



SonicOS 7.1

Dashboard

Administration Guide

SONICWALL®

Contents

SonicOS Overview	4
Working with SonicOS	4
SonicOS Workflow	6
How to Use the SonicOS Administration Guides	7
Guide Conventions	8
About Dashboard	9
System View	9
Access Point View	10
Topology View	11
Capture ATP View	12
Policy Overview	13
System	14
Device	14
Summary	15
Traffic Distribution	16
Top Users	17
Insights	18
Observed Threats	19
Top Countries	20
DNS Filtering	21
Access Points	23
Feature Limitations	24
Access Point Snapshot	24
Client Association	24
Real-Time Bandwidth	24
Client Report	24
OS Type	25
Radio	25
Top Client	25
Real-Time Client Monitor	25
Client Report and Client Monitor Filtering	25
Topology	26
Managing the Topology View	26

Managing Access Points in the Topology View	27
Editing an Access Point	27
Showing Statistics	27
Monitoring Status on an Access Point	28
Deleting an Access Point	28
SonicWall Support	29
About This Document	30

SonicOS Overview

This guide is a part of the SonicOS collection of administrative guides that describes how to administer and monitor the SonicWall family of firewalls. SonicOS provides network administrators the management interface, API (Application Program Interface), and the Command Line Interface (CLI) for firewall configuration by setting objects to secure and protect the network services, to manage traffic, and to provide the desired level of network service. This guide focuses on the **Dashboard** feature.

Topics:

- [Working with SonicOS](#)
- [Dashboard Introduction](#)
- [How to Use the SonicOS Administration Guides](#)
- [Guide Conventions](#)

Working with SonicOS

SonicOS provides a web management interface for configuring, managing, and monitoring the features, policies, security services, connected devices, and threats to your network. SonicOS runs on top of SonicCore, SonicWall's secure underlying operating system.

The SonicOS management interface facilitates:

- Setting up and configuring your firewall
- Configuring external devices like access points or switches
- Configuring networks and external system options that connect to your firewall
- Defining objects and policies for protection
- Monitoring the health and status of the security appliance, network, users, and connections
- Monitoring traffic, users, and threats
- Investigating events

SonicWall offers two different modes of operation in SonicOS; the modes differ mainly in the areas of policy, object configuration and diagnostics.

- *Policy Mode* provides a unified policy configuration work flow. It combines Layer 3 to Layer 7 policy enforcement for security policies and optimizes the work flow for other policy types. This unified policy work flow gathers many security settings into one place, which were previously configured on different pages of the management interface.
- *Classic Mode* is more consistent with earlier releases of SonicOS; you need to develop individual policies and actions for specific security services. The Classic Mode has a redesigned interface.

This table identifies which modes can be used on the different SonicWall firewalls:

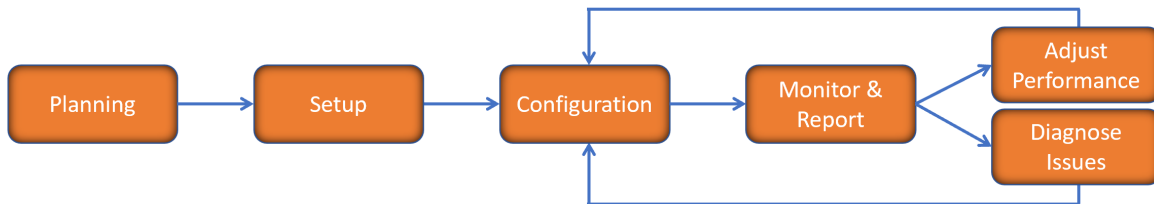
Firewall Type	Classic Mode	Policy Mode	Comments
TZ Series	yes	no	The entry level TZ Series, also known as desktop firewalls, deliver revamped features such as 5G readiness, better connectivity options, improved threat, SSL and decryption performance that address HTTPS bandwidth issues; built-in SD-WAN, and lawful TLS 1.3 decryption support.
NSa Series	yes	no	NSa firewalls provide your mid sized network with enhanced security . They are designed specifically for businesses with 250 and up. it can provide cloud-based and on-box capabilities like TLS/SSL decryption and inspection, application intelligence and control, SD-WAN, real-time visualization, and WLAN management.
NSsp 10700, NSsp 11700, NSsp 13700	yes	no	The NSsp platforms high-end firewalls that deliver the advanced threat protection and fast speeds that large enterprises, data centers, and service providers need.
NSsp 15700	no	yes	The NSsp 15700 is designed for large distributed enterprises, data centers, government agencies and services providers. It provides advanced threat protection like Real-Time Deep Memory Inspection, multi-instance firewall configuration, and unified policy creation and modification, with scalability and availability.
NSv Series	yes	yes	The NSv series firewalls offers all the security advantages of a physical firewall with the operational and economic benefits of virtualization. The NSv firwalls can operate in either Policy Mode or Classic Mode. You can switch between modes, but some configuration information from extra interfaces is removed.

In addition to the management interface, SonicOS also has a full-featured API and a CLI to manage the firewalls. For more information, refer to:

- [SonicOS API Reference Guide](#)
- [SonicOS Command Line Interface Reference Guide](#)

SonicOS Workflow

When working with SonicWall products, you can use the following workflow as a guide for setting up your security solution.

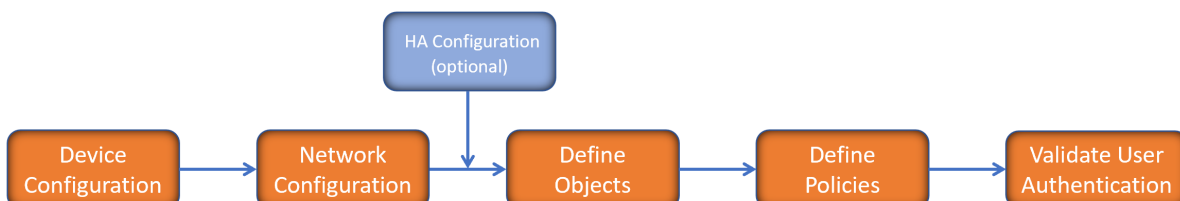


You begin your planning as you start making your purchasing decisions. Your sales partners can help you assess your environment and make recommendations based on the kinds of security services you need. You can learn more about SonicWall products by reviewing [product information](#) and [solutions](#). After selecting the solution, you can schedule your implementation.

After planning and scheduling your solution, you begin setting up the firewalls. The [Getting Started Guides](#) for your products can help you begin setting up the pieces to your solution. The getting started guides are designed to help you install the firewall to a minimal level of operation. Before performing any detailed configuration tasks described in the SonicOS Administration Guides, you should have your firewall set up and basic operation validated.

The configuration block of the workflow refers to the many tasks that combine to define how your firewall is integrated into your security solution and how it behaves when protecting your environment. Depending on the features of your security solution, this task can be quite complex. The System Administration Guides are broken into the key command sets and features. Some documents may be used for all solutions, but others may be used only if you integrated that feature into your solution. For example, High Availability or Wireless Access Points are not necessarily used by all customers. More information about a feature's workflow is presented in the feature administration guide. Refer to the [specific Administration Guide for a SonicOS feature](#) for more information.

Configuration tends to be a one-time activity, although you might make minor adjustments after monitoring performance or after diagnosing an issue. The configuration activity can be broken down into the more detailed flow as the following figure shows. This also mirrors the key functions that are listed across the top of the management interface.

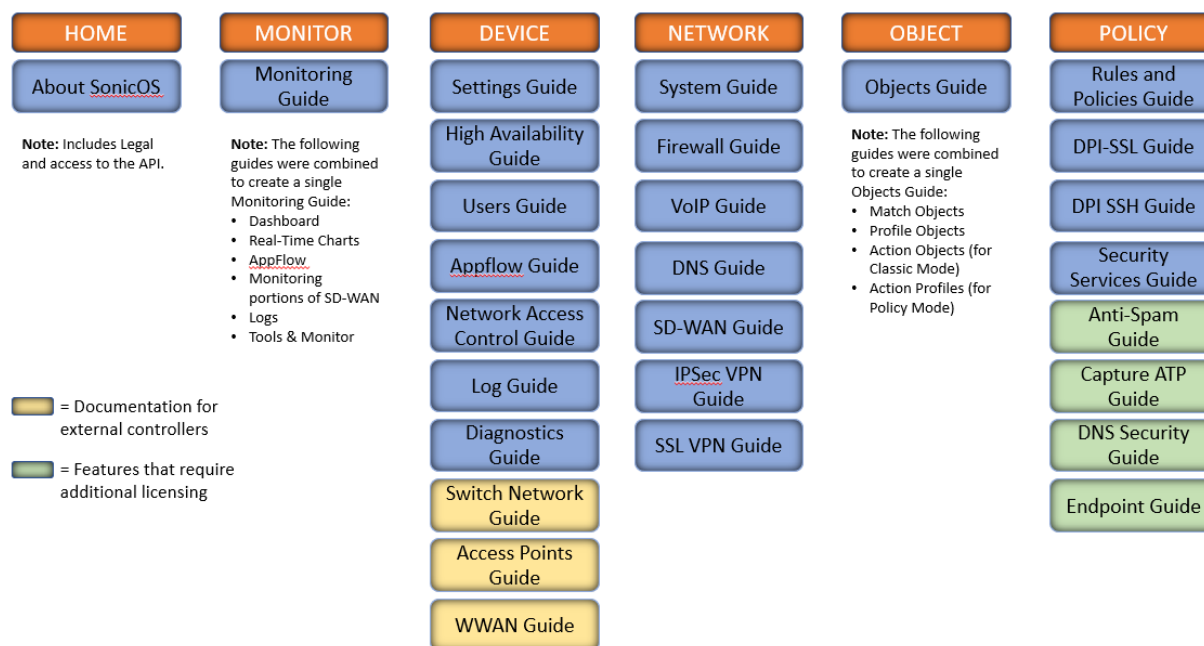


There is some flexibility in the order in which you do things, but this is the general workflow you would follow when configuring your firewall. Start by defining the settings on the firewall. Next you set up the system and other devices that your firewall is connected to, and you can choose to implement High Availability when done. After your device, network, and system is configured, you should define the objects that you want to monitor. Then you use those objects to define the policies that protect your environment. The final step to preparing your setup is to validate the user authentication.

How to Use the SonicOS Administration Guides

The *SonicOS Administration Guide* is a collection of guides that detail the features represented by each of the main menu items in the management interface. Within each guide, you can find topics covering commands in that menu group, along with procedures and in-depth information. The exceptions are the *SonicOS Monitoring Guide* and the *SonicOS Objects Guide* which combine the topics for each of those functions into a single book.

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



The SonicOS Administration Guides, along with related documentation, such as the getting started guides, are available on the [Technical Documentation portal](#).

Guide Conventions

These text conventions are used in this guide:

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

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

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

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

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

Convention	Description
Bold text	Used in procedures to identify elements in the management 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.
Function Menu group > Menu item	Indicates a multiple step menu choice on the user interface. For example, NETWORK System > Interfaces means to select the NETWORK functions at the top of the window, then click on System in the left navigation menu to open the menu group (if needed) and select Interfaces to display the page.
Code	Indicates sample computer programming code. If bold, it represents text to be typed in the command line interface.
<Variable>	Represents a variable name. 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, such as serialnumber=2CB8ED000004 .
Italics	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.

About Dashboard

The Dashboard feature is a key function of SonicWall SonicOS, where you can quickly see if anything in your network is impacting performance. This part of the guide describes the elements of the different views and how they can be used to drill down to more detailed information. The Dashboard can be your starting place for monitoring performance. Symbols and colors are used to indicate whether things are operational, need attention, or if a problem needs to be resolved. Each view provides visibility into the health of the associated network elements. The Dashboard shows different options depending upon whether you are operating in Classic Mode or Policy Mode and the features licensed for your network:

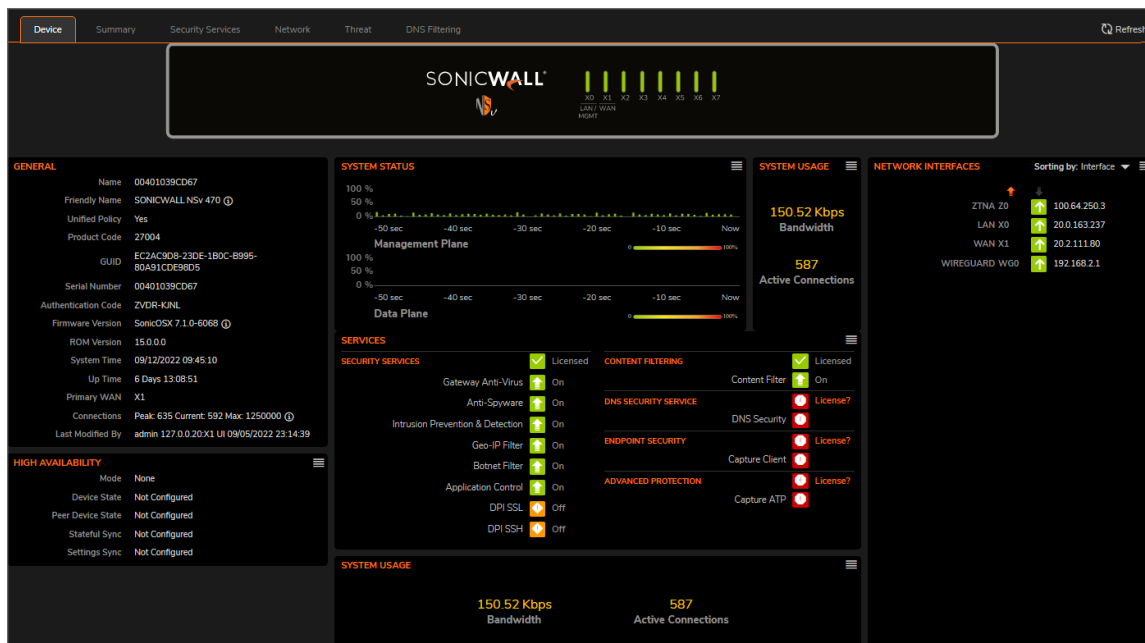
Topics:

- [System View](#)
- [Access Point View](#)
- [Capture ATP View](#)
- [Topology View](#)
- [Policy Overview](#)


① **NOTE:** The images in this document may not be an exact match of what you see when you manage your firewall. The interface you see reflects the type of firewall you chose and the features you configured and licensed. Specific differences are noted when possible.

System View

The **System** view of the SonicOS Dashboard provides a summary of the information that the firewall. The navigation path for the **System** view is **HOME > Dashboard > System**.



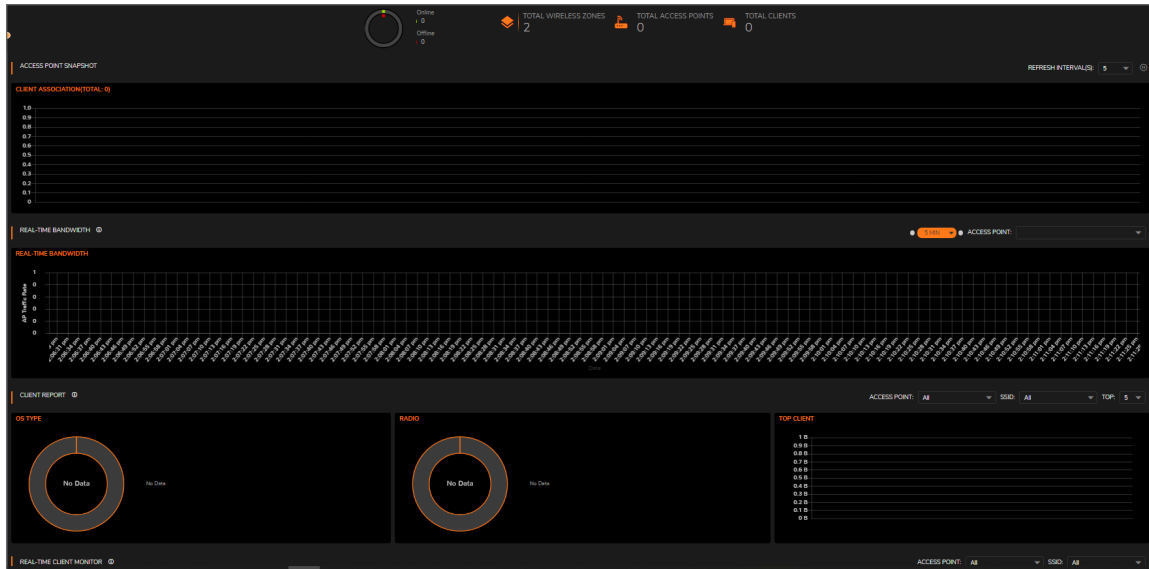
The **System** view offers a high level view of the system performance. You can select different tabs for different types of summaries. They include **Device**, **Summary**, **Security Services**, **Network**, **Threat**, and **DNS Filtering**. Each pane on the tab represents a specific feature being tracked. If you see issues that need more investigation,

you can drill down on the options icon, , in the upper right corner. This takes you to other reports that can help you narrow the source of the issue.

For more information about the **System** option, refer to [SonicOS 7.1 System Administration Guide](#).

Access Point View

The **Access Points** view of the SonicOS Dashboard summarizes the information about the access points in the network. The navigation path for the **Access Points** view is **HOME > Dashboard > Access Points**.



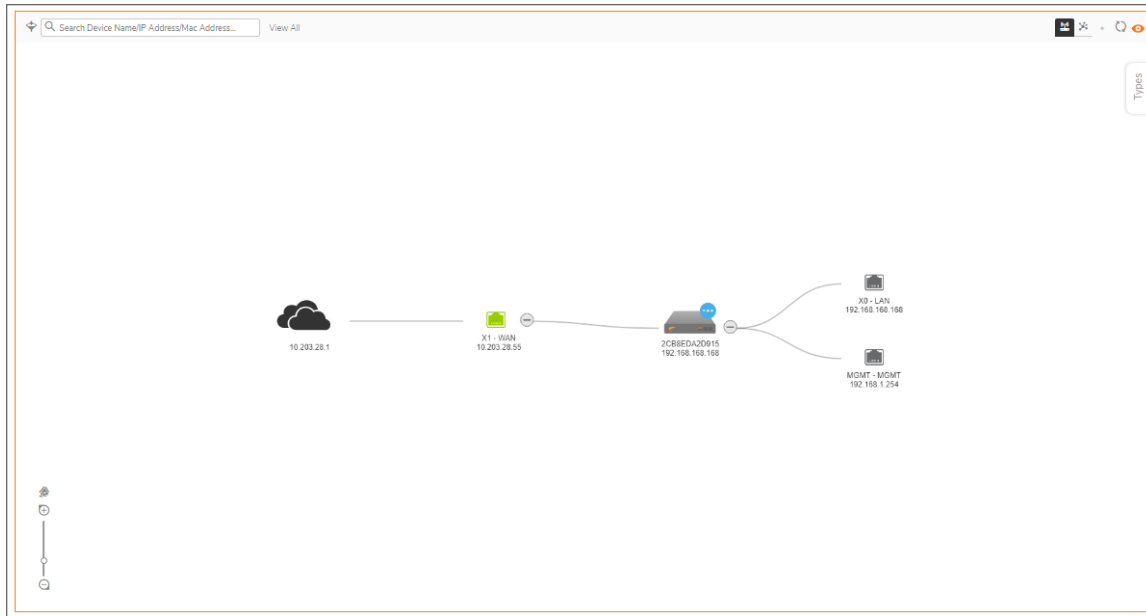
The **Access Points** view offers a high level view of the performance of the access points in the network. You can review the summaries across the top of the page and then scroll to see the different reports.

① | **NOTE:** If you have no access points configured, the reports will be blank.

For more information about the access point, refer to [SonicOS 7.1 Access Points Administration Guide](#).

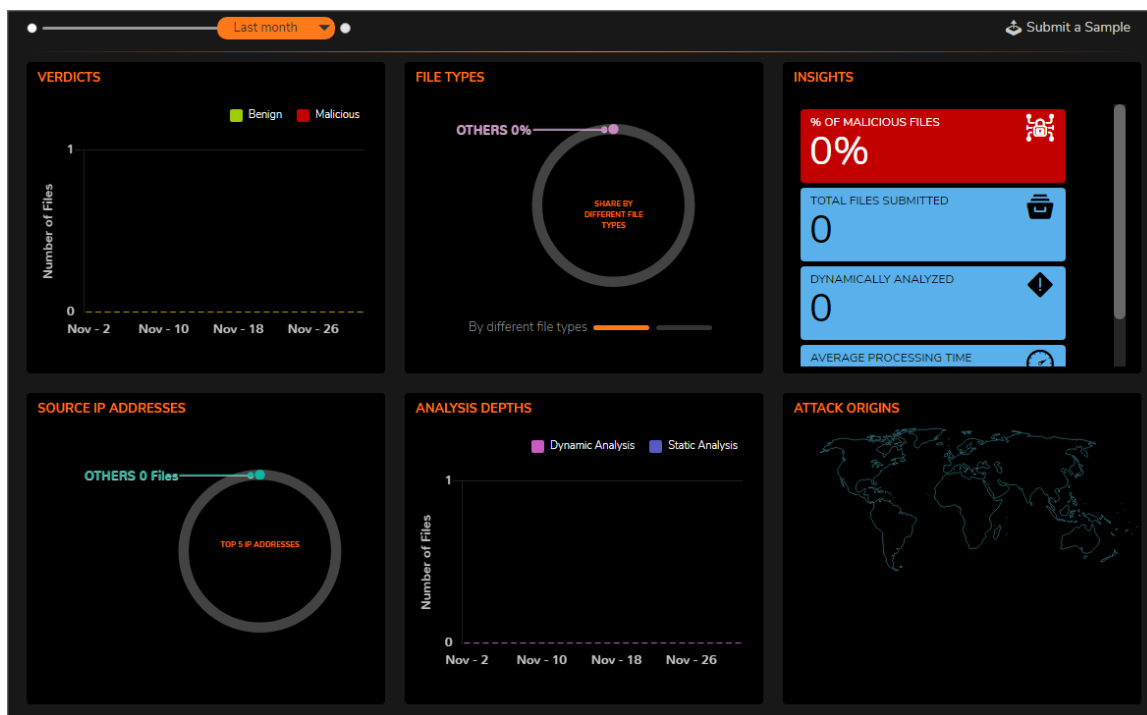
Topology View

The **Topology** view of the SonicOS Dashboard provides a graphic view of the network. The navigation path for the **Topology** view is **Home > Dashboard > Topology**.



Capture ATP View

The **Capture ATP** view of the SonicOS Dashboard, you can quickly see in one place which files are being sent to the backend for scanning and which ones are being blocked. The navigation path for the **Capture ATP** view is **.HOME > Dashboard > Capture ATP**.




For more information about the Capture ATP, refer to [SonicOS 7.1 Capture ATP Administration Guide](#).

Policy Overview

When operating in Policy Mode, the **Policy Overview** option displays on the dashboard. The SonicOS Dashboard summarizes policy effectiveness for different match attributes. The navigation path for the **Policy Overview** is **HOME > Dashboard > Policy Overview**



You can review the different types of summaries by selecting the different tabs: **Policies**, **Objects**, **Groups**, and **Profiles and Signatures**. If you see issues that need more investigation, you can drill down on the options icon, , in the upper right corner. This takes you to other reports that can help you narrow the source of the issue.

For more information about managing in Policy Mode, refer to [SonicOS 7.1 Rules and Policies Administration Guide for Policy Mode](#).

System

Think of the **System** view as the starting point for most tasks. From the **System** page, you can select one of the tabs to see the data from a specific point of view

Topics:

- [Device](#)
- [Summary](#)
- [Network](#)
- [Threat](#)

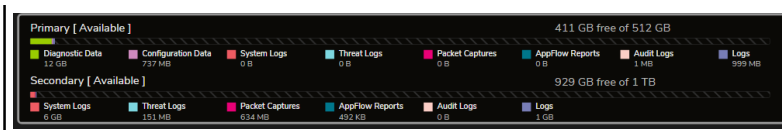
❗ | **IMPORTANT:** Zero Touch is not supported in SonicOS when implemented with on-premises Analytics.


Device

HOME | Dashboard > System | Device displays the relevant information for the unit connected to your system. You have a physical view of the firewall at the top with window, followed by panes that summarize various information categories.



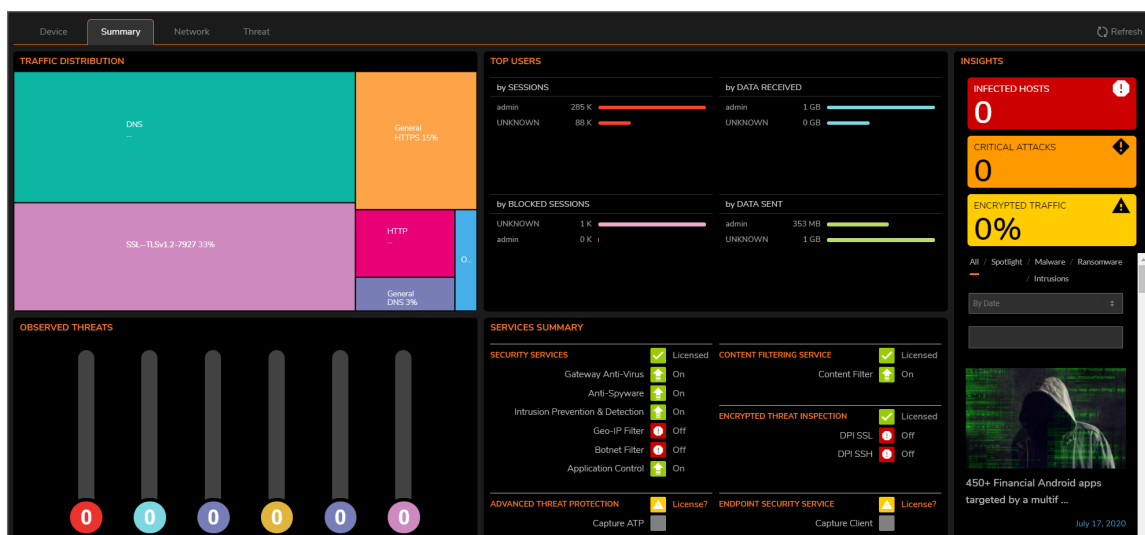
❗ | **NOTE:** The image above illustrates and NSsp 10700 with the Storage feature. Your firewall view may vary slightly depending on the features you enabled and the type of firewall you have. For example, if you have extra storage, you can select **Storage** option, and see how the storage is distributed among the various logs as shown below.



If you see issues on the dashboard that need more investigation, you can drill down on the options icon, , in the upper right corner. This takes you to other reports that can help you narrow the source of the issue.

Summary

The System Summary —located at **HOME | Dashboard > System > Summary**, provides a high-level view of the status of your security infrastructure. It summarizes the activity in easy-to-read, color-coded indicators. You can review the Summary and see at-a-glance when any issues might need investigating.



The **Summary** shows your devices and a representation of the traffic being generated. It allows you to view the devices in a geographical view using a map that you can zoom in and out of. The devices are marked on the map.

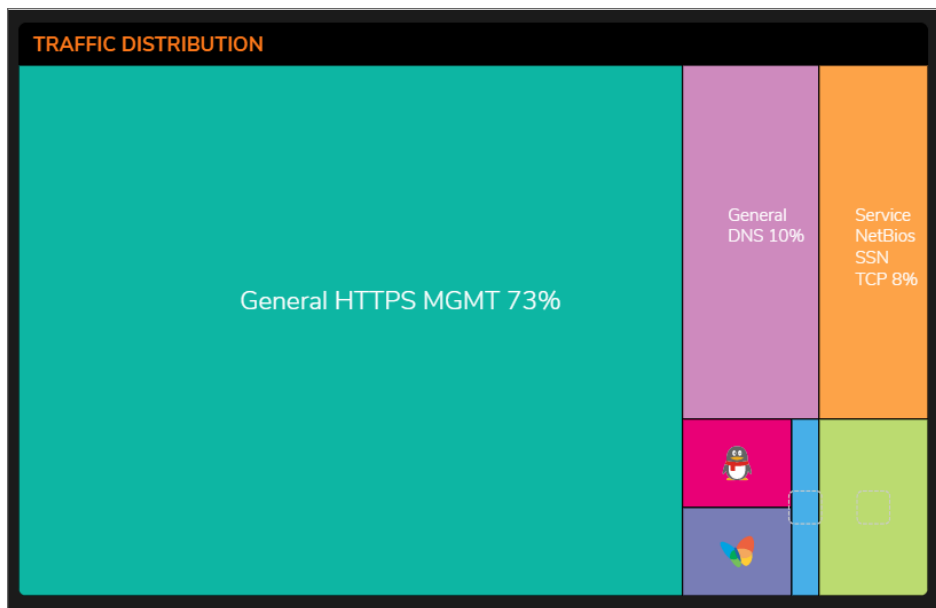
The following table describes the components that make up the **System Summary**.

SYSTEM SUMMARY

Feature	Description
Traffic Distribution	Displays all traffic within your infrastructure including threats and their locations.
Top Users	Provides data as it relates to the users connected to the system.
Insights	Provides a high-level view of the overall status of your security infrastructure.
Observed Threats	Tracks the number of system connections reporting triggered threats.
Top Countries	Show Top Countries sorted by Sessions

Traffic Distribution

The **TRAFFIC DISTRIBUTION** window displays all traffic within your infrastructure including threats and their locations. The threats are visually placed on the global map. You can use the roller on your mouse to zoom in or zoom out on a threat. This kind of data allows you to perform a deep dive on all the information available to you.



TRAFFIC DISTRIBUTION shows your devices and a representation of all traffic being generated. This window allows you to view the devices with a geographical view using a map that you can zoom in and out of. The devices are marked on the map.

This map provides PRIVATE IPs, FIREWALLS, THREATS, INCOMING TRAFFIC, and OUTGOING TRAFFIC information.

You can drill-down for more information on the TRAFFIC MAP segment as well. Use the mouse wheel to Zoom in and out on the global map or use the vertical + and - slider on the left side of the map. Click the flags and icons on the map to drill-down for additional details.

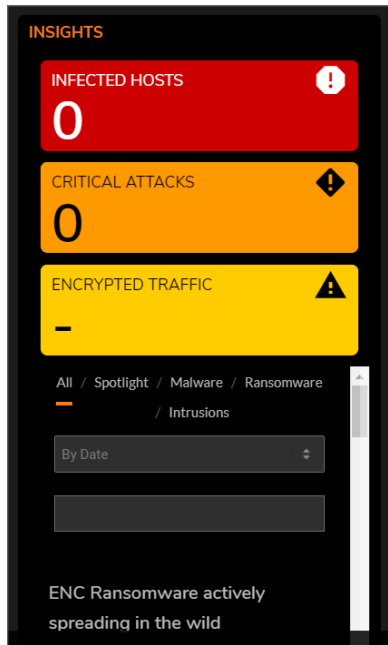
Top Users

The **Top Users** report window provides data as it relates to the users connected to the system. You can track user-level transactions and activities by filtering on several different options, including sessions, bytes received, bytes sent, and bytes blocked.



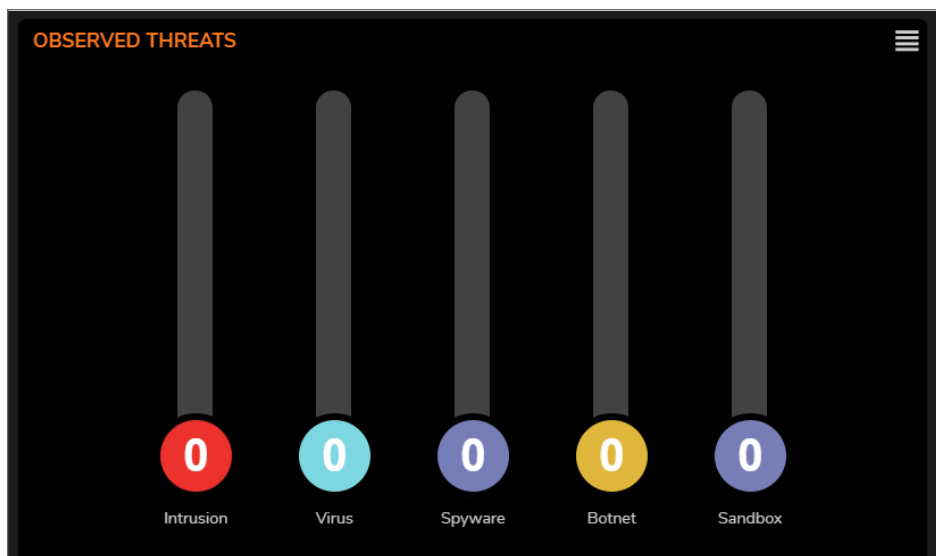
Insights

The Insights window provides a high-level view of the overall status of your security infrastructure. This window summarizes the activity in easy-to-read, color-coded indicators. You can review the Insights and see at-a-glance whether any issues need investigation, as well as additional filtering through spotlighting, malware, ransomware, intrusions, or all the above.



Observed Threats

Observed Threats tracks the number of system connections reporting triggered threats. The default view is Total connections, but you can filter with top intrusions, viruses, spyware, and botnets in the Threat drop-down lists. Navigate to **HOME | Dashboard > System > Threat** to see the various threat reports available. Click the **View Details** icon in each window to expand the available filtering options.



Top Countries

The **Top Countries by Sessions** report provides data as it relates to the country locations connected to the system.



COUNTRY	SESSIONS
? Private	54.27 KB
? Unknown	1.41 KB

[View Details...](#)

You can track location-level transactions and activities by filtering on several different options including **Top Countries by:**

- **Dropped**
- **Bytes Received**
- **Bytes Sent**



Click **View Details** to see complete reporting on all Countries located in **MONITOR | AppFlow > AppFlow Report | Location**.

DNS Filtering

The DNS Filtering reports provide an summary and allows you to export the data.



The **DNS Filtering Data** pane shows the number of events by category:

- **Allow**
- **Block**
- **Negative Reply**
- **Forge IP**

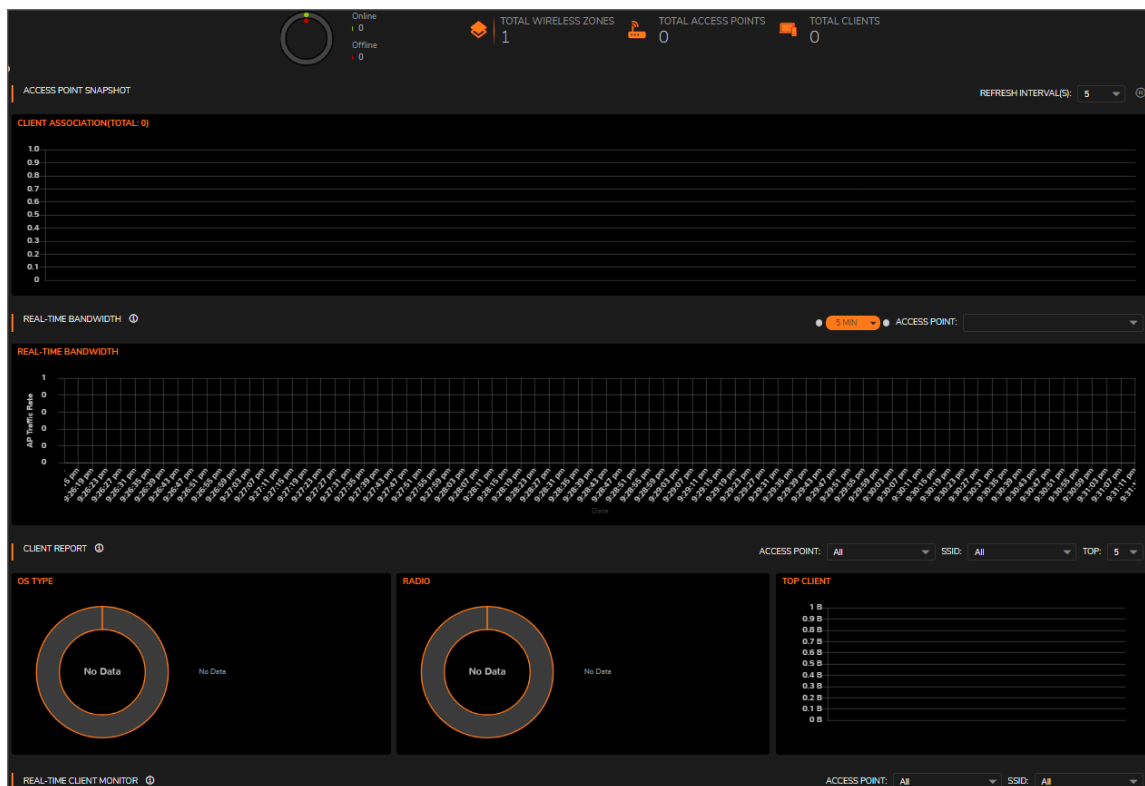
The **Top Security** pane identifies the malware detected by type. You can select a **Graph** view or a **List** view by clicking the appropriate icon. The categories and counts are provided in either view.

The **Top Mature** pane identifies the how much adult, or mature, content traverses your network. The categories and number of events are listed. You can select either a **Graph** view or a **List** view of the data by clicking the appropriate icon.

The **Top Enterprise** pane identifies the how much content can be identified by Gaming, Social or Sports enterprises. The categories and number of events are listed. You can select either a **Graph** view or a **List** view of the data by clicking the appropriate icon.

Access Points

For SonicWave, **HOME | Dashboard > Access Points** uses charts and graphs to help visualize the data related to the access points that are connected to your network. You can display both real-time status and historical status, as well as each client's rate, OS type, and host name. This Dashboard also displays the status of the SonicWave devices and provides information to help with monitoring problematic diagnosis.



A summary of the access points are shown at the top of the page. The data is presented as a doughnut chart; online is green and offline is red. The Online status includes operational, disabled, rebooting, and in IDS scanning mode. Offline status includes unresponsive and initializing states.

The count for the **Total Wireless Zones**, **Total Access Points** and **Total Clients** are also displayed.

Feature Limitations

SonicWave and SonicPoint AC device status is displayed on when the device is managed by a SonicWall firewall. Both the firewall and the access point needs to be functional or no valid data can be exchanged. SonicWave access points always retain a seven-day history of the dashboard data. However, because of memory limitations, SonicPoint AC devices lose all history data when they are rebooted.

Access Point Snapshot

One graph is shown in the **Access Point Snapshot** section. In the right corner, you can specify the refresh interval for these charts. Select the number of minutes from the drop-down menu; the options range from 5 to 10 minutes.

Client Association

The **Client Association** chart shows the number of clients associated with each access point in the configuration. The number of users is shown in bar chart form.

Real-Time Bandwidth

A graph showing the bandwidth being used by the selected access point is displayed in the **Real-Time Bandwidth** section of the **HOME | Dashboard > Access Points**.

① | **NOTE:** Only SonicPoint ACe/ACi/N2 and SonicWave devices support the **Real-Time Bandwidth** feature.

SonicOS shows a stacked chart of the real-time traffic on the selected access point(s). The Y value is the total traffic, both received and transmitted. By default, all access points are selected for the display.

To select the refresh interval, select the interval period from the drop-down menu by the chart title. Options are: 1 minute, 2 minutes, 5 minutes, 10 minutes, and 60 minutes.

To change the access point being displayed, go to the **Access Point** drop-down menu and select a different device. The chart updates with the data for that access point.

Client Report

Three graphs are shown in the **Client Report** section of the **HOME | Dashboard > Access Points: OS Type, Radio, and Top Client**.

① | **NOTE:** Only SonicPoint ACe/ACi/N2 and SonicWave devices support the **Client Report** feature.

OS Type

The **OS Type** pie chart displays the percentages of connected Windows clients, Macintosh clients, Linux clients, iPhones, Android, and so on. If the client has not generated any HTTP traffic, it might show as **Unknown**.

① | **NOTE:** Only SonicPoint ACe/ACi/N2 and SonicWave devices support the **OS Type** feature.

Radio

The **Client Report** also provides a **Radio** chart. The **Radio** chart shows the percentage of clients connected to the 2.4GHz radio and the 5GHz radio.

① | **NOTE:** Only SonicPoint ACe/ACi/N2 and SonicWave devices support the **Radio** feature.

Top Client

The **Top Client** chart shows the clients who are using the most bandwidth. By going to the **TOP** field and selecting a number from the drop-down menu, you can show the top 5, top 10, top 15 or top 20 consumers for bandwidth. The values for both transmitting and receiving data are shown for the top users.

① | **NOTE:** Only SonicPoint ACe/ACi/N2 and SonicWave devices support the **Top Client** feature.

Real-Time Client Monitor

A graph showing the client connection details is displayed in the **Real-Time Client Monitor** section of the **HOME | Dashboard > Access Points**. This provides the detail for each user connected through the access points. You can see MAC addresses, host names, OS type, volume of traffic being received (Rx), and the volume of traffic being transmitted (Tx).

① | **NOTE:** Only SonicPoint ACe/ACi/N2 and SonicWave devices support the **Real-Time Client Monitor** feature.

Client Report and Client Monitor Filtering

You can filter the output in both the **Client Report** section and the **Real-Time Client Monitor** section by selecting **All** or a specific access point in the **Access Point** drop-down menu, and/or by selecting **All** or a specific SSID in the **SSID** drop-down menu.

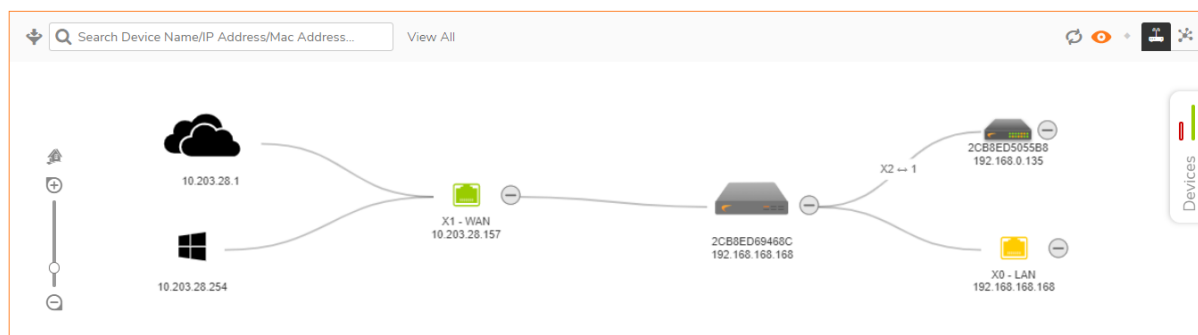
① | **NOTE:** Only SonicPoint ACe/ACi/N2 and SonicWave devices support client detail filtering.

Topology

On the **HOME | Dashboard > Topology** page, devices can be managed with the **Topology** feature. **Topology** shows the network topology from the SonicWall firewall to the wireless access point. The access point real-time status can be monitored, and the context menu also provides configuration options.

This feature shows the logical relationship among all WAN, LAN, and WLAN zone devices, and provides a way to manage devices directly in the **Topology**.

The **HOME | Dashboard > Topology** page displays a tree-like or mesh diagram showing connected devices known to the firewall and their relationships, similar to the following figure:



Topics:

- [Managing the Topology View](#)
- [Managing Access Points in the Topology View](#)

Managing the Topology View

The Topology View is a simple interface. It provides the means to keep the view current and to modify the physical devices in the infrastructure.

You can also get detailed information on each of the devices in the Topology View. Just run your cursor over the device and a tool-tip bubble pops up. Depending on the type of device, it shows information like Name, IP

address, Interface, and Model. For access points, you can also see additional information like status and number of clients.

Each access point also uses color to indicate status:

- Green = online
- Red = offline
- Yellow = busy

Managing Access Points in the Topology View

The Topology View has a context menu with commands that can be used to manage your access points.

① | **NOTE:** Only access points have context menus. None of the other devices in the topology map do.

Topics:

- [Editing an Access Point](#)
- [Showing Statistics](#)
- [Monitor Status on an Access Point](#)
- [Deleting an Access Point](#)

Editing an Access Point

To edit an access point in the Topology View::

1. Navigate to **HOME | Dashboard > Topology**.
2. Roll your mouse over the access point you want to edit.
3. Right-click on the access point.
4. Select **Edit this Access Point**.
5. Make changes to the object configuration as needed.
6. Click **OK** to save new settings.

Showing Statistics

To show statistics for an access point:

1. Navigate to **HOME | Dashboard > Topology**.
2. Roll your mouse over the access point you want to show.
3. Right-click on the access point.
4. Select **Show Access Point Statistics**.

5. Click **REFRESH** if you want to refresh the statistics.
6. Click **OK** when done.

Monitoring Status on an Access Point

To edit an access point in the Topology View:

1. Navigate to **HOME | Dashboard > Topology**.
2. Roll mouse over the access point you want to monitor.
3. Right-click on the access point.
4. Select **Monitor Access Point Status**.
The Access Point Monitor shows system status for the access point. It includes CPU usage, Memory Usage, Rx Rates and Tx Rates.
5. Click **REFRESH** if you want to refresh the data.
6. Click the **Details** icon if you want to see the details on the access point.
7. Click **OK** when done.

Deleting an Access Point

To delete an access point in the Topology View:

1. Navigate to **HOME | Dashboard > Topology**.
2. Roll your mouse over the access point you want to delete.
3. Right-click on the access point.
4. Select **Delete Access Point**.
5. Confirm that you want to delete the access point; cancel if you do not.

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

SonicOS Dashboard Administration Guide

Updated - December 2023

Software Version - 7.1

232-006092-00 Rev A

Copyright © 2023 SonicWall Inc. All rights reserved.

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

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

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

End User Product Agreement

To view the SonicWall End User Product Agreement, go to: <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