Network Security Manager (On-Premises)

Getting Started Guide

SONICWALL®

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 13
Obtaining the Image 15
Obtaining a New Licensed Image 15
Obtaining a Trial Version 19
Downloading NSM for an Existing Instance 20

Installing NSM on ESXi Server 22
Installing on ESXi Server 22
Connecting to the Console from ESXI 28

Installing NSM on Hyper-V 30
Preparing the Windows Server System 30
Installing NSM On-Premises on Hyper-V 30
Connecting to the Console from Hyper-V 35

Installing NSM on KVM 37
Deploying NSM on KVM via Virtual Machine Manager 37

Installing NSM on Azure 48

NSM Settings and Registration 55
Configuring NSM Network Settings 56
Registering NSM 57

Associating Firewalls on MSW 59
Unregistering NSM 60

Console Operations 61
Management Console Operations 61
NSM Management Console Menu 63
System Info 64
Network Interfaces 65
Diagnostics 65
NTP Server 67
System Update 68
Reboot/Shutdown 68
About 69
Logs 69
Using SafeMode on the Management Console 70
Enabling SafeMode 70
Disabling SafeMode 71
Configuring Network Interfaces in SafeMode 71
Installing a Software Upgrade in SafeMode 75
Downloading Logs in SafeMode 76

Using NSM 78
Interface Overview 78
Dashboard 79
Creating a Tenant 81
Creating a New User 82
Adding a Device 84

Integrate On-Prem Analytics with NSM 85
Integrate SonicWall Analytics in NSM 85
Enable Analytics While Adding a New Device 86
Enable Firewall to View Analytics Data 87
Accessing Analytics Data 88

Upgrade Instructions 90
Upgrade Using Management Console 90
Upgrading SonicOS Firmware 93

SonicWall Support 95
About This Document 96

1

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

ⓘ | **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 factor-authentication (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 Guide	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: • 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**.
🕒	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.
✓	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>`	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=<*your serial number*>, 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.

ⓘ | **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 • Create a user • Add a device	Using NSM

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.

ⓘ **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.

ⓘ **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 latest associated firmware that can be managed by Network Security Manager.

Generation	Firewall Model	Latest Supported SonicOS Version
Gen 6	**SOHO W**	6.5.4
	TZ Series: TZ300, TZ300W, TZ300P, TZ350, TZ350W, TZ400, TZ400W, TZ500, TZ500W, TZ600, TZ600P	6.5.4
	NSv Series: NSv 10, NSv 25, NSv 50, NSv 100, NSv 200, NSv 300, NSv 400, NSv 800, NSv 1600	6.5.4
	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
	NSsp Series: NSsp 12400, NSsp 12800	6.5.4
Gen 7	**TZ Series:** TZ80, TZ270, TZ270W, TZ370, TZ370W, TZ470, TZ470W, TZ570, TZ570W, TZ570P, TZ670	7.1.3
	NSv Series: NSv 270, NSv 470, NSv 870	7.1.3
	NSa Series: NSa 2700, NSa 3700	7.1.3
	NSsp Series: NSsp 15700	7.1.3

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 7.0	1-500	4 core, 24 GB RAM
	ESXi 8.0	500-3000	8 core, 48 GB RAM
Hyper-V	Windows 2019	1-500	4 core, 24 GB RAM
	Windows 2022	500-3000	8 core, 48 GB RAM

Platform	Version	Number of Firewalls	Minimum Configuration
KVM	Linux Kernel 2.6.17 or above 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.	1-500	4 core, 24 GB RAM
		500-3000	8 core, 48 GB RAM
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.
- **TZ80 Devices**
    - TZ80 devices is available only as a bundle. NSM On-prem and SaaS firewall management is bundled as a service in a firewall license bundles.

- NSM on-prem has to be registered with the NSM base license to manage TZ80 devices using firewall management service license bundled with firewall license bundles.
- TZ80 devices will function only with a valid license.

  ⓘ | **NOTE:** TZ80 hardware will not function after a 30 days trail period without a valid license.
- TZ80 devices have to be bundled with **Secure Connect** license or **Advanced Protection Service Suite (APSS)** license.

Firewall License Bundle	NSM SaaS
Secure Connect	Allows 24x7 device management support.
Advanced Protection Service Suite (APSS)	Allows device management along with • SaaS Advanced Reporting & Analytics (7 days) • DNS Filtering • Gateway Anti-malware/Intrusion Prevention/App Control • Content Filtering Service • Comprehensive Anti-Spam Service • Capture Advanced Threat Protection • 24x7 Support

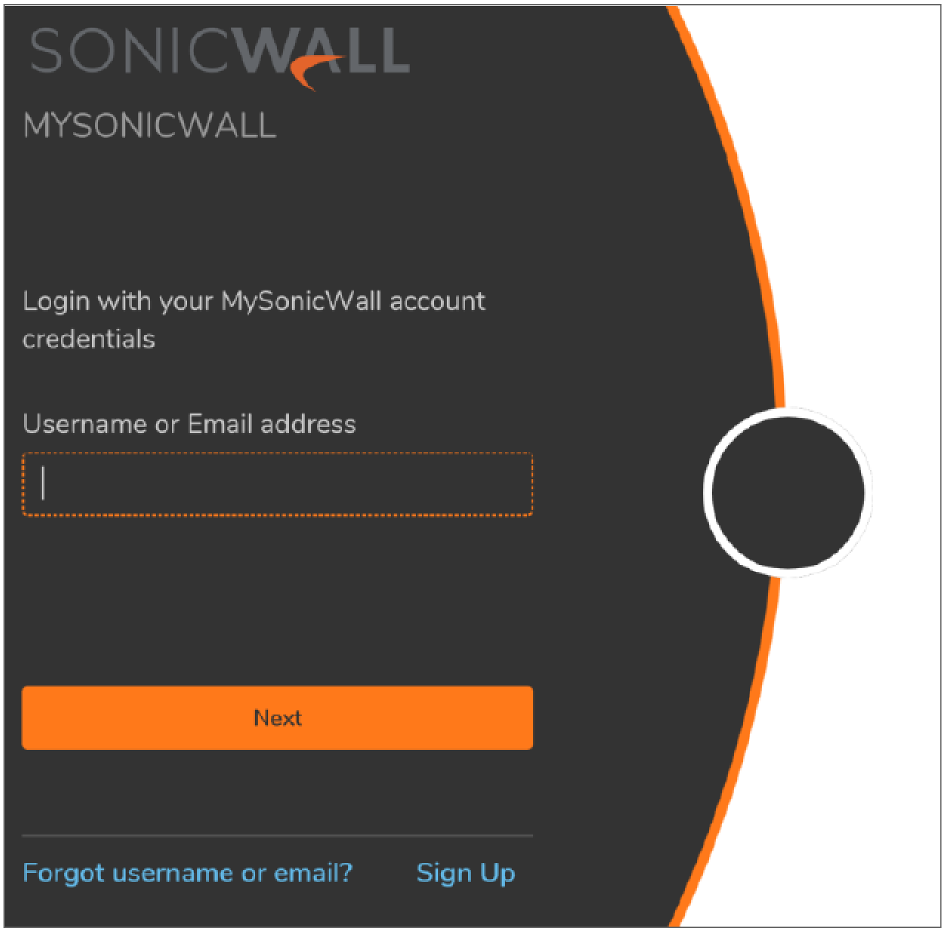
Creating an MSW Account

A MySonicWall account is required to register the NSM instance.

ⓘ | **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.



Login with your MySonicWall account credentials

Username or Email address

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.

ⓘ | **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

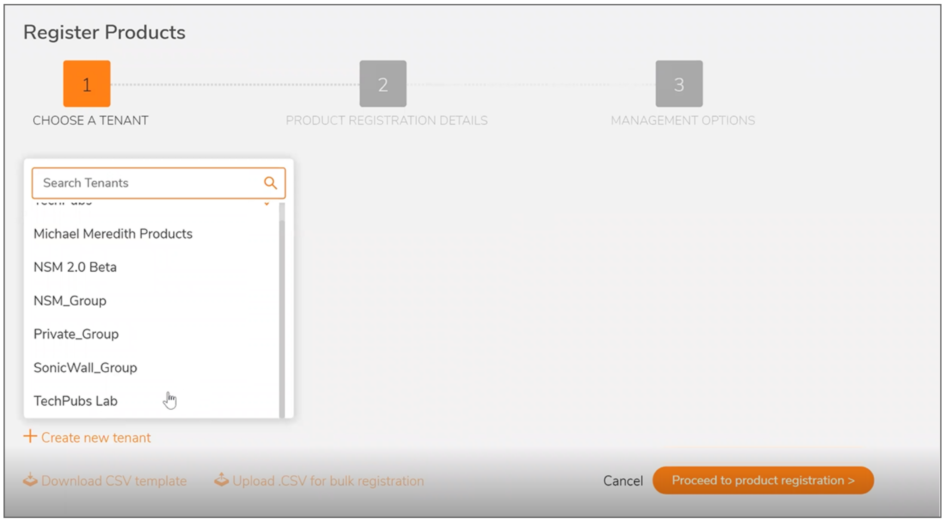
To download NSM for the first time, you need an Activation Key to access the image.

1. Log in to MySonicWall.

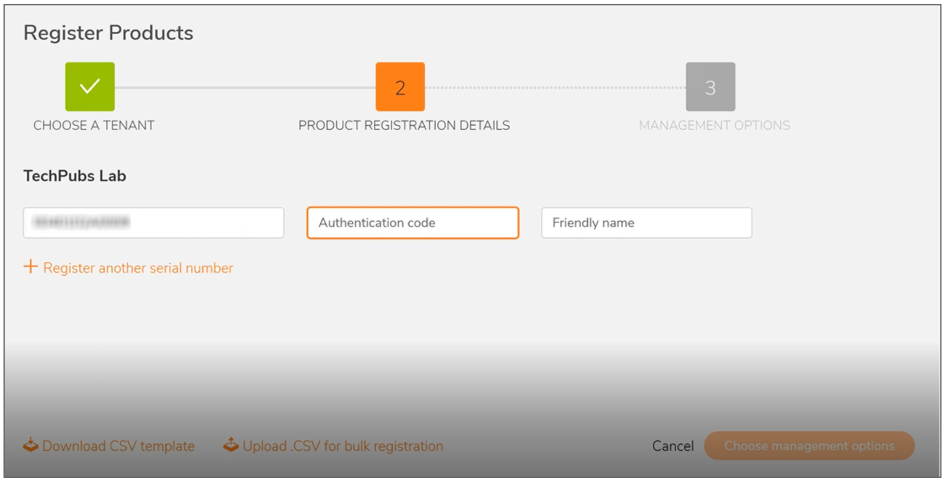
   ⓘ | **NOTE:** If you do not have a MySonicWall account, refer to Creating an MSW Account.

2. Navigate to **Product Management > My Products**.

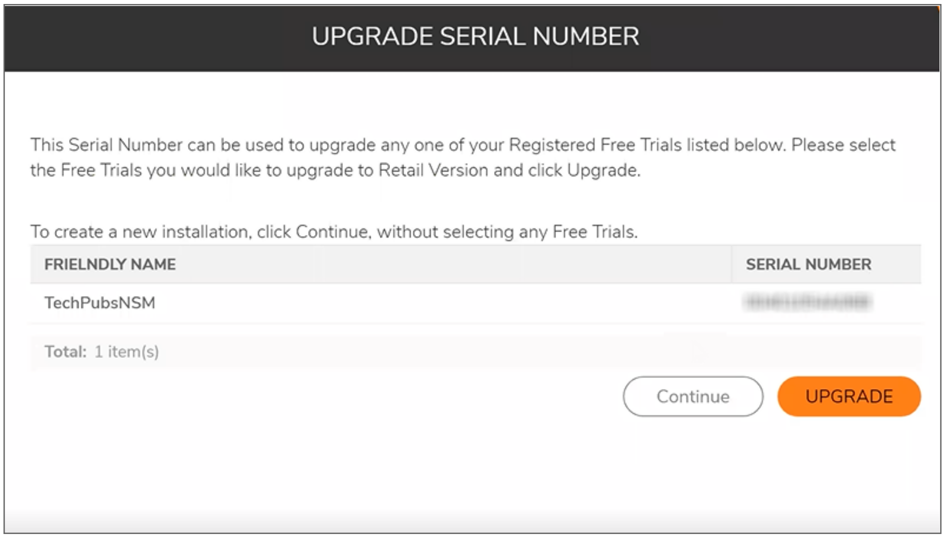
3. Click **Register Products**.



4. Choose a **Tenant**.



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



UPGRADE SERIAL NUMBER

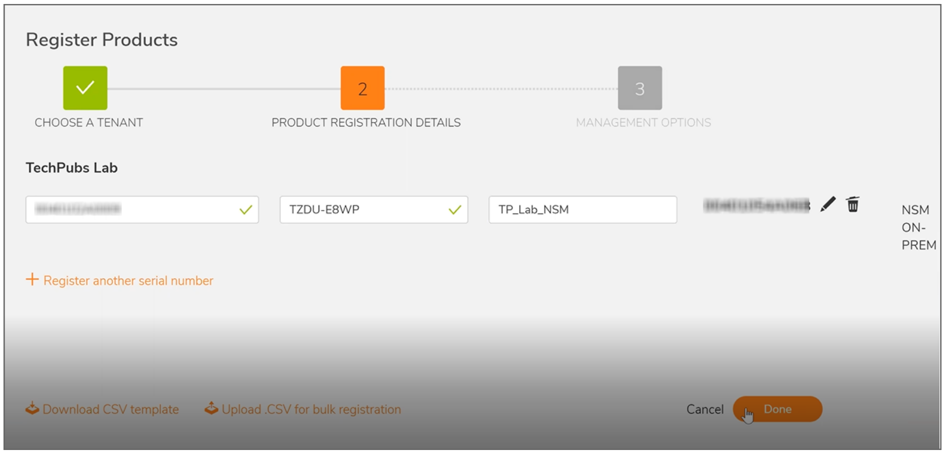
This Serial Number can be used to upgrade any one of your Registered Free Trials listed below. Please select the Free Trials you would like to upgrade to Retail Version and click Upgrade.

To create a new installation, click Continue, without selecting any Free Trials.

FRIELNDLY NAME	SERIAL NUMBER
TechPubsNSM	[redacted]

Total: 1 item(s)

7. Click **Upgrade**.



Register Products

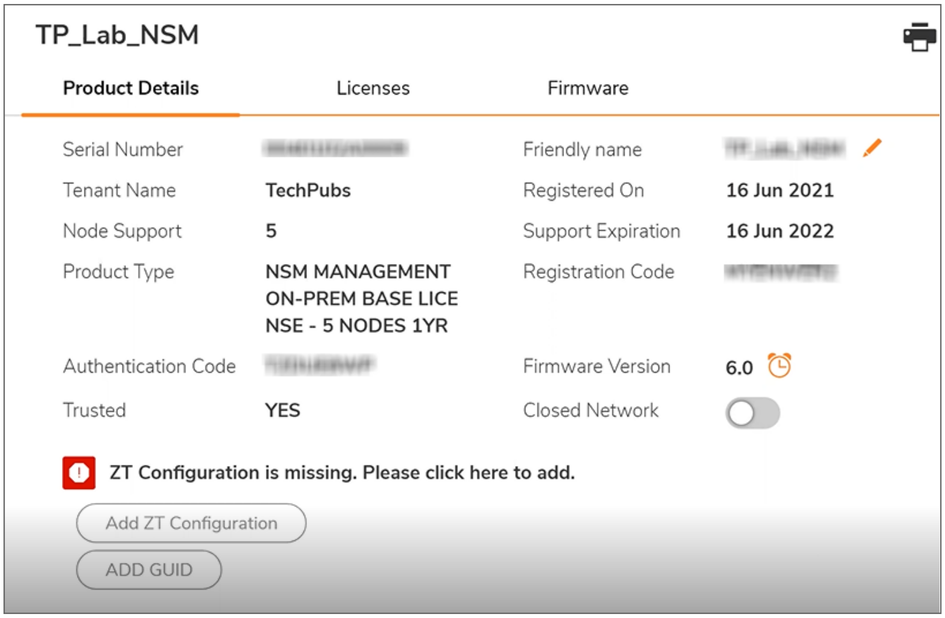
✓
CHOOSE A TENANT
2
PRODUCT REGISTRATION DETAILS
3
MANAGEMENT OPTIONS

TechPubs Lab

[redacted] ✓	TZDU-E8WP ✓	TP_Lab_NSM	[redacted]	NSM ON-PREM

+ Register another serial number
Download CSV template
Upload .CSV for bulk registration
Cancel
Done

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



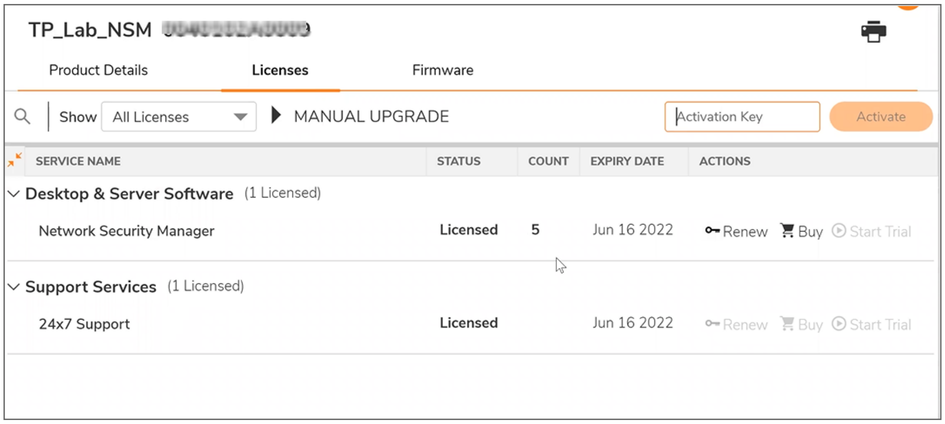
TP_Lab_NSM

Serial Number	[redacted]	Friendly name	[redacted]
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	[redacted]
Authentication Code	[redacted]	Firmware Version	6.0
Trusted	YES	Closed Network	

ZT Configuration is missing. Please click here to add.

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

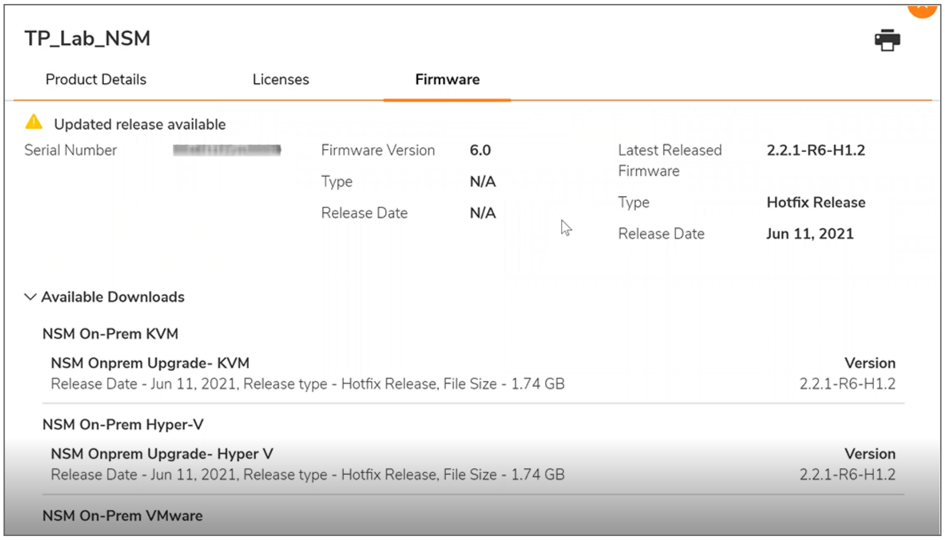
9. Select the **Licenses** tab to view the details of the license.



TP_Lab_NSM [redacted]

SERVICE NAME	STATUS	COUNT	EXPIRY DATE	ACTIONS
Desktop & Server Software (1 Licensed)				
Network Security Manager	Licensed	5	Jun 16 2022	Renew Buy Start Trial
Support Services (1 Licensed)				
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.



TP_Lab_NSM

⚠ Updated release available

Serial Number	[redacted]	Firmware Version	6.0	Latest Released Firmware	2.2.1-R6-H1.2
		Type	N/A	Type	Hotfix Release
		Release Date	N/A	Release Date	Jun 11, 2021

Available Downloads

NSM On-Prem KVM

NSM Onprem Upgrade- KVM — Version 2.2.1-R6-H1.2
Release Date - Jun 11, 2021, Release type - Hotfix Release, File Size - 1.74 GB

NSM On-Prem Hyper-V

NSM Onprem Upgrade- Hyper V — Version 2.2.1-R6-H1.2
Release Date - Jun 11, 2021, Release type - Hotfix Release, File Size - 1.74 GB

NSM On-Prem VMware

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

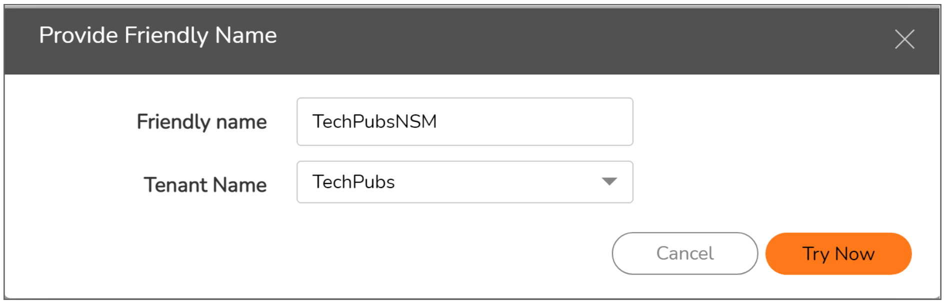
Obtaining a Trial Version

To obtain a trial version:

1. Log in to MySonicWall.

   ⓘ | **NOTE:** 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

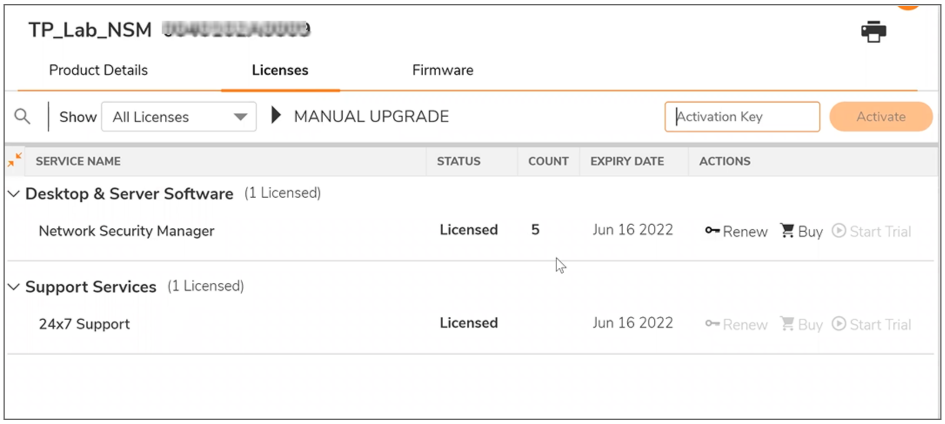
Friendly name	TechPubsNSM
Tenant Name	TechPubs

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:

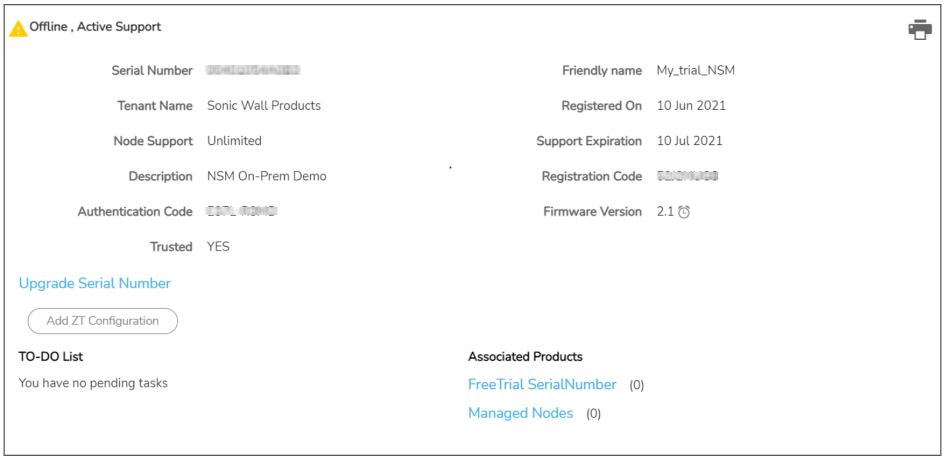
1. After logging into your MySonicWall account, navigate to **Product Management > My Products**.
2. Find the **Friendly Name** of the NSM instance in your product list, and click on **Activate Service** (the **Key** icon on the right side of the table).
3. Type the **Activation Key** in the appropriate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



TP_Lab_NSM [redacted]

SERVICE NAME	STATUS	COUNT	EXPIRY DATE	ACTIONS
Desktop & Server Software (1 Licensed)				
Network Security Manager	Licensed	5	Jun 16 2022	Renew Buy Start Trial
Support Services (1 Licensed)				
24x7 Support	Licensed		Jun 16 2022	Renew Buy Start Trial

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



Offline , Active Support

Serial Number	[redacted]	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	[redacted]
Authentication Code	[redacted]	Firmware Version	2.1
Trusted	YES		

TO-DO List

You have no pending tasks

Associated Products

FreeTrial SerialNumber (0)

Managed Nodes (0)

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

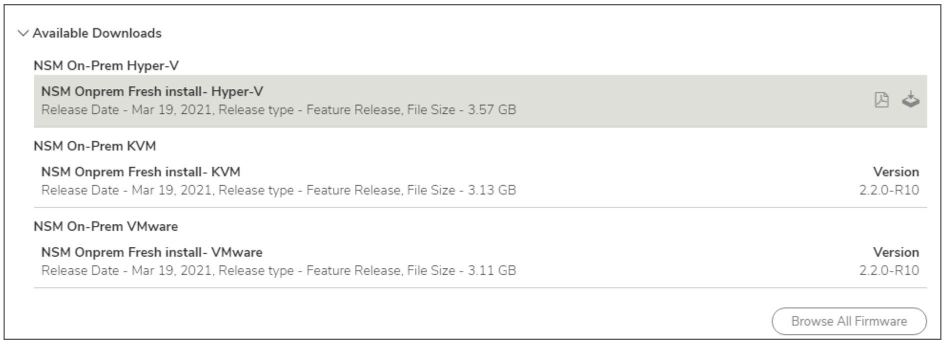
Downloading NSM for an Existing Instance

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

NSM On-Prem KVM

NSM Onprem Fresh install- KVM
Release Date - Mar 19, 2021, Release type - Feature Release, File Size - 3.13 GB
Version
2.2.0-R10

NSM On-Prem VMware

NSM Onprem Fresh install- VMware
Release Date - Mar 19, 2021, Release type - Feature Release, File Size - 3.11 GB
Version
2.2.0-R10

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.

3

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.

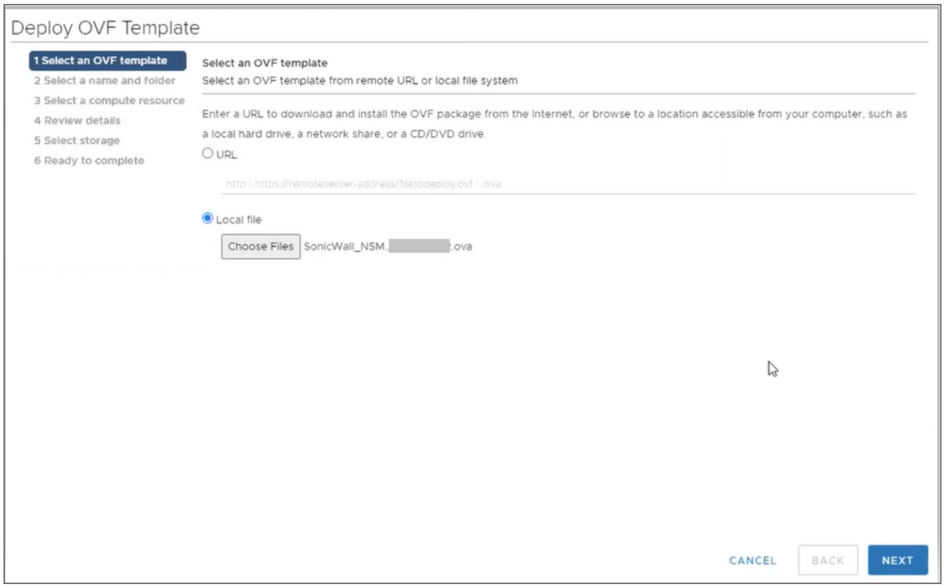
ⓘ | **NOTE:** The elements of VMware must already be in place and the administrator must be familiar with the basics of deploying a virtual appliance on the ESXi server.

To install NSM On-Premises on ESXi server:

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

   ⓘ | **NOTE:** Install NSM after setting up your virtual system.

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



Deploy OVF Template

1 Select an OVF template
2 Select a name and folder
3 Select a compute resource
4 Review details
5 Select storage
6 Ready to complete

Select an OVF template

Select an OVF template from remote URL or local file system

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

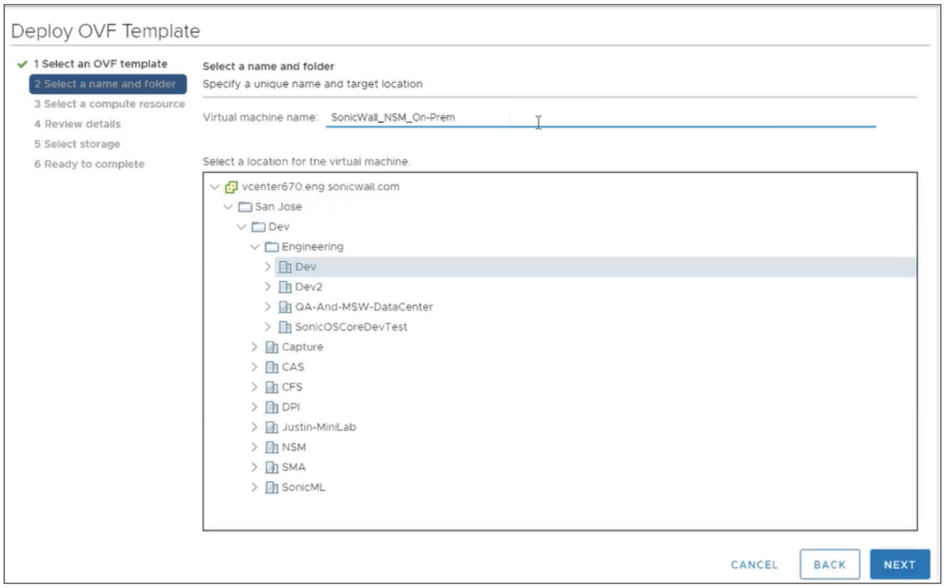
○ URL

http | https://remoteserver-address/filetodeploy.ovf | .ova

● Local file

Choose Files SonicWall_NSM.[redacted].ova

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 Template

✓ 1 Select an OVF template
2 Select a name and folder
3 Select a compute resource
4 Review details
5 Select storage
6 Ready to complete

Select a name and folder

Specify a unique name and target location

Virtual machine name: SonicWall_NSM_On-Prem

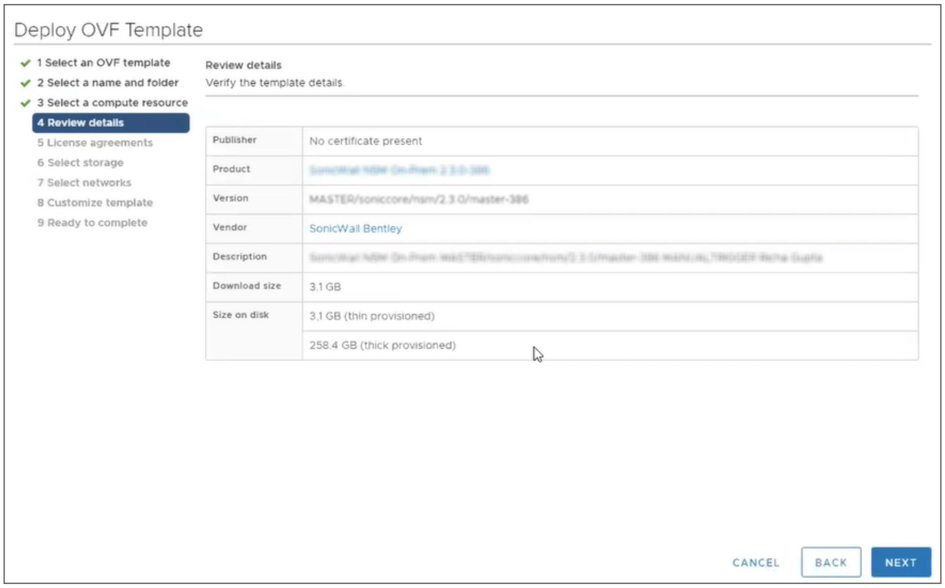
Select a location for the virtual machine.

- vcenter670.eng.sonicwall.com
  - San Jose
    - Dev
      - Engineering
        - Dev
        - Dev2
        - QA-And-MSW-DataCenter
        - SonicOSCoreDevTest
      - Capture
      - CAS
      - CFS
      - DPI
      - Justin-MiniLab
      - NSM
      - SMA
      - SonicML

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.**



Deploy OVF Template

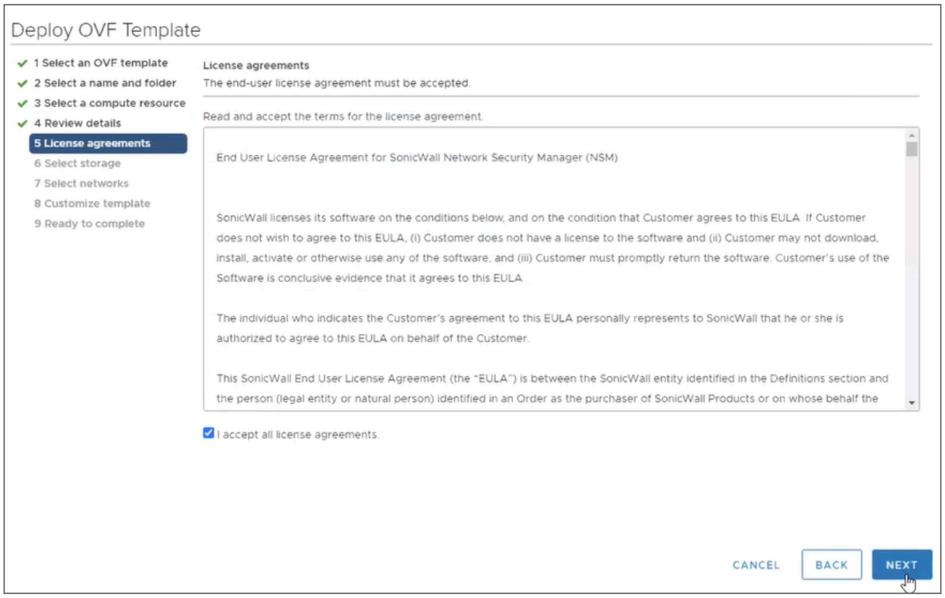
Review details

Verify the template details.

Publisher	No certificate present
Product	[redacted]
Version	MASTER/soniccore/nsm/2.3.0/master-386
Vendor	SonicWall Bentley
Description	[redacted]
Download size	3.1 GB
Size on disk	3.1 GB (thin provisioned)
	258.4 GB (thick provisioned)

ⓘ | **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**.



Deploy OVF Template

License agreements

The end-user license agreement must be accepted.

Read and accept the terms for the license agreement.

End User License Agreement for SonicWall Network Security Manager (NSM)

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.

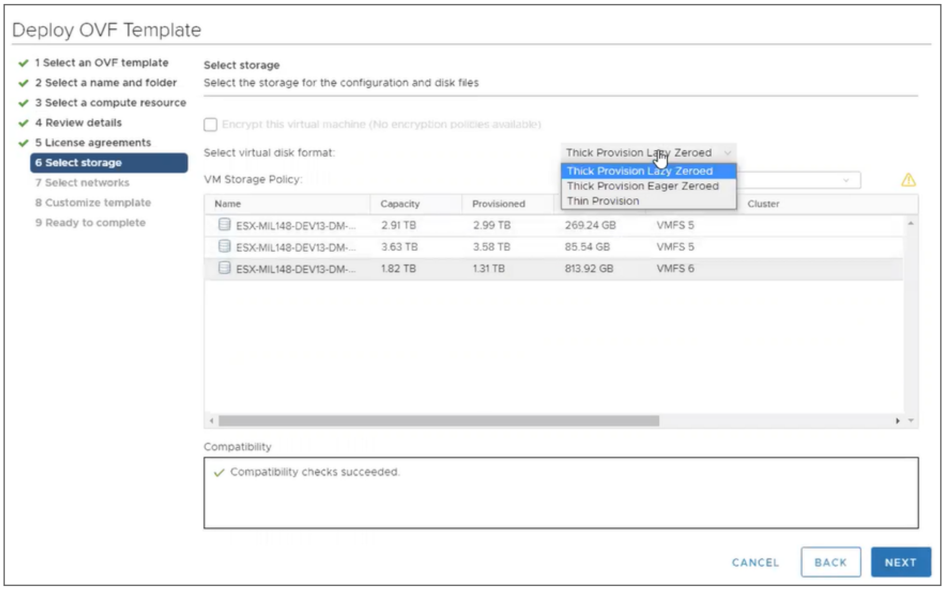
The individual who indicates the Customer's agreement to this EULA personally represents to SonicWall that he or she is authorized to agree to this EULA on behalf of the Customer.

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

☑ I accept all license agreements.

12. Click **Next**.

13. **Select virtual disk format** from the drop-down list. Make sure **Thick Provision** is selected to prevent over-provisioning of storage.



Deploy OVF Template

✓ 1 Select an OVF template
✓ 2 Select a name and folder
✓ 3 Select a compute resource
✓ 4 Review details
✓ 5 License agreements
6 Select storage
7 Select networks
8 Customize template
9 Ready to complete

Select storage
Select the storage for the configuration and disk files

□ Encrypt this virtual machine (No encryption policies available)

Select virtual disk format: Thick Provision Lazy Zeroed
- Thick Provision Lazy Zeroed
- Thick Provision Eager Zeroed
- Thin Provision

VM Storage Policy:

Name	Capacity	Provisioned			Cluster
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	

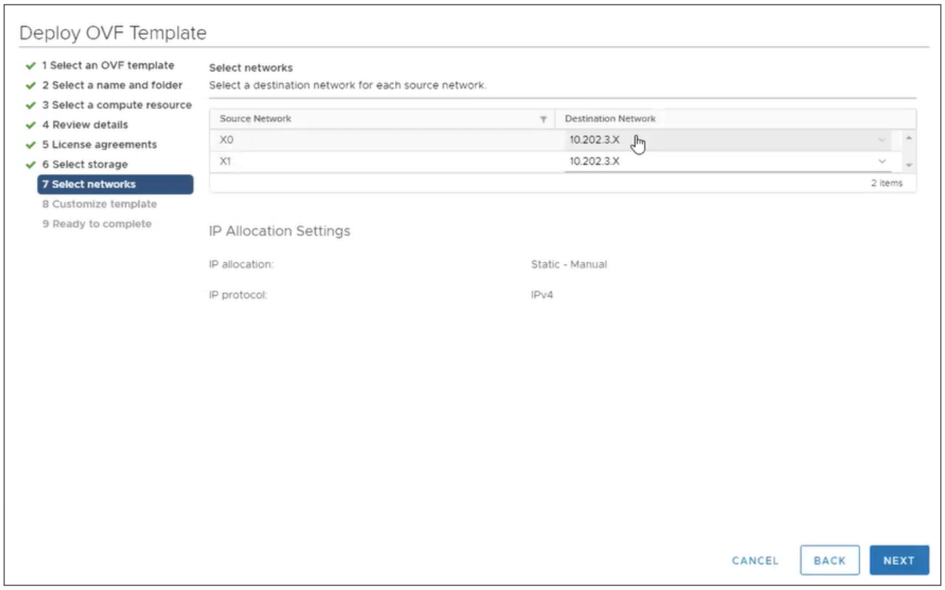
Compatibility
✓ Compatibility checks succeeded.

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

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

15. In the **Select networks** screen, set up interface**X0** 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.



Deploy OVF Template

✓ 1 Select an OVF template
✓ 2 Select a name and folder
✓ 3 Select a compute resource
✓ 4 Review details
✓ 5 License agreements
✓ 6 Select storage
7 Select networks
8 Customize template
9 Ready to complete

Select networks
Select a destination network for each source network.

Source Network	Destination Network
X0	10.202.3.X
X1	10.202.3.X

2 items

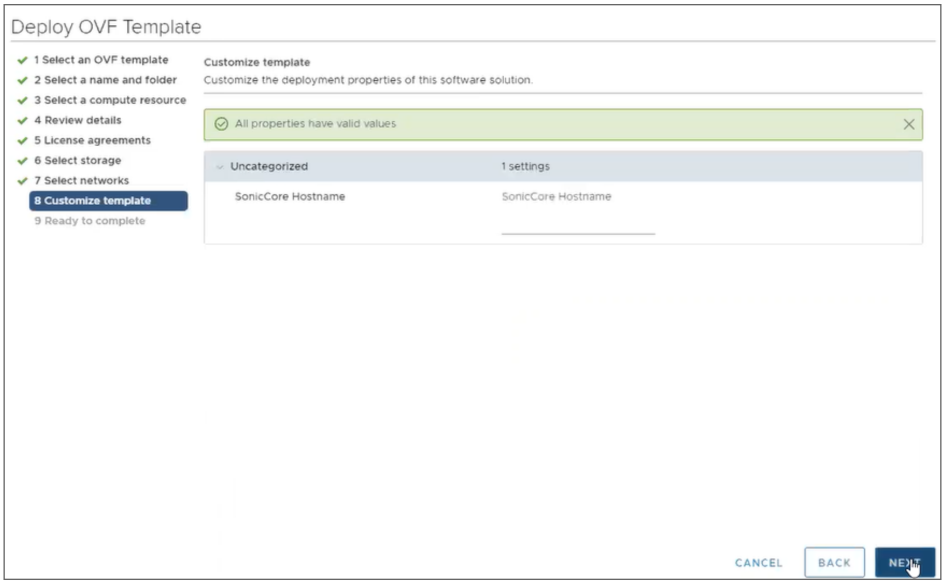
IP Allocation Settings

IP allocation: Static - Manual

IP protocol: IPv4

ⓘ | **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**.



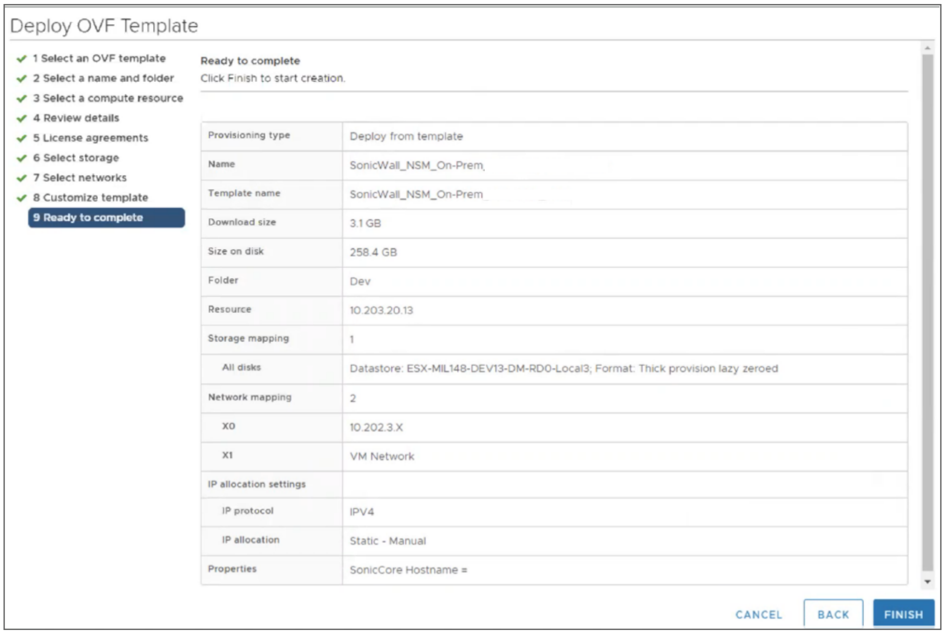
Customize template

Customize the deployment properties of this software solution.

All properties have valid values

Uncategorized	1 settings
SonicCore Hostname	SonicCore Hostname

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



Ready to complete

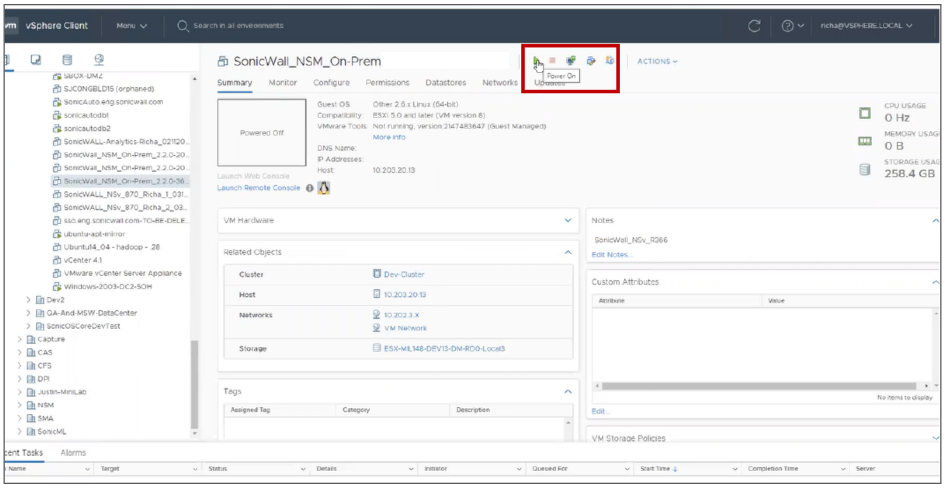
Click Finish to start creation.

Provisioning type	Deploy from template
Name	SonicWall_NSM_On-Prem
Template name	SonicWall_NSM_On-Prem
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-RD0-Local3; Format: Thick provision lazy zeroed
Network mapping	2
X0	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.



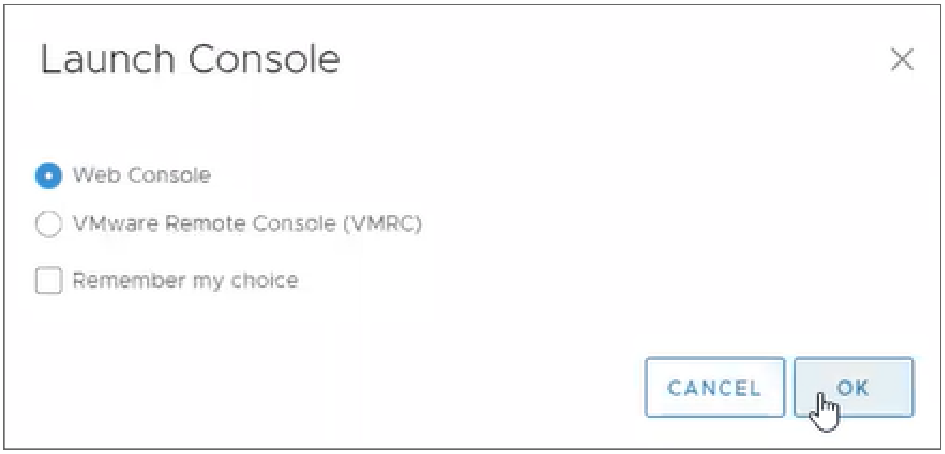
Guest OS: Other 2.6.x Linux (64-bit)
Compatibility: ESXi 5.0 and later (VM version 8)
VMware Tools: Not running, version:2147483647 (Guest Managed)
More info
DNS Name:
IP Addresses:
Host: 10.203.20.13

CPU USAGE 0 Hz
MEMORY USAGE 0 B
STORAGE USAGE 258.4 GB

Notes: SonicWall_NSv_R366

Cluster	Dev-Cluster
Host	10.203.20.13
Networks	10.202.3.x VM Network
Storage	ESX-ML148-DEV13-DM-RD0-Local3

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



Launch Console

● Web Console

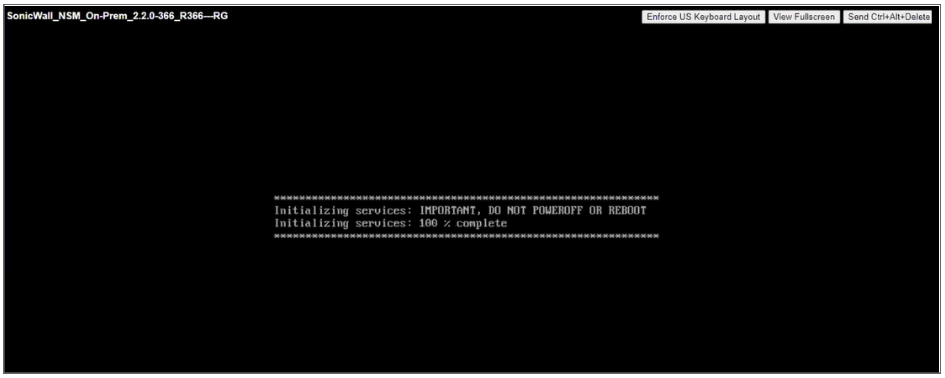
○ VMware Remote Console (VMRC)

□ Remember my choice

CANCEL OK

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

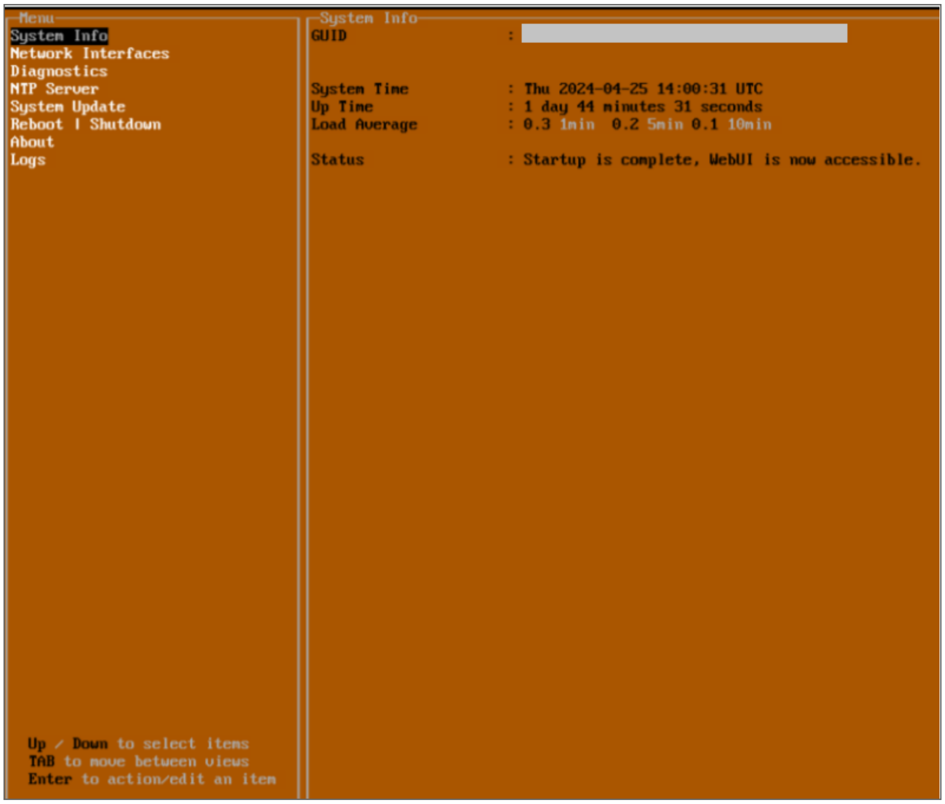
The system console shows a boot message. Depending on the resources available to your system, this initial boot up may take 10 to 15 minutes; you can monitor the % complete in the console to track progress.



SonicWall_NSM_On-Prem_2.2.0-366_R366---RG
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete

```
****************************************************************
Initializing services: IMPORTANT, DO NOT POWEROFF OR REBOOT
Initializing services: 100 % complete
****************************************************************
```

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

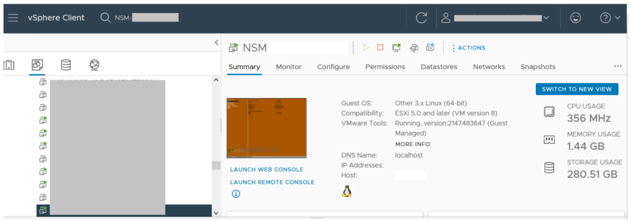


```
GUID                 : [redacted]


System Time          : Thu 2024-04-25 14:00:31 UTC
Up Time              : 1 day 44 minutes 31 seconds
Load Average         : 0.3 1min  0.2 5min 0.1 10min

Status               : Startup is complete, WebUI is now accessible.
```

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**.



Guest OS: Other 3.x Linux (64-bit)
Compatibility: ESXi 5.0 and later (VM version 8)
VMware Tools: Running, version:2147483647 (Guest Managed)
DNS Name: localhost
IP Addresses:
Host:

CPU USAGE 356 MHz
MEMORY USAGE 1.44 GB
STORAGE USAGE 280.51 GB

[redacted]

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

4

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

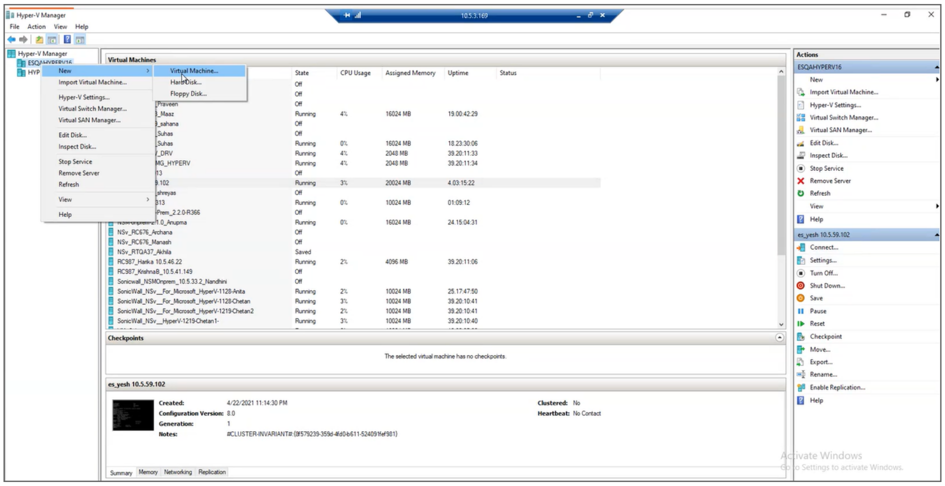
Before installing an NSM On-Premises instance on Hyper-V, prepare the Windows Server system:

- Install Windows Server 2019 or 2022.
- Install the Hyper-V Role in the Windows Server system. Refer to the Microsoft documentation at Install-the-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**.



Virtual Machines

	State	CPU Usage	Assigned Memory	Uptime	Status
	Off				
	Off				
_Praveen	Off				
3_Maaz	Running	4%	16024 MB	19.00:42:29	
9_sahana	Off				
_Suhas	Off				
_Suhas	Running	0%	16024 MB	18.23:30:06	
/_DRV	Running	4%	2048 MB	39.20:11:33	
MG_HYPERV	Running	4%	2048 MB	39.20:11:34	
13	Off				
9.102	Running	3%	20024 MB	4.03:15:22	
_shreyas	Off				
313	Running	0%	10024 MB	01:09:12	
-Prem_2.2.0-R366	Off				
1.0_Anupma	Running	0%	16024 MB	24.15:04:31	
NSv_RC676_Archana	Off				
NSv_RC676_Manash	Off				
NSv_RTQA37_Akhila	Saved				
RC987_Harika 10.5.46.22	Running	2%	4096 MB	39.20:11:06	
RC987_KrishnaB_10.5.41.149	Off				
Sonicwall_NSMOnprem_10.5.33.2_Nandhini	Off				
SonicWall_NSv__For_Microsoft_HyperV-1128-Anita	Running	2%	10024 MB	25.17:47:50	
SonicWall_NSv__For_Microsoft_HyperV-1128-Chetan	Running	3%	10024 MB	39.20:10:41	
SonicWall_NSv__For_Microsoft_HyperV-1219-Chetan2	Running	2%	10024 MB	39.20:10:41	
SonicWall_NSv__HyperV-1219-Chetan1-	Running	3%	10024 MB	39.20:10:40	

Checkpoints

The selected virtual machine has no checkpoints.

es_yesh 10.5.59.102

Created: 4/22/2021 11:14:30 PM

Configuration Version: 8.0

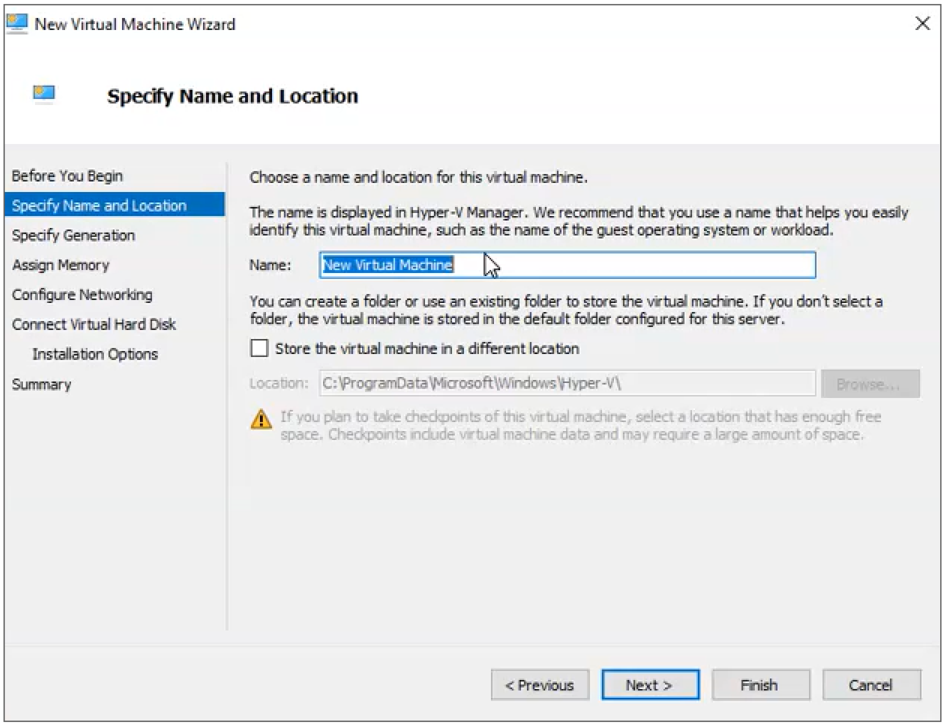
Generation: 1

Notes: #CLUSTER-INVARIANT#:{8f579239-359d-4fd0-b611-524091fef981}

Clustered: No

Heartbeat: No Contact

The **New Virtual Machine Wizard** window is displayed.



Specify Name and Location

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 helps you easily identify this virtual machine, such as the name of the guest operating system or workload.

Name: New Virtual Machine

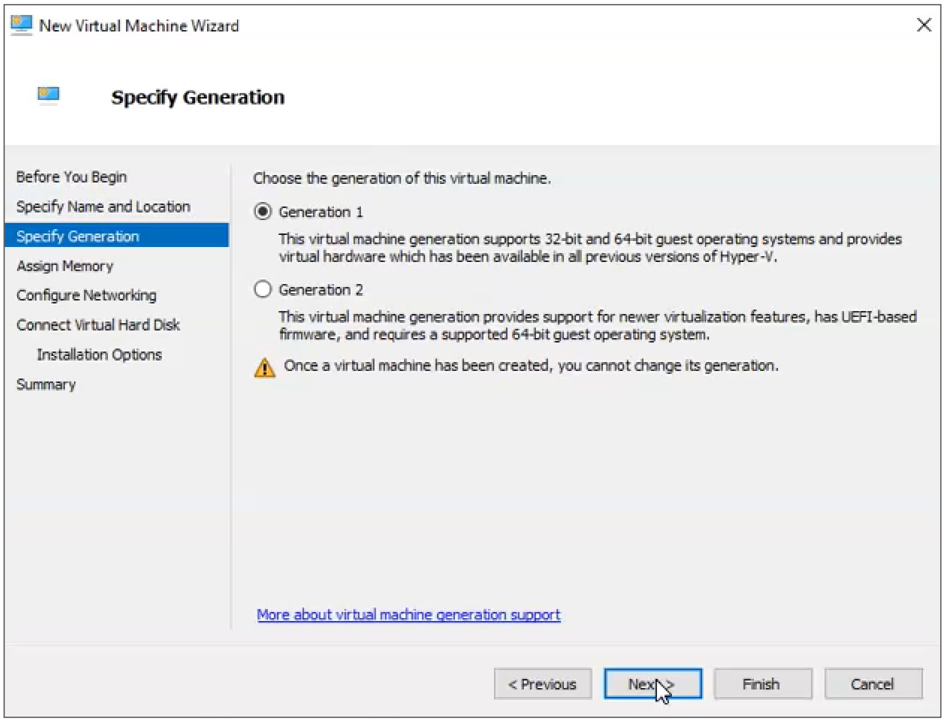
You can create a folder or use an existing folder to store the virtual machine. If you don't select a folder, the virtual machine is stored in the default folder configured for this server.

☐ Store the virtual machine in a different location

Location: C:\ProgramData\Microsoft\Windows\Hyper-V\

If you plan to take checkpoints of this virtual machine, select a location that has enough free space. Checkpoints include virtual machine data and may require a large amount of space.

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



New Virtual Machine Wizard

Specify Generation

Choose the generation of this virtual machine.

● Generation 1

This virtual machine generation supports 32-bit and 64-bit guest operating systems and provides virtual hardware which has been available in all previous versions of Hyper-V.

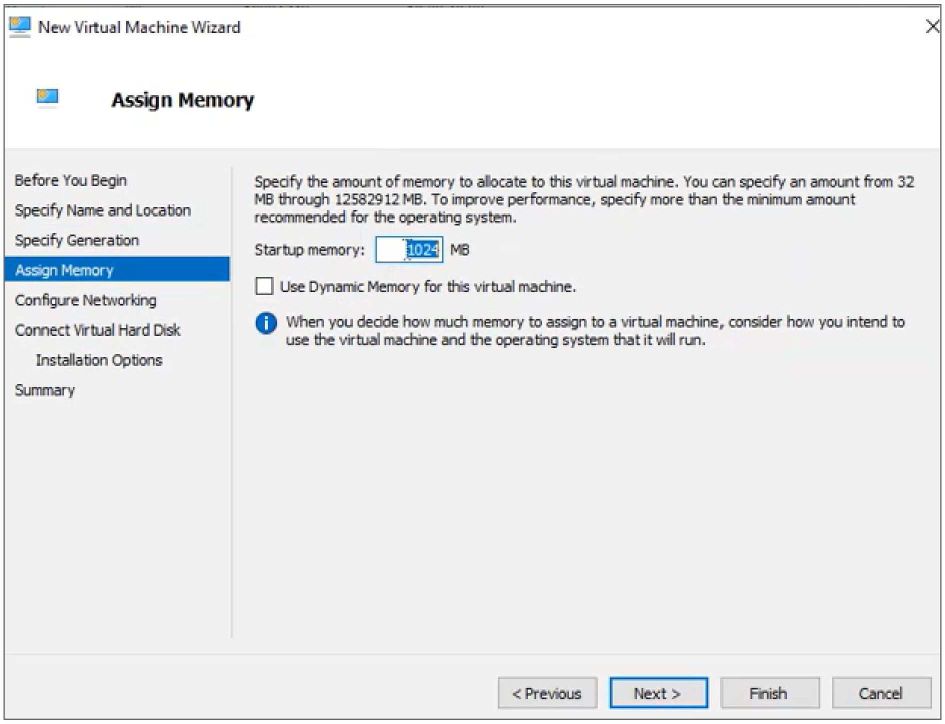
○ Generation 2

This virtual machine generation provides support for newer virtualization features, has UEFI-based firmware, and requires a supported 64-bit guest operating system.

⚠ Once a virtual machine has been created, you cannot change its generation.

More about virtual machine generation support

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



New Virtual Machine Wizard

Assign Memory

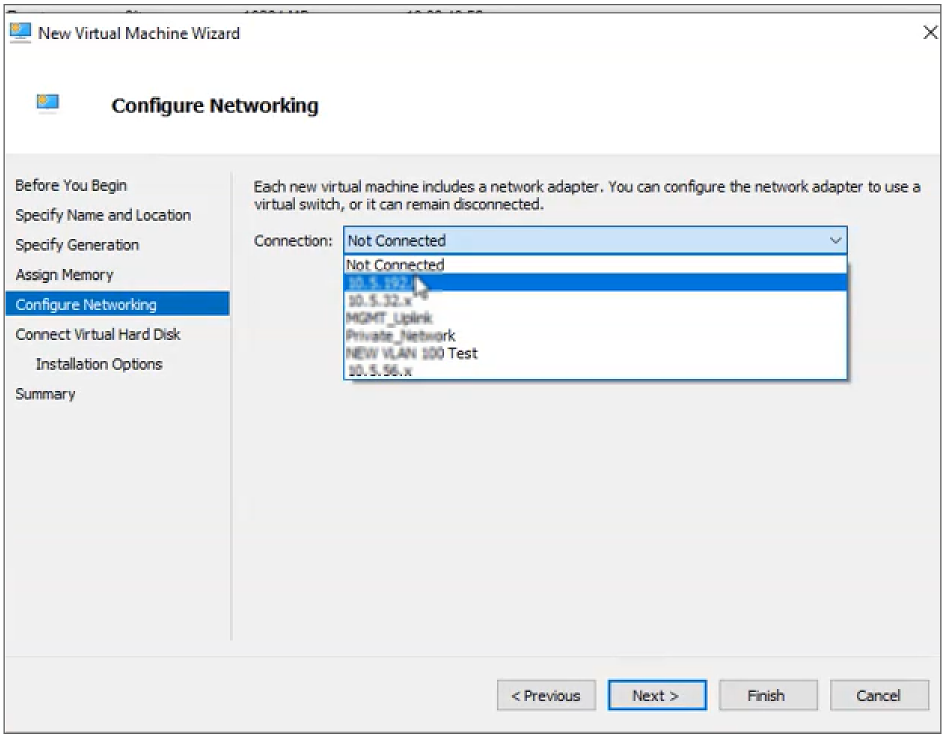
Specify the amount of memory to allocate to this virtual machine. You can specify an amount from 32 MB through 12582912 MB. To improve performance, specify more than the minimum amount recommended for the operating system.

Startup memory: 1024 MB

□ Use Dynamic Memory for this virtual machine.

ⓘ 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.

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



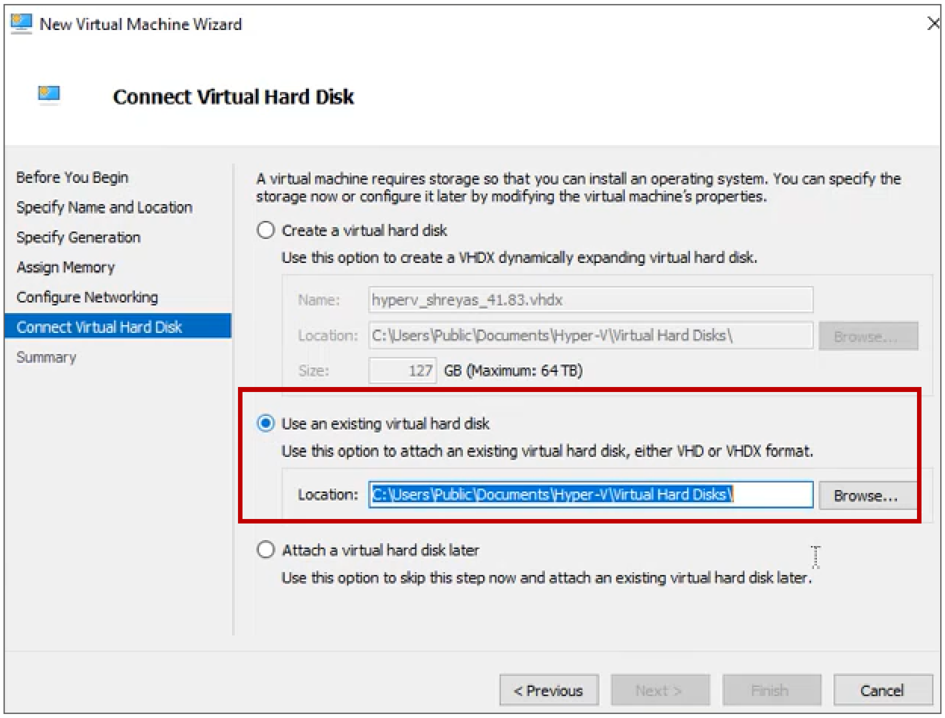
New Virtual Machine Wizard

Configure Networking

Each new virtual machine includes a network adapter. You can configure the network adapter to use a virtual switch, or it can remain disconnected.

Connection: Not Connected

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



New Virtual Machine Wizard

Connect Virtual Hard Disk

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.

Name: hyperv_shreyas_41.83.vhdx

Location: C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks\

Size: 127 GB (Maximum: 64 TB)

● Use an existing virtual hard disk

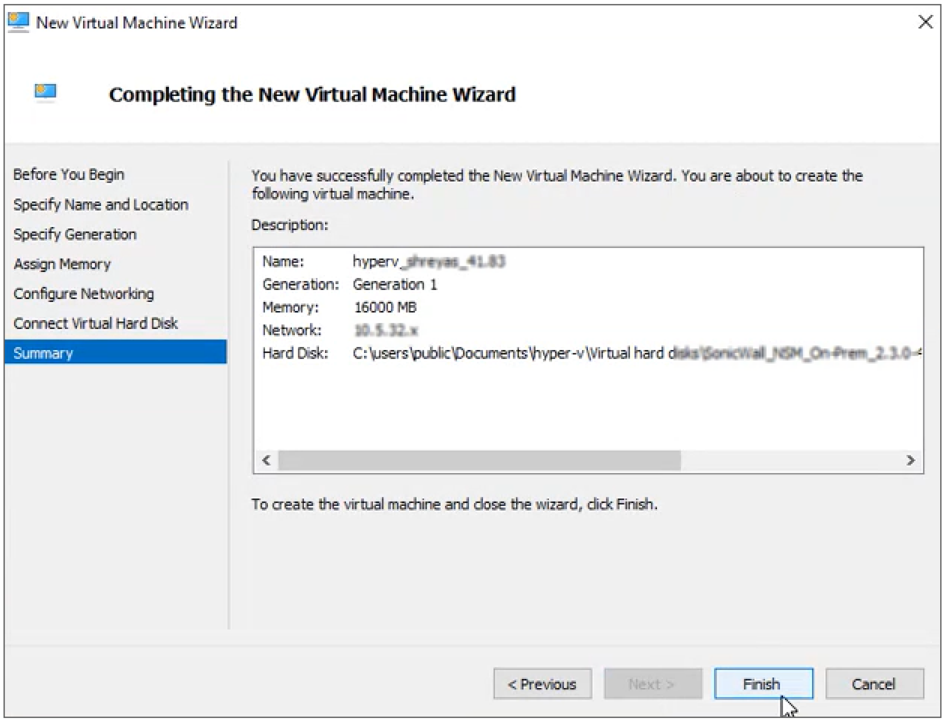
Use this option to attach an existing virtual hard disk, either VHD or VHDX format.

Location: C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks\

○ Attach a virtual hard disk later

Use this option to skip this step now and attach an existing virtual hard disk later.

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 Wizard
Completing the New Virtual Machine Wizard
Before You Begin
Specify Name and Location
Specify Generation
Assign Memory
Configure Networking
Connect Virtual Hard Disk
Summary
< Previous
Next >
Finish
Cancel

You have successfully completed the New Virtual Machine Wizard. You are about to create the following virtual machine.

Description:

Name: hyperv_[redacted]
Generation: Generation 1
Memory: 16000 MB
Network: [redacted]
Hard Disk: C:\users\public\Documents\hyper-v\Virtual hard [redacted]

To create the virtual machine and close the wizard, click Finish.

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

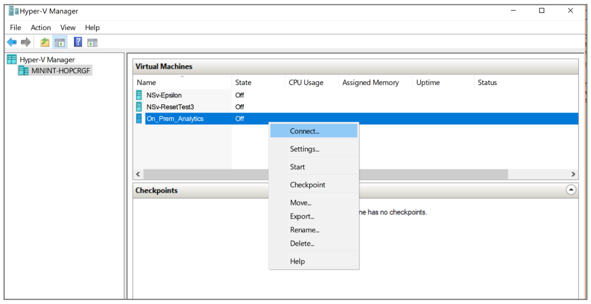
You can easily use the NSM Management Console to view and configure various parameters for NSM. It can also be used for diagnostics. When using Hyper-V you can connect to the NSM Management Console in the following way:

- Using the Hyper-V remote console to access the NSM On-Premises command line interface

  ⓘ **NOTE:** In the following procedure, the public IP address is the WAN IP address appearing in **Hyper-V Virtual Machine Connection**.

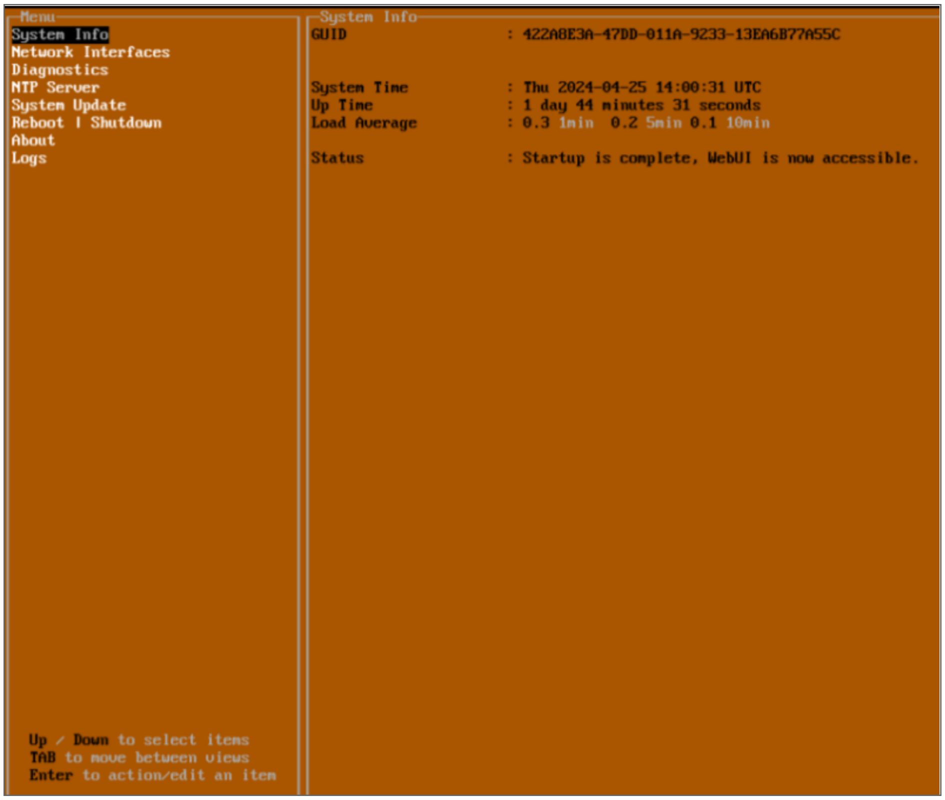
To connect to the management console through the Hyper-V Manager::

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



Name	State	CPU Usage	Assigned Memory	Uptime	Status
NSv-Epsilon	Off				
NSv-ResetTest3	Off				
On_Prem_Analytics	Off				

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



```
Menu                            System Info
System Info                     GUID                  : 422A8E3A-47DD-011A-9233-13EA6B77A55C
Network Interfaces
Diagnostics
NTP Server                      System Time           : Thu 2024-04-25 14:00:31 UTC
System Update                   Up Time               : 1 day 44 minutes 31 seconds
Reboot | Shutdown               Load Average          : 0.3 1min  0.2 5min 0.1 10min
About
Logs                            Status                : Startup is complete, WebUI is now accessible.




  Up / Down to select items
  TAB to move between views
  Enter to action/edit an item
```

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

5

Installing NSM on KVM

Topics:

- Deploying NSM on KVM via Virtual Machine Manager

Deploying NSM on KVM via Virtual Machine Manager

This section describes how to create a virtual machine via Virtual Machine Manager. This application can be opened by either running the virt manager command, $ virt-manager, or by opening it through your system.

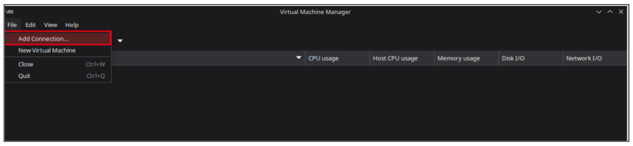
virt-manager uses **libvirt** virtualization API, which provides a common interface for managing virtual machines for KVM. It can manage both local and remote virtual machines, allowing users to administer VMs hosted on different physical servers. This guide assumes the VM is being set up on a local server. The process for setting up on remote server is identical to that of setting it up on a local server, the only difference being the QEMU/KVM connection is managing the remote server instead of the local server. If there is a remote connection ready to use, switch to it before proceeding with the guide.

ⓘ | **NOTE:** Nested Virtualization is not supported for NSM on-Prem.

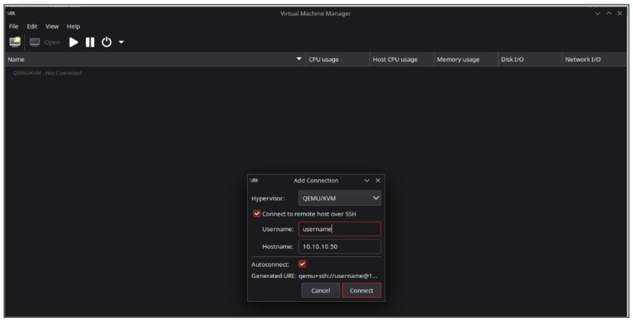
ⓘ | **NOTE:** Deploying the OVA image of SonicWALL NSM on Prem in a KVM environment using image conversion is not supported.

To add a new connection to the remote server:

1. To open the virtual machine manager, navigate to **File** and select **Add Connection**.



2. In the **Add Connection** window, select **QEMU/KVM** and enter the **Username** and **Hostname**. Check the boxes for **Connect to remote host over SSH** and **Autoconnect**.



Hypervisor: QEMU/KVM

☑ Connect to remote host over SSH

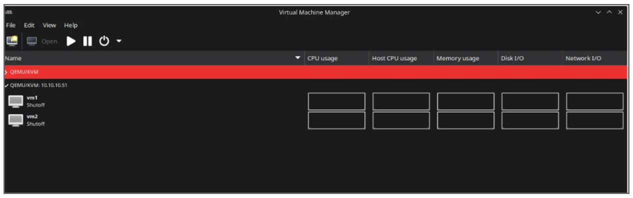
Username: username

Hostname: 10.10.10.50

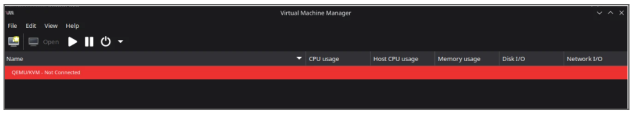
Autoconnect: ☑

Generated URI: qemu+ssh://username@1...

3. Once the connection is established, you should be able to see the virtual machines running (if any) on the remote machine in the virt-manager interface.



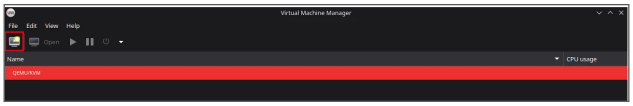
virt-manager shows a “QEMU/KVM - Not Connected” banner if it does not find any QEMU/KVM connection.



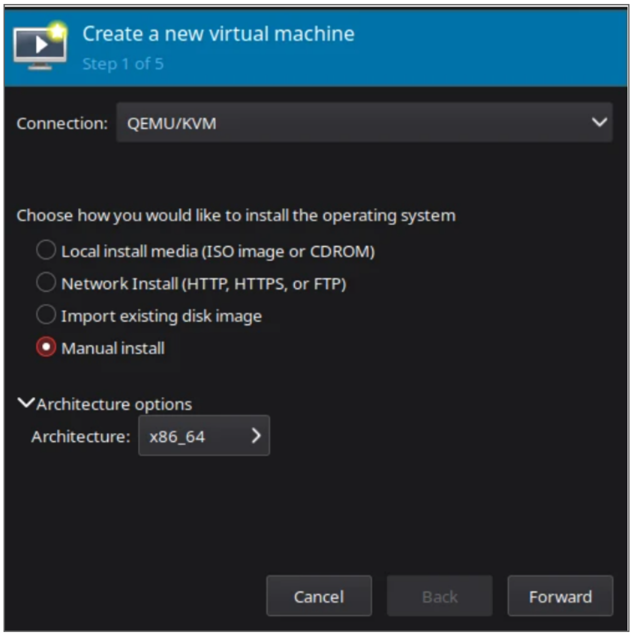
ⓘ | **NOTE:** Ensure the QEMU/KVM connection (local or remote) is working before proceeding.

To create a new NSM On-Premises VM:

1. Click on the create new virtual machine icon.



2. Select **QEMU/KVM** as **Connection** from the drop-down, select **Manual Install** radio button, and **x86_64** as the **Architecture**.



Create a new virtual machine

Step 1 of 5

Connection: QEMU/KVM

Choose how you would like to install the operating system

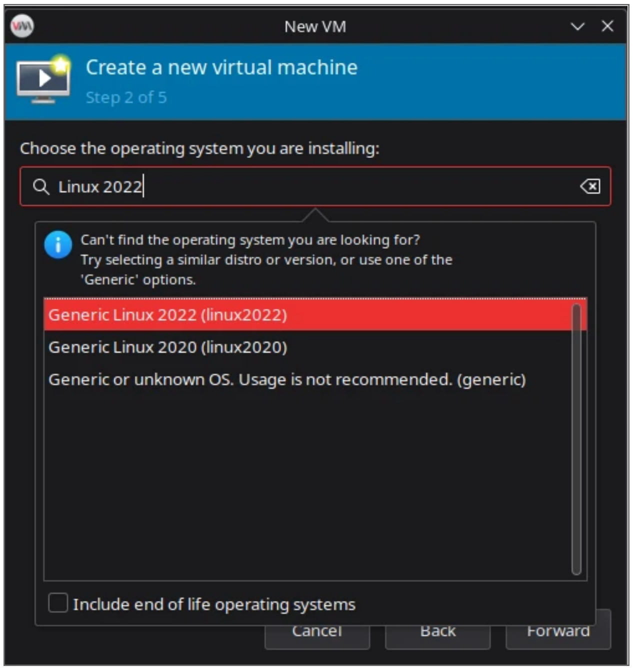
- ○ Local install media (ISO image or CDROM)
- ○ Network Install (HTTP, HTTPS, or FTP)
- ○ Import existing disk image
- ● Manual install

Architecture options

Architecture: x86_64

3. Select OS type as **Generic Linux 2022**.

   ⓘ | **NOTE:** If **Generic Linux 2022** is not available, you can use **Generic Linux 2020** or **Generic Linux**, but they are known to cause performance degradations.



Create a new virtual machine

Step 2 of 5

Choose the operating system you are installing:

Linux 2022

Can't find the operating system you are looking for? Try selecting a similar distro or version, or use one of the 'Generic' options.

Generic Linux 2022 (linux2022)

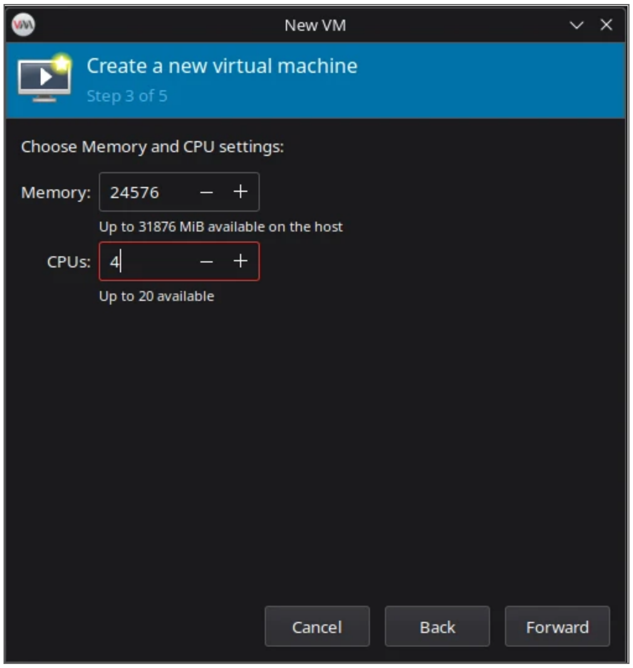
Generic Linux 2020 (linux2020)

Generic or unknown OS. Usage is not recommended. (generic)

□ Include end of life operating systems

4. Set Memory and CPU.

   ⓘ | **NOTE:** Memory of 24576 or 24 GiB, and 4 CPU cores are minimum recommended configurations.


New VM

Create a new virtual machine

Step 3 of 5

Choose Memory and CPU settings:

Memory: 24576

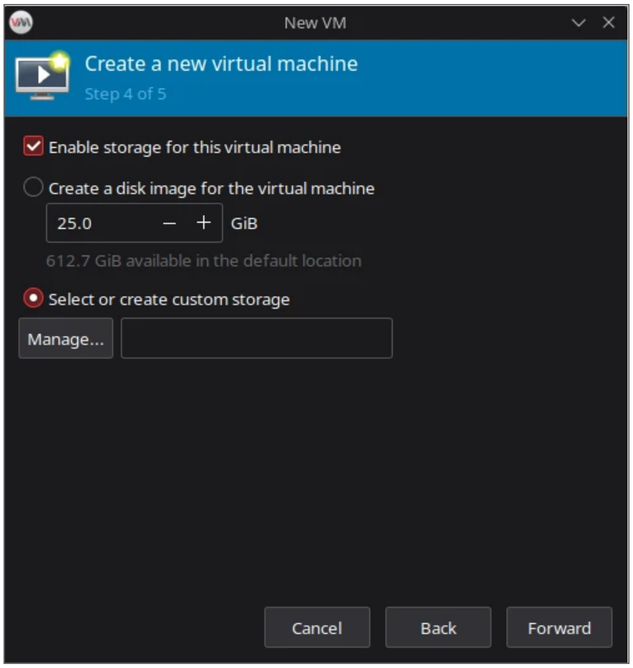
Up to 31876 MiB available on the host

CPUs: 4

Up to 20 available

5. Select the **Enable storage for this Virtual Machine**, and select **Select or create custom storage**.

   ⓘ **NOTE:** A copy of the SonicWALL_NSM-on-Prem-2.4.0-930.img must exist in /var/lib/libvirt/images before proceeding.


New VM

Create a new virtual machine

Step 4 of 5

☑ Enable storage for this virtual machine

○ Create a disk image for the virtual machine

25.0 GiB

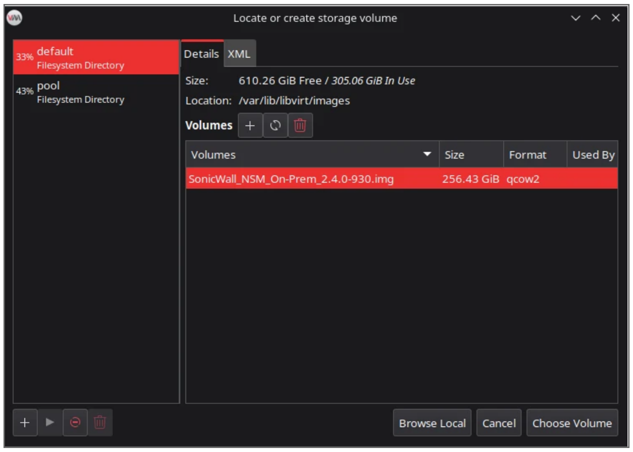
612.7 GiB available in the default location

● Select or create custom storage

6. Click **Manage**.

7. Use the copy of the **qcow2** image file as the VM disk volume. Click on **Choose Volume** to select the image volume.

   ⓘ **NOTE:** /var/lib/libvirt/images is the default location used by libvirt. To use a different location, create an additional storage pool (Using '+' button in the bottom left) and set the preferred location.



Locate or create storage volume

33% default
Filesystem Directory

43% pool
Filesystem Directory

Details | XML

Size: 610.26 GiB Free / *305.06 GiB In Use*

Location: /var/lib/libvirt/images

Volumes

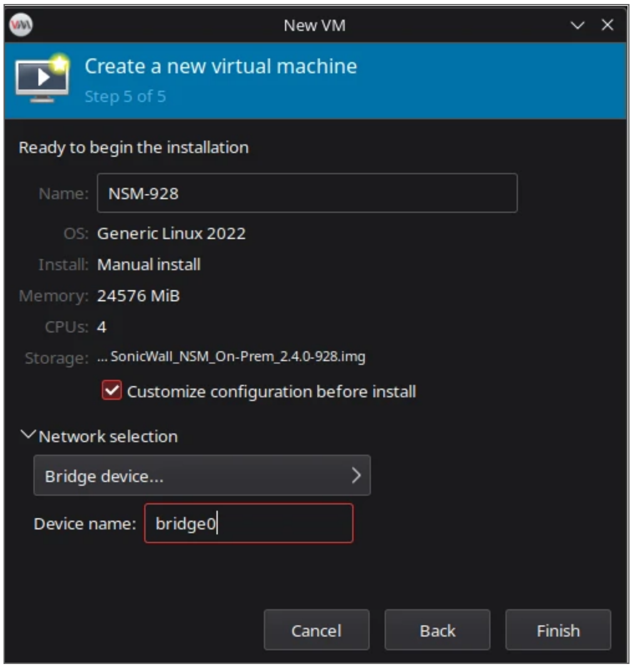
Volumes	Size	Format	Used By
SonicWall_NSM_On-Prem_2.4.0-930.img	256.43 GiB	qcow2	

8. Enter a VM name. Check the box for **Customize configuration before install**.

9. Set the **Network Selection** to **Bridge device**.

   ⓘ **NOTE:** Bridge interface is recommended for NSM On-Premises VMs for their simplicity and performance. Using NAT or Macvtap may cause issues with reachability, or network performance.

10. Click **Finish**.



New VM

Create a new virtual machine
Step 5 of 5

Ready to begin the installation

Name: NSM-928

OS: Generic Linux 2022

Install: Manual install

Memory: 24576 MiB

CPUs: 4

Storage: ...SonicWall_NSM_On-Prem_2.4.0-928.img

☑ Customize configuration before install

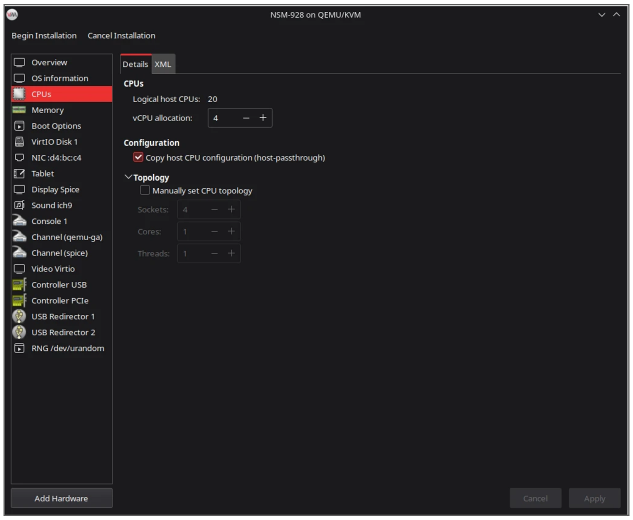
Network selection

Bridge device...

Device name: bridge0

11. Navigate to **CPU** tab, select the **host-passthrough**. Uncheck the **Topology** section.

ⓘ | **NOTE:** Do not use any CPU emulation for best performance and compatibility.



CPUs

Logical host CPUs: 20

vCPU allocation: 4

Configuration

☑ Copy host CPU configuration (host-passthrough)

Topology

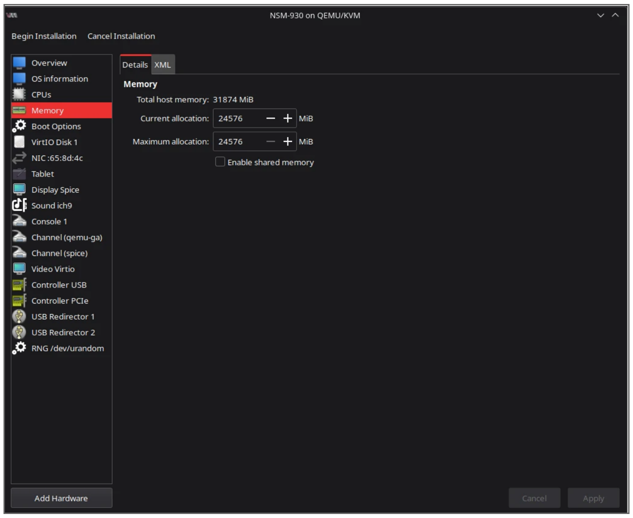
□ Manually set CPU topology

Sockets: 4

Cores: 1

Threads: 1

12. Navigate to **Memory** tab, make sure that **Enable Shared Memory** is unchecked. This may introduce side channels that could potentially be used to leak information across multiple guests.



Memory

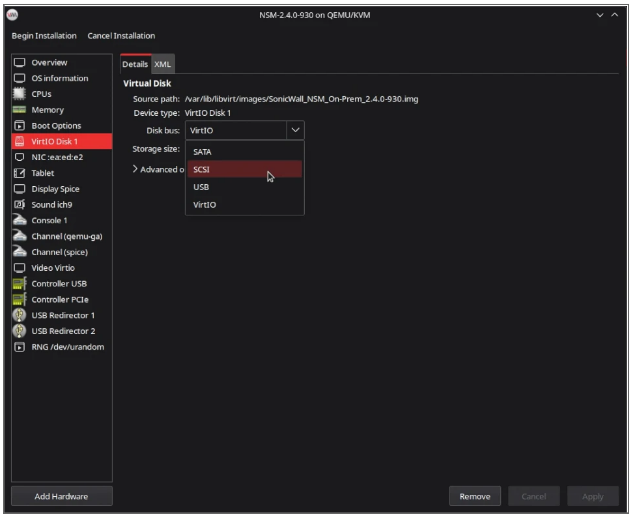
Total host memory: 31874 MiB

Current allocation: 24576 MiB

Maximum allocation: 24576 MiB

□ Enable shared memory

13. Navigate to **VirtIO Disk 1** tab, set the **Disk bus** to SCSI from the dropdown menu.



Virtual Disk

Source path: /var/lib/libvirt/images/SonicWall_NSM_On-Prem_2.4.0-930.img

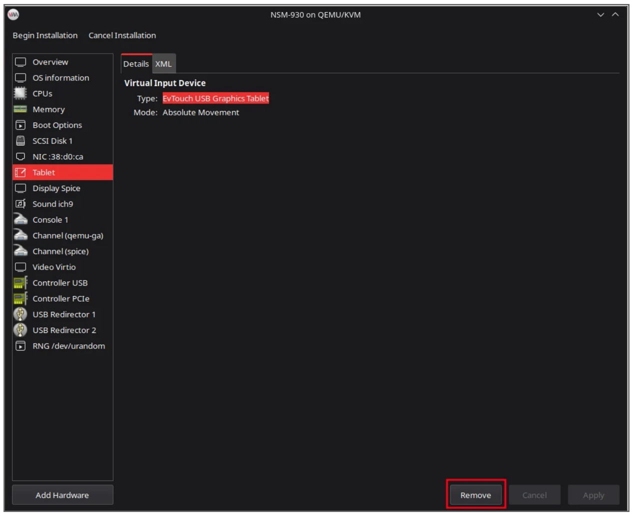
Device type: VirtIO Disk 1

Disk bus: VirtIO

Storage size:

14. Click **Apply**.

15. Navigate to **Tablet** tab, remove unnecessary devices, if they are attached.

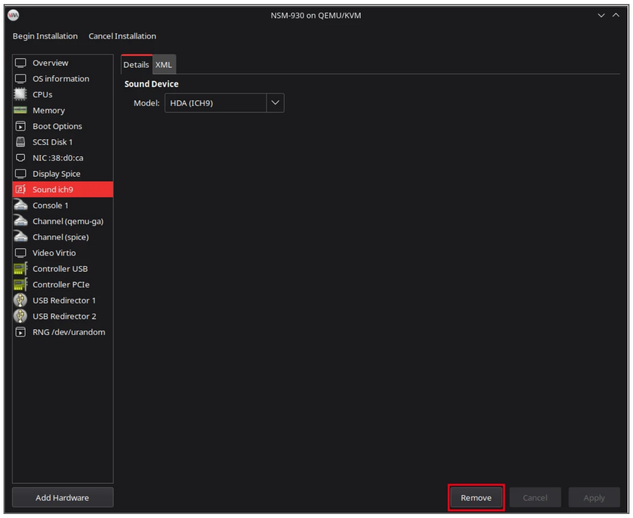


Virtual Input Device

Type: EvTouch USB Graphics Tablet

Mode: Absolute Movement

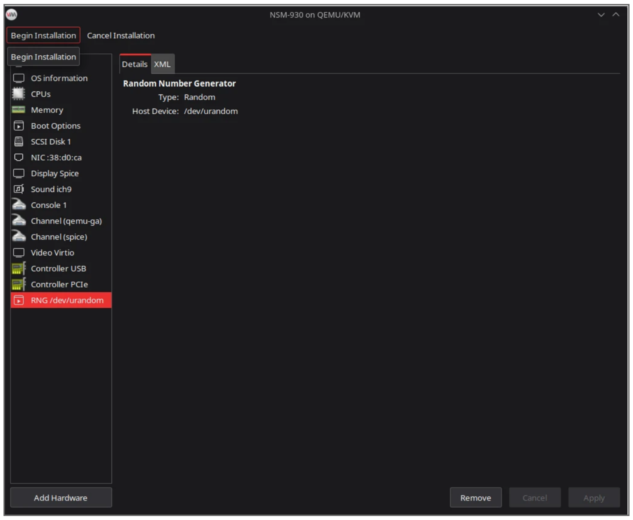
16. Navigate to Sound ich9, remove unnecessary devices, if they are attached.



Sound Device

Model: HDA (ICH9)

17. Click **Begin Installation** in the top-left corner.

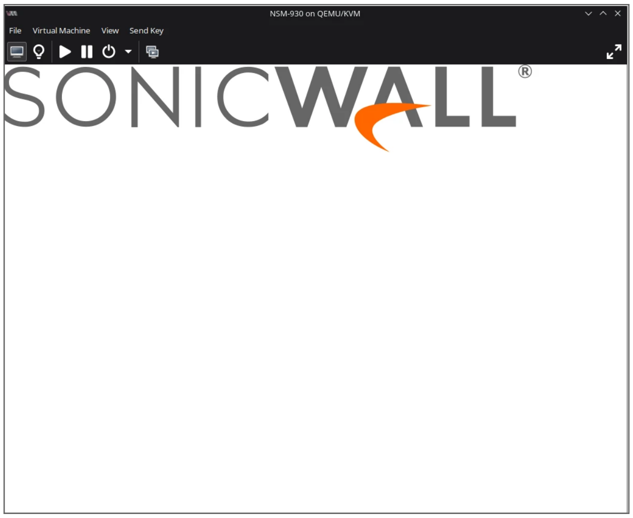


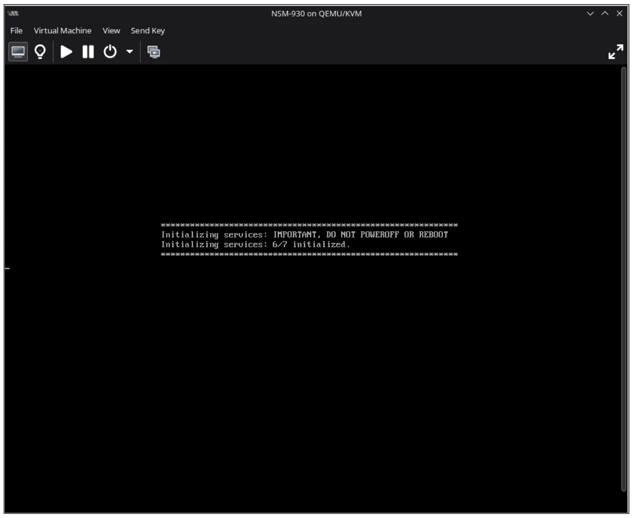
Random Number Generator

Type: Random

Host Device: /dev/urandom

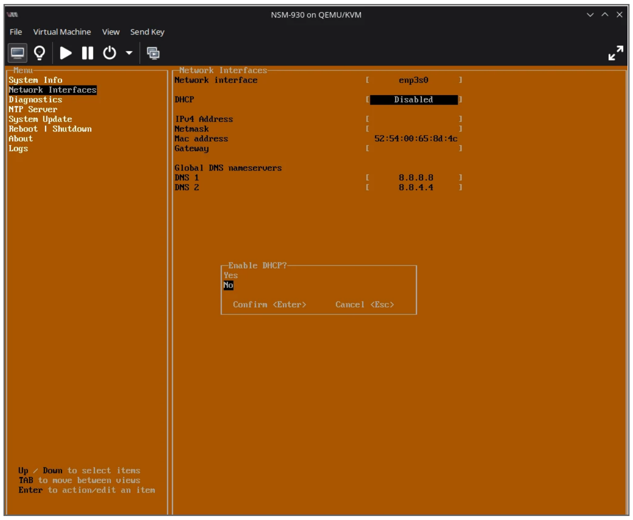
18. The NSM on-Prem VM boots up, initialises and starts the management console. The first boot of the VM can take up to 15 minutes, depending on the underlying hardware.





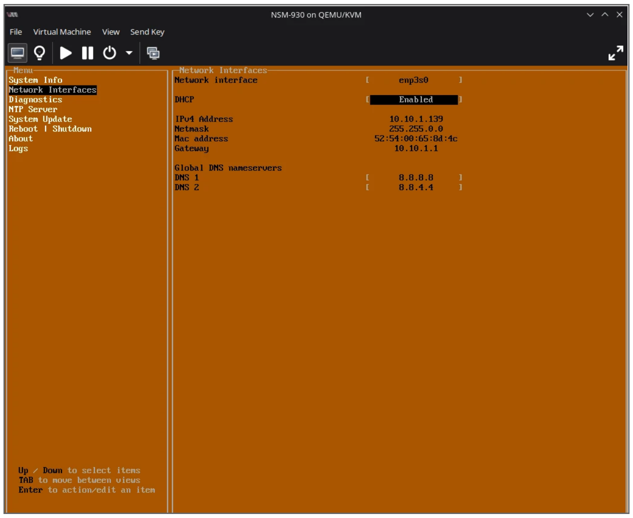
```
**************************************************************
Initializing services: IMPORTANT, DO NOT POWEROFF OR REBOOT
Initializing services: 6/7 initialized.
**************************************************************
```

19. Once the Management Console is active, use the arrow keys to navigate to the “Network Interfaces” pane → DHCP → Press Enter on Disabled → Enable the DHCP by selecting “Yes”. Save the setting.



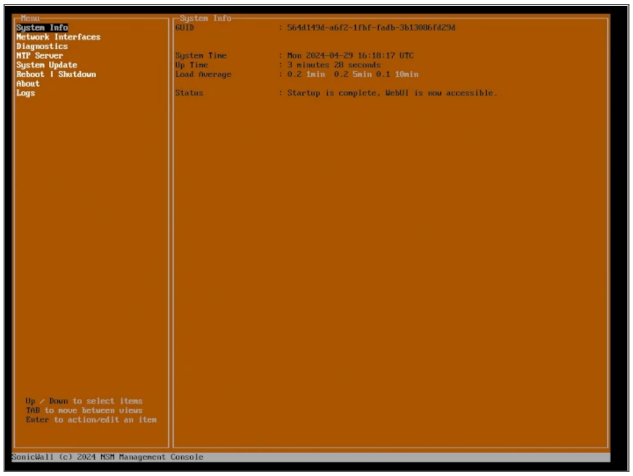
```
Menu                         Network Interfaces
System Info                  Network interface             [    enp3s0     ]
Network Interfaces
Diagnostics                  DHCP                          [   Disabled    ]
NTP Server
System Update                IPv4 Address                  [               ]
Reboot | Shutdown            Netmask                       [               ]
About                        Mac address                    52:54:00:65:8d:4c
Logs                         Gateway                       [               ]

                             Global DNS nameservers
                             DNS 1                         [    8.8.8.8    ]
                             DNS 2                         [    8.8.4.4    ]

                                  Enable DHCP?
                                  Yes
                                  No

                                    Confirm <Enter>     Cancel <Esc>

  Up / Down to select items
  TAB to move between views
  Enter to action/edit an item
```

20. This will assign the NSM on-Prem VM an IP address if the network interface is attached to a network with a DHCP server. If not, then proceed with setting a static IP for the VM. The NSM on-Prem Getting Started Guide goes into more detail about Network Management with Management Console.

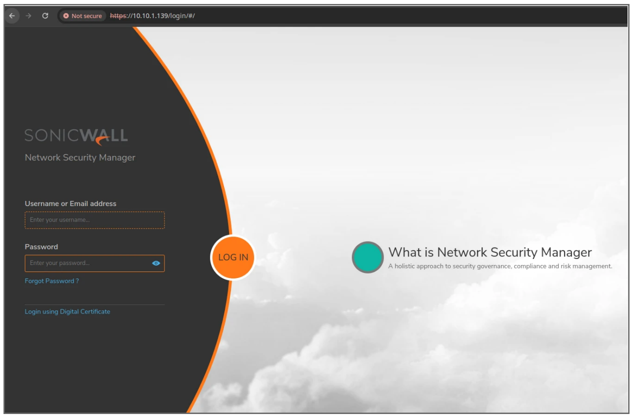


```
Menu                         Network Interfaces
System Info                  Network interface             [    enp3s0     ]
Network Interfaces
Diagnostics                  DHCP                          [    Enabled    ]
NTP Server
System Update                IPv4 Address                     10.10.1.139
Reboot | Shutdown            Netmask                          255.255.0.0
About                        Mac address                    52:54:00:65:8d:4c
Logs                         Gateway                           10.10.1.1

                             Global DNS nameservers
                             DNS 1                         [    8.8.8.8    ]
                             DNS 2                         [    8.8.4.4    ]

  Up / Down to select items
  TAB to move between views
  Enter to action/edit an item
```

21. Once the “Status:” of the system is “Startup is complete, Web UI is now accessible.” in System Info pane Head to the IP address on a browser to access the web UI.



```
-Menu-                          -System Info-
System Info                     GUID              : 564d149d-a6f2-1fbf-fadb-3b13086fd29d
Network Interfaces
Diagnostics                     System Time       : Mon 2024-04-29 16:18:17 UTC
NTP Server                      Up Time           : 3 minutes 28 seconds
System Update                   Load Average      : 0.2 1min  0.2 5min 0.1 10min
Reboot | Shutdown
About                           Status            : Startup is complete, WebUI is now accessible.
Logs

  Up / Down to select items
  TAB to move between views
  Enter to action/edit an item

SonicWall (c) 2024 NSM Management Console
```


Not secure
https://10.10.1.139/login/#/
SONICWALL
Network Security Manager
Username or Email address
Enter your username...
Password
Enter your password...
Forgot Password ?
Login using Digital Certificate
LOG IN
What is Network Security Manager
A holistic approach to security governance, compliance and risk management.

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.

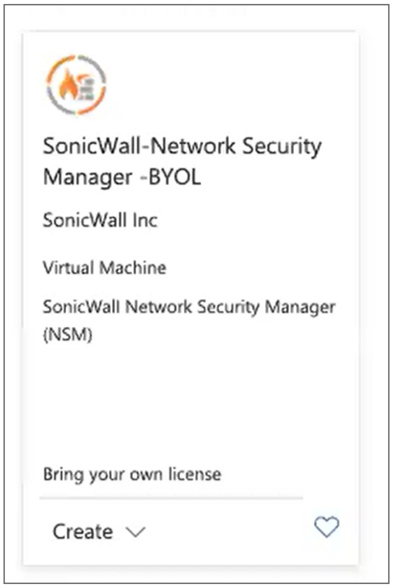
6

Installing NSM on Azure

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 Security Manager -BYOL

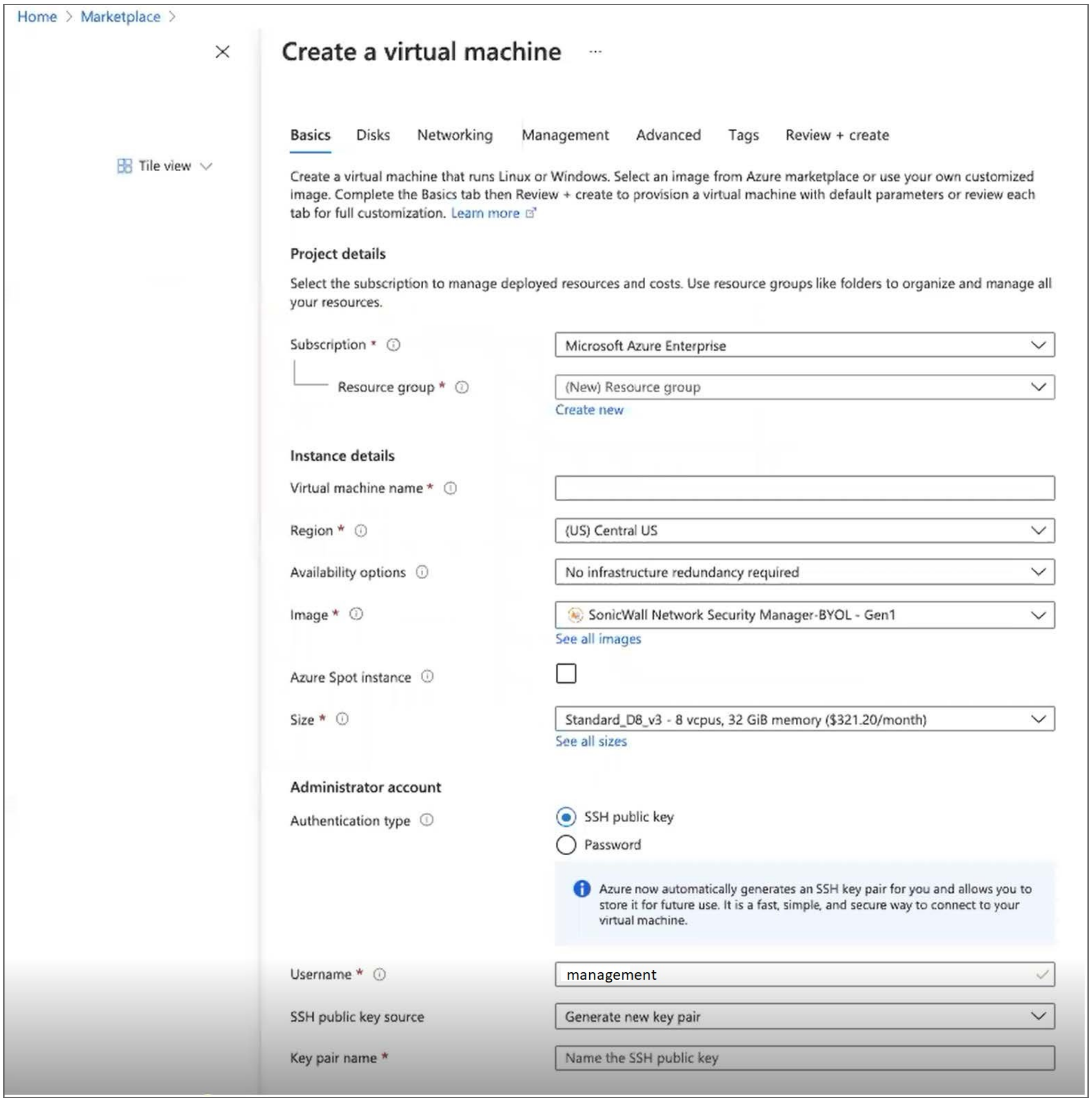
SonicWall Inc

Virtual Machine

SonicWall Network Security Manager (NSM)

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 machine

Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image. Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization. Learn more

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription *: Microsoft Azure Enterprise

Resource group *: (New) Resource group

Instance details

Virtual machine name *:

Region *: (US) Central US

Availability options: No infrastructure redundancy required

Image *: SonicWall Network Security Manager-BYOL - Gen1

Azure Spot instance: □

Size *: Standard_D8_v3 - 8 vcpus, 32 GiB memory ($321.20/month)

Administrator account

Authentication type: ● SSH public key ○ Password

Azure now automatically generates an SSH key pair for you and allows you to store it for future use. It is a fast, simple, and secure way to connect to your virtual machine.

Username *: management

SSH public key source: Generate new key pair

Key pair name *: Name the SSH public key

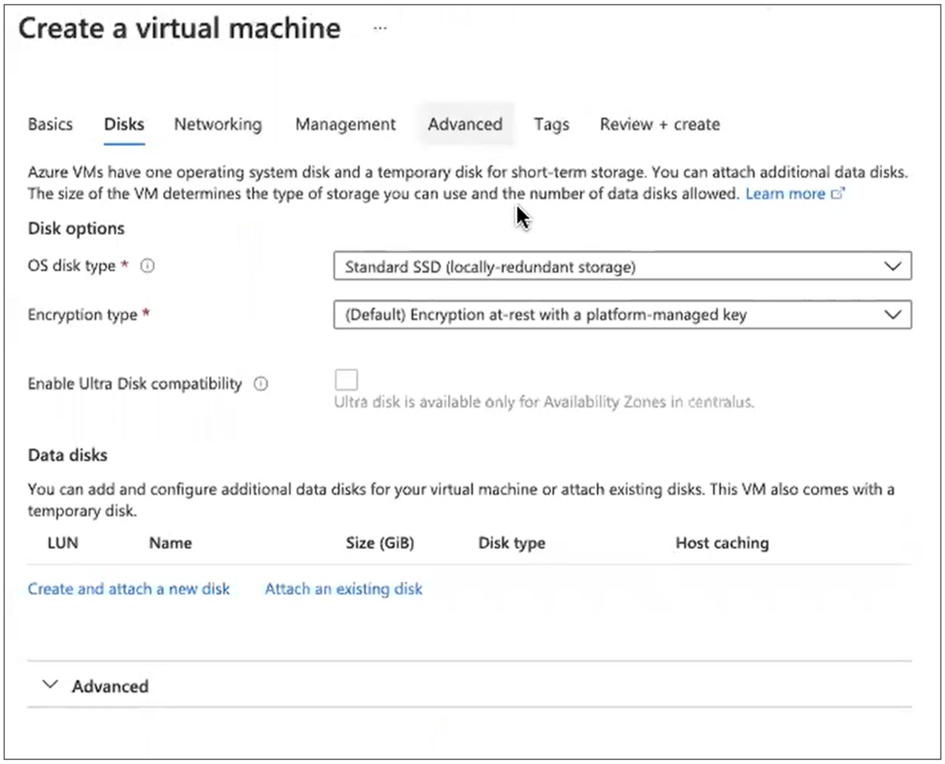
5. Type an easy-to-identify name in the **Name** field and click **OK**.
6. Enter the **Virtual machine name**. It can be the same as the **Resource group name**, if you want.
7. Set the **Region**.
8. From the **Image** drop-down list, select the **SonicWall-Network Security Manager -BYOL**.
9. Leave **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 virtual machine

Azure VMs have one operating system disk and a temporary disk for short-term storage. You can attach additional data disks. The size of the VM determines the type of storage you can use and the number of data disks allowed. Learn more

Disk options

OS disk type *: Standard SSD (locally-redundant storage)

Encryption type *: (Default) Encryption at-rest with a platform-managed key

Enable Ultra Disk compatibility: □ Ultra disk is available only for Availability Zones in centralus.

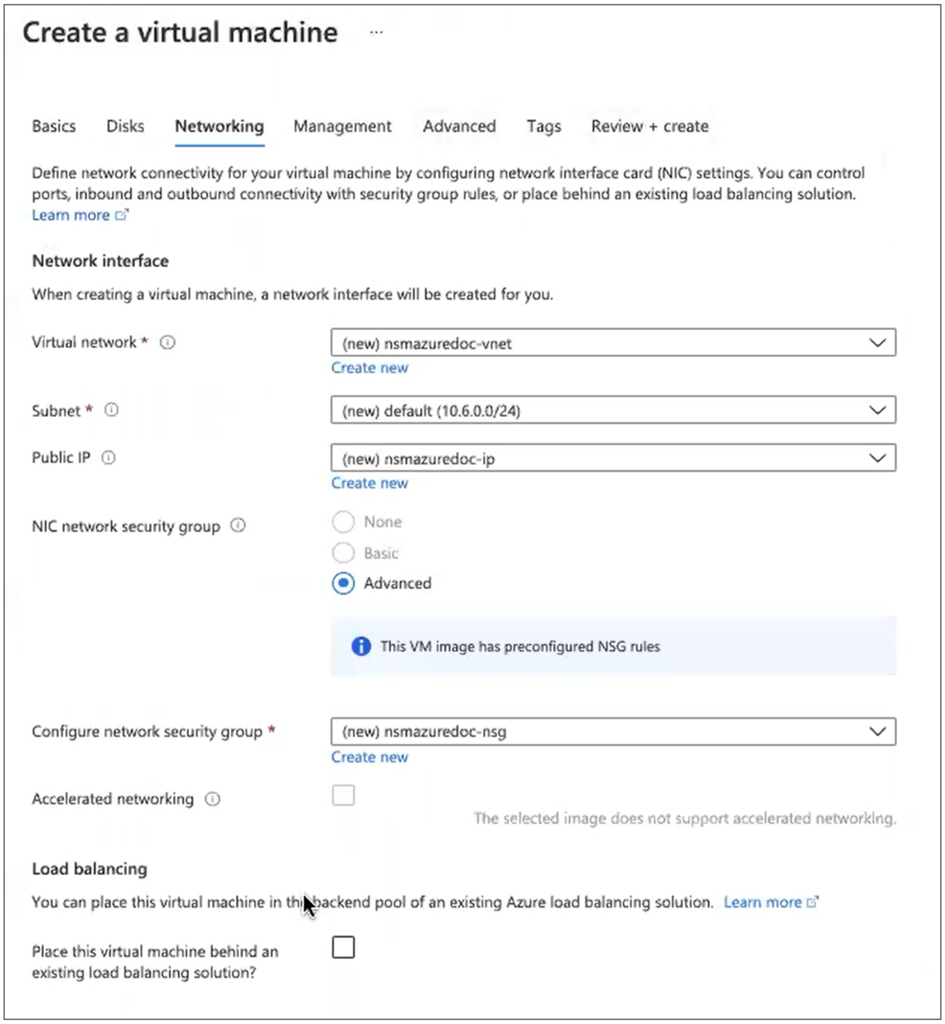
Data disks

You can add and configure additional data disks for your virtual machine or attach existing disks. This VM also comes with a temporary disk.

LUN	Name	Size (GiB)	Disk type	Host caching

16. Use the defaults on the Disks tab.

17. Click **Next : Networking >**.



Create a virtual machine ...

Basics | Disks | **Networking** | Management | Advanced | Tags | Review + create

Define network connectivity for your virtual machine by configuring network interface card (NIC) settings. You can control ports, inbound and outbound connectivity with security group rules, or place behind an existing load balancing solution. Learn more

Network interface

When creating a virtual machine, a network 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 group : ○ None ○ Basic ● Advanced

This VM image has preconfigured NSG rules

Configure network security group * : (new) nsmazuredoc-nsg
Create new

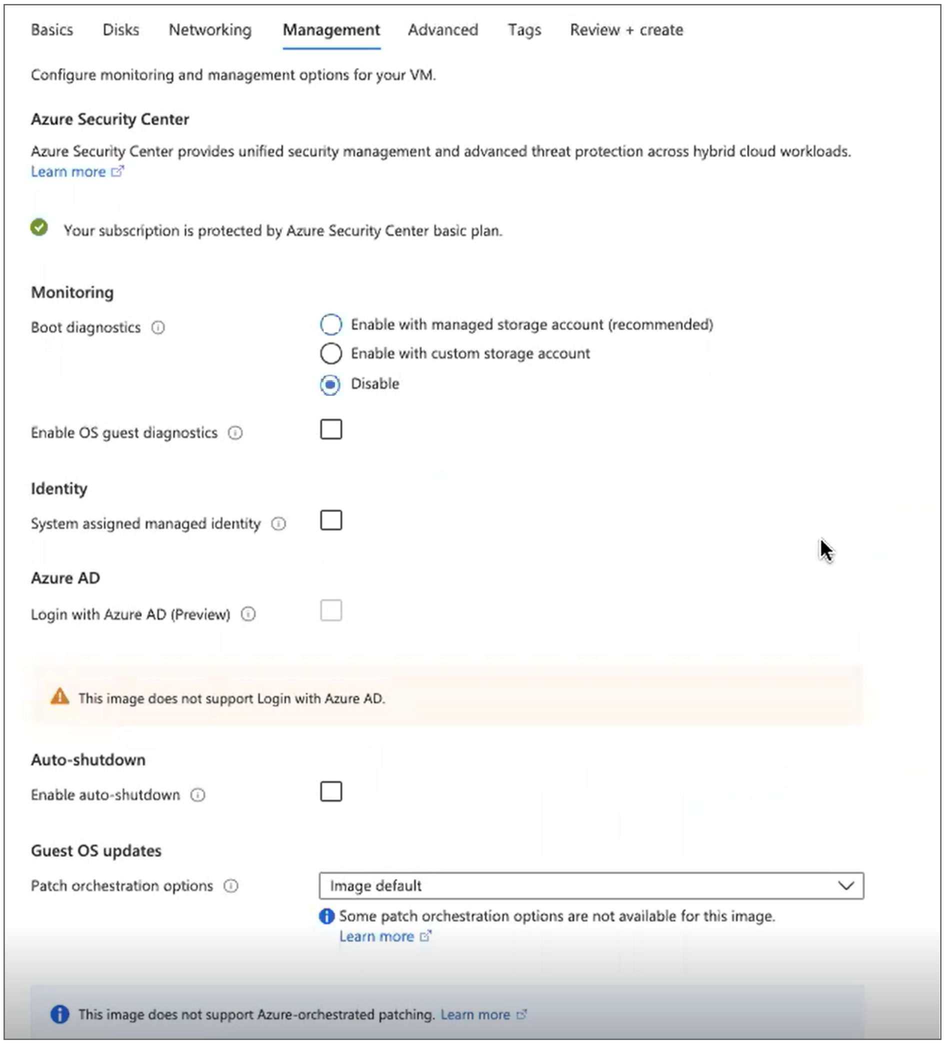
Accelerated networking : □
The selected image does not support accelerated networking.

Load balancing

You can place this virtual machine in the backend 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 >**.



Configure monitoring and management options for your VM.

Azure Security Center

Azure Security Center provides unified security management and advanced threat protection across hybrid cloud workloads.
Learn more

✓ Your subscription is protected by Azure Security Center basic plan.

Monitoring

Boot diagnostics ⓘ
○ Enable with managed storage account (recommended)
○ Enable with custom storage account
● Disable

Enable OS guest diagnostics ⓘ □

Identity

System assigned managed identity ⓘ □

Azure AD

Login with Azure AD (Preview) ⓘ □

⚠ This image does not support Login with Azure AD.

Auto-shutdown

Enable auto-shutdown ⓘ □

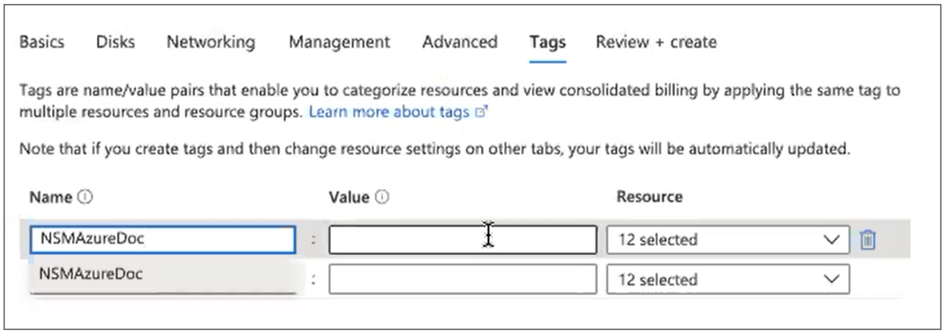
Guest OS updates

Patch orchestration options ⓘ Image default

ⓘ Some patch orchestration options are not available for this image.
Learn more

ⓘ This image does not support Azure-orchestrated patching. Learn more

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 >**.



Tags are name/value pairs that enable you to categorize resources and view consolidated billing by applying the same tag to multiple resources and resource groups. Learn more about tags

Note that if you create tags and then change resource settings on other tabs, your tags will be automatically updated.

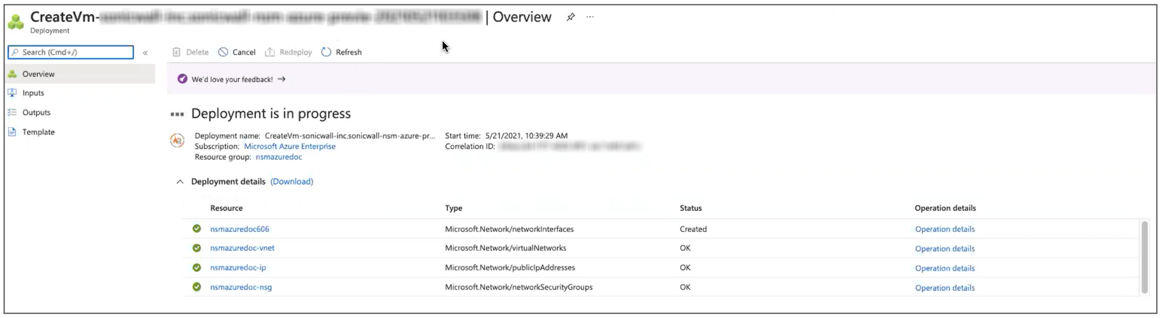
Name		Value	Resource
NSMAzureDoc	:		12 selected
NSMAzureDoc	:		12 selected

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-[redacted] | Overview

Deployment

Deployment is in progress

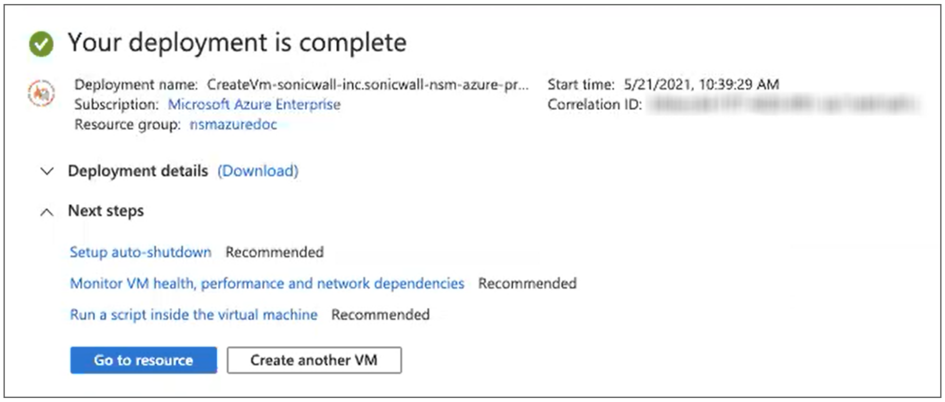
Deployment name: CreateVm-sonicwall-inc.sonicwall-nsm-azure-pr...
Subscription: Microsoft Azure Enterprise
Resource group: nsmazuredoc

Start time: 5/21/2021, 10:39:29 AM
Correlation ID: [redacted]

Deployment details (Download)

Resource	Type	Status	Operation details
nsmazuredoc606	Microsoft.Network/networkInterfaces	Created	Operation details
nsmazuredoc-vnet	Microsoft.Network/virtualNetworks	OK	Operation details
nsmazuredoc-ip	Microsoft.Network/publicIpAddresses	OK	Operation details
nsmazuredoc-nsg	Microsoft.Network/networkSecurityGroups	OK	Operation details

A message displays when the deployment is complete.



Your deployment is complete

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: [redacted]

Deployment details (Download)

Next steps

Setup auto-shutdown Recommended

Monitor VM health, performance and network dependencies Recommended

Run a script inside the virtual machine Recommended

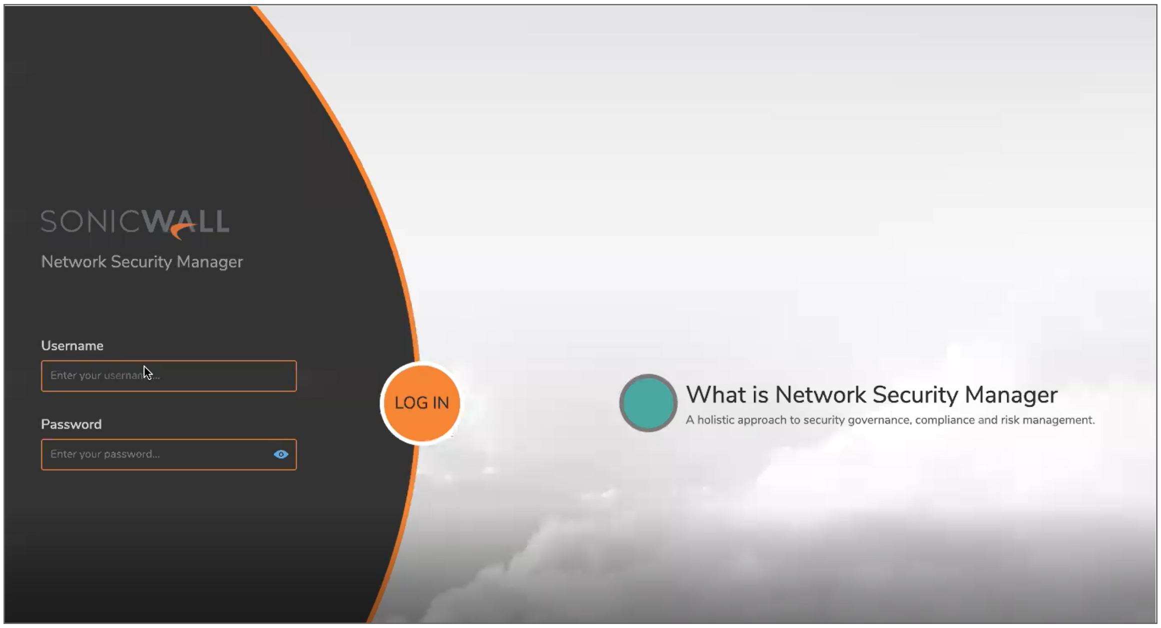
29. Click **Go to resource** from the deployment complete page.

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.

When the activity is complete, the NSM login banner appears.



SONICWALL

Network Security Manager

Username

Enter your username...

Password

Enter your password...

What is Network Security Manager

A holistic approach to security governance, compliance and risk management.

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

7

NSM Settings and Registration

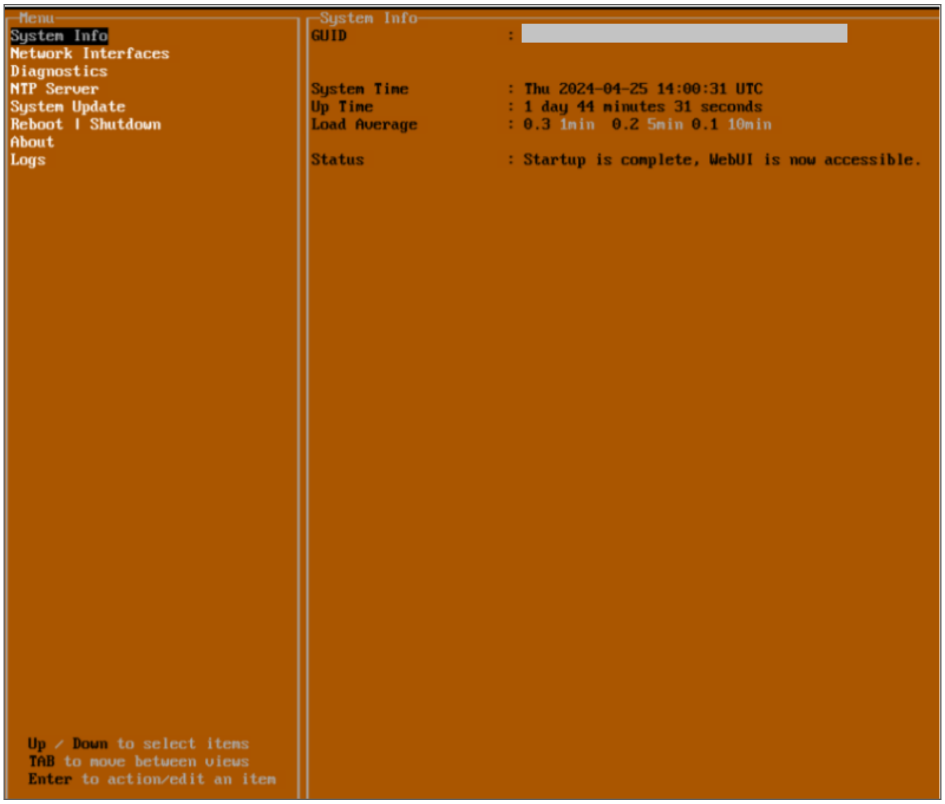
After the installation of the NSM image is complete, you need to define the network settings and register your product.

Topics:

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

Configuring NSM Network Settings

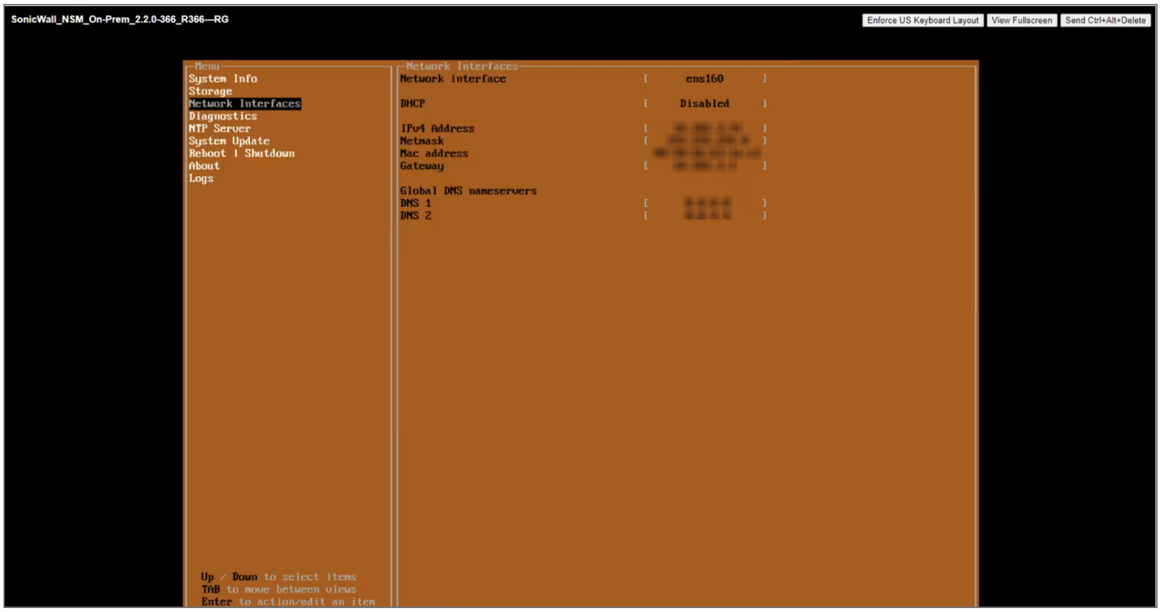
1. Open the NSM Management Console.



```
GUID                    : [redacted]

System Time             : Thu 2024-04-25 14:00:31 UTC
Up Time                 : 1 day 44 minutes 31 seconds
Load Average            : 0.3 1min  0.2 5min 0.1 10min

Status                  : Startup is complete, WebUI is now accessible.
```

```
Up / Down to select items
TAB to move between views
Enter to action/edit an item
```

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


SonicWall_NSM_On-Prem_2.2.0-366_R366—RG
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete

```
Menu                      Network Interfaces
System Info               Network interface              [     ens160     ]
Storage
Network Interfaces        DHCP                           [    Disabled    ]
Diagnostics
NTP Server                IPv4 Address                   [   [redacted]   ]
System Update             Netmask                        [   [redacted]   ]
Reboot | Shutdown         Mac address                        [redacted]
About                     Gateway                        [   [redacted]   ]
Logs
                          Global DNS nameservers
                          DNS 1                          [   [redacted]   ]
                          DNS 2                          [   [redacted]   ]

  Up / Down to select items
  TAB to move between views
  Enter to action/edit an item
```

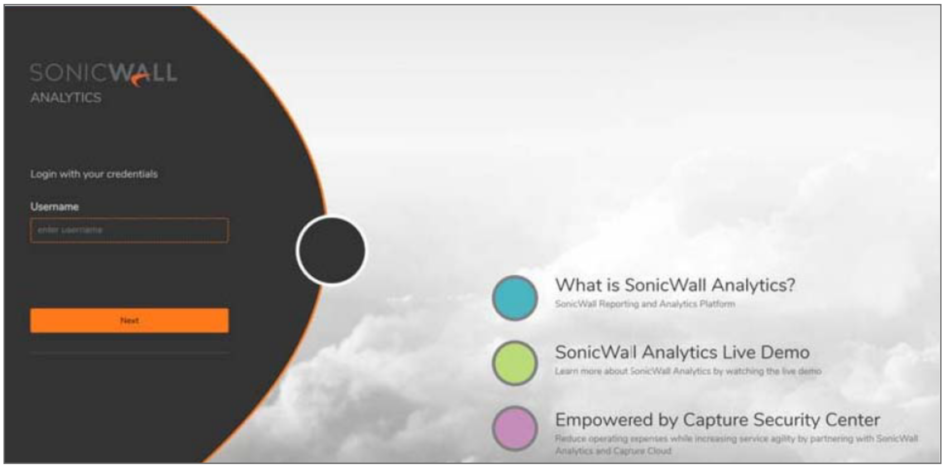
3. Select **ens160**.
4. Navigate to the **DHCP** field, and press **Enter**.
5. Select **No** and press **Enter** to confirm.
6. Update the **IPv4 Address**, the **Netmask**, and **Gateway**.
7. Save the settings.
8. Enter the **DNS 1** and **DNS 2** and Save **Changes**.
9. To verify that all the network 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 ANALYTICS

Login with your credentials

Username: enter username

What is SonicWall Analytics?

SonicWall Reporting and Analytics Platform

SonicWall Analytics Live Demo

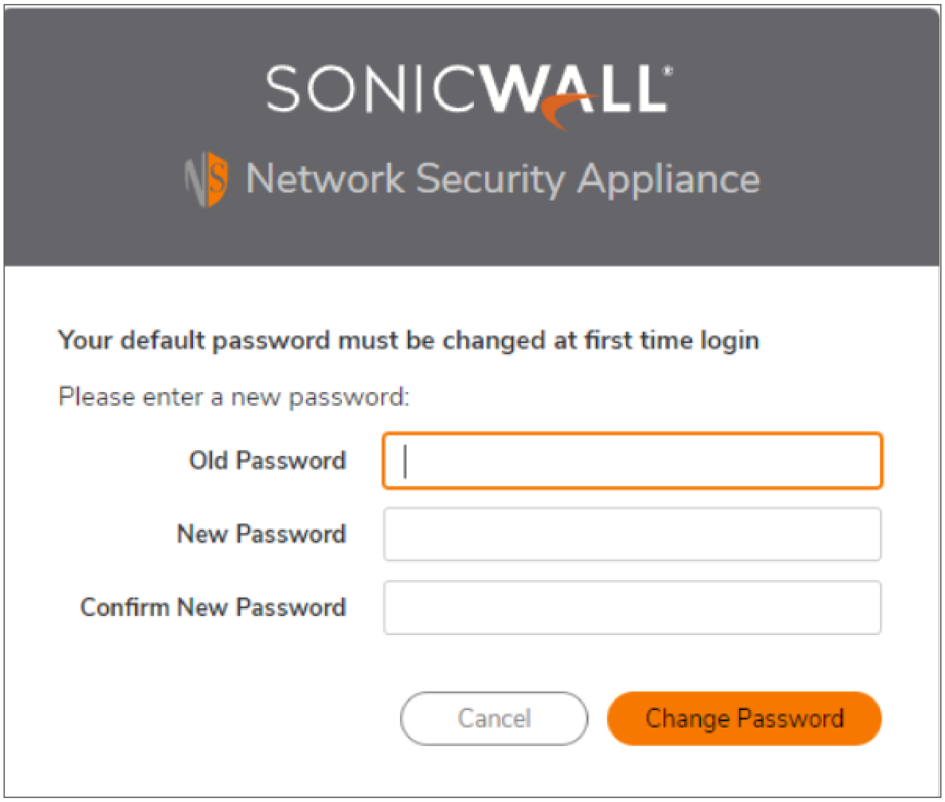
Learn more about SonicWall Analytics by watching the live demo

Empowered by Capture Security Center

Reduce operating expenses while increasing service agility by partnering with SonicWall Analytics and Capture Cloud

2. For initial access, log in using **admin** and **password** as our credentials. On successful login with default password, you will be prompted to change default password. On successful change of default password, the first time you access NSM, it presents an initialization wizard.

ⓘ | **NOTE:** Changing the default password is mandatory.



SONICWALL

Network Security Appliance

Your default password must be changed at first time login

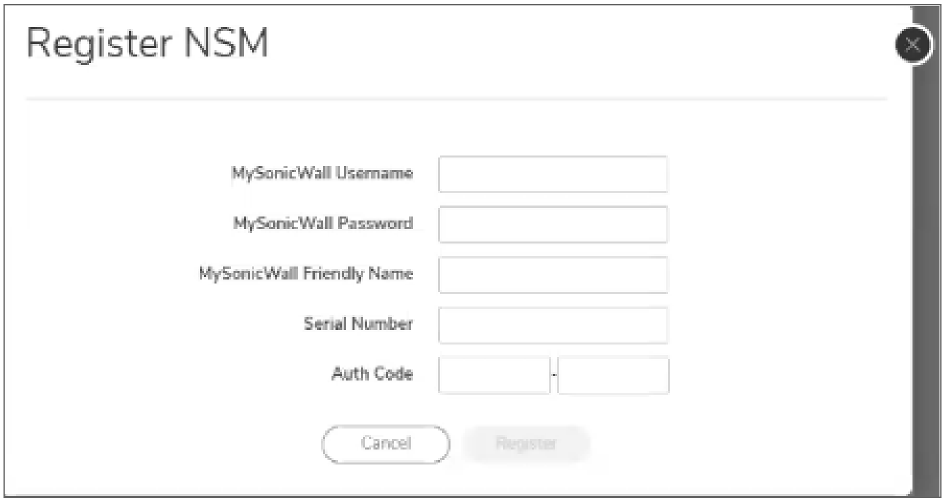
Please enter a new password:

Old Password

New Password

Confirm New Password

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**.



Register NSM

MySonicWall Username

MySonicWall Password

MySonicWall Friendly Name

Serial Number

Auth Code

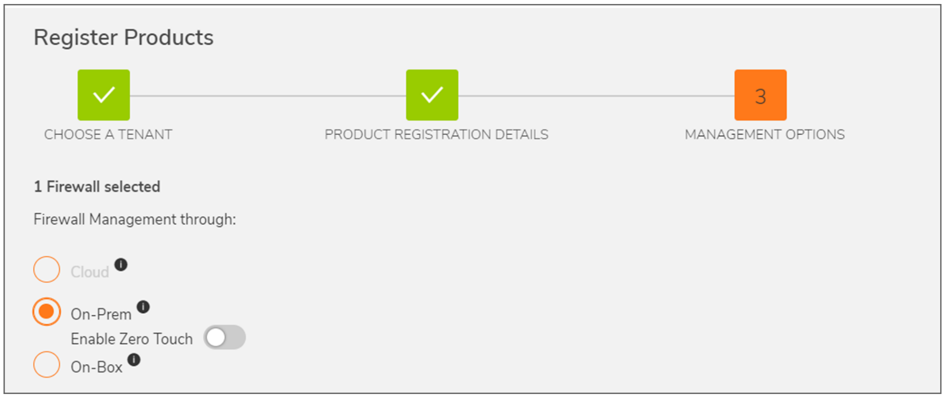
7. To confirm registration, navigate to **Manager View | System > Settings > Licenses**.
8. Validate that the status of your NSM is **Licensed**.
9. Click **Synchronize** to synchronize your NSM instance with the License Manager on MSW.

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

✓ CHOOSE A TENANT — ✓ PRODUCT REGISTRATION DETAILS — 3 MANAGEMENT OPTIONS

1 Firewall selected

Firewall Management through:

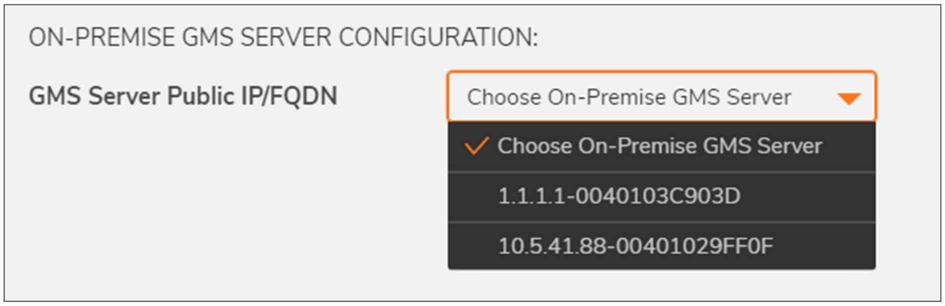
○ Cloud

● 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.



ON-PREMISE GMS SERVER CONFIGURATION:

GMS Server Public IP/FQDN: Choose On-Premise GMS Server

- ✓ Choose On-Premise GMS Server
- 1.1.1.1-0040103C903D
- 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.

8

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.

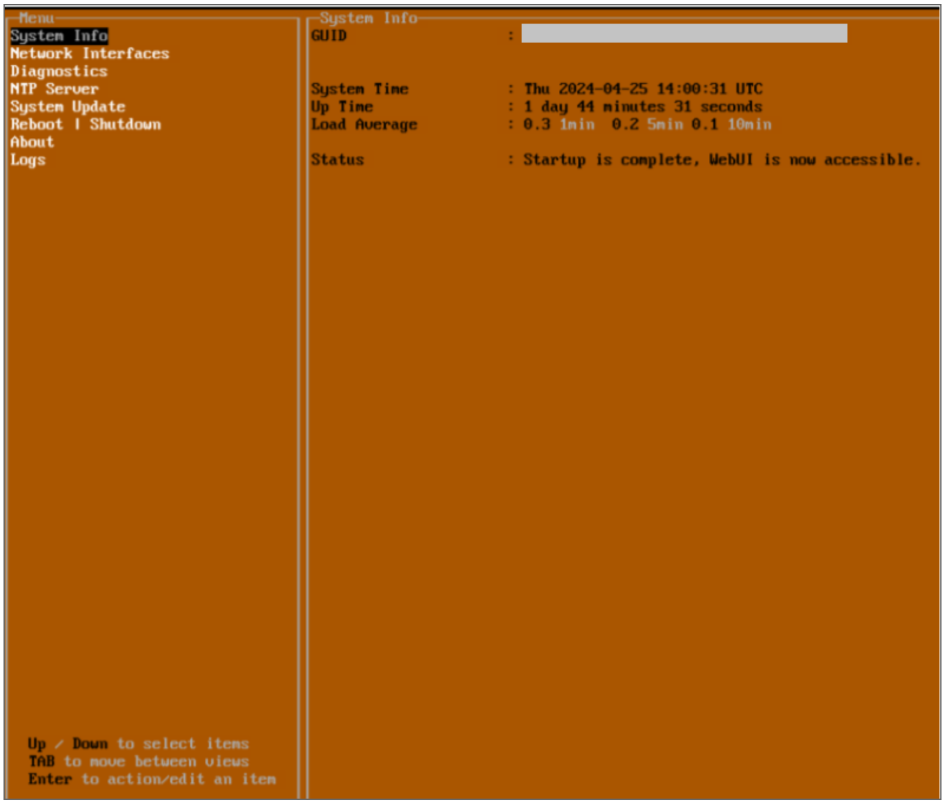
Topics:

- 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:

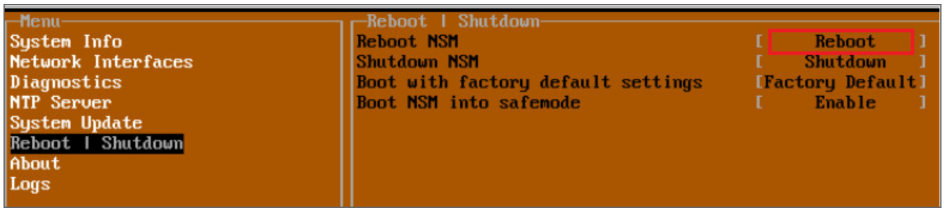


```
Menu                          System Info
System Info                   GUID                 : [redacted]
Network Interfaces
Diagnostics
NTP Server                    System Time          : Thu 2024-04-25 14:00:31 UTC
System Update                 Up Time              : 1 day 44 minutes 31 seconds
Reboot | Shutdown             Load Average         : 0.3 1min  0.2 5min 0.1 10min
About
Logs                          Status               : Startup is complete, WebUI is now accessible.




  Up / Down to select items
  TAB to move between views
  Enter to action/edit an item
```

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.

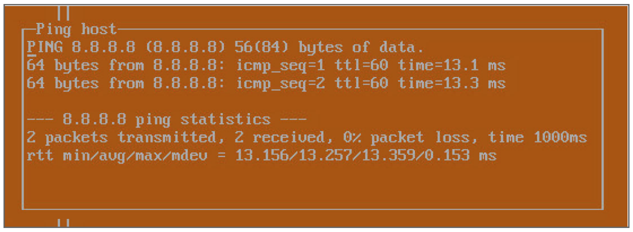
4. In the main view, use the up/down arrow keys to move the focus between options. Items shown inside square brackets denote actionable items.



```
Menu                  Reboot | Shutdown
System Info           Reboot NSM                                [    Reboot     ]
Network Interfaces    Shutdown NSM                              [   Shutdown    ]
Diagnostics           Boot with factory default settings        [Factory Default]
NTP Server            Boot NSM into safemode                    [    Enable     ]
System Update
Reboot | Shutdown
About
Logs
```

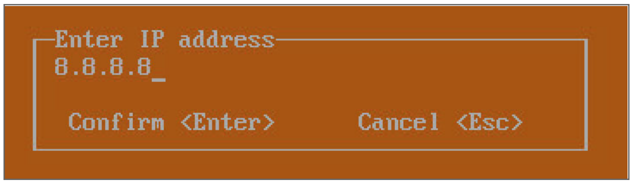
5. To select an option for editing or to choose the associated action, use the up/down arrow keys to move the focus to the editable/actionable items and press **Enter**.

   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:



```
Ping host
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=60 time=13.1 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=60 time=13.3 ms

--- 8.8.8.8 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1000ms
rtt min/avg/max/mdev = 13.156/13.257/13.359/0.153 ms
```

Some dialogs are for input:



```
Enter IP address
8.8.8.8_

 Confirm <Enter>        Cancel <Esc>
```

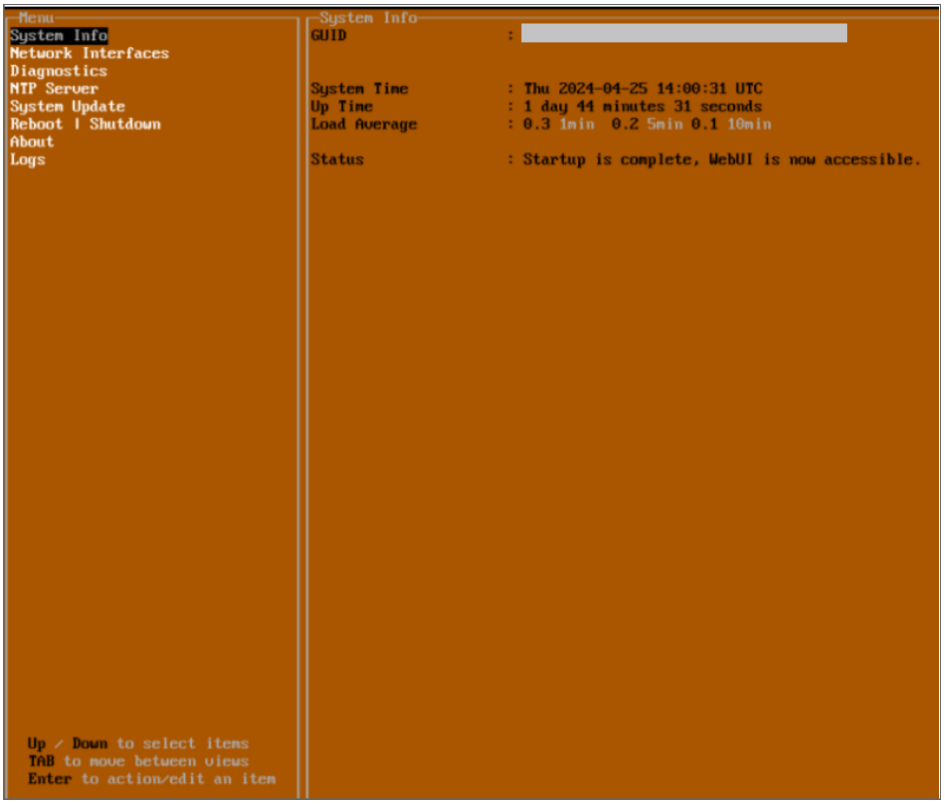
6. Use the arrow keys as needed to move between selections in the dialog. To change a value, press **Backspace** to erase each character, then type in the new value. When ready, press **Enter** to commit the change or perform the selected action. You can dismiss the dialog by pressing **Esc**.

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



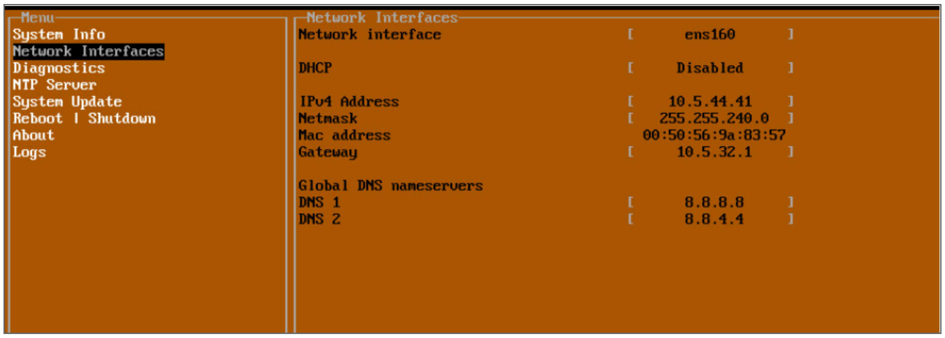
```
System Info
GUID                    : [redacted]


System Time             : Thu 2024-04-25 14:00:31 UTC
Up Time                 : 1 day 44 minutes 31 seconds
Load Average            : 0.3 1min  0.2 5min 0.1 10min

Status                  : Startup is complete, WebUI is now accessible.
```

```
Up / Down to select items
TAB to move between views
Enter to action/edit an item
```

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

- **GUID** – Every On-Premises NSM 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.
- **Status** - This shows the startup status of NSM.

Network Interfaces



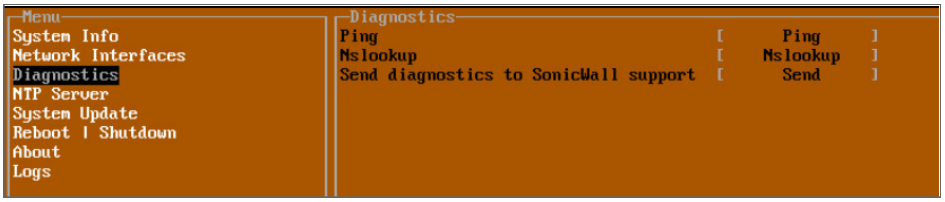
```
Menu                          Network Interfaces
System Info                   Network interface        [    ens160     ]
Network Interfaces
Diagnostics                   DHCP                     [   Disabled    ]
NTP Server
System Update                 IPv4 Address             [  10.5.44.41   ]
Reboot | Shutdown             Netmask                  [ 255.255.240.0 ]
About                         Mac address               00:50:56:9a:83:57
Logs                          Gateway                  [   10.5.32.1   ]

                              Global DNS nameservers
                              DNS 1                    [    8.8.8.8    ]
                              DNS 2                    [    8.8.4.4    ]
```

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**.



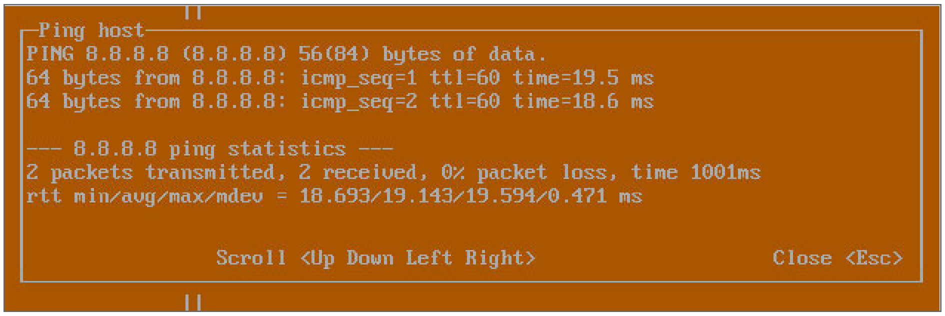
```
Menu                    Diagnostics
System Info             Ping                                  [    Ping     ]
Network Interfaces      Nslookup                              [  Nslookup   ]
Diagnostics             Send diagnostics to SonicWall support [    Send     ]
NTP Server
System Update
Reboot | 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.



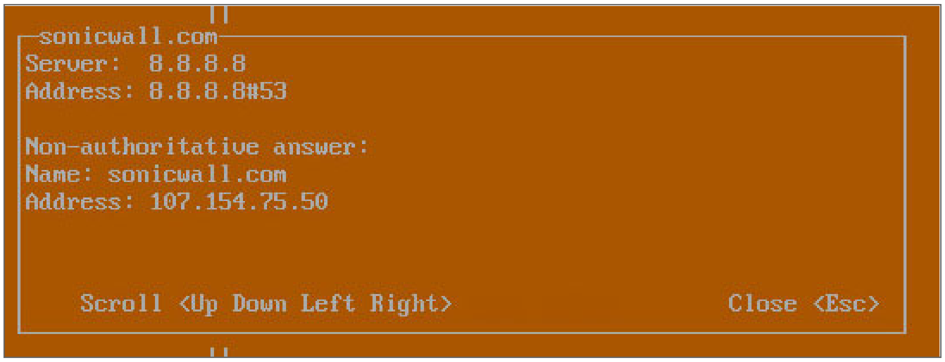
```
Ping host
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=60 time=19.5 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=60 time=18.6 ms

--- 8.8.8.8 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 18.693/19.143/19.594/0.471 ms

                Scroll <Up Down Left Right>                   Close <Esc>
```

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.



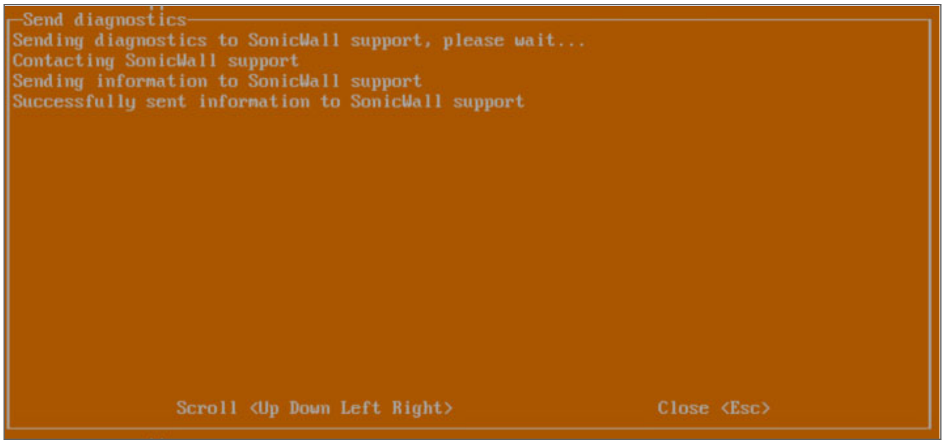
```
sonicwall.com
Server:  8.8.8.8
Address: 8.8.8.8#53

Non-authoritative answer:
Name: sonicwall.com
Address: 107.154.75.50


    Scroll <Up Down Left Right>                   Close <Esc>
```

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.

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



```
Send diagnostics
Sending diagnostics to SonicWall support, please wait...
Contacting SonicWall support
Sending information to SonicWall support
Successfully sent information to SonicWall support

                Scroll <Up Down Left Right>                Close <Esc>
```

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.

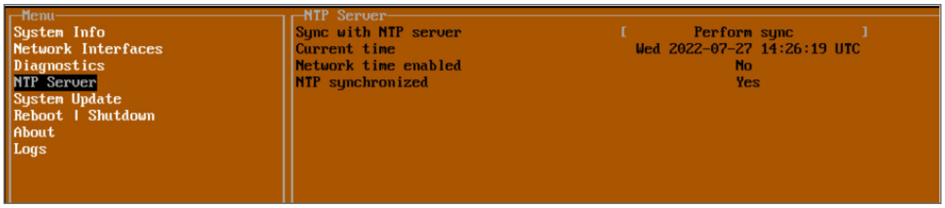
Common reasons for the report failing to send include:

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

ⓘ | **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.



```
Menu                  NTP Server
System Info           Sync with NTP server                    [        Perform sync        ]
Network Interfaces    Current time                              Wed 2022-07-27 14:26:19 UTC
Diagnostics           Network time enabled                                  No
NTP Server            NTP synchronized                                      Yes
System Update
Reboot | Shutdown
About
Logs
```

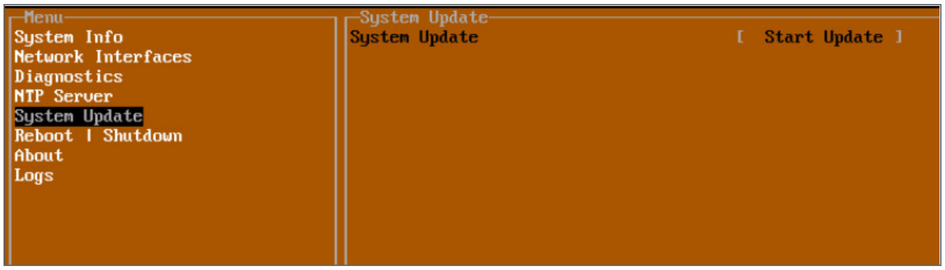
The **NTP Server** screen displays the following information:

- **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

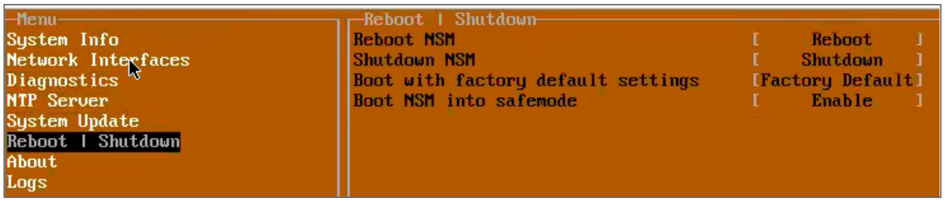
The **System Update** screen provides function to start the system update.



```
Menu                              System Update
System Info                       System Update                      [  Start Update ]
Network Interfaces
Diagnostics
NTP Server
System Update
Reboot | Shutdown
About
Logs
```

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                          [     Reboot     ]
Network Interfaces                Shutdown NSM                        [    Shutdown    ]
Diagnostics                       Boot with factory default settings  [Factory Default]
NTP Server                        Boot NSM into safemode              [     Enable     ]
System Update
Reboot | Shutdown
About
Logs
```

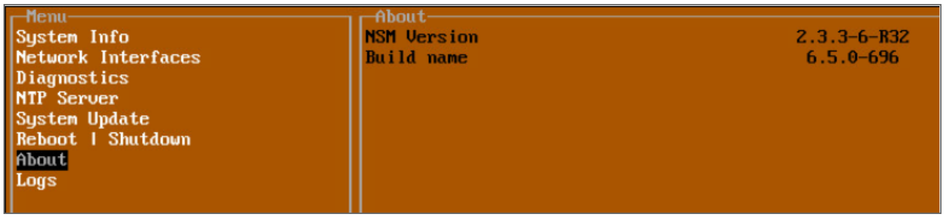
To perform an action, position the focus and then press **Enter** to select the desired action. Select **Yes** in the confirmation dialog, then press **Enter** again.

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

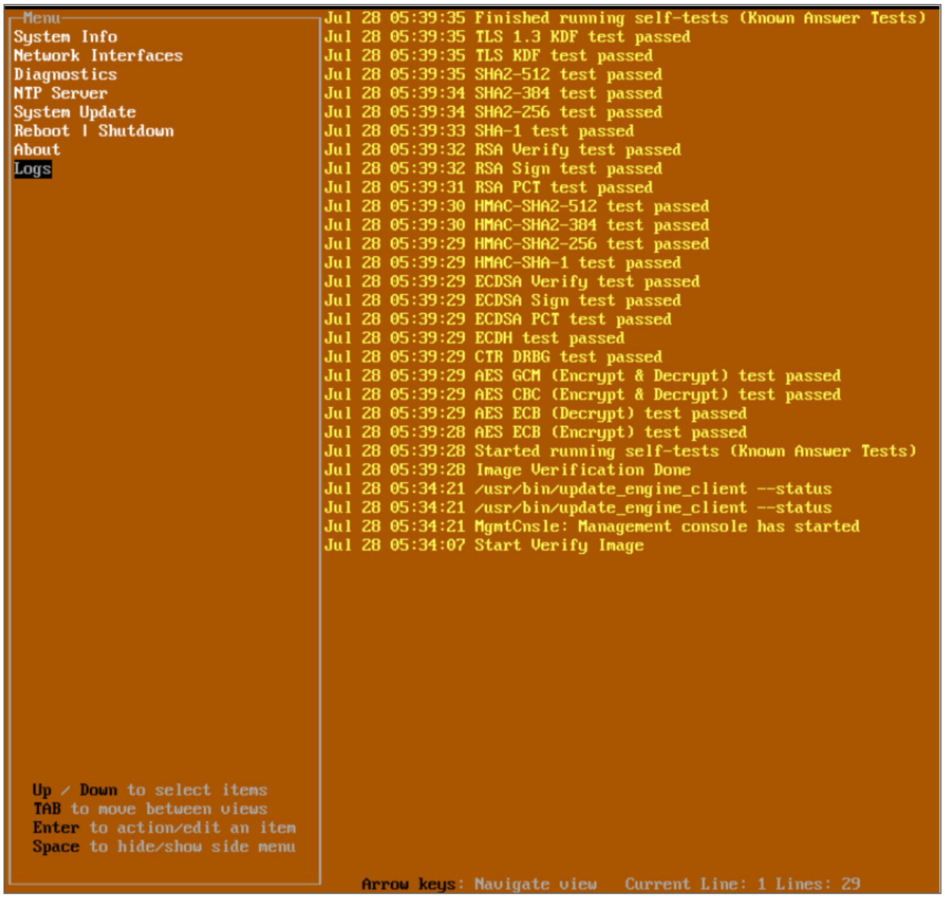
The About screen provides information about the software version and build.



```
NSM Version                                2.3.3-6-R32
Build name                                  6.5.0-696
```

Logs

The Logs screen displays log events for the instance.


Menu
System Info
Network Interfaces
Diagnostics
NTP Server
System Update
Reboot | Shutdown
About
Logs
Up / Down to select items
TAB to move between views
Enter to action/edit an item
Space to hide/show side menu

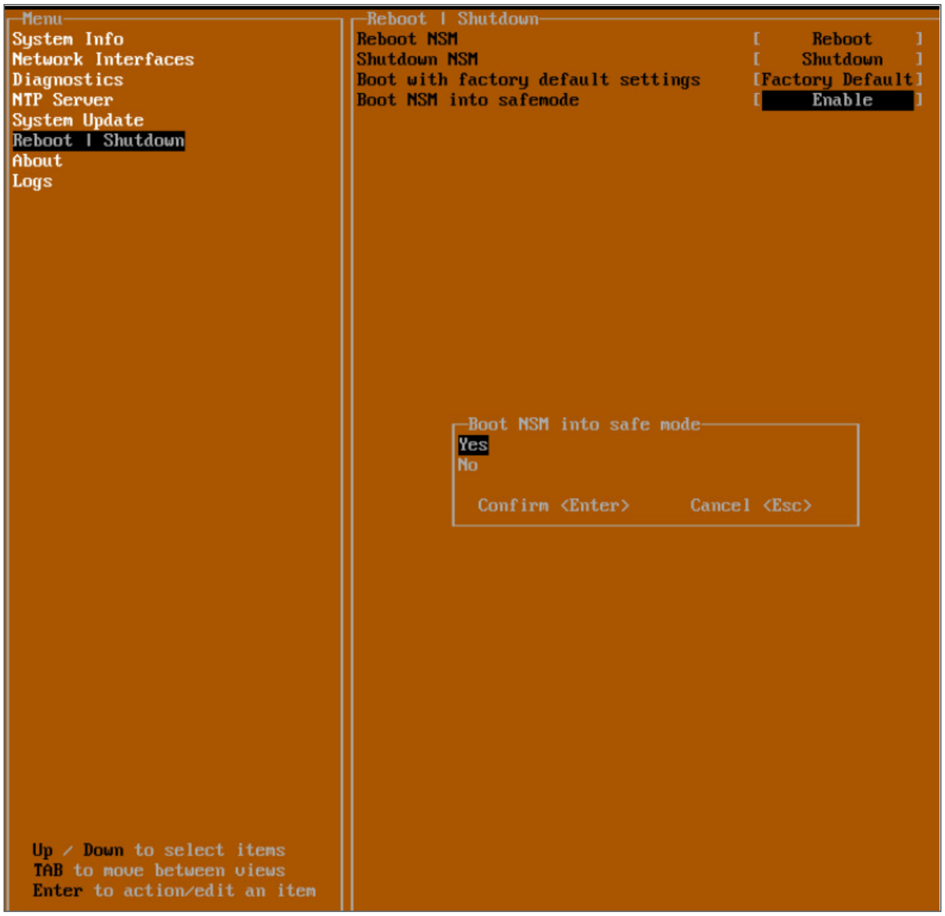
```
Jul 28 05:39:35 Finished running self-tests (Known Answer Tests)
Jul 28 05:39:35 TLS 1.3 KDF test passed
Jul 28 05:39:35 TLS KDF test passed
Jul 28 05:39:35 SHA2-512 test passed
Jul 28 05:39:34 SHA2-384 test passed
Jul 28 05:39:34 SHA2-256 test passed
Jul 28 05:39:33 SHA-1 test passed
Jul 28 05:39:32 RSA Verify test passed
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 Verify test passed
Jul 28 05:39:29 ECDSA Sign test passed
Jul 28 05:39:29 ECDSA PCT test passed
Jul 28 05:39:29 ECDH test passed
Jul 28 05:39:29 CTR DRBG test passed
Jul 28 05:39:29 AES GCM (Encrypt & Decrypt) test passed
Jul 28 05:39:29 AES CBC (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_client --status
Jul 28 05:34:21 /usr/bin/update_engine_client --status
Jul 28 05:34:21 MgmtCnsle: Management console has started
Jul 28 05:34:07 Start Verify Image

    Arrow keys: 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.



```
Menu                              Reboot | Shutdown
System Info                       Reboot NSM                          [    Reboot     ]
Network Interfaces                Shutdown NSM                        [   Shutdown    ]
Diagnostics                       Boot with factory default settings  [Factory Default]
NTP Server                        Boot NSM into safemode              [    Enable     ]
System Update
Reboot | Shutdown
About
Logs

                                            Boot NSM into safe mode
                                            Yes
                                            No

                                              Confirm <Enter>      Cancel <Esc>

  Up / Down to select items
  TAB to move between views
  Enter to action/edit an item
```

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**.

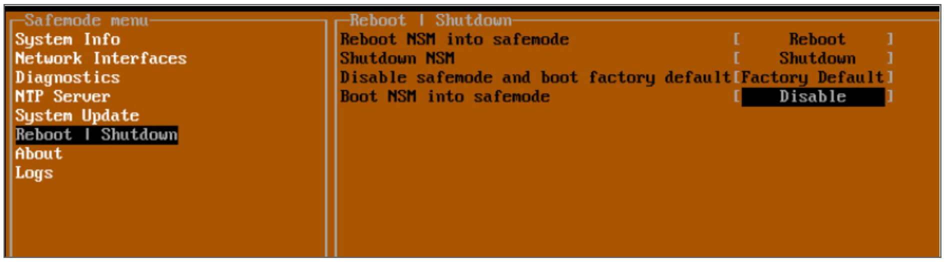
The NSM On-Premises instance immediately reboots and comes back up in SafeMode.

ⓘ | **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**.



```
Safemode menu                    Reboot | Shutdown
System Info                      Reboot NSM into safemode                  [     Reboot     ]
Network Interfaces               Shutdown NSM                              [    Shutdown    ]
Diagnostics                      Disable safemode and boot factory default[Factory Default]
NTP Server                       Boot NSM into safemode                    [    Disable     ]
System Update
Reboot | Shutdown
About
Logs
```

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.

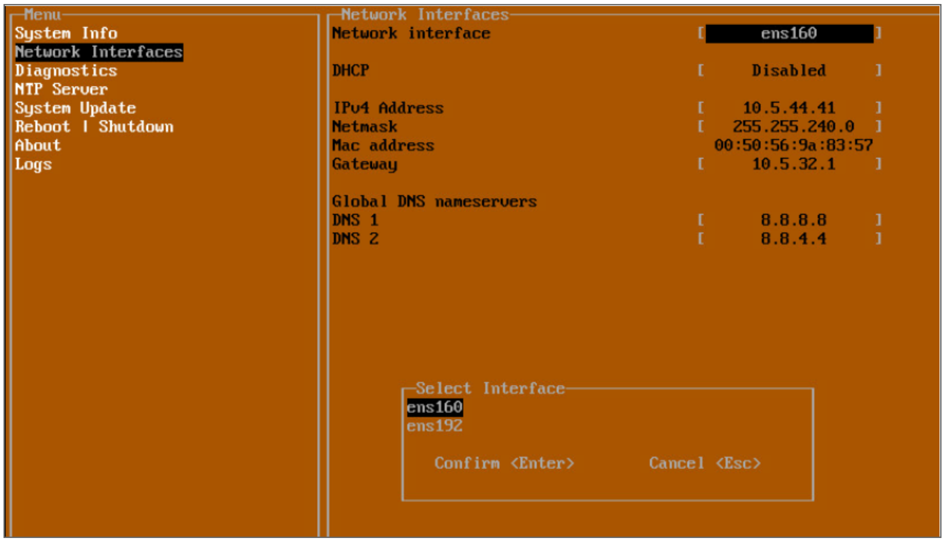
- **DHCP** – Determines whether addressing is static or handled automatically and dynamically by a DHCP server.
- **IPv4 Address** – The current IPv4 address currently assigned to the Management Interface.
- **Netmask** – The current Netmask assigned to the Management Interface.
- **Mac Address** – The 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.



```
Menu                    Network Interfaces
System Info             Network interface                        [     ens160     ]
Network Interfaces
Diagnostics             DHCP                                     [    Disabled    ]
NTP Server
System Update           IPv4 Address                             [   10.5.44.41   ]
Reboot | Shutdown       Netmask                                  [  255.255.240.0 ]
About                   Mac address                               00:50:56:9a:83:57
Logs                    Gateway                                  [   10.5.32.1    ]

                        Global DNS nameservers
                        DNS 1                                    [    8.8.8.8     ]
                        DNS 2                                    [    8.8.4.4     ]

                                Select Interface
                                ens160
                                ens192

                                   Confirm <Enter>         Cancel <Esc>
```

To edit an interface:

1. 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.

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

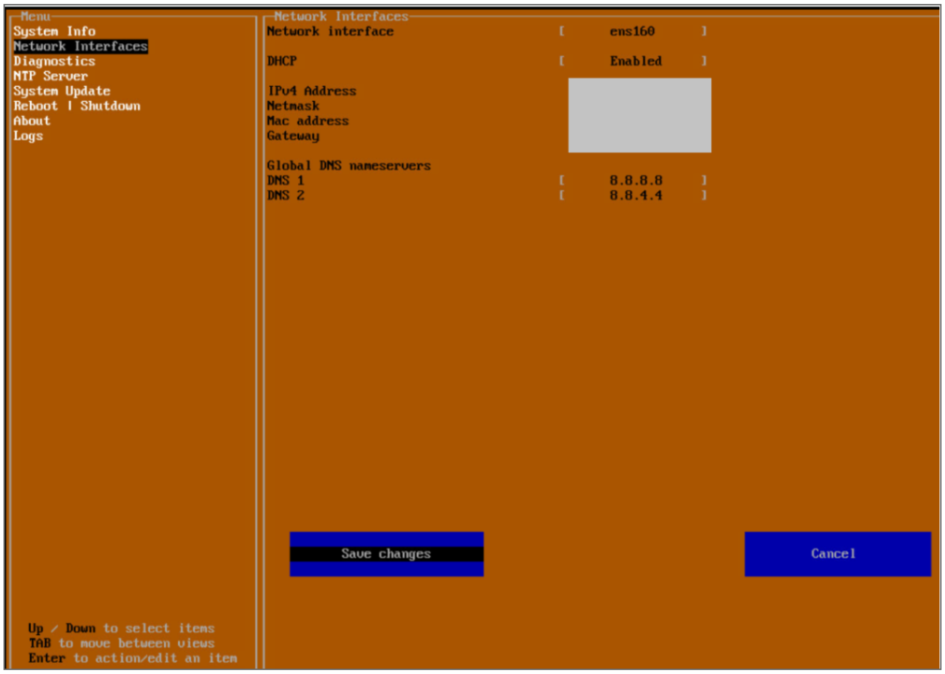
   The IPv4 and IPv6 addresses, Netmask, MAC address, Gateway, and DNS settings are displayed on the screen above the interface selection dialog.

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

   The on-screen dialog displays the current IP address.

4. Navigate into the dialog and make the desired changes, then press **Enter** to close the dialog or press **Esc** to cancel and close the dialog.

5. Two new buttons appear on the screen after you make changes to an interface setting: **Save changes** and **Cancel**. You can use the **Tab** key to navigate to these buttons.



```
Network interface          [      ens160      ]

DHCP                       [      Enabled     ]

IPv4 Address               [redacted]
Netmask
Mac address
Gateway

Global DNS nameservers
DNS 1                      [      8.8.8.8     ]
DNS 2                      [      8.8.4.4     ]
```

```
Up / Down to select items
TAB to move between views
Enter to action/edit an item
```

ⓘ **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

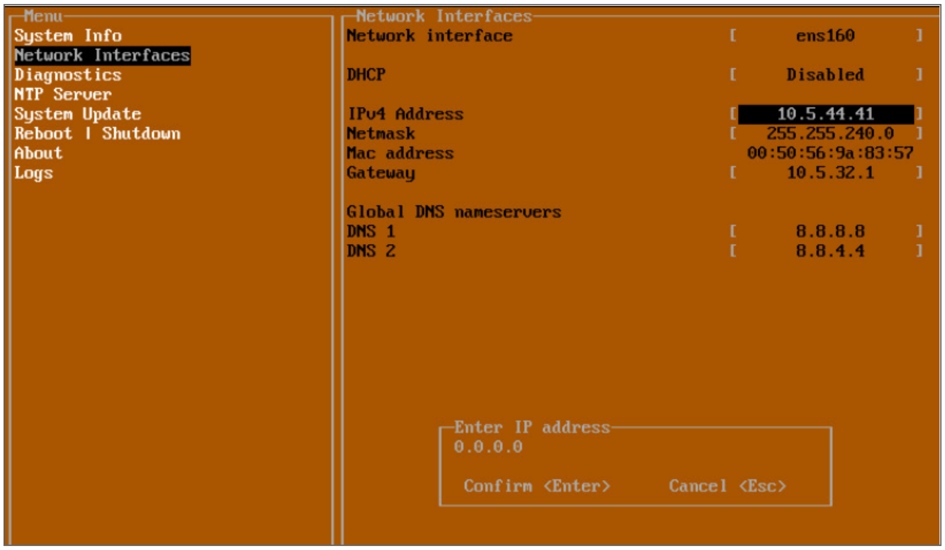
You can disable an interface while in SafeMode.

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**.

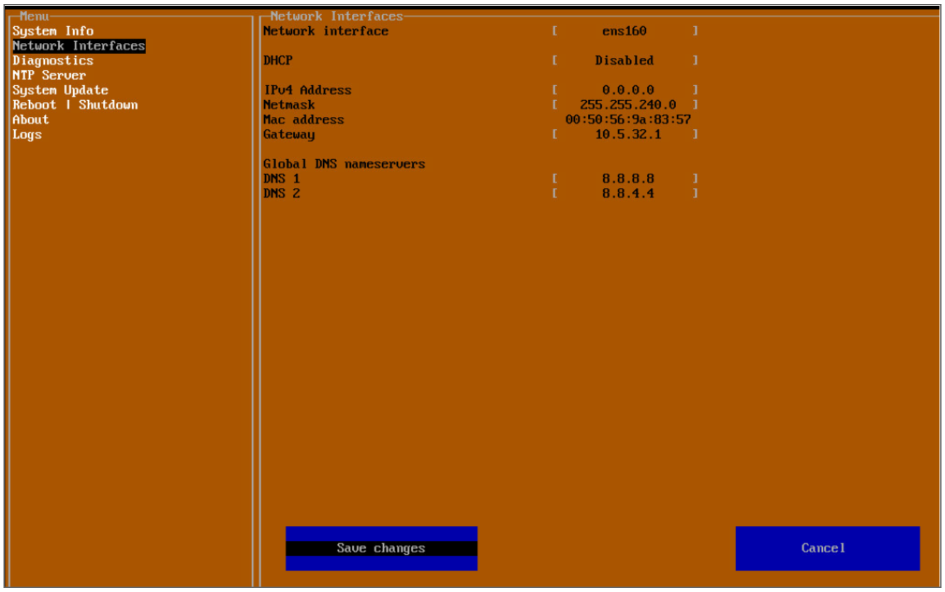
   The IPv4 and IPv6 addresses, Netmask, MAC address, Gateway, and DNS settings are displayed on the screen above the interface selection dialog.
3. For example, select **IPv4 Address** and press **Enter**.

   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**.



```
Network Interfaces
Network interface                     [      ens160       ]

DHCP                                  [     Disabled      ]

IPv4 Address                          [    10.5.44.41     ]
Netmask                               [   255.255.240.0   ]
Mac address                             00:50:56:9a:83:57
Gateway                               [     10.5.32.1     ]

Global DNS nameservers
DNS 1                                 [      8.8.8.8      ]
DNS 2                                 [      8.8.4.4      ]

          Enter IP address
          0.0.0.0
```

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



```
Network interface          [      ens160      ]

DHCP                       [     Disabled     ]

IPv4 Address               [      0.0.0.0     ]
Netmask                    [   255.255.240.0  ]
Mac address                 00:50:56:9a:83:57
Gateway                    [     10.5.32.1    ]

Global DNS nameservers
DNS 1                      [      8.8.8.8     ]
DNS 2                      [      8.8.4.4     ]
```

6. The interface is disabled.

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

Installing a Software Upgrade in SafeMode

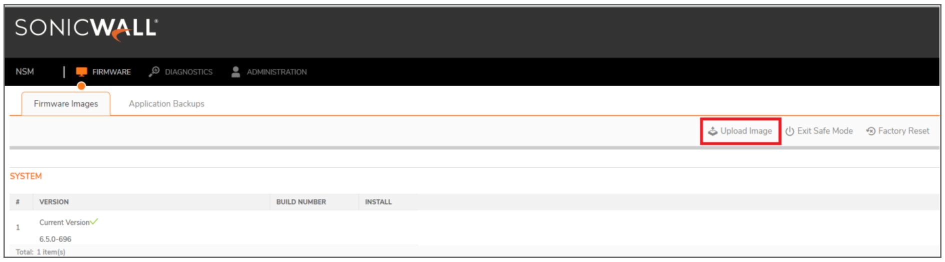
SWI files are used to upgrade NSM On-Premises. You can download the latest SWI image file from MySonicWall.

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.

ⓘ | **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.

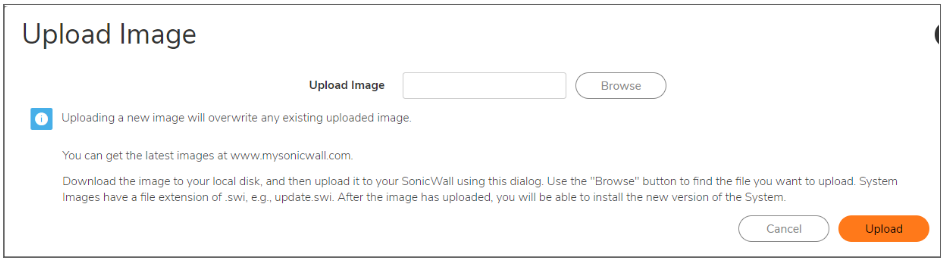


SYSTEM

#	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.



Uploading a new image will overwrite any existing uploaded image.

You can get the latest images at www.mysonicwall.com.

Download the image to your local disk, and then upload it to your SonicWall using this dialog. Use the "Browse" button to find the file you want to upload. System Images have a file extension of .swi, e.g., update.swi. After the image has uploaded, you will be able to install the new version of the System.

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.

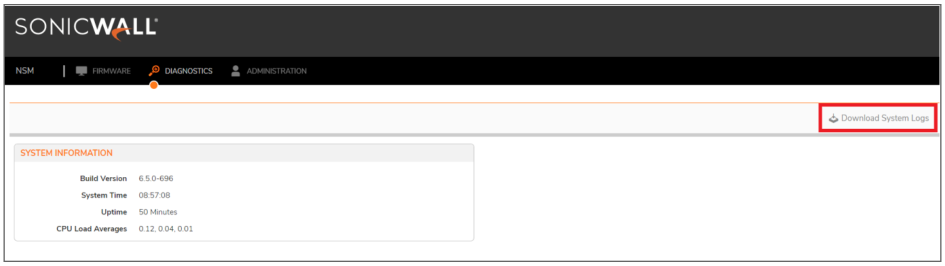
Downloading Logs in SafeMode

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.



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.

9

Using NSM

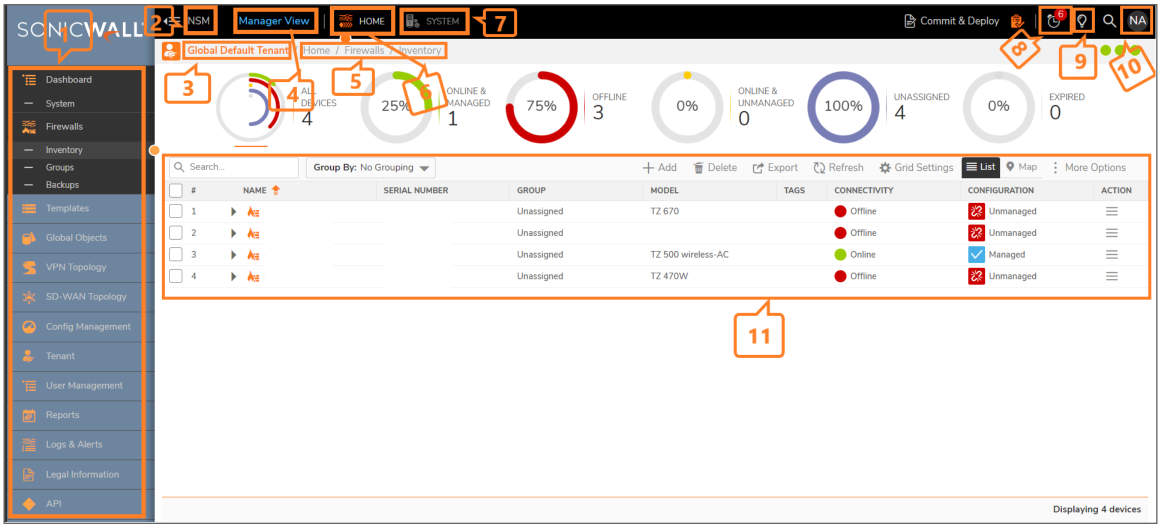
Once your NSM instance is operational, you can begin setting it up to manage your network. The instructions provided here are intended to help you get started, but for more detailed information refer to the *Network Security Manager Administration Guide* which is available at the Technical Documentation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



□	#	NAME	SERIAL NUMBER	GROUP	MODEL	TAGS	CONNECTIVITY	CONFIGURATION	ACTION
□	1			Unassigned	TZ 670		● Offline	Unmanaged	☰
□	2			Unassigned			● Offline	Unmanaged	☰
□	3			Unassigned	TZ 500 wireless-AC		● Online	✓ Managed	☰
□	4			Unassigned	TZ 470W		● Offline	Unmanaged	☰

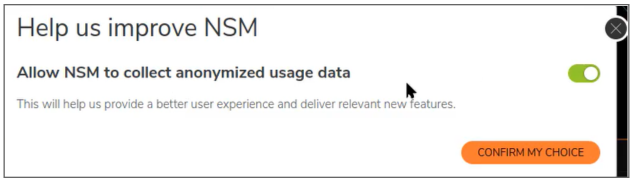
Reference	Interface Item	Description
1	Left command menu	Displays the primary tasks and commands that can be selected. The command menu varies depending upon which view you are in and the command option you have selected.
2	Show/hide commands icon	Acts as a switch to show or hide the left command menu. 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.

ⓘ **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 .

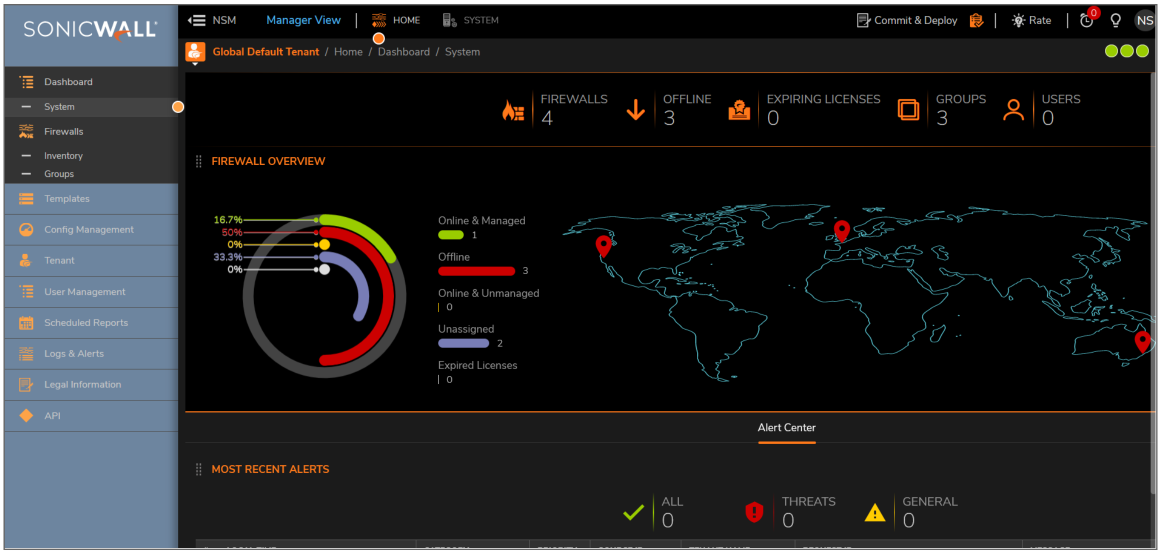
ⓘ **NOTE:** When user logs in for the first time, a pop-up displays to enable/disable the **Allow NSM to collect anonymized usage data** to help improve the NSM. The pop-up continues to display till the action is performed once.



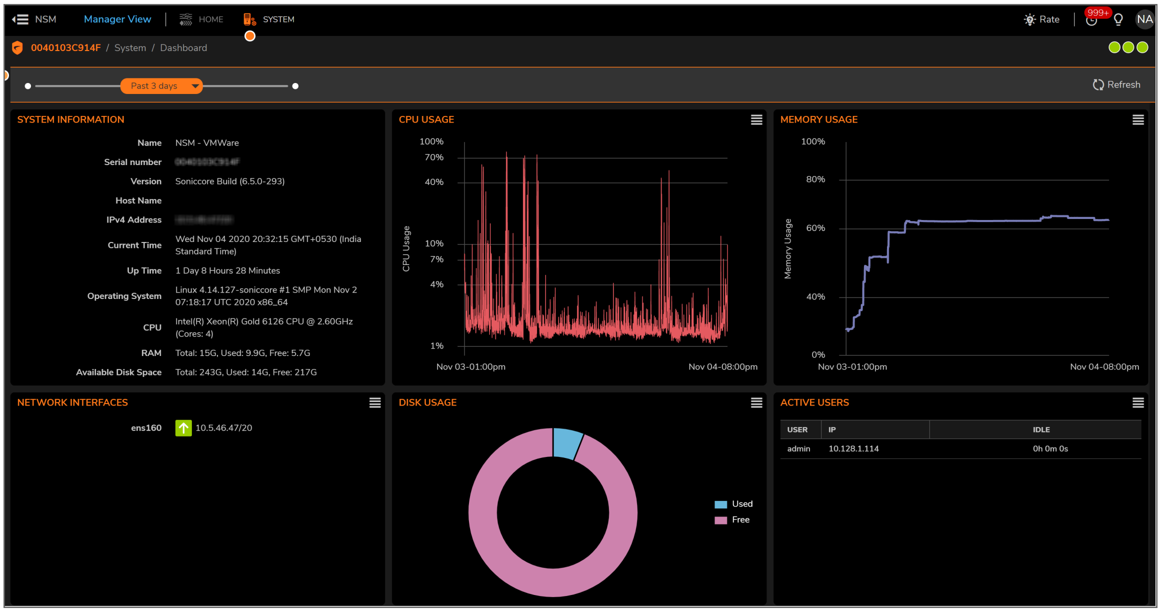
Help us improve NSM

Allow NSM to collect anonymized usage data

This will help us provide a better user experience and deliver relevant new features.



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:



SYSTEM INFORMATION

Name	NSM - VMWare
Serial number	[redacted]
Version	Soniccore Build (6.5.0-293)
Host Name	
IPv4 Address	[redacted]
Current Time	Wed Nov 04 2020 20:32:15 GMT+0530 (India Standard Time)
Up Time	1 Day 8 Hours 28 Minutes
Operating System	Linux 4.14.127-soniccore #1 SMP Mon Nov 2 07:18:17 UTC 2020 x86_64
CPU	Intel(R) Xeon(R) Gold 6126 CPU @ 2.60GHz (Cores: 4)
RAM	Total: 15G, Used: 9.9G, Free: 5.7G
Available Disk Space	Total: 243G, Used: 14G, Free: 217G

NETWORK INTERFACES

ens160	10.5.46.47/20

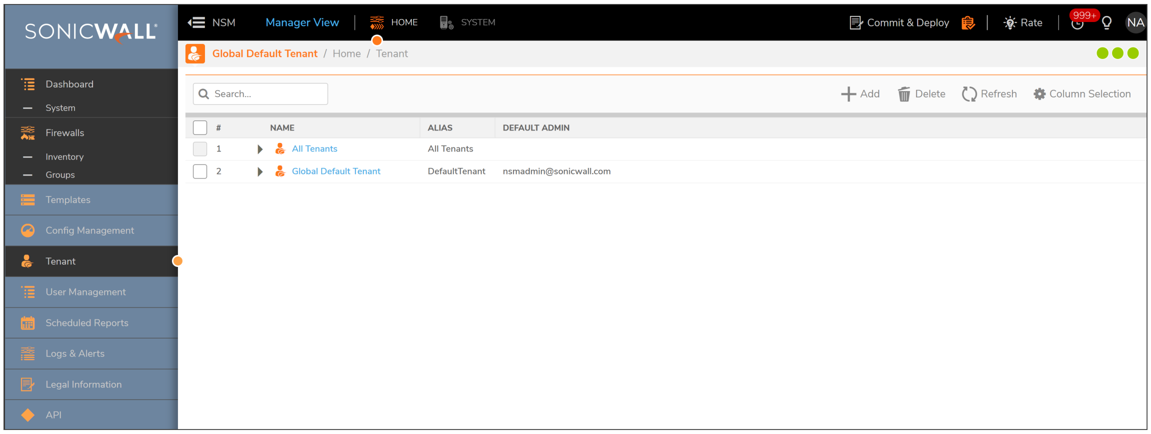
ACTIVE USERS

USER	IP	IDLE
admin	10.128.1.114	0h 0m 0s

Creating a Tenant

To create a tenant on NSM:

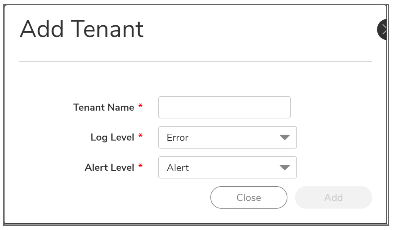
1. In **Home** view, click **Tenant**.



#	NAME	ALIAS	DEFAULT ADMIN
1	All Tenants	All Tenants	
2	Global Default Tenant	DefaultTenant	nsmadmin@sonicwall.com

2. Click **Add** icon.

3. In the **Add Tenant** window, enter **Tenant Name**, and select **Log Level** and **Alert Level**.



Tenant Name *	
Log Level *	Error
Alert Level *	Alert

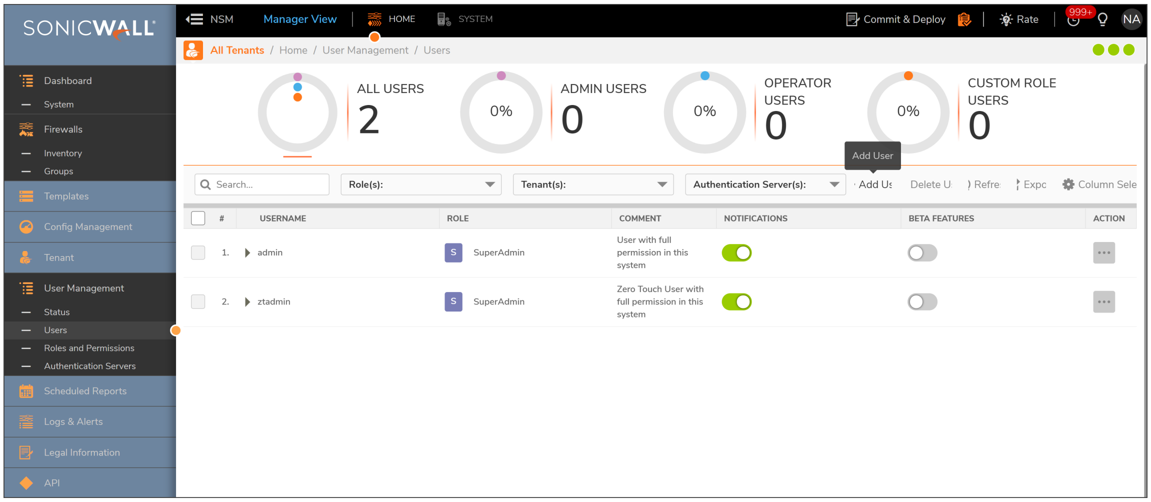
4. Click **Add**.

5. Register devices under the tenant.

Creating a New User

To create users:

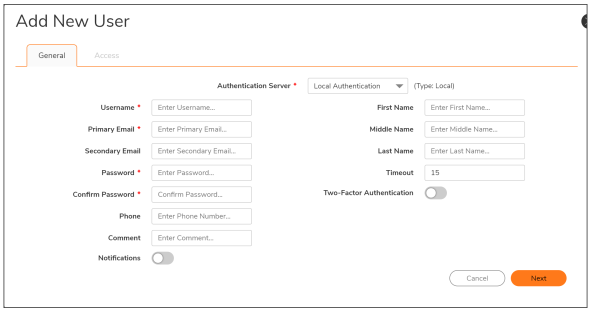
1. In **Home** view, navigate to **User Management > Users**.



#	USERNAME	ROLE	COMMENT	NOTIFICATIONS	BETA FEATURES	ACTION
1.	admin	S SuperAdmin	User with full permission in this system	●	○	···
2.	ztadmin	S SuperAdmin	Zero Touch User with full permission in this system	●	○	···

2. Click **Add User**.

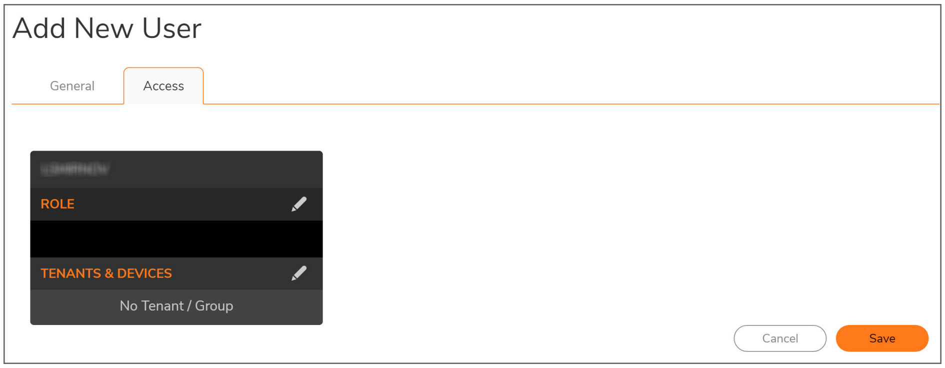
3. In the **Add New User** window, enter details of the new user.



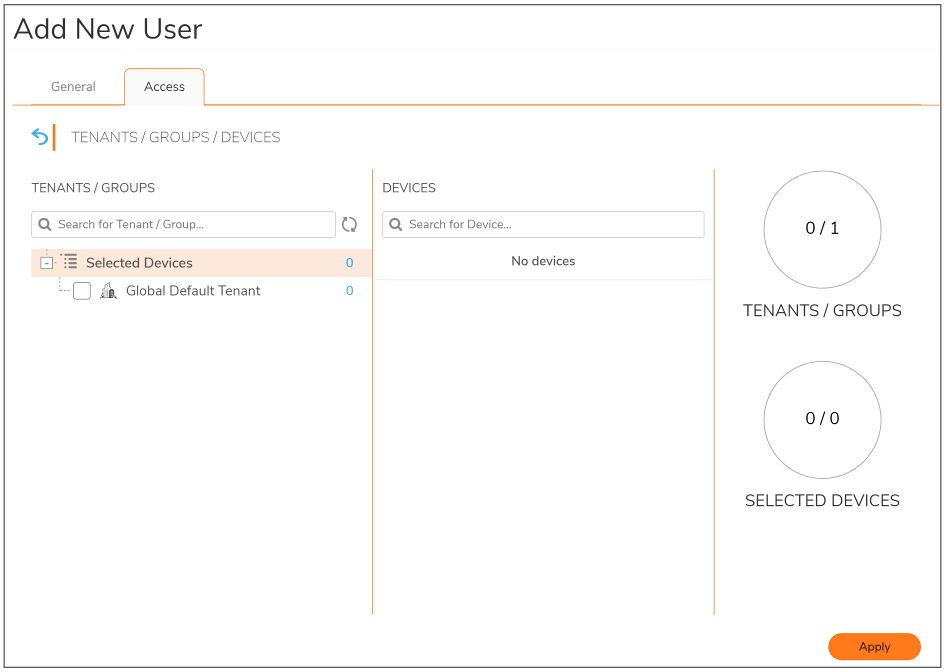
Authentication Server * Local Authentication (Type: Local)

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	○		

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



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**.

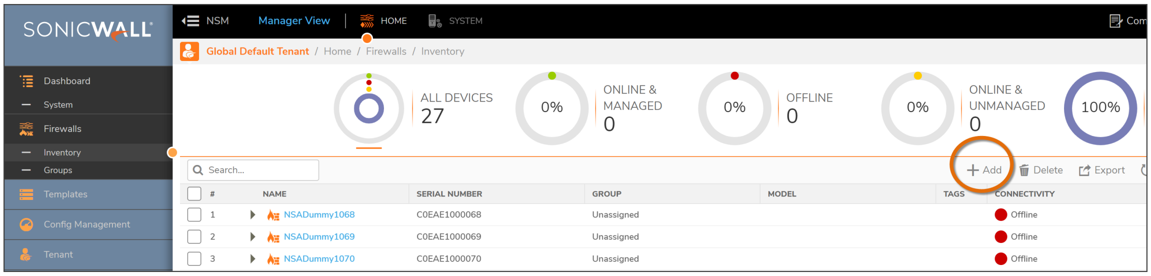


9. Select **TENANTS/GROUPS** and **DEVICES** from the options provided.
10. Click **Apply**.

Adding a Device

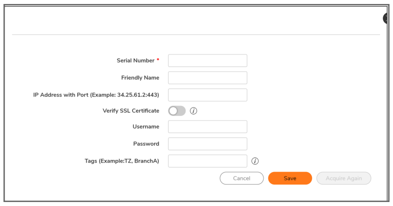
To add a device to firewall inventory:

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



□	#	NAME	SERIAL NUMBER	GROUP	MODEL	TAGS	CONNECTIVITY
□	1	NSADummy1068	C0EAE1000068	Unassigned			● Offline
□	2	NSADummy1069	C0EAE1000069	Unassigned			● Offline
□	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	○ ⓘ
Username	
Password	
Tags (Example:TZ, BranchA)	ⓘ

5. Click **Save.**

10

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

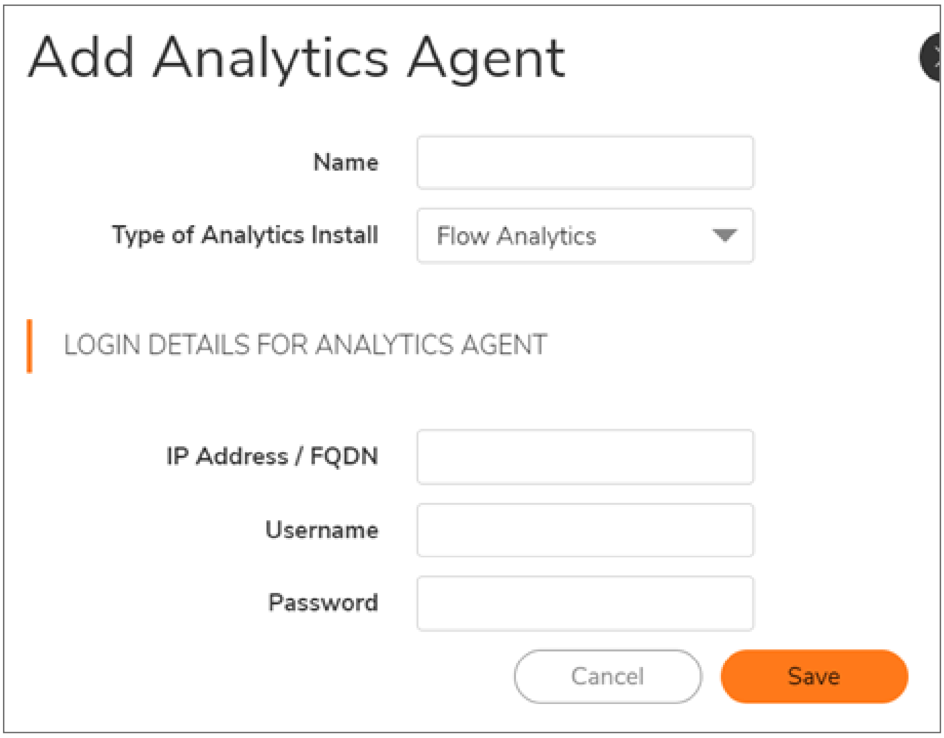
ⓘ **NOTE:** Before proceeding with NSM integration please ensure desired SonicWall Analytics is working fine and firewall is configured to send data to analytics.

- 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 ANALYTICS AGENT

IP Address / FQDN

Username

Password

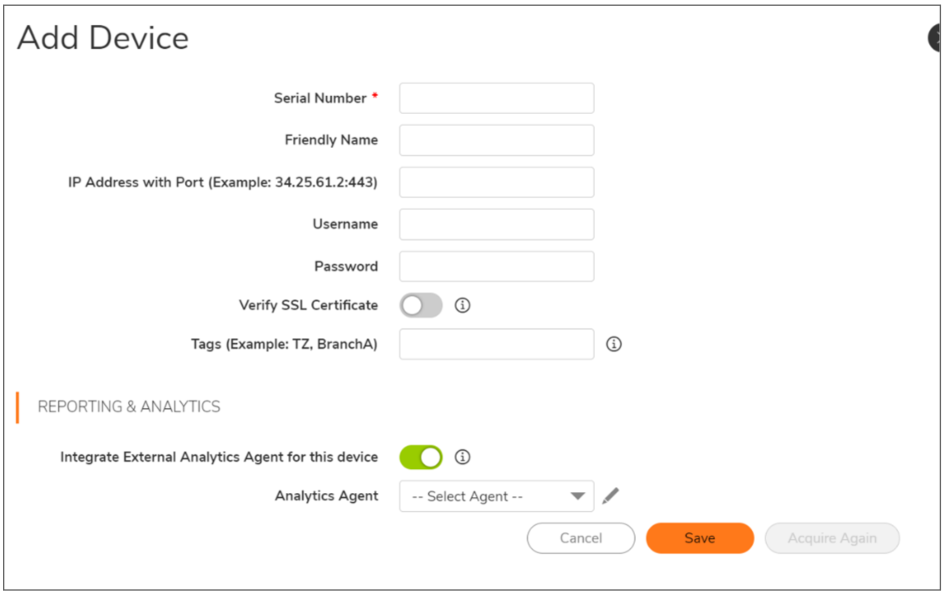
6. Click **Save**.

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.

> ⓘ **NOTE:** 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: off

Tags (Example: TZ, BranchA)

REPORTING & ANALYTICS

Integrate External Analytics Agent for this device: on

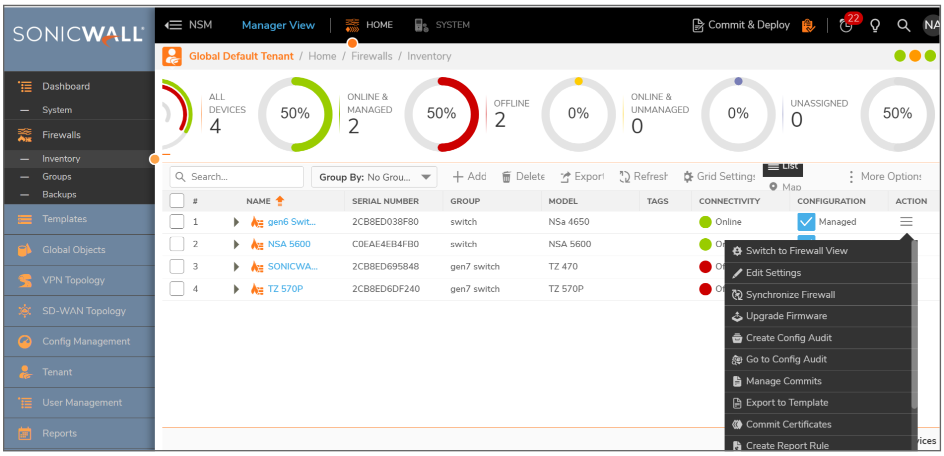
Analytics Agent: -- Select Agent --

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 icon below **Action** column and click on **Edit Settings**.



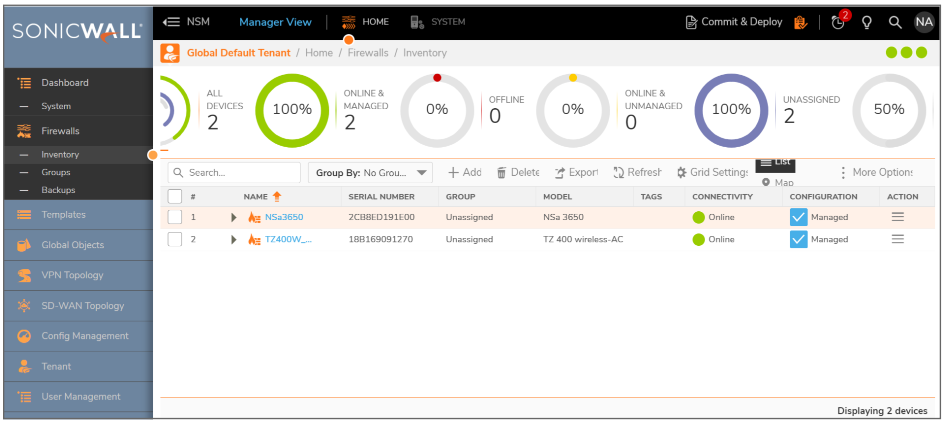
#	NAME	SERIAL NUMBER	GROUP	MODEL	TAGS	CONNECTIVITY	CONFIGURATION	ACTION
1	gen6 Swit...	2CB8ED038F80	switch	NSa 4650		Online	Managed	☰
2	NSA 5600	C0EAE4EB4FB0	switch	NSA 5600		On		
3	SONICWA...	2CB8ED695848	gen7 switch	TZ 470		Of		
4	TZ 570P	2CB8ED6DF240	gen7 switch	TZ 570P		Of		

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.



Global Default Tenant / Home / Firewalls / Inventory

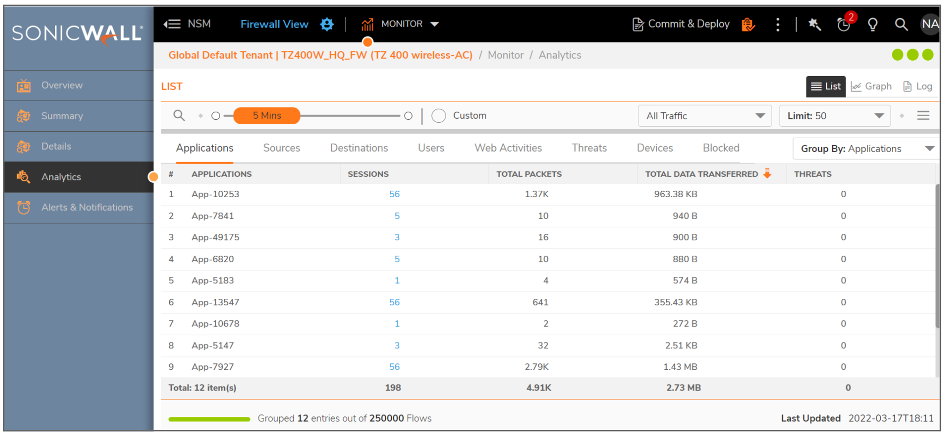
ALL DEVICES 2 — 100% — ONLINE & MANAGED 2 — 0% — OFFLINE 0 — 0% — ONLINE & UNMANAGED 0 — 100% — UNASSIGNED 2 — 50%

#	NAME	SERIAL NUMBER	GROUP	MODEL	TAGS	CONNECTIVITY	CONFIGURATION	ACTION
1	NSa3650	2CB8ED191E00	Unassigned	NSa 3650		● Online	☑ Managed	≡
2	TZ400W_...	18B169091270	Unassigned	TZ 400 wireless-AC		● Online	☑ Managed	≡

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**



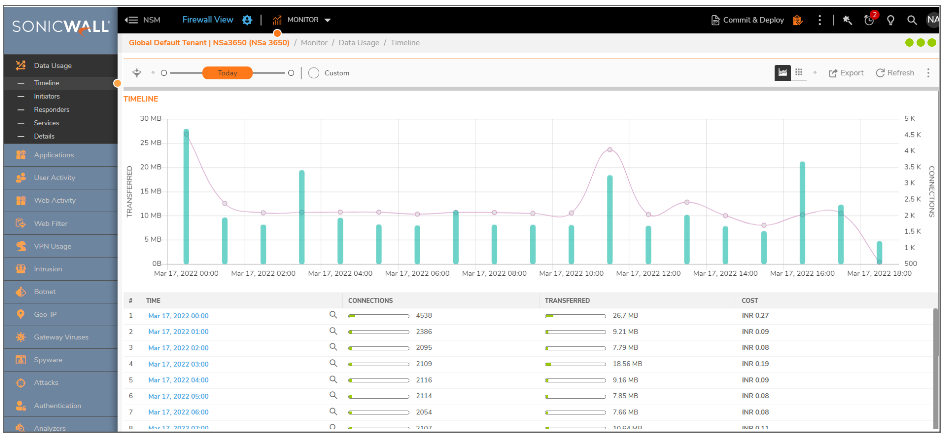
Global Default Tenant | TZ400W_HQ_FW (TZ 400 wireless-AC) / Monitor / Analytics

#	APPLICATIONS	SESSIONS	TOTAL PACKETS	TOTAL DATA TRANSFERRED	THREATS
1	App-10253	56	1.37K	963.38 KB	0
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**



#	TIME	CONNECTIONS	TRANSFERRED	COST
1	Mar 17, 2022 00:00	4538	26.7 MB	INR 0.27
2	Mar 17, 2022 01:00	2386	9.21 MB	INR 0.09
3	Mar 17, 2022 02:00	2095	7.79 MB	INR 0.08
4	Mar 17, 2022 03:00	2109	18.56 MB	INR 0.19
5	Mar 17, 2022 04:00	2116	9.16 MB	INR 0.09
6	Mar 17, 2022 05:00	2114	7.85 MB	INR 0.08
7	Mar 17, 2022 06:00	2054	7.66 MB	INR 0.08
8	Mar 17, 2022 07:00	2107	10.64 MB	INR 0.11

11

Upgrade Instructions

This section describes more about the following topics:

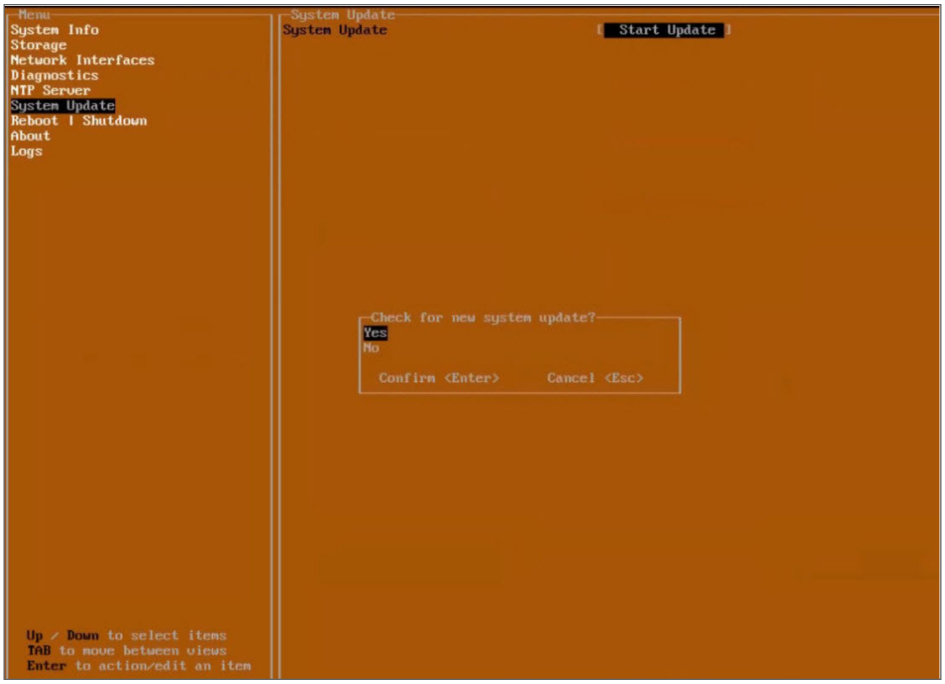
- Upgrade Using Management Console
- Upgrading SonicOS Firmware

ⓘ **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

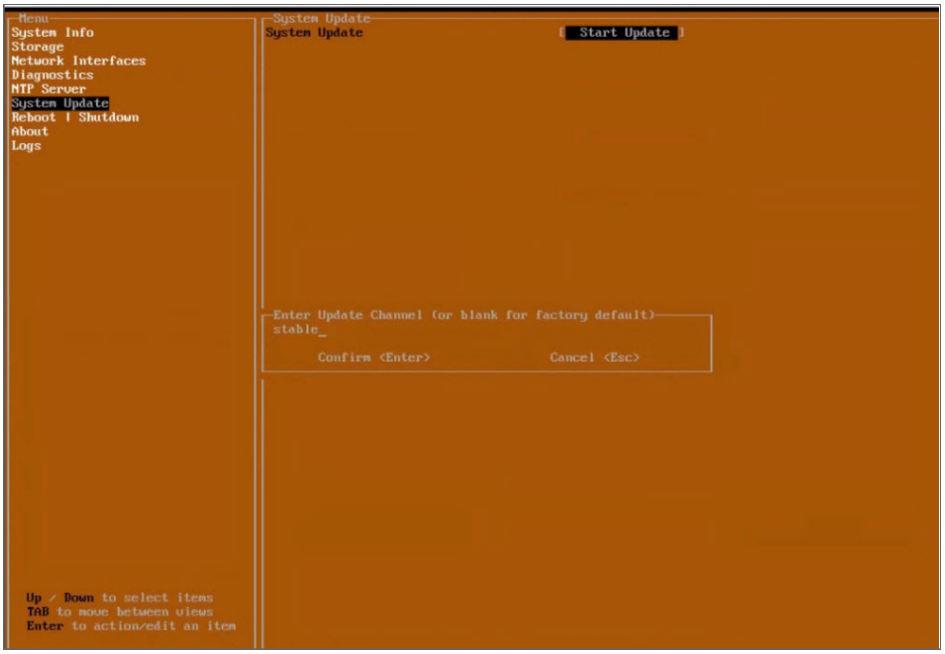
When upgrading from NSM 2.3.3 to NSM 2.3.4, the Firmware Settings page provides you a tool tip that directs you to upgrade using the NSM Management Console. The settings and configuration data is preserved across upgrades.

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                              System Update
System Info                       System Update                    [ Start Update ]
Storage
Network Interfaces
Diagnostics
NTP Server
System Update
Reboot | Shutdown
About
Logs

                                          Check for new system update?
                                          Yes
                                          No

                                           Confirm <Enter>       Cancel <Esc>

  Up / Down to select items
  TAB to move between views
  Enter to action/edit an item
```

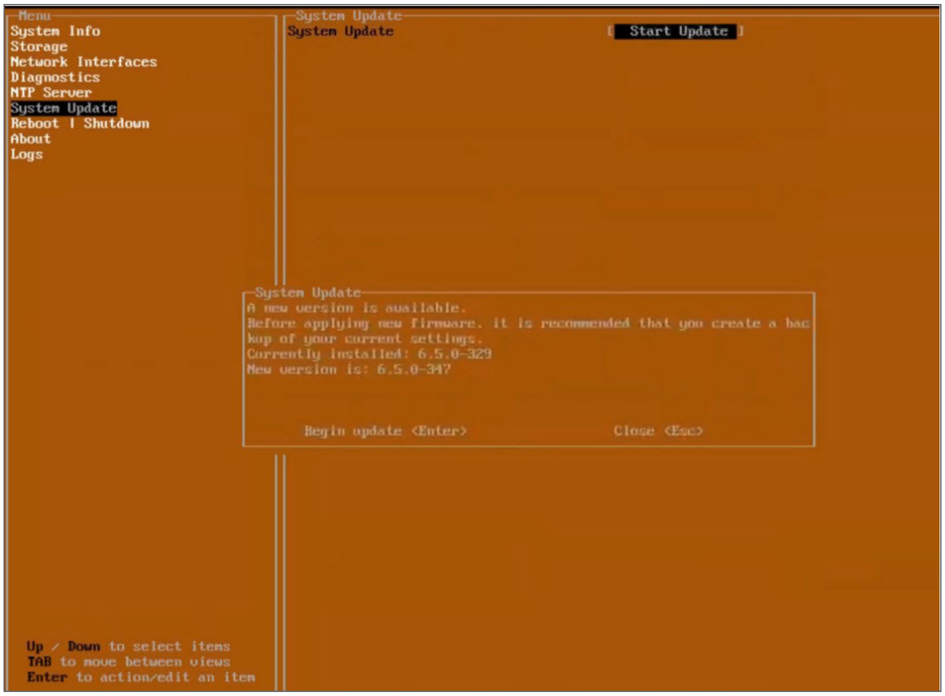
6. Press **Ctrl+P** to view or edit the update channel.



```
Menu                              System Update
System Info                       System Update                    [ Start Update ]
Storage
Network Interfaces
Diagnostics
NTP Server
System Update
Reboot | Shutdown
About
Logs

                                  Enter Update Channel (or blank for factory default)
                                  stable_
                                        Confirm <Enter>                Cancel <Esc>

  Up / Down to select items
  TAB to move between views
  Enter to action/edit an item
```

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

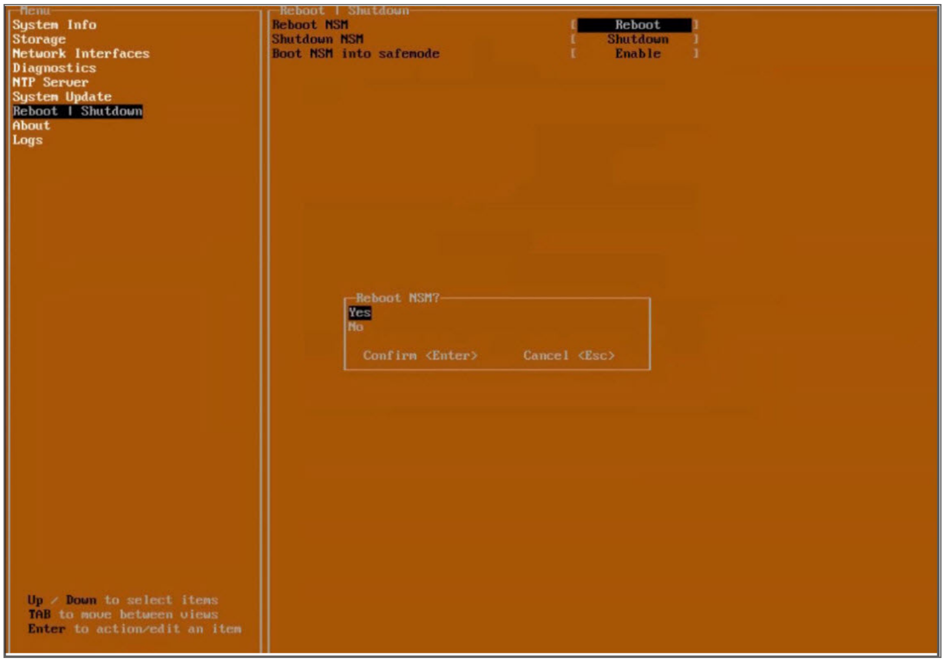
7. When the upgrade version is displayed, click **Enter** to begin the update. This downloads and installs the update. During this process, you can close the downloading window by tapping **Esc**.



```
Menu                              System Update
System Info                       System Update                     [ Start Update ]
Storage
Network Interfaces
Diagnostics
NTP Server
System Update
Reboot | Shutdown
About
Logs

                             System Update
                             A new version is available.
                             Before applying new firmware. it is recommended that you create a bac
                             kup of your current settings.
                             Currently installed: 6.5.0-329
                             New version is: 6.5.0-347


                                    Begin update <Enter>                    Close <Esc>

  Up / Down to select items
  TAB to move between views
  Enter to action/edit an item
```

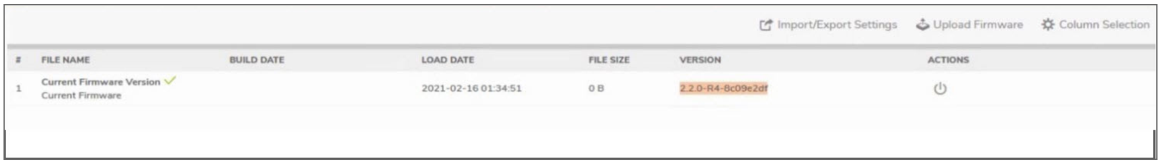
IMPORTANT: The NSM On-Premises VM is operational during update process.

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



```
Menu                             Reboot | Shutdown
System Info                      Reboot NSM                      [     Reboot     ]
Storage                          Shutdown NSM                    [    Shutdown    ]
Network Interfaces               Boot NSM into safemode          [     Enable     ]
Diagnostics
NTP Server
System Update
Reboot | Shutdown
About
Logs

                                         Reboot NSM?
                                         Yes
                                         No

                                           Confirm <Enter>       Cancel <Esc>

  Up / Down to select items
  TAB to move between views
  Enter to action/edit an item
```

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

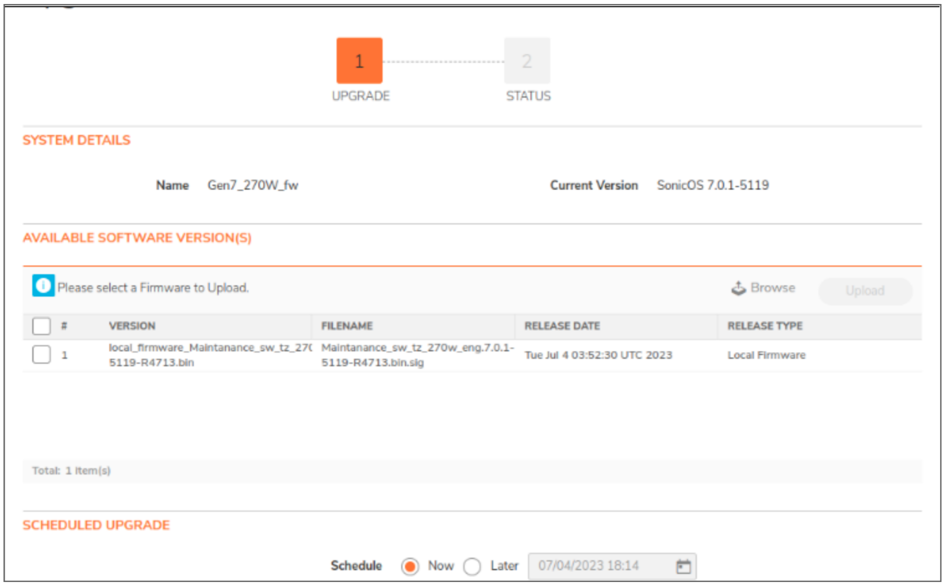


#	FILE NAME	BUILD DATE	LOAD DATE	FILE SIZE	VERSION	ACTIONS
1	Current Firmware Version ✓ Current Firmware		2021-02-16 01:34:51	0 B	2.2.0-R4-8c09e2df	

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.



SYSTEM DETAILS

Name Gen7_270W_fw

Current Version SonicOS 7.0.1-5119

AVAILABLE SOFTWARE VERSION(S)

Please select a Firmware to Upload.

□ #	VERSION	FILENAME	RELEASE DATE	RELEASE TYPE
□ 1	local_firmware_Maintanance_sw_tz_27(5119-R4713.bin	Maintanance_sw_tz_270w_eng.7.0.1- 5119-R4713.bin.sig	Tue Jul 4 03:52:30 UTC 2023	Local Firmware

Total: 1 Item(s)

SCHEDULED UPGRADE

Schedule ● Now ○ Later 07/04/2023 18:14

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.

The Support Portal enables you to:

- View Knowledge Base articles and Technical Documentation
- View and participate in the Community Forum discussions
- View Video Tutorials
- Access MySonicWall
- Learn about SonicWall Professional Services
- Review SonicWall Support services and warranty information
- Register at SonicWall University for training and certification

About This Document

Network Security Manager (On-Premises) Getting Started Guide
Updated - December 2024
232-005716-00 Rev J

Copyright © 2024 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