



Cisco Network Insights Advisor Application for Cisco DCNM User Guide, Release 2.x

First Published: 2020-01-31

Last Modified: 2020-02-20

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



CONTENTS

CHAPTER 1	New and Changed Information	1
	New and Changed Information	1

CHAPTER 2	Cisco Network Insights Advisor Installation	3
	About Cisco Network Insights Advisor	3
	Hardware Requirements	3
	Downloading Cisco Network Insights Advisor from the Cisco App Center	4
	Installing Cisco Network Insights Advisor in Cisco DCNM	4
	Enabling Cisco Network Insights Advisor in Cisco DCNM	5

CHAPTER 3	Cisco Network Insights Advisor Setup and Settings	7
	About Cisco Network Insights Advisor on Cisco DCNM	7
	Guidelines and Limitations	8
	Cisco NIA Initial Setup	9
	Setting Up the Device Connector	9
	About Device Connector	9
	Configuring the Intersight Device Connector	9
	Claiming a Device	12
	Cisco NIA Settings	13
	Navigating Cisco NIA	14

CHAPTER 4	Using Cisco Network Insights Advisor	19
	Using the Cisco NIA Application	19
	Main Dashboard	19
	Advisories Dashboard	20
	Notices Dashboard	23

Issues Dashboard 24

Devices Dashboard 27

TAC Assist Dashboard 29

 User Initiated Upload to Cloud 29

 TAC Initiated Pull from Cloud 30

Jobs Dashboard 31

 Fabric 31

 Global 32

CHAPTER 5 **Troubleshooting Cisco NIA Application 39**

 Debugging Cisco NIA Application 39

 Troubleshooting Cisco NIA on Cisco DCNM 46



CHAPTER 1

New and Changed Information

This chapter contains the following sections:

- [New and Changed Information, on page 1](#)

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.

Table 1: New Features and Changed Behavior in the Cisco Network Insights Advisor application for Cisco DCNM Release 2.0.x

Feature	Description	Release
Metadata refresh	When Cisco NIA is updated to latest from the app settings, the application fetches the latest metadata published version.	2.0.1
Advisory Report	Download Advisory Report as an excel file from the Browse Advisories work pane. Each advisory tab in the excel file lets you view the notices, issues, advisories, and anomaly details for devices in the fabric.	2.0.1
Connected TAC Assist	Connected TAC Assist allows the user to collect logs for specified devices and lets the user upload the logs to the cloud. It also enables Cisco TAC to trigger on-demand collection of logs for specified user devices and pull the logs from cloud.	2.0.1

Feature	Description	Release
Fabric Job	The fabric job provides access to configure and schedule bug scan and compliance check jobs that run across the fabric.	2.0.1
Flow State Validator	The global job provides access to configure and schedule flow state validator jobs that run across the network. The flow state validator helps detect and isolate problematic nodes in the network.	2.0.1
Software Upgrade Path and Upgrade Impact	View the device specific upgrade path to the Cisco NIA recommended release. Check non-disruptive or disruptive result to the first-hop of the path, and view release notes for versions in the upgrade path.	2.0.1



CHAPTER 2

Cisco Network Insights Advisor Installation

This chapter contains the following sections:

- [About Cisco Network Insights Advisor, on page 3](#)
- [Downloading Cisco Network Insights Advisor from the Cisco App Center, on page 4](#)
- [Installing Cisco Network Insights Advisor in Cisco DCNM, on page 4](#)
- [Enabling Cisco Network Insights Advisor in Cisco DCNM, on page 5](#)

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).

Hardware Requirements

This section describes the Cisco DCNM 11.3(1) LAN deployment requirements for Cisco NIA app software telemetry. A Cisco DCNM-native HA deployment is recommended.

Table 2: Hardware Requirements for Deployments up to 80 Switches

Node	Deployment Mode	CPU	Memory	Storage	Network
Cisco DCNM	OVA/ISO	16 vCPUs	32G	500G HDD	3x NIC
Computes (x3)	OVA/ISO	32 vCPUs	64G	500G HDD	3x NIC

Table 3: Hardware Requirements for Deployments from 81 to 250 Switches

Node	Deployment Mode	CPU	Memory	Storage	Network
Cisco DCNM	OVA/ISO	16 vCPUs	32G	500G HDD	3x NIC
Computes (x3)	ISO	40 vCPUs	256G	2.4TB HDD	3x NIC*

* Network card: Quad-port 10/25G


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.

Step 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.

Step 2 Search for Cisco Network Insights Advisor application on the search bar.

Step 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.

Step 4 Review the license agreement and, if OK, click **Agree and download**.

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

What to do next

Make sure the following requirements are met:

- Note the download location of the Cisco Network Insights Advisor file on your local machine.
- 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:

-
- Step 1** You must have administrator credentials to install Cisco Network Insights Advisor applications.
- Step 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.
 - Subnet Requirements for OOB and IB pool: For details on subnet requirements for OOB and IB pool, refer to the [Subnet Requirements](#) section.
 - 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.
- Step 3** You must stop and uninstall any Cisco NIA 1.0.x app prior to installing Cisco NIA 2.x app.
-

What to do next

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.

-
- Step 1** Login to Cisco DCNM GUI with admin privileges.
- Step 2** Click **Application** on the left navigation bar.
- Step 3** Click **Open** from the Cisco NIA application dialog.
- The Cisco Network Insights Advisor application dialog appears.
- Step 4** Check the **Help Cisco improve its products** option.

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



CHAPTER 3

Cisco Network Insights Advisor Setup and Settings

This chapter contains the following sections:

- [About Cisco Network Insights Advisor on Cisco DCNM, on page 7](#)
- [Guidelines and Limitations, on page 8](#)
- [Cisco NIA Initial Setup, on page 9](#)
- [Setting Up the Device Connector, on page 9](#)
- [Cisco NIA Settings, on page 13](#)
- [Navigating Cisco NIA, on page 14](#)

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 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)



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

Guidelines and Limitations


The following are the guidelines and limitations for the Cisco Network Insights Advisor (Cisco NIA) application in the Cisco DCNM:

- IPv6 is not supported for Cisco NIA application in the Cisco DCNM.
- The Cisco NIA application requires that physical servers hosting Cisco DCNM computes as VMs are at least Cisco C220-M4 category. It is also required that a compute be hosted on a data store with a dedicated hard disk of at least 500GB.
- Cisco NIA app retains the collected logs using TAC Assist for 24 hours.
- Cisco NIA app retains the collected technical support information using bag scan for 24 hours.
- Cisco NIA does not support multi-site domain fabric type.
- Cisco NIA does not support nodes with IPv6 management address on Cisco DCNM.
- For remote authentication of Cisco NIA on AAA or TACAS or LDAP:
 - You must have `admin` credentials.

- The LAN credentials must be properly set.

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.

-
- Step 1** Once Cisco NIA app is installed and after your first log in, a welcome dialog appears. Click **Begin Setup**. A **Setup** dialog appears.
- Step 2** In **Data Collection Setup**, click **Configure**.
The **Data Collection Setup** dialog appears. In the **Fabrics** list are fabrics that were discovered during the Cisco NIA application installation.
- Step 3** Check only the fabrics you want visible to the Cisco NIA application.
- Step 4** Click **Ok**.
The **Setup** dialog appears with the selected fabrics appearing in **Data Collection Setup**. You can edit the selected fabric(s) by clicking **Edit configuration**. You can return to the setup utility anytime by clicking the settings icon  and choose **Rerun Setup**.
-

Setting Up the Device Connector

This section describes setting up the device connector for Cisco NIA app on Cisco DCNM.

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, on page 9](#).

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 virtual appliance that helps manage and monitor devices through the Cisco NIA app. The Device Connector provides a secure

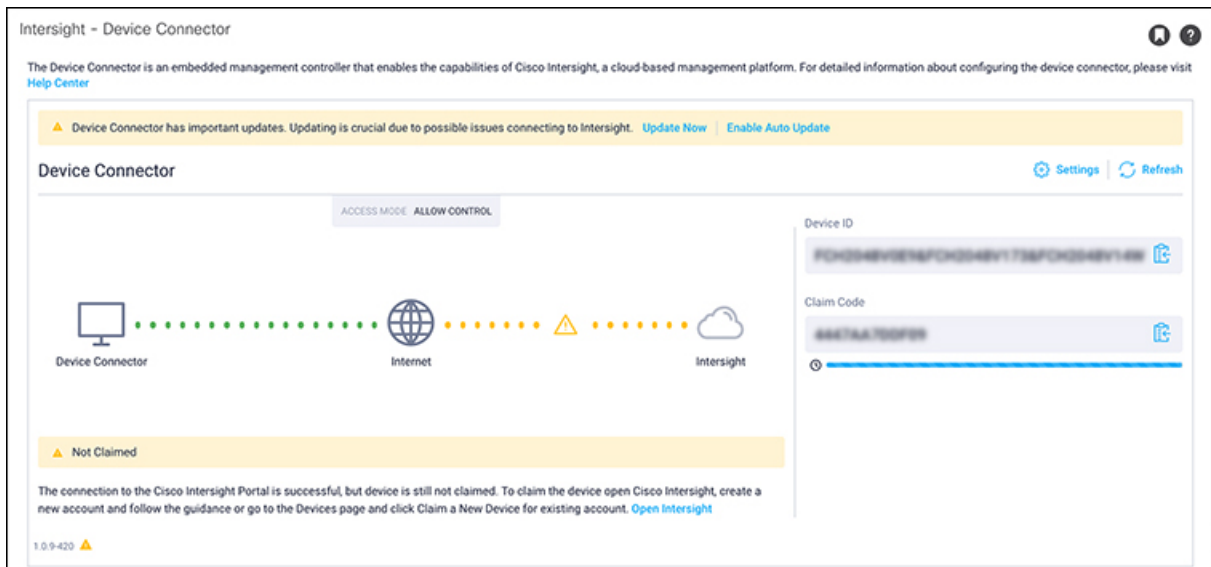
way for connected Cisco DCNM to send and receive information from the Cisco Intersight portal, using a secure Internet connection.

To setup the Device Connector, follow these steps:

Step 1 On the Cisco DCNM navigation pane, click Administration.

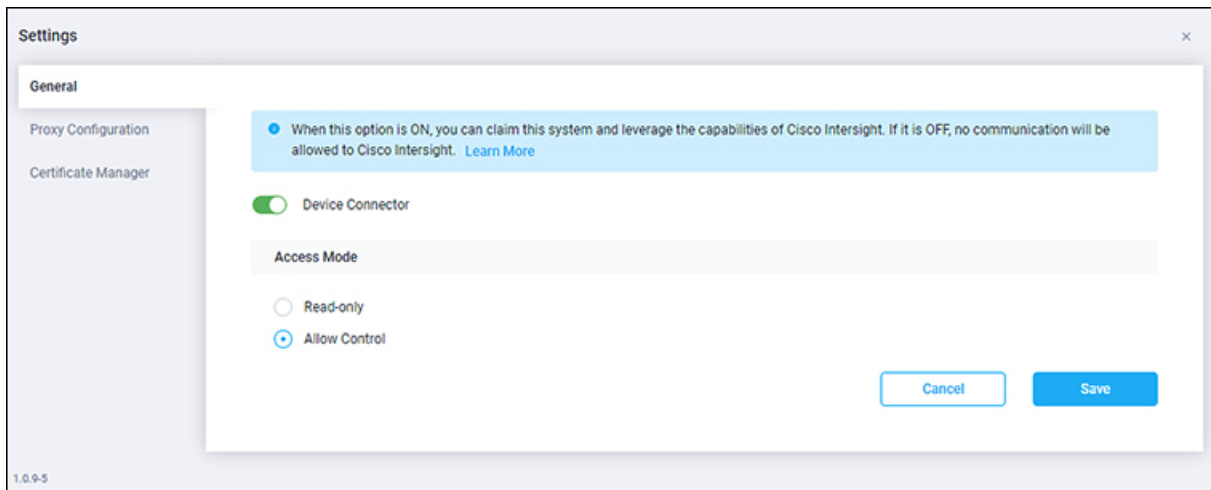
Step 2 Under the Cisco DCNM Server list, click Device Connector.

The Device Connector work pane appears:



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

The **Settings - General** dialog appears:



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

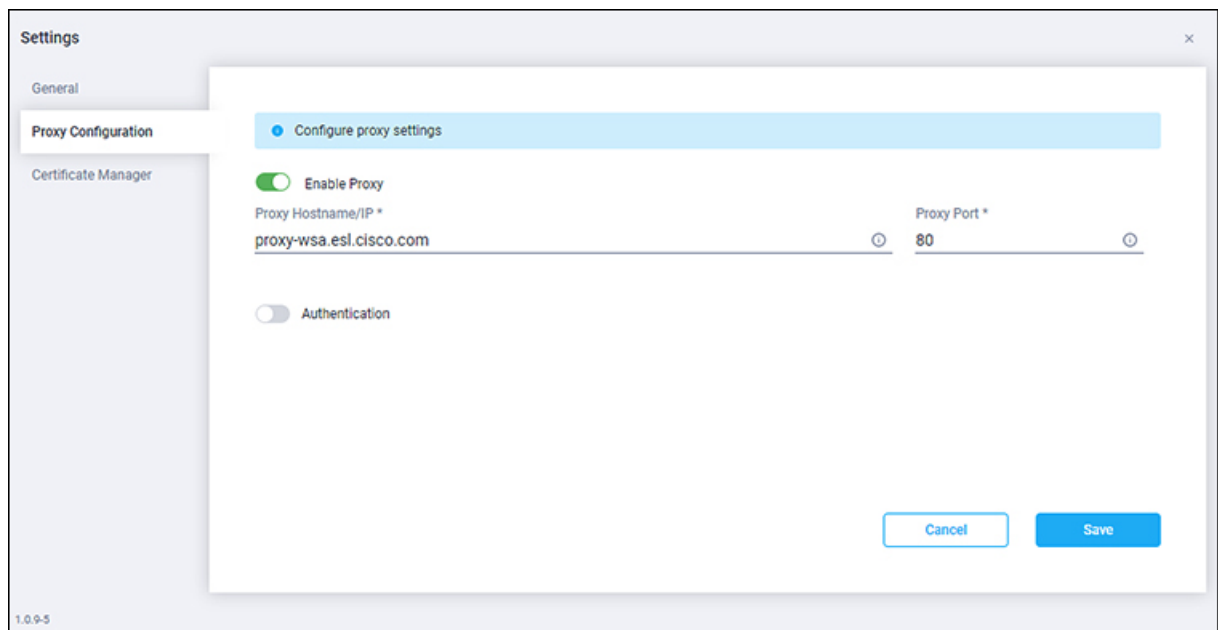
Read-only: This option ensures that no changes are made to this device from Intersight. For example, actions such as upgrading firmware or a profile deployment will not be allowed in the Read-Only mode. However, the actions depend on the features available for a particular system.

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.

Step 4 Set the Device Connector to on (green highlight) and choose **Allow Control**.

Step 5 Click **Proxy Configuration**.

The **Settings - Proxy Configuration** dialog appears.



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.

Note Proxy settings are required for Network Insights.

Step 6 Enable the proxy (green highlight) and enter a hostname and port number.

Step 7 Optional: If proxy authentication is required, enable it (green highlight) and enter a username and password.

Step 8 Click **Save**.

Claiming a Device

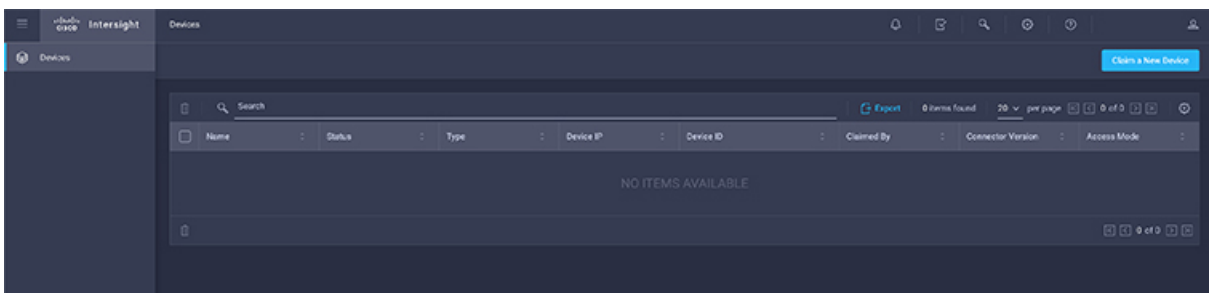
Before you begin

Configure the Intersight Device Connector information from the Cisco DCNM site using the instructions provided in [Configuring the Intersight Device Connector, on page 9](#).

Step 1 Log into the Cisco Intersight cloud site:

<https://www.intersight.com>

Step 2 In the Cisco Intersight cloud site, under the **Devices** tab, click **Claim a New Device**.



The **Claim a New Device** page appears.

Step 3 Go back to the Cisco DCNM site and navigate back to the **Intersight - Device Connector** page.

- On the menu bar, choose **System** > **System Settings**.
- In the **Navigation** pane, click **Intersight**.

Step 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.

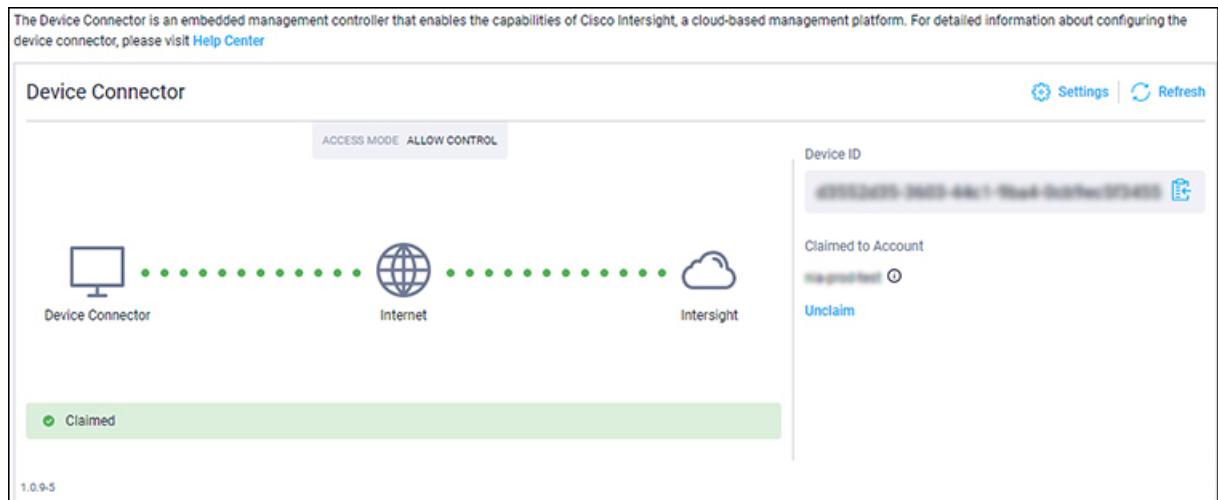
Click on the clipboard next to the fields in the Cisco DCNM site to copy the field information into the clipboard.

Step 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.

Step 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.



Note 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.

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.

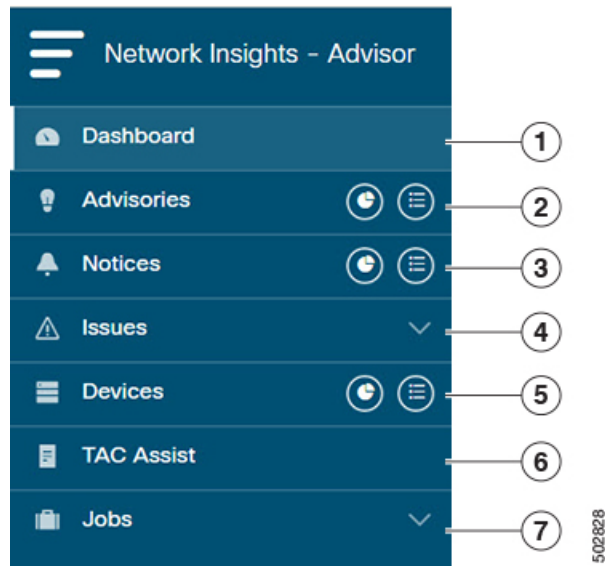
Property	Description
	<p>Device Connector Status: Identifies the current connection status of the Cisco NIA application to the Cisco Intersight cloud and the device connector claim condition. Possible connection statuses are:</p> <ul style="list-style-type: none"> • Not Connected: The Cisco NIA application 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. • Connected / Claimed: The Cisco NIA application is connected to the Cisco Intersight cloud and the device connector has been claimed by the customer. <p>For more information, see Configuring the Intersight Device Connector, on page 9.</p>
	<p>Inbox: View messages from Cisco regarding software upgrades or other relevant information about devices on your network.</p> <p>Note This is a preview feature.</p>
	<p>Clicking on this icon invokes a list menu allowing you to make changes to the following:</p> <ul style="list-style-type: none"> • 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 Connector is connected and claimed. See Configuring the Intersight Device Connector, on page 9 for details. • Rerun Setup—Allows you to edit the Data Collection Setup by adding or removing the fabrics.
	<p>Displays the online help for Cisco NIA application.</p>

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:



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

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

3 Notices: Displays notices applicable to the hardware and software in your network.

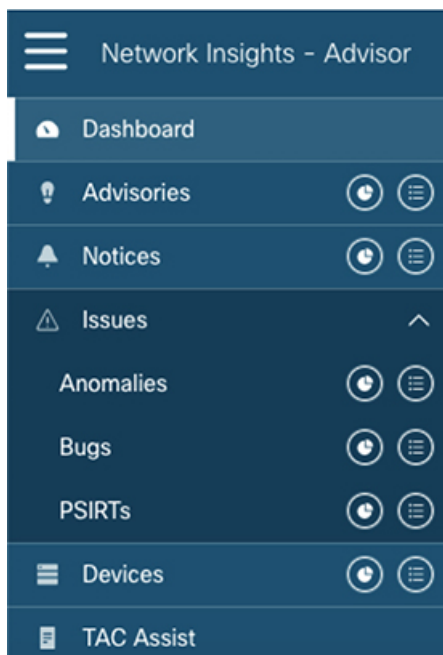
4 Issues: Displays anomalies, bugs, and Product Security Incident Response Team (PSIRT) alerts.

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

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

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

Additional functions are :



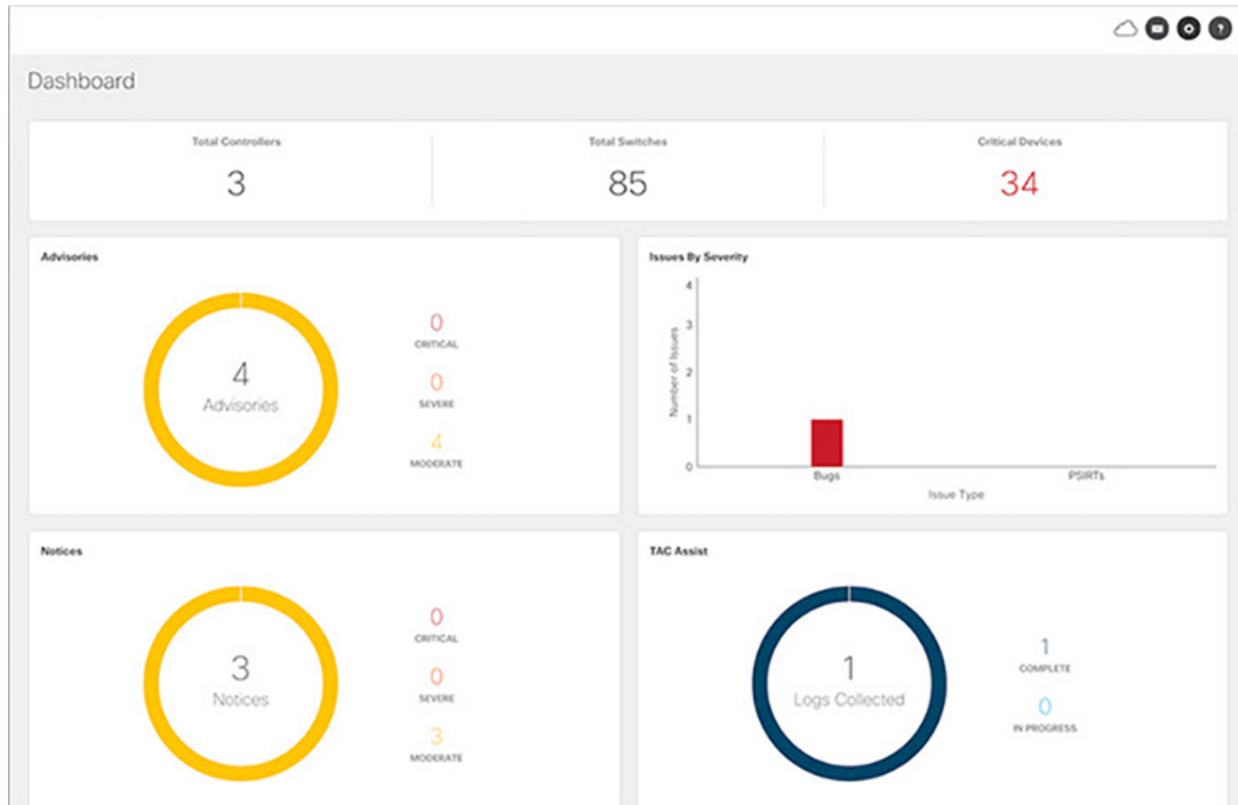
1 Dashboard View icon: Provides immediate access to top usage or issues for the selected information type.

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

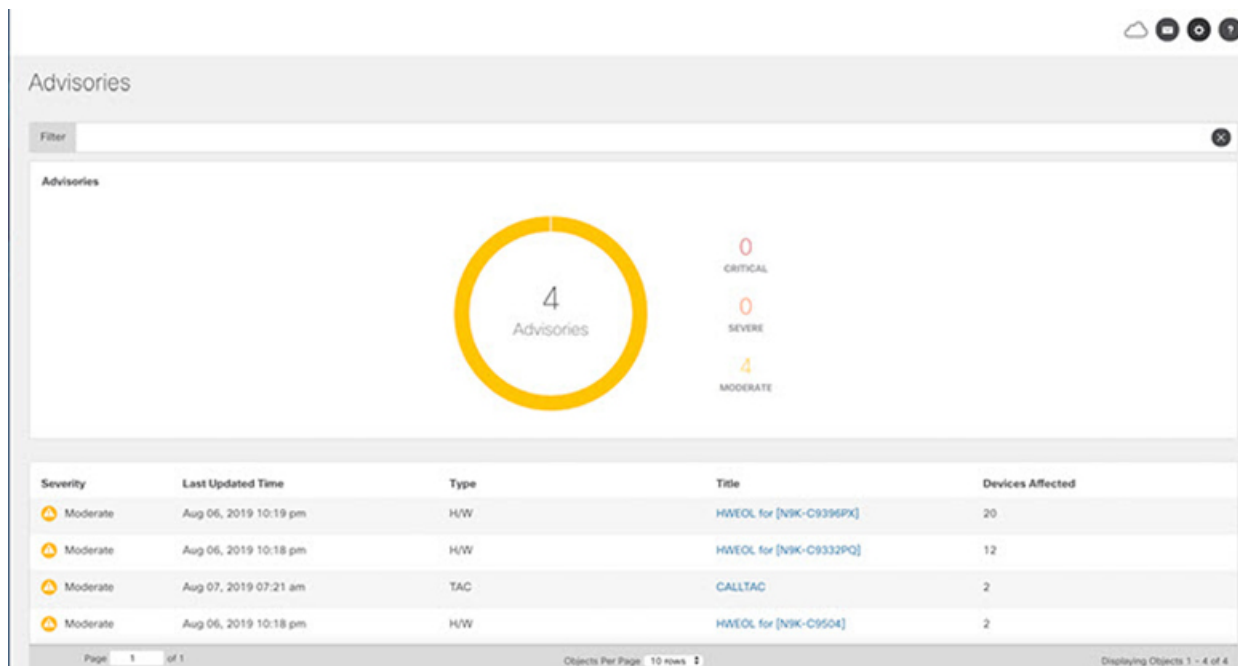
Work Pane

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:



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

2 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

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.
- **Notices:** Includes notices 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.



CHAPTER 4

Using Cisco Network Insights Advisor

This chapter contains the following sections:

- [Using the Cisco NIA Application, on page 19](#)

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: <ul style="list-style-type: none">• 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	<p>Displays a list of all advisories or only for the filtered severity or type. Column labels are:</p> <ul style="list-style-type: none"> • Severity • Last Updated Time • Type • Title: Click the link in the Title column to view details about the advisory. <p>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.</p> <ul style="list-style-type: none"> • 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.

The screenshot displays the 'Advisory Detail' page in the Data Center Network Manager. It features a 'Recommended version is 7.0(3)17(6)' section with a 'Rerun Upgrade Impact' button. Below this is an 'Upgrade Paths' table with the following data:

Recommended Upgrade Paths	Devices Affected	Non Disruptive	Disruptive
7.0(3)7(1) --> 7.0(3)17(6) --> 7.0(3)17(6)	1	1	-

The 'Upgrade Impact Result' table shows the following data:

Device Name	Version	Result	Last Run Time
DTOR-2	7.0(3)7(1)	NONDISRUPTIVE	Jan 16, 2020 11:21 am

The 'Bugs' section shows a bug with the following details:

Severity	Bug	Title	Devices Affected
Moderate	CSCw51737	NIR -EX all interface counters stop incrementing	1

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 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.

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 connected to Cisco Intersight cloud. See [Configuring the Intersight Device Connector, on page 9](#) 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.

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

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.

STATUS	DEVICES	FABRIC	START TIME	JOB ID
Complete	2	mutate-fab	Dec 15, 2019 09:10:37 am	TACASSISTNWB7vifSjgNqXTTJtbA

Device Name	Related Job ID	Status	Status Message	Log Location	Cloud
L81_STMORITZ	N/A	Success		/var/ahw/vols/ceti/uploads/TACAS SISTNWB7vifSjgNqXTTJtbA	Upload
ACC21_SAPPORO	N/A	Success		/var/ahw/vols/ceti/uploads/TACAS SISTNWB7vifSjgNqXTTJtbA	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 collection 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 20](#).

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 24](#) 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(2.18)	N9K-C9372Q	VxLAN_Scale	1.2.1.9	●	1.2.5.13	Installed
ext-core1	SAL1929F56D	9.3(1.55)	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)890.246)	N9K-C93180YC-EX	SID	1.2.1.1	●	1.2.5.13	Installed
Spine1-Seattle	FDO2138139Y	9.3(2)	N9K-C93180YC-EX	VxLAN_DHANA	1.1.1.1	●	1.2.5.13	Installed
Spine2-Seattle	FDO212022YE	9.3(2)	N9K-C93180YC-EX	VxLAN_DHANA	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	FDO201700Q7	9.3(3)890.703)	N9K-C9322C	VxLAN_Scale	1.2.5.13	✓	1.2.2.1	Installed
site3-mgmt-1	FDO21411553	9.3(3)	N9K-C93180LD-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 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.

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.

View Flow State Validator

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.

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-tp1	FDO213016XJ	9.3(1)	VxLAN_Scale	Yes	Device image version not compatible	1.0.0.1	1.0.0.1
pod2-ext-tp2	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)ML9(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	FDO201700Q7	9.3(3)DH9(0.703)	VxLAN_Scale	No	Package Version Compatible	1.2.5.13	1.2.1.1
site3-msgw-1	FDO21411553	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	VEIF NAME	BUN TYPE	FLOW TYPE	
Complete	Mar 27, 2020 09:30:02 pm	FSV12883061754684140917	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]	FDO23359F1C	port-channel1001	1001	OSCO	SUCCESS	SUCCESS	FULL run successful			View D
2	wolf-redhorse-1	six-doppelbock1	FDO2112241F	Ethernet1/3	N/A	OSCO	SUCCESS	SUCCESS	FULL run successful			View D
2	wolf-redhorse-1	six-doppelbock1	FDO2112241F	Ethernet1/3	12	OSCO	SUCCESS	SUCCESS	FULL run successful			View D
2	wolf-redhorse-1	six-doppelbock1	FDO2112241F	Ethernet1/18	2	OSCO	SUCCESS	SUCCESS	FULL run successful			View D
2	wolf-redhorse-1	six-doppelbock1	FDO2112241F	Ethernet1/33 Ethernet1/63	N/A	OSCO	SUCCESS	SUCCESS	FULL run successful			View D
2	wolf-redhorse-1	six-doppelbock1	FDO2112241F	Ethernet1/33 Ethernet1/63	12	OSCO	SUCCESS	SUCCESS	FULL run successful			View D
3	six-doppelbock1	scahaw1	FDO213699WM	Ethernet1/21	N/A	OSCO	SUCCESS	SUCCESS	FULL run successful			View D
3	six-doppelbock1	scahaw1	FDO213699WM	Ethernet1/22	N/A	OSCO	SUCCESS	SUCCESS	FULL run successful			View D

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 09:10:02 pm - SCHEDULED - PENDING
Mar 27, 2020 09:10:03 pm - FSV - PENDING - WARNING: Removed device scbaa2 from list of supported devices for FSR discovery as compatible FSV NPM is not installed.
Mar 27, 2020 09:10:04 pm - FSV - PENDING - Starting FSR discovery with 3 devices
Mar 27, 2020 09:10:07 pm - FSV - PENDING - 1 FSR found for Source IP 41.1.1.101 and Destination IP 10.11.22.2
Mar 27, 2020 09:10:08 pm - FSV - PENDING - Flow state validation started in QUICK mode for device ID FPO21350F1C, device Name wolf-redHorse-1 and incoming interface port-channel1001, ingress VLAN 1001
Mar 27, 2020 09:11:25 pm - FSV - PENDING - Flow state validation success for device ID FPO21350F1C device Name wolf-redHorse-1 and incoming interface port-channel1001, ingress VLAN 1001
Mar 27, 2020 09:11:26 pm - FSV - PENDING - Flow state validation started in QUICK mode for device ID FPO2112241F, device Name sxx-doppelbockl and incoming interface Ethernet1/3
Mar 27, 2020 09:11:44 pm - FSV - PENDING - Flow state validation success for device ID FPO2112241F device Name sxx-doppelbockl and incoming interface Ethernet1/3
Mar 27, 2020 09:11:44 pm - FSV - PENDING - Flow state validation started in QUICK mode for device ID FPO2112241F, device Name sxx-doppelbockl and incoming interface Ethernet1/3, ingress VLAN 12
Mar 27, 2020 09:12:03 pm - FSV - PENDING - Flow state validation success for device ID FPO2112241F device Name sxx-doppelbockl and incoming interface Ethernet1/3, ingress VLAN 12
Mar 27, 2020 09:12:05 pm - FSV - PENDING - Flow state validation started in QUICK mode for device ID FPO2112241F, device Name sxx-doppelbockl and incoming interface Ethernet1/18, ingress VLAN 2
Mar 27, 2020 09:12:22 pm - FSV - PENDING - Flow state validation success for device ID FPO2112241F device Name sxx-doppelbockl and incoming interface Ethernet1/18, ingress VLAN 2
Mar 27, 2020 09:12:23 pm - FSV - PENDING - Flow state validation started in QUICK mode for device ID FPO2112241F, device Name sxx-doppelbockl and incoming interface Ethernet1/33 Ethernet1/63
Mar 27, 2020 09:12:49 pm - FSV - PENDING - Flow state validation success for device ID FPO2112241F device Name sxx-doppelbockl and incoming interface Ethernet1/33 Ethernet1/63
Mar 27, 2020 09:12:50 pm - FSV - PENDING - Flow state validation started in QUICK mode for device ID FPO2112241F, device Name sxx-doppelbockl and incoming interface Ethernet1/33 Ethernet1/63, ingress VLAN 12
Mar 27, 2020 09:13:10 pm - FSV - PENDING - Flow state validation success for device ID FPO2112241F device Name sxx-doppelbockl and incoming interface Ethernet1/33 Ethernet1/63, ingress VLAN 12
Mar 27, 2020 09:13:21 pm - FSV - PENDING - Flow state validation started in QUICK mode for device ID FPO2116059M, device Name scbaa1 and incoming interface Ethernet1/21
Mar 27, 2020 09:13:30 pm - FSV - PENDING - destination IP 10.11.22.2 attached to end device ID FPO2116059M device Name scbaa1
Mar 27, 2020 09:13:32 pm - FSV - PENDING - Flow state validation started in QUICK mode for device ID FPO2116059M, device Name scbaa1 and incoming interface Ethernet1/22
Mar 27, 2020 09:13:42 pm - FSV - PENDING - destination IP 10.11.22.2 attached to end device ID FPO2116059M device Name scbaa1
Mar 27, 2020 09:13:43 pm - FSV - PENDING - Flow state validation success for device ID FPO2116059M device Name scbaa1 and incoming interface Ethernet1/22
Mar 27, 2020 09:13:44 pm - FSV - PENDING - Flow state validation started in FUL mode for device ID FPO21350F1C, device Name wolf-redHorse-1 and incoming interface port-channel1001, ingress VLAN 1001
Mar 27, 2020 09:13:45 pm - FSV - PENDING - Flow state validation started in FUL mode for device ID FPO2112241F, device Name sxx-doppelbockl and incoming interface Ethernet1/3
Mar 27, 2020 09:13:46 pm - FSV - PENDING - Flow state validation started in FUL mode for device ID FPO2116059M, device Name scbaa1 and incoming interface Ethernet1/21
Mar 27, 2020 09:14:16 pm - FSV - PENDING - Flow state validation success in FUL mode for device ID FPO2112241F device Name sxx-doppelbockl and incoming interface Ethernet1/3
Mar 27, 2020 09:14:34 pm - FSV - PENDING - Flow state validation success in FUL mode for device ID FPO2116059M device Name scbaa1 and incoming interface Ethernet1/21
Mar 27, 2020 09:15:45 pm - FSV - PENDING - Flow state validation success in FUL mode for device ID FPO21350F1C device Name wolf-redHorse-1 and incoming interface port-channel1001
Mar 27, 2020 09:15:46 pm - FSV - PENDING - Flow state validation started in FUL mode for device ID FPO2112241F, device Name sxx-doppelbockl and incoming interface Ethernet1/3, ingress VLAN 12
Mar 27, 2020 09:15:47 pm - FSV - PENDING - Flow state validation started in FUL mode for device ID FPO2116059M, device Name scbaa1 and incoming interface Ethernet1/22
Mar 27, 2020 09:16:19 pm - FSV - PENDING - Flow state validation success in FUL mode for device ID FPO2112241F device Name sxx-doppelbockl and incoming interface Ethernet1/3
Mar 27, 2020 09:16:37 pm - FSV - PENDING - Flow state validation success in FUL mode for device ID FPO2116059M device Name scbaa1 and incoming interface Ethernet1/22
Mar 27, 2020 09:16:38 pm - FSV - PENDING - Flow state validation started in FUL mode for device ID FPO2112241F, device Name sxx-doppelbockl and incoming interface Ethernet1/18, ingress VLAN 2
Mar 27, 2020 09:17:17 pm - FSV - PENDING - Flow state validation success in FUL mode for device ID FPO2112241F device Name sxx-doppelbockl and incoming interface Ethernet1/18
Mar 27, 2020 09:17:18 pm - FSV - PENDING - Flow state validation started in FUL mode for device ID FPO2112241F, device Name sxx-doppelbockl and incoming interface Ethernet1/33 Ethernet1/63
Mar 27, 2020 09:18:07 pm - FSV - PENDING - Flow state validation success in FUL mode for device ID FPO2112241F device Name sxx-doppelbockl and incoming interface Ethernet1/33 Ethernet1/63
Mar 27, 2020 09:18:08 pm - FSV - PENDING - Flow state validation started in FUL mode for device ID FPO2112241F, device Name sxx-doppelbockl and incoming interface Ethernet1/33 Ethernet1/63, ingress VLAN 12
Mar 27, 2020 09:19:01 pm - FSV - PENDING - Flow state validation success in FUL mode for device ID FPO2112241F device Name sxx-doppelbockl 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

Flow State Validator details for wolf-redHorse-1

STATUS

Complete

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

Hop	From Device	Description	Command	Status	Error	Action
1	Source	Port-Channel member port state validator	show consistency-checker membership port-channels interface port-channel11 brief	Pass		View Details
2	wolf-redHorse	Port-Channel member port state validator	show consistency-checker membership port-channels interface port-channel1001 brief	Pass		View Details
2	wolf-redHorse	Physical Front Panel Port Link state validator	show consistency-checker link-state interface Ethernet1/63 brief	Pass		View Details
2	wolf-redHorse	Physical Front Panel Port Link state validator	show consistency-checker link-state interface Ethernet1/3 brief	Pass		View Details
2	wolf-redHorse	Physical Front Panel Port Link state validator	show consistency-checker link-state interface Ethernet1/33 brief	Pass		View Details
2	wolf-redHorse	L3 physical routed port state validator	show consistency-checker l3-interface interface vlan 2 brief	Pass		View Details
3	sxx-doppelbockl	Gateway mac state validator	show consistency-checker gwmacdb interface vlan 1001 brief	Pass		View Details
3	sxx-doppelbockl			successful		View Details

[Edit this config](#)

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	six-doppelbock1	FDD2112241F	2	Ethernet1/18
Ethernet1/3	Ethernet1/3	six-doppelbock1	FDD2112241F	N/A	Ethernet1/3
Ethernet1/3.10	Ethernet1/3	six-doppelbock1	FDD2112241F	12	Ethernet1/3
port-channel11	Ethernet1/33	six-doppelbock1	FDD2112241F	N/A	Ethernet1/33
port-channel11	Ethernet1/63	six-doppelbock1	FDD2112241F	N/A	Ethernet1/63
port-channel11.12	Ethernet1/33	six-doppelbock1	FDD2112241F	12	Ethernet1/33
port-channel11.12	Ethernet1/63	six-doppelbock1	FDD2112241F	12	Ethernet1/63

Page 1 of 1

Objects Per Page 10 rows

Displaying Objects 1 - 7 of 7

successful

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.
-



CHAPTER 5

Troubleshooting Cisco NIA Application

This chapter contains the following sections:

- [Debugging Cisco NIA Application, on page 39](#)
- [Troubleshooting Cisco NIA on Cisco DCNM, on page 46](#)

Debugging Cisco NIA Application

Cisco NIA Application Start

To debug Cisco NIA app start in bootstrap, check the following file in compute nodes for any issues in Cisco NIA app specific install hooks.

```
/var/afw/applogs/NIA/NIAshook_Cisco_afw_log.old
```

Example:

```
2019-06-05 22:04:32,345 INFO          config.py:016 Running in APIC
```

```
.....
```

```
2019-06-05 22:04:32,782 INFO      kafka_configure.py:064 Kafka Correct config=True
```

```
2019-06-05 22:04:32,782 INFO apic_configure_nia.py:033 Start hook passed kf_done=True
```

```
Clean hooks are in /var/afw/applogs/NIA/NIAshook_Cisco_afw_log.old
```

The first login for Cisco NIA app takes some time for UI transition. The following message is displayed until application loads completely.

```
Please wait while Application data is being loaded.
```

Cisco NIA Application User Interface

- Most common user interface issues are due to receiving unexpected data from the APIs. Open the developer tools network tab and repeat the last action. It displays the API data received.
 - For issues with APIs, troubleshoot the backend logs.
 - For successful API requests and responses, check the developer tools console tab for errors, empty or unexpected data in the UI.
- After initial installation, the application needs time for UI transition and load completely. For any errors take screenshots before and after reproducing an issue.

- Take a screenshot of full network capture saved as a HAR from your browser. Open a service request and attach a HAR recording, backend logs, and screenshots for root cause analysis.

Statistics Telemetry

Statistics telemetry enables Cisco to collect statistics, inventory, and other telemetry information from customer networks. To debug statistics telemetry:

- Make sure that Device Connector is connected to Intersight cloud and claimed using the Device Connector user interface.
- Make sure that telemetry streaming is enabled. Check the check box for **Help Cisco improve its products**.
- Log into the compute node where the Device Connector is running.

```
# docker ps | grep "device \\\ intersight"
# docker exec it <dc container> bash
```

- In the logs directory, check the Device Connector logs for any failures related to inventory or etl update. Record the errors, collect Device Connector details, and collect Cisco NIA tech-support.

Advisory Report

Advisory report allows the user to export all advisory information from a link on the Advisories list view. To debug perform the following steps:

- From your browser tools page, right click Inspect, and click the network tab in your browser. Check if `/getAdvisoryReport` endpoint HTTP call status is success.
- For a failed API call, view Active Data micro-service logs to check for any errors thrown in the micro-service. Collect Active Data micro-service logs for further analysis.

If the API call is successful, but the file is not downloaded, check any popup blockers are enabled in the browser.

Debugging Software Upgrade Path and Upgrade Impact

1. From your browser tools page, check if POST to `upgradepath` endpoint is successful and input or output data is as expected.
2. To check the upgrade impact logs:
 - a. Log into the compute node where the upgrade impact container is running.


```
# docker ps | grep "upgradeimp"
# docker exec -it <container_id> bash
```
 - b. Check for any errors in the upgrade impact logs from the logs directory.
 - c. Make a note of the POST data, errors, screenshots of UI and collect Cisco NIA tech support.

The following are the examples for `upgradepath`.

Cisco NXOS

```
time="2020-01-22 07:43:59.485" level=info msg="new AdvMap=74522df14dfcas-UPG-admin"
file="upgradepath:204"
```

```
time="2020-01-22 07:43:59.485" level=info msg="Starting issumatrix call nxos 7.0(3)I7(1)
9.3(1)" file="upgradepath:277"
time="2020-01-22 07:43:59.485" level=info msg="Res output:[7.0(3)I7(1) 7.0(3)I7(5a) 9.3(1)]"
file="upgradepath:297"
time="2020-01-22 07:43:59.486" level=info msg="Sending POST response" file="upgradepath:258"
```

Notices

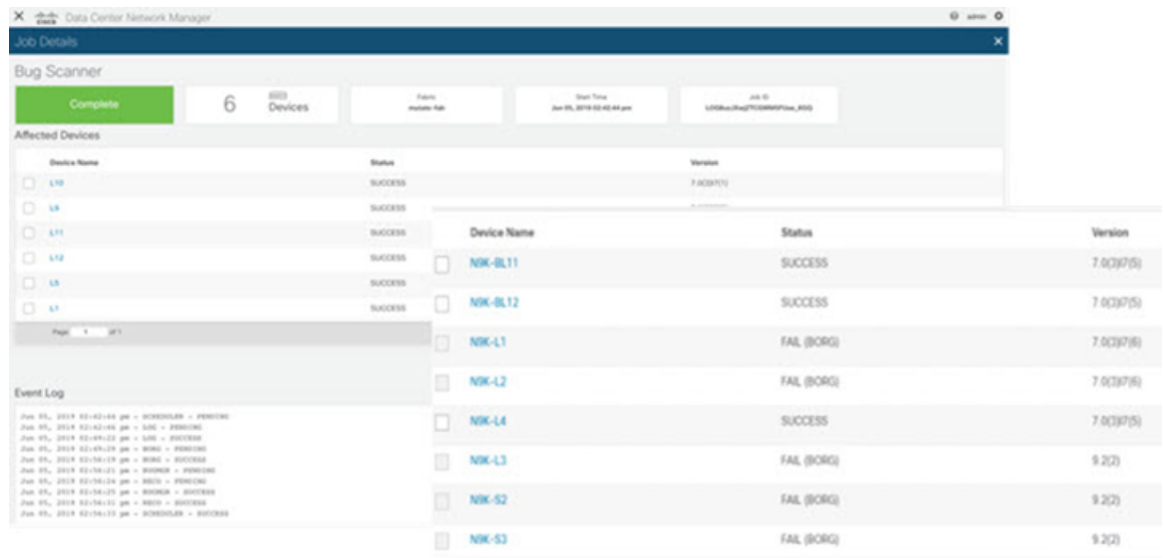
To debug notices:

- Connect to the Intersight cloud and claim the Device Connector atleast once.
- Make sure that all the devices are available in the network.
- Make sure that all data is downloaded successfully.
- In case no notices appear, collect device connector details and collect Cisco NIA tech-support.

Bugs and PSIRTs

To debug for bug scan and PSIRTs:

- Connect to the Intersight cloud and claim the Device Connector atleast once.
- Make sure that all the devices are available in the network.
- Make sure that all metadata is downloaded successfully.
- Configure the on-demand bug scan.
- Check for the bug scan on-demand job progress.



- In the log archiver, check the tech-support logs collected from switch.
 - In case the logs are not collected, then collect infra tech-support.
 - In case the collected logs do not show the bugs, then collect Cisco NIA tech-support.

TAC Assist On-demand

To debug TAC assist on-demand job:

- Check the status of the job in the **Job List** page.
- In the log archiver, check that the logs are successfully collected from the switches.
- Check the logs are available in Cisco DCNM.
- Collect the Cisco NIA tech-support in case of a failure.

Running Jobs

To debug abort or partial failures:

- Check that the infra services are up and running (Kafka, AFW). Collect infra tech-support if the services are not running.
- Collect Cisco NIA tech-support if the infra services are up and running.

Enhanced TAC Assist - User Initiated Upload to Cisco Cloud

In the user initiated TAC assist, the user collects the logs for specified devices and then uploads the collected logs to Cisco cloud. To debug perform the following steps:

- Make sure that Device Connector is connected to Intersight cloud and claimed using the Device Connector user interface.
- Log into the compute node where the Device Connector is running.

```
# docker ps | grep "device \\\ intersight"
# docker exec it <dc container> bash
```

- In the logs directory, check the Device Connector logs for any failures related to inventory or etl update. Record the errors, collect device connector details and collect Cisco NIA tech-support.

Example for uploading logs to Cisco cloud.

```
T22:05:35.087-0800 info stdplugins/techsupport.go:107
  Received request to collect techsupport for device: FDO22242J62, type: switch
{"traceId": "AS0cb8885d3e0ad999ec14d74a5074cbd6", "traceId":
"PE98f043ee82967a1831f5a8c9eedfe25b"}
T22:05:35.087-0800 info stdplugins/techsupport.go:166
  Invoking techsupport function. {"traceId": "AS0cb8885d3e0ad999ec14d74a5074cbd6",
"traceId": "PE98f043ee82967a1831f5a8c9eedfe25b"}
T22:05:35.087-0800 info niatech/techsupport.go:370
{"traceId": "AS0cb8885d3e0ad999ec14d74a5074cbd6", "traceId":
"PE98f043ee82967a1831f5a8c9eedfe25b"}
T22:05:35.087-0800 info niatech/techsupport.go:371      FDO22242J62
{"traceId": "AS0cb8885d3e0ad999ec14d74a5074cbd6", "traceId":
"PE98f043ee82967a1831f5a8c9eedfe25b"}
T22:05:35.122-0800 info niatech/techsupport.go:339
  Got device model from dp
{"traceId": "AS0cb8885d3e0ad999ec14d74a5074cbd6", "traceId":
"PE98f043ee82967a1831f5a8c9eedfe25b"}
File start being uploaded:
T12:34:17.630-0800 info niatech/techsupport.go:425
  Nashville: Finished techsupport collection with deviceType: switch, deviceId:
FDO22232LMZ
```

```

{"traceId": "ASc1a31b74ce56d39c3080fc97a4eba779", "traceId":
"PE0194accfee60ba13eee45ff21fa32b81"}
T12:34:17.630-0800 info niatech/techsupport.go:426
    Nashville: Initiating techsupport upload with deviceType: switch, deviceId:
FDO22232LMZ
{"traceId": "ASc1a31b74ce56d39c3080fc97a4eba779", "traceId":
"PE0194accfee60ba13eee45ff21fa32b81"}

```

Flow State Validator First Hop Router Discovery

In the following scenarios collect Cisco NIA app and agent tech-support from affected switches for further debugging.

- Make sure that source IP or source MAC is available in the devices installed with compatible Cisco NIA agent RPM.
- In case FHR discovery fails and source IP or source MAC is available in Address Resolution Protocol (ARP) or MAC table for a device, then check if the device is not excluded from list of supported devices for FHR discovery.

The following is an example for flow state validator event log.

```

02:23:56pm - FSV - PENDING - WARNING: Removed devices ext-core1 Ex_Leaf site2-spine2
from list of supported devices for FHR discovery as compatible FSV RPM is not installed;

```

- If the following error occurs in error log, then check for SIM output in flow state validator log. It occurs when SIM is unable to connect to the device to execute CLI hosted by Cisco NIA agent. Ping the compute node where SIM is running on the device to check if it works.

```

02:23:57 pm - FSV - PENDING - WARNING: FHR discovery skipped for devices tor1
due to connectivity failure.

```

- If the following error occurs in error log, then check for SIM output in flow state validator log. It occurs when SIM receives no or malformed data from Cisco NIA agent. In this case check if compatible Cisco NIA agent RPM is installed in the switch.

```

02:23:57 pm - FSV - PENDING - WARNING: FHR discovery failure,
received invalid response from agent.

```

- The following error occurs when source IP or source MAC is not available in Address Resolution Protocol (ARP) or MAC table of devices included for flow state validator job.

```

12:19:09 pm - FSV - ABORT - WARNING: FHR not found for
Source IP 60.0.0.11 and Destination IP 60.101.0.72

```

Flow State Validator Quick and Full Run

The following are debugging details for quick run and full run in a flow state validator job. In all these scenarios collect Cisco NIA app and agent tech-support from affected switches for further debugging.

- The flow tracing stops and fails immediately when agent returns failure while running in quick mode.
- In full mode the consistency checker runs in parallel in all the devices belonging to flow path. Consistency check errors are reported from multiple devices in flow summary table. See the flow summary table for errors and collect details for further debugging.
- If the following error appears in the error log, then check if the device is listed in the list of active devices for this flow state validator job. If not listed, then click **Device Count** to check the reason for exclusion in the flow detail page.

```
04:12:44 pm - FSV - PENDING - WARNING: Device ID SAL123456 Device Name spine1 not found
in FSV supported device list, Skipping...
```

- If the following error appears in the error log, then check for the SIM output in flow state validator log. It occurs when SIM receives no or malformed data from Cisco NIA agent. In this case check if compatible Cisco NIA agent RPM is installed in switch. Collect Cisco NIA agent tech-support from affected device.

```
02:23:57 pm - FSV - PENDING - WARNING: Flow state validation failed for
device ID FDO453245 device Name Spine, received invalid response from agent, Skipping...
```

- If the following error appears in the error log, then check for the SIM output in flow state validator log. It occurs when SIM is unable to connect device to execute CLI hosted by Cisco NIA agent. Ping the compute node where SIM is running on the device to check if it works.

```
02:23:57 pm - FSV - PENDING - WARNING: Flow state validation failed for
device ID FDO453245 device Name eor1 due to error device connectivity failure, Skipping...
```

- The flow state validator job is declared failure, if either quick run fails or consistency checker fails in full mode, or no path can not be traced to reach destination node.

Cisco NIA Log Paths

Collect the following logs to debug:

- Cisco DCNM:

- Within the container.

```
/opt/nia/<microservice>/log/<rotated log file>

bash-4.2# env|grep NIA
NIA_MS_LOGFILE=core.log
NIA_MS_HOME=/opt/nia/core/
NIA_MS_LOGDIR=/opt/nia/core/log
```

- On each compute.

```
/var/afw/applogs/NIA/appid_Cisco_afw_log/<logfile>
```

- Docker logs.

```
-f <container_id>
```

- Cisco DCNM master.

```
[root@dncm-mr2-node115 ~]# appmgr afw fetch-logs Cisco:NIA
```

Cisco DCNM Infra Log Paths

To debug logs:

- SIM on each compute logs.

```
[root@compute2 sim]# pwd
/var/afw/applogs/simagent_Cisco_afw_log/sim
[root@compute2 sim]# ls -lrth
total 3.7M
lrwxrwxrwx 1 root root 29 Jun 2 21:12 sim.log -> /var/log/toHost/sim/sim.log.1
-rw-r--r-- 1 root root 3.7M Jun 5 15:29 sim.log.1
```

- CETI on each compute logs.


```
[root@compute2 ceti_Cisco_afw_log]# pwd
/var/afw/applogs/ceti_Cisco_afw_log
[root@compute2 ceti_Cisco_afw_log]# ls -lrth
total 11M
lrwxrwxrwx 1 root root 26 Jun 5 14:15 ceti.log -> /var/log/toHost/ceti.log.1
-rw-r--r-- 1 root root 11M Jun 4 11:28 ceti.log.1
```

- Kafka, Zookeeper, ElasticSearch logs.

```
[root@compute2 applogs]# pwd
/var/afw/applogs
drwxr-xr-x 3 root root 4096 Jun 2 20:53 elasticsix_Cisco_afw_log
drwxr-xr-x 3 root root 4096 Jun 2 20:53 zookeeper_Cisco_afw_log
drwxr-xr-x 3 root root 4096 Jun 2 20:53 kafka_Cisco_afw_log
```

- Kafka, Zookeeper, ElasticSearch Docker logs.

```
docker ps --format 'table {{.ID}} {{.Image}}' | egrep "elastic:6|kafka|zookeeper"

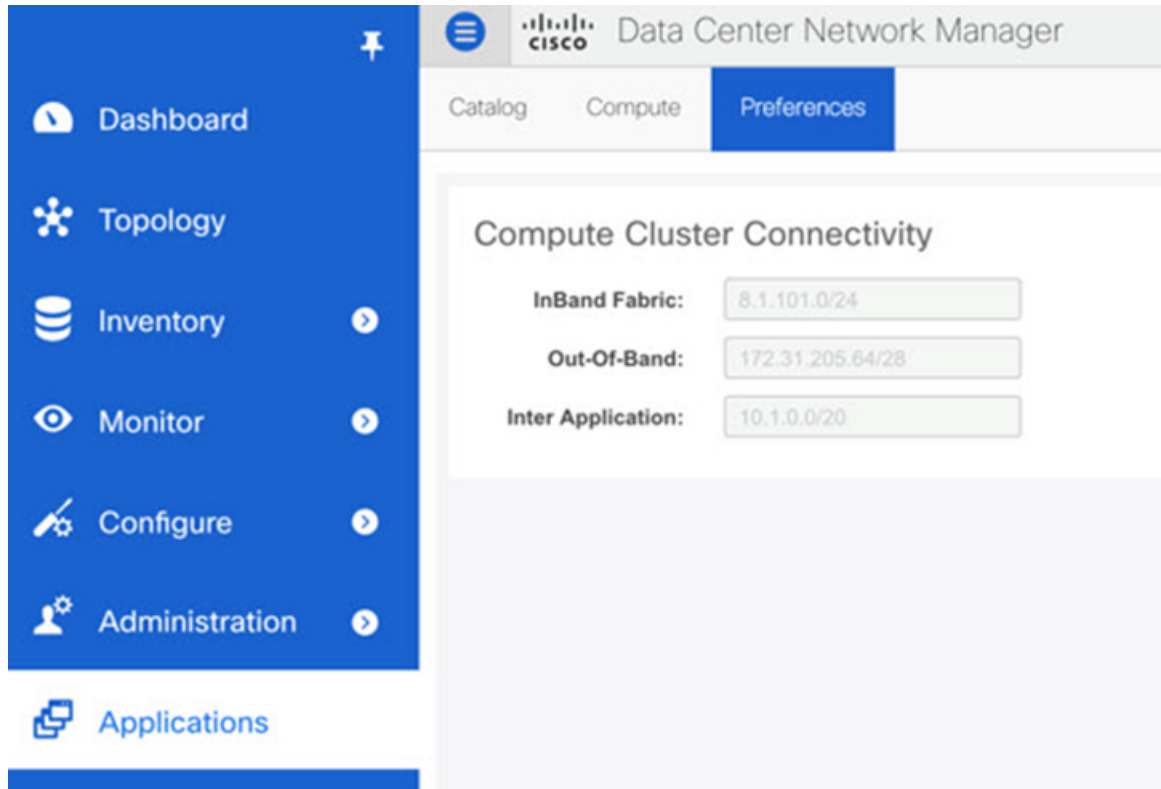
CONTAINER ID IMAGE
8335f5140d42 172.31.205.60:5000/dcnmkafka:2.11_2.1.1
8c98df915797 172.31.205.60:5000/dcnmzookeeper:3.4.12
2e7e79eb22f0 172.31.205.60:5000/dcnmelastic:6.1.4
```

```
docker logs 8335f5140d42
Infra:
[root@dcnm-master ~]# appmgr afw fetch-logs Cisco:stalker
[root@dcnm-master ~]# appmgr afw fetch-logs Cisco:ceti
[root@dcnm-master ~]# appmgr afw fetch-logs Cisco:kafka
[root@dcnm-master ~]# appmgr afw fetch-logs Cisco:elasticsix
```

Troubleshooting Cisco NIA on Cisco DCNM

Device Reachability and Authentication

Figure 1: Device Reachability



The following table summarizes the device reachability and authentication errors.

Problem	Solution
Device reachability	<ul style="list-style-type: none"> • Cisco NIA needs to reach the Management IP of each device it monitors to be able to perform bug scan, compliance check, TAC assist, and upgrade impact. • Connectivity to the Management IP of each device is through eth1 of SIM container and computer node. • The connectivity to the Management IP of each device is automatically taken care, when compute cluster is setup and out-of-band is entered.

Problem	Solution
Device authentication	<ul style="list-style-type: none"> • To discover devices, you need administrator credentials for device <code>username</code> in Cisco DCNM. Or, you need LAN credentials for the device to discover devices.
Infra	<ul style="list-style-type: none"> • Kafka: Check In Sync Replicas (ISR) for kafka related issues. • Elastic Search: Check HTTP errors for elastic search related issues. • SIM/CETI: Check Cisco DCNMcontainer logs. • Check for any loss of compute nodes. • Check Cisco DCNM master to standby failover.

Figure 2: Device Authentication Configuration

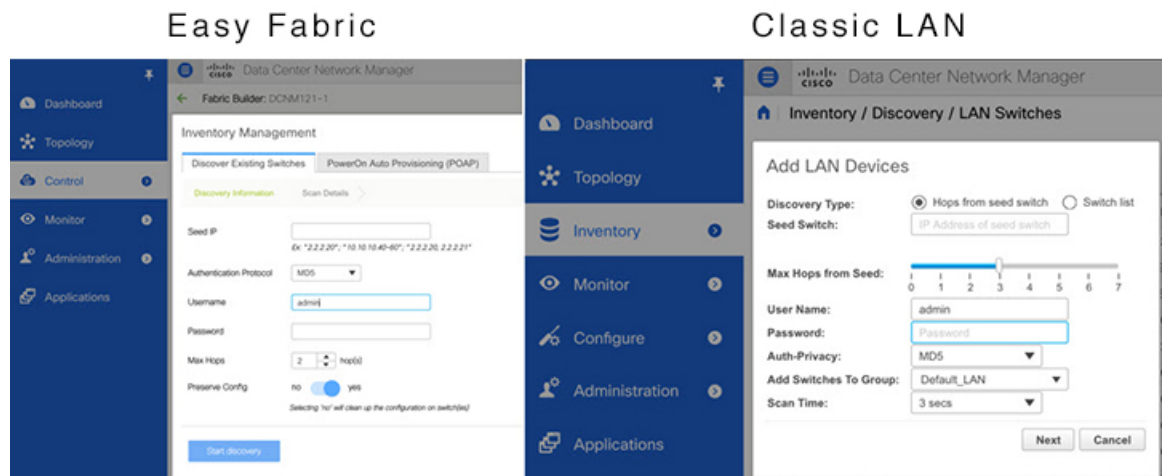
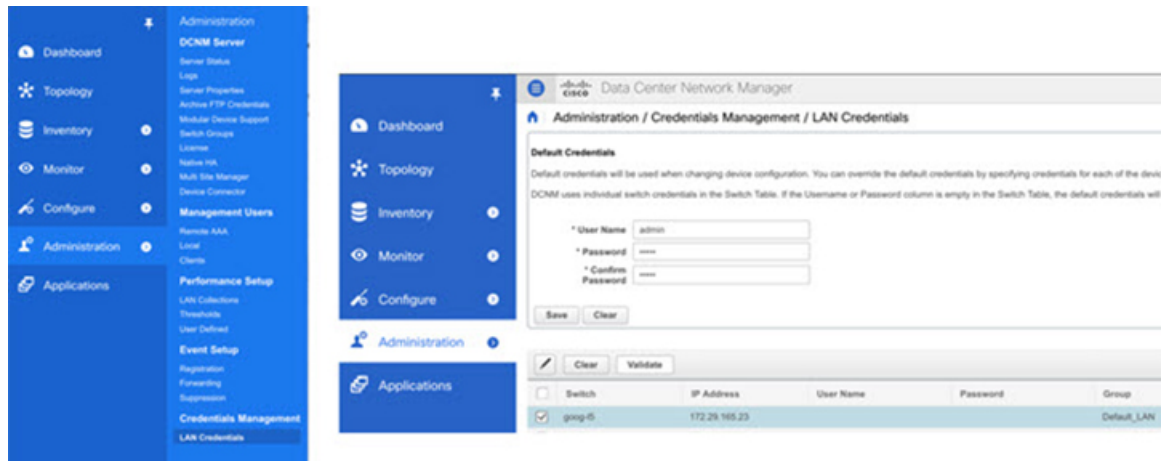


Figure 3: Device Authentication LAN Credentials



Enhanced TAC Assist - TAC Initiated Pull from Cisco Cloud

The following table summarizes how to troubleshoot errors for Cisco TAC triggered on-demand collection of logs for specified devices, which were pulled from Cisco cloud.

Problem	Solution
The app returns a 404 error, "The serial number is not present in DP inventory" when triggering the technical support job.	<ul style="list-style-type: none"> • Make sure the device must be registered as endpoint in Device Connector. • Borgcore has a scheduler job to monitor the Device Connector claim change and devices change. After you claim the Device Connector or upload a newly added device, allow 5 minutes for Borgcore to detect the change and register correspondingly. After 5 minutes if the issue still exists, check Borgcore > techsupport log and check the registration log for errors.
The app returns an error, "NotFound" "The requested device is not registered in the system" when triggering fast-start job.	<ul style="list-style-type: none"> • Make sure the device you want to collect is registered in the same cloud. If the problem still persists, it could be due to duplicate claim of the same device. Intersight returns error if there is more than one device with the same serial number and PID combination. • Duplicate claim of the device can occur when Device Connector was unclaimed and claimed again without deleting the Device Connector from the Intersight UI. Unclaiming the Device Connector from UI will not delete the MO from the Intersight database.

Software Upgrade Path

The following table summarizes the troubleshooting scenarios for software upgrade path.

Problem	Solution
Unable to see an upgrade path after running bug scan or having a software EOL.	If bug scan or software EOL advisory displays “Contact Cisco Technical Assistance Center (TAC)” then upgrade path cannot be shown, since there is no target version to check against. Software version advisories are required to see an upgrade path, which shows the recommended version.
In the upgrade path link for two releases, multi-hop is displayed, but Cisco NIA displays single hop.	If an internal error occurs while calculating the upgrade path, Cisco NIA defaults to the single hop. See the section below for debugging upgrade path issues.
Newer version is not displayed in the recommended release or in the upgrade path.	<ul style="list-style-type: none"> • Check for the cloud connectivity and for the latest version of metadata. • If the latest version is available to run, then run metadata update and bug scan update.

