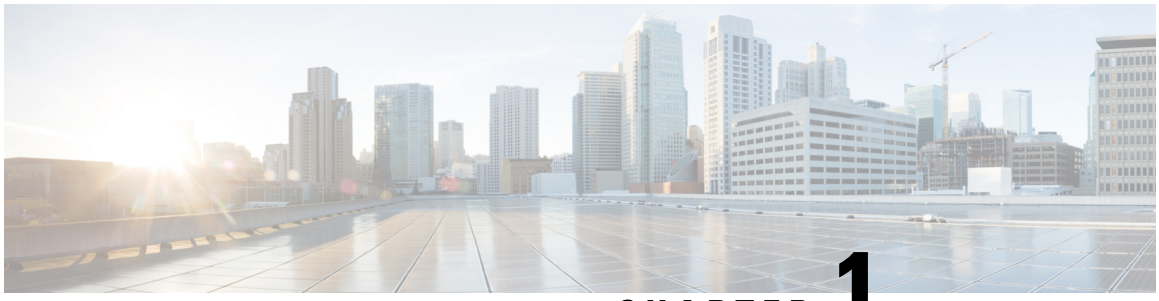
Cisco Network Insights Advisor Application for Cisco APIC User Guide, Release 2.x

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

This chapter contains the following sections:

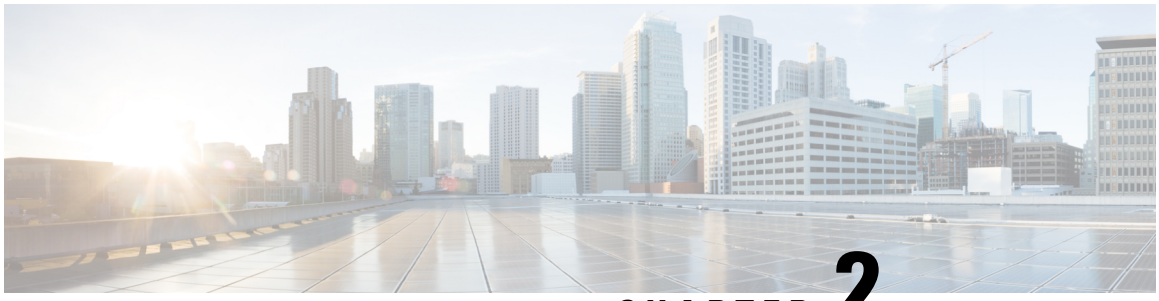
New and Changed Information

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 app for Cisco APIC 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
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
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

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
Software Upgrade Path	View the recommended upgrade path to the recommended release. Also see the release notes, procedure, caveats and open defects 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 Cisco Application Services Engine

Cisco Network Insights Advisor (Cisco NIA) application consists of monitoring utilities that can be added to the Cisco Application Services Engine using the Cisco Application Policy Infrastructure Controller (Cisco APIC).

Downloading Cisco NIA Application from the Cisco App Center

This section contains the steps required to download Cisco NIA application in the Cisco APIC in preparation for installation.

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 APIC GUI.
  a. Login to the Cisco APIC 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.

Installing Cisco NIA Application on Cisco Application Services Engine

This section contains the steps required to install Cisco Network Insights Advisor application on the Cisco Application Services Engine using the Cisco APIC. This set up is required for Cisco NIA application to show important information and gather relevant data.

Before you begin

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

- You have installed and configured Cisco Application Services Engine.
- You must have administrator credentials to install Cisco Network Insights Advisor application.

Step 1 Log in to the Cisco APIC GUI with admin privileges.

Step 2 Click **Admin** tab and then click **Downloads** from the top navigation bar.

Step 3 Click **Service Engine** from the tabs on the far-right side. Then select **Upload File**.

The **Add File to Service Engine** dialog appears.

Step 4 In the **URL** enter the http address and click **Submit**.

You can click **Refresh** icon ↻ on the far-right side of the Downloads work pane to check the upload status.

Step 5 Once the **Status** is complete then click the **Apps** tab.

The Cisco NIA application installation progress dialog appears.

The **Service Engine** dialog describes that the application is for configuring the Cisco Application Services Engine cluster.

Step 6 Once the installation is complete then click **Enable** in the Cisco NIA application dialog.

Step 7 Click the **Apps** tab. Then click **Open** from the Cisco NIA application dialog.

The **Welcome to Network Insights Advisor** dialog appears for the first installation.

What to do next

When the installation is complete, the application opens to **Welcome to Network Insights Advisor** dialog. Continue with the setup of the Cisco Network Insights Advisor application located in the Cisco NIA Initial Setup section of the next chapter.

Disable Cisco NIA Application on Cisco Application Services Engine

This section contains the steps required to disable a Cisco Network Insights Advisor application on the Cisco Application Services Engine .

Before you begin

Before you begin to disable Cisco Network Insights Advisor application, make sure you have administrator credentials for Cisco Network Insights Advisor application.

Step 1 Log in to the Cisco APIC GUI with admin privileges.

Step 2 Click the **Apps** tab on the top navigation bar.

Step 3 Click **Disable** on the top right corner of the Cisco NIA application dialog.

Step 4 Click **Yes** on the disable application dialog.

What to do next

You can re-enable the Cisco Network Insights Advisor application on the Cisco NIA application dialog.

Delete Cisco NIA Application on Cisco Application Services Engine

This section contains the steps required to delete a Cisco Network Insights Advisor application on the Cisco Application Services Engine .

Before you begin

- You must disable the Cisco NIA app before you delete the app on the Cisco Application Services Engine.
- You need administrator credentials for Cisco Network Insights Advisor application.

Step 1 Log in to the Cisco APIC GUI with admin privileges.

Step 2 Click the **Apps** tab on the top navigation bar.

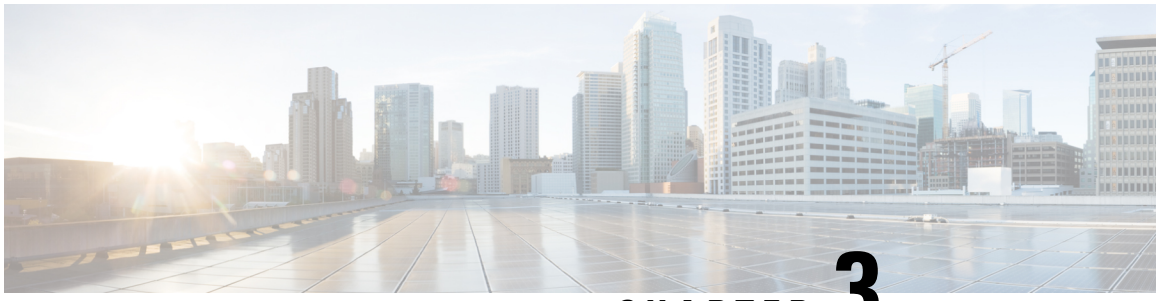
Step 3 Click **Delete** on the top right corner of the Cisco NIA application dialog.

Step 4 Click **Yes** on the delete application dialog.

The Cisco NIA application is removed.

What to do next

You can install the Cisco Network Insights Advisor application on Cisco Application Services Engine. See Installing Cisco NIA Application on Cisco Application Services Engine, on page 4 for details.



CHAPTER 3

Cisco Network Insights Advisor Setup and Settings

This chapter contains the following sections:

About Cisco Network Insights Advisor

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 you 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 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.

The Cisco NIA app consists of the following components:

- Advisories
    - Software Upgrades
    - Cisco Recommendations
    - Reports

- Notices
  - EoL/EoS Dates
  - Field Notices
- Issues
  - Anomalies
  - Bug/PSIRT Reports
- Devices
- TAC Assist
  - Log Collection
  - Technical Support to Cloud
  - Enhanced TAC Assist
- Jobs
  - Fabric

Cisco NIA Initial Setup

This section contains the steps required to set up the Cisco NIA app in the Cisco APIC. This set up is required for the 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**.

An **App Setup** dialog appears.

The Cisco NIA app is enabled with Cisco APIC.

Step 2 Uncheck **Help Cisco improve its products** to stop sending the CX telemetry data to the cloud.

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
	**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. • **Connected / Claimed**: The Cisco NIA application is connected to the Cisco Intersight cloud and the device connector has been claimed by the customer. For more information, see Setting Up the Intersight Device Connector below.
	**Inbox**: View messages from Cisco regarding software upgrades or other relevant information about devices on your network.
	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. • **Rerun Setup**—Allows you to edit the Data Collection Setup by adding or removing the fabric.
	Displays the online help for Cisco NIA application.

Setting Up the Device Connector

This secion describes setting up the device connector for Cisco NIA on Cisco APIC.

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.

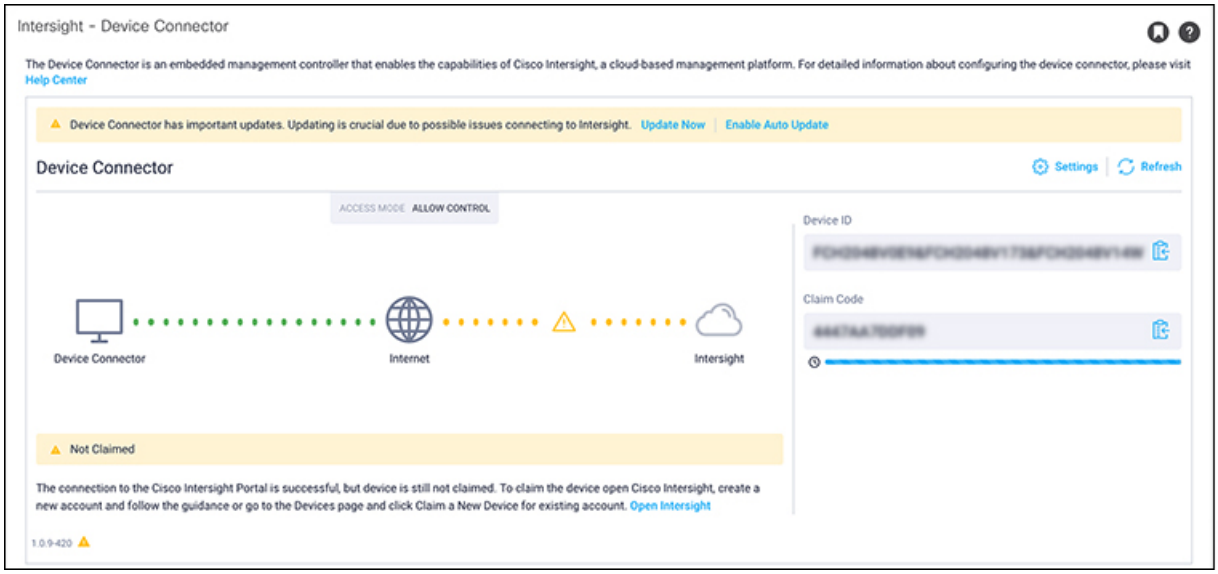
When an Intersight-enabled device or application starts, the Device Connector starts at boot by default, and attempts to connect to the cloud service. If the **Auto Update** option is enabled, the Device Connector is automatically updated to the latest version through a refresh by the Intersight service when you connect to Intersight. For more information on the **Auto Update** option, see Configuring the Intersight Device Connector, on page 10.

Note The Cisco NIA app supports only one active Device Connector at a time, either on Cisco APIC or on Cisco Application Services Engine. If you want to switch to use Device Connector on Cisco Application Services Engine, you must first turn off the Device Connector on Cisco APIC.

Configuring the Intersight Device Connector

Step 1 In the Cisco APIC GUI, click **System** > **System Settings** > **Intersight**.

The Device Connector work pane appears:



- If you see green dotted lines connecting **Internet** to **Intersight** in the **Device Connector** graphic, and the text **Claimed** underneath the graphic, then your Intersight Device Connector is already configured and connected to the Intersight service, and the device is claimed.
- If you see yellow dotted lines and a caution icon connecting **Internet** to **Intersight** in the **Device Connector** graphic, and the text **Not Claimed** underneath the graphic, then your Intersight Device Connector is not yet configured and connected to the Intersight service, and the device is not yet claimed. Follow these procedures to configure the Intersight Device Connector and connect to the Intersight service, and claim the device.

Note If you see red dotted lines connecting **Internet** to **Intersight** in the **Device Connector** graphic, that means that you configured the proxy incorrectly in Step 6.

Step 2 Determine if you would like to update the software at this time, if there is a new Device Connector software version available.

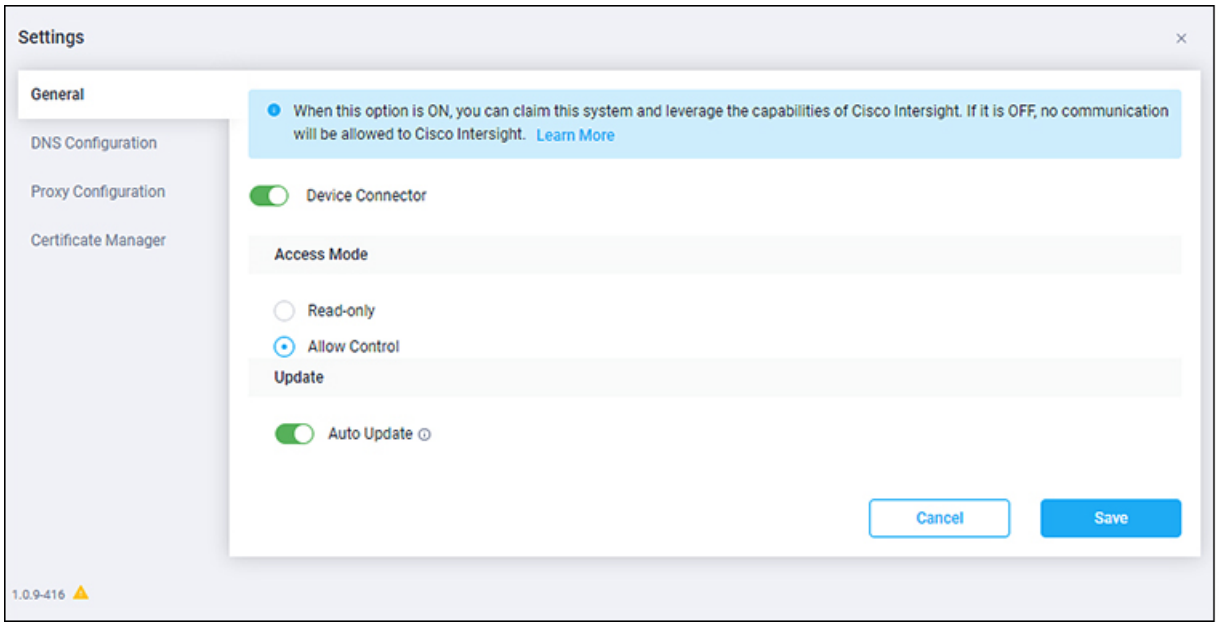
If there is a new Device Connector software version available and you do not have the **Auto Update** option enabled, you will see a message towards the top of the screen, telling you that Device Connector has important updates available.

- If you do not want to update the software at this time, go to Step 3 to begin configuring the Intersight Device Connector.

- If you would like to update the software at this time, click one of the two links in the yellow bar towards the top of the page, depending on how you would like to update the software:
  - **Update Now**: Click this link to update the Device Connector software immediately.
  - **Enable Auto Update**: Click this link to go to the **General** page, where you can toggle the **Auto Update** field to ON, which allows the system to automatically update the Device Connector software. See Step 4c for more information.

Step 3 Locate the **Settings** link to the right of the **Device Connector** heading and click the **Settings** link.

The **Settings** page appears, with the **General** tab selected by default.



Step 4 In the **General** page, configure the following settings.

a) In the **Device Connector** field, determine if you want to allow communication between the device and Cisco Intersight.

The **Device Connector** option (enabled by default) enables you to claim the device and leverage the capabilities of Intersight. If it is turned OFF, no communication will be allowed to Intersight.

b) In the **Access Mode** field, determine if you want to allow Intersight the capability to make changes to this device.

Access Mode enables you to allow full read/write operations from the cloud or restrict changes made to this device from Intersight.

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

c) In the **Auto Update** field, determine if you want to allow the system to automatically update the software.

- Toggle ON to allow the system to automatically update the software.
- Toggle OFF so that you manually update the software when necessary. You will be asked to manually update the software when new releases become available in this case.

Note If the **Auto Update** option is turned OFF, that may periodically cause the Device Connector to be out-of-date, which could affect the ability of the Device Connector to connect to Intersight.

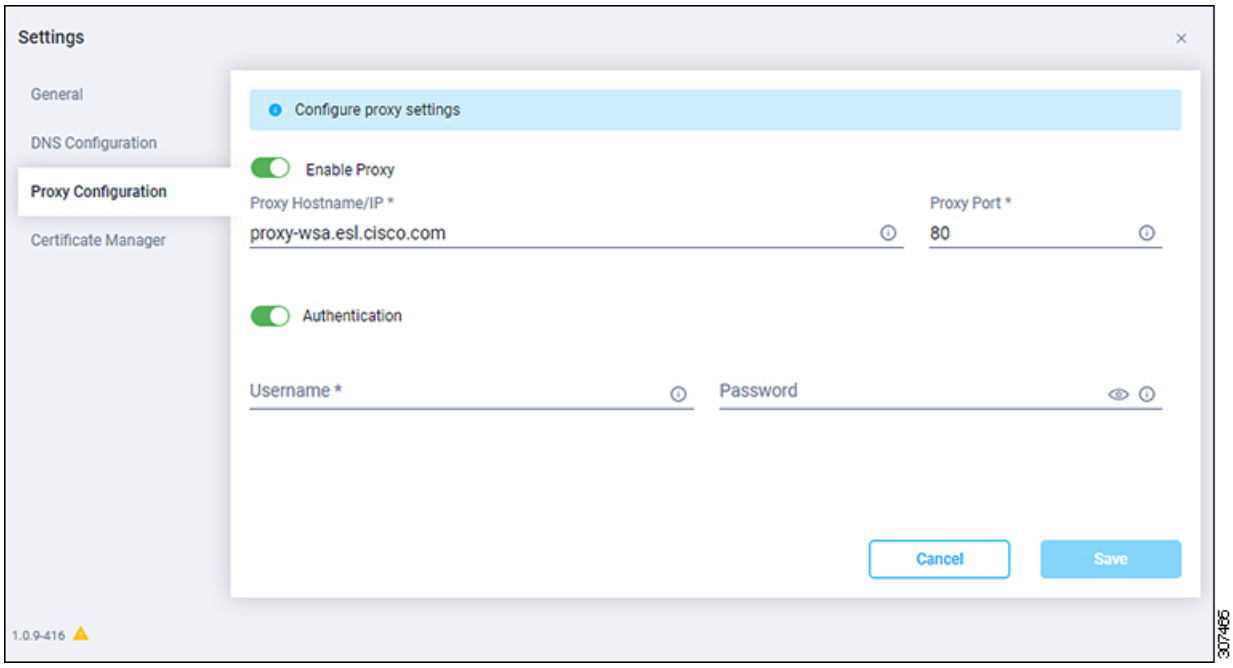
Step 5 When you have completed the configurations in the **General** page, click **Save**.

The **Intersight - Device Connector** overview pages appears again. At this point, you can make or verify several configure settings for the Intersight Device Connnector:

- If you want to configure the proxy that the Device Connector will use to communicate with the Intersight cloud, go to Step 6.
- If you want to manage certificates with the Device Connector, go to Step 9.

Step 6 If you want to configure the proxy that the Device Connector will use to communicate with the Intersight cloud, click **Settings**, then click **Proxy Configuration**.

The **Proxy Configuration** page appears.



Step 7 In the **Proxy Configuration** page, configure the following settings.

In this page, you can configure the proxy that the Device Connector will use to communicate with the Intersight cloud.

Note The Device Connector does not mandate the format of the login credentials; they are passed as-is to the configured HTTP proxy server. Whether or not the username must be qualified with a domain name depends on the configuration of the HTTP proxy server.

a) In the **Enable Proxy** field, toggle the option to ON to configure the proxy settings.

b) In the **Proxy Hostname/IP** field, enter a Proxy Hostname and IP Address.
c) In the **Proxy Port** field, enter a Proxy Port.
d) In the **Authentication** field, toggle the **Authentication** option to ON to configure the proxy authentication settings, then enter a Proxy Username and Password for authentication.

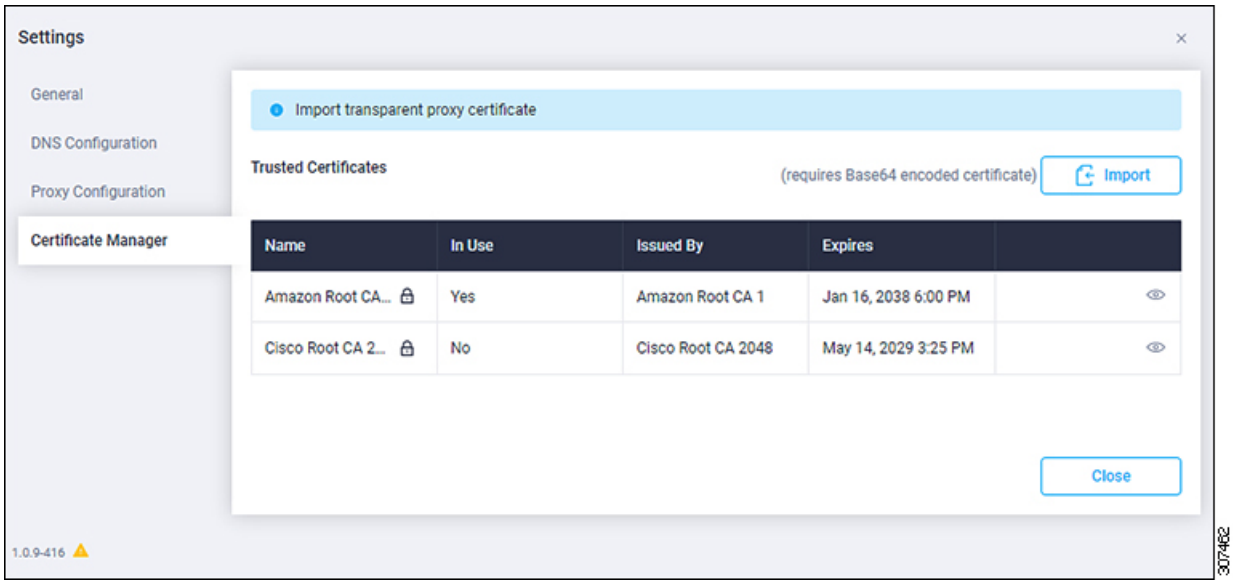
Step 8 When you have completed the configurations in the **Proxy Configuration** page, click **Save**.

The **Intersight - Device Connector** overview pages appears again.

If you want to make manage certificates with the Device Connector, go to the next step.

Step 9 If you want to manage certificates with the Device Connector, click **Settings**, then click **Certificate Manager**.

The **Certificate Manager** page appears.



Step 10 In the **Certificate Manager** page, configure the following settings.

By default, the device connector trusts only the built-in svc.ucs-connect.com certificate. If the device connector establishes a TLS connection and a server sends a certificate that does not match the built-in svc.ucs-connect.com certificate, the device connector terminates TLS connections because it cannot determine if the server is a trusted device or not.

Click **Import** to import a CA signed certificate. The imported certificates must be in the *.pem (base64 encoded) format. After a certificate is successfully imported, it is listed in the list of Trusted Certificates and if the certificate is correct, it is shown in the In-Use column.

View these details for a list of certificates that are used to connect to svc.ucs-connect.com (intersight.com):

- **Name**—Common name of the CA certificate.
- **In Use**—Whether the certificate in the trust store was used to successfully verify the remote server.
- **Issued By**—The issuing authority for the certificate.
- **Expires**—The expiry date of the certificate.

Delete a certificate from the list of Trusted certificates. However, you cannot delete bundled certificates (root+intermediate certificates) from the list. The lock icon represents the Bundled certificates.

Step 11 When you have completed the configurations in the **Certificate Manager** page, click **Close**.

You can claim the device using the instructions provided in Claiming a Device, on page 14.

Claiming a Device

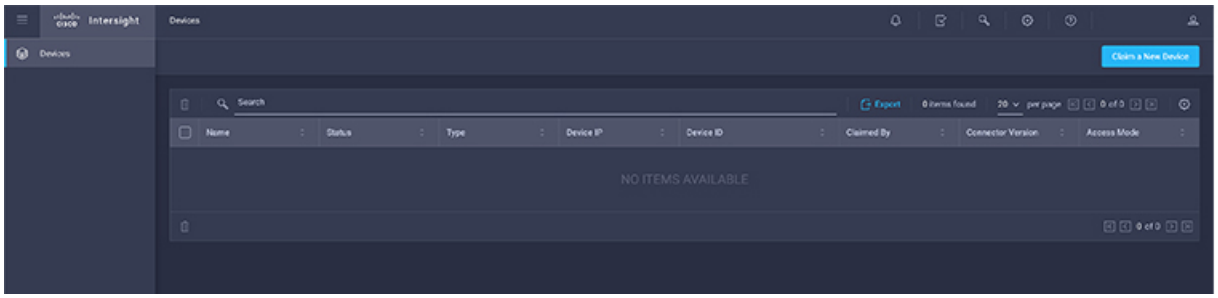
Before you begin

Configure the Intersight Device Connector information from the Cisco APIC site using the instructions provided in Configuring the Intersight Device Connector, on page 10.

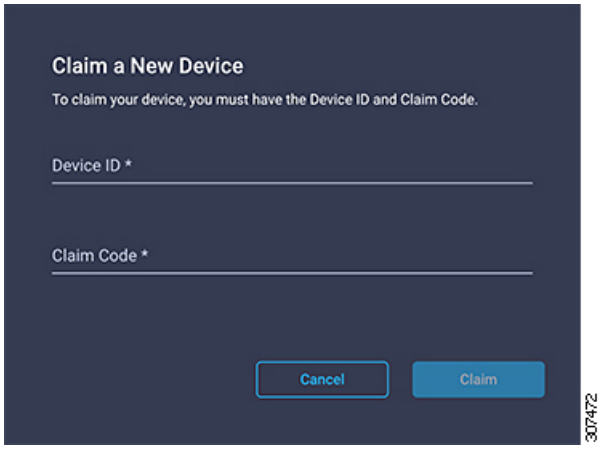
Step 1 Log into the Cisco Intersight cloud site:

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 APIC 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**.

Step 4 Copy the **Device ID** and **Claim Code** from the Cisco APIC site and paste them into the proper fields in the **Claim a New Device** page in the Intersight cloud site.

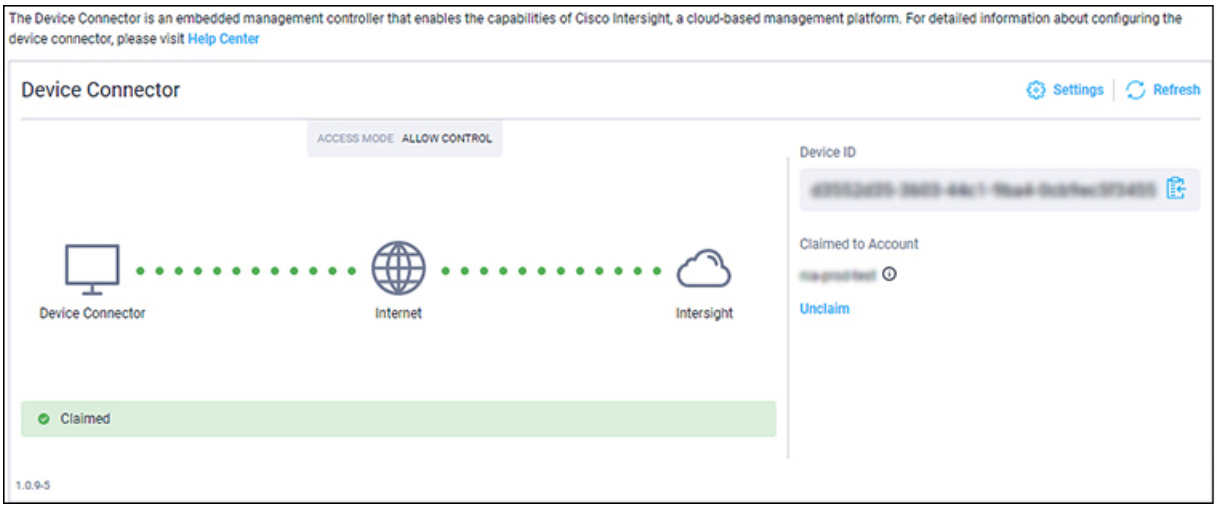
Click on the clipboard next to the fields in the Cisco APIC site to copy the field information into the clipboard.

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 APIC system, with Connected shown in the Status column.

Step 6 Go back to the **Intersight - Device Connector** page in the Cisco APIC 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.

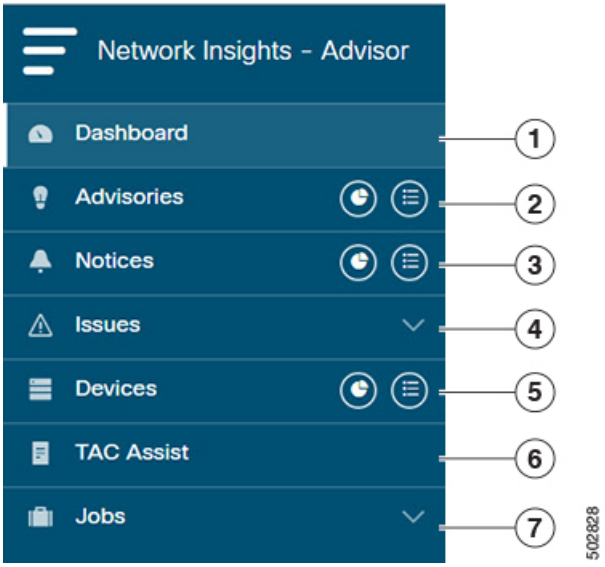
If you decide to unclaim this device for some reason, locate the **Unclaim** link in the **Intersight - Device Connector** page and click that link.

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, devices, and 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, hardware and software bugs and Product Security Incident Response Team (PSIRT) alerts applicable to your network.

5 Devices: Sorts devices by device name, serial number, IP address, version, and platform.

6 TAC Assist: Collects logs for specified devices that can be attached to service requests using the Cisco Intersight Cloud.

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

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

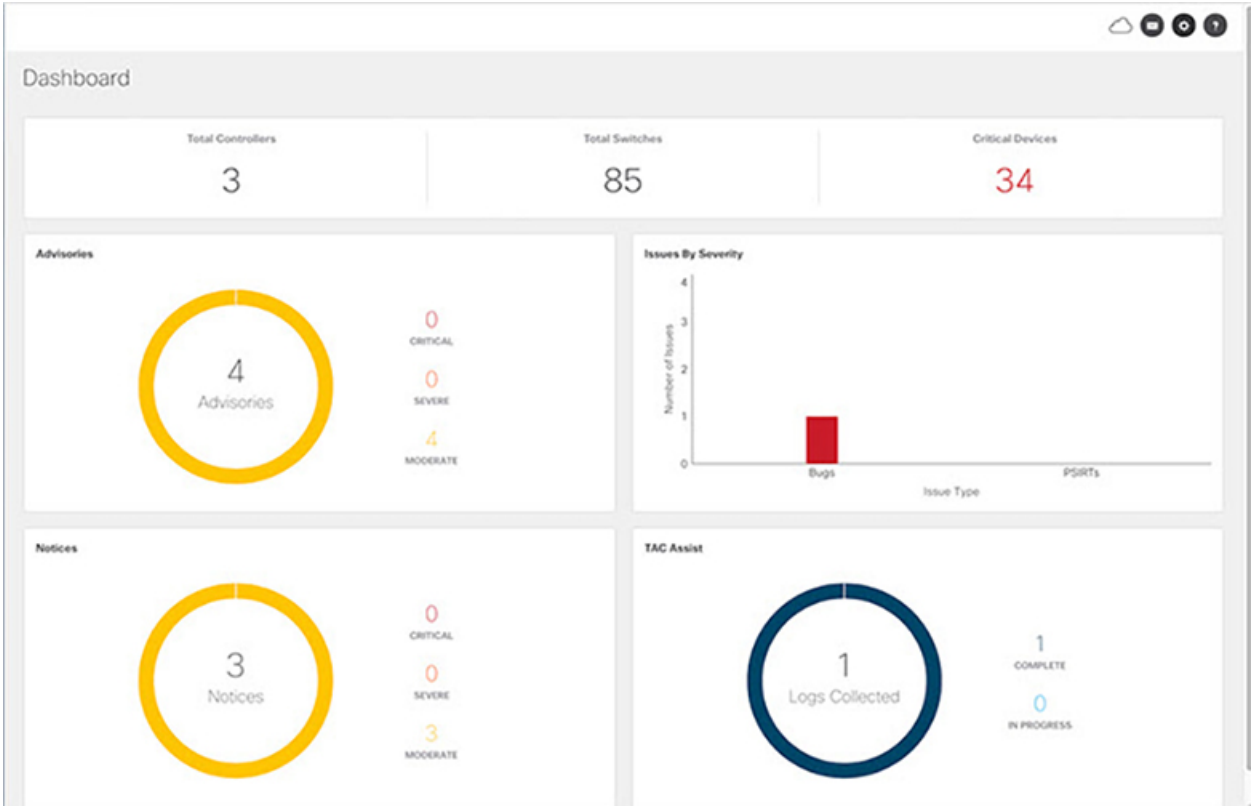
2 Browse View icon: Provides a detailed view of the alert(s) and access to more granular detail.

3 Configure icon: Displays the list of currently scheduled jobs and allows for the configuration of bug scanner and compliance check.

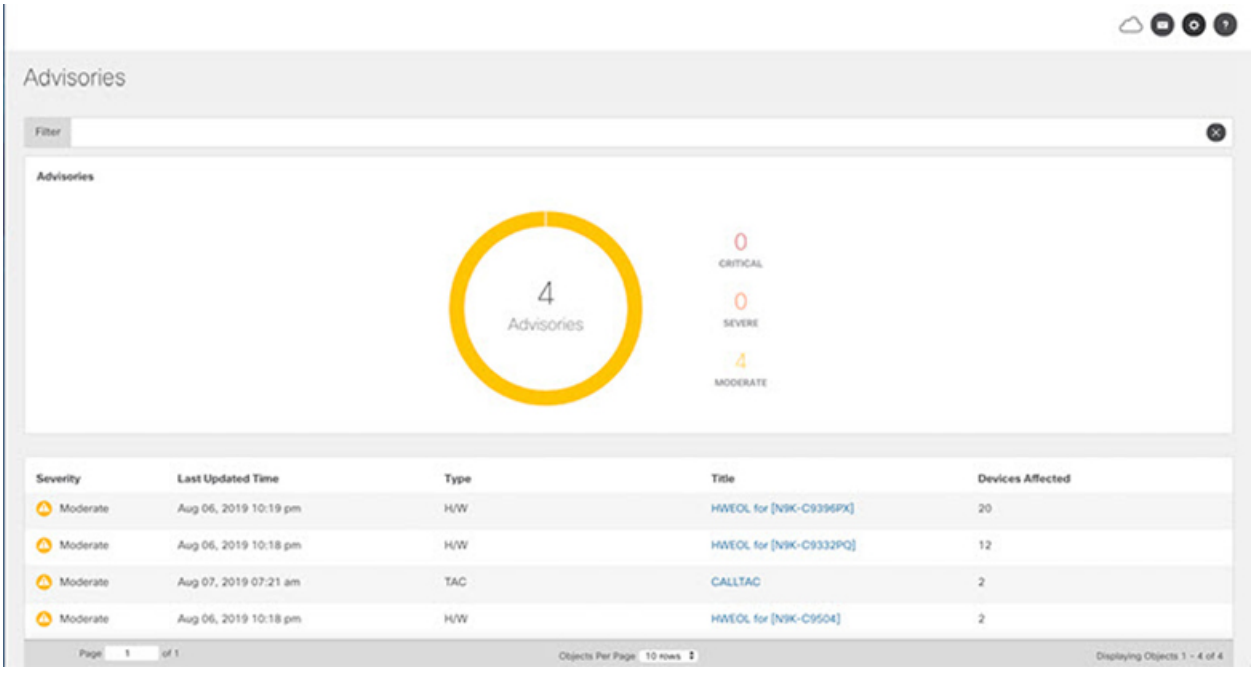
Work Pane

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

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 from which browse window the details work pane was initiated.
- Notices: Includes notices affecting devices in your network.
- Devices Affected: Includes 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.

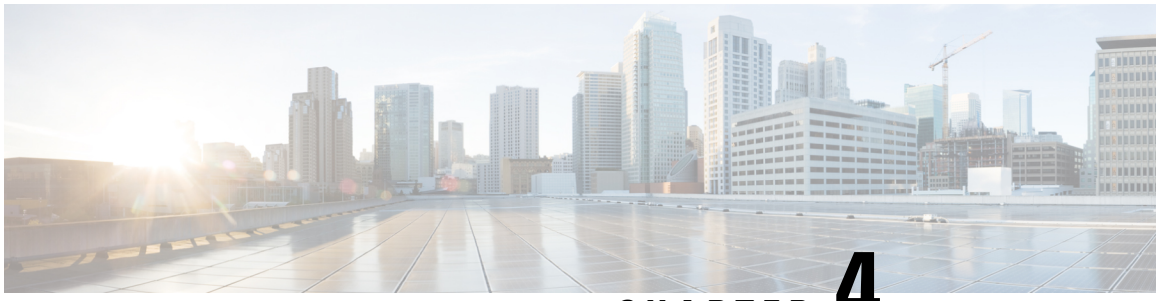
The **Log Collection** section displays the new job triggered for TAC Assist. The **Job Details** page lists the TAC Assist logs.

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 to 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.



CHAPTER 4

Using Cisco Network Insights Advisor

This chapter contains the following sections:

Using the Cisco Network Insights Advisor Application

Each Cisco Application Centric Infrastructure (Cisco ACI) switch 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, TAC Assist logs applicable to your network, schedule and configure bug scan, and compliance check jobs.

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

Property	Description
Issues By Severity	Displays the total number of issues (anomalies, bugs, and PSIRTs) delivered for software and hardware in your network.
Notices	Displays the total number of notices delivered for devices in your network.
TAC Assist	Displays the total number of TAC assist logs currently being collected or finished being collected.
Jobs	Provides access to configure and schedule bug scan and compliance check 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
- CALL TAC
- Advisory Report
- Software Upgrade Path

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 a specific compliance.
  - TAC - Returns matches for CALL TAC advisories.

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

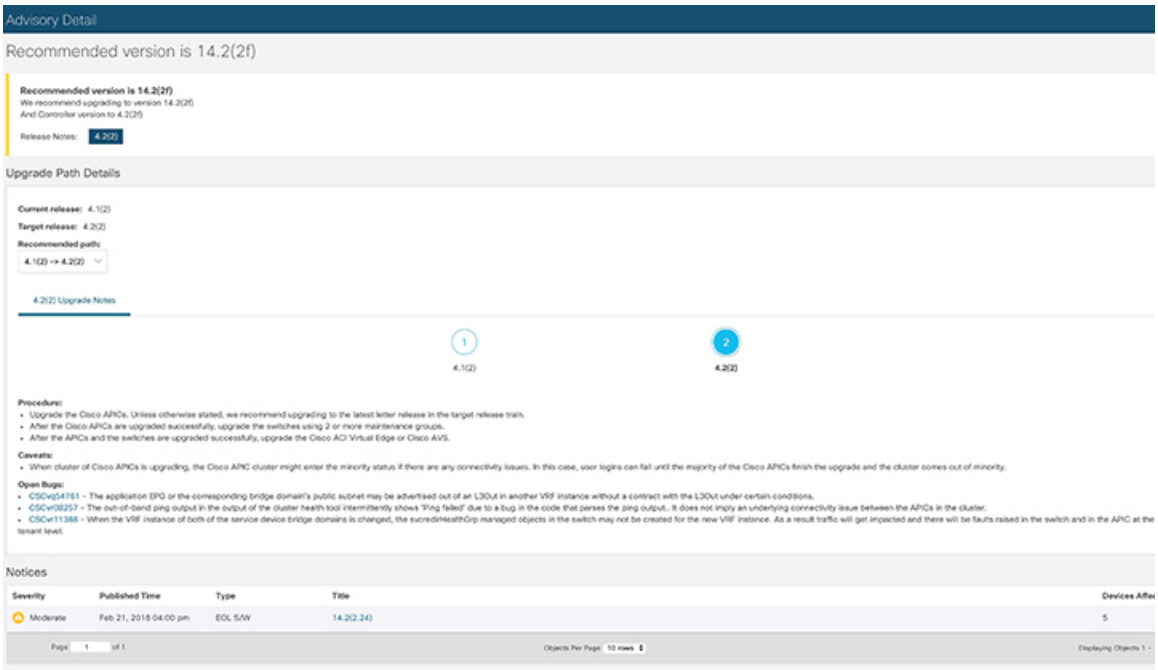
Property	Description
Advisories List	Displays a list of all advisories or only for the filtered severity or type. Column labels are: • Severity • Last Updated Time • Type • Title: Click the link in the **Title** column to view details about the advisory. **Note** **CALLTAC**: The Call TAC advisory encompasses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

Software Upgrade Path

When upgrading to a recommended software version, Cisco NIA app displays the procedure, caveats, and open defects for versions in the upgrade path.

There could be multiple paths to reach from current release to recommended release. You can choose the path in the **Recommended path** dropdown from the **Upgrade Path Details** page.

See the release notes for Cisco NIA app for recommended upgrade path to the recommended release.



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

Browse Notices

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

Filters

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

- Operators - display notices using an operator. Valid operators are:

    - = = - display notices with an exact match.

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

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

Issues Dashboard

Issues is divided into these components:

- Anomalies - Displays the number of Anomalies (internal Fabric failures) and their severity level detected in the fabric nodes.
- Bugs - Known bugs that are automated and have show tech with matching signatures
- PSIRTs - Product Security Incident Response Team notices

Anomalies Dashboard

The main dashboard displays the anomalies detected in the fabric nodes.

Property	Description
Anomaly Severity by Devices	Displays the number of Anomalies (internal Fabric failures) and their severity level. Clicking on the area shows detail fault information, such as **Devices Affected**, **Severity** and **Anomaly Score**.
Anomalies Affecting	Displays the number of anomalies by their type. Anomaly types include: • Versions • Platforms

Browse Anomalies

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

Filters

You can refine the displayed anomalies 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 severity's 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:
  - Control Plane - Returns matches for compliance check anomalies.
  - Management Plane - Returns matches for compliance check anomalies.
  - Data Palne - Returnd matches for compliance check anomalies.
  - Traffic Check - Returns matches for compliance check anomalies.
  - Forwarding Check - Returns matches for compliance check anomalies.
  - State Validator - Returns matches for compliance check anomalies.

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.
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 are past the **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** link for more details.
Device by (chart)	Display different versions of software and type of platforms detected.
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

Issue	Critical (Red)	Severe/Moderate/Low (Amber)	None (Green)
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 the 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 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 Intersight cloud.

Before you begin

Before you upload the collected logs to cloud, make sure the fabric is conneced to Cisco Intersight cloud. See Configuring the Intersight Device Connector, on page 10 for details.

Step 1 Click **TAC Assist** from the Cisco APIC navigation pane.

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

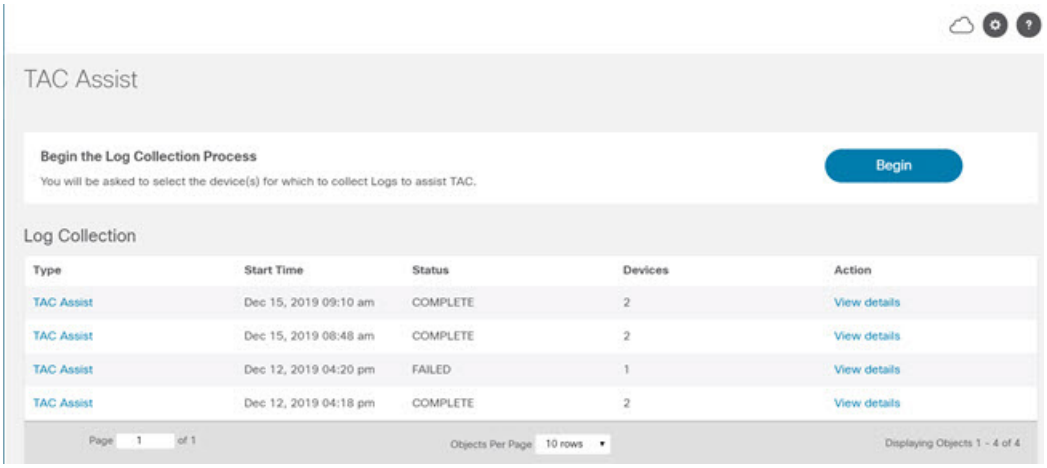
The Collect Logs dialog appears.

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.

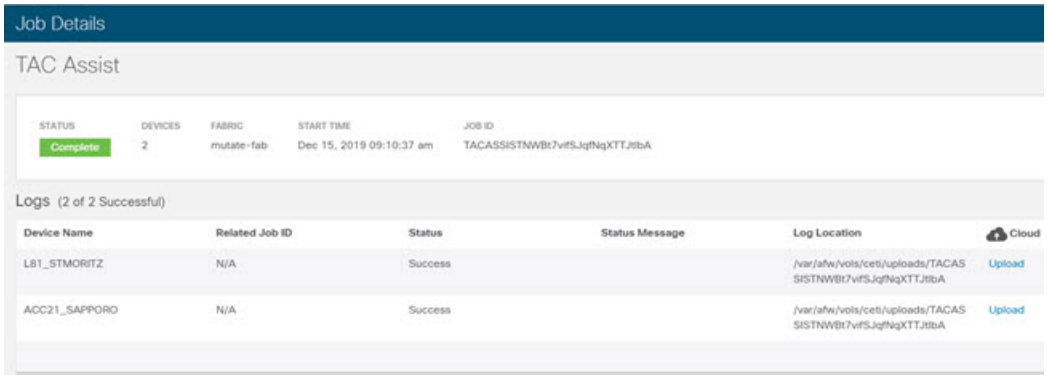
Step 4 From the **Collect Logs** page check the checkbox next to the device for which you want to collect logs. If you want to choose all of the devices in the list, check the checkbox next to the **Device Name** column.

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



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.



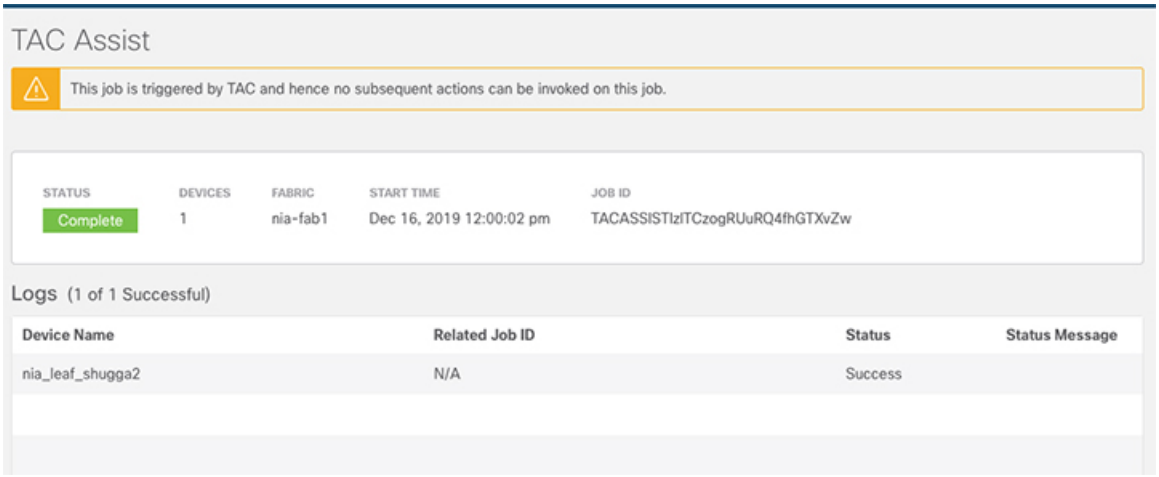
Step 6 Click **Upload** to upload the collected logs to Cisco Intersight cloud.

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 and 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.



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.

Fabric

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

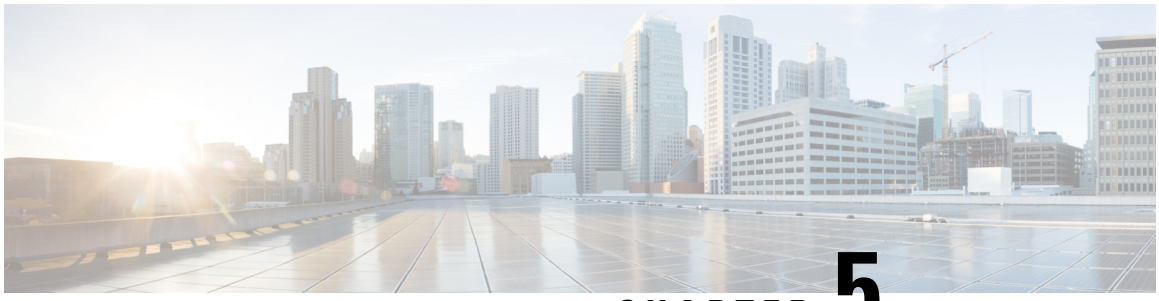
3. Click the browse view icon on the left navigation pane to view the scheduled jobs for the selected fabric and time range from the **Fabric Job List** page.

   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 the anomaly details.



CHAPTER 5

Troubleshooting Cisco NIA Application

This chapter contains the following sections:

Debugging Cisco NIA Application

Cisco NIA Application Start

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 for complete loading. For any errors, take screenshots before and after reproducing an issue.
- Take a screenshot of full network capture saved as HAR from you 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 successful.
- If the API call failed, view Active Data micro-service logs to check for any errors thrown in the micro-service. Collect Active Data micro-service logs for furthur 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

From your browser tools page, check if POST to *upgradepath* endpoint is successful and input or output data is as expected.

The following are the examples for *upgradepath*.

```
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"
```

Cisco APIC

```
time="2020-01-22 07:43:59.579" level=info msg="new AdvMap=s18sd3903s406sdssdbc-UPG-admin"
file="upgradepath:204"
time="2020-01-22 07:43:59.579" level=info msg="Starting issumatrix call aci 4.0(1) 4.2(3)"
 file="upgradepath:277"
time="2020-01-22 07:43:59.579" level=info msg="Res output:[4.0(1) 4.2(1) 4.2(3)]"
file="upgradepath:297"
time="2020-01-22 07:43:59.579" level=info msg="Init s18sd3903s406sdssdbc-UPG-admin{4.0(1)
4.2(1)}" file="upgradepath:216"
time="2020-01-22 07:43:59.579" level=info msg="Bugs output:map[4.2(1):0xc0004e2720
4.2(3):0xc0004e2780]" file="upgradepath:359"
time="2020-01-22 07:43:59.579" level=info msg="Sending POST response" file="upgradepath:258"
```

Notices

To debug notices:

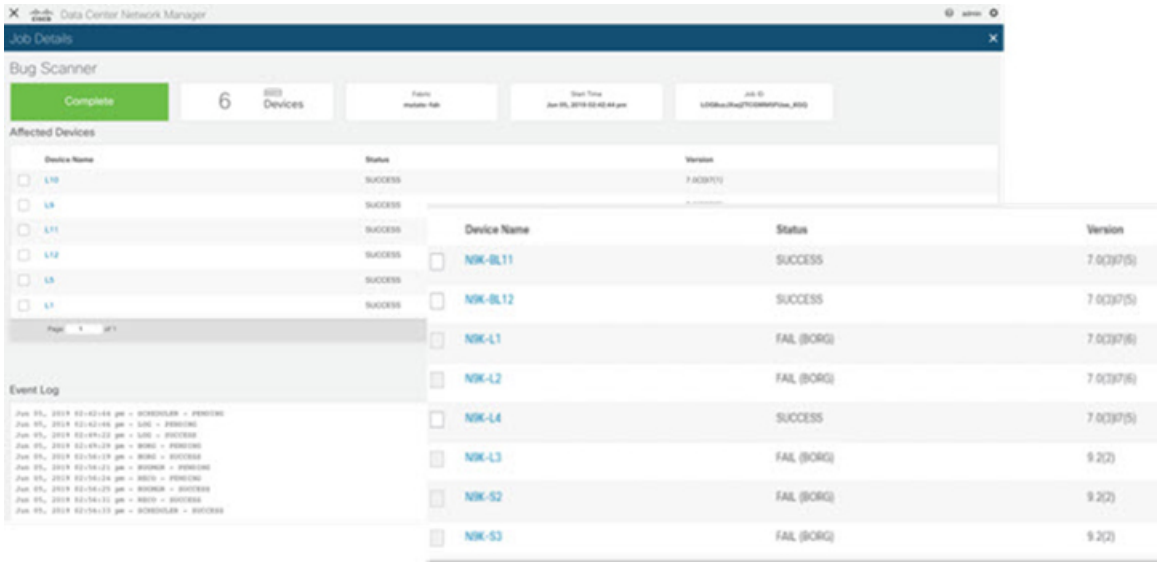
- Connect to the Intersight cloud and claim the Device Connector atleast once.
- Make sure that all the devices are available in the network.

- 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.
- In the collected logs, check all the paths are reported for the logs.
- Collect the Cisco NIA tech-support in case of a failure.

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"}
```

Cisco NIA Log Paths

Collect the logs to debug:

- Cisco APIC logs:
  - Within the container.

    ```
    /home/app/log/<microservice>
    ```
  - On each compute.

    ```
    /data2/logs/Cisco_NIA
    ```
  - Docker logs.

    ```
    /nomad logs –f <job_id>
    ```

- Collect Cisco NIA logs.

  Use tech-support policy for Cisco NIA application.

Troubleshooting Cisco NIA Application on Cisco APIC

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.	• 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.	• 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 summerizes 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 dispalyed in the recommended release or in the upgrade path.	• 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.