Wireless Network Manager

Administration Guide

SONICWALL®

Contents

1

Getting Started with Wireless Network Manager

This SonicWall Wireless Network Manager Administration Guide gives you information to manage the security of your network.

Topics:

- About Wireless Network Manager
- Using the Wireless Network Manager Interface

About Wireless Network Manager

SonicWall Wireless Network Manager is a cloud-based network management system that simplifies Wi-Fi Access Points and secure Switches, access-point deployment, management, and monitoring. Wireless Network Manager is fully integrated with Capture Security Center, Capture Security Appliance, providing seamless integration with MySonicWall, Licensing, and the SonicExpress mobile app on your mobile device. The cloud-based infrastructure is user-friendly and resilient, simplifying access, control, and troubleshooting. Wireless Network Manager is deployed across multiple regions, and is accessible from anywhere through an Internet connection.

The SonicWave access point devices in the Wireless Network Manager network handle all aspects of authentication, association, fast and secure roaming, data forwarding, and power and channel management. Even if the Internet goes down, the Wi-Fi stays up, so you can still reach critical network resources such as files, servers and databases.

Using the Wireless Network Manager Interface

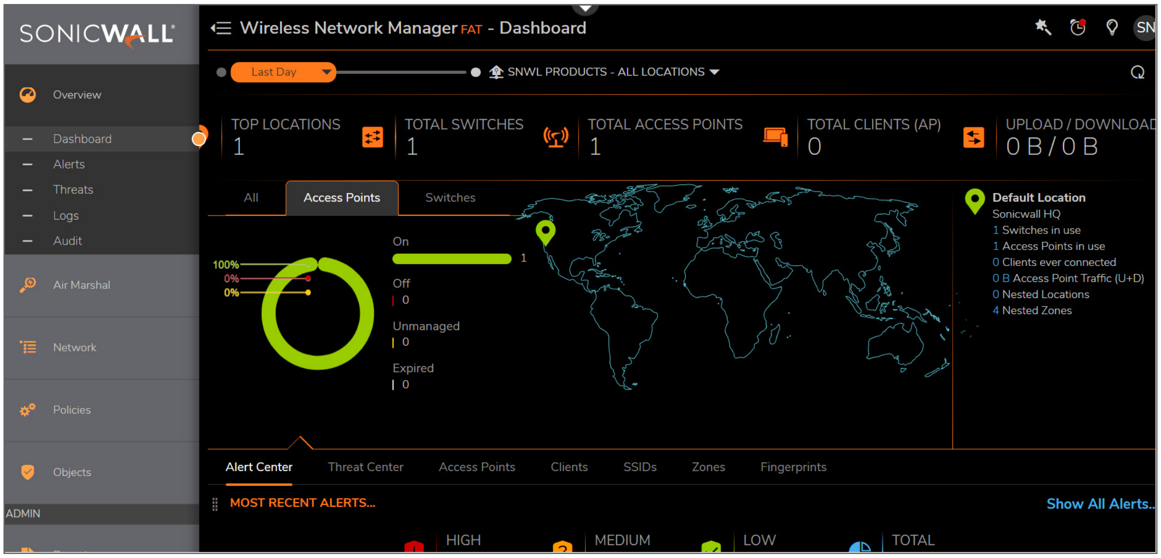
The first screen that appears when you launch Wireless Network Manager is the main screen seen below. It is from this screen that most of the activities and options start in Wireless Network Manager. The Wireless Network Manager user interface has a main navigation pane down the left side. It is from this pane that the user makes choices for navigating through the various Wireless Network Manager tools, features, and displays. The small arrow at the top middle of the screen sends you back to the Capture Security Center. Many of the secondary screens have an icon on the upper right border of the screen that, when clicked, sends you back to the main screen for that navigation pane item.

Clicking an option on the left navigation pane can sometimes open other choices. The principal headings on the navigation pane are:

- Overview
- Air Marshal
- Network
- Policies
- Objects
- Admin (which includes Reports, Users, Settings, and Certificates)
- Tools (which includes WiFi Planner)

Click on a heading, some of these areas can be expanded or collapsed to show any additional sections or just the main headings.

The **Dashboard**, shown here, is the screen that is active when you sign in. On the screen below, all of the topics on the navigation pane are expanded to show the full range of choices. The small orange circle to the right of the navigation pane indicates which choice is currently active on the screen. This marker carries through the various screens resulting from steps started on the main screen. Other choices also appear from time to time within the various screens. By hovering over one of your locations, for example, you can bring up information about it. On some screens, hovering over a row brings up options to be applied to that row.



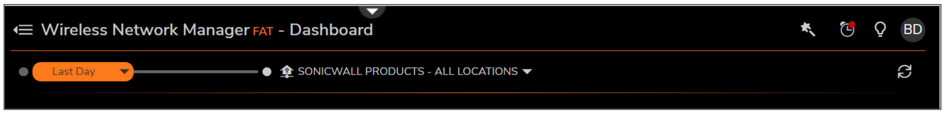
The topics available in this guide explains each of the choices on the navigation pane, describing the selections that are available, and the screens and features that appear with each selection. This will help you configure and use Wireless Network Manager.

Using Wireless Network Manager Guide

The Wireless Network Manager User Guide is an intuitive option available in the interface that guides you the steps needed to setup a new device. It also displays a screenshot of the interface as you navigate using the arrows. In each step, there is a button that directs you to the page where you can perform the necessary actions.

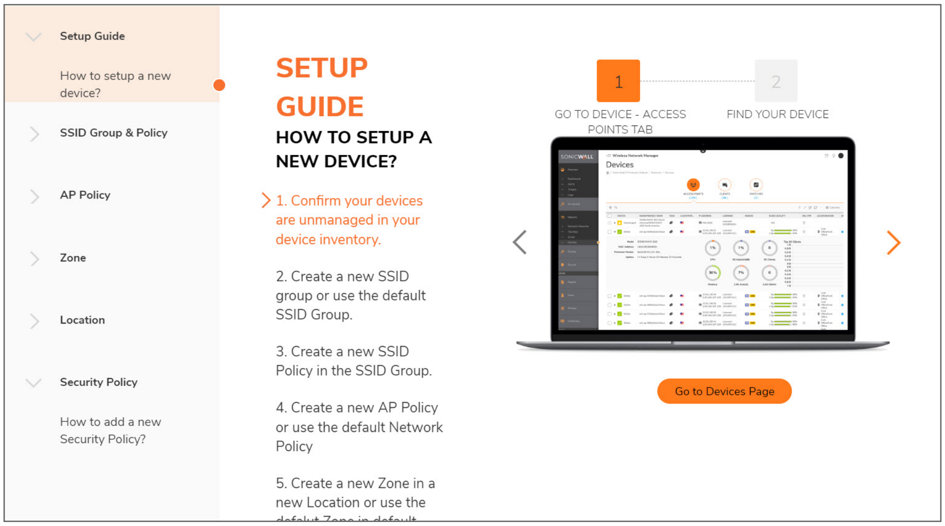
To navigate to Wireless Network Manager Guide:

1. In the first screen that appears when you launch Wireless Network Manager, there are icons on the top right of the screen. Click and it opens WirelessGuide in a separate window.


Wireless Network Manager FAT - Dashboard
BD
Last Day
SONICWALL PRODUCTS - ALL LOCATIONS

   You can choose to resize, minimize or close the window. While going through the steps, you may close the window and if you click the icon again, you can resume from where you left off.

2. You can see the sections listed in the left view, step-by-step instructions in the right view with the screenshot of the respective steps. You also have an option to choose **Creating New** if you are creating a new device; or **Default** for the default settings.



SETUP GUIDE

HOW TO SETUP A NEW DEVICE?

1. Confirm your devices are unmanaged in your device inventory.

2. Create a new SSID group or use the default SSID Group.

3. Create a new SSID Policy in the SSID Group.

4. Create a new AP Policy or use the default Network Policy

5. Create a new Zone in a new Location or use the

2

Overview

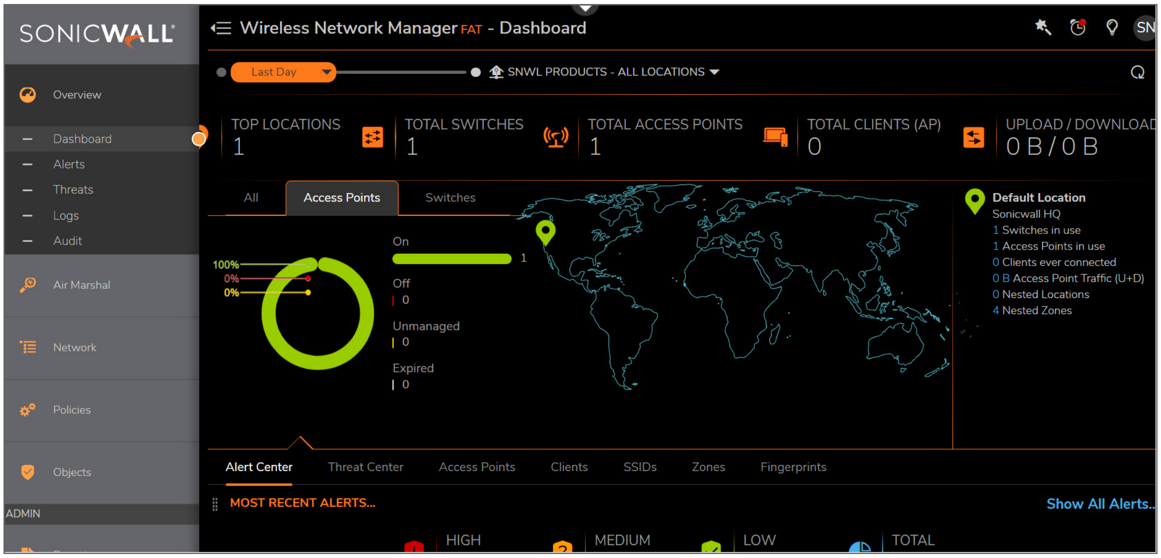
The **Overview**, at the top of the navigation pane, includes four screen sets:

- Dashboard
- Alerts
- Threats
- Logs
- Audit

These screens provide an overview of the information Wireless Network Manager can provide, and allow the user to make choices about configuring the Wireless Network Manager environment.

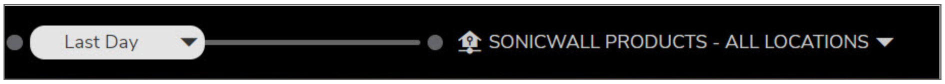
Dashboard

The **Dashboard** provides a global map that displays all of your wireless deployment sites around the world.



- The deployment details regarding the total number of devices and total traffic appear when you hover over each access point location on the map.

- The time slider tool at the top of the screen, can be used to adjust the time period displayed.

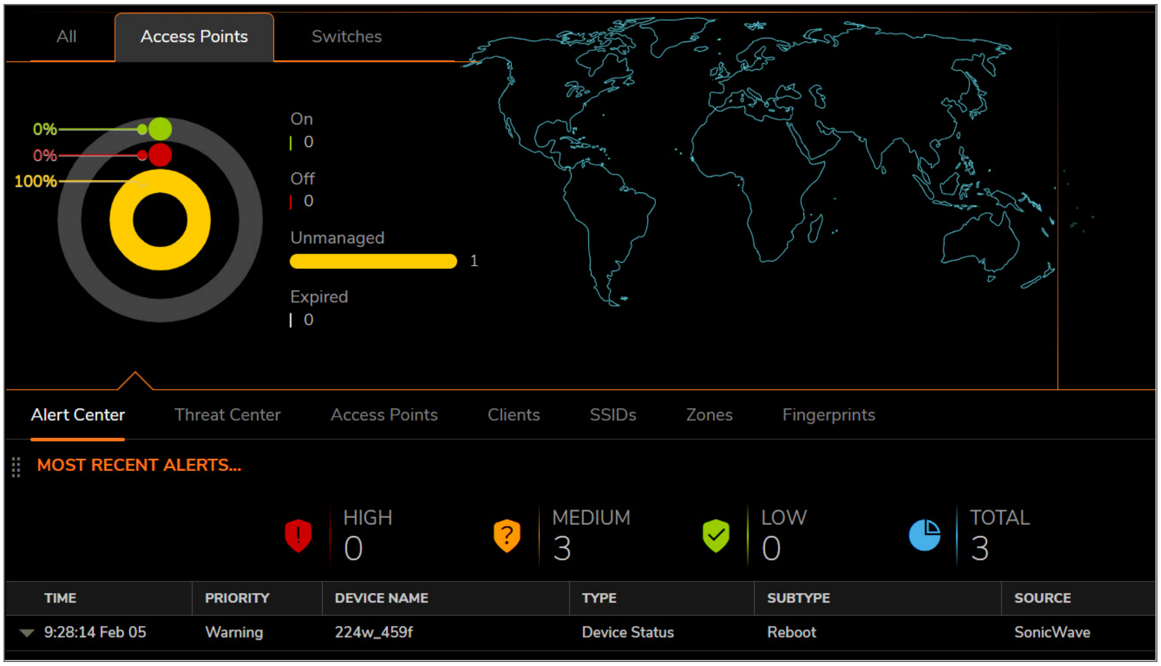


You can select any of the following:

- **Last Day**: The events that have taken place within the previous 24 hours
- **Last Week**: The events that have taken place within the previous 7 days
- **Last 30 Days**: The events that have taken place within the previous 30 days

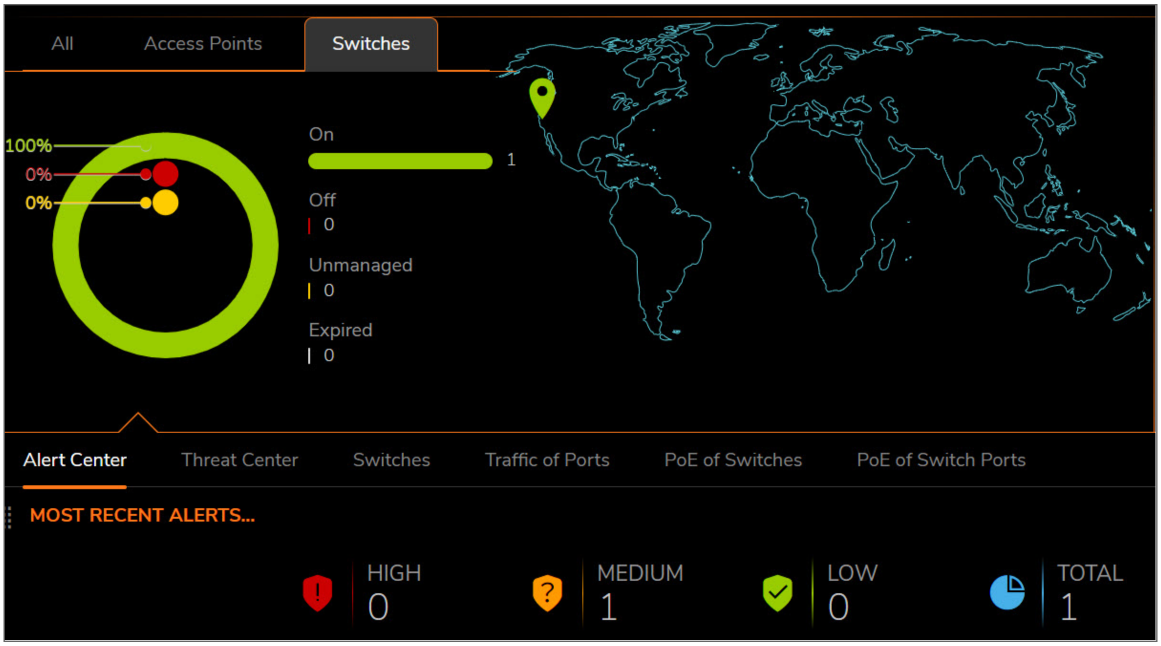
The three tabs display different options further down on the page. By default the **All** tab is selected (as shown in the screen above) in the top half of the screen that also displays the options down - **Alert Centre** and **Threat Centre.**

If you select the tab **Access Points**, the screen displays the AP statistics for the access points on-line, off-line, unmanaged, and with expired licenses. When you select this tab, the options down displayed are **Alert Centre**, **Threat Centre**, **Access Points**, **Clients**, **SSIDs**, **Zones**, and **Fingerprints**.



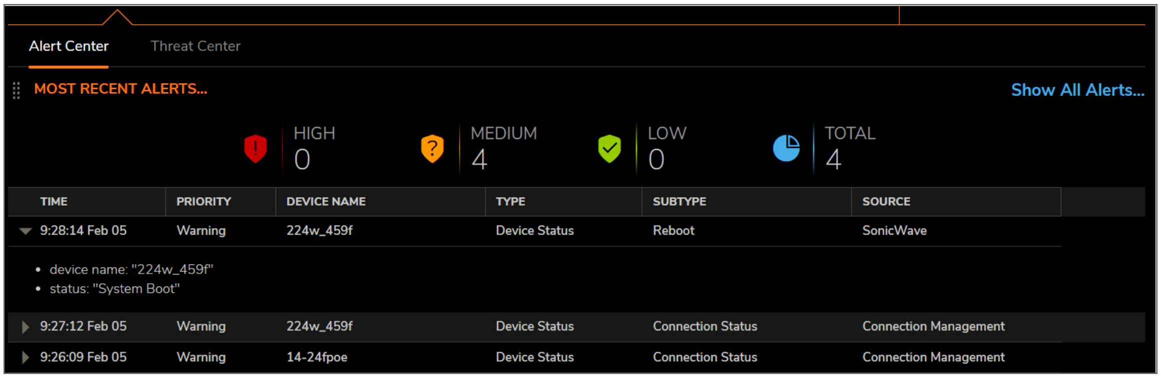
TIME	PRIORITY	DEVICE NAME	TYPE	SUBTYPE	SOURCE
9:28:14 Feb 05	Warning	224w_459f	Device Status	Reboot	SonicWave

If you select the tab **Switches**, the screen displays the statistics for the switches in use - online, off-line, unmanaged, and expired. The options displayed down are **Alert Centre**, **Threat Centre**, **Switches**, **Traffic of Ports**, **PoE of Switches**, and **PoE of Switch Ports.**



More information on these tabs are further explained below.

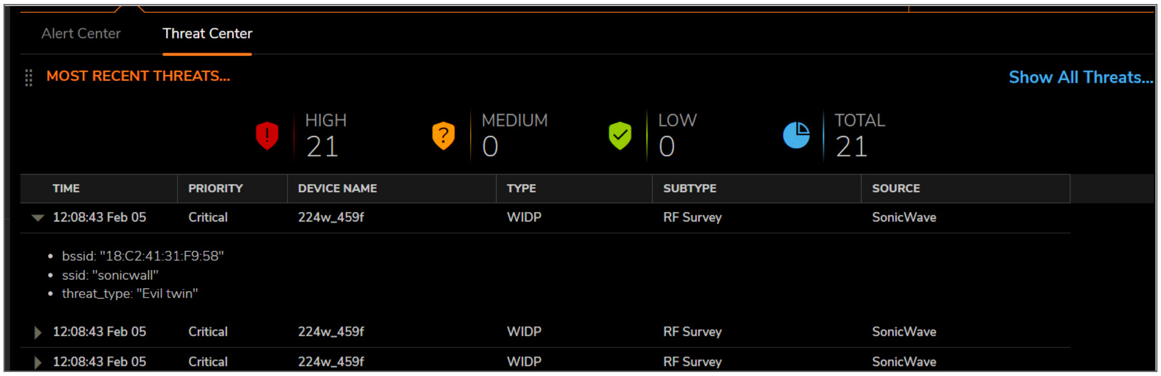
- **Alert Center** is the first of seven bars across the middle of the screen that can be clicked to display the traffic data summaries and visual overviews. When the main screen first comes up, **Alert Center** is active. Clicking the **Alert Center** bar lists the most recent alerts.



TIME	PRIORITY	DEVICE NAME	TYPE	SUBTYPE	SOURCE
9:28:14 Feb 05	Warning	224w_459f	Device Status	Reboot	SonicWave
• device name: "224w_459f" • status: "System Boot"					
9:27:12 Feb 05	Warning	224w_459f	Device Status	Connection Status	Connection Management
9:26:09 Feb 05	Warning	14-24fpoe	Device Status	Connection Status	Connection Management

The columns display **Time**, **Priority**, **Device Name**, **Type** (type of the threat), **Sub Type** (picked up by which type of security policy), and **Source** (the source access point).

- The **Threat Center** bar shows the same screen but with the most recent threats in the bottom panel. The columns display **Time**, **Priority**, **Device Name**, **Type** (type of the threat), **Sub Type** (picked up by which type of security policy), and **Source** (the source access point).

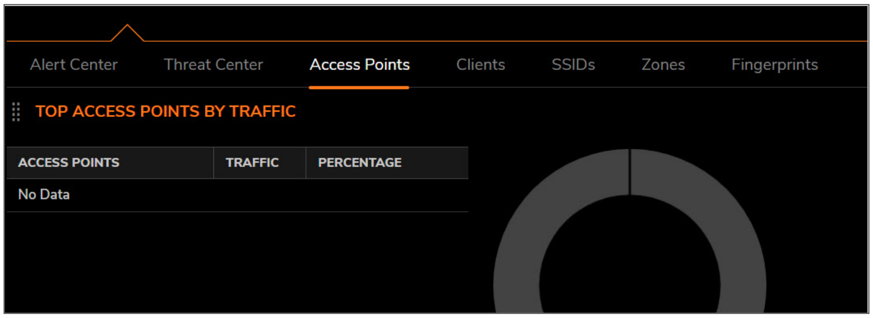


MOST RECENT THREATS...

HIGH 21 | MEDIUM 0 | LOW 0 | TOTAL 21

TIME	PRIORITY	DEVICE NAME	TYPE	SUBTYPE	SOURCE
12:08:43 Feb 05	Critical	224w_459f	WIDP	RF Survey	SonicWave
• bssid: "18:C2:41:31:F9:58" • ssid: "sonicwall" • threat_type: "Evil twin"					
12:08:43 Feb 05	Critical	224w_459f	WIDP	RF Survey	SonicWave
12:08:43 Feb 05	Critical	224w_459f	WIDP	RF Survey	SonicWave

- When the **Access Points** bar is clicked, it lists the top access points by traffic. The top panel still displays the overview of your network and the access point status.



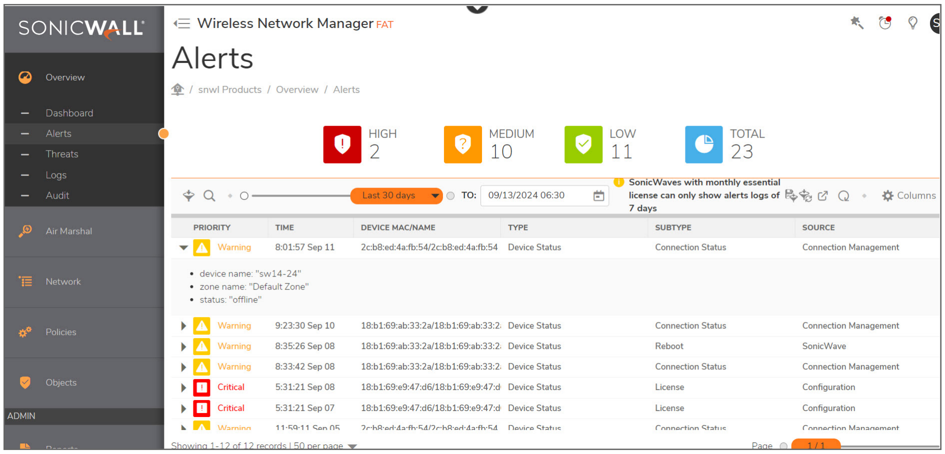
TOP ACCESS POINTS BY TRAFFIC

ACCESS POINTS	TRAFFIC	PERCENTAGE
No Data		

- The **Clients** bar lists the top client devices by traffic.
- The **SSIDs** bar lists the top SSIDs by traffic.
- The **Zones** bar lists the top zones by traffic.
- The **Fingerprints** bar lists the client devices in your hierarchy with the operating system each one is using. In real time, it detects the connection of all client devices to your access points, and monitors their activity to display the top fingerprints by traffic.
- The **Switches** bar lists the traffic utilization percentage on switch interfaces.
- The **Traffic of Ports** bar lists the traffic history of the switch.
- The **PoE of Switches** lists the power draw details.
- The **PoE of Switch Ports** lists the PoE history of switch.

Alerts

Right below **Dashboard** on the navigation pane are the **Alerts**, with detailed information about the alerts detected in your network.



Alerts

/ snwl Products / Overview / Alerts

HIGH 2 | MEDIUM 10 | LOW 11 | TOTAL 23

Last 30 days TO: 09/13/2024 06:30

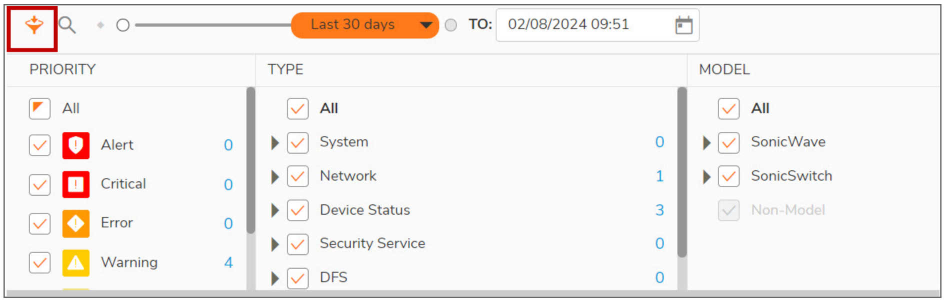
SonicWaves with monthly essential license can only show alerts logs of 7 days

Columns

PRIORITY	TIME	DEVICE MAC/NAME	TYPE	SUBTYPE	SOURCE
Warning	8:01:57 Sep 11	2c:b8:ed:4a:fb:54/2c:b8:ed:4a:fb:54	Device Status	Connection Status	Connection Management
• device name: "sw14-24" • zone name: "Default Zone" • status: "offline"					
Warning	9:23:30 Sep 10	18:b1:69:ab:33:2a/18:b1:69:ab:33:2	Device Status	Connection Status	Connection Management
Warning	8:35:26 Sep 08	18:b1:69:ab:33:2a/18:b1:69:ab:33:2	Device Status	Reboot	SonicWave
Warning	8:33:42 Sep 08	18:b1:69:ab:33:2a/18:b1:69:ab:33:2	Device Status	Connection Status	Connection Management
Critical	5:31:21 Sep 08	18:b1:69:e9:47:d6/18:b1:69:e9:47:d	Device Status	License	Configuration
Critical	5:31:21 Sep 07	18:b1:69:e9:47:d6/18:b1:69:e9:47:d	Device Status	License	Configuration
Warning	11:59:11 Sep 05	2c:b8:ed:4a:fb:54/2c:b8:ed:4a:fb:54	Device Status	Connection Status	Connection Management

Showing 1-12 of 12 records | 50 per page Page 1 / 1

There is a time line that can be set for several different time periods. The first column shows the **Priority**, of each alert and its criticality. You can also filter the alerts based on the **Type** and **Model** as well.



Last 30 days TO: 02/08/2024 09:51

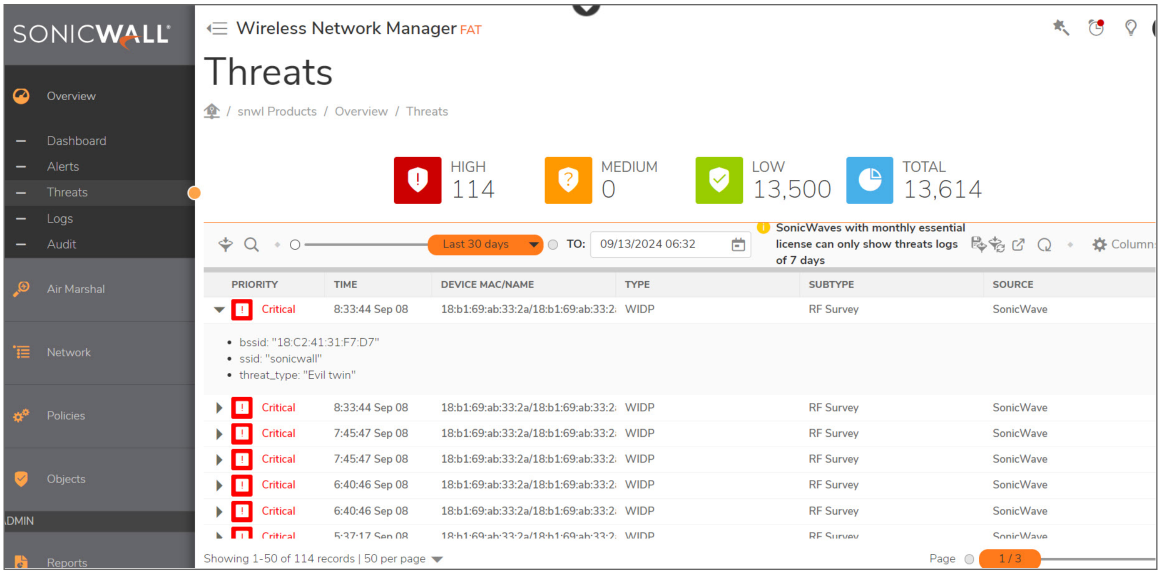
PRIORITY		TYPE		MODEL
☑ All		☑ All		☑ All
☑ Alert	0	☑ System	0	☑ SonicWave
☑ Critical	0	☑ Network	1	☑ SonicSwitch
☑ Error	0	☑ Device Status	3	☑ Non-Model
☑ Warning	4	☑ Security Service	0	
		☑ DFS	0	

ⓘ **NOTE:** For the SonicWave devices with the monthly Essential License, the alerts are displayed only for one week where as, for the devices with Advanced License, the alerts are displayed for one month. For a Switch with the monthly Essential License, the alerts are displayed for one month.

Threats

The **Threats** option brings up a similar screen detailing the threats during the chosen time period.

One of the options in the upper part of the **Threats** page is a check box to activate or deactivate **Wireless Intrusion Detection and Prevention (WIDP)** in the Wireless Network Manager. You can configure this feature on the **Policies > Policy Hierarchy > WIDP** page. (Refer to WIDP for more information). WIDP can detect and prevent attacks from rogue access points in the network.



SonicWaves with monthly essential license can only show threats logs of 7 days

PRIORITY	TIME	DEVICE MAC/NAME	TYPE	SUBTYPE	SOURCE
Critical	8:33:44 Sep 08	18:b1:69:ab:33:2a/18:b1:69:ab:33:2:	WIDP	RF Survey	SonicWave

- bssid: "18:C2:41:31:F7:D7"
- ssid: "sonicwall"
- threat_type: "Evil twin"

PRIORITY	TIME	DEVICE MAC/NAME	TYPE	SUBTYPE	SOURCE
Critical	8:33:44 Sep 08	18:b1:69:ab:33:2a/18:b1:69:ab:33:2:	WIDP	RF Survey	SonicWave
Critical	7:45:47 Sep 08	18:b1:69:ab:33:2a/18:b1:69:ab:33:2:	WIDP	RF Survey	SonicWave
Critical	7:45:47 Sep 08	18:b1:69:ab:33:2a/18:b1:69:ab:33:2:	WIDP	RF Survey	SonicWave
Critical	6:40:46 Sep 08	18:b1:69:ab:33:2a/18:b1:69:ab:33:2:	WIDP	RF Survey	SonicWave
Critical	6:40:46 Sep 08	18:b1:69:ab:33:2a/18:b1:69:ab:33:2:	WIDP	RF Survey	SonicWave
Critical	5:37:17 Sep 08	18:b1:69:ab:33:2a/18:b1:69:ab:33:2:	WIDP	RF Survey	SonicWave

Showing 1-50 of 114 records | 50 per page

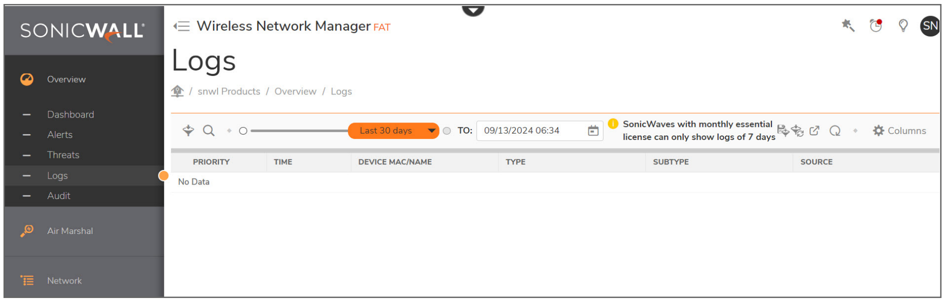
Page 1 / 3

ⓘ **NOTE:** For the SonicWave devices with the monthly Essential License, the threats are displayed only for one week where as, for the devices with Advanced License, the threats are displayed for one month. For a Switch with the monthly Essential License, the threats are displayed for one month.

Logs

Wireless Network Manager has a dedicated event log page. Selecting this option gives an overview of the logs requested for the chosen time period.

ⓘ **NOTE:** For the SonicWave devices with the monthly Essential License, the logs are displayed only for one week where as, for the devices with Advanced License, the logs are displayed for one month. For a Switch with the monthly Essential License, the logs are displayed for one month.



Logs

TO: 09/13/2024 06:34

SonicWaves with monthly essential license can only show logs of 7 days

PRIORITY	TIME	DEVICE MAC/NAME	TYPE	SUBTYPE	SOURCE
No Data					

Click on the filter icon and check the boxes for the **Priority**, **Type** of log collection, or **Model** of the device to enable.

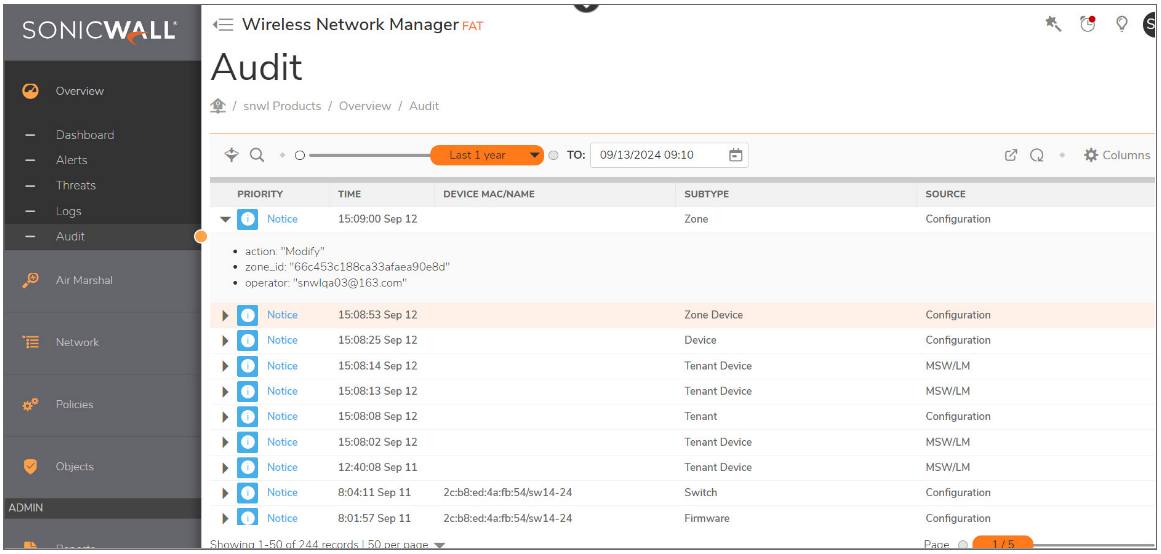
The main options to choose from include:

All	Type	Model
• Error • Warning • Notice	System: • CPU Status • Memory Status • Watchdog • Schedule 802.11: • Association • Disassociation • Mac Filter • Authentication • Deauthentication • Neighbor Report • WNM Sleep • BSS Transition 802.1X: • Authentication • Deauthentication WPA (Wi-Fi Protected Access): • WPA Group Key • WPA Handshake • WPA MIC Failure • EAP (Extensible Authentication Protocol) DFS: • CAC (Channel Available Check). User Authentication: • Guest Authentication. RRM (Radio Resource Management): • Band Steering • Auto Channel • RSSI Threshold • Client Balance Network:	SonicWave • SonicWave 231C • SonicWave 231O • SonicWave 224W • SonicWave 432O • SonicWave 432I • SonicWave432E • SonicWave 681 • SonicWave 641 • SonicWave 621 Sonic Switch • SWS12-8 • SWS12-8FPOE • SWS 12-10FPOE • SWS14-24 • SWS14-24FPOE • SWS14-48 • SWS14-48FPOE •

All	Type	Model
	• SSL VPN • 3G/4G/LTE Modem • Firewall BLE (Bluetooth Low Energy): • System Status • Command Status BLE is configured on the **Policy** > **Policy Hierarchy** page. Mesh: • Mesh Peer Status • Mesh Interface • Mesh Role Cloud Management: • Cloud Command Switch: • CLI • CFA • SNTP • FM • VLAN • AST • LBD • POE • System	

Audit

Wireless Network Manager has an **Audit** page. The administrator can view the audit logs for the last one year and filter by time period and different types of audit logs.



Audit

/ snwl Products / Overview / Audit

TO: 09/13/2024 09:10

PRIORITY	TIME	DEVICE MAC/NAME	SUBTYPE	SOURCE
Notice	15:09:00 Sep 12		Zone	Configuration

- action: "Modify"
- zone_id: "66c453c188ca33afaea90e8d"
- operator: "snwlqa03@163.com"

PRIORITY	TIME	DEVICE MAC/NAME	SUBTYPE	SOURCE
Notice	15:08:53 Sep 12		Zone Device	Configuration
Notice	15:08:25 Sep 12		Device	Configuration
Notice	15:08:14 Sep 12		Tenant Device	MSW/LM
Notice	15:08:13 Sep 12		Tenant Device	MSW/LM
Notice	15:08:08 Sep 12		Tenant	Configuration
Notice	15:08:02 Sep 12		Tenant Device	MSW/LM
Notice	12:40:08 Sep 11		Tenant Device	MSW/LM
Notice	8:04:11 Sep 11	2c:b8:ed:4a:fb:54/sw14-24	Switch	Configuration
Notice	8:01:57 Sep 11	2c:b8:ed:4a:fb:54/sw14-24	Firmware	Configuration

Showing 1-50 of 244 records | 50 per page

Page 1 / 5

Click on the filter icon to select further audit options.

Click on ↗ to export the information to an Excel.

There are the options to refresh the page and select the columns.

3

Using Air Marshal

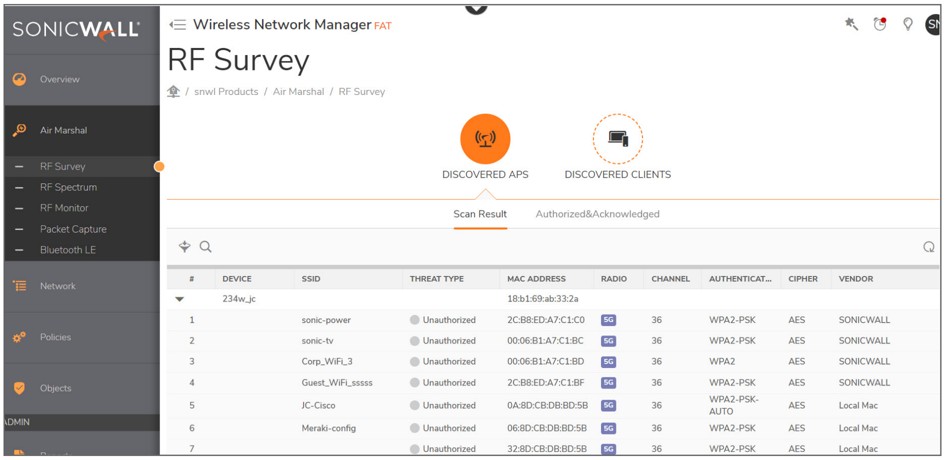
Use Air Marshal to monitor and configure radio frequency (RF) selections in the Wireless Network Manager hierarchy.

Topics:

- RF Survey
- RF Spectrum
- RF Monitor
- Packet Capture
- Bluetooth LE

RF Survey

The **RF Survey** pages provide general information and configuration options related to the radio frequencies of the access points.



#	DEVICE	SSID	THREAT TYPE	MAC ADDRESS	RADIO	CHANNEL	AUTHENTICAT...	CIPHER	VENDOR
	234w_jc			18:b1:69:ab:33:2a					
1		sonic-power	Unauthorized	2C:B8:ED:A7:C1:C0	5G	36	WPA2-PSK	AES	SONICWALL
2		sonic-tv	Unauthorized	00:06:B1:A7:C1:BC	5G	36	WPA2-PSK	AES	SONICWALL
3		Corp_WiFi_3	Unauthorized	00:06:B1:A7:C1:BD	5G	36	WPA2	AES	SONICWALL
4		Guest_WiFi_sssss	Unauthorized	2C:B8:ED:A7:C1:BF	5G	36	WPA2-PSK	AES	SONICWALL
5		JC-Cisco	Unauthorized	0A:8D:CB:DB:BD:5B	5G	36	WPA2-PSK-AUTO	AES	Local Mac
6		Meraki-config	Unauthorized	06:8D:CB:DB:BD:5B	5G	36	WPA2-PSK	AES	Local Mac
7			Unauthorized	32:8D:CB:DB:BD:5B	5G	36	WPA2-PSK	AES	Local Mac

- Choosing **RF Survey** gives a visual overview of the system’s environment.
- The bottom panel displays a row with information for each online device.

- Clicking the arrow at the left end of the row expands or collapses the section to show more SSID information.

Discovered Aps

You can manually authorize, unauthorize, and acknowledge the access points using the **Discovered APS** > **Scan Result** tab. Wireless Network Manager will consider the acknowledged APs as legitimate.

> ⓘ **NOTE:** To view **RF Survey** and authorize an access point, navigate to **AP Policy** > **Default Policy** > **Configuration** icon. On the **Configuration** page, click on the **WIDP** tab and the **RF Monitor** is enabled by default.

To authorize an access point:

1. Navigate to the **Air Marshal > RF Survey** page.
2. Click **Discovered APs**.
3. **Scan Result** is displayed by default, to view the list of detected access points.
4. On the right of the access point for which you want to authorize, click the **Authorize** icon .
5. In the **Threat Type** column, the access point now displays as **Authorized**.

To unauthorize an access point:

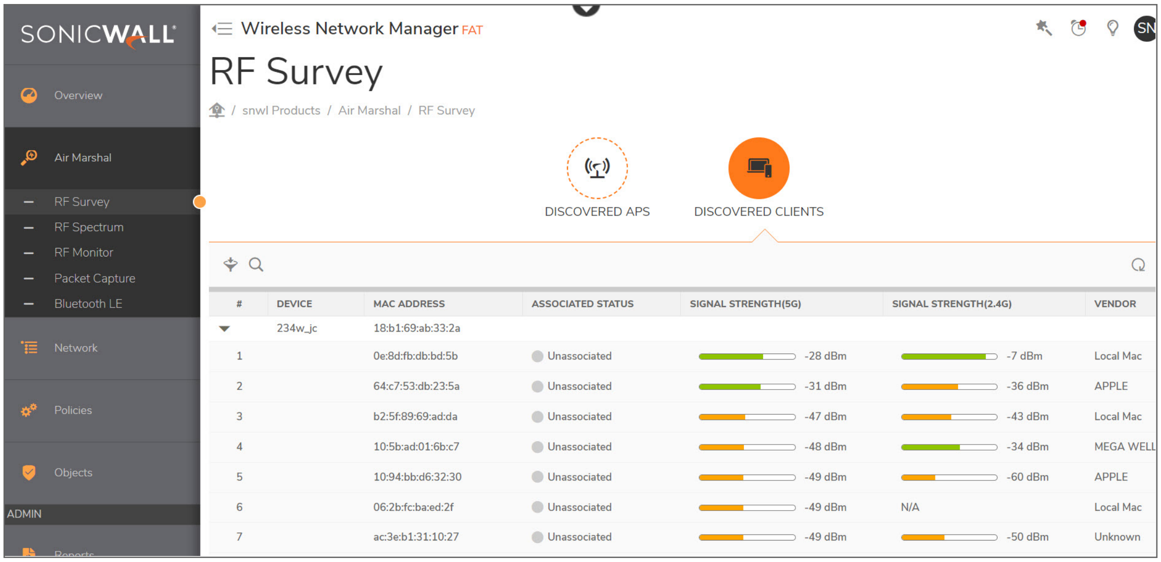
1. Navigate to the **Air Marshal > RF Survey** page.
2. Click **Discovered APs**.
3. Click on the **Authorized&Acknowledged** tab to view the list of authorized access points.
4. On the right of the access point for which you want to unauthorize, click the **Delete** icon.
5. In the **Scan Result** table, in the **Threat Type** column, the access point now displays as **Unauthorized**.

Other than this, you also have the option to acknowledge the access points by clicking ✓.

The **Authorized&Acknowledged** tab also helps to delete the access points by clicking the 🗑.

Discover and Report Unassociated Wireless Clients

Although some wireless clients may not be associated with a specific access point, they will still send occasional probe requests. The access points can collect the information about these clients and trace their locations. The information will be displayed on the **Air Marshal > RF Survey > Discovered Clients** page.



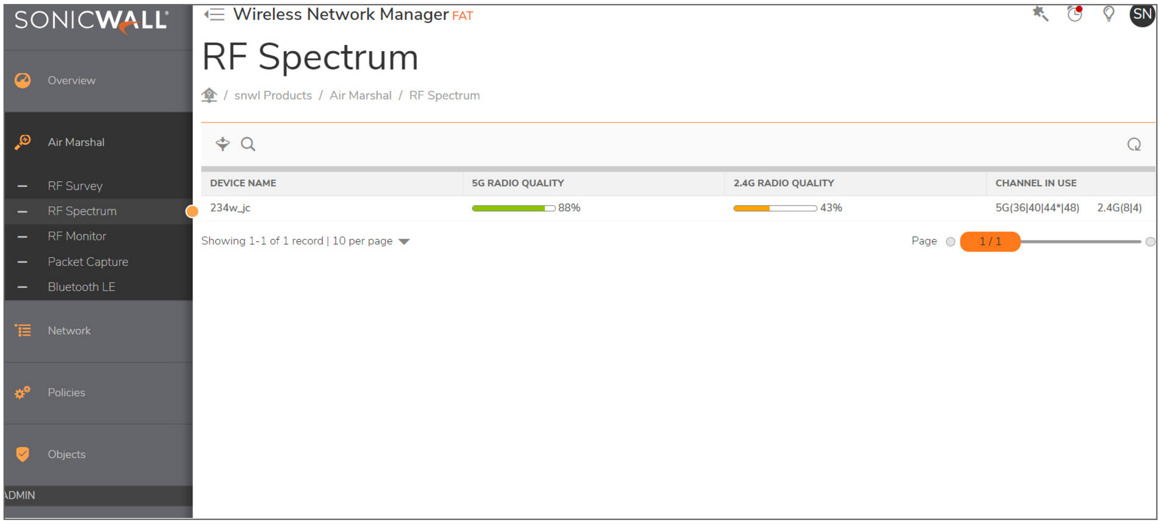
RF Survey

/ snwl Products / Air Marshal / RF Survey

#	DEVICE	MAC ADDRESS	ASSOCIATED STATUS	SIGNAL STRENGTH(5G)	SIGNAL STRENGTH(2.4G)	VENDOR
	234w_jc	18:b1:69:ab:33:2a				
1		0e:8d:fb:db:bd:5b	Unassociated	-28 dBm	-7 dBm	Local Mac
2		64:c7:53:db:23:5a	Unassociated	-31 dBm	-36 dBm	APPLE
3		b2:5f:89:69:ad:da	Unassociated	-47 dBm	-43 dBm	Local Mac
4		10:5b:ad:01:6b:c7	Unassociated	-48 dBm	-34 dBm	MEGA WELL
5		10:94:bb:d6:32:30	Unassociated	-49 dBm	-60 dBm	APPLE
6		06:2b:fc:ba:ed:2f	Unassociated	-49 dBm	N/A	Local Mac
7		ac:3e:b1:31:10:27	Unassociated	-49 dBm	-50 dBm	Unknown

RF Spectrum

The **RF Spectrum** page lists the access points in your hierarchy, with the details of the Radio Quality on each of the bands it is on.



RF Spectrum

/ snwl Products / Air Marshal / RF Spectrum

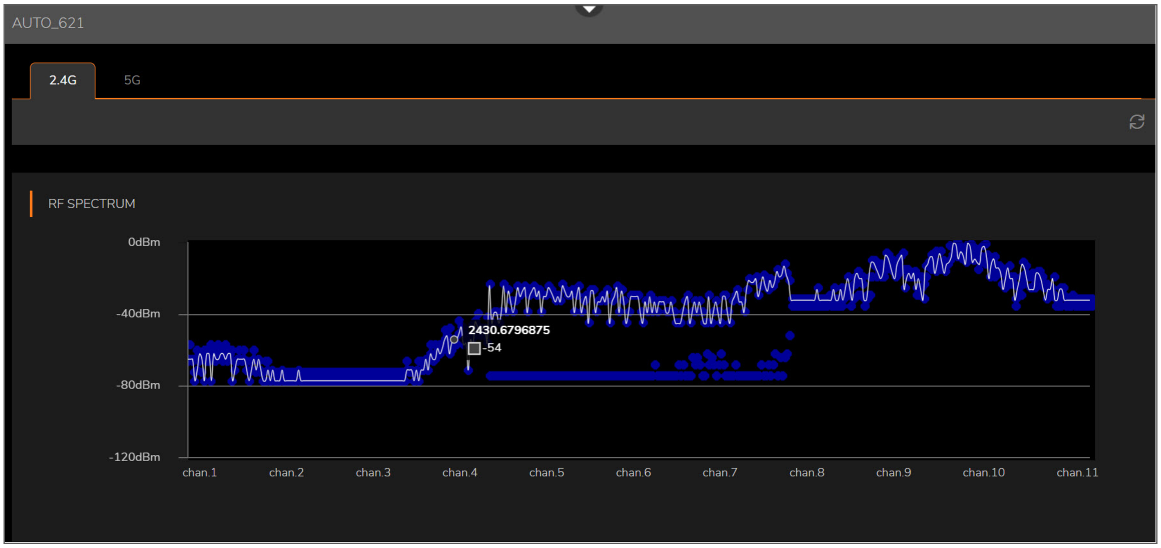
DEVICE NAME	5G RADIO QUALITY	2.4G RADIO QUALITY	CHANNEL IN USE
234w_jc	88%	43%	5G(36|40|44*|48) 2.4G(8|4)

Showing 1-1 of 1 record | 10 per page

Page 1 / 1

The **RF Spectrum** page displays the RF Spectrum and the Channel Utilization of the device. If the device is on two bands, click the band number in the upper left corner to show that band information. Hovering over parts of the charts gives readouts and averages.

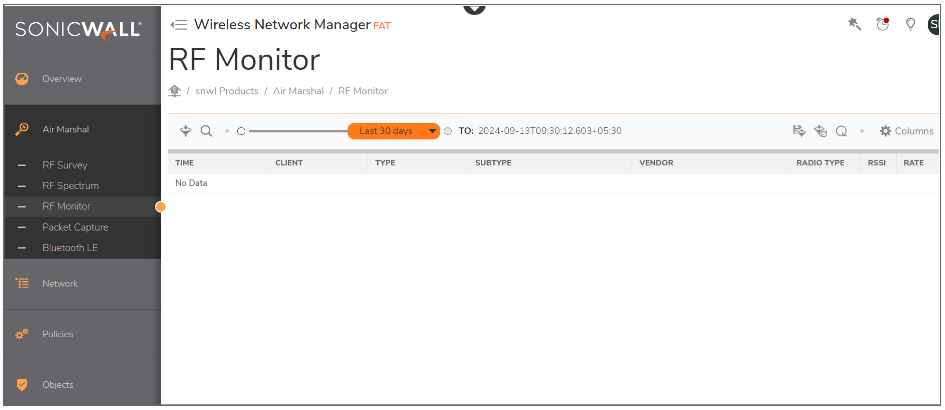
Clicking on the right end of the row brings up details of the RF Spectrum, if it is supported on that device.



RF Monitor

The SonicOS RF Monitoring provides real-time threat monitoring and management of SonicPoint radio frequency traffic. SonicOS RF monitoring also provides a system for the centralized collection of RF threats and traffic statistics that offer a way to easily manage RF capabilities directly from the SonicWall security appliance gateway.

The **RF Monitoring** page provides a central location for selecting RF signature types, viewing discovered RF threat stations, and adding discovered threat stations to a watch list.



RF Monitor

/ snwl Products / Air Marshal / RF Monitor

TO: 2024-09-13T09:30:12.603+05:30

TIME	CLIENT	TYPE	SUBTYPE	VENDOR	RADIO TYPE	RSSI	RATE
No Data							

ⓘ | **NOTE: RF Monitor** is disabled by default.

To activate RF Monitor:

1. Navigate to **Policies > AP Policies**.
2. Select the AP policy for which you want to enable RF monitoring.

3. Navigate to **Policies > Policy Hierarchy > WIDP**.
4. Activate **RF Monitoring**.
5. Change the duration of the **Measurement Interval (Seconds)** if you want it to be different from the default value.
6. Click **OK**.

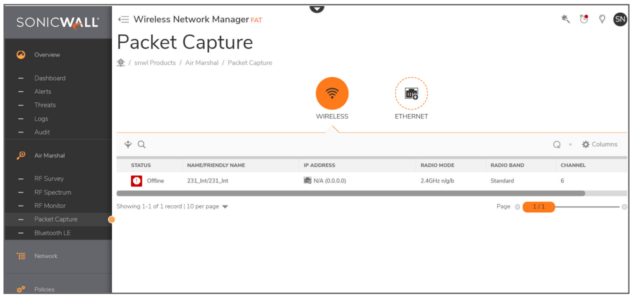
Packet Capture

Packet Capture is a debugging tool that allows the capturing of wireless and wired packets. Packet Capture utilizes the .pcap file format for display and analysis by the popular tools such as Wireshark.

The Packet Capture feature provides a live snapshot of traffic on the network, that can be immensely helpful in diagnosing and troubleshooting network issues. This feature provides an in-depth type of troubleshooting that users can use to gather packet data from a client site and get the output into a readable file.

This feature is supported for SonicWave access points. Users will be able to configure the capture settings for each SonicWave, show the status of the SonicWave, the number of packets captured, and the size of the packet buffer. Users will also be able to download the captured packets file for each SonicWave.

Click **Airmarshal** > **Packet Capture** to navigate to this page.



STATUS	NAME/FRIENDLY NAME	IP ADDRESS	RADIO MODE	RADIO BAND	CHANNEL
Offline	231_Int/231_Int	N/A (0.0.0.0)	2.4GHz n/g/b	Standard	6

Showing 1-1 of 1 record | 10 per page

Page 1 / 1

Packet Capture page feature provides two options:

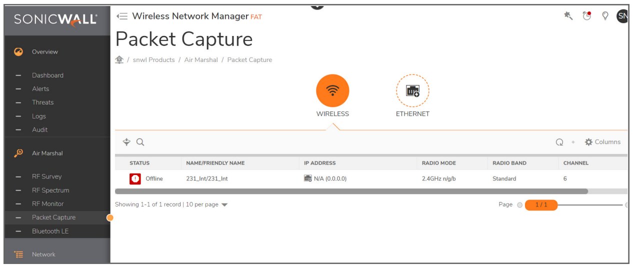
- Wireless
- Ethernet

Wireless

When you click **Airmarshal** > **Packet Capture** the **Wireless** tab is displayed by default, as shown in the previous screen.

This page displays a list of all available SonicWaves(APs), and each row on this list shows the basic information and status of a SonicWave device.

Click on the unfold arrow button to view the details of this device's wireless data capture settings. The information such as Wireless Packet Capture Radio Settings and Wireless Packet Capture Buffer Statics are displayed



Packet Capture

/ snwl Products / Air Marshal / Packet Capture

STATUS	NAME/FRIENDLY NAME	IP ADDRESS	RADIO MODE	RADIO BAND	CHANNEL
Offline	231_Int/231_Int	N/A (0.0.0.0)	2.4GHz n/g/b	Standard	6

Showing 1-1 of 1 record | 10 per page

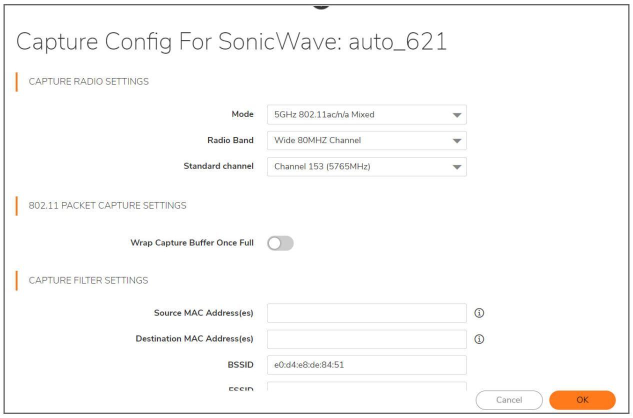
Page 1 / 1

You can also do the options described below:

- Click on the configure icon to open the wireless data capture settings page for that SonicWave. More information of configuration is explained further below.
- Click on the download icon to download the already captured packets.
- Click on the clear buffer icon to clear the captured packets buffer.
- Click **Start Capture** to start the capture. You can see the buffer statistics as **Trace Active**.
- Click on **Stop Capture** to finish the capture. You can see the buffer statistics as **Trace Off**.

To Configure the Wireless Packet Capture:

1. Click on the configure icon hovering the mouse to the right hand side of the device. The wireless data capture settings page is displayed.



Capture Config For SonicWave: auto_621

CAPTURE RADIO SETTINGS

Mode: 5GHz 802.11ac/n/a Mixed

Radio Band: Wide 80MHZ Channel

Standard channel: Channel 153 (5765MHz)

802.11 PACKET CAPTURE SETTINGS

Wrap Capture Buffer Once Full

CAPTURE FILTER SETTINGS

Source MAC Address(es)

Destination MAC Address(es)

BSSID: e0:d4:e8:de:84:51

ESSID

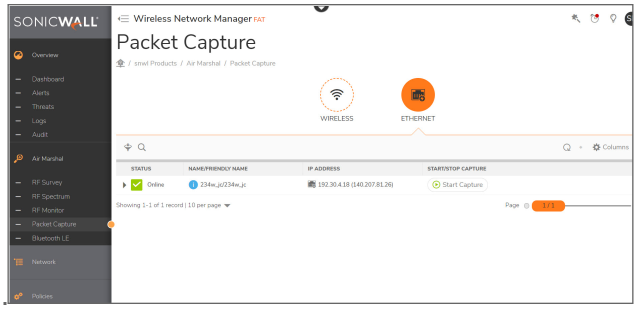
2. Specify the **Capture Radio Settings** options:
   - **Mode** - The options are 2.4GHz 802.11n/g/b Mixed, 5GHz 802.11n/a Mixed, and 5GHz 802.11ac/n/a Mixed.
   - **Radio Band** - The options are Standard 20MHZ Channel, Wide 40MHZ Channel, and Wide 80MHZ Channel.
   - **Standard Channel** - Choose a frequency channel as per your requirement.
3. Specify the **802.11 Packet Capture Settings** option. You can either enable or disable the **Wrap Capture Buffer Once Full** option.
4. Specify the Capture Filter Settings options:

- **Source MAC Address**
- **Destination MAC Address**
- Basic Service Set Identifier (**BSSID**)
- Extended Service Set Identifier (**ESSID**)
- Toggle the option on or off for **Enable Bidirectional Address Matching**
- Toggle the option on or off for **Exclude Beacon**
- Toggle the option on or off for **Exclude Probe Request**
- Toggle the option on or off for **Exclude Probe Response**
- Toggle the option on or off for **Exclude Control**
- Toggle the option on or off for **Exclude Data**

5. Click **OK** to save the changes.

Ethernet

Click **Airmarshal** > **Packet Capture** > **Ethernet** tab to view and edit the Packet Capture settings for ethernet data.



Packet Capture

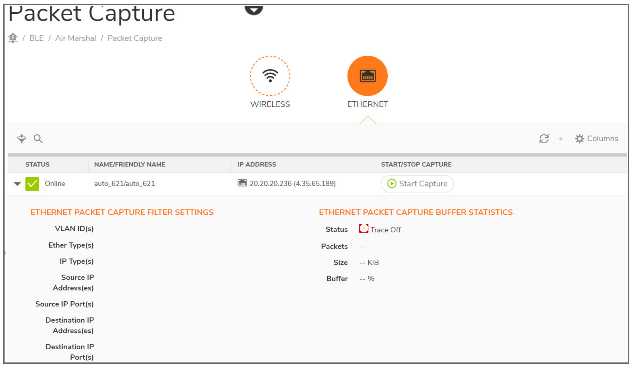
/ snwl Products / Air Marshal / Packet Capture

STATUS	NAME/FRIENDLY NAME	IP ADDRESS	START/STOP CAPTURE
Online	234w_jc/234w_jc	192.30.4.18 (140.207.81.26)	Start Capture

Showing 1-1 of 1 record | 10 per page

Page 1 / 1

Click on the unfold arrow button to view the details of this device's ethernet data capture settings. The information such as Ethernet Packet Capture Filter Settings and Ethernet Packet Capture Buffer Statics are displayed.



Packet Capture

/ BLE / Air Marshal / Packet Capture

STATUS	NAME/FRIENDLY NAME	IP ADDRESS	START/STOP CAPTURE
Online	auto_621/auto_621	20.20.20.236 (4.35.65.189)	Start Capture

ETHERNET PACKET CAPTURE FILTER SETTINGS

VLAN ID(s)
Ether Type(s)
IP Type(s)
Source IP Address(es)
Source IP Port(s)
Destination IP Address(es)
Destination IP Port(s)

ETHERNET PACKET CAPTURE BUFFER STATISTICS

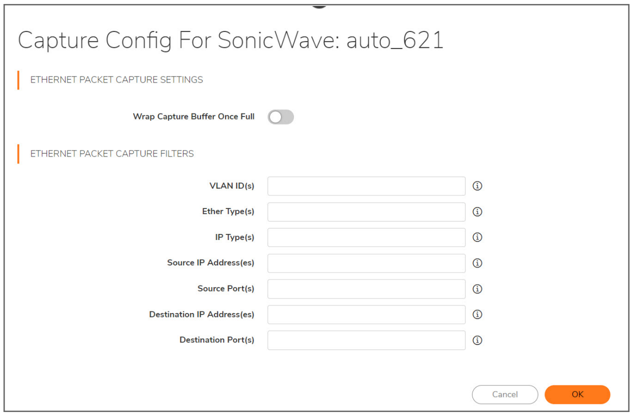
Status	Trace Off
Packets	--
Size	-- KiB
Buffer	-- %

You can also do the options described below:

- Click on the configure icon to open the ethernet data capture settings page for that SonicWave. More information of configuration is explained further below.
- Click on the download icon to download the already captured packets.
- Click on the clear buffer icon to clear the captured packets buffer.
- Click **Start Capture** to start the capture. You can see the buffer statistics as **Trace Active**.
- Click on **Stop Capture** to finish the capture. You can see the buffer statistics as **Trace Off**.

To Configure the Ethernet Packet Capture:

1. Click on the configure icon hovering the mouse to the right hand side of the device. The ethernet data capture settings page is displayed.



Capture Config For SonicWave: auto_621

ETHERNET PACKET CAPTURE SETTINGS

Wrap Capture Buffer Once Full ○

ETHERNET PACKET CAPTURE FILTERS

VLAN ID(s)

Ether Type(s)

IP Type(s)

Source IP Address(es)

Source Port(s)

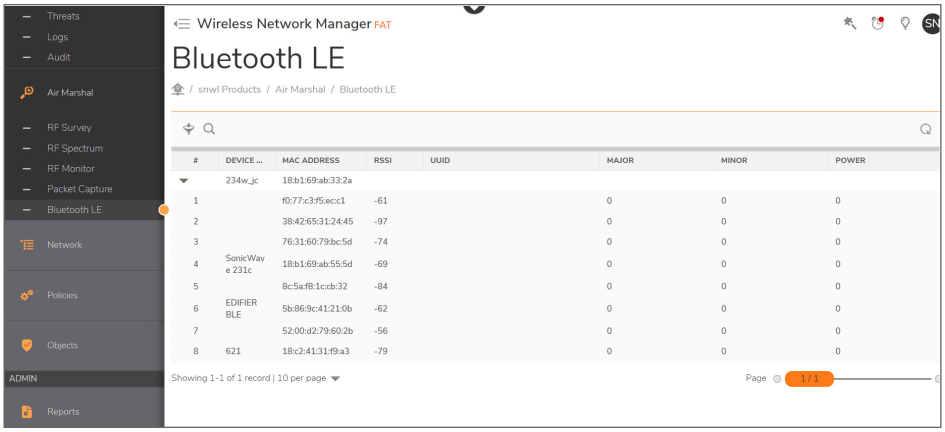
Destination IP Address(es)

Destination Port(s)

2. Specify the **Ethernet Packet Capture Settings** option. You can either enable or disable the **Wrap Capture Buffer Once Full** option.
3. Specify the **Ethernet Packet Capture Filters**. For each of these fields you can specify a maximum of 10 types separated by commas. Negative values are accepted. All values should be of the same type- either positive or negative.
    - **VLAN IDs**
    - **Ether Types**
    - **IP Types**
    - **Source IP Addresses**
    - **Source Ports**
    - **Destination IP Addresses**
    - **Destination Ports**
4. Click **OK** to save the changes.

Bluetooth LE

The **Bluetooth LE** page displays information about Bluetooth Low Energy (BLE) scan for each device.



Bluetooth LE

snwl Products / Air Marshal / Bluetooth LE

#	DEVICE ...	MAC ADDRESS	RSSI	UUID	MAJOR	MINOR	POWER
▼	234w_jc	18:b1:69:ab:33:2a					
1		f0:77:c3:f5:ec:c1	-61		0	0	0
2		38:42:65:31:24:45	-97		0	0	0
3		76:31:60:79:bc:5d	-74		0	0	0
4	SonicWave 231c	18:b1:69:ab:55:5d	-69		0	0	0
5		8c:5a:f8:1c:cb:32	-84		0	0	0
6	EDIFIER BLE	5b:86:9c:41:21:0b	-62		0	0	0
7		52:00:d2:79:60:2b	-56		0	0	0
8	621	18:c2:41:31:f9:a3	-79		0	0	0

Showing 1-1 of 1 record | 10 per page

Page 1 / 1

BLE is available for transferring small amounts of data between nearby devices. The screen gives information about all the devices, or only those that are online.

For each device, it displays:

- Device name
- MAC Address
- RSSI
- UUID
- Power Information.

ⓘ | **NOTE:** BLE Scan reporting is only supported on SonicWave 224w models.

4

Managing Your Network

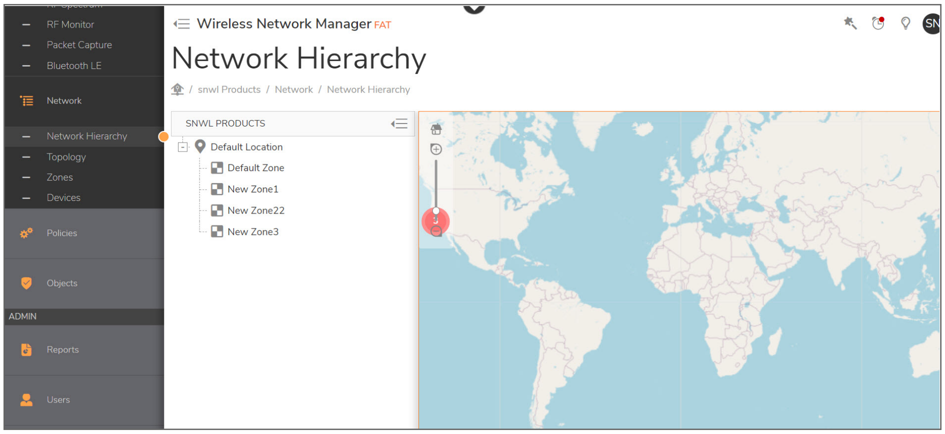
The **Network** page helps you configure your network.

Topics:

- Network Hierarchy
- Network Topology
- Zones
- Devices

Network Hierarchy

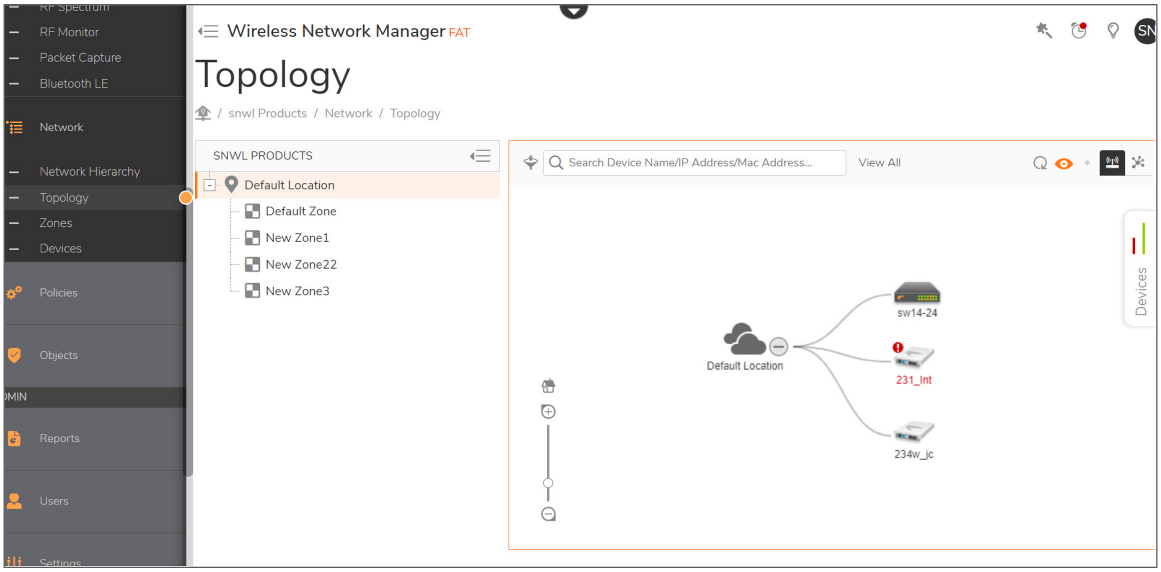
After you have configured your network hierarchy, use the **Network Hierarchy** page to add, delete, edit, and copy locations, edit and delete zones, and manage zone policies in your tenant hierarchy.



For more information on setting up your hierarchy in Wireless Network Manager, refer to the *Wireless Network Manager Getting Started Guide*. This and other documentation are available under the product name “Secure Cloud Wireless” on the SonicWall support website at: https://www.sonicwall.com/support/technical-documentation/.

Network Topology

After you have configured your network hierarchy, use the **Network Topology** page view the logical arrangements of nodes and connections in the network.



You can also view the information including Device Name, Status, Location, Zone, IP Address, and MAC Address.

Zones

The **Zones** page displays Information about all the zones you have created. You can configure your zones using this page.

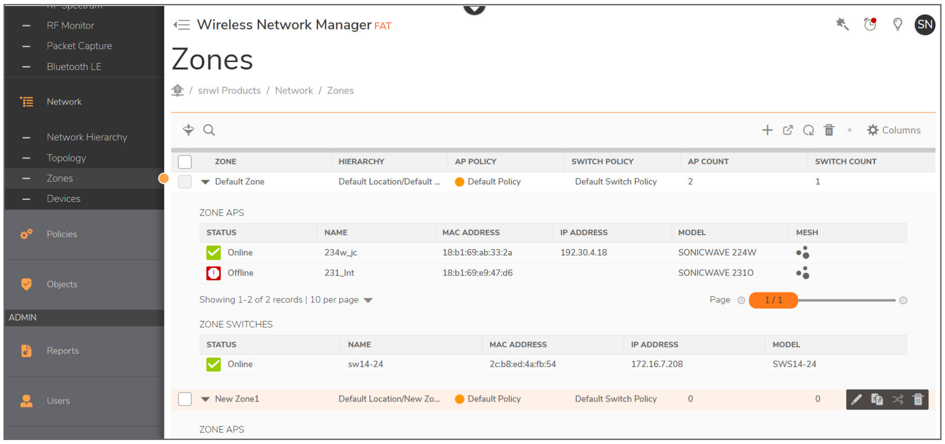
Zones are used to define the devices.

For example:

Zone 1: AP1+AP2+ Switch1 , Use AP-Policy-1, Switch Policy-1

Zone 2: AP3+Switch2+Switch3, Uses AP-Policy-2, Switch Policy-2

To create a Zone, you have to select the Location/AP/Switch Policy. You can add a device while creating a zone or later whenever you want the device to use this Zone Policy.



Zones

/ snwl Products / Network / Zones

	ZONE	HIERARCHY	AP POLICY	SWITCH POLICY	AP COUNT	SWITCH COUNT
□	Default Zone	Default Location/Default ...	● Default Policy	Default Switch Policy	2	1

ZONE APS

STATUS	NAME	MAC ADDRESS	IP ADDRESS	MODEL	MESH
✓ Online	234w_jc	18:b1:69:ab:33:2a	192.30.4.18	SONICWAVE 224W	
! Offline	231_Int	18:b1:69:e9:47:d6		SONICWAVE 231O	

Showing 1-2 of 2 records | 10 per page

Page 1 / 1

ZONE SWITCHES

STATUS	NAME	MAC ADDRESS	IP ADDRESS	MODEL
✓ Online	sw14-24	2c:b8:ed:4a:fb:54	172.16.7.208	SWS14-24

	ZONE	HIERARCHY	AP POLICY	SWITCH POLICY	AP COUNT	SWITCH COUNT
□	New Zone1	Default Location/New Zo...	● Default Policy	Default Switch Policy	0	0

ZONE APS

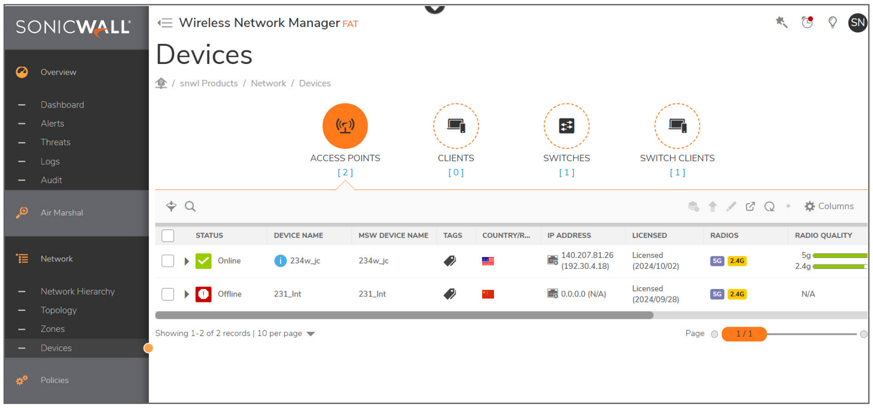
Icon	Definition
＋	Click this icon to add a new zones.
↗	Click this icon to export data into an Excel or PDF file.
⟳	Click this icon to refresh or reload the page.
🗑	Click this icon to delete the selected options.
⚙	Click this icon to select the grid settings or the required columns. This helps you to view or hide the selected columns and customize the data with the desired fields.

- Select a Zone on the bottom panel to see its place in the:
  - Zone name
  - Hierarchy
  - AP Policy
  - Switch Policy
  - Access Point (AP) Count
  - Switch Count
- To add a zone, click on the **+ Add Zone** on the top right of the page.
- To **Edit**, **Copy**, **Transfer Devices**, or **Delete** a zone, hover over the options on the right end of the row.
- The **Transfer Devices** option makes it possible to move a device from one zone to another in one step.
- By expanding the **Zone** row, you get more information about each of the Zone APs and Switches. This includes its:
  - Status (online or not)
  - Name
  - MAC Address
  - IP Addresses

- Model
- Mesh Group (if it is part of one)

Devices

The **Devices** page provides options for different types of devices. When you click on Network > Devices, the Access Points tab is displayed by default.



STATUS	DEVICE NAME	MSW DEVICE NAME	TAGS	COUNTRY/R...	IP ADDRESS	LICENSED	RADIOS	RADIO QUALITY
Online	234w_jc	234w_jc			140.207.81.26 (192.30.4.18)	Licensed (2024/10/02)	5G 2.4G	5g 2.4g
Offline	231_Int	231_Int			0.0.0.0 (N/A)	Licensed (2024/09/28)	5G 2.4G	N/A

Showing 1-2 of 2 records | 10 per page

Page 1 / 1

The **Devices** page provides the option to add devices to a zone and upgrade the selected devices, when required. You can add a single managed device or a group of unmanaged devices to a zone.

Topics:

- Managing Access Points
- Managing the Configuration of Access Points
- Upgrading the Firmware for Specific Access Points
- Viewing the Wireless Client Journey
- Viewing the Wireless Client Journey
- Managing Switch Clients
- Using Tags to Manage Access Points and SSIDs

Managing Access Points

Access Point Devices are part of your Network Hierarchy host the **Client Devices** (the phones and computers that communicate through them).

Access Points provides configuration and management information about access points. When you initially log on to Wireless Network Manager, all the SonicWave access points registered under your MySonicWall account are listed as inventory on this screen.

There is a filter icon on the left which lets you choose the devices to be displayed.

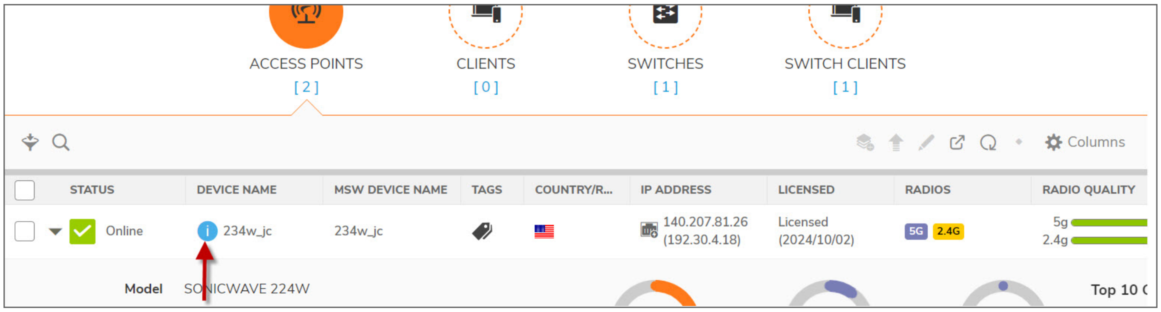
The middle panel shows the **Network** structure with the **Status** summary of each of the access points:

- With the AP managed, you will have options as **Online, Offline,** and **Unmanaged.**
- **License** information
- **Model** information

The **SSL-VPN** column in the bottom chart shows a colored **S** to show whether **SSL VPN** is enabled or not for that device. If the **S** is:

- Green - The SSL VPN is connected.
- Red - The SSL VPN is disconnected.
- Gray - The SSL VPN is disabled.

If your firmware needs upgrading, a blue icon is diplayed on left of the AP name. Hover over the hover the icon and it shows as **New product firmware available**.



□	STATUS	DEVICE NAME	MSW DEVICE NAME	TAGS	COUNTRY/R...	IP ADDRESS	LICENSED	RADIOS	RADIO QUALITY
□	✓ Online	234w_jc	234w_jc			140.207.81.26 (192.30.4.18)	Licensed (2024/10/02)	5G 2.4G	5g 2.4g

Model SONICWAVE 224W

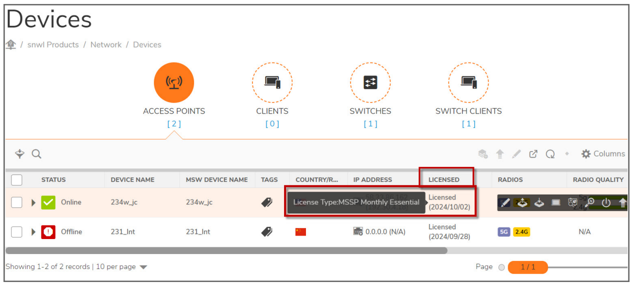
Top 10 (

By hovering over the **Licensed** column, you can view the **License Type** of each device.

The different types of licenses include:

- Annual License
    - Basic
    - Advanced
    - CATP Only
    - CAV Only
    - CFS Only
- Monthly License
    - AP - Essentail/Advanced
    - Switch- Essential

The License Type does not depend on the renewal date.



Devices

/ snwl Products / Network / Devices

☐	STATUS	DEVICE NAME	MSW DEVICE NAME	TAGS	COUNTRY/R...	IP ADDRESS	LICENSED	RADIOS	RADIO QUALITY
☐	✓ Online	234w_jc	234w_jc		License Type:MSSP Monthly Essential		Licensed (2024/10/02)		
☐	! Offline	231_Int	231_Int			0.0.0.0 (N/A)	Licensed (2024/09/28)	5G 2.4G	N/A

Showing 1-2 of 2 records | 10 per page

Page 1 / 1

The Configuration options for each access point in your network are made available by hovering along the right of the screen. For more information refer to Managing the Configuration of Access Points

Topics:

- Managing the Configuration of Access Points
- Upgrading the Firmware for Specific Access Points
- SonicWave Diagnostics

Managing the Configuration of Access Points

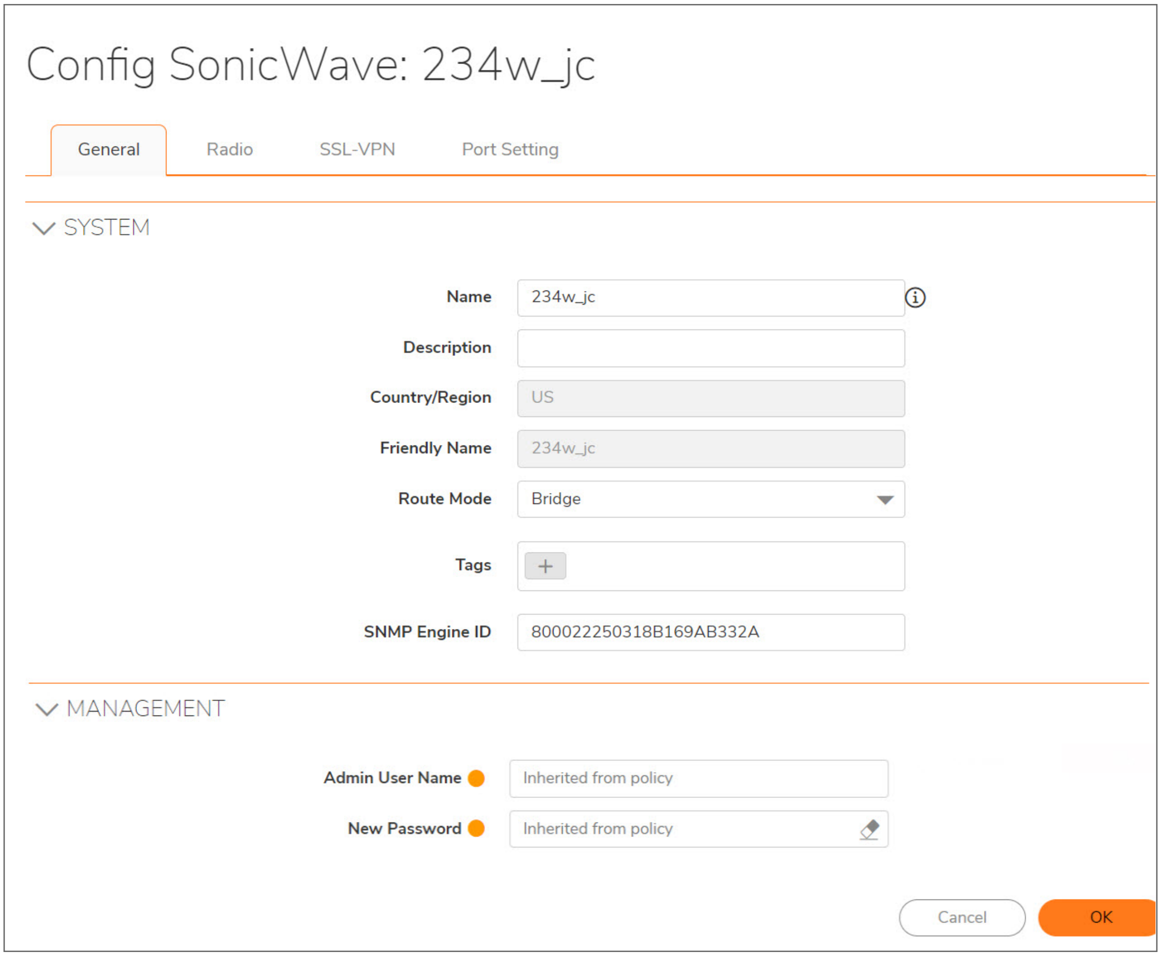
The Configuration options for each access point in your network are made available by hovering along the right of the screen.

Topics:

- General
- Radio
- SSL VPN
- Port Settings

General

Click on **Config/Edit** on the right of the SonicWave row to display the **Configuration** screen. The **General** tab is displayed by default.



Config SonicWave: 234w_jc

SYSTEM

Name: 234w_jc

Description:

Country/Region: US

Friendly Name: 234w_jc

Route Mode: Bridge

Tags: +

SNMP Engine ID: 800022250318B169AB332A

MANAGEMENT

Admin User Name ●: Inherited from policy

New Password ●: Inherited from policy

You can configure the access point to use any of these **Route Modes**:

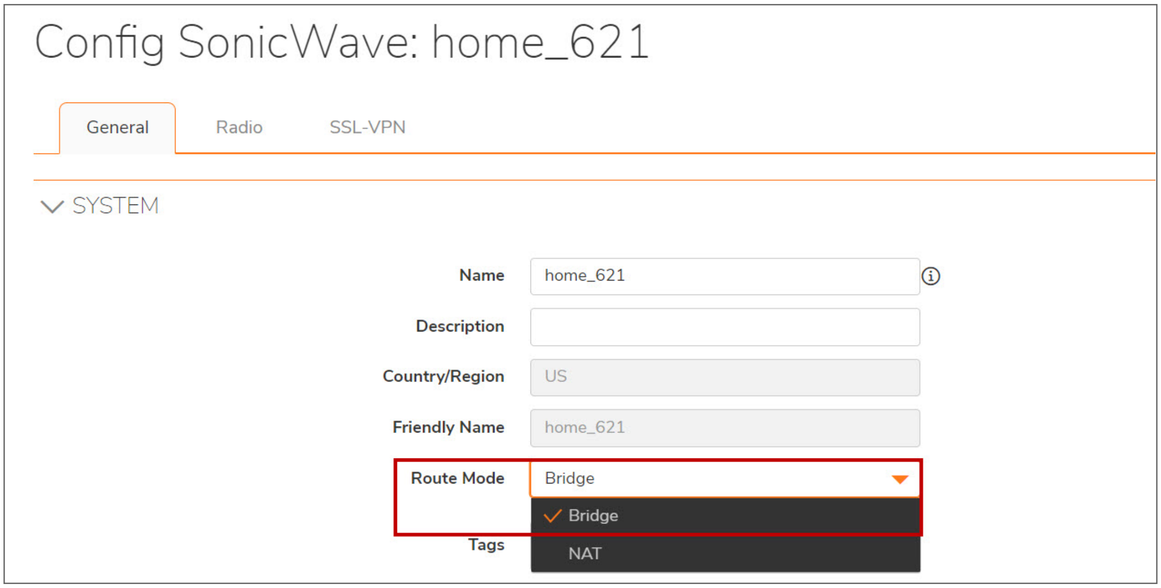
- Bridge Mode
- NAT Mode

Bridge Mode

You can set the SonicWave mode to Bridge mode.

To change the SonicWave mode to Bridge mode:

1. Click **General**.
2. Select **Bridge** from the **Route Mode** drop-down list.



Config SonicWave: home_621

Name: home_621

Description:

Country/Region: US

Friendly Name: home_621

Route Mode: Bridge

NAT Mode

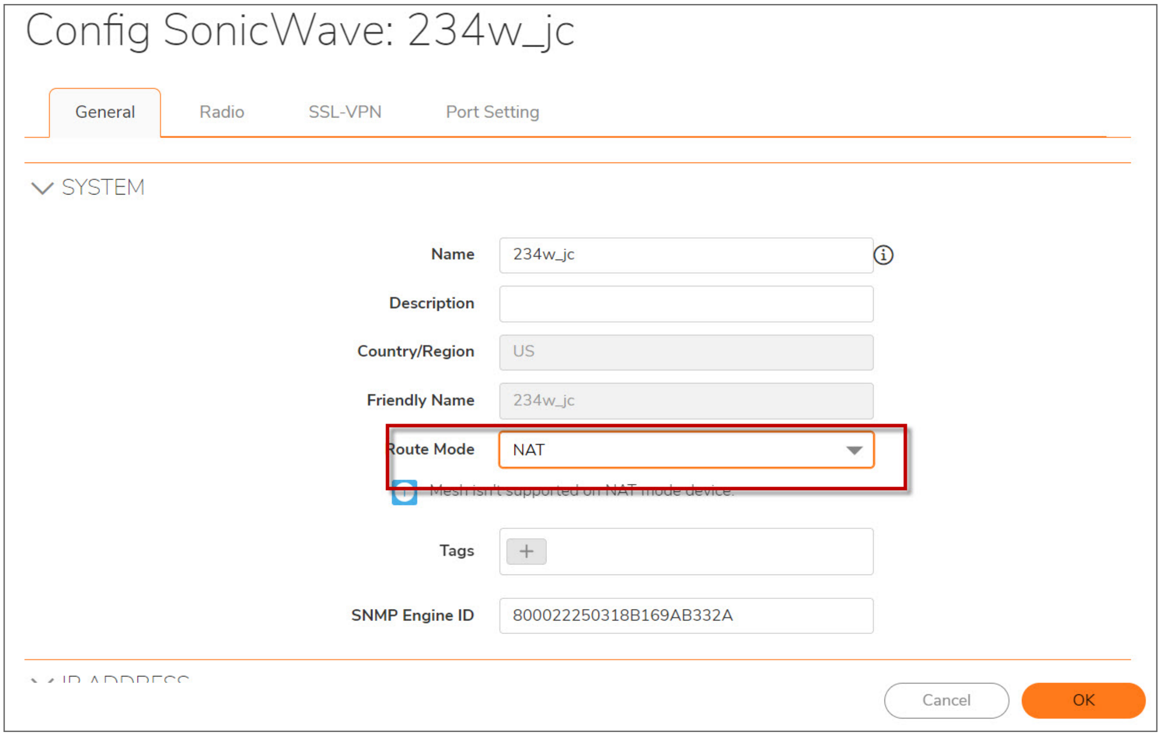
Wireless Network Manager provides SonicWave NAT mode in addition to the previous Bridge mode.

NAT mode is usually used on single access point deployment. With NAT mode, the user does not need to set up a special DHCP server for the client. SonicWave sets up a DHCP server for each VAP automatically.

When NAT mode is configured, **Static IP Address** configuration is supported. For more details, follow the steps given below.

ⓘ | **NOTE:** Mesh network is not supported for the devices configured to use NAT mode.

ⓘ | **NOTE:** 4G/LTE mode is only supported on NAT mode.



Config SonicWave: 234w_jc

Name	234w_jc
Description	
Country/Region	US
Friendly Name	234w_jc
Route Mode	NAT

Mesh isn't supported on NAT mode device.

Tags	+
SNMP Engine ID	800022250318B169AB332A

To change the SonicWave mode to NAT mode:

1. Click **General**.
2. Select **NAT** from the **Route Mode** list.

When NAT mode is configured, **Static IP Address** configuration is supported.

To configure a static IP address:

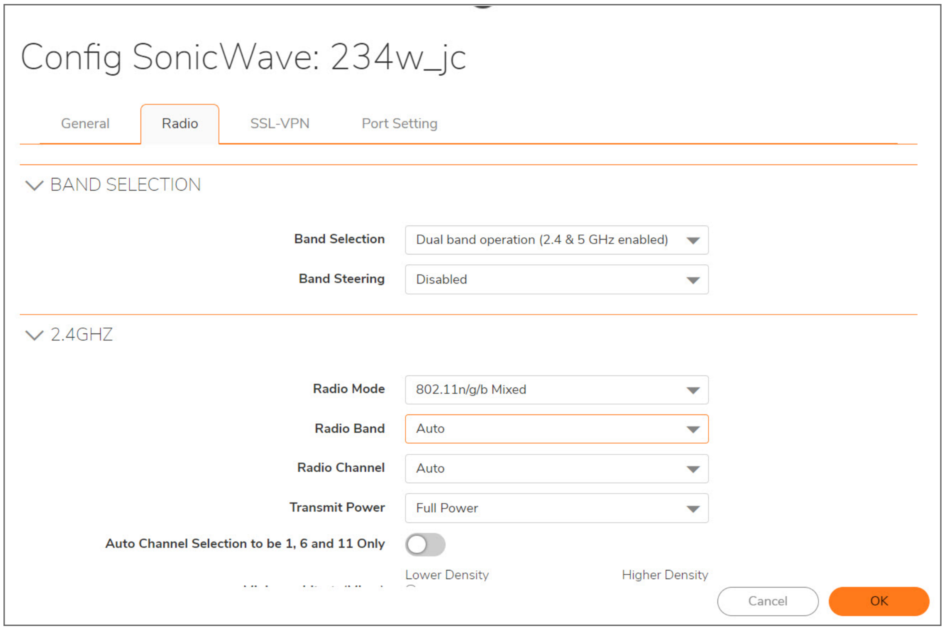
1. Navigate to the **Network > Devices** page.
2. Select **Access Points**.
3. On the right of the device row, click **Config/Edit.** The **Config SonicWave** page displays.
4. Click **General.**
5. Set the route mode to **NAT**.
6. In the **IP Address** section:
   a. Set the mode to **Static**.
   b. Set the static IP settings in the associated fields. This includes **Static IP**, **Netmask**, **Gateway**, **Primary DNS**, and **Secondary DNS**.
7. Click **OK**.

To configure for a DHCP IP address:

1. Navigate to the **Network > Devices** page.
2. Select **Access Points**.
3. On the right of the device row, click **Config/Edit**. The **Config SonicWave** page displays.
4. Click **General**
5. Set the route mode to **NAT**.
6. In the **IP Address** section, set the mode to **DHCP**.
7. Click **OK**.

Radio

The **Radio** page provides the administrator with control over Band Selection and various configuration options for each of the available bands - Dual Band Operation (2.4 and 5 GHz enabled, 2.4 GHz only, 5 GHz only, and Disabled.



Config SonicWave: 234w_jc

BAND SELECTION

Band Selection	Dual band operation (2.4 & 5 GHz enabled)
Band Steering	Disabled

2.4GHZ

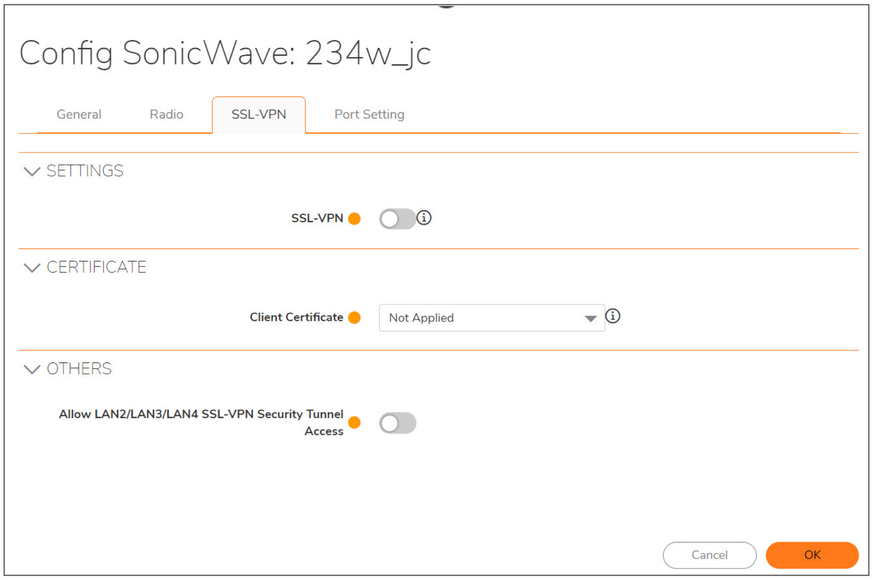
Radio Mode	802.11n/g/b Mixed
Radio Band	Auto
Radio Channel	Auto
Transmit Power	Full Power
Auto Channel Selection to be 1, 6 and 11 Only	○

Wireless Data Traffic Minimum Rate Control on the **Configure SonicWave** page improves wireless efficiency, since transfers at lower rates takes up excess available air time. Roaming improves with this feature, since, by disabling slow (*i.e.* bad) connections, the system forces devices to roam earlier.

SSL VPN

This feature provides support for SSL-VPN connections to SonicWall Secure Mobile Access (SMA) appliances and SonicWall firewalls and can be done with NX VPN or CT VPN.

When the SonicWave is in standalone mode, the administrator can configure SSL-VPN settings from the web management interface. The SonicWave wireless access point will then launch an AvConnect client and control process, to provide the secure tunnel for wireless client access.



Config SonicWave: 234w_jc

SETTINGS

SSL-VPN ●

CERTIFICATE

Client Certificate ● Not Applied

OTHERS

Allow LAN2/LAN3/LAN4 SSL-VPN Security Tunnel Access ●

For more information on editing SSL-VPN, refer to Editing SSL-VPN

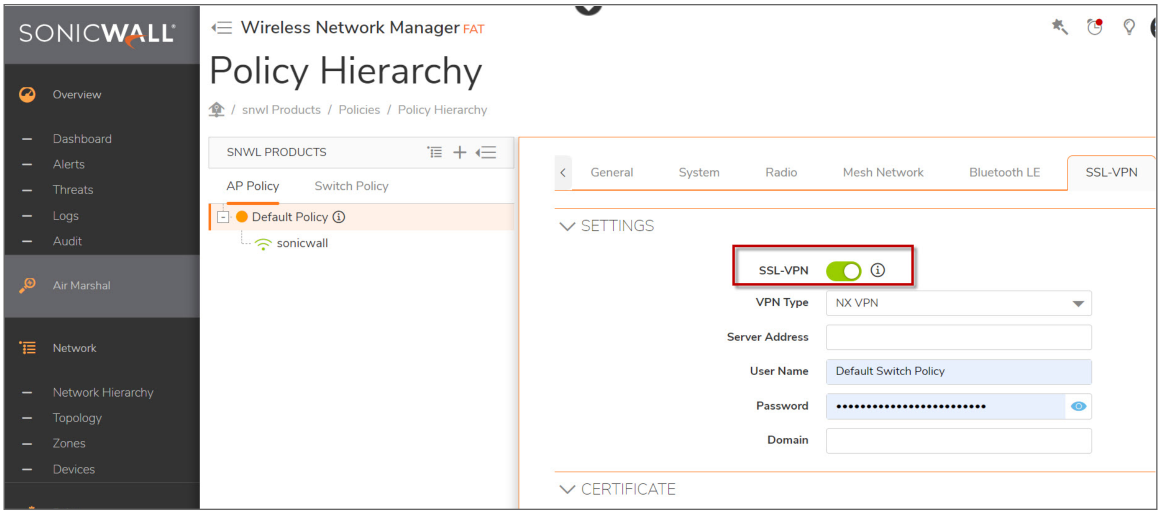
Topics:

- Activating SSL VPN
- Certificate
- Others

Activating SSL VPN

To activate the SSL-VPN options for a device:

1. Navigate to **Policies > Policy Hierarchy**.
2. Select the AP Policy.
3. Click the **SSL-VPN** tab.
4. In the **Settings** section, click the **SSL-VPN** slider to activate SSL-VPN support.



SSL-VPN: on

VPN Type: NX VPN

Server Address:

User Name: Default Switch Policy

Password: ••••••••••••••••••••••••

Domain:

5. Enter the values for the options for **SSL-VPN** connection, including the **VPN Type**, **Server Address**, **User Name**, **Password**, and **Domain**.

6. In the **Certificate** section, from the **Client Certificate** drop-down list, select the certificate you want used for the policy.

   ⓘ | **NOTE:** The CT VPN supports the certificate option where as NX VPN does not.

7. In the **Others** section, click the **Allow Security Tunnel Access** for LAN2/LAN3/Lan4.

8. Click **OK**.

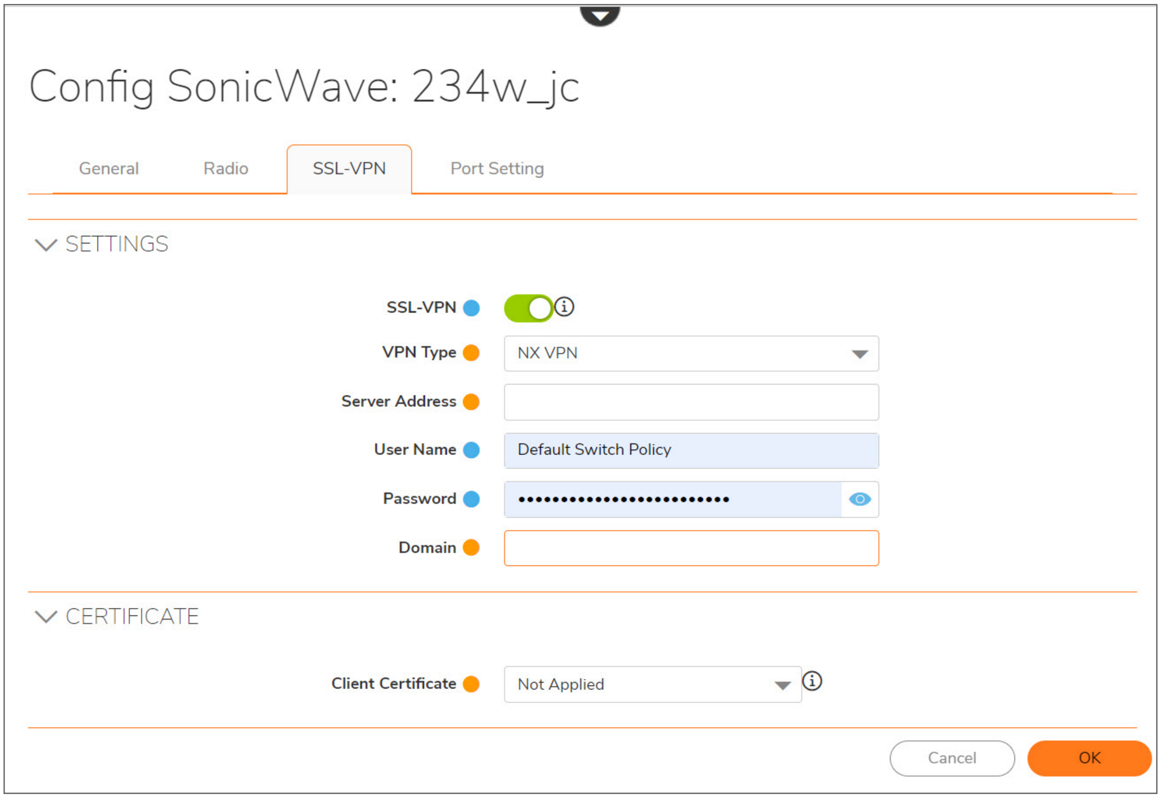
Editing SSL-VPN

You can edit the SSL-VPN from the **Network** > **Devices** page.

To edit SSL VPN:

1. Click on **Config/Edit** on the right of the SonicWave row to display the **Configuration** screen.
2. Click on the **SSL-VPN** tab.
3. Modify the required fields.

4. Click **OK** to save the changes.



Config SonicWave: 234w_jc

SETTINGS

SSL-VPN: On

VPN Type: NX VPN

Server Address:

User Name: Default Switch Policy

Password: ••••••••••••••••••••••••

Domain:

CERTIFICATE

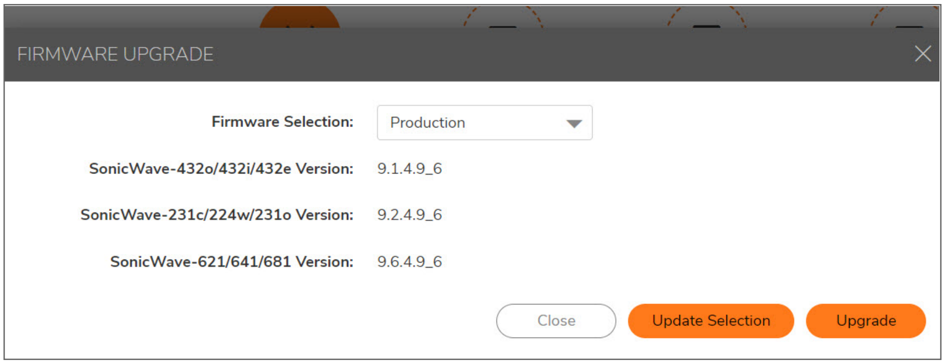
Client Certificate: Not Applied

Upgrading the Firmware for Specific Access Points

Wireless Network Manager, administrators can upgrade the firmware for specific SonicWave access points managed by Wireless Network Manager.

To upgrade the firmware for an access point:

1. Navigate to **Network > Devices**.
2. On the right of the access point for which you want to upgrade the firmware, click the **Upgrade** icon ⬆.
   The **Firmware Upgrade** dialog displays.



FIRMWARE UPGRADE

Firmware Selection: Production

SonicWave-432o/432i/432e Version: 9.1.4.9_6

SonicWave-231c/224w/231o Version: 9.2.4.9_6

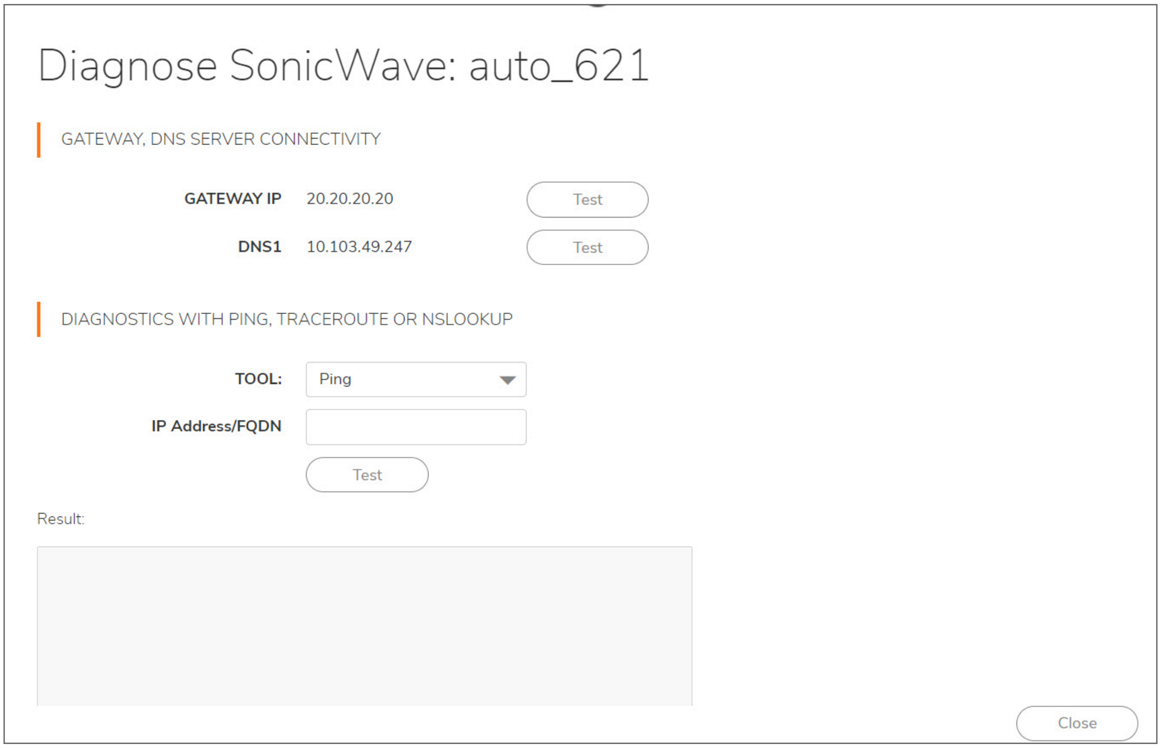
SonicWave-621/641/681 Version: 9.6.4.9_6

3. From the **Firmware Selection** list, select the type of firmware upgrade you want to perform:
    - **Production**: The latest approved firmware release
    - **Beta**: The latest Beta version firmware for the device
    - **Patch**: The latest patch release to currently installed firmware
    - **Previous Stable**

    The version number of the associated firmware selection will be displayed.
4. Click **Update Selection** to update the firmware selection.
5. Click **Upgrade**.
6. When the **Upgrade command sent to online access points** message displays, click **OK**.

SonicWave Diagnostics

You can use the Diagnostics to test the connections of your SonicWave wireless access points.



Diagnose SonicWave: auto_621

GATEWAY, DNS SERVER CONNECTIVITY

GATEWAY IP 20.20.20.20

DNS1 10.103.49.247

DIAGNOSTICS WITH PING, TRACEROUTE OR NSLOOKUP

TOOL: Ping

IP Address/FQDN

Result:

Topics:

- Testing Connectivity With Your Gateway or DNS Addresses
- Testing Connectivity With Ping, Traceroute, or NSLookup

Testing Connectivity With Your Gateway or DNS Addresses

You can test the connectivity of the SonicWave with your gateway or DNS addresses.

To test the connectivity of a SonicWave with your gateway or DNS addresses:

1. Navigate to the **Network > Devices** pages.
2. On the row for the device you want to test, hover over the far right area until the configuration icons appear.

   ⓘ | **IMPORTANT:** The device must be online.

3. Select the **Diagnostics** (Magnifier) icon. the **Diagnose SonicWave** page displays.
4. Specify the **Target (host name or IP address)**.
5. In the **Gateway, DNS Connectivity** section, click **Test** next to the diagnostic test you want to run. The results will be displayed next to that **Test** button.
6. Click **Close** to close the **Diagnose SonicWave** page.

Testing Connectivity With Ping, Traceroute, or NSLookup

You can use the Diagnostics to test the connections of your SonicWave using either through pings or a trace route.

To test the connectivity of a SonicWave using pings or a trace route:

1. Navigate to the **Network > Devices** pages.
2. On the row for the device you want to test, hover over the far right area until the configuration icons appear.

   ⓘ | **IMPORTANT:** The device must be online.

3. Select the Diagnostics (Magnifier) 🔍 icon. the **Diagnose SonicWave** page displays.
4. In the **Diagnostics with Ping or Trace route** section, select the option from the **Tool** drop down that you want to use:
   - **Ping**
   - **Traceroute**
   - **NSLookup**
5. In the **IP Address/Hostname** field, enter the IP address or fully qualified domain name (FQDN) you want to test.
6. Click **Test**. The results will be displayed below the **Result** section.
7. Click **Close** to close the **Diagnose SonicWave** page.

Viewing the Wireless Client Journey

Wireless client journey is a feature administrators can track the behavior of wireless clients connected to a SonicWave, such as connection and disconnection of the wireless client.

To view the wireless client history:

1. Navigate to **Network > Devices**.
2. Click **Clients** from the items available at the top of the page. All of the wireless clients connected through SonicWave wireless access points are listed in the table.
3. Hover over a specific device to access the different icons :
   - Displays the logs.
   - + Click to add the devices to the Client MAC Address Group. When you want to add a client mac to group, you must go to address group page to create a new group (if address group page has no groups), then click this button in client page, and you will see the group you added.

     ⓘ | **NOTE:** You can only select one group.

Address group page will display the client mac information in the group and the client mac AO will be displayed in address objects page.

- 🗑 Disconnects the connected clients device. It takes around 10 seconds for the changes to take into effect.

  This button remains gray and can’t be clicked when client is disconnected. When client status is connected, the button can be clicked.

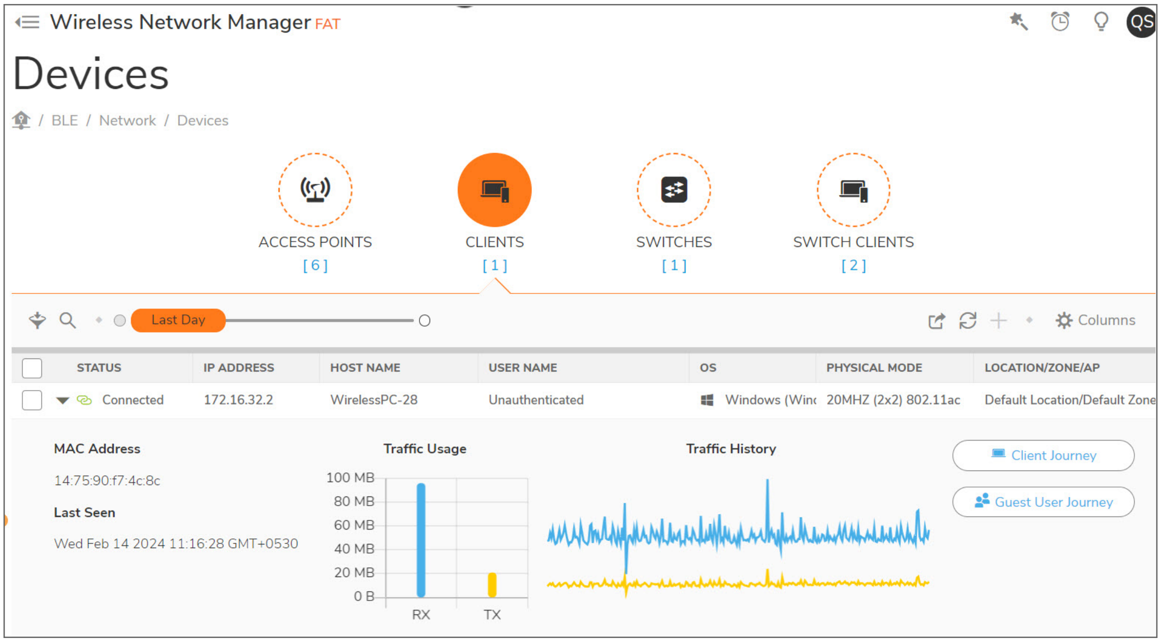
  By clicking this button, the clients SSID gets disconnected. But this entry will not be changed in 5 minutes. After 5 minutes, the entry client status will be changed to disconnected.

- 👤 Status of the sign-on

  - Navigate to **Policies> SSID Policies** page to edit SSID the connected client.Go to **Guest Portal** page, not only click-through option, select other options besides **None**.
  - After using client to connect SSID, you will be redirected to login website page. If this option is selected upon login, this icon changes to and **‘log out user’.**
  - To login again, navigate to the website and enter the credentials.
  - After 5 minutes, the user name will be changed to unauthenticated, and gets disabled and displayed as **'user has been logout'**.
  - When you don’t login to this page, the client host username will be unauthenticated, and the button gets disabled and displays as **‘user has been logout’**
  - When Guest Portal type is selected as first option **None** and connects to SSID, this button remains gray and is displayed as **'guest disabled'.**

- ✎ Edits the host name field.

4. Click on a specific wireless client to displays the details for that device.



Devices

BLE / Network / Devices

□	STATUS	IP ADDRESS	HOST NAME	USER NAME	OS	PHYSICAL MODE	LOCATION/ZONE/AP
□	Connected	172.16.32.2	WirelessPC-28	Unauthenticated	Windows (Winc	20MHZ (2x2) 802.11ac	Default Location/Default Zone

MAC Address

14:75:90:f7:4c:8c

Last Seen

Wed Feb 14 2024 11:16:28 GMT+0530

5. The information displayed for the wireless client includes:

   - MAC Address
   - Status
   - IP address
   - Host Name
   - User Name
   - Operating System
   - Physical Mode
   - Location, Zone, and Access Point
   - SSID
   - Radio
   - Connection Quality
   - RSSI
   - Vendor
   - Last Seen time

   The **Traffic Usage** graph displays the bandwidth details of the device.

   The **Traffic History** graph displays the current and historical traffic for the device.

   There are two kind of client journey messages listed in the wireless client details:

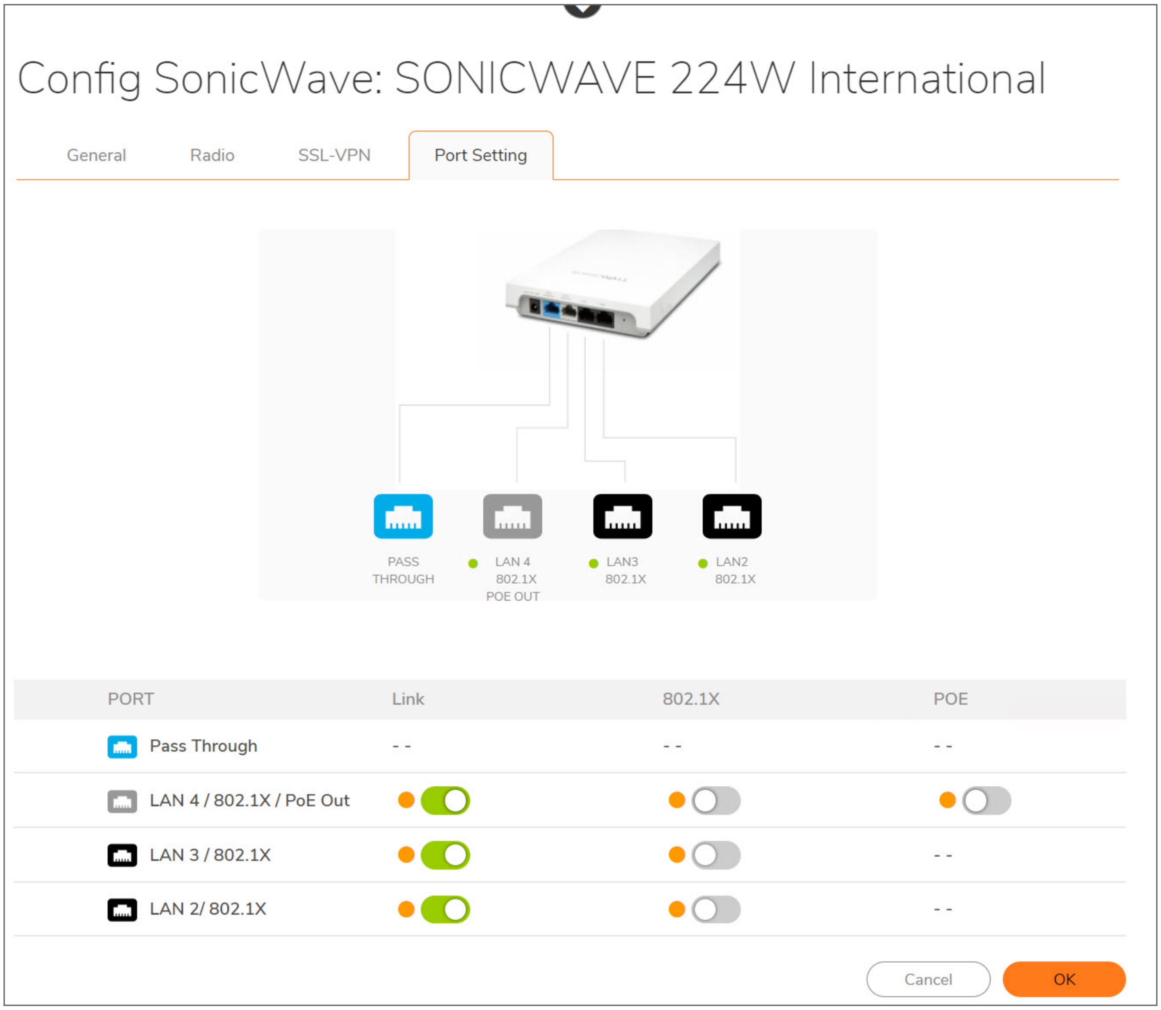
   - **Client Journey** - The connection and disconnection times of the client
   - **Guest User Journey** - The behavior of any guest users who logged in using that wireless client

ⓘ | **NOTE:** The maximum tracking period for a device is 30 days.

Port Settings

Wireless Network Manager provides a way for the user to enable or disable the LAN switch port. By default, the switch ports are down. To access this feature, edit the chosen device on this screen.

ⓘ | **NOTE:** This feature is only available for the SonicWave 224w.



Config SonicWave: SONICWAVE 224W International

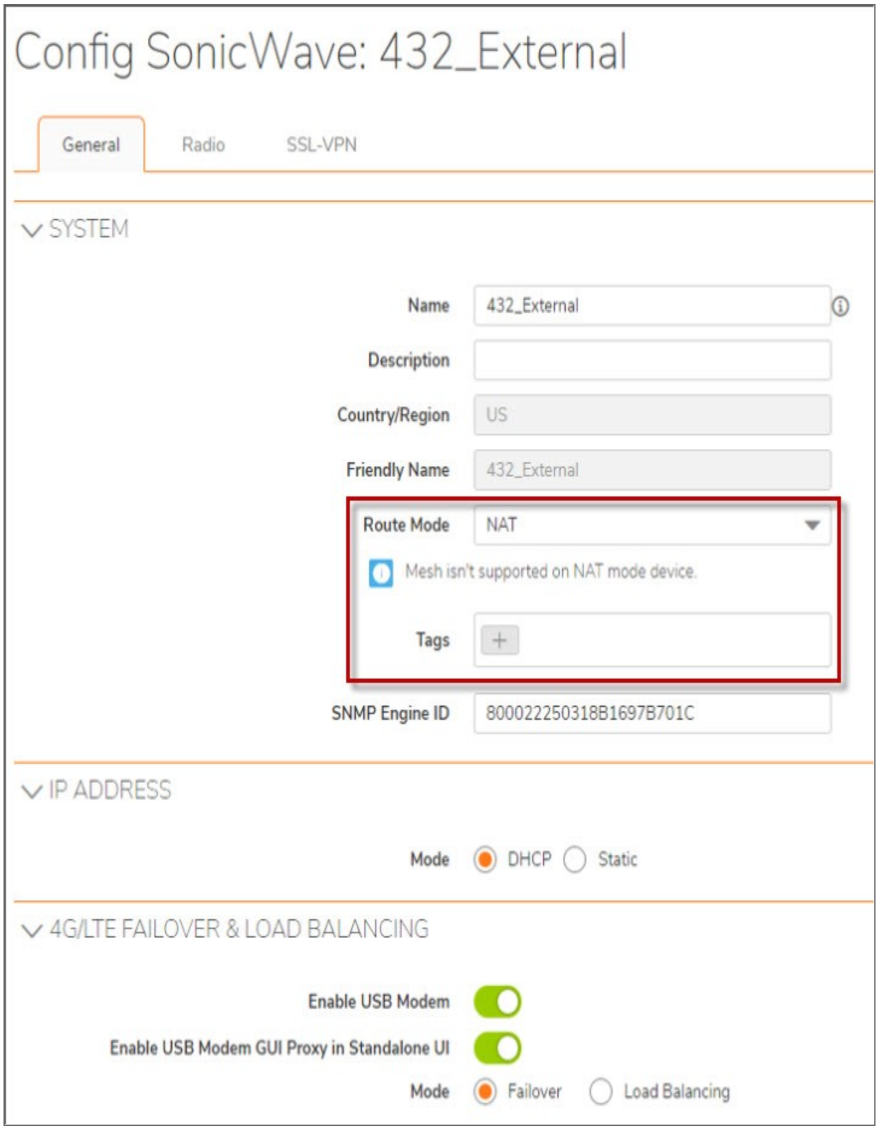
PORT	Link	802.1X	POE
Pass Through	- -	- -	- -
LAN 4 / 802.1X / PoE Out	● ☑	● ☐	● ☐
LAN 3 / 802.1X	● ☑	● ☐	- -
LAN 2/ 802.1X	● ☑	● ☐	- -

Wireless Network Manager provides Failover and Load Balancing support with 4G/LTE USB modems in SonicWave under cloud management.

By clicking on **Config/Edit** in the device row), then clicking on the **General** tab, you can edit a device on the **Config SonicWave** screen.

NOTE: The access point must be a model with a USB port.

The WAN load balance mode selections appear when the switch is in NAT mode.



Config SonicWave: 432_External

SYSTEM

Name	432_External
Description	
Country/Region	US
Friendly Name	432_External
Route Mode	NAT

Mesh isn't supported on NAT mode device.

Tags	+
SNMP Engine ID	800022250318B1697B701C

IP ADDRESS

Mode ● DHCP ○ Static

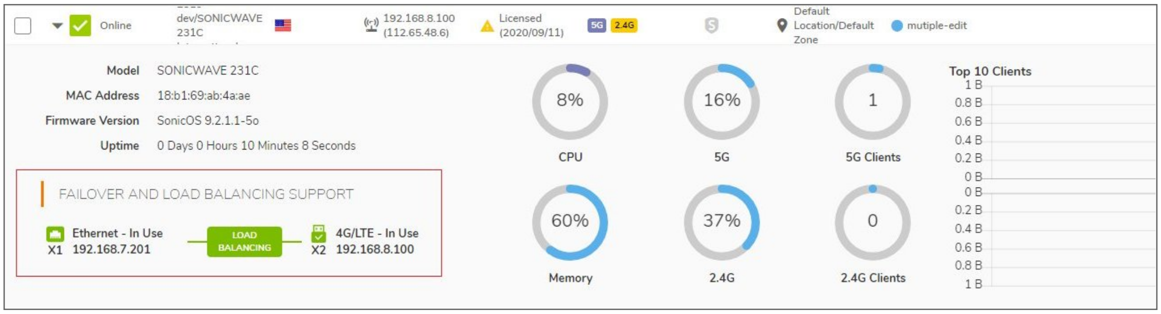
4G/LTE FAILOVER & LOAD BALANCING

Enable USB Modem: On

Enable USB Modem GUI Proxy in Standalone UI: On

Mode ● Failover ○ Load Balancing

When applied, these indicators are displayed:



Online dev/SONICWAVE 231C 192.168.8.100 (112.65.48.6) Licensed (2020/09/11) Default Location/Default Zone mutiple-edit

Model SONICWAVE 231C

MAC Address 18:b1:69:ab:4a:ae

Firmware Version SonicOS 9.2.1.1-5o

Uptime 0 Days 0 Hours 10 Minutes 8 Seconds

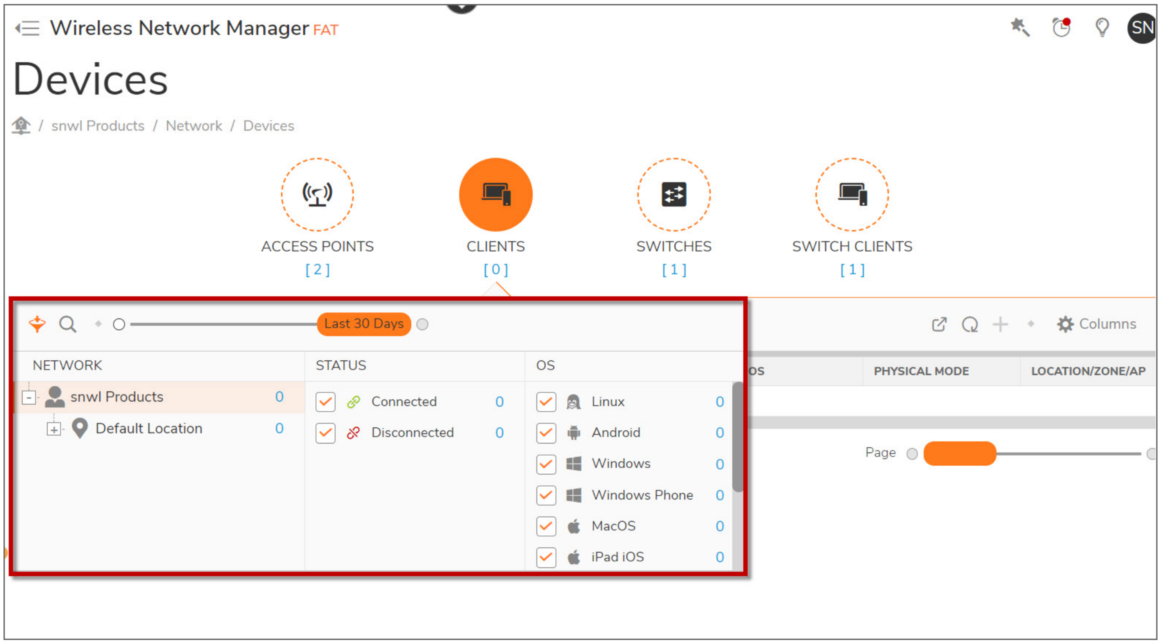
FAILOVER AND LOAD BALANCING SUPPORT

X1 Ethernet - In Use 192.168.7.201 LOAD BALANCING X2 4G/LTE - In Use 192.168.8.100

The **Clients** page displays status information for the Client Devices, as seen below. At the top, there is a time line that can be slid from left to right to show:

- Last Day
- Last Week
- Last 30 Days.

It also displays the operating system used by each one of the Client Devices.



Wireless Network Manager FAT

Devices

snwl Products / Network / Devices

ACCESS POINTS [2] CLIENTS [0] SWITCHES [1] SWITCH CLIENTS [1]

NETWORK		STATUS		OS	
snwl Products	0	☑ Connected	0	☑ Linux	0
Default Location	0	☑ Disconnected	0	☑ Android	0
				☑ Windows	0
				☑ Windows Phone	0
				☑ MacOS	0
				☑ iPad iOS	0

The bottom panel has columns that give more information about each device.

Managing Switches

You can use Wireless Network Manager to manage features of connected SonicWall Switches.

These Switch management features are supported by Wireless Network Manager in this release:

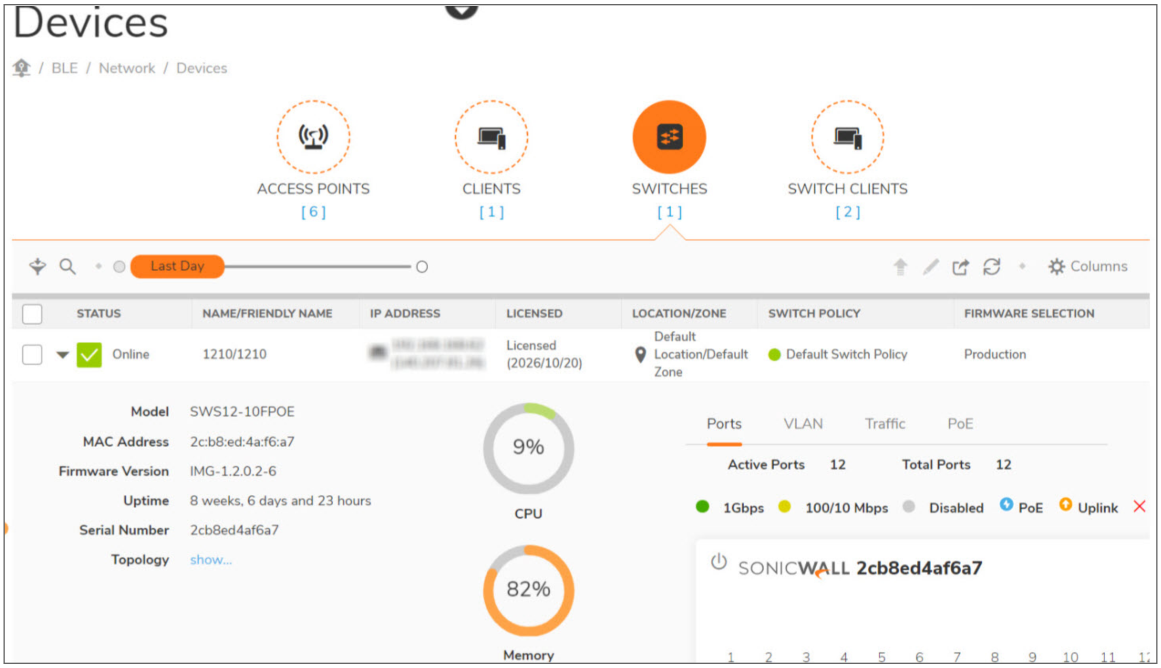
- Dashboard
- Network IPv4 Network
- System Information
- User Management
- ARP Global
- ARP Table
- Authentication
- Firmware Images - Upgrade
- DHCP Snooping - settings
- DHCP Relay
- Port Settings - QoS
- Port Settings - POE
- Port Settings - Security - 802.1x
- Port Settings - ACL Binding (IPv4)
- Port Settings - Advanced
- STP - Settings - Bridge Priority
- LBD - Global
- Link Aggregation
- Jumbo Frames
- MAC Address Table - Static MAC address
- MAC Address Table - Dynamic MAC address
- LLDP - Global Settings
- IGMP Snooping
- Multicast Filtering
- QoS
- Port Statistics
- Static Routes (IPv4)
- 802.1x
- DoS
- ACL Management
- 802.1Q
- Voice VLAN
- Log

ⓘ **NOTE:** For the Switch to be managed by Wireless Network Manager, the switch firmware must be version 1.0.0.3-12s or higher. It is highly recommended to upgrade the Switch firmware to version 1.1 once it is being managed by Wireless Network Manager.

To manage a Switch:

1. Navigate to **Network > Devices**.
2. Click **Switches**.
3. Select the switch you want to manage and hover over the far right section of the row to access the

management icons.



Devices

BLE / Network / Devices

ACCESS POINTS [6] CLIENTS [1] SWITCHES [1] SWITCH CLIENTS [2]

Last Day Columns

STATUS	NAME/FRIENDLY NAME	IP ADDRESS	LICENSED	LOCATION/ZONE	SWITCH POLICY	FIRMWARE SELECTION
Online	1210/1210	[redacted]	Licensed (2026/10/20)	Default Location/Default Zone	Default Switch Policy	Production

Model	SWS12-10FPOE
MAC Address	2c:b8:ed:4a:f6:a7
Firmware Version	IMG-1.2.0.2-6
Uptime	8 weeks, 6 days and 23 hours
Serial Number	2cb8ed4af6a7
Topology	show...

9% CPU

82% Memory

Ports VLAN Traffic PoE

Active Ports 12 Total Ports 12

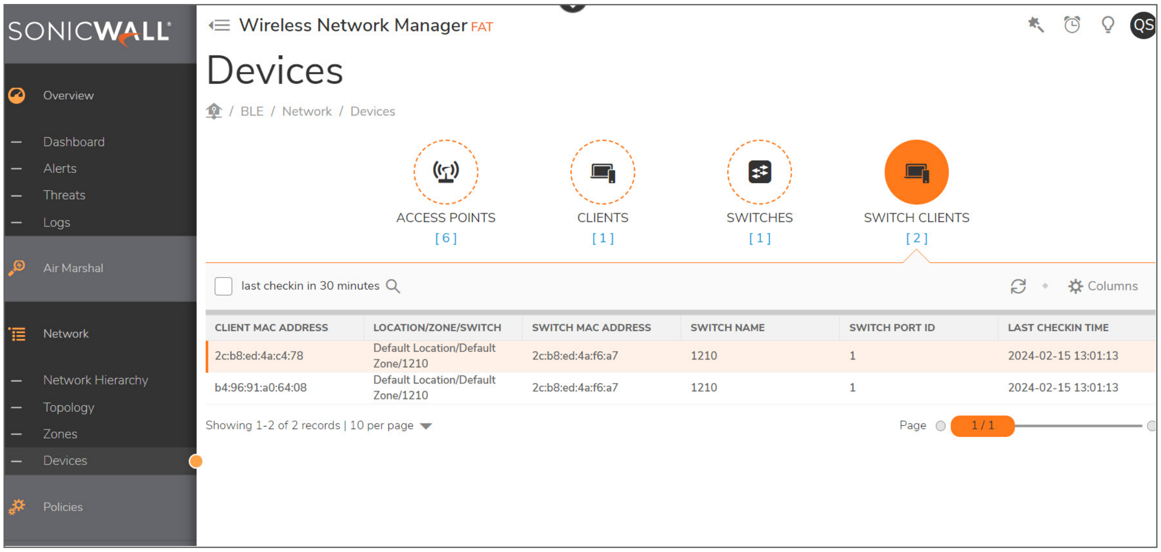
1Gbps 100/10 Mbps Disabled PoE Uplink

SONICWALL 2cb8ed4af6a7

Managing Switch Clients

You can use Wireless Network Manager to manage features of connected SonicWall Switch clients.

Navigate to **Network** > **Devices** > **Switch Clients** tab and the following page is displayed.



Wireless Network Manager FAT

Devices

BLE / Network / Devices

ACCESS POINTS [6] CLIENTS [1] SWITCHES [1] SWITCH CLIENTS [2]

□ last checkin in 30 minutes Columns

CLIENT MAC ADDRESS	LOCATION/ZONE/SWITCH	SWITCH MAC ADDRESS	SWITCH NAME	SWITCH PORT ID	LAST CHECKIN TIME
2c:b8:ed:4a:c4:78	Default Location/Default Zone/1210	2c:b8:ed:4a:f6:a7	1210	1	2024-02-15 13:01:13
b4:96:91:a0:64:08	Default Location/Default Zone/1210	2c:b8:ed:4a:f6:a7	1210	1	2024-02-15 13:01:13

Showing 1-2 of 2 records | 10 per page

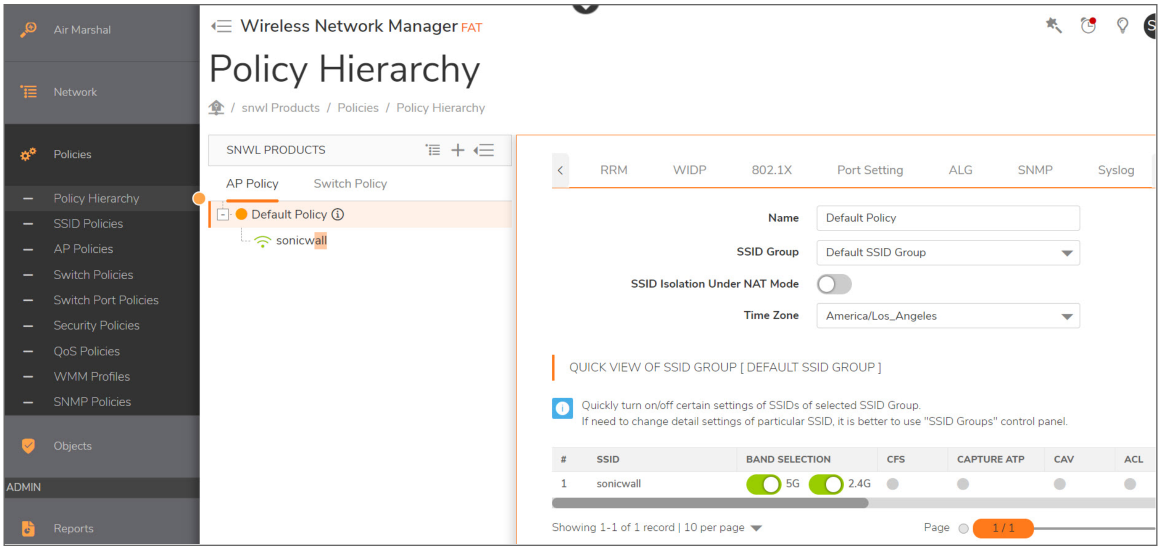
Page 1 / 1

Switch Client feature provides the search option to discover a client faster with their MAC address to discover the switch, ports and location it is associated with. Click on 🔍 and search for the MAC address in the search field to find a specific client or device.

5

Managing Policies

The Policies section helps you to navigate to the Policy Hierarchy and other pages including AP Policies, Security Policies, and so on.



Name: Default Policy

SSID Group: Default SSID Group

SSID Isolation Under NAT Mode

Time Zone: America/Los_Angeles

QUICK VIEW OF SSID GROUP [DEFAULT SSID GROUP]

Quickly turn on/off certain settings of SSIDs of selected SSID Group.
If need to change detail settings of particular SSID, it is better to use "SSID Groups" control panel.

#	SSID	BAND SELECTION	CFS	CAPTURE ATP	CAV	ACL
1	sonicwall	5G 2.4G	●	●	●	●

Showing 1-1 of 1 record | 10 per page

Page 1 / 1

The AP Policies, Security Policies, and SSIDs are marked with different symbols, so they can be clearly distinguished from each other:

- **AP Policies** have a colored ball
- Each type of **Security Policy** has its own square symbol
- **SSIDs** are labeled with a Wi-Fi symbol

The color of the symbol changes with its status:

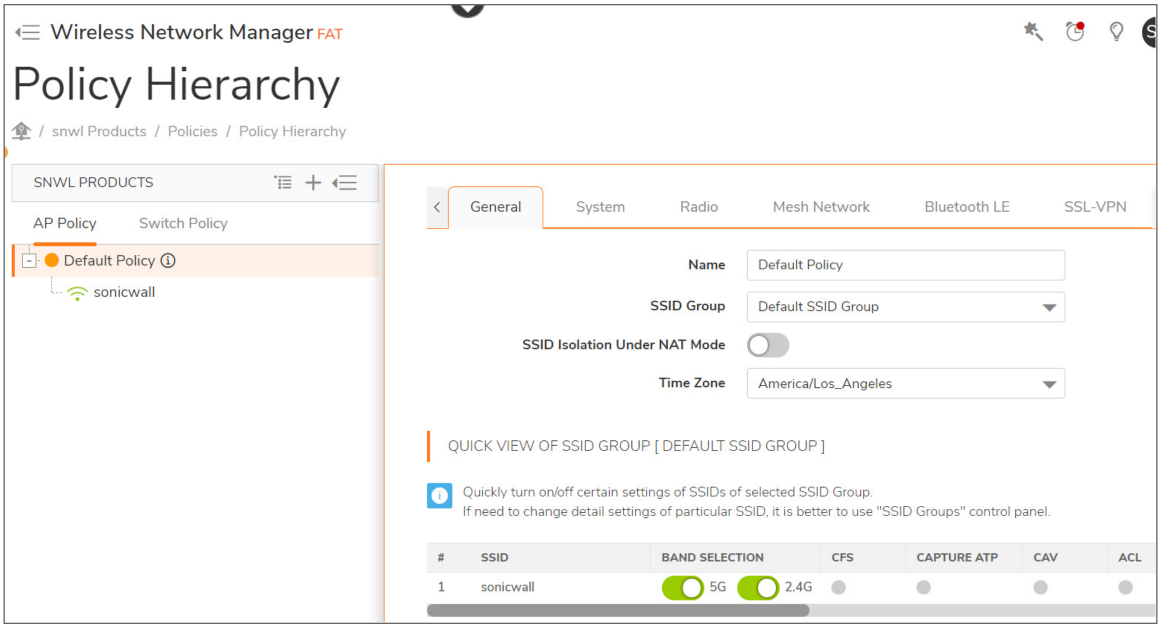
- The **AP Policy** ball is orange if it is in a default condition, or blue if it has been manually configured. When it is blue, it still retains its default settings, but in addition it has those that were manually set. Clicking on a **AP Policy** blue ball returns it to its default condition.
- The square **Security Policy** symbol can be green if fully enabled, orange if partially enabled, or gray if not enabled, as indicated by the screen tips when you hover over the symbol.

Topics:

- Policy Hierarchy
- SSID Policies
- AP Policies
- Select a Switch Policy
- Managing Switch Port Policies
- Security Policies
- QoS Policies
- Wi-Fi Multimeda (WMM) Profiles
- Managing SNMP Policies

Policy Hierarchy

The **Policy Hierarchy** page provides settings for monitoring, creating and managing the policies on your network. The middle pane displays both **AP Policy** and **Switch Policy**, that gives an overview of your AP policy structure, with the Tenant/Group at the top.



Wireless Network Manager FAT

Policy Hierarchy

/ snwl Products / Policies / Policy Hierarchy

SNWL PRODUCTS

AP Policy | Switch Policy

Default Policy

sonicwall

General | System | Radio | Mesh Network | Bluetooth LE | SSL-VPN

Name	Default Policy
SSID Group	Default SSID Group
SSID Isolation Under NAT Mode	○
Time Zone	America/Los_Angeles

QUICK VIEW OF SSID GROUP [DEFAULT SSID GROUP]

Quickly turn on/off certain settings of SSIDs of selected SSID Group.
If need to change detail settings of particular SSID, it is better to use "SSID Groups" control panel.

#	SSID	BAND SELECTION	CFS	CAPTURE ATP	CAV	ACL
1	sonicwall	5G 2.4G	●	●	●	●

Topics:

- Select an AP Policy
- Select a Switch Policy
- Select an SSID
- Select a Security Policy

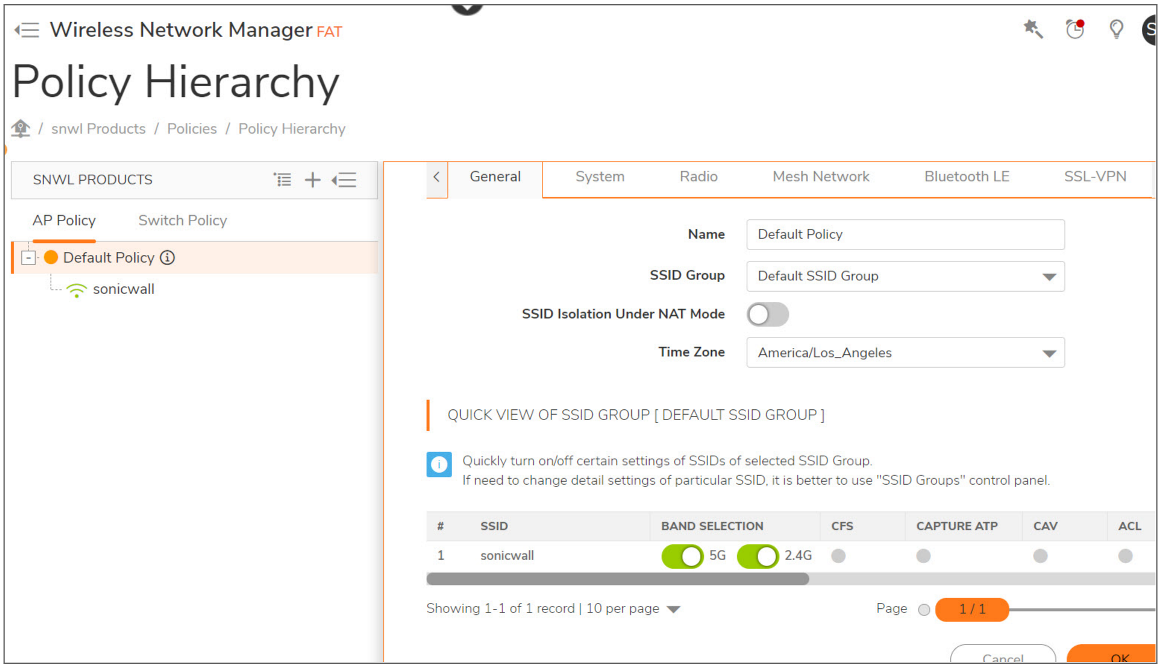
Select an AP Policy

Selecting an AP Policy listed in the **Policy Hierarchy** page brings up these information fields on the right pane, that you can edit further if required:

- General
- System
- Radio
- Mesh Network
- Bluetooth
- SSL VPN
- RRM (Radio Resource Management)
- WIDP
- 802.1X
- Port Settings
- ALG
- SNMP
- Syslog

General

When you click **Policies > Policy Hierarchy > Select an AP policy**, the **General** tab appears on the right screen by default:



Name: Default Policy

SSID Group: Default SSID Group

SSID Isolation Under NAT Mode: ○

Time Zone: America/Los_Angeles

QUICK VIEW OF SSID GROUP [DEFAULT SSID GROUP]

Quickly turn on/off certain settings of SSIDs of selected SSID Group.
If need to change detail settings of particular SSID, it is better to use "SSID Groups" control panel.

#	SSID	BAND SELECTION	CFS	CAPTURE ATP	CAV	ACL
1	sonicwall	● 5G ● 2.4G	○	○	○	○

Showing 1-1 of 1 record | 10 per page

Page 1 / 1

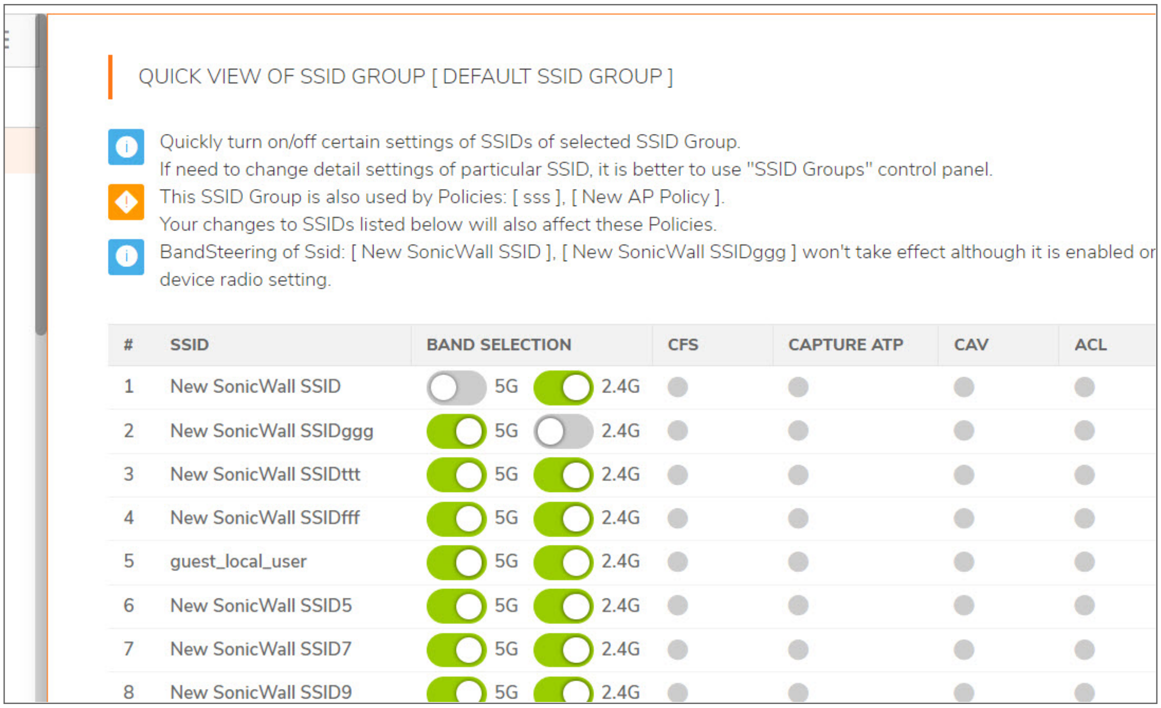
At the top of the screen is the **Name** of the policy and the **SSID Group** it applies to. The **Default Policy**, at the top of the hierarchy, is the policy that is always in effect, no matter which other policies are applied for a particular

SSID. It is an automatic attribute of the **Tenant/Group** through the access points used in the hierarchy, and it applies to the entire hierarchy.

You can enable or disable **SSID Isolation Under NAT Mode**. This feature allows clients to be isolated even when they connect to the same SSID. It also isolates the clients between SSIDs.

The last field is for the **Time Zone**.

QUICK VIEW OF SSID GROUP - Gives a list of the SSID's in the group, with a table of configurations applied to them.



QUICK VIEW OF SSID GROUP [DEFAULT SSID GROUP]

Quickly turn on/off certain settings of SSIDs of selected SSID Group.
If need to change detail settings of particular SSID, it is better to use "SSID Groups" control panel.

This SSID Group is also used by Policies: [sss], [New AP Policy].
Your changes to SSIDs listed below will also affect these Policies.

BandSteering of Ssid: [New SonicWall SSID], [New SonicWall SSIDggg] won't take effect although it is enabled or
device radio setting.

#	SSID	BAND SELECTION	CFS	CAPTURE ATP	CAV	ACL
1	New SonicWall SSID	○ 5G ● 2.4G	●	●	●	●
2	New SonicWall SSIDggg	● 5G ○ 2.4G	●	●	●	●
3	New SonicWall SSIDttt	● 5G ● 2.4G	●	●	●	●
4	New SonicWall SSIDfff	● 5G ● 2.4G	●	●	●	●
5	guest_local_user	● 5G ● 2.4G	●	●	●	●
6	New SonicWall SSID5	● 5G ● 2.4G	●	●	●	●
7	New SonicWall SSID7	● 5G ● 2.4G	●	●	●	●
8	New SonicWall SSID9	● 5G ● 2.4G	●	●	●	●

The columns listed in the **Quick View of SSID Group** table, are explained below:

- **SSID Name**
- **Band Selection** - You can change the band for the SSID.
- **CFS** - Content Filtering Service is a web filtering security service that blocks inappropriate, unproductive, and illegal or malicious web content according user specifications. The table shows if this service is active on the SSID or group of SSIDs.
- **Capture ATP** - Capture Advanced Threat Protection is a cloud-based feature that analyzes files and determines if the file is malicious or acceptable.
- **CAV** - Cloud AV is a security policy that provides real-time file-virus scanning and reporting without consuming local computing resources. A record of the analysis is kept for a selected period of time.
- **ACL** - Access Control is a policy that manages access to mac address objects and access object groups over time. It prevents unnecessary duplication when a similar or the same packet issue is detected.
- **Geo-IP & Botnet** - These two blocking features are shown or activated on this screen.

- **Geo-IP** allows network administrators to block connections to or from a particular geographic location. It uses the IP address to determine the location of the intended connection.
- A **Botnet** can be used to steal data, send spam, and allow an attacker to access a device and its connection. This feature is activated and configured by the administrator to block Botnet access to the network.

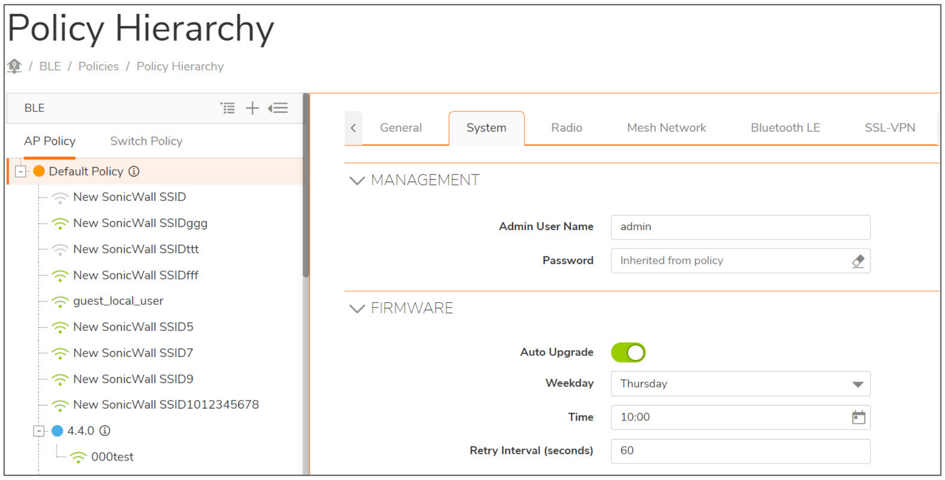
- **App Control - This toggle activates or deactivates application control.**
- **SSL VPN** - This selection enables or disables SSL VPN.
- **Authentication** - This column gives the authentication details for the SSID.
- **Hide SSID** - This is a toggle to enable or disable visibility of the SSID.
- **Active** - This toggle activates or deactivates the SSID.

System

When you click **Policies > Policy Hierarchy > Select an AP policy > System**, these fields appear on the right screen:

- **Management**, at the top, has an **Admin User Name** field and a **Password** field.
- **Firmware** has a toggle to **Auto Upgrade** the firmware, and time information for the upgrade. It also provides the **Retry Interval** in seconds.
- **Reboot** has the option to schedule the reboots of access points in Wireless Network Manager. This helps the users to be disconnected accordingly, and the memory of access points to be cleared including the association tables.
- **Others** has a toggle to choose whether the **LED** is on or off.

Click **OK** to save the configuration and return to the **General** screen.



Admin User Name: admin

Password: Inherited from policy

Auto Upgrade: on

Weekday: Thursday

Time: 10:00

Retry Interval (seconds): 60

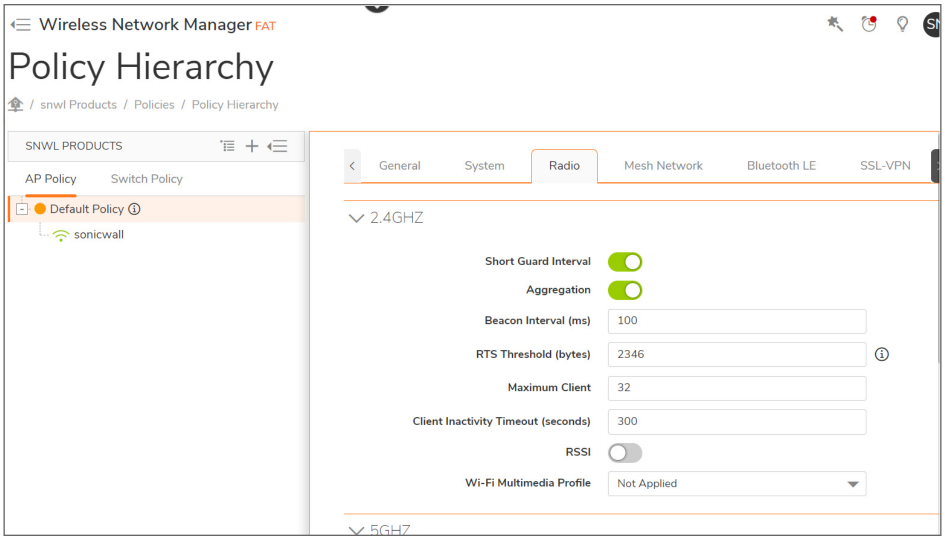
Radio

The **Radio** bar gives toggled choices concerning **Short Guard Interval** and **Aggregation**, along with fields in which to enter information. You can enter:

- **Short Guard Interval**
- **Aggregation**
- **Beacon Interval**
- **RTS Threshold**
- **Maximum Client**
- **Client Inactivity Timeout**
- **RSSI**
- **Wi-Fi Multimedia Profile**

Using the field for enabling or disabling **RSSI**, and for setting a threshold limit. in a high density Wi-Fi deployment, the user can set a desired RSSI Threshold on SonicWave. When a SonicWave goes off to prevent a low RSSI client connection, the client device can navigate to a nearby access point and get a higher connection rate and quality.

Each of these is available for 2.4 GHZ and 5 GHZ.



2.4GHZ

Short Guard Interval: on
Aggregation: on
Beacon Interval (ms): 100
RTS Threshold (bytes): 2346
Maximum Client: 32
Client Inactivity Timeout (seconds): 300
RSSI: off
Wi-Fi Multimedia Profile: Not Applied

Click **OK** to save the configuration and return to the **General** screen.

Mesh Network

The **Mesh Network** bar gives extra flexibility to the communication between the access points and the router. With Mesh Network, the access point devices are in constant communication among themselves to monitor the traffic that is passing in and out of the system. This constant communication makes it possible for them to reroute packets along alternate paths dynamically, if required.

- If **Mesh Radio** is enabled, the **Bluetooth LE advertisement** is enabled in access points for mobile APP connect.
- You can choose these options for the **Mesh Radio** bandwidth:
  - **5 GHZ**
  - **2.4 GHZ**
  - **Disabled**

  You can also choose the **RSSI**.

Click **OK** to save the configuration and return to the **General** screen.

Bluetooth

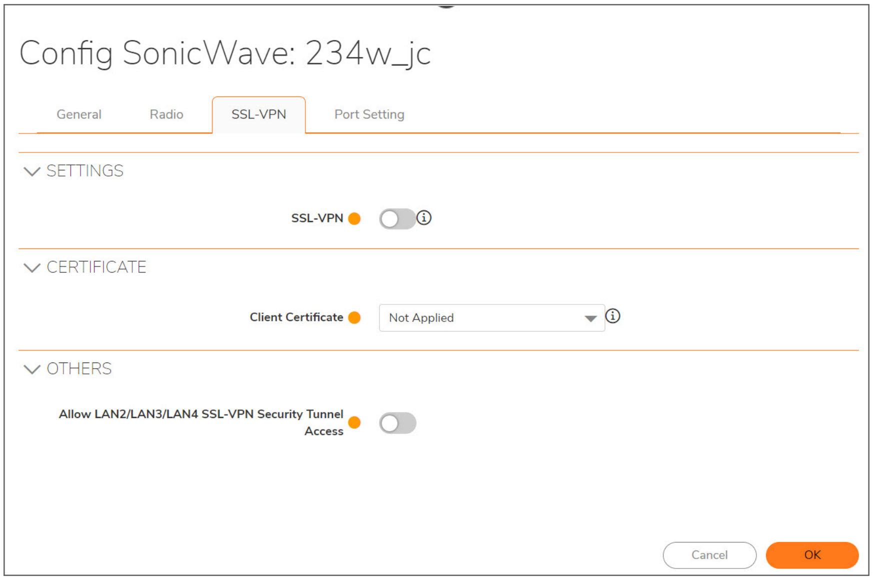
At **Policies > Policy Hierarchy > Select any AP policy > Bluetooth LE**, you can choose whether **Advertisement** and **iBeacon** are enabled. There is also a field for filling in the **UUID** when the option **iBeacon** is enabled. If it is required, a valid UUID must be entered before you can exit this screen. If the **Advertisement** toggle is disabled, there are no other choices on this screen.

Click **OK** to save the configuration and return to the **General** screen.

SSL VPN

This feature provides support for SSL-VPN connections to SonicWall Secure Mobile Access (SMA) appliances and SonicWall firewalls and can be done with NX VPN or CT VPN.

When the SonicWave is in standalone mode, the administrator can configure SSL-VPN settings from the web management interface. The SonicWave wireless access point will then launch an AvConnect client and control process, to provide the secure tunnel for wireless client access.



Config SonicWave: 234w_jc

For more information on editing SSL-VPN, refer to Editing SSL-VPN

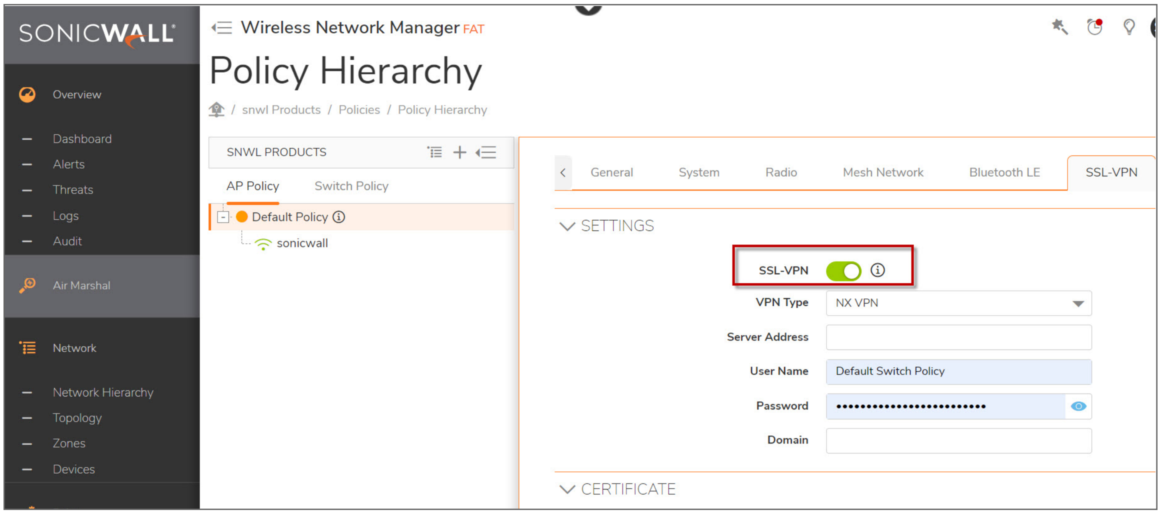
Topics:

- Activating SSL VPN
- Certificate
- Others

Activating SSL VPN

To activate the SSL-VPN options for a device:

1. Navigate to **Policies > Policy Hierarchy**.
2. Select the AP Policy.
3. Click the **SSL-VPN** tab.
4. In the **Settings** section, click the **SSL-VPN** slider to activate SSL-VPN support.



SSL-VPN: On

VPN Type: NX VPN

Server Address:

User Name: Default Switch Policy

Password: ••••••••••••••••••••••••

Domain:

5. Enter the values for the options for **SSL-VPN** connection, including the **VPN Type**, **Server Address**, **User Name**, **Password**, and **Domain**.
6. In the **Certificate** section, from the **Client Certificate** drop-down list, select the certificate you want used for the policy.

   ⓘ | **NOTE:** The CT VPN supports the certificate option where as NX VPN does not.
7. In the **Others** section, click the **Allow Security Tunnel Access** for LAN2/LAN3/Lan4.
8. Click **OK**.

Certificate

You can specify which client certificate should be used for the policy.

To specify a client certificate:

1. Navigate to **Policies > Policy Hierarchy**.
2. Select the AP Policy.
3. Click the **SSL-VPN** tab.
4. In the **Certificate** section, from the **Client Certificate** drop-down list, select the certificate you want used for the policy.
5. Click **OK**.

Others

This section allows you to allow your LAN connections SSL-VPN security tunnel access.

To allow SSL-VPN security tunnel access:

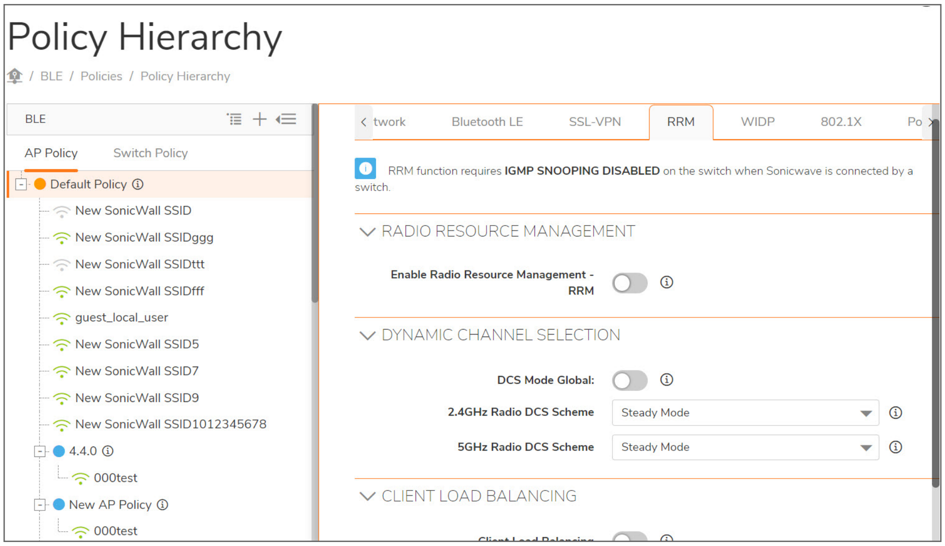
1. Navigate to **Policies > Policy Hierarchy**.
2. Select the AP Policy.

3. Click the **SSL-VPN** tab.
4. In the **Others** section, click the **Allow LAN2/LAN3/LAN4 SSL-VPN Security Tunnel Access** slider to allow SSL-VPN security tunnel access.
5. Click **OK**.

RRM (Radio Resource Management)

The RRM page contains these sections:

- **Radio Resource Management**
- **Dynamic Channel Selection**
- **Client Load Balancing**



RRM function requires **IGMP SNOOPING DISABLED** on the switch when Sonicwave is connected by a switch.

Enable Radio Resource Management - RRM ○

DCS Mode Global: ○

2.4GHz Radio DCS Scheme Steady Mode

5GHz Radio DCS Scheme Steady Mode

The Global Dynamic Channel Selection (DCS) helps to choose the proper channel for the SonicWave devices. Based on the DCS algorithm, the system uses RRM to take action dynamically, directing the client device to the AP that can give it the best signal. Global DCS is not available on SonicWave appliances that do not have a scan radio, such as the SonicWave 224w.

Radio Resource Management

To configure the Radio Resource Management options:

1. Navigate to **Policies > Policy Hierarchy.**
2. Select the AP Policy and click on the RRM.
3. In the **Radio Resource Management** section, click the **Enable Radio Resource Management - RRM** slider to activate or deactivate RRM.

4. In the **Station Quality Threshold (1 - 50)** field, enter the threshold value for the station quality. The default value is 20. Station Quality is the health index to track and assess the status of the wireless client connection varying between 1 and 50. The bigger index value means wireless station is connected with higher data rate and less packet drop. The wireless client is disconnected if station quality is below threshold being configured.
5. In the **Radio Quality Threshold (1 - 50)** field, enter the threshold value for the radio quality. The default value is 20. Radio quality is the health index to track and assess the status of radio band utilization which varies between 1 and 50. The bigger index value means radio band utilization is lower with less packet drop. The radio TX power is lowered down if the radio quality is below threshold being configured.

Dynamic Channel Selection

Wireless Network Manager supports Global DCS with RRM in the cloud.

To activate Dynamic Channel Selection:

1. Navigate to **Policies > Policy Hierarchy**.
2. Select the AP Policy and the RRM.
3. In the **Dynamic Channel Selection** section, click the **DCS Mode Global** slider to activate or deactivate Dynamic Channel Selection.

To configure Dynamic Channel Selection:

1. Navigate to **Policies > Policy Hierarchy > RRM**.
2. Locate the **Dynamic Channel Selection** section.
3. From the **2.4GHz Radio DCS Scheme** list, select the mode you want to use:
    - **Safe Mode**: This is a conservative mode that switches to a better channel, but only when no client devices are connected. This is the default setting.
    - **Steady Mode**: This is a moderate mode that checks periodically for a better channel in the background.
    - **Swift Mode**: This is a more aggressive mode that switches to better channel as soon as a high level of noise or interference is detected on the current channel.
4. From the **5 GHz Radio DCS Scheme** list, select the mode you want to use:
    - **Safe Mode**: This is a conservative mode that switches to a better channel, but only when no client devices are connected. This is the default setting.
    - **Steady Mode**: This is a moderate mode that checks periodically for a better channel in the background.
    - **Swift Mode**: This is a more aggressive mode that switches to better channel as soon as a high level of noise or interference is detected on the current channel.

Client Load Balancing

The Client Load Balancing feature balances the number of connected clients among different APs within the same L2 layer network, using calculations based on the RSSI between Clients and APs.

This feature uses information about the station load of each AP(all APs are under L2 and connected with each other), and makes wireless station probes to steer the client to the best available AP, based on the STA's good web surfing precondition. This helps to steering the client to the best available AP, improving the performance and reducing the loss and latency for mission-critical applications.

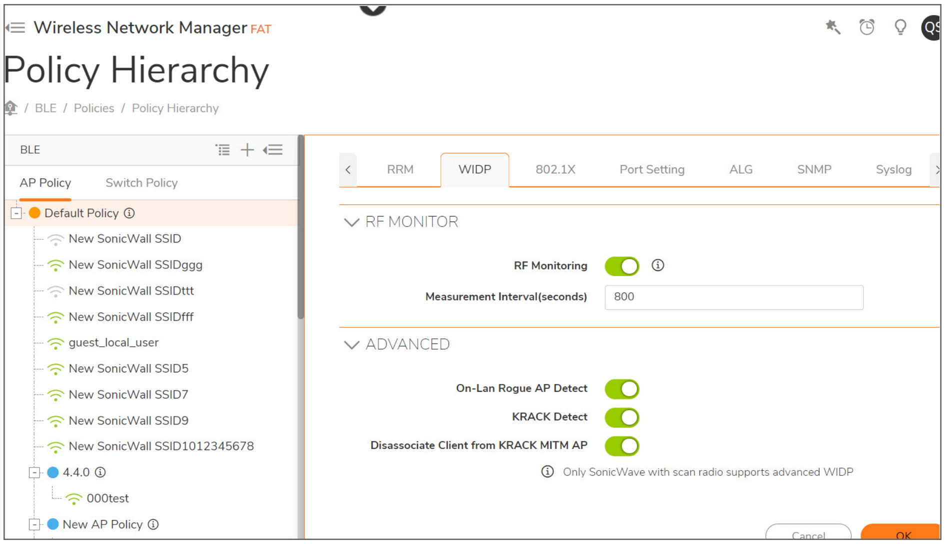
Enable the option **Client Load Balancing** if required, and click **OK** to save your selections.

WIDP

Wireless Network Manager supports Wireless Intrusion Detection and Prevention (WIDP). The WIDP support provides:

- On-LAN Rogue AP detect
- KRACK Detect
- Disassociate Client from KRACK MITM AP.

You can configure WIDP in the wireless cloud platform from the **Policies > Policy Hierarchy >** Select **WIDP** screen from **the AP Policy**.



RF Monitoring ●

Measurement Interval(seconds) 800

On-Lan Rogue AP Detect ●

KRACK Detect ●

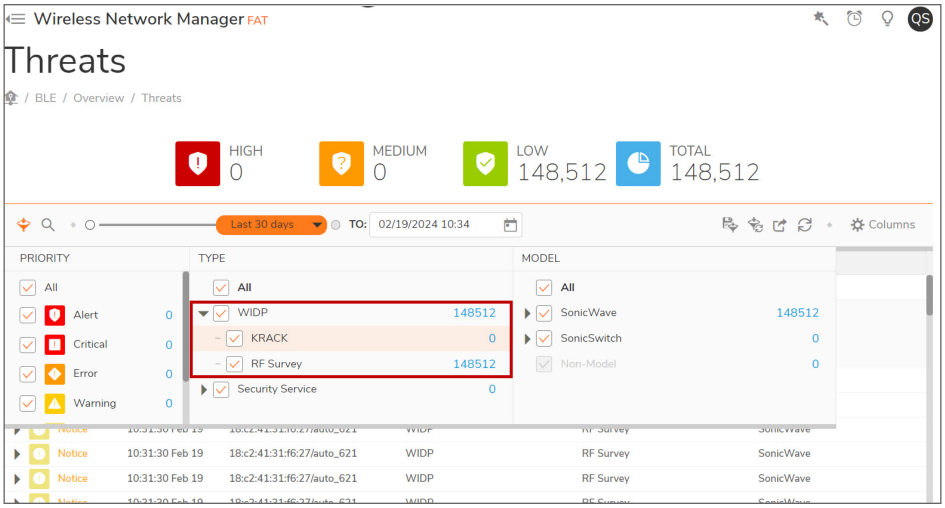
Disassociate Client from KRACK MITM AP ●

Only SonicWave with scan radio supports advanced WIDP

There are two sections on the screen, **RF Monitor** and **Advanced**. Click to activate specific functions for devices with this policy. Advanced functions only works for SonicWave access points with scan radio.

These screens show how the information from these features appear on the WNM management interface.

LAN ROGUE AP DETECTION AND ATTACK DETECTION AND PREVENTION



Wireless Network Manager FAT

Threats

/ BLE / Overview / Threats

HIGH 0 | MEDIUM 0 | LOW 148,512 | TOTAL 148,512

Last 30 days TO: 02/19/2024 10:34 Columns

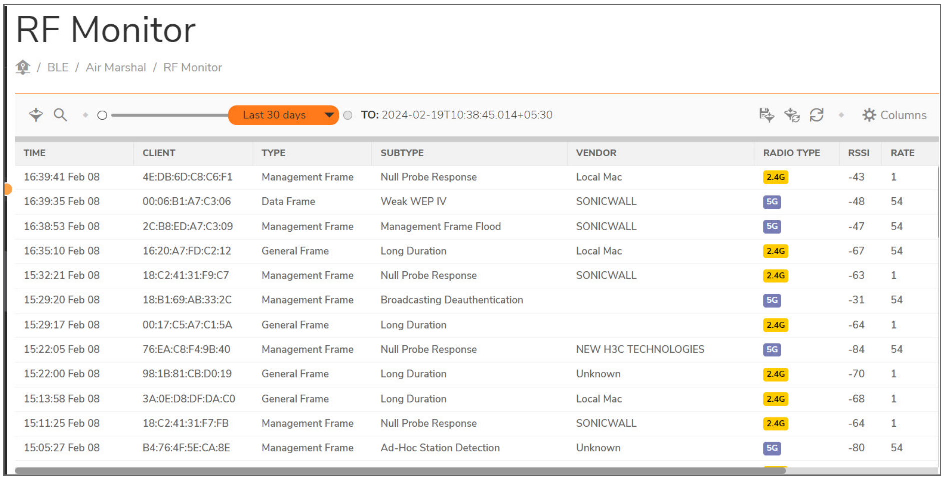
PRIORITY
- ☑ All
- ☑ Alert 0
- ☑ Critical 0
- ☑ Error 0
- ☑ Warning 0

TYPE
- ☑ All
- ☑ WIDP 148512
  - ☑ KRACK 0
  - ☑ RF Survey 148512
- ☑ Security Service 0

MODEL
- ☑ All
- ☑ SonicWave 148512
- ☑ SonicSwitch 0
- ☑ Non-Model 0

Notice	10:31:30 Feb 19	18:c2:41:31:f6:27/auto_621	WIDP	RF Survey	SonicWave
Notice	10:31:30 Feb 19	18:c2:41:31:f6:27/auto_621	WIDP	RF Survey	SonicWave

RF MONITOR



RF Monitor

/ BLE / Air Marshal / RF Monitor

Last 30 days TO: 2024-02-19T10:38:45.014+05:30 Columns

TIME	CLIENT	TYPE	SUBTYPE	VENDOR	RADIO TYPE	RSSI	RATE
16:39:41 Feb 08	4E:DB:6D:C8:C6:F1	Management Frame	Null Probe Response	Local Mac	2.4G	-43	1
16:39:35 Feb 08	00:06:B1:A7:C3:06	Data Frame	Weak WEP IV	SONICWALL	5G	-48	54
16:38:53 Feb 08	2C:B8:ED:A7:C3:09	Management Frame	Management Frame Flood	SONICWALL	5G	-47	54
16:35:10 Feb 08	16:20:A7:FD:C2:12	General Frame	Long Duration	Local Mac	2.4G	-67	54
15:32:21 Feb 08	18:C2:41:31:F9:C7	Management Frame	Null Probe Response	SONICWALL	2.4G	-63	1
15:29:20 Feb 08	18:B1:69:AB:33:2C	Management Frame	Broadcasting Deauthentication		5G	-31	54
15:29:17 Feb 08	00:17:C5:A7:C1:5A	General Frame	Long Duration		2.4G	-64	1
15:22:05 Feb 08	76:EA:C8:F4:9B:40	Management Frame	Null Probe Response	NEW H3C TECHNOLOGIES	5G	-84	54
15:22:00 Feb 08	98:1B:81:CB:D0:19	General Frame	Long Duration	Unknown	2.4G	-70	1
15:13:58 Feb 08	3A:0E:D8:DF:DA:C0	General Frame	Long Duration	Local Mac	2.4G	-68	1
15:11:25 Feb 08	18:C2:41:31:F7:FB	Management Frame	Null Probe Response	SONICWALL	2.4G	-64	1
15:05:27 Feb 08	B4:76:4F:5E:CA:8E	Management Frame	Ad-Hoc Station Detection	Unknown	5G	-80	54

802.1X

ⓘ | **NOTE:** 802.1X is currently only for SonicWave 224 models.

802.1X is an IEEE standard for media-level (Layer 2) access control, offering the capability to permit or deny network connectivity based on the identity of the end user or device.

802.1X enables port-based access control using authentication. An 802.1X-enabled port can be dynamically enabled or disabled based on the identity of the user or device that connects to it.

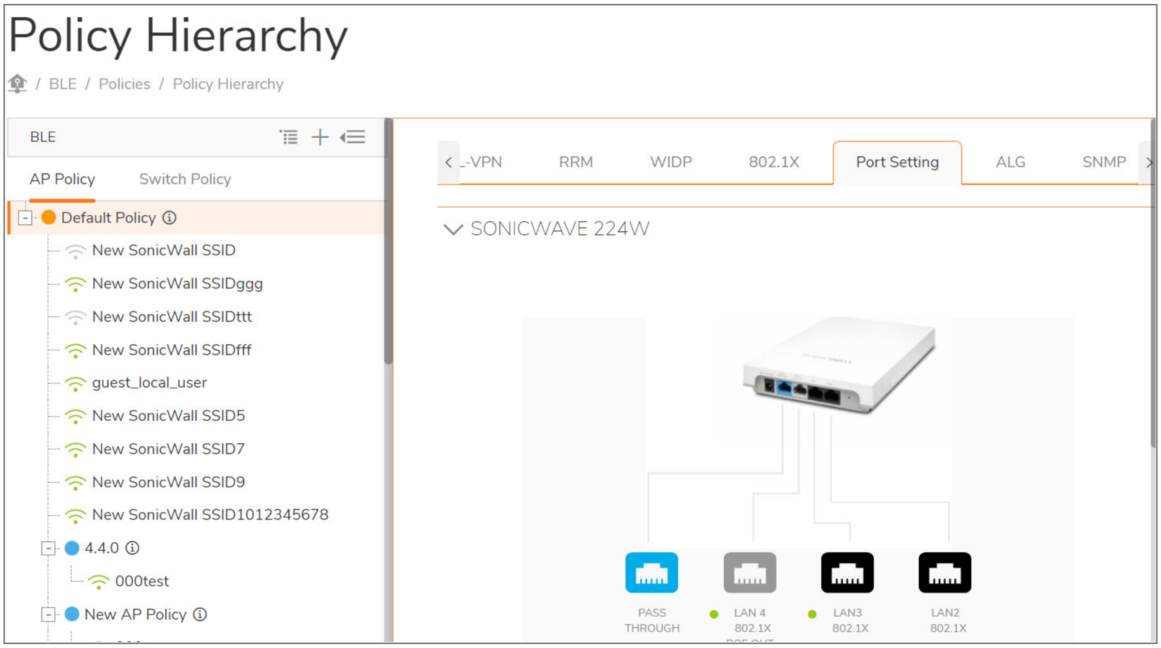
802.1X uses these protocols:

- Extensible Authentication Protocol (EAP): The message format and framework defined by RFC 4187 that provides a way for the supplicant and the authenticator to negotiate an authentication method (the EAP method).
- EAP method: Defines the authentication method; that is. the credential type and how it is submitted from the supplicant to the authentication server using the EAP framework. Common EAP methods used in 802.1X networks are EAP-Transport Layer Security (EAP-TLS) and Protected EAP-Microsoft Challenge Handshake Authentication Protocol version 2 (PEAP-MSCHAPv2).
- EAP over LAN (EAPoL): An encapsulation defined by 802.1X for the transport of the EAP from the supplicant to the switch over IEEE 802 networks. EAPoL is a Layer 2 protocol.
- RADIUS: The de facto standard for communication between the switch and the authentication server. The authenticator extracts the EAP payload from the Layer 2 EAPoL frame and encapsulates the payload inside a Layer 7 RADIUS packet.

To activate 802.1X support for a device:

1. Navigate to **Policies > Policy Hierarchy**.
2. Select the AP Policy.
3. Scroll to and click the **802.1X** tab.
4. Fill in the values needed for the **EAP Settings** and **RADIUS Server**, and **RADIUS Accounting Server**.
5. Click the **Port Setting** tab.
6. Select the device you want to configure.
7. In the **802,1X** column, activate the slider for the ports for which you want to use the 802.1X protocol.
8. Click **OK**.

Port Setting



For more information on Port Settings, refer Port Settings.

ALG

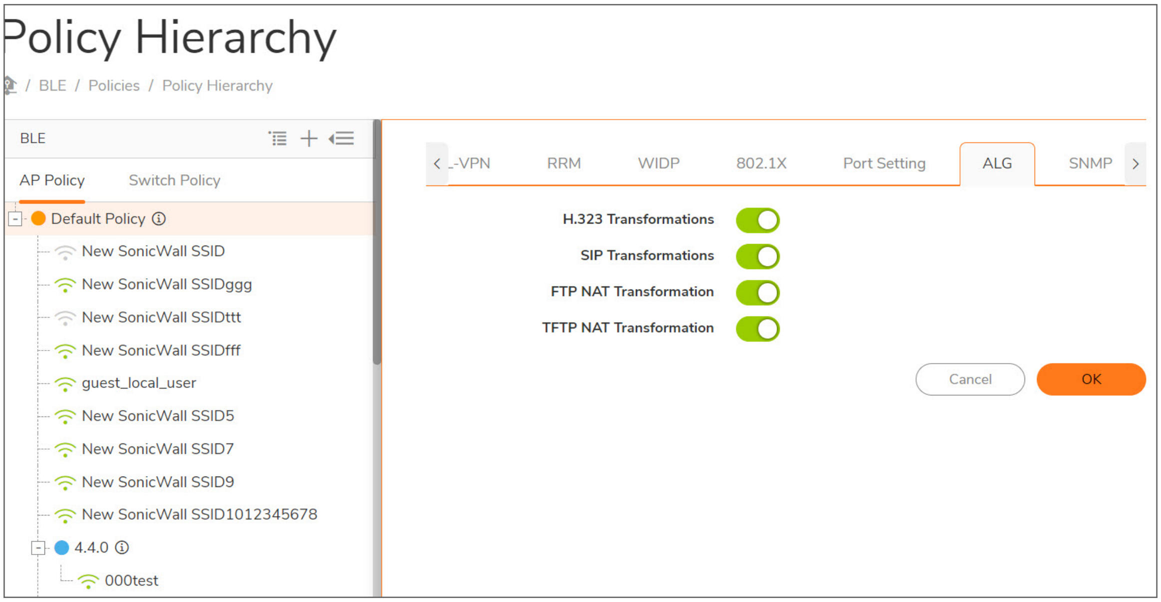
Wireless Network Manager 4.5.0 supports the SIP and H.323 VoIP protocols. These protocols are widely used by voice gateways, hardware terminals (such as IP phones), and software clients (like Netmeeting, Gnomemeeting and OpenPhone).

Wireless Network Manager supports these calling models:

- Internal Endpoint Call External Endpoint Though Gatekeeper/SIP-Server: The internal endpoint and the external endpoint are registered with a gatekeeper/SIP-server outside of the SonicWave wireless access points. The internal endpoint calls the external endpoint by calling its email address, user name or even a phone number.
- External Endpoint Call Internal Endpoint Though Gatekeeper/SIP-Server: The internal endpoint and the external endpoint are registered with a gatekeeper/SIP-server outside of the SonicWave wireless access points. The external endpoint calls the internal endpoint by calling its email address, user name or even a phone number.
- Internal Endpoint Call Another Internal Endpoint Though Gatekeeper/SIP-Server: The internal endpoint A and the internal endpoint B are registered with a gatekeeper/SIP-server outside of their SonicWave wireless access points. They call each other by calling the peer's email address, user name or even a phone number.

To activate a ALG protocol:

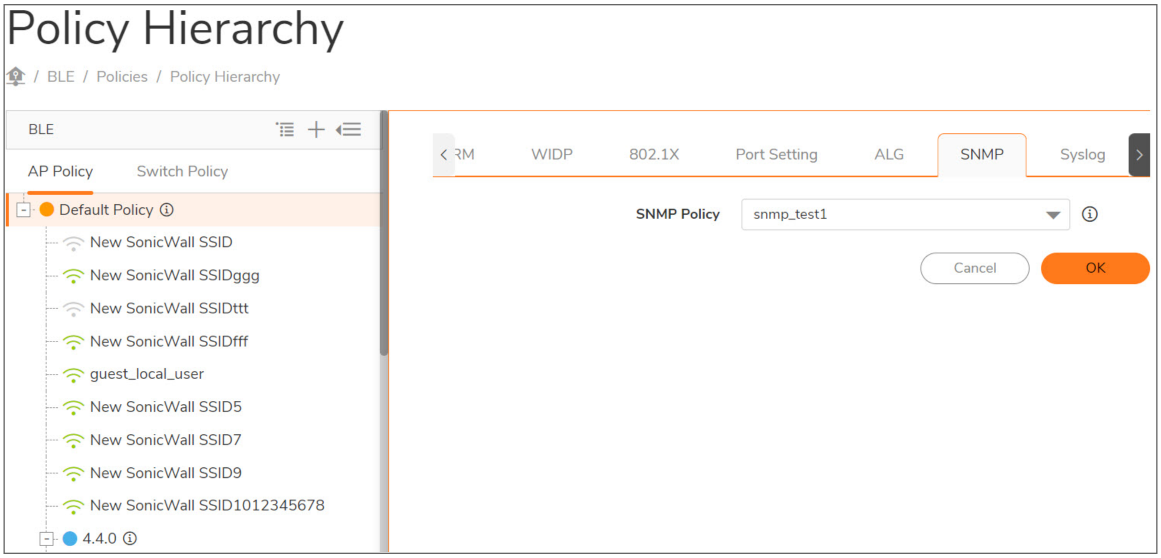
1. Navigate to **Policies > Policy Hierarchy**.
2. Select the AP Policy and click on the **ALG** tab.
3. Activate **H.323 Transformations** to use the H.323 protocol.
4. Activate **SIP Transformations**, **FTP NAT Transformation, TFTP NAT Transformation** to use the SIP protocol.
5. Click **OK**.



H.323 Transformations: on
SIP Transformations: on
FTP NAT Transformation: on
TFTP NAT Transformation: on

SNMP

Select the SNMP Policy to be applied to the policy hierarchy.



Policy Hierarchy

/ BLE / Policies / Policy Hierarchy

BLE

AP Policy | Switch Policy

- Default Policy ⓘ
  - New SonicWall SSID
  - New SonicWall SSIDggg
  - New SonicWall SSIDttt
  - New SonicWall SSIDfff
  - guest_local_user
  - New SonicWall SSID5
  - New SonicWall SSID7
  - New SonicWall SSID9
  - New SonicWall SSID1012345678
- 4.4.0 ⓘ

SNMP Policy: snmp_test1

For more information, refer to Managing SNMP Policies

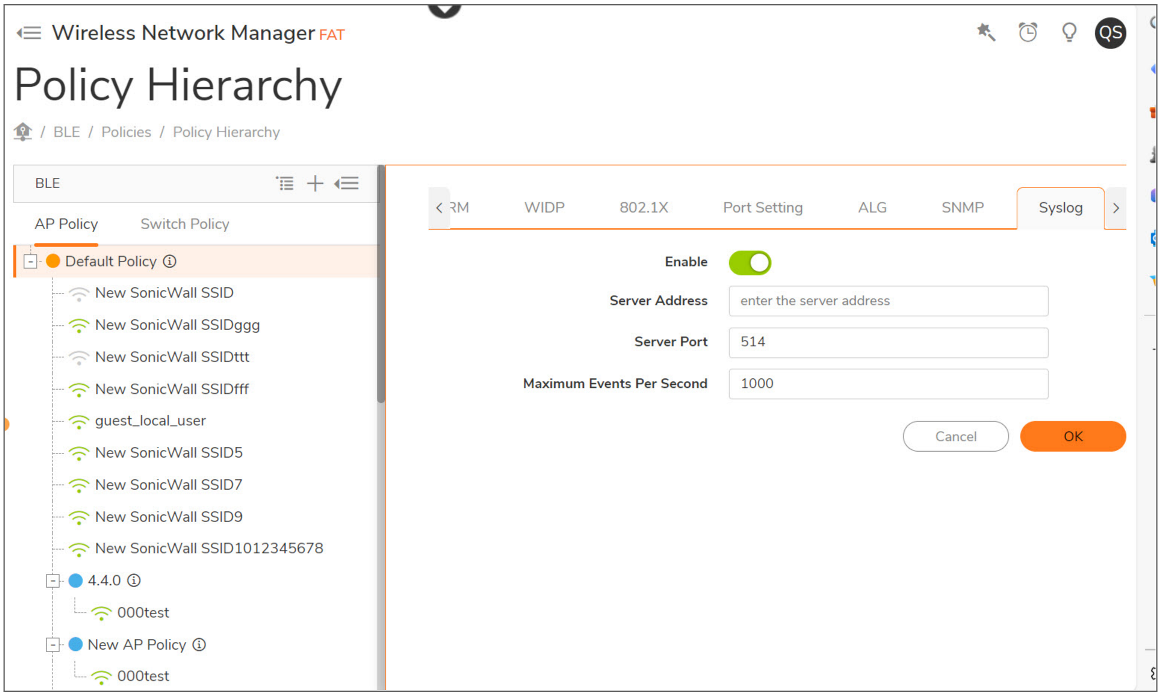
Syslog

Syslog is an IETF RFC 5425 standard protocol for computer logging and collection that is popular in Unix-like operating systems including servers, networking equipments, and IoT devices. The log messages generated by a device creates a record of events that occur on the operating system or application. The purpose of the message is to provide administrators with information regarding important events, health information and other normal or abnormal happenings that could prove useful when troubleshooting or working through a serurity-related issue.

Currently, access point can generate a variety of logs, such as WIDP, Secruty Services, network, etc. However, those logs can only send to WNM backend server to store. So this is an automated local access point for the customers to redirect all events and alerts for either an individual AP or all the APs to a local syslog server.

To activate Syslog for a device:

1. Navigate to **Policies > Policy Hierarchy**.
2. Select the AP Policy.
3. Scroll to and click the **Syslog** tab.
4. Select the **Enable** option to activate Syslog.
5. Specify the **Server Address**, **Server Port**, and **Maximum Events per Second**.
6. Click **OK** to save the changes.



Enable: ●

Server Address: enter the server address

Server Port: 514

Maximum Events Per Second: 1000

You can also enable Syslog from Settings > Notification Centre. For more information, refer to Notification Center.

Select a Switch Policy

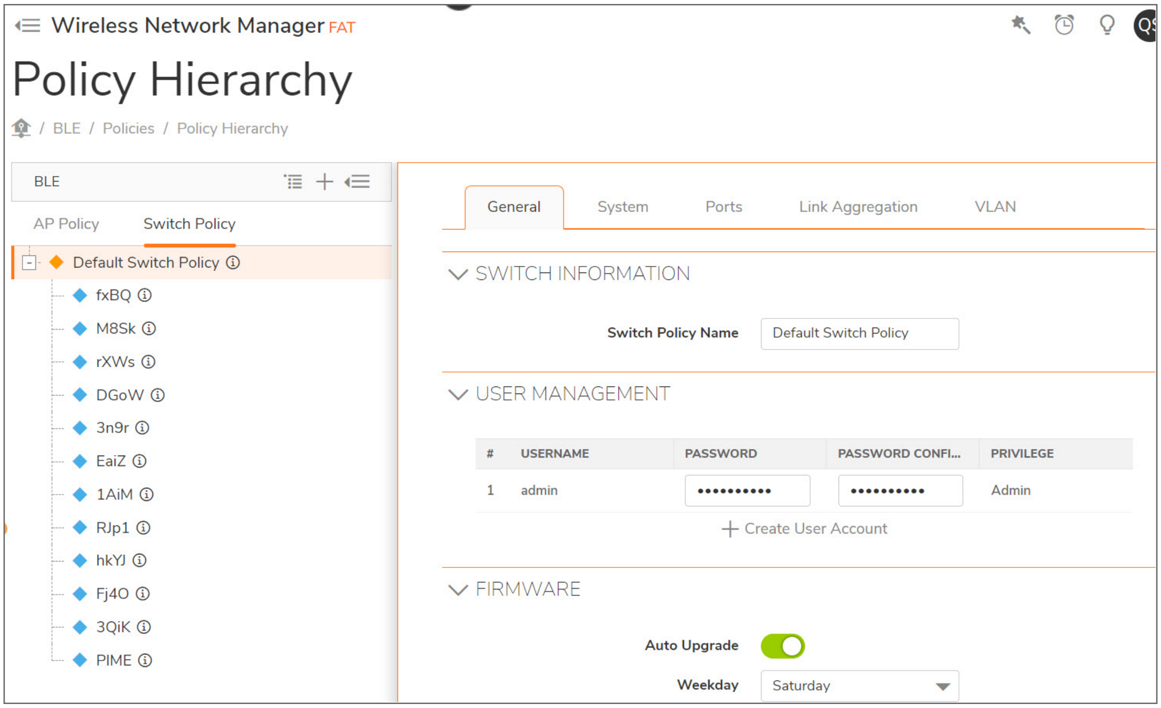
Switch policies offers a centralized and efficient approach to configuring multiple sections of your SonicWall Switch. These configurations are synced with Wireless Network Manager managed Switch and reflects on both the Switch and the Wireless Network Manager interface.

Selecting a Switch Policy in the hierarchy structure brings up these information fields where changes can be made:

- General
- System
- Ports
- Link Aggregation
- VLAN

General

From **Policy Hierarchy** window, click on the **Switch Policy** tab and the **General** tab is displayed by default for the Default Switch Policy.



Wireless Network Manager FAT

Policy Hierarchy

/ BLE / Policies / Policy Hierarchy

SWITCH INFORMATION

Switch Policy Name: Default Switch Policy

USER MANAGEMENT

#	USERNAME	PASSWORD	PASSWORD CONFI...	PRIVILEGE
1	admin	••••••••••	••••••••••	Admin

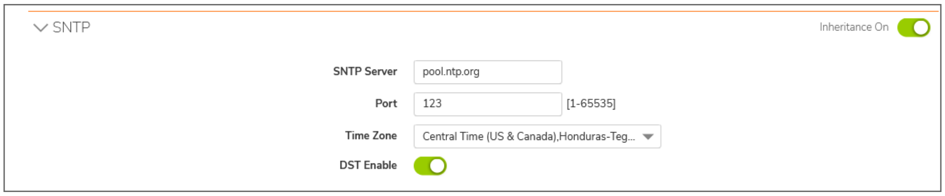
FIRMWARE

Auto Upgrade: On

Weekday: Saturday

In the **General** tab, specify the following information:

- **Switch Information** - Specify the **Switch Policy** Name.
- **User Management** - Specify or create user specifying the **User Name**, **Password**, and **Privilege** for the user.
- **Firmware** - Enable the **Auto Upgrade** option for auto firmware upgrade and specify the **Week Day**, **Time**, and **Retry Interval** details.
- **SNTP** - Specify the **SNTP Server**, **Port**, and **Time Zone.** Select the **DST Enable** option if the time-zone selected has DST.



SNTP

Inheritance On

SNTP Server: pool.ntp.org

Port: 123 [1-65535]

Time Zone: Central Time (US & Canada),Honduras-Teg...

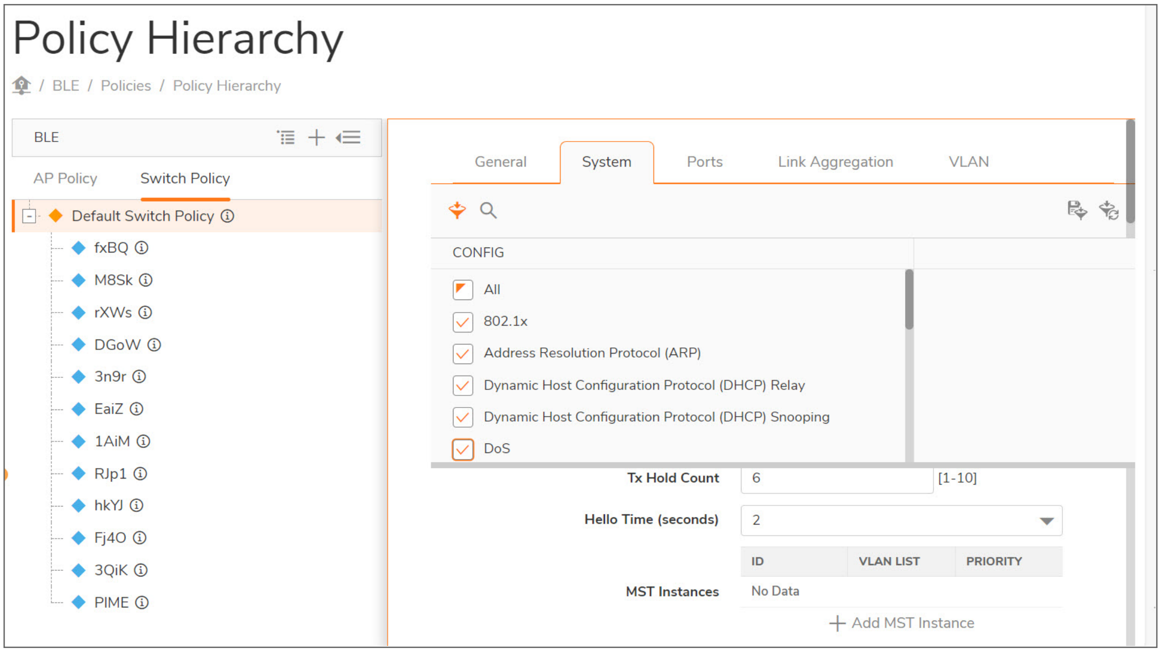
DST Enable: On

ⓘ **NOTE:** The **DST Enable** option helps users to automatically or manual adjust their system time to reflect the observance of Daylight Saving Time. If you select the **DST enable** toggle bar to active mode (green), the firmware upgrade and the port schedule options will be updated automatically according to this.

- **Management VLAN** - Specify the **VLAN ID** and **Configuration**. All management interfaces can be accessed only from VLAN.

System

The **System** tab provides you the options to edit the System information and also to filter the required configurations, save or reset the filters.



Tx Hold Count: 6 [1-10]

Hello Time (seconds): 2

MST Instances:

ID	VLAN LIST	PRIORITY
No Data		

ⓘ **NOTE:** You can also inherit each entities from the default policy enabling the toggle bar **Inherited from default policy** on the right side of the respective features.

This page helps you to configure the following information:

Topics:

- Spanning Tree Protocol
- Link Layer Discovery Protocol
- Voice VLAN
- Quality of Service (QoS)
- Internet Group Management Protocol (IGMP) Snooping
- Dynamic Host Configuration Protocol (DHCP) Snooping
- Dynamic Host Configuration Protocol (DHCP) Relay
- Loopback Detection
- Jumbo Frames
- Multicast Filtering
- 802.1X
- Static Route IPV4
- DoS
- Radius Server
- Mirror Settings
- Address Resolution Protocol
- Static MAC Address Table
- SNMP

Spanning Tree Protocol

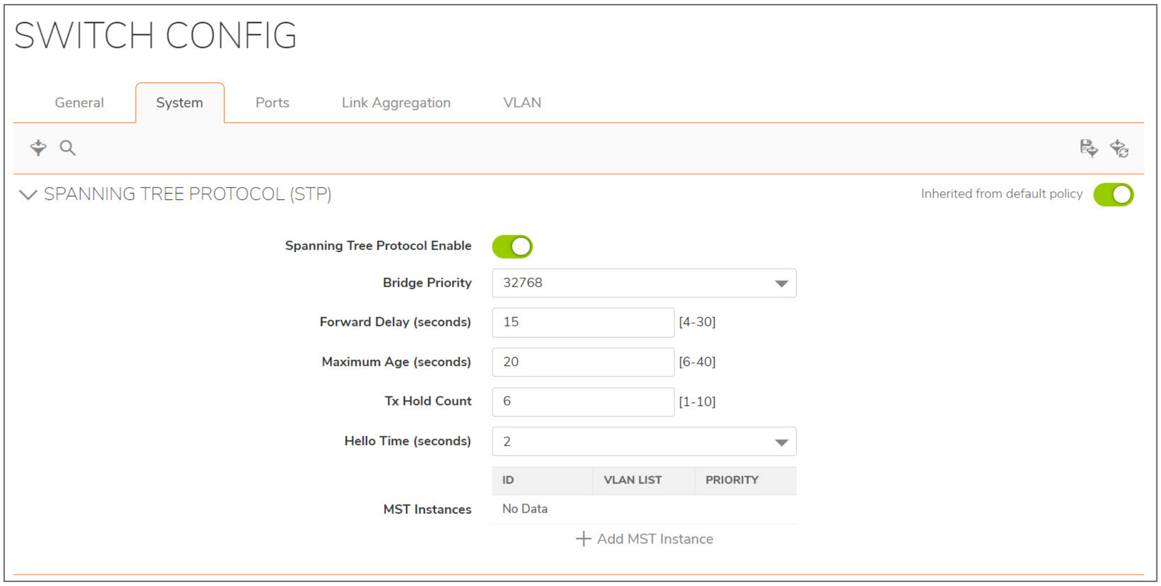
The Spanning Tree Protocol (STP) can be used to detect and disable network loops, and to provide backup links between Switches. This allows the Switch to interact with other bridging devices in your network to ensure that only one route exists between any two stations on the network, and provide backup links which automatically take over when a primary link goes down.

STP provides a tree topology for the Switch. There are different types of Spanning tree versions, supported, including Spanning Tree Protocol (STP) IEEE802.1D, Multiple Spanning Tree Protocol (MSTP) IEEE802.1w, and Rapid Spanning Tree Protocol (RSTP) IEEE802.1s. Please note that only one spanning tree can be active on the Switch at a time.

Spanning Tree Protocol (STP) is a Layer 2 protocol that runs on Switches. Spanning Tree Protocol (STP) allows you to ensure that you do not create loops when you have redundant paths in the network. STP provides a single active path between two devices on a network in order to prevents loops from being formed when the Switch is interconnected via multiple paths.

STP uses a distributed algorithm to select a bridging device that serves as the root for the spanning tree network. It does this by selecting a root port on each bridging device to incur the lowest path cost when forwarding a packet from that device to the root device. It then selects a designated bridging device from each LAN which incurs the lowest path cost when forwarding a packet from that LAN to the root device. Next, all ports connected to designated bridging devices are assigned as designated ports. After determining the lowest cost spanning tree, it enables all root ports and designated ports, disabling all other ports. Network packets are therefore only forwarded between root ports and designated ports, eliminating any possible network loops. STP provides a single active path between two devices on a network in order to prevent loops from being formed when the Switch is interconnected via multiple paths.

Once a stable network topology has been established, all bridges listen for Hello Bridge Protocol Data Units (BPDUs) transmitted from the Root Bridge of the Spanning Tree. If a bridge does not receive a Hello BPDU after a predefined interval (known as the Maximum Age), the bridge will assume that the link to the Root Bridge is down and unavailable. This bridge then initiates negotiations with other bridges to reconfigure the network to reestablish a valid network topology.



SWITCH CONFIG

Spanning Tree Protocol Enable	●
Bridge Priority	32768
Forward Delay (seconds)	15 [4-30]
Maximum Age (seconds)	20 [6-40]
Tx Hold Count	6 [1-10]
Hello Time (seconds)	2

MST Instances

ID	VLAN LIST	PRIORITY
No Data		

To activate the Spanning Tree Protocol options for a device:

1. Navigate to **Policies > Policy Hierarchy > Switch Policy**.
2. Select the **System** tab.
3. Enable the toggle bar, **Spanning Tree Protocol Enable** under the Spanning Tree Protocol section.
4. Select the **Bridge Priority**. When Switches or bridges are running STP, each is assigned a priority. After exchanging BPDUs, the Switch with the lowest priority value becomes the root bridge. The default value is: 32768.
5. Specify the **Forward Delay** in seconds. The minimum value is 4 and the maximum value is 30.
6. Specify the **Maximum Age** in seconds. The minimum value is 6 and the maximum value is 40.
7. Specify the **Tx Hold Count**. The minimum value is 1 and the maximum value is 10.
8. Choose the **Hello Time** in seconds from the drop-down. This is the amount of time between each bridge protocol data unit sent on a port.The options are one or two.
9. Specify the **MST** details. The VLAN ID number range is from 1 to 4094. Choose the **Priority** from the drop-down. When Switches or bridges are running STP, each is assigned a priority. After exchanging BPDUs, the Switch with the lowest priority value becomes the root bridge. The default value is: 32768. The range is

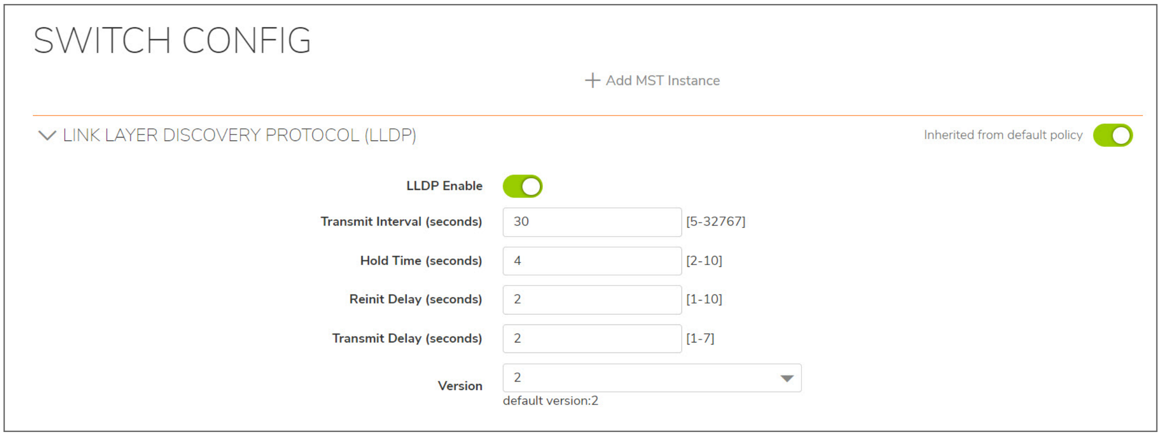
from 0-61440. The bridge priority is a multiple of 4096.

You can add more MST instances clicking on the add icon.

Link Layer Discovery Protocol

Link Layer Discovery Protocol (LLDP) is the IEEE 802.1AB standard for Switches to advertise their identity, major capabilities, and neighbors on the 802 LAN. LLDP allows users to views the discovered information to identify system topology and detect faulty configurations on the LAN. LLDP is essentially a neighbor discovery protocol that uses Ethernet connectivity to advertise information to devices on the same LAN and store information about the network. The information transmitted in LLDP advertisements flow in one direction only; from one device to its neighbors. This information allows the device to quickly identify a variety of other devices, resulting in a LAN that interoperates smoothly and efficiently.

LLDP transmits information as packets called LLDP Data Units (LLDPDUs). A single LLDP Protocol Data Unit (LLDP PDU) is transmitted within a single 802.3 Ethernet frame. A basic LLDPDU consists of a set of Type-Length-Value elements (TLV), each of which contains information about the device. A single LLDPDU contains multiple TLVs. TLVs are short information elements that communicate complex data. Each TLV advertises a single type of information.



Inherited from default policy: on

LLDP Enable: on

Transmit Interval (seconds): 30 [5-32767]

Hold Time (seconds): 4 [2-10]

Reinit Delay (seconds): 2 [1-10]

Transmit Delay (seconds): 2 [1-7]

Version: 2
default version:2

To activate the Link Layer Discovery Protocol:

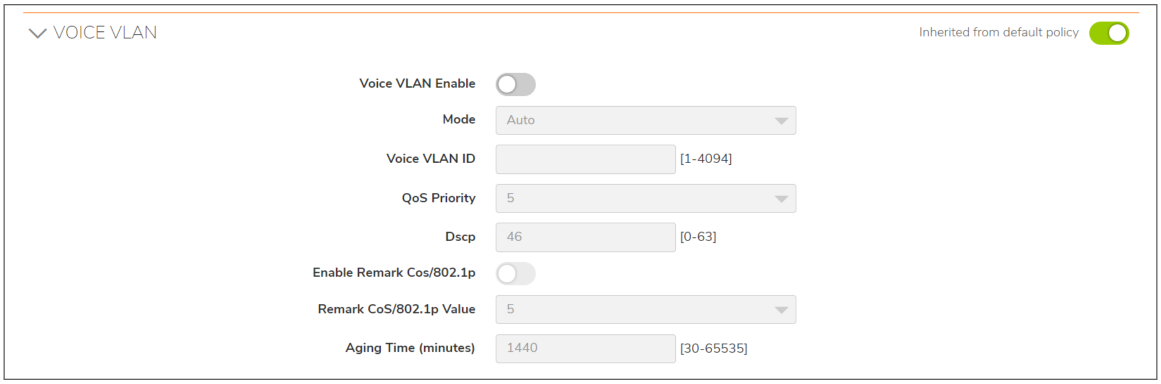
1. Navigate to **Policies > Policy Hierarchy > Switch Policy**.
2. Select the **System** tab and scroll down to the Link Layer Discovery Protocol section.
3. Enable the toggle bar, **LLDP Enable**.
4. Specify the **Transmit Interval** in seconds. the interval at which LLDP advertisement updates are sent. The default value is 30. The range is from 5 to 32767.
5. Specify the **Hold** time in seconds. This is the time that LLDP packets are held before packets are discarded and measured in multiples of the Advertised Interval. The default is 4. The range is from 2-10.
6. Specify the **Reinit Delay** in seconds. Reinitialization delay is the amount of time of delay before reinitializing LLDP. The default is 2. The range is from 1-10.
7. Specify the **Transmit** Delay in seconds. This is the time that passes between successive LLDP frame

transmissions. The default is 2 seconds. The range is 1-7 seconds.

8. Select the **Version** from the drop-down. The default version is 2.

Voice VLAN

You can enhance your Voice over IP (VoIP) service by configuring ports to carry IP voice traffic from IP phones on a specific VLAN. Voice VLAN provides QoS to VoIP, ensuring that the quality of the call does not deteriorate if the IP traffic is received erratically or unevenly.



Inherited from default policy ●

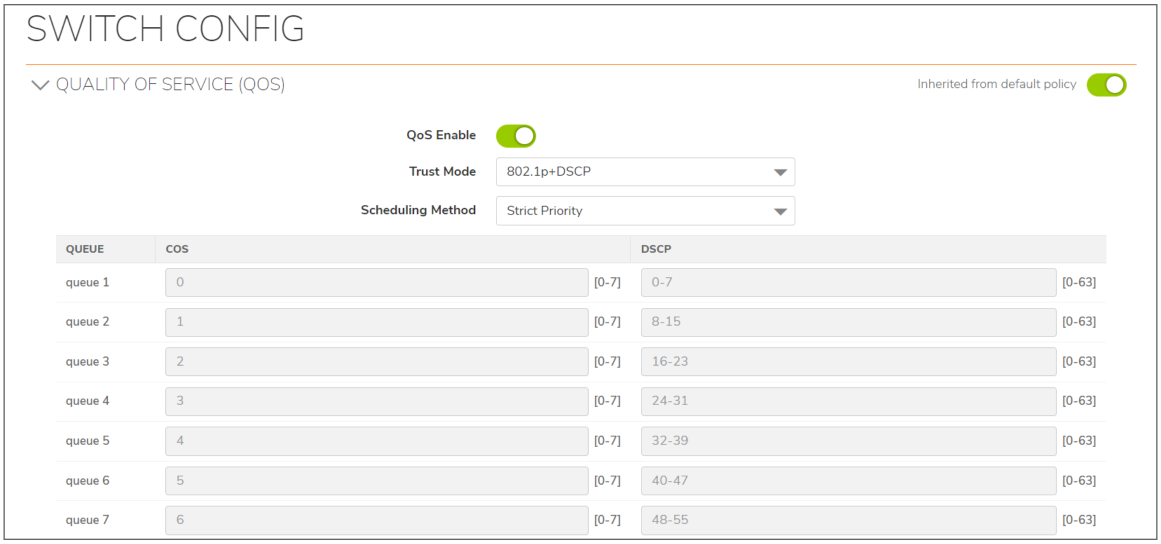
Voice VLAN Enable	○	
Mode	Auto	
Voice VLAN ID		[1-4094]
QoS Priority	5	
Dscp	46	[0-63]
Enable Remark Cos/802.1p	○	
Remark CoS/802.1p Value	5	
Aging Time (minutes)	1440	[30-65535]

To activate Voice VLAN:

1. Navigate to **Policies > Policy Hierarchy > Switch Policy**.
2. Select the **System** tab and scroll down to the Voice VLAN section.
3. Enable the toggle bar, **Voice VLAN**.
4. Select the **Mode**. The options are Auto and OUI.
5. Specify the **Voice VLAN ID**. The range is from 1 to 4094. Only one Voice VLAN is supported on the Switch.
6. Select the **QoS Priority**. Options are from 1 to 7. Priority Tagging places a priority tag in a specified frame placing it in a priority queue once received and enabling it to be prioritized ahead of other frames.
7. Specify the **DSCP**. Differentiated Services Code Point (DSCP) defines a value from 0 to 63 that maps to a certain traffic classification. The range is from 0-63.
8. If you select OUI mode, you can select the **Enable Remark Cos/802.1p** option. This defines a service priority for traffic on the Voice VLAN. The priority of any received VoIP packet is overwritten with the new priority when the Voice VLAN feature is active on a port.
9. Specify the Remark Cos/802.1p values. The range is from 0 to 7.
10. Specify the **Aging Time** in minutes. The range is from 30 to 65535.
11. Specify the **OUI Address** and **Description**.

Quality of Service (QoS)

From here, you can configure the QoS port settings for the Switch. Select a port you wish to set and choose a CoS value from the drop-down box.



SWITCH CONFIG

QUALITY OF SERVICE (QOS)

Inherited from default policy

QoS Enable

Trust Mode: 802.1p+DSCP

Scheduling Method: Strict Priority

QUEUE	COS		DSCP	
queue 1	0	[0-7]	0-7	[0-63]
queue 2	1	[0-7]	8-15	[0-63]
queue 3	2	[0-7]	16-23	[0-63]
queue 4	3	[0-7]	24-31	[0-63]
queue 5	4	[0-7]	32-39	[0-63]
queue 6	5	[0-7]	40-47	[0-63]
queue 7	6	[0-7]	48-55	[0-63]

To activate QoS:

1. Navigate to **Policies > Policy Hierarchy > Switch Policy**.
2. Select the **System** tab and scroll down to the QoS section.
3. Enable the toggle bar, **QoS Enable**.
4. Select the **Trust Mode**. The options are 802.1p, DSCP or both together. Trust mode helps you to enable to trust any CoS packet marking at ingress.
5. Select the **Scheduling Method**. Options are Strict Priority and WRR.
6. If you select WRR scheduling method, specify the class of service priority value - **COS** (the range is from 0 to 7), DSCP (the range is from 0 to 63), WRR (the range is from 0-128).

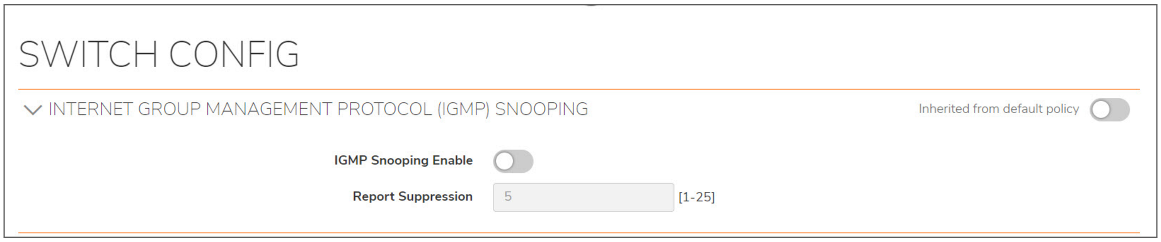
Internet Group Management Protocol (IGMP) Snooping

Internet Group Management Protocol (IGMP) Snooping allows a Switch to forward multicast traffic intelligently. Multicasting is used to support real-time applications such as videoconferencing or streaming audio. A multicast server does not have to establish a separate connection with each client. It merely broadcasts its service to the network, and any host that wishes to receive the multicast register with their local multicast Switch.

A multicast group is a group of end nodes that want to receive multicast packets from a multicast application. After joining a multicast group, a host node must continue to periodically issue reports to remain a member. Any multicast packets belonging to that multicast group are then forwarded by the Switch from the port.

A Switch supporting IGMP Snooping can passively snoop on IGMP Query, Report, and Leave packets transferred between IP Multicast Switches and IP Multicast hosts to determine the IP Multicast group membership. IGMP Snooping checks IGMP packets passing through the network and configures Multicasting accordingly. Based on the IGMP query and report messages, the Switch forwards traffic only to the ports that request the multicast traffic.

It enables the Switch to forward packets of multicast groups to those ports that have validated host nodes. The Switch can also limit flooding of traffic to IGMP designated ports. This improves network performance by restricting the multicast packets only to Switch ports where host nodes are located. IGMP Snooping significantly reduces overall Multicast traffic passing through your Switch. Without IGMP Snooping, Multicast traffic is treated in the same manner as a Broadcast transmission, which forwards packets to all ports on the network.



SWITCH CONFIG

INTERNET GROUP MANAGEMENT PROTOCOL (IGMP) SNOOPING

Inherited from default policy

IGMP Snooping Enable

Report Suppression 5 [1-25]

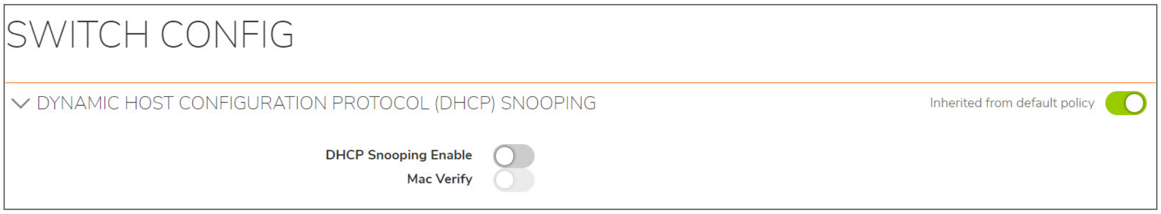
To activate the IGMP Snooping:

1. Navigate to **Policies > Policy Hierarchy > Switch Policy**.
2. Select the **System** tab and scroll down to the IGMP Snooping section.
3. Enable the toggle bar, **IGMP Snooping Enable**.
4. Specify the **Report Suppression.** The range is from 1 to 25.

Dynamic Host Configuration Protocol (DHCP) Snooping

DHCP snooping is a layer 2 security technology built into the operating system of a capable network switch that drops DHCP traffic determined to be unacceptable. The fundamental use case for DHCP snooping is to prevent unauthorized (rogue) DHCP servers offering IP addresses to DHCP clients.

Dynamic Host Configuration Protocol (DHCP) assigns dynamic IP addresses to devices on a network. DHCP ensures that network devices have a different IP address every time the device connects to the network.



SWITCH CONFIG

DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP) SNOOPING

Inherited from default policy

DHCP Snooping Enable

Mac Verify

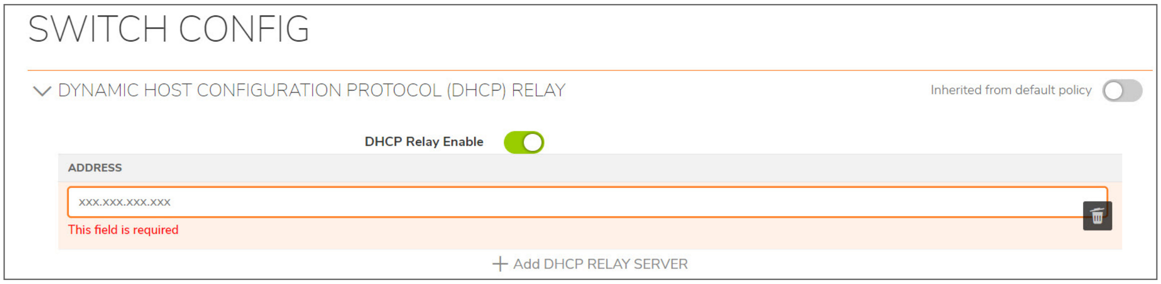
To activate the DHCP Snooping:

1. Navigate to **Policies > Policy Hierarchy > Switch Policy**.
2. Select the **System** tab and scroll down to the IGMP Snooping section.
3. Enable the toggle bar, **DHCP Snooping Enable**.

4. Enable the toggle bar Mac Verify. If the device receives a packet on an untrusted interface and the source MAC address and the DHCP client hardware address do not match, address verification causes the device to drop the packet, if you enable this option.

Dynamic Host Configuration Protocol (DHCP) Relay

DHCP Relay is an option used to have local hosts communicate to a DHCP server in another network and switch works as a relay device.


SWITCH CONFIG

DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP) RELAY

Inherited from default policy

DHCP Relay Enable

ADDRESS

xxx.xxx.xxx.xxx

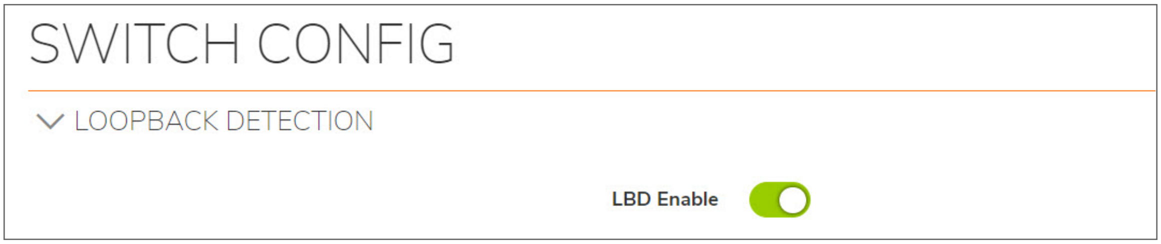
This field is required

To activate the DHCP Relay:

1. Navigate to **Policies > Policy Hierarchy > Switch Policy**.
2. Select the **System** tab and scroll down to the DHCP Relay section.
3. Enable the toggle bar, **DHCP Relay Enable**.
4. Click on **Add DHCP Relay Server**.
5. Specify the IP Address of the **DHCP Relay Server**.
6. Enable the toggle bar Mac Verify. If the device receives a packet on an untrusted interface and the source MAC address and the DHCP client hardware address do not match, address verification causes the device to drop the packet, if you enable this option.

Loopback Detection

Loopback Detection (LBD) is a feature on the switch that provides protection against loops by transmitting loop protocol packets out of ports where loop protection has been enabled. When the switch sends out a loop protocol packet and then receives the same packet, it shuts down the port that received the packet. LBD operates independently of Spanning Tree Protocol (STP). After a loop is discovered, the port that received the loops is placed in the Shut Down state. A trap is sent and the event is logged.


SWITCH CONFIG

LOOPBACK DETECTION

LBD Enable

To activate the Loopback Detection:

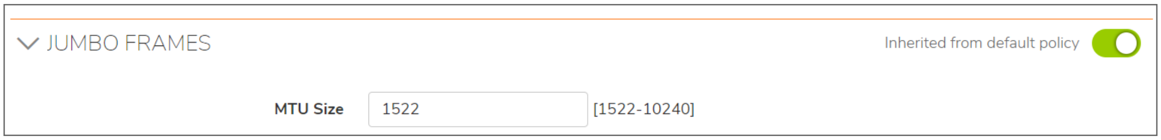
1. Navigate to **Policies > Policy Hierarchy > Switch Policy**.
2. Select the **System** tab and scroll down to the Loopback Detection section.
3. Enable the toggle bar, **Loopback Detection**.

Jumbo Frames

Ethernet has used the 1500 byte frame size since its inception. Jumbo frames are network-layer PDUs that have a size much larger than the typical 1500 byte Ethernet Maximum Transmission Unit (MTU) size. Jumbo frames extend Ethernet to 10240 bytes, making them large enough to carry an 8 KB application datagram plus packet header overhead. If you intend to leave the local area network at high speeds, the dynamics of TCP will require you to use large frame sizes.

The SonicWall Layer 2 Switch supports a Jumbo Frame size of up to 10240 bytes. Jumbo frames need to be configured to work on the ingress and egress port of each device along the end-to-end transmission path.

Furthermore, all devices in the network must also be consistent on the maximum Jumbo Frame size, so it is important to do a thorough investigation of all your devices in the communication paths to validate their settings. Enter the size of jumbo frame. The range is from 1522- 10240 bytes.



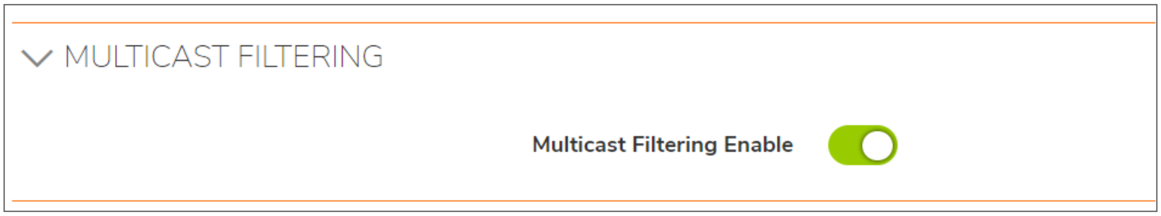
MTU Size 1522 [1522-10240]

To activate the Jumbo Frames:

1. Navigate to **Policies > Policy Hierarchy > Switch Policy**.
2. Select the **System** tab and scroll down to the Jumbo Frames section.
3. Specify the size of the Jumbo Frame.

Multicast Filtering

Multicast is a form of communication that allows multiple transmissions of multimedia and streaming data to specific recipients at the same time. Enabling the Multicast Filtering feature on your switch lets you sort out selective multiple transmissions for devices connected to the network.



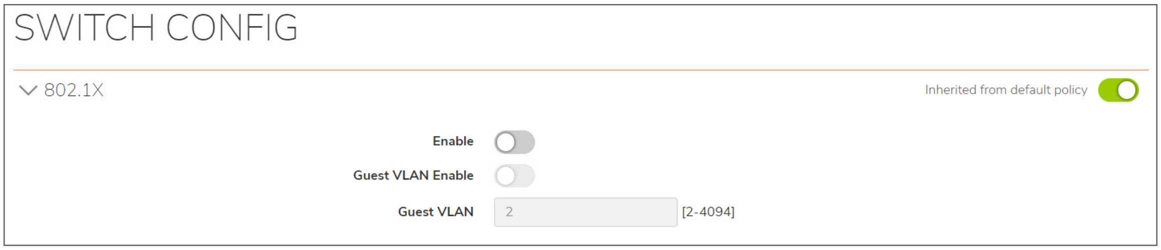
Multicast Filtering Enable

To activate Multicast Filtering:

1. Navigate to **Policies > Policy Hierarchy > Switch Policy**.
2. Select the **System** tab and scroll down to the Multicast Filtering section.
3. Select the toggle bar **Multicast Filtering Enable**.

802.1X

You can configure the port settings as they relate to 802.1X. You can also choose to Enable or Disable the VLAN ID.



SWITCH CONFIG

802.1X

Inherited from default policy

Enable

Guest VLAN Enable

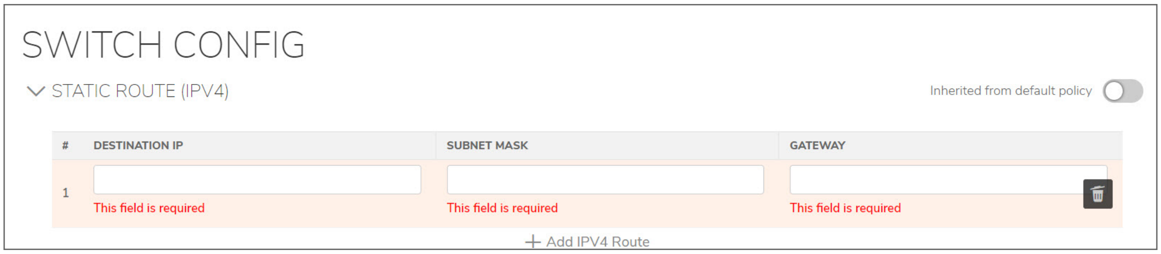
Guest VLAN 2 [2-4094]

To activate the 802.1X:

1. Navigate to **Policies > Policy Hierarchy > Switch Policy**.
2. Select the **System** tab and scroll down to the 802.1X section.
3. Enable the toggle bar, **Enable**.
4. Enable the toggle bar **Guest VLAN Enable**.
5. Specify the **Guest VLAN** number. The range is from 2 to 4094.

Static Route IPV4

Static routes are manually added to a routing table through direct configuration. Using a static route, a switch can learn about a route to a remote network that is not directly attached to one of its interfaces.



SWITCH CONFIG

STATIC ROUTE (IPV4)

Inherited from default policy

#	DESTINATION IP	SUBNET MASK	GATEWAY
1	This field is required	This field is required	This field is required

+ Add IPV4 Route

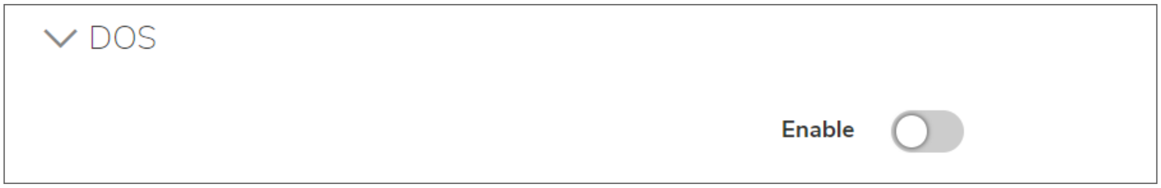
To activate Static Route IPV4:

1. Navigate to **Policies > Policy Hierarchy > Switch Policy**.
2. Select the **System** tab and scroll down to the Static Route (IPV4) section.
3. Click on **Add IPV4 Route**.

4. Specify the **Destination IP**, the IP address of the destination host/network.
5. Specify the **Subnet Mask**, the network mask for the particular subnet.
6. Specify the **Gateway**, the next hop IP address for the traffic.

DoS

DoS (Denial of Service) is used for classifying and blocking specific types of DoS attacks. From here, you can configure the Switch to monitor and block different types of attacks:



DOS

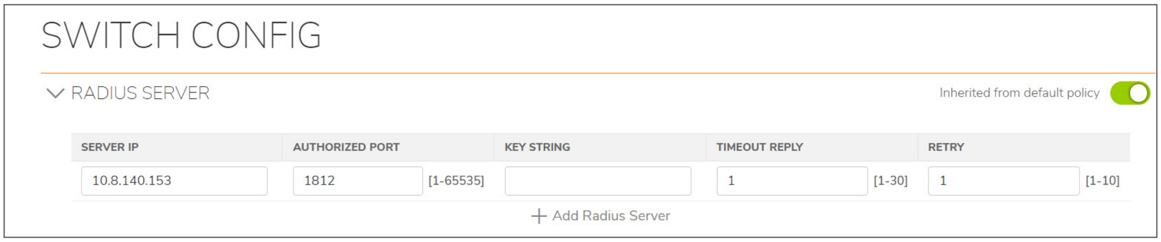
Enable ○

To activate DoS:

1. Navigate to **Policies > Policy Hierarchy > Switch Policy**.
2. Select the **System** tab and scroll down to the DoS section.
3. Enable the toggle bar to activate DoS.

Radius Server

RADIUS (Remote Authorization Dial-In User Service) servers provide security for networks. Radius servers provide authentication and authorization for networks. The Radius server maintains a user database, which contains authentication information. The Switch passes information to the configured Radius server, which can authenticate a user name and password before authorizing use of the network.



SWITCH CONFIG

RADIUS SERVER

Inherited from default policy ●

SERVER IP	AUTHORIZED PORT	KEY STRING	TIMEOUT REPLY	RETRY
10.8.140.153	1812 [1-65535]		1 [1-30]	1 [1-10]

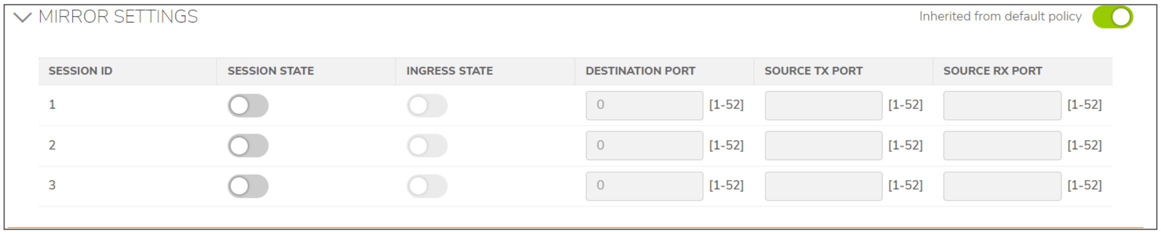
+ Add Radius Server

To activate Radius Server:

1. Navigate to **Policies > Policy Hierarchy > Switch Policy**.
2. Select the **System** tab and scroll down to the Radius Server section.
3. Click on **Add Radius Server**.
4. Specify the **Server IP**, the radius server IP address.
5. Specify the **Authorized Port** number. Enter any port number between 1 to 65535.

6. Specify the **Key String**, used for encrypting all Radius communication between the device and the Radius server.
7. Specify the **Timeout Reply**. Enter the amount of time the device waits for an answer from the Radius Server before switching to the next server. Enter any value between 1 to 30.
8. Specify the **Retry** option. Enter the number of transmitted requests sent to the Radius server before a failure occurs. Enter any value between 1 to 10.

Mirror Settings



MIRROR SETTINGS

Inherited from default policy

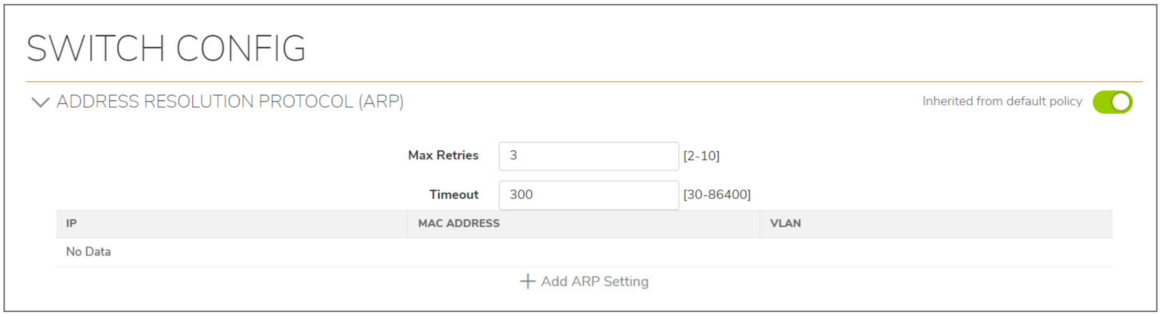
SESSION ID	SESSION STATE	INGRESS STATE	DESTINATION PORT	SOURCE TX PORT	SOURCE RX PORT
1	○	○	0 [1-52]	[1-52]	[1-52]
2	○	○	0 [1-52]	[1-52]	[1-52]
3	○	○	0 [1-52]	[1-52]	[1-52]

To activate Mirror Setting:

1. Navigate to **Policies > Policy Hierarchy > Switch Policy**.
2. Select the **System** tab and scroll down to the Mirror Settings section.
3. Enable the **Session State** toggle bar.
4. Enable the **Ingress State** toggle bar.
5. Specify the **Destination Port**. The range is from 1 to 52.
6. Specify the **Source TXPort**. The range is from 1 to 52.
7. Specify the **Source RXPort**. The range is from 1 to 52

Address Resolution Protocol

Address Resolution Protocol (ARP) is a protocol that maps an Internet Protocol address to a MAC address that is recognized in the local network. ARP is used to keep track of all devices that are directly connected IP subnets of the Switch. The Switch maintains an ARP table which is made of mapped IP addresses and MAC addresses. When a packet needs to be routed to a certain device, the Switch looks up the IP address of the device in its ARP table to obtain the MAC address of the destination device.



SWITCH CONFIG

ADDRESS RESOLUTION PROTOCOL (ARP)

Inherited from default policy

Max Retries: 3 [2-10]

Timeout: 300 [30-86400]

IP	MAC ADDRESS	VLAN
No Data		

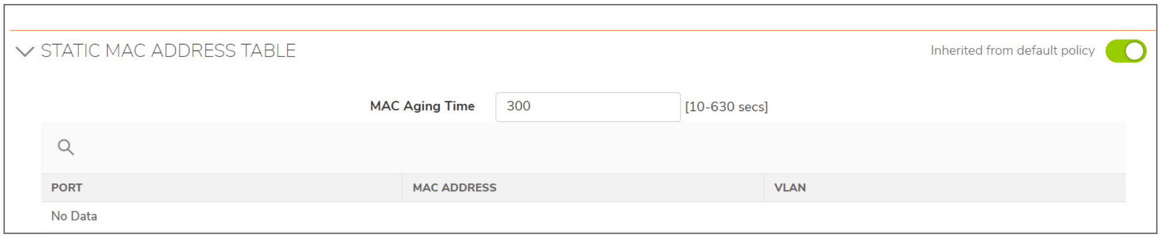
To activate Address Resolution Protocol:

1. Navigate to **Policies > Policy Hierarchy > Switch Policy**.
2. Select the **System** tab and scroll down to the Address Resolution Protocol section.
3. Specify the **Max Retries**. The Max Retries count specifies the maximum number of attempts made before removing an ARP entry. The default value is 3 and the range of the Max Retries count is 2 to 10
4. Specify the ARP **Timeout** in the field. The default value is 300 seconds. After the time out period, the ARP entries are removed from the table.
5. In the ARP Setting section, Specify the **IP**.
6. Specify the **Mac Address**.
7. Specify the **VLAN** option.

   You can add more ARP settings clicking on the add icon.

Static MAC Address Table

The address table lists the destination MAC address, the associated VLAN ID, and port number associated with the address. When you specify a Static MAC address, you are set the MAC address to a VLAN and a port; thus it makes an entry into its forwarding table. These entries are then used to forward packets through the Switch. Static MAC addresses along with the Switch's port security allow only devices in the MAC address table on a port to access the Switch.



MAC Aging Time 300 [10-630 secs]

PORT	MAC ADDRESS	VLAN
No Data		

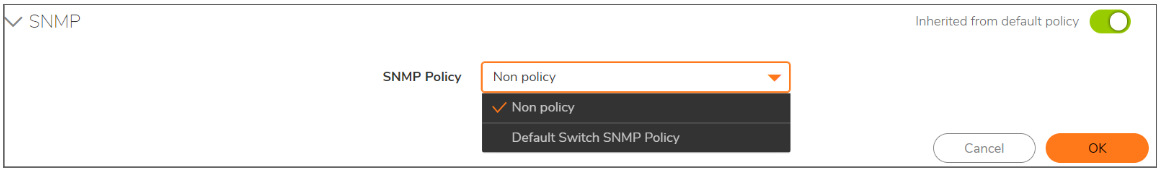
To activate Static MAC Address Table:

1. Navigate to **Policies > Policy Hierarchy > Switch Policy**.
2. Select the **System** tab and scroll down to the Static MAC Address Table section.
3. Specify the **MAC Aging Time**. The range is 10-630 seconds.
4. Specify the **Mac Settings - Port**, **MAC Address**, and **VLAN** in the respective fields.

   You can also search for a MAC Address, Port, Switch or Location using the **Search** field from here.

SNMP

Using this option you can specify the switch SNMP policy.



SNMP

Inherited from default policy

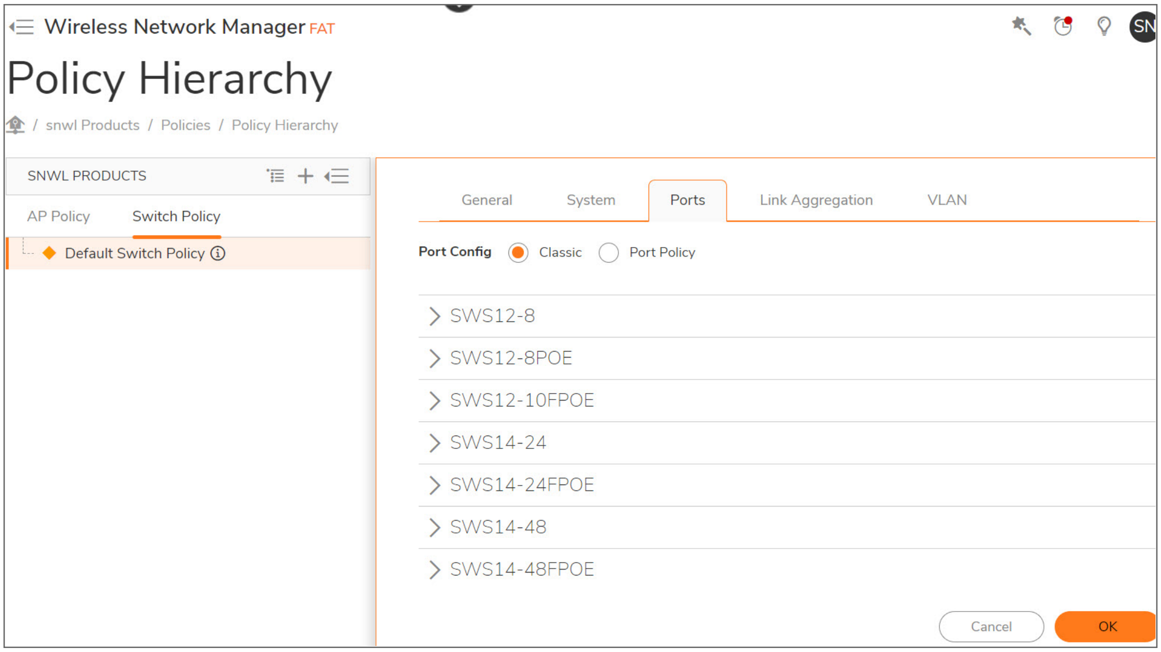
SNMP Policy: Non policy

To activate SNMP:

1. Navigate to **Policies > Policy Hierarchy > Switch Policy**.
2. Select the **System** tab and scroll down to the SNMP section.
3. Select the option from the **SNMP Policy** drop-down.

Ports

The **Ports** tab helps you change the configuration of the ports on the Switch in order to find the best balance of speed and flow control according to your preferences.



Wireless Network Manager FAT

Policy Hierarchy

/ snwl Products / Policies / Policy Hierarchy

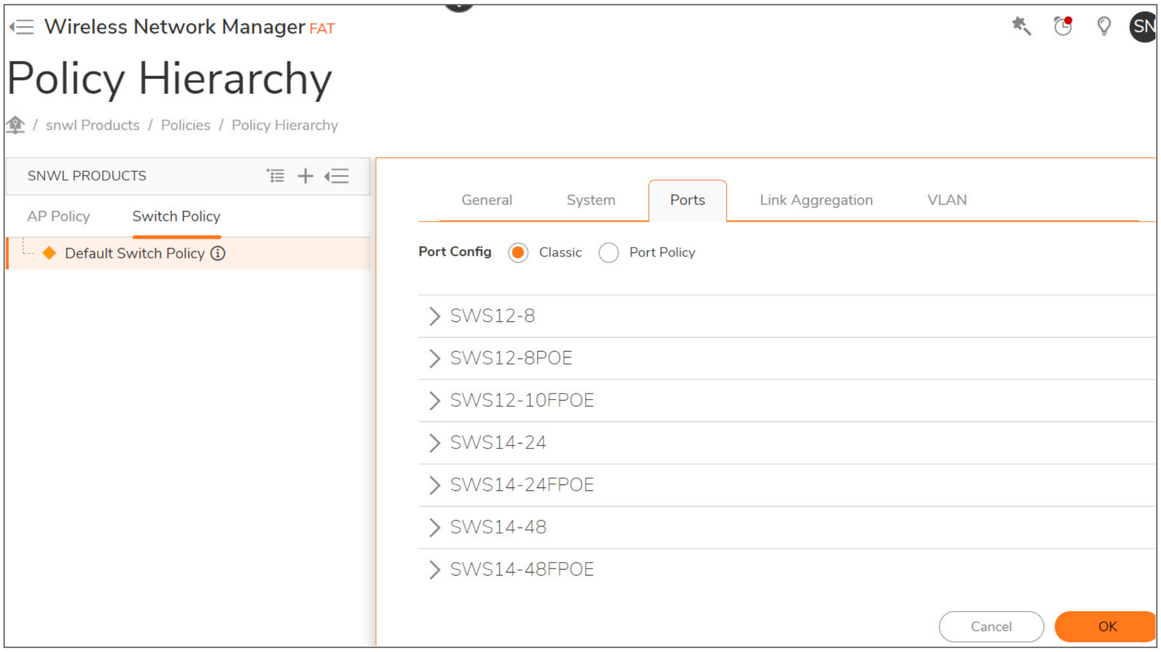
Port Config ● Classic ○ Port Policy

You can select two modes in this **Ports** tab:

- Classic Switch Policy
- Port Policy

Classic Switch Policy

The **Classic** option helps you change the configuration of the ports on the Switch in order to find the best balance of speed and flow control according to your preferences in the Classic mode.



Port Config ● Classic ○ Port Policy

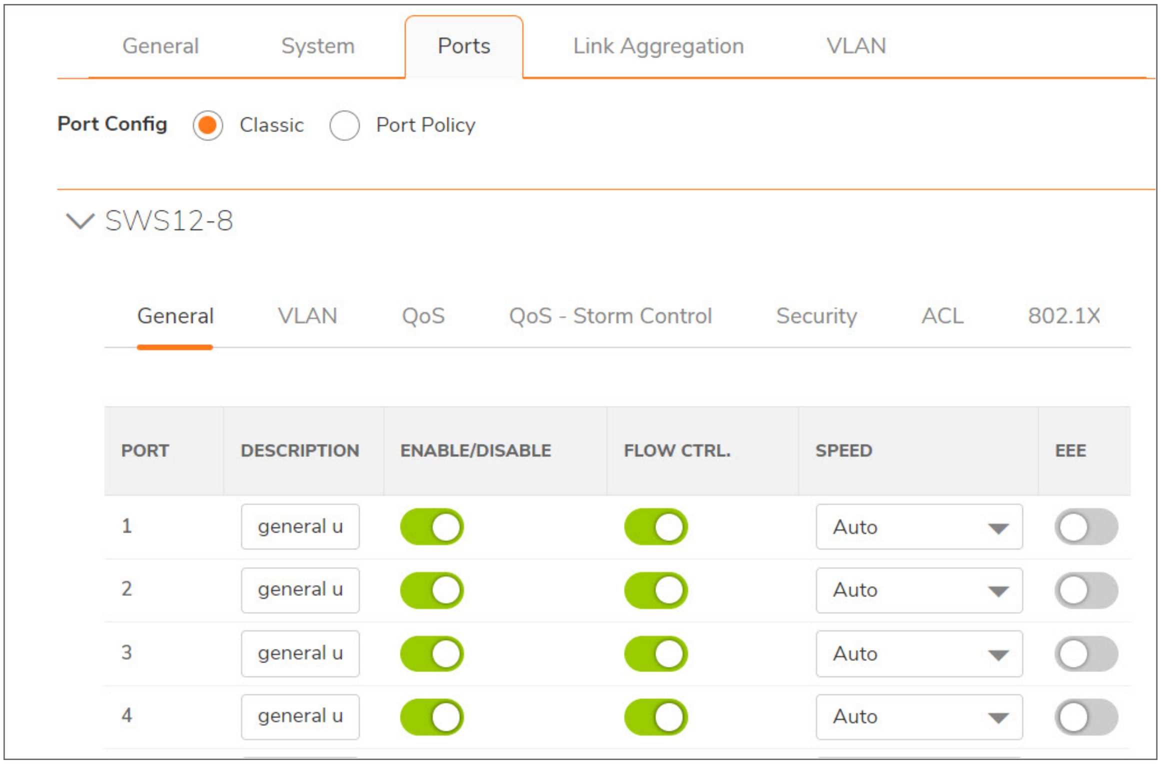
- SWS12-8
- SWS12-8POE
- SWS12-10FPOE
- SWS14-24
- SWS14-24FPOE
- SWS14-48
- SWS14-48FPOE

If you select the Classic Mode, the **Ports** tab helps you to edit the ports details including:

- General
- VLAN
- QoS
- QoS Storm Control
- Security
- ACL
- 802.1X
- POE

General

General tab helps you to edit the general details of the ports.



Port Config ● Classic ○ Port Policy

SWS12-8

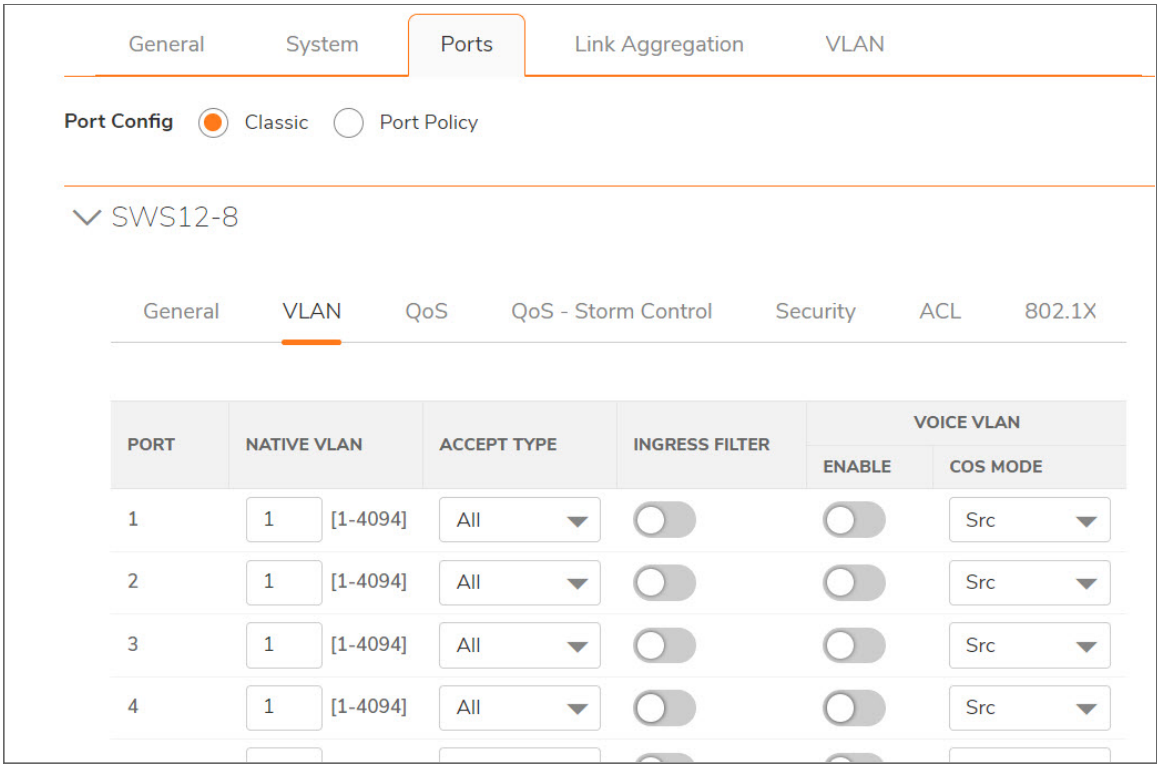
PORT	DESCRIPTION	ENABLE/DISABLE	FLOW CTRL.	SPEED	EEE
1	general u	●	●	Auto ▾	○
2	general u	●	●	Auto ▾	○
3	general u	●	●	Auto ▾	○
4	general u	●	●	Auto ▾	○

This includes editing the following:

- Description
- Enable/Disable
- Flow Control
- Speed
- Enable/Disable EEE
- Enable/Disable DHCP Snooping Trust
- LACP Timeout

VLAN

The VLAN tab helps you to edit the VLAN details of the ports.



Port Config ● Classic ○ Port Policy

SWS12-8

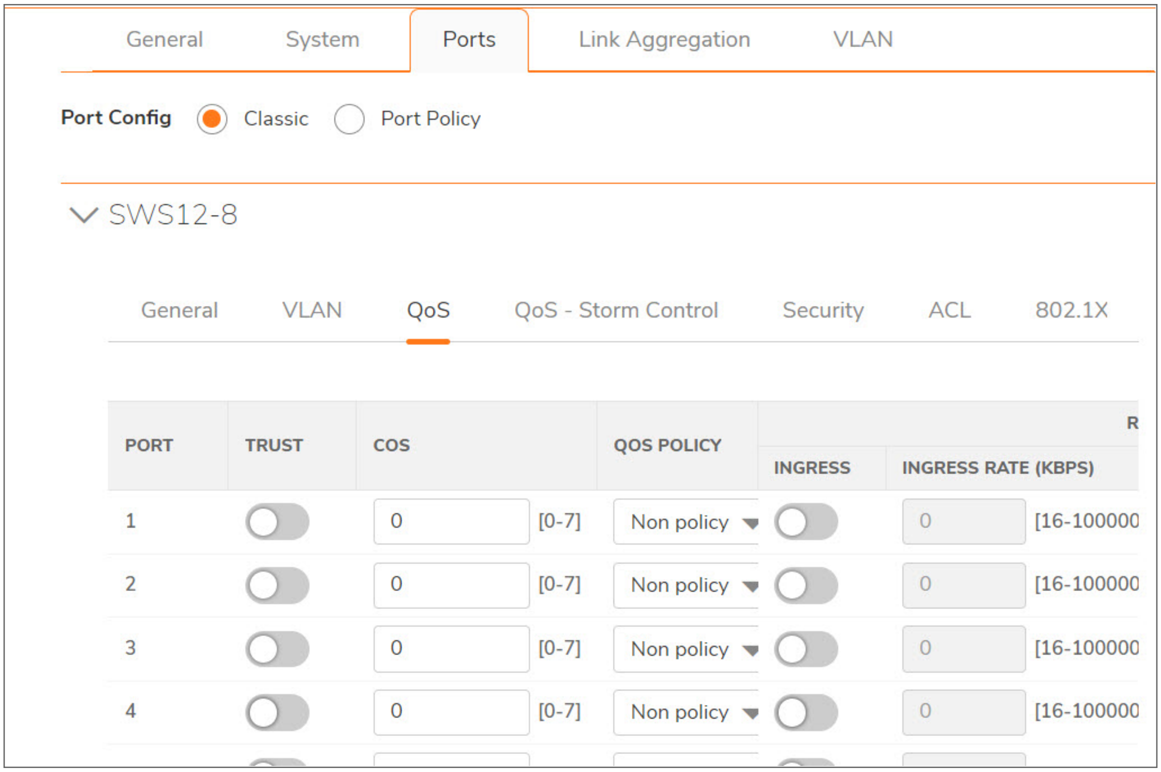
PORT	NATIVE VLAN	ACCEPT TYPE	INGRESS FILTER	VOICE VLAN	
				ENABLE	COS MODE
1	1 [1-4094]	All	○	○	Src
2	1 [1-4094]	All	○	○	Src
3	1 [1-4094]	All	○	○	Src
4	1 [1-4094]	All	○	○	Src

This includes editing the following:

- Native VLAN
- Accept Type
- Ingress Filter
- Enabling VLAN
- Voice VLAN COS Mode

QoS

The QoS tab helps you to edit the QoS details of the ports.



Port Config ● Classic ○ Port Policy

SWS12-8

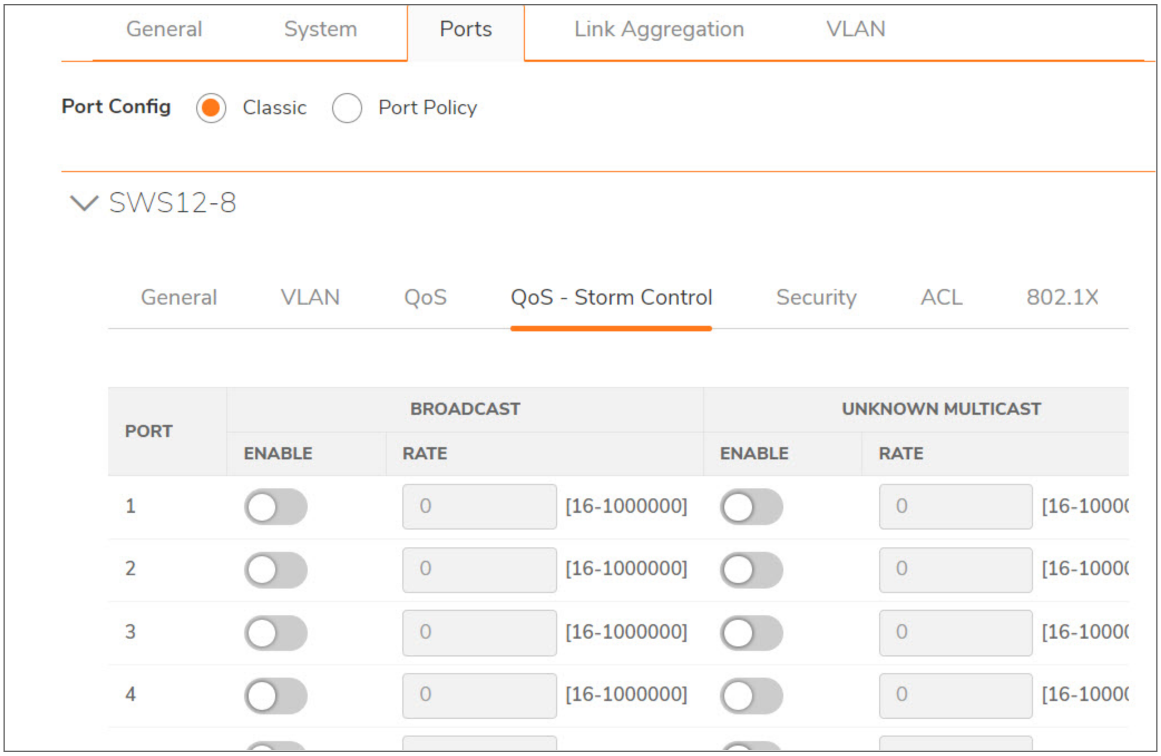
PORT	TRUST	COS		QOS POLICY	R		
					INGRESS	INGRESS RATE (KBPS)	
1	○	0	[0-7]	Non policy	○	0	[16-100000
2	○	0	[0-7]	Non policy	○	0	[16-100000
3	○	0	[0-7]	Non policy	○	0	[16-100000
4	○	0	[0-7]	Non policy	○	0	[16-100000

This includes editing the following:

- Enable or disable Trust
- COS
- QoS Policy
- Ingress
- Ingress Rate (KBPS)
- Egress
- Egress Rate (KBPS)

QoS Storm Control

The QoS Storm Control tab helps you to edit the QoS Storm Control details of the ports.



Port Config ● Classic ○ Port Policy

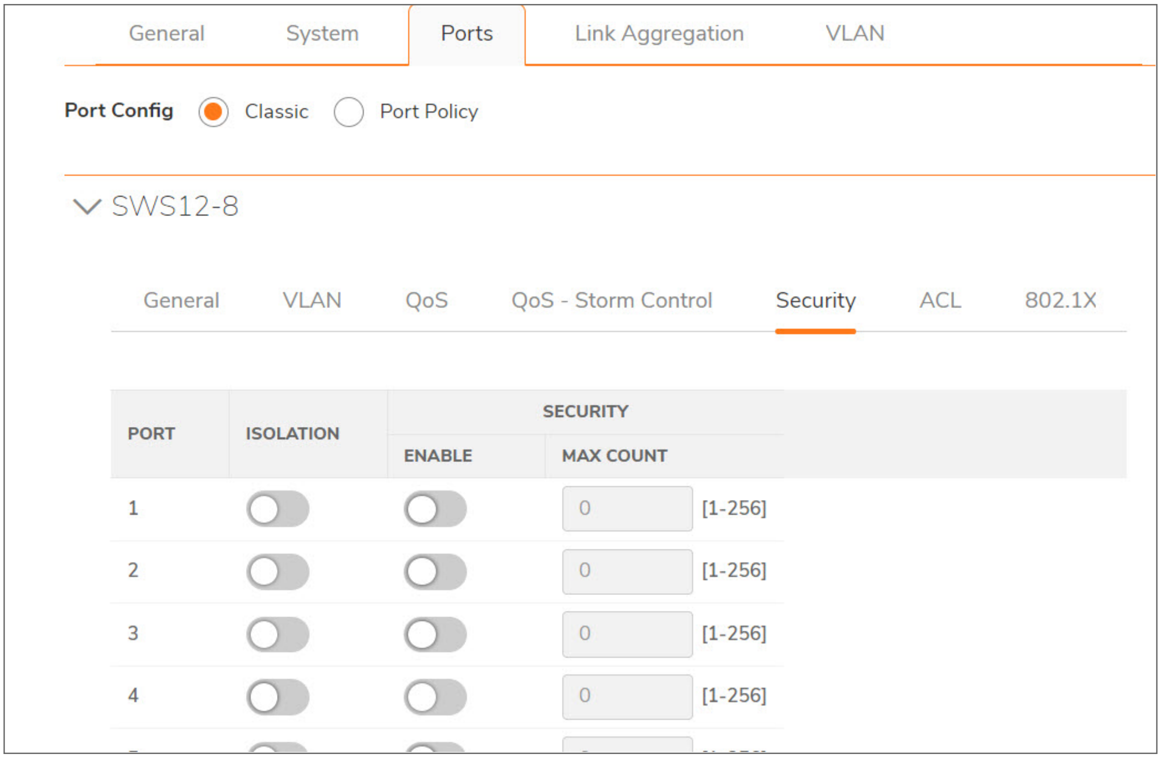
PORT	BROADCAST			UNKNOWN MULTICAST		
	ENABLE	RATE		ENABLE	RATE	
1	○	0	[16-1000000]	○	0	[16-1000
2	○	0	[16-1000000]	○	0	[16-1000
3	○	0	[16-1000000]	○	0	[16-1000
4	○	0	[16-1000000]	○	0	[16-1000

This includes editing the following:

- Broadcast Rate
- Unknown Multicast
- Unknown Unicast

Security

The Security tab helps you to edit the Security details of the ports.



Port Config ● Classic ○ Port Policy

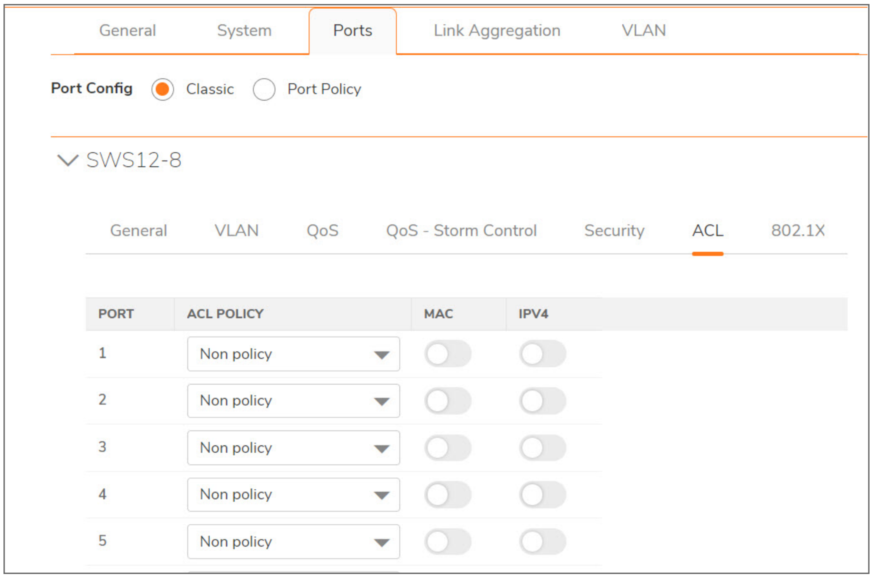
PORT	ISOLATION	SECURITY	
		ENABLE	MAX COUNT
1	○	○	0 [1-256]
2	○	○	0 [1-256]
3	○	○	0 [1-256]
4	○	○	0 [1-256]

This includes editing the following:

- Isolation
- Security Max Count

ACL

The ACL tab helps you to edit the ACL details of the ports.



Port Config ● Classic ○ Port Policy

SWS12-8

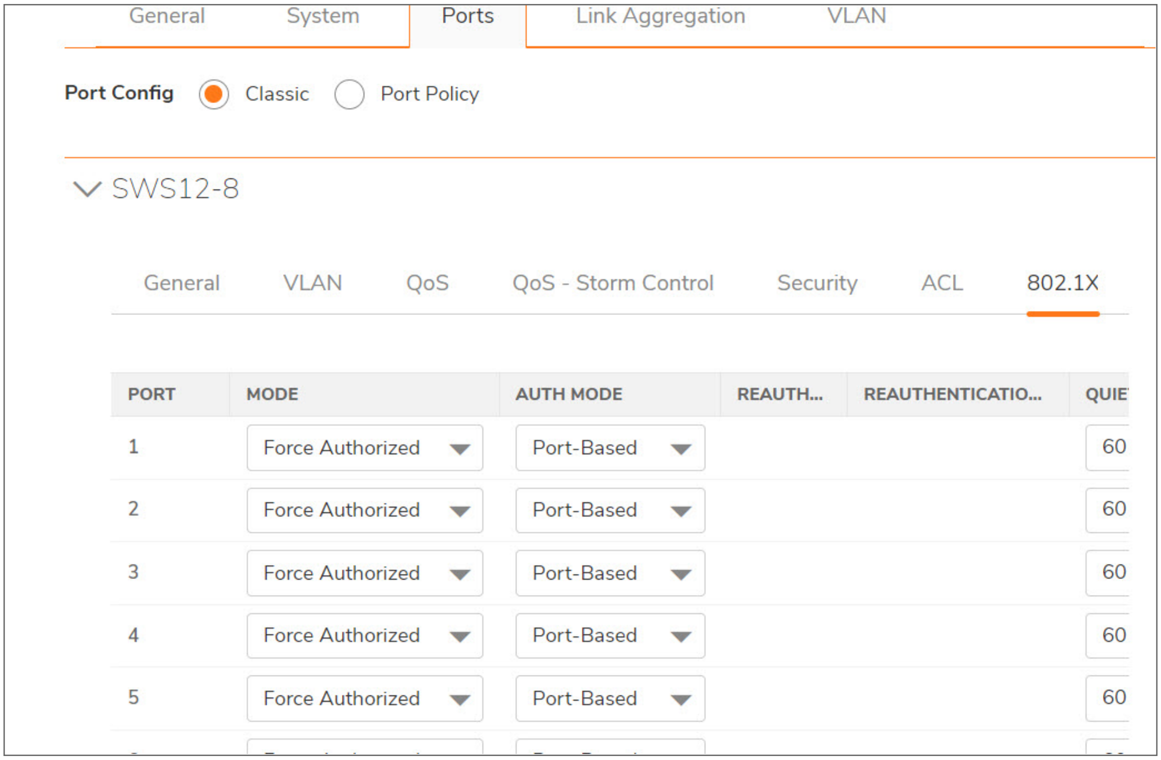
PORT	ACL POLICY	MAC	IPV4
1	Non policy	○	○
2	Non policy	○	○
3	Non policy	○	○
4	Non policy	○	○
5	Non policy	○	○

This includes editing the following:

- ACL Policy
- MAC
- IPV4

802.1X

The 802.1X tab helps you to edit the 802.1X details of the ports.



Port Config ● Classic ○ Port Policy

PORT	MODE	AUTH MODE	REAUTH...	REAUTHENTICATIO...	QUIE
1	Force Authorized	Port-Based			60
2	Force Authorized	Port-Based			60
3	Force Authorized	Port-Based			60
4	Force Authorized	Port-Based			60
5	Force Authorized	Port-Based			60

Wireless Network Manager also provides the **802.1X MAB** authentication, an access control technique to authenticate the client devices. The 802.1x MAC Authentication Bypass (MAB) allows a device without an 802.1x supplicant running on it to authenticate against RADIUS via MAC address. This uses the MAC Address of a device to determine the network access to be provided to the hosts.

To enable the MAB authentication ensure that the switch is Online and the **802.1X** is always enabled in the **System** Tab.

ⓘ | **IMPORTANT:** You need to add radius server before using 802.1X.

ⓘ | **NOTE:** If you select MAB mode, the authenticate host is MAB only. If you select Hybrid mode, the authenticate host is EAP but if the host does not support EAP mode, it falls back to MAB mode. If you select Disable, the authenticate host is EAP only.

ⓘ | **NOTE:** Multi-authentication/multi-host is supported only when the authentication mode is MAC-Based, and not when the authentication mode is Port-Based.

You can edit all the following options from this tab:

- Mode
- Auth Mode
- Re-authentication
- Re-authentication Period
- Quiet Period
- Supplicant Period

- Max Retry
- Guest VLAN
- Radius VLAN Assign
- MAB Mode
- MAX Host

Port Policy

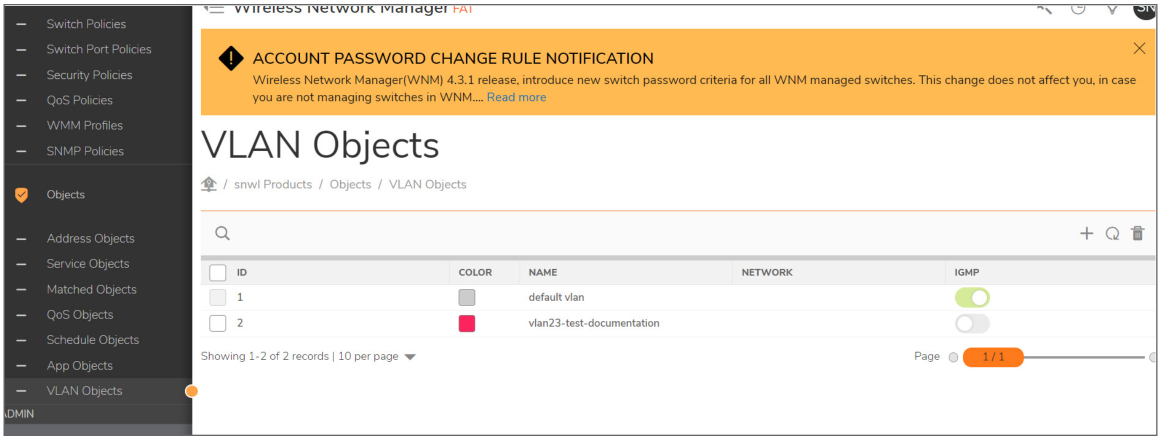
The **Ports** tab helps you to apply the port policy that you have created to the switch.

To add a port policy to a switch, the pre-requisites are to create a VLAN and then a Switch Port Policy. These procedures are described below in the Pre-requisites section.

To Apply Switch Port Policy to a Switch:

1. Create a VLAN.
    a. Go to **Objects** > **VLAN Objects**. For more information, refer to VLAN Objects and create a VLAN.

    The created VLAN will be displayed as given below.



ACCOUNT PASSWORD CHANGE RULE NOTIFICATION

Wireless Network Manager(WNM) 4.3.1 release, introduce new switch password criteria for all WNM managed switches. This change does not affect you, in case you are not managing switches in WNM.... Read more

VLAN Objects

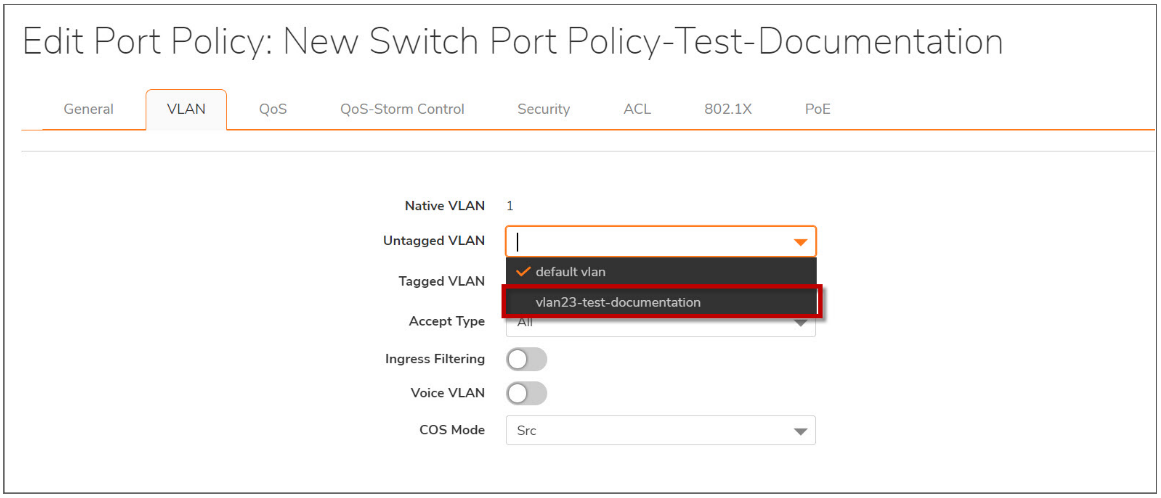
/ snwl Products / Objects / VLAN Objects

☐ ID	COLOR	NAME	NETWORK	IGMP
☐ 1	⬜	default vlan		●
☐ 2	🟥	vlan23-test-documentation		○

Showing 1-2 of 2 records | 10 per page

Page 1 / 1

2. Create a Switch Port Policy. For more information, refer to Switch port Policies VLAN.
3. Apply the VLAN to the Switch Port Policy.
    a. Go to **Policies** > **Switch Port Policies** > **Edit Port Policies** > **VLAN** tab
    b. Select the VLAN from the **Untagged VLAN** drop down list.



Edit Port Policy: New Switch Port Policy-Test-Documentation

Native VLAN 1

Untagged VLAN

Tagged VLAN

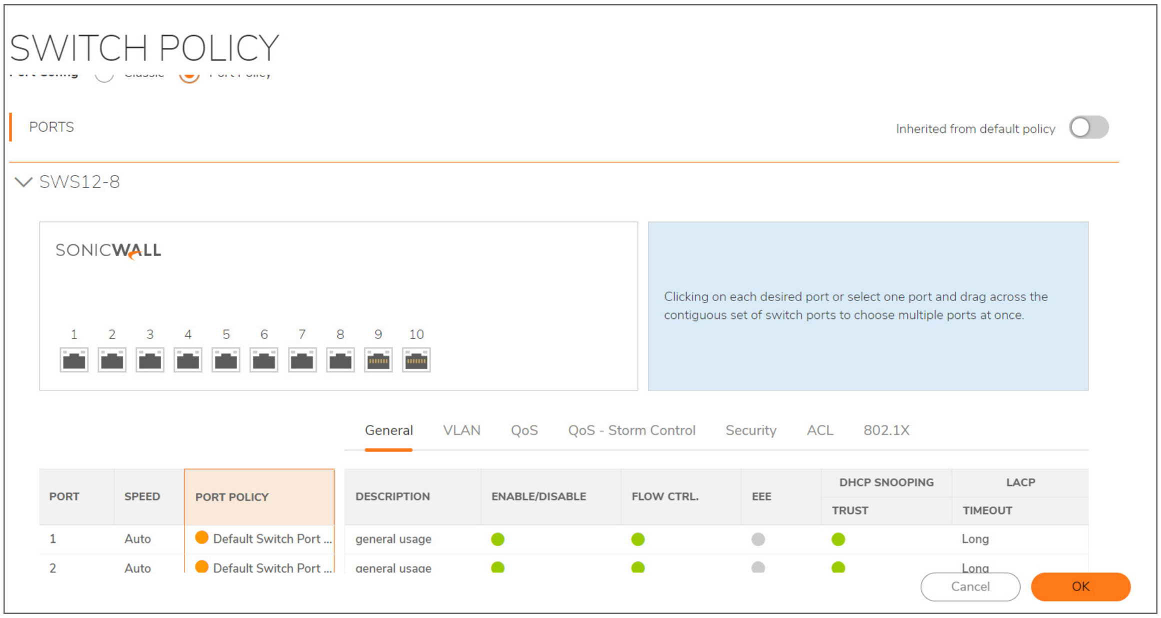
Accept Type All

Ingress Filtering ○

Voice VLAN ○

COS Mode Src

4. To save the VLAN to the port policy, click **OK**.
5. Apply the switch port policy to the switch:
   a. Go to **Policies** > **Switch Policies**
   b. On the **Switch Policies** page, click on the edit button hovering to the right side of the switch policy that you want to edit.
   c. On the Switch Policy configuration page, click on the **Ports** tab.
   d. Select the **Port Policy** radio button.
   e. Click → and select the Switch you need to configure. By default, the page is displayed as given below.



SWITCH POLICY

PORTS

Inherited from default policy ○

SWS12-8

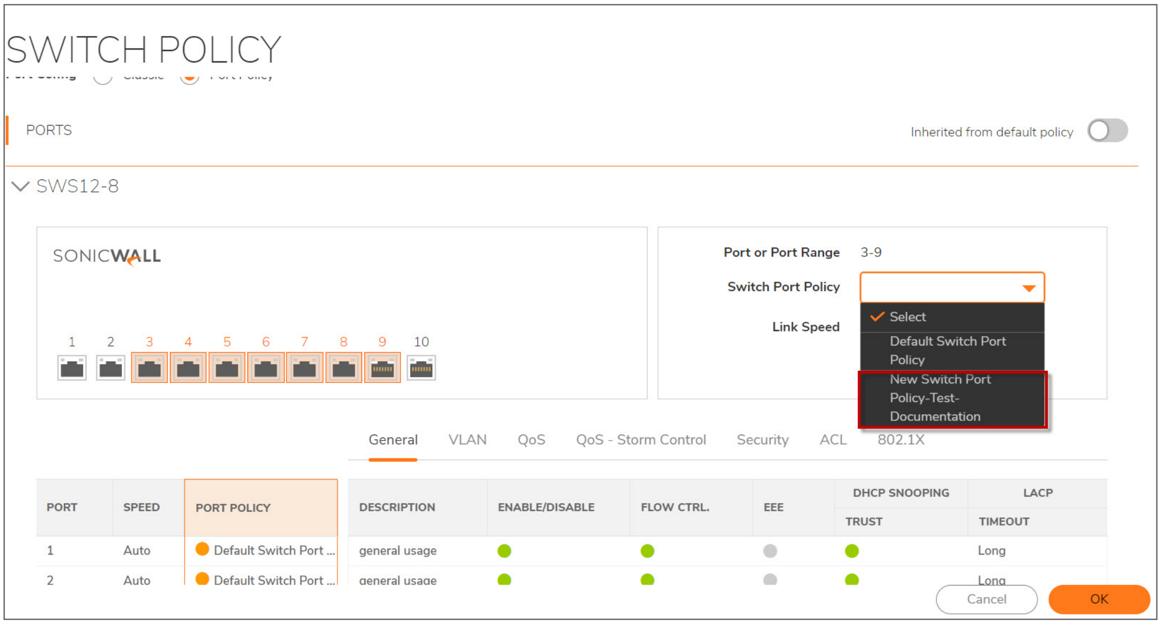
Clicking on each desired port or select one port and drag across the contiguous set of switch ports to choose multiple ports at once.

PORT	SPEED	PORT POLICY	DESCRIPTION	ENABLE/DISABLE	FLOW CTRL.	EEE	DHCP SNOOPING	LACP
							TRUST	TIMEOUT
1	Auto	● Default Switch Port ...	general usage	●	●	●	●	Long
2	Auto	● Default Switch Port ...	general usage	●	●	●	●	Long

f. Click on any of the desired port, and the options to apply the **Switch Port Policy** and **Link Speed** are displayed on the right side as given below.

g. Select the ports to apply the switch port policy and link speed. You can select one or multiple any ports from the left box by dragging.

h. Select the required **Switch Port Policy** from the drop down.



SWITCH POLICY

PORTS

Inherited from default policy

SWS12-8

Port or Port Range 3-9

Switch Port Policy

Link Speed

PORT	SPEED	PORT POLICY	DESCRIPTION	ENABLE/DISABLE	FLOW CTRL.	EEE	DHCP SNOOPING	LACP
							TRUST	TIMEOUT
1	Auto	● Default Switch Port ...	general usage	●	●	●	●	Long
2	Auto	● Default Switch Port ...	general usage	●	●	●	●	Long

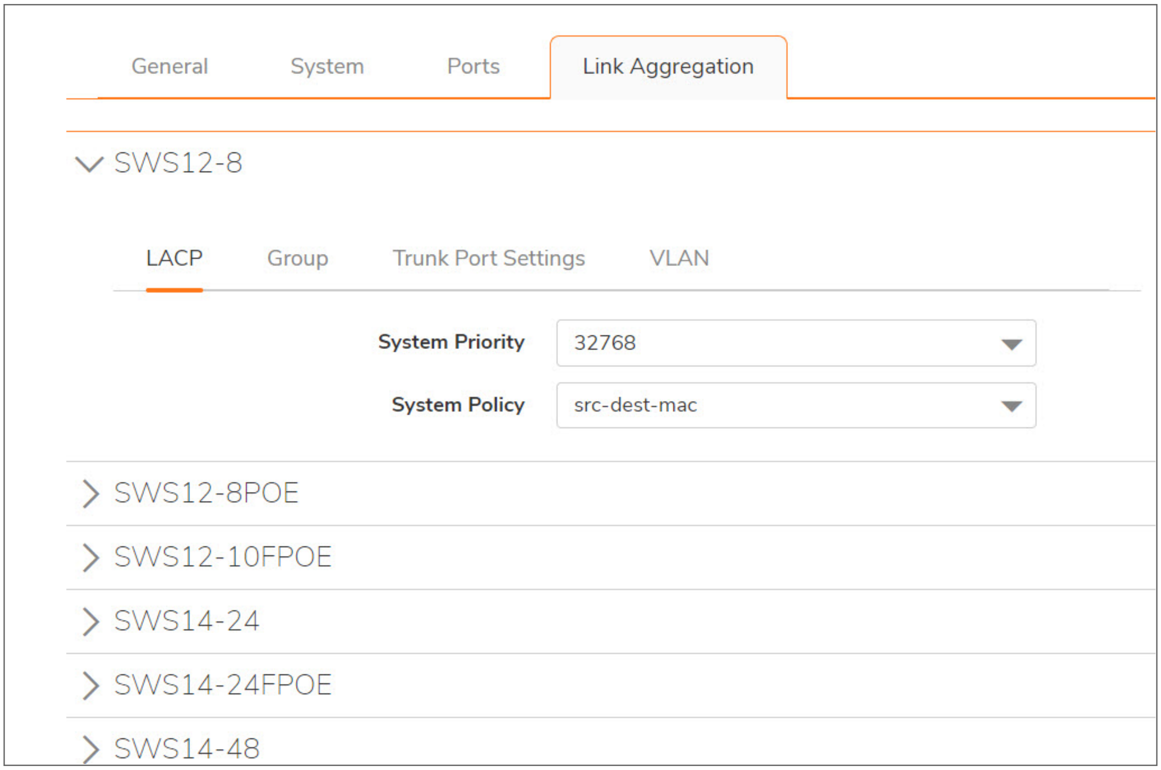
i. Select the **Link Speed**.

j. Click **OK** to save the changes.

Link Aggregation

A Link Aggregation Group (LAG) optimizes port usage by linking a group of ports together to form a single, logical, higher-bandwidth link. Aggregating ports multiplies the bandwidth and increases port flexibility for the Switch. Link Aggregation is most commonly used to link a bandwidth intensive network device (or devices), such as a server, to the backbone of a network.

The participating ports are called Members of a port trunk group. Since all ports of the trunk group must be configured to operate in the same manner, the configuration of the one port of the trunk group is applied to all ports of the trunk group. Thus, you will only need to configure one of any of the ports in a trunk group. A specific data communication packet will always be transmitted over the same port in a trunk group. This ensures the delivery of individual frames of a data communication packet will be received in the correct order. The traffic load of the LAG will be balanced among the ports according to Aggregate Arithmetic. If the connections of one or several ports are broken, the traffic of these ports will be transmitted on the normal ports, so as to guarantee the connection reliability.



System Priority: 32768

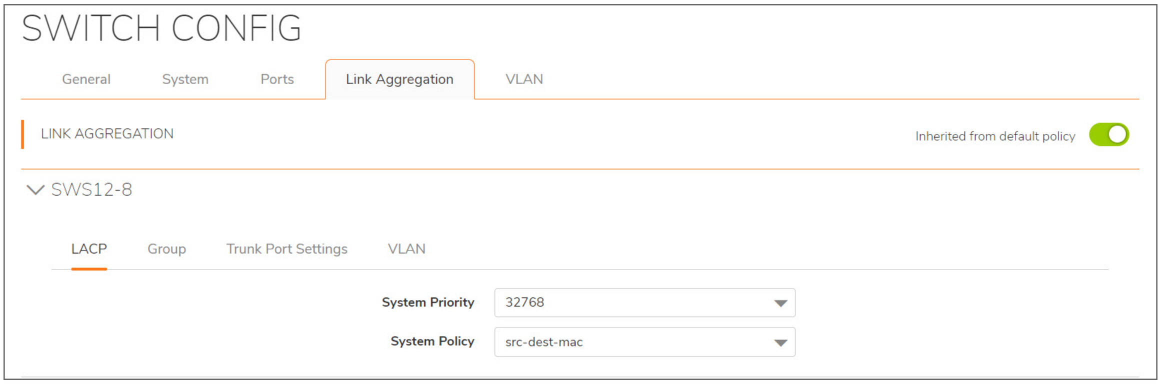
System Policy: src-dest-mac

The **Link Aggregation** tab helps you to edit the following information:

- LACP
- Group
- Trunk Port Settings
- VLAN

LACP

LACP is a dynamic protocol which helps to automate the configuration and maintenance of LAG's. The main purpose of LACP is to automatically configure individual links to an aggregate bundle, while adding new links and helping to recover from link failures if the need arises. LACP can monitor to verify if all the links are connected to the authorized group. LACP is a standard in computer networking, hence LACP should be enabled on the Switch's trunk ports initially in order for both the participating Switches/devices that support the standard, to use it.



Inherited from default policy: on

System Priority: 32768

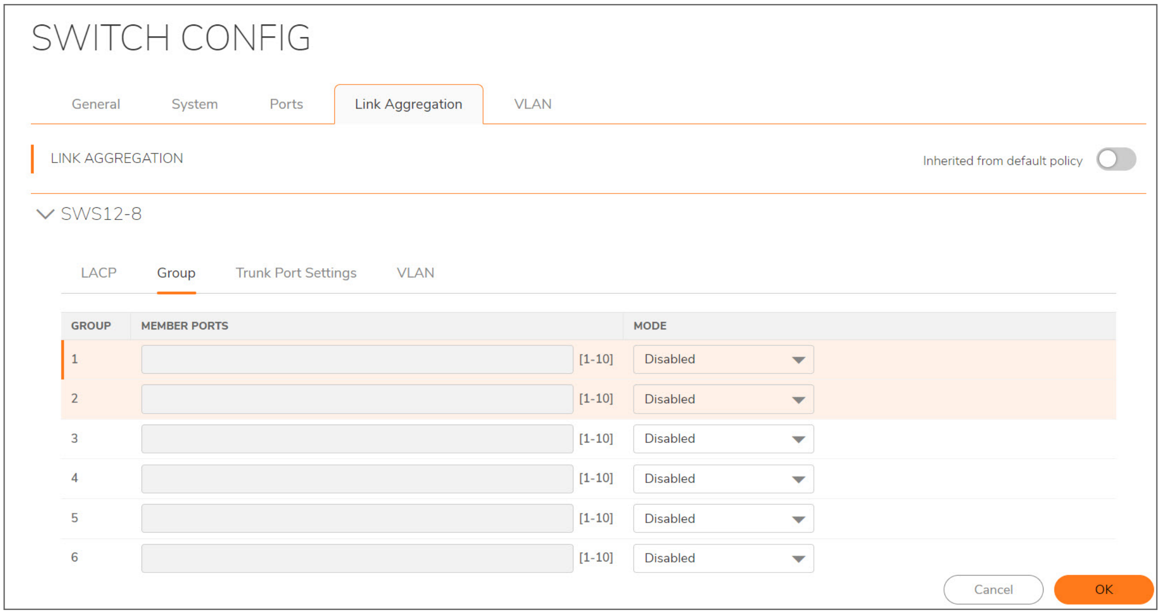
System Policy: src-dest-mac

You can edit all the following options from this tab:

- System Priority
- System Policy

Group

Clicking on **Link Aggregation** > **Group** tab helps you to change the mode of the member ports.



Inherited from default policy: off

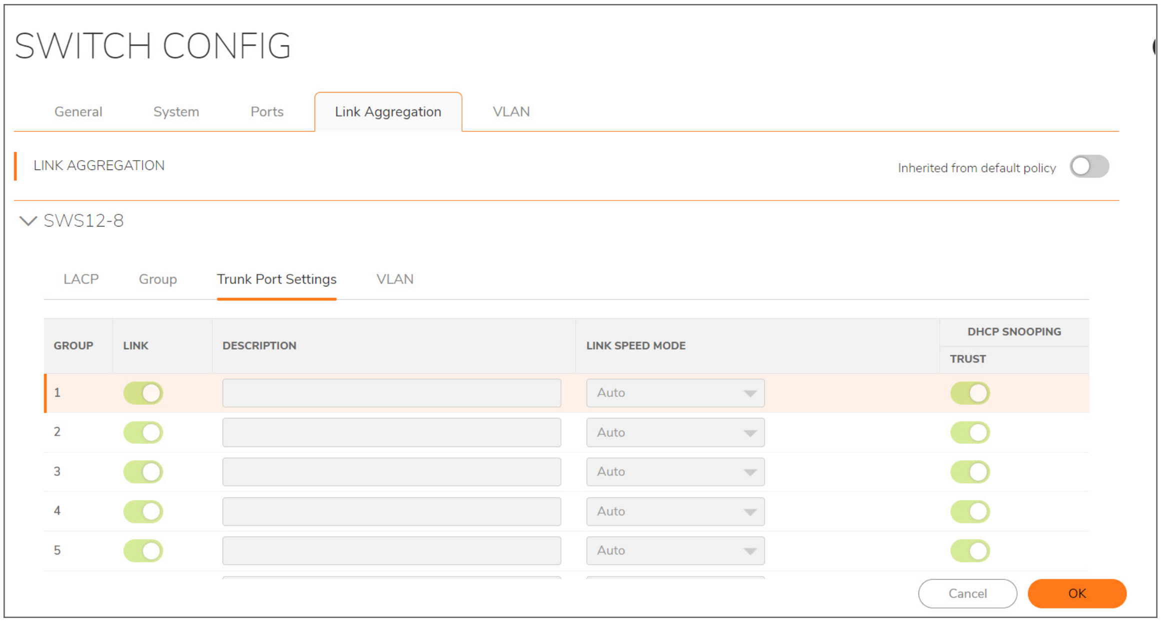
GROUP	MEMBER PORTS	MODE
1	[1-10]	Disabled
2	[1-10]	Disabled
3	[1-10]	Disabled
4	[1-10]	Disabled
5	[1-10]	Disabled
6	[1-10]	Disabled

You can edit all the following options from this tab:

- Member Ports
- Mode

Trunk Port Settings

Clicking on **Link Aggregation** > **Trunk Port Settings** tab helps you to change the Link Speed Mode and Trust details.



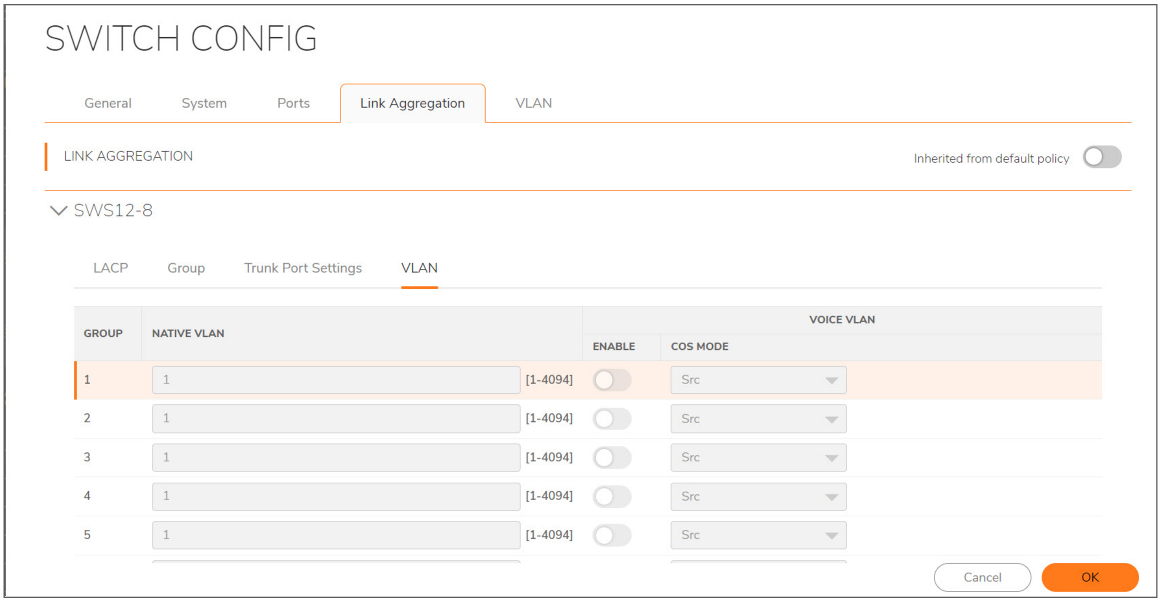
GROUP	LINK	DESCRIPTION	LINK SPEED MODE	DHCP SNOOPING
				TRUST
1	●		Auto	●
2	●		Auto	●
3	●		Auto	●
4	●		Auto	●
5	●		Auto	●

You can edit all the following options from this tab:

- Link
- Description
- Link Speed Mode
- DHCP Snooping Trust

VLAN

Clicking on **Link Aggregation** > **VLAN** tab helps you to change the VLAN details.



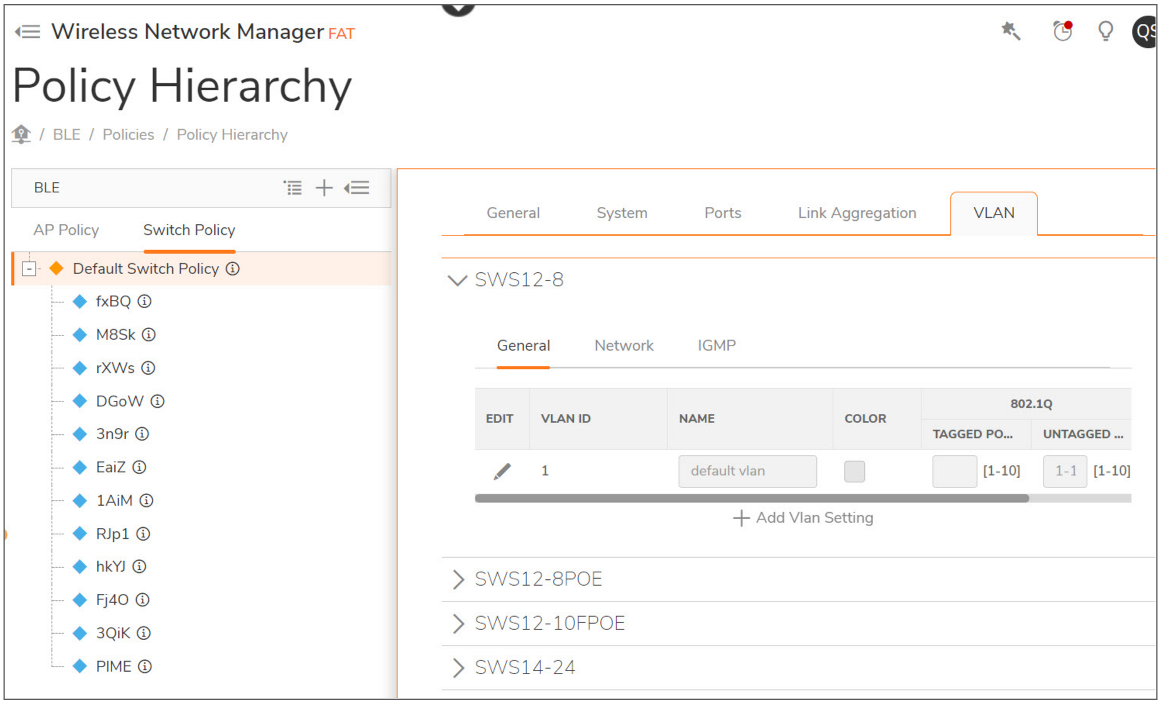
GROUP	NATIVE VLAN		VOICE VLAN	
			ENABLE	COS MODE
1	1	[1-4094]	○	Src
2	1	[1-4094]	○	Src
3	1	[1-4094]	○	Src
4	1	[1-4094]	○	Src
5	1	[1-4094]	○	Src

You can edit all the following options from this tab:

- Native VLAN (The range is from 1 to 4094)
- Enable/Disable Voice VLAN
- COS Mode

VLAN

The **Switch Policy** >**VLAN** tab helps you to edit the VLAN details of the ports.



Wireless Network Manager FAT

Policy Hierarchy

/ BLE / Policies / Policy Hierarchy

BLE

AP Policy Switch Policy

- Default Switch Policy
  - fxBQ
  - M8Sk
  - rXWs
  - DGoW
  - 3n9r
  - EaiZ
  - 1AiM
  - RJp1
  - hkYJ
  - Fj4O
  - 3QiK
  - PIME

General System Ports Link Aggregation VLAN

SWS12-8

General Network IGMP

EDIT	VLAN ID	NAME	COLOR	802.1Q	
				TAGGED PO...	UNTAGGED ...
	1	default vlan		[1-10]	1-1 [1-10]

+ Add Vlan Setting

SWS12-8POE

SWS12-10FPOE

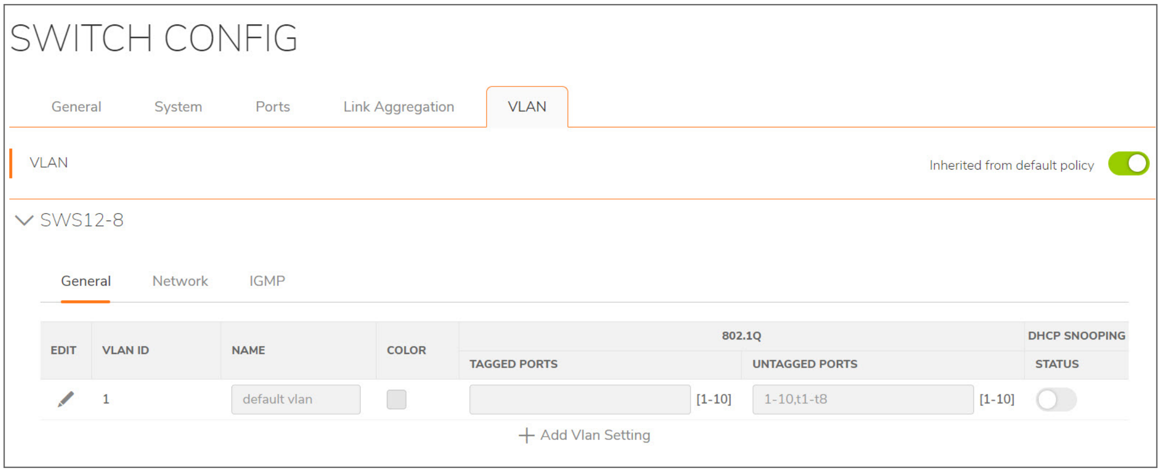
SWS14-24

The **VLAN** tab helps you to edit the information of the following:

- General
- Network
- IGMP

General

Clicking on **VLAN** > **General** tab helps you to change the general features of VLAN settings.



SWITCH CONFIG

General System Ports Link Aggregation VLAN

VLAN

Inherited from default policy

SWS12-8

General Network IGMP

EDIT	VLAN ID	NAME	COLOR	802.1Q		DHCP SNOOPING
				TAGGED PORTS	UNTAGGED PORTS	STATUS
	1	default vlan		[1-10]	1-10,t1-t8 [1-10]	

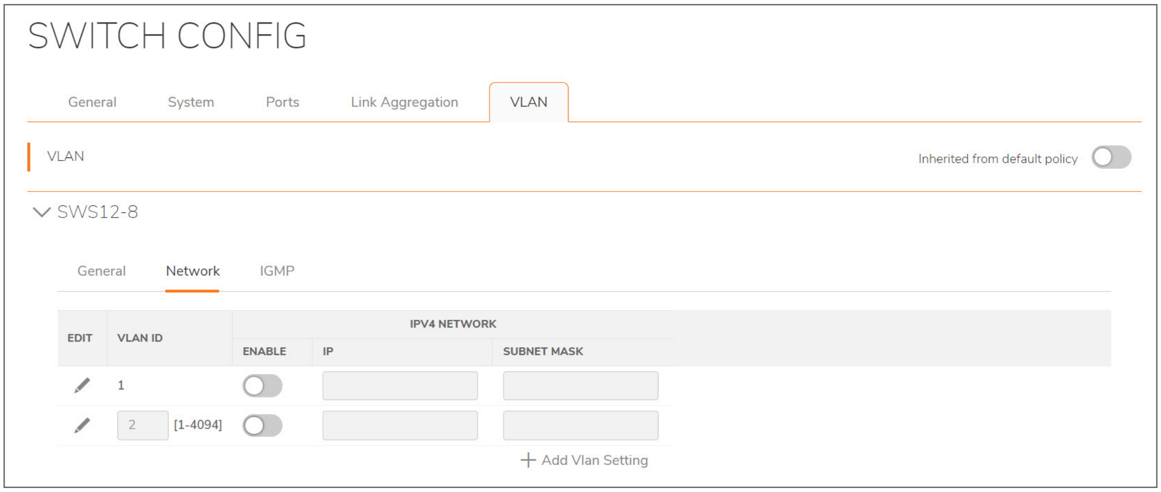
+ Add Vlan Setting

You can edit the following options from this tab:

- VLAN ID (the number range is from 1 to 4094)
- Name
- Color
- Tagged Ports (the range depends on the model)
- Untagged Ports (the range depends on the model)
- DHCP Snooping Status

Network

Clicking on **VLAN** > **Network** tab helps you to change the network settings.



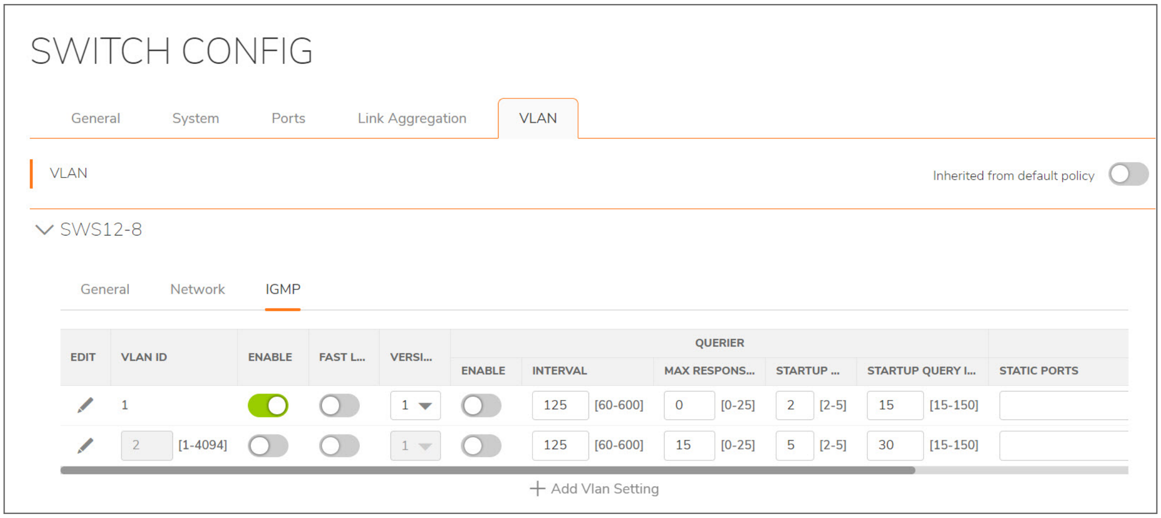
EDIT	VLAN ID	IPV4 NETWORK		
		ENABLE	IP	SUBNET MASK
	1	○		
	2 [1-4094]	○		

You can edit the following options from this tab:

- VLAN ID (the number range is from 1 to 4094)
- Enable/Disable IPv4 network
- IP
- Subnet Mask

IGMP

Clicking on **VLAN** > **IGMP** tab helps you to change the network settings.



EDIT	VLAN ID	ENABLE	FAST L...	VERSI...	QUERIER					STATIC PORTS
					ENABLE	INTERVAL	MAX RESPONS...	STARTUP ...	STARTUP QUERY I...	
	1	●	○	1	○	125 [60-600]	0 [0-25]	2 [2-5]	15 [15-150]	
	2 [1-4094]	○	○	1	○	125 [60-600]	15 [0-25]	5 [2-5]	30 [15-150]	

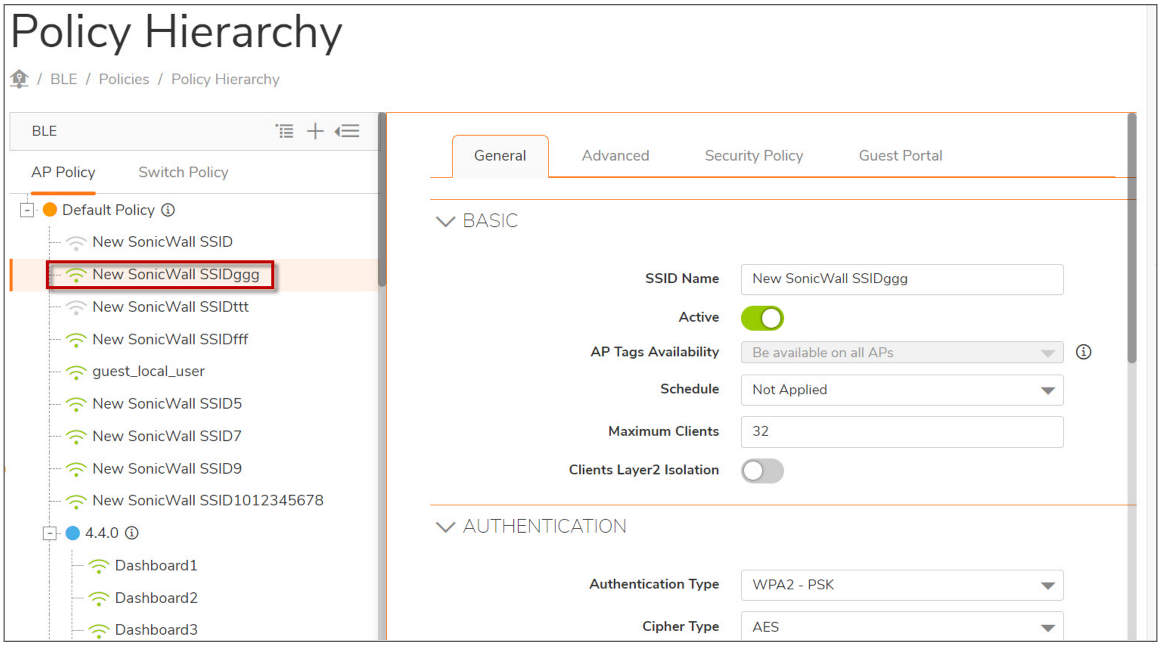
You can edit the following options from this tab:

- VLAN ID (the number range is from 1 to 4094)
- Enable/Disable
- Enable/Disable Fast Leave
- Version of IGMP
- Enable/Disable Quierier Interval
- Interval
- Max Response Interval (The range is 0-25)
- Startup Query Counter (The range is 2-5)
- Startup Query Interval (The range is 15-150)
- Static Ports (The range is 1-10)
- Forbidden Ports (The range is 1-10)

Select an SSID

The SSIDs are marked with the Wi-Fi symbol. They sometimes depend only on the Default Policy, and sometimes have other AP policies applied to them. They can also have Security Policies applied, such as CFS-1 and ACL-1.

Clicking on an SSID policy name in the middle pane of the **Policy > Policy Hierarchy** page brings up several options for configuring the SSIDs in your network.


Policy Hierarchy

/ BLE / Policies / Policy Hierarchy

BLE

AP Policy | Switch Policy

- Default Policy ⓘ
  - New SonicWall SSID
  - New SonicWall SSIDggg
  - New SonicWall SSIDttt
  - New SonicWall SSIDfff
  - guest_local_user
  - New SonicWall SSID5
  - New SonicWall SSID7
  - New SonicWall SSID9
  - New SonicWall SSID1012345678
  - 4.4.0 ⓘ
    - Dashboard1
    - Dashboard2
    - Dashboard3

General | Advanced | Security Policy | Guest Portal

BASIC

SSID Name	New SonicWall SSIDggg
Active	●
AP Tags Availability	Be available on all APs
Schedule	Not Applied
Maximum Clients	32
Clients Layer2 Isolation	○

AUTHENTICATION

Authentication Type	WPA2 - PSK
Cipher Type	AES

Topics:

- General
- Advanced
- Security Policies
- Guest Portal

SSID Policies

The **Policies > SSID Policies** page is used for creating and managing SSID policies. The table of SSIDs and SSID groups has fields for **Name** (of group)/**SSID**, **Band Selection**, and **Security**, which shows which security policies are applied to the SSID or to the group.

The next columns are:

- **SSL VPN**
- **Authentication**
- **Max Clients**
- **Hide SSID**
- **Tags**

These settings apply only to the individual SSIDs.

Hovering over the:

- Items in the **Security** column of this screen brings up details about the security policy indicated for this SSID or this group.
- Row brings up options to:
    - **Edit** and **Delete** for individual SSIDs
    - **Edit**, **Add**, **Copy**, and **Delete** for SSID groups

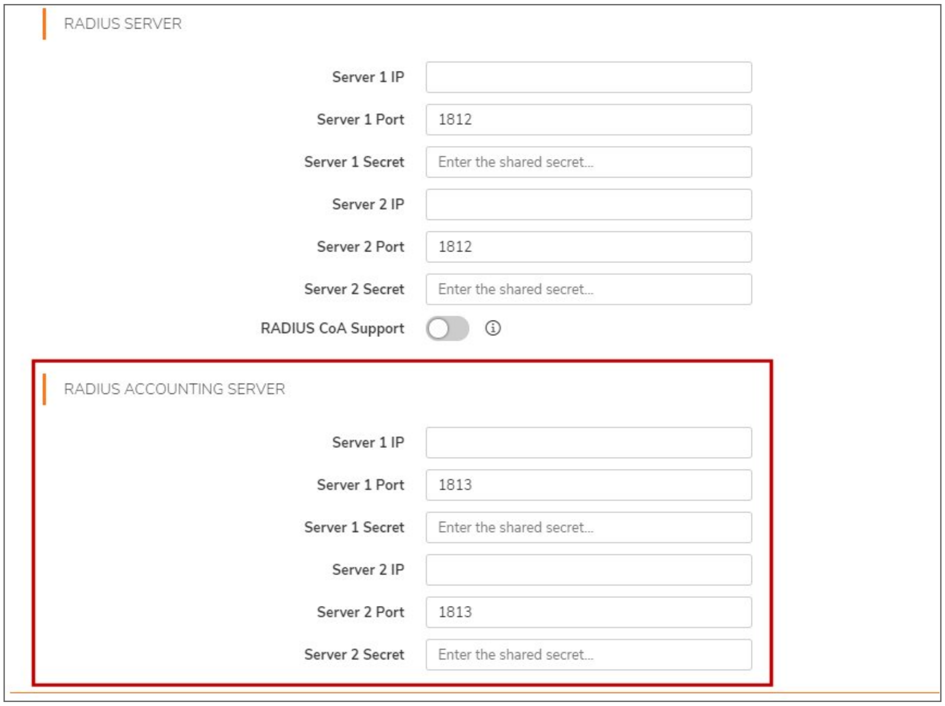
Topics:

- Adding SSID Security Policies
- Editing SSID Security Policies

Adding SSID Security Policies

Click on the **+ Add** on an SSID group row to bring up this **Add SSID** screen. These are the same fields you consulted or configured in the Select an SSID section from the central pane of the **Policy > Policy Hierarchy** screen. These fields are applied to the new SSID you are adding.

General - For RADIUS Accounting Support, go to **Policies > SSID Policies > Add** (in the SSID row) **> General > Authentication Type WPA2 - EAP**. The page allows you to configure RADIUS accounting support on the new SSID for this authentication type.



RADIUS SERVER

Server 1 IP	
Server 1 Port	1812
Server 1 Secret	Enter the shared secret...
Server 2 IP	
Server 2 Port	1812
Server 2 Secret	Enter the shared secret...
RADIUS CoA Support	○ ⓘ

RADIUS ACCOUNTING SERVER

Server 1 IP	
Server 1 Port	1813
Server 1 Secret	Enter the shared secret...
Server 2 IP	
Server 2 Port	1813
Server 2 Secret	Enter the shared secret...

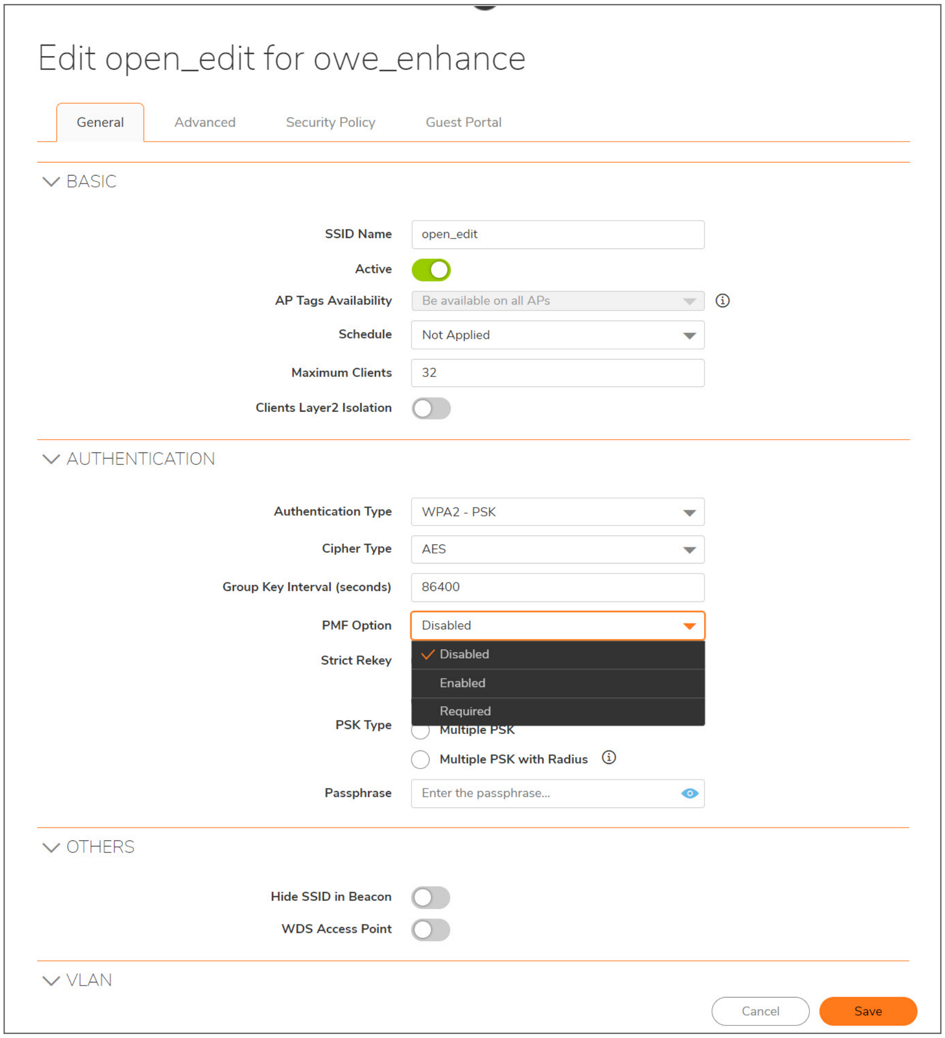
Click **RADIUS CoA Support** if you want to enable the connected devices to act as a RADIUS dynamic authorization server and respond to RADIUS Change of Authorization (CoA) and disconnect messages sent by the RADIUS server.

Editing SSID Security Policies

Click on **Edit** on an SSID row to display the **Edit SSID** screen. These are the same fields you consulted or configured in the Select an SSID section from the central pane of the **Policy > Policy Hierarchy** screen. Now these fields are applied to a new SSID you have selected from the **SSID Policy** screen.

- **PMF** - **Policies > SSID Policies > Edit** (in an SSID row) **> General / Authentication** provides an approved amendment to the IEEE 802.11 standard to protect wireless management frames, the IEEE 802.11W-2009. It is also known as the Protected Management Frames (PMF) standard. The chosen SSID can be edited so the PMF option is:
  - **Disabled**
  - **Enabled**
- **WDS** - The bottom of the screen has a toggle to select whether this access point is part of a Wireless Distribution System (WDS). A WDS is a group of access points associated together in such a way as to

expand the range of the signal availability.



Edit open_edit for owe_enhance

BASIC

SSID Name: open_edit

Active: on

AP Tags Availability: Be available on all APs

Schedule: Not Applied

Maximum Clients: 32

Clients Layer2 Isolation: off

AUTHENTICATION

Authentication Type: WPA2 - PSK

Cipher Type: AES

Group Key Interval (seconds): 86400

PMF Option: Disabled

- ✓ Disabled
- Enabled
- Required

Strict Rekey

PSK Type: ○ Multiple PSK ○ Multiple PSK with Radius

Passphrase: Enter the passphrase...

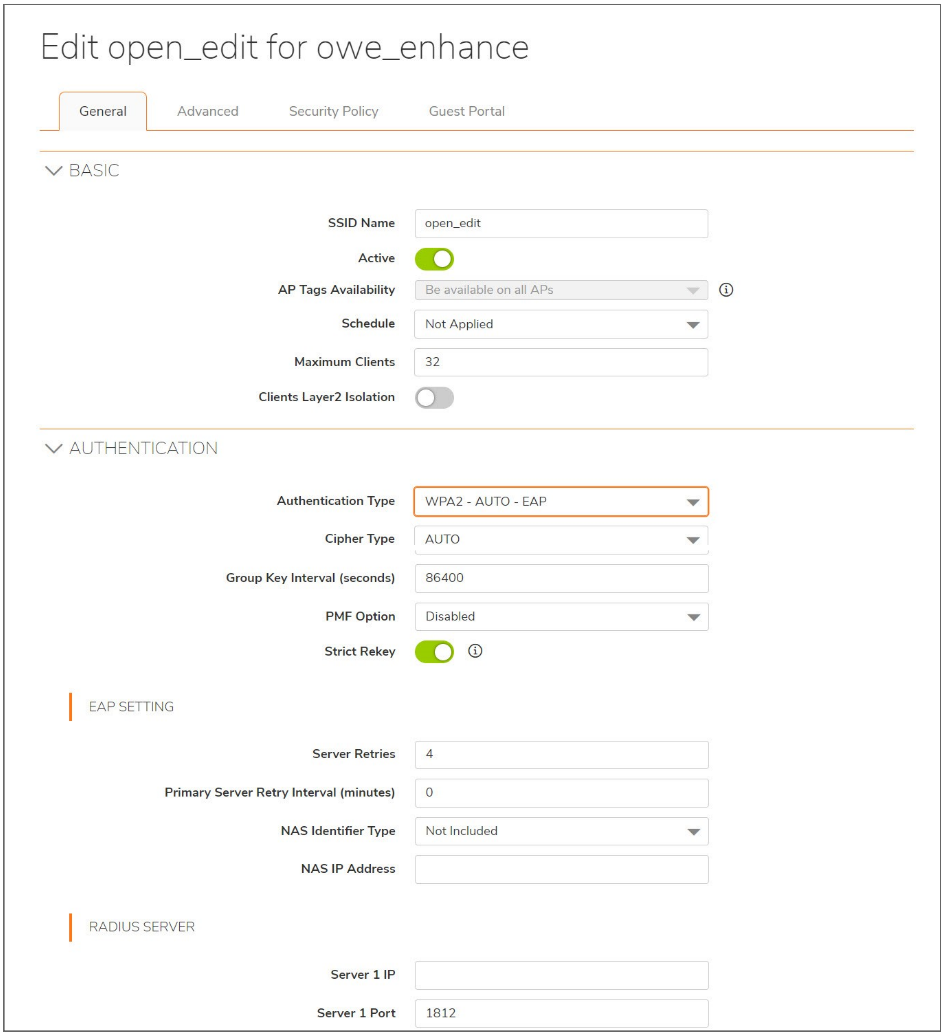
OTHERS

Hide SSID in Beacon: off

WDS Access Point: off

VLAN

The **Edit SSID** page can also be used to configure the RADIUS Accounting Server. This configuration option is available on the **Policies > SSID Policies > Edit > SSID Edit screen**.



Edit open_edit for owe_enhance

BASIC

SSID Name	open_edit
Active	on
AP Tags Availability	Be available on all APs
Schedule	Not Applied
Maximum Clients	32
Clients Layer2 Isolation	off

AUTHENTICATION

Authentication Type	WPA2 - AUTO - EAP
Cipher Type	AUTO
Group Key Interval (seconds)	86400
PMF Option	Disabled
Strict Rekey	on

EAP SETTING

Server Retries	4
Primary Server Retry Interval (minutes)	0
NAS Identifier Type	Not Included
NAS IP Address	

RADIUS SERVER

Server 1 IP	
Server 1 Port	1812

General

Selecting an SSID displays the **General** page with these sections:

- Basic
- Authentication
- Others
- VLAN

Some of the fields on this page are read-only, and some require information.

Basic

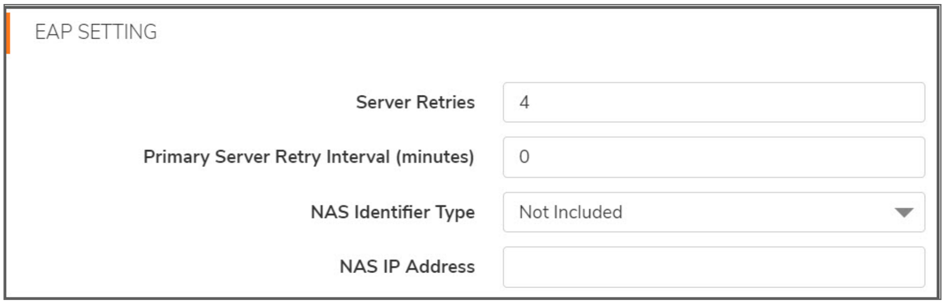
- **SSID Name** - This is populated with the name of the SSID you selected in the middle pane.
- **Active** - This toggle indicates whether the SSID is active or not.
- **AP Tags Availability** - From the AP Tags Availability list, select the tag(s) you want to apply to the SSID.
- **Schedule** - In this field, you can select a schedule for this SSID among those you have created, or you can leave it **Not Applied**.
- **Maximum Clients** - The maximum clients this SSID can service is usually fixed.
- **Clients Layer 2 Isolation** - Selecting this option adds Layer 2 Isolation.

Authentication

- **Authentication Type** - This field allows you to choose an authentication type for the SSID.
- **Cipher Type** - Auto is the only choice for the cipher type in this case.
- **Group Key Interval (seconds)** - Select this option for the Group Key Interval in seconds.
- **PMF Option** - The PMF option can be enabled, disabled, or required.
- **Strict rekey** - Disabling the strict rekey process can potentially help improve connectivity in environments with a lot of wireless interference.
- **PSK Type** - Choose **Unique PSK**, **Multiple PSK**, **Multiple PSK with Radius** using the radio button. When multiple PSK is selected, you need to add a client PSK setting. Click the + icon from **MULTIPLE PSK** to add client PSK global policy. From the **Client MAC Address Group** dropdown, choose the desired policy and enter the passphrase. Click **Add** to continue.

  ⓘ | **NOTE:** To assign VLAN ID, you need to enable VLAN.

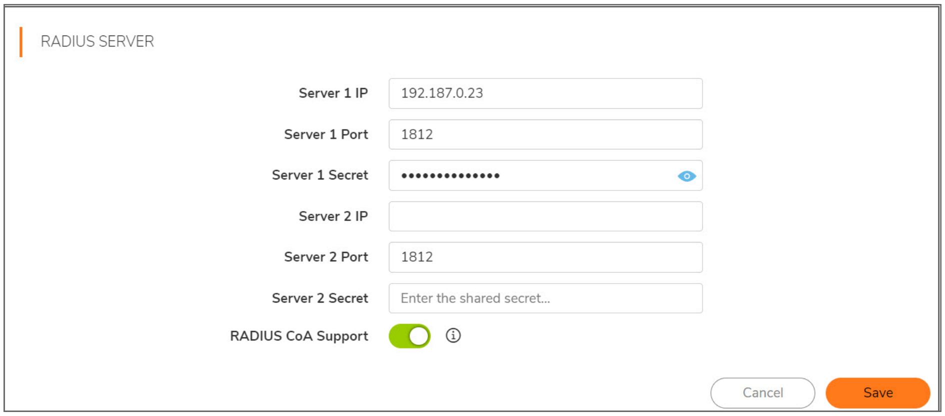
  If you choose Multiple PSK with Radius, you need to input **EAP Setting** options like number of server tries, primary server retry interval (in minutes), NAS identifier, NAS IP Address.

  EAP SETTING

Server Retries	4
Primary Server Retry Interval (minutes)	0
NAS Identifier Type	Not Included
NAS IP Address	

  For **Radius Server** and **Radius Accounting Server**, the Server IP address for the respective ports and server secret key has to be provided.



RADIUS SERVER

Server 1 IP: 192.187.0.23

Server 1 Port: 1812

Server 1 Secret: ••••••••••••••

Server 2 IP:

Server 2 Port: 1812

Server 2 Secret: Enter the shared secret...

RADIUS CoA Support: On

- **Passphrase** -A passphrase is required before you can complete any configuration changes.

Disabling the Strict Rekey

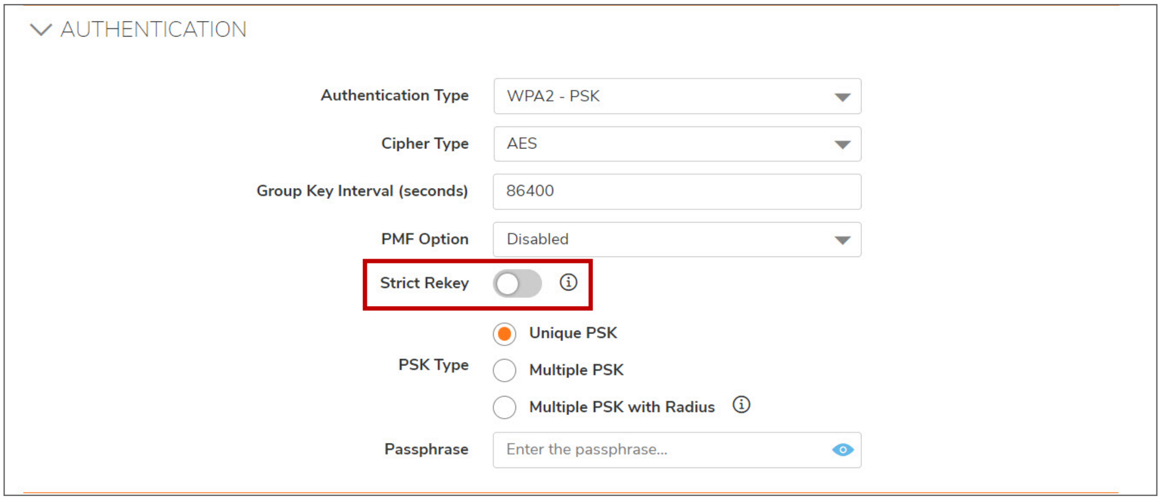
When there is a lot of wireless interference, the connection to SonicWave can encounter performance issues. Disabling the strict rekey process can potentially help improve connectivity in those environments.

To disable the strict rekey:

1. Navigate to **Policies > Policy Hierarchy**.
2. Select an SSID policy.
3. Select the **General** tab.
4. In the **Authentication** section, click **Strict Rekey** to the off position.

   ⓘ | **NOTE:** The **Strict Rekey** option is only available for WPA-PSK and WPA-EAP settings.

ⓘ | **IMPORTANT:** While disabling **Strict Rekey** can improve connectivity when there is significant wireless interference, it provides a less secure connection.



AUTHENTICATION

Authentication Type: WPA2 - PSK

Cipher Type: AES

Group Key Interval (seconds): 86400

PMF Option: Disabled

Strict Rekey: Off

PSK Type: ● Unique PSK ○ Multiple PSK ○ Multiple PSK with Radius

Passphrase: Enter the passphrase...

Others

- **Hide SSID in Beacon** - This is an option for the activation/deactivation of visibility.
- **WDS Access Point** - This selection shows whether this access point is part of a WDS (Wireless Distribution System). A WDS is a method for extending the reach of a network of access points by making some of them dependent on others.

VLAN

The VLAN option provides the ID for the VLAN to be used only in Bridge mode.

Dynamic VLAN Support

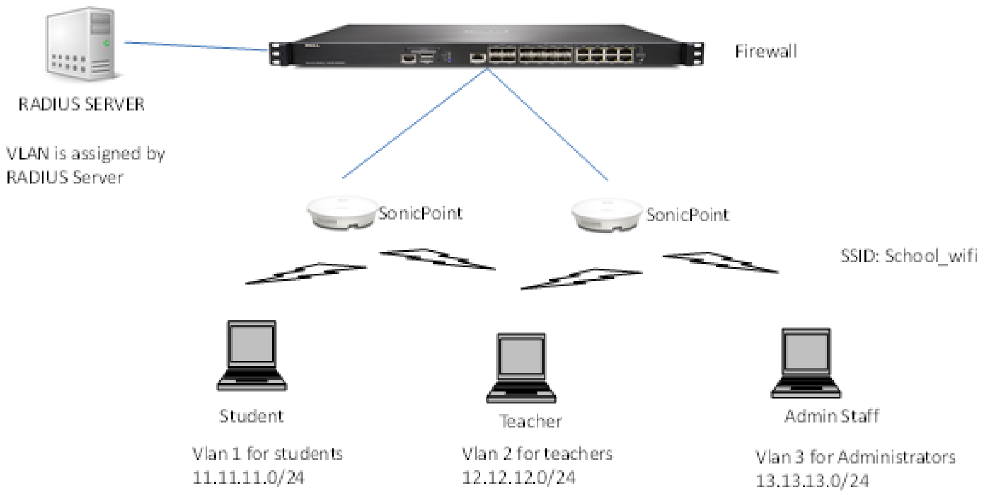
Dynamic VLAN support allows wireless clients to connect to access points using the same SSID (EAP) broadcasted by multiple SonicWave wireless access points. Wireless clients are assigned to different VLAN subnet by the RADIUS server according to their user groups and RADIUS server policy. Wireless clients do not need to connect to a specified SSID for their user group.

The RADIUS server assigns a VLAN ID to a user based on these attributes:

- IETF 64 (Tunnel Type): this is set to VLAN.
- IETF 65 (Tunnel Medium Type): this is set to 802.
- IETF 81 (Tunnel Private Group ID): this is set to VLAN ID.

In this example, only one SSID is broadcasted school-wide. Students, teachers, administration staff all connect to same SSID. The RADIUS server assigns them to different zones or subnets based on their login ID.

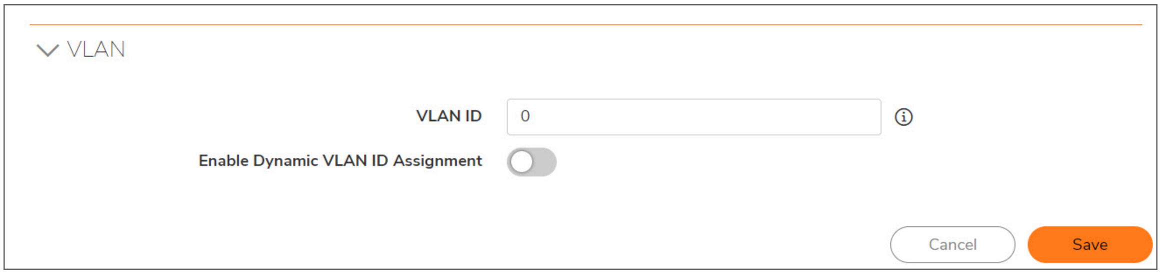
DYNAMIC VLAN EXAMPLE



To configure dynamic VLAN settings:

1. Navigate to the **Polices > Policy Hierarchy** page.
2. Select an existing SSID or create a new one.
3. In the **Authentication** section, set the **Authentication Type** to one of the **WPA - EAP** authentication types.

   ⓘ **NOTE:** Dynamic VLAN SSIDs can only be configured when the authentication type is set to one of **WPA - EAP** authentication types.
4. In the **VLAN** section, set the VLAN IDs. Toggle the button on or off to enable or disable Dynamic VLAN ID Assignment.



VLAN ID: 0

Enable Dynamic VLAN ID Assignment: ○ off

Advanced

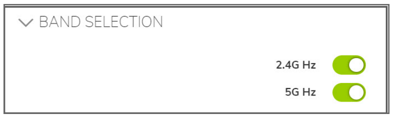
All of the selections on the **Advanced** page can be toggled to enable and disable specific features.

Topics:

- Band Selection
- IEEE802.11R
- IEEE 802.11K
- IEEE802.11V
- SSL-VPN Security Tunnel Access
- DNS
- Agile Multiband

Band Selection

- **2.4G Hz** - You can choose either band or both for this SSID.
- **5G Hz** - You can choose either band or both for this SSID.

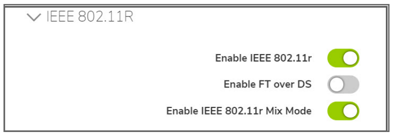


2.4G Hz: ● on

5G Hz: ● on

IEEE802.11R

- **Enable IEEE 802.11r**



IEEE 802.11R

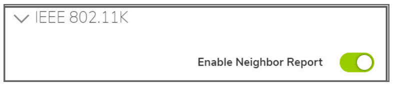
Enable IEEE 802.11r ☑

Enable FT over DS ☐

Enable IEEE 802.11r Mix Mode ☑

IEEE 802.11K

- **Enter Neighbor Report**

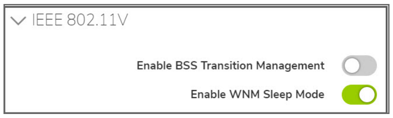


IEEE 802.11K

Enable Neighbor Report ☑

IEEE802.11V

- **Enable BSS Transition Management**
- **Enable WNM Sleep Mode**



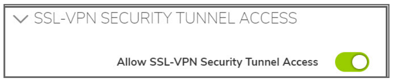
IEEE 802.11V

Enable BSS Transition Management ☐

Enable WNM Sleep Mode ☑

SSL-VPN Security Tunnel Access

- **Allow SSL-VPN Security Tunnel Access**



SSL-VPN SECURITY TUNNEL ACCESS

Allow SSL-VPN Security Tunnel Access ☑

DNS

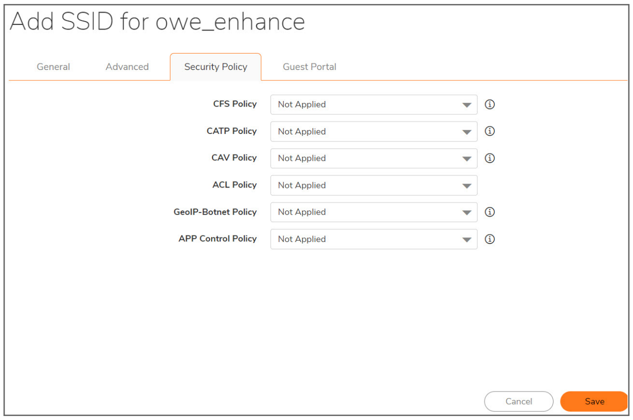
- **Proxy Client DNS Request On Bridge Mode**

Agile Multiband

- **Enable Multiband (MBO)**
- **Association Disallowed (MBO)**

Security Policies

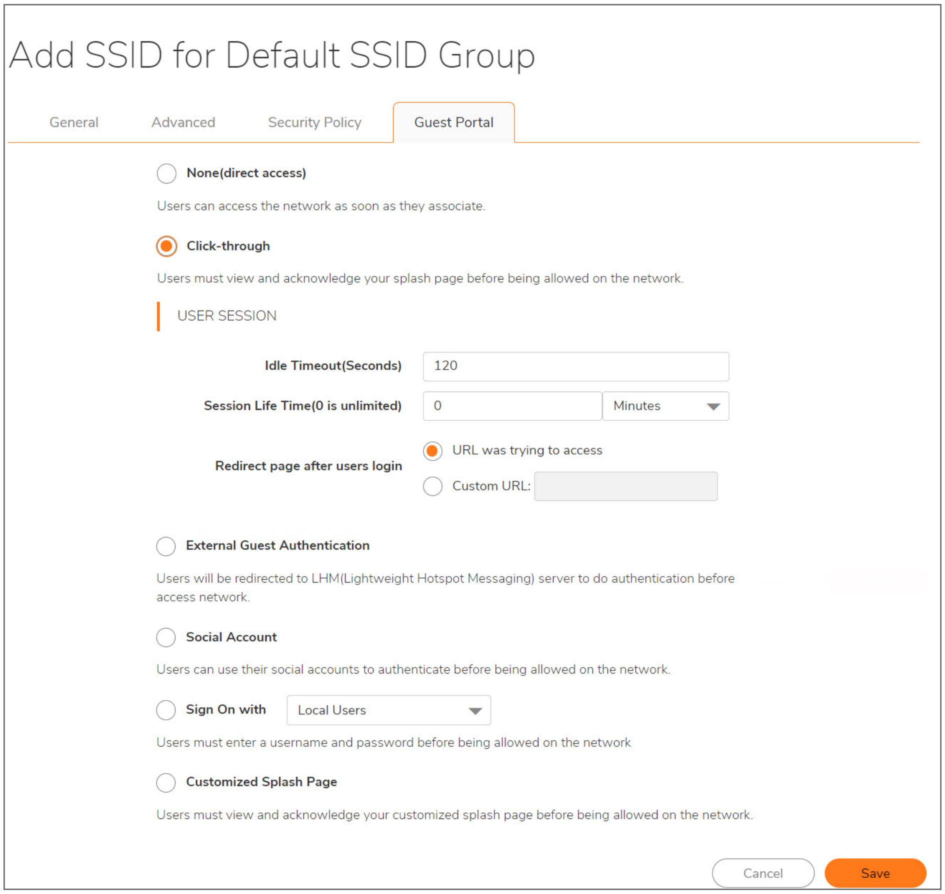
The **Security Policies** tab allows you to select which security policies to apply to this SSID. Some of the security policies might have several versions, created to be applied separately to SSIDs or groups of SSIDs. All of the policies configured on your network are available for activation.



CFS Policy	Not Applied
CATP Policy	Not Applied
CAV Policy	Not Applied
ACL Policy	Not Applied
GeoIP-Botnet Policy	Not Applied
APP Control Policy	Not Applied

Guest Portal

From the **Guest Portal** page you can choose the type of authentication to require of users wanting to sign on to a session, and the details of the session. You can choose what type of access you will allow and which type of credentials must be presented. When you click in the box next to the access type, more access and user session options appear.



○ None(direct access)

Users can access the network as soon as they associate.

● Click-through

Users must view and acknowledge your splash page before being allowed on the network.

USER SESSION

Idle Timeout(Seconds) 120

Session Life Time(0 is unlimited) 0 Minutes

Redirect page after users login ● URL was trying to access ○ Custom URL:

○ External Guest Authentication

Users will be redirected to LHM(Lightweight Hotspot Messaging) server to do authentication before access network.

○ Social Account

Users can use their social accounts to authenticate before being allowed on the network.

○ Sign On with Local Users

Users must enter a username and password before being allowed on the network

○ Customized Splash Page

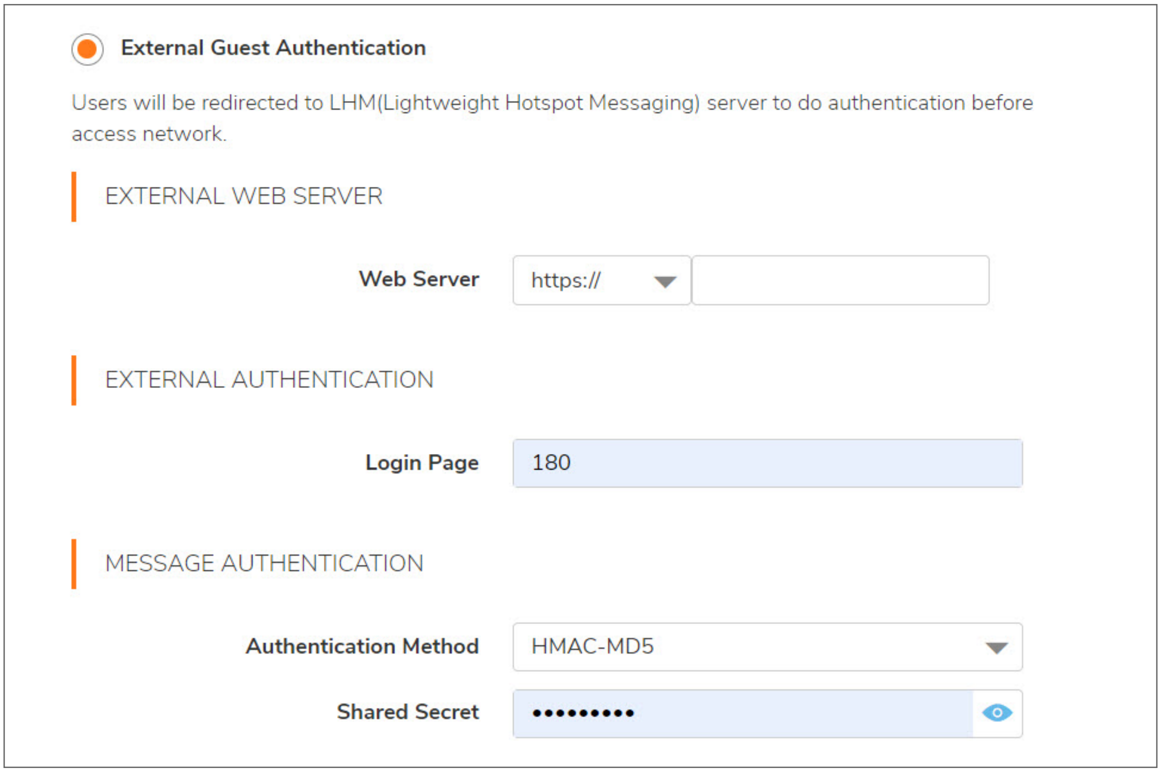
Users must view and acknowledge your customized splash page before being allowed on the network.

For this service, there is a customized screen for Cloud Captive Portal and Guest Services support. A captive portal is a web page (also called a splash screen) displayed before the guests can access the Internet using a desktop or mobile device. Captive portals allow administrators to block Internet access until the guest has completed some defined process, such as looking at an acceptable use policy screen and clicking on a button indicating agreement to the terms of the policy.

If the guest user attempts to access any other pages before successful authentication has been completed, they will be redirected back to the authentication page.

Currently Wireless Network Manager supports the following six authentication methods, as seen on the screen above:

- **None (direct access)** - If this method is selected, there is no authentication.
- **Click-through** - The user must view and acknowledge your splash page.
- **External Guest Authentication** - The user is redirected for outside authentication.



● External Guest Authentication

Users will be redirected to LHM(Lightweight Hotspot Messaging) server to do authentication before access network.

EXTERNAL WEB SERVER

Web Server: https://

EXTERNAL AUTHENTICATION

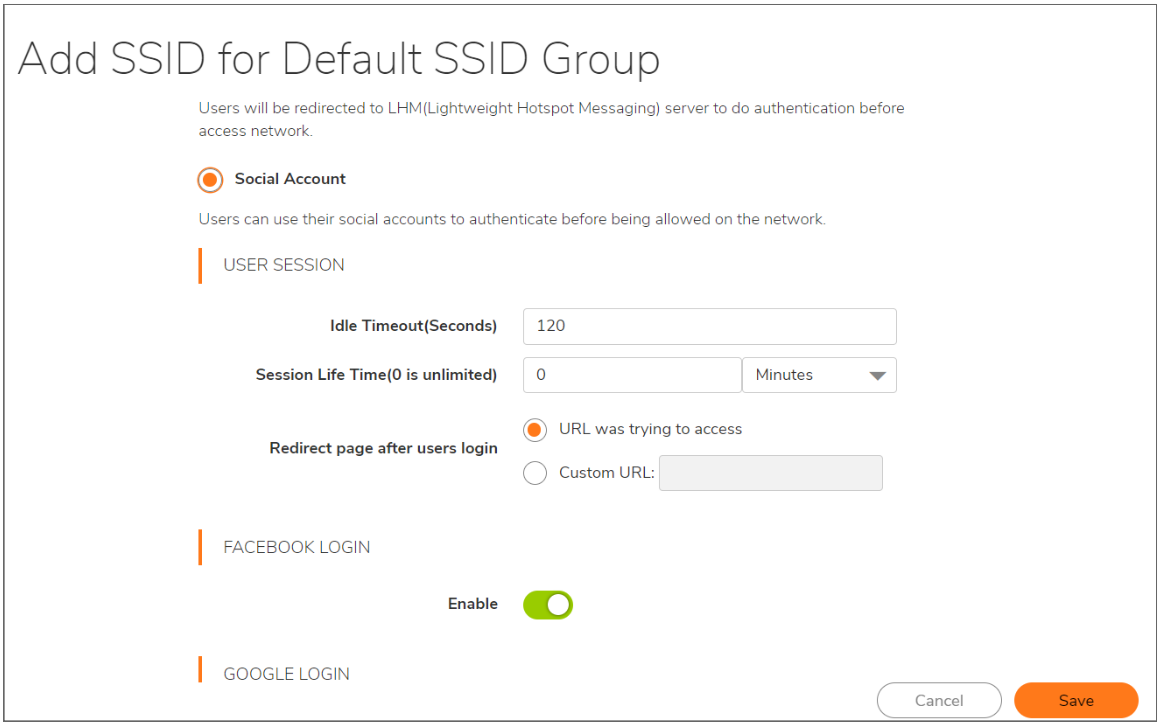
Login Page: 180

MESSAGE AUTHENTICATION

Authentication Method: HMAC-MD5

Shared Secret: ●●●●●●●●●

- **Social Account** - The social account splash page is shown below:



Add SSID for Default SSID Group

Users will be redirected to LHM(Lightweight Hotspot Messaging) server to do authentication before access network.

● Social Account

Users can use their social accounts to authenticate before being allowed on the network.

USER SESSION

Idle Timeout(Seconds): 120

Session Life Time(0 is unlimited): 0 Minutes

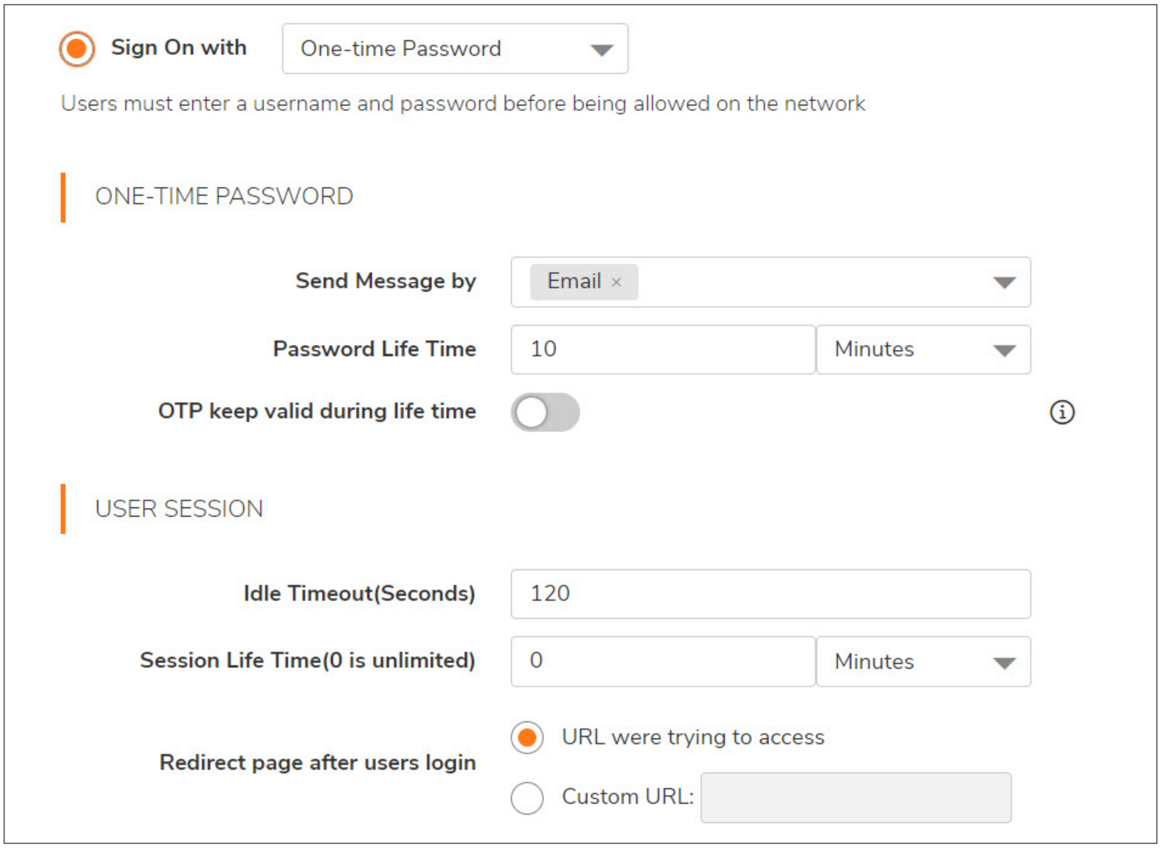
Redirect page after users login: ● URL was trying to access ○ Custom URL:

FACEBOOK LOGIN

Enable

GOOGLE LOGIN

- **Sign On with -** The user must enter a user name and password before being allowed on the network.



● Sign On with: One-time Password

Users must enter a username and password before being allowed on the network

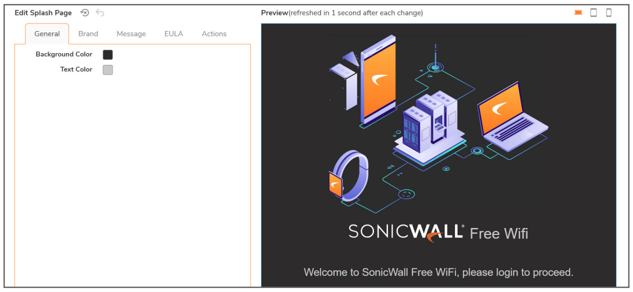
ONE-TIME PASSWORD

Send Message by	Email ×
Password Life Time	10 Minutes
OTP keep valid during life time	

USER SESSION

Idle Timeout(Seconds)	120
Session Life Time(0 is unlimited)	0 Minutes
Redirect page after users login	● URL were trying to access ○ Custom URL:

- **Customized Splash Page** - The user must view and acknowledge your customized splash page before being allowed on the network.



Edit Splash Page

Background Color ■

Text Color □

Preview(refreshed in 1 second after each change)

SONICWALL Free Wifi

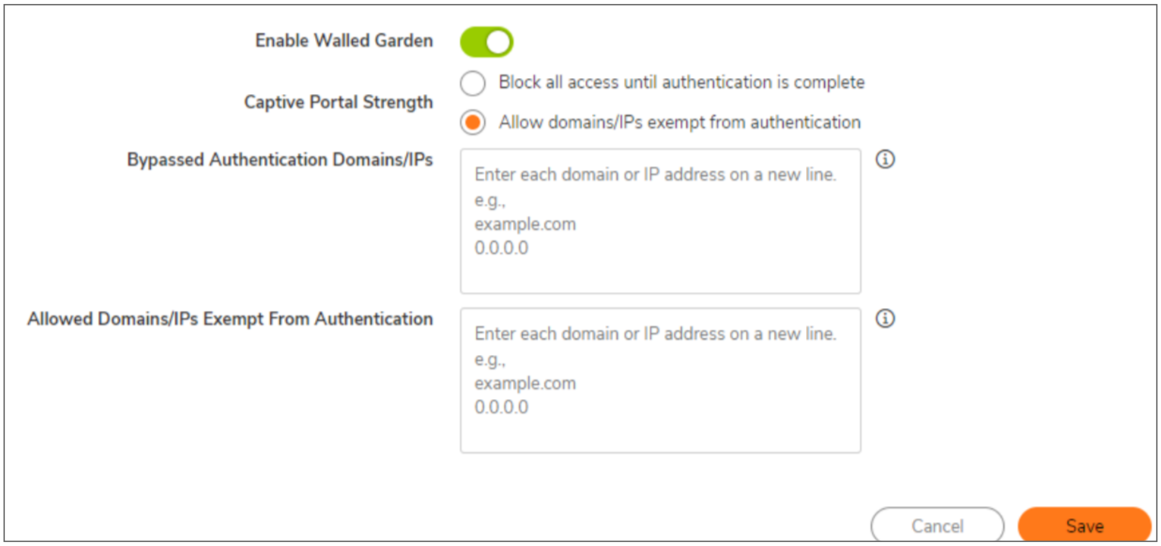
Welcome to SonicWall Free WiFi, please login to proceed.

- **Advanced** - This option is displayed if you do not select **None** from the **Basic** options.

  Enable the toggle bar for **Enable Walled Garden**, if required.

  A walled garden is a user interface function that helps the end user to create an allowed list of URLs and IP addresses that users of a captive portal is allowed to access prior to authentication. For example, to allow patrons of a restaurant connect to the Wi-Fi, and browse the restaurant's menu pages prior to their gaining full internet access via registering an email address or logging in via social media.

  Select the Captive Portal Strength radio button **Block all access until the authentication is complete** and provide the list in the box **Bypassed Authentication Domains and IPs**. If you select the option **Allow Domains/IPs Exempt from Authentication**, provide the list in that box.



Enable Walled Garden

Captive Portal Strength ○ Block all access until authentication is complete
● Allow domains/IPs exempt from authentication

Bypassed Authentication Domains/IPs

Enter each domain or IP address on a new line.
e.g.,
example.com
0.0.0.0

Allowed Domains/IPs Exempt From Authentication

Enter each domain or IP address on a new line.
e.g.,
example.com
0.0.0.0

Click **OK** to apply your selections.

Sign-on Settings

While you edit SSID Policy, the **Guest Portal** tab provides different sign-on options that are described further.

Topics:

- Sign-on with One-Time Passwords
- Sign-on with Local Users Authentication
- Sign-on with RADIUS Server Authentication
- Sign-on with LDAP Server Authentication
- Sign-on with Active Directory Server Authentication
- User Authentication through Totp
- Sign-on with SAML Authentication

Sign-on with One-Time Passwords

Customers must get their one-time password by email or SMS before being allowed to connect to the network.

To use One-Time Password authentication for sign-on:

1. Navigate to **Policies > Policy Hierarchy**.
2. Click on the **SSID Policy**.
3. Hover over right section of the line of the SSID you want to configure. When the icons appear, click the **Edit** (pencil) icon. The **Edit SSID** page displays.
4. Click the **Guest Portal** tab.
5. Select **Sign On with**.
6. Select **One-time Password** from the list.
7. In the **One-Time Password** section, enter whether the one-time password should be delivered by twilio billing for SMS.

ⓘ **NOTE:** To use SMS to send one-time passwords, must Configuring Twilio Billing for SMS on the **General > Settings** page.

Configuring Twilio Billing for SMS

To configure Twilio billing for SMS:

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

You will now be billed on a per-SMS basis via Twilio. Prices can range by country; the typical cost per SMS ranges from $0.01 per SMS for the United States to over $0.10 per SMS for certain carriers in Europe. A complete, up-to-date pricing list is available at https://www.twilio.com/sms/pricing#outbound-pricing.

Sign-on with LDAP Server Authentication

To use LDAP server authentication for sign-on:

1. Navigate to **Policies > Policy Hierarchy**.
2. Click on an **SSID Policy**.
3. Hover over right section of the line of the SSID you want to configure. When the icons appear, click the **Edit** (pencil) icon. The **Edit SSID** page displays.
4. Click the **Guest Portal** tab.
5. Select **Sign On with**.
6. Select the LDAP server you want to use for authentication.
7. In the **LDAP Server** section, configure the settings as required for your organization.

Sign-on with Active Directory Server Authentication

To use Active Directory server authentication for sign-on:

1. Navigate to **Policies > Policy Hierarchy**.
2. Click on **SSID Policy**.
3. Hover over right section of the line of the SSID you want to configure. When the icons appear, click the **Edit** (pencil) icon. The **Edit SSID** page displays.
4. Click the **Guest Portal** tab.
5. Select **Sign On with**.
6. Select the Active Directory server you want to use for authentication.
7. In the **Active Directory Server** section, configure the settings as required for your organization.

Sign-on with RADIUS Server Authentication

ⓘ **NOTE:** Customers must sign in using their RADIUS username and password before being allowed to connect to the network.

After a user enters their username and password:

1. Those credentials will be passed to the SonicWave.
2. The SonicWave will create a RADIUS authentication packet and send it to the RADIUS server.
    - If the RADIUS server successfully authenticates the credentials: it replies with a `Access-Accept` packet to the SonicWave.
    - If the RADIUS server cannot authenticate the credentials: it replies with a `Access-Reject` packet to the SonicWave.

These RADIUS authentication methods are supported:

- PAP
- CHAP

- MSCHAPv1
- MSCHAPv2

The RADIUS server must be configured for at least one of those methods.

ⓘ | **NOTE:** MSCHAPv1 or MSCHAPv2.is recommended.

The SonicWave will first attempt to send the RADIUS packet using MSCHAPv2 and MSCHAPv1 authentication. If both of those authentication methods fail, it will then attempt to send the RADIUS packet using CHAP and PAP authentication.

To use RADIUS Directory server authentication for sign-on:

1. Navigate to **Policies > Policy Hierarchy**.
2. Click on **SSID Policy**.
3. Hover over right section of the line of the SSID you want to configure. When the icons appear, click the **Edit** (pencil) icon. The **Edit SSID** page displays.
4. Click the **Guest Portal** tab.
5. Select **Sign On with**.
6. Select the My RADIUS Server you want to use for authentication.
7. In the **RADIUS Server** section, configure the settings as required for your organization.

Sign-on with SAML Authentication

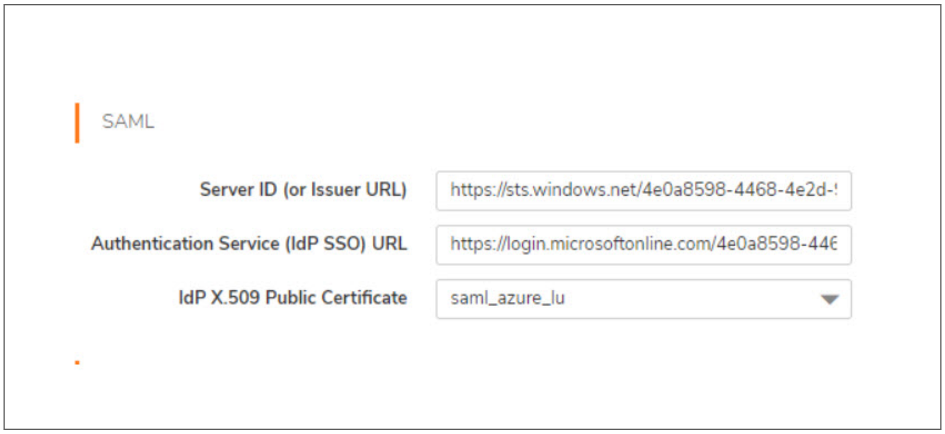
When creating IDP application on SAML provider, following SSO URL and SP Entity ID needs to be provided.

Reply URL (Assertion Consumer Service URL): https://auth.mysonicwave.com/lhmapi/saml/?acs

Identifier (Entity ID): https://auth.mysonicwave.com/lhmapi/saml/metadata/

To use SAML authentication for sign-on:

1. Navigate to **Policies > SSID Policies**.
2. Click on the **SSID Policy**.
3. Hover over right section of the line of the SSID you want to configure. When the icons appear, click the **Edit** (pencil) icon. The **Edit SSID** page displays.
4. Click the **Guest Portal** tab.
5. From **Sign On with** dropdown, select **SAML**. Input the URL in Server ID and Authentication Service. Choose the certificate from the list.



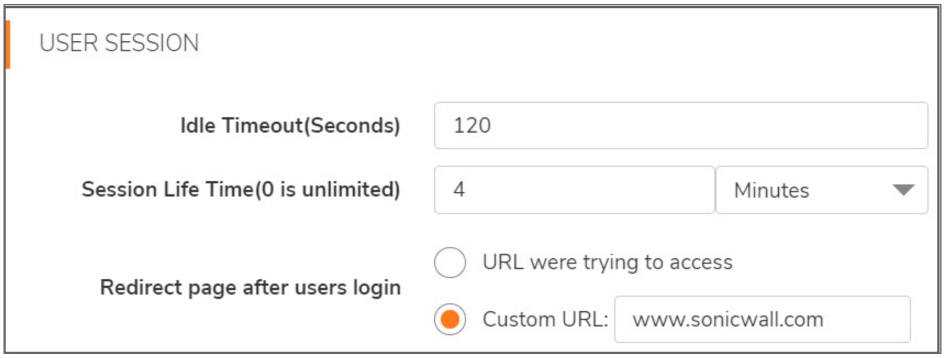
SAML

Server ID (or Issuer URL): https://sts.windows.net/4e0a8598-4468-4e2d-!

Authentication Service (IdP SSO) URL: https://login.microsoftonline.com/4e0a8598-446

IdP X.509 Public Certificate: saml_azure_lu

6. From **USER SESSION**, enter Idle Timeout (in seconds) and Session Life time (in minutes).
7. You can choose to redirect the users to a URL you were trying to access or to a custom URL.



USER SESSION

Idle Timeout(Seconds): 120

Session Life Time(0 is unlimited): 4 Minutes

Redirect page after users login:
○ URL were trying to access
● Custom URL: www.sonicwall.com

Wireless Guest TOTP Authentication

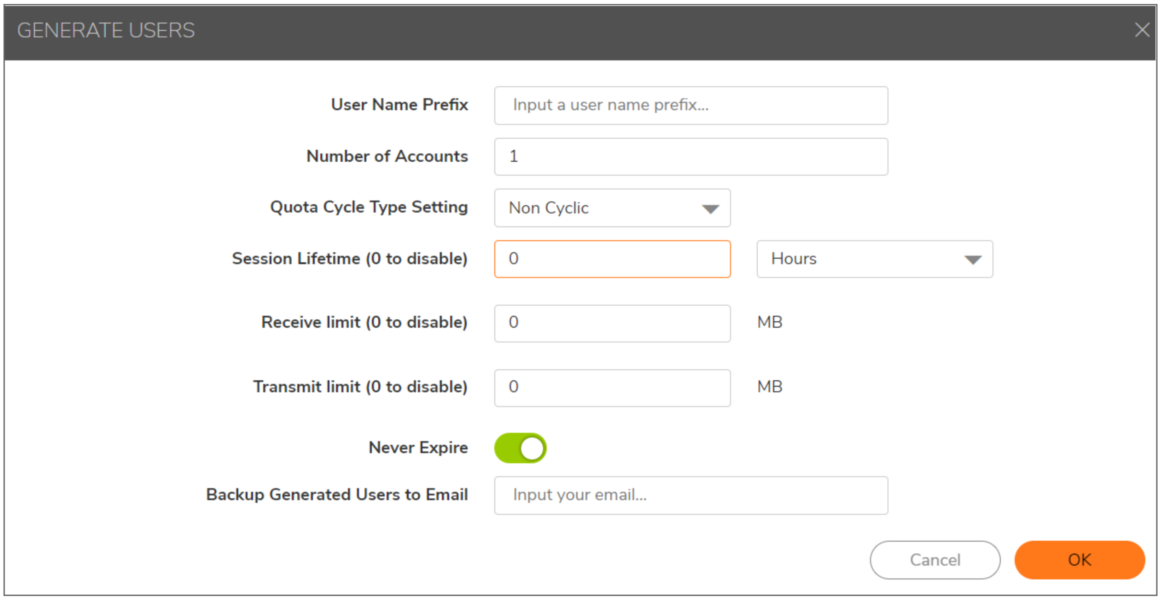
The Time-Based One Time Password is a multi-factor authentication scheme that enabled third party integration to generate secure time-based OTP via third party authentication Apps such as Google authenticator, Microsoft authenticator etc.

TOTP is an alternative to traditional two-factor authentication methods. TOTP passwords keep on changing and are valid for only short window in time, because of which TOTP is considered more secure OTP solution. Before logging into guest authentication, you need to make sure to have an active internet service to view the code in the application.

To generate Totp User:

1. Navigate to **Admin > Users**. Select **Time-based-One-time-Password.**
2. Click 👥 add icon on the right view of the screen.
3. Enter the details of the user

- **User Name Prefix** - Enter the username.
- **Number of Accounts** - Specify the number of accounts (in numbers).
- **Quota Cycle Type Setting** - From the Quota cycle type setting list, select:
  - Non Cyclic (default)
  - Per Day
  - Per Week
  - Per Month
- **Session Lifetime (0 to disable)** - Specify the duration for how long a guest login session remains active after it has been activated. By default, activation occurs the first time a guest user logs into an account. The field cannot exceed 4 characters.
- **Receive Limit (0 to disable)** - Enter the amount (in MB) the amount of data the user can receive. The range is from 0 (unlimited) to 999999999 MB to maximum (the field cannot exceed 9 characters). If the set value is zero, the limit is disabled and it works as unlimited.
- **Transmit Limit (0 to disable)** - Enter the amount (in MB) the amount of data the user can receive. The range is from 0 (unlimited) to 999999999 MB to maximum (the field cannot exceed 9 characters). If the set value is zero, the limit is disabled and it works as unlimited.
- **Backup Generated Users to Email** - Enter an email address to receive the code. Please note that an active internet connection is needed to receive the code.
- Click **OK**.



GENERATE USERS

User Name Prefix	Input a user name prefix...	
Number of Accounts	1	
Quota Cycle Type Setting	Non Cyclic	
Session Lifetime (0 to disable)	0	Hours
Receive limit (0 to disable)	0	MB
Transmit limit (0 to disable)	0	MB
Never Expire	●	
Backup Generated Users to Email	Input your email...	

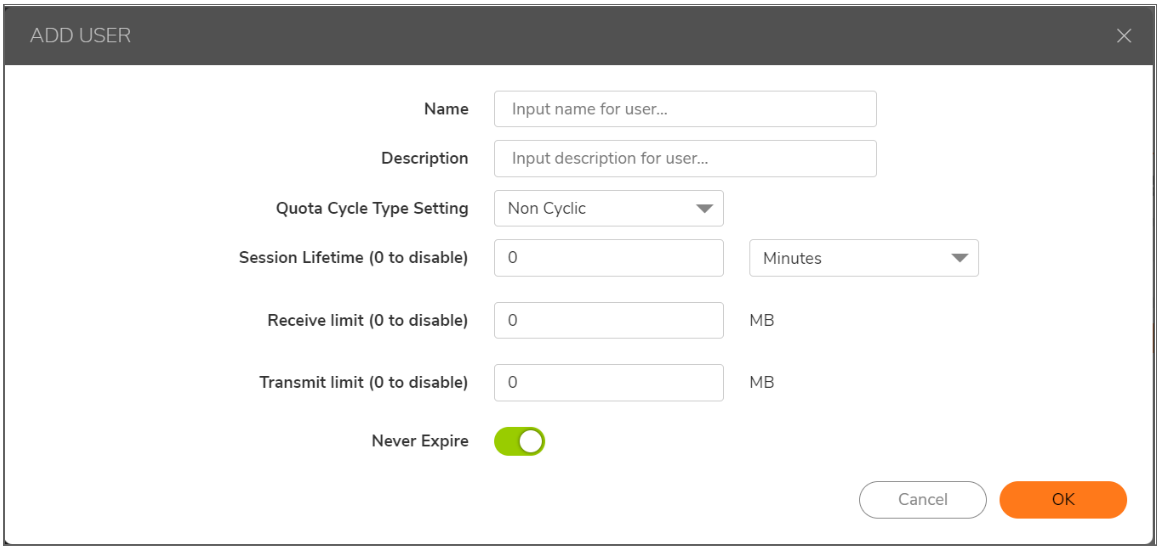
To add Totp User:

1. Navigate to **Users**.
2. Select the tab **Time-based-One-time-Password**.

3. Click add icon on the right view of the screen.

4. Enter the details of the user:

- **Name** - Enter the name of the user.
- **Description** - Enter a description (not mandatory).
- **Password** - Enter the Password. This is mandatory.
- **Quota Cycle Type Setting** - From the Quota cycle type setting list, select:
  - Non Cyclic (default)
  - Per Day
  - Per Week
  - Per Month
- **Session Lifetime (0 to disable)** - Specify the duration for how long a guest login session remains active after it has been activated. By default, activation occurs the first time a guest user logs into an account.
- **Receive Limit (0 to disable)** - Enter the amount (in MB) the amount of data the user can receive. The range is from 0 (no data can be received) to 9999 MB to Unlimited (default). If the set value is zero, the limit is disabled and it works as unlimited.
- **Transmit Limit (0 to disable)** - Enter the amount (in MB) of data the user can send. The range is from 0 (no data can be sent) to 9999 MB to Unlimited (default).
- **Never Expire** - Toggle on or off to set to never expire.
- Click **OK**.



ADD USER

Name: Input name for user...

Description: Input description for user...

Quota Cycle Type Setting: Non Cyclic

Session Lifetime (0 to disable): 0 Minutes

Receive limit (0 to disable): 0 MB

Transmit limit (0 to disable): 0 MB

Never Expire: ●

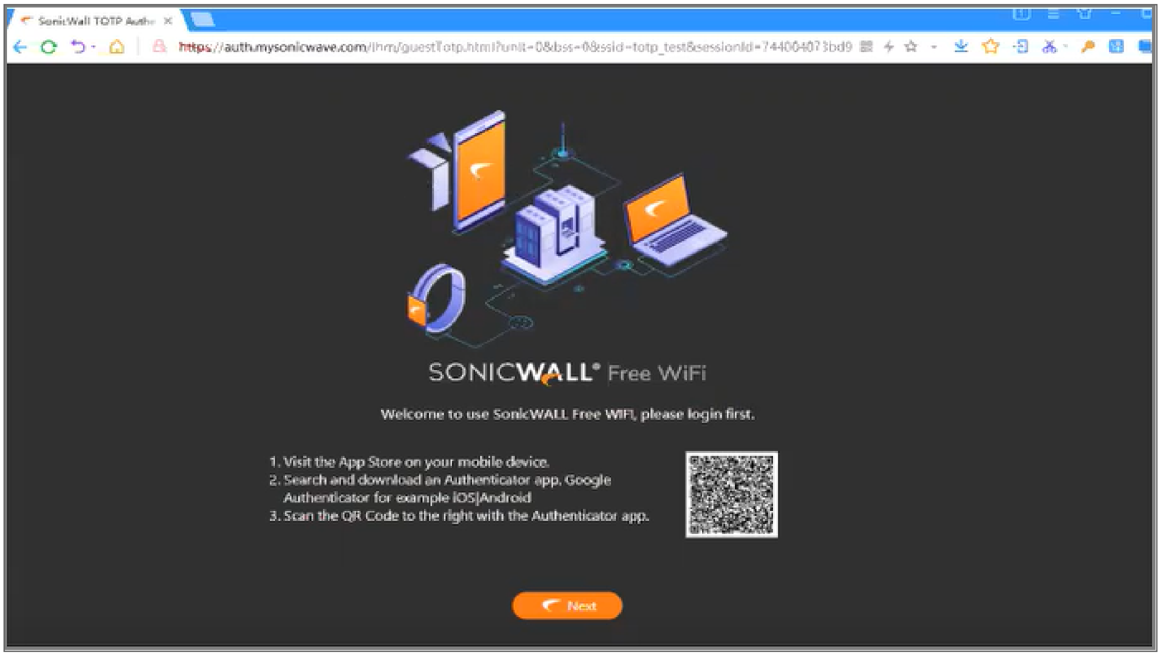
To delete Totp User:

1. Navigate to **Admin > Users**. Select **Time-based-One-time-Password.**
2. Check the box of the user to delete.

3. Click **Delete** icon.

User Authentication through Totp

When the user log in for the first time, a QR code is displayed on the screen. You need to install an authenticator app like Google Authenticator to scan the QR code.


SonicWall TOTP Authe
https://auth.mysonicwave.com/lhm/guestTotp.html?unit=0&bss=0&ssid=totp_test&sessionId=744004073bd9
SONICWALL® Free WiFi

Welcome to use SonicWALL Free WIFI, please login first.

1. Visit the App Store on your mobile device.
2. Search and download an Authenticator app, Google Authenticator for example iOS|Android
3. Scan the QR Code to the right with the Authenticator app.

Once the QR code is scanned, it displays a unique code on your phone screen. Enter the 6 digit code to login.

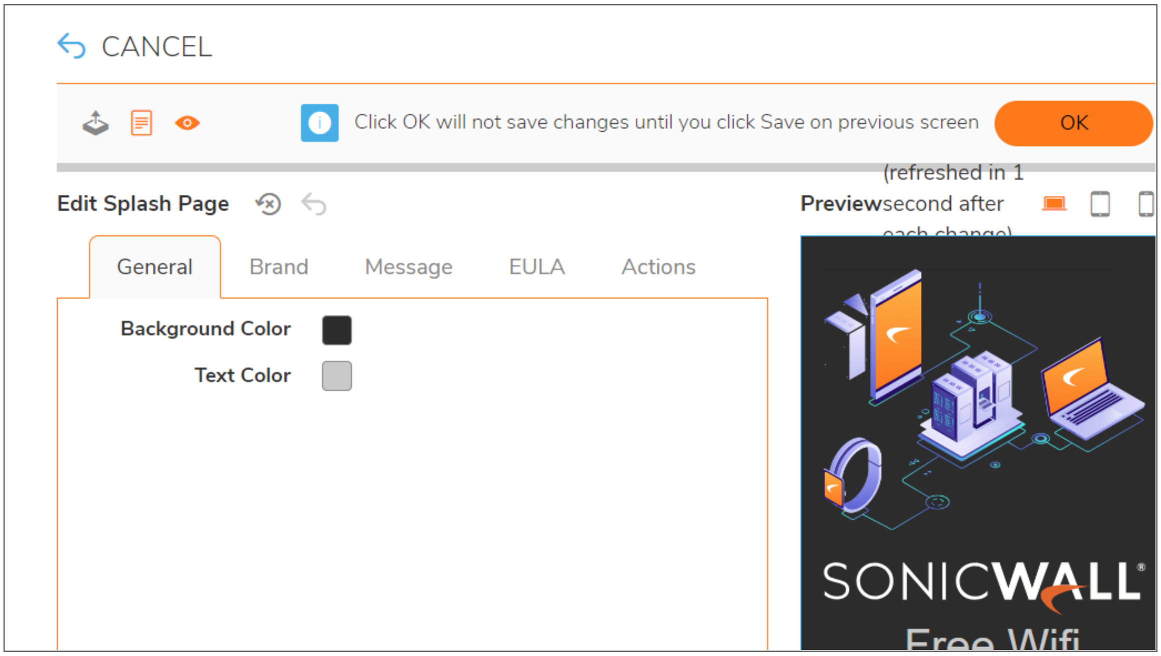
For the subsequent logins, you can specify the user name and login to the guest portal.

ⓘ **NOTE:** To reconnect using the wireless connection again, you need to enter the 6 digit code through the splash screen to login.

Customized Splash Page

On the **Guest Portal** page, click on the edit icon pertaining to the **Customized Splash Page**.

The **Edit Splash Page** is displayed.


CANCEL
Click OK will not save changes until you click Save on previous screen
OK
Edit Splash Page
Preview
(refreshed in 1 second after each change)
General
Brand
Message
EULA
Actions
Background Color
Text Color
SONICWALL
Free Wifi

Click on the **General** tab and set the **Background Color** and **Text Color**.

Click on **Brand** tab and set the **Poster**, **Logo**, and **Custom HTML** options.

Click on **Message** tab and enable the text message.

Click on **EULA** tab and enable the EULA options, if required.

Click on the **Actions** tab and specify the **Input Fields** and **Buttons**.

Enhancements to customizing the splash page include:

- Use a Linked Image on the Customized Splash Page
- Collect User Feedback from a Customized Splash Page

Use a Linked Image on the Customized Splash Page

You can now use a linked image instead of a static image on your customized splash page.

To use a linked image:

1. Navigate to the **Policies > Policy Hierarchy** page.
2. Click on an SSID Policy.
3. Hover over right section of the line of the SSID you want to configure. When the icons appear, click the **Edit** (pencil) icon.
4. Select the **Guest Portal** tab.
5. Select **Customized Splash Page**.
6. Click the **Customize Splash Page** (pencil) to the right.

7. Select the **Brand** tab.
8. From the **Poster File** list, select ****use url****.
9. In the field that appears below, enter the URL where the image is located.
10. Click **OK** to save all of your changes.

Collect User Feedback from a Customized Splash Page

You can add a link on the login page that opens a new screen where users can provide their feedback and contact information. You can also enable and customize an end user license agreement and message along with this, clicking on the respective tabs.

To add a user feedback form:

1. Navigate to the **Policies > Policy Hierarchy** page.
2. Click on an SSID Policy.
3. Hover over right section of the line of the SSID you want to configure. When the icons appear, click the **Edit** (pencil) icon.
4. Select the **Guest Portal** tab.
5. Select **Customized Splash Page**.
6. Click the **Customize Splash Page** (pencil) to the right.
7. Select the **Actions** tab.
8. Activate **Feedback Enabled**.
9. Click **OK** to save all of your changes.

Select a Security Policy

Security Policies in the policy hierarchy are represented by their symbols. Each type of Security Policy has a different symbol, which carries through all the pages in Wireless Network Manager. When they are applied to an SSID, the symbol is green.

Clicking the **Security Policy** symbol in the policy hierarchy brings up a page with editable configuration selections the user can pick for that of type of policy.

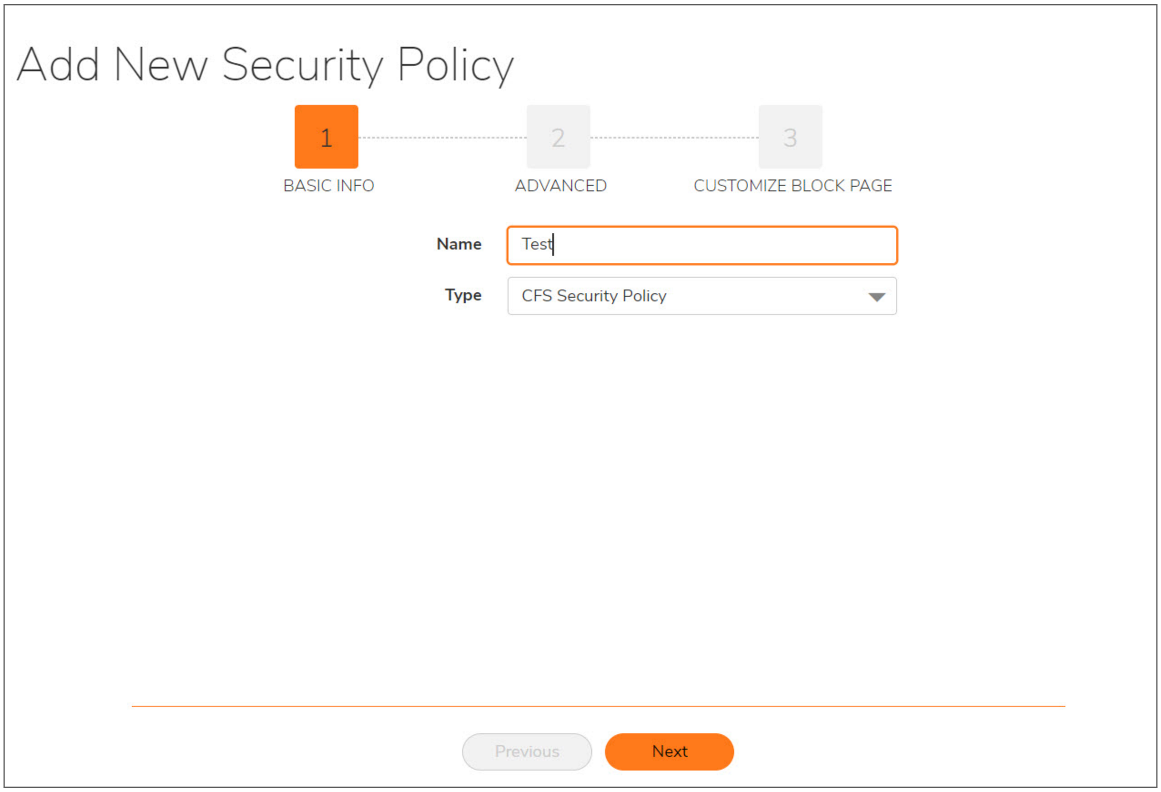
The **Security Policies** page provide you with the options to configure each type of security policy selected from the Policy Hierarchy. For more information, refer to Objects.

Topics:

- CFS (Content Filtering Service)
- CATP (Capture Advanced Threat Protection)
- CAV (Cloud Gateway Anti-Virus)
- ACL
- Geo-IP & Botnet
- APP Control Security Policy

CFS (Content Filtering Service)

Clicking on a CFS policy in the middle pane brings up the Basic Information page displaying the details like **Name**, and **Type** options:



Add New Security Policy

Name: Test

Type: CFS Security Policy

Specify the name and click **Next.**

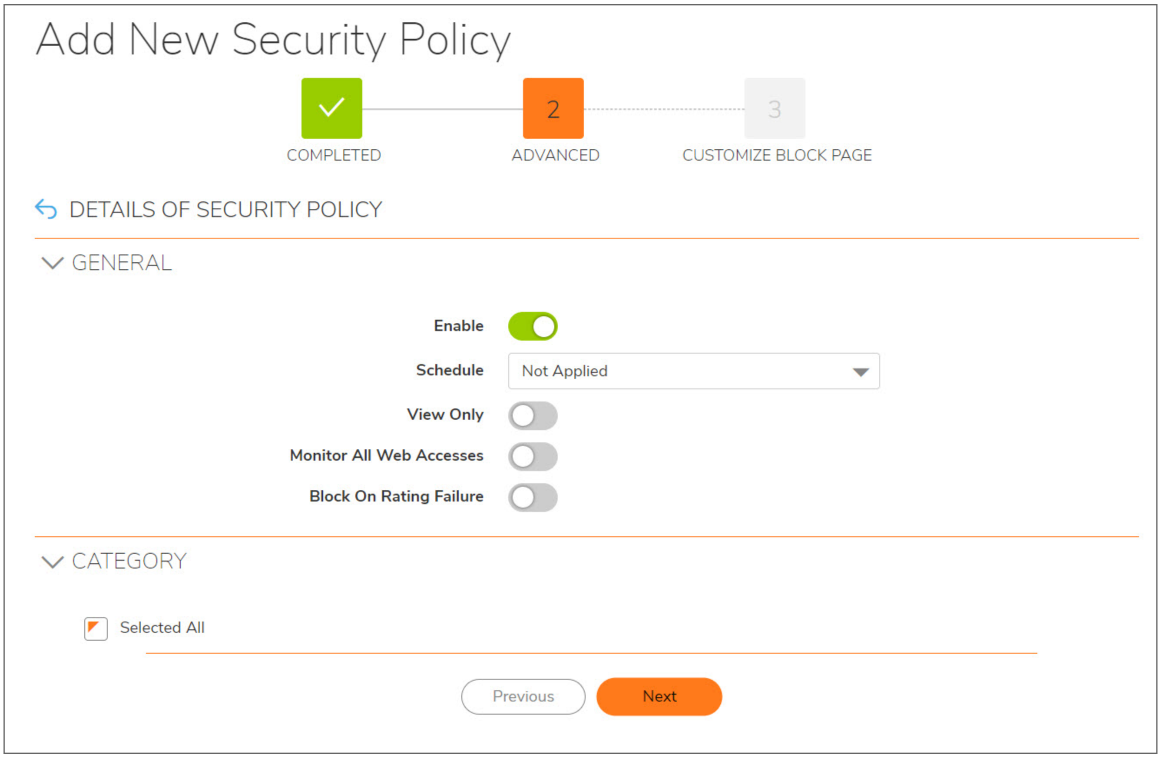
The **Advanced** tab displays the following options:

- General
- Category
- Enabling or Disabling Reputation
- URI List

General

In the **Advanced** tab provide the following details:

- **Enable** - This is a toggle for enabling or disabling this policy.
- **Schedule** - Select the schedule options from the drop-down menu.
- **View Only** - This is a toggle for logging the occurrence of sites with the selected content, but still allowing them to pass through.
- **Monitor All Web Accesses** - Enable this to monitor all the web accesses, and record all the URLs passing through CFS, regardless of whether there is a hit selected category or not.
- **Block on Rating Failure** - Enable this toggle to block on rating failure, if required. When the rating fails, network access that cannot be rated is blocked. For example, like the scenarios when the rating server is closed or unreached.



Enable: on

Schedule: Not Applied

View Only: off

Monitor All Web Accesses: off

Block On Rating Failure: off

Category

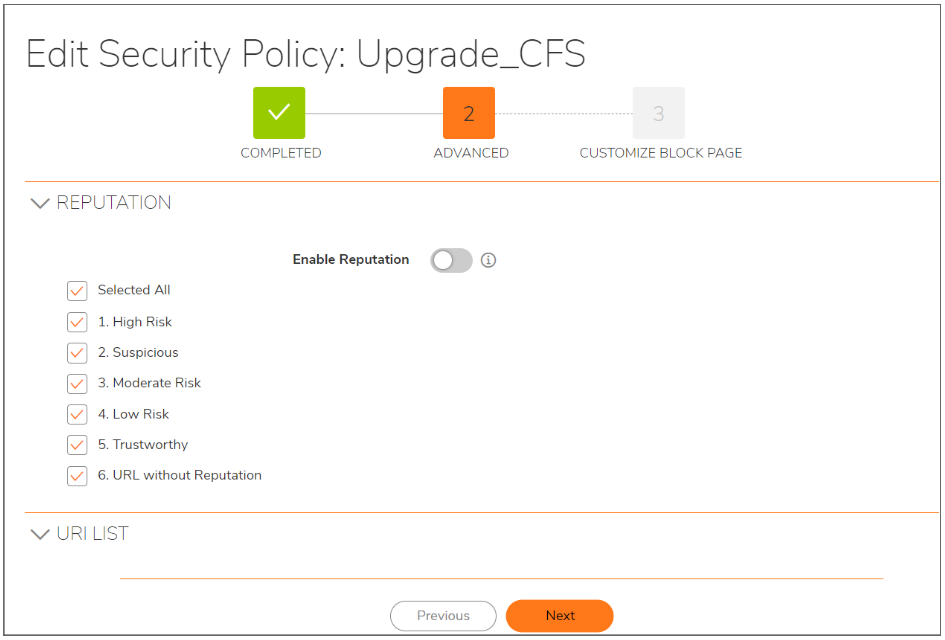
This part of the page has a list of options for types of sites that can be blocked by this policy. Make your selection, or click **Select All** to block files in all the categories listed.

Enabling or Disabling Reputation

You can enable or disable this section by toggling the button to on or off.

ⓘ | **NOTE:** Filtering by reputation will take effect, only if the Category filtering result is enabled.

Select individual options by using the checkbox or select all of the options by clicking **Selected all**.



Edit Security Policy: Upgrade_CFS

Enable Reputation ○

☑ Selected All
☑ 1. High Risk
☑ 2. Suspicious
☑ 3. Moderate Risk
☑ 4. Low Risk
☑ 5. Trustworthy
☑ 6. URL without Reputation

URI List

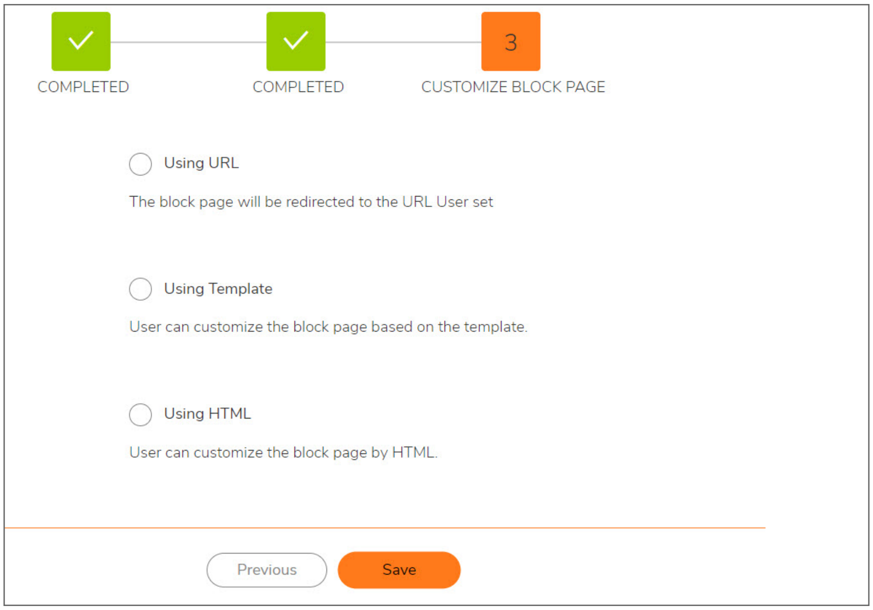
This section of the screen is for the creation of Whitelists and Blacklists.

- An **Allowlist** is a list of URIs that are to be allowed to pass no matter what other security configurations or policies would prevent them from passing.
- A **Blocklist** is a list of URIs that are blocked no matter what. If there is a conflict, Blacklists take priority over Whitelists.

Customize Block Page

You can customize the Block page using URL, Template, or HTML from this page.

Select the required options and click **Save**.



○ Using URL

The block page will be redirected to the URL User set

○ Using Template

User can customize the block page based on the template.

○ Using HTML

User can customize the block page by HTML.

CATP (Capture Advanced Threat Protection)

When you select a CATP (Capture Advanced Threat Protection) policy, it shows the Name and Type fields. Click **Next** to display the options given below:

- General
- File Types
- Protocols
- MD5 Exclusion List

General

- **Enable** - This toggle allows you to enable and disable this policy.
- **Schedule** - Select the required option from the drop down.
- **Block Until Verdict** - This toggle allows you to make a decision about uncertain files. If preprocessing decides that a file is uncertain, it is sent to CATP for further analysis. You can choose to take a chance on the uncertain file if you are confident that it is probably safe, or at least not too dangerous. If you prefer to wait for further analysis to confirm its safety, you can select **Block Until Verdict**.
- **Max File Size (KB)** - the maximum size of files allowed to be downloaded.

  ⓘ **NOTE:** For some SonicWave models, the maximum size will be reduced to 5120KB due to the memory limitations of those specific access points.

File Types

This part of the page has check boxes where you can pick which file types you want supported by CATP. The options include **Archive**, **Executable**, **Microsoft Office**, **Microsoft Office Extended**, and **PDF**.

Protocols

This part of the page lists the protocols that can selected for the CATP policy:

- **HTTP**
- **SMTP**
- **FTP**

MD5 Exclusion List

This part of the page is available for creating lists for exclusion from blocking, or discarding lists that have been created. You can click the add icon and add MD5 Hash to the exclusion list.

Customize Block Page

You can customize the Block page using URL, Template, or HTML from this page. Select the required options and click **Save**.

You can select **None** if you do not need any of these.

CAV (Cloud Gateway Anti-Virus)

This selection is a **Cloud AV Security Policy** named CAV-1. When you select a **CAV** policy, it shows the **Name** and **Type** fields. Click **Next** to display the options given below in the **Advanced** page:

- General
- File Types
- Protocols
- MD5 Exclusion List

General

- **Enable** - This toggle allows you to enable and disable this policy.
- **Schedule** - Select the required option from the drop down.
- **Max File Size (KB)** - the maximum size of files allowed to be downloaded.

  ⓘ **NOTE:** For some SonicWave models, the maximum size will be reduced to 5120KB due to the memory limitations of those specific access points.

File Types

This part of the page has check boxes where you can pick which file types you want supported by CAV. The options are **Archive**, **Executable**, **Microsoft Office**, **Microsoft Office Extended**, and **PDF**.

Protocols

This part of the page lists the protocols that can selected for the CAV policy:

- HTTP
- SMTP
- FTP

MD5 Exclusion List

This part of the page is available for creating lists for exclusion from blocking, or discarding lists that have been created. You can click the add icon and add MD5 Hash to the exclusion list.

Customize Block Page

You can customize the Block page using URL, Template, or HTML from this page. Select the required options and click **Save**.

You can select **None** if you do not need any of these.

ACL

This selection is an ACL policy that is configured on this network. This feature provides Virtual Access Point (VAP) Bandwidth Management control on SonicWave appliances under Wireless Network Manager.

When you select **ACL**, it shows the Name and Type fields. Click **Next** to display the **Advanced** page with the following options:

- General
- Authentication/Association MAC Filtering
- ACL
- Bandwidth Management

General

- **Enable** - This policy can be enabled or disabled.

Authentication/Association MAC Filtering

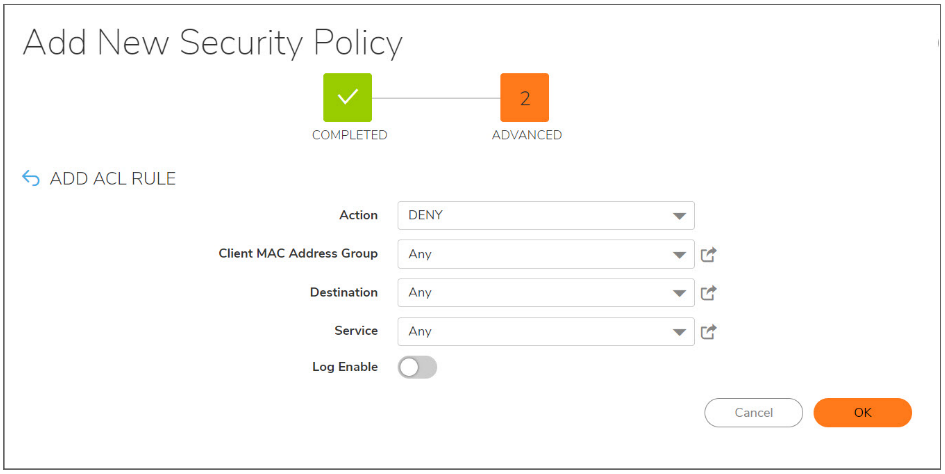
- **Mode** - The mode can be either Allow, Deny, or Disabled.
- **Client MAC Address Group** - The name of the address group.

ACL

Wireless Network Manager provides support for Layer 2 (L2), Layer 3 (L3), and Layer 4 (L4) access control list (ACL) support for SonicWave access points.

- **Action** - The mode can be either Allow, Deny, or Disabled.
- **Client MAC Address Group** - The name of the address group.

Click on the Add icon to add an ACL Rule and the **Add ACL Rule** page displays.



Add New Security Policy

Action: DENY

Client MAC Address Group: Any

Destination: Any

Service: Any

Log Enable: ○

Select the **Action**, **Client MAC Address Group**, **Destination**, **Service** and **Log Enable**, and click **OK** to save the changes.

After you create all the ACLs, you can increase or decrease the priority in the list clicking on the up or down arrows pertaining to the right hand side of the each ACL. You can also either edit or delete any ACL.

Bandwidth Management

Specify the details for Bandwidth Management.

- **Enable** - You can select to enable or disable bandwidth management.
- **Direction** - Choose one of these:
  - **Both directions**
  - **Up link (Client to AP)**
  - **Down link (AP to Client)**
- **Down Min/Max Rate (kbps)** - Downstream minimum and maximum rates.
- **Up Min/Max Rate (kbps)** - Upstream minimum and maximum rates
- **All Clients** - This is a toggle to enable or disable all clients. If you want to apply this configuration to all clients, select **All Clients**. If you want to apply it only to an restricted IP group, toggle **All Clients** off, and set the **Client IP Group** in the field that appears below the **All Clients** field.

- **Client IP Group** - Select the **IP Group** to which these selections apply. This field is only available when **All Clients** is off.

Geo-IP & Botnet

For information about configuring these security policies, refer to Geo-IP & Botnet

APP Control Security Policy

To create a new application control policy:

1. Navigate to **Security > Security Policies**.
2. On the **Access Points** tab, click Add (**+**). The **Add New Security Policy** dialog displays.
3. In the **Name** field, enter a name for your new security policy.
4. From the **Type** list, select **APP Control Security Policy**.
5. Click **Next**.
6. In the **General** section, select **Enable** to activate the new policy.
7. Select the **Schedule** option from the drop-down.
8. In the **App Rules** section, click Add (**+**) to associate security rules with the policy.
9. Add **App Group** and **Operation**.

   ⓘ **NOTE:** You can increase and decrease the priority, edit or delete the App Rules hovering the mouse over the right hand side of the rules and clicking on the respective icons.
10. Click **OK**.

The new policy is now displayed in the list of available security policies.

AP Policies

The options on the **AP Policies** page are used to create and manage AP policies. When you click **Add +** on the top right, or **Edit** in a policy row, you see pages with the same information fields for consulting or configuring as those discussed in Select an AP Policy.

For more information on the explanation of each settings, refer to Select an AP Policy

Using Tags to Manage Access Points and SSIDs

By default, all access points in a network broadcast all of their enabled SSIDs simultaneously. While this is desired for most deployment situations, there may be cases where specific SSIDs should only be broadcast from a specific access point or group of access points. Tags can be used to partition your wireless network into both physical, or security-based segments, and for basic management purposes.

Topics:

- Using Tags to Manage Access Points
- Using Tags to Manage SSIDs

Using Tags to Manage Access Points

Tags can be used to partition your wireless network into both physical, or security-based segments, and for basic management purposes.

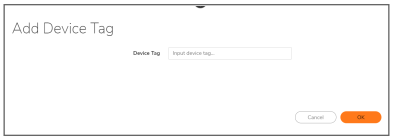
Topics:

- Adding Tags to an Access Point
- Removing Tags Associated with an Access Point
- Viewing Tags Associated with an Access Point

Adding Tags to an Access Point

To add a tag to an access point:

1. Navigate to **Network > Devices**.
2. On the right of the access point for which you want to add a tag, click the **Edit** icon.
3. The **General** tab is displayed by default.
4. On the **Tags** field, click on the **Add Device Tag** icon (**+**). and the **Add Device Tag** dialog displays.

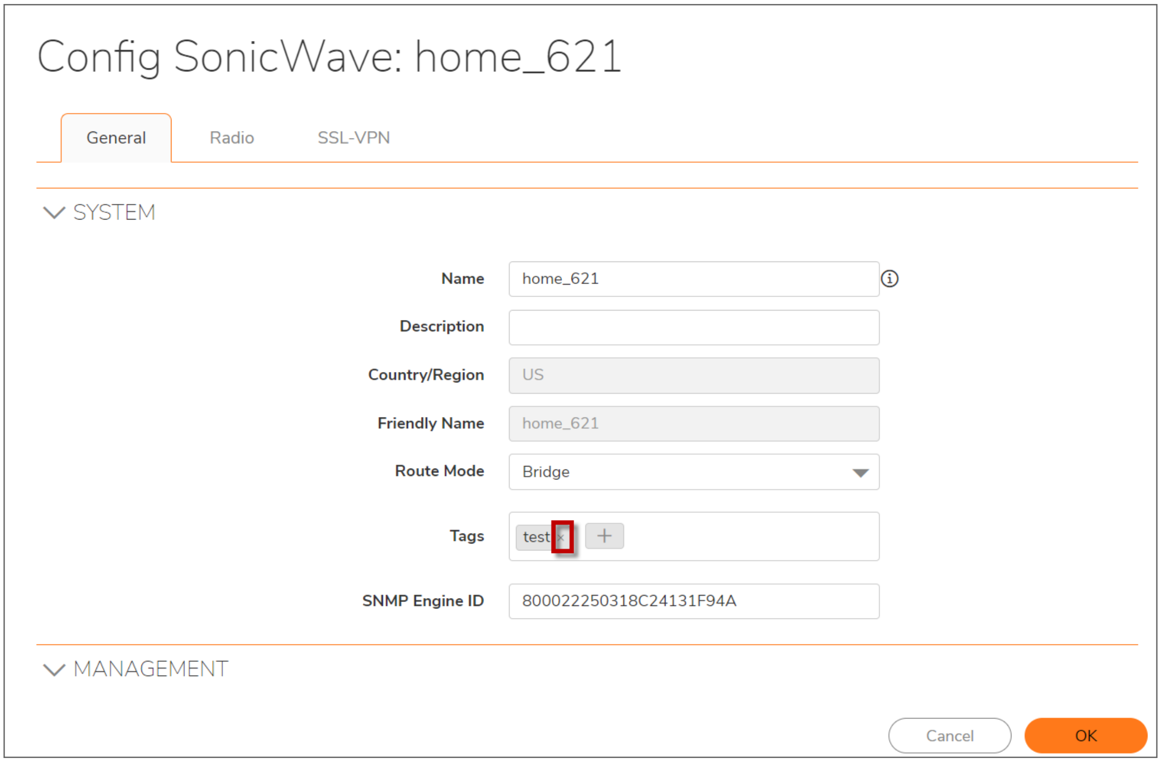


Add Device Tag

Device Tag: Input device tag...

5. In the **Device Tag** field, enter the name for the tag you want to create.
6. Click **OK** to save the tag.
7. Click **OK** to save the configuration changes for the access point.

After adding a Device Tag, you can remove the tag if required by clicking the (**x**) pertaining to the tag.



Config SonicWave: home_621

Name: home_621
Description:
Country/Region: US
Friendly Name: home_621
Route Mode: Bridge
Tags: test
SNMP Engine ID: 800022250318C24131F94A

Removing Tags Associated with an Access Point

To remove a tag associated with an access point:

1. Navigate to **Network > Devices**.
2. On the right of the access point for which you want to delete a tag, click the **Edit** icon.
3. The **General** tab is displayed by defaut.
4. Next to **Device Tags**, click on **X** next to the tag you want to delete.
5. Click **OK**.

Viewing Tags Associated with an Access Point

To view the tags associated with an access point:

1. Navigate to **Network > Devices**.
2. On the right of the access point to which you want to view the associated tags, hover over the **Tag** icon. The tags associated with the access point will display in a small pop-up window.

Using Tags to Manage SSIDs

By default, all access points in a network broadcast all of their enabled SSIDs simultaneously. While this is desired for most deployment situations, there may be cases where specific SSIDs should only be broadcast from a specific access point or group of access points. Tags can be used to partition your wireless network into both physical- or security-based segments, and for basic management purposes.

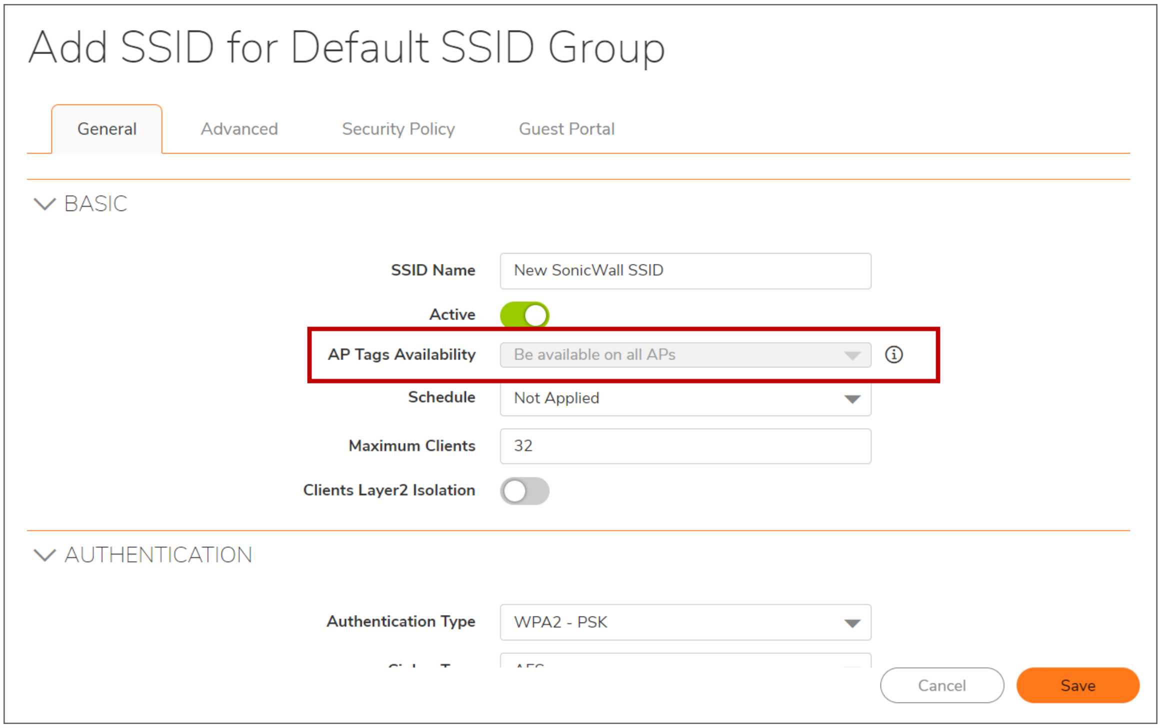
Topics:

- Adding Tags to an SSID Group
- Removing Tags from an SSID Group
- Viewing Tags Associated with an SSID Group

Adding Tags to an SSID Group

To add a tag to an SSID group:

1. Navigate to **Policies > SSID Policies**.
2. On the right of the SSID to which you want to add a tag, click on the (**+**) icon. The **Add SSID** window is displayed.
3. From the Basic section, select the **AP Tags Availability** list, and apply the tag(s) to the SSID.



Add SSID for Default SSID Group

SSID Name: New SonicWall SSID

Active: ●

AP Tags Availability: Be available on all APs

Schedule: Not Applied

Maximum Clients: 32

Clients Layer2 Isolation: ○

Authentication Type: WPA2 - PSK

4. Click **OK**.

Removing Tags from an SSID Group

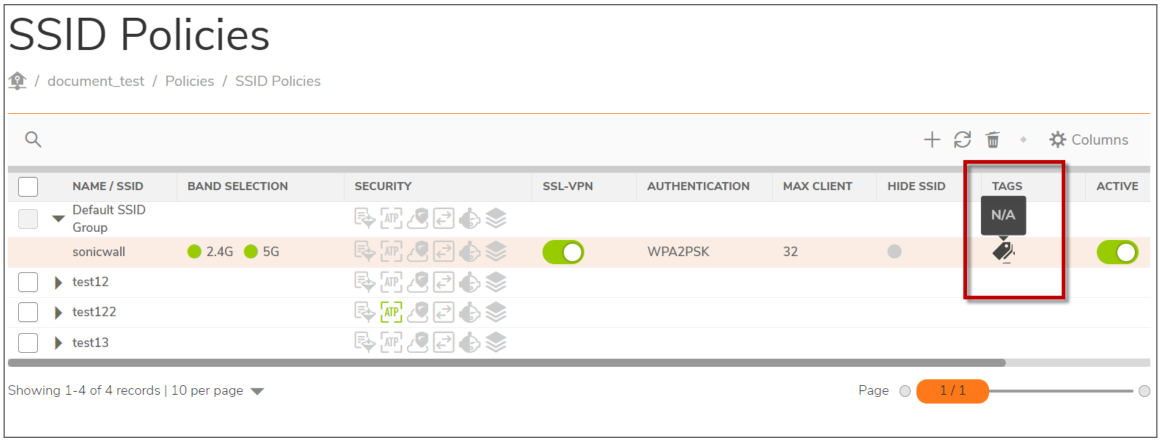
To remove a tag from an SSID group:

1. Navigate to **Policies > SSID Policies**.
2. On the right of the SSID to which you want to remove a tag, click the **Edit** icon.
3. From the **AP Tags Availability** list, click the (**X**) next to the tag you want to delete.
4. Click **OK**.

Viewing Tags Associated with an SSID Group

To view the tags associated with an SSID group:

1. Navigate to **Policies > SSID Policies**.
2. On the right of the SSID to which you want to view the associated tags, hover over the **Tag** icon. The tags associated with the SSID group will display in a small popup window.



SSID Policies

/ document_test / Policies / SSID Policies

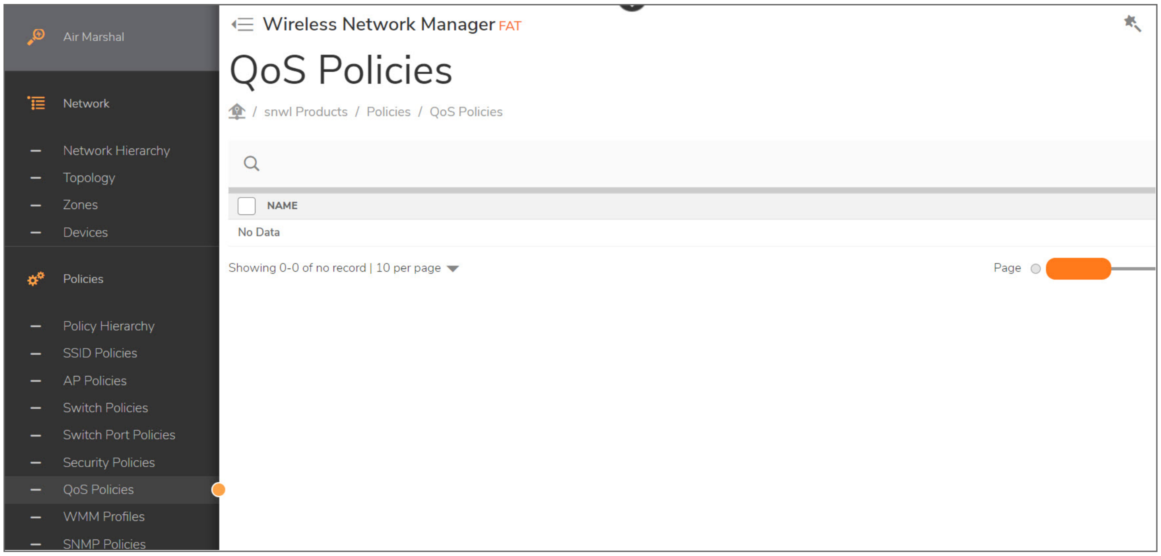
□	NAME / SSID	BAND SELECTION	SECURITY	SSL-VPN	AUTHENTICATION	MAX CLIENT	HIDE SSID	TAGS	ACTIVE
□	Default SSID Group							N/A	
	sonicwall	● 2.4G ● 5G		●	WPA2PSK	32	●		●
□	test12								
□	test122								
□	test13								

Showing 1-4 of 4 records | 10 per page

Page 1 / 1

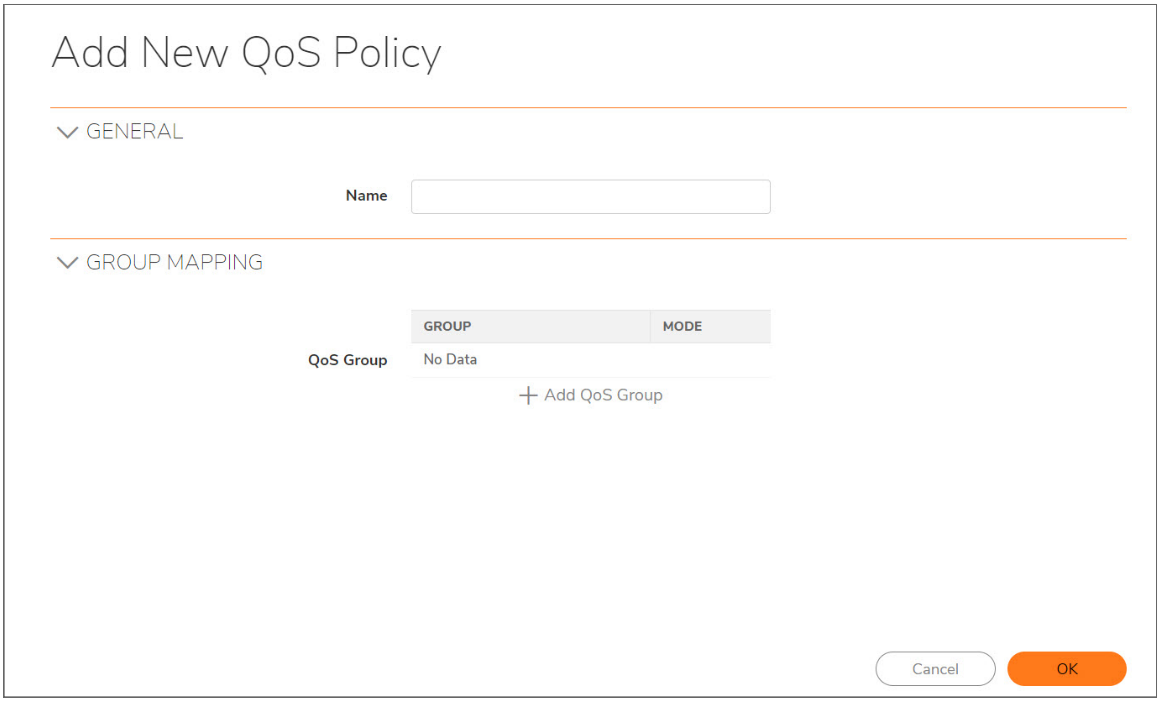
QoS Policies

The **Policies > QoS Policies** page provides options for creating or editing QoS Policies.



To create a new QoS Policy:

1. Navigate to **Policies > QoS Policies**.
2. Click Add (**+**). The **Add New QoS Policy** dialog displays.



3. Specify a group name.
4. Click (**+**) and select **QoS Group** in the **Group Mapping** section from the drop down.

5. Select the **Mode** from the drop down and enter the value in the field .
6. Click **OK**.

Wi-Fi Multimeda (WMM) Profiles

Wireless Network Manager allows you to create and manage Wi-Fi Multimeda (WMM) profiles and assign them to specific SonicWave access points.

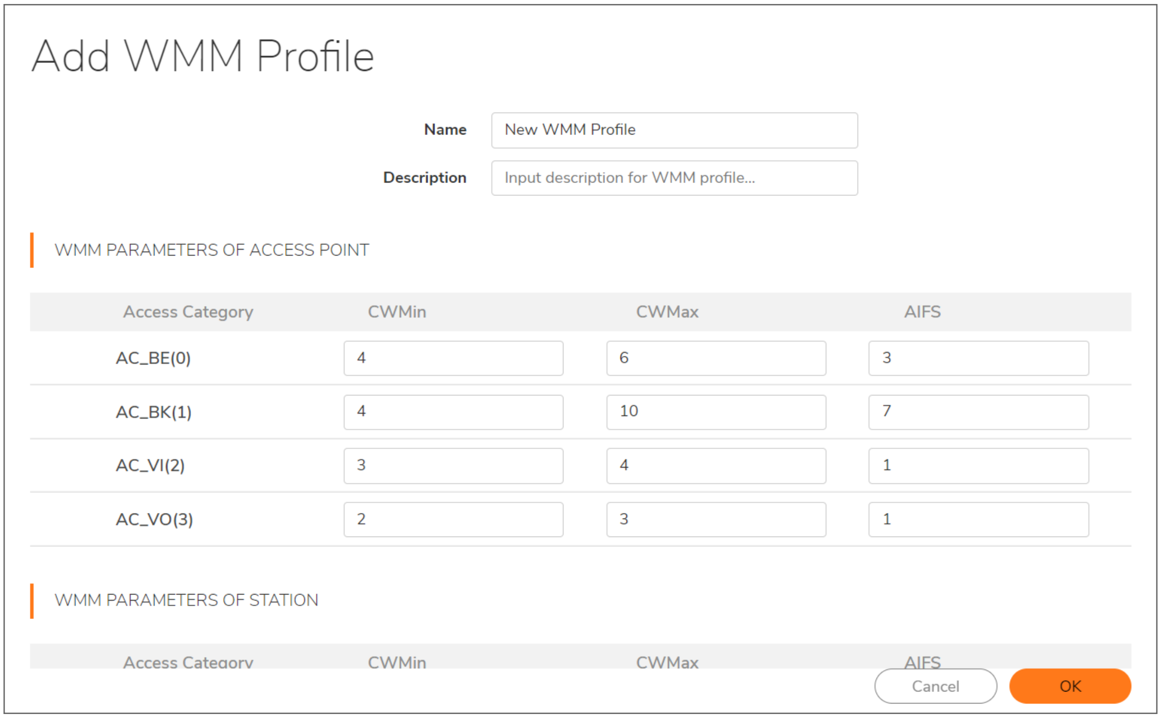
Topics:

- Creating Wi-Fi Multimeda (WMM) Policies
- Enabling Wi-Fi Multimeda (WMM) Policies

Creating Wi-Fi Multimeda (WMM) Policies

To create an WMM profile:

1. Navigate to **Policies > WMM Profiles**.
2. Click the plus icon (+) at the far right of the table. The **Add WMM Profile** dialog displays.



Add WMM Profile

Name: New WMM Profile

Description: Input description for WMM profile...

WMM PARAMETERS OF ACCESS POINT

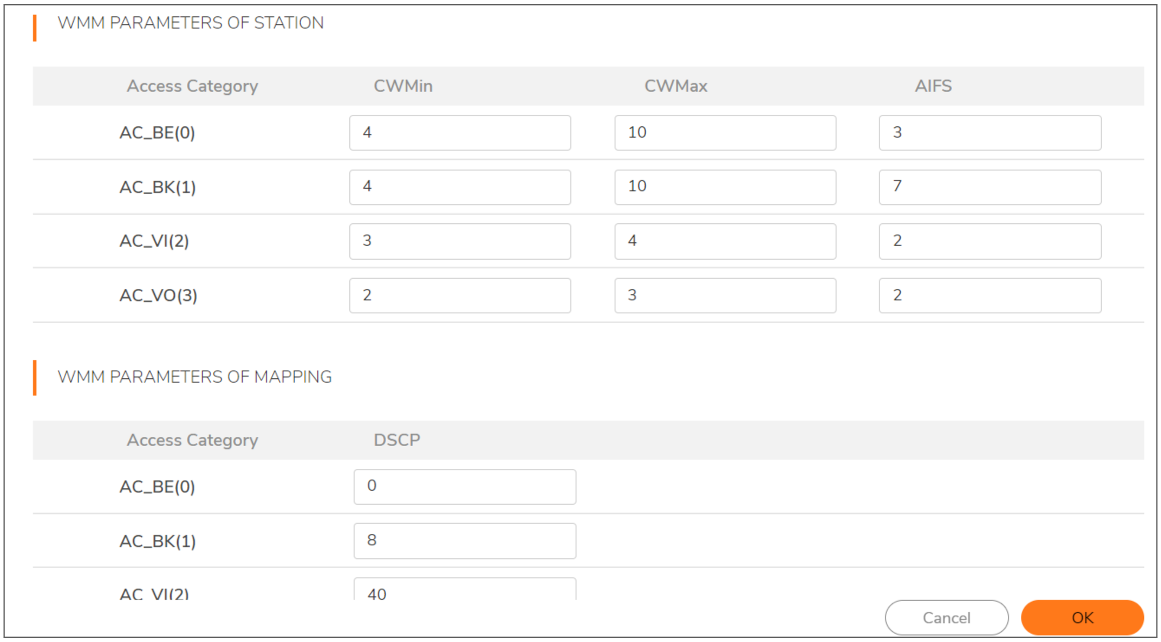
Access Category	CWMin	CWMax	AIFS
AC_BE(0)	4	6	3
AC_BK(1)	4	10	7
AC_VI(2)	3	4	1
AC_VO(3)	2	3	1

WMM PARAMETERS OF STATION

Access Category	CWMin	CWMax	AIFS

3. In the **Name** field, enter a name for the profile.
4. In the **Description** field, enter a short description for the profile. (This is optional.)

5. Enter the values required for **WMM Parameters of Access Point** including **CWMin**, **CWMax**, and **AIFS** values.
6. Enter the values required for **WMM Parameters of Station** including **CWMin**, **CWMax**, and **AIFS** values.
7. Enter the values required for **WMM Parameters of Mapping** including **DSCP**.



WMM PARAMETERS OF STATION

Access Category	CWMin	CWMax	AIFS
AC_BE(0)	4	10	3
AC_BK(1)	4	10	7
AC_VI(2)	3	4	2
AC_VO(3)	2	3	2

WMM PARAMETERS OF MAPPING

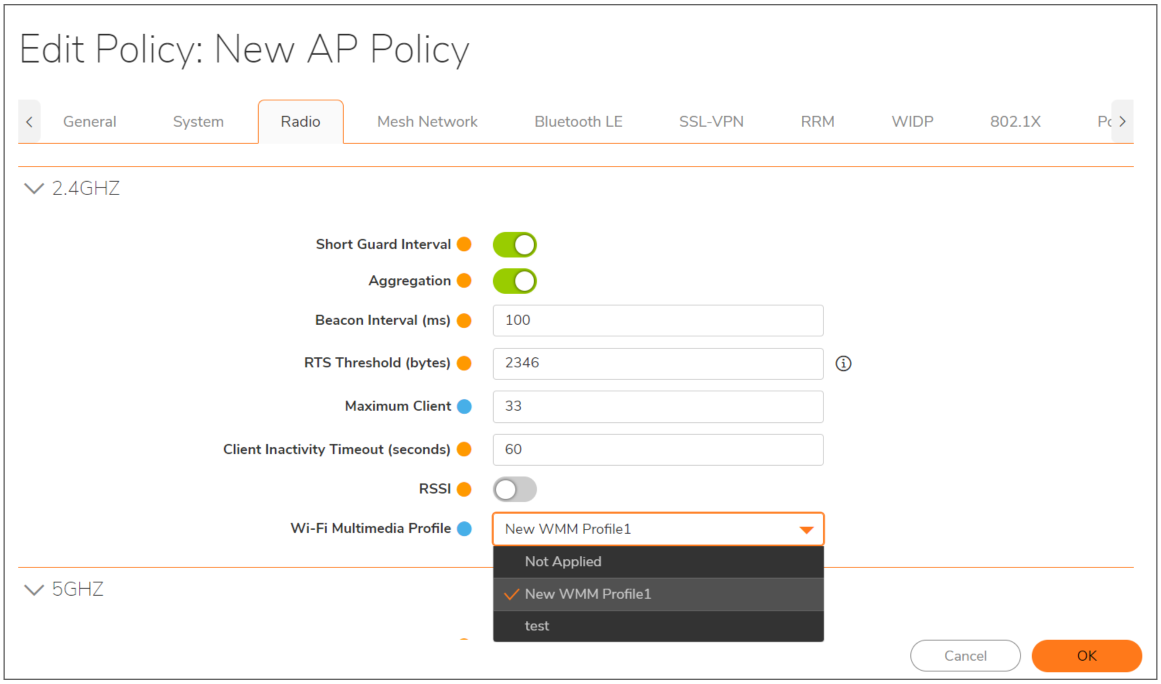
Access Category	DSCP
AC_BE(0)	0
AC_BK(1)	8
AC_VI(2)	40

8. Click **OK**.

Enabling Wi-Fi Multimeda (WMM) Policies

To enable an WMM profile for an access point:

1. Navigate to **Policies > AP Policies**.
2. On the right of the AP Policy for which you want to enable a WMM profile, click the **Edit** icon.
3. Click the **Radio** tab.
4. From the **WMM Profile** list, select the WMM profile you want applied to the access point.



Edit Policy: New AP Policy

2.4GHZ

Short Guard Interval: On

Aggregation: On

Beacon Interval (ms): 100

RTS Threshold (bytes): 2346

Maximum Client: 33

Client Inactivity Timeout (seconds): 60

RSSI: Off

Wi-Fi Multimedia Profile: New WMM Profile1

5. Click **OK**.

Managing Switch Policies

Topics:

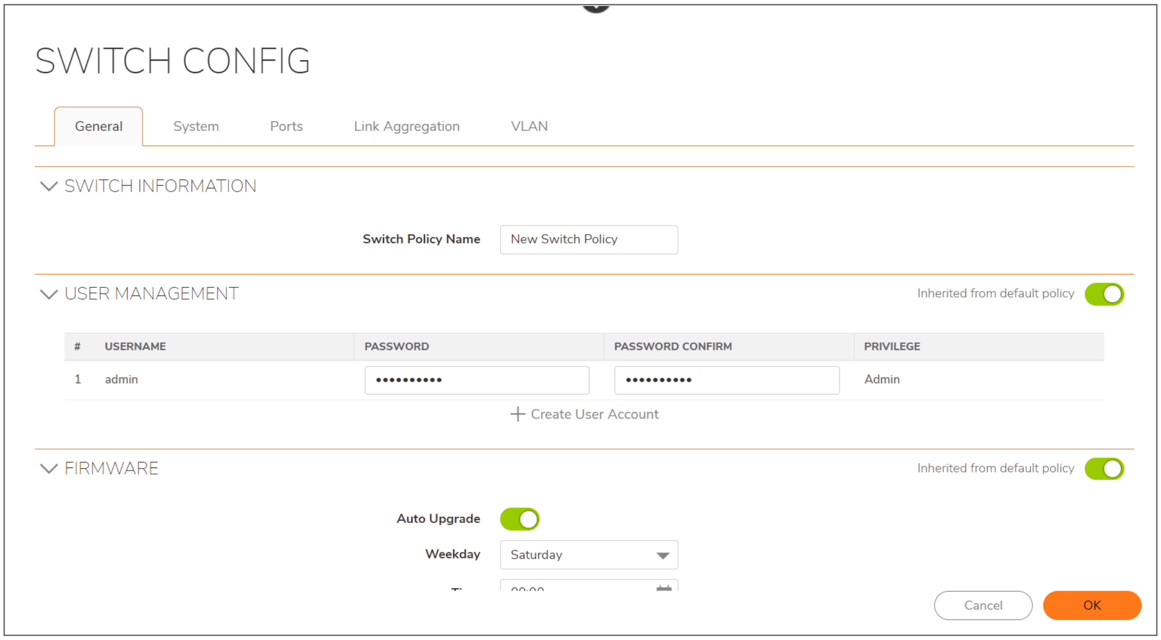
- Adding Switch Policies
- Editing Switch Policies

For more information on configuring and using the SonicWall Switch, refer to the *Switch Administration Guide*. This and other documentation are available under the product name “Switch” on the SonicWallSonicWall support website at: https://www.sonicwall.com/support/technical-documentation/.

Adding Switch Policies

To add a Switch policy:

1. Navigate to **Policies > Switch Polices**.
2. Click the Add (**+**) icon to create a policy. The **Switch Config** page displays.



SWITCH CONFIG

SWITCH INFORMATION

Switch Policy Name: New Switch Policy

USER MANAGEMENT — Inherited from default policy

#	USERNAME	PASSWORD	PASSWORD CONFIRM	PRIVILEGE
1	admin	••••••••••	••••••••••	Admin

FIRMWARE — Inherited from default policy

Auto Upgrade: on

Weekday: Saturday

3. Set the options for the new policy. For detailed information, refer to Select a Switch Policy.

   ⓘ **NOTE:** You only need to set the options where you want them to be different from the **Default Switch Policy**. If you want the change to affect all Switches, edit the **Default Switch Policy** instead of creating a new Switch policy.

4. Click **OK**.

For more information on configuring and using the SonicWall Switch, refer to the *Switch Administration Guide*. This and other documentation are available under the product name “Switch” on theSonicWall support website at: https://www.sonicwall.com/support/technical-documentation/.

Editing Switch Policies

To edit a Switch policy:

1. Navigate to **Policies > Switch Polices**.
2. Click the **Edit** (pencil) icon to edit an existing policy. The **Switch Config** page displays.

   ⓘ **NOTE:** To change the policy options for all of the Switches, edit the **Default Switch Policy**.

3. Update the options for the existing policy as per the requirement, clicking on each tab.
4. Click **OK**.

For more information on configuring and using the SonicWall Switch, refer to the *Switch Administration Guide*. This and other documentation are available under the product name “Switch” on the SonicWallSonicWall support website at: https://www.sonicwall.com/support/technical-documentation/.

Managing Switch Port Policies

Wireless Network Manager provides the option of manually creating the VLAN for each switch

When a network admin has to configure multiple switches with a same VLAN, the admin needs to manually create the VLAN for each switch.

> **NOTE:** VLAN Object should be applied to a Port Policy and Port Policy should be assigned to any port of the Switch Policy.

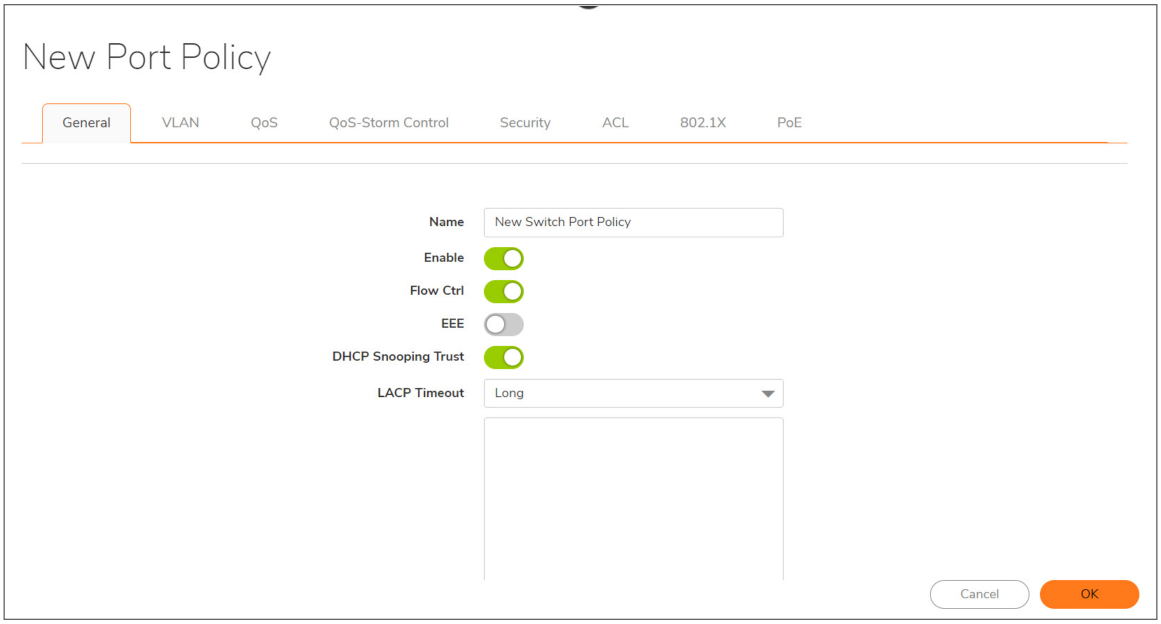
Topics:

- Adding Switch Port Policies
- Editing Switch Policies

Adding Switch Port Policies

To add a Switch Port policy:

1. Navigate to **Policies > Switch Port Polices**.
2. Click the Add (**+**) icon to create a policy. The **New Port Policy** page displays.



New Port Policy

Name	New Switch Port Policy
Enable	☑
Flow Ctrl	☑
EEE	☐
DHCP Snooping Trust	☑
LACP Timeout	Long

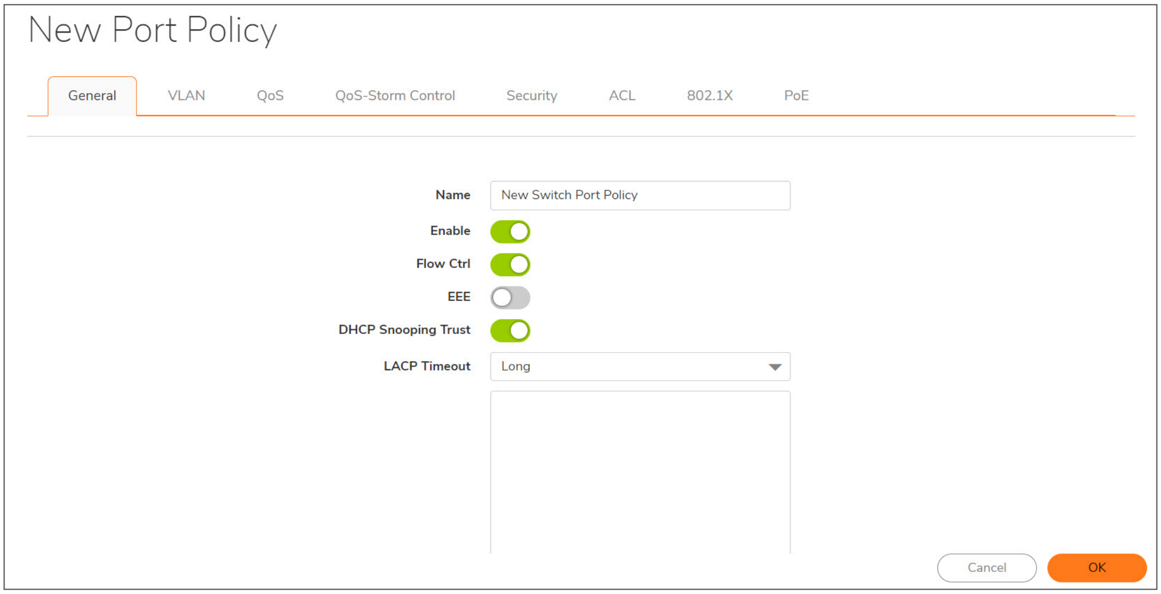
The options in the **New Port Policy** page are:

- General
- VLAN

- QoS
- QoS Storm Control
- Security
- ACL
- 802.1X
- POE

General

The **General** tab helps you to edit the general details of the port policies.



Name: New Switch Port Policy

Enable ●

Flow Ctrl ●

EEE ○

DHCP Snooping Trust ●

LACP Timeout: Long

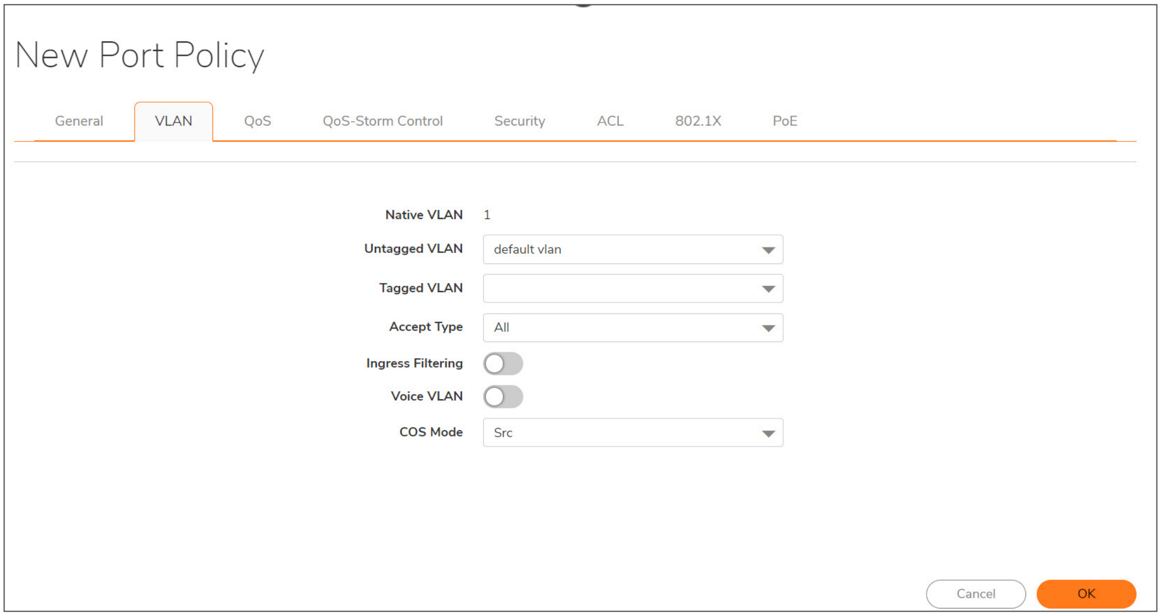
This includes editing the following:

- **Name**
- **Enable** toggle bar
- **Flow Control** toggle bar
- **EEE** toggle bar
- **DHCP Snooping Trust** toggle bar
- **LACP Time out**
- **Description/Comment**

VLAN

The **VLAN** tab helps you to edit the VLAN details of the port policies.

The VLAN should be created in the **Objects > VLAN Objects** page.



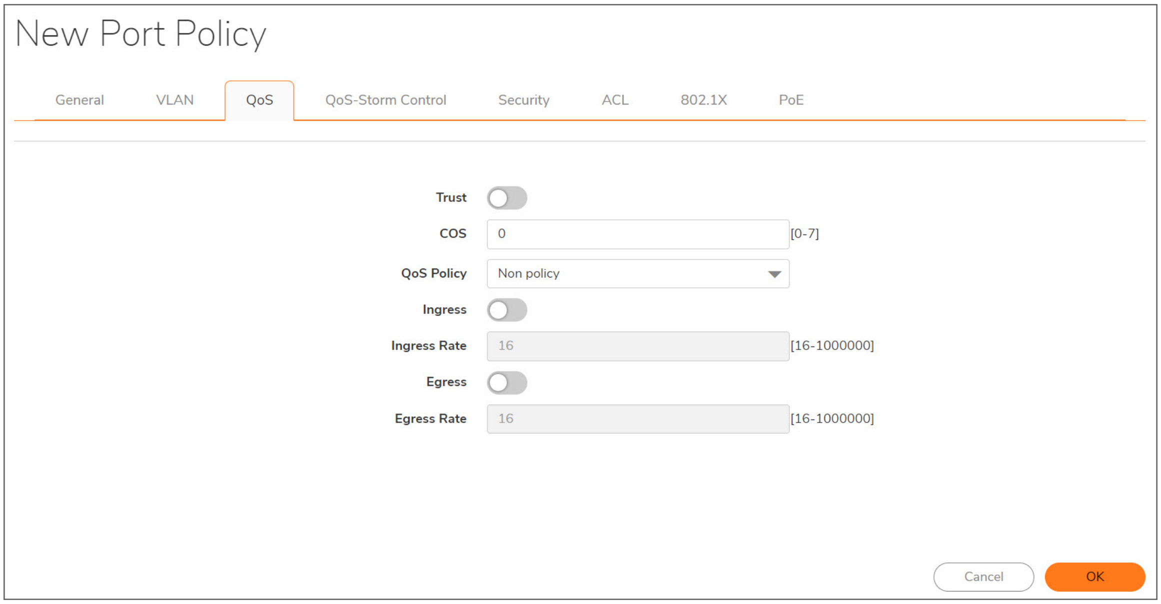
Native VLAN	1
Untagged VLAN	default vlan
Tagged VLAN	
Accept Type	All
Ingress Filtering	○
Voice VLAN	○
COS Mode	Src

This includes editing the following:

- Native VLAN
- Untagged VLAN
- Tagged VLAN
- Accept Type
- Ingress Filtering
- Voice VLAN
- COS Mode

QoS

The **QoS** tab helps you to edit the QoS details of the port policies.



New Port Policy

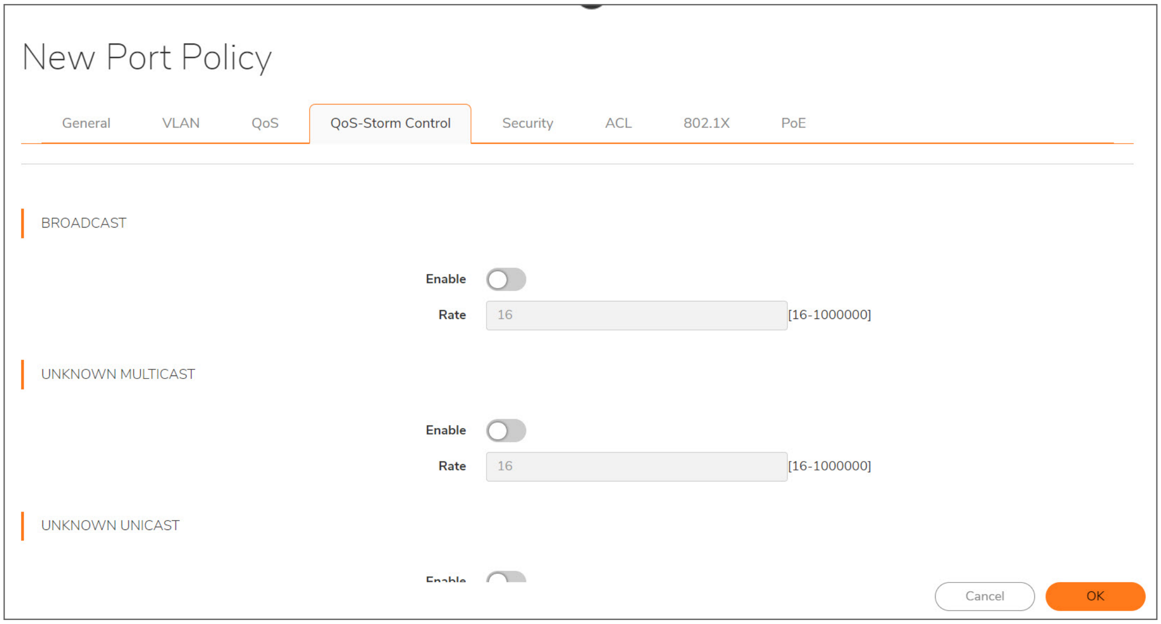
Trust	○	
COS	0	[0-7]
QoS Policy	Non policy	
Ingress	○	
Ingress Rate	16	[16-1000000]
Egress	○	
Egress Rate	16	[16-1000000]

This includes editing the following:

- Enable or disable Trust
- COS
- QoS Policy
- Ingress
- Ingress Rate (KBPS)
- Egress
- Egress Rate (KBPS)

QoS Storm Control

The **QoS Storm Control** tab helps you to edit the QoS Storm Control details of the port policies.



New Port Policy

BROADCAST

Enable

Rate 16 [16-1000000]

UNKNOWN MULTICAST

Enable

Rate 16 [16-1000000]

UNKNOWN UNICAST

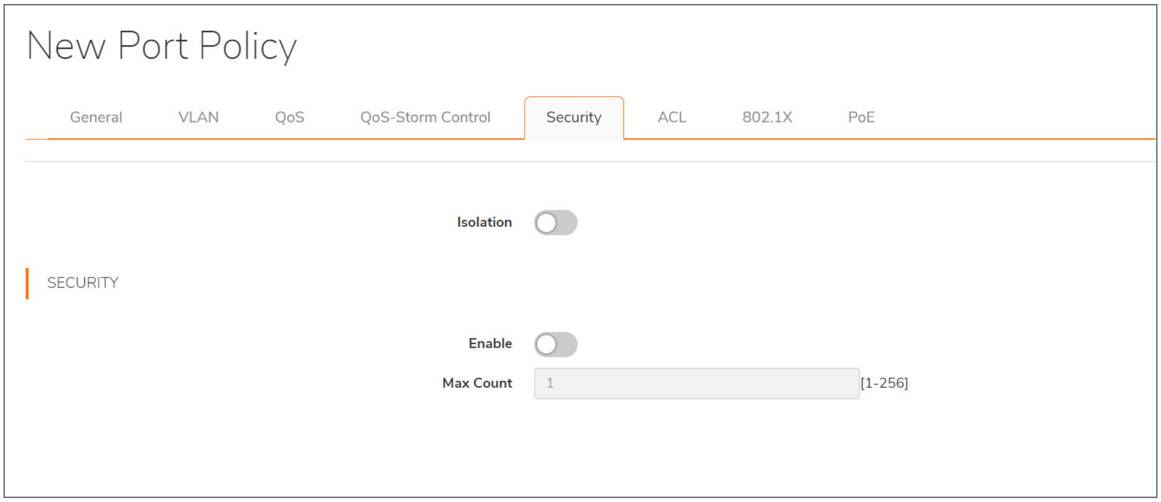
Enable

This includes editing the following:

- Broadcast Rate
- Unknown Multicast
- Unknown Unicast

Security

The **Security** tab helps you to edit the Security details of the port policies.



New Port Policy

Isolation

SECURITY

Enable

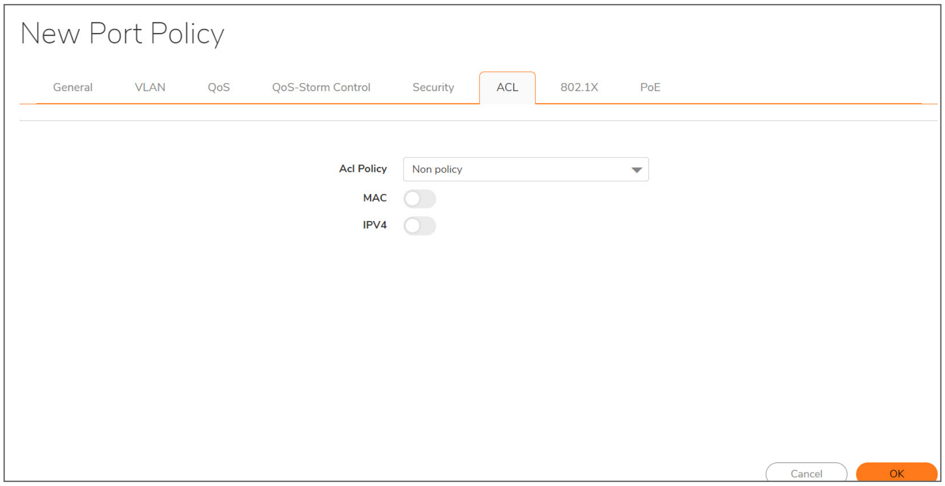
Max Count 1 [1-256]

This includes editing the following:

- Isolation
- Security Max Count

ACL

The **ACL** tab helps you to edit the ACL details of the port policies.



Acl Policy: Non policy

MAC

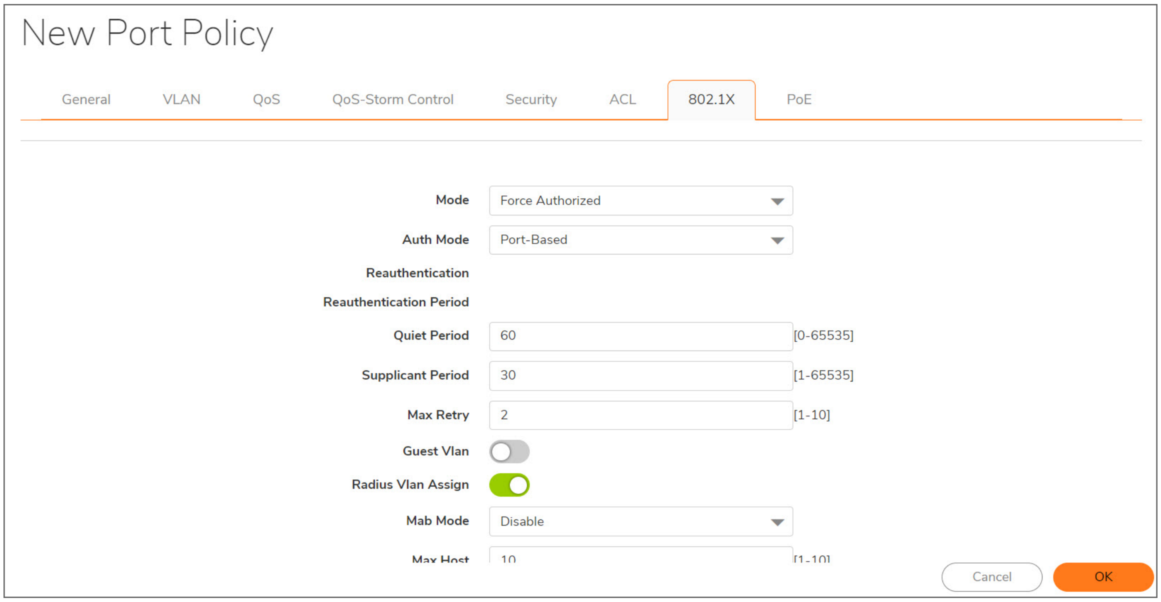
IPV4

This includes editing the following:

- ACL Policy
- MAC
- IPV4

802.1X

The **802.1X** tab helps you to edit the 802.1X details of the port policiess.



Mode: Force Authorized
Auth Mode: Port-Based
Reauthentication
Reauthentication Period
Quiet Period: 60 [0-65535]
Supplicant Period: 30 [1-65535]
Max Retry: 2 [1-10]
Guest Vlan: ○ off
Radius Vlan Assign: ● on
Mab Mode: Disable
Max Host: 10 [1-10]

Wireless Network Manager also provides the **802.1X MAB** authentication, an access control technique to authenticate the client devices. The 802.1x MAC Authentication Bypass (MAB) allows a device without an 802.1x supplicant running on it to authenticate against RADIUS via MAC address. This uses the MAC Address of a device to determine the network access to be provided to the hosts.

To enable the MAB authentication ensure that the switch is Online and the **802.1X** is always enabled in the **System** Tab.

ⓘ **IMPORTANT:** You need to add radius server before using 802.1X.

ⓘ **NOTE:** If you select MAB mode, the authenticate host is MAB only. If you select Hybrid mode, the authenticate host is EAP but if the host does not support EAP mode, it falls back to MAB mode. If you select Disable, the authenticate host is EAP only.

ⓘ **NOTE:** Multi-authentication/multi-host is supported only when the authentication mode is MAC-Based, and not when the authentication mode is Port-Based.

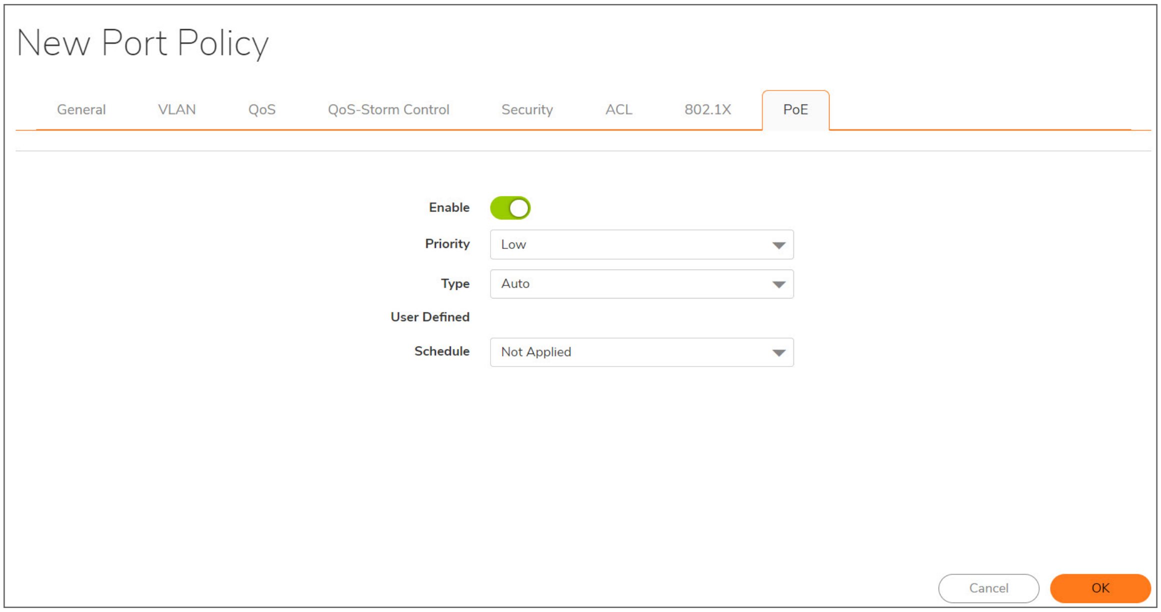
You can edit all the following options from this tab:

- Mode
- Auth Mode
- Re-authentication
- Re-authentication Period
- Quiet Period
- Supplicant Period
- Max Retry
- Guest VLAN
- Radius VLAN Assign

- MAB Mode
- MAX Host

POE

The **POE** tab helps you to edit the POE details of the port policies, if it is a POE model.



New Port Policy

Enable: on

Priority: Low

Type: Auto

User Defined

Schedule: Not Applied

You can edit all the following options from this tab:

- Enable/Disable Port
- Priority
- Type
- Schedule

Editing Switch Port Policies

To edit a Switch Port policy:

1. Navigate to **Policies > Switch Port Polices**.
2. Click the **Edit** (pencil) icon to edit an existing policy. The **Edit Port Policy** page displays.
3. Update the options for the existing policy as per the requirement, clicking on each tab.
4. Click **OK**.

Security Policies

The **Security Policies** page displays all of the security policies that have been configured on your network and provides options for managing, adding, and editing security policies. These policies add extra layers of security beyond that available from AP Policies. Hovering over the right end of each row enables:

- **Edit**
- **Copy**
- **Delete**

The columns display the following information:

- **Name** - The distinct name that was given to the policy by the administrator when it was created or last edited. If desired, it can include information about what type of policy it is.
- **Applied SSID Group** - The group of SSIDs to which the policy is applied.
- **Type** - The symbol of the security policy in the appropriate color (green for on, red for off). Hovering over the security policy symbol gives a screen tip saying which type of policy it is and whether or not it is enabled.
- **Active** - Toggles on and off for this security policy.
- **Schedule** - The applied scheduled policy.

Only licensed security policies can be applied to an SSID or SSID group managed in your Wireless Network Manager network. If you try to apply a policy that is not licensed, a screen tip appears indicating that this policy needs to be licensed.

Wireless Network Manager advanced security services include these policies:

- Content Filtering Service
- Capture Advanced Threat Protection
- Cloud Anti-Virus
- Access Control Policies
- Geo-IP & Botnet
- Application Control

Content Filtering Service

The Wireless Network Manager Content Filtering Service (CFS) is a web-filtering service that blocks inappropriate, unproductive, and illegal or malicious web content according to your specifications. CFS inspects web page traffic based on HTTP and HTTPS protocols, and blocks or logs websites based on pre-configured blacklists and whitelists. CFS includes tools for creating and applying policies that allow or deny access to sites based on individual or group identity, time of day, and over 90 other categories you pre-select. This feature is based on SonicWave Virtual Access Point (Virtual SSID) architecture. All user configuration is VAP (Virtual Access Point)-based.

Topics:

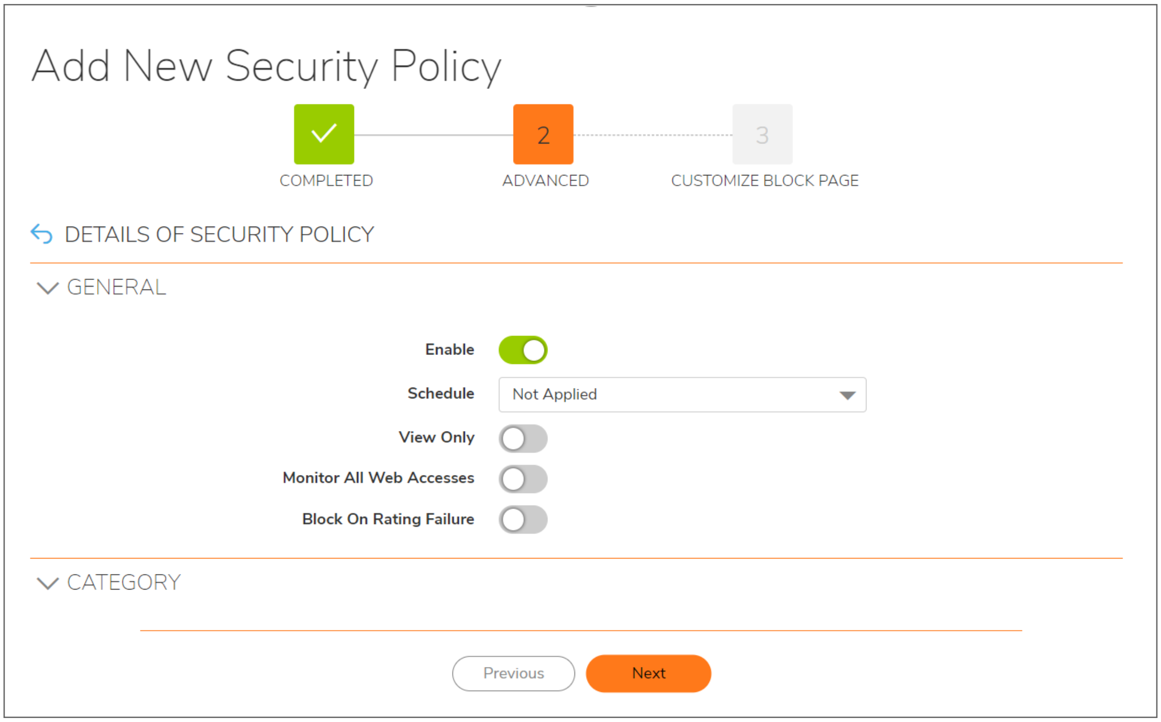
- Creating Content Filtering Service Security Policies
- Editing Content Filtering Service Categories
- Adding Sites to the Allowlists and Blocklists

Creating Content Filtering Service Security Policies

You can create CFS security policies and select which categories you want them to block.

To create a CFS security policy:

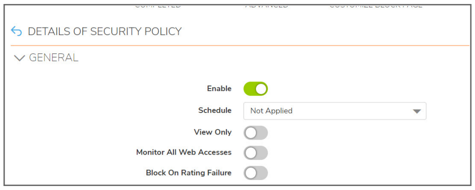
1. Navigate to **Policies > Security Policies**.
2. Click **Add +**. The **Add New Security Policy** page displays.
3. In the **Name** field, enter a name for the policy.
4. In the **Type** field, select **CFS Security Policy** from the drop down list.
5. Click **Next**. The **Add New Security Policy** screen displays.



Add New Security Policy

Enable: on
Schedule: Not Applied
View Only: off
Monitor All Web Accesses: off
Block On Rating Failure: off

6. Toggle **Enable** to enable the CFS policy you are creating. From the dropdown list, choose the **Schedule**.



DETAILS OF SECURITY POLICY

GENERAL

Enable ●

Schedule: Not Applied

View Only ○

Monitor All Web Accesses ○

Block On Rating Failure ○

7. Click **View Only** if you want CFS to log website access instead of blocking the websites.
8. Select **CFS Categories**, **Reputation**, and **URI List (Blacklist** and **Whitelist)**, based on your requirements. To select all the categories, click **Select All**.
9. When you click **OK**, the CFS policy is enabled and listed on the **Security > Security Policies** page according to the criteria you have chosen.

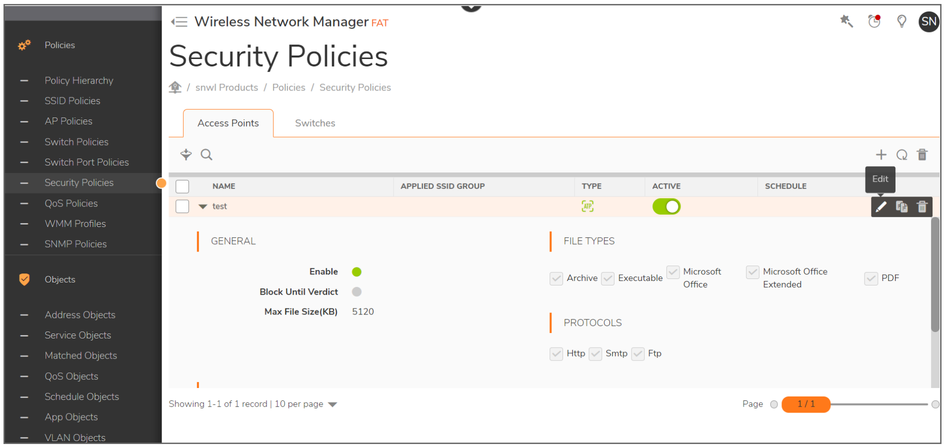
For more information on customizing the block page, refer Customizing Blockpage.

Editing Content Filtering Service Categories

The CFS categories that provide customization options for blocking specific types of websites can be changed at any time.

To edit Content Filtering Service categories:

1. Navigate to **Security > Security Policies**.



Security Policies

/ snwl Products / Policies / Security Policies

NAME	APPLIED SSID GROUP	TYPE	ACTIVE	SCHEDULE
test			●	

GENERAL

Enable ●

Block Until Verdict ○

Max File Size(KB) 5120

FILE TYPES

☑ Archive ☑ Executable ☑ Microsoft Office ☑ Microsoft Office Extended ☑ PDF

PROTOCOLS

☑ Http ☑ Smtp ☑ Ftp

Showing 1-1 of 1 record | 10 per page

Page 1 / 1

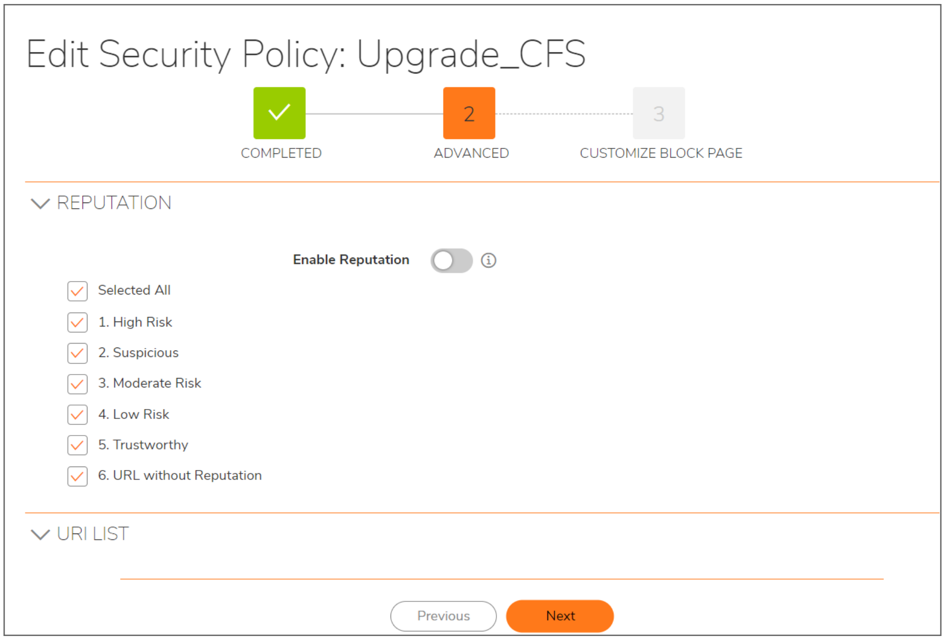
2. Click **Edit** next to the policy you want to change. The **Edit Security Policy** page displays.
3. Click **Select All** to select all Content Filtering Service categories, or choose specific categories to block specific types of websites.
4. Click **Submit** to apply the Content Filtering Service policy.

Enabling or Disabling Reputation

You can enable or disable this section by toggling the button to on or off.

ⓘ | **NOTE:** Filtering by reputation will take effect, only if the Category filtering result is enabled.

Select individual options by using the checkbox or select all of the options by clicking **Selected all**.



Edit Security Policy: Upgrade_CFS

Enable Reputation ○

☑ Selected All
☑ 1. High Risk
☑ 2. Suspicious
☑ 3. Moderate Risk
☑ 4. Low Risk
☑ 5. Trustworthy
☑ 6. URL without Reputation

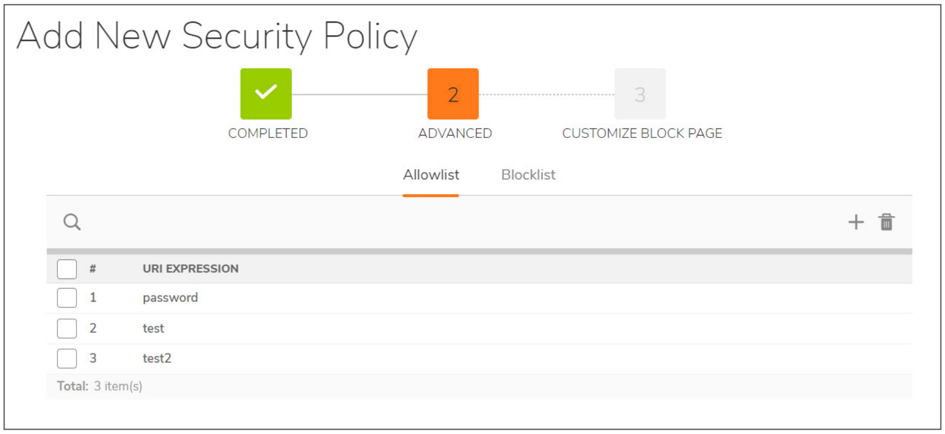
Adding Sites to the Allowlists and Blocklists

In addition to specific categories, one or several sites can be put on a list by a CFS policy from which all communication is either:

- Allowlist
- Blocklist

To add a URI to a Allowlist or Blocklist:

1. Navigate to **Security > Security Policies**.
2. Click **Edit** next to the policy you want to change. The **Edit Security Policy** page displays. The policy you are changing appears in the title line of the page.
3. In the **URI List** section at the bottom of the screen, select either the Allowlist or Blocklist, then click **Add +** or **Delete**. This screen is only available if a CFS policy has been chosen for editing. The **Edit Security Policy: CFS - ADD URI TO Allowlist/Blocklist** screen appears.
4. Type the name of the URI you wish to block or allow, then click **Add**. The URI is added to the list you specified. The screen below shows a URI being added to an Allowlist.


Add New Security Policy

☐	#	URI EXPRESSION
☐	1	password
☐	2	test
☐	3	test2

Total: 3 item(s)

5. A site can be removed from a list by clicking **Delete** before clicking **OK**.

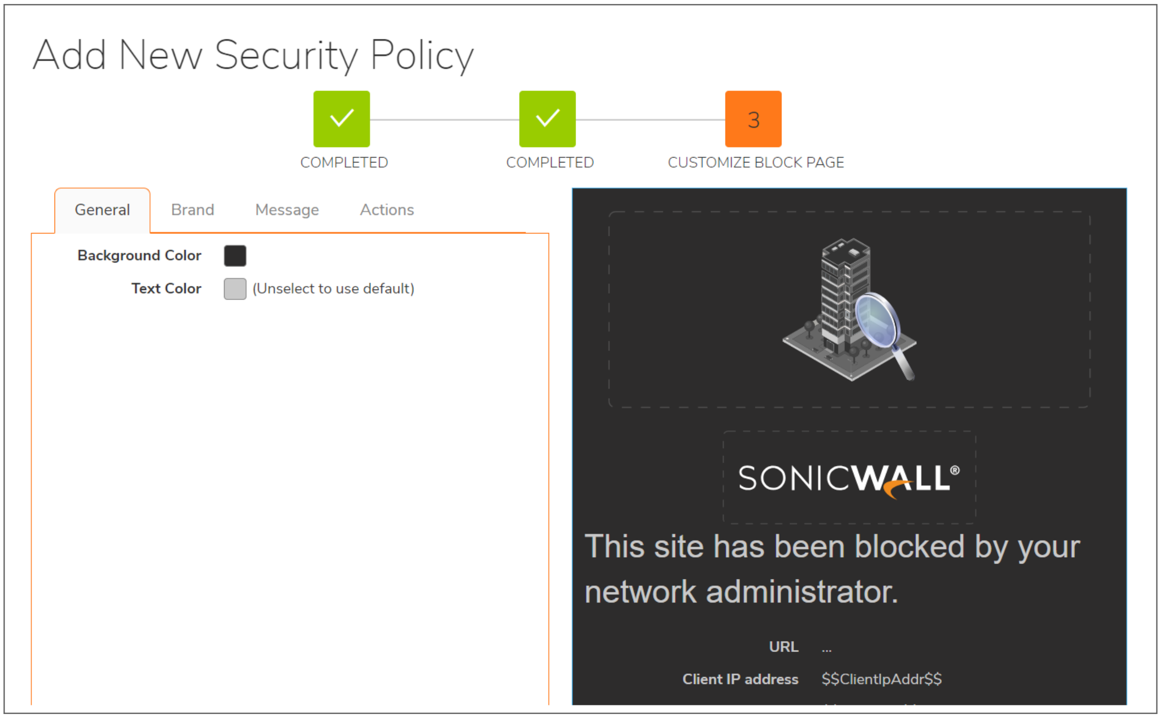
Customizing Blockpage

You can fully customize the web page that is displayed to the user when access to a blocked site is attempted.

The customized block message can be done when you are creating CFS, CATP, Cloud AV security policies. You can also edit the existing policies by clicking **Edit** icon and apply the customized blockpage to the selected policies.

To customize a blockpage:

1. Navigate to **Security > Security Policies**.
2. Click Add **+**. The **Add New Security Policy** page displays.
3. Enter a name and choose the type of Policy and click **Next.**
4. In the **Advanced page**, choose the required options and click **Next.**
5. In **Customize Block** Page, choose the options using the radio buttons.
   - **None -** When selected, the customize blockpage will be disabled. This is the default option.
   - **Using URL** - Choose this option if you would like to redirect to a specific URL. Enter the URL in **Input URL** text box.
   - **Using Template -** You can customize a template and show a personalized blockpage. Click the Edit icon and choose the template and error message to be displayed. A preview is displayed on the right view instantly for you to view the message and make changes.
     You can also upload a picture by clicking **Toggle Upload Pane** and choose an image.



Add New Security Policy

COMPLETED — COMPLETED — 3 CUSTOMIZE BLOCK PAGE

General | Brand | Message | Actions

Background Color ■

Text Color □ (Unselect to use default)

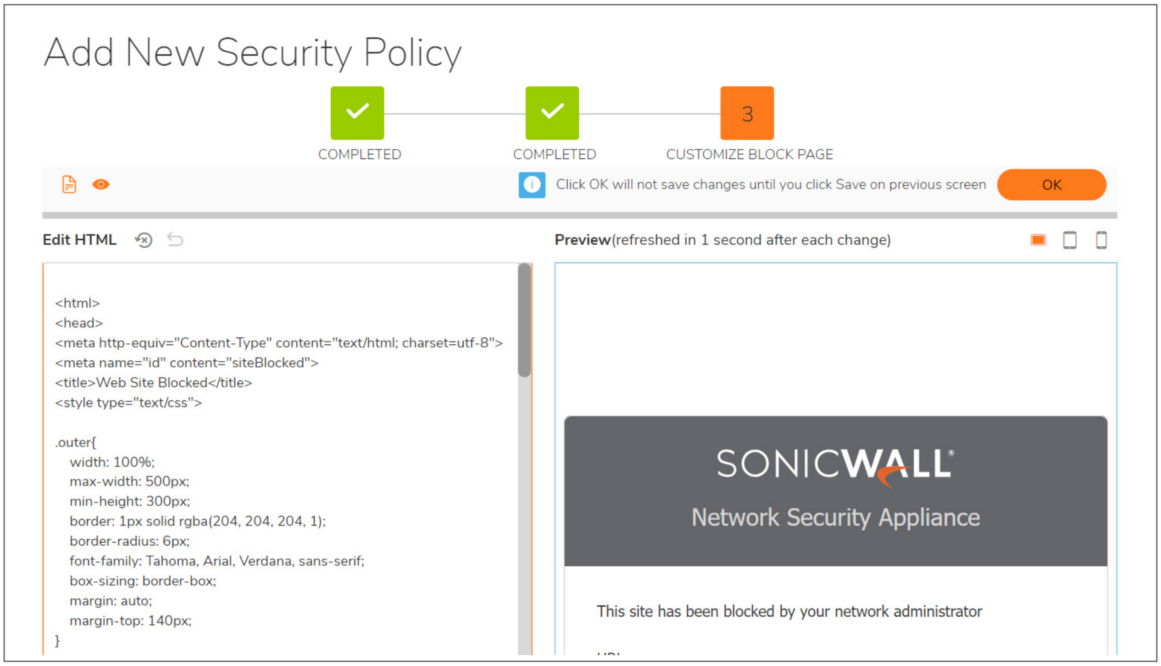
SONICWALL

This site has been blocked by your network administrator.

URL ...

Client IP address $$ClientIpAddr$$

- **Using HTML -** You can customize the block page by HTML. Click the edit icon and edit the HTML.



Add New Security Policy

COMPLETED — COMPLETED — 3 CUSTOMIZE BLOCK PAGE

Click OK will not save changes until you click Save on previous screen [OK]

Edit HTML

```
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<meta name="id" content="siteBlocked">
<title>Web Site Blocked</title>
<style type="text/css">

.outer{
    width: 100%;
    max-width: 500px;
    min-height: 300px;
    border: 1px solid rgba(204, 204, 204, 1);
    border-radius: 6px;
    font-family: Tahoma, Arial, Verdana, sans-serif;
    box-sizing: border-box;
    margin: auto;
    margin-top: 140px;
}
```

Preview(refreshed in 1 second after each change)

SONICWALL

Network Security Appliance

This site has been blocked by your network administrator

6. It is important to save the changes before proceeding to the next screen. Click **Save**.

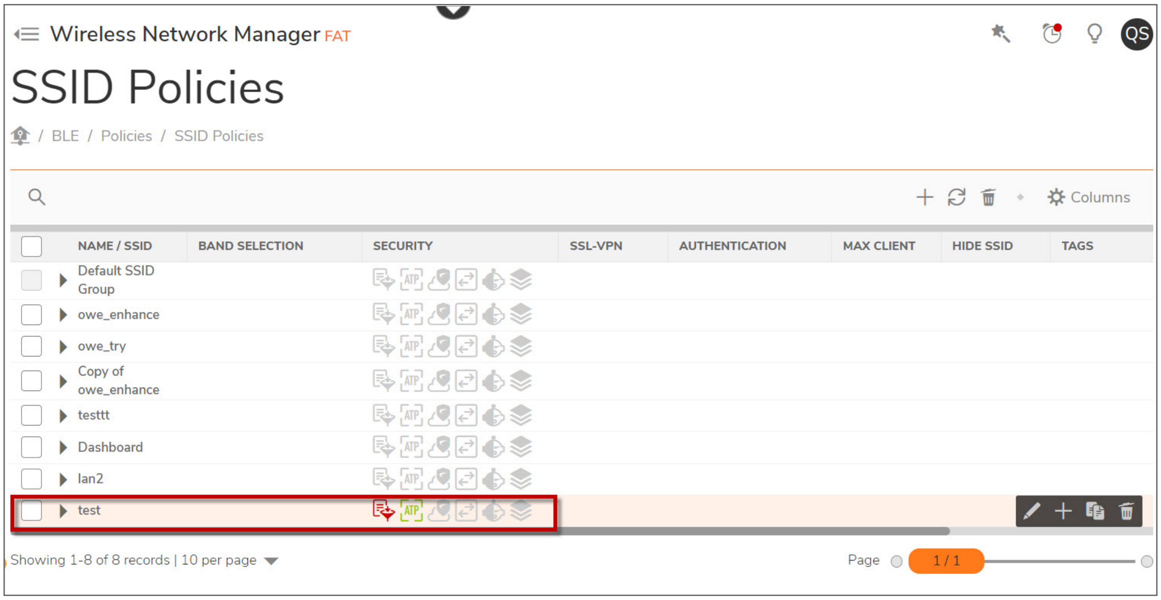
Applying a Security Policy to an SSID Group

Once you have created a Security Policy, such as a CFS or CATP policy, you can apply it to an SSID Group. This information applies to any security policy you create.

To apply a security policy to an SSID group:

1. Navigate to **Policies > SSID Policies**. A page displays that lists all of your SSID groups and the security policies applied to them.
2. Click **+ Add** at the top right to bring up the **Add SSID Group** page. This gives you the choice to create a new SSID group to which you can apply this policy.
3. Add an **SSID Group Name** and click **OK**. You have created an SSID Group to which you can apply the policy. It can be seen on the **SSID Policies** screen.
4. Click **+ Add** on the right side of the screen in the row for your SSID Group. The **Add SSID** screen displays.The name of the SSID you are adding appears in the title line of the page.
5. Click the **General > Basic**.
6. Enter the **SSID Name** you created.
7. Authenticate with your passphrase. This is mandatory.
8. Click the **Security Policy** tab.
9. From the drop down list, select the type of policy you want to apply.
10. Click **Save**.
11. On the **SSID Policies** screen, click to expand the SSID Group you created and show your SSID.
12. The **Security** column shows that the security policy is applied.
13. If you want to edit the SSID Group to have a different policy applied, click **Config/Edit** at the end of the row to go to the Edit SSID, with the name of the group in the title line.
14. Click **Security Policy** and select the policy to be applied.

15. Click **Save**, to see in the **Security** column that the correct policy has been applied.


Wireless Network Manager FAT
SSID Policies
/ BLE / Policies / SSID Policies
Columns
QS

□	NAME / SSID	BAND SELECTION	SECURITY	SSL-VPN	AUTHENTICATION	MAX CLIENT	HIDE SSID	TAGS
□	Default SSID Group							
□	owe_enhance							
□	owe_try							
□	Copy of owe_enhance							
□	testtt							
□	Dashboard							
□	lan2							
□	test		ATP					

Showing 1-8 of 8 records | 10 per page

Page 1 / 1

Capture Advanced Threat Protection

Capture Advanced Threat Protection (Capture ATP) is a cloud-based feature that analyzes files and determines if the file is malicious or acceptable. Capture ATP inspects files of up to 10MB, and is able to block threats before they can do any damage. All files submitted to Capture ATP are preprocessed before analysis, and separated in three categories. Malicious files are quarantined, while acceptable files are delivered directly to the client. If preprocessing determines a file to be malicious or acceptable, the file is not further analyzed by Capture ATP. Only the third category, those whose status cannot be immediately determined, are submitted to Capture ATP for complete analysis. Until this complete analysis is performed, Capture ATP works on the basis of Block Until Verdict if this option is selected. With Block Until Verdict, no files are delivered to the client before they pass rigorous analysis and are determined to be acceptable.

A streamlining feature called MD5 Hash Exclusion lists allows you to upload an MD5 hash and compare it with the SonicWall database of specified hash exclusions. This can speed up the analysis of files that are similar or the same as files that have recently been received for analysis.

Capture ATP supports many configurations of file types (archive files, executable files, Microsoft Office, Microsoft Office Extended , or PDF files). In order to expedite the process, the user has the possibility of excluding certain known files from file inspection, and either allow them or block them automatically.

ⓘ | **NOTE:** Wireless Network Manager supports the HTTP, SMTP, and FTP protocols.

For more information about Capture ATP, see the latest SonicOS *Security Configuration* administration documentation available under the product name Secure Wireless Access on the SonicWall support website at: https://www.sonicwall.com/support/technical-documentation/.

Topics:

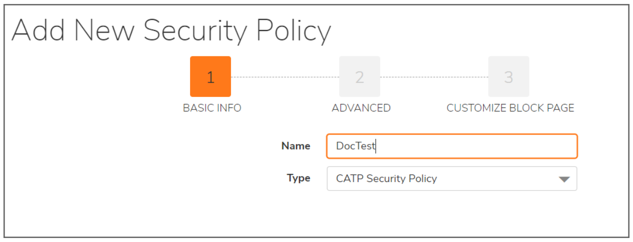
- Creating Capture Advanced Threat Protection Security Policies
- Adding an MD5 Hash to the Exclusion List

Creating Capture Advanced Threat Protection Security Policies

In order to take advantage of Capture Advanced Threat Protection (CATP or Capture ATP), create Capture ATP security policies as described below and select the categories of files you want to block. Once you have created a policy, apply it to an SSID group as explained in Applying a Security Policy to an SSID Group.

To create a Capture ATP security policy:

1. Navigate to **Security > Security Policies**.
2. Click **Add +** to add a new security policy. The **Add New Security Policy** page displays.
3. Enter the name of the policy.
4. From the **Policy Type** list, select **CATP Security Policy**.



Add New Security Policy

Name DocTest

Type CATP Security Policy

5. Click **Next**. The **Advanced** page displays.
6. In the **General** section, click **Enable** to enable the Capture ATP policy you have selected. Unselect it to disable the policy.
7. Choose the **Schedule** from the drop-down list.
8. Click the **Block Until Verdict** to enable to decide whether questionable files should be allowed to pass.

   If you are not concerned about their safety, you can allow them. If you do not want to take the chance of their being dangerous, select **Block Until Verdict**.
9. Optionally, you can set a **Maximum File Size**. The default maximum size is 10240 bytes. For SonicWave 231c/224w/231o models, the maximum size will reduce to 5120KB due to limited memory."
   The following table shows the maximum size supported on the models:

Models	Maximum size
SonicWave231c/231o/224w	5,120 KB
SonicWave432i/432e/432o	10,240 KB
SonicWave621	1,024 KB
SonicWave641/681	10,240 KB

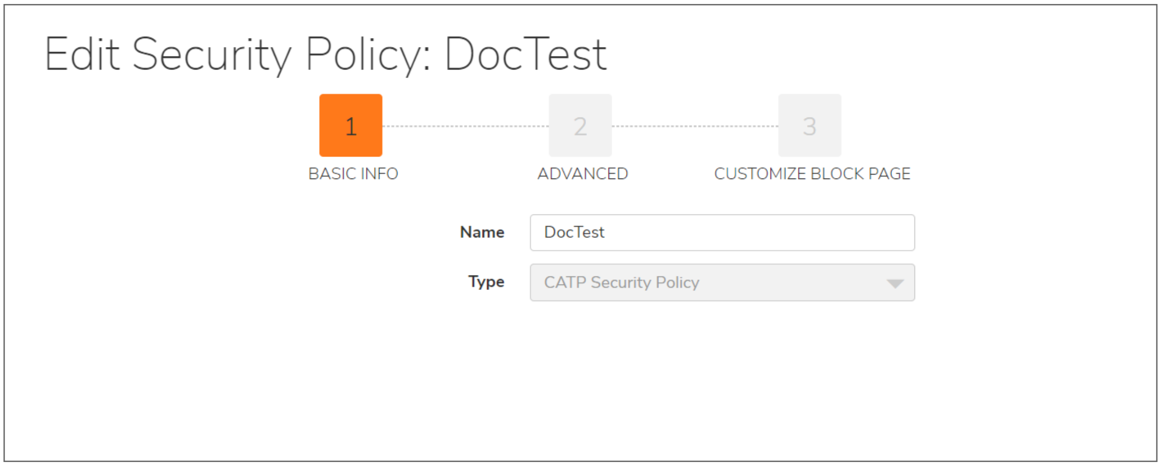
10. You can set the acceptable files types by checking any of the **File Types** boxes.
11. Select the **Protocol(s)** as required.
12. Specify the **MD5 Exclusion List**. For more information, refer to Adding an MD5 Hash to the Exclusion List.
13. Click **Save** to save your selections.

The policy is now listed on the **Security > Security Policies** page.

Adding an MD5 Hash to the Exclusion List

To add an MD5 hash to the exclusion list for a CATP policy:

1. Navigate to **Security > Security Policies**.
2. Click **Edit** next to the CATP policy. The **Edit Security Policy** screen displays.

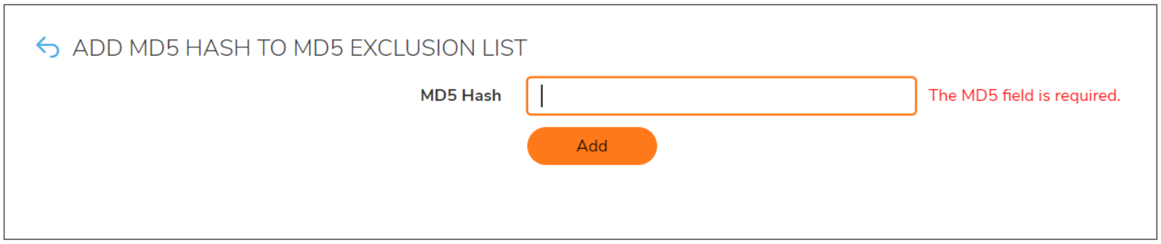


Edit Security Policy: DocTest

Name: DocTest

Type: CATP Security Policy

3. Click **Next** to go to the **Advanced** page.
4. In the **MD5 Exclusion List** section at the bottom of the screen, click the **+** icon. The policy-specific **Edit Security Policy** screen appears, allowing you to add an MD5 Hash to the MD5 Exclusion List.
5. Type the 32-digit hexadecimal number in the **MD5 Hash** field.



ADD MD5 HASH TO MD5 EXCLUSION LIST

MD5 Hash:

The MD5 field is required.

6. Click **Add**.
7. Click **OK**.

The MD5 hash is added to the **MD5 Exclusion List**.

Cloud Anti-Virus

Cloud Anti-Virus (Cloud AV) is an advanced feature of Wireless Network Manager. This cloud-based anti-virus service provides real-time file virus scanning and reporting without consuming local computing resources. Multi-Engine Cloud AV is supported on the SonicWave appliance. Once you have created Cloud AV security policies, you can add them to an SSID group by following the steps in Applying a Security Policy to an SSID Group.

To create a new Cloud AV policy:

1. Navigate to **Security > Security Policies**.
2. Click **Add +**. The first **Add New Security Policy** displays.
3. In the **Name** field, enter the name of the security policy you want to add.
4. From the **Type** list, select **Cloud-AV Security Policy**.
5. Click **Next**. The **Advanced** Page displays. Select the required options, as required. These include **General**, **File Types**, **Protocols**, and **MD5 Exclusion List**.
6. Click **Next** to go to the **Customize Block** Page.
7. Specify the required options in the **Customize Block** page.
8. Select the desired options and click **Save**.

Access Control Policies

The Access Control Policies (ACL) manages access to MAC Address Objects and Access Object groups. Once you have created and configured the security policy, you can apply it to an SSID group as explained in Applying a Security Policy to an SSID Group.

Topics:

- Creating Mac Address Objects
- Creating Address Object Groups
- Creating and Editing Access Control Policies

Creating and Editing Access Control Policies

Create or edit the Access Control Policies (ACLs) to allow or deny access to address objects or address groups.

To create or edit an access control policy:

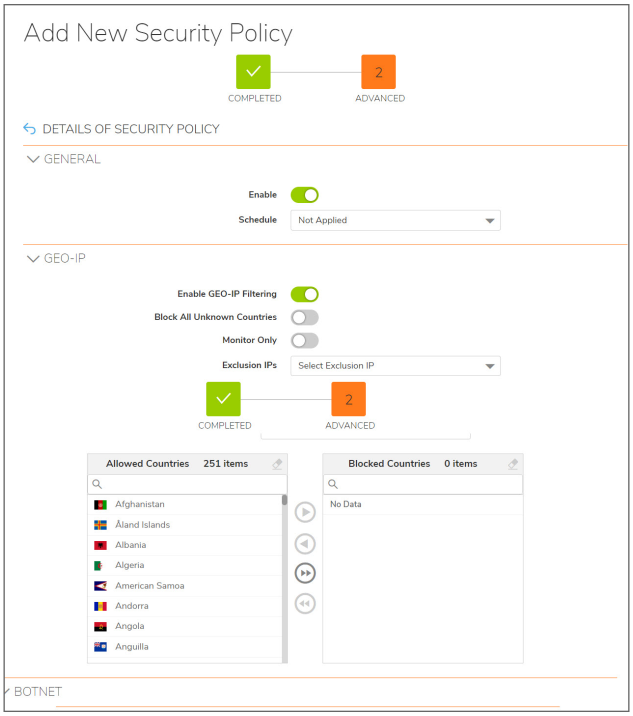
1. Navigate to **Security > Security Policies**.
2. Click **Add +** or **Config/Edit**. The **Add/Edit New Security Policy** page displays.
3. Enter an **ACL Policy Name**.

4. From the **Type** list, select **ACL Security Policy**.
5. Click **Next**. The **Advanced** screen displays.
6. In the **General** section, click **Enable** to enable the access control security policy.
7. In the **Authentication /Association MAC Filtering** section, select the **Mode** and **Client MAC Address Group**.
8. In the **ACL** section, Select **Deny** or **Allow** from the **Mode** menu as required.
9. From the **Address Group** list, select an address group or create an address object group from the **Security > Security Objects** page. For more information, refer to Applying a Security Policy to an SSID Group.
10. In the **Bandwidth Management** section, click **Enable** to enable bandwidth management.
11. Configure the other fields in the section.
12. Be sure **All Clients** is disabled, so that you can apply this new policy to a group of SSIDs.
13. Select the **Client IP Group** on the field that appears when you disable **All Clients**.
14. For the **Client IP Address Group**, select a new ACL security object .
15. Click **OK** to apply the changes.
16. Navigate to **Policies > SSID Policies**.
17. Click **+ Add** on the end of the row SSID for **Default SSID Group**. The **Add SSID for Default SSID Group** screen displays.
18. Click **Security Policy**.
19. Choose the policy you want applied from the drop down list.
20. Click **OK** to apply the ACL policy.

The ACL policy is configured and added to the list.

Geo-IP & Botnet

These two security features provide extra safety by allowing you to choose specific countries to block, or to block attacks from Botnets. These are networks of compromised computers transmitting malware, spam, or other destructive files. Each of these features need separate licenses, available from MySonicWall.



Add New Security Policy

DETAILS OF SECURITY POLICY

GENERAL

Enable: ●

Schedule: Not Applied

GEO-IP

Enable GEO-IP Filtering: ●

Block All Unknown Countries: ○

Monitor Only: ○

Exclusion IPs: Select Exclusion IP

Allowed Countries 251 items	Blocked Countries 0 items
Afghanistan	No Data
Åland Islands	
Albania	
Algeria	
American Samoa	
Andorra	
Angola	
Anguilla	

BOTNET

This page gives you the options of enabling Geo-IP and/or Botnet blocking on this policy.

1. Fill in your **GEO-IP** and **Botnet** choices, including any IPs you wish to exclude from the ban.
2. Click **Save** to apply the selections you have made.

Application Control

Application awareness is crucial to application control, which is an important feature of modern firewall systems. There are types of applications that Wireless Network Manager can detect include:

- Application Protocols: Such as FTP and SSH, which represent communications between hosts
- Clients: Such as web browsers and email clients, which represent software running on the host
- Web Applications: Such as MPEG video and Facebook, which represent the content or requested URL for HTTP traffic

Wireless Network Manager allows SonicWave access points to detect applications and control their activities on your network. Wireless Network Manager identifies applications in network traffic according to the characteristics specified in the detector. For example, the system can identify an application by an ASCII pattern in the packet header.

For more information refer to App Objectsand APP Control Security Policy

Managing SNMP Policies

Wireless Network Manager provides support for SNMP v3 for SonicWave devices.

Topics:

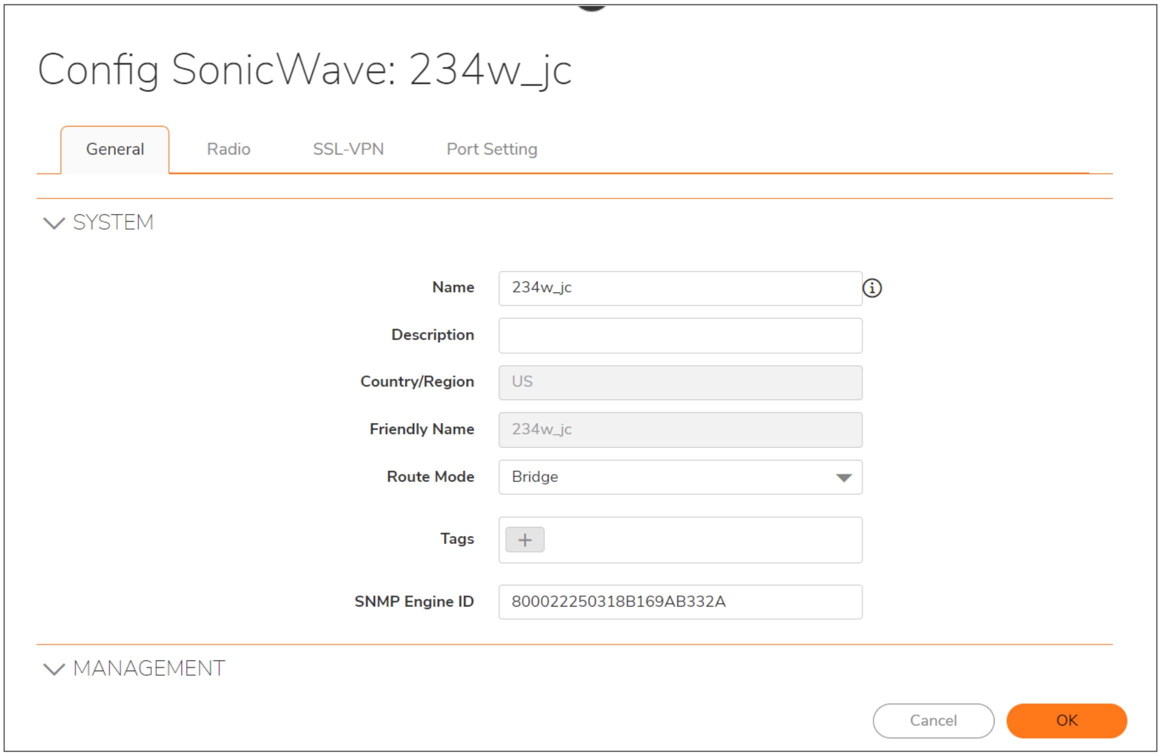
Setting the SNMP ID

Each SNMP agent maintains local information to be used in SNMP v3 message exchanges so that the agent receives incoming messages and sends Trap messages to a manager.

ⓘ | **IMPORTANT:** The **SNMP Engine ID** must be defined before SNMP v3 can be enabled.

To set the SNMP ID:

1. Navigate to **Network > Devices**.
2. On the far right of the line in the list for the device you want to configure, click the **Edit (pencil)** icon. The **Config SonicWave** page is displayed.
3. Click on the **General** tab.
4. In the **System** section, in the **SNMP Engine ID** field, enter the SNMP engine ID.


Config SonicWave: 234w_jc

Name	234w_jc
Description	
Country/Region	US
Friendly Name	234w_jc
Route Mode	Bridge
Tags	+
SNMP Engine ID	800022250318B169AB332A

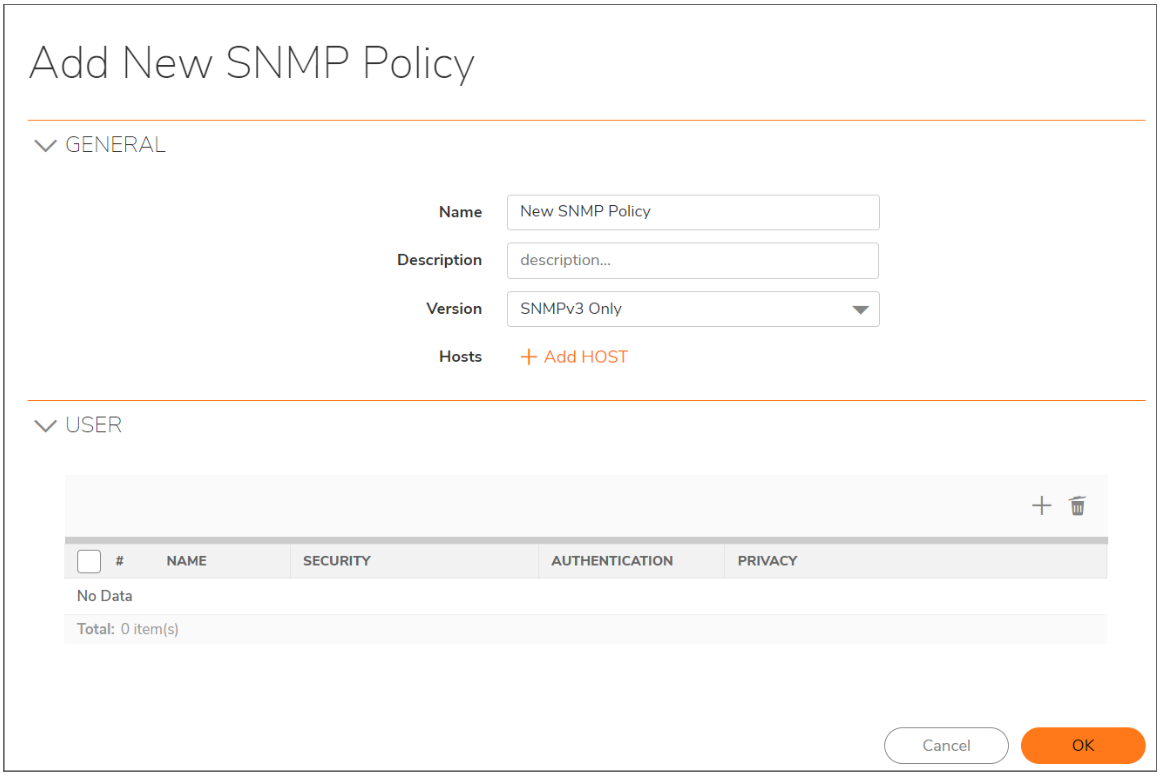
5. Click **OK**.

Adding SNMP Policies

To add an SNMP policy:

1. Navigate to **Policies > SNMP Policies**.
2. Click the **Add Policy** icon (**+**) at the top left of the table. The **Add New SNMP Policy** dialog displays.
3. In the **General** section:
    a. In the **Name** field, enter a name for the policy.
    b. In the **Description** field, enter a brief description for the policy. (This field is optional.)

c. From the **Version** list, select the SNMP version to which the policy should apply.



Add New SNMP Policy

GENERAL

Name: New SNMP Policy

Description: description...

Version: SNMPv3 Only

Hosts: + Add HOST

USER

□	#	NAME	SECURITY	AUTHENTICATION	PRIVACY

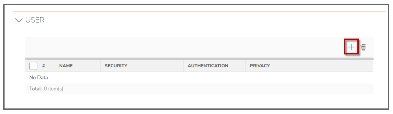
No Data

Total: 0 item(s)

d. Add Hosts by clicking **+ Add HOST**.

4. In the **User** section:

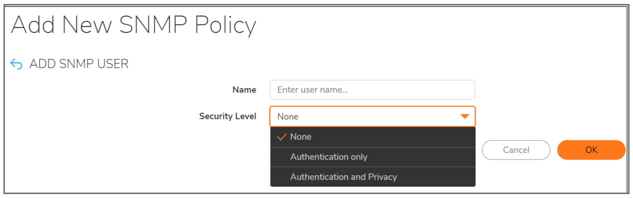
a. Click the **Add User** icon (**+**) at the top left of the table. The **Add SNMP User** dialog displays.



b. In the **Name** field, enter the name for the user.

c. From the **Security Level** list, list the security level you want applied to the user:

- **None**
- **Authentication only**
- **Authentication and Privacy**



Add New SNMP Policy

ADD SNMP USER

Name: Enter user name...

Security Level: None

d. If you selected the opion **Authentication Only,** from the **Authentication Method** list, select authentication method you want used. In the **Authentication Key** field, enter the authentication key.

e. If you selected the opion **Authentication and Privacy**, from the **Encryption Method** list, select encryption method you want used. In the **Encryption Key** field, enter the encryption key. (**Authentication and Privacy** only)

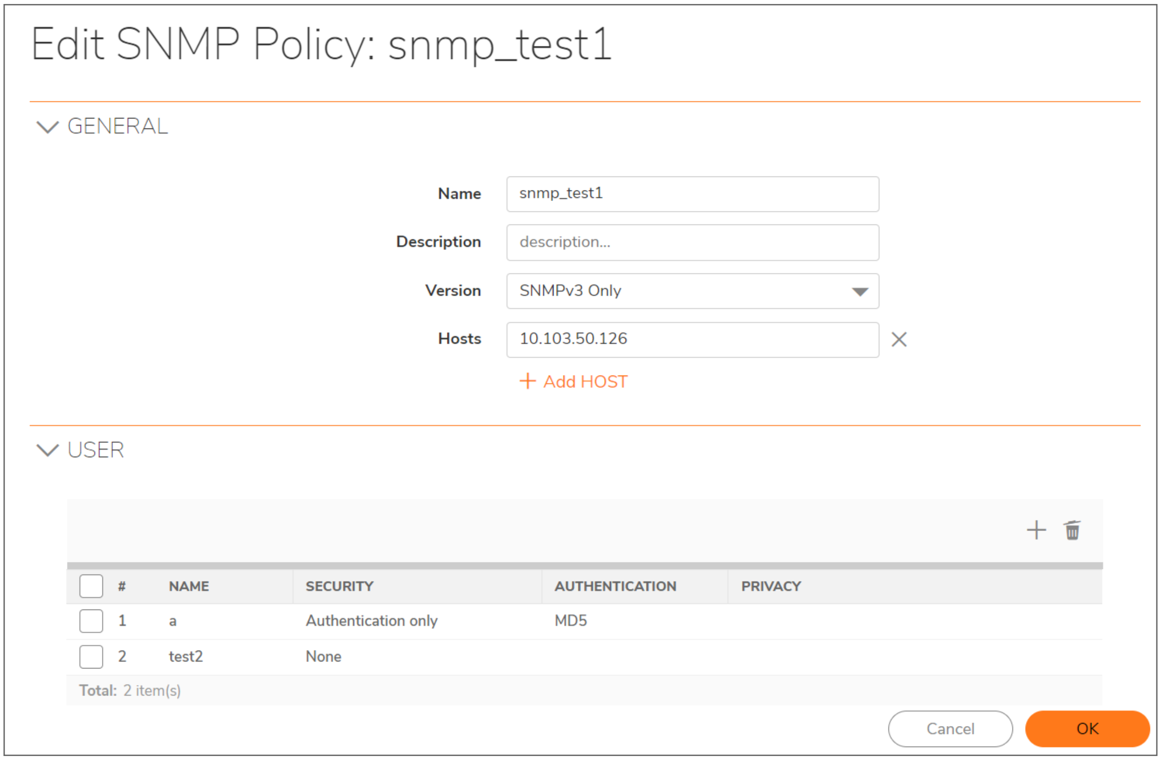
f. Click **OK**.

5. Click **OK** to add policy.

Editing SNMP Policies

To edit an SNMP policy:

1. Navigate to **Policies > SNMP Policies**.
2. Click the **Edit** icon (pencil) on far right of the line in the table where the policy is listed. The **Edit SNMP Policy** dialog displays.



Edit SNMP Policy: snmp_test1

GENERAL

Name	snmp_test1
Description	description...
Version	SNMPv3 Only
Hosts	10.103.50.126

USER

□	#	NAME	SECURITY	AUTHENTICATION	PRIVACY
□	1	a	Authentication only	MD5	
□	2	test2	None		

Total: 2 item(s)

3. Make any changes needed to the fields. (Refer to Adding SNMP Policies for more information about each of the fields.)
4. Click **OK**.

Deleting SNMP Policies

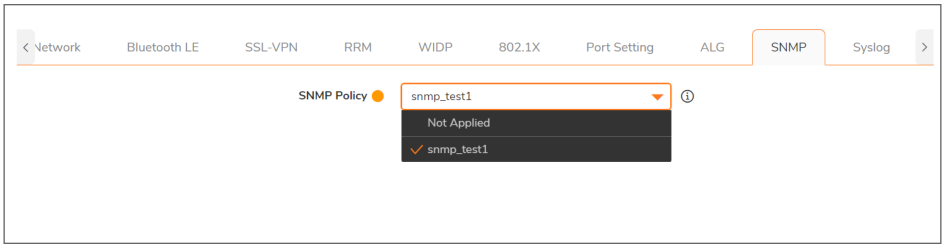
To edit an SNMP policy:

1. Navigate to **Policies > SNMP Policies**.
2. Click the **Delete** icon on far right of the line in the table where the policy is listed. A confirmation dialog displays.
3. Click **OK**.

Setting SNMP Policies

To set an SNMP policy:

1. Navigate to **Policies > AP Policies**.
2. You can create a new policy or edit an existing one. Click + to add a new policy or ✎ to edit the existing one.
3. The **Add Policy** or **Edit Policy** dialog displays.
4. Click on the **SNMP** tag.



SNMP Policy ● snmp_test1

Not Applied

✓ snmp_test1

5. From the **SNMP Policy** list, select the SNMP policy you want to apply for the device.

For information on creating SNMP policies, refer to Adding SNMP Policies.

Managing Switch SNMP Policies

Wireless Network Manager provides support for Switch SNMP for SonicWave devices.

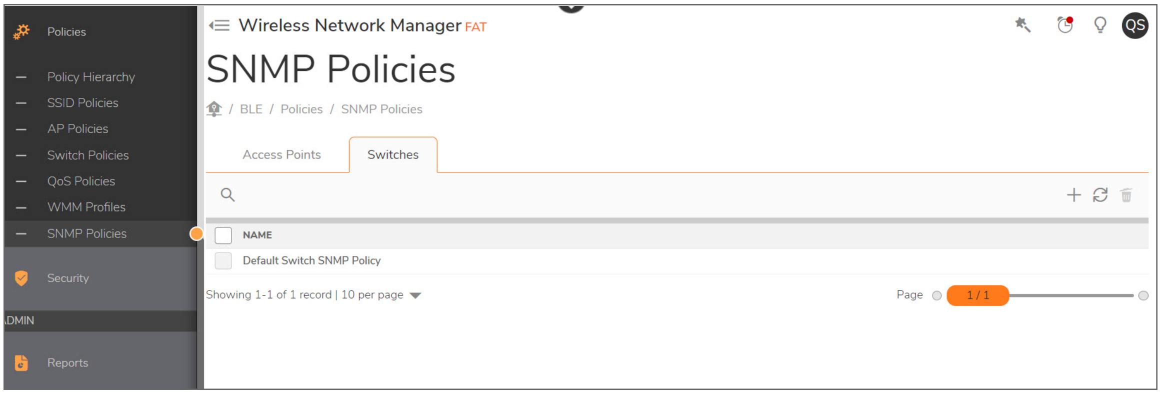
Topics:

- Adding Switch SNMP Policies
- Editing Switch SNMP Policies
- Applying Switch SNMP Policies

Adding Switch SNMP Policies

To add a Switch policy:

1. Navigate to **Policies > SNMP Polices**.
2. Go to **Switches** tab.



SNMP Policies

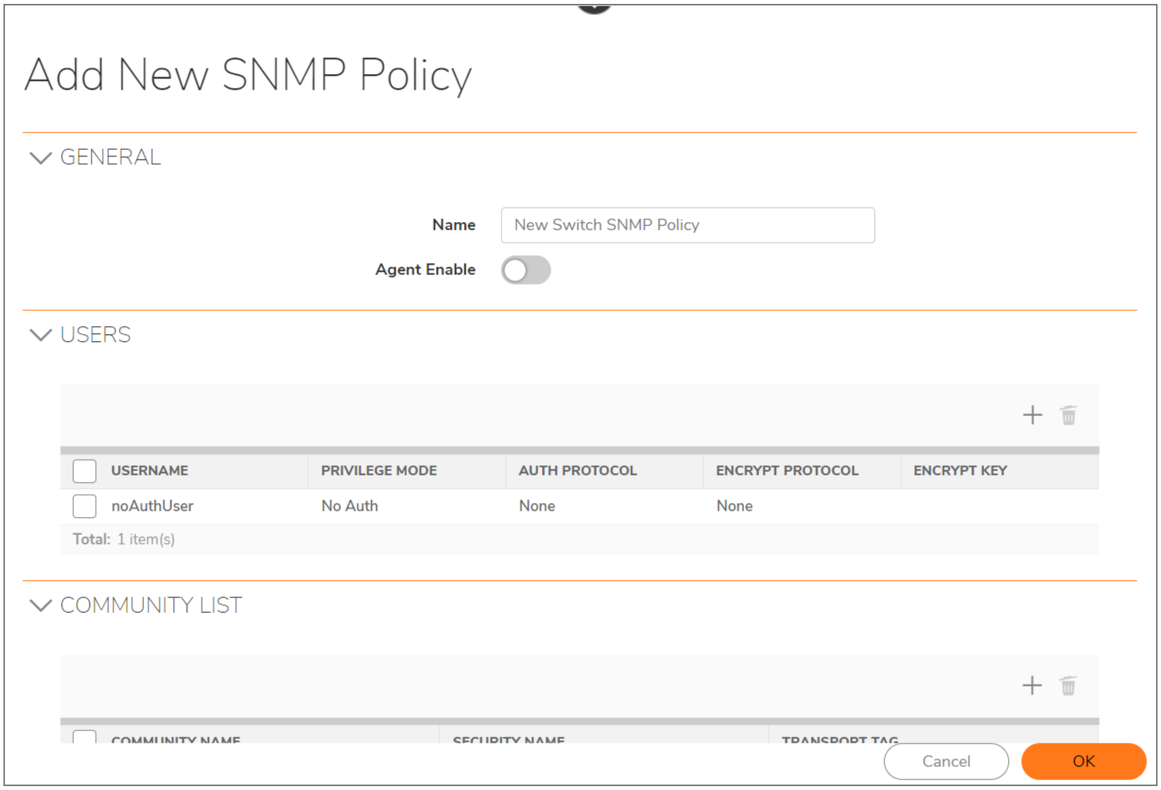
/ BLE / Policies / SNMP Policies

☐	NAME
☐	Default Switch SNMP Policy

Showing 1-1 of 1 record | 10 per page

Page 1 / 1

3. Click the **Add Policy** (**+**) icon to create a policy. The **Add New SNMP Policy** page displays.



Add New SNMP Policy

GENERAL

Name: New Switch SNMP Policy

Agent Enable: ○

USERS

☐	USERNAME	PRIVILEGE MODE	AUTH PROTOCOL	ENCRYPT PROTOCOL	ENCRYPT KEY
☐	noAuthUser	No Auth	None	None	

Total: 1 item(s)

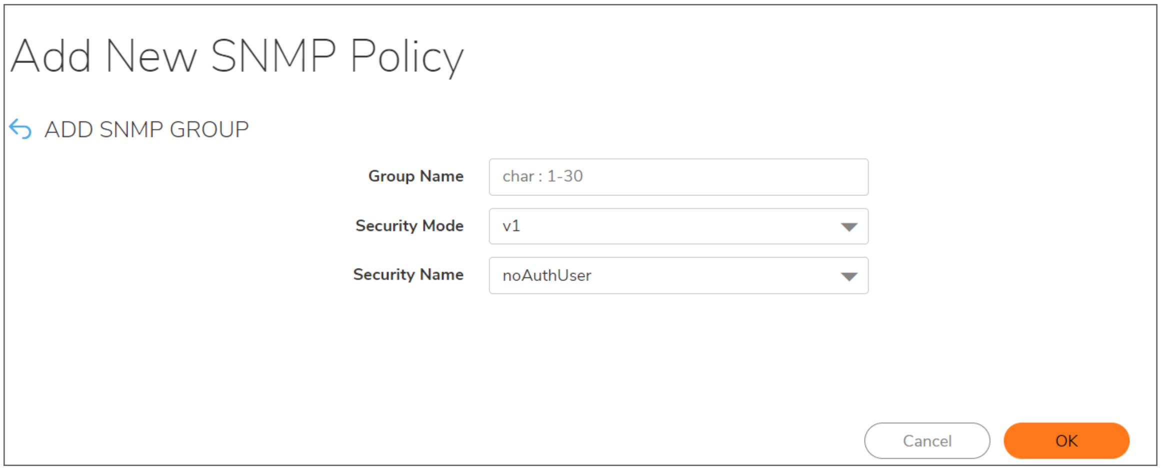
COMMUNITY LIST

☐	COMMUNITY NAME	SECURITY NAME	TRANSPORT TAG

4. Enter the **Switch Policy Name**.

5. In the Users section, click **+** to create a new user.
6. Add the **Privilege Mode**, **Authentication Protocol**, **Authentication Password**, **Encrypt Protocol**, and **Encrypt Key**.
7. Add other parameters including **Community List**, **Group List**, **Access List**, **View List**, **Target Params**, **Target Address**, and **Notify Settings** as required.

   Clicking on + pertaining to each option displays a new window with the fields to be added. For example, if you click on + pertaining to the **Group List** option, a new window **Add SNMP Group** is displayed as given below.



Group Name: char : 1-30

Security Mode: v1

Security Name: noAuthUser

   Similarly add each options as per your requirement.

8. Click **OK**. The newly created SNMP Policy will get displayed under the **Switches** Tab.

For more information on configuring and using the SonicWall Switch, refer to the *Switch Administration Guide*. This and other documentation are available under the product name “Switch” on theSonicWall support website at: https://www.sonicwall.com/support/technical-documentation/.

Editing Switch SNMP Policies

To edit a Switch SNMP policy:

1. Navigate to **Policies > SNMP Polices**.
2. Click the **Edit** (pencil) icon to edit an existing policy. The **Edit SNMP Policy** page displays.
3. Update the required options for the existing policy.
4. Click **OK**.

For more information on configuring and using the SonicWall Switch, refer to the *Switch Administration Guide*. This and other documentation are available under the product name “Switch” on the SonicWallSonicWall support website at: https://www.sonicwall.com/support/technical-documentation/.

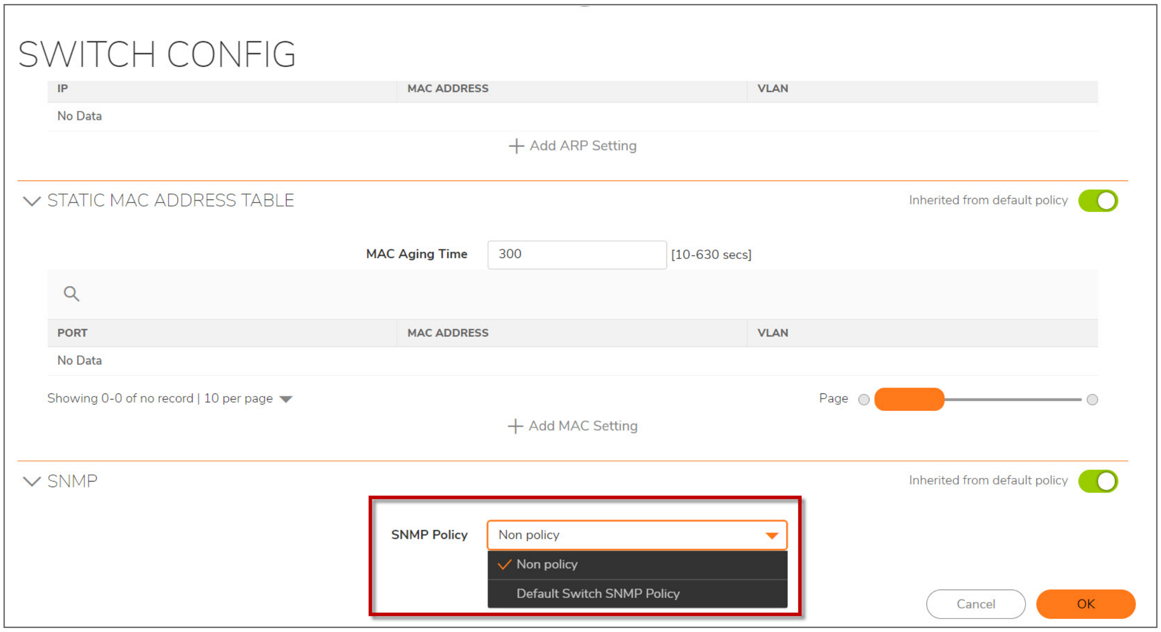
Applying Switch SNMP Policies

Once you have created a Switch SNMP policy, you can apply the object you created. This information applies to any security policy you create.

After attaching Switch SNMP Policy to Switch Policies, the SNMP feature will work on Switch.

To apply SNMP Switch Policies:

1. Navigate to **Policies > Switch Policies.**
2. Click ✎ and edit an existing switch policy, or create a new policy clicking **+**.
3. Go to **System** tab and scroll down to **SNMP** section.
4. Choose the policy from the drop-down list.



SWITCH CONFIG

IP	MAC ADDRESS	VLAN
No Data		

+ Add ARP Setting

STATIC MAC ADDRESS TABLE — Inherited from default policy

MAC Aging Time: 300 [10-630 secs]

PORT	MAC ADDRESS	VLAN
No Data		

Showing 0-0 of no record | 10 per page

SNMP — Inherited from default policy

SNMP Policy: Non policy

5. Click **OK**.

6

Objects

Topics:

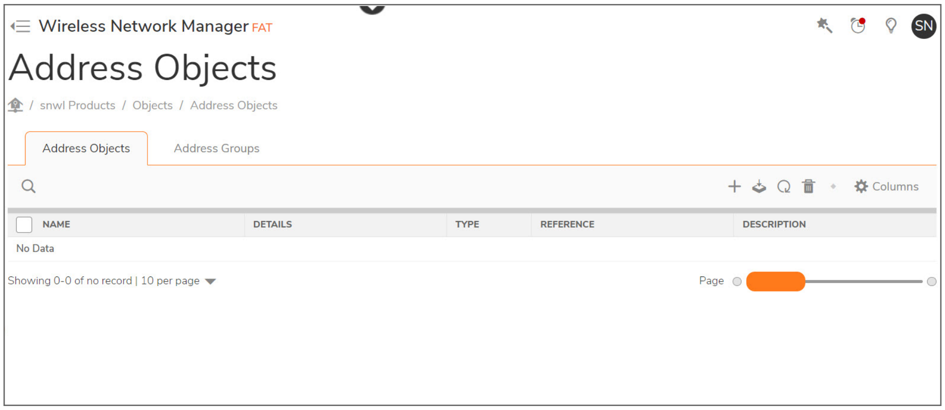
- Address Objects
- Service Objects
- Matched Objects
- QoS Objects
- Schedule Objects
- App Objects

Address Objects

The **Objects > Address Objects** page provides options for creating or editing security objects. The objects can be edited as:

- **Address Objects**
- **Address Groups**

The **Address Objects** page displays a list of address objects with their applied security policies, where you can configure or delete object.


Wireless Network Manager FAT
SN
Address Objects
/ snwl Products / Objects / Address Objects
Address Objects
Address Groups
Columns
Page

NAME	DETAILS	TYPE	REFERENCE	DESCRIPTION
No Data				

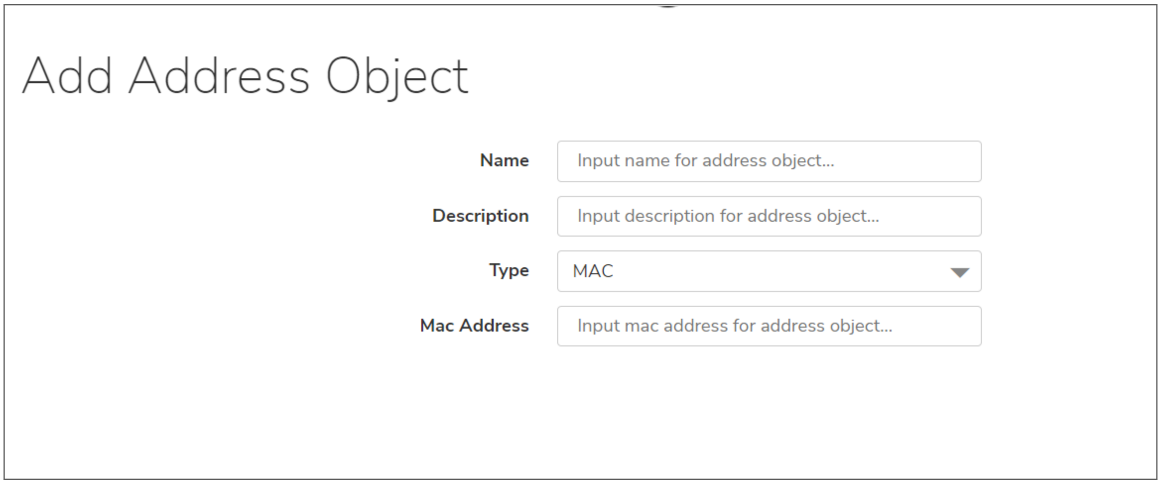
Showing 0-0 of no record | 10 per page

The **Address Objects** page also provides you the option to import Address Objects from Excel. To do this, select the file to import and click ⬇ to display the **Import MAC Addresses** window. Select a file to import and click **Import**.

Creating Mac Address Objects

To create a MAC address object:

1. Navigate to **Objects > Address Objects**
2. Click **Add +**. The **Add Address Object** screen displays.



Add Address Object

Name	Input name for address object...
Description	Input description for address object...
Type	MAC
Mac Address	Input mac address for address object...

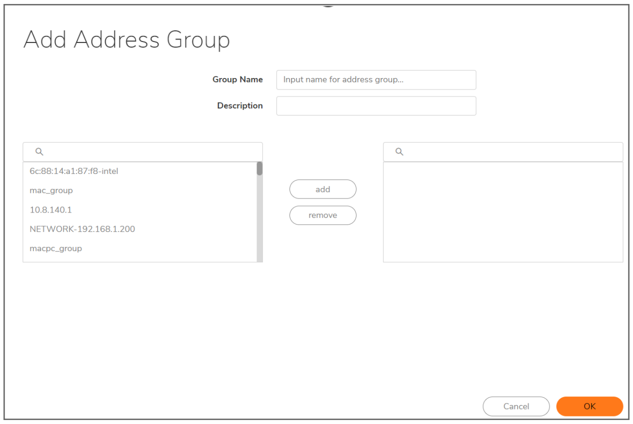
3. Enter a **Name** for the address object.
4. Enter a **Description** for the address object.
5. From the **Type** list, select **MAC**.
6. Enter the **MAC Address** for the address object.
7. Click **OK**.

The MAC address is added to the **Address Objects** list.

Creating Address Object Groups

To create an address object groups:

1. Navigate to **Objects > Address Groups**.
2. Click **Add +**. The **Add Address Group** page displays.



Add Address Group

Group Name: Input name for address group...

Description:

3. On this screen, you can choose the settings for the group.

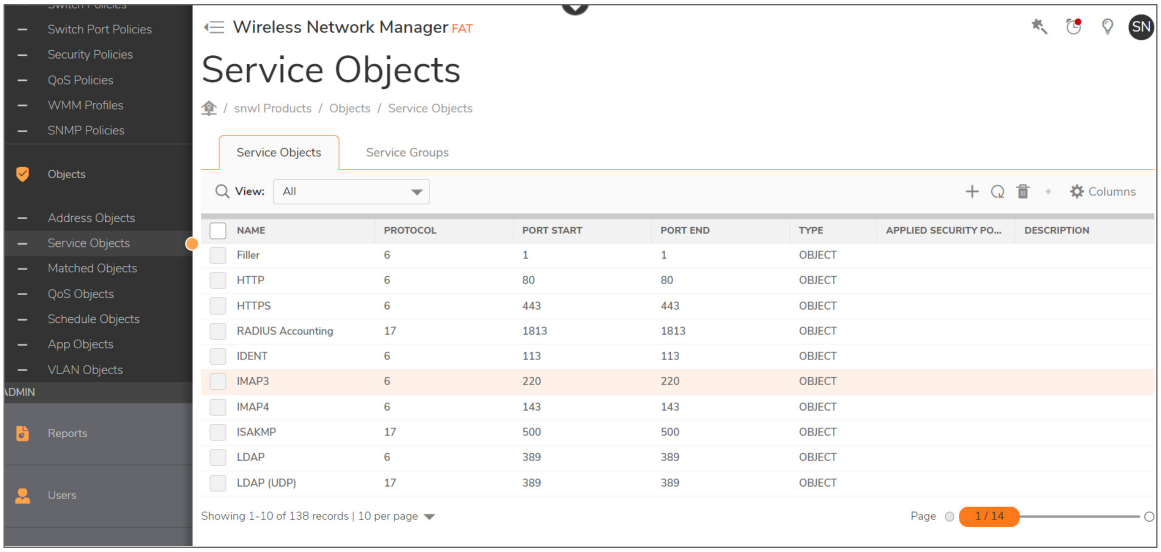
   Fill in the group **Name** and **Description**, then add or remove settings by moving them left or right.

4. Click **OK** to add the address group.

The Address Group is added to the list.

Service Objects

The **Objects > Service Objects** page provides options for creating or editing Service Objects and Service Groups.



Service Objects

View: All

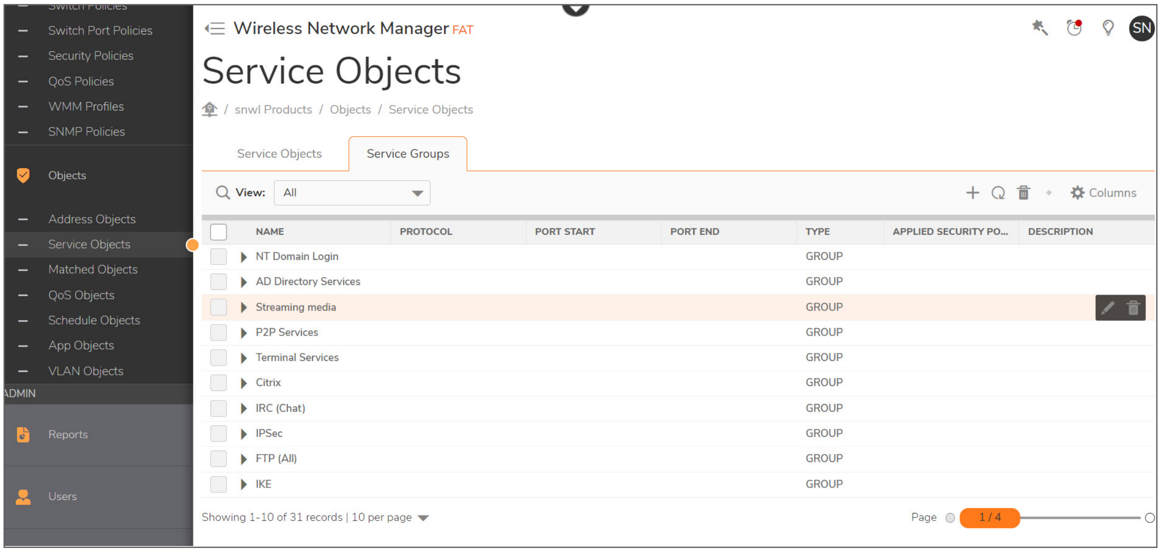
NAME	PROTOCOL	PORT START	PORT END	TYPE	APPLIED SECURITY PO...	DESCRIPTION
Filler	6	1	1	OBJECT		
HTTP	6	80	80	OBJECT		
HTTPS	6	443	443	OBJECT		
RADIUS Accounting	17	1813	1813	OBJECT		
IDENT	6	113	113	OBJECT		
IMAP3	6	220	220	OBJECT		
IMAP4	6	143	143	OBJECT		
ISAKMP	17	500	500	OBJECT		
LDAP	6	389	389	OBJECT		
LDAP (UDP)	17	389	389	OBJECT		

Showing 1-10 of 138 records | 10 per page

Page 1 / 14

Service Group

The **Service Group** tab displays the available application groups. You can also create, modify, and delete on this tab.



NAME	PROTOCOL	PORT START	PORT END	TYPE	APPLIED SECURITY PO...	DESCRIPTION
NT Domain Login				GROUP		
AD Directory Services				GROUP		
Streaming media				GROUP		
P2P Services				GROUP		
Terminal Services				GROUP		
Citrix				GROUP		
IRC (Chat)				GROUP		
IPSec				GROUP		
FTP (All)				GROUP		
IKE				GROUP		

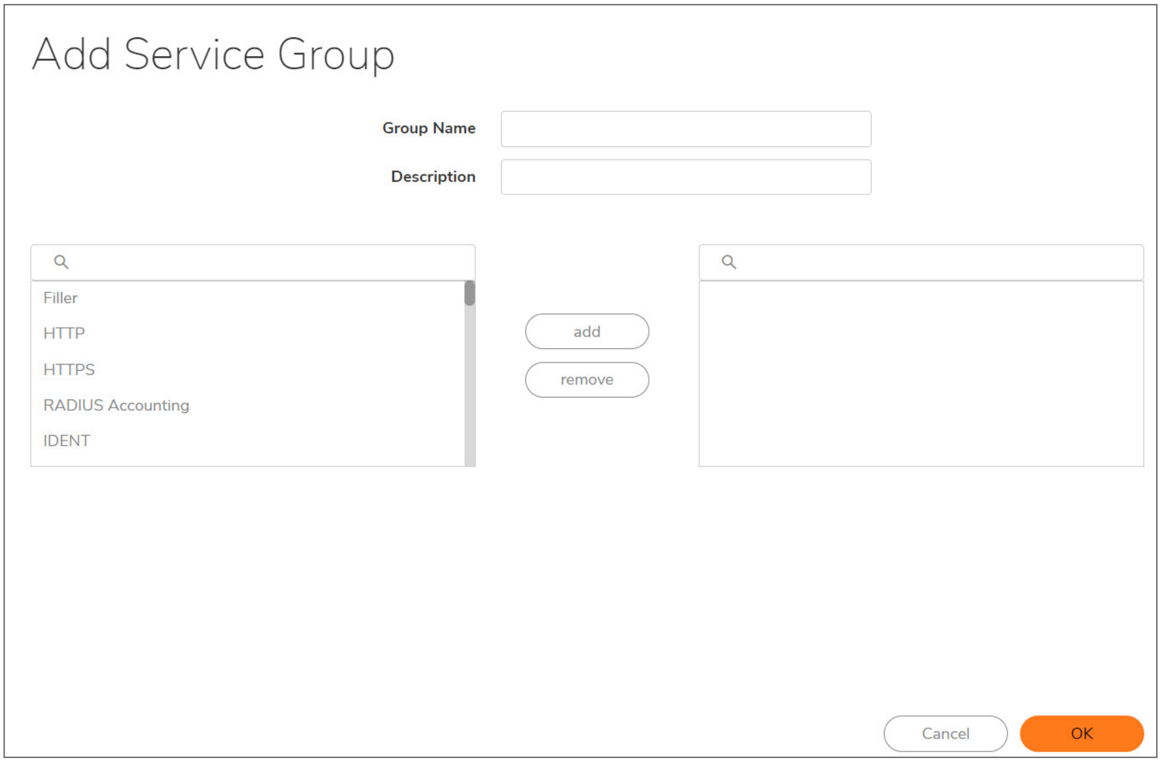
Showing 1-10 of 31 records | 10 per page

1 / 4

To create a new Service Group:

1. Navigate to **Objects > Service Objects**.
2. Click the **Service Group** tab.

3. Click Add (**+**). The **Add Service Group** dialog displays.



Add Service Group

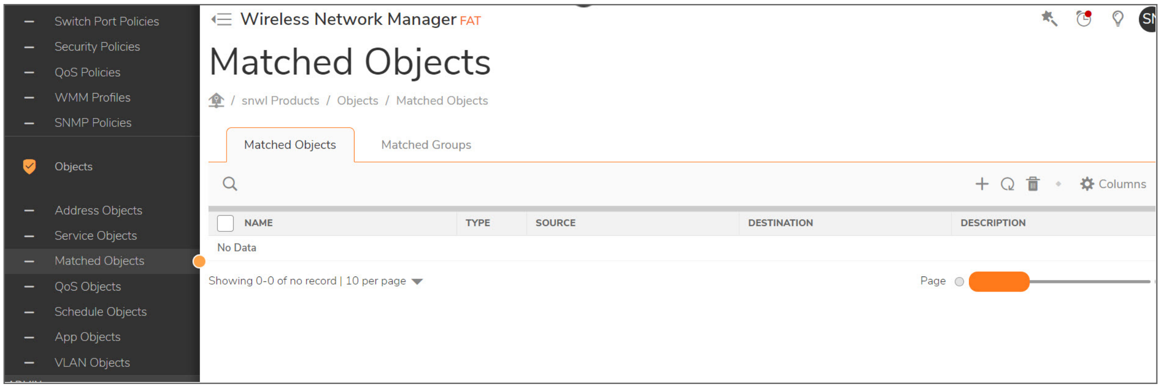
Group Name

Description

4. Specify a group **Name** and **Description**.
5. From the list, select **service-protocols**.
6. In list on the left, select the protocols you want included in your new App Group. On this screen, you can choose the settings for the group.
7. Click **Add**.
8. Click **OK**.

Matched Objects

The **Objects > Matched Objects** page provides options for creating or editing Matched Objects and Matched Groups.

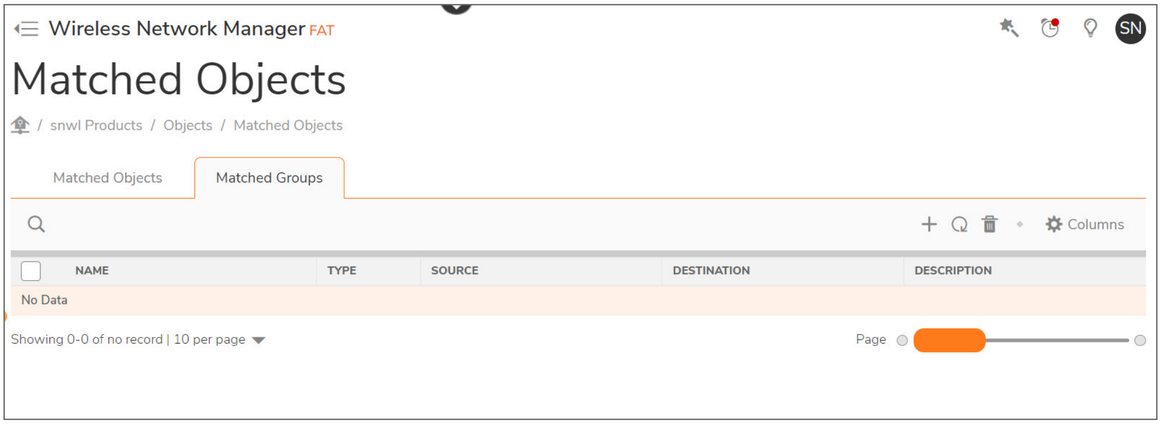


NAME	TYPE	SOURCE	DESTINATION	DESCRIPTION
No Data				

Showing 0-0 of no record | 10 per page

Matched Group

The **Matched Group** tab displays the available matched groups. You can also create, modify, and delete matched groups on this tab.


Wireless Network Manager FAT
SN
Matched Objects
snwl Products / Objects / Matched Objects
Matched Objects
Matched Groups
Columns

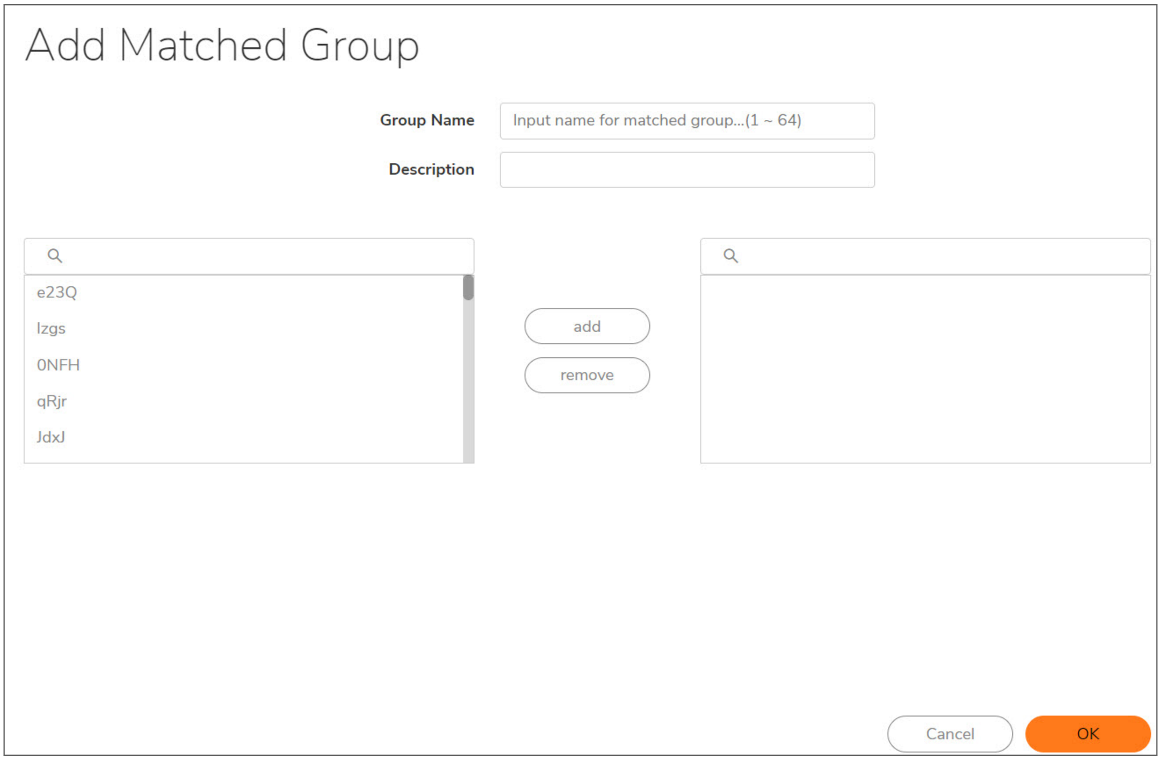
NAME	TYPE	SOURCE	DESTINATION	DESCRIPTION
No Data				

Showing 0-0 of no record | 10 per page

To create a new Matched Group:

1. Navigate to **Objects > Matched Objects**.
2. Click the **Matched Group** tab.

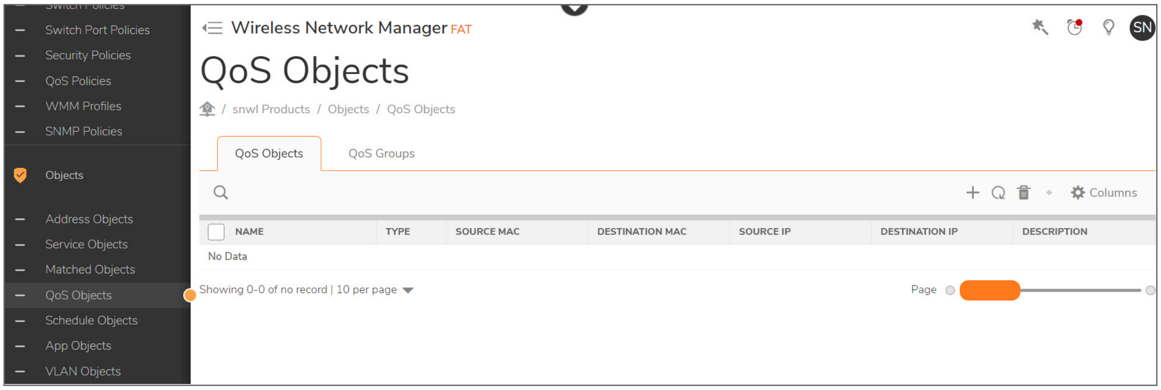
3. Click Add (**+**). The **Add Matched Group** dialog displays.



4. Specify a group name and description.
5. From the list, select **protocols**.
6. In list on the left, select the protocols you want included in your new Matched Group. On this screen, you can choose the settings for the group.
7. Click **Add**.
8. Click **OK**.

QoS Objects

The **Objects QoS Objects** page provides options for creating or editing QoS Objects and QoS Groups.

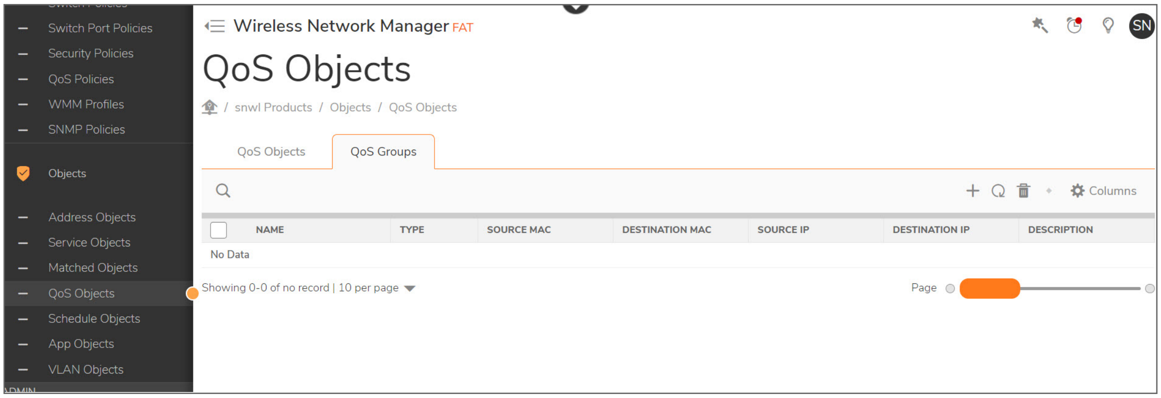


□	NAME	TYPE	SOURCE MAC	DESTINATION MAC	SOURCE IP	DESTINATION IP	DESCRIPTION
No Data							

Showing 0-0 of no record | 10 per page

QoS Group

The **QoS Group** tab displays the available QoS groups. You can also create, modify, and delete QoS groups on this tab.



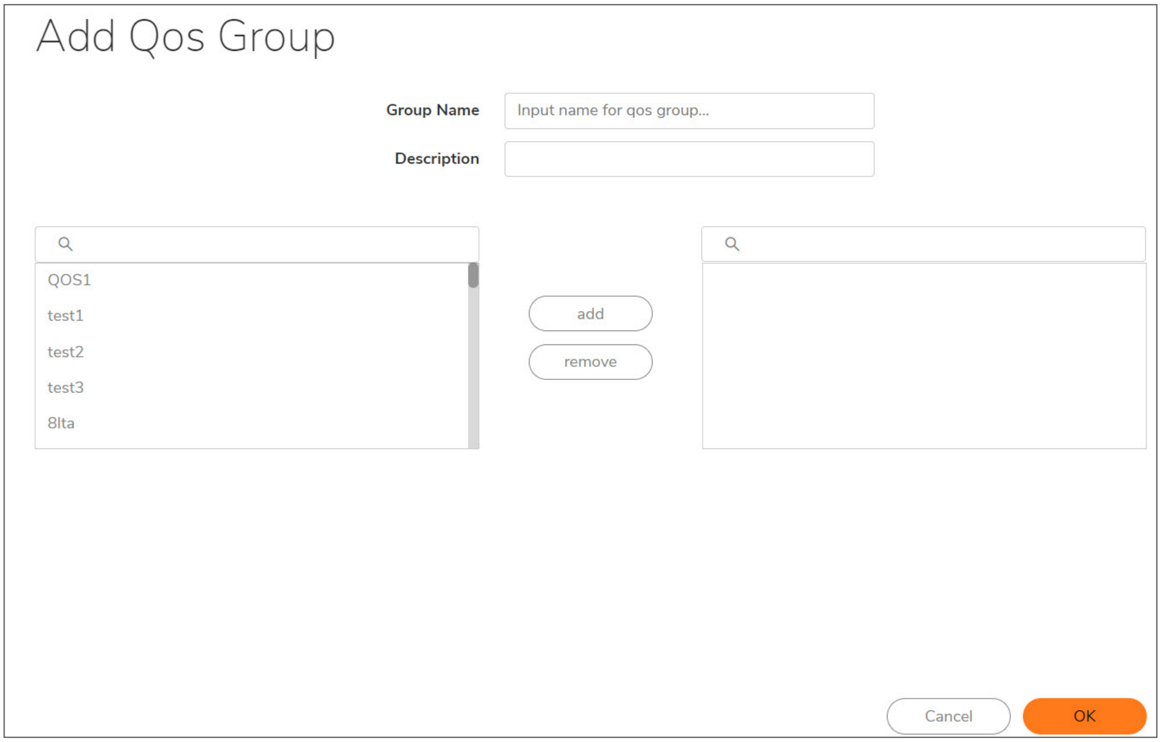
□	NAME	TYPE	SOURCE MAC	DESTINATION MAC	SOURCE IP	DESTINATION IP	DESCRIPTION
No Data							

Showing 0-0 of no record | 10 per page

To create a new QoS Group:

1. Navigate to **Objects > QoS Objects**.
2. Click the **QoS Group** tab.

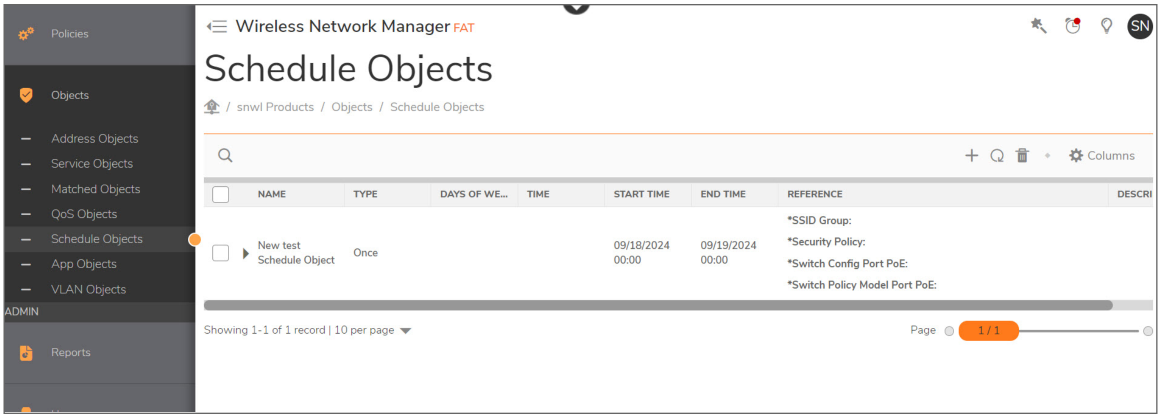
3. Click Add (**+**). The **Add QoS Group** dialog displays.



4. Specify a group name and description.
5. From the list, select **protocols**.
6. In list on the left, select the protocols you want included in your new QoS Group. On this screen, you can choose the settings for the group.
7. Click **Add**.
8. Click **OK**.

Schedule Objects

Scheduling device activation or deactivation and other processes can automate some of the administrator's tasks.



Schedule Objects

/ snwl Products / Objects / Schedule Objects

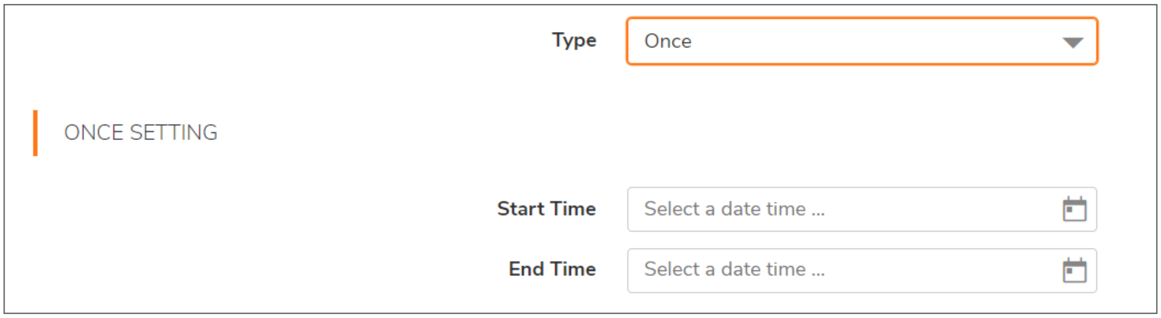
NAME	TYPE	DAYS OF WE...	TIME	START TIME	END TIME	REFERENCE	DESCRI
New test Schedule Object	Once			09/18/2024 00:00	09/19/2024 00:00	*SSID Group: *Security Policy: *Switch Config Port PoE: *Switch Policy Model Port PoE:	

Showing 1-1 of 1 record | 10 per page

Page 1 / 1

To schedule device activation or deactivation and other processes:

1. Navigate to **Objects > Schedule Objects**.
2. Click **Config/Edit** (on the schedule row). You can set a schedule for the VAP (Virtual Access Point) on the SonicWave appliance to become activated or deactivated. OR Alternatively, Click **Add +** top right to create a Schedule Object.
3. On the first **Add Schedule Object** screen, specify the **Name**, **Description**, and **Type** of your new schedule object. You can select the Type as **Once**, **Recurring**, or **Mixed**. Further options are displayed according to your selection. This feature helps Admins to define a periodic or static time schedule.
   - If you select **Once**, select the **Start Time** and **End Time** clicking on the calendar icon. Select the date from the calendar and set the time for Hours and Minutes.



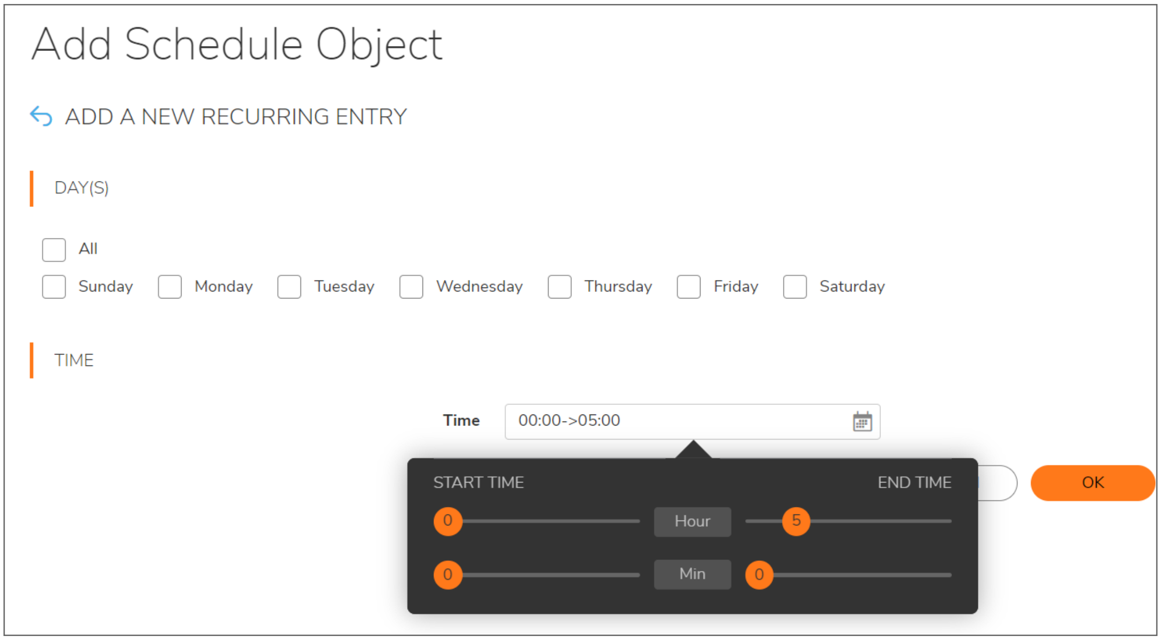
Type: Once

ONCE SETTING

Start Time: Select a date time ...

End Time: Select a date time ...

   - If you select **Recurring**, click on the **Add** icon below on the right side, and add the recurring entry. You have to specify the **Days** and **Time**.



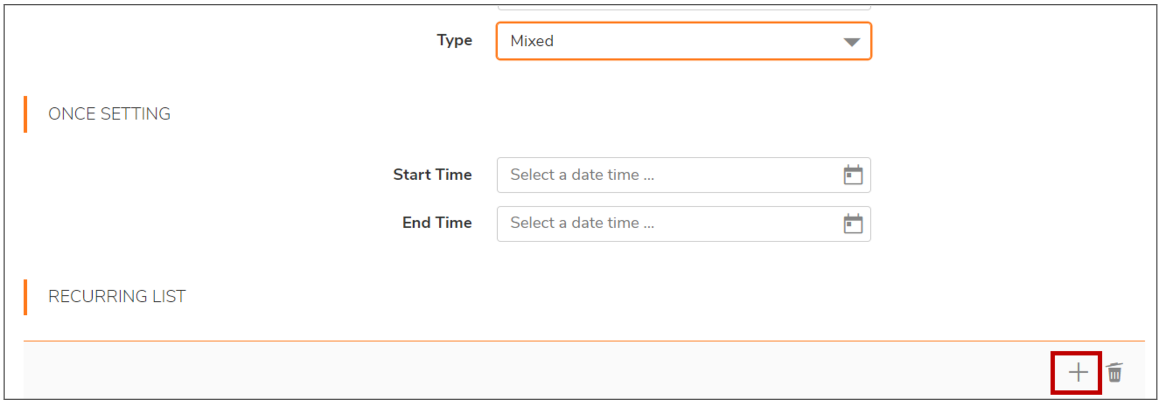
Add Schedule Object

ADD A NEW RECURRING ENTRY

Time: 00:00->05:00

DAY(S)
□ All
□ Sunday □ Monday □ Tuesday □ Wednesday □ Thursday □ Friday □ Saturday
TIME
START TIME
END TIME
0
Hour
5
0
Min
0
OK

- If you select **Mixed**, specify the **Once Setting** and **Recurring list** in the similar way.



Type: Mixed

Start Time: Select a date time ...

End Time: Select a date time ...

4. On the next **Add Schedule Object** screen, click **+Add a New Recurring Entry** to select schedule information .
5. In the **Time** section, drag the selections along the time bar to choose the start and end times.
6. Click **OK** to apply your settings
7. Click **OK** again to return to the **Schedule Objects** list.
8. Go to **Policies > SSID Settings** and select the schedule object you created.
9. Apply this SSID to the SonicWave appliance you wish to configure.

The Security Policy becomes activated or deactivated in the SonicWave appliance according to the selected schedule.

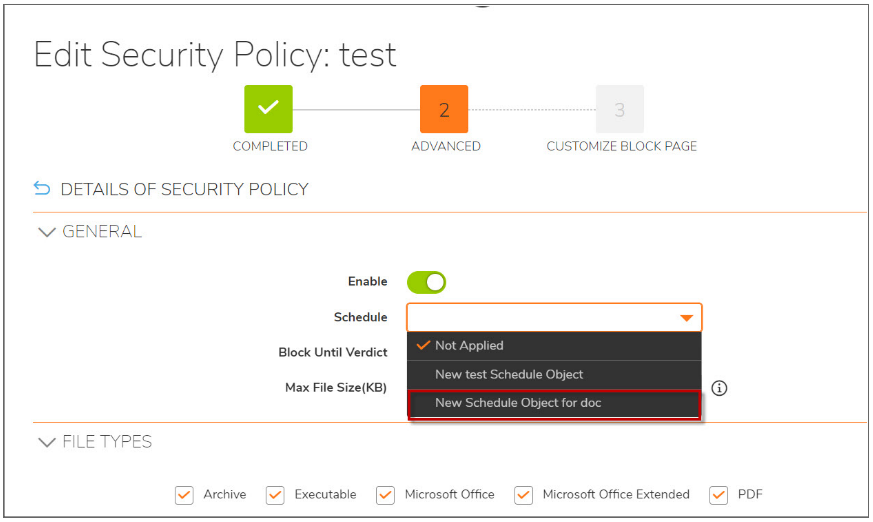
Scheduling VAP Security Policy

Scheduling VAP Security Policy activation or deactivation and other processes can automate some of the administrator’s tasks. The VAP Security Policy Schedule is a function that schedule the corresponding security policy at a specified time or periodically.

- **Security Policy**: CFS, CATP, CAV, APP Control, GeoIP_Botnet.
- **Schedule mode**: **Once**, **Recurring**, or **Mixed**.

To schedule VAP security policy activation or deactivation :

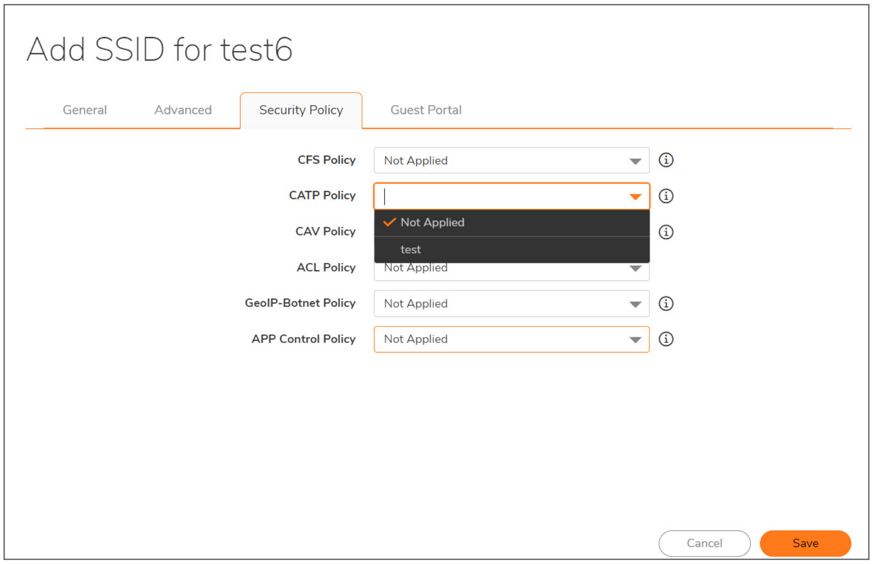
1. Navigate to **Objects > Schedule Objects**.
2. Click **Config/Edit** (on the schedule row). You can set a schedule for the VAP Security Policies on the SonicWave appliance to become activated or deactivated. Or, Click **Add +** top right to create a Schedule Object.
3. On the first **Add Schedule Object** screen, specify the **Name**, **Description**, and **Type** of your new schedule object.
4. On the next **Add Schedule Object** screen, click **+ Add a New Recurring Entry** to set the schedule information .
5. In the **Time** section, drag the selections along the time bar to choose the start and end times.
6. Click **OK** to apply your settings
7. Click **OK** again to return to the **Schedule Objects** list.
8. Go to **Security Policies**, apply the schedule object you created to the security policies [including CFS, CATP, CAV, App Control, Geoip_Botnet policy]



Edit Security Policy: test

☑ Archive ☑ Executable ☑ Microsoft Office ☑ Microsoft Office Extended ☑ PDF

9. Go to **Policies > SSID Settings** > **Security Policy** tab, click on the add icon and apply the security policies you created to SSID profile.



Add SSID for test6

CFS Policy	Not Applied
CATP Policy	✓ Not Applied test
CAV Policy	
ACL Policy	Not Applied
GeoIP-Botnet Policy	Not Applied
APP Control Policy	Not Applied

10. Apply this SSID to the SonicWave appliance if required.

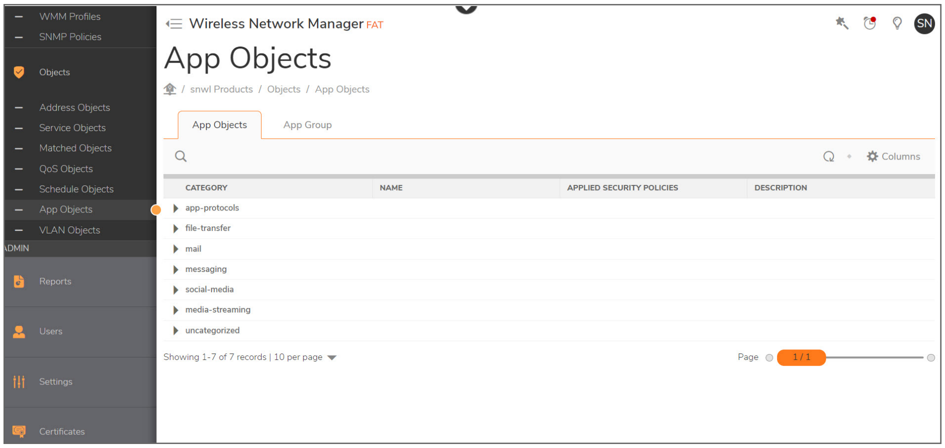
Schedule the corresponding security policy at a specified time OR periodically.

The security policy becomes activated or deactivated in the SonicWave appliance according to the selected schedule.

App Objects

The **Objects > App Objects** page provides options for creating or editing application objects.

The **App Objects** tab displays the available application objects.



App Objects

/ snwl Products / Objects / App Objects

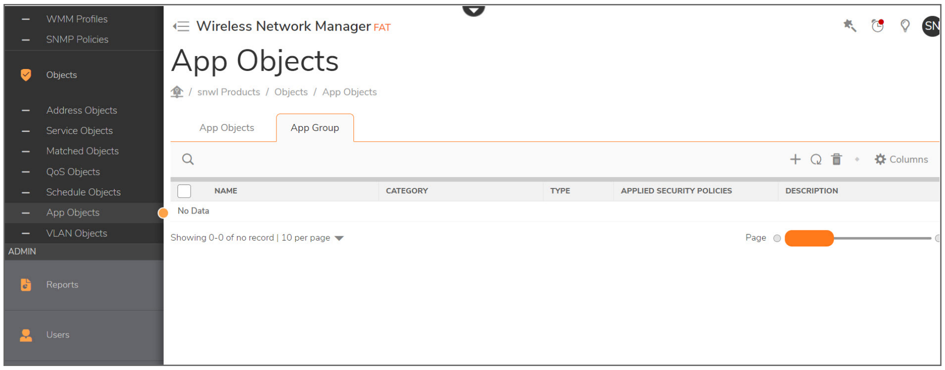
CATEGORY	NAME	APPLIED SECURITY POLICIES	DESCRIPTION
app-protocols			
file-transfer			
mail			
messaging			
social-media			
media-streaming			
uncategorized			

Showing 1-7 of 7 records | 10 per page

Page 1 / 1

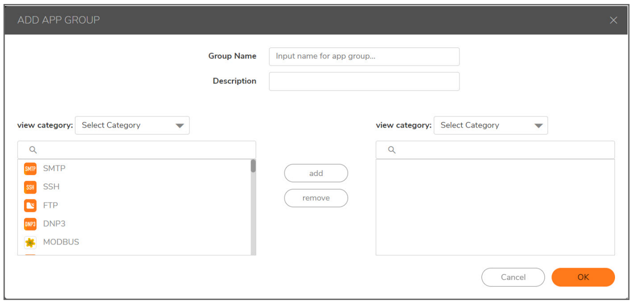
App Group

The **App Group** tab displays the available application groups. You can also create, modify, and delete on this tab.



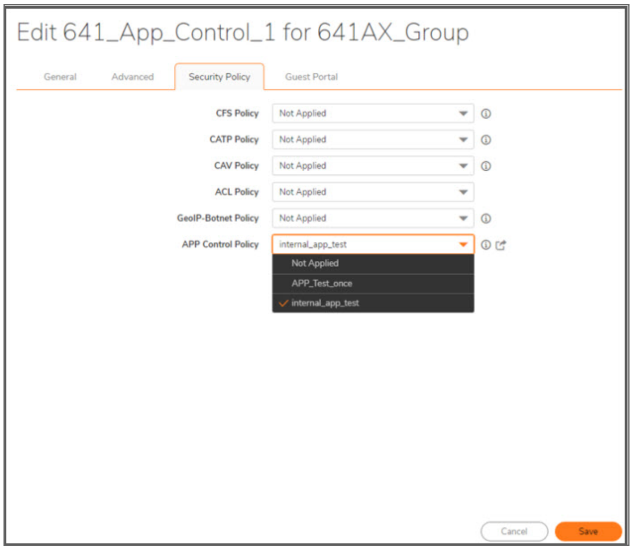
To create a new App Group:

1. Navigate to **Objects > App Objects**.
2. Click the **App Group** tab.
3. Click Add (**+**). The **Add App Group** dialog displays.



4. Specify a group **Name** and **Description**.
5. From the list, select **app-protocols**.
6. In list on the left, select the protocols you want included in your new App Group. On this screen, you can choose the settings for the group.
7. Click **Add**.
8. Click **OK**.
9. Add a schedule object in **WNM schedule objects** page.

   Go to **Policies > SSID Settings > Security Policies** tab, click on the add icon and apply the App Control policy and apply schedule.



Edit 641_App_Control_1 for 641AX_Group

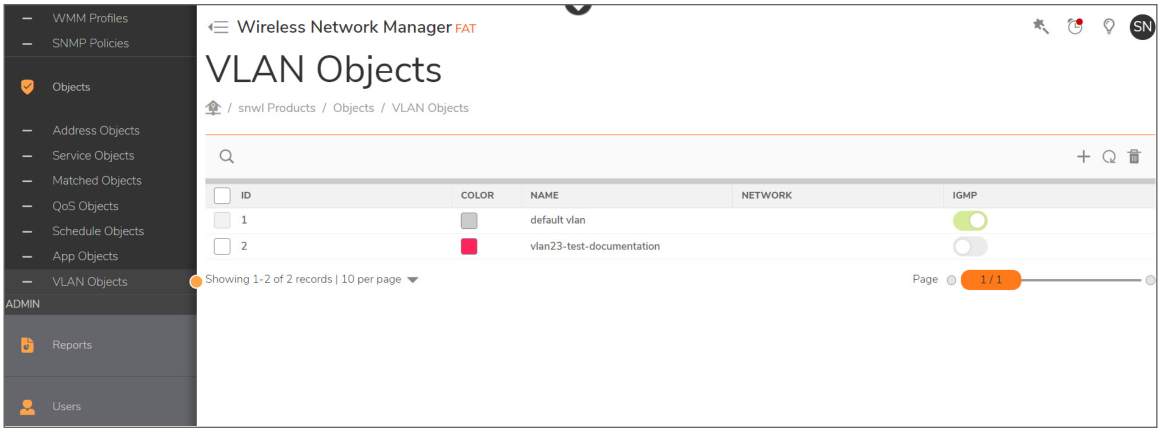
CFS Policy	Not Applied
CATP Policy	Not Applied
CAV Policy	Not Applied
ACL Policy	Not Applied
GeoIP-Botnet Policy	Not Applied
APP Control Policy	internal_app_test

VLAN Objects

The **Objects > VLAN Objects** page provides options for creating or editing VLAN objects.

The **VLAN Objects** tab displays the available VLAN objects.

You should apply the VLAN Object to the **Tagged/Untagged** list in the **Port Policy > VLAN** tab.



VLAN Objects

/ snwl Products / Objects / VLAN Objects

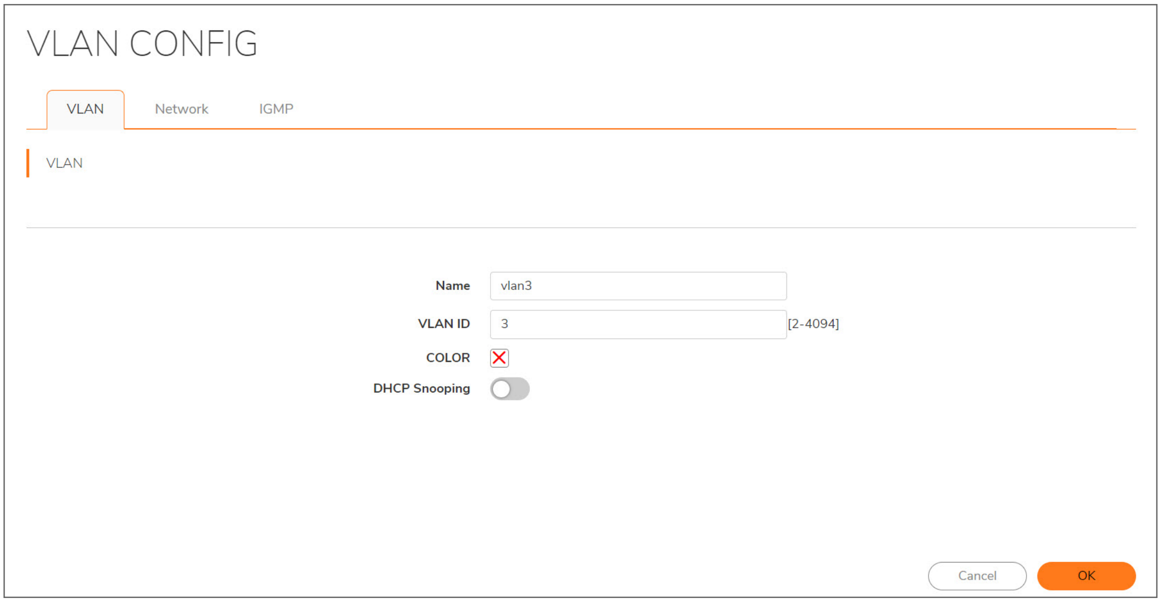
☐ ID	COLOR	NAME	NETWORK	IGMP
☐ 1	▨	default vlan		●
☐ 2	🟥	vlan23-test-documentation		○

Showing 1-2 of 2 records | 10 per page

Page 1 / 1

To create a new VLAN:

1. Navigate to **Objects > VLAN Objects**.
2. Click Add (**+**). The **VLAN Config** page displays.



VLAN CONFIG

Name: vlan3

VLAN ID: 3 [2-4094]

COLOR: ☒

DHCP Snooping: ○

3. Specify a group **Name** and **VLAN ID**.
4. Select a color.
5. Specify the DHCP Snooping status.
6. Select the **Network** tab and specify the following details:
   - Enable/Disable IPV4 Network
   - IP Address
   - Subnet Mask
7. Select the IGMP tab and specify the following details:
   - VLAN ID (the number range is from 1 to 4094)
   - Enable/Disable
   - Enable/Disable Fast Leave
   - Version of IGMP
   - Enable/Disable Quierier Interval
   - Interval (The range is 60-600)
   - Max Response Interval (The range is 0-25)
   - Startup Query Counter (The range is 2-5)
   - Startup Query Interval (The range is 15-150)

  - Static Ports (The range is 1-52)
  - Forbidden Ports (The range is 1-52)

8. Click **OK** to save the changes.

7

Admin

The Admin section helps to manage the reports, users, settings, and certificates.

Topics:

- Reports
- Users
- Settings
- Certificates

Reports

The administrator can generate reports by navigating to the **Admin > Reports** section. Reports can be formatted and delivered as PDF documents.

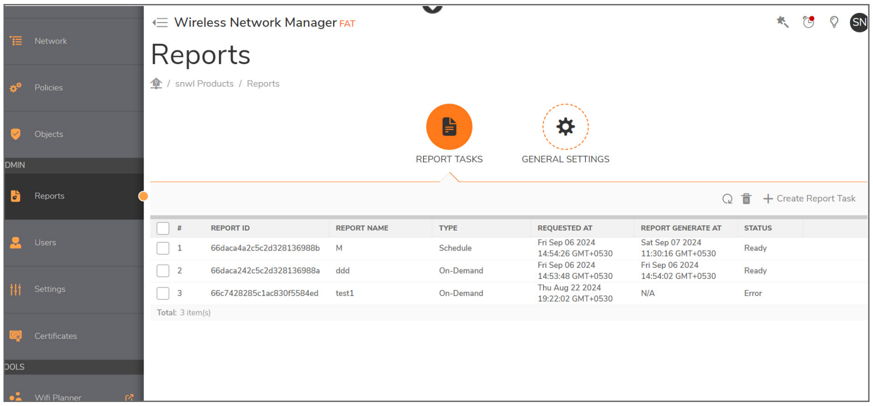
Topics:

- Generating Report Tasks
- General Settings

Generating Report Tasks

To generate a report:

1. Navigate to **Admin > Reports > REPORT TASKS.**



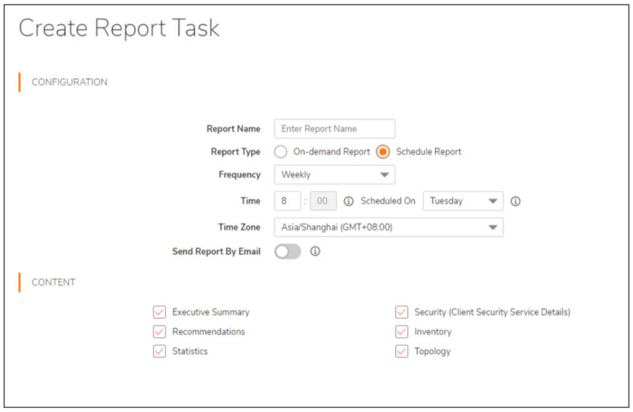
Reports

/ snwl Products / Reports

□	#	REPORT ID	REPORT NAME	TYPE	REQUESTED AT	REPORT GENERATE AT	STATUS
□	1	66daca4a2c5c2d328136988b	M	Schedule	Fri Sep 06 2024 14:54:26 GMT+0530	Sat Sep 07 2024 11:30:16 GMT+0530	Ready
□	2	66daca242c5c2d328136988a	ddd	On-Demand	Fri Sep 06 2024 14:53:48 GMT+0530	Fri Sep 06 2024 14:54:02 GMT+0530	Ready
□	3	66c7428285c1ac830f5584ed	test1	On-Demand	Thu Aug 22 2024 19:22:02 GMT+0530	N/A	Error

Total: 3 item(s)

2. Click the icon **+ Create Report Task.**
3. Enter the **Report Name.**
4. Choose the Report Type as
   - **On-demand Report** - When selected this option, you need to choose the options from the Interval as last 24 hours, 7 days, 30 days.
   - **Scheduled Report** - When selected this option, you can set a time for the reports to be generated. You can have reported sent via email in addition to being able to download them from Wireless Network Manager.



Create Report Task

CONFIGURATION

Report Name: Enter Report Name

Report Type: ○ On-demand Report ● Schedule Report

Frequency: Weekly

Time: 8 : 00 Scheduled On Tuesday

Time Zone: Asia/Shanghai (GMT+08:00)

Send Report By Email: ○

CONTENT

☑ Executive Summary
☑ Recommendations
☑ Statistics
☑ Security (Client Security Service Details)
☑ Inventory
☑ Topology

Choose the **Frequency**.Frequency can be **Daily**, **Weekly**, and **Monthly**.

- If you select **Daily**, select the **Time** and **Time Zone** options.
- If you select **Weekly**, select the **Time**, **Day,** and **Time Zone** options.

- If you select **Monthly**, select the **Time**, **Schedule on** (the dates of the month), and **Time Zone** options. The report will be generated at the time and day of a month set by user based on that selected time zone.

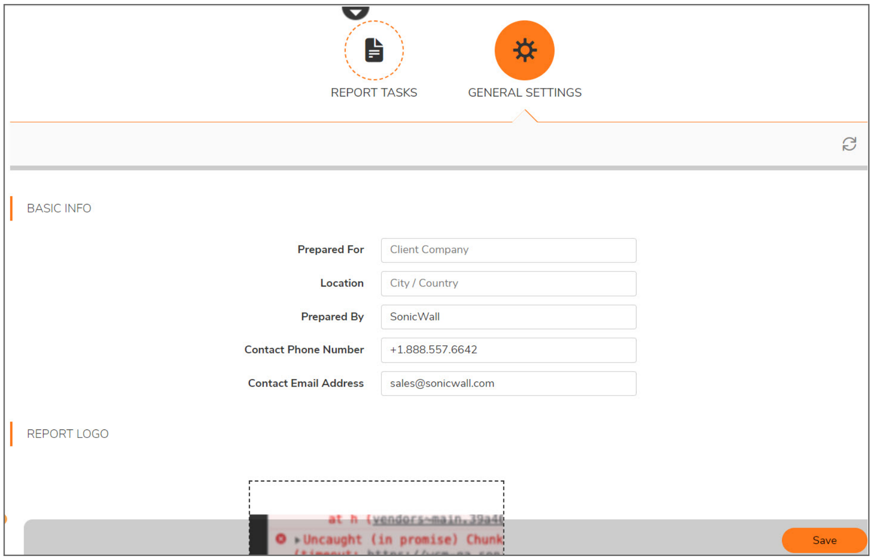
5. Click the toggle to enable or disable to **Send Report By Email** to activate sending the report by email.
6. In the **BCC To Email address** field, enter the email address to which you want the reports to be sent.
7. To send the report to additional email addresses:
    - Click the plus sign **(+) next to Add Email Address**.
    - Enter the email address to which you want the reports to be sent.

      Repeat these steps to send the report to additional email addresses.

      Click the **X** next to an email address to remove it from the list.
8. From the **Content** section, select the information to be included in the reports to be generated. Each report can be configured differently by making different selections on this screen.
9. Click **OK**.

General Settings

You can configure the WNM general settings and logo.



Prepared For: Client Company

Location: City / Country

Prepared By: SonicWall

Contact Phone Number: +1.888.557.6642

Contact Email Address: sales@sonicwall.com

```
at h (vendors~main.39a4c
▸Uncaught (in promise) Chunk
```

To configure the settings:

1. Navigate to **Admin > Reports > GENERAL SETTINGS**.
2. Fill in the fields on the screen for:
    - **Prepared for**
    - **Location**
    - **Prepared By**

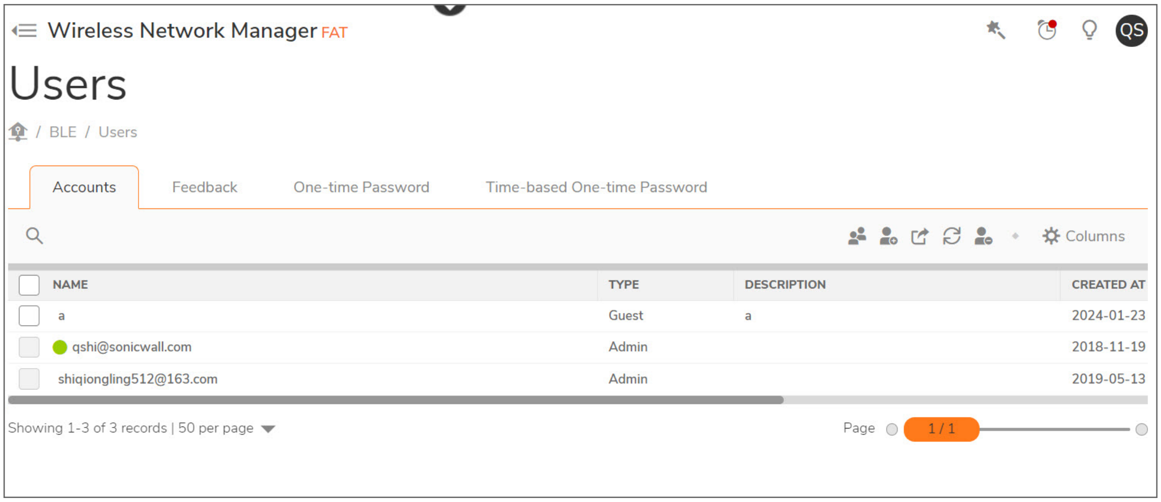
- **Contact Phone Number**
- **Contact Email Address**

3. Upload a logo to be displayed in the PDF report.
4. Click **Save** icon on the top right or click **Save**.

Users

The **Users** page displays a list of all of the current users. There are columns for

- **Name**
- **Type**
- **Description**
- **Created at**
- **Expire Time**
- **Quota**



NAME	TYPE	DESCRIPTION	CREATED AT
a	Guest	a	2024-01-23
qshi@sonicwall.com	Admin		2018-11-19
shiqiongling512@163.com	Admin		2019-05-13

Showing 1-3 of 3 records | 50 per page

You can **Edit** or **Delete** the user from the icons on the right end of the row.

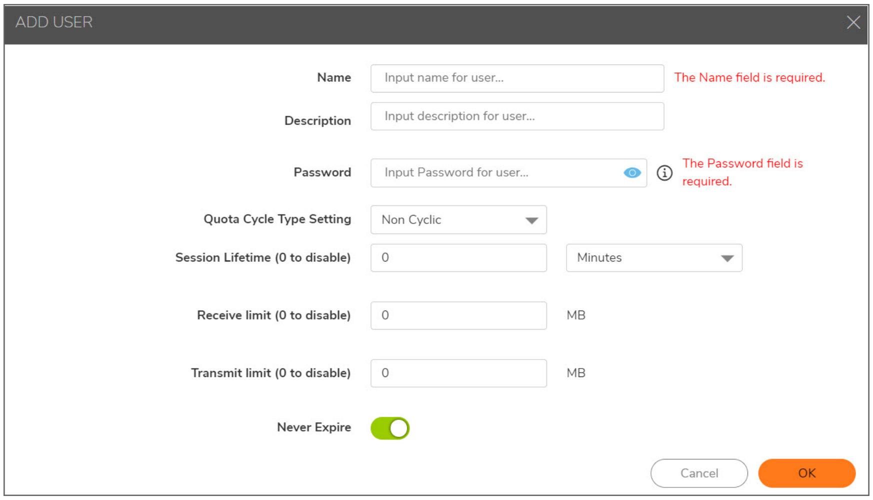
Configuring User Quota Control

The user quota control feature provides quota control based on the user's account. The quota can be specified as a session lifetime, or a transmit, or receive traffic limit. With a cyclic quota, a user can not access the Internet upon meeting the account quota until the next cycle (day, week, or month) begins. If the quota cycle is Non Cyclic, the user is unable to access the Internet upon meeting the quota.

To configure the quota for the user:

1. Navigate to **Admin > Users**. Select Accounts.

2. Click add icon on the right view of the screen. The **Add User** page is displayed.



ADD USER

Name: Input name for user... The Name field is required.

Description: Input description for user...

Password: Input Password for user... The Password field is required.

Quota Cycle Type Setting: Non Cyclic

Session Lifetime (0 to disable): 0 Minutes

Receive limit (0 to disable): 0 MB

Transmit limit (0 to disable): 0 MB

Never Expire: ●

3. Enter the details of the user:

- **Name** - Enter the name of the user.
- **Description** - Enter a description (not mandatory)
- **Password** - Set a password.
- **Quota Cycle Type Setting** - From the Quota cycle type setting list, select:
  - Non Cyclic (default)
  - Per Day
  - Per Week
  - Per Month
- **Session Lifetime (0 to disable)** - Specify the duration for how long a guest login session remains active after it has been activated. By default, activation occurs the first time a guest user logs into an account.
- **Receive Limit (0 to disable)** - Enter the amount (in MB) the amount of data the user can receive. The range is from 0 (no data can be received) to 9999 MB to Unlimited (default). If the set value is zero, the limit is disabled and it works as unlimited.
- **Transmit Limit (0 to disable)** - Enter the amount (in MB) of data the user can send. The range is from 0 (no data can be sent) to 9999 MB to Unlimited (default). If the set value is zero, the limit is disabled and it works as unlimited.
- **Never Expire** - Toggle on or off to set to never expire.
- Click **OK**.

Additionally, you can also generate multiple users clicking the **Generate Users** button.

Settings

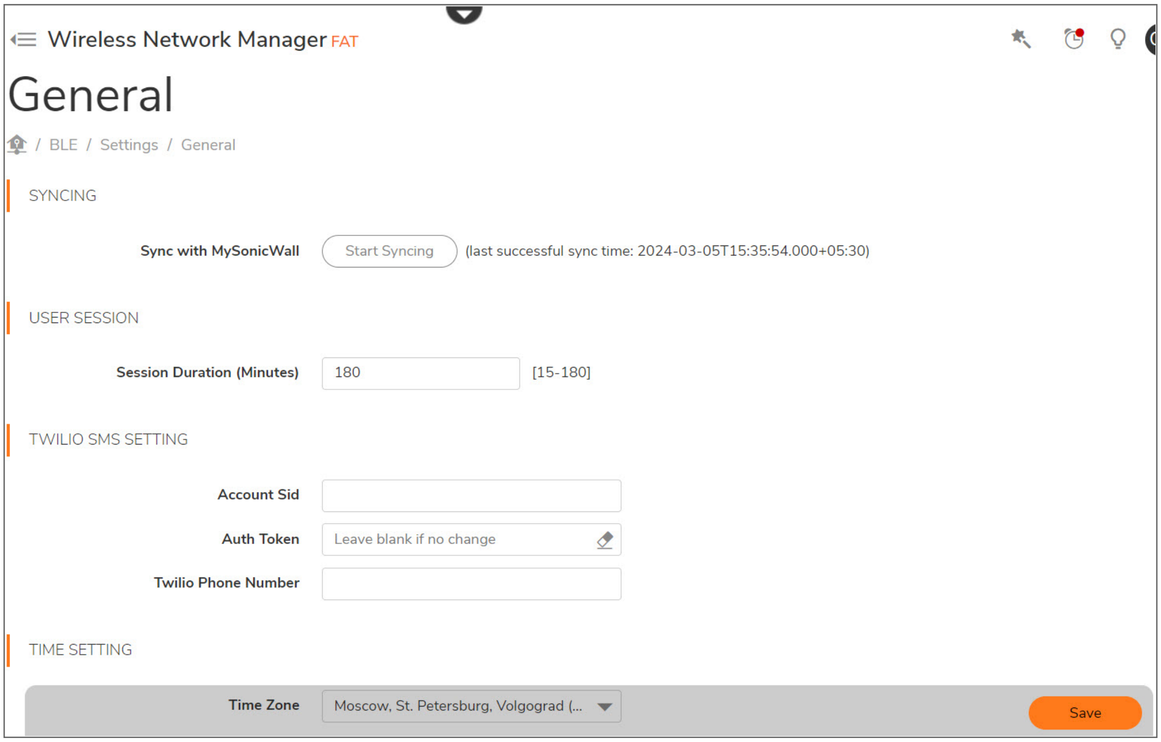
The **Settings** section provides an option for upgrading SonicWave access point firmware and syncing with MySonicWall. This section also provides an option for upgrading the Switch firmware.

Topics:

- General
- Firmware
- Notification Center

General

On the **General** page, administrators can fill in **Syncing** information.



Sync with MySonicWall (last successful sync time: 2024-03-05T15:35:54.000+05:30)

Session Duration (Minutes): 180 [15-180]

Account Sid:

Auth Token: Leave blank if no change

Twilio Phone Number:

Time Zone: Moscow, St. Petersburg, Volgograd (...

Wireless Network Manager allows the users to set the minimum and maximum session timeout. The session duration options are for the idle sessions, after which the user has to re-authenticate or provide the credentials again to log in. Session duration can be anywhere between 15 to 180.

The **Twilio SMS Configuration** settings helps the user to receive SMS notifications on the configured mobile number. For more information, refer to Configuring Twilio Billing for SMS.

The **Syncing** section provides a **Start Syncing** button that initiates syncing with MySonicWall. You might need to do this if you have been making changes to your hierarchy or devices.

Client Timezone

Administrators can configure the time zone for their connected devices. When the administrator first logs in, the default time zone is set based on the information in their MySonicWall account. In Wireless Network Manager 4.5.0, administrators can set the time based on their needs.

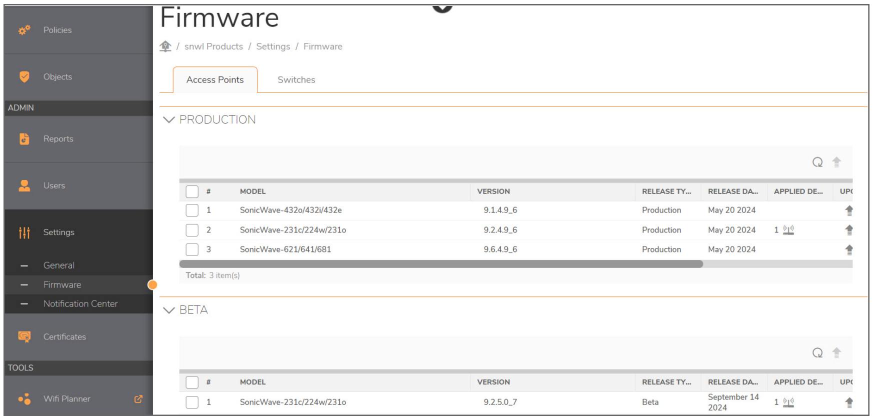
To set the timezone:

1. Navigate to the **Settings > General** page.
2. In the **Time Setting** section, select the time zone you want from the **Time Zone** list.
3. Click **Save** to save the changed settings.

After setting the time zone, when the administrator exports the log file or receives any notification emails, the time will be displayed according to their time zone setting.

Firmware

Administrators can selectively upgrade specific devices in order to install firmware upgrades or patches within their environment.



Firmware

/ snwl Products / Settings / Firmware

PRODUCTION

□	#	MODEL	VERSION	RELEASE TY...	RELEASE DA...	APPLIED DE...	UP(
□	1	SonicWave-432o/432i/432e	9.1.4.9_6	Production	May 20 2024		⬆
□	2	SonicWave-231c/224w/231o	9.2.4.9_6	Production	May 20 2024	1	⬆
□	3	SonicWave-621/641/681	9.6.4.9_6	Production	May 20 2024		⬆

Total: 3 item(s)

BETA

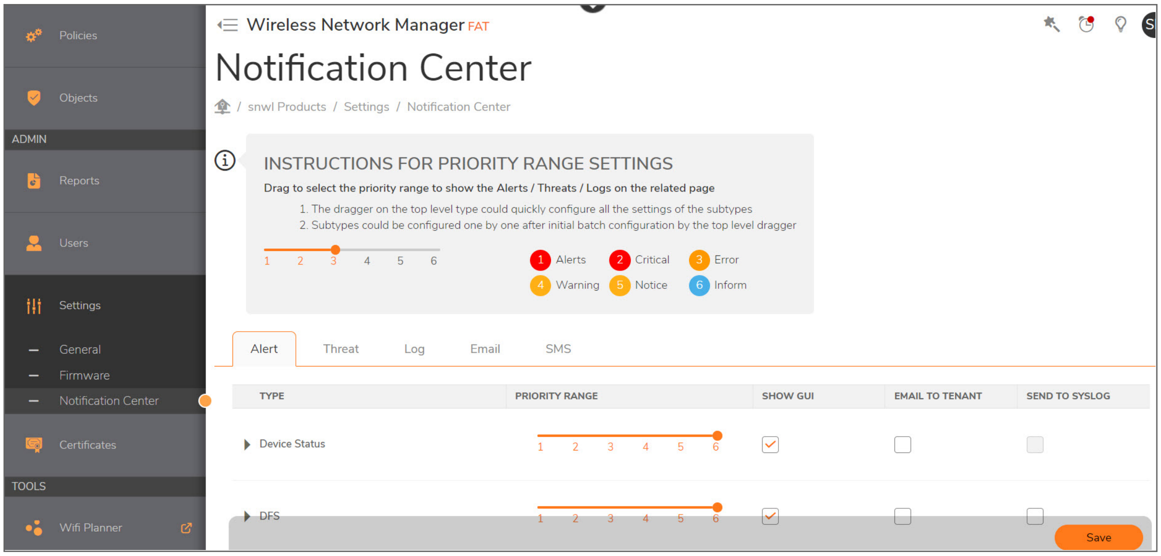
□	#	MODEL	VERSION	RELEASE TY...	RELEASE DA...	APPLIED DE...	UP(
□	1	SonicWave-231c/224w/231o	9.2.5.0_7	Beta	September 14 2024	1	⬆

To update the firmware:

1. Navigate to the **Settings > Firmware** page.
2. In the **Upgrade** column, select the icon to upgrade the device.
3. When the **Upgrade command sent to online access points message** displays, click **OK**.

Notification Center

The **Notification Center** page provides Wireless Network Manager administrators with options for filtering the information they receive.



Notification Center

snwl Products / Settings / Notification Center

INSTRUCTIONS FOR PRIORITY RANGE SETTINGS

Drag to select the priority range to show the Alerts / Threats / Logs on the related page

1. The dragger on the top level type could quickly configure all the settings of the subtypes
2. Subtypes could be configured one by one after initial batch configuration by the top level dragger

TYPE	PRIORITY RANGE	SHOW GUI	EMAIL TO TENANT	SEND TO SYSLOG
Device Status	1 2 3 4 5 6	☑	□	□
DFS	1 2 3 4 5 6	☑	□	□

Clicking on these options display pages where you can make selections concerning notifications:

- **Alert**
- **Threat**
- **Log**
- **Email**
- **SMS**

Within these **Types** are several subtypes that can be brought up by expanding the main type. These pages have an easy-to-use interface for setting priorities for each of the related screens. The dragger makes it easy to select the desired priority for each event, since they can be set both as a batch and individually. Instructions for the use of this tool are on the screen.

Alert

- The **Alert** page has a table to select each **Type** of alert put out by Wireless Network Manager:
  - **Priority Range**
  - **Show GUI**
  - **Email to Tenant**
  - **Send to Syslog**

  The **Types** are set in groups:

  - **System**
  - **Network**

- **Security Service** (which includes **CFS, Capture ATP, Cloud AV, GeoIP, Botnet, App Control.**)
- **Device Status**
- **DFS**
- **Switch** (which includes **CLI, System, LBD, RESTful, POE.**)

Threat

The **Threat** page has types for WIDP (Wireless Intrusion Detection & Prevention):

- **WIDP**
- **Security Service**

Log

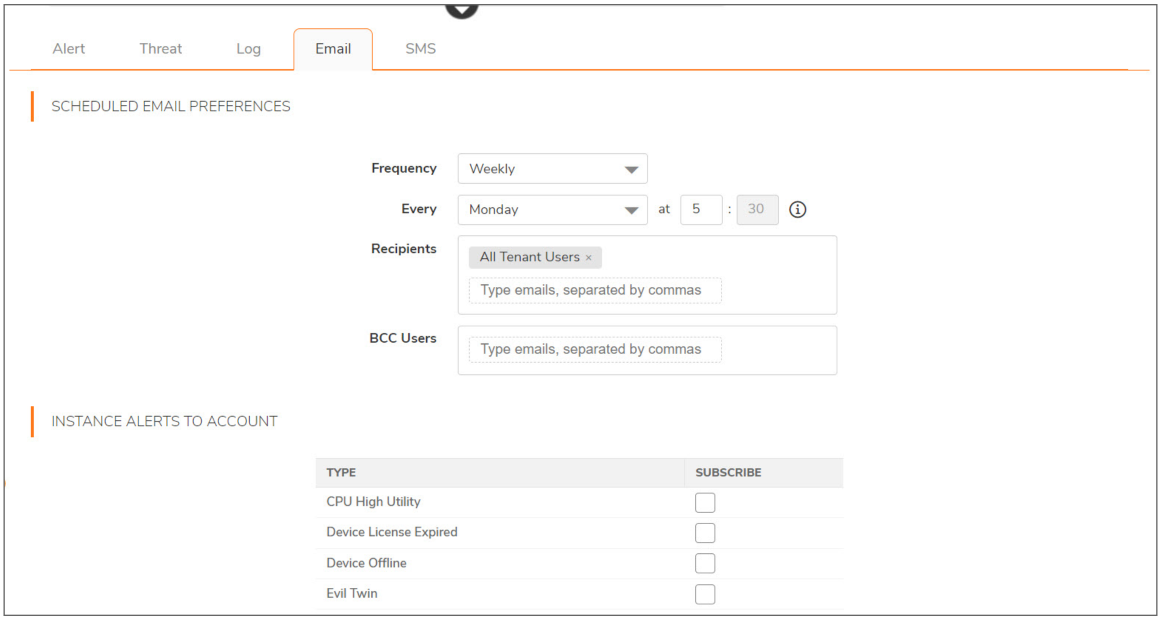
The **Log** page shows several choices for the **Type** of log notifications available.

The types of log notifications are:

- **System**
- **802.11**
- **802.1X**
- **WPA**
- **DFS**
- **User Authentication**
- **RRM (Radio Resource Management)**
- **Network**
- **BLE (Bluetooth Low Energy)**
- **Mesh**
- **Cloud Management**
- **Audit**
- **Switch**

Email

The **Email** page displays the frequency of the notifications and a list of the email addresses where copies should be sent.



SCHEDULED EMAIL PREFERENCES

Frequency: Weekly

Every: Monday at 5 : 30

Recipients: All Tenant Users ×
Type emails, separated by commas

BCC Users: Type emails, separated by commas

INSTANCE ALERTS TO ACCOUNT

TYPE	SUBSCRIBE
CPU High Utility	□
Device License Expired	□
Device Offline	□
Evil Twin	□

The **Scheduled Email Preferences** include the following options:

- Frequency
- Week Day and Time
- Recipients (You can select **All Tenant Users** or individual users)
- BCC Users

ⓘ **NOTE:** When you select the Inherit Email Addresses from Schedule option, the Recipients and BCC Users options are disabled automatically.

The **Instance Alerts to Account** include the following options:

- Type to Subscribe
- Device Offline Alert Threshold in minutes
- Inherit Email Addresses from Schedule
- Recipients (You can select **All Tenant Users** or individual users)
- BCC Users

SMS Event Notifications

You can receive notifications via SMS when certain events occur.

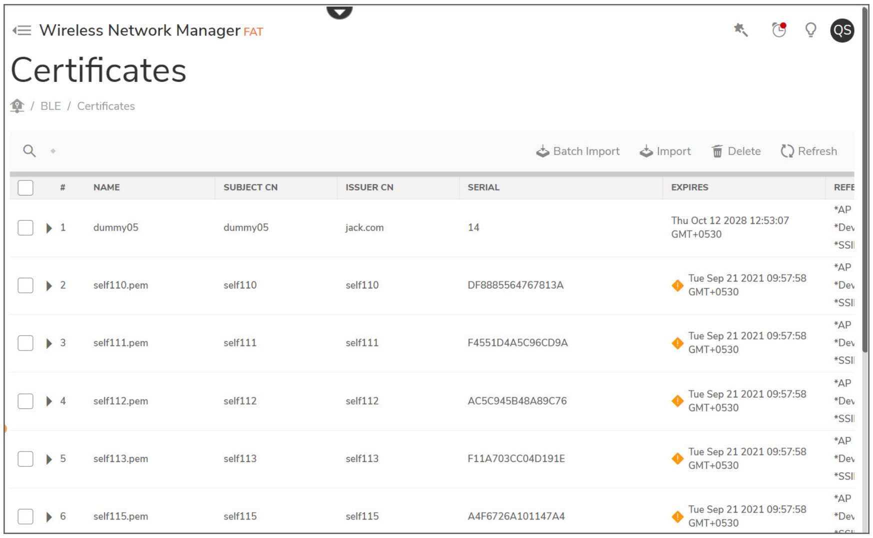
To activate SMS notifications:

1. If you have done so already, set up your Configuring Twilio Billing for SMS.
2. Navigate to **Settings > Notifications Center**.

3. In the **SMS Settings** section, enter the telephone number to which the SMS notifications should be sent.
4. In the **Events** section, select the events for which you want SMS notifications. The available events include:
    - **Cpu High Utility**
    - **Memory High Utility**
    - **Radar Detection**
    - **Firmware Upgrade**
    - **Device On/Offline**
    - **Device License Expired**
    - **Evil Twin**
5. Click **Save**.

Certificates

Click on **Certificates** in the **Admin** section at the bottom of the navigation pane, to access the certificates.



□	#	NAME	SUBJECT CN	ISSUER CN	SERIAL	EXPIRES	REFE
□	1	dummy05	dummy05	jack.com	14	Thu Oct 12 2028 12:53:07 GMT+0530	*AP *Dev *SSI
□	2	self110.pem	self110	self110	DF8885564767813A	Tue Sep 21 2021 09:57:58 GMT+0530	*AP *Dev *SSI
□	3	self111.pem	self111	self111	F4551D4A5C96CD9A	Tue Sep 21 2021 09:57:58 GMT+0530	*AP *Dev *SSI
□	4	self112.pem	self112	self112	AC5C945B48A89C76	Tue Sep 21 2021 09:57:58 GMT+0530	*AP *Dev *SSI
□	5	self113.pem	self113	self113	F11A703CC04D191E	Tue Sep 21 2021 09:57:58 GMT+0530	*AP *Dev *SSI
□	6	self115.pem	self115	self115	A4F6726A101147A4	Tue Sep 21 2021 09:57:58 GMT+0530	*AP *Dev

You can **Batch Import**, **Import**, **Delete** certificates and **Refresh** the page.

Topics:

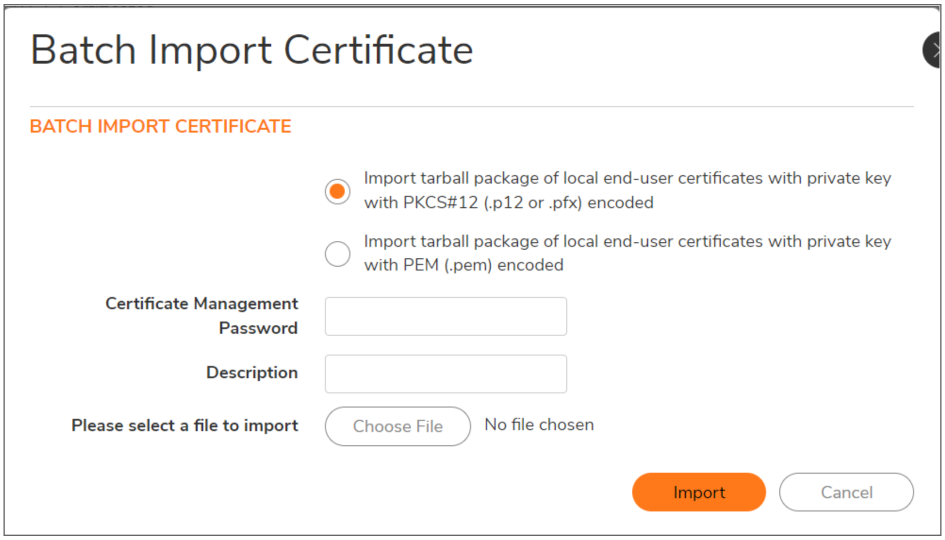
- Batch Import
- Import Certificates

Batch Import

Wireless Network Manager provides the option to batch import the certificates.

To batch import the certificates:

1. Click on **Certificates** > **Batch Import**. The **Batch Import Certificate** window is displayed.



Batch Import Certificate

BATCH IMPORT CERTIFICATE

● Import tarball package of local end-user certificates with private key with PKCS#12 (.p12 or .pfx) encoded

○ Import tarball package of local end-user certificates with private key with PEM (.pem) encoded

Certificate Management Password

Description

Please select a file to import Choose File No file chosen

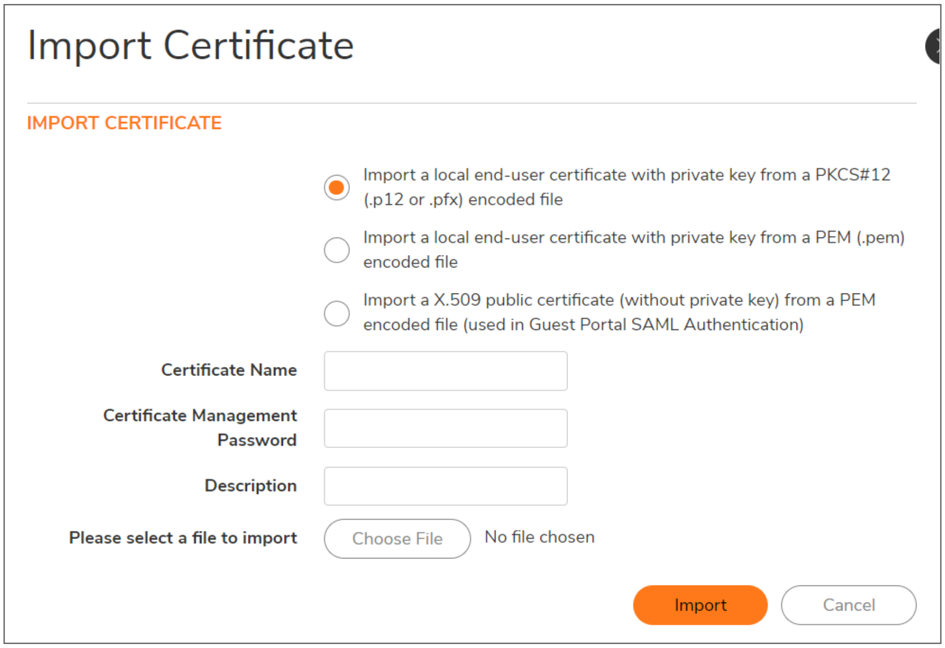
2. Select any of the following options as per your requirement:
    - Import tarball package of local end-user certificates with private key with PKCS#12 (.p12 or .pfx) encoded
    - Import tarball package of local end-user certificates with private key with PEM (.pem) encoded
3. Specify the **Certificate Management Password**.
4. Specify the **Description**.
5. Click **Choose File** and import the file from local system.
6. Click **Import**.

Import Certificates

Wireless Network Manager supports the use of the certificates for Active Directory (AD) and Guest Portal SAML authentication.

To import certificates:

1. Click on **Certificates** > **Import**. The **Import Certificate** window is displayed.



Import Certificate

IMPORT CERTIFICATE

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

○ Import a local end-user certificate with private key from a PEM (.pem) encoded file

○ Import a X.509 public certificate (without private key) from a PEM encoded file (used in Guest Portal SAML Authentication)

Certificate Name

Certificate Management Password

Description

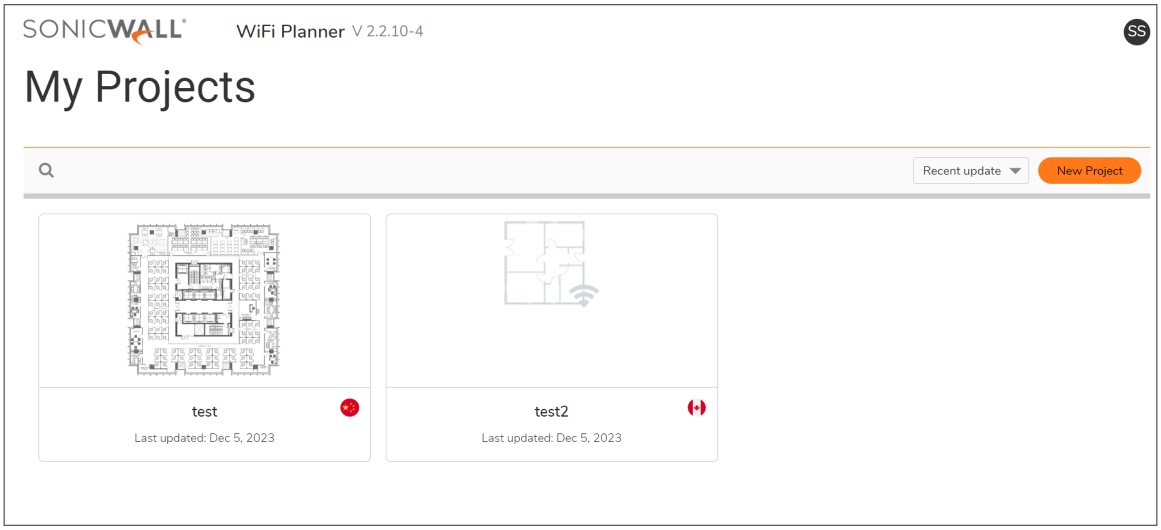
Please select a file to import | Choose File | No file chosen

2. Select any of the following options:
   - Import a local end-user certificate with private key from a PKCS#12 (.p12 or .pfx) encoded file
   - Import a local end-user certificate with private key from a PEM (.pem) encoded file
   - Import a X.509 public certificate (without private key) from a PEM encoded file (used in Guest Portal SAML Authentication)
3. Specify the **Certificate Name**.
4. Specify the **Certificate Management Password**, if you had selected the first option in Step 2.
5. Specify the **Description**.
6. Click **Choose File** and import the file from local system.
7. Click **Import**.

For more information on editing the SAML SSID, refer to Sign-on with SAML Authentication.

Using the WiFi Planner

WiFi Planner is in the **Tools** section at the bottom of the navigation pane. Click on **WiFi Planner** to access the login for the tool.



After using Wireless Network Manager to configure your network hierarchy, policies, and SSIDs as described in the *Wireless Network Manager Getting Started Guide* and the other sections in this guide, use the WiFi Planner to determine optimal SonicWave access point placement and Wi-Fi SonicWave model. WiFi Planner helps users to chose the AP model. WiFi Planner simulates deployment with SonicWall wireless products in your Wireless Network Manager zones. You can

- create and configure new projects and floor plans
- upload, scale, and manage existing floor plans
- include or exclude specific areas from Wi-Fi coverage

WiFi Planner can also be used to plan and configure access point deployment for security networks managed by a SonicWallnetwork security appliance.

For more information about the WiFi Planner, refer to the *WiFi Planner User Guide*. The *Wireless Network Manager Getting Started Guide*, the WiFi Planner *User Guide*, and other documentation are available under the product name “Secure Cloud Wireless” on the SonicWall support website: https://www.sonicwall.com/support/technical-documentation/.

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.

The Support Portal enables you to:

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

About This Document

Wireless Network Manager Administration Guide
Updated - September 2024
232-005776-00 Rev J

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