



Network Security Manager

Administration Guide

SONICWALL®

Contents

Network Security Manager Overview	4
About Network Security Manager	4
API Support	5
Legal Information	5
Conventions	6
Guide Conventions	6
UI Conventions	6
Related Documents	7
Dashboard	8
Summary	9
Network	10
Threat	11
Firewalls	13
Device Inventory	13
Device Status	15
Managing Devices	19
Device Groups	24
Working with Device Groups	25
Backups	28
Scheduling Backups	30
Archiving TSR	30
Archiving EXP	30
Templates	32
Templates Inventory	32
Creating Templates	34
Editing Templates	34
Viewing Template Configuration	35
Creating Duplicate Template	35
Modifying Template Attributes	35
Applying Templates	36
View Template Status	37
Deleting Templates	37
Configuration Management	39
Approval Groups	39
Approval Workflow Settings	39

Approval Group Management	40
Configuration Management Workflow	43
Viewing Pending-Configuration Updates	43
Committing and Deploying the Updates	44
Discarding Pending Configurations	46
Monitoring Commits	47
Managing Commits	48
Editing Commits	48
Redeploying Commits	48
Rescheduling Commits	49
Deleting Commits	49
Auditing Configuration Changes	50
Tenants	51
CSC Users	52
CSC User Status	52
Users	53
Sorting and Filtering	54
Editing CSC Users	54
Support Portal Users	55
Roles and Permissions	56
Scheduled Reports	58
Managing the Schedules	58
Creating Scheduled Reports	59
Editing Schedule	62
Running Reports Manually	63
Setting the Report Date Range	63
Archived Reports	64
Downloading Archived Reports	65
System Events	66
Configuring Log Settings	66
Viewing System Events	66
SonicWall Support	69
About This Document	70

Network Security Manager Overview

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

Topics:

- [About Network Security Manager](#)
- [API Support](#)
- [Legal Information](#)
- [Conventions](#)
- [Related Documents](#)

About Network Security Manager

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; it provides comprehensive visibility, 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 the network security services with a single-pane-of-glass experience.

This security management platform is a SaaS (Software-as-a-Service) or an on-premises offering, depending on your needs. The SaaS offering is accessible on-demand, via the cloud, with virtually unlimited system scalability to support multiple tenants with thousands of security nodes under each one. The solution's redundant and distributed architecture 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.

The on-premises offering is for those customers that don't want to opt for a cloud solution. It can be deployed on multiple form factors such as ESXi and Hyper-V. The architecture allows you to scale to 10,000 devices under management and will support migration from Global Management System (GMS) in the future release.

NSM offers many salient features:

- On-boarding 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
- Make informed decision and policy actions to any threat, quickly and in real time, with detailed reporting and powerful analytics

NSM can manage both Gen6 and Gen7 SonicWall firewalls. SonicOS 6.4.5 is the minimum version allowed for management by NSM.

API Support

A RESTful (Representational State Transfer) API (application programming interface) has been developed for Network Security Manager. This allows you to either script or build custom user interface elements to manage a unit or tenant if you do not want to use the default user interface. Managed service providers (MSPs) may find this feature especially useful when customizing the product for their use. Navigate to **Manager View|API** for details.

COPYRIGHT & LIMITED LIABILITY

© 2020 SonicWall Inc. ALL RIGHTS RESERVED.

SonicWall is a registered trademark of SonicWall Inc. All other trademarks are property of their respective owners.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OR MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON- INFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT, OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

SONICWALL END USER PRODUCT AGREEMENT

PLEASE READ THIS AGREEMENT CAREFULLY BEFORE USING SONICOS API BY DOWNLOADING, INSTALLING OR USING THIS API, YOU ACCEPT AND AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT. FOR DELIVERIES OUTSIDE THE UNITED STATES OF AMERICA, PLEASE GO TO NSM API SPECIFICATION <https://nsm-uswest.sonicwall.com/api/docs/nsm> AND SONICOS API SPECIFICATION <https://nsm-uswest.sonicwall.com/api/docs/sonicos> TO VIEW THE APPLICABLE VERSION OF API FOR YOUR PRODUCT. IF YOU DO NOT AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT, DO NOT DOWNLOAD, INSTALL OR USE THIS API.

In the **SONICWALL END USER PRODUCT** section, links to the *NSM API Specification* and the *SonicOS API Specification* are provided. Do not download, use or install the APIs if you do not agree to the terms of the End Product User Agreement.

Legal Information

SonicWall Network Security Manager is protected by copyright and is provided as *is*. The details associated with this status are provided on the **Legal Information** page. Navigate to **Manager View | > Legal Information** to read the details:

- Copyright and Limited Liability
- SonicWall End User Product Agreement

For deliveries outside the United States, go to [SonicWall End User General Product Agreement](#) for more details.

COPYRIGHT & LIMITED LIABILITY

© 2020 SonicWall Inc. ALL RIGHTS RESERVED.

SonicWall is a registered trademark of SonicWall Inc. All other trademarks are property of their respective owners.

END USER PRODUCT AGREEMENT

The terms and conditions applicable to your download and use of this product are located at <https://www.sonicwall.com/legal/#tab-id-3> ("Agreement"). Please read this Agreement carefully as it contains provisions such as how you may use the product and associated restrictions, warranties and warranty disclaimers, limitation on damages and remedies that may be claimed, audit rights. BY DOWNLOADING, INSTALLING OR USING THIS PRODUCT, YOU ACCEPT AND AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT, DO NOT DOWNLOAD, INSTALL, ACCESS OR USE THE PRODUCT BECAUSE YOU DO NOT HAVE A LICENSE TO THE PRODUCT.

Conventions

The *Network Security Manager Administration Guide* guide makes use of the following conventions:

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

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 option is selected. Then click on Firewall in the left-hand menu, and select Groups .
Computer code	Indicates sample code or text to be typed at a command line.
<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 <i>serialnumber=<your serial number></i> , replace the variable and brackets with the serial number from your device: <i>serialnumber=C0AEA0000011</i> .
Italic	Indicates the name of a technical manual. Also indicates emphasis on certain words in a sentence, such as the first instance of a significant term or concept.

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 Definition

Icon



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 an unknown status.



Indicates the device is online.



Indicates the device is offline.



Indicates the device is unmanaged.



Indicates the device is managed.

Related Documents

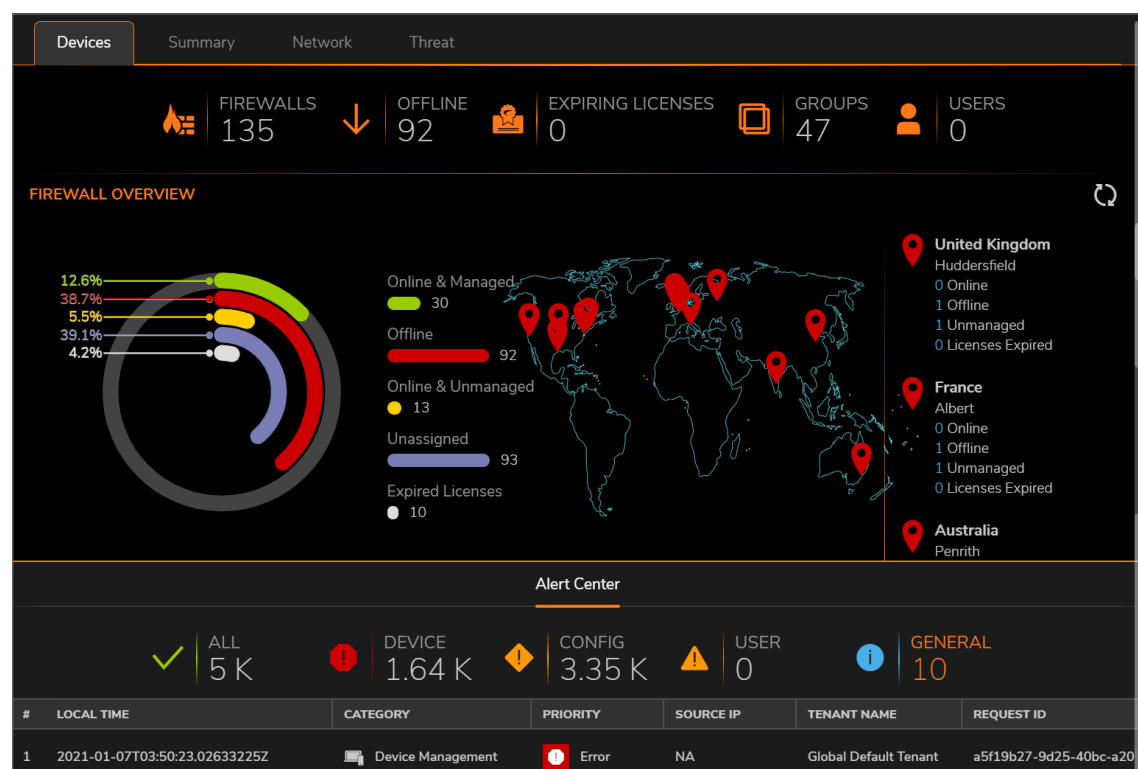
The NSM documentation includes the following:

- *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 Dashboard provides a visual status of the security infrastructure. You can review the Dashboard and see at a glance if any issues need investigating. The system dashboard has four tabs: **Device**, **Summary**, **Network**, and **Threat**. You can quickly see the summary of status of devices, traffic distribution, and threats to know whether you have issues and where to focus to resolve them.

The default view of system dashboard is **Devices** dashboard. It shows a summary of the devices and alerts in your infrastructure.



① **NOTE:** For the on-premises solution, the only view on the Dashboard is the Devices view. There are no other tab options at the top of the graph. The tab Devices, Summary, Network and Threat are only seen on the SaaS version of NSM, and these are described in the following sections.

At the top of the dashboard, you see a summary of your devices:

- **FIREWALLS:** Displays the number of firewalls that you intend to manage through NSM. Click **FIREWALLS** to list all the firewalls in the **Inventory** page.

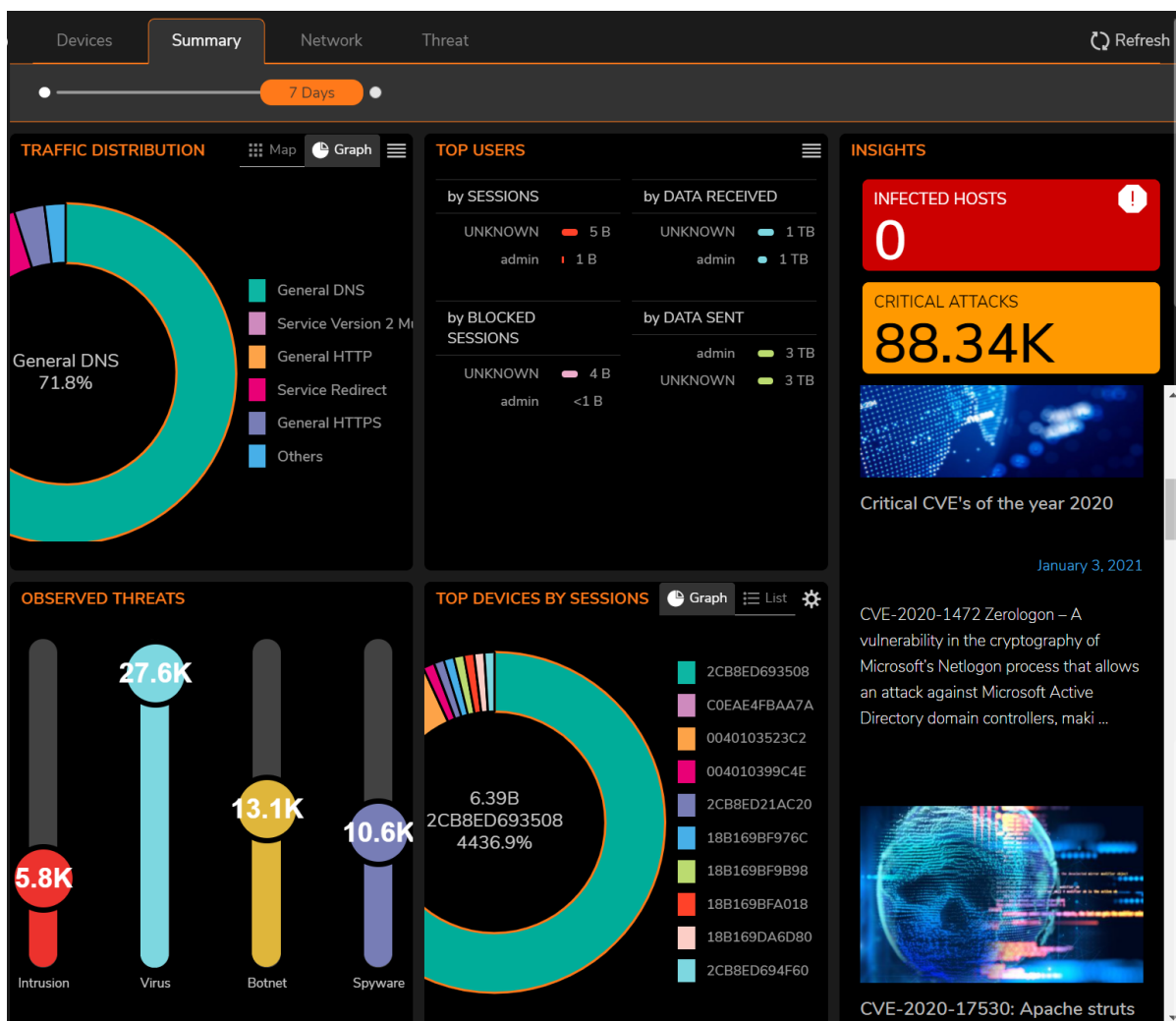
- **OFFLINE:** Displays the number of firewalls that are offline. Click **OFFLINE** to list the offline devices in the **Inventory** page.
- **EXPIRING LICENSES:** Displays the number of expiring firewall licenses.
- **GROUPS:** Displays the number of device groups. Click **GROUPS** to list the device groups.

The **FIREWALL OVERVIEW** section shows how many devices are **ONLINE & MANAGED**, **OFFLINE**, **ONLINE & UNMANAGED** and **UNASSIGNED**. A pie chart representation of firewall overview is also displayed. The geographical locations of the firewalls are shown on the map. For more details of the devices in a particular location, click the map location.

The **Alert Center** is shown at the bottom of the **Device** dashboard. An alert summary is provided and you can click on any of the categories—**All**, **Threats**, or **General** to open the **Notification Center** and see all the alerts for the selected category. The most recent alerts are displayed in a tabular format below the summary.

Summary

The **Summary** tab in the **Dashboard > System** page displays information on **TRAFFIC DISTRIBUTION**, **TOP USERS**, **OBSERVED THREATS**, and **TOP DEVICES BY SESSIONS** in your network infrastructure, for the period selected in the slider at the top.

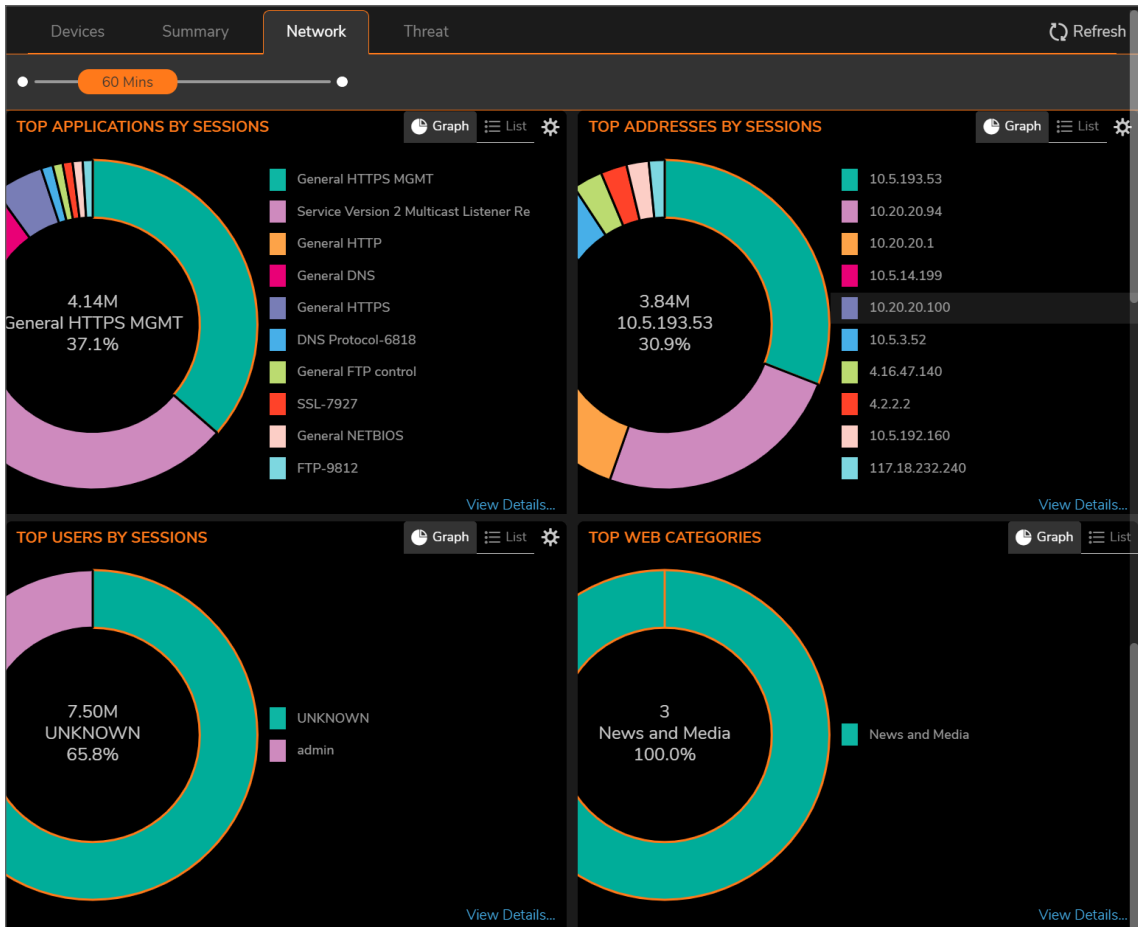


- **TRAFFIC DISTRIBUTION:** Shows the graphical representation of the percent distribution of the number of network sessions based on protocol.
- **TOP USERS:** Shows the top users by the number of sessions, amount of data received, amount of data sent, and the number of blocked connections.
- **OBSERVED THREATS:** Shows the different types of threats and the number of threats of each threat type across managed devices.
- **TOP DEVICES BY SESSIONS:** Shows the list of devices that are sorted in descending order of the category you select. Click the **Gear** icon to select your desired category; the default selection is **Sessions**.

The **Insights** section (scroll to the right if it's not visible) gives information about number of infected hosts and the number of critical attacks.

Network

The **Network** tab in the **Dashboard > System** page shows data pertaining to transactions in your network infrastructure.

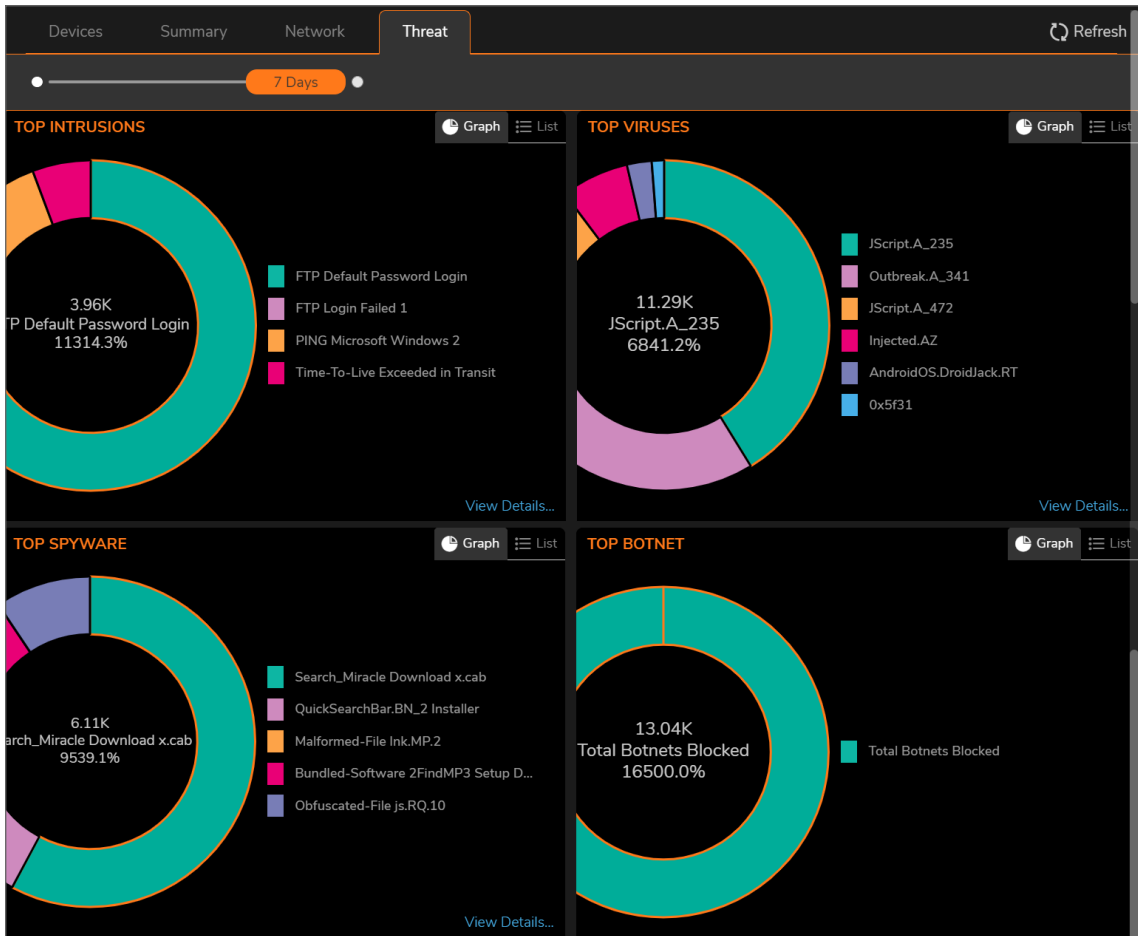


The following data is displayed on the Network page: types of applications that run in your infrastructure; IP addresses that initiate sessions; users that initiate sessions; web categories; and countries from which connections are initiated. Each space enables you to filter the data with available options. There is an option to switch to Graph and List view.

For more details on the data displayed in each space, click **View Details** link available at the bottom.

Threat

The **Threat** tab in the **Dashboard > System** page shows top threats by type, including the viruses, intrusions, spyware, and botnet. For more details on threats of a particular threat type, click **View Details**. There is an option to switch to Graph and List view.



For more information on monitoring the displayed threat data, see *Analytics and Reporting* document available at <https://www.sonicwall.com/support/technical-documentation/>.

① **NOTE:** The ability to drill down to specific details of an incident is dependent up on the licensing options you purchased. Having **Analytics** added ensures the broadest access to information.

Firewalls

Topics:

- [Device Inventory](#)
- [Device Groups](#)

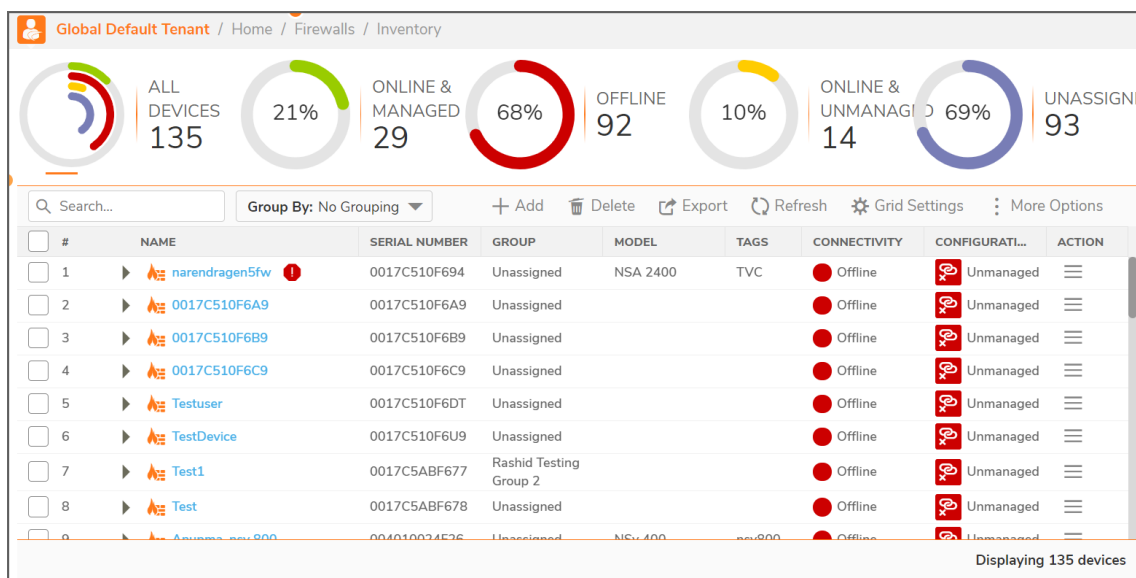
Device Inventory

The **Inventory** page (**Manager View | Firewalls > Inventory**) provides the inventory and activity status of all the firewalls and appliances managed by the Network Security Manager. Multi-tenant administrators can click on the tenant name and select any other tenant to see the devices associated with the selected tenancy.

To customize columns, click **Column Selection** and select or clear the options to include or hide the data of the columns. The menu bar above the table shows: **All Devices**— total number of devices; number of devices that are **ONLINE & MANAGED**, **OFFLINE**, **ONLINE & UNMANAGED** and **UNASSIGNED**. You can click these icons to list the devices—one category at a time—all the devices, online and managed by NSM, offline, online and unmanaged by NSM, and devices that are not assigned to any group.

The menu bar below the Firewall View lets you to search using the Keyword and Group By from the available options in the drop-down list.

- **Search** : Enter the Keyword and the list brings up the desired search results
- **Group By** : From the drop-down list, choose the options to No Grouping, Model, Connectivity, Managed Status, Group Name and they are displayed below.
- **Add** : The Add icon lets you to Add Device and Import Add Device File. Click Add Device and input Serial number, IP Address, User name and Password. To import device, click Add Device File and choose the files. Only xml, csv and json file types are supported.
- **Delete** : Select any device to delete and click this icon.
- **Export** : Click this icon to Export Device Inventory data to a .CSV file.
- **Refresh** : Refreshes the devices in the list.
- **Grid Settings** : This option lets you to Show or Hide Columns, Rearrange using Drag and Drop. You can also restore them to defaults or tick the boxes and click Apply.
- **More Options** : There are additional options which enables to Archive the selected configuration and download Add device JSON and CSV files to your local machine.



The following information is displayed for each firewall:

- **Appliance details:** Details of the firewall, such as: **FRIENDLY NAME**, **SERIAL NUMBER**, **TENANT NAME**—Tenant to which the appliance is registered to, **GROUP**— Device Group, if the firewall belongs to any, **MODEL**, **IP ADDRESS**, **TAGS**, **SonicOS VERSION** that runs on the firewall.
- **TEMPLATES APPLIED:** The templates applied to the firewall, if any.
- **ZERO TOUCH:** Activation status of zero-touch feature or status of zero-touch connection between firewall and NSM for zero-touch enabled device. For detailed information on zero-touch status of a firewall, see [Zero Touch Status](#)
- **CONNECTIVITY:** Status of connectivity between NSM and firewall.
 - **Green icon**— NSM can reach the firewall.
 - **Red icon**— NSM cannot reach the firewall.
- **CONFIGURATION**
 - **Blue icon**—Device acquisition was successful and firewall configuration is synchronized with NSM; firewall is in managed state.
 - **Red icon**—Device acquisition was either successful or unsuccessful; the firewall configuration is not synchronized with NSM as it was modified locally. Therefore, the firewall is in unmanaged state.
 - In this state, commits cannot be deployed on to the firewall.

Using the table as the central location, you can: switch to Firewall View to manage any system listed, for example: edit settings, upgrade software, and so on. For any firewall, click **Ellipses** icon in the ACTION column and select appropriate option to perform any of the listed actions on the firewall:

- **Access Firewall View:** Click **Switch to Firewall View** to access firewall management interface. For information on how to perform configuration changes to a firewall, see SonicOS documentation.
- **Edit Settings:** Click **Edit Settings** to edit settings of the firewall. For information on editing settings of a firewall, see [Editing Device Settings](#).
- **Synchronize Firewall:** A successfully-acquired firewall's management status changes to **unmanaged** state when the firewall is locally modified. Click **Synchronize Firewall** to synchronize

firewall configuration with NSM so that the management status is set to **Managed**. See [Synchronizing Firewall Configuration with NSM](#).

When firewall is in unmanaged stage, commits cannot be deployed on to the firewall.

- **Upgrade Firmware:** Click **Upgrade Firmware** to upgrade firmware on the firewall. For information on upgrading firmware, see [Upgrading SonicOSX Firmware](#).
- **Archive Config :** Archives the selected configuration.
- **Audit:** Click **Audit** to access Audit page. To perform audits, see [Auditing Configuration Changes](#).
- **Managing Commits:** Click **Manage Commits** to access Commits page. To manage commits, see [Monitoring Commits](#)
- **Scheduled Reports:** Click **Scheduled Reports** to set a schedule to generate PDF reports at regular intervals. For information on creating scheduled reports, see [Creating Scheduled Reports](#).
- **Export to Template :** Part of the device configuration to be exported to the Template.
- **Log-in to Unit :** This option is a fast and easy way to log into the managed firewall device-level.
- **Delete Firewall :** Deletes the selected Firewall.
- **Upload Keyset File :** Choose a License File by clicking Browse and click Upload.

Device Status

Click the caret icon next to a device name and then click the available options for more information on the device such as **Management Status**, **License Details**, **Analytics & Reporting Status**, and **Templates & Firmware Versions**.

The screenshot displays the Device Status dashboard. At the top, there are five circular progress indicators showing the status of devices: ALL DEVICES (8), ONLINE & MANAGED (3, 38%), OFFLINE (3, 38%), ONLINE & UNMANAGED (2, 25%), and UNASSIGNED (0, 0%). Below this is a search bar and navigation options like Export, Refresh, Column Selection, and More Options. A table lists three devices with columns for #, Friendly Name, Serial Number, Groups, Model, Tags, Connectivity, Configuration, and Action. The first device is TZ500W-NOAM-10 (Offline, Unmanaged), the second is TZ400W-India-01 (Offline, Unmanaged), and the third is TZ600-NOAM-01 (Online, Managed). Below the table are tabs for Management Status, License Details, ZT, Analytics & Reporting Status, and Templates & Firmware Versions. The Management Status section shows connectivity (Up), configuration (InSync), and zero touch status (Acquired). The System Details section shows model (TZ 600), serial number (18B169F4B5A4), friendly name (TZ600-NOAM-01), group name (NOAM), tenant (NSM20-DEMO-NEW), firmware version (SonicOS Enhanced 6.5.4.6-70n), and last modified by (admin.127.0.0.1.X1.GMS.UTC.07/05/2020 01:31:00).

#	FRIENDLY NAME	SERIAL NUMBER	GROUPS	MODEL	TAGS	CONNECTIVITY	CONFIGURATION	ACTION
1	TZ500W-NOAM-10	18B16979D860	NOAM	TZ 500 wireless-AC		Offline	Unmanaged	...
2	TZ400W-India-01	18B169E610A0	India	TZ 400 wireless-AC		Offline	Unmanaged	...
3	TZ600-NOAM-01	18B169F4B5A4	NOAM	TZ 600		Online	Managed	...

Topics:

- [Management Status](#)
- [System Details](#)
- [Templates Applied](#)
- [License Details](#)
- [Available SonicOS Versions](#)
- [Zero Touch Status](#)
- [Multi-device Firmware Upgrade](#)

Management Status

NSM manages a firewall, when: firewall acquisition is successful, firewall configuration is synchronized with NSM, and NSM can reach the firewall. For information on performing firewall acquisition, see *NSM Getting Started Guide* available at <https://www.sonicwall.com/support/technical-documentation/>.

MANAGEMENT STATUS gives information of the status of the device and device-management through NSM.

MANAGEMENT STATUS

Connectivity	Status of connectivity between NSM and firewall. <ul style="list-style-type: none">• Up(green icon)— NSM can reach firewall.• Down(red icon)— NSM cannot reach firewall.
Configuration	Status of synchronization of firewall configuration with NSM. <ul style="list-style-type: none">• Green icon—Synchronization successful• Red icon—Synchronization failed
Acquired	Status of firewall acquisition by NSM. <ul style="list-style-type: none">• Green icon—Acquisition successful• Red icon—Acquisition failed• Yellow icon—Acquisition is in progress
Zero Touch	Activation status of the zero-touch feature or status of zero-touch connection between firewall and NSM for zero-touch enabled device. <ul style="list-style-type: none">• A gray icon indicates Zero Touch feature was disabled.• A red icon indicates that the Zero Touch connection failed.• A yellow icon indicates that the system is waiting for a Zero Touch connection from the firewall.• A green icon indicates that the firewall is connected successfully to NSM using zero-touch.

System Details

The **SYSTEM DETAILS** section displays the following details of a system:

SYSTEM DETAILS

Term	Definition
Model	Device model.
Serial Number	Serial number of the device
Friendly Name	Friendly name of the device, if entered when registering the firewall.
IP Address	IP Address of the device.
Username	Username
Group Name	Device group, if the device belongs to any group.

Term	Definition
Tenant	The tenant to which the firewall is registered to.
Verify SSL Certificate	Status of SSL certificate verification.
Firmware Version	The SonicOS version that runs on the device
Last Modified By	User that modified device configuration the last time.
Product Code	Product code of the firewall.
Memory	RAM capacity of the system.
ROM Version	ROM version running on the device.
Safemode Version	Safemode Version
Up Time	Duration for which the device is online.
Current Time	Current time.
Auth Code	Authorization code of the firewall.
Registration Code	Registration code of the firewall.
Prefs Changed	Status of preferences changed.

License Details

The **LICENSE DETAILS** section shows the activation status of all the licenses associated with your device and also notifies if the licenses are nearing expiration.

The list of licenses is given here:

- Nodes/Users
- Global VPN Client
- VPN SA
- SSL VPN
- WAN Acceleration Client
- Botnet Filter
- App Visualization
- App Control
- Gateway AV/Anti-Spyware/Intrusion Prevention/App Control/App Visualization
- Content Filtering Client
- Capture Client (Advanced)
- Deep Packet Inspection for SSL (DPI-SSL)
- Premium Content Filter
- SonicOSX Expanded
- DPI-SSL Enforcement
- Virtual Assist
- E-Mail Filtering Service

- WAN Acceleration Software
- Comprehensive/Advanced Gateway Security Suite
- Deep Packet Inspection for SSH (DPI-SSH)
- Comprehensive Anti-Spam Service
- SYSLOG Analytics
- Capture Advanced Threat Protection
- Capture Client McAfee Malware Engine
- Global VPN Client Enterprise
- External IDS Support
- Analyzer
- Stateful High Availability

Available SonicOS Versions

The **AVAILABLE VERSIONS** section under **Templates & Firmware Versions** shows all the SonicOS versions available for firewall upgrade. NSM downloads these versions from MySonicWall. To upgrade SonicOS software on your device, see [Upgrading SonicOSX Firmware](#).

Zero Touch Status

The **ZERO TOUCH STATUS** section under **ZT, Analytics & Reporting Status** provides information on zero-touch connection between firewall and NSM. The **ZERO TOUCH STATUS** section is displayed only for firewalls that have zero-touch feature enabled.

ZERO TOUCH STATUS

Term	Description
Enabled	Displays the status of the Zero-Touch connection between firewall and NSM. <ul style="list-style-type: none"> • A red icon indicates Zero Touch connection has failed. • A yellow icon indicates that the system is waiting for a Zero Touch connection from the firewall. • A green icon indicates that the firewall is connected successfully to NSM using zero-touch.
Connection State	Status of zero-touch connection between firewall and NSM.
Zero Touch Proxy Address	The IP address of proxy server for Zero Touch deployment.
Last HeartBeat Time	Time at which heartbeat of the firewall was heard the last time.
Last Request Time Sent	Time at which the request was sent to firewall the last time.
Connection Initiation Time	Time at which zero touch connection is initiated.
HeartBeat Ack Received Time	Time at which the heartbeat acknowledgment is received by the firewall.

Managing Devices

Several functions are provided so you can easily manage your nsm infrastructure.

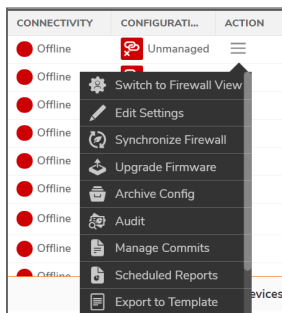
Topics:

- [Editing Device Settings](#)
- [Synchronizing Firewall Configuration with NSM](#)
- [Upgrading SonicOSX Firmware](#)
- [Creating Backup of Device Configuration](#)
- [Manual Firewall Acquisition](#)

Editing Device Settings

To edit settings of a device:

1. Navigate to **Manager View | Firewalls > Inventory** page.
2. Hover over the device for which want to edit the settings, click **Ellipses** icon in the **ACTION** column and select **Edit Settings**.



3. In the **Edit Settings** dialog:
 - For a device that is managed successfully by NSM, you can edit only the `Friendly Name` and `Tags`.
 - For a device that isn't acquired yet, you can edit `Friendly Name`, `Tags` and perform manual acquisition. To manually acquire a firewall, see [Manual Firewall Acquisition](#) .

- For a device that has failed acquisition, you can edit `Friendly Name`, `Tags`.

Edit Settings

Serial Number *

Friendly Name

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

Verify SSL Certificate ⓘ

Username

Password *

Tags (Example:TZ, BranchA) ⓘ

DEVICE ACQUISITION STATUS

❌ Connection failed to device

❌ Failed to synchronize configuration

✅ Acquired

ⓘ Your device might reboot to enable Reporting & Analytics

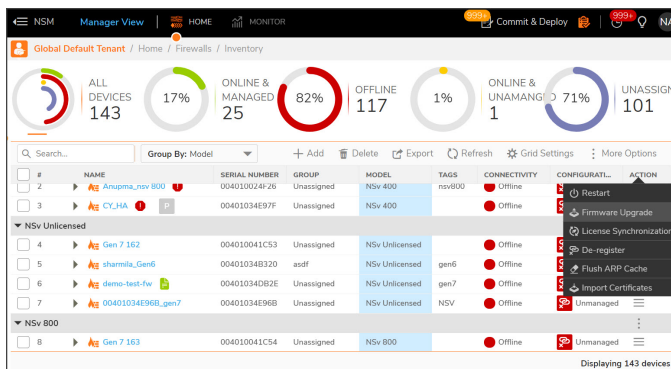
4. Click **Save**.

Multi-device Firmware Upgrade

You can now upgrade multiple firewalls from a group of devices in a single action.

To perform group upgrade of devices:

1. Navigate to **Manager View | Firewalls > Inventory** page.
2. Hover over the device for which want to edit the settings, click **Ellipses** icon in the **ACTION** column and select **Firmware Upgrade**.



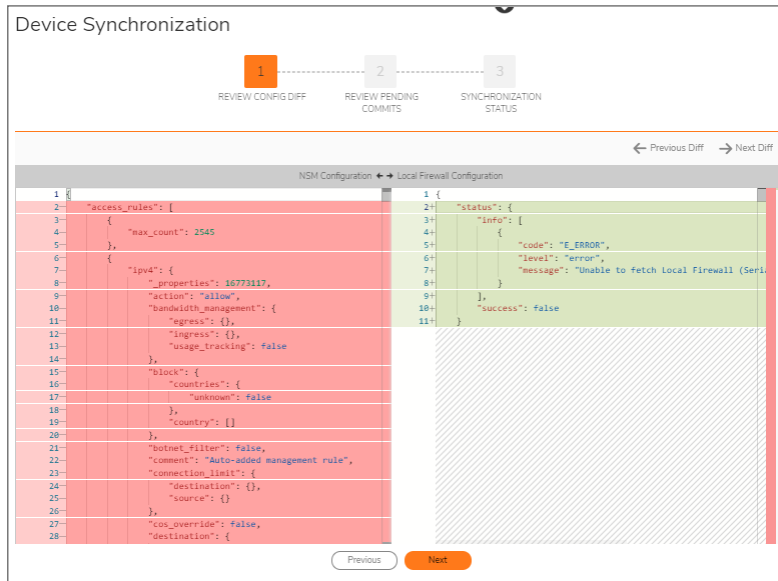
3. There are 3 steps to perform upgrade. Select the devices in the group by checking the box.
4. Browse and select the Firmware and click **Next** to proceed to the next screen .
 - a. Schedule Now - Choose this to upgrade instantly.
 - b. Set Schedule - Set a future date to upgrade.
5. Click **Upgrade**.

Synchronizing Firewall Configuration with NSM

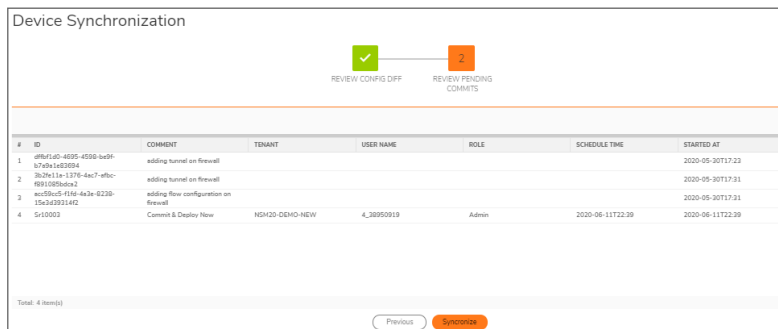
The management status of a firewall changes to **Unmanaged** state when the firewall is locally modified. You need to synchronize firewall configuration with NSM to set the device in **Managed** state.

To synchronize firewall configuration with NSM:

1. Navigate to **Manager View | Firewalls > Inventory**.
2. Click the **Ellipses** icon in the **Action** column for the firewall you want to synchronize the changes with NSM, and select **Synchronize Firewall**.
3. In the **Synchronize Firewall** dialog, click **Review Diff**.
4. In the **Device Synchronization** wizard:
 - a. Review the configuration differences between NSM configuration and the local firewall configuration.



- b. Click **Next**.
- c. Review the pending commits.



- d. Click **Synchronize**.
- e. Click **OK** in the Warning dialog. Synchronization process runs.
- f. Click **Close**.

The firewall is now managed by NSM, thus the **CONFIGURATION** status changes to **Managed** in the **Firewall Inventory** page.

Upgrading SonicOSX 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.

#	VERSION	FILENAME	RELEASE DATE	RELEASE TYPE
1	6.5.4.6-79n	sw_tz-400w_eng_6.5.4.6-79n.sig	May 29, 2020	Maintenance Release

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 the **AVAILABLE SOFTWARE VERSION(S)** section.
 2. Select **Now** in the **SCHEDULED UPGRADE** section, if not selected.
 3. Click **Upgrade**.
 - **To schedule software upgrade:**
 1. Select the required software version In the **AVAILABLE SOFTWARE VERSION(S)** section.
 2. Select **Later** in **SCHEDULED UPGRADE** section and set the schedule for upgrade in **Upgrade Time** box.
 3. Click **Upgrade**

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.

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. Navigate to **Manager View | Firewalls > Inventory**.
2. Hover over the firewall, click the **Ellipsis** icon in the **Action** column and select **Edit Settings**.

#	FRIENDLY NAME	SERIAL NUMBER	TENANT NAME	GROUPS	MODEL	IP ADDRESS	TAGS	VERSION	TEMPLATES APP.	ZERO TOUCH	CONNECTIVITY	CONFIGURATION	MANAGED	ACTION
1	TZ500W-NDAM-10	18B16979D860	NSM20-DEMO-NEW	NOAM	TZ 500 wireless-AC	103.19.168.166-903		SonicOS Enhanced 6.5.4.6-79h	BO Template	Online	Online	Managed	Managed	
2	TZ600W-NDAM-01	18B169610A0	NSM20-DEMO-NEW	Indie	TZ 600 wireless-AC	Zero Touch		SonicOS Enhanced 6.5.4.6-79h	Test Test Senjay All DNS NTP settings: TEST SSL	Offline	Offline	Switch to Firewall View	Managed	Switch to Firewall View
3	TZ600-NDAM-03	18B169F485A4	NSM20-DEMO-NEW	NOAM	TZ 600	Zero Touch		SonicOS Enhanced 6.5.4.6-79h	NA	Online	Online	Managed	Managed	Edit Settings
4	TZ350-Switch-NDAM-10	ZCB8E0238B00	NSM20-DEMO-NEW	NOAM	TZ 350 wireless-AC	103.19.168.166-901		SonicOS Enhanced 6.5.4.6-79h	NA	Online	Online	Managed	Managed	Sync to Ariza Firewall
5	TZ350-NDAM-SonicNve-10	ZCB8E0238B40	NSM20-DEMO-NEW	Indie	TZ 350 wireless-AC	Zero Touch		SonicOS Enhanced 6.5.4.6-66h-49323110-12h	NA	Online	Online	Managed	Managed	Upgrade Software
6	NS44850-NDAM-02	ZCB8E02C8D80	NSM20-DEMO-NEW	NOAM	NS4 4850	103.19.168.166-902		SonicOS Enhanced 6.5.4.6-79h	All DNS NTP settings	Online	Online	Managed	Managed	Archive Config
7	SONIC250W-Touin-Home-03	ZCB8E03AF4A0	NSM20-DEMO-NEW	Indie	SONIC250 wireless-N	Zero Touch		SonicOS Enhanced 6.5.4.6-79h	DNS Template	Online	Online	Managed	Managed	Audit
8	TZ370-NDAM-01	ZCB8E089440C	NSM20-DEMO-NEW	Test	TZ 370	Zero Touch		SonicOS 7.0.0-P369	Test Senjay TestSenjay Test	Online	Online	Managed	Managed	Manage Commits

3. Enter **IP Address with Port** for your device.
4. Enter your **Username** and **Password** of your NSM user account.

Edit Settings

Serial Number * 2CB8ED2C9480

Friendly Name 2CB8ED2C9480

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

Verify SSL Certificate ⓘ

Username

Password *

Tags (Example:TZ, BranchA) ⓘ

Your device might reboot to enable Reporting & Analytics

DEVICE ACQUISITION STATUS

- Not acquired
- Connection failed to device
- Failed to synchronize configuration

Cancel Save Acquire Again

5. Click **Save** and **Acquire Again**.

As part of the device acquisition process, NSM establishes connection to the device, configures the firewall to send out syslog heartbeats so its health can be monitored, and then the pulls the status and configuration of the firewall.

The status of the device acquisition is displayed in **DEVICE ACQUISITION STATUS** section; If the acquisition is successful, you will see a green icon next to **Acquired**. The firewall is now managed by NSM, and the **CONFIGURATION** is displayed as **Managed** in the **Firewall Inventory** page.

Edit Settings

Serial Number * 2CB8ED2CBD80

Friendly Name NSa4650-NOAM-01

IP Address with Port (Example: 34.25.61.2:443) * 103.19.168.166:9024

Verify SSL Certificate ⓘ

Username nsmuserbeta@sonicwall.co

Password *

Tags (Example:TZ, BranchA) ⓘ

Your device might reboot to enable Reporting & Analytics

DEVICE ACQUISITION STATUS

- Acquired
- Connected to device.
- Configuration synchronized.

Cancel Save Acquire Again

Device Groups

NSM enables you to create device group(s), deploy and manage common configurations across all the devices of a device group using templates. You can create device groups based on your requirement, for

example: geographical location, business function and so on. To create a device group, see [Creating Device Groups](#)

The **Manager View | Firewalls > Groups** page displays the device groups that are created under the **Root Group**. To review the configuration of a device group in the **Group View**, click on the group name. The devices that are not part of any device groups are listed under **Unassigned Firewalls**.

Multi-tenant administrators can click on the Tenant name and select any other tenant to display and manage the groups created under that tenant. You can also select **All Tenants** option to display and manage device groups of all the tenants in a single pane of glass.

In the table you can see the all the device groups listed. Click the caret icon next to the group name to see devices that are part of the device group.

DEVICE GROUPS

Term	Description
Group	Name of the device group.
Tenant Name	Tenant under which the device group is created.
SERIAL NUMBER	Serial numbers of devices that are part of a device group.
TAGS	Tags, if entered when creating the device group.
ZERO TOUCH	Activation status of the zero-touch feature or status of zero-touch connection between firewall and NSM for zero-touch enabled device.
Link	Status of a firewall that is part of the group. <ul style="list-style-type: none">• Up—Firewall is healthy.• Down— Status check of the firewall failed because firewall could be down or the connection between firewall and NSM failed.
State	Status of device acquisition and management by NSM. <ul style="list-style-type: none">• Green icon—Device acquisition was successful; firewall is being managed through NSM.• Red icon—Device acquisition failed; firewall can't be managed through NSM.
Action	Actions that can be performed on a device group

Working with Device Groups

From the **Manager View**, you can create, update, and delete a device group. You can add a firewall to any device group, and you can add a device group under any existing device groups to create a hierarchical structure.

If you want to view configuration of a particular group, navigate to **Manager View | Firewalls > Groups** and click on the group. You are taken to the Group View. The default location is **Group View | HOME > Dashboard > System**. Here you can monitor various dashboard views that include **Summary**, **Network**, and **Threat**. Click the gear arrow beside **Group View** to return to the **Manager View**.

Topics:

- [Creating Device Groups](#)
- [Editing Device Groups](#)
- [Creating Backup of Device-Group Configuration](#)
- [Deleting Device Groups](#)

Creating Device Groups

A device group enables you to easily deploy common configurations across all the devices of the group using templates. You can create device groups based on your requirement, for example: geographical location, business function and so on.

To create a device group:

1. Navigate to **Manager View | Firewalls > Inventory** page.
2. Click **Add**.

The screenshot shows the 'Add Device Group' interface. It includes a 'GROUP SETTINGS' section with the following fields: Tenant (NSM20_DEMO), Parent Group (Root Group), and Friendly Name (Test). There is a 'Tags' field with the example 'TZ, BranchA'. Below these are two lists: 'Unassigned Devices' (1 item) and 'In Group' (2 items). The 'In Group' list shows 'NSV200-NOAM-01' and 'NSa4650-NOAM-100'. A 'Selected: 2 of 3 items' indicator is at the bottom, along with 'Cancel' and 'Save' buttons.

3. Enter the **Friendly Name** and **Tags** in their respective fields.
4. Select devices listed in **Unassigned Devices** to add to the group being created and click caret-right icon.
The devices are moved to In Group list.
5. Click **Save**.

The newly created group is listed under the default group—Root Group, which cannot be deleted.

To create a device group under another device group:

1. Hover over the group under which you want to create a new device group.
2. Click the **Ellipses** icon in the Action column and select **Add a Group under this Group**.
3. Follow steps 3 through 5 in the above procedure for creating a device group.

The newly created group is added under the selected parent group. Click the caret icon next to the parent group to view the newly added group.

Editing Device Groups

You can edit a device group to: add Unassigned Firewall(s) to the group; remove firewalls from the group; update friendly name and tags.

To edit a device group:

① | **NOTE:** The **Root Group** cannot be edited.

1. Navigate to **Manager View | Firewalls > Groups**.
2. In the **Action** field for the group you want to edit, select **Edit Device Group**.
3. Make changes to the **Friendly Name** and **Tags** fields, if needed.

Add Device Group

GROUP SETTINGS

Tenant: Global Default Tenant

Parent Group: Root Group

Friendly Name: Enter Friendly Name...

Tags (Example: TZ, BranchA):

Unassigned Devices: 91 items

In Group: 0 items

Devices:

- vk_01 (18B169BF9B98)
- test 64 build (004010351EC3)
- sharath_nsv (004010351ED4)
- satish-no-mod (18B169DA6D00)
- rhishi-3g-4g (18B169114E7C)
- raviGuru (C0EAE4EB5076)
- karan_NSA_noconfig (2CB8ED040D00)
- jeff22 (004010357A0F)
- hFw_gen7 (004010351FA2)
- gfdgfd (356665454523)
- gen7-ap (2CB8ED4AC978)

Selected: 0 of 91 items

Cancel Save

4. To add devices to the group, select devices in the **Unassigned Devices** list and click the caret-right icon to move them to the **In Group**. To remove devices from the group, select the devices in **In Group** list and click the left-caret icon to move the devices to the **Unassigned Devices** list.

① | **NOTE:** To move devices from one device group to another, first you need to delete the devices from one group and then add them to the other group from Unassigned Firewalls list.

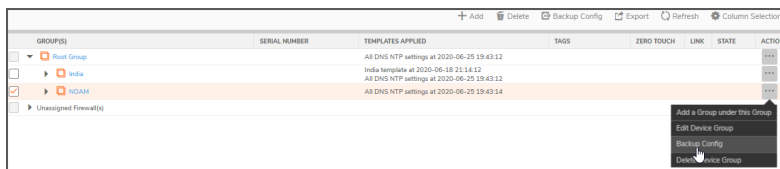
① | **NOTE:** When you add a device to a group that already has a template applied to it, the template configuration is made available to the newly added device and therefore you need to commit and deploy the available updates on to the device.

5. Click **Save**.

Creating Backup of Device-Group Configuration

To create a backup of device-group configuration:

1. Navigate to **Manager View | Firewalls > Groups**.
2. Hover over the device group for which you want to create a backup and click the **Ellipses** icon in the **ACTION** column.
3. Select **Backup Config**.



4. Click **OK** to confirm.

Deleting Device Groups

- ① **NOTE:** When you delete a device group, all the sub-groups also get deleted. All devices under the device group and its sub-groups will be automatically assigned to the parent group—**Root Group**.
- ① **NOTE:** When you delete a sub-group, all devices under the group is automatically assigned to its parent group.

To delete device group(s):

1. Navigate to **Manager View | Firewalls > Groups**.
2. Select the group(s) you want delete.
3. Click the **Delete** icon.
4. Click **Confirm**.

Backups

To create a backup of the device configuration:

1. Navigate to **Manager View | Firewall View > Backups**
2. Click **Add** icon to Add Schedule. There are 3 steps to add schedule.
Schedule Configuration - Enter Schedule Name, choose Daily Interval, Schedule Time, Edit Weekly Schedule Day. If you choose to Edit Weekly Schedule Day, toggle the switch and choose a day from the drop-down list. You are required to select at least one Backup Type and check the box as TSR or EXP and click **Next** to proceed to Device Selection screen.

Device Selection - In the Device Selection screen, choose the devices that are online and offline connectivity from the list. Toggle the switch to Show only online devices which filters the devices that are online. Click **Next** after choosing the devices to review.

#	DEVICE	SERIAL NUMBER	CONNECTIVITY
<input checked="" type="checkbox"/>	1 Test Firewall 1	004010351F2A	Online
<input type="checkbox"/>	2 00401034E96B_gen7	00401034E96B	Online
<input checked="" type="checkbox"/>	3 CY_251	004010283E72	Online
<input type="checkbox"/>	4 narendragen5fw	0017C510F694	Offline
<input type="checkbox"/>	5 0017C510F6A9	0017C510F6A9	Offline
<input checked="" type="checkbox"/>	6 0017C510F6B9	0017C510F6B9	Offline
<input type="checkbox"/>	7 0017C510F6C9	0017C510F6C9	Offline
<input type="checkbox"/>	8 Testuser	0017C510F6DT	Offline
<input type="checkbox"/>	9 TestFirewall	0017C510F6E9	Offline

Review - In the last step, the Schedule configuration and Device Selection is displayed for review. If you want to change any information listed there, click **Previous** or click **Save** to schedule task.

Schedule Name	Device 3 Backup	#	DEVICE	SERIAL NUMBER
Schedule Interval	Weekly	1	Test Firewall 1	004010351F2
Schedule Time	05:30 AM - 06:30 AM	2	0017C510F6B9	0017C510F6E
Schedule Day	Sunday	3	CY_251	004010283E7
Backup Type	EXP			

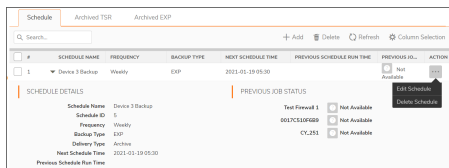
3. Click **Delete** icon to delete any selected schedule from the list.
4. **Refresh** icon refreshes the list

5. Column Selection allows to choose which options can be displayed in the schedule by checking the box.

Scheduling Backups

This section lists all the created backup schedules. To know, how to add schedule, see [Backups](#).

1. Navigate to **Manager View | Firewalls > Backups** page.
2. Expand the scheduled backup from the list. It displays Schedule details and Previous Job Status. Hover over the item for which want to edit the schedule, click **Ellipses** icon in the **ACTION** column and select **Edit Schedule**.



3. **Delete Schedule** deletes the selected item.

Archiving TSR

The archived TSR backup types are displayed in this tab with File Name, Date and Time, Device Name, Serial Number and User Name. To know, how to add schedule, see [Backups](#).

Hover over the item for which want to view, click **Ellipses** icon in the **ACTION** column and select **Download TSR** and **Delete TSR**.

The icons on the top also lets to download and delete the TSR files. Click **Refresh** to refresh the list. **Column Selection** allows to choose which options can be displayed in the schedule by checking the box.

#	FILE NAME	DATE & TIME	DEVICE NAME	SERIAL NUMBER	USER	ACTION
1	test_004010340AP9 Jan_17_20	2021-01-18 01:09	vs_per6	004010340AP9	NSM Administrator	<input type="checkbox"/> Download <input type="checkbox"/> Delete <input type="checkbox"/> Refresh <input type="checkbox"/> Column Selection
2	test_004010340AP9 Jan_17_20	2021-01-18 01:02	vs_per6	004010340AP9	NSM Administrator	<input type="checkbox"/> Download <input type="checkbox"/> Delete <input type="checkbox"/> Refresh <input type="checkbox"/> Column Selection
3	test_004010340AP9 Jan_17_20	2021-01-18 01:56	vs_per6	004010340AP9	NSM Administrator	<input type="checkbox"/> Download <input type="checkbox"/> Delete <input type="checkbox"/> Refresh <input type="checkbox"/> Column Selection
4	test_004010340AP9 Jan_17_20	2021-01-18 01:14	vs_per6	004010340AP9	NSM Administrator	<input type="checkbox"/> Download <input type="checkbox"/> Delete <input type="checkbox"/> Refresh <input type="checkbox"/> Column Selection
5	test_004010340AP9 Jan_17_20	2021-01-17 21:56	vs_per6	004010340AP9	NSM Administrator	<input type="checkbox"/> Download <input type="checkbox"/> Delete <input type="checkbox"/> Refresh <input type="checkbox"/> Column Selection
6	test_004010340AP9 Jan_17_20	2021-01-17 21:12	vs_per6	004010340AP9	NSM Administrator	<input type="checkbox"/> Download <input type="checkbox"/> Delete <input type="checkbox"/> Refresh <input type="checkbox"/> Column Selection
7	test_004010340AP9 Jan_17_20	2021-01-17 21:08	vs_per6	004010340AP9	NSM Administrator	<input type="checkbox"/> Download <input type="checkbox"/> Delete <input type="checkbox"/> Refresh <input type="checkbox"/> Column Selection
8	test_004010340AP9 Jan_17_20	2021-01-17 21:08	vs_per6	004010340AP9	NSM Administrator	<input type="checkbox"/> Download <input type="checkbox"/> Delete <input type="checkbox"/> Refresh <input type="checkbox"/> Column Selection
9	test_004010340AP9 Jan_17_20	2021-01-17 19:40	vs_per6	004010340AP9	NSM Administrator	<input type="checkbox"/> Download <input type="checkbox"/> Delete <input type="checkbox"/> Refresh <input type="checkbox"/> Column Selection
10	test_004010340AP9 Jan_17_20	2021-01-17 15:37	vs_per6	004010340AP9	NSM Administrator	<input type="checkbox"/> Download <input type="checkbox"/> Delete <input type="checkbox"/> Refresh <input type="checkbox"/> Column Selection
11	test_004010340AP9 Jan_17_20	2021-01-17 15:37	vs_per6	004010340AP9	NSM Administrator	<input type="checkbox"/> Download <input type="checkbox"/> Delete <input type="checkbox"/> Refresh <input type="checkbox"/> Column Selection

Download TSR option downloads the selected TSR to a zip file in *.txt* format.

Archiving EXP

The archived EXP backup types are displayed in this tab with File Name, Date and Time, Device Name, Serial Number and User Name. To know, how to add schedule, see [Backups](#).

Hover over the item for which want to view the , click **Ellipses** icon in the **ACTION** column and select **Download EXP** and **Delete EXP** .

The icons on the top also lets to download and delete the EXP files. Click **Refresh** to refresh the list. **Column Selection** allows to choose which options can be displayed in the schedule by checking the box.

ID	FILE NAME	DATE & TIME	DEVICE NAME	SERIAL NUMBER	USER	ACTION
1	test_004010340AP9_inh_37_2	2021-01-18 03:09	svr_gen6	004010340AP9	NSM Administrator	⋮
2	test_004010340AP9_inh_37_2	2021-01-18 03:42	svr_gen6	004010340AP9	NSM Administrator	⋮
3	test_004010340AP9_inh_37_2	2021-01-18 03:58	svr_gen6	004010340AP9	NSM Administrator	⋮
4	test_004010340AP9_inh_37_2	2021-01-18 03:14	svr_gen6	004010340AP9	NSM Administrator	⋮
5	test_004010340AP9_inh_37_2	2021-01-17 21:56	svr_gen6	004010340AP9	NSM Administrator	⋮
6	test_004010340AP9_inh_37_2	2021-01-17 21:12	svr_gen6	004010340AP9	NSM Administrator	⋮
7	test_004010340AP9_inh_37_2	2021-01-17 21:08	svr_gen6	004010340AP9	NSM Administrator	⋮
8	test_004010340AP9_inh_37_2	2021-01-17 21:08	svr_gen6	004010340AP9	NSM Administrator	⋮
9	test_004010340AP9_inh_37_2	2021-01-17 19:40	svr_gen6	004010340AP9	NSM Administrator	⋮
10	test_004010340AP9_inh_37_2	2021-01-17 15:37	svr_gen6	004010340AP9	NSM Administrator	⋮
11	test_004010340AP9_inh_37_2	2021-01-17 15:27	svr_gen6	004010340AP9	NSM Administrator	⋮

Download EXP option downloads the selected EXP to a zip file in *.txt* format.

Templates

Templates allow you to effectively deploy and manage common configurations across firewalls. Template can be developed to set definitions for **Device**, **Network**, **Objects** and **Policies** settings on numerous firewalls. It brings scalability to the overall firewall management process. These templates can be reused or reworked for other configurations.

Topics:

- [Templates Inventory](#)
- [Creating Templates](#)
- [Editing Templates](#)
- [Viewing Template Configuration](#)
- [Creating Duplicate Template](#)
- [Modifying Template Attributes](#)
- [Applying Templates](#)
- [Deleting Templates](#)
- [Golden Template](#)

Templates Inventory

Navigate to **Manager View > Templates** to see the inventory of all your templates in a tabular format. Multi-tenant administrators can click on the tenant name (highlighted in the below image) and select any other tenant to list the templates associated with the selected tenancy.

You can use the **Search** feature to find a specific template to use. To customize columns, click **Column Selection**, and select or clear the options to include or hide the data of the selected columns.

#	NAME	DESCRIPTION	ZERO TOUCH	USER	ROLE	ACTIVE TENANTS	APPLIED TO	ACTION
1	Syslogs	Syslogs		Rinkoo R	Admin	ExtBeta 2.0-37	1 Syslogs 0 Devices	

TEMPLATE DETAILS		APPLIED TO
Name	Syslogs	Root Group
Description	Syslogs	
Active Tenants	ExtBeta 2.0-37	
User	Rinkoo R	
Role	Admin	
Deploy Time	2020-05-13T03:11 AM	

The following details are displayed for each template listed on the Templates page:

TEMPLATE DETAILS

NAME	Name of the tenant
DESCRIPTION	Gives more information on the template, if included when creating the template.
ZERO TOUCH	Displays the deployment status of template-configuration on to zero-touch devices. <ul style="list-style-type: none"> • Enabled: The template configuration is auto-deployed on to the target zero-touch devices when applied. • Disabled: The template configuration needs to be committed and deployed on to the target devices when applied.
USER ROLE	Management role of the user that created the template.
ACTIVE TENANTS	Tenant to which the template is associated with.
APPLIED TO	Active target devices and groups for the template

To switch to the **TEMPLATE VIEW**, click on a template name or click on **Edit Template** in the Action menu.

The screenshot shows the 'Editing Template Configuration' page for 'template_test'. The page has a top navigation bar with 'NSM', 'Template View', and a 'Click to switch to Manager View' button. Below the navigation bar are buttons for 'View Template Details', 'Apply Template', and 'Done'. The main content area is divided into sections: 'FIREWALL NAME' with a 'Firewall's Domain Name' input field and an 'Auto-Append HA/Clustering suffix to Firewall Name' toggle; 'FEATURE VISIBILITY' with an 'Enable IPv6' toggle; and 'ADMINISTRATOR NAME & PASSWORD' with an 'Administrator Login Name' input field (set to 'admin'), a 'Change Password' button, a 'One-time Passwords Method' dropdown (set to 'Disabled'), and an 'Unbind TOTP Key' button.

You can also access other functionality clicking the options in the **Action** field. The actions you can perform on the Templates page are listed here:

- [Creating Templates](#)
- [Editing Templates](#)
- [Viewing Template Configuration](#)
- [Modifying Template Attributes](#)
- [Creating Duplicate Template](#)
- [Deleting Templates](#)
- [Applying Templates](#)

Creating Templates

You can build templates that you can use repeatedly to apply configurations to the firewalls in your environment.

To create a template:

1. Navigate to **Template View > Templates**.
2. Click **Add Template**.
3. Enter the **Template Name**.
4. From the type, choose SonicOS or SonicOSX. The templates can be applied to specific devices that are running the OS.
5. To enable automated deployment of the template configuration to Zero-Touch devices when the template is applied to target group(s) or device(s), enable or disable **Zero Touch** option. Offline devices will be updated once they come online.
6. Enter a valid **Description**. This is optional.
7. Click **Create**.
8. **Confirm** that you want to switch to **Template View** if you want to define your template now; otherwise click **Cancel** to see that your template is added to the inventory.

To define your template, see [Editing Templates](#).

Editing Templates

If a template—applied to device group(s) or device(s)—is edited, the configuration changes are not automatically committed to the devices. You need to commit and deploy the changes so that the changes are pushed to the devices. To perform commit and deploy, see [Committing and Deploying the Updates](#)

① **NOTE:** The updates made to a zero touch template are automatically deployed to the applied zero-touch devices.

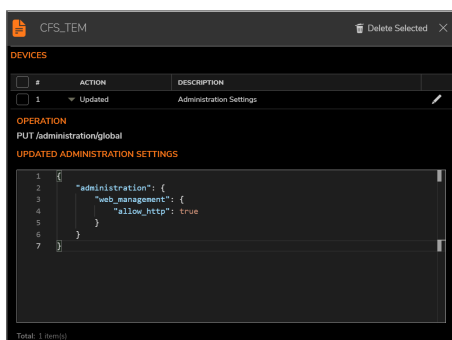
To define or edit a template:

1. If not already in Template View, either click the template name or select **Edit Template** in the **Action** field.
2. Navigate to other options in **Template View: Device, Network, Object, or Policy**.
3. Using the interface commands under each of these options, define the various parameters of your template. For information on performing configuration in these fields, see SonicOS documentation at <https://www.sonicwall.com/support/technical-documentation/>.
4. After you update the template, click **View Templates Details** to see the updates done to the default. All the updates done to the template configuration are captured here.
5. Click **Close** to return to **Template** inventory.

Viewing Template Configuration

To view template configuration:

1. Navigate to **Manager View > Templates**.
2. Click **Ellipses** icon in Action column for any template and select **View Template Configuration**. The configuration changes are listed in the dialog displayed.



3. Click the **Edit** icon next to the operation to edit the template configuration as required.
4. To delete the selected template, check the devices and click **Delete Selected**.

Creating Duplicate Template

You can create a duplicate of any template and then edit the configuration to use it on other devices.

To create a duplicate template:

1. Navigate to **Manager View > Templates**.
2. Click **Ellipses** icon in the **Action** column for any template and select **Clone Template**.
3. Click **OK** in the dialog displayed.

The duplicate template is now available on the **Templates** page with name **clone<template name>**. To tweak the attributes of the newly created template, see [Modifying Template Attributes](#). To make changes to the configuration of the newly created template, see [Editing Templates](#).

Modifying Template Attributes

To modify template-attributes:

1. Navigate to **Manager View > Templates**.
2. Hover over a template and click **Ellipses** icon in the **ACTION** column, and then select **Modify Template Attributes**.
3. In the **Edit Template** dialog, edit the template attributes as needed. The name of the template and description can be added as a reference.

4. Click **Update**.
5. Click **Confirm** to switch to the Template View; click **Cancel** otherwise.

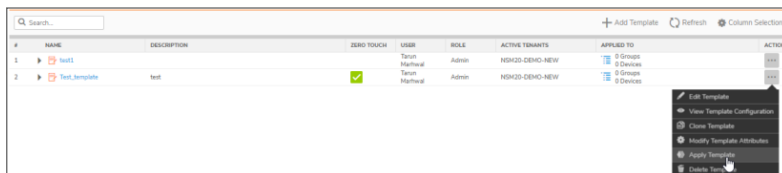
Applying Templates

You need to apply a template to deploy and manage common configurations across devices. When you apply a template to device group(s), you can deploy and manage configuration across all the devices of the group (s). You also have an option to apply a template to selected devices within any group.

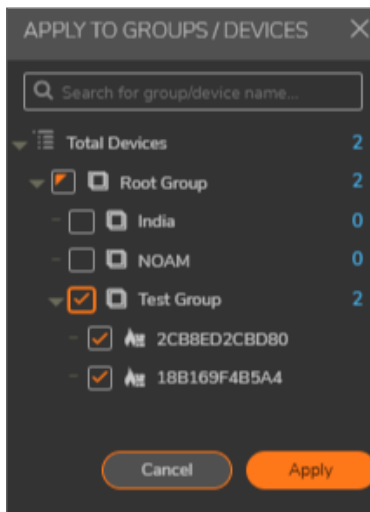
NSM supports application of multiple templates to device group(s) or device(s): To overwrite the configuration of the devices associated with any template, you can apply another template.

To apply a template:

1. Navigate to **Manager View > Templates**.
2. Hover over a template that you want to apply, click on the **Action** column and select **Apply Template**.



3. Select the device group(s) or devices within any group (s) to apply the template.
 - ① **IMPORTANT:** A template cannot be applied to device(s) that don't belong to any group. Hence, Unassigned Firewalls aren't displayed in the dialog.



4. Click **Save**.

If **Zero Touch** option is enabled for a template, the configuration of the template is auto-deployed to applied Zero-Touch devices; Offline devices will be updated once they come online. For non Zero Touch devices, the configuration updates available at each device needs to be committed and deployed to push the updates to the devices. For information on committing and deploying updates, see [Committing and Deploying the Updates](#).

View Template Status

To view template status:

1. Navigate to **Manager View > Templates**.
2. Hover over a template that you want to apply, click on the **Action** column and select **View Template Status**.

DEVICE NAME	RESULT	OPERATION(S)	FAILURE(S)	COMPLETION TIME	SUMMA
▼ Total Devices	Done	5/5	0		
▼ vram-group					
vk_01	Success	5/5	0	2021-02-13 12:32:02	Templa

3. Expand the device name to view the status of the listed templates.
4. Click **Close** to return to **Template** inventory.

Deleting Templates

① **NOTE:** By deleting a template associated with devices, you cannot perform configuration rollback on the target group(s) and device(s).

To delete a template:

1. Navigate to **Manager View > Templates**.
2. Hover over the template you wish to delete and click Ellipses icon in the **Action** column.

3. Select **Delete Template**.
4. Click **Confirm**.

Configuration Management

NSM supports different types and sizes of customers interested in managing their firewalls in the Cloud. A configuration change that is defined on the NSM side is referred to as PENDING CONFIGS, and for the changes to be effective on the firewalls, the changes need to be committed and deployed.

Topics:

- [Approval Groups](#)
- [Configuration Management Workflow](#)
- [Auditing Configuration Changes](#)

Approval Groups

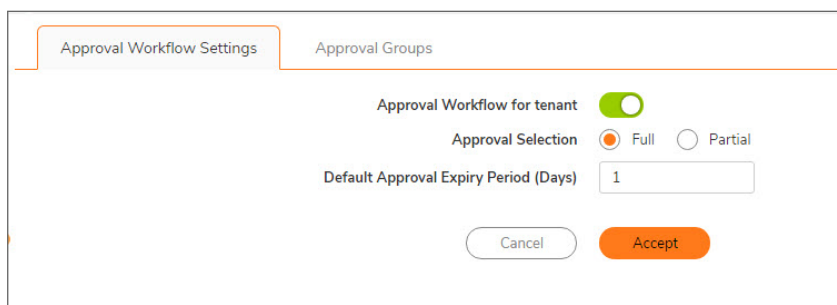
NSM has the ability to configure an approval process when planning and scheduling changes to the configuration (commits). Approval groups can be defined and enabled on a per tenant basis. You can also enforce partial approval, where one of a group of people can approve, or complete approval, where everyone has to approve. Customize the Approval Groups table by clicking **Column Selection**.

Topics:

- [Approval Workflow Settings](#)
- [Approval Group Management](#)

Approval Workflow Settings

Approval Groups allows you to enable and set up approvals for proposed system updates. .



The screenshot shows a dialog box titled "Approval Workflow Settings" with a sub-tab "Approval Groups". The settings are as follows:

- Approval Workflow for tenant:** A toggle switch that is currently turned on (green).
- Approval Selection:** Two radio buttons: "Full" (selected) and "Partial".
- Default Approval Expiry Period (Days):** A text input field containing the number "1".
- Buttons:** "Cancel" and "Accept".

To enable approvals:

1. Navigate to **Home | Config Management > Approval Groups**.
2. Enable the switch for **Approval Workflow for tenant** (move it to green).
3. Select whether full approval is required or if partial approval is allowed.
4. Set the number of day required to get the approval in the **Default Approval Expire Period** field. The default is **1** day.
5. Click **Accept**.

Approval Group Management

On the Approval Groups tab, you have to tools to manage the approval groups that you've defined for your tenants.

GROUP NAME	DESCRIPTION	GROUP USERS	APPROVER LIST	ACTION
SKTestAdmins	Admin Approvers for FW changes	1 User	1 Approver 1 Notificant	...
Demotest1	test	1 User	1 Approver 1 Notificant	...
Test_group_1	test	2 Users	2 Approvers 1 Notificant	...

The Approval Groups table lists all the approval that have been defined. It provides the group name, description, the number of users in the list and the type of user (whether they are an approver or a notificant).

To see more details about a particular group, click the caret by the Group Name. The entry expands to you can see the users that make up the list.

#	USER	USER ROLE
1	Admin	Admin
2	NSM Administrator	SuperAdmin

Topics:

- [Searching the Approval Groups](#)
- [Adding a New Approval Group](#)
- [Editing an Approval Group](#)
- [Deleting an Approval Group](#)
- [Setting the Default Approval Group](#)

Searching the Approval Groups

You can search for a specific approval group by using the name or description.

1. Type the string that you are searching for in the **Name** or **Description** field.
2. Press return and the table is filtered. You can use both fields at the same time to do further filtering.

3. Clear the filters to restore the full table.

Adding a New Approval Group

To add a new approval group:

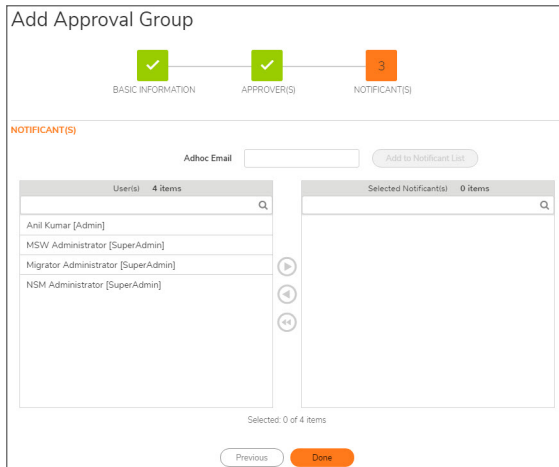
1. Navigate to **Home | Config Management > Approval Groups** and select the **Approval Groups** tab.
2. Click the **+Add** icon.

The screenshot shows the 'Add Approval Group' form with three steps: 1. BASIC INFORMATION (highlighted in orange), 2. APPROVER(S), and 3. NOTIFICANT(S). The 'BASIC INFORMATION' section contains a 'Name' field and a larger 'Description' field. At the bottom, there are 'Cancel' and 'Next' buttons.

3. Type the **Name** of the approval group.
4. Type the **Description** in the field provided. Make it unique so you can easily search on it if needed. A maximum of 256 characters are allowed.
5. Click **Next**.

The screenshot shows the 'Add Approval Group' form with three steps: 1. BASIC INFORMATION (highlighted with a green checkmark), 2. APPROVER(S) (highlighted in orange), and 3. NOTIFICANT(S). The 'APPROVER(S)' section features two columns: 'Users| 5 items' and 'Selected Approver(s)| 0 items'. The 'Users' column lists: Anil Kumar [Admin], MSW Administrator [SuperAdmin], Migrator Administrator [SuperAdmin], NSM Administrator [SuperAdmin], and ZT Administrator [SuperAdmin]. Navigation arrows are present between the columns. At the bottom, there are 'Previous' and 'Next' buttons.

6. In the **Users** column, select the users that you want to act as approvers for this group, and click the right arrow to move them to the **Selected Approvers** column.
① | NOTE: If the user you want is not listed, you need to go to MySonicWall to set them up.
7. Click **Next**.



8. In the **Users** column, select the users that you want to receive notice when approval is required, and click the right arrow to move them to the **Selected Notificants** column.
9. If you want to send notice to people not listed as users, enter their email in the **Adhoc Email** field and click **Add to Notificant List**.
10. Click **Done**.
11. Verify that the group appears in the table.

Editing an Approval Group

To edit an approval group:

1. Navigate to **Home | Config Management > Approval Groups** and select the **Approval Groups** tab.
2. Select the group name of the group you want to edit.
3. In the **Action** column, select **Edit**.
4. Navigate through the screens and make the changes needed.
5. Click **Done**.
6. Verify that the changes appear in the table.

Deleting an Approval Group

To delete an approval group:

1. Navigate to **Home | Config Management > Approval Groups** and select the **Approval Groups** tab.
2. Select the group name of the group you want to delete.
3. In the **Action** column, select **Delete**.
 - ① **NOTE:** If you want to delete several groups at once, check the box beside each one and click the **Delete** icon at the top of the table.
4. Confirm that you want to delete the selected group by clicking **Yes**. A confirmation message shows that the delete was completed successfully.

Setting the Default Approval Group

To set a new default approval group:

1. Navigate to **Home | Config Management > Approval Groups** and select the **Approval Groups** tab.
2. Click the **Set Default** icon.



The screenshot shows a web interface for setting the default approval group. At the top, it says "Default Approval Group". Below that is a dropdown menu with "SKTestAdmins" selected. At the bottom, there are two buttons: "Reset" and "Update".

3. Select the approval group from the drop-down list.
4. Click **Update**.

Configuration Management Workflow

Use the following workflow to prepare changes and push them to the devices.

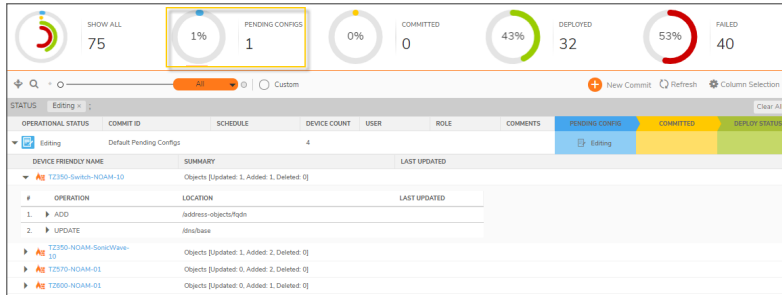
1. Perform firewall configuration changes through NSM.
You can perform configuration changes on firewalls by applying template to device group(s) or configuring changes in the **Firewall View**. To perform configuration in the Firewall View, see SonicOS documentation.
2. View pending configuration updates for the devices. See [Viewing Pending-Configuration Updates](#)
3. Perform commit and deploy to push the updates to managed devices. See [Committing and Deploying the Updates](#)
4. Monitor commits to check the deployment status of commits and take necessary action. See [Managing Commits](#).

Viewing Pending-Configuration Updates

The configuration changes performed on devices through NSM (either in **FIREWALL VIEW** or by applying templates to device groups) need to be committed (so that the changes are locked), and then deployed on the devices to push the updates to the devices.

To view pending configurations:

1. Navigate to **Manager view | Config Management > Commits** page.
2. Click **PENDING CONFIGS** at the top of the page.



3. Click the item that has the **OPERATIONAL STATUS** as **Editing**.
4. All the devices to which the configuration changes are applicable are displayed.
5. Click the caret icon next to a device name to see the configuration changes that are awaiting commit and deploy.

The operations are listed, for example: add, update, and so on. Click the caret icon next to the listed operation to see the JSON script of the operation performed. To perform commit and deploy, refer to [Committing and Deploying the Updates](#)

Committing and Deploying the Updates

After configuration updates are performed on devices through NSM either in Firewall View or by applying templates, you can review the updates (see [Viewing Pending-Configuration Updates](#)), and then commit (so that the changes are locked) and deploy the changes to the device(s) for the updates to be effective.

The commit and deploy action can be performed in any of following ways:

- **In the Firewall View: Commit & Deploy** menu allows you to commit and deploy updates for a firewall. After the configuration changes are made to any device, the **Commit and Deploy** menu item notifies configuration updates that are awaiting commit and deploy. See [Committing and Deploying Updates in the Firewall View](#).
- **In the Manager View:** From the **Commit & Deploy** wizard in the **Manager View**, you can commit and deploy configuration updates to the device(s). See [Committing and Deploying Updates to Device\(s\) in the Manager View](#).

Committing and Deploying Updates in the Firewall View

You can commit and deploy the configuration updates for any firewall in the Firewall View.

To commit and deploy the configuration updates on a firewall:

1. Navigate to the **Firewall View**.
 2. To see the pending configuration updates on a firewall, click **Commit and Deploy**.
- ① **NOTE:** You will see a notification on the **Commit and Deploy** option only when there are any pending configurations.



3. In the **Commit & Deploy Pending Changes** wizard:

- a. Enter the `Commit ID` and `Comments` in their respective fields. To commit and deploy the changes instantly, click **Deploy Now**. To schedule commit and deploy operations, navigate through the screens by clicking **Next** and choose a schedule date

Commit & Deploy Pending Changes

1 DEVICES 2 SCHEDULE 3 SUMMARY 4 COMMIT STATUS

PENDING CHANGES

Commit ID (Example: Case_100022) * Ticket-1613571869001

Comment * Commit & Deploy Now

Search... Discard Refresh

#	OPERATION	URI
1	▶ UPDATE	/address-groups/ipv4/name/RBL%20User%20White%20List
2	▶ ADD	/address-objects/ipv4
3	▶ ADD	/address-objects/ipv4
4	▶ ADD	/address-objects/ipv4
5	▶ ADD	/address-objects/ipv4
6	▶ ADD	/address-objects/ipv4
7	▶ ADD	/address-objects/ipv4
8	▶ ADD	/address-objects/ipv4

Total: 11 item(s)

Cancel Next Deploy Now

- b. If you select **Deploy Now**, a confirmation message on commit status is displayed.
- c. If you click **Next**, it allows you to set the schedule to a later time. Click **Commit** to commit items and **Deploy Now** at the scheduled time.
- d. A confirmation message on commit status is displayed. The deployment process runs at the scheduled time.
- e. Click **Close**.
- f. To see the deployment status of the commit items, see [Monitoring Commits](#).

Committing and Deploying Updates to Device(s) in the Manager View

From the **Commit & Deploy** wizard in the **Manager View**, you can commit and deploy configuration updates to the device(s).

1. Navigate to the **Manager View**.
2. View pending configuration updates. See [Viewing Pending-Configuration Updates](#)
3. Do one of the following:
 - Click **Commit & Deploy** in the upper-right corner of any page in the Manager View.
 - Navigate to **Config Management > Commits**, and click **New Commit**.

4. In the **Commit & Deploy Pending Changes** dialog, click the caret icon next to each device name in the **Devices** section to review the pending configuration updates.
5. Select the device(s) to commit and deploy pending configuration updates on all the selected device(s), enter `Commit ID` and `Comment` for your reference.

6. Click **Next**.
7. In the **SCHEDULE TIME** section, select either of the options:
 - **Now**—To commit and deploy the changes instantly. Skip to step 8.
 - **Set Schedule** —To commit now, and then deploy the changes as per the schedule.
8. If you selected **Set Schedule**, you need to set the schedule.
9. Click **Next**.
10. In the **Commit & Deploy Pending Changes** section, review your changes before committing.
11. Click **Commit**.
12. The status of commit is displayed in the **COMMIT STATUS** section.
For scheduled deployment, the configuration changes will be deployed at the scheduled time; for instantaneous deployment, configuration changes will be deployed shortly after committing the changes.

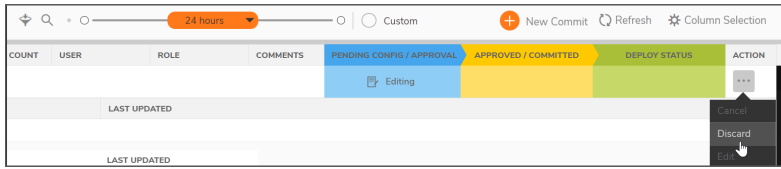
13. Click **Redirect to All Commits** to view the commits and their status. See [Monitoring Commits](#).

Discarding Pending Configurations

You can discard the pending configurations when you don't intend to commit and deploy the configuration changes.

To discard pending configurations:

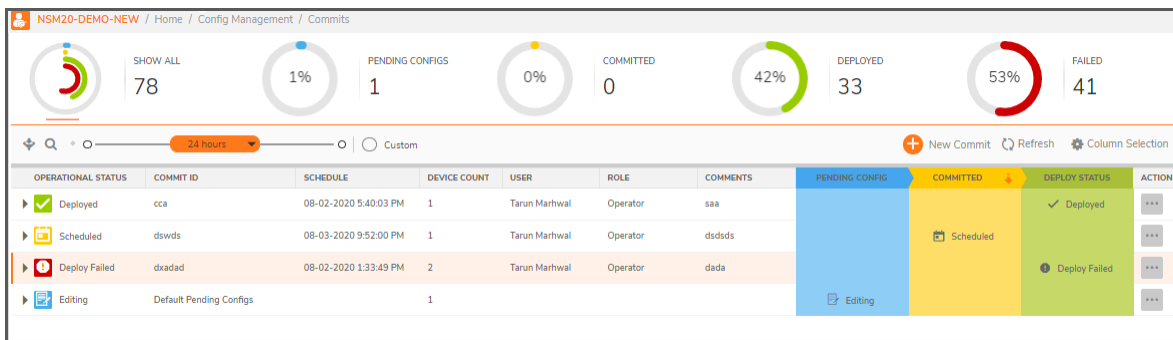
1. Navigate to **Manager view | Config Management > Commits**.
2. Hover over the item that shows **Editing** as its **OPERATIONAL STATUS** and click the **Ellipses** icon in the **ACTION** column.
3. Select **Discard**.



4. Click **Yes** in the confirmation dialog.

Monitoring Commits

The **Manager view | Config Management > Commits** page displays the information, such as, pending configuration updates and deployment status of commits. You can also manage commits from this page. See [Managing Commits](#).



You can customize what contents appear in the **Commits** table. The following list shows all the options. Click **Column Selection** and select or clear the selection of items to include or exclude data of any category in the table.

COMMITTS

Term	Description
OPERATIONAL STATUS	Status of the commit.
COMMIT ID	The user-assigned ID for the commit.
SCHEDULE	The Time at which the commit is deployed or when the commit should be deployed as per the schedule.
DEVICE COUNT	Number of devices to which the configuration changes are to be deployed.
USER	User that performed commit.
ROLE	Management role of user.
COMMENTS	The comment entered when creating a

Term	Description
	commit.
PENDING CONFIG / APPROVAL	Editing —configuration updates that are pending commit and deploy operations.
APPROVED / COMMITTED	Status of the commit.
DEPLOY STATUS	The deployment status of the commit.

Managing Commits

This section provides information on managing commits.

Topics:

- [Editing Commits](#)
- [Rescheduling Commits](#)
- [Redeploying Commits](#)
- [Deleting Commits](#)

Editing Commits

① | **NOTE:** You can edit only the commits that are scheduled for deployment.

To edit a commit:

1. Navigate to **Manager view | Config Management > Commits**.
2. Hover over the commit and click the **Ellipses** icon in the **ACTION** column.
3. Click **Edit**.
4. Click **Yes** in the **Confirmation** dialog.

Redeploying Commits

You can redeploy commits that have failed deployment.

To redeploy a commit:

1. Navigate to **Manager view | Config Management > Commits**.
2. Hover over the commit and click the **Ellipses** icon in the **ACTION** column.
3. Click **Redeploy**.
4. In the **Redeploy Commit** dialog, select one of the options:

- **Now**—to deploy instantaneously
 - **Set Schedule**—to set the schedule for deployment
5. If you selected **Set Schedule**, set the **Schedule Date**.
 6. Click **Submit**.

Rescheduling Commits

To reschedule a commit:

1. Navigate to **Manager view | Config Management > Commits**.
2. Hover over the commit and click the **Ellipses** icon in the **ACTION** column.
3. Click **Reschedule**.
4. In the **Reschedule Commit** dialog, select one of the options:

- **Now**—to deploy instantaneously
 - **Set Schedule**—set the schedule for deployment
5. If you selected **Set Schedule**, set the **Schedule Date**.
 6. Click **Submit**.

Deleting Commits

① **NOTE:** You can delete the commits that are scheduled for deployment and ones that are already deployed.

To delete a commit:

1. Navigate to **Manager view | Config Management > Commits**.
2. Hover over the commit and click the **Ellipses** icon in the **ACTION** column.

3. Click **Delete**.

a. Click **Yes** in the **Confirmation** dialog.

A success message is displayed if deletion is successful.

The **OPERATIONAL STATUS** of the commit changes to **Canceled** in the **Commits** page.

Auditing Configuration Changes

When managing multiple firewalls in an environment with multiple users, you want to be able to audit changes made by all the users to firewall address objects and groups. Network Security Manager shows who made changes that affect the rules and overall security of your devices.

This data is shown in the **Audit** table at **MANAGER VIEW > Config Management > Audit**. You can adjust the period of the audit by adjusting the slider at the top of the page to the predefined values. The table lists all the commits performed by the users on any device selected from the Devices drop-down list.

To view the configuration of the device after any particular commit / deploy operation, click caret icon next to the **DATE & TIME** field of the commit.

#	DATE & TIME	USER	ROLE	COMMIT ID	TYPE	COMMENTS
1	2020-05-21T22:16 PM	System	NA	NA	NA	Initial Registration

To view differences between configurations:

1. Navigate to **Template View > Config Management > Audit**.

2. Select two commits to compare.

#	DATE & TIME	USER	ROLE	COMMIT ID	TYPE	COMMENTS
1	2021-02-17T20:27 PM	nsmadmin	SuperAdmin	Ticket-1613573749494	Committed	Auto-backup of device configuration after commit - Commit & Deploy Now, CommitId:Ticket-1613573749494
2	2021-02-17T20:25 PM	nsmadmin	SuperAdmin	Ticket-1613573445995	Committed	Auto-backup of device configuration after commit - Commit & Deploy Now, CommitId:Ticket-1613573445995

3. Click on **Config Diff**. A color-coded display shows where the differences appear. Green text represents configuration data that was added. Red text represents data that was deleted, and blue is the value of the parameter.

4. To see a side-by-side comparison of the complete difference in configurations, click on **Full Diff**.

Tenants

The **Manager View | Tenants** page shows details of all the MSW tenants you have access to. You can manage or monitor all the firewalls that are registered to these tenants through NSM, based on your user role.

Adding tenants, assigning users to tenants, and assigning user roles can be performed only in MSW. To add tenants, assign users to tenants, and assign permission to users, see MSW online help.

Click on any tenant displayed on the Tenants page to access data corresponding to the selected tenant, across all the tabs listed in the left pane. The table displays the below information for each tenant:

Term	Definition
Name	Tenant name.
MSW TENANT ID	ID assigned to the tenant in MSW.
ALIAS	Another name (if any).
DEFAULT ADMIN	Email address of the default admin.

Click the caret icon next to a tenant name to view more details of the tenant.

CSC Users

The **Manager View | CSC Users** command set provides information on all the users that have been setup for access to the tenant you have logged into. Those users can manage firewalls through NSM, based on user roles assigned to them.

Topics:

- [CSC User Status](#)
- [Users](#)
- [Support Portal Users](#)
- [Roles and Permissions](#)

CSC User Status

The **Manager View | CSC Users > Status** page provides information of all the active user sessions.

#	USER	IP	ROLE	LOGIN TIME	ACTIVE	IDLE	REMAINING TIME
1	nsmadmin	10.65.20.121	SuperAdmin	2021-02-17 22:21:27		0h 0m 0s	0h 48m 0s
2	nsmadmin	10.65.20.121	SuperAdmin	2021-02-17 20:44:08		0h 46m 57s	0h 1m 3s

The following information is displayed for each active user session:

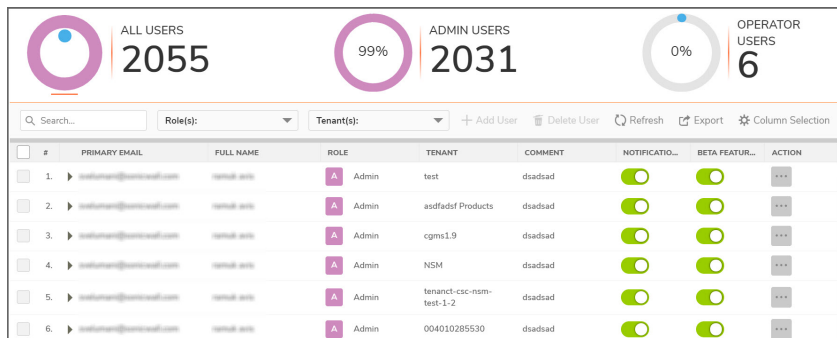
Term	Definition
USER	User that has an active session.
IP	IP address of the system that hosts user session.
EMAIL	Email address of the user.
ROLE	Management role of the user.
LOGIN TIME	Timestamp of the user login.
ACTIVE	Activity status
IDLE	Duration for which the user remains inactive.
REMAINING TIME	The time remaining in their login session.

To log out the user(s):

1. Select the user(s) and click **Logout User(s)**.
2. Click **OK** to confirm.

Users

The users listed on the **Users** page (**Manager View | CSC Users > Users**) are assigned to a tenant in MySonicWall (MSW). You can add CSC users for any tenant, assign users to a tenant and assign user roles only through MSW. For information on assigning users to tenants and assigning user roles, refer to the MSW online help.



The table on the **Users** page gives the following details for any user listed:

Term	Definition
PRIMARY EMAIL	Email address of the user.
FULL NAME	Full name of the user.
ROLE	Management role of the user; this role is assigned in MSW. <ul style="list-style-type: none"> • SuperAdmin- Provides complete access to the user. User can add or update or delete the following: Users, Tenants, and Devices in MSW. • Admin - User can configure firewall; edit UserInfo (Email/timeout); add or delete devices in MSW • Operator - User can configure firewalls. • Support - No Configuration Mode; user can only view firewall configurations. • ReadOnly - No Configuration Mode; user can only view firewall configurations. • Guest - No Configuration Mode; user can only view firewall configurations.
TENANT(S)	Tenant(s) to which the user has access to.
COMMENT	Any comment if added.
NOTIFICATION	A switch that enables or disables notifications for a user.
BETA FEATURES	A switch that enables or disables beta features for a user.
ACTION	Provides the options edit or delete a user.

Topics:

- [Sorting and Filtering](#)
- [Editing CSC Users](#)

Sorting and Filtering

The Users table can be sorted, searched, and filtered to find a specific user or type of user. At the top of the page, you can use the graphs to filter the table contents. The default is to show all users, but if you click on the other options, **Admin Users** or **Operator User**, for example, the table filters itself to show only the type of user chosen.

The fields at the top of the table offer other filtering options. Enter a string of characters in the search field and the table responds as you type. You can select specific roles or tenants to provide additional filtering.

At any time you can export the data to a CSV file by clicking the **Export** icon.

Editing CSC Users

Most major changes to users, including deleting users, need to be performed in MSW. However, some features can be edited locally.

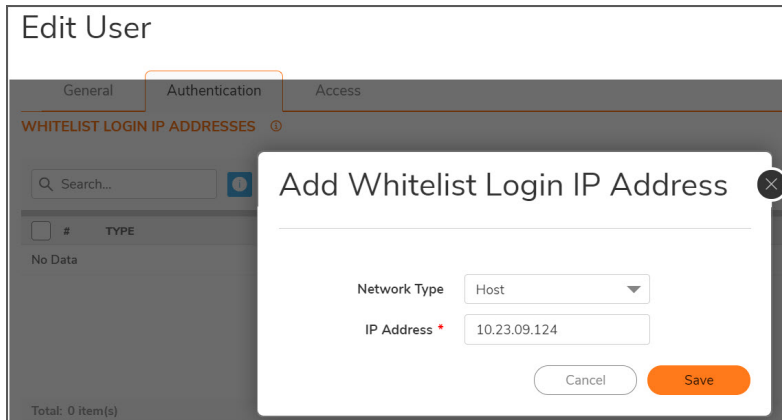
To update user information:

1. Navigate to **Manager View | CSC Users > Users**.
2. Hover over the user that you want to edit and click **Edit** option in the **ACTION** column.

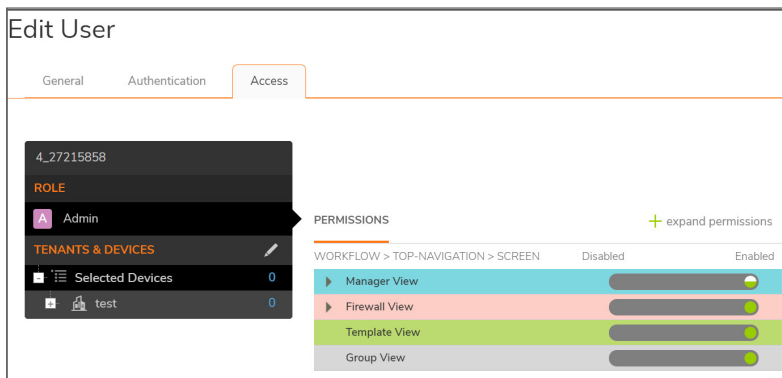
The screenshot shows the 'Edit User' dialog box with the following fields and values:

Field	Value
Username	4.27215858
Primary Email	4.27215858@cs.com
Secondary Email	Enter Secondary Email...
Comment	dsadsad
First Name	johndoe
Middle Name	
Last Name	doe
Phone	408-555-1234
Timeout	20
Notifications	Checked

3. In the **Edit User** dialog, enter the following:
 - **Secondary Email**—Secondary email address of the user
 - **Comment**—Any valid comment
 - **Notifications**—Enable or disable notifications
 - **Timeout**—The duration after which the user is logged out
4. In the **Authentication** dialog, you can Whitelist login IP addresses. The IP address that are not added in the Whitelist Login IP Addresses will be blocked.



- a. Click **Add** to add Whitelist login IP Address.
 - b. From the **Network Type**, choose the option **Host**, **Range** or **Network**.
 - Host** - When selected Host, input the IP address of the whitelist device.
 - Range** - When selected Range, enter starting and ending IP range
 - Network** - When selected Network, enter Network name and Netmask. The user's IP address is automatically checked whether the user is logging in from an allowed IP whenever a login is attempted.
5. Click the **Access** tab to see the various permissions and devices access.



6. Click on the **Role** to see the permissions granted to this user. You can click the **+** icon to expand the permissions list to see the detail behind it. Click again to collapse permissions.
7. Click the Edit icon in **TENANTS & DEVICES** to associate tenants and devices together and click **Apply**.
8. Return to the **General** tab and click **Save**.

Support Portal Users

Navigate to **Manager View | CSC Users > Support Portal Users** set up user permissions for using the Support Portal. All current users are listed in a table and you can use the search field to filter the list by typing in a string of characters. The table identifies the support user type (Admin or User) and shows whether they are enabled to use the support portal or not.

#	EMAIL	TYPE	ENABLED
<input type="checkbox"/>			
<input type="checkbox"/>	1	Support Admin	<input checked="" type="checkbox"/>
<input type="checkbox"/>	2	Support User	<input checked="" type="checkbox"/>
<input type="checkbox"/>	3	Support User	<input checked="" type="checkbox"/>
<input type="checkbox"/>	4	Support User	<input checked="" type="checkbox"/>
<input type="checkbox"/>	5	Support User	<input checked="" type="checkbox"/>
<input type="checkbox"/>	6	Support User	<input checked="" type="checkbox"/>
<input type="checkbox"/>	7	Support Admin	<input checked="" type="checkbox"/>
<input type="checkbox"/>	8	Support User	<input checked="" type="checkbox"/>
<input type="checkbox"/>	9	Support User	<input checked="" type="checkbox"/>
<input type="checkbox"/>	10	Support User	<input checked="" type="checkbox"/>
<input type="checkbox"/>	11	Support User	<input checked="" type="checkbox"/>

To create a Support Portal user:

1. Navigate to **Manager View | CSC Users > Support Portal Users**.
2. Click the **+Add** icon.

Create Support Portal User

Email *

Type

Enabled

3. Type the email of the user you are adding.
4. Select the type of user from the drop-down list.
5. Enable the user's access.
6. Click **Save**.

Users can be deleted by selecting a user and clicking the **Delete** icon.

Roles and Permissions

The functions of the administrative and support roles are defines on the Roles and Permissions page. Here you determine what actions each roles is allowed to take. You can see a summary of the definitions in the table, and you can see the details by clicking on the caret beside the role name.

#	ROLE NAME	BASE ROLE	MANAGER VIEW PERMISSL...	FIREWALL VIEW PERMISSL...	TEMPLATE VIEW PERMISSL...	GROUP VIEW PERMISSION	ACTION
1	SuperAdmin	SuperAdmin	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	...

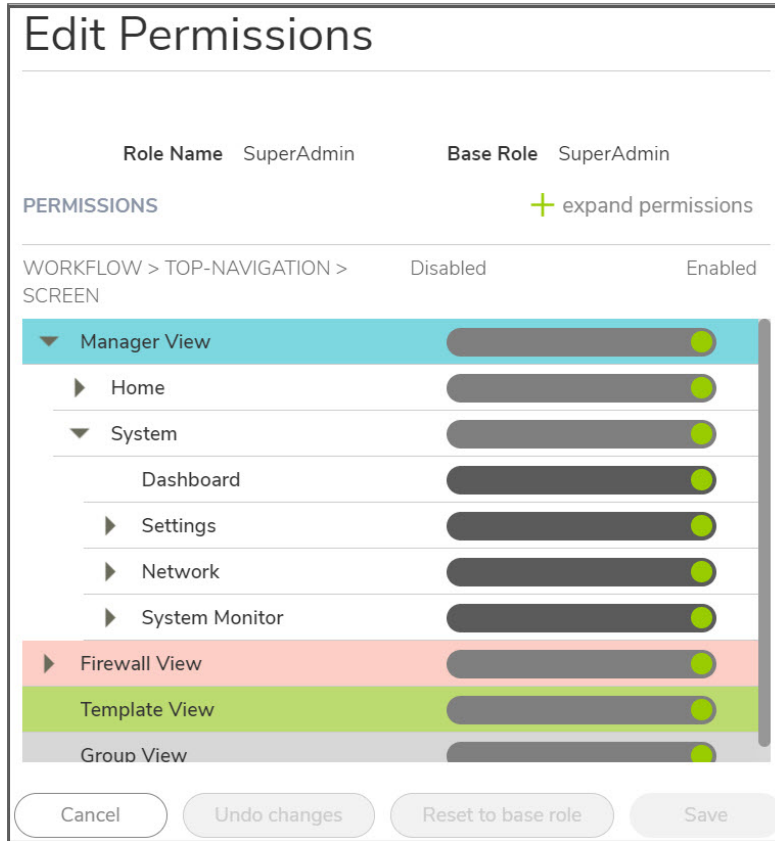
PERMISSIONS + expand permissions

WORKFLOW > TOP-NAVIGATION > SCREEN Disabled Enabled

- ▶ Manager View
- ▼ Firewall View
 - Home
 - Monitor
 - Device
 - Network
 - Object
 - Policy
- Template View
- Group View

To edit the permissions assigned to each role:

1. Navigate to **Manager View | CSC Users > Roles and Permissions**.
 - a. Select the **Edit** command in the Action column for the role you want to change.



2. Expand the permissions and find the parameters that you want to change.
 - ① **NOTE:** When the state is enabled, the green circle means that all the children parameters are also enabled. A half green circle indicates that some children parameters are in a disabled state. A gray circle indicates that all children are disabled.
3. Slide the indicator to enabled or disabled as needed.
4. Click **Save** to retain the settings.

Scheduled Reports

You can set up schedules to generate reports at regular intervals. As part of scheduling, you need to specify the following: **report type and the type of information that you wish to include; devices or groups for which the reports should be generated; how often the reports are delivered; and the medium for report delivery.**

Managing the Schedules

The table on **Manager View | Scheduled Reports > Rule** page displays the shows the scheduled reports that are created. The details of each scheduled report are shown in a tabular format.

The screenshot displays a dashboard with four circular progress indicators: ALL SCHEDULES (6), SUCCESS (33%, 2), FAIL (50%, 3), and IN PROGRESS (0%, 0). Below these is a search bar and action buttons: + Add, Delete, Refresh, Run Now, Run for date range, and Column Selection. A table lists one report: SubscriptionReport, Weekly, Management, Archive, with last run time 2021-02-13 05:34 and next schedule time 2021-02-20 05:30. Below the table are two expandable sections: SCHEDULE DETAILS and SCHEDULE UNIT STATUS DETAILS.

#	SCHEDULE NAME	SCHEDULE TYPE	REPORT TYPE	DELIVERY TYPE	LAST RUN TIME	NEXT SCHEDULE TIME	LAST RUN STATUS	ACTION
1	SubscriptionReport	Weekly	Management	Archive	2021-02-13 05:34	2021-02-20 05:30	Success	...

SCHEDULES TABLE

Term	Description
SCHEDULE NAME	Name of the scheduled report.
SCHEDULE TYPE	Execution frequency of the scheduled report.
REPORT TYPE	Report type—Flow or CTA or Management
DELIVERY TYPE	Medium for delivering the PDF report.
LAST RUN TIME	Timestamp when the scheduled report was executed the last time.
NEXT SCHEDULE TIME	Timestamp when the scheduled report will be executed the next time.

Term	Description
LAST RUN STATUS	Status of the report that was executed the last time.
ACTION	Displays options to edit or delete the schedule.

In addition to the above data, more information about a rule is displayed when you click the caret icon next to the schedule name.

- **Schedule ID:** ID assigned to the scheduled report by NSM
- **Owner:** User that created the scheduled report
- **Report Type:** Report type—Flow or CTA or Management
- **SCHEDULE UNIT STATUS DETAILS:** Status of the report execution for each device

Several icons at the top right corner of the table help you manage your schedules. Refer to the image and table below to learn more about them.

Success	Number of reports that were successfully executed the last time.
Fail	Number of reports that failed execution the last time.
In Progress	Number of reports that are currently running.
Add	To set up a new scheduled report.
Delete	To delete the selected scheduled report.
Refresh	Refresh the page.
Run Now	To generate the selected report(s) instantly.
Run for date range	To generate the selected report(s) to obtain data over a custom period.
Column Selection	Choose which options to be displayed in the table

Creating Scheduled Reports

You can set up **Flow** report or **CTA** (Capture Threat Assessment) report or **Management** report.

You can also create scheduled reports for a firewall in the **Firewall View (Home | Schedule > Reports Rules)** page. The procedure for creating scheduled reports in the **Firewall View** is similar to creating a scheduled report in the Manager View as given below.

To create a scheduled report:

1. Navigate to **Manager View | Scheduled Reports > Rule**.
2. Click the **+ Add** icon above the table.
The **ADD SCHEDULE** wizard is displayed.

3. In the **REPORT CONFIGURATION** page:

- a. Type the **Report Name**.
- b. Type the **Report Description**.
- c. Select the Report Type: **Flow**, **CTA**, or **Management**.

The options displayed in the **REPORTS** section depend on the selected report type. For information on the categories that you want in your report, see *Analytics and Reporting* document.

- **RealTime Reports:** This section provides applications rate, interface bandwidth, cpu usage and connection rate over a period of time.
 - **Dashboard Reports:** This section provides top 10 for applications, threats, users, URLs, IPs, countries, bandwidth queue usage for traffic traversing through the firewall during specified times.
 - **Details Reports:** This section provides detailed view of the applications, threats, users, URLs, IPs, countries usage for traffic traversing through the firewall during specified times.
- d. Select the type of information you want in your report from the options displayed. You can include all the data by selecting **Select All**.
 - e. Click **Next**.

4. In the **DEVICE SELECTION** page:

- a. Select one of the following options: **Firewall**—to select firewalls, **Group**—To select device groups, or **Tenant**—To select the tenant you have logged into.
Tenant option is not available for **Flow** Reports.

Add Schedule

1 REPORT CONFIGURATION
 2 DEVICE SELECTION
 3 DELIVERY CONFIGURATION
 4 REVIEW

Firewall
 Group
 ⓘ Select a maximum of 5 devices

#	DEVICE	SERIAL NUMBER	IP ADDRESS
<input type="checkbox"/> 1	narendragen5fw	0017C510F694	10.5.18.53
<input type="checkbox"/> 2	0017C510F6A9	0017C510F6A9	1.2.2.3
<input type="checkbox"/> 3	0017C510F6B9	0017C510F6B9	2.2.2.1.1
<input type="checkbox"/> 4	0017C510F6C9	0017C510F6C9	test23
<input type="checkbox"/> 5	Testuser	0017C510F6DT	93.393.34.2
<input type="checkbox"/> 6	TestDevice	0017C510F6U9	93.39.34.24
<input type="checkbox"/> 7	Test1	0017C5ABF677	1.1.1.1
<input type="checkbox"/> 8	Test	0017C5ABF678	34.64.74.13

- b. Click **Next**.
5. In the **DELIVERY CONFIGURATION** page:
- a. Select the **Delivery Interval**. You can choose **Daily**, **Weekly**, or **Monthly**.

Add Schedule

1 REPORT CONFIGURATION
 2 DEVICE SELECTION
 3 DELIVERY CONFIGURATION
 4 REVIEW

Delivery Interval
 Daily
 Weekly
 Monthly

Schedule Time

Edit Weekly Reports Schedule Day
 Sunday

Delivery Type
 Archive
 Email

Password Protect

Use Custom Logo

Select a Logo

Upload a Logo

- b. Specify the **Schedule Time**.
- c. For **Weekly Reports**, enable **Edit Weekly Reports Schedule Day** and select the required day to specify the day when to receive the report. The default option is **Sunday**.
- d. For **Monthly Reports**, enable **Edit Monthly Reports Schedule Date** and select the appropriate date to receive the report. The default date is **7**.
- e. Select the **Delivery Type** to indicate whether the report is set up for archiving or emailing, or

both.

If you have selected delivery type as **Email**, you need to provide information on the email recipient in `Email Destination`—user role of the recipient and `Email ID` fields. Enter the `Email Subject` and `Email Body`. `Email Body` is optional.

- f. If you have enabled email delivery type, you can choose to receive compressed report by enabling **Zip Report**.
 - g. If you want added security for the report, enable **Password Protect**. Enter and confirm the password when asked.
 - h. To use a custom logo in your reports, enable **Use Custom Logo** and select or upload a logo from your local system.
 - i. Click **Next**.
6. Review report settings, click **Save**.

Add Schedule

STEP 1 CONFIGURATION DEVICE SELECTION DELIVERY CONFIGURATION REVIEW 4

Cover Logo: checkmark.png
Cover Image: [Teal Checkmark]
Schedule Name: scvdec
Schedule Interval: Weekly
Report Type: Flow
Schedule Delivery: Archive
Report Configuration: [+] RealTime Reports
Device Selection: [+] Firewall

Previous Save

If you have successfully created a scheduled report, a success message is displayed. The newly created report is displayed on Rules page.

Editing Schedule

To edit the rule for a scheduled:

1. Navigate to **Manager View | Scheduled Reports > Rule**.
2. In the **ACTION** column, click the **Ellipses** icon for the schedule you want to edit, and select **Edit Schedule**.

Global Default Tenant / Home / Scheduled Reports / Rules

ALL SCHEDULES: 7
SUCCESS: 29% (2)
FAIL: 43% (3)
IN PROGRESS: 0%

#	SCHEDULE NAME	SCHEDULE TYPE	REPORT TYPE	DELIVERY TYPE	LAST RUN TIME	NEXT SCHEDULE TIME	LAST RUN STATUS	ACTION
1	SubscriptionReport	Weekly	Management	Archive	2021-02-13 05:34	2021-02-20 05:30	Success	...
2	weekly	Weekly	Management	Archive	2021-02-12 05:30	2021-02-19 05:30	Failed (Not R...	...
3	Newreport	Weekly	Flow	Archive	2021-02-15 12:49	2021-02-21 05:30	Not Availa...	...
4	test	Daily	Management	Archive	2021-02-17 05:30	2021-02-18 05:30	Success	...
5	test	Weekly	CTA	Archive	2021-02-16 21:41	2021-02-21 12:30	Failed (Device does no...	...
6	Test	Weekly	CTA	Archive	2021-02-17 12:33	2021-02-21 12:30	Failed (Device does no...	...
7	scvdic	Daily	Flow	Archive	2021-02-18 05:30		Not Available	...

- You can make necessary changes in the **CREATE SCHEDULE** wizard. See [Creating Scheduled Reports](#) for reference.

Running Reports Manually

You can run a scheduled report anytime, and need not wait for the report to run at the scheduled time. Running the report just after scheduling helps you to check if your configurations have been saved and are scheduled as you have planned.

To run a scheduled report instantly:

- Navigate to **Manager View | Scheduled Reports > Rule**.
- Select the checkbox next to the schedule name and click **Run Now** at the top of the table.

#	SCHEDULE NA...	SCHEDULE TYPE	REPORT TYPE	DELIVERY TYPE	LAST RUN TIME	NEXT SCHEDULE TIME	LAST RUN S...	ACTION
<input checked="" type="checkbox"/>	SubscriptionRepor	Weekly	Management	Archive	2021-02-13 05:34	2021-02-20 05:30	Success	...

- Click **OK** in the dialog displayed. **LAST RUN STATUS** changes to **In progress** and eventually changes to **Success** if the report runs successfully.

If you had configured **Archive** as one of the **DELIVERY TYPE** options for the scheduled report, the report you generated is available for download. For more information on working with the archived reports, see [Downloading Archived Reports](#).

Setting the Report Date Range

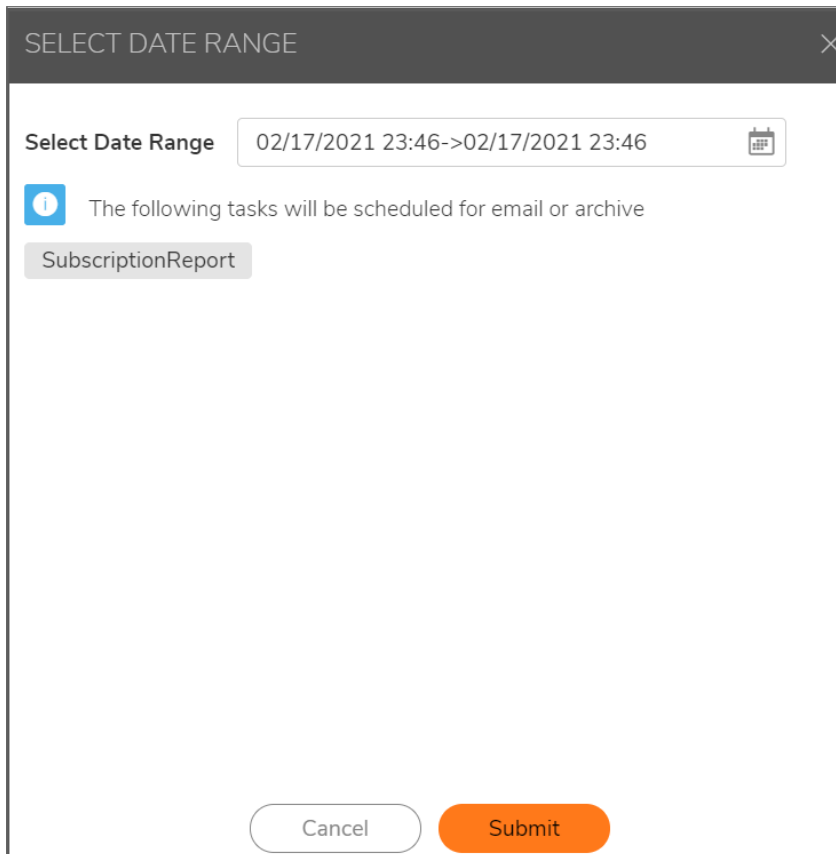
To generate a report to obtain data over a custom period, you need to specify the date range.

To set the date range:

- Navigate to **Manager View | Scheduled Reports > Rule**.
- Select the checkbox next to schedule name and click **Run for date range** at the top of the table.

#	SCHEDULE NA...	SCHEDULE TYPE	REPORT TYPE	DELIVERY TYPE	LAST RUN TIME	NEXT SCHEDULE TIME	LAST RUN S...	ACTION
<input checked="" type="checkbox"/>	SubscriptionRepor	Weekly	Management	Archive	2021-02-13 05:34	2021-02-20 05:30	Success	...

- Click the calendar icon and select the date range by clicking and holding the mouse button on a start date and dragging it to the end date, highlighting the range.



4. Click **Submit**.

The report runs instantly; it includes data for the specified date range.

Archived Reports

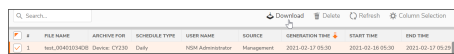
Navigate to **Manager View | Scheduled Reports > Archive** to view the archived reports. Each report shows the following details:

FILE NAME	Name of the report
ARCHIVE FOR	Device name to archive
SCHEDULE TYPE	Frequency at which the PDF reports are generated
USER NAME	User that ran the scheduled report manually
SOURCE	Report type
GENERATION TIME	Time at which the PDF report was generated
START TIME; END TIME	Displays the interval for which the data is captured in the generated report.
ACTION	Options to download or delete the report

Downloading Archived Reports

To download an archived report:

1. Navigate to **Manager View | Scheduled Reports > Archive**.
2. Select the checkbox(es) next to the schedule name(s) for which you want to download the report, and click **Download** icon at the top of the table.



The screenshot shows a table with a search bar at the top and a toolbar with 'Download', 'Delete', 'Refresh', and 'Column Selection' buttons. The table has columns for 'FILE NAME', 'ARCHIVE FOLDER', 'SCHEDULE TYPE', 'USER NAME', 'STATUS', 'GENERATION TIME', 'START TIME', and 'END TIME'. A single row is visible with a checked checkbox in the first column and a download icon in the second column.

FILE NAME	ARCHIVE FOLDER	SCHEDULE TYPE	USER NAME	STATUS	GENERATION TIME	START TIME	END TIME	
<input checked="" type="checkbox"/>	test_004223420	Device Config	Day	NSM Administrator	Management	2021-02-17 09:30	2021-02-18 09:30	2021-02-17 09:30

3. Click **OK** in the **DOWNLOAD CONFIRMATION** dialog.

System Events

NSM maintains an Event log for tracking potential security threats.

Configuring Log Settings

You can configure LOGS AND ALERTS SETTINGS on the **Manager View | Logs & Alerts > Settings** page to configure the items that needs to be tracked in the Events page. You can filter the entries to limit the data display to only those events of interest.

① | **NOTE:** Debug log settings can be performed only by Super Admins or Tech Support representatives.

The **Log Level** shows the severity or priority of an event. The **Alert Level** drop-down shows options that indicate whether an alert message will be sent for this event.

△ | **CAUTION:** Changing the Event Priority may have serious consequences as the Event Priority for all events will be changed. Setting the Event Priority to a level that is lower than the Log Level will cause those events to be filtered out.

To perform logs and alerts settings:

1. Navigate to **Manager View | Logs & Alerts > Settings** page.
2. Select an option in **Log Level** drop-down and set the corresponding **Alert Level** as required.
You can set appropriate alert levels for other log levels available.

LOGS AND ALERTS SETTINGS

Log Level: Info

Alert Level: Alert

Cancel Save

3. Click **Save**.

Viewing System Events

The **Manager View | Logs & Alerts > Events** page displays the system events and their details based on the filter you set.

#	LOCAL TIME	CATEGORY	PRIORITY	MESSAGE	SOURCEIP	TENANT NAME	REQUESTID
1	2020-07-02 16:54:58	Device Management	Info	Device Summary successfully fetched	122.171.59.202	NSMQ2-DEMO-NEW	a6f72acc-2066-94d9-b6c9-76630a6d49f5
2	2020-07-02 16:54:45	Device Management	Info	Device Summary successfully fetched	137.97.249.171	NSMQ2-DEMO-NEW	1350594c-d184-90ac-a248-255ea9598c211
3	2020-07-02 16:54:27	Device Management	Info	Device Summary successfully fetched	122.171.59.202	NSMQ2-DEMO-NEW	8364bd46-3566-9a61-e8b5-e750c3ca679
4	2020-07-02 16:54:14	Device Management	Info	Device Summary successfully fetched	137.97.249.171	NSMQ2-DEMO-NEW	d903c183-952c-9966-ba7a-e93794d8969e
5	2020-07-02 16:53:57	Device Management	Info	Device Summary successfully fetched	122.171.59.202	NSMQ2-DEMO-NEW	561d8aaf-c225-9737-8848-512d891cd8b
6	2020-07-02 16:53:43	Device Management	Info	Device Summary successfully fetched	137.97.249.171	NSMQ2-DEMO-NEW	06c79d17-c108-92ed-9f70-e211d1c1f5c3
7	2020-07-02 16:53:27	Device Management	Info	Device Summary successfully fetched	122.171.59.202	NSMQ2-DEMO-NEW	811a7044-6489-985e-9aed-482238ea2ce
8	2020-07-02 16:53:12	Device Management	Info	Device Summary successfully fetched	137.97.249.171	NSMQ2-DEMO-NEW	865e4957-8577-9e15-9a28-f9223331a1a8
9	2020-07-02 16:52:56	Device Management	Info	Device Summary successfully fetched	122.171.59.202	NSMQ2-DEMO-NEW	20564172-a172-9527-a972-98c363380a3d
10	2020-07-02 16:52:41	Device Management	Info	Device Summary successfully fetched	137.97.249.171	NSMQ2-DEMO-NEW	9944c7a4-e0d4-9794-b1f5-be532e69b304
11	2020-07-02 16:52:26	Device Management	Info	Device Summary successfully fetched	122.171.59.202	NSMQ2-DEMO-NEW	5986a3b7-4732-91a1-81a3-daf9981a100
12	2020-07-02 16:52:10	Device Management	Info	Device Summary successfully fetched	137.97.249.171	NSMQ2-DEMO-NEW	b5c3a08b-bd73-912b-84bd-00e6791e03e
13	2020-07-02 16:51:56	Device Management	Info	Device Summary successfully fetched	122.171.59.202	NSMQ2-DEMO-NEW	0aaa3d9b-20d6-9990-8a16-1b3dc2ba3c08
14	2020-07-02 16:51:39	Device Management	Info	Device Summary successfully fetched	137.97.249.171	NSMQ2-DEMO-NEW	ed2f6f7-c280-9001-8a56-797344240232

Click the **gear** icon at the upper-right corner and select the items that you want as columns in the Event Log. You can also search for an event in the **Search** box. You can export the event logs to a CSV file using **Export** option.

You can configure the following to view the events of your desired combination:

Period	You can set the duration to view the events for the selected period using the slider at the top of the table.
Priority	Priority level of the event, such as Info (information) or Error. <ul style="list-style-type: none"> Emergency Critical Alert Error Warning Notice Info Debug Trace Trace 2
Category	Category of the event. <ul style="list-style-type: none"> All Category Notification Configuration API Device Management Reporting and Analytics Reporting User

The following details are displayed for each event logged:

LOCAL TIME	Time at which the event is logged
CATEGORY	Category to which the logged event belongs to.
PRIORITY	Priority level of the event

MESSAGE	Information on the event
SOURCEIP	IP address of the source device
TENANT NAME	Tenant for which the log is triggered
REQUEST ID	A unique ID for every event that was created

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 Administration Guide

Updated - March 2021

232-005314-01 Rev B

Copyright © 2021 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