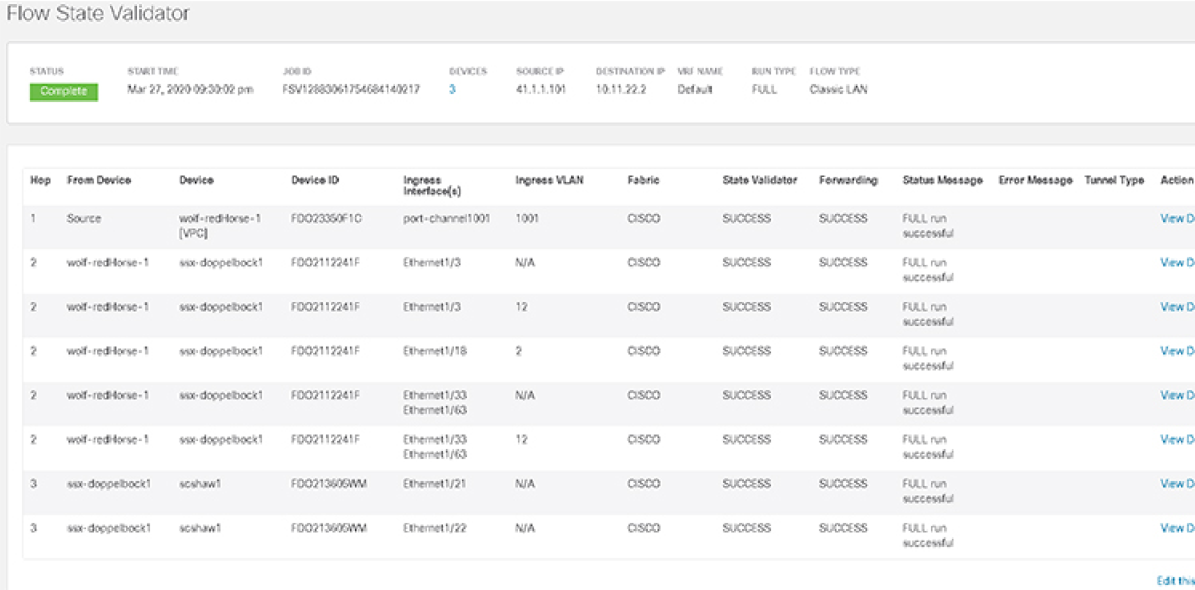
Flow State Validator - Device Info

Device Name	Serial Number	Version	Fabric	Excluded	Message	Current FSV Ver.	Min. FS
site2-spine2	SAL1937NVTU	9.3(2.19)	VxLAN_Scale	Yes	Package version not Compatible, Upgrade required	1.2.1.9	1.2.1.1
ext-core1	SAL1920F56D	9.3(1.50)	VxLAN_Scale	Yes	Package Not Installed		
pod2-ext-rp1	FDO213016XJ	9.3(1)	VxLAN_Scale	Yes	Device image version not compatible	1.0.0.1	1.0.0.1
pod2-ext-rp2	FDO213810CF	9.3(1)	VxLAN_Scale	Yes	Device image version not compatible	1.0.0.1	1.0.0.1
Ex_Leaf	FDO2012037Y	9.3(2)IIL9(0.238)	SID	Yes	Device image version not compatible	1.2.1.1	1.2.1.1
Spine1-Seoul	FDO2138139Y	9.3(2)	VxLAN_DHINA	Yes	Device image version not compatible	1.1.1.1	1.2.1.1
Spine2-Seoul	FDO212022YE	9.3(2)	VxLAN_DHINA	Yes	Device image version not compatible	1.1.1.1	1.2.1.1
site11-leaf-1111	FDO22460E3T	9.3(3)	VxLAN_Scale	No	Package Version Compatible	1.2.5.13	1.2.1.1
dcicore-2	FDO20170QQ7	9.3(3)IDI9(0.703)	VxLAN_Scale	No	Package Version Compatible	1.2.5.13	1.2.1.1
site3-msgw-1	FDO21411SS3	9.3(3)	VxLAN_Scale	No	Package Version Compatible	1.2.5.13	1.2.1.1

Page 1 of 8

Objects Per Page 10 rows

- Flow Summary: Consists of the device related information, which the flow state validator job traversed. Each row indicates a path traversed in the flow from source IP address to the destination IP address along with other details such as ingress interface, forwarding status, path source, and destination.



Flow State Validator

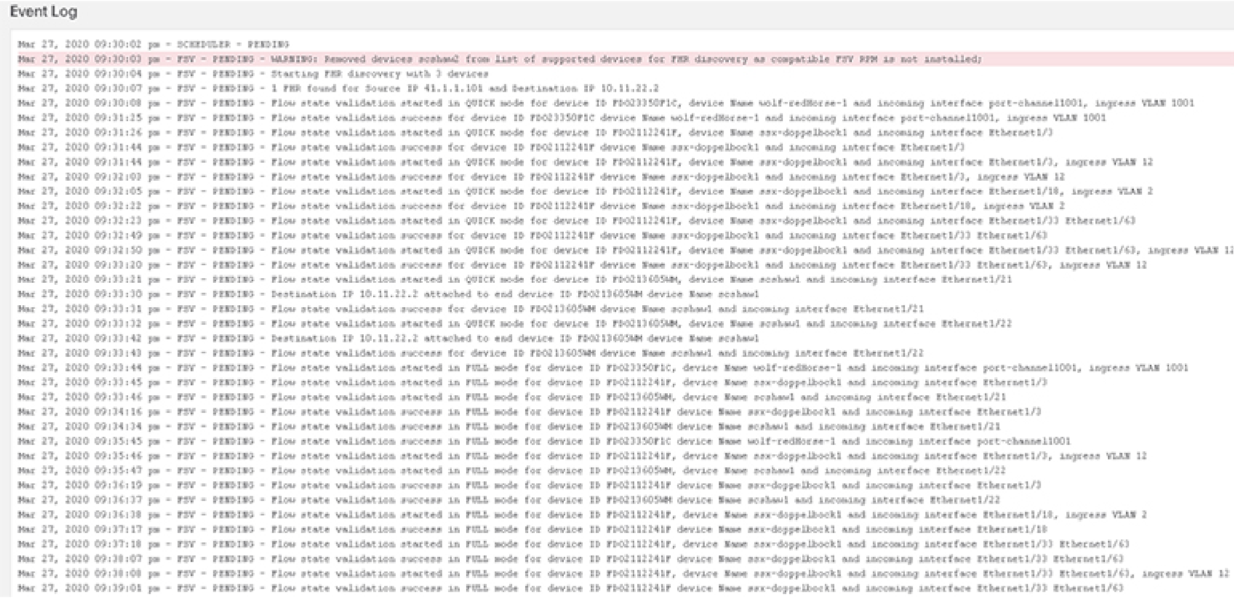
STATUS	START TIME	JOB ID	DEVICES	SOURCE IP	DESTINATION IP	VRF NAME	RUN TYPE	FLOW TYPE
Complete	Mar 27, 2020 09:30:02 pm	FSV12883061754684140217	3	41.1.1.101	10.11.22.2	Default	FULL	Classic LAN

Hop	From Device	Device	Device ID	Ingress Interface(s)	Ingress VLAN	Fabric	State Validator	Forwarding	Status Message	Error Message	Tunnel Type	Action
1	Source	wolf-redHorse-1 [VPC]	FDO23350F1C	port-channel1001	1001	CISCO	SUCCESS	SUCCESS	FULL run successful			View D
2	wolf-redHorse-1	ssx-doppelbock1	FDO2112241F	Ethernet1/3	N/A	CISCO	SUCCESS	SUCCESS	FULL run successful			View D
2	wolf-redHorse-1	ssx-doppelbock1	FDO2112241F	Ethernet1/3	12	CISCO	SUCCESS	SUCCESS	FULL run successful			View D
2	wolf-redHorse-1	ssx-doppelbock1	FDO2112241F	Ethernet1/18	2	CISCO	SUCCESS	SUCCESS	FULL run successful			View D
2	wolf-redHorse-1	ssx-doppelbock1	FDO2112241F	Ethernet1/33 Ethernet1/63	N/A	CISCO	SUCCESS	SUCCESS	FULL run successful			View D
2	wolf-redHorse-1	ssx-doppelbock1	FDO2112241F	Ethernet1/33 Ethernet1/63	12	CISCO	SUCCESS	SUCCESS	FULL run successful			View D
3	ssx-doppelbock1	scshaw1	FDO213606WM	Ethernet1/21	N/A	CISCO	SUCCESS	SUCCESS	FULL run successful			View D
3	ssx-doppelbock1	scshaw1	FDO213606WM	Ethernet1/22	N/A	CISCO	SUCCESS	SUCCESS	FULL run successful			View D

Edit this

The **Current Running Global Jobs** lists the jobs that are currently executing. While the flow state validator job is progressing, click the job title to view the **Event Log** for the job.

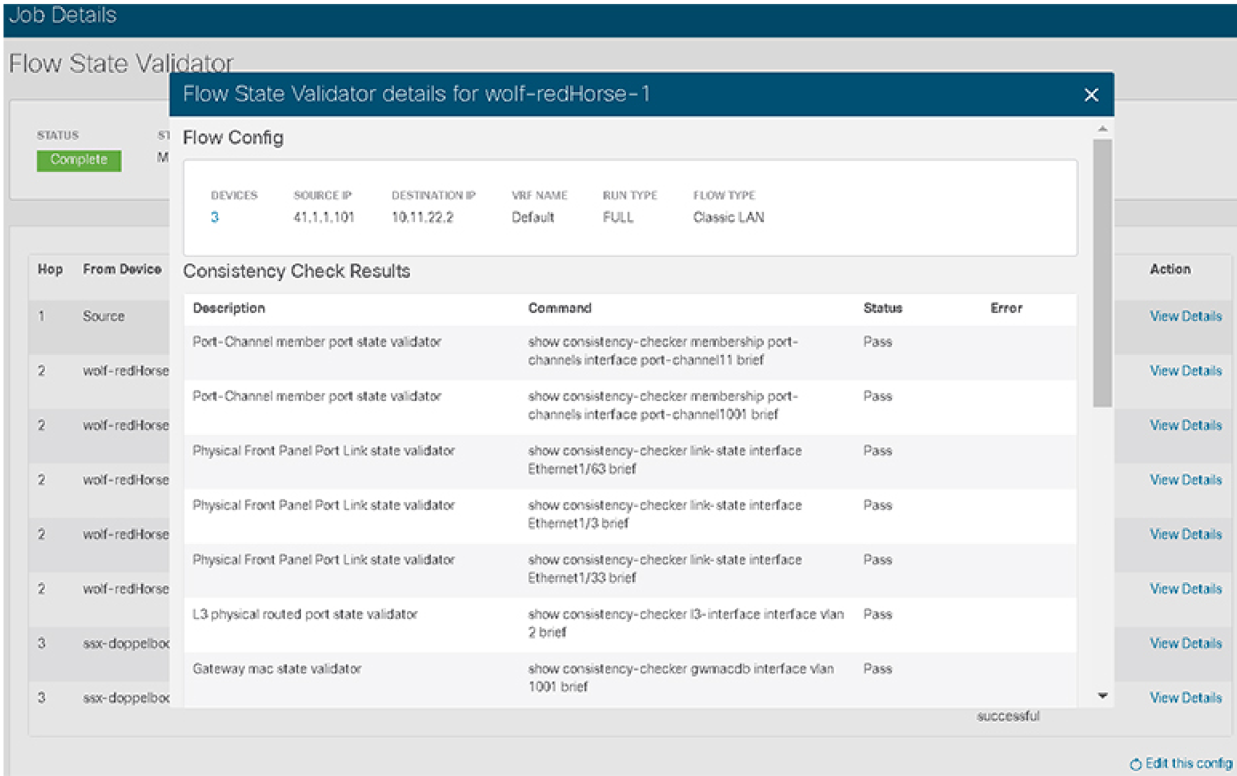
The **Event Log** consists of job logs helpful for checking and debugging the job as it progresses. The log includes information such as devices discovered, warnings, and errors.



Event Log

```
Mar 27, 2020 09:30:02 pm - SCHEDULER - PENDING
Mar 27, 2020 09:30:03 pm - FSV - PENDING - WARNING: Removed devices scshaw2 from list of supported devices for FHR discovery as compatible FSV RPM is not installed;
Mar 27, 2020 09:30:04 pm - FSV - PENDING - Starting FHR discovery with 3 devices
Mar 27, 2020 09:30:07 pm - FSV - PENDING - 1 FHR found for Source IP 41.1.1.101 and Destination IP 10.11.22.2
Mar 27, 2020 09:30:08 pm - FSV - PENDING - Flow state validation started in QUICK mode for device ID FDO23350F1C, device Name wolf-redHorse-1 and incoming interface port-channel1001, ingress VLAN 1001
Mar 27, 2020 09:31:25 pm - FSV - PENDING - Flow state validation success for device ID FDO23350F1C device Name wolf-redHorse-1 and incoming interface port-channel1001, ingress VLAN 1001
Mar 27, 2020 09:31:26 pm - FSV - PENDING - Flow state validation started in QUICK mode for device ID FDO2112241F, device Name ssx-doppelbock1 and incoming interface Ethernet1/3
Mar 27, 2020 09:31:44 pm - FSV - PENDING - Flow state validation success for device ID FDO2112241F device Name ssx-doppelbock1 and incoming interface Ethernet1/3
Mar 27, 2020 09:31:44 pm - FSV - PENDING - Flow state validation started in QUICK mode for device ID FDO2112241F, device Name ssx-doppelbock1 and incoming interface Ethernet1/3, ingress VLAN 12
Mar 27, 2020 09:32:03 pm - FSV - PENDING - Flow state validation success for device ID FDO2112241F device Name ssx-doppelbock1 and incoming interface Ethernet1/3, ingress VLAN 12
Mar 27, 2020 09:32:05 pm - FSV - PENDING - Flow state validation started in QUICK mode for device ID FDO2112241F, device Name ssx-doppelbock1 and incoming interface Ethernet1/18, ingress VLAN 2
Mar 27, 2020 09:32:22 pm - FSV - PENDING - Flow state validation success for device ID FDO2112241F device Name ssx-doppelbock1 and incoming interface Ethernet1/18, ingress VLAN 2
Mar 27, 2020 09:32:23 pm - FSV - PENDING - Flow state validation started in QUICK mode for device ID FDO2112241F, device Name ssx-doppelbock1 and incoming interface Ethernet1/33 Ethernet1/63
Mar 27, 2020 09:32:49 pm - FSV - PENDING - Flow state validation success for device ID FDO2112241F device Name ssx-doppelbock1 and incoming interface Ethernet1/33 Ethernet1/63
Mar 27, 2020 09:32:50 pm - FSV - PENDING - Flow state validation started in QUICK mode for device ID FDO2112241F, device Name ssx-doppelbock1 and incoming interface Ethernet1/33 Ethernet1/63, ingress VLAN 1
Mar 27, 2020 09:33:20 pm - FSV - PENDING - Flow state validation success for device ID FDO2112241F device Name ssx-doppelbock1 and incoming interface Ethernet1/33 Ethernet1/63, ingress VLAN 12
Mar 27, 2020 09:33:21 pm - FSV - PENDING - Flow state validation started in QUICK mode for device ID FDO213605WM, device Name scshaw1 and incoming interface Ethernet1/21
Mar 27, 2020 09:33:30 pm - FSV - PENDING - Destination IP 10.11.22.2 attached to end device ID FDO213605WM device Name scshaw1
Mar 27, 2020 09:33:31 pm - FSV - PENDING - Flow state validation success for device ID FDO213605WM device Name scshaw1 and incoming interface Ethernet1/21
Mar 27, 2020 09:33:32 pm - FSV - PENDING - Flow state validation started in QUICK mode for device ID FDO213605WM, device Name scshaw1 and incoming interface Ethernet1/22
Mar 27, 2020 09:33:42 pm - FSV - PENDING - Destination IP 10.11.22.2 attached to end device ID FDO213605WM device Name scshaw1
Mar 27, 2020 09:33:43 pm - FSV - PENDING - Flow state validation success for device ID FDO213605WM device Name scshaw1 and incoming interface Ethernet1/22
Mar 27, 2020 09:33:44 pm - FSV - PENDING - Flow state validation started in FULL mode for device ID FDO23350F1C, device Name wolf-redHorse-1 and incoming interface port-channel1001, ingress VLAN 1001
Mar 27, 2020 09:33:45 pm - FSV - PENDING - Flow state validation started in FULL mode for device ID FDO2112241F, device Name ssx-doppelbock1 and incoming interface Ethernet1/3
Mar 27, 2020 09:33:46 pm - FSV - PENDING - Flow state validation started in FULL mode for device ID FDO213605WM, device Name scshaw1 and incoming interface Ethernet1/21
Mar 27, 2020 09:34:16 pm - FSV - PENDING - Flow state validation success in FULL mode for device ID FDO2112241F device Name ssx-doppelbock1 and incoming interface Ethernet1/3
Mar 27, 2020 09:34:34 pm - FSV - PENDING - Flow state validation success in FULL mode for device ID FDO213605WM device Name scshaw1 and incoming interface Ethernet1/21
Mar 27, 2020 09:35:45 pm - FSV - PENDING - Flow state validation success in FULL mode for device ID FDO23350F1C device Name wolf-redHorse-1 and incoming interface port-channel1001
Mar 27, 2020 09:35:46 pm - FSV - PENDING - Flow state validation started in FULL mode for device ID FDO2112241F, device Name ssx-doppelbock1 and incoming interface Ethernet1/3, ingress VLAN 12
Mar 27, 2020 09:35:47 pm - FSV - PENDING - Flow state validation started in FULL mode for device ID FDO213605WM, device Name scshaw1 and incoming interface Ethernet1/22
Mar 27, 2020 09:36:19 pm - FSV - PENDING - Flow state validation success in FULL mode for device ID FDO2112241F device Name ssx-doppelbock1 and incoming interface Ethernet1/3
Mar 27, 2020 09:36:37 pm - FSV - PENDING - Flow state validation success in FULL mode for device ID FDO213605WM device Name scshaw1 and incoming interface Ethernet1/22
Mar 27, 2020 09:36:38 pm - FSV - PENDING - Flow state validation started in FULL mode for device ID FDO2112241F, device Name ssx-doppelbock1 and incoming interface Ethernet1/18, ingress VLAN 2
Mar 27, 2020 09:37:17 pm - FSV - PENDING - Flow state validation success in FULL mode for device ID FDO2112241F device Name ssx-doppelbock1 and incoming interface Ethernet1/18
Mar 27, 2020 09:37:18 pm - FSV - PENDING - Flow state validation started in FULL mode for device ID FDO2112241F, device Name ssx-doppelbock1 and incoming interface Ethernet1/33 Ethernet1/63
Mar 27, 2020 09:38:07 pm - FSV - PENDING - Flow state validation success in FULL mode for device ID FDO2112241F device Name ssx-doppelbock1 and incoming interface Ethernet1/33 Ethernet1/63
Mar 27, 2020 09:38:08 pm - FSV - PENDING - Flow state validation started in FULL mode for device ID FDO2112241F, device Name ssx-doppelbock1 and incoming interface Ethernet1/33 Ethernet1/63, ingress VLAN 1
Mar 27, 2020 09:39:01 pm - FSV - PENDING - Flow state validation success in FULL mode for device ID FDO2112241F device Name ssx-doppelbock1 and incoming interface Ethernet1/33 Ethernet1/63
```

Click **View Details** for further details such as consistency check and path information. In case consistency check fails, you can select the failed devices and run bug scan or TAC assist on these devices.



Job Details

Flow State Validator

STATUS: Complete

Flow State Validator details for wolf-redHorse-1

Flow Config

DEVICES	SOURCE IP	DESTINATION IP	VRF NAME	RUN TYPE	FLOW TYPE
3	41.1.1.101	10.11.22.2	Default	FULL	Classic LAN

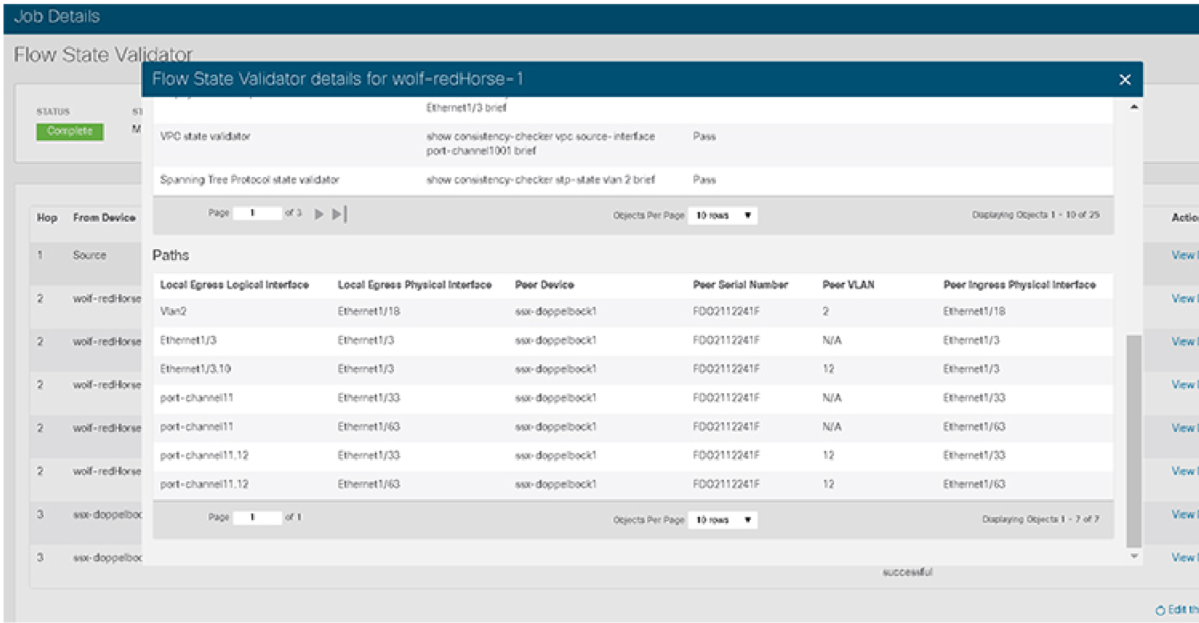
Consistency Check Results

Description	Command	Status	Error
Port-Channel member port state validator	show consistency-checker membership port-channels interface port-channel11 brief	Pass	
Port-Channel member port state validator	show consistency-checker membership port-channels interface port-channel1001 brief	Pass	
Physical Front Panel Port Link state validator	show consistency-checker link-state interface Ethernet1/63 brief	Pass	
Physical Front Panel Port Link state validator	show consistency-checker link-state interface Ethernet1/3 brief	Pass	
Physical Front Panel Port Link state validator	show consistency-checker link-state interface Ethernet1/33 brief	Pass	
L3 physical routed port state validator	show consistency-checker l3-interface interface vlan 2 brief	Pass	
Gateway mac state validator	show consistency-checker gwmacdb interface vlan 1001 brief	Pass	

Hop	From Device	Action
1	Source	View Details
2	wolf-redHorse	View Details
2	wolf-redHorse	View Details
2	wolf-redHorse	View Details
2	wolf-redHorse	View Details
2	wolf-redHorse	View Details
3	ssx-doppelboc	View Details
3	ssx-doppelboc	View Details

successful

Edit this config



Job Details

Flow State Validator

Flow State Validator details for wolf-redHorse-1

	Ethernet1/3 brief	
VPC state validator	show consistency-checker vpc source-interface port-channel1001 brief	Pass
Spanning Tree Protocol state validator	show consistency-checker stp-state vlan 2 brief	Pass

Page 1 of 3 · Objects Per Page 10 rows · Displaying Objects 1 - 10 of 25

Paths

Local Egress Logical Interface	Local Egress Physical Interface	Peer Device	Peer Serial Number	Peer VLAN	Peer Ingress Physical Interface
Vlan2	Ethernet1/18	ssx-doppelbock1	FDO2112241F	2	Ethernet1/18
Ethernet1/3	Ethernet1/3	ssx-doppelbock1	FDO2112241F	N/A	Ethernet1/3
Ethernet1/3.10	Ethernet1/3	ssx-doppelbock1	FDO2112241F	12	Ethernet1/3
port-channel11	Ethernet1/33	ssx-doppelbock1	FDO2112241F	N/A	Ethernet1/33
port-channel11	Ethernet1/63	ssx-doppelbock1	FDO2112241F	N/A	Ethernet1/63
port-channel11.12	Ethernet1/33	ssx-doppelbock1	FDO2112241F	12	Ethernet1/33
port-channel11.12	Ethernet1/63	ssx-doppelbock1	FDO2112241F	12	Ethernet1/63

Page 1 of 1 · Objects Per Page 10 rows · Displaying Objects 1 - 7 of 7

Reuse Flow State Validator to Start Another Job

Use this procedure to edit the configuration for a previous flow state validator job:

Step 1 Click the browse view icon on the left navigation pane to view the **Global Job List** page. Change the time range from the calendar on this page to view the previously configured jobs list.

Step 2 Click the job from the **Job Details** page to display the flow state validator details.

Step 3 From the bottom right corner of the page click **Edit this config** to edit the configuration details.

Step 4 Click **Run** to execute the job with new configuration.