Network Security Manager

On-Premises Getting Started Guide

SONICWALL®

Contents

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.

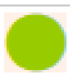
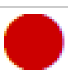
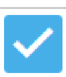
Conventions

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 associated firmware can be managed by Network Security Manager.

Firewall Model	SonicOS Version
SOHO W	6.5.4

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

System Requirements

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

Topics:

- Capacity Requirements
- Scaling Up
- Licensing Model

Capacity Requirements

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

Platform	Version	Number of Firewalls	Minimum Configuration
VMware	ESXi 6.7	1-500	4 core, 24 GB RAM
	ESXi 7.0	500-3000	8 core, 48 GB RAM
Hyper-V	Windows 2016	1-500	4 core, 24 GB RAM
		500-3000	8 core, 48 GB RAM
KVM	Linux Kernel 2.6.17 or above	1-500	4 core, 24 GB RAM
	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.	500-3000	8 core, 48 GB RAM

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

Scaling Up

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

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

Live Monitor	Monitors how NSM is behaving in real time
Process Monitor	Shows the processes running on the NSM system and the utilization associated with each
Service Monitor	Shows what services are running on the NSM system and the utilization associated with each
System Report	Displays the historical reports for CPU, memory, and disk utilization

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

Licensing Model

The licensing model is described below:

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

Creating an MSW Account

A MySonicWall account is required to register the NSM instance.

ⓘ | **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.

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:

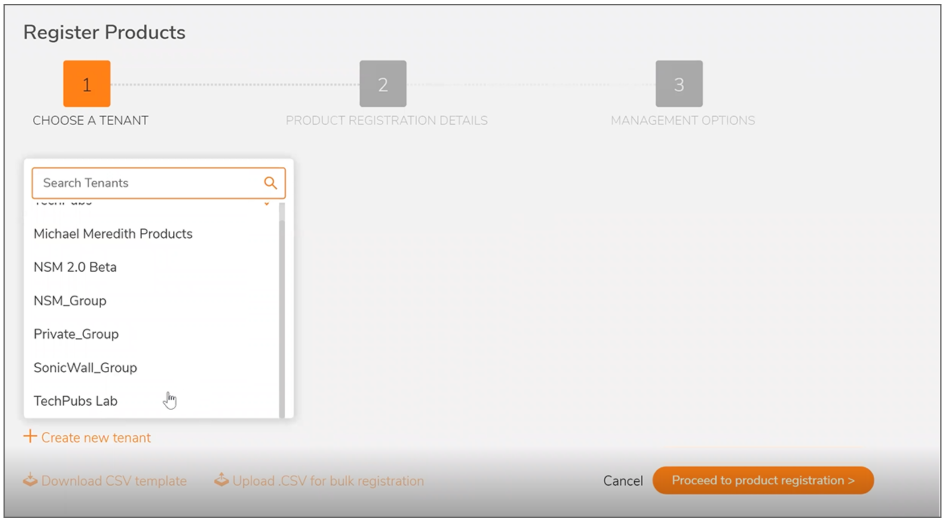
- Obtaining a New Licensed Image
- Obtaining a Trial Version
- Downloading NSM for an Existing Instance

Obtaining a New Licensed Image

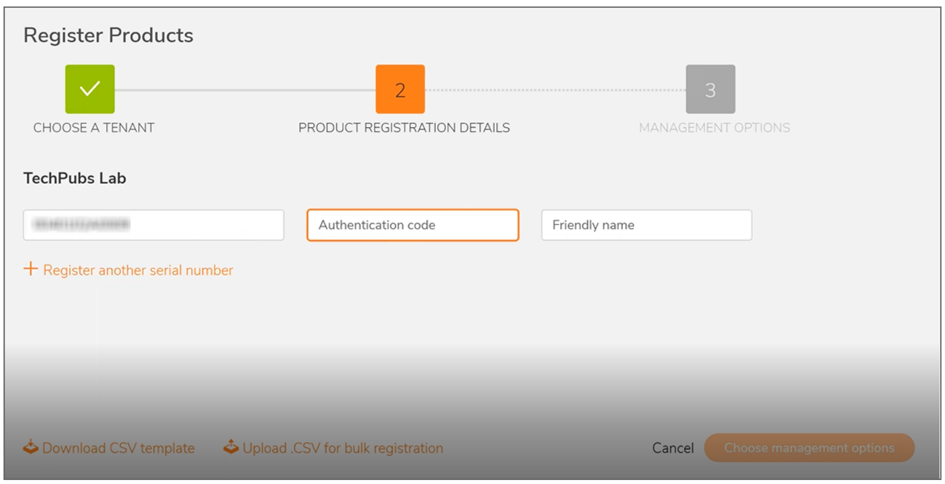
To download NSM for the first time, you need an Activation Key to access the image.

1. Log in to MySonicWall.

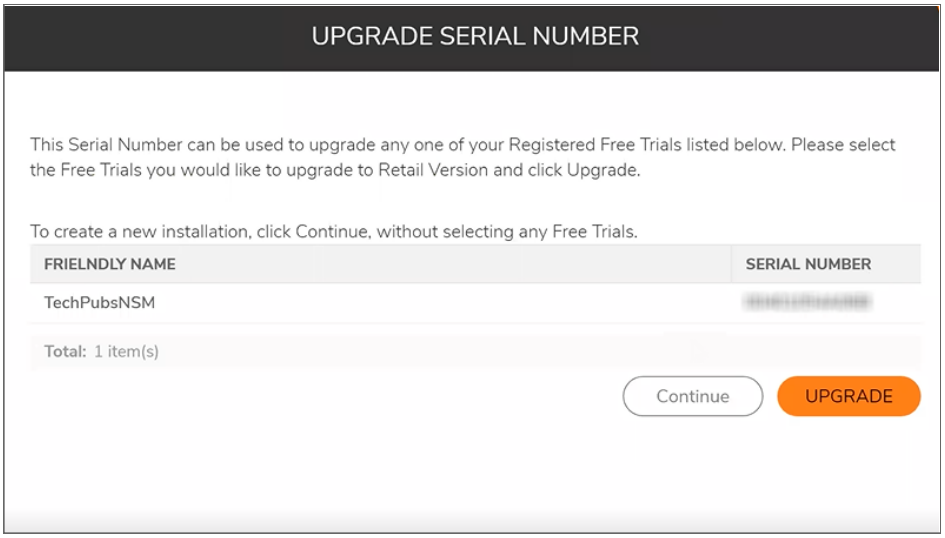
   ⓘ | **NOTE:** If you do not have a MySonicWall account, refer to Creating an MSW Account.
2. Navigate to **Product Management > My Products**.
3. Click **Register Products**.



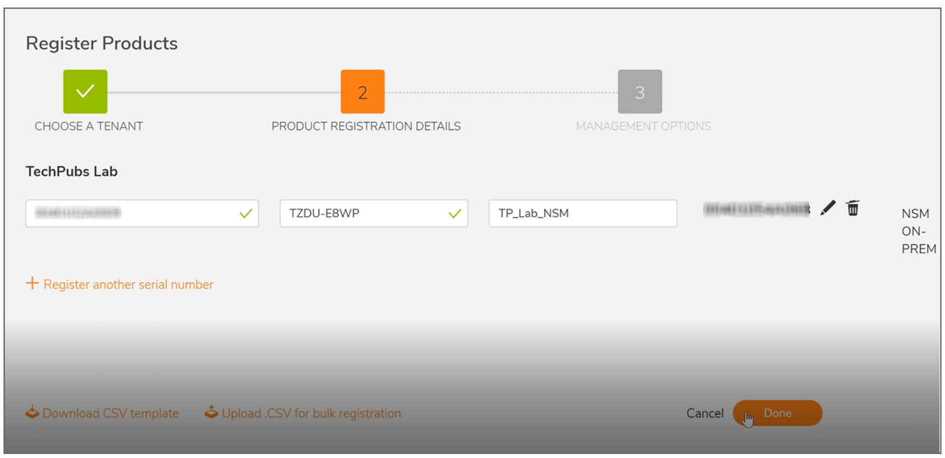
4. Choose a **Tenant**.



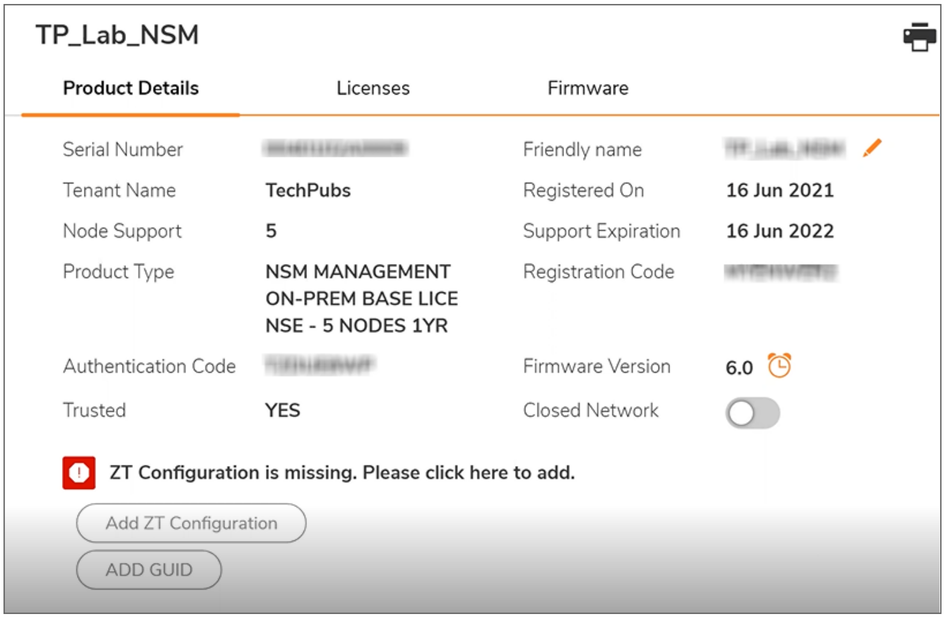
5. Specify the **Serial Number**, **Authentication Code**, and **Friendly Name**.
6. From the drop-down, select **Upgrade Serial Number**.



7. Click **Upgrade**.

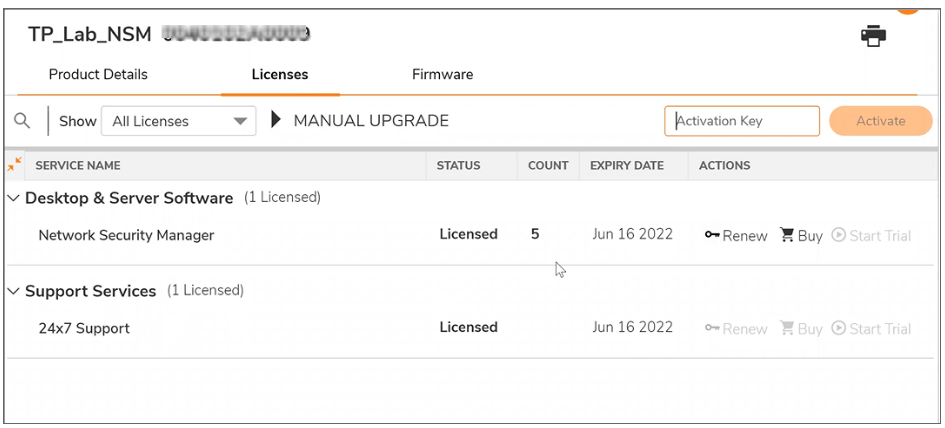


8. Verify the details and click **Done**. When the installation is complete, you can view the details further as given below.

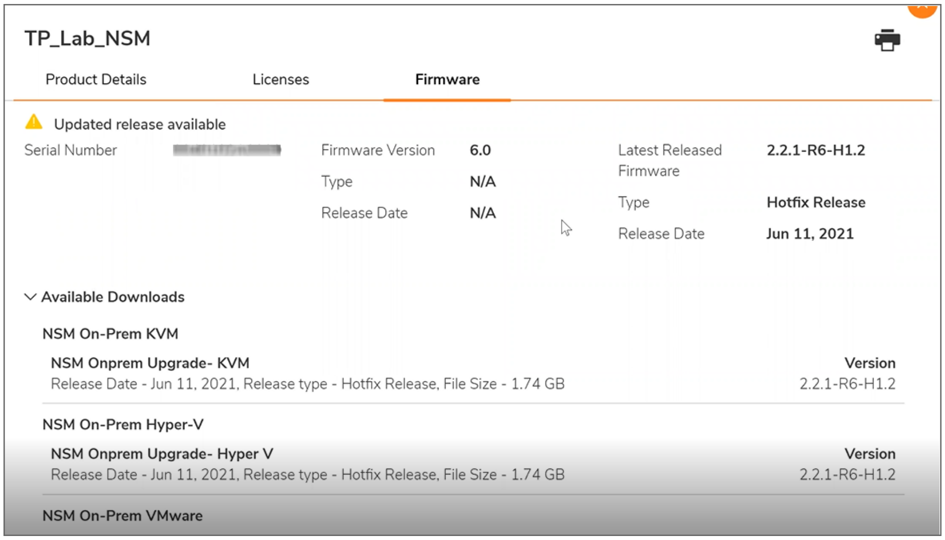


You have the option to add ZT configuration or you can do it later as required.

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



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



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

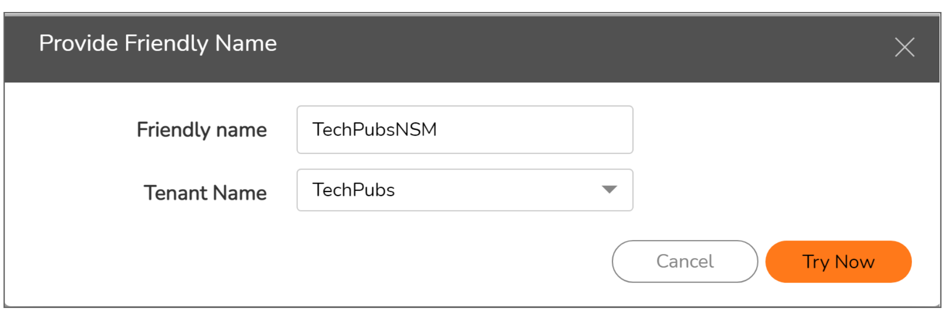
Obtaining a Trial Version

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**.

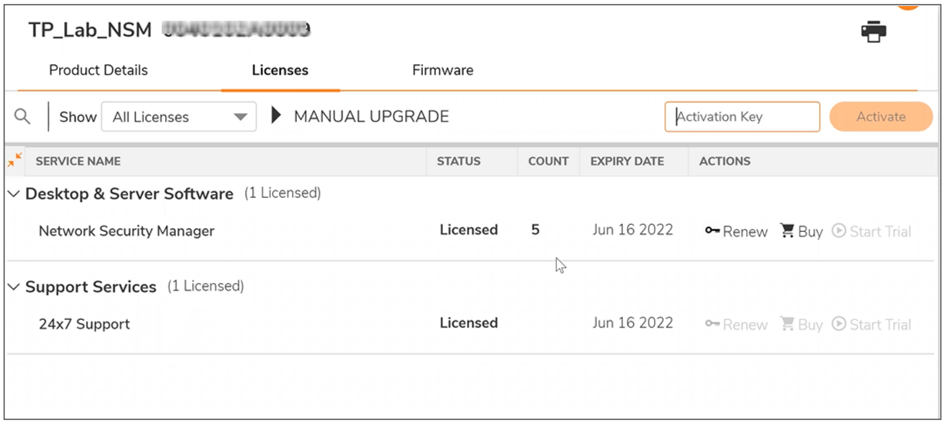


4. Enter a **Friendly Name**.
5. Select a **Tenant Name** from the drop-down list.
6. Click **Try Now**.

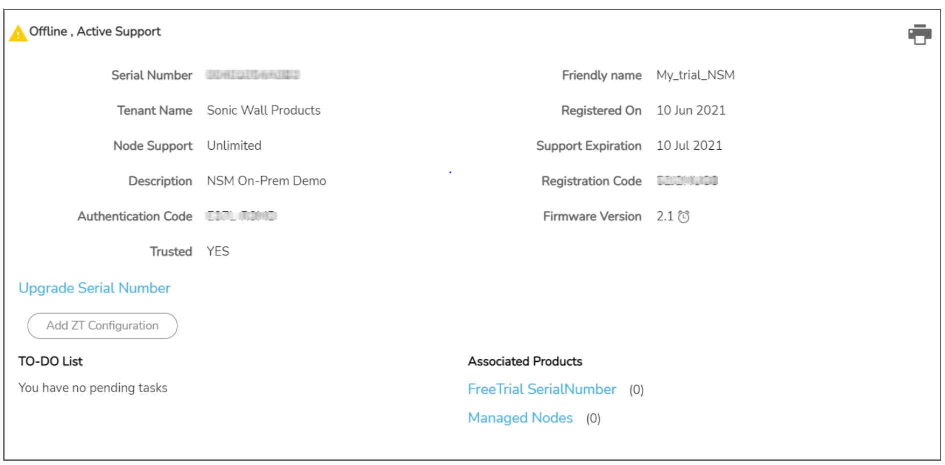
When you purchase NSM, you need to activate the license.

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**.



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



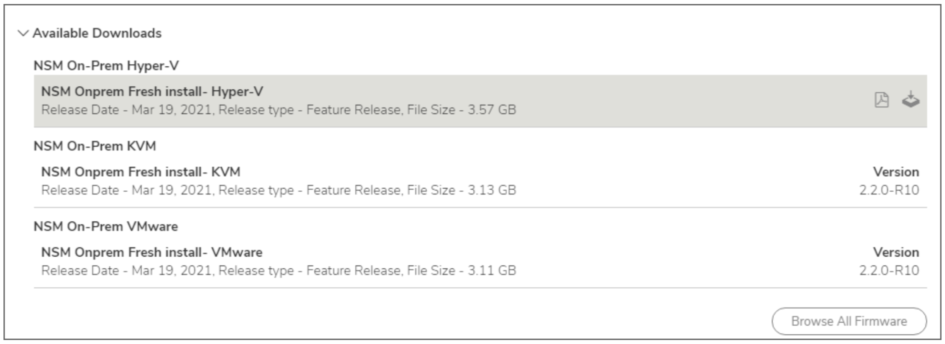
While in MySonicWall, you should download the NSM image for later installation.

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.



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

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.

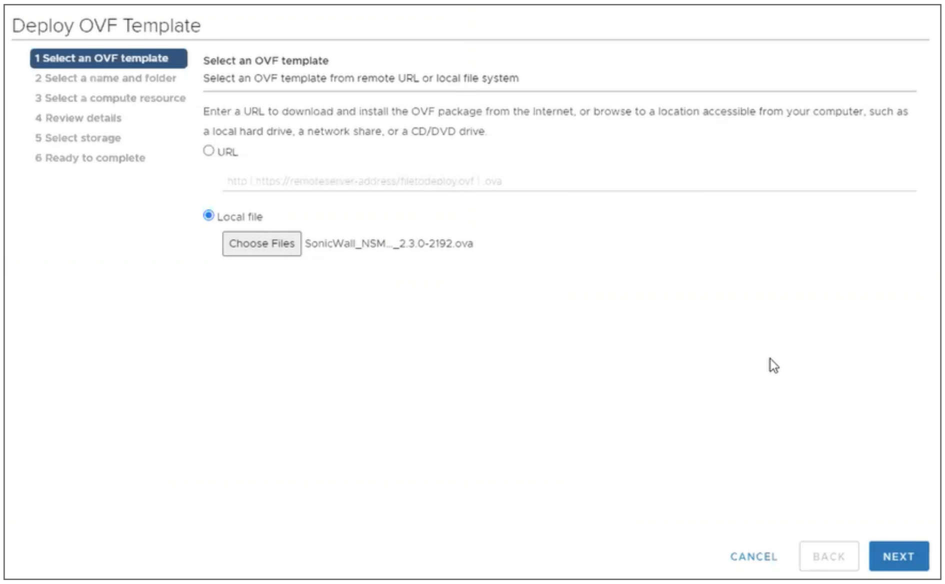
ⓘ | **NOTE:** The elements of VMware must already be in place and the administrator must be familiar with the basics of deploying a virtual appliance on the ESXi server.

To install NSM On-Premises on ESXi server:

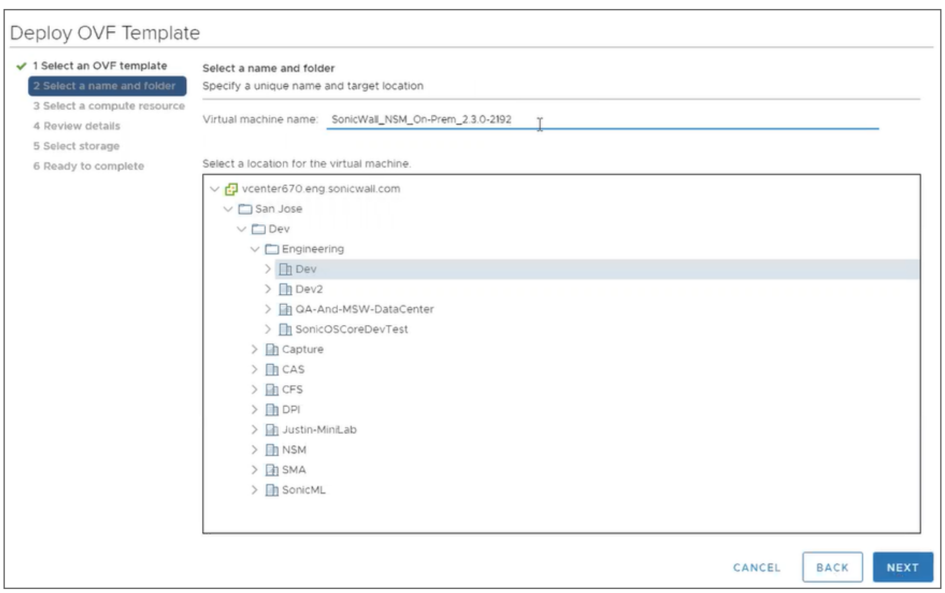
1. Access vSphere and log in to your ESXi server.

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

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

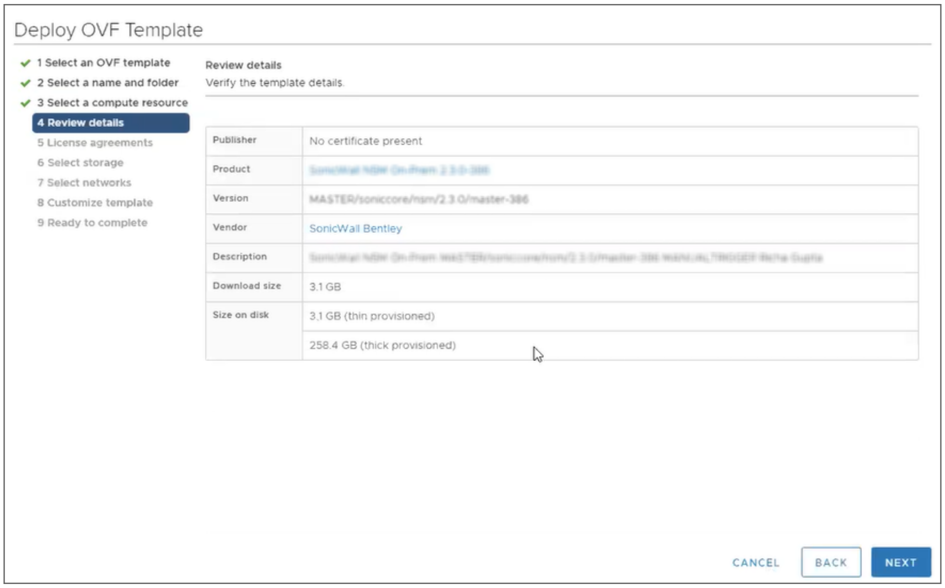


3. Select **Local file** and click on **Choose Files**.
4. Navigate to where you stored the NSM OVA file to select it.
5. Click **Open**.
6. On the wizard, click **Next**.
7. Specify the **Virtual machine name** for the NSMOn-Premises instance. Be sure it's a meaningful name so you can easily find it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



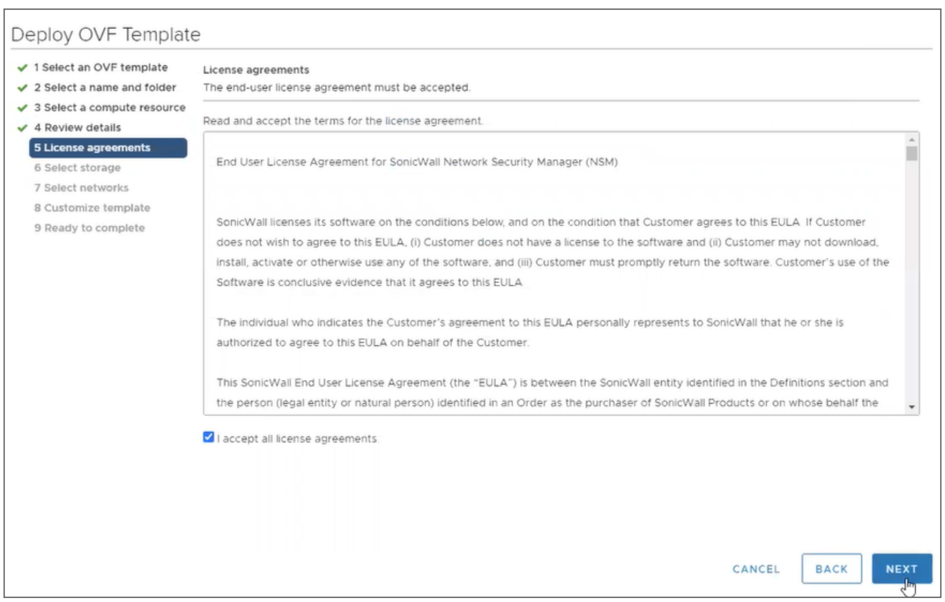
8. Select the location for the virtual machine and click **Next**.

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.**

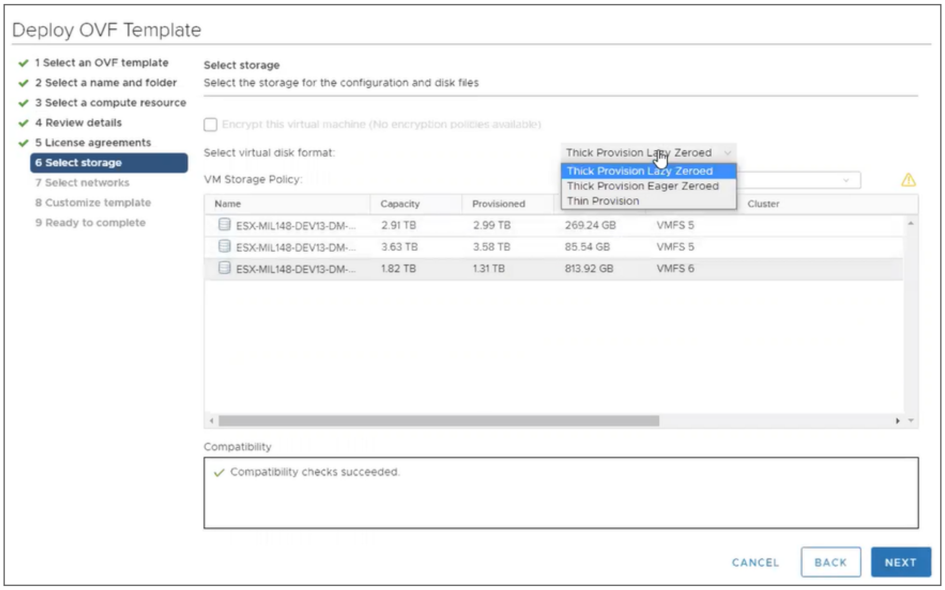


ⓘ | **NOTE:** The details you see on this screen are specific to your deployment.

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



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

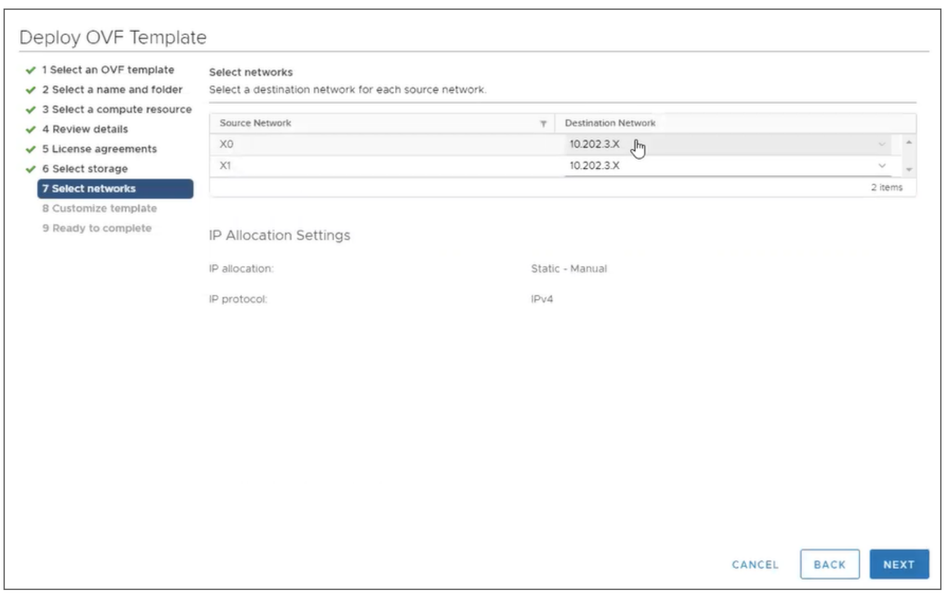


14. Select a data store from the table and click **Next**.

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

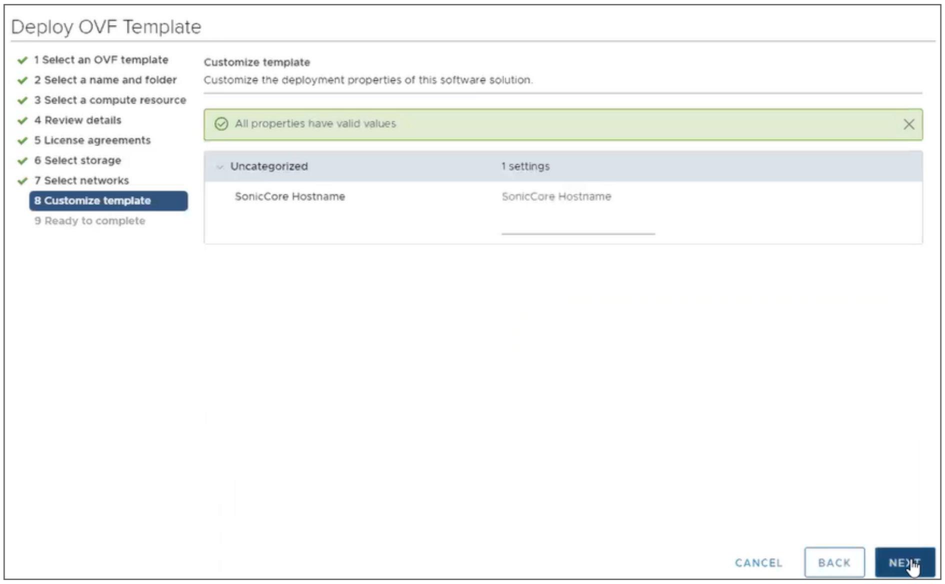
15. In the **Select networks** screen, set up interface**X0** to access the network.

    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.

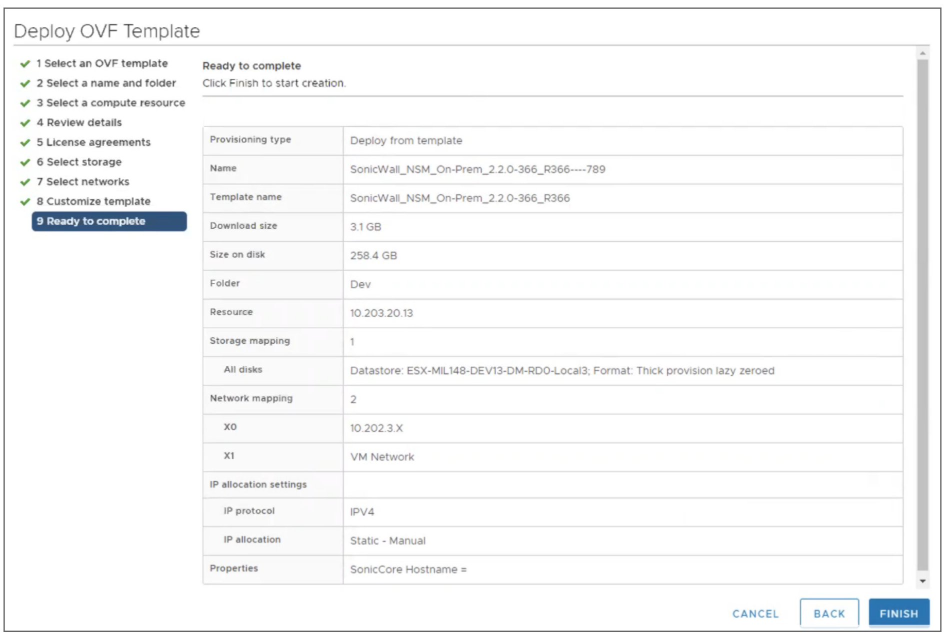


ⓘ | **IMPORTANT: X1** (the default WAN Interface) is set to **DHCP** by default, with **HTTPS management** enabled for the NSM On-Premises instance, as this configuration eases deployments in virtual/cloud environments.

16. Click **Next**.



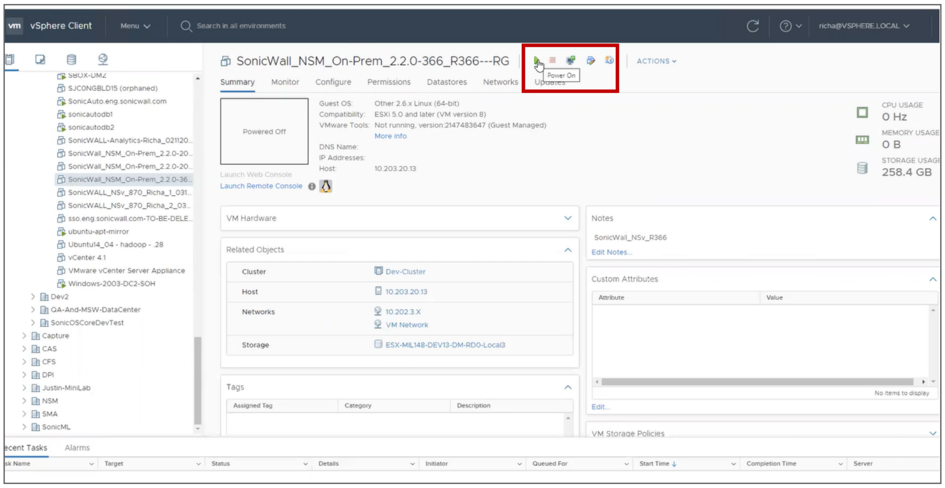
17. In the **Customize template** screen, verify the information, and click **Next**.



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.

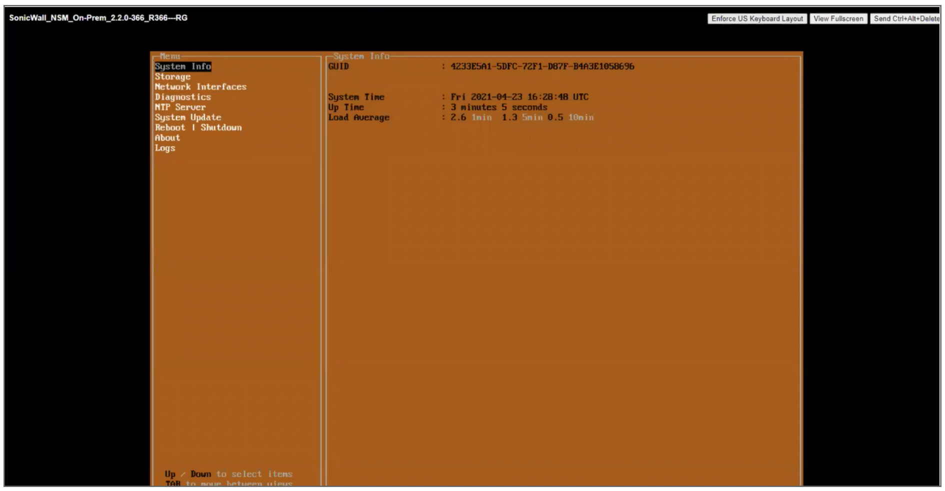


20. Click on the large **Powered Off** button in the **Summary** page (upper left corner). to launch the console.

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

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

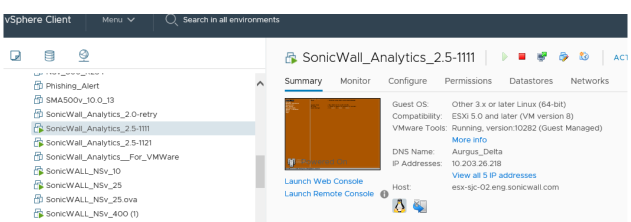
When the initial boot is complete, the Management Console displays.



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

Connecting to the Console from ESXI

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



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

4

Installing NSM on Hyper-V

Topics:

Preparing the Windows Server System

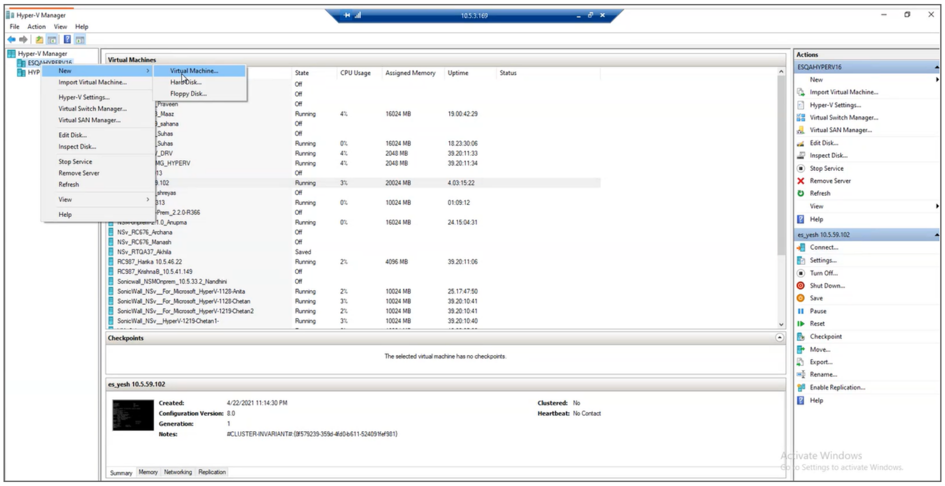
Before installing an NSM On-Premises instance on Hyper-V, prepare the Windows Server system:

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

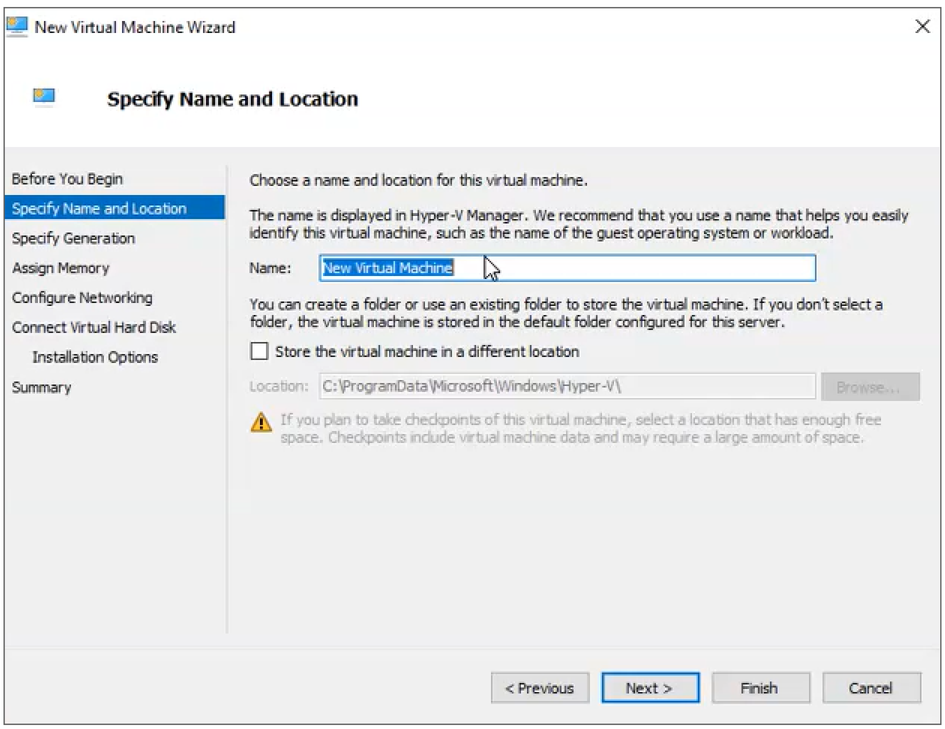
Installing NSM On-Premises on Hyper-V

To install NSM On-Premises on Hyper-V:

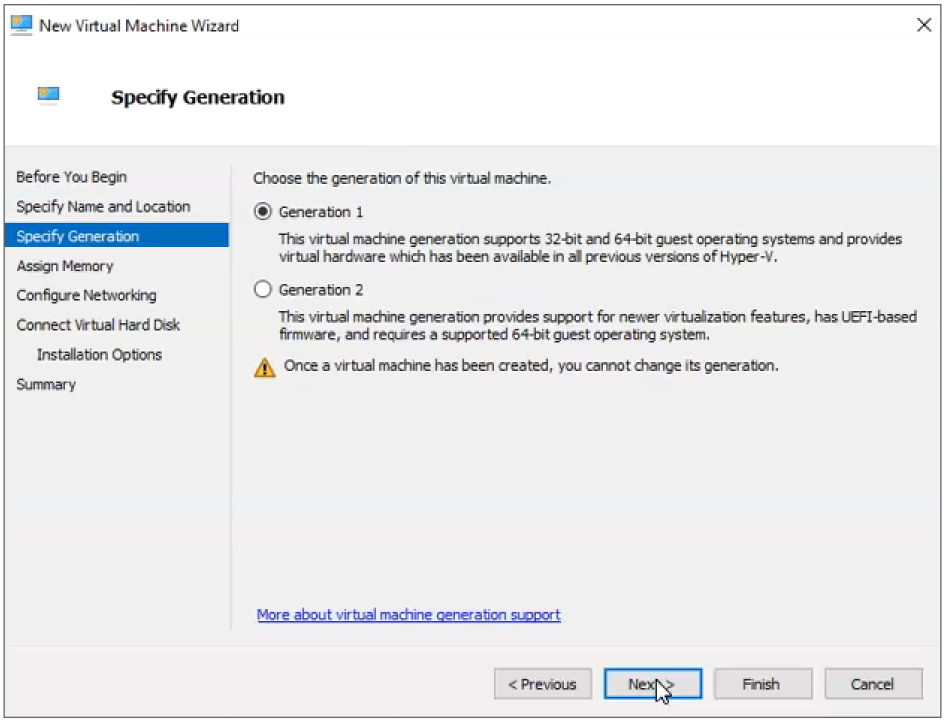
1. Log in to Hyper-V to select the VM.
2. Right click on the name of the VM.
3. Click **New > Virtual Machine**.



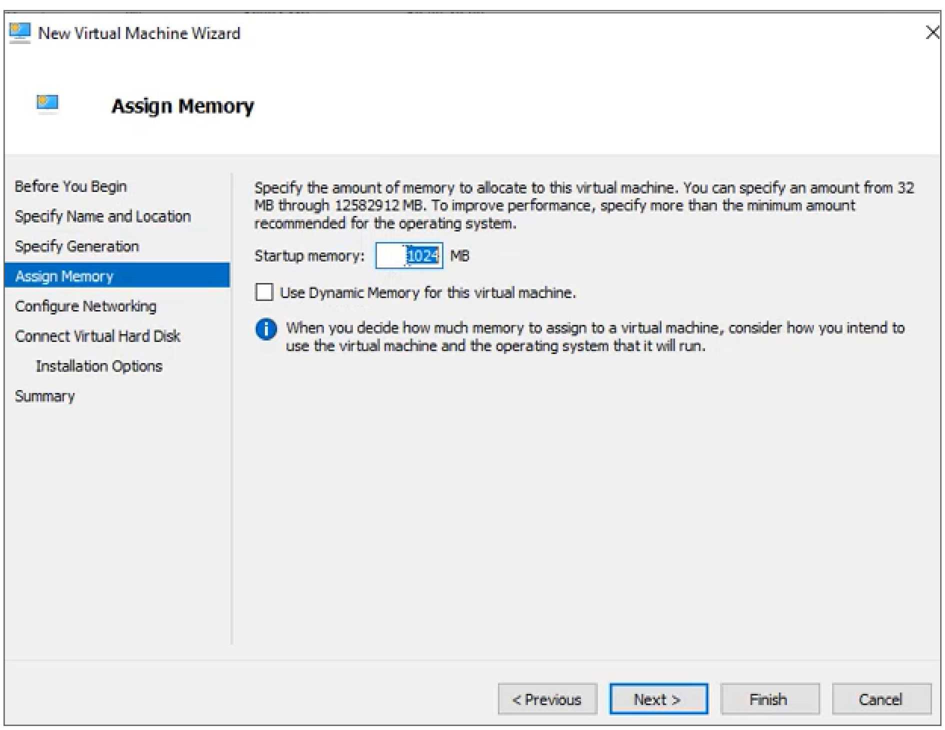
The **New Virtual Machine Wizard** window is displayed.



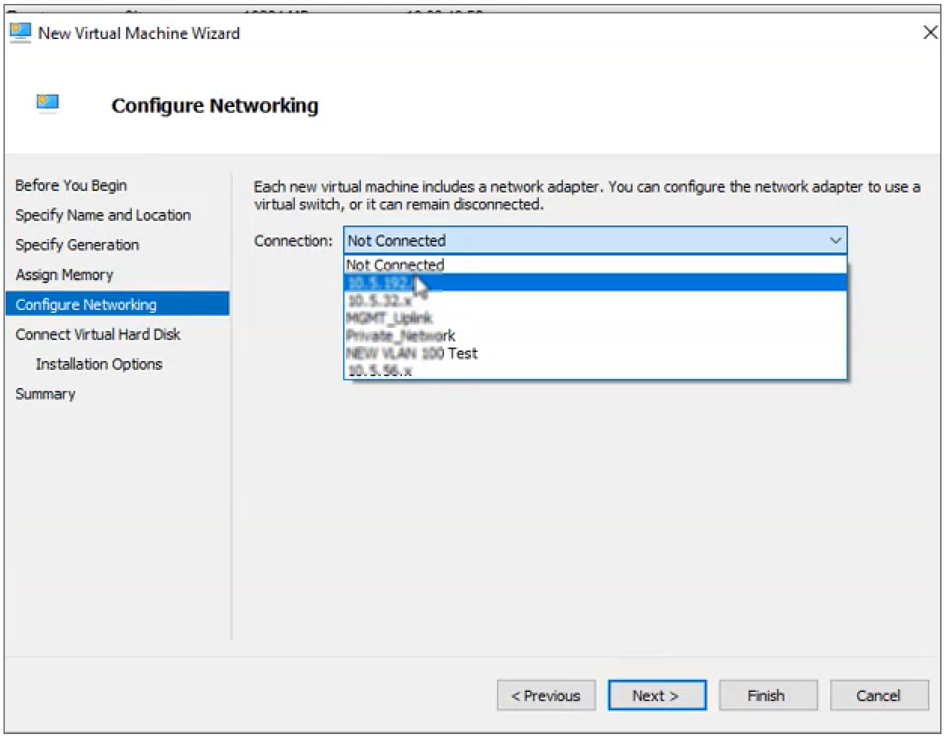
4. Specify the name and location of the VM.
5. Click **Next**.



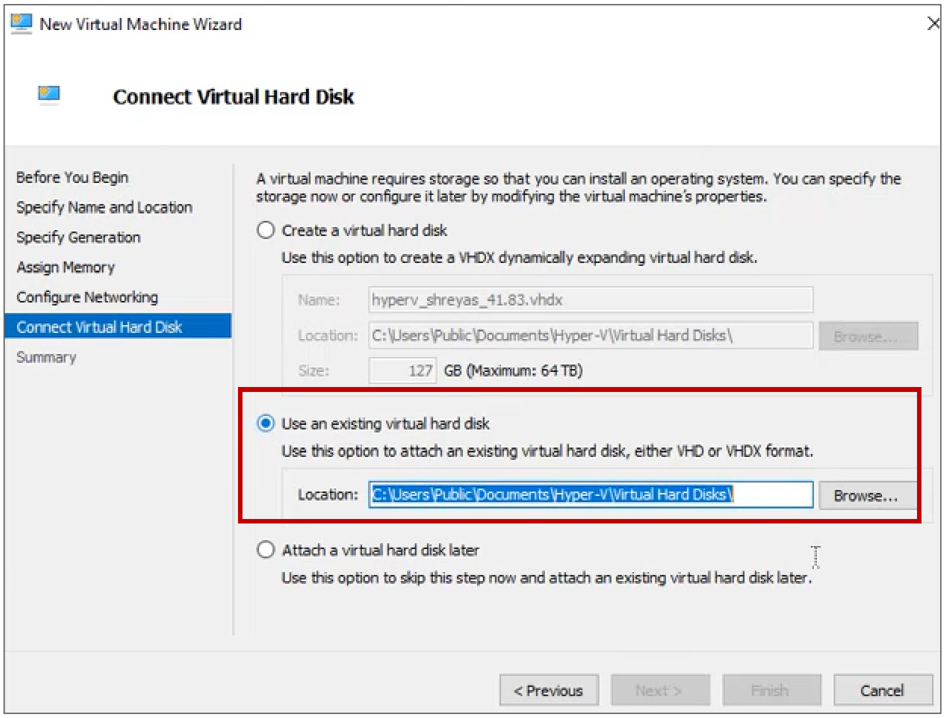
6. Specify the **Generation** as **Generation 1**.
7. Click **Next**.



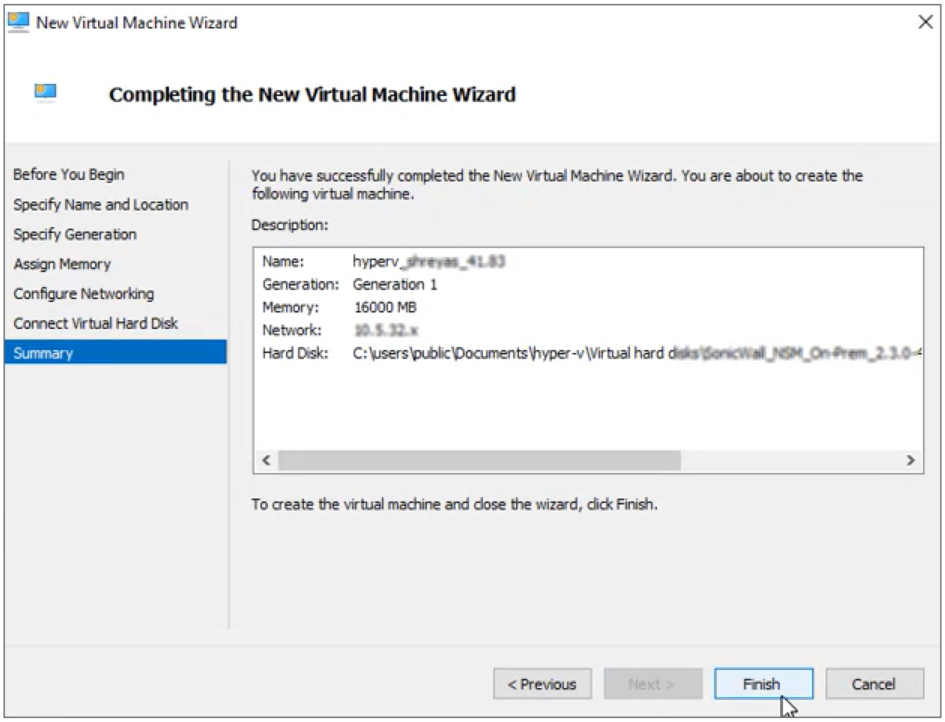
8. Assign memory to the VM.
9. Click **Next**.



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



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.



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

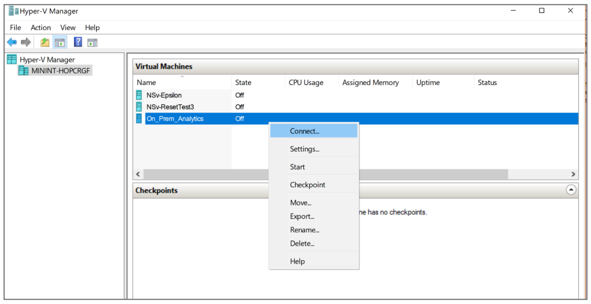
You can easily use the NSM Management Console to view and configure various parameters for NSM. It can also be used for diagnostics. When using Hyper-V you can connect to the NSM Management Console in the following way:

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

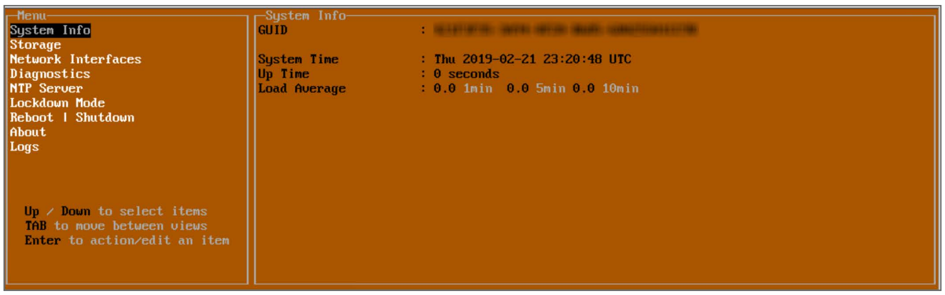
  NOTE: In the following procedure, the public IP address is the WAN IP address appearing in **Hyper-V Virtual Machine Connection**.

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**.



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



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

5

Installing NSM on KVM

Topics:

Preparing the KVM Server

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

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

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

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

```
$ sudo kvm-ok
```

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

```
$ sudo apt install cpu-checker
```

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

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

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

Installing KVM

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

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

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

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

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

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

```
$ sudo systemctl enable --now libvirtd
```

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

```
$ lsmod | grep -i kvm
```

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

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

Deploying NSM on KVM

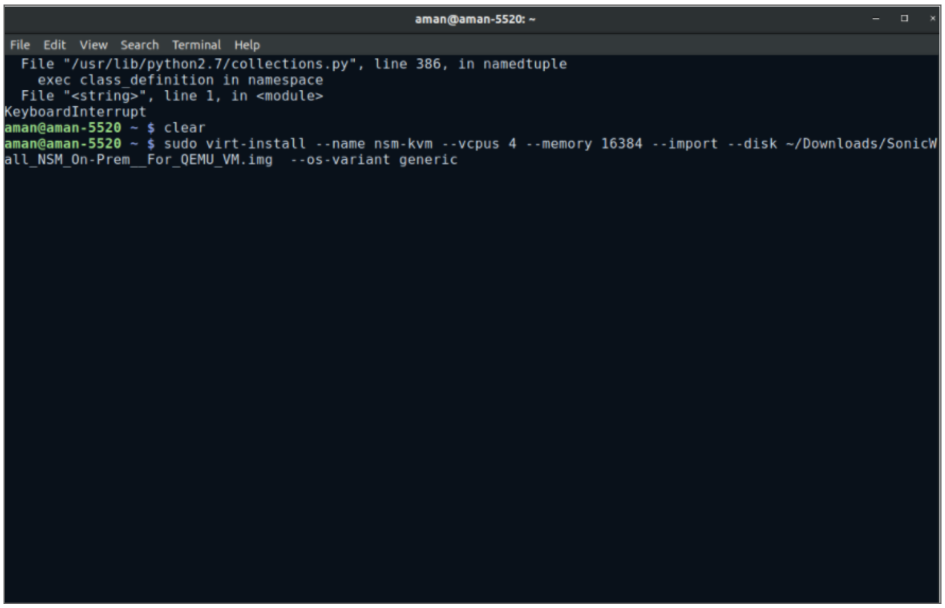
This section describes more about the following topics:

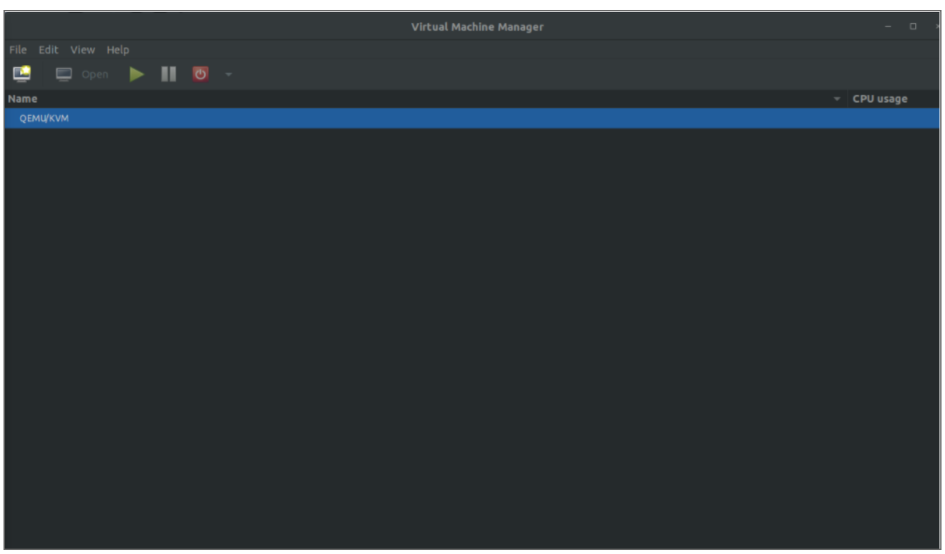
- Creating a Virtual Machine via Command Line
- Creating a Virtual Machine via Virtual Manager

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

Creating a Virtual Machine via Command Line

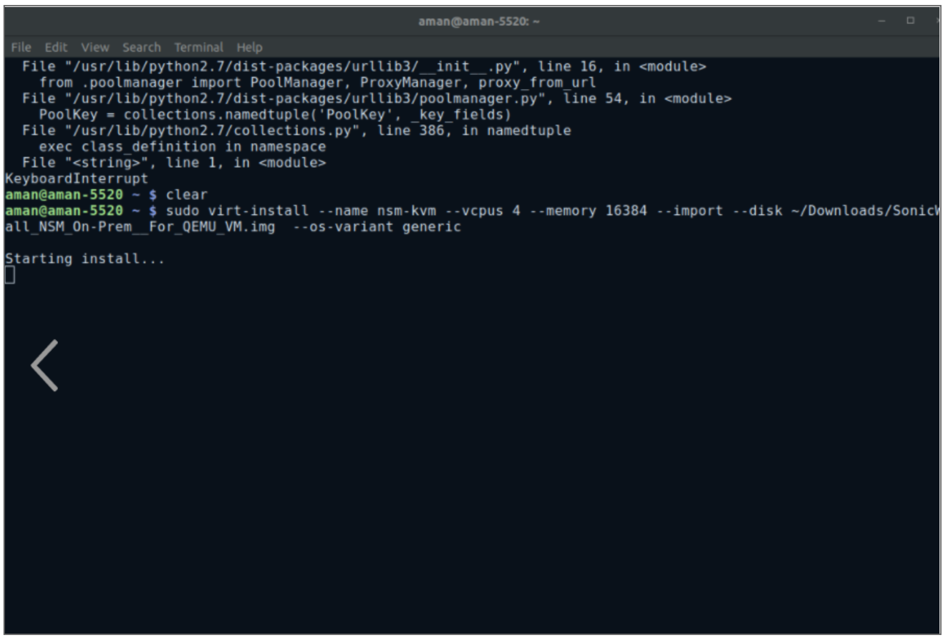
The virt-install command-line tool is used for creating virtual machines on the terminal. A number of parameters are required when creating a virtual machine. To create a virtual machine execute the following command (replace the image file path with the appropriate file):

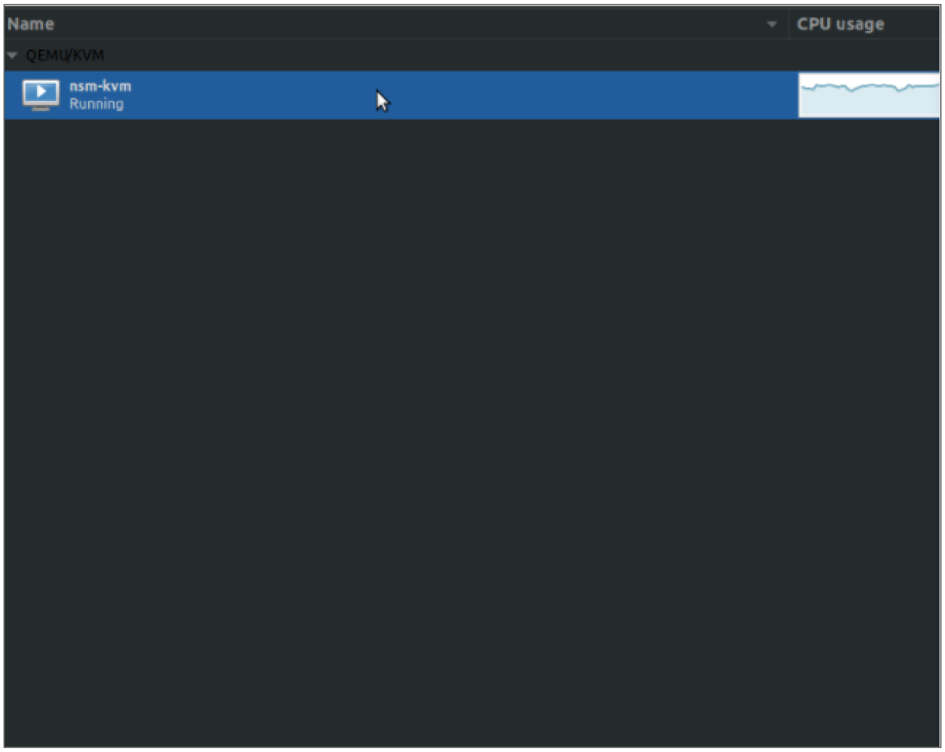


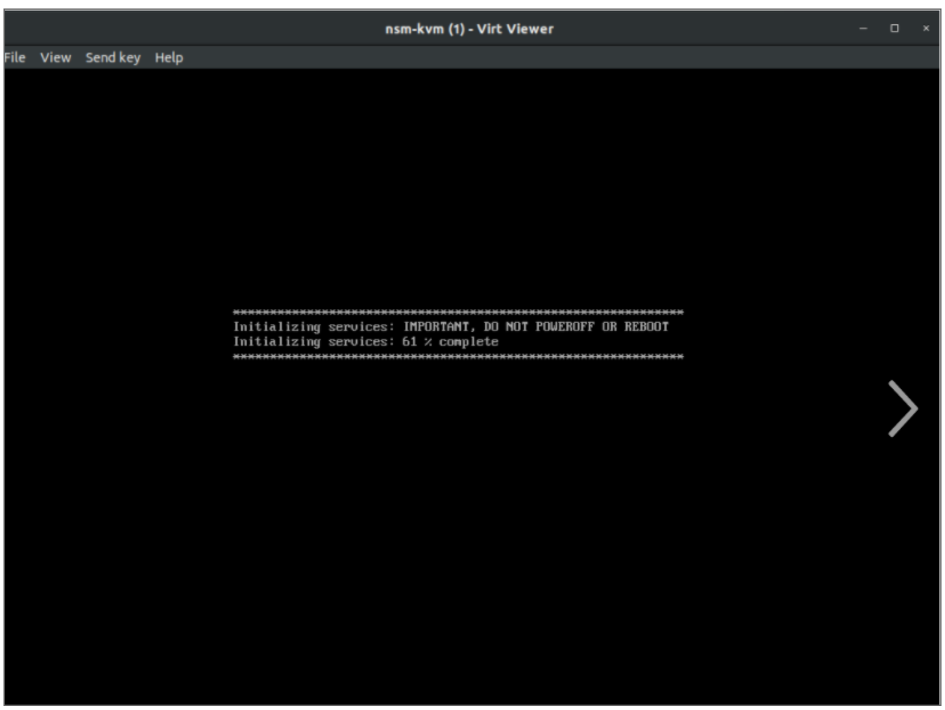


```
$ sudo virt-install --name nsm --vcpus 4 --memory 16384  --import --disk
/home/ghan/Downloads/SonicWall_NSM_On-Prem__For_QEMU_VM.img --os-variant generic
```

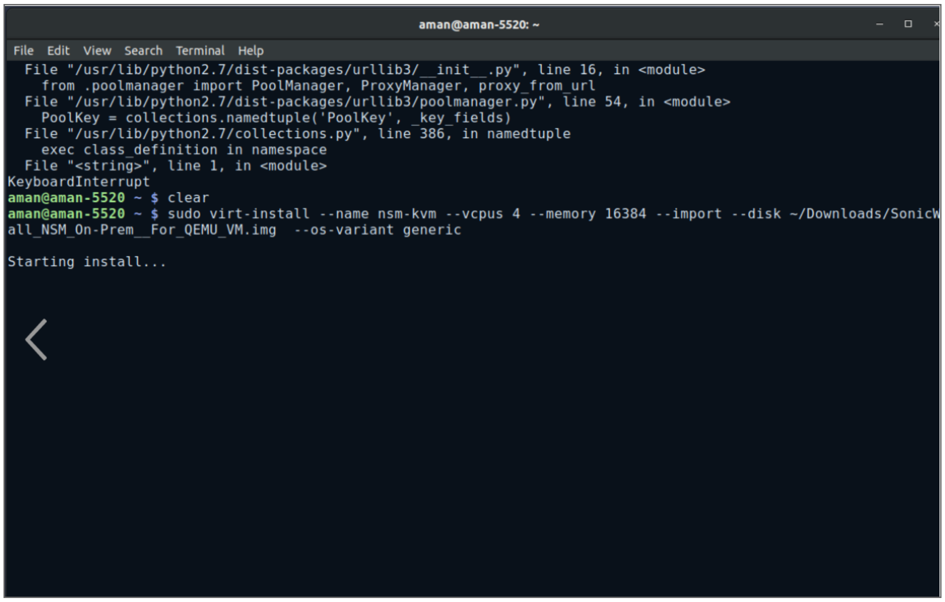
- The “--name” option specifies the name of the new virtual machine.
- The “--vcpus” option indicates the CPU cores, which in this case is set to 4 cores.
- The “--memory” indicates the RAM capacity, which is 16 GB. Note that this requires your host to have a large memory for the best working experience.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

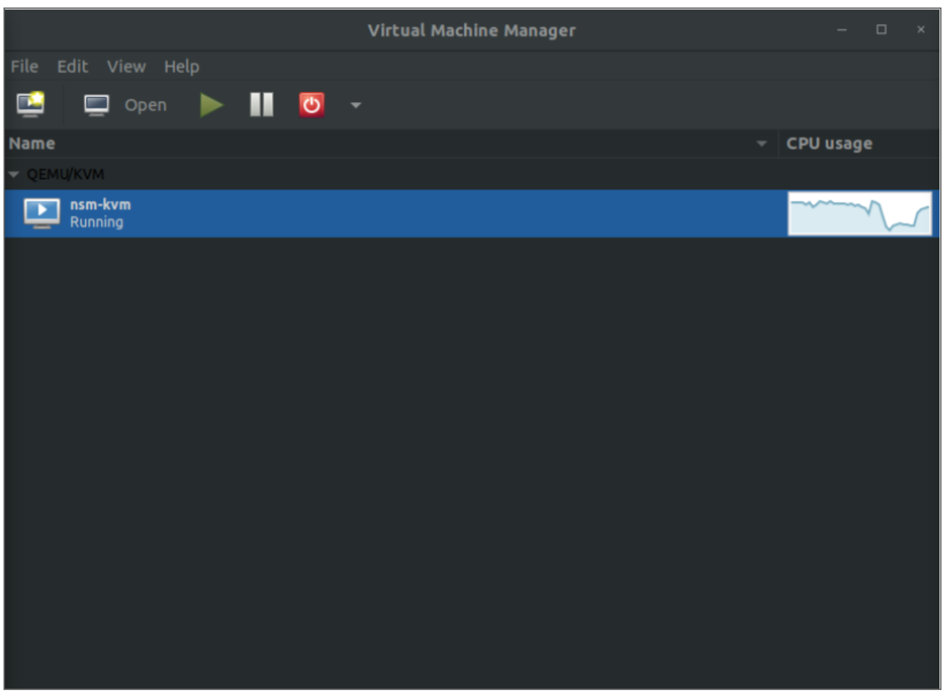


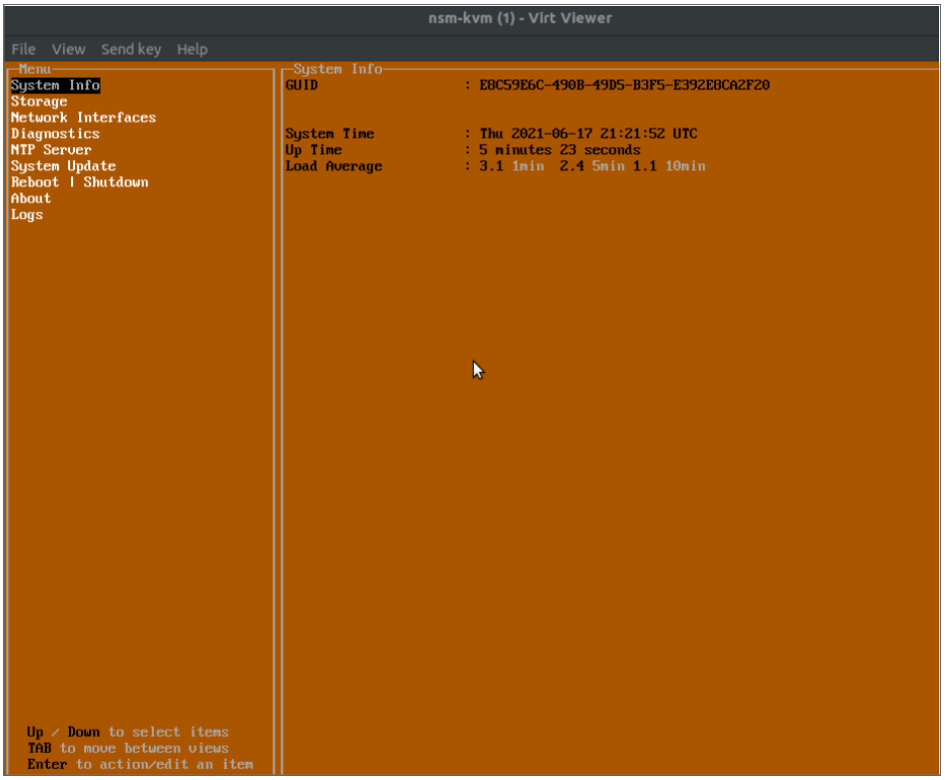




Immediately after executing the command, the virtual machine boots up and the installer gets ready for the installation of the virtual machine.


aman@aman-5520: ~
File Edit View Search Terminal Help
File "/usr/lib/python2.7/dist-packages/urllib3/__init__.py", line 16, in <module>
from .poolmanager import PoolManager, ProxyManager, proxy_from_url
File "/usr/lib/python2.7/dist-packages/urllib3/poolmanager.py", line 54, in <module>
PoolKey = collections.namedtuple('PoolKey', _key_fields)
File "/usr/lib/python2.7/collections.py", line 386, in namedtuple
exec class_definition in namespace
File "<string>", line 1, in <module>
KeyboardInterrupt
aman@aman-5520 ~ $ clear
aman@aman-5520 ~ $ sudo virt-install --name nsm-kvm --vcpus 4 --memory 16384 --import --disk ~/Downloads/SonicW
all_NSM_On-Prem__For_QEMU_VM.img --os-variant generic
Starting install...

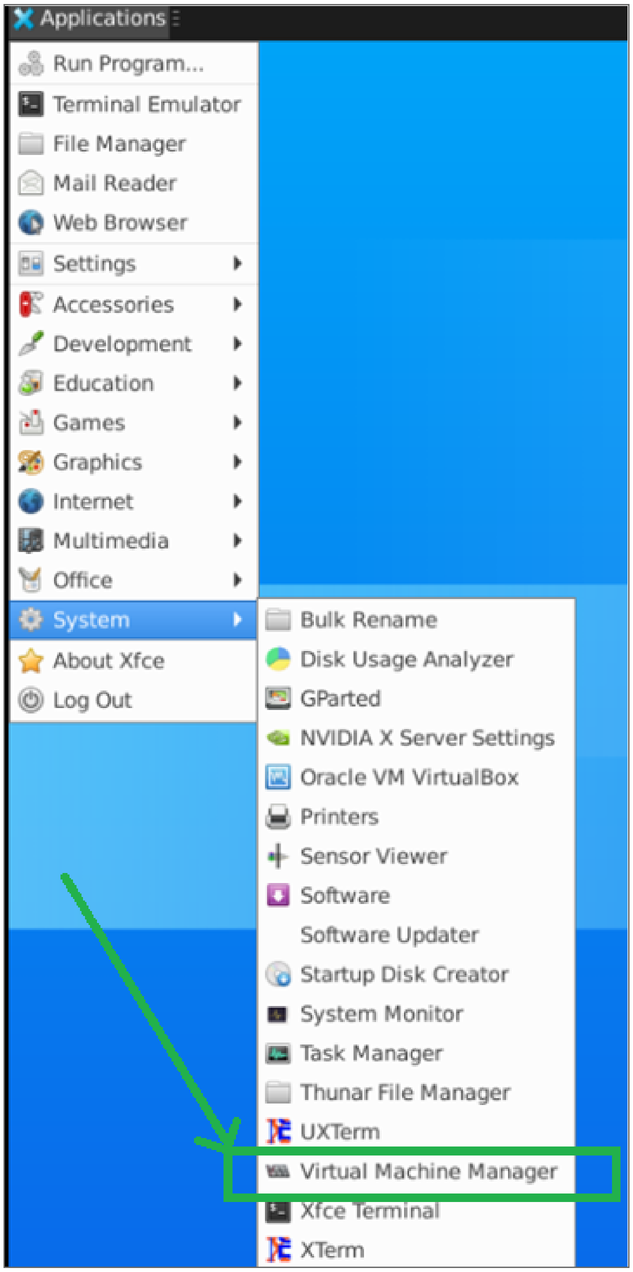

Virtual Machine Manager
File Edit View Help
Open
Name
CPU usage
QEMU/KVM
nsm-kvm
Running

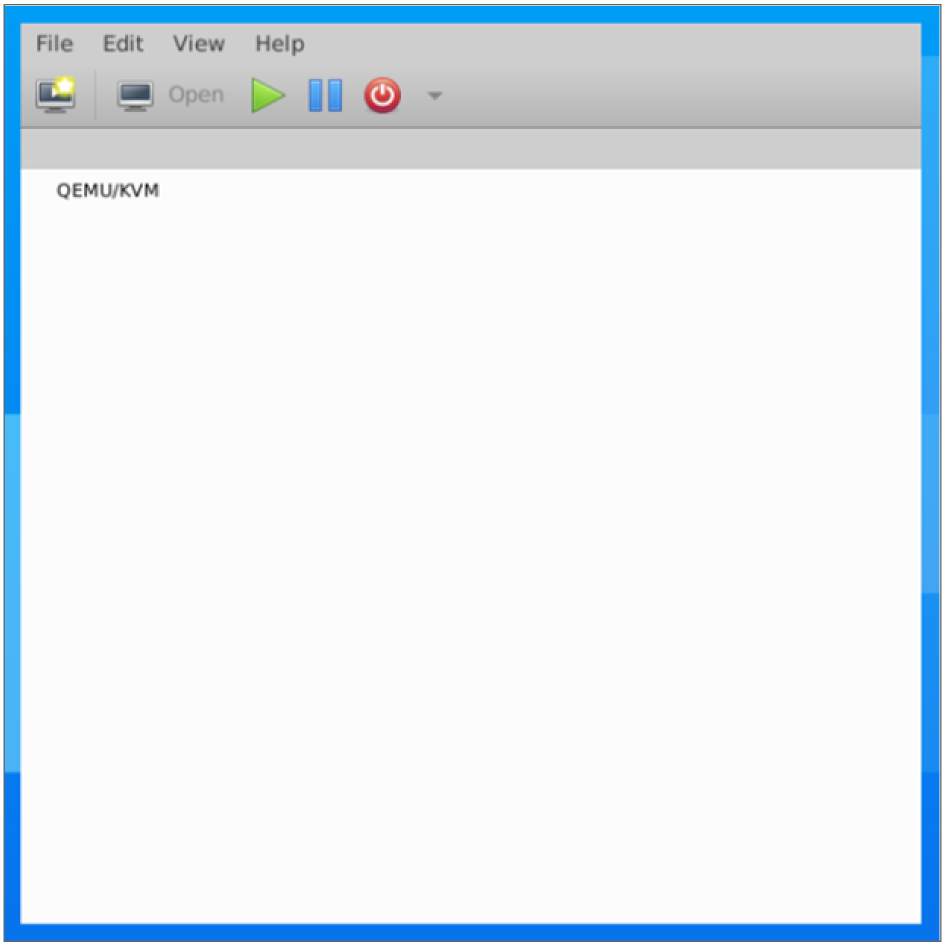


Creating a Virtual Machine via Virtual Manager

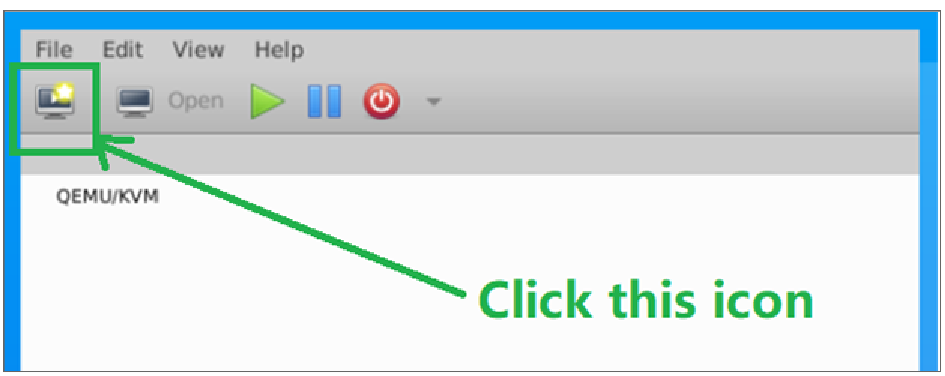
You can create a virtual machine through by using the Virtual Machine Manager application. This application can be opened by either running the virt manager command, $ virt-manager, or by opening it through your system:

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

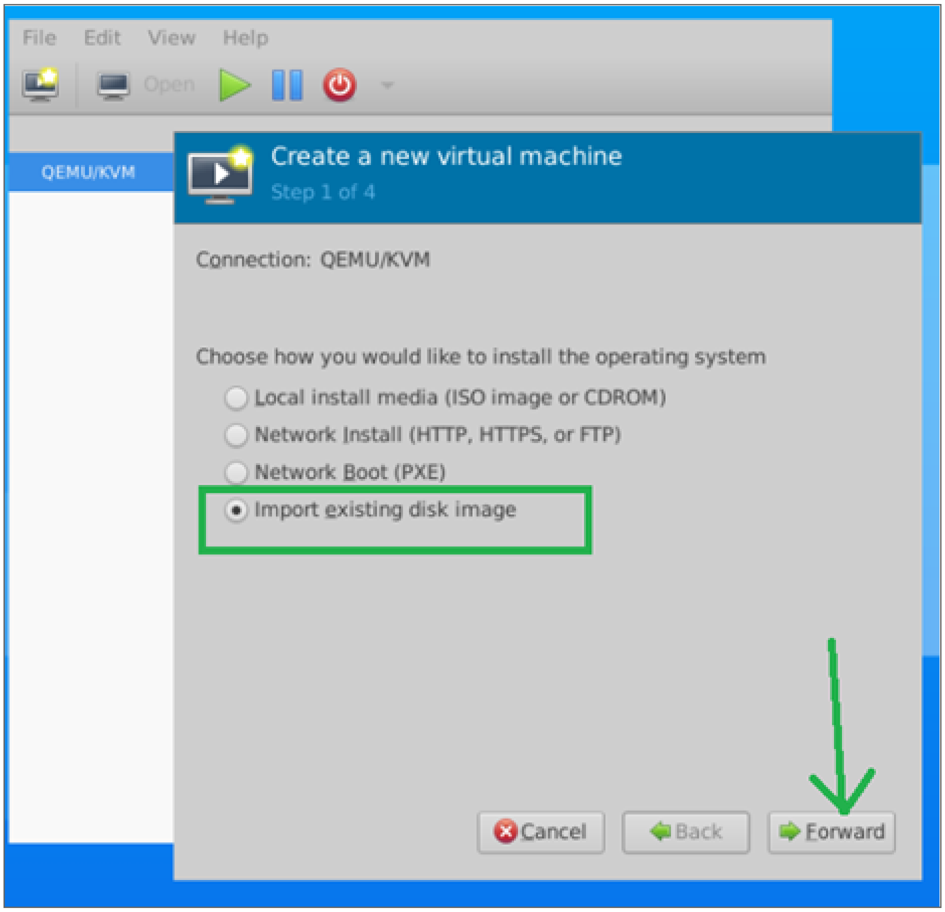

Applications
Run Program...
Terminal Emulator
File Manager
Mail Reader
Web Browser
Settings
Accessories
Development
Education
Games
Graphics
Internet
Multimedia
Office
System
About Xfce
Log Out
Bulk Rename
Disk Usage Analyzer
GParted
NVIDIA X Server Settings
Oracle VM VirtualBox
Printers
Sensor Viewer
Software
Software Updater
Startup Disk Creator
System Monitor
Task Manager
Thunar File Manager
UXTerm
Virtual Machine Manager
Xfce Terminal
XTerm



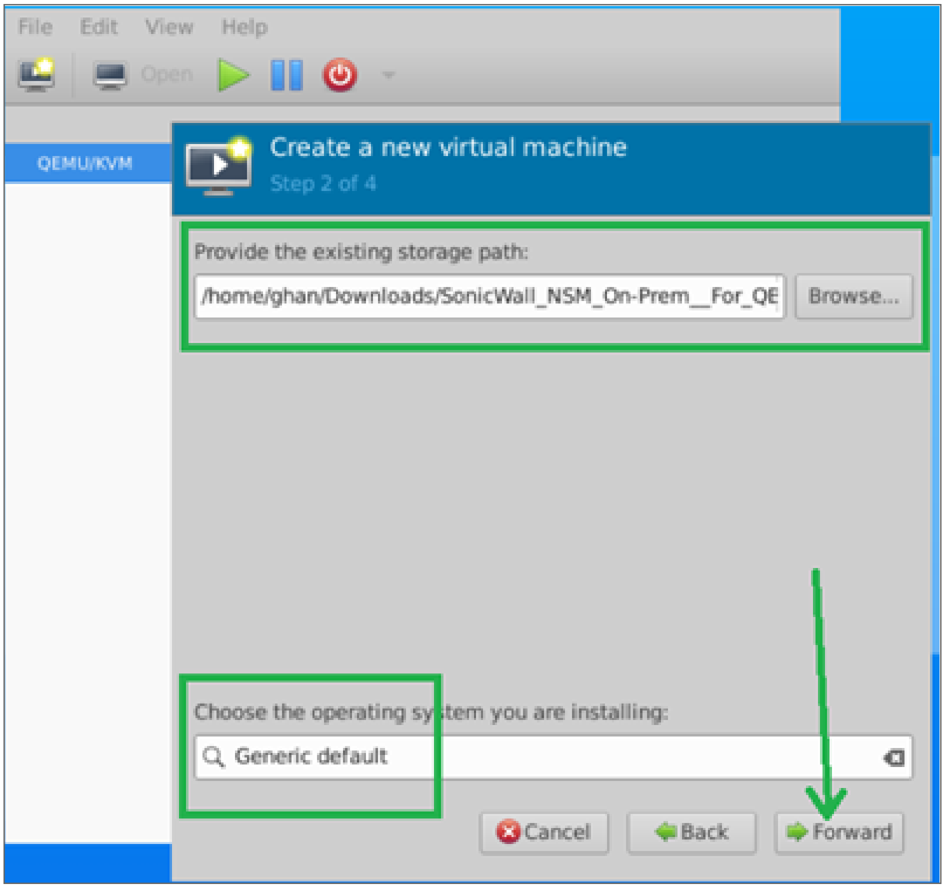
2. Click the monitor icon to start creating a virtual machine.



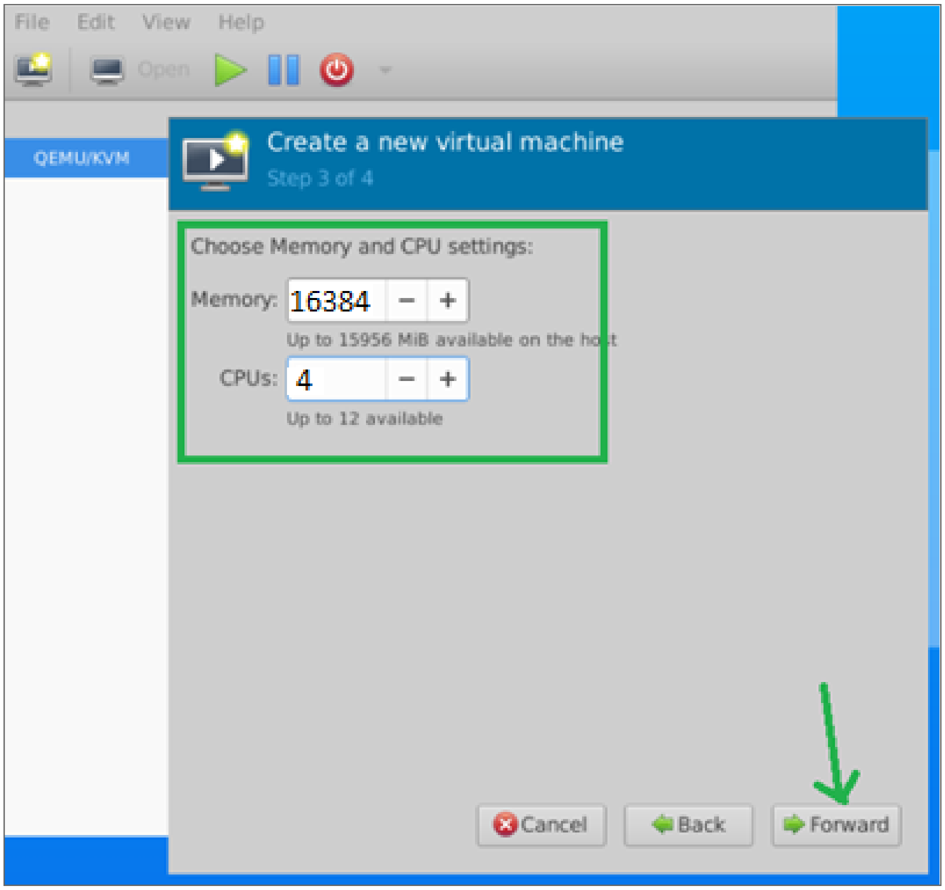
3. On the pop-up window, choose **Import existing disk image**.



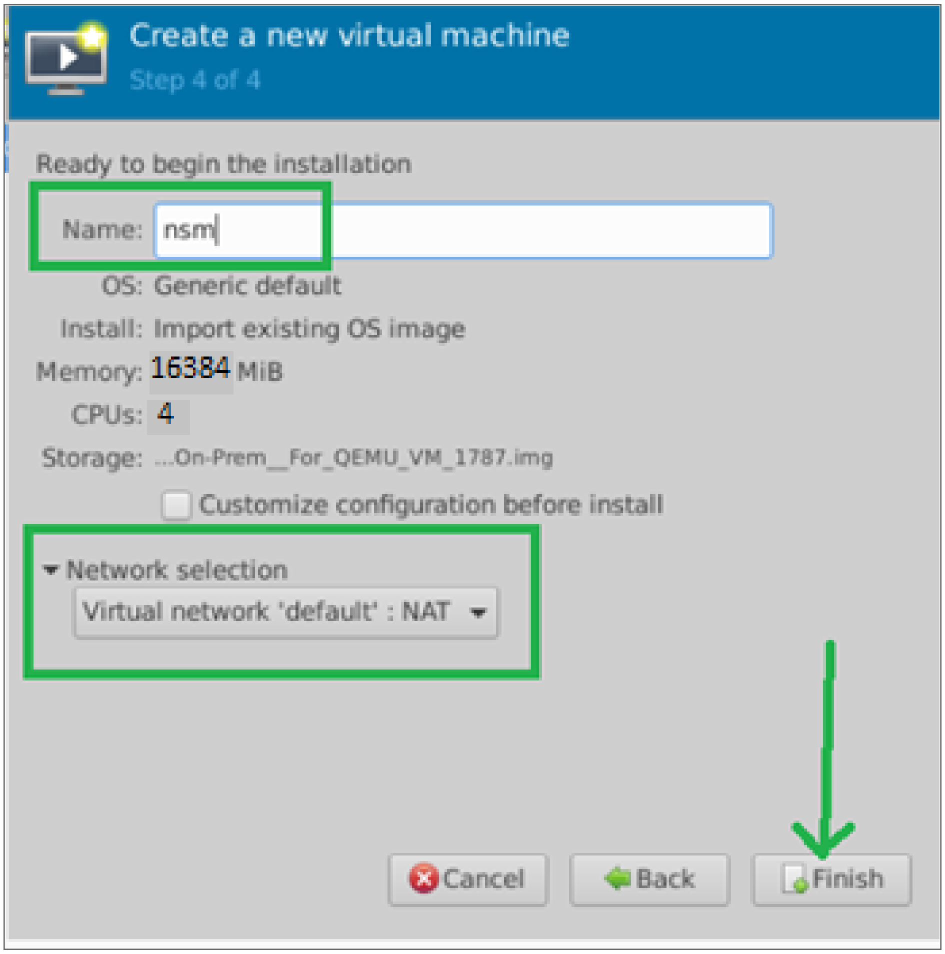
4. Click **Forward** to continue.
5. Browse your local directory and locate the image file, and then type in ‘Generic default’ in the **Operating System** field.
6. Click **Forward**.



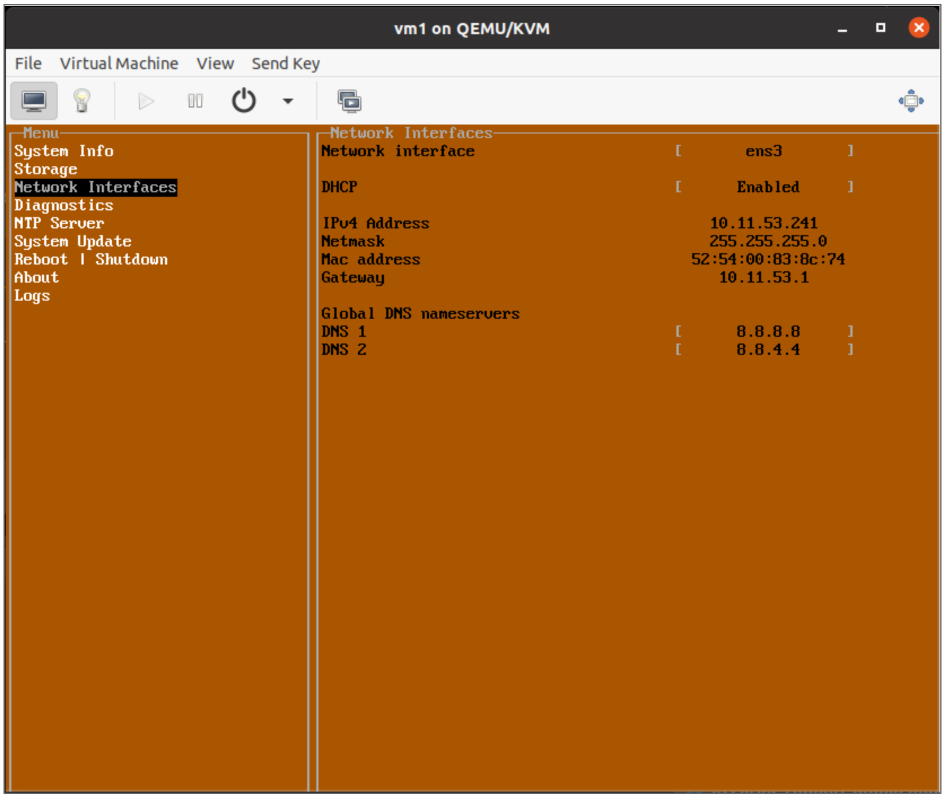
7. Next, set the memory to 16 (GB), and CPU to 4 (cores) and click **Forward**.

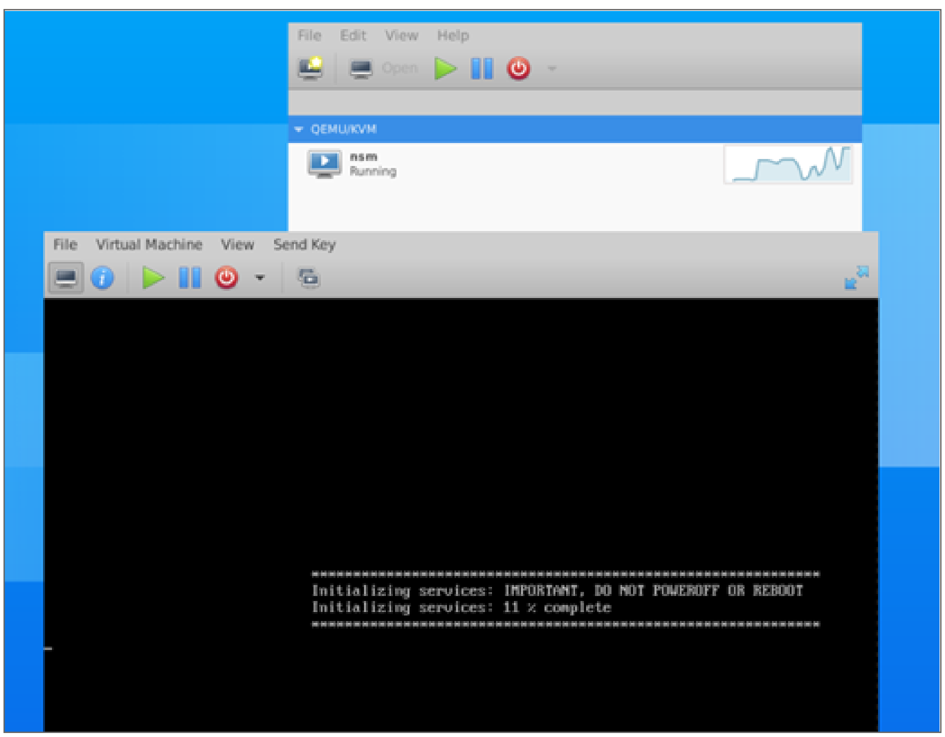


8. Set the VM name.
9. Choose the network option (default is NAT).
10. Click **Finish**. You can access the NSM UI from the host system only if the Network selection is in NAT mode. For the public access, please configure the Network to **Bridge** mode.



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


vm1 on QEMU/KVM
File Virtual Machine View Send Key
Menu
System Info
Storage
Network Interfaces
Diagnostics
NTP Server
System Update
Reboot | Shutdown
About
Logs
Network Interfaces
Network interface [ens3]
DHCP [Enabled]
IPv4 Address 10.11.53.241
Netmask 255.255.255.0
Mac address 52:54:00:83:8c:74
Gateway 10.11.53.1
Global DNS nameservers
DNS 1 [8.8.8.8]
DNS 2 [8.8.4.4]


File Edit View Help
QEMU/KVM
nsm
Running
File Virtual Machine View Send Key
Initializing services: IMPORTANT, DO NOT POWEROFF OR REBOOT
Initializing services: 11 % complete

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

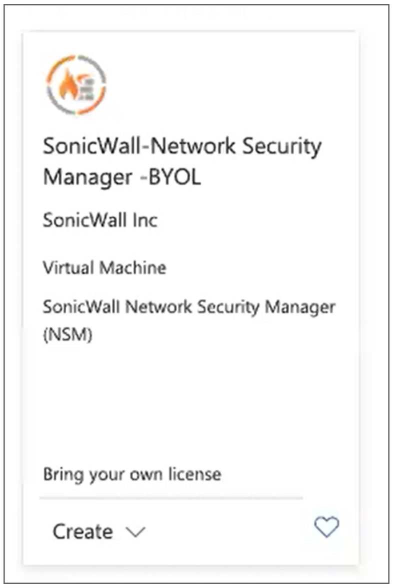
6

Installing NSM on Azure

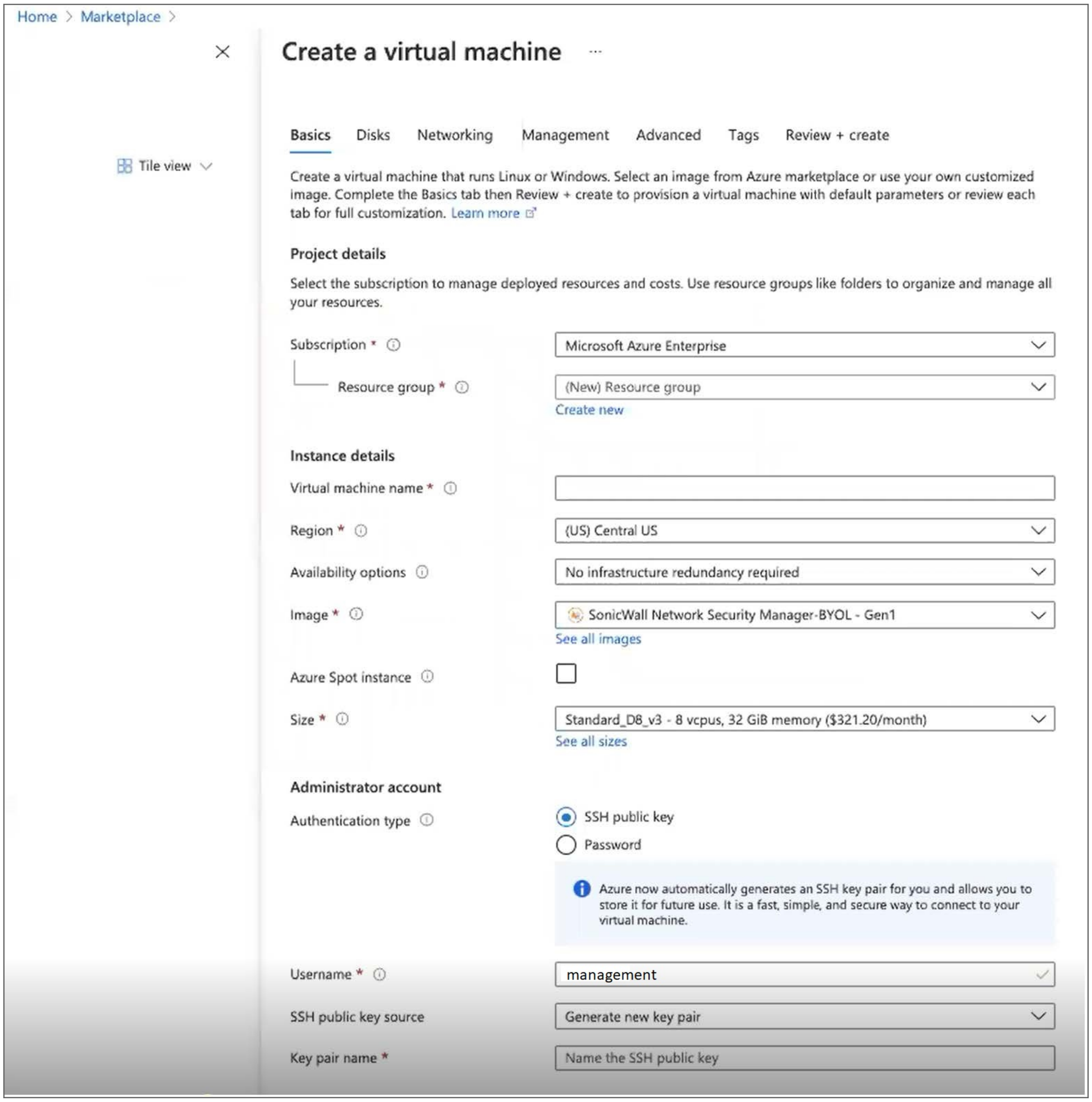
This chapter provides you with the information on how to deploy the NSM file on your Azure server.

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**.

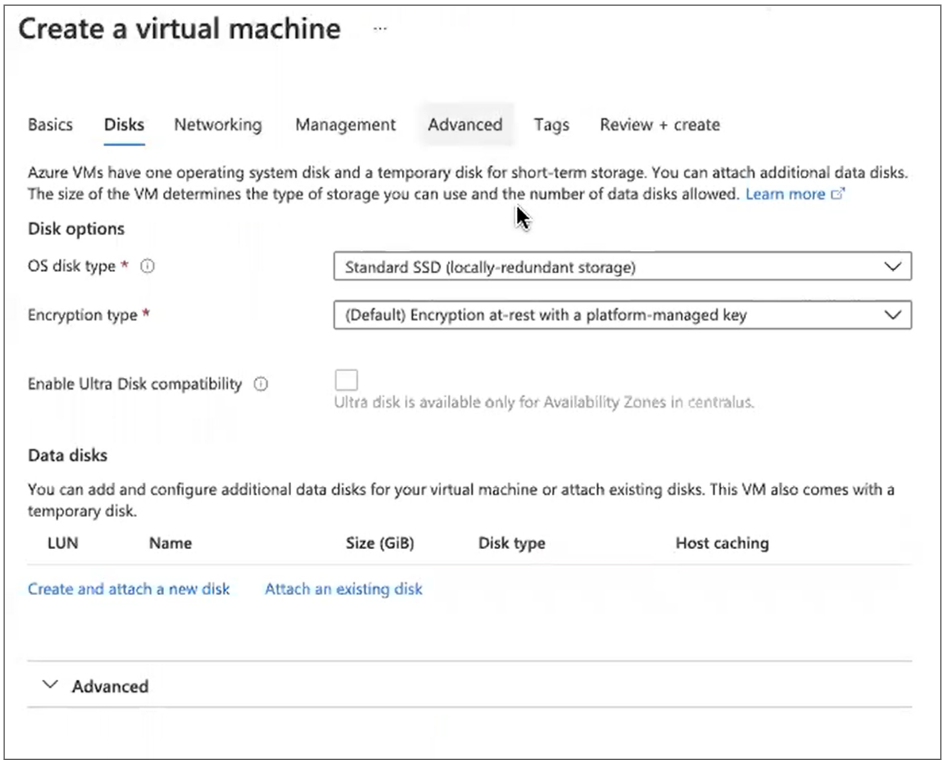


4. On the **Basics** tab to **Create a virtual machine**, select **Create new** in the **Resource group** field.

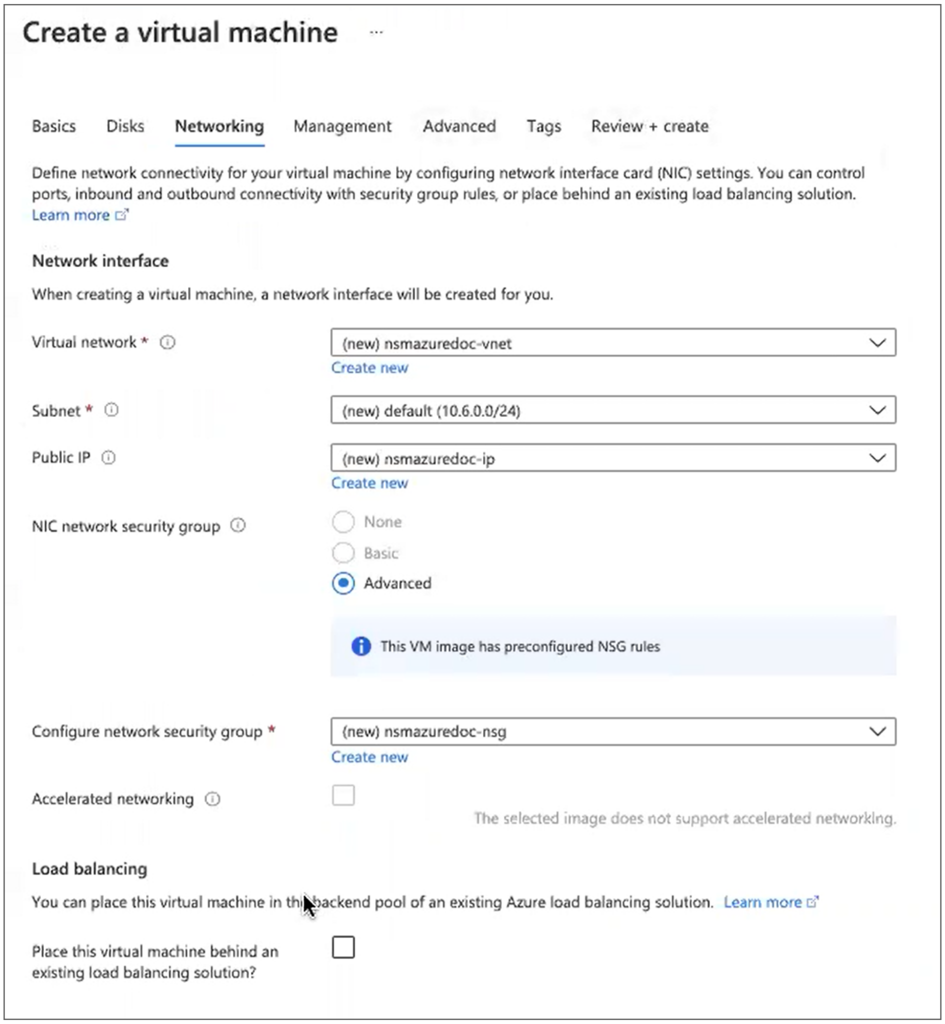


5. Type an easy-to-identify name in the **Name** field and click **OK**.
6. Enter the **Virtual machine name**. It can be the same as the **Resource group name**, if you want.
7. Set the **Region**.
8. From the **Image** drop-down list, select the **SonicWall-Network Security Manager -BYOL**.
9. Leave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

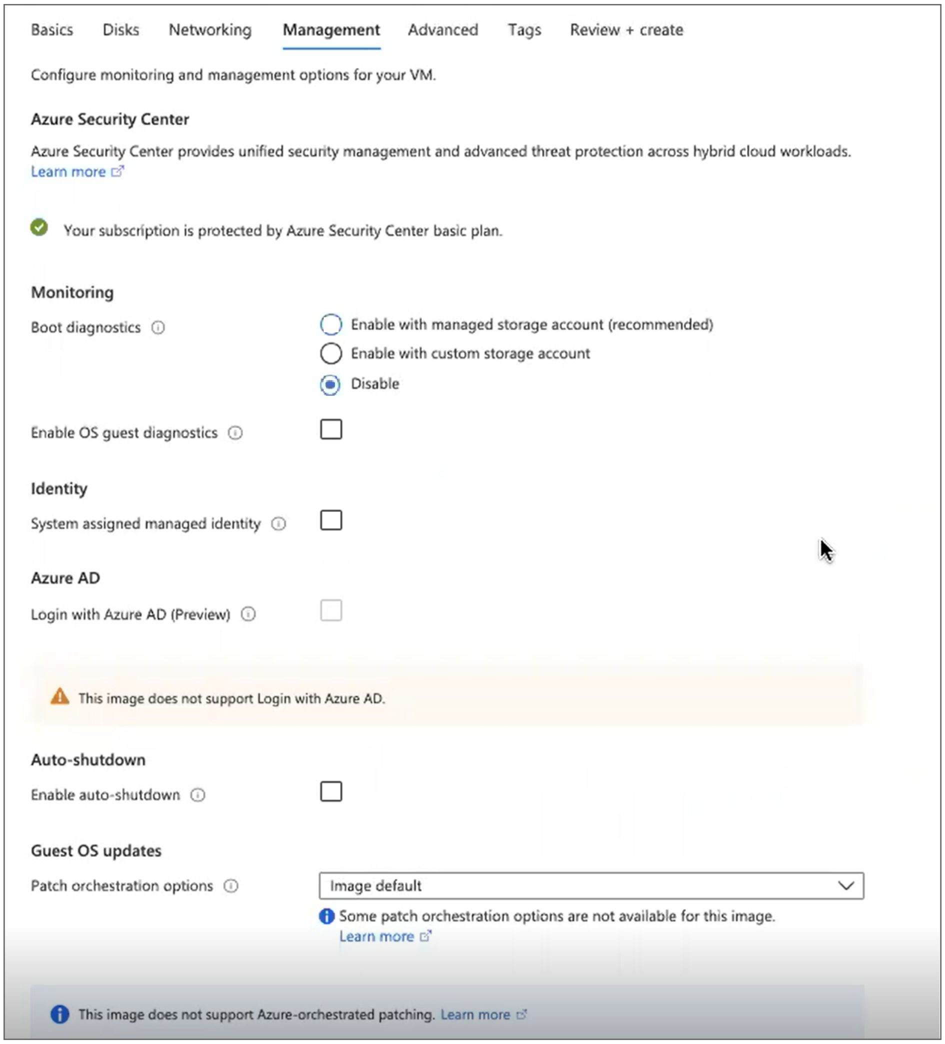
12. Define the **Username** as "**management**". If you fail to do so, you will not be able to access NSM console and need to redeploy the NSM image.
13. Generate a public key through command lin: `ssh -keygen`.
14. Copy and paste that key in SSH public key field.
15. Click **Next : Disks >**.



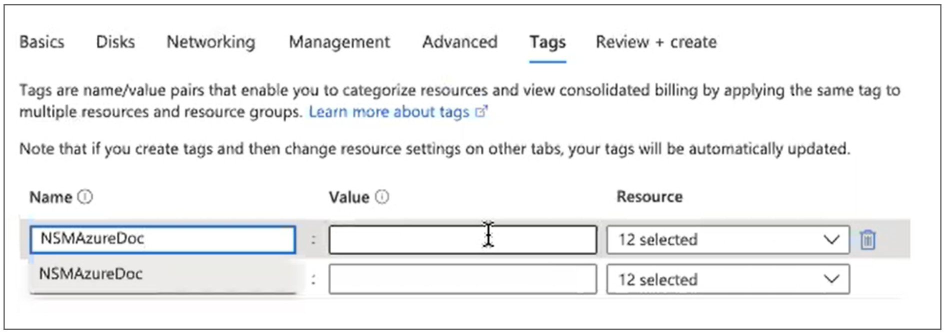
16. Use the defaults on the Disks tab.
17. Click **Next : Networking >**.



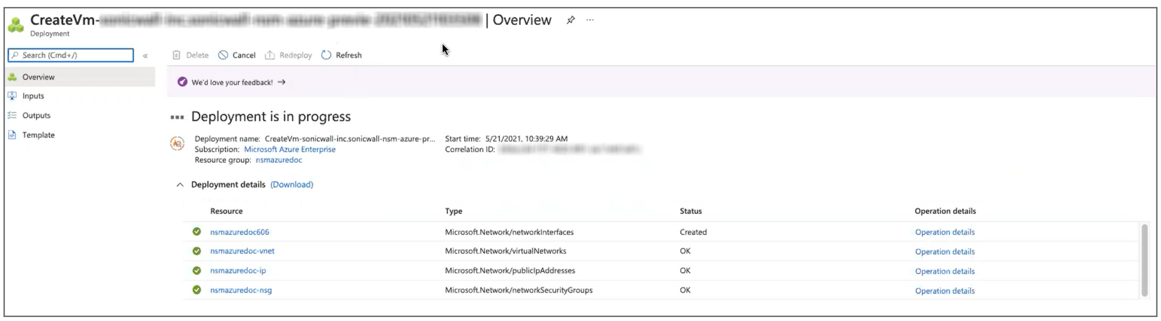
18. Configure the network settings for your environment. The default settings can also work.
19. Click **Next : Management >**.



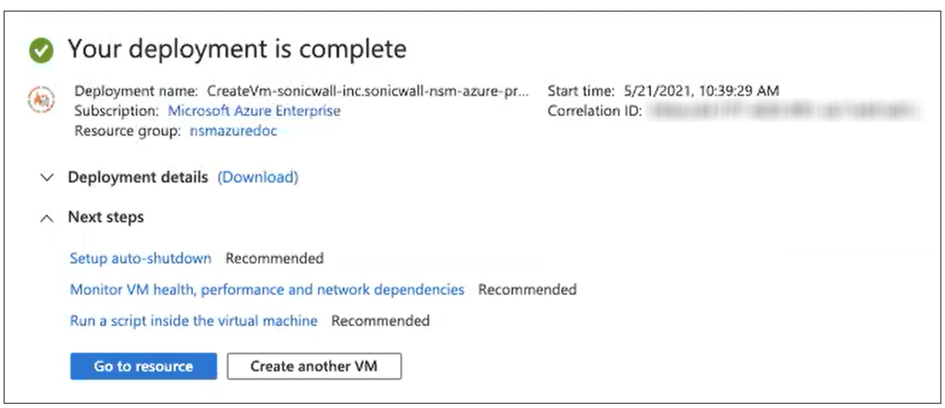
20. Disable the Boot Diagnostics setting.
21. Set the rest of the management options as you want for your implementation. The default settings can also work.
22. Click **Next : Advanced >**.
23. Keep the defaults on the **Advanced** tab.
24. Click **Next : Tags >**.



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.



A message displays when the deployment is complete.



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.

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

NSM Settings and Registration

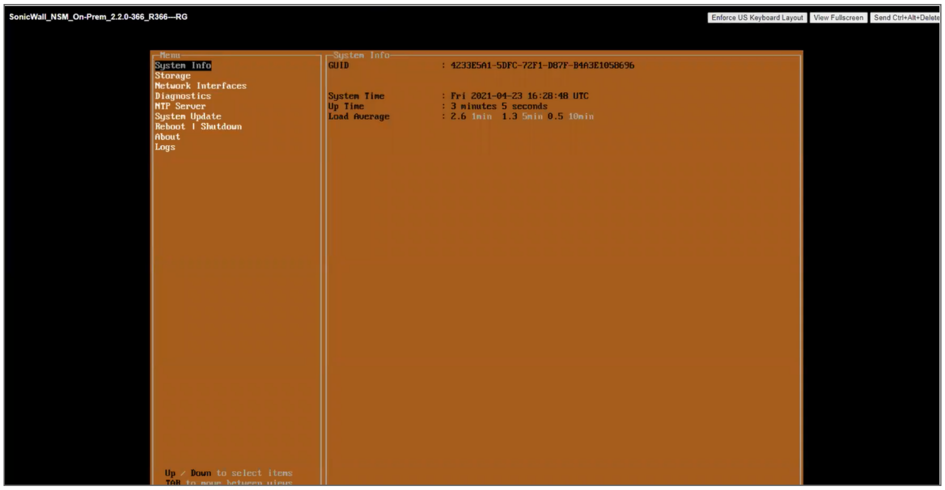
After the installation of the NSM image is complete, you need to define the network settings and register your product.

Topics:

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

Configuring NSM Network Settings

1. Open the NSM Management Console.



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

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.

2. For initial access, log in using **admin** and **password** as our credentials. The first time you access NSM, it presents an initialization wizard.

   ⓘ | **NOTE:** It is recommended to change the default password after the initial configuration.

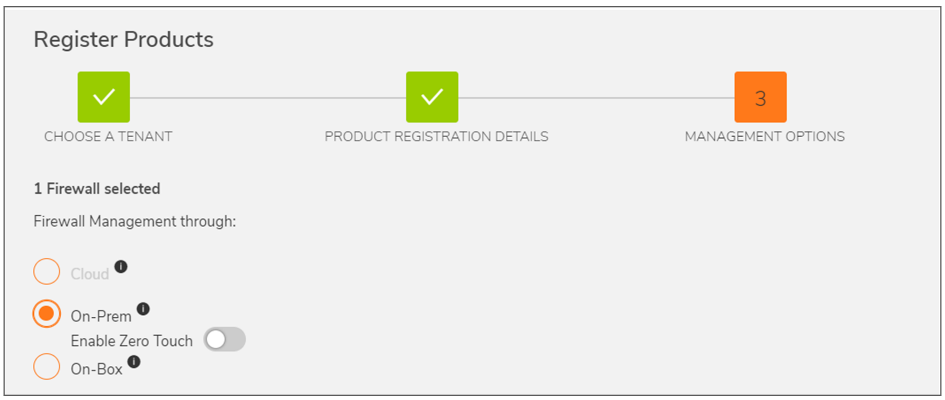
3. Enter your MySonicWall **Username** and **Password**.
4. Enter a **MySonicWall Friendly Name**.
5. Enter the **Serial Number** and **Authorization Code** received from your sales representative.
6. Click **Register**.
7. To confirm registration, navigate to **Manager View | System > Settings > Licenses**.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

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

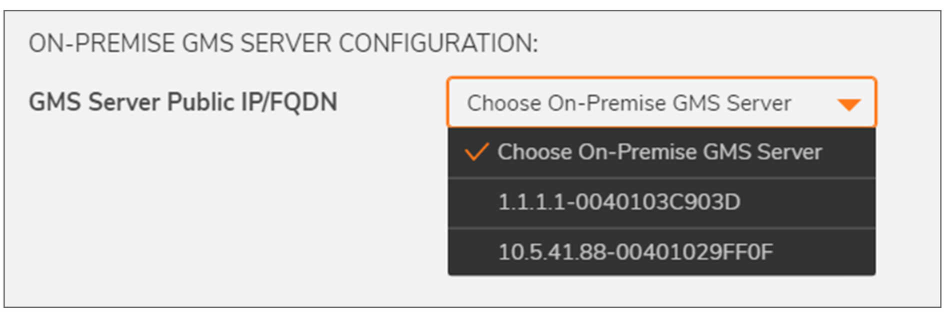
Associating Firewalls on MSW

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

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



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



7. Click **Save/Register**.

Unregistering NSM

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

Console Operations

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

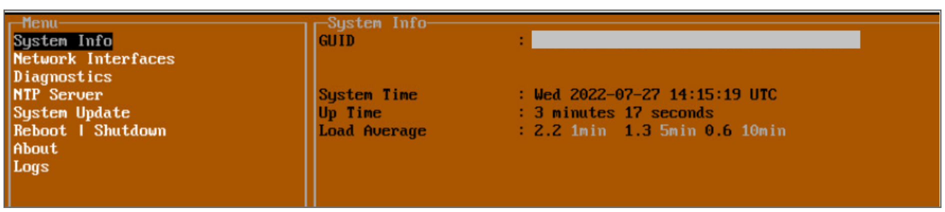
Topics:

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

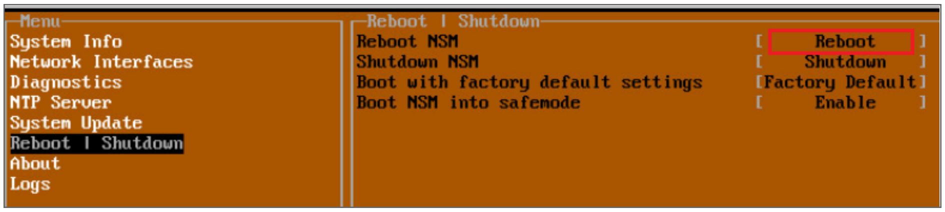
Management Console Operations

To access the Management Console:

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

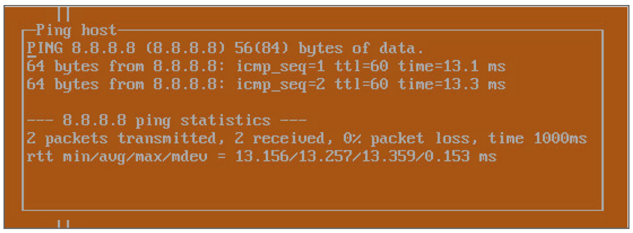


2. The main menu is displayed in the side menu (left panel). Use the up/down arrow keys to move the focus between menu items. As the focus shifts, the right pane displays the options and information for that menu item. The currently selected item is highlighted in black.
3. Press the **Tab** key to move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

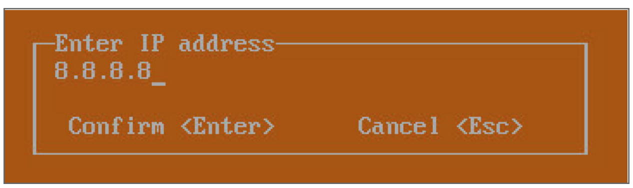


5. To select an option for editing or to choose the associated action, use the up/down arrow keys to move the focus to the editable/actionable items and press **Enter**.

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



   Some dialogs are for input:



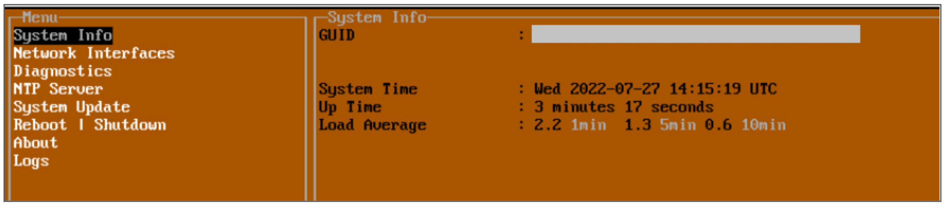
6. Use the arrow keys as needed to move between selections in the dialog. To change a value, press **Backspace** to erase each character, then type in the new value. When ready, press **Enter** to commit the change or perform the selected action. You can dismiss the dialog by pressing **Esc**.

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

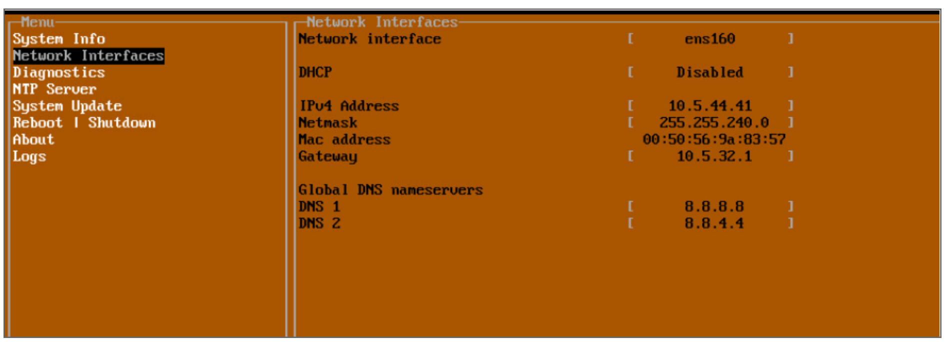
System Info



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

- **GUID** – Every On-Premises Analytics instance has a GUID which is displayed here.
- **System Time** – This is the current system time on the NSM On-Premises instance.
- **Up Time** – This is the total time that the NSM On-Premises instance has been running.
- **Load Average** – This shows the average CPU load for the last 1 minute, 5 minutes and 10 minutes. You can change the Average load time durations to view the CPU load over longer or shorter time periods.

Network Interfaces

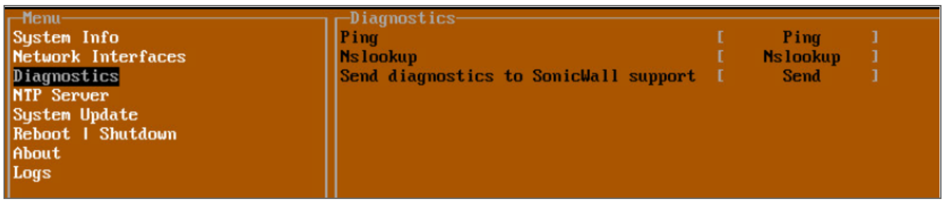


In the **Network Interface** screen, you can configure these settings.

- **Network Interface** – This is the current interface serving as the management interface. This defaults to ens160.
- **DHCP** - This displays if the DHCP is enabled or disabled.
- **IPv4 Address** – This is the IPv4 address currently assigned to the management interface.
- **Netmask** – This is the netmask currently assigned to the management interface.
- **Mac Address** – This is the MAC address of the management interface.
- **Gateway** – This is the default gateway currently in use by the NSM On-Premises instance.
- **DNS** – This is a list of the DNS servers currently being used by the NSM On-Premises instance.

Diagnostics

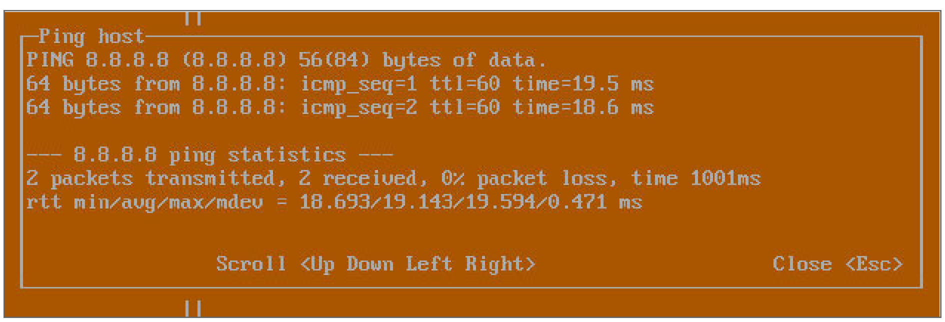
The **Diagnostics** screen provides the **Ping** and **Nslookup** tools to test connectivity between the management interface and the local network. **Ping** is used to test whether hosts in the network are reachable. **Nslookup** is available for sending DNS queries from the NSM On-Premises instance. Another option is to **Send diagnostics to SonicWall support**.



To use ping:

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

   The ping output is displayed in the Ping host dialog.

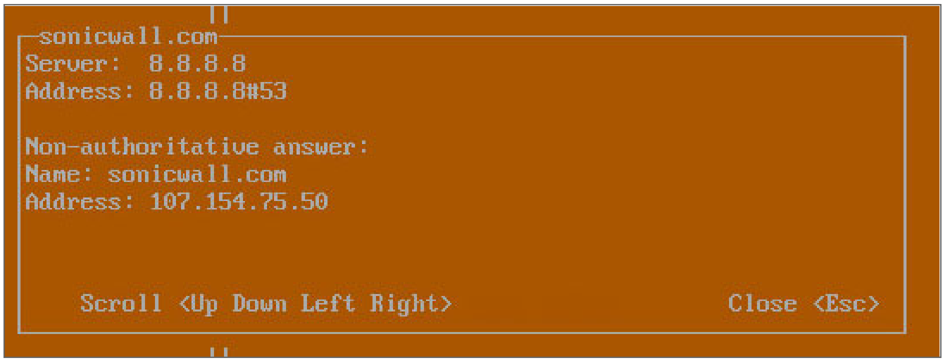


5. Press the **Esc** key to close the dialog.

To use Nslookup:

1. Select **Diagnostics** in the Menu and press **Tab** to move the focus into the **Diagnostics** screen.
2. Select **Nslookup** to highlight it and press **Enter** to display the **Enter** hostname dialog.
3. Navigate into the dialog, press **Backspace** to clear the current value, and then type in the hostname that you want to look up with a DNS query.
4. Press **Enter**.

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



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

To send Diagnostic Report:

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

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

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

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

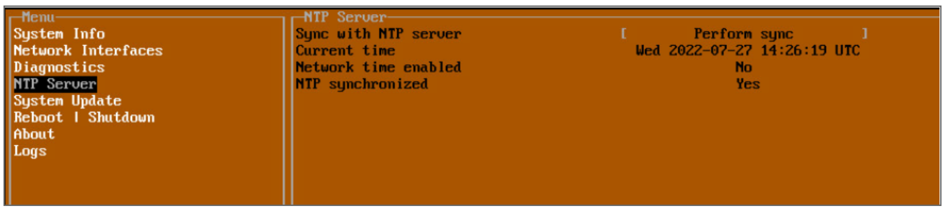
Common reasons for the report failing to send include:

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

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

NTP Server

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

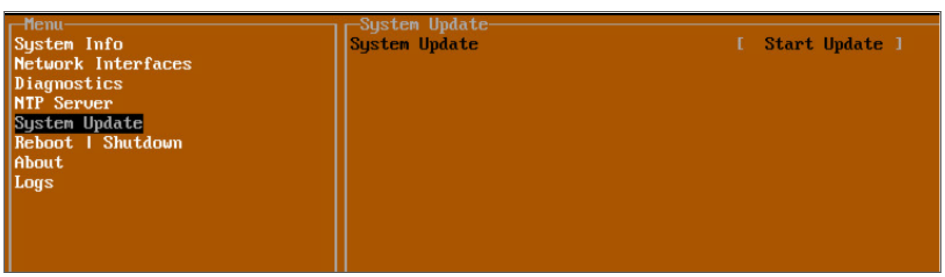


The **NTP Server** screen displays the following information:

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

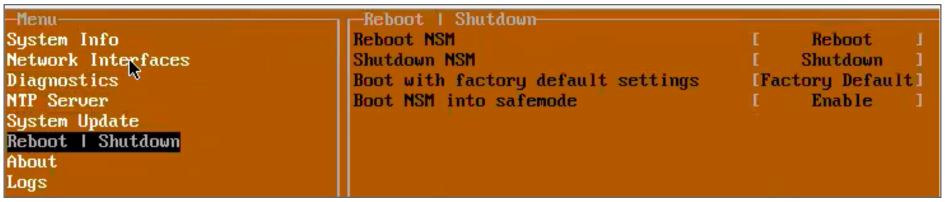
System Update

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



Reboot/Shutdown

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



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

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

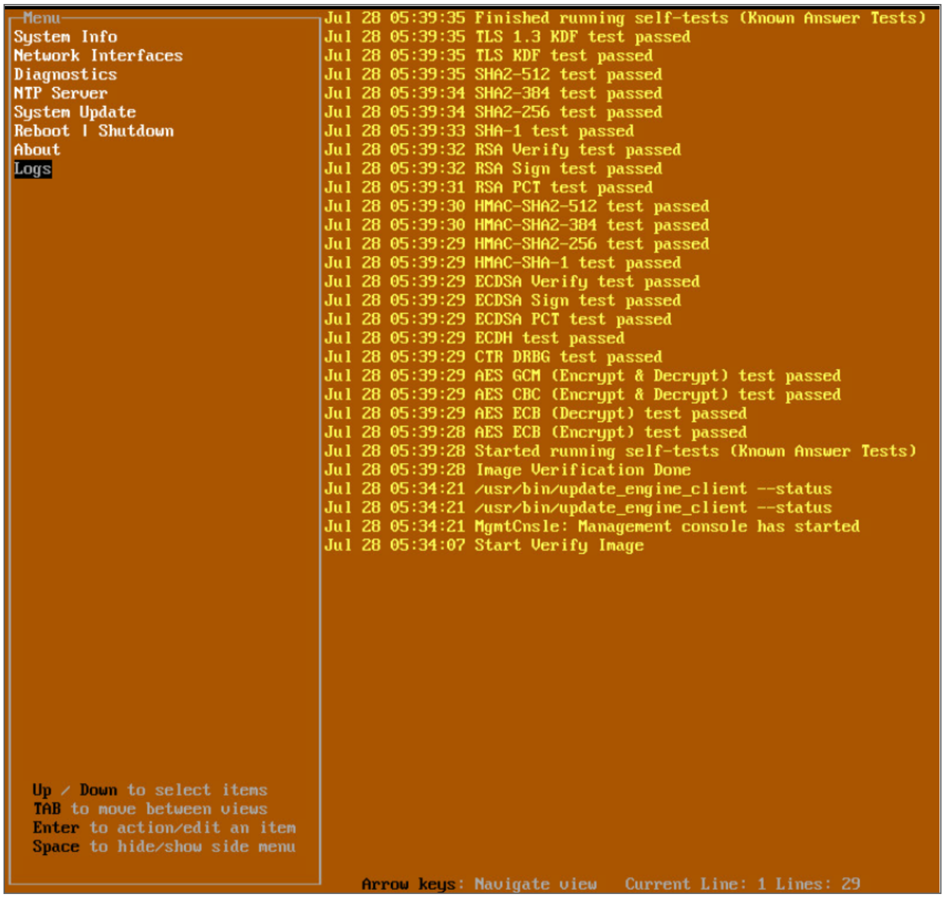
- **Reboot GMS**– Restarts the instance with current configuration settings.
- **Shutdown GMS** – Powers off the instance.
- **Boot with factory default settings** – Restarts the instance using factory default settings. All configuration settings are erased.
- **Boot GMS into safeMode** – Puts the NSM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

About

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

Logs

The Logs screen displays log events for the instance.

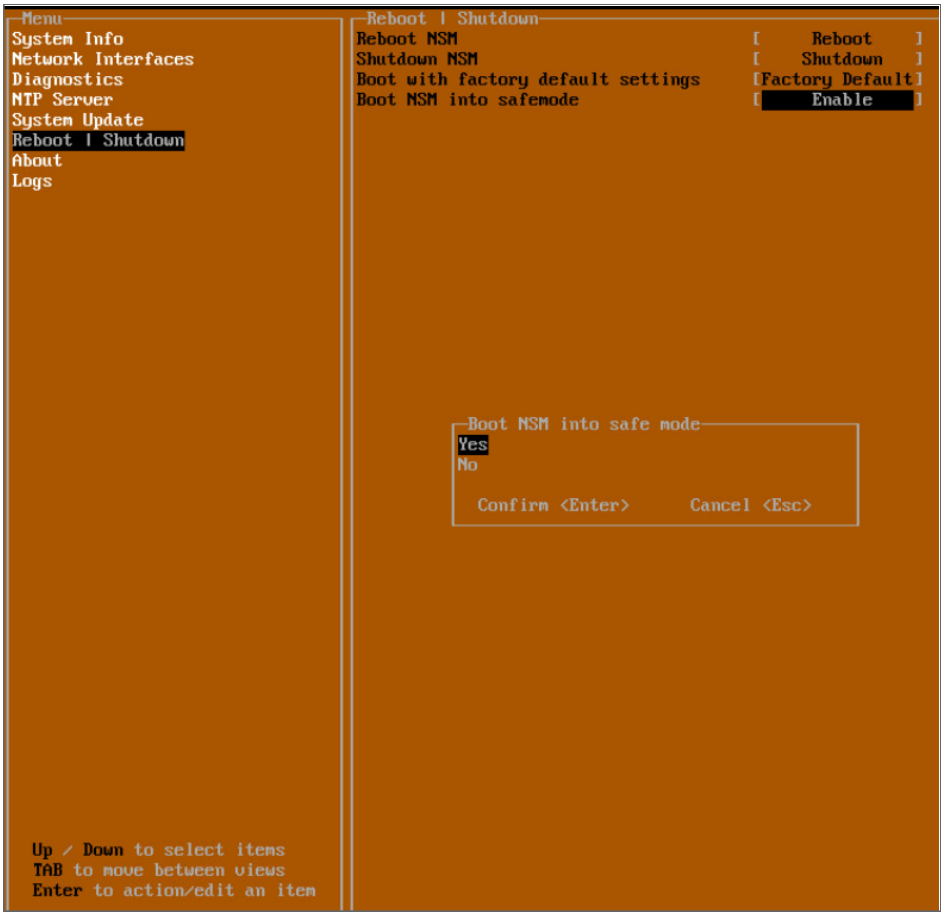


Using SafeMode on the Management Console

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

Enabling SafeMode

SafeMode can be enabled from the management console.



To enable SafeMode:

1. Access the NSM On-Premises through the respective virtual machine monitor remote console.
2. In the console, select the **Reboot | Shutdown** option and then press **Enter**.
3. Navigate down to the **Boot SonicWall into safemode** option to highlight **Enable**, and then press **Enter**.
4. Select **Yes** in the confirmation dialog.
5. Press **Enter**.

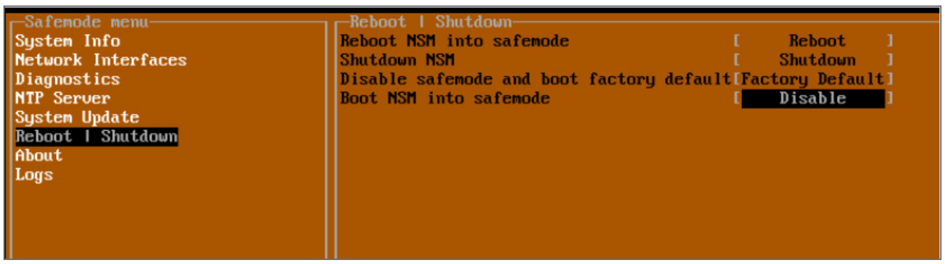
The NSM On-Premises instance immediately reboots and comes back up in SafeMode.

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

Disabling SafeMode

To disable SafeMode:

1. In the SafeMode menu in the Management Console, select the **Reboot | Shutdown** option and press **Enter**.
2. In the **Reboot | Shutdown** screen, navigate down to the **Boot SonicWall into SafeMode** option to highlight **Disable**, and then press **Enter**.
3. Select **Yes** in the confirmation dialog.
4. Press **Enter**.



The NSM On-Premises instance immediately reboots and boots up in normal mode.

Configuring Network Interfaces in SafeMode

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

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

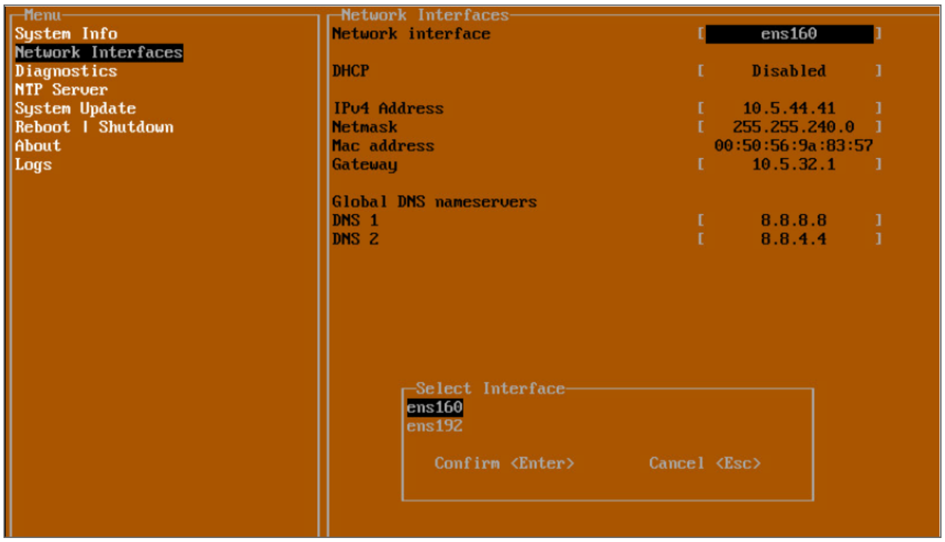
- **Network Interface** – This is the currently selected interface. This defaults to **ens160**. Use this to select any of the NSM On-Premises interfaces.
- **DHCP** – Determines whether addressing is static or handled automatically and dynamically by a DHCP server.
- **IPv4 Address** – The current IPv4 address currently assigned to the Management Interface.
- **Netmask** – The current Netmask assigned to the Management Interface.
- **Mac Address** – The MAC address of the Management Interface.
- **IPv6 Address** – The currently assigned IPv6 address of the Management Interface.
- **Gateway** – The current Default Gateway currently in use by the NSv appliance.
- **DNS** – A list of the current DNS servers currently being used by the NSv appliance.

Topics:

- Configuring Interface Settings
- Disabling an Interface

Configuring Interface Settings

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



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.

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

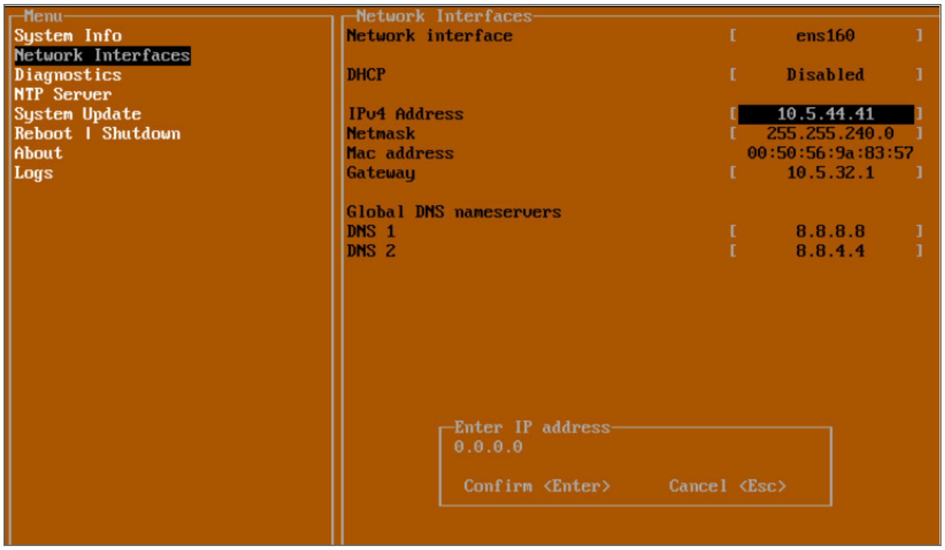
You can disable an interface while in SafeMode.

To disable an interface:

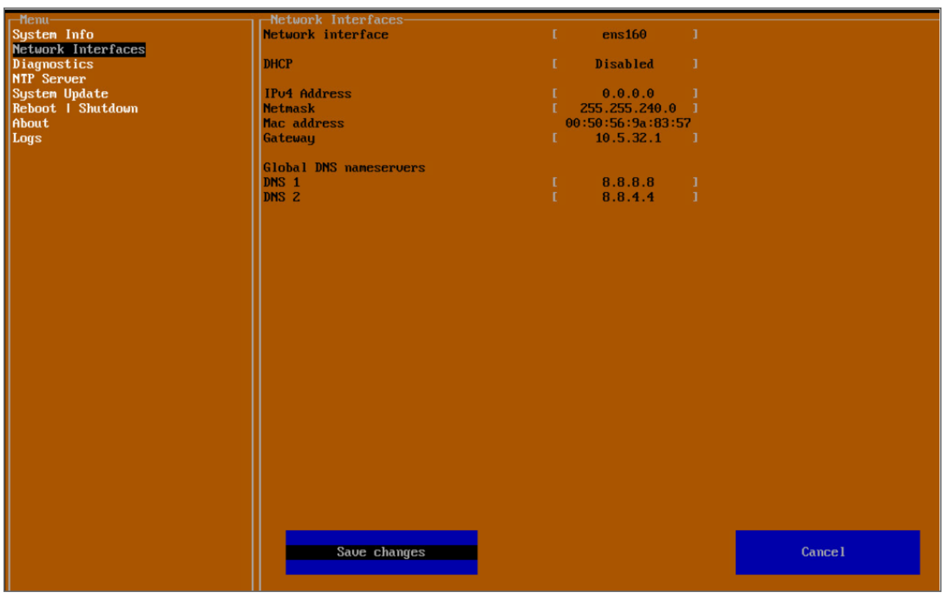
1. In the SafeMode **Network Interfaces** screen, select the **Network interfaces** option.
2. Select the interface you wish to edit and press **Enter**.
   The IPv4 and IPv6 addresses, Netmask, MAC address, Gateway, and DNS settings are displayed on the screen above the interface selection dialog.
3. 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**.



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



6. The interface is disabled.

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

Installing a Software Upgrade in SafeMode

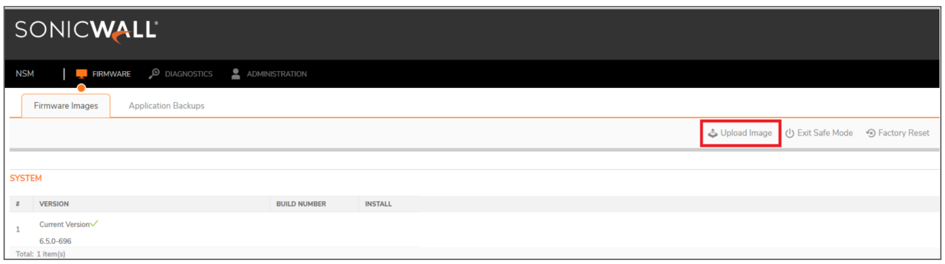
SWI files are used to upgrade NSM On-Premises. You can download the latest SWI image file from MySonicWall.

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.

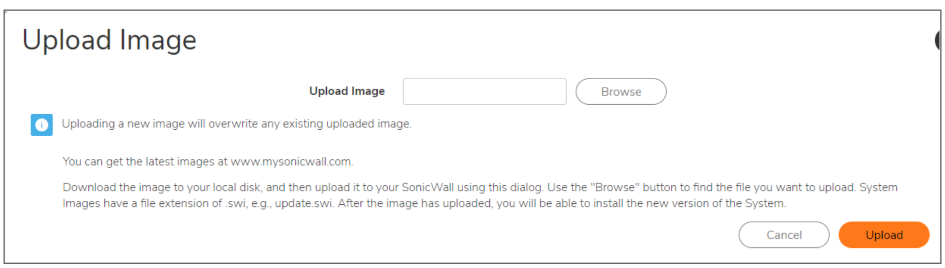
ⓘ | **NOTE:** In SafeMode, the web management interface is only available via **http** (not https).

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.



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



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

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

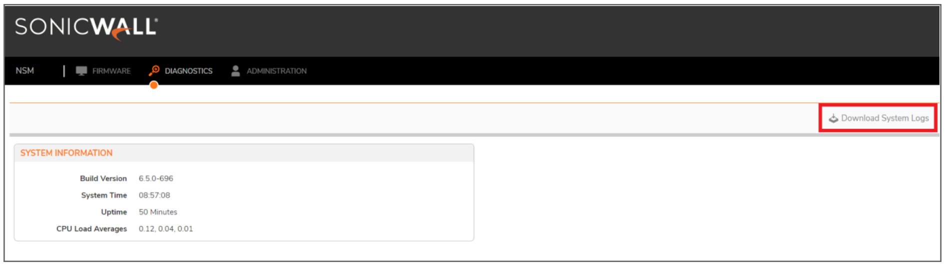
Downloading Logs in SafeMode

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.



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

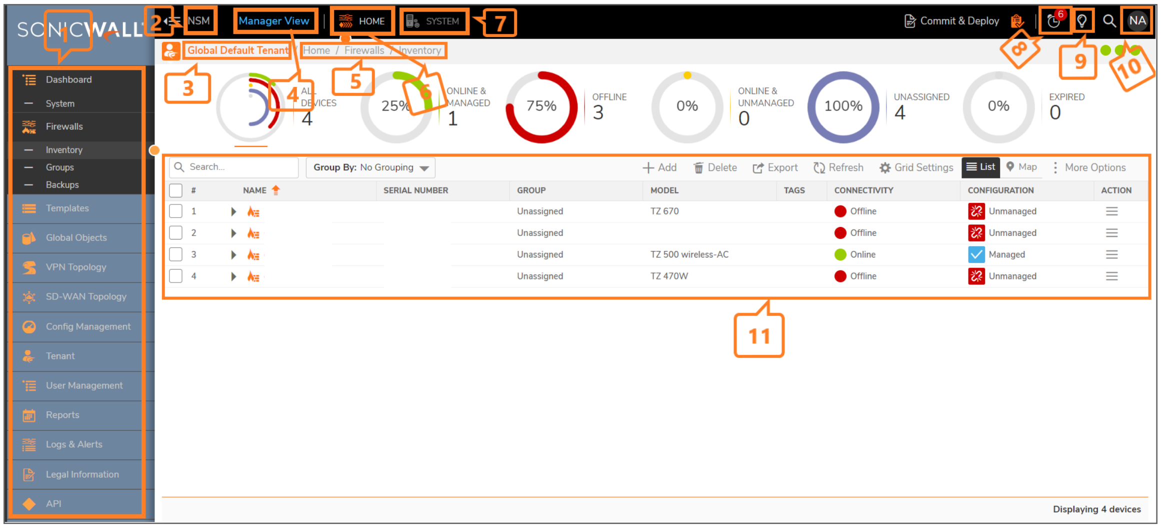
Once your NSM instance is operational, you can begin setting it up to manage your network. The instructions provided here are intended to help you get started, but for more detailed information refer to the *Network Security Manager Administration Guide* which is available at the Technical Documentation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



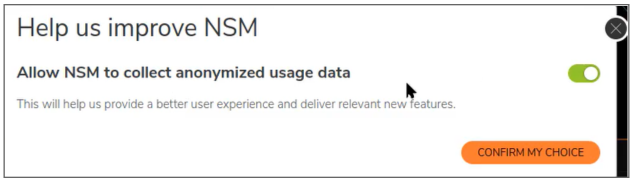
Reference	Interface Item	Description
1	Left command menu	Displays the primary tasks and commands that can be selected. The command menu varies depending upon which view you are in and the command option you have selected.
2	Show/hide commands icon	Acts as a switch to show or hide the left command menu.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

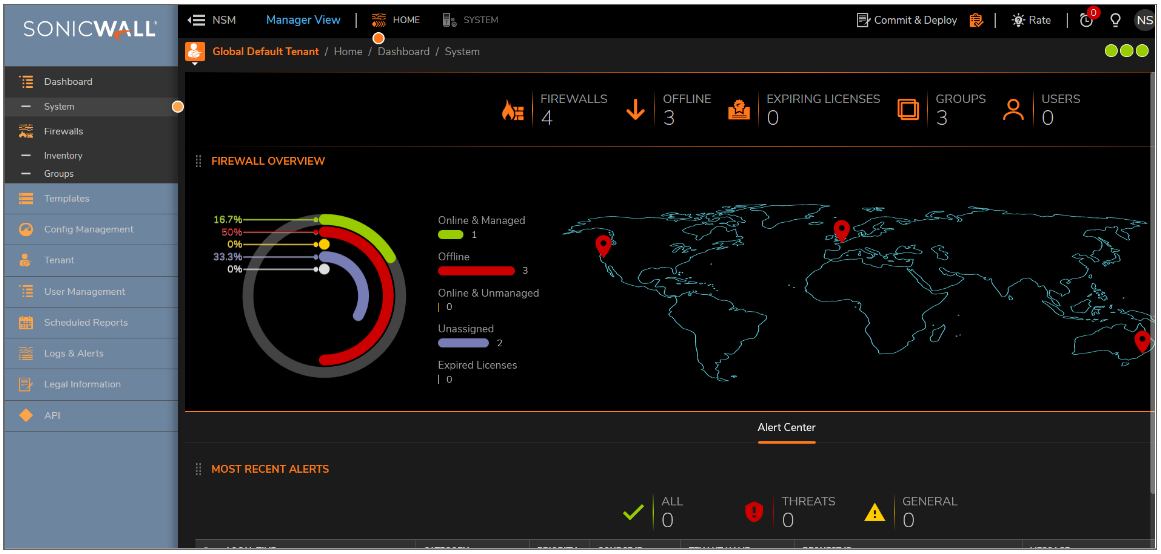
NOTE: Information on the **Commit & Deploy Wizard** is provided in the *Network Security Manager Administration Guide*.

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.



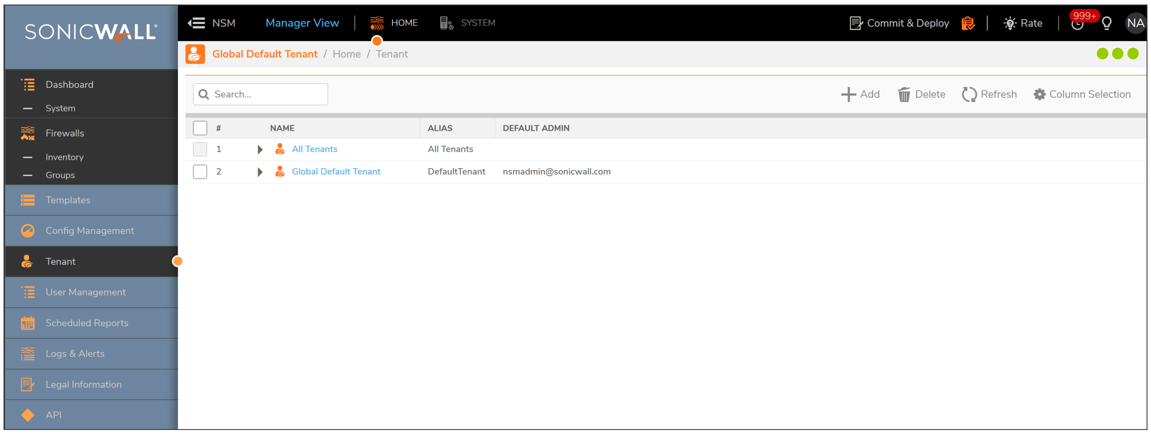


The three green notification icons at the top of the interface display more information on CPU Utilization, Memory Utilization, and Disk Utilization. Click on **View Details** to take a deep dive into the system monitoring details:

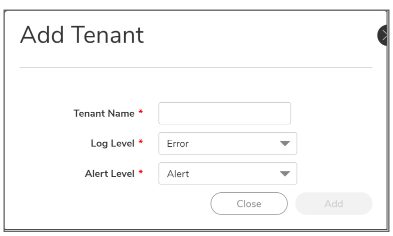
Creating a Tenant

To create a tenant on NSM:

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



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

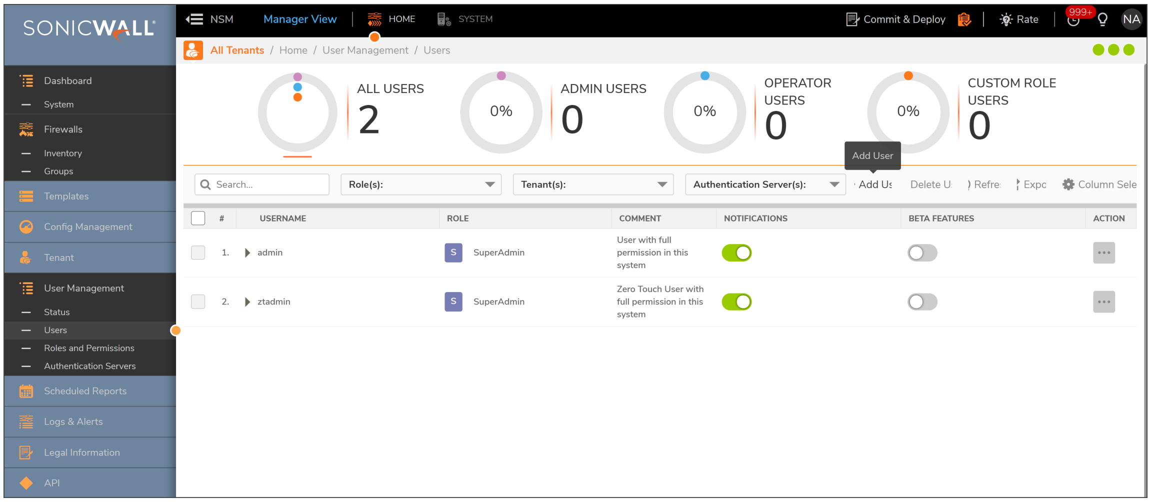


4. Click **Add**.
5. Register devices under the tenant.

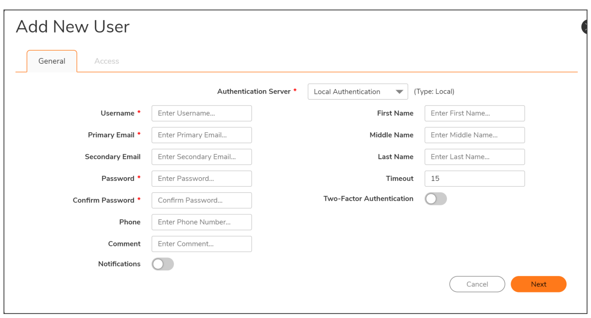
Creating a New User

To create users:

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

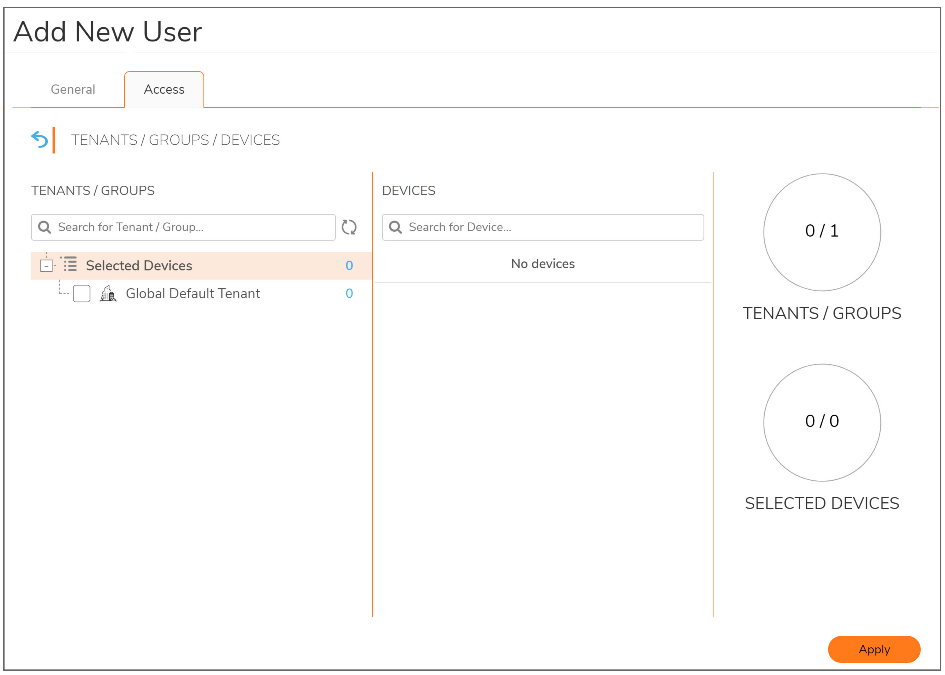


2. Click **Add User**.
3. In the **Add New User** window, enter details of the new user.



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**.

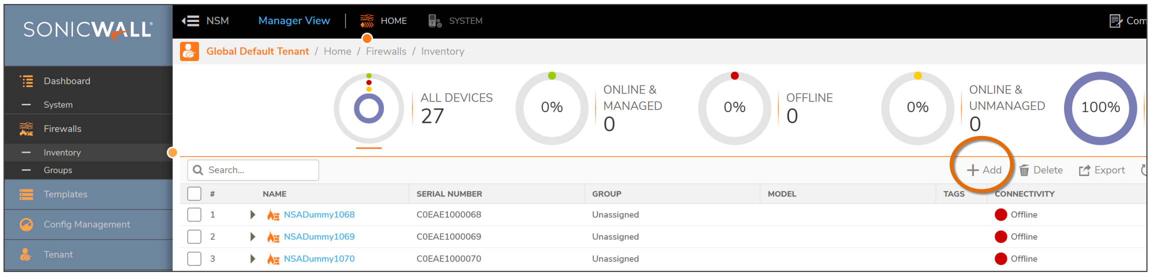


9. Select **TENANTS/GROUPS** and **DEVICES** from the options provided.
10. Click **Apply**.

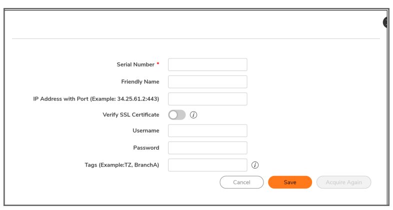
Adding a Device

To add a device to firewall inventory:

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



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



5. Click **Save.**

Integrate On-Prem Analytics with NSM

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

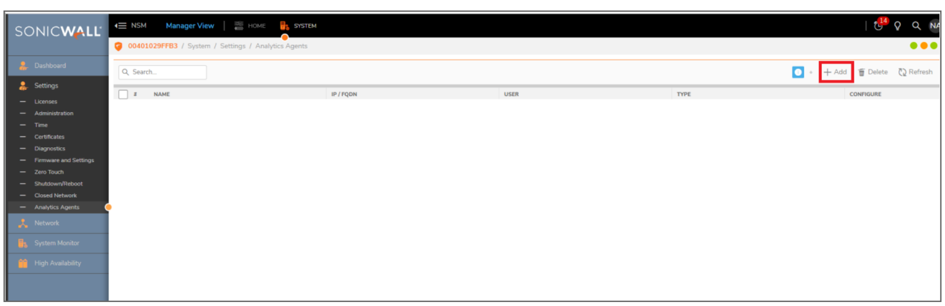
NOTE: Before proceeding with NSM integration please ensure desired SonicWall Analytics is working fine and firewall is configured to send data to analytics.

- Integrate SonicWall Analytics in NSM
- Enable Analytics While Adding a New Device
- Enable Firewall to View Analytics Data
- Accessing Analytics Data

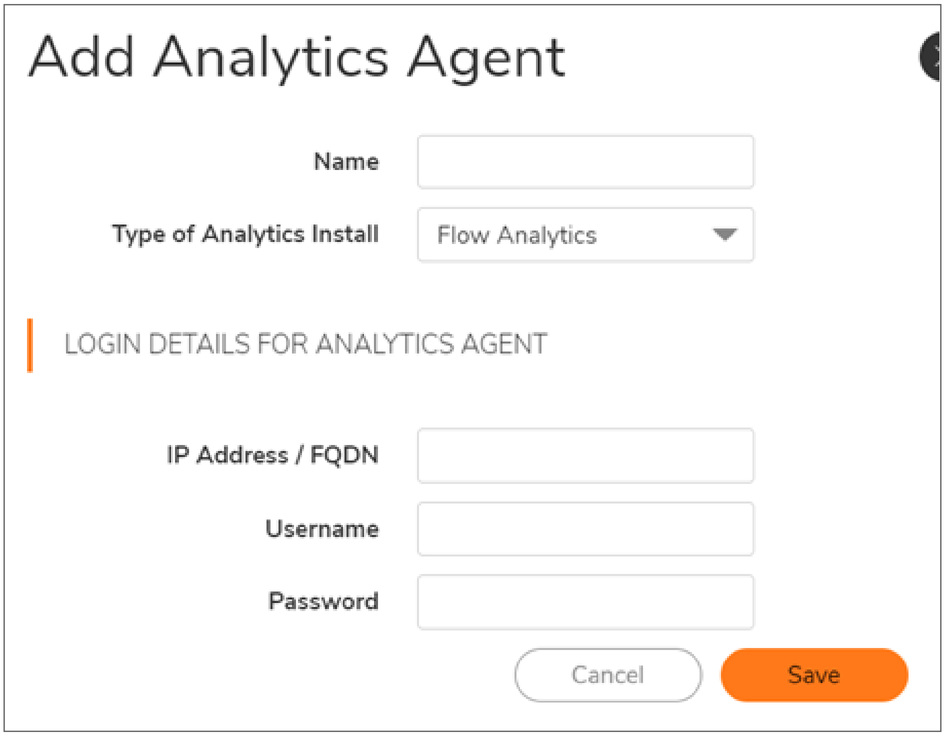
Integrate SonicWall Analytics in NSM

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.



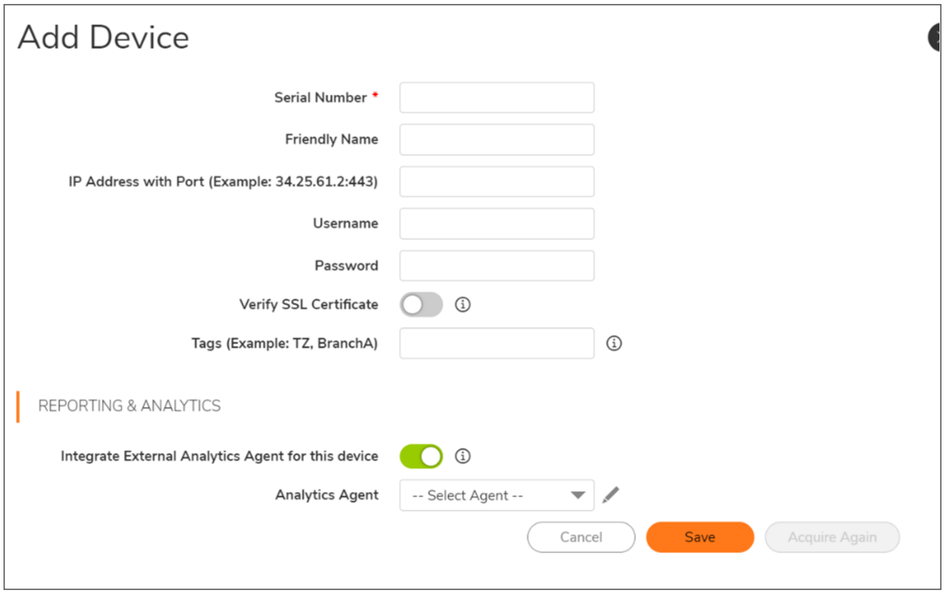
6. Click **Save**.

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.

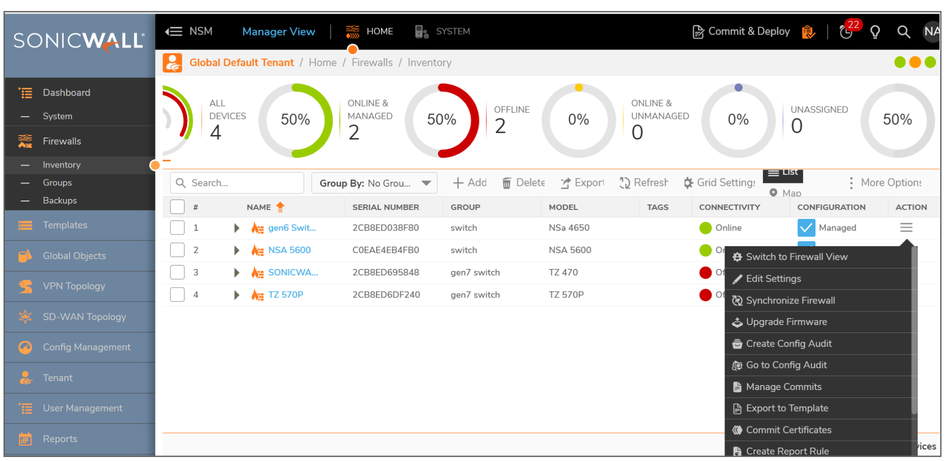


6. Click **Save**.

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**.

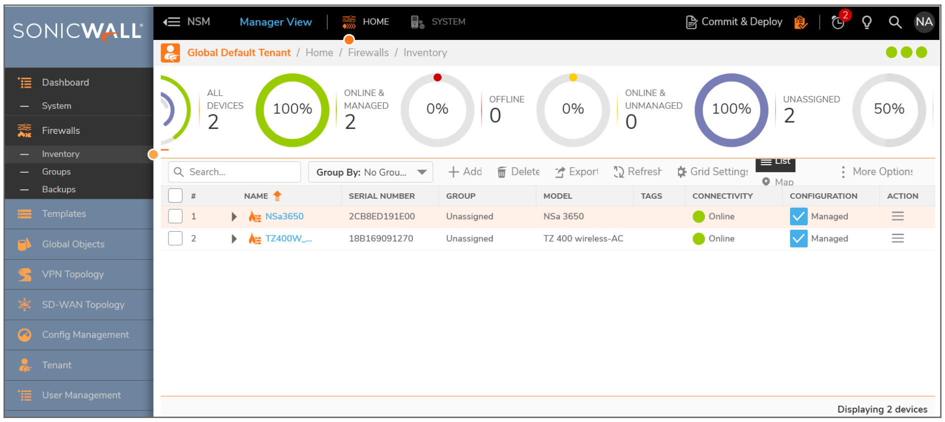


3. Under Reporting and Analytics, enable the **Integrate External Analytics Agent for this device** button.
4. Select the added analytics agent from the dropdown of **Analytics Agent** field.
5. Click **Save**.

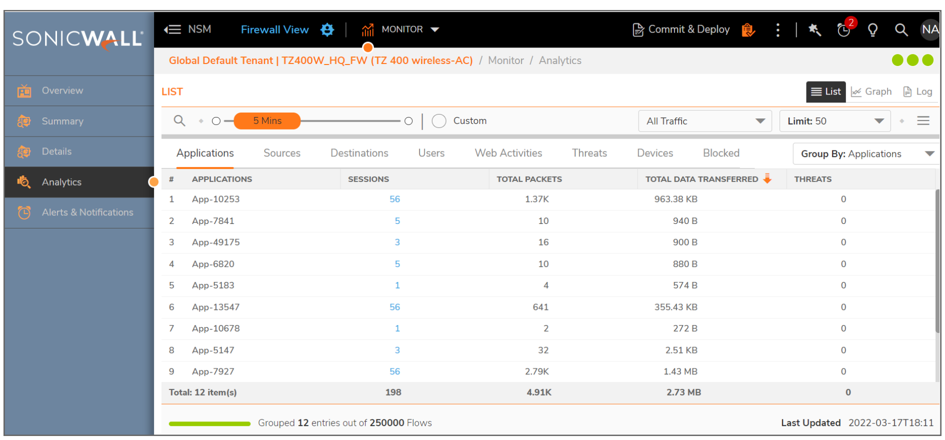
Accessing Analytics Data

To access analytics data in NSM:

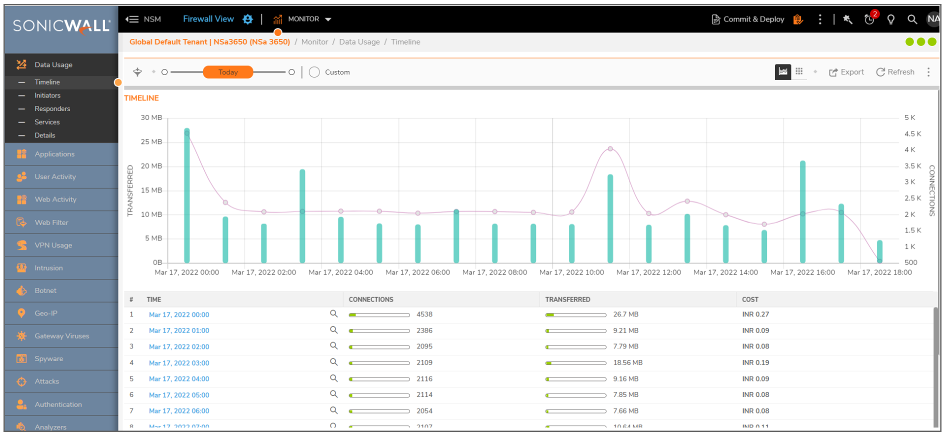
1. Under Home, navigate to **Firewalls > Inventory**.
2. Click on the firewall which you have integrated with either IPFIX or Syslog to view that particular Firewall View.



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



- **Syslog**



11

Upgrade Instructions

This section describes more about the following topics:

- Upgrade Using Management Console
- Upgrading SonicOS Firmware

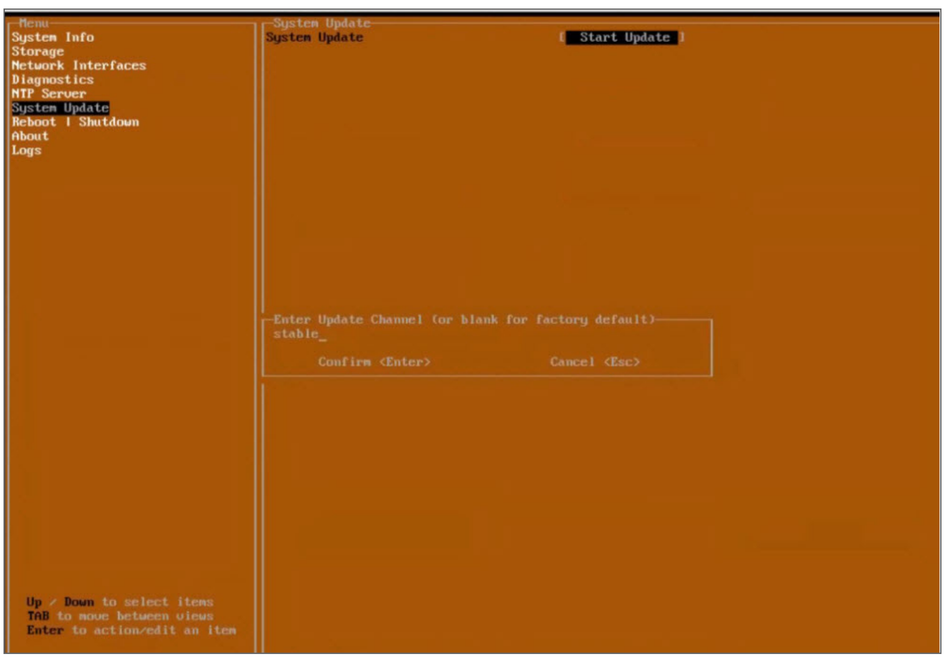
ⓘ **IMPORTANT:** Before upgrading your NSM system, take a backup of your configuration. Follow the steps provided in Taking Backup of NSM On-Premises before Upgrade.

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.

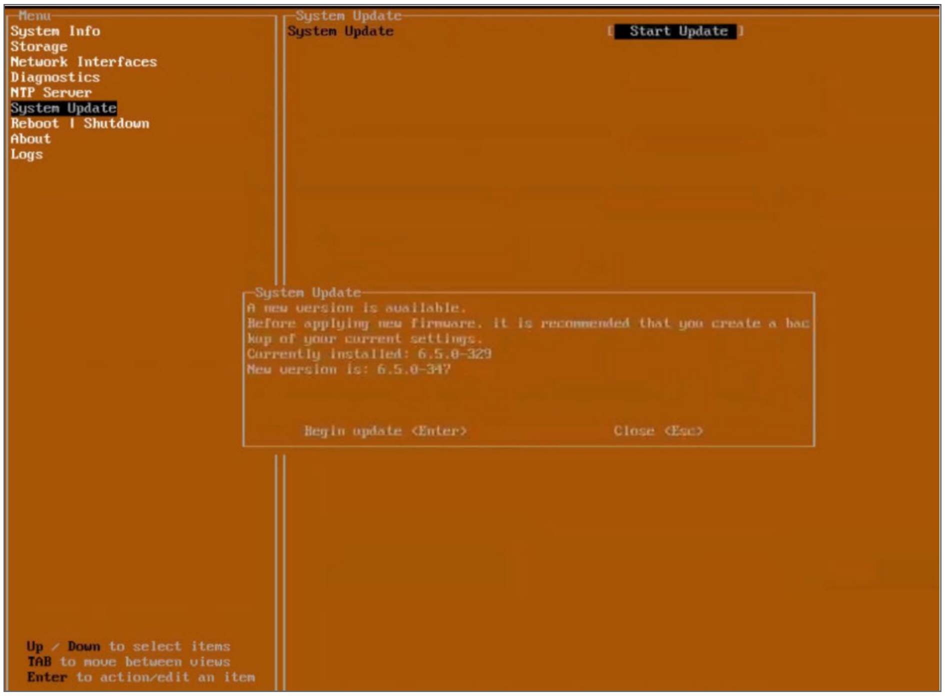
1. Open the NSM Management Console in an NSM On-Premises Virtual Machine.
2. Right click the VM and click **Open Console**. Ensure that NSM on-premises virtual machine has access to internet.
3. Open **Network Interfaces** menu and make any changes to network configuration, if required.
4. Navigate to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

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



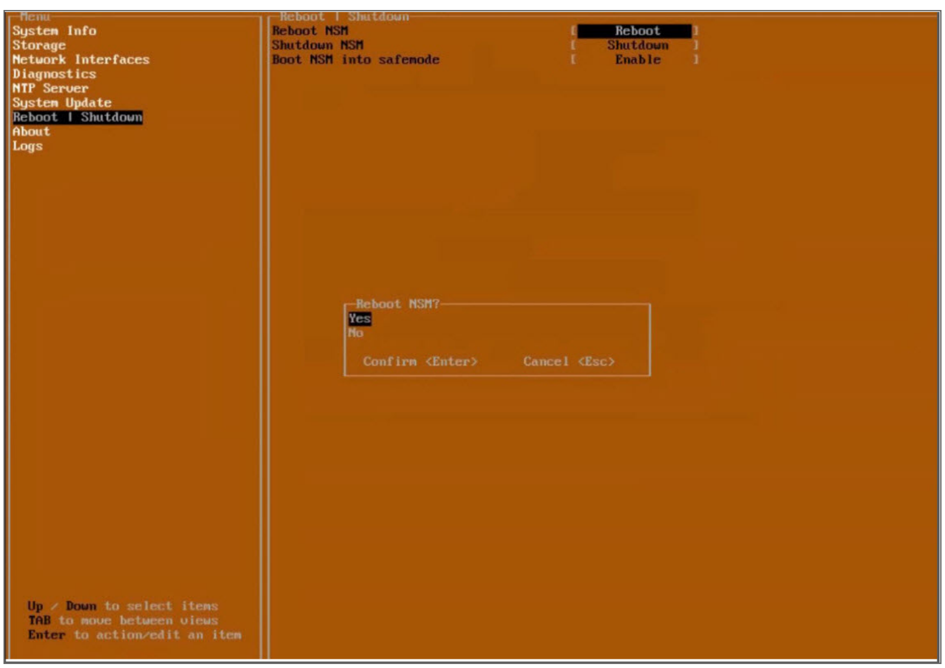
IMPORTANT: Updates are provided over update channels. The default channel is **Stable**.

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**.



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

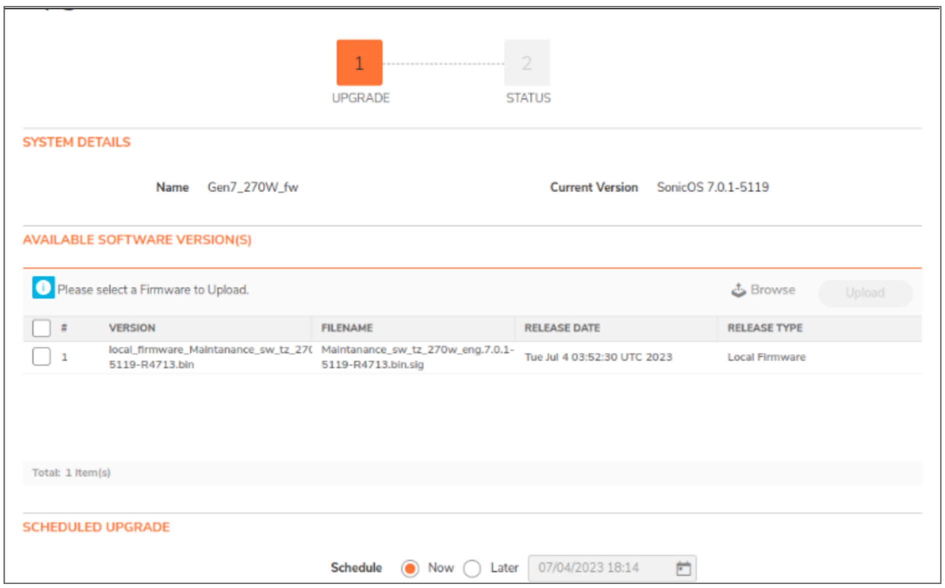


9. Log in and navigate to **SYSTEM > Settings > Firmware and Settings** to confirm that the firmware is updated.

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.



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

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

12

SonicWall Support

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

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

The Support Portal enables you to:

- View knowledge base articles and technical documentation
- View and participate in the Community forum discussions at https://community.sonicwall.com/technology-and-support.
- View video tutorials
- Access https://mysonicwall.com
- Learn about SonicWall Professional Services
- Review SonicWall Support services and warranty information
- Register for training and certification
- Request technical support or customer service

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

About This Document

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

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