Cisco Network Insights Advisor Application for Cisco APIC User Guide, Release 1.0.x

First Published: 2019-07-15

Last Modified: 2019-12-05

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 1.0.x

Feature	Description	Release
Cisco Network Insights Advisor App on Cisco Application Services Engine.	Cisco Application Services Engine supports Cisco APIC, Release 3.2(8).	1.0.3
Cisco Network Insights Advisor App on Cisco Application Services Engine.	This guide was released to provide a description of Cisco Network Insights Advisor app on Cisco Application Services Engine with Cisco APIC.	1.0.2

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).

Software Requirements

The following are software requirements for Cisco Network Insights Advisor on Cisco Application Services Engine with Cisco APIC.

Table 2: Software Requirements for Cisco NIA on Cisco Application Services Engine with Cisco APIC

Software	Release
Cisco Application Policy Infrastructure Controller (Cisco APIC). Refer to Cisco APIC for details.	3.2(8) and 4.1(2m)
Cisco Application Services Engine. Refer to Cisco Application Services Engine for details.	1.1.0a

Hardware Requirements

The following are required for the Cisco NIA application running on Cisco Application Services Engine with the Cisco APIC:

Table 3: Hardware Requirements for Cisco NIA on Cisco Application Services Engine with the Cisco APIC

Feature	Hardware
Cisco Application Policy Infrastructure Controller (Cisco APIC)	Use existing Cisco APIC cluster L2 and L3
The Cisco Application Services Engine cluster	SE-CL-L3

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 Log in to the Cisco App Center to download the application.

- If you have admin privileges, you can log in to the Cisco APIC GUI with admin privileges.

Step 2 Choose **Apps**.

Step 3 Click the **Download Applications** icon ⬇ on the far-right side of the work pane.

A new browser tab or window opens to the Cisco App Center.

Step 4 Search for Cisco Network Insights Advisor application on the search bar.

Step 5 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 6 Review the license agreement and, if OK, click **Agree and download**.

The Cisco NIA application is downloaded to your local machine.

What to do next

Note the download location of the Cisco NIA file on your local machine. Make sure to move the downloaded Cisco NIA file to a http server, which can then be uploaded to Cisco Application Services Engine using the Cisco APIC.

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

Using Cisco Network Insights Advisor

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.

Cisco NIA app consists of the following components:

- Advisories
  - Software Upgrades
  - Cisco Recommendations
- Notices
  - EoL/EoS Dates
  - Field Notices
- Issues

  - Bug/PSIRT Reports

- TAC Assist
  - Log Collection

Guidelines and Limitations

The following are the usage guidelines and limitations for the Cisco NIA app running on the Cisco Application Services Engine:

- With the Technical Assitance Center (TAC) Assist feature for the selected switches, you can download the logs locally. The user can manually collect the logs and upload to the Cisco Service Request from the folder location provided to the user. The user can select up to 5 devices to download the logs locally.
- Cisco NIA app retains the collected logs using TAC Assist for 24 hours.
- Cisco NIA app retains the collected technical support information using bug scan for 24 hours.
- Pods on your network must have between 1 and 100 switches. Pod with no switches will not appear in the Cisco NIA app list. If you select a Pod with more than 100 switches, initial setup will not complete and you will be prompted to select fabric(s) with 100 or lower number of devices.

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.

Before you begin

Before you begin the initial set up of the Cisco NIA application, make sure the following prerequisites are met:

- You have installed Cisco NIA app and the application has launch correctly.
- Pods on your network must have between 1 and 100 switches. Pods with no switches will not appear in the list.

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

A **Setup** dialog appears.

Step 2 In **Data Collection Setup**, click **Configure**.

The **Data Collection Setup** dialog appears. In the **Pod** list are pods that were discovered during the Cisco NIA application installation.

Step 3 Check only the pods you want visible to the Cisco NIA application.

Step 4 Click **Ok**.

The **Setup** dialog appears with the selected pods appearing in **Data Collection Setup**. You can edit the selected pod(s) by clicking **Edit configuration**. You can return to the setup utility anytime by clicking the settings icon ⚙ and choose **Rerun Setup**.

Once a pod or pods are defined, Cisco NIA app requires some internal configuration time before becoming operational. The Apps icon on the top displays a blue wheel, which confirms that the app is hosted on Cisco Application Services Engine rather than hosted locally.

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
Pod	Choose a Pod containing the devices you want visible to the Cisco NIA application.
☁	**Device Connector Status**: Identifies the current connection status of the Cisco NIA application to the Cisco Intersight cloud and the device connector claim condition. Possible connection statuses are: • **Not Connected**: The Cisco NIA application is not connected to the Cisco Intersight cloud. • **Connected / Not Claimed**: The Cisco NIA application is connected to the Cisco Intersight cloud but the device connector has not been claimed by the customer. • **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: • **Configuration**—Displays currently running jobs and allows for the configuration of the bug scanner. • **Job List**—Displays the list of scheduled jobs. • **About Network Insights**—Displays an information dialog identifying the version number of the NIA application. • **Rerun Setup**—Allows you to edit the Data Collection Setup by adding or removing Pod.

Bug Scan

? **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 flags the corresponding defects. Cisco NIA app also generates an advisory for the customer. For further details, see Advisories from Using the Cisco Network Insights Advisor Application, on page 19.

Setting Up the Device Connector

This secion describes setting up the device connector for Cisco NIAon 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.

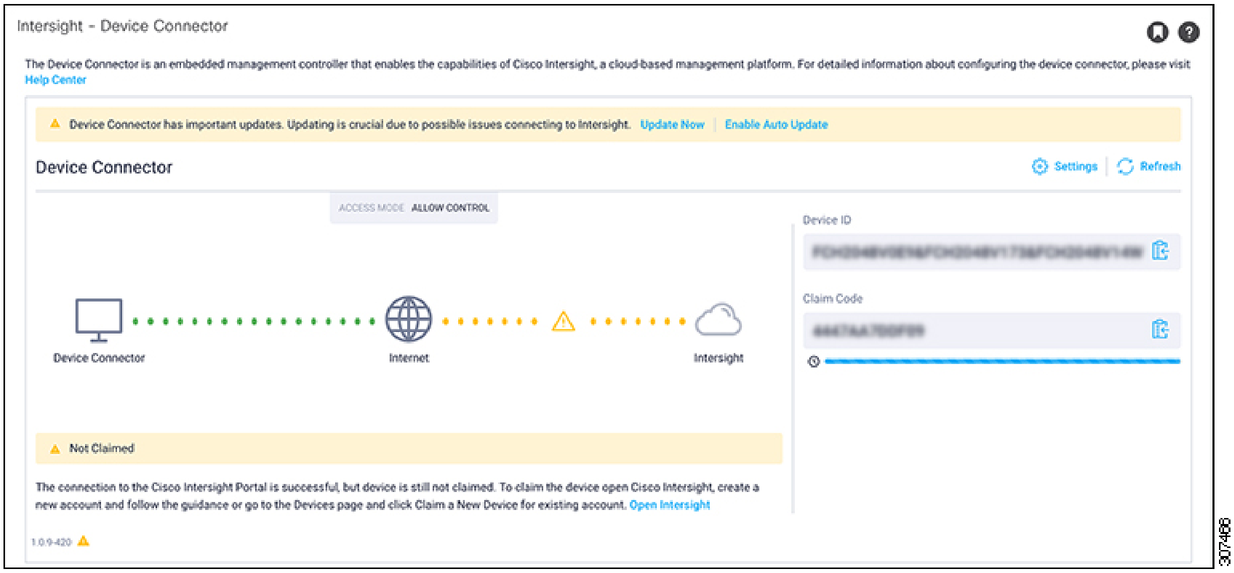
Configuring the Intersight Device Connector

Step 1 On the Cisco Application Services Engine Device Connector navigation pane, click **Administration**.

Step 2 From the Server list on the navigation pane, click **Device Connector**.

Step 3 In the **Navigation** pane, click **Intersight**.

The Device Connector work pane appears:



Intersight - Device Connector

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

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

Device Connector

Device ID: [redacted]

Claim Code: [redacted]

⚠ Not Claimed

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

1.0.9-420 ⚠

- 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 8.

Step 4 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 5 to begin configuring the Intersight Device Connector.

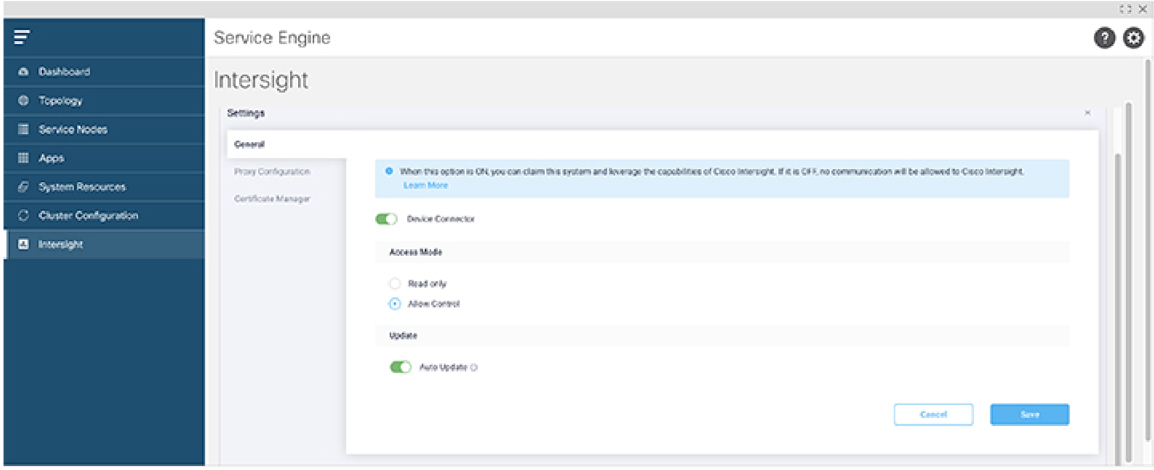
- If you would like to update the software at this time, click one of the two links in the yellow bar towards the top of the page, depending on how you would like to update the software:

  - **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 6c for more information.

Step 5 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.



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

Device Connector: ON

Access Mode

○ Read only
● Allow Control

Update

Auto Update: ON

Step 6 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.

We recommend that you toggle the **Auto Update** option to ON so that the system automatically updates the software. Note that toggling the **Auto Update** option to ON means that the Device Connector will automatically upgrade its image whenever there is any upgrade push from Intersight.

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

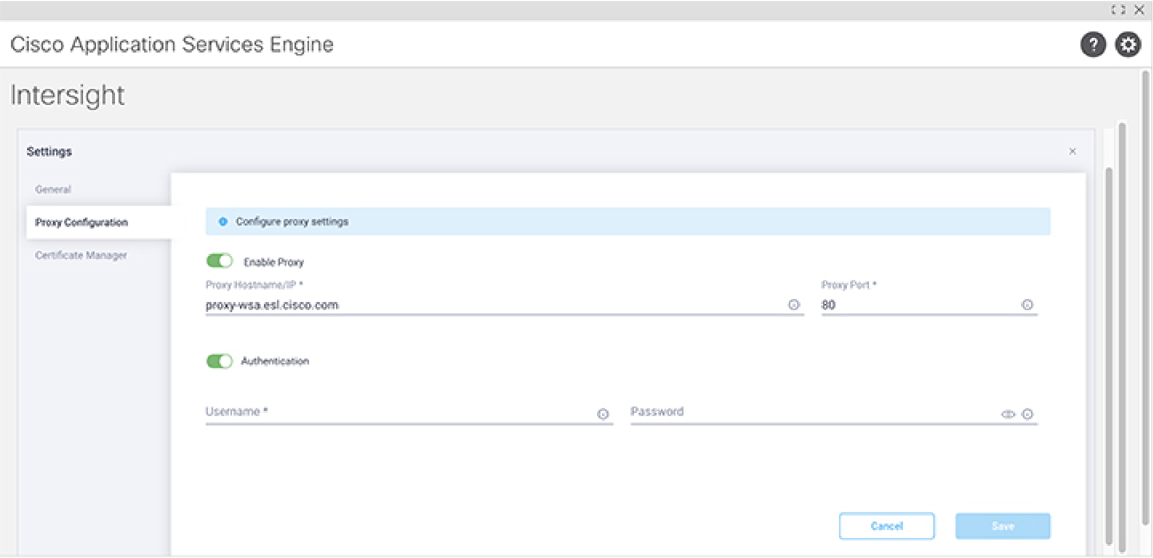
The **Intersight - Device Connector** overview pages appears again. At this point, you can make or verify several configure settings for the Intersight Device Connnector:

- If you want to configure the proxy that the Device Connector will use to communicate with the Intersight cloud, go to step 8.
- If you want to manage certificates with the Device Connector, go to step 11.

The Cisco Application Services Engine requires you to configure the Proxy Settings for the Intersight Device Connector.

Step 8 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.



Enable Proxy: ON

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

Proxy Port *: 80

Authentication: ON

Username *

Password

Step 9 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.

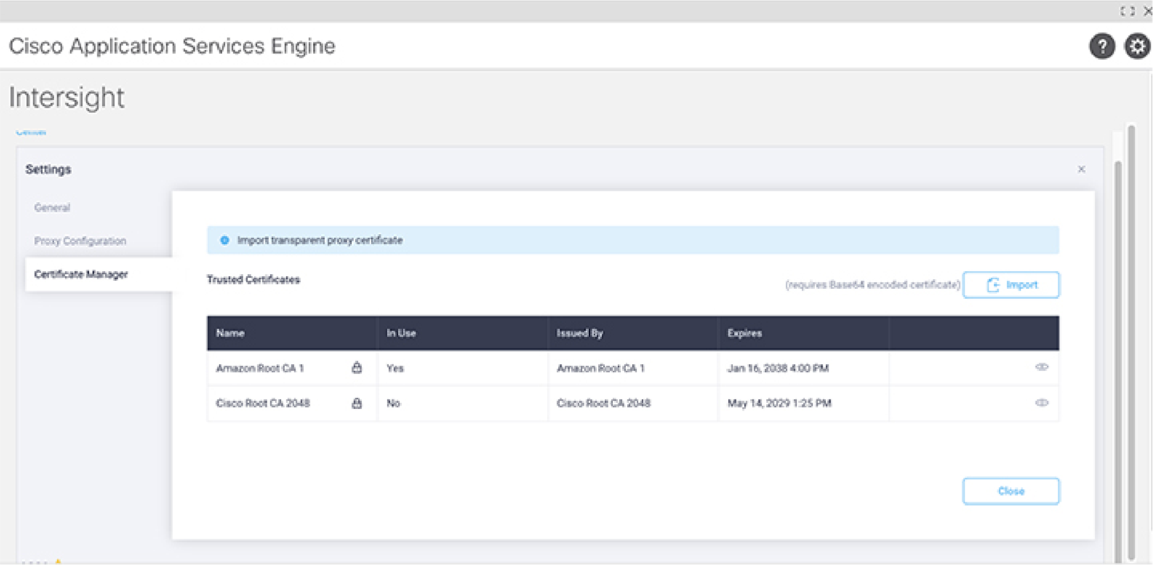
Step 10 When you have completed the configurations in the **Proxy Configuration** page, click **Save**.

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

The **Certificate Manager** page appears.


Cisco Application Services Engine
Intersight
Settings
General
Proxy Configuration
Certificate Manager
Import transparent proxy certificate
Trusted Certificates
(requires Base64 encoded certificate)
Import
Close

Name	In Use	Issued By	Expires
Amazon Root CA 1	Yes	Amazon Root CA 1	Jan 16, 2038 4:00 PM
Cisco Root CA 2048	No	Cisco Root CA 2048	May 14, 2029 1:25 PM

Step 12 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 13 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

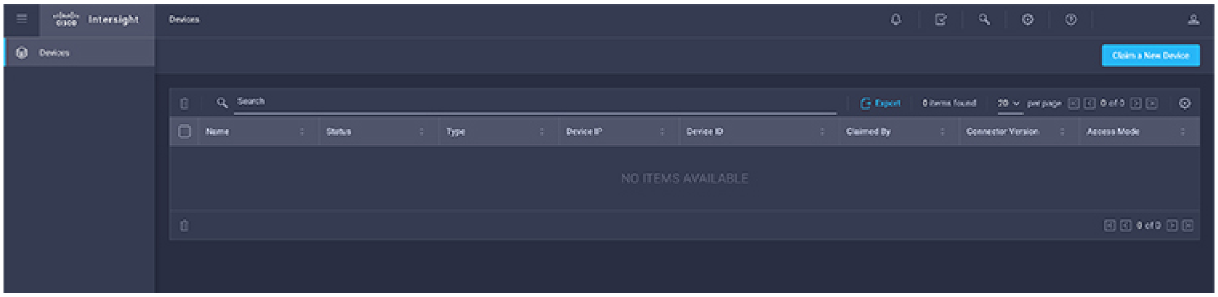
Before you begin

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:

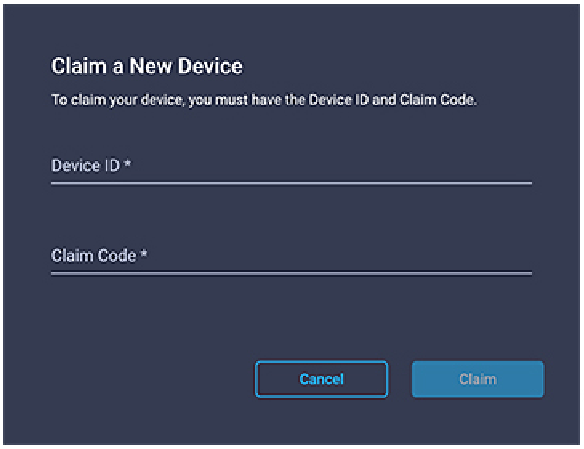
https://www.intersight.com

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



	Name	Status	Type	Device IP	Device ID	Claimed By	Connector Version	Access Mode
NO ITEMS AVAILABLE								

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



Claim a New Device

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

Device ID *

Claim Code *

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.

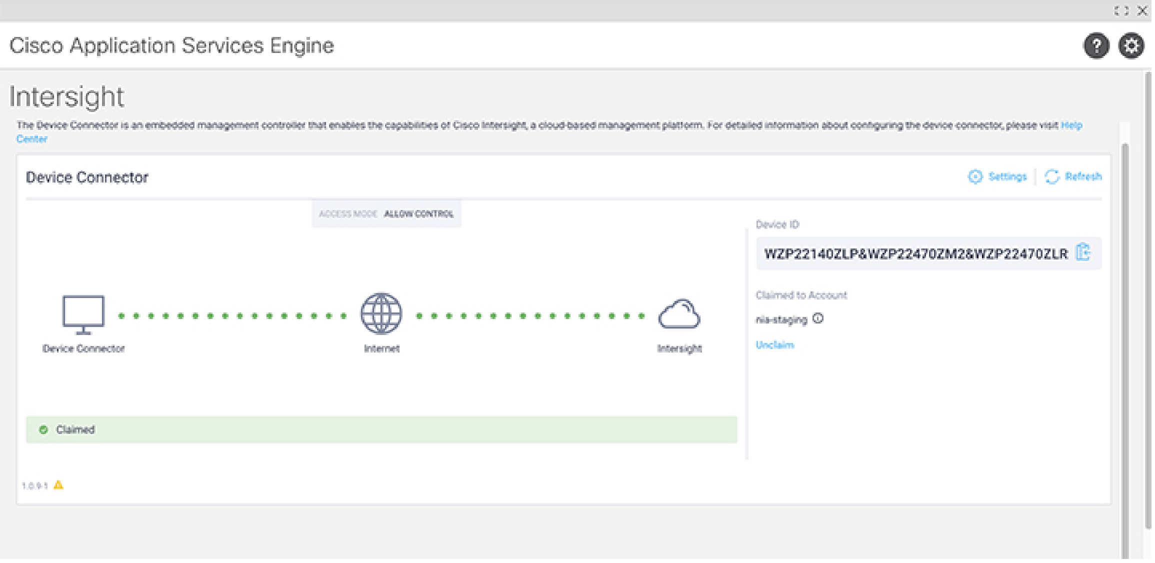
Click on the clipboard next to the fields in the Cisco APIC site to copy the field information into the clipboard.

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.



Cisco Application Services Engine

Intersight

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

Device Connector

Settings | Refresh

ACCESS MODE ALLOW CONTROL

Device ID

WZP22140ZLP&WZP22470ZM2&WZP22470ZLR

Claimed to Account

nia-staging

Unclaim

Claimed

1.0.9-1

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

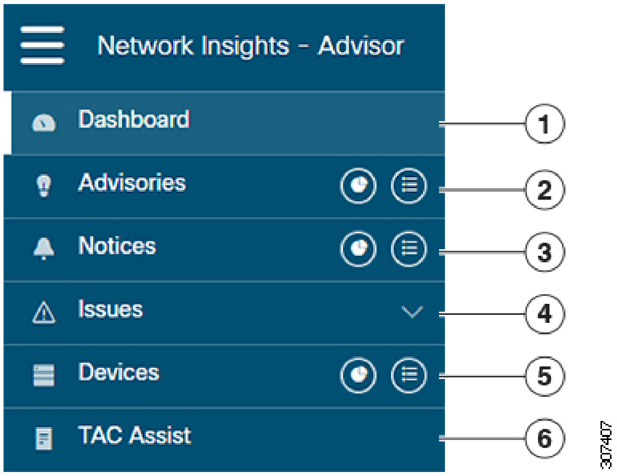
If you decide to unclaim this device for some reason, locate the **Unclaim** link in the **Intersight - Device Connector** page and click that link.

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 six 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.

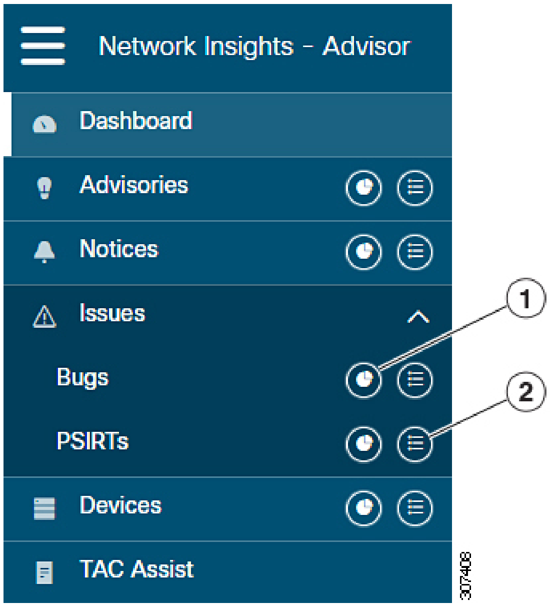
3 Notices: Displays notices applicable to the hardware and software in your network.

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

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

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

Additional functions are :



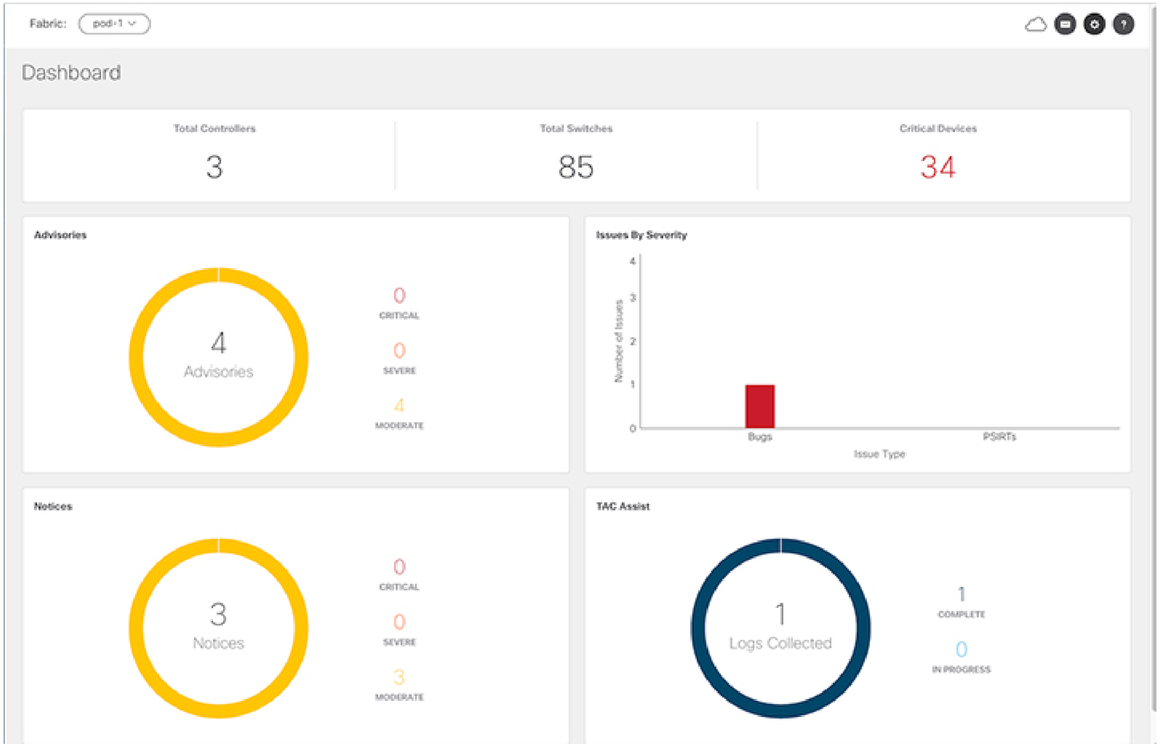
1 Dashboard View icon: Provides immediate access to top usage or issues for the selected alert type.

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

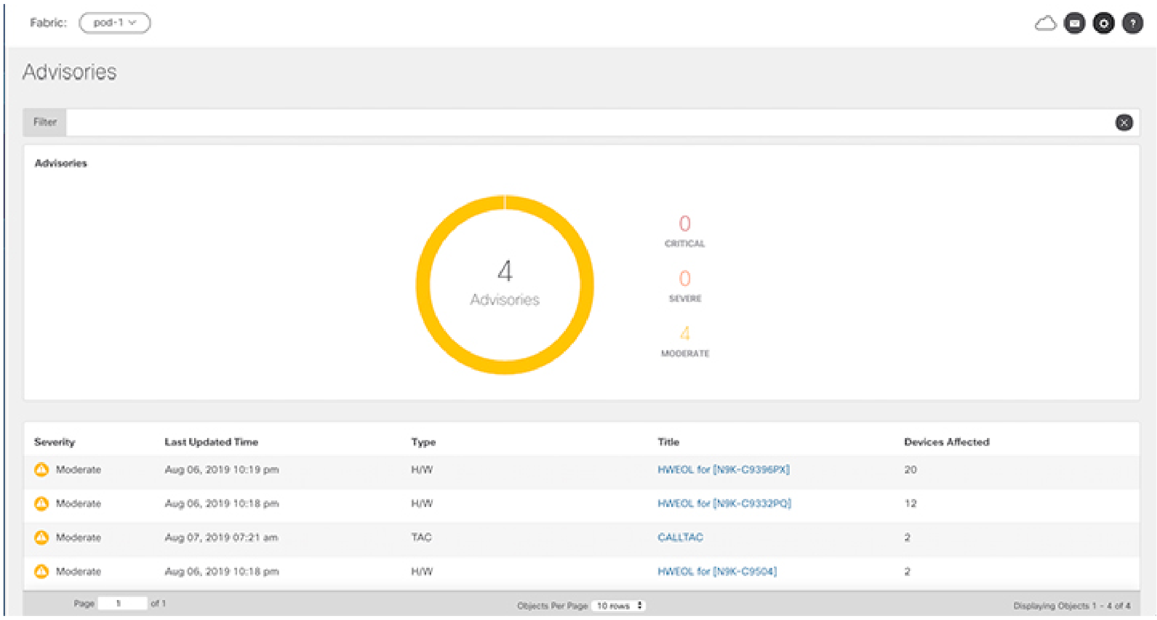
Work Pane

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

Dashboard Work Pane



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



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

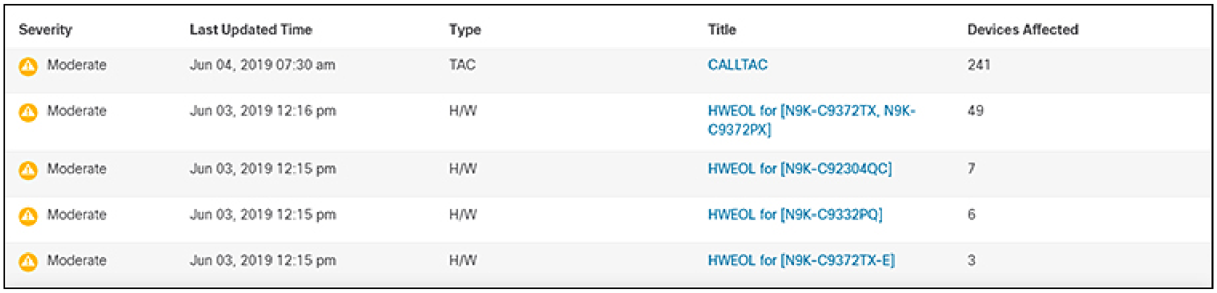
Page 1 of 1 Objects Per Page 10 rows Displaying Objects 1 - 4 of 4

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

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

Browse Work Pane

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



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

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

Details Work Pane

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

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

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 and TAC Assist logs applicable to your network.

Property	Description
Total Controllers	Displays the total number of controllers in your network.
Total Switches	Displays the total number of switches in your network.

Property	Description
[Critical | Moderate | Healthy] Devices	Displays the total number of devices determined to be in one of the following categories: • Critical Devices • Moderate Devices • Healthy Devices Device counts in the higher category (Critical is highest) appear in the displayed count. If no devices are currently in the Critical category, then the device count of the Moderate category is displayed. If no issues are detected in any device, then the device count of the Healthy category is displayed.
Advisories	Displays the total number of advisories delivered for software and hardware in your network.
Issues By Severity	Displays the total number of issues (anomalies, bugs, and PSIRTs) delivered for software and hardware in your network.
Notices	Displays the total number of notices delivered for devices in your network.
TAC Assist	Displays the total number of TAC assist logs currently being collected or finished being collected.

Advisories

Advisories Dashboard

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

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

- Software or hardware upgrades to address bugs, PSIRTs, and field notices
- Contacting the Technical Assistance Center (TAC)

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.

Property	Description
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.

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.
  - 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

Notices

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

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

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.

Property	Description
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.

Property	Description
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

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
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

TAC Assist Dashboard

The TAC Assist dashboard allows you to collect logs for devices in your network. These logs can be attached to Service Requests (SRs) for further analysis.

1. Click **Begin** to initiate the log collection process.

   The Collect Logs dialog appears.

2. 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.

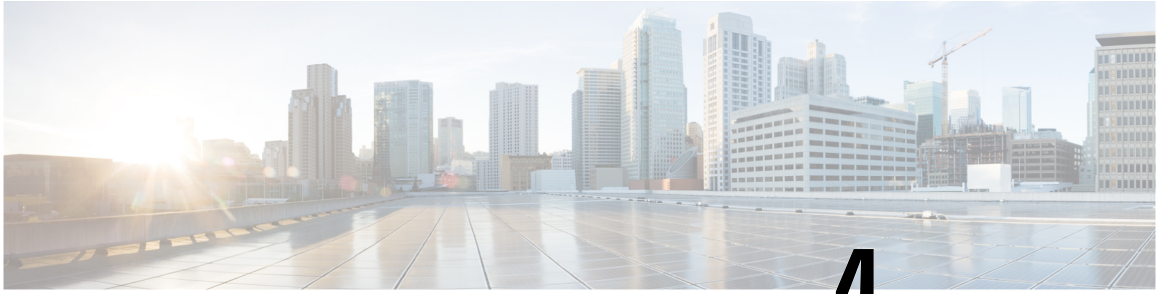
   - IP Address - display devices that are assigned a specific IP address.

3. Place a check in the checkbox next to the device for which you wan to collect logs. If you want to choose all of the devices in the list, place a check in the checkbox next to the **Device Name** column title.

4. Click **Collect Logs**.

   A TAC Assist job message appears on the TAC Assist dashboard. Once the logs are collected, Cisco NIA displays the location where they can be accessed on the Cisco APIC. TAC Assist is allowed for completed bug scan jobs and as long as logs are available in the storage.

   You can go to the **Completed Jobs** section, click **Devices** and click **Collect Logs**. In the Cisco APIC, you can click **TAC Assist Result** for all the nodes and click to download the logs locally.



CHAPTER 4

Upgrade Cisco Network Insights Advisor

This chapter contains the following sections:

Upgrading Cisco NIA Application on Cisco Application Services Engine

Upgrading Cisco NIA app on Cisco Application Services Engine is not supported. To upgrade to the latest version of Cisco NIA app, you must delete the existing version of Cisco NIA app on Cisco Application Services Engine and install the latest version.