



# Cisco Network Assurance Engine Release Notes, Release 5.1(1)

# Table of Contents

|  |    |
|--|----|
| Introduction .....                                 | 3  |
| New Software Features .....                        | 4  |
| Open Issues .....                                  | 6  |
| Resolved Issues .....                              | 8  |
| Known Issues .....                                 | 9  |
| Software Compatibility Information .....           | 10 |
| Hardware Compatibility Information .....           | 12 |
| Verified Scalability Limits for ACI Fabric .....   | 13 |
| Verified Scalability Limits for NX-OS Fabric ..... | 15 |
| Licensing Information .....                        | 17 |
| Cisco NAE App Compatibility Information .....      | 18 |
| Software Compatibility Information .....           | 19 |
| Verified Scalability .....                         | 20 |
| Usage Guidelines .....                             | 21 |
| Related Content .....                              | 22 |
| Legal Information .....                            | 23 |

First Published: 2020-11-18

Last Modified: 2022-01-20

**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)

© 2017-2022 Cisco Systems, Inc. All rights reserved.

# Introduction

This document describes the features, caveats, and limitations for the Cisco Network Assurance Engine (NAE).

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

See [Related Content](#) for information regarding additional product documentation.



The documentation set for this product strives to use bias-free language. For the purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

| Date              | Description   |
|-------------------|---|
| January 20, 2022  | Release 5.1(1c) patch became available.                                 |
| May 21, 2021      | Added CSCvx61734 to Open Issues.  |
| April 27, 2021    | Release 5.1(1b) patch for Cisco NAE app and appliance became available. |
| December 22, 2020 | Release 5.1(1a) for Cisco NAE app became available.                     |
| November 13, 2020 | Release 5.1(1) for Cisco NAE appliance became available.                |

# New Software Features

## New Software Features in Release 5.1(1)

| Feature  | Description  |
|--|--|
| Cisco NAE app support on Cisco Nexus Dashboard               | Cisco NAE app can be deployed as a service on Cisco Nexus Dashboard.   |
| MSO Assurance Group support                                  | An MSO Assurance Group is supported by Cisco NAE. Cisco NAE queries the sites that Cisco MSO manages and controls the configurations.  |
| NX-OS Fabric Assurance enhancements                          | <ul style="list-style-type: none"><li>• For NX-OS fabric assurance, Layer 2 VNI and Layer 3 VNI are added as resources.</li><li>• Resource aggregations are supported for VLAN and VRF resources for What query results.</li><li>• BETA feature: The Policy Delta feature for DCNM Assurance Group analyzes the changed nodes or switches across two epochs and obtains a co-related view of what has changed in the NX-OS switches.</li></ul> |
| Policy-Based Redirect Service Graph Assurance                | Service Graphs are assured when certain specified conditions are met.  |
| Multi-Tier fabric topology support for ACI                   | Starting from Cisco NAE release 5.1(1), multi-tier fabric topology for ACI is supported.   |
| Pre-Change Analysis enhancements                             | Additional Fabric Access Policy filters are now available for pre-change analysis jobs.  |
| BD to EPG Relationship Configuration Compliance              | You can create a BD configuration compliance rule to set the maximum number of EPGs with which the BD can be associated.   |
| Smart Event details using a URL                              | You can view Smart Event details using a URL.  |
| Naming Rules Compliance for Additional Object Selector Types | Contract, Filter, and Subject selectors are additional Object Selector types that are compliant with Naming rules.   |
| Configuration Compliance Containment Equality Check          | For Configuration Compliance Containment Check, the <b>Allow addition of new configuration objects</b> field enables you to choose whether to raise a violation event for a new object that is added or deleted in Cisco APIC.   |
| Customized Next Step   | When creating a new Event Rule, a <b>Customize Next Step Message</b> field is available to enter the suggested next steps for a user.  |

| Feature                | Description   |
|------------------------|---|
| Cisco APIC 5.1 support | Cisco APIC Release 5.1 is supported by Cisco NAE Release 5.1(1).  |
| New Smart Events       | <p>The following smart events are introduced in this release:</p> <ul style="list-style-type: none"> <li>• MSO Fabric Events</li> <li>• Policy-Based Redirect Assurance Events</li> <li>• NX-OS EVPN and Endpoint Events</li> </ul> |
| New API commands       | <p>The following API commands are added:</p> <ul style="list-style-type: none"> <li>• Read the life cycle state of a Smart Event.</li> <li>• Manage fabrics of type NX-OS and MSO in addition to ACI.</li> </ul>                    |

# Open Issues

Click the bug ID to access the Bug Search tool and see additional information about the bug. The "Exists In" column of the table specifies the releases in which the bug exists. A bug might also exist in other releases.

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

| Bug ID                     | Description  | Exists in |
|----------------------------|--|-----------|
| <a href="#">CSCvu21980</a> | Cisco NAE does not detect overlapping external subnet with BD subnet.  | 5.1(1)    |
| <a href="#">CSCvu67993</a> | In some cases, the smart event <code>VPC_DOMAIN_INCONSISTENT</code> displays configuration status as <b>Invalid</b> . Check the smart event <code>VPC_PARAMETERS_INCONSISTENT</code> for more information. | 5.1(1)    |
| <a href="#">CSCvu60329</a> | Using the API <code>allow_unsupported_object_modification_is_true</code> for a PCA job, may result in false positive or negative smart events.   | 5.1(1)    |
| <a href="#">CSCvu81037</a> | Cisco NAE raises the incorrect warning level smart events on port channels (PC) and virtual port channels (vPC) that are used for L3Out under certain conditions.  | 5.1(1)    |
| <a href="#">CSCvu32911</a> | When there is a vPC type-2 mismatch in Interface-VLAN routing and Output Queuing parameters, Cisco NAE does not generate <code>VPC_DOMAIN_INCONSISTENT</code> smart event.                                 | 5.1(1)    |
| <a href="#">CSCvu77756</a> | When there is a mismatch in vPC Output-Queuing type-2 parameter, Cisco NAE does not generate <code>VPC_PARAMETERS_INCONSISTENT</code> smart event.   | 5.1(1)    |
| <a href="#">CSCvv11505</a> | When you perform a search by pasting the value in the search field, the value is pasted twice.   | 5.1(1)    |
| <a href="#">CSCvv11593</a> | Smart event <code>INRA_PARTIAL_FAILURE</code> for endpoint is generated intermittently due to certain query failure.   | 5.1(1)    |
| <a href="#">CSCvw16617</a> | After the compliance requirement configuration is imported, the download button does not work.   | 5.1(1)    |
| <a href="#">CSCvw18650</a> | In some cases, the Explorer incorrectly displays that 2 EPGs can not talk in the reverse direction when they can talk.   | 5.1(1)    |
| <a href="#">CSCvw30230</a> | Collection time on NX-OS fabrics will take longer on Cisco NAE app on Cisco Nexus Dashboard as compared to the Cisco NAE appliance (OVA).  | 5.1(1)    |
| <a href="#">CSCvw28319</a> | Security Flow table for inter tenant configurations across sites may display incorrect entries.  | 5.1(1)    |



| Bug ID                     | Description   | Exists in |
|----------------------------|---|-----------|
| <a href="#">CSCvv73587</a> | False positives are generated for smart event <code>CONNECTED_EP_LEARNING_ERROR</code> with endpoint learning across sites.         | 5.1(1)    |
| <a href="#">CSCvw64163</a> | Cisco NAE app uninstall operation is stuck and does not proceed if the Cisco Nexus Dashboard cluster has a ND node down.            | 5.1(1)    |
| <a href="#">CSCvx79646</a> | Unable to start Directed Acyclic Graph (DAG) after you upgrade from Cisco NAE app release 5.1(1a) to Cisco NAE app release 5.1(1b). | 5.1(1)    |
| <a href="#">CSCvx61734</a> | <code>UNSUPPORTED_SOFTWARE_VERSION_ON_DCNM</code> event is generated on epoch runs though it is supported.                          | 5.1(1)    |

# Resolved Issues

Click the bug ID to access the Bug Search Tool and see additional information about the bug. The "Fixed In" column of the table specifies whether the bug was resolved in the base release or a patch release. Click the bug ID to access the Bug Search tool and see additional information about the bug.

| Bug ID                     | Description   | Fixed In |
|----------------------------|---|----------|
| <a href="#">CSCvv08622</a> | If you apply the severity filter on the search field and access the Event page from the prefix table, the event table does not display any results.                                 | 5.1(1)   |
| <a href="#">CSCvv09871</a> | Performing a search for subnet or route in Global Search or Event Suppression page does not display the results in the events table. The results are displayed in the prefix table. | 5.1(1)   |
| <a href="#">CSCvv08248</a> | Download option for PCA jobs with tenant configuration size exceeding 8KB is disabled.  | 5.1(1)   |
| <a href="#">CSCvx29695</a> | Creating a compliance requirement when you import Cisco APIC 5.1.2e configuration results in an error.  | 5.1(1b)  |
| <a href="#">CSCwa47285</a> | Evaluation of Cisco NAE for Log4j RCE (Log4Shell) vulnerability.  | 5.1(1c)  |

# Known Issues

Click the Bug ID to access the Bug Search Tool and see additional information about the bug. The "Exists In" column of the table specifies the releases in which the known behavior exists. A bug might also exist in releases.

| Bug ID                     | Description   | Exists In        |
|----------------------------|---|------------------|
| <a href="#">CSCvi51374</a> | For scale configurations, a few API queries (notably the prefix, Policy CAM, or endpoint table) can result in an HTTP error code 500 due to a high load on the DB/backend.            | 5.1(1) and later |
| <a href="#">CSCvk36185</a> | Renaming or replacing a filter entry does not show change in epoch health delta.  | 5.1(1) and later |
| <a href="#">CSCvo42680</a> | LOG_PERMIT_POLICY_ENFORCED smart event is generated for the actrlRule that has threshold, redir action.   | 5.1(1) and later |
| <a href="#">CSCvq70757</a> | For an object with the same key for either <b>Event Table</b> , <b>Endpoint Table</b> or <b>Prefix Table</b> , the search display may show multiple rows depending on the time range. | 5.1(1) and later |
| <a href="#">CSCvv73587</a> | <b>CONNECTED_EP_LEARNING_ERROR</b> smart event is displayed for end points that belong to different site in MSO use case.   | 5.1(1) and later |

## Important Notes

- Epochs from MSO fabrics cannot be imported or exported. MSO epochs are included in the total epochs count from the **Historical Time Range** area in the **Schedule Import/Export Historical Data** screen, but Cisco NAE will not export the MSO epoch. If inline exports are enabled, it will not apply to epochs generated from an MSO assurance group. As an example, if there are 2 ACI fabrics and 1 MSO fabric, then 6 ACI epochs would be exported, and 3 MSO epochs are expected to fail to export. The historical export job as a whole will be displayed as a failure in the **Export History** area. The user can obtain more information about why the job was marked as a failure by clicking **Action** > **Download Failed Epoch Log**. A line similar to the following will be displayed for each MSO epoch in that time range:

```
2020-10-31 02:05:12.048' ERROR Failed to export epoch 2c0fc24b-2060b3fd-ad31-3274-8785-90caa15803b6 from fabric 2c0fc24b-02cf179e-0761-43ce-a4f8-59793e6b3d33 collected at 1604109696000: Epochs from MSO fabrics cannot be imported or exported.'
```

- In case of multiple APICs (sites) managed by MSO, Cisco NAE may falsely report **CONNECTED\_EP\_LEARNING\_ERROR** or **FABRIC\_EP\_LEARNING\_ERROR** in APIC epochs for endpoints that belong to different APIC (site). These events can be suppressed using event suppression rules.
- Under heavy, highly parallelized search query workloads, global search may require the installation of the next higher NAE model for additional memory. For example, a 40 leaf node fabric that can normally be analyzed with NAE-V500-S might require installation of NAE-V1000-M to support heavy, highly parallelized global search usage.

# Software Compatibility Information

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

## Cisco ACI Fabric Compatibility Information



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

Table 1. Cisco ACI Fabric Compatibility Information

| Cisco APIC Release | Cisco ACI-Mode NX-OS Switch Software Release for Cisco Nexus 9000 Series ACI-Mode Switches |
|--------------------|--|
| 5.1                | 15.1   |
| 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   |

## 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 2. Supported Load Balancers

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

# Cisco NAE support for MSO Compatibility Information

*Cisco NAE support for MSO Compatibility Information*

Cisco NAE release 5.1.1 supports MSO release 3.x.

For details about MSO and ACI support, see **Multi-Site Orchestrator and Cisco APIC Interoperability Support** in [Cisco ACI Multi-Site Orchestrator Installation and Upgrade Guide, Release 3.x](#).

## Cisco NX-OS Fabric Compatibility Information with DCNM Assurance Group

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

| <b>Cisco DCNM Release</b>   | <b>Cisco Nexus 9000 Series NX-OS</b>                                      | <b>Switch Support</b>   | <b>Topology and Deployment</b>                        |
|---|---|---|---|
| <ul style="list-style-type: none"><li>• 11.4(1)</li><li>• 11.3(1)</li></ul> | <ul style="list-style-type: none"><li>• 9.3(5)</li><li>• 9.3(3)</li></ul> | 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 |

# Hardware Compatibility Information

The Cisco APIC hardware compatibility information for Cisco NAE can be accessed at the following website:

<https://www.cisco.com/c/en/us/support/switches/nexus-9000-series-switches/products-release-notes-list.html>

# Verified Scalability Limits for ACI Fabric

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

*Table 4. 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 5. 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<br><br>Requirements of type Compliance Requirement and Naming Convention<br><br>10<br><br>Requirements of type Segmentation, Traffic Selector, and SLA |

|  |   |
|--|---|
| <p>EPG pair limit check per Requirement (includes both directions)</p> | <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> |
| <p>Fabric wide rules</p>   | <p>150 K</p>  |

*Table 6. 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 7. 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                                |
| 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 8. 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   |

| <b>Feature</b>                          | <b>Scale Limit for Appliance Model: Small</b> | <b>Scale Limit for Appliance Model: Medium</b> |
|---|---|--|
| 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 9. Verified Scalability Limits for Explorer*

| <b>Feature</b>                                    | <b>Scale Limit</b> |
|---|--------------------|
| Total number of associations that can be explored | 500,000            |

# Licensing Information

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

See the [Cisco Nexus Dashboard and Cisco Data Center Day 2 Operations Solution Suite Ordering Guide](#) for more information.

See the *Cisco Network Assurance Engine Installation and Upgrade Guide* for information regarding Smart Licensing.

## End-of-Life and End-of-Sale Notices

The End-of-Life (EoL) and End-of-Sale (EoS) notices for Cisco NAE can be accessed from the following website:

<https://www.cisco.com/c/en/us/products/data-center-analytics/network-assurance-engine/bulletin-listing.html>

# Cisco NAE App Compatibility Information

# Software Compatibility Information

Table 10. Compatibility Information

| Product Name          | Release   |
|-----------------------|---|
| Cisco Nexus Dashboard | <ul style="list-style-type: none"><li>• 2.0.2</li><li>• 2.0.1</li></ul>   |
| Cisco DCNM            | <ul style="list-style-type: none"><li>• 11.4(1)</li><li>• 11.3(1)</li></ul>   |
| Cisco APIC            | <ul style="list-style-type: none"><li>• 5.1(2)</li><li>• 5.1(1)</li><li>• 5.0(2)</li><li>• 5.0(1)</li><li>• 4.2(7)</li><li>• 4.2(6)</li><li>• 4.2(5)</li><li>• 4.2(4)</li><li>• 4.2(3)</li><li>• 3.2(9)</li></ul> |

See the [Compatibility Matrix](#) for more information.

# Verified Scalability

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

*Table 11. Verified Scalability Limits*

| <b>Feature</b>   | <b>Scale Limit for<br/>Deployment Profile:<br/>Small</b> | <b>Scale Limit for<br/>Deployment Profile:<br/>Medium</b> | <b>Scale Limit for<br/>Deployment Profile:<br/>Large</b> |
|------------------|--|---|--|
| APIC Fabric Size | 50 leaf switches   | 100 leaf switches   | 400 leaf switches  |
| DCNM Fabric Size | 50 leaf switches   | 100 leaf switches   | 400 leaf switches  |
| MSO Size         | Up to 4 ACI fabrics                                      | Up to 4 ACI fabrics                                       | Up to 4 ACI fabrics                                      |

See the [Cisco Nexus Dashboard Cluster Sizing](#) for more information.

# Usage Guidelines

This section lists usage guidelines for the Cisco NAE.

- The Cisco NAE appliance leverages email as the mechanism for password recovery. We strongly recommend that you configure the SMTP server information, as that is required by the admin for password recovery. You can configure SMTP server information during Day 0 setup or after you setup the Cisco NAE appliance. To configure SMTP server after Day 0, perform the following steps:
  1. Choose **Settings > Appliance Administration**.
  2. Click the details icon on the **Appliance Settings** card.
  3. Enter the SMTP server information.
- Admin can use the following two methods to change the user's password.
  - In the **Change Password** form, enter the user's current password and then enter the new password.
  - Use the **Forgot Password** link. The SMTP server must be configured in order to reset the password using the forgot password link.
- Ensure that the last octet of the IP address is unique for each VM in the cluster. In the Cisco NAE appliance, hostname is created using last octet of VM's IP address. If the VMs in the Cisco NAE cluster are assigned the same last octet, they will get the same hostname which will lead to issues while forming the cluster.
- We recommend that you upload only one file at a time per VM in the cluster. Uploading multiple files at the same time can lead to the appliance being unresponsive. this recommendation applies to offline datasets and the upload bundle.
- Appliance settings must be configured on only one VM in the Cisco NAE cluster. Do not configure the appliance settings on more than one VM simultaneously.
- The data collected by the Cisco NAE appliance from an unsupported version of APIC or switch, may result in generation of false positives. Assurance events will also be generated. See [Compatibility Information](#) .

# Related Content

The Cisco NAE documentation can be accessed from the following website:

<https://www.cisco.com/c/en/us/support/data-center-analytics/intent-assurance/tsd-products-support-series-home.html>

| <b>Document</b>  | <b>Description</b>                                   |
|--|--|
| <i>Cisco Network Assurance Engine Release Notes</i>                  | This document.                                       |
| <i>Cisco Network Assurance Engine Installation and Upgrade Guide</i> | Describes how to install and upgrade the Cisco NAE.  |
| <i>Cisco Network Assurance Engine Getting Started Guide</i>          | Describes how to configure and manage the Cisco NAE. |
| <i>Cisco Network Assurance Engine Fundamentals Guide</i>             | Describes some of the use cases for the Cisco NAE.   |
| <i>Cisco Network Assurance Engine Smart Events Reference Guide</i>   | Describes the smart events found in the Cisco NAE.   |
| <i>Cisco Network Assurance Engine REST API User Guide</i>            | Describes the REST APIs found in the Cisco NAE.      |

## Documentation Feedback

To provide technical feedback on this document, or to report an error or omission, send your comments to [cisconae-docfeedback@cisco.com](mailto:cisconae-docfeedback@cisco.com). We appreciate your feedback.



# Legal Information

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: [www.cisco.com/go/trademarks](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)

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.

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