



# Using Cisco Network Insights Advisor

---

This chapter contains the following sections:

- [About Cisco Network Insights Advisor, on page 1](#)
- [Guidelines and Limitations, on page 2](#)
- [Cisco NIA Initial Setup, on page 2](#)
- [Setting Up the Device Connector, on page 3](#)
- [Cisco NIA Settings, on page 7](#)
- [Navigating Cisco NIA, on page 8](#)
- [Using the Cisco NIA Application, on page 11](#)

## 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 customers 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
- Job Configuration
  - Schedule Driven (Compliance, Bug scan)
  - On Demand




---

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

---

## Guidelines and Limitations

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

- IPv6 is not supported for Cisco NIA application in the Cisco DCNM.
- The Cisco NIA application requires that physical servers hosting Cisco DCNM computes as VMs are atleast Cisco C220-M4 category. It is also required that a compute be hosted on a data store with a dedicated hard disk of atleast 500GB.
- Cisco NIA app retains the collected logs using TAC Assist for 24 hours.
- Cisco NIA app retains the collected technical support information using bag scan for 24 hours.

## Cisco NIA Initial Setup

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

### Before you begin

- You have installed and launched the Cisco NIA application.
- Fabrics on your network must have between 1 and 250 switches. Fabrics with no switches will not appear in the list. If you select a fabric with more than 250 switches, initial setup will not complete and you will be prompted to select fabric(s) with 250 or lower number of devices.

---

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


A **Setup** dialog appears.

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

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

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

**Step 4** Click **Ok**.

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

---

Once a fabric or fabrics are defined, Cisco NIA app requires some internal configuration time before becoming operational.

## Setting Up the Device Connector

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

### About Device Connector

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

When an Intersight-enabled device or application starts, the Device Connector starts at boot by default, and attempts to connect to the cloud service. If the **Auto Update** option is enabled, the Device Connector is automatically updated to the latest version through a refresh by the Intersight service when you connect to Intersight. For more information on the **Auto Update** option, see [Configuring the Intersight Device Connector, on page 3](#).

### Configuring the Intersight Device Connector

Cisco NIA application is connected to the Cisco Intersight cloud portal through a Device Connector which is embedded in the management controller of the Cisco DCNM platform. Cisco Intersight is a virtual appliance that helps manage and monitor devices through the Cisco NIA app. The Device Connector provides a secure way for connected Cisco DCNM to send and receive information from the Cisco Intersight portal, using a secure Internet connection.

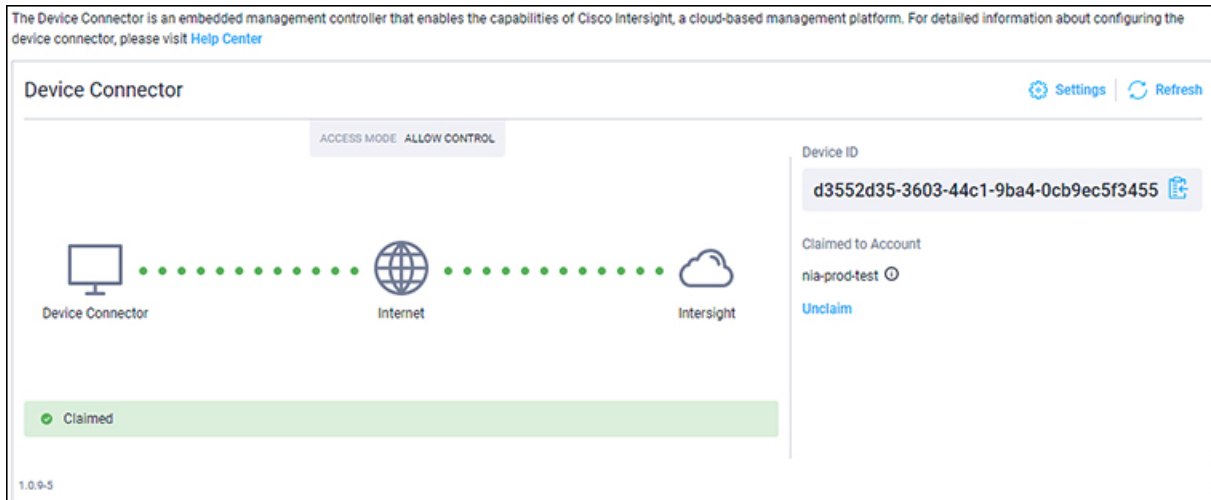
To setup the Device Connector, follow these steps:

---

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

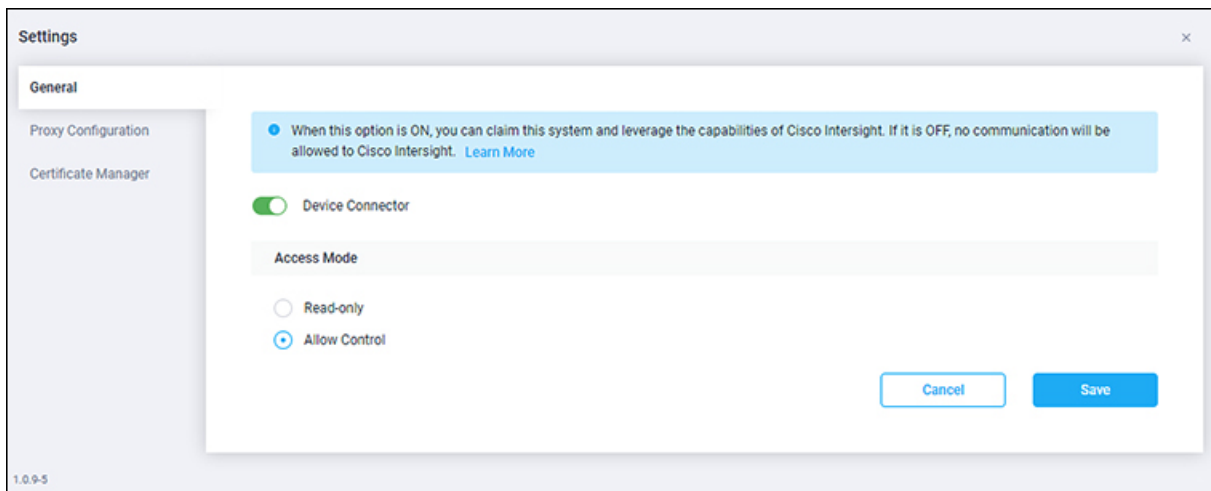
**Step 2** Under the Cisco DCNM Server list, click Device Connector.

The Device Connector work pane appears:



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

The **Settings - General** dialog appears:



#### **Device Connector** (switch)

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

#### **Access Mode**

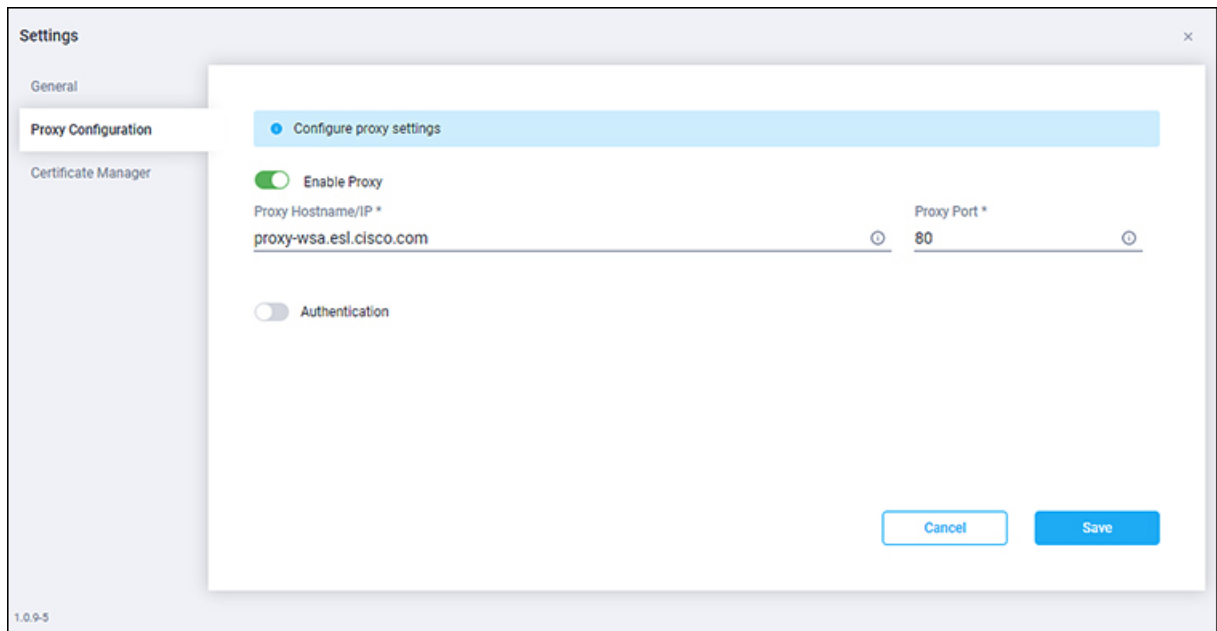
**Read-only:** This option ensures that no changes are made to this device from Intersight. For example, actions such as upgrading firmware or a profile deployment will not be allowed in the Read-Only mode. However, the actions depend on the features available for a particular system.

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

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

**Step 5** Click **Proxy Configuration**.

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



**Enable Proxy** (switch)

Enable HTTPS Proxy to configure the proxy settings.

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

**Authentication** (switch)

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

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

**Note** Proxy settings are required for Network Insights.

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

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

**Step 8** Click **Save**.

## Claiming a Device

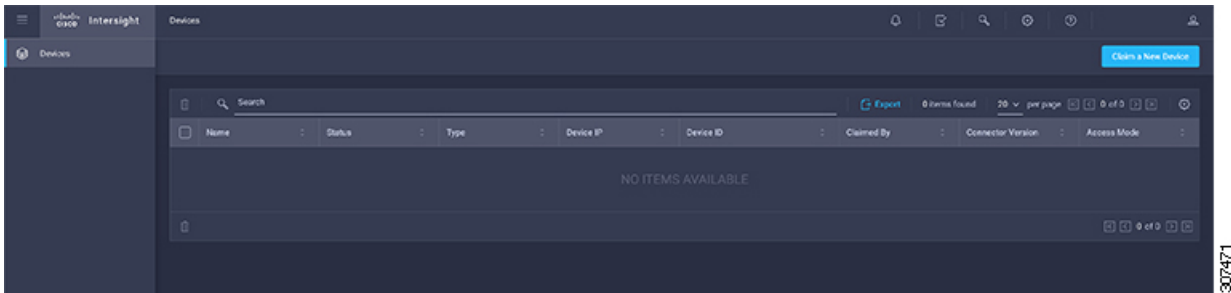
### Before you begin

Configure the Intersight Device Connector information from the Cisco APIC site using the instructions provided in [Configuring the Intersight Device Connector, on page 3](#).

**Step 1** Log into the Cisco Intersight cloud site:

<https://www.intersight.com>

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



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

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

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

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

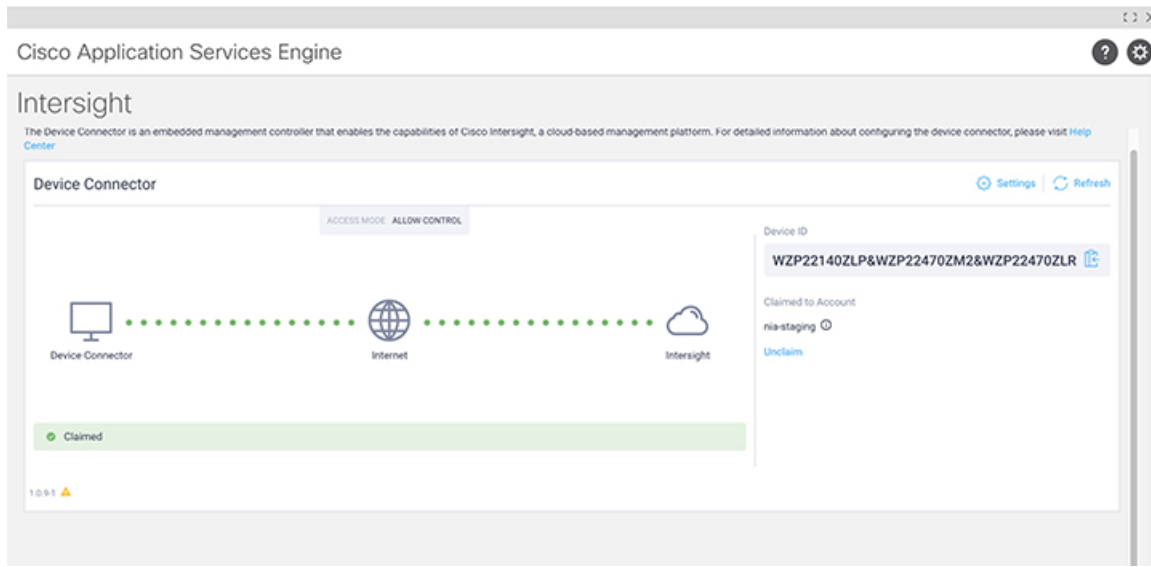
Click on the clipboard next to the fields in the Cisco APIC site to copy the field information into the clipboard.

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

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

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

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




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



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

## 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 application settings. The following table describes each:

Property	Description
<b>Fabric</b>	Choose a fabric containing the devices you want visible to the Cisco NIA application.
	<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.</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.</li> </ul> <p>For more information, see <a href="#">Configuring the Intersight Device Connector, on page 3</a>.</p>

Property	Description
	<p><b>Inbox:</b> View messages from Cisco regarding software upgrades or other relevant information about devices on your network.</p> <p><b>Note</b> This is a preview feature.</p>
	<p>Clicking on this icon invokes a list menu allowing you to make changes to the following:</p> <ul style="list-style-type: none"> <li>• <b>Configuration</b>—Displays currently running jobs and allows for the configuration of the bug scanner and compliance check.</li> <li>• <b>Job List</b>—Displays list of running and completed jobs. Includes a time range setting to display running/completed jobs during a specific time period.</li> <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 published version. This requires that the using of the Cisco Intersight Device Connector is connected and claimed. See <a href="#">Configuring the Intersight Device Connector, on page 3</a> for details.</li> <li>• <b>Rerun Setup</b>—Allows you to edit the Data Collection Setup by adding or removing fabrics.</li> </ul>

### Bug Scan

 **Bug Scan:** User can schedule or run an on-demand bug scan on their network. The Cisco NIA app collects technical support information from all the devices and runs them against known set of signatures and flags the corresponding defects. The Cisco NIA app also generates an advisory for the customer. For further details, see Advisories from [Using the Cisco NIA Application, on page 11](#).

### Compliance Check

The Cisco NIA app scans customer configurations periodically and checks it against [Cisco NX-OS Hardening Guide](#). Such configurations are flagged as anomalies that customers can fix. Once fixed these anomalies are removed from the system.

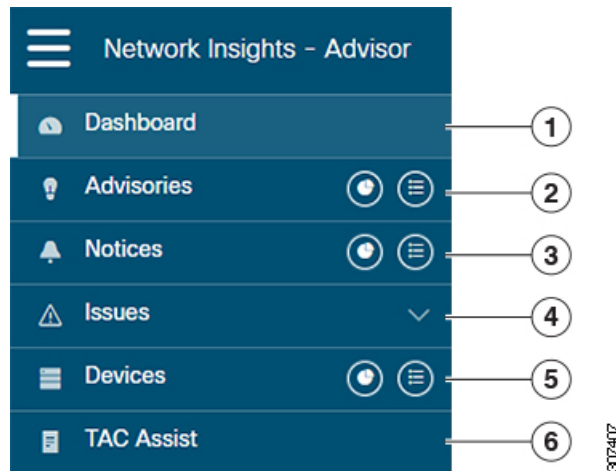
## Navigating Cisco NIA

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, and collected TAC assist logs.

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

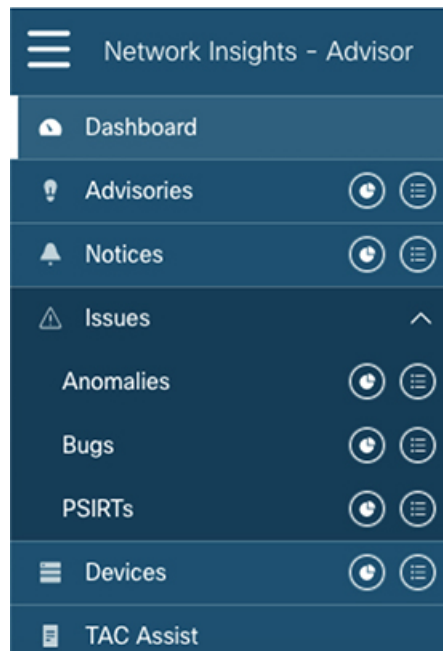
**3** Notices: Displays notices applicable to the hardware and software in your network.

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

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

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

Additional functions are :



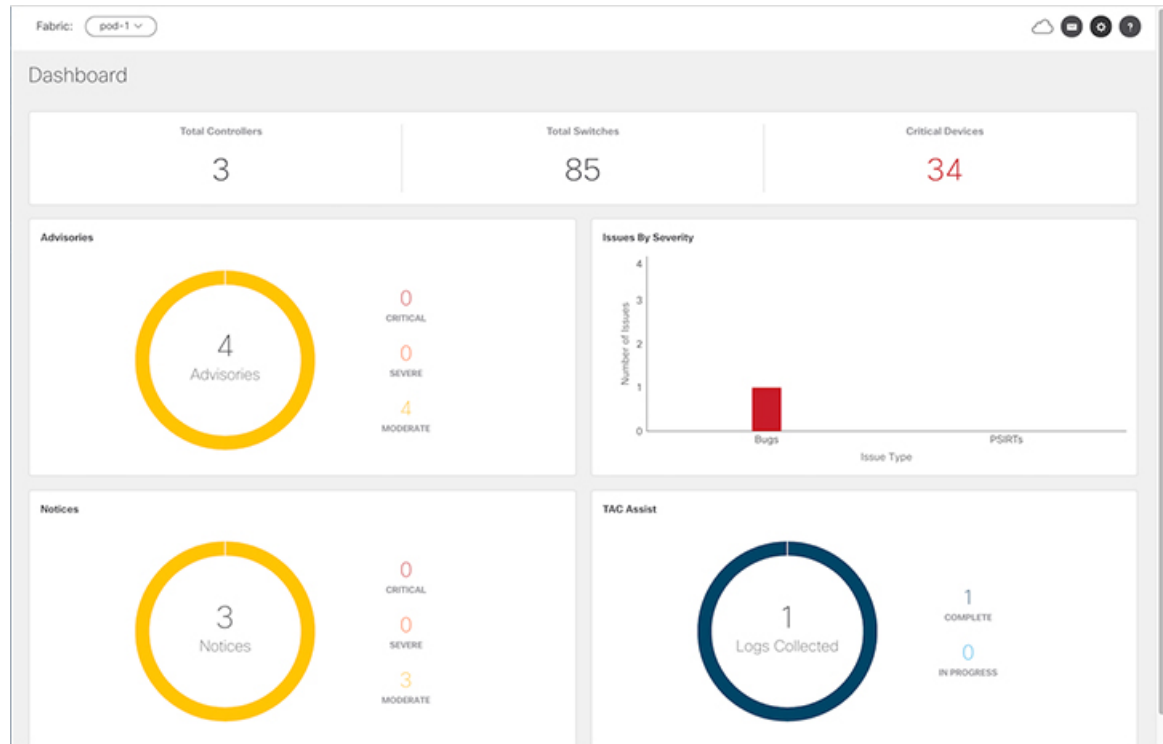
**1** Dashboard View icon: Provides immediate access to top usage or issues for the selected information type.

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

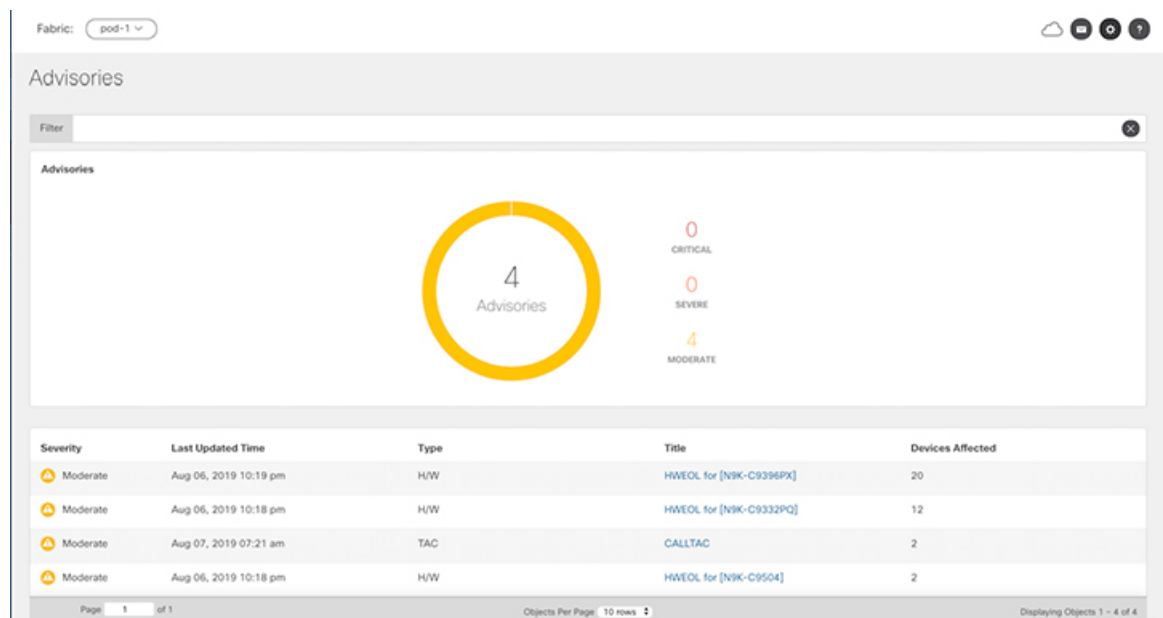
## Work Pane

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

### Dashboard Work Pane



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



- 1 Launches the Browse work pane with all of the items displayed from the graph in the information tile.
- 2 Launches the Browse work pane with only the selected items displayed from the number in the information tile.

### Browse Work Pane

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

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

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

### Details Work Pane

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

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

## Using the Cisco NIA Application

Each Cisco device known to the Cisco NIA application is analyzed to help be more proactive about issues and anomalies in the network. Use the dashboard in the Cisco NIA application to view relevant information and select specific items to view details.

### Main Dashboard

The Cisco NIA application main dashboard provides immediate access to a high-level view of the advisories, notices, issues and TAC Assist logs applicable to your network.

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.

Property	Description
[ <b>Critical</b>   <b>Moderate</b>   <b>Healthy</b> ] <b>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 (anomalies, bugs, and PSIRTs) delivered for software and hardware in your network.
<b>Notices</b>	Displays the total number of notices delivered for devices in your network.
<b>TAC Assist</b>	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. NIA considers this information and recommends:

- Software or hardware upgrades to address bugs, PSIRTs, and field notices
- Contacting the Technical Assistance Center (TAC)
- Measuring a software upgrade impact (disruptive/non-disruptive)
- Compliance configurations

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.

Property	Description
<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.

### Filters

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

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

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

### Software Upgrade Impact

When attempting to upgrade to a recommended software version, Cisco NIA app helps to determine the potential impact of the upgrade to the device for which the upgrade was suggested. The upgrade impact checks for NX-OS version and configuration compatibility. BIOS compatibility is currently not checked. The returned result indicates if the upgrade will be disruptive or non-disruptive.



**Note** The **feature scp-server** command should be enabled on the devices for the upgrade impact check to function.

Software upgrade recommendations typically appear in the Advisories list after a bug scan is completed. To initiate an upgrade impact, follow these steps:

1. In the navigation pane, click the browse view icon next to the **Advisories** option.
2. In the advisories list table, locate the software upgrade recommendation identified by the S/W Ver. in the **Type** column.
3. Click the software version in the **Title** column and then click **Run Upgrade Impact**.

The **Advisories Detail** dialog appears.

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

A note appears in the **Advisory Details** dialog stating that the "Upgrade Impact is currently running". In the **Upgrade Impact Results** table, the devices that could be impacted by the upgrade are listed and the **Result** column indicates that the impact process is "PENDING". Once the upgrade impact begins, the **Result** column changes to "RUNNING".

Once complete, the upgrade impact result can be one of the following:

- **NON-DISRUPTIVE:** Devices can likely be upgraded to the new suggested software version without disrupting the network.
- **DISRUPTIVE:** Devices can be upgraded to the new suggested software version but with disruption, described by the reason on the result dialog.
- **FAIL:** A technical error occurred, described by the reason on the result dialog.

The information provided by the upgrade impact utility helps in making the determination to upgrade or not.

## 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
<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 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
<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.

### Issues

Issues is divided into these components:

- Anomalies - Compliance check violations
- Bugs - Known bugs that are automated and have show tech with matching signatures
- PSIRTs - Product Security Incident Response Team notices

### Anomalies Dashboard

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

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

### Browse Anomalies

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

### Filters



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

- Operators - display anomalies using an operator. Valid operators are:
  - = - display anomalies with an exact match.
- Severity - display anomalies only for a specific severity. Valid severities are:
  - Critical - Returns matches for critical anomalies.
  - Severe - Returns matches for severe anomalies.
  - Moderate - Returns matches for moderate anomalies.
- Type - display anomalies only for a specific type. Valid types are:
  - Compliance - Returns matches for anomalies for a specific compliance mandate or requirement.

Property	Description
<b>Anomalies Chart</b>	Displays the anomaly chart for all anomalies or only for the filtered severity or type.
<b>Anomalies List</b>	Displays a list of all anomalies or only for the filtered severity or type.

### Bugs Dashboard

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

Property	Description
<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.
<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 severity's 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.

### 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.
<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 severity's 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.

## 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
<b>Device Issues</b>	Displays the number of devices that have reached <b>End of Maintenance</b> 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> for more details.
<b>Device by (chart)</b>	Displays the different versions of software and types of hardware 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.

### Maintenance Score

The following table identifies the criteria used to calculate the maintenance score displayed in the Devices dashboard and Browse Devices table.

Issue	 <b>Critical (Red)</b>	 <b>Severe/Moderate/Low (Amber)</b>	 <b>None (Green)</b>
End of Maintenance Support	Less than 365 days to the end of support date	Between 365 days and 730 days to the end of support date	Greater than 730 days to the end of support date
Bugs	Any severity 1 and/or severity 2 bugs	Other than severity 1 or severity 2 bugs	No (0) bugs
Field Notices	Any applicable field notice	N/A	No applicable field notices
Compliance Failure	More than 2 compliance failures	One to two compliance failures	No (0) compliance failures
PSIRTs	Any severity 1 and/or severity 2 PSIRTs	Other than severity 1 or severity 2 PSIRTs	No (0) PSIRTs

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

### Browse Devices

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

### Filters

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

- Operators - display devices using an operator. Valid operators are:
  - == - display devices with an exact match.
  - contains - display device names or platform identifiers containing entered text or symbols. This operator must be followed by text and/or symbols.
  - != - display devices that are not equal to the entered text or symbols. This operator must be followed by text and/or symbols.
- Platform - display devices that are a specific type defined by the platform ID.
- Device Name - display devices that are specifically named.
- Version - displays devices based on the software version running on them.

Property	Description
<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>	Displays a list of all devices or only for the filtered device name or platform product ID. Click a name in the <b>Device Name</b> 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 box 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 want 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 app displays the location where they can be accessed on the Cisco DCNM Server.

