

Network Security Manager

On-Premises System

Administration Guide

SONICWALL[®]

Contents

About Network Security Manager	4
About NSM	4
About the System Option	5
Conventions	5
Guide Conventions	6
UI Conventions	7
Related Documents	7
 Dashboard	 9
System Information	10
CPU Usage	10
Memory Usage	11
Network Interfaces	11
Disk Usage	12
Active Users	12
 Settings	 13
Licenses	13
Administration	14
Time	16
Setting Time	17
Adding an NTP Server	17
Deleting an NTP Server	18
Certificates	18
Common Access Card (CAC) Authentication	19
Diagnostics	21
Diagnostics Tests	21
Tech Support Report	22
Firmware and Settings	23
Backups/Restore Feature	23
Configure a Scheduled NSM File System Backup	24
Configure a Scheduled NSM File System Backup via SCP	25
View NSM File System Backups	27
Create a NSM File System Backup	27
Create SCP of a NSM File System Backup	29
Import a NSM File System Backup	29
Export a NSM File System Backup	31

Delete a NSM File System Backup	32
Restore NSM to a File System Backup	33
Backup/Restore NSM using Safemode	35
Zero Touch	38
Shutdown/Reboot	38
Closed Network	39
Network	41
Settings	41
Interface	42
Routes	42
System Monitor	44
Settings	44
Live Monitor	45
Process/Service Monitor	45
System Report	46
High Availability	47
Status	47
Settings	48
Advanced Settings	49
Virtual IP	49
HA Modes and Terminologies	50
Backup/Restore in High Availability Setup	51
Configure a Scheduled Backup in High Availability Setup	51
Restore Feature in High Availability Setup	52
NSM Management Console	56
Upgrade Instructions using Upgrade Package	56
Upgrade Instructions without Upgrade Package	59
SonicWall Support	62
About This Document	63

About Network Security Manager

SonicWall® Network Security Manager is a web-based application that centralizes management for the SonicWall family of network security appliance and web services. This on-premises solution automates the steps to set up an appliance and offers robust reporting and management tools.

Topics:

- [About NSM](#)
- [About the System Option](#)
- [Conventions](#)
- [Related Documents](#)

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 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.

The on-premises solution enables organizations to centrally and reliably manage a single small network to one or more enterprise-class deployments with the flexibility to scale without increasing management and administrative overhead. NSM offers many salient features:

- 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.
- High Availability that allows two identical NSMs to be configured to provide a reliable continuous connection to the public internet.
- Azure and KVM hypervisor deployments.

- Account Lockout feature, designed to prevent unauthorized access to the Network Security Manager environment and other brute-force attacks, social engineering, and phishing. This disables the user account if incorrect passwords are entered after a specified number of failed attempts during a given period. Admin can set the lockout duration until the locked account is released either after a specified time or manually done by an administrator when three unsuccessful log in attempts in 15 minutes are exceeded.
- Certificate management feature that enables a user interface to facilitate the management of digital certificates for all Network Security Manager managed firewalls. This enhances trust established between parties in a secure communication session.
- NSM adds support for the firewall series Gen 7 NSa 2700 and TZ Series (270, 370, and 470) running SonicOS as well as NSsp and Gen 7 NSv, with multi-tenancy and unified policy management features.
- Login To Unit that provides admins a fast and easy access to the managed firewall device-level UI directly from the device inventory page of Network Security Manager.
- Multi-Device Upgrade Feature to upgrade multiple firewalls from a group of devices in NSM instead of manually upgrading each firewall. Admins can execute them using NSM APIs as well.
- Security feature to grant admin rights based on specific IP address ranges. The IP restrictions can be added in 3 formats - single IP, an IP range, or a specific network with a subnet mask.
- Configure or edit virtual or network interfaces using templates.

NSM can manage both Gen6 and Gen7 SonicWall firewalls. SonicOS 6.5.4.6 is the recommended version, but NSM can on-board the older Gen6 Firewall versions as well.

About the System Option

The **System** command set provides a centralized user interface, where the administrator can manage and monitor the on-premises NSM solution. You use the commands associated with the **System** option to configure NSM, manage NSM performance, monitor activities, and manage upgrades and licensing. The tools supporting this task include:

- Dashboard
- Settings for the NSM application
- Network settings, interfaces, and routes
- Monitoring for the system parameters that comprise the on-premises solution
- High Availability option to provide a reliable continuous connection to the public internet.

Conventions

The Network Security Manager On-Premises SystemAdministration Guide makes use of the following conventions:

- [Guide Conventions](#)
- [UI Conventions](#)

Guide Conventions

The following text conventions are used in this guide:

Convention

Bold text

Menu view or mode | Menu item > Menu item

Computer code

<Computer code italic>

Italic

Use

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.

Indicates a multiple step menu choice on the user interface. For example, **Manager View | HOME > Firewall > Groups** means that you are in the Manager View with the **HOME** option selected. Then click on **Firewall** in the left-hand menu, and select **Groups**.

Indicates sample code or text to be typed at a command line.












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=C0ABC00000321.

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.

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. Also indicates that a configuration is in sync and acquired.
	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 or a warning. 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:
	Indicates an alert.
	Indicates the device is online.
	Indicates the device is offline.
	Indicates unmanaged devices.
	Indicates managed devices.
	Indicates that Zero Touch Connection is disabled for a device.

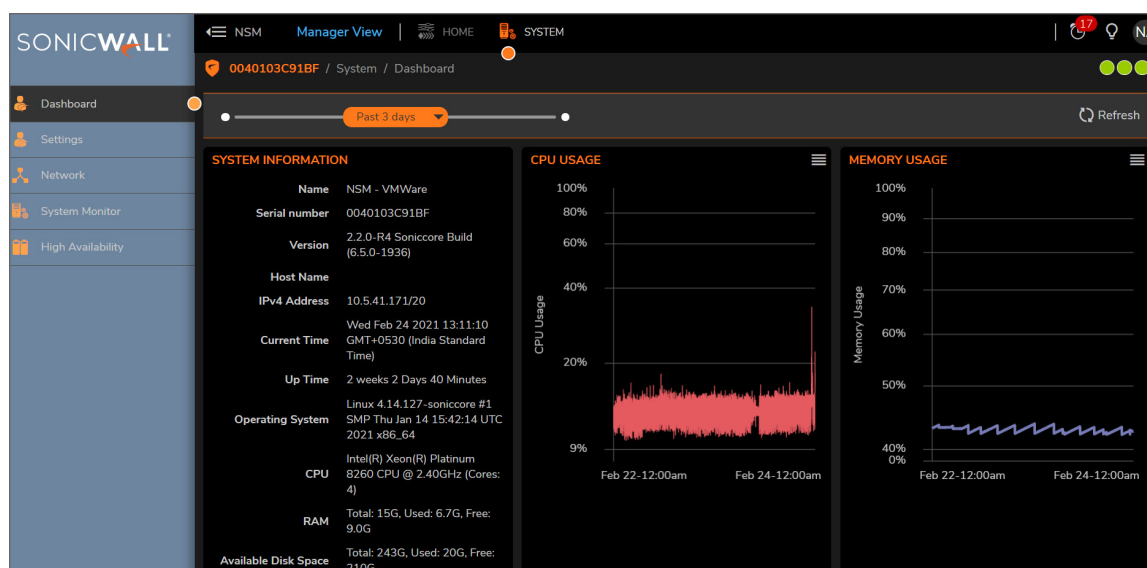
Related Documents

The NSM documentation includes the following:

- *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**.
- The *Network Security Manager Getting Started Guide* describes how to license and configure a basic NSM setup.
- The *NSM Administration Guide* reviews the management tasks for administering your security infrastructure.
- The *Network Security Manager Reporting and Analytics Administration Guide* discusses how to use the reporting and analytics features.
- *Network Security Manager On-Premises System Administration* describes the system administration tasks for an on-premises deployment of NSM.
- The *NSM Release Notes* summarizes the new features for the product.

Dashboard

The System Dashboard provides information and status for the On-Premises NSM implementation.



You can customize the interval for the Dashboard by sliding the orange bar above the graphs to the left or the right. You can select one of several predefined intervals. The ranges differ from the **Past 24 hours** to the **Past 5 days**. Refresh the data by clicking the **Refresh** icon on the right.

The data in the Dashboard includes:

- System Information
- CPU Usage
- Memory Usage
- Network Interfaces
- Disk Usage
- Active Users

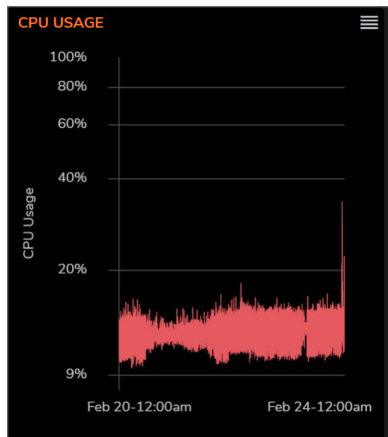
System Information

The information about the system hosting the On-Premises NSM is displayed in the upper left tile on the **Dashboard**. This is a read only data; the tile has no active links.

SYSTEM INFORMATION	
Name	NSM - VMWare
Serial number	0040103C91BF
Version	2.2.0-R4 Soniccore Build (6.5.0-1936)
Host Name	
IPv4 Address	10.5.41.171/20
Current Time	Wed Feb 24 2021 13:11:10 GMT+0530 (India Standard Time)
Up Time	2 weeks 2 Days 40 Minutes
Operating System	Linux 4.14.127-soniccore #1 SMP Thu Jan 14 15:42:14 UTC 2021 x86_64
CPU	Intel(R) Xeon(R) Platinum 8260 CPU @ 2.40GHz (Cores: 4)
RAM	Total: 15G, Used: 6.7G, Free: 9.0G
Available Disk Space	Total: 243G, Used: 20G, Free: 210G

CPU Usage

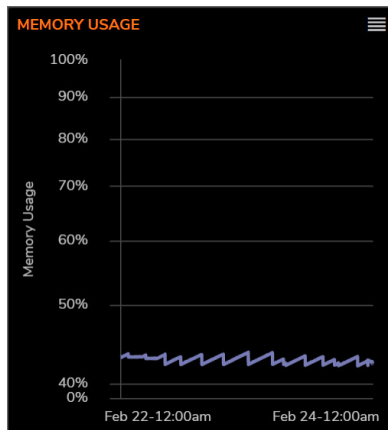
The CPU Usage tile summarizes the CPU usage in graph form. You can easily see when the high and low usage times occur, and by adjusting the time interval to shorter period, you can see better granularity on the graph.



Click on the icon in the upper right corner to **Show System Report**. This redirects you to **System Monitor > System Report** to view a more detailed graph on CPU Utilization.

Memory Usage

The Memory Usage tile summarizes the memory usage in graph form. You can easily see when the high and low usage times occur, and by adjusting the time interval to shorter period, you can see better granularity on the graph.



Click on the icon in the upper right corner to **Show System Report**. This redirects you to **System Monitor > System Report** to view a more detailed graph on Memory Utilization.

Network Interfaces

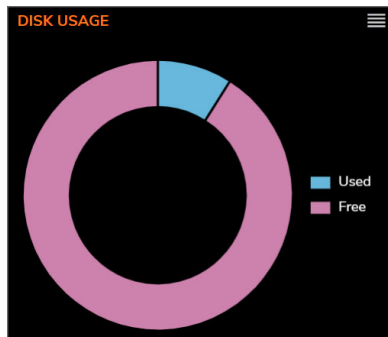
The Network Interfaces tile lists the network interfaces for your system. The icon shows the status of the interfaces.



Click on the icon in the upper right corner to **Show Network Interfaces**. This redirects you to **Network > Interfaces** to view the details on each interface.

Disk Usage

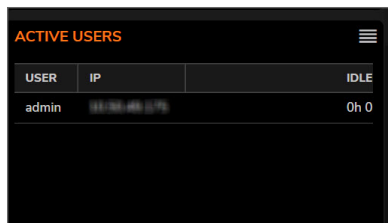
The Disk Usage tile summarizes the memory usage using a pie chart. Click on either the **Free** or **Used** segment to see the percentage allocated to each.



Click on the icon in the upper right corner to **Show System Report**. This redirects you to **System Monitor > System Report**; you may need to scroll down to view the Disk Utilization graph.

Active Users

The Active Users tile lists the users who are currently logged in.



A table titled "ACTIVE USERS" with a hamburger menu icon in the top right. The table has three columns: "USER", "IP", and "IDLE". There is one row of data showing the user "admin" with an IP address of "10.10.10.10" and an idle time of "0h 0".

USER	IP	IDLE
admin	10.10.10.10	0h 0

Click on the icon in the upper right corner to **Show Active Users**. This redirects you to **Home | User Management > Status** to view more information about the user and their session. You can also log out a user from this page.

Settings

Most of the tasks for setting up NSM for an on-premises implementation are grouped under settings.

Topics:

- [Licenses](#)
- [Administration](#)
- [Time](#)
- [Certificates](#)
- [Diagnostics](#)
- [Firmware and Settings](#)
- [Zero Touch](#)
- [Shutdown/Reboot](#)
- [Closed Network](#)

Licenses

Manage your NSM licenses by navigating to **System | Settings > Licenses**.

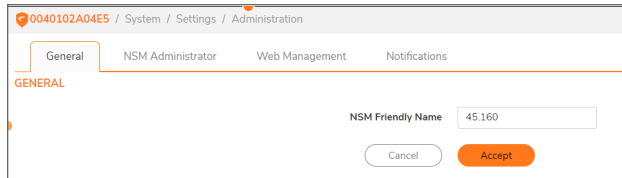
SERVICES	STATUS	EXPIRY DATE	ACTIONS
▼ Security Service Info (1 licensed) Network Security Manager	Licensed Count: 5	08 Feb 2022	Upgrade Renew
▼ Support Service Info (1 licensed) 24x7 Support	Licensed	08 Feb 2022	

The Licenses page lists both your Security Services and the Support Service information. You can quickly confirm the status of licensing, count, the expiration date and action status of each.

From this page you can also upgrade your NSM, start a trial, renew, or activate service.

Administration

Set your NSM administrative settings by navigating to **System | Settings > Administration**.

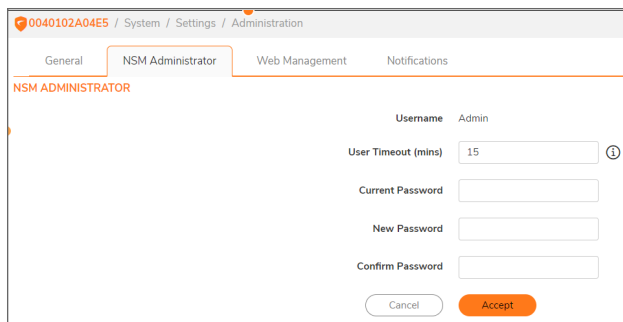
A screenshot of the NSM Administration interface. The breadcrumb trail at the top reads "0040102A04E5 / System / Settings / Administration". Below this is a tab bar with four tabs: "General", "NSM Administrator", "Web Management", and "Notifications". The "General" tab is selected and highlighted with an orange border. Below the tabs, the text "GENERAL" is displayed in orange. The main content area contains a label "NSM Friendly Name" followed by a text input field containing the value "45.160". At the bottom of the form are two buttons: "Cancel" and "Accept".

To name your system:

1. Navigate to **System | Settings > Administration**.
2. On the **General** tab, enter the **NSM Friendly Name** in the field provided.
3. Click **Accept**.

To set up your administrator settings:

1. Navigate to **System | Settings > Administration**.

A screenshot of the NSM Administration interface, showing the "NSM Administrator" tab selected. The breadcrumb trail at the top is "0040102A04E5 / System / Settings / Administration". The tab bar shows "General", "NSM Administrator", "Web Management", and "Notifications", with "NSM Administrator" highlighted. Below the tabs, the text "NSM ADMINISTRATOR" is displayed in orange. The main content area contains the following fields: "Username" with the value "Admin", "User Timeout (mins)" with a value of "15" and an information icon, "Current Password", "New Password", and "Confirm Password". At the bottom are "Cancel" and "Accept" buttons.

2. Select the **NSM Administrator** tab.
3. Enter the **User Timeout** in minutes. If set to **-1**, NSM never logs out.
4. Type the **Current Password**.
5. Enter the **New Password** and confirm it.
6. Click **Accept**.

To define the web management settings:

1. Navigate to **System | Settings > Administration**.
2. Select the **Web Management** tab.

3. Enter the **HTTPS Port** in the field provided.
4. Select **Certificate** from the drop-down list. You can manage Certificates from **Settings > Certificates**.
5. Toggle the button to enable or disable **Digital Certificate Authentication**. Enabling this option lets you to login using CAC authentication.
 ⓘ | **NOTE:** If you change this setting, it may disconnect and log out all users.
6. Click **Accept**.

Notifications - SMTP Settings

To define the mail server settings

1. Navigate to **System | Settings > Administration > Notifications**.
2. Select the **SMTP Settings** tab.

3. Enter the name or IP address for the **Mail Server** in the field provided.
4. Define the **From E-mail address**.
5. Select **Advanced Settings** to view more options.
6. (Optional) Select **Skip TLS Cert Verification** if you want to skip the TLS certificate verifications.
7. Specify the **SMTP Port**.

8. Select the **Connection Security Method**.
9. Select **Authentication Type**.
10. Specify the **User Name** and **Password**
11. Enter the **E-mail address** to which the notifications have to be sent. This is the mail address is used to receive messages sent from the system.

① **NOTE:** This mail address is used to send One Time Password for **Forgot Password** feature in the login page of NSM.
12. Click **Accept**.

Notifications - Twilio Settings

To define the Twilio settings

1. Navigate to **System | Settings > Administration > Notifications**.
2. Select the **Twilio Settings** tab.

3. **Account SID** - This acts as a user name. It can be found on your twilio project setting (<https://www.twilio.com/console/project/settings>) under the API credential.
4. **Authentication Token** - This acts as a password. It can be found on your twilio project setting (<https://www.twilio.com/console/project/settings>) under the API credential.
5. **Phone Number** - This should be same the as your Twilio registered number.
6. Click **Accept**.

Time

The Time page helps you set the system time and setup the Network Timer Protocol (NTP) servers.

Topics:

- [Setting Time](#)
- [Adding an NTP Server](#)
- [Deleting an NTP Server](#)

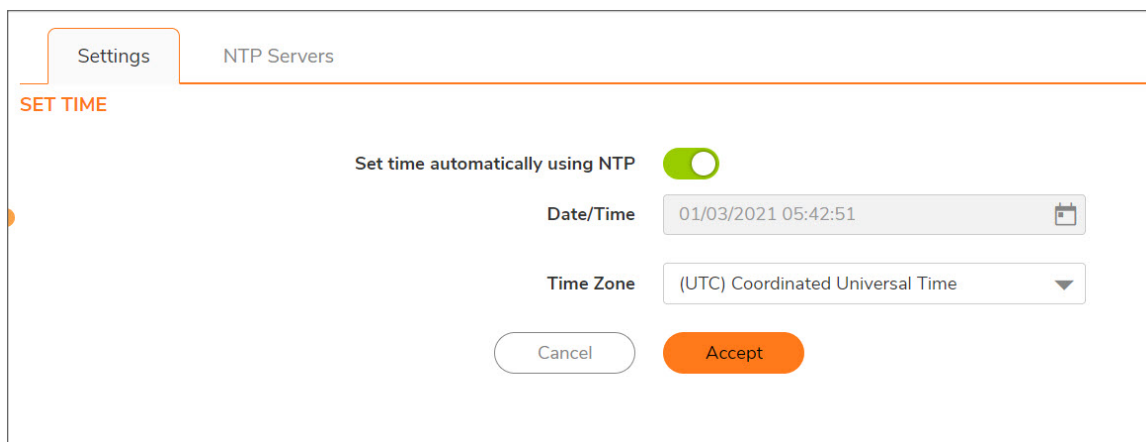
Setting Time

You can set the time to be managed using an NTP (Network Timer Protocol) server.

On the **Settings** tab, enable the switch for the option **Set Time automatically using NTP**.

To set the system time manually:

1. Navigate to **System | Time > Settings**.



2. Set the **Date/Time** using the icon in the field provided.
3. Select the **Time Zone**.
4. Click **Accept**.

Adding an NTP Server

To add an NTP server:

1. Navigate to **System | Settings > Time**.
2. Select the **NTP Servers** tab.
3. Click on **+Add**.



4. Enter the **NTP Server** in the field provided.
5. Click **Add**.

The server you have newly added appears in the list.

Deleting an NTP Server

To delete an NTP server:

1. Navigate to **System | Settings > Time**.
2. Select the **NTP Servers** tab.
3. Select the NTP Server you need to delete from the list.
4. Click **Delete**.
5. Click **OK** to confirm the deletion.

The server you have deleted is removed from the list.

Certificates

Manage your certificates on the **Certificates** page. Navigate to **System | Settings > Certificates** to see the list of certificates.

Search...

Generate Self Signed Certificate

Import

Delete

Refresh

<div><input type="checkbox"/></div>	#	CERTIFICATES	TYPE	VALIDATION	EXPIRATION	ACTION
<div><input type="checkbox"/></div>	1	localhost	RSA	2019-10-22 18:52:35	2029-10-19 18:52:35	<div><div></div></div>

The following functions can be used to manage your certificates:

Search	Use the Search function to find a specific certificate or filter to a set with similar parameters.
Generate Self Signed Certificate	Click this icon to generate a single certificate.
Import	To import a list of certificates: <ol style="list-style-type: none">1. Click the Import icon to a list of active certificates.2. Browse your computer for the folder name and select it.3. Enter the password if applicable.4. Click Upload.
Delete	Select the certificate you want to delete and click the Delete icon. You can select multiple certificates to delete at the same time.
Refresh	Clicking Refresh updates the certificate list.

There are two options to import the certificates -

- Local certificate with private key.
- CA certificate from encoded file.

❗ | **NOTE:** Only one certificate can be used as a CAC authentication certificate.

Select **Import a local end-user certificate with private key from a PKCS#12 (.p12 or .pfx) encoded file**.

Next, enter the **Certificate Name** and the **Certificate Management Password** (the password you defined when creating the .pfx file). Click **Import**.

Import a CA certificate from a PKCS#7 (.p7b), PEM (.pem) or DER (.der or .cer) encoded file

Click **Add File** and browse to locate and open your Certificate .pfx file. Click **Upload** to upload the selected certificate.

Common Access Card (CAC) Authentication

A **Common Access Card (CAC)** is a United States Department of Defense (DoD) smart card used by military personnel and other government and non-government personnel who require highly secure access over the Internet. A CAC uses PKI authentication and encryption. Using a CAC requires an external card reader connected on a USB port.

NSM on-prem supports CAC Authentication to authenticate the access to the NSM On-prem system.

In order to use the CAC authentication, you are required to set up the following

1. Import CA certificate in NSM through **System | Settings > User Management > Authentication Servers > Authentication type**. For more details, refer Authentication Servers.

Add Authentication Server

Settings Schema

Authentication Type * Digital Certificate ⓘ

Name * CAC

CA Certificate * blrgmsqa.com

+ Add CA Certificate

Save

2. **Create or Import Digital Authentication Certificate** – Create or import a digital certificate from a PKCS#7 (.p7b), PEM (.pem) or DER (.der or .cer) encoded file; or a local end-user certificate with private key from a PKCS#12 (.p12 or .pfx) encoded file. Refer [Certificates](#) to create or import digital authentication certificate.

ⓘ | **NOTE:** Only one certificate can be used as a CAC authentication certificate.

Import Certificate

☒ Import a local end-user certificate with private key from a PKCS#12 (.p12 or .pfx) encoded file

☐ Import a CA certificate from a PKCS#7 (.p7b), PEM (.pem) or DER (.der or .cer) encoded file

Password:

Please select a Certificate

Add File

Cancel Upload

3. Enable Digital Certificate Authentication under **System | Settings > Administration > Web Management**. Refer [Administration](#) section for more information.

ⓘ | **NOTE:** CAC option is shown only if this is enabled.

General NSM Administrator Web Management Notifications

WEB MANAGEMENT SETTINGS

HTTPS Port: 443

Certificate: localhost ⓘ

Digital Certificate Authentication: ☒

Cancel Accept

4. **Add User** - Choose Authentication server as **CAC** for the user. Navigate to **System | User Management > Users > Add User**.

ⓘ | **NOTE:** User name should match the Certificate common name.

Add New User

General Authentication Access

Authentication Server * Local Authentication (Type: Local)

Local Authentication

Username * admin

Primary Email * nsadmin@sonicwall.com

Secondary Email * user@access.com

Password * *****

Confirm Password * *****

Comment * User with full permission in

First Name * NSM

Middle Name * Enter Middle Name...

Last Name * Administrator

Phone * 0

Timeout * 60

Notifications ☒

Cancel Save

Diagnostics

On-Premises NSM provides tools for helping you diagnose issues with your system. Navigate to **System | Settings > Diagnostics**.

Diagnostics Tests Tech Support Report

Connectivity Trace Route Ping

Test All Test Selected

<input type="checkbox"/> TEST	TEST RESULTS	TIMESTAMP	PROGRESS
<input type="checkbox"/> License Manager Connectivity			
<input type="checkbox"/> Database Connectivity			

Topics:

- [Diagnostics Tests](#)
- [Tech Support Report](#)

Diagnostics Tests

The diagnostics tests tab provides the tools to validate connectivity, trace routes and ping an IP address.

Use the Connectivity tests to validate connectivity to the systems listed in the table. Check the test you want to run and click on the link **Test All** or **Test Selected**. The results are reported in the table as shown below:

Diagnostics Tests

Tech Support Report

Connectivity

Trace Route

Ping

TEST

TEST RESULTS

TIMESTAMP

PROGRESS

License Manager Connectivity

License Manager is Up and Running

03/03/2021 11:39:11

Database Connectivity

Database connection test: OK

03/03/2021 11:39:09

Test All

Test Selected

Click on the information icon next to **License Manager Connectivity** to see the name of the License Manager Host.

To trace a route:

1. Click on the tab **Trace Route**.
2. Enter the IP address for the host you are tracing.
3. Click **Go**.

To ping an address:

1. Click on the tab **Ping**.
2. Enter the IP address for the device you are pinging.
3. Click **Go**.

Tech Support Report

When you have issues, you can create a Tech Support Report (TSR) directly from NSM. It includes all the data needed for SonicWall Support to help you. Navigate to **System | Settings > Diagnostics** and select the **Tech Support Report** tab.

Diagnostics Tests	Tech Support Report
TECH SUPPORT REPORT	
Log Rotation Size	<input type="text" value="100"/> MB
<input type="button" value="Cancel"/> <input type="button" value="Accept"/>	
DOWNLOAD TSR	
Include Logs	<input checked="" type="checkbox"/>
<input type="button" value="Download TSR"/>	

Set the **Log Rotation Size** for the data to be included in the TSR information. The maximum size allowed is 100 MB. If you want to include the logs in your TSR enable the switch. Click **Download TSR**. Submit the information in the TSR provided to SonicWall Support.

Firmware and Settings

Manage your NSM firmware on the **Firmware and Settings** page. Navigate to **System | Settings > Firmware and Settings**.

FIPS Import/Export Settings Upload Firmware Factory Reset Column Selection				
#	FILE NAME	LOAD DATE	VERSION	ACTIONS
1	Current Firmware ✓			

The table lists key statistics about the firmware like File Name, Load Date, Version and Actions that can be performed.

The columns on the table can be customized by clicking Column Selection and checking which columns you want to appear.

① | **NOTE:** Firmware can be upgraded through this page for NSM 2.3.4 and higher versions.

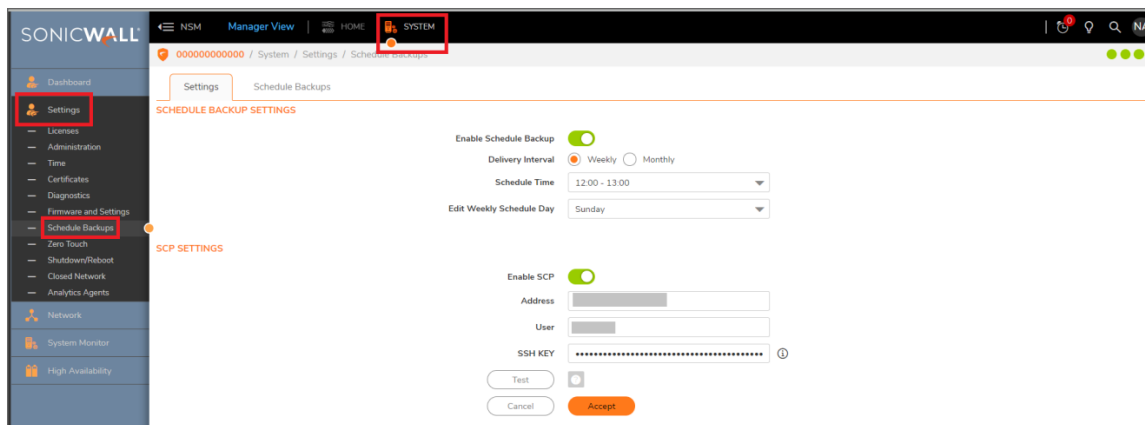
Other actions include:

Import/Export Settings	Use this command to import or export the firmware settings.
Upload Firmware	Use this command to upload a new firmware version and upgrade the system using a .swi file.
Factory Reset	Use this command to factory reset the NSM system.

Backups/Restore Feature

NSM provides the ability to schedule backups as per your requirements. Backup and restore feature helps to restore the NSM system to revoke back to any required setup. This feature helps to bring back the NSM system in case of any system corrupt or GUI becoming non-responsive.

To access the Schedule Backups page, navigate to **System | Settings > Schedule Backups**. This page helps to setup a scheduled system backup, view the backups, import a backup and create a new backup.



① **NOTE:** During a Backup/Restore process the NSM system reboots. Backup/Restore process takes approx 10 minutes to complete. During this process NSM system will be inaccessible.

Topics:

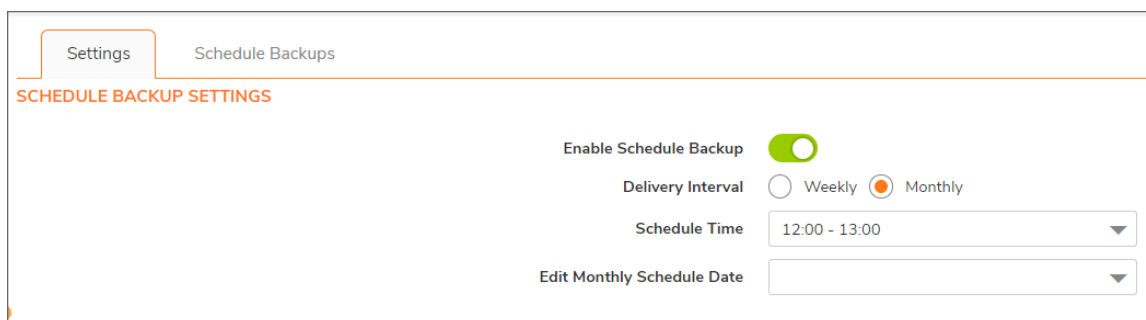
- [Configure a Scheduled NSM File System Backup](#)
- [Configure a Scheduled NSM File System Backup via SCP](#)
- [View NSM File System Backups](#)
- [Create a NSM File System Backup](#)
- [Create SCP of a NSM File System Backup](#)
- [Import a NSM File System Backup](#)
- [Export a NSM File System Backup](#)
- [Delete a NSM File System Backup](#)
- [Restore NSM to a File System Backup](#)
- [Backup/Restore NSM using Safemode](#)

Configure a Scheduled NSM File System Backup

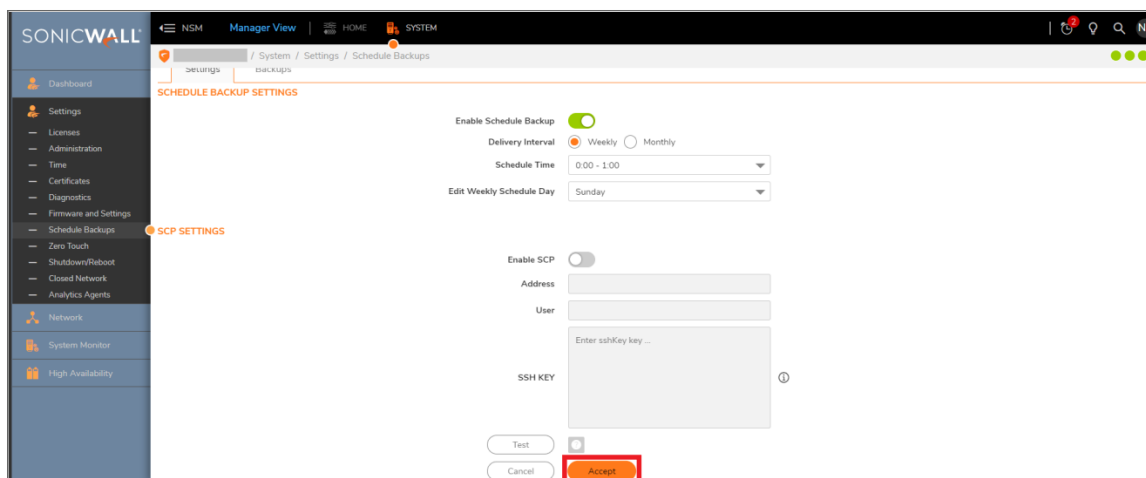
This section allows to create a NSM system backup in a scheduled date/day and scheduled time. The schedule backup helps to restore the system to any backups created in case the NSM system gets corrupted at any point of time.

To configure a scheduled file system backup:

1. Enable the **Enable Schedule Backup** toggle button.



2. Select the **Delivery Interval** to be **Weekly** or **Monthly**.
3. Select the **Schedule Time** value from the drop-down.
4. Select the **Edit Weekly Schedule Day** value from the drop-down list or **Edit Monthly Schedule Date** value from the drop-down list.
5. Click on Accept button.



Configure a Scheduled NSM File System Backup via SCP

This section allows to create a NSM system backup in a scheduled date/day and scheduled time and upload it to another system via scp. Uploading the backup to another system helps to restore the NSM during any system failure.

To configure a file system backup via SCP:

1. Enable the **Enable SCP** toggle button.

SCP SETTINGS

Enable SCP ☒

Address

User

☒ SSH Key ☐ Password

Enter sshKey key ...

SSH KEY

Test Cancel Accept

2. Enter the IP address of the machine to which the backups would be uploaded under **Address** text box.
3. Enter the username under the **User** textbox.
4. Select to use **SSH Key** or **Password**.
 - For **SSH Key**, enter the value of **SSH KEY**.
 - For **Password**, enter the **Password**.
5. Click on the **Test** button to test the ssh address is accessible or not.

SONICWALL NSM Manager View

000000000000 / System / Settings / Schedule Backups

Dashboard

Settings

Success
scp test is success

Enable Schedule Backup ☒

Delivery Interval ☐ Weekly ☒ Monthly

Schedule Time 12:00 - 13:00

Edit Monthly Schedule Date

SCP SETTINGS

Enable SCP ☒

Address 10.194.53.114/jmp/

User abkumar

SSH KEY

Test Cancel Accept

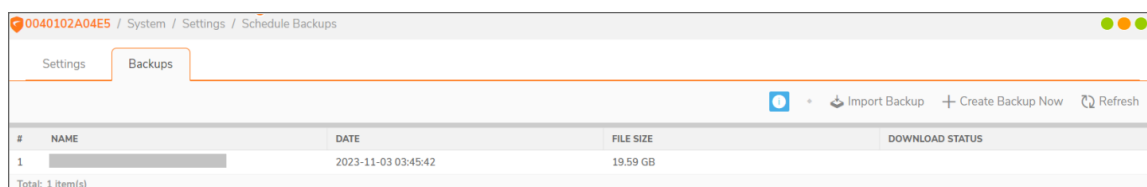
6. On successful test of SCP, click on **Accept** button.

View NSM File System Backups

This section allows to view all the NSM system backups. It also gives you the information about the last backup and the next backup.

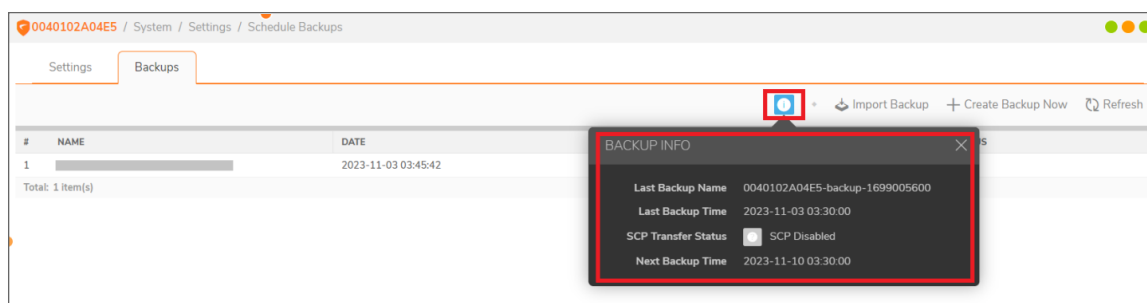
To view all the file system backups:

1. Navigate to **System | Settings > Schedule Backups > Backups**.
2. This page displays all the created file system backups.



To view the backup information:

1. Navigate to **System | Settings > Schedule Backups > Backups**.
2. Click on the information icon



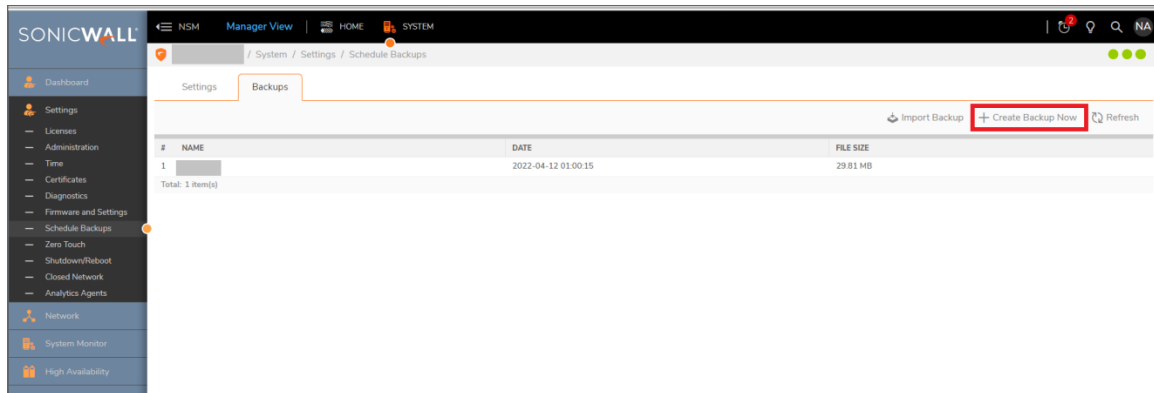
Create a NSM File System Backup

This section allows to create a NSM system backup manually from NSM GUI.

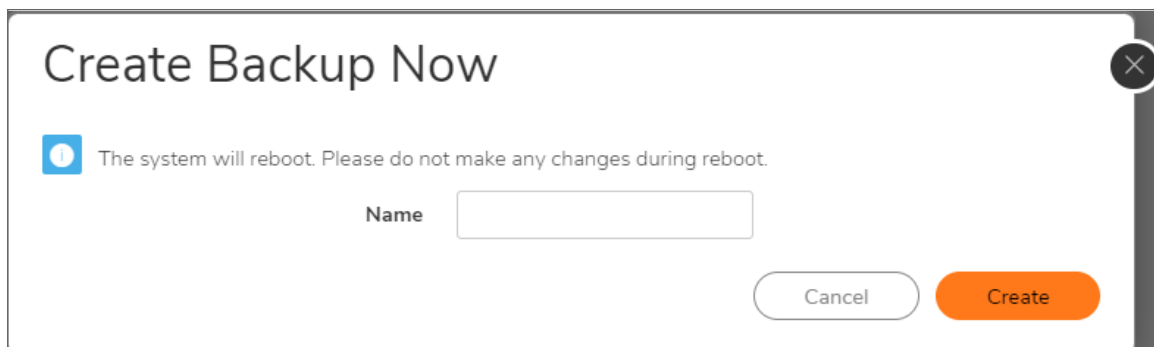
① **NOTE:** If NSM GUI is down please refer to [Backup/Restore NSM using Safemode](#) to backup the system using safemode.

To create a file system backup manually:

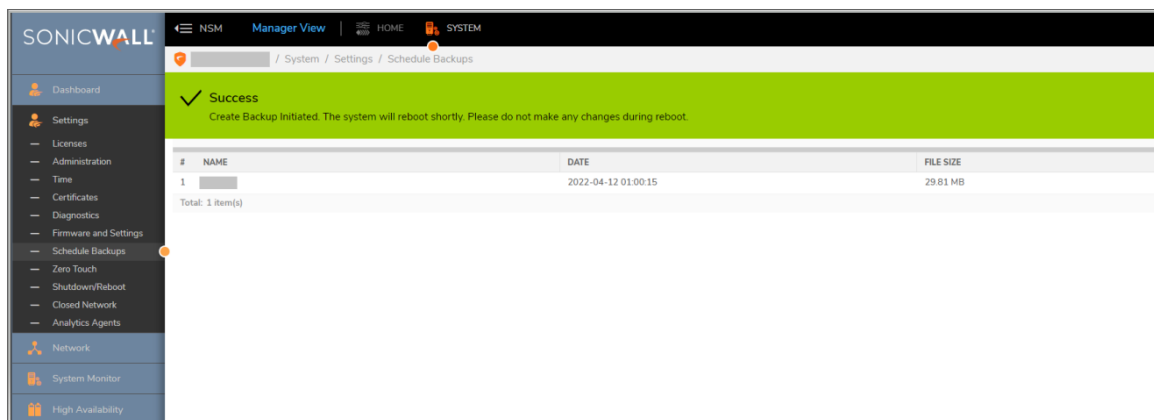
1. Navigate to **System | Settings > Schedule Backups > Backups**.
2. Click on **Create Backup Now**.



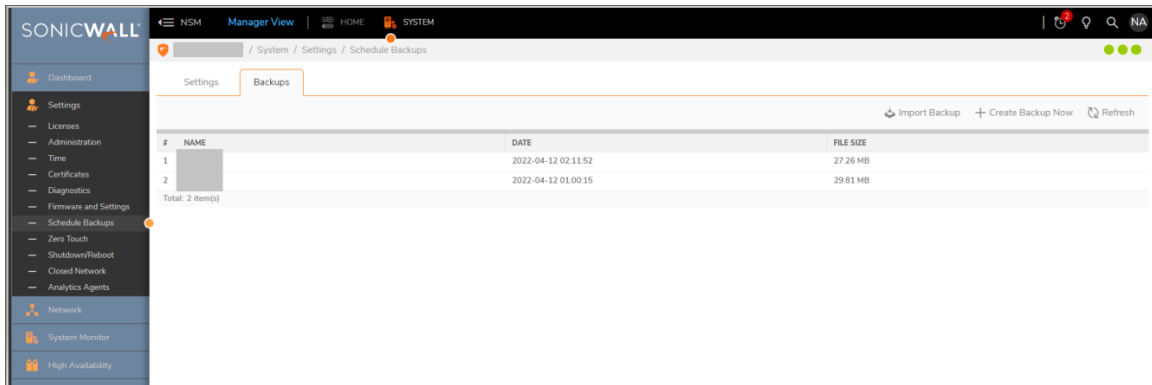
3. Enter a name for the backup in **Name** text box.



4. Click **Create**.
5. On clicking create a Success message is displayed.
 - ① **NOTE:** To create a backup the system needs to reboot and it will take 10 to 15 minutes for the system to be up and running.



6. Once the system is up and running, login to NSM and navigate to **System | Settings > Schedule Backups > Backups** and verify the backup is displayed in the list of backups.




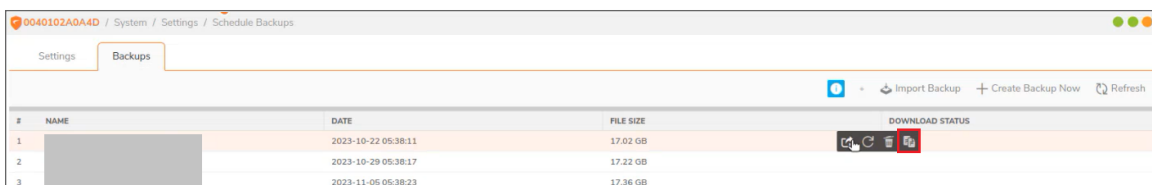
Create SCP of a NSM File System Backup

This allows to create an SCP of the NSM system backup.

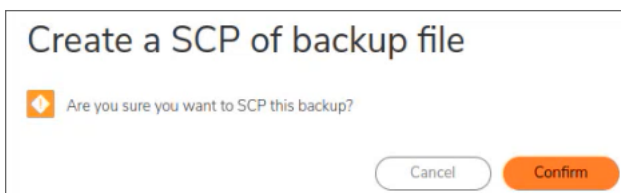
① **NOTE:** This feature works only when SCP is enabled. To enable SCP, refer to [Configure a Scheduled NSM File System Backup via SCP](#).

To create SCP of a file system backup:

1. Navigate to **System | Settings > Schedule Backups > Backups**.
2. Hover on the system backup to be copied.
3. Click on the SCP icon .



4. On prompting to confirm the create SCP of the backup file process, click on **Confirm**.

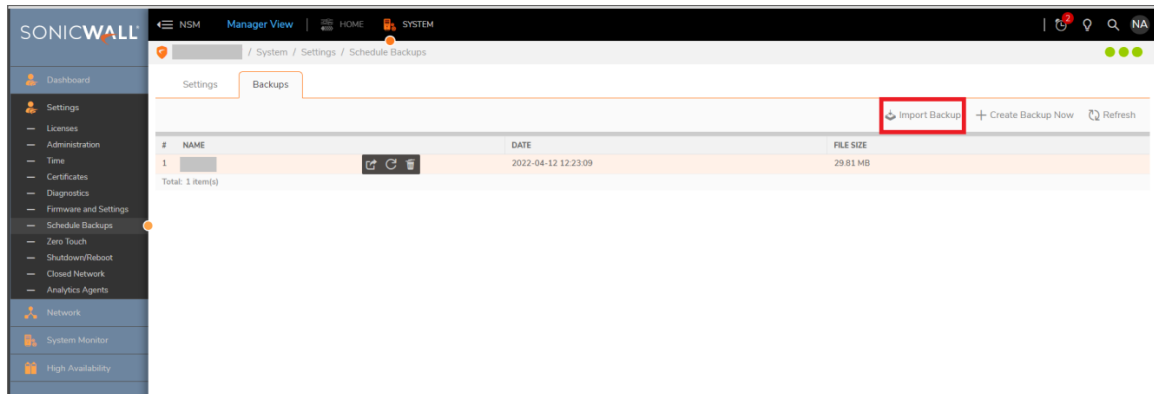


Import a NSM File System Backup

This section allows to import a NSM system backup from local drive.

To import a file system backup:

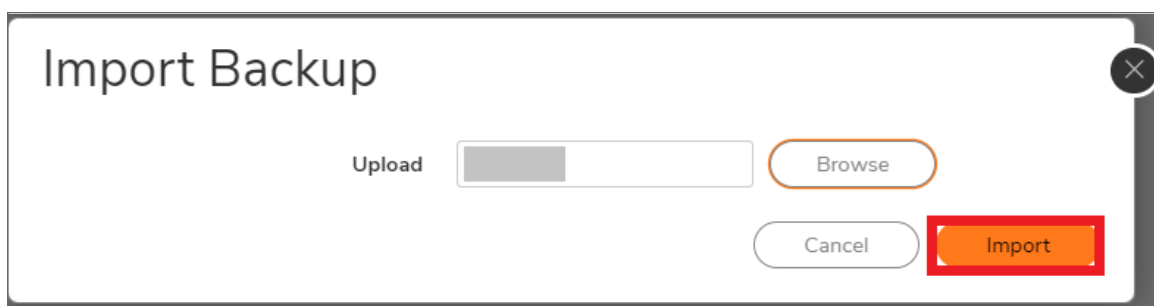
1. Navigate to **System | Settings > Schedule Backups > Backups**.
2. Click on **Import Backup**.



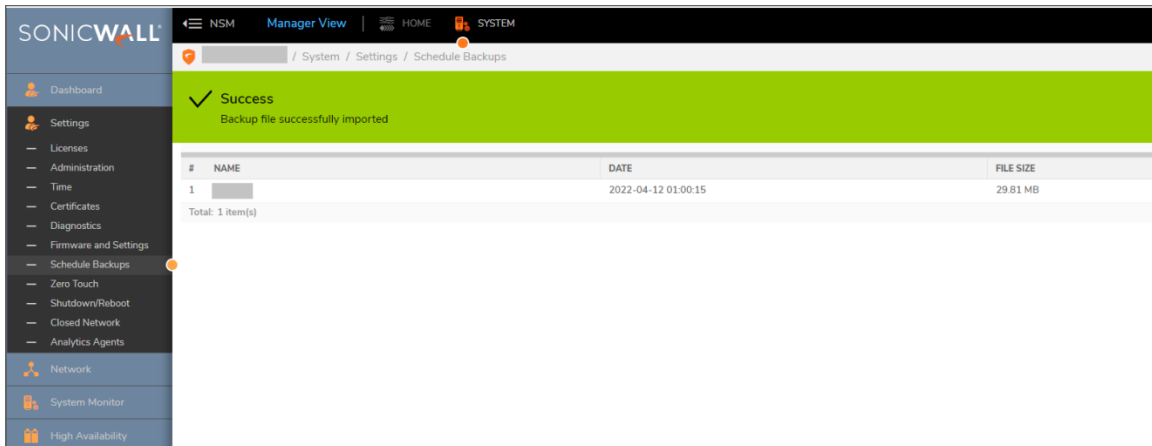
3. Click on **Browse** button and select the backup file to be imported from your local drive.



4. Click on **Import** button.



5. On successful import of the backup, **Success** message is displayed.




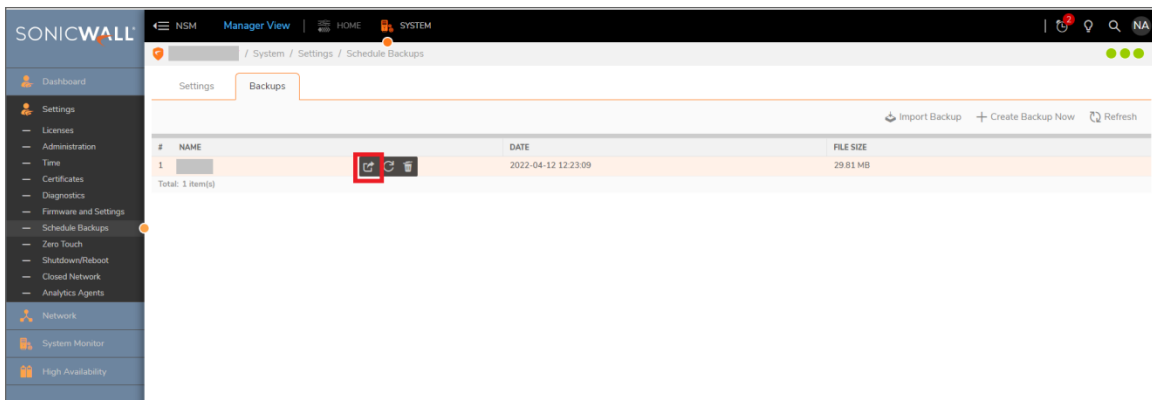
Export a NSM File System Backup

This section allows to export a created NSM system backup.

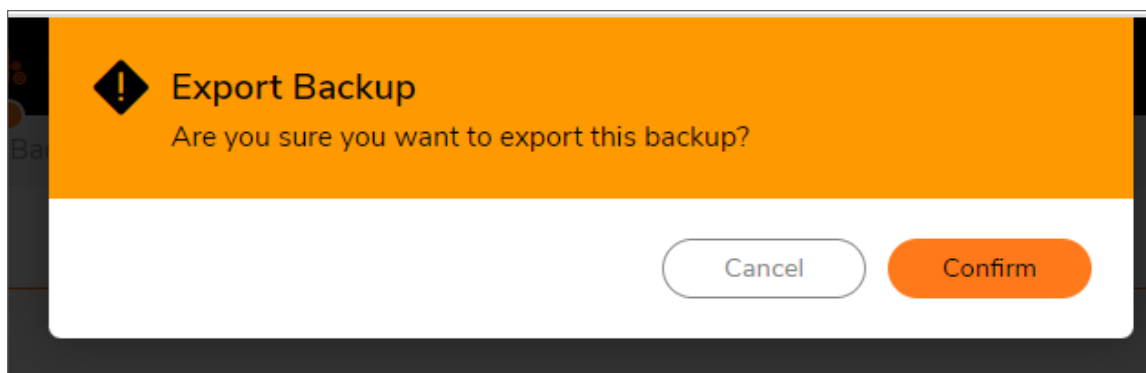
To export a file system backup:

1. Navigate to **System | Settings > Schedule Backups > Backups**.
2. Hover on the system backup to be exported.

3. Click on the export icon .




4. On prompting to confirm the export backup process, click on **Confirm**.

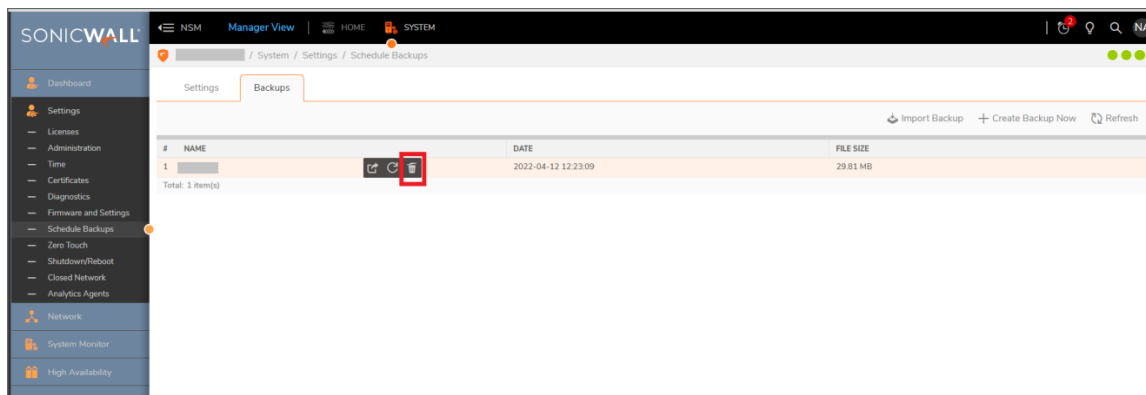


Delete a NSM File System Backup

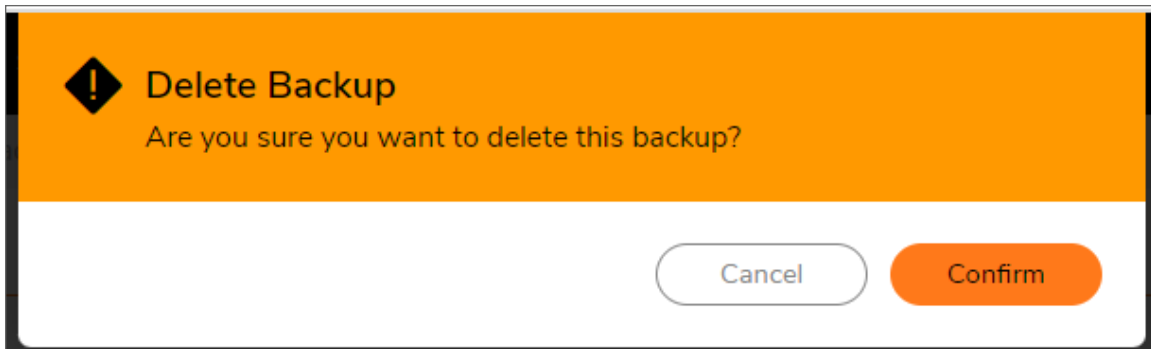
This section allows to delete a created NSM system backup.

To delete a file system backup:

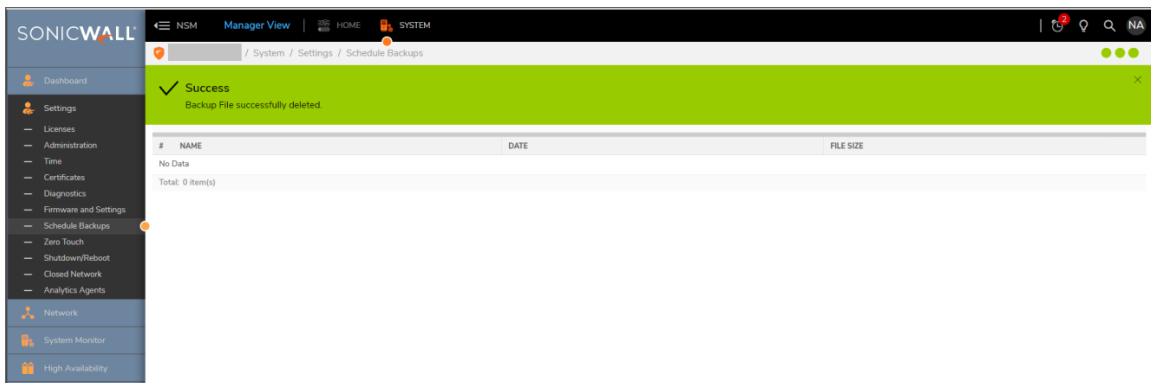
1. Navigate to **System | Settings > Schedule Backups > Backups**.
2. Hover on the system backup to be deleted.
3. Click on the delete icon .



4. On prompting to confirm the delete process, click on **Confirm**.



5. On successfully deleting the backup, **Success** message is displayed.



Restore NSM to a File System Backup


This section allows to restore NSM to a created file system backup from NSM GUI.

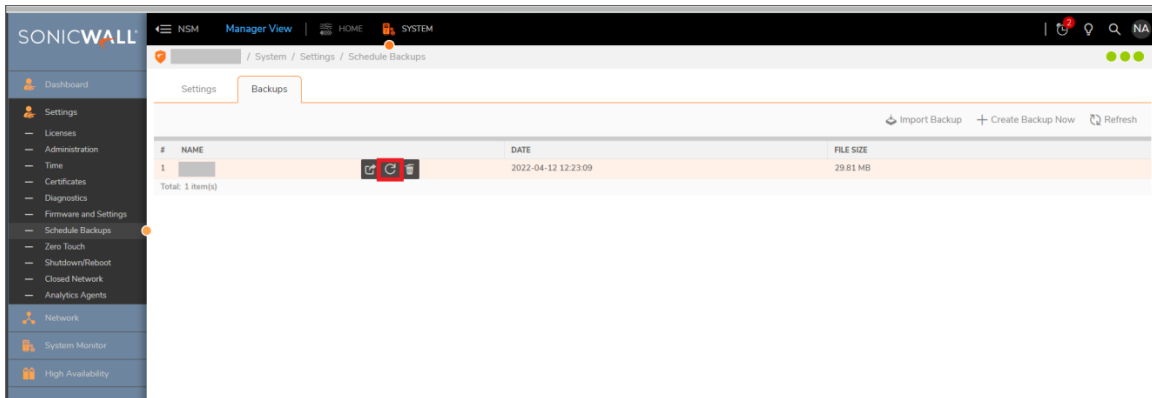
Scenario 1: NSM is working fine and NSM GUI is accessible.

When NSM is working fine and NSM GUI is accessible, the backup can be restored directly from the backups present in the NSM GUI.

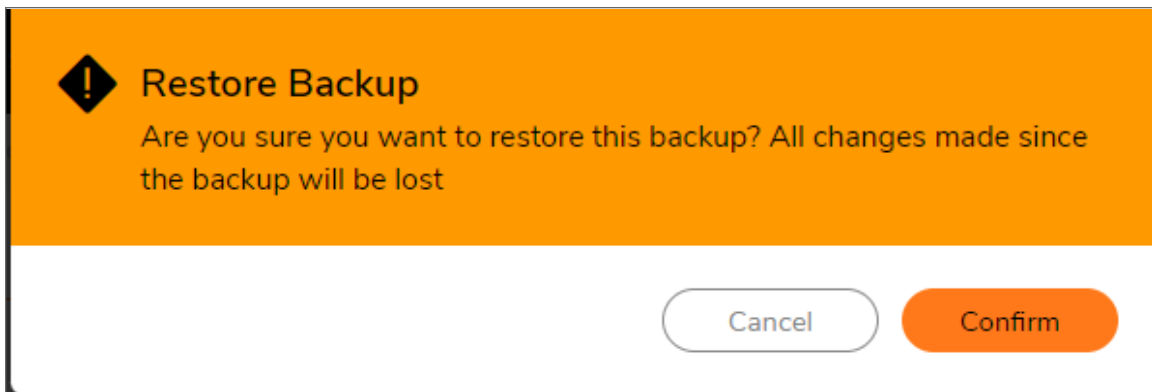
To restore NSM to a created file system backup present in NSM GUI:

1. Navigate to **System | Settings > Schedule Backups > Backups**.
2. Hover on the system backup to which the NSM has to be restored.

3. Click on the restore icon .



- On prompting for confirm the restore process, click on **Confirm**.



Scenario 2: NSM is working fine but NSM GUI is not accessible.

If NSM GUI is down please refer to [Backup/Restore NSM using Safemode](#) to restore the system using safemode.

Scenario 3: NSM system is corrupted .:

When NSM system is corrupted neither the GUI will be accessible nor the safe mode will work. In this scenario the NSM system has to be re-imaged and then any backup created via SCP in another system can be used to restore the system.

To restore NSM to a file system backup present in another server:

- Copy the required backup file from the server to your local drive.
- Import the backup file to the NSM system from local drive following the steps in [Import a NSM File System Backup](#)
- Restore the imported backup file using the steps in [To restore NSM to a created file system backup present in NSM GUI](#)

Backup/Restore NSM using Safemode

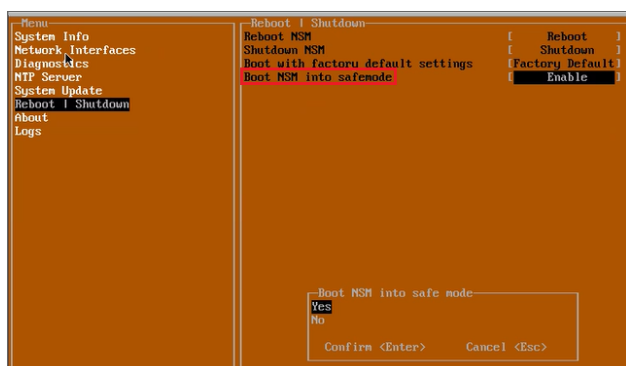
In a scenario where NSM GUI becomes non-responsive and backup/restore is not possible using NSM GUI, the backup using safemode can be used.

To enter NSM in safemode:

1. Log into the NSM console using KVM, VMWare, Hyper-V or Azure.
2. Navigate to Reboot | Shutdown.



3. Enable the **Boot NSM into safemode**. Click on **Yes** when prompted for confirmation to **Boot NSM into safe mode**.



4. The NSM system reboots to run in safemode.
① | **NOTE:** It takes around 10 minutes to reboot in safemode.



5. After successful reboot, log into NSM using <http://NSMIPAddress>.

Steps to backup/restore using safemode:

1. Navigate to **Firmware > Application Backups**.

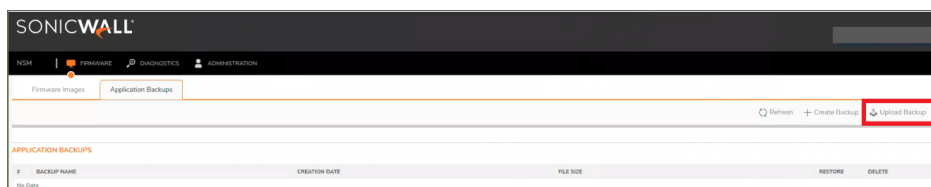


- a. To create a new backup, click on **Create Backup**. Then enter the name of the backup and click on **Create Backup**.

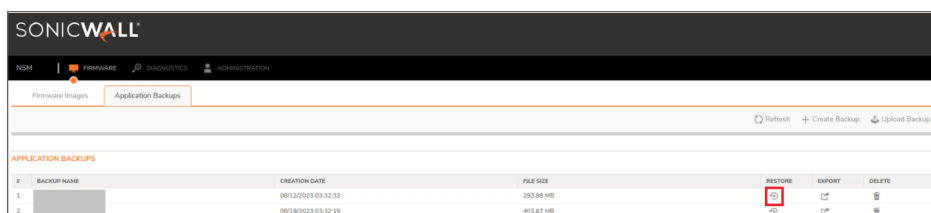


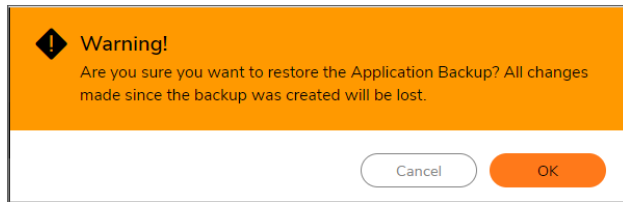
The 'Create Application Backup' dialog box is shown. It contains the text: 'To create a new Application Backup, enter the name and press OK. The backup may take a few minutes to be created and will then be added to the list of available backups.' There is a text input field labeled 'Backup Name' and two buttons: 'Create Backup' (highlighted in orange) and 'Cancel'.

- b. To upload a backup from local drive, click on **Upload Backup**, select the backup file from local drive and click upload.

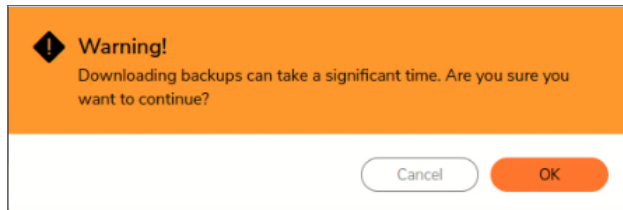
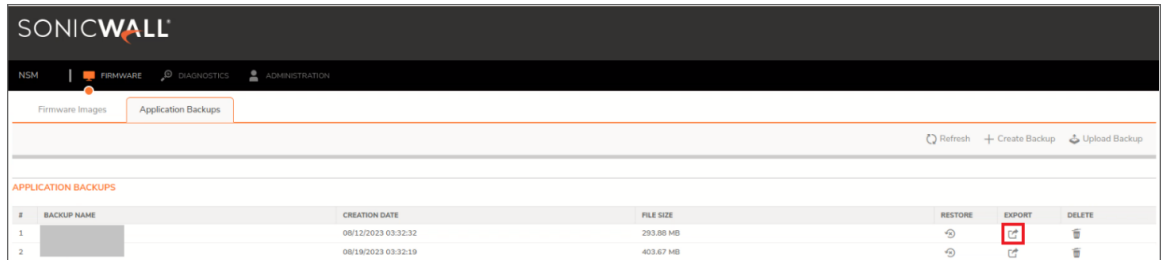


- c. To restore a backup, click on the restore icon beside the system backup to which the NSM has to be restored. On prompting for confirm the restore process, click on **OK**.

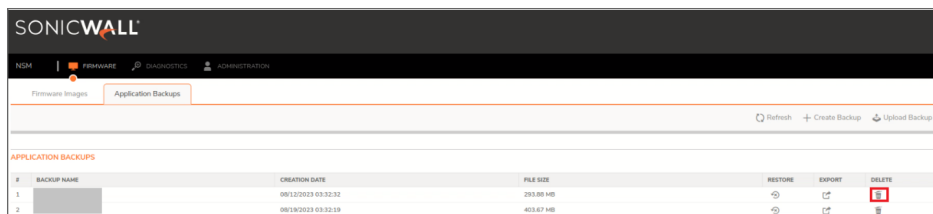




- d. To export a backup, click on the export icon beside the system backup which has to be exported. On prompting for confirmation, click on **OK**.

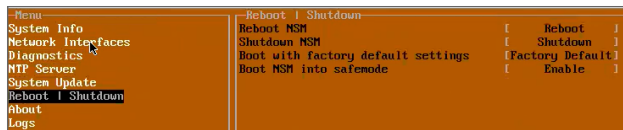


- e. To delete a backup, click on the delete icon beside the system backup.

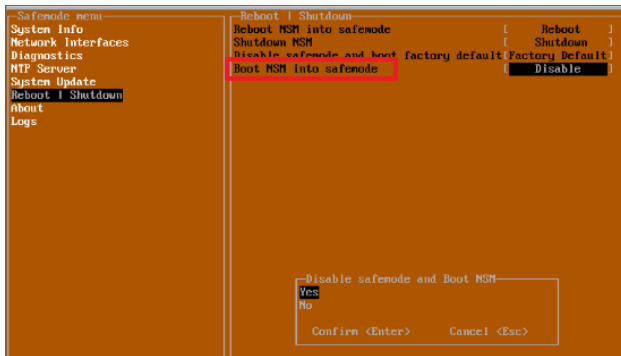


To exit from safemode:

1. Log into the NSM console using KVM, VMWare, Hyper-V or Azure.
2. Navigate to Reboot | Shutdown.



3. Disable the **Boot NSM into safemode**. Click on **Yes** when prompted for confirmation to **Boot NSM into safe mode**.



Zero Touch

NSM has automated the process of acquiring and configuring your firewalls with the Zero Touch feature as well as providing the mechanism to manage your firewalls with “zero” touch when you are setting it up for management. The firewall need only be registered in MySonicWall and enabled for Zero Touch.

① | **NOTE:** Firewall registration can be completed even before you receive the unit.

When you get the firewall, plugged it in for power and connected to the internet for this feature to operate. Beyond that, the firewall, NSM, and other entities within the network infrastructure function together to bring the unit under management.

Q Search...

Zero Touch

Refresh

Column Selection

#	FIREWALL SERIAL	REMOTE ADDRESS	ENABLED	CONNECTION STATE	UP TIME
No Data					

For the Zero Touch feature to function correctly, you must have SonicOS 6.5.1.1-42n or later running on your firewall. New firewall shipments already have that version and Zero Touch enabled in the firmware.

Shutdown/Reboot

Use this command to shut down, reboot or safemode reboot your NSM system. Navigate to **System | Settings > Shutdown/Reboot**.

Warning! This action will disconnect all users. The restarting process takes several minutes. Any unsaved changes will be lost.

Shutdown
Restart

Use Shutdown to power down the system.

Use Restart to power down and reset the system.

Use the Safemode reboot to power down and reset the system in Safemode.

❗ | **IMPORTANT:** Either of these actions disconnects all users. The restarting process takes several minutes and any unsaved changes are lost.

Closed Network

Closed Network support feature helps you to run one or more private networks that are completely shut-off from the outside environment. You can license the NSM managed firewall without contacting License Manager (LM) or (MSW), when onboarding and patching SonicWall firewall to preserve the privacy and security of the closed networks.

Navigate to **System | Settings > Closed Network**.

The screenshot shows the 'Closed Network' configuration page. At the top, there's a section 'IMPORT SIGNATURES / LICENSES' with a 'Closed Network File' label and an 'Import' button. Below this, there are two status sections: 'NSM LICENSE' and 'DEVICE SIGNATURE'. The 'NSM LICENSE' section shows a status of 'Successfully imported NSM registration and licenses' and 'Last Updated' as 'Not available'. The 'DEVICE SIGNATURE' section shows a status of 'There is no Signature file updated' and 'Last Updated' as 'Not available'. Below these, there's a 'DEVICE LICENSE' section with a table. The table has columns: '#', 'SERIAL NUMBER', 'FRIENDLY NAME', 'UPDATED', 'STATUS', and 'KEYSET'. The table is currently empty, showing 'No Data' and 'Total: 0 item(s)'. There are also 'Update Firewall' and 'Refresh' buttons.

To import Network Files:

1. Click **Import**.
2. Click **Browse** and select the license file you need to import from your computer.
3. Click **Upload**.

❗ | **NOTE:** You can import only a ZIP file with .LIC extension.

The imported network is listed with the details including Serial Number, Friendly Name, Status, and Keyset data.

An imported closed network file contains the NSM License along with the firewall license and signature files. After the Closed network file is imported in NSM, you can add the devices as usual in the **Firewalls > Inventory** page. After adding or acquiring the device successfully, the device gets registered automatically. The device license will be updated in the **Device > Licenses** page and the NSM **Firewalls > Inventory** page.

NSM Manager View HOME SYSTEM			
000000000000 / System / Settings / Licenses			
<div> <div> <div>Q</div> <div>View: All</div> </div> <div> <div>Friendly Name: Narendra-onprem-11.114.25.43</div> <div>Serial Number: 00401112397963</div> </div> </div>			
SERVICES	STATUS	EXPIRY DATE	ACTIONS
<div>▼ Security Service Info (1 licensed)</div> <div>Network Security Manager</div>	Licensed Count: 25	15 Mar 2022	
<div>▼ Support Service Info (1 licensed)</div> <div>24x7 Support</div>	Licensed	15 Mar 2022	

You can also update a firewall from the Closed Network page.

To Update a Firewall:

1. Select the firewall from the list.
2. Click **Update Firewall**.

Network

Use the Network command to define the network infrastructure for your On-Premises NSM system.

Topics:

- [Settings](#)
- [Interface](#)
- [Routes](#)

Settings

You can set up your host and DNS servers by navigating to **System | Network > Settings**.

HOST

Name:

Domain:

DNS

DNS Server 1:

DNS Server 2:

DNS Server 3:

To setup the host:

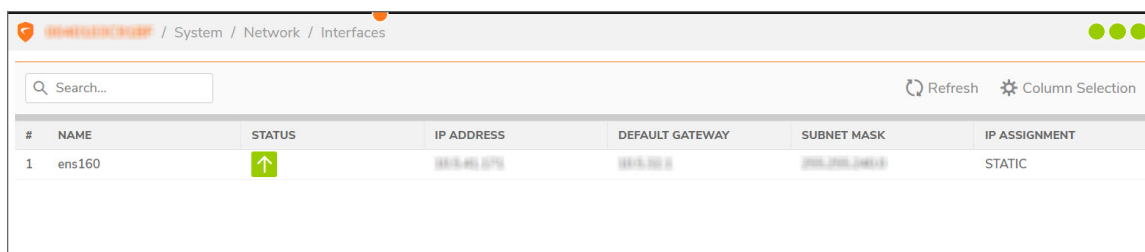
1. In the Host section, input the server **Name** in the field provided.
2. Add the **Domain** name.
3. Click **Accept**.

To set up a DNS server:

1. In the DNS section, input the IP address in the field provided. You can add IP addresses for up to three DNS server.
2. Click **Accept**.

Interface

To see the network interfaces for your NSM system, navigate to **System | Network > Interfaces**.



Search...						
Refresh Column Selection						
#	NAME	STATUS	IP ADDRESS	DEFAULT GATEWAY	SUBNET MASK	IP ASSIGNMENT
1	ens160	↑	192.168.1.175	192.168.1.1	255.255.255.0	STATIC

Use the **Search** field to find a specific interface or filter on a parameter. Use **Column Selection** to customize which column display.

Routes

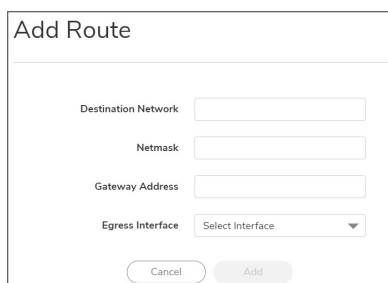
Use the Routes page to manage the network routes for your NSM implementation. Navigate to **System | Network > Routes**. You can add, edit or delete the routes.



Search...					
View: All + Add Delete Refresh					
#	DESTINATION NETWORK	NETWORK MASK	EGRESS INTERFACE	GATEWAY IP	ACTION
1	default	0.0.0.0	ens160	192.168.1.1	...

To add a route:

1. Click the **+Add** icon.

A dialog box titled "Add Route" with a light gray border. Inside, there are four input fields: "Destination Network", "Netmask", "Gateway Address", and "Egress Interface". The "Egress Interface" field is a dropdown menu with "Select Interface" and a downward arrow. At the bottom, there are two buttons: "Cancel" and "Add".

Add Route

Destination Network

Netmask

Gateway Address

Egress Interface

2. Add a name for the **Destination Network**.
3. Input the **Netmask**.
4. Enter the **Gateway Address**.
5. Select the **Egress Interface** from the drop-down list.
6. Click **Add**.

To edit a network route:

1. Select the route that you want to edit.
2. In the Action column, click the **Action** icon and select **Edit**.
① | **NOTE:** You cannot edit the default routes.
3. Make changes to fields as needed.
4. Click **Save**.

To delete a network route:

1. Select the route that you want to delete.
2. In the Action column, click the **Action** icon and select **Delete**. Or you can click on the **Delete** icon above the table.
① | **NOTE:** You cannot delete the default routes.
① | **NOTE:** You can delete multiple routes at once by checking the boxes to the right of the names and clicking the **Delete** icon.
3. Confirm the delete as needed.

System Monitor

Use the System Monitor commands to monitor and assess the performance of your NSM implementation.

Topics:

- [Settings](#)
- [Live Monitor](#)
- [Process/Service Monitor](#)
- [Service Monitor](#)
- [System Report](#)

Settings

Use the Settings page to set the thresholds for CPU, memory and disk utilization. Navigate to **System | System Monitor > Settings**.

The screenshot displays the 'Settings' page for the System Monitor, organized into three sections: CPU UTILIZATION, MEMORY UTILIZATION, and DISK UTILIZATION. Each section contains two horizontal sliders for setting thresholds. The first slider is for 'Warning' notifications, and the second is for 'Critical' notifications. The 'Warning' sliders have predefined ranges: 60% to 80% for CPU and Memory, and 50% to 75% for Disk. The 'Critical' sliders have predefined ranges: 85% to 95% for CPU and Memory, and 80% to 95% for Disk. The current settings are: CPU Warning at 70%, CPU Critical at 90%, Memory Warning at 69%, Memory Critical at 89%, Disk Warning at 63%, and Disk Critical at 88%. At the bottom of the form are 'Cancel' and 'Accept' buttons.

Utilization Type	Warning Threshold	Critical Threshold
CPU UTILIZATION	70%	90%
MEMORY UTILIZATION	69%	89%
DISK UTILIZATION	63%	88%

Use the sliding bars in the first column to set the threshold for warning notifications. The Warning range is predefined to span from 60% to 80% for CPU and memory utilization. It spans from 50% to 75% for the disk utilization. Slide the orange button to the setting you want, and you will be sent a notice that the utilization has risen to the Warning level.

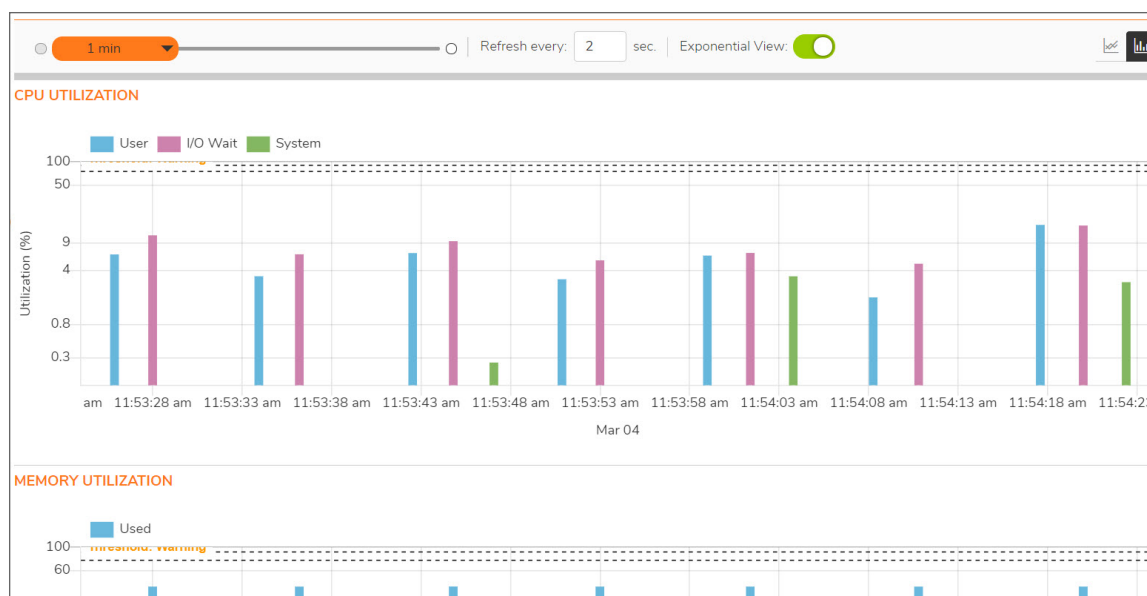
Use the sliding bars in the second column to set the threshold for critical notification levels. The Critical range is predefined to span from 85% to 95% for CPU and memory utilization. It spans from 80% to 95% for the disk

utilization. Slide the orange button to the setting required, and you will be sent a notice that the utilization has risen to Critical level.

Be sure to click **Accept** when you finish defining your thresholds.

Live Monitor

Use the Live Monitor to see how the NSM is behaving in real time. Navigate to **System | System Monitor > Live Monitor**.



When first reaching the Live Monitor page, you may want to define the settings for the report.

- Using the orange slider bar to set the interval for the report. The predefined intervals range from **1 min** to **60 min**.
- Set the Refresh period in seconds.
- Enable or disable the **Exponential View**.
- Using the icons to the right you can change between a line graph and a bar chart.

Process/Service Monitor

Use the **Process/Service Monitor** to see the processes/services that are running on the NSM system and the utilization associated with them. Navigate to **System | System Monitor > Process/Service Monitor**.

0040102A04E5 / System / System Monitor / Process/Service Monitor					
Q Search...			Refresh Column Selection		
#	PROCESS/SERVICE	CPU (%)	MEMORY (%)	STATUS	ACTION
1	redis	0.10	0.00	Started	Start Restart Stop
2	mongo	1.00	4.30	Started	Start Restart Stop
3	maria	0.10	0.80	Started	Start Restart Stop
4	elasticsearch	2.20	30.00	Started	Start Restart Stop
5	fluentd	0.00	2.10	Started	Start Restart Stop
6	neo4j	0.70	7.50	Started	Start Restart Stop
7	apiDocServer	0.00	0.20	Started	Start Restart Stop
8	graphDatabaseManager	0.00	0.10	Started	Start Restart Stop

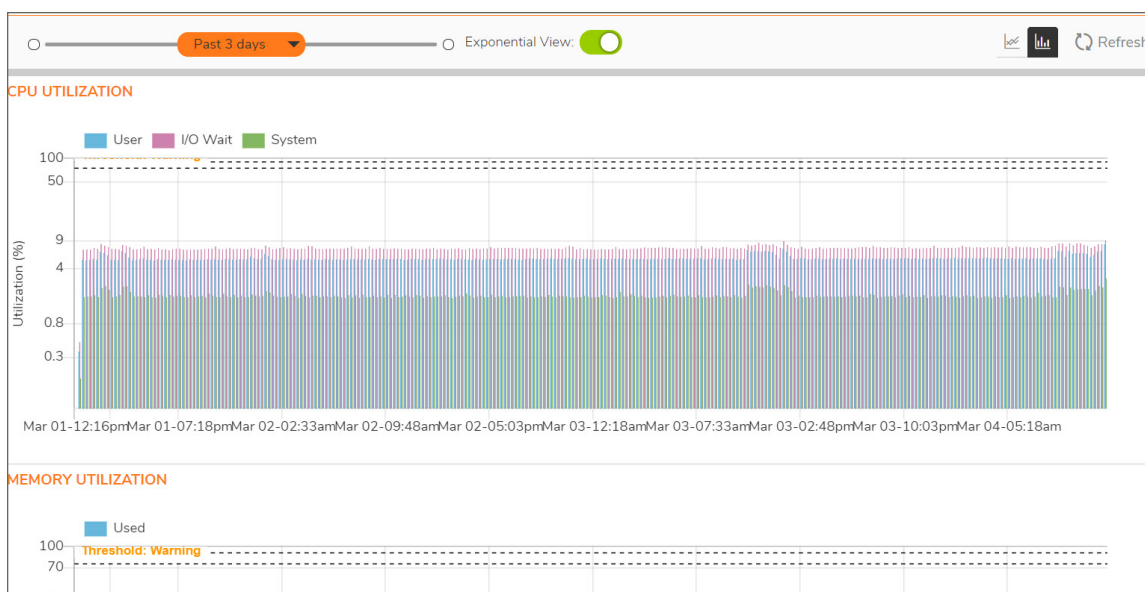
You can use the **Search** field to search for a specific process/service or filter to a set of similar processes/services. The table responds as you type.

Click the **Refresh** icon to refresh the data in the table.

You can also view the status of the services, start, restart, or stop them.

System Report

The System Report page displays the historical reports for CPU, memory, and disk utilization. Navigate to **System | System Monitor > System Report**.



When first reaching the System Report page, you may want to define the settings for the report.

- Using the orange slider bar to set the period for the report. The predefined periods range from **Past 24 hours** to **Past 5 days**.
- Enable or disable the **Exponential View**.
- Using the icons to the right, change between a line graph and a bar chart.
- Click **Refresh** to update the data in the table.

High Availability

High Availability feature allows two identical NSMs to be configured to provide a reliable continuous connection. Two NSMs will be identical only when all the settings under **System > Settings** and **System > Network > Settings** are identical. One NSM is configured as the primary, and an identical NSM is configured as the secondary. If the primary NSM fails, the secondary NSM takes over to secure a reliable connection for the protected network. Two NSMs configured in this way are also known as a High Availability pair (HA pair).

Use the System Monitor page to monitor and assess the performance of your NSM implementation.

Topics:

- [Status](#)
- [Settings](#)
- [Advanced Settings](#)
- [Virtual IP](#)
- [HA Modes and Terminologies](#)
- [Backup/Restore in High Availability Setup](#)

Status

Use the Status page to monitor and assess the status information of your NSM High Availability. You can also view the configuration and license details, and refresh the page to view the latest information.

HIGH AVAILABILITY STATUS

Status

Primary ACTIVE

Primary State

ACTIVE

Secondary State

STANDBY

Active Up Time

3 weeks 6 Days 22 Hours 59 Minutes

Found Peer

Yes

Settings Synchronized

Yes

HIGH AVAILABILITY CONFIG

HA Mode

Active/Standby

HIGH AVAILABILITY LICENSES

Primary Stateful HA Licensed

Yes

Secondary Stateful HA Licensed

Yes

Settings

Use the Settings page to view the general settings of the NSM High Availability. You can view the Primary and Secondary device details in this page.

You can change the modes of High Availability to **None** or **Active/Standby**.

NOTE: For more details on High Availability modes, refer to [HA Modes and Terminologies](#).

WARNING: It is recommended to keep the preempt mode disabled.

You can enter the secondary device details and click **Accept** to save the changes.

GENERAL SETTINGS

Mode

Active / Standby

Enable Preempt Mode

☐

Enable Encryption for Control Communication

☒

HA DEVICES

PRIMARY DEVICE

Serial Number

ens160

SECONDARY DEVICE

Serial Number

ens160

Cancel

Accept

Advanced Settings

Use the Advanced page to monitor the advanced settings of your NSM High Availability implementation. You can edit and save the settings including Heartbeat Interval, Failover Trigger Level, Probe Interval, and the missed Probe Counts.

Hover the mouse over the info icon to view more details of each settings. Click **Accept** to save the changes.

You can also synchronize the settings and force the Active/Standby failover by clicking the respective buttons in the **Diagnostics** section.

① **NOTE:** If any of the settings under **System > Settings** and **System > Network > Settings** are updated in Active NSM, it does not replicate to Standby NSM automatically. You must perform a force Active/Standby failover by clicking the **Force Active/Standby Failover** button to make the Standby node as Active and change the required settings to bring the HA pair back to it's identical state.

ADVANCED SETTINGS

Heartbeat Interval (seconds)

10

ⓘ

Failover Trigger Level (missed heartbeats)

7

ⓘ

Probe Interval (seconds)

20

ⓘ

Probe Count (missed probes)

3

ⓘ

Cancel

Accept

DIAGNOSTICS

Synchronize Settings

Force Active/Standby Failover

Virtual IP

Use the Virtual IP page to set the virtual IP details of NSM High Availability. You can view the details including Virtual IP address, Probe IP Address, and the Probe Monitoring status.

<div><div>Search...</div><div>Refresh</div></div>					
#	NAME	VIRTUAL IP ADDRESS	PROBE IP ADDRESS	PROBE MONITORING	CONFIGURE
1	ens160	10.5.41.173	9.9.9.9	✓	


Click  to edit the Virtual IP settings. You can edit, enable, or disable the Probe IP Address using this option.

Virtual IP Settings

Interface

ens160

Virtual IP Address



Probe IP Address

☒

Cancel

OK

HA Modes and Terminologies

Modes	Definitions
None	Selecting None activates a standard high availability configuration and NSM failover functionality, with the option of enabling stateful High Availability.
Active/Standby	<p>Active/Standby mode provides basic high availability with the configuration of two identical NSMs as a High Availability pair. The Active NSM handles all traffic, while the Standby NSM shares its configuration settings and can take over at any time to provide continuous network connectivity if the Active NSM stops working.</p> <p>By default, Active/Standby mode is stateless, meaning that network connections must be re-established after a failover. To avoid this, stateful synchronization can be licensed and enabled with Active/Standby mode. In this stateful High Availability mode, the dynamic state is continuously synchronized between the Active and Standby NSMs. When the Active NSM encounters a fault condition, stateful failover occurs as the Standby NSM takes over the Active role with no interruptions to the existing network connections.</p>
Terms	Definitions
Active	The operative condition of an NSM. The Active identifier is a logical role that can be assumed by either a primary or secondary NSM.
Primary	The principal NSM. The primary identifier is a manual designation and is not subject to conditional changes. Under normal operating conditions, the primary NSM operates in an Active role.
Secondary	The subordinate NSM. The secondary identifier is a relational designation and is assumed by an NSM when paired with a primary NSM. Under normal operating conditions, the secondary NSM operates in a standby mode. Upon failure of the primary NSM, the secondary NSM assumes the Active role.
HA	High Availability: non-state, NSM failover capability.

Failover	The actual process in which the Standby NSM assumes the Active role following a qualified failure of the Active NSM. Qualification of failure is achieved by various configurable physical and logical monitoring facilities.
Preempt	Applies to a post-failover condition in which the primary NSM has failed, and the secondary NSM has assumed the Active role. Enabling Preempt causes the primary NSM to seize the Active role from the secondary after the primary NSM has been restored to a verified operational state.
Standby (Idle)	The passive condition of an NSM. The standby identifier is a logical role that can be assumed by either a primary or secondary NSM. The Standby NSM assumes the Active role upon a determinable failure of the Active NSM.

Backup/Restore in High Availability Setup

To access the Schedule Backups page, navigate to **System | Settings > Schedule Backups** in Active NSM system. This page helps to setup a scheduled system backup, view the backups, import a backup and create a new backup.

Topics:

- [Configure a Scheduled Backup in High Availability Setup](#)
- [Restore Feature in High Availability Setup](#)

Configure a Scheduled Backup in High Availability Setup

This section describes how scheduled backup works in a High Availability setup.

- ① **NOTE:** Backup can be scheduled only in an Active NSM system. Standby NSM system can't schedule a backup but Standby system triggers a backup run after 30 minutes of the scheduled backup in Active NSM system.
- ① **NOTE:** When NSM is configured in a HA pair, it is recommended to create or edit system backup schedules on an Active Primary NSM server.

Scenario: Primary NSM is Active setup and Secondary NSM is Standby setup

In this scenario when a backup is scheduled to run at a time, say t_1 , in Primary NSM system following the steps in [Configure a Scheduled NSM File System Backup](#), a backup is by default scheduled to be run in the Secondary NSM system at a time which is 30 minutes after the scheduled time in primary system i.e (t_1+30).

When the backup is being created at time t_1 , the Primary NSM system reboots. At this time the Secondary NSM system becomes Active setup and after reboot the Primary NSM system becomes the Standby setup.

After 30 minutes (t1+30) when the backup is being created in Secondary NSM system, it reboots. At this time the Primary NSM system again becomes Active setup and after reboot the Secondary NSM system becomes the Standby setup.

Restore Feature in High Availability Setup

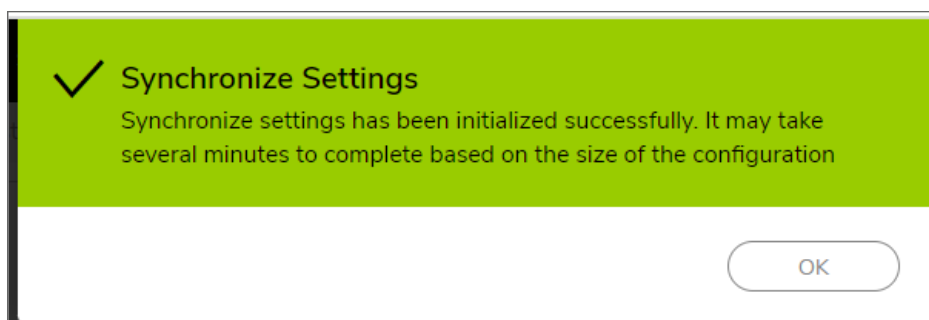
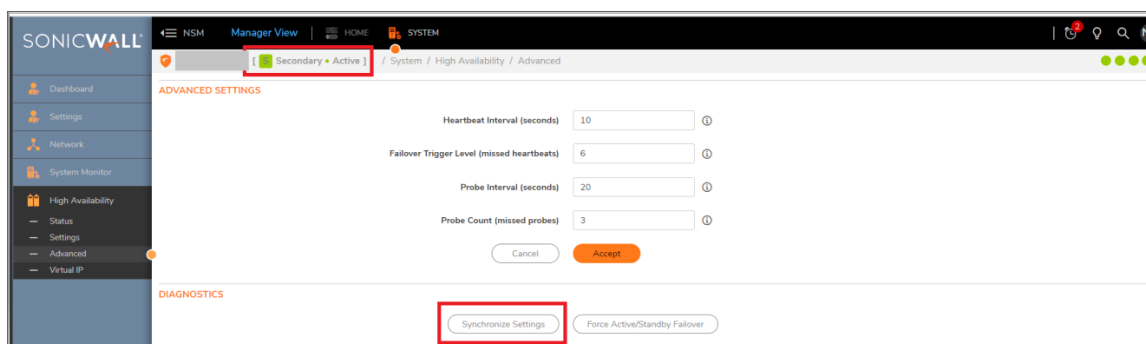
This section describes how restore feature works under various scenarios in a High Availability setup.

Scenario 1: Primary NSM system gets corrupted and Secondary NSM system is working fine.

When the Primary NSM system which was Active goes down, the Secondary NSM system which was on Standby now becomes Active.

Below are the steps to restore back the Primary NSM system:

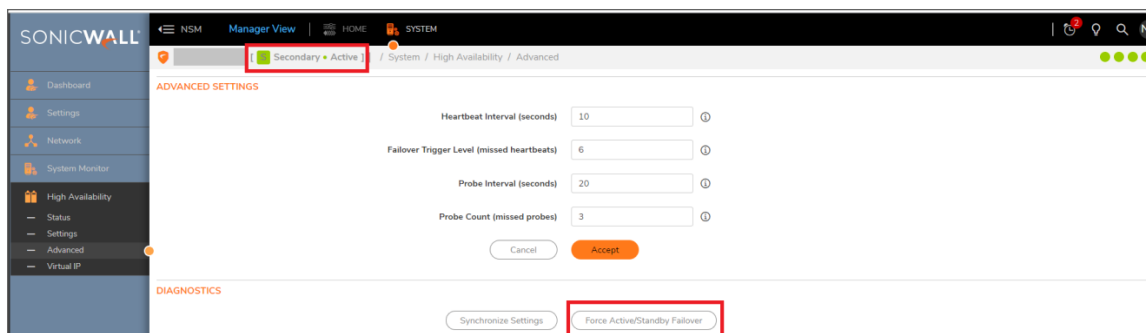
1. Restore back the Primary system using any of the applicable scenarios described under [Restore NSM to a File System Backup](#).
2. After successful restoration of Primary NSM system, the Secondary NSM system automatically pushes the settings to Primary. To manually synchronize the settings from Secondary system to Primary system, log into the Secondary system, navigate to **System | High Availability > Advanced** and click on **Synchronize Settings** under **Diagnostics**.



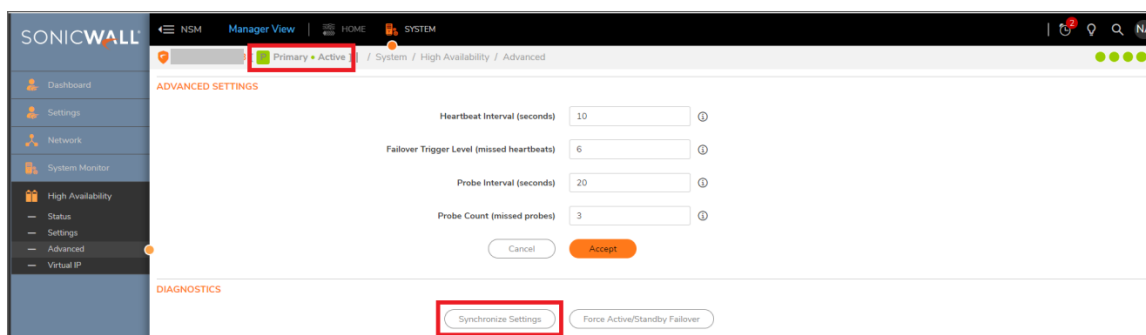
① **NOTE:** To verify that the Primary and Secondary NSM systems are in syn, navigate to **System | High Availability > Status** and verify that the value for **Settings Synchronized** to be **In Sync**

- After successful synchronization, now the Secondary NSM system is still Active and the Primary NSM system acts as Standby.

If you need to make the Primary NSM system Active, log into the Secondary system, navigate to **System | High Availability > Advanced** and click on **Force Active/Standby Failover** under **Diagnostics**.



- After a successful failover, the Primary now acts as Active system and Secondary acts as Standby. Next log into Primary NSM system, navigate to **System | High Availability > Advanced** and click on **Synchronize Settings** under **Diagnostics**.



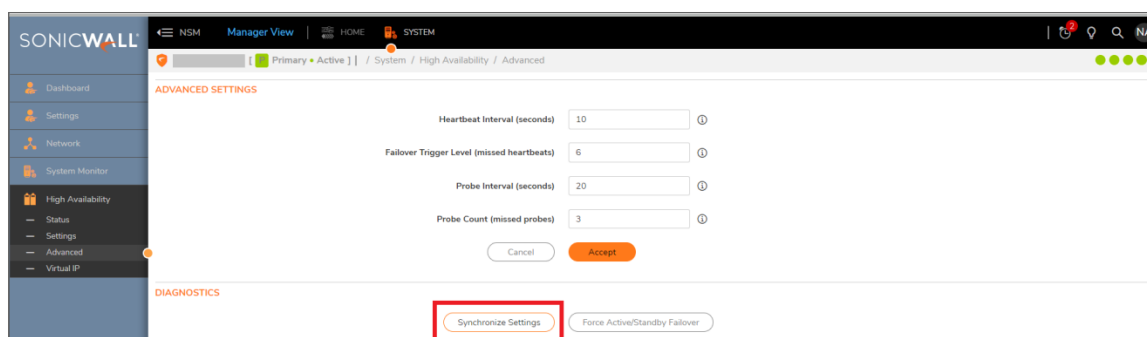
Scenario 2: Secondary NSM system gets corrupted and Primary NSM system is working fine.

In this scenario the Primary NSM system is the Active system and the Secondary NSM system is the Standby system.

Below are the steps to restore back Secondary NSM system:

- Restore back the Secondary NSM system using any of the applicable scenarios described under **Restore NSM to a File System Backup**.
- Log into Primary NSM system, navigate to **System | High Availability > Advanced** and click on

Synchronize Settings under Diagnostics.

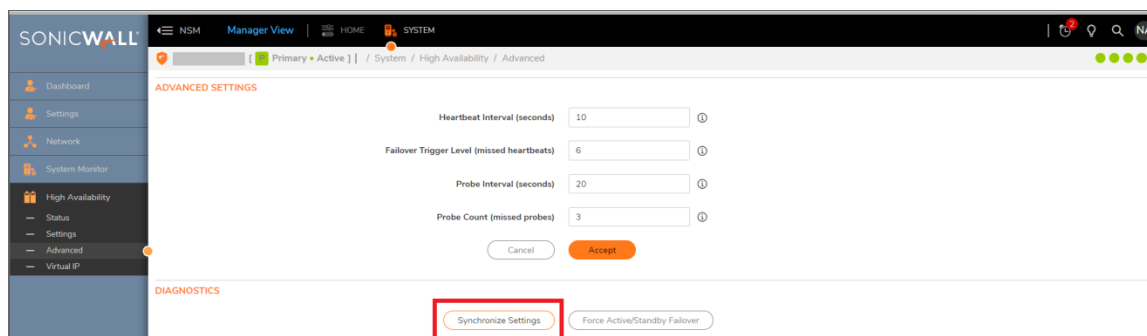


Scenario 3: Both the Primary NSM system and the Secondary NSM system gets corrupted.

In this scenario the Primary NSM system is the Active system and the Secondary NSM system is the Standby system and both got corrupt.

Below are the steps to restore back the Primary NSM system and the Secondary NSM system:

1. Restore back the Primary NSM system using any of the applicable scenarios described under [Restore NSM to a File System Backup](#).
2. Restore back the Secondary NSM system using any of the applicable scenarios described under [Restore NSM to a File System Backup](#).
3. Log into Primary NSM system, navigate to **System | High Availability > Advanced** and click on **Synchronize Settings** under **Diagnostics**.



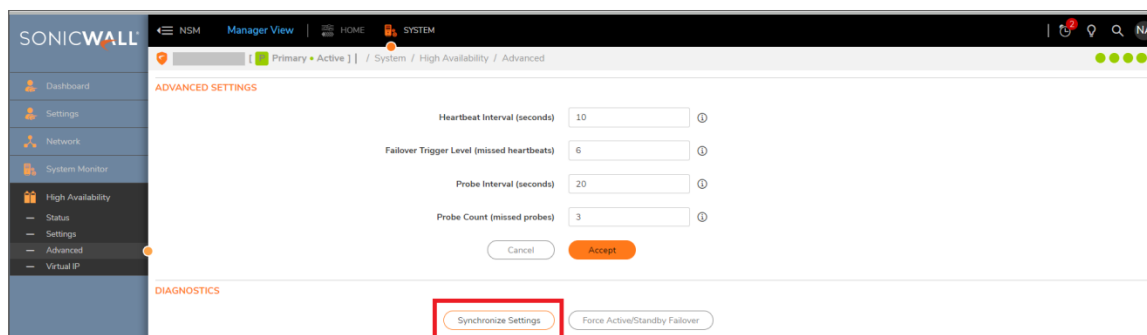
Scenario 4: Both the Primary NSM system and the Secondary NSM system are working fine and Primary system needs to be restored to an older backup.

In this scenario the Primary NSM system is the Active system and the Secondary NSM system is the Standby system and both are working fine. For any reason, the Primary NSM system needs to be restored to an older backup.

Below are the steps to restore the Primary NSM system to an older backup:

1. Shutdown the Secondary NSM system. Refer to [Shutdown/Reboot](#).
2. Restore back the Primary NSM system using any of the applicable scenarios described under [Restore NSM to a File System Backup](#).

3. Power on the Secondary NSM system using KVM, VMWare, Hyper-V or Azure.
4. Log into Primary NSM system, navigate to **System | High Availability > Advanced** and click on **Synchronize Settings** under **Diagnostics**.



NSM Management Console

This chapter describes the steps to upgrade firmware on an existing NSM On-Premises System installation.

To upgrade firmware when upgrade package(SWI file) is available please refer to [Upgrade Instructions using Upgrade Package](#).

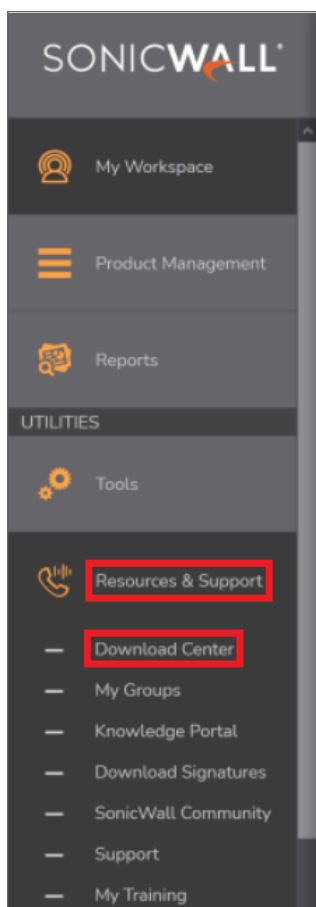
To upgrade firmware when upgrade package(SWI file) is not available please refer to [Upgrade Instructions without Upgrade Package](#).

Upgrade Instructions using Upgrade Package

This section describes the steps to upgrade NSM to NSM 2.2.5 and above using upgrade package(SWI File).

The directions are listed below:

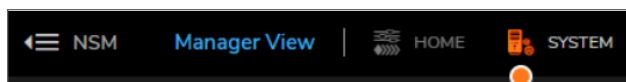
1. Login to **MySonicWall account** and navigate to **Resources & Support | Download Center**.



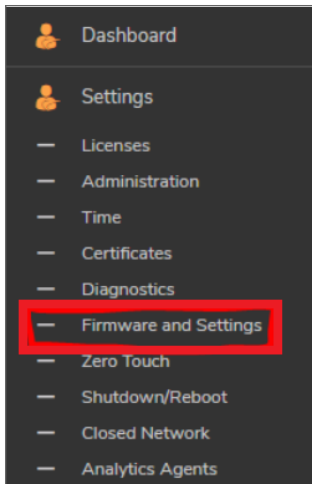
2. On the main page, search for NSM and select the file to download.

NSM-x						
#	NAME	OEM	LANGUAGE	VERSION	RELEASE DATE	RELEASE TYPE
1	NSM On-Prem 4.0.0	SonicWall, Inc	English			Feature Release

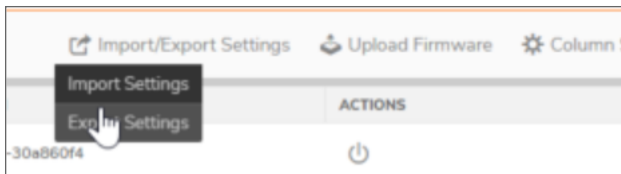
3. Save the file to your local system.
4. Login to existing NSM On-Prem Appliance.
5. Click on **System** at the top of the page.



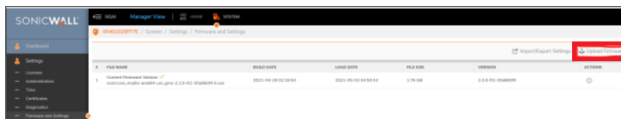
6. Navigate to **Settings | Firmware and Settings**.



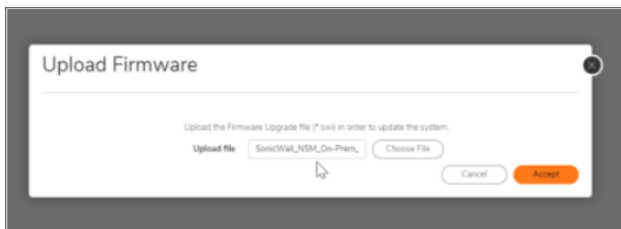
7. It is a best practice to first click the **Export Settings** option to save a backup of the current NSM configuration.



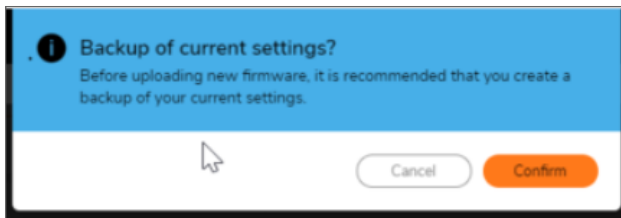
8. Click on **Upload Firmware**.



9. Browse to the firmware file downloaded in step 3 above then choose the file and click **Accept**.

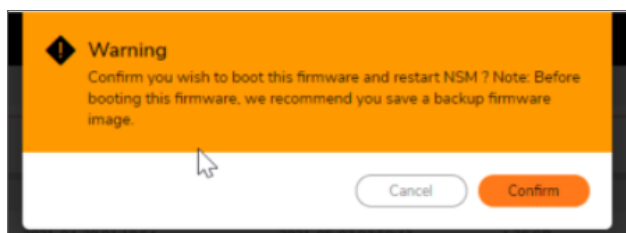


10. Click **Confirm** to continue with the upload of the firmware file.



- Once uploaded, you will see an updated page with the Current Firmware Version and the Uploaded Firmware Version. Under **Actions**, click the Power Icon on the **Uploaded Firmware Version** line and this will trigger the firmware upgrade. Click **Confirm** when the Warning banner pops up.

FILE NAME	RELEASE DATE	LAST DATE	FILE SIZE	VERSION	ACTIONS
Current Firmware Version: 2.2.0-NSM-20200901-0001	2020-09-01 00:00:00	2020-09-01 00:00:00	1.76 MB	2.2.0-NSM-20200901-0001	⏻
Uploaded Firmware Version: 2.2.0-NSM-20200901-0001	2020-09-01 00:00:00	2020-09-01 00:00:00	1.76 MB	2.2.0-NSM-20200901-0001	⏻



- Once this is done, you have completed the firmware upgrade process. You should now see the new firmware version listed as the current firmware version and your upgrade is complete.

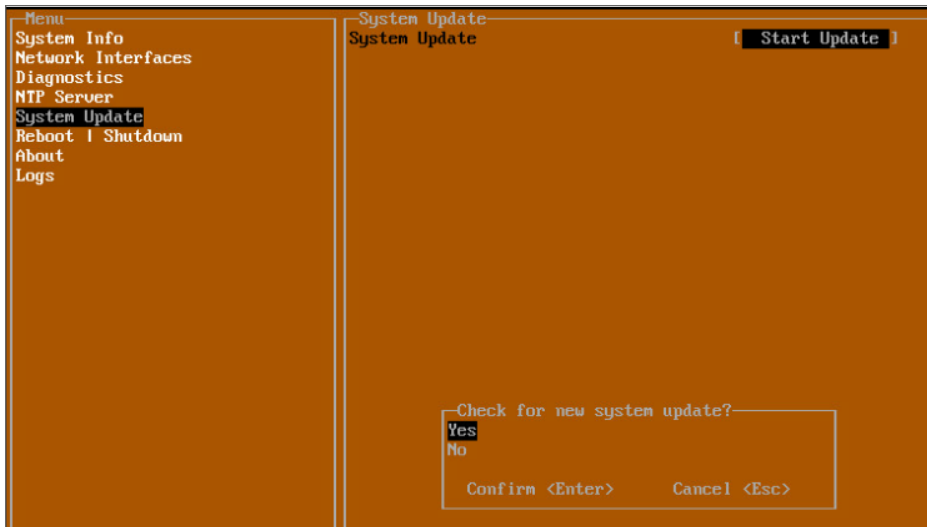
Upgrade Instructions without Upgrade Package

When upgrading from NSM to NSM 2.2.5 and below, 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.

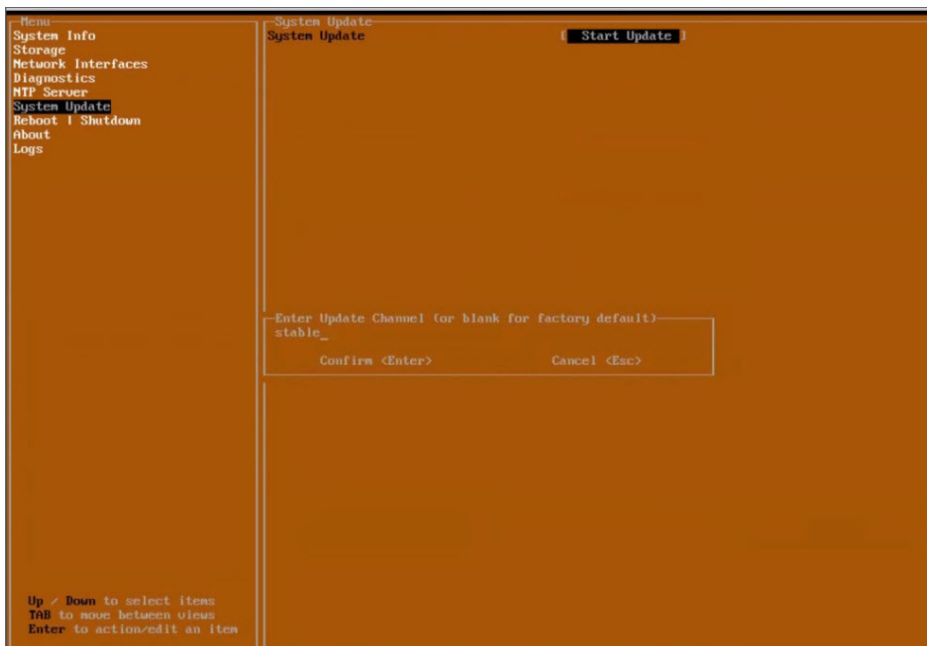
- ① | **NOTE:** The concepts and processes to upgrade NSM 2.1.1 for ESXi, KVM, and Hyper-V to NSM 2.2 are almost similar.

The directions are listed below:

- Open the NSM Management Console in NSM On-Premises Virtual Machine.
 - ① | **NOTE:** For VMWare ESXi, right click on the VM and click **Open Console**.
- Ensure that NSM on-premises virtual machine has access to internet.
- Open **Network Interfaces** menu and make any changes to network configuration, if required.
- Navigate to **System Update**.
- Click **Start Update** and then click **Yes** to check for new available updates.

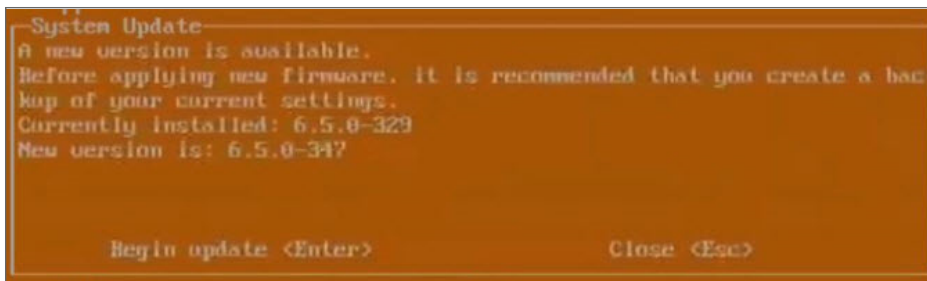


6. Press **Ctrl+P** to view or edit the update channel.



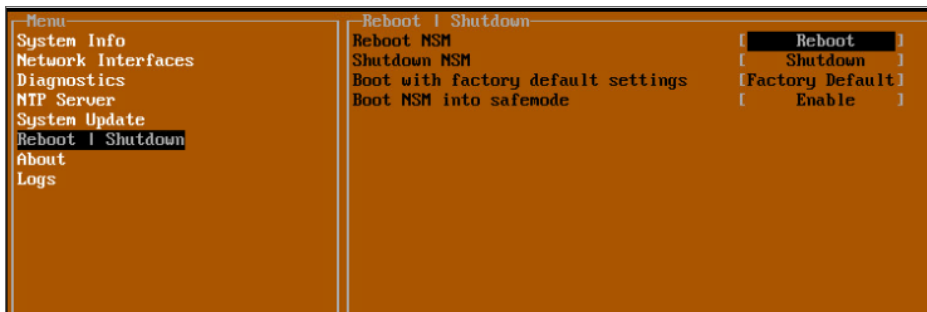
① | **IMPORTANT:** Updates are provided over update channels. The default channel is **Stable**.

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 clicking **Esc**.



① | **NOTE:** 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.

Import/Export Settings Upload Firmware Column Selection						
#	FILE NAME	BUILD DATE	LOAD DATE	FILE SIZE	VERSION	ACTIONS
1	Current Firmware Version ✓ Current Firmware		2021-02-16 01:34:51	0 B	2.2.0-14-9c09c20f	⏻

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

① | **NOTE:** A NOTE icon indicates supporting information.

① | **IMPORTANT:** An IMPORTANT icon indicates supporting information.

① | **TIP:** A TIP icon indicates helpful information.

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

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

Network Security Manager On-Premises System Administration Guide
Updated - November 2023
232-005511-00 Rev G

Copyright © 2023 SonicWall Inc. All rights reserved.

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

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

End User Product Agreement

To view the SonicWall End User Product Agreement, go to:(missing or bad snippet).

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