



Cisco NAE Policy Explorer Application Release Notes, Releases 1.2 and 2.0

Table of Contents

NAE Policy Explorer, Releases 1.2 and 2.0	3
Introduction	3
NAE Policy Explorer Support	3
Usage Guidelines	5
Caveats	6
Open Caveats	6

First Published: 2019-07-8

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.

NAE Policy Explorer, Releases 1.2 and 2.0

This document describes the features, caveats, and usage guidelines for the NAE Policy Explorer.

Additional product documentation is listed in the **Related Documentation** section.

Release notes are sometimes updated with new information about restrictions and caveats.

Table 1 shows the online change history for this document.

Table 1. Online History Change

Date	Description
July 8, 2019	Created the release notes for the 1.2 and 2.0 releases.

Introduction

The NAE Policy Explorer provides 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.

This application uses a structured Natural Query Language to help Operations teams explore policy associations, get visibility, and perform connectivity analysis between end points, EPGs, and other networking assets.

NAE Policy Explorer Support

The following table shows supported features, APIC versions, and footprint information by release. New software features supported in releases 2.0 and 1.2 are listed here. Existing software features that are available starting with Release 1.0 are also listed in this table.

Table 2. NAE Policy Explorer Features by Release

Release	Feature	Supported with APIC Release	App Footprint
Releases 2.0	<ul style="list-style-type: none"> • What Queries with 'and' and 'or' • Can Queries with ports, protocols and port ranges • Can Queries with 'any' keyword for selected object 	APIC release 4.0(1h) and later	8 GB
Release 1.2	<ul style="list-style-type: none"> • What Queries with 'and' and 'or' • Can Queries with ports, protocols and port ranges • Can Queries with 'any' keyword for selected object 	APIC release 3.2(5f) and later	2 GB
Release 1.0	<ul style="list-style-type: none"> • What Query: What EPs are connected to EPG:X and BD:Y • Can Query: Can A talk to B or Can A talk to B via C • Can Queries with 'any' keyword for selected object 	APIC release 3.2(5f) and later	2 GB

Usage Guidelines

The NAE Policy Explorer, Release 1.2 and Release 2.0 are compatible with Cisco Application Policy Infrastructure Controller, Release 4.0(1h).

Caveats

Open Caveats

This section lists the open caveats. Click the bug ID to access the Bug Search tool and see additional information about the bug.

Release notes are sometimes updated with new information about restrictions and caveats.



The following open caveats apply to NAE Policy Explorer Release 2.0 and not to Release 1.2.

Table 3. Open Caveats in APIC Release 4.0(1h)

Bug ID	Description
CSCvq17245	NAE Policy Explorer app provides duplicate entries for Can Query between EPGs with contract preferred group (CPG) enabled.