Switch

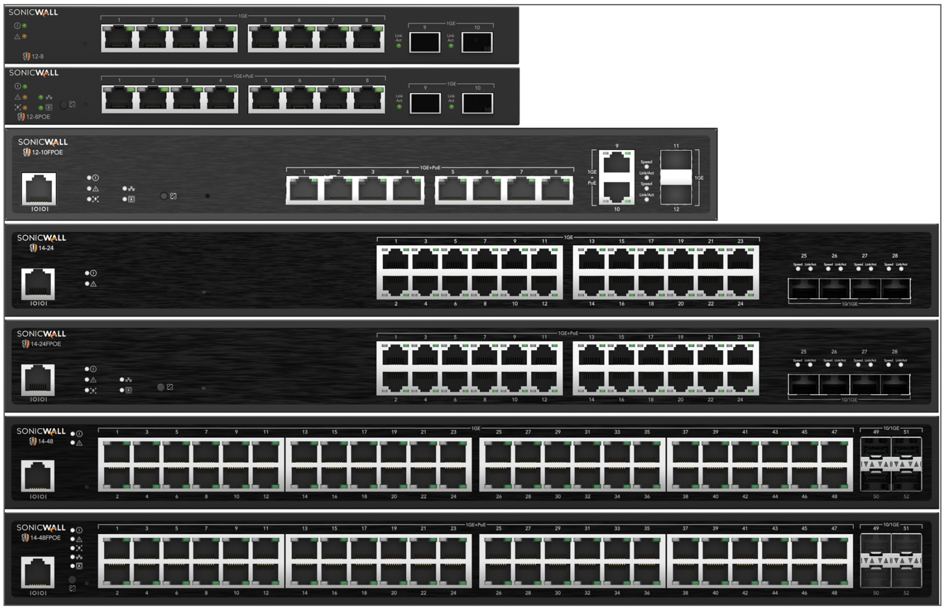
Administration Guide

SONICWALL®

Contents

1

Product Overview



The SonicWall Switches are layer 2 devices specially designed to support Access Points and IP Surveillance cameras, VOIP phones, and other PoE-Capable devices as well as other Ethernet-based networking equipment or computers. The SWS Switch provides simple, yet powerful PoE manageability with features such as: IEEE 802.3af or IEEE 802.3at/af ports, PoE port management, and loopback detection.

Package Contents

Your SWS Switch package will contain the following items:*

- SonicWall Switch
- Quick Installation Guide
- Power Adapter
- Wall Mount Kit

- Ground Screw Kit
- Power Cord
- Rack Mount Kit

*(all items must be in package to issue a refund)

Maximum data rates are based on IEEE 802.3ab standards. Actual throughput and range may vary depending on distance between devices or traffic and bandwidth load in the network. Features and specifications subject to change without notice. Trademarks and registered trademarks are the property of their respective owners. For United States of America: Copyright ©2021 SonicWall. All rights reserved. Compliant with FCC - This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his/her own expense.

Technical Specifications

	SWS12-10FPOE	SWS14-24	SWS14-24FPOE	SWS14-48	SWS14-48FPOE
1 Gb RJ45	10	24	24	48	48
1 Gb SFP	2				
1 / 10 Gb SFP+1		4	4	4	4
Fans	1	—	2	1	3
Power Supply	180 W	25 W	480 W	60 W	900 W
Power Input	100-240 VAC 50-60 Hz	100-240 VAC 50-60 Hz	100-240 VAC 50-60 Hz	100-240 VAC 50-60 Hz	100-240 VAC 50-60 Hz
PoE Ports	8	—	24	—	48
PoE Standards	802.3af/at	—	802.3af/at	—	802.3af/at
PoE Power	130 W	—	410 W	—	730 W
Maximum PoE Power per Port	30 W	—	30 W	—	30 W
Operating Temperature	0 — 40oC	0 — 40oC	0 — 40oC	0 — 40oC	0 — 40oC
Humidity (non-condensing)	5 — 95%	5 — 95%	5 — 95%	5 — 95%	5 — 95%

	SWS12-8	SWS12-8POE
1 Gb RJ45	8	8
1 Gb SFP1	2	2
Power Supply	24W external adapter	65W external adapter
Power Input	12 VDC	54 VDC
PoE Ports	—	8
PoE Standards	—	802.3af
PoE Power	—	55 W
Maximum PoE Power per Port	—	15.4 W
Operating Temperature	0 — 40oC	0 — 40oC
Humidity (non-condensing)	5 — 95%	5 — 95%

Port Functions:

8, 10, 24, or 48 10/100/1000Mbps Ports in the front panel

(Depending on model)

2 or 4 100/1000Mbps/10G SFP Ports (Depending on model) 1 RJ 45 Port

PoE Capability:

PoE Standard:

Port 1~8, 24, or 48 Support IEEE 802.3at/af

12-8POE 8 ports

12-10FPOE 8 ports

14-24FPOE 24 ports

14-48FPOE 48 ports

PoE Capable Ports:

Port 1~8, 24, 48 can output up to 30 Watts

12-8POE 8 ports

12-10FPOE 8 ports

14-24FPOE 24 ports

14-48FPOE 48 ports

LED Indicator

Device:

Power LED x1 Fault LED x1 PoE Max LED x1

LAN Mode LED x1 PoE Mode LED x1

Copper Ports:

LAN/PoE Mode LED x 1

Link/Act LED x 1

SFP Ports:

Link/Act LED x 1

Environment & Mechanical:

Temperature Range

Operating: 32 to 104°F/0 to 40°C

Storage: -40 to 158°F/-40 to 70 °C

Humidity (non-condensing): 5% - 95%

Switching:

802.3ad compatible Link Aggregation 802.1D Spanning Tree (STP)

802.1w Rapid Spanning Tree (RSTP)

802.1s Multiple Spanning Tree (MSTP)

Voice VLAN

Queue

CoS based on 802.1p priority CoS based on physical port CoS based on TOS

CoS based on DSCP BootP/DHCP Client Firmware Burn-Proof

Port-based Access Control 802.1X

802.1X Guest VLAN

Port Security

Port Isolation

Storm Control

Attack Prevention- DOS

Access Control List (ACL)

TFTP Client BootP/DHCP Client

TFTP upgrade

Command Line Interface (CLI) SNTP

RMONv1 SYSLOG

PoE Management

Power on/off per port

Power Class Configuration

Power feeding with priority

User-defined power limit

Supported SonicWall and 3rd party SFP and SFP+ Modules that can be used with SonicWall Switches

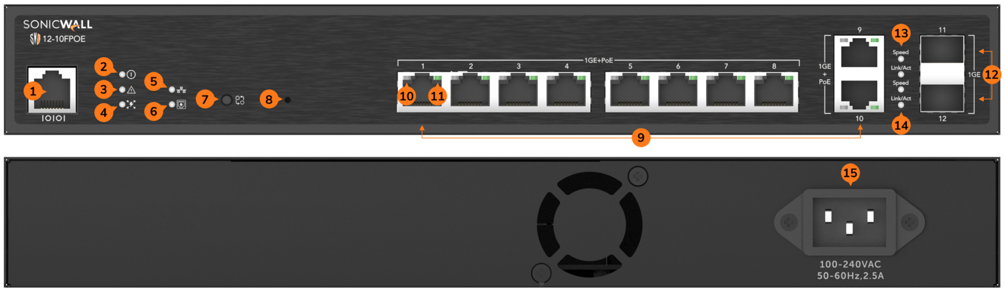
The following table provides a list of supported 3rd party SFP and SFP+ modules that can be used with SonicWall Switches.

ⓘ | **NOTE: X**=Supported in the table below.

VENDOR	MODEL	SPEED	MEDIA	MODE	SWS12-8	SWS12-8POE	SWS12-10FPOE	SWS14-24	SWS14-24FPOE	SWS14-48	SWS14-48FPOE
SonicWall	01-SSC-9785	10G	Fiber	MMF (850nm)				x	x	x	x
SonicWall	01-SSC-9786	10G	Fiber	SMF (1310nm)				x	x	x	x
SonicWall	01-SSC-9787 (1M)	10G	Copper	Twinax				x	x	x	x
SonicWall	01-SSC-9790	1G	Fiber	SMF (1310nm)	x	x	x	x	x	x	x
SonicWall	01-SSC-9789	1G	Fiber	MMF (850nm)	x	x	x	x	x	x	x
SonicWall	01-SSC-9791	10/100/1000	Copper		x	x	x	x	x	x	x
SonicWall	02-SSC-1874	10G/5G/2.5G	Copper					x	x	x	x
Finisar	FTLX8571D3BCL	10G	Fiber	MMF (850nm)				x	x	x	x

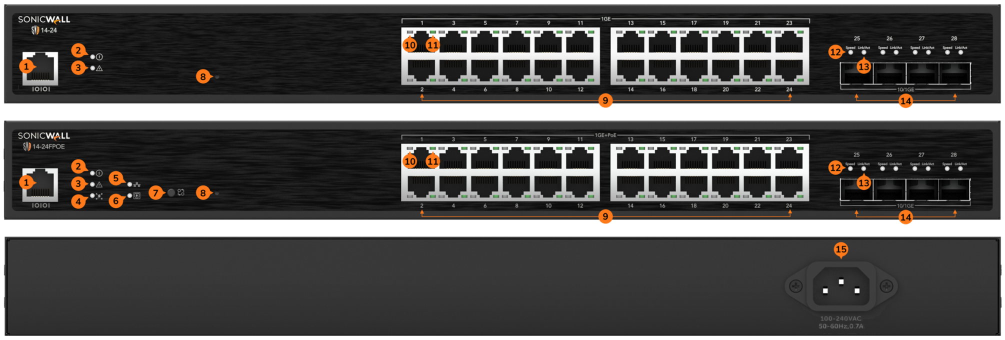
Cisco	SFP-H10GB-CU7M	10G	Copper	Twinax				x	x	x	x
Cisco	SFP-H10GB-CU3M	10G	Copper	Twinax				x	x	x	x
Finisar	FTLX8574D3BCL	10G	Fiber	MMF (850nm)				x	x	x	x
Finisar	FTLX1471D3BCL	10G	Fiber	SMF (1310nm)				x	x	x	x
EnGenius	SFP2213-10	1000			x	x	x	x	x	x	x
EnGenius	SFP2185-05	1000			x	x	x	x	x	x	x
Planet	MGB-LX (LC,10km)1000 Base-LX	1000			x	x	x	x	x	x	x
Planet	MGB-SX (LC,550m)1000 Base-SX	1000			x	x	x	x	x	x	x
Mini GBIC	SFP-4200	1000			x	x	x	x	x	x	x
Apac Opto	LM28-C3S-TC-N	1000			x	x	x	x	x	x	x
D-LInk	DEM-310GT 1000BASE-LX	1000			x	x	x	x	x	x	x
D-LInk	DEM-311GT 1000BASE-SX	1000			x	x	x	x	x	x	x
LevelOne	SFP-3841	1000			x	x	x	x	x	x	x
LevelOne	SFP-4210	1000			x	x	x	x	x	x	x
AXCEN	AXGE-5854-0511	1000			x	x	x	x	x	x	x
10Gtek	AXS85-192-M3	10G						x	x	x	x
AXCEN	AXXE-3386-0531	10G						x	x	x	x
AXCEN	AXXE-5886-05B1	10G						x	x	x	x
Huawei	SFP-10G-LR	10G						x	x	x	x
AvaGO	AFCT-701ASDZ	10G						x	x	x	x
AvaGO	AFBR-709ASMZ	10G						x	x	x	x

Physical Interface - 10 Port Switch



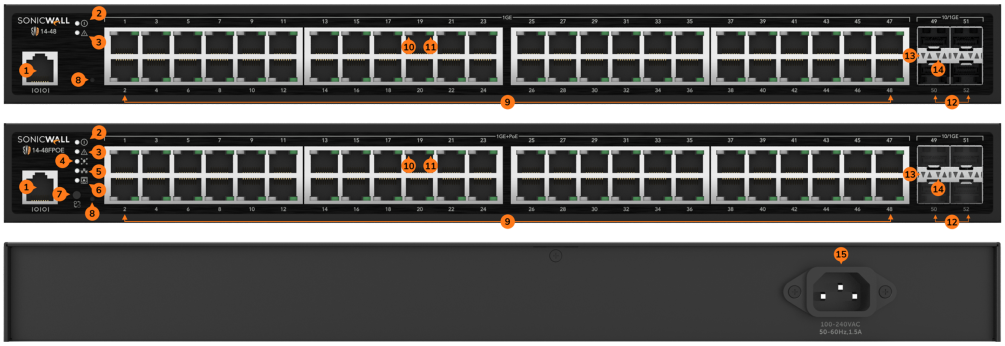
1. RJ45 Console Port
2. Power LED: Light off = Power off; Solid Light = Power On.
3. Fault LED: Light off = Normal Behavior; Solid Light = Error.
4. PoE Max LED: Light off = Additional PoE device may still be added; Solid Light = The PoE device’s output power has exceeded total PoE limit. No additional devices can be powered on via PoE.
5. LAN Mode LED: Light off = LAN mode is not activated; Solid Light = LAN mode is activated.
6. PoE Mode LED: Light off = PoE mode is not activated; Solid Light = PoE mode is activated.
7. LED Mode Selector: Press to change between LAN and PoE mode.
8. Reset Button: Press to reset the device to factory default settings.
9. RJ-45 LAN Ports: 10/100/1000 Mbps RJ-45 LAN ports.
10. LAN Mode LED (Per Copper Port): Light off = No link is established on the port; Solid Amber Light = A valid 100 Mpbs link is established on the port.
11. Link/Act LED (Per Copper Port): Light off = No link is established on the port; Solid Light = A valid link is established on the port; Blinking Light = Packet transmission on the port.
12. Speed LED (Per SFP Port). Solid Amber Light should be 10 Gbps Link, Solid Green Light should be 1 Gbps link.
13. Link/Act LED (Per SFP Port).
14. SFP Ports: Small form factor pluggable ports: 1 or 10 Gbps ports.
15. Power Connector.

Physical Interface - 24 Port Switch



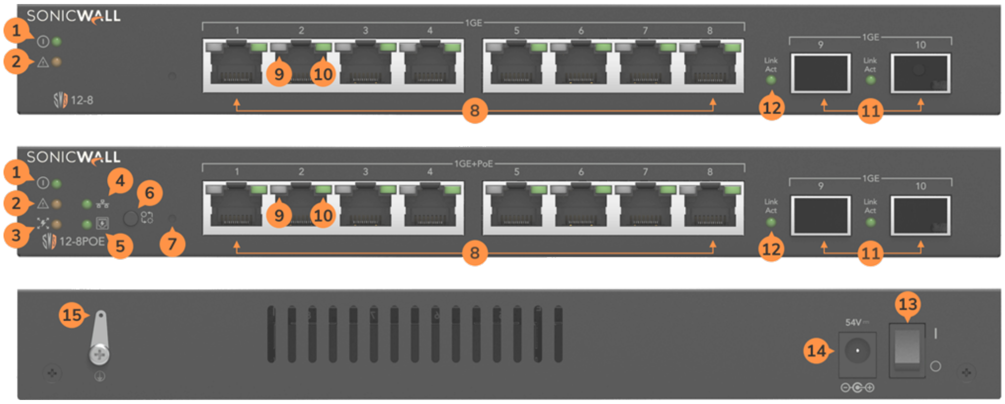
1. RJ45 Console Port
2. Power LED: Light off = Power off; Solid Light = Power On.
3. Fault LED: Light off = Normal Behavior; Solid Light = Error.
4. PoE Max LED: Light off = Additional PoE device may still be added; Solid Light = The PoE device’s output power has exceeded total PoE limit. No additional devices can be powered on via PoE.
5. LAN Mode LED: Light off = LAN mode is not activated; Solid Light = LAN mode is activated.
6. PoE Mode LED: Light off = PoE mode is not activated; Solid Light = PoE mode is activated.
7. LED Mode Selector: Press to change between LAN and PoE mode.
8. Reset Button: Press to reset the device to factory default settings.
9. RJ-45 LAN Ports: 10/100/1000 Mbps RJ-45 LAN ports.
10. LAN Mode LED (Per Copper Port): Light off = No link is established on the port; Solid Amber Light = A valid 100 Mpbs link is established on the port.
11. Link/Act LED (Per Copper Port): Light off = No link is established on the port; Solid Light = A valid link is established on the port; Blinking Light = Packet transmission on the port.
12. Speed LED (Per SFP Port). Solid Amber Light should be 10 Gbps Link, Solid Green Light should be 1 Gbps link.
13. Link/Act LED (Per SFP Port).
14. SFP Ports: Small form factor pluggable ports: 1 or 10 Gbps ports.
15. Power Connector.

Physical Interface - 48 Port Switch



1. RJ45 Console Port
2. Power LED: Light off = Power off; Solid Light = Power On.
3. Fault LED: Light off = Normal Behavior; Solid Light = Error.
4. PoE Max LED: Light off = Additional PoE device may still be added; Solid Light = The PoE device’s output power has exceeded total PoE limit. No additional devices can be powered on via PoE.
5. LAN Mode LED: Light off = LAN mode is not activated; Solid Light = LAN mode is activated.
6. PoE Mode LED: Light off = PoE mode is not activated; Solid Light = PoE mode is activated.
7. LED Mode Selector: Press to change between LAN and PoE mode.
8. Reset Button: Press to reset the device to factory default settings.
9. RJ-45 LAN Ports: 10/100/1000 Mbps RJ-45 LAN ports.
10. LAN Mode LED (Per Copper Port): Light off = No link is established on the port; Solid Amber Light = A valid 100 Mpbs link is established on the port.
11. Link/Act LED (Per Copper Port): Light off = No link is established on the port; Solid Light = A valid link is established on the port; Blinking Light = Packet transmission on the port.
12. Speed LED (Per SFP Port). Solid Amber Light should be 10 Gbps Link, Solid Green Light should be 1 Gbps link.
13. Link/Act LED (Per SFP Port).
14. SFP Ports: Small form factor pluggable ports: 1 or 10 Gbps ports.
15. Power Connector.

Physical Interface - 8 Port Switch



1. Power LED: Light off = Power off; Solid Light = Power On.
2. Fault LED: Light off = Normal Behavior; Solid Light = Error.
3. PoE Max LED: Light off = Additional PoE device may still be added; Solid Light = The PoE device’s output power has exceeded total PoE limit. No additional devices can be powered on via PoE.
4. LAN Mode LED: Light off = LAN mode is not activated; Solid Light = LAN mode is activated.
5. PoE Mode LED: Light off = PoE mode is not activated; Solid Light = PoE mode is activated.
6. LED Mode Selector: Press to change between LAN and PoE mode.
7. Reset Button: Press to reset the device to factory default settings.
8. RJ-45 LAN Ports: 1 Gbps
9. LAN Mode LED (Per Copper Port): Light off = No link is established on the port; Solid Amber Light = A valid 100 Mpbs link is established on the port; Solid Green Light = A valid 1000 Mbps link is established on the port.
10. Link/Act LED (Per Copper Port): Light off = No link is established on the port; Solid Light = A valid link is established on the port; Blinking Light = Packet transmission on the port.
11. SFP Ports: Small form factor pluggable ports: 1 Gbps ports.
12. Link/Act LED.
13. On/Off button.
14. Power Input.
15. Optional connector allows connection to ground.

Management Interface

The SWS FPoE+ Switch features an embedded Web interface for the monitoring and management of your device.

- Connecting the Switch to a Network
- Web Access

Connecting the Switch to a Network

Discovery in a Network with a DHCP Server:

Use this procedure to setup the Switch within a network that uses DHCP.

1. Connect the supplied Power Adapter (cord) to the Switch and plug the other end into an electrical outlet. Turn the power switch on the back of the device to the ON position. Verify the power LED indicator is lit on the Switch.
2. Wait for the Switch to complete booting up. It might take a minute for the Switch to completely boot up.
3. Connect one end of a Category 5/6 Ethernet cable into the Gigabit (10/100/1000) Ethernet port on the Switch front panel and the other end to the Ethernet port on the computer. Verify that the LED on the Ethernet ports of the Switch are green.
4. Once your computer is on, ensure that your TCP/IP is set to On or Enabled. Open Network Connections and then click Local Area Connection. Select Internet Protocol Version 4 (TCP/IPv4). If your computer is already on a network, ensure that you have set it to a Static IP Address on the Interface (Example: 192.168.168.10 and the Subnet mask address as 255.255.255.0).
5. Open a web browser on your computer. In the address bar of the web browser, enter https://192.168.168.169 and click Enter.
6. A login screen will appear. By default, the username is admin and the password is password. Enter the current password of the Switch and then click Login.
7. Once logged in, navigate to Network > IPv4 and check if VLAN 1 is set to obtain IP from DHCP, if not click on Action and change the Configuration to DHCP.
8. Click **Apply** to save the settings.
9. Connect the Switch to your network (DHCP enabled).
10. On the DHCP server, find and write down the IP address allocated to the device. Use this IP address to access the management interface.

Discovery on a Network without a DHCP Server:

This section describes how to set up the SWS Switch in a network without a DHCP server. If your network has no DHCP service, you must assign a static IP address to your Switch in order to log in to the web-based Switch management.

1. Connect the supplied Power Adapter (cord) to the Switch and plug the other end into an electrical outlet. Turn the Power Switch on the back of the device to the ON Position. Verify the Power LED indicator is lit on the Switch.
2. Wait for the Switch to complete booting up. It might take a minute or so for the Switch to completely boot up.
3. Connect one end of a Category 5/6 Ethernet cable into the Gigabit (10/100/1000) Ethernet port on the Switch front panel and the other end to Ethernet port on the computer. Verify that the LED on Ethernet ports of the Switch are green.
4. Once your computer is on, ensure that your TCP/IP is set to On or Enabled. Open Network Connections and then click Local Area Connection. Select Internet Protocol Version 4 (TCP/IPv4).
5. If your computer is already on a network, ensure that you have set it to a Static IP Address on the Interface (Example: 192.168.168.10 and the Subnet mask address as 255.255.255.0).
6. Open a web browser on your computer. In the address bar of the web browser, enter https://192.168.168.169 and click Enter.
7. A login screen will appear. By default, the password is password. Enter the current password of the Switch and then click Login.
   To make access to the web-based management interface more secure, it's highly recommended that you change the password to something more unique.
8. Once logged in, Navigate to **System > Network > IPV4**, click on **Action** and change the Configuration to **Static** to configure the **IP settings** of the management interface.
9. Enter the IP address, Subnet mask, and Gateway.
10. Click **Apply** to update the system.

Web Access

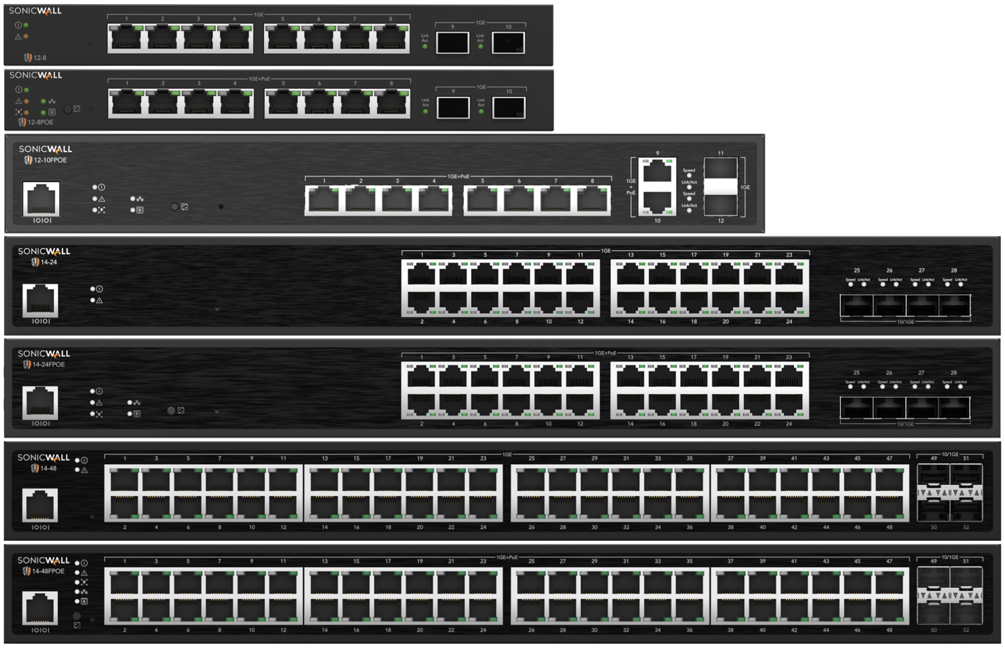
Use this procedure to access the management interface through a Web browser for device configuration.

1. Open a Web browser on your computer and enter the following address (default):
   https://192.168.168.169/
2. On the login screen, use the following information: *UserName: admin, Password: password*

To make access to the web-based management interface more secure, it's highly recommended that you change the password to something more unique.

2

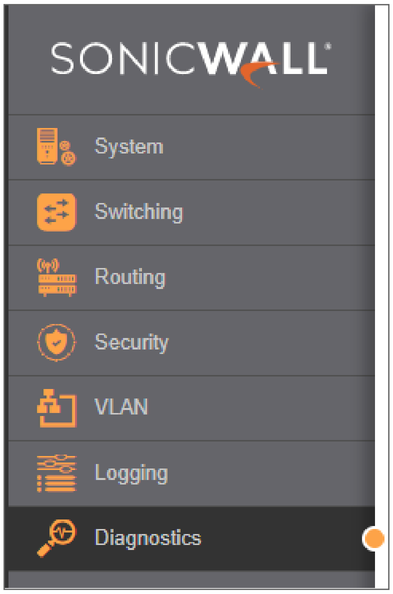
System Management



The navigation pane at the left of the Web browser interface contains a System tab that enables you to manage your SWS Switch with features under the following main menu options:

- System
- Switching
- Routing
- Security
- VLAN
- Logging
- Diagnostics

The description that follows in this chapter describes configuring and managing the system settings within the Switch.



System

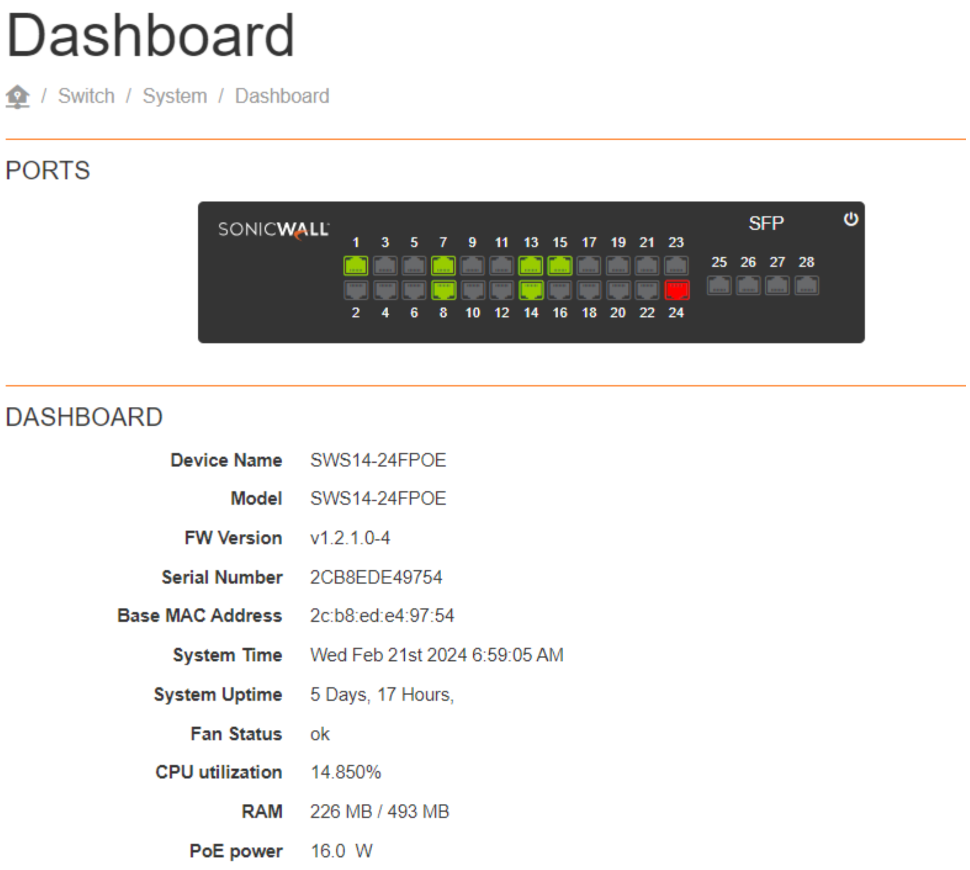
You can configure and manage the following system settings within the Switch.

- Dashboard
- Network
- Administration
- System Information
- User Management
- Simple Network Management Protocol
- Address Resolution Protocol
- Authentication
- Firmware and Settings
- DHCP Snooping
- DHCP Relay
- Time

Dashboard

The Dashboard screen contains general device information about the Switch, including the device name, Firmware version, MAC address, and System Uptime.

Device Name	Displays the device name of the Switch.
Model	Displays the model name of the Switch.
FW version	Displays the installed firmware version of the Switch.
Serial Number	Displays the serial number of the Switch.
Base MAC address	Displays the MAC address of the device.
System Time	Displays the system time in the following format: day, month, date, year, hour, minute, seconds.
System Uptime	Displays the amount of time since the most recent device reset. hours, and minutes. For example, the display will read: 3 days, 6 hours, 10 minutes.
Fan Status	Displays the fan status of the Switch.
CPU utilization	Displays the utilization of CPU in percentage.
RAM	Displays the RAM usage.
PoE power	Displays the usage of Power over Ethernet (PoE) power.



Dashboard

/ Switch / System / Dashboard

PORTS

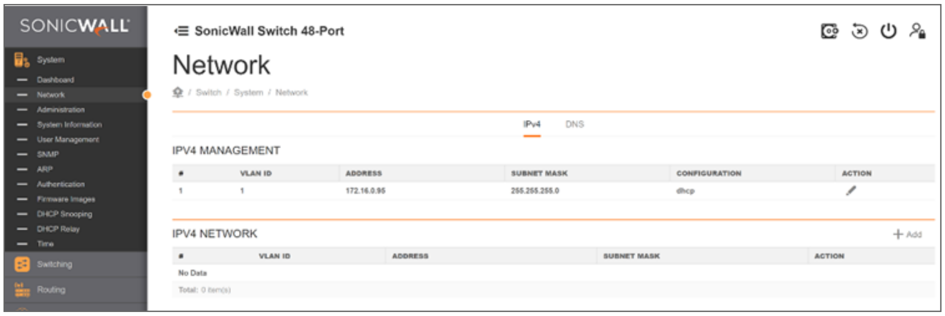
DASHBOARD

Device Name	SWS14-24FPOE
Model	SWS14-24FPOE
FW Version	v1.2.1.0-4
Serial Number	2CB8EDE49754
Base MAC Address	2c:b8:ed:e4:97:54
System Time	Wed Feb 21st 2024 6:59:05 AM
System Uptime	5 Days, 17 Hours,
Fan Status	ok
CPU utilization	14.850%
RAM	226 MB / 493 MB
PoE power	16.0 W

Network

The Network screen contains fields for assigning IP addresses. IP addresses are either defined as static or are retrieved using the Dynamic Host Configuration Protocol (DHCP). DHCP assigns dynamic IP addresses to devices on a network. DHCP ensures that network devices can have a different IP address every time the device connects to the network.

ⓘ **NOTE:** Note the following when configuring IP Addresses: If the device fails to retrieve an IP address through DHCP, the default IP address is 192.168.168.169.



SonicWall Switch 48-Port

Network

IPV4 MANAGEMENT

#	VLAN ID	ADDRESS	SUBNET MASK	CONFIGURATION	ACTION
1	1	172.16.0.95	255.255.255.0	dhcp	

IPV4 NETWORK

#	VLAN ID	ADDRESS	SUBNET MASK	ACTION
No Data				

Total: 0 item(s)

To access the page, click Network under the **System** menu.

Network has two types of configurations IPv4 management and IPv4 network.

IPv4 Network

IPv4 Network session is to configure an ip to a vlan manually which has **VLAN ID**, **IP Address** and **Subnet Mask**.

IPv4 Management

Select whether you wish to enable Static or DHCP for Auto-Configuration. Next, enter the information for the IP address, gateway, and DNS servers.

To be managed over the network, the Switch needs an IP Address to be assigned. The Network screen contains fields for assigning IP addresses. IP addresses are either defined as Static or are retrieved using the Dynamic Host Configuration Protocol (DHCP). 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.

ⓘ **IMPORTANT:** If the device fails to retrieve an IP address through DHCP, the default IP address is: 192.168.168.169 and the factory default subnet mask is: 255.255.255.0.

To access the page, click IPv4 Management under Network in the System manual highlighted below.

VLAN ID	Select the VLAN ID
Address	Enables the IP address to be configured automatically by the DHCP server. Select this option if you have a DHCP server that can assign the Switch an IP address, subnet mask, default gateway address, and a domain name server IP address automatically. Selecting this field disables Vlan ID, Address, Subnet mask, and Gateway fields.
Subnet Mask	A Bitmask that determines the extent of the subnet that the Switch is on. This should be labeled in the form: xxx.xxx.xxx.xxx, where each xxx is a number (represented in decimals) between 0 and 255. The value should be 255.0.0.0 for a Class A network, 255.255.0.0 for a Class B network, and 255.255.255.0 for a Class C network, but custom subnet masks are allowed. Enter the IP subnet mask of your Switch in dotted decimal notation. The factory default value is: 255.255.255.0.
Default Gateway	The default gateway address is displayed based on the DHCP server configured. For Static and BOOTP configuration, you can enter the IP address for the default gateway based on your need.

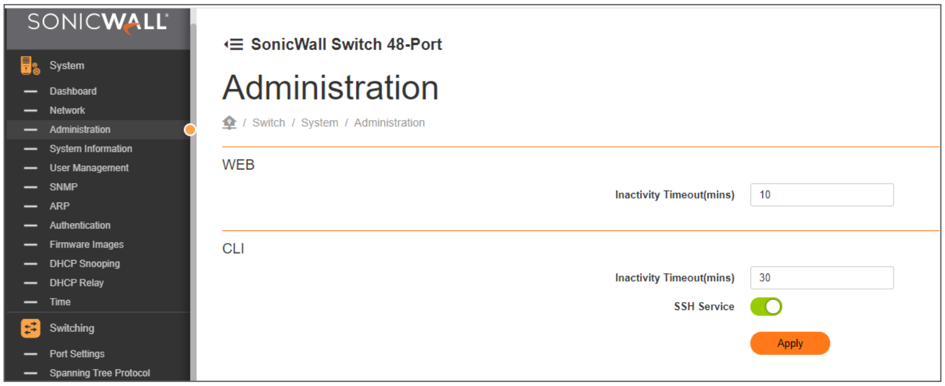
Configuration	Select the type of server configuration. • Static • BOOTP • DHCP

Click **Apply** to update the system settings.

Administration

Web Settings

The SonicWall Layer 2 PoE+ Switch provides a built-in browser interface that enables you to configure and manage the Switch via Hypertext Transfer Protocol Secure (Https) requests selectively to help prevent security breaches on the network.



SonicWall Switch 48-Port

Administration

Switch / System / Administration

WEB

Inactivity Timeout(mins) 10

CLI

Inactivity Timeout(mins) 30

SSH Service ●

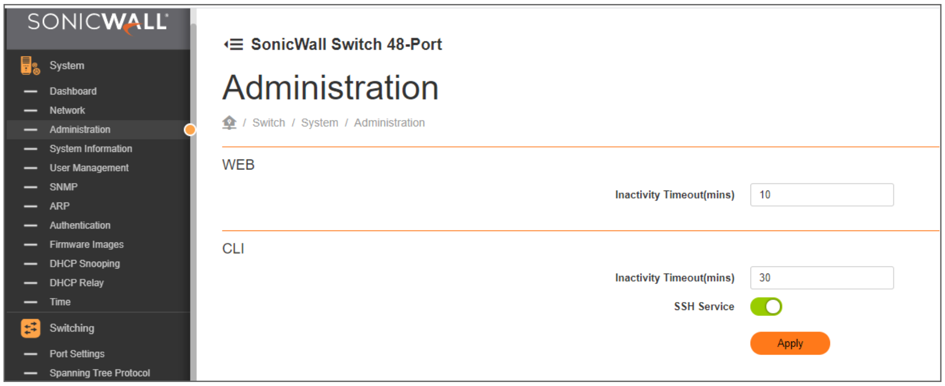
Apply

The default **Inactivity Timeout** is set to 10 minutes.

SSH Settings

Secure Shell (SSH) is a cryptographic network protocol for secure data communication network services. SSH is a way of accessing the command line interface on the network Switch. The traffic is encrypted, so it is difficult to eavesdrop on as it creates a secure connection within an insecure network such as the internet. Even if an attacker was able to view the traffic, the data would be incomprehensible without the correct encryption key to decode it.

Inactivity Timeout	Enter the amount of time that elapses before the SSH Service is timed out. The default is 30 minutes. The range is from 0-10000 minutes.
SSH Service	Select whether SSH is Enabled or Disabled. This is enabled by default.



SonicWall Switch 48-Port

Administration

Switch / System / Administration

WEB

Inactivity Timeout(mins) 10

CLI

Inactivity Timeout(mins) 30

SSH Service ●

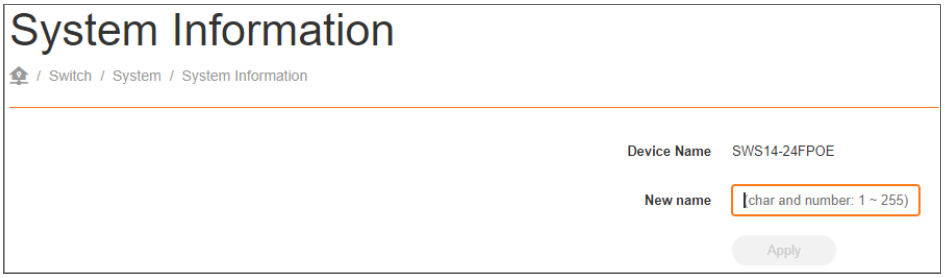
Apply

Click **Apply** to save the changes to the system.

System Information

The System Information screen contains general device information including the system name, system location, and system contact for the Switch.

Device Name	Displays the device name.
New Name	Enter the name you wish to use to identify the Switch. You can use up to 255 alphanumeric characters. ⓘ **NOTE:** The special characters that are supported and not supported: Not supported special characters: !%&+;"'?| Supported special characters: ~`@#$^*()_-={}[]:<>,./



System Information

Switch / System / System Information

Device Name SWS14-24FPOE

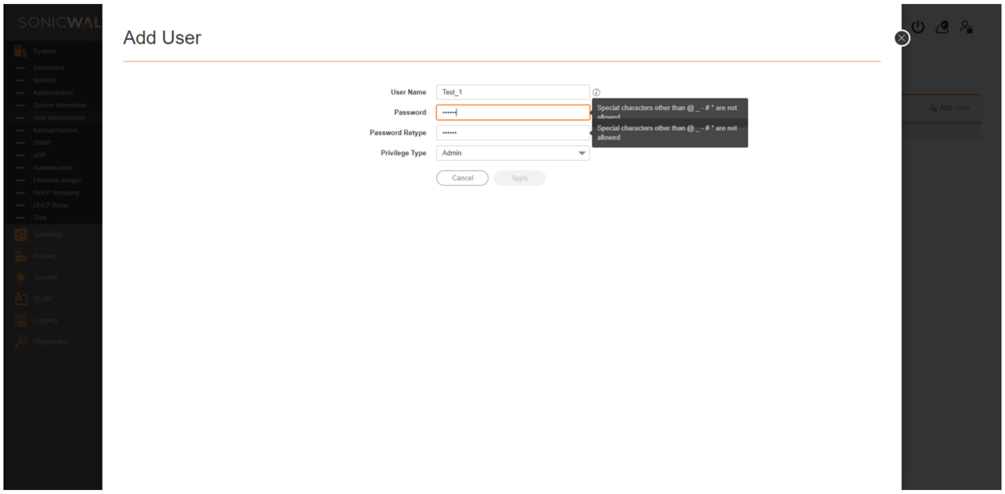
New name (char and number: 1 ~ 255)

Click **Change** to save the changes to the system.

User Management

From here, you can add or edit user accounts for the Switch. Click the Add User button to add an account or the Edit button to edit an existing account.

User Name	Enter a username. You can use up to 18 alphanumeric characters.
Password	Enter a new password for accessing the Switch.
Password Retype	Repeat the new password used to access the Switch.
Privilege Type	Select Admin or User from the list to regulate access rights.


Add User

User Name: Test_1

Password: ••••••

Password Retype: ••••••

Privilege Type: Admin

Special characters other than @ _ - # * are not allowed

Special characters other than @ _ - # * are not allowed

Click **Apply** to accept the changes or **Cancel** to discard them.

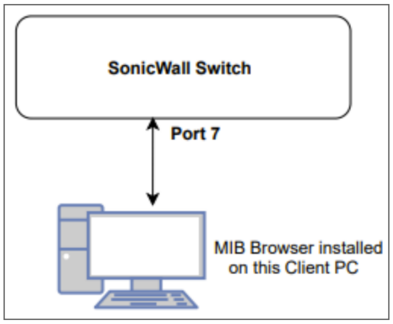
Simple Network Management Protocol

Simple Network Management Protocol (SNMP) is an Application Layer protocol designed specifically for managing and monitoring network devices. Simple Network Management Protocol (SNMP) is a popular protocol for network management. It is used for collecting information from and configuring network devices such as; servers, printers, hubs, Switches, and routers on an Internet Protocol (IP) network.

Several versions of SNMP are supported on SonicWall Switches. They are v1, v2c, and v3.

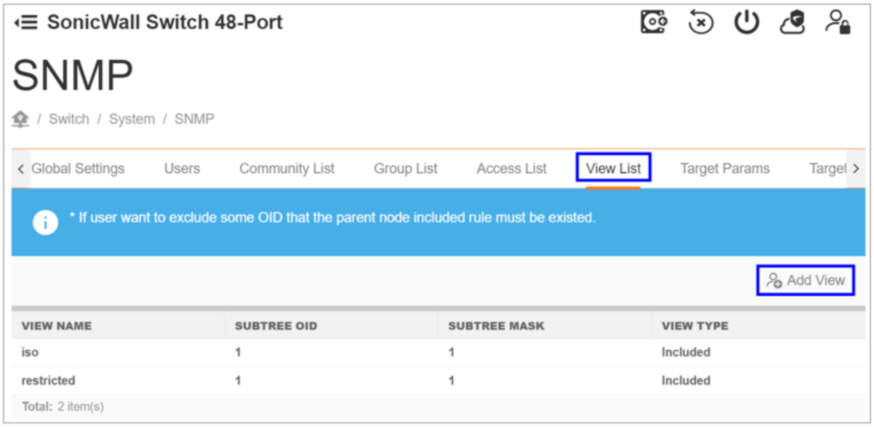
- SNMPv1, which is defined in RFC 1157 “A Simple Network Management Protocol (SNMP)”, is a standard that defines how communication occurs between SNMP-capable devices and specifies the SNMP message types. Version 1 is the simplest and most basic of versions. There may be times where it’s required to support older hardware.
- SNMPv2c, which is defined in RFC 1901 “Introduction to Community-Based SNMPv2,” RFC 1905, “Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2)”, and RFC 1906 “Transport Mappings for Version 2 of the Simple Network Management Protocol (SNMPv2)”. SNMPv2c updates protocol operations by introducing a Get Bulk request and authentication based on community names. Version 2c adds several enhancements to the protocol, such as support for “Informs”. Because of this, v2c has become the most widely used version. Unfortunately, a major weakness of v1 and v2c is security.
- SNMP v3 adds a security feature that overcomes the weaknesses in v1 and v2c. If possible, it is recommended that you use v3- especially if you plan to transmit sensitive information across unsecured links. However, the extra security feature makes configuration a little more complex. An agent translates the local management information from the managed Switch into a form that is compatible with SNMP.

Classic diagram of SonicWall Switch for SNMP Testing



Add View List

- View name
  - The View Name should be all views in **READ VIEW**, **WRITE VIEW**, and, **NOTIFY VIEW** in Access list table.

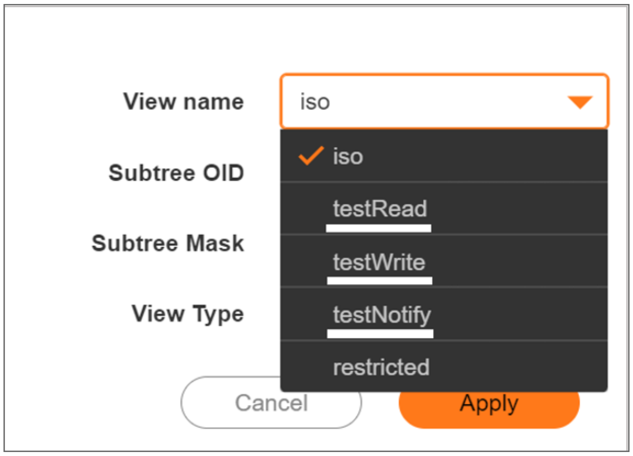


* If user want to exclude some OID that the parent node included rule must be existed.

VIEW NAME	SUBTREE OID	SUBTREE MASK	VIEW TYPE
iso	1	1	Included
restricted	1	1	Included

Total: 2 item(s)

  - Click on **Add View**



- Subtree OID
  - Number in 1-20
- Subtree mask level

  Subtree mask level in SNMP (Simple Network Management Protocol) refers to a technique used to simplify the management of a large number of related objects in an SNMP MIB (Management Information Base).

  A subtree mask is a bit pattern that is used to match a group of related objects in a MIB. The subtree mask level specifies the depth of the tree at which the subtree mask is applied. This means that only the objects within the specified subtree will be affected by the mask. For example, if the subtree mask level is set to 2, then the mask will only affect objects within the second level of the MIB tree. This allows administrators to apply the same configuration or settings to a group of related objects without affecting other objects in the MIB.

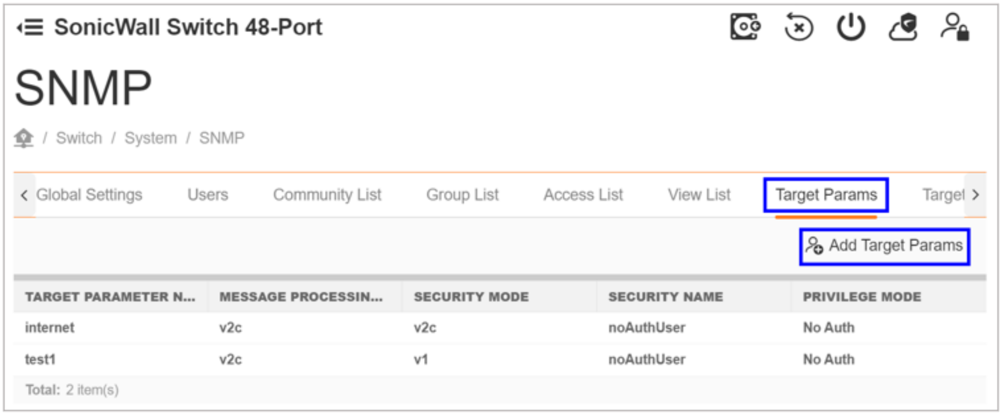
  - String with 1-20 characters.

    ⓘ | **NOTE:** mask level should not exceed OID level.
- View type
  - Selection
    - Included
    - Excluded

Add Target Params

On Target Params option, the maximum entries of **Target Params** is 10.

Click on **Add Target Params** and add target param.

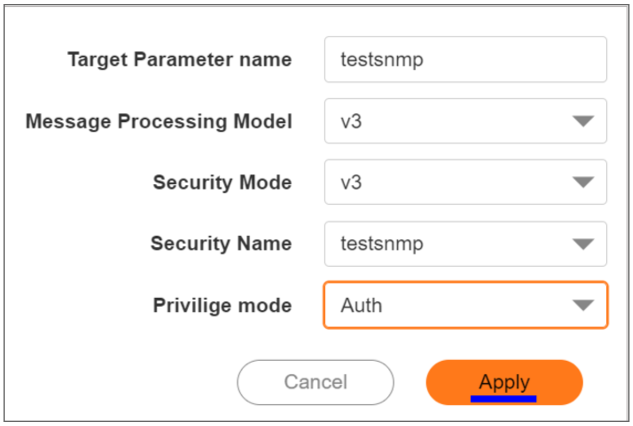


SNMP

/ Switch / System / SNMP

TARGET PARAMETER N...	MESSAGE PROCESSIN...	SECURITY MODE	SECURITY NAME	PRIVILEGE MODE
internet	v2c	v2c	noAuthUser	No Auth
test1	v2c	v1	noAuthUser	No Auth

Total: 2 item(s)



Target Parameter name	testsnmp
Message Processing Model	v3
Security Mode	v3
Security Name	testsnmp
Privilige mode	Auth

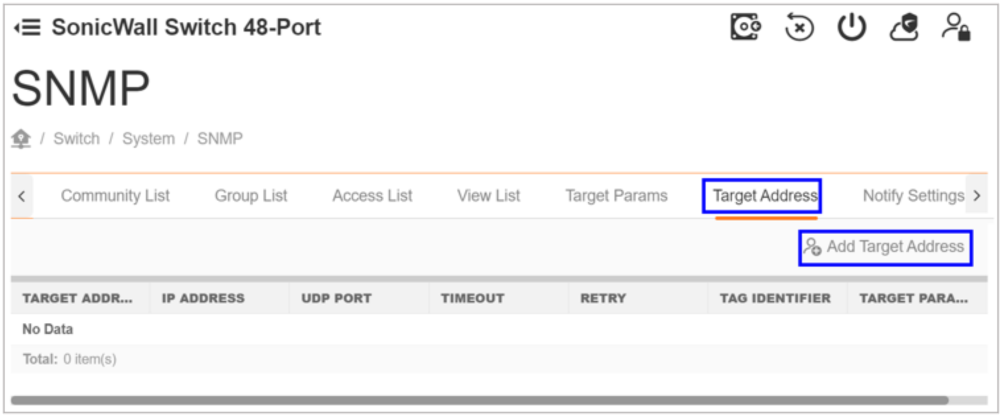
Target Parameter Name	• String with 1-20 characters. • Text field is only enabled on newly created entry.
Message Processing Model	• Selection • Options is the same as security mode. • v1 • v2c • v3
Security Mode	• Selection • Options • v1 • v2c • v3
Security Name	• Selection • Options are usernames in Users list table

Privilege Mode	• Selection • No auth • Auth • Priv

Click **Apply** to accept the changes or Cancel to discard them.

Add Target Address

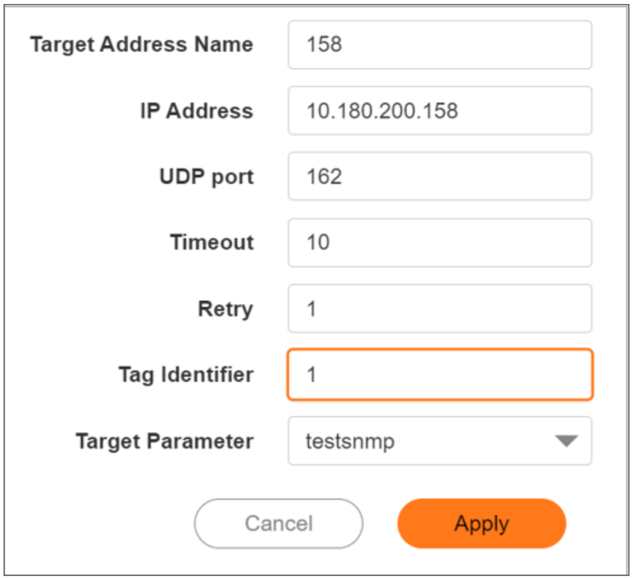
On Target Address option, the maximum entries of **Target Address** is 10.



TARGET ADDR...	IP ADDRESS	UDP PORT	TIMEOUT	RETRY	TAG IDENTIFIER	TARGET PARA...
No Data						

Total: 0 item(s)

Click on **Add Target Address**.



Target Address Name	158
IP Address	10.180.200.158
UDP port	162
Timeout	10
Retry	1
Tag Identifier	1
Target Parameter	testsnmp

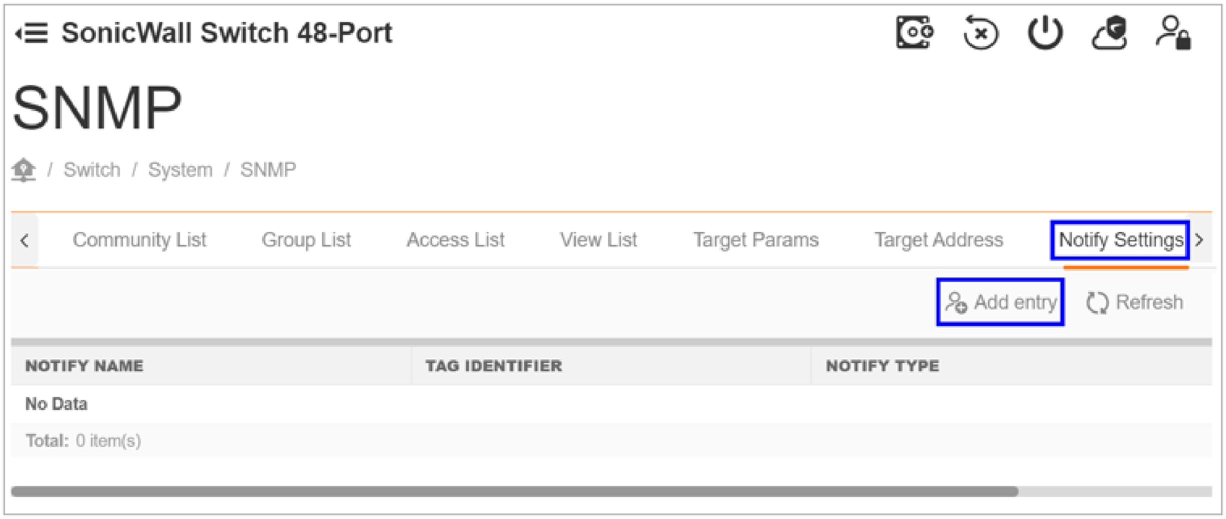
Target Address Name	Custom string with 1-32 characters
IP Address	String in IP format.

UDP Port	Number in 1-65535
Timeout	Number in 1-300
Retry	Number in 1-255
Tag Identifier	Custom string with 1-20 characters.
Target Parameter	• Selection • Options should be **Target Parameter Names** in Target Params list table.

Click **Apply** to accept the changes or Cancel to discard them.

Add Notify Setting

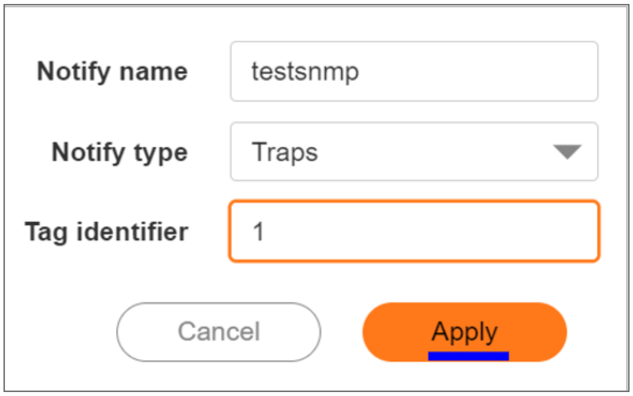
On **Notify Setting** option , the maximum entries of Notify Setting is 10.



NOTIFY NAME	TAG IDENTIFIER	NOTIFY TYPE
No Data		

Total: 0 item(s)

Click **Add entry** to Add notify list entry.



Notify name	testsnmp
Notify type	Traps
Tag identifier	1

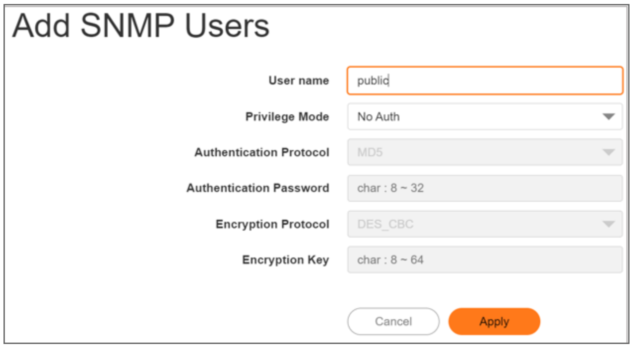
Notify Name	Custom string with 1-32 characters.

Tag identifier	• Custom string with 1-20 characters. • This field only works when Tag Identifier is filled in target address list
Notify type	• Selection • Traps • Informs

SNMP Traps/Informs

To send SNMP Traps/Informs:

1. Add **User** with Privilege Mode is **No Auth**(such as **public**)



Add SNMP Users

User name: public

Privilege Mode: No Auth

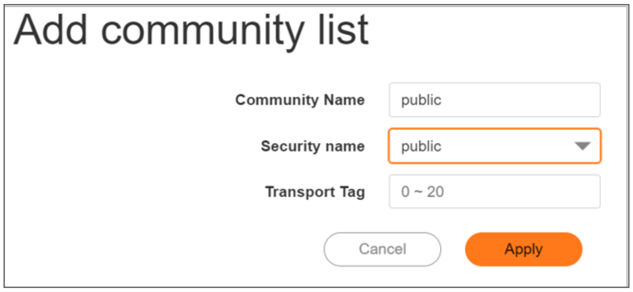
Authentication Protocol: MD5

Authentication Password: char : 8 ~ 32

Encryption Protocol: DES_CBC

Encryption Key: char : 8 ~ 64

2. **Add Community List** which the security name is the username in Users



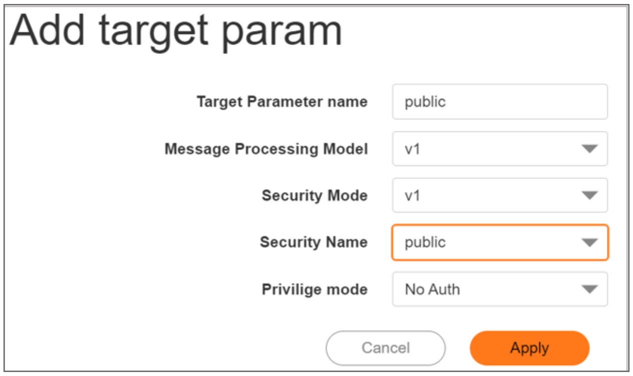
Add community list

Community Name: public

Security name: public

Transport Tag: 0 ~ 20

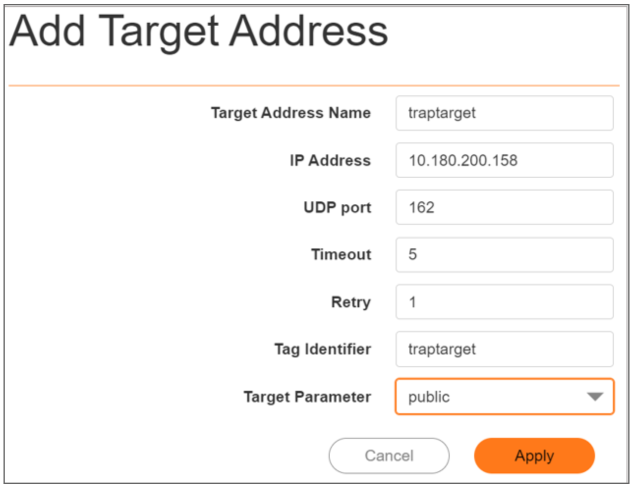
3. Add **TARGET PARAMS** and select the parameters as needed



Add target param

Target Parameter name	public
Message Processing Model	v1
Security Mode	v1
Security Name	public
Privilige mode	No Auth

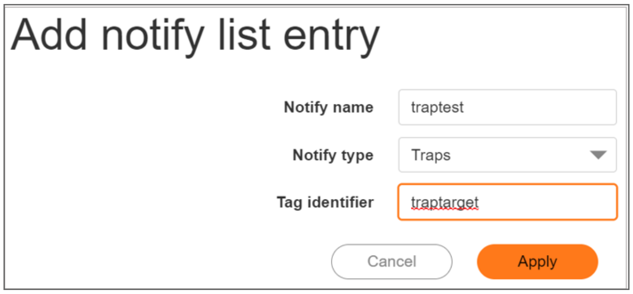
4. Add **TARGET ADDRESS** and fill out the parameters as needed



Add Target Address

Target Address Name	traptarget
IP Address	10.180.200.158
UDP port	162
Timeout	5
Retry	1
Tag Identifier	traptarget
Target Parameter	public

5. Add **NOTIFY SETTINGS** and fill out the parameters as needed

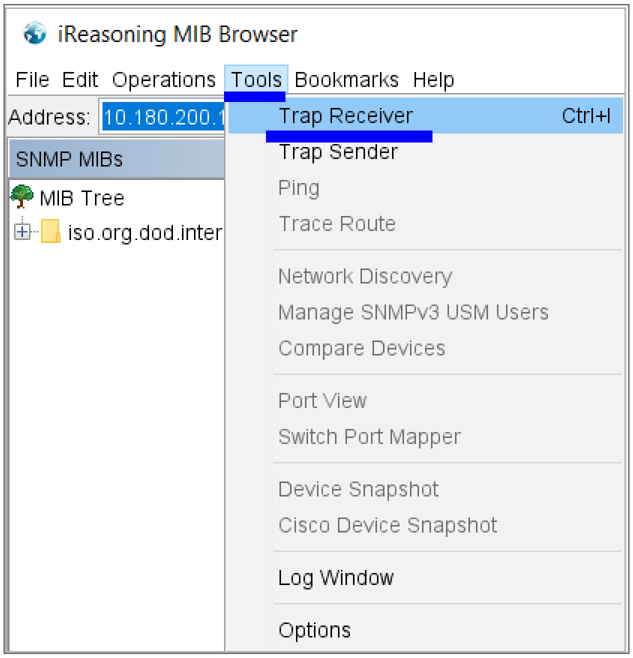


Add notify list entry

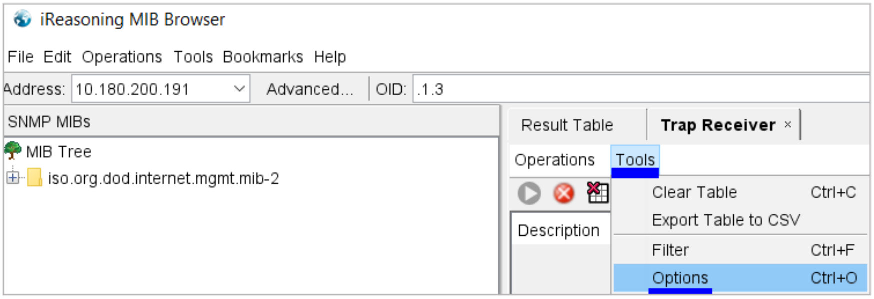
Notify name	traptest
Notify type	Traps
Tag identifier	traptarget

6. Using iReasoning MIB Browser to confirm the SNMP Trap Function

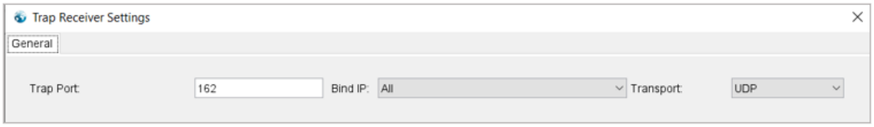
a. Download iReasoning MIB Browser, then Navigate to **Tools** >**Trap Receiver**



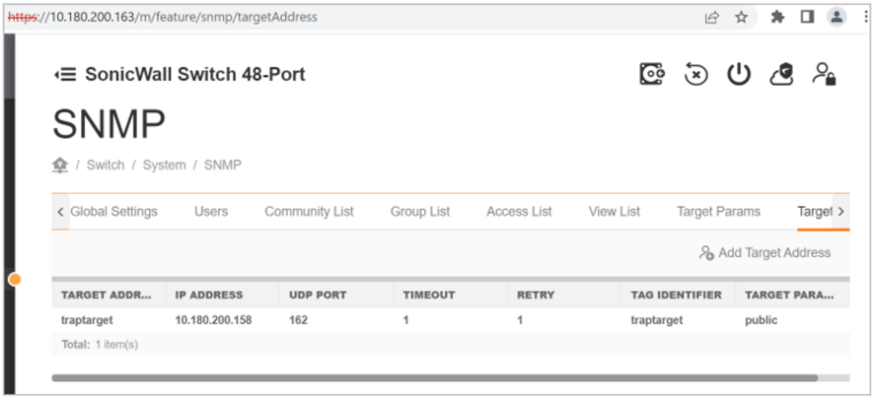
b. Click **Tools** >**Options**



c. Make sure the Trap Port is same as the **TARGET ADDRESS**



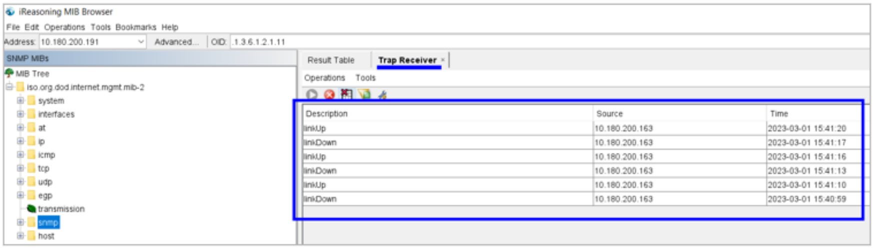
Trap Port: 162 Bind IP: All Transport: UDP



TARGET ADDR...	IP ADDRESS	UDP PORT	TIMEOUT	RETRY	TAG IDENTIFIER	TARGET PARA...
traptarget	10.180.200.158	162	1	1	traptarget	public

Total: 1 item(s)

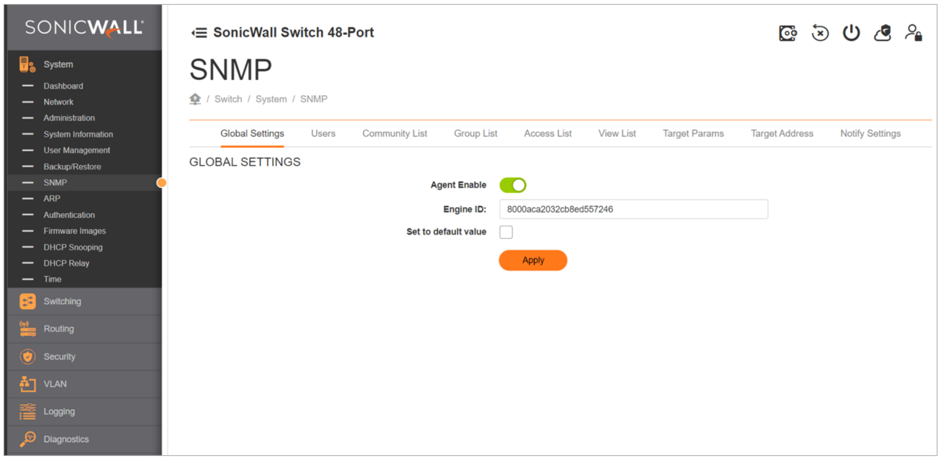
d. Trigger some SNMP Traps(such as **link up** or **link down**)



Description	Source	Time
linkUp	10.180.200.163	2023-03-01 15:41:20
linkDown	10.180.200.163	2023-03-01 15:41:17
linkUp	10.180.200.163	2023-03-01 15:41:16
linkDown	10.180.200.163	2023-03-01 15:41:13
linkUp	10.180.200.163	2023-03-01 15:41:10
linkDown	10.180.200.163	2023-03-01 15:40:59

How to configure SNMP on SonicWall Switch

1. Enable SNMP Agent

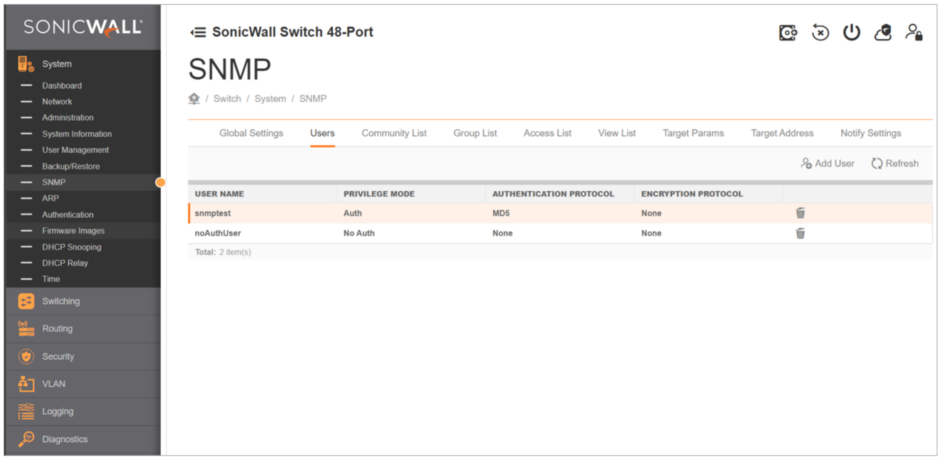


Agent Enable: ●

Engine ID: 8000aca2032cb8ed557246

Set to default value: □

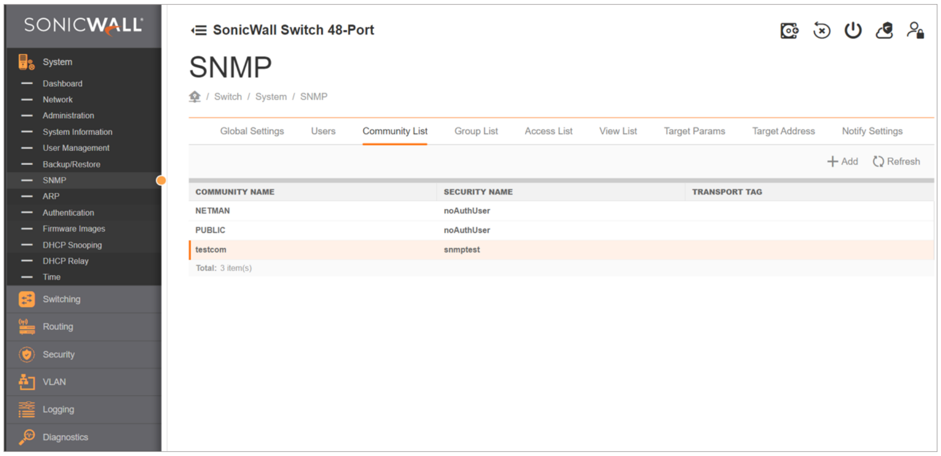
2. Add SNMP Users with Privilege Mode ‘Auth’ and Authentication Protocol ‘MD5’ (in my case user created is ‘snmptest’)



USER NAME	PRIVILEGE MODE	AUTHENTICATION PROTOCOL	ENCRYPTION PROTOCOL
snmptest	Auth	MD5	None
noAuthUser	No Auth	None	None

Total: 2 item(s)

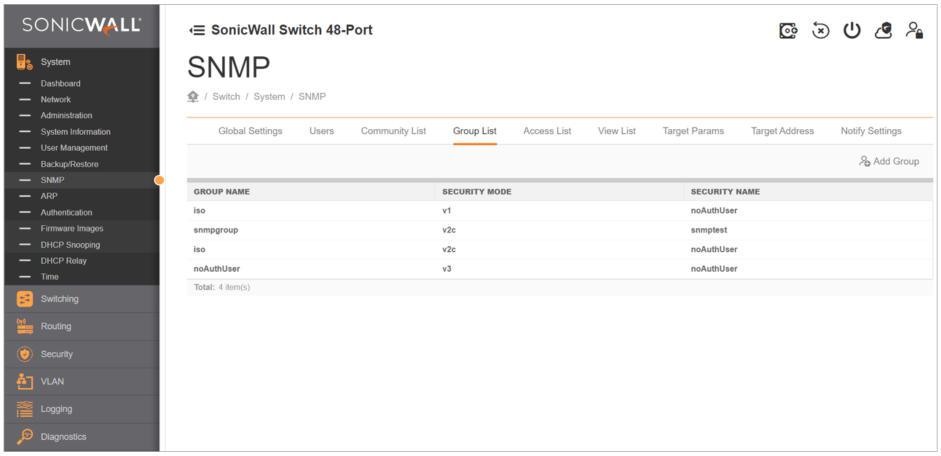
3. Add community list and call the Security name created in Step 2



COMMUNITY NAME	SECURITY NAME	TRANSPORT TAG
NETMAN	noAuthUser	
PUBLIC	noAuthUser	
testcom	snmptest	

Total: 3 item(s)

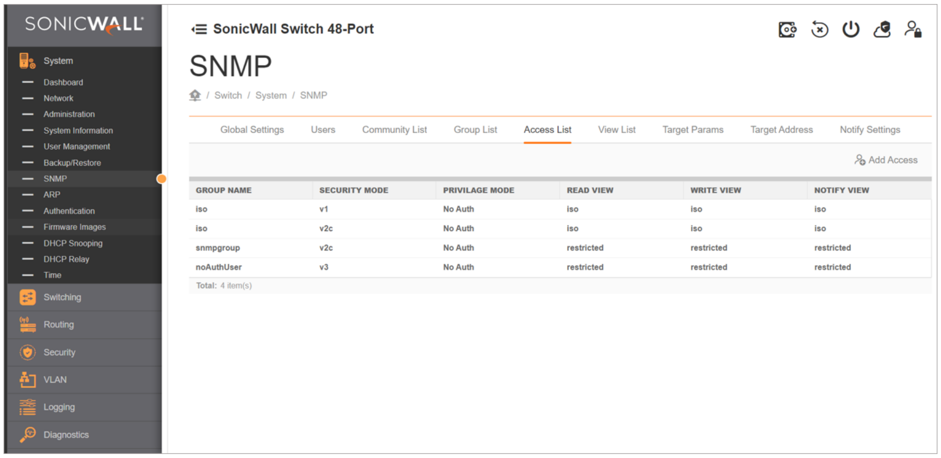
4. Add Group with Security mode as V2C and Security name created in Step 2



GROUP NAME	SECURITY MODE	SECURITY NAME
iso	v1	noAuthUser
snmpgroup	v2c	snmptest
iso	v2c	noAuthUser
noAuthUser	v3	noAuthUser

Total: 4 item(s)

5. Add Access to the list - Security mode as V2C and configure Read, Write and Notify view as ‘restricted’.



SNMP

GROUP NAME	SECURITY MODE	PRIVILAGE MODE	READ VIEW	WRITE VIEW	NOTIFY VIEW
iso	v1	No Auth	iso	iso	iso
iso	v2c	No Auth	iso	iso	iso
snmpgroup	v2c	No Auth	restricted	restricted	restricted
noAuthUser	v3	No Auth	restricted	restricted	restricted

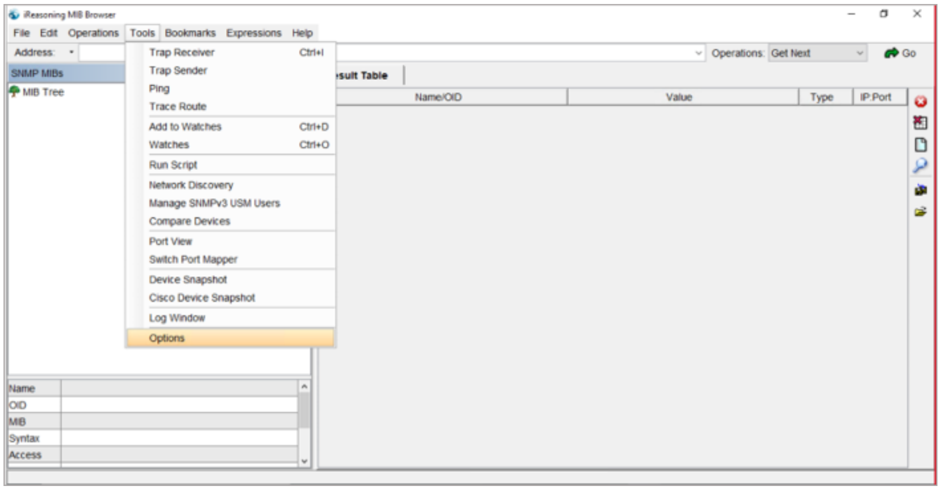
Total: 4 item(s)

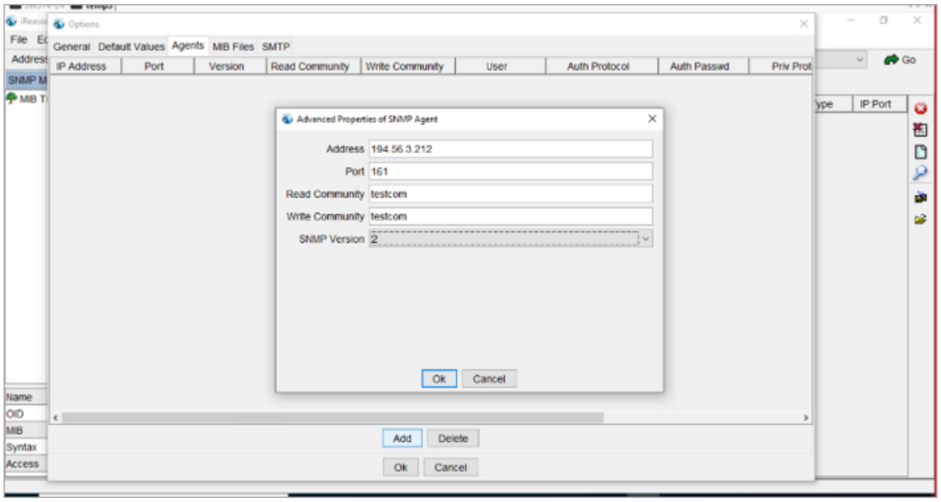
SNMP supported OID’s in 1.2.0.1-2s

SL	SNMP Parameter	OID
1	Runtime/Uptime	1.3.6.1.2.1.1.3.0
2	Port Link Status	1.3.6.1.2.1.2.2.1.8.X
3	Port Description	1.3.6.1.2.1.2.2.1.2.X
4	Temperature	1.3.6.1.2.1.99.1.1.1.4.4
5	Firmware Version	1.3.6.1.2.1.47.1.1.1.1.9.1
6	Port Speed/Active Speed	1.3.6.1.2.1.2.2.1.5.X
7	Port Auto Negotiation	1.3.6.1.2.1.26.5.1.1.1. X.1
8	Port Duplex	1.3.6.1.2.1.10.7.2.1.19.X
9	Port Rx Counter	1.3.6.1.2.1.2.2.1.10.X
10	Port Tx Counter	1.3.6.1.2.1.2.2.1.16.X
11	Model Name	1.3.6.1.2.1.47.1.1.1.1.13.1
12	Switch Name/System Name	1.3.6.1.2.1.1.5.0
13	IP address	1.3.6.1.2.1.4.20.1.1
14	Serial Number	1.3.6.1.2.1.47.1.1.1.1.11.1
15	System MAC address	1.3.6.1.2.1.2.2.1.6.61
16	Vendor Name	1.3.6.1.2.1.47.1.1.1.1.12.1

How to Configure SNMP/MIB Browser on Client PC

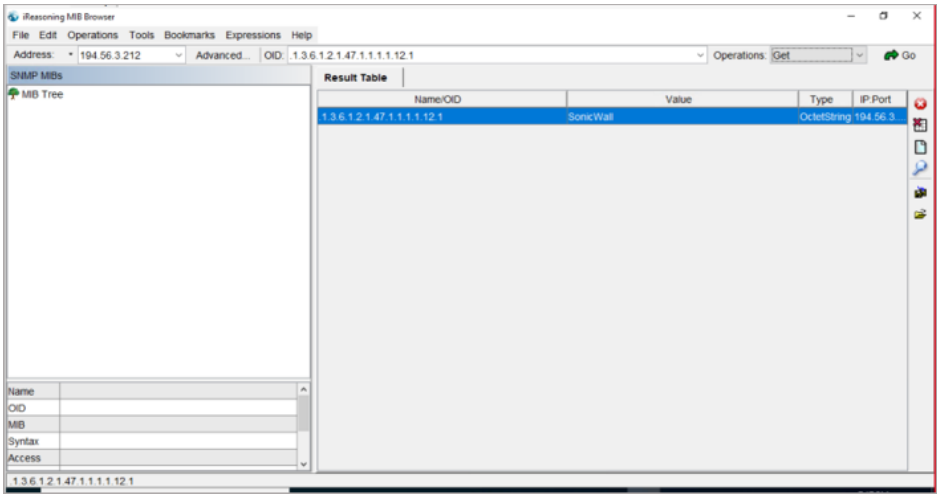
1. Download ireasoning mib browser from https://www.ireasoning.com/download.shtml
2. Install and Launch the MIB browser
3. Navigate to **Tools > options > Agents > Add agent**





Address 194.56.3.212
Port 161
Read Community testcom
Write Community testcom
SNMP Version 2

4. Enter the OID’s Provided above and start with SNMP operations.



Address: 194.56.3.212
OID: .1.3.6.1.2.1.47.1.1.1.1.12.1
Operations: Get

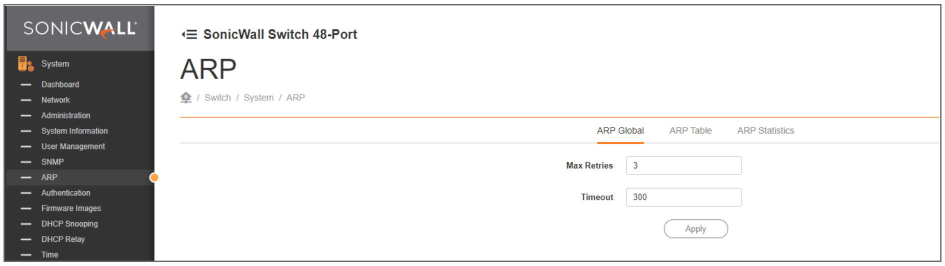
Name/OID	Value	Type	IP:Port
1.3.6.1.2.1.47.1.1.1.1.12.1	SonicWall	OctetString	194.56.3...

.1.3.6.1.2.1.47.1.1.1.1.12.1

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.

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.
Timeout	Enter the ARP time out in the Timeout field. The default value is 300 seconds. After the time out period, the ARP entries are removed from the table.



Max Retries: 3

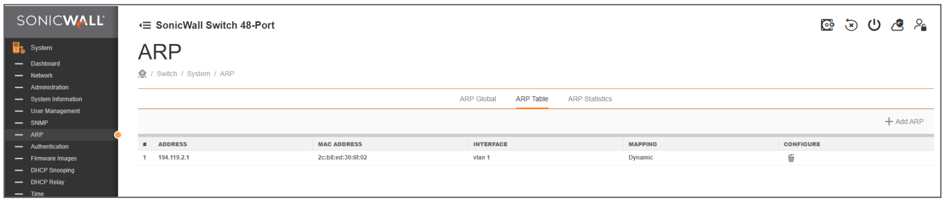
Timeout: 300

Click **Apply** to save the changes to the system.

ARP Table

The Switch maintains an ARP table which is made of mapped IP addresses and MAC addresses.

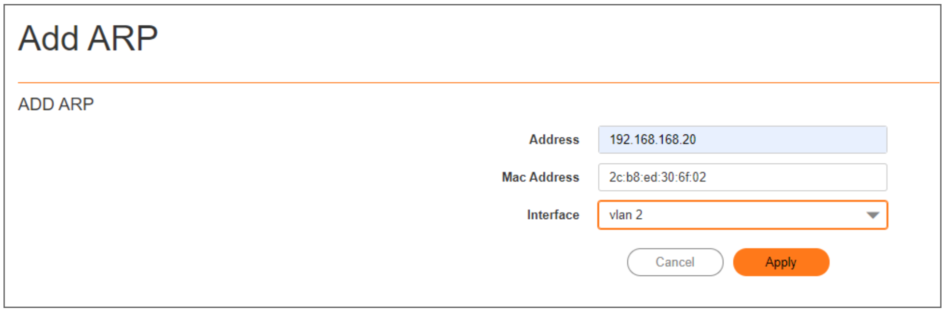
IP Address	The IP address of the host to which the MAC address is configured.
MAC Address	MAC address of the host.
Interface	Displays the VLAN interface of the host.
Mapping	Displays the mapping status as Dynamic or Static.



#	ADDRESS	MAC ADDRESS	INTERFACE	MAPPING	CONFIGURE
1	194.119.2.1	2c:b8:ed:30:6f:02	vlan 1	Dynamic	🗑

To add an entry in the ARP Table:

1. Click **Add ARP** above the table.
   The **Add ARP** screen appears.
2. In the **Address** field, enter the IP address of the host to which the MAC address is to be configured.
3. In the **MAC Address** field, enter the MAC address of the host in the MAC address field.
4. In the **Interface** drop-down, select the required VLAN interface.
5. Click **Apply** to save the changes.



Add ARP

ADD ARP

Address: 192.168.168.20

Mac Address: 2c:b8:ed:30:6f:02

Interface: vlan 2

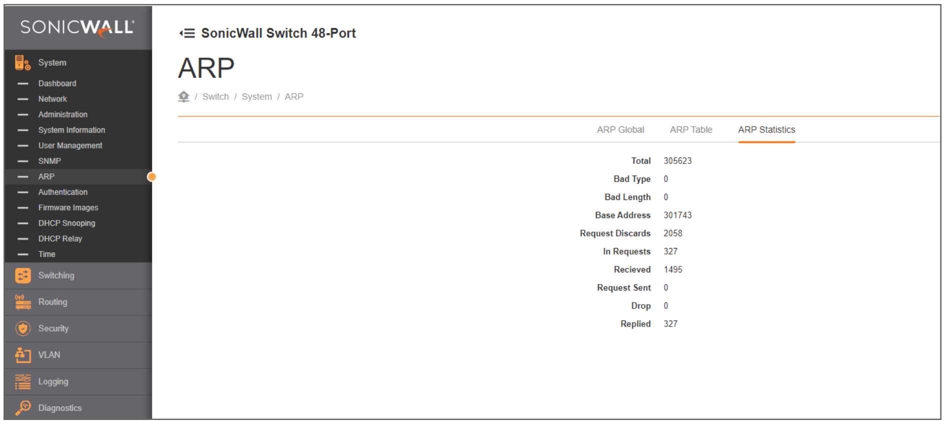
To delete an entry from the ARP Table:

1. Click **Configure** on the entry which you to delete.
   A Confirmation dialog appears.
2. Click **Confirm** to delete the entry from the ARP table.

ARP Statistics

The ARP Statistics section displays a summary of all ARP data when mapping an Internet Protocol address to a MAC address.

Total	The total number of ARP packets available on the interface.
Bad Type	The number of ARP requests rejected due to bad type.
Bad Length	The number of ARP requests rejected due to bad length.
Base Address	The number of ARP requests rejected due to bad address.
Request Discards	The number of ARP packets received that are not of a known type. They are not ARP requests or ARP responses.
In Requests	The number of ARP requests received on the interface.
Received	The number of ARP packets received on the interface.
Request Sent	The number of ARP requests transmitted over the interface.
Drop	The number of ARP requests dropped over the interface.
Replied	The number of ARP replies received over the interface.



SonicWall Switch 48-Port

ARP

/ Switch / System / ARP

Total	305623
Bad Type	0
Bad Length	0
Base Address	301743
Request Discards	2058
In Requests	327
Recieved	1495
Request Sent	0
Drop	0
Replied	327

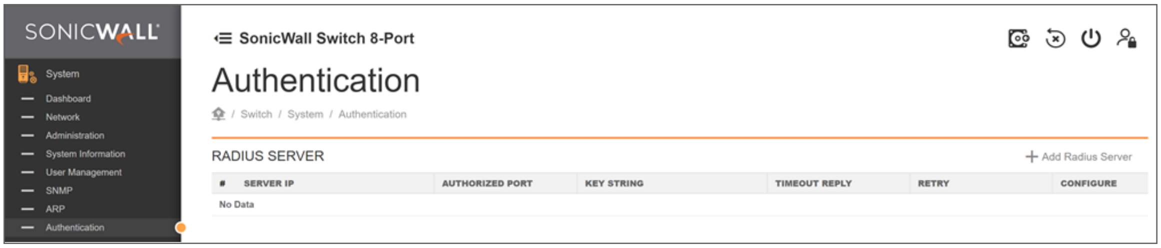
Authentication

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.

ⓘ | **NOTE:** You can add a maximum of 5 Radius servers.

ⓘ | **NOTE:** All the below fields in the table are mandatory and user defined.

Server IP	Enter the Radius Server IP address.
Authorized Port	Enter the authorized port number. Enter any port number between 1 to 65535.
Key String	Enter the Key String used for encrypting all Radius communication between the device and the Radius server.
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.
Retry	Enter the number of transmitted requests sent to the Radius server before a failure occurs. Enter any value between 1 to 10.



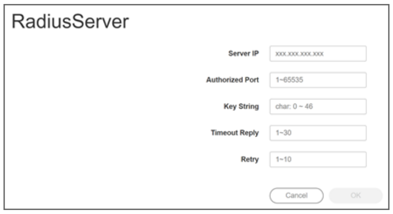
SonicWall Switch 8-Port

Authentication

/ Switch / System / Authentication

RADIUS SERVER

#	SERVER IP	AUTHORIZED PORT	KEY STRING	TIMEOUT REPLY	RETRY	CONFIGURE
No Data						



RadiusServer

Server IP: xxx.xxx.xxx.xxx

Authorized Port: 1~65535

Key String: char: 0 ~ 46

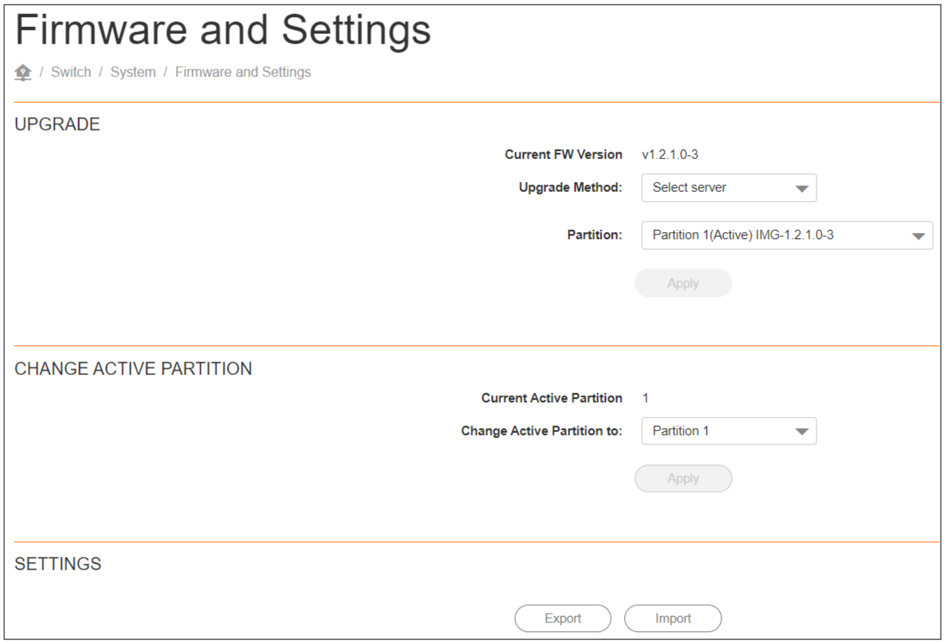
Timeout Reply: 1~30

Retry: 1~10

Firmware and Settings

The Switch maintains two versions of the Switch image in its permanent storage. One image is the active image, and the second image is the backup image. The Dual Image screen enables the user to select which partition will be set as active after the next reset. The Switch boots and runs from the active image. If the active image is corrupt, the system automatically boots from the non- active image.

Upgrade Method	You can upgrade the Switch Firmware using the following methods: • Upload File • SonicWall Cloud server
Available Firmware	Select the available firmware in the Switch for upgrade process.
Partition	SonicWall Switch supports two partition with one of them being ACTIVE at a time.
Current Active Partition	This displays the partition which is currently ACTIVE.
Change Active Partition	This option is used to change the active parition to the other one. Switch reboots post this action.
Settings	You can export and import the Switch Firmware configuration file using the following methods: • Export- You can export your complete set of configuration data to a local machine as `.cfg` file. For example, the downloaded file name is `SWS14-24FPOE_v1.2.1.X-X.cfg` • Import- You can import the configuration data from a local machine as `.cfg` file into your appliance.


Firmware and Settings

UPGRADE

Current FW Version v1.2.1.0-3

Upgrade Method: Select server

Partition: Partition 1(Active) IMG-1.2.1.0-3

CHANGE ACTIVE PARTITION

Current Active Partition 1

Change Active Partition to: Partition 1

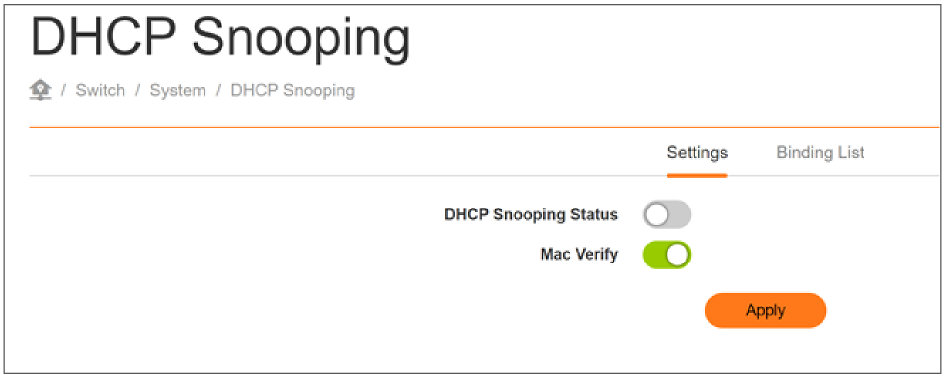
SETTINGS

Click **Apply** to save the changes on this page.

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.

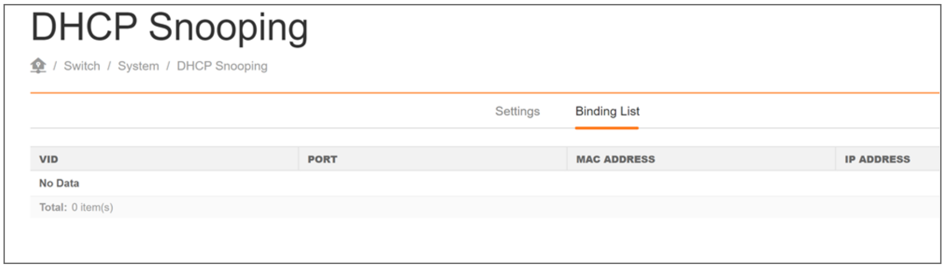
DHCP Snooping Status	Enable or Disable DHCP Snooping
MAC Verify	Enable this setting If the device receives a packet on an untrusted interface and the source MAC address and the DHCP client hardware address do not match, address verification causes the device to drop the packet


DHCP Snooping

DHCP Snooping Status: off

Mac Verify: on

Binding List	This list shows the current statistics of vlan id, ports, mac address and the respective IP Address

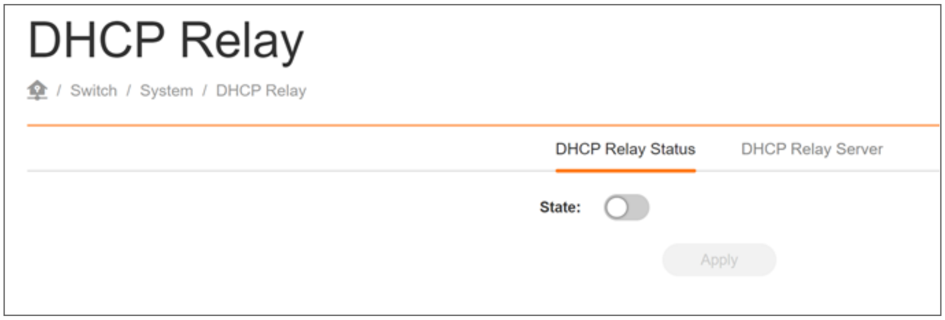


VID	PORT	MAC ADDRESS	IP ADDRESS
No Data			
Total: 0 item(s)			

DHCP Relay

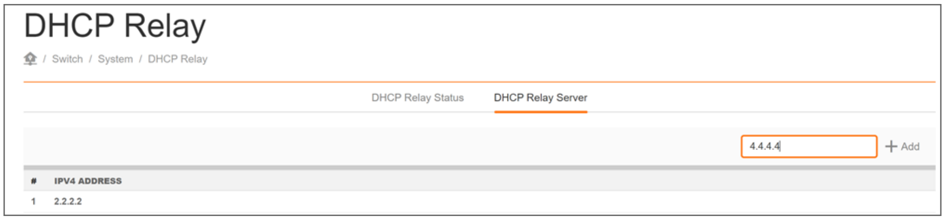
DHCP Relay is an option used to have local hosts communicate to a DHCP server in another network and switch works as a relay device.

State	Enable this option to make use of DHCP Relay option.



State: ○

DHCP Relay Server	Enter the IP Address of the DHCP Server and Click on Add.



4.4.4.4

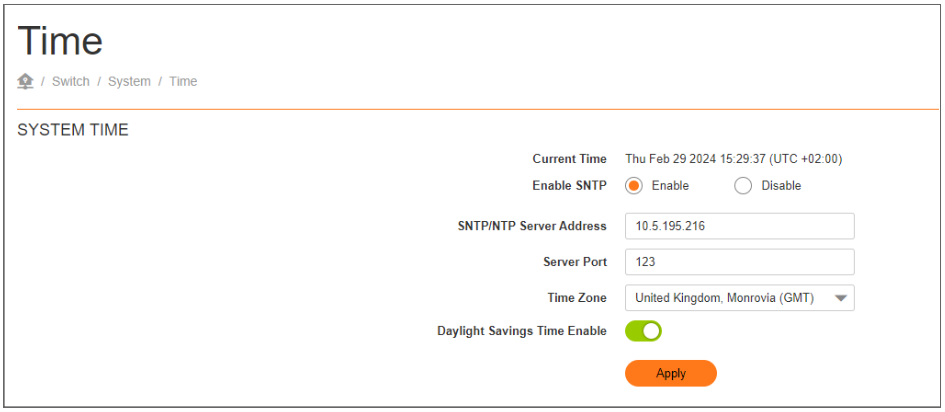
#	IPV4 ADDRESS
1	2.2.2.2

Time

Use the Time screen to view and adjust date and time settings. The Switch supports Simple Network Time Protocol (SNTP). SNTP assures accurate network device clock time synchronization up to the millisecond. Time synchronization is performed by a network SNTP server. This software operates only as an SNTP client and cannot provide time services to other systems.

In the **System Time** section you can use the following options:

Options	Description
Current time	Displays the current time.
Enable SNTP	Select whether to Enable or Disable the SNTP server. The system time is set via an SNTP sever.
Time Zone	Select the difference between Greenwich Mean Time (GMT) and local time.
SNTP/NTP Server Address	Enter the SNTP or NTP sever IP address or hostname.
Server Port	Displays the time sever port.
Daylight Saving Time (DST)	Enable to reflect the observance of daylight saving time. ⓘ **NOTE:** Notes on countries observing and non observing Daylight Saving Time. When selecting countries where DST is not observed, the DST option is disabled by default and user cannot enable. When group of countries is selected, with some observing DST and others not, the user has the flexibility to enable or disable DST according to their preference.


Time

/ Switch / System / Time

SYSTEM TIME

Current Time: Thu Feb 29 2024 15:29:37 (UTC +02:00)

Enable SNTP: ● Enable ○ Disable

SNTP/NTP Server Address: 10.5.195.216

Server Port: 123

Time Zone: United Kingdom, Monrovia (GMT)

Daylight Savings Time Enable: ●

To configure date/time through SNTP:

1. In the **Enable SNTP** settings, select the **Enable** option to configure the date or time through SNTP.
2. In the **SNTP/NTP Server Address** field, enter the IP address or the host name of the SNTP/NTP server.
3. Enter the port number on the SNTP server to which SNTP requests are sent. The valid range is from 1–65535. The default is 123.
4. In the **Time Zone Offset** list, select by country or by the Coordinated Universal Time (UTC/GMT) time zone in which the Switch is located.
5. If required, select **Daylight Saving Time** to reflect the observance of daylight saving time.
6. Click **Apply** to update the system settings.

To configure date/time manually:

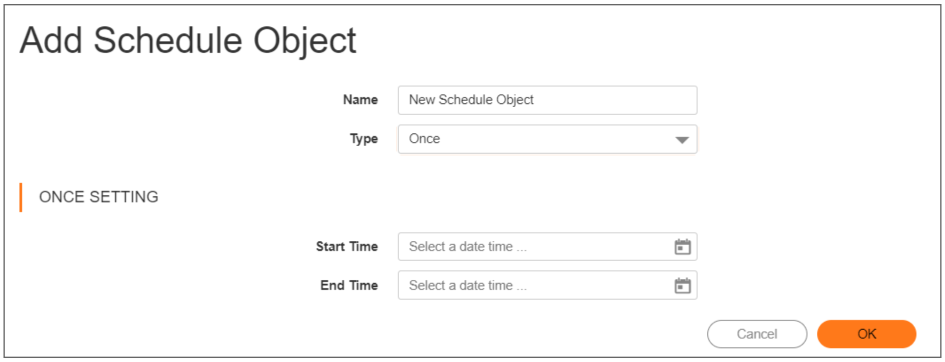
1. In the **Enable SNTP** settings, select the **Disable** option to configure the date or time manually.
2. In the **Manual Time** settings, select the date, time, and time zone you wish to set.
3. Click **Apply** to update the system settings.

In the **Schedule** section you can configure a time schedule for connected Power over Ethernet (PoE) enabled devices that are active only during business hours. This helps save energy, reduce electricity consumption, and lower associated costs.

To add a schedule:

Utilize the scheduling feature to manage the timing of PoE ports on the Switch. Create a schedule object, and then apply it across the PoE ports.

1. Click + icon to add the schedule object.
2. Enter a name for the new schedule.
3. Select the type of schedule from the list:
   - **Once**- This option allows you to add one schedule profile, where you can select the **Start** and **End** date and time of the schedule.



Add Schedule Object

Name: New Schedule Object

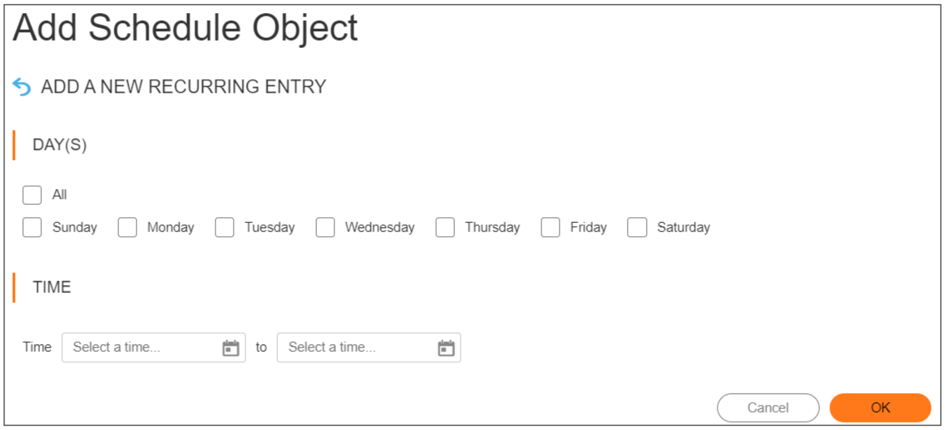
Type: Once

ONCE SETTING

Start Time: Select a date time ...

End Time: Select a date time ...

   - **Recurring**-This option allows you to add recurring entries. You can select the day and time for each schedule. Each profile allows scheduling up to seven entries.



Add Schedule Object

ADD A NEW RECURRING ENTRY

DAY(S)

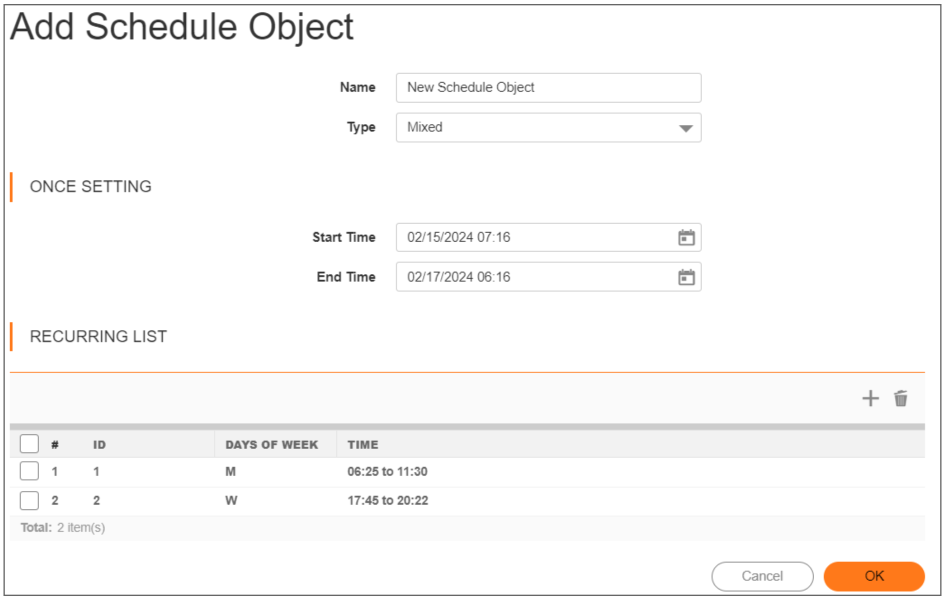
□ All

□ Sunday □ Monday □ Tuesday □ Wednesday □ Thursday □ Friday □ Saturday

TIME

Time: Select a time... to Select a time...

- **Mixed**- Allows to add both once and recurring schedule entries. You can select the day and time for each schedule in both **Once** and **Recurring** settings.



Add Schedule Object

Name: New Schedule Object

Type: Mixed

ONCE SETTING

Start Time: 02/15/2024 07:16

End Time: 02/17/2024 06:16

RECURRING LIST

☐	#	ID	DAYS OF WEEK	TIME
☐	1	1	M	06:25 to 11:30
☐	2	2	W	17:45 to 20:22

Total: 2 item(s)

Next go to the **Switching > Port Settings > PoE** tab to select these schedule profiles that are available for PoE usage on the switch port.

Switching

The Switching tab exhibits complete standard-based Layer 2 switching capabilities, including: Link Aggregation, 802.1D single Spanning Tree Protocol, 802.1w Rapid Spanning Tree Protocol, 802.1s Multiple Spanning Tree Protocol, MAC Address Table, Internet Group Management Protocol (IGMP) Snooping, 802.1ab Link Layer Discovery Protocol (LLDP). Utilize these features to configure the Switch to your preferences.

Topics:

Port Settings

This section provides you the configuration information of Port Settings of Switch.

- Port Settings
- Quality of Service
- PoE
- Security
- ACL Binding
- Advanced

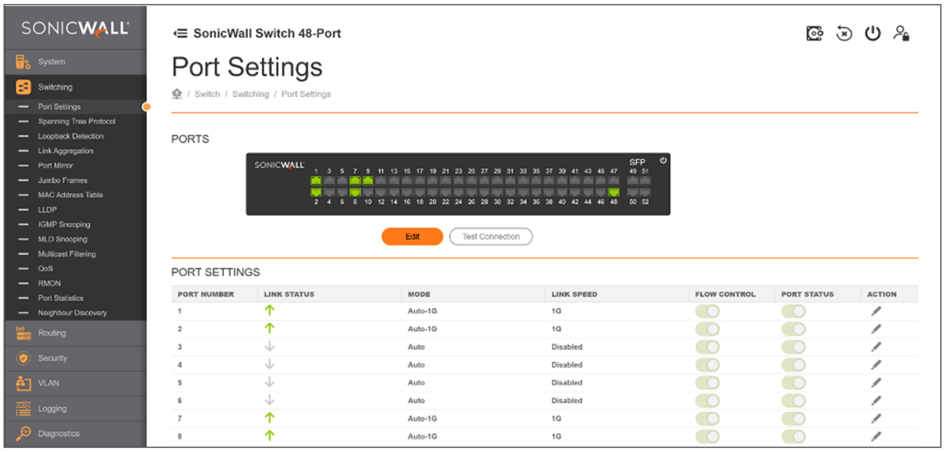
Port Settings

Use this screen to view and configure Switch port settings. The Port Settings feature lets 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. Configuring Gigabit ports require additional factors to be considered when arranging your preferences for the Switch compared to 10/100 ports. To access the page, in the **Ports** image, select the port which you to configure and click **Edit**.

Port Number	Displays the port number.
Status	Indicates whether the link is up or down.
Flow Control	A concentration of traffic on a port decreases port bandwidth and overflows buffer memory causing packet discards and frame losses. Flow Control is used to regulate transmission of signals to match the bandwidth of the receiving port. The Switch uses IEEE802.3x flow control in full duplex mode and backpressure flow control in half duplex mode. IEEE802.3x flow control is used in full duplex mode to send a pause signal to the sending port, causing it to temporarily stop sending signals when the receiving port memory buffers fill. Back Pressure flow control is typically used in half duplex mode to send a “collision” signal to the sending port (mimicking a state of packet collision) causing the sending port to temporarily stop sending signals and resend later.

Mode	Select the speed and the duplex mode of the Ethernet connection on this port. Selecting Auto (Auto-Negotiation) allows one port to negotiate with a peer port automatically to obtain the connection speed and duplex mode that both ends support. When auto-negotiation is turned on, a port on the Switch negotiates with the peer automatically to determine the connection speed and duplex mode. If the peer port does not support auto negotiation or turns off this feature, the Switch determines the connection speed by detecting the signal on the cable and using half duplex mode. When the Switch's auto-negotiation is turned off, a port uses the pre-configured speed and duplex mode when making a connection, thus requiring you to make sure that the settings of the peer port are the same in order to connect.
Port Description	Add port description. You add use up to 127 characters.

Click **Apply** to update the system settings.



Port Settings

PORT SETTINGS

PORT NUMBER	LINK STATUS	MODE	LINK SPEED	FLOW CONTROL	PORT STATUS	ACTION
1	↑	Auto-1G	1G	○	○	✎
2	↑	Auto-1G	1G	○	○	✎
3	↓	Auto	Disabled	○	○	✎
4	↓	Auto	Disabled	○	○	✎
5	↓	Auto	Disabled	○	○	✎
6	↓	Auto	Disabled	○	○	✎
7	↑	Auto-1G	1G	○	○	✎
8	↑	Auto-1G	1G	○	○	✎

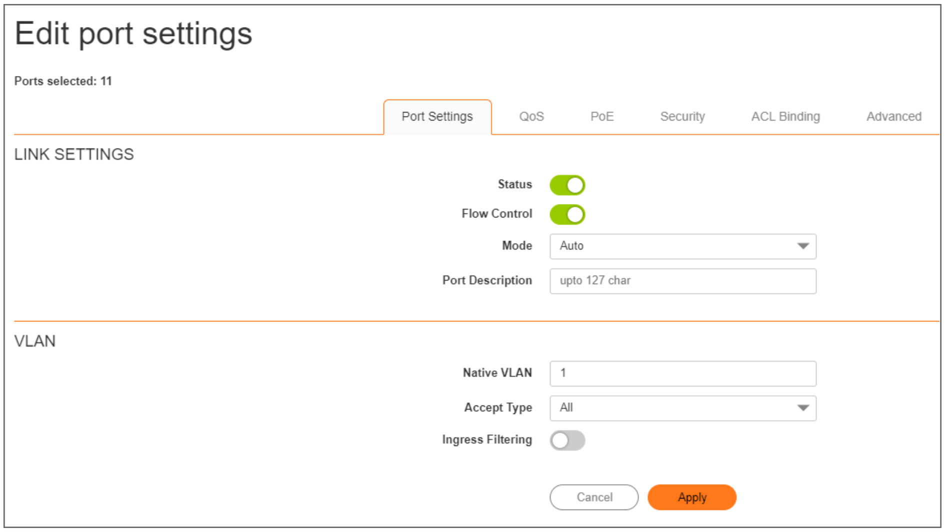
Native VLAN

When an Untagged packet enters a Switch port, the Native VLAN (Port VLAN ID) will be attached to the untagged packet and forward frames to a VLAN specified VID part of the Native VLAN. A packet received on a given port would be assigned that port's NATIVE VLAN and then be forwarded to the port that corresponded to the packet's destination address. If the Native VLAN of the port that received the packet is different from the Native VLAN of the port that is to transmit the packet, the Switch will drop the packet. Within the Switch, different Native VLAN mean different VLANs, so VLAN identification based upon the Native VLAN cannot create VLANs that extend outside a given Switch. If no VLANs are defined on the Switch, all ports are then assigned to a default VLAN with a NATIVE VLAN equal to 1.

ⓘ | **NOTE:** To enable Native VLAN functionality, the following requirements must be met:

- All ports must have a defined Native VLAN.
- If no other value is specified, the NATIVE VLAN is used.
- If you wish to change the port’s default NATIVE VLAN, you must first create a VLAN that includes the port as a member.

NATIVE VLAN	Enter the Native VLAN value. The range is from 1-4094.
Accept Type	Select Tagged Only and Untagged Only from the list. • Tagged Only: The port discards any untagged frames it’s receives. The port only accepts tagged frames. • Untagged Only: Only untagged frames received on the port are accepted. • All: The port accepts both tagged and untagged frames.
Ingress Filtering	Specify how you wish the port to handle tagged frames. Select Enabled or Disabled from the list. • Enabled: tagged frames are discarded if VID does not match the NATIVE VLAN of the port. • Disabled: All frames are forwarded in accordance with the IEEE 802.1Q VLAN.



Edit port settings

Ports selected: 11

LINK SETTINGS

Status: on

Flow Control: on

Mode: Auto

Port Description: upto 127 char

VLAN

Native VLAN: 1

Accept Type: All

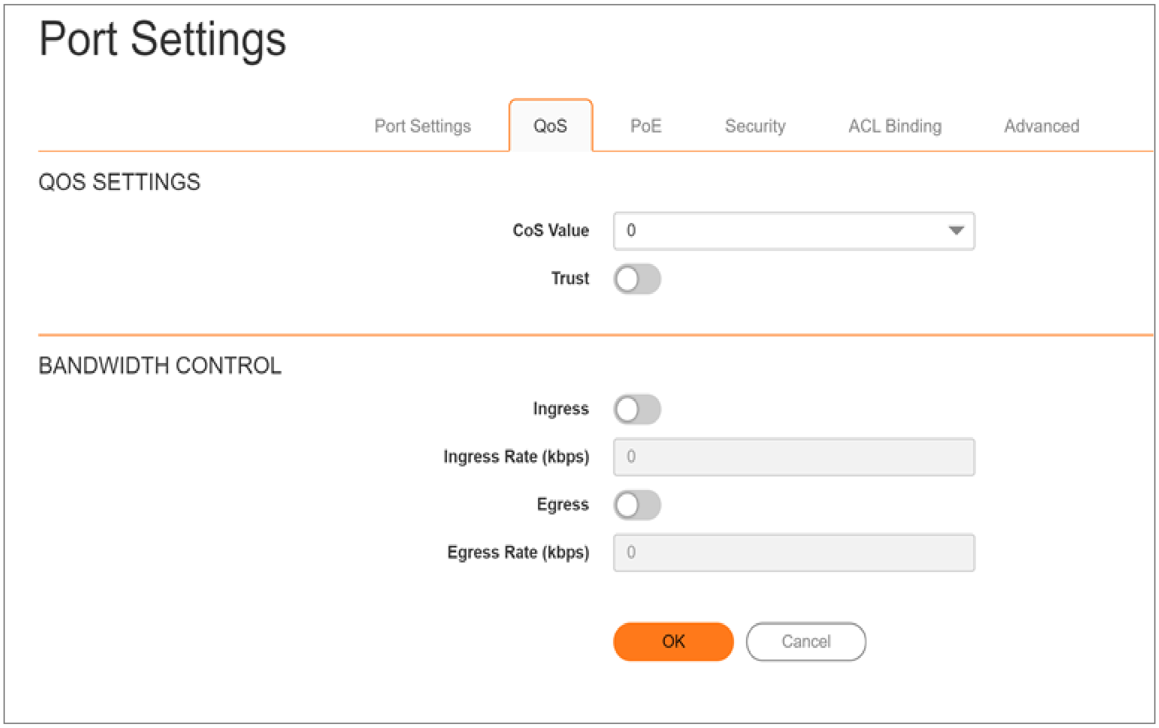
Ingress Filtering: off

Click **Apply** to update the system settings.

QoS Settings

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. Next, Select to Enable or Disable the Trust setting to let any CoS packet be marked at ingress.

CoS (Class of Service) Value	Select the CoS priority tag values, where 0 is the lowest and 7 is the highest.
Trust	Select Enable to trust any CoS packet marking at ingress and select Disable to not trust any CoS packet marking at ingress.



CoS Value: 0

Trust: ○

Ingress: ○

Ingress Rate (kbps): 0

Egress: ○

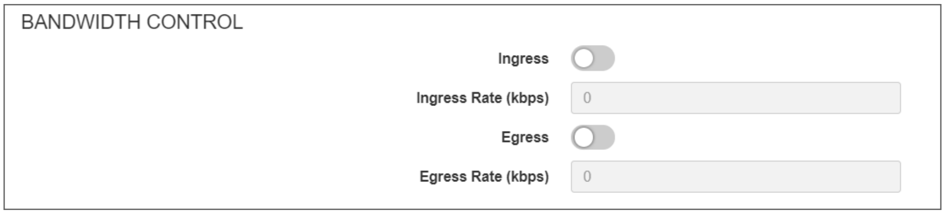
Egress Rate (kbps): 0

Click **Apply** to save the changes to the system.

Bandwidth Control

The Bandwidth Control feature allows users to define the bandwidth settings for a specified port’s Ingress Rate Limit and Egress Rate.

Ingress	Select to Enable or Disable ingress on the interface.
Ingress Rate	Enter the ingress rate in kilobits per second. The Gigabit Ethernet ports have a maximum speed of 1000000 kilobits per second.
Egress	Select from the drop down box to Enable or Disable egress on the interface .
Egress Rate	Enter the egress rate in kilobits per second. The Gigabit Ethernet ports have a maximum speed of 1000000 kilobits per second.



BANDWIDTH CONTROL

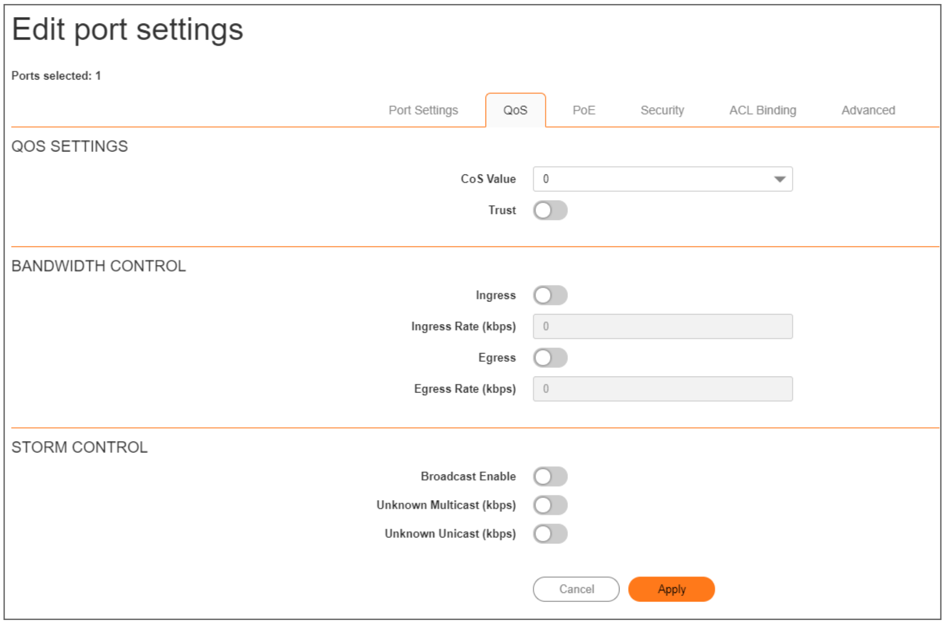
Ingress	○
Ingress Rate (kbps)	0
Egress	○
Egress Rate (kbps)	0

Click **Apply** to save the changes to the system.

Storm Control

Storm Control limits the amount of Broadcast, Unknown Multicast, and Unknown Unicast frames accepted and forwarded by the Switch. Storm Control can be enabled per port by defining the packet type and the rate that the packets are transmitted at. The Switch measures the incoming Broadcast, Unknown Multicast, and Unknown Unicast frames rates separately on each port, and discards the frames when the rate exceeds a user-defined rate.

Broadcast Enable	Enter the broadcast rate in kilobits per second. The Gigabit Ethernet ports have a maximum speed of 1000000 kilobits per second. If the rate of broadcast traffic ingress on the interface increases beyond the configured threshold, the traffic is dropped.
Unknown Multicast	Enter the Unknown Multicast rate in kilobits per second. The Gigabit Ethernet ports have a maximum speed of 1000000 kilobits per second. If the rate of broadcast traffic ingress on the interface increases beyond the configured threshold, the traffic is dropped.
Unknown Unicast	Enter the Unknown Unicast rate in kilobits per second. The Gigabit Ethernet ports have a maximum speed of 1000000 kilobits per second. If the rate of broadcast traffic ingress on the interface increases beyond the configured threshold, the traffic is dropped.



Edit port settings

Ports selected: 1

QOS SETTINGS

CoS Value: 0

Trust: ○

BANDWIDTH CONTROL

Ingress: ○

Ingress Rate (kbps): 0

Egress: ○

Egress Rate (kbps): 0

STORM CONTROL

Broadcast Enable: ○

Unknown Multicast (kbps): ○

Unknown Unicast (kbps): ○

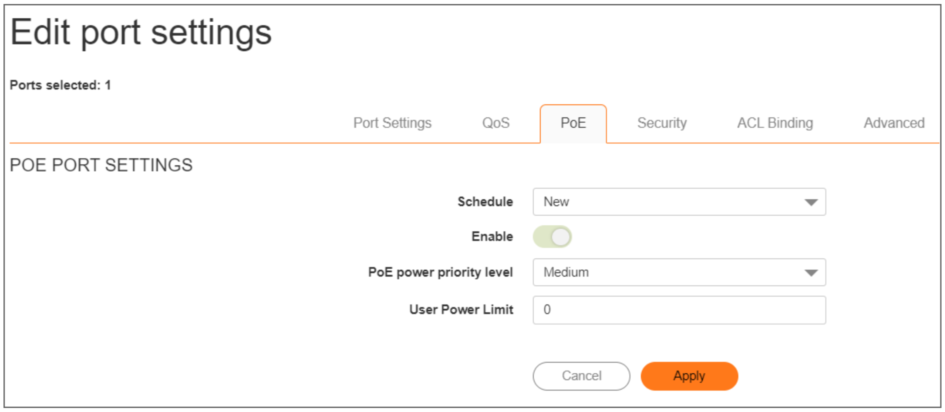
Click **Apply** to save the changes to the system.

PoE

The SonicWall PoE Switches supports Power over Ethernet as defined by the IEEE 802.3 af and at standards. Refer to Technical Specifications section for exact model and power sourcing details.

- SWS12-8POE :Ports 1-8 supports IEEE802.3 af . The maximum power budget is 55 Watts.
- SWS12-10FPOE :Ports 1-8 supports IEEE802.3 af and at. The maximum power budget is 130 Watts.
- SWS14-24FPOE : Ports 1-24 supports IEEE802.3 af and at. The maximum power budget is 410 Watts.
- SWS14-48FPOE : Ports 1-48 supports IEEE802.3 af and at. The maximum power budget is 730 Watts.

To access the page, edit a Port on a PoE switch and navigate to the **PoE** tab.



Edit port settings

Ports selected: 1

POE PORT SETTINGS

Schedule: New

Enable: ●

PoE power priority level: Medium

User Power Limit: 0

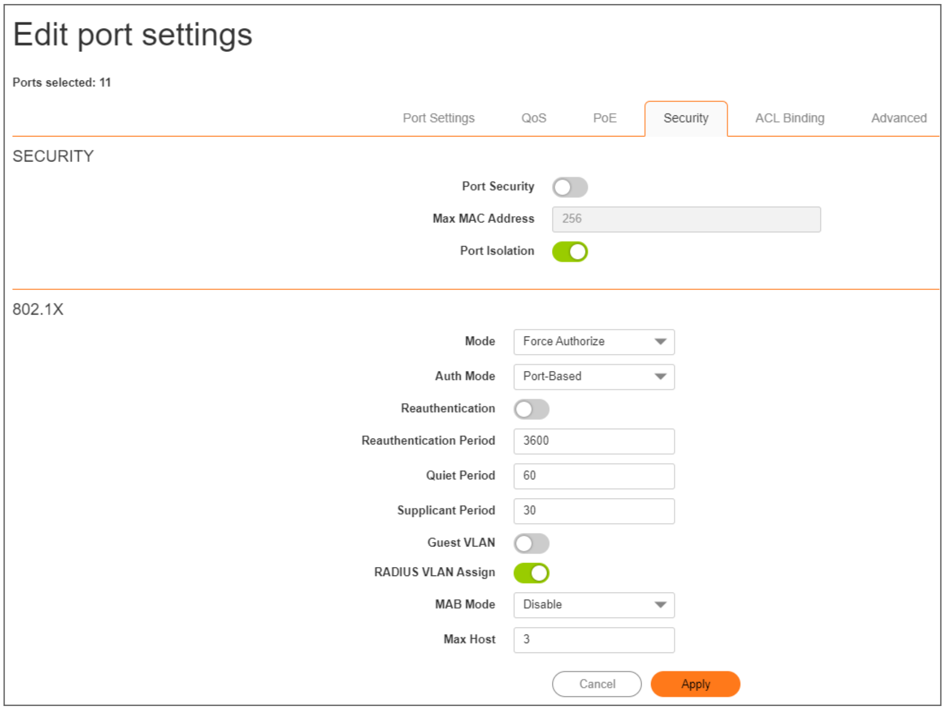
Settings	Description
Schedule	This setting displays all the schedule profiles created in **Time > Schedule**. ⓘ **NOTE:** When a Schedule profile is selected, the **Enable** option is not available and the power supply works as per the schedule.
Enable	This setting is available only when you want to configure PoE without schedule profiles. • If selected, this setting provides power to the connected device using the PoE module. • If unselected, this setting disables and halts the power supply to the connected device using the PoE module.
PoE power priority level	This setting establishes the power priority level for the port. When the port priority level is set to high, that port is prioritized to receive power. The following priority levels are available: • Low • Medium • High • Critical The default priority level is Low.
User Power Limit	This setting sets the maximum amount of power that can be delivered by a port. ⓘ **NOTE:** The User Power Limit can only be implemented when the Class value is set to User-Defined.

Click **Apply** to update the system settings.

Security

Network security can be increased by limiting access on a specific port to users with specific MAC addresses. Port Security prevents unauthorized device to the Switch prior to stopping auto-learning processing.

Max MAC Address	Enter the maximum number of MAC Addresses that can be learned on the port. The range is from 1-256.
Port Security	Select Enabled or Disabled for the port security feature for the selected port.



Edit port settings

Ports selected: 11

SECURITY

Port Security ○

Max MAC Address 256

Port Isolation ●

802.1X

Mode Force Authorize

Auth Mode Port-Based

Reauthentication ○

Reauthentication Period 3600

Quiet Period 60

Supplicant Period 30

Guest VLAN ○

RADIUS VLAN Assign ●

MAB Mode Disable

Max Host 3

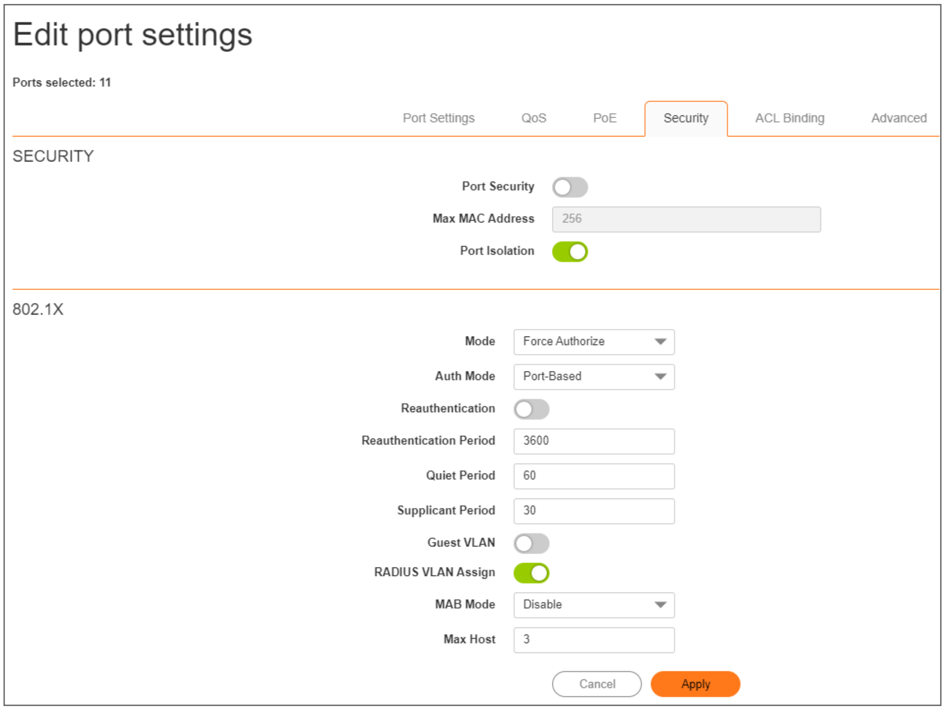
Click **Apply** to save the changes to the system.

802.1X

From here, you can configure the port settings as they relate to 802.1X. First, select the mode from the drop-down box. Next, choose whether to Enable or Disable reauthentication for the port. Enter the amount of time span that you wish to elapse for the Reauthentication period, Quiet Period, and Supplicant Period. After this, enter the Max number of times you wish for the Switch to retransmit and EAP request. Finally, choose whether you wish to Enable or Disable the VLAN ID.

Port Security	Displays the ports for which the 802.1X information is displayed.
Mode	Select the Auto or Force UnAuthorized or Force Authorized mode from the list.
Auth Mode	**Port-based**: Once a host passes the authentication, every host on the port gains access to the network. **MAC-based**: Allows one host or multiple hosts for authentication. Each host is authenticated individually.
Re-authentication	Select whether port reauthentication is Enabled or Disabled.
Re-authentication period	Enter the time span in which the selected port is reauthenticated. The default is 3600 seconds.
Quiet Period	Enter the number of the device that remains in the quiet state following a failed authentication exchange. The default is 60 seconds.

Supplicant Period	Enter the amount of time that lapses before an EAP request is resent to the supplicant. The default is 30 seconds.
Guest VLAN	Select whether guest VLAN ID is Enabled or Disabled.
RADIUS VLAN Assign	Displays the status of RADIUS VLAN Assignment.
MAB	MAB-mode: authenticate host with MAB only. Hybrid-mode: authenticate host with EAP. If host does not support EAP mode, it will fall back to MAB authentication mode. Disable: authenticate host with EAP only.
Max Host	The max number of hosts allowed to be authenticated. When the value is set 1 This value is only effective when using MAC-based mode. You can add up to 1 - 10 The default value is 3.



Edit port settings

Ports selected: 11

SECURITY

Port Security	○
Max MAC Address	256
Port Isolation	●

802.1X

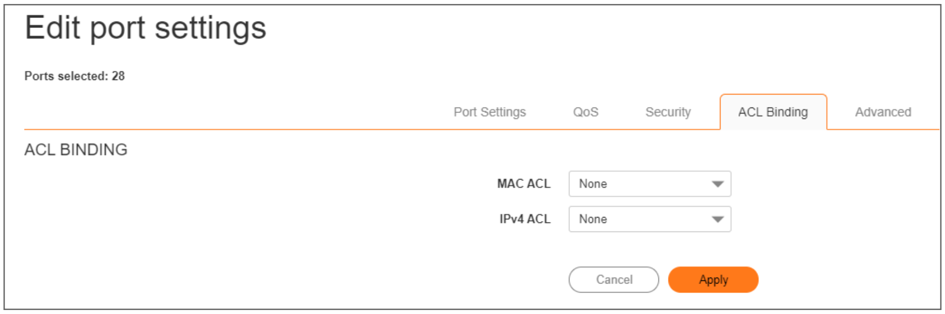
Mode	Force Authorize
Auth Mode	Port-Based
Reauthentication	○
Reauthentication Period	3600
Quiet Period	60
Supplicant Period	30
Guest VLAN	○
RADIUS VLAN Assign	●
MAB Mode	Disable
Max Host	3

ACL Binding

ACL Binding is a configuration setting that allows a user to choose a particular ACL for an ACL check. An ACL check is an additional check used to determine what operations a user can perform regarding particular items or item types.

Port	Select the port for which the ACLs are bound to.
MAC ACL	The ACL is MAC address based.

IPv4 ACL	The ACL is IP address based.



Edit port settings

Ports selected: 28

ACL BINDING

MAC ACL: None

IPv4 ACL: None

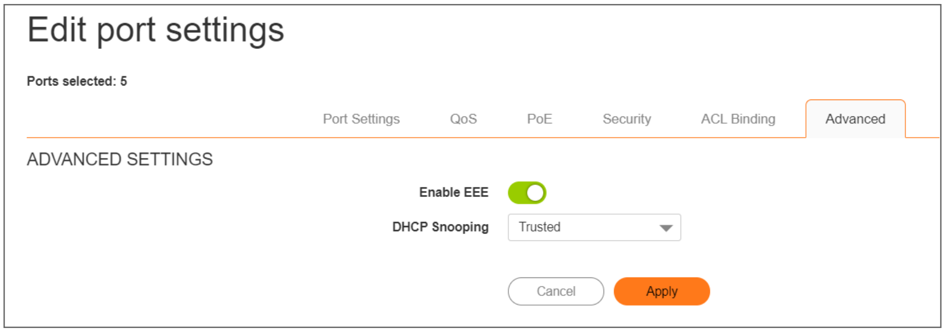
Advanced

Energy Efficient Ethernet (EEE), an Institute of Electrical and Electronics Engineers (IEEE) 802.3az standard, reduces the power consumption of physical layer devices during periods of low link utilization. EEE saves energy by allowing PHY non-essential circuits shut down when there is no traffic.

Network administrators have long focused on the energy efficiency of their infrastructure, and the SonicWall Layer 2 Switch complies with the IEEE's Energy-Efficient Ethernet (EEE) standard to give you even more control. The EEE- compliant Switch offers users the ability to utilize power that Ethernet links use only during data transmission. Lower Power Idle (LPI) is the method for achieving the power saving during Ethernet idle time.

Use the EEE Configuration page to configure Energy Efficient Ethernet.

Enable EEE	Enable or Disable EEE for the specified port.
DHCP Snooping	Select one of the following: • Trusted- Server packets received on trusted ports are forwarded. • Untrusted- Server packets (DHCP offer packets) received on untrusted ports are dropped.



Edit port settings

Ports selected: 5

ADVANCED SETTINGS

Enable EEE: ●

DHCP Snooping: Trusted

Click **Apply** to update the system settings.

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.

Network Loops

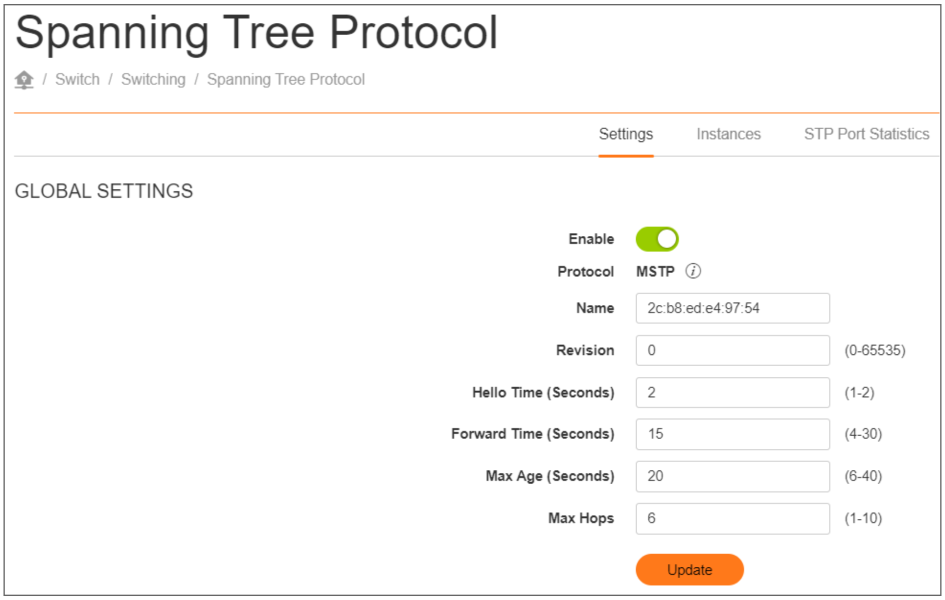
Loops occur when alternate routes exist between hosts. Loops in an extended network can cause the Switch to forward traffic indefinitely, resulting in increased traffic and reducing network efficiency. Once the STP is enabled and configured, primary links are established and duplicated links are blocked automatically. The reactivation of the blocked links is also accomplished automatically. STP provides a tree topology and other Spanning tree versions supported include STP, Multiple Spanning Tree Protocol (MSTP), and Rapid Spanning Tree Protocol (RSTP). Please note that only one spanning tree can be active on the Switch at a time. The default setting is: MSTP.

Multiple Spanning Tree Protocol (MSTP) defined in IEEE 802.1s, enables multiple VLANs to be mapped to reduce the number of spanning-tree instances needed to support a large number of VLANs. If there is only one VLAN in the network, a single STP works appropriately.

If the network contains more than one VLAN however, the logical network configured by a single STP would work, but it becomes more efficient to use the alternate paths available by using an alternate spanning tree for different VLANs or groups of VLANs. MSTP (which is based on RSTP for fast convergence) is designed to support independent spanning trees based on VLAN groups. MSTP provides multiple forwarding paths for data traffic and enables load balancing.

STP and RSTP prevent loops from forming by ensuring that only one path exists between the end nodes in your network. RSTP is designed as a general replacement for the slower, legacy STP. RSTP is also incorporated into MSTP. With STP, convergence can take up to a minute to complete in a larger network. This can result in the loss of communication between various parts of the network during the convergence process so STP can subsequently can lose data packets during transmission.

RSTP on the other hand is much faster than STP. It can complete a convergence in seconds, so it greatly diminishes the possible impact the process can have on your network compared to STP. RSTP reduces the number of state changes before active ports start learning, pre- defining an alternate route that can be used when a node or port fails and retain the forwarding database for ports insensitive to changes in the tree structure when reconfiguration occurs.



Enable	●	
Protocol	MSTP	
Name	2c:b8:ed:e4:97:54	
Revision	0	(0-65535)
Hello Time (Seconds)	2	(1-2)
Forward Time (Seconds)	15	(4-30)
Max Age (Seconds)	20	(6-40)
Max Hops	6	(1-10)

Select whether to enable or disable the Spanning Tree function for the Switch and click **Update** to update the system settings.

Global Settings

Global settings are available under Spanning Tree Protocol Settings Tab. The Root Bridge serves as an administrative point for all Spanning Tree calculations to determine which redundant links to block in order to prevent network loops.

All other decisions in a spanning tree network, such as ports being blocked and ports being put in a forwarding mode, are made regarding a root bridge. The root bridge is the “root” of the constructed “tree” within a spanning tree network. Thus, the root bridge is the bridge with the lowest bridge ID in the spanning tree network. The bridge

ID includes two parts; the bridge priority (2 bytes) and the bridge MAC address (6 bytes). The 802.1d default bridge priority is: 32768. STP devices exchange Bridge Protocol Data Units (BPDUs) periodically. All bridges “listen” for Hello BPDUs (Bridge Protocol Data Units) transmitted from the root bridge. If a bridge does not get a Hello BPDU after a predefined interval (called the Maximum Age), the bridge assumes that the link to the root bridge is down. The bridge then initiates negotiations with other bridges to reconfigure the network to re-establish a valid network topology.

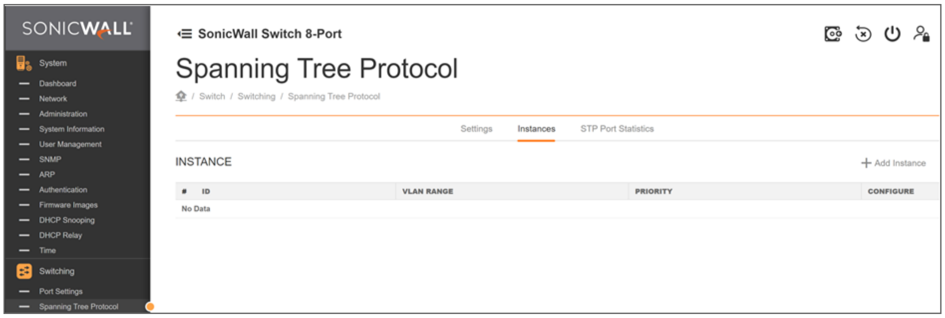
Name	This name uniquely identifies the MSTI (Multiple Spanning Tree Instance). Enter a descriptive name (up to 32 characters) for an MST region. The default is the MAC address name of the device running MSTP.
Revision	Displays the Spanning Tree Configuration Revision. Default revision is 0. ⓘ | **NOTE:** Decimal values cannot be configured.
Hello Time	Displays the Switch Hello Time. This is the amount of time between each bridge protocol data unit sent on a port. The default is 2 seconds.
Forward Time	Displays the Switch Forward Delay Time. This is the time (in seconds) the Root Switch will wait before changing states (called listening to learning).
Max Age	Displays the bridge Switch Maximum Age Time. This is the amount of time a bridge waits before sending a configuration message. The default is 20 seconds. ⓘ | **NOTE:** Ensure to calculate the Max Age using 2*(ForwardDelay - 1)>=MaxAge >= 2*(Hello Time + 1).
Max Hops	Displays the BPDU Hop count. The max hop count is the maximum number of hops the BPDU can traverse before getting discarded and also before the information held for a port is aged out. The default count is 10.

MST Instance Settings

Multiple Spanning Tree Protocol, or MSTP enables the grouping of multiple VLANs with the same topology requirements into one Multiple Spanning Tree Instance (MSTI). MSTP then builds an Internal Spanning Tree (IST) for the region containing commonly configured MSTP bridges. Instances are not supported in STP or RSTP. Instead, they have the same spanning tree in common within the VLAN. MSTP provides the capability to logically divide a Layer 2 network into regions. Every region can contain multiple instances of spanning trees. In MSTP, all of the interconnected bridges that have the same MSTP configuration comprise an MST region.

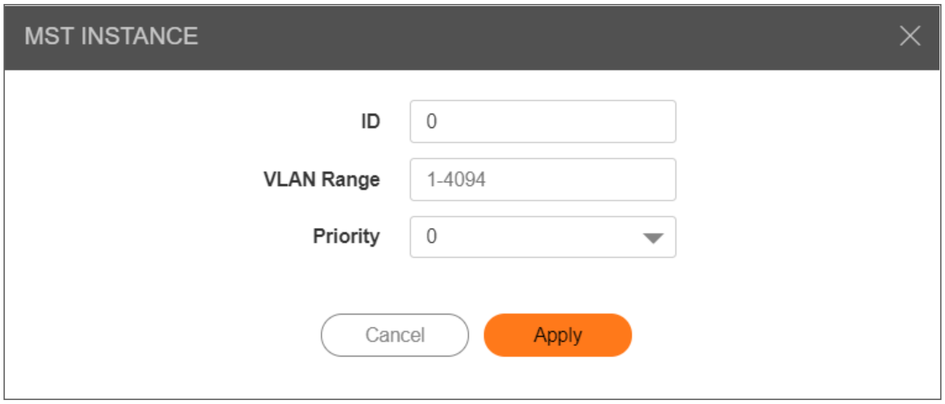
A Common Spanning Tree (CST) interconnects all adjacent MST Regions and acts as a virtual bridge node for communications between STP or RSTP nodes in the global network. MSTP connects all bridges and LAN segments with a single Common and Internal Spanning Tree (CIST). The CIST is formed as a result of the running spanning tree algorithm between Switches that support STP, RSTP, and MSTP protocols. Once you specify the VLANs you wish to include in a Multiple Spanning Tree Instance (MSTI), the protocol will automatically build an MSTI tree to maintain connectivity among each of the VLANs. MSTP maintains contact with the global network because each instance is treated as an RSTP node in the Common Spanning Tree (CST).

Click **Add Instance** to configure the MST settings. Next, enter information for the VLAN Range and choose the priority you wish to use from the drop-down list.



INSTANCE

#	ID	VLAN RANGE	PRIORITY	CONFIGURE
No Data				



ID: 0

VLAN Range: 1-4094

Priority: 0

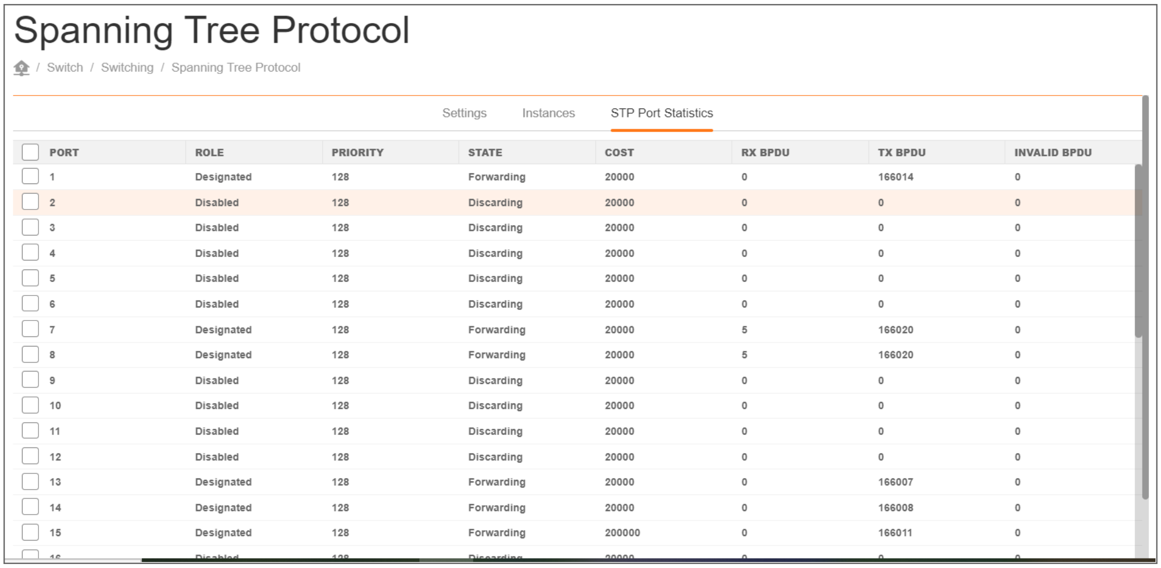
ID	Displays the ID of the MST group that is created. A maximum of 15 groups can be set for the Switch.
VLAN Range	Enter the VLAN ID range from for the configured VLANs to associate with the MST ID. The VLAN ID number range is from 1 to 4094.
Priority	Select the bridge priority value for the MST. When 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.

- Click **Apply** to accept the changes or the **Cancel** to discard them.

ⓘ | **NOTE:** You cannot create an MST instance with an already created VLAN ID.

STP Port Statistics

The Port Statistics section displays a summary of the currently used STP, and port details such as port number, port role, port state and port status.



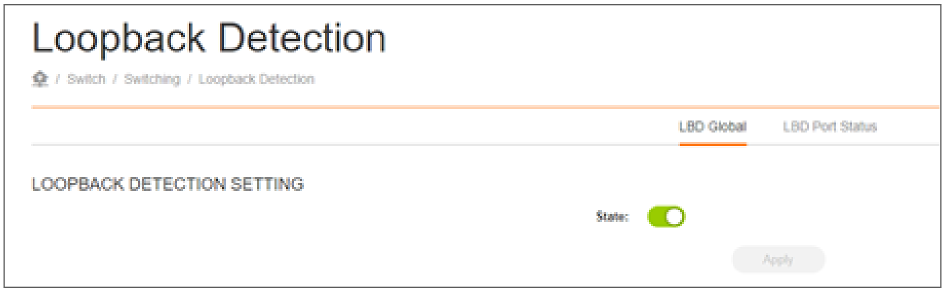
☐ PORT	ROLE	PRIORITY	STATE	COST	RX BPDU	TX BPDU	INVALID BPDU
☐ 1	Designated	128	Forwarding	20000	0	166014	0
☐ 2	Disabled	128	Discarding	20000	0	0	0
☐ 3	Disabled	128	Discarding	20000	0	0	0
☐ 4	Disabled	128	Discarding	20000	0	0	0
☐ 5	Disabled	128	Discarding	20000	0	0	0
☐ 6	Disabled	128	Discarding	20000	0	0	0
☐ 7	Designated	128	Forwarding	20000	5	166020	0
☐ 8	Designated	128	Forwarding	20000	5	166020	0
☐ 9	Disabled	128	Discarding	20000	0	0	0
☐ 10	Disabled	128	Discarding	20000	0	0	0
☐ 11	Disabled	128	Discarding	20000	0	0	0
☐ 12	Disabled	128	Discarding	20000	0	0	0
☐ 13	Designated	128	Forwarding	20000	0	166007	0
☐ 14	Designated	128	Forwarding	20000	0	166008	0
☐ 15	Designated	128	Forwarding	200000	0	166011	0
☐ 16	Disabled	128	Discarding	20000	0	0	0

Port	Displays the port for which statistics are displayed.
Role	Displays the designated (connected port link status) or disabled ports (no connection).
Priority	Displays the priority value of the port (0-240 with multiples of 16). Default priority is 128.
State	Displays the forwarding or discarding or root status of the port.
Cost	Displays the port’s path cost value that contributes to the path cost of paths containing this particular port (0-200000000).
RX BPDU	Displays the port received BPDUs.
TX BPDU	Displays the port transmitted BPDUs.
Invalid BPDU	Displays the port invalid BPDUs received.

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.

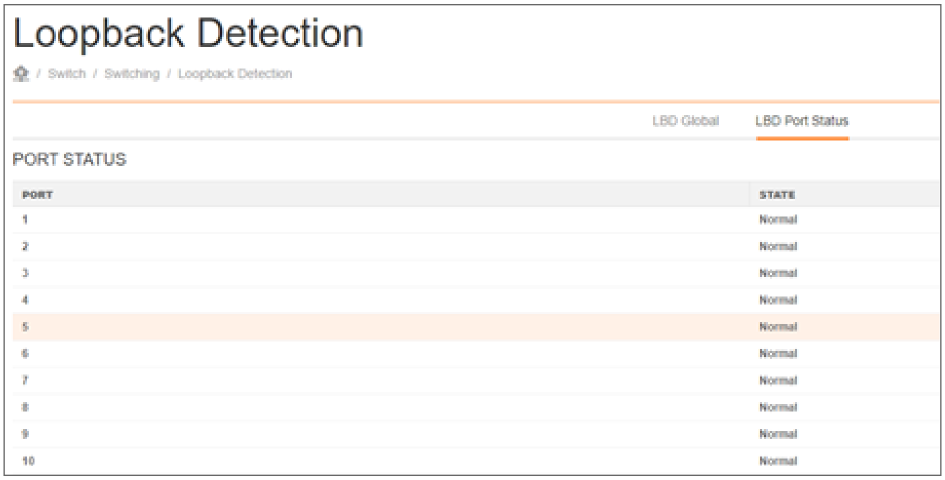
Settings	Select whether to enable or disable the Loop back detection on the Switch.



LOOPBACK DETECTION SETTING

State: ●

State	Display the Port status is normal or blocked by LBD function.



PORT STATUS

PORT	STATE
1	Normal
2	Normal
3	Normal
4	Normal
5	Normal
6	Normal
7	Normal
8	Normal
9	Normal
10	Normal

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.

When you aggregate ports, the ports and LAG must fulfill the following conditions:

- All ports within a LAG must be the same media/ format type.
- A VLAN is not configured on the port.
- The port is not assigned to another LAG.
- The Auto-negotiation mode is not configured on the port.
- The port is in full-duplex mode.
- All ports in the LAG have the same ingress filtering and tagged modes.
- All ports in the LAG have the same back pressure and flow control modes.
- All ports in the LAG have the same priority.
- All ports in the LAG have the same transceiver type

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.

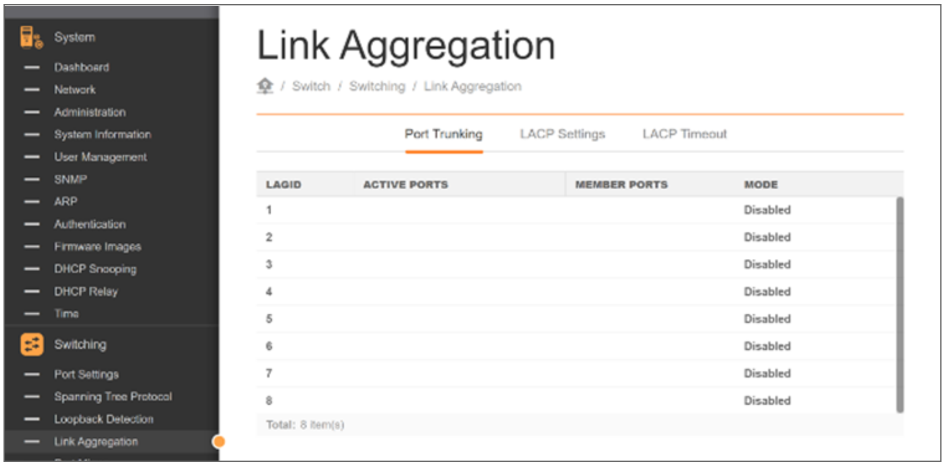
Port Trunking

Port Trunking allows you to assign physical links to one logical link that functions as a single, higher-speed link, providing dramatically increased bandwidth. Use Port Trunking to bundle multiple connections and use the combined bandwidth as if it were a single larger "pipe".

ⓘ | **IMPORTANT:** You must enable Trunk Mode before you can add a port to a trunk group.

To access the page, navigate to **Switching > Link Aggregation > Port Trunking**.

LAG ID	Displays the number of the given trunk group. You can utilize up to 8 link aggregation groups and each group consisting up to 8 ports on the Switch.
Active Ports	Displays the active participating members of the trunk group
Member Port	Select the ports you wish to add into the trunk group. Up to eight ports per group can be assigned.
Mode	LACP allows for the automatic detection of links in a Port Trunking Group when connected to a LACP-compliant Switch. You will need to ensure both the Switch and device connected to are the same mode in order for them to function, otherwise they will not work. Static configuration is used when connecting to a Switch that does not support LACP. • Static – The Link Aggregation is configured manually for specified trunk group. • LACP – The Link Aggregation is configured dynamically for specified trunk group.

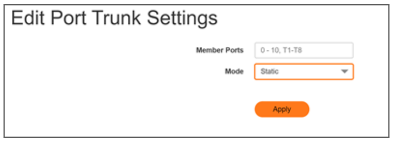


Link Aggregation

/ Switch / Switching / Link Aggregation

LAGID	ACTIVE PORTS	MEMBER PORTS	MODE
1			Disabled
2			Disabled
3			Disabled
4			Disabled
5			Disabled
6			Disabled
7			Disabled
8			Disabled

Total: 8 item(s)



Edit Port Trunk Settings

Member Ports: 0 - 10, T1-T8

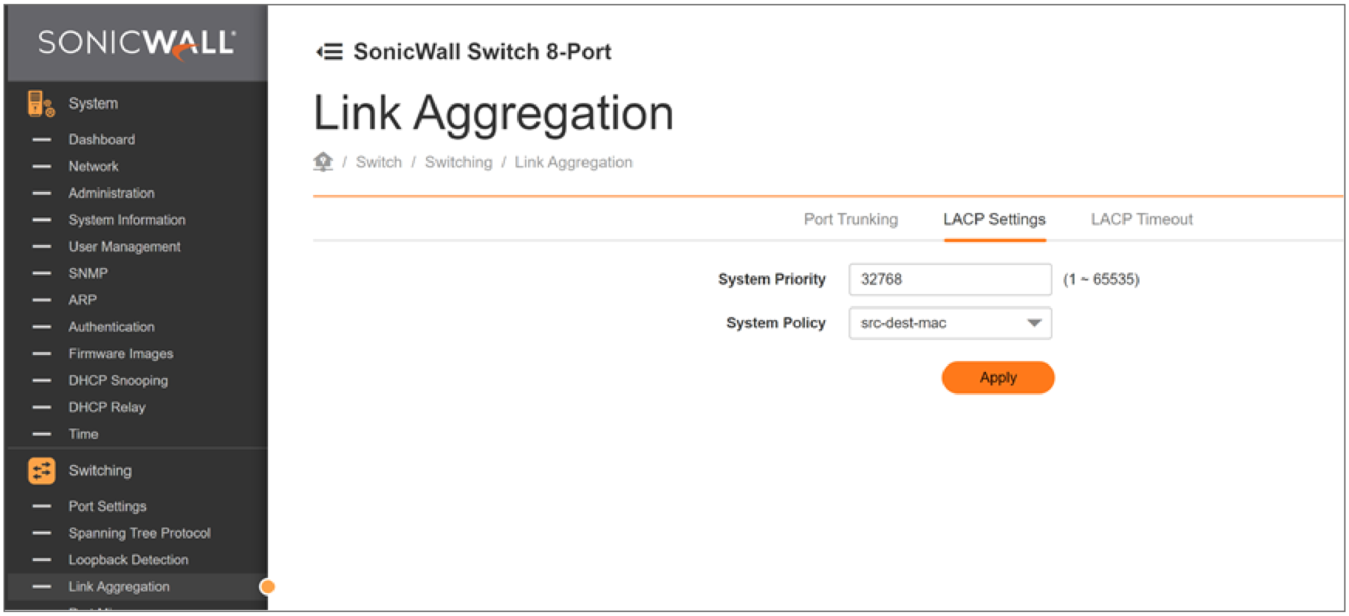
Mode: Static

Click **Apply** to accept the changes or **Cancel** to discard them.

Link Aggregation Control Protocol Settings

Assign a system priority to run with Link Aggregation Control Protocol (LACP) and is become for a backup link if a link goes down. The lowest system priority is allowed to make decisions about which ports it is actively participating in case a link goes down. If two or more ports have the same LACP port priority, the port with the lowest physical port number will be selected as the backup port. If a LAG already exists with the maximum number of allowed port members, and LACP is subsequently enabled on another port using a higher priority than an existing member, the newly configured port will replace the existing port member that has a lower priority. A smaller number indicates a higher priority level. The range is from 0-65535 and default is: 32768.

System Priority	Enter the LACP priority value to the system. The default is 32768 and the range is from 1-65535.
System Policy	Enter the LACP load distribution algorithm. The default is src-dest-mac.



System Priority: 32768 (1 ~ 65535)

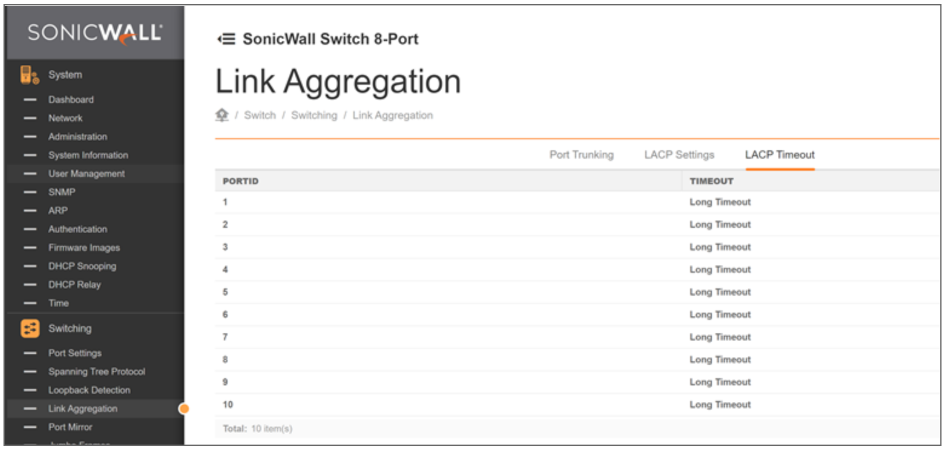
System Policy: src-dest-mac

Click **Apply** to update the system settings.

Link Aggregation Control Protocol Timeout

Link Aggregation Control Protocol (LACP) allows the exchange of information with regard to the link aggregation between two members of aggregation. The LACP Time Out value is measured in a periodic interval. Check first whether the port in the trunk group is up. When the interval expires, it will be removed from the trunk. Set a Short Timeout (one second) for busy trunked links to ensure that disabled ports are removed from the trunk group as soon as possible. The default value for LACP time out is: Long Timeout.

Timeout	Select the administrative LACP timeout. Long - Long timeout value. Short - Short timeout value.
Long	The LACP PDU will be sent for every 30 seconds, and the LACP timeout value is 90 seconds.
Short	The LACP PDU will be sent every second. The timeout value is 3 seconds.



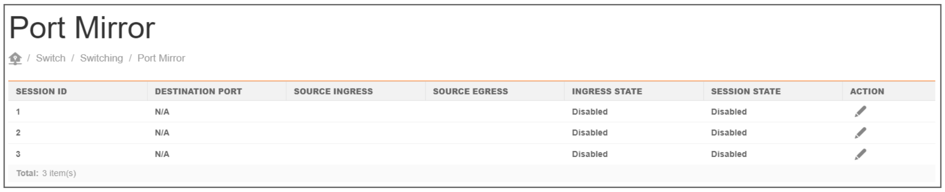
Link Aggregation

PORTID	TIMEOUT
1	Long Timeout
2	Long Timeout
3	Long Timeout
4	Long Timeout
5	Long Timeout
6	Long Timeout
7	Long Timeout
8	Long Timeout
9	Long Timeout
10	Long Timeout

Total: 10 item(s)

Port Mirror

Port Mirroring allows the sending of a copy of network packets seen on one or more switch ports to another switch port called the mirror port. By connecting to the mirror port, you can monitor traffic passing through the mirrored ports.



Port Mirror

SESSION ID	DESTINATION PORT	SOURCE INGRESS	SOURCE EGRESS	INGRESS STATE	SESSION STATE	ACTION
1	N/A			Disabled	Disabled	✎
2	N/A			Disabled	Disabled	✎
3	N/A			Disabled	Disabled	✎

Total: 3 item(s)

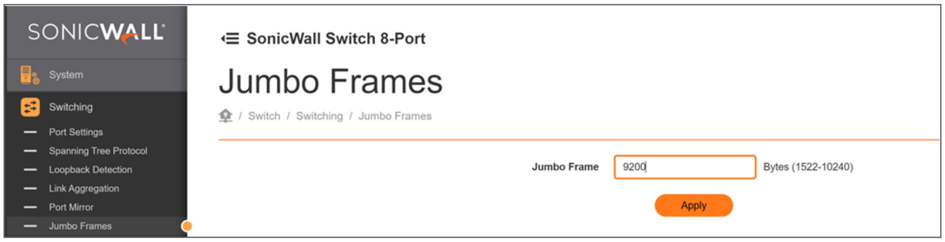
Session ID	Displays the three sessions.
Destination Port	Displays the destination port to which the traffic is monitored.
Source Ingress	Displays the port for which incoming traffic is mirrored as part of a port mirroring configuration.
Source Egress	Displays the port for which outgoing traffic is mirrored as part of a port mirroring configuration.
Ingress State	Displays the state, either enable or disable of the ingress traffic
Session State	Displays the session state, either the port mirror is enabled or disabled.
Action	Allows to edit the port mirror entries like session state, destination port, source TX and RX port and ingress state.

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.



Jumbo Frame 9200 Bytes (1522-10240)

Click **Apply** to update the system settings

MAC Address Table

The MAC address table contains address information that the Switch uses to forward traffic between the inbound and outbound ports. All MAC addresses in the address table are associated with one or more ports. When the Switch receives traffic on a port, it searches the Ethernet switching table for the MAC address of the destination. If the MAC address is not found, the traffic is flooded out all of the other ports associated with the VLAN. All of the MAC address that the Switch learns by monitoring traffic are stored in the Dynamic address. A Static address allows you to manually enter a MAC address to configure a specific port and VLAN.

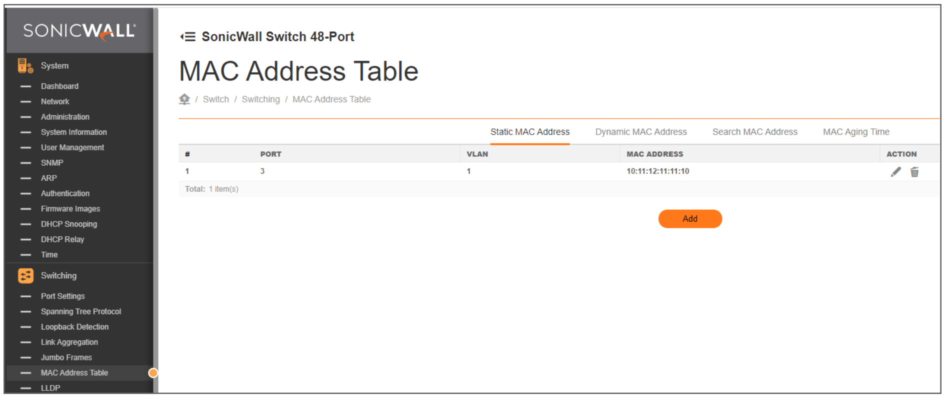
Static MAC Address

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.

To access the page, click **Static MAC Address** under the Switching tab.

Index	Displays the index for the Static MAC Address table.

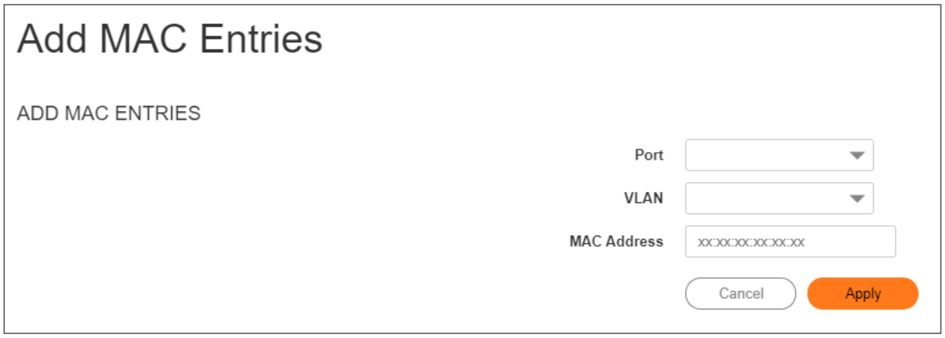
Port	Select the port where the MAC address entered in the previous field will be automatically forwarded.
VLAN	Enter the VLAN ID on which the IGMP snooping querier is administratively enabled and for which the VLAN exists in the VLAN database.
MAC Address	Enter a unicast MAC address for which the switch has forwarding or filtering information.



MAC Address Table

#	PORT	VLAN	MAC ADDRESS	ACTION
1	3	1	10:11:12:11:11:10	

Total: 1 item(s)



Add MAC Entries

ADD MAC ENTRIES

Port

VLAN

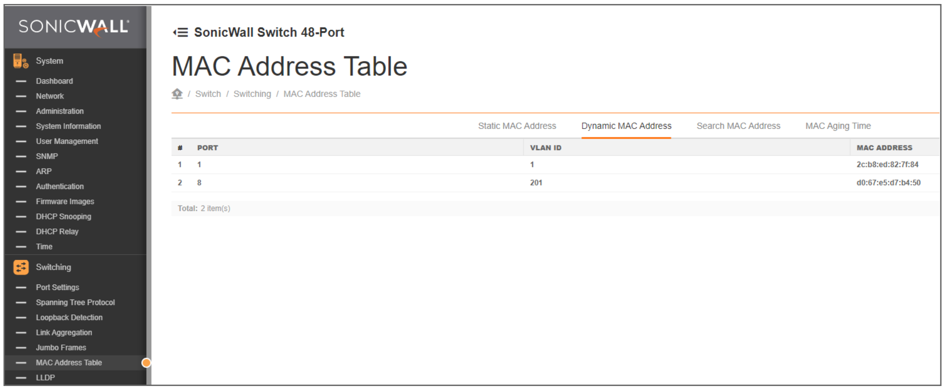
MAC Address xx:xx:xx:xx:xx:xx

Click **Apply** to accept the changes or **Cancel** to discard them.

Dynamic MAC Address

The Switch will automatically learn the device’s MAC address and store it to the Dynamic MAC address table. If there is no packet received from the device within the aging time, the Switch adopts an aging mechanism for updating the tables from which MAC address entries will be removed from related network devices. The Dynamic MAC Address Table shows the MAC addresses and their associated VLANs learned on the selected port.

Port	Select the port to which the entry refers.
VLAN ID	Displays the VLAN ID for the specified MAC address
MAC Address	Displays the MAC addresses that the Switch learned from a specific port.



#	PORT	VLAN ID	MAC ADDRESS
1	1	1	2c:b8:ed:82:7f:84
2	8	201	d0:67:e5:d7:b4:50

Total: 2 item(s)

Link Layer Discovery Protocol

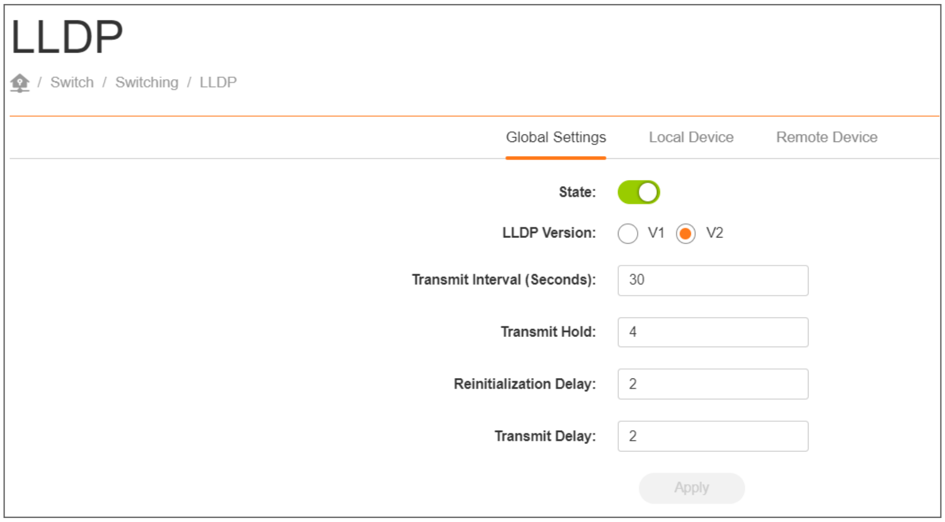
Link Layer Discovery Protocol (LLDP) is the IEEE 802.1AB standard for Switches to advertise their identity, major capabilities, and neighbors on the 802 LAN. LLDP allows users to views the discovered information to identify system topology and detect faulty configurations on the LAN. LLDP is essentially 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.

Global Settings

Select whether to Enable or Disable the LLDP feature on the Switch. Next, enter the Transmission interval, Holdtime Multiplier, Reinitialization Delay parameter, and the Transmit Delay parameter. When finished, click **Apply** to update the system settings.

State	Select Enabled or Disabled to activate LLDP for the Switch.
LLDP Version	Select the required LLDP version. By deafult V2 is selected.
Transmission Interval	Enter the interval at which LLDP advertisement updates are sent. The default value is 30. The range is from 5-32767.
Transmit Hold	Enter the amount of 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.
Reinitialization Delay	Enter the amount of time of delay before reinitializing LLDP. The default is 2. The range is from 1-10.
Transmit Delay	Enter the amount of time that passes between successive LLDP frame transmissions. The default is 2 seconds. The range is 1-8191 seconds.



LLDP

State: On

LLDP Version: ○ V1 ● V2

Transmit Interval (Seconds): 30

Transmit Hold: 4

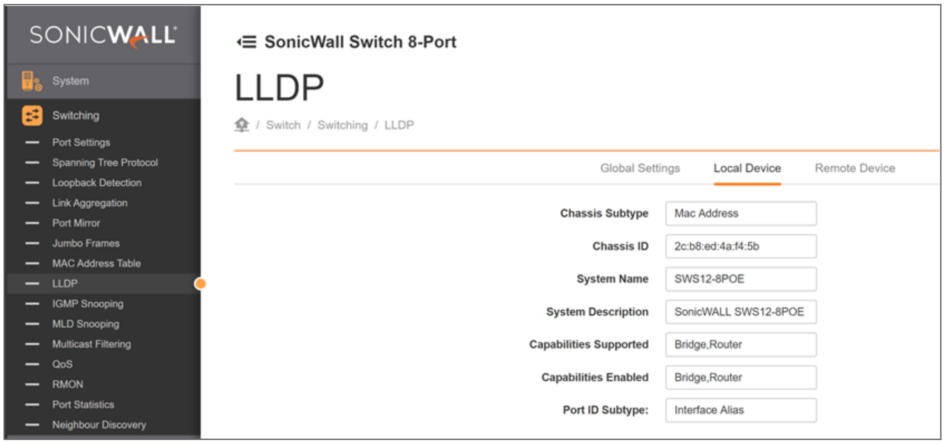
Reinitialization Delay: 2

Transmit Delay: 2

Local Device

LLDP devices must support chassis and port ID advertisement, as well as the system name, system ID, system description, and system capability advertisements. Here, you can view detailed LLDP information for the SonicWall Switch.

Chassis Subtype	Displays the chassis ID type.
Chassis ID	Displays the chassis ID of the device transmitting the LLDP frame.
System Name	Displays the administratively assigned device name.
System Description	Describes the device.
Capabilities Supported	Describes the device functions.
Capabilities Enabled	Describes the device functions.
Port ID Subtype	Displays the port ID type.



SonicWall Switch 8-Port

LLDP

Chassis Subtype: Mac Address

Chassis ID: 2c:b8:ed:4a:f4:5b

System Name: SWS12-8POE

System Description: SonicWALL SWS12-8POE

Capabilities Supported: Bridge,Router

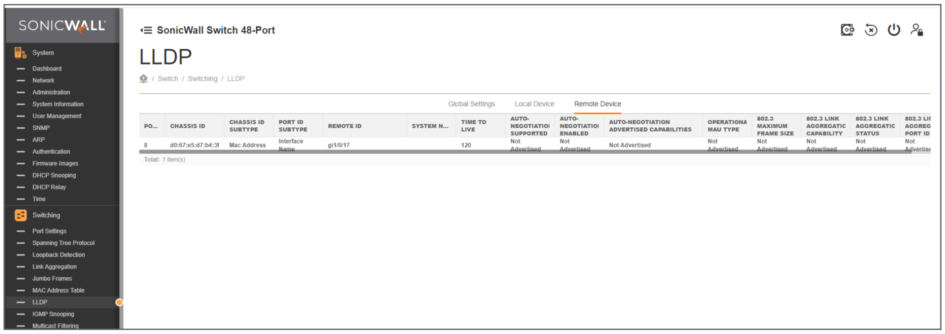
Capabilities Enabled: Bridge,Router

Port ID Subtype: Interface Alias

Remote Device

LLDP devices must support chassis and port ID advertisement, as well as the system name, system ID, system description, and system capability advertisements. From here you can viewing detailed LLDP Information for the remote Switch. To scroll, click on the arrow at the top right of the screen.

Port	Displays the port.
Chassis ID Subtype	Displays the chassis ID type.
Chassis ID	Displays the chassis ID of the device that is transmitting the LLDP frame.
Port ID Subtype	Displays the port ID type.
Remote ID	Displays the Remote ID.
System Name	Displays the administratively assigned device name.
Time to Live	Displays the time.
Auto-Negotiation Supported	Displays state for the Auto- Negotiation Supported.
Auto-Negotiation Enabled	Displays state for the Auto- Negotiation Enabled.
Auto-Negotiation Advertised Capabilities	Displays the type of Auto- Negotiation Advertised Capabilities.
Operational MAU Type	Displays the type of MAU.
802.3 Maximum Frame Size	Displays the size of 802.3 Maximum Frame.
802.3 Link Aggregation Capabilities	Displays the 802.3 Link Aggregation Capabilities.
802.3 Link Aggregation Status	Displays the status of 802.3 Link Aggregation.
802.3 Link Aggregation Port ID	Displays the port ID of 802.3 Link Aggregation.



PO...	CHASSIS ID	CHASSIS ID SUBTYPE	PORT ID SUBTYPE	REMOTE ID	SYSTEM N...	TIME TO LIVE	AUTO-NEGOTIATIOI SUPPORTED	AUTO-NEGOTIATIOI ENABLED	AUTO-NEGOTIATION ADVERTISED CAPABILITIES	OPERATIONA MAU TYPE	802.3 MAXIMUM FRAME SIZE	802.3 LINK AGGREGATIC CAPABILITY	802.3 LINK AGGREGATIC STATUS	802.3 LII AGGREG PORT ID
8	d0:67:e5:d7:b4:3f	Mac Address	Interface Name	gi1/0/17		120	Not Advertised	Not Advertised	Not Advertised	Not Advertised	Not Advertised	Not Advertised	Not Advertised	Not Advertise

Total: 1 item(s)

IGMP Snooping

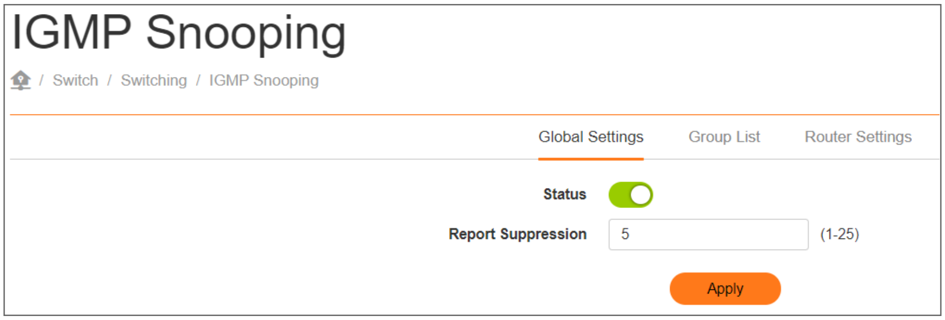
Internet Group Management Protocol (IGMP) Snooping allows a Switch to forward multicast traffic intelligently. Multicasting is used to support real-time applications such as videoconferencing or streaming audio. A multicast server does not have to establish a separate connection with each client. It 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.

IGMPv1	Defined in RFC 1112. An explicit join message is sent to the Switch, but a timeout is used to determine when hosts leave a group.
IGMPv2	Defined in RFC 2236. Adds an explicit leave message to the join message so that Switch can more easily determine when a group has no interested listeners on a LAN.
IGMPv3	Defined in RFC 3376. Support for a single source of content for a multicast group.


IGMP Snooping

/ Switch / Switching / IGMP Snooping

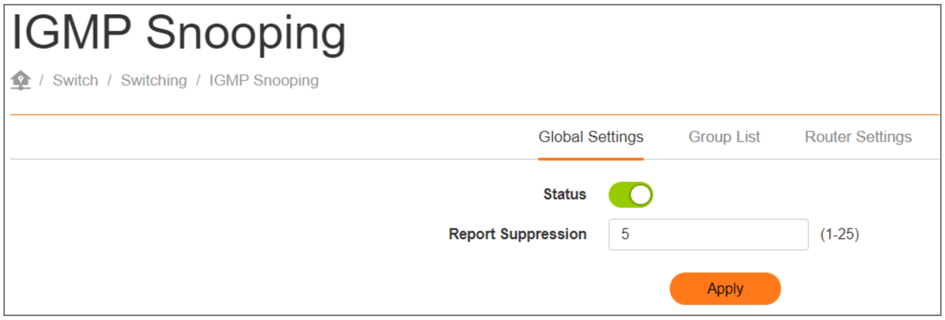
Status: on

Report Suppression: 5 (1-25)

Global Settings

Click to enable or disable the IGMP Snooping feature for the Switch.

Status	Select to Enable or Disable IGMP Snooping on the Switch. The switch snoops all IGMP packets it receives to determine which segments should receive packets directed to the group address when enabled.
Report Suppression	The Report Suppression feature limits the amount of membership reports the member sends to multicast capable routers.



IGMP Snooping

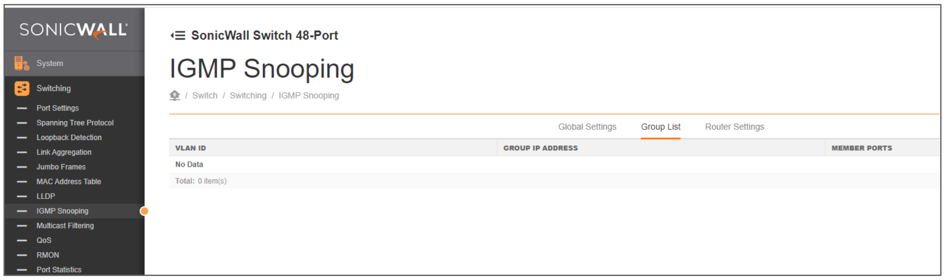
Status: on

Report Suppression: 5 (1-25)

Click **Apply** to update the system settings.

Group List

The Group List displays VLAN ID, Group IP Address, and Members Port in the IGMP Snooping List.



SonicWall Switch 48-Port

IGMP Snooping

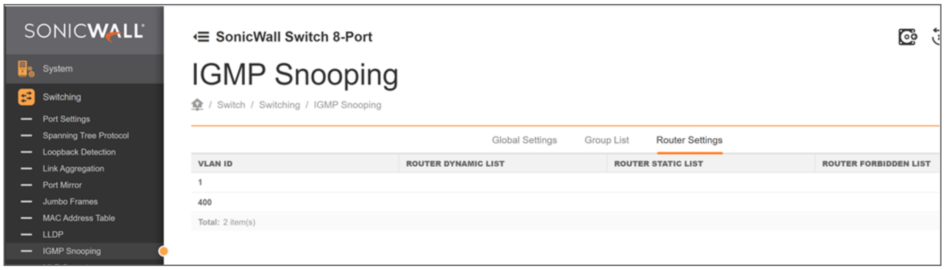
VLAN ID	GROUP IP ADDRESS	MEMBER PORTS
No Data		

Total: 0 item(s)

Router Settings

The Router Settings shows the learned multicast router attached port if the port is active and a member of the VLAN. Select the VLAN ID you would like to configure and enter the Static and Forbidden ports for the specified VLAN IDs. All IGMP packets snooped by the Switch will be forwarded to the multicast router reachable from the port.

VLAN ID	Displays the VLAN ID.
Router Dynamic List	Displays router ports that have been dynamically configured.
Router Forbidden List	Designates a range of ports as being disconnected to multicast-enabled routers. Ensures that the forbidden router port will not propagate routing packets out.
Router Static list	Designates a range of ports as being connected to multicast- enabled routers. Ensures that the all packets will reach the multicast- enabled router



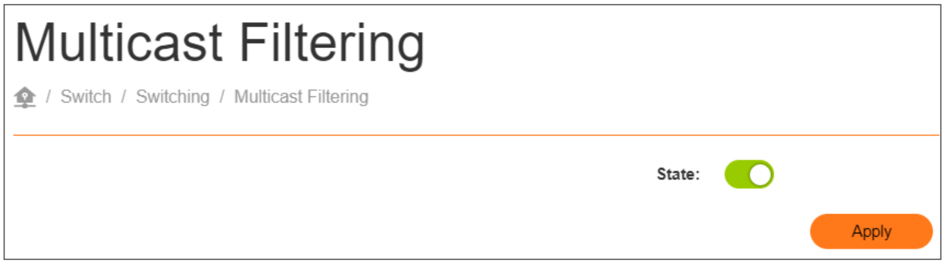
VLAN ID	ROUTER DYNAMIC LIST	ROUTER STATIC LIST	ROUTER FORBIDDEN LIST
1			
400			

Total: 2 item(s)

Click **Apply** to accept the changes or **Cancel** to discard them.

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.



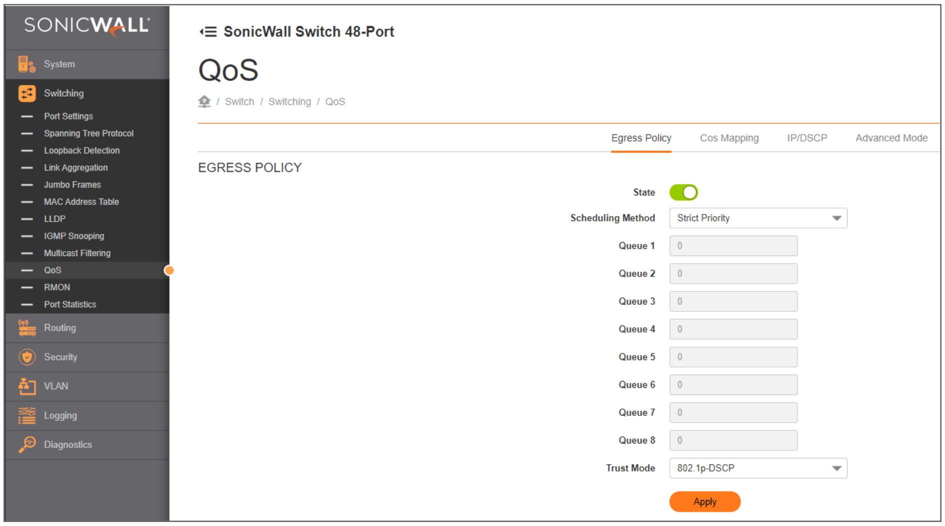
Select whether to enable or disable the Multicast Filtering function.

Quality of Service

Quality of Service (QoS) provides the ability to implement priority queuing within a network. QoS enables traffic to be prioritized, while excessive broadcast and multicast traffic to be avoided. Traffics such as Voice and Video streaming which requires a minimal delay can be assigned to a high priority queue, while other traffic can be assigned to a lower priority queue resulting in uninterrupted actions.

State	Select whether QoS is enabled or disabled on the switch.
Scheduling Method	Selects the Strict Priority or WRR to specify the traffic scheduling method. • Strict Priority – Specifies traffic scheduling based strictly on the queue priority. • WRR – Use the Weighted Round-Robin (WRR) algorithm to handle packets in priority classes of service. It assigns WRR weights to queues.

Trust Mode	Select which packet fields to use for classifying packets entering the Switch. • DSCP – Classify traffic based on the DSCP (Differentiated Services Code Point) tag value. • 1p–Classify traffic based on the 802.1p. The eight priority tags that are specified in IEEE802.1p are from 1 to 8.



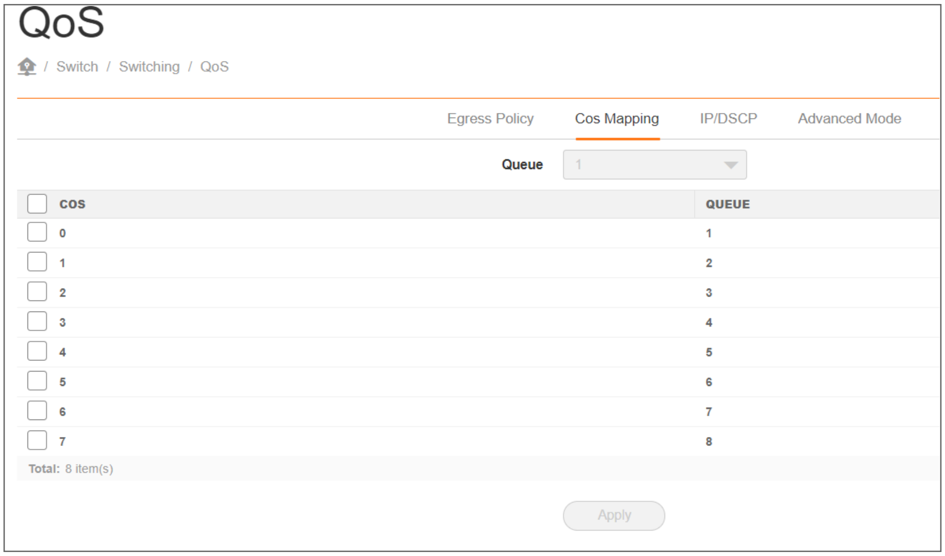
EGRESS POLICY

State	On
Scheduling Method	Strict Priority
Queue 1	0
Queue 2	0
Queue 3	0
Queue 4	0
Queue 5	0
Queue 6	0
Queue 7	0
Queue 8	0
Trust Mode	802.1p-DSCP

Class of Service Mapping

Use the Class of Service (CoS) Mapping feature to specify which internal traffic class to map to the corresponding CoS value. CoS allows you to specify which data packets have greater precedence when traffic is buffered due to congestion.

CoS (Class of Service)	Displays the CoS priority tag values, where 0 is the lowest and 7 is the highest.
Queue	Check the CoS priority tag box and select the Queue values for each CoS value in the provided fields. Eight traffic priority queues are supported and the field values are from 1-8, where one is the lowest priority and eight is the highest priority.



QoS

□ COS	QUEUE
□ 0	1
□ 1	2
□ 2	3
□ 3	4
□ 4	5
□ 5	6
□ 6	7
□ 7	8

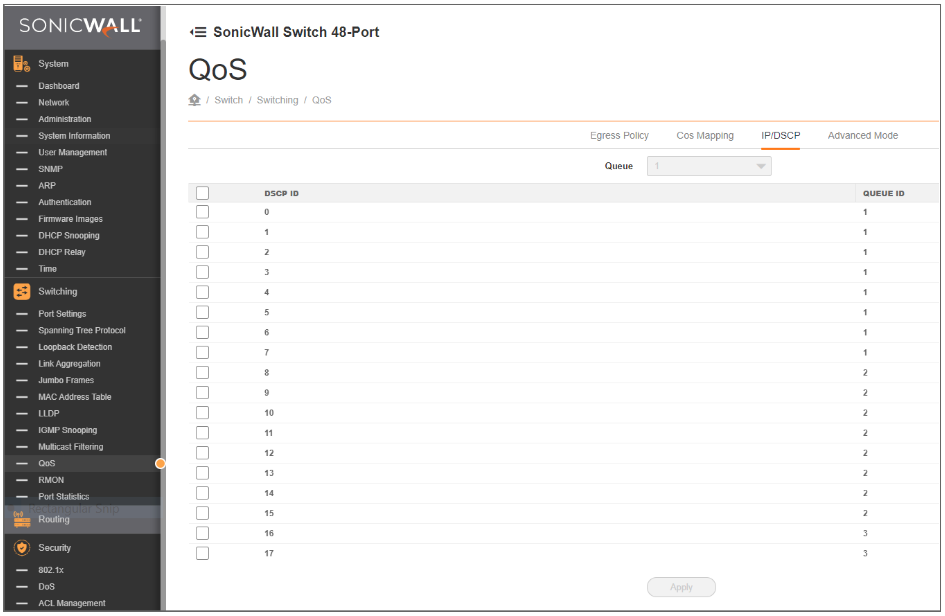
Total: 8 item(s)

Click **Apply** to save the changes to the system.

IP/DSCP Mapping

Use IP/Differentiated Services Code Point (DSCP) Mapping feature to specify which internal traffic class to map to the corresponding DSCP values. DSCP Mapping increases the number of definable priority levels by reallocating bits of an IP packet for prioritization purposes.

IP/DSCP (Differentiated Services Code Point)	Displays the packet's DSCPvalues, where 0 is the lowest and 63 is the highest.
Queue	Check the CoS priority tag box and select the Queue values for each DSCP in the provided fields. Eight traffic priority queues are supported and the field values are from 1-8, where one is the lowest priority and eight is the highest priority.



Queue: 1

☐	DSCP ID	QUEUE ID
☐	0	1
☐	1	1
☐	2	1
☐	3	1
☐	4	1
☐	5	1
☐	6	1
☐	7	1
☐	8	2
☐	9	2
☐	10	2
☐	11	2
☐	12	2
☐	13	2
☐	14	2
☐	15	2
☐	16	3
☐	17	3

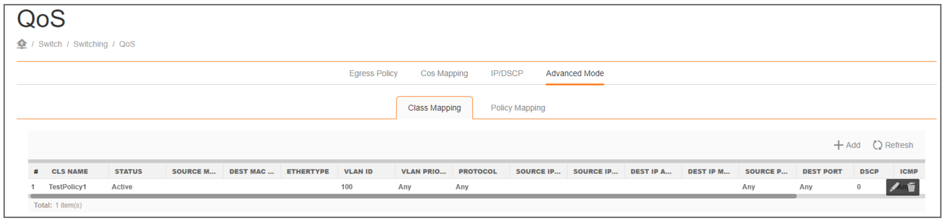
Click **Apply** to save the changes to the system.

Class Mapping

Class mapping uses the Access Control List (ACL) rules to Quality of Service (QoS) settings to control the traffic within a network. ACLs and Access Control Elements (ACE) are defined to indicate the traffic which should be permitted or denied into the network.

CLS Name	Displays the class mapping name.
Status	Displays the status of the class mapping whether it is active or not.
Source MAC Address	Displays the source MAC address.
Dest MAC Address	Displays the destination MAC address.
Ethertype	Displays the Ethertype value. The range is from 0600-FFFF.
VLAN ID	Enter the VLAN ID to which the MAC address is attached. The range is from 1-4094.
VLAN Priority	Displays the priority of VLAN. The range is from 0-7. 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.
Protocol	Displays the protocol defined for the class mapping.
Source IP Address	Displays the source IP address.
Source IP Mask	Displays the mask of the new source IP address.
Dest IP Address	Displays the destination IP address.
Dest IP Mask	Displays the mask of the new destination IP address.

Source Port	Displays the source port that is matched to the class mapping.
Dest Port	Displays the destination port that is matched to the class mapping.
DSCP	Differentiated Services Code Point (DSCP) defines a value from 0 to 63 that maps to a certain traffic classification.
ICMP	Displays the type of the ICMP.
ICMP Code	Displays the ICMP code. The range is from 0-255.
Action	Displays the type of action selected. The actions are DSCP to match or 802.1p to match.


QoS

/ Switch / Switching / QoS

#	CLS NAME	STATUS	SOURCE M...	DEST MAC ...	ETHERTYPE	VLAN ID	VLAN PRIO...	PROTOCOL	SOURCE IP...	SOURCE IP...	DEST IP A...	DEST IP M...	SOURCE P...	DEST PORT	DSCP	ICMP
1	TestPolicy1	Active				100	Any	Any					Any	Any	0	Any

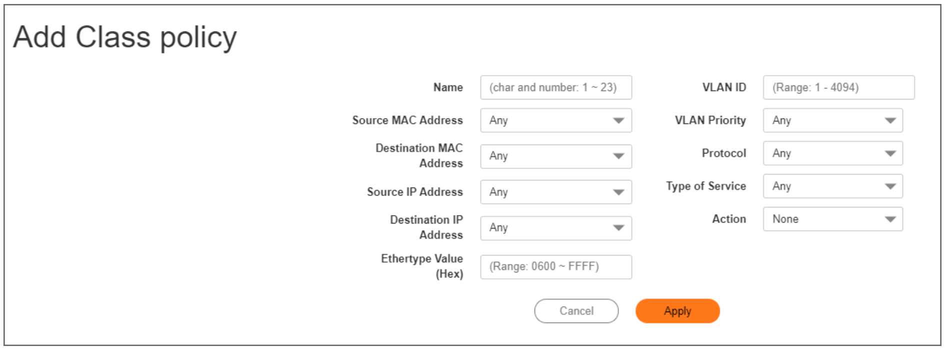
Total: 1 item(s)

Adding a Class Policy

From here, you can configure the details pertaining to a class policy. Click **Add** to add a new class policy.

Name	Enter the name for the class policy. You can use up to 23 alphanumeric characters.
Source MAC Address	Select the Source MAC Address from the drop-down. • Selecting **User Defined** option allows you to define your Source MAC Address. In the Source MAC Value field, enter the required value.
Destination MAC Address	Select the Destination MAC Address from the drop-down. • Selecting **User Defined** option allows you to define your Destination MAC Address. In the Destination MAC Value field, enter the required value.
Source IP Address	Select the Source IP Address from the drop-down. • Selecting **User Defined** option allows you to define your Source IP Address. In the Source IP Mask field, enter the required value.
Destination IP Address	Select the Destination IP Address from the drop-down. • Selecting **User Defined** option allows you to define your Destination IP Address. In the Destination IP Mask field, enter the required value.
Ethertype Value (Hex)	Enter the Ethertype value. The range is from 0600-FFFF.
VLAN ID	Enter the VLAN ID range from the configured VLANs to associate with the Class Policy. The VLAN ID number range is from 1 to 4094.
VLAN Priority	Select the VLAN Priority from the drop-down. • Selecting **802.1p to match** option allows you to define your VLAN Priority. The VLAN ID Priority range is from 0 to 7.

Protocol	Select Any or Select from a List in the drop down menu. Based on the protocol selection, the fields for the protocol appears.
Type of Service	Select the Type of Service from the drop-down • Selecting **DSCP to match** option allows you to define the DSCP value. The range is from 0-63.
Action	Select the Type of Action from the drop-down. • Selecting **802.1p to match** option allows you to define VLAN Priority. The VLAN ID Priority range is from 0 to 7. • Selecting **DSCP to match** option allows you to define the DSCP value. The range is from 0-63.



Add Class policy

Name	(char and number: 1 ~ 23)	VLAN ID	(Range: 1 - 4094)
Source MAC Address	Any	VLAN Priority	Any
Destination MAC Address	Any	Protocol	Any
Source IP Address	Any	Type of Service	Any
Destination IP Address	Any	Action	None
Ethertype Value (Hex)	(Range: 0600 ~ FFFF)		

Click **Apply** to save the changes to the system.

Editing a Class Policy

To edit a class policy:

1. In the Class Mapping table, hover on the class policy which you want to edit and click **Edit** icon.
2. Make the necessary changes and click **Apply** to save the settings.

Deleting a Class Policy

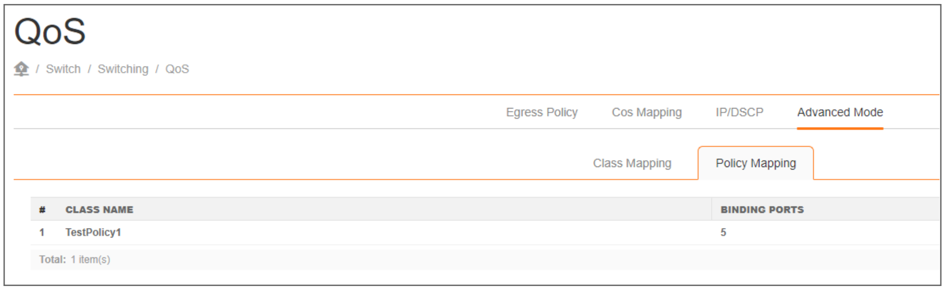
To delete a class policy:

1. In the Class Mapping table, hover on the class policy which you want to delete and click **Delete** icon.
   A confirmation dialog appears.
2. Click **Confirm** to delete a class policy.
   The class policy is removed from the Class Mapping table.

Policy Mapping

The Policy Mapping screen contains information on the class mapping policy and ports.

Class Name	Displays the class mapping name.
Binding Ports	Displays the port mapped to the class policy. The range is from 0 to 52.



#	CLASS NAME	BINDING PORTS
1	TestPolicy1	5

Total: 1 item(s)

Editing a Policy Mapping

To edit a policy mapping:

1. In the Policy Mapping table, hover on the class name which you want to edit and click **Edit** icon.
2. Make the necessary changes and click **Apply** to save the settings.

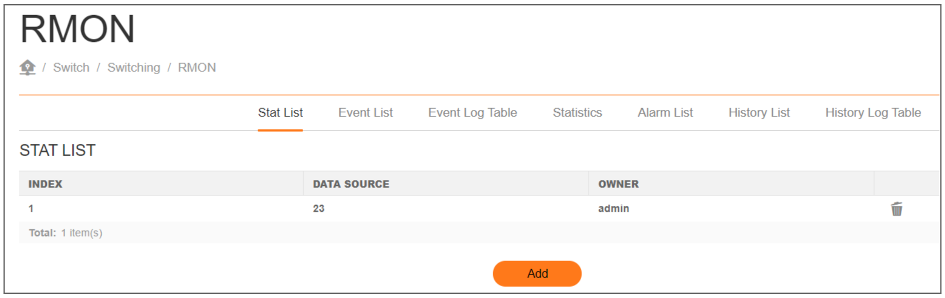
Remote Network Monitoring

Remote Network Monitoring (RMON) is used for support monitoring and protocol analysis of LANS by enabling various network monitors and console systems to exchange network-monitoring data through the Switch.

Stat List

The Stat List page displays general information about the Switch in terms of its data source and owners.

Index	Displays the entry number for the Stat List table.
Data Source	Displays the data source from which the data is collected.
Owner	Displays the name of the owner of the RMON group of statistics.



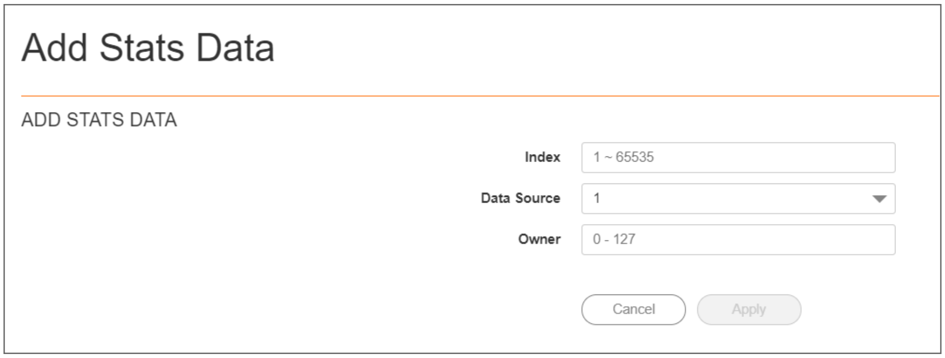
STAT LIST

INDEX	DATA SOURCE	OWNER
1	23	admin

Total: 1 item(s)

To add Stats Data:

1. Click **Add**.
   The **Add Stats Data** page displays.
2. In the **Index** field, enter the entry number for the Stat List table. The range is from 1- 65535.
3. In the **Data Source** drop-down, select the data source from which the data is to be collected.
4. In the **Owner** field, enter the name of the owner of the RMON group of statistics . The range is from 0- 127.
5. Click **Apply** to save the changes.



Add Stats Data

ADD STATS DATA

Index: 1 ~ 65535

Data Source: 1

Owner: 0 - 127

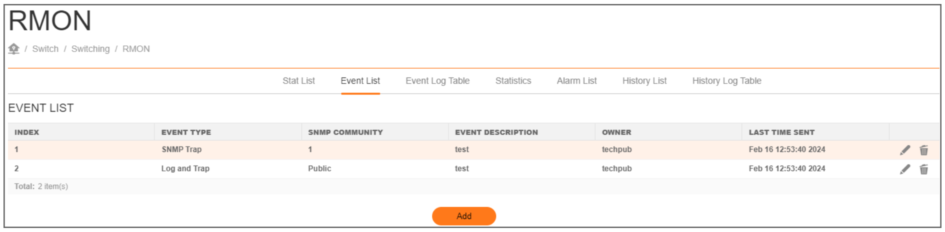
To delete Stats Data:

1. Click **Delete** icon on the stat list which you want to delete.
   A confirmation dialog appears.
2. Click **Confirm** to delete the Stats Data from the table.

Event List

The **Event List** defines RMON events on the Switch.

Index	Enter the entry number for Event.
Event Type	Select the event type. • Log – The event is a log entry. • SNMP Trap – The event is a trap. • Log and Trap – The event is both a log entry and a trap.
SNMP Community	Enter the community to which the event belongs created in **System > SNMP > Community**.
Description	Displays the number of good broadcast packets received on the interface.
Owner	Enter the switch that defined the event.



EVENT LIST

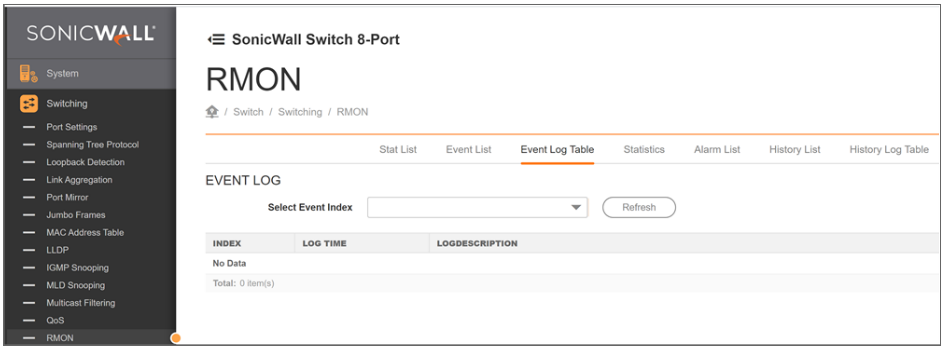
INDEX	EVENT TYPE	SNMP COMMUNITY	EVENT DESCRIPTION	OWNER	LAST TIME SENT
1	SNMP Trap	1	test	techpub	Feb 16 12:53:40 2024
2	Log and Trap	Public	test	techpub	Feb 16 12:53:40 2024

Total: 2 item(s)

Event Log Table

From here, you can view specific Event logs for the Switch. Choose an Event log you wish to view from the drop-down list.

Select the index of the Event Log from the list.



EVENT LOG

Select Event Index

INDEX	LOG TIME	LOGDESCRIPTION
No Data		

Total: 0 item(s)

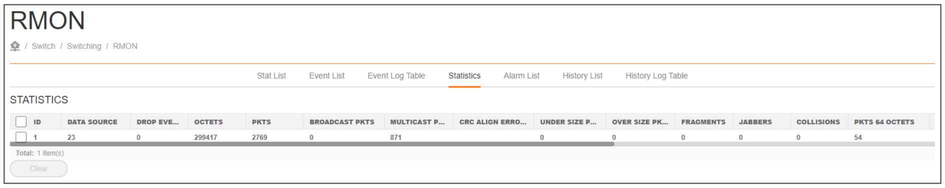
Click **Apply** to accept the changes or **Cancel** to discard them.

Statistics

The Statistics page displays general information about the Switch in terms of its ports and packet transmissions.

ID	Shows the specific port for which RMON statistics are displayed.
Data Source	Displays the data source from which the data is collected.
Drop Event	Displays the number of dropped events that have occurred on the port.
Octets	Displays the sample number from which the statistic taken.
Pkts	Displays the number of octets received on the port.
Broadcast Pkts	Displays the number of good broadcast packets received on the port. This number does not include Multicast packets.
Multicast Pkts	Displays the number of good Multicast packets received on the port.
CRC Align Errors	Displays the number of CRC and Align errors that have occurred on the port.
Under Size Pkts	Displays the number of undersized packets (less than 64 octets) received on the port.

Over Size Pkts	Displays the number of oversized packets (over 1518 octets) received on the port.
Fragments	Displays the number of fragments received on the port.
Jabbers	Displays the total number of received packets that were longer than 1518 octets.
Collisions	Displays the number of collisions received on the port.
Pkts 64 Octets	Displays the number of 64-byte frames received on the port.
Pkts 65 to 127 Octets	Displays the number of 65 to 127 byte packets received on the port.
Pkts 128 to 255 Octets	Displays the number of 128 to 255 byte packets received on the port.
Pkts 256 to 511 Octets	Displays the number of 256 to 511 byte packets received on the port.
Pkts 512 to 1023 Octets	Displays the number of 512 to 1023 byte packets received on the port.
Pkts 1024 to 1518 Octets	Displays the number of 1024 to 1518 byte packets received on port.


RMON

STATISTICS

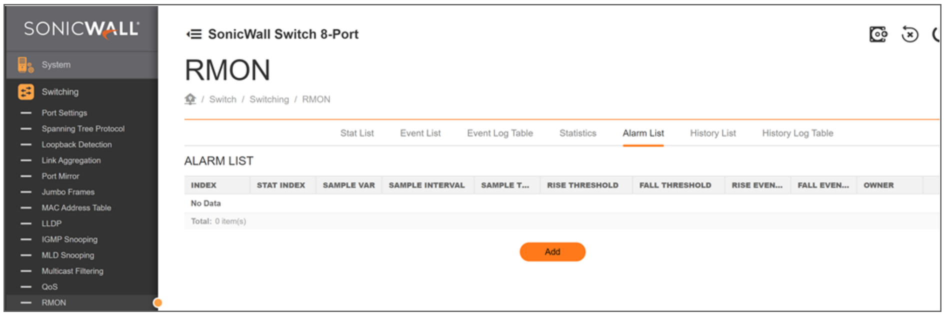
☐ ID	DATA SOURCE	DROP EVE...	OCTETS	PKTS	BROADCAST PKTS	MULTICAST P...	CRC ALIGN ERRO...	UNDER SIZE P...	OVER SIZE PK...	FRAGMENTS	JABBERS	COLLISIONS	PKTS 64 OCTETS
☐ 1	23	0	299417	2769	0	871		0	0	0	0	0	54

Total: 1 item(s)

Alarm List

You can configure Network alarms to occur when a network problem is detected. Choose your preferences for the alarm from the drop-down boxes.

Index	Enter the entry number for the History Log Table. Sample Port – Select the port from which the alarm samples were taken.
Sample Variable	Select the variable of samples for the specified alarm sample.
Sample Interval	Enter the alarm interval time.
Sample Type	Select the sampling method for the selected variable and comparing the value against the thresholds. • Absolute – Compares the values with the thresholds at the end of the sampling interval. • Delta – Subtracts the last sampled value from the current value.
Rise Threshold	Enter the rising number that triggers the rising threshold alarm.
Fall Threshold	Enter the falling number that triggers the falling threshold alarm
Rise Event	Enter the event number by the falling alarm are reported.
Fall Event	Enter the event number by the falling alarms are reported.
Owner	Enter the Switch that defined the alarm.



ALARM LIST

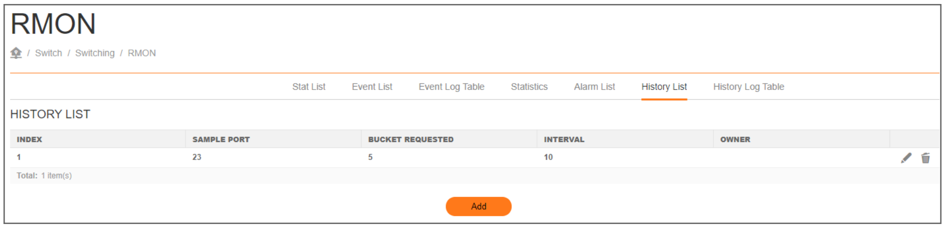
INDEX	STAT INDEX	SAMPLE VAR	SAMPLE INTERVAL	SAMPLE T...	RISE THRESHOLD	FALL THRESHOLD	RISE EVEN...	FALL EVEN...	OWNER
No Data									

Total: 0 item(s)

History List

The RMON History List screen contains information about samples of data taken from the ports.

Index	Enter the entry number for the History Log Table.
Sample Port	Select the port from which the history samples were taken.
Bucket Requested	Enter the number of samples to be saved. The range is from 1- 50.
Interval	Enter the time that samples are taken from the ports. The field range is from 1-3600.
Owner	Enter the RMON user that requested the RMON information. The range is from 0-32 characters.



HISTORY LIST

INDEX	SAMPLE PORT	BUCKET REQUESTED	INTERVAL	OWNER
1	23	5	10	

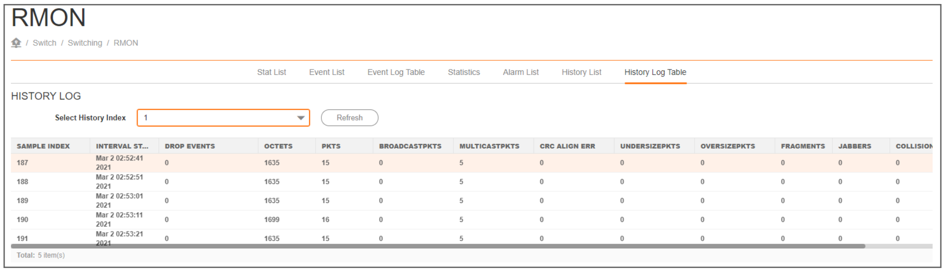
Total: 1 item(s)

History Log Table

From here, you can view the History Index for History Logs on the Switch. Select a History Index to view from the drop-down box.

Sample Index	Displays the index value for the sample which is collected on the port for a particular interval of time.
Interval Start	Displays the starting time for the sample collected on the port.
Drop Events	Displays the number of dropped events that have occurred on the port.
Octets	Displays the sample number from which the statistic taken.
Pkts	Displays the number of octets received on the port.

Broadcast Pkts	Displays the number of good broadcast packets received on the port. This number does not include Multicast packets.
Multicast Pkts	Displays the number of good Multicast packets received on the port.
CRC Align Errors	Displays the number of CRC and Align errors that have occurred on the port.
Under Size Pkts	Displays the number of undersized packets (less than 64 octets) received on the port.
Over Size Pkts	Displays the number of oversized packets (over 1518 octets) received on the port.
Fragments	Displays the number of fragments received on the port.
Jabbers	Displays the total number of received packets that were longer than 1518 octets.
Collisions	Displays the number of collisions received on the port.
Utilization	Displays the type of Octets packet frames received on the port.



RMON

/ Switch / Switching / RMON

HISTORY LOG

Select History Index: 1

SAMPLE INDEX	INTERVAL ST...	DROP EVENTS	OCTETS	PKTS	BROADCASTPKTS	MULTICASTPKTS	CRC ALIGN ERR	UNDERSIZEPKTS	OVERSIZEPKTS	FRAGMENTS	JABBERS	COLLISION
187	Mar 2 02:52:41 2021	0	1635	15	0	5	0	0	0	0	0	0
188	Mar 2 02:52:51 2021	0	1635	15	0	5	0	0	0	0	0	0
189	Mar 2 02:53:01 2021	0	1635	15	0	5	0	0	0	0	0	0
190	Mar 2 02:53:11 2021	0	1699	16	0	5	0	0	0	0	0	0
191	Mar 2 02:53:21 2021	0	1635	15	0	5	0	0	0	0	0	0

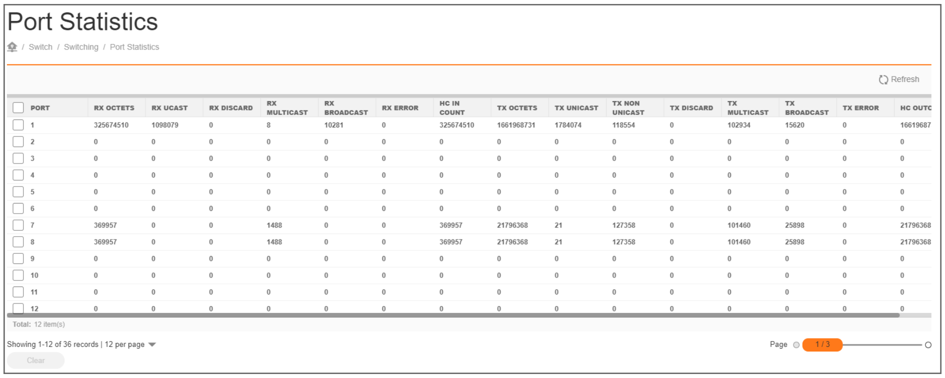
Total: 5 item(s)

Port Statistics

The Port Statistics section displays a summary of all port traffic statistics regarding the monitoring features on the Switch.

Port	Displays the port for which statistics are displayed.
RX OCTETS	Displays the number of all packets received on the port.
RX UCAST	Displays the number of Unicast packets received on the port.
RX NON UCAST	Displays the number of Unicast packets received on the port.
RX DISCARD	Displays the number of received packets discarded on the port.
RX MULTICAST	Displays the number of Multicast packets received on the port.
RX BROADCAST	Displays the number of Broadcast packets received on the port.
RX ERROR	Displays the number of errors received on the port.
HC IN COUNT	Displays the total number of packets received on the port.
TX OCTETS	Displays the number of all packets transmitted on the port.
TX UNICAST	Displays the number of Unicast packets transmitted on port.
TX NON UNICAST	Displays the number of Unicast packets transmitted on the port.

TX DISCARD	Displays the number of transmitted packets discarded on the port.
TX MULTICAST	Displays the number of Multicast packets transmitted on the port.
TX BROADCAST	Displays the number of Broadcast packets transmitted on the port.
TX ERROR	Displays the number of errors transmitted on the port.
HC OUT COUNT	Displays the total number of packets transmitted on the port.



Port Statistics

/ Switch / Switching / Port Statistics

Refresh

□	PORT	RX OCTETS	RX UCAST	RX DISCARD	RX MULTICAST	RX BROADCAST	RX ERROR	HC IN COUNT	TX OCTETS	TX UNICAST	TX NON UNICAST	TX DISCARD	TX MULTICAST	TX BROADCAST	TX ERROR	HC OUTC
□	1	325674510	1098079	0	8	10281	0	325674510	1661968731	1784074	118554	0	102934	15620	0	16619687
□	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
□	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
□	4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
□	5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
□	6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
□	7	369957	0	0	1488	0	0	369957	21796368	21	127358	0	101460	25898	0	21796368
□	8	369957	0	0	1488	0	0	369957	21796368	21	127358	0	101460	25898	0	21796368
□	9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
□	10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
□	11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
□	12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Total: 12 item(s)

Showing 1-12 of 36 records | 12 per page

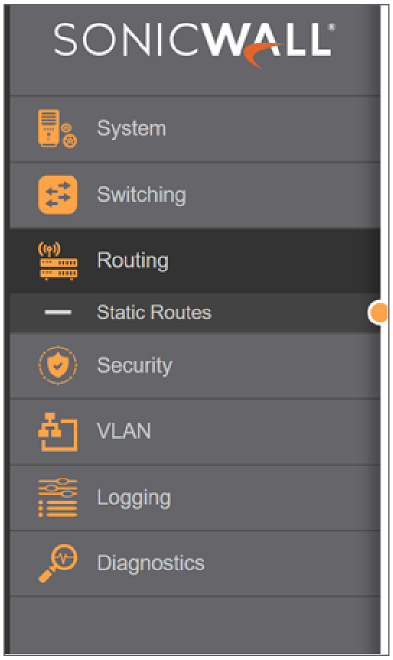
Clear

Page 1 / 3

ⓘ | **NOTE:** To refresh the data, click on the **Refresh** button.

Routing

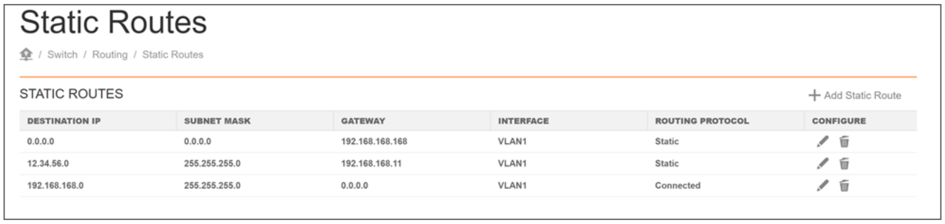
Routing is the process of selecting a path for traffic in a network or between or across multiple networks.



Static Routes

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.

Destination IP	Enter the IP address of the destination host/network.
Subnet Mask	Enter the network mask for the particular subnet.
Gateway	Enter the next hop IP address for the traffic.
Interface	This refers to the outgoing interface which is uplink.
Routing Protocol	This is either Static or Connected. This is not editable.
Configure	Use this option to edit or delete the existing static routes.



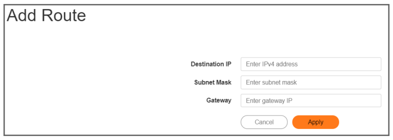
Static Routes

/ Switch / Routing / Static Routes

STATIC ROUTES

DESTINATION IP	SUBNET MASK	GATEWAY	INTERFACE	ROUTING PROTOCOL	CONFIGURE
0.0.0.0	0.0.0.0	192.168.168.168	VLAN1	Static	✎ 🗑
12.34.56.0	255.255.255.0	192.168.168.11	VLAN1	Static	✎ 🗑
192.168.168.0	255.255.255.0	0.0.0.0	VLAN1	Connected	✎ 🗑

Click **Add Static Route** and update the details. Then Click **Apply** to add the new route.



Add Route

Destination IP: Enter IPv4 address

Subnet Mask: Enter subnet mask

Gateway: Enter gateway IP

Security

The Security page allows you to configure the following:

- 802.1X Security
- Denial of Service
- ACL Management

802.1X Security

The IEEE-802.1X port-based authentication provides a security standard for network access control with RADIUS servers and holds a network port disconnected until authentication is completed. With 802.1X port-based authentication, the supplicant provides credentials, such as user name, password, or digital certificate to the authenticator, and the authenticator forwards the credentials to the authentication server for verification. If the authentication server determines the credentials are valid, the supplicant (client device) is allowed to access resources located on the protected side of the network. The Switch uses 802.1X to enable or disable port access control, to enable or disable the Guest VLAN, and to enable or disable the forwarding EAPOL (Extensible Authentication Protocol over LANs) frames.

Mac Authentication Bypass

802.1X MAB is an access control technique which using the MAC address of a device to determine what kind of network access should be provided to hosts. For MAB authentication mechanism, switch will transmit Access-Request message to RADIUS server, with device MAC address. If the MAC address is valid, the RADIUS server will return a RADIUS Access-Accept message. This message indicates to the switch that the endpoint should be allowed access to the port. No further authentication methods will be tried if MAB succeeds.

Host-based 802.1X enables the switch to allow only one or multiple hosts to gain access to the network. Each host on the port should be authenticated individually. Packets from unauthorized hosts will be dropped on the port.

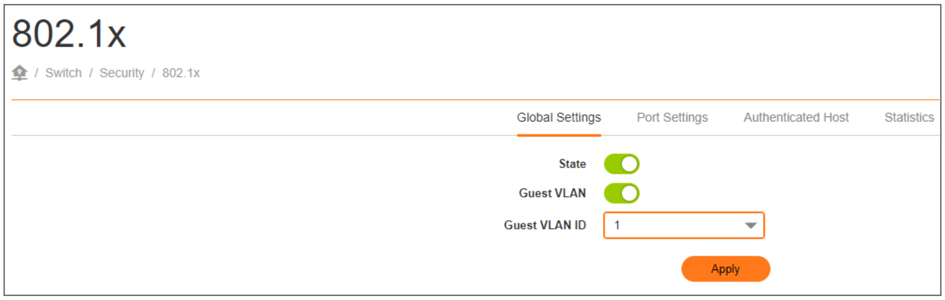
Behaviors and Restrictions

1. For MAB authentication mechanism, switch will transmit Access-Request message with host source MAC address as user and password. In radius server configuration, the format of the MAC address should be 12 hexadecimal digits, all lowercase and no punctuation.
2. If the host source MAC address is saved as static MAC in **MAC Address Table**, the MAC address will not be progressed during MAB process.
3. Switch can handle 10 different MAB requests at the same time per port for authentication.
4. In **hybrid_mode**, host will be authenticated with EAP by default. If host does not support EAP capability, it will fall back to **MAB authentication** mode.
5. In **MAC-based** mode, traffic from hosts not allowed for authentication will be dropped.
6. Before configuring **MAC-based authentication** mode, this port must be set **port control auto**. (Mac-Based mode can only be enabled when dot1x port-control is auto.)
7. Each host is authenticated separately when using **MAC-based authentication** mode.
8. Guest **VLAN** and **RADIUS VLAN** assignment have no effect in **MAC-based** mode. (Mac-Based mode can only be enabled when dot1x guest vlan and radius vlan assignment are disabled.)
9. In **MAC-based** mode, host information will be cleared after configuring max host number. Hosts that have passed authentication will have to be authenticated again.
10. Host information will be cleared after authentication mode, link up status or MAB mode has changed.
11. **Mac-Based** mode does not support MAB hybrid mode.(**Mac-Based** mode can only be enabled when dot1x MAB is mab_mode or disabled.)
12. Max host count is only effective when using **MAC-based authentication** mode.

Global Settings

From here, you can select whether to Enable or Disable 802.1X for the Switch. If enabled, next choose whether to Enable or Disable the Guest VLAN for the Switch. Finally, select the VLAN ID you wish from the list.

State	Select whether authentication is Enabled or Disabled on the Switch.
Guest VLAN	Select whether Guest VLAN is Enabled or Disabled on the Switch. The default is Disabled.
Guest VLAN ID	Select the guest VLAN ID from the list of currently defined VLANs.



802.1x

/ Switch / Security / 802.1x

State ●

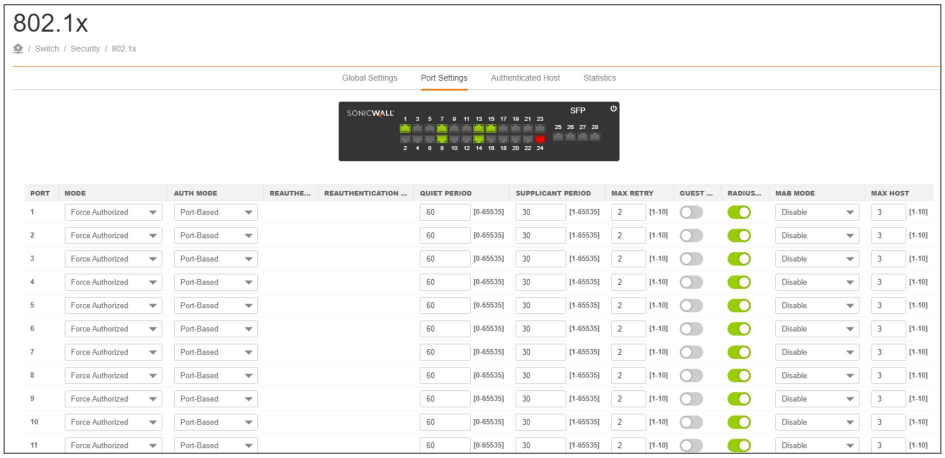
Guest VLAN ●

Guest VLAN ID 1

Click **Apply** to save the changes to the system.

Port Settings

This port settings displays similar settings to view and configure Switch port settings along with Auth mode, MAB Mode and Max Host.



802.1x

/ Switch / Security / 802.1x

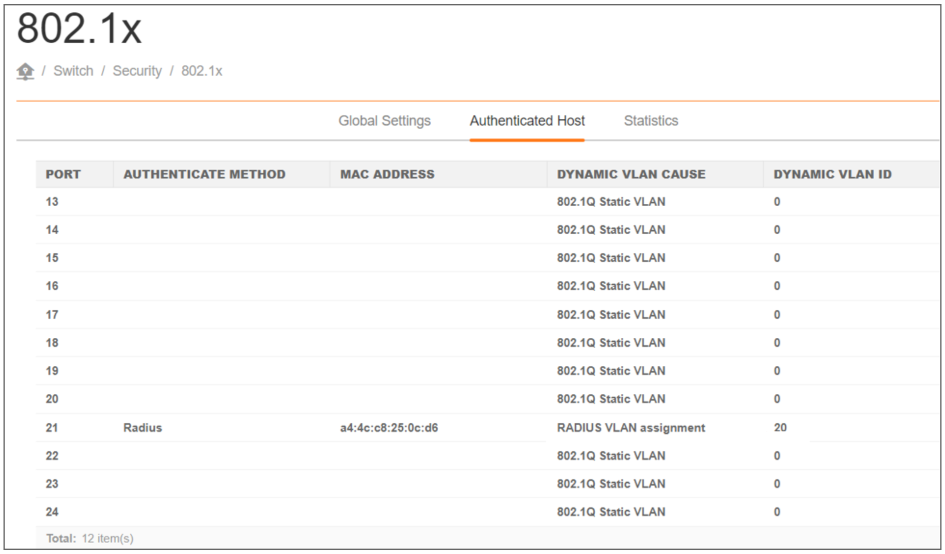
PORT	MODE	AUTH MODE	REAUTHE...	REAUTHENTICATION ...	QUIET PERIOD	SUPPLICANT PERIOD	MAX RETRY	GUEST ...	RADIUS...	MAB MODE	MAX HOST
1	Force Authorized	Port-Based			60 [0-65535]	30 [1-65535]	2 [1-10]	○	●	Disable	3 [1-10]
2	Force Authorized	Port-Based			60 [0-65535]	30 [1-65535]	2 [1-10]	○	●	Disable	3 [1-10]
3	Force Authorized	Port-Based			60 [0-65535]	30 [1-65535]	2 [1-10]	○	●	Disable	3 [1-10]
4	Force Authorized	Port-Based			60 [0-65535]	30 [1-65535]	2 [1-10]	○	●	Disable	3 [1-10]
5	Force Authorized	Port-Based			60 [0-65535]	30 [1-65535]	2 [1-10]	○	●	Disable	3 [1-10]
6	Force Authorized	Port-Based			60 [0-65535]	30 [1-65535]	2 [1-10]	○	●	Disable	3 [1-10]
7	Force Authorized	Port-Based			60 [0-65535]	30 [1-65535]	2 [1-10]	○	●	Disable	3 [1-10]
8	Force Authorized	Port-Based			60 [0-65535]	30 [1-65535]	2 [1-10]	○	●	Disable	3 [1-10]
9	Force Authorized	Port-Based			60 [0-65535]	30 [1-65535]	2 [1-10]	○	●	Disable	3 [1-10]
10	Force Authorized	Port-Based			60 [0-65535]	30 [1-65535]	2 [1-10]	○	●	Disable	3 [1-10]
11	Force Authorized	Port-Based			60 [0-65535]	30 [1-65535]	2 [1-10]	○	●	Disable	3 [1-10]

Port	Displays the ports for which the 802.1X information is displayed
Mode	Select the Auto or Force UnAuthorized or Force Authorized mode from the list.
AuthMode	Select the Port-Based or MAC-Based from the list.
Reauthentication	Displays whether port reauthentication is Enabled or Disabled.
Reauthentication Period	Displays the time span in which the selected port is reauthenticated.
Quiet Period	Enter the number of the device that remains in the quiet state following a failed authentication exchange. The default is 60 seconds.

Supplicant Period	Enter the amount of time that lapses before an EAP request is resent to the supplicant. The default is 30 seconds.
Max Retry	Enter the maximum number of times that the switch retransmits an EAP request to the client before it times out the authentication session. The default is 2 times
Guest VLAN	Select whether Guest VLAN is Enabled or Disabled on the Switch. The default is Disabled.
RADIUS VLAN Assign	Displays the status of RADIUS VLAN Assignment.
MAB Mode	Select the MAB-mode, Hybrid-mode, or Disable from the list.

Authenticated Host

The Authenticated Host section displays the authenticated Port, Authenticate Method, MAC Address, Dynamic VLAN Cause and Dynamic VLAN ID.



802.1x

/ Switch / Security / 802.1x

PORT	AUTHENTICATE METHOD	MAC ADDRESS	DYNAMIC VLAN CAUSE	DYNAMIC VLAN ID
13			802.1Q Static VLAN	0
14			802.1Q Static VLAN	0
15			802.1Q Static VLAN	0
16			802.1Q Static VLAN	0
17			802.1Q Static VLAN	0
18			802.1Q Static VLAN	0
19			802.1Q Static VLAN	0
20			802.1Q Static VLAN	0
21	Radius	a4:4c:c8:25:0c:d6	RADIUS VLAN assignment	20
22			802.1Q Static VLAN	0
23			802.1Q Static VLAN	0
24			802.1Q Static VLAN	0

Total: 12 item(s)

Port	Displays the ports information.
Authentication Settings	Displays the selected authentication type.
MAC Address	Displays the MAC Address.
Dynamic VLAN Cause	Displays the method that authorized users on the access interface fall to Dynamic VLAN.
Dynamic VLAN ID	Displays the authorized users on the access interface to the RADIUS assignment VLAN ID

Port Statistics

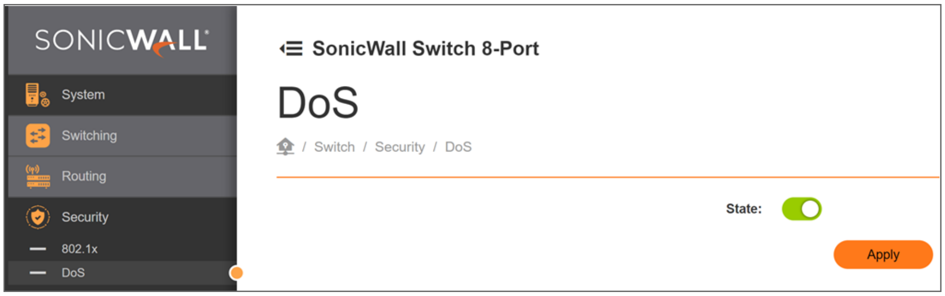
The Port Statistics section displays a summary of all port traffic statistics on the Switch.

Port No	Displays the port for which statistics are displayed.
TX REQID	Displays the number of 802.1x-Request/Identity messages transmitted on the port.
TX REQ	Displays the number of transmitted 802.1x-Request frames other than Request/Identity on the port.
TX TOTAL	Displays the total number of EAPOL messages transmitted on the port.
RX START	Displays the number of EAPOL-Start messages received on the port.
RX LOGOFF	Displays the number of 802.1x-Logoff messages received on the port.
RX RES	Displays the number of 802.1x-Response/Identity frames received on the port.
RX RESP	Displays the number of 802.1x-Response messages received other than Response/Identity.
RX INVALID	Displays the number of invalid EAPOL messages received on the port.
RX LEN ERR	Displays the number of EAPOL messages with incorrect length received on the port.
RX TOTAL	Displays the number of EAPOL messages received on the port.
RX VERSION	Displays the version number of the EAPOL message received on the port.
LAST RX SRC MAC	Displays the source MAC address in the last EAPOL message received on the port.

Denial of Service

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:

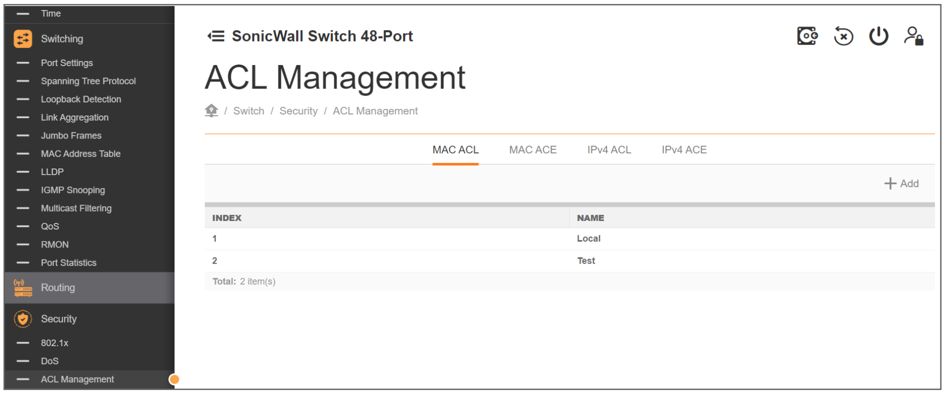
State: Enable or disable DoS to prevent the switch from DoS attacks



Click **Apply** to save the changes to the system.

ACL Management

Access Control List (ACL) allows you to define classification rules or establish criteria to provide security to your network by blocking unauthorized users and allowing authorized users to access specific areas or resources. ACLs can provide basic security for access to the network by controlling whether packets are forwarded or blocked at the Switch ports. Access Control Lists (ACLs) are filters that allow you to classify data packets according to a particular content in the packet header, such as the source address, destination address, source port number, destination port number, and more. Packet classifiers identify flows for more efficient processing. Each filter defines the conditions that must match for inclusion in the filter. ACLs are used to provide traffic flow control, restrict contents of routing updates, and determine which types of traffic are forwarded or blocked. This criterion can be specified on a basis of the MAC address or IP address.



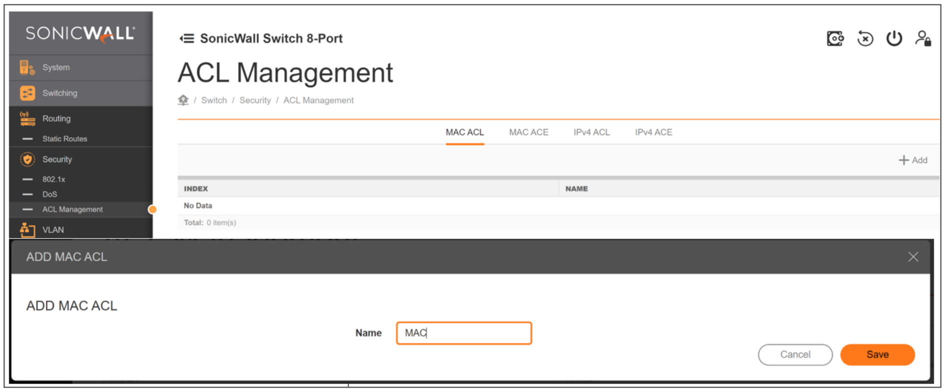
INDEX	NAME
1	Local
2	Test

Total: 2 item(s)

MAC ACL

Allows an MAC Based Access Control Lists (ACLs) to be defined. Enter the name of the MAC based ACL name in the index box. You can type up to 32 alphanumeric characters.

Index	Displays the current number of ACLs.
Name	Enter the MAC based ACL name. You can use up to 32 alphanumeric characters.



INDEX	NAME
No Data	

Total: 0 item(s)

ADD MAC ACL

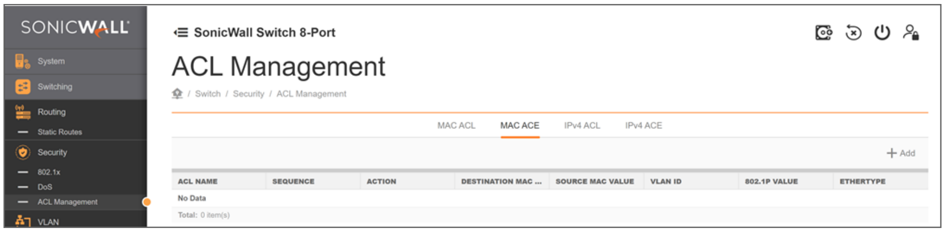
Name: MAC

Click **Save** to accept the changes or **Cancel** to discard them.

MAC-Based ACE

Allows Mac-Based Access Control Entry (ACE) to be defined within a configured ACL.

ACL Name	Select the ACL from the list.
Sequence	Enter the sequence number which signifies the order of the specified ACL relative to other ACLs assigned to the selected interface. The valid range is from 1-2147483646, 1 being processed first.
Action	Select what action taken if a packet matches the criteria. • Permit – Forward packets that meet the ACL criteria. • Deny– Drops packets that meet the ACL criteria.
Destination MAC Value	Enter the destination MAC address.
Source MAC Value	Enter the source MAC address.
VLAN ID	Enter the VLAN ID to which the MAC address is attached in MAC ACE. The range is from 1-4094.
802.1p Value	Enter the 802.1p value. The range is from 0-7.
Ethertype Value	Enter the Ethertype value. The range is from 0600-FFFF.

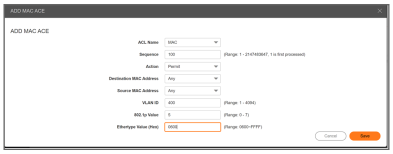


ACL Management

/ Switch / Security / ACL Management

ACL NAME	SEQUENCE	ACTION	DESTINATION MAC ...	SOURCE MAC VALUE	VLAN ID	802.1P VALUE	ETHERTYPE
No Data							

Total: 0 item(s)



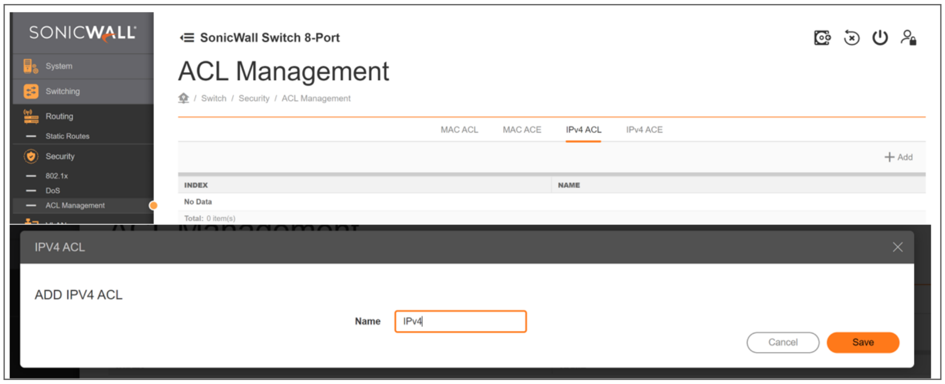
ADD MAC ACE

ACL Name	MAC	
Sequence	100	(Range: 1 - 2147483647, 1 is first processed)
Action	Permit	
Destination MAC Address	Any	
Source MAC Address	Any	
VLAN ID	400	(Range: 1 - 4094)
802.1p Value	5	(Range: 0 - 7)
Ethertype Value (Hex)	0600	(Range: 0600~FFFF)

IPv4 ACL

Allows the IP Based ACL to be defined.

Index	Displays the current number of ACLs.
Name	Enter the IP based ACL name. You can use up to 32 alphanumeric characters.



ACL Management

IPV4 ACL

ADD IPV4 ACL

Name: IPv4

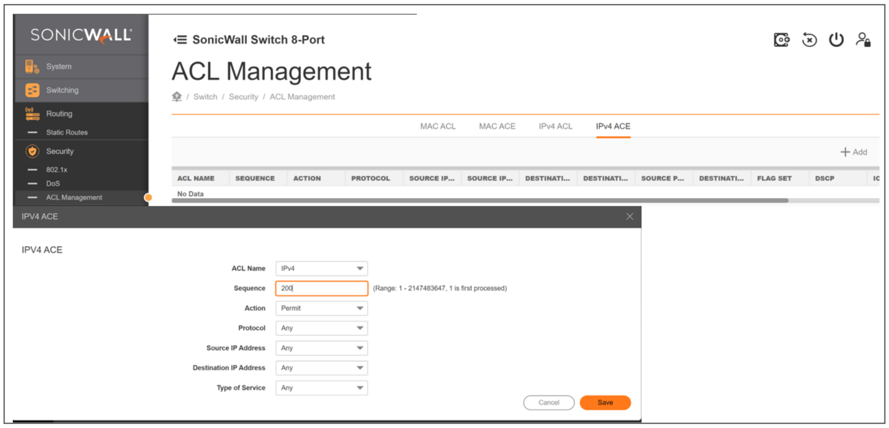
Click **Save** to accept the changes or **Cancel** to discard them.

IPv4-Based ACE

Allows IP Based Access Control Entry (ACE) to be defined within a configured ACL.

ACL Name	Select the ACL from the list.
Sequence	Enter the sequence number which signifies the order of the specified ACL relative to other ACLs assigned to the selected inter- face. The valid range is from 1-2147483646, 1 being processed first.
Action	Select what action to take if a packet matches the criteria. • Permit – Forwards packets that meet the ACL criteria. • Deny– Drops packets that meet the ACL criteria.
Protocol	Select Any, Protocol ID, or Select from a List in the drop-down menu. • Protocol ID – Enter the protocol in the ACE to which the packet is matched. • Select from List–Selects the protocol from the list in the provided field.
Source IP Address	Select Any or User defined.
Source IP Address Value	Enter the source IP address.
Source IP Network Mask	Enter the mask of the new source IP address.
Destination IP Address	Select Any or User defined.
Destination IP Address Value	Enter the destination IP address.
Destination IP Network Mask	Enter the mask of the designation IP address.

ICMP	Select Any, Protocol ID, or Select from the List in drop down menu. • Protocol ID – Enter the protocol in the ACE to which the packet is matched. The range is from 0-255. • Select from List– Select the ICMP from the list in the provided field.
ICMP Code	Enter the ICMP code. The range is from 0-255.
Source Port	Select Single or Range from the list. Enter the source port that is matched to the packets. The range is from 0-65535.
Destination Port	Select Single or Range from the list Enter the destination port that is matched to the packets. The range is from 0-65535.
Type of Service	Enter the DSCP. The range is from 0-63.



ACL NAME	SEQUENCE	ACTION	PROTOCOL	SOURCE IP...	SOURCE IP...	DESTINATI...	DESTINATI...	SOURCE P...	DESTINATI...	FLAG SET	DSCP	IC
No Data												

IPV4 ACE

ACL Name: IPv4

Sequence: 200 (Range: 1 - 2147483647, 1 is first processed)

Action: Permit

Protocol: Any

Source IP Address: Any

Destination IP Address: Any

Type of Service: Any

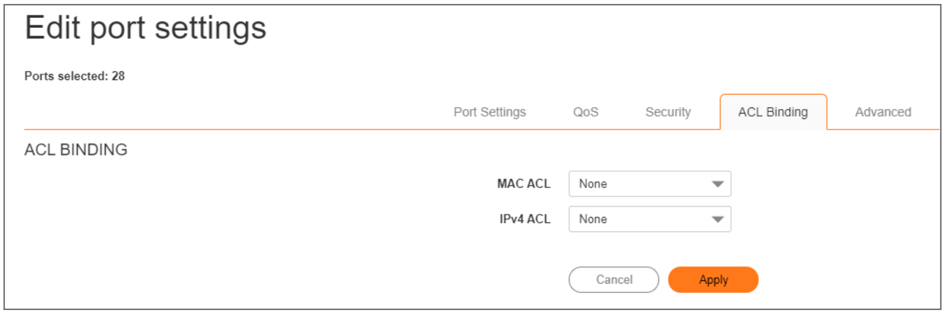
Click **Apply** to save the changes to the system.

After creating the MAC or IPv4ACL, you can bind it with a port by applying it in the Switch port settings. Select a port to edit, then navigate to the ACL binding section.

ACL Binding

ACL Binding is a configuration setting that allows a user to choose a particular ACL for an ACL check. An ACL check is an additional check used to determine what operations a user can perform regarding particular items or item types.

Port	Select the port for which the ACLs are bound to.
MAC ACL	The ACL is MAC address based.
IPv4 ACL	The ACL is IP address based.



Edit port settings

Ports selected: 28

ACL BINDING

MAC ACL: None

IPv4 ACL: None

VLAN

A Virtual LAN (VLAN) is a group of ports that form a logical Ethernet segment on a Layer 2 Switch which provides better administration, security, and management of multicast traffic. A VLAN is a network topology configured according to a logical scheme rather than a physical layout. When you use a VLAN, users can be grouped by logical function instead of physical location. All ports that frequently communicate with each other are assigned to the same VLAN, regardless of where they are physically on the network. VLANs let you logically segment your network into different broadcast domains so that you can group ports with related functions into their own separate, logical LAN segments on the same Switch. This allows broadcast packets to be forwarded only between ports within the VLAN which can avoid broadcast packets being sent to all the ports on a single Switch. A VLAN also increases network performance by limiting broadcasts to a smaller and more manageable logical broadcast domain. VLANs also improve security by limiting traffic to specific broadcast domains.

Topics:

- 802.1Q
- Voice VLAN

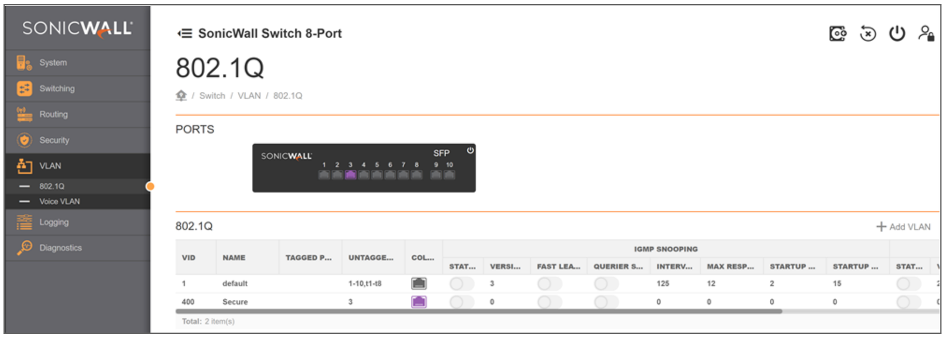
802.1Q

Each VLAN in a network has an associated VLAN ID, which appears in the IEEE 802.1Q tag in the Layer 2 header of packets transmitted on a VLAN. The IEEE802.1Q specification establishes a standard method for tagging Ethernet frames with VLAN membership information. The key for IEEE802.1Q to perform its functions is in its tags. 802.1Q-compliant Switch ports can be configured to transmit tagged or untagged frames. A tag field containing VLAN information can be inserted into an Ethernet frame. When using 802.1Q VLAN configuration, you configure ports to be a part of a VLAN group. When a port receives data tagged for a VLAN group, the data is discarded unless the port is a member of the VLAN group.

VLAN ID	Displays the VLAN ID for which the network policy is defined. The range of the VLAN ID is from 1-4096.
Name	Enter the VLAN name. You can use up to 32 alphanumeric characters.
Tagged Port	Frames transmitted from this port are tagged with the VLAN ID.
Untagged Port	Frames transmitted from this port are untagged.

ⓘ **IMPORTANT:** Port-based VLAN and 802.1Q VLAN are mutually exclusive. If you enable port-based VLAN, then 802.1Q VLAN is disabled.

ⓘ **NOTE:** The Switch's default setting is to assign all ports to a single 802.1Q VLAN(VID 1). Please keep this in mind when configuring the VLAN settings for the Switch.



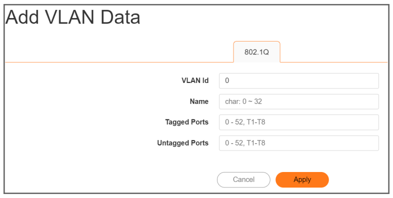
802.1Q

VID	NAME	TAGGED P...	UNTAGGE...	COL...	IGMP SNOOPING									
					STAT...	VERSI...	FAST LEA...	QUERIER S...	INTERV...	MAX RESP...	STARTUP ...	STARTUP ...	STAT...	V
1	default		1-10,t1-t8	⬛	○	3	○	○	125	12	2	15	○	2
400	Secure		3	🟪	○	0	○	○	0	0	0	0	○	0

Total: 2 item(s)

To add an item to the 802.1Q list, follow the below steps:

1. Click the Add button.
2. Enter the VID and name in the VID and Name text boxes.
3. Enter the tagged Ports as required.
4. Enter the Untagged Ports as required.



Add VLAN Data

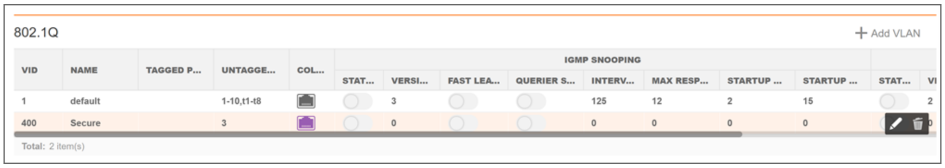
802.1Q

VLAN Id	0
Name	char: 0 ~ 32
Tagged Ports	0 - 52, T1-T8
Untagged Ports	0 - 52, T1-T8

5. Click **Apply** to accept the changes or **Cancel** to discard them.

To delete an item in the 802.1Q list, follow the below steps::

1. Click the Delete button in the row you want to remove an item from. A confirmation dialog is displayed.



802.1Q

VID	NAME	TAGGED P...	UNTAGGE...	COL...	IGMP SNOOPING									
					STAT...	VERSI...	FAST LEA...	QUERIER S...	INTERV...	MAX RESP...	STARTUP ...	STARTUP ...	STAT...	VI
1	default		1-10,t1-t8	⬛	○	3	○	○	125	12	2	15	○	2
400	Secure		3	🟪	○	0	○	○	0	0	0	0		0

Total: 2 item(s)

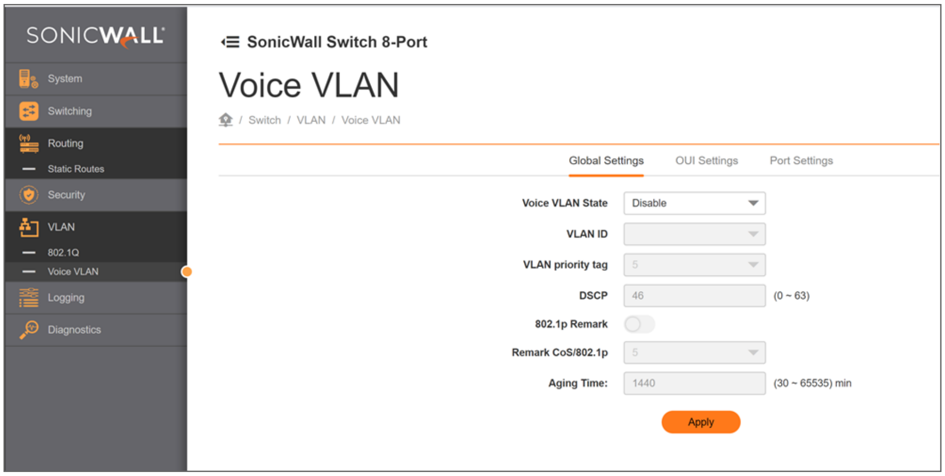
2. Click **Apply** to continue or **Cancel** to abort the changes.

Voice VLAN

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.

Voice VLAN State	Select Disable, Auto or OUI for Voice VLAN state on the Switch.
VLAN ID	Sets the Voice VLAN ID for the network. Only one Voice VLAN is supported on the Switch.
VLAN Priority Tag	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.
DSCP	Differentiated Services Code Point (DSCP) defines a value from 0 to 63 that maps to a certain traffic classification. ⓘ | **NOTE:** Decimal values cannot be configured.
802.1p Remark	Enable this function to have outgoing voice traffic to be marked with the selected CoS value.
Remark CoS/802.1p	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. (Range: 0-7; Default: 5)
Aging Time	The aging time is used to remove a port from voice VLAN if the port is an automatic VLAN member. When the last voice device stops sending traffic and the MAC address of this voice device is aged out, the voice VLAN aging timer will be started. The port will be removed from the voice VLAN after expiration of the voice VLAN aging timer. If the voice traffic resumes during the aging time, the aging timer will be reset and stop. The range for aging time is from 1 – 65535 minutes. The default is 1440 minutes.



Voice VLAN

Voice VLAN State: Disable

VLAN ID:

VLAN priority tag: 5

DSCP: 46 (0 ~ 63)

802.1p Remark: ○

Remark CoS/802.1p: 5

Aging Time: 1440 (30 ~ 65535) min

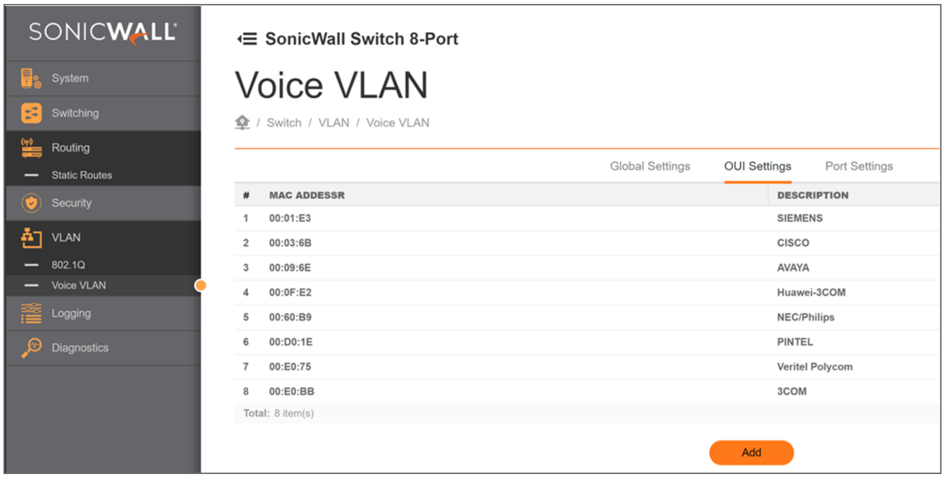
Click **Apply** to update the system settings.

OUI Settings

The Switches determines whether a received packet is a voice packet by checking its source MAC address. VoIP traffic has a preconfigured Organizationally Unique Identifiers (OUI) prefix in the source MAC address. You can manually add specific manufacturer's MAC addresses and description to the OUI table. All traffic received on the Voice VLAN ports from the specific IP phone with a listed OUI is forwarded on the voice VLAN.

To configure the OUI settings, click the Edit button to re-configure the specific entry. Click the Delete button to remove the specific entry and click the Add button to create a new OUI entry.

Port	Enter the OUI to the Voice VLAN. The following OUI are enabled by default. The following OUI are enabled by default. 00:E0:BB - Assigned to 3COM IP Phones. 00:03:6B - Assigned to Cisco IP Phones. 00:E0:75 - Assigned to Veritel IP Phones. 00:D0:1E - Assigned to Pingtel IP Phones. 00:01:E3 - Assigned to Siemens IP Phones. 00:60:B9 - Assigned to NEC/Philips IP Phones. 00:0F:E2 - Assigned to H3C IP Phones. 00:09:6E - Assigned to Avaya IP Phones.
Index	Displays the voice VLAN OUI sequence ID.
OUI Address	This is the globally unique ID assigned to a vendor by the IEEE to identify VoIP equipment.
Description	Displays the ID of the VoIP equipment vendor.



SonicWall Switch 8-Port

Voice VLAN

/ Switch / VLAN / Voice VLAN

#	MAC ADDESSR	DESCRIPTION
1	00:01:E3	SIEMENS
2	00:03:6B	CISCO
3	00:09:6E	AVAYA
4	00:0F:E2	Huawei-3COM
5	00:60:B9	NEC/Philips
6	00:D0:1E	PINTEL
7	00:E0:75	Veritel Polycom
8	00:E0:BB	3COM

Total: 8 item(s)

Port Settings

Voice VLAN provides QoS to VoIP, ensuring that the quality of voice does not deteriorate if the IP traffic is received unevenly.

Port	Displays the port to which the Voice VLAN settings are applied.
State	Select Enabled to enhance VoIP quality on the selected port. The default is Disabled.
CoS Mode	Select Src or All from the list. • **Src** : Src QoS attributes are applied to packets with OUIs in the source MAC address • **All** : QoS attributes are applied to packets that are classified to the Voice VLAN.
Operate Status	Displays the operating status for the Voice VLAN on the selected port.

Click **Apply** to update the system settings.

Logging

The Syslog Protocol allows devices to send event notification messages in response to events, faults, or errors occurring on the platform as well as changes in configuration or other occurrences across an IP network to syslog servers. It then collects the event messages, providing powerful support for users to monitor network operation and diagnose malfunctions. A Syslog-enabled device can generate a syslog message and send it to a Syslog server.

Syslog is defined in RFC 3164. The RFC defines the packet format, content, and system log related information of Syslog messages. Each Syslog message has a facility and severity level. The Syslog facility identifies a file in the Syslog server. Refer to the documentation of your Syslog program for details. The following table describes the Syslog severity levels.

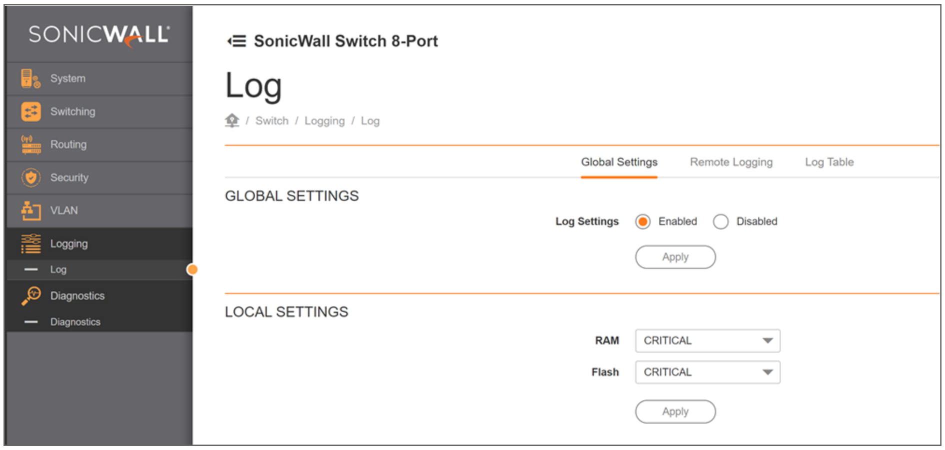
Code	Severity	Description	General Description
0	Emergency	System is unusable	An emergency condition usually affecting multiple apps/ servers/sites. Direct Attention is required.
1	Alert	Actions must be taken immediately	Should be corrected immediately. Notify staff who can fix the problem promptly.
2	Critical	Critical conditions	Should be corrected immediately, but indicates failure in a secondary system.
3	Error	Error conditions	Non-urgent failures, these should be relayed to developers or admins; each item should be resolved promptly.

4	Warning	Warning conditions	Warning message that indicates an error will occur if action is not taken.
5	Notice	Normal but significant conditions	Events that are unusual but not error inducing. No immediate action required.
6	Informational	Informational message	Normal operational status may be gained for reporting procedures.
7	Debug	Debug-level messages	Information useful to developers for debugging applications.

Global Settings

From here, you can Enable or Disable the Log settings for the Switch.

Use the radio buttons to enable or disable the system log.



SonicWall Switch 8-Port

Log

Switch / Logging / Log

GLOBAL SETTINGS

Log Settings ● Enabled ○ Disabled

LOCAL SETTINGS

RAM: CRITICAL

Flash: CRITICAL

Click **Apply** to update the system settings.

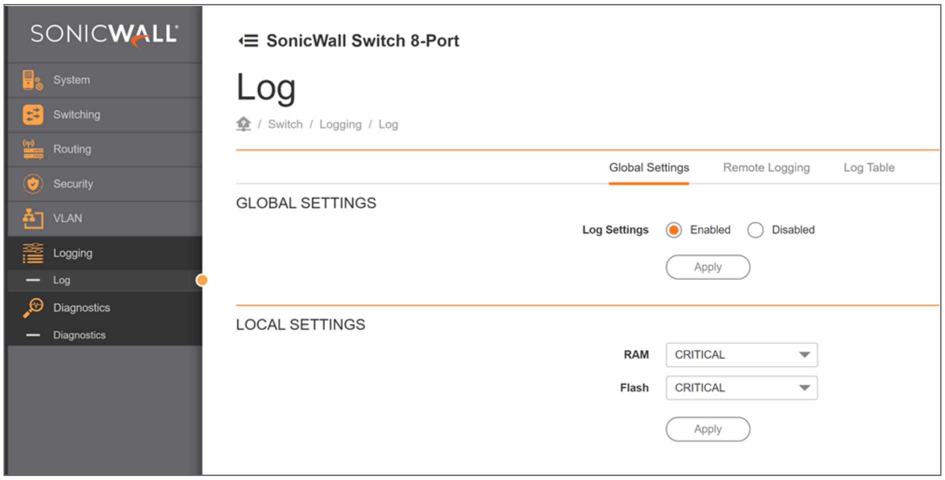
Local Settings

The Switch supports log output to two directions: Flash and RAM. The information stored in the system's Flash log will be lost after the Switch is rebooted or powered off, whereas the information stored in the system's RAM will be kept effective even if the Switch is rebooted or powered off.

Logs with the selected severity level and all logs of greater severity are sent to the host. For example, if you select Error, the logged messages include Error, Critical, Alert, and Emergency.

Target	The method for saving the switch log, to Flash, RAM or both.

Flash	Log erased after reboot or power off
RAM	Log stored in RAM. Will only be erased after system reset.
Severity Level	Refer to severity level table.
EMERGENCY	Select Yes or No from the list. If the Switch is not functioning properly, an emergency log message is saved to the specified logging location.
ALERT	Select Yes or No from the list. If there is a serious Switch malfunction, then all Switch features are down.
CRITICAL	Select Yes or No from the list. A critical log is saved if a critical Switch malfunction occurs.
ERROR	Select Yes or No from the list. If triggered, a device error has occurred.
WARNING	Select Yes or No from the list. The device is functioning, but an operational problem has occurred.
NOTICE	Select Yes or No from the list. This will provide information about the Switch.
INFO	Select Yes or No from the list. This will provide information about the Switch.
DEBUG	Select whether the Yes or No from the list. This will provide a debugging message.



SonicWall Switch 8-Port

Log

/ Switch / Logging / Log

Global Settings Remote Logging Log Table

GLOBAL SETTINGS

Log Settings ● Enabled ○ Disabled

Apply

LOCAL SETTINGS

RAM CRITICAL

Flash CRITICAL

Apply

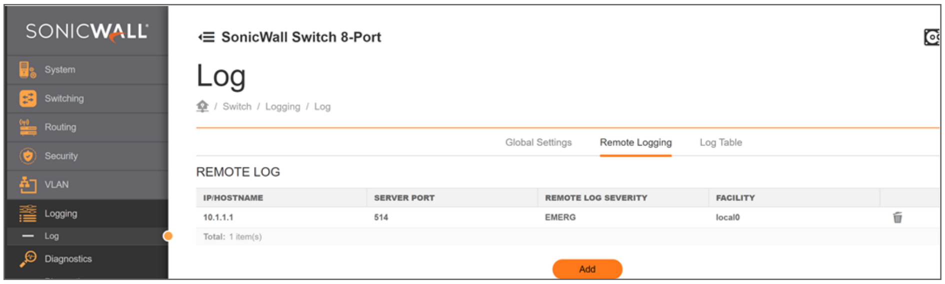
Click **Apply** to accept the changes or **Cancel** to discard them.

Remote Logging

Remote logging enables the Switch to send system logs to the Log Server. The Log Server helps to centralize system logs from various devices such as Access Points so that the user can monitor and manage the whole network. Click the Add button and select the severity level of events you wish to log.

IP/Hostname	Specify the IP address or host name of the host configured for the Syslog.
Server Port	Specify the port on the host to which Syslog messages are sent. The default port is 514.

Remote Log Severity	Refer to severity level table on page 25 or 27. Logs with the selected severity level and all logs of greater severity are sent to the host. For example, if you select Error, the logged messages include Error, Critical, Alert, and Emergency
Facility	The log facility is used to separate out log messages by application or by function, allowing you to send logs to different files in the syslog server. Use the drop-down menu to select local0, local1, local2, local3, local4, local5, local6, or local7.



REMOTE LOG

IP/HOSTNAME	SERVER PORT	REMOTE LOG SEVERITY	FACILITY
10.1.1.1	514	EMERG	local0

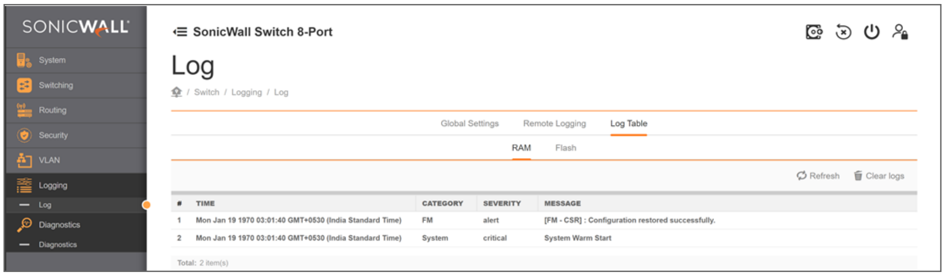
Total: 1 item(s)

Click **Apply** to accept the changes or **Cancel** to discard them.

Log Table

From here, users can view and delete the history log. Select the Log Target you wish to view from the drop- down box.

Index	A counter incremented whenever an entry to the Switch’s history log is made. It displays the last entry (highest sequence number) first.
Time	Displays the time of the log entry.
Category	Displays the category of the history log entry. for example, If the name of a VLAN group is changed, the category will display “VLAN”. If a device is connected to the Switch, the category will display “Port”.
Severity	Displays the level of severity of the log entry. Messages are assigned a severity code.
Message	Displays text describing the event that triggered the history log entry.



#	TIME	CATEGORY	SEVERITY	MESSAGE
1	Mon Jan 19 1970 03:01:40 GMT+0530 (India Standard Time)	FM	alert	[FM - CSR] : Configuration restored successfully.
2	Mon Jan 19 1970 03:01:40 GMT+0530 (India Standard Time)	System	critical	System Warm Start

Total: 2 item(s)

Click **Clear Logs** to clear the buffered log in the memory Diagnostics.

Diagnostics

This section provides you the configuration information for the following:

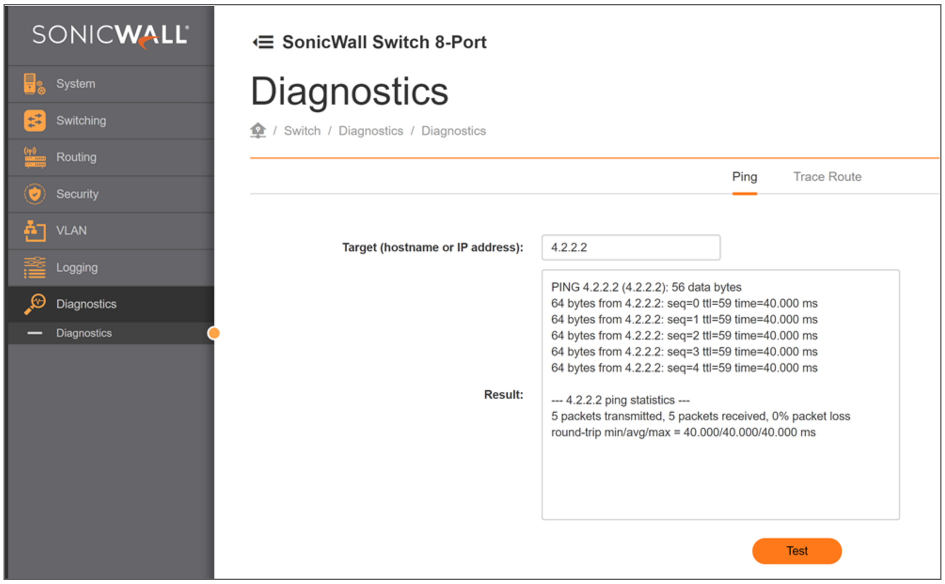
- Ping
- Trace Route
- Download required tech support files

Ping

The Packet INternet Groper (Ping)Test allows you to verify connectivity to remote hosts. The Ping test operates by sending Internet Control Message Protocol (ICMP) request packets to the tested host and waits for an ICMP response. In the process it measures the time from transmission to reception and records any packet loss.Send a ping request to a specified IPv4 address. Check whether the Switch can communicate with a particular network host before testing.

You can vary the test parameters by entering the data in the appropriate boxes. To verify accuracy of the test, it is recommended that you run multiple tests in case of a test fault or user error.

Target	Enter the IP address or the host name of the station you want the Switch to ping to.
Result	Displays the Ping Test results.



Target (hostname or IP address): 4.2.2.2

Result:

```
PING 4.2.2.2 (4.2.2.2): 56 data bytes
64 bytes from 4.2.2.2: seq=0 ttl=59 time=40.000 ms
64 bytes from 4.2.2.2: seq=1 ttl=59 time=40.000 ms
64 bytes from 4.2.2.2: seq=2 ttl=59 time=40.000 ms
64 bytes from 4.2.2.2: seq=3 ttl=59 time=40.000 ms
64 bytes from 4.2.2.2: seq=4 ttl=59 time=40.000 ms

--- 4.2.2.2 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 40.000/40.000/40.000 ms
```

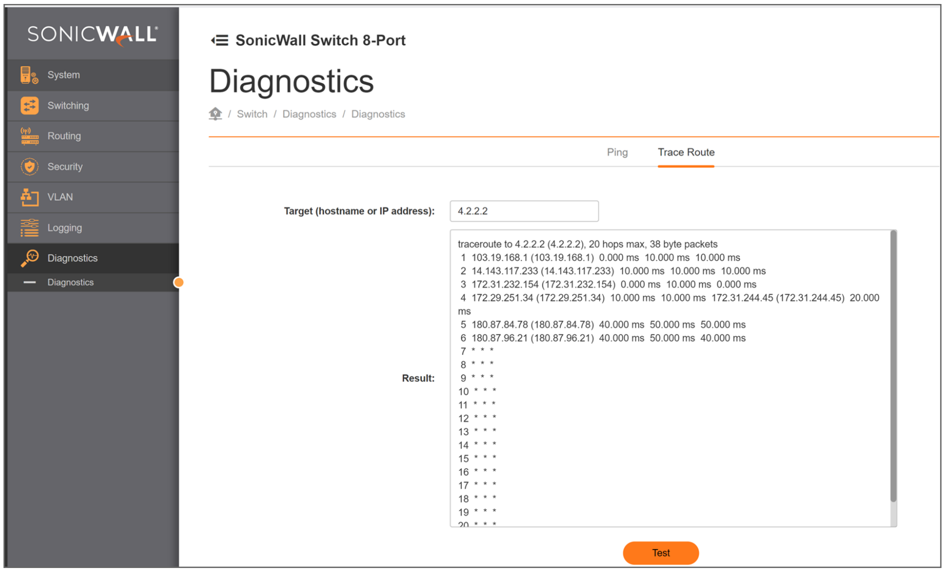
Trace Route

The traceroute feature is used to discover the routes that packets take when traveling to their destination. It will list all the routers it passes through until it reaches its destination, or fails to reach the destination and is discarded.

In testing, it will tell you how long each hop from router to router takes via the trip time of the packets it sends and receives from each successive host in the route.

Target	Enter the IP address or the host name of the station you wish the Switch to ping to.
Result	Displays the trace route results.

Click **Test** to initiate the trace route.



Target (hostname or IP address): 4.2.2.2

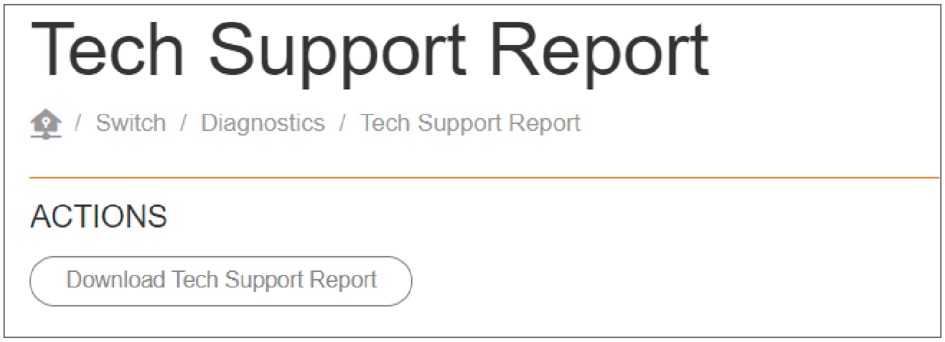
Result:

```
traceroute to 4.2.2.2 (4.2.2.2), 20 hops max, 38 byte packets
 1  103.19.168.1 (103.19.168.1)  0.000 ms  10.000 ms  10.000 ms
 2  14.143.117.233 (14.143.117.233)  10.000 ms  10.000 ms  10.000 ms
 3  172.31.232.154 (172.31.232.154)  0.000 ms  10.000 ms  0.000 ms
 4  172.29.251.34 (172.29.251.34)  10.000 ms  10.000 ms  172.31.244.45 (172.31.244.45)  20.000
ms
 5  180.87.84.78 (180.87.84.78)  40.000 ms  50.000 ms  50.000 ms
 6  180.87.96.21 (180.87.96.21)  40.000 ms  50.000 ms  40.000 ms
 7  * * *
 8  * * *
 9  * * *
10  * * *
11  * * *
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
```

Download required tech support files

To download required tech support files:

1. Go to Switch > Diagnostics > Tech Support Report.
2. Click Download Tech Support Report.

   Tech Support Report

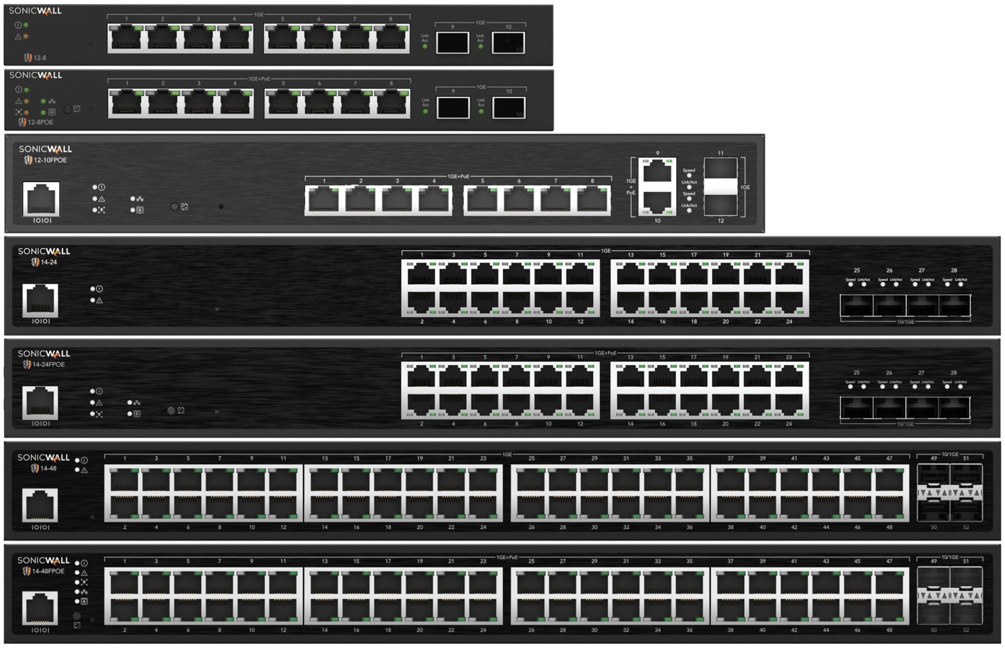
   / Switch / Diagnostics / Tech Support Report

   ACTIONS

   A Confirmation dialog appears.
3. Click **Confirm** to download the Tech support report.

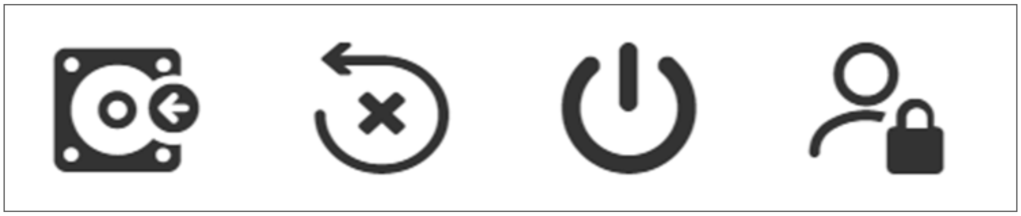
3

System Maintenance



Maintenance functions are available from the maintenance bar. Maintenance functions include: upgrading firmware, resetting the configuration to factory default standards, rebooting the device, and logging out of the interface.

The following represents the Maintenance Menu bar:

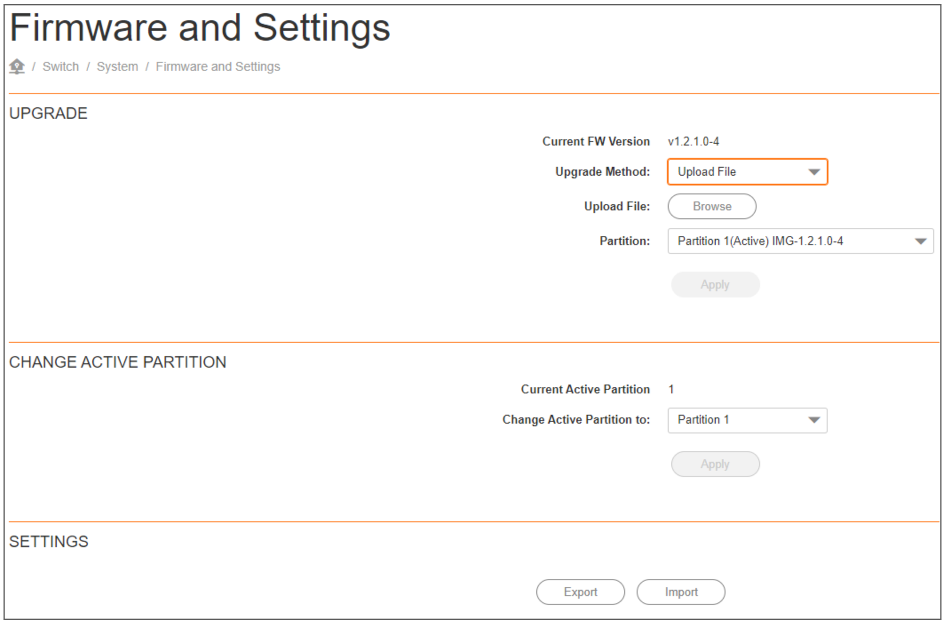


Upgrading

You can upgrade the firmware using two methods.

Follow this procedure to upgrade the Firmware using Upload File method:

1. Click to start the upgrade process.
2. In the **Upgrade Method**drop-down, select **Upload File** option.
3. Click **Browse** to the select the location where you have stored your new firmware file.
4. Select the new firmware file and click **Open**.
5. In the **Partition** drop-down, select the required partition for the upgrade process.
6. Click **Apply** and follow the on-screen instructions to complete the Firmware Upgrade.



Firmware and Settings

/ Switch / System / Firmware and Settings

UPGRADE

Current FW Version v1.2.1.0-4

Upgrade Method: Upload File

Upload File:

Partition: Partition 1(Active) IMG-1.2.1.0-4

CHANGE ACTIVE PARTITION

Current Active Partition 1

Change Active Partition to: Partition 1

SETTINGS

A prompt displays to confirm the Firmware Upgrade.

ⓘ | **NOTE:** The Upgrade process may require a few minutes to complete.

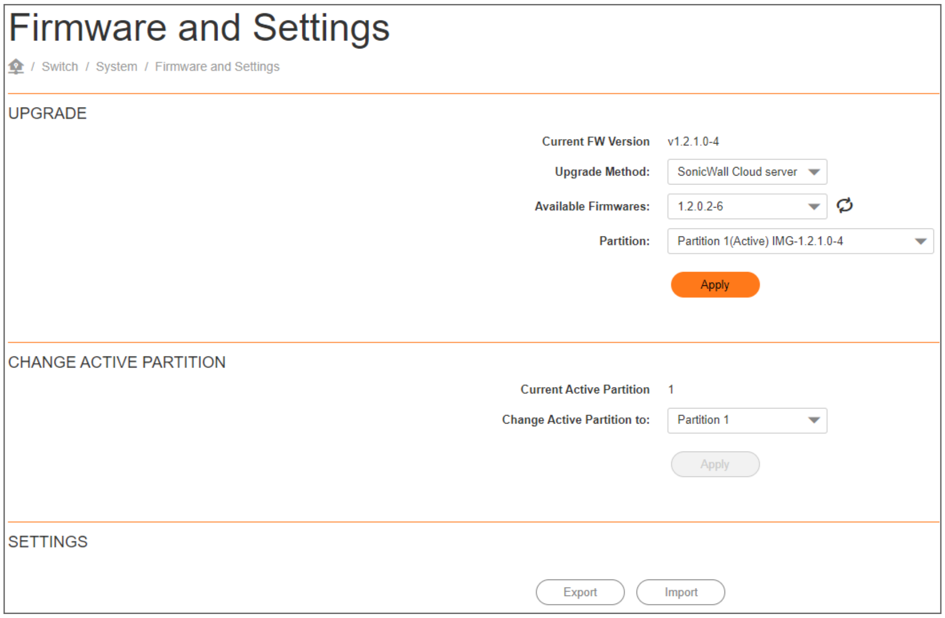
Follow this procedure to upgrade the Firmware using SonicWall Cloud Server method:

1. Click to start the upgrade process.
2. In the **Upgrade Method** drop-down, select **SonicWall Cloud server** option.
3. In the **Available Firmwares** drop-down, select the required firmware you want to upgrade.

4. Click ⟳ to fetch the latest firmwares from **SonicWall Cloud server**.
5. In the **Partition** drop-down, select the required partition for the upgrade process.
6. Click **Apply** and follow the on-screen instructions to complete the Firmware Upgrade.

   A prompt displays to confirm the Firmware Upgrade.

ⓘ | **NOTE:** The Upgrade process may require a few minutes to complete.



Firmware and Settings

Switch / System / Firmware and Settings

UPGRADE

Current FW Version: v1.2.1.0-4

Upgrade Method: SonicWall Cloud server

Available Firmwares: 1.2.0.2-6

Partition: Partition 1(Active) IMG-1.2.1.0-4

CHANGE ACTIVE PARTITION

Current Active Partition: 1

Change Active Partition to: Partition 1

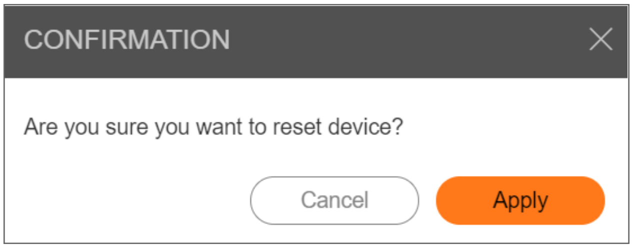
SETTINGS

Resetting

⚠ | **WARNING: The Reset function will delete all configuration information from the current device.**

Follow this procedure to reset the Switch back to factory default settings:

1. Click ⊗ to start the reset process.
2. When a prompt displays, click **Apply** to confirm the reset or **Cancel** to quit the procedure.

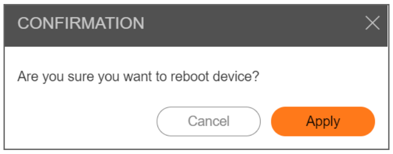


Are you sure you want to reset device?

Rebooting

Follow this procedure to reboot the Switch:

1. Click ⏻ to start the reboot process.
2. When a prompt displays, click **Apply** to confirm the reboot process or **Cancel** to quit the procedure.

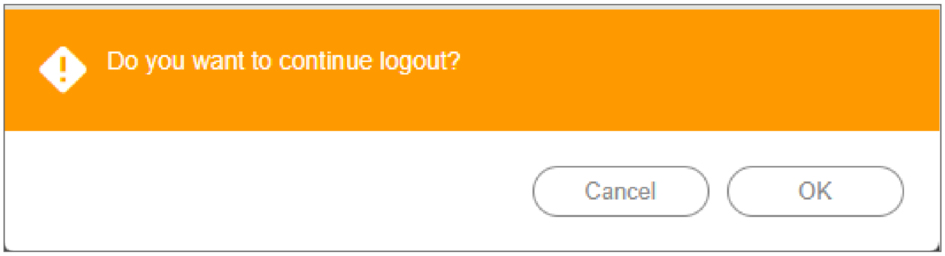


Are you sure you want to reboot device?

Logging Out

Follow this procedure to log out the current profile from the user interface:

1. Click 🔒 icon in the Maintenance menu bar.
2. When a prompt displays, click **OK** to confirm the logout or **Cancel** to quit the logout.



Do you want to continue logout?

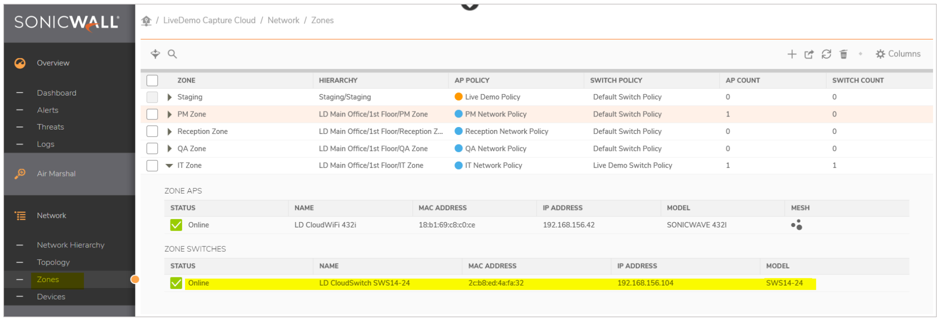
You are logged out from the Switch application.

4

Switch Troubleshooting

Steps to create VLAN from WNM on the switch

- Log into the WCM portal
- Make sure the switches are part of zones and online in the **Device** section.
- To ensure Navigate to **Network>>Zones.**



/ LiveDemo Capture Cloud / Network / Zones

ZONE	HIERARCHY	AP POLICY	SWITCH POLICY	AP COUNT	SWITCH COUNT
Staging	Staging/Staging	Live Demo Policy	Default Switch Policy	0	0
PM Zone	LD Main Office/1st Floor/PM Zone	PM Network Policy	Default Switch Policy	1	0
Reception Zone	LD Main Office/1st Floor/Reception Z...	Reception Network Policy	Default Switch Policy	0	0
QA Zone	LD Main Office/1st Floor/QA Zone	QA Network Policy	Default Switch Policy	0	0
IT Zone	LD Main Office/1st Floor/IT Zone	IT Network Policy	Live Demo Switch Policy	1	1

ZONE APS

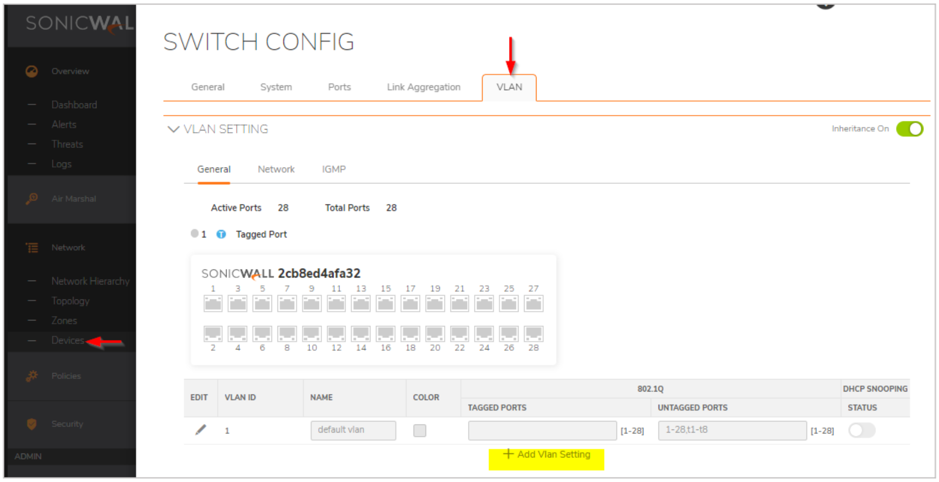
STATUS	NAME	MAC ADDRESS	IP ADDRESS	MODEL	MESH
✓ Online	LD CloudWiFi 432i	18:b1:69:c8:c0:ce	192.168.156.42	SONICWAVE 432I	

ZONE SWITCHES

STATUS	NAME	MAC ADDRESS	IP ADDRESS	MODEL
✓ Online	LD CloudSwitch SWS14-24	2c:b8:ed:4a:fa:32	192.168.156.104	SWS14-24

- Navigate to **Network>>Devices>>Switches>>edit>>VLAN**.

ⓘ | **NOTE:** This only if you have 1 switch and not using the switch policy.



SWITCH CONFIG

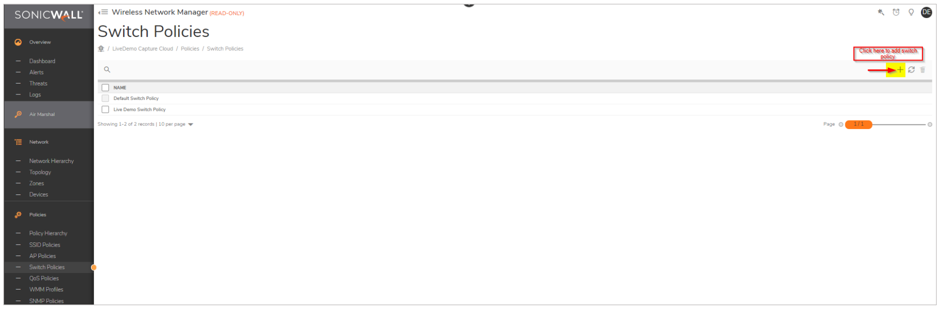
VLAN SETTING

Active Ports 28 Total Ports 28

1 T Tagged Port

EDIT	VLAN ID	NAME	COLOR	802.1Q		DHCP SNOOPING
				TAGGED PORTS	UNTAGGED PORTS	STATUS
✎	1	default vlan	□	[1-28]	1-28,t1-t8 [1-28]	○

- If you have More than 1 Switch then make use of switch policies, for this Navigate to **Policies>>Switch Policies**, Click on **Add**.



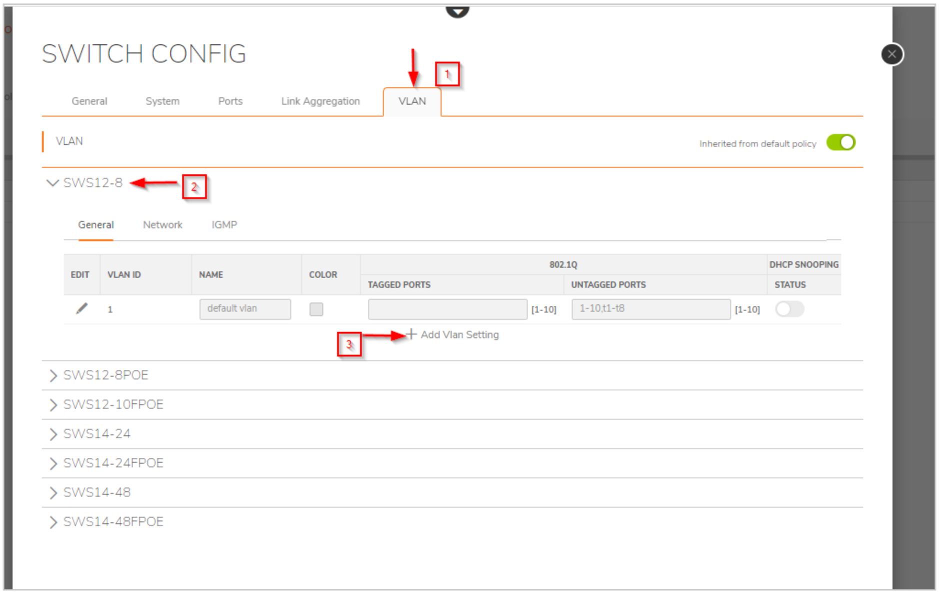
Switch Policies

/ LiveDemo Capture Cloud / Policies / Switch Policies

□ NAME
□ Default Switch Policy
□ Live Demo Switch Policy

Showing 1-2 of 2 records | 10 per page

- Now Go to **VLAN**, select the switch model to which you want to add VLAN, Click on **Add VLAN settings**.

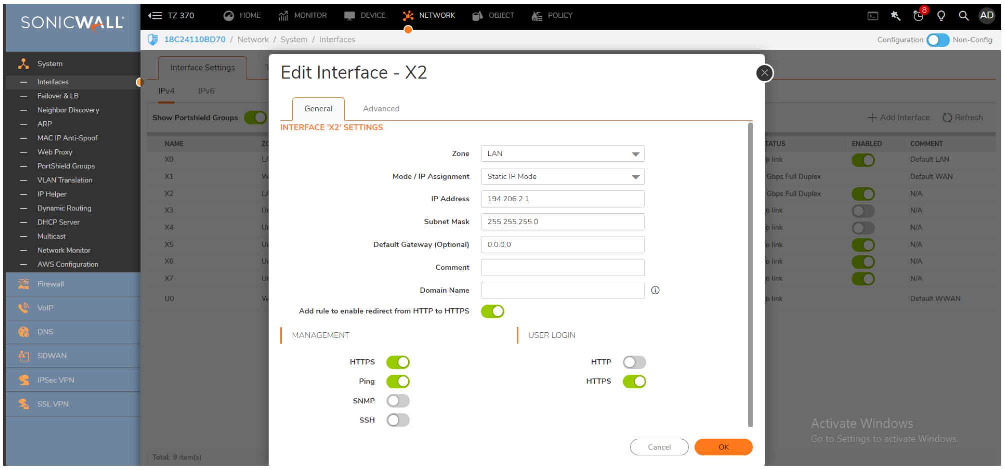


EDIT	VLAN ID	NAME	COLOR	802.1Q		DHCP SNOOPING
				TAGGED PORTS	UNTAGGED PORTS	STATUS
✎	1	default vlan	□	[1-10]	1-10,t1-t8 [1-10]	○

Communication flow between Firewall and Switch before it get authenticated

ⓘ **IMPORTANT:** If switch **Auto-Discovery** is not working when a third party switch is in the middle between SW firewall and SW switch. where LLDP packets are not forwarded, in such case you can add the switch manually.

Configure Interface in LAN zone which is connected from firewall to switch. Navigate to **Network>interfaces** select the interface(X2) and click on Edit.



Edit Interface - X2

INTERFACE 'X2' SETTINGS

Zone: LAN
Mode / IP Assignment: Static IP Mode
IP Address: 194.206.2.1
Subnet Mask: 255.255.255.0
Default Gateway (Optional): 0.0.0.0
Comment:
Domain Name:
Add rule to enable redirect from HTTP to HTTPS: On

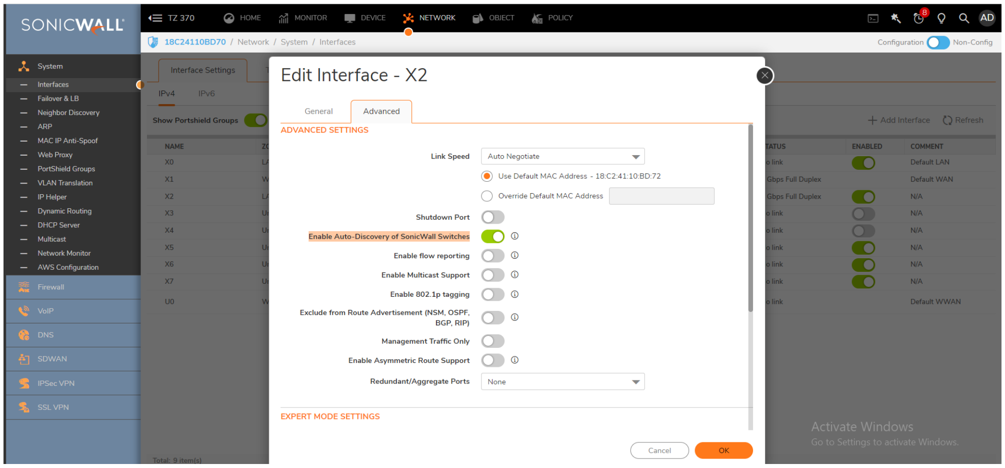
MANAGEMENT
- HTTPS: On
- Ping: On
- SNMP: Off
- SSH: Off

USER LOGIN
- HTTP: Off
- HTTPS: On

NAME	ZO	STATUS	ENABLED	COMMENT
X0	LA	o link	On	Default LAN
X1	W	Gbps Full Duplex		Default WAN
X2	LA	Gbps Full Duplex	On	N/A
X3	U	o link	Off	N/A
X4	U	o link	Off	N/A
X5	U	o link	On	N/A
X6	U	o link	On	N/A
X7	U	o link	On	N/A
U0	W	o link		Default WWAN

In the Same interface edit and go to **Advanced** tab and enable the toggle button **Enable Auto-Discovery of SonicWall Switches**.

ⓘ **NOTE:** Max of eight switches can be added to the firewall.



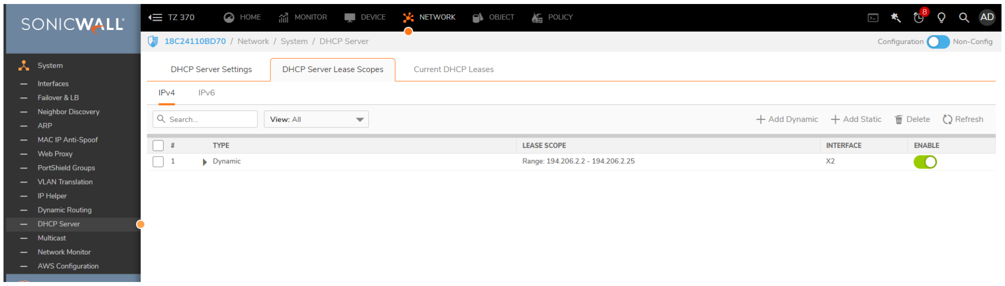
Edit Interface - X2

ADVANCED SETTINGS

Link Speed: Auto Negotiate
● Use Default MAC Address - 18:C2:41:10:BD:72
○ Override Default MAC Address
Shutdown Port: Off
Enable Auto-Discovery of SonicWall Switches: On
Enable flow reporting: Off
Enable Multicast Support: Off
Enable 802.1p tagging: Off
Exclude from Route Advertisement (NSM, OSPF, BGP, RIP): Off
Management Traffic Only: Off
Enable Asymmetric Route Support: Off
Redundant/Aggregate Ports: None

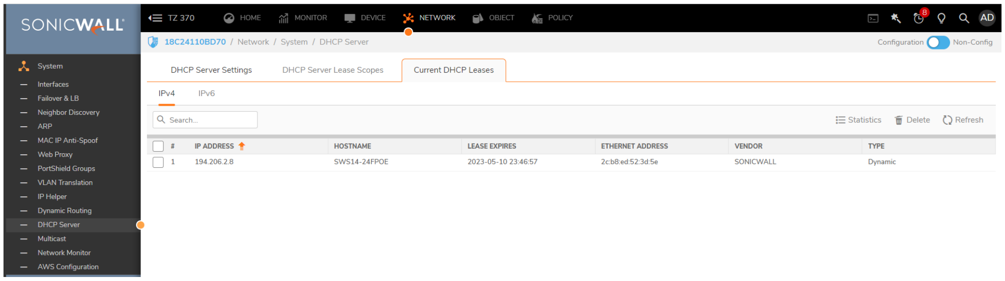
EXPERT MODE SETTINGS

Now, check and confirm if **DHCP Server lease scopes** is enabled for that interface.



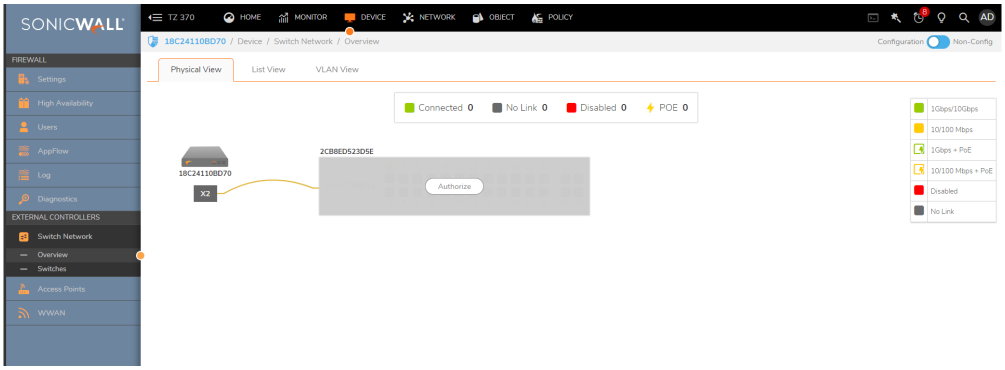
#	TYPE	LEASE SCOPE	INTERFACE	ENABLE
1	Dynamic	Range: 194.206.2.2 - 194.206.2.25	X2	●

Once the switch gets an IP from the interface (X2) check and confirm from the **Current DHCP Leases** tab.

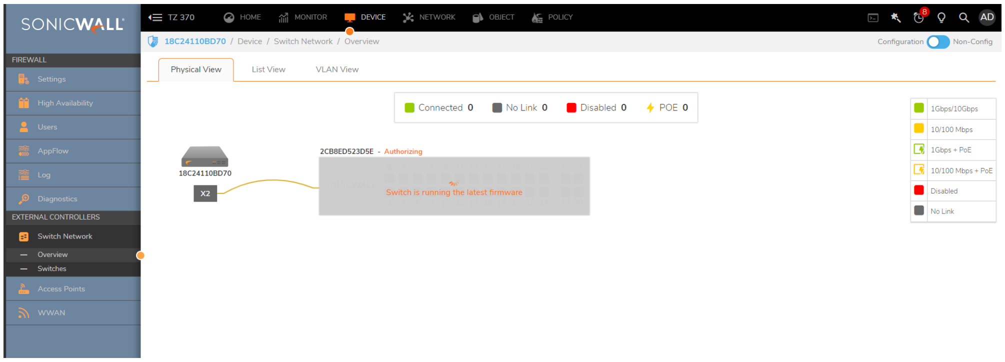


#	IP ADDRESS	HOSTNAME	LEASE EXPIRES	ETHERNET ADDRESS	VENDOR	TYPE
1	194.206.2.8	SWS14-24FPOE	2023-05-10 23:46:57	2c:b8:ed:52:3d:5e	SONICWALL	Dynamic

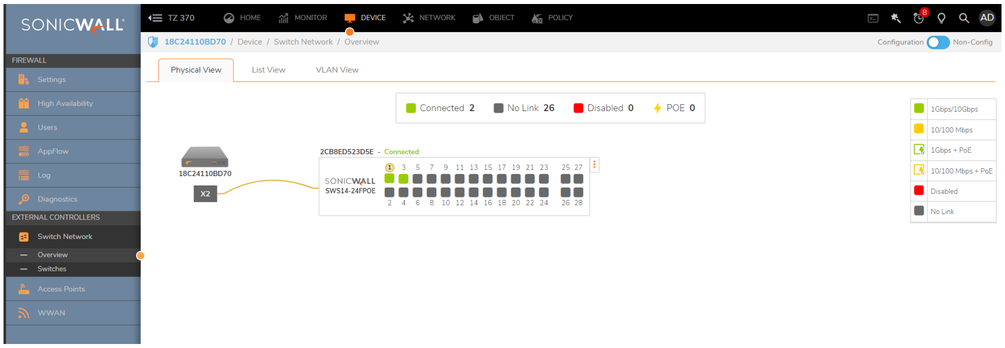
Navigate to **External Controllers**> **Overview**>**Physical View** and check for switch getting authorized.



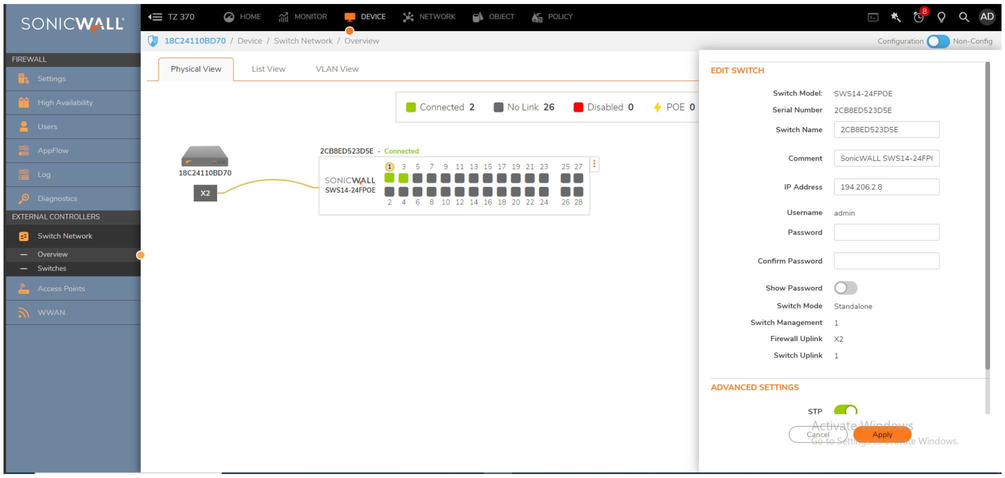
Click on **authorize** button



After completing authorization the switch gets added successfully.



Now, you can edit the Switch configuration.



EDIT SWITCH

Switch Model: SWS14-24FPOE
Serial Number 2CB8ED523D5E
Switch Name 2CB8ED523D5E
Comment SonicWALL SWS14-24FP(
IP Address 194.206.2.8
Username admin
Password
Confirm Password
Show Password ○
Switch Mode Standalone
Switch Management 1
Firewall Uplink X2
Switch Uplink 1

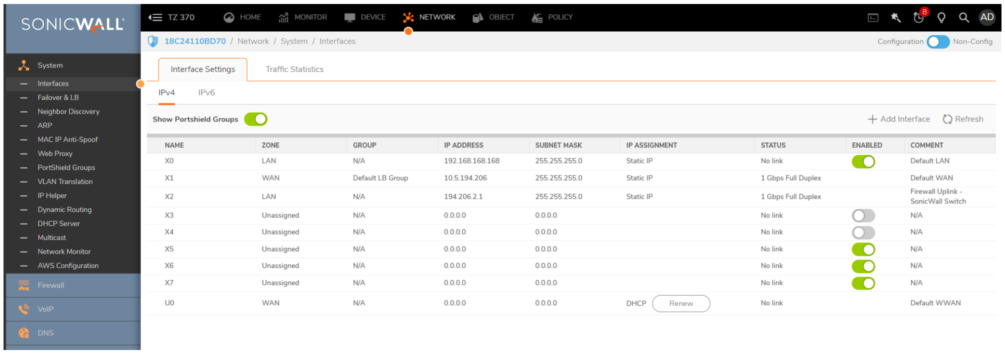
ADVANCED SETTINGS

STP ●

Cancel Apply

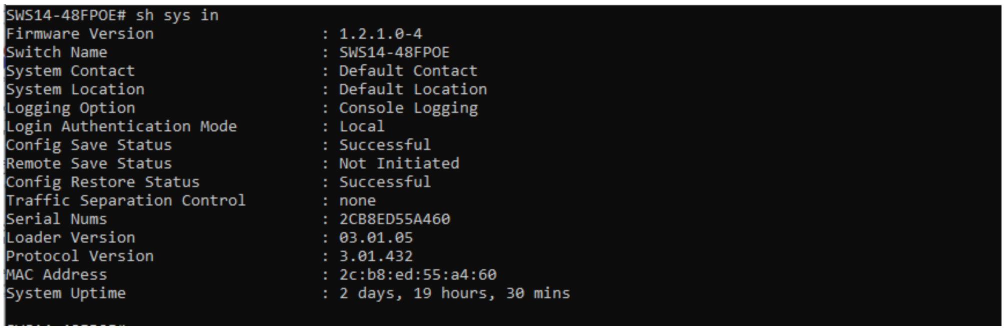
Activate Windows
Go to Settings to activate Windows.

you can view the X2 interface comment section.



NAME	ZONE	GROUP	IP ADDRESS	SUBNET MASK	IP ASSIGNMENT	STATUS	ENABLED	COMMENT
X0	LAN	N/A	192.168.168.168	255.255.255.0	Static IP	No link	●	Default LAN
X1	WAN	Default LB Group	10.5.194.206	255.255.255.0	Static IP	1 Gbps Full Duplex		Default WAN
X2	LAN	N/A	194.206.2.1	255.255.255.0	Static IP	1 Gbps Full Duplex		Firewall Uplink - SonicWall Switch
X3	Unassigned	N/A	0.0.0.0	0.0.0.0		No link	○	N/A
X4	Unassigned	N/A	0.0.0.0	0.0.0.0		No link	○	N/A
X5	Unassigned	N/A	0.0.0.0	0.0.0.0		No link	●	N/A
X6	Unassigned	N/A	0.0.0.0	0.0.0.0		No link	●	N/A
X7	Unassigned	N/A	0.0.0.0	0.0.0.0		No link	●	N/A
U0	WAN	N/A	0.0.0.0	0.0.0.0	DHCP Renew	No link		Default WWAN

View the Switch CLI information



```
SWS14-48FPOE# sh sys in
Firmware Version                 : 1.2.1.0-4
Switch Name                      : SWS14-48FPOE
System Contact                   : Default Contact
System Location                  : Default Location
Logging Option                   : Console Logging
Login Authentication Mode        : Local
Config Save Status               : Successful
Remote Save Status               : Not Initiated
Config Restore Status            : Successful
Traffic Separation Control       : none
Serial Nums                      : 2CB8ED55A460
Loader Version                   : 03.01.05
Protocol Version                 : 3.01.432
MAC Address                      : 2c:b8:ed:55:a4:60
System Uptime                    : 2 days, 19 hours, 30 mins
```

If the switch add is stuck in authorize state and after rebooting the firewall if the switch is not yet added , and also switch add fails after this case, then please follow the below steps:

1. Check from switch CLI whether you are able to reach the firewall interface (Ping).
2. If the switch and firewall communication is working still the switch state is **authorized** state or **stuck** then Reboot the firewall.
3. If the issue still remains same then remove and add the switch once again(In this scenario you need to factory reset and add).
4. Under **Firewall** > **Configure terminal** > **clear switch-database**

   ⚠ **WARNING: this will clear all the switch data that is present in the firewall, Please do not use this case when multiple switches are added and issue is seen while adding a new switch, this command will clear all the switch data and needs to add all the switch from the beginning.**
5. Reset the switch to Factory default.
6. Once the switch gets the IP from the DHCP range, it appears to authorize the switch.

Daisy chain mode using SonicWall Switches

To setup a Daisy Chain mode using Sonicwall Switches refer to Daisy chain mode using SonicWall Switches.

Add SonicWall Switch manually to SonicWall UTM

To add SonicWall switch manually to the SonicWall UTM without using auto-discovery feature refer to How to add SonicWall Switch manually to SonicWall UTM

Deploy SonicWall switches when SonicWall UTM is in High availability mode

The switches can be deployed with one or two dedicated uplinks and also with common uplinks, refer to How to deploy SonicWall switches when SonicWall UTM is in High availability mode

Building LACP between SonicWall firewall and switch firewall

To build LACP between SonicWall firewall and switch firewall refer to How to build LACP between SonicWall firewall and switch firewall using 10G port

6

SonicWall Support

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

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

The Support Portal enables you to:

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

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

About This Document

Switch Administration Guide
Updated - March 2024
232-005592-00 Rev F

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