Secure Web Gateway
Virtual Appliance
Initial Configuration Guide
for High-Performance Models

Platform: VMware vSphere Hypervisor

Version 6.7.x and later

Broadcom reserves the right to make changes without further notice to any products or data herein to improve reliability, function, or design. Information furnished by Broadcom is believed to be accurate and reliable. However, Broadcom does not assume any liability arising out of the application or use of this information, nor the application or use of any product or circuit described herein, neither does it convey any license under its patent rights nor the rights of others.

Document Revision: 05/2021

Additional Restrictions

ProxySG Appliances

Within sixty (60) days of the date from which the User powers up the ProxySG appliance ("Activation Period"), the Administrator must complete the ProxySG licensing requirements as instructed by the ProxySG to continue to use all of the ProxySG features. Prior to the expiration of the Activation Period, the ProxySG software will deliver notices to install the license each time the Administrator logs in to manage the product. Failure to install the license prior to the expiration of the Activation Period may result in some ProxySG features becoming inoperable until the Administrator has completed licensing.

Proxy Client:

The Administrator may install the Proxy Client only on the number of personal computers licensed to them. Each personal computer shall count as one "user" or "seat." The ProxyClient software may only be used with Blue Coat ProxySG appliances. The Administrator shall require each user of the Blue Coat ProxyClient software to agree to a license agreement that is at least as protective of Blue Coat and the Blue Coat ProxyClient software as the Blue Coat EULA.

ProxySG Virtual Appliances, MACH5 or Secure Web Gateway (SWG) Edition:

The ProxySG Virtual Appliances (MACH5 or Secure Web Gateway edition) are licensed on either a perpetual or subscription basis for a maximum number of concurrent users. Support for the Virtual Appliances will be subject to the separate support agreement entered into by the parties if the Administrator licenses the Virtual Appliances on a perpetual basis. The Virtual Appliances will (a) not function upon expiration of the subscription if the Administrator licenses the Virtual Appliances on a subscription basis; or (b) if the traffic exceeds the maximum number of concurrent users/connections, features may not function beyond the maximum number of concurrent users/connections. This means that, in these cases, the network traffic will only be affected by the default policy set by the Administrator (either pass or deny). Such cessation of functionality is by design, and is not a defect in the Virtual Appliances. The Administrator may not install the same license key or serial number on more than one instance of the Virtual Appliance. The Administrator may move the Virtual Appliance along with its license key and serial number to a different server, provided that server is also owned by the Administrator and the Administrator permanently deletes the prior instance of the Virtual Appliance on the server on which it was prior installed. The Virtual Appliances require a third party environment that includes software and/or hardware not provided by Blue Coat, which the Administrator will purchase or license separately. Blue Coat has no liability for such third party products.

Contents

Chapter 1: Overview

Chapter 2: Before You Begin

Chapter 3: Create the SWG VA

Chapter 4: Configure the SWG Virtual Appliance

Appendix A: Supplemental Information

Chapter 1: Overview

The Secure Web Gateway Virtual Appliance (SWG VA) is a software solution that can be installed and deployed on a server running VMware vSphere Hypervisor. SWG VA facilitates server consolidation by co-existing with other virtual machines on a single hardware platform, including Symantec Content Analysis and Blue Coat ProxySG Virtual Appliance MACH5 Edition. With the SWG VA providing security, the other virtual machines can provide branch office services (such as Domain Controller, print, DNS, and DHCP), as well as any VMware-certified software applications.

Symantec is VMware Ready™, having worked closely with VMware to ensure that the SWG VA runs efficiently in the virtual environment and meets all technical criteria and specifications.

Note: VMware Ready is a validation program designed to provide the best possible user experience among virtual appliances deployed in production. This status indicates that Symantec has followed best practices and that the SWG VA is optimized for VMware vSphere, helping to ensure “ready-to-run” reliability and security.

Section 1 About This Guide

This guide is intended for users who are deploying and running the high-performance model SWG VA on VMware's vSphere Hypervisor. It provides information on the minimum system requirements and instructions for creating and configuring a virtual ProxySG appliance.

The following topics are covered in this guide:

- "Before You Begin" on page 13
- "Create the SWG VA" on page 23
- "Configure the SWG Virtual Appliance" on page 33
- "Supplemental Information" on page 47

Note: MySymantec (https://support.symantec.com) has the most up-to-date version of this guide.

Section 2 Conventions Used in This Guide

This guide uses the following typographical conventions:

Convention	Example
Terms that identify buttons, fields, menus, or options on the user are shown in bold Arial font.	1. Select **Maintenance > Licensing > Install**. 2. Click **Retrieve**.
Text that you must type exactly is denoted using bold, Courier New font.	Enter **`https://`** **<ProxySG_*IP_address*>`:8082/mgmt`**
Information that is variable and specific to your environment is denoted in angle brackets and in italics.	<ProxySG_*IP_address*> in `https://` <ProxySG_*IP_address*>`:8082/mgmt`

Section 3 Terminology

The following table lists the terms used in this guide.

Term	Definition
Appliance Serial Number	A string of numbers that uniquely identify a virtual appliance. On the first bootup, you must enter the appliance serial number to begin initial configuration on the SWG VA. High-performance model serial numbers have "59" as the middle digits.
Datastore	Storage defined in VMware vSphere Hypervisor, made up of one or more physical disks.
Director	The Symantec Director is a centralized management platform for managing ProxySG configurations and policies. It allows you to manage multiple ProxySG appliances in your deployment.
Enable Mode	A mode that allows administrative privileges on the command line interface (CLI) of the ProxySG appliance. You can make changes to the configuration in this mode.
Enable Password	A password used to enter enable mode so that you can modify settings and configure an appliance. Enable mode is for administrators who are authorized to configure an appliance.
VMware vSphere Hypervisor	The physical computer (host server) on which VMware's virtualization product is installed. The vSphere Hypervisor provides CPU and memory resources, access to storage, and network connectivity to multiple virtual machines.
Management Console	The web interface for configuration of the SWG VA. Enter the following URL in the web browser to directly access the Management Console: `https://<ProxySG_IP_address>:8082` <ProxySG_*IP_address*> is the IP address of your SWG VA.
OVF	Open Virtualization Format. A format for packaging and distributing virtual machines. The OVF file in the Virtual Appliance Package (VAP) is an XML text file that defines the attributes of a specific virtual machine package.
SWG VA	A ProxySG with a Secure Web Gateway (SWG) license running as a virtual appliance on VMware's vSphere Hypervisor.
SGOS	The ProxySG operating system.
Symantec Network Protection Licensing Portal	Licensing portal for licensing your SWG VA. https://services.bluecoat.com/eservice_enu/licensing/register.cgi

Term	Definition
VAP	The Virtual Appliance Package is the zip file that contains the OVF file and the virtual disk file (.vmdk) required for creating the SWG VA. It also includes a PDF of this guide, the *Initial Configuration Guide for SWG VA High-Performance Models*.
Virtual Machine	An instance of an operating system and one or more applications that run in an isolated partition of a VMware vSphere Hypervisor. SWG VA is a virtual machine.
VLAN	Virtual Local Area Network. A local area network (LAN) that is created with software. It maps clients (hosts) logically rather than physically, and extends across LAN segments instead of remaining in one physical LAN.

Chapter 2: Before You Begin

This chapter assumes that you have configured your hardware platform as a VMware vSphere Hypervisor, created datastores, and configured the vSphere Hypervisor for network access. For information on setting up your vSphere Hypervisor, refer to VMware documentation.

Before you proceed with creating the Secure Web Gateway Virtual Appliance (SWG VA), perform the following tasks:

- ❐ "Verify Support for VMware Products" on page 14
- ❐ "Verify System Requirements" on page 15
- ❐ "Verify Resource Availability" on page 17
- ❐ "Retrieve Appliance Serial Numbers" on page 19
- ❐ "Create a Virtual Switch" on page 21

Note: The instructions in this document are for vSphere Client version 5.5.

Section 1 Verify Support for VMware Products

Refer to the following table to ensure that your virtual machine supports the version of VMware.

Your SGOS version	Supported VMware versions
6.7.x, 7.1.x, and 7.2.x	ESXi 5.5, 6.0, 6.5, and 6.7

Note: SWG VA supports VMotion, Distributed Resource Scheduling (DRS), High Availability (HA), clustering, and resource pools. However, SWG VA images do not support VMWare Tools or the per-machine HA monitoring feature included with VMWare Tools.

Supported Virtual Hardware Versions

In SGOS 6.7.x and later, the virtual hardware version is set automatically to the highest level that the ESX server supports. For example, if the version is ESXi 6.0, the virtual hardware version is 11.

For more information on VMware and virtual hardware versions, refer to the following VMware article:

https://kb.vmware.com/s/article/1003746

Section 2 Verify System Requirements

To achieve the best performance on the SWG VA, it is important that you install the software on a system that meets the specified requirements. Follow these guidelines to guarantee satisfactory performance and operation of the SWG VA.

The host server must be on VMware's Hardware Compatibility List (see the list at http://www.vmware.com/resources/compatibility/search.php). The server must have sufficient virtual resources to run a SWG VA, as described below.

Note: The following requirements reflect Symantec's test environment. Using the same or a similar configuration should achieve satisfactory performance of the SWG VA; however, you should expect different performance results if your resources or virtual drive configuration are different from the configuration described in Table 2–1 and Table 2–2. Be aware that over-provisioning CPUs can cause license suspension, but under-provisioning can cause sub-optimal VA performance and operation.

Table 2–1 General System Requirements

Resource	Requirement
Virtual CPU **Note:** You must reserve at least the minimum CPU. See "Reserve Resources for the SWG VA" on page 29.	1 GHz (minimum); 2.6 GHz (recommended)
Minimum storage space per disk	100 GB

The following table lists requirements for each model, including recommended and alternate virtual drive configurations. Symantec recommends creating 100GB virtual drives, although models with higher storage requirements can have larger drives. Note that each virtual drive must be the same size.

Note: After you have deployed your virtual appliance, you should have the number of virtual disks that the model requires (listed in the following table) plus a boot disk. The boot disk is automatically created during deployment.

Table 2–2 Model-Specific Requirements

Model	Virtual CPUs	Virtual Memory (GB)	Total Storage (GB)	Recommended Virtual Disk Configuration	Alternate Disk Configurations
SG-VA-C1XS	1	4	100	1x100GB	n/a
SG-VA-C1S	1	4	100	1x100GB	n/a
SG-VA-C1M	1	6	100	1x100GB	n/a
SG-VA-C1L	1	8	100	1x100GB	n/a
SG-VA-C2S	2	8	100	1x100GB	n/a
SG-VA-C2M	2	12	100	1x100GB	n/a
SG-VA-C2L	2	16	100	1x100GB	n/a
SG-VA-C4S	4	16	200	2x100GB	n/a
SG-VA-C4M	4	24	200	2x100GB	n/a
SG-VA-C4L	4	32	200	2x100GB	n/a
SG-VA-C8S	8	32	400	4x100GB	2x200GB
SG-VA-C8M	8	48	400	4x100GB	2x200GB
SG-VA-C8L	8	64	400	4x100GB	2x200GB
SG-VA-C16S	16	64	800	8x100GB	4x200GB 2x400GB
SG-VA-C16M	16	96	800	8x100GB	4x200GB 2x400GB
SG-VA-C16L	16	128	800	8x100GB	4x200GB 2x400GB

Note: With fewer disks, more throughput is required per disk. See "Throughput Requirements Per Virtual Disk" on page 55 for disk read and write throughput rates per disk.

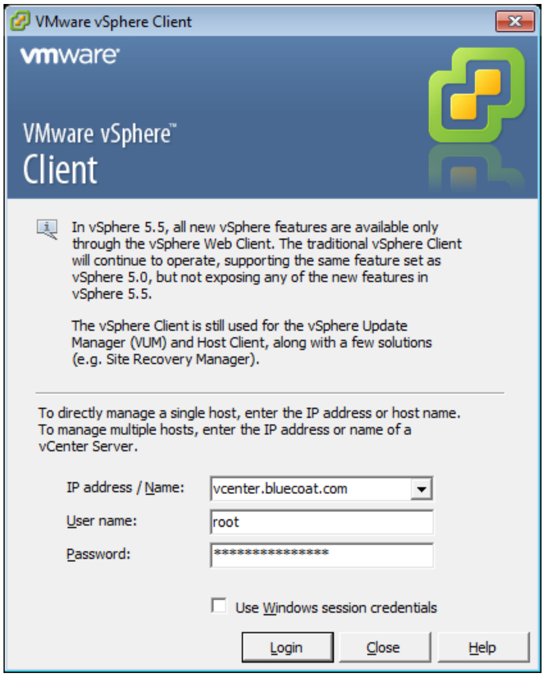
Section 3 Verify Resource Availability

Because all virtual appliances use a hardware resource pool that can be shared and assigned as needed, you must verify that the vSphere Hypervisor meets the minimum hardware requirements for the SWG VA model that you have purchased.

The following instructions describe how to verify system resources on the vSphere Hypervisor using a VMware client. The client is used to connect directly to a vSphere Hypervisor or indirectly to a vSphere Hypervisor through vCenter Server.

To verify resource availability:

1. Use your VMware client to log in to the vSphere Hypervisor.



In vSphere 5.5, all new vSphere features are available only through the vSphere Web Client. The traditional vSphere Client will continue to operate, supporting the same feature set as vSphere 5.0, but not exposing any of the new features in vSphere 5.5.

The vSphere Client is still used for the vSphere Update Manager (VUM) and Host Client, along with a few solutions (e.g. Site Recovery Manager).

To directly manage a single host, enter the IP address or host name. To manage multiple hosts, enter the IP address or name of a vCenter Server.

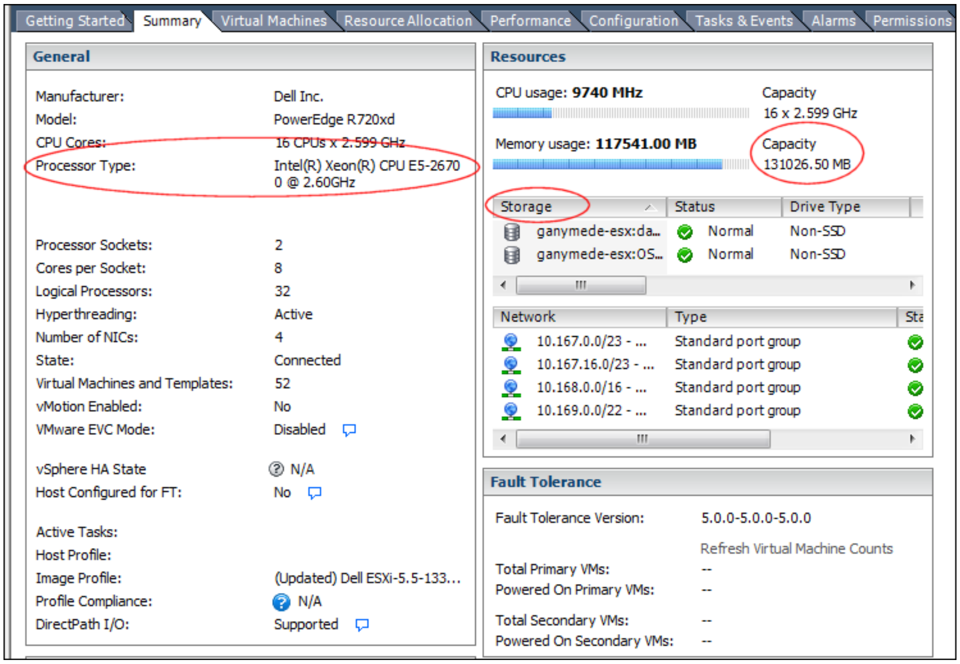
IP address / Name: vcenter.bluecoat.com

User name: root

Password: ***************

□ Use Windows session credentials

2. To display the summary of the vSphere Hypervisor's resources, select the ESX server and click the **Summary** tab.



General

Manufacturer:	Dell Inc.
Model:	PowerEdge R720xd
CPU Cores:	16 CPUs x 2.599 GHz
Processor Type:	Intel(R) Xeon(R) CPU E5-2670 0 @ 2.60GHz
Processor Sockets:	2
Cores per Socket:	8
Logical Processors:	32
Hyperthreading:	Active
Number of NICs:	4
State:	Connected
Virtual Machines and Templates:	52
vMotion Enabled:	No
VMware EVC Mode:	Disabled
vSphere HA State	N/A
Host Configured for FT:	No
Active Tasks:	
Host Profile:	
Image Profile:	(Updated) Dell ESXi-5.5-133...
Profile Compliance:	N/A
DirectPath I/O:	Supported

Resources

CPU usage: **9740 MHz** Capacity 16 x 2.599 GHz

Memory usage: **117541.00 MB** Capacity 131026.50 MB

Storage	Status	Drive Type
ganymede-esx:da...	Normal	Non-SSD
ganymede-esx:OS...	Normal	Non-SSD

Network	Type	Sta
10.167.0.0/23 - ...	Standard port group	✓
10.167.16.0/23 - ...	Standard port group	✓
10.168.0.0/16 - ...	Standard port group	✓
10.169.0.0/22 - ...	Standard port group	✓

Fault Tolerance

Fault Tolerance Version:	5.0.0-5.0.0-5.0.0
	Refresh Virtual Machine Counts
Total Primary VMs:	--
Powered On Primary VMs:	--
Total Secondary VMs:	--
Powered On Secondary VMs:	--

3. Verify adequate resource availability.

   a. In the **General** panel, confirm that the processor speed meets or exceeds requirements. See Table 2–1, "General System Requirements" on page 15.

   b. In the **Resources** panel, beside **Memory usage**, confirm that the memory **Capacity** meets or exceeds requirements of your SWG VA model. For example, the SG-VA-C8M requires 48 GB RAM. See Table 2–2, "Model-Specific Requirements" on page 16.

   c. In the **Resources** panel, in the **Storage** section, confirm that there is adequate free space on a local datastore on the vSphere Hypervisor to accommodate the disk requirements of your SWG VA model. For example, the SG-VA-C8M requires a total storage space of 400 GB.

Section 4 Retrieve Appliance Serial Numbers

The Symantec eFulfillment email you received after placing your order for SWG VA appliances contains activation codes for retrieving appliance serial numbers from the Symantec Network Protection Licensing Portal.

Note: Be sure to use the correct serial number for your SWG VA. It helps ensure that your license is valid.

To retrieve appliance serial numbers:

1. Make sure you have a MySymantec username and password. In addition to retrieving appliance serial numbers, these credentials are required for obtaining your license and downloading software upgrades.

   If you do not have a MySymantec account, contact NP_Customercare@symantec.com.

   For additional contact information, see https://support.symantec.com.

2. Locate the email you received from Symantec. This email contains the software activation codes as well as a link to the BCLP.

3. Log in to BCLP.

   a. Click the link embedded in the email (https://services.bluecoat.com/eservice_enu/licensing/register.cgi).
   The web browser displays the BCLP page.

   b. On the BCLP login screen, enter your MySymantec username and password, and then click **Login**.
   A Home page displays.

4. In the **Enter Activation Code** field, enter any activation code that is listed in your email; the system retrieves all serial numbers from the same purchase order.

   a. Type the code as it appears in the email, or copy and paste it into the **Enter Activation Code** field.

   b. Click **Next**.
   The License Agreement page displays.

5. Read and accept the License Agreement.

   a. Read the license agreement.

   b. Select **I accept** at the bottom of the page.

   c. Click **Next**.
   A serial numbers page displays.

6. Record the appliance serial number(s). You will refer to the serial number when you perform initial configuration on the SWG VA.

   Perform one of the following tasks to note the appliance serial number:

   - Write down the serial number(s) listed on the screen.
   - Download a comma-separated values (CSV) file containing all of the serial numbers. Click the link beside **Download as CSV file** and save the file to disk.

For future reference, record the location and name of the SWG VA with the serial number.

Note: Each appliance serial number is unique. When performing initial configuration on the SWG VA, make sure that you use a dedicated serial number for each instance of a SWG VA. If you reuse a serial number, the SWG VA license could be suspended. See "Serial Numbers and Licensing" on page 50 for more information.

Connection Limits

The SWG VA supports a maximum number of concurrent connections and enforces this by limiting the number of unique clients. Connections will be queued after the connection limit is reached.

Use the `show license` CLI command to verify the number of concurrent users (i.e., connections) your SWG VA is licensed for.

To upgrade the connection limit for your SWG VA, see "How do I upgrade the connection limit for the SWG VA?" on page 51. Note that you will need to reboot after upgrading the license to reset the connection limits.

Section 5 Create a Virtual Switch

A virtual machine has virtual network interfaces that are not physically cabled to a network interface card (NIC) on the vSphere Hypervisor host. To provide network access, a virtual switch (vSwitch) is required to logically connect the virtual network interfaces on the virtual machine to a physical NIC on the vSphere Hypervisor host.

By default, the vSphere Hypervisor creates a vSwitch that is connected to a physical NIC. You can use this default vSwitch, use a vSwitch created for an existing deployment, or create a new vSwitch for the SWG VA.

If you are running SGOS 6.7.5.10 or earlier, the SWG VA can include up to four virtual network interfaces—0:0, 1:0, 2:0, and 3:0. If you are running SGOS 6.7.5.11 or later, the SWG VA can include up to ten virtual network interfaces—0:0, 1:0, 2:0, 3:0, 4:0, 5:0, 6:0, 7:0, 8:0, and 9:0.

If your network topology requires additional interfaces for handling management traffic to the SWG VA, you can create vSwitches for the interfaces or use an existing vSwitch that provides the connectivity you require.

Note: If you use VLANs for segregating traffic within the vSphere Hypervisor or across your network, you must enable VLAN trunking on all interconnecting devices such as switches or routers. This guide does not include information on VLAN configurations.

To create a virtual switch:

1. In your VMware client, select the virtual machine that will host the SWG VA.
2. Click the **Configuration** tab and select **Hardware** > **Networking.**
3. Click **Add Networking**.
4. In the wizard that appears, select **Virtual Machine** in the **Connection Types** dialog box. Click **Next**.
5. Select the switch and the NIC to manage the traffic to and from the SWG VA. Create a new switch if necessary. The physical NIC will be mapped to the virtual switch. Click **Next**.
6. Specify the **Network Label**. The default label is **VM Network*.***
7. Make sure that the **VLAN ID** menu has **None (0)** selected.

   Note: This guide assumes that you do not use VLANs. If you use VLANs, select **All (4095)** to enable VLAN trunking. This value enables Virtual Guest Machine Tagging mode on the switch, and allows the virtual switch to preserve VLAN tags between the virtual machine and the external switch/router.

8. Click **Next**.

9. Verify the details and click **Finish**.

Chapter 3: Create the SWG VA

This chapter describes how to deploy a virtual appliance on the vSphere Hypervisor and ensure that the SWG VA has the resources available for optimal performance.

To create the SWG VA, you must have administrator privileges on the vSphere Hypervisor.

This chapter covers the following topics:

- ❒ "Download the Virtual Appliance Package" on page 24
- ❒ "Deploy a SWG VA" on page 26
- ❒ "Reserve Resources for the SWG VA" on page 29
- ❒ "Power on the SWG VA" on page 31

Note: The instructions in this chapter are for vSphere Client version 5.5.

Section 1 Download the Virtual Appliance Package

The Virtual Appliance Package (VAP) is a zip file that contains the following files:

- Open Virtualized Format (OVF) file

Note: If the VM is running ESXi 6.x, use the OVF file with "ESXi6.x" in its name in "Deploy a SWG VA" on page 26.

- Virtual Machine Disk Format (VMDK) file
- A PDF of this document, the *Initial Configuration Guide for SWG VA High-Performance Models*

Note: If you have already downloaded the VAP, skip this procedure and proceed to "Deploy a SWG VA" on page 26.

To download the VAP:

1. Go to MySymantec:

   https://support.symantec.com
2. Select **Downloads > Network Protection (Blue Coat) Downloads**.
3. When prompted, log in with your MySymantec credentials.
4. Select your product.
5. Select your appliance model (if applicable).
6. Select a software version.
7. Accept the License Agreement.
8. Select the file(s) to download and click **Download Selected Files**.

   Note: The first time you download files, you are prompted to install the Download Manager. Follow the onscreen prompts to download and run the installer. For more information, refer to https://www.symantec.com/support-center/getting-started.
9. The Download Manager window opens. Select the download location.

   Note: Complete instructions are also available online at:
   https://www.symantec.com/support-center/getting-started
   Bookmark this page for future reference.
10. Extract the contents of the VAP file.

    The files should be extracted to a location that can be accessed from the system running the VMware client or vCenter Server.

Note: Because the `.ovf` file includes a pointer to the `.vmdk` file, you must extract and store the contents of the `.zip` file within the same folder. Do not rename the files.

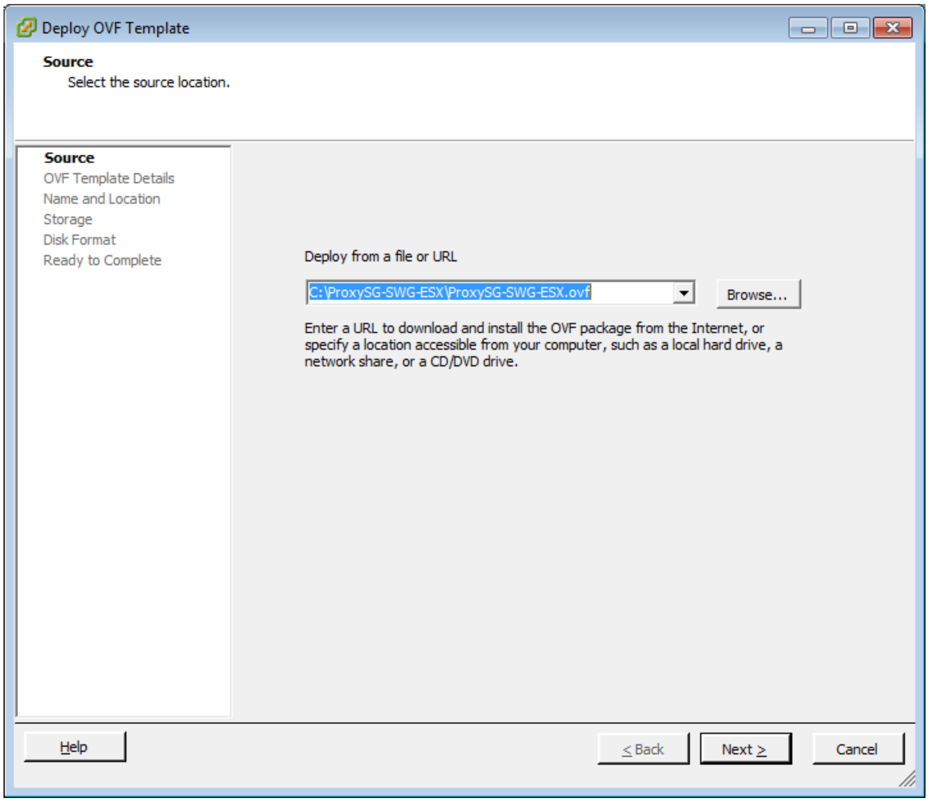
Section 2 Deploy a SWG VA

If the VM is running ESXi 6.x, remember to select the OVF file with “ESXi6.x” in its name when importing the SWG VA.

To deploy a SWG VA:

1. Create the SWG VA on your host vSphere Hypervisor.
   a. In your VMware client, select your host vSphere Hypervisor.
   b. Select **File** > **Deploy OVF Template.** The Deploy OVF Wizard begins.

> **Note:** The equivalent command in VI Client is **File** > **Virtual Appliance** > **Import.**



Deploy OVF Template

Source

Select the source location.

Deploy from a file or URL: C:\ProxySG-SWG-ESX\ProxySG-SWG-ESX.ovf

Enter a URL to download and install the OVF package from the Internet, or specify a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

   c. In the **Deploy from a file or URL** field, browse to the location of the OVF file.
      Alternatively, copy and paste the URL of an OVF file.
      Click **Next**.
   d. Verify the OVF template details and click **Next**.
   e. Enter a name for the SWG VA, such as *SGVA_Sydney*. (The default name is *ProxySG Model SWG*). You should enter a name that is unique within your vSphere Hypervisor host.
   f. Select an **Inventory Location**. Click **Next**.
   g. In the **Configuration** dialog, select the SWG VA model, for example, *SG-VA-C2S*.

Note: If you have purchased a SG-VA-C1XS model, choose SG-VA-C1S from the Configuration list, since these two models have the same basic configuration.

h. In the **Storage** dialog, select a datastore with sufficient free space for your SWG VA model. See Table 2–2, "Model-Specific Requirements" on page 16 for disk space requirements. Click **Next**.

i. In the **Disk Format** dialog, select one of the thick provisioning types for the virtual disk format and click **Next**.

j. In the **Network Mapping** dialog, specify the networks for each interface.

k. Click **Next**.

l. Review the deployment settings and click **Finish** to begin creating the SWG VA.
See the **Recent Tasks** panel for the progress bar indicating the percentage complete.

2. (Required only if you plan to use the third and fourth interfaces) Enable the vSwitch for the third and fourth interfaces.

   a. Select the SWG VA on the vSphere Hypervisor Server.

   b. Right click and select **Edit Settings**.

   c. Select **Hardware** > **Network Adapter 3**.

   d. In the **Device Status** panel, mark the **Connect at power on** check box.
   If necessary, repeat these steps for the fourth interface.

   e. Click **OK**.

   Note: When the VA is first imported, it has one 100 GB data drive attached. Depending on your SWG VA model, you may need to create additional virtual disks. For example, the SG-VA-C16S requires 800 GB of storage space so you must create additional drives, with each drive being the same size. See Table 2–2, "Model-Specific Requirements" on page 16.

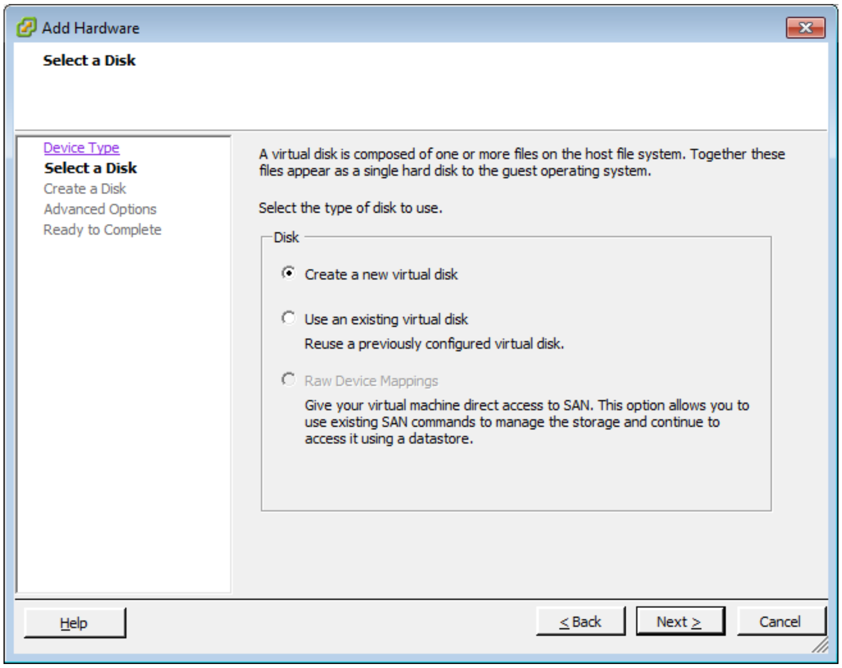
3. Create additional virtual disks as required for your SWG VA model.

   a. Select the SWG VA on the vSphere Hypervisor Server.

   b. Right click and select **Edit Settings**.

   c. In the **Hardware** tab, click **Add**.

d. Select **Hard Disk** and click **Next**.



Add Hardware

Select a Disk

A virtual disk is composed of one or more files on the host file system. Together these files appear as a single hard disk to the guest operating system.

Select the type of disk to use.

Disk

● Create a new virtual disk

○ Use an existing virtual disk
Reuse a previously configured virtual disk.

○ Raw Device Mappings
Give your virtual machine direct access to SAN. This option allows you to use existing SAN commands to manage the storage and continue to access it using a datastore.

e. Choose **Create a new virtual disk** and click **Next**.

f. Specify the size. Note that each virtual drive must be the same size.

g. Select a **Location**.

Note: For optimal performance, create each virtual disk on a different physical disk.

h. Modify **Advanced Options** if required, and click **Next**.

Note: Virtual disks must be thick provisioned (either Lazy or Eager Zeroed).

i. Click **Finish**.

j. Repeat steps 3a–3i for each virtual disk that your SWG VA model requires.

4. Click **OK** to close the Virtual Machine Properties window.

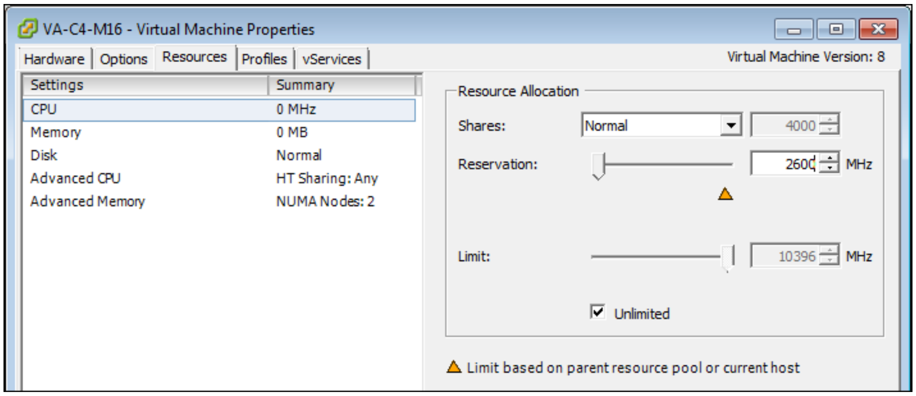
Section 3 Reserve Resources for the SWG VA

Symantec recommends reserving memory and CPU core(s) for the SWG VA. If resource allocation is not accurate for the SWG VA, the virtual appliance might not perform optimally.

If the vSphere Hypervisor host does not have the available resources to satisfy the resource reservations, the SWG VA will not power on.

To reserve resources:

1. Determine the appropriate value for the CPU reservation. The reservation should be the full CPU frequency of all cores.
   a. In your VMware client, select the vSphere Hypervisor host.
   b. Click the **Summary** tab.
   c. Under **General**, note the processor speed (for example, 2.60 GHz).
   d. Multiply this number by 1,000 to obtain the value in MHz.
      For example, 1000 x 2.6 = 2600 MHz.
   e. Multiply this value by the number of cores. With two cores, the CPU reservation in this example would be 2 x 2600 = 5200 MHz.
2. Specify the CPU reservation value for the SWG VA.
   a. Select the SWG VA on the vSphere Hypervisor host.
   b. Right click and select **Edit Settings.**
      The **Virtual Machine Properties** window opens.
   c. On the **Resources** tab, select **CPU.**



VA-C4-M16 - Virtual Machine Properties

Virtual Machine Version: 8

Settings	Summary
CPU	0 MHz
Memory	0 MB
Disk	Normal
Advanced CPU	HT Sharing: Any
Advanced Memory	NUMA Nodes: 2

Resource Allocation

Shares: Normal 4000

Reservation: 2600 MHz

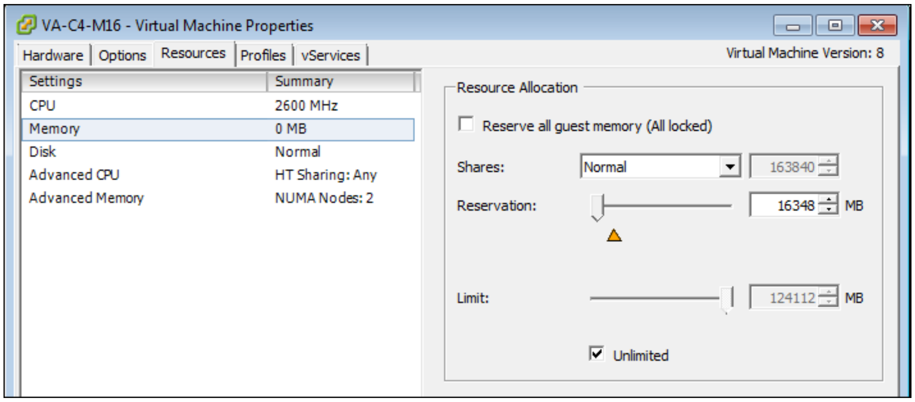
Limit: 10396 MHz

☑ Unlimited

⚠ Limit based on parent resource pool or current host

   d. Specify the **Reservation** value for the CPU that you determined in Step 1e. Ensure this value is larger than the minimum specified in "Verify System Requirements" on page 15 ; for example, change the **Reservation** value to 5200 MHz.
      Retain the default values for the other options.
3. Specify the memory reservation for the SWG VA.

a. On the **Resources** tab, select **Memory.**



VA-C4-M16 - Virtual Machine Properties

Virtual Machine Version: 8

Settings	Summary
CPU	2600 MHz
Memory	0 MB
Disk	Normal
Advanced CPU	HT Sharing: Any
Advanced Memory	NUMA Nodes: 2

Resource Allocation

□ Reserve all guest memory (All locked)

Shares: Normal 163840

Reservation: 16348 MB

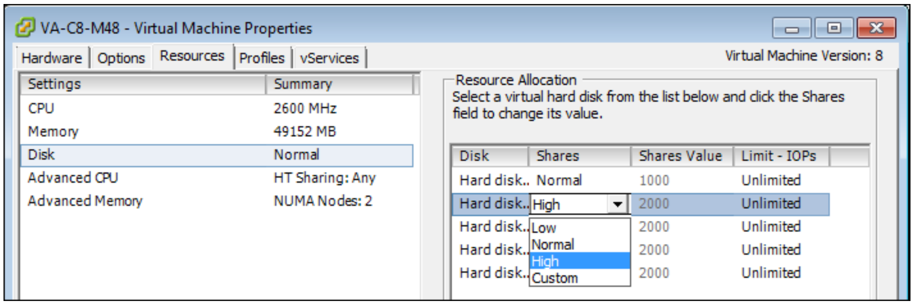
Limit: 124112 MB

☑ Unlimited

b. Specify the **Reservation** value for memory allotted to the SWG VA. Input the value for Virtual Memory recommended for your SWG VA model; see Table 2–2, "Model-Specific Requirements" on page 16. Retain the default values for the other options.

4. Recommended if the SWG VA's datastore is shared by other virtual machines on the vSphere Hypervisor Server:
Give the virtual disks on the SWG VA a higher priority access to the physical disks on the vSphere Hypervisor Server.

a. On the **Resources** tab, select **Disk**.



VA-C8-M48 - Virtual Machine Properties

Virtual Machine Version: 8

Settings	Summary
CPU	2600 MHz
Memory	49152 MB
Disk	Normal
Advanced CPU	HT Sharing: Any
Advanced Memory	NUMA Nodes: 2

Resource Allocation

Select a virtual hard disk from the list below and click the Shares field to change its value.

Disk	Shares	Shares Value	Limit - IOPs
Hard disk..	Normal	1000	Unlimited
Hard disk..	High	2000	Unlimited
Hard disk..	Low	2000	Unlimited
Hard disk..	Normal	2000	Unlimited
Hard disk..	High Custom	2000	Unlimited

b. For each virtual drive, change the value to **High** in the **Shares** field. Setting this value to high ensures that the SWG VA gains higher priority access to disk resources, as compared to other virtual machines that use the same physical disks.

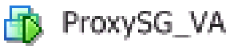
5. Click **OK** to save your settings.

For additional settings you may want to modify, see "Optional Settings for Optimal Performance" on page 56.

Section 4 Power on the SWG VA

To power on the SWG VA:

1. Log in to the vSphere Hypervisor Server using your VMware client.
2. Select the SWG VA.
3. Right click and select **Power > Power On**.
   When the SWG VA is powered on, a green arrow appears next to its virtual machine name.



ProxySG_VA

Chapter 4: Configure the SWG Virtual Appliance

This chapter describes how to perform the initial setup and configuration of the Secure Web Gateway Virtual Appliance (SWG VA) for transparent redirection of traffic. The following topics are covered in this chapter:

- "Prepare for Initial Configuration" on page 34
- "Complete Initial Configuration" on page 35
- "Verify Your Configuration" on page 39
- "Retrieve and Install the SWG VA License" on page 40
- "When to Power Off the SWG VA" on page 42
- "Monitor the SWG VA" on page 43
- "Additional References" on page 45

Note: The instructions in this chapter are for vSphere Client version 5.5.

Section 1 Prepare for Initial Configuration

Use the **Console** tab on your VMware client to access the SWG VA for initial configuration. The setup script prompts you to configure basic network settings, including adding an interface IP address and setting up administrative credentials for console access.

The following table summarizes the prompts in the setup wizard. Before you launch the setup wizard, obtain and record the information specific to your deployment in this table. After you have recorded your settings in the table, see "Complete Initial Configuration" on page 35.

Description	Value	My Values
Appliance Serial Number	Refer to the appliance serial number that you recorded in "Retrieve Appliance Serial Numbers" on page 19.	
Manual setup or use Director	If using Director, you must configure a registration password or *shared secret* on the Director. The same password must be entered while performing the initial configuration. The shared secret is required because the SWG VA does not have an appliance certificate at this point. **Note:** When you install a license from MySymantec, an appliance certificate is also installed. After you install the license, you can change your configuration to use Director subjugation. The appliance certificate is used instead of the shared secret when subjugating with Director.	
Interface configuration	Identify the IP addresses and subnet masks for the interfaces. You also have an option to assign a VLAN ID to each interface. If you use VLANs for segregating traffic within the vSphere Hypervisor Server or across your network, you must enable VLAN trunking on all interconnecting devices such as switches or routers. This guide does not include information on VLAN configurations.	
Default gateway	Provide the IP address for the default gateway.	
Primary DNS server	Provide the IP address for the primary DNS server.	
Administrator username (ID) and password	The password you assign here will also be used for accessing enable mode in the command line interface (CLI). Enable mode allows you to make configuration changes. The default enable username is *admin*.	

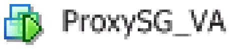
Section 2 Complete Initial Configuration

Complete initial configuration of the SWG VA:

1. Verify that your SWG VA is powered on.

   a. Log in to the vSphere Hypervisor Server using your VMware client.

   b. Check for power on status. If the SWG VA is powered on, a green arrow appears next to its virtual machine name.



ProxySG_VA

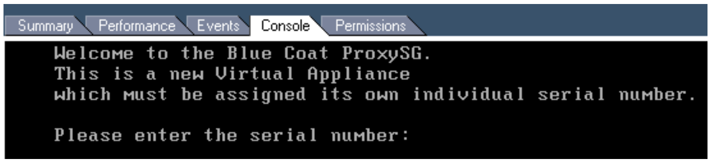
2. Access the virtual console of the SWG VA on the vSphere Hypervisor Server.

   a. Select the SWG VA on the vSphere Hypervisor Server.

   b. Select the **Console** tab and click inside the console window to activate your mouse.

3. The appliance serial number is unique for each appliance and must be used on only one SWG VA. For more information, see "Retrieve Appliance Serial Numbers" on page 19.

   a. Enter the appliance serial number at the prompt.



```
Welcome to the Blue Coat ProxySG.
This is a new Virtual Appliance
which must be assigned its own individual serial number.

Please enter the serial number:
```

Note: The leading zeros are significant for serial numbers. Enter all 10 digits at the prompt.

   b. Press Enter.

4. Follow the prompts and enter the details in the setup script.

   a. Press Enter three times to activate the serial console.

Note: To release the mouse from the VMware client's ***Console*** tab, press Ctrl+Alt.

   b. When asked **How do you plan to configure this appliance?** specify your preference for either configuring the SWG VA manually or using Director.
   If you are using Director, assign a registration password on Director and enter the password in the setup console when prompted. For information on setting up a registration password, refer to the *Symantec Director Configuration and Management Guide*.

   c. At the **Enter interface number to configure** prompt, specify an interface.

d. You are prompted **Is the IP address to be configured on a non-native VLAN?** Specify **Y** or **N**.
Note that if you use VLANs for segregating traffic within the vSphere Hypervisor Server or across your network, you must enable VLAN trunking on all interconnecting devices such as switches or routers. This guide does not include information on VLAN configurations.

e. Specify the IP address and subnet mask for the selected interface.

f. Specify the IP address for the default gateway.

g. Specify the IP address for the DNS server.

h. Change the username for administrative access on the SWG VA. The default username is *admin*.

i. Add a password for allowing administrative access privilege.

j. When prompted, enter your Enable password.

k. At the **Do you want to secure the serial port?** prompt, specify **Y** or **N**.

l. When asked **Restrict access to authorized workstations?** specify **Y** or **N** to indicate whether you allow non-authorized workstations to access the Management Console.

5. Press Enter three times to activate the serial console.
6. (If necessary) Repeat the previous steps to configure more interfaces.
7. Close the Console:

a. Press Ctrl+Alt to release the mouse from the Console.

b. Click an area outside of the Console tab.

Section 3 Deploying the SWG VA in a Proxy Chain

If you have a forward proxy deployment where the SWG VA is installed as the downstream proxy and cannot connect directly to the following Symantec servers, you must configure the SWG VA to forward this traffic to an upstream proxy that has access to the Symantec servers:

- https://download.bluecoat.com
- https://services.bluecoat.com
- https://validation.es.bluecoat.com
- https://subscription.es.bluecoat.com

To allow the SWG VA to communicate with Symantec servers, create an HTTP forwarding host on the SWG VA and ensure that `download-via-forwarding` is enabled (it is enabled by default). You can add the host to the default forwarding sequence, but if you do not want to forward all traffic through the default sequence, you must install policy to allow forwarding to Symantec servers.

Note: If you have this type of deployment and do not perform these steps, the SWG VA will be unable to connect to the server and the license may be suspended.

To configure the SWG VA:

1. Select the SWG VA on the vSphere Hypervisor Server.
2. To access the virtual console, select the **Console** tab and click inside the console window to activate your mouse.
3. Press Enter three times to activate the serial console.
4. Select the CLI option and enter your credentials.
5. Enter `enable` to go into Enable mode, and then enter your Enable password when prompted.
6. Enter the following bolded commands:

Note: If you do not want to forward all client HTTP requests to the hosts specified in the sequence, do not enter the `default-sequence add <host_alias>` command shown below. Instead, you will configure policy to use the forwarding host. For more information on forwarding and proxy chaining, refer to the *SGOS Administration Guide.*

```
#conf t
Enter configuration commands, one per line.  End with CTRL-Z.
#(config)forwarding
#(config forwarding)create host <host_alias> <host_name> http proxy
  ok
#(config forwarding)default-sequence add <host_alias>
  ok
```

```
#(config forwarding)download-via-forwarding enable
  ok
```

In the commands above:

- *<host_alias>* is a name that you specify for this host
- *<host_name>* is the name of the host domain, such www.mysite.com, or its IP address

7. Close the Console:

   a. Press Ctrl+Alt to release the mouse from the Console.

   b. Click an area outside of the Console tab.

8. (If necessary) If you did not add the host to the default forwarding sequence, install the following policy:

```
<Forward>
     condition=bluecoat_services forward(<host_alias>)

define url.domain condition bluecoat_services
     validation.es.bluecoat.com
     services.bluecoat.com
     download.bluecoat.com
     subscription.es.bluecoat.com
end
```

In the policy above, *<host_alias>* is the forwarding host you configured in the CLI.

Section 4 Verify Your Configuration

Do the following to verify your configuration.

Verify Network Connectivity

To verify that the traffic in your network is being intercepted as required, use the `ping`, `traceroute` or `test` CLI command. See the *SGOS Command Line Interface Reference* for more information.

Verify Management Console Access

The Management Console is a graphical web interface that allows you to manage, configure and monitor the SWG VA. The Management Console requires a supported browser and version of Java Runtime Environment (JRE). To identify the browsers and JRE version supported for your operating system, refer to the following article:

http://www.symantec.com/docs/TECH245893

To log in to the Management Console:

1. In a web browser, go to the following URL:

   ```
   https://<IP_address>:8082
   ```

   The default management port is 8082.
   `<IP_address>` is the IP address you configured in "Complete Initial Configuration" on page 35.

   Note: When you enter the URL for the Management Console, the browser may display an error about an untrusted connection or security certificate. Depending on the browser you use, you must proceed with the connection to access the Management Console or add an exception to allow access to the web site. For specific instructions, refer to the documentation for the browser.

2. In the prompt that appears, enter the user name and password that you created in "Complete Initial Configuration" on page 35. The Management Console displays.

Section 5 Retrieve and Install the SWG VA License

To retrieve and install the SWG VA license for the first time, the SWG VA appliance must be allowed access to the following Symantec servers:

- https://download.bluecoat.com
- https://services.bluecoat.com

> **Note:** If the SWG VA is a downstream proxy and cannot access these servers directly, make sure you have performed the additional configuration steps in "Upgrade and Downgrade Considerations" on page 53 before completing the procedure below.

The SWG VA license contains data that is used to uniquely identify the SWG VA as a Blue Coat appliance.

> **Note:** If a license is not installed, after you power on the appliance, users who open a browser window will see an exception page indicating that the device is not licensed.

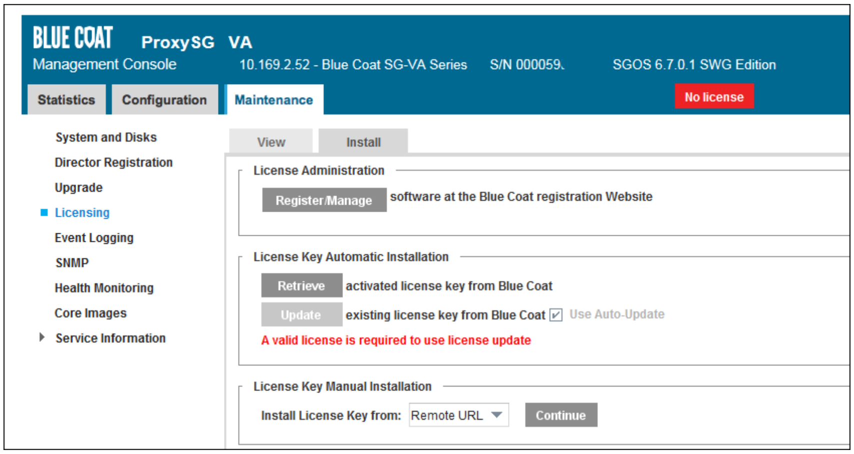
Before you begin:

- Set up DNS; see "Configuring DNS" in the *SGOS Administration Guide.*
- Confirm NTP is working, or add local NTP servers, and verify the system time is correct; see "Accessing the Appliance" in the *SGOS Administration Guide.*

> **Note:** If you have blocked the Symantec NTP servers, add a local server.

Retrieve and install the SWG VA license:

1. In the Management Console, select **Maintenance** > **Licensing** > **Install**.



10.169.2.52 - Blue Coat SG-VA Series S/N 000059. SGOS 6.7.0.1 SWG Edition

Register/Manage software at the Blue Coat registration Website

Retrieve activated license key from Blue Coat

Update existing license key from Blue Coat

A valid license is required to use license update

Install License Key from: Remote URL

2. Click **Retrieve**.

3. In the dialog that opens:
    a. Enter your MySymantec account login information.
    b. Click **Request License**. The Confirm License Install dialog opens.
    c. Click **OK** to begin license retrieval.
4. (Optional) Click **Show results** to verify a successful retrieval. If any errors occur, verify that you are connected to the Internet.
5. Click **Close**.

After you complete the license installation, you do not have to reboot or shut down the appliance.

Note: The Symantec WebFilter (formerly BCWF) license is not included with the high-performance models of SWG VA and must be purchased separately.

Prevent Licensing Issues

To prevent licensing issues, ensure the SWG VA is allowed network access to the license validation server at https://validation.es.bluecoat.com. If communication with the server fails, the license may be suspended; thus, a constant Internet connection is required for the SWG VA to communicate regularly with the license validation server to confirm that the serial number is not being used on another SWG VA.

If the license validation server detects duplicate serial numbers, your license is invalidated. See “Serial Numbers and Licensing” on page 50 for more information.

If the SWG VA license expires, the appliance stops processing requests. In explicit deployments, traffic to intercepted services is denied. For details on license expiration behavior, refer to the “Licensing” chapter in the *SGOS Administration Guide*.

If the configured CPU count exceeds the limit in your license, the license is suspended.

Section 6 When to Power Off the SWG VA

Some tasks that you perform on the SWG VA require a shutdown. When you do any of the following, save all of your configuration changes and then power off the SWG VA:

- Backing up the SGOS configuration
- Upgrading the server software
- Taking the server offline for maintenance
- Migrating the SWG VA to a different server
- Installing additional or higher-capacity drives on the vSphere Hypervisor host
- Adding a serial port to the SWG VA

Powering off the SWG VA

To power off the SWG VA, in the command line interface (CLI), enter the enable password to go into privileged mode. Then, issue the `shutdown` command.

Alternatively, you can power off the SWG VA in the VMWare client:

1. In the VMWare client, select the SWG VA.
2. Right click and select **Power > Power Off**.

Note: Symantec recommends that you use the `shutdown` command instead of powering off the SWG VA using the vSphere client to avoid losing recent configuration changes.

Section 7 Monitor the SWG VA

It is important to keep tabs on the health of your SWG VA. If a component does not function correctly, learning of it in a timely manner allows you to take action before it fails or causes other problems.

The SWG VA monitors the health of a variety of components and determines the state of each component at one-minute intervals. The state indicates the condition of the monitored component:

- **OK**—The monitored component is behaving within normal operating parameters.
- **WARNING**—The monitored component is outside typical operating parameters and may require attention.
- **CRITICAL**—The monitored component is failing or has exceeded its critical threshold.

The health state displays at the top right corner of the Management Console and in the **State** field on the health monitoring licensing page (**Statistics** > **Health Monitoring** > **Licensing**).

The current state of a component is determined by the relationship between its current value and its monitoring thresholds. The **Warning** and **Critical** states have thresholds associated with them.

Each component's health state begins at **OK**. If the value exceeds the **Warning** threshold and remains there for the threshold's specified interval, the component's health transitions to the **Warning** state and the SWG VA issues a warning alert.

When a component is in the **Warning** state and the **Critical** threshold is exceeded for the specified interval, the component health transitions to the **Critical** state and an error alert is issued.

If the problem is resolved, the value returns below the **Warning** threshold. If the value stays below the **Warning** threshold longer than the specified interval, the state returns to **OK**.

To edit the thresholds, click **Set Thresholds** at the bottom of the **Maintenance** > **Health Monitoring** tab. For more information on thresholds, see the *SGOS Administration Guide*.

License Monitoring for the SWG VA

If there is a problem with the SWG VA license, the health state displays **Warning** or **Critical**.

Several metrics on the **Maintenance** > **Health Monitoring** tab can help you determine if there is a licensing issue and what you can do to resolve it. These metrics are specific to the SWG VA:

- **License Server Communication Status**—Monitors the connection to the license validation server.

If the connection to the license validation server is lost, the **State** field (**Statistics** > **Health Monitoring** > **Licensing**) displays the health state and the **Value** field displays the number of days remaining until the license is suspended. The health state depends on the threshold that is set:

- **Warning**—Default interval is six days before license suspension.
- **Critical**—Default interval is 0 days before license suspension.

If there is an error with the communication status, re-establish connection to the license validation server. The state returns to **OK** if connection is successful. If you do not re-establish the connection within seven days, the SWG VA license is suspended. The SWG VA must communicate successfully with the license validation server to restore proxy functionality.

❒ **License Validation Status**—Monitors the validity of the SWG VA license, ensuring no duplicate serial numbers are in use.

If the license validation server detects a duplicate serial number, the **State** field (**Statistics** > **Health Monitoring** > **Licensing**) displays the health state and the **Value** field displays the number of days remaining until the license is suspended. The health state depends on the threshold that is set:

- **Warning**—Default interval is 30 days before license suspension.
- **Critical**—Default interval is 0 days before license suspension.

If the license validation server detects a duplicate license and the license is not disabled before the grace period expires, the license is suspended. You must delete the SWG VA with the duplicate license to restore proxy functionality.

❒ **Configured CPU Count**— The number of configured CPUs on the virtual appliance is compared to the number available on the license. For example, if the SWG VA is licensed for eight CPUs and only six are configured, the appliance has under-provisioned CPUs. Or if the SWG VA is licensed for two CPUs and three are configured, the appliance has over-provisioned CPUs. Use the `show license` CLI command to see the maximum CPU count in your license.

- **Warning**: The SWG VA has under-provisioned CPUs and is not taking advantage of all CPUs included with the license.
- **Critical**: The SWG VA has over-provisioned CPUs and exceeds the licensed maximum limit. The license is suspended until you reduce the configured CPU count or install a different license that has a higher CPU count.

❒ **Configured Memory**— The amount of configured virtual memory is compared to the amount allowed by the license. For example, if the SWG VA is licensed for 32 GB of virtual memory and is configured for 24 GB, the appliance has under-provisioned memory.

- **Warning**: The SWG VA has under-provisioned memory and is not taking advantage of all virtual memory included with the license. To reprovision memory, edit the hardware settings for the SWG VA.

Section 8 Additional References

You have completed configuring and verifying your initial configuration on the SWG VA. For further information, use the context-sensitive online help in the Management Console. You can also refer to the latest version of the following documents at:

https://support.symantec.com/us/en/documentation.1145522.2116810.html

- *SGOS Administration Guide* for complete product documentation on SGOS
- *Command Line Interface Reference* for documentation on SGOS CLI commands

Appendix A: Supplemental Information

This appendix answers some questions you may have about the following topics and the SWG VA:

- "Features" on page 48
- "Serial Numbers and Licensing" on page 50
- "Upgrade and Downgrade Considerations" on page 53
- "Throughput Requirements Per Virtual Disk" on page 55
- "Optional Settings for Optimal Performance" on page 56

Section 1 Features

This section covers the following topics:

- "How do features vary between the various ProxySG editions and licenses?" on page 48
- "Can I manage SWG VA using Sky UI?" on page 49

How do features vary between the various ProxySG editions and licenses?

The table below shows a high-level comparison of features available in the full Proxy Edition appliance, Blue Coat ProxySG VA MACH5 Edition, SWG VA, and high-performance SWG VA.

Table A-1

Feature	Proxy Edition	ProxySG VA MACH5 Edition	SWG VA	High-Performance SWG VA
Authentication	Full	LDAP and IWA used for the Symantec Web Security Service	Full	Full
Web Filtering (Symantec WebFilter)	Yes	No	Yes	Yes
SSL Proxy	Yes	Yes	Yes	Yes
HTTP Proxy	Yes	Yes	Yes	Yes
HTTPS Reverse Proxy	Yes	No	Yes	Yes
CIFS Proxy	Yes	Yes	No	No
MAPI Proxy	Yes	Yes	Yes	Yes
Streaming Proxy	Yes	Yes	Yes	Yes
ICAP Support	Yes	No	Yes	Yes
Object Caching	Yes	Yes	Yes	Yes
Video Caching	Yes	Yes	Yes	Yes
Byte Caching	Yes	Yes	No	No

Table A-1

Feature	Proxy Edition	ProxySG VA MACH5 Edition	SWG VA	High-Performance SWG VA
Central Management	Director, Management Center	Director, Management Center	Director, Management Center	Director, Management Center
Reporting	Reporter, Web Security Service, Management Center	Reporter, Web Security Service, Management Center	Reporter, Web Security Service, Management Center	Reporter, Web Security Service, Management Center
ProxyClient Management	Full	Acceleration only	Security only	Security only
Client Manager for Unified Agents	Yes	No	Yes	Yes

Can I manage SWG VA using Sky UI?

The Sky UI and its features are not available in the SWG VA.

Section 2 Serial Numbers and Licensing

This section covers the following topics about serial numbers and licensing:

How can I prevent duplicate serial numbers?

Do not reuse serial numbers.

The SWG VA periodically connects to the license validation server to confirm that the license is still valid. If the license validation server detects a duplicate serial number, the SWG VA displays a warning beside **License Validation Status** on the **Health Monitoring** tab (**Maintenance** > **Health Monitoring**). When the license is in this state, you have a specified number of days to determine which SWG VAs have duplicate serial numbers and then delete the duplicates (the default time window is 30 days). If you do not delete the duplicates within the specified time window, the license is suspended.

License suspension disables proxy functionality and the Management Console displays the **Duplicate serial number detected** error message. If you receive this error message, go to http://www.symantec.com/docs/TECH241266 and follow the steps in the article to resolve the issue.

Can I configure more CPUs than my license allows?

Your license specifies the maximum number of CPUs for your SWG VA. If you have configured more than the maximum, your license will be suspended. The SWG VA event log shows an error and the health monitoring alert shows **Critical**. See "Monitor the SWG VA" on page 43.

Why is my license suspended?

First, verify that you do not have duplicate serial numbers (see "How can I prevent duplicate serial numbers?") and that you have not exceeded the number of CPUs that your license allows (see "Can I configure more CPUs than my license allows?"). To determine the number of CPUs that your license allows, issue the `show license` CLI command.

If the license validation status still has a warning, the SWG VA might be unable to connect to the Internet.

If the SWG VA has not been able to contact the license validation server, the license will not be reactivated until connectivity to the Internet is restored. To fix this problem, troubleshoot network connection problems within your deployment.

If the SWG VA is a downstream proxy in a forward proxy deployment and cannot access Symantec websites directly, make sure that you have created and configured an HTTP forwarding host.

How do I renew my subscription for the SWG VA?

Your original Symantec eFulfillment email contains details about the subscription, including the Start Date and End Date for the subscription.

To renew your subscription for the SWG VA:

1. Contact NP_customercare@symantec.com.
2. After Customer Care renews your subscription, update the license key through the Management Console. See "How do I update the license key?" on page 52.
3. To verify that the subscription has been updated, click the **View** tab and confirm that the licensed components have new expiration dates.

Note: You cannot request a user limit upgrade and renew a subscription on a single order; the upgrade and renewal must be on separate orders.

How do I upgrade the connection limit for the SWG VA?

To increase the connection limit for your SWG VA, contact NP_customercare@symantec.com. After your order is processed, you will receive a Symantec eFulfillment email with the upgrade activation code. Then, log in to the Symantec Network Protection Licensing Portal to upgrade.

You will need the following information to upgrade:

- the serial number of the SWG VA that you want to upgrade
- the upgrade activation code that you received in your Symantec eFulfillment email

To upgrade the connection limit for the SWG VA:

1. Go to the Symantec Network Protection Licensing Portal:

   https://support.bluecoat.com/eservice_enu/licensing/register.cgi
2. Log in with your MySymantec username and password.
3. Select **ProxySG** > **SG Upgrades**.
4. In the **Appliance Serial Number** field, enter the serial number for the SWG VA that you want to upgrade.
5. In the **Activation Code** field, enter the upgrade activation code that you received in your Symantec eFulfillment email.
6. Click **Submit**.
7. Update the license file. Follow the instructions in "How do I update the license key?" on page 52.
8. Reboot the appliance to reset the connection limits.

9. To verify that the connection limit for the SWG VA has been upgraded, click the **View** tab and confirm that the number of concurrent users has increased.

Note: You cannot request a connection limit upgrade and renew a subscription on a single order; the upgrade and renewal must be on separate orders.

How do I update the license key?

Install the license key file through the SWG VA Management Console.

1. Launch the SWG VA Management Console.
2. Select **Maintenance > Licensing > Install**.
3. In the License Key Automatic Installation section, click **Update**. A Confirm License Install dialog opens.
4. Click **OK**.

Section 3 Upgrade and Downgrade Considerations

You can upgrade SGOS 6.7.x to a later version, but you *cannot* downgrade a SWG VA high-performance model to pre-6.7 SGOS versions.

Note: Upgrading a MACH5 VA or SWG V100 to SGOS 6.7 will not convert the VA to a high-performance model. You must purchase a new license to use a high-performance model.

Before you upgrade, note that:

- You must have a valid, unexpired license to upgrade your virtual appliance software. If your license has expired, you must renew your subscription with Symantec before you can upgrade the software.
- You do not require a VAP to upgrade SGOS on the VA; VAPs are used for initial configuration only. The upgrade process for a VA is the same as for a physical appliance. See the *ProxySG Upgrade/Downgrade WebGuide* for details.

Upgrade SGOS

Upgrading the SGOS version consists of associating the activation code with the existing serial number, and then rebooting the appliance to apply changes.

Use the procedure outlined in "Upgrade the VA Model" below, but skip steps 7 through 9 because they are needed only for VA model upgrades.

Upgrade the VA Model

Upgrading the VA model consists of associating the activation code with the serial number, updating the license file, and increasing CPU, memory, and number of disks as allowed by the new model (see "Model-Specific Requirements" on page 16). Use the following instructions after you order an upgrade from Symantec.

1. Go to the Symantec Network Protection Licensing Portal:

   https://support.bluecoat.com/eservice_enu/licensing/register.cgi

2. Log in with your MySymantec username and password.
3. Select **ProxySG** > **SG Upgrades**.
4. In the **Appliance Serial Number** field, enter the serial number for the SWG VA that you want to upgrade.
5. In the **Activation Code** field, enter the upgrade activation code that you received in your Symantec eFulfillment email.
6. Click **Submit**.
7. Update the license file to ensure that updating resources does not cause licensing errors. Follow the instructions in "How do I update the license key?" on page 52.
8. Reboot the appliance.

9. Follow the instructions in "Reserve Resources for the SWG VA" on page 29 to specify additional CPU cores, memory, and disks as allowed by the upgraded model. Note that over-provisioning CPUs can cause license suspension, but under-provisioning can cause sub-optimal VA performance and operation.

   See "Verify System Requirements" on page 15 for details.

10. Reboot the appliance.

11. Check the appliance health status. If you encounter health warnings or errors, see in "Serial Numbers and Licensing" on page 50. Alternatively, search for Symantec knowledge base articles:

    https://support.symantec.com/en_US/proxysg.html

Section 4 Throughput Requirements Per Virtual Disk

Although Symantec recommends each virtual disk be sized at 100GB, SWG VA models with higher storage requirements can have larger virtual drives. Be aware that throughput per virtual disk is inversely proportional to the number of drives. With fewer drives, more throughput is required per disk. Note that the throughput requirements are peak numbers for peak network throughput.

Table A–1 Throughput per 100GB Drive

Model	Number of Drives	Drive Size (GB)	Disk Read Throughput (Mbps)	Disk Write Throughput (Mbps)	Read Request Rate (IOPS)	Write Request Rate (IOPS)
SG-VA-C1	1	100	2.00	16.00	85.00	65.00
SG-VA-C2	1	100	5.00	30.00	135.00	125.00
SG-VA-C4	2	100	3.00	32.50	122.50	127.50
SG-VA-C8	4	100	2.75	31.25	117.50	122.50
SG-VA-C16	8	100	2.25	25.62	100.62	104.37

Table A–2 Throughput per 200GB Drive

Model	Number of Drives	Drive Size (GB)	Disk Read Throughput (Mbps)	Disk Write Throughput (Mbps)	Read Request Rate (IOPS)	Write Request Rate (IOPS)
SG-VA-C8	2	200	5.50	62.50	235.00	245.00
SG-VA-C16	4	200	4.50	51.25	201.25	208.75

Table A–3 Throughput per 400GB Drive

Model	Number of Drives	Drive Size (GB)	Disk Read Throughput (Mbps)	Disk Write Throughput (Mbps)	Read Request Rate (IOPS)	Write Request Rate (IOPS)
SG-VA-C16	2	400	9.00	102.50	402.50	417.50

Section 5 Optional Settings for Optimal Performance

In addition to the recommended settings described in "Reserve Resources for the SWG VA" on page 29, you may also want to consider the guidelines and settings described below.

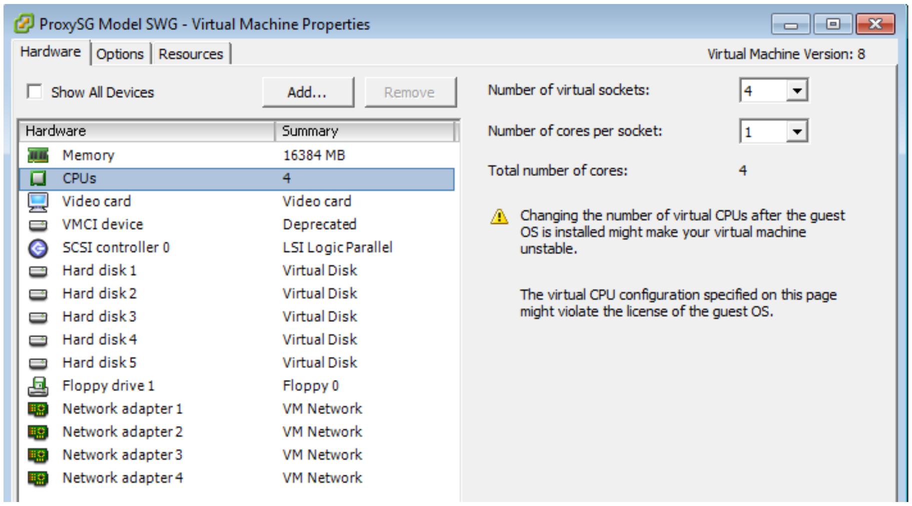
Guidelines for Optimal Performance

For optimal performance of the SWG VA, follow these guidelines:

- Configure each virtual disk on a separate physical disk.
- When you back up your system configuration, use the archiving feature in the SWG VA; do not take snapshots of the SWG VA configuration. Snapshots are detrimental to the performance of the SWG VA, and they also occupy a lot of disk space.
- Suspending the SWG VA suspends all traffic going through it. It may result in dropped connections, depending on when the suspension occurs and the protocols in use. Clients must reconnect when the SWG VA becomes available again; however, suspending and resuming traffic creates a poor performance experience for users.
- Refer to the *Sizing Guide* for hardware specifications, and ensure that your hardware meets or exceeds the guidelines for best performance.

Setting Number of CPU Sockets and Cores

If your virtual machine has multiple CPUs, Symantec recommends setting the **Number of virtual sockets** to the number of CPUs and the **Number of cores per socket** to 1. For example if your SWG VA has four CPUs:



ProxySG Model SWG - Virtual Machine Properties

Hardware	Summary
Memory	16384 MB
CPUs	4
Video card	Video card
VMCI device	Deprecated
SCSI controller 0	LSI Logic Parallel
Hard disk 1	Virtual Disk
Hard disk 2	Virtual Disk
Hard disk 3	Virtual Disk
Hard disk 4	Virtual Disk
Hard disk 5	Virtual Disk
Floppy drive 1	Floppy 0
Network adapter 1	VM Network
Network adapter 2	VM Network
Network adapter 3	VM Network
Network adapter 4	VM Network

Number of virtual sockets: 4

Number of cores per socket: 1

Total number of cores: 4

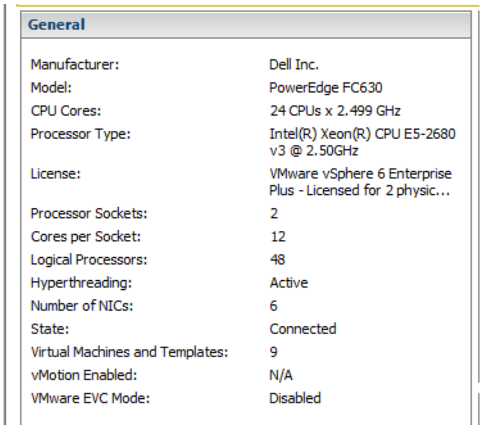
⚠ Changing the number of virtual CPUs after the guest OS is installed might make your virtual machine unstable.

The virtual CPU configuration specified on this page might violate the license of the guest OS.

Note: The following settings could negatively impact other virtual machines on your ESX server.

Setting Logical Processor Affinity and NUMA Memory Affinity

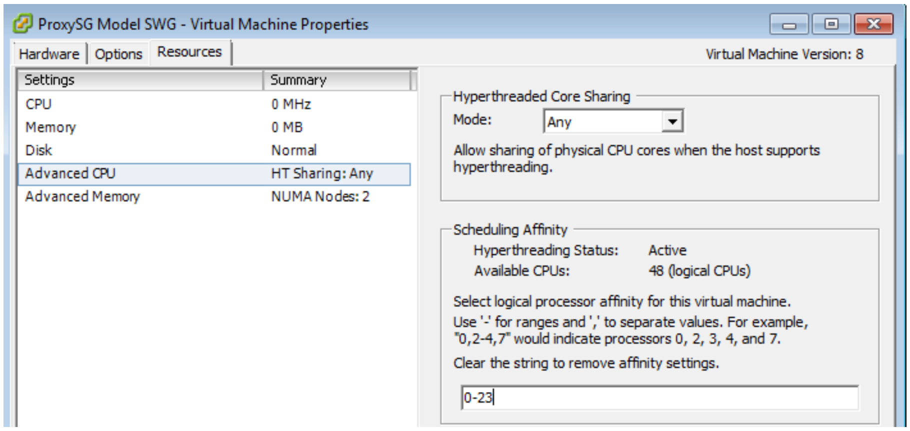
These settings are applicable if the virtual machine has multiple CPUs and the host has multiple processor sockets.



General

Manufacturer:	Dell Inc.
Model:	PowerEdge FC630
CPU Cores:	24 CPUs x 2.499 GHz
Processor Type:	Intel(R) Xeon(R) CPU E5-2680 v3 @ 2.50GHz
License:	VMware vSphere 6 Enterprise Plus - Licensed for 2 physic...
Processor Sockets:	2
Cores per Socket:	12
Logical Processors:	48
Hyperthreading:	Active
Number of NICs:	6
State:	Connected
Virtual Machines and Templates:	9
vMotion Enabled:	N/A
VMware EVC Mode:	Disabled

Set the CPU Scheduling Affinity to the logical processors on the same CPU. For example, if the host has 24 processors per socket, the scheduling affinity is set to any of the 24 logical processors on CPU0.



ProxySG Model SWG - Virtual Machine Properties

Hardware | Options | Resources — Virtual Machine Version: 8

Settings	Summary
CPU	0 MHz
Memory	0 MB
Disk	Normal
Advanced CPU	HT Sharing: Any
Advanced Memory	NUMA Nodes: 2

Hyperthreaded Core Sharing

Mode: Any

Allow sharing of physical CPU cores when the host supports hyperthreading.

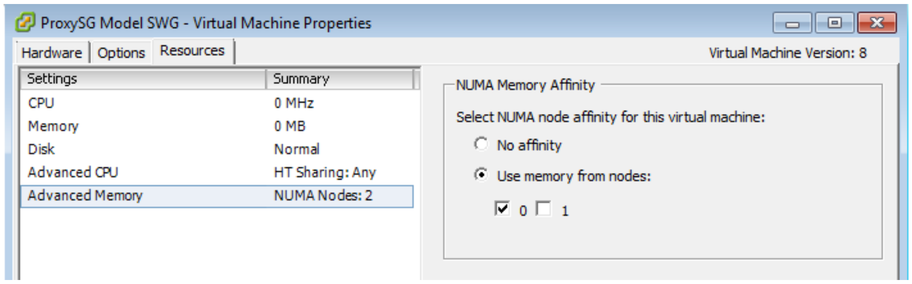
Scheduling Affinity

Hyperthreading Status: Active
Available CPUs: 48 (logical CPUs)

Select logical processor affinity for this virtual machine.
Use '-' for ranges and ',' to separate values. For example, "0,2-4,7" would indicate processors 0, 2, 3, 4, and 7.
Clear the string to remove affinity settings.

0-23

The NUMA Memory Affinity should be set to use memory from Node 0.



ProxySG Model SWG - Virtual Machine Properties

Hardware | Options | Resources — Virtual Machine Version: 8

Settings	Summary
CPU	0 MHz
Memory	0 MB
Disk	Normal
Advanced CPU	HT Sharing: Any
Advanced Memory	NUMA Nodes: 2

NUMA Memory Affinity

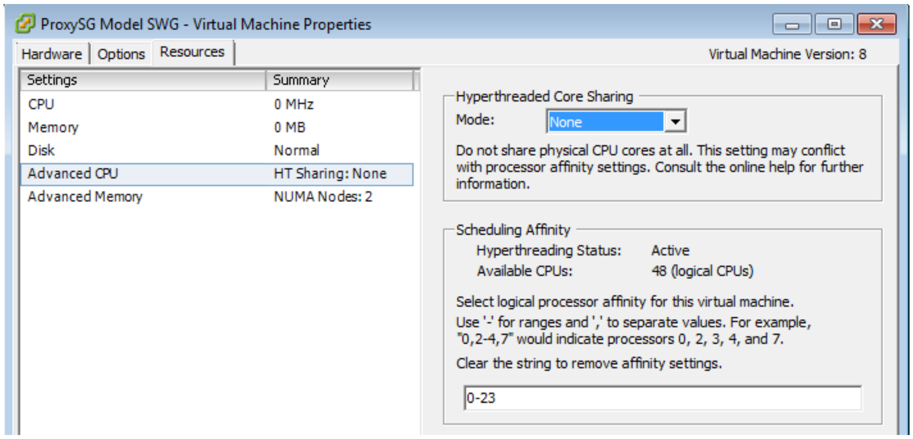
Select NUMA node affinity for this virtual machine:

○ No affinity
● Use memory from nodes:

☑ 0 □ 1

Disabling Hyperthreaded Core Sharing

When the virtual machine is expected to handle network throughput of 1 Gbps or more and hyperthreading controls are exposed by the hypervisor, Symantec recommends disabling hyperthreaded core sharing for maximum performance.


ProxySG Model SWG - Virtual Machine Properties
Hardware
Options
Resources
Virtual Machine Version: 8

Settings	Summary
CPU	0 MHz
Memory	0 MB
Disk	Normal
Advanced CPU	HT Sharing: None
Advanced Memory	NUMA Nodes: 2

Hyperthreaded Core Sharing

Mode: None

Do not share physical CPU cores at all. This setting may conflict with processor affinity settings. Consult the online help for further information.

Scheduling Affinity

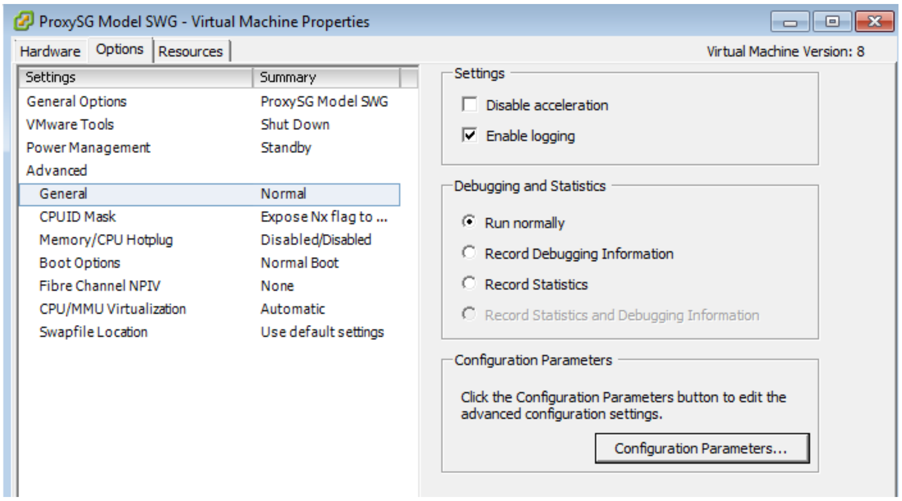
Hyperthreading Status: Active
Available CPUs: 48 (logical CPUs)

Select logical processor affinity for this virtual machine.
Use '-' for ranges and ',' to separate values. For example, "0,2-4,7" would indicate processors 0, 2, 3, 4, and 7.
Clear the string to remove affinity settings.

0-23

Setting Latency Sensitivity

To set latency sensitivity, click the **Configuration Parameters** button.


ProxySG Model SWG - Virtual Machine Properties
Hardware
Options
Resources
Virtual Machine Version: 8
Configuration Parameters...

Settings	Summary
General Options	ProxySG Model SWG
VMware Tools	Shut Down
Power Management	Standby
Advanced	
General	Normal
CPUID Mask	Expose Nx flag to ...
Memory/CPU Hotplug	Disabled/Disabled
Boot Options	Normal Boot
Fibre Channel NPIV	None
CPU/MMU Virtualization	Automatic
Swapfile Location	Use default settings

Settings

□ Disable acceleration

☑ Enable logging

Debugging and Statistics

● Run normally

○ Record Debugging Information

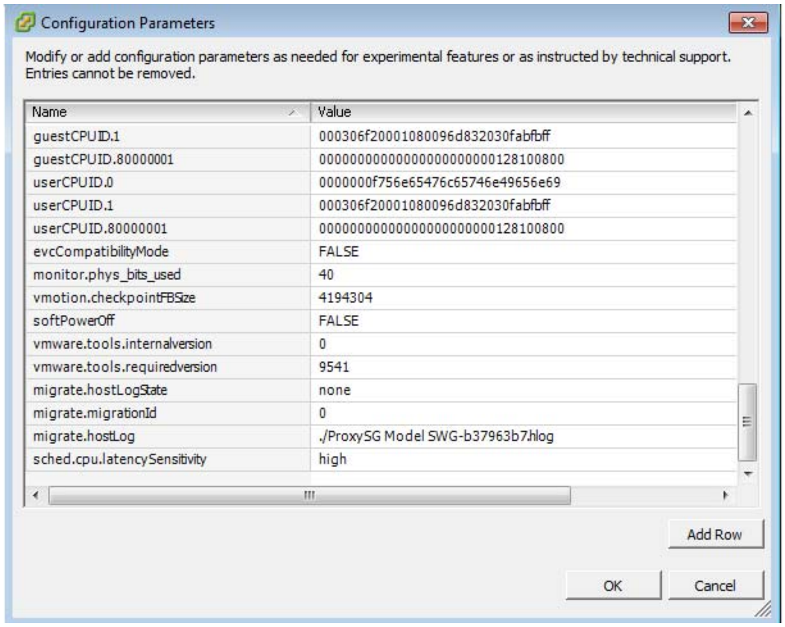
○ Record Statistics

○ Record Statistics and Debugging Information

Configuration Parameters

Click the Configuration Parameters button to edit the advanced configuration settings.

Add a parameter with the **Name** *sched.cpu.latencySensitivity* and **Value** *high*.



Modify or add configuration parameters as needed for experimental features or as instructed by technical support. Entries cannot be removed.

Name	Value
guestCPUID.1	000306f20001080096d832030fabfbff
guestCPUID.80000001	00000000000000000000000128100800
userCPUID.0	0000000f756e65476c65746e49656e69
userCPUID.1	000306f20001080096d832030fabfbff
userCPUID.80000001	00000000000000000000000128100800
evcCompatibilityMode	FALSE
monitor.phys_bits_used	40
vmotion.checkpointFBSize	4194304
softPowerOff	FALSE
vmware.tools.internalversion	0
vmware.tools.requiredversion	9541
migrate.hostLogState	none
migrate.migrationId	0
migrate.hostLog	./ProxySG Model SWG-b37963b7.hlog
sched.cpu.latencySensitivity	high