



Network Security Manager 2.6

Getting Started Guide

for SaaS

SONICWALL®

Contents

Overview	3
About NSM	3
Related Documents	4
Conventions	6
UI Conventions	6
Guide Conventions	6
Before Starting	8
SaaS Prerequisites	8
Supported Firewalls	8
Browser Requirements	9
SaaS Licensing Model	9
Firewall Types and Firmware	10
SaaS Importing Firewall Configurations	11
Creating an MSW Account	12
Setting Up NSM SaaS	14
Registering Your SaaS Appliance	14
Enabling Zero Touch	17
Zero Touch Deployment	17
Manual Firewall Acquisition	17
Creating Backup of Device Configuration	19
Using NSM	20
Dashboard	20
Creating a New User	21
Creating a Tenant	22
Upgrade Instructions	24
Upgrade Using Management Console	24
Upgrading SonicOS Firmware	27
SonicWall Support	29
About This Document	30

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](#)

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
<i>About Network Security Manager</i>	Provides an overview of the product and describes the base modes of operation, the navigation and icons, and the Notification Center .	<p>Read this document gain an understanding of basic tasks before diving into specific NSM topics and tasks in the other books. These include:</p> <ul style="list-style-type: none"> • Overview of NSM • Review of basic workflows • Introduction to the Dashboard and monitoring • Navigation • Notification Center <p>This document applies to both SaaS and On-Premises instances.</p>

Document	Description	When to Use It
<i>Network Security Manager Administration Guide</i>	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.
<i>Network Security Manager Reporting and Analytics Administration Guide</i>	Discusses how to use the reporting and analytics features.	<p>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.</p> <p>The Advanced license is needed to access all the Analytics features.</p>
<i>Network Security Manager On-Premises System Administration Guide</i>	Describes the system administration tasks for an on-premises deployment of NSM.	<p>Read this document to understand how to configure and manage an on-premises instance of NSM. It includes:</p> <ul style="list-style-type: none"> • System Dashboard • System settings • Network settings • System monitoring • High Availability (HA) configuration <p>This document applies to On-Premises instances only.</p>
<i>Network Security Manager Getting Started Guide for SaaS</i>	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.
<i>Closed Network Feature Guide</i>	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.
<i>NSM Release Notes</i>	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 .
<code>Computer code</code>	Indicates sample code or text to be typed at a command line.
<i><Computer code italic></i>	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 <code>serialnumber=<your serial number></code> , replace the variable and brackets with the serial number from your device: <code>serialnumber=C0ABC0000001</code> .
<i>Italic</i>	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.

Before Starting

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

Topics:

- [Installation Quick Start](#)
- [Supported Firewalls](#)
- [Creating an MSW Account](#)

SaaS 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 instance must be in a single Group or Tenancy.
- Each firewall should have HTTPS management enabled.

① **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.

Supported Firewalls

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

		Latest Supported SonicOS Version
Generation	Firewall Model	

Gen 6	SOHO W	6.5.4
	TZ Series: TZ300, TZ300W, TZ300P, TZ350, TZ350W, TZ400, TZ400W, TZ500, TZ500W, TZ600, TZ600P	6.5.4
	NSv Series: NSv 10, NSv 25, NSv 50, NSv 100, NSv 200, NSv 300, NSv 400, NSv 800, NSv 1600	6.5.4
	NSA Series: NSA 2600, NSA 3600, NSA 4600, NSA 5600, NSA 6600	6.5.4
	NSa Series: NSa 2650, NSa 3650, NSa 4650, NSa 5650, NSa 6650, NSa 9250, NSa 9450, NSa 9650	6.5.4
	NSsp Series: NSsp 12400, NSsp 12800	6.5.4
Gen 7	TZ Series: TZ270, TZ270W, TZ370, TZ370W, TZ470, TZ470W, TZ570, TZ570W, TZ570P, TZ670	7.1.2
	NSv Series: NSv 270, NSv 470, NSv 870	7.1.2
	NSa Series: NSa 2700, NSa 3700	7.1.2
	NSsp Series: NSsp 15700	7.1.2

Browser Requirements

NSM is a cloud service that can be accessed over the internet by using one of these supported browsers:

Browser Supported	Notes
Google Chrome	Latest version ⓘ NOTE: This is the preferred browser for the real-time graphics display on the Dashboard.
Apple Safari	Latest version
Microsoft Edge	Latest version
Mozilla Firefox	Latest version

SaaS Licensing Model

The SaaS licensing model is described as below:

- **Gen6 and Gen 7 Devices -**
 - Device has to be licensed with **NSM Essential License** or **NSM Advanced License** to be able to be managed by NSM SaaS.

Firewall License	NSM SaaS
NSM Essential License	Allows device management and 7 days of basic reporting.

Firewall License	NSM SaaS
NSM Advanced License	Allows device management along with comprehensive reporting and analytics.

- **TZ80 Devices -**

- TZ80 devices will be available only as a bundle. NSM will be bundled as a service in a firewall license bundles.
- TZ80 devices will function only with a valid license.
 ⓘ | **NOTE:** TZ80 hardware will not function after a 30 days trial period without a valid license.
- TZ80 devices have to be bundled with **Secure Connect** license or **Advanced Protection Service Suite (APSS)** license or **Managed Protection Service Suite (MPSS)**.

Firewall License Bundle	NSM SaaS
Secure Connect	Allows device management. Supports add on data retention pack for 7 days, 30 days, 90 days, and 365 days of reporting and analytics.
Advanced Protection Service Suite (APSS)	Allows device management along with <ul style="list-style-type: none"> • 7 days of advanced reporting and analytics. • DNS Filtering. • Content Filtering service. • Gateway Anti-malware/Intrusion Prevention/App Control. • Comprehensive Anti-Spam Service. • Capture Advanced Threat Protection. • Support of add on data retention pack for 30 days, 90 days, and 365 days of reporting and analytics.
Managed Protection Service Suite (MPSS)	Allows all features of APSS license but only for 30 days. There is no support for add-on data retention pack.

- NSM will not support 7-days SonicWall Flow Report (SFR) for TZ80 firewalls. The TZ80 device and related data, including any reporting and analytics data stored in NSM, will be deleted from NSM after 90 days of the TZ80 bundle license expiry.

Firewall Types and Firmware

The following firewall models can be managed by the Network Security Manager services.

	Management	Reporting	Analytics
Entry Level Firewalls	SOHO W	SOHO W	SOHO W
	TZ Series	TZ Series	TZ Series
	NSv 10-100	NSv 10-100	NSv 10-100
Mid-Range Firewalls	NSa 2500-6600	NSa 2500-6600	NSa 2500-6600
	NSa 2650-6650	NSa 2650-6650	NSa 2650-6650
	NSv 200-400	NSv 200-400	NSv 200-400
High-End Firewalls	SuperMassive 9000	NSM On-Premises can store the logs locally and with management in CSC-MA.	NSM On-Premises can store the logs locally and with management in CSC-MA.
	12K Series		
	NSa 9250-9650		
	NSv 800-1600		
Zero Touch Deployment	SOHO-W with firmware 6.5.2 or later		
	TZ Series, NSA Series, NSa Series with firmware 6.5.1.1 or later		
	Not supported for SOHO, NSv Series or SuperMassive Series		

Additional requirements include:

- Each firewall needs to be licensed with the Comprehensive/Advanced Gateway Security Suite (CGSS/AGSS).
- The firewalls in the configuration must be a part of a tenant.
- Each firewall must have HTTPS management enabled.

❗ **IMPORTANT:** For manually added firewalls, if a firewall is behind a NAT device, the HTTPS management port must be opened for the cloud services to communicate with the firewall. This does not apply to firewalls that use Zero Touch Deployment.

SaaS Importing Firewall Configurations

The import of configuration settings is not supported from SonicWall firewalls in an NSM configuration.

You can export the configuration settings to support re-deployment of an instance after it is set up.

❗ **NOTE:** SonicWall recommends that you do not use the VMware snapshot functionality. For more information, see <https://kb.vmware.com/s/article/1025279>.

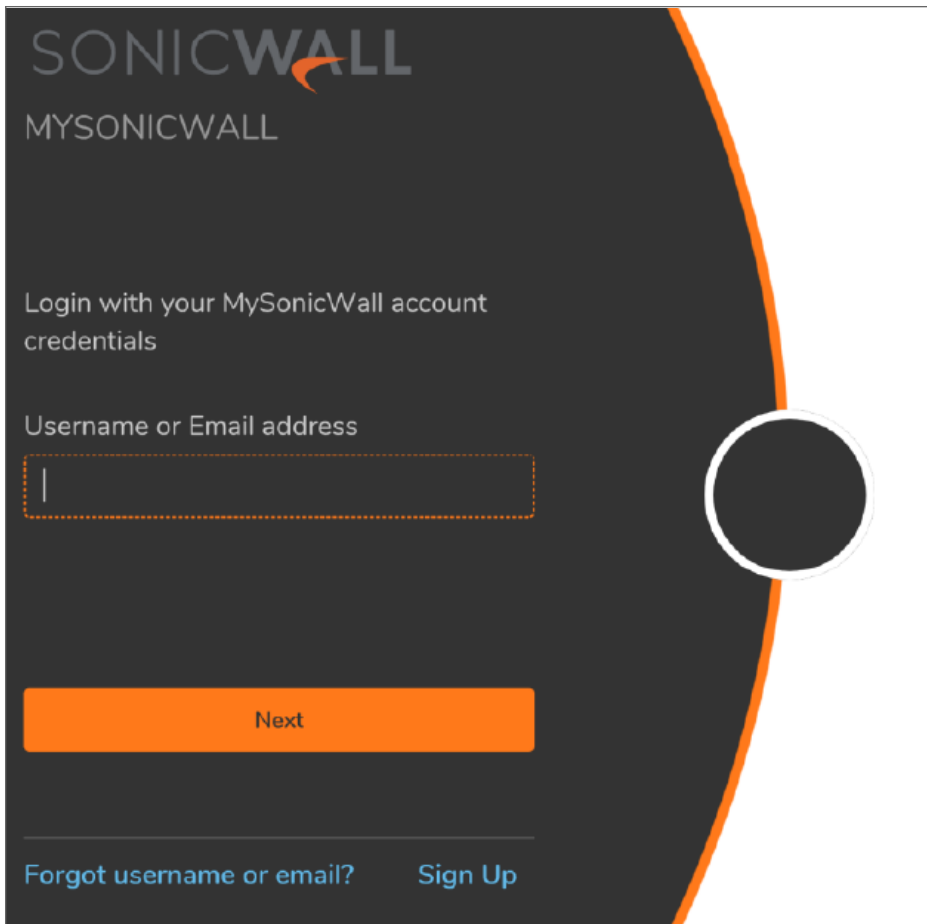
Creating an MSW Account

A MySonicWall account is required to register the NSM instance.

① | **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.

Setting Up NSM SaaS

Use topics in this chapter to set up NSM SaaS appliance.

- [Creating a Tenant](#)
- [Creating a Tenant](#)
- [Creating a Tenant](#)
- [Manual Firewall Acquisition](#)
- [Creating Backup of Device Configuration](#)

Registering Your SaaS Appliance

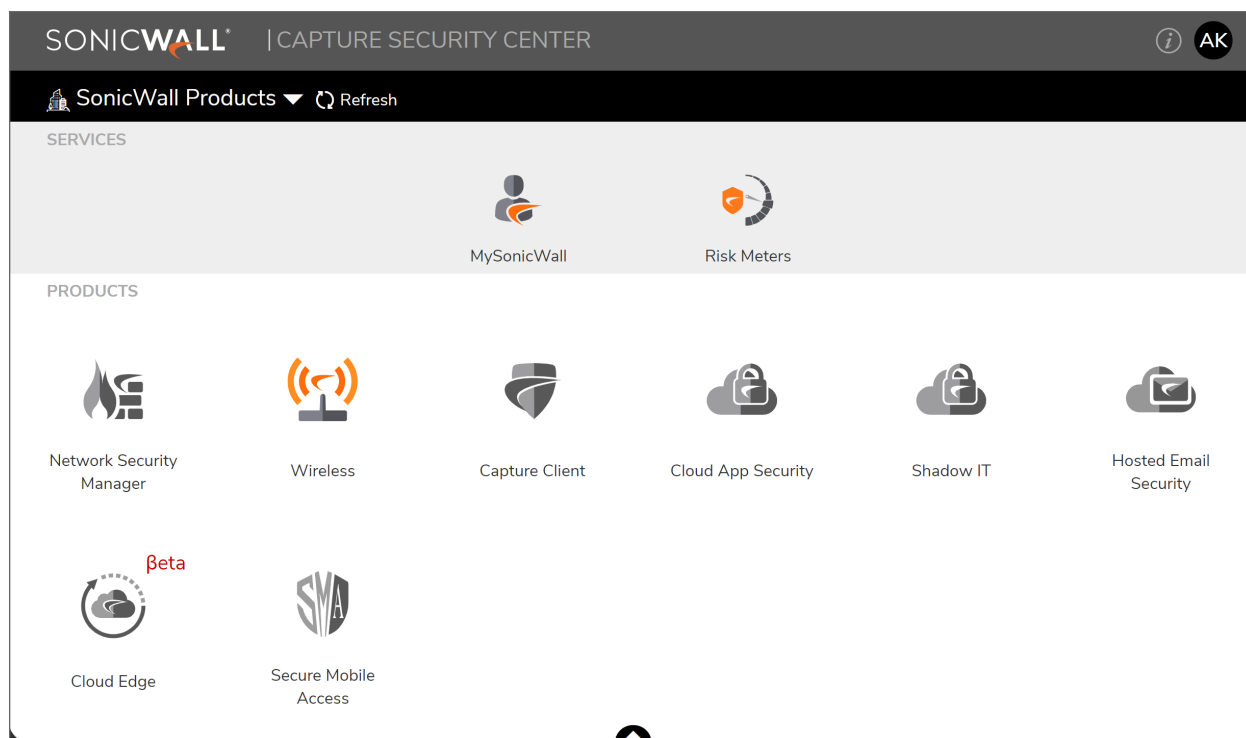
Before starting this section, be sure to have the serial number and the authentication code. You can get that from a label on the firewall or on the box it came in.

To register the appliance:

1. Navigate to <https://cloud.sonicwall.com>.
2. Log in using your MySonicWall credentials.
3. Select the **MySonicWall** tile.
4. Click **Register products**.
5. Create a tenant.
6. Select a tenant and register the device.
7. Enter the serial number and the authentication code.
8. Enter a friendly name.
9. Click **Choose management options**.
10. Select **Cloud**.

① **NOTE:** You need to enable the NSM license to get the **Cloud** option. The only option that is enabled is **On-Box**. To enable the **Cloud** option, go to **Licensing** and enable the NSM license. Then select the **Cloud** option.

11. Navigate back to the Network Security Manager by clicking the down arrow at the top of the screen.
12. Click the **Licensing** tile.
13. Click the **Try** button next to the firewall you are setting up.
14. Wait for a few seconds until you see the green confirmation at the bottom of the screen.
15. Navigate back to the Capture Security Center by clicking the down arrow at the top of the screen.



16. Click on **Firewalls** tile to sign-into NSM. You are directed to **Firewall Inventory** page where you can start managing registered firewalls.

SONICWALL

NSM

Manager View

HOME

MONITOR

Commit & Deploy

9:30 AM

NA

Global Default Tenant / Home / Firewalls / Inventory

ALL DEVICES

125

ONLINE & MANAGED

28

68%

OFFLINE

85

10%

ONLINE & UNMANAGED

12

ED66%

UNASSIGNED

82

Q Search...

Group By: No Grouping

+ Add

Delete

Export

Refresh

Grid Settings

More Options

<input type="checkbox"/>	#	NAME	SERIAL NUMBER	GROUP	MODEL	TAGS	CONNECTIVITY	CONFIGURATION	ACTION
<input type="checkbox"/>	1	testnsmtggrp01	NSA1234567890	Unassigned	NSA 2400	TVC	Offline	Unmanaged	
<input type="checkbox"/>	2	testnsmtggrp02	NSA1234567890	Unassigned			Offline	Unmanaged	
<input type="checkbox"/>	3	testnsmtggrp03	NSA1234567890	Unassigned			Offline	Unmanaged	
<input type="checkbox"/>	4	testnsmtggrp04	NSA1234567890	Unassigned			Offline	Unmanaged	
<input type="checkbox"/>	5	TestDevice	NSA1234567890	Unassigned			Offline	Unmanaged	
<input type="checkbox"/>	6	TestDevice	NSA1234567890	Unassigned			Offline	Unmanaged	
<input type="checkbox"/>	7	Test1	NSA1234567890	Rashid Testing Group 2			Offline	Unmanaged	
<input type="checkbox"/>	8	Test1	NSA1234567890	Unassigned			Offline	Unmanaged	
<input type="checkbox"/>	9	Testnsmtggrp05	NSA1234567890	Unassigned	NSv 400	nsv800	Offline	Unmanaged	
<input type="checkbox"/>	10	Test1	NSA1234567890	testsk			Offline	Unmanaged	
<input type="checkbox"/>	11	Test-7-800	NSA1234567890	Unassigned	NSv Unlicensed		Offline	Unmanaged	
<input type="checkbox"/>	12	Test-7-800	NSA1234567890	Unassigned	NSv 800		Offline	Unmanaged	
<input type="checkbox"/>	13	testnsmtggrp06_group	NSA1234567890	Unassigned	NSv 800	NSV	Offline	Unmanaged	

Enabling Zero Touch

Zero Touch Deployment allows firewalls to be automatically acquired by your network infrastructure with minimal user intervention. It pushes policies, performs firmware upgrades and synchronizes licenses. You must opt in for Zero Touch Deployment by setting it up in your MySonicWall profile.

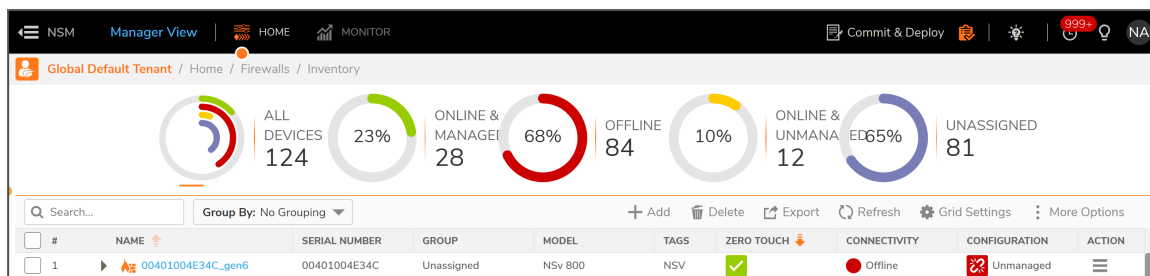
To set up Zero Touch:

1. Login to your MySonicWall account.
2. Navigate to **My Workspace > My Reports**.
3. Click on a product's serial number.
4. In the **PRODUCT DETAILS** page, under **Active Support**, toggle the **Enable Zero Touch** switch.

Zero Touch Deployment

Zero Touch Deployment is initiated before you plug your firewall into the network. You need to enable Zero Touch by setting it up in your MySonicWall profile. Refer to [Enabling Zero Touch](#) for more information.

To validate Zero Touch status, navigate to **Manager View | HOME > Firewalls > Inventory**.



Refer to the **ZERO TOUCH** column to see the status of the Zero Touch connection. If you mouse over the icon, a pop-up defines the status further as shown in the following example.

VERSION	ZERO TOUCH
SonicOS Enhanced 6.5.1.3-12n	✓
Waiting for Zero Touch connection from firewall	⏸
Unknown	⚠

Manual Firewall Acquisition

Under certain conditions you may opt to acquire a firewall manually rather than using Zero Touch.

- ① **NOTE:** When acquiring manually, **SSL cert verify** is enabled by default. This is set as a security feature, but if proper SSL certification is not enabled on the firewall, the firewall does not get acquired.

To acquire a firewall manually:

1. Click on the three dots under **Action** in the Firewall Inventory page.

#	NAME	SERIAL NUMBER	GROUP	MODEL	TAGS	CONNECTIVITY	CONFIGURATION	ACTION
1	TZ300-ghan	18B169BFA018	Unassigned	TZ 300		Online	Managed	<ul style="list-style-type: none">Switch to Firewall ViewEdit SettingsSynchronize FirewallUpgrade FirmwareArchive ConfigAuditManage CommitsScheduled ReportsExport to TemplateDelete Firewall

2. Select **Edit Settings**.

Edit Settings

Serial Number: 18B169BFA018

Friendly Name: TZ300-ghan

IP Address with Port (Example: 34.25.61.2:443): 10.194.52.89

Verify SSL Certificate: ☒

Username: admin

Password:

Tags (Example: TZ, BranchA): TZ, BranchA

DEVICE ACQUISITION STATUS

- ☒ Connected to device.
- ☒ Configuration synchronized.
- ☒ Acquired

Your device might reboot to enable Reporting & Analytics

Cancel Save Acquire Again

3. Enter **IP Address with Port**, **Username**, and **Password**.
4. Click **Save** and **Acquire**.

NSM pulls the status and configuration of the firewall as part of the acquisition. It also configures the firewall to send out syslog heartbeats so its health can be monitored. The firewall shows in green if the acquisition is successful.

Creating Backup of Device Configuration

Creating configuration backups enables you to restore a firewall configuration anytime.

To create a configuration backup of a device:

1. Navigate to **Manager View | Firewalls > Inventory**.
2. Hover over the device for which you want to create a configuration backup and click **Ellipses** icon in the **Action** column.
3. Select **Archive Config**.
4. Click **OK** to confirm.

To validate the backup:

1. Navigate to **Manager View | Config Management > Audit**.
2. Select the appropriate device from the **Devices** drop-down list.
3. View the entries in the **Audit** table to find the backup.
4. Click the arrow next to the date of the backup. The entry expands to show the configuration file that was backed up.

Using NSM

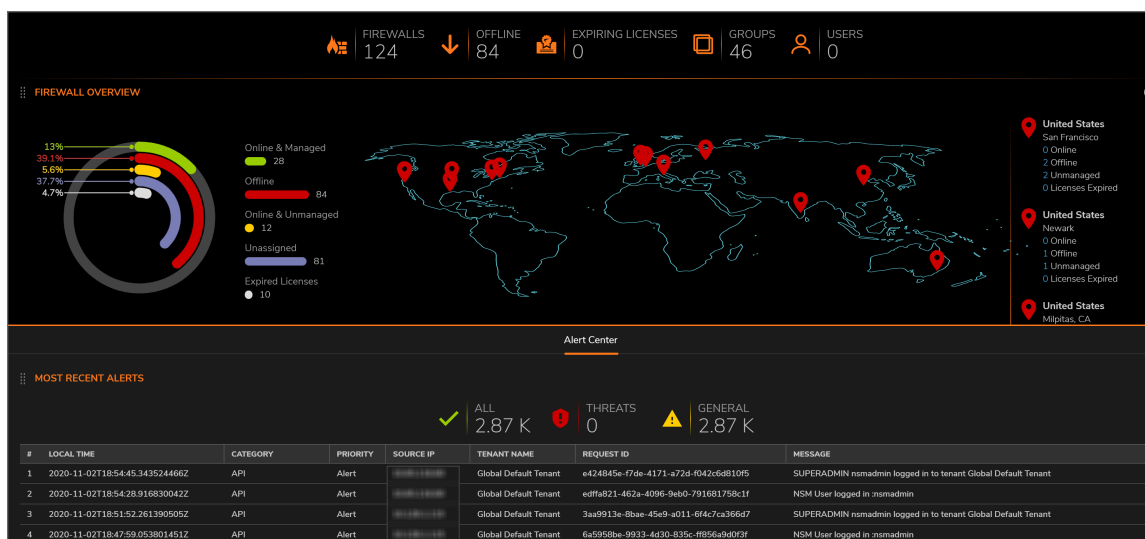
This section describes more about the following topics:

- [Dashboard](#)
- [Creating a New User](#)
- [Creating a Tenant](#)

Dashboard

The **Dashboard** provides a visual status of the security infrastructure. The Dashboard is separated into **Devices**, **Summary**, **Network** and **Threat** tabs.

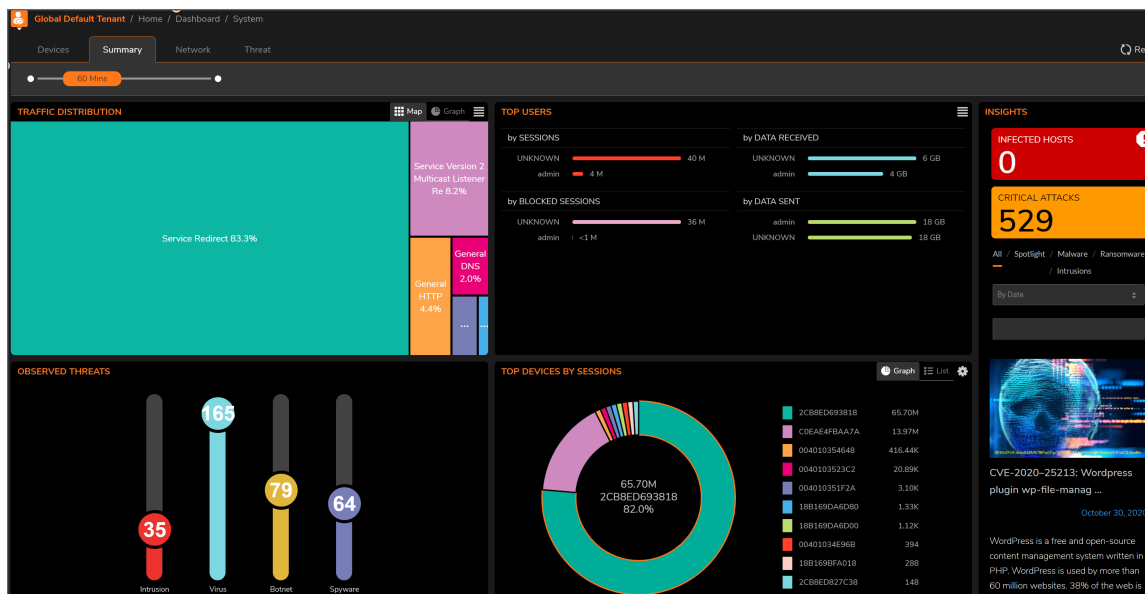
The **Devices** Dashboard shows a summary of the devices in your infrastructure.



At the top of the dashboard, you see a summary of your devices, followed by the **Firewall Overview**. The overview shows how many devices are **Online & Managed**, **Offline**, **Online & Unmanaged**, **Unassigned**, and **Expired Licenses**. The **Alert Center** is shown at the bottom of the dashboard. An alert summary is provided and

you can click on **Show All Alerts ...** to open the **Notification Center** and see all the alerts. The alerts are shown in table form below the summary.

The **Summary** Dashboard shows more detail. The **Summary** view shows **Traffic Distribution**, **Top Users** and **Observed Threats**. The other two tabs allow you to drill down on **Network** and **Threat** information.



Creating a New User

To add users:

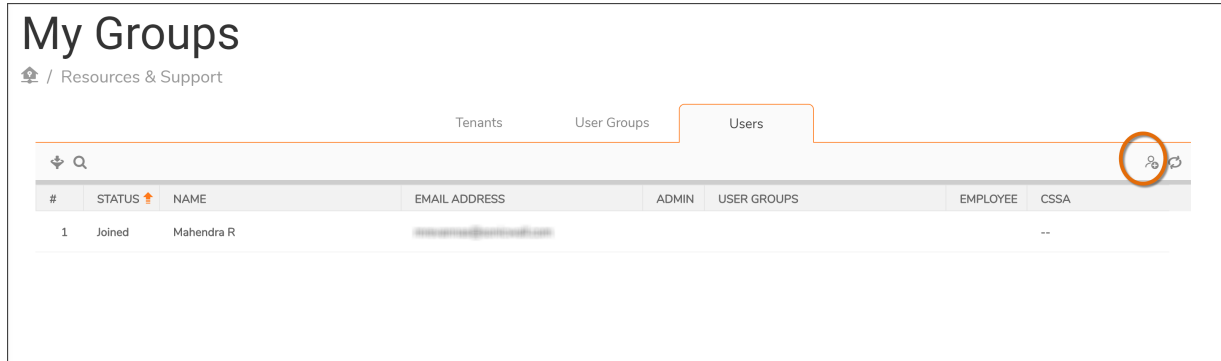
1. Log into your mysonicwall.com account.
2. Under **Resources and Support**, click **My Groups**.

The screenshot shows the 'MyGroups' page in the MySonicWall interface. The page has a sidebar with navigation links: 'My Workspace', 'Product Management', 'Reports', 'UTILITIES', 'Tools', 'Resources & Support', 'Download Center', 'My Groups', 'Knowledge Portal', 'SonicWall Community', 'Support', and 'My Training'. The main content area is titled 'MyGroups' and includes a sub-header 'Resources & Support'. Below this, there are tabs for 'Tenants', 'User Groups', and 'Users'. The 'Users' tab is selected, displaying a table with the following data:

#	TENANT NAME	USER GROUP	TOTAL PRODUCTS	OWN GROUP	DEFAULT GROUP
1	004010278638	SonicWall Users	0	✓	
2	Firewall	SonicWall Users	0	✓	
3	NSM 2.0 Beta	SonicWall Users	1	✓	
4	New	SonicWall Users	0	✓	
5	SonicWall Products	SonicWall Users	2	✓	✓

At the bottom of the table, it says 'Total: 5 items'.

3. Click the **Users** tab.



My Groups
/ Resources & Support

Tenants User Groups **Users**

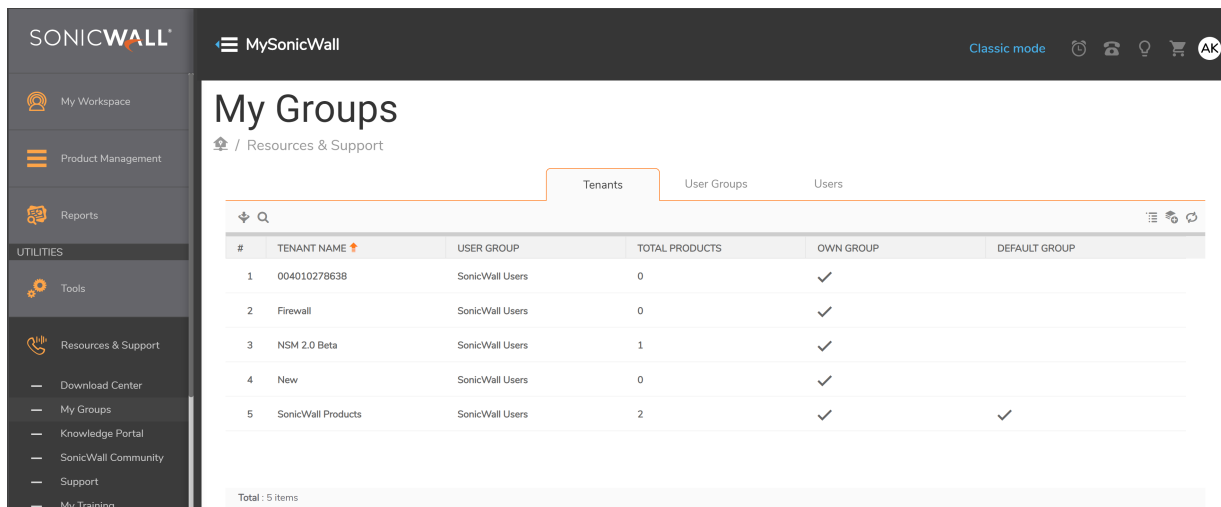
#	STATUS	NAME	EMAIL ADDRESS	ADMIN	USER GROUPS	EMPLOYEE	CSSA
1	Joined	Mahendra R	mahendra@sonicwall.com				--

4. Click the New User icon.
5. In the Create New User window, enter the details and click **Confirm**.

Creating a Tenant

To add users:

1. Log into your mysonicwall.com account.
2. Under **Resources and Support**, click **My Groups**.



SONICWALL MySonicWall Classic mode

My Groups
/ Resources & Support

Tenants User Groups Users

#	TENANT NAME	USER GROUP	TOTAL PRODUCTS	OWN GROUP	DEFAULT GROUP
1	004010278638	SonicWall Users	0	✓	
2	Firewall	SonicWall Users	0	✓	
3	NSM 2.0 Beta	SonicWall Users	1	✓	
4	New	SonicWall Users	0	✓	
5	SonicWall Products	SonicWall Users	2	✓	✓

Total: 5 items

3. Click the **New Tenant** icon located on the right-hand side.



4. In the **Create New Tenant** window, enter a name for the tenant and select UserGroup.

CREATE NEW TENANT

×

Enter a group name to create new tenant to share the products

Tenant Name

TenantGroup

UserGroup Name

SonicWall Users

Cancel

Confirm

5. Click **Confirm**.
6. Register new devices under this tenant.

Upgrade Instructions

This section describes more about the following topics:

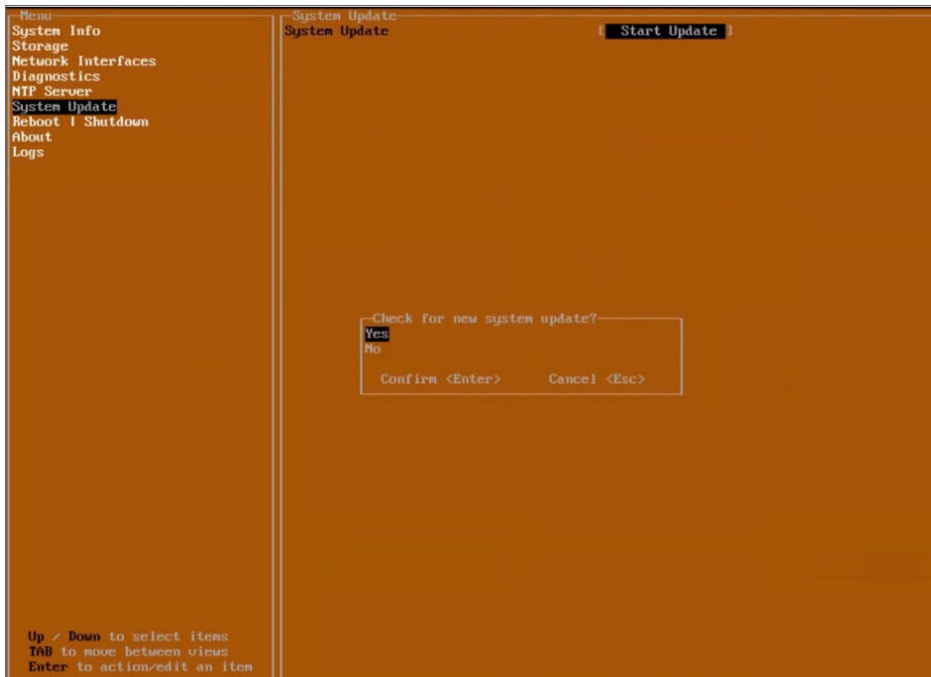
- [Upgrade Using Management Console](#)
- [Upgrading SonicOS Firmware](#)

① | **IMPORTANT:** Before upgrading your NSM system, take a backup of your configuration. Follow the steps provided in [Taking Backup of NSM SaaS before Upgrade](#).

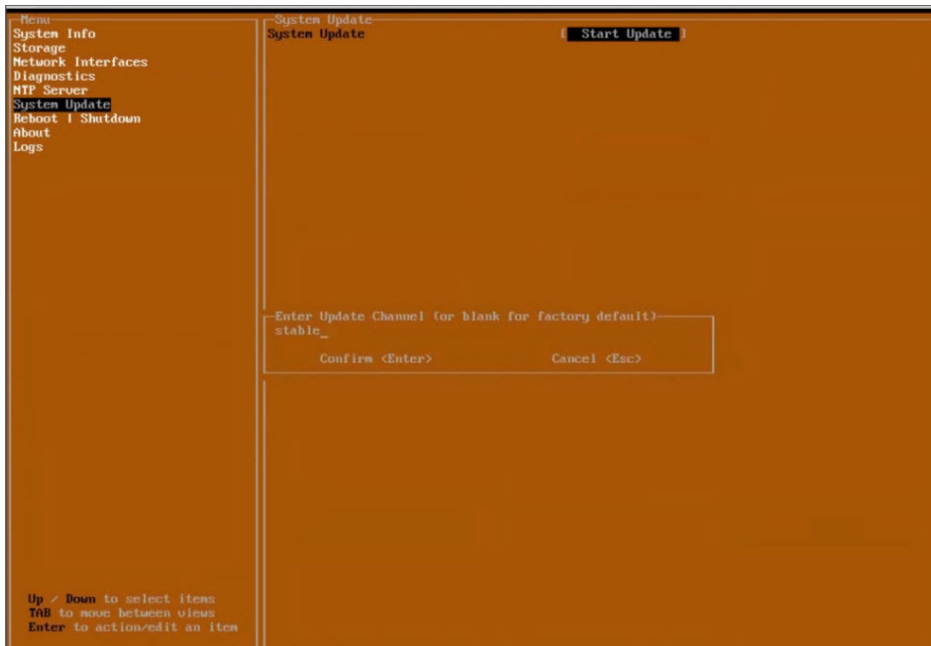
Upgrade Using Management Console

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.

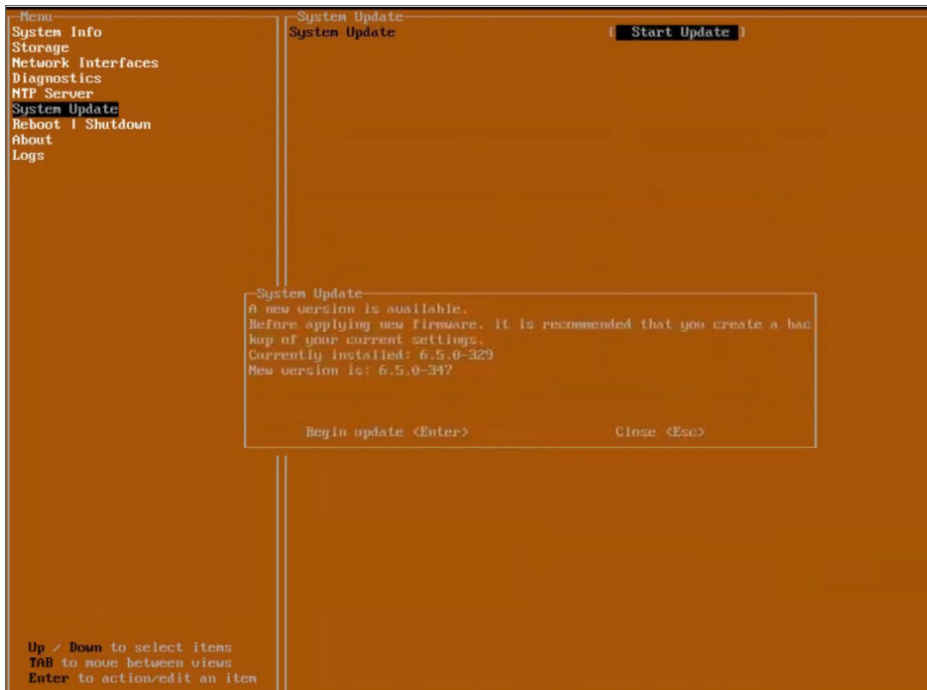


6. Press **Ctrl+P** to view or edit the update channel.



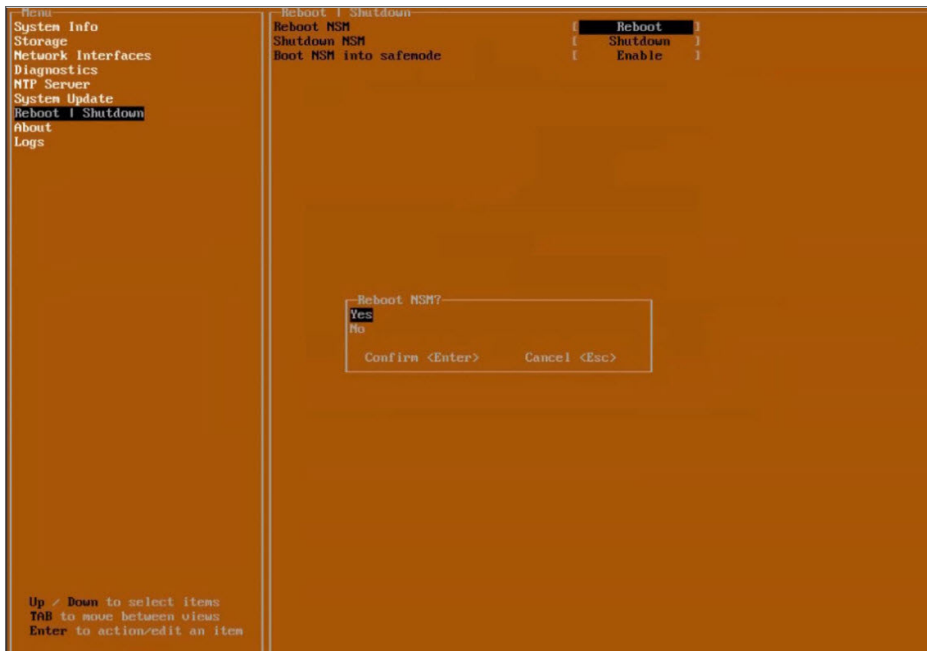
IMPORTANT: Updates are provided over update channels. The default channel is **Stable**.

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.

Import/Export Settings Upload Firmware Column Selection						
#	FILE NAME	BUILD DATE	LOAD DATE	FILE SIZE	VERSION	ACTIONS
1	Current Firmware Version ✓ Current Firmware		2021-02-16 01:34:51	0 B	2.2.0-R4-8c09e2df	⏻

Upgrading SonicOS Firmware

To upgrade SonicOS firmware on a firewall:

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

1

2

UPGRADE

STATUS

SYSTEM DETAILS

Name

Gen7_270W_fw

Current Version

SonicOS 7.0.1-5119

AVAILABLE SOFTWARE VERSION(S)

Please select a Firmware to Upload.

Browse

Upload

<input type="checkbox"/>	#	VERSION	FILENAME	RELEASE DATE	RELEASE TYPE
<input type="checkbox"/>	1	local_firmware_Maintenance_sw_tz_270-5119-R4713.bin	Maintenance_sw_tz_270w_eng.7.0.1-5119-R4713.bin.sig	Tue Jul 4 03:52:30 UTC 2023	Local Firmware

Total: 1 Item(s)

SCHEDULED UPGRADE

Schedule

☒ Now ☐ Later

07/04/2023 18:14

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

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

SonicWall Support

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

The [Support Portal](#) provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year.

The [Support Portal](#) enables you to:

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

About This Document

Network Security Manager SaaSGetting Started Guide for SaaS

Updated - October 2024

Software Version - 2.6

232-005712-00 Rev B

Copyright © 2024 SonicWall Inc. All rights reserved.

The information in this document is provided in connection with SonicWall and/or its affiliates' products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of products.

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

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

End User Product Agreement

To view the SonicWall End User Product Agreement, go to: <https://www.sonicwall.com/legal/end-user-product-agreements/>.

Open Source Code

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

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