Cisco Network Insights Advisor for Cisco DCNM User Guide, Release 2.1.x

Table of Contents

First Published: 2020-10-02

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

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 figuresincluded in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbersin illustrative content is unintentional and coincidental.

The Cisco Network Insights Advisor Application for Cisco DCNM User Guide

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 of the new features up to this release.

New Features and Changed Behavior in the Cisco Network Insights Advisor application for Cisco DCNM Release 2.1.x

Feature	Description	Release	Where Documented
Bug fixes	This release includes bug fixes.	2.1.2	Cisco Network Insights Advisor for Cisco DCNM release Notes 2.1.2
Trigger Bug Scan	On the Network Insights Setup page you can select to trigger a bug scan for all the fabrics you have selected in the Network Insights Setup page.	2.1.1	Cisco NIA Initial Setup
UI enhancements	Browse dashboards for Advisories, Bugs, PSIRTs, and Notices summarize additional details of the device, generates detailed view reports, and displays the anomaly score for the devices affected.	2.1.1	Browse Advisories, Issues Dashboard, Browse Devices
TAC Assist enhancements	Cisco NIA app uses the device connectivity issue notifier on Cisco DCNM to communicate with the devices, which identifies the unhealthy node interactions on the device. TAC assist does not collect logs for these nodes.	2.1.1	TAC Assist Dashboard

Feature	Description	Release	Where Documented
Flow State Validator enhancements	The topology view displays all the devices that are traversed to reach the destination. It displays all available paths to the destination. It performs consistency check on each of the devices and displays the aggregated overlay and underlay information.	2.1.1	View Flow State Validator
Pre Bug Scan PSIRTs	PSIRTs for the devices discovered by Cisco NIA are now shown without having to run a bug scan. If metadata is updated from cloud, a bug scan should be run to show updated PSIRTs that are applicable to the devices.	2.1.1	PSIRTs Dashboard
Device Connectivity Warning	Cisco NIA app cannot communicate with the device through SIM when the device is not configured properly. When you try to run an on-demand Bug Scan, TAC Assist, or Compliance job, the device connectivity warning is shown next to such a device which has an issue.	2.1.1	Device Connectivity Warning

Cisco Network Insights Advisor Installation

About Cisco Network Insights Advisor

Cisco Network Insights Advisor (Cisco NIA) application monitors utilities that can be added to the Cisco Data Center Network Manager (Cisco DCNM).

Downloading Cisco Network Insights Advisor from the Cisco App Center

This section contains the steps required to download Cisco Network Insights Advisor applications in the Cisco DCNM in preparation for installation.

Before you begin

You must have administrative credentials to download Cisco NIA application in Cisco DCNM.

Procedure

1. Access the Cisco DC App Center site in one of the two ways:
   - Go to Cisco DC App Center, or
   - If you have admin privileges, go through the Cisco DCNM GUI.
     a. Login to the Cisco DCNM GUI as admin.
     b. Choose **Apps**.
     c. Click the **Download Applications** icon ⭳ on the far-right side of the work pane. A new browser tab or window opens to the Cisco DC App Center.
2. Search for Cisco Network Insights Advisor application on the search bar.
3. Select the Cisco Network Insights Advisor application you want to download and click **Download** for that app to begin the process of downloading the app to your local machine.
4. Review the license agreement and, if OK, click **Agree and download**.

   The Cisco Network Insights Advisor application is downloaded to your local machine.

5. Make a note of the download location of the Cisco Network Insights Advisor file on your local machine.
6. Make sure the downloaded file can be accessed by the Cisco DCNM. If it cannot, move the file to a device and/or location where it can be installed on the Cisco DCNM.

Installing Cisco Network Insights Advisor in Cisco DCNM

This section contains the steps required to install Cisco Network Insights Advisor applications in the

Cisco DCNM.

Before you begin

Before you begin installing a Cisco NIA application, make sure the following requirements are met:

1. You must have administrator credentials to install Cisco Network Insights Advisor applications.
2. You must have three compute servers installed and in the “Joined” state. For more information regarding the installation, discovery, and addition of compute servers, refer to the following sections:
    - Compute Installation: For details on compute installation, refer to the Installing a DCNM Compute section.
    - DVS Security Settings: For details on DVS security settings, refer to the Networking Policies for OVA Installation section. If this setting is not configured correctly, devices will not be accessible from Cisco Network Insights Advisor resulting in incomplete Jobs. A warning icon is displayed for the device in the user interface.
    - Subnet Requirements for OOB and IB pool: For details on subnet requirements for OOB and IB pool, refer to the Subnet Requirements section. If the OOB and IP pool subnet are not configured correctly, devices will not be accessible from Cisco Network Insights Advisor resulting in incomplete Jobs. A warning icon is displayed for the device in the user interface.
    - Creating a Compute Cluster: For details on creating a compute cluster, refer to the Enabling the Compute Cluster section.
    - Adding Computers in Web UI: For details on adding computers in web UI, refer to the Adding Computers into the Cluster Mode section.
3. You must stop and uninstall any Cisco NIA 1.0.x app prior to installing Cisco NIA 2.x app.
4. When the installation is complete, the application opens to a Welcome dialog where initial setup is performed. Continue with the setup of the Cisco NIA application located in the Initial Setup section of the next chapter.

Enabling Cisco Network Insights Advisor in Cisco DCNM

This section contains the steps required to enable or disable the Cisco NIA application.

Before you begin

Before you begin enable or disable the Cisco NIA application, make sure the following prerequisites are met:

- You must have administrator privileges for Cisco DCNM GUI.
- You have installed Cisco NIA app and the application has launched correctly.

Procedure

1. Login to Cisco DCNM GUI with admin privileges.
2. Click **Application** on the left navigation bar.
3. Click **Open** from the Cisco NIA application dialog.

   The Cisco Network Insights Advisor application dialog appears.

4. Check the **Help Cisco improve its products** option.

   Uncheck this option to stop sending environment specific data to Cisco Intersight.

Cisco Network Insights Advisor Setup and Settings

About Cisco Network Insights Advisor on Cisco DCNM

The Cisco Network Insights Advisor (Cisco NIA) application monitors a data center network and pinpoints issues that can be addressed to maintain availability and reduce surprise outages. Cisco NIA's understanding of your network allows it to provide proactive advice with a focus on maintaining availability and alerting customers about potential issues that can impact up-time.

The Cisco NIA app collects the CPU, device name, device pid, serial number, version, memory, device type, and disk usage information for the nodes in the fabric.

The Cisco NIA app provides TAC Assist functionalities which are useful when working with Cisco TAC. It provides a way for Cisco Customers to collect tech support across multiple devices and upload those tech supports to Cisco Intersight Cloud. These tech support are accessible to our TAC teams when helping customers through a resolution of a Service Request. Additionally, it enables capability for our TAC teams to collect tech support on demand for a particular device.

Cisco NIA app consists of the following components:

- Advisories
    - Software Upgrades
    - Cisco Recommendations
- Notices
    - EoL/EoS Dates
    - Field Notices
- Issues
    - Bug/PSIRT Reports
- Devices
- TAC Assist
    - Log Collection
    - Technical Support to Cloud
    - Enhanced TAC Assist
- Jobs

  - Fabric
  - Global (Flow State Validator)

> In this chapter, a "network" refers to a fabric in a LAN fabric and a switch group in a Classic LAN.

Guidelines and Limitations

- IPv6 is not supported for Cisco Network Insights Advisor application in the Cisco DCNM.
- The Cisco Network Insights Advisor application requires that physical servers hosting Cisco DCNM computes as VMs are atleast Cisco C220-M4 category. It is also required that a compute be hosted on a data store with a dedicated hard disk of atleast 500GB.
- After metadata update you need to run manual bug scan to reflect PSIRTs.
- Cisco Network Insights Advisor does not support multiple site domain fabric type.
- Cisco Network Insights Advisor does not support nodes with IPv6 management address on Cisco DCNM.
- For remote authentication of Cisco Network Insights Advisor on AAA or TACAS or LDAP:
  - You must have `admin` credentials.
  - The LAN credentials must be properly set.
- When the Device Connector is unclaimed from the on-premise GUI Cisco NIA application, the Device Connector must be unclaimed from Intersight for TAC Assist’s connected TAC functionality to work.
- TAC Assist started from Cisco NIA app will not show up in Cisco NI Base and vice versa.
- Cisco DCNM allows `network-admin` and `network-operator` roles to assign read or write access for specific fabrics. Cisco Network Insights Advisor app displays only those fabrics that are granted permission.
- Cisco NIA app does not allow RBAC role on Cisco DCNM.

Cisco NIA Initial Setup

This section contains the steps required to set up Cisco NIA app in the Cisco DCNM. This set up is required for Cisco NIA app to show important information and gather relevant data.

1. Once Cisco NIA app is installed and after your first log in, a welcome dialog appears. Click **Begin Setup**.

   The Cisco NIA app is enabled with Cisco DCNM.

2. The **Network Insights Setup** page appears with the selected fabrics in Configuration. Click **Edit configuration** to choose the site(s). You can return to the setup utility anytime by clicking the settings icon ⚙ and choose **Network Insights Setup**.

   The list consists of the sites that were discovered during the Cisco NIA application installation.

   a. Check only the sites you want visible to the Cisco NIA application.

   b. Click **Ok**.

3. Check the box to **Trigger Bug Scan**. Once this option is enabled in the first time setup, it does not appear in the rerun setup.

4. Check the box to **Help Cisco improve it's products**.

   Uncheck the box to stop sending the CX telemetry data to Cisco Intersight Cloud.

5. Click **Done**.

Cisco NIA Settings

Settings

Displayed across the top of the work pane is a group of icons and a list menu comprising the Cisco NIA app settings. The following table describes each:

Property	Description
Fabric	Choose a fabric containing the devices you want visible to the Cisco NIA application.
☁	**Device Connector Status**: Identifies the current connection status of the Cisco NIA application to the Cisco Intersight Cloud and the device connector claim condition. Possible connection statuses are: • **Not Connected**: The Cisco NIA application is not connected to the Cisco Intersight Cloud. • **Connected / Not Claimed**: The Cisco NIA application is connected to the Cisco Intersight Cloud but the device connector has not been claimed by the customer. Cisco NIA app collects telemetry data. • **Connected / Claimed**: The Cisco NIA application is connected to the Cisco Intersight Cloud and the device connector has been claimed by the customer. Cisco NIA uses TAC assist and metadata refresh in connected and claimed. For more information, see Configuring the Intersight Device Connector.
✉	**Inbox**: View messages from Cisco regarding software upgrades or other relevant information about devices on your network. NOTE: This is a preview feature.

Property	Description
⚙	Clicking on this icon invokes a list menu allowing you to make changes to the following: • **About Network Insights**—Displays an information dialog identifying the version number of the Cisco NIA application. Click **Update to Latest** to fetch the latest metadata published version. This requires that the using of the Cisco Intersight Device Connecter is connected and claimed. See Configuring the Intersight Device Connector for details. • **Network Insights Setup**—Allows you to edit the Network Insights Setup configurations by adding or removing the fabrics.
?	**User Guide**—The documentation for installation, configuration, and use of Cisco NIA application.

Setting Up the Device Connector

About Device Connector

Devices are connected to the Intersight portal through a Device Connector that is embedded in the management controller of each system. Device Connector provides a secure way for the connected devices to send information and receive control instructions from the Cisco Intersight portal, using a secure Internet connection.

When an Intersight-enabled device or application starts, the Device Connector starts at boot by default, and attempts to connect to the cloud service. If the **Auto Update** option is enabled, the Device Connector is automatically updated to the latest version through a refresh by the Intersight service when you connect to Intersight. Auto Update is enabled by default for Cisco DCNM. For more information on the **Auto Update** option, see Configuring the Intersight Device Connector.

Configuring the Intersight Device Connector

Cisco NIA application is connected to the Cisco Intersight cloud portal through a Device Connector which is embedded in the management controller of the Cisco DCNM platform.

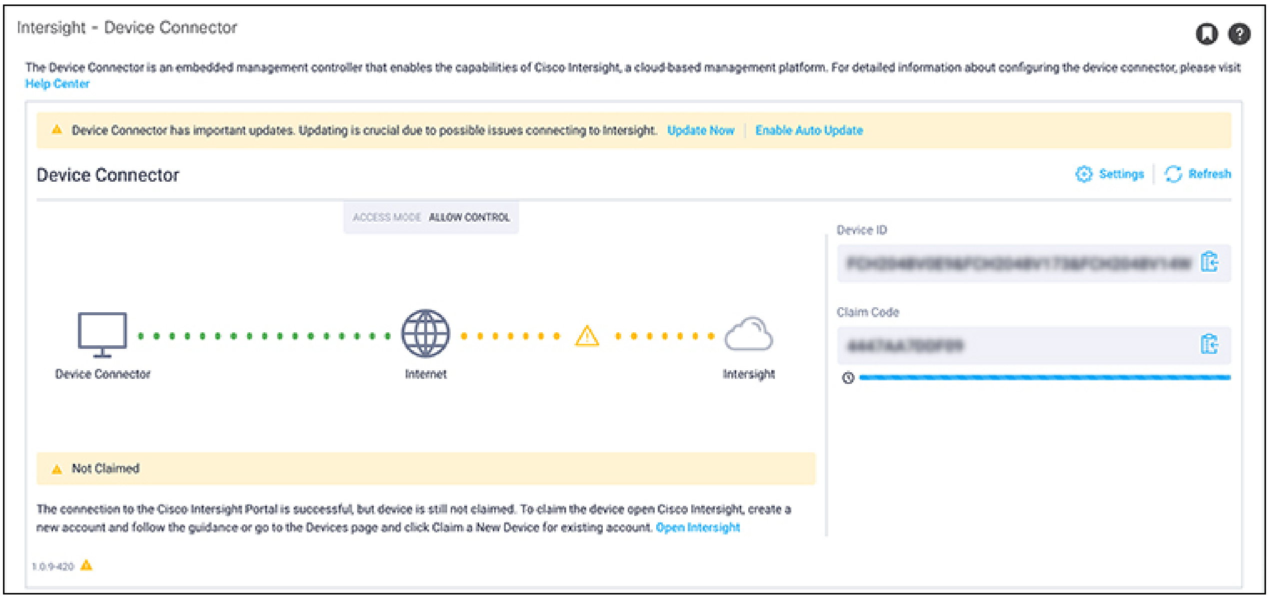
Cisco Intersight is a management platform delivered as a service. Cisco DCNM platform has a Device Connector that is packaged with the software that connects to Cisco Intersight Cloud. Device Connector is used to provide Cisco NIA Cloud connectivity feature sets.

The Device Connector provides a secure way for connected Cisco DCNM to send and receive information from the Cisco Intersight portal, using a secure Internet connection.

To setup the Device Connector, follow these steps:

1. On the Cisco DCNM navigation pane, click Administration.
2. Under the Cisco DCNM Server list, click Device Connector.

   The Device Connector work pane appears:



Intersight - Device Connector

The Device Connector is an embedded management controller that enables the capabilities of Cisco Intersight, a cloud-based management platform. For detailed information about configuring the device connector, please visit Help Center

⚠ Device Connector has important updates. Updating is crucial due to possible issues connecting to Intersight. Update Now | Enable Auto Update

Device Connector

Device ID

[redacted]

Claim Code

[redacted]

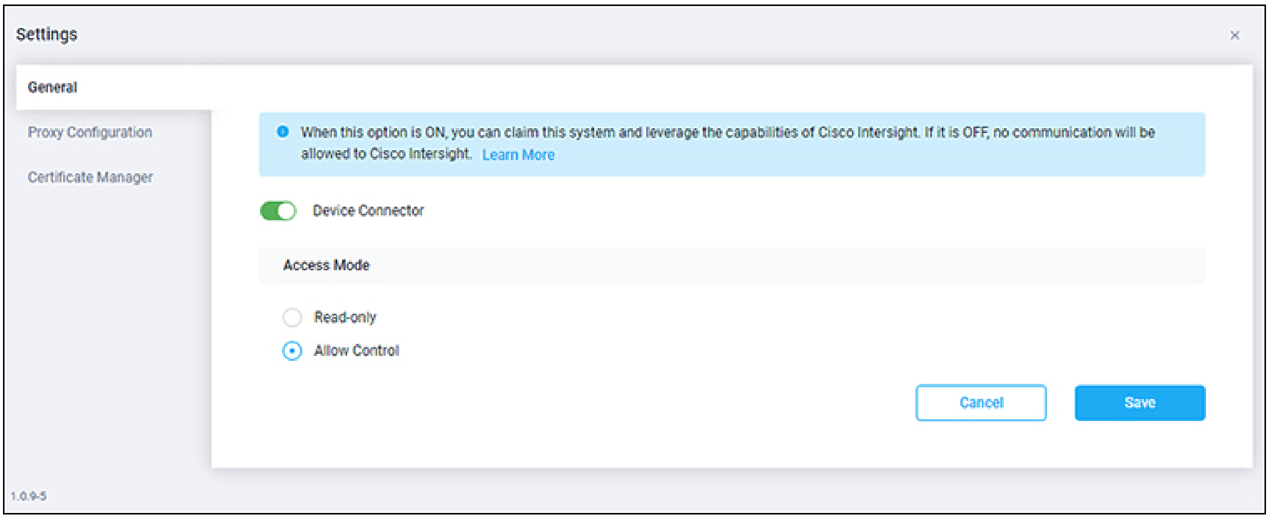
⚠ Not Claimed

The connection to the Cisco Intersight Portal is successful, but device is still not claimed. To claim the device open Cisco Intersight, create a new account and follow the guidance or go to the Devices page and click Claim a New Device for existing account. Open Intersight

1.0.9-420 ⚠

3. At the far right of the screen, click **Settings**.

The *Settings - General* dialog appears:



Settings

When this option is ON, you can claim this system and leverage the capabilities of Cisco Intersight. If it is OFF, no communication will be allowed to Cisco Intersight. Learn More

Device Connector: ON

Access Mode

○ Read-only

● Allow Control

The DC version for Cisco DCNM is 1.0.9-286.

Device Connector (switch)

This is the main switch for the Device Connector communication with Cisco Intersight. When the switch is on (*green highlight*), the system is claimed and the capabilities of the Cisco Intersight can be leveraged. If the switch is off (*gray highlight*), no communication can occur between the platform and Cisco Intersight.

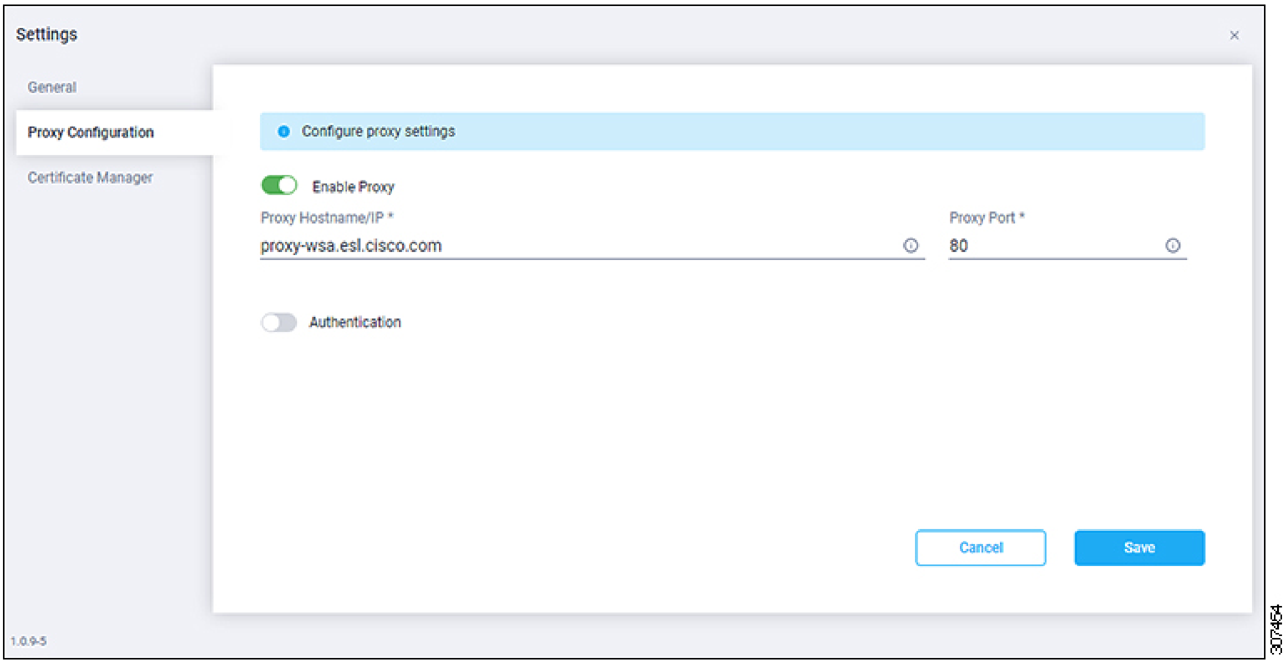
Access Mode

Read-only: This option ensures that no changes are made to this device from Intersight. For example, actions such as upgrading firmware or a profile deployment will not be allowed in the Read-Only mode. However, the actions depend on the features available for a particular system.

Allow Control: This option (selected by default) enables you to perform full read/write operations from the appliance, based on the features available in Cisco Intersight. This function is not used for changes from Cisco Cloud to customer network.

4. Set the Device Connector to on (green highlight) and choose **Allow Control**.
5. Click **Proxy Configuration**.

   The *Settings - Proxy Configuration* dialog appears.



Enable Proxy: on

Proxy Hostname/IP *: proxy-wsa.esl.cisco.com

Proxy Port *: 80

Authentication: off

Enable Proxy(switch)

Enable HTTPS Proxy to configure the proxy settings.

Proxy Hostname/IP * and **Proxy Port** *: Enter a proxy hostname or IP address, and a proxy port number.

Authentication(switch)

Enable proxy access through authentication. When the switch is on (green highlight), authentication to the proxy server is required. If the switch is off (gray highlight), no authentication is required.

Username* and **Password**: Enter a user name and password for authentication.

*Proxy settings are required for Network Insights.

6. Enable the proxy (green highlight) and enter a hostname and port number.
7. Optional: If proxy authentication is required, enable it (green highlight) and enter a username and password.
8. Click **Save**.

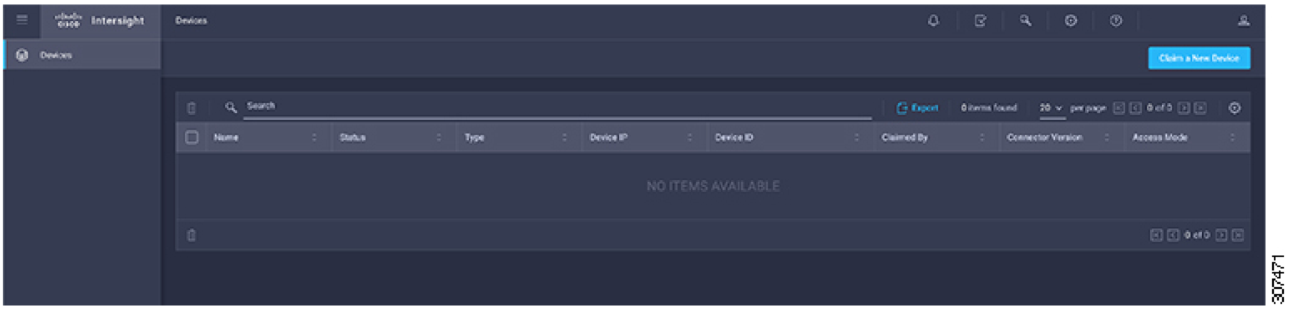
Claiming a Device

Before you begin

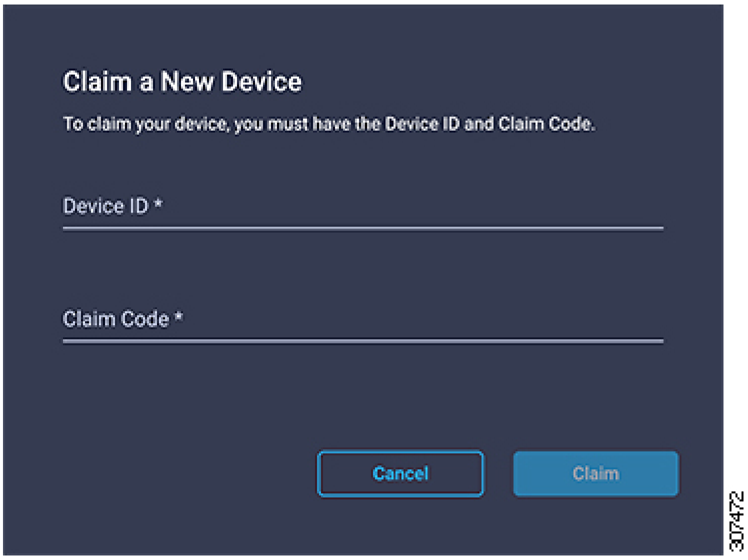
Configure the Intersight Device Connector information from the Cisco DCNM site using the instructions provided in Configuring the Intersight Device Connector.

Procedure

1. Log into the Cisco Intersight cloud site: https://www.intersight.com
2. In the Cisco Intersight cloud site, under the **Devices** tab, click **Claim a New Device**.



The *Claim a New Device* page appears.



Claim a New Device

To claim your device, you must have the Device ID and Claim Code.

3. Go back to the Cisco DCNM site and navigate back to the *Intersight - Device Connector* page.
   a. On the menu bar, choose **System** > **System Settings**
   b. In the **Navigation** pane, click **Intersight**.
4. Copy the **Device ID** and **Claim Code** from the Cisco DCNM site and paste them into the proper fields in the *Claim a New Device* page in the Intersight cloud site.

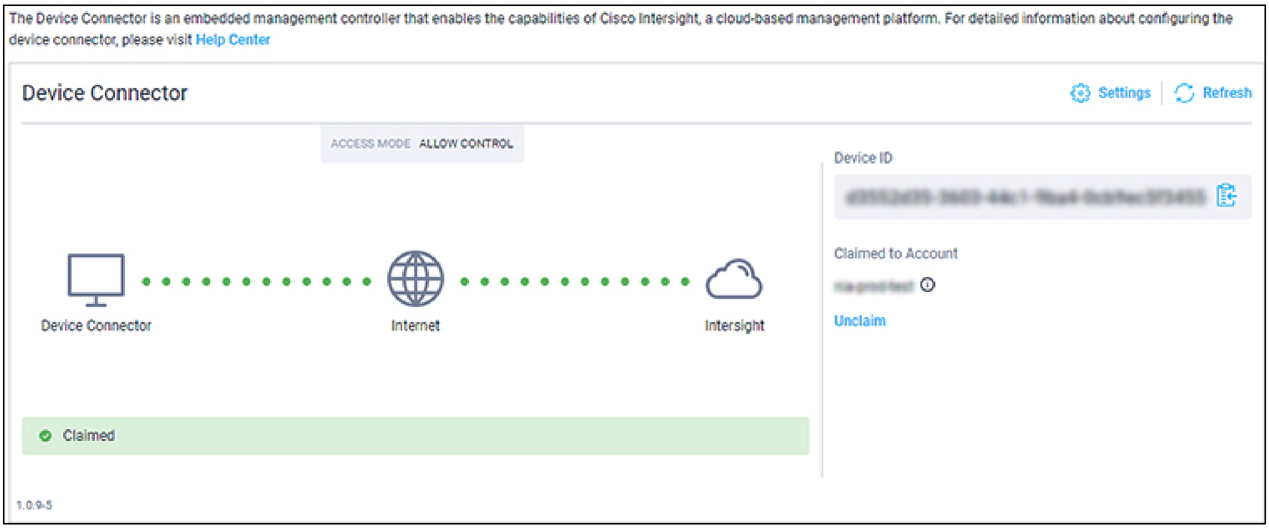
   Click on the clipboard next to the fields in the Cisco DCNM site to copy the field information into the clipboard.

5. In the *Claim a New Device* page in the Intersight cloud site, click **Claim**.

   You should see the message "Your device has been successfully claimed" in the *Claim a New Device* page. Also, in the main page, you should see your Cisco DCNM system, with **Connected** shown in the Status column.

6. Go back to the *Intersight - Device Connector* page in the Cisco DCNM GUI and verify that the system was claimed successfully.

   You should see green dotted lines connecting **Internet** to **Intersight** in the **Device Connector** graphic, and the text **Claimed** underneath the graphic.



The Device Connector is an embedded management controller that enables the capabilities of Cisco Intersight, a cloud-based management platform. For detailed information about configuring the device connector, please visit Help Center

Device Connector

ACCESS MODE ALLOW CONTROL

Device ID

[redacted]

Claimed to Account

[redacted]

Unclaim

Claimed

1.0.9-5

> You may have to click **Refresh** in the *Intersight - Device Connector* page to update the information in the page to the current state.

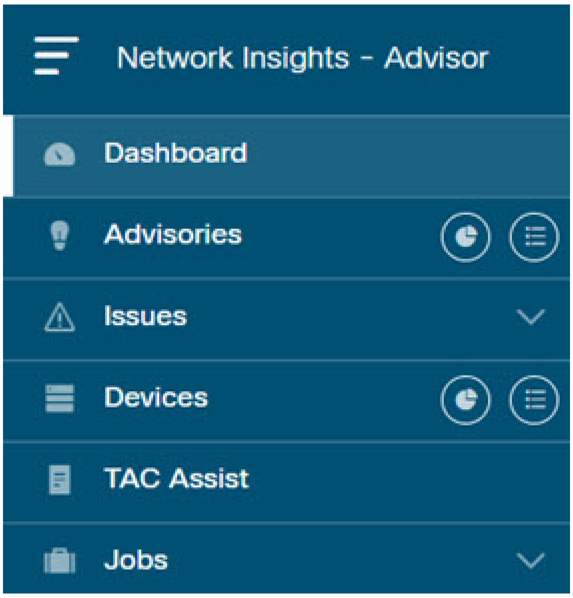
If you decide to unclaim this device for some reason, locate the **Unclaim** link in the *Intersight - Device Connector* page and click that link.

Navigating Cisco NIA

The Cisco NIA application window is divided into two parts: the Navigation pane and the Work pane.

Navigation Pane

The Cisco NIA app navigation pane divides the collected data into seven categories:



Dashboard: The main dashboard for the Cisco NIA application providing immediate access to total advisories, issues, notices, and collected TAC assist logs.

Advisories: Displays hardware, software, and hardening check advisories applicable to your network.

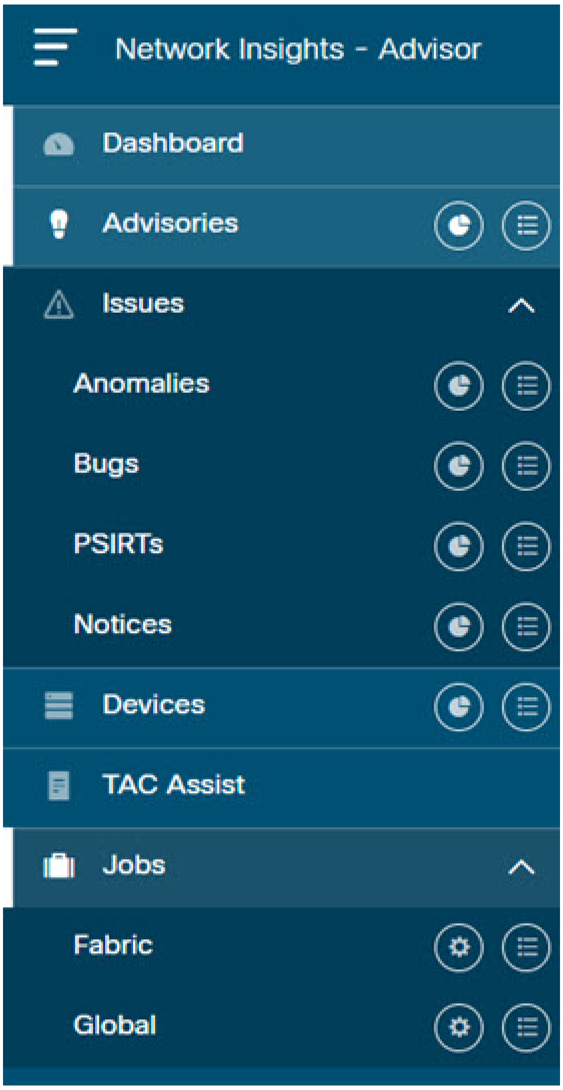
Issues: Displays anomalies, bugs, Product Security Incident Response Team (PSIRT) alerts, and notices.

Devices: Sorts devices by issue, platform/version, or maintenance score.

TAC Assist: Collects logs for specified devices that can be attached to service requests.

Jobs: Provides access to configure and schedule bug scan and compliance check jobs that run for a specific fabric.

Additional functions are :



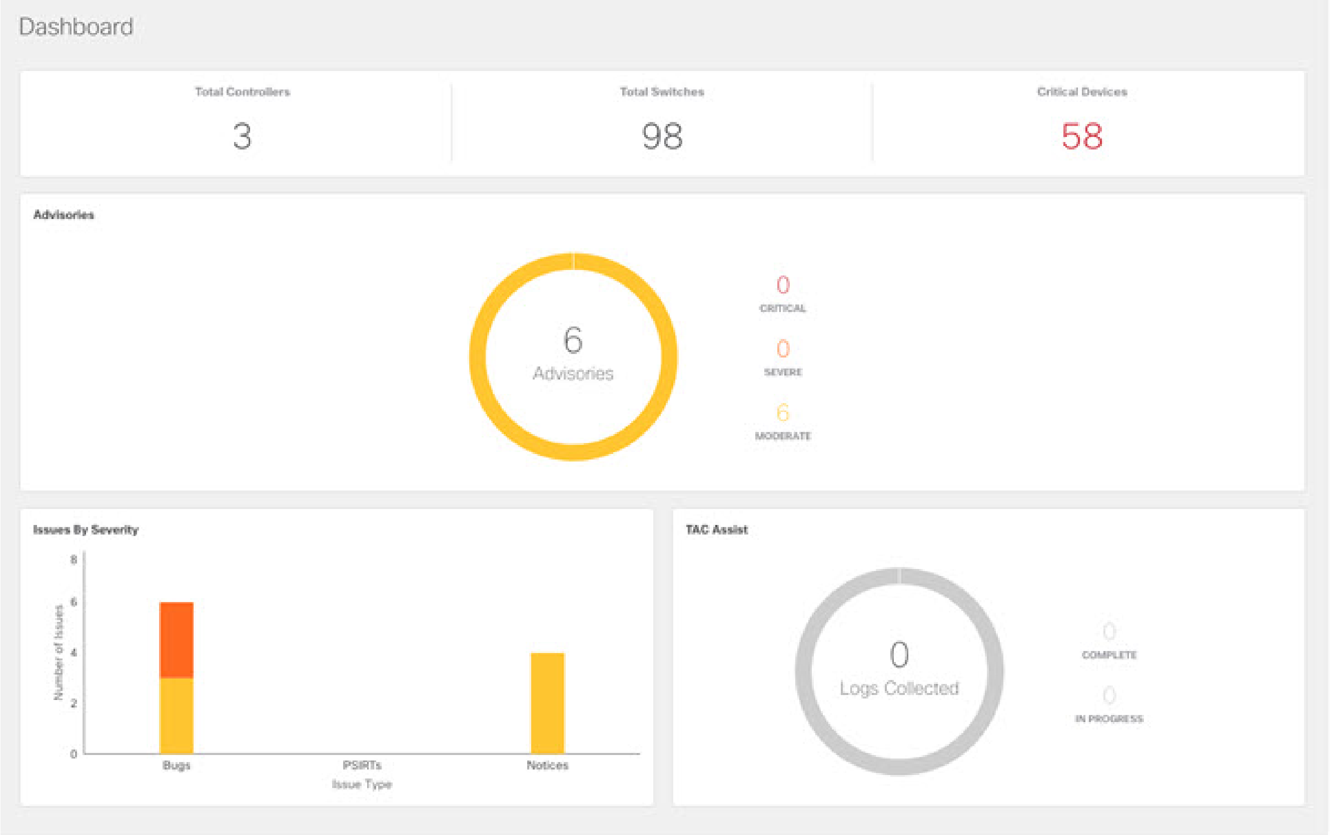
Dashboard View icon: Provides immediate access to top usage or issues for the selected information type.

Browse View icon: Provides a detailed view of the information and access to more granular detail.

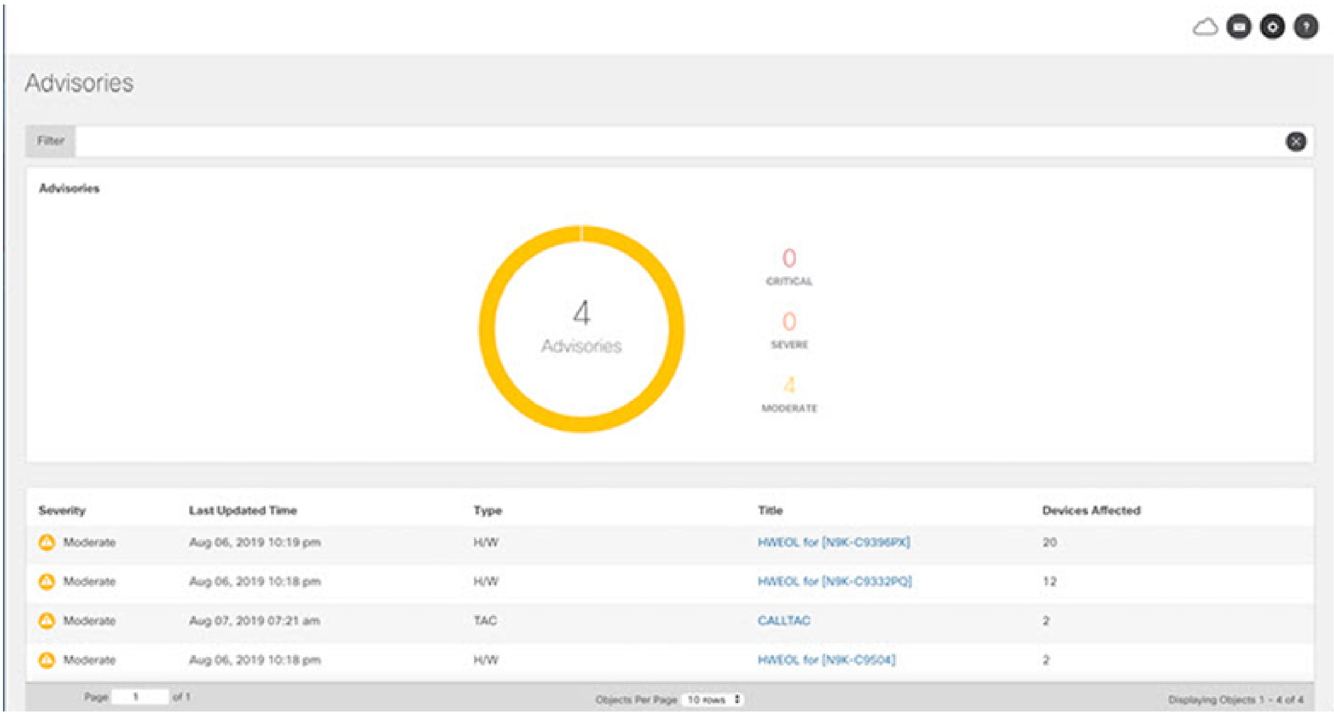
Work Pane

The work pane is the main viewing location in the Cisco NIA application. All information tiles, graphs, charts, and lists appear in the work pane.

Dashboard Work Pane



In an information tile, you can usually click on a numeric value to switch to the Browse work pane:



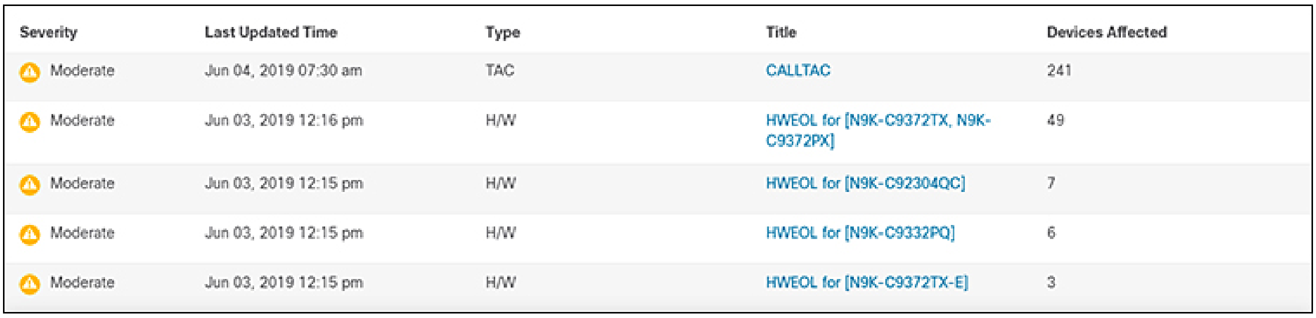
Severity	Last Updated Time	Type	Title	Devices Affected
Moderate	Aug 06, 2019 10:19 pm	H/W	HWEOL for [N9K-C9396PX]	20
Moderate	Aug 06, 2019 10:18 pm	H/W	HWEOL for [N9K-C9332PQ]	12
Moderate	Aug 07, 2019 07:21 am	TAC	CALLTAC	2
Moderate	Aug 06, 2019 10:18 pm	H/W	HWEOL for [N9K-C9504]	2

Launches the Browse work pane with all of the items displayed from the graph in the information tile.

Launches the Browse work pane with only the selected items displayed from the number in the information tile.

Browse Work Pane

The Browse work pane isolates the data for the parameter chosen on the Dashboard. The Browse work pane displays a top node lists, graphs over time, and lists all the nodes in an order defined by the anomaly score:



Severity	Last Updated Time	Type	Title	Devices Affected
⚠ Moderate	Jun 04, 2019 07:30 am	TAC	CALLTAC	241
⚠ Moderate	Jun 03, 2019 12:16 pm	H/W	HWEOL for [N9K-C9372TX, N9K-C9372PX]	49
⚠ Moderate	Jun 03, 2019 12:15 pm	H/W	HWEOL for [N9K-C92304QC]	7
⚠ Moderate	Jun 03, 2019 12:15 pm	H/W	HWEOL for [N9K-C9332PQ]	6
⚠ Moderate	Jun 03, 2019 12:15 pm	H/W	HWEOL for [N9K-C9372TX-E]	3

307411

Clicking on one of the nodes in the list opens the Details work pane for that selection.

Details Work Pane

The Details work pane provides resource details about the item selected in the event list on the Browse work pane. The Details work pane consists of:

- General Information: Includes information about the selected object. This varies based on which browse window the details work pane was initiated.
- Issues: Includes issues affecting devices in your network.
- Devices Affected: Displays the number of affected devices in your network.

Devices

The Devices page displays the devices by device name, serial number, IP address, version, and platform.

TAC Assist

The TAC Assist work pane lets you collect logs for specified devices that can be attached to service requests using the Cisco Intersight Cloud. It lets you check the device(s) for which you can collect logs to assist TAC.

The **Log Collection** section displays the new job triggered for TAC Assist. The **Job Details** page lists the TAC Assist logs.

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.

Jobs

The configuration icon from the **Jobs** > **Fabric** lets you configure a scheduled bug scan and compliance check for the selected fabric.

The browse icon from the **Jobs** > **Fabric** lets you view the scheduled jobs for the selected fabric and time range from the *Fabric Job List* page.

The configuration icon from the **Jobs** > **Global** lets you configure and schedule Flow State Validator jobs that run across the network. The Flow State Validator gathers information about flow related issues.

Cisco Network Insights Advisor Dashboard

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.
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. Cisco 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.
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. ℹ **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

Click an advisory from the summary pane to display the **Anomaly Detail** page.

Click the **Issue**, **Bug**, or **PSIRT** for the side panel to display additional details.

The **Devices Affected** section summarizes the devices with the anomalies. Click the **Device Name** to display the side summary panel for quick view of the summary with general information about the device and additional advisory and anomaly details.

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.

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.

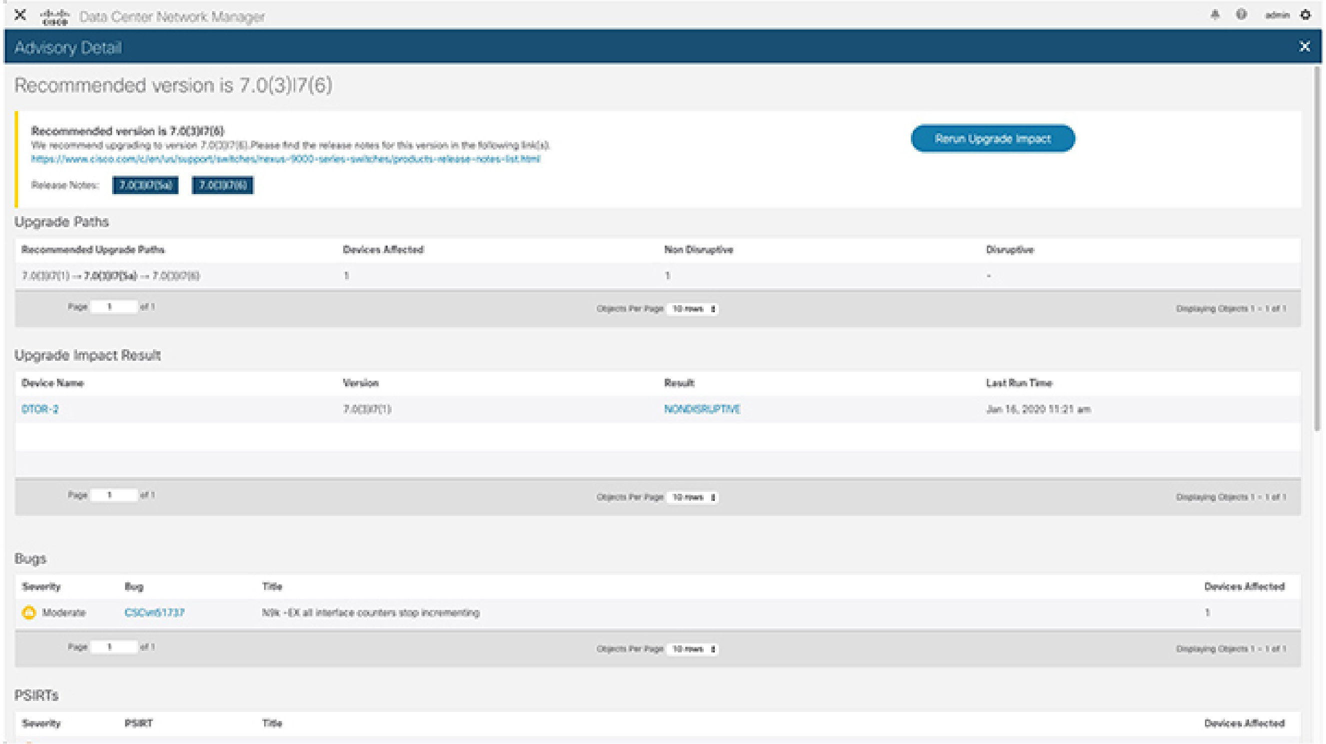
4. Click **Upgrade Impact** and then click **Run Upgrade Impact** on the *Confirm Action* dialog.

   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.


Data Center Network Manager
admin
Advisory Detail
Rerun Upgrade Impact
Release Notes: 7.0(3)I7(5a) 7.0(3)I7(6)

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

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

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
- Notices - Field notices such as end-of-life notices for switch hardware and software

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.

Property	Description
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.

Property	Description
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 severities 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.

Click a row from the bug summary pane to display the **Bug Detail** page.

Click **View Advisory** for additional details about the bug.

The **Devices Affected** section summarizes the devices with the anomalies. Click the **Device Name** to display the side summary panel for quick view of the summary with general information about the device and additional advisory and anomaly details.

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.
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.

Property	Description
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 severities 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.

Click a row from the PSIRTs summary pane to display the **PSIRTs Detail** page.

Click **View Advisory** for additional details about the PSIRT.

The **Devices Affected** section summarizes the devices with the anomalies. Click the **Device Name** to display the side summary panel for quick view of the summary with general information about the device and additional advisory and anomaly details.

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.

Property	Description
Moderate Notices	Displays the number of moderate notices that are applicable to devices in your network.
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 severities 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 notices 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.

Click a row from the Notices summary pane to display the **Notices Detail** page.

Click **View Advisory** for additional details about the notice.

The **Devices Affected** section summarizes the devices with the anomalies. Click the **Device Name** to display the side summary panel for quick view of the summary with general information about the device and additional advisory and anomaly details.

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 Versions, Platforms	Displays the different versions of software and types of hardware detected per platform.
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 about the advisories and issues.

Browse Devices

On the **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

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

You can view, sort, and filter devices through the Browse Devices work pane.

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. The list summarizes device name, serial number, IP address, version, CRV, platform. Click a name in the **Device Name** field to display the details for that device. The device with connectivity issue has a warning icon next in the **Device Name**. Hover over the icon for additional connectivity details. The **CRV** column displays the recommended version for the device.

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.

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 Cisco Intersight Cloud.

The Connected TAC Assist has two modes:

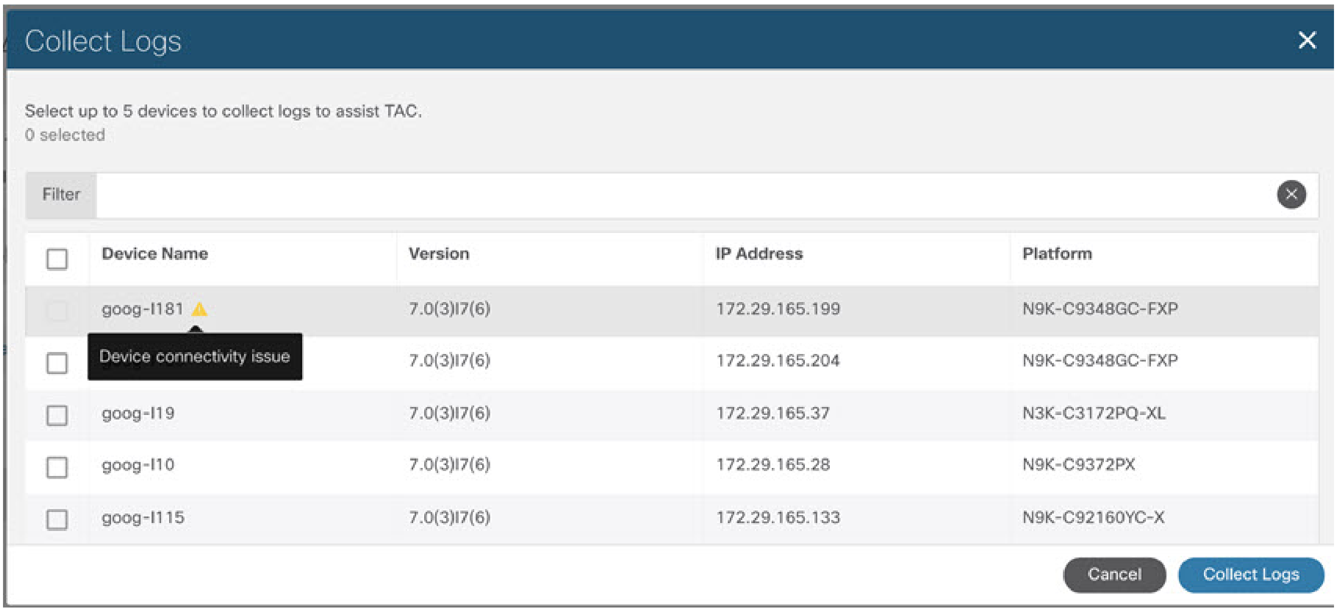
- User initiated - The user collects the logs for specified devices and then the user uploads the collected logs to Cisco Intersight Cloud.
- TAC initiated - Cisco TAC triggered on-demand collection of logs for specified devices and pulls the logs from Cisco Intersight Cloud.

Device Connectivity Warning

Cisco NIA app uses the Cisco DCNM Switch Interaction Manager (SIM) to communicate with the devices present in the network. In case the fabric / switch is not configured properly, Cisco NIA cannot communicate with the device through SIM.

When you try to run an on-demand Bug Scan, TAC Assist, or Compliance job, the device connectivity warning is shown next to such a device which has an issue. Also, such problematic devices are not selectable since Cisco NIA cannot connect to them.

This warning is also displayed on the Devices Browse page if a user wants to know which switches are not reachable by Cisco NIA.



Select up to 5 devices to collect logs to assist TAC.
0 selected

	Device Name	Version	IP Address	Platform
□	goog-I181 ⚠	7.0(3)I7(6)	172.29.165.199	N9K-C9348GC-FXP
□	Device connectivity issue	7.0(3)I7(6)	172.29.165.204	N9K-C9348GC-FXP
□	goog-I19	7.0(3)I7(6)	172.29.165.37	N3K-C3172PQ-XL
□	goog-I10	7.0(3)I7(6)	172.29.165.28	N9K-C9372PX
□	goog-I115	7.0(3)I7(6)	172.29.165.133	N9K-C92160YC-X

User Initiated Upload to Cisco Intersight Cloud

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

Before you begin

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

Procedure

1. Click **TAC Assist** in the Cisco DCNM navigation pane.
2. Click **Begin** to initiate the log collection process.

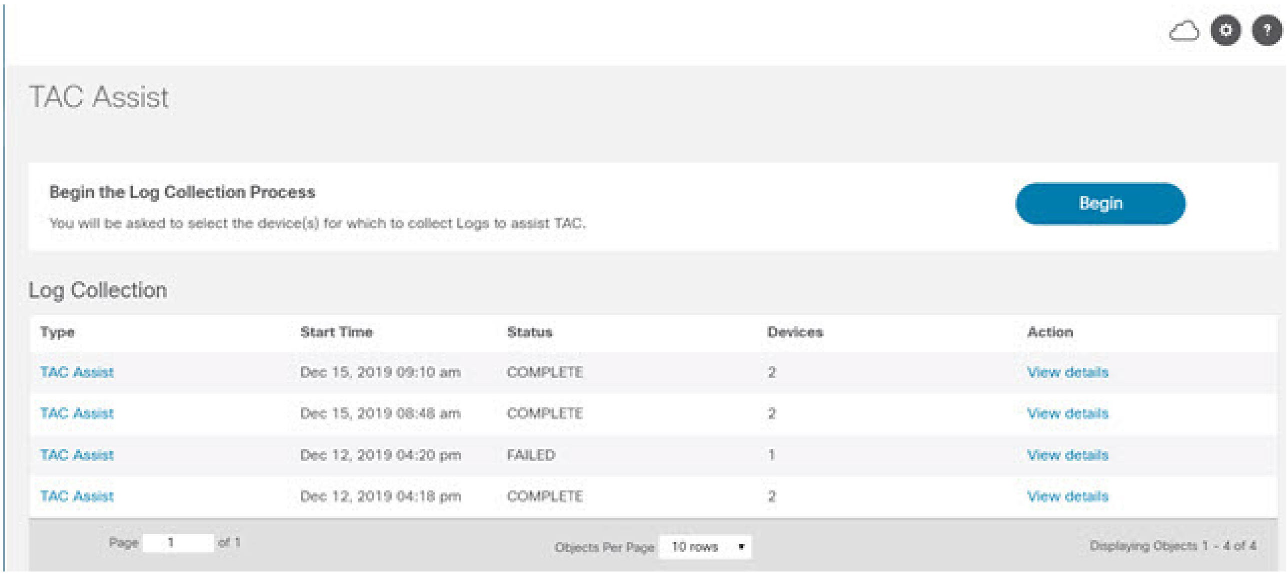
   The Collect Logs dialog appears.

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.

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 initiated 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.

Begin

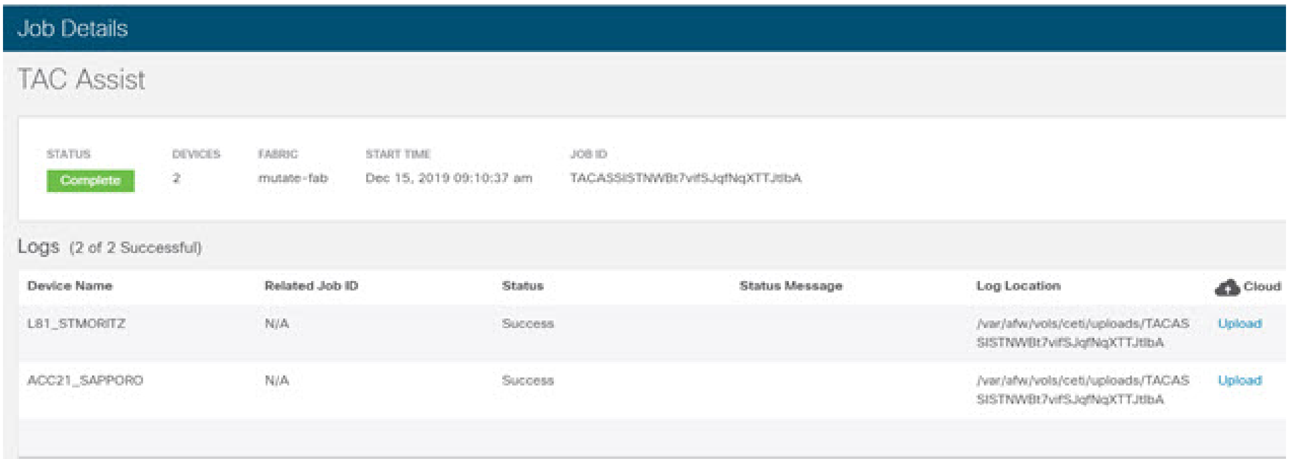
Log Collection

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

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 Cisco Intersight 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

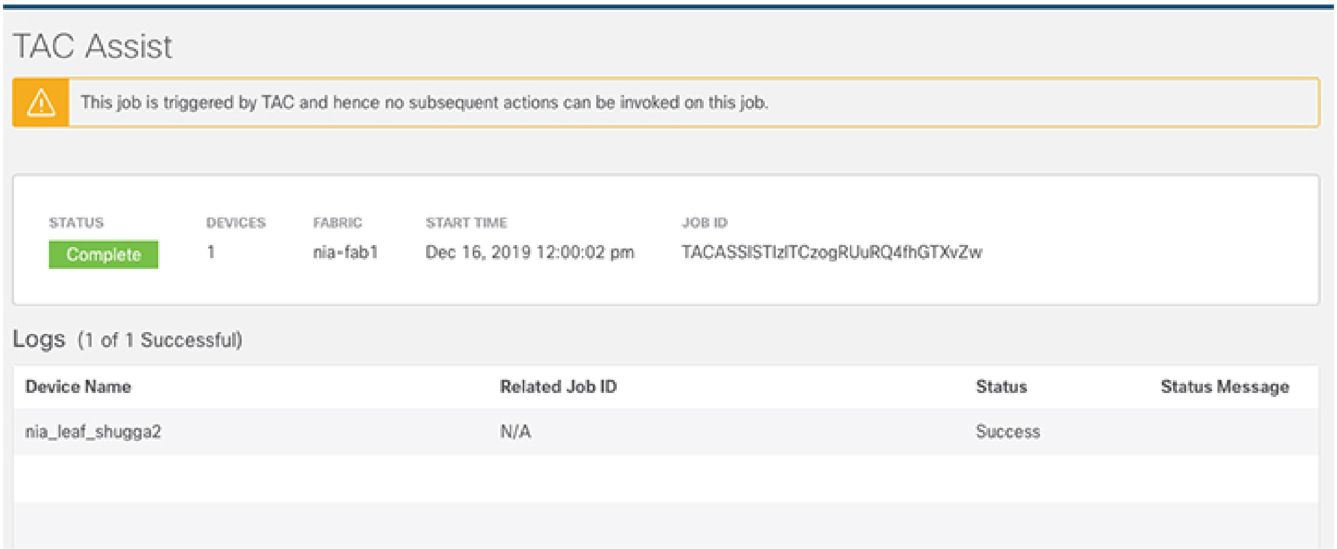
6. Click **Upload** to upload the collected logs to Cisco Intersight Cloud.

   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.

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.

In case the fabric is not configured properly to communicate with the device, Cisco NIA app notifies the following:

- The device is not configured for node interaction.
- You can not run on-demand bug scan job on the device.
- Cisco NIA app can’t connect to the device.

If the node interaction is not healthy on the device, you can’t select the device for bug scan to collect logs. The device can not be selected to configure a job.

Configure Bug Scan

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

   The Fabric Job Configuration page appears.

2. Click **Configure** to schedule a on-demand bug scan 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.

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 and view anomaly details.

Configure Compliance Check

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

   The Fabric Job Configuration page appears.

2. Click **Configure** to schedule a on-demand 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.

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** > ⚙ on the left navigation pane to schedule a global job that gathers information about your network across all fabrics.

Start Flow State Validator

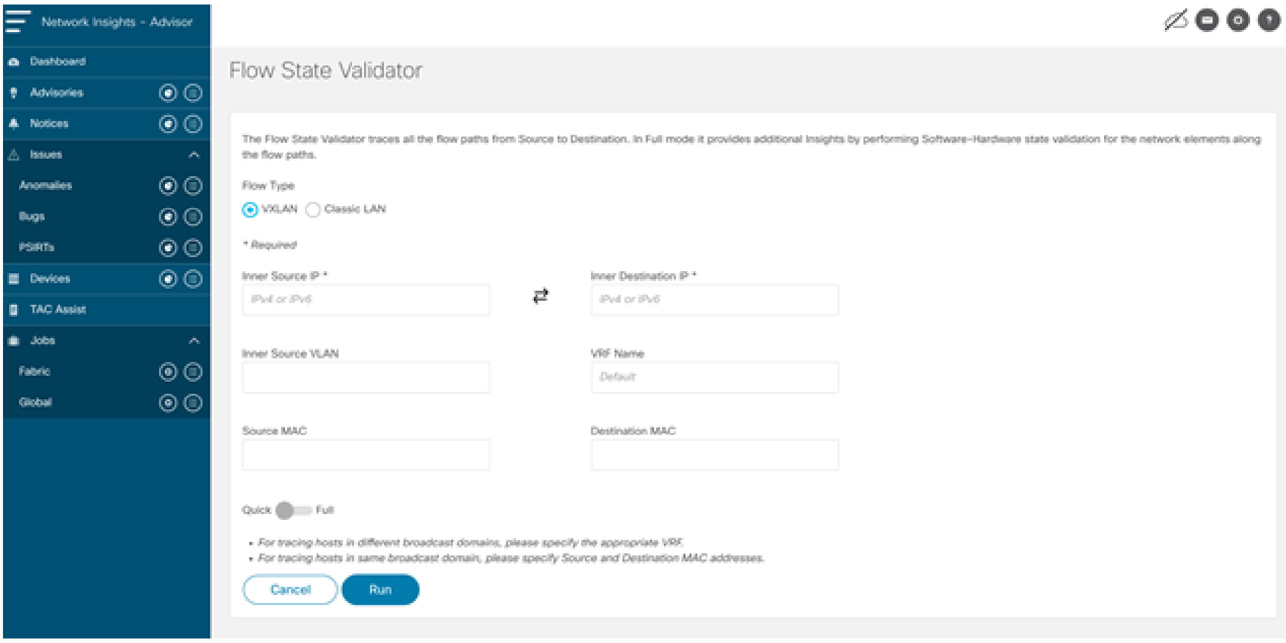
Use this procedure to schedule a flow state validator job for all the devices compatible with flow state validator.

1. Choose **Jobs** > **Global** from the left navigation pane.
2. On the Global Job Configuration page click **Configure**.
3. Choose **VXLAN** or **Classic LAN** installation mode.
4. Enter the required fields and optional 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.

5. 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.

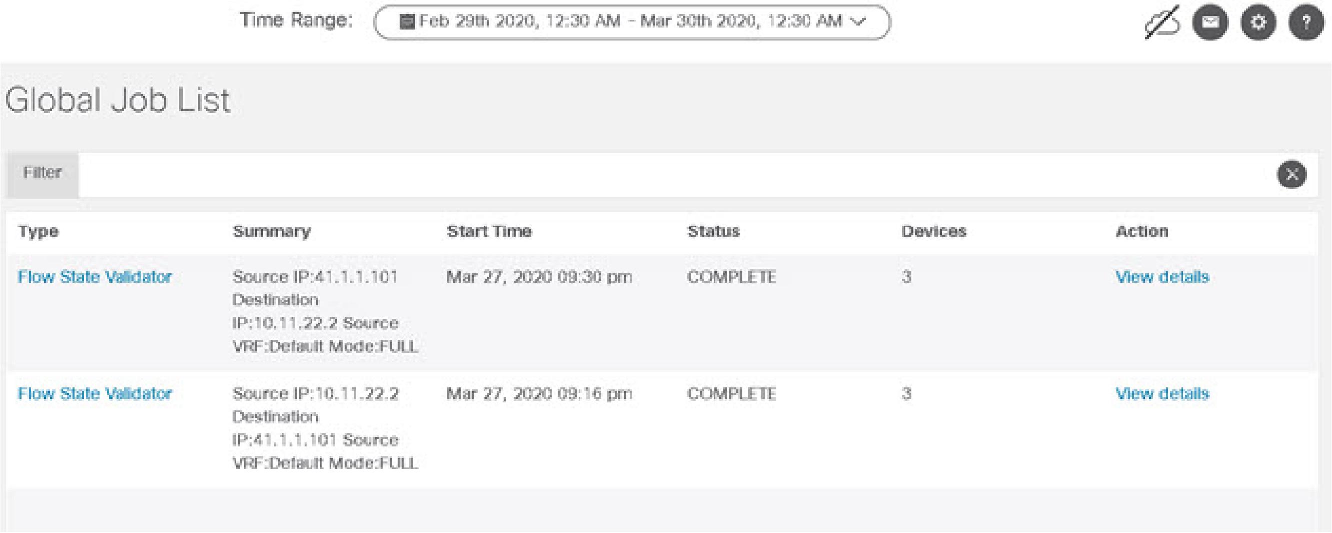
6. Click **Run** to run the flow state validator job.

View Flow State Validator

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

Currently Running Global Jobs

The **Currently Running Global Jobs** lists the jobs that are currently executing.



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

Global Job List

Filter

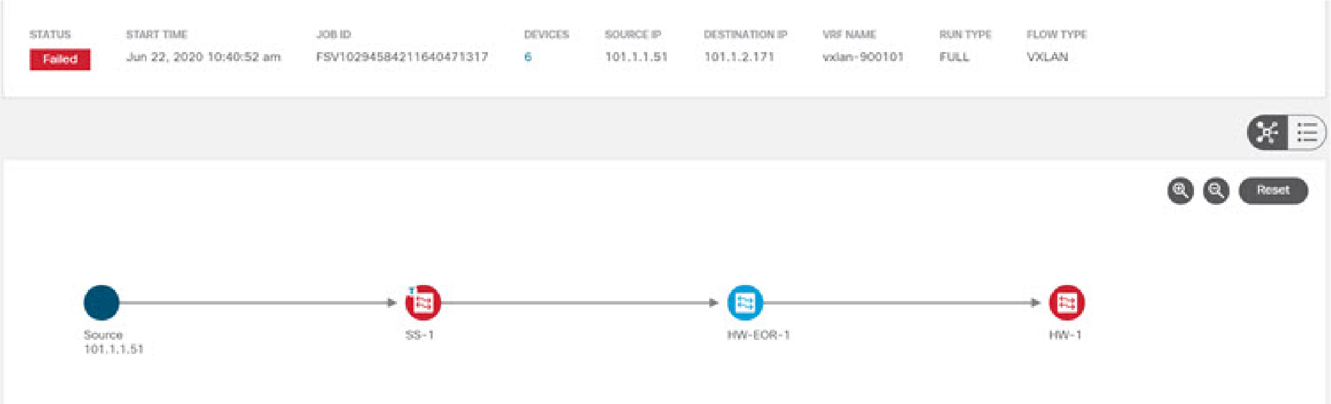
Type	Summary	Start Time	Status	Devices	Action
Flow State Validator	Source IP:41.1.1.101 Destination IP:10.11.22.2 Source VRF:Default Mode:FULL	Mar 27, 2020 09:30 pm	COMPLETE	3	View details
Flow State Validator	Source IP:10.11.22.2 Destination IP:41.1.1.101 Source VRF:Default Mode:FULL	Mar 27, 2020 09:16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

Click a **Flow State Validator** job or click **View Details** from the list to display the **Job Details** page. The job details page shows the tabular and topological view of the job. On the right corner of the page, toggle between tabular and topological view of the job.

Topology View

The Topology view displays all the devices that are traversed to reach the destination. It displays all available paths to the destination. It performs consistency check on each of the devices and displays the aggregated overlay and underlay information.

In a VXLAN type job, the topology view represents the VXLAN encapsulation between source and destination. Encapsulation and decapsulation happen along the source and destination between the sites.



STATUS	START TIME	JOB ID	DEVICES	SOURCE IP	DESTINATION IP	VRF NAME	RUN TYPE	FLOW TYPE
Failed	Jun 22, 2020 10:40:52 am	FSV10294584211640471317	6	101.1.1.51	101.1.2.171	vxlan-900101	FULL	VXLAN

Click the device in the topology view to display flow state validator job details for the node. This page summarizes the flow configuration, consistency checker results where the errors occurred, and the paths for the job.

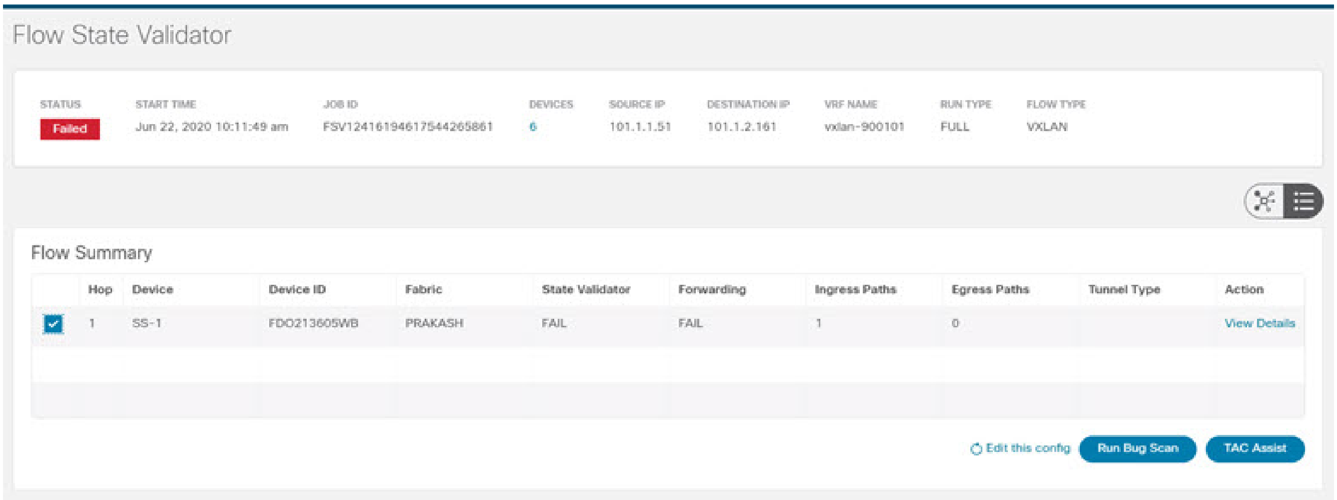
While tracing the path for a site for each ingress interface, the overlay and underlay for a VXLAN type job are represented in the consistency checker results.

Each row in the consistency checker represents a device. Details of the device such as egress path, ingress path, peer device, and peer VLAN are aggregated within a row. Click **View Details** for additional details.

Tabular View

The tabular view summarizes the devices that are running the flow state validator job. The consistency check results show multiple paths for the job. Each row describes a device.

Each detail view aggregates the paths for a device. Click **View Details** for additional 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.



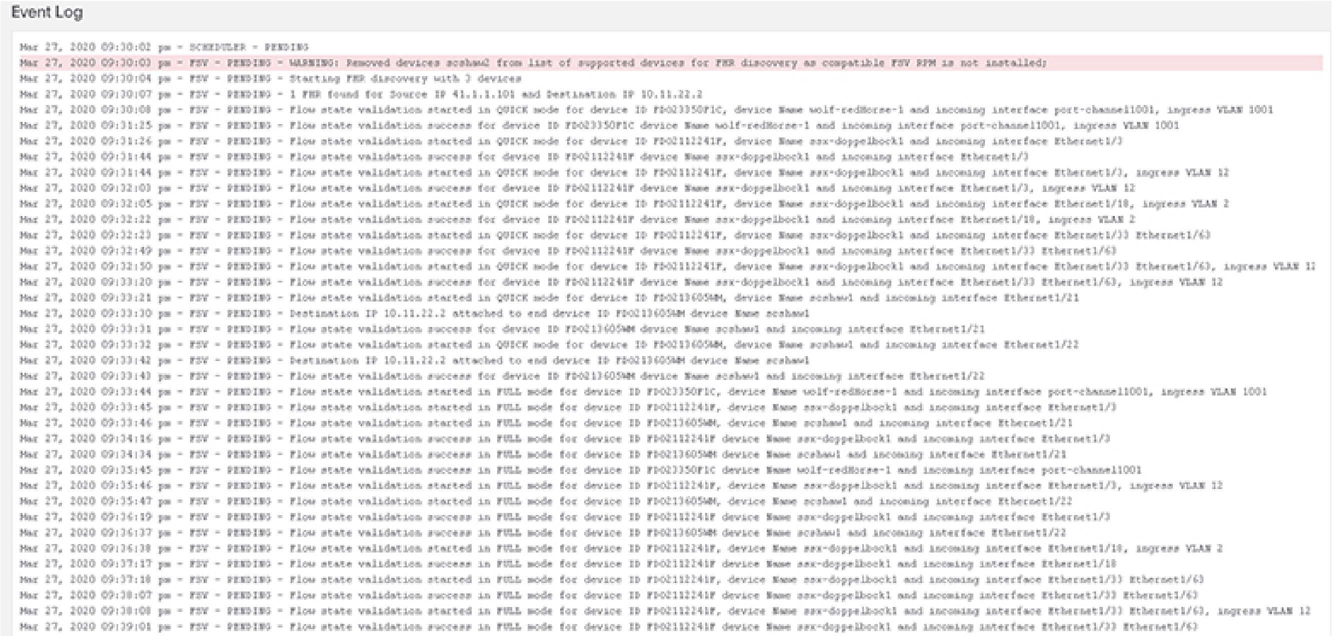
Flow State Validator

STATUS	START TIME	JOB ID	DEVICES	SOURCE IP	DESTINATION IP	VRF NAME	RUN TYPE	FLOW TYPE
Failed	Jun 22, 2020 10:11:49 am	FSV12416194617544265861	6	101.1.1.51	101.1.2.161	vxlan-900101	FULL	VXLAN

Flow Summary

	Hop	Device	Device ID	Fabric	State Validator	Forwarding	Ingress Paths	Egress Paths	Tunnel Type	Action
☑	1	SS-1	FDO213605WB	PRAKASH	FAIL	FAIL	1	0		View Details

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

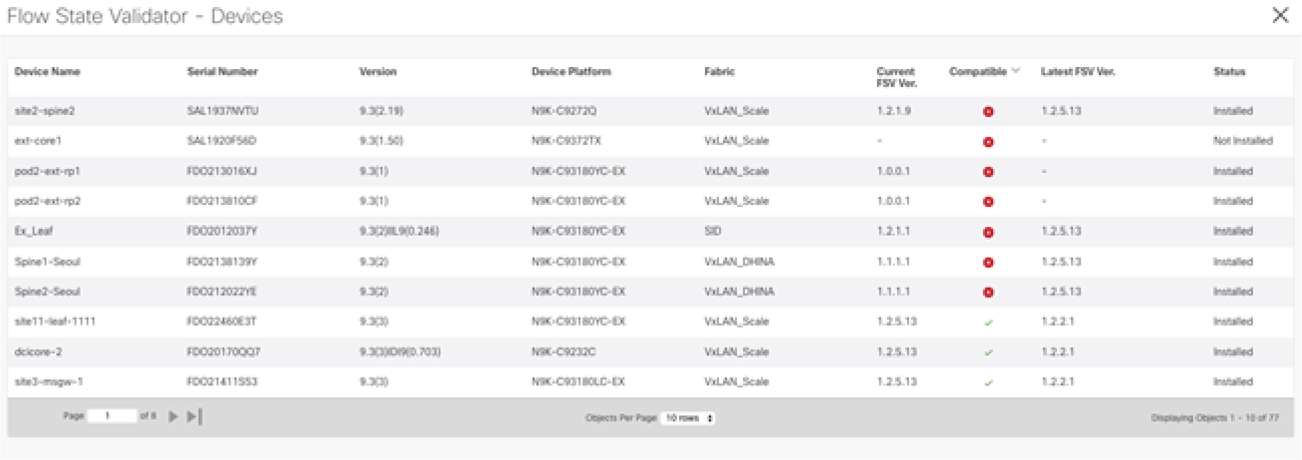


Event Log

```
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 12
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 12
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
```

Job Configs

On the **Global Job Configuration** page, the **Job configs** section lists the 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	FDO212022YE	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	FDO21411SS3	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.

Reuse Flow State Validator to Start Another Job

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

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.

2. Click the job from the **Job Details** page to display the flow state validator details.
3. Click **Edit this config** to edit the configuration details.
4. Click **Run** to execute the job with new configuration.