



# Using Cisco Network Insights Advisor

This chapter contains the following sections:

- [Using the Cisco Network Insights Advisor Application, on page 1](#)

## Using the Cisco Network Insights Advisor Application

Each Cisco Application Centric Infrastructure (Cisco ACI) switch known to the Cisco NIA application is analyzed to help be more proactive about issues and anomalies in the network. Use the dashboard in the Cisco NIA application to view relevant information and select specific items to view details.

### Main Dashboard

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

Property	Description
<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>	Displays the total number of devices determined to be in one of the following categories: <ul style="list-style-type: none"><li>• Critical Devices</li><li>• Moderate Devices</li><li>• Healthy Devices</li></ul> 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.
<b>Advisories</b>	Displays the total number of advisories delivered for software and hardware in your network.

Property	Description
<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.
<b>Jobs</b>	Provides access to configure and schedule bug scan and compliance check jobs that run across the fabric.

## Advisories Dashboard

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

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

- Software or hardware upgrades to address bugs, PSIRTs, and field notices
- CALL TAC
- Advisory Report
- Software Upgrade Path

Property	Description
<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
Advisories Chart	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 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 4.2(2f)

Release Notes: [4.2\(2f\)](#)

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

1 4.1(2) 2 4.2(2)

**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:**

- CSCw24181 - The application EPG or the corresponding bridge domain's public subnet may be advertised out of an L3Out in another VRF instance without a contract with the L3Out under certain conditions.
- CSCw02257 - 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 VRF instance of both of the service device bridge domains is changed, the sucsdHealthGrp managed objects in the switch may not be created for the new VRF 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 Affe
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 -

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

## Issues Dashboard

Issues is divided into these components:

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

### Anomalies Dashboard

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

Property	Description
Anomaly Severity by Devices	Displays the number of Anomalies (internal Fabric failures) and their severity level. Clicking on the area shows detail fault information, such as <b>Devices Affected</b> , <b>Severity</b> and <b>Anomaly Score</b> .
Anomalies Affecting	Displays the number of anomalies by their type. Anomaly types include: <ul style="list-style-type: none"> <li>• Versions</li> <li>• Platforms</li> </ul>

## Browse Anomalies

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

### Filters

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

- Operators - display anomalies using an operator. Valid operators are:
  - = = - display anomalies with an exact match.
- Severity - display anomalies only for a specific severity. Valid severity's are:
  - Critical - Returns matches for critical anomalies.
  - Severe - Returns matches for severe anomalies.
  - Moderate - Returns matches for moderate anomalies.
- Type - display anomalies only for a specific type. Valid types are:
  - Control Plane - Returns matches for compliance check anomalies.
  - Management Plane - Returns matches for compliance check anomalies.
  - Data Plane - Returns matches for compliance check anomalies.
  - Traffic Check - Returns matches for compliance check anomalies.
  - Forwarding Check - Returns matches for compliance check anomalies.
  - State Validator - Returns matches for compliance check anomalies.

## Bugs Dashboard

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

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




## Devices Dashboard




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

Property	Description
Device Issues	Displays the number of devices that are past the <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> 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	 <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

<b>Issue</b>	 <b>Critical (Red)</b>	 <b>Severe/Moderate/Low (Amber)</b>	 <b>None (Green)</b>
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 Dashboard

The TAC Assist dashboard has the Connected TAC Assist feature, which lets the user collect and upload the logs for the devices in your network to Cisco Intersight cloud. It also enables Cisco TAC to trigger on-demand collection of logs for specified user devices and pull the logs from cloud.

The Connected TAC Assist has two modes:

- User initiated - The user collects the logs for specified devices and then user uploads the collected logs to Cisco cloud.
- TAC triggered - Cisco TAC triggers on-demand collection of logs for specified devices and pulls the logs from Cisco cloud.

## User Initiated Upload to Cloud

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

### Before you begin

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

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

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

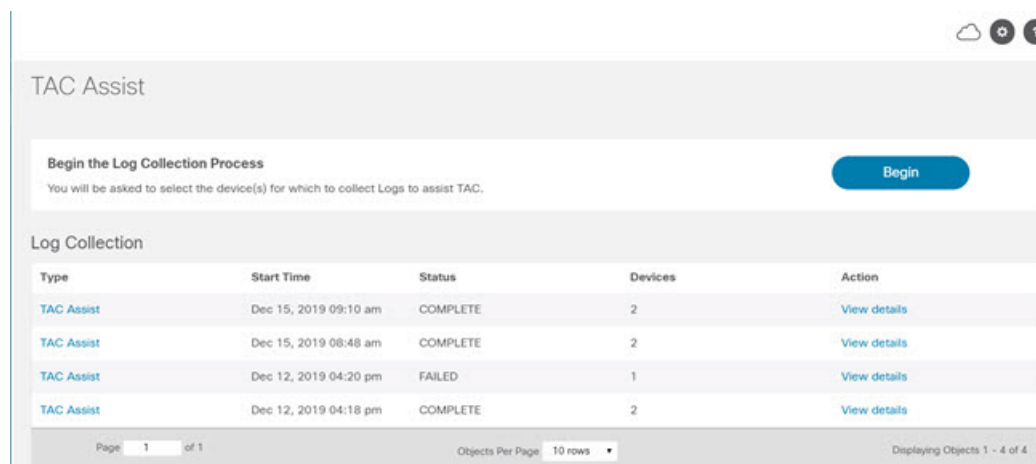
The Collect Logs dialog appears.

**Step 3** To display specific devices in the list, use the filter utility:

- Operators - display devices using an operator. Valid operators are:
  - = - display devices with an exact match. This operator must be followed by text and/or symbols that are the exact software version, product ID, device name, or assigned IP address of the device.
  - contains - display device names or platform identifiers containing entered text or symbols. This operator must be followed by text and/or symbols.
- Version - display devices that are running a specific software version.
- Platform - display devices that are a specific type defined by the platform ID.
- Device Name - display devices that are specifically named.
- IP Address - display devices that are assigned a specific IP address.

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

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



The screenshot shows the 'TAC Assist' interface. At the top right, there are icons for cloud, settings, and help. Below the title, 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 control showing 'Page 1 of 1' and 'Objects Per Page: 10 rows'. The footer of the table area says 'Displaying Objects 1 - 4 of 4'.

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

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

Job Details					
TAC Assist					
STATUS	DEVICES	FABRIC	START TIME	JOB ID	
Complete	2	mutate-fab	Dec 15, 2019 09:10:37 am	TACASSISTNWB7vifSjgNqXTTjtbA	
Logs (2 of 2 Successful)					
Device Name	Related Job ID	Status	Status Message	Log Location	Cloud
L81_STMORITZ	N/A	Success		/var/afw/vois/ceti/uploads/TACASSISTNWB7vifSjgNqXTTjtbA	Upload
ACC21_SAPORO	N/A	Success		/var/afw/vois/ceti/uploads/TACASSISTNWB7vifSjgNqXTTjtbA	Upload


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

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

## TAC Initiated Pull from Cloud

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

Click **View Details** from list of logs to display the job details page.

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.

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

The Fabric Job Configuration page appears.

2. Click **Configure** to schedule a on-demand bug scan or compliance check job for the selected fabric.

Choose the scheduled job time and date and click **Apply**.

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

To display specific devices in the list, use the filter utility:

- Operators - display devices using an operator. Valid operators are:
  - == - display devices with an exact match. This operator must be followed by text and/or symbols that are the exact time, summary, start time, status, devices, and action for the fabric.
  - contains - display device names or platform identifiers containing entered text or symbols. This operator must be followed by text and/or symbols.
- Status - display devices with a specific status.
- Summary - display devices that have a specific summary.

The **Bug Scan**: User can schedule or run an on-demand bug scan on their network. Cisco NIA app collects technical support information from all the devices and runs them against known set of signatures, and then flags the corresponding defects. Cisco NIA app also generates an advisory for the customer. For further details, see Advisories from [Advisories Dashboard, on page 2](#).

The **Compliance Check**: User can schedule or run an on-demand Compliance Check on their network. Cisco NIA app collects technical support information from the selected devices and runs them against known set of signatures, and then flags the defects that are not compliant. Cisco NIA app also generates an anomaly list for the customer. For further details, see Anomalies from [Issues Dashboard, on page 6](#) and view the anomaly details.

