



Cisco Network Assurance Engine  
Installation and Upgrade Guide,  
Release 5.0(1)

# Table of Contents

Cisco Network Assurance Engine .....	3
Overview .....	3
Architecture .....	5
Management and Network Connectivity .....	7
Assurance Control Modes .....	11
Installation Requirements .....	13
System Requirements .....	13
Hypervisor Requirements .....	14
Supported Browsers .....	14
Cisco HyperFlex Systems Support .....	14
Software Compatibility Information .....	16
ACI Features Assured by Cisco NAE .....	18
ACI Features Not Supported by Cisco NAE .....	20
NX-OS Features Assured by Cisco NAE .....	22
NX-OS Features Not Supported by Cisco NAE .....	23
Verified Scalability Limits for ACI Fabric .....	24
Verified Scalability Limits for NX-OS Fabric .....	25
Increasing Disk Size .....	28
Installing Cisco Network Assurance Engine .....	29
Prerequisites .....	29
Prerequisites for ACI .....	29
Prerequisites for DCNM .....	29
Guidelines and Limitations .....	30
Installation and Initial Configuration Workflow .....	31
Installing the Cisco NAE OVA .....	31
Setting Up the Cisco NAE Appliance .....	32
Editing Time Configuration for a Host .....	35
Uploading Certificates .....	36
Uploading A LDAP Certificate .....	36
Uploading A Certificate Authority Signed Certificate for the Web Server .....	37
Smart Licensing .....	40
Introduction to Smart Licensing .....	40
More About Smart Licensing .....	40
Smart Licensing Evaluation Period .....	40
Smart Licensing Authorization Status .....	41
Smart Licensing Authorization Guidelines .....	42
Smart Licensing Usage Guidelines .....	43
Pre-Registration Verifications .....	43

Initial Cisco NAE Login and Smart Licensing Pre-Registration .....	43
Transport Setting .....	44
Registering for Smart Licensing With Direct Connect to CSSM .....	44
Registering for Smart Licensing With Transport Gateway/Cisco Smart Software Manager On- Prem .....	45
Using HTTPS for Transport Gateway/Cisco Smart Manager On-Prem .....	46
Registering for Smart Licensing With HTTP or HTTPS Proxy .....	47
Deregister .....	48
Renew Authorization .....	48
Renew Registration .....	49
Reregister Product If Already Registered .....	49
Troubleshooting Cisco NAE Licensing .....	49
Upgrading and Downgrading Cisco Network Assurance Engine .....	51
Supported Upgrade Paths for Cisco NAE .....	51
Upgrading Cisco NAE OVA .....	52
Creating VM Snapshots .....	53
Downgrading Cisco NAE .....	54
Migrating Cisco Network Assurance Engine Appliance .....	55
Migrating Cisco NAE Appliance .....	55

First Published: 2020-07-24

Last Revised: 2021-03-05

**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)

© 2017-2021 Cisco Systems, Inc. All rights reserved.

# Cisco Network Assurance Engine

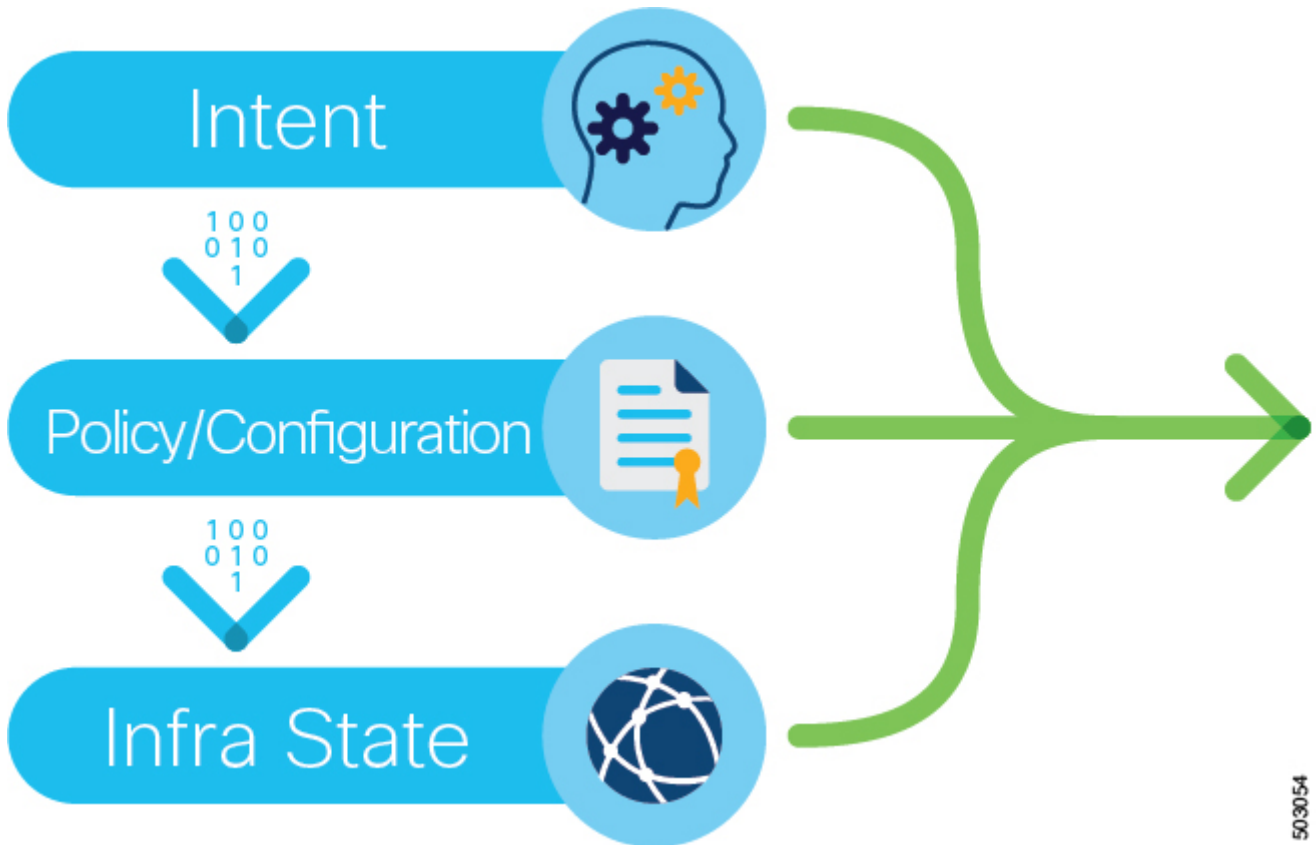
## Overview

The Cisco Network Assurance Engine (NAE) software provides operators with a new approach to manage SDN-based data centers confidently. The Cisco NAE software is built on a comprehensive formal model of the network, combined with deep domain knowledge of networking. The Cisco NAE software provides operations teams with continuous and proactive network verification and intent assurance.

Business drivers such as cloud, mobile, and digitization trends are demanding more from modern data centers, rapidly increasing their scale, rate of change, and complexity. With NX-OS fabrics, Cisco Application Centric Infrastructure (ACI) and other SDN technologies, network infrastructures have evolved to provide programmable interfaces, automation, agility, and virtualization. However, operational tools still center around traditional approaches, such as probe tools, packet sniffers, and the command line interface (CLI) to reason about the network. These are inherently reactive-after-the-fact, manual, and rely on the tribal knowledge of a handful of experts to reasonably reconstruct a network state.

Cisco NAE release 5.0(1) and onwards, the assurance engine supports analysis for both ACI and NX-OS data center fabric deployments. NAE support for NX-OS fabric is made possible with onboarding DCNM.

The Cisco NAE software takes the intent from the controller as a logical policy, or it derives the intent as well as configurations and the data plane (infra) state from each switch device, to build a network-wide model of the underlay, overlay, and virtualization layers.



503054

Figure 1. Taking/Deriving the intent, policy, configuration, and the infra state from a device



Figure 2. Network-wide model of the underlay, overlay, and virtualization layers

Leveraging formal mathematical techniques and a deep understanding of the networking domain, the Cisco NAE software is able to answer three fundamental questions about the network:

1. How do I guarantee that I have not introduced errors into the fabric while specifying my policy and configuration?
  - In SDN networks, the impact of a misconfiguration is amplified with centralized automation
  - With increased frequency of changes, misconfigurations are much more common

## 2. How do I understand the actual current state of the network?

- Dynamic events (protocol learning, VM mobility, and so on) can make the network deviate from the intended state
- Central intent has to be propagated to multiple nodes in a large distributed system; consistency issues are unavoidable in such systems
- With multiple abstraction layers in SDN networks, manually inspecting and reconstructing the network state and configuration has become prohibitively challenging

## 3. How do I rapidly diagnose the network for the root cause when issues arise?

- How do I identify these lingering issues before they impact the application?
- How do I reduce the cost of downtime?

By proactively running this broad set of checks on the network model and providing deep visibility across the fabric, the Cisco NAE software transforms the operating mode from reactive to proactive. The Cisco NAE software enables operators to predict network outages and vulnerabilities before they impact business, reduce risk while accelerating changes and migrations, and rapidly find the root cause of problems. With a complete diagnostic record and compliance rules, operators can ensure continuous compliance and satisfy audits.



Not all features are supported across Cisco ACI and Cisco DCNM Assurance Groups. Please check the Release Notes and other documentation for support details related to your Assurance Group.

## Architecture

The Cisco NAE can be deployed as a cluster of three virtual machines. The main components include:



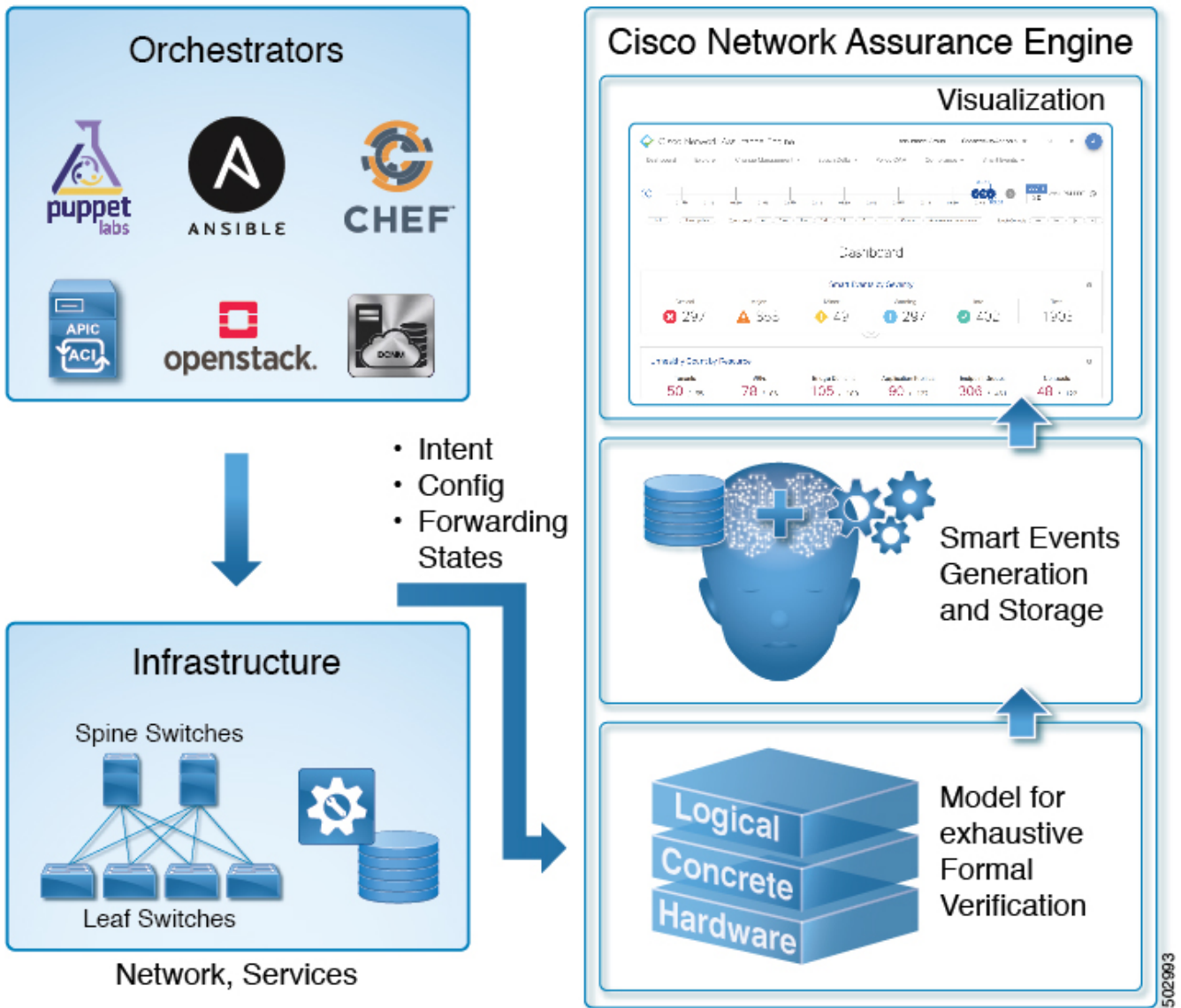


Figure 3. Cisco NAE Architecture

- Data collection—The data collection components are responsible for discovering the fabric comprising of the APIC or DCNM controller(s) for ACI and NX-OS respectively, spine switches, and leaf switches. Data collection components also poll the discovered fabric to collect APIC logical model in case of ACI, DCNM topology in case of NX-OS, and switch concrete model data via REST API interface. The forwarding tables stored in the switch hardware memory such as TCAMs are collected using the SSH interface.
- Formal Modeling—The formal modeling component uses mathematical based techniques to determine if the intent specified in the ACI Assurance Group or DCNM Assurance Group has been met.
- Smart Events— The results of the analysis and formal modeling are generated as **Smart Events** and they are displayed in the Smart Events tab in the GUI.
- Visualization— A graphical representation of the analysis performed by the Cisco NAE and the information generated by the Cisco NAE is displayed in the **Visualization** area of the GUI. The visualization area is a powerful tool for quickly discovering problems with network nodes and configuration, and also seeing a detailed view of each issue.



Not all features are supported across ACI and DCNM Assurance Groups. Please check the Release Notes and other documentation for support details related to your Assurance Group for support information.

## Management and Network Connectivity

The Cisco NAE can be deployed as a cluster of three virtual machines.

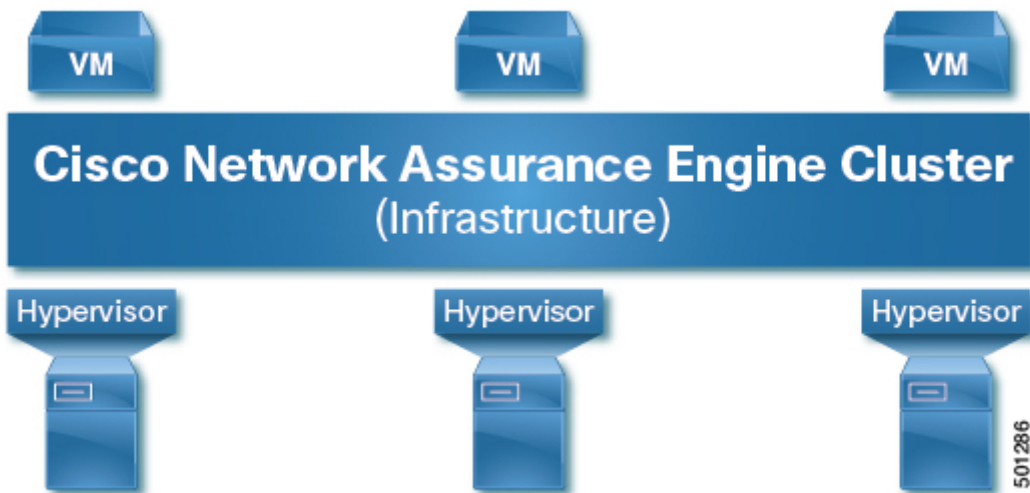


Figure 4. Cisco NAE Appliance

Cisco NAE can be deployed using the following design options to access the management network of the fabric.

- Out-of-band management interface
- In-band management interface (for Cisco ACI fabric)

By default, out-of-band management interface will be used to access the management network of the Cisco ACI fabric. If out-of-band management interface is not configured, then in-band management interface will be used. If both out-of-band management interface and in-band management interface are configured, then out-of-band management interface will be used.



See the *Cisco Network Assurance Engine App Installation and Upgrade Guide* for information on Cisco NAE app on Cisco Application Services Engine.

### Out-of-Band Management Access

With out-of-band management access (OOB), the Cisco NAE appliance can access the ACI or the NX-OS fabric on the out-of-band network. We recommend that you use out-of-band management access to connect the Cisco NAE.

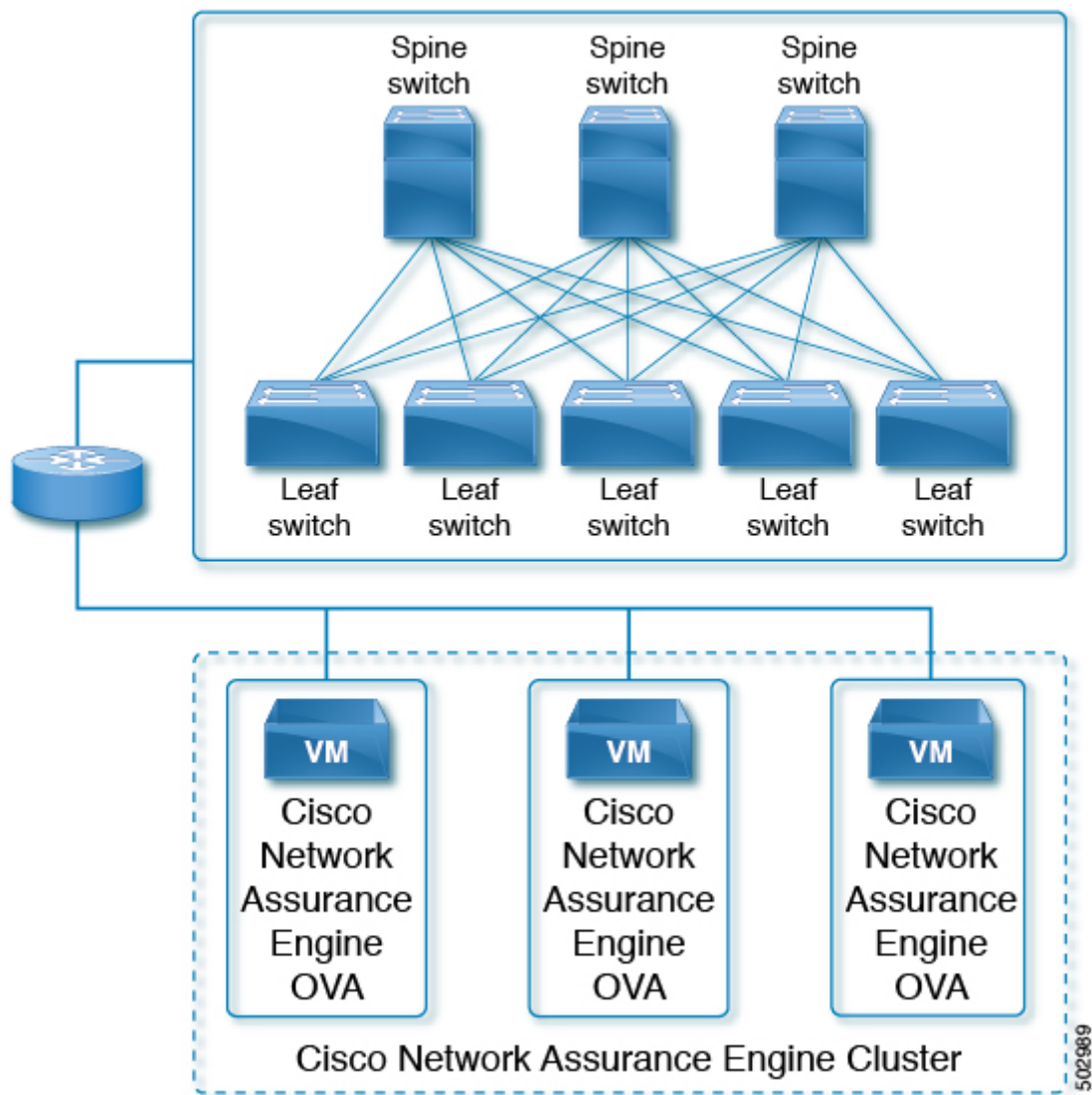


Figure 5. Out-of-Band Management Access

### In-Band Management Access (Currently, this is supported for ACI Assurance Group only)

With in-band management access, the Cisco NAE appliance will use the leaf switches for in-band access to the ACI fabric.

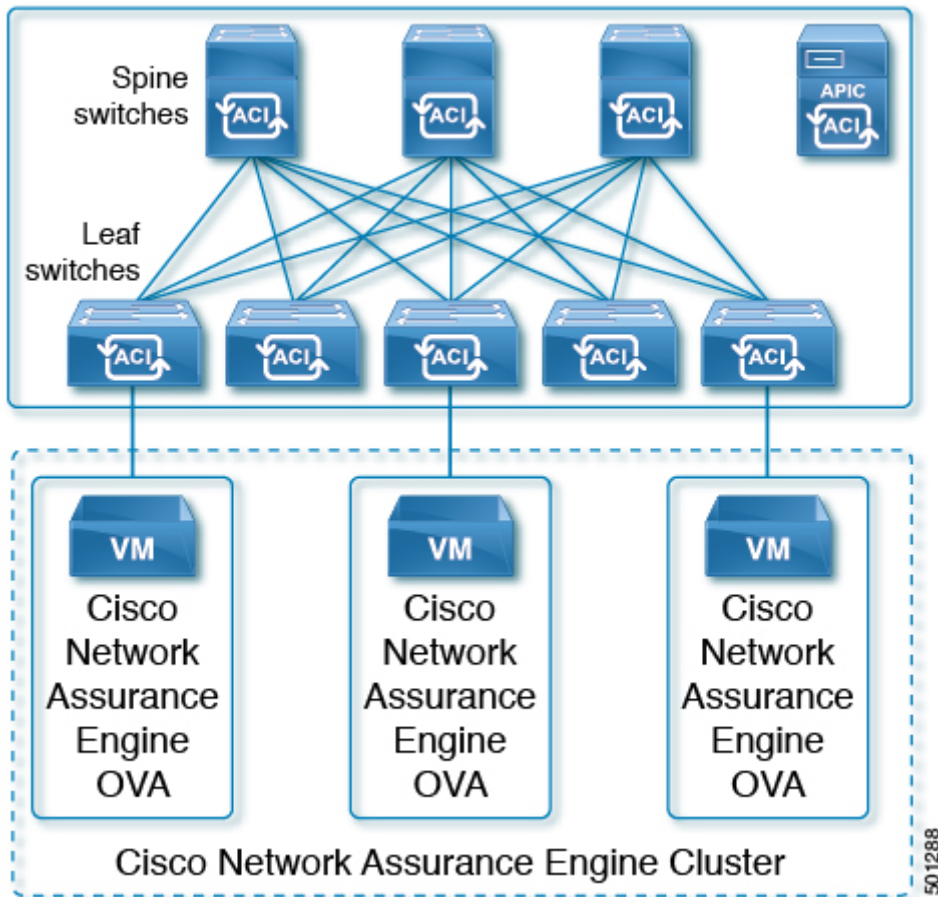


Figure 6. In-Band Management Access

## Network Address Translation (NAT) Deployment (Supported for ACI Assurance Group only)

Starting with Cisco NAE release 2.1(1), Network Address Translation (NAT) deployment is supported. NAT can be deployed using out-of-band management or in-band management interface. Cisco NAE can access Cisco ACI fabric deployed across the NAT boundary. In this topology, Cisco NAE communicates with Cisco APIC through NAT.

The following deployment options for NAT are supported:

- NAT with out-of-band management interface

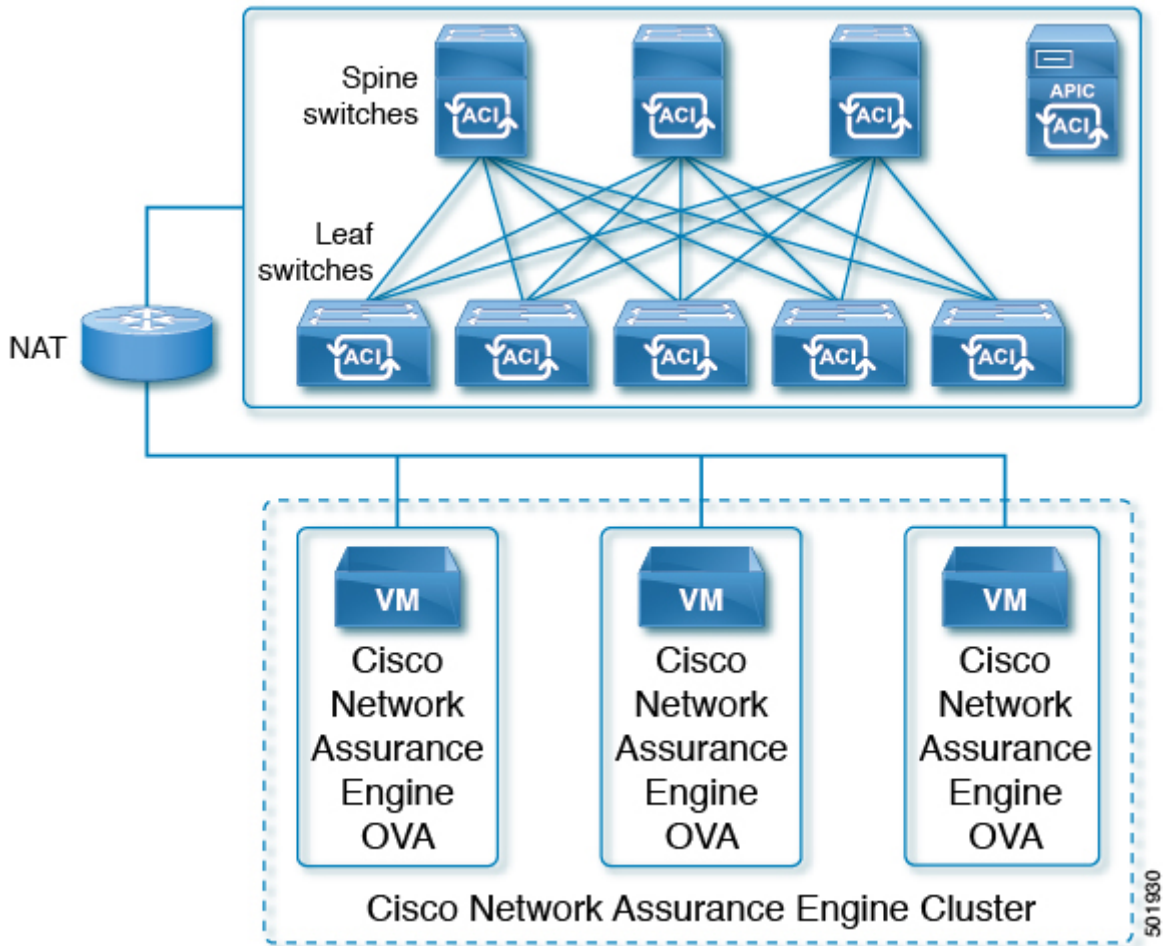


Figure 7. NAT with Out-of-Band Management Access

- NAT with in-band management interface

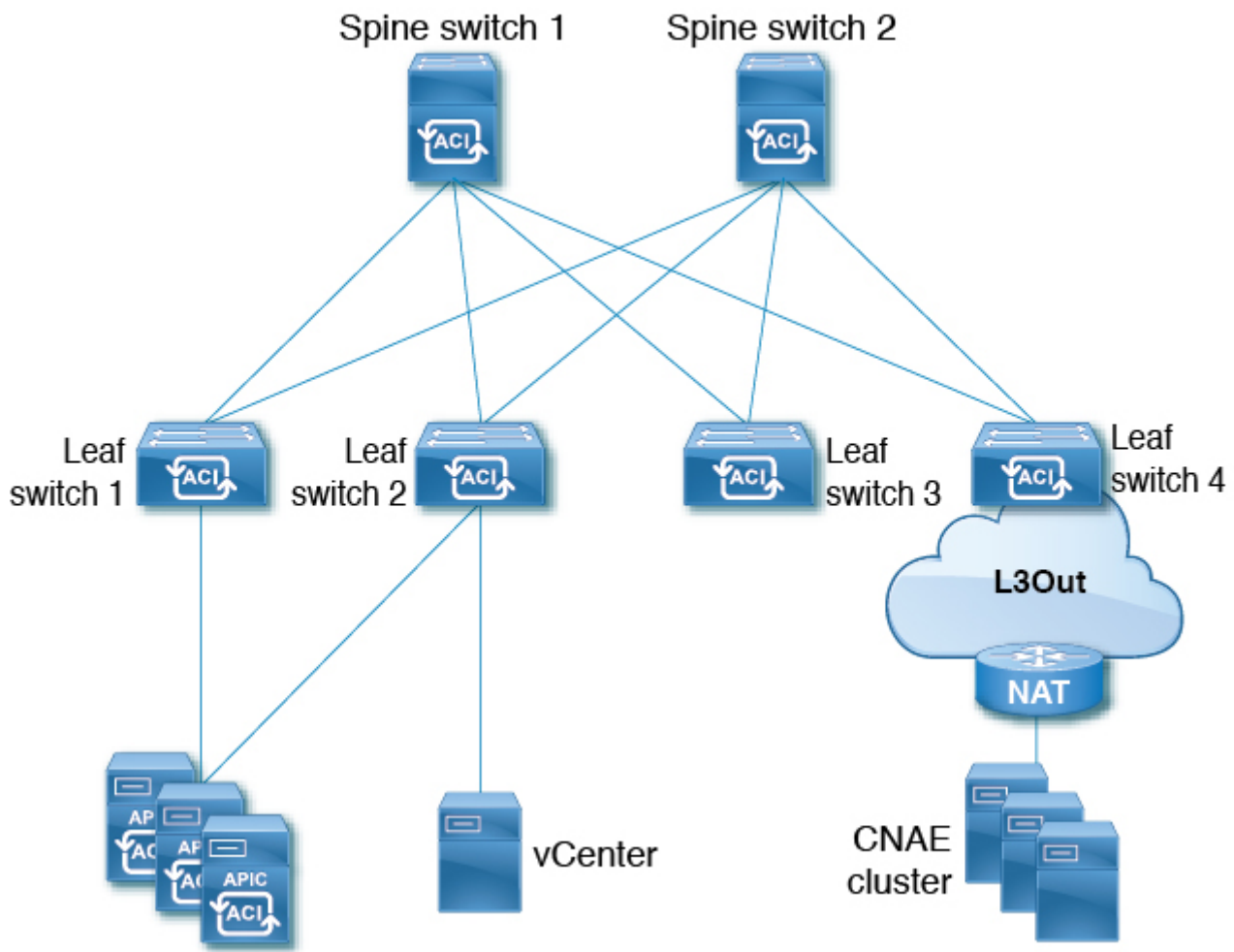


Figure 8. NAT with In-Band Management Access

## Important Notes

- For Cisco NAE deployment behind NAT, there should not be any overlaps between out-of-band subnets and in-band subnets in the network.
- Ensure that in-band and out-of-band IP addresses are routable for Cisco NAE to access the ACI fabric.

## 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 fabric, either ACI or NX-OS.

- 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.
- A NX-OS fabric is made up of all leaf switches and spine switches. The DCNM controller collects the NX-OS topology information. Only the leaf switches and spine switches are analyzed together as part of the Assurance Group.

A single instance of Cisco NAE can analyze an online collection of both ACI and DCNM Assurance

501867

Groups, in a round robin, using the fabric scheduler function. A single instance of Cisco NAE can also analyze both ACI and DCNM Assurance Group offline collection data sets.

Optionally, an Assurance Entity (if it exists in the ACI fabric) can be included in the Assurance Group. An Assurance Entity is an ancillary item in the ACI fabric that provides support to the overall fabric. For example, a load balancer would be considered an ancillary item in an ACI fabric and could be included in an 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 Cisco NAE release 4.0(1), you can analyze multiple Assurance Groups. See the *Cisco NAE Getting Started Guide* for more information.

# Installation Requirements

## System Requirements

There are three models currently shipping with Cisco NAE: Small, Medium, and Large. The following tables identify the system requirements for installing the Cisco NAE.

Table 1. System Requirements

Requirement	Appliance Model: Small	Appliance Model: Medium	Appliance Model: Large
Model	NAE-V500-S	NAE-V1000-M	NAE-V2000-L
Virtual Machines	3 VMs	3 VMs	3 VMs
CPU (vCores per VM)	8	12	24
Memory (GB per VM)	40	64	96
Disk	1 TB in total per VM	2 TB in total per VM	4 TB in total per VM
Storage	SSD	SSD	SSD
APIC Fabric Size	50 leaf switches for a 3 VM cluster	100 leaf switches for a 3 VM cluster	400 leaf switches for a 3 VM cluster
NX-OS Fabric Size	40 leaf switches for a 3 VM cluster	100 leaf switches for a 3 VM cluster	N/A

## Important Notes

- Starting from release 3.0(1), HDD storage is not supported.
- In a production environment, the supported and required configuration for Virtual Disks is to use Thick Provision. In the Lab environment if you have configured the Cisco NAE appliance using Thin Provision, you must not use the same appliance in the production environment.
- The recommended Intel processor for vCPUs mentioned in the table System Requirements is Intel® Xeon® CPU E5-2697A v4 @ 2.60GHz, or later.
- For a particular Cisco NAE model, the disk space required depends on the retention period of the epoch data. To increase the disk size, See [Increasing Disk Size](#).
- The IOPS performance numbers for storage system SSDs tested are as follows:
  - Sequential Read (up to) 550 MB/s
  - Sequential Write (up to) 500 MB/s
  - Random Read (100% Span) 84000 IOPS
  - Random Write (100% Span) 27000 IOPS
  - Read/Write Latency < 70 μs



## Important Notes for Cisco ACI Fabric Support Only

- Network latency requirement for reachability to APIC or fabric <30ms latency and 500Mbps bandwidth.

## Hypervisor Requirements

Requirement	Description
VMware vSphere	ESXi 5.5, 6.0, 6.5, 6.7

## Important Notes

- VMware Virtual Machine File System (VMFS5) datastore is required for VMware vSphere.
- Download the Cisco NAE software image based on the Cisco NAE appliance model type and the VMware vSphere version. For ESXi version 5.5, use the Cisco NAE software image for VMware vSphere version 6.0.

For example, to install Cisco NAE, Release 2.0(1b) software, for appliance model small and for VMware version ESXi version 5.5, download the image [cisco\\_nae\\_v500\\_s2\\_k9-2.0.1b\\_6.0-install.zip](#).

- VMware vSphere vMotion or live migration must be disabled for all three VMs in the NAE cluster.

## Supported Browsers

- Chrome

## Cisco HyperFlex Systems Support

The following section lists the system requirements for Cisco NAE on Cisco HyperFlex Systems.

Requirement	Description
HyperFlex Model	HX240c M5 SFF Hybrid (HX240C-M5SX)
HyperFlex Release	4.0(1b)
VMware vSphere Release	VMware ESXi 6.5
Number of servers	3
Memory	<ul style="list-style-type: none"><li>• Free: 433.58 GB</li><li>• Used: 78.07 GB</li><li>• Capacity: 511.65 GB</li></ul>
Storage	SSD
Disk	1.5 TB * 18

<b>Requirement</b>	<b>Description</b>
Processor	Intel® Xeon® Platinum 8176 CPU @ 2.10GHz

# Software Compatibility Information

The following tables list the compatibility information for the Cisco NAE.



Release versions of the Cisco APIC and the Cisco NX-OS software that are not listed in the table below are not supported.

*Table 2. Cisco ACI Fabric Compatibility Information*

<b>Cisco APIC Release</b>	<b>Cisco ACI-Mode NX-OS Switch Software Release for Cisco Nexus 9000 Series ACI-Mode Switches</b>
5.0	15.0
4.2	14.2
4.1	14.1
4.0	14.0
3.2	13.2
3.1	13.1
3.0	13.0
2.3	12.3
2.2	12.2
2.1	12.1
2.0	12.0
1.3	11.3
1.2	11.2

Table 3. Cisco NX-OS Fabric Compatibility Information with DCNM Assurance Group

Cisco DCNM Release	Cisco Nexus 9000 Series NX-OS	Switch Support	Topology and Deployment
11.3.1 11.4.1	9.3(3)	The 9300-EX, -FX, -FX2, and -GX platform switches and the 9500 platform switches with -EX and -FX line cards are supported.	BGP eVPN VXLAN topology and deployments are supported

## Supported Load Balancers

The following table lists the supported load balancers for the Cisco NAE. (Currently, this is supported for ACI Assurance Group only.)

Table 4. Supported Load Balancers

Load Balancer Name	Release
F5 BIG-IP LTM	12.1.3
F5 BIG-IP LTM	14.1.0

# ACI Features Assured by Cisco NAE

The following section lists the ACI features assured by the Cisco NAE.

## Supported Fabric Deployment Options

- Stretched Fabric
- Multipod
- Remote Leaf

## ACI Mode

- Network Mode
- Application Mode

## APIC Policy

- Networking Policy
- Security Policy
- Access Policy

## Tenancy

- Multi Tenant
- Application Profile
- Endpoint Group (EPG)
- Bridge Domain
- Virtual Routing and Forwarding (VRF)
- Contract and Filters
- IPv4 support
- IPv6 support
- Contract and Filters: For contracts, Policy CAM Optimization is supported. Standard contracts with deny action are also supported. Earlier, standard contracts with permit action only were supported. (To get further details, see [Policy CAM Optimization Is Assured.](#))

## EPG

- Application EPG
- External L3Out EPG
- Contract Preferred Group

## **Access Domain Profile**

- Physical
- L3OutP

## **Smart Event Use Cases**

- Policy Analysis
- Tenant End Points
- Tenant Forwarding
- Tenant Security
- Policy CAM Optimization (To get further details, see [Policy CAM Optimization Is Assured.](#))

## **APIC Connectivity to Cisco NAE**

- Out-of-Band Management (OOB)
- In-Band Management
- Network Address Translation (NAT)

## **ACI Features**

- GOLF (Layer 3 EVPN Services for Fabric WAN)

## Policy CAM Optimization Is Assured

Policy CAM Optimization is assured by Cisco NAE.



In Cisco NAE release 4.0(1), for Policy CAM optimization, the **Enable no stats** directive in contract subjects is supported. Policy CAM optimization using the **Enable Policy Compression** directive in contract subjects is not supported. The **Enable no stats** directive is available starting in the Cisco APIC Release 3.2(x) feature set. The **Enable Policy Compression** directive is available in the Cisco APIC Release 4.0(x) feature set.

## ACI Features Not Supported by Cisco NAE

The following ACI features are not supported by the Cisco NAE

- Cisco ACI Multi-Site
- Microsegmentation
- vPOD
- Intra-EPG contracts
- Service Graphs (To get further details, see [Service Graphs Are Not Assured.](#))
- Contract Inheritance

## Service Graphs Are Not Assured

Service graphs are not assured by Cisco NAE. With the introduction of the current Cisco NAE release, spurious smart events will not be raised if an ACI fabric setup fulfills ALL of the following requirements:

- A service graph template must have route redirect enabled.
- Only a single service node is supported, and the service node must be in the GoTo mode Function Type under the Function Node properties.
- If the **threshold-redir** command is used, the threshold down action must be set to **permit**.
- The direct connect option for service graphs is not supported, therefore the value must be set to **False**.
- The set of provider/consumer BDs must not overlap with the set of shadow EPG BDs. Additionally, every shadow EPG must have its own BD.
- The provider EPG and the consumer EPG must be one of the following types: an L3Out InstP, an application EPG, or a vzAny.
- In a transit-routing case with a PBR contract, the provider L3Out and consumer L3Out must be different L3Outs.
- There must be a single service graph per contract, and the service graph must be bi-directional.
- There must be no filters set on function node connectors under the service graph template.
- Only one service graph per contract is supported.
- Subnets on logical interface contexts are not supported.
- Backup PBR policy (introduced in Cisco APIC Release 4.2) is not supported.



Inter-VRF service graph support is a beta feature in this release. **UNSUPPORTED\_SERVICE\_CHAINING\_FEATURE\_DETECTED** will not be raised for the inter-VRF service graph feature.



## **NX-OS Features Assured by Cisco NAE**

The following section lists the NX-OS feature assured by the Cisco NAE.

Only the network BGP EVPN VXLAN topology is supported.

### **Supported Fabric Deployment Options**

Although DCNM can manage multiple sites for Cisco NAE support, only one assurance group maps to one such site.

# NX-OS Features Not Supported by Cisco NAE

The following NX-OS features are not supported by the Cisco NAE

- Currently, when ISIS is the underlay protocol for backup routing between VPC pairs, Cisco NAE will not report any smart event for the neighborship status.
- The following implementations are currently not supported with BGP EVPN topology:
  - FEX on VPC
  - Layer 3 over VPC
  - Super-spine topology
  - Layer 2 backdoor connection between inter-sites
  - Fabric interconnect
  - Breakout interfaces on switches

The following Cisco NAE areas are not supported for NX-OS:

- View Query and How Query in the Explorer Page
- Policy Analysis
- Policy Delta in the Epoch Delta Page
- Policy CAM
- Pre-Change Analysis
- Compliance
- Assured Entities such as Load Balancers and Firewall

# Verified Scalability Limits for ACI Fabric

The following table lists the maximum verified scalability limits for the Cisco NAE .

Table 5. Verified Scalability Limits

Feature	Scale Limit for Appliance Model: Small	Scale Limit for Appliance Model: Medium	Scale Limit for Appliance Model: Large
APIC Fabric Size	50 leaf switches	100 leaf switches	400 leaf switches
Number of VMs	3	3	3
Policy CAM Rules	200 K	400 K	400 K
Endpoints	50 K	100 K	100 K
Number of Prefix Matches	25 K	50 K	50 K
Total number of smart events, endpoints, and prefixes	300 K	500 K	600 K
Number of Concurrent Assurance Analysis	1	1	1
Analysis Interval in ACI Network Mode	15 minutes or more	15 minutes or more	30 minutes or more
Analysis Interval in ACI Application Mode	25 minutes or more	15 minutes or more	Not Supported

Table 6. Verified Scalability Limits for Compliance

Compliance Checks	Scale Limit
Total number of Requirement Sets that can be active at a given time	3
Number of Requirements per Requirement Set	200  Requirements of type Compliance Requirement and Naming Convention  10  Requirements of type Segmentation, Traffic Selector, and SLA

EPG pair limit check per Requirement (includes both directions)	<p>1000</p> <p>The scale limit is applicable if the compliance requirement flag <b>enable_aggregate_event_for_tenant</b> is set to false using Cisco NAE REST APIs.</p> <p>500</p> <p>The scale limit is applicable for the violated EPG pairs if the compliance requirement flag <b>enable_aggregate_event_for_tenant</b> is set to true using Cisco NAE REST APIs.</p> <p>NOTE: In the latter case, only 50 tenants are supported, and the option to enable the aggregate info events will be present only for Segmentation requirements using a tenant object selector. If the option is enabled, there will no longer be any info events for EPG pairs, and only EPG pair-based violation events will be generated.</p>
Fabric wide rules	150 K

Table 7. Verified Scalability Limits for Explorer

Feature	Scale Limit
Total number of associations we can explore	500 K
Fabric wide rules	150 K

## Verified Scalability Limits for NX-OS Fabric

The following tables lists the maximum verified scalability limits.

Table 8. Verified Scalability Limits for Cisco NAE with Cisco NX-OS Fabric

Feature	Cisco NX-OS Fabric Scale Limits
System Routing Template	Default
VXLAN VTEPs	38
VXLAN Layer 2 VNIs	2,000
VXLAN Layer 3 VNIs/VRFs	900
VXLAN Multicast Groups	100
VXLAN Overlay MAC Addresses	64,000
VXLAN Overlay IPv4 Host Routes	60,000

Feature	Cisco NX-OS Fabric Scale Limits
VXLAN Overlay IPv6 Host Routes	16,000
VXLAN Overlay IGMP Snooping Groups	800
VXLAN IPv4 LPM Routes	2,264
VXLAN IPv6 LPM Routes	2,256
VLANs on VTEP Node	2,900 (Total VLANs)
STP Logical Ports	2,900
VPC Port Channels	32
Underlay IS-IS Neighbors	11
Underlay PIM Neighbors	9 (Spine switches), 3 (Leaf switches)

Table 9. Verified Scalability Limits for OVA Deployment

Feature	Scale Limit for Appliance Model: Small	Scale Limit for Appliance Model: Medium
Cisco NX-OS Fabric Size	40 leaf switches	100 leaf switches
Number of VMs	3	3
Number of Prefix Matches (LPM routes)	4,500	4,500
IPv4/IPv6 Host	See the scales in <b>Verified Scalability Limits for Cisco NAE with Cisco NX-OS.</b>	See the scales in <b>Verified Scalability Limits for Cisco NAE with Cisco NX-OS.</b>
Layer 2 MAC Addresses	<b>See table ABOVE</b>	<b>See table ABOVE</b>
Total Number of Smart Events, Endpoints, and Prefixes	16,000	16,000
Number of Concurrent Assurance Analysis	1 concurrent and 4 scheduler serial	1 concurrent and 4 scheduler serial
Analysis Interval	15 minutes or more	15 minutes or more

Table 10. Verified Scalability Limits for Explorer

Feature	Scale Limit
Total number of associations that can be explored	500,000

## Important Notes

- For production analysis, the supported Assurance Group setting for **Analysis Interval** is 15 minutes or more. An interval below 15 minutes should be only used for lab or test purposes.
- Depending on the complexity of the configured policies, in some cases, it has been observed that the run time exceeds 15 minutes, especially for the Cisco NAE small appliance. This issue can be addressed in the following ways:

- Set a polling interval of greater than 15 minutes to provide more time for the computation to finish.
- Deploy a Cisco NAE medium appliance. The run time may come down below 15 minutes as there is more processing power and memory in the medium appliance to finish the analysis sooner.
- On rare occasions, it has been observed that the appliance may not be able to analyze the security policy complexity of the rules on a given switch. As a result, the Cisco NAE will skip the security policy analysis for that particular switch and carry out the rest of the analysis normally. It is important to note the following:
  - The security radial view will show the contracts on the switch for which the analysis could not be run as **Green** to facilitate security contract visualization.
  - The following **System Assurance** event will be generated to indicate that the security analysis of a given switch could not be performed.
    - EVENT: UNABLE\_TO\_PERFORM\_SECURITY\_ANALYSIS\_FOR\_SWITCH
    - CATEGORY : SYSTEM
    - SUBCATEGORY: ASSURANCE\_CONTROL
    - Primary object: Leaf switch on which the security policy analysis could not be performed.
    - Description: The Cisco NAE appliance could not perform tenant security analysis for this particular leaf switch. This happens as the rule complexity grows beyond the bounds of the first generation solver.
- Support for a scale limit of 400 leaf switches for the Large appliance in the ACI network mode is a beta feature in this release.

# Increasing Disk Size

Use this procedure to increase the disk size of the Cisco NAE VM in VMware vSphere.

## Procedure

1. Log in to Cisco NAE.
2. Choose **Settings > Assurance Group Configuration**.
3. Select the Assurance Group and click the stop icon to stop the analysis.
4. Log in to VMware vSphere (or vCenter) Client.
5. Select the Cisco NAE VM.
6. From the **Actions** menu, choose **Power > Shut Down Guest OS** to shut down the VM gracefully.
7. Choose **Edit Settings > Virtual Hardware > Hard Disk 2**.
8. Enter the desired disk size.
9. Click **OK**.
10. Repeat steps 5-9 for all the 3 VMs.
11. From the **Actions** menu, choose **Power > Power On** to power on the VM.
12. Power on all the 3 VMs.
13. To verify, log in to Cisco NAE. Choose **Settings > Appliance Administration**.
14. The disk usage is displayed in the **Assurance Data Controls** tile.



Decreasing the disk size is not supported and may result in complete loss of data and/or the Cisco NAE appliance. As a result, you may have to reinstall the appliance. We recommend that you increase the disk size gradually.

# Installing Cisco Network Assurance Engine

## Prerequisites

- You have installed the Python version 2.7.11 or later to perform offline analysis.
- You have the IP addresses, subnet mask, and gateway information for the Cisco NAE appliance.
- You have the IP addresses of the primary and secondary DNS server.
- You have the IP addresses of the primary and secondary NTP server.
- You have the credentials for the SMTP server.
- Cisco NAE VMs should have unrestricted communication between them, preferably in the same VLAN.
- If the 3 Cisco NAE VMs are being deployed across multiple servers, then the servers must be time synced to the same time source before setting up the Cisco NAE appliance or the installation will fail during database setup. See [Setting Up Cisco NAE Appliance](#).

## Prerequisites for ACI

- Ensure that ports 443 and 22 are open for HTTPS and SSH communication between the Cisco NAE and the APIC.

## Prerequisites for DCNM

- By default, the switches should already be enabled with **feature nxapi** for a LAN fabric that is managed by DCNM. For REST API queries from Cisco NAE to the switches on the LAN fabric to work, all the switches must have **feature nxapi** enabled. Without **feature nxapi** enabled, the REST API query will fail and only a partial analysis of the fabric may occur.
- See [Compatibility Information](#) for more details about what is supported.
- For details related to DCNM setup, see the following URLs:
  - DCNM 11.4.1 setup-
    - [Cisco DCNM Installation and Upgrade for LAN Fabric Deployment](#)
    - [Creating a New VXLAN BGP EVPN Fabric](#)
    - [Managing a Brownfield VXLAN BGP EVPN Fabric](#)
  - DCNM 11.3.1 setup-
    - [Cisco DCNM Installation and Upgrade for LAN Fabric Deployment](#)
    - [Creating a New VXLAN BGP EVPN Fabric](#)
    - [Managing a Brownfield VXLAN BGP EVPN Fabric](#)



## Guidelines and Limitations

Cisco NAE release 4.0(1) introduced the global search feature. In order to support this feature without increasing the VM footprint of the Cisco NAE cluster, Cisco NAE will only function if all three VMs are up and running. This differs from previous releases, where Cisco NAE would continue to function in a degraded mode if a single VM was lost.

In the event of a single VM being lost, you may access the NAE GUI on either of the two remaining VMs.

To view the details about the state of the cluster, navigate to **Settings > Appliance Status > Appliance Installation Status**.

You may be able to recover the single VM that was lost by rebooting that VM. If more assistance is needed in recovering the cluster, contact Cisco TAC.

# Installation and Initial Configuration Workflow

Installation and initial configuration of the Cisco NAE includes the following steps:

1. Installing the Cisco NAE OVA. See [Installing Cisco NAE OVA](#).
2. Setting up the Cisco NAE appliance. See [Setting Up Cisco NAE Appliance](#).
3. Performing analysis on the Assurance Group in online mode or offline mode.
  - a. To perform online analysis, see the *Cisco NAE Getting Started Guide*.
  - b. To perform offline analysis, see the *Cisco NAE Getting Started Guide*.
4. Configure local users or configure authentication domains .
  - a. To configure local users for accessing the Cisco NAE appliance, see the *Cisco NAE Getting Started Guide*.
  - b. To configure authentication domains, see the *Cisco NAE Getting Started Guide*.

## Installing the Cisco NAE OVA

Use this procedure to install the Cisco NAE OVA.

### Before You Begin

- You need administrator privileges to connect to VMware vSphere or vCenter.
- You have the Cisco NAE OVA image. The OVA image set contains a set of OVAs for the different appliance flavors. You will receive the OVA for the appliance flavor based on the license you purchased.
- You have the IP address, subnet mask, and gateway information for the Cisco NAE appliance.

### Procedure

1. Log in to VMware vSphere (or vCenter) Client.
2. In the **Navigation** pane, choose the **Data Center** for deployment.
3. Choose **File > Deploy OVF Template**. The **Deploy OVF Template** window appears.
4. In the **Source** pane, browse to the location, choose the file, and click **Open** to choose your OVF source location.
5. In the **OVF Template Details** pane, verify the details and click **Next**.
6. In the **End User License Agreement** pane, read the license agreement and click **Accept**.
7. In the **Name and Location** pane, do the following:
  - a. (Optional) In the **Name** field, enter the VM name.
  - b. Choose the **Inventory** Location where the Cisco NAE is being deployed and click **Next**.
8. In the **Host/Cluster** pane, choose the required cluster and click **Next**.
9. In the **Storage** pane, choose the location in which to store virtual machine files.

10. In the **Disk Format** pane, enter the data store and the required space for the appliance.
11. In the **Disk Format** pane, click the **Thick Provision** button, and click **Next**.



In a production environment, the supported and required configuration for Virtual Disks is to use Thick Provision. In the Lab environment if you have configured the Cisco NAE appliance using Thin Provision, you must not use the same appliance in the production environment.

12. In the **Properties** pane, provide the following information and click **Next**:
  - IP Address
  - Subnet Mask
  - Gateway
13. In the **Ready to Complete** pane, verify the options selected and click **Finish**.
14. Reserve all of the memory allocated to each virtual machine to avoid performance issues.
15. Edit VM settings to setup disk 1 on a different physical datastore than disk 2.
16. Power on the VM.
17. Cisco NAE virtual appliance is deployed as a cluster of three virtual machines. Repeat the steps to deploy the remaining virtual machines in the cluster.



You must perform the installation on one VM at a time. Do not perform the installation on all 3 VMs simultaneously.

18. After the three virtual machines boots up, copy and paste the Cisco NAE IP address that appears into a supported web browser to access the Cisco NAE Login page.

## Setting Up the Cisco NAE Appliance

The Cisco NAE virtual appliance is deployed as a cluster of three virtual machines. Use this procedure to set up your administrator profile, configure DNS, NTP, and SMTP server, and add virtual machines for fabric configuration.

### Before You Begin

- You have the IP addresses of the virtual machines.
- You have the IP address of the primary and secondary DNS server.
- You have the IP address of the primary and secondary NTP server.
- You have the host name of the SMTP server.

### Procedure

1. Use the Cisco NAE IP address obtained from the procedure [Setting Up Cisco NAE Appliance](#) to access the Cisco NAE Login page.
2. Log in to the Cisco NAE. The **Appliance Setup** form appears.

3. Complete the following fields for **Administrator Profile**.
  - a. Enter the email address.
  - b. Enter the password and enter the password again to confirm.
4. Complete the following fields for **Cluster Configuration**.



You must add at least three virtual machines to the cluster. The IP address of the Virtual Machine 1 is pre-populated. Ensure that each of these VMs are reachable before clicking Submit, and power must remain on during installation.

- a. Click + to add Virtual Machine 2 to the cluster and enter the IP address of the virtual machine.
  - b. Click + to add Virtual Machine 3 to the cluster and enter the IP address of the virtual machine.
5. Complete the following fields for **DNS Server**.

DNS servers are configured for hostname resolution. Cisco NAE validates the reachability of the DNS servers. You must specify at least one DNS server.

- a. Enter the IP address of the primary DNS server.
- b. (Optional) Enter the IP address of the secondary DNS server.

6. Complete the following fields for **NTP Server**.

NTP servers are configured to synchronize time. Cisco NAE validates the reachability of the NTP servers. For configuring remote NTP server, you must specify at least one NTP server.



Cisco NAE uses local NTP service to ensure all the VMs in its cluster have synchronized time. The time source for local NTP service can be an external NTP server or the local VM time of the primary VM in the cluster. We recommend that you use the external NTP server option in a production environment as time source rather than local VM time of primary VM. It is highly recommended that you set time correctly during the installation of the appliance via external NTP server or at the host of the VM used for installation. Setting time back or in future in the appliance VMs or in the host post installation is not supported and can result in unpredictable behavior including but not limited to loss of data in some scenarios. If you need to set time back post installation then the supported method is to re-install the appliance and set time correctly.

- a. Check **Use External NTP Server** check box to configure external NTP server.
  - 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 the local NTP. See [Editing Time Configuration for a Host](#).

7. Complete the following fields for SMTP server.

Cisco NAE appliance leverages email as the mechanism for password recovery. SMTP Server

configuration is required for password recovery.



We strongly recommended that you configure the SMTP server information, since it is required by the admin for password recovery.

- 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.
8. Click **Submit**. The **Summary Configuration** page is displayed. It may take approximately 10 minutes for the **Summary Configuration** to be displayed.
9. Verify the configuration and click **Launch Cisco Network Assurance Engine**.

# Editing Time Configuration for a Host

Use this procedure to edit time configuration for a host in VMware vSphere.

## Procedure

1. Log in to VMware vSphere (or vCenter) Client.
2. Choose **Inventory > Hosts and Clusters**.
3. Select the host to set the date and time.
4. Choose **Configuration > Time Configuration**
5. Choose the **Time** and **Date** from the drop-down list.
6. Click **OK**.
7. Reboot the virtual machines.



Once you edit the time configuration for the host, you cannot set up the NTP server using the Cisco NAE appliance.

# Uploading Certificates

## Uploading A LDAP Certificate

Use this procedure to upload a LDAP certificate.

### Before you begin

- You have obtained the LDAP server certificate.
- You have the permission to access and upload the certificate.
- You have the certificate path and certificate alias.

### Procedure

1. Obtain the LDAP server certificate from your LDAP server administrator.
2. Upload the file (.crt, .cer or .pem) to the server.

```
scp ldapserver.crt admin@VM IP address :/tmp
```



The certificate file must be in PEM format.

3. Log in to a VM in the Cisco NAE appliance as the admin user.
4. Change the file permissions to 755.

Example:

```
chmod 755 /tmp/ldapserver.crt
```

5. Run the command:

```
python /lib/candid/python/InstallLdapCertificate.py.
```

6. Enter the admin password.
7. Enter the certificate path. Certificate path is the location of the LDAP certificate in PEM format.

Example:

```
/tmp/ldapserver.crt
```

8. Enter the certificate alias. Certificate alias name is human readable alpha numeric assigned to the certificate in the application.



Once the certificate is installed, you will receive the message *LDAP certificate installation is successful*.

9. To use the installed certificate, log in to the Cisco NAE appliance using the chrome browser. In the Log in page from the drop-down list, select the authentication domain.

10. (Optional) Run the command `python /lib/candid/python/GetLdapCertificate.py` to check the installed certificates.
11. (Optional) Run the command `python /lib/candid/python/DeleteLdapCertificate.py` to delete installed LDAP certificate. You cannot delete the default certificate.

## Troubleshooting

The following table describes how to troubleshoot installation issues.

Table 11. Error Messages

Error Messages	Solution
Given certificate path <code>/tmp/ldapsrvr.crt</code> is not present	Verify the file path and permission as mentioned step 4.
Given certificate <code>/tmp/ldapsrvr.crt</code> is not in the expected file extensions (.cer, .pem, .crt)	Verify the file extension. The supported file extensions are .cer, .pem, and .crt.
Given certificate <code>tmp/ldapsrvr.crt</code> is not valid	Verify the integrity of certificate.
Provided LDAP certificate already exists	The LDAP certificate is already installed.

## Uploading A Certificate Authority Signed Certificate for the Web Server

Cisco NAE appliance includes default self-signed certificates for the web server.

After installing the Cisco NAE appliance, you can replace the default web server certificate with any Certificate Authority (CA) signed certificate.

### Before you begin

- You have generated the CA signed certificate that you want to upload to the appliance.
- You have the permission to access and upload the certificate.
- For the CA signed web server certificate, the certificate path and certificate key path are available.

### Procedure

Perform the following steps to upload a CA signed web server certificate. Uploading a CA signed web server certificate will replace the default self-signed web server certificate.

1. Choose one of the IP addresses in your NAE cluster and create a DNS entry for that IP address with the desired server name.

For example, if you installed the NAE cluster on IP addresses 10.0.0.7, 10.0.0.8, and 10.0.0.9, you should create the DNS entry to map `cisco-nae.your-domain.com` to 10.0.0.9.

2. Generate a Certificate Signing Request (CSR) with OpenSSL. You must use RSA, and we



recommend a key size of 2048 bits.

Example:

```
openssl req -new -newkey rsa:2048 -nodes -keyout webserver.key -out webserver.csr
```

3. When prompted to enter the common name for the certificate, enter the fully-qualified domain name (FQDN). Ensure that it matches the DNS entry you created in step 1.
4. Order your CA signed web server certificate using the contents of the Certificate Signing Request (.csr) file you just created.



Too access all the VM's with the same certificate, add the hostnames as Subject Alternative Names (SANs) while requesting the certificate.

5. Keep the Private Key (.key) file in a safe location, following your organization's Information Security recommendations.
6. Once you receive your CA signed web server certificate file, upload both the certificate file (.crt, .cer, or .pem) and the private key file (.key) to the server:

```
scp webserver.crt admin@cisco-nae.your-domain.com:/tmp
```

```
scp webserver.key admin@cisco-nae.your-domain.com:/tmp
```



The certificate file must be in PEM or DER format, and the private key file must be in PEM format.

7. Log in to a VM in the Cisco NAE appliance as the admin user.
8. Change the file permissions to 755.

Example:

```
chmod 755 /tmp/webserver.crt chmod 755 /tmp/webserver.key
```

9. Run the command:

```
python /lib/candid/python/InstallWebCertificate.py
```

10. Enter the admin password.
11. Enter the certificate path. Certificate path is the location of the CA signed web server certificate in PEM or DER format.

Example:

```
/tmp/webserver.crt
```

12. Enter the private key path. Private key path is the location of the key for the certificate file in PEM format.

Example:

```
/tmp/webserver.key
```



The private key path must not be protected by a password.



Once the web certificate is installed, you will receive the message *Web Certificate installation is successful. Delete the additional copy of the private key.* You must delete the additional copy of the private key that has 755 permissions.

13. To view the certificate, log in to the Cisco NAE appliance using the Chrome browser.

Click More Tools > Developer Tools > Security > View Certificate to view the certificate.



The certificate will be installed on the VM on which the script is executed. Repeat the procedure to install the certificate on the remaining virtual machines in the Cisco NAE cluster.

## Troubleshooting

The following table describes how to troubleshoot installation issues.

Table 12. Error Messages

Error Messages	Solution
Given certificate path <code>/tmp/webserver.crt</code> is not present	Verify the file path and permission as mentioned in step 8.
Given certificate key path <code>/tmp/webserver.key</code> is not present	Verify the file path and permission as mentioned in step 8.
Given certificate <code>/tmp/webserver.crt</code> is not in the expected file extensions (.cer, .pem, .crt)	Verify the file extension. The supported file extensions are .cer, .pem, and .crt.
Given certificate key <code>/tmp/webserver.key</code> is not in the expected file extensions (.key)	Verify the file extension. The supported file extension is .key.
Given certificate <code>tmp/webserver.crt</code> is not valid	Verify the integrity of certificate.
Given certificate <code>tmp/webserver.key</code> is not valid	Verify the integrity of certificate.
Could not start Apache server with the given certificate/key. Verify the certificate-key pair. Restored old certificates.	Verify if the certificate-key pair is valid.

# Smart Licensing

## Introduction to Smart Licensing

Cisco Smart Licensing is a flexible licensing model that provides you with an easier, faster, and more consistent way to purchase and manage software across the Cisco portfolio and across your organization. And it's secure – you control what users can access. With Smart Licensing you get:

- **Easy Activation:** Smart Licensing establishes a pool of software licenses that can be used across the entire organization—no more PAKs (Product Activation Keys).
- **Unified Management:** My Cisco Entitlements (MCE) provides a complete view into all of your Cisco products and services in an easy-to-use portal, so you always know what you have and what you are using.
- **License Flexibility:** Your software is not node-locked to your hardware, so you can easily use and transfer licenses as needed.

To use Smart Licensing, you must first set up a Smart Account on Cisco Software Central ([software.cisco.com](https://software.cisco.com)).

For a more detailed overview on Cisco Licensing, go to [cisco.com/go/licensingguide](https://cisco.com/go/licensingguide)

## More About Smart Licensing

Smart Licensing is enabled in Cisco NAE.

The following URLs provide you with additional information about Smart Licensing:

- The customer log in URL to access your [CSSM account](#).
- [Cisco Smart Accounts URL](#)

The following URLs are additional resources that you can refer:

- [Training Materials and Resources URL](#)
- [Smart Accounts and Smart Licensing URL](#)

## Smart Licensing Evaluation Period

After you log into Cisco NAE and before you register with CSSM (Cisco Smart Software Manager), Smart Licensing is automatically in the Evaluation Period. The Evaluation Period is global for all the license entitlements. The Evaluation Period lasts 90 days (usage days and not calendar days). Cisco NAE starts to countdown the clock when it receives the report of the first license consumption. After Cisco NAE is registered with CSSM, the Evaluation Period countdown clock stops and Smart Licensing is in the Registered state. If Cisco NAE is unregistered, the countdown clock starts again, and Smart Licensing returns to the Evaluation Period. After 90 days, the Evaluation Period expires and cannot be reset. You will not be able to use Cisco NAE after the evaluation period expires and you are not registered.



If Cisco NAE is unregistered, the Cisco NAE functionality is not affected. In unregistered mode, functionality is stopped after evaluation period ends.

## Smart Licensing Authorization Status

Table 13. Smart Licensing Authorization Status

State	Description
Evaluation	The Evaluation period lasts 90 usage days. Smart Licensing is automatically enabled. Before you register Cisco NAE with CSSM, the Smart Licensing is automatically placed in the Evaluation Period.
Evaluation Expired	The Evaluation Expired status is displayed after 90 days of usage, if you have not registered by then.
Authorization Expired	<p>The Authorization Expired status is displayed if you cannot reach CSSM, for a period of 90 days continuously, due to a network issue. The following are typical examples of why you could see a License Authorization Expired status (there could be other reasons):</p> <ul style="list-style-type: none"><li>• A network issue prevents the renewal of authorization</li><li>• An issue with license compliance</li></ul>
Authorized	<p>In the Authorized state, a license entitlement request is received by CSSM (Cisco Smart Software Manager). CSSM has verified that the reported number of licenses in use do not exceed the total number of licenses purchased for an entitlement. CSSM returns In-Compliance.</p> <p>The authorization is valid for 90 days. Cisco NAE sends the entitlement request every day to renew the authorization.</p>

State	Description
Out of Compliance (OOC)	<p>The license can be in the Out of Compliance state in CSSM for one of the following reasons:</p> <ul style="list-style-type: none"> <li>• The number of licenses in use exceed the total number of licenses purchased for an entitlement.</li> <li>• The purchased licenses are subscription-based and have expired.</li> </ul>

## Smart Licensing Authorization Guidelines

The following guidelines related to smart licensing authorization are implemented currently:

- In **Evaluation** mode, the following banner is displayed on the top of the Cisco NAE GUI to remind you that they have not yet registered Cisco NAE with CSSM: **Smart Licensing is not registered. Evaluation period ends in <number of> days.**
- In **Evaluation Expired** mode, the following red banner displays to remind you that you must register Cisco NAE with CSSM: **Evaluation Period has expired.**
- When an entitlement is in **Out of Compliance** (OOC) state, the following banner is displayed: **Smart Licensing is Out of Compliance.**
- When Cisco NAE loses network connectivity with CSSM, the following messages may display:

License Authorization Status	Description
Authorization Expired	<p>After Cisco NAE is registered with CSSM, Cisco NAE periodically (every day) reports all the licenses consumed to CSSM for authorization even if there are no changes in the licenses consumed. If Cisco NAE loses network connectivity with CSSM, the reporting of licenses consumed may fail. As a result, in the <b>Installed License Details</b> area, the <b>License Authorization Status</b> field displays as <b>Authorization Expired.</b></p>
ID Certificate Expired	<p>If Cisco NAE loses network connectivity with CSSM for a long time, and if after multiple retries, Cisco NAE is unable to automatically renew the ID certificate, the ID certificate (valid for one year) can expire. When the ID certificate expires, the user is automatically placed in the unregistered mode and in the <b>Installed License Details</b> area, the <b>License Authorization Status</b> field displays as <b>Evaluation.</b></p>

# Smart Licensing Usage Guidelines

- Smart Licensing registration steps that follow in this section apply to obtaining a new Cisco NAE.
- Users that upgrade to Cisco NAE, release 4.1(1) from an earlier release will also be in the unregistered and evaluation mode. In order to register, they must contact their Cisco Sales Representative. Their representative will convert their existing licenses to the Smart Licenses and deposit them into CSSM. If they do not have a CSSM account already, a new CSSM account will be created for them.
- If there is a license violation for a feature that is enabled on Cisco NAE, the feature functionality will not be disabled, and there will be no impact on system functionality. The system will continue to operate. The banner on top of the Cisco NAE GUI displays that you are non-compliant.
- To force authorization and entitlement status outside of the automated schedule, you must click the refresh icon that is located at the top of the **Smart License Usage** table in the Cisco NAE GUI. This synchronization can take between 90 and 120 seconds to complete.

## Pre-Registration Verifications

### Verification Checklist for CSSM Configurations

The following is a user checklist for readiness and configurations required with CSSM:

- Verify that you have the appropriate Smart Account and Virtual Accounts created.
- If you have purchased smart-enabled licenses from Cisco Commerce, then verify that your user-purchased licenses are populated.
- As you begin the Cisco NAE Smart Licensing registration, work with your Cisco TAC engineer to ensure that you are ready with the appropriate CSSM items.

### Verification Checklist for Smart Licensing and Cisco NAE Configurations

Your DNS settings must be configured in Cisco NAE to resolve to <https://software.cisco.com>

## Initial Cisco NAE Login and Smart Licensing Pre-Registration

With Cisco NAE release 4.1(1), when you first log in to the GUI, the display in the top banner of the GUI landing page displays the following message: **Smart License is not registered. Evaluation period ends in <number of> day(s)**. This indicates that Smart Licensing is not configured with CSSM.

There is a hyperlink in the banner, **View License Details**, that takes you directly to the Smart Licensing GUI location. You can also manually navigate to the Smart Licensing GUI area as follows: **Settings > License**.

In the Smart Licensing GUI screen, the **Install License Details** area is displayed where you can choose the appropriate method to register that suits your environment.

To register, there are different methods to connect to CSSM that are described in the following sections.

## Transport Setting

The following different methods of Transport Setting network connectivity with CSSM are available:

Transport Setting	Description
Direct connect to Cisco Smart Software Manager (CSSM)	Choose this setting if your Cisco NAE has access to the internet and it can directly connect with CSSM.
Transport Gateway/Smart Software Manager Satellite	Choose this setting if Cisco NAE cannot directly connect with CSSM using the internet. You must install a physical transport gateway or a smart software manager satellite. You must use Smart Software Manager Satellite Enhanced Edition 6.0.0 or a higher version. You can download the software at the following URL: <a href="https://www.cisco.com/c/en/us/buy/smart-accounts/software-manager-satellite.html">https://www.cisco.com/c/en/us/buy/smart-accounts/software-manager-satellite.html</a>
HTTP/HTTPS Proxy	Choose this setting if you already have an existing third-party web server (Apache) forward proxy to enable access to CSSM.

## Registering for Smart Licensing With Direct Connect to CSSM

Register Cisco NAE with Cisco Smart Software Manager (CSSM)

### Before You Begin

- To register for Smart Licensing using this method, Cisco NAE must have Internet access available.
- Your CSSM Smart Software Licensing account must be created and available.

### Procedure

1. Login to your [CSSM Smart Software Licensing account](#).
2. In the **Smart Licensing** pane, in the **Product Instance Registration Tokens** area, click the **New Token** button to create a token.
3. In the **Create Registration Token** dialog box, your account information is displayed.

4. In the **Description** field, enter a description for your token.
5. In the **Expire After** field, enter the number of days after which the token will expire. Cisco recommends a value of 30 days. The value can be between 1 and 365.
6. Click **Create Token** to generate a new token for your account.
7. Click inside the new token row, which is displayed in the **Product Instance Registration Tokens** area, and copy the content.
8. Next, login to the Cisco NAE GUI.
9. Navigate to **Settings** (⚙️) and click License. In the **Installed License Details** area, the **Registration State** displays as **Unregistered**, and **License Authorization Status** displays **Evaluation**.
10. In the **Transport Setting** field, **Direct** is chosen by default. This value is the direct connect to CSSM.



**Reregister product if already registered** field must only be checked if you are already registered and you want to reregister.

11. In the **Register Smart License** dialog box, paste the token value that was copied from CSSM, and click the **Register** button. Wait until the **Registration State** field displays **Registered**.

The **Installed License Details** area changes the **Authorization Status** field from **Evaluation** to **Authorized**.

This completes the registration.

## Registering for Smart Licensing With Transport Gateway/Cisco Smart Software Manager On-Prem

Register Cisco NAE with Cisco Smart Software Manager (CSSM)

### Before You Begin

- To register for Smart Licensing using this method, Cisco NAE must have Cisco Transport Gateway installed with the software as a physical or virtual machine.
- Your CSSM Smart Software Licensing account must be created and available.
- If using HTTPS to communicate with your on-prem Transport Gateway/Cisco Smart Manager, see [Using HTTPS for Transport Gateway/Cisco Smart Manager On-Prem](#).

### Procedure

1. Go to your [CSSM Smart Software Licensing account](#), and perform the following actions:
  - a. In the **Smart Licensing** pane, in the **Product Instance Registration Tokens** area, click the **New Token** button to create a token.
  - b. In the **Create Registration Token** dialog box, your account information is displayed.



- c. In the **Description** field, enter a description for your token.
  - d. In the **Expire After** field, enter the number of days after which the token will expire. Cisco recommends a value of 30 days. The value can be between 1 and 365.
  - e. Click **Create Token** to generate a new token for your account.
  - f. Click inside the new token row, which is displayed in the **Product Instance Registration Tokens** area, and copy the content.
2. Next, login to the Cisco NAE GUI.
  3. Navigate to **Settings** (⚙️), and click **License**. In the **Installed License Details** area, the Registration State displays as **Unregistered**, and **License Authorization Status** displays **Evaluation**.
  4. In the **Transport Setting** field, click **Edit/View**.
  5. In the **Transport Settings** dialog box, choose the **Transport Gateway/Cisco Smart Software Manager On-Prem** radio button.
  6. In the **URL** field, enter the appropriate URL that matches your Transport Setting selection. Click **Apply**.



The URL field, contains the URL to communicate with the Transport Gateway by default. You must include the port number on the Transport Gateway.

7. In the **Install License Details** area, click the **Register** button.
8. In the **Register Smart License** dialog box, in the **Registration Token** field, paste the copied registration token from your Smart Account, and click **Register**.



**Reregister product if already registered** field must only be checked if you are already registered and you want to reregister.

In the **License Details** area, wait until the **Registration State** field displays **Registered**. The **Authorization Status** field changes from **Evaluation** to **Authorized**.

This completes the registration.

## Using HTTPS for Transport Gateway/Cisco Smart Manager On-Prem

To configure the on-prem Cisco Smart Software Manager (CSSM) to communicate securely over HTTPS you must include the Cisco Licensing Root CA in the default JVM certificate authority trust store.

If the Cisco Licensing Root CA is not included in the default JVM certificate authority trust store, the smart licensing registration will fail with the following error message:

```
sun.security.validator.ValidatorException: PKIX path building failed:
sun.security.provider.certpath.SunCertPathBuilderException: unable to find valid
certification path to requested target
```

Contact your Cisco TAC representative so they can help you include the Cisco Licensing Root CA by using a script, **import-licensing-rootca.sh**, that will apply the required patch. Details are provided in the following Cisco TechZone article that Cisco TAC can access:

<https://techzone.cisco.com/t5/Candid-Knowledge-Base/CNAE-4-1-1-Smart-Licensing-Transport-Gateway-Invalid-Response/ta-p/1469313>

After you apply the patch, perform the following steps to configure SSL to communicate with CSSM On-Prem.

1. Log in to the Cisco NAE GUI.
2. Choose **Settings > License**.
3. In the **Transport Setting** field, click **Edit/View**.
4. In the **Transport Settings** dialog box, choose the **Transport Gateway/Cisco Smart Software Manager On-Prem** radio button.
5. In the **URL** field, enter the correct HTTPS URL to your CSSM On-Prem host. For example, <https://{valid-hostname}/SmartTransport> where {valid-hostname} is the Smart Licensing Satellite/On-Prem Server's common name.
6. Click **Apply**.

## Registering for Smart Licensing With HTTP or HTTPS Proxy

You can use this method to register for Smart Licensing by using a normal HTTP proxy server to relay messages to CSSM. This method works if you do not have internet or you do not have connectivity to <http://www.cisco.com> from Cisco NAE. In addition, there is also no transport gateway or satellite manager availability installed in your premises to allow the proxy to request CSSM.

If you register using this method, the Apache server has been tested and is recommended for use. You will be required to provide the IP address of the Apache server.

### Procedure

1. Go to your [CSSM Smart Software Licensing account](#), and perform the following actions:
  - a. In the **Smart Licensing** pane, in the **Product Instance Registration Tokens** area, click the **New Token** button to create a token.
  - b. In the **Create Registration Token** dialog box, your account information is displayed.
  - c. In the **Description** field, enter a description for your token.

- d. In the **Expire After** field, enter the number of days after which the token will expire. Cisco recommends a value of 30 days. The value can be between 1 and 365.
  - e. Click **Create Token** to generate a new token for your account.
  - f. Click inside the new token row, which is displayed in the **Product Instance Registration Tokens** area, and copy the content.
2. Next, login to the Cisco NAE GUI.
  3. Navigate to **Settings** (⚙️), and click **License**. In the **Installed License Details** area, the **Registration State** displays as **Unregistered**, and **License Authorization Status** displays **Evaluation**.
  4. In the **Transport Setting** field, choose the **HTTP or HTTPS Proxy** registration method. The following note is displayed: **Smart Licensing data will be via an intermediate HTTP or HTTPS proxy**.
  5. In the **URL** field, enter the appropriate URL.
  6. In the **Port** field, enter the port number that will be used.
  7. Click **Apply**.
  8. In the **Installed License Details** area in the Cisco NAE GUI, click the **Register** button.
  9. In the **Registration Token** field, paste the copied registration token from your Smart Account.



**Register product if already registered** field must only be checked if you are already registered and you want to reregister.

10. Click **Register**.

In the **License Details** area, wait until the **Registration State** field displays **Registered**. The **Authorization Status** field changes from **Evaluation** to **Authorized**.

This completes the registration.

## Deregister

The **Deregister** button is displayed in the **Installed License Details** area after you are registered. When you click the **Deregister** button, it releases the product and release all the entitlements currently used by the product. The entitlements are released on CSSM. On the Cisco NAE, the entitlements return to the Evaluation period.

## Renew Authorization

Cisco NAE synchronizes the license authorization status from CSSM once every day.

When a license usage is changed (consumed or released) and you wish to see the changes immediately, you can manually renew the authorization status from CSSM by clicking the refresh icon that is located at the top of the **Smart License Usage** table.

# Renew Registration

The **Renew Registration** button is displayed in the **Installed License Details** area after you are registered. It is recommended that you renew your registration every six months. To manually renew the registration, click the **Renew Registration** button. The renewal validates the ID and certificates that were exchanged during registration and your renewal is successful.



The Smart Agent attempts to automatically renew the registration every six months. If there is a connection loss, the automatic registration might fail, so the **Renew Registration** button allows you to manually renew the registration.

## Reregister Product If Already Registered

If you encounter an instance when Cisco NAE has not deregistered successfully and it fails, the backend will still be associated with the instance ID. In such cases, to register the device again you must use a force option which is to reregister.

If you have already registered Smart Licensing with your Cisco NAE earlier, you can reregister the Smart License during the subsequent times you use Cisco NAE. This prevents your registration from failing.

To reregister Cisco NAE, check the check box for the **Reregister product if already registered** dialog box in the Cisco NAE GUI by navigating to the **Settings > License** area. Click **Register**.

## Troubleshooting Cisco NAE Licensing

### Smart Licensing Cisco NAE Registration Failed

Your registration fails upon registering Cisco NAE with the following message displayed in the **Licenses** area as a banner: **Invalid response from licensing cloud**.

To troubleshoot such a registration failure, verify the following items:

- Verify that your DNS server is configured to resolve to `www.software.cisco.com`. Perform a DNS lookup from Cisco NAE to verify this configuration.
- Verify that you used the correct port numbers when you configured the Transport Gateway, the Smart Software Manager Satellite, or the HTTP/HTTPS proxy mode.
- If you are using HTTPS Proxy mode, the issue could be due to a certificate mismatch. Verify that your certificate is the correct one.
- If you are using the Smart Software Manager Satellite mode, and you have generated an SSL certificate by providing a hostname, you must use the same hostname instead of the IP address while configuring the Smart Software Satellite mode in Cisco NAE. Similarly, if you have generated an SSL certificate by providing an IP address, you must use the same IP address instead of the hostname while configuring the Smart Software Satellite mode in Cisco NAE.

## Smart Licensing Registration with Smart Software Manager Satellite has Failed

You must use a private certificate when you use Smart Software Manager Satellite as your Transport Setting. If you choose Cisco Smart Software Manager Satellite as your Transport Setting and use the HTTPS protocol, you must first download a certificate from the Cisco web site. Then, you must import the certificate into the Cisco NAE before registering the Cisco NAE. Otherwise, the registration will fail. Only Cisco Smart Software Manager Satellite (using HTTPS protocol) requires an import certificate. Other Transport Settings, such as Cisco Transport Gateway (HTTPS) and third-party Apache proxy server (HTTPS) do not require you to have an import certificate.

### Registration Failed Due to an Expired Token

Your registration failed due to an expired token. To troubleshoot such a registration failure issue, verify the following items:

The error message is self-explanatory and can be viewed under **Settings > License**. If registering with the Smart Software Manager Satellite server, use the token from the satellite manager to register. Do not use the token from CSSM.

### Out of Compliance Message Upon Registration

If you see an **Out of Compliance** message in Cisco NAE upon registering, check the following items:

- In the Cisco NAE, navigate to **Settings > License > Smart License Usage**, and double-click the item that is displayed as **Out of Compliance**. The dialog box that opens will provide details about the features consumed by the Cisco NAE. Verify whether you have adequate licenses of the required type in your smart account.
- When using the Smart Software Manager Satellite server, verify that the licenses in your smart account and in the Satellite server account are synchronized. If they are not synchronized, perform a manual or a network synchronization between the smart account and Smart Software Manager Satellite server.

The license may also remain in the **Out of Compliance** state in CSSM for one of the following reasons:

- The purchased licenses are subscription-based and have expired.
- The number of licenses in use exceed the total number of licenses purchased for an entitlement. Even if the count is fixed to match the number of licenses, the **Out of Compliance** state can remain for up to 24 hours, until the system is refreshed.

### License Authorization Expired

When this fault occurs, first check if there is any network connectivity issue between the Cisco NAE and CSSM. After fixing the network connectivity issue, log in to the Cisco NAE GUI, and click the refresh icon that is located at the top of the **Smart License Usage** table. This action manually renews the authorization status from CSSM.

# Upgrading and Downgrading Cisco Network Assurance Engine

## Supported Upgrade Paths for Cisco NAE

The following table lists the supported upgrade paths for the Cisco NAE.

Table 14. Supported Upgrade Paths for Cisco NAE

From	To
4.1(2)	5.0(1)
4.1(1)	4.1(2)
4.0(1b)	4.1(2)
3.1(1)	4.0(1b)
3.0(1a)	3.1(1)
2.1(1b)	3.0(1a)
2.0(1b)	2.1(1b)

### Important Notes



Before starting the upgrade process you must create snapshots of the VM. See [Creating VM Snapshots](#)

- During the upgrade process, ensure that the connectivity to the Cisco NAE is not disrupted and the power to any of the Cisco NAE VMs is not disconnected. Failure to comply can lead to the appliance being in an unusable state.
- Unusually high datastore read/write latency could lead to upgrade failures.
- During the upgrade process, ensure that all the VMs are up and running. Partial upgrades of the VMs is not supported.
- Upgrading from release 2.0(1b) to release 3.0(1a) is a two step process.
  1. Upload the bundle for release 2.1(1b) and upgrade to release 2.1(1b).
  2. Upload the bundle for 3.0(1a) and upgrade to release 3.0(1).



Do not upload the 2.1(1b) and 3.0(1a) bundles simultaneously.

- When you upgrade from Cisco NAE release 2.0(1) or 2.1(1) to release 4.0(1), the epochs from the releases 2.0(1) and 2.1(1) will not be visible in the GUI . To access the epochs from the releases 2.0(1) and 2.1(1), contact your Cisco account team before the upgrade.
- Prior to upgrading to Cisco NAE release 4.0(1), you must delete all the unnecessary offline analysis files using the **Offline File Management** page in the NAE GUI. See the section *Managing Offline Analysis* in the *Cisco NAE Getting Started Guide* for more information.

- If a large number of offline analysis files (100 or more) were uploaded to the previous releases of NAE, then after upgrading to NAE release 4.0(1), there may be a lag of up to two hours before the uploaded files from the previous releases are available for analysis. This lag does not impact the offline analysis files that are uploaded to NAE release 4.0(1).
- To address the issue in [CSCvo182291](#), Cisco has released the Security Advisory, [Cisco Network Assurance Engine CLI Access with Default Password Vulnerability](#). The default password vulnerability affects Cisco NAE Release 3.0(1) and is fixed in Cisco NAE Release 3.0(1a). To upgrade to Cisco NAE Release 3.1(1), you must first upgrade to Cisco NAE Release 3.0(1a). After upgrading from Cisco NAE Release 3.0(1) to Cisco NAE Release 3.0(1a), you must change the administrator password using the GUI to fix the vulnerability.

## Upgrading Cisco NAE OVA

Use this procedure to upgrade the Cisco NAE OVA.

### Before You Begin

- You have downloaded the Cisco NAE bundle file.
- All the VMs must be active at the time of the upgrade process.
- You have created snapshots of the VM. See [Creating VM Snapshots](#)

### Procedure

1. Download the Cisco Network Assurance Engine Virtual Appliance upgrade bundle from [Cisco.com](#).
2. Unzip the file. When you unzip the file, the following 2 files are displayed
  - *nae\_ova-release number.bundle*
  - *nae\_ova-release number.bundle.md5sum*



You must upload the *nae\_ova-release number.bundle* file to the Cisco NAE appliance.

3. Choose **Settings > Appliance Administration**.
4. Click the details icon on the **Software Management** tile.
5. Click **Upload Bundle File** to upload the bundle file (*nae\_ova-release number.bundle*) targeted for upgrade.
6. In the **Upload Bundle File** form, complete the following fields.
  - a. Click **Browse** to upload the bundle file.
  - b. Select the **Upload Bundle File**.
  - c. Click **Add**. After the file has been uploaded successfully, it is displayed in the Upload table.
7. In the Upload table, select the bundle file.
8. From the **Actions** menu, choose **Install**. The **Software Management** form displays the status of

the software upgrade for each individual virtual machine in the Cisco NAE appliance cluster. After the upgrade has been completed successfully, the Cisco NAE login page appears. Choose **Install** only from one VM to upgrade the entire Cisco NAE cluster.

9. Enter your credentials to access the Cisco NAE GUI.



You must perform the online analysis on any Assurance Group only after the upgrade has been completed successfully.

## Troubleshooting Upgrade Failure

Contact Cisco TAC immediately for any issues related to the upgrade process. If you encounter any issues related to the upgrade process, leave the system in the original failed state and contact Cisco TAC.

See the *Cisco NAE Getting Started Guide* for information on downloading tech support logs.

## Creating VM Snapshots

Use this procedure to create VM snapshots.

### Procedure

1. Stop all online analysis.
  - a. Choose **Settings > Assurance Configuration**.
  - b. Select the Assurance Group and click the **Stop** icon.
2. Log in to VMware vCenter or vSphere Client and shut down all the VMs of the Cisco NAE appliance.



Use the normal shutdown procedure using **Shutdown Guest OS** to shut down the VMs. Do not use the **Power Off** option.

3. In the vCenter or vSphere Client, create a new snapshot of each VM of the Cisco NAE appliance.
4. Power on all the VMs of the Cisco NAE appliance. You must power on all the VMs only once all the snapshots have been successfully completed.



# Downgrading Cisco NAE

## Important Notes

- You cannot downgrade from within the Cisco NAE appliance.
- After you upgrade to the release 4.1(x), 4.0(1), 3.1(1), 3.0(1a) or 2.1(1b), you cannot downgrade back to the release 4.0(1), 3.1(1), 3.0(1a), 2.1(1b) or 2.0(1b) build from which the upgrade was performed.
  - If downgrade capability is desired, you **must** take a VM snapshot before performing the upgrade. See [Creating VM Snapshots](#).
  - Any configuration, as well as epochs and smart events generated after upgrading will be lost after a downgrade.
  - Before choosing to restore the cluster from the VM snapshot, contact Cisco TAC to see if any problem can be resolved without needing to take this action.
- The VM snapshot will continue to grow in size and consume disk space if it is kept for a long period of time. Ensure that you eventually delete the VM snapshot.

# Migrating Cisco Network Assurance Engine Appliance

## Migrating Cisco NAE Appliance

There are three models currently shipping with Cisco NAE: Small, Medium, and Large. Use this procedure to migrate the Cisco NAE appliance model.

The supported migration paths include:

- Migration from small to medium appliance model
- Migration from medium to large appliance model

### Procedure

1. Log in to the Cisco NAE appliance as root.
2. Log in to VMware vSphere Web Client (Flash) and power off all the VMs of the Cisco NAE appliance.



Use the **Power Off** option. Do not use the **Shutdown Guest OS** to shut down the VMs.

4. Select the VM and choose **Edit Settings > Virtual Hardware**.
5. Update the **CPU**, **Memory**, and **Hard Disk** from the drop-down list based on the migration path. Use the **CPU**, **Memory**, and **Hard Disk** values listed in the table below.

Migration Path	CPU	Memory	Disk
Migrating from small to medium appliance model	12	64 GB	2 TB
Migrating from medium to large appliance model	24	96 GB	4 TB

6. Choose **Edit Settings > vApp Options > Properties > OVA Flavor**.
7. In the **Edit Properties** window, enter the model name in the **Default Type** field. The model name is case sensitive. Use the **Default Type** value listed in the table below.

Migration Path	Model Name
Migrating from small to medium appliance model	medium
Migrating from medium to large appliance model	large

8. Click **Ok**.
9. Power on all the VMs.
10. To verify, perform the following steps:
  - a. Log in to the VMs using Secure Shell (SSH) as an admin.
  - b. Verify if the model is updated in the `cat/etc/candid/version.properties` file.
  - c. Log in to the Cisco NAE GUI. Choose **Settings** > **About Network Assurance Engine** to view the appliance model.