# Network Security Manager

## Administration Guide

SONICWALL®

# Contents


**Network Security Manager Overview** ..... **6**
About Network Security Manager ..... 6
Related Documents ..... 7
API Support ..... 8
Legal Information ..... 9
Conventions ..... 9
Guide Conventions ..... 10
UI Conventions ..... 10

**Dashboard** ..... **12**
Summary ..... 13
Network ..... 15
Threat ..... 15

**Firewalls** ..... **17**
Device Inventory ..... 17
Device Status ..... 21
Managing Devices ..... 25
Firewall View ..... 33
Device Groups ..... 35
Working with Device Groups ..... 36
Backups ..... 39
Scheduling Backups ..... 41
Archiving TSR ..... 41
Archiving EXP ..... 42

**Templates and Variables** ..... **43**
Templates ..... 43
Templates Inventory ..... 44
Creating Templates ..... 45
Editing Templates ..... 46
Viewing Template Configuration ..... 46
Creating Duplicate Template ..... 47
Modifying Template Attributes ..... 47
Applying Templates ..... 48
View Template Status ..... 49
Deleting Templates ..... 49
Storage ..... 50

Golden Template ..... 51
Preparing the Firewall ..... 51
Exporting the Firewall Configuration into Template ..... 52
Editing Golden Template ..... 53
Applying Template to Device Groups or Devices ..... 54
Committing and Deploying the Updates ..... 55
Variable Data ..... 55
Template Variables Overview ..... 55
Add Variable ..... 56
Edit Variable ..... 57
Resolve Variable ..... 57
Delete Variable ..... 58
Using Template Variables ..... 59
Creating Variables within Templates ..... 59

**SonicWall Switch Configuration in Template ..... 61**
Before Adding a Switch ..... 61
Add Switch ..... 62
Edit Port ..... 63
Switches ..... 66
Network ..... 66
Users ..... 67
Static routes ..... 68
802.1x ..... 68
Radius server ..... 69
ARP ..... 70

**Certificates ..... 71**
Navigating Certificates ..... 71
New Signing Request ..... 72
Commit and Deploy Certificate(s) ..... 73
Configuring SCEP ..... 74
Importing Certificates ..... 74
Deleting Certificates ..... 75

**Configuration Management ..... 77**
Approval Groups ..... 77
Approval Workflow Settings ..... 77
Approval Group Management ..... 78
Searching the Approval Groups ..... 79
Adding a New Approval Group ..... 79
Editing an Approval Group ..... 81
Deleting an Approval Group ..... 81
Setting the Default Approval Group ..... 81

Configuration Management Workflow ..... 82
Committing and Deploying the Updates ..... 82
Viewing Pending Configuration Updates ..... 85
Discarding Pending Configurations ..... 86
Monitoring Commits ..... 86
Managing Commits ..... 87
Auditing Configuration Changes ..... 89

**Tenants ..... 91**

**VPN Topology ..... 92**
IPsec VPN Topology ..... 92
Topologies ..... 92
Security Associations ..... 103
IPsec Monitor ..... 104
Global Settings ..... 104

**SD-WAN Topology ..... 107**
Configuring SD-WAN ..... 107
Basic Information ..... 108
Rules and Devices ..... 108
Service Rule ..... 109
Application Rule ..... 111
Device Selection ..... 112

**CSC Users ..... 113**
CSC User Status ..... 113
Users ..... 114
Sorting and Filtering ..... 115
Editing CSC Users ..... 115
Support Portal Users ..... 118
Roles and Permissions ..... 119
Authentication Servers ..... 122

**Scheduled Reports ..... 125**
Managing the Schedules ..... 125
Creating Scheduled Reports ..... 126
Editing Schedule ..... 130
Running Reports Manually ..... 131
Setting the Report Date Range ..... 131
Archived Reports ..... 132
Downloading Archived Reports ..... 133

**System Events ..... 134**

Configuring Log Settings ..... 134
Alerts and Notifications ..... 135
Configuring Twilio Setting for SMS ..... 137
Viewing System Events ..... 137

**SonicWall Support ..... 140**
About This Document ..... 141

1

# 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
- Related Documents
- API Support
- Legal Information
- Conventions


## 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-enable 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.

# Related Documents

In addition to this document, which describes how to set up and configure an On-Premises instance of NSM on various types of virtual machines, the NSM document set is made up of the following:

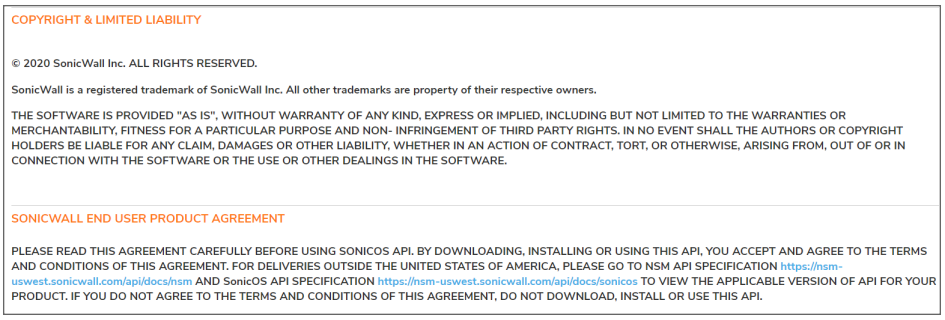
| Document | Description | When to Use It |
|---|---|---|
| *About Network Security Manager* | Provides an overview of the product and describes the base modes of operation, the navigation and icons, and the **Notification Center**. | Read this document gain an understanding of basic tasks before diving into specific NSM topics and tasks in the other books. These include:<br>• Overview of NSM<br>• Review of basic workflows<br>• Introduction to the Dashboard and monitoring<br>• Navigation<br>• Notification Center<br>This document applies to both SaaS and On-Premises instances. |
| *NSMAdmin Guide* | Provides details on NSM features for administering your instance of NSM. | Read this document to learn how to configure and maintain NSM. Use the workflows from above as a checklist for the sequence of actions and feature descriptions. This document applies to both SaaS and On-Premises instances. |

| Document | Description | When to Use It |
|---|---|---|
| *Network Security Manager Reporting and Analytics Administration Guide* | Discusses how to use the reporting and analytics features. | Read this document to learn what types of reports are available and how to navigate within them. It also describes how to schedule reports and define their contents. This document applies to both SaaS and On-Premises instances.<br><br>The Advanced license is needed to access all the Analytics features. |
| *Network Security Manager On-Premises System Administration Guide* | Describes the system administration tasks for an on-premises deployment of NSM. | Read this document to understand how to configure and manage an on-premises instance of NSM. It includes:<br>• System Dashboard<br>• System settings<br>• Network settings<br>• System monitoring<br>• High Availability (HA) configuration<br><br>This document applies to On-Premises instances only. |
| *Network Security Manager Getting Started Guide for SaaS* | Describes how to license and configure a basic SaaS NSM instance. | Read this document to learn how to license and configure a SaaS instance of NSM. This document applies to SaaS instances only. |
| *Closed Network Feature Guide* | Describes how to deploy NSM on a closed network. | Read this document to learn how to set up on-premises NSM in an environment that has no external network connections. This instance operates in a closed network. This document applies to On-Premises instances only. |
| *NSM Release Notes* | Summarizes the new features for the product and provides information on the closed and resolved issues. | Read this document to review the list of resolved and known issues for this release. This document applies to both SaaS and On-Premises instances of NSM. |

To access the NSM documentation, navigate to the Technical Documentation portal.

# 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.

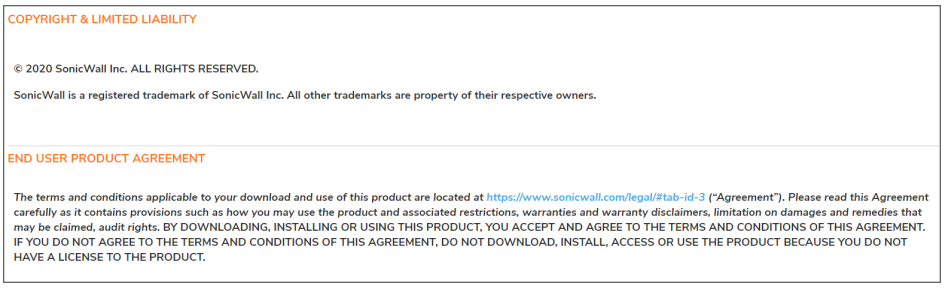
In the **SONICWALL END USER PRODUCT** section, links to the *NSM API Specification* and the *SonicOS API Specification* are provided. Do not download, use or install the APIs if you do not agree to the terms of the End Product User Agreement.

# 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. |
| *`<Computer code italic>`* | Represents a variable name when used in command line instructions within the angle brackets. The variable name and angle brackets need to be replaced with an actual value. For example, in the segment *serialnumber=<your serial number>*, replace the variable and brackets with the serial number from your device: serialnumber=C0AEA0000011. |
| ***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.

**To Reviewers:** Validate that these icons are still used and defined properly.

| Status Icon | Definition |
|---|---|
|  | Indicates that a process is in progress. In some instances, specific details are provided: for example, Requesting Licenses. |
| | Indicates that a process has completed successfully. May provide the message Success or something with more detail like Device parameters set up in Cloud Capture Security Center complete. |
| | Indicates that a task is in process or pending the completion of another task. The message Pending is usually displayed, as well. |
| | Indicates a potential issue. Messages provide additional detail to help you resolve the issue. |

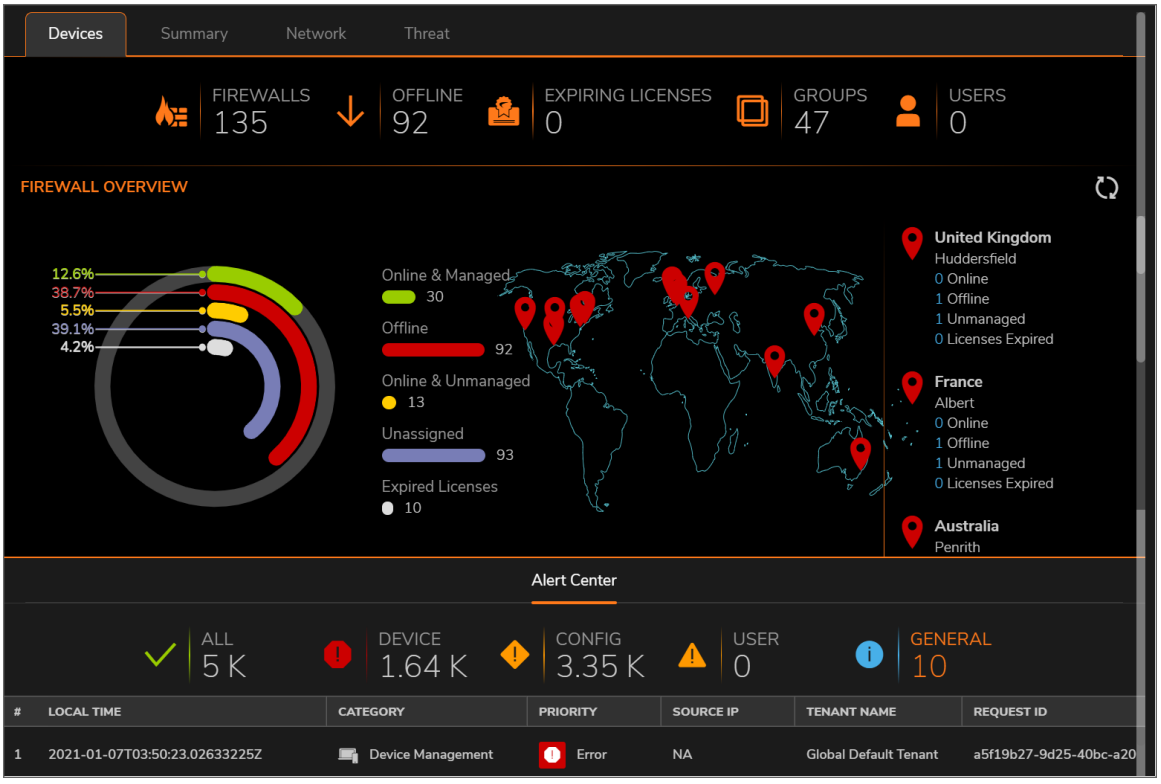
| Status Icon | Definition |
|---|---|
| | Indicates an error. Additional information may be provided via an information icon. Click the icon or mouse over it to see the message:<br><br>For example, Gateway Firewall is not available in CSC. |
|  | Indicates an unknown status. |
| | Indicates the device is online. |
| | Indicates the device is offline. |
| | Indicates the device is unmanaged. |
| | Indicates the device is managed. |

2

# 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.




**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:

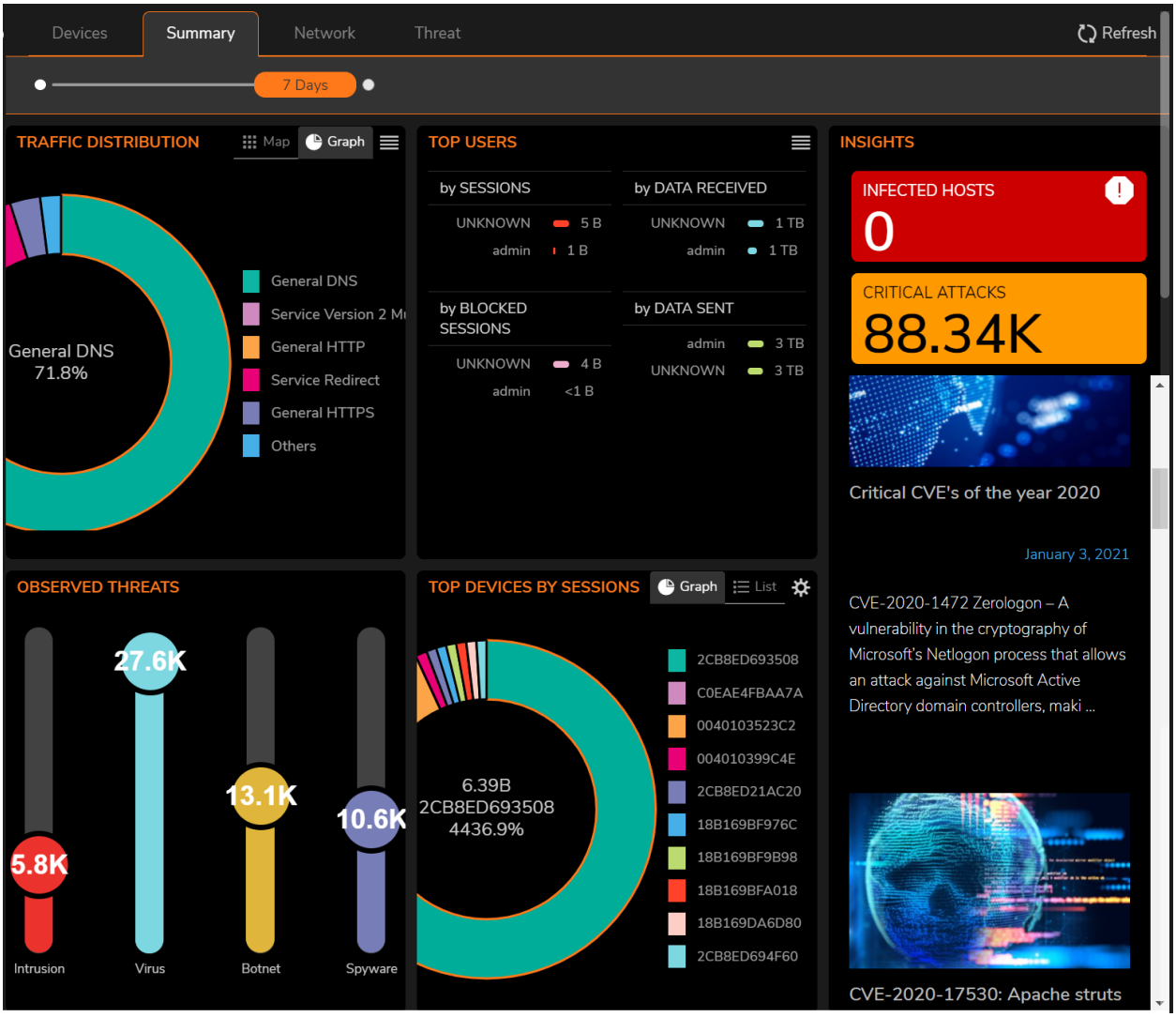
- **FIREWALLS**: Displays the number of firewalls that you intend to manage through NSM. Click **FIREWALLS** to list all the firewalls in the **Inventory** page.
- **OFFLINE**: Displays the number of firewalls that are offline. Click **OFFLINE** to list the offline devices in the **Inventory** page.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

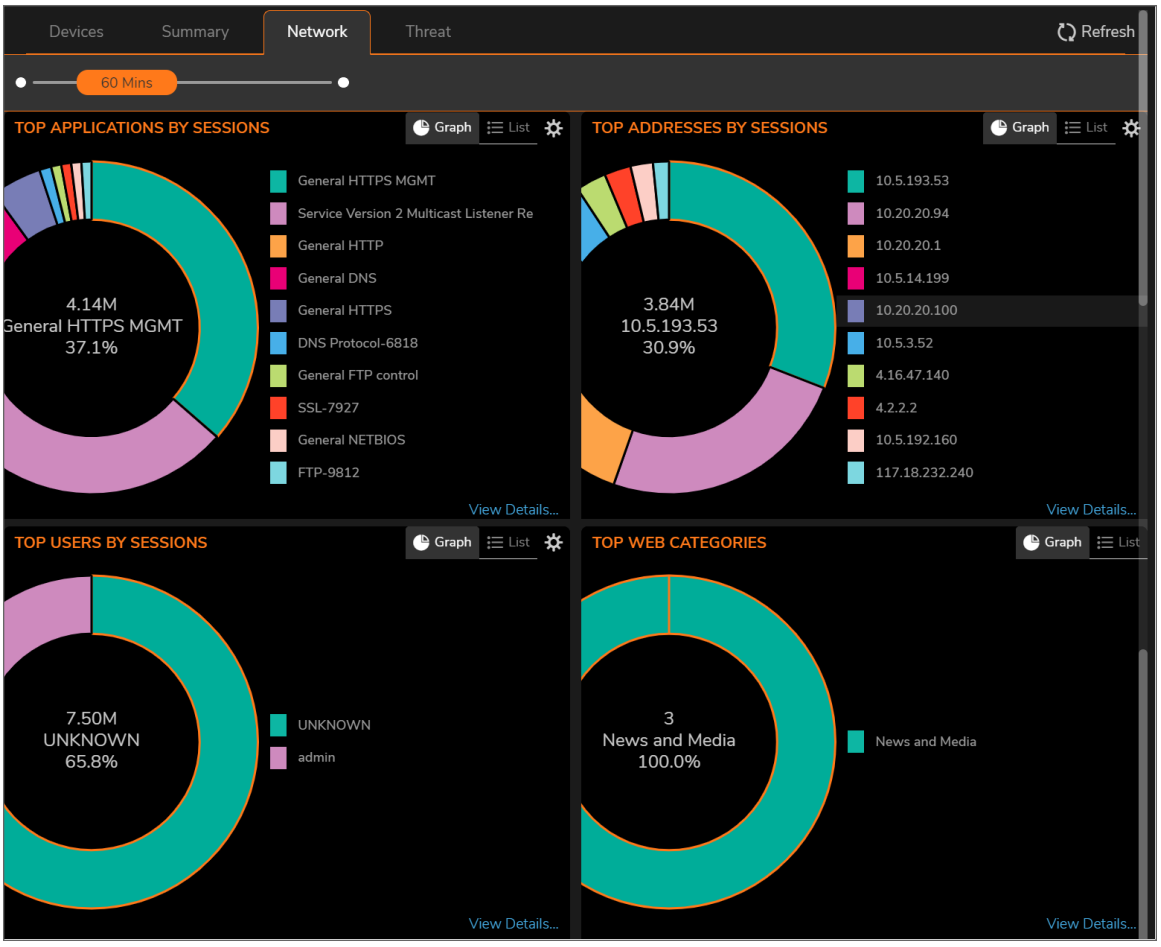



- **TRAFFIC DISTRIBUTION**: Shows the graphical representation of the percent distribution of the number of network sessions based on protocol.
- **TOP USERS**: Shows the top users by the number of sessions, amount of data received, amount of data sent, and the number of blocked connections.
- **OBSERVED 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.



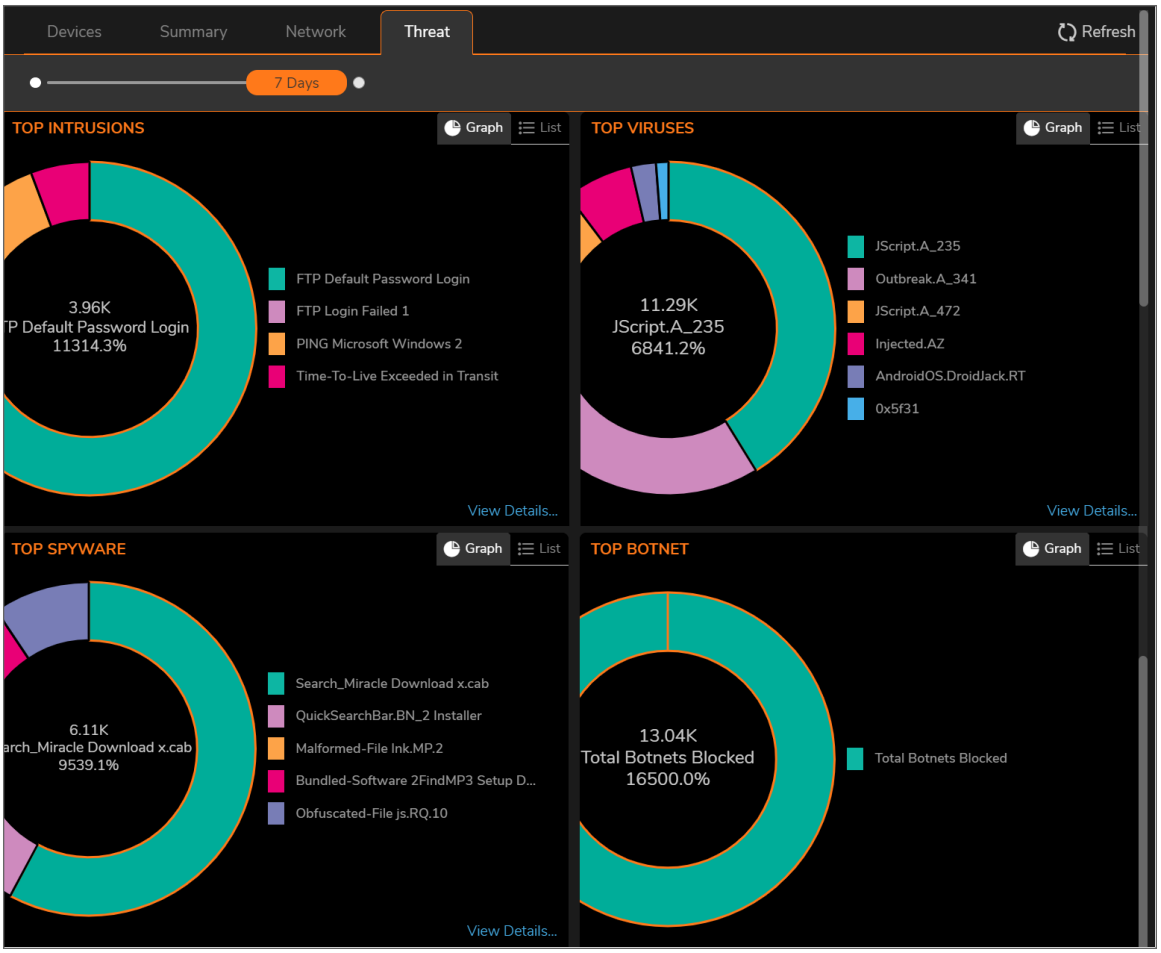

The following data is displayed on the Network page: types of applications that run in your infrastructure; IP addresses that initiate sessions; users that initiate sessions; web categories; and countries from which connections are initiated. Each space enables you to filter the data with available options.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

**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.

3

# Firewalls

The Firewall command set includes the following: POp

- Device Inventory
- Device Groups
- Backups

# 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**.

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.

ⓘ **NOTE:** There will be a delay while updating the device status if you have not migrated your firewall to Instant Connect. See Zero Touch Status

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.

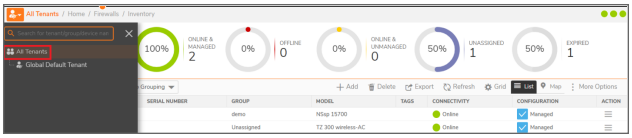
The menu bar below the Firewall View lets you to search using the Keyword and Group By from the available options in the drop-down list.

- **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.

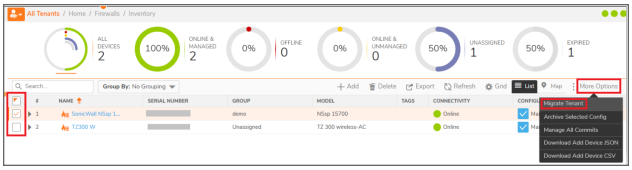
- **Add** : The Add icon lets you to Add Device and Import Add Device File. Click **Add Device** and input Serial number, IP Address, User name and Password. To import device, click **Add Device** File and choose the files. Only xml,csv and json file types are supported.
- **Delete** : Select any device 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 Selected Config**.
    - **Download Add Device JSON** files to your local machine.
    - **Download Add Device CSV** files to your local machine.
    - **Migrate Tenant** from **All Tenants** to any specific tenant group.
      ⓘ | **NOTE:** This option is available only for **All Tenants** group.

      ***To migrate a tenant:***

      1. Select **All Tenants**.

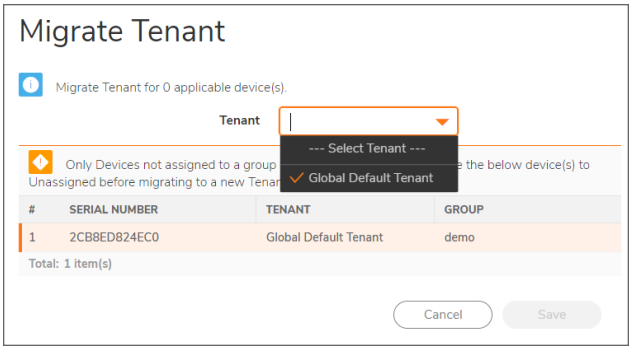
      

      2. Select the firewall you want to migrate.
         ⓘ | **NOTE:** Only devices which are not assigned to a group can be migrated.
      3. Click **More Options > Migrate Tenant**.

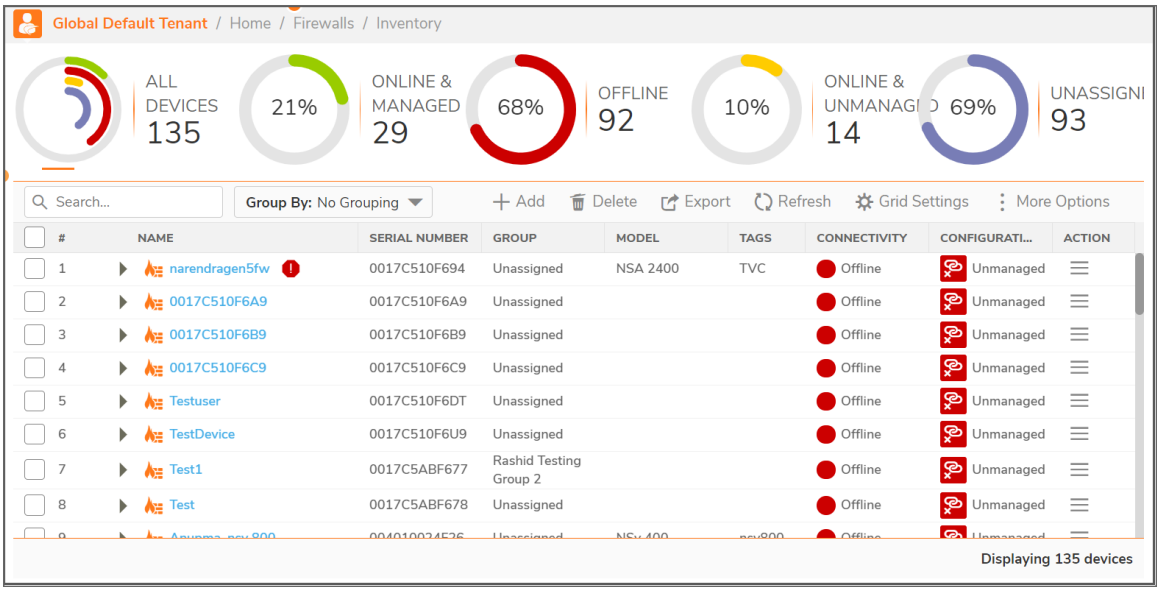
      4. Select the **Tenant** from the drop-down to which you want to migrate.

5. Click **Save**.

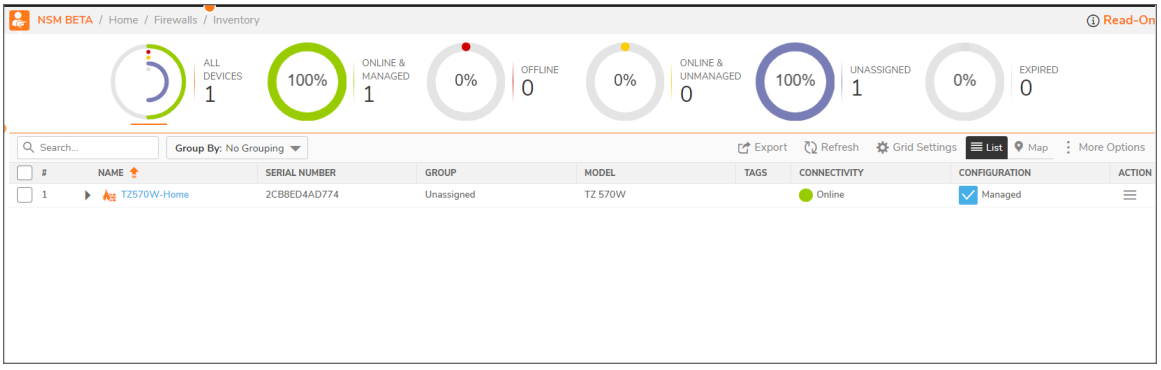



**NOTE:** The **Add** and **Delete** options are only available for **NSM On-Prem** and not for **NSM SaaS**. For NSM SaaS, the Add and Delete options are available through MySonicWall.com.

**NSM On-Prem Interface:**




**NSM SaaS Interface:**



The following information is displayed for each firewall when you click the arrow next to the Firewall name:

- **Management Status**
  Details of the Management status, such as: Connectivity, Configuration, Acquired, Zero Touch.
  - **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.
  - **Acquired** : Displays whether the device is acquired.
  - **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.
- **System Details** : Details of the firewall, such as: **Model**, **Serial Number**,**Friendly Name**, **Group Name**—Device Group, if the firewall belongs to any,**Tenant Name**—Tenant to which the appliance is registered to, **Firmware Version** that runs on the firewall, **Last Modified By**, if the details are modified.
- **License Details** : Lists the license details. You need to register the firewall in www.mysonicwall.com and activate NSM license to view the information.
- **Analytics and Reporting Status** : Provides the details of Flow Management, such as, Remote IP, Firewall Settings, Flow Forwarder, Flow Agent, and AnalyzerNG.
- **Templates and Firmware Versions** : The templates applied to the firewall, if any. The firmware version that runs on the firewall.
- **High Availability** : Provides information of the High Avaliability mode, Primary and Secondary device.

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:

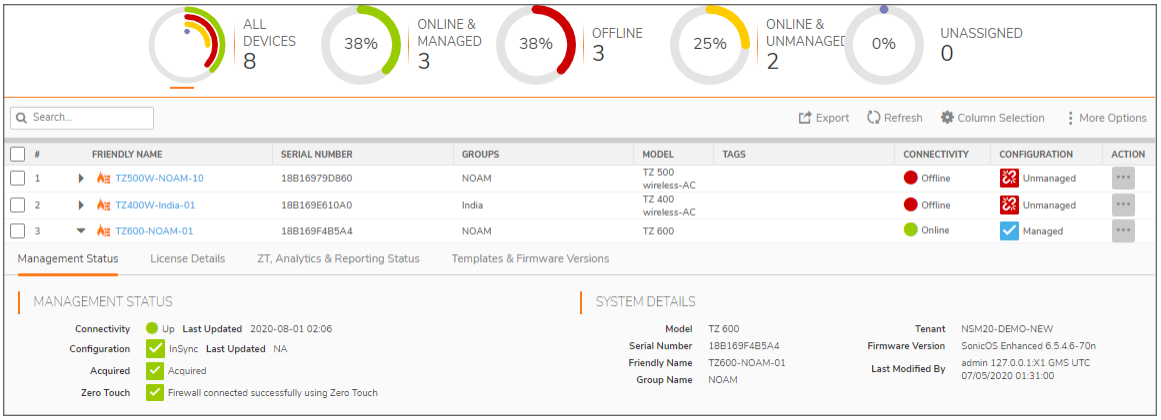
- **Access Firewall View**: Click **Switch to Firewall View** to access firewall management interface. For information on how to perform configuration changes to a firewall, see SonicOS documentation.
- **Edit Settings**: Click **Edit Settings** to edit settings of the firewall. For information on editing 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 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**.




**Topics:**

- Management Status
- System Details
- Templates Applied
- License Details
- Template and Firmware 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.<br>• **Up**(green icon)— NSM can reach firewall.<br>• **Down**(red icon)— NSM cannot reach firewall. |
| **Configuration** | Status of synchronization of firewall configuration with NSM.<br>• **Green icon**—Synchronization successful<br>• **Red icon**—Synchronization failed |
| **Acquired** | Status of firewall acquisition by NSM.<br>• **Green icon**—Acquisition successful<br>• **Red icon**—Acquisition failed<br>• **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.<br>• A **gray** icon indicates Zero Touch feature was disabled.<br>• A **red** icon indicates that the Zero Touch connection failed.<br>• A **yellow** icon indicates that the system is waiting for a Zero Touch connection from the firewall.<br>• 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. |

| Term | Definition |
|---|---|
| **Group Name** | Device group, if the device belongs to any group. |
| **Tenant** | The tenant to which the firewall is registered to. |
| **Firmware Version** | The SonicOS version that runs on the device |
| **Last Modified By** | User that modified device configuration the last time. |

# 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.

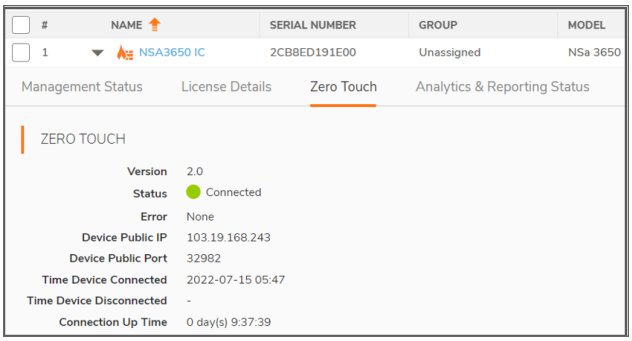
The list of licenses is given here:

- Global VPN Client
- SSL VPN
- Botnet Filter
- Nodes/Users
- 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)
- SonicOSX Expanded
- DPI-SSL Enforcement
- 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

# 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.




## VERSION 2.0

Zero Touch 2.0 (also known as Instant Connect) is a new microservices-based architecture to simplify on-boarding of firewalls and establish a reliable connectivity between NSM and firewall. With the new architecture, there is no change in the ports used for communication between NSM and firewall.

### ZEROTOUCH STATUS

| Term | Description |
|---|---|
| **Status** | Status of Zero touch 2.0 between firewall and NSM |
| **Error** | Displays any error with the status of connection. |
| **Device Public IP** | The IP address of the device. |
| **Device Public Port** | Port number of the device. |
| **Time Device Connected** | Time at which zero touch connection is initiated and firewall is connected with NSM. |
| **Time Device Disconnected** | Time at which zero touch connection drops and firewall is disconnected from NSM. |
| **Connection Up Time** | Total time at which the connection is active. |

## Template and Firmware 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.

# Managing Devices

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

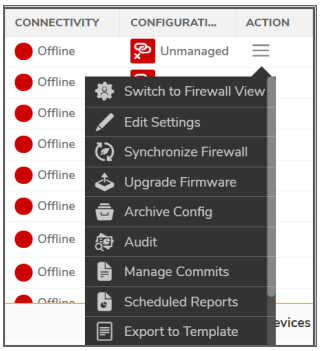
**Topics:**

- Editing Device Settings
- Multi-device Firmware Upgrade
- Upgrading Firmware
- Synchronizing Firewall Configuration with NSM
- Creating Backup of Device Configuration
- Manual Firewall Acquisition

## Editing Device Settings

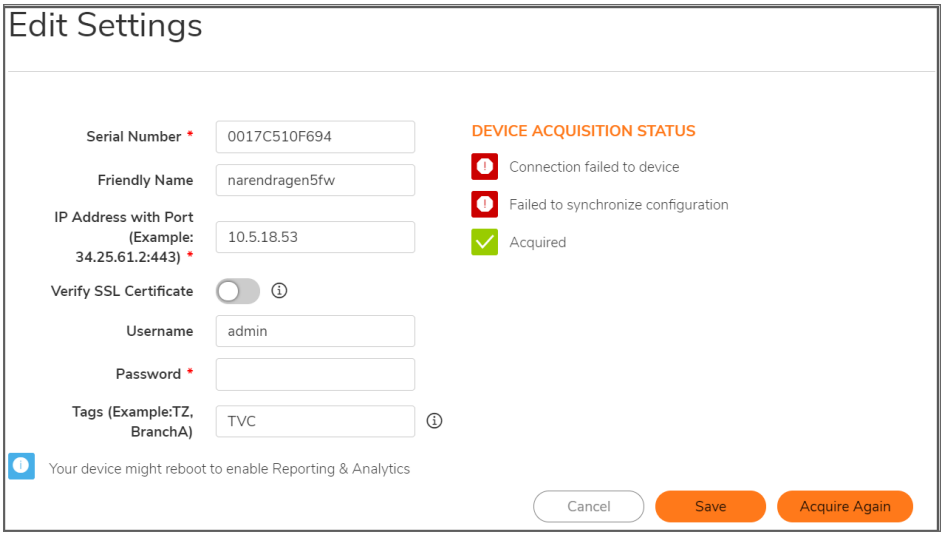
***To edit settings of a device:***

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`.



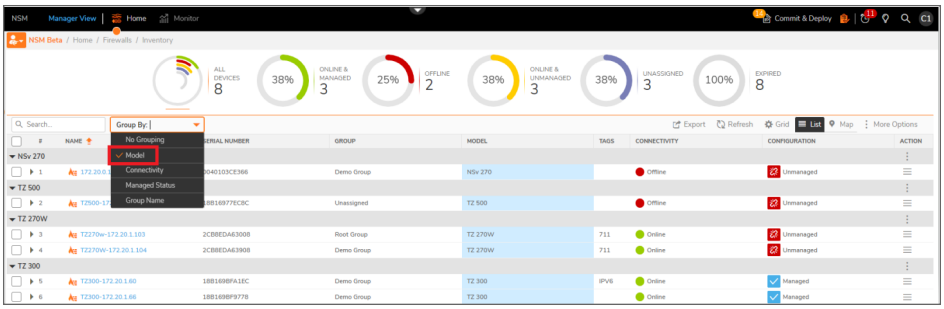

4. Click **Save**.

# Multi-device Firmware Upgrade

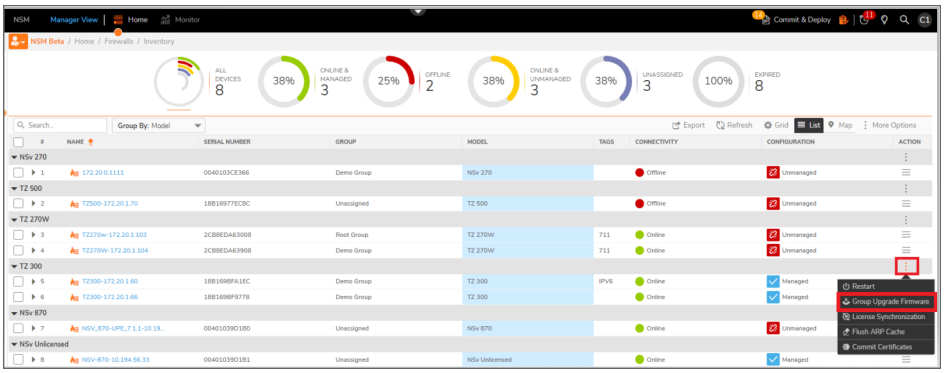
You can now upgrade multiple firewalls from a group of devices in a single action. This action is applicable to a maximum of 15-20 devices at once.

***To perform group upgrade of devices:***

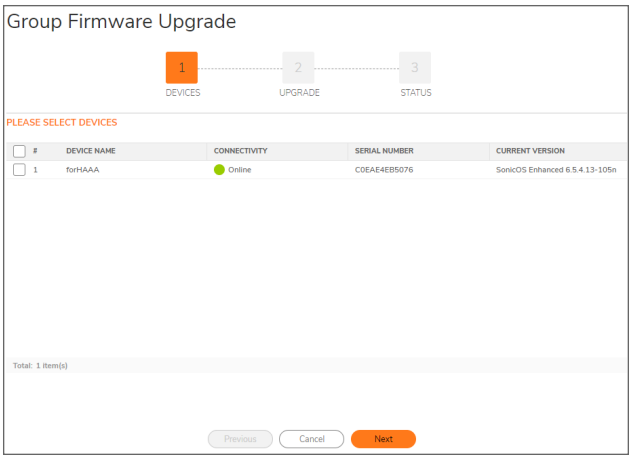
1. Navigate to **Manager View | Firewalls > Inventory** page.
2. Select **Model** from the drop-down for **Group By**.



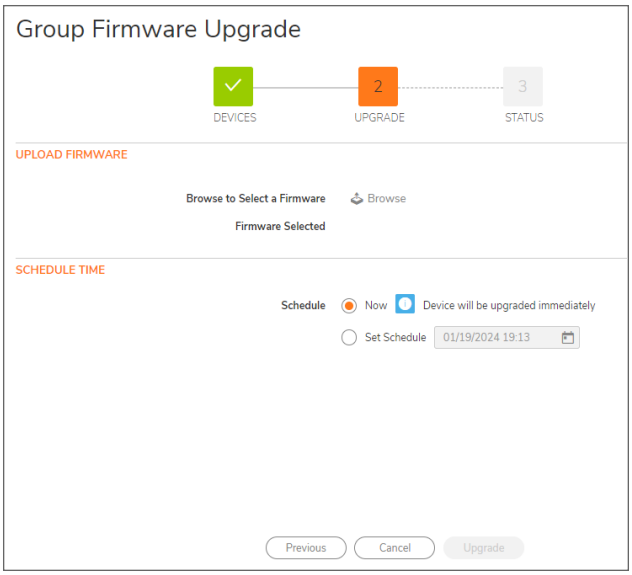

3. Select the three dots in the **ACTION** column for the group of devices you want to upgrade and select **Group Upgrade Firmware**.




4. There are 3 steps to perform upgrade. Select the devices in the group by checking the box. Click **Next**.




5. Under **UPLOAD FIRMWARE**, click **Browse** and select the firmware .
6. Under **SCHEDULE TIME**, select either
    a. **Schedule Now** - Choose this to upgrade instantly.
    b. **Set Schedule** - Set a future date to upgrade.
7. Click **Upgrade**.

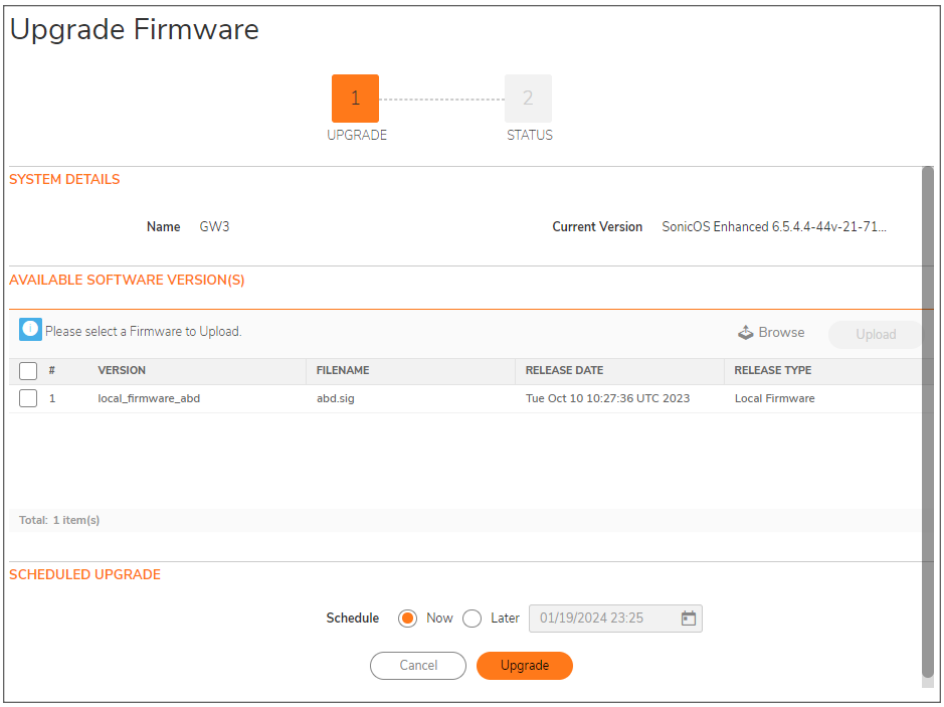



# Upgrading Firmware

***To upgrade firmware on a firewall:***

1. Navigate to **Manager View | Firewalls > Inventory** page.
2. Click **Ellipses** icon in the **ACTION** column for the device you want to upgrade firmware for, and then select **Upgrade Firmware**.

   The **Upgrade Firmware** dialog is displayed.



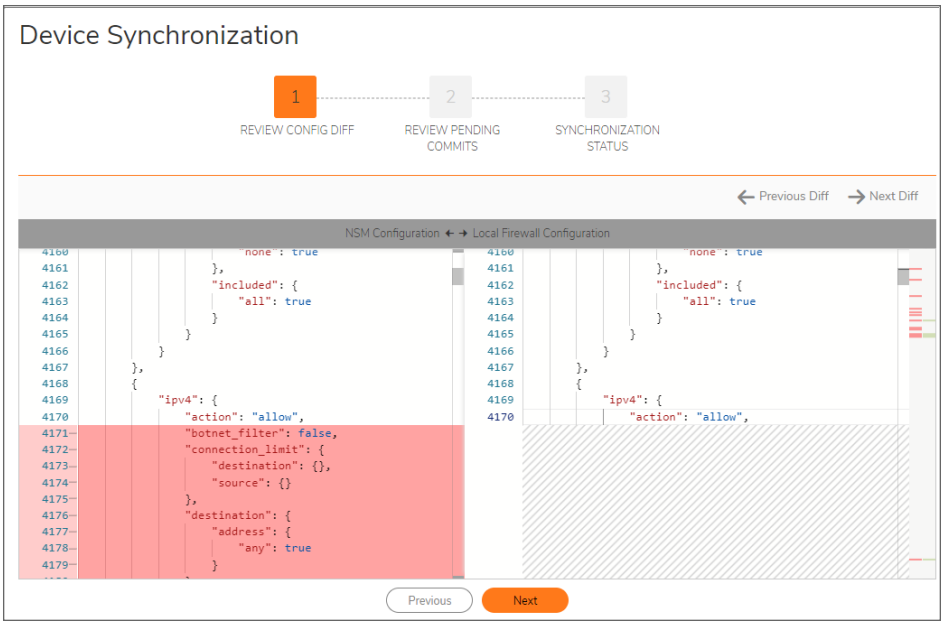

3. Do one of the following:
    - **To upgrade to any available version on your Local system**:
        1. In the **AVAILABLE SOFTWARE VERSION(S)** section, click **Browse** and select the swi file in your system.
        2. Click **Upload**.
    - **To upgrade to any available version instantly**:
        1. In the **AVAILABLE SOFTWARE VERSION(S)** section, select the required software version from the list.
        2. In the **SCHEDULED UPGRADE** section, select **Now** to instal immediately.
        3. Click **Upgrade**.
    - **To schedule software upgrade**:
        1. In the **AVAILABLE SOFTWARE VERSION(S)** section, select the required software version from the list.
        2. In the **SCHEDULED UPGRADE** section, select **Later** to schedule a time.
        3. Click **Upgrade**.

# Synchronizing Firewall Configuration with NSM

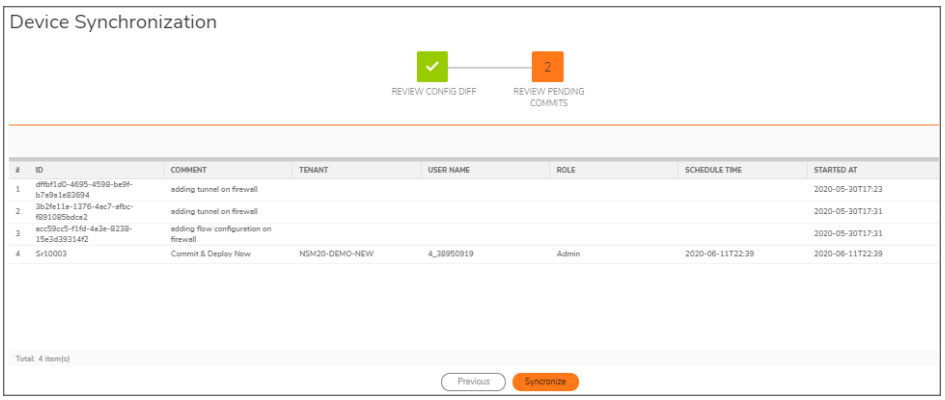
The management status of a firewall changes to **Unmanaged** state when the firewall is locally modified. You need to synchronize firewall configuration with NSM to set the device in **Managed** state.

***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.

# 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 **Home | 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 **Create Backup Configuration**.
4. Click **OK** to confirm.

***To validate the backup:***

1. Navigate to **Home | 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.

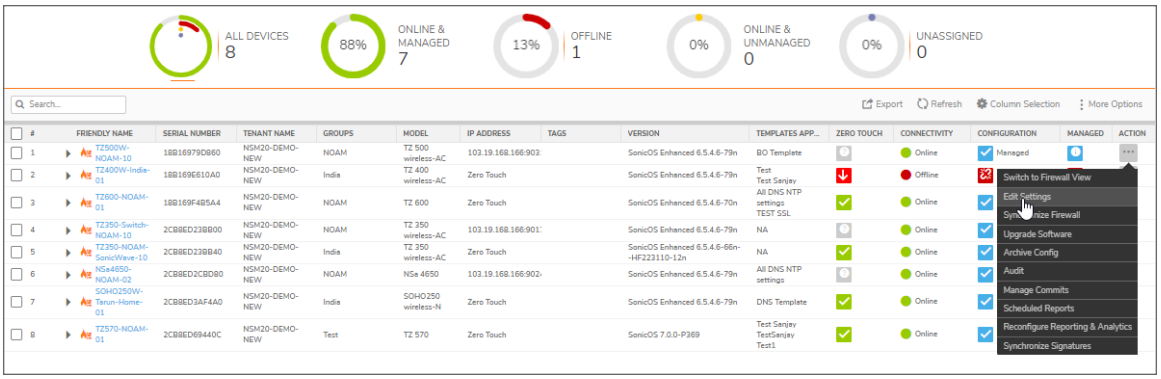
# Manual Firewall Acquisition

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

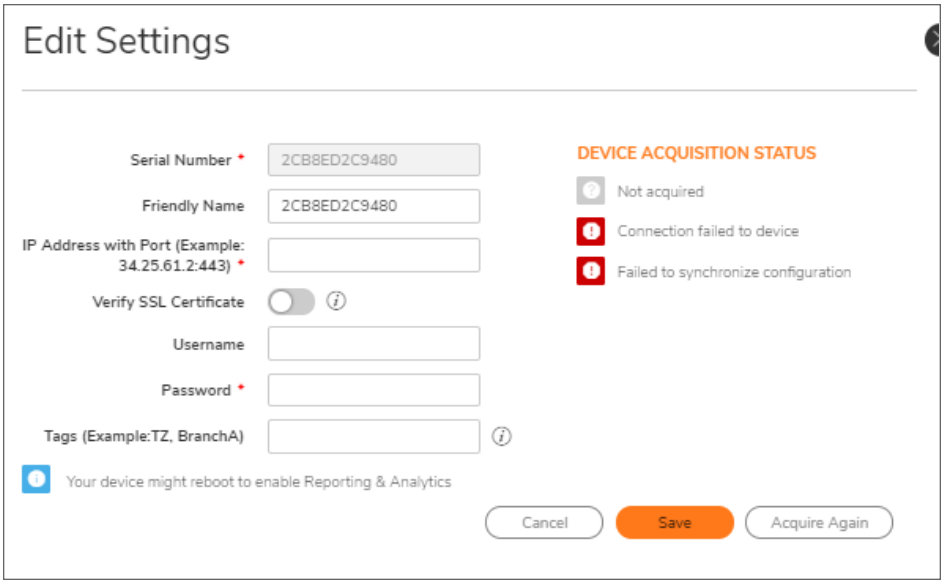
ⓘ **NOTE:** When acquiring manually, **SSL cert verify** is enabled by default. This is set as a security feature, but if proper SSL certification is not enabled on the firewall, the firewall does not get acquired.

***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**.



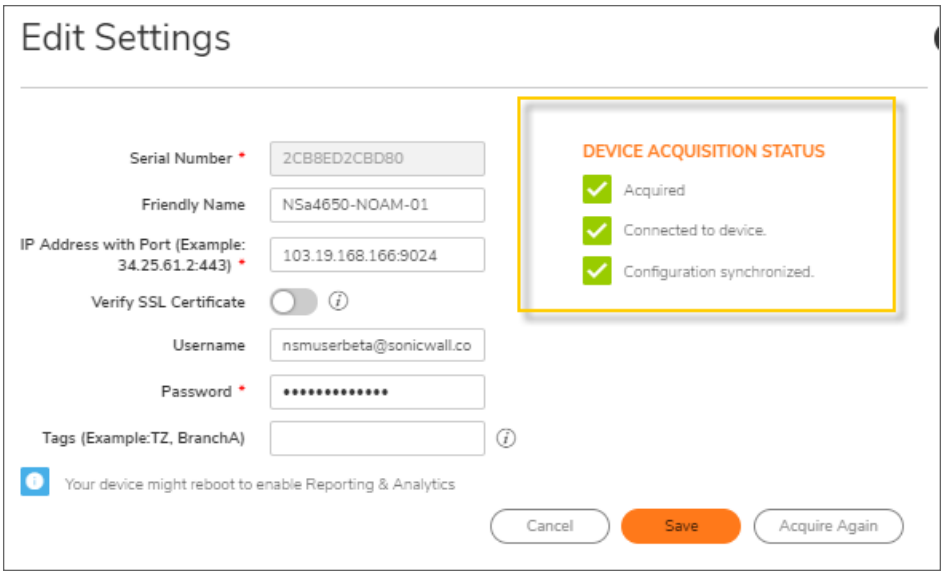

3. Enter **IP Address with Port** for your device.
4. Enter your **Username** and **Password** of your NSM user account.




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 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.



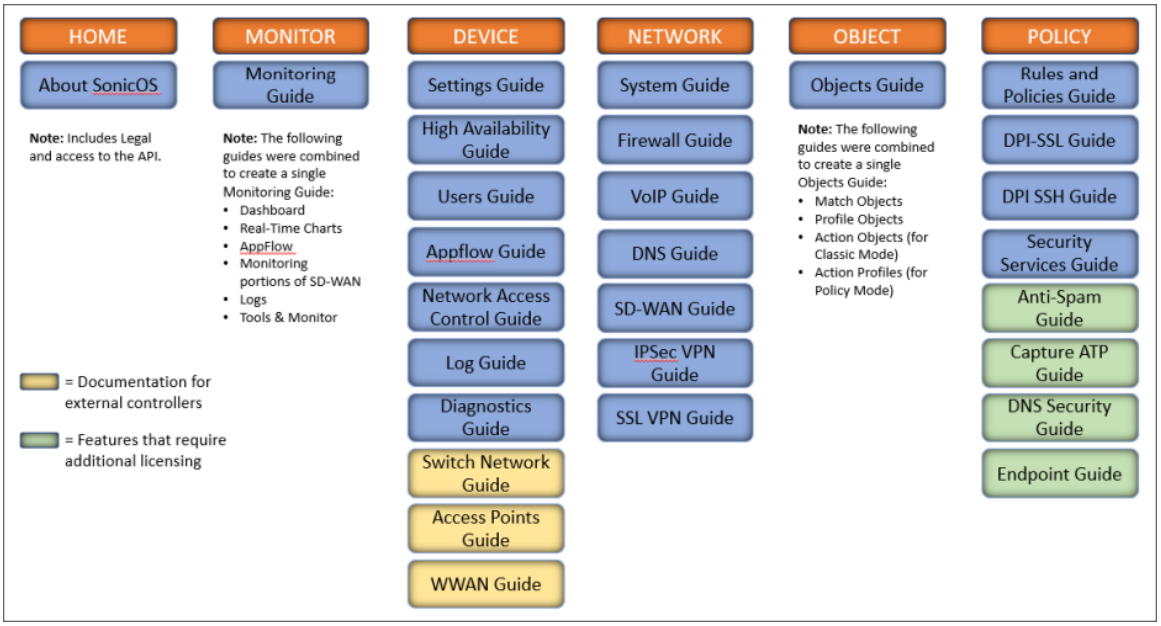

# Firewall View

The **Firewall View** of NSM, allows to perform advanced functions on the firewalls.

The tabs in Firewall View are described in details under the SonicOS Administration Guide.

The SonicOS Administration Guide is a collection of guides that detail the features represented by each of the main menu items in the Firewall View. Within each guide, you can find topics covering commands in that menu group, along with procedures and in-depth information.

To help you understand how the books align with the features and commands, the following figure shows the books organized like the Firewall View interface.

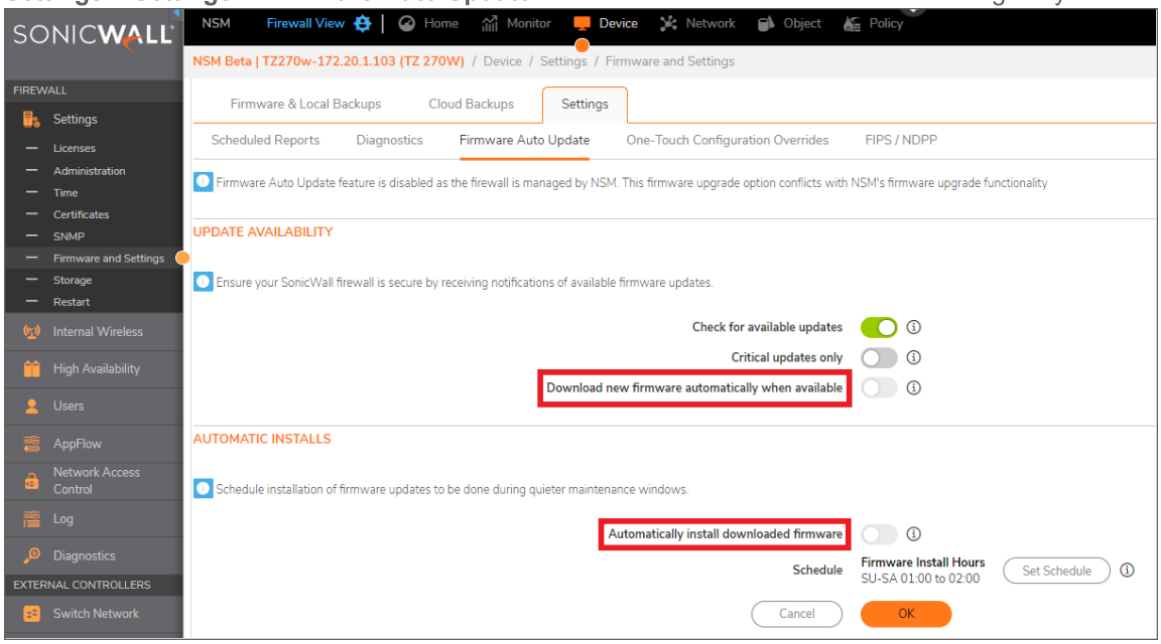



The SonicOS Administration Guides, along with related documentation are available on the https://www.sonicwall.com/support/technical-documentation/.

***To access the Firewall View:***

1. Navigate to **Firewall > Inventory**.
2. Click on the firewall for which you want to access the **Firewall View** for.

**NOTE:** The Firmware Auto Update feature present in SonicOS 7.1 and above can conflict with the Upgrade Firmware feature available in NSM. To avoid, these conflicts, **Download new firmware automatically when available** and **Automatically install downloaded firmware** options under **Device > Firmware and Settings > Settings > Firmware Auto Update** are disabled in NSM if the device is managed by NSM.




# 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. |

| Term | Description |
|---|---|
| **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.<br>• **Up**—Firewall is healthy.<br>• **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.<br>• **Green icon**—Device acquisition was successful; firewall is being managed through NSM.<br>• **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:**

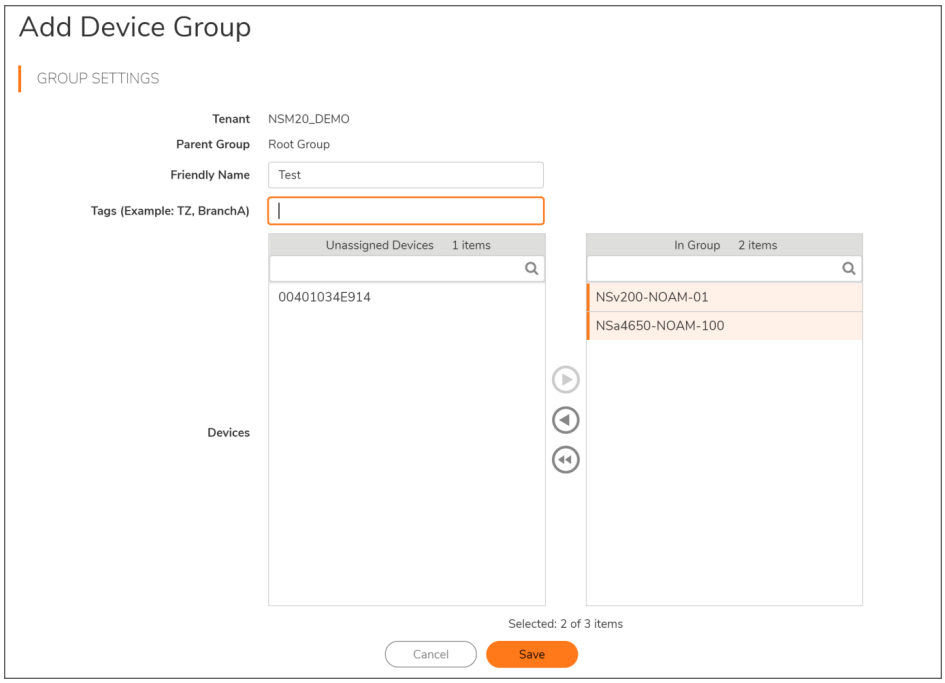

- Creating Device Groups
- Editing Device Groups
- Creating Backup of Device-Group Configuration
- Deleting Device Groups


# 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**.




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.

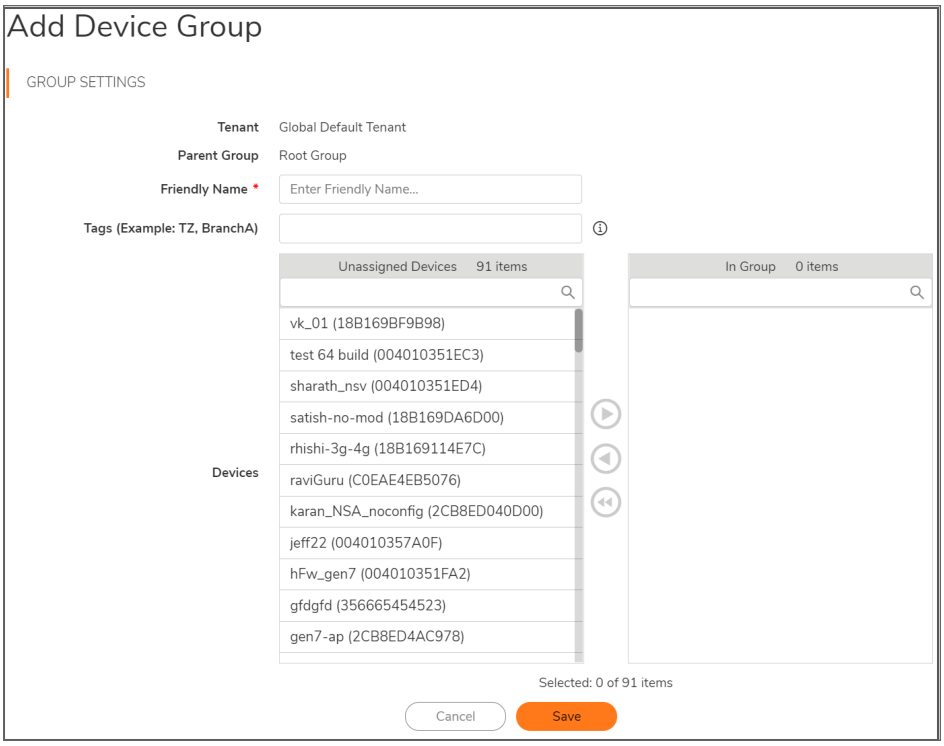
# Editing Device Groups

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:***

ⓘ | **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.




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.

   ⓘ | **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.

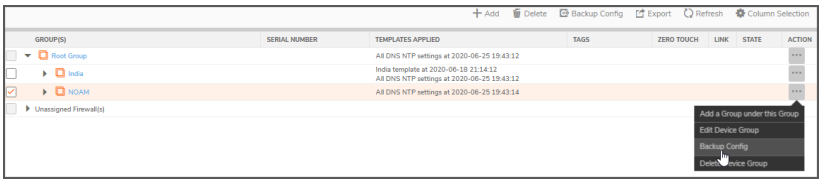
   ⓘ | **NOTE:** When you add a device to a group that already has a template applied to it, the template configuration is made available to the newly added device and therefore you need to commit and deploy the available updates on to the device.

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

ⓘ **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**.

ⓘ **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**.

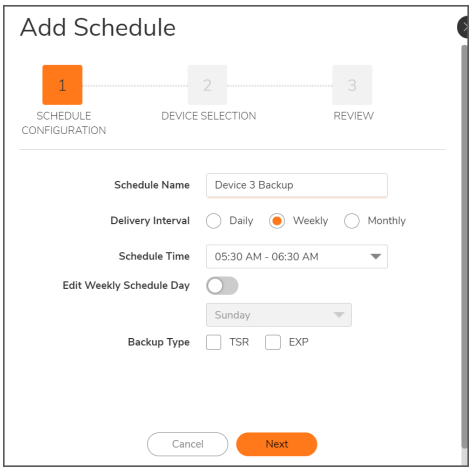
# Backups

NSM backup enables you to backup the devices configuration. You can schedule the backup daily, weekly or monthly depending on the changes that are made to the firewall.

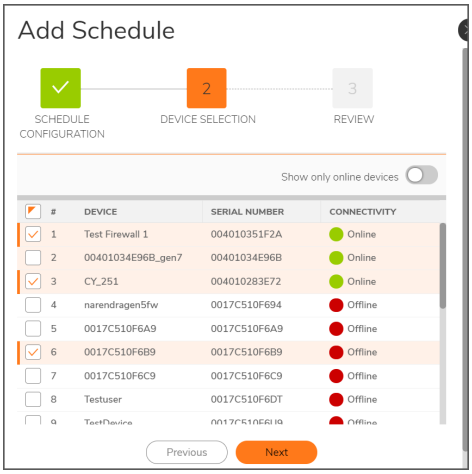
To create a backup of the device configuration:

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

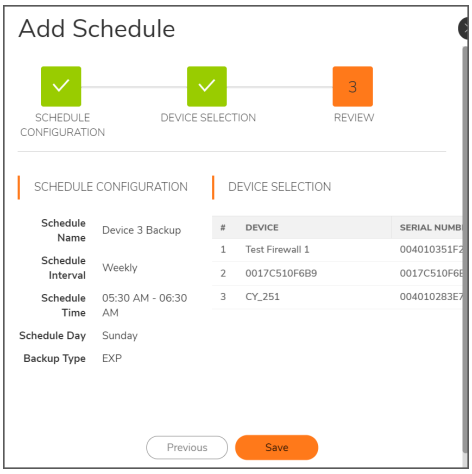
click **Next** to proceed to Device Selection screen.




**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.




**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.

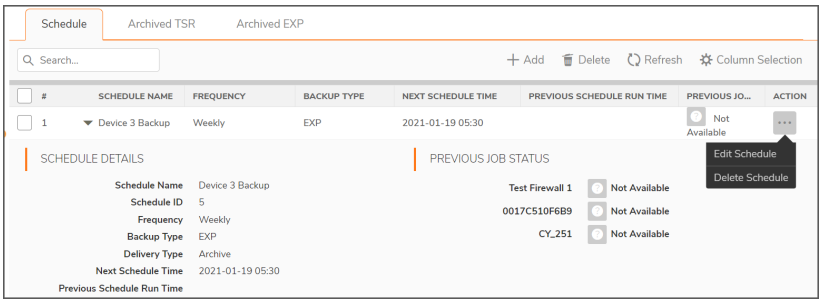



3. Click **Delete** icon to delete any selected schedule from the list.
4. **Refresh** icon refreshes the list
5. Column Selection allows to choose which options can be displayed in the schedule by checking the box.

# Scheduling Backups

This section lists all the created backup schedules. To know, how to add schedule, refer 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**.



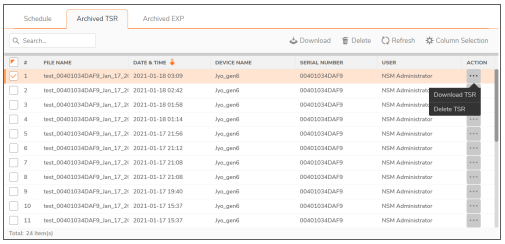

3. **Delete Schedule** deletes the selected item.

# 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, refer Creating 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.



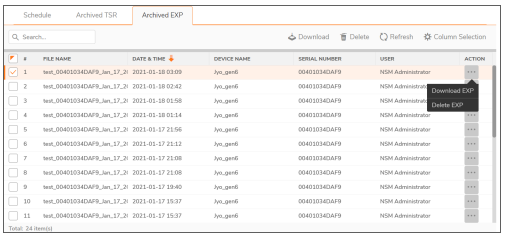

**Download TSR** option downloads the selected TSR to a zip file in *.txt* format.

# 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, refer Creating 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.




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

4

# Templates and Variables

Templates allow you to effectively deploy and manage common configurations across firewalls. When used with the Template Variable you can create variable objects during template configuration and assign firewall specific parameters within a Template configuration

**Topics:**


- Templates
- Golden Template
- Variable Data


## Templates

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.

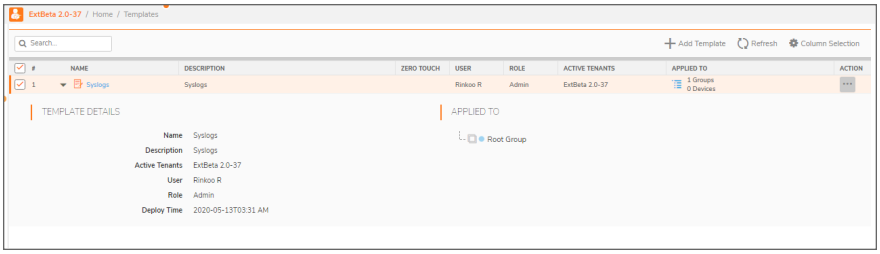
**Topics:**


- Templates Inventory
- Creating Templates
- Editing Templates
- Viewing Template Configuration
- Creating Duplicate Template
- Modifying Template Attributes
- Applying Templates
- Deleting Templates
- Storage

# 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.

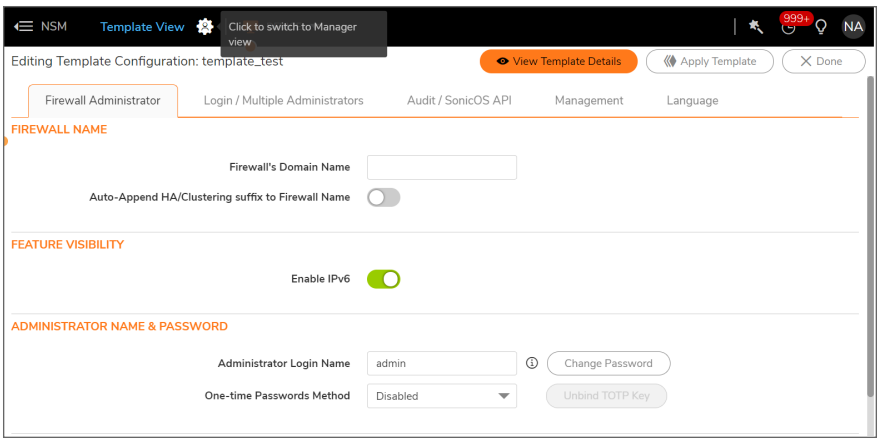



The following details are displayed for each template listed on the Templates page:

### 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.<br>• **Enabled**: The template configuration is auto-deployed on to the target zero-touch devices when applied.<br>• **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.




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 SonicOSor SonicOS. 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

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

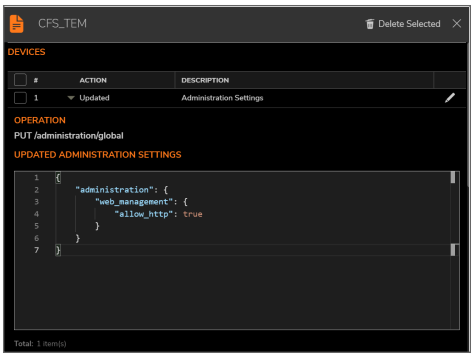
***To define or edit a template:***

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**.
   **NOTE:** While deleting object from template, NSM performs depedency check to ensure object is not used in any 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.

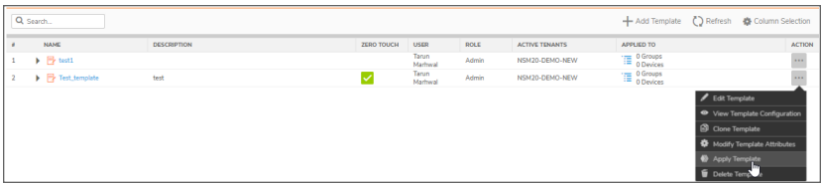
# Applying Templates

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.

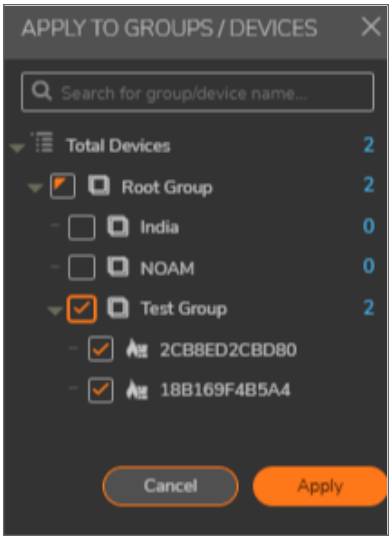
***To apply a template:***

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.

   **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.



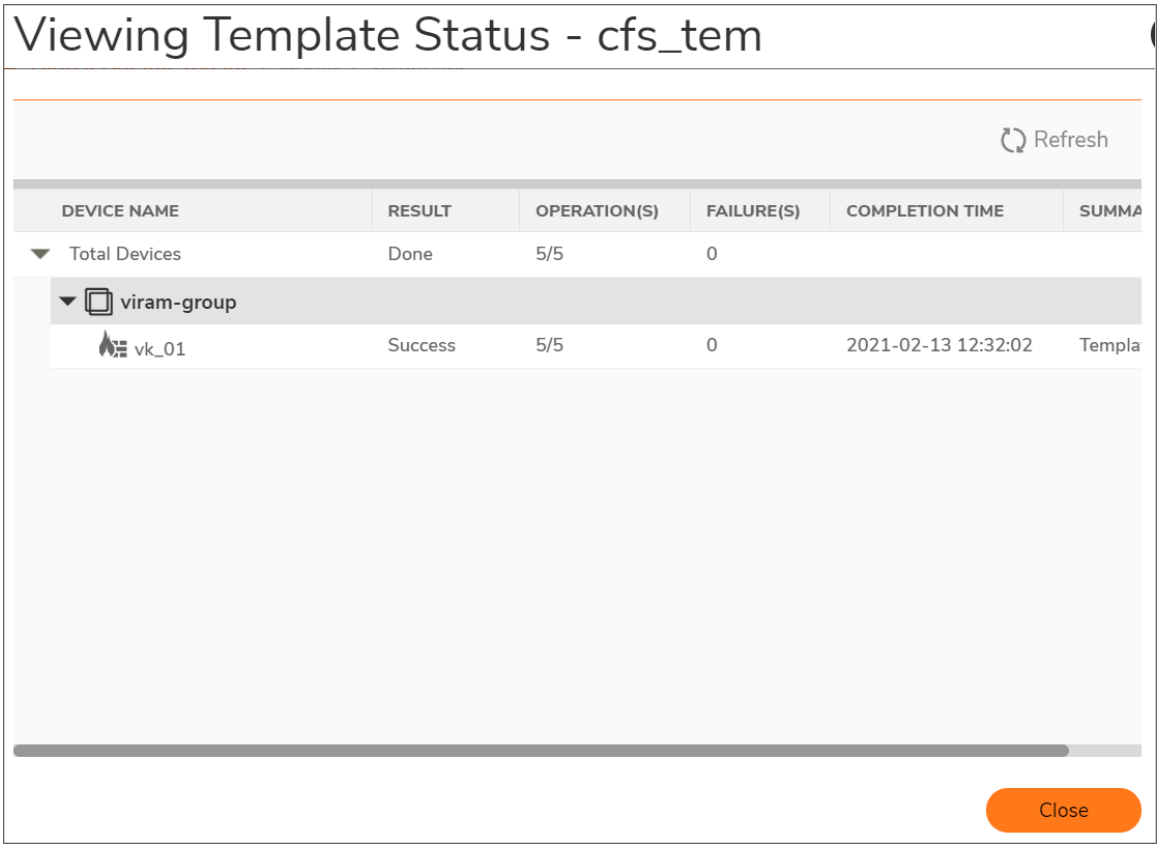

4. Click **Save**.

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.**




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

# Deleting Templates

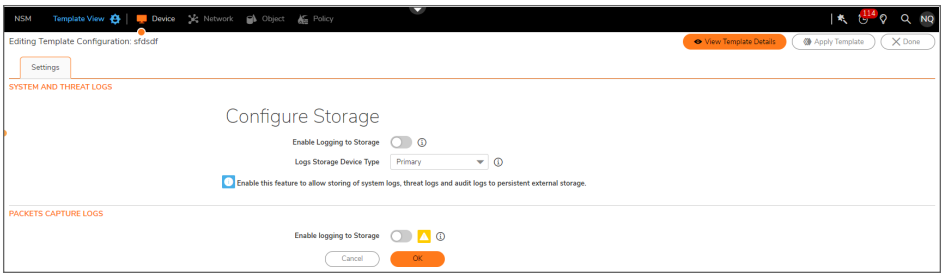
ⓘ **NOTE:** By deleting a template associated with devices, you cannot perform configuration rollback on the target group(s) and device(s).

***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**.

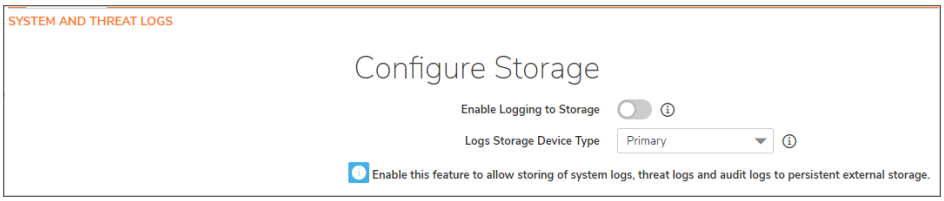
# Storage

The **DEVICE | Settings > Storage** page on the **Template View** allows you to enable the storage options for the System and Threat Logs as well as the Packet Capture Logs.

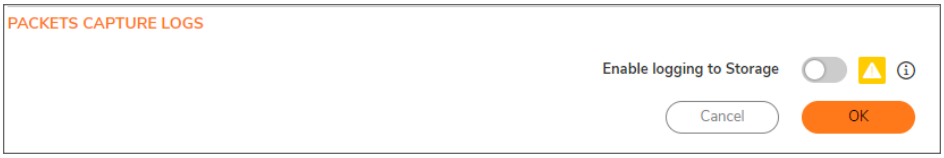



***To enable storage settings:***

1. Navigate to **Template View > Device**.
2. Click on the **Storage** tab under **Settings**.
3. Configure the following options under System and Threat Logs:
   - Enable the **Enable Logging to Storage** for storing system logs, threat logs, audit logs, and AppFlow report data to the External Storage.
   - Select **Primary** or **Secondary** from the **Logs Storage Device Type** drop-down.




4. Enable the **Enable Logging to Storage** option under Packets Capture Logs.



5. Click **OK**.
6. Click on **Apply Template** to apply the storage settings to the template.

ⓘ | **NOTE:** Enabling **Enable Logging to Storage** requires a reboot for the changes to take effect.

# Golden Template

Golden configuration template can be used to increase the operational efficiency and minimize configuration errors. Customers with large no of tenants and firewalls (Distributed enterprises and MSSPs) can convert a gold standard device configuration into a template which could be applied to the new devices. The administrator can select a device from the firewall inventory page and export its configuration as a golden template.

**Topics:**


- Preparing the Firewall
- Exporting the Firewall Configuration into Template
- Editing Golden Template
- Applying Template to Device Groups or Devices
- Committing and Deploying the Updates


# Preparing the Firewall

Before exporting the firewall configuration into the golden template you must ensure the following prerequisites:

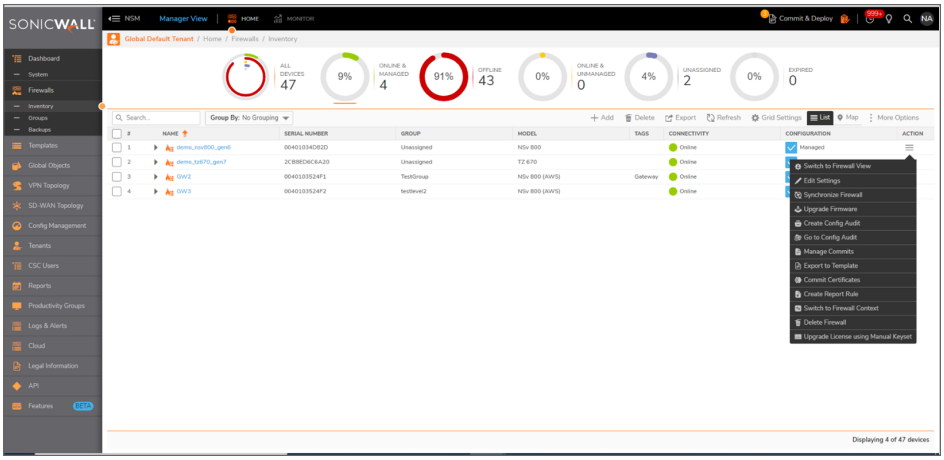
- The source and target device model must be running on the same operating system for successful deployments:
  - If you are exporting a template from Gen6 device, then it is not supported to Gen7 device.
  - If you are exporting a template from SonicOS, then it is not supported to SonicOSX.
- Licenses on both source and target firewalls are same.
- The target firewalls are factory reset.
- Create device group structure as per the requirement of the organization.
- Add unassigned devices to the corresponding groups on which the template is going to be applied.
- Ensure that the source firewalls and target firewalls are in **Managed** state in NSM. If not, then you need to synchronize the firewall before exporting, using the **Action** column.

  ⓘ | **NOTE:** It is recommended that you force synchronize the source firewalls which will be exported after upgrading or using a new NSM release. Otherwise, the bug fixes and improvements on the firewall management inside NSM will not be reflected.

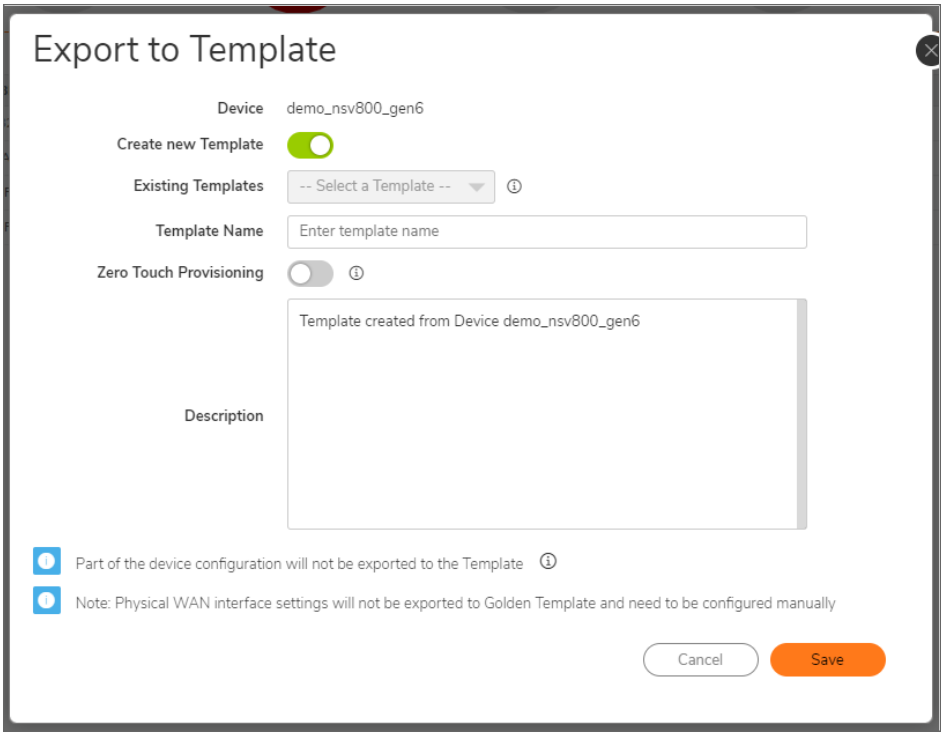
# Exporting the Firewall Configuration into Template

***To export firewall configuration into golden template:***

1. Navigate to **Manage View > Firewalls > Inventory**.
2. Choose a firewall and click on **Export to Template**.




3. On the **Export to Template** dialog page, enter the **Template Name**.



4. 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 Provisioning option. Offline devices will be updated once they come online.
5. Enter a valid **Description**. This is an optional requirement.
6. Click **Save** to successfully export the firewall configuration into the golden template.

   ⓘ **NOTE:** Only the custom objects are exported to the template configuration. This helps you to exclude default configurations and successfully deploy other essential custom objects to factory default firewalls.

   ⓘ **NOTE:** The following configurations will not be exported to the template:

   - Time
   - VLAN Translation
   - Routing

# Editing Golden Template

After successfully exporting the firewall configuration into the golden template you will be automatically directed to the Template page.

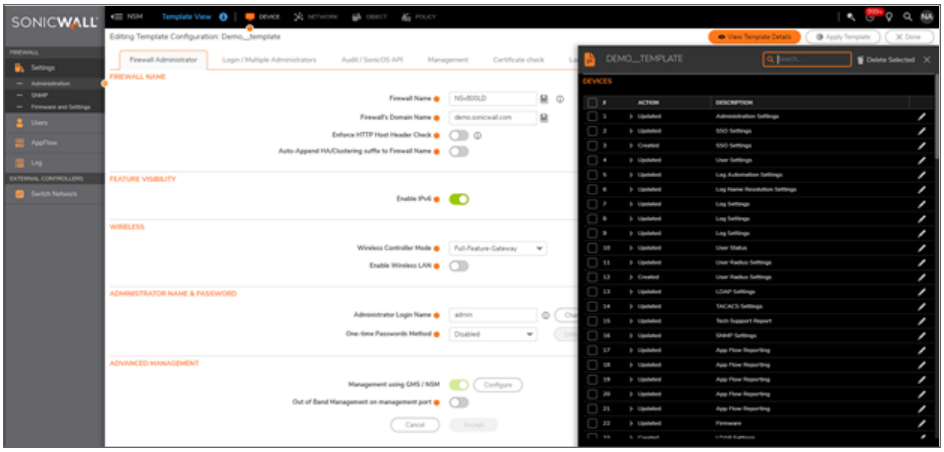
***To edit golden template:***

1. Click the new template name or select **Edit Template** in the **Action** field to open the **Template View**.
2. Navigate to other options in Template View: **Device**, **Network**, **Object**, or **Policy**.
3. Manually make changes to the exported configuration and add variables for device specific values as needed.

   ⓘ **NOTE:** It is recommended that you do not delete the configurations from View Template Configuration as it breaks dependencies.

   ⓘ **NOTE:** Since physical WAN interfaces are not exported, edit physical WAN interface settings under **Network > Interfaces** in template.
4. After you update the template, click **View Templates Details** to view the exported configurations and new

edits.



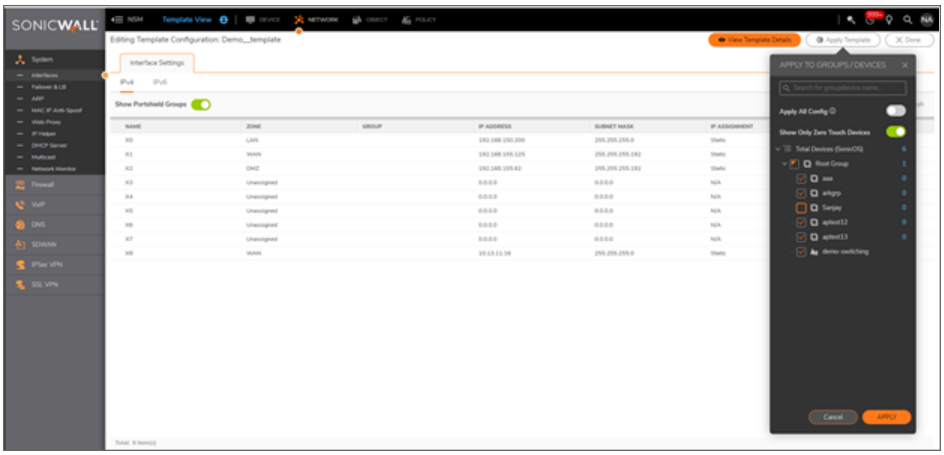
# Applying Template to Device Groups or Devices

You need to apply a template to review any apply errors and edit the template if needed to fix the errors.

ⓘ **NOTE:** NSM identifies and groups dependent configurations automatically before committing it to unapplied firewalls.

***To apply a template:***

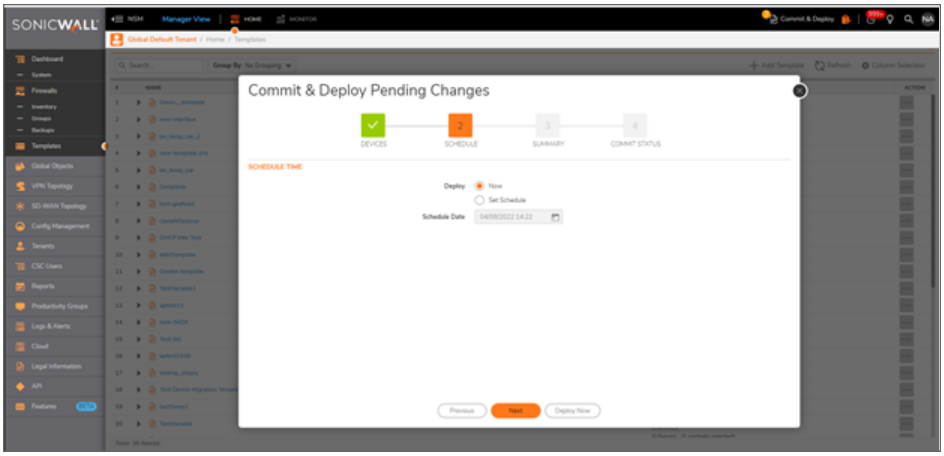
1. Click on the **Apply Template** button on the **Template View**. You can apply template on the **Manager View** using on the **Action** column next to the template that you want to apply.



2. Select the device group(s) or devices within any group (s) to apply the template.
3. Click **Save**.

# Committing and Deploying the Updates

1. Click on **Commit & Deploy** wizard from the **Manager View**.




2. Review devices and changes for deployment.
3. Create commit and deploy immediately or schedule for deployment later.
4. Once deployment is complete, review errors and make changes as needed.

# Variable Data

The Template Variable allows administrators to create variable objects use during template configuration. They can assign firewall specific parameters with unique values as variable objects within a Template.

**Topics:**


- Template Variables Overview
- Add Variable
- Edit Variable
- Resolve Variable
- Delete Variable
- Using Template Variables
- Creating Variables within Templates


# Template Variables Overview

When the Template is applied to devices in device groups, it automatically asks administrators to resolve the variable with device's unique value for the assigned device. Thus, the variable preserves the uniqueness of the

device-specific value during the commit and deploy process. Examples of such parameters are: IP Address, Hostname, FDQN or any octet of the IP address object.

Using Template Variables in the configuration workflow simplifies the automatic provisioning of device-specific configurations for each firewall across hundreds of locations. The available Template Variables are listed at **Objects > Variables**. At this same page administrators can Add Variable, Edit Variable, and Resolve Variable. After the variables are set up, they are selected from inside the template. Configuration items in the Template that support variables have the icon next to them.

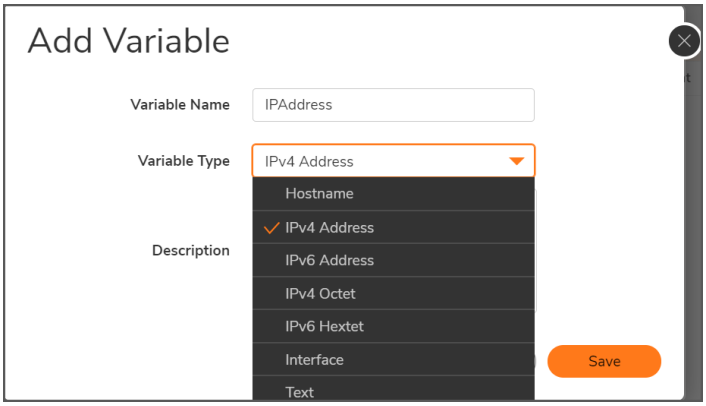
Variables can also be created while editing a template. Refer to Creating Variables within Templates for more information.

When working with Templates and Variables, you need to commit and deploy the changes so that they are pushed to the devices. To perform commit and deploy, refer Committing and Deploying the Updates

# Add Variable

***To add Variable Objects:***

1. Navigate to **Manager View | Global Objects > Variables** page.
2. Click **Add Variable**. Enter the Variable Name. From the Variable Type, choose the type as **IPv4 address, IPv6 address, IPv4 octet, IPv6 Hextet, Interface** and **Text.**




ⓘ **NOTE:** The Variable cannot be deleted once it is applied to the devices as a part of template configuration.

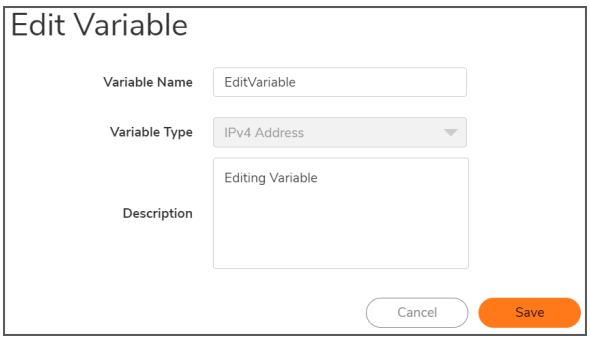
3. Click **Save**. The saved Variables are displayed in the list.
4. To delete any of the created variables from the list, check the box and click **Delete** icon.
5. **Refresh** icon at the top, refreshes the list.
6. **Column Selection** allows to choose which options can be displayed in the Variables screen by checking the box. You can also search for a specific variable from the list by typing the keyword in the search box.

# Edit Variable

***To edit Variable Objects:***

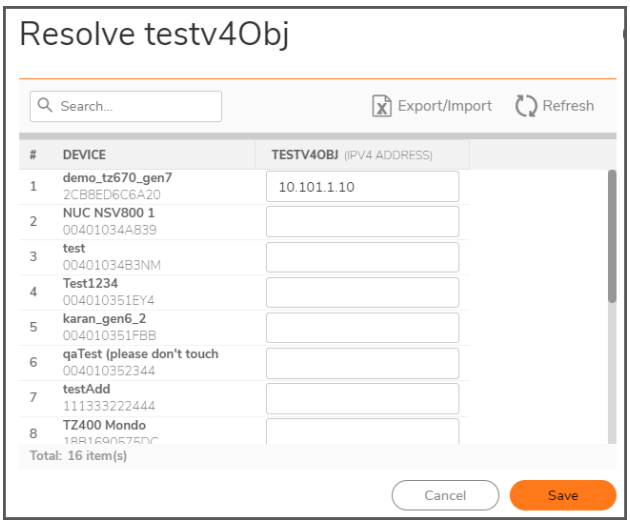
1. Navigate to **Manager View |Global Objects > Template Variables** page.
2. In the Action column, click **Edit Variable**.

   **NOTE:** Once a variable is used inside a template, it cannot be edited or modified; only the description field can be edited. For unused variables, you can change the Variable name and the description.
3. Edit the details and click **Save**.




# Resolve Variable

Resolve variables allows you to import and export the variables that are displayed in the list. The variables can be exported as a .CSV file and can be imported from a .CSV file.
**NOTE:** Make sure you update the exported CSV file and upload the same CSV to import the data.

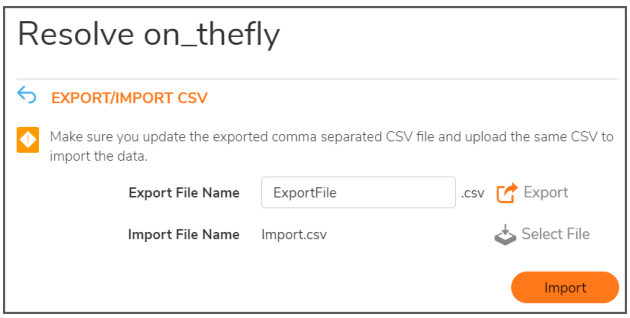


***To view Resolve Variables:***

1. Navigate to **Manager View | Global Objects > Variables** page.
2. In the Action column, Click **Resolve Variable**.
3. Click Export/Import icon.
4. Click **Refresh** icon to refresh the list.

## Export/Import CSV

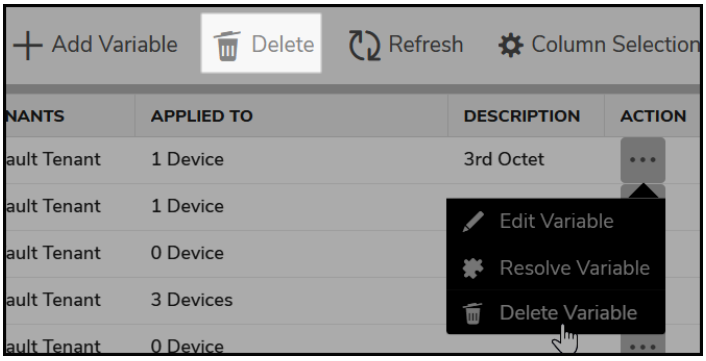
Click **Export/Import** icon and enter a file name in the Export File Name text box.
**NOTE:** Make sure you update the exported comma separated CSV file and upload the same CSV to import the data. Only CSV files are allowed.




# Delete Variable

***To delete Variable Objects:***

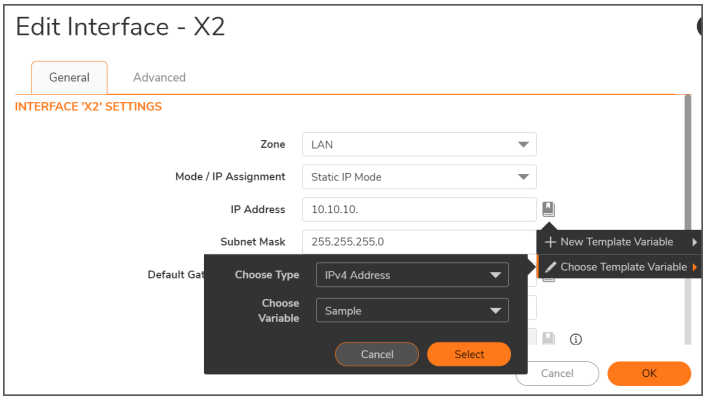
1. Navigate to **Manager View | Global Objects > Template Variables** page.
2. In the Action column, click **Delete Variable**.
   You can also delete a variable by selecting a specific entry(s) and click **Delete** icon.
   **NOTE:** Only the variables that are not in use can be deleted.



# Using Template Variables

When working with the templates, you have the option to choose a variable when defining parameters within a Template.

1. Navigate to **Manager View | Templates**.
2. Highlight a template and select **Edit Template** from the **Options** column.
3. Complete the fields as described in Editing Templates
4. For fields with the Variables icon associated with it, click the icon and select **Choose Template Variable** and select the **Choose Type** and **Choose Variable** from the drop down list and click **Select**.Upon saving, variables are saved in Template configuration.

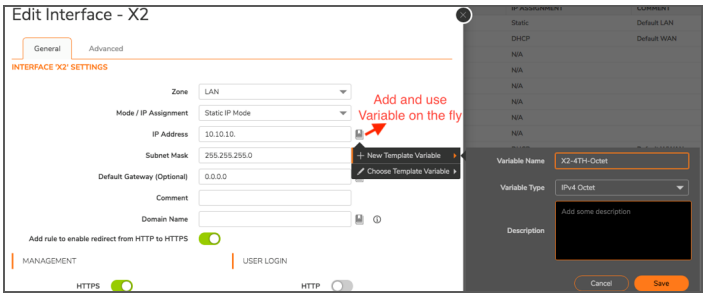



# Creating Variables within Templates

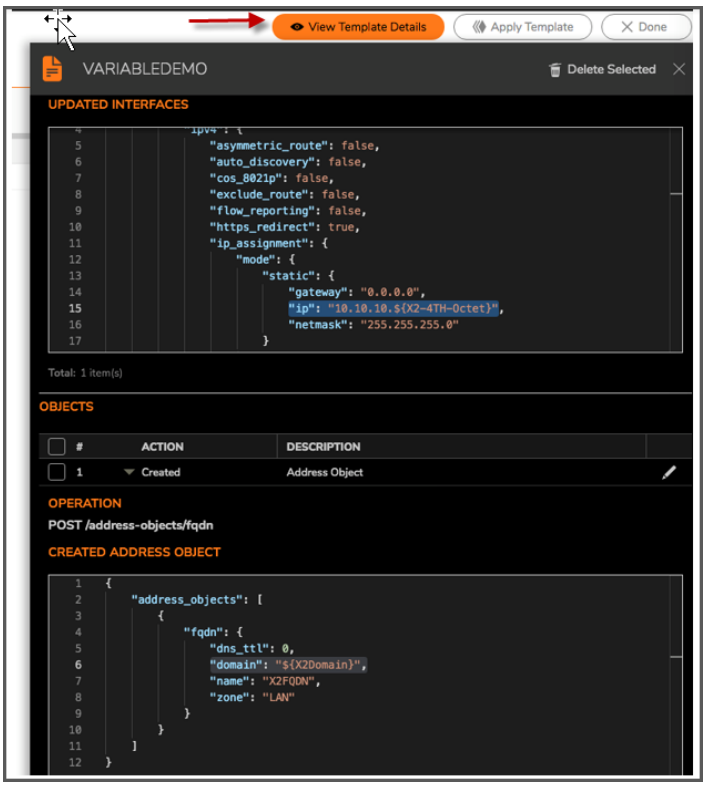
For some fields, you have the option to create a Variable when editing a Template. The process is very similar to creating the Variable on the **Global Objects > Variable Data** page.

***To create a variable while editing a template:***

1. Navigate to **Manager View | Templates**.
2. Highlight a template and select **Edit Template** from the **Options** column.
3. Complete the fields as described in Editing Templates
4. For fields with the Variables icon associated with it, click the icon and select **New Template Variable**.




5. Before applying the Template, you need to resolve the Variable values for devices to be applied. Refer Resolve Variable to know more information.
6. Click **View Template Details** to view the saved configuration.

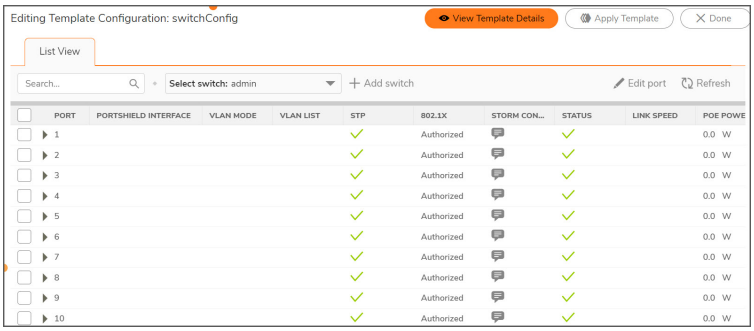


5

# SonicWall Switch Configuration in Template

The Switch command shows the details of available switches in the **SWITCH CONFIGURATION** table. To add a switch, click the **Add switch.** To edit the port, click **Edit** icon on any field.

You can now choose the values from the Template variables by creating a new variable object or by selecting a variable object from the existing list.




## Before Adding a Switch

- Be sure to first register your Switch on MySonicWall.
- Consider the firewall/switch topology to be implemented. Refer to or the Switch Getting Started Guide available at https://www.sonicwall.com/support/technical-documentation.
- When adding a Switch manually, first check that it is configured to factory defaults. This can be ensured by depressing the reset Switch for 10 seconds or from the Switch Local UI, or the Command Line Interface.
- When adding a management link to a Switch manually, ensure that the DHCP lease range supports default management IP address.
- The firewall interface linking to the Switch interface must have the Enable Auto-Discovery of SonicWall Switches option enabled. Edit the firewall interface and enable this option on the Advanced screen of the Edit Interface dialog.

- The firewall interface linking to the Switch interface cannot be a Port Shield host and no other firewall interface can be port shielded to it. The firewall interface linking to the Switch cannot be a Port Shield group member, that is, it cannot be port shielded to another firewall interface.

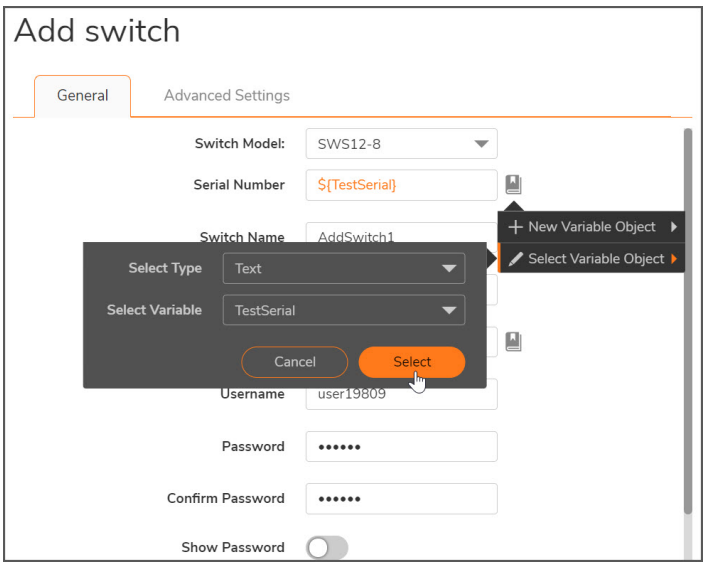
**Topics:**


- Add Switch
- Edit Port


# Add Switch

***To add a switch:***

1. Navigate to **Template View | Switch Network > Overview.**
2. Click **Add Switch**.




**Add switch - General**

- **Switch Model** - Choose the Switch model from the drop down list.
- **Serial Number**- Enter the Serial Number of the switch device. You can now choose the serial number by creating a new variable object or by selecting a variable object from the existing list. Click the icon to add or select a variable.
- **Switch Name** - To identify the switch.
- **Comment** - You can add a comment and this field is optional.
- **IP Address** - Enter the IP Address or choose a variable by clicking the icon.
- **User Name** - User name
- **Password** - Enter a new password for accessing the Switch.

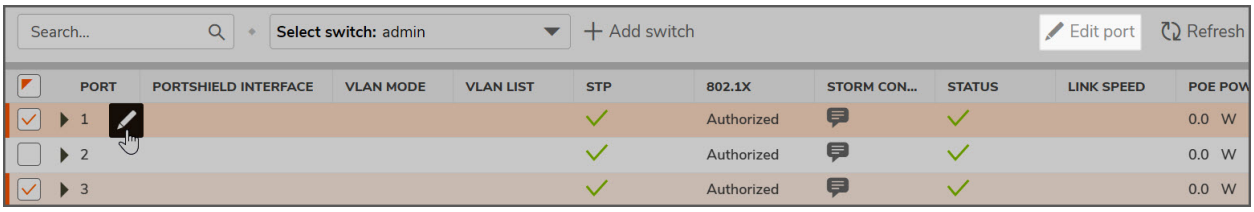
- **Confirm Password** - Re-enter the password. Both passwords need to match.
- **Show Password** - You may toggle this on to display or hide the password.
- **Switch Mode** - From the drop down, choose the switch mode. By default, it is Standalone mode.
- **Switch Management** - Choose the number in the drop down.
- **Firewall Uplink** - The uplink on which the switch is managed by the firewall. Choose the value in the drop down list.
- **Switch Uplink** - Choose the value in the drop down list.

**Add switch - Advanced Settings**

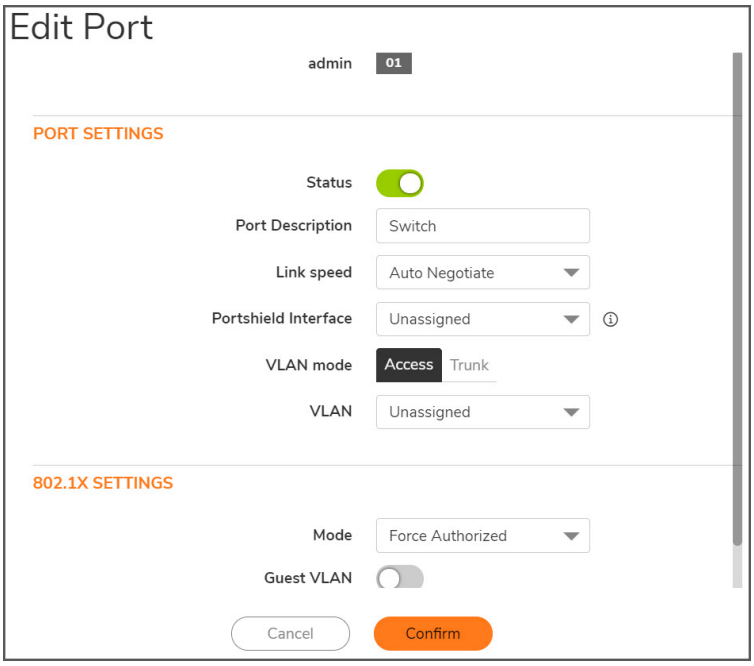
- **STP** - Toggle this to enable or disable Spanning Tree Protocol (STP).
- **STP Mode** - Choose the STP mode from Multiple or Rapid.
- **Jumbo Frame Size** - Input the Jumbo Frame Size. The value can range from 1522 to 10240.

# Edit Port

You can choose a single or multiple switch(es) and click the icon on any field or click **Edit Port** icon on the top.



### Edit Port - General



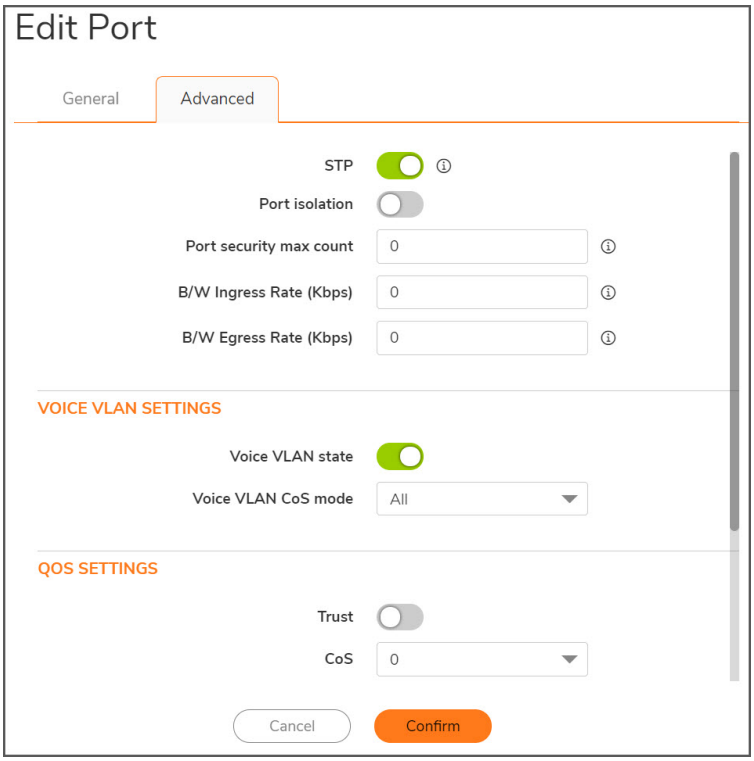

#### PORT SETTINGS

- **Status -** Toggle the status to enabled or disabled.
- **Port Description** - Enter a port description to identify.
- **Link Speed** - Choose the link speed from the list. The default option is Auto Negotiate.
- **Portshield Interface** - Choose the options from the dropdown list. Portshield options maybe disabled for External switch options.
- **VLAN Mode** - Choose the mode from **Access** and **Trunk**.
- **VLAN** - By default, this option is **Unassigned**.

#### 802.1X SETTINGS

- **Mode** - Select Auto, Force Authorized or Force Unauthorized from the list.
- **Guest VLAN** - Status whether it is enabled or disabled on the Switch. The Default is disabled.
- **Radius VLAN Assign** - Toggle to assign Radius VLAN.

### Edit Port - Advanced




- **STP** - Toggle the STP to enabled or disabled.

  **NOTE:** STP has to be enabled on switch before editing port STP.
- **Port Isolation** - Toggle to enable or disable port isolation.
- **Post security max count** - Default is 0, which disables port security. Range is 0-256. This is the maximum number of MAC addresses that can be learned on the port. Network security can be increased by limiting access on a specific port to users with specific MAC addresses.
- **B/W Ingress Rate (Kbps)** - Default is 0, which disables ingress bandwidth control. Allowed values are multiples of 16 between 0 and 1,000,000.
- **B/W Egress Rate (Kbps)** - Default is 0, which disables egress bandwidth control. Allowed values are multiples of 16 between 0 and 1,000,000.

**VOICE LAN SETTINGS**

- **Voice LAN State** - Toggle to enable or disable Voice LAN State.
- **Voice VLAN CoS mode** - Default is Source. Selections for the Class of Service mode include Source or All.

**QOS SETTINGS** - Quality of Service allows certain traffic types, such as voice or video streaming, to be prioritized.

- **Trust** - Toggle this to enable or disable Trust mode for incoming packets by clicking the slider. Enable this to classify traffic based on the IEEE 802.1p standard (using the 8 CoS priority tags).
- **CoS** - Select the CoS priority to set the priority for packets entering on this port. Default is 0. Range is 0-7 for Class of Service tags, with 0 (background) and 1 (best effort) the lowest priority and, 7 being the highest priority in the traffic forwarding queue.

**STORM CONTROL SETTINGS -** Storm Control limits the amount of Broadcast, Unknown Multicast, and Unknown Unicast frames accepted and forwarded by the Switch. Storm Control can be enabled per port by defining the packet type and the rate of packet transmission. The Switch discards the frames when the rate exceeds the defined rate.

- **Broadcast Rate (Kbps)** - Default is 0, which disables port broadcast. Allowed values are multiples of 16 between 0 and 1,000,000.
- **Unknown Multicast Rate (Kbps)** - Default is 0, which disables port unknown multicast.Allowed values are multiples of 16 between 0 and 1,000,000.
- **Unknown Unicast Rate (Kbps)** - Default is 0, which disables port unknown unicast. Allowedvalues are multiples of 16 between 0 and 1,000,000.

# Switches

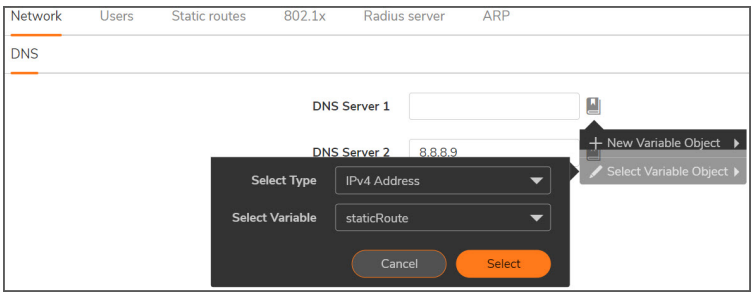
This section describes the various tabs listed in individual switch. You can choose a switch on the top and edit the options listed.

**Topics:**


- Network
- Users
- Static routes
- 802.1x
- Radius server
- ARP

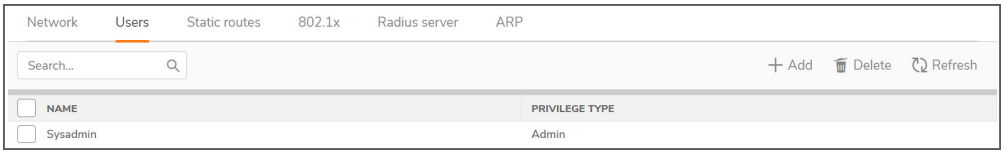

# Network

You can now choose the DNS Server 1 and 2 by creating a new variable object or by selecting a variable object from the existing list. Click the icon to add or select a variable.



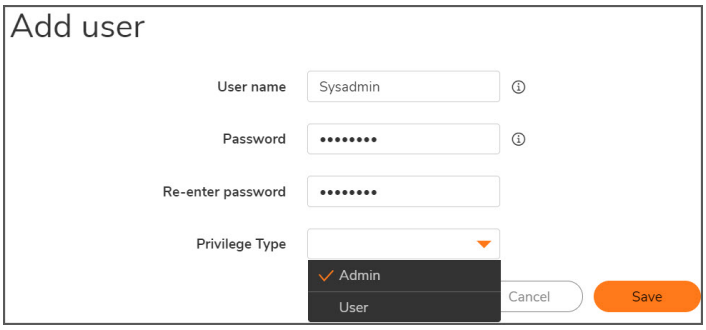

# Users

This screen displays all the users configured for the switch. You can add, delete or edit users from this page.




***To add a user:***

1. Navigate to **Template View | Switch Network > Switches**.
2. Click **Add** icon.



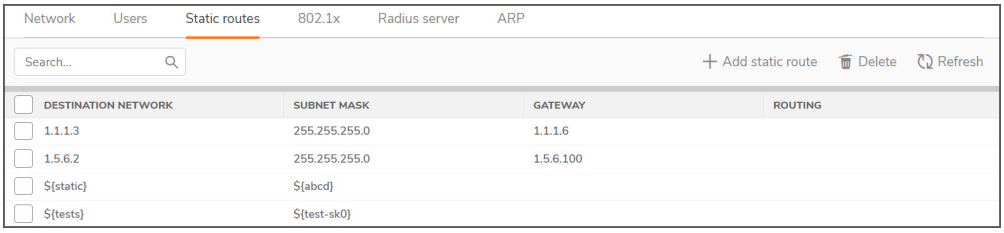

3. Enter the user name.
4. Enter and confirm the Authentication Password.
5. Select the Privilege Type. The options are **Admin** or **User**.
6. Click **Save**.

***To delete a user:***

1. Navigate to **Template View | Switch Network > Switches**..
2. Check the box to delete the users. You can choose to delete the selected ones or all users.
3. Click **Delete**.

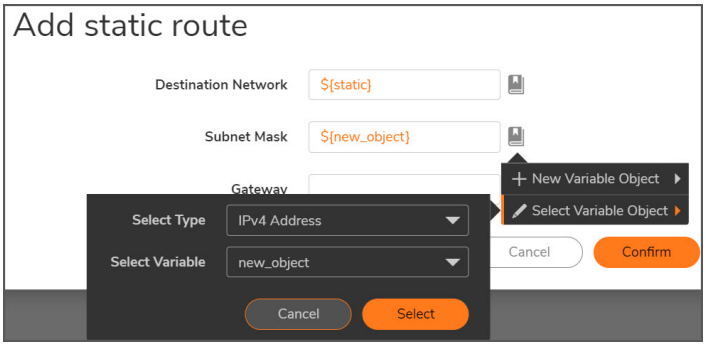
# Static routes

The Static Routes screen shows all the network destinations and gateway information for the switches added to the firewall.




***To add a user:***

1. Navigate to **Template View | Switch Network > Switches**.
2. Click **Add static route** icon.



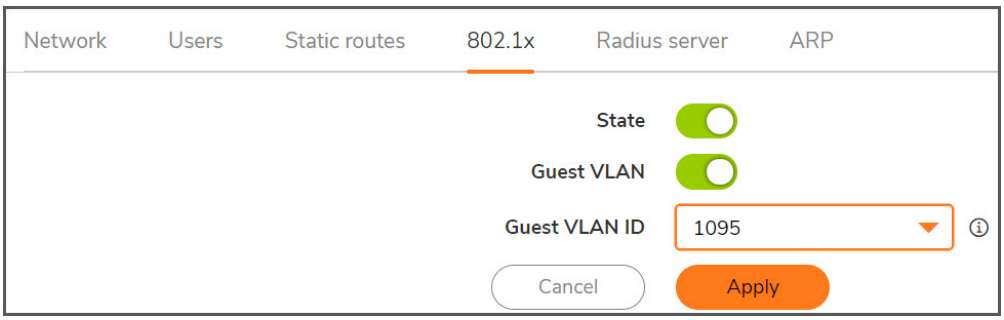

3. Choose a variable by clicking the icon and add a new variable object or select a variable object from the list.
4. Enter the Gateway address.
5. Click **Confirm**.

***To delete a static route:***

1. Navigate to **Template View | Switch Network > Switches**..
2. Check the box for the route to delete. You can choose to delete the selected ones or all.
3. Click **Delete Static Route(s)**.

# 802.1x

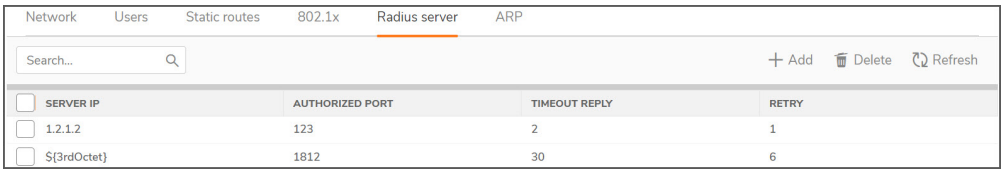
This feature allows enabling or disabling 802.1X based authentication for Guest VLAN users.




- **State** - Toggle to enable or disable the state. When disabled, you cannot change the Guest VLAN and input the ID.
- **Guest VLAN** - Toggle to enable or disable Guest VLAN.
- **Guest VLAN ID** - The values are between 2 to 4094.

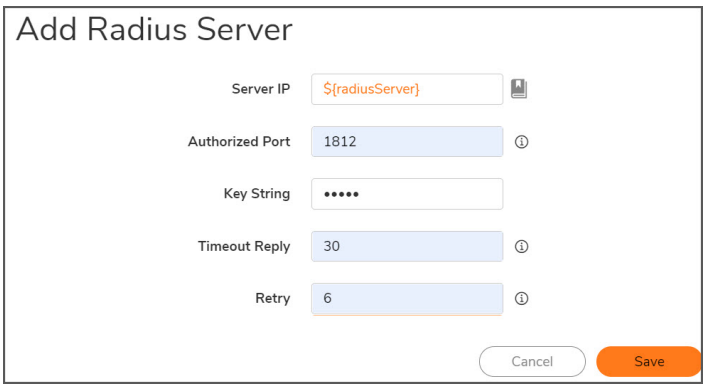
# Radius server

The RADIUS server authenticates client requests either with an approval or reject. RADIUS Server not only authenticates users based on the username and password but also authorizes based on the configured policy – whether the User group to which the user belongs is authorized or not; time constraints and various other policies if configured.




***To add a radius server:***

1. Navigate to **Template View | Switch Network > Switches**.
2. Click **Add** icon.



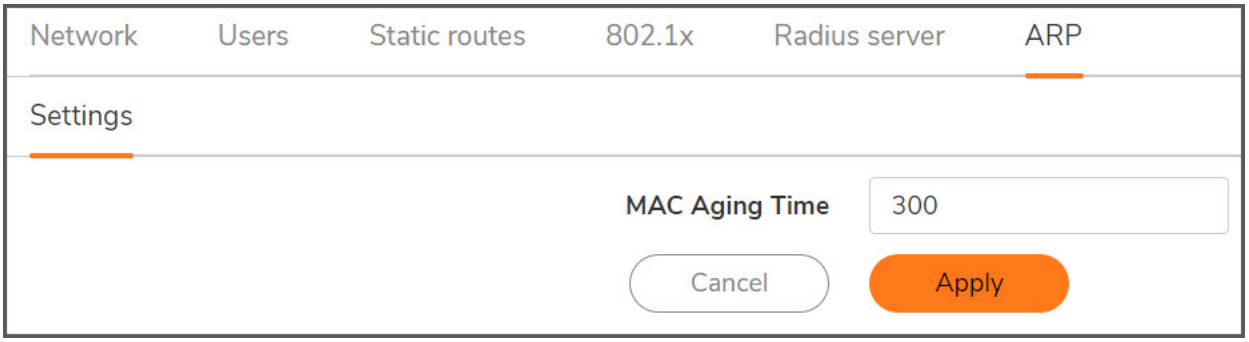
3. Choose a variable by clicking the icon and add a new variable object or select a variable object from the list.
4. Enter the authorized port value in the text box.
5. Input the key string.
6. Enter the Timeout value in seconds.
7. Enter the retry time(s)
8. Click **Save**.

***To delete a radius server:***

1. Navigate to **Template View | Switch Network > Switches**..
2. Check the box for the server to delete. You can choose to delete the selected ones or all.
3. Click **Delete.**

# ARP

You can use the ARP (Address Resolution Protocol) window to manage the static and dynamic MAC addresses of the switch.




The MAC Aging time specifies the time before an entry ages and is discarded from the MAC address table. The range is from 0 to 630; The default value is 300 seconds.
**NOTE:** Disabling MAC aging time is not recommended.

6

# Certificates

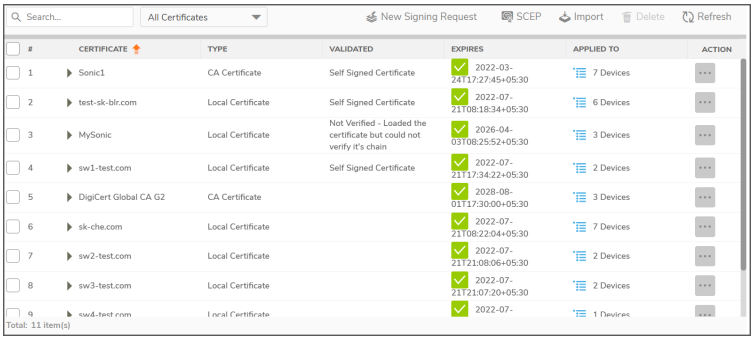
A digital certificate is an electronic means to verify identity by using a trusted third-party known as a Certificate Authority (CA). SonicWall supports third-party certificates in addition to the existing Authentication Service.

SonicWall security appliances interoperate with any X.509v3-compliant provider of Certificates. However, SonicWall security appliances have been tested with these vendors of Certificate Authority Certificates:

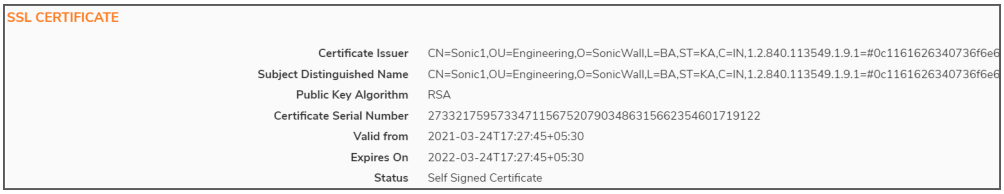
- Entrust
- Microsoft
- OpenCA
- OpenSSL and TLS
- VeriSign

## Navigating Certificates

Navigate to **Manager View > Global Objects > Certificates** displays the details for Certificate Authority (CA) Certificates and local certificates that you have imported or configured in NSM which can be deployed into Firewalls. It also provides all the settings for managing CA and Local Certificates.




Expand each Certificate using the arrow to view additional information like **Certificate Issuer, Subject Distinguished Name, Public Key Algorithm, Certificate Serial Number, Valid From, Expires On,** and **Status**.



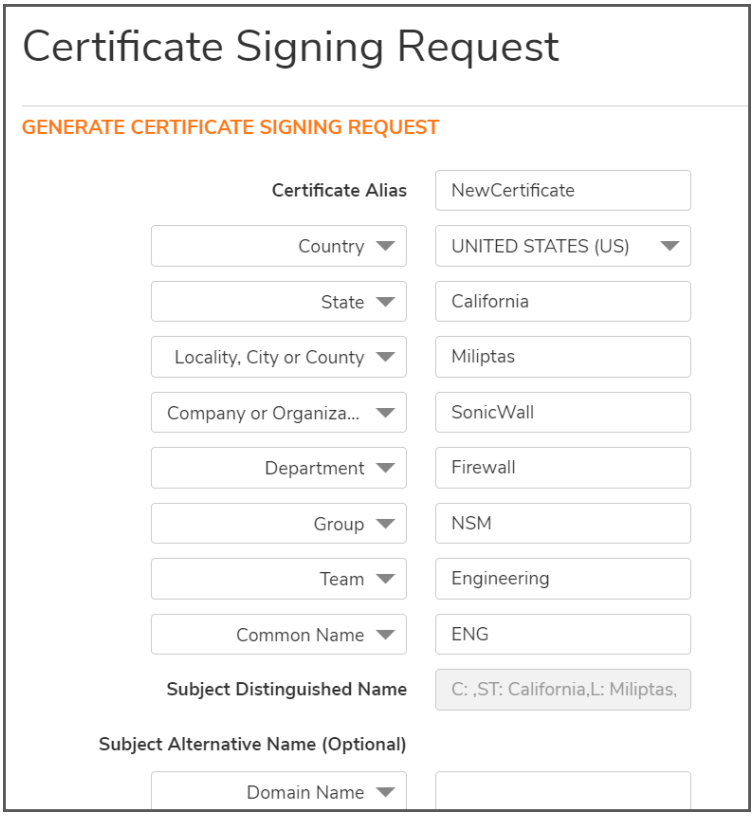

You can also search for a specific certificate using the Search box or choose from the drop down list and select the desired option.

- **All Certificates** - Displays all certificates and certificate requests.
- **Imported certificates** - Displays all imported certificates.
- **Certificate signing Request** - Displays the pending requests.
- **Expired certificates** - Displays all expired certificates.

# New Signing Request

This allows you to generate a certificate request towards getting your own SSL/TLS certificate.

Navigate to **Manager View > Global Objects > Certificates** and select **New Signing Request**. A screen is displayed which requires you to fill the details.

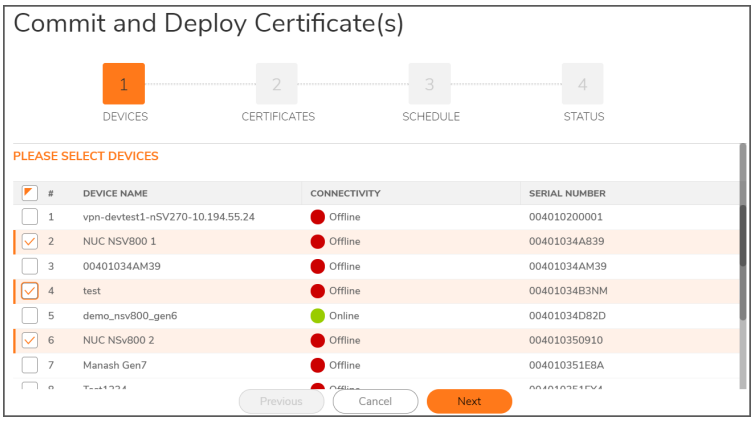


- **Certificate Alias** - Specify a name for the certificate in the Certificate Alias field.
- **Country (default), State, Locality or County, Company or Organization** - From the drop down list, choose the Country name.
- **Country, State (default); Locality, City, or County; Company or Organization; Department**
- **Locality, City, or County (default); Company or Organization; Department; Group; Team**
- **Company or Organization (default), Department, Group, Team**
- **Department (default), Group, Team, Common Name, Serial Number, E-mail Address**
- **Group (default), Team, Common Name, Serial Number, E-mail Address**
- **Team (default), Common Name, Serial Number, E-mail Address**
- **Common Name (default), Serial Number, E-mail Address**
- **Subject Distinguished Name** - As you enter the Subject Name attribute(s), the Subject Distinguished Name field is populated.
- **Subject Alternative Name (Optional)** - The entries are optional and can be selected by clicking the drop down list.
    - **Domain Name, Domain Name (default), E-mail Address, IPv4 Address**.
    - Signature Algorithm - Choose the algorithm from **MD5, SHA1, SHA256, SHA284, SHA512**
    - Subject Key Type - The default value is **RSA**.
    - Subject Key Size / Curve - Choose the subject key size from **1024 bits (default), 1536 bits, 2048 bits, 4096 bits**

Click **Generate** to view the generated certificate request in the Certificates screen. To exit the screen, click **Back**.

# Commit and Deploy Certificate(s)

Once the certificate is generated, you can commit and deploy them instantly or schedule at a selected time. You can review the updates (see ), and then commit (so that the changes are locked) and deploy the certificates.



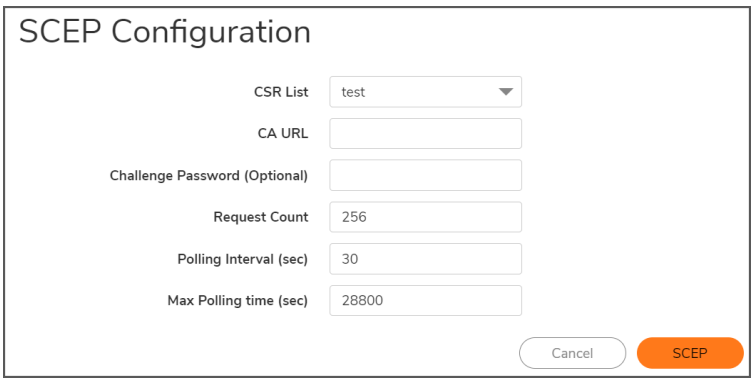

There are 3 steps to commit and deploy certificates.

1. From the **DEVICES** list, choose one or more devices and click **Next**. The devices that are listed displays the name, connectivity status and Serial Number.
2. In the next screen, choose one or more certificates and click **Next**. The certificate displays the type (Local or CA), validated status, Date of Expiry. To continue, click **Next** or click **Back** to go to the previous screen.
3. The next screen allows you to schedule the changes now or at a later date. Click **Apply** to proceed or **Back** to go to the previous screen.
    a. **Now** - To apply the certificate immediately.
    b. **Set Schedule** - Choose a later date to apply the certificate as per the schedule.
4. The last screen, **STATUS** displays the selected devices and the status of the commits.

# Configuring SCEP

SCEP protocol simplifies the certificate issuance process by using a URL and a shared secret to communicate with a PKI.

Navigate to **Manager View > Global Objects > Certificates** and select **SCEP**. A screen is displayed which requires you to fill the details.



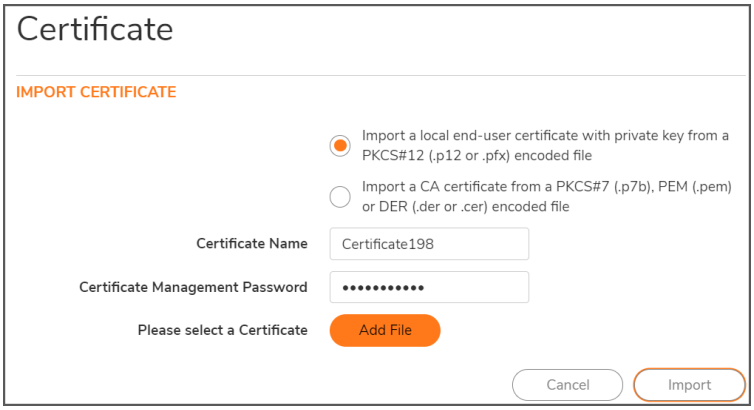

- **CSR List** - Select a certificate signing request (CSR) from the list if one has been uploaded.
- **CA URL** - Enter the URL of the certificate authority.
- **Challenge Password (Optional)** - Enter the password used to authenticate the enrollment request.
- **Request Count** - The default is 256.
- **Polling Interval (sec)** - The default is 30.
- **Max Polling Time(sec)** - The default is 28800.

Click **SCEP** to apply the SCEP configuration.

# Importing Certificates

There are two options to import the certificates -

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




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

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

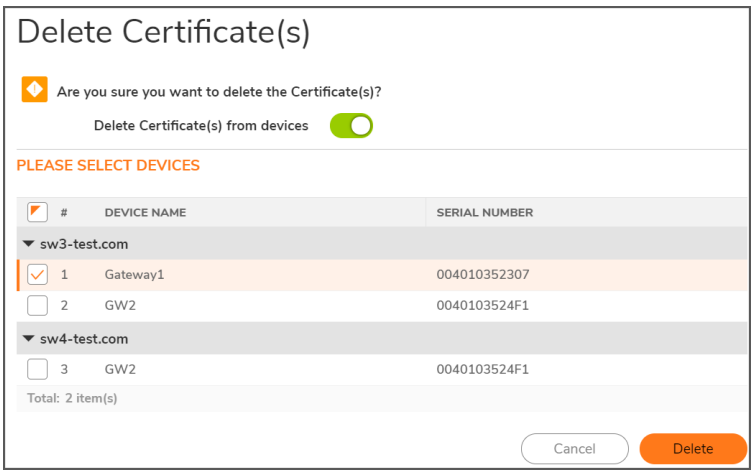
**Import a CA certificate from a PKCS#7 (.p7b), PEM (.pem) or DER (.der or .cer) encoded file**

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

# Deleting Certificates

You can delete the certificates that are displayed in the list and also the applied devices.

1. Navigate to **Manager View > Global Objects > Certificates** and select **Delete** icon. To delete multiple certificate(s), check the box(es) in the list. You can also click Ellipses icon in the **ACTION** column and select **Delete** icon for single certificate.
2. You are prompted to choose the applied devices. Toggling the button **Delete Certificate(s) from devices** to 'on' lets you to choose to delete certificates from the devices. Select the checkbox(es) for the applied devices you want to delete.
3. Click **Delete**.


Delete Certificate(s)
Are you sure you want to delete the Certificate(s)?
Delete Certificate(s) from devices
PLEASE SELECT DEVICES
# DEVICE NAME SERIAL NUMBER
sw3-test.com
1 Gateway1 004010352307
2 GW2 0040103524F1
sw4-test.com
3 GW2 0040103524F1
Total: 2 item(s)
Cancel
Delete

7

# 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

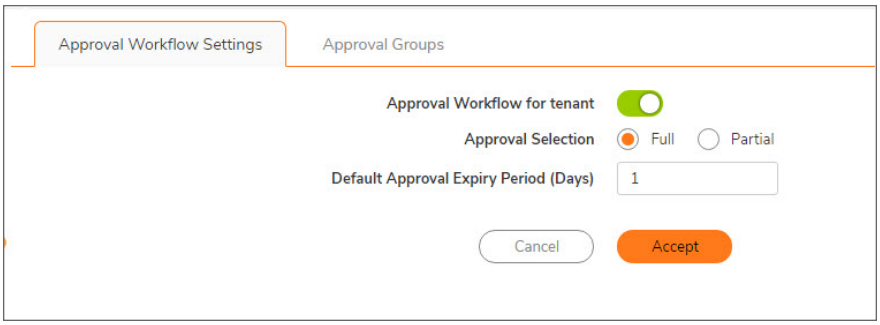
NSM has the ability to configure an approval process when planning and scheduling changes to the configuration (commits). Approval groups can be defined and enabled on a per tenant basis. You can also enforce partial approval, where one of a group of people can approve, or complete approval, where everyone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

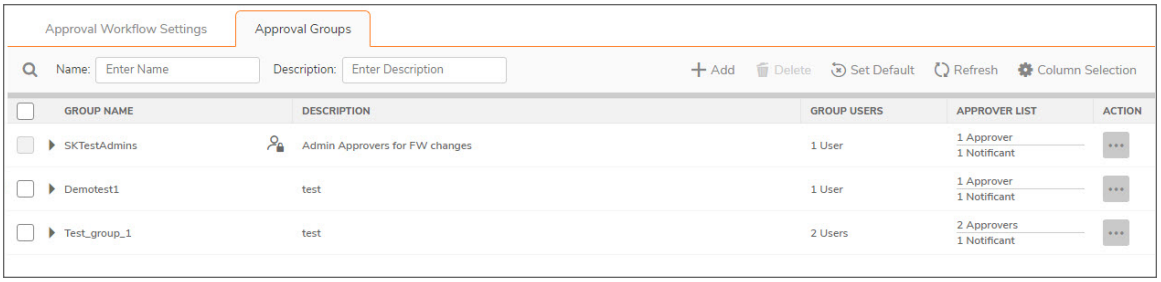



***To enable approvals:***

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**.

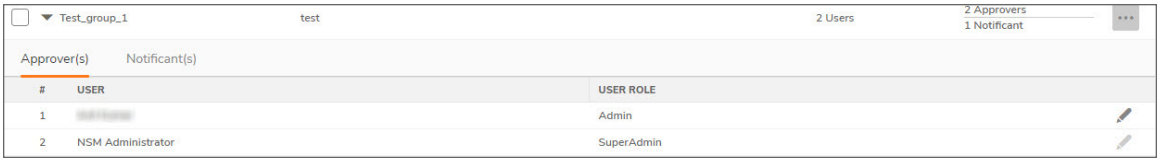
# Approval Group Management

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




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.



**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

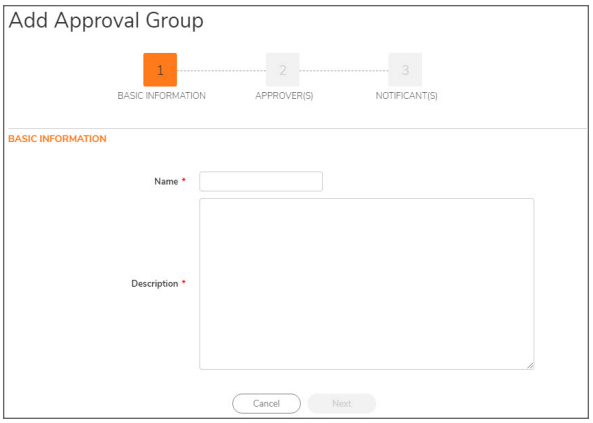
You can search for a specific approval group by using the name or description.

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.

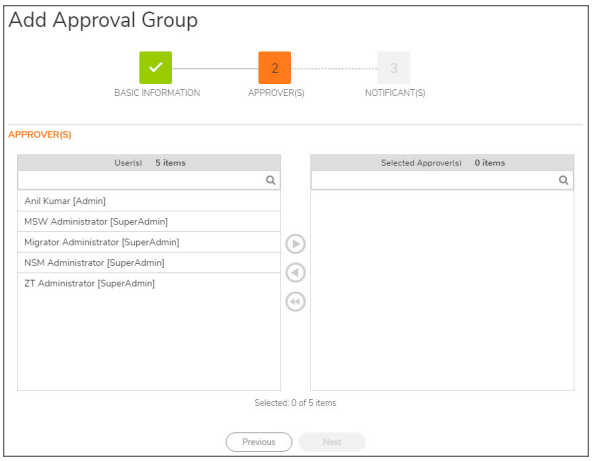
# Adding a New Approval Group

***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.



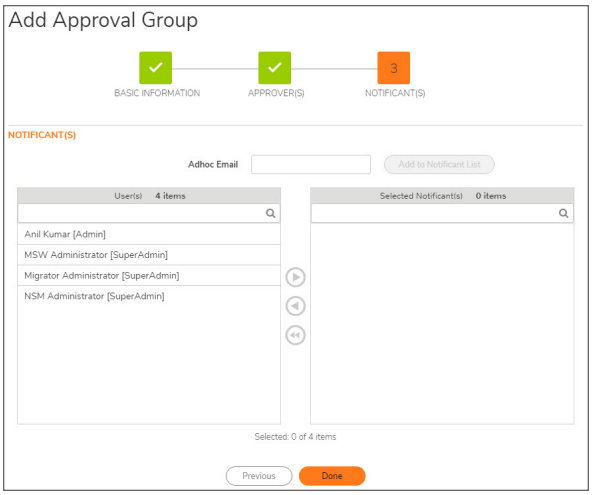

3. Type the **Name** of the approval group.
4. Type the **Description** in the field provided. Make it unique so you can easily search on it if needed. A maximum of 256 characters are allowed.
5. Click **Next**.




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.

   ⓘ | **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:***

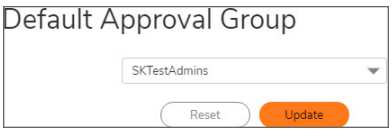
1. Navigate to **Home | Config Management > Approval Groups** and select the **Approval Groups** tab.
2. Select the group name of the group you want to delete.
3. In the **Action** column, select **Delete**.

   ⓘ **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.




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.
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.

# 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 ), 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.

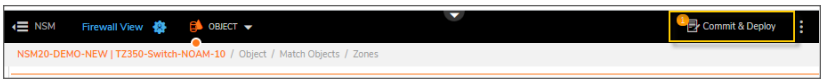
## Committing and Deploying Updates in the Firewall View

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

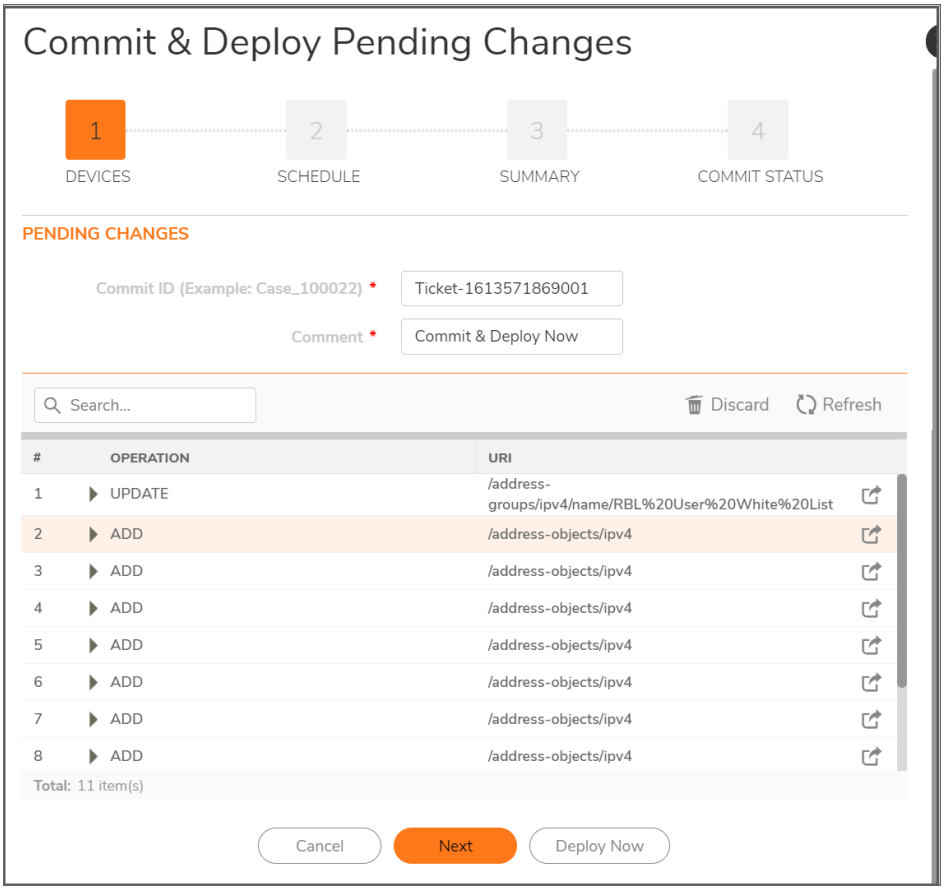
***To commit and deploy the configuration updates on a firewall:***

1. Navigate to the **Firewall View**.
2. To see the pending configuration updates on a firewall, click **Commit and Deploy**.

   **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

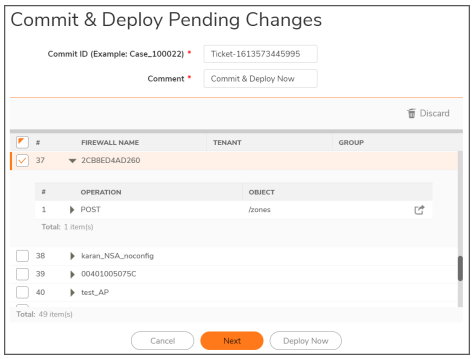



   b. If you select **Deploy Now**, a confirmation message on commit status is displayed.
   c. If you click **Next**, it allows you to set the schedule to a later time. Click **Commit** to commit items and **Deploy Now**at the scheduled time.
   d. A confirmation message on commit status is displayed. 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

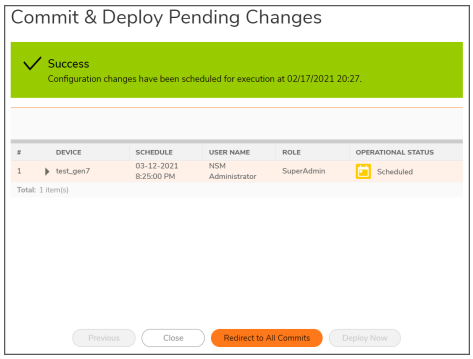
From the **Commit & Deploy** wizard in the **Manager View**, you can commit and deploy configuration updates to the device(s).

1. Navigate to the **Manager View**.
2. View pending configuration updates. See
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.



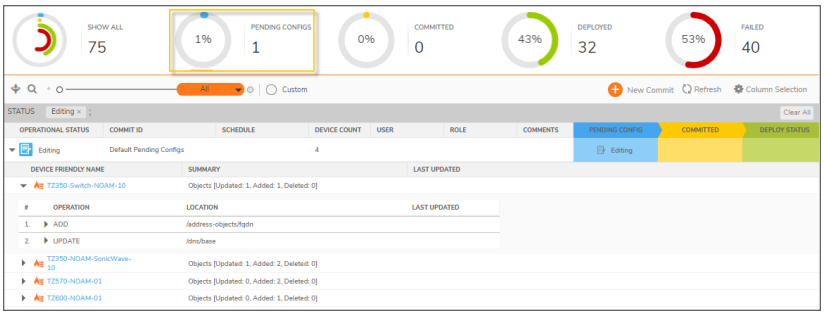

13. Click **Redirect to All Commits** to view the commits and their status. See Monitoring Commits.

# 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.

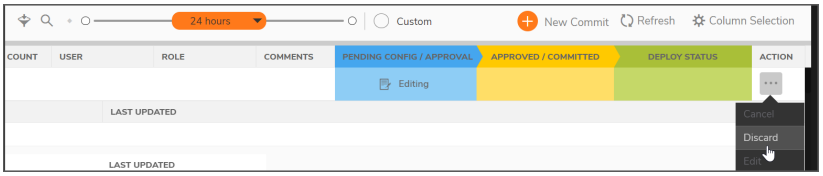
The operations are listed, for example: add, update, and so on. Click the caret icon next to the listed operation to see the JSON script of the operation performed. To perform commit and deploy, refer to Committing and Deploying the Updates

# 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:***

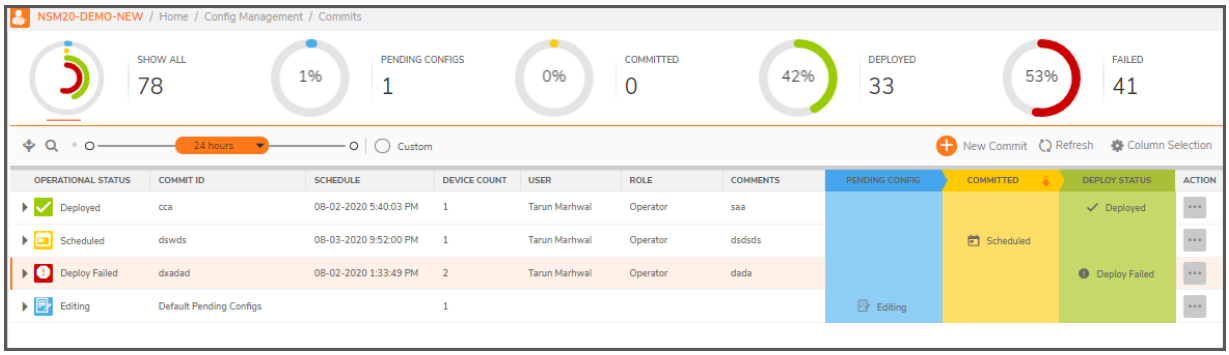
1. Navigate to **Manager view | Config Management > Commits**.
2. Hover over the item that shows **Editing** as its **OPERATIONAL STATUS** and click the **Ellipses** icon in the **ACTION** column.
3. Select **Discard**.




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.

**COMMITS**

| Term | Description |
|---|---|
| **OPERATIONAL STATUS** | Status of the commit. |

| Term | Description |
|---|---|
| **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 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

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

***To edit a commit:***

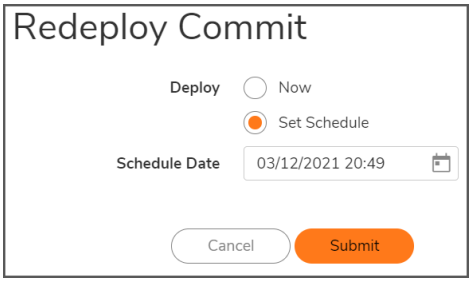
1. Navigate to **Manager view | Config Management > Commits**.
2. Hover over the commit and click the **Ellipses** icon in the **ACTION** column.
3. Click **Edit**.
4. Click **Yes** in the **Confirmation** dialog.

## 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:

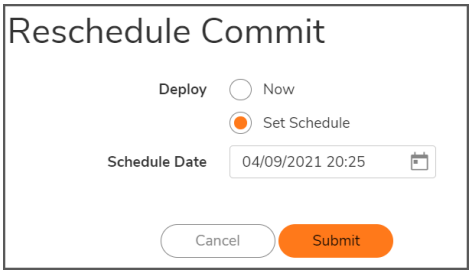



   - **Now**—to deploy instantaneously
   - **Set Schedule**—to set the schedule for deployment
5. If you selected **Set Schedule**, set the **Schedule Date**.
6. Click **Submit**.

# 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

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

***To delete a commit:***

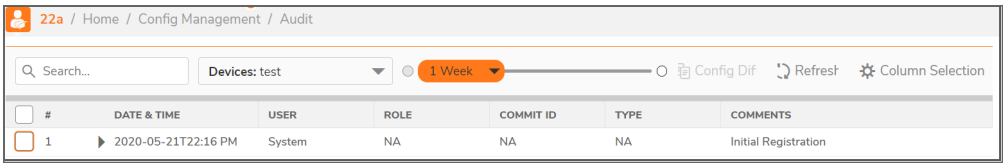
1. Navigate to **Manager view | Config Management > Commits**.
2. Hover over the commit and click the **Ellipses** icon in the **ACTION** column.
3. Click **Delete**.
    a. Click **Yes** in the **Confirmation** dialog.
    A success message is displayed if deletion is successful.
    The **OPERATIONAL 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.

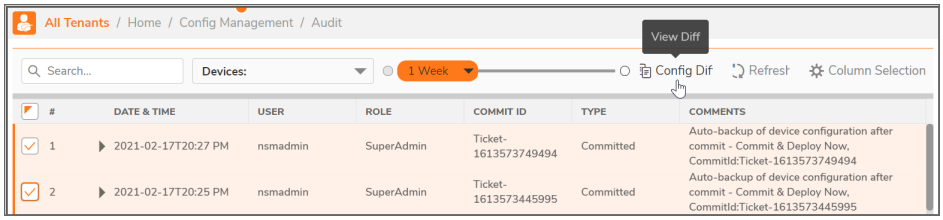
This data is shown in the **Audit** table at **MANAGER VIEW> Config Management > Audit**. You can adjust the period of the audit by adjusting the slider at the top of the page to the predefined values. The table lists all the commits performed by the users on any device selected from the Devices drop-down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




***To view differences between configurations:***

1. Navigate to **Template View > Config Management > Audit**.
2. Select two commits to compare.



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**.

8

# 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.

9

# VPN Topology

VPN centralizes and simplifies the configuration of VPN settings and policies. The adding of VPN Topology and the setup process is wizard based which guides through every step. It simplifies monitoring the traffic going through VPN tunnels.

**Topics:**

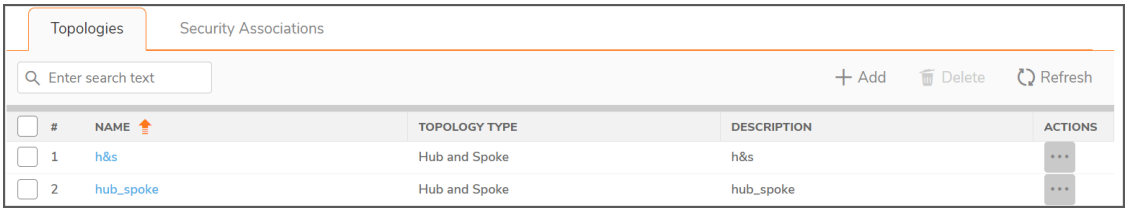

- IPsec VPN Topology
- Security Associations
- IPsec Monitor
- Global Settings


# IPsec VPN Topology

VPN Topology allows you to add the VPN or VPN configuration and monitoring. The VPN Topology Wizard allows you to create an IPSec VPN Hub-and-Spoke topology across their headquarters, branch offices and data centers using an easy-to-use wizard.

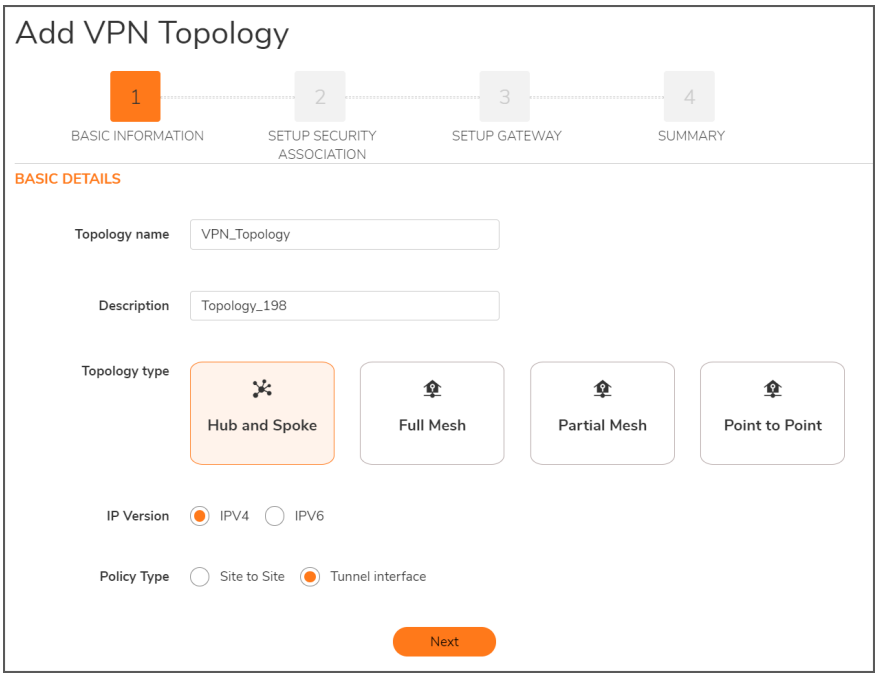
## Topologies

The created VPN Topologies that can be used in NSM are displayed in the list.



***To add VPN Topology:***

1. Click **Add** to add new VPN Topology.
2. There are 4 steps to add the topology. Click **Next** after each screen to add the topology.




The following section provides detailed information of each wizard -

1. Basic Information
2. Setup Security Association
3. Setup Gateway
4. Summary

***To edit existing VPN Topology:***

1. Navigate to **Home | VPN > IPsec VPN Topology** and select the item from the list.
2. In the Action column, select **Edit**.
3. Navigate through the screens and make the changes needed.
4. Click **Done**.
5. Verify that the changes appear in the table.

# Hub and Spoke

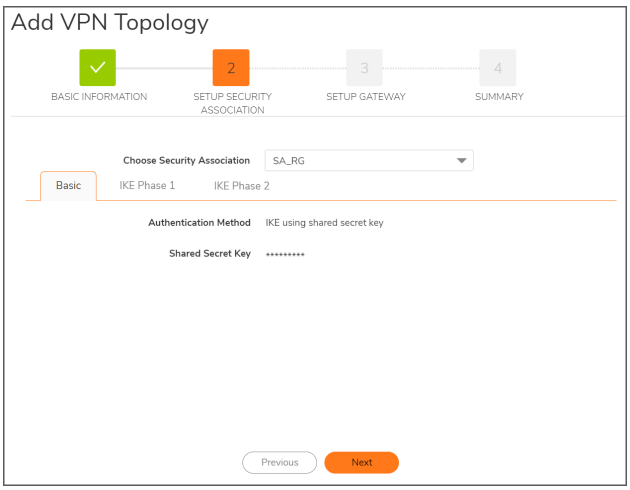
## BASIC INFORMATION

- **Topology Name** : Enter a name to identify the Topology.
- **Description** : This field is a mandatory field to move to the next screen. You can enter a short description to identify the topology.
- **Topology Type** : Choose a type from the options :
    - **Hub and Spoke** - The network design where the central device is located.
- **IP Version** : The version of IP that can be used.
    - IPV4 - 32-Bit IP address which is numeric.
    - IPV6 - 128-Bit IP address which is alpha-numeric.
- **Policy Type** : Type of the policy
    - **Site to Site** - Choose this option if there is a connection between two or more networks
    - **Tunnel Interface** - Choose this option to create connection between peers and Virtual Tunnel Interfaces.

## SETUP SECURITY ASSOCIATION

Choose a security association from the drop down list.
**NOTE:** The list is displayed only if there are any existing security associations available. To know how to add security association, refer Adding Security Association.

Once the security association is selected from the list, two tabs appear which displays the information while creating the security association. For more information on how to add Security Association, refer Security Associations.

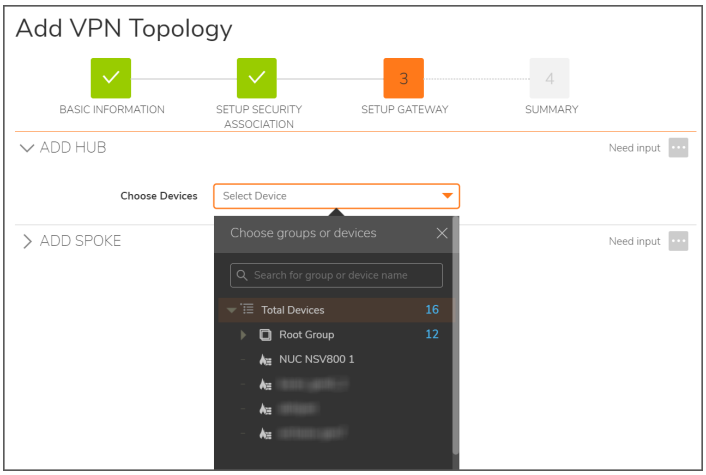


## SETUP GATEWAY

This screen allows you to add the topology type you selected in the previous screen.

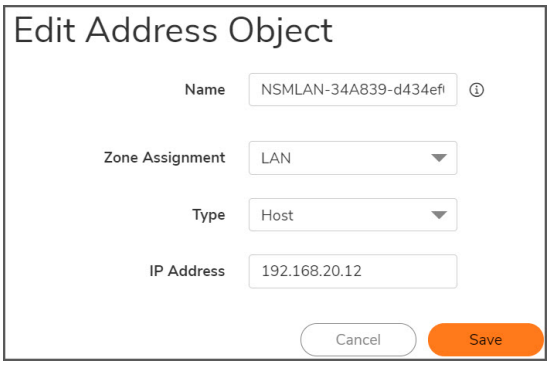
## ADD HUB

1. From the **Choose devices** drop down, select devices that are part of a group. You can also search for the devices or groups in the list by typing the name in the input field.
   **NOTE:** You can only select the devices that are part of a group.



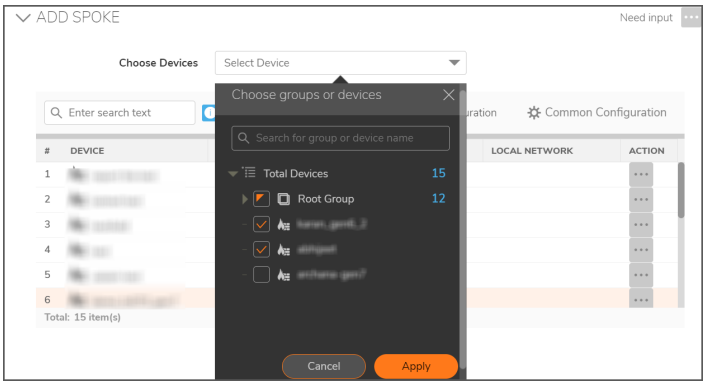

2. After selecting a device, you are required to choose the following options
   a. **Choose Devices** - Choose devices from the drop down list.
   b. **WAN Interface** - From the drop down list, select WAN Interface.
   c. **Primary Gateway** - Enter the primary gateway in the text box.
   d. **Secondary Gateway** - Enter the secondary gateway in the text box.
   e. **Local IKE ID Criteria** - Click the radio button to choose from Firewall ID, IPV4 Address, Domain Name, Key Identifier, and Email Address.
   f. **IKE ID** - This field is auto-populated and cannot be edited.
   g. **Protected Networks** - From the drop down list, select the network. Click the **Edit** icon to add or

edit Address Object and Group.

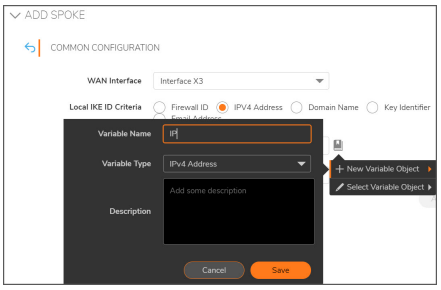



## ADD SPOKE

1. From the Choose devices drop down, select groups or devices by checking the box. You can also search for the devices or groups in the list by typing the name in the input field. Click **Apply** to select the device. The devices that are selected are displayed in a list.
   **NOTE:** Hub and Spokes should not have overlapping IP Addresses in any of the fields.




2. To use the common configuration, click **Common Configuration** icon.
   After selecting the common configuration, you are required to choose the following options :
   a. **Reference Device** - From the drop down list, select the reference device.
   b. **WAN Interface** - Choose WAN interface from the list. The options get enabled only after selecting Reference device.
   c. **Local IKE ID Criteria** - Click the radio button to choose from Firewall ID, IPV4 Address, Domain Name, Key Identifier, and Email Address.
      You can now add or create variable objects in common configuration. Click the variable icon and select new to create a new variable or choose an existing variable.




d. **IKE ID** - This field is auto-populated and cannot be edited.

e. **Local Network** - Enter the local network IPV4 address.

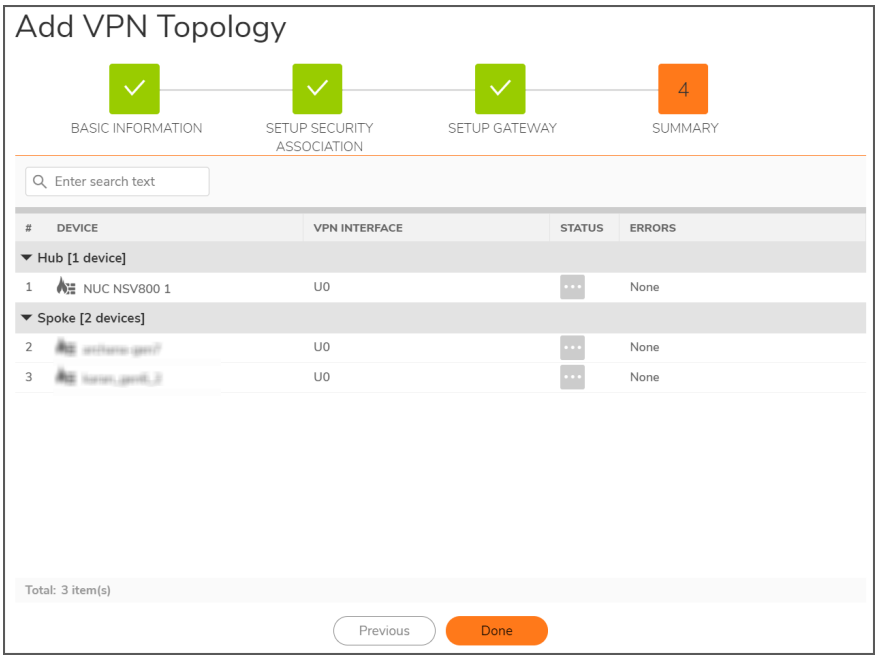
f. Check the box to enable or disable auto-increment local network.

3. To edit the configuration of the device, go to the Action column and select **Edit** icon.

## SUMMARY

This is the last step to create a VPN Topology. It displays the summary of the selected hub and spokes with the Device Name, VPN Interface, Status and Errors. In case if there are any errors, you are required to view and resolve them before adding a topology.

Click **Done** to finish and exit the wizard or **Previous** to go back to the previous screen.



# Full Mesh Topology

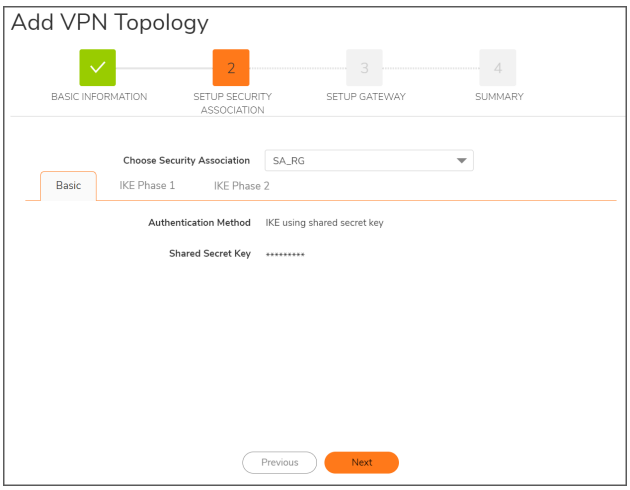
## BASIC INFORMATION

- **Topology Name** : Enter a name to identify the Topology.
- **Description** : This field is a mandatory field to move to the next screen. You can enter a short description to identify the topology.
- **Topology Type** -
    - **Full Mesh** - It provides a connection from each node to every other node on the network.
- **IP Version** : The version of IP that can be used.
    - IPV4 - 32-Bit IP address which is numeric.
    - IPV6 - 128-Bit IP address which is alpha-numeric.
- **Policy Type** : Type of the policy
    - **Site to Site** - Choose this option if there is a connection between two or more networks
    - **Tunnel Interface** - Choose this option to create connection between peers and Virtual Tunnel Interfaces.

## SETUP SECURITY ASSOCIATION

Choose a security association from the drop down list.
**NOTE:** The list is displayed only if there are any existing security associations available. To know how to add security association, refer Adding Security Association.

Once the security association is selected from the list, two tabs appear which displays the information while creating the security association. For more information on how to add Security Association, refer Security Associations.

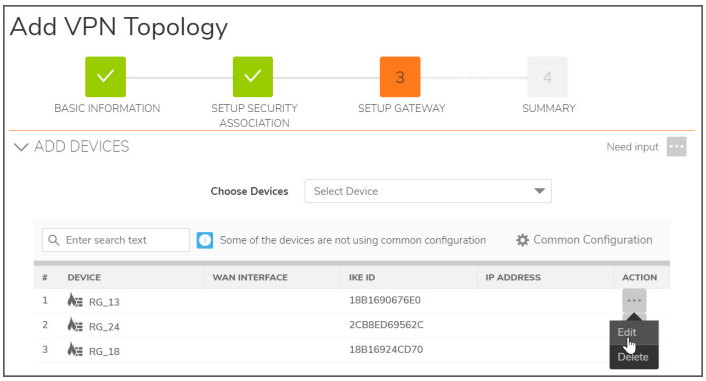


## SETUP GATEWAY

This screen allows you to add the topology type you selected in the previous screen.

## ADD DEVICES

1. From the **Choose devices** drop down, select devices that are part of a group. You can also search for the devices or groups in the list by typing the name in the input field.
   **NOTE:** You can only select the devices that are part of a group.

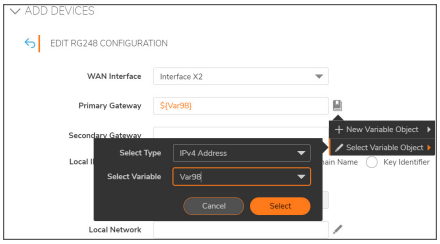



2. After selecting the devices, you are required to edit the device configuration. Click Ellipses icon in the **ACTION** column and select **Edit** icon.

   a. **Choose Devices** - Choose devices from the drop down list.

   b. **WAN Interface** - From the drop down list, select WAN Interface.

      You can now add or create variable objects in common configuration. Click the variable icon and select new to create a new variable or choose an existing variable.




   c. **Primary Gateway** - Enter the primary gateway in the text box.

   d. **Secondary Gateway** - Enter the secondary gateway in the text box.

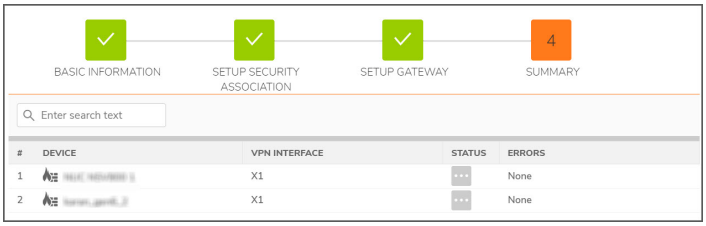
   e. **Local IKE ID Criteria** - Click the radio button to choose from Firewall ID, IPV4 Address, Domain Name, Key Identifier, and Email Address.

   f. **IKE ID** - This field is auto-populated and cannot be edited.

   g. **IP Address** - Enter the IP Address

### SUMMARY

This is the last step to create a VPN Topology. It displays the summary of the selected devices with the Device Name, VPN Interface, Status and Errors. In case if there are any errors, you are required to view and resolve them before adding a topology.




Click **Done** to finish and exit the wizard or **Previous** to go back to the previous screen.

# Point to Point Topology

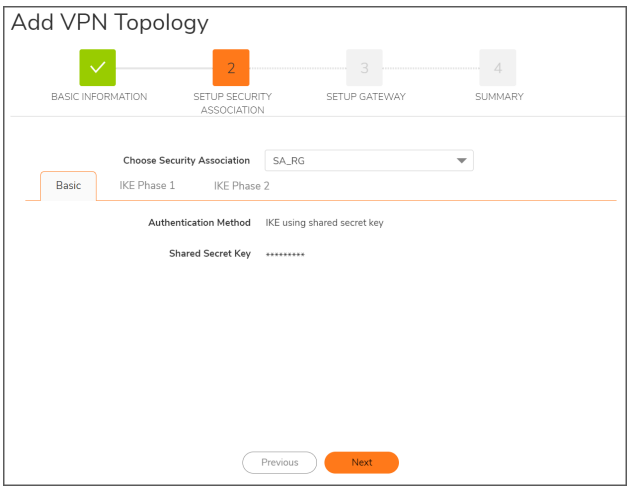
## BASIC INFORMATION

- **Topology Name** : Enter a name to identify the Topology.
- **Description** : This field is a mandatory field to move to the next screen. You can enter a short description to identify the topology.
- **Topology Type** -
    - **Point to Point** - This connects two nodes directly together with a common link..
- **IP Version** : The version of IP that can be used.
    - IPV4 - 32-Bit IP address which is numeric.
    - IPV6 - 128-Bit IP address which is alpha-numeric.
- **Policy Type** : Type of the policy
    - **Site to Site** - Choose this option if there is a connection between two or more networks
    - **Tunnel Interface** - Choose this option to create connection between peers and Virtual Tunnel Interfaces.

## SETUP SECURITY ASSOCIATION

Choose a security association from the drop down list.
**NOTE:** The list is displayed only if there are any existing security associations available. To know how to add security association, refer Adding Security Association.

Once the security association is selected from the list, two tabs appear which displays the information while creating the security association. For more information on how to add Security Association, refer Security Associations.




## SETUP GATEWAY

This screen allows you to add the topology type you selected in the previous screen.

## ADD DEVICE 1

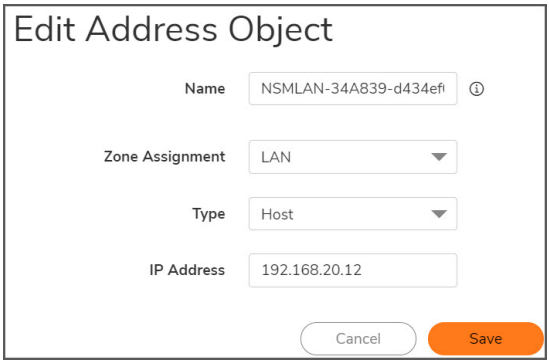
1. From the **Choose devices** drop down, select devices that are part of a group. You can also search for the devices or groups in the list by typing the name in the input field.
   **NOTE:** You can only select the devices that are part of a group.

2. After selecting a device, you are required to choose the following options
   a. **Choose Devices** - Choose devices from the drop down list.
   b. **WAN Interface** - From the drop down list, select WAN Interface.
   c. **Primary Gateway** - Enter the primary gateway in the text box.
   d. **Secondary Gateway** - Enter the secondary gateway in the text box.

e. **Local IKE ID Criteria** - Click the radio button to choose from Firewall ID, IPV4 Address, Domain Name, Key Identifier, and Email Address.

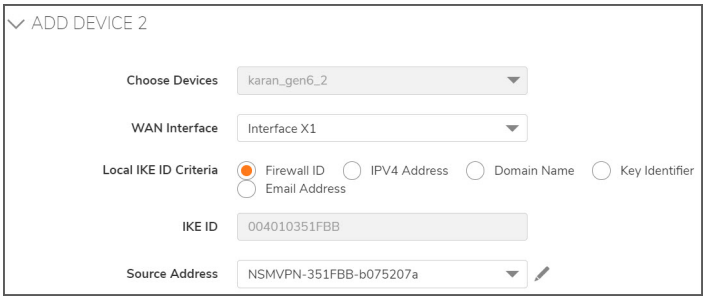
f. **IKE ID** - This field is auto-populated and cannot be edited.

g. **Source Address** - From the drop down list, select the address. Click the **Edit** icon to add or edit Address Object and Group.




## ADD DEVICE 2

1. From the Choose devices drop down, select groups or devices by checking the box. You can also search for the devices or groups in the list by typing the name in the input field. Click **Apply** to select the device. The devices that are selected are displayed in a list.
**NOTE:** Device 1 and Device 2 should not have overlapping IP Addresses in any of the fields.




2. To use the common configuration, click **Common Configuration** icon.
After selecting the common configuration, you are required to choose the following options :

   a. **Reference Device** - From the drop down list, select the reference device.

   b. **WAN Interface** - Choose WAN interface from the list. The options get enabled only after selecting Reference device.

   c. **Local IKE ID Criteria** - Click the radio button to choose from Firewall ID, IPV4 Address, Domain Name, Key Identifier, and Email Address.

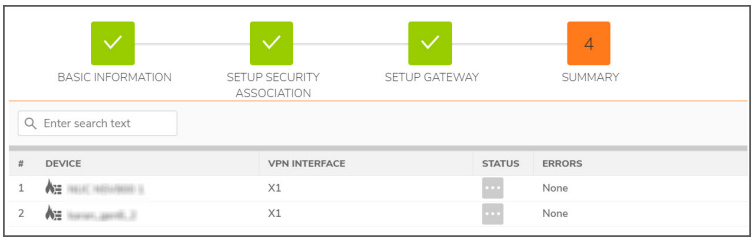
   d. **IKE ID** - This field is auto-populated and cannot be edited.

   e. **Source Address** - From the drop down list, choose a source address or click **Edit** icon to add New address object or group.

3. To edit the configuration of the device, go to the Action column and select **Edit** icon.

### SUMMARY

This is the last step to create a VPN Topology. It displays the summary of the selected devices with the Device Name, VPN Interface, Status and Errors. In case if there are any errors, you are required to view and resolve them before adding a topology.




Click **Done** to finish and exit the wizard or **Previous** to go back to the previous screen.

# Security Associations

Security Association (SA) is an agreement between two IPsec peers or endpoints. The Security Association contains all the information required for the two peers to exchange data securely. In particular IKE Security Associations are used to specify the type of authentication and which group to use.

***To add security association:***

1. Click **Add** to add new security association.
2. There are 3 screens to add the association. Click **Save** after each screen to proceed or **Cancel** to exit.
3. **Basic** - Enter the information in each screen :
    a. **Security Association Name** - Input a name to identify the security association
    b. **Authentication Method**- Choose an authentication method to establish a secure IPSec VPN.
        - **IKE Using shared secret key** - Selecting this option requires you to use IKE Phase 1 and 2.
        - **Manual Key** - Selecting this option opens IPSec SA options.
        - **Certificates** - Selecting this option lets you select local certificates for individual devices when creating a VPN Topology.
    c. **Shared Secret Key** - Password for the VPN gateway.
4. **IKE Phase 1**
    a. **Exchange Mode** - Choose the mode.
    b. **Authentication** - Choose the authentication.
    c. **Encryption** - Choose the encryption.
    d. **DH Group** - Choose the DH group.
    e. **LifeTime** - Enter IKE Phase 1 Lifetime in seconds between 120 to 9999999.

5. **IKE Phase 2**
    a. **Protocol** - Choose the protocol.
    b. **Authentication** - Choose the authentication.
    c. **Encryption** - Choose the encryption.
    d. **Enable Perfect Forward Security** - Check the box to enable or disable perfect forward security.
    e. **LifeTime** - Enter IKE Phase 2 Lifetime in seconds between 120 to 9999999.

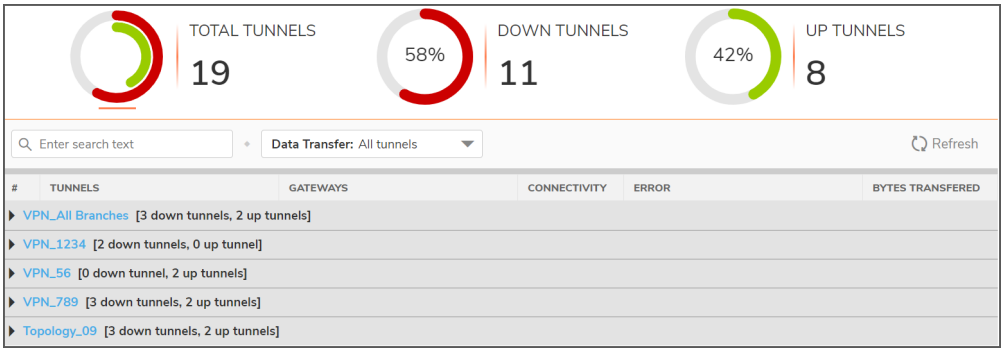
# IPsec Monitor

This screen displays all the VPN Topologies that are available and lets you to monitor them. It gives information on the Total Tunnels, Down Tunnels, Up Tunnels, Monitor connection status, data transferred, and errors. You can also search in the text box and filter the desired information from **Data Transfer** drop down list.

**Red** - Indicates the Down Tunnels.

**Green** - Indicates the Up Tunnels.

Click **Refresh** icon to refresh the list.




# Global Settings

This screen displays all the settings that can be changed or modified to the VPN Topology. The screen is categorized based on different options available for each section.

- **GLOBAL SETTINGS**
    - **Enable VPN** - Toggle the button to enable or disable VPN.
    - **Enable Fragmented Packet Handling** - Toggle the button to enable or disable the breaking of packets into fragments.
    - **Ignore df don't fragment bit** - Toggle the button to enable or disable the packets don't need to be fragmented

- **DEAD PEER DETECTION**
  - **Enable VPN** - Toggle the button to enable or disable VPN.
  - **Dead peer Detection Interval** - Enter the timeout interval (in seconds) to detect a dead Internet Key Exchange (IKE) peer. The number of seconds between “heartbeats.” The minimum is 3 seconds, the maximum is 120 seconds, and the default value is 60 seconds.
  - **Failure trigger level (Missed heartbeats)** - Enter the number of missed heartbeats. The minimum is 3 heartbeats, the maximum is 10, and the default value is 3. If the trigger level is reached, the VPN connection is dropped by the security appliance.
  - **Enable IKE dead peer detection on idle VPN settings** - Select this setting if you want idle VPN connections to be dropped by the security appliance after the time value defined in the Dead Peer Detection Interval for Idle VPN Sessions (seconds) field. The minimum time is 60 seconds, the maximum is 3600 seconds, and the default value is 600 seconds (10 minutes).
- **IKEV2 SETTINGS**
  - **Send IKEv2 cookie notify** - Sends cookies to IKEv2 peers as an authentication tool.
  - **Send IKEv2 SPF notify** - Sends an invalid Security Parameter Index (SPI) notification to IKEv2 peers when an active IKE security association (SA) exists.
    - **IKEv2 dynamic client proposal** - SonicOS provides IKEv2 Dynamic Client Support, which provides a way to configure the Internet Key Exchange (IKE) attributes rather than using the default settings.

      Clicking the **Configure** button launches the Configure IKEv2 Dynamic Client Proposal dialog.
      - **DH Group**: Group 1, Group 2,...

        256-bit Random ECP Group

        384-bit Random ECP Group

        521-bit Random ECP Group

        192-bit Random ECP Group

        224-bit Random ECP Group
      - **Encryption**: DES, 3DES (default), AES-128, AES-192, AES-256.
      - **Authentication** : MD5, SHA1 (default), SHA256, SHA384, or SHA512.
- **OTHER SETTINGS**
  - **Clean up Active Tunnels when Peer Gateway DNS name resolves to a different IP address** : Breaks down SAs associated with old IP addresses and reconnects to the peer gateway.
  - **Send tunnel traps only when IPV4 changes** : Reduces the number of VPN tunnel traps that are sent by only sending traps when the tunnel status changes.
  - **Use Radius in** : When using RADIUS to authenticate VPN client users, RADIUS will be used in its MSCHAP (or MSCHAPv2) mode. The primary reason for choosing to do this would be so that VPN client users can make use of the MSCHAP feature to allow them to change expired passwords at login time.

- **MSCHAP and MSCHAPv2** : Click the radio button to select the mode. Click **Configure** to view additional settings
    - **DNS Servers** - Selecting this option automatically populates the DNS and WINS settings. This option is selected by default.
    - **Specify Manually**- If you do not want to use the SonicWall security appliance network settings, select Specify Manually, and type the IP address of your DNS Server in the DNS Server 1 field. You can specify two additional DNS servers.
    - **WINS Server** - Configure a WINS server in the WINS Server 1 field. You can configure a second WINS server, also.

10

# SD-WAN Topology

This feature enables to deploy and monitor an enterprise-wide SD-WAN network by using an intuitive self-guided work flow. It centrally establishes and enforce application-based traffic and other traffic steering configurations across and between thousands of sites.

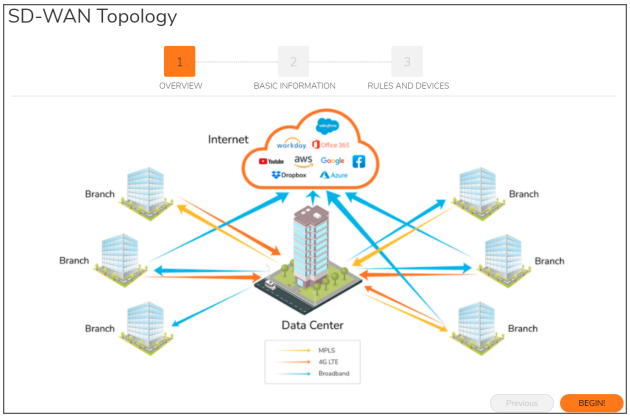
The new design topology enables you to create the work flow in 3 steps.

**Topics:**


- Configuring SD-WAN
- Service Rule
- Application Rule


## Configuring SD-WAN

Navigate to **Manager View | SD-WAN Topology** page and click **Begin**.



**Topics:**

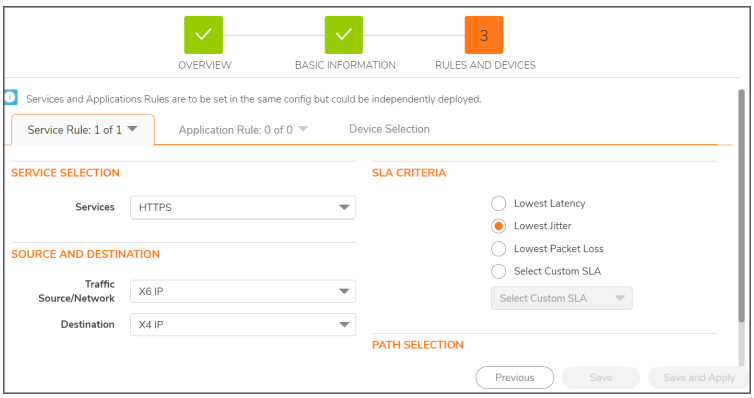
- Basic Information
- Rules and Devices
- Service Rule
- Application Rule
- Device Selection

# Basic Information

1. **Config Name** - Enter a Configuration Name in the text box. If this field is left blank, the system automatically assigns a name to this template.
2. **Traffic Type** - Choose Traffic type as Internet or Branch Data Center.
   **Internet** - This option can be used for all internet-based applications such as ring central, office 365 etc.
   **Branch Data Center** - This option can be used for applications that are running on the data center. A VPN Topology needs to be created as a prerequisite for this option, so that VPN tunnels are available for Path selection. To add a new topology, refer IPsec VPN Topology.
3. **Description** - Enter a description to identify the configuration.
4. **Tags** - Enter a tag to identify.
5. **Device Type** - Choose the device type from SonicOS or SonicOS.
   **NOTE:** You cannot change the device type once it is saved.
   Click **Next** to continue or **Previous** to go back.

# Rules and Devices

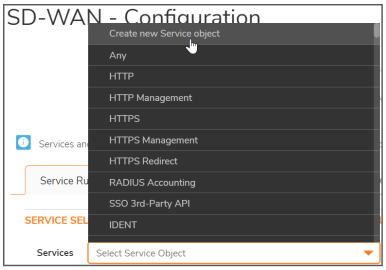
Rules and Devices screen allows you to choose Service Rule, Application Rule, and Device Selection.

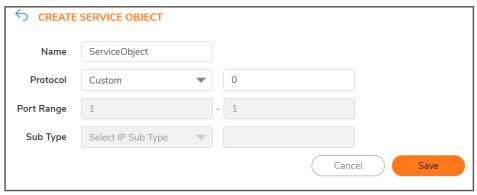



# Service Rule

### SERVICE SELECTION

Services - From the drop down list, you can use the predefined service objects. You can also create a new Service Object by choosing Create new Service object. Services and Applications Rules are to be set in the same configuration, but could be independently deployed.




- **Name** - Enter a name to identify the Service Object.
- **Protocol** - From the drop down list, you can use the predefined protocol. If you want to use a custom protocol, choose **Custom** from the drop down list. Enter the custom protocol in the text box.
- **Port Range** - For some of the predefined protocols, the port range is selected by default.
- **Sub Type** - Choose a Sub Type from the drop down list. This field is available only for selected protocols.

# SLA Criteria

Choose the SLA from the following options by clicking the radio button.

- Lowest Latency
- Lowest Jitter
- Lowest Packet Loss
- Select Custom SLA - To create custom SLA, select Custom SLA.

# SOURCE AND DESTINATION

Choose the source and destination using the drop down list.

- Traffic Source / Network - From the drop down list, choose a source.
- Destination - From the drop down list, choose a destination.

# PATH SELECTION

These are the settings that help determine the network path that fulfills a specific network performance criteria, from a pool of available network paths.

**NOTE:** There should be minimum 2 interfaces selected in the path selection.

**WAN Interface** - From the drop down list, choose WAN Interface. You can also add Physical and Virtual Interface. You can select multiple WAN Interfaces, which will be used for load-balancing as well as dynamic path selection based on the SLA criteria.

**Physical Interface -** Following are the fields for physical interface

- **By Name** - Use "By Name" to add a specific physical interface with a label. Examples: X20, U15, W18.
- **By Range** - Use "By Range" to add a range of physical interfaces with a common label. Examples: X20-X30, U15-U20, W18-W19.

After choosing the option, click Add to add the physical interface. elect Virtual Interface to view additional settings

**Virtual Interface** - Following are the fields for Virtual interface

**INTERFACE SETTINGS - GENERAL**

- Zone - Input a zone name.
- VLAN Tag - VLAN tag 0 or 1
- Parent Interface - Choose an interface from the drop down list.
- Mode / IP Assignment - From the drop down list, choose the mode as Static IP, Tap, Wire, DHCP.
- IP Address - Enter a valid IPV4 address.
- Subnet Mask - Enter a subnet mask address.
- Default Gateway (Optional) - Enter Default Gateway address. This field is optional.
- Comment - You can enter a comment and this field is optional.
- Add rule to enable redirect from HTTP to HTTPS - Toggle to enable or disable the rule.
- MANAGEMENT - Toggle the button to enable or disable the options from HTTPS, Ping, SNMP, SSH.
- USER LOGIN - Toggle the button to enable or disable the user login options from HTTP and HTTPS.

**INTERFACE SETTINGS - ADVANCED**

- Link Speed - Enter the link speed. You can choose the default MAC address which is 00:00:00:00:00:00 or override the default address by typing in the box below.
- Enable Auto-Discovery of SonicWall Switches - Toggle this to enable or disable auto discovery of SonicWall Switches.
- Enable flow reporting - Toggle this to enable or disable flow reporting on flows created for this interface
- Enable Multicast Support - Toggle this to enable or disable multicast Reception on the Interface
- Exclude from Route Advertisement (NSM, OSPF, BGP, RIP) - Toggle this to enable or disable. Enabling this option will exclude the interface from Route Advertisement.
- Enable Default 802.1p CoS - Toggle this to enable or disable 802.1p. After it is enabled, choose an option from the drop down list.
- Enable Asymmetric Route Support - Toggle this to enable or disable asymmetric Route Support on the Interface.

**Backup WAN Interface** - From the drop down list, choose backup WAN Interface.

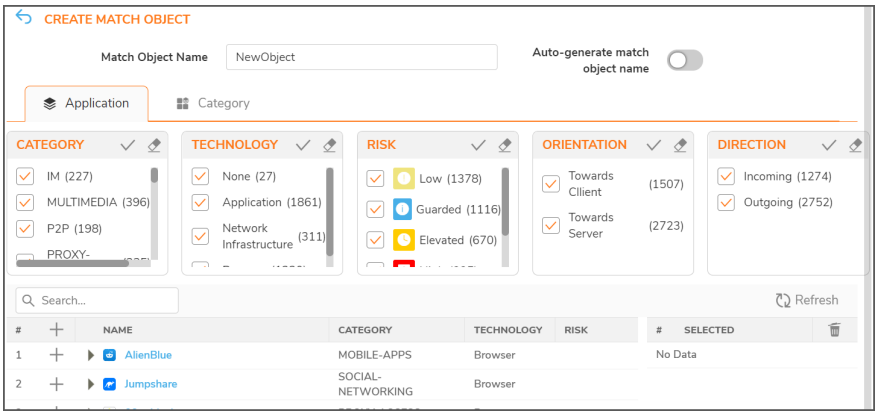
## WAN INTERFACE HEALTH CHECK PROBES

- Probe Target - Choose the Probe Target from the drop down list.
- Probe Type - Choose the type as Ping or TCP and enter the value in the text box.

# Application Rule

### APPLICATION SELECTION

From the drop down list, you can use the predefined application objects (if any). You can also create a new Application Object by choosing **Create new App object**. You can specify an app object name or enable auto generated name by toggling the button.
Go to **Category** tab and select the desired category from the list.



# Device Selection

This screen shows the devices that are selected and the group that they belong to. You can assign as data center, branch office or unassigned from the options listed.
Once the settings are changed, click **Save and Apply** to proceed saving the changes or **Previous** to go back to the previous screen.

You need to commit and deploy the changes so that the changes are pushed to the devices. To perform commit and deploy, refer Committing and Deploying the Updates

11

# CSC Users

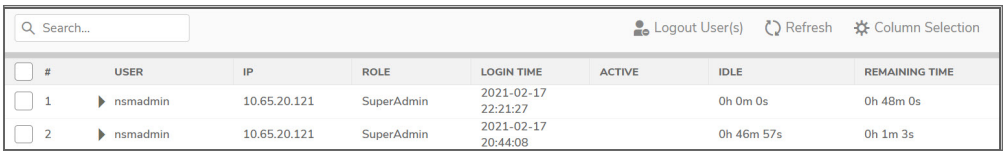
The **Manager View | CSC Users** command set provides information on all the users that have been setup for access to the tenant you have logged into. Those users can manage firewalls through NSM, based on user roles assigned to them.

**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.




The following information is displayed for each active user session:

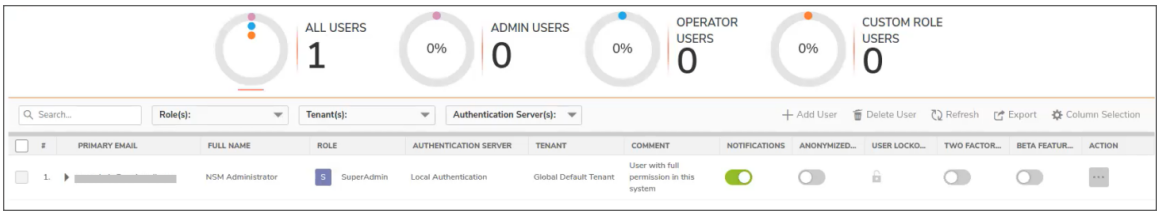
| Term | Definition |
|---|---|
| **USER** | User that has an active session. |
| **IP** | IP address of the system that hosts user session. |
| **EMAIL** | Email address of the user. |
| **ROLE** | Management role of the user. |
| **LOGIN TIME** | Timestamp of the user login. |
| **ACTIVE** | Activity 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.

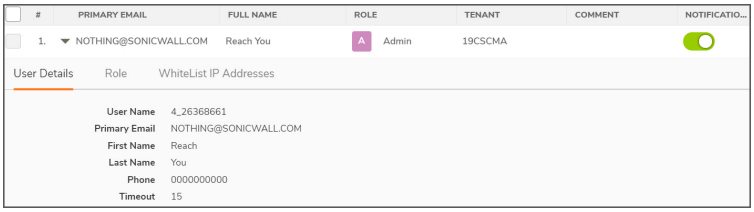



The table on the **Users** page gives the following details for any user listed:

| 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.<br>• **SuperAdmin**- Provides complete access to the user. User can add or update or delete the following: **Users**, **Tenants**, and **Devices** in MSW. This user has the ability to reset password in case if the user has forgotten the login password.<br>• **Admin** - User can configure firewall; edit **UserInfo** (Email/timeout); add or delete devices in MSW<br>• **Operator** - User can configure firewalls.<br>• **Support** - No Configuration Mode; user can only view firewall configurations.<br>• **ReadOnly** - No Configuration Mode; user can only view firewall configurations.<br>• **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. |
| **ANONYMIZED USAGE DATA** | A switch that allows or disallow NSM to collect anonymized usage data. |

| Term | Definition |
|---|---|
| **BETA FEATURES** | A switch that enables or disables beta features for a user. |
| **ACTION** | Provides the options edit or delete a user. |

Expand each user to view additional information:




**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.

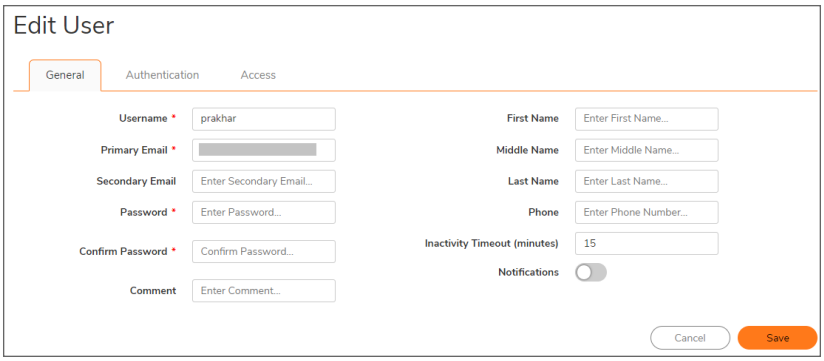
At any time you can export the data to a CSV file by clicking the **Export** icon.

# Editing CSC Users

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

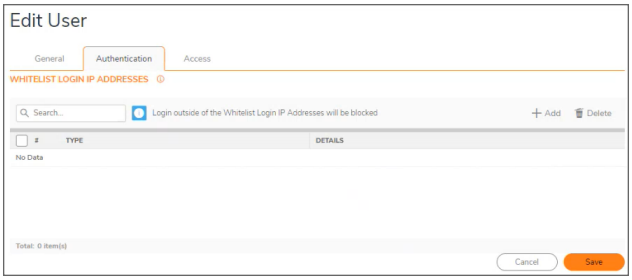
***To update user information:***

1. Navigate to **Manager View | CSC Users > Users**.
2. Click the **Edit** option in the **ACTION** column of the user you want to edit.

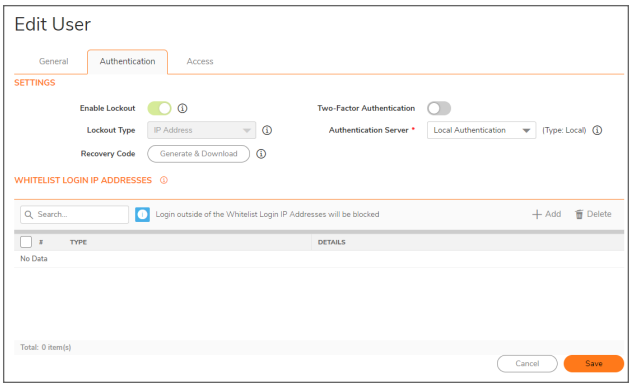



3. In the **General** tab, enter the following and click **Save**:
    - **Secondary Email**—Secondary email address of the user.
    - **Comment**—Any valid comment.
    - **Notifications**—Enable or disable notifications.
    - **Timeout**—The duration after which the user is logged out.
4. For Authentication Server, choose **Local Authentication** or **CAC (Common Access Card)** from the list.
5. Click on the **Authentication** tab.

**NSM SaaS Interface**:




**NSM On-Prem Interface**:



6. In the **Authentication** tab, the **SETTINGS** section is available only for **NSM On-Prem** and not for **NSM SaaS**.

   Under **SETTINGS** (only for On-Prem users):

   a. You can **Enable Lockout**, which will lockout a user for some time after repeated failed login attempts to protect user credentials.

   b. Select the **Lockout Type** from the dropdown options: **IP Address**, **User**.

      IP Address - User is locked out only from the Source IP Address used for failed logins.

      User - User is locked out from all IP Addresses.

   c. You can enable the **Two-Factor Authentication**.

   d. Select the **Authentication Server** from the dropdown.

   e. You must generate and download the **Recovery Code**. This **Recovery Code** along with OTP sent to Email Address configured in SMPT settings is used to reset the NSM Password in case if login password is forgotten.

      ⓘ | **NOTE:** This feature is available only for Super Admin users.

      ⓘ | **NOTE:** SMTP Server under **System | Settings > Administrator > Notifications** has to be configured to get OTP while resetting.

      ⓘ | **NOTE:** This Recovery code can be used only one time. It has to be regenerated once used.

   Under **WHITELIST LOGIN IP ADDRESS**:

   a. You can Whitelist login IP addresses. The IP address that are not added in the Whitelist Login IP Addresses will be blocked.

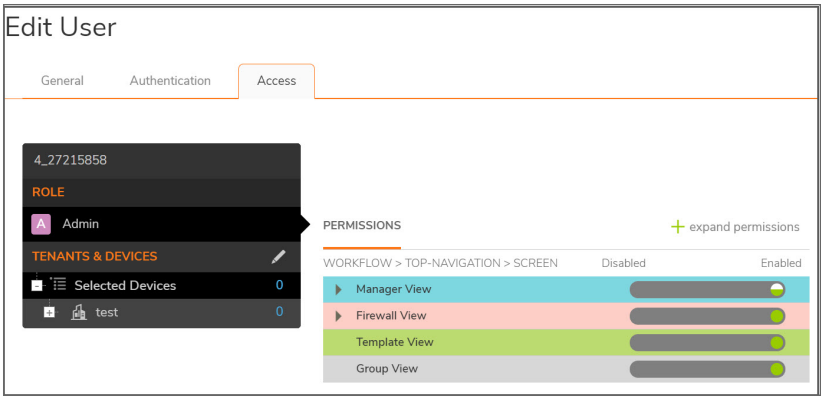
      ***To Whitelist login IP addresses:***

      1. Click **Add**.
      2. Select the **Network Type** from the dropdown options: **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.
      3. Enter the **IP address** to be whitelisted.

4. Click **Save**.

b. Click **Save**.

7. Click the **Access** tab to see the various permissions and devices access.




8. In the Access tab,

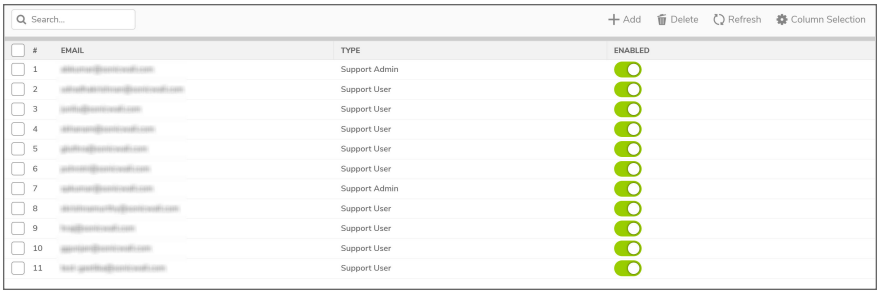
a. Click on the **Role** to see the permissions granted to this user. Yo can click the **+** icon to expand the permissions list to see the detail behind it. Click again to collapse permissions.

b. Click the Edit icon in **TENANTS & DEVICES** to associate tenants and devices together and click **Apply**.

c. Click **Save**

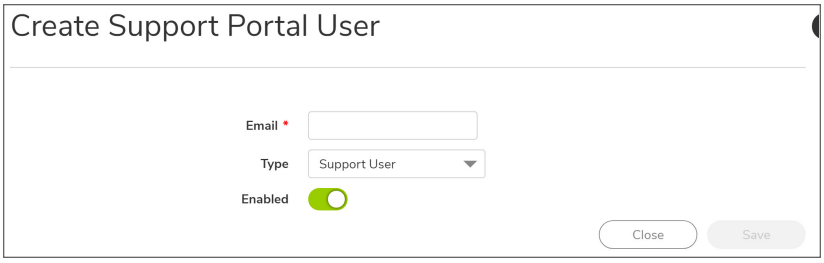
# Support Portal Users

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.




***To create a Support Portal user:***

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

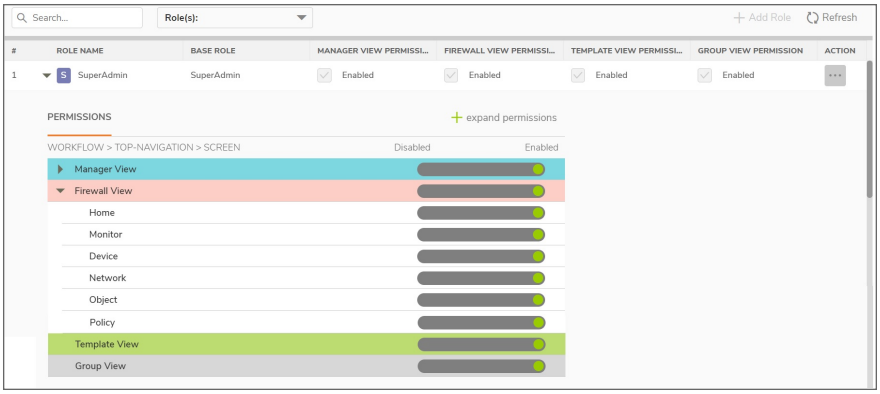



3. Type the email of the user you are adding.
4. Select the type of user from the drop-down list.
5. Enable the user's access.
6. Click **Save**.

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

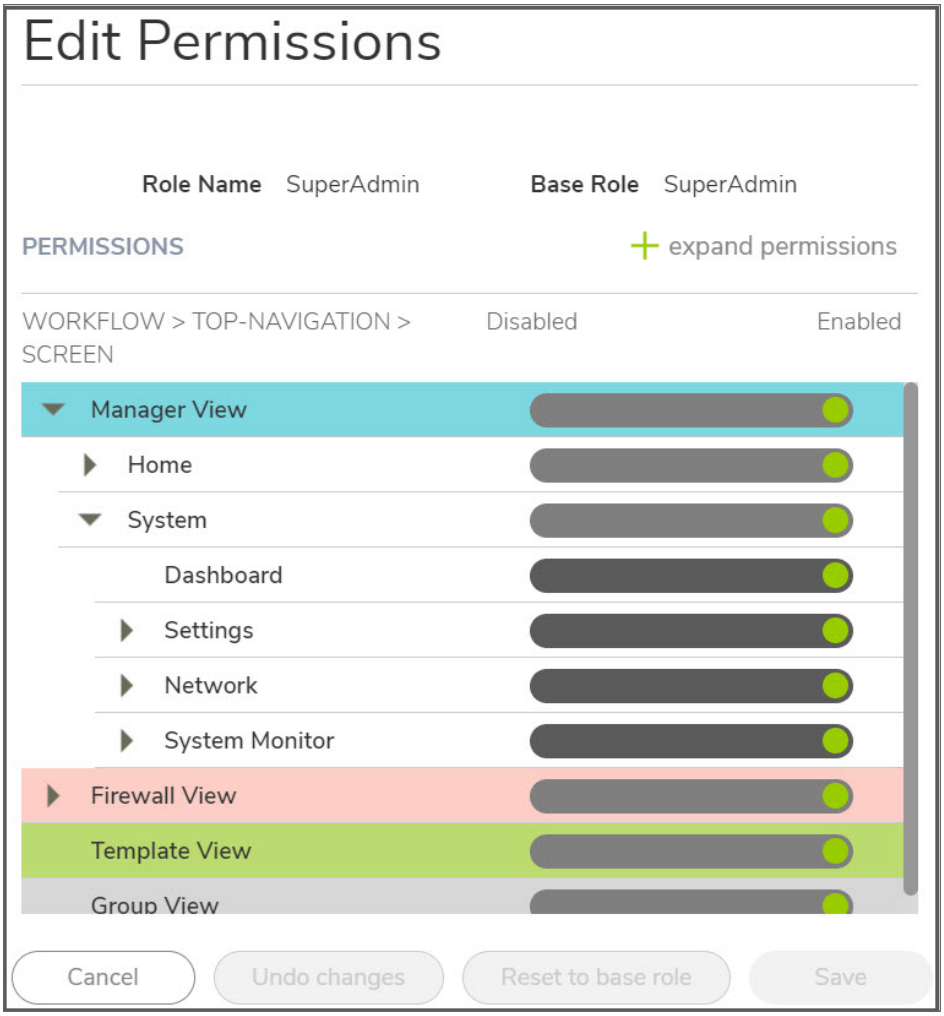
# Roles and Permissions

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.


Search...
Role(s):
Add Role
Refresh
#
ROLE NAME
BASE ROLE
MANAGER VIEW PERMISSI..
FIREWALL VIEW PERMISSI..
TEMPLATE VIEW PERMISSI..
GROUP VIEW PERMISSION
ACTION
1
SuperAdmin
SuperAdmin
Enabled
Enabled
Enabled
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.

   ⓘ **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.

# Authentication Servers

This feature is specific to On-premises solution where you can add the authentication types like **Active Directory, LDAP, RADIUS** and**, Digital Certificate**.

***To add authentication servers:***

1. Click **Add** to add new authentication servers.
2. Authentication Type - There are four options to choose - **Active Directory, LDAP, RADIUS** and**, Digital Certificate**. This indicates the type of the Remote Authentication Server if it is an LDAP server, a Windows Active Directory, a RADIUS Server or a Digital Certificate. The configuration values for Active Directory and LDAP are same.

## Add Authentication Server - Settings

- **Name** - Enter the name to identify the authentication server.
- **IP/FQDN** - The hostname or the IP address of the Remote authentication server. Example: [mydc.example.com], [X.X.X.X] (ip address), [company.com].
- **Port** - The default LDAP over TLS port number is TCP 636. The default LDAP(unencrypted) port number is TCP 389, but you can select from the Standard port choices drop-down menu for more options. If you are using a custom listening port on your LDAP server, specify it here.
- **Protocol Version** - Choose a protocol version from the list. This is the LDAP protocol version on which the remote LDAP/AD server is running on
- **Base Distinguished Name** - A distinguished name, that is, a globally unique name for a user. The base DN for a directory (say example.com) should be written in the form: [dc=example,dc=com].
- **Use SSL** - Toggle this option to specify whether to use SSL for binding to the remote server. This is strongly recommended. For this, the remote server's CA certificate or the root certificate of the CA that signed the server's certificate should be present in KeyStore of SGMS as trusted CAs.
- **SSL Port** - The default value is 636 in case of LDAP/AD servers.
- **Anonymous Login** - Some LDAP servers allow for the tree to be accessed anonymously. If your server supports this (MS AD generally does not), then you could select this option.
- **Login User Distinguished Name** - Distinguished name is used to authenticate to Directory Server when performing a bind. The value for this field should be specified as a DN (Distinguished Name). Example: [uid=xyz, ou=People, dc=example, dc=com] , [cn=jdoe, cn=users, dc=sv, dc=company, dc=com]
- **Login Password** - Enter the password for the login user DN.
- **Connection Timeout (msecs)** - Timeout period(in milliseconds). After this period of time, the connection attempt with the remote server will be given up if it is not successful.

# Authentication Type - RADIUS

### PRIMARY RADIUS SERVER

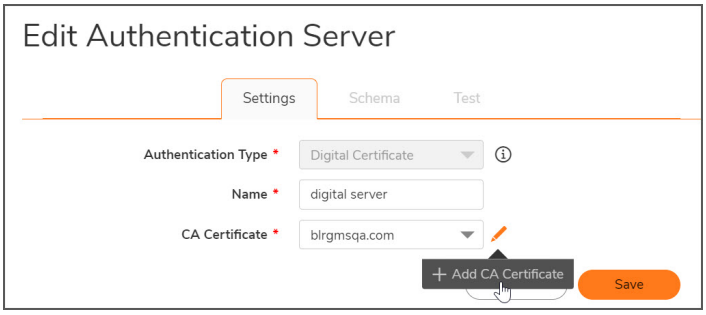
- **IP/FQDN** - The hostname or the IP address of the Remote authentication server. Example: [mydc.example.com], [X.X.X.X] (ip address), [company.com].
- **Port** - The default LDAP over TLS port number is TCP 636. The default LDAP(unencrypted) port number is TCP 389, but you can select from the Standard port choices drop-down menu for more options. If you are using a custom listening port on your LDAP server, specify it here.
- **Shared Secret** - The alphanumeric Shared Secret can range from 1 to 31 characters in length. The shared secret is case sensitive.
- **Authentication Protocol** - From the drop down list, choose the RADIUS Authentication Protocol to be used for authentication.
- **Radius Timeout (seconds)** - The allowed range is 1-60 seconds with a default value of 5.
- **Max Retries** - Enter the number of times SonicOS will attempt to contact the RADIUS server. If the RADIUS server does not respond within the specified number of retries, the connection is dropped. This field can range between 0 and 10, with a recommended setting of 3 RADIUS server retries.

### BACKUP RADIUS SERVER

- IP/FQDN
- **Port** - The default LDAP over TLS port number is TCP 636. The default LDAP(unencrypted) port number is TCP 389, but you can select from the Standard port choices drop-down menu for more options. If you are using a custom listening port on your LDAP server, specify it here.
- **Shared Secret** - The alphanumeric Shared Secret can range from 1 to 31 characters in length. The shared secret is case sensitive.

# Authentication Type - Digital Certificate

- Name - Enter the name to identify the authentication server.
- CA Certificate - From the drop down list, choose any existing certificates. To add a new certificate, click Edit icon and select Add CA Certificate.



- Select **Import a local end-user certificate with private key from a PKCS#12 (.p12 or .pfx) encoded file.**
- Next, enter the **Certificate Name** and the **Certificate Management Password** (the password you defined when creating the .pfx file). Click **Import**.
- **Import a CA certificate from a PKCS#7 (.p7b), PEM (.pem) or DER (.der or .cer) encoded file**
- Click **Add File** and browse to locate and open your Certificate .pfx file. Click **Import** to import the selected certificate.

# Add Authentication Server - Schema

**USER DIRECTORY LDAP SCHEMA**

- LDAP Schema - From the list choose the desired option. Selecting any of the predefined schemas will automatically populate the fields used by that schema with their correct values. Selecting User defined will allow you to specify your own values – use this only if you have a specific or proprietary LDAP schema configuration.

**USER OBJECTS**

- **Object Class** - Select the attribute that represents the individual user account. The name of one of the standard object classes that the users belong to.
- **Login Name Attribute** - The attribute name on the LDAP/AD server which represents the user id. This is the attribute on the LDAP server whose value would be used as the user id on the SGMS Login Page. *Example*: uid, sAMAccountName etc.
- **First Name Attribute** - The attribute name on the LDAP server which represents First Name. *Example*: givenName.
- **Last Name Attribute** - The attribute name on the LDAP server which represents Last name. *Example*: sn.
- **Email Attribute** - The attribute name on the LDAP server which represents email id. *Example*: mail.
- **Telephone Attribute** - The attribute name on the LDAP server which represents Telephone number. *Example*: telephoneNumber.

**USER DIRECTORY LDAP SCHEMA**

- **Allow Only AD Group Members** - Toggle the button to allow or deny AD Group Members. When enabled, it allows only those users that are members of the specified Active Directory Groups to login into NSM. With this option, it is also necessary to select the Host Type as [Active Directory] on the Settings Panel.
- **Active Directory Group(s)** - Specify the AD Group names, members of which should be allowed to login into NSM. Multiple AD Groups can be specified as semicolon delimited. Example: [NSMUsers], [ADGroup1;AD group2;NSM Users;Group4]

12

# Scheduled Reports

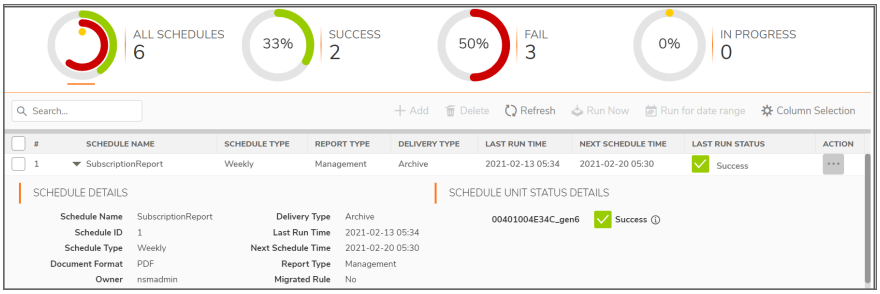
You can set up schedules to generate reports at regular intervals. As part of scheduling, you need to specify the following: **report type and the type of information that you wish to include**; **devices or groups for which the reports should be generated**; **how often the reports are delivered**;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

**Topics:**


- Creating Scheduled Reports
- Editing Schedule
- Running Reports Manually
- Archived Reports


## 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.




### SCHEDULES TABLE

| Term | Description |
|---|---|
| **SCHEDULE NAME** | Name of the scheduled report. |

| Term | Description |
|---|---|
| **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. |
| **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, **CTA** (Capture Threat Assessment) report, **Management** report or **Firewall Summary** 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**, **Management**, or **Firewall Summary**.
      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.

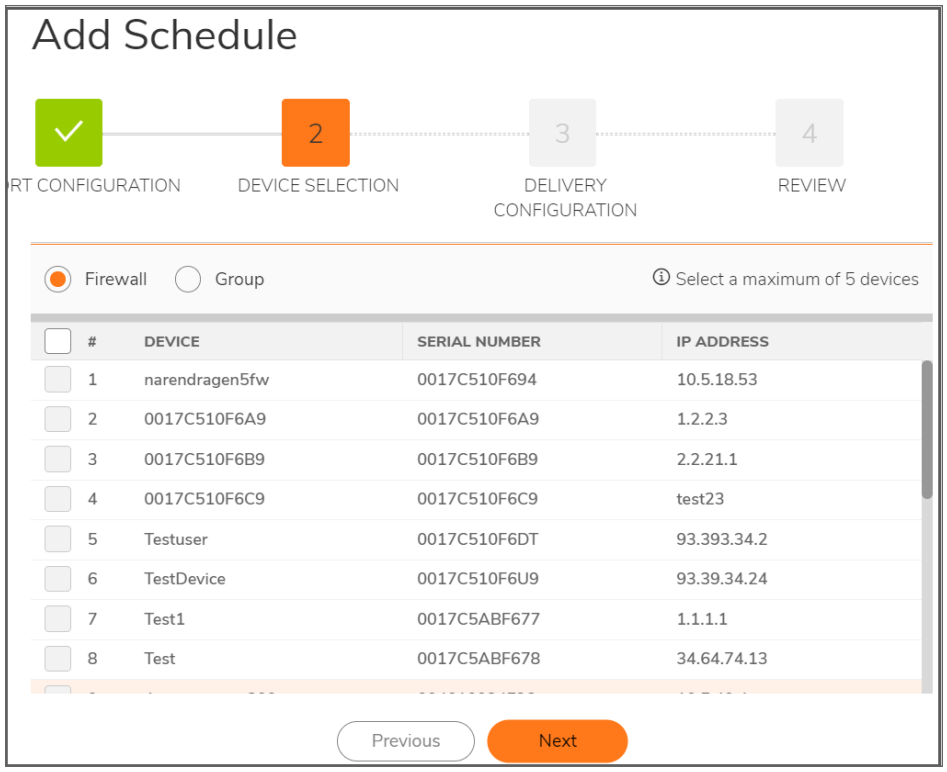
d. Select the type of information you want in your report from the options displayed. You can include all the data by selecting **Select All**.

e. Click **Next**.

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

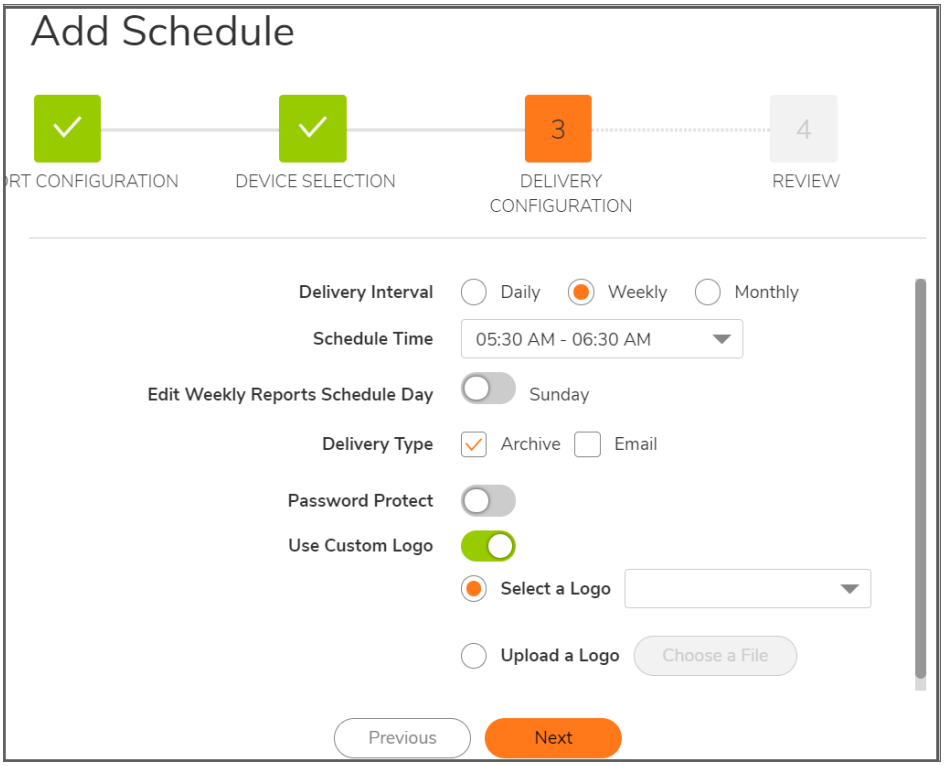
a. Select one of the following options: **Firewall**—to select firewalls, **Group**—To select device groups, or **Tenant**—To select the tenant you have logged into.

**Tenant** option is not available for **Flow** Reports.

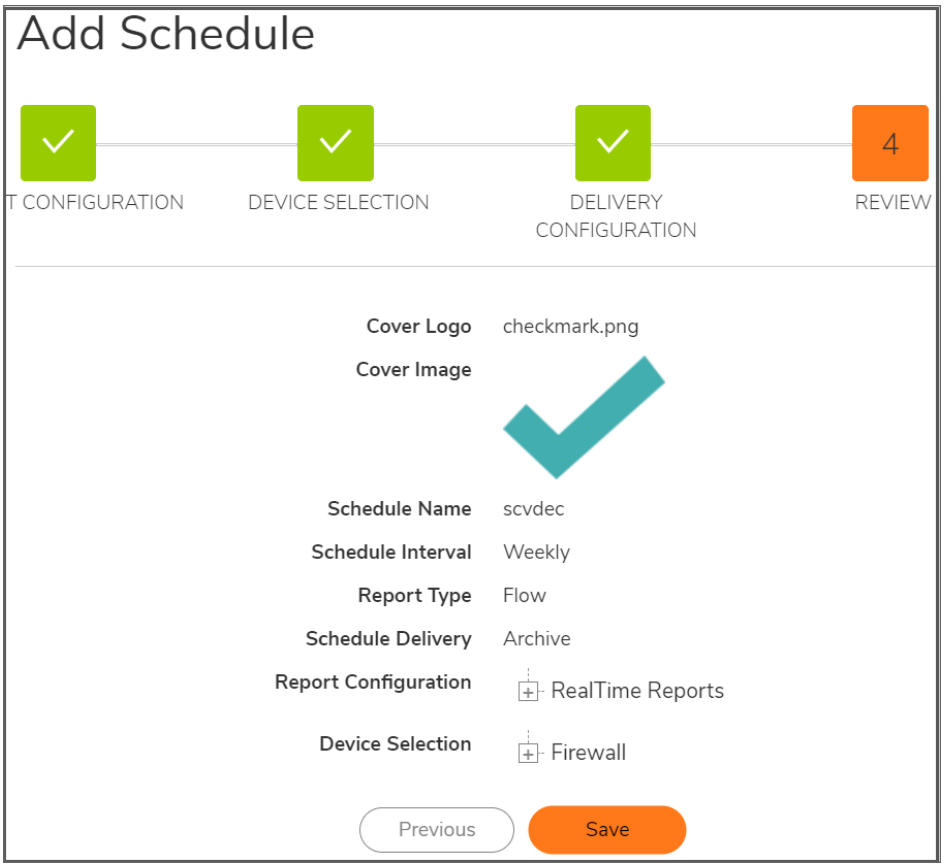



b. Click **Next**.

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




    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.**

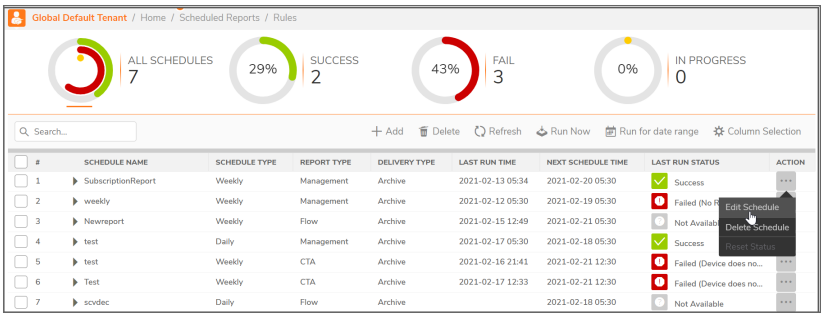



If you have successfully created a scheduled report, a success message is displayed. The newly created report is displayed on Rules page.

# 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**.



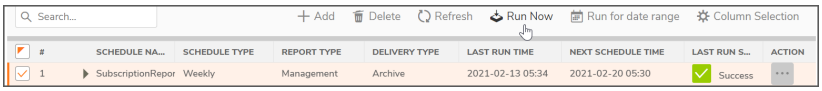

3. You can make necessary changes in the **CREATE SCHEDULE** wizard.
   See Creating Scheduled Reports for reference.

# 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:***

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




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

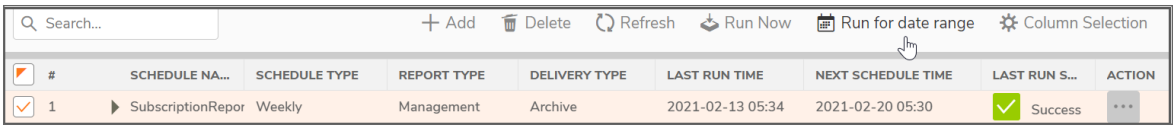
If you had configured **Archive** as one of the **DELIVERY TYPE** options for the scheduled report, the report you generated is available for download. For more information on working with the archived reports, see Downloading Archived Reports.

# Setting the Report Date Range

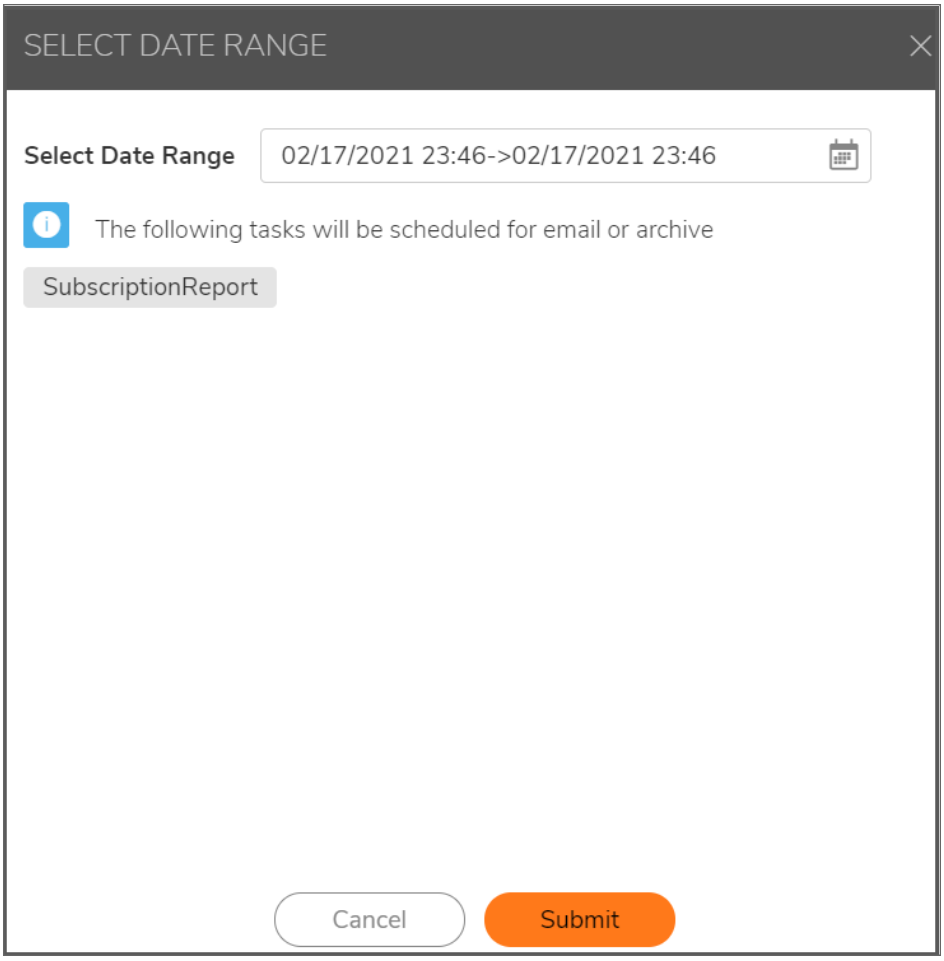
To generate a report to obtain data over a custom period, you need to specify the date range.

***To set the date range:***

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




3. 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.

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

13

# System Events

NSM maintains an Event log for tracking potential security threats.

**Topics:**


- Configuring Log Settings
- Alerts and Notifications
- Configuring Twilio Setting for SMS
- Viewing System Events


# 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.

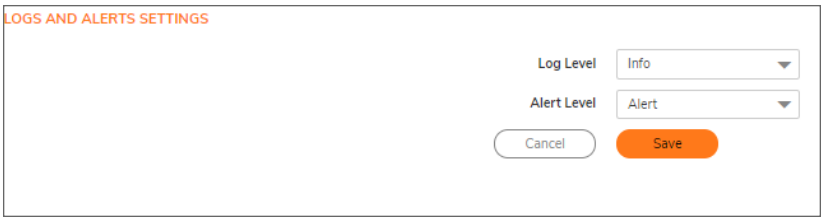
ⓘ | **NOTE:** Debug log settings can be performed only by Super Admins or Tech Support representatives.

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.



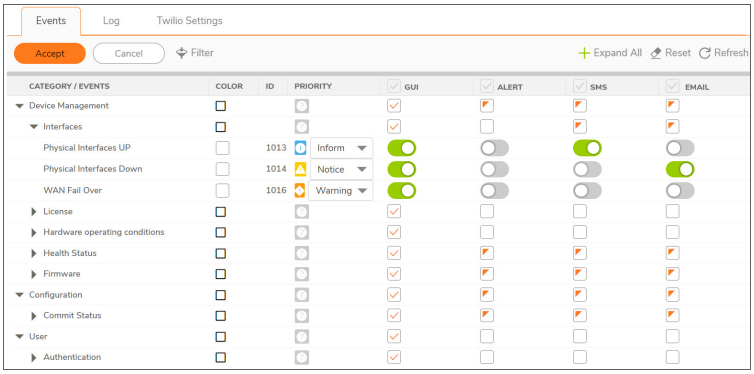

3. Click **Save**.

# Alerts and Notifications

In the new settings screen, you can now view the **CATEGORY / EVENTS** and change the priority of the event based on their severity. The alerts and notifications can be customized and change the way they display in the Notification center or alert.

When enabled, a notification or alert is triggered in a event level.

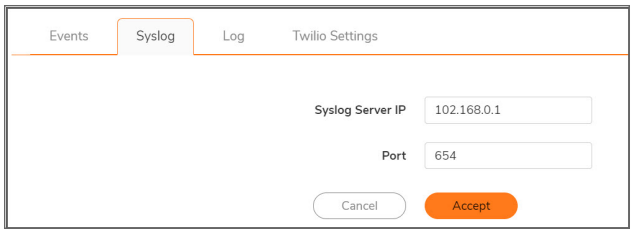
**NOTE:** It is recommended to upgrade to the latest firmware for the alerts to be triggered. Refer Upgrading SonicOSX Firmware.




### Category

- **Device Management**
  - **Interfaces** - Device Physical Interfaces status whether it is up or down.
  - **License** - Alerts the user when any of the previously activated firewall security services or NSM licenses are expiring.
  - **Hardware operating conditions** - Alerts when there is a hardware failure with Fan, power supply, network cards reset, and system disk status.
  - **Health Status** -Alerts when a device is disconnected with NSM or a local change is made to the firewall outside of NSM , and when device goes into unmanaged state.
  - **HA Failover** - Alerts if a primary or a secondary device fails or in the case of a failover.

        - **Firmware** - Alerts when there is a new firmware version available and if a firmware upgrade fails or applied successfully to the firewall.
    - **Configuration**
        - **Commit Status** - Alerts when a new firewall configuration commit from NSM fails on the firewall or successfully applied.
    - **User**
        - **Authentication** - Alerts when the user logs in and logs out .

| Term | Definition |
|---|---|
| **CATEGORY / EVENTS** | The events are displayed in a category. Expand each category to view the associated events. |
| **COLOR** | This helps color code the events in the Events page. |
| **ID** | Unique ID of the event. You can use this ID to search for a particular event in the Filter. |
| **PRIORITY** | Priority of the event. Expand each event and choose an option from the drop down. The available priorities are **Emergency, Alert, Critical, Error, Warning, Notice, Inform, Debug, Mixed**. |
| **GUI** | Choose to enable or disable the event to be displayed in the graphical user interface (GUI) under Notification center. Toggle each event to enable or disable the notification. If you check the box at the category level, it gets disabled for all the events listed under the category. |
| **ALERT** | Choose to alert and send the notifications in the group. |
| **SMS** | When enabled, an SMS is sent to the registered phone number of the user in the tenant. To view the contact information, refer Users. |
| **EMAIL** | Choose this option to receive notifications through email. |
| **SYSLOG** | You can configure the syslog information by clicking the **SYSLOG** tab on the top. Enter the Syslog Server IP and Port and click **Accept**.<br>  |

**Expand All** - Expands all the categories and displays the events.

**Reset** - Resets all the alerts and notifications to default settings.

**Refresh** - Refreshes the information.

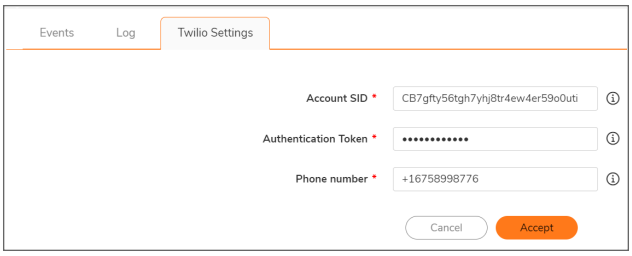
**Accept** - After you make any changes to the notifications, click **Accept** to save them.

**Filter** - Lets you to filter the events by name, priority, ID.

# Configuring Twilio Setting for SMS

***To configure Twilio setting for SMS:***

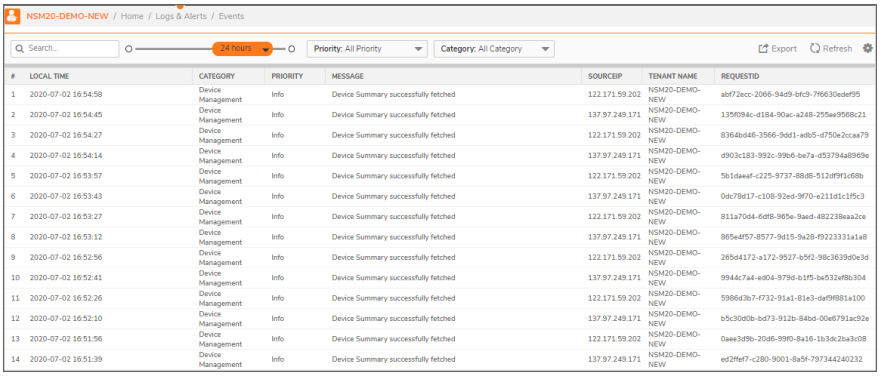
1. Create a Twilio SMS acccount
    a. Create a Twilio SMS account at www.twilio.com
    b. Enter in credit card information to create an account with full privileges.
    c. Purchase a phone number with Programmable SMS capabilities.
    d. Record your Account SID and the Authentication Token values on your main twilio.com/user/account page.
2. Configure Twilio setting in Network Security Manager
    a. Open the Network Security Manager Dashboard.
    b. Navigate to the **Logs and Alerts > Settings** page.
    c. In the **Twilio SMS Setting** section, enter your:
        - **Twilio Account Sid**
        - **Auth Token**
        - **Twilio Phone Number**




ⓘ **NOTE:** You will now be billed on a per-SMS basis via Twilio. Prices can range by country. A complete, up-to-date pricing list is available at https://www.twilio.com/sms/pricing#outbound-pricing.

# Viewing System Events

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




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.<br>• Emergency<br>• Critical<br>• Alert<br>• Error<br>• Warning<br>• Notice<br>• Info<br>• Debug<br>• Trace<br>• Trace 2 |
| **Category** | Category of the event.<br>• All Category<br>• Notification<br>• Configuration<br>• API<br>• Device Management<br>• Reporting and Analytics<br>• Reporting<br>• 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 |

14

# SonicWall Support

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

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

The Support Portal enables you to:

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

# About This Document

Network Security Manager Administration Guide
Updated - July 2024
232-005314-01 Rev R

Copyright © 2024 SonicWall Inc. All rights reserved.

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

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

## End User Product Agreement

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

## Open Source Code

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

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