



Cisco NAE Policy Explorer Application User Guide

Table of Contents

Cisco NAE Policy Explorer App	3
About NAE Policy Explorer App	3
Use Cases	3
Compatibility Information	5
Important Notes	5
Verified Scalability Limits	6
Verified Scalability Limits for NAE Policy Explorer App, Release 1.0 and Release 1.2	6
Verified Scalability Limits for NAE Policy Explorer App, Release 2.0	6
Licensing Information	8
Supported Browsers	8
Supported ACI Features	8
Not Supported ACI Features	8
Guidelines and Limitations	9
Creating a Query using NAE Policy Explorer	10
Procedure	10
Supported Queries	12
Supported What Queries	12
Supported Can Queries	15

First Published: 2019-07-03

Last Modified: 2019-07-24

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 NAE Policy Explorer App

About NAE Policy Explorer App

The NAE Policy Explorer app 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 NAE Policy Explorer app 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 app allows operators to easily discover associations between traditional networking constructs such as VRFs, subnets, VLANs to the ACI object model.

The app is based on natural language query interface. The 3 types of queries supported by the app 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*.

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.

Compatibility Information

The following table lists the compatibility information for the NAE Policy Explorer app.

Table 1. Cisco ACI Compatibility Information

NAE Policy Explorer Release	Cisco APIC Release	Cisco ACI-Mode NX-OS Switch Software Release for Cisco Nexus 9000 Series ACI-Mode Switches
2.0	4.0	14.0
1.2	<ul style="list-style-type: none">• 4.0• 3.2	<ul style="list-style-type: none">• 14.0• 13.2
1.0	<ul style="list-style-type: none">• 4.0• 3.2	<ul style="list-style-type: none">• 14.0• 13.2

Important Notes

- The NAE Policy Explorer app, Release 1.0 and Release 1.2 has a maximum size limit of 2 GB.
- The NAE Policy Explorer app, Release 2.0 has a maximum size limit of 8 GB of memory.
- The NAE Policy Explorer app, Release 1.0 and Release 1.2 has a maximum size limit of 2 GB on Cisco APIC release 3.2 and 4.0. If the ACI policy configuration utilizes more than 2 GB of memory, the snapshot action fails.

Verified Scalability Limits

Verified Scalability Limits for NAE Policy Explorer App, Release 1.0 and Release 1.2

The following tables lists the maximum verified scalability limits for the NAE Policy Explorer app.

Table 2. Verified Scalability Limits for ACI Network Mode

Feature	Scale
Number of APIC Controllers	3, 5, or 7 node APIC cluster
Number of leaf switches	40
Number of tenants	10
Number of end point groups (EPGs)	100
Number of bridge domains (BDs)	100
Number of VRFs	10
Number of end points	2 K

Table 3. Verified Scalability Limits for ACI Application Mode

Feature	Scale
Number of APIC Controllers	3, 5, or 7 node APIC cluster
Number of leaf switches	20
Number of contracts/filters	100
Number of actrIRules fabric wide	10 k
Number of tenants	5
Number of end point groups (EPGs)	100
Number of bridge domains (BDs)	100
Number of VRFs	5
Number of end points	1 K

Verified Scalability Limits for NAE Policy Explorer App, Release 2.0

The following tables lists the maximum verified scalability limits for the NAE Policy Explorer app.

Table 4. Verified Scalability Limits for ACI Network Mode

Feature	Scale
Number of APIC Controllers	3, 5, or 7 node APIC cluster
Number of leaf switches	40
Number of tenants	20
Number of end point groups (EPGs)	500
Number of bridge domains (BDs)	500

Feature	Scale
Number of VRFs	20
Number of end points	4 K

Table 5. Verified Scalability Limits for ACI Application Mode

Feature	Scale
Number of APIC Controllers	3, 5, or 7 node APIC cluster
Number of leaf switches	40
Number of contracts/filters	250
Number of actrIRules fabric wide	100 k
Number of tenants	20
Number of end point groups (EPGs)	300
Number of bridge domains (BDs)	300
Number of VRFs	10
Number of end points	4 K

Licensing Information

The NAE Policy Explorer app can be downloaded from the ACI App store.

For licensing information see the the *NAE Policy Explorer Ordering Guide*.

Supported Browsers

- Chrome

Supported ACI Features

The following ACI features are supported by the NAE Policy Explorer app.

- All scopes of contracts such as global, tenant, application profile, VRF
- Taboo contracts
- vzAny contracts
- Unenforced VRF's
- Contract preferred groups

Not Supported ACI Features

The following ACI features are not supported by the NAE Policy Explorer app.

- IPv6
- Microsegmentation
- Deny contracts
- Service graphs

Guidelines and Limitations


- In the NAE Policy Explorer app, only one policy snapshot is available for analysis at a time. If you choose another snapshot for analysis, the model results for the previous snapshot are discarded from memory and have to be recomputed.
- Local file system persistence is supported for the NAE Policy Explorer app.
- Upgrading the NAE Policy Explorer app is not supported. Reinstalling the app results in loss of the existing data.

Creating a Query using NAE Policy Explorer

Use this procedure to create a query using the NAE Policy Explorer app.

Procedure

1. Log in to the Network Connectivity Explorer app.
2. Choose one of the two options:
 - a. Perform the following steps when you log in to the Network Connectivity Explorer app for the first time.
 - i. In the **Timeline**, click the camera icon to take a snapshot and perform analysis.
 - ii. Enter the credentials for Cisco APIC.
 - b. If you have logged in to the app previously, in the **Timeline** select the snapshot to make it active. Analysis is carried out against an active snapshot.
 - A snapshot can be in one of the following colors:
 - Dark Blue: This indicates that the the snapshot is ready for analysis.
 - Light Blue: This indicates that the collection is in progress.
 - The size of the snapshot indicates the status of the snapshot.
 - Small: This indicates that the snapshot collection failed.
 - Big: This indicates that the snapshot collection is successful.
3. 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](#). The results of the query are displayed in the results table.
4. 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.
5. Click **Source** and select one or more entities from the results table.
6. Click **Destination** and select one or more entities from the results table.
7. Click **Can they talk** to determine if the two entities can communicate with each other.
8. (Optional) Click **Reverse Query** to reverse the source and destination entities for a Can query.
9. Click **Which entities can talk** to view the communication between the entities. In the radial view, the connectivity between entities is displayed with a solid colored arc.



If the query results are large, the message “Too much data to display” is displayed. Use the Search bar to create a more specific query for the results to be displayed.
9. Select the arc connecting the two entities and click **How do they talk**. The following communication details are displayed in the **How do they talk** results table.
 - Source: The source EPG.
 - Destination: The destination EPG.

- Flow Origin: Type of flow.
- Flow Owner: The object DN responsible for the flow.
- Ether Type: The ethernet type.
- Protocol: The protocol (TCP or UDP) used for communication.
- Source Port From: The protocol of the starting port of the source port range.
- Source Port To: The protocol of the ending port of the source port range.
- Destination Port From: The protocol of the starting port of the destination port range.
- Destination Port To: The protocol of the ending port of the destination port range.
- TCP Rules: The TCP session rules.

Supported Queries

The following table lists the queries supported by the NAE Policy Explorer app.

Supported What Queries

Table 6. Supported What Queries

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

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

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

Supported Can Queries

Table 7. Supported Can Queries

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

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

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

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