



Contents

Overview	. 4
About NSM	. 4
Related Documents	. 5
Conventions	. 7
UI Conventions	. 7
Guide Conventions	. 7
Before Starting	9
Installation Quick Start	. 9
Prerequisites	10
Supported Firewalls	10
System Requirements	11
Capacity Requirements	.11
Scaling Up	.12
Licensing Model	.12
Creating an MSW Account	.12
Obtaining the Image	.14
Obtaining a New Licensed Image	.14
Obtaining a Trial Version	.18
Downloading NSM for an Existing Instance	. 19
Installing NSM on ESXi Server	21
Installing on ESXi Server	.21
Connecting to the Console from ESXI	.27
Installing NSM on Hyper-V	.28
Preparing the Windows Server System	.28
Installing NSM On-Premises on Hyper-V	.28
Connecting to the Console from Hyper-V	.33
Installing NSM on KVM	.35
Preparing the KVM Server	.35
Installing KVM	.36
Deploying NSM on KVM	.36
Creating a Virtual Machine via Command Line	.37
Creating a Virtual Machine via Virtual Manager	.41
Installing NSM on Azure	50

NSM Settings and Registration	
Configuring NSM Network Settings	
Registering NSM	
Associating Firewalls on MSW	60
Unregistering NSM	60
Console Operations	61
Management Console Operations	61
NSM Management Console Menu	62
System Info	63
Network Interfaces	63
	64
NTP Server	
System Update	
About	
About	
Lising SafeMode on the Management Console	
Enabling SafeMode	
Disabling SafeMode	70
Configuring Network Interfaces in SafeMode	
Installing a Software Upgrade in SafeMode	73
Downloading Logs in SafeMode	74
Using NSM	
Interface Overview	76
Dashboard	
Creating a Tenant	79
Creating a New User	
Adding a Device	
Integrate On-Prem Analytics with NSM	
Integrate SonicWall Analytics in NSM	
Enable Analytics While Adding a New Device	84
Enable Firewall to View Analytics Data	85
Accessing Analytics Data	
Upgrade Instructions	
Upgrade Using Management Console	
Upgrading SonicOS Firmware	91
SonicWall Support	
About This Document	

Overview

SonicWall's Network Security Manager (NSM) is a web-based application that centralizes management, reporting, and analytics for the SonicWall family of network security appliances.

Topics:

- About NSM
- Related Documents
- Conventions

(i) **NOTE:** Information about upgrading NSM is provided in Upgrade Instructions.

About NSM

SonicWall Network Security Manager (NSM) is the next generation firewall management application that provides a holistic approach to security management. The approach is grounded in the principles of simplifying and automating various tasks to achieve better security operation and decision-making, while reducing the complexity and time required. NSM gives you everything you need for firewall management; comprehensive visibility and granular control and the capacity to govern the entire SonicWall network security operations with greater clarity, precision, and speed. This is all managed from a single, function-packed interface that can be accessed from any location using a browser-enabled device. Firewalls can be centrally managed to provision all of the network security services with a single-pane-of-glass experience.

For ease of deployment, this security management platform is available as SaaS (Software as a Service) and as an on-premises offering. The on-premises solutions can be installed on ESXi, Hyper-V, KVM, or Azure system. It is accessible on-demand, via the cloud, with virtually unlimited system scalability to support multiple tenants with thousands of security modes under each one. The solution's redundant and distributed architecture enables organizations to centrally and reliably manage a single small network to multiple enterprise-class deployments. It has the flexibility to scale without increasing management and administrative overhead.

NSM offers many salient features:

- · On-board hundreds of devices with Zero-Touch Deployment easily
- Group devices based on geographic location, business functions or customers with Device Groups
- · Enforce consistent security across all your devices with Device Templates

- Quickly decide in real time what policy actions to take against any threat using detailed reporting and powerful analytics
- Centrally configure policies with the Unified Policy Management feature. Unified Policy Management provides the integrated management of various security policies for enterprise-grade firewalls.
- Easily configure devices with two new template types (in addition to the master golden configuration) for SonicOS and SonicOSX devices. It helps take configuration from baseline devices and apply it to the other devices or groups.

NSM can manage both Gen6 and Gen7 SonicWall firewalls, but SonicOS 6.5.4.6 is the recommended minimum version. NSM adds support for the firewall series Gen 7 NSa 2700 and TZ Series running SonicOS as well as NSsp and Gen 7 NSv, with multi-tenancy and unified policy management features.

NSM On-Premises also provides distinctive features like High Availability (HA), Closed Network and two factorauthentication (2FA) for stronger security and increased productivity and flexibility. The High Availability feature allows two identical SonicWall firewalls to be configured to provide a reliable continuous connection to the public internet. The Closed Network support feature is ideal for customers that run one or more private networks that are completely shut-off from the outside environment. Customers can license the NSM managed firewall without contacting License Manager (LM) or MySonicWall (MSW), when onboarding and patching SonicWall firewall to preserve the privacy and security of the closed networks. NSM on-premises also provides an added level of security with the two-factor authentication to address the increasing number of cyber security attacks.

For more information on the features, refer to *Network Security Manager Administration Guide* at Technical Documentation portal.

Related Documents

In addition to this document, which describes how to set up and configure an On-Premises instance of NSM on various types of virtual machines, the NSM document set is made up of the following:

Document	Description	When to Use It	
About Network Security Manager	Provides an overview of the product and describes the base modes of operation, the navigation and icons, and the Notification Center .	Read this document gain an understanding of basic tasks before diving into specific NSM topics and tasks in the other books. These include:	
		Overview of NSM	
		Review of basic workflows	
		 Introduction to the Dashboard and monitoring 	
		Navigation	
		Notification Center	
		This document applies to both SaaS and On- Premises instances.	

Document	Description	When to Use It
Network Security Manager Administration Guide	Provides details on NSM features for administering your instance of NSM.	Read this document to learn how to configure and maintain NSM. Use the workflows from above as a checklist for the sequence of actions and feature descriptions. This document applies to both SaaS and On-Premises instances.
Network Security Manager Reporting and Analytics Administration Guide	Discusses how to use the reporting and analytics features.	Read this document to learn what types of reports are available and how to navigate within them. It also describes how to schedule reports and define their contents. This document applies to both SaaS and On-Premises instances.
		The Advanced license is needed to access all the Analytics features.
Network Security Manager On-Premises System Administration	Describes the system administration tasks for an on- premises deployment of NSM.	Read this document to understand how to configure and manage an on-premises instance of NSM. It includes:
Guide		System Dashboard
		System settings
		Network settings
		System monitoring
		High Availability (HA) configuration
		This document applies to On-Premises instances only.
Network Security Manager Getting Started Guide for SaaS	Describes how to license and configure a basic SaaS NSM instance.	Read this document to learn how to license and configure a SaaS instance of NSM. This document applies to SaaS instances only.
Closed Network Feature Guide	Describes how to deploy NSM on a closed network.	Read this document to learn how to set up on- premises NSM in an environment that has no external network connections. This instance operates in a closed network. This document applies to On-Premises instances only.
NSM Release Notes	Summarizes the new features for the product and provides information on the closed and resolved issues.	Read this document to review the list of resolved and known issues for this release. This document applies to both SaaS and On- Premises instances of NSM.

To access the NSM documentation, navigate to the Technical Documentation portal.

Conventions

The Network Security Manager Getting Started Guide makes use of the following conventions:

- Guide Conventions
- UI Conventions

UI Conventions

When acquiring devices for management and reporting, the **Status** option uses colored icons to indicate the various states of the devices being monitored and managed.

Status Icon	Definition
	Indicates that a process is in progress. In some instances, specific details are provided: for example, Requesting Licenses .
~	Indicates that a process has completed successfully. May provide the message Success or something with more detail like Device parameters set up in Cloud Capture Security Center complete .
0	Indicates that a task is in process or pending the completion of another task. The message Pending is usually displayed, as well.
•	Indicates a potential issue. Messages provide additional detail to help you resolve the issue.
	Indicates an error. Additional information may be provided via an information icon. Click the icon or mouse over it to see the message: for example, Gateway Firewall is not available in CSC .
	Indicates the device is online.
	Indicates the device is offline.
\$	Indicates unmanaged devices.
\checkmark	Indicates managed devices.

Guide Conventions

The following text conventions are used in this guide:

Convention	Use
Bold text	Used in procedures to identify elements in the user interface like dialog boxes, windows, screen names, messages, and buttons. Also used for file names and text or values you are being instructed to select or type into the interface.
Menu view or mode Menu item > Menu item	Indicates a multiple step menu choice on the user interface. For example, Manager View HOME
	> Firewall > Groups means verify you are in Manager View first and that the HOME options is selected. Then click on Firewall in the left-hand menu, and select Groups.
Computer code	Indicates sample code or text to be typed at a command line.
<computer code="" italic=""></computer>	Represents a variable name when used in command line instructions within the angle brackets. The variable name and angle brackets need to be replaced with an actual value. For example in the segment serialnumber=< <i>your serial</i> <i>number</i> >, replace the variable and brackets with the serial number from your device: serialnumber=C0ABC0000001.
Italic	Indicates the name of a technical manual. Also indicates emphasis on certain words in a sentence, such as the first instance of a significant term or concept.

2

Before Starting

This chapter describes the prerequisites before installing and managing NSM on different platforms.

Topics:

- Installation Quick Start
- Prerequisites
- Supported Firewalls
- System Requirements
- Creating an MSW Account
- Obtaining the Image

() NOTE: If you are upgrading NSM, refer to Upgrade Instructions for more information.

Installation Quick Start

Use this checklist to guide you through the getting started process.

(i) **NOTE:** Your virtual sever must already be in place and you should be familiar with the basics of deploying virtual servers.

Step	Action to Take	Reference
1	Ensure that any prerequisites are met. These include confirming that your firewalls are supported and you have appropriate licensing, your system meets minimum requirements, and you have an MSW account.	Before Starting
2	Obtain your image. NOTE: The Azure image is obtained from the Microsoft Marketplace rather than MSW and is described in Installing NSM on Azure.	Obtaining the Image

Step	Action to Take	Reference
3	Install the NSM virtual appliance on your system. Each platform that NSM can run on is described in a separate chapter.	For EXSi: Installing NSM on ESXi Server For Hyper-V: Installing NSM on Hyper-V For KVM: Installing NSM on KVM
		For Azure: Installing NSM on Azure
4	Configure the NSM network settings	Configuring NSM Network Settings
5	Register NSM.	Registering NSM
6	Set up a basic configuration: Create a tenant 	Using NSM

- Create a user
- Add a device

Additional information is available in Console Operations and Upgrade Instructions.

Prerequisites

The prerequisites are similar for each platform NSM can be installed on.

- Each firewall must be licensed with the Comprehensive/Advanced Gateway Security Suite (CGSS/AGSS).
- Firewalls supported by an NSM On-Premises instance must be in a single Group or Tenancy.
- The firewalls added to NSM On-Premises are not a part of CSC (Capture Security Center) or NSM SaaS.
- Each firewall should have HTTPS management enabled.

(i) **IMPORTANT:** If a firewall is behind a NAT device, the HTTPS management port must be opened for the cloud services to communicate with the firewall.

(i) **NOTE:** For a KVM implementation, ensure that your Linux system supports KVM and download the image file to your Linux system (for example, SonicWall_NSM_On-Prem__For_QEMU_VM.img) to your Linux machine.

Supported Firewalls

The following firewalls and the associated firmware can be managed by Network Security Manager.

Firewall Model	SonicOS Version
SOHO W	6.5.4

TZ Series: TZ300, TZ300W, TZ300P, TZ350, TZ350W, TZ400, TZ400W, TZ500, TZ500W, TZ600, TZ600P	, 6.5.4
TZ Series: TZ270, TZ270W, TZ370, TZ370W, TZ470, TZ470W, TZ570, TZ570W, TZ570P, TZ670	7
NSv Series: NSv 10, NSv 25, NSv 50, NSv 100, NSv 200, NSv 300, NSv 400, NSv 800, NSv 1600	6.5.4
NSv Series: NSv 270, NSv 470, NSv 870	7
NSA Series: NSA 2600, NSA 3600, NSA 4600, NSA 5600, NSA 6600	6.5.4
NSa Series: NSa 2650, NSa 3650, NSa 4650, NSa 5650, NSa 6650, NSa 9250, NSa 9450, NSa 9650	6.5.4
NSa Series: NSa 2700, NSa 3700	7
NSsp Series: NSsp 12400, NSsp 12800	6.5.4
NSsp Series: NSsp 15700	7

System Requirements

Use the following information to plan the size and licensing needed for your system.

Topics:

- Capacity Requirements
- Scaling Up
- Licensing Model

Capacity Requirements

To be used efficiently, NSM recommends the following minimum requirements for the different platforms.

Platform	Version	Number of Firewalls	Minimum Configuration
VMware	ESXi 6.7	1-500	4 core, 24 GB RAM
	ESXi 7.0	500-3000	8 core, 48 GB RAM
Hyper-V	Windows 2016	1-500	4 core, 24 GB RAM
		500-3000	8 core, 48 GB RAM
KVM	Linux Kernel 2.6.17 or above Before installing KVM on Ubuntu, you have to verify if	1-500	4 core, 24 GB RAM
	the hardware supports KVM. Availability of CPU virtualization extensions such as AMD-V and Intel-VT is the minimum requirement for installing KVM.	500-3000	8 core, 48 GB RAM

Platform	Version	Number of Firewalls	Minimum Configuration
Azure	Standard_D4_v2 Standard_D5_v2	1-500	8 core, 28 GB RAM
		500-3000	16 core, 56 GB RAM

Scaling Up

NSM provides tools to monitor and assess the performance of your NSM implementation. You can define the performance thresholds for utilization of your CPU, memory, and disk. You can set a Warning range and Critical range for any of these parameters. When the range for any of them is exceeded, you can make plans to scale your system accordingly.

NSM also provides several system performance graphs that you can monitor to see how the system is behaving in real time. These include:

Live Monitor	Monitors how NSM is behaving in real time
Process Monitor	Shows the processes running on the NSM system and the utilization associated with each
Service Monitor	Shows what services are running on the NSM system and the utilization associated with each

System Report Displays the historical reports for CPU, memory, and disk utilization

For more information refer to the "System Monitor" section in the Network Security Manager On-Premises System Administration Guide.

Licensing Model

The licensing model is described below:

- Subscription are available for 1-year, 3-year, or 5-year periods.
- One base license supports up to five devices.
- NSM on-premises licensing is node based, with a base license of five nodes and add-on licenses for additional nodes after that.

Creating an MSW Account

A MySonicWall account is required to register the NSM instance.

(i) 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.

SONIC WALL mysonicwall	
Login with your MySonicWall account credentials	
Username or Email address	
Next	
Forgot username or email? Sign Up	

- 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 you have set up the authenticator, you need only push a button to confirm.
- 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.

Identify whether you are interested in beta testing new products.

- 9. Click **Continue** to go to the **EXTRAS** page.
- 10. Select whether you want to add additional contacts to be notified for contract renewals.
- 11. If you opted for additional contacts, input the information and click Add Contact.
- 12. Click Finish.
- 13. 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.
- 14. Click **Done**. You are returned to the login window so you can login into MySonicWall with your new account.

Obtaining the Image

You can purchase NSM On-Premises from a distributor or download a free trial from MySonicWall. The trial provides a 30-day license after which you need to purchase or remove it. When you purchase NSM you receive a fulfillment email with your Activation Key which you use to officially licenses our product.

(i) **NOTE:** NSM images for VMware, Hyper-V and KVM are available at MySonicWall. The image for an Azure system is available on the Microsoft Azure Marketplace.

Topics:

- Obtaining a New Licensed Image
- Obtaining a Trial Version
- Downloading NSM for an Existing Instance

Obtaining a New Licensed Image

To download NSM for the first time, you need an Activation Key to access the image.

1. Log in to MySonicWall.

(i) | NOTE: If you do not have a MySonicWall account, refer to Creating an MSW Account.

- 2. Navigate to Product Management > My Products.
- 3. Click Register Products.

Register Products		
1	2	3
CHOOSE A TENANT	PRODUCT REGISTRATION DETAILS	MANAGEMENT OPTIONS
Search Tenants	٩	
Michael Meredith Products	Ť	
NSM 2.0 Beta		
NSM_Group		
Private_Group		
SonicWall_Group		
TechPubs Lab 🖉		
+ Create new tenant		
Download CSV template		Cancel Proceed to product registration >

4. Choose a **Tenant**.

Register Products		
	2 PRODUCT REGISTRATION DETAILS	3 MANAGEMENT OPTIONS
TechPubs Lab		
	Authentication code	Friendly name
Register another serial number		
Download CSV template		Cancel Choose management options

- 5. Specify the Serial Number, Authentication Code, and Friendly Name.
- 6. From the drop-down, select **Upgrade Serial Number**.

UPGRADE SE	RIAL NUMBER	
This Serial Number can be used to upgrade any one of the Free Trials you would like to upgrade to Retail Versi	your Registered Free Trials listed below. Pl on and click Upgrade.	lease select
To create a new installation, click Continue, without sele	ecting any Free Trials.	
FRIELNDLY NAME	SERIAL	NUMBER
TechPubsNSM	10110111	111000
Total: 1 item(s)		
	Continue	UPGRADE

7. Click Upgrade.

Register Products				
CHOOSE A TENANT	PRODUCT REGISTRATION	DETAILS MA	ANAGEMENT OPTIONS	
TechPubs Lab				
10110011153/04/00100	V TZDU-E8WP	✓ TP_Lab_NSM	(10)-0011(1172-0)-0(101	NSM ON- PREM
+ Register another serial number				
🗢 Download CSV template 🔹 U			Cancel 📗 Done	

8. Verify the details and click **Done**. When the installation is complete, you can view the details further as given below.

TP_Lab_NSM			ē
Product Details	Licenses	Firmware	
Serial Number	100.0611112.0100000	Friendly name	111.1.48.14534
Tenant Name	TechPubs	Registered On	16 Jun 2021
Node Support	5	Support Expiration	16 Jun 2022
Product Type	NSM MANAGEMENT ON-PREM BASE LICE NSE - 5 NODES 1YR	Registration Code	W142404/2012
Authentication Code	11031414035447	Firmware Version	6.0 🕓
Trusted	YES	Closed Network	0
Configuratio Add ZT Configura ADD GUID	n is missing. Please click her	re to add.	

You have the option to add ZT configuration or you can do it later as required.

9. Select the Licenses tab to view the details of the license.

TP_Lab_NSM	02A0009					-
Product Details	Licenses	Firmware				
Q Show All Licenses		AL UPGRADE		A	ctivation Key	Activate
× SERVICE NAME		STATUS	COUNT	EXPIRY DATE	ACTIONS	
imes Desktop & Server Softwa	re (1 Licensed)					
Network Security Manager		Licensed	5	Jun 16 2022	•- Renew	📱 Buy 🕑 Start Trial
✓ Support Services (1 License)	sed)		(r			
24x7 Support		Licensed		Jun 16 2022	• Renew	📱 Buy 🕑 Start Trial

10. To download the firmware, select the **Firmware** tab. The available download options are displayed.

Product Details	Licenses	Firm	ware			
Updated release	e available					
Serial Number	and all the states of the	Firmware Version	6.0		Latest Released	2.2.1-R6-H1.2
		Туре	N/A		Firmware	
		Release Date	N/A		Туре	Hotfix Release
				G-	Release Date	Jun 11, 2021
✓ Available Downlo	ads					
NSM On-Prem K	/M					
NSM Onprem U	pgrade- KVM					Version
Release Date - Ju	un 11, 2021, Release ty	/pe - Hotfix Release, F	ile Size -	1.74 GB		2.2.1-R6-H1.2
NSM On-Prem Hy	yper-V					
NSM Onprem U	pgrade- Hyper V					Version
	11 2021 D.I.	LING DUILING	Tile Cine	17400		221 06 412

11. Hover the mouse over the required firmware and click with to download the software and save in your local system.

Obtaining a Trial Version

To obtain a trial version:

- Log in to MySonicWall.
 INOTE: If you do not have a MySonicWall account, refer to Creating an MSW Account.
- 2. Navigate to **Product Management > Trial Software**.
- 3. Select Network Security Manager (NSM) On-Prem.

Provide Friendly Name Friendly name Tenant Nam		×
Friendly name	TechPubsNSM	
Tenant Name	TechPubs 🔹	
		Cancel Try Now

- 4. Enter a Friendly Name.
- 5. Select a Tenant Name from the drop-down list.
- 6. Click Try Now.

When you purchase NSM, you need to activate the license.

To activate a trial NSM license:

- 1. After logging into your MySonicWall account, navigate to **Product Management > My Products**.
- 2. Find the **Friendly Name** of the NSM instance in your product list, and click on **Activate Service** (the **Key** icon on the right side of the table).
- 3. Type the **Activation Key** in the appropriate field and click **Activate**.

Product Details	Licenses	Firmware					
C Show All Licenses		UPGRADE		ł	Activation Key		Activate
SERVICE NAME		STATUS	COUNT	EXPIRY DATE	ACTIONS		
Desktop & Server Softwa	re (1 Licensed)						
Network Security Manager		Licensed	5	Jun 16 2022	•- Renew	🖁 Buy 🕞 S	tart Tria
Support Services (1 Licens	sed)		6				
24x7 Support		Licensed		Jun 16 2022	•Renew	🖫 Buy 🕑 S	tart Tria

You also have an option to upgrade the Serial Number under Product Details.

🔥 Offline , Active Support				-
Serial Number	ODHLU104A0003	Friendly name	My_trial_NSM	
Tenant Name	Sonic Wall Products	Registered On	10 Jun 2021	
Node Support	Unlimited	Support Expiration	10 Jul 2021	
Description	NSM On-Prem Demo	Registration Code	5010HW00	
Authentication Code	C07L-R0H0	Firmware Version	2.1 🖸	
Trusted	YES			
Upgrade Serial Number				
Add ZT Configuration				
TO-DO List		Associated Products		
You have no pending tasks		FreeTrial SerialNumber (0)		
		Managed Nodes (0)		

While in MySonicWall, you should download the NSM image for later installation.

Downloading NSM for an Existing Instance

To download the NSM image:

- 1. Navigate to **Product Management > My Products**.
- 2. Find the Friendly Name of the NSM instance in your product list, and click on the Serial Number.

- 3. Select **Firmware** at the top of the page. The NSM downloads for each platform are listed.
- 4. Click on the platform you want to download to highlight the options on the right.

✓ Available Downloads	
NSM On-Prem Hyper-V	
NSM Onprem Fresh install- Hyper-V Release Date - Mar 19, 2021, Release type - Feature Release, File Size - 3.57 GB	L 🕹
NSM On-Prem KVM	
NSM Onprem Fresh install- KVM	Version
Release Date - Mar 19, 2021, Release type - Feature Release, File Size - 3.13 GB	2.2.0-R10
NSM On-Prem VMware	
NSM Onprem Fresh install- VMware	Version
Release Date - Mar 19, 2021, Release type - Feature Release, File Size - 3.11 GB	2.2.0-R10
	Browse All Firmware

- 5. Click on the **Download** icon to download the image.
- 6. Store the image where you an easily access it when you begin the installation.

Installing NSM on ESXi Server

Topics:

- Installing on ESXi Server
- Connecting to the Console from ESXI

Installing on ESXi Server

Install NSM On-Premises by deploying an OVA file to your ESXi server. The OVA file contains the software components needed. Deploy the OVA file by using the vSphere or vCenter client, which is 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.

To install NSM On-Premises on ESXi server:

1. Access vSphere and log in to your ESXi server.

(i) NOTE: Install NSM after setting up your virtual system.

2. Right-click on your system and select Deploy OVF Template.

3 Select screpute resource 4 Review details 5 Select storage 6 Ready to complete Her a URL to download and install the OVF package from the internet, or browse to a location accessible from your comput a local hard drive, a network share, or a CD/DVD drive. ○ URL. http://remotesenser.address/filetodeolog/ovf i ova ● Local file Choose Files Sonic/Wall_NSM2.3.0-2192.ova	Select an OVF template Select a name and folder	Select an OVF template Select an OVF template from remote URL or local file system	
Choose Files Sonic Wall_NSM2.3.0-2192 ova	Select a compute resource Review details Select storage Ready to complete	Enter a URL to download and install the OVF package from the internet, or browse to a loc a local hard drive, a network share, or a CD/DVD drive. O URL . http://temotesenver-address/fietodeolog.ovf ova @ Local file	ation accessible from your computer, such
		Choose Files SonicWall_NSM2.3.0-2192.ova	lş.

- 3. Select Local file and click on Choose Files.
- 4. Navigate to where you stored the NSM OVA file to select it.
- 5. Click Open.
- 6. On the wizard, click **Next**.
- 7. Specify the **Virtual machine name** for the NSMOn-Premises instance. Be sure it's a meaningful name so you can easily find it lists and tables.

Deploy OVF Templat	e						
 1 Select an OVF template 2 Select a name and folder 	Select a name and folder Specify a unique name and target location						
3 Select a compute resource 4 Review details 5 Select storage 6 Ready to complete	Virtual machine name:						
o reeuy to comprete	v © venter670 eng sonicwall.com v San Jose v Engineering > Dev > Casture > Casture > Dev >						
	CANCEL	BACK					

8. Select the location for the virtual machine and click **Next**.

- 9. On the next screen, **Select a compute resource** on which to deploy the template and click **Next**. The system validates the resources so it may take some time before the next window appears.
- 10. In the Review details screen, verify the template details and click Next.

elect a name and folder	Review details Verify the template details.						
elect a compute resource							
cense agreements	Publisher	No certificate present					
elect storage	Product	SpricMat NBH On-Prem 2 3-0-000					
elect networks ustomize template	Version	MASTER/soniccore/nsm/2.3.0/master-386					
eady to complete	Vendor	Vendor SonicWail Bentley					
	Description	Suni-Mar New On-Pren Web7999/suni-sun/hun/2.3.0/mediar-396 web/cat,786569 Reha Suglia					
	Download size	3.1 GB					
	Size on disk	3.1 GB (thin provisioned)					
		258.4 GB (thick provisioned)					

(i) NOTE: The details you see on this screen are specific to your deployment.

11. On the License agreements screen, read the agreement, select I accept all license agreements.

a name and folder	License agreements					
a name and rolder	The end-user license agreement must be accepted. Read and accept the terms for the license agreement.					
w details						
e agreements						
storage	End User License Agreement for SonicWall Network Security Manager (NSM)					
networks						
nize template						
9 Ready to complete	SonicWall licenses its software on the conditions below, and on the condition that Customer agrees to this EULA. If Customer					
	does not wish to agree to this EULA, (i) Customer does not have a license to the software and (ii) Customer may not download.					
	install, activate or otherwise use any of the software, and (iii) Customer must promptly return the software. Customer's use of the					
	Software is conclusive evidence that it agrees to this EULA					
	The individual who indicates the Customer's agreement to this EULA personally represents to SonicWall that he or she is					
	authorized to agree to this EULA on behalf of the Customer.					
	This SonicWall End User License Agreement (the "EULA") is between the SonicWall entity identified in the Definitions section and					
	the person (legal entity or natural person) identified in an Order as the purchaser of SonicWall Products or on whose behalf the					
	This SonicWall End User License Agreement (the "EULA") is between the SonicWall entity identified in the Definitions section the person (legal entity or natural person) identified in an Order as the purchaser of SonicWall Products or on whose behalf I accept all license agreements.					

- 12. Click Next.
- 13. Select virtual disk format from the drop-down list. Thick Provision is recommended to help prevent over-provisioning of storage.

2 Select a name and folder	Select storage						
3 Select a compute resource 4 Review details	Frervet this virtual machine (No encryption polities available)						
5 License agreements	Select virtual disk format:			Thick Provisio	n Lanky Zeroed 🗸		
6 Select storage 7 Select networks	VM Storage Policy:			Thick Provision	on Lazy Zeroed	-	
8 Customize template	Name	Capacity	Provisioned	Thin Provision	n	Cluster	
9 Ready to complete	ESX-MIL148-DEV13-DM	2.91 TB	2.99 TB	269.24 GB	VMFS 5		
	ESX-MIL148-DEV13-DM	3.63 TB	3.58 TB	85.54 GB	VMFS 5		
	ESX-MIL148-DEV13-DM	1.82 TB	1.31 TB	813.92 GB	VMFS 6		
	•						,
	Compatibility						
		andad					

14. Select a data store from the table and click **Next**.

(i) **NOTE:** The minimum storage requirement is 260 GB.

15. In the Select networks screen, set up interfaceX0 to access the network.

This is the same naming convention as a SonicWall firewall. **X1** is considered a WAN interface so the Destination Network should be changed to an externally accessible subnet.

1 Select an OVF template 2 Select a name and folder	Select networks Select a destination network for each source network.					
3 Select a compute resource	Source Network	т	Destination Network			
5 License agreements	X0		10.202.3.X Jm			
6 Select storage	X1		10.202.3.X		~	
7 Select networks 8 Customize template					2 item	15
9 Ready to complete	IP Allocation Settings					
	IP allocation:	Stati	c - Manual			
	IP protocol:	IPv4				
				CANCEL	BACK NE	

- (i) **IMPORTANT:** X1 (the default WAN Interface) is set to **DHCP** by default, with **HTTPS management** enabled for the NSM On-Premises instance, as this configuration eases deployments in virtual/cloud environments.
- 16. Click Next.

Select a compute resource	Customize the deployment properties of	Customize the deployment properties of this software solution.						
Review details	O All properties have valid values	2						
Select storage	 Uncategorized 	1 settings						
Customize template	SonicCore Hostname	SonicCore Hostname						
Ready to complete								

17. In the **Customize template** screen, verify the information, and click **Next**.

 1 Select an OVF template 2 Select a name and folder 3 Select a compute resource 	Ready to complete Click Finish to start creation.						
 4 Review details 5 License agreements 	Provisioning type	Deploy from template					
✓ 6 Select storage	Name	SonicWall_NSM_On-Prem_2.2.0-366_R366789					
 8 Customize template 	Template name	SonicWall_NSM_On-Prem_2.2.0-366_R366					
9 Ready to complete	Download size	3.1 GB					
	Size on disk	258.4 GB					
	Folder	Dev					
	Resource	10.203.20.13					
	Storage mapping	1					
	All disks	Datastore: ESX-MIL148-DEV13-DM-RDO-Local3; Format: Thick provision lazy zeroed					
	Network mapping	2					
	xo	10.202.3.X					
	X1	VM Network					
	IP allocation settings						
	IP protocol	IPV4					
	IP allocation	Static - Manual					
	Properties	SonicCore Hostname =					

18. In the **Ready to complete** screen, verify all fields and click **Finish** to create the NSv appliance. The name of the new NSM On-Premises appears in the left pane of the vSphere window when complete.

The deployment will take some time; you can view the summary and details on the **Summary** page of the vSphere Client.

19. When the deployment is complete, be sure the new virtual system is selected and click 💒 to power on the system.

2 8 2	🗄 SonicWall_N	SM_On-Prem_2.2.0-366	6_R366RG	h <u>= *</u>	🖗 🗐 Actions -		
SBOX-DM2	Summary Monitor	Configure Permissions Dat	astores Networks	Power On Jpanes			
S.J.UNGELUS (Ophianed) Sociulation of sonovellicom Socialidade of sonovellicom Socialidade Socialidade	Powered Off Launch Web Console Launch Remote Console	Guest OS: Other 2.6.x Linux (6 Compatibility: ESXI 5.0 and later (VMware Tools: Not running, version More info DNS Name: IP. Addresses: Host: 10.203.20.13	4-bit) VM version 8) 1:2147483647 (Guest Manage	ed)			CPU USAGE O HZ MEMORY USA O B STORAGE USA 258.4 GB
SonicWALL_NSv_870_Richa_2_03 So.eng.sonicwall.com-TO-BE-DELE	VM Hardware			~	Notes		,
Ubuntu14_04 - hadoop28 Center 4.1	Related Objects			^	SonicWall_NSv_R366 Edit Notes		
VMware vCenter Server Appliance Windows-2003-DC2-SOH	Cluster	Dev-Cluster			Custom Attributes		
> Dev2	Host	10.203.20.13			Attribute	Value	
> D QA-And-MSW-DataCenter > D SonicOSCoreDevTest	Networks	♀ 10.202.3.X ♀ VM Network					
> In Capture > In CAS > In CFS	Storage	ESX-MIL148-DEV	/13-DM-RD0-Local3				
> In DPI > In Justin-MiniLab	Tags			^	×		 No items to display
> 🖻 NSM > 📄 SMA	Assigned Tag	Category	Description	*	Edt		
> 🗈 SonicML					VM Storage Policies		

20. Click on the large **Powered Off** button in the **Summary** page (upper left corner). to launch the console.

Launch Console	\times
Web Console VMware Remote Console (VMRC) Remember my choice	
CANCEL	

21. Keep the default selection, and click **OK** to launch the **Web Console**.

The system console shows a boot message. Depending on the resources available to your system, this initial boot up may take 10 to 15 minutes; you can monitor the % complete in the console to track progress.



When the initial boot is complete, the Management Console displays.

SonicWall_NSM_On-Prem_2.2.0-366_R366RG			Enforce US Keyboard Layout View Fullscreen Send Ctrl+Alt+Delet
Sustan Info	System Info	+ 42332501_50FC_22F1_082F_8403F1058696	
Storage	GOTD	· 16556501-5010-7611-0071-010561050050	
Network Interfaces			and the second
Diagnostics	System Time	: Fri 2021-04-23 16:28:48 UTC	
Susten Update	Load Average	: 2.6 1nin 1.3 5nin 0.5 10nin	
Reboot Shutdown			
About			and the second
Logs			
			Contraction of the second s
			the second s
The results are results and results and			
이 방송			
Up 2 Down to collect Itoms			
TOR to nous between users			

Next, you should use the console to configure the network settings. This establishes your ability to access NSM through a browser. Refer to Configuring NSM Network Settings for details.

Connecting to the Console from ESXI

You can easily use the NSM Management Console to view and configure various parameters for NSM. It can also be used for diagnostics. To launch the NSM Management Console in an ESXi environment, simply go to the virtual machine monitor and choose **Launch Web Console** or **Launch Remote Console**.



For details on what's available on the NSM Management Console refer to Console Operations.

Installing NSM on Hyper-V

Topics:

- Preparing the Windows Server System
- Installing NSM On-Premises on Hyper-V
- Connecting to the Console from Hyper-V

Preparing the Windows Server System

Before installing an NSM On-Premises instance on Hyper-V, prepare the Windows Server system:

- Install Windows Server 2012 or 2016.
- Install the Hyper-V Role in the Windows Server system. Refer to the Microsoft documentation at Installthe-HyperV role-on-windows-server.

Installing NSM On-Premises on Hyper-V

To install NSM On-Premises on Hyper-V:

- 1. Log in to Hyper-V to select the VM.
- 2. Right click on the name of the VM.
- 3. Click New > Virtual Machine.

Manager								1	Actions
Virt Virt	ual Machines								ESQAHYPERV16
INEW INC. INC.	virtua Machine	State	CPU Usage	Assigned Memory	Uptime	Status		^	New
import virtual Machin	e Harduisk	04							Ch. Immed Midwel Markins
Hyper-V Settings	Hoppy Disk	08							import virtual instanting
Virtual Switch Manag	If Man	Bureires		10034 MD	10.00.42.20				Hyper-V Settings
Virtual SAN Manager.	- Andrea	OF		Track the	12.0004.20				Virtual Switch Manager
Evit Dirk	Suhes	Of							🔬 Virtual SAN Manager
Increast Dick	Suhas	Bunning	0%	16024 MB	18.23:30:06				🚅 Edit Disk
mapped proces	DRV	Bunning	4%	2048 MB	39.20:11:33				P Inspect Disk
Stop Service	MG_HYPERV	Running	47,	2048 MB	39.20:11:34				Step Senice
Remove Server	13	OH							
Refresh	9.102	Running	37.	20024 MB	4.03:15:22				A nemove server
View	> 013	Bussies	02	10024 MP	01/09/12				O Ketresh
11-la	Press 2 2 0 R355	01	0.0	TOTAL TIME	01.02.14				View
Hep	Aniprio 10 Aniprio	Bunning	0%	16024 MB	24.15.04.31				👔 Help
8	VSv_RC676_Archana	0#							es yesh 10.5.59,102
	VSv_RC676_Manash	Off							Connect
	vSv_RTQA37_Akhia	Saved							P. falling
	4C967_Harka 10.5.46.22	Hunning	2%	4096 MB	39.20.11.06				Seconga.
	Scienced NSMCrosses 10.5.22.2 Narothini	01							 Turn Ott
i i i	SonicWall NSv For Monach HoneyV-1128-Anta	Burning	27.	10024 MR	25 17 47 50				Shut Down
	SonicWall NSv For Microsoft HyperV-1128-Chetan	Bunning	37.	10024 MB	39.20:10:41				Save
8	SonicWall_NSvFor_Microsoft_HyperV-1219-Chetan2	Running	2%	10024 MB	39.20:10:41				11 Pause
	SonicWall_NSvHyperV-1219-Chetan 1-	Running	37.	10024 MB	39.20:10:40			~	IÞ Reset
Che	ckpoints	-							Checkpoint
									P Move
				The selected virtual ma	achine has no checkp	oints.			Export
									# Rename
es	resh 10.5.59.102								1 Enable Replication
	Greated: 4/22/2021 11:14	IO PM				Chustere	where Na		Help
	Configuration Version: 8.0					Hearthe	sat: No Contact		-
	Generation: 1								

The New Virtual Machine Wizard window is displayed.

🖳 New Virtual Machine Wiz	tard	X
Specify Nar	ne and Location	
Before You Begin Specify Name and Location Specify Generation Assign Memory Configure Networking Connect Virtual Hard Disk	Choose a name and location for this virtual machine. The name is displayed in Hyper-V Manager. We recommend that you use a name that lidentify this virtual machine, such as the name of the guest operating system or workd Name: Name: New Virtual Machine You can create a folder or use an existing folder to store the virtual machine. If you de folder, the virtual machine is stored in the default folder configured for this server. Store the virtual machine in a different location	helps you easily bad.] on't select a
Summary	Location: C: \ProgramData\Microsoft\Windows\Hyper-V\ f you plan to take checkpoints of this virtual machine, select a location that has e space. Checkpoints include virtual machine data and may require a large amount o	Browsess
	< Previous Next > Finish	Cancel

- 4. Specify the name and location of the VM.
- 5. Click Next.



- 6. Specify the Generation as Generation 1.
- 7. Click Next.

New Virtual Machine Wizar	d	×
Assign Memo	rγ	
Before You Begin Specify Name and Location Specify Generation Assign Memory Configure Networking Connect Virtual Hard Disk Installation Options Summary	Specify the amount of memory to allocate to this virtual machine. You can specify an amount from 32 MB through 12582912 MB. To improve performance, specify more than the minimum amount recommended for the operating system. Startup memory: Image: MB Use Dynamic Memory for this virtual machine. Image: MB When you decide how much memory to assign to a virtual machine, consider how you intend to use the virtual machine and the operating system that it will run.	
	< Previous Next > Finish Cancel	

- 8. Assign memory to the VM.
- 9. Click Next.

Configure N	letworking		
Before You Begin Specify Name and Location Specify Generation Assign Memory Configure Networking Connect Virtual Hard Disk Installation Options Summary	Each new viri virtual switch Connection:	ual machine includes a network adapter. You c or it can remain disconnected. Not Connected 10.5.123 MGMT_Liplink Physics_Detwork NEW VLAN 200 Test 10.5.56.x	an configure the network adapter to use
		< Previous N	ext > Finish Cancel

- 10. Select the network.
- 11. Click Next. The Connect Virtual Hard Disk screen is displayed.

New Virtual Machine Wiza	ard	×
Connect Vir	tual Hard Disk	
Before You Begin Specify Name and Location Specify Generation Assign Memory	A virtual machine requires storage so that you can install an operating system. You can specify the storage now or configure it later by modifying the virtual machine's properties. Create a virtual hard disk Use this option to create a VHDX dynamically expanding virtual hard disk.	
Configure Networking	Name: hyperv_shreyas_41.83.vhdx	
Connect Virtual Hard Disk	Location: C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks\ Browse	
Summary	Size: 127 GB (Maximum: 64 TB)	
	Use an existing virtual hard disk Use this option to attach an existing virtual hard disk, either VHD or VHDX format. Location: C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks\ Browse	
	Attach a virtual hard disk later Use this option to skip this step now and attach an existing virtual hard disk later.	
	< Previous Next > Einish Cancel	

- 12. Select Use an existing virtual hard disk option.
- 13. Click **Browse** and select the NSM VHD file.
- 14. Click **Next**to see the **Summary** screen.

🖳 New Virtual Machine Wiza	rd
Completing	the New Virtual Machine Wizard
Before You Begin Specify Name and Location Specify Generation	You have successfully completed the New Virtual Machine Wizard. You are about to create the following virtual machine. Description:
Assign Memory Configure Networking Connect Virtual Hard Disk Summary	Name: hyperv_sream Generation: Generation 1 Memory: 16000 MB Network: B Hard Disk: C: \users \public \Documents \hyper-v \Virtual hard data Sencental _MA_O Hard Disk: C: \users \public \Documents \hyper-v \Virtual hard data Sencental _MA_O To create the virtual machine and dose the wizard, dick Finish.
	< Previous Next > Finish Cancel

- 15. In the **Summary** screen, verify the details, and click **Finish**.
- 16. To connect to the console, select the NSM On-Premises instance with a left-click and then right-click to select **Connect**.

When the installation and reboot is complete, go to NSM Settings and Registration to configure your network settings and register NSM.

Connecting to the Console from Hyper-V

You can easily use the NSM Management Console to view and configure various parameters for NSM. It can also be used for diagnostics. When using Hyper-V you can connect to the NSM Management Console in the following way:

- Using the Hyper-V remote console to access the NSM On-Premises command line interface
 - (i) **NOTE:** In the following procedure, the public IP address is the WAN IP address appearing in **Hyper-V Virtual Machine Connection**.

To connect to the management console through the Hyper-V Manager::

1. Bring up the Hyper-V Manager, select the NSM On-Premises instance with a left-click and then right-click to select **Connect**.

Hyper-V Manager						-	×
File Action View Help							
• 🔿 🙍 🖬 🖬							
Hyper-V Manager	Virtual Machines						
	Name	State	CPU Usage	Assigned Memory	Uptime	Status	
	NSv-Epsion NSv-ResetTest3	Off					
	On_Prem_Analytics	Off					
			Connect				
			Settings				
			Start				
	<		Checkpoint				
	Checkpoints		Moun				6
			Emort	he has no checkp	oints.		
			Paparea				
			Delate				
			Delete				
			Help				

2. After the VM boots up, the Management Console appears.

-Henu- System Info	System Info GUID	- 111777 - 1018 - 1018 - 1018 - 1018 - 1018 - 1018
storage Network Interfaces Diagnostics MTP Server Lockdawn Mode Reboot I Shutdown About Logs	Systen Tine Up Tine Load Average	: Thu 2019-02-21 23:20:48 UTC : 0 seconds : 0.0 1min 0.0 5min 0.0 10min
Up / Down to select itens TAB to nove between views Enter to action/edit an iten		

For details on what's available on the NSM Management Console refer to Console Operations.

Installing NSM on KVM

5

Topics:

- Preparing the KVM Server
- Installing KVM
- Deploying NSM on KVM

Preparing the KVM Server

Before installing KVM on Ubuntu, you have to verify if the hardware supports KVM. Availability of CPU virtualization extensions such as AMD-V and Intel-VT is the minimum requirement for installing KVM.

To check whether the Ubuntu system supports virtualization, run the following command. If the outcome is greater than 0, then it implies that virtualization is supported:

```
$ egrep -c '(vmx|svm)' /proc/cpuinfo
```

To check if your system supports KVM virtualization, execute the following command:

\$ sudo kvm-ok

If the "kvm-ok" utility is not present on your server, you can install it by running the following command:

\$ sudo apt install cpu-checker

Now execute the "kvm-ok" command to probe your system:

\$ sudo kvm-ok
INFO: /dev/kvm exists
KVM acceleration can be used

The output clearly indicates that you are ready to proceed with the installation of KVM.

Installing KVM

After confirming that your system can support KVM virtualization, you can start installing KVM. To install KVM, virt-manager, bridge-utils and other dependencies, run the following command:

\$ sudo apt install -y qemu qemu-kvm libvirt-daemon libvirt-clients bridge-utils virt-manager

- The gemu package (quick emulator) is an application that allows you to perform hardware virtualization.
- The qemu-kvm package is the main KVM package.
- The libvritd-daemon is the virtualization daemon.
- The bridge-utils package helps you create a bridge connection to allow other users to access a virtual machine other than the host system.
- The virt-manager is an application for managing virtual machines through a graphical user interface.

Next, you need to confirm that the virtualization daemon, libvritd-daemon, is running by executing the following command:

```
$ sudo systemctl status libvirtd
libvirtd.service - Virtualization daemon
Loaded: loaded (/lib/systemd/system/libvirtd.service; enabled; vendor preset: enabled)
Active: active (running) since Sun 2020-10-18 15:08:34 PDT; 1 months 16 days ago
```

If you want to start it on boot, you can run this command:

\$ sudo systemctl enable --now libvirtd

To check if the KVM modules are loaded, run the following command:

\$ lsmod | grep -i kvm

From the output, you can observe the presence of the kvm_intel module. However, this is the case for Intel processors. For AMD CPUs, you get the kvm_amd output instead:

```
$ lsmod | grep -i kvm
kvm_intel 282624 0
kvm 663552 1 kvm_intel
```

Deploying NSM on KVM

This section describes more about the following topics:

- Creating a Virtual Machine via Command Line
- Creating a Virtual Machine via Virtual Manager
After installing KVM successfully, you have to create a virtual machine by following any of the two methods. You can create a virtual machine on the command-line or using the KVM virt-manager graphical interface (preferred).

Creating a Virtual Machine via Command Line

The virt-install command-line tool is used for creating virtual machines on the terminal. A number of parameters are required when creating a virtual machine. To create a virtual machine execute the following command (replace the image file path with the appropriate file):



		Virtual Machine Manager	>
🔛 🔲 Open 🕨 📗	0 -		
Name			✓ CPU usage

\$ sudo virt-install --name nsm --vcpus 4 --memory 16384 --import --disk
/home/ghan/Downloads/SonicWall_NSM_On-Prem__For_QEMU_VM.img --os-variant generic

- The "--name" option specifies the name of the new virtual machine.
- The "--vcpus" option indicates the CPU cores, which in this case is set to 4 cores.
- The "--memory" indicates the RAM capacity, which is 16 GB. Note that this requires your host to have a large memory for the best working experience.
- The "--import" option specifies that the virtual machine is imported from the virtual disk image specified by the "--disk" option which points to the image file path.
- The "--os-variant" option is set to "generic" in this case.





Immediately after executing the command, the virtual machine boots up and the installer gets ready for the installation of the virtual machine.

aman@aman-5520: ~ – 🗆
File Edit View Search Terminal Help
<pre>File "/usr/lib/python2.7/dist-packages/urllib3/_initpy", line 16, in <module> from .poolmanager import PoolManager, ProxyManager, proxy from url file "/usr/lib/python2.7/dist-packages/urllib3/poolmanager.py", line 54, in <module> PoolKey = collections.namedtuple('PoolKey', key fields) File "/usr/lib/python2.7/collections.py", line 386, in namedtuple exec class definition in namespace File "<strings", 1,="" <module="" in="" line=""> KeyboardInterrupt aman@aman-5520 ~ \$ clear amaneman-5520 ~ \$ sudo virt-installname nsm-kvmvcpus 4memory 16384importdisk ~/Downloads/Sonic all_NSM_On-Prem_For_QEMU_VM.imgos-variant generic</strings",></module></module></pre>

	Virtual Machine Manager	– 🗆 ×
File Edit View Help		
🔛 🔲 Open 🕨 🚺 🖸		
Name		CPU usage
✓ QEMU/KVM		
Running		

		nsm-kvm (1) - Virt Viewer	
Menu System Info Storage	System Info GUID	: E8C59E6C-490B-49D5-B3F5-E392E8CA2F20	
Network Interfaces Diagnostics NTP Server System Update Reboot I Shutdown About Logs	System Time Up Time Load Average	: Thu 2021-06-17 21:21:52 UTC : 5 minutes 23 seconds : 3.1 1min 2.4 5min 1.1 10min	
		 ▶	
Up ∕ Down to select items TAB to move between views Enter to action∕edit an item			

Creating a Virtual Machine via Virtual Manager

You can create a virtual machine through by using the Virtual Machine Manager application. This application can be opened by either running the virt manager command, \$ virt-manager, or by opening it through your system:

1. If you have access to the console, you can open the virtual machine manager under **Applications** | **System > Virtual Machine Manager**.





2. Click the monitor icon to start creating a virtual machine.

File Edit View Help
🔛 💻 Open 🕨 🚺 🥝 👻
QEMU/KVM
Click this is an

3. On the pop-up window, choose Import existing disk image.



- 4. Click Forward to continue.
- 5. Browse your local directory and locate the image file, and then type in 'Generic default' in the **Operating System** field.
- 6. Click Forward.



7. Next, set the memory to 16 (GB), and CPU to 4 (cores) and click Forward.



- 8. Set the VM name.
- 9. Choose the network option (default is NAT).
- 10. Click **Finish**. You can access the NSM UI from the host system only if the Network selection is in NAT mode. For the public access, please configure the Network to **Bridge** mode.

Create a new virtual machine Step 4 of 4	
Ready to begin the installation Name: nsm	
OS: Generic default Install: Import existing OS image Memory: 16384 MiB	
CPUs: 4 Storage:On-Prem_For_QEMU_VM_1787.img Customize configuration before install	
✓ Network selection Virtual network 'default' : NAT	
😢 Cancel 🛛 🐳 Back	Finish

Once it's done, you should see the Management Console. You can navigate to the **Network Interface** section to get the IPv4 address of VM and access the NSM UI by using it.

	vm1 on QEMU/KVM	-	• 🛛
File Virtual Machine View Send Ke	y .		
📃 💡 ト 🗉 😃 🗸			6D
Menu	Network Interfaces	 _	
System Info	Network interface	ens3	
Network Interfaces	DHCP	Enabled	
NTP Server	IPv4 Address	10.11.53.241	
System Update	Netmask	255.255.255.0	
Reboot Shutdown	Mac address	52:54:00:83:8c:74	
Logs	Gateway	10.11.55.1	
2090	Global DNS nameservers		
	DNS 1	8.8.8.8	
	DNS 2	8.8.4.4	

F	ile Edit View Help	
	🚔 📃 Open 🕨 🔢 🥹 👻	
	QEMURVM	
	Running	\sim
File Virtual Machine View Send	d Key	
💻 🕡 🕨 🖬 🥹 🔹 🤻	6	E Sa Carlor
	Initializing services: IMPORTANT, DO NOT POWEROFF OR REBO	T
	Initializing services: 11 × complete	****

To open NSM in browser, provide the network information in the management console. When the installation and reboot is complete, go to NSM Settings and Registration to configure the network settings and register NSM.

Installing NSM on Azure

6

This chapter provides you with the information on how to deploy the NSM file on your Azure server.

To deploy from Azure Marketplace:

- 1. Navigate to the Azure services portal.
- 2. Select Marketplace.
- 3. Find the SonicWall-Network Security Manager tile and select Create.

SonicWall-Network : Manager -BYOL	Security
SonicWall Inc	
Virtual Machine	
SonicWall Network Securi (NSM)	ity Manager
Bring your own license	

4. On the Basics tab to Create a virtual machine, select Create new in the Resource group field.

×	Create a virtual mac	hine	
	Basics Disks Networking	Management Advanced Tags Review + create	
🔀 Tile view ∨	Create a virtual machine that runs Lin image. Complete the Basics tab then tab for full customization. Learn mor	nux or Windows. Select an image from Azure marketplace or use your own Review + create to provision a virtual machine with default parameters or re 🖻	customized review each
	Project details		
	Select the subscription to manage de your resources.	eployed resources and costs. Use resource groups like folders to organize a	nd manage a
	Subscription * (i)	Microsoft Azure Enterprise	~
	Resource group * ①	(New) Resource group	~
	Academice group	Create new	
	Instance details		
	Virtual machine name * ①		
	Region * 🕕	(US) Central US	~
	Availability options 🕕	No infrastructure redundancy required	~
	Image * 🛈	SonicWall Network Security Manager-BYOL - Gen1	~
		See all images	
	Azure Spot instance ①		
	Size * ①	Standard_D8_v3 - 8 vcpus, 32 GiB memory (\$321.20/month)	~
		See all sizes	
	Administrator account		
	Authentication type ①	 SSH public key 	
		O Password	
		Azure now automatically generates an SSH key pair for you and al store it for future use. It is a fast, simple, and secure way to conne- virtual machine.	llows you to ct to your
	Username * 🛈	management	
	SSH public key source	Generate new key pair	~

- 5. Type an easy-to-identify name in the **Name** field and click **OK**.
- 6. Enter the Virtual machine name. It can be the same as the Resource group name, if you want.
- 7. Set the **Region**.
- 8. From the Image drop-down list, select the SonicWall-Network Security Manager -BYOL.
- 9. Leave Azure Spot instance unchecked.
- 10. Select the size of your virtual machine. The recommended sizes have been tested with NSM. You can see the Capacity Requirements section to learn more about the recommended machine sizes.
- 11. In Authentication type, select SSH public key.

- 12. Define the **Username** as **"management**". If you fail to do so, you will not be able to access NSM console and need to redeploy the NSM image.
- 13. Generate a public key through command lin: ssh -keygen.
- 14. Copy and paste that key in SSH public key field.
- 15. Click **Next : Disks >**.

Create	a vi	rtual mac	hine				
Basics	Disks	Networking	Management	Advanced	Tags	Review + create	
Azure VMs The size of	have on the VM	e operating syste determines the ty	em disk and a temp /pe of storage you	orary disk for s can use and th	hort-term e number	storage. You can attach additional of of data disks allowed. Learn more	data disks.
Disk optio	ns			l.	÷.		
OS disk typ	e * 🕕		Standard	SSD (locally-red	lundant s	torage)	\sim
Encryption	type *		(Default) E	Encryption at-re	est with a	platform-managed key	\sim
Enable Ultr	a Disk co	ompatibility 🛈	Ultra disk is	available only	for Availa	bility Zones in centralus.	
Data disks	5						
You can ad temporary	d and co disk.	onfigure addition	al data disks for you	ur virtual machi	ne or atta	ach existing disks. This VM also come	s with a
LUN	N	ame	Size (GiB)	Disk t	ype	Host caching	
Create and	aitach a	i new disk At	tach an existing dis	k			
✓ Adva	anced						

- 16. Use the defaults on the Disks tab.
- 17. Click Next : Networking >.

Create a virtual mach	line
Pasies Dieles Naturating	Management Advanced Toos Devices create
basics Disks Networking	Management Advanced Tags Review + create
Define network connectivity for your v ports, inbound and outbound connect Learn more 😅	irtual machine by configuring network interface card (NIC) settings. You can control ívity with security group rules, or place behind an existing load balancing solution.
Network interface	
When creating a virtual machine a net	work interface will be created for you
When creating a writian machine, a ner	work interface will be created for you.
Virtual network * 🕕	(new) nsmazuredoc-vnet
	Create new
Subnet * 🛈	(new) default (10.6.0.0/24)
Public IP 🛈	(new) nsmazuredoc-ip
	Create new
NIC network security aroup	○ None
·····	Basic
	Advanced
	0
	1 This VM image has preconfigured NSG rules
Configure network security group *	(new) nsmazuredoc-nsg
	Create new
Accelerated networking	
, <u> </u>	The selected image does not support accelerated networking
Lead below does	
Load balancing	
You can place this virtual machine in the	high ackend pool of an existing Azure load balancing solution. Learn more 🖻
Place this virtual machine behind an existing load balancing solution?	

- 18. Configure the network settings for your environment. The default settings can also work.
- 19. Click Next : Management >.

Basics	Disks	Networking	Management	Advanced	Tags	Review + create	
Configure	e monitori	ing and manager	nent options for yo	ur VM.			
Azure Se	curity Ce	enter					
Azure See Learn mo	curity Cen re 🖻	ter provides unifi	ed security manage	ement and adv	anced thre	eat protection across hybrid c	loud workloads.
🛛 You	r subscript	tion is protected	by Azure Security C	enter basic pla	in.		
Monitor	ing						
Boot diag	nostics (D	C Enable	with managed	d storage a	account (recommended)	
			O Enable	with custom s	storage ac	count	
			Disabl	e			
Enable O	S guest di	agnostics 🕕					
Identity							
System a	ssigned m	nanaged identity	0				
Azure Al	D						1
Login wit	h Azure A	D (Preview) 🕕					
A Th	iis image d	loes not support Lo	ogin with Azure AD.				
Auto-sh	utdown						
Enable au	ito-shutdo	i) nwa					
Guest O	S update	s					
Patch orc	hestration	options 🕕	Image de	fault			\sim
			Some pa Learn m	atch orchestrat ore	ion optior	ns are not available for this im	age.
A Th	is image d	loes not support A	zure-orchestrated pa	tching, Learn m	ore of		

- 20. Disable the Boot Diagnostics setting.
- 21. Set the rest of the management options as you want for your implementation. The default settings can also work.
- 22. Click Next : Advanced >.
- 23. Keep the defaults on the **Advanced** tab.
- 24. Click **Next : Tags >**.

Basics [Disks	Networking	Management	Advanced	Tags	Review + create	
Tags are na multiple res	ime/valu	e pairs that ena	ble you to categoria	ze resources and	d view cor	solidated billing by apply	ing the same tag to
manupicies	Jources	ind resource gr	Sups. count more a	bout tags o			
Note that if	f you cre	ate tags and the	en change resource	settings on oth	er tabs, yo	our tags will be automatica	ally updated.
Note that if	f you cre	ate tags and the	en change resource	settings on oth	er tabs, yo	our tags will be automatica	ally updated.
Note that if Name ①	f you cre	ate tags and the	en change resource Value ①	settings on oth	er tabs, yo	our tags will be automatica	ally updated.
Note that if Name ① NSMAzu	f you cre ureDoc	ate tags and the	en change resource Value ()	settings on oth	er tabs, yc	Resource	ally updated.

- 25. Define tags for you NSM instance. Using easy-to-remember tags can help you when searching a long list of VMs for a particular instance. You can set the **Value** the same as the **Name**.
- 26. Click Next : Review = Create >.
- 27. Review the settings that make up your VM to ensure accuracy. Click **Previous** to make corrections on prior tabs, if necessary.
- 28. Click Create to validate your VM and create the NSM instance. This step a few minutes to complete.

CreateVm-	ite	amional nan-azure gravie 20210221	i stalili Overview 🖈 …		
		Delete 🚫 Cancel 🕕 Redeploy 🖒 Refresh	•		
🙏 Overview	0	We'd love your feedback! →			
😨 Inputs					
š≣ Outputs		Deployment is in progress			
Template	۲	Deployment name: CreateVm-sonicwall-inc.sonicwall-nsm-azure-pr Subscription: Microsoft Azure Enterprise Resource group: nsmazuredoc	Start time: 5/21/2021, 10:39:29 AM Correlation ID:		
	^	Deployment details (Download)			
		Resource	Туре	Status	Operation details
		osmazuredoc606	Microsoft.Network/networkInterfaces	Created	Operation details
		onsmazuredoc-vnet	Microsoft.Network/virtualNetworks	ок	Operation details
		📀 nsmazuredoc-ip	Microsoft.Network/publicIpAddresses	ок	Operation details
		onsmazuredoc-nsg	Microsoft.Network/networkSecurityGroups	ок	Operation details

A message displays when the deployment is complete.

Ø	Your deployment is complete	
۲	Deployment name: CreateVm-sonicwall-inc.sonicwall-nsm-azure-pr Sta Subscription: Microsoft Azure Enterprise Resource group: nsmazuredoc	art time: 5/21/2021, 10:39:29 AM prrelation ID:
\sim	Deployment details (Download)	
^	Next steps	
	Setup auto-shutdown Recommended	
	Monitor VM health, performance and network dependencies Recommende	ed
	Run a script inside the virtual machine Recommended	
	Go to resource Create another VM	

- 29. Click **Go to resource** from the deployment complete page.
- 30. Navigate to **Overview**.
- 31. Copy the IP address and paste it into a browser window. If the window returns an error, that's an indicator that deployment activity is still taking place.

You can set up the IP address through the NSM Management Console. Refer to Configuring Interface Settings for details.





Now you can begin configuring the network settings and licensing NSM. Refer to Registering NSM for the next steps.

NSM Settings and Registration

After the installation of the NSM image is complete, you need to define the network settings and register your product.

Topics:

- Configuring NSM Network Settings
- Registering NSM
- Associating Firewalls on MSW
- Unregistering NSM

Configuring NSM Network Settings

1. Open the NSM Management Console.

System Into System Into Heining Billion: Heining System Time: Privation System Time: System Time: System Time: System: System: System: System Time:	SonicWall_NSM_On-Prem_2.2.0-366_R366RG			Enforce US Keyboard Layout View Fullscreen Send Ctrl+Alt+Delete
Spring Bridge Returns interfaces Dispose in the fraces Rebuck 1 Skitchan Robot				
Spitom from Spitom from Hetwork later faces Higher fac				
Up ← Down to select items	Henu-	System Info-	1 42220EA1 EDEC 2221 DOTE DAA2210E0606	
<pre>Network interfaces Biggmostics hTP devoet Pheboot 1 Shutdeen Photo 1 Shutdeen Photo 1 Shutdeen Photo 2 Shutdeen Photo 2</pre>	Storage	GOTE	· 12332301-3010-7211-0071-010321030030	
Biagmontine hTF Searce Phone Notest Logs Up_r Rean to select items	Network Interfaces			
MT Server bytate by	Diagnostics	System Time	: Fri 2021-04-23 16:28:48 UTC	
ibiard generation initiaries de la constante de la constante de la constante de la constante logy Ug ∠ Roun to select items	NTP Server	Up Tine	3 minutes 5 seconds	
ibot Logi Ug ∕ Roun to select Lines	Beboot I Shutdown	Load noerage	. 2.0 1010 1.3 3010 0.3 10010	
Logz Ug_ Poun to select item	About			
Ug ≠ Roun to scient items	Logs			
lg ∕ Roun to select Lines				and the second
lg_r Roun to select Lines				
lg ∕ Roun to select Lines				
lg_r Roun to select lines				THE PARTY PARTY PARTY AND A
Ug ≠ Roun to scient items				
Ug ≠ Roun to select items				
Ug ≠ Boun to scient items				
Ug ≠ Boun to scient itons				THE PROPERTY PROPERTY AND A DESCRIPTION OF
Ug ≠ Boun to scient items				
Ug ≠ Boun to scient itons				
ųg,∠ Poun to select items				
ųg,∡ poun to select items				
ųg,∡ Poun to select items				
ųg,∡ poun to select items				
lg_r∕Roun to select items				
Ug.∠ Down to select items				
ųg_√ Roun to select items				
Up,∞ Down to select items				
Up ≠ Down to select itoms				
Up ≠ Down to science itoms				
Up ∞ Down to select items				
Up ≠ Bown to scheet items				
Up ≠ Down to select items				
Up / Down to select items				
Up / Down to select items				and the state of the state of the state of the
	Up / Down to select items			

2. Navigate to the **Network Interface** setting, and press **Enter**.

SonicWall_NSM_On-Prem_2.2.0-366_	_R366RG			Enforce US Keyboard Layout	View Fullscreen Send Ctrl+Alt+Delete
	- Henu	-Network Interfaces			
	System Info	Network interface	I ens160 J		
	Storage Network Interfaces	DHCP	Disabled 1		
	Diagnostics	IPud Addresse	A DESCRIPTION OF		
	System Update	Netnask	i an an i		
	Reboot I Shutdown About	Mac address Gateway			
	Logs				
		Global DMS nameservers DMS 1	1		
		DNS 2	1		
	Up / Down to select items				
	TAB to move between views Enter to action/edit an item				

- 3. Select ens160.
- 4. Navigate to the **DHCP** field, and press **Enter**.
- 5. Select No and press Enter to confirm.
- 6. Update the IPv4 Address, the Netmask, and Gateway.
- 7. Save the settings.
- 8. Enter the **DNS 1** and **DNS 2** and Save **Changes**.
- 9. To verify that all the network settings were defined correctly, ping the IPv4 address from the command prompt to make sure you can access NSM.

Registering NSM

After setting up your virtual machine and downloading the NSM image, the next step is to synchronize the NSM instance with the MSW licensing information.

To register and configure NSM:

1. Enter the IPv4 address of the NSM instance in a web browser.

SONICWALL	
Login with your credentials	
Usemame	
enter saeraante	
	What is SonicWall Analytics? SonicWall Reporting and Analytics Platform
	SonicWall Analytics Live Demo Larm more about SonicWall Analytics by watching the five damo
18 20	Empowered by Capture Security Center Rebuse operating service agility by partnering with ServicWat Analytics and Capture Cloud

- 2. For initial access, log in using **admin** and **password** as our credentials. The first time you access NSM, it presents an initialization wizard.
 - (i) **NOTE:** It is recommended to change the default password after the initial configuration.

Register NSM	
MySonicWall Username	
MySonicWall Password	
MySonicWall Friendly Name	
Serial Number	
Auth Code	
Cancel	Register

- 3. Enter your MySonicWall Username and Password.
- 4. Enter a MySonicWall Friendly Name.
- 5. Enter the Serial Number and Authorization Code received from your sales representative.
- 6. Click Register.
- 7. To confirm registration, navigate to Manager View | System > Settings > Licenses.
- 8. Validate that the status of your NSM is **Licensed**.
- 9. Click **Synchronize** to synchronize your NSM instance with the License Manager on MSW.

While working on MSW, you can also associate firewalls with the NSM On-Premises instance.

Associating Firewalls on MSW

Rather than adding firewalls for management through NSM, you can opt to associate the firewalls to NSM through MySonicWall.

- 1. After signing into MySonicWall, navigate to My workspace and click on Register Products.
- 2. Choose the same tenant as chosen for the NSM On-Premises instance.
- 3. Type in the serial number, authentication code and friendly name of the firewall.
- 4. Chose On-Prem in the management options.

Register Products		
		3
CHOOSE A TENANT	PRODUCT REGISTRATION DETAILS	MANAGEMENT OPTIONS
1 Firewall selected Firewall Management through:		
Cloud ¹		
 On-Prem Enable Zero Touch On-Box 		

- 5. Enable Zero Touch.
- 6. Select the NSM On-Premises IP from the GMS Server Public IP/FQDN drop-down list.

GMS Server Public IP/FQDN Choose On-Premise GMS Server Choose On-Premise GMS Server 1.1.1.1-0040103C903D	ON-PREMISE GMS SERVER CONFIGURATION:				
✓ Choose On-Premise GMS Server 1.1.1.1-0040103C903D	GMS Server Public IP/FQDN	Choose On-Premise GMS Server 🛛 🔻			
1.1.1.1-0040103C903D		✓ Choose On-Premise GMS Server			
		1.1.1.1-0040103C903D			
10.5.41.88-00401029FF0F		10.5.41.88-00401029FF0F			

7. Click Save/Register.

Unregistering NSM

You can unregister your NSM On-Premises instance directly from the management interface. Deregistration puts the instance into the unregistered state. You need to contact customer support team to do trust reset before you can reuse the NSM serial number. Then you can use the serial number to register the same or another instance. Only one NSM On-Premises instance is allowed per serial number. Be sure to delete the old, now unused VM.

Console Operations

The NSM Management Console provides additional options for viewing and changing system and network settings. You can also use it to run diagnostics, reboot the system and other functions.

Topics:

- Management Console Operations
- NSM Management Console Menu
- Using SafeMode on the Management Console

Management Console Operations

To access the Management Console:

1. Navigate to the virtual machine manager, select your NSM On-Premises, and right-click on **Connect**. The Management Console appears:

r-Menu	Tr-System Info	
System Info	GUID	
Network Interfaces		
Diagnostics	11	
NTP Server	System Time	: Wed 2022-07-27 14:15:19 UTC
System Update	Up Time	: 3 minutes 17 seconds
Reboot I Shutdown	Load Average	: 2.2 1min 1.3 5min 0.6 10min
About	11	
Logs	11	
	11	

- 2. The main menu is displayed in the side menu (left panel). 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.
- 3. Press the Tab key to move the focus from side menu to the main view (right pane), or vice versa.
- 4. In the main view, use the up/down arrow keys to move the focus between options. Items shown inside square brackets denote actionable items.



5. 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 **Enter**.

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:



 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.

NSM Management Console Menu

NSM on-premises management menu choices are described in the following sections:

- System Info
- Network Interfaces
- Diagnostics
- NTP Server
- System Update
- Reboot/Shutdown
- About
- Logs

System Info

Menu System Info Network Interfaces			I
Diagnostics NTP Server System Update Reboot I Shutdown Ahout	System Time Up Time Load Average	: Wed 2022-07-27 14:15:19 UTC : 3 minutes 17 seconds : 2.2 1min 1.3 5min 0.6 10min	
Logs			

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

- GUID Every On-Premises Analytics instance has a GUID which is displayed here.
- System Time This is the current system time on the NSM On-Premises instance.
- Up Time This is the total time that the NSM On-Premises instance has been running.
- Load Average 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.

Network Interfaces



In the Network Interface screen, you can configure these settings.

- **Network Interface** This is the current interface serving as the management interface. This defaults to ens160.
- **DHCP** This displays if the DHCP is enabled or disabled.
- 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.
- Gateway This is the default gateway currently in use by the NSM On-Premises instance.
- DNS This is a list of the DNS servers currently being used by the NSM On-Premises instance.

Diagnostics

The **Diagnostics** 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 NSM On-Premises instance. Another option is to **Send diagnostics to SonicWall support**.

r-Menu	-Diagnostics		
System Info	Ping	Ping	
Network Interfaces	Nslookup	Ns lookup	
Diagnostics	Send diagnostics to SonicWall support	Send	
NTP Server			
System Update			
Reboot Shutdown			
About			
Logs			

To use ping:

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

To send Diagnostic Report:

In the **Diagnostics** screen, you can send diagnostics to SonicWall Technical Support.

(i) **NOTE:** Your NSM On-Premises instance must have internet access to send the diagnostics report to SonicWall Support.



- 1. To send the diagnostics report, select Send in the main view to highlight it.
- 2. Press **Enter**. A dialog box showing the diagnostics send output is displayed. The last message indicates success or failure.
- 3. 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

(i) **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.

Henu System Info Network Interfaces Diagnostics NTP Server System Update Reboot I Shutdown About Logs	NTP Server Sync with NTP server Current time Network time enabled NTP synchronized	l Perform sync 1 Wed 2022-07-27 14:26:19 UTC No Yes
---	--	--

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

- Sync with NTP server This button forces the NSM On-Premises instance's NTP client to perform a sync with the configured NTP server(s).
- Current time The current time on the NSM On-Premises instance.
- **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 NSM On-Premises instance is currently synchronized with the configured NTP servers.

System Update

The System Update screen provides function to start the system update.



Reboot/Shutdown

The **Reboot | Shutdown** screen provides functions for rebooting the instance, returning to factory defaults, and enabling SafeMode.

Menu	-Reboot Shutdown	
System Info	Reboot NSM	I Reboot J
Network Interfaces	Shutdown NSM	I Shutdown 1
Diagnostics ¹⁴	Boot with factory default settings	[Factory Default]
NTP Server	Boot NSM into safemode	I Enable 1
System Update		
Reboot Shutdown		
About		
Logs		

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 GMS- Restarts the instance with current configuration settings.
- Shutdown GMS Powers off the instance.
- **Boot with factory default settings** Restarts the instance using factory default settings. All configuration settings are erased.
- **Boot GMS into safeMode** Puts the NSM On-Premises instance into SafeMode. In this product, SafeMode does not offer additional functionality.

About

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



Logs

The Logs screen displays log events for the instance.

Menu	Jul 28 A5:39:35 Finished running self-tests (Known Answer Tests)
Sustem Info	Jul 28 A5:39:35 TIS 1 3 KDF test nassed
Netuenk Intenfaceo	In 20 AC 30:30:30 TIS TIS ANT CLASS ANT
Discussion	Jul 20 05.35.35 ILS NOT LEST passed
Diagnostics	
nir server	Jul 28 05:39:34 SHH2-384 test passed
System Update	Jul 28 05:39:34 SHA2-256 test passed
Reboot I Shutdown	Jul 28 05:39:33 SHA-1 test passed
About	Jul 28 05:39:32 RSA Verify test passed
Logs	Jul 28 05:39:32 RSA Sign test passed
	Jul 28 05:39:31 RSA PCT test passed
	Jul 28 05:39:30 HMAC-SHA2-512 test passed
	Jul 28 05:39:30 HMAC-SHA2-384 test passed
	Jul 28 05:39:29 HMAC-SHA2-256 test passed
	Jul 28 05:39:29 HMAC-SHA-1 test passed
	Jul 28 05:39:29 ECDSA Verifu test passed
	Jul 28 A5:39:29 ECDSA Sign test passed
	Jul 28 05:39:29 FCDSA PCT test passed
	Jul 28 A5:39:29 FCDH test passed
	Jul 28 05:39:29 CTR DRRC test passed
	Jul 20 05:35:25 CIN DADG (Est passed
	Jul 20 05:35:25 HES GEN (Encrypt a Decrypt) test passed
	Jul 28 05:39:29 HES UBU (Encrypt & Decrypt) test passed
	Jul 28 05:39:29 AES ECB (Decrypt) test passed
	Jul 28 05:39:28 AES ECB (Encrypt) test passed
	Jul 28 05:39:28 Started running self-tests (Known Answer Tests)
	Jul 28 05:39:28 Image Verification Done
	Jul 28 05:34:21 /usr/bin/update_engine_clientstatus
	Jul 28 05:34:21 /usr/bin/update_engine_clientstatus
	Jul 28 05:34:21 MgmtCnsle: Management console has started
	Jul 28 05:34:07 Start Verify Image
Up / Down to select items	
TAB to move between views	
Enter to action/edit an item	
Space to hide/show side menu	
	Arrow keus: Navigate view Current Line: 1 Lines: 29

Using SafeMode on the Management Console

- Enabling SafeMode
- Disabling SafeMode
- Configuring Network Interfaces in SafeMode
- Configuring Interface Settings
- Disabling an Interface
- Installing a Software Upgrade in SafeMode
- Downloading Logs in SafeMode

Enabling SafeMode

SafeMode can be enabled from the management console.



To enable SafeMode:

- 1. Access the NSM On-Premises through the respective virtual machine monitor remote console.
- 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 NSM On-Premises instance immediately reboots and comes back up in SafeMode.

(i) **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 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 NSM On-Premises instance immediately reboots and boots up in normal mode.

Configuring Network Interfaces in SafeMode

When the Management Console is in SafeMode, the **Network Interfaces** screen in the NSM On-Premises Console provides features to configure the NSM On-Premises interfaces:

() | NOTE: Changes made to interfaces in SafeMode are not persistent between reboots.

- **Network Interface** This is the currently selected interface. This defaults to **ens160**. Use this to select any of the NSM On-Premises interfaces.
- **DHCP** Determines whether addressing is static or handled automatically and dynamically by a DHCP server.
- 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.

Topics:

- Configuring Interface Settings
- Disabling an Interface

Configuring Interface Settings

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

Network interface	E	ens160	1
DHCP		Disabled	
IPu4 Address		10.5.44.41	
Netmask		255.255.240.	01
Mac address		00 : 50 : 56 : 9a : 83	:57
Gateway		10.5.32.1	
GIODAI DHS NAMESERVERS			
		8.8.8.8	
JMS Z		8.8.4.4	
-Select Interface			
	-Network Interfaces Network interface DHCP IPo4 Address Netmask Mac address Gateway Global DNS nameservers DNS 1 DNS 2 -Select Interface ens160 ens192 Confirm (Enter)	Network Interfaces Network interface Network interface [DHCP [IPu4 Address [Metnask [Mac address [Gateway [Global DNS nameservers [DNS 1 [DNS 2 [Select Interface [ems160 [confirm <enter> Cancel</enter>	Network Interfaces ems160 DHCP I Disabled IPu4 Address I 0.5.44.41 Netmask I 255.255.240. Mac address 00:50:56:9a:83 Gateway I 10.5.32.1 Global DNS nameservers I 8.8.8.8 DNS 1 I 8.8.4.4 Select Interface ens160 ems192 Confirm (Enter) Cancel (Esc)

To edit an interface:

- In the SafeMode Network Interfaces screen, select the Network interface option and then press Enter. The Select Interface list appears, displaying all of the interfaces available on the NSM On-Premises instance.
- 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.
- 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.

Henu	-Network Interfaces			
System Info	Network interface	ens160		
Network Interfaces				
Diagnostics	DHCP	Enabled		
NTP Server	TRud Allows			
System Update	IPU4 Address			
About	Mag address			
Logs	Gateway			
	in course			
	Global DNS nameservers			
	DNS 1	8.8.8.8		
	DNS 2	8.8.4.4		
	Save changes		Cance 1	
I Im ∠ Down to select items — I				
Up / Down to select items TAB to move between views				

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

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

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 Network Interfaces screen, select the Network interfaces option.
- 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. For example, select IPv4 Address and press Enter.
The on-screen dialog displays the current IP address.

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

r-Menu				
System Info	Network interface		ens160	
Network Interfaces				
Diagnostics	DHCP		Disabled	
NTP Server				
System Update	IPu4 Address	E	10.5.44.41	1
Reboot Shutdown	Netmask	L. L.	255.255.240.0	9]
About	Mac address	0	0:50:56:9a:83	:57
Logs	Gateway		10.5.32.1	
	Global DNS nameservers			
	DNS 1		8.8.8.8	
	DNS 2		8.8.4.4	
	Enter IP address			
	0.0.0			
	Confirm (Enter)			

5. Press Tab to select the Save changes button and then press Enter.

r Menu	Network Interfaces		
Sustem Info	Network interface	[ens160]	
Network Interfaces			
Diagnostics	DUCD	I Disabled 1	
Diagnostics	DHCT	i Disabica i	
MIP Server			
System Update	IPu4 Address	[0.0.0.0]	
Reboot Shutdown	Netmask	[255.255.240.0]	
About	Mac address	00:50:56:9a:83:57	
Lows	Gateway	F 10 5 32 1 1	
2093	du cowig	101010111	
	Clarks I DNC services		
	Global DMS nameservers		
	DNS 1	[8.8.8.8]	
	DNS 2	[8.8.4.4]	
	Sava altanuas		0
	Save changes		Cancel

6. The interface is disabled.

(i) **NOTE:** Disabling DHCP may be sufficient to disable the interface.

Installing a Software Upgrade in SafeMode

SWI files are used to upgrade NSM On-Premises. You can download the latest SWI image file from MySonicWall.

In SafeMode, you can upload a new SWI image and apply it to the NSM On-Premises instance. The SafeMode web management interface is used to perform an upgrade, rather than SafeMode in the Management Console. When viewing the Management Console in SafeMode, the URL for the SafeMode web interface is displayed at the bottom of the screen.

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

To install a new system image from SafeMode:

- 1. With the NSM On-Premises instance in SafeMode, view the 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				
NSM 📮 FIRMWARE 🔎 DIAG	inostics 💄 administration			
Firmware Images Application Ba	ackups			
			🕹 Upload Image 🔱 Exit Safe Mode 🧃	Factory Reset
SYSTEM				
# VERSION	BUILD NUMBER	INSTALL		
1 Current Version				
6.5.0-696 Total: 1 item(s)				

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.

Upload Image	
Upload Image	Browse
Uploading a new image will overwrite any existing uploaded image	je.
You can get the latest images at www.mysonicwall.com.	
Download the image to your local disk, and then upload it to your Images have a file extension of .swi, e.g., update.swi. After the im	SonicWall using this dialog. Use the "Browse" button to find the file you want to upload. System age has uploaded, you will be able to install the new version of the System.
	Cancel Upload

- 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

The NSM On-Premises Instance reboots with the new image.

Downloading Logs in SafeMode

When the NSM On-Premises instance 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. Login to NSM management console in SafeMode.
- 2. Navigate **DIAGNOSTICS** tab.

SONIC	LC	
NSM 📃 FIRMWARE		
	•	
		💩 Download System Logs
SYSTEM INFORMATION		
Build Version	6.5.0-696	
System Time	08:57:08	
Uptime	50 Minutes	
CPU Load Averages	0.12, 0.04, 0.01	

3. Click the **Download System Logs** button. On prompting for confirmation, click on **Confirm**. A compressed file is downloaded which contains a number of files, including a **console_logs** file that contains detailed logging information.

Using NSM

9

Once your NSM instance is operational, you can begin setting it up to manage your network. The instructions provided here are intended to help you get started, but for more detailed information refer to the *Network Security Manager Administration Guide* which is available at the Technical Documentation portal.

Topics:

- Interface Overview
- Dashboard
- Creating a Tenant
- Creating a New User
- Adding a Device

Interface Overview

Understanding the NSM interface design and layout can help you more easily navigate the functions within NSM. When you first log into NSM, the Inventory table is the default page shown. Using the Inventory table as an example, the general interface layout is mapped in the following figure.

SCNCWALL	2 NSM Manager V	iew 🞆 HOME 🔒 SYSTEM	7		🕞 Commit	: & Deploy 良	C Q NA
``	Global Default Tenant	Home / Firewalls / Inventory				~ (~)	ៃ 🗗 🐔
'≣ Dashboard			OFFINE	ONLINE &			
— System		DEVICES 25% MANAGED	75% 3	0% UNMANAG	SED 100% 4	0%	0
Firewalls							
— Inventory — Groups	Q. Search	Group By: No Grouping		+ Add 🗂 Delete 📑 Ext	port 🖏 Refresh 🛛 🔅 Grid Settings	≣ List ♀ Map	: More Options
— Backups	# NAME 🔶	SERIAL NUMBER	GROUP	MODEL	TAGS CONNECTIVITY	CONFIGURATION	ACTION
🗮 Templates	1)		Unassigned	TZ 670	Offline	🔀 Unmanaged	=
🞒 Global Objects	2 🕨 👫		Unassigned		Offline	Unmanaged	≡
S VPN Topology	3 ▶ Å ∰		Unassigned	TZ 500 wireless-AC	Online	Managed	=
SD-WAN Topology	4 ▶ ♠∺ -		Unassigned	TZ 470W	Offline	Unmanaged	=
				ــ/_)		
Conng Management				11			
🜲 Tenant					,		
' User Management							
💼 Reports							
🞽 Logs & Alerts							
Legal Information							
🔶 API							Displaying 4 devices
							Displaying 4 devices

Reference	Interface Item	Description
1	Left command menu	Displays the primary tasks and commands that can be selected. The command menu varies depending upon which view you are in and the command option you have selected.
2	Show/hide commands icon	Acts as a switch to show or hide the left command menu. Click it to hide the command menu; click it again to show it.
3	Tenant name	Shows the name of the tenant whose data you are viewing. This is also a drop- down menu; click the tenant name to see all the tenants associated with your NSM instance.
4	View name	Shows which view is active in the interface. The Manager View is active in the example and is the default. The view represents the top level grouping of related tasks and commands. Refer to NSM Views for more details.
5	Command path	Shows the series of menu items selected to get to the information shown in the work space. In the documentation this same path is represented as HOME > Firewall View> Inventory . Sometimes this series of commands is also called the bread crumbs.
6	Home Command	Acts as the Home command for the selected option.
7	System	Displays the System overview of NSM.
8	Notification icon	Opens the Notification Center. The number above the icon indicates the number of alerts detected. Refer to Notification Center for more details.
9	Help icon	Opens the Technical Documentation website where you can access the product documentation.
10	User icon	Shows the initials of the user that's logged in but it also acts as a drop-down list. It shows the user name, user profile, the version of the product and the Log Out option.
11	Work space	Displays the data associated with the menu options or commands selected. This can be a table, as shown in the example, a dashboard or a series of options to select or define.

(i) **NOTE:** Information on the **Commit & Deploy Wizard** is provided in the *Network Security Manager Administration Guide*.

Dashboard

SonicWall offers the option to host NSM on-premises hosted on your organization's local server. When you log in, NSM on-prem provides is the Manager View .

(i) **NOTE:** When user logs in for the first time, a pop-up displays to enable/disable the **Allow NSM to collect anonymized usage data** to help improve the NSM. The pop-up continues to display till the action is performed once.





The three green notification icons at the top of the interface display more information on CPU Utilization, Memory Utilization, and Disk Utilization. Click on **View Details** to take a deep dive into the system monitoring details:



Creating a Tenant

To create a tenant on NSM:

1. In Home view, click Tenant.

SONICWALL	€ изм	Manager View	SYSTE	М		🛃 Con	nmit & Deploy	😥 🔅	Rate 😌 Q NA
	Global	Default Tenant / Home /	Tenant						•••
📜 Dashboard	Q Search.					+ Add	🗑 Delete	🗘 Refresh	🔅 Column Selection
- System		NAME	41145	DEFAULT ADMIN			_		
💥 Firewalls			ALIAS	DEPAGLI ADMIN					
- Inventory	I	All Tenants	All Tenants						
- Groups	2	🕨 💩 Global Default Tena	ant DefaultTenant	nsmadmin@sonicwall.com					
🧮 Templates									
Config Management									
ᡖ Tenant	•								
' User Management									
Scheduled Reports									
Logs & Alerts									
	1								
🔶 API									

- 2. Click Add icon.
- 3. In the Add Tenant window, enter Tenant Name, and select Log Level and Alert Level.

Add Tenant			•
Tenant Name *			
Log Level *	Error	•	
Alert Level *	Alert	-	
	Close		dd

- 4. Click Add.
- 5. Register devices under the tenant.

Creating a New User

To create users:

1. In **Home** view, navigate to **User Management > Users**.

SONICWALL	A Manager View	SYSTEM		🕞 Commit & Deploy 🌔 🔆 Rate 🛛	999+ Q NA
	📙 All Tenants / Home / User Management / U	Isers			•••
Dashboard	ALL USERS	ADMIN	USERS OPERATOR	CUSTOM ROLE	
- System	2	0% 0	0% OSERS	0% OSERS	
— Inventory				Add User	
— Groups	Q Search Role(s):	Tenant(s):	Authentication Server(s):	Add Us Delete U Refre Expo	🏟 Column Sele
Templates					
Config Management	# USERNAME	ROLE	User with full	BETA FEATURES	ACTION
👃 Tenant	1. 🕨 admin	S SuperAdmin	permission in this system		••••
📜 User Management	2. > ztadmin	S SuperAdmin	Zero Touch User with full permission in this		
— Status — Users			system	9	
 Roles and Permissions 					
 Authentication Servers 					
Scheduled Reports					
Logs & Alerts					
- Legal Information					
🔶 API					

- 2. Click Add User.
- 3. In the Add New User window, enter details of the new user.

Add New User				
General Access				
	Authentica	ation Server *	Local Authentication 🛛 🔻	ype: Local)
Username *	Enter Username		First Name	Enter First Name
Primary Email *	Enter Primary Email		Middle Name	Enter Middle Name
Secondary Email	Enter Secondary Email		Last Name	Enter Last Name
Password *	Enter Password		Timeout	15
Confirm Password	Confirm Password		Two-Factor Authentication	
Phone	Enter Phone Number			
Comment	Enter Comment			
Notifications				
				Cancel Next

4. Click **Next** to go to the **Access** tab.

Add New User	
General Access	
USINGRAE(W	
ROLE	
TENANTS & DEVICES	
No Tenant / Group	
	Cancel Save

- 5. Click the **Edit** icon for **ROLE**.
- 6. Select the role from the drop-down list and click **Save**.
- 7. Return to the main **Access** tab.
- 8. Click the Edit icon for TENANTS & DEVICES.

Add New User			
General Access			
5 TENANTS / GROUPS / DEVICES			
TENANTS / GROUPS		DEVICES	
Q Search for Tenant / Group	Q	Q Search for Device	(0/1)
Selected Devices	0	No devices	
🛄 🋕 Global Default Tenant	0		TENANTS / GROUPS
			0/0 SELECTED DEVICES

- 9. Select **TENANTS/GROUPS** and **DEVICES** from the options provided.
- 10. Click Apply.

Adding a Device

To add a device to firewall inventory:

- 1. Log in to NSM.
- 2. Click **Firewall > Inventory**.

SONICWALL	Image NSM Manager View mage HOM Image NSM Manager View mage HOM Image NSM Manager View mage HOM Image HOM	E 📑 SYSTEM			🛃 Con
	Biobal Default Tenant / Home / Firewall	s / Inventory			
Dashboard			ONLINE &	•	
— System	(\mathbf{O})	ALL DEVICES	0% MANAGED	0% OFFLINE	0% UNMANAGED 100%
👫 Firewalls		27	0	0	0
— Inventory	•				
— Groups	Q Search				🕇 🕂 Add 🖉 📅 Delete 🛛 🖆 Export 🕻
Templates	# NAME	SERIAL NUMBER	GROUP	MODEL	TAGS CONNECTIVITY
O Config Management	🗌 1 🗼 🙀 NSADummy1068	C0EAE1000068	Unassigned		Offline
	2 🕨 🙀 NSADummy1069	C0EAE1000069	Unassigned		Offline
👃 Tenant	🔲 3 🕨 🙀 NSADummy1070	C0EAE1000070	Unassigned		Offline

- 3. Click Add > Add Unit.
- 4. Enter the serial number and other information.

Serial Number *	
Friendly Name	
IP Address with Port (Example: 34.25.61.2:443)	
Verify SSL Certificate	0
Username	
Password	
Tags (Example:TZ, BranchA)	0

5. Click Save.

Integrate On-Prem Analytics with NSM

On-prem NSM integrates with SonicWall On-prem Analytics to provide integrated user interface to manage firewall policy and monitor network traffic. On-prem NSM can be integrated with SonicWall IPFIX or Syslog based analytics. After integration of on-prem NSM and on-prem analytics, data collected by the SonicWall analytics is available within NSM user interface. To integrate on-prem NSM and analytics requires specifying detail of analytics system in NSM, then enabling firewall to view analytic data and accessing firewall analytic data

- (i) NOTE: Before proceeding with NSM integration please ensure desired SonicWall Analytics is working fine and firewall is configured to send data to analytics.
 - Integrate SonicWall Analytics in NSM
 - Enable Analytics While Adding a New Device
 - Enable Firewall to View Analytics Data
 - Accessing Analytics Data

Integrate SonicWall Analytics in NSM

To add On-Prem Analytics details in NSM:

- 1. Access NSM using IP address. Login with username and password.
- 2. Under System, navigate to Settings > Analytics Agent.
- 3. Click on Add.



- 4. Enter the **Name** of the analytics agent and select **Type of Analytics Install** from the drop down. You can select Flow Analytics for Analytics On-Prem IPFIX and Syslog Analytics for Analytics On-Prem Syslog.
- 5. Enter the login details of the analytics agent.

Add Analytics	Agent
Name	
Type of Analytics Install	Flow Analytics 👻
LOGIN DETAILS FOR ANALYT	TICS AGENT
IP Address / FQDN	
Username	
Password	
	Cancel Save

6. Click Save.

Enable Analytics While Adding a New Device

To add an analytics agent while adding a new device:

- 1. Under Home, navigate to **Firewalls > Inventory**.
- 2. Click on Add.
- 3. Add the new device information.
- 4. Under Reporting and Analytics, enable the Integrate External Analytics Agent for this device button.
- 5. Select the added analytics agent from the dropdown of **Analytics Agent** field.
 - INOTE: You can also add a new agent here by clicking on ✓ icon and selecting Add Analytics Agent in Analytics Agent field.

Add Device	•
Serial Number *	
Friendly Name	
IP Address with Port (Example: 34.25.61.2:443)	
Username	
Password	
Verify SSL Certificate	0
Tags (Example: TZ, BranchA)	0
REPORTING & ANALYTICS	
Integrate External Analytics Agent for this device	0
Analytics Agent	Select Agent 💌 💉
	Cancel Save Acquire Again

6. Click Save.

Enable Firewall to View Analytics Data

To add an analytics agent for zero-touch enabled or already added device in NSM::

- 1. Under Home, navigate to Firewalls > Inventory.
- 2. Select the firewall on which Analytics is running and click on \equiv icon below **Action** column and click on **Edit Settings**.

SONICWALL	← NSM Manager View	HOME 📑 SYSTEM		🕞 Commit & Do	eploy 😥 🥙 Q 🛛 🗤
	Blobal Default Tenant / Ho	me / Firewalls / Inventory			•••
Dashboard					
— System	DEVICES 50%	MANAGED 50%	offline 0%	UNMANAGED 0%	UNASSIGNED 50%
🚎 Firewalls	4	12		0	U
— Inventory					
— Groups	Q Search	Group By: No Grou 💌 🕂 🕂	Add 🍵 Delete 🛛 📩 Export	🕽 Refresh 🛛 🛱 Grid Setting:	More Options
— Backups	# NAME 🕇	SERIAL NUMBER GROU	JP MODEL	TAGS CONNECTIVITY	CONFIGURATION ACTION
Templates	🗌 1 🔹 🕨 📩 gen6 Swit	2CB8ED038F80 swite	h NSa 4650	😑 Online	Managed 📃
📫 Global Objects	🗌 2 🕨 📐 NSA 5600	COEAE4EB4FB0 swite	h NSA 5600	😑 Of 😝 Swit	ch to Firewall View
	🔄 3 🔹 🕨 🛵 SONICWA	2CB8ED695848 gen7	switch TZ 470	ei 🖌 Edit :	Settings
S VPN Topology	🗌 4 🔹 🕨 🙀 TZ 570P	2CB8ED6DF240 gen7	switch TZ 570P		- hronize Firewall
🔅 SD-WAN Topology				دو دربر ا	rade Firmware
0				↓	to Config Audit
Config Management					
Tenant				99 00 0	Coning Audit
				Mana	age Commits
User Management				🛱 Expo	rt to Template
Reports				🚷 Com	mit Certificates
				🖪 Crea	te Report Rule Vices

- 3. Under Reporting and Analytics, enable the Integrate External Analytics Agent for this device button.
- 4. Select the added analytics agent from the dropdown of **Analytics Agent** field.
- 5. Click Save.

Accessing Analytics Data

To access analytics data in NSM:

- 1. Under Home, navigate to **Firewalls > Inventory**.
- 2. Click on the firewall which you have integrated with either IPFIX or Syslog to view that particular Firewall View.

	E NSM Manager View	HOME 📑 SYSTEM		🕞 Commit & Deploy	🏚 🤁 O 🔍 NA
	Biobal Default Tenant / Home	/ Firewalls / Inventory			•••
 Dashboard System Firewalls 	ALL DEVICES 100%	ONLINE & 0%	OFFLINE 0% ONLINE UNMAN 0	& 100%	UNASSIGNED 50%
— Inventory (— Groups	Q. Search Grou	p By: No Grou ▼ + Add	🗑 Delete 📑 Export 🛯 💭 Refres	F 🛱 Grid Setting:	More Option:
— Backups	# NAME 🔶	SERIAL NUMBER GROUP	MODEL TAG	S CONNECTIVITY	CONFIGURATION ACTION
Templates	1) NSa3650	2CB8ED191E00 Unassign	ed NSa 3650	Online	Managed
Global Objects	2	18B169091270 Unassign	ed TZ 400 wireless-AC	Online	Managed =
S VPN Topology					
🔅 SD-WAN Topology					
Config Management					
👃 Tenant					
' User Management					Displaying 2 devices

- 3. Navigate to the Monitor View to see the various analytics data as per the tabs on the left of the page.
 - IPFIX

	✓ NSM Firewall View	🔅 🕂 🎆 MONITOR 👻		🔓 Commit & Deploy 🏻 😩	: 🔩 🧬 🔉 Q NA
	Global Default Tenant TZ40	0W_HQ_FW (TZ 400 wireless-	AC) / Monitor / Analytics		•••
📺 Overview	LIST				🗮 List 📈 Graph 🔒 Log
🐌 Summary	Q + O - 5 Mins -		Custom	All Traffic 🗸	Limit: 50 💌 🔹 🚍
🐌 Details	Applications Sources	Destinations Users	Web Activities Threats	Devices Blocked	Group By: Applications
to Analytics	# APPLICATIONS	SESSIONS	TOTAL PACKETS	TOTAL DATA TRANSFERRED	THREATS
	1 App-10253	56	1.37K	963.38 KB	0
Alerts & Notifications	2 App-7841	5	10	940 B	0
	3 App-49175	3	16	900 B	0
	4 App-6820	5	10	880 B	0
	5 App-5183	1	4	574 B	0
	6 App-13547	56	641	355.43 KB	0
	7 App-10678	1	2	272 B	0
	8 App-5147	3	32	2.51 KB	0
	9 App-7927	56	2.79K	1.43 MB	0
	Total: 12 item(s)	198	4.91K	2.73 MB	0
	Grouped 12	entries out of 250000 Flows			Last Updated 2022-03-17T18:11

Syslog



11

Upgrade Instructions

This section describes more about the following topics:

- Upgrade Using Management Console
- Upgrading SonicOS Firmware
- (i) **IMPORTANT:** Before upgrading your NSM system, take a backup of your configuration. Follow the steps provided in Taking Backup of NSM On-Premises before Upgrade.

Upgrade Using Management Console

When upgrading from NSM 2.3.3 to NSM 2.3.4, the Firmware Settings page provides you a tool tip that directs you to upgrade using the NSM Management Console. The settings and configuration data is preserved across upgrades.

- 1. Open the NSM Management Console in an NSM On-Premises Virtual Machine.
- 2. Right click the VM and click **Open Console**. Ensure that NSM on-premises virtual machine has access to internet.
- 3. Open Network Interfaces menu and make any changes to network configuration, if required.
- 4. Navigate to System Update.
- 5. Click Start Update and then click Yes to check for new available updates.

Menu	-Sustem Undate	
System Info	System Update	[Start Update]
Storage		
Network Interfaces		
Diagnostics		
NTP Server		
System Update		
Reboot I Shutdown		
About		
rogz		
	-Check for new sustem undate	7
	Ves	
	No	
	Confirm (Enter) Cance	1 (Esc)
Her a Name An and have strong		
ToP to much between us		
For the setion ordit an item		
Enter to action/east an item		

6. Press Ctrl+P to view or edit the update channel.

- Menu	-Susten Indate		
Sustem Info	Susten Undate	[Start Undate]	
Storage			
Network Interfaces			
Diagnostics			
NTP Server	11		
System Update			
Reboot I Shutdown			
About			
Logs			
	11		
	-Enter Update Channel (or		
	stable		
	Confirm (Enter)		
	I Contraction of the second		
	11		
Up / Down to select items			
TAB to move between views			
Enter to action/edit an item			
	and the second se		

IMPORTANT: Updates are provided over update channels. The default channel is **Stable**.

7. When the upgrade version is displayed, click **Enter** to begin the update. This downloads and installs the update. During this process, you can close the downloading window by tapping **Esc**.

Menu	Sustem Undate		
Susten Info	Susten Undate	[Start Undate]	
Storage			
Network Interfaces			
Diamostics			
NTP Server			
Sustem Undate			
Reboot 1 Shutdown			
About			
Logo			
Logs			
	sten Update		
1 1	ew version is available.		
	ore applying new firmware. it is a		
	Begin opdate (Enter)		
In / Down to colocit itoms			
TAP to move between winner			
Patra to not in tell			

IMPORTANT: The NSM On-Premises VM is operational during update process.

8. Restart your system when the update is complete. Rebooting your system re-initializes the NSM On-Premises services

r Menu	r Reboot I Shutdown
Sustem Info	Rehaat NSM Rehaat
Stonage	Chutdown NCH Chutdown
Storage	
Metwork Interfaces	BOOU MSH INTO SAIEMODE L LMADIE J
Diagnostics	
NTP Server	
Susten Indate	
Pahaat I Shutdaux	
Al mut	
HDOUT	
Logs	
	Reboot NSN?
	Yes Control of the second s
	No
	Confirm (Entro) Concel (Enc)
	CONTITA CENCERS CANCEL CESCS
Up / Down to select items	
TAB to move between views	
Enter to actionzedit an item	
and the and the care an item	

9. Log in and navigate to **SYSTEM > Settings > Firmware and Settings** to confirm that the firmware is updated.

					C* Import/Export Settings	🕹 Upload Firmware	🔆 Column Selection
=	FILE NAME	BUILD DATE	LOAD DATE	FILE SIZE	VERSION	ACTIONS	
1	Current Firmware Version 🗸 Current Firmware		2021-02-16 01:34:51	0 B	2.2.0-R4-8c09e2df	Ċ	

Upgrading SonicOS Firmware

To upgrade SonicOS firmware on a firewall:

- 1. Navigate to Manager View | Firewalls > Inventory page.
- 2. Hover a firewall, click **Ellipses** icon in the **ACTION** column, and then select **Upgrade Software**. The **Software Upgrade** dialog is displayed.

		1		
		UPGRADE S	TATUS	
VCTEM DI	ETAIL C			
TSTEM DE	ETAILS			
	Name Gen7_270W_fw		Current Version SonicOS 7.	0.1-5119
VAILABLE	E SOFTWARE VERSION(S)			
1 Please	e select a Firmware to Upload.			A Browse
	select a r in male to oproud.			• Sionse Opioad
#	VERSION	FILENAME	RELEASE DATE	RELEASE TYPE
1	local_firmware_Maintanance_sw_tz_2 5119-R4713.bin	7(Maintanance_sw_tz_270w_eng.7.0.1- 5119-R4713.bin.sig	Tue Jul 4 03:52:30 UTC 2023	Local Firmware
Total: 1 iter	m(s)			
Total: 1 Iter	m(s)			
Total: 1 Iter	m(s) D UPGRADE			

- 3. Do one of the following:
 - To upgrade to any available version on your Local system:
 - 1. In the **NEW SOFTWARE VERSION(S)** section, click **Browse** and select the setup file in your system.
 - 2. Click Upload.
 - To upgrade to any available version instantly:
 - 1. Select the required software version In AVAILABLE SOFTWARE VERSION(S).
 - 2. Select Now in SCHEDULED UPGRADE, if not selected.
 - 3. Click Upgrade.

- To schedule software upgrade:
 - 1. Select the required software version in **AVAILABLE SOFTWARE VERSION(S)**.
 - 2. Select Later in SCHEDULED UPGRADE and set the schedule for upgrade in Upgrade Time box.
 - 3. Click Upgrade.

12

SonicWall Support

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

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 and participate in the Community forum discussions at https://community.sonicwall.com/technology-and-support.
- View video tutorials
- Access https://mysonicwall.com
- 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

Network Security Manager On-Premises Getting Started Guide Updated - July 2023 232-005716-00 Rev F

Copyright © 2023 SonicWall Inc. All rights reserved.

The information in this document is provided in connection with SonicWall 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 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. 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/legal/end-user-product-agreements/.

Open Source Code

SonicWall Inc. 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 Attn: Jennifer Anderson 1033 McCarthy Blvd Milpitas, CA 95035