# Network Security Manager

## About NSM

# Contents

1

# About Network Security Manager

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. This cloud solution automates the steps to set up an appliance and offers robust reporting and management tools.

**Topics:**

- About NSM
- Related Documents
- API Support
- Legal Information
- Conventions

## About NSM

SonicWall Network Security Manager (NSM) is the next generation firewall management application that provides a holistic approach to security management. The approach is grounded in the principles of simplifying and automating various tasks to achieve better security operation and decision-making, while reducing the complexity and time required. NSM gives you everything you need for firewall management; comprehensive visibility and granular control and the capacity to govern the entire SonicWall network security operations with greater clarity, precision, and speed.

This is all managed from a single, function-packed interface that can be accessed from any location using a browser-enabled device. Firewalls can be centrally managed to provision all of the network security services with a single-pane-of-glass experience.

SonicWall NSM provides both on-premise and cloud options. The user experience and features differ for both the on-premise and the SaaS versions, though the command remains much the same for both. For example, the blue navigation on the left indicates that you are on the NSM on-premise version whereas it is black for NSM on cloud. For more details about the on-premise options, see NSM On-Premises.

For ease of deployment, this security management platform provides a SaaS (Software-as-a-Service) offering. It 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.

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 adds support for the firewall series Gen 7 NSa 2700 and TZ Series running SonicOS as well as NSsp and Gen 7 NSv, with multi-tenancy and unified policy management features.
- Unified Policy Management that provides the integrated management of various security policies for enterprise-grade firewalls. This offers a centralized location for configuring policies.
- Login To Unit that provides admins a fast and easy access to the managed firewall device-level UI directly from the device inventory page of NSM.
- Account Lockout feature, designed to prevent unauthorized access to the NSMenvironment and other brute-force attacks, social engineering, and phishing. This disables the user account if incorrect passwords are entered after a specified number of failed attempts during a given period. Admin can set the lockout duration until the locked account is released either after a specified time or manually done by an administrator when three unsuccessful log in attempts in 15 minutes are exceeded.
- Multi-Device Upgrade Feature to upgrade multiple firewalls from a group of devices in NSM instead of manually upgrading each firewall. Admins can execute them using NSM APIs as well.
- High Availability that allows two identical NSMs to be configured to provide a reliable continuous connection to the public internet.
- Closed Network support feature is ideal for customers that run one or more private networks that are completely shut-off from the outside environment. Customers can license the NSM managed firewall without contacting License Manager (LM) or MySonicWall (MSW), when onboarding and patching SonicWall firewall to preserve the privacy and security of the closed networks.
- Security feature to grant admin rights based on specific IP address ranges. The IP restrictions can be added in 3 formats - single IP, an IP range, or a specific network with a subnet mask.
- Two template types for the devices SonicOS and SonicOSX. This is apart from a master golden configuration template for large customers, to take configuration from baseline devices and apply it to the other devices or groups.
- Configure or edit virtual or network interfaces using templates.
- Certificate management feature that enables a user interface to facilitate the management of digital certificates for all NSM managed firewalls. This enhances trust established between parties in a secure communication session.
- Schedule EXP and TSR Backups feature enables the admins to restore the firewall back faster and easier in an event of SW/HW failure.
- Azure and KVM hypervisor deployments

NSM can manage both Gen6 and Gen7 SonicWall firewalls. SonicOS 6.5.4.6 is the recommended version, but NSM can on-board the older Gen6 Firewall versions as well. The 7-day reporting has minimum version requirement of SonicOS 6.5.4.6.

# 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. |
| *Network Security Manager Administration Guide* | Provides details on NSM features for administering your instance of NSM. | Read this document to learn how to configure and maintain NSM. Use the workflows from above as a checklist for the sequence of actions and feature descriptions. This document applies to both SaaS and On-Premises instances. |
| *Network Security Manager Reporting and Analytics Administration Guide* | Discusses how to use the reporting and analytics features. | Read this document to learn what types of reports are available and how to navigate within them. It also describes how to schedule reports and define their contents. This document applies to both SaaS and On-Premises instances.<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>This document applies to On-Premises instances only. |

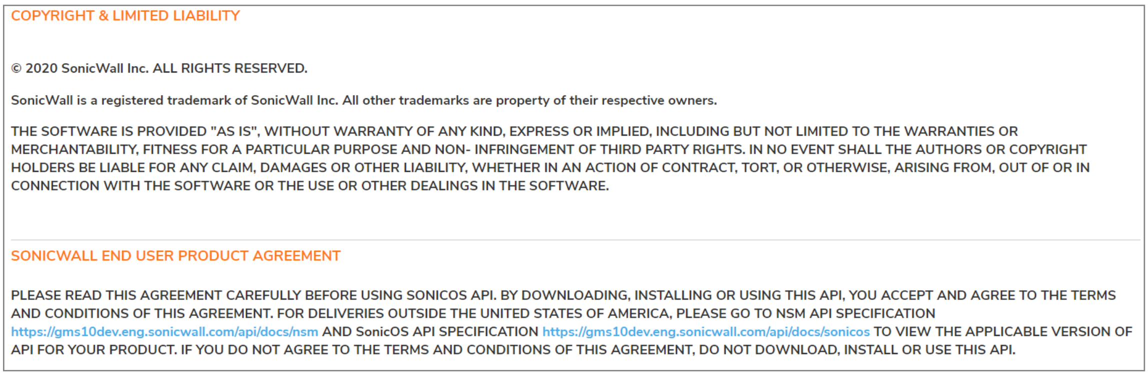
| Document | Description | When to Use It |
|---|---|---|
| *Network Security Manager Getting Started Guide for SaaS* | Describes how to license and configure a basic SaaS NSM instance. | Read this document to learn how to license and configure a SaaS instance of NSM. This document applies to SaaS instances 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://gms10dev.eng.sonicwall.com/api/docs/nsm AND SonicOS API SPECIFICATION https://gms10dev.eng.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.

ⓘ | **NOTE:** The image content differs for the SaaS and the On-premise versions.

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.

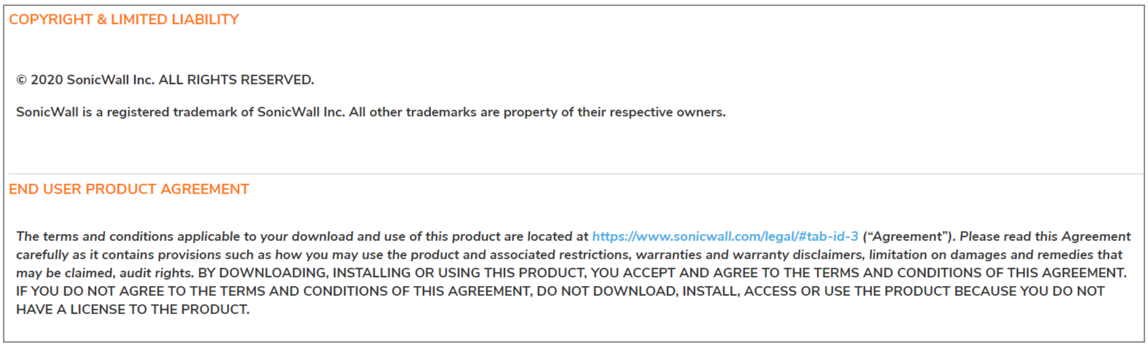
# Legal Information

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 | HOME > 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

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

About Network Security Manager 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**<br>**> 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 |

| Convention | Use |
|---|---|
| | 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.

| 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.<br>Also indicates that a configuration is in sync and acquired. |
| 🕒 | Indicates that a task is in process or pending the completion of another task. The message Pending is usually displayed, as well. |
| ⚠ | Indicates a potential issue or a warning. Messages provide additional detail to help you resolve the issue. |
| ❗ | Indicates an error. Additional information may be provided via an information icon. Click the icon or mouse over it to see the message:<br>For example, Gateway Firewall is not available in CSC. |
| 🛡 | Indicates an alert. |
| 🟢 | Indicates the device is online. |
| 🔴 | Indicates the device is offline. |
| 🔗✕ | Indicates unmanaged devices. |

| Status Icon | Definition |
|---|---|
| ☑ | Indicates managed devices. |
| ? | Indicates that Zero Touch Connection is disabled for a device. |

# NSM Workflows

NSM is specifically designed to deal with the complexities of deploying and managing firewalls. NSM is very easy to use, and the enhancements for Zero Touch deployments ensure that it takes just seconds to on-board a device. Firewalls can be centrally managed to provision all of the network security services with a single-pane-of-glass experience.

NSM provides a unified management experience to address the challenges in the workflow including:

- Governing Centrally
- Managing Risk
- Managing Compliance

## Governing Centrally

NSM with a complete API-ready architecture, helps customers to do the following for governing centrally:

### Step 1: Set the parameters required in MSW

a. **Set up License:** Use MSW to license your site, activate or purchase licenses, to further set up your tenants or groups and access other security solutions.

b. **Set up Tenants:** You can create Tenants in MSW before you start working with NSM. When you bring your infrastructure under NSM, the tenants you have created in MSW are updated automatically in NSM.
The **Tenants** option gives you access to any other tenants. You can also view the tenants from Firewall View alternatively.

ⓘ | **NOTE:** MSW also offers embedded provide assistance where needed.

### Step 2: Register your new or existing devices

You can enable a two-factor authentication code when registering your firewall. Get the serial number and activation key to get the through the firewall. As you register and configure the firewall devices, enable the Zero Touch option for your devices.

## Step 3: Create Device Groups

When the devices are first passed to NSM, all the devices appear in the Unassigned group by default. You can leave them unassigned, but the ease of management come from grouping those with similar policy or management requirements and applying changes to the group. You can define groups based on geography, functions or other business requirement.

## Step 4: Add Devices to the Device Groups

You can select the tenants from the Manager View. NSM allows multiple nesting inside your device groups. You can move a device from an unassigned firewall default group to your desired group from the NSW interface.

## Step 5: Create, Commit, and Deploy Templates

Now certain common rules are to be implemented to the firewalls and this can be easily done with the help of creating a template. By defining a template you can set configuration for multiple devices. You can create a new template, or clone or select an existing one.

As soon as you create a new template, or clone or select one existing template, the Template View is selected. You search for an existing template by going to the **Template Inventory** option to view the list of templates from which view the detailed information of each templates using the expand option.

While creating a template, NSM enables you to do the following:

- **Add, Delete or Modify Address Objects:** When you create a template globally, you can add **Address Objects** required for the template. You can manually add, delete, or modify the address objects. This include the options which may be highly crucial for your business operations, like adding multiple geographical zones, or a global root group. You can also have subgroups with devices nested under it with a parent-child configuration setup. Click the global Template Pane to view the breakdown of all the configurations you have made to the template. You can view the current template definition, tweak the attributes, or modify the parameters further as required.
- **MSSP configuration changes:** MSSP can enforce certain basic requirements or rules in place for all customers, or variations for individual clients. NSM provides unified management experience for MSSP through an API-driven architecture. Templates can also be created at tenant level. The API option in Manage View helps you to automate your tasks on daily basis.
- **Create a template for multiple tenants:** You can create a template and apply the changes globally for multiple tenants. For instance, you can divide your tenants according to the location (for example, North America, Asia, and so on), and set different rules and definitions for each of them.

The types of template you should create include the following:

- **Zero Touch (ZT) Templates:** Though you can manage devices manually, a ZT template is always a suggested best practice to onboard the ZT managed devices with standard configuration. If you configure ZT option for a firewall in MSW, the changes are automatically pushed to the once you login to NSM.
- **Configure Templates for multiple branches:** Templates help build flexibility and efficiencies into

the process of applying policies to your devices:

  - Create configuration templates for multiple branches with different policy requirements.
  - Create, clone, or select an existing template for each group of devices or independent device.
  - Create a global template and assign an address object to it, including names and zones.
  - Create variables for subgroups or particular IP addresses and deploy that to multiple firewalls used within a distributed enterprise.
- **Commit the changes in a scheduled time:** The changes you defined in the templates are still in NSM but are not deployed yet. Committing the changes is rather locking or saving them, or just scheduling it. You have to push these changes to firewall to deploy them. You can either commit them to deploy right away, or you can either schedule time for it too.
- **Push:** After you save, validate, and approve the committed configuration options, you may need to push the configuration template manually to all ZT managed devices. Click the **Commit and Deploy** option to implement the changes in effect. You can also view the **Pending Configuration Changes** before you push the commit.

# Managing Risk

NSM can also be instrumental in the ongoing monitoring and troubleshooting issues.

**Topics:**

- Case 1: Troubleshooting Performance Issues
- Case 2: Analytics and Visibility
- Case 3: Notifications of Alerts
- Case 4: On-boarding Administrators

## Case 1: Troubleshooting Performance Issues

NSM reporting options help you troubleshoot the issues and manage the performance with a quick glance. It aggregates a broader view of crucial information, which it presents in the **Dashboard**, **Notification Center**, and various summary reports. The Notification Center alerts you to the critical issues that need your immediate attention and you can deep dive into the detailed reports Live MONITOR option.

For example, a particular firewall has a performance issue, you can view the threat in the Dashboard. You can drill down to the issue further using Live Monitor, analyze the issue, and take immediate action. For instance, if you identify certain applications that hog the bandwidth of a network, you can go to Manage View, access the template, and make changes to the configuration to protect yourself. You might block the applications that are using larger bandwidth or even isolating the firewall, and thus remediate the issue.

## Case 2: Analytics and Visibility

The daily, weekly, and monthly options for receiving reports help you to analyze and track the behavior of active users. You can evaluate and troubleshoot high-priority concerns including bandwidth related issues, identifying the top applications, and so forth. The Detailed reports, RealTime reports, and the Dashboard reports help you to get the detailed view of interface bandwidth, CPU usage, and connection rates for the required duration of time, among others. You can either set schedules to receive emails of the reports or run them manually too.

## Case 3: Notifications of Alerts

You can view the complete status of your network infrastructure by customizing your view of Notification Center. It displays all the details for alerts, threats, network usage, web activities, and geographical locations.

Define the rules to trigger the alerts based on the rules you set at the device level and set the priority for them. You can enable system pop-ups, retention of historical data, or email notifications to receive the alerts. You can also search and filter the alerts according to your core requirements. NSM provides a History table to save the notifications that you can keep and access at anytime.

## Case 4: On-boarding Administrators

You can define the roles and privileges for NSM users in MySonicWall. Different types of users include **SuperAdmin**, **Admins**, **Operators**, **Support users**, **ReadOnly users**, and **Guests**. Each of these user types are assigned permissions and access based on those roles. For example, Super administrators and administrators have the privilege to edit user roles and configure the firewalls. You can view the details of all the users who have access to a particular tenant on the **CSC Users** page.

# Managing Compliance

NSM also helps users to manage and maintain the security compliances.

**Topics:**

- Case 1: Review the Changes
- Case 2: Configuration Audit
- Case 3: Reporting and Scheduling

## Case 1: Review the Changes

Using the **Config Diff** options, you can quickly view the changes made to the configurations. The **Config Diff** feature also allows you to deploy firewalls by any required parameters.

**Config Diff** gives you an overall picture of what has been added, modified, or deleted in the firewalls. It also shows the value of the parameters, before and after the configuration changes have been made.

For example, a specific user removed a device out of a template. The configurations that already existed for that device will remain unchanged. Later when the user applies another template on the top, the new configuration gets deployed to the firewall. You can easily review such changes with the help of the **Config Diff** feature.

When comparing two audit items, you can also view a side by side comparison in **Full Diff**.

# Case 2: Configuration Audit

NSM saves and archives the configuration changes both before and after they are implemented. This makes it easy for you to audit the changes that are being made by all the users to firewall address objects or groups. It is easy to trace or dive deeper into the changes that impact the overall security of the devices, especially when managing multiple firewalls in an environment.

For example, A device group has been added by someone in the network, during the past week. This change may not have any direct changes on the firewalls. But you can easily identify the changes in the NSM Audit, that a specific user has created a device group and has moved some firewalls under it.

The Audit option helps you to validate the backups for your restored firewall configuration. You can see the complete changes in JSON view by accessing **Config Mgmt > Audit**. You can also select two different items and execute a comparative analysis.

# Case 3: Reporting and Scheduling

The real-time reporting and scheduling option improves the tracking and accountability of the NSM users as you are notified even when a small change occurs in the network. The report configuration option helps you to set parameters for your reports. The device selection option helps you to get customized reports for your device groups, firewall, or tenants. You can also schedule the frequency and the medium of the reports with the delivery configuration option.

You can manage, customize and schedule audit inventory reports in NSM. You can provide password protections and define custom logos for the reports. NSM provides the option to clone these reports and modify them for future use.

The basic 7-day reporting provided by NSM offers top level insight into traffic, network activities, and threats at unit, group, and tenant level. You can create group or device level aggregate reports as well. The 7-day reporting can be extended by adding the Analytics license.

3

# Dashboards and Monitor

The Dashboard provides a visual status of the security infrastructure. Dashboard also enables you to visualize status of the security infrastructure and assess the performances.

MONITOR menu assists you keep your cyber data safe and secure by navigating to the detailed insights provided in the reports, achieving a higher-level view of data, and generating custom threat intelligence reports.

This section describes more about:

- Dashboards
- Monitor

## Dashboards

Dashboard enables you to visualize status of the security infrastructure, assess the performances, and monitor the issues that need investigation, at a glance. The analytical dashboard NSM provides is an optimal solution to quickly analyze the cyber security risks and recognize how to resolve them.

NSM dashboard provides a comprehensive overview of the status of devices, traffic distribution, and all the threats by the type for the users to prepare and respond to them when required. This also helps the users to improve the control over their cyber security measures.

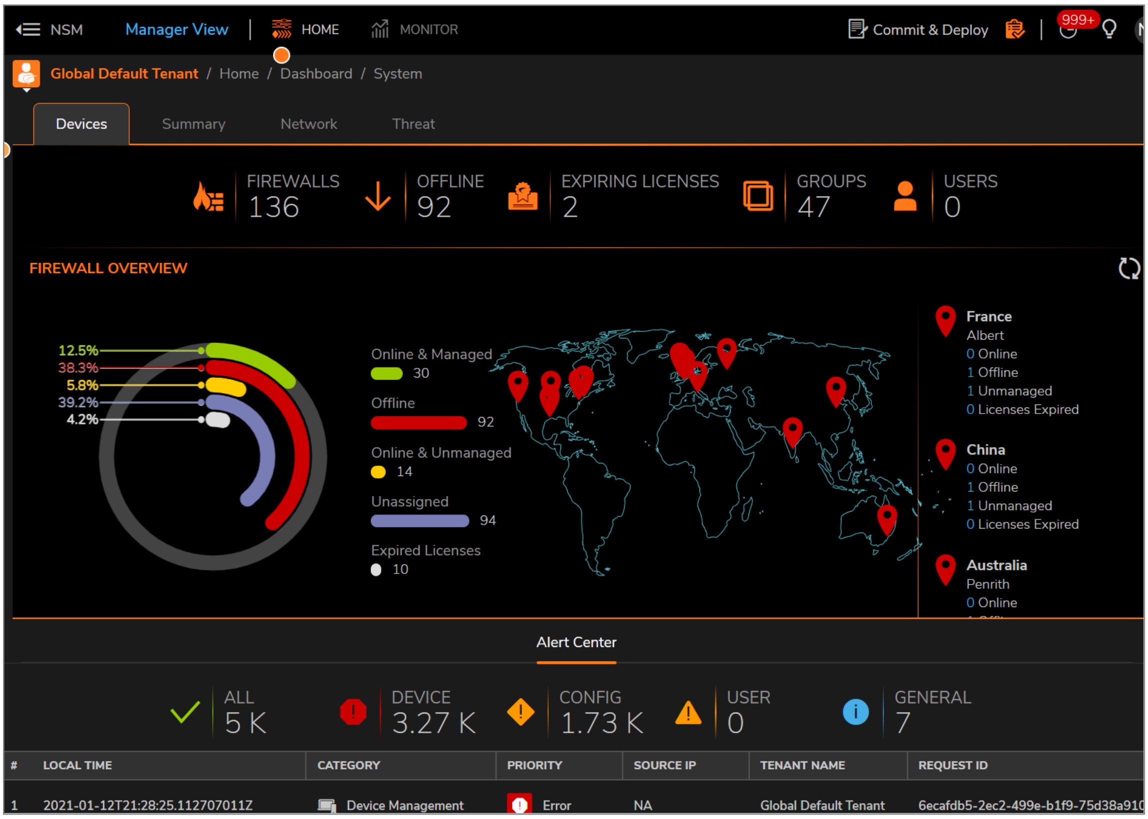
The system dashboard NSM provides has four tabs:

- **Devices**
- **Summary**
- **Network**
- **Threat**

The default view is **Devices** dashboard.

### Devices

The DEVICE tab on the dashboard shows the summary of the devices and alerts in your infrastructure.



| # | LOCAL TIME | CATEGORY | PRIORITY | SOURCE IP | TENANT NAME | REQUEST ID |
|---|---|---|---|---|---|---|
| 1 | 2021-01-12T21:28:25.112707011Z | Device Management | Error | NA | Global Default Tenant | 6ecafdb5-2ec2-499e-b1f9-75d38a910 |

The DEVICE tab shows you a summary of your devices:

- **FIREWALLS**: Displays the number of firewalls that you intend to manage through NSM. Click **FIREWALLS** to list 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 licenses.
- **GROUPS**: Displays number of device groups. Click GROUPS to list the device groups.
- **USERS:** Displays the number of CSC users online.

The **FIREWALL OVERVIEW** section shows the status of all devices, number of devices **Online and Managed**, **Offline**, **Online and Unmanaged**, **Unassigned,** and with the **Expired Licenses**. A pie chart representation of firewall overview is also displayed. The geographical locations of the firewalls are shown on the map. Hover the mouse over the map or scroll the list on the right-hand side to view more details of the devices in a particular location.

The **Alert Center** is shown at the bottom of the dashboard. An alert summary is provided and you can click on any of the categories—**All**, **Device, Config, User**, or **General** to view the details of the selected category in the **Notification Center.** You can also view the most recent alerts in the table below the summary. The table lists the details including Local Time, Category of the device, Priority, Source IP, Tenant Name, and Request ID.

## Summary

The **Summary** tab shows **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. These sections provide the Map, Graph, and List views to navigate into the details.

The **Top Devices by Sessions** data can be filtered down further to get the statistics of Data Sent, Data Received, Applications, Viruses, Intrusions, Spyware, and Botnet Blocked.

The **Summary** tab also shows the **Insights** section giving information about the number of infected hosts and the number of **Critical Attacks**. You can drill down further by selecting the Date or Alphabetical order. The search options provided in this page help you to find the details faster. You can also search and filter your data using the options **All**, **Spotlight**, **Malware**, **Ransomware**, or **Intrusions**.

The **Summary** tab also provides additional information on key logging and the potent key loggers.

## Network

The **Network** tab shows data pertaining to transactions in your network infrastructure. This include the details of **Top Applications by Sessions**, **Top Addresses by Sessions**, **Top Users by Sessions**, and **Top Web Categories** from which the connections are initiated. Each space enables you to filter the data with available options

You can analyze the data for top applications, top addresses, and top users by sessions and drill down to get the statistics. This include Data Sent, Data Received, Virus, Intrusions, Spyware, Access Rule Blocked, Threats Blocked, GEO-IP Blocked, Botnet Blocked, Total Data Transferred, and Total Blocked.

All these sections provide Graph and List views to navigate into the details. You can also drill down further by clicking on the **View Details** link.

## Threat

The **Threat** tab shows the details of threats by type including the **Top Viruses**, **Top Intrusions**, **Top Spyware**and **Top Botnet**.

All these sections provide Graph and List views to navigate into the details. You can drill down further by clicking on the **View Details** link.

# Monitor

NSM MONITOR menu assists you keep your cyber data safe and secure by navigating to the detailed insights provided in the reports, achieving a higher-level view of data, and generating custom threat intelligence reports. As the sophistication of cyber attacks also grows, the MONITOR menu helps you to safeguard your information, by performing the most vigorous and robust cyber security assessments.

You can take a deep dive into the comprehensive details of applications, users, viruses, intrusions, spyware, web categories, IP addresses and locations. MONITOR option thus helps you to detect all the vulnerabilities in your network infrastructure and remediate improved secure policies when needed.

NSM allows you to monitor data available from different views such as **Firewall View** and **Manage View**, where you can view the Live Monitor and Live Reports. You can also access and monitor data from different places in the application. For instance, when you are in **Manage mode**, you can click MONITOR menu to check the Connection status within the selected time frame. You can view the connection details, the transferred data, blocked viruses, intrusions, spyware, botnet and GEO-IP information. Another example is when you are in **Firewall mode**, you can view the list of devices in inventory. Click the name of a device and you can monitor the detailed information of Device, Summary, Network and Threat about that particular device as well.

MONITOR option provides the options to filter the Applications, App Categories and App Risk. You can adjust the slider at the top to select the time frame, or select the specific dates required from the custom option, and view the narrative results in Grid view, or Chart and Grid view. You can search for the tenants and view up to 8000 reports at a time. You can also generate flow report in PDF, download capture threat assessments into a CTA file, or export grid data as a CSV file.

For more information about the MONITOR view, refer to *Network Security Manager Reporting and Analytics Administration Guide*.

# 4

# NSM Navigation

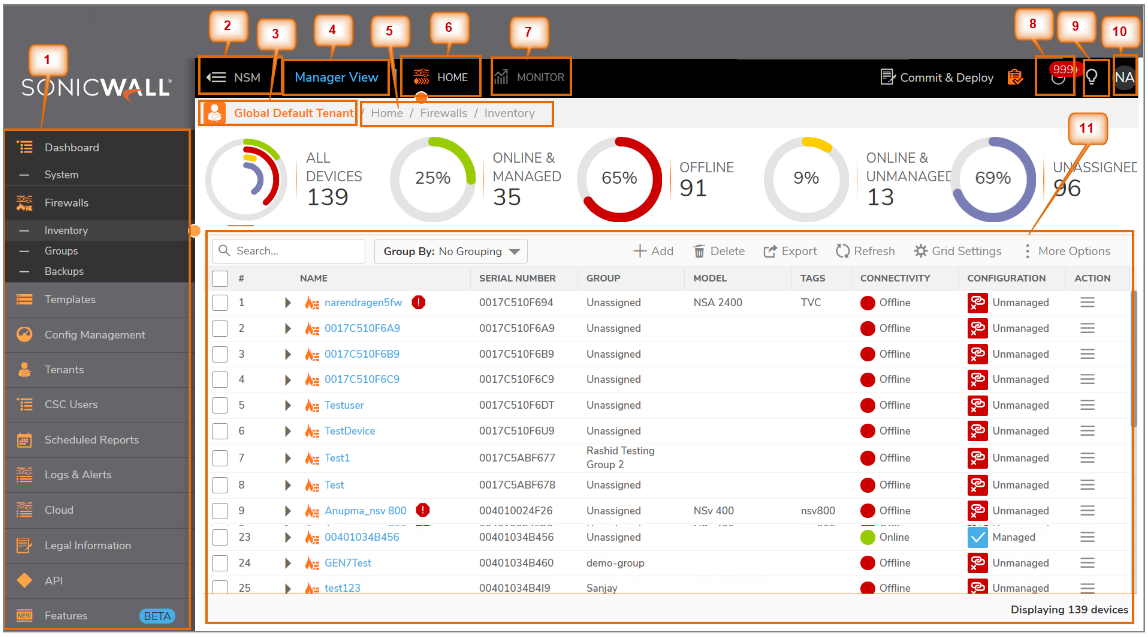
NSM is a centralized management application that addresses automation, control, and visibility of your security elements. It uses a tiered, or layered, approach to managing complex inter-related information. Understanding how the tasks and commands are grouped on the interface can help you effectively navigate to the commands and views you need.

Many of the elements across the tool have been unified. For example, the Inventory table looks similar to the Templates table. Once you know how to navigate one you can easily navigate others. This section describes the layout and the common navigation tools and icons used throughout NSM.

**Topics:**

## Interface Overview

Understanding the NSM interface design and layout can help you more easily navigate the functions within NSM. When you first log into NSM, the Inventory table is the default page shown. Using the Inventory table as an example, the general interface layout is mapped in the following figure.



| | # | NAME | SERIAL NUMBER | GROUP | MODEL | TAGS | CONNECTIVITY | CONFIGURATION | ACTION |
|---|---|---|---|---|---|---|---|---|---|
| □ | 1 | narendragen5fw | 0017C510F694 | Unassigned | NSA 2400 | TVC | Offline | Unmanaged | ≡ |
| □ | 2 | 0017C510F6A9 | 0017C510F6A9 | Unassigned | | | Offline | Unmanaged | ≡ |
| □ | 3 | 0017C510F6B9 | 0017C510F6B9 | Unassigned | | | Offline | Unmanaged | ≡ |
| □ | 4 | 0017C510F6C9 | 0017C510F6C9 | Unassigned | | | Offline | Unmanaged | ≡ |
| □ | 5 | Testuser | 0017C510F6DT | Unassigned | | | Offline | Unmanaged | ≡ |
| □ | 6 | TestDevice | 0017C510F6U9 | Unassigned | | | Offline | Unmanaged | ≡ |
| □ | 7 | Test1 | 0017C5ABF677 | Rashid Testing Group 2 | | | Offline | Unmanaged | ≡ |
| □ | 8 | Test | 0017C5ABF678 | Unassigned | | | Offline | Unmanaged | ≡ |
| □ | 9 | Anupma_nsv 800 | 004010024F26 | Unassigned | NSv 400 | nsv800 | Offline | Unmanaged | ≡ |
| □ | 23 | 00401034B456 | 00401034B456 | Unassigned | | | Online | Managed | ≡ |
| □ | 24 | GEN7Test | 00401034B460 | demo-group | | | Offline | Unmanaged | ≡ |
| □ | 25 | test123 | 00401034B4I9 | Sanjay | | | Offline | Unmanaged | ≡ |

Displaying 139 devices

| Reference | Interface Item | Description |
|---|---|---|
| 1 | Left command menu | Displays the primary tasks and commands that can be selected. The command menu varies depending upon which view you are in and the command option you have selected. |
| 2 | Show/hide commands icon | Acts as a switch to show or hide the left command menu. Click it to hide the command menu; click it again to show it. |
| 3 | Tenant name | Shows the name of the tenant whose data you are viewing. This is also a drop-down menu; click the tenant name to see all the tenants associated with your NSM instance. |
| 4 | View name | Shows which view is active in the interface. The Manager View is active in the example and is the default. The view represents the top level grouping of related tasks and commands. Refer to NSM Views for more details. |
| 5 | Command path | Shows the series of menu items selected to get to the information shown in the work space. In the documentation this same path is represented as **HOME > Firewall View> Inventory**. Sometimes this series of commands is also called the bread crumbs. |
| 6 | Home Command | Acts as the Home command for the selected option. |
| 7 | MONITOR | Acts as the MONITOR for the selected option. |
| 8 | Notification icon | Opens the Notification Center. The number above the icon indicates the number of alerts detected. Refer to Notification Center for more details. |

| Reference | Interface Item | Description |
|---|---|---|
| 9 | Help icon | Opens the Technical Documentation website where you can access the product documentation. |
| 10 | User icon | Shows the initials of the user that's logged in but it also acts as a drop-down list. It shows the user name, the version of the product and the **Log Out** option. |
| 11 | Work space | Displays the data associated with the menu options or commands selected. This can be a table, as shown in the example, a dashboard or a series of options to select or define. |

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

# Task-Oriented Navigation

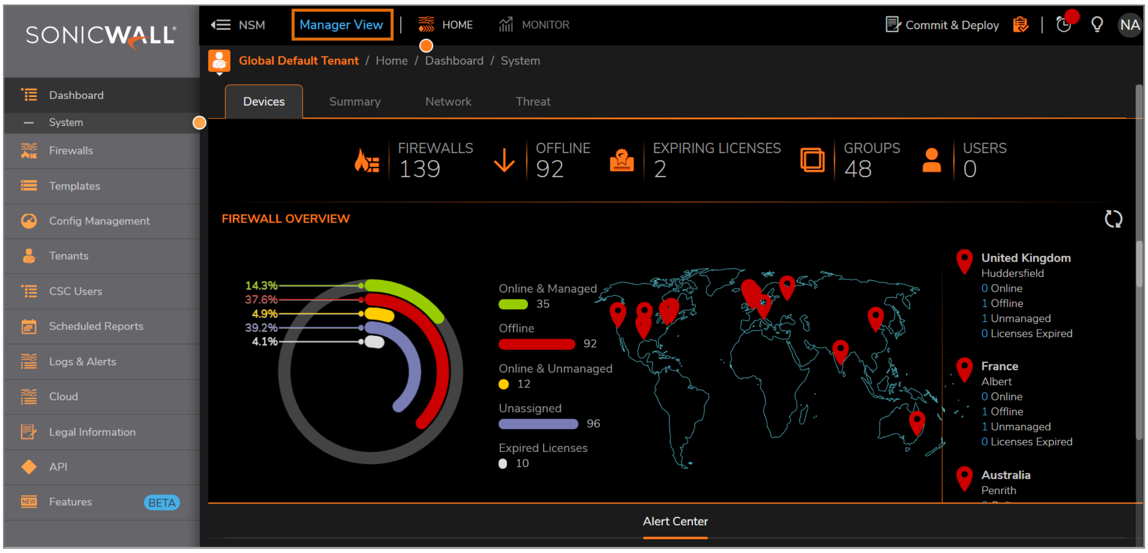
The user interface for NSM has been designed to group similar tasks and workflows. Through selection of views and options, the commands are displayed for the tasks you need to perform.

**Topics:**

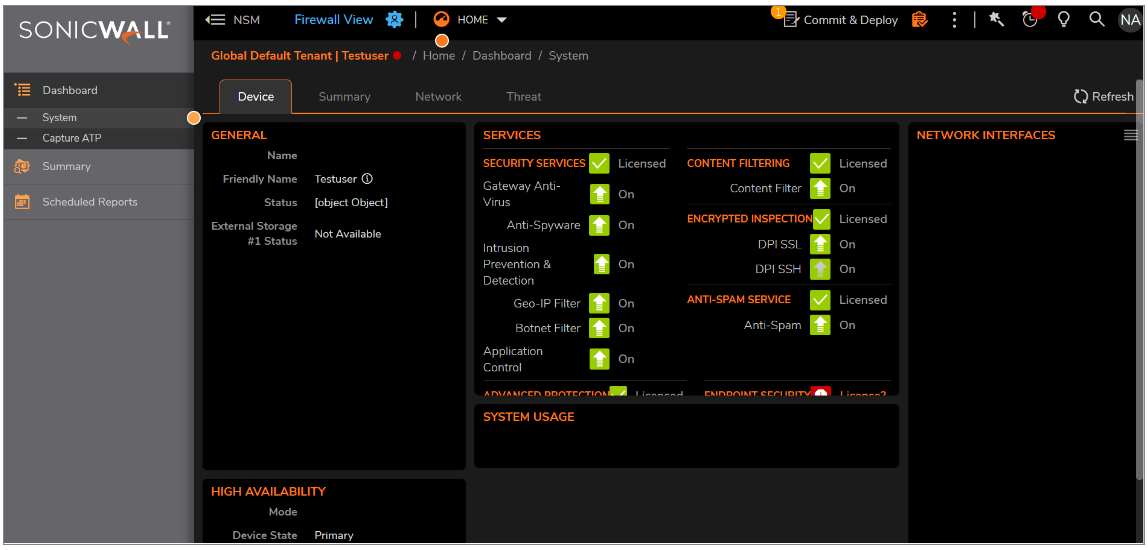
- NSM Views
- Command Options

# NSM Views

Network Security Manager organizes its workflows into modes or views. When you first log in, the default view is the **Manager View**. The view is indicated in the header at the top of the window. The key tasks for managing your networking infrastructure are organized into this view. You have options across the top of the window and commands in the left-hand command menu.



Depending on the tasks you choose to perform, you may be sent to another view to access the commands for those tasks. For example, if you want to look at a specific device and make changes, navigate to **HOME > Firewall > Inventory** and click the device you want to update. You are taken to the **Firewall View**. This displays the options and commands available to you.

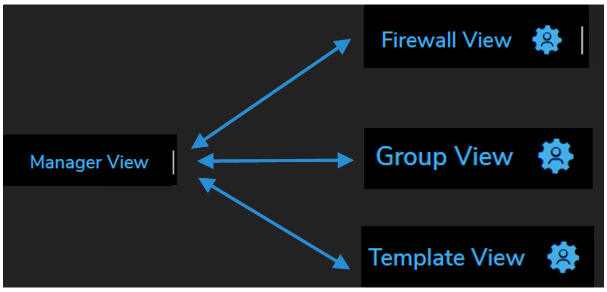


The following table describes all the views and how to access them:

| Interface View | How to Access the View |
|---|---|
| **Manager View** | This is the default view when you log into NSM, and you can perform or initiate most management functions in this view. Click ⚙ to return from another view and switch to **Manager View**. |
| **Firewall View** | Use this view to manage individual devices. Navigate to **HOME > Firewall > Inventory** and click on the device you want to manage to go to Firewall View. |
| **Group View** | Navigate to **HOME > Firewall > Groups** and click on the group you want to view or |

| Interface View | How to Access the View |
|---|---|
| | change. From this view you can monitor and modify groups of devices that you have defined within your infrastructure. |
| Template View | Navigate to **HOME > Templates** and click on one of the templates in the table. From this view you can modify or define all the parameter needed for a device template. |

Navigation between the views is an out-and-back model.



When you go to another view from the **Manager View**, you have to come back to **Manager View** clicking ⚙ before going to something else. For example, you cannot go to **Template View** from the **Firewall View**.

After going into a new view, additional options are displayed across the top of the screen. These include **HOME**, **MONITOR**, and so forth. You can select one of the options from across the top of the page, which then displays the associated command options in the left command menu.

# Command Options

Once you navigate to a view, several command options appear at the top of the page, next to the name of the view. After selecting an option, a new set of commands appears in the left-hand menu. The following table correlates the which options are available with each view.

| NSM View | Command Options Available |
|---|---|
| Manager View | HOME<br>MONITOR |
| Firewall View | HOME<br>MONITOR<br>DEVICE<br>NETWORK<br>OBJECT<br>POLICY |
| Group View | HOME<br>MONITOR |

| NSM View | Command Options Available |
|---|---|
| | DEVICE<br>NETWORK<br>OBJECT<br>POLICY |
| Template View | DEVICE<br>NETWORK<br>OBJECT<br>POLICY |

Refer Interface Map for more details.

# Interface Management

The NSM user interface is designed to be consistent across features and command options. Tables use similar filtering, icons, and formats. Features provide fields, drop-down lists, or check boxes to select. This results in a better user experience as you navigate from screen to screen or feature to feature. The interface is dynamic, so changes are made without you having to reload your browser. Being dynamic has no impact on the web server, CPU utilization, bandwidth, or other performance factors. You can leave your browser window on a dynamically updating page indefinitely with no impact to the performance of your system.

More details about interface management include:

- Icons and Buttons
- Table Tools
- Tool tips

# Icons and Buttons

NSM provides a good user experience with the characteristics of a great interface. NSM sets clear expectations for the users to navigate and scan information faster. The unique, intuitive icons provided by NSM direct the users to where they need to go, much easier.

The icons and their functions are described below:

| Icons and Labels | Definition |
|---|---|
| **Left Command Menu Icons for Manager View** | |
| ☰ | Indicates the Dashboard icon and label. |
| 🔥 | Indicates the Firewalls icon and label. |
| ☰ | Indicates the Templates icon and label. |

| Icons and Labels | Definition |
|---|---|
| **Left Command Menu Icons for Manager View** | |
| | Indicates the Config Management icon and label. |
| | Indicates the Tenants icon and label. |
| | Indicates the CSC Users icon and label. |
| | Indicates the Scheduled Reports icon and label. |
| | Indicates the Logs & Alerts, and the Clouds icons. |
| | Indicates the Legal Information icon and label. |
| ◆ | Indicates the API icon and label. |
| NEW | Indicates the icon to view the new features. |
| **Left Command Menu Icons for Other Views** | |
| | Indicates the Summary and Details icon in the MONITOR page. |
| | Indicates the Settings icon in the DEVICE page. |
| | Indicates the Users icon in the DEVICE page. |
| | Indicates the High Availability icon in the DEVICE page. |
| | Indicates the Diagnostics icon in the DEVICE page. |
| | Indicates the Switch Network icon in the DEVICE page. |
| | Indicates the Access Point icon in the DEVICE page. |
| | Indicates the System icon in the NETWORK page. |
| | Indicates the VoIP icon in the NETWORK page. |
| | Indicates the DNS icon in the NETWORK page. |
| | Indicates the SDWAN icon in the NETWORK page. |
| | Indicates the IpSec VPN icon in the NETWORK page. |

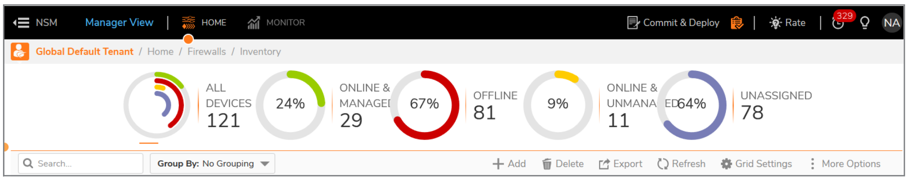
| Icons and Labels | Definition |
|---|---|
| **Left Command Menu Icons for Manager View** | |
| | Indicates the SSL VPN icon in the NETWORK page. |
| | Indicates the Match Objects icon in the OBJECT page. |
| | Indicates the Profile Objects icon in the OBJECT page. |
| | Indicates the Action Objects icon in the OBJECT page. |
| | Indicates the Rules and Policies icon in the POLICY page. |
| | Indicates the Security Services icon in the POLICY page. |
| | Indicates the Anti-Spam icon in the POLICY page. |
| S | Indicates the Endpoint Security icon in the POLICY page. |
| ATP | Indicates the Capture ATP icon in the POLICY page. |
| DPI SSL | Indicates the DPI-SSL icon in the POLICY page. |
| DPI SSH | Indicates the DPI-SSH icon in the POLICY page. |
| **Dashboard Icons** | |
| | Indicates the Manager View and HOME views. |
| | Indicates the MONITOR view. |
| | Indicates the collapse icon on the menu bar. |
| | Indicates the expand icon on the menu bar. |
| | Indicates the icon to switch back to the Manager View from other views. |
| | Indicates the Firewalls icon on the Dashboard Devices tab. |
| ● | Indicates the users who are offline on the Dashboard Devices tab. |
| | Indicates the number of expiring licenses on the Dashboard Devices tab. |

| Icons and Labels | Definition |
|---|---|
| **Left Command Menu Icons for Manager View** | |
| ⧉ | Indicates the number of groups who are online on the Dashboard Devices tab. |
| 👤 | Indicates the number of users online on the Dashboard Devices tab. |
| 🔄 | Indicates the icon to refresh dashboard. |
| ✓ | Indicates the all alerts icon on the Dashboard Devices tab. |
| ! | Indicates the threats for the devices, on the Dashboard Devices tab. |
| ! | Indicates the general configuration errors on the Dashboard Devices tab. |
| ⚠ | Indicates the user operation errors on the Dashboard Devices tab. |
| i | Indicates the icon to view the general information on the Dashboard Devices tab. |
| ⚙ | Indicates the options provided in the NETWORK and the Summary tabs such as Top Applications, Top Addresses, Top Users and Top Web Categories for various categories including Data Sent, Data Received, Virus, Intrusions, and so on. |
| ▦ | Indicates the map view of data on the dashboard. |
| ◔ | Indicates the graph view for the Summary, Network, or Threat tabs on the dashboard. |
| ☰ | Indicates the list data display for the Summary, Network, or Threat tabs on the dashboard. |
| ≡ | Indicates the icon to view more information of the reports including Users, Applications, and so on. |
| 📝 | Indicates icon to the Commit and Deploy wizard. |
| 📋 | Indicates the icon to view the Commit and Deploy History. |
| 🕓 | Indicates the icon to view the notification center. |
| 💡 | Indicates the icon to view the online help. |
| Operational Status Icons | |

| Icons and Labels | Definition |
|---|---|
| **Left Command Menu Icons for Manager View** | |
| 📝 | Indicates that a configuration that is being edited. |
| ✍ | Indicates that an approval is pending for the configuration. |
| ⊘ | Indicates that a configuration is cancelled. |
| ! | Indicates that a deployment is failed. |
| ✓ | Indicates that a configuration is deployed. |
| ••• | Indicates that a configuration is being deployed. |
| 📅 | Indicates that a configuration deployment is scheduled. |
| 📋 | Indicates that a configuration change is committed. |
| ◆! | Indicates that an approval is overdue for a configuration. |
| 👍 | Indicates that a configuration is approved. |
| 👎 | Indicates that a configuration is rejected. |

# Table Tools

Table tools provided by NSM helps you to filter, manage and get the custom view of the data effortlessly. The table tools are easy to use with a logical structure that makes the content easy to understand.



The following section describes the table tools provided by NSM and their descriptions:

| Table Icons | Definition |
|---|---|
| ● | Indicates the device is online. |

| Table Icons | Definition |
|---|---|
| ● | Indicates the device is offline. |
| + | Indicates the button to add a new schedule, device groups, templates, and so on. |
| 🗑 or ⊖ | Indicates the button to delete the selected options. |
| ↗ | Indicates the icon to export data into a CSV file. |
| ⟳ | Indicates the button to refresh or reload the page. |
| ⚙ | Indicates the icon to select the grid settings or the required columns. This helps you to view or hide the selected columns and customize the data with the desired fields. |
| ⋮ | Indicates More Options such as Manage Configurations and Manage Commits. |
| ☰ | Indicates the action icon on the **Firewalls > Inventory** page. Enables you to do the action items such as Switch to Firewall View, Edit Settings, Synchronize Firewall, Upgrade Software, Backup Config, Audit, Manage Commits, Scheduled Reports, and Delete Firewall.<br>For Templates, this icon indicates the options to Edit Template, View Template Configuration, Clone Template, Modify Template Attributes, Apply Template, and Delete Template. |
| ⚙ | Indicates the icon to switch to Firewall View from an **Action** button. |
| ✎ | Indicates the icon to edit settings from an **Action** button. This is also the icon to edit template on the **Templates** page. |
| ⟳ | Indicates the icon to synchronize firewall from an **Action** button. |
| ⇪ | Indicates the icon to upgrade firmware from an **Action** button. |
| 🗄 | Indicates the icon to archive configuration from an **Action** button. |
| 🔍 | Indicates the Audit icon from an **Action** button. |
| 📄 | Indicates the icon to manage commits from an **Action** button. |
| 📄 | Indicates the icon to view scheduled reports from an **Action** button. |

| Table Icons | Definition |
|---|---|
| 📄 | Indicates the icon to export to template from an **Action** button. |
| ⇄ | Indicates the icon to log-in to unit from an **Action** button. |
| 🗑 | Indicates the icon to delete firewall from an **Action** button. Also indicates the icon to delete templates from an **Action** button on Templates page. |
| ⭱ | Indicates the icon to upload keyset file from an **Action** button. |
| ••• | Indicates the Action icon from **Firewalls > Groups** or **Firewalls > Backups** pages. |
| ⚙ | Indicates the button to backup configurations for the selected series of entries in the Firewalls Groups tab.<br>You can create Local, Cloud, or Schedule Backups with this option. |
| ⤓ | Indicates the button to run the scheduled report options. You can test the selected files with the help of this option.<br>Also indicates the button to download files such as archived reports to the required folder. |
| 📝 | Indicates the icon to select templates in the Templates section. |
| ☰ | Indicates that a particular template is not applied to any device or groups. If it is applied already, this icon displays the number of Total Devices and Root Groups. |
| 👁 | Indicates the icon to view template configuration from an **Action** button in the Templates page. |
| ⧉ | Indicates the icon to clone template from an **Action** button in the Templates page. |
| ⚙ | Indicates the icon to modify template attributes from an **Action** button in the Templates page. |
| ◆ | Indicates the icon to apply template from an **Action** button in the Templates page. |
| ▤ | Indicates the icon to view the template status from an **Action** button in the Templates page. |
| ⟲ | Indicates the icon to set the default approval groups. |
| ⊕ | Indicates the button to commit a new configuration in the Config Management section. |
| ⏷ | Indicates the icon to filter the required options. For example, to filter the devices for the topology options, options, operational status, and so on.<br>In Reports section, this indicates the icon to download reports. |

| Table Icons | Definition |
|---|---|
| 🗐 | Indicates the button to view the difference between two configurations you select. You can compare the difference in the **Config Diff** window. |
| 👤 or 👤 | Shows the list of tenants in the Tenants section. |
| ✎ | Indicates the button to edit the details. For example, port details of the networks, tenants, and so on. |
| 👤⊖ | Indicates the button to log out the selected users in the CSC Users Status section. |
| ○ | Indicates the button to enable certain options or notifications.<br>For example, to show legends for applications, bandwidth, packet rate, packet size, connection rate, and so on. |
| ● | Indicates the button to disable certain options or notifications.<br>For example, to disable beta features, hide legends for applications, bandwidth, packet rate, packet size, connection rate, and so on. |
| 📅 | Indicates the button to run the options for the selected date range. |
| ? | Indicates that Zero Touch Connection is disabled for a device.<br>Also indicates that the last run status is not available for a scheduled report. |
| 📝 or ⟫ | Indicates the commit and deploy wizard. |
| 👤🔒 | Indicates that the user is a Super Admin. |
| ▦ | Indicates the grid only view. |
| 📈 | Indicates the chart and grid view. |
| ⏸ or ⏸ | Indicates the button to pause the refresh option for intervals, live reports, and so on. |
| ▶ | Indicates the button to play live reports. |
| 💡 | Indicates the button to view the page description that shows the real-time view of the packets forwarded by the firewall. |
| 🔓 | Indicates if the CSC user is locked-out or not. |
| ✓ | Indicates active users. Also indicates the operational status that configuration changes are deployed. |
| ↓ | Indicates the icon that the zero touch connection is down. |

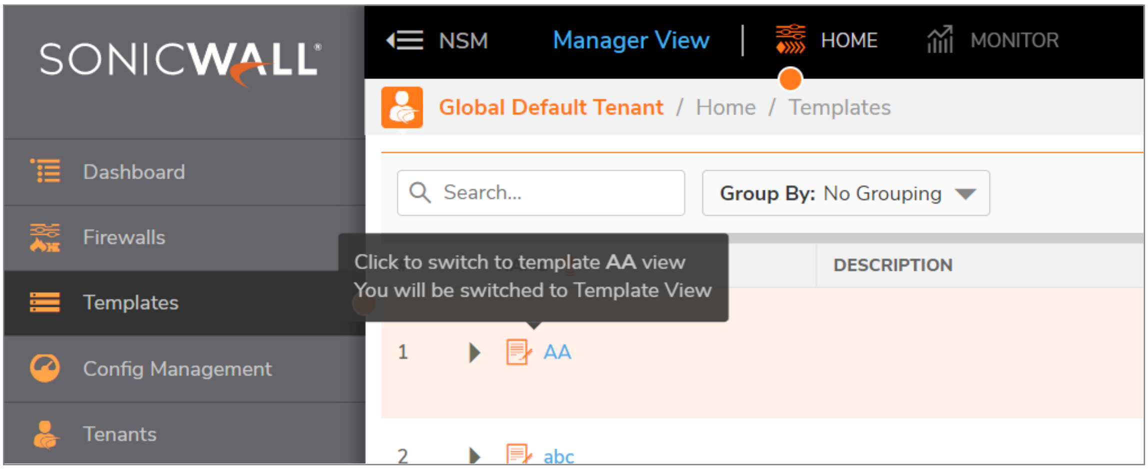
| Table Icons | Definition |
|---|---|
| ↑ | Indicates the icon that the link is up. |
| ✓ | Indicates the icon that the firewall connected has the zero touch option. Also indicates that the zero touch option is enabled for a template. |
| ✎ | Indicates the icon to edit user. |
| 📶 | Indicates the icon to view bar chart for the reports. |
| 📈 | Indicates the icon to view stacked chart for the reports. |
| 🔄 | Indicates the icon to synchronize data for the security services summary. |
| 📜 | Indicates the icon to view the SCEP configuration for certificates. |
| ✍ | Indicates the icon to generate certificate signing requests. |
| 👁 | Indicates the button to show labels. |
| ⊘ | Indicates the button to hide labels. |
| 📡 | Indicates the icon to view the topology view of the devices. |
| ✳ | Indicates the icon to view the topology view of the networks. |
| ❐ | Indicates the icon to switch to Group View from Manager View, or to navigate to the root group from Group View. |
| 🔥 | Indicates the icon to switch to Firewall View from Manager View. |
| ▼ | Indicates the collapse icon. |
| ▶ | Indicates the expand icon. |
| ☑ | Indicates the icon to mark all alerts as read, in the Notification Center Inbox. |
| ⇪ | Indicates the button to upload new firmware from your local device. |
| ⚙ | Indicates the button to create changes in the settings of firmware. This include making changes to Schedule Reports, Diagnostics, FIPS, NDPP and so on. |

| Table Icons | Definition |
|---|---|
| ☰ | Indicates the button to show the user count. |
| 🪄 | Indicates the icon to view wizard from Firewall View and Template View. |

## Tool tips

NSM, to improve the on-boarding experience of the users, provides tool tips and offers advice in the right place at the right time. You can just hover the mouse over a field to get the in-app contextual messages that provide additional information about the specific features. Tool tips offer you relevant contextual help to understand the functionality of the features faster.

The tool tips pop up with helpful hints, suggestions, and explanations for the paired elements.



Click to switch to template AA view
You will be switched to Template View

# Finding Information

You can get help from anywhere in the user interface. Simply click the **Help** icon in the upper right-hand corner, and a new window opens. A filtered URL is sent to the Technical Documentation portal so that only NSM documents are shown. However, if you need to explore other topics, the entire technical documentation library is available to you. Set or clear filters as needed to refine your search for information.

Because NSM integrates SonicOS into its device management structure, the SonicOS documentation is a key part of the information available to you. NSM documents address infrastructure management:

- Views and data associated with your whole environment
- Views and data associated with groups of devices
- Tools, like templates and configuration management, that can be leveraged across multiple devices or groups
- Summaries provided for monitoring

The tools and commands to manage individual devices are SonicOS tools and commands; the interface is the same too. As such, you are referred to SonicOS documentation for device management details. When filtering for SonicOS documentation, be sure to select version 7.

5

# Notification Center

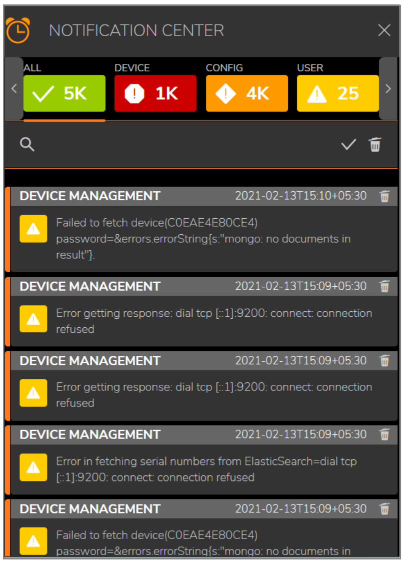
The Notification Center shows administrators and users the status of their network infrastructure. It summarizes the number of notices, threats operational notices and general notices. You can also set the rules for the notices and acknowledge them.

**Topics:**

- Understanding Notifications
- Managing the Alerts
- Defining Alerts and Notifications
- Managing Notification History

## Understanding Notifications

The Notification Center is a separate pane that provides the status and activities being monitored and recorded by NSM. After clicking the Notification Center icon at the top of the interface, the Notification Center opens to show **All** alerts, **Threats**, **Operations** alerts, **User** alerts and **General** alerts. Each option shows how many unread alerts appear in that particular category.



DEVICE MANAGEMENT 2021-02-13T15:10+05:30

Failed to fetch device(C0EAE4E80CE4) password=&errors.errorString{s:"mongo: no documents in result"}.

DEVICE MANAGEMENT 2021-02-13T15:09+05:30

Error getting response: dial tcp [::1]:9200: connect: connection refused

DEVICE MANAGEMENT 2021-02-13T15:09+05:30

Error getting response: dial tcp [::1]:9200: connect: connection refused

DEVICE MANAGEMENT 2021-02-13T15:09+05:30

Error in fetching serial numbers from ElasticSearch=dial tcp [::1]:9200: connect: connection refused

DEVICE MANAGEMENT 2021-02-13T15:09+05:30

Failed to fetch device(C0EAE4E80CE4) password=&errors.errorString{s:"mongo: no documents in

Individual alert messages arrive and are displayed in the body of the Notification Center. They are triggered based on how the alerts are defined in the Rules. The individual messages show the alert name, the firewall name and the time they are triggered. They are listed in the order they arrive, and colored icon illustrates the priority of the alert: high (red), medium (orange), or low (yellow).

# Managing the Alerts

The Notification Center provides some basic tools for accessing and managing the list of alerts. In the section beneath the summaries, you can filter, acknowledge or delete alerts.

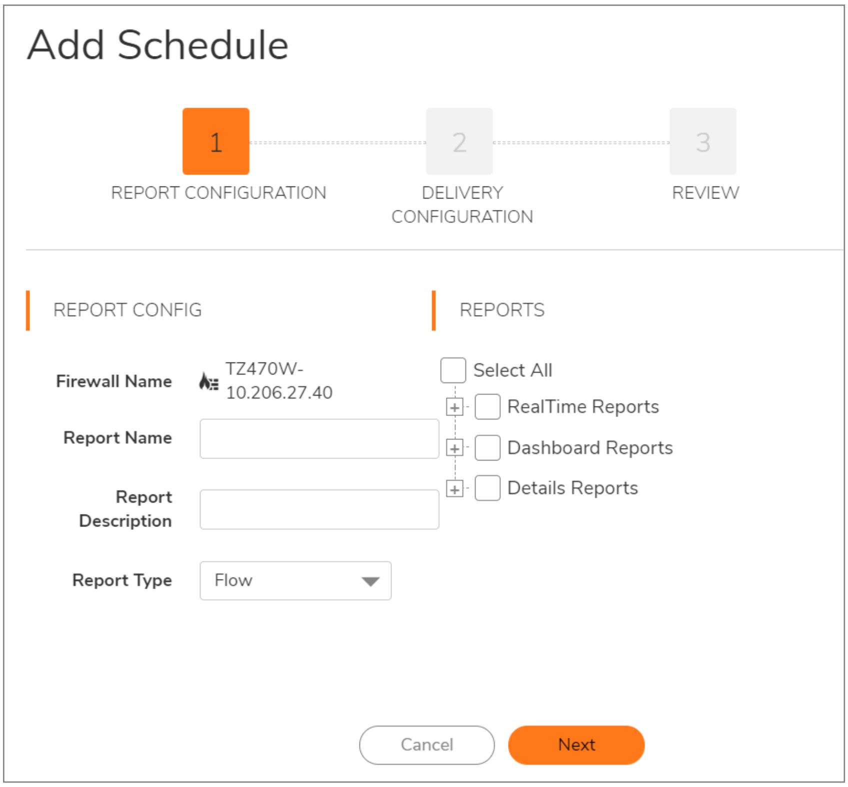
- **To sort the alerts**, click the alert types at the top of the Notification Center. The type you selected is then displayed in the list.
- **To search by firewall name**, alert name, message or details, click in the **Search...** field and enter the information you want to search. As you type, the list of alerts narrows to meet the criteria. Clear your search by clearing the search field.
- **To mark a single alert as read**, Click the white check mark at the top of the list to acknowledge all the alerts as having been read. You can also click the yellow icon pertaining to each alert to acknowledge them.
- **To delete a single alert**, click the **Delete** icon on each alert. To delete all the alerts in the view, click the **Delete All Alerts** icon at the top of the list.
- To close the **Notification Center**, click the **X** at the top.

# Defining Alerts and Notifications

You can set up several different types of alerts and corresponding rules for them, but they have to be defined at the device level.

***To define an alert:***

1. Navigate to the Inventory list at **Manager View | HOME > Firewall > Inventory**.
2. Click the system you want to set up an alert for. The system will redirect you to the **Firewall View**.
3. Navigate to **Scheduled Reports > Rules**.
4. Click **+ Add Rule**.



Add Schedule

1 REPORT CONFIGURATION — 2 DELIVERY CONFIGURATION — 3 REVIEW

REPORT CONFIG

Firewall Name: TZ470W-10.206.27.40

Report Name:

Report Description:

Report Type: Flow

REPORTS

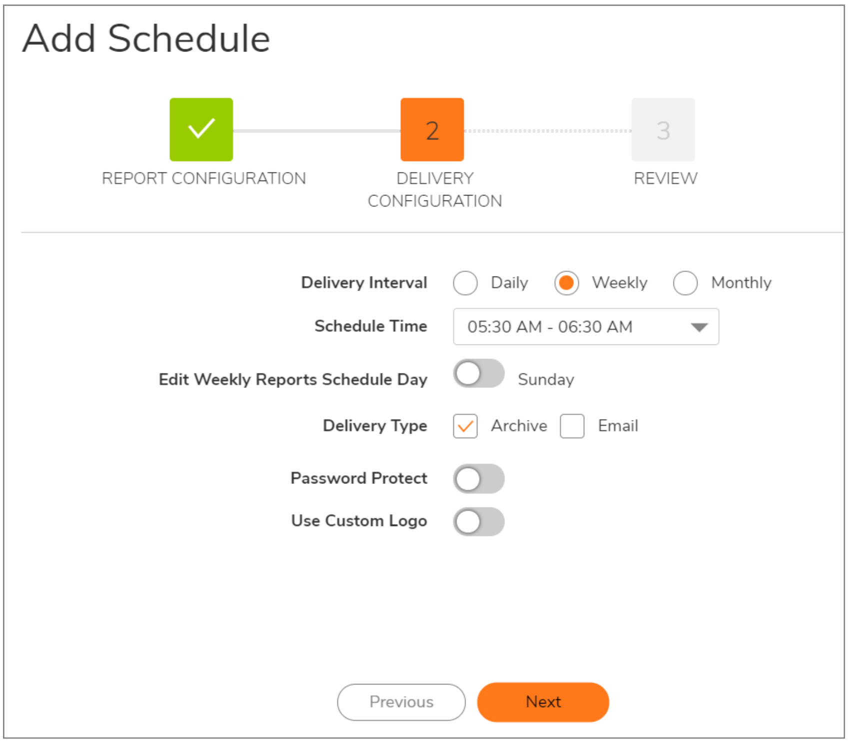
- □ Select All
- □ RealTime Reports
- □ Dashboard Reports
- □ Details Reports

5. On the **Details** page of the wizard:
   a. Enter the **Report Name**.
   b. Enter the **Report Description**.
   c. Select the **Report Type**. The options are **Flow**, **CTA**, and **Management**.
   d. From **Reports** section, select the type of the report. Click + to drill down to the specific report. You can also select all if required.

      The options depend on the Report Type you have previously selected.

      - If you have selected Flow, the options are **RealTime Reports**, **Dashboard Reports**, and **Details Reports**.
      - If you have selected CTA, the options are **CTA Reports**.
      - If you have selected Management, the options are **Subscription Reports** and **Inventory Reports**.
   e. Click **Next**.
6. On the **Device Selection** page, select the desired **Firewall** or **Group**.
7. Click **Next**.

8. On the **Delivery Configuration** page:



Add Schedule

Delivery Interval ○ Daily ● Weekly ○ Monthly

Schedule Time 05:30 AM - 06:30 AM

Edit Weekly Reports Schedule Day Sunday

Delivery Type ☑ Archive □ Email

Password Protect

Use Custom Logo

a. Select the **Delivery Interval**. The options are **Daily**, **Weekly**, and **Monthly**. The options you would see for scheduling the alert depends on the Delivery Interval you have selected.

b. Select the **Schedule Time** from the drop-down.

c. (Conditional) Select the **Schedule Day** if you have selected Weekly or Monthly options for the Delivery Interval.

d. Select the **Delivery Type**. The options are **Archive** or **Email**.

e. Select **Email Destination** from the drop-down menu.

f. Specify the **Email ID**, **Subject** and **Email Body**.

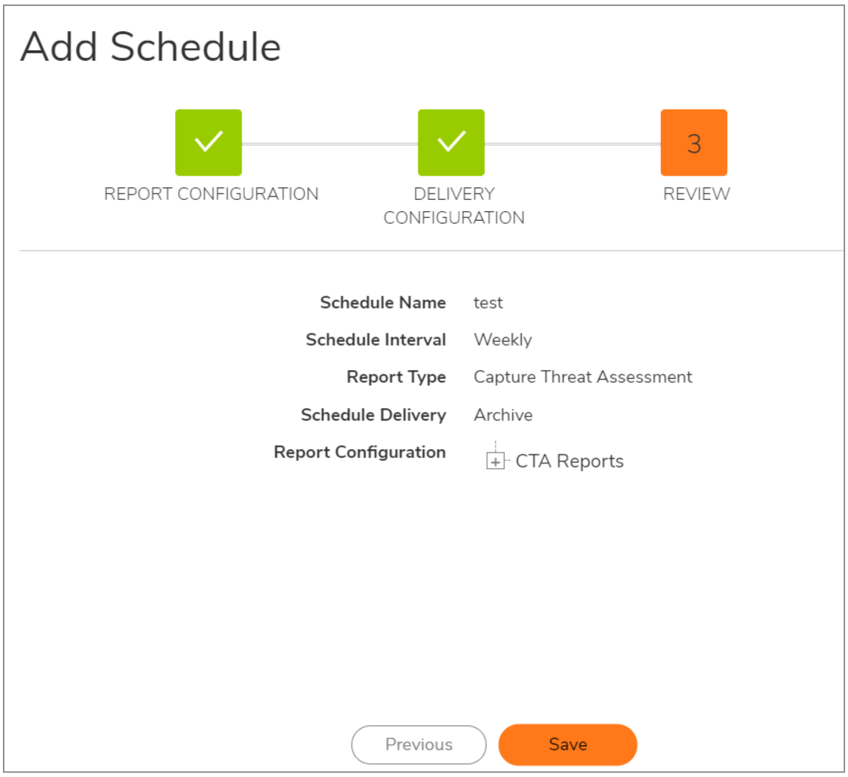
g. Select the option to **ZIP Report**, if required.

h. Select the option **Password Protect** to protect the data with a password.

i. Select the option Use Custom Logo to use a customized logo.

j. Click **Next**.

9. On the Review page:



Add Schedule

Schedule Name test

Schedule Interval Weekly

Report Type Capture Threat Assessment

Schedule Delivery Archive

Report Configuration ⊞ CTA Reports

a. Review the rule. If adjustments are needed, click **Previous** to go back to the other screens and make the appropriate changes.

b. Click **Save** if the rule is correct.

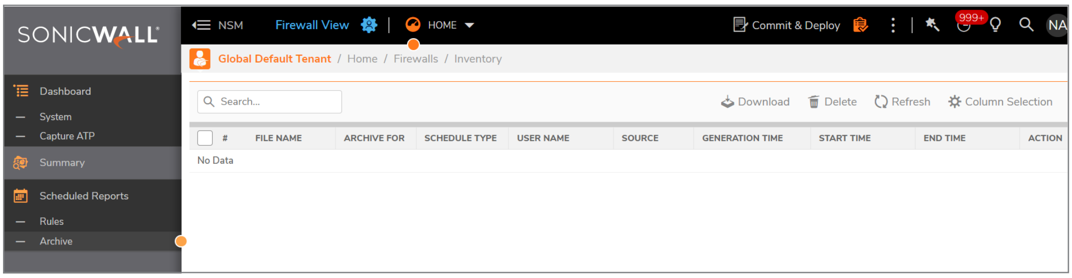
10. Verify that the rule appears in the Rules table.

# Managing Notification History

If you enable saving the History notifications when you set up a rule, the history of the alerts and notifications you received is saved in the History table. The history can be useful when analyzing threats by giving you the ability to access this data at any time for analysis. The notifications and history are tracked at a device level. You need to go to the **Firewall View** of a device to access the History log. You can also export the History log to a CSV file for further analysis.

### *To access the History log:*

1. Navigate to **Manager View | Firewalls > Inventory**.
2. Click the firewall for which you want to see the History logs.
3. Click **Scheduled Reports > Archive**.

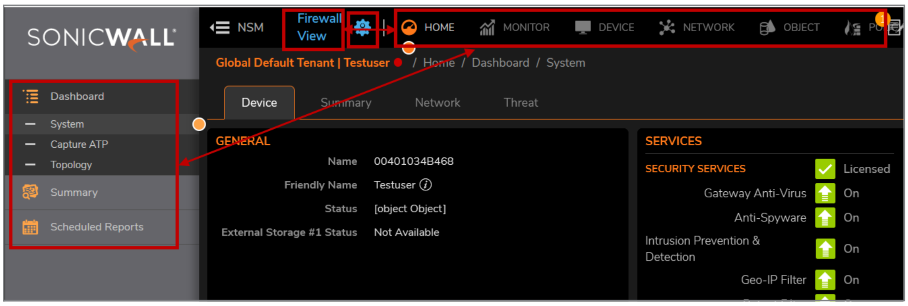


| □ | # | FILE NAME | ARCHIVE FOR | SCHEDULE TYPE | USER NAME | SOURCE | GENERATION TIME | START TIME | END TIME | ACTION |
|---|---|---|---|---|---|---|---|---|---|---|

No Data

# Interface Map

This chapter provides a map of the interface that you can use as a reference to find a specific command. It also refers you to the appropriate documentation for information about that command.



Name 00401034B468
Friendly Name Testuser
Status [object Object]
External Storage #1 Status Not Available

SECURITY SERVICES ✓ Licensed
Gateway Anti-Virus On
Anti-Spyware On
Intrusion Prevention & Detection On
Geo-IP Filter On

ⓘ **NOTE:** The list of commands you can see for each View depends on the user roles, privileges, and the license type that you have.

- Manager View: HOME and MONITOR
- Firewall View
- Group View
- Template View

# Manager View: HOME and MONITOR

This chapter provides a map of the Manager View and MONITOR interfaces that you can use as a reference to find a specific command. It refers you to the appropriate documentation for information about that command.

| NSM View | Options | Left Command Menu |
|---|---|---|
| Manager View | HOME | • Dashboard<br>• System<br>• Firewalls<br>• Inventory<br>• Groups<br>• Templates |

| NSM View | Options | Left Command Menu |
|---|---|---|
| | | Config Management<br>Approval Groups<br>Commits<br>Audit<br>Tenants<br>CSC Users<br>Status<br>Users<br>Support Portal Users<br>Roles and Permissions<br>Users and Devices<br>Scheduled Reports<br>Rules<br>Archive<br>Logs & Alerts<br>Settings<br>Events<br>Cloud<br>Cluster<br>Diagnostics<br>Flow Forwarder Agents<br>Zero Touch Agents<br>Legal Information<br>API |
| Manager View | MONITOR | Summary<br>Applications<br>Users<br>Viruses<br>Intrusions<br>Spyware<br>Web Categories<br>Addresses<br>Locations<br>Details<br>Applications<br>Users<br>Viruses<br>Intrusions<br>Spyware |

| NSM View | Options | Left Command Menu |
|---|---|---|
|  |  | • Web Categories<br>• Addresses<br>• Locations |

# Firewall View

This chapter provides a map of the Firewall View interface that you can use as a reference to find a specific command. It also refers you to the appropriate documentation for information about that command.

| NSM View | Options | Left Command Menu |
|---|---|---|
| Firewall View | HOME | • Dashboard<br>• System<br>• Capture ATP<br>• Topology<br>• Summary<br>• Applications<br>• Users<br>• Viruses<br>• Intrusions<br>• Spyware<br>• Web Categories<br>• Addresses<br>• Locations<br>• Scheduled Reports<br>• Rules<br>• Archive |
| Firewall View | MONITOR | • Overview<br>• Live Monitor<br>• Live Report<br>• Details<br>• Applications<br>• Users<br>• Viruses<br>• Intrusions<br>• Spyware<br>• Web Categories<br>• Addresses<br>• Locations |
| Firewall View | DEVICE | • Settings |

| NSM View | Options | Left Command Menu |
|---|---|---|
|  |  | ◦ Status<br>◦ Licenses<br>◦ Administration Guide<br>◦ Time<br>◦ Certificates<br>◦ SNMP<br>◦ Firmware and Settings<br>◦ Restart<br>• Internal Wireless<br>◦ Status<br>◦ Settings<br>◦ Security<br>◦ Advanced<br>◦ MAC Filter List<br>◦ IDS<br>◦ Virtual Access Point<br>• High Availability<br>◦ Settings<br>◦ Advanced<br>◦ Monitoring<br>• Users<br>◦ Status<br>◦ Settings<br>◦ Local Users & Groups<br>◦ Guest Services<br>◦ Guest Accounts<br>• App Flow<br>◦ Flow Reporting<br>◦ GMSFlow Server<br>• Log<br>◦ Settings<br>◦ Syslog<br>◦ Automation<br>◦ Name Resolution<br>◦ AWS<br>• Diagnostics<br>◦ Tech Support Report<br>◦ DNS Name Lookup |

| NSM View | Options | Left Command Menu |
|---|---|---|
| | | - Network Path<br>- Ping<br>- Trace Route<br>- Real-Time Blacklist<br>- Reverse Name Lookup<br>- Geo and Botnet<br>- PMTU Discovery<br>• Switch Network<br>- Overview<br>- Switches<br>• Access Points<br>- Settings<br>- Firmware Management<br>- Floor Plan View<br>- Topology<br>- Station Status<br>- IDS<br>- Advanced IDP<br>- Packet Capture<br>- Virtual Access Point<br>- RF Monitoring<br>- FairNet<br>- Wi-Fi Multimedia<br>- 3G/4G/LTE WWAN |
| Firewall View | NETWORK | • System<br>- Interfaces<br>- Failover & LB<br>- Neighbor Discovery<br>- ARP<br>- MAC IP Anti-Spoof<br>- Web Proxy<br>- PortShield Groups<br>- VLAN Translation<br>- IP Helper<br>- Dynamic Routing<br>- DHCP Server<br>- Multicast<br>- Network Monitor<br>- AWS Configuration<br>• Firewall |

| NSM View | Options | Left Command Menu |
|---|---|---|
| | | Advanced<br>Flood Protection<br>SSL Control<br>Cipher Control<br>RBL Filter<br>Bandwidth Management<br>VoIP<br>Settings<br>DNS<br>Settings<br>Dynamic DNS<br>DNS Proxy<br>DNS Security<br>SDWAN<br>Groups<br>SLA Probes<br>SLA Class Objects<br>Path Selection Profiles<br>Rules<br>IPSec VPN<br>Rules and Settings<br>Advanced<br>DHCP over VPN<br>L2TP Server<br>AWS VPN<br>SSL VPN<br>Server Settings<br>Client Settings<br>Portal Settings<br>Virtual Office |
| Firewall View | OBJECT | Match Objects<br>Zones<br>Addresses<br>Services<br>URL Lists<br>Match Objects<br>Schedules<br>Dynamic Group<br>Email Addresses<br>Packet Dissection Objects |

| NSM View | Options | Left Command Menu |
|---|---|---|
| | | • Profile Objects<br>• Bandwidth<br>• QoS Marking<br>• Content Filter<br>• DHCP Option<br>• AWS<br>• Action Objects<br>• App Rule Actions<br>• Content Filter Actions |
| Firewall View | POLICY | • Rules and Policies<br>• Access Rules<br>• NAT Rules<br>• Routing Rules<br>• Content Filter Rules<br>• App Rules<br>• Anti-Spam<br>• Status<br>• Settings<br>• Security Services<br>• Summary<br>• Content Filter<br>• Gateway Anti-Virus<br>• Intrusion Prevention<br>• Anti-Spyware<br>• Geo-IP Filter<br>• Botnet Filter<br>• Capture ATP<br>• Settings<br>• Scanning History<br>• Endpoint Security<br>• DPI SSL Enforcement<br>• Client AV Enforcement<br>• Client CF Enforcement<br>• Capture ATP<br>• Settings<br>• Scanning History |

# Group View

This chapter provides a map of the Group View interface that you can use as a reference to find a specific command. It also refers you to the appropriate documentation for information about that command.

| NSM View | Options | Left Command Menu |
|---|---|---|
| Group View | HOME | • Dashboard<br>◦ System<br>◦ Topology<br>• Summary<br>◦ Applications<br>◦ Users<br>◦ Viruses<br>◦ Intrusions<br>◦ Spyware<br>◦ Web Categories<br>◦ Addresses<br>◦ Locations<br>• Scheduled Reports<br>◦ Rules<br>◦ Archive |
| Group View | MONITOR | • Details<br>◦ Applications<br>◦ Users<br>◦ Viruses<br>◦ Intrusions<br>◦ Spyware<br>◦ Web Categories<br>◦ Addresses<br>◦ Locations |
| Group View | DEVICE | • Settings<br>◦ Administration<br>◦ Certificates<br>◦ SNMP<br>◦ Firmware and Settings<br>• Users<br>◦ Settings<br>◦ Local Users & Groups<br>◦ Guest Services<br>◦ Guest Accounts |

| NSM View | Options | Left Command Menu |
|---|---|---|
| | | - App Flow<br>  - Flow Reporting<br>  - GMSFlow Server<br>- Log<br>  - Settings<br>  - Syslog<br>  - Automation<br>  - Name Resolution<br>- Switch Network<br>  - Overview<br>  - Switches |
| Group View | NETWORK | - System<br>  - ARP<br>  - MAC IP Anti-spoof<br>  - Web Proxy<br>  - IP Helper<br>  - Dynamic Routing<br>  - DHCP Server<br>  - Multicast<br>  - Network Monitor<br>- Firewall<br>  - Advanced<br>  - Flood Protection<br>  - SSL Control<br>  - Cipher Control<br>  - RBL Filter<br>  - Bandwidth Management<br>- VoIP<br>  - Settings<br>- DNS<br>  - Settings<br>  - Dynamic DNS<br>  - DNS Proxy<br>  - DNS Security<br>- SDWAN<br>  - Groups<br>  - SLA Probes<br>  - SLA Class Objects<br>  - Path Selection Profiles |

| NSM View | Options | Left Command Menu |
|---|---|---|
| | | • Rules<br>• IPSec VPN<br>• Rules and Settings<br>• Advanced<br>• DHCP over VPN<br>• L2TP Server<br>• SSL VPN<br>• Server Settings<br>• Client Settings<br>• Portal Settings<br>• Virtual Office |
| Group View | OBJECT | • Match Objects<br>• Zones<br>• Addresses<br>• Services<br>• URI Lists<br>• Match Objects<br>• Schedules<br>• Dynamic Group<br>• Email Addresses<br>• Profile Objects<br>• Endpoint Security<br>• Bandwidth<br>• QoS Marking<br>• Content Filter<br>• DHCP Option<br>• Action Objects<br>• App Rule Actions<br>• Content Filter Actions |
| Group View | POLICY | • Rules and Policies<br>• Access Rules<br>• NAT Rules<br>• Routing Rules<br>• Content Filter Rules<br>• App Rules<br>• Endpoint Rules<br>• DPI-SSL<br>• Client SSL<br>• Server SSL |

| NSM View | Options | Left Command Menu |
|---|---|---|
| | | • DPI-SSH<br>• Settings<br>• Security Services<br>• Summary<br>• Content Filter<br>• Gateway Anti-Virus<br>• Intrusion Prevention<br>• Anti-Spyware<br>• Geo-IP Filter<br>• Botnet Filter<br>• App Control<br>• Anti-Spam<br>• Settings<br>• Endpoint Security<br>• DPI SSL Enforcement<br>• Client AV Enforcement<br>• Client CF Enforcement |

# Template View

This chapter provides a map of the Template View interface that you can use as a reference to find a specific command. It also refers you to the appropriate documentation for information about that command.

| NSM View | Options | Left Command Menu |
|---|---|---|
| Template View | DEVICE | • Settings<br>• Administration Guide<br>• SNMP<br>• Firmware and Settings<br>• Users<br>• Settings<br>• Local Users and Groups<br>• Guest Services<br>• Guest Accounts<br>• App Flow<br>• Flow Reporting<br>• AppFlow Agent<br>• Log<br>• Settings |

| NSM View | Options | Left Command Menu |
|---|---|---|
| | | • Syslog<br>• Automation<br>• Name Resolution |
| Template View | NETWORK | • System<br>  • ARP<br>  • MAC IP Anti-Spoof<br>  • Web Proxy<br>  • IP Helper<br>  • DHCP Server<br>  • Multicast<br>  • Network Monitor<br>• Firewall<br>  • Advanced<br>  • Flood Protection<br>  • SSL Control<br>  • Cipher Control<br>  • RBL Filter<br>  • Bandwidth Management<br>• VoIP<br>  • Settings<br>• DNS<br>  • Settings<br>  • Dynamic DNS<br>  • DNS Proxy<br>  • DNS Security<br>• SDWAN<br>  • Groups<br>  • SLA Probes<br>  • SLA Class Objects<br>  • Path Selection Profiles<br>  • Rules<br>• IPSec VPN<br>  • Rules and Settings<br>  • Advanced<br>  • DHCP over VPN<br>  • L2TP Server<br>• SSL VPN<br>  • Server Settings<br>  • Client Settings<br>  • Portal Settings |

| NSM View | Options | Left Command Menu |
|---|---|---|
| Template View | OBJECT | • Match Objects<br>◦ Zones<br>◦ Addresses<br>◦ Services<br>◦ URI Lists<br>◦ Match Objects<br>◦ Schedules<br>◦ Dynamic Group<br>◦ Email Addresses<br>• Profile Objects<br>◦ Endpoint Security<br>◦ Bandwidth<br>◦ QoS Marking<br>◦ Content Filter<br>◦ DHCP Option<br>• Action Objects<br>◦ App Rule Actions<br>◦ Content Filter Actions |
| Template View | POLICY | • Rules and Policies<br>◦ Access Rules<br>◦ NAT Rules<br>◦ Routing Rules<br>◦ Content Filter Rules<br>◦ App Rules<br>◦ Endpoint Rules<br>• DPI-SSL<br>◦ Client SSL<br>◦ Server SSL<br>• DPI-SSH<br>◦ Settings<br>• Security Services<br>◦ Summary<br>◦ Content Filter<br>◦ App Control<br>◦ Gateway Anti-Virus<br>◦ Intrusion Prevention<br>◦ Anti-Spyware<br>◦ Geo-IP Filter<br>◦ Botnet Filter<br>• Anti-Spam |

| NSM View | Options | Left Command Menu |
|---|---|---|
| | | • Settings<br>• Endpoint Security<br>• DPI SSL Enforcement<br>• Client AV Enforcement<br>• Client CF Enforcement<br>• Capture ATP<br>• Settings |

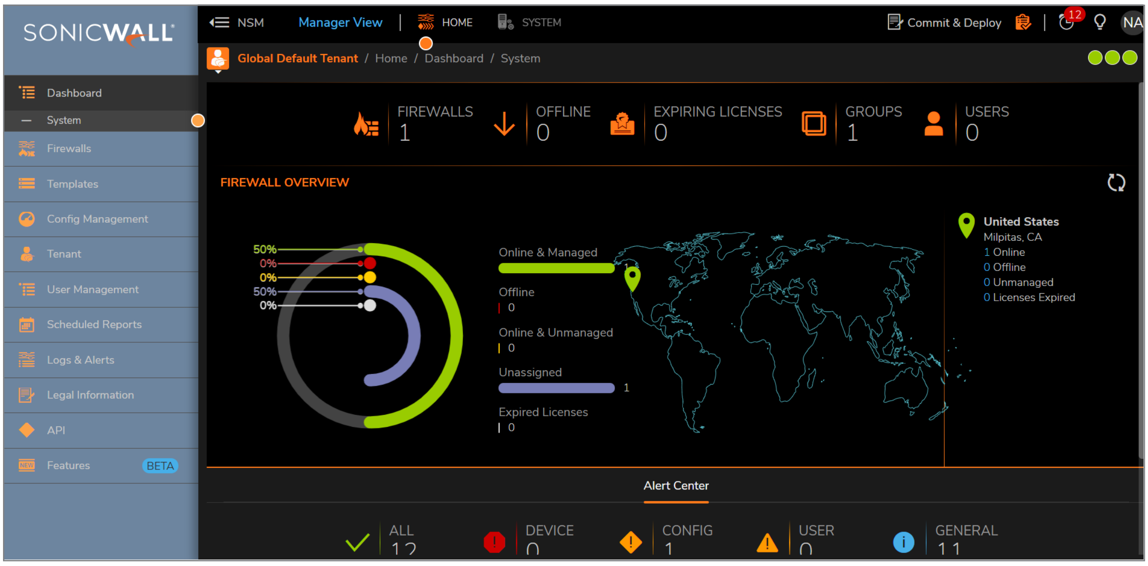
7

# NSM On-Premises

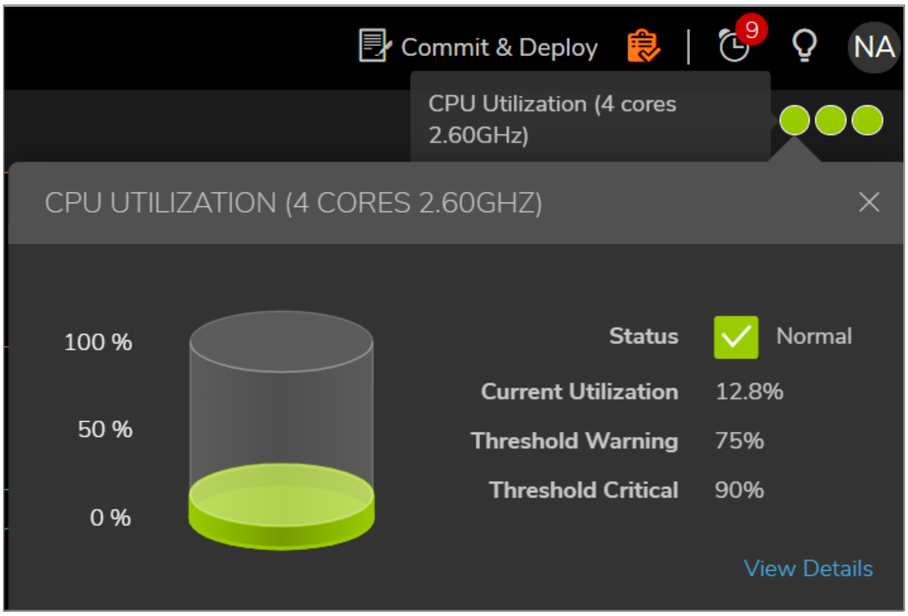
SonicWall offers the option to host NSM on-premises hosted on your organization's local server. NSM on-premises also provides an added level of security by enabling two factor authentication to address the increasing number of cyber security attacks.

When you log in, NSM on-prem provides is the Manager View SYSTEM option by default.

For more information on SYSTEM dashboard, see section Dashboards.



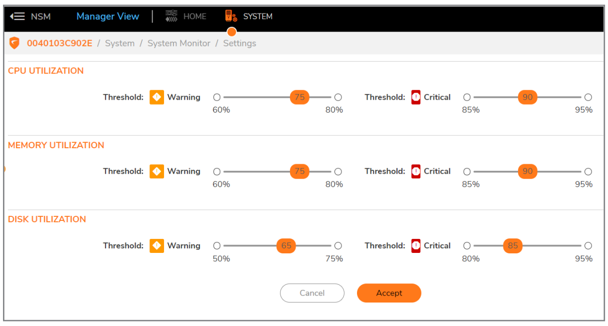
The three green notification icons at the top of the interface display more information on CPU Utilization, Memory Utilization, and Disk Utilization.



CPU UTILIZATION (4 CORES 2.60GHZ)

| | |
|---|---|
| Status | ✓ Normal |
| Current Utilization | 12.8% |
| Threshold Warning | 75% |
| Threshold Critical | 90% |

Click on **View Details** to take a deep dive into the system monitoring details:



CPU UTILIZATION

Threshold: Warning 75 Threshold: Critical 90

MEMORY UTILIZATION

Threshold: Warning 75 Threshold: Critical 90

DISK UTILIZATION

Threshold: Warning 65 Threshold: Critical 85

# Command Options

The following table correlates the which options are available with each view for an NSM on-premise dashboard.

| NSM View | Command Options Available |
|---|---|
| Manager View | HOME<br>SYSTEM |
| Firewall View | HOME<br>DEVICE<br>NETWORK<br>OBJECT<br>POLICY |

| NSM View | Command Options Available |
|---|---|
| Group View | HOME<br>DEVICE<br>NETWORK<br>OBJECT<br>POLICY |
| Template View | DEVICE<br>NETWORK<br>OBJECT<br>POLICY |

Refer to Interface Map for a more detailed NSM interface map.

# On-Prem Icons and Buttons

This section describes some of the icons and options for the NSM on-premises.

| Icons and Labels | Definition |
|---|---|
| **Left Command Menu Icons** | |
| ☰ | Indicates the User Management icon and label. |
| | Indicates the High Availability icon from SYSTEM view. |
| | Indicates the System Monitor icon on the left navigation in the SYSTEM view. |
| | Indicates the Network icon on the left navigation in the SYSTEM view. |
| | Indicates the icon to view Dashboard and Settings in the SYSTEM view. |
| | Indicates the Switching icon in the NETWORK view. |
| **Dashboard Icons** | |
| | Indicates the SYSTEM view. |
| 🟢🟢🟢 | Indicates the notifications for CPU, Memory, and Disk utilization on the Dashboard. |
| ☰ | Indicates the icon to show system reports on the System Dashboard. |

| Icons and Labels | Definition |
|---|---|
| **Left Command Menu Icons** | |
| **Other Icons** | |
| 🔑 | Indicates the icon to change the password for a particular user in User Management section. |
| ○ | Indicates the icon to enable some modes. For example, the Exponential View for a Live Monitor in the System Monitor section. |
| ● | Indicates the icon to disable some modes. For example, the Exponential View for a Live Monitor in the System Monitor section. |
| 🔓 | Indicates that the user is not locked out. |
| + | Indicates the icon to expand permissions, in the Roles and Permissions tab of User Management section. |
| 🟩 | Indicates the icon to collapse permissions, in the Roles and Permissions tab of User Management section. |

8

# SonicWall Support

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

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

The Support Portal enables you to:

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

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

# About This Document

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

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

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

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

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

About Network Security Manager
Updated - June 2021
232-005315-01 Rev B

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