



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

# Table of Contents

The Cisco Network Insights Advisor Application for Cisco APIC User Guide .....	3
New and Changed Information .....	4
Cisco Network Insights Advisor Installation .....	6
About Cisco Network Insights Advisor on Cisco Application Services Engine .....	6
Downloading Cisco NIA Application from the Cisco App Center .....	6
Add a Site on Cisco Application Services Engine Using GUI .....	6
Installing Cisco NIA Application on Cisco Application Services Engine .....	7
Disable Cisco NIA Application on Cisco Application Services Engine .....	8
Delete Cisco NIA Application on Cisco Application Services Engine .....	8
Cisco Network Insights Advisor Setup and Settings .....	9
About Cisco Network Insights Advisor .....	9
Guidelines and Limitations .....	10
Cisco NIA Initial Setup .....	10
Cisco NIA Settings .....	11
Setting Up the Intersight Device Connector .....	13
About Device Connector .....	13
Configuring the Intersight Device Connector .....	13
Claiming a Device .....	17
Navigating Cisco NIA .....	20
Navigation Pane .....	20
Work Pane .....	21
Cisco Network Insights Advisor Dashboard .....	24
Main Dashboard .....	24
Advisories Dashboard .....	25
Issues Dashboard .....	28
Devices Dashboard .....	32
TAC Assist Dashboard .....	34
User Initiated Upload to Cisco Intersight Cloud .....	34
TAC Initiated Pull from Cisco Intersight Cloud .....	36
Jobs Dashboard .....	36
Fabric .....	37
Troubleshooting Cisco NIA Application on Cisco APIC .....	39
Cisco NIA Application Start .....	39
Cisco NIA Application User Interface .....	39
Statistics Telemetry .....	39
Advisory Report .....	40
Debugging Software Upgrade Path .....	40
Notices .....	41

Bugs and PSIRTs .....	41
TAC Assist On-demand .....	41
Enhanced TAC Assist - User Initiated Upload to Cisco Intersight Cloud .....	42
Cisco NIA Log Paths .....	43
Device Reachability and Authentication .....	44
Enhanced TAC Assist - TAC Initiated Pull from Cisco Intersight Cloud .....	44
Software Upgrade Path .....	45

First Published: 2020-10-02

**Americas Headquarters**

Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA

<http://www.cisco.com>

Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 527-0883

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

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

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

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

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

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

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

© 2017-2020 Cisco Systems, Inc. All rights reserved.

# **The Cisco Network Insights Advisor Application for Cisco APIC User Guide**

# New and Changed Information

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

*Table 1. New Features and Changed Behavior in the Cisco Network Insights Advisor app for Cisco APIC Release 2.1.x*

<b>Feature</b>	<b>Description</b>	<b>Release</b>	<b>Where Documented</b>
Bug fixes	This release includes bug fixes.	2.1.2	Cisco NIA for Cisco APIC Release Notes 2.1.2
Add Site	Add a site on Cisco Application Services Engine. Cisco NIA app installed on Cisco Application Services Engine can access the added sites.	2.1.1	<a href="#">Add a Site on Cisco Application Services Engine Using GUI</a>
Multiple Site support	The multiple site configuration enables you to onboard the site from the list of available sites.	2.1.1	<a href="#">Cisco NIA Multiple Site Setup</a>
UI enhancements	Browse dashboards for Advisories, Bugs, PSIRTs, and Notices summarize additional details of the device, generates detailed view reports, and displays the anomaly score for the devices affected.	2.1.1	<a href="#">Browse Advisories, Issues Dashboard, Browse Devices</a>
TAC Assist enhancements	Cisco NIA app uses the device connectivity issue notifier on Cisco APIC to communicate with the devices, which identifies the unhealthy node interactions on the device. TAC assist does not collect logs for these nodes.	2.1.1	<a href="#">TAC Assist Dashboard</a>

<b>Feature</b>	<b>Description</b>	<b>Release</b>	<b>Where Documented</b>
Pre Bug Scan PSIRTs	PSIRTs for the devices discovered by Cisco NIA are now shown without having to run a bug scan. If metadata is updated from cloud, a bug scan should be run to show updated PSIRTs that are applicable to the devices.	2.1.1	<a href="#">PSIRTs Dashboard</a>




# Cisco Network Insights Advisor Installation

## 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.

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.

2. Search for Cisco Network Insights Advisor application on the search bar.
3. Select the Cisco Network Insights Advisor application you want to download and click **Download** for that app to begin the process of downloading the app to your local machine.
4. Review the license agreement and, if OK, click **Agree and download**.

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

## Add a Site on Cisco Application Services Engine Using GUI

Use this procedure to add a site on to the Cisco Application Services Engine using GUI. Any apps installed on Cisco Application Services Engine can access the added sites.

### Before you begin

- You have installed and configured the Cisco Application Services Engine.
- You must have administrator credentials to install Cisco NIA application.

## Procedure

1. Log in to the Cisco Application Services Engine GUI with admin privileges.
2. Click **Infrastructure** > **Sites** on the left navigation pane.
3. Click **Actions** > **Add Site** from the far-right side.
4. On the **Add Site** page enter the following:
  - Site Name, Site ID, Controller IP, User Name, Password, Login Domain, and Inband EPG. Controller IP is a comma separated list of IP addresses to access the site.
5. Click **Submit**. This adds a site to the node. Any apps installed on Cisco Application Services Engine can access the added sites.
6. Continue with the installation of the Cisco Network Insights Advisor application on Cisco Application Services Engine using GUI.

## 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.

## Procedure

1. Log in to the Cisco APIC GUI with admin privileges.
2. Click **Admin** tab and then click **Downloads** from the top navigation bar.
3. Click **Service Engine** from the tabs on the far-right side. Then select **Upload File**. The *Add File to Service Engine* dialog appears.
4. In the **URL** enter the http address and click **Submit**. You can click the **Refresh** icon  on the far-right side of the Downloads work pane to check the upload status.
5. Once the *Status* is complete, 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.
6. Once the installation is complete, click **Enable** in the Cisco NIA application dialog.
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.

8. When the installation is complete, the application opens to the *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.

### Procedure

1. Log in to the Cisco APIC GUI with admin privileges.
2. Click the **Apps** tab on the top navigation bar.
3. Click **Disable** on the top right corner of the Cisco NIA application dialog.
4. Click **Yes** on the disable application dialog. 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 NIA.
- You need administrator credentials for Cisco Network Insights Advisor application.

### Procedure

1. Log in to the Cisco APIC GUI with admin privileges.
2. Click the **Apps** tab on the top navigation bar.
3. Click **Delete** on the top right corner of the Cisco NIA application dialog.
4. Click **Yes** on the delete application dialog. The Cisco NIA application is removed.

# Cisco Network Insights Advisor Setup and Settings

## 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

## Guidelines and Limitations


- When the Device Connector is unclaimed from the on-premise GUI Cisco NIA application, the Device Connector must be unclaimed from Intersight for TAC Assist's connected TAC functionality to work.
- TAC Assist started from Cisco NIA application will not show up in Cisco NI Base and vice versa.

## 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.

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

A Setup dialog appears. The Cisco NIA app is enabled with Cisco APIC.

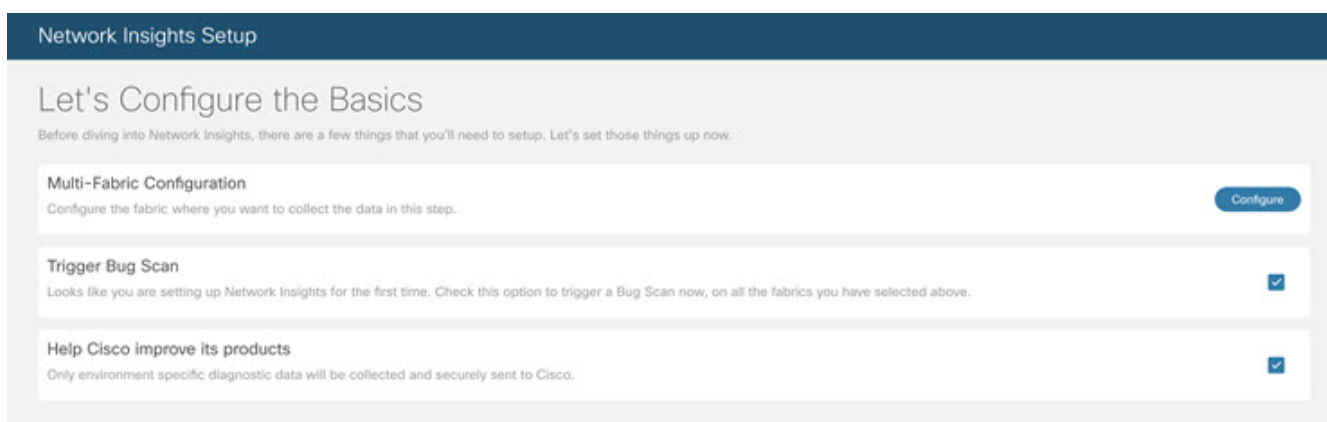
2. The **Network Insights Setup** page appears with the selected fabrics in the *Multi-Site Configuration*. Click **Edit configuration** to choose the site(s). You can return to the setup utility anytime by clicking the settings icon  and choose **Network Insights Setup**.

See [Cisco NIA Multiple Site Setup](#) for details.

3. Check the box to **Trigger Bug Scan**. Once this option is enabled in the first time setup, it does not appear in the rerun setup.
4. Check the box to **Help Cisco improve it's products**.

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

5. Click **Done**.



## Cisco NIA Multiple Site Setup

The multiple site configuration enables you to enable or onboard the site from the list of available sites on Cisco NIA. Click **Edit Configuration** for a list of sites, status, enable, and disable sites. The

site status is disabled by default.



The **Network Insights Setup - Multi-Site Configuration** page displays the list of sites.



1. Select the sites you want visible to the Cisco NIA app.
2. Click **OK**.

## 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
	<p><b>Device Connector Status:</b> 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"><li>• <b>Not Connected:</b> The Cisco NIA application is not connected to the Cisco Intersight Cloud.</li><li>• <b>Connected / Not Claimed:</b> The Cisco NIA application is connected to the Cisco Intersight Cloud but the device connector has not been claimed by the customer. Cisco NIA app collects telemetry data.</li><li>• <b>Connected / Claimed:</b> The Cisco NIA application is connected to the Cisco Intersight Cloud and the device connector has been claimed by the customer. Cisco NIA app uses TAC assist and metadata refresh in connected and claimed.</li></ul> <p>For more information, see <a href="#">Setting Up the Intersight Device Connector</a>.</p>
	<p><b>Inbox:</b> View messages from Cisco regarding software upgrades or other relevant information about devices on your network.</p>

Property	Description
	<p>Clicking on this icon invokes a list menu allowing you to make changes to the following:</p> <ul style="list-style-type: none"> <li>• <b>About Network Insights</b>—Displays an information dialog identifying the version number of the Cisco NIA application. Click <b>Update to Latest</b> to fetch the latest metadata published version. This requires that the using of the Cisco Intersight Device Connector is connected and claimed.</li> <li>• <b>Rerun Setup</b>—Allows you to edit the Data Collection Setup by adding or removing the fabric.</li> </ul>
	<p><b>User Guide</b>—The documentation for installation, configuration, and use of Cisco NIA application.</p>

# Setting Up the Intersight Device Connector

## About Device Connector

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

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

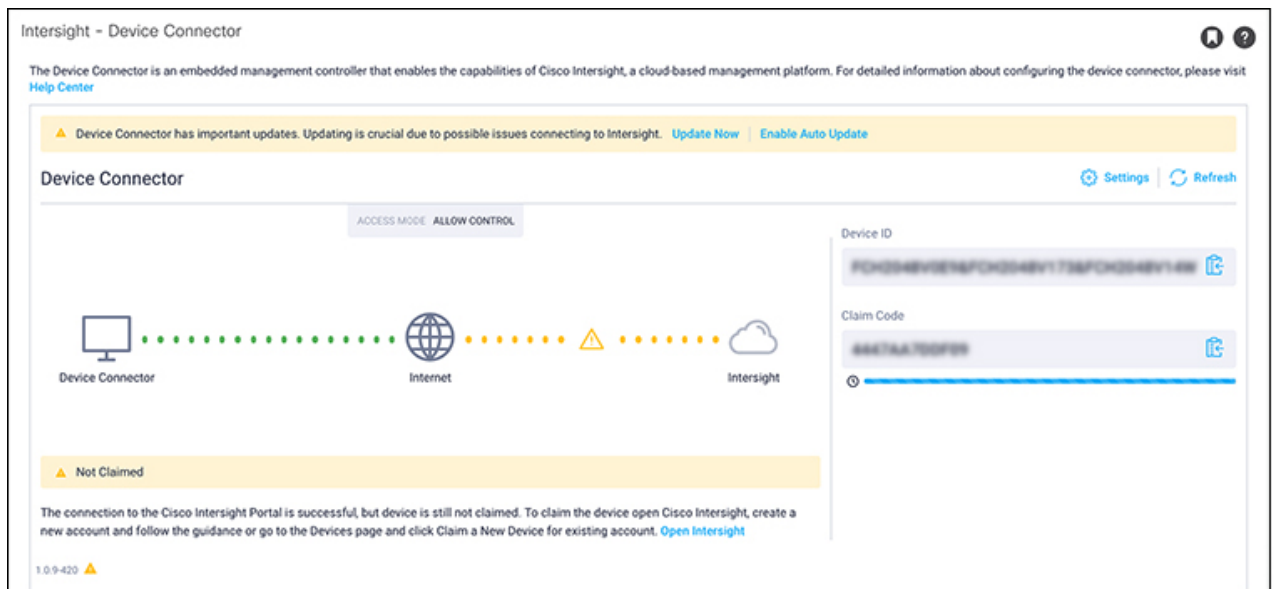


The Cisco NIA app supports only one active Device Connector at a time, either on Cisco APIC or on Cisco Application Services Engine. If you want to switch to use Device Connector on Cisco Application Services Engine, you must first turn off the Device Connector on Cisco APIC.

## Configuring the Intersight Device Connector

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.



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.

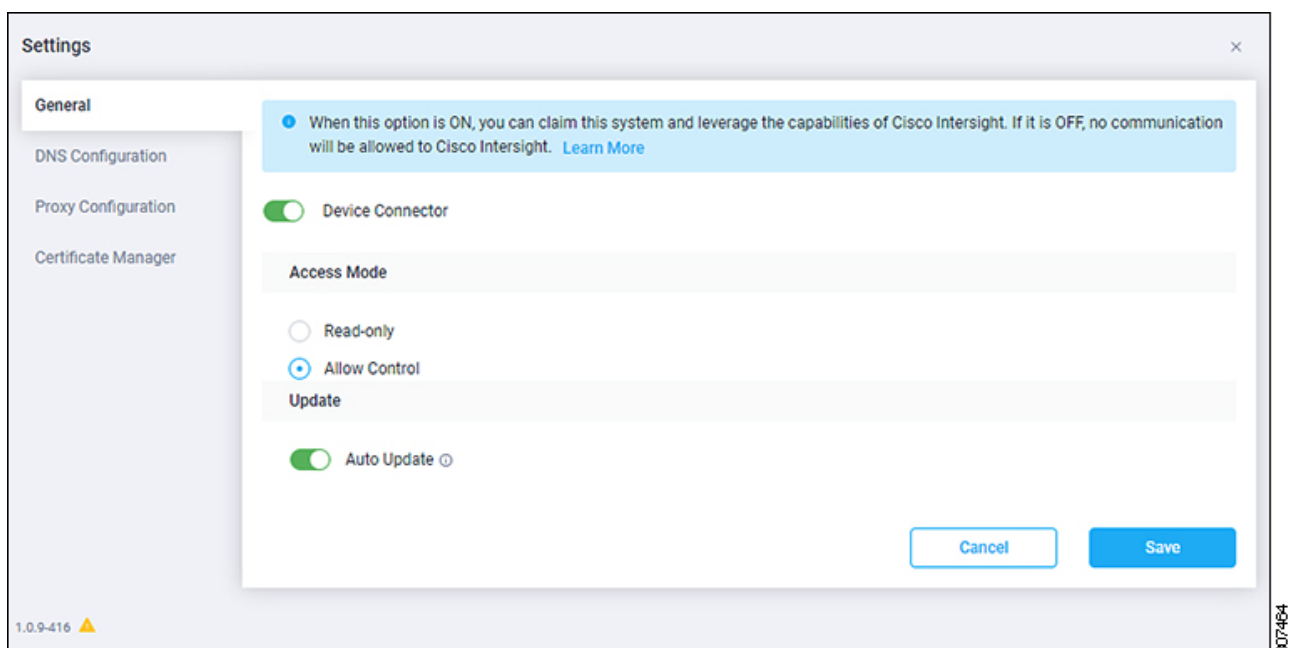
2. Determine if you would like to update the software at this time, if there is a new Device Connector software version available.

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.

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.



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.



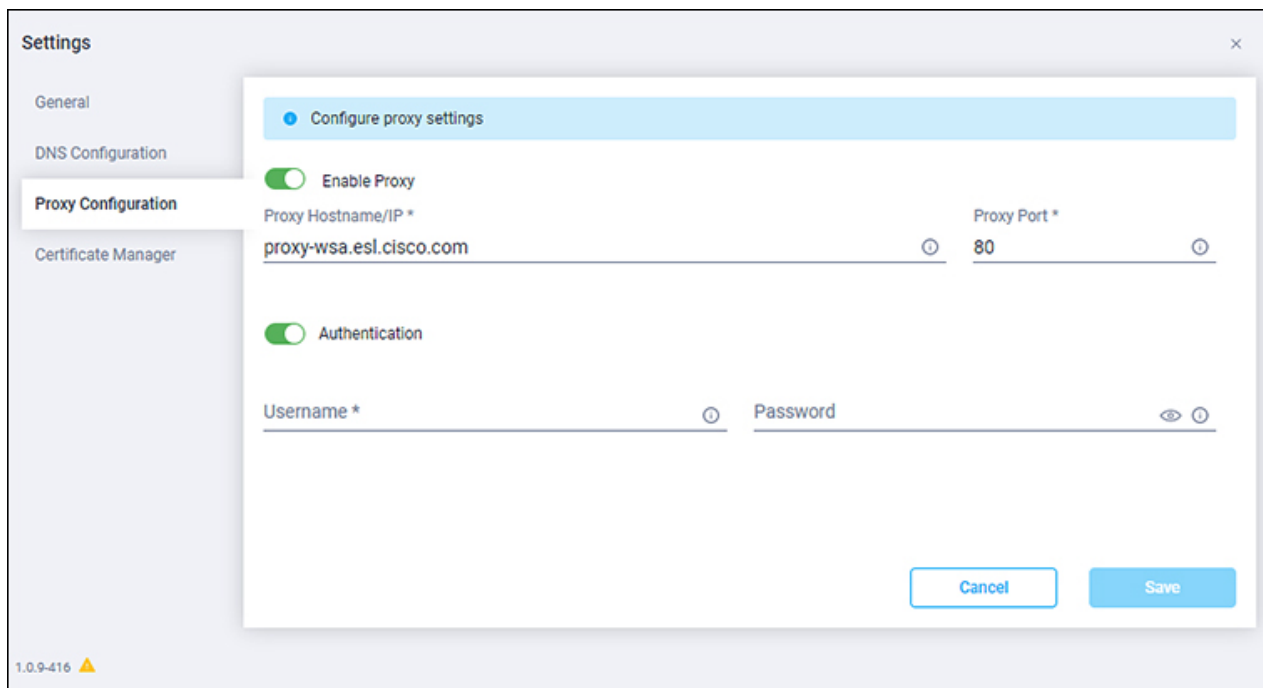
If the **Auto Update** option is turned OFF, that may periodically cause the Device Connector to be out-of-date, which could affect the ability of the Device Connector to connect to Intersight.

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

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

- 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.
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.



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.



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.

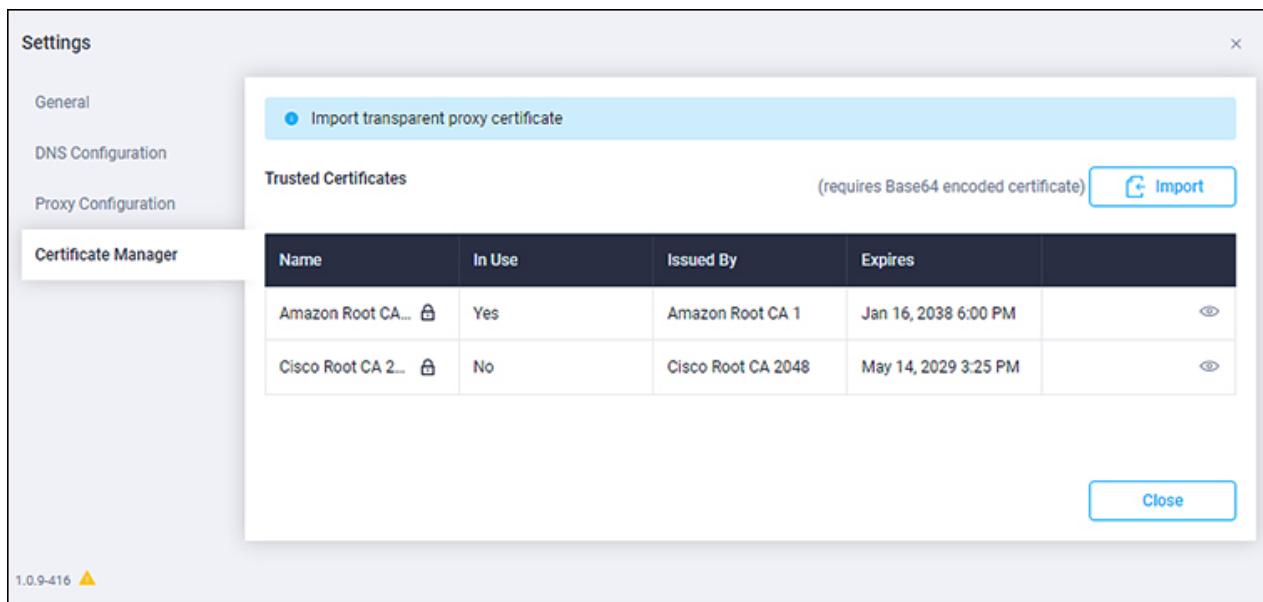
- a. In the **Enable Proxy** field, toggle the option to ON to configure the proxy settings.
  - b. In the **Proxy Hostname/IP** field, enter a Proxy Hostname and IP Address.
  - c. In the **Proxy Port** field, enter a Proxy Port.
  - d. In the **Authentication** field, toggle the **Authentication**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

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

The *Certificate Manager* page appears.



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.

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](#).

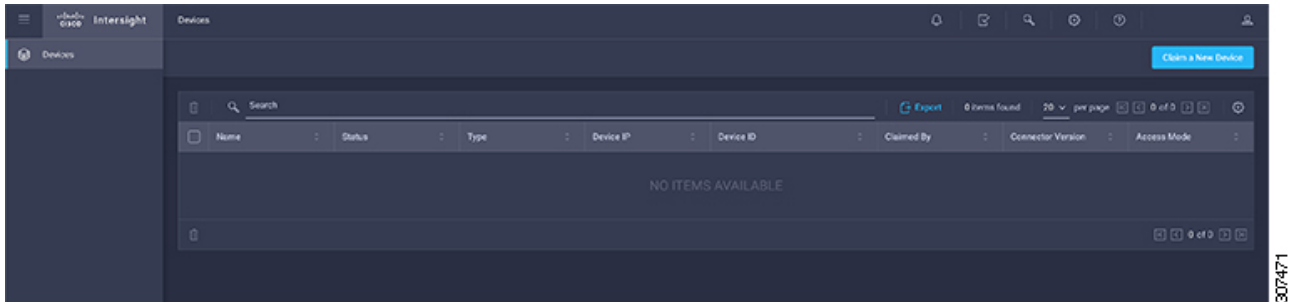
## Claiming a Device

## Before you begin

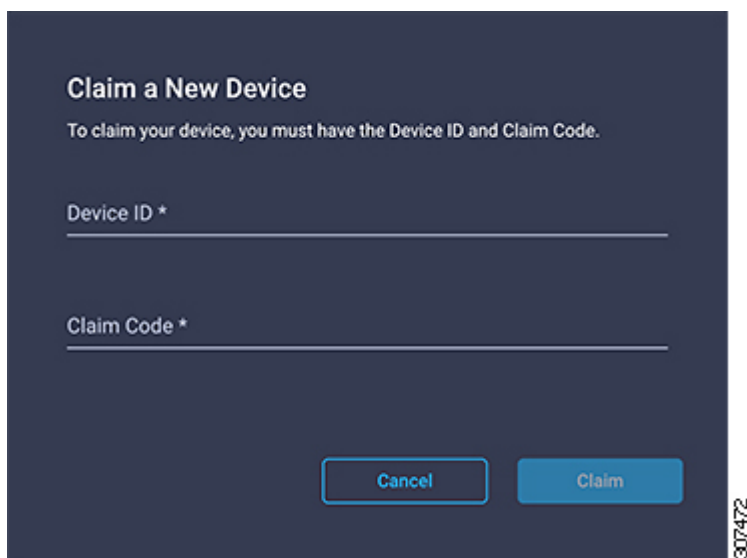
Configure the Intersight Device Connector information from the Cisco APIC site using the instructions provided in [Configuring the Intersight Device Connector](#).

## Procedure

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



The *Claim a New Device* page appears.



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**.
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.

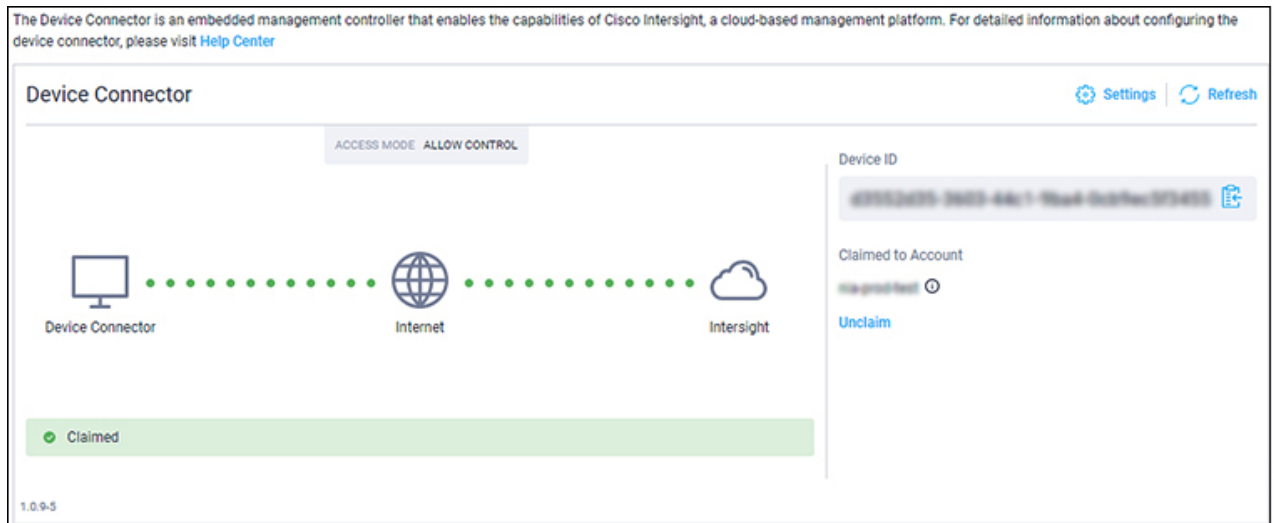
Click on the clipboard next to the fields in the Cisco APIC site to copy the field information into the clipboard.

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.

- 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.



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

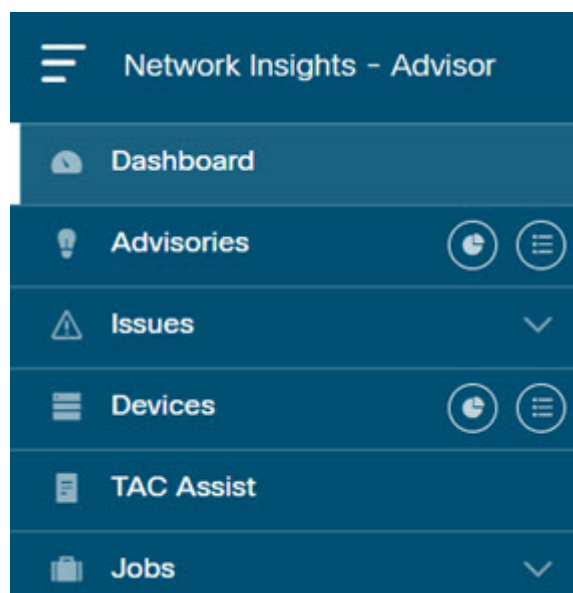
If you decide to unclaim this device for some reason, locate the **Unclaim** link in the *Intersight - Device Connector* page and click that link.

# Navigating Cisco NIA

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

## Navigation Pane

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



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

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

**Issues:** Displays hardware and software bugs, Product Security Incident Response Team (PSIRT) alerts, and notices applicable to your network.

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

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

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

### Icons

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

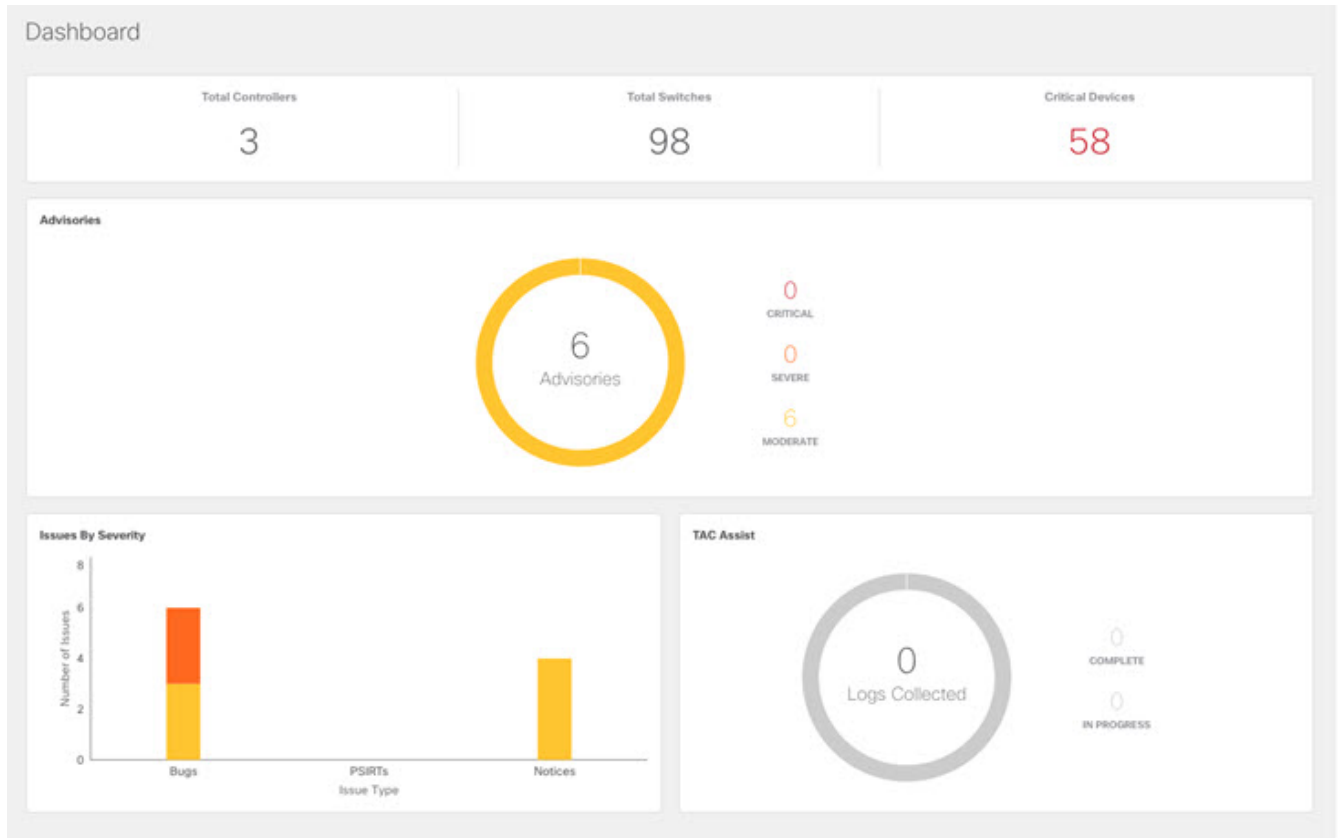
**Browse View icon:** Provides a detailed view of the alert(s) and access to more granular detail.

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

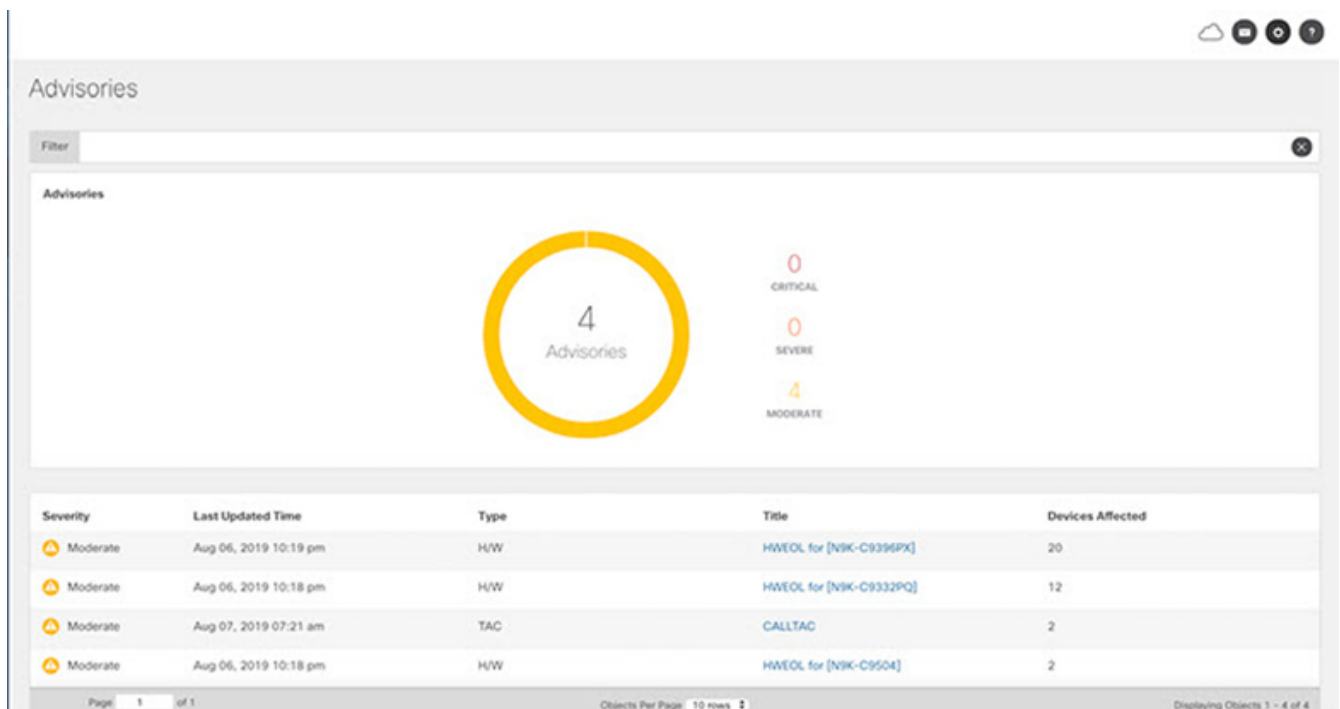
# Work Pane

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:



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



tile.

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

## Browse Work Pane

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

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

307411

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

## Details Work Pane

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

- **General Information:** Includes information about the selected object. This varies based on 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 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.

# Cisco Network Insights Advisor Dashboard

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
<b>Total Controllers</b>	Displays the total number of controllers in your network.
<b>Total Switches</b>	Displays the total number of switches in your network.
<b>[ Critical   Moderate   Healthy ] Devices</b>	<p>Displays the total number of devices determined to be in one of the following categories:</p> <ul style="list-style-type: none"><li>• Critical Devices</li><li>• Moderate Devices</li><li>• Healthy Devices</li></ul> <p>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.</p>
<b>Advisories</b>	Displays the total number of advisories delivered for software and hardware in your network.
<b>Issues By Severity</b>	Displays the total number of issues (bugs, PSIRTs, and notices) delivered for software and hardware in your network.
<b>TAC Assist</b>	Displays the total number of TAC assist logs currently being collected or finished being collected.
<b>Jobs</b>	Provides access to configure and schedule bug scan that runs 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
<b>Critical Advisories</b>	Displays the number of critical advisories that are applicable to devices in your network.
<b>Severe Advisories</b>	Displays the number of severe advisories that are applicable to devices in your network.
<b>Moderate Advisories</b>	Displays the number of moderate advisories that are applicable to devices in your network.
<b>Advisory Type by Devices</b>	Displays the advisory types and the number of affected devices in your network for each.
<b>Advisories Affecting (Version, Platforms)</b>	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
<b>Advisories Chart</b>	Displays the advisory chart for all advisories or only for the filtered severity or type.

Property	Description
<b>Advisories List</b>	<p data-bbox="802 165 1458 241">Displays a list of all advisories or only for the filtered severity or type. Column labels are:</p> <ul data-bbox="826 282 1458 533" style="list-style-type: none"> <li data-bbox="826 282 963 315">• Severity</li> <li data-bbox="826 338 1102 371">• Last Updated Time</li> <li data-bbox="826 394 919 427">• Type</li> <li data-bbox="826 450 1458 533">• Title: Click the link in the <b>Title</b> column to view details about the advisory.</li> </ul> <div data-bbox="900 568 1458 1330" style="border-left: 1px solid #ccc; padding-left: 10px; margin-top: 10px;">  <p data-bbox="1043 582 1430 1330"><b>CALLTAC:</b> 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> </div> <ul data-bbox="826 1379 1075 1413" style="list-style-type: none"> <li data-bbox="826 1379 1075 1413">• Devices Affected</li> </ul>

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

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

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

## Software Upgrade Path

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.

Advisory Detail

Recommended version is 14.2(2f)

**Recommended version is 14.2(2f)**  
 We recommend upgrading to version 14.2(2f)  
 And Controller version to 4.3(2f)

Release Notes: [4.3\(2f\)](#)

Upgrade Path Details

Current release: 4.1(2)  
 Target release: 4.2(2)  
 Recommended path:  
 4.1(2) => 4.2(2)

4.2(2) Upgrade Notes

**Procedure:**

- Upgrade the Cisco APICs. Unless otherwise stated, we recommend upgrading to the latest letter release in the target release train.
- After the Cisco APICs are upgraded successfully, upgrade the switches using 2 or more maintenance groups.
- After the APICs and the switches are upgraded successfully, upgrade the Cisco ACI Virtual Edge or Cisco AVS.

**caveats:**

- When cluster of Cisco APICs is upgrading, the Cisco APIC cluster might enter the minority status if there are any connectivity issues. In this case, user logins can fail until the majority of the Cisco APICs finish the upgrade and the cluster comes out of minority.

**Open Bugs:**

- CSCvg54761 - The application EPG or the corresponding bridge domain's public subnet may be advertised out of an L3Out in another VSF instance without a contract with the L3Out under certain conditions.
- CSCv08257 - The out-of-band ping output in the output of the cluster health tool intermittently shows "Ping failed" due to a bug in the code that parses the ping output. It does not imply an underlying connectivity issue between the APICs in the cluster.
- CSCw11388 - When the VSF instance of both of the service device bridge domains is changed, the sucredHealthOrp managed objects in the switch may not be created for the new VSF instance. As a result traffic will get impacted and there will be faults raised in the switch and in the APIC at the tenant level.

Notices

Severity	Published Time	Type	Title	Devices Affected
Moderate	Feb 21, 2018 04:00 pm	EOL S/W	14.2(24)	5

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

## Issues Dashboard

Issues is divided into these components:

- Bugs - Known bugs that are automated and have show tech with matching signatures
- PSIRTs - Product Security Incident Response Team notices
- Notices - Displays field notices such as end-of-life notices for specific switch hardware and software in your network and categorizes notices by severity.

## 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
<b>Critical Bugs</b>	Displays the number of critical bugs that are applicable to devices in your network.
<b>Severe Bugs</b>	Displays the number of severe bugs that are applicable to devices in your network.
<b>Moderate Bugs</b>	Displays the number of moderate bugs that are applicable to devices in your network.

Property	Description
<b>Bug Severity by Devices (chart)</b>	Displays the bug types and the number of affected devices in your network for each.
<b>Bugs Affecting (Versions, Platforms)</b>	Displays the number of bugs affecting software versions or hardware platforms.

## Browse Bugs

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

### Filters

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

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

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

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

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

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

## PSIRTs Dashboard

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

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



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

## Browse PSIRTs

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

### Filters

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

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

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

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

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

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

## Notices Dashboard

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

Property	Description
<b>Critical Notices</b>	Displays the number of critical notices that are applicable to devices in your network.
<b>Severe Notices</b>	Displays the number of severe notices that are applicable to devices in your network.
<b>Moderate Notices</b>	Displays the number of moderate notices that are applicable to devices in your network.
<b>Notices Chart (by notice type)</b>	Displays the notice types and the number of affected devices in your network for each.
<b>Notices Affecting (Versions, Platforms)</b>	Displays the number of notices affecting software versions or hardware platforms.

## Browse Notices

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

### Filters

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

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

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

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

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

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

## Devices Dashboard


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

Property	Description
<b>Device Issues</b>	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 <b>Recommended Version Info</b> link for more details.
<b>Device by (chart)</b>	Display different versions of software and type of platforms detected.
<b>Top Devices by Maintenance Score</b>	Displays the top six devices in critical order based on the maintenance score. The maintenance score is derived from notices and issues seen for each device according to criteria in the table below.  Click on any device in this category to reveal additional details about the advisories and issues.

### Browse Devices

On the **Maintenance Score** the following table identifies the criteria used to calculate the maintenance score displayed in the Devices dashboard and Browse Devices table.


**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
PSIRTs	Any severity 1 and/or severity 2 PSIRTs	Other than severity 1 or severity 2 PSIRTs	No (0) PSIRTs

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

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

Property	Description
<b>Devices Chart</b>	Displays the Devices chart for all devices or only for the filtered device name or platform product ID.
<b>Devices List</b>	<p>Displays a list of all devices or only for the filtered device name or platform product ID.</p> <p>The list summarizes device name, serial number, IP address, version, CRV, platform.</p> <p>Click a name in the <b>Device Name</b> field to display the details for that device. The device with connectivity issue has an  icon next in the <b>Device Name</b>. Hover over the icon for additional connectivity details.</p> <p>The <b>CRV</b> column displays the recommended version for the device.</p>

## Filters

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

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

- Device Name - display devices that are specifically named.
- Version - displays devices based on the software version running on them.

## TAC Assist Dashboard

The TAC Assist dashboard has the Connected TAC Assist feature, which lets the user collect and upload the logs for 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 Cisco Intersight 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 Intersight Cloud.
- TAC initiated - Cisco TAC triggers on-demand collection of logs for specified devices and pulls the logs from Cisco Intersight Cloud.

### Device Connectivity Notifier for TAC Initiated Assist

Cisco NIA app uses the device connectivity issue notifier on Cisco APIC to communicate with the devices. The notifier checks for TAC triggered on-demand collection of logs. In case the fabric is not configured properly to communicate with the device, Cisco NIA app notifies the following:

- The device is not configured for node interaction.
- You can not run any TAC assist job on the device.
- Cisco NIA can't connect to the device.

If the node interaction is not healthy on the device, you can't select the device for TAC assist to collect logs. The device is greyed out for you to select. See [Browse Devices](#) for details.

## User Initiated Upload to Cisco Intersight Cloud

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

### Before you begin

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

### Procedure

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

The Collect Logs dialog appears.

3. To display specific devices in the list, use the filter utility:
  - Operators - display devices using an operator. Valid operators are:
    - **==** - display devices with an exact match. This operator must be followed by text and/or symbols that are the exact software version, product ID, device name, or assigned IP address of the device.
    - **contains** - display device names or platform identifiers containing entered text or symbols. This operator must be followed by text and/or symbols.
  - Version - display devices that are running a specific software version.
  - Platform - display devices that are a specific type defined by the platform ID.
  - Device Name - display devices that are specifically named.
  - IP Address - display devices that are assigned a specific IP address.
4. From the *Collect Logs* page check the checkbox next to the device for which you want to collect logs. If you want to choose all of the devices in the list, check the checkbox next to the *Device Name* column.

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

The screenshot shows the TAC Assist interface. At the top right, there are icons for cloud, settings, and help. Below the header, there is a section titled 'Begin the Log Collection Process' with a blue 'Begin' button and a note: 'You will be asked to select the device(s) for which to collect Logs to assist TAC.' Below this is a 'Log Collection' table with the following data:

Type	Start Time	Status	Devices	Action
TAC Assist	Dec 15, 2019 09:10 am	COMPLETE	2	<a href="#">View details</a>
TAC Assist	Dec 15, 2019 08:48 am	COMPLETE	2	<a href="#">View details</a>
TAC Assist	Dec 12, 2019 04:20 pm	FAILED	1	<a href="#">View details</a>
TAC Assist	Dec 12, 2019 04:18 pm	COMPLETE	2	<a href="#">View details</a>

At the bottom of the table, there is a pagination bar showing 'Page 1 of 1', 'Objects Per Page 10 rows', and 'Displaying Objects 1 - 4 of 4'.

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

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

**Job Details**

TAC Assist

STATUS	DEVICES	FABRIC	START TIME	JOB ID
Complete	2	mutate-fab	Dec 15, 2019 09:10:37 am	TACASSISTNWBt7vifSjqfNqXTTJtbA

Logs (2 of 2 Successful)

Device Name	Related Job ID	Status	Status Message	Log Location	Cloud
L81_STMORITZ	N/A	Success		/var/afw/vols/ceti/uploads/TACASSISTNWBt7vifSjqfNqXTTJtbA	Upload
ACC21_SAPPORO	N/A	Success		/var/afw/vols/ceti/uploads/TACASSISTNWBt7vifSjqfNqXTTJtbA	Upload

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


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

## TAC Initiated Pull from Cisco Intersight Cloud

The Connected TAC Assist also enables Cisco TAC to initiate an on-demand collection of logs for specified user devices and pulls the logs from Cisco Intersight 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.

# Fabric

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

## Bug Scan

User can schedule or run an on-demand bug scan on their network. Cisco NIA app collects technical support information from all the devices and runs them against known set of signatures, and then flags the corresponding defects. Cisco NIA app also generates an advisory for the customer. For further details, see Advisories from [Advisories Dashboard](#).

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

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

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

## Configure Bug Scan

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

The Fabric Job Configuration page appears.

2. Click **Configure** to schedule a on-demand bug scan 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:
  - <li> = - 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.
    - == - 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.

# Troubleshooting Cisco NIA Application on Cisco APIC

## 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 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 Cisco 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 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

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

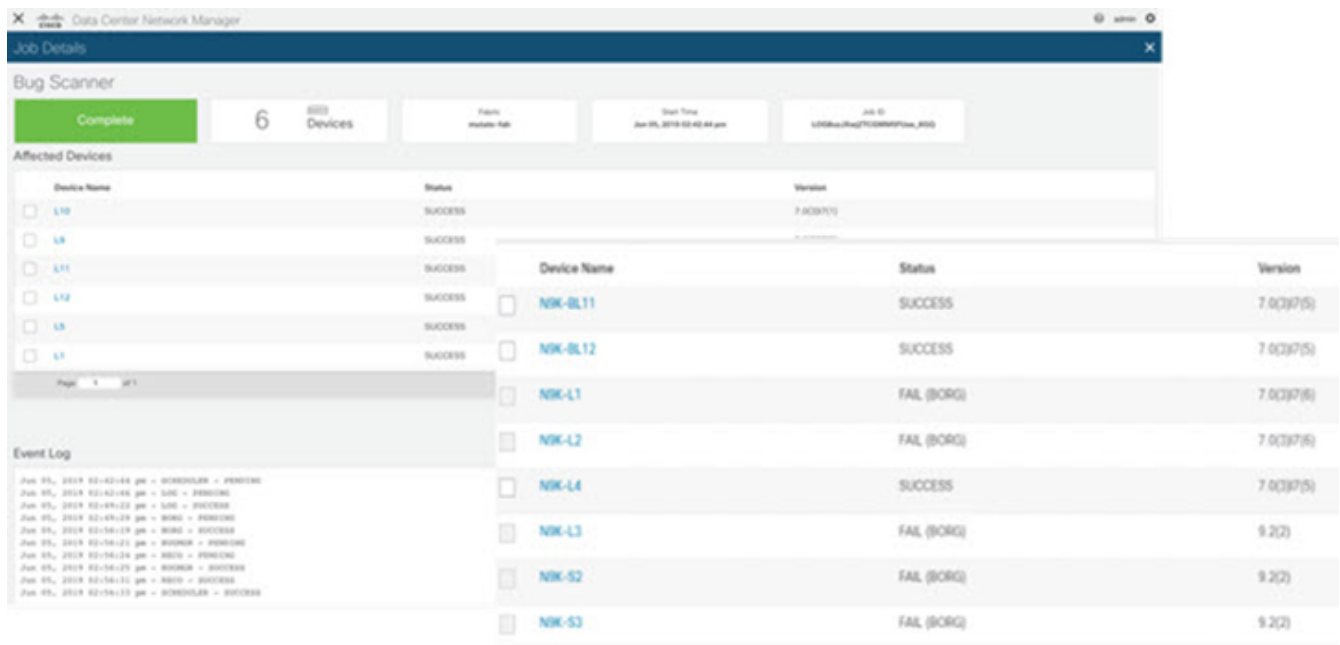
To debug notices:

- Connect to Cisco Intersight Cloud and claim the Device Connector at least 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 Cisco Intersight Cloud and claim the Device Connector at least 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 Intersight Cloud

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

- Make sure that Device Connector is connected to Cisco 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 Intersight Cloud.

```

T22:05:35.087-0800 info stdplugins/techsupport.go:107
    Received request to collect techsupport for device: FD022242J62, 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      FD022242J62
{"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:
FD022232LMZ
{"traceId": "ASc1a31b74ce56d39c3080fc97a4eba779", "traceId":
"PE0194accfee60ba13eee45ff21fa32b81"}
T12:34:17.630-0800 info niatech/techsupport.go:426
    Nashville: Initiating techsupport upload with deviceType: switch,
deviceId: FD022232LMZ
{"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.

# Device Reachability and Authentication

The following table summarizes the device reachability and authentication errors.

Problem	Solution
Device reachability	<ul style="list-style-type: none"><li>• Cisco NIA needs to reach the <b>Management IP</b> of each device it monitors to be able to perform bug scan, compliance check, TAC assist, and upgrade impact.</li><li>• Connectivity to the <b>Management IP</b> of each device is through eth1 of SIM container and computer node.</li><li>• The connectivity to the <b>Management IP</b> of each device is automatically taken care, when compute cluster is setup and <b>out-of-band</b> is entered.</li></ul>
Device authentication	<ul style="list-style-type: none"><li>• To discover devices, you need administrator credentials for device <code>username</code> in Cisco NIA.  Or, you need LAN credentials for the device to discover devices.</li></ul>
Infra	<ul style="list-style-type: none"><li>• Kafka: Check In Sync Replicas (ISR) for kafka related issues.</li><li>• Elastic Search: Check HTTP errors for elastic search related issues.</li><li>• SIM/CETI: Check Cisco APIC container logs.</li><li>• Check for any loss of compute nodes.</li></ul>

## Enhanced TAC Assist - TAC Initiated Pull from Cisco Intersight 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 Intersight Cloud.

Problem	Solution
<p>The app returns a 404 error, "The serial number is not present in DP inventory" when triggering the technical support job.</p>	<ul style="list-style-type: none"> <li>• Make sure the device must be registered as endpoint in Device Connector.</li> <li>• 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 &gt; techsupport log and check the registration log for errors.</li> </ul>
<p>The app returns an error, "NotFound" "The requested device is not registered in the system" when triggering fast-start job.</p>	<ul style="list-style-type: none"> <li>• Make sure the device you want to collect is registered in the same Cisco Intersight 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.</li> <li>• 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.</li> </ul>

## Software Upgrade Path

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

Problem	Solution
<p>Unable to see an upgrade path after running bug scan or having a software EOL.</p>	<p>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.</p>
<p>In the upgrade path link for two releases, multi-hop is displayed, but Cisco NIA displays single hop.</p>	<p>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.</p>



<b>Problem</b>	<b>Solution</b>
Newer version is not displayed in the recommended release or in the upgrade path.	<ul style="list-style-type: none"><li data-bbox="826 165 1458 244">• Check for Cisco Intersight Cloud connectivity and for the latest version of metadata.</li><li data-bbox="826 266 1458 344">• If the latest version is available to run, then run metadata update and bug scan update.</li></ul>