



Cisco Nexus 1000 Virtual Edge for VMware vSphere Release Notes, Release 5.2(1)SV5(1.3a)

First Published: 2020-06-29

This document describes the features, limitations, and bugs for Cisco Nexus 1000 Virtual Edge for VMware vSphere (Cisco Nexus 1000VE) Release 5.2(1)SV5(1.3a).

Use this document in combination with documents listed in the [Related Documentation](#) section.

Contents

This document includes the following sections:

- [Introduction, page 2](#)
- [Software Compatibility, page 2](#)
- [Configuration Scale Limits, page 2](#)
- [Important Notes and Limitations, page 3](#)
- [Using the Bug Search Tool, page 5](#)
- [Resolved Bugs, page 6](#)
- [Open Bugs, page 6](#)
- [MIB Support, page 6](#)
- [Related Documentation, page 7](#)
- [Documentation Feedback, page 7](#)
- [Obtaining Documentation and Submitting a Service Request, page 8](#)



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Introduction

Cisco Nexus 1000VE provides a distributed, virtual switch that extends across multiple virtualized hosts. Cisco Nexus 1000VE manages a data center defined by the vCenter Server. Each server in the data center is represented as a line card in Cisco Nexus 1000VE and can be managed similar to a line card in a physical Cisco switch.

Cisco Nexus 1000VE consists of the following components:

- Virtual Supervisor Module (VSM), which contains the Cisco CLI, configuration, and high-level features.
- Virtual Service Engine (VSE), which acts as a line card and runs in each virtualized server to handle packet forwarding and other localized functions.

Software Compatibility

The servers that run the Cisco Nexus 1000VE VSM and VSE must be in the VMware Hardware Compatibility list.

Cisco Nexus 1000VE Release 5.2(1)SV5(1.3a) is a maintenance release and supports vSphere 6.5U2 and later release trains. Cisco Nexus 1000VE supports all virtual machine network adapter types that VMware vSphere supports.

Refer to the VMware documentation when choosing a network adapter. For more information, see the VMware Knowledge Base article #1001805.

[Table 1](#) lists the minimum software versions compatibility between Cisco VSG, Cisco PNSC, and Cisco Nexus 1000VE.

Table 1 **Software Compatibility**

Cisco Nexus 1000VE Version	Cisco VSG Version	Cisco PNSC Version	VMware vCenter Version
5.2(1)SV5(1.3a)	<ul style="list-style-type: none"> • VSG 2.2.2 	<ul style="list-style-type: none"> • PNSC 3.5.1b 	<ul style="list-style-type: none"> • Versions 6.5U2, 6.7U1, 6.7U2, and 6.7U3 for both, Windows and Linux vCenter appliances.

Configuration Scale Limits

The following topics provide configuration scale limit information:

- [Cisco Nexus 1000VE Configuration Scale Limits, page 2](#)
- [Cisco VSG Configuration Scale Limits, page 3](#)

Cisco Nexus 1000VE Configuration Scale Limits

[Table 2](#) lists the configuration scale limits supported in Cisco Nexus 1000VE, Release 5.2(1)SV5(1.3a). Features that do not apply are marked as N/A.

Table 2 Cisco Nexus 1000VE Configuration Scale Limits

Features	Cisco Nexus 1000VE	
	VSE	vDS
Host/DVS	N/A	64
Total vEth Ports	300	4000
vEthernet interfaces per port profile	300	N/A
Port Profile	N/A	2000
VLANs	4094	4094
ACLs	64	64
MAC address per vSE	32000	32000
ACEs per ACL	128	128
PVLAN	N/A	123
SPAN/ERSPAN Sessions	16	16
Cisco Trustsec	<ul style="list-style-type: none"> • 4K IPSGT Mappings (2000 CLI + 2000 SXP) • 1K SUBNET-SGT Mappings (512 CLI + 512 SXP) • 32 SGACLs • 32 ACE's in 3 SGACL's • 8 SXP Peers. • 1K SGT policies. • 300 Device Tracking entries. 	<ul style="list-style-type: none"> • 4K IPSGT Mappings (2000 CLI + 2000 SXP) • 1K SUBNET-SGT Mappings (512 CLI + 512 SXP) • 32 SGACLs • 32 ACE's in 3 SGACL's • 8 SXP Peers. • 1K SGT policies. • 300 Device Tracking entries.

Cisco VSG Configuration Scale Limits

[Table 3](#) lists the configuration scale limits that apply and supersede the scale numbers shown in Cisco Nexus 1000V Configuration Scale Limits section for Cisco VSG.

Table 3 Cisco VSG Configuration Scale Limits

Feature	VSE	vDS
VSG	150 protected by VSG	2400 ports protected by VSG

Important Notes and Limitations

This section lists important notes and limitations for Cisco Nexus 1000VE:

- It is recommended that Nexus1000v administrator save the configuration of VSM (using the **write memory** command) before conducting HOST reboot or VSM/VSE reboot. This ensures all port-profile mappings of VM ports to be saved on VSM and when VSM/VSE comes back online, all the port-profile mappings are restored. It is even better to save VSM configuration whenever there are changes in port-profile mappings of VM ports, so that any unforeseen HOST reboots or VSM/VSE reboots does not make VSM to lose port-profile mappings.
- The HTML5 based vCenter plugin is supported only for the installation/upgrade. For migration, you must use the flex-based plugin. It is recommended to migrate from Classical Nexus 1000V to Release 5.2(1)SV5(1.2) and then upgrade to Release 5.2(1)SV5(1.3a).
- CTS tagging over DPDK is not supported with RBACLs.
- vMotion service gets enabled for VMkernel adapter automatically that causes migration of unwanted VMKernel adapters to outside trunk vDS which eventually affect some services supported on those VMKernel ports. Please refer VMware documentation or Online public forum discussions for more information.
- We do not recommend you to change the Management IP and Domain Id after establishing the SVS connection. However, if you need to the Management IP and Domain Id after change establishing the SVS connection, see *Cisco Nexus 1000VE for VMware vSphere System Management Configuration Guide*.
- For VSEs, the IP addresses are allocated from the Network IP Pool. Hence, after upgrading Cisco Nexus 1000VE Release from a Release from the earlier version to 5.2(1)SV5(1.3), the VSE IP address may not be the same as previously allocated.
- VSE module number indices displayed using the **show module** are dynamically allocated from an internal pool. Hence, module number indices will change after you upgrade Cisco Nexus 1000VE Release from a Release from earlier version to 5.2(1)SV5(1.3a).
- Service disruption is expected during the upgrade process. Ensure that you have sufficient maintenance window during the upgrade process.
- The non-participating vEthernet ports on Cisco Nexus 1000 VE VSMs are deleted every 30 minutes.
- We recommend you to use Cisco Nexus 1000VE Manager vCenter Plugin to deploy or migrate N1KVE. For detailed information, see *Cisco Nexus 1000VE Installation, Migration, and Upgrade Guide*.
- We recommend you to use vmk0 IP address for adding the host to the vCenter. VSE module attach might fail if ESXi host is added using IP address of another VMK.
- We recommend you not to use **write erase** and **reload vsm** commands because they erase entire startup configuration including default port-profiles. Otherwise you need to manually move the ports to respective port-profiles, after the reload.
- Virtual Ethernet port are dynamically assigned and are not fixed for virtual machines.
- There is some traffic loss after a Virtual Machine (vMotion) is migrated from one host to another.
- Cisco Nexus 1000VE supports installation of VSM on VMware vSphere ESXi, CSP 2100, and N1100.
- Bulk migration of all the Virtual machine adapters attached to a port group configured in Nexus 1000VE VSM to any other destination network is not supported.
- Bulk migration of Virtual Network Adapters to Cisco Nexus 1000VE vDS should be limited to batches of 50 ports, with a delay of 30 seconds between batches.
- If Cisco Nexus 1000VE VSE management port-group is a part of the virtual standard switch, you must ensure that the same port-group is replicated in all the ESXi Hosts on which the VSE is to be installed or upgraded.

- Ensure that the management port-group is unique across all the vDS in the Datacenter.
- Only one uplink port-profile is supported on Cisco Nexus 1000VE per ESXi Host. If an ESXi Host in Cisco Nexus 1000V utilizes multiple uplink port-profiles, then consolidate to a single uplink port-profile before migration.
- Only Hosts using common uplink Ethernet port profile can be migrated as a batch.
- Ensure that you have configured different vmknics for Cisco Nexus 1000V specific services (for example, ERSPAN/VSG) and VMware specific services (for example, vMotion) before the migration.
- If the ERSPAN source and destination are in different subnets, and if the ERSPAN source is an L3 control VM kernel NIC attached to a Cisco Nexus 1000VE VSE, you must enable proxy-ARP on the upstream switch. If you do not enable proxy-ARP on the upstream switch (or router, if there is no default gateway), ERSPAN packets are not sent to the destination.
- DHCP is not supported for VSM management IP. The management IP must be configured statically.
- When a VSE communicates with the Cisco VSG in Layer 3 mode, an additional header with 94 bytes is added to the original packet. You must set the MTU to a minimum of 1594 bytes to accommodate this extra header for any network interface through which the traffic passes between the VSE and Cisco VSG. These interfaces can include the uplink port profile, the proxy ARP router, or a virtual switch.
- To upload VSE OVF file to the content library in VMware vCenter version 6.0, the URL option should be used. You cannot upload VSE from the local machine.

Using the Bug Search Tool

Use the Bug Search tool to search for a specific bug or to search for all bugs in a release.

Step 1 Go to <http://tools.cisco.com/bugsearch>.

Step 2 At the Log In screen, enter your registered Cisco.com username and password; then, click **Log In**. The Bug Search page opens.



Note If you do not have a Cisco.com username and password, you can register for them at <http://tools.cisco.com/RPF/register/register.do>.

Step 3 To search for a specific bug, enter the bug ID in the Search For field and press **Return**.

Step 4 To search for bugs in the current release:

- a. In the Search For field, enter **Cisco Nexus 1000VE** and press **Return**. (Leave the other fields empty.)
- b. When the search results are displayed, use the filter tools to find the types of bugs you are looking for. You can search for bugs by modified date, status, severity, and so forth.

To export the results to a spreadsheet, click the **Export Results to Excel** link.

Resolved Bugs

The following table lists the resolved bugs in Cisco Nexus 1000VE Release 5.2(1)SV5(1.3a). The IDs are linked to the Cisco Bug Search tool.

Table 4 *Resolved Bugs in Cisco Nexus 1000VE for VMware vSphere*

Bug ID	Description
CSCvt90921	NG 1.3 : SNMP ACL is causing N1KVE VSM to crash consistently.
CSCvq62948	vEth Port-profile to IPG movement won't happen randomly.
CSCvr43183	Some IPSGT entries are not displayed on VSM.
CSCvt30182	Cisco IOS, IOS XE, and NX-OS Software SGT Exchange Protocol Denial of Service Vulnerability.
CSCvu10050	Cisco NX-OS Software Unexpected IP in IP Packet Processing Vulnerability.

Open Bugs

The following table lists the open bugs in Cisco Nexus 1000VE Release 5.2(1)SV5(1.3a). The IDs are linked to the Cisco Bug Search tool.

Table 5 *Open Bugs in Cisco Nexus 1000VE for VMware vSphere*

Bug ID	Description
CSCvs17554	Traffic drop from VMs connected to Nexus1000VE VSE at 'vmxnet3' (inside-trunk mapped adapter).
CSCvs08376	CTS device tracking entries are not removed from the ipsgt table after rebooting the VSE module.
CSCvs38753	VM interfaces are not moving to the correct IPGs after the host reboot.
CSCvr88984	CTS role-based counters are not appropriate.

MIB Support

The Cisco Management Information Base (MIB) list includes Cisco proprietary MIBs and many other Internet Engineering Task Force (IETF) standard MIBs. These standard MIBs are defined in Requests for Comments (RFCs). To find specific MIB information, you must examine the Cisco proprietary MIB structure and related IETF-standard MIBs supported by the Cisco Nexus 1000VE.

The MIB Support List is available at the following FTP site:

<ftp://ftp.cisco.com/pub/mibs/supportlists/nexus1000v/Nexus1000VMIBSupportList.html>

Documentation Feedback

To provide technical feedback on this document or report an error or omission, send your comments to nexus1k-docfeedback@cisco.com.

We appreciate your feedback.

Related Documentation

This section lists the documents used with the Cisco Nexus 1000VE and available on [Cisco.com](https://www.cisco.com) at the following URL:

<https://www.cisco.com/c/en/us/support/switches/nexus-1000ve/tsd-products-support-series-home.html>

General Information

Cisco Nexus 1000VE Release Notes

Install and Upgrade

Cisco Nexus 1000VE Installation, Migration, and Upgrade Guide

Cisco VSG for VMware vSphere, Release 5.2(1)VSG2(2.2) and Cisco Prime NSC, Release 3.5.1a Installation and Upgrade Guide

Configuration Guides

Cisco Nexus 1000VE Layer 2 Switching Configuration Guide

Cisco Nexus 1000VE Security Configuration Guide

Cisco Nexus 1000VE System Management Configuration Guide

Troubleshooting, Password Recovery, System Messages Guides

Cisco Nexus 1000VE Troubleshooting Guide

Cisco Nexus 1000V Switch for VMware vSphere

[Cisco Nexus 1000V Switch for VMware vSphere Documentation](#)

Cisco Cloud Services Platform 2100

[Cisco Cloud Services Platform 2100 Documentation](#)

Virtual Security Gateway

[Cisco Virtual Security Gateway Documentation](#)

Cisco Prime Network Services Controller

[Cisco Prime Network Services Controller Documentation](#)

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.

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. 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. (1721R)

Internet Protocol (IP) addresses that are used in the examples, command display output, and figures within this document are for illustration only. If an actual IP address appears in this document, it is coincidental.

© 2020 Cisco Systems, Inc. All rights reserved.