# SonicWall<sup>®</sup> NS $_{v}$ Series on ESXi

**Getting Started Guide** 



## Contents

Introducing NSv Series
Feature Support Information 4
Node Counts Per Platform
Installation File / Supported Platforms
Hardware Compatibility
Product Matrix and Requirements
Backup and Recovery Information
Best Practices and Recommendations
High Availability Configurations
Exporting and Importing Firewall Configurations
Upgrading to a Higher Capacity NSv Model
Creating a MySonicWall Account
Installing NSv Series on ESXi
Obtaining the OVA from MySonicWall
Installing the NSv Appliance
Viewing and Editing Virtual Machine Settings
Troubleshooting Installation Configuration
Licensing and Registering Your NSv25
Registering the NSv Appliance from SonicOS 25
Registering with Zero-Touch Deployment
Deploying from CSC Management
Getting the Latest Firmware for the NSv
Deploying from GMS On-Premises
Getting the Latest Firmware for the NSv
Registering an NSv Manually in a Closed Network 29
Deregistering Your NSv
Converting a Free Trial License to Full License
SonicOS Management
Managing SonicOS on the NSv Series
Using SonicOS on an Unregistered NSv
Using System Diagnostics in SonicOS
Check Network Settings
Using the Virtual Console
Using the ESXi Remote Console to Configure the WAN or LAN Interfaces
Using the NSv Management Console
System Info
Management Network
Test Management Network 45
Diagnostics
NTP Server

SonicWall NSv Series ESXi Getting Started Guide Contents

Lockdown Mode
Reboot   Shutdown
About
Logs
Using SafeMode on the NSv
Enabling SafeMode
Disabling SafeMode
Configuring the Management Network in SafeMode53
Installing a New SonicOS Version in SafeMode56
Downloading Logs in SafeMode57
Control Mall Company
Sonicwall Support
About This Document

# Introducing NS<sub>v</sub> Series

1

This *SonicWall® NSv Series on ESXi Getting Started Guide* describes how to install SonicWall NSv on VMware ESXi and provides basic configuration information.

The SonicWall<sup>®</sup> Network Security Virtual Series (SonicWall<sup>®</sup> NSv Series) is SonicWall's virtualized next-generation firewall appliance that provides Deep Packet Inspection (DPI) security and segmentation in virtual environments. With some platform specific differences, SonicOS running on the NSv Series ESXi offers the same feature functionality and security features of a physical appliance, with comparable performance. SonicOS Virtual is a fully featured 64-bit SonicOS powered by SonicCore.

#### **Topics:**

- Feature Support Information on page 4
- Node Counts Per Platform on page 6
- Installation File / Supported Platforms on page 6
- Product Matrix and Requirements on page 7
- Backup and Recovery Information on page 8
- Best Practices and Recommendations on page 8
- High Availability Configurations on page 8
- Exporting and Importing Firewall Configurations on page 9
- Upgrading to a Higher Capacity NSv Model on page 9
- Creating a MySonicWall Account on page 10

# Feature Support Information

The SonicWall NSv Series for VMware ESXi has nearly all the features and functionality of a SonicWall NSa hardware appliance running SonicOS 6.5.4 firmware.

SonicWall GMS 8.7 and higher versions are supported for management of SonicWall NSv Series virtual appliances running 6.5.4.v. GMS 8.4 can manage NSv Series running 6.5.0.v.

For information about supported features, refer to the *SonicOS 6.5 NSv* administration documentation. This and other documents for the SonicWall NSv Series are available when you select **NS**v Series ESXi as the **Product** at: https://www.sonicwall.com/support/technical-documentation. The Key Feature Support of NSv for ESXi table lists the key SonicOS features and whether they are supported or unsupported on deployments of the NSv for ESXi.

#### **Feature Support List**

Component	Feature	Status
Network Interfaces	Override MAC Address	Not supported
Network Interfaces	DHCPv6 Prefix Delegation (PD)	Not supported

#### **Feature Support List**

Component	Feature	Status
Network Interfaces	IPv6 Management	Supported
Network Interfaces	6rd	Not supported
Network	Portshield Groups	Not supported
Network Interfaces	L2 Bridge Mode	Not supported
Network Interfaces	Native Bridge	Not supported
Network Interfaces	Wire Mode v4	Supported
Network Interfaces	Wire Mode v6	Supported
Network Interfaces	PPPoE	Not supported
Network Interfaces	РРТР	Not supported
Network Interfaces	L2TP	Not supported
Network Interfaces	Tap Mode	Not supported
Network Interfaces	Link Aggregation	Not supported
Network Interfaces	Port Redundancy	Not supported
Network Interfaces	IP Unnumbered	Not supported
Network Interfaces	VLAN Translation	Supported
Network Interfaces	Users IPv6	Supported
Network Interfaces	DHCP Servers	Supported
Network Interfaces	VLAN Interfaces	Supported
Network Interfaces	Jumbo Frames	Supported
Network Interface	SDWAN	Supported
Firewall Settings	Zero Touch	Supported
Firewall Settings	QoS Mapping	Supported
Firewall Settings	Multicast	Supported
High Availability	Active/Passive	Supported
High Availability	Active-Active DPI	Not supported
High Availability	Stateful Sync	Supported
		Virtual MAC not supported.
		Dynamic ARP entries not supported.
Switching		Not supported
3G/4G Modem		Not supported
Wireless		Not supported
SonicPoints		Not supported
SSL VPN	SSL VPN for IPv6	Supported
Virtual Assist		Not supported
WAN Acceleration		Not supported
VoIP	H.323	Supported
VoIP	SIP	Supported

# Node Counts Per Platform

The supported node count varies by NSv platform. This is the maximum number of nodes/users that can connect to the NSv at any one time, and is displayed on the **System Status** page in the **MONITOR** view. The **Maximum Node Counts Per Platform** table shows this information.

#### **Maximum Node Counts Per Platform**

Platform	Maximum Node Count
NSv 10	10
NSv 25	25
NSv 50	50
NSv 100	100
NSv 200 and higher	Unlimited

Node counts are calculated by SonicOS as follows:

- Each unique IP address is counted.
- Only flow to the WAN side is counted.
- GVC and SSL VPN connections terminated to the WAN side are counted.
- Internal zone to zone is not counted.
- Guest users are not counted.

A log event is generated when the node count exceeds the limit.

# Installation File / Supported Platforms

Release Version	Supported Hypervisor Versions
SonicOS 6.5 for NSv Series ESXi	ESXi 5.5 or higher <sup>1</sup>

1. ESXi 6.5 or higher is recommended for production environments. The ESXi vswitch configuration should have the **MAC address changes** option enabled.

### Hardware Compatibility

SonicWall NSv Series is supported on ESXi running on relatively modern chipsets, Intel Penryn and above (2008). If the chipset is too old, the installation will halt with the message, "This system does not support SSE4\_1." For more information, see https://kb.vmware.com/s/article/1005764.

# **Product Matrix and Requirements**

The following tables show the hardware resource requirements for the SonicWall NSv Series virtual appliances.

#### NSv Series Resource Requirements

Product Models	NSv 10	NSv 25	NSv 50	NSv 100
Maximum Cores <sup>1</sup>	2	2	2	2
Minimum Total Cores	2	2	2	2
Management Cores	1	1	1	1
Maximum Data Plane Cores	1	1	1	1
Minimum Data Plane Cores	1	1	1	1
Network Interfaces	8	8	8	8
Supported IP/Nodes	10	25	50	100
Minimum Memory Required <sup>2</sup>	4G	4G	4G	4G
Minimum Hard Disk/Storage	60GB	60GB	60GB	60GB

1. If the actual number of cores allocated exceeds the number of cores defined in the above table, extra cores will be used as CPs. Multiple CP support is introduced in 6.5.4.v.

2. Memory requirements are higher with Jumbo Frames enabled. See the Memory Requirements on NS*v with Jumbo Frames Enabled vs Disabled* table.

Product Models	NSv 200	NSv 300	NSv 400	NSv 800	NSv 1600
Maximum Cores <sup>1</sup>	2	3	4	8	16
Minimum Total Cores	2	2	2	2	2
Management Cores	1	1	1	1	1
Maximum Data Plane Cores	1	2	3	7	15
Minimum Data Plane Cores	1	1	1	1	1
Network Interfaces	8	8	8	8	8
Supported IP/Nodes	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited
Minimum Memory Required <sup>2</sup>	6G	8G	8G	10G	12G
Minimum Hard Disk/Storage	60G	60G	60G	60G	60G

1. If the actual number of cores allocated exceeds the number of cores defined in the above table, extra cores will be used as CPs. Multiple CP support is introduced in 6.5.4.v.

2. Memory requirements are higher with Jumbo Frames enabled. See the Memory Requirements on NSv with Jumbo Frames Enabled vs Disabled table.

On NSv ESXi deployments with Jumbo Frame support enabled, the Minimum Memory requirements are higher. This increases TCP performance. See the Memory Requirements on NSv with Jumbo Frames Enabled vs Disabled table below.

#### Memory Requirements on NSv with Jumbo Frames Enabled vs Disabled

NSv Model	Minimum Memory – Jumbo Frames Enabled	Minimum Memory – Jumbo Frames Disabled
NSv 10 / 25 / 50 / 100	6G	4G
NSv 200	6G	4G
NSv 300	8G	6G

#### Memory Requirements on NSv with Jumbo Frames Enabled vs Disabled

NSv Model	Minimum Memory – Jumbo Frames Enabled	Minimum Memory – Jumbo Frames Disabled
NSv 400	10G	8G
NSv 800	14G	10G
NSv 1600	18G	12G

### **Backup and Recovery Information**

In certain situations, it might be necessary to contact SonicWall Technical Support, use SafeMode, or de-register the NSv appliance:

- If the splash screen remains displayed, this can indicate that the disk is corrupted. Please contact SonicWall Technical Support for assistance.
- If the disk is not recoverable, then the NSv appliance needs to be deregistered with MySonicWall. See Deregistering Your NSv on page 30 for information.
- If SonicOS does not boot up, you can go into SafeMode and download the log files, upload a new SonicOS image, or take other actions. For information about SafeMode, see Using SafeMode on the NSv on page 50.
- If SonicOS fails three times during the boot process, it will boot into SafeMode. Verify that the minimum required memory is available and allocated based on the NSv model. If it still cannot boot up, download the logs while in SafeMode and contact SonicWall Technical Support for assistance.

### **Best Practices and Recommendations**

- Configuration settings import is not supported from SonicWall physical appliances to NSv Series ESXi.
- SonicWall NSv Series supports the **vmxnet3** VMware Network Adapter Type. Exactly 8 virtual network interfaces (vNICs) are supported on each NSv platform. Adding and removing interfaces is supported, but the total must stay within the range of 2 to 8.
- To configure Virtual Interfaces in NSv on ESXi, map the NSv parent interface for the virtual interface to a port group with the VLAN ID 4095 (Trunk Port). ESXi treats a port group with VLAN 4095 as a Trunk Port.
- SonicWall recommends that you do *not* use the ESXi snapshot functionality. For more information, see https://kb.vmware.com/s/article/1025279.

# **High Availability Configurations**

NSv virtual firewalls deployed on ESXi can be configured as high availability Active/Standby pairs to eliminate a single point of failure and provide higher reliability. Two identical NSv instances are configured so that when the primary fails, the secondary takes over to maintain communications between the Internet and the protected network. These redundant NSv instances may share the same license when registered on MySonicWall as associated products. For details, refer to SonicOS 6.5.4 NSv Updates.

Additional licensing allows configuration of an Active/Standby pair to handle a Stateful failover in which the Standby NSv takes over without having to initialize network connections and VPNs. However, dynamic ARP entries and common virtual MACs are not currently supported. For more details, see the High Availability section in SonicOS NSv 6.5.4 System Setup.

# Exporting and Importing Firewall Configurations

Moving configuration settings from SonicWall physical appliances to the NSv Series is not supported. However, configuration settings may be moved from one NSv to another. See the SonicOS 6.5 NSv Series Updates administration book and the SonicOS 6.5.4 NSv Series Upgrade Guide on the Technical Publications portal for more information about exporting and importing configuration settings.

Go to https://www.sonicwall.com/support/technical-documentation/ and select "NSv Series" as the product.

# Upgrading to a Higher Capacity NS<sub>v</sub> Model

It is possible to move up to a higher capacity NSv model, but not down to a lower capacity model. For instructions refer to the SonicOS 6.5.4 NSv Series Upgrade Guide on the Technical Publications portal. Go to https://www.sonicwall.com/support/technical-documentation/ and select "NSv Series" as the product.

For details on the number of process and memory to allocate to the VM to upgrade, refer to Product Matrix and Requirements on page 7.

To update the VM for processors and memory allocations, power-down the VM then right click on the VM and select "Edit Settings". The processor and memory settings then appear:

Edit Settings SonicWALL_NSv_50		×
Virtual Hardware VM Options		
		ADD NEW DEVICE
> CPU	2 ~	0
> Memory	6 GB ~	
> Hard disk 1	50.080078125 GB ~	
> SCSI controller 0	LSI Logic Parallel	
> Network adapter 1	10.203.26.X v	Connect
> Network adapter 2	10.203.26.X V	Connect
> Network adapter 3	10.203.26.X V	
> Network adapter 4	10.203.26.X V	✓ Connect
> Network adapter 5	10.203.26.X ∨	✓ Connect
		CANCEL

# Creating a MySonicWall Account

A MySonicWall account is required to obtain the OVA file for initial installation of the NSv Series ESXi virtual firewall, for product registration to enable full functionality of SonicOS features, and for access to licensed security services. For a High Availability configuration, MySonicWall provides a way to associate a secondary NSv that can share security service licenses with your primary appliance.

**NOTE:** MySonicWall registration information is not sold or shared with any other company.

#### To create a MySonicWall account:

- 1 In your web browser, navigate to https://www.mysonicwall.com.
- 2 In the login screen, click the **Sign Up** link.

	ALL		
MISONICWALL			
Login with your MySon credentials Username or Email add	icWall accour dress	ıt	
		□	
		_ \	
Next	:		

- 3 Complete the account information, including email and password.
- 4 Enable two-factor authentication if desired.
- 5 If you enabled two-factor authentication, select one of the following authentication methods:
  - Email (one-time passcode) where an email with a one-time passcode is sent each time you log into your MySonicWall account.
  - **Microsoft/Google Authentication App** where you use a Microsoft or Google authenticator application to scan the code provided. If you are unable to scan the code, you can click on a link for a secret code. Once the code is scanned, you need only click a button.
- 6 Click on **Continue** to go to the **COMPANY** page.
- 7 Complete the company information and click **Continue**.
- 8 On the **YOUR INFO** page, select whether you want to receive security renewal emails.
- 9 Identify whether you are interested in beta testing of new products.

- 10 Click **Continue** to go to the **EXTRAS** page.
- 11 Select whether you want to add additional contacts to be notified for contract renewals.
- 12 If you opted for additional contacts, input the information and click Add Contact.
- 13 Click Finish.
- 14 Check your email for a verification code and enter it in the **Verification Code** field. If you did not receive a code, contact Customer Support by clicking on the link.
- 15 Click **Done**. You are returned to the login window so you can login into MySonicWall with your new account.

## 2

# Installing NS<sub>v</sub> Series on ESXi

#### **Topics:**

- Obtaining the OVA from MySonicWall on page 12
- Installing the NSv Appliance on page 13
- Viewing and Editing Virtual Machine Settings on page 19
- Troubleshooting Installation Configuration on page 21

# Obtaining the OVA from MySonicWall

Refer to the purchase confirmation email for information about downloading the OVA files.

If you do not have a MySonicWall account, see Creating a MySonicWall Account on page 10 for information about creating one.

#### To perform initial registration and obtain the OVA file for deployment:

- 1 In a browser, log into your MySonicWall account.
- 2 Navigate to My Products > Register Product.
- 3 Fill in the Serial Number, Friendly Name, Product Group, and Authentication Code fields, and then click Register.

SONIC <b>WALL</b>   MySo	nicWall		
Home	Register Product		
Product Management	Add New	Product Olient Distribution Group	
Register Product	Fields marked by (*) are mandatory.	e Product e client bistribution group	
My Client Licenses	General Info		
Free Trial Software	Serial Number: 🧿		*
CFC Management	Friendly Name:	SonicOS Virtual 209	
Get NFR Licenses	Product Group:		
Bulk Activation	Authentication Code: ?		
Bulk Activation Status			
Register Anything		Register	

4 The **Registration Code** is displayed. Make a note of it.

You are now given access to the OVA file for your NSv model.

5 Download the OVA file and save it to your management computer.

You are now ready to deploy the OVA on your ESXi server. See Installing the NSv Appliance on page 13 for information.

After your NSv installation is complete, boot up SonicOS and log in. See Managing SonicOS on the NSv Series on page 33 for information.

Once you have connected and have internet access from the NSv, you must register your NSv Series instance using the Registration Code to complete the registration process. See Registering the NSv Appliance from SonicOS on page 25.

If your NSv is deployed in a closed network, see Registering an NSv Manually in a Closed Network on page 29.

# Installing the NS<sub>v</sub> Appliance

SonicWall NSv Series is installed by deploying an OVA file to your ESXi server. Each OVA file contains the software components needed. Deploy the OVA file by using the vSphere or vCenter client, which are available with ESXi.



(i) NOTE: The elements of VMware must already be in place and the administrator must be familiar with the basics of deploying a virtual appliance on the ESXi server.

TIP: Step 14 has some important information about selecting your networks. Even if you don't need all (i) these step-by-step instructions, be sure to follow the instructions in Step 14 to avoid connectivity issues after the deployment.

#### To perform a fresh install of NSv Series on ESXi:

- 1 Download the NSv Series OVA file from MySonicWall to a computer with vSphere / vCenter access.
- 2 Access vSphere or vCenter and log on to your ESXi server.
- 3 Navigate to the location where you want to install the virtual machine, and select the folder.
- 4 To begin the import process, click Actions and select Deploy OVF Template.



- 5 In the Select template screen, select Local file:
  - Local file Click Browse and navigate to the NSv Series OVA file that you previously downloaded.

🍘 De	ploy OVF Template	(?) »
1 3 2 9 3 9 4 F 5 9 6 F	Select template Select name and location Select a resource Review details Select storage Ready to complete	Select template         Select an OVF template.         Enter a URL to download and install the OVF package from the Internet, or browse to a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.         URL         ✓ Local file         Browse         ▲ Use multiple selection to select all the files associated with an OVF template (.ovf, .vmdk, etc.)
		Back Next Finish Cancel

- 6 Click Next.
- 7 In the **Select name and location** screen, type a descriptive name for the NSv appliance into the **Name** field, and then select the location for it from the ESXi folder structure.

🎲 Deploy OVF Template		? »
<ul> <li>1 Select template</li> <li>2 Select name and location</li> <li>3 Select a resource</li> <li>4 Review details</li> <li>5 Select storage</li> <li>6 Ready to complete</li> </ul>	Select name and location         Enter a name for the OVF and select a deployment location.         Name       SonicWall_NSv_R80         Filter       Browse         Select a datacenter or folder.            ✓ @ vcenter.sce.hvnc.net             Mano            Select a datacenter or folder.	
	Back Next f	Finish Cancel

- 8 Click Next.
- 9 In the Select a resource screen, click Next to accept the default resource for the selected folder, or select a different resource and then click Next. Wait while the resource is validated. This is the resource pool where you want to deploy the template.

8	Deploy OVF Template	• •
~ ~	<ol> <li>Select template</li> <li>Select name and location</li> <li>Select a resource</li> </ol>	Select a resource Select where to run the deployed template.
	<ul><li>4 Review details</li><li>5 Select storage</li><li>6 Ready to complete</li></ul>	Select a host or cluster or resource pool or vapp.    Select a host or cluster
		Back Next Finish Cancel

10 In the Review details screen, verify the template details and then click Next.

🍘 Deploy OVF Template						? H
<ul> <li>1 Select template</li> <li>2 Select name and location</li> </ul>	Review details Verify the template	details.				
✓ 3 Select a resource	Publisher	SonicWall Inc. (Trusted certificate)				
4 Review details	Download size	1.0 GB				
5 Accept license agreements 6 Select storage	Size on disk	1.6 GB (thin provisioned) 66.3 GB (thick provisioned)				
<ul><li>7 Select networks</li><li>8 Customize template</li><li>9 Ready to complete</li></ul>	Description	SonicWall_NSv_R80				
			Back	Next	Finish	Cancel

11 In the Accept license agreements screen, read the agreement, click Accept and then click Next.

Peploy OVF Template	(?) »
<ul> <li>Deploy OVF Template</li> <li>1 Select template</li> <li>2 Select name and location</li> <li>3 Select a resource</li> <li>4 Review details</li> <li>5 Accept license agreements</li> <li>6 Select storage</li> <li>7 Select networks</li> <li>8 Customize template</li> <li>9 Ready to complete</li> </ul>	Accept license agreements Read and accept the license agreements associated with this template before continuing.      SonicWall End User Product Agreement PLEASE READ THIS AGREEMENT CAREFULLY BEFORE USING THIS PRODUCT. BY DOWNLOADING, INSTALLING OR USING THIS PRODUCT, YOU ACCEPT AND AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT. FOR DELIVERIES OUTSIDE THE UNITED STATES OF AMERICA, PLEASE GO TO HTTPS://WWW.SONICWALL.COM/LEGAL/EUPAASPX TO VIEW THE APPLICABLE VERSION OF THIS AGREEMENT FOR YOUR REGION, IF YOU DO NOT AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT FOR YOUR REGION, IF YOU DO NOT AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT FOR YOUR REGION, IF YOU DO NOT AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT OR THE APPLICABLE VERSION OF THIS AGREEMENT FOR YOUR REGION, DO NOT DOWNLOAD, INSTALL OR USE THIS PRODUCT. This SonicWall End User Product Agreement (the "Agreement") is made between you, the Customer' or "You") and the Provider, as defined below. 1. Definitions. Capitalized terms not defined in context shall have the meanings assigned to them below: (a) "Affiliate" means any legal entity controlled by, or under common control with a party to this Agreement, for so long as such control relationship exists. (b) "Appliance" means a computer hardware product upon which Software is pre-installed and delivered. (c) "Documentation" means the user manuals and documentation that Provider makes available for the Products, and all copies of the foregoing.
	Accept Back Next Finish Cancel

12 In the **Select storage** screen, first select a datastore from the table. This is the location where you want to store the virtual machine files.

1 Select template	Select storage Select location to store the	e files for the de	eploved template			
2 Select name and location						
3 Select a resource	Select virtual disk format:	Thick provision	on lazy zeroed	•		
4 Review details	VM storage policy:	None		•		
5 Accept license agreements	Show datastores from	Storage DRS of	clusters 🚯			
6 Select storage	Filter					
7 Select networks		<b>a</b>				
8 Customize template	Datastores Datastore	Clusters			the constants of	
9 Ready to complete				C	) 🃡 🍱 ( <b>q</b> Filt	er 🔹
	Name		Status	VM storage policy	Capacity	Free
	O 🗐 NAS		<ul> <li>Normal</li> </ul>	VM Encryption Po	33.48 TB	8.87 TB
	⊙ 📑 SSD-esx2		Normal	VM Encryption Po	222.25 GB	82.87 GB
	● SSD-esx2 ● ■ sys-esx2		<ul> <li>Normal</li> <li>Normal</li> </ul>	VM Encryption Po VM Encryption Po	222.25 GB 2.5 GB	82.87 GB 1.92 GB
	<ul> <li>SSD-esx2</li> <li>sys-esx2</li> <li>YM2</li> </ul>		Normal     Normal     Normal     Normal	VM Encryption Po VM Encryption Po VM Encryption Po	222.25 GB 2.5 GB 33.48 TB	82.87 GB 1.92 GB 8.95 TB
	SSD-esx2     sys-esx2     YM2		<ul> <li>Normal</li> <li>Normal</li> <li>Normal</li> </ul>	VM Encryption Po VM Encryption Po VM Encryption Po	222.25 GB 2.5 GB 33.48 TB	82.87 GB 1.92 GB 8.95 TB
	Image: SSD-esx2       Image: Sys-esx2       Imag		Normal     Normal     Normal     Normal	VM Encryption Po VM Encryption Po VM Encryption Po	222.25 GB 2.5 GB 33.48 TB	82.87 GB 1.92 GB 8.95 TB
	● 📄 SSD-esx2 ● 📑 sys-esx2 ● 📑 VM2		<ul> <li>Normal</li> <li>Normal</li> <li>Normal</li> </ul>	VM Encryption Po VM Encryption Po VM Encryption Po	222.25 GB 2.5 GB 33.48 TB	82.87 GB 1.92 GB 8.95 TB
	● 📄 SSD-esx2 ● 📑 sys-esx2 ● 📑 VM2		<ul> <li>Normal</li> <li>Normal</li> <li>Normal</li> </ul>	VM Encryption Po VM Encryption Po VM Encryption Po	222.25 GB 2.5 GB 33.48 TB	82.87 GB 1.92 GB 8.95 TB

- 13 Leave the default settings for the datastore provisioning and click **Next**. The default is **Thick Provision** Lazy Zeroed.
- 14 In the **Select networks** screen, *first sort the list of interfaces* by clicking the **Source Network** column heading. Then select the vswitch networks that are mapped to the NSv appliance interfaces. The source networks are the NSv appliance interfaces (X0, X1, X2, X3, X4, X5, X6, X7), and the destination networks are the vswitch ports of your existing vswitch network configuration. If your vswitch networks are not fully configured, you can further adjust the interface/vswitch port pairs after the import.

(i) NOTE: The ESXi vswitch configuration should have the option for MAC address changes enabled for the vswitch ports connected to the NSv.

For advanced configurations (DVS), consult the ESXi documentation on vswitch configuration.

Typically, the NSv Series is deployed between your internal network and a network with internet access, and therefore you map the source **X0** to your LAN network (vswitch port), and map the source **X1** to the WAN network (vswitch port) with connectivity to the internet.

(i) **IMPORTANT: SONICOS\_X1** (the default WAN Interface) is set to **DHCP** by default, with **HTTPS management** enabled for the NSv Series, as this configuration eases deployments in virtual/cloud environments.

**NOTE:** System defaults for the X0 and X1 interfaces are:

- X0 Default LAN 192.168.168.168
- X1 Default WAN DHCP addressing, with HTTPS and Ping management enabled

**NOTE:** Configuration settings import from physical firewalls to the NSv Series is not supported.

🍘 Deploy OVF Template		? )
<ul> <li>1 Select template</li> <li>2 Select name and location</li> </ul>	Select networks Select a destination network for each so	purce network.
<ul> <li>3 Select a resource</li> </ul>	Source Network	Destination Network
<ul> <li>4 Review details</li> </ul>	SONICOS_X0	VLAN 4 - DMZ
<ul> <li>5 Accept license agreements</li> </ul>	SONICOS_X6	VLAN 4 - DMZ
✓ 6 Select storage	SONICOS_X5	VLAN 4 - DMZ
7 Select networks	SONICOS_X7	VLAN 4 - DMZ
8 Customize template	SONICOS_X2	VLAN 4 - DMZ
9. Ready to complete	SONICOS_X1	VLAN 4 - DMZ
5 Neady to complete	SONICOS_X4	VLAN 4 - DMZ
	SONICOS_X3	VLAN 4 - DMZ
	IP Allocation Settings IP protocol: IPv4	IP allocation: Static - Manual 0
		Back Next Finish Cancel
🍞 Deploy OVF Template		(2) N
<ul> <li>1 Select template</li> </ul>	Select networks	

<ul> <li>1 Select template</li> <li>2 Select name and location</li> </ul>	Select networks Select a destination network for each s	ource network.
✓ 3 Select a resource	Source Network	Destination Network
✓ 4 Review details	SONICOS_X0	VLAN 2 - main
✓ 5 Accept license agreements	SONICOS_X6	VLAN 100
✓ 6 Select storage	SONICOS_X5	VLAN 100
7 Select networks	SONICOS_X7	VLAN 100
8 Customize template	SONICOS_X2	VLAN 100
9. Ready to complete	SONICOS_X1	VLAN 4 - DMZ
5 Ready to complete	SONICOS_X4	VLAN 100
	SONICOS_X3	VLAN 100 +
	Description - SONICOS_X1 SonicOS X1 Interface (Default: DHCP) IP Allocation Settings IP protocol: IPv4	IP allocation: Static - Manual 🕕
		Back Next Finish Cancel

15 Click Next.

16 In the **Ready to complete** screen, review the settings and click **Finish** to create the NSv appliance. To change a setting, click **Back** to navigate back through the screens to make a change.

🈚 Deploy OVF Template		@ »
<ul> <li>1 Select template</li> <li>2 Select name and location</li> </ul>	Ready to complete Review configuration data.	
✓ 3 Select a resource	Name	SonicWall NSV
<ul> <li>4 Review details</li> </ul>	Source VM name	SonicWall_NSv_R80
<ul> <li>5 Accept license agreements</li> </ul>	Download size	1.0 GB
<ul> <li>6 Select storage</li> </ul>	Size on disk	66.3 GB
<ul> <li>7 Select networks</li> </ul>	Datacenter	sce
<ul> <li>8 Customize template</li> </ul>	Resource	192.168.1.11
9 Ready to complete	Storage mapping	1
	▶ Network mapping	8
	▹ IP allocation settings	IPv4, Static - Manual
	Properties	SonicCore Hostname = SonicWall NSv
		Back Next Finish Cancel

The name of the new NSv appliance appears in the left pane of the vSphere or vCenter window when complete.

The next step is to power on your NSv virtual firewall in the vSphere or vCenter interface. See Viewing and Editing Virtual Machine Settings on page 19 for information about powering on your NSv and related topics.

Once your NSv virtual firewall is powered on, the next step is to register it on MySonicWall. See Registering the NSv Appliance from SonicOS on page 25 for information about registering your NSv.

Other related topics are:

- Registering an NSv Manually in a Closed Network on page 29
- Managing SonicOS on the NSv Series on page 33
- Using System Diagnostics in SonicOS on page 36
- Using the Virtual Console on page 38

# Viewing and Editing Virtual Machine Settings

When logged into vSphere or vCenter, you can view and edit some basic information for your NSv Series instance.

With your NSv Series instance selected in the left pane, click **ACTIONS** to view the options.



Select Power to choose from Power On, Power Off, Shut Down Guest OS, Restart Guest OS, and other options.

Select **Open Remote Console** to launch the same *ESXi Remote Console* that you get with the **Launch Remote Console** link on the **Summary** screen.

Select **Edit Settings** to open the Edit Settings dialog where you can access settings for the number of CPUs, Memory size, Hard disk size, Network adapters, and other items in the ESXi configuration for this NSv Series instance.

	· · · · ·	
	ADD NEV	V DEVICE
> CPU	2 ~	0
> Memory	8 GB ~	
> Hard disk 1	68.4140625 GB V	
> SCSI controller 0	LSI Logic Parallel	
> Network adapter 1	sonicosv_x0 🗸 🗹 Connect	ed
> Network adapter 2	10.203.26.X V Connected	
> Network adapter 3	sonicosv_x2 v 🛛 Connect	ed
> Network adapter 4	sonicosv_x3 v 🛛 Connect	ed
Network adapter 5	sonicosv_x4 🗸 🗹 Connect	ed

The ESXi Network adapters are mapped to the NSv Series interfaces as follows:

#### Network Adapters to NSv Series Interfaces Mapping

Network Adapter #	NSv Series Interface	Default IP	Default Zone
Network adapter 1	x0	192.168.168.168	LAN
Network adapter 2	x1	DHCP	WAN
Network adapter 3	x2	N/A	LAN
Network adapter 4	x3	N/A	LAN
Network adapter 5	x4	N/A	LAN
Network adapter 6	x5	N/A	LAN
Network adapter 7	x6	N/A	LAN
Network adapter 8	х7	N/A	LAN

# Troubleshooting Installation Configuration

If the NSv fails to come up, follow the instruction in Using the NSv Management Console on page 42 to go to the NSv Management Console window or the SonicOS CLI window. Check the boot messages:

() NOTE: The error messages shown below indicate that the virtual firewall cannot boot.

### Insufficient Memory Assignment

The following messages will appear if the virtual machine has insufficient memory. This may occur when doing an NSv installation or a NSv product upgrade.

#### SonicOS boot message:

Insufficient memory 4 GB, minimum memory required 10 GB for NSv model: "NSv 800 Beta" Power off the Network Security virtual appliance and assign 10 GB to this virtual appliance.

This message can also appear in the Management Console logs as shown in the two following screen shots.



NOTE: For details on navigating the NSv Management Console to troubleshoot the installation, see Using the NSv Management Console on page 42.

Memory may be insufficient without a insufficient memory log entry:



### Incompatible CPU

If the CPU does not support AES instructions the following message will appear:

CPU Model Intel(R) Xeon(R) CPU E5-2420 0 @ 1.90GHz is not supported by SonicWall Network Security Virtual CPU Model Intel(R) Xeon(R) CPU E5-2420 0 @ 1.90GHz does not support the Advanced Encryption Standard(AES) instructions Refer to Getting Started Guide and install the SonicWall Network Virtual on a supported platform

The message can also be seen in the logs provided by the management console:

r-Menu	Mar 30 16:56:01 localhost Initializing SonicWall support services
System Info	Mar 30 16:56:00 localhost Completed configuring the operating environment for SonicOS
Management Network	Mar 30 16:56:00 localhost This NSu model supports 8 CPU, current CPU count is only 2, for impr
Test Management Network	Mar 30 16:56:00 localhost Total memory installed 8099184 Kb
Diagnostics	Mar 30 16:55:15 localhost CPU model Intel(R) Xeon(R) CPU E5-2420 0 @ 1,90GHz does not support
NTP Server	Mar 30 16:55:15 localhost CPU model Intel(R) Xeon(R) CPU E5-2420 0 @ 1.90GHz does not support
Lockdown Mode	Mar 30 16:55:15 localhost CPU flags: fou ume de use tsc msr pae mce cx8 apic sep mtrr poe mca
Sustem Undate	Mar 30 16:55:15 localhost CPU count: 2, Model "Intel(R) Xeon(R) CPU E5-2420 0 @ 1.90GHz"
Reboot   Shutdown	Mar 30 16:55:15 localhost Configuring the overating environment for SonicOS
About	Rebot
Logs	Mar 30 16:55:01 localhost Unconfigure the operating environment for SonicOS
	Mar 30 16:50:29 localbost Initializing Sonicial I sumort services
	Mar 30 15:20:32 localhost this NSv model supports 8 CPU, current CPU count is only 2, for impr
	Mar 30 15:20:32 localhost Total memory installed 8099184 Kb
Up / Down to select items	Mar 30 15:20:32 localhost CPU flags: fpu ume de pse tsc msr pae mce cx8 apic sep mtrr pge mca
TAB to move between views	Mar 30 15:20:32 localhost CPU count: 2, Model "Intel(R) Xeon(R) CPU E5-2420 0 @ 1.90GHz"
Enter to action/edit an item	Mar 30 15:20:31 localhost Configuring the operating environment for SonicOS
Space to hide/show side menu	Reboot
	Mar 30 15:10:39 localhost Initializing SonicWall support services
	Anness herest Manifester stars - Comment Lines 4 Lines 140

#### If the CPU does not support SSE 4.1 or 4.2 instructions the following message will appear:

CPU Model Intel(R) Xeon(R) CPU E5-2420 0 @ 1.90GHz is not supported by SonicWall Network Security Virtual CPU Model Intel(R) Xeon(R) CPU E5-2420 0 @ 1.90GHz does support SSE 4.1 or 4.2 instructions

Refer to Getting Started Guide and install the SonicWall Network Virtual on a supported platform

### Incorrect CPU Configuration

All cores must be on the same socket. Customer needs to change the CPU configuration in settings.

The SonicWall Network Security requires all virtual CPU to reside on a single socket. Power down the virtual machine and adjust the CPU configuration such that all CPU reside on the same socket

(i) **NOTE:** The above error may occur when EVC masks the CPU capability. https://communities.vmware.com/thread/536227 resolution is to disabled EVC.

### Insufficient Resources at Time of Configuration

If the ESXi infrastructure where the NSv is being installed has poor performance the following message may appear at time of installation:

If the above message occurs during initialization, more information is available in the logs:

System Info	Apr 02 16:18:27 lc	ocalhost This	initialization process	is taking l	longer than expected,	load ave ge: 1.10, time: 250 seconds
Management Network	Apr 02 16:18:26 lc	ocalhost This	initialization process	is taking l	longer than expected,	load ave ge: 1.10, time: 249 seconds
Test Management Network	Apr 02 16:18:25 1c	acalhost This	initialization process	is taking 1	longer than expected.	load aue me: 1.10, time: 248 seconds
Diagnostics	Apr 02 16:18:24 1c	calhost This	initialization process	is taking 1	onger than expected	load ave me: 1 10, time: 247 seconds
NTD Senuer	Ann 02 16:10:22 1a	an lheat This	initialization process	in taking 1	langer than expected	lead and get 1 10 time: 246 percende
T - 1 Jacob Ma Ja	npr 02 10.10.23 10	Juannost mis	initialization process	is taking i	longer than expected,	Tuan ave get 1.10, time: 240 seconds
Lockdown Hode	Apr 02 16:18:22 10	ocalhost This	initialization process	is taking I	longer than expected,	load ave ge: 1.11, time: 245 seconds
System Update	Apr 02 16:18:21 Ic	ocalhost This	initialization process	is taking l	longer than expected,	load ave ge: 1.11, time: 244 seconds
Reboot   Shutdown	Apr 02 16:18:20 lc	ocalhost This	initialization process	is taking l	longer than expected,	load ave ge: 1.11, time: 243 seconds
About	Apr 02 16:18:19 lc	ocalhost This	initialization process	is taking l	longer than expected,	load ave ge: 1.11, time: 242 seconds
Logs	Apr 02 16:18:17 lo	calhost This	initialization process	is taking l	longer than expected.	load ave ge: 1.11, time: 241 seconds
	Anr 02 16:18:16 1c	acalhost This	initialization process	is taking l	longer than expected.	load aue ge: 1.12, time: 240 seconds
	Ann 02 16:18:15 1c	calhoet This	initialization process	ie taking l	ongen than expected	load ave met 1 12 time: 239 seconds
	02 16:10:13 16	alboat This	initialization process	in taking 1	longer than expected	load aug get 1.12) time: 239 seconds
	npr 02 10.10.14 10	Juannost mils	initialization process	is taking i	longer than expected,	That are get 1.12, time: 200 seconds
	Hpr 02 16:18:13 10	ocalhost This	initialization process	is taking I	longer than expected,	load ave ge: 1.12, time: 237 seconds
	Apr 02 16:18:12 Ic	ocalhost This	initialization process	is taking l	longer than expected,	load ave ge: 1.13, time: 23b seconds
	Apr 02 16:18:11 lc	ocalhost This	initialization process	is taking l	longer than expected,	load ave ge: 1.13, time: Z35 seconds
	Apr 02 16:18:10 lc	ocalhost This	initialization process	is taking l	longer than expected,	load ave ge: 1.13, time: 234 seconds
	Apr 02 16:18:09 1c	ocalhost This	initialization process	is taking 1	longer than expected,	load ave ge: 1.13, time: 233 seconds
	Anr 02 16:18:08 1c	ncalhost This	initialization process	is taking l	inner than expected.	Inad aue ge: 1.13, time: 232 seconds
	Apr 02 16:18:07 1c	calhost This	initialization process	is taking I	innger than expected.	load aue me: 1.15, time: 231 seconds
	App 02 16:18:06 1c	calhost This	initialization process	ie taking l	longen than expected	load ave met 1 15, time: 230 seconds
	02 16:10:00 10	alboat This	initialization process	io taking 1	longer than expected	load avo get 1.15) time: 229 seconds
	Hpr 02 16:10:05 10	Juannust Inis	initialization process	IS CARING I	longer than expected,	Tuda due ye. 1.15, time. 225 seconds
	Hpr 02 16:18:04 10	ocalnost inis	initialization process	is taking I	longer than expected,	load ave ge: 1.15, time: 220 seconds
	Apr 02 16:18:03 Ic	ocalhost This	initialization process	is taking I	longer than expected,	load ave ge: 1.15, time: 227 seconds
	Apr 02 16:18:02 lc	ocalhost This	initialization process	is taking l	longer than expected,	load ave ge: 1.16, time: 226 seconds
	Apr 02 16:18:01 lc	ocalhost This	initialization process	is taking l	longer than expected,	load ave ge: 1.16, time: 225 seconds
	Apr 02 16:18:00 lc	ocalhost This	initialization process	is taking l	longer than expected,	load ave ge: 1.16, time: 224 seconds
	Amr 02 16:17:59 1c	ncalhost This	initialization process	is taking l	onger than expected.	Inad aue ge: 1.16, time: 223 seconds
	Apr 02 16:17:58 1c	calhost This	initialization process	is taking I	onger than expected.	load aue me: 1.16, time: 222 seconds
	App 02 16:17:57 1c	calhost This	initialization process	is taking 1	onger than expected	load ave me: 1 17, time: 221 seconds
	Ann 02 16:17:56 1c	albost This	initialization process	in taking 1	longen than expected	load ave get 1 17 time: 220 seconds
	02 10:17:50 IC	Juliust mis	initialization process	is taking i	longer than expected,	load ave go: 1.17, time: 220 seconds
	Hpr 02 10.17.55 IU	Juannost Inis	initialization process	is caking i	longer than expected,	Tuda ave get 1.17, time, 215 seconds
	Apr 02 16:17:54 Ic	ocalhost This	initialization process	is taking I	longer than expected,	load ave ge: 1.17, time: 218 seconds
	Apr 02 16:17:53 lc	ocalhost This	initialization process	is taking l	longer than expected,	load ave ge: 1.17, time: 217 seconds
	Apr 02 16:17:52 lc	ocalhost This	initialization process	is taking l	longer than expected,	load ave ge: 1.19, time: 216 seconds
	Apr 02 16:17:51 lc	ocalhost This	initialization process	is taking l	longer than expected,	load ave ge: 1.19, time: 215 seconds
	Apr 02 16:17:50 lc	ncalhost This	initialization process	is taking 1	onger than expected.	load ave ge: 1.19, time: 214 seconds
	Apr 02 16:17:48 1c	acalhost This	initialization process	is taking 1	onger than expected.	load ave ge: 1.19, time: 213 seconds
	Apr 02 16:17:47 1c	calbost This	initialization process	is taking	longer than expected	load aug ge: 1 19, time: 212 seconds
	Ann 02 16:17:46 1c	albort This	initialization process	in taking 1	longen than expected,	load aus we' 1 21 time' 211 seconds
the la party designations advect	Ann 02 16:17:46 10	the the	initialization process	is taking I	tonger than expected,	land ave go: 1.21, time: 210 seconds
up y pown to select items	mpr 02 16:17:45 10	Julianiost Inis	initialization process	is caking i	unger than expected,	Tuad ave get 1.217 time. 210 seconds
TAB to move between views	Apr 02 16:17:44 1c	ocalhost This	initialization process	is taking l	longer than expected,	load ave ge: 1.21, time: 209 seconds
Enter to action/edit an item	Apr 02 16:17:43 lc	ocalhost This	initialization process	is taking l	longer than expected,	load ave ge: 1.21, time: 208 seconds
Space to hide/show side menu	Apr 02 16:17:42 lc	ocalhost This	initialization process	is taking l	longer than expected,	load ave ge: 1.22, time: 207 seconds
	Apr 02 16:17:41 lc	ocalhost This	initialization process	is taking 1	longer than expected,	load ave ge: 1.22, time: 206 seconds

### **Incorrect Network Adapter Configuration**

If the user adds a non-VMXNET3 driver the following error will appear on boot.

The SonicWall Network Security Virtual network adapters have been modified NSv configuration supports 8 VMXNET ethernet adapters Currently 1 non VMXNET3 ethernet adapters are configured Power down the virtual machine and remove the 1 non VMXNET3 network adapters

### **Incorrect Number of Network Adapters**

The NSv supports exactly 8 VMXNET3 Network adapters. If the customer adds or removes a VMXNET3 Network adapter the below error message will appear.

The SonicWall Network Security Virtual network adapters have been modified NSv requires 8 ethernet adapters, currently 7 are configured Power down the virtual machine and configure the additional 1 VMXNEt network adapters

### Insufficient Memory When Jumbo Frames Enabled

The below error message appears on boot when Jumbo frames have been enabled and there is insufficient memory. Resolution is to power off the VM and increase the memory.

Insufficient memory 5 GB. The minimum memory required is 10 GB for NSv model: "NSv 400" with the jumbo frame feature enabled Power off the Network Security virtual applicane and assign 10 GB of memory to this virtual appliance

# Licensing and Registering Your NS<sub>v</sub>

#### **Topics:**

- Registering the NSv Appliance from SonicOS on page 25
- Registering with Zero-Touch Deployment on page 27
- Registering an NSv Manually in a Closed Network on page 29
- Deregistering Your NSv on page 30
- Converting a Free Trial License to Full License on page 31

# Registering the $NS_{v}$ Appliance from SonicOS

Once you have installed and configured network settings for your NSv Series appliance, you can log into SonicOS management and register it in your MySonicWall account. Registration of your SonicWall NSv Series follows the same process as for SonicWall hardware-based appliances.

(i) **NOTE:** System functionality is extremely limited if registration is not completed. See Using SonicOS on an Unregistered NSv on page 33 for more information.

#### To register your NSv appliance:

- 1 Point your browser to your NSv Series WAN or LAN IP address and log in as the administrator (default *admin / password*).
- 2 Click the **Register** link in the top banner or on the **MONITOR | System > Status** page.

SONICWALL	Network Security Virtual	MONITOR	INVESTIGATE	MANAGE		<u>Register</u>   Help   Logout
Current Status System Status > User Sessions	The password hass Log messages can Cloud backup not e System Inform Mode: Product Code: GUID: Firmware Version:	n't been changed. not be sent becaus inabled - Click here NSV Unicensed 70000 SonicOS Enhanc	a you have not specif to enable. Show Mul ed 6.5.0.2-8y-sonicosy-3	ied an outbound ti-Core Monitor 374cf82cf8	SMTP server address. Security Services Nodes/Users: SSL VPN Nodes/Users: Your SonkWall is not registered. Click here to Register your SonicWall.	Mode: Configuration > Show All License Information 10 Hodes (0 in use) 2 Hodes (0 in use)

3 Enter your MySonicWall credentials and click LOGIN to log into MySonicWall.

SONICWALL"	etwork Security Virtual	OR INVESTIGATE	MANAGE
Current Status System Status Viser Sessions	MySonicWall username/email Password LOGIN	]	
	Forgot your Username or Password Create MySonicWall account	?	

4 In the **Serial Number** and **Authentication Code** fields, enter the corresponding values you received after purchasing your NSv Series virtual firewall.

Serial Number	
Authentication Code	
Friendly Name	
SUBMIT	

- 5 Type a descriptive name for the NSv into the **Friendly Name** field.
- 6 Click **SUBMIT**.
- 7 The licensing server acquires the necessary information from the NSv Series appliance and your MySonicWall account.
- 8 Acknowledge the registration completion notification by clicking **CONTINUE**.

SonicOS automatically restarts and then displays the login page.

9 Log into SonicOS.

On the **MANAGE** view under **Updates**, the **Licenses** page now shows your NSv appliance as **Licensed**.

10 In the **Licenses** page, you can activate security service free trials, enable available services, and click to purchase other services you want.

# Registering with Zero-Touch Deployment

The SonicWall NSv Series for ESXi is Zero-Touch enabled. Zero-Touch makes it easy to register your unit and add it to SonicWall Capture Security Center or SonicWall GMS On-Premises for management and reporting.

#### **Topics:**

- Deploying from CSC Management on page 27
- Deploying from GMS On-Premises on page 28

## Deploying from CSC Management

#### 1) Register:

- Point your browser to <a href="https://cloud.sonicwall.com">https://cloud.sonicwall.com</a> and log into your MySonicWall account or create an account.
- In Capture Security Center, click the mySonicWall tile to launch the MySonicWall Dashboard.
- Click the Add Product button to launch the QUICK REGISTER dialog and then type in the serial number of your SonicWall NSv. Click Confirm.

You should receive the NSv serial number and authentication code with your purchase confirmation email.

- In the **REGISTER A PRODUCT** dialog, fill in the **Friendly name** and **Authentication code**, and select the **Tenant Name**. By default, all products are placed under **SonicWall Products Tenant**.
- Click Register.

#### 2) Enable Zero-Touch and CSC Management and Reporting:

- MySonicWall recognizes your appliance model and displays the **Zero Touch** option. Enable **Zero Touch** and then click **Register** again. A success message is displayed to indicate Zero-Touch readiness.
- In MySonicWall, navigate to Product Management > My Products, select the appliance, and click the Try button to enable the license for CSC Management and Reporting (if not enabled already). A success message displays.
- 3) Connect and Power On the VM:
- NOTE: The NSv must be able to obtain an IP address via DHCP from the WAN connection. You may use as static IP address. For details on using the NSv Management Console to setup a static IP address, see Management Network on page 45.

**CSC Management** automatically acquires the unit (it can take up to 30 minutes for initial acquisition). Once the unit is acquired, you can begin management.

To view the status of your NSv instance:

- In MySonicWall, pull down the curtain for Capture Security Center.
- Using the same Tenant as you selected during registration, click the Management tile.
- Click the appliance serial number or friendly name under **DEVICE MANAGER** to display its status.

### Getting the Latest Firmware for the NSv

1 In Capture Security Center, click the mySonicWall tile.

- 2 Navigate to **Resources & Support > My Downloads** and select your product firmware from the **Product Type** drop-down menu.
- 3 Click the link for the firmware you want and save the file to a location on your computer.
- 4 Pull down the curtain for Capture Security Center.
- 5 Using the same Tenant as you selected during registration, click the **Management** tile.
- 6 In **DEVICE MANAGER**, click on the NSv instance in the left pane.
- 7 In the center pane, go to the **Register/Upgrades > Firmware Upgrade** page.
- 8 Click the Choose File button to select the firmware you just downloaded, then click Upgrade from Local File.

### Deploying from GMS On-Premises

 PREREQUISITE: GMS 8.7 or higher is required. Be sure that your GMS system is Zero-Touch enabled. Refer to the knowledge base article at: https://www.sonicwall.com/support/knowledge-base/?sol\_id=190205183052590

### 1) Register:

- Log into your MySonicWall account or create an account at www.mysonicwall.com.
- Click the Add Product button to launch the QUICK REGISTER dialog and then type in the serial number of your SonicWall appliance. Click Confirm.

You can find the serial number and authentication code on the shipping box or appliance label.

- In the **REGISTER A PRODUCT** dialog, fill in the **Friendly name** and **Authentication code**, and select the **Tenant Name**. By default, all products are placed under **SonicWall Products Tenant**.
- Click Register.

#### 2) Enable Zero-Touch:

- MySonicWall recognizes your NSv model and displays the **Zero Touch** option. Enable **Zero Touch**.
- Select the desired GMS Public IP from the **GMS Server Public IP/FQDN** drop-down list. The **ZeroTouch Agent Public IP/FQDN** field is populated with the associated IP address.

IMPORTANT: Verify that both of these IP addresses are the same as those you configured during the prerequisite process.

• Click Register.

#### 3) Connect and Power On VM:

() NOTE: The NSv must be able to obtain an IP address via DHCP from the WAN connection. If you need to use a static IP address, refer to the details on using the NSv Management Console, see Management Network on page 45.

**GMS** automatically acquires the unit (it can take up to 30 minutes for initial acquisition). Once the unit is acquired, you can begin management.

To view the status of your NSv instance:

- Log into GMS and navigate to the **FIREWALL** view.
- Click on the appliance in the left pane to display the status.

### Getting the Latest Firmware for the NS<sub>v</sub>

- 1 In a web browser, navigate to www.mysonicwall.com.
- 2 Navigate to **Resources & Support > My Downloads** and select your product firmware from the **Product Type** drop-down menu.
- 3 Click the link for the firmware you want and save the file to a location on your computer.
- 4 In GMS, navigate to the **FIREWALL** view and click on the NSv instance in the left pane.
- 5 In the center pane, go to the Manage > Register/Upgrades > Firmware Upgrade page.
- 6 Click the **Choose File** button to select the firmware you just downloaded, then click **Upgrade from Local File**.

# Registering an NSv Manually in a Closed Network

() **NOTE:** This registration method uses Manual Upgrade and is **not** recommended for normal product registration on products that have internet access. See Registering the NSv Appliance from SonicOS on page 25 for the recommended registration method on products with internet access.

In a closed network, your NSv does not have internet access and cannot communicate directly with the SonicWall licensing server. To complete the registration process, you need to obtain information from MySonicWall and then log into SonicOS on your NSv and enter that information.

NOTE: System functionality is extremely limited if registration is not completed. See Using SonicOS on an Unregistered NSv on page 33 for more information.

#### To register an NSv virtual firewall in a closed network environment:

- 1 Log into your NSv appliance and navigate to the **MONITOR | System Status** page.
- 2 Make a note of the **GUID**, or leave the page open in your browser. The **GUID** is displayed in the **System Information** section.

NOTE: If the GUID is already updated on MySonicWall, it is necessary to de-register and restart the NSv. See Deregistering Your NSv on page 30. If your NSv cannot connect with MySonicWall, contact Technical Support to de-register the GUID from MySonicWall.

- 3 In another browser tab or window, log into your MySonicWall account.
- 4 Navigate to My Products and click on the entry for your NSv appliance.
- 5 Click on the + next to GUID. Enter the GUID into the dialog box and click Update.
- 6 To get the **License Keyset**, first click the key icon. The **License Keyset** is displayed. This is a binary representation of all the service licenses activated on your NSv.
- 7 Select the License Keyset and copy it to your clipboard.
- 8 Log into your NSv appliance or return to that browser window if still logged in.
- 9 Navigate to the **MANAGE | Licenses** page in SonicOS.
- 10 Under Manual Upgrade, paste the License Keyset into the Enter keyset field.

Manual Upgrade			
Enter keyset			
Please also specify fol	owing info:		
Serial Number:			
Registration Code:			
APPLY			

- 11 In the **Serial Number** and **Authentication Code** fields, enter the corresponding values you received after purchasing your NSv Series virtual firewall.
- 12 In the **Registration Code** field, enter the registration code you received when you did the initial registration in MySonicWall to obtain the OVA file. See **Obtaining the OVA from MySonicWall** on page 12 for more information.
- 13 Click APPLY to register the NSv and activate the licensed services.
- 14 Click ACCEPT.

Your NSv virtual firewall is now registered.

# Deregistering Your NSv

You can deregister your NSv directly from the SonicOS management interface. Deregistration puts the virtual appliance into the unregistered state and deletes the binding between it and its serial number in MySonicWall. Then you can use the serial number to register the same or another NSv instance. Only one NSv instance is allowed per serial number.

(i) NOTE: Only an NSv which was registered online can be deregistered. If the NSv was registered using the offline method, deregistration is not supported. Contact Technical Support for assistance.

#### To deregister an NSv:

- 1 Log into the SonicOS management interface on your NSv virtual appliance.
- 2 Navigate to the Updates | Setting page in the MANAGE view.
- 3 Select **Export Configuration** from the **Import/Export Configuration** drop-down list to export your current configuration settings before deregistering your NSv.

● Import/Export Configuration		
Import Configuration		
Export Configuration (h) ild Date		

This makes it possible to import the settings to another NSv instance.

CAUTION: Be sure to export your configuration settings before deregistering your NSv. You cannot recover them after deregistration.

- 4 Navigate to the **Updates | Licenses** page in the **MANAGE** view.
- 5 Under Manage Security Services Online, click the DEREGISTER button.



6 Click **OK** in the confirmation dialog.

This will deregister the unit an Click "OK" to proceed?	d put it back to unregistered state.
	OK Cancel

If deregistration is successful, the virtual appliance will return to the unregistered state. You can see the **Register** link in the top banner of SonicOS and the message "Your SonicWall is not registered" on the **MONITOR | System > Status** page.

If deregistration fails, an error message is displayed in the status bar at the bottom of the SonicOS management interface.

# Converting a Free Trial License to Full License

A SonicWall NSv instance installed as a 30-day free trial can easily be converted to a full production licensed NSv instance.

#### To convert your free trial to a production version:

- 1 Purchase a SonicWall NSv license from a distributor. You will receive a fulfillment email with the new serial number and authentication code.
- 2 Log into SonicOS on your free trial instance.
- 3 Navigate to the Updates | Licenses page in the MANAGE view.
- 4 Under Manage Security Services Online, click the DEREGISTER button.
- 5 Click **OK** in the confirmation dialog. The virtual firewall returns to the unregistered state.

6 Click the **Register** link in the top banner or on the **MONITOR | System > Status** page.

SONICWALL	Network Security Virtual	MONITOR	INVESTIGATE	MANAGE		<u>Register</u>   Help   Logout 신)
Current Status System Status User Sessions	The password ha: Log messages car     (i) Cloud backup not	sn't been changed. nnot be sent because enabled - Click here	e you have not speci to enable.	fied an outbound s	SMTP server address.	Hode: Configuration ►
	System Inform	nation	Show Mu	lti-Core Monitor	Security Services	Show All License Information
	Model:	NSv Unlicensed			Nodes/Users:	10 Nodes (0 in use)
	Product Code:	70000			SSL VPN Nodes/Users:	2 Nodes (0 in use)
	GUID:	Built des Finder			Your SonicWall is not regi	stered.
	Firmware Version:	SonicOS Enhance	ed 6.5.0.2-8v-sonicosv-	374cf82cf8	Click here to Register your Se	onicWall.

7 Enter your MySonicWall credentials and then click LOGIN.

MySonicWall username/email			
Password			
	LOGIN		

- 8 Enter the **Serial Number** and **Authentication Code** you received after purchasing your NSv Series instance.
- 9 Click SUBMIT.
- 10 The licensing server acquires the necessary information from the NSv Series appliance and your MySonicWall account. If asked, you can specify a **Friendly Name** or **Product Group** for the NSv Series appliance.
- 11 Acknowledge the registration completion notification by clicking the **OK** button.

SonicOS automatically restarts and then displays the login page.

12 Log into SonicOS.

In the **MONITOR** view, the **System > Status** page now shows your licensed security services, and the **Register** link is no longer displayed.

13 In the **MANAGE** view on the **Updates** | **Licenses** page, you can activate security service free trials, enable available services, and click to purchase other services you want.

SonicOS Management

**Topics:** 

- Managing SonicOS on the NSv Series on page 33
- Using SonicOS on an Unregistered NSv on page 33
- Using System Diagnostics in SonicOS on page 36

# Managing SonicOS on the NSv Series

The X1 interface is the default WAN Interface and is set to use DHCP addressing by default, with HTTPS management enabled. To ease testing, you can utilize a DHCP server on the X1 connected network. If DHCP is not available, use the console to access the CLI and configure a static IP address.

The X0 interface is the default LAN interface, and also has HTTPS management enabled. Its IP address is set to 192.168.168 by default. You can map this interface to your own network during initial deployment of the OVF template. After deployment, you can reconfigure the IP address to an address in your network.

To change the configuration of either X1 or X0, refer to Using the ESXi Remote Console to Configure the WAN or LAN Interfaces on page 38.

#### To log into SonicOS for management of the NSv:

1 Point your browser to either the LAN or WAN IP address. The login screen is displayed.

When the X1 WAN interface is using DHCP addressing, DNS is also enabled. You can generally access the WAN address from any machine in your network.

If you have an existing network on 192.168.168.0/24 in your environment, you can access the default IP address of the X0 LAN interface of your NSv Series from a computer on that network for SonicOS management. The NSv Series X0 IP address is 192.168.168.168 by default.

2 Enter the administrator credentials (default *admin / password*) and press Enter.

The SonicOS management interface is displayed. You can navigate and update the configuration just as you would with any SonicWall network security appliance.

## Using SonicOS on an Unregistered NSv

The SonicOS management interface provides fewer features on an unregistered NSv Series appliance than on a registered NSv. The Available SonicOS Pages on Unregistered NSv table provides a summary of the available features on an unregistered NSv.

Top Level View	Page Group	Page Within Group	Description
MONITOR	System Status	n/a	System information, Node license, Alerts, Network interface settings
	User Sessions	SSL-VPN Sessions	User sessions connected via SSL VPN
		Active Users	Active user session information; Logout button for users
		Active Guest Users	Active guest user session information; Logout button for guest users
		User Monitor	Graph of logged in users over time for client logins and web based logins
INVESTIGATE	Event Logs	n/a	Log event table, dynamically updated, filterable, searchable, one-click details
	Connection Logs	n/a	Connection log, source/destinations, protocols, bytes transferred, filterable, searchable, flush option
	SD-WAN Connection Logs	n/a	Connection log, source/destinations, protocols, bytes transferred
	Appflow Logs	n/a	Requires App Visualization license, which requires registration
	System Diagnostics	n/a	TSR access and Diagnostic tools: Check Network Settings Ipv6 Check Network Settings Connections Monitor Multi-Core Monitor Core Monitor Link Monitor Packet Size Monitor DNS Name Lookup Find Network Path Ping Core 0 Process Monitor Real-time Black List Lookup Reverse Name Resolution Connection Limit TopX TraceRoute PMTU Discovery Web Server Monitor User Monitor See Using System Diagnostics in SonicOS on page 36 for information.
MANAGE	Licenses	n/a	Node license information, MySonicWall access, Manual Upgrade
	Firmware & Backups	n/a	Firmware versions, Local Backup, Settings import/export, Settings options to send to SonicWall Support

#### Available SonicOS Pages on Unregistered NSv

Top Level View	Page Group	Page Within Group	Description
	Restart	n/a	Restarts the virtual firewall after confirmation
	Appliance	Base Settings	Firewall name, Admin username and password, Login security, Multiple administrator, Web/SSH/GMS management, Client certificate checks, and Language settings
		SNMP	Enable SNMP
		Certificates	View and Import certificates, Generate certificate signing requests, SCEP for issuing certificates to endpoint devices
		System Time	Time and time zone, NTP server settings
		System Schedules	Schedule settings
	Network	Interfaces	Interface settings, Traffic statistics
		Failover & Load Balancing	Enable load balancing, LB Group configuration, Statistics
		Zones	Zone settings
		VLAN Translation	VLAN Translation configuration
		DNS	IPv4 DNS settings
		DNS Proxy	Enable DNS Proxy, DNS proxy and cache settings
		Routing	Route policies, OSPF, RIP
		ARP	Static ARP entries, ARP settings and cache
		Neighbor Discovery	Static NDP entries, NDP settings and cache
		MAC-IP Anti-spoof	Interface anti-spoof settings, cache, detected list
		DHCP Server	Enable DHCPv4 Server, Configure lease scopes, View current leases
		IP Helper	Enable IP Helper, Configure relay protocols and policies, Refresh DHCP relay leases
		Web Proxy	Proxy forwarding, User proxy servers
		Dynamic DNS	DDNS Profile settings
		SD-WAN module	
		AWS configuration	
	Log Settings	Base Setup	Logging and alert levels, per-category settings
		SYSLOG	Syslog settings, servers
		Automation	Email settings for sending logs and alerts, Solera Capture Stack

#### Available SonicOS Pages on Unregistered NSv

#### Available SonicOS Pages on Unregistered NSv

Top Level View	Page Group	Page Within Group	Description
		Name Resolution	DNS and NetBios methods
		Analyzer	Requires Analyzer license, which requires registration
	Legal	n/a	End User Product Agreement
	API		

# Using System Diagnostics in SonicOS

The **Tools | System Diagnostics** page on the **INVESTIGATE** view provides several diagnostic tools that help troubleshoot various kinds of network problems and process monitors, to help you resolve many of the common issues you might face. Each tool is different from the others so the display changes with the tool. However, some of the data management functions are common among the tools.

Nearly all the tools have these buttons at the bottom of the window:

ACCEPT	CANCEL		REFRESH
Button		Function	
ACCEPT		Saves any changes you made to the diagnostic support report or diagn	ostic tool.
CANCEL		Cancels any changes you initially made to the diagnostic support repordiagnostic tool.	t or

Some tools have management functions to help you manage lists of data. These operate much like the options on the other logs and reports.

Refreshes the data being displayed in the **Diagnostic Tools** section.

• Search

REFRESH

- Filter
- Toggling between views (IPv4 vs. IPv6, for example)
- Refresh
- Export
- Clear

Select the tool you want from the **Diagnostic Tool** drop-down menu in the **Tools | System Diagnostics** page. The Check Network Settings tool is described below. See the *SonicOS for Network Security Virtual 6.5 Investigate* administration documentation for complete information about the available diagnostic tools.

### **Check Network Settings**

Diagnostic To	ols					
Diagnostic Tool:	Check	Network Settings		•		
Check Network S	ettings					
General Networ	k Conne	ection				
Server		IP Address	Test Results	Notes	Timestamp	Progress Test
Default Gatewa	ay (X1)	> 10.203.28.1				TEST
DNS Server 1		→ 10.200.0.52				TEST
DNS Server 2		→ 10.200.0.53				TEST
Security Manag	ement					
Server		IP Address	Test Results	Notes	Timestamp	Progress Test
V My SonicWall		N/A				TEST
License Manage	er	N/A				TEST
TEST ALL SEL	ECTED					

**Check Network Settings** is a diagnostic tool that automatically checks the network connectivity and service availability of several pre-defined functional areas of the NSv Series, returns the results, and attempts to describe the causes if any exceptions are detected. This tool helps you locate the problem area when users encounter a network problem.

Specifically, Check Network Settings automatically tests the following functions:

- Default Gateway settings
- DNS settings
- MySonicWall server connectivity
- License Manager server connectivity
- Content Filter server connectivity

The return data consists of two parts:

- Test Results Provides a summary of the test outcome
- Notes Provides details to help determine the cause if any problems exist

The Check Network Settings tool is dependent on the **Network Monitor** feature available on the **Tools** | **Network Probes** on the **INVESTIGATE** view. Whenever the **Check Network Settings** tool is being executed (except during the Content Filter test), a corresponding Network Monitor Policy appears on the **Tools** | **Network Probes** page, with a special diagnostic tool policy name in the form:

diagTestPolicyAuto <IP address/Domain name> 0

(i) NOTE: Log messages show the up/down status of some of these special network objects. These objects, however, live for only three seconds and then are deleted automatically.

To use the **Check Network Settings** tool, first select it in the **Diagnostic Tools** drop-down list and then click the **Test** button in the row for the item that you want to test. The results are displayed in the same row. A green check mark signifies a successful test, and a red X indicates that there is a problem.

To test multiple items at the same time, select the **Server** checkbox at the top of the table to select all items or select the checkbox for each desired item and then click **TEST ALL SELECTED**.

If probes fail, you can click the blue arrow to the left of the I**P Address** field of the failed item to jump to the configuration page to investigate the root cause.

5

# Using the Virtual Console

**Topics:** 

- Using the ESXi Remote Console to Configure the WAN or LAN Interfaces on page 38
- Using the NSv Management Console on page 42
- Using SafeMode on the NSv on page 50

# Using the ESXi Remote Console to Configure the WAN or LAN Interfaces

You can use the ESXi remote console to set the IP address and network settings of the NSv Series interfaces, to change between static and DHCP addressing, and to enable SonicOS management on your NSv Series instance.

For example, depending on your network environment, you might need to configure a static IP address on your NSv Series X1 WAN interface. If you do so, you need to configure HTTPS management to allow remote management over the WAN.

The NSv Series X0 IP address is 192.168.168.168 by default. If your LAN network uses a different IP address range, then you may want to configure your NSv Series X0 IP address with an address in your existing LAN network. This will allow you to manage SonicOS from a computer on your LAN.

The *ESXi Remote Console* allows you to log into the NSv Series console and use the command line interface (CLI) to configure these network settings.

NOTE: To type within the console window, click your mouse inside the window. To regain control of your mouse, press Ctrl+Alt.

#### To use the console to enable SonicOS management:

- 1 Log into vSphere or vCenter and select your NSv Series instance in the left pane.
- 2 Do one of the following to open the ESXi remote console:
  - Click on the image of the console to access the console in browser window.

🖧 SonicWall_Network_Sec			
Summary N	Ionitor	Configure	
		Guest OS: Compatibility: VMware Tools	
n Powered On		DNS Name: IP Addresses:	
Launch Remote C	Console	Host:	

• Click Launch Remote Console.

- Click Actions > Open Remote Console.
- 3 Click inside the console window.

**NOTE:** Press **Ctrl+Alt** to regain control of your mouse, or with the browser access method simply move your mouse away from the console area.

4 Log in using the administrator credentials.

```
      Product Model
      : NSu Unlicensed

      Product Code
      : 70000

      Firmware Version
      : SonicOS Enhanced 6.5.0.2-8u-sonicosu-37--25793204

      Serial Number
      : 00000000000

      X0 IP Addresses
      : 192.168.168.168

      Not licensed: product not enabled. Register with MySonicWall for licensing.

      **** Startup time:
      04/25/2018 18:14:27.048 ****

      Copyright (c) 2018 SonicWall
```

5 To use a static IP address for the WAN, type the following sequence of commands to enable a static IP and management access on the X1 WAN interface. The command prompt will change as you enter or exit different command levels. This command sequence shown below uses example IP address settings in the 10.203.26.0 network, which should be replaced with the correct settings for your environment.

```
configure t
interface x1
ip-assignment WAN static
ip 10.203.26.228 netmask 255.255.255.0
gateway 10.203.26.1
exit
management https
management ping
management ssh
exit
commit
```

After entering commit, the console displays Applying changes and other status information, then displays the config prompt. Type exit to return to the admin command level and prompt.

```
admin@000000000000> configure t
config(00000000000)# interface x1
(edit-interface[X1])# ip-assignment WAN static
(edit-WAN-static[X1])# ip 10.203.26.228 netmask 255.255.0
(edit-WAN-static[X1])# gateway 10.203.26.1
(edit-WAN-static[X1])# exit
(edit-interface[X1])# management https
(edit-interface[X1])# management ping
(edit-interface[X1])# management ssh
(edit-interface[X1])# exit
config(00000000000)# commit
× Applying changes...
% Status returned processing command:
   commit
% Changes made.
config(00000000000)#
```

6 To return to DHCP for the WAN address, type the following sequence of commands to enable DHCP and management access on the X1 WAN interface. The command prompt will change as you enter or exit different command levels.

```
configure t
interface x1
ip-assignment WAN dhcp
exit
management https
management ping
management ssh
exit
commit
```

After entering commit, the console displays Applying changes and other status information, then displays the config prompt. After a few seconds, the assigned DHCP address is displayed. You can access the SonicOS web management interface at that address.

7 You can use the show status command at the admin prompt to view the assigned IP address for the X1 (WAN) interface and other information.

1					
admin@000000000	000> show statu:	S			
	====				
Sustem Information:					
	====				
Model:		NSv Unlicensed			
Product Code:		70000			
Serial Number:					
Authentication	Code:				
GUID:		COMPLEX PRODUCE BALL OF MUSICAL			
Firmware Versio	n:	SonicOS Enhanced 6.5.0.2-8v-sonicosv-3725793204			
Safemode Versio	n:	6.5.0.0			
RUM Version:		5.0.0.0 2.254 - 2.4 2500 MUL Intel(D) Manu(D) CDU DE 2000 - 2.0.2 (0000			
Total Moreover		3.35% - Z X Z555 MHZ INTEILKI XEONIKI UPU E5-Z650 03 @ Z.60GHZ			
Suster Tire:		D GD NHT 04.26.2018 12:41:46			
Jystem IIme.		01/20/2010 12.11.10 0 Date 18.30.02			
Connections:		Peak: 77 Current: A Max: 512			
Connection Usar	e:	$\hat{\mathbf{h}}$ $\hat{\mathbf{h}$ $\hat{\mathbf{h}}$ $\hat{\mathbf{h}}$ $\hat{\mathbf{h}}$ $\hat{\mathbf{h}}$ $\hat{\mathbf{h}}$ $\mathbf{h$			
Last Modified B	u:	admin CLI 04/26/2018 12:37:45			
	2				
Security Servic	es:				
Nadaa dlaana t		10 Natas(Q in usa)			
NUGESZUSERS:	0000	$\frac{10}{2}$ Nodes (0 in use)			
llintual Assist	Nodes/licens'	1  Nodes(A  in use)			
Registration St.	atus:	Your SomicWall is not registered			
negrourderon ou	u vus.	ibai obnickati is not registerea			
Network Interfa	ces:				
Maria		The Office			
HAME VO(LON)	102 160 160 160	LINK Status P. 10 Chao Full Dualey			
	10 203 26 229	10 Gbps Full Duplex			
X2(Imassigned)	A A A A	10 Gbns Full Dunley			
X3(Ilmassigned)	0.0.0.0	10 Gbps Full Duplex			
X4(Ilmassigned)	0.0.0.0	10 Gbps Full Duplex			
X5(Unassigned)	0.0.0.0	10 Gbps Full Duplex			
X6(Unassigned)	0.0.0.0	10 Gbps Full Duplex			
X7(Unassigned)	0.0.0.0	10 Gbps Full Duplex			
admin00000000					

8 To change the X0 LAN static IP address, use the following commands:

**NOTE:** SonicOS HTTPS management is enabled by default on the X0 interface.

For a static IP address in an example 10.10.10.0/24 LAN network, enter:

```
configure t
interface x0
ip 10.10.10.100 netmask 255.255.255.0
exit
exit
commit
```

9 When IP address configuration and management settings are complete, type restart to reboot NSv Series with the new settings.

**NOTE:** Press **Ctrl+Alt** to regain control of your mouse.

After configuring an IP address and enabling management, you can log into SonicOS on your NSv Series instance from a browser, or ping the virtual appliance from a command window or other application.

# Using the NS<sub>v</sub> Management Console

The NSv management console provides options for viewing and changing system and network settings, running diagnostics, rebooting SonicOS, and other functions. The NSv management console can be accessed after you log into the ESXi remote console.

#### To access and navigate the management console:

- 1 Log into the ESXi remote console by selecting your NSv in the vSphere or vCenter interface and clicking Actions > Open Remote Console, then clicking inside the console window. Use your initial login credential (admin / password) to get to the SonicOS prompt.
- 2 Press Ctrl+s and then press the spacebar to toggle between the ESXi remote console and the NSv management console. That is, press the Ctrl key and 's' key together, then release and press the spacebar.

Menu- System Info Management Network Test Management Network Diagnostics NTP Server Lockdown Mode System Update Reboot I Shutdown About	System Info Model Product Code Serial Number Model Name SonicOS Version GUID System Time Up Time	: SonicWall Network Security - Virtual Series : 70000 : : NSU Unlicensed Beta : 6.5.0.0 : : Tue 2018-03-27 20:58:06 UTC : 41 minutes 35 seconds : 41 minutes
rodz	Sonic0S	· 1.1 Imin 1.1 Smin 1.0 Iumin
Up / Down to select items TAB to move between views Enter to action/edit an item	To log into the So https://192.168.	micWall web interface visit:
SonicWall (c) 2018   Uptime 41 mi	nutes	ICtrl-s spacebar] to switch console

- 3 The main menu is displayed in the side menu (left pane). Use the up/down arrow keys to move the focus between menu items. As the focus shifts, the right pane displays the options and information for that menu item. The currently selected item is highlighted in black.
- 4 Press the **Tab** key to move the focus from side menu to the main view (right pane), or vice versa.
- 5 In the main view, use the up/down arrow keys to move the focus between options. Items shown inside square brackets denote actionable items.



6 To select an option for editing or to choose the associated action, use the up/down arrow keys to move the focus to the editable/actionable items and press the **Enter** key.

An edit/selection dialog is displayed in the middle of the main view below the option list. Some dialogs have selectable actions and some are only for information:



Some dialogs are for input:



7 Use the arrow keys as needed to move between selections in the dialog. To change a value, press Backspace to erase each character, then type in the new value. When ready, press Enter to commit the change or perform the selected action. You can dismiss the dialog by pressing Esc.

The NSv management menu choices are described in the following sections:

- System Info on page 44
- Management Network on page 45
- Test Management Network on page 45
- Diagnostics on page 47
- NTP Server on page 48
- Lockdown Mode on page 48
- Reboot | Shutdown on page 49
- About on page 49
- Logs on page 50

## System Info

Menu	System Info	
System Info	Model	: SonicWall Network Security - Virtual Series
Management Network	Product Code	: 70000
Test Management Network	Serial Number	
Diagnostics	Model Name	: NSv Unlicensed Beta
NTP Server	SonicOS Version	: 6.5.0.0
Lockdown Mode	GUID	
System Update		
Reboot   Shutdown	System Time	: Tue 2018-03-27 20:58:06 UTC
About	Up Time	: 41 minutes 35 seconds
Logs	CPU Load	: 1.1 1min 1.1 5min 1.0 10min
	SonicOS	: Operational
Un / Down to collect items		
TOP to move between wiews		
Fator to action (adit an item	To log into the S	onichall web interface wight:
Enter to action/cuit an item	https://102.169	UNICWAII WED INCEPTALE VISIC,
	neeps 152.100.	
Somichall (c) 2019   Untime 41 mix	wtee	[Ctrl_a anachar] to quitch correcte
Sourceare (C) 2010 I Obrime At wit	iu ies	tetri-s spacebari to switch consule

Some of the information in the **System Info** screen is dynamic. The following information is displayed:

- Model This is the model of the NSv appliance.
- **Product code** This is the product code of the NSv appliance.
- Serial Number The serial number for the appliance; this is a number unique to every NSv instance deployed. This number can be used to identify the NSv appliance on MySonicWall.
- **Model Name** This is the model name of the NSv appliance.
- **SonicOS Version** This is the currently running SonicOS version of the NSv appliance.
- **GUID** Every NSv instance has a GUID which is displayed here.
- System Time This is the current system time on the NSv appliance.
- Up Time This is the total time that the NSv appliance has been running.
- Average Load This shows the average CPU load for the last 1 minute, 5 minutes and 10 minutes. You can change the Average load time durations to view the CPU load over longer or shorter time periods.
- SonicOS This presents the current state of the SonicOS service on the NSv. Operational is displayed here when the SonicOS service is running normally, Not Operational when there is a problem with the service and Operational (debug) if the service is currently running in debug mode.

### Management Network

VMRC - 📕 - 🖶 🖽			«
Menu System Info Managgement Network	Management Network Management interface	X1	
Test Management Network Diagnostics	IPv4 Address Netmask	10.202.9.244 255.255.255.0	
Lockdown Mode Reboot   Shutdown	IPu6 Address Gateway	600. fe80::250:56ff:fe9f:c394 10.202.9.1	
About Logs	DNS 1 DNS 2	8.8.8.8 8.8.4.4	
Up / Down to select items TAB to move between views Enter to action/edit an item	To log into the SonicWall w		
Space to hide/show side menu	https://10.202.9.244/		
SonicWall (c) 2018   Uptime 9 min	utes	[Ctrl-s spacebar] to swit	ch console

In the **Management Network** screen, the network settings displayed in the white text are read-only except when the management console is in SafeMode. In SafeMode, you can configure these settings.

- Management Interface This is the current interface serving as the management interface. This defaults to X1.
- IPv4 Address This is the IPv4 address currently assigned to the management interface.
- Netmask This is the netmask currently assigned to the management interface.
- Mac Address This is the MAC address of the management interface.
- IPv6 address This is the IPv6 address currently assigned to the management interface.
- Gateway This is the default gateway currently in use by the NSv appliance.
- **DNS** This is a list of the DNS servers currently being used by the NSv appliance.

### **Test Management Network**

Menu- System Info Management Network Test Management Network Diagnostics NTP Server Lockdown Mode System Update Reboot I Shutdown About Logs	Test Management Network Ping Nslookup [ Nslookup ]
	Enter IP address 192.168.8.1_ Confirm <enter> Cancel <esc></esc></enter>
Up / Down to select items TAB to move between views Enter to action/edit an item	
SonicWall (c) 2018   Uptime 3 minu	tes [Ctrl-s spacebar] to switch console

The **Test Management Network** screen provides the **Ping** and **Nslookup** tools to test connectivity between the management interface and the local network. **Ping** is used to test whether hosts in the network are reachable. **Nslookup** is available for sending DNS queries from the NSv appliance.

#### To use Ping:

- 1 Select **Test Management Network** in the Menu and press **Tab** to move the focus into the **Test Management Network** screen.
- 2 Select **Ping** to highlight it and then press **Enter** to display the **Enter IP address** dialog.
- 3 Navigate into the dialog, press **Backspace** to clear the current value, and then type in the IP address that you want to ping.
- 4 Press Enter.

The ping output is displayed in the **Ping host** dialog.



5 Press the **Esc** key to close the dialog.

#### To use Nslookup:

- 1 Select **Test Management Network** in the Menu and press **Tab** to move the focus into the **Test Management Network** screen.
- 2 Select **Nslookup** to highlight it and press **Enter** to display the **Enter hostname** dialog.

Menu- System Info Management Network Test Management Network Diagnostics NTP Server Lockdown Mode System Update Reboot I Shutdown About Logs	-Test Management Network- Ping [ Ping Nslookup [ Nsloo	յ ] հար]
Up / Down to select items TAB to move between views Enter to action/edit an item	Enter hostname sonicwall.com Confirm <enter> Cancel <esc></esc></enter>	
SonicWall (c) 2018   Uptime 5 minu	tes [Ctrl-s spacebar] to swite	h consol

- 3 Navigate into the dialog, press **Backspace** to clear the current value, and then type in the hostname that you want to look up with a DNS query.
- 4 Press Enter.

The Nslookup query results are displayed in an information dialog. You can scroll up and down within the dialog by using the up/down arrow keys.



5 Press the **Esc** key to close the dialog.

### Diagnostics



In the **Diagnostics** screen, you can send diagnostics to SonicWall Technical Support. This has the same functionality as clicking **SEND DIAGNOSTIC REPORTS TO SUPPORT** in the **INVESTIGATE | Tools | System Diagnostics** page of the SonicOS web management interface.

() NOTE: Your NSv appliance must have internet access to send the diagnostics report to SonicWall Support.

To send the diagnostics report, select **Send** in the main view to highlight it, then press **Enter**. A dialog box showing the diagnostics send output is displayed. The last message indicates success or failure.



Press the Esc key to close the dialog.

Any errors during the Send process are displayed in the Send diagnostics dialog box.

Common reasons for the report failing to send include:

- Misconfigured/missing default gateway
- Misconfigured/missing DNS servers
- Inline proxy

**NOTE:** The Send Diagnostics tool does not currently work through HTTP proxies.

### NTP Server



In the **NTP Server** screen, you can synchronize with an NTP server. For complete NTP Server configuration options, log into the SonicOS management interface and navigate to the **MANAGE | Appliance > System Time** page.

The **NTP Server** screen displays the following information:

- Sync with NTP server This button forces the NSv appliance's NTP client to perform a sync with the configured NTP server(s).
- **Current time** The current time on the NSv appliance.
- Network time enabled A Yes/No value determining whether the NTP client is currently configured to keep in sync with an NTP server.
- NTP synchronized A Yes/No value determining if the NSv appliance is currently synchronized with the configured NTP server(s).

### Lockdown Mode

-Menu	Lockdown Mode		
System Info	Enable lockdown	Enable	
Management Network			
Test Management Network			
Diagnostics			
NTP Server			
Lockdown Mode			
Reboot   Shutdown			
About			
Logs			

In the **Lockdown Mode** screen, you can enable *Strict Lockdown* mode. When enabled, the management console is effectively disabled. A dialog box that cannot be closed is permanently displayed on the management console. This prevents any person from accessing the management console.

To enable Strict Lockdown mode, select **Enable** and then press **Enter**.

**CAUTION:** Be careful about enabling Strict Lockdown mode. Strict Lockdown mode cannot be disabled.

### **Temporary Lockdown Mode**

A temporary lockdown mode can be enabled and disabled in SonicOS on the **MANAGE | Appliance > Base** Settings page. You can enable lockdown mode by clearing the Enable management console checkbox under the Advanced Management section, and can disable lockdown mode by selecting the checkbox. Click ACCEPT after each change.

The management console will automatically be enabled/disabled a few seconds after it has been enabled/disabled in the SonicOS web interface page.

## Reboot | Shutdown



The **Reboot | Shutdown** screen provides functions for rebooting the NSv appliance, enabling debug mode, and enabling SafeMode. To perform an action, position the focus and then press **Enter** to select the desired action. Select **Yes** in the confirmation dialog, then press **Enter** again.

The actions available on the **Reboot | Shutdown** screen are:

- **Reboot SonicWall** Restarts the NSv Series virtual appliance with current configuration settings.
- **Shutdown SonicWall** Powers off the NSv Series virtual appliance.
- **Boot with factory default settings** Restarts the NSv Series virtual appliance using factory default settings. All configuration settings will be erased.
- **Boot SonicWall into debug** Restarts the NSv Series virtual appliance into debug mode. Normally this operation is performed under the guidance of SonicWall Technical Support.
- **Boot SonicWall into safemode** Puts the NSv Series virtual appliance into SafeMode. For more information, see Using SafeMode on the NSv on page 50.

### About

Menu	About	
System Info	SonicWall SonicCore	
Management Network	Version	6.5.0
Test Management Network	Build name	6.5.0-288+SonicCore-SonicOsV-6.5-Daily
Diagnostics		
NTP Server		
Lockdown Mode		
Reboot   Shutdown		
About		

The About screen provides information about the software version and build.

### Logs

The **Logs** screen displays log events for the NSv appliance.

-Menu	Apr 25 20:31:54 localhost Automatic secure crash analysis reporting is enabled
System Info	Apr 25 20:31:54 localhost Periodic secure diagnostic reporting for support purposes is enabled
Management Network	Apr 25 20:31:54 localhost Initializing SonicWall support services
Test Management Network	Apr 25 20:31:52 localhost Completed configuring the operating environment for SonicOS
Diagnostics	Apr 25 20:31:52 localhost Completed configuring the operating environment for SonicOS
NTP Server	Apr 25 20:31:51 localhost Model: "NSv 800" supports 8 CPU, current CPU count is only 2, for im
Lockdown Mode	Apr 25 20:31:51 localhost Total memory installed 10237296 Kb
System Update	Apr 25 20:31:51 localhost CPU flags: fpu ume de pse tsc msr pae mce cx8 apic sep mtrr pge mca
Reboot   Shutdown	Apr 25 20:31:51 localhost CPU count: 2, Model "Intel(R) Xeon(R) CPU E5-2690 v3 @ 2.60GHz"
About	Apr 25 20:31:51 localhost Configuring the operating environment for SonicOS
Logs	Reboot
	Apr 25 20:29:50 localhost Unconfigure the operating environment for SonicOS
	Apr 25 20:04:26 localhost Automatic secure crash analysis reporting is enabled
	Apr 25 20:04:26 localhost Periodic secure diagnostic reporting for support purposes is enabled
	Apr 25 20:04:26 localhost Initializing SonicWall support services
	Apr 25 20:04:25 localhost Completed configuring the operating environment for SonicOS
	Apr 25 20:04:25 localhost No system information file available
	Apr 25 20:04:25 localhost Total memory installed 10237296 Kb
	Apr 25 20:04:25 localhost CPU flags: fpu ume de pse tsc msr pae mce cx8 apic sep mtrr pge mca
	Apr 25 20:04:25 localhost CPU count: 2, Model "Intel(R) Xeon(R) CPU E5-2690 v3 @ 2.60GHz"
	Apr 25 20:04:24 localhost Configuring the operating environment for SonicOS
Up / Down to select items	
TAB to move between views	
Enter to action/edit an item	
Space to hide/show side menu	
	Arrou keys: Navigate view Current Line: 1 Lines: 21
SonicWall (c) 2018   Uptime 23 ho	urs, 48 minutes [Ctrl-s spacebar] to switch console

# Using SafeMode on the $NS_{v}$

The NSv appliance will enter SafeMode if SonicOS restarts three times unexpectedly within 200 seconds. When the NSv appliance is in SafeMode, the appliance starts with a very limited set of services and features enabled. This is useful when trying to troubleshoot issues. The NSv appliance can also be configured to boot into SafeMode by using the **Reboot | Shutdown** screen.

In SafeMode, some of the features the management console provides are different in the following ways:

- Configurable interfaces
- Configurable default gateway
- Configurable DNS servers

**NOTE:** Changes made to interfaces in SafeMode are *not* persistent between reboots.

When the NSv is in SafeMode, the SonicOS service is one of the services that is not enabled and is shown as *Not operational* on the SafeMode **System Info** screen.

The SafeMode Management Console always starts with the **System Info** screen.

-Safemode menu-	-System Info					
System Info	Mode 1	: SonicWall Network Security - Virtual Series				
Management Network	Product Code	: 70000				
Test Management Network	Serial Number					
Diagnostics	Model Name	: NSv Unlicensed Beta				
NTP Server	SonicOS Version	: 6.5.0.0				
System Update	GUID	: Second a second second second second second F				
Reboot   Shutdown						
About	System Time	: Tue 2018-03-13 21:57:22 UTC				
Logs	Up Time	: 6 hours 33 minutes 19 seconds				
	CPU Load	: 0.0 1min 0.0 5min 0.0 10min				
	SonicOS	: Not operational				
Up / Down to select items						
TAB to move between views						
Enter to action/edit an item	SonicWall is in saf	emode, to access recovery options visit:				
	http://192.168.14.2	10/				
SonicWall (c) 2018   Uptime 6 hour	s, 32 minutes	[safemode]				

NOTE: To exit SafeMode, disable it on the Reboot | Shutdown screen or deploy a new firmware image. See Disabling SafeMode on page 52 and Installing a New SonicOS Version in SafeMode on page 56 for more information.

#### **Topics:**

- Enabling SafeMode on page 51
- Disabling SafeMode on page 52
- Configuring the Management Network in SafeMode on page 53
- Installing a New SonicOS Version in SafeMode on page 56
- Downloading Logs in SafeMode on page 57

### **Enabling SafeMode**

SafeMode can be enabled from the management console.

#### To enable SafeMode:

- 1 Access the NSv management console as described in Using the NSv Management Console on page 42.
- 2 In the console, select the **Reboot | Shutdown** option and then press **Enter**.

3 Navigate down to the **Boot SonicWall into safemode** option to highlight **Enable**, and then press **Enter**.



- 4 Select **Yes** in the confirmation dialog.
- 5 Press Enter.

The NSv immediately reboots and comes back up in SafeMode.



**NOTE:** In SafeMode, the web interface is served from an HTTP server. The HTTPS server is not started in SafeMode.

### **Disabling SafeMode**

#### To disable SafeMode:

- 1 In the SafeMode menu in the NSv management console, select the **Reboot | Shutdown** option and press **Enter**.
- 2 In the **Reboot | Shutdown** screen, navigate down to the **Boot SonicWall into safemode** option to highlight **Disable**, and then press **Enter**.



- 3 Select **Yes** in the confirmation dialog.
- 4 Press Enter.

The NSv immediately reboots and boots up in normal mode.

### **Configuring the Management Network in SafeMode**

When the Management Console is in SafeMode, the **Management Network** screen provides features to configure the NSv appliance interfaces:

- **Management Interface** This is the currently selected interface. This defaults to X1. Use this to select any of the NSv appliance interfaces.
- IPv4 Address The current IPv4 address currently assigned to the Management Interface.
- Netmask The current Netmask assigned to the Management Interface.
- Mac Address The MAC address of the Management Interface.
- IPv6 Address The currently assigned IPv6 address of the Management Interface.
- Gateway The current Default Gateway currently in use by the NSv appliance.
- **DNS** A list of the current DNS servers currently being used by the NSv appliance.

**NOTE:** Changes made to interfaces in SafeMode are *not* persistent between reboots.

**Topics:** 

- Configuring Interface Settings on page 53
- Disabling an Interface on page 55

### **Configuring Interface Settings**

In SafeMode, the **Management Network** screen includes editable and actionable items which are read-only when the management console is in normal mode.

-Safemode menu				
Ogo tos. Tato	Management interface	E	X1	1
Management Network	Third Address		402 460 44 200	
Diagnostics	Irug Haaress Netmask		192.108.14.200 255 255 248 0	
NTP Server	Mac address		AA:Ac:29:ba:Ae:99	
Sustem Undate	IPu6 Address	fe	80::20c:29ff:feba:e	:99
Reboot I Shutdown	Gateway		192.168.8.1	
About	DNS 1			
Logs	DNS 2			
Up ∕ Down to select items TAB to move between views Enter to action∕edit an item	SonicWall is in safemode, to http://192.168.14.200/ or htt	Cancel <e access recove p://192.168.1</e 	sc> ry options visit: .254/	
SonicHall (c) 2018   Untime 5 hou	ne 43 minutes			
Sourcearr (C) 2010 I Ohrime S und	(S) IJ MIMUES			

#### To edit an interface:

1 In the SafeMode Management Network screen, select the Management interface option and then press Enter.

The Select Interface list appears,	displaying all of the interfaces available on the NSv.

Safemode menu	Management interface	r ¥1	1
Management Network	nanagement interrace	1 A1	
Toot Management Noter rk	IPv4 Address	[ 192.168.14.200	
Diagnostics	Netmask	[ 255.255.248.0	
Sustem Undate	IPu6 Address	fe80::20c:29ff:feb	ate99
Reboot I Shutdown	Gateway	[ 192.168.8.1	
About	DNS 1		
Logs	DNS 2		
	Select Interface X0 X2 X3 X4 X5 X6 X7 Confirm <enter></enter>	Cancel <esc></esc>	
Up ∕ Down to select items TAB to move between views Enter to action∕edit an item	SonicWall is in safemode, to a http://192.168.14.200/ or http	access recovery options visit p://192.168.1.254/	:
SonicWall (c) 2018   Uptime 5 hou	rs, 43 minutes		Esafemode

2 Select the interface you wish to edit and press Enter.

The IPv4 and IPv6 addresses, Netmask, MAC address, Gateway, and DNS settings are displayed on the screen above the interface selection dialog.

3 To edit the IPv4 address, select IPv4 Address on the screen and press Enter.

The on-screen dialog displays the current IP address.

- 4 Navigate into the dialog and make the desired changes, then press **Enter** to close the dialog or press **Esc** to cancel and close the dialog.
- 5 Two new buttons appear on the screen after you make changes to an interface setting: **Save changes** and **Cancel**. You can use the **Tab** key to navigate to these buttons.

-Safemode menu	-Management Network		
System Info	Management interface		
Management Network			
Test Management Network	IPv4 Address	[ 192.168.14.210	1
Diagnostics	Netmask	[ 255.255.248.0	1
NTP Server	Mac address	00:0c:29:ba:0e:99	
Sustem Update	IPu6 Address	fe80::20c:29ff:feba:e	
Reboot   Shutdown	Gatewau	[ 192.168.8.1	
About	DNS 1	[ 8.8.8.8	
Logs	DNS 2	[ 8.8.4.4	
Up / Down to select items TAB to move between views Enter to action/edit an item	Save changes SonicWall is in safemode, to http://192.168.14.210/ or ht	access recovery options visit: tp://192.168.1.254/	Cancel
SonicWall (c) 2018   Untime 6 hour	rs. 1 minute		[safemode

**NOTE:** You cannot navigate to the left navigation pane until you either save changes or cancel using these buttons.

Do one of the following:

- To make changes to other settings for this interface, navigate to the desired setting, press Enter, make the changes in the dialog, then press Enter to close the dialog for that setting. Repeat for other settings, as needed.
- If finished making changes to the settings for this interface, press **Tab** to navigate to the **Save changes** button and then press **Enter** to save your changes.
- Press **Tab** to navigate to the **Cancel** button and then press **Enter** to cancel all changes to the settings for this interface.

### **Disabling an Interface**

You can disable an interface while in SafeMode.

#### To disable an interface:

- 1 In the SafeMode Management Network screen, select the Management interface option.
- 2 Press Enter.

The **Select Interface** list appears, displaying all of the interfaces available on the NSv.

3 Select the interface you wish to edit and press Enter.

The IPv4 and IPv6 addresses, Netmask, MAC address, Gateway, and DNS settings are displayed on the screen above the interface selection dialog.

4 Select IPv4 Address and press Enter.

The on-screen dialog displays the current IP address.

5 Navigate into the dialog and change the IP address to **0.0.0.0**, then press **Enter**.

Safemode menu System Info Management Network Test Management Network Diagnostics NTP Server System Update Reboot I Shutdown About Logs	Hanagement Network Management interface IPu4 Address Network Mac address IPu6 Address Gateway DNS 1 DNS 2	[ [ fe80 [ [ [	X1 192.168.0.15 200:29:5a:19:dd ::200:29ff:fe5a:1 192.168.0.1 8.8.8 8.8.4.4	] ] 19dd ] ]
Up / Down to select items TAB to move between views Enter to action/edit an item	Enter IP address 0.0.0.0_ Confirm <enter> Can SonicWall is in safemode, to access http://192.168.0.15/ or http://192.</enter>	icel <esc> : recovery 168.1.254</esc>	options visit:	

The Save changes button is displayed.

6 Press Tab to navigate to the Save changes button and then press Enter.

The interface is disabled.

Management Network Management interface	ŗ	X1	
IPu4 Address Netmask Mac. address		Not configured	
IPu6 Address Gateway DNS 1 DNS 2		fe80::20c:29ff:fe5a:19 192.168.0.1 8.8.8.8 8.8.4.4	dd ] ] ]

### Installing a New SonicOS Version in SafeMode

SWI files are used to upgrade SonicOS. You can download the latest SWI image file from MySonicWall.

In SafeMode, you can upload a new SonicOS SWI image and apply it to the NSv appliance. The SafeMode web management interface is used to perform an upgrade, rather than SafeMode in the NSv management console. When viewing the NSv management console in SafeMode, the URL for the SafeMode web interface is displayed at the bottom of the screen.

**NOTE:** In SafeMode, the web management interface is only available via http (not https).

#### To install a new SonicOS from SafeMode:

- 1 With the NSv in SafeMode, view the NSv management console. At the bottom of the screen, the URL for the SafeMode web management interface is displayed.
- 2 In a browser, navigate to the URL provided at the bottom of the Management Console screen. The SafeMode web management interface displays.

SONICWALL Ne	twork Security Virtual					
SonicOS is running in Safe Mode         Safe Mode will allow you to do any of the following:       SonicOS Product Info         > Download the Safe Mode Logs for troubleshooting by the SonicWall Support Team       Model: NSv Unlicensed         > Upload new SonicOS application images       Product Code: 70000         > Boot your choice of application image       GUID:         > Restore the settings to their factory default values       Serial Number:						
Image Management						
Restart 🕝 Refresh 🔹 Uploa	d Image					
Current Image Version ✓ 6.5.0.2-8v-sonicosv- 37–25793204	Import Date 4/25/2018, 6:14:00 PM	Last Used Date 4/25/2018, 6:14:03 PM	Status Not Running: Safe Mode	Boot () ,	Image Actions N/A	

3 Click the **Upload Image** button to select an SWI file and then click **Upload** to upload the image to the appliance. A progress bar provides feedback on the file upload progress. Once the upload completes, the image is available in the **Image Management** list in the SafeMode web interface.

- 4 In the row with the uploaded image file, click the **Boot** button and select one of the following:
  - Boot Uploaded Image with Current Configuration
  - Boot Uploaded Image with Factory Default Configuration

nage Management start © Refresh 💿 Upload I	mage				
Current Image Version ✓ 6.5.0.2-8v-sonicosv-37-rt207f34d	Import Date 4/12/2018, 4:28:26 PM	Last Used Date 4/12/2018, 4:28:45 PM	Status Not Running: Safe Mode	Boot	Image Actions
Uploaded Image Version 6.5.0.2-8v-sonicosv-37-f207f34d	Load Date 4/12/2018, 4:49:31 PM	Build Date 4/12/2018, 3:39:33 AM		Boot () v	Image Actions
			Boot Uploaded Image (6.5.0.2-8v-sc with Current Configuration Boot Uploaded Image (6.5.0.2-8v-sc with Factory Default Configuration	onicosv-37f207f34d) onicosv-37f207f34d)	

The NSv appliance reboots with the new image.

### **Downloading Logs in SafeMode**

When the NSv appliance is in SafeMode, extra logging information is kept that can be downloaded. The logs are available from the SafeMode web management interface, which can be accessed via the URL provided at the bottom of the Management Console screen.

**NOTE:** In SafeMode, the web management interface is only available via http (not https).

#### To download logs from SafeMode:

- 1 With the NSv in SafeMode, view the NSv management console. At the bottom of the screen, the URL for the SafeMode page in the web UI is displayed.
- 2 In a browser, navigate to the URL provided at the bottom of the Management Console screen. The SafeMode web management interface displays.

SONIC <b>WALL</b> " Ne	twork Security Virtual				
SonicOS is running in Safe Mode Safe Mode will allow you to do any of t > Download the Safe Mode Logs t > Upload new SonicOS applicatio > Boot your choice of application > Restore the settings to their fact Download Safe Mode Logs	he following: for troubleshooting by the SonicWa n images mage ory default values	ll Support Team	SonicOS Product Info Model: NSv Unlicensed Product Code: 70000 GUID: Serial Number:		
Image Management					
Restart 🕝 Refresh 🔹 Uploa	d Image				
Current Image Version ✓ 6.5.0.2-8v-sonicosv- 37–25793204	<b>Import Date</b> 4/25/2018, 6:14:00 PM	Last Used Date 4/25/2018, 6:14:03 PM	Status Not Running: Safe Mode	Boot	Image Actions N/A

3 Click the **Download Safe Mode Logs** button. A compressed file is downloaded which contains a number of files, including a *console\_logs* file that contains detailed logging information.

# SonicWall Support

Technical support is available to customers who have purchased SonicWall products with a valid maintenance contract and to customers who have trial versions.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. To access the Support Portal, go to https://www.sonicwall.com/support.

The Support Portal enables you to:

- View knowledge base articles and technical documentation
- View video tutorials
- Access MySonicWall
- Learn about SonicWall professional services
- Review SonicWall Support services and warranty information
- Register for training and certification
- Request technical support or customer service

To contact SonicWall Support, visit https://www.sonicwall.com/support/contact-support.

# **About This Document**

#### Legend

 $\wedge$ 

WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death.

CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

(i) IMPORTANT, NOTE, TIP, MOBILE, or VIDEO: An information icon indicates supporting information.

NSv VMware Getting Started Guide Updated - October 2019 Software Version - 6.5.4 232-004955-00 Rev C

#### Copyright © 2019 SonicWall Inc. All rights reserved.

SonicWall is a trademark or registered trademark of SonicWall Inc. and/or its affiliates in the U.S.A. and/or other countries. All other trademarks and registered trademarks are property of their respective owners

The information in this document is provided in connection with SonicWall Inc. and/or its affiliates' products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of SonicWall products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, SONICWALL AND/OR ITS AFFILIATES ASSUME NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON- INFRINGEMENT. IN NO EVENT SHALL SONICWALL AND/OR ITS AFFILIATES BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF SONICWALL AND/OR ITS AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SonicWall and/or its affiliates make no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. SonicWall Inc. and/or its affiliates do not make any commitment to update the information contained in this document.

For more information, visit https://www.sonicwall.com/legal.

#### **End User Product Agreement**

To view the SonicWall End User Product Agreement, go to: https://www.sonicwall.com/en-us/legal/license-agreements. Select the language based on your geographic location to see the EUPA that applies to your region.

#### **Open Source Code**

SonicWall is able to provide a machine-readable copy of open source code with restrictive licenses such as GPL, LGPL, AGPL when applicable per license requirements. To obtain a complete machine-readable copy, send your written requests, along with certified check or money order in the amount of USD 25.00 payable to "SonicWall Inc.", to:

General Public License Source Code Request SonicWall Inc. Attn: Jennifer Anderson 1033 McCarthy Blvd Milpitas, CA 95035