



Installing the Cisco VSG

This chapter contains the following sections:

- [Information About the Cisco VSG, on page 1](#)
- [Prerequisites for Installing the Cisco VSG Software, on page 2](#)
- [Obtaining the Cisco VSG Software, on page 3](#)
- [Installing the Cisco VSG Software, on page 3](#)
- [Configuring Initial Settings, on page 7](#)
- [Verifying the Cisco VSG Configuration, on page 10](#)
- [Where to Go Next, on page 11](#)

Information About the Cisco VSG

This section describes how to install and complete the basic configuration of the Cisco VSG for Cisco Nexus 1000v Series switch software.

- [Host and VM Requirements, on page 1](#)
- [Cisco VSG and Supported Cisco Nexus 1000V Series Device Terminology, on page 2](#)

Host and VM Requirements

The Cisco VSG has the following requirements:

- Microsoft SCVMM R2
- Virtual Machine (VM)
 - 64-bit VM is required.
 - x86 Intel or AMD server with a 64-bit processor.
 - 2 GB RAM, recommended space is 4 GB RAM.
 - 3 NICs.
 - Minimum 3 GB hard disk space with LSI Logic Parallel adapter (default), recommended space is 4 GB hard disk.
 - Minimum CPU speed of 1.5 GHz.

Cisco VSG and Supported Cisco Nexus 1000V Series Device Terminology

This table lists the terminology used in the Cisco VSG implementation.

Term	Description
Logical Switch	Logical switch that spans one or more servers. It is controlled by one VSM instance.
NIC	Network interface card.
Server hosting SCVMM	Service that acts as a central administrator for Microsoft Hyper-V hosts that are connected on a network. The server directs actions on the VMs and the VM hosts.
Virtual Ethernet Module (VEM)	Part of the Cisco Nexus 1000V Series switch that switches data traffic. It runs on a Microsoft Hyper-V host. Up to 64 VEMs are controlled by one VSM. All the VEMs that form a switch domain should be in the same virtual data center as defined by the Hyper-V server.
Virtual Machine (VM)	Virtualized x86 PC environment in which a guest operating system and associated application software can run. Multiple VMs can operate on the same host system concurrently.
vPath	Component in the Cisco Nexus 1000V Series switch with a VEM that directs the appropriate traffic to the Cisco VSG for policy evaluation. It also acts as fast path and can short circuit part of the traffic without sending it to the Cisco VSG.
Virtual Security Gateway (VSG)	Cisco software that secures virtual networks and provides firewall functions in virtual environments using the Cisco Nexus 1000V Series switch by providing network segmentation.
Virtual Supervisor Module (VSM)	Control software for the Cisco Nexus 1000V Series distributed virtual device that runs on a Virtual Machine (VM) and is based on Cisco NX-OS.
SCVMM	System Center Virtual Machine Manager Connect remotely to Hyper-V server. It is the primary interface for creating, managing, and monitoring VMs, their resources, and their hosts. It also provides console access to VMs.

Prerequisites for Installing the Cisco VSG Software

The following components must be installed and configured:

- On the Cisco Nexus 1000V Series switch, configure two port profiles for the Cisco VSG: one for the service VLAN and the other for the HA VLAN. (You will be configuring the Cisco VSG IP address on the Cisco VSG so that the Cisco Nexus 1000V Series switch can communicate with it.)

Details about configuring VLANs and port profiles on the Cisco Nexus 1000V Series switch are available in the Cisco Nexus 1000V Series switch documentation.

Obtaining the Cisco VSG Software

You can obtain the Cisco VSG software files at this URL:

<http://software.cisco.com/download/navigator.html>

Installing the Cisco VSG Software

You can install the Cisco VSG software on a VM by using an ISO image file from the CD.

Installing the Cisco VSG Software from an ISO File

Before you begin

Ensure that you have:

- Installed Microsoft SCVMM 2012 R2 or Microsoft SCVMM 2016.
- Downloaded the Cisco VSG ISO image and uploaded it to the server (C:\ProgramData\Virtual Machine Manager Library Files\ISO). Refresh the library server under the Library tab.
- Cisco VSG-Data port profile: VSG-Data.
- Cisco VSG-ha port profile: VSG-ha.
- HA ID.
- IP/subnet mask/gateway information for the Cisco VSG.
- Admin password.
- 2 GB RAM and 3 GB hard disk space.
- Cisco PNSC IP address.
- The shared secret password.
- IP connectivity between Cisco VSG and Cisco PNSC.
- Cisco VSG NSC-PA image name (vnm-cvsgpa.2.1.2a.bin).

Step 1 Launch SCVMM.

Step 2 On the **VMs and Services** tab, click **Create Virtual Machine**.

Step 3 In the **Create Virtual Machine** Wizard, in the **Select Source** screen, check **Create the new virtual machine with a blank virtual hard disk** radio button, and click **Next**.

Step 4 In the **Specify Virtual Machine Identity** screen, enter the name for the Cisco VSG in the **Virtual machine name** field, and click **Next**.

Figure 1: Create Virtual Machine Wizard - Specify Virtual Machine Identity

The screenshot shows the 'Specify Virtual Machine Identity' step of the 'Create Virtual Machine Wizard'. The window title is 'Create Virtual Machine Wizard'. The main title of the step is 'Specify Virtual Machine Identity'. On the left, there is a navigation pane with the following options: 'Select Source', 'Specify Virtual Machine Identity' (which is selected), 'Configure Hardware', 'Select Destination', 'Select Cloud', 'Add Properties', and 'Summary'. The main area contains two input fields: 'Virtual machine name:' with the text 'VSG-1-primary' entered, and 'Description:' which is currently empty. At the bottom of the main area, there is an information icon and a note: 'The virtual machine name identifies the virtual machine to VMM. The name does not have to match the computer name of the virtual machine. However, using the same name ensures consistent displays in System Center Operations Manager.' At the bottom right of the window, there are three buttons: 'Previous', 'Next', and 'Cancel'.

350434

Step 5 In the **Configure Hardware** section, do the following:

- Under **General**, choose **Memory**, choose the **Static** option, and enter 2048 MB in the **Virtual machine memory** field.
- Under **Bus Configuration**, choose the primary disk and enter 3 in the Size (GB) field.
- Choose the virtual DVD Drive, select the **Existing ISO image file** radio button and browse for the VSG ISO within the SCVMM Library.
- Choose the **Network Adapter** drop-down near the top of the Create Virtual Machine Wizard and create two new Network Adapters.
 - Under the **Network Adapters** section, choose **Network Adapter 1**, then choose **Connected to a VM network** and browse for the appropriate network corresponding to the network segment for the VSG's data interface.

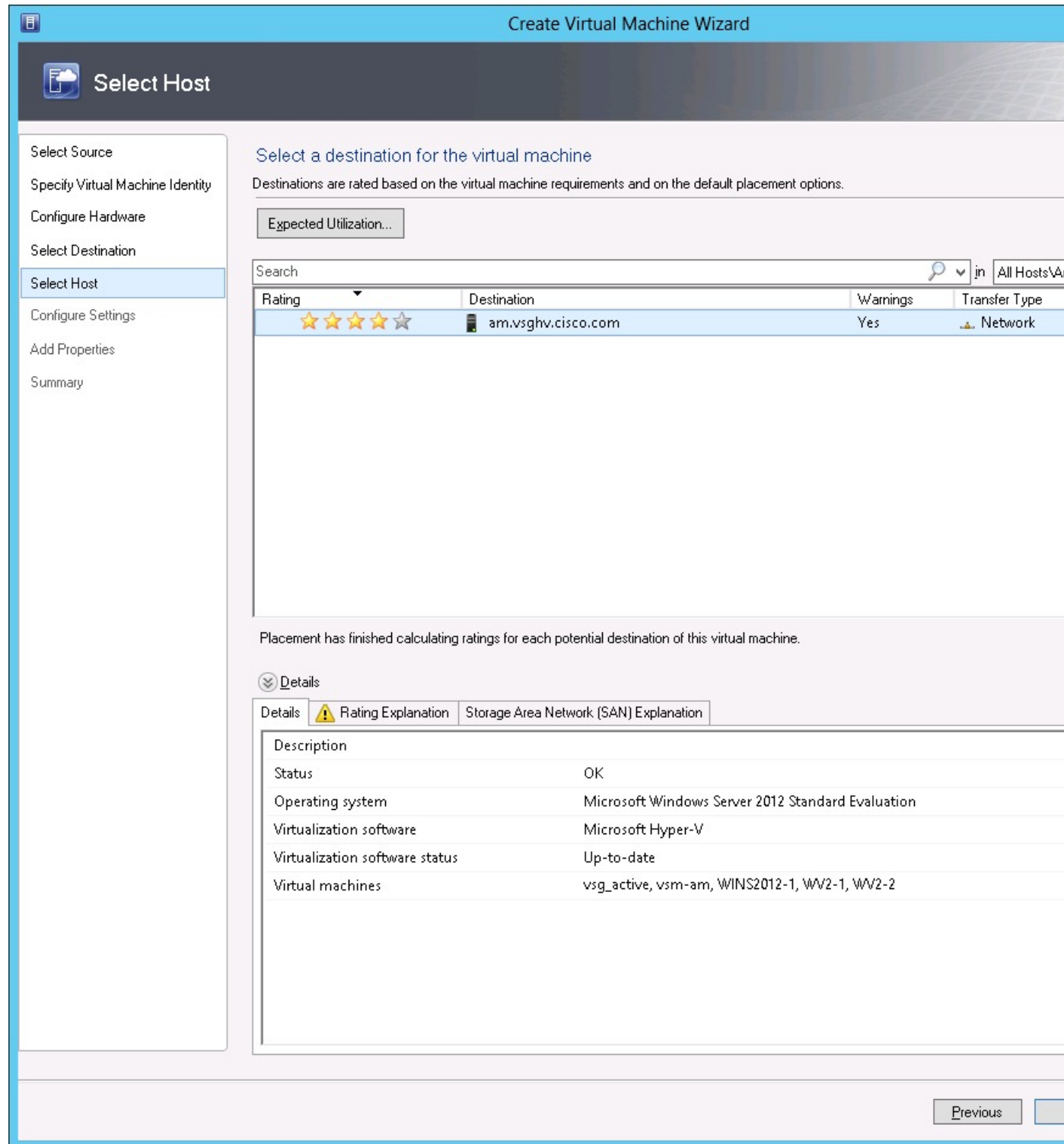
- From the **Classification** drop-down list, choose the port-profile corresponding to the VSG's data interface.

Note Repeat Step d to create network adapters for service interface.

Step 6 In the **Select Destination** section, choose **Place the virtual machine in a host** and choose the host group on which you want to store the VSG from the drop-down and click **Next**.

Step 7 In the **Select Host** section, select the host that you want to place the VSG on and click **Next**.

Figure 2: Create Virtual Machine Wizard - Select Host



Step 8 In the **Configure Settings** section, review the virtual machine settings to ensure they are correct and click **Next**.

- Step 9** (Optional) In the **Add Properties** section, choose **Other Linux (64-bit) from the Operating System** drop-down list, and then click **Next**.
- Step 10** In the **Summary** section, click **Create**.
- Step 11** Choose the VSG in the **VMs and Services** tab and click **Power On**.
- Step 12** Connect to the VSG using **Connect or View -> Connect via Console**.
-

Configuring Initial Settings

This section describes how to configure the initial settings on Cisco VSG and configure a standby Cisco VSG with its initial settings. For configuring a standby Cisco VSG, see [Configuring Initial Settings on a Secondary Cisco VSG, on page 10](#) section.

You can connect to a VSG VM console through the SCVMM user interface by right-clicking a VM instance and connecting to it.

- Step 1** Navigate to the **Console** tab in the VM.
- The Cisco Nexus 1000V Series switch opens the **Console** window and boots the Cisco VSG software.
- Step 2** At the `Enter the password for "admin" prompt`, enter the password for the admin account and press **Enter**.
- Step 3** At the prompt, confirm the admin password and press **Enter**.
- Step 4** At the `Enter HA role[standalone/primary/secondary]` prompt, enter the HA role that you want to use and press **Enter**.
- This can be one of the following:
- standalone
 - primary
 - secondary
- Step 5** At the `Enter the ha id(1-1024)` prompt, enter the HA ID for the pair and press **Enter**.
- Note** If you entered **secondary** in the earlier step, the HA ID for this system must be the same as the HA ID for the primary system.
- Step 6** If you want to perform basic system configuration, at the `Would you like to enter the basic configuration dialog (yes/no)` prompt, enter **yes** and press **Enter**, then complete the following steps.
- a) At the `Create another login account (yes/no) [n]` prompt, do one of the following:
- To create a second login account, enter **yes** and press **Enter**.
 - Press **Enter**.
- b) (Optional) At the `Configure read-only SNMP community string (yes/no) [n]` prompt, do one of the following:
- To create an SNMP community string, enter **yes** and press **Enter**.

- Press **Enter**.

c) At the Enter the Virtual Security Gateway (VSG) name prompt, enter **VSG-demo** and press **Enter**.

Step 7 At the Continue with Out-of-band (mgmt0) management configuration? (yes/no) [y]: prompt, enter **yes** and press **Enter**.

Step 8 At the Mgmt IPv4 address: prompt, enter **10.10.10.11** and press **Enter**.

Step 9 At the Mgmt IPv4 netmask prompt, enter **255.255.255.0** and press **Enter**.

Step 10 At the Configure the default gateway? (yes/no) [y] prompt, enter **yes** and press **Enter**.

Step 11 At the Enable the telnet service? (yes/no) [y]: prompt, enter **no** and press **Enter**.

Step 12 At the Configure the ntp server? (yes/no) [n] prompt, enter **NTP server** information and press **Enter**.

The following configuration will be applied:

```
Interface mgmt0
ip address 10.10.10.11 255.255.255.0
no shutdown
vrf context management
ip route 0.0.0.0/10.10.11.1
no telnet server enable
ssh key rsa 768 force
ssh server enable
feature http-server
ha-pair id 25
```

Step 13 At the Would you like to edit the configuration? (yes/no) [n] prompt, enter **n** and press **Enter**.

Step 14 At the Use this configuration and save it? (yes/no) [y]: prompt, enter **y** and press **Enter**.

Step 15 At the VSG login prompt, enter the name of the admin account you want to use and press **Enter**.

The default account name is admin.

Step 16 At the Password prompt, enter the name of the password for the admin account and press **Enter**.

You are now at the Cisco VSG node.

On the VSG, Configuring the Cisco Prime NSC Policy Agent

Once the Cisco PNSC is installed, you must register the VSG with the Cisco PNSC.



Note Cisco VSG is supported as VSB on Nexus Cloud Services platform only.

Before you begin

Make sure that you know the following:

- The Cisco PNSC policy-agent image is available on the VSG (for example, vnmc-vsopa.2.1.2a.bin)



Note The string **vsghv-pa** must appear in the image name as highlighted.

- The IP address of the Cisco PNSC.
- The shared secret password you defined during the Cisco PNSC installation.
- That IP connectivity between the VSG and the Cisco PNSC is working.



Note If you upgrade your VSG, you must also copy the latest Cisco VSG policy agent image. This image is available in the Cisco PNSC image bundle to boot from a flash drive and to complete registration with the Cisco PNSC.



Note VSG clock should be synchronized with the Cisco PNSC clock.

Step 1 On the VSG, enter the following commands:

```
VSG-Firewall# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
VSG-Firewall(config)# nsc-policy-agent
VSG-Firewall(config-nsc-policy-agent)# registration-ip 10.193.72.242
VSG-Firewall(config-nsc-policy-agent)# shared-secret Sgate123
VSG-Firewall(config-nsc-policy-agent)# policy-agent-image vnm-c-vsgpa.2.1.2a.bin
VSG-Firewall(config-nsc-policy-agent)# copy running-config startup-config
[#####] 100%
Copy complete, now saving to disk (please wait)...
VSG-Firewall(config-nsc-policy-agent)# exit
```

Step 2 Check the status of the NSC policy agent configuration to verify that you have installed the Cisco PNSC correctly and it is reachable by entering the **show nsc-pa status** command. This example shows that the Cisco PNSC is reachable and the installation is correct:

```
VSG-Firewall(config)# show nsc-pa status
NSC Policy-Agent status is - Installed Successfully. Version 2.1(2a)-vsg
```

The VSG is now registered with the Cisco PNSC.

Example

This example shows that the Cisco PNSC is unreachable or an incorrect IP is configured:

```
vsg# show nsc-pa status
NSC Policy-Agent status is - Installation Failure
Cisco PNSC not reachable.
vsg#
```

This example shows that the NSC policy-agent is not configured or installed:

```
vsg# show nsc-pa status
NSC Policy-Agent status is - Not Installed
```

Configuring Initial Settings on a Secondary Cisco VSG

You can configure a standby Cisco VSG by logging in to the Cisco VSG you have identified as secondary and using the following procedure to configure a secondary Cisco VSG with its initial settings.

-
- Step 1** Navigate to the **Console** tab in the VM.
Cisco Nexus 1000V Series switch opens the **Console** window and boots the Cisco VSG software.
- Step 2** At the `Enter the password for "admin"` prompt, enter the password for the admin account and press **Enter**.
- Step 3** At the prompt, confirm the admin password and press **Enter**.
- Step 4** At the `Enter HA role[standalone/primary/secondary]` prompt, enter the **secondary** HA role and press **Enter**.
- Step 5** At the `Enter the ha id(1-1024)` prompt, enter **25** for the HA pair Id and press **Enter**.
- Note** The HA ID uniquely identifies the two Cisco VSGs in an HA pair. If you are configuring Cisco VSGs in an HA pair, make sure that the ID number you provide is identical to the other Cisco VSG in the pair.
- Step 6** At the `VSG login` prompt, enter the name of the admin account you want to use and press **Enter**.
The default account name is `admin`.
- Step 7** At the `Password` prompt, enter the name of the password for the admin account and press **Enter**.
You are now at the Cisco VSG node.
-

Verifying the Cisco VSG Configuration

To display the Cisco VSG configuration, perform this task:

Command	Purpose
<code>show interface brief</code>	Displays a brief status and interface information.

This example shows how to verify the Cisco VSG configurations:

```
firewall# show interface brief
-----
Port      VRF      Status IP Address      Speed  MTU
-----
mgmt0    --      up      10.2.71.43      --     1500
-----
Port      VRF      Status IP Address      Speed  MTU
-----
data0    --      up              --             --     9000
```

Where to Go Next

After installing and completing the initial configuration of the Cisco VSG, you can configure firewall policies on the Cisco VSG through the Cisco Prime NSC.

