



# Cisco Network Assurance Engine Getting Started Guide, Release 4.0(1)

# Table of Contents

Cisco Network Assurance Engine GUI .....	3
Overview of the GUI .....	3
Cisco NAE GUI Icons .....	3
Settings Menu .....	6
Timeline .....	7
Summary Boards Area .....	8
Hot Topics Area .....	8
Global Search .....	9
Smart Events Area .....	11
Exporting Data from the GUI .....	12
Perform Analysis .....	13
Assurance Control Modes .....	13
Performing Online Analysis .....	13
Performing Offline Analysis .....	15
Offline Data Collection Script .....	16
Schedule Assurance Group Analysis .....	17
Cisco Network Assurance Engine Licensing .....	18
Cisco NAE License .....	18
Updating License .....	19
Cisco Network Assurance Engine User Access and Authentication .....	20
User Access and Authentication .....	20
Creating a User Account .....	20
Prerequisites for LDAP .....	20
Creating a New Authentication Domain .....	21
Explorer .....	23
About Explorer .....	23
Use Cases .....	24
Workflow .....	24
Guidelines and Limitations .....	26
Creating a Query .....	27
Viewing What or Can Query Results .....	28
Viewing View Query Results .....	29
Supported Queries .....	31
Epoch Delta Analysis .....	38
Epoch Delta Analysis .....	38
Guidelines and Limitations .....	39
Creating Epoch Delta Analysis .....	39
Viewing Delta Analysis Results .....	40

Viewing Health Delta Analysis .....	40
Viewing Policy Delta Analysis .....	41
Compliance Analysis .....	43
Compliance Analysis Tab .....	43
Manage Compliance .....	44
Manage Compliance Tab .....	44
Creating Object Selector .....	44
Creating Traffic Selector .....	45
Creating Compliance Requirement .....	46
Creating Compliance Requirement Set .....	48
Smart Event Management .....	49
Smart Event Dashboard .....	49
Lifecycle of a Smart Event .....	49
Smart Event Suppression .....	52
Smart Event Suppression Workflow .....	52
Creating New Event Rule .....	54
Creating New Event Ruleset .....	54
Managing Cisco Network Assurance Engine .....	56
Managing User Accounts .....	56
Managing Passphrase .....	56
Managing Appliance Settings .....	57
Managing Assurance Groups .....	58
Managing Offline Analysis .....	59
Setting Log Levels .....	59
Viewing Data Storage Usage .....	60
Deleting Bundle File .....	60
Managing Epoch Delta Analysis .....	60
Managing Authentication Domains .....	61
Managing Object Selectors .....	61
Managing Traffic Selectors .....	62
Managing Compliance Requirements .....	62
Managing Compliance Requirement Sets .....	63
Managing Event Rules .....	63
Managing Event Rulesets .....	63
Troubleshooting .....	65
Downloading Logs .....	65
Appliance Events .....	65
Appliance Event Types .....	65
Troubleshooting Scenarios .....	68

First Published: 2019-08-26

Last Modified: 2019-11-08

**Americas Headquarters**

Cisco Systems, Inc.

170 West Tasman Drive

San Jose, CA 95134-1706

USA

<http://www.cisco.com>

Tel: 408 526-4000

800 553-NETS (6387)

Fax: 408 527-0883

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

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

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

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

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

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

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

© 2017-2019 Cisco Systems, Inc. All rights reserved.

# Cisco Network Assurance Engine GUI

## Overview of the GUI

The Cisco NAE GUI is a browser-based graphical user interface that communicates internally with the Cisco NAE software engine by exchanging REST API messages. At the top of the GUI are several tabs, and each tab expands to reveal subtabs. Choosing a subtab opens the respective inspector page. An inspector page provides information about the smart events for the respective portion of your network. Each inspector page generally has several areas and panes, and multiple dashlets in the areas.

On most pages, you can jump to the different areas by clicking the corresponding circular button in the middle of the right edge of the page. The blue circle is the currently-displayed area.

A dashlet is a small panel that provides a summary of a specific type of information that relates to the content of a page. The exact layout varies by inspector page.






























The GUI contains the following pages:































- Dashboard tab—Provides a high-level overview of the health of the fabric.
- Change Management tab
  - Policy Analysis—Provides information about the assurance on policy analysis changes.
- Epoch Delta tab—Provides information about the state of the fabric between two epochs.
- Policy CAM tab—Provides information about the Policy CAM utilization in the Assurance Group.
- Compliance tab—Provides information about the state and health of the IT infrastructure.
- Smart Events tab—Provides information about all of the smart events.
- Explore tab—Enables you to discover assets and their object associations in an easy-to-consume natural language query format.
- Global Search icon—Locates objects that you specify in the **Search** field, and the results appear below the **Search** field.
- Assurance Group drop-down list—Enables you to choose which assurance group to analyze. Green color icon indicates an active Assurance Group.
- Settings menu—Enables you to perform various miscellaneous tasks, such as configure an assurance group, configure the log level settings, perform an offline analysis, manage users, view the REST API documentation, and see information about your installation of the Cisco NAE.
- User menu—Enables you to change your password, edit user account, or log out of the Cisco NAE.

## Cisco NAE GUI Icons









The following table provides a description of the Cisco NAE GUI icons.

Table 1. Cisco NAE GUI Icons

Icon	Description
	A button that adds a virtual machine.
	A button that removes a virtual machine.
	A button that displays more options for a dashlet. In most cases, the options enable you to toggle a dashlet's view between the grid view and chart view.
	A button that closes an overlay or removes data.
	An icon that indicates a drop-down list.
	A button that opens the form to edit data.
	A button that opens the form to view details.
	A button that provides helpful tips.
	An icon that indicates information events.
	An icon that indicates minor events.
	An icon that indicates major events.
	An icon that indicates critical events.
	An icon that indicates warning events.
	A button that closes a mode.
	A button that plays or starts data fetching.
	A button that stops data fetching.
	A button that refreshes a page or dashlet.
	A button that opens the settings menu.
	A button that opens the global search form.
	An icon that indicates a server issue.
	A button that expands the Policy CAM bar.
	A button that expands the Events Trend dashlet.
	A button that collapses the Events Trend dashlet.
	A button in the <b>Settings</b> menu that opens a form that displays information about the installed Cisco NAE software build.
	A button in the <b>Settings</b> menu that opens the assurance control configuration form.
	A button in the <b>Settings</b> menu that opens the appliance status form.
	A button in the <b>Settings</b> menu that opens the appliance settings form.
	A button in the <b>Settings</b> menu that opens the offline file management form.
	A button in the <b>Settings</b> menu that opens the offline analysis form.

Icon	Description
	A button in the <b>Settings</b> menu that opens the user management form.
	A button in the <b>Settings</b> menu allows you to download tech support logs.
	A button in the <b>Settings</b> menu that allows you to download offline collection script.
	An icon in the radial view of the visualization area that indicates an endpoint group.
	An icon that you hover the mouse cursor over to see legend information.
	An icon in the Timeline area that goes back to the previous epoch selection.
	An icon in the Timeline area that displays the oldest epoch.
	An icon in the Timeline area that displays the latest epoch.
	An icon in the Timeline area that displays the next epoch.
	An icon in the Timeline area that displays the previous epoch.
	An icon that customizes the columns in a table.
	An icon that indicates that the table can be sorted.
	An icon that indicates allows you to change the order of a column in a table.
	An icon that indicates a selected object.
	A button for Assurance Group List view
	An icon for Assurance Group In progress / running indicator
	An icon for Assurance Group Status indicator
	A button for Assurance Group Tile / Card view
	An icon for an epoch that was generated prior to Cisco NAE release 4.0(1)
	An icon for an epoch where the smart event is cleared
	An icon for an epoch where the smart event is clearing
	An icon for an epoch where the smart event is raised
	A button to move to next
	A button to move to previous
	An icon to indicate a filter
	An icon to indicate Policy CAM utilization > 90%
	An icon to indicate Policy CAM utilization 0% - 60%
	An icon to indicate Policy CAM utilization 75% - 90%
	An icon to indicate Policy CAM utilization 60% - 75%
	A button for date selection



Icon	Description
	A button for time selection or scheduled
	A button to view the Cisco NAE Fundamentals Guide
	A button to view the Cisco NAE Getting Started Guide
	A button to view the Cisco NAE Release Notes
	A button to view the Cisco NAE Rest API Swagger Interface
	A button to view the Cisco NAE Smart Events Reference Guide
	A button to view the Cisco NAE REST API User Guide
	A button to view the Cisco NAE Installation and Upgrade Guide

## Settings Menu

The **Settings** menu enables you to perform various tasks, such as configure an assurance group, configure the log level settings, perform an offline analysis, manage users, view the REST API documentation, and see information about your installation of the Cisco NAE. The menu contains the following items:

- **Assurance Groups**—Enables you to add, delete, or modify an assurance group.
- **Download Offline Collection Script**—Downloads the offline collection script.
- **Offline File Management**—Enables you to upload previously-downloaded fabric data so that you can use the Cisco NAE in offline data analysis mode. You can also delete offline data.
- **Offline Analysis**—Enables you to perform offline data analysis. Cisco NAE provides one-time assurance of the offline data.
- **Appliance Administration**—Displays details of the Cisco NAE appliance cluster such as information about each individual virtual machine in the cluster, software version installed, the configured log level settings for the appliance, the disk usage, and authentication domain details.
- **Appliance Status**—Displays the smart events that relate to the appliance.
- **User Management**—Enables you to create user accounts and change the password of the accounts.
- **Download Tech Support Logs**—Downloads the tech support logs as a .tar file to your local system.
- **License**—Enables you to update an Cisco NAE license.
- **Appliance Documentation**—Enables you to view and download Cisco NAE documentation.
- **About Cisco Network Assurance Engine**—Displays information about your installation of the Cisco NAE.

# Timeline

The timeline is located near the top of the inspector pages. The timeline shows the date and time of data collection (not analysis). Data is represented by dots on the timeline, which are referred to as epochs.

An epoch is a period of time in your network's history during which the Cisco NAE collected and analyzed data. The size of the epoch gives a rough indication of the quantity of smart events at that time, with a larger epoch indicating more smart events.

An epoch can be one of the following colors:

- Gray—This indicates normal operation containing info events.
- Flashing Blue—This indicates that the Cisco NAE is currently running an analysis on the data.
- Red—This indicates critical errors are detected for an EPOCH during online analysis.
- Blue—This indicates an analysis based on offline data collection.

By default, the timeline shows a time range of 2 hours and 45 minutes with markings at 15 minute intervals to give you an estimate of when the data collection occurred. You can hover the mouse cursor over an epoch to see the exact time that the data collection occurred.

To export data, click **Export Data**. This allows you save the data collected for a selected EPOCH during online analysis for offline analysis at a later time.

You can change the time range by clicking one of the preset time durations under the timeline, or you can click **Custom** to specify a time range of your choice. Optionally, you can hover over an epoch to highlight it (do not click the epoch), then click and drag the mouse cursor over the timeline to choose that area as the custom time range. You can scroll backward or forward in time by intervals of the chosen time range (with a default of 2 hours and 45 minutes) by clicking the left or right arrow buttons that are located at either end of the timeline.

The date and time displayed to the right of the timeline represents the date and time of the currently chosen epoch. Use the arrows under the timeline to go to the first epoch, go to the previous epoch, go to the next epoch, or go to the last epoch. The **Live Updates** button sets the timeline to display the current date and time. The **Epochs with my events** button sets the timeline to display the epochs that contain one or more events that have been assigned to a particular user.



When you assign an event from one user to another, the events are not reflected in the **Epochs with my events** timeline immediately. To view the epochs with reassigned events you must either refresh the page or select a different Assurance Group.

We recommended that you view less than 500 epochs at one time. If you have a lot of epochs in a selected time-range, you can drag on the timeline to zoom into a smaller time window.

# Summary Boards Area

The summary boards area provides a broad view of the issues that the Cisco NAE discovered in the fabric. For most pages, the summary boards area consists of the first two rows of dashlets. The exact composition of the summary area varies by page. For example, the **Policy CAM** page has one row for Summary Board, while the **Policy Analysis** page under **Change Analysis** has more rows.

For most pages, the dashlet in the first row provides the number of each type of smart event. The following list provides the types of events:

- **Critical**—Critical smart events indicate issues that you must address as soon as possible.
- **Major**—Major smart events indicate serious issues that do not stop your Assurance Group from functioning, but you should address them as soon as possible.
- **Minor**—Minor smart events indicate issues that are not serious, but you should address them eventually.
- **Warning**—Warning smart events indicate things that are not issues now, but they have the potential to become issues later.
- **Info**—Info smart events generally indicate objects that are healthy. A low number of info smart events can indicate that there are issues in the fabric, while a high number of info smart events can indicate that most objects are healthy.
- **Total**—The total number of smart events of all types on the page.

The second row usually contains two dashlets. The second row provides a different way (compared to the first row) of categorizing the issues.

# Hot Topics Area

The hot topics area usually consists of a group of two or three dashlets. The exact number of dashlets varies by page.

The hot topics area helps you to determine which issues to resolve first by listing the objects of a particular type (leaf switches, tenants, endpoint groups, or application profiles) that have the most issues.

For the inspector pages with dashlets, the dashlets display the top four or five objects that have the most issues of the type indicated by the dashlet's title, such as endpoint counts or route count. The title of each dashlet is a drop-down list that you can use to change the type of object for which the dashlet displays data.

You can click a violations count in a dashlet to go to the Smart Events area and have the area display more information about Smart Events of the appropriate severity type for the appropriate type of object.

# Expanded Dashlet View

At the bottom of each dashlet is a link that opens a page with an expanded dashlet view. The expanded view displays the same data for all objects (not just the top four or five) of the type that is

appropriate for the dashlet. You can choose the type of object using the title drop-down list.

Some of the columns have a search field in which you can type a string, which narrows the table to only those objects whose values contain the string for that column's parameter.

You can sort the table by one of the columns in descending or ascending order by clicking the **Sort** button next to the column's header. Clicking the button multiple times cycles through the sort options, and clicking on a different column's sort button resets the previous column's sort order and sorts the table by the new column. Optionally, you can hold **Shift** and click more than one of the **Sort** buttons to sort by multiple columns.

You can click a violations count to close the expanded dashlet view, go to the Smart Events area, and have the area display more information about Smart Events of the appropriate severity type for the appropriate type of object. Also, in the visualization area, the filter becomes set to filter for the Smart Events of the object that you clicked and the **View Control** options get set based on what you clicked. You can use this functionality only if the violation count is greater than 0.

## Global Search

Global Search searches for objects (across multiple epochs) that you specify in the **Search** field. When you click in the **Search** field, you can search by resource name or DN. Clicking again in the **Search** field, allows you to add additional resource names or DNs to further qualify your search.


The results of the Global Search appear in three tables below the **Search** field.


- All Smart Events: Contains Smart Events data.
- Tenant Endpoint Details: Contains endpoint data.
- Prefix Table: Contains L3 forwarding data.

## Performing Global Search

Use this procedure to perform a global search.

### Procedure

1. Launch Global Search by clicking the global search icon  (located in the upper right of the NAE GUI)
2. Click date/time (left of the **Search** field) to display the the pop-up window to configure the From date/time or To date/time period for the search.
  - You can configure the date by clicking a specific day in the calendar that appears.
  - You can configure the time by clicking the time field and adjusting the time of day in the time pop-up window. The number of epochs that exist in the configured time period appears below the calendars.
3. Click **Apply** to save your From date/time and To date/time specifications.
4. Click the **Search** field to specify the objects to search for.
  - Each additional unique object adds a logical AND condition to the global search.

- Each additional non-unique object adds a logical OR condition between the same object type to the global search.
- As each object is added to the search field, the global search feature provides search results dynamically.
- You can clear all the search objects from the **Search** field by clicking the remove data icon  (located at the right side of the search field).

## Guidelines and Limitations

The following apply to performing a global search:

- The maximum number of search parameters is 25.
- The default From date/time through To date/time period is one day.
- The maximum number of epochs that global search supports is 288 epochs or up to 3 days.
- A search for all objects (blank search) is done by not specifying search objects, clicking the search field, and pressing the Enter key.
- Global Search (Cisco NAE release 4.0(1) and later) supports searching for Cisco ACI GOLF routes by specifying the Route object. The results of the global search appear in the Prefix Table with an External dynamic (golf) subnet type.
- Depending on the global search results, multiple rows may be displayed for same event, prefix or endpoints in the global search result tables.

## Viewing Global Search Results

The tables below the **Search** field contain the global search results:

Table	Description
All Smart Events	Smart Events data
Tenant Endpoint Details	Endpoint data
Prefix Table	L3 forwarding data

## Guidelines and Limitations

The following apply to viewing results of a global search:

- You can filter the Global Search results by clicking the filter icons located above the timeline. A highlighted icon enables the filter, such as for a specific severity or for a specific event category.
- You can select an epoch by clicking an indicated epoch located on the timeline below the **Search** field.
- The timeline that appears with Global Search does not have the zoom in/zoom out controls as the timeline that appears in each of the tabs of the NAE GUI. Instead, highlighting a group of adjacent epochs on the Global Search timeline magnifies the scale of the timeline (zoom in). Clicking the dates to the right of the timeline resets the timeline scale.
- Epochs that appear on the timeline as a solid color icon indicate epochs that were created with

Cisco NAE release 4.0(1) or later releases. Epochs that appear on the timeline as a 2-color icon (🟡🟢) indicate epochs that were created with Cisco NAE release 3.1(1) or earlier releases.

- Global search does not support configuring a search containing epochs that were created with Cisco NAE release 3.1(1) or earlier releases with epochs that were created with Cisco NAE release 4.0(1) or later releases.
- Search results that contain smart events related to Cisco ACI GOLF routes (Cisco NAE release 4.0(1) and later), can be displayed by entering GOLF in the filter field of the Subnet/Route column in the Prefix Table.
- When viewing All Smart Events:
  - Click **Aggregated** to view the aggregated Global Search results organized by smart events in the Event Name column.
    - Click a smart event in the Event Name column to view every individual occurrence of the smart event across epochs.
  - Click **Individual** to view every individual occurrence of the smart event across epochs.
    - Click a timestamp in the Epochs column to view the lifecycle and details of the smart event that occurred in that epoch.


## Smart Events Area

By default, the smart events area lists all of the smart events that are relevant to the inspector page. For example, the smart events area of the **Policy Analysis** inspector page shows policy analysis smart events. The title of the table indicates the total quantity of smart events that are on the table. For example, a title of "Policy Smart Events by Severity" displays the policy smart events.

The columns of the smart events table vary depending on the inspector page, although all smart events tables have the following columns:

- **Severity**—The severity type of the smart event, represented by the icon for that severity type. This column has a search field that enables you to filter for smart events of the severity type that you specify. Enter the severity type as a string in the field. The possible severity types are as follows:
  - Critical
  - Major
  - Minor
  - Warning
  - Info
- **Event Category**—The Category for the smart event.
- **Event Subcategory**—The subcategory for the smart event.
- **Event Name**—The code for the smart event.
  - You can click a code to expand the row to display the additional information about the smart event. Depending on the settings for displaying smart event attributes, a table with Epochs

information is displayed for each instance of the smart event.

You may export the information in the smart events table. Clicking the **Settings** icon  allows you to specify an export to CSV or to JSON.

At the bottom right of the smart smart events area, you can choose how many rows to display on a page.

See the *Cisco Network Assurance Engine Smart Events Reference Guide* for more information.



If the event suppression feature is activated, the smart event count and the smart events listed take into account the event rules.

See [About Smart Event Suppression](#) for more information.

## Exporting Data from the GUI

Starting from Cisco NAE release 2.1(1), you can export the data from certain tables in the GUI to JSON and CSV format.

Exporting the data from all the **Smart Events** tables in the GUI is supported.



The export of the Prefix table or the Endpoint Details table in the GUI is not supported in Cisco NAE release 4.0(1).

To export data to the JSON format, navigate to the table in the inspector page and then choose **Table Settings > Export to JSON**.

To export data to the CSV format, navigate to the table in the inspector page and then choose **Table Settings > Export to CSV**.

### Important Notes

- The data from all the columns in the table are exported irrespective of the columns selected in the **Column Customization** setting for the table.
- Ordering the table columns using the **Column Customization** setting does not affect the order of the columns when the data is exported.
- In each export instance you can export the data contained in 10,000 rows. To export the data from a table containing more than 10,000 rows, you must select the rows containing the dataset to be exported.

# Perform Analysis

## Assurance Control Modes

Cisco NAE assurance control capability enables you to analyze the Assurance Group in two modes, online analysis and offline analysis.

An Assurance Group is comprised of the entire ACI fabric. An ACI fabric is made up of the APIC host and all leaf switches and spine switches controlled by the APIC controller. All the network nodes (APIC controller, leaf switches and spine switches) are analyzed together as part of the Assurance Group.

Assurance control involves collecting data from the Assurance Group, running the analysis to create a model with the collected data, and generating the results. The results are then displayed on the **Dashboard**.

Online analysis provides assurance on the Assurance Group in real time. In online analysis data collection, model generation, and results generation are carried out simultaneously. In the online mode the collected data is analyzed immediately after collection followed by result generation. This is repeated after a fixed time interval as specified by the operator.

Offline analysis provides a one-time assurance of the Assurance Group. Offline analysis offers the flexibility of decoupling the data collection stage from the analysis stage. In offline analysis data is collected using a Python script and the collected data is then uploaded to Cisco NAE to provide one-time assurance. The collected data can also be analyzed at a later time. It enables the operator to collect the data during change management windows and then perform the analysis. It also fulfills compliance requirements of an organization.

Beginning with release 4.0(1), you can analyze multiple Assurance Groups. See [Schedule Assurance Group Analysis](#) for more information.

## Performing Online Analysis

An Assurance Group provides Intent Assurance for a group of entities at the same time. Assurance Group configuration allows you to configure the entities that need to be analyzed together. Performing online analysis allows the Cisco NAE to collect data from the Assurance Group, build a model with the collected data, and generate results. The results are displayed on the **Dashboard** as Epochs.

Use this procedure to perform online analysis.

### Before You Begin

- You must have the credentials to access the APIC hosts.
- APIC admin writePriv privileges allow information collection on the APIC host and leaf switches. You must have APIC admin writePriv privileges to configure export policy.



## Procedure

1. Choose **Settings > Assurance Groups**.
2. Click **Create New Assurance Group**.
3. Complete the following fields for **Create New Assurance Group**.
  - a. In the **Name** field, enter the name.
  - b. In the **Description** field, enter the description.
  - c. Check the **Switch to online mode** check box, to automatically analyze the Assurance Group in real time. Ensure that **Switch to online mode** check box is selected.
  - d. In the **Username** field, enter the user name to access the APIC hosts.
  - e. In the **Password** field, enter the password to access the APIC hosts.
  - f. From the **Analysis Interval** drop-down list, choose the interval to run the analysis. Analysis interval includes the time to collect data from APIC and the switches, analyze the data to build a model, generate results, and display them on the Dashboard. For production environments, the recommended analysis interval is a minimum of 15 minutes. An interval below 15 minutes should be used only in lab environments or for testing.
  - g. From the **Analysis Timeout** drop-down list, choose the time the system needs to wait before terminating the analysis. This value should be greater than the **Analysis Interval**.
  - h. Check the **Start Immediately** check box, to start the analysis of the selected Assurance Group immediately.
4. Complete the following fields for **APIC Hosts**.
  - a. In the **APIC Hostname 1** field, enter the APIC host name in the format apic1.example.com.
  - b. Click + to add another APIC host name. We recommend that you add all the APIC hosts to the Assurance Group.
5. Complete the following fields for **Collection Settings**. Collection settings are required for NAT and epoch delta analysis. See [Creating Epoch Delta Analysis](#). See [Management and Network Connectivity](#).
  - a. Check the **Use APIC Configuration Export Policy** check box, to export configuration policy for policy delta.
  - b. Click **Show**.
  - c. Select the **Export Format**.
  - d. In the **Export Policy Name** field, enter policy name.
  - e. Check the **Use NAT Configuration File** check box, to upload a file that has the Network Address Translation (NAT) table.
  - f. Click **Show**.
  - g. Click **Download NAT Configuration File Template**.
  - h. Enter the public and private IP address mapping in the NAT configuration CSV file to indicate the NAT translation that needs to be used to access the APIC hosts.
  - i. Click **Browse** to upload the CSV formatted NAT configuration file containing the public and

private IP address mapping to be used to access the Assurance Groups.

j. In the **File Name** field, enter the file name and click **Upload**.

6. Click **Save**.

7. The status of the analysis is displayed in the Data Collection form. Cisco NAE performs analysis on only one fabric at a time. To perform analysis on another fabric, you must stop the analysis on the current fabric and then start the analysis on another fabric. You can perform the following actions:

- Click the play icon to start the analysis.
- Click the stop icon to stop the analysis.
- See [Managing Assurance Group](#).

8. To view the results of the analysis, click **Dashboard**. See [Timeline](#). Ensure that you have the correct Assurance Group selected to view the results. Click **Assurance Group** and select the Assurance Group from the drop-down list.

9. To export data, select a epoch dot on the timeline and click **Export Data**.

## Performing Offline Analysis

Use the procedure to perform offline analysis. See the [Offline Data Collection Script](#) for information about the Offline Data Collection Script.

### Procedure

1. Choose **Settings > Download Offline Collection Script** to download the python script.
2. Run the downloaded script to collect the data for assurance. See README for more information.



The python offline data collection script is only supported on Mac OS or CentosOS. Running the script from a Windows server will result in an error and Cisco NAE will indicate that the APIC version is unsupported.

3. Choose **Settings > Offline File Management** to upload the collected data.
4. Click **Create New Upload**.
5. In the **Create New Upload** form, complete the following fields.
  - a. Click **Browse** to upload the collected data to provide one-time assurance.
  - b. In the **Name** field, enter the name of the file.
  - c. In the **Description** field, enter the description.
6. Click **Submit**. After the file has been uploaded successfully, it is displayed in the Upload table.
7. Choose **Settings > Offline Analysis**.
8. In the **New Offline Analysis** form, complete the following fields.
  - a. In the **Analysis Name** field, enter the name of the offline analysis.
  - b. From the **File** drop-down list, choose the file with the collected data.

- c. From the **Assurance Group** drop-down list, choose the Assurance Group.
  - d. (Optional) Click + to add another Assurance Group. Use this form if you want to define a new Assurance Group.
  - e. From the **Analysis Timeout** drop-down list, choose the time the system needs to wait before terminating the analysis. You can also enter the time the system needs to wait before terminating the analysis.
9. Click **Run** to run the offline analysis. After the offline analysis is completed, the status is displayed in the **New Offline Analysis** form. Cisco NAE performs analysis on only one fabric at a time. To perform analysis on another fabric, you must stop the analysis on the current fabric and then start the analysis on another fabric.
10. To view the results of the analysis, click **Dashboard**. See [Timeline](#).

## Offline Data Collection Script

The Cisco Network Assurance Engine offline data collection script is a Python script that polls the Cisco Application Policy Infrastructure Controllers (APICs), spine switches, and leaf switches for a series of REST API and CLI calls. For information about the REST API calls and CLI calls, see the `readme.md` file that is included with the script.

The script has the following dependencies:

- Python 2.7.11+
- Ubuntu/OS X /Cent OS
- Python dependencies
  - Requests (Python REST library)
  - Paramiko (Python SSH library)
  - Setuptools (Python packaging library)

See the `readme.md` file for information on the Python dependencies and the process to install the dependencies in a virtual environment. The `readme.md` file provides the complete list of objects and show commands collected from the Cisco APIC, spine switches, and leaf switches. The `readme.md` file is available inside the same zip file with the offline analysis script file. The offline analysis script is downloadable directly from the Cisco NAE appliance from the settings menu.

The workstation on which the script is being launched must have out-of-band management connectivity to the Cisco APICs, leaf switches, and spine switches. Make sure that every node in the Cisco ACI fabric has an out-of-band management IP address configured. Make sure that the firewall does not block HTTPS (for using the REST API) and SSH (for connecting to the leaf switches and spine switches). Make sure that the proxy settings are properly set to allow HTTPS connections.

The `readme.md` file provides the syntax for using the script. By default, the script will run 3 iterations of the data collection at a 5 minute interval between iterations, although you can specify the number of iterations by using the **-iterations** option. The total expected collection time ranges between 18 to 20 minutes from start to finish for 3 epochs for a fabric with around 20 leaf switches. Larger fabrics will take longer time depending on complexity of the configuration and scale of the

fabric.

## Schedule Assurance Group Analysis

Starting from release 4.0(1), you can schedule an analysis for multiple Assurance Groups sequentially. When you schedule an analysis for multiple Assurance Groups, the analysis is performed using the round-robin scheduling algorithm.

### Important Notes

- Scheduling analysis for multiple Assurance Groups is only supported for online analysis.
- The Assurance Groups must be located in the same data center.
- You can schedule the analysis for up to four Assurance Groups.
- Stop any analysis on the Assurance Group before creating a schedule.

### Procedure

Use this procedure to schedule the analysis for Assurance Groups.

1. Choose **Settings > Assurance Groups**.
2. (Optional) In the Assurance Group page, click the **Sort** icon to sort the Assurance Groups by Name, Operational Mode, or Schedule.
3. Click **Schedule** located on the right side of the **Assurance Groups** page.
4. In the **Analysis Interval** field, choose the desired interval. The analysis interval enables you to schedule the wait time between the scheduled Assurance Group runs. The default analysis interval is 15 minutes. The interval value must be between 5 mins to 24 hours in multiples of 5 mins.
5. Select the Assurance Groups. You cannot schedule an analysis for Assurance Groups running offline analysis.
6. In the **Timeline**, the scheduled order of the Assurance Groups and the approximate time to run the analysis is displayed. Review the schedule and click **Activate**.

# Cisco Network Assurance Engine Licensing

## Cisco NAE License

Starting with Cisco NAE release 2.1(1a), licensing is enabled in Cisco NAE. Cisco NAE software will offer full functionality for a period of 30 days after installation. After this period expires, data collection and analysis will continue in Cisco NAE release 2.1(1a), but in subsequent releases the analysis will stop.

Starting with Cisco NAE release 4.0(1), after the expiry of the trial license (30 days after installation), the analysis will stop. Users are urged to request a license as soon as Cisco NAE is installed.

The types of licenses available for Cisco NAE include:

- Trial license: Allows the use of Cisco NAE software for a period of 30 days. Allows the use of Cisco NAE to conduct a Proof of Value trial.
- Production license: Allows the use of Cisco NAE software for the term specified in the purchase contract.
- Not-For-Resale (NFR) license: Valid for a period of 365 days from the date of installation. This license is available for partners ONLY to train and get familiar with the software. This is an unlimited feature license available at no cost to the partner.

## Workflow For Obtaining Cisco NAE License

1. After Cisco NAE is installed, a Trial license is automatically enabled. The Trial license is valid for a period of 30 days.
2. Contact your account representative to request for a valid license before the Trial license expires.
3. Choose **Settings** > **About Network Assurance Engine**, to obtain the Appliance ID and Appliance Model information.
4. Provide the following details when you request for a valid license.
  - a. Appliance ID
  - b. Customer Name
  - c. License Type
  - d. Appliance Model
5. Upload the valid license to Cisco NAE. See [Updating License](#).

# Updating License

Use this procedure to update the Cisco NAE license.

## Procedure

1. Choose **Settings > License**.
2. Click **Update License**.
3. In the **Upload License File**, click **Browse** to upload a valid license (.tar) file as is.
4. Click **Upload**.



## Upload License File

File  nae\_license\_CiscoLab\_2019-06-22\_08-11-45.367231.tar

File Name

The License details are displayed on the **License Page**

# Cisco Network Assurance Engine User Access and Authentication

## User Access and Authentication

In Cisco NAE, an administrator can choose to configure users on the Cisco NAE appliance itself and not to use external AAA servers. These users are called local users. To configure local users, see [Creating a User Account](#).

Cisco NAE also allows administrators to grant access to users configured on externally managed authentication servers such as Lightweight Directory Access Protocol (LDAP). To authenticate users with an LDAP server See [Creating a New Authentication Domain](#).

A login domain defines the authentication domain for a user. Login domains can be set to the Local, or LDAP. When accessing the UI, the Cisco NAE offers a drop-down list of domains to enable the user to select the correct authentication domain. The default is Local.

## Session Management

In Cisco NAE, you can view or delete active user sessions using the REST API. These operations cannot be performed using the GUI.

See the *Cisco Network Assurance Engine REST API User Guide* for more information.

## Creating a User Account

Use this procedure to create a new user account. Only an administrator can create a user.

### Procedure

1. Choose **Settings > User Management**.
2. Click **Create New User Account**.
3. Complete the following fields for **Create New User Account**.
  - a. In the **Email** field, enter the email address of the user.
  - b. In the **Username** field, enter the username of the user account.
  - c. In the **Password** field, enter the password to access the user account.
  - d. Click **Save**.

## Prerequisites for LDAP

LDAP has the following prerequisites:

- You have configured the LDAP server.
- You have the created the Cisco NAE users on the LDAP server.

- You have created a group for Cisco NAE users.
- You have added the Cisco NAE users to the group.
- You have the base DN, bind DN, and group DN on the LDAP server.

## Creating a New Authentication Domain

Use this procedure to create a new authentication domain. Only an administrator can create an authentication domain.

### Before You Begin

- You have the host name or IP address, port number, bind DN, base DN, and group DN of the LDAP server.

### Procedure

1. Choose **Settings > Appliance Administration**.
2. Click the details icon on the **Authentication Domains** tile.
3. Click **Create New Authentication Domain**
4. Complete the following fields for **Create New Authentication Domain**.
  - a. In the **Name** field, enter the name of the authentication domain.
  - b. (Optional) In the **Description** field, enter the description of the authentication domain.
  - c. From the **Authentication Type** drop-down list, choose the authentication type such as LDAP.
5. Complete the following fields for **LDAP Server Configuration**.
  - a. In the **Hostname** field, enter the hostname or the IP address of the LDAP server.
  - b. (Optional) Click + to add another hostname. You can configure a maximum of 3 LDAP servers.
  - c. Check **LDAPS** check box to connect to the LDAP server using a secure connection.
  - d. In the **Port Number** field, enter the port number of the LDAP server. The valid port range is 0-5535.
  - e. (Optional) In the **Bind DN** field, enter the bind DN in the format `cn=NAE User,ou=Systems,ou=IT,ou=Departments,dc=nae_customer,dc=com`.
  - f. (Optional) In the **Bind Password** field, enter the bind DN password.
  - g. In the **Base DN** field, enter the base DN in the format `dc=nae_customer,dc=com`.
  - h. In the **Timeout** field, enter the timeout in seconds. The valid timeout range is 0-15 seconds for each host.
  - i. In the **Group DN** field, enter the group DN for the Cisco NAE users in the format `cn=NAE group,ou=groups,dc=nae_customer,dc=com`. Only the users belonging to the LDAP group will be granted access to the appliance.
  - j. In the **Filter** field, enter the filter in the format `(&(objectclass=person)(cn=$userId))`. Filter



is used as a criteria to search for the user in the LDAP server.

k. The **Attribute** field, is pre-populated.

l. Click **Test Connection** to test the connection for the LDAP server.

i. From the **LDAP Server** drop-down list, choose the LDAP server.

ii. Enter the username and password to test the credentials on the LDAP server.

iii. Click **Test**.

6. Click **Save**.

# Explorer

## About Explorer

The **Explorer** feature in NAE analyses a policy snapshot from the Cisco APIC to enable data center operators and architects to:

- Explore the ACI object models and associations
- Verify connectivity and segmentation between network assets

The **Explorer** feature allows network operators to discover assets and their object associations in an easy-to-consume natural language query format. Operators can quickly get visibility into their infrastructure and connectivity or segmentation between assets. The **Explorer** feature allows operators to easily discover associations between traditional networking constructs such as VRFs, subnets, VLANs to the ACI object model.

The Explorer feature is based on natural language query interface. The types of queries supported by the feature include:

- **What Query:** Answers how the different ACI networking entities are related to each other.

Example:

1. What EPGs are associated with VRF: */uni/tn-secure/ctx-secure*
2. What EPs are associated with INF: *topology/pod-1/paths-101/pathep-[eth1/3]* or VRF: *uni/tn-secure/ctx-ctx1*
3. What EPGs are associated with BD: *uni/tn-secure/BD-BD1* and LEAF: *:topology/pod-1/node-103*

- **Can Query:** Answers whether the entities in the ACI policy can communicate with each other. Can queries can also be used to determine if the entities in the ACI policy can communicate using protocols such as TCP, UDP, or ICMP and the source and destination ports used for communication.

Example:

1. Can entity *A* talk to entity *B*.
2. Can EPG: *uni/tn-secure/ap-AP0/epg-B* talk to EPG: *uni/tn-secure/ap-AP0/epg-A* on tcp dport: *80* sport: *10*

- **How Query:** Provides details on the communication between the entities in the ACI policy.

Example: How does EPG *X* talk to EPG *Y*.

- **View Query:** Provides the visual indication of the interface status for any leaf switch in the assurance group.

Example: View interfaces on leaf *X*.

# Use Cases

- **Design verification:** Ad-hoc query model enables operators to quickly understand and reason about their infrastructure. The natural language query model returns search results and associations in an easy to understand tabular format. In a single concise view, operators are able to answer design verification questions or discover deviations from organizational best practices.
- **Lightweight book-keeping:** Administration and maintenance teams can provide on demand visibility into the current state of their policy and networking infrastructure allowing inventory, book-keeping, and asset tracking procedures to be lightweight.
- **Connectivity and Segmentation:** Easily answer connectivity questions between a pair of assets or containers of assets. For example, if a group of EPGs needs to be quarantined, the Can query can quickly answer if policy has been correctly setup.

# Workflow

The **Explorer** page provides a consolidated view of all the security, forwarding, and endpoint issues based on the query.

It enables you to explore the connectivity between entities by creating a query. The Can query determines if the entities can communicate with each other. The default Can query, *Can Any talk to Any* displays the entire EPG to EPG connectivity. The How query displays the configuration used for communication between the entities and the health of the connectivity. The connectivity can be healthy or unhealthy. If the connectivity is healthy, using the **Connectivity Table** you can determine the health of the connectivity. If the connectivity is unhealthy, you can use the **Policy**, **Forwarding**, and **Endpoint** tabs to determine the possible cause. The possible causes for unhealthy connectivity include security violations, forwarding violations, and endpoint point violations.

The color of the flow between the EPG pair indicates the maximum severity of smart events across the **Policy**, **Forwarding**, and **Endpoints** tab. The color of the icon in each tab indicates the individual severity of the smart events included in the corresponding tab.

- Red Color indicates critical smart events
- Orange color indicates major smart events
- Yellow color indicates minor smart events
- Blue color indicates warning smart events
- Green color indicates warning info events

The color of the icon in each tab will help you identify if the issues related to security violations, forwarding violations, and endpoint point violations.

For example if the issues are related to security violations, you can use the **Connectivity Table**, **Prefix Table**, and **Forwarding Smart Events** to determine the smart events associated with the security issue. In the **Prefix Table**, you can click **Subnet/Route** to see information regarding the prefixes. In the **Forwarding Smart Events** table you can click the smart event to determine the objects in your fabric that are affected by the issue, the Passing or Failing checks performed on the

smart event and suggested steps to resolve the issue.

## Guidelines and Limitations

- In the **Explorer** page, only one epoch is available for analysis at a time. If you choose another epoch for analysis, the model results for the previous epoch are discarded from memory and have to be recomputed.
- In the **Explorer** page, multiple users can simultaneously explore the same epoch at a given time. Multiple users cannot simultaneously explore different epochs at a given time. When multiple users try to explore different epochs at the same time, the error message **Do you want to use the newly selected epoch instead?** is displayed.
- The Explorer feature is supported only for IPv4 prefixes.
- All queries created using the Explorer feature are unidirectional.
- To explore the APIC resources successfully using the Explorer feature, the APIC policy must contain either valid endpoints such as fv:CEp or valid EPGs.
- In the **Explorer** page, if the analysis fails, the error message *Analysis has failed* is displayed. Download the tech support logs for **Explorer** and contact Cisco TAC to resolve the issue.
  - a. Choose **Settings > Download Tech Support Logs** to download the tech support logs.
  - b. On VM-3, navigate to `/hadoop/log/` directory to locate the following logs for explorer.

```
explorerService/explorer.log
```

```
connectivityAnalysisService/connectivityAnalysisService.log
```

# Creating a Query

Use this procedure to create a query using the Explorer feature.

## Procedure

1. Choose **Explorer**.
2. In the **Timeline** select an epoch for analysis. When you select an epoch, the data to explore is loaded on demand.



You can only select an epoch created in release 4.0(1) to create a query.

3. Perform the following steps for a What or Can query.
  - a. On the **Search** bar, enter a What or Can query. The query must include two groups of one or more entities from the ACI policy. See [Supported Queries](#). By default, the Any to Any query view is displayed.
  - b. The results of the query are displayed in the results table. The results table is only available for a What query. Click the entity on the results table to view the DN information. Click the number on the results table to view details about the entity in the ACI policy.
  - c. Click **Source** and select one or more entities from the results table.
  - d. Click **Destination** and select one or more entities from the results table.
  - e. Click **Can they talk** to determine if the two entities can communicate with each other.
  - f. (Optional) Click **Reverse Query** to reverse the source and destination entities for a Can query.
  - g. In the **Which entities can talk** area, click **EPG** tab to view the the communication between the EPGs. The EPG view displays connectivity information between different EPGs as configured in the APIC policy. In the radial view, the connectivity between entities is displayed with a solid colored arc.



If the query results are large, the message “The query returned too much data to display” is displayed. Use the From EPG and To EPG Search bar to create a more specific query for the results to be displayed. You can also select a single resource from the **Would you like to check connectivity of a single resource** drop-down list to create a specific query.

- h. In the **Which entities can talk** area, click **Prefix** tab to view the the communication between the prefixes. The prefix view displays connectivity information between prefixes as configured in the APIC policy or learnt prefixes. In the radial view, the connectivity between the prefixes is displayed with a solid colored arc.



If the query results are large, the message “The query returned too much data to display” is displayed. Use the From EPG and To EPG Search bar to create a more specific query for the results to be displayed. You can also select a single resource from the **Would you like to check connectivity of a single resource** drop-down list to create a specific query.



Can queries containing large associations such as vzAny may timeout. Use the From EPG and To EPG Search bar to create a more specific query.



For a query between prefixes, if the number of EPGs shared by the prefixes is greater than 25, the Endpoint table fails to load the data and displays an error message. Create an EPG to EPG query to display the results in the Endpoint table.

- i. Select the arc connecting the two entities and click **How do they talk** to view the the communication details.
  - j. See [Viewing What or Can Query Results](#). for information about query results.
4. Perform the following steps for a View query.
- a. On the **Search** bar, enter a View query. The query must include two groups of one or more entities from the ACI policy. See [Supported Queries](#).
  - b. The results of the table are displayed in the **Physical Interfaces** page. See [Viewing View Query Results](#). for information about query results.

## Viewing What or Can Query Results

The **How do they talk** page displays the communication details between the entities from the ACI policy.

The color of the flow indicates the maximum severity of smart events across the **Policy**, **Forwarding**, and **Endpoints** tab. The color of the icon in each tab indicates the individual severity of the smart events included in the corresponding tab.

- Red Color indicates critical smart events
- Orange color indicates major smart events
- Yellow color indicates minor smart events
- Blue color indicates warning smart events
- Green color indicates warning info events
- The **Policy** tab enables you to explore the security policy issues based on the query.
- The **Forwarding** tab enables you explore a prefix or pair of prefixes issues based on the query.
- The **Endpoints** tab to explore the endpoint issues based on the query.

## Procedure

1. Click **Policy** to view the information regarding the health of the contracts between the EPG pairs. The **Policy** health information is displayed in the **Connectivity Table**, **Security Flow Table**, and **Security Smart Events** table.
  - a. The **Connectivity Table** displays the connectivity details between the EPGs and prefixes.
  - b. The **Security Flow Table** displays the communication details between the EPGs.
  - c. The **Security Smart Events** table displays the security smart events based on the query.
2. Click **Forwarding** to view the the information regarding the health of the subnets between the EPG pairs. The **Forwarding** health information is displayed in the **Connectivity Table**, **Prefix Table**, and **Forwarding Smart Events** table.
  - a. The **Connectivity Table** displays displays the connectivity details between the EPGs and prefixes.
  - b. The **Prefix Table** displays detailed connectivity information about all the routes in the assurance group. This information shows which prefixes may communicate successfully, and which prefixes may have communication issues.
  - c. The **Forwarding Smart Events** table displays the forwarding smart events based on the query.
3. Click **Endpoints** to view the the information regarding the health of the endpoints between the EPG pairs. The **Endpoints** health information is displayed in the **Connectivity Table**, **Tenant Endpoints Details**, table and **Endpoints Smart Events** table.
  - a. The **Connectivity Table** displays displays the connectivity details between the EPGs and prefixes.
  - b. The **Tenant Endpoints Details** table displays information about diagnosing endpoint learning errors for the fabric in the assurance group.
  - c. The **Endpoints Smart Events** displays the endpoint smart events based on the query.

## Viewing View Query Results

**Physical Interfaces** page displays the physical interface health and provides the visual indication of the interface status for any leaf switch in the assurance group based on the query.



The **Physical Interface View** area displays information about one leaf switch at a time.

## Procedure

1. If an endpoint is attached to a particular interface, an image of the leaf switch is displayed as a two-dimensional image. The switch ports are color coded to display the status for each port. The color for each port matches its smart event severity by color.
2. Hover over the **i** icon located above the leaf switch image to view the legend for the status icons.
3. Click one of the switch ports in the switch image, to view the details of the smart event



associated with that port, in the **Forwarding Smart Events** table.

4. For additional filtering, check or uncheck the tabs in the **View Control** area. View controls assist with fast navigation to the interfaces that are under your scrutiny.
  - a. Under **Interface Usage**, the interfaces are classified into three types based upon intent.
    - **Configured Interfaces:** This interface is made available by the assurance group policy, and it is ready for use by the EPGs.
    - **Partially Configured Interfaces:** This interface is available to be allocated for consumption by EPGs, and it is either in an unconfigured or a partially configured state.
    - **Used Interfaces:** This interface is allocated by the assurance group policy, and it is consumed by the EPGs.



The **Used Interfaces** tab is selected by default.

- b. Under **Interface Operational Status**, the interfaces are classified by their operational status:
  - **Oper Down:** This interface is operationally down due to issues such as link failure, error disabled, suspended state.
  - **Oper Up:** This interface is operational with no known issues.
  - **Admin Down:** The operator has administratively shut down this interface.



Under **Interface Operational Status**, the tabs **Oper Down**, **Oper Up**, and **Admin Down** are selected by default.

# Supported Queries

The following table lists the queries supported by the **Explorer** feature.

## Supported What Queries

Table 2. Supported What Queries

Query	Entity	Operator	Entity
What BDs are associated with	<ul style="list-style-type: none"> <li>• ?</li> <li>• Any</li> <li>• Any?</li> <li>• BD</li> <li>• ENCAP</li> <li>• EP</li> <li>• EPG</li> <li>• INF</li> <li>• LEAF</li> <li>• VRF</li> </ul>	<ul style="list-style-type: none"> <li>• And</li> <li>• Or</li> </ul>	<ul style="list-style-type: none"> <li>• Any</li> <li>• Any?</li> <li>• BD</li> <li>• ENCAP</li> <li>• EP</li> <li>• EPG</li> <li>• INF</li> <li>• LEAF</li> <li>• VRF</li> </ul>
What ENCAPs are associated with	<ul style="list-style-type: none"> <li>• ?</li> <li>• Any</li> <li>• Any?</li> <li>• BD</li> <li>• ENCAP</li> <li>• EP</li> <li>• EPG</li> <li>• INF</li> <li>• LEAF</li> <li>• VRF</li> </ul>	<ul style="list-style-type: none"> <li>• And</li> <li>• Or</li> </ul>	<ul style="list-style-type: none"> <li>• Any</li> <li>• Any?</li> <li>• BD</li> <li>• ENCAP</li> <li>• EP</li> <li>• EPG</li> <li>• INF</li> <li>• LEAF</li> <li>• VRF</li> </ul>

<b>Query</b>	<b>Entity</b>	<b>Operator</b>	<b>Entity</b>
What EPGs are associated with	<ul style="list-style-type: none"> <li>• ?</li> <li>• Any</li> <li>• Any?</li> <li>• BD</li> <li>• ENCAP</li> <li>• EP</li> <li>• EPG</li> <li>• INF</li> <li>• LEAF</li> <li>• VRF</li> </ul>	<ul style="list-style-type: none"> <li>• And</li> <li>• Or</li> </ul>	<ul style="list-style-type: none"> <li>• Any</li> <li>• Any?</li> <li>• BD</li> <li>• ENCAP</li> <li>• EP</li> <li>• EPG</li> <li>• INF</li> <li>• LEAF</li> <li>• VRF</li> </ul>
What EPs are associated with	<ul style="list-style-type: none"> <li>• ?</li> <li>• Any</li> <li>• Any?</li> <li>• BD</li> <li>• ENCAP</li> <li>• EP</li> <li>• EPG</li> <li>• INF</li> <li>• LEAF</li> <li>• VRF</li> </ul>	<ul style="list-style-type: none"> <li>• And</li> <li>• Or</li> </ul>	<ul style="list-style-type: none"> <li>• Any</li> <li>• Any?</li> <li>• BD</li> <li>• ENCAP</li> <li>• EP</li> <li>• EPG</li> <li>• INF</li> <li>• LEAF</li> <li>• VRF</li> </ul>
What INFs are associated with	<ul style="list-style-type: none"> <li>• ?</li> <li>• Any</li> <li>• Any?</li> <li>• BD</li> <li>• ENCAP</li> <li>• EP</li> <li>• EPG</li> <li>• INF</li> <li>• LEAF</li> <li>• VRF</li> </ul>	<ul style="list-style-type: none"> <li>• And</li> <li>• Or</li> </ul>	<ul style="list-style-type: none"> <li>• Any</li> <li>• Any?</li> <li>• BD</li> <li>• ENCAP</li> <li>• EP</li> <li>• EPG</li> <li>• INF</li> <li>• LEAF</li> <li>• VRF</li> </ul>

<b>Query</b>	<b>Entity</b>	<b>Operator</b>	<b>Entity</b>
What Inventory is associated with	<ul style="list-style-type: none"> <li>• ?</li> <li>• Any</li> <li>• Any?</li> <li>• BD</li> <li>• ENCAP</li> <li>• EP</li> <li>• EPG</li> <li>• INF</li> <li>• LEAF</li> <li>• VRF</li> </ul>	<ul style="list-style-type: none"> <li>• And</li> <li>• Or</li> </ul>	<ul style="list-style-type: none"> <li>• Any</li> <li>• Any?</li> <li>• BD</li> <li>• ENCAP</li> <li>• EP</li> <li>• EPG</li> <li>• INF</li> <li>• LEAF</li> <li>• VRF</li> </ul>
What Leafs are associated with	<ul style="list-style-type: none"> <li>• ?</li> <li>• Any</li> <li>• Any?</li> <li>• BD</li> <li>• ENCAP</li> <li>• EP</li> <li>• EPG</li> <li>• INF</li> <li>• LEAF</li> <li>• VRF</li> </ul>	<ul style="list-style-type: none"> <li>• And</li> <li>• Or</li> </ul>	<ul style="list-style-type: none"> <li>• Any</li> <li>• Any?</li> <li>• BD</li> <li>• ENCAP</li> <li>• EP</li> <li>• EPG</li> <li>• INF</li> <li>• LEAF</li> <li>• VRF</li> </ul>
What VRFs are associated with	<ul style="list-style-type: none"> <li>• ?</li> <li>• Any</li> <li>• Any?</li> <li>• BD</li> <li>• ENCAP</li> <li>• EP</li> <li>• EPG</li> <li>• INF</li> <li>• LEAF</li> <li>• VRF</li> </ul>	<ul style="list-style-type: none"> <li>• And</li> <li>• Or</li> </ul>	<ul style="list-style-type: none"> <li>• Any</li> <li>• Any?</li> <li>• BD</li> <li>• ENCAP</li> <li>• EP</li> <li>• EPG</li> <li>• INF</li> <li>• LEAF</li> <li>• VRF</li> </ul>

## Supported Can Queries

Table 3. Supported Can Queries

Query	Entity	Operator	Protocol	Destination Port	Source Port
Can BD <b>bd_name</b> talk to	<ul style="list-style-type: none"> <li>• BD</li> <li>• ENCAP</li> <li>• EP</li> <li>• EPG</li> <li>• INF</li> <li>• LEAF</li> <li>• VRF</li> <li>• Subnet</li> <li>• ANY*</li> </ul>	On	<ul style="list-style-type: none"> <li>• TCP</li> <li>• UDP</li> <li>• ICMP</li> </ul>	<ul style="list-style-type: none"> <li>• Port Number</li> <li>• Port Range</li> <li>• Well-known Port</li> </ul>	<ul style="list-style-type: none"> <li>• Port Number</li> <li>• Port Range</li> <li>• Well-known Port</li> </ul>
Can ENCAP <b>encap_name</b> talk to	<ul style="list-style-type: none"> <li>• BD</li> <li>• ENCAP</li> <li>• EP</li> <li>• EPG</li> <li>• INF</li> <li>• LEAF</li> <li>• VRF</li> <li>• Subnet</li> <li>• ANY*</li> </ul>	On	<ul style="list-style-type: none"> <li>• TCP</li> <li>• UDP</li> <li>• ICMP</li> </ul>	<ul style="list-style-type: none"> <li>• Port Number</li> <li>• Port Range</li> <li>• Well-known Port</li> </ul>	<ul style="list-style-type: none"> <li>• Port Number</li> <li>• Port Range</li> <li>• Well-known Port</li> </ul>
Can EP <b>ep_name</b> talk to	<ul style="list-style-type: none"> <li>• BD</li> <li>• ENCAP</li> <li>• EP</li> <li>• EPG</li> <li>• INF</li> <li>• LEAF</li> <li>• VRF</li> <li>• Subnet</li> <li>• ANY*</li> </ul>	On	<ul style="list-style-type: none"> <li>• TCP</li> <li>• UDP</li> <li>• ICMP</li> </ul>	<ul style="list-style-type: none"> <li>• Port Number</li> <li>• Port Range</li> <li>• Well-known Port</li> </ul>	<ul style="list-style-type: none"> <li>• Port Number</li> <li>• Port Range</li> <li>• Well-known Port</li> </ul>

Query	Entity	Operator	Protocol	Destination Port	Source Port
Can EPG <i>epg_name</i> talk to	<ul style="list-style-type: none"> <li>• BD</li> <li>• ENCAP</li> <li>• EP</li> <li>• EPG</li> <li>• INF</li> <li>• LEAF</li> <li>• VRF</li> <li>• Subnet</li> <li>• ANY*</li> </ul>	On	<ul style="list-style-type: none"> <li>• TCP</li> <li>• UDP</li> <li>• ICMP</li> </ul>	<ul style="list-style-type: none"> <li>• Port Number</li> <li>• Port Range</li> <li>• Well-known Port</li> </ul>	<ul style="list-style-type: none"> <li>• Port Number</li> <li>• Port Range</li> <li>• Well-known Port</li> </ul>
Can INF <i>inf_name</i> talk to	<ul style="list-style-type: none"> <li>• BD</li> <li>• ENCAP</li> <li>• EP</li> <li>• EPG</li> <li>• INF</li> <li>• LEAF</li> <li>• VRF</li> <li>• Subnet</li> <li>• ANY*</li> </ul>	On	<ul style="list-style-type: none"> <li>• TCP</li> <li>• UDP</li> <li>• ICMP</li> </ul>	<ul style="list-style-type: none"> <li>• Port Number</li> <li>• Port Range</li> <li>• Well-known Port</li> </ul>	<ul style="list-style-type: none"> <li>• Port Number</li> <li>• Port Range</li> <li>• Well-known Port</li> </ul>
Can LEAF <i>leaf_name</i> talk to	<ul style="list-style-type: none"> <li>• BD</li> <li>• ENCAP</li> <li>• EP</li> <li>• EPG</li> <li>• INF</li> <li>• LEAF</li> <li>• VRF</li> <li>• Subnet</li> <li>• ANY*</li> </ul>	On	<ul style="list-style-type: none"> <li>• TCP</li> <li>• UDP</li> <li>• ICMP</li> </ul>	<ul style="list-style-type: none"> <li>• Port Number</li> <li>• Port Range</li> <li>• Well-known Port</li> </ul>	<ul style="list-style-type: none"> <li>• Port Number</li> <li>• Port Range</li> <li>• Well-known Port</li> </ul>

Query	Entity	Operator	Protocol	Destination Port	Source Port
Can VRF <i>vrf_name</i> talk to	<ul style="list-style-type: none"> <li>• BD</li> <li>• ENCAP</li> <li>• EP</li> <li>• EPG</li> <li>• INF</li> <li>• LEAF</li> <li>• VRF</li> <li>• Subnet</li> <li>• ANY*</li> </ul>	On	<ul style="list-style-type: none"> <li>• TCP</li> <li>• UDP</li> <li>• ICMP</li> </ul>	<ul style="list-style-type: none"> <li>• Port Number</li> <li>• Port Range</li> <li>• Well-known Port</li> </ul>	<ul style="list-style-type: none"> <li>• Port Number</li> <li>• Port Range</li> <li>• Well-known Port</li> </ul>
Can Subnet <i>subnet_name</i> talk to	<ul style="list-style-type: none"> <li>• BD</li> <li>• ENCAP</li> <li>• EP</li> <li>• EPG</li> <li>• INF</li> <li>• LEAF</li> <li>• VRF</li> <li>• Subnet</li> <li>• ANY*</li> </ul>	On	<ul style="list-style-type: none"> <li>• TCP</li> <li>• UDP</li> <li>• ICMP</li> </ul>	<ul style="list-style-type: none"> <li>• Port Number</li> <li>• Port Range</li> <li>• Well-known Port</li> </ul>	<ul style="list-style-type: none"> <li>• Port Number</li> <li>• Port Range</li> <li>• Well-known Port</li> </ul>
Can ANY talk to	<ul style="list-style-type: none"> <li>• BD</li> <li>• ENCAP</li> <li>• EP</li> <li>• EPG</li> <li>• INF</li> <li>• LEAF</li> <li>• VRF</li> <li>• ANY</li> </ul>	—	—	—	—



The **Operator**, **Protocol**, **Destination Port**, and **Source Port** are not supported in CAN queries for these ANY entities.

Table 4. Supported View Queries

Query	Entity
View interfaces on	Leaf <code>leaf_name</code>



# Epoch Delta Analysis

## Epoch Delta Analysis

Cisco NAE performs analysis of an Cisco ACI fabric at regular intervals called epoch and the epoch data is collected in 15 minute intervals.

At each epoch, Cisco NAE captures a snapshot of the controller policies and the fabric run time state, performs analysis, and generates smart events. The smart events generated describe the health of the network at that epoch.

Epoch delta analysis enables you to analyze the difference in the policy, run time state, and the health of the network between two epochs. Epoch delta analysis consists of the following components:

- **Analysis Management:** Enables you to create a new delta analysis and manage existing analysis. See [Creating Epoch Delta Analysis](#).
- **Delta Analysis:** Enables you to view results of successful delta analysis such as health delta and policy delta. See [Viewing Delta Analysis Results](#).

## Health Delta

**Health Delta** analyses the difference in the health of the fabric across the two epochs. The results are displayed in the following areas:

- **Smart Event Count:** Displays the difference in smart event count per severity across the two epochs.
- **Health Delta by Resources:** Displays the count of resources by type (for example, Tenants, EPGs, contracts) that have seen a change in their health. The changes can either be issues resolved or new issues detected.
- **All Smart Events:** The **Aggregated** view displays the delta status for each smart event name across the two epochs. The **Individual** view displays the delta status for each smart event across the two epochs and also the failing conditions for the event.

## Policy Delta

**Policy Delta** analyzes the differences in the policy between the two epochs and provides a correlated view of what has changed in the ACI Fabric.

The policy delta view enables you to:

- View the changed policy objects between the two epochs.
- View the added, modified, and deleted policy configurations between the two epochs.
- Export the policy configuration for the earlier epoch policy and later epoch policy.
- Search for text in added, modified, deleted, and unchanged areas in the policy delta.

- View the context around the modified areas in the policy delta.
- View the difference in the APIC audit logs across the two epochs.

To view the policy delta between the two epochs, you must configure the collection settings for an Assurance Group. See [Performing Online Analysis](#).

## Guidelines and Limitations

The following general guidelines are applicable to Epoch Delta Analysis:

- While you are currently allowed to create more than one Epoch Delta Analyses at any given time, we recommend that you do not queue more than one Delta Analysis at any given time. In addition, we recommend that you wait for some time (approximately 10 minutes) between creating new analyses to avoid the risk of adversely impacting the run time of the concurrent online assurance group analysis. The interdependency arises because the Epoch Delta Analysis results in an increased load on the database. Sustained high-database load from multiple back-to-back Delta Analyses may affect the run-time of the online analysis.

The following guidelines and limitations are applicable for policy delta:

- The **APIC Configuration Export Policy** must be configured. See [Performing Online Analysis](#).
- The **APIC Configuration Export Policy** must be of the same format (XML/JSON) for both the epochs.
- The policy delta will not be performed if there are any APIC configuration export policy collection errors.

## Creating Epoch Delta Analysis

Use this procedure to create an epoch delta analysis.

### Before You Begin

- You have configured the collection settings for an Assurance Group. See [Performing Online Analysis](#).
- APIC admin writePriv privileges allow information collection on the APIC host and leaf switches. You must have APIC admin writePriv privileges to configure the **APIC Configuration Export Policy**.

### Procedure

1. Choose **Epoch Delta > Manage Delta Analysis**.
2. Click **Create New Delta Analysis**.
3. Complete the following fields for **Create New Delta Analysis**.
  - a. In the **Name** field, enter the name. The name must be unique across all the analyses.
  - b. In the **Description** field, enter the description.

- c. From the **Earlier Epoch** drop-down list, choose the first epoch for the delta analysis. You can also use the timeline to select an earlier epoch. See [Timeline](#) for more information.
- d. From the **Later Epoch** drop-down list, choose the second epoch for the delta analysis. You can also use the timeline to select a later epoch.



The two epochs selected for the delta analysis must belong to the same Assurance Group.

4. Click **Run**.
5. The status of the delta analysis is displayed in the **Delta Analysis** table. Cisco NAE performs one delta analysis at a time. To perform another delta analysis, you must stop the current delta analysis and then start the another delta analysis. See [Managing Epoch Delta Analysis](#).
6. To view the results of the delta analysis, select a delta analysis from the **Delta Analysis** table. From the Actions menu, choose **View Results**. See [Viewing Delta Analysis Results](#).

## Viewing Delta Analysis Results

Use this procedure to view the results of the delta analysis.


- To view the results of health delta analysis, See [Viewing Health Delta Analysis](#).
- To view the results of Policy delta analysis, See [Viewing Policy Delta Analysis](#).

## Viewing Health Delta Analysis

Use this procedure to view the results of the health delta analysis.

### Procedure





1. Choose **Epoch Delta > Delta Analysis**.
2. Click **Health Delta** to view the results of the health of the fabric.
  - a. **The Smart Event Count** displays the difference in the smart event count per severity across the two epochs. The first count represents the smart events found only in the earlier epoch. The second count represents the smart events common in both the epochs. The third count represents the smart events found only in the later epoch.
    - i. Click the smart event count to view the smart event details.
  - b. The **Health Delta By Resources** displays the health delta across various APIC resource types. It also displays the count of the resources with issues, without issues, and the total resources.
    - i. Click the resource count to view the resources associated with the resource count.
    - ii. Hover on the resource name to view the resource DN.
    - iii. Click the resource name to view the smart event details for that resource.
  - c. In the **Search** bar use the multiple filters to search for smart events.

- i. Click **Add Filters** to filter by resources and then by resource name or DN.
  - ii. Click the  icon to filter by the epochs used for the delta analysis.
- d. The **All Smart Events** table displays the aggregated and individual view of the smart event delta.
- i. Click **Aggregated** to view the delta status for each smart event name across the two epochs. The **Count** column displays the consolidated number of events across the two epochs.
  - ii. Click **Individual** to view displays the delta status for each smart event across both the epochs and also the failing conditions for the event. Click **Event Name** to view the smart event details.

## Viewing Policy Delta Analysis

Use this procedure to view the results of the policy delta analysis.

### Procedure

1. Choose **Epoch Delta > Delta Analysis**.
2. Click **Policy Delta** to view the results of the policy changes across the two epochs. Policy Delta includes 3 panels, Changed Policy Object, Policy Viewer, and Audit Log.
3. The **Changed Policy Object** panel, displays the changed policy object tree across the two epochs.
  - a. Drill down on a particular object to view the object types that have changed. The number indicates the number of changes to the object.
  - b. Select the changed object type to view the smart events that have changed.
  - c. Click DN link to access the affected object type in APIC.
  - d. Click **Show Changes** to view the changes in the Policy Viewer and Audit Log panels. The corresponding changes in the Policy Viewer and Audit Log panels are highlighted.
  - e. Use the **Search** bar to perform a DN search.
4. The **Policy Viewer** panel displays the policy configuration across the earlier and later epochs. The policy configuration for the earlier epoch is called the earlier epoch policy. The policy configuration for the later epoch is called the later epoch policy.
  - a. Use the color coding to visualize the added, deleted, modified, and unchanged content across the two policies. Click the  icon for information about the color coding.
  - b. The  icon lists the line numbers for the content in the earlier epoch policy. The  icon lists the line numbers for the content in the later epoch policy.
  - c. Click **Show More Above** or **Show More Below** to display more content.
  - d. Click the  icon to export the earlier epoch policy or to export the later epoch policy.
  - e. Enter a value in the **Search** bar to perform a text search.
    - i. Select **ALL** to search across all the content in the earlier epoch policy and later epoch policy.

- ii. Select **Changed** to search across the changed content in the earlier epoch policy and later epoch policy.
5. Cisco NAE collects audit logs from APIC and computes the difference in the audit logs between the two epochs. The **Audit Log** panel then displays all the audit logs that were created between the two epochs. A correlated view of what has change in the datacenter is displayed in the **Audit Log** panel. When you select a particular object in the **Changed Policy Object** panel, the relevant difference is highlighted in the **Policy Viewer** panel and the relevant audit log is highlighted in the **Audit Log** panel. APIC audit logs are records of user-initiated events such as logins and logouts or configuration changes that are required to be auditable. For every epoch, the audit log history is limited to last 24 hrs.
- a. In the audit log panel, green color indicates the audit log attributes such as VLAN that have been added. Red color indicates the audit log attributes that have been deleted. Yellow color indicates the audit log attributes that have been modified.
  - b. Use the **Search** bar to perform a DN, User ID, or text search.
  - c. Hover on an audit log entry to view when the changes were made and who made the changes. The timestamp on the audit log entry corresponds to the the timestamp on the APIC audit log.
  - d. Click Audit Log entry to access the affected object type in APIC.

# Compliance Analysis

## Compliance Analysis Tab

Every epoch verifies compliance analysis results. In each epoch, one event for every requirement that is analyzed is raised. For example, if an assurance group runs a compliance analysis on an epoch every 15 minutes, and there are two requirements associated with the epoch, two smart events will be raised.

When an epoch runs for a specific assurance group, all the active requirement sets that are associated with that assurance group are verified and validated.



To be included as an active requirement set, you must associate your compliance requirement to the assurance group and activate the compliance requirement.

# Manage Compliance

## Manage Compliance Tab

The **Manage Compliance** tab enables the user to verify Segmentation Compliance and Service Level Agreement (SLA) compliance, traffic restriction compliance, and configuration compliance. Compliance can be used to set up regulatory compliance rules. With segmentation compliance, the user can establish walled areas around a set of entities that must not communicate with other entities. SLA compliance can also set up rules for entities that must talk with other entities. Traffic restriction compliance requirements allow the user to specify restrictions on protocols and ports for communication between objects.

In the NAE UI, the user specifies their compliance requirements. The NAE appliance, verifies in the subsequent epochs, whether the compliance requirements are satisfied by the policy that is configured on Cisco APIC. If satisfied, an event is raised stating that the compliance requirement is satisfied. One event per requirement per epoch is raised. For example, if an assurance group runs a compliance analysis on an epoch every 15 minutes, and there are two requirements associated with the epoch, two smart events will be raised.

The following examples provide you with information about the compliance **include** and **exclude** rules:

- Contains EPGs in Tenants with names that start with “a” or ending with “z”. EPGs in Tenants such as “abz” that satisfy both criteria are included only once.
- Contains EPGs in Tenants with names that start with “a” and are also in VRFs where the Tenant is “xyz” and the VRF name contains “c”. For example: When an EPG under Tenant “abc” that is in a VRF with DN uni/tn-xyz/ctx-abcde is selected, verify that both the Tenant and the VRF criteria match. An EPG under Tenant “abc” that is in a VRF with DN uni/tn-xyz1/ctx-abcde is not selected because the VRF Tenant does not match.
- Contains all EPGs under Tenants that begin with “a” except those that contain “d”. For example: An EPG under Tenant “abc” is selected. An EPG under Tenant “abcd” is not selected.
- Contains all EPGs under Tenants that begin with “a” except those EPGs that are also in the VRF with DN uni/tn-rrr/ctx-sss.

## Creating Object Selector

Use this procedure to create an Object Selector.

### Before You Begin

- At least one assurance group must be created.

### Procedure

1. Choose **Compliance > Manage Compliance > Object Selectors**.
2. Click **Create New Object Selector**.

3. In the **Create New Object Selector** dialog box, **Object Selector Name** field, enter the name. The name must be unique across all the assurance groups.
4. In the **Description** field, enter the description. (Optional step)
5. In the **Object Selector Type** field, from the drop-down options, choose the appropriate object type.



Based upon your object selector type (for example EPG, VRF, BD) the associated included and excluded objects are displayed for you to select.



If you had EPG selectors chosen in an earlier release of Cisco NAE, after the upgrade to Cisco NAE release 4.0(1), the EPG selectors will automatically display in the current Object Selector table and they will be associated with the EPG Selector type.

5. In the Included and Excluded Object fields, from the drop-down options, choose the relevant objects.



You may use multiple match criteria, and the included objects will be a union and intersection of the criteria that you choose.

6. Click the **Preview** hyperlink to view objects selected by the new object selector. The objects displayed are based upon objects configured in the APIC in the last epoch.



**BETA FEATURE:** Using the preview link to view the objects that are included or excluded in the object selector is a Beta feature in Cisco NAE Release 4.0(1). To provide Beta feedback on this feature, send your comments to your Cisco account team.



When creating the new object selector, you can preview the objects that are included or excluded in the object selector before you save the newly created object selector with your selections. You can also filter the list by the object Distinguished Name/Name. If the preview list requires further modifications or filtering, close the preview dialog box and tweak your selections for included and excluded objects based upon your preference. Then preview the list once again. After you are satisfied with the preview list, close the dialog box.

7. Click **Save**. Your Object Selectors are created. The list of object selectors is displayed under the **Object Selectors** tab.

For additional details about editing or deleting object selectors, see [Managing Object Selectors](#).

## Creating Traffic Selector

Use this procedure to create a traffic selector.





You must configure the Traffic Selectors before configuring the Compliance Requirement and the Compliance Requirement Sets (in that order of sequence).

## Before You Begin

- At least one assurance group must be created.

## Procedure

1. Choose **Compliance > Manage Compliance > Traffic Selectors**.
2. Click **Create New Traffic Selector**.
3. Complete the following fields for **Create New Traffic Selector**.
  - a. In the **Traffic Selector Name** field, enter the name. The name must be unique across all the analyses.
  - b. In the **Description** field, enter the description. (Optional step)
  - c. In the **Talk On** area, from the **EtherType** field drop-down options, choose the appropriate EtherType.



Certain **EtherType** choices will require you to make additional choices from drop-down lists that appear based upon your selections.

4. To add additional EtherType options, click **Add On**, and choose additional EtherType options.
5. Click **Save**.

Your traffic selectors are created. The list of traffic selectors is displayed under the **Traffic Selectors** tab.

For additional details about editing or deleting traffic selectors, see [Managing Traffic Selectors](#).

## Creating Compliance Requirement

Use this procedure to create a compliance requirement.

## Before You Begin

- At least one assurance group must be created.
- Your object selectors are created.
- Your traffic selectors are created.

## Procedure

1. Choose **Compliance > Manage Compliance > Compliance Requirements**.
2. Click **Create New Compliance Requirement**.
3. Complete the following fields for **Create New Compliance Requirement**.

- a. In the **Compliance Requirement Name** field, enter the name. The name must be unique across all the analyses.
  - b. In the **Description** field, enter the description. (Optional step)
4. In the **Compliance Type** area, perform the appropriate steps to specify the requirements depending on your preference.
- a. If you choose **Segmentation** perform the following steps:
    - i. Click **Enter EPG Selector A name** and choose an EPG selector name from the list.
    - ii. Choose the appropriate communication operator if available (**Must Not talk to** is chosen by default).
    - iii. Click **Enter EPG Selector B name**, and choose an EPG selector name from the list.
  - b. If you choose **SLA** perform the following steps:
    - i. Click **Enter EPG Selector A name** and choose an EPG selector name from the list.
    - ii. Choose the appropriate communication operator if available (**Must Not talk to** is chosen by default).
    - iii. Click **Enter EPG Selector B name**, and choose an EPG selector name from the list.
    - iv. Click **Select Traffic Selector name** and choose a traffic selector name.
  - c. If you choose **Traffic Restriction** perform the following steps:
    - i. Click **Enter EPG Selector A name** and choose an EPG selector name from the list.
    - ii. Choose the appropriate communication operator if available (**Must Not talk to** is chosen by default).



When you choose the value **Must Not Talk To**, Cisco NAE verifies that the EPGs do not communicate with the specified protocol in the traffic selector field. When you choose the value **May Talk To**, Cisco NAE verifies that the EPGs cannot communicate on protocols other than the protocol specified in the traffic selector field.

- iii. Click **Enter EPG Selector B name**, and choose an EPG selector name from the list.
  - iv. Click **Select Traffic Selector name** and choose a traffic selector name.
- d. If you choose **Configuration** perform the following steps:
- i. Click **Enter Object Selector name** and choose an object selector name from the list.
  - ii. The communication operator (for example **Must Have**) is displayed.
  - iii. Click **Enter Attribute**, and choose the desired attribute from the list.
  - iv. Choose the appropriate operator from **Equal to** or **Not Equal to**.
  - v. Click **Enter Attribute Value**, and choose the desired attribute value from the list.



As part of object selectors for Configuration Compliance Type, only BD and VRF are supported. You can select more than one attribute in one configuration compliance requirement.

5. Click **Save**.

You have created a compliance requirement. For additional details about editing or deleting compliance requirements, see [Managing Compliance Requirements](#).

## Creating Compliance Requirement Set

Use this procedure to create a compliance requirement set.

### Before You Begin

- At least one epoch analysis has been completed.
- Your object selectors and requirements are created.

### Procedure

1. Choose **Compliance > Manage Compliance > Compliance Requirement Sets**.
2. Click **Create New Compliance Requirement Set**.
3. Complete the following fields for **Create New Compliance Requirement Set**.
  - a. In the **Compliance Requirement Set Name** field, enter the name. The name must be unique across all the analyses.
  - b. In the **Description** field, enter the description. (Optional step).
  - c. In the **Associate to current Assurance Group** field, check the checkbox.



You can only associate with the current assurance group.

- d. In the **Activate this Compliance Requirement Set** field, check the checkbox if you want to activate the requirement set.



When an epoch runs for a specific assurance group, all the active requirement sets that are associated with that assurance group are verified and validated.

- e. In the **Associated Requirements** area, click the **Associate** link to choose the requirements that you want to associate from the **Associate Requirements** table.



Similarly, you can disassociate requirements by clicking the **Disassociate** link.

- f. Click **Save**.

You have created a compliance requirement set. For additional details about editing or deleting compliance requirement sets, see [Managing Compliance Requirement Sets](#).

# Smart Event Management

## Smart Event Dashboard

In the **Smart Event Dashboard**, the smart events are organized by severity, category, subcategory, and name.

You can manage the display of the smart events by:

- Clicking one of the icons in the Smart Events by Severity bar displays only the smart events of the specified severity. All the smart events are displayed when clicking Total in the Smart Events by Severity bar.
- Clicking **Aggregated** displays groups of smart events identified by event name.
- Clicking **Individual** displays every instance of the smart event.

A smart event contains the following information:



- **Description**—A description of the smart event.
- **Impact**—The negative impact that the smart event has on your fabric.
- **Affected Objects**—The objects in your fabric that are affected by the issue. The primary affected objects are highlighted.
- **Checks**—The Passing or Failing checks performed on the Smart Event and suggested steps to resolve the issue. Every passing or failing condition has a check code associated with it. The same check code may be used for a passing or failing condition and may be reused across Smart Events with different event codes.
- **Event ID/Code**—The ID and code associated with the Smart Event.



## Lifecycle of a Smart Event

The lifecycle of a smart event appears as an overview summary timeline when displaying the details of an individual smart event. The lifecycle of a smart event is a graphical representation of the individual smart event occurrences in the epochs on the timeline. The color of the epoch icons signify the severity of the smart event. The magnification of the lifecycle can be controlled with the Zoom Level controls below the timeline.

### Zoom Level: Lifecycle

Selecting the Lifecycle Zoom Level (default magnification) displays the time when the smart event reached a certain state. (A gray color icon indicates the smart event did not reach the threshold for the state.)

Lifecycle State	Description
 First Raised	Initial occurrence of the smart event and the affected object.
 Last Raised	Last occurrence of the smart event and the affected object.

Lifecycle State	Description
 Clearing	Smart event and affected object did not occur in one subsequent epoch.
 Cleared	Smart event and affected object did not occur in two subsequent epochs.



In addition to these four smart event states, the `CONNECTED_EP_LEARNING_ERROR` and the `FABRIC_EP_LEARNING_ERROR` smart events have a Raising state that precedes the First Raised state. If a `CONNECTED_EP_LEARNING_ERROR` and the `FABRIC_EP_LEARNING_ERROR` smart event occurs in an epoch, it is in the Raising state. If it occurs in the next consecutive epoch, it is then considered to be in the First Raised state.

### Example


If you have four consecutive epochs with the earlier epochs containing the occurrence of a smart event, the lifecycle of the smart event would have the following chronology when displayed with the Lifecycle Zoom Level.

- The initial occurrence of the smart event is contained in Epoch1.
  - The First Raised state indicates Epoch1.
- The last occurrence of the smart event is contained in Epoch2.
  - The Last Raised state indicates Epoch2.
- The smart event did not occur in Epoch3.
  - The Clearing state indicates Epoch3.
- The smart event did not occur in Epoch4.
  - The Cleared state indicates Epoch4.


### Zoom Level: Magnified

Selecting a more granular Zoom Level (or clicking one of the icons on the timeline) increases the magnification of the timeline and displays epochs where the smart event occurred.

With the increased timeline magnification, you can navigate among the epochs by clicking one of the epochs or by using the navigation controls (located below the timeline and to the right of the Zoom Level). The selected epoch displays the date/time for the epoch as well as detailed information for the smart event occurrence.

Clicking the settings icon  in the Action column opens a menu so that you can edit one of the following pieces of information for the smart event:

- Operation Status: [New, In Progress, or Closed]
- Assign to: Assign to a UserId
- Comment: Add a comment
- Tags: Add a metadata tag

Upon completion of editing these pieces of information, the updated information is displayed in the detailed information for the smart event. You can search the individual smart events by Operation Status, UserID, or Tag value by making these columns a visible attribute to the individual smart event by setting **Column Customization**  and typing the desired search term in the filter field of the appropriate column.

For example, if you edit an individual smart event to have a metadata tag of "Rare event" and add the Tags column to the table of individual smart events using **Column Customization**; you can search for the smart event by typing "Rare event" in the filter field of the Tags column.

## Previous Occurrence and Next Occurrence

If NAE has access to information about the lifecycle of the smart event that is contained in earlier or later epochs, you can click on **Previous Occurrence** or **Next Occurrence** to display these lifecycles.



Lifecycle does not support epochs from Cisco NAE release 3.1(1) and earlier releases.

# Smart Event Suppression

A smart event in Cisco NAE provides information about the state of your network at the time represented by the epoch. Smart events are categorized as either Critical, Major, Minor, Warning, or Informational. Smart event suppression feature enables you to suppress smart events in the Cisco NAE UI and view only the smart events that are relevant.

## Smart Event Suppression Workflow

Smart event suppression workflow includes the following steps:

1. Create event rules: An event rule enables you to match a smart event against a rule using the match criteria.
  - An event rule contains the match criteria required to match a smart event against the rule and the action that should be applied on the matched smart event.
  - You can use attributes such as severity, category, subcategory, event code, affected object, and check code to define the match criteria for the event rule.
  - A match criteria can contain one attribute or multiple attributes.
    - If a match criteria contains multiple attributes, then the events containing all the attributes will be matched.
    - If an match criteria contains multiple check codes, then the events containing any one check code will be matched.
    - If an match criteria contains multiple affected objects, then the events containing all of the affected objects will be matched.
  - If an event rule contains multiple match criteria, then the events containing the union of the match criteria will be matched.
  - Each event rule can have only one action. The options include **Suppressed**, **Never Suppressed**, and **No Action**.
  - An event rule containing the option **Never Suppressed**, supersedes an event rule containing the option **Suppressed**.
  - An event rule containing the option **No Action**, cannot be added to an event ruleset.

See [Creating New Event Rule](#) for more information.

2. Add event rules to event rulesets: An event ruleset enables you to group event rules and associate them with an Assurance Group. The event rules are applied when you activate the event ruleset.
  - An event ruleset contains event rules.
  - An event rule can be part of multiple event rulesets.
  - An event ruleset can be associated with an assurance group or with multiple assurance groups.
  - An event ruleset can be activated or deactivated.

- When the event ruleset is activated, the event rules are applied.

See [Creating New Event Ruleset](#) for more information.

## Manage Event Rules

On the **Smart Events** inspector page, the user can create and manage event rules and event rulesets under the **Manage Event Rules** tab.

## Current Epoch Event Rules Snapshot

On the **Smart Events** inspector page, the user can view the event rules for the current epoch selected in the timeline under the **Current Epoch Event Rules Snapshot** tab.

Click **Smart Events Count** to view the smart events that match the event rule.



# Creating New Event Rule


Use this procedure to create a new event rule.

## Procedure

1. Choose **Smart Events > Manage Events Rules > Event Rule**.
2. Click **Create New Event Rule**.
3. Complete the following fields for **Create New Event Rule**.
  - a. In the **Event Rule Name** field, enter the name.
  - b. In the **Description** field, enter the description.
  - c. From the **Suppression** drop-down list, choose, the action for the event rule. The default is **No Action**. An event rule containing the action **Never Suppressed**, supersedes an event rule containing the action **Suppressed**. An event rule containing the option **No Action**, cannot be added to an event ruleset.
4. Click **Add New Match Criteria** to define the match criteria for the event rule.
  - a. Select the attributes for the match criteria. You can use severity, category, subcategory, event code, affected object, and check code to define the attribute for the match criteria.



If multiple affected objects are included in the match criteria, then the events containing all the affected objects will be matched. If multiple check codes are included in the match criteria, then the events containing any one check code will be matched.

- d. Click the  icon and click **Done**.
- e. Check the checkbox for the match criteria.



If an event rule contains multiple match criteria, then the events containing the union of the match criteria will be matched.

- d. Click **Save**.
5. The new event rule is displayed in the **New Event Rule** table below.


# Creating New Event Ruleset

Use this procedure to create a new event ruleset.

## Before You Begin

- You have created an event rule.

## Procedure

1. Choose **Smart Events > Manage Events Rules > Event Rulesets**.
  2. Click **Create New Event Ruleset**.
  3. Complete the following fields for **Create New Event Ruleset**.
    - a. In the **Event Ruleset Name** field, enter the name.
    - b. In the **Description** field, enter the description.
    - c. Check the **Associate to Current Assurance Group** checkbox to associate the event ruleset to the current Assurance Group. To activate the event ruleset, it must be associated with an Assurance Group.
      - i. To associate the event ruleset at a later time, see [Managing Event Rulesets](#).
      - ii. To associate the event ruleset with another Assurance Group, see [Managing Event Rulesets](#).
    - d. Check the **Activate this Compliance Requirement Set** checkbox to activate the event ruleset. To activate the event ruleset at a later time, see [Managing Event Rulesets](#).
  4. In the **Associate Event Rules** area, click the **Associate Never Suppressed Event Rules** to choose the event rules that you want to associate from the **Never Suppress Event Rule** table. Click **Associate**.
  5. In the **Associate Event Rules** area, click the **Associate Suppressed Event Rules** to choose the event rules that you want to associate from the **Suppressed Event Rule** table. Click **Associate**.
- 
- If you include a combination of Never Suppressed Event Rules and Suppressed Event Rules in your event ruleset, the Never Suppressed Event Rules will take precedence over the Suppressed Event Rules.
6. (Optional) To disassociate an event rule, select the event rule and click **Disassociate**.
  7. Click **Save**.

# Managing Cisco Network Assurance Engine

## Managing User Accounts

Use this procedure to manage user accounts.

### Procedure

1. Choose **Settings > User Management**.
2. Select the user account.
3. From the **Action** column, choose the **Settings** icon.
4. To change the password of the user, click **Change Password**. Complete the following fields for **Change Password**.
  - a. In the **Current Password** field, enter the current password.
  - b. In the **Password** field, enter the new password.
    - i. The password must adhere to the password policy defined in the **Passphrase Configuration** page.
    - ii. The password must have characters from the following characters types: lowercase, uppercase, digit, symbol.
    - iii. The allowed symbols include: `_ ! @ # $ % ^ & * ( )`
  - c. In the **Confirm Password** field, enter the new password again.
  - d. Click **Save**.
5. To edit a user account, click **Edit User Account**. Complete the following fields for **Edit User Account**.
  - a. In the **Email** field, update the email address.
  - b. Click **Save**.
6. To delete a user account, click **Delete**. You cannot delete an Admin user.
  - a. In the **Delete User** form, click **Delete**.

## Managing Passphrase

In Cisco NAE, an administrator can define the password policy for users accessing the appliance.

Use this procedure to configure the password requirements for Cisco NAE.

### Procedure

1. Choose **Settings > Appliance Administration**.
2. Click the details icon on the **Passphrase Configuration** tile.
3. Complete the following fields for **Passphrase Configuration**.

- a. From the **Minimum passphrase length** drop-down list, choose the minimum length for the password. The default value for **Minimum passphrase length** is 15 characters. The default value for **Maximum passphrase length** is 256 characters.
- b. From the **Password lifetime** drop-down list, choose the time (in days) before the user account is disabled if the password is not changed. The default value is 3650 days.
- c. From the **Expiry warning period** drop-down list, choose the warning (in days) before the user account is given a grace period if the password is not changed. Expiry warning period is the number of days prior to the **Password lifetime**, when a user is warned that the password is about to expire. The default is 14 days. In addition to the **Password lifetime**, the user is also given a **Grace period** to change the password.
- d. From the **Grace period** drop-down list, choose the grace period (in days) before the user account is disabled. Grace period is the number of days in addition to the **Password lifetime** to change the password before the user account is disabled. The default is 3 days.



Once the grace period expires, the admin user will be forced to change the password upon the next log in. Non-admin users will be locked out and the admin user will have to reset their password.

- e. From the **Passphrase generation** drop-down list, choose the option to generate an instant password.

## Managing Appliance Settings

Use this procedure to manage the Cisco NAE appliance settings.

### Procedure

1. Choose **Settings > Appliance Administration**.
2. Click the details icon on the **Appliance Settings** tile.
3. To modify the DNS server, complete the following fields for **DNS Server**.
  - a. Enter the IP address of the primary DNS server.
  - b. (Optional) Enter the IP address of the secondary DNS server.
4. To modify the NTP server, complete the following fields for **NTP Server**.
  - a. Check **Use External NTP Server** check box to configure external NTP server.



We recommend that you use an external NTP server to configure NTP servers. We recommend you to set the NTP time in sync with the local time.


- i. Enter the domain name of the primary NTP server.
  - ii. (Optional) Enter the domain name of the secondary NTP server.
  - b. Uncheck **Use External NTP Server** check box to configure local NTP server.
5. To modify the SMTP server, complete the following fields for SMTP server.

- a. Enter the host name of the SMTP server.
  - b. Enter the port number. Examples include common default ports, SMTP port number 25, or secure SMTP (SSL) port number 465.
  - c. (Optional) Check the **SSL** check box to configure SSL for SMTP.
    - i. Enter the username and password to access the SMTP server.
6. Click **Submit**.

## Managing Assurance Groups

Use this procedure to manage an Assurance Group.

### Procedure


1. Choose **Settings > Assurance Groups**.
  2. Click **Create New Assurance Group** to add an Assurance Group. See [Performing Online Analysis](#).
  3. Click the **Settings** icon to perform the following actions:
    - a. Click **View** to view details of an Assurance Group. This option is enabled when the Assurance Group is in a running state.
    - b. Click **Edit** to edit an existing Assurance Group. Stop the analysis before editing an Assurance Group.
- 
- To edit a NAT configuration file, download the NAT configuration file template, update the file, and then upload it to the Cisco NAE appliance. See [Performing Online Analysis](#).
- c. Click **Delete** to delete an Assurance Group. Stop the analysis before deleting an Assurance Group.
    - The delete operation only deletes the Assurance Group settings in the Cisco NAE.
    - When you delete the Assurance Group, all the analyses corresponding to the Assurance Group will be deleted.
    - To delete an Assurance Group that is part of a schedule, you must first delete the Assurance Group from the schedule and then delete the Assurance Group.
  4. Click **View Schedule** to perform the following actions:
    - a. Click **View Schedule** to view the scheduled order of the Assurance Groups and the approximate time to run the analysis.
    - b. To modify the schedule, select or deselect the Assurance Groups and then choose the desired interval. Review the updated schedule in the **Timeline** and click **Activate**.
    - c. To delete an Assurance Group from an existing schedule, click the Assurance Group to deselect. Review the updated schedule in the **Timeline** and click **Activate**.
    - d. To delete a schedule, click **Delete**. You can only delete a schedule once it is completed.

5. Click the **Start Online Analysis** icon to run the analysis. If the Assurance Group is part of an active schedule, the schedule will stop and the analysis will start on the selected Assurance Group.
6. Click the **Run Analysis on Demand** icon to run the online analysis for a specified number of times. If the Assurance Group is part of an active schedule, the schedule will stop and the analysis will start on the selected Assurance Group.
7. Click **Stop** to stop the analysis on the Assurance Group. If the Assurance Group is part of an active schedule, the analysis on the Assurance Group will stop.

## Managing Offline Analysis

Use this procedure to manage offline analysis.

### Procedure

1. Choose **Settings > Offline Analysis**.
2. . Click **Create New Offline Analysis** to perform online analysis. See [Performing Offline Analysis](#).
3. Select an offline analysis and click the  icon in the **Action** column to perform the following actions:
  - a. Choose **View Epochs** to To view the epochs.
  - b. Choose **Delete** to delete the offline analysis. You cannot delete an offline analysis while the analysis is in progress.



When you delete an offline analysis all the epochs and the epoch delta objects associated with the offline analysis will be deleted.

## Setting Log Levels

Use this procedure to set the log levels.

### Procedure

1. Choose **Settings > Appliance Administration**.
2. Click the details icon on the **Log Level Settings** tile.
3. For each category, choose the log level from the drop-down list. By default, the log levels are set to **Error** setting.
4. Click **Save**.
5. (Optional) Click **Restore to Factory Default**, to reset the log level to the default value.
6. To download the logs, choose **Settings > Download Tech Support Logs**.

# Viewing Data Storage Usage

In the Cisco NAE appliance, analysis data is auto purged once the usage is above 80% and the analysis will be stopped once the analysis is above 90%.

- Only the oldest analysis data is deleted when the data storage usage reaches 80% or above.
- Once the data storage usage is above 90%, the analysis will be stopped. Even if the analysis is stopped due to the 90% threshold, Cisco NAE will continue purging the oldest analysis data until the usage falls below 80%.
- In the rare event that Cisco NAE has stopped the analysis due to the 90% threshold safeguard, the administrator must manually restart the analysis once the usage falls below 80%.

Use this procedure to view the data storage usage of the appliance.

## Procedure

1. Choose **Settings > Appliance Administration**.
2. The data storage usage is displayed in the **Assurance Data Controls** tile.

# Deleting Bundle File

Use this procedure to delete the Cisco NAE bundle file.




## Procedure

1. Choose **Settings > Appliance Administration**.
2. Click the details icon on the **Software Management** tile.
3. In the Upload table, select the bundle file.
4. From the **Actions** menu, choose **Delete**.
5. Click **Delete**.

# Managing Epoch Delta Analysis

Use this procedure to manage a epoch delta analysis.

## Procedure

1. Choose **Epoch Analysis > Epoch Delta Analysis**.
2. Click **Analysis Management**.
3. In the **Delta Analysis** table, select a delta analysis and click the  icon to edit the name.
4. Click the  icon and then choose **Delete** to delete the delta analysis. To delete a delta analysis that is running, you must stop the delta analysis before deleting.
5. Click the  icon and then choose **Stop** to stop a running delta analysis.

6. Click the  icon and then choose **View Results** to view the results of a delta analysis.

## Managing Authentication Domains

Use this procedure to manage authentication domains. Only an administrator can manage authentication domains.

### Procedure

1. Choose **Settings > Appliance Administration**.
2. Click the details icon on the **Authentication Domains** tile.
3. Select the authentication domain.
4. From the **Action** column, choose the **Settings** icon.
5. To edit an authentication domain, click **Edit**. You cannot edit the name of the authentication domain.
6. To delete an authentication domain, click **Delete**. You cannot delete the Local authentication domain.



When you delete an authentication domain, all the users in the authentication domain will be logged out from the appliance.


## Managing Object Selectors

Use this procedure to manage Object selectors.

### Before You Begin

- You have created at least one object selector.

### Procedure

1. Choose **Compliance > Manage Compliance > Object Selectors**.
2. In the Object Selector table that is displayed, click the  icon in the **Action** column for the object selector you want to manage.
3. Choose the action to perform from the following options:
  - a. Choose **Edit** to edit the object selector from the Object Selectors table.
  - b. Choose **Delete** to delete the object selector, and in the **Delete Object Selector** dialog box that is displayed, confirm **Delete**.



If the Object Selector that you want to delete is used in a requirement, remove the association and then delete the Object selector.

- c. Choose **Copy** to copy the values of the existing object selector to create a new object selector, and perform the following actions:



- i. In the **Create New Object Selector** dialog box, in the **Object Selector Name** field, add a name.
- ii. In the remaining pre-populated fields, modify any values as appropriate.
- iii. Click **Save**.


## Managing Traffic Selectors

Use this procedure to manage traffic selectors.

### Before You Begin

- You have created at least one traffic selector.

### Procedure

1. Choose **Compliance > Manage Compliance > Traffic Selectors**.
2. In the Traffic Selector table that is displayed, click the  icon in the **Action** column for the Traffic selector you want to manage.
3. Choose the action to perform from the following options:
  - a. Choose **Edit** to edit the traffic selector from the Traffic Selectors table.
  - b. Choose **Delete** to delete the traffic selector, and in the **Delete Traffic Selector** dialog box that is displayed, confirm **Delete**.



If the Traffic Selector that you want to delete is used in a requirement, remove the association and then delete the traffic selector.


## Managing Compliance Requirements

Use this procedure to manage compliance requirements.

### Before You Begin

- You have created at least one compliance requirement.

### Procedure

1. Choose **Compliance > Manage Compliance > Compliance Requirements**.
2. Click the  icon in the **Action** column for the compliance requirement you want to manage.
3. Choose the action to perform from the following options:
  - a. Choose **Edit** to edit the compliance requirement from the **Edit Compliance Requirement** area.
  - b. Choose **Delete** to delete the compliance requirement, and in the **Delete Compliance Requirement** dialog box that is displayed, confirm **Delete**.



If the Compliance Requirement that you want to delete is used in a requirement set, remove the association and then delete the Compliance Requirement.


## Managing Compliance Requirement Sets

Use this procedure to manage compliance requirement sets.

### Before You Begin

- You have created at least one compliance requirement set.

### Procedure

1. Choose **Compliance > Manage Compliance > Compliance Requirement Sets**.
2. Click the  icon in the **Action** column for the compliance requirement you want to manage.
3. Choose the action to perform from the following options:
  - a. Choose **Edit** to edit the compliance requirement set from the **Edit Requirement Set** area.
  - b. Choose **Delete** to delete the compliance requirement set, and in the **Delete Requirement Set** dialog box that is displayed, confirm **Delete**.



If the Requirement Set is associated with an assurance group, disassociate the Requirement Set and then delete the Requirement Set.


## Managing Event Rules

Use this procedure to manage event rules.

### Before You Begin

- You have created at least one event rule.

### Procedure

1. Choose **Smart Events > Manage Events Rules > Event Rules**.
2. Select an event rule and click the  icon in the **Action** column to perform the following actions:
  - a. Choose **Edit** to edit the event rule.
  - b. Choose **Copy** to copy the event rule.
  - c. Choose **Delete** to delete the event rule.
3. Click an event rule to view the details of the event rule.



## Managing Event Rulesets

Use this procedure to manage event rulesets.

## Before You Begin

- You have created at least one event ruleset.

## Procedure

1. Choose **Smart Events** > **Manage Events Rules** > **Event Rulesets**.
2. Select an event ruleset and click the  icon in the **Action** column to perform the following actions:
  - a. Choose **Associate** to associate the event ruleset to the current Assurance Group.
  - b. To associate the event ruleset to a different assurance group,
    - i. Select the Assurance Group from the **Assurance Group** drop-down list.
    - ii. Select the event ruleset and click the  icon in the **Action** column.
    - iii. Choose **Associate**.
  - c. Choose **Activate** to activate the event ruleset. To activate an event ruleset, it must be associated with an Assurance Group. Activating an event ruleset not associated with an Assurance Group, automatically associates the event ruleset with the current Assurance Group and activates the event ruleset.
  - d. Choose **Disassociate** to disassociate the event ruleset from the current Assurance Group. Disassociating an active event ruleset will deactivate the event ruleset.
  - e. Choose **Deactivate** to deactivate the event ruleset.
  - f. Choose **Edit** to edit the event ruleset.
  - g. Choose **Copy** to copy the event ruleset.
  - h. Choose **Delete** to delete the event ruleset. Deleting a ruleset does not delete the rules included in the ruleset.

# Troubleshooting

## Downloading Logs

Use this procedure to download the logs for the Cisco NAE appliance.

### Procedure

1. Choose **Settings > Download Tech Support Logs**. The logs are collected from each VM in the cluster and they are aggregated into a tar file. Downloading logs can take up to several minutes. Do not refresh the browser during the download.
2. (Optional) If it is taking more than 5 minutes for the tech support logs to be downloaded, you can access the logs using the following procedure. You can also use this procedure, if you receive an error message while downloading the tech support logs.
  - a. Contact Cisco TAC to obtain the one time password (OTP) for root access.
  - b. Log in to one of the VMs of the appliance as root.
  - c. Run the following command:

```
/usr/lib/candid/share/support/tech_support --logs --dir /hadoop/network-audits  
--output tech_support
```

- d. Download the following tar file from the VM and provide it to TAC for debugging.

```
/hadoop/network-audits/tech_support.<timestamp>.tar
```

## Appliance Events

Cisco NAE raises **Appliance Events** to monitor the health of the appliance. These events are generated as part of the cron job that is installed on all the hosts and the cron job is configured to run every 5 mins. The **Appliance Events** are useful for troubleshooting the appliance.

### Procedure

1. Choose **Settings > Appliance Status**.
2. Click **Event Name** to view the details of the event.

## Appliance Event Types

The **Appliance Events** are categorized into the following types.

## Provisioned Capacity Events

These events monitor the appliance capacity provisioned with respect to the defined specifications of the appliance. These events are generated at every reboot. The different specifications are defined for the different flavors of the appliance. The following events are included in this category.

1. APPLIANCE\_PROVISIONED\_CAPACITY\_BELOW\_SPEC
2. APPLIANCE\_PROVISIONED\_CAPACITY\_ABOVE\_SPEC
3. APPLIANCE\_PROVISIONED\_CAPACITY\_AT\_SPEC

## Local Filesystem Usage Events

These events monitor the storage usage on each of the hosts.

The following events are included in this category.

1. APPLIANCE\_FILESYSTEM\_NORMAL
2. APPLIANCE\_FILESYSTEM\_EXCEEDED\_LOW\_WATERMARK
3. APPLIANCE\_FILESYSTEM\_EXCEEDED\_HIGH\_WATERMARK

## Web Server Events

These events monitor the health of the web servers. The following events are included in this category.

1. APPLIANCE\_WEB\_SERVICES\_OPERATION\_NORMAL
2. APPLIANCE\_WEB\_SERVICES\_PARTIAL\_FAILURE
3. APPLIANCE\_WEB\_SERVICES\_COMPLETE\_FAILURE

## Application Server Events

These events monitor the health of the application servers. The following events are included in this category.

1. APPLIANCE\_APPLICATION\_OPERATION\_NORMAL
2. APPLIANCE\_APPLICATION\_PARTIAL\_FAILURE
3. APPLIANCE\_APPLICATION\_COMPLETE\_FAILURE

## Database Events

These events monitor the health of the database. The following events are included in this category.

1. APPLIANCE\_DATABASE\_OPERATION\_NORMAL
2. APPLIANCE\_DATABASE\_PARTIAL\_FAILURE
3. APPLIANCE\_DATABASE\_REACHED\_LOW\_THRESHOLD
4. APPLIANCE\_DATABASE\_AT\_PURGE\_LIMIT

## **Analysis Latency Events**

These events monitor the time taken to analyze the data. Each analysis is associated with an analysis interval and analysis must be completed within the specified interval time.

The following events are included in this category.

1. ANALYSIS\_COMPLETED
2. ANALYSIS\_COMPLETED\_BUT\_TOOK\_TOO\_LONG
3. ANALYSIS\_TIMED\_OUT

## **Analysis Application Events**

These events monitor the health of the analysis application.

The following events are included in this category.

1. APPLIANCE\_ANALYSIS\_ENGINE\_OPERATION\_NORMAL
2. APPLIANCE\_ANALYSIS\_ENGINE\_FAILURE

## **HDFS Filesystem Events**

These events monitor the health of the namenodes and datanodes.

The following events are included in this category.

1. APPLIANCE\_FILESYSTEM\_OPERATION\_NORMAL
2. APPLIANCE\_FILESYSTEM\_PARTIAL\_FAILURE
3. APPLIANCE\_FILESYSTEM\_COMPLETE\_FAILURE

## **YARN Events**

These events monitor the health of the resource Managers and node managers.

The following events are included in this category.

1. APPLIANCE\_INFRA\_RESOURCE\_OPERATION\_NORMAL
2. APPLIANCE\_INFRA\_RESOURCE\_PARTIAL\_FAILURE
3. APPLIANCE\_INFRA\_RESOURCE\_COMPLETE\_FAILURE

## **Host Reachability Events**

These events monitor if all the hosts are reachable from all other hosts in cluster. A ping test is used to test reachability of the hosts.

The following events are included in this category.

1. ALL\_CLUSTER\_MEMBERS\_ARE\_REACHABLE

## Troubleshooting Scenarios

This section contains information about possible solutions for common troubleshooting scenarios for the Cisco NAE appliance.

### Problem

Unavailability of the datastore in the host results in the failure of the file system IO located in the guest VM of the Cisco NAE appliance. As a result, the guest VM's kernel filesystem driver marks the mounted file system as read-only making the Cisco NAE appliance unavailable. The functionality of the Cisco NAE appliance such as generating new epochs, collecting tech support logs, and accessing the UI is affected.

### Solution

To resolve this issue, contact Cisco TAC.