Switch

Administration Guide

SONICWALL®

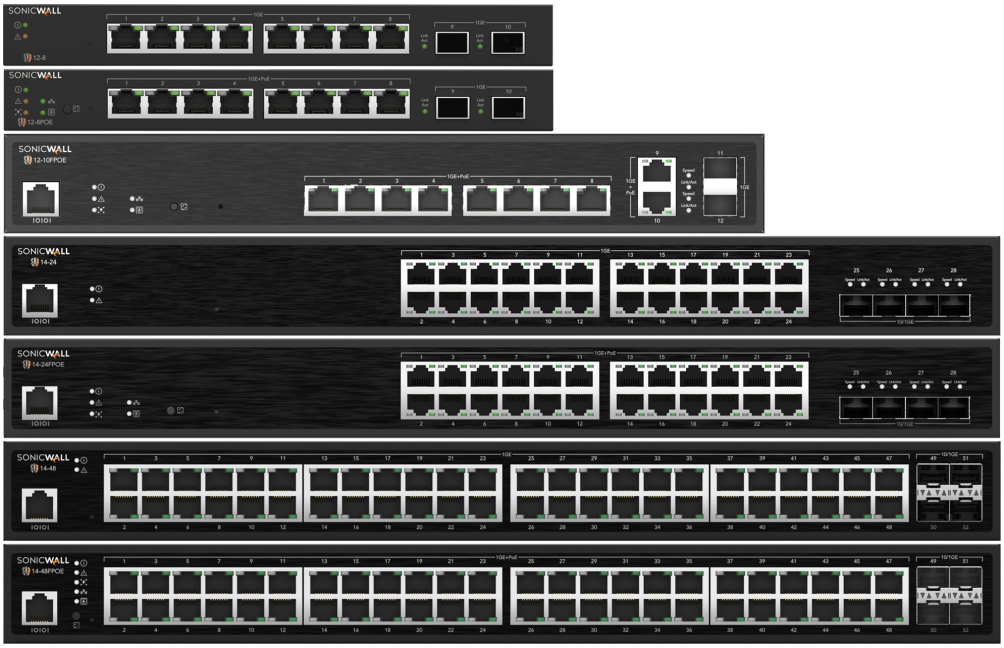
Contents

1

Product Overview

The SonicWall Switch can be managed through Wireless Network Manager (WNM), SonicWall a firewall, or a standalone/local user interface. This guide focuses on the administrative management via the local user interface.

To learn more about managing SonicWall Switch via Firewall, refer to SonicOS Switch Network Administrator Guide and via WNM, refer to the Wireless Network Manager Administrator Guide.



The SonicWall Switches are layer 2 devices specially designed to support PoE-capable and Ethernet-based network devices.

Switch Series Features - Across All Models:

- Provides simple, yet powerful PoE manageability with features such as IEEE 802.3af or IEEE 802.3at/af ports.
- Security and Visibility features like:

    - MAB (MAC authentication bypass)
    - DHCP Snooping
    - 802.1x authentication
    - Syslog collection
    - IP/MAC ACL
    - ACL
    - IEEE 802.1x authentication port-based
    - IEEE 802.1x guest and Fallback VLAN
- Layer 2 features like:
    - Jumbo frames
    - Auto-negotiation for port speed and duplex
    - MDI/MDIX auto-crossover
    - MAC bridging/STP
    - Rapid Spanning Tree Protocol (RSTP)

Package Contents

Your 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)

Technical Specifications

NOTE: 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. 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.

	SWS12-8	SWS12-8POE
1 Gb RJ45	8	8
1 Gb SFP1	2	2
Fans	-	-
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 — 40°C	0 — 40°C
Humidity (non-condensing)	5 — 95%	5 — 95%

	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+		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 — 40°C	0 — 40°C	0 — 40°C	0 — 40°C	0 — 40°C
Humidity (non-condensing)	5 — 95%	5 — 95%	5 — 95%	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)
- LED Indicator

ⓘ | **NOTE:** All ports cannot run at 30 Watts at the same time and are limited to the power limitations per SWS.

Device:

- Power LED x1 Fault LED x1 PoE Max LED x1
- LAN Mode LED x1 PoE Mode LED x1
- RJ45 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

Management Functions:

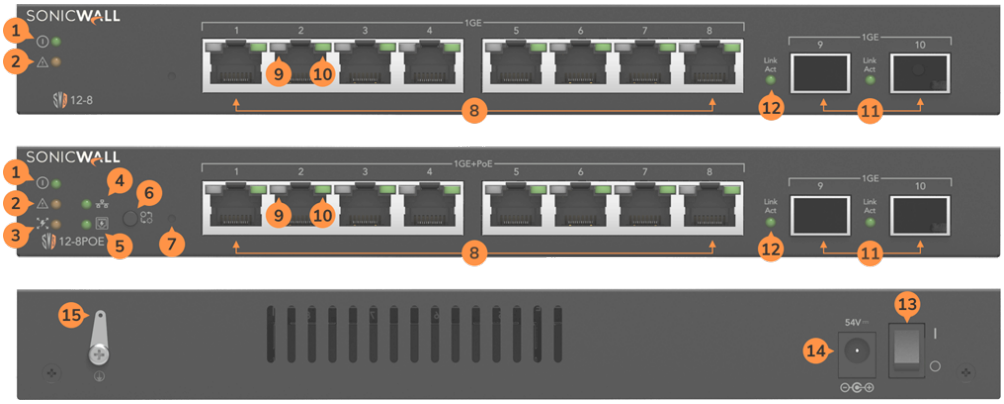
- Attack Prevention- DOS
- Access Control List (ACL)

- 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 third-party SFP and SFP+ Modules

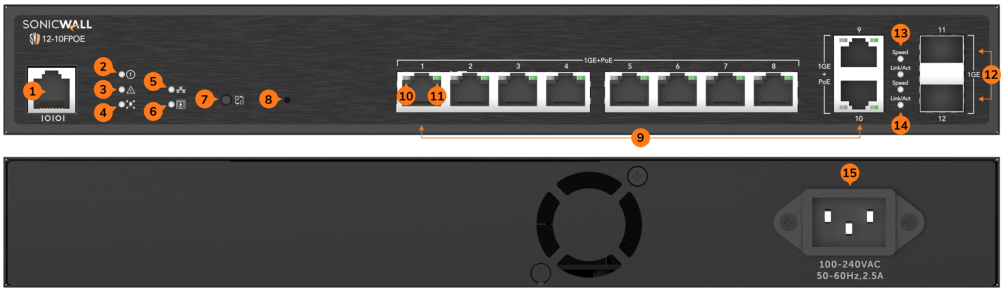
Here is a list of supported third-party SFP and SFP+ modules that are compatible with the switches. Refer to Supported 3rd party SFP and SFP+ modules.

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 = Power Available; Solid Light = Power Exceeded.
4. LAN LED: Light Off = Not activated; Solid Light = Activated.
5. PoE LED: Light Off = Not activated; Solid Light = Activated.
6. LED Mode Selector: Press to change between LAN and PoE LED monitoring.
7. Reset Button: Press to reset the device to factory default settings.
8. RJ45 LAN Ports: 10/100/1000 Mbps or 1 Gbps.
9. LAN LED (Per RJ45 Port): Light Off = No Link; Solid Amber Light = 100 Mbps Link Active; Solid Green Light = 1000 Mbps or 1 Gbps.
10. Link/Act LED (Per RJ45 Port): Light Off = No Link; Solid Light = Link Active; Blinking Light = Actively Transmitting / Receiving.
11. SFP Ports: Small Form-factor Pluggable ports: 1 Gbps ports.
12. Link/Act LED: Light Off = No Link; Solid Light = Link Active; Blinking Light = Actively Transmitting / Receiving.
13. On/Off button.
14. Power Input.
15. Optional connector allows connection to ground.

Physical Interface - 10 Port Switch

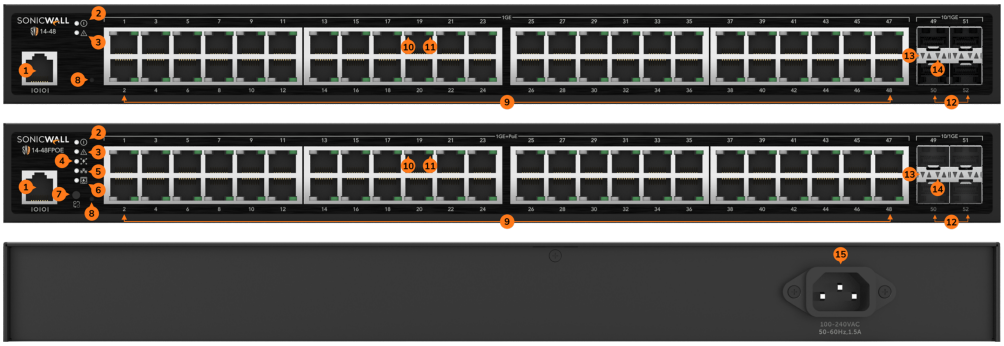


1. RJ45 Console Port
2. Power LED: Light Off = Power Off; Solid Light = Power On.
3. Fault LED: Light Off = Normal Behavior; Solid Light = Error.
4. PoE Max LED: Light Off = Power Available; Solid Light = Power Exceeded.
5. LAN LED: Light Off = Not activated; Solid Light = Activated.
6. PoE LED: Light Off = Not activated; Solid Light = Activated.
7. LED Mode Selector: Press to change between LAN and PoE LED monitoring.
8. Reset Button: Press to reset the device to factory default settings.
9. RJ45 LAN Ports: 10/100/1000 Mbps or 1 Gbps.
10. LAN LED (Per RJ45 Port): Light Off = No Link; Solid Amber Light = 100 Mbps Link Active
11. Link/Act LED (Per RJ45 Port): Light Off = No Link; Solid Light = Link Active; Blinking Light = Actively Transmitting / Receiving.
12. Speed LED (Per SFP Port). Solid Green Light indicates 1 Gbps link.
13. Link/Act LED (Per SFP Port).
14. SFP Ports: Small Form-factor Pluggable ports: 1 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 = Power Available; Solid Light = Power Exceeded.
5. LAN LED: Light Off = Not activated; Solid Light = Activated.
6. PoE LED: Light Off = Not activated; Solid Light = Activated.
7. LED Mode Selector: Press to change between LAN and PoE LED monitoring.
8. Reset Button: Press to reset the device to factory default settings.
9. RJ45 LAN Ports: 10/100/1000 Mbps or 1 Gbps.
10. LAN LED (Per RJ45 Port): Light Off = No Link; Solid Amber Light = 100 Mbps Link Active
11. Link/Act LED (Per RJ45 Port): Light Off = No Link; Solid Light = Link Active; Blinking Light = Actively Transmitting / Receiving.
12. Speed LED (Per SFP Port). Solid Amber Light indicates10 Gbps Link, Solid Green Light indicates 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 = Power Available; Solid Light = Power Exceeded.
5. LAN LED: Light Off = Not activated; Solid Light = Activated.
6. PoE LED: Light Off = Not activated; Solid Light = Activated.
7. LED Selector: Press to change between LAN and PoE LED monitoring.
8. Reset Button: Press to reset the device to factory default settings.
9. RJ45 LAN Ports: 10/100/1000 Mbps or 1 Gbps.
10. LAN Mode LED (Per RJ45 Port): Light Off = No Link; Solid Amber Light = 100 Mbps Link Active.
11. Link/Act LED (Per RJ45 Port): Light Off = No Link; Solid Light = Link Active; Blinking Light = Actively Transmitting / Receiving.
12. Speed LED (Per SFP Port). Solid Amber Light indicates 10 Gbps Link, Solid Green Light indicates 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.

Device Management

The SonicWall Switch features an embedded Web interface for the monitoring and management of the 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. For 8 port switch, 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 (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. On the designated computer, assign a static IP address to the connected Ethernet adapter using 192.168.168.10 with a subnet mask of 255.255.255.0.
5. Using a web browser, browse to https://192.168.168.169
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**.
   ⓘ | **NOTE:** A prompt is displayed to change the password immediately if it is a new installation.
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 Switch in a network without a DHCP server. If the network does not have a DHCP service, a static IP address must be assigned to access the web-based 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 (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. On the designated computer, assign a static IP address to the connected Ethernet adapter using 192.168.168.10 with a subnet mask of 255.255.255.0.

5. Using a web browser, browse to https://192.168.168.169
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**.
   ⓘ | **NOTE:** A prompt is displayed to change the password immediately if it is a new installation.
7. 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.
8. Enter the IP address, Subnet mask, and Gateway.
9. Click **Apply** to update the system.

Capacity Matrix

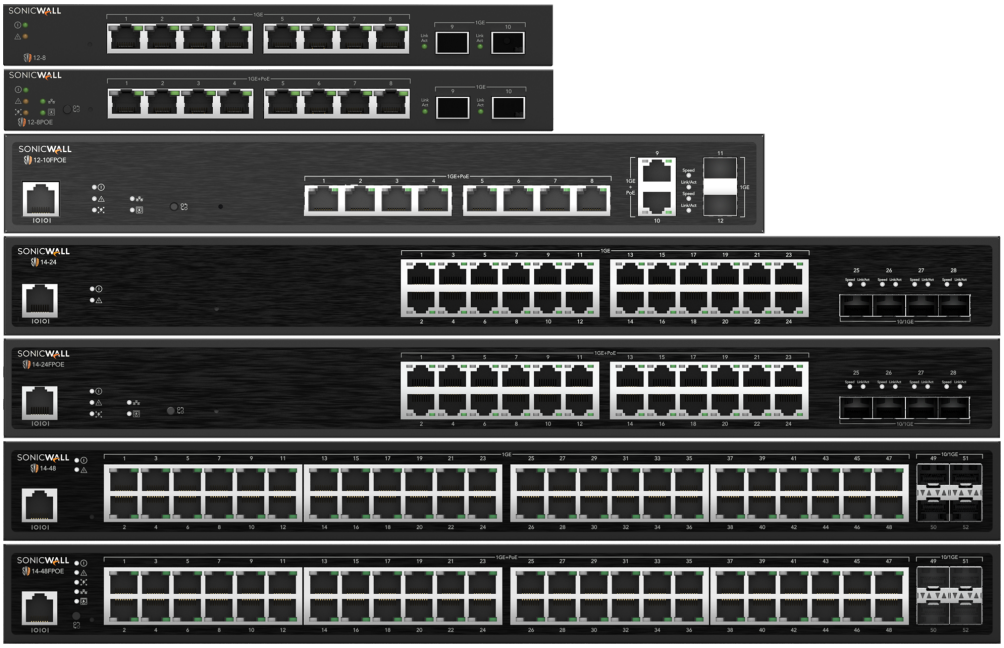
The capacity matrix allows you to view the total maximum capacity entries of various settings, VLAN IDs, names, addresses, and so on that are available for the SonicWall Switch.

Component	Maximum entries
IP Settings	
IPv4 Network VLAN ID	3
ARP table	
Address	Static+Dynamic=1000, Static=256
Static Route	
IPv4- Destination IP	59
DHCP Snooping	
VLAN Settings- VLAN ID	256
Binding list- VLAN ID	254
VLAN Statistics- VLAN ID	256
DHCP Relay	
Server Address	5
Port Trunking	
Group	8
Member Ports	8
Mirror Settings	
Destination Port	1
Source TX Port	19
Source RX Port	19
MST Instance Settings	
MST ID	16
MAC AddressTable	
Static MAC Address- Index	256
Dynamic MAC Address- Index	
SWS12-8, SWS12-8POE, SWS12-10FPOE	8K
SWS14-24, SWS14-24FPOE	32K
SWS14-48, SWS14-48FPOE	32K

Component	Maximum entries
Jumbo Frame	
SWS12 series	1522-9216 bytes
SWS14 series	1522-10240 bytes
802.1Q	
VLAN ID	256
OUI Settings	
Index	16
User Management	
User Name	20
SNMP (maximum entry lengths)	
User Name	82
Community Name	42
Group Name	50
Access List- Group Name	82
View Name	50
Target Parameter Name	10
Target Address Name	10
Notify Name	10
ACL	
MAC ACL	16
MAC ACE	128
IPv4 ACL	16
IPv4 ACE	128
Radius Server	
Index	5
Port Security	
Max MAC Address	256
RMON	
Stat List- Index	60
Event List- Index	50
Alarm List- Index	50
History List- Index	50
Log	
Remote Logging- IP/Hostname	8
Log Table- Display logs in	50

2

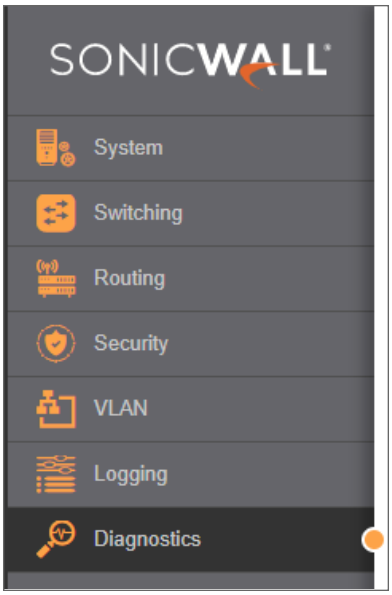
System Management



The navigation pane at the left of the Web browser interface contains a System Management Panel that enables the management of the switch features with 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

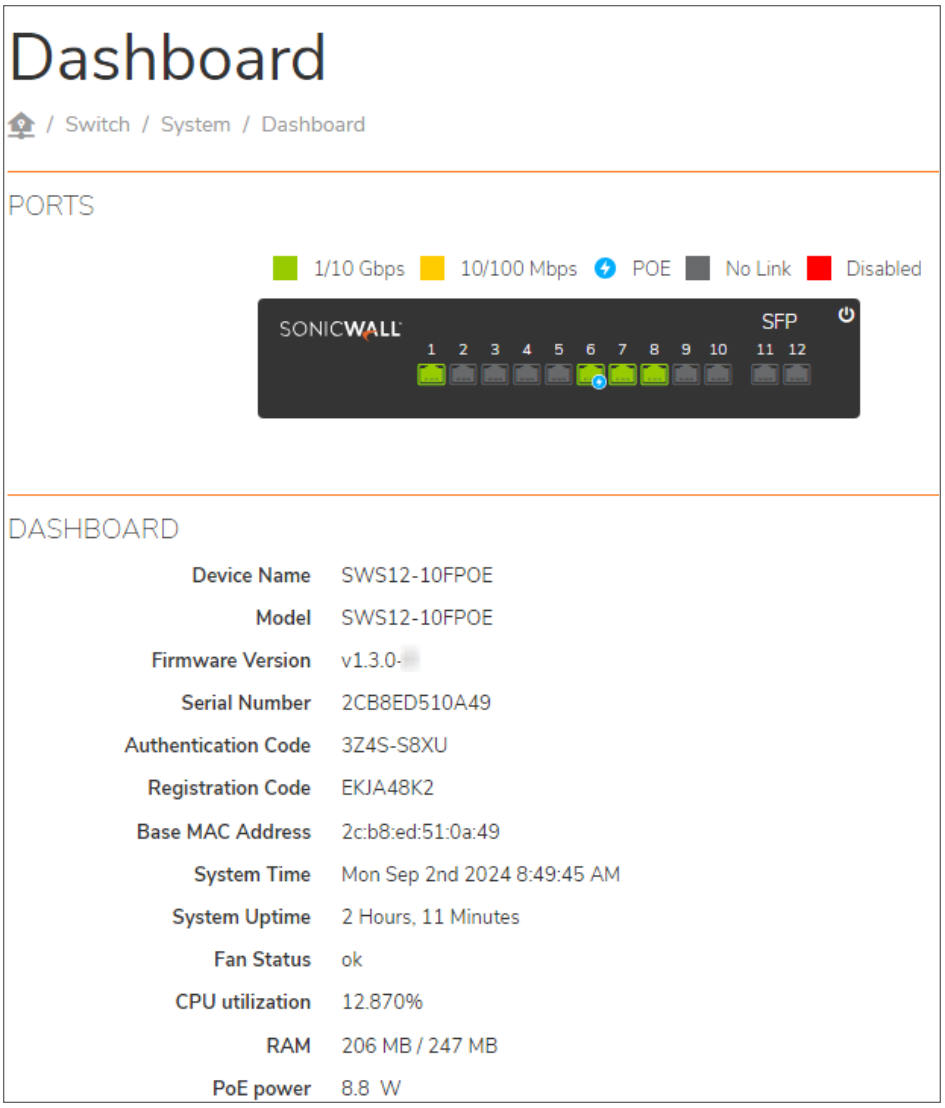
System menu option is divided into the following sections to allow configuration and management of the switch.

- 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.

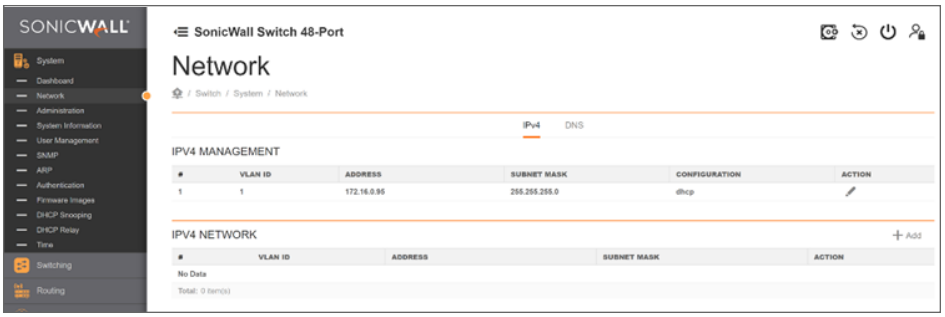
Device Name	Displays the device name of the Switch.
Model	Displays the model name of the Switch.
Firmware version	Displays the installed firmware version of the Switch.
Serial Number	Displays the serial number of the Switch.
Authentication Code	Displays an 8-character code that acts as a hardware identifier of the Switch
Registration Code	Displays the code generated when the Switch is registered and will be available in MySonicWall.
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.



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.



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 Static or DHCP for IP address management.. If using a static IP, enter the IP address, subnet mask, gateway, and DNS servers.

To be managed over the network, the Switch needs an IP Address. The Network screen contains fields for assigning an IP addresses. IP addresses are either defined as Static or are retrieved using the DHCP. DHCP assigns a 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, hover over the VLAN ID and click the edit icon.

VLAN ID	Select the VLAN ID. The default VLAN ID is 1.
Address	Enables the IP address to be configured automatically by the DHCP server. Select this option for 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 for the 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, enter the IP address for the default gateway of the network.

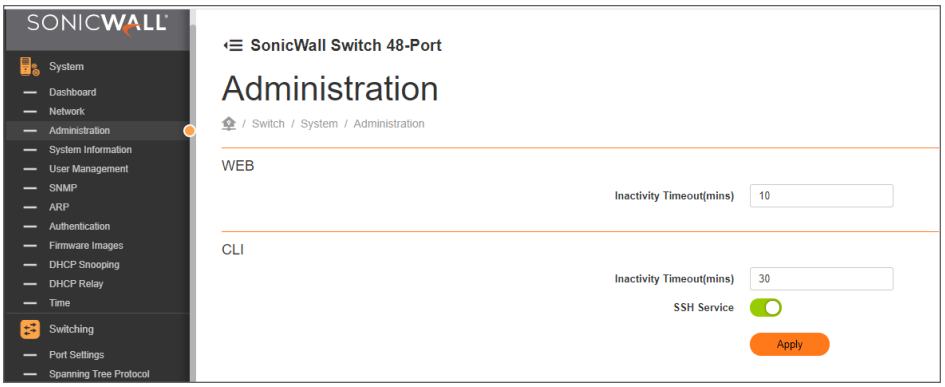
Configuration	Select the type of server configuration. • Static • BOOTP • DHCP

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

Administration

Web Settings

The Switch provides a built-in browser interface that enables the configuration and management of the Switch via Hypertext Transfer Protocol Secure (HTTPS) requests securely to help prevent security breaches on the network.

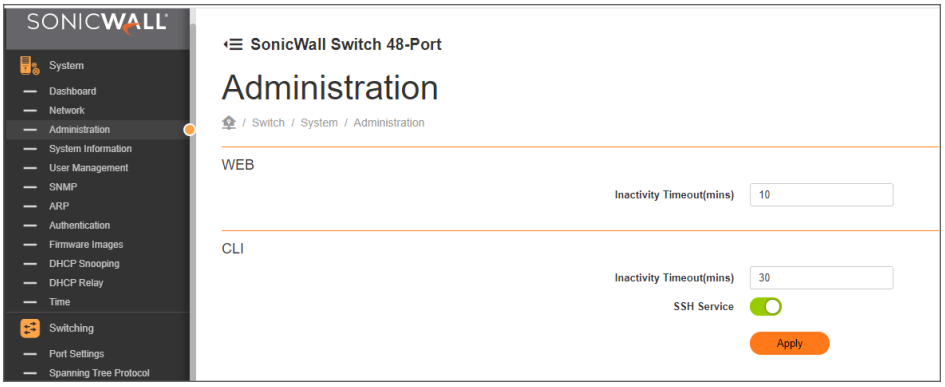


The default **Inactivity Timeout** is set to 10 minutes.

SSH Settings

Secure Shell (SSH) is a cryptographic network protocol for secure data communication and command execution. 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.



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.

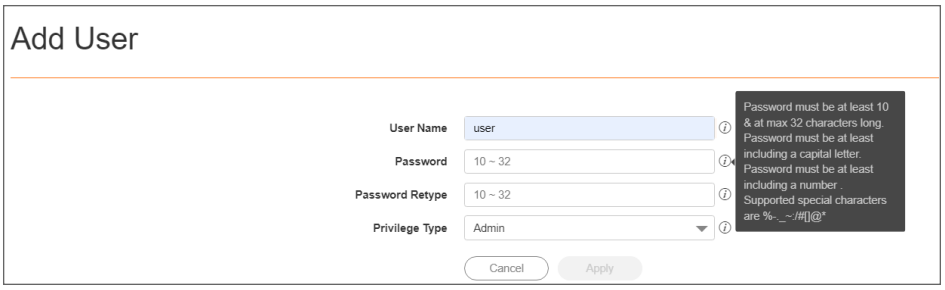
Device Name	Displays the device name.
New Name	Enter the name used to identify the Switch using up to 255 alphanumeric characters. ⓘ | **NOTE:** List of Supported and Unsupported special Characters: • Supported special characters: ~`@#$^*()_-={}[]:<>,./ • Not supported special characters: !%&+;"'?|

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

User Management

This section allows for the adding and editing of users to access the Switch. Click the **Add User** button to add an account or the **Edit** button to edit an existing account. An account with user privileges can only view settings; it has no right to change the switch's settings. An account with admin privileges can configure all switch functions.

User Name	Enter a username using up to 18 alphanumeric characters. Only letters a-z, numbers 0-9 and _ are allowed.
Password	Enter a new password for accessing the Switch. Ensure to use a complex password.
Password Retype	Repeat the new password used to access the Switch.
Privilege Type	Select **Admin** or **User** from the list to regulate access rights.



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

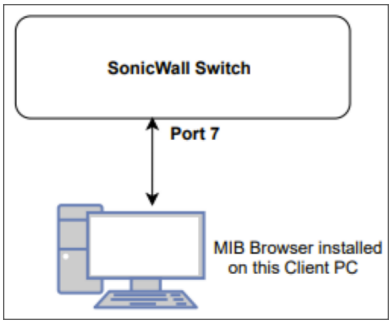
Simple Network Management Protocol

Simple Network Management Protocol (SNMP) is an Application Layer protocol designed specifically for managing and monitoring network devices. 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.

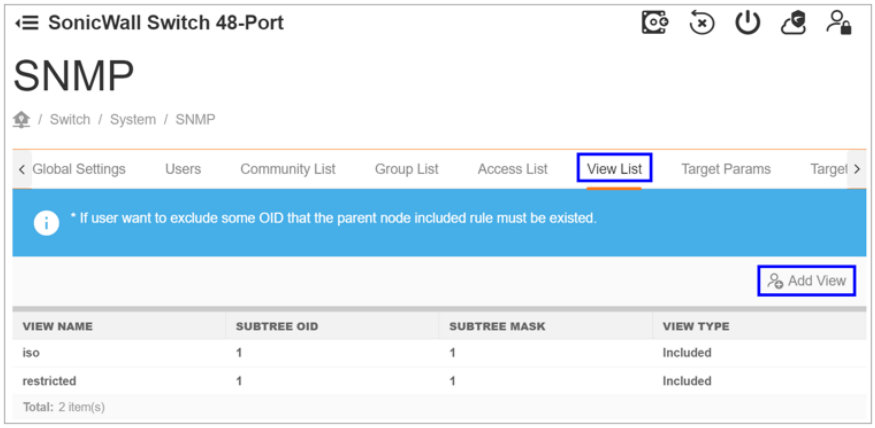
- SNMPv1, which is defined in RFC 1157 “A Simple Network Management Protocol (SNMP)”, is a standard that defines how communication occurs between SNMP-capable devices and specifies the SNMP message types. Version 1 is the simplest and most basic of versions. There may be times where it’s required to 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. It is recommended to 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

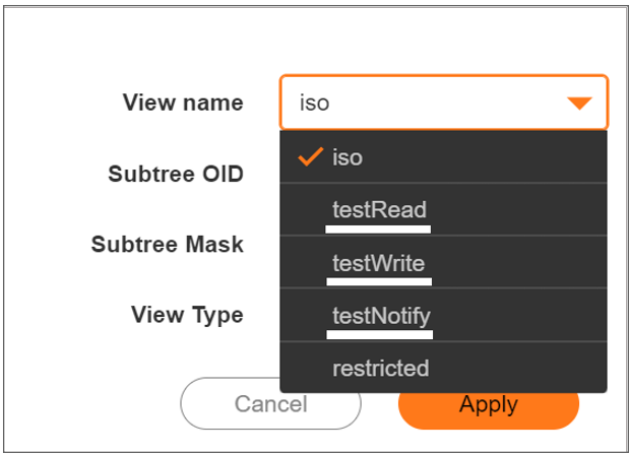


Add View List

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



  - 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).

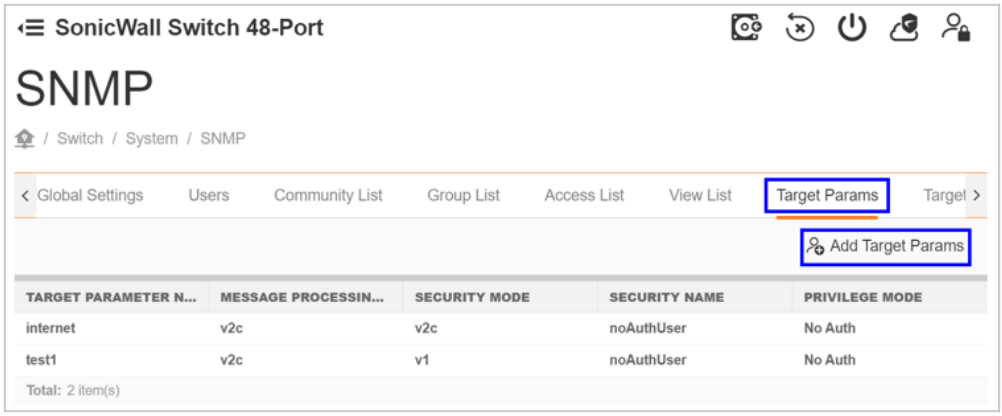
  A subtree mask is a bit pattern that is used to match a group of related objects in a MIB. The subtree mask level specifies the depth of the tree at which the subtree mask is applied. This means that only the objects within the specified subtree will be affected by the mask. For example, if the subtree 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.

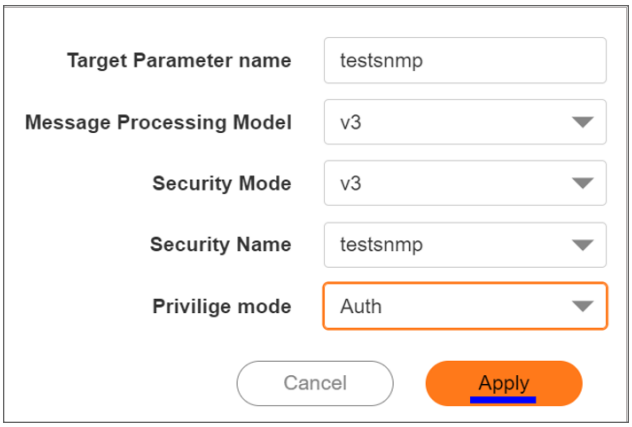
      ⓘ | **NOTE:** mask level should not exceed OID level.
- View type
    - Selection
        - Included
        - Excluded

Add Target Params

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

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





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

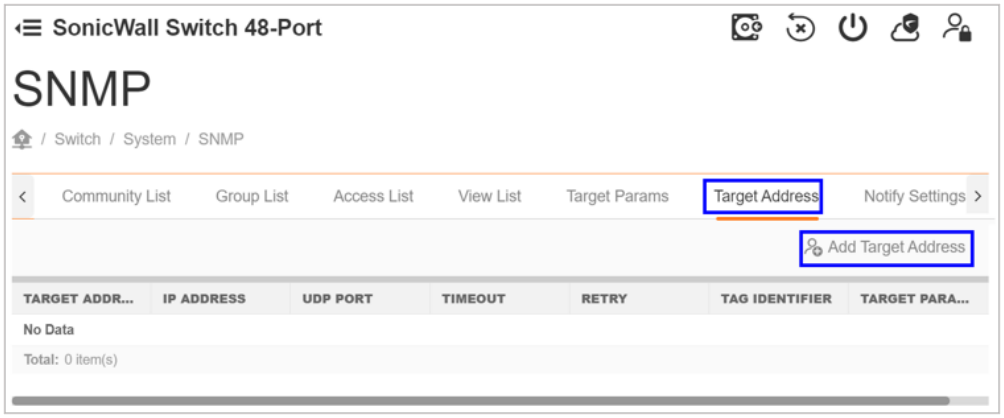
Security Name	• Selection • Options are usernames in Users list table

Privilege Mode	• Selection
	  • No auth
	  • Auth
	  • Priv

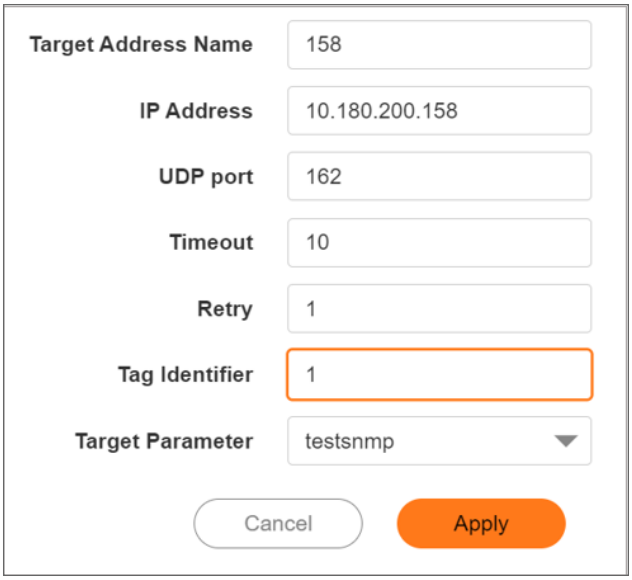
Click **Apply** to accept the changes or Cancel to discard them.

Add Target Address

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



Click on **Add Target Address**.



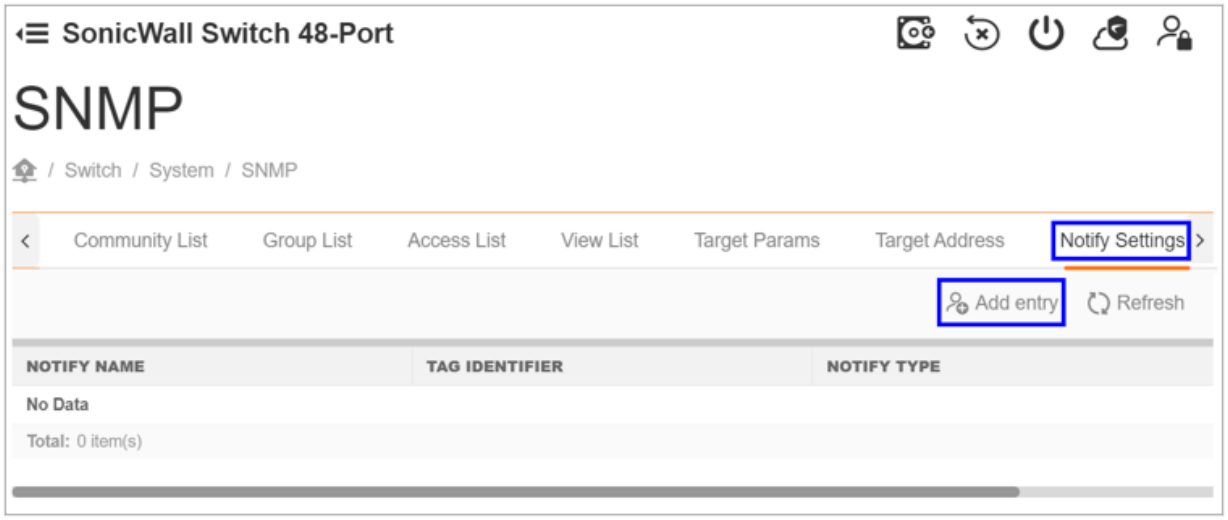
Target Address Name	Custom string with 1-32 characters
IP Address	String in IP format.

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.

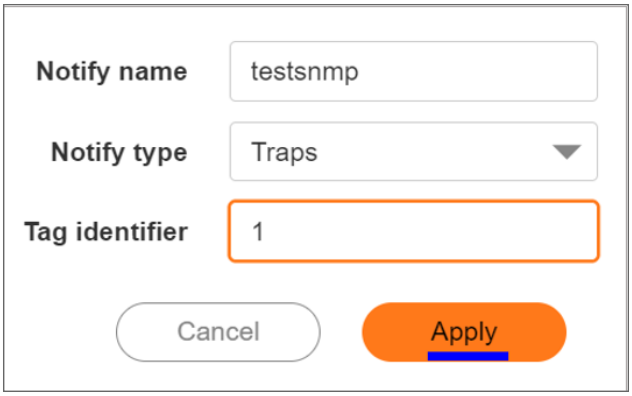
Click **Apply** to accept the changes or Cancel to discard them.

Add Notify Setting

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



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



Notify Name	Custom string with 1-32 characters.

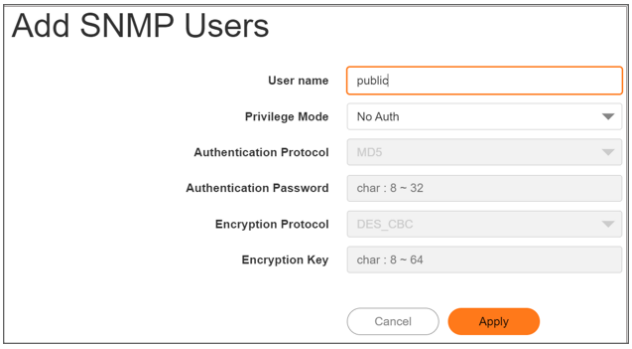
Tag identifier	• Custom string with 1-20 characters. • This field only works when Tag Identifier is filled in target address list

Notify type	• Selection
	  • Traps
	  • Informs

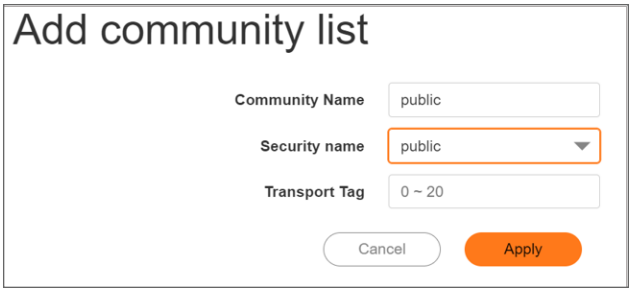
SNMP Traps/Informs

To send SNMP Traps/Informs:

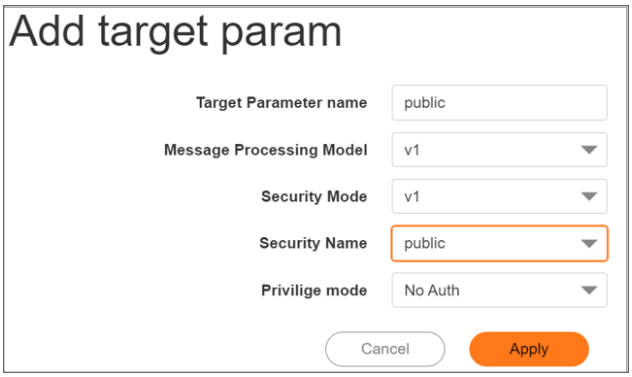
1. Add **User** with Privilege Mode is **No Auth**(such as **public**)



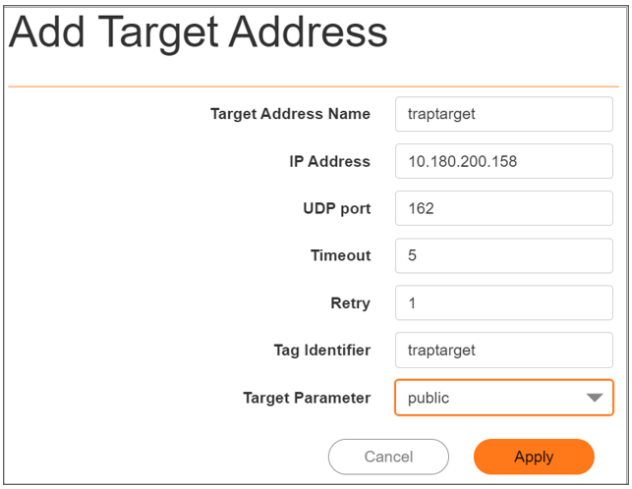
2. **Add Community List** which the security name is the username in Users



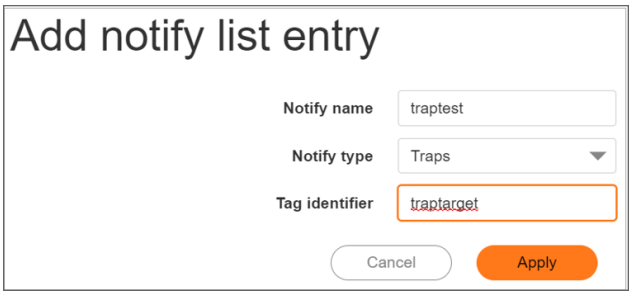
3. Add **TARGET PARAMS** and select the parameters as needed



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

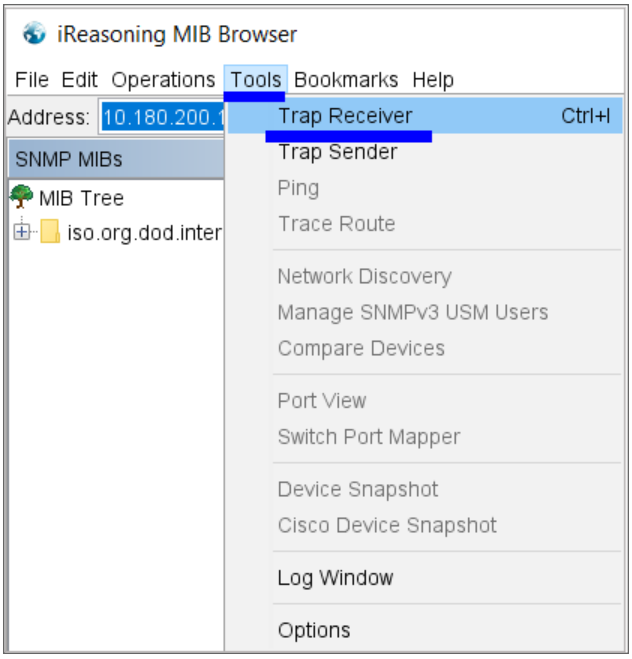


5. Add **NOTIFY SETTINGS** and fill out the parameters as needed

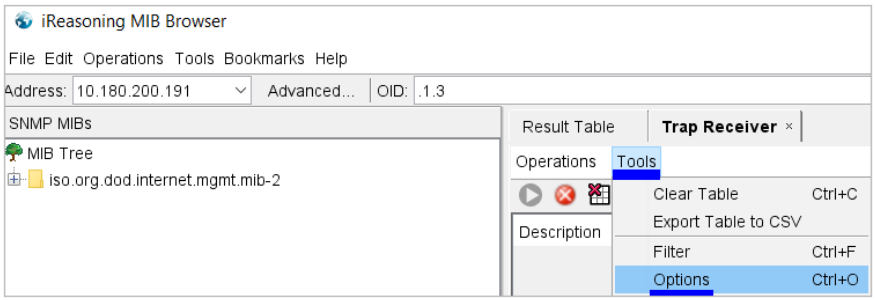


6. Using iReasoning MIB Browser to confirm the SNMP Trap Function

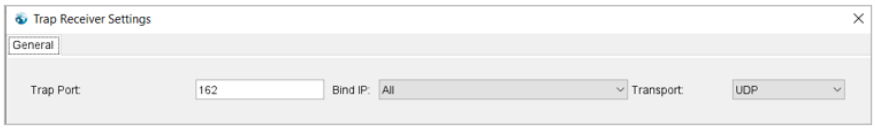
a. Download iReasoning MIB Browser, then Navigate to **Tools** >**Trap Receiver**

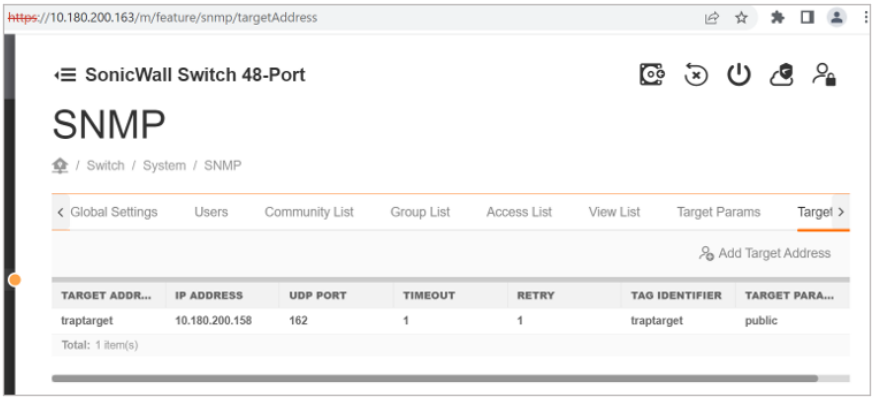


b. Click **Tools** >**Options**

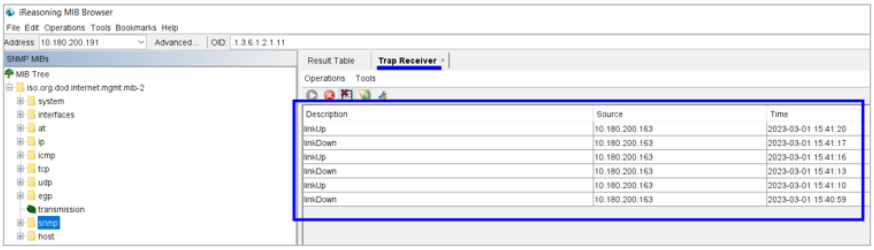


c. Make sure the Trap Port is same as the **TARGET ADDRESS**



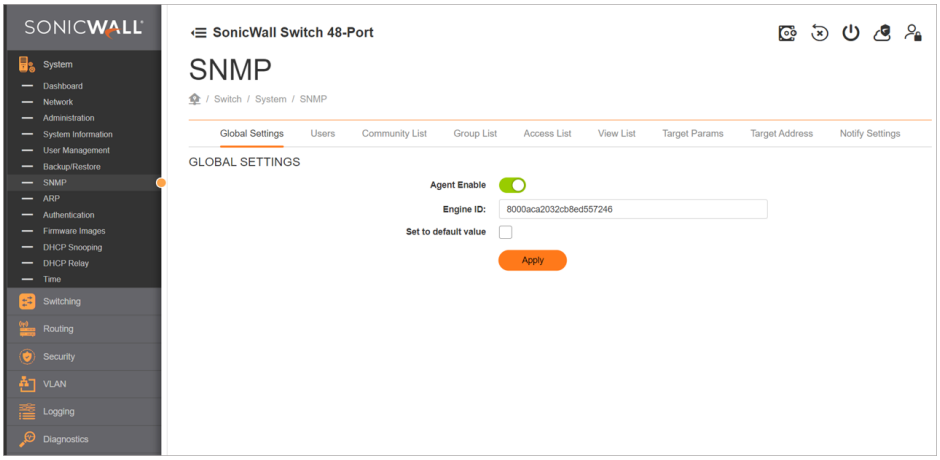


d. Trigger some SNMP Traps(such as **link up** or **link down**)

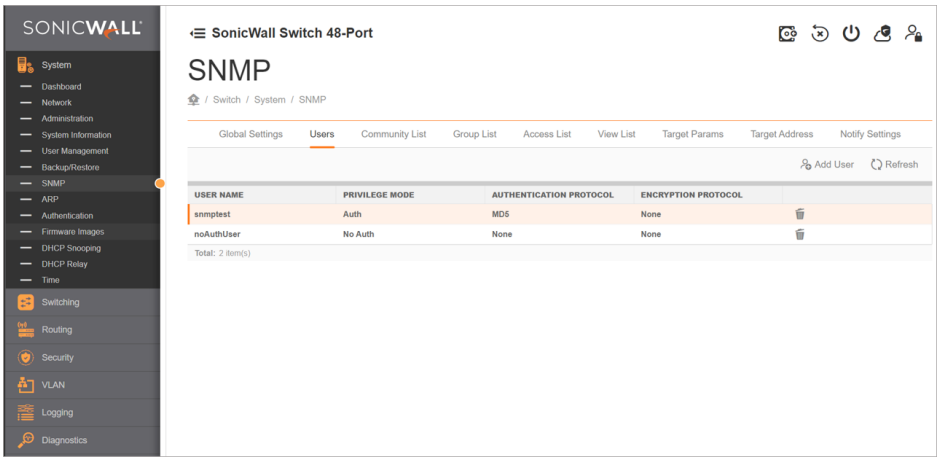


How to configure SNMP on SonicWall Switch

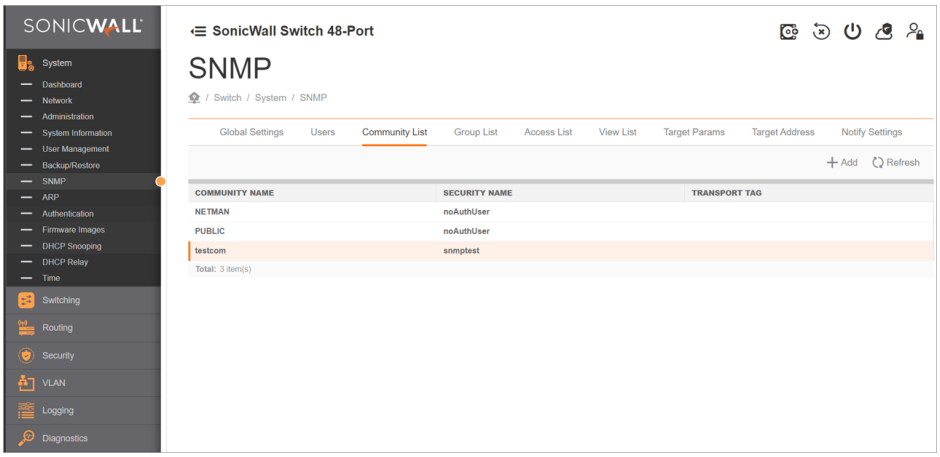
1. Enable SNMP Agent



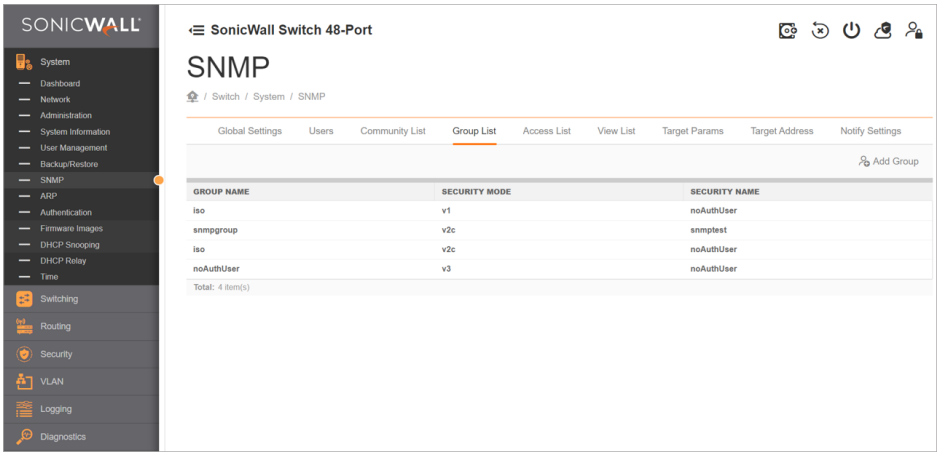
2. Add SNMP Users with Privilege Mode ‘Auth’ and Authentication Protocol ‘MD5’ (in this example, the user created is ‘snmptest’)



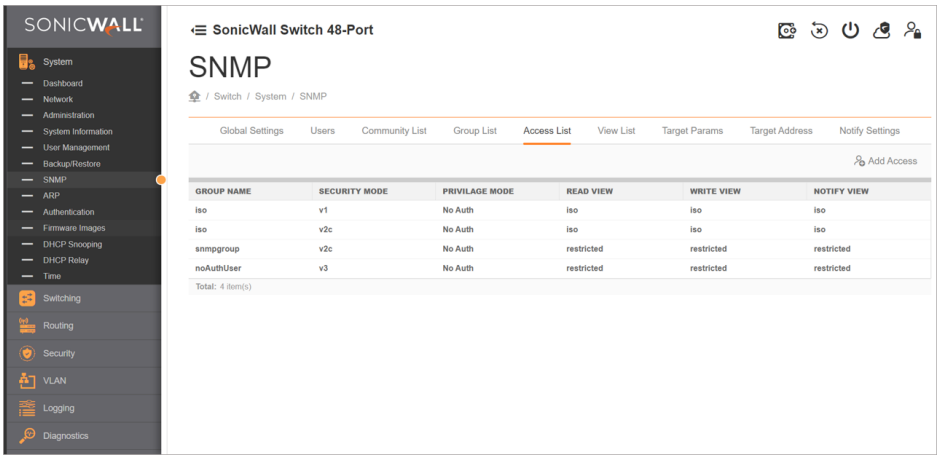
3. Add community list and call the Security name created in Step 2



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



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



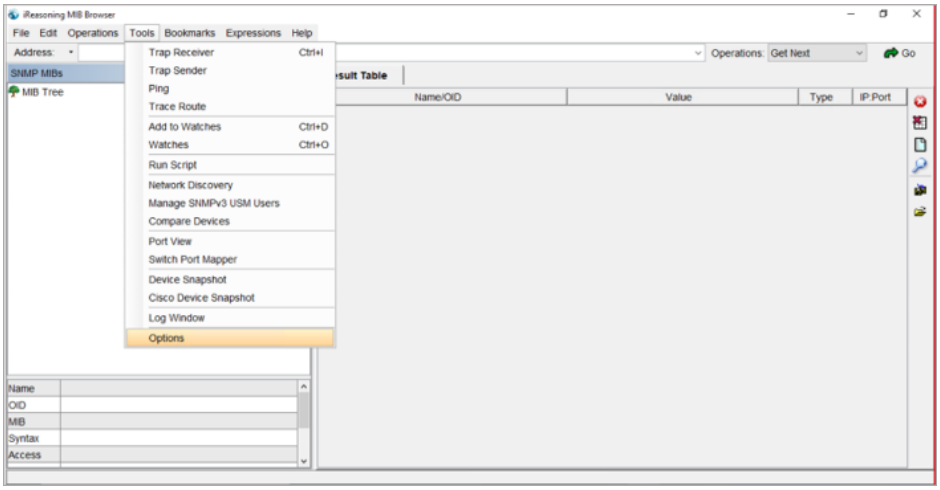
SNMP supported OID's in 1.2.0.1-2s

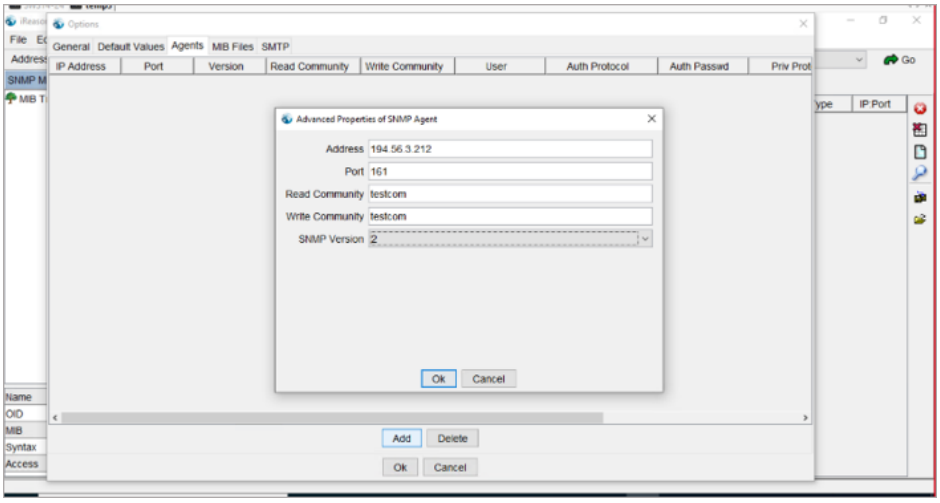
SL	SNMP Parameter	OID
1	Runtime/Uptime	1.3.6.1.2.1.1.3.0
2	Port Link Status	1.3.6.1.2.1.2.2.1.8.X
3	Port Description	1.3.6.1.2.1.2.2.1.2.X
4	Temperature	1.3.6.1.2.1.99.1.1.1.4.4
5	Firmware Version	1.3.6.1.2.1.47.1.1.1.1.9.1
6	Port Speed/Active Speed	1.3.6.1.2.1.2.2.1.5.X
7	Port Auto Negotiation	1.3.6.1.2.1.26.5.1.1.1. 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

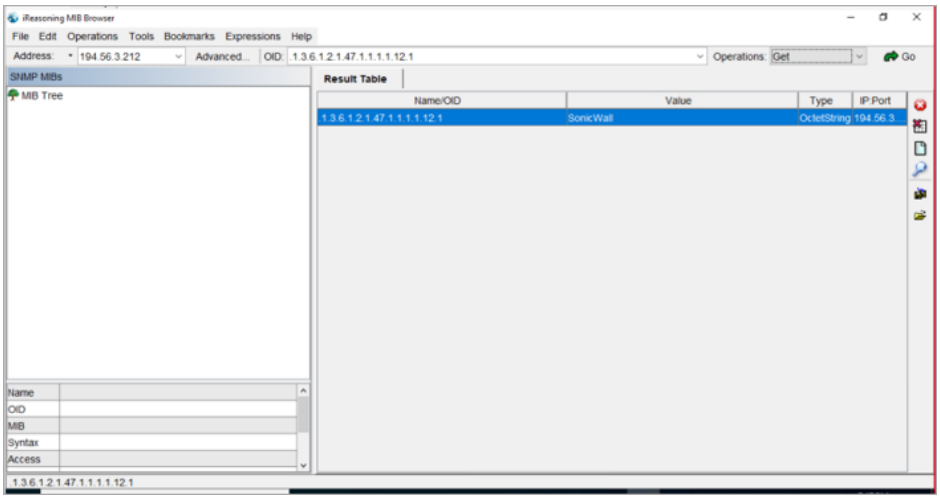
For this example, iReasoning MIB browser was used, but any MIB browser can be used.

1. Navigate to **Tools > options > Agents > Add agent**.





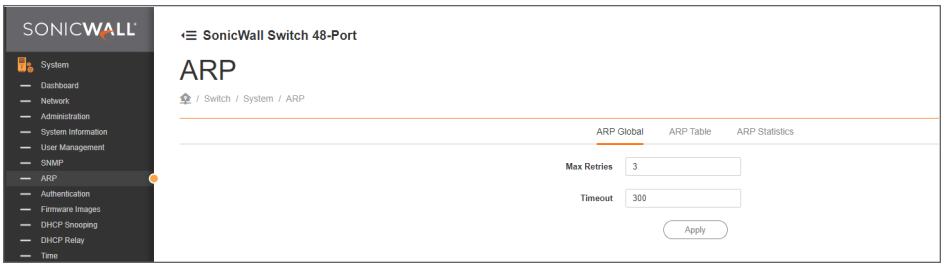
2. Enter the OID's Provided above and start with SNMP operations.


iReasoning MIB Browser
File Edit Operations Tools Bookmarks Expressions Help
Address: 194.56.3.212
Advanced...
OID: 1.3.6.1.2.1.47.1.1.1.1.12.1
Operations: Get
Go
SNMP MIBs
MIB Tree
Result Table
Name/OID
Value
Type
IP:Port
1.3.6.1.2.1.47.1.1.1.1.12.1
SonicWall
OctetString
194.56.3.
Name
OID
MIB
Syntax
Access
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 (IP) 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 comprised 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.

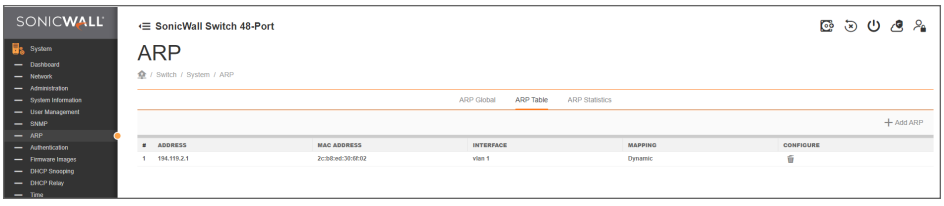


Click **Apply** to save the changes to the system.

ARP Table

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

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



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.

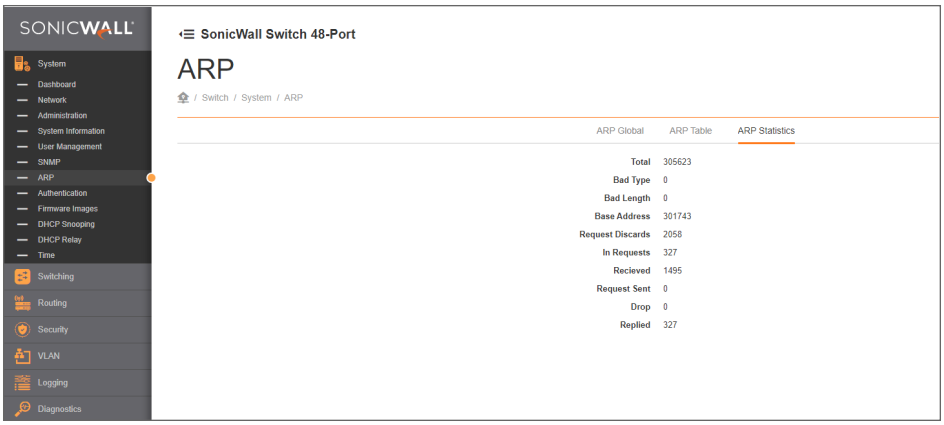
To delete an entry from the ARP Table:

1. Click **Configure** on the entry 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.



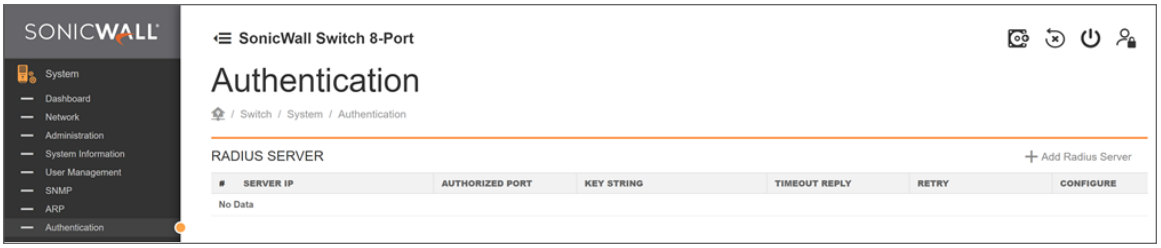
Authentication

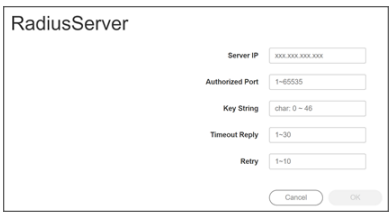
RADIUS (Remote Authorization Dial-In User Service) servers provide security for networks. RADIUS servers provide authentication and authorization for networks. The RADIUS server maintains a user database, which contains authentication information. The Switch passes information to the configured RADIUS 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.

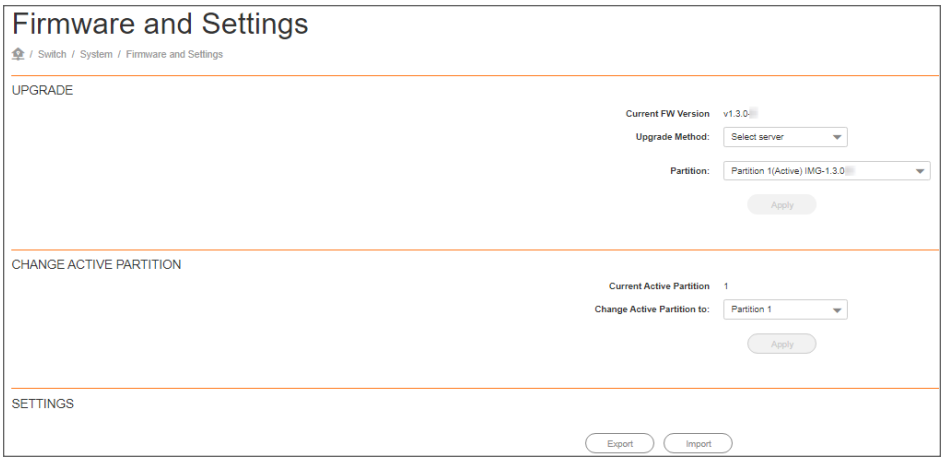




Firmware and Settings

The Switch maintains two versions of the firmware image in its permanent storage. One image is the active image, and the second image is the backup image. The Switch boots and runs from the active image. If the active image is corrupt, the system automatically boots from the backup image.

Upgrade Method	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	Export and import the Switch Firmware configuration file using the following methods: • Export- 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- Import the configuration data from a local machine as `.cfg` file into your appliance.

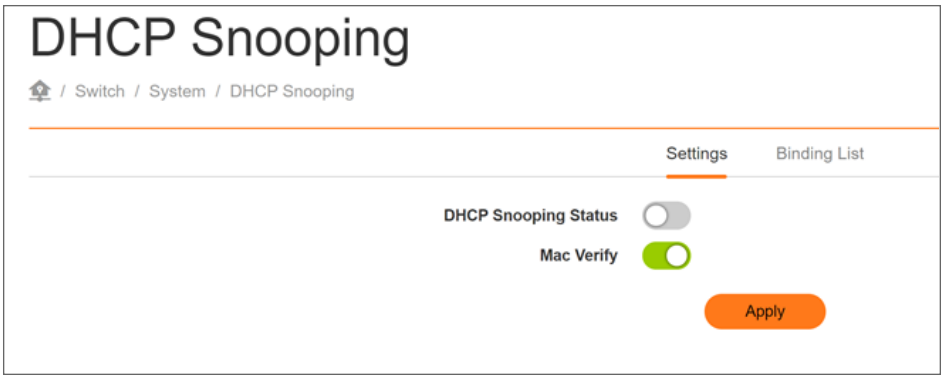


Click **Apply** to save the changes on this page.

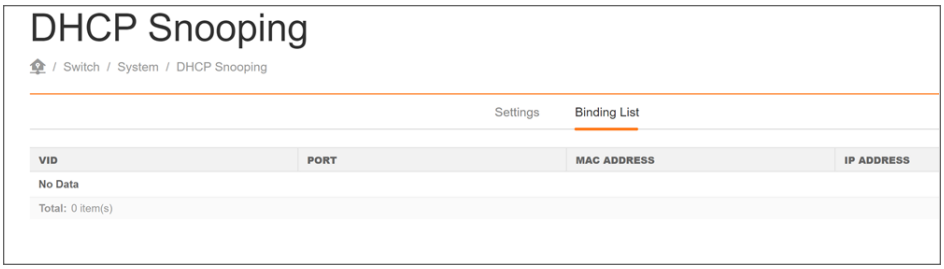
DHCP Snooping

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



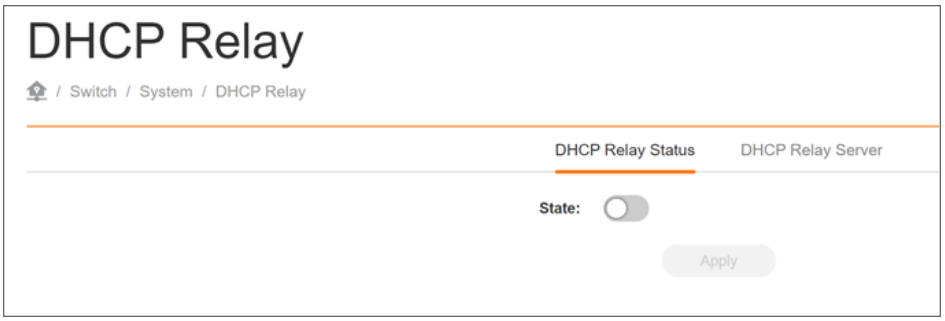
Binding List	This list shows the current statistics of VLAN ID, ports, MAC address and the respective IP Address



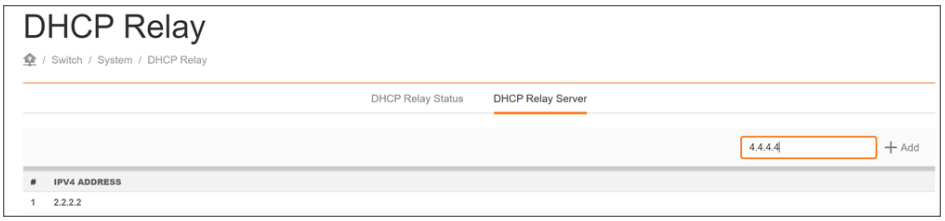
DHCP Relay

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

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



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

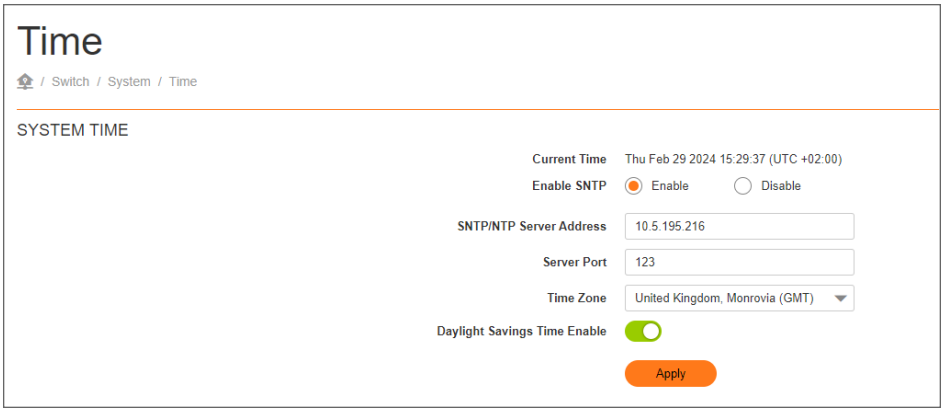


Time

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.
SNTP/NTP Server Address	Enter the SNTP or NTP sever IP address or hostname.
Server Port	Displays the time sever port.
Time Zone	Select the difference between Greenwich Mean Time (GMT) and local time.
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.



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:

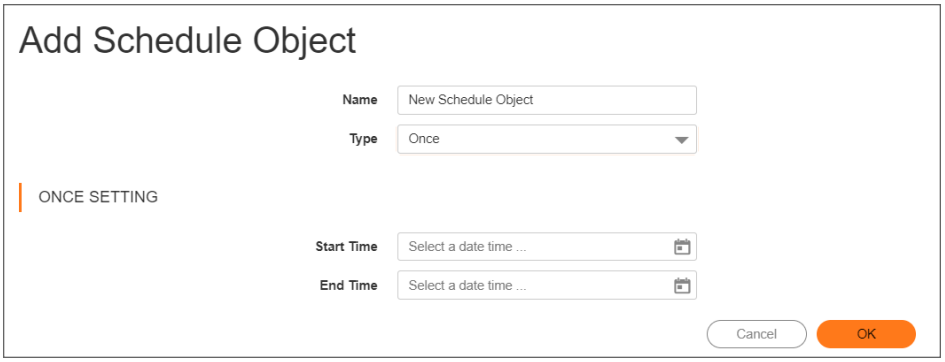
1. In the **Enable SNTP** settings, select the **Disable** option to configure the date or time manually.
2. In the **Manual Time** settings, select the date, time, and choose the appropriate time zone.
3. Click **Apply** to update the system settings.

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.

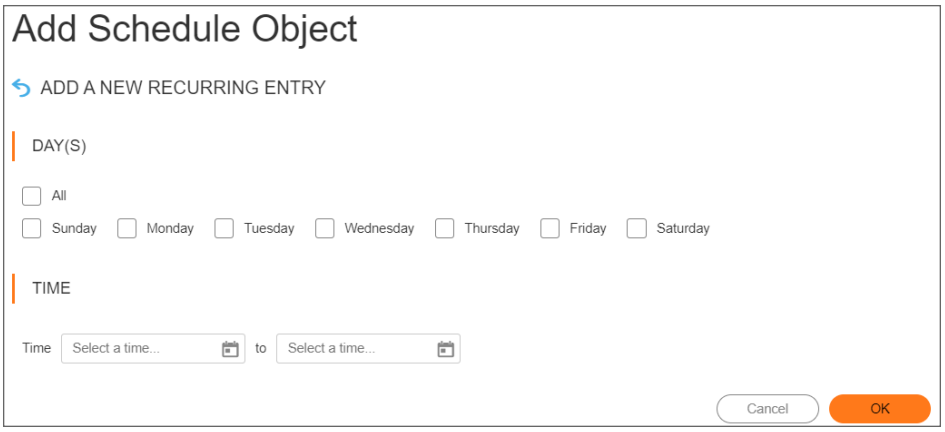
To add a schedule:

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.

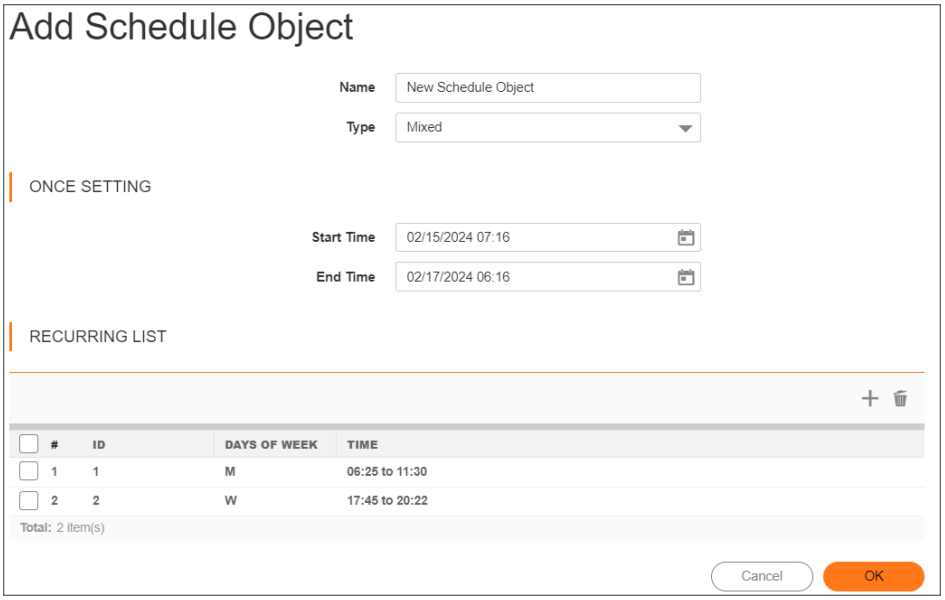
1. Click + icon to add the schedule object.
2. Enter a name for the new schedule.
3. Select the type of schedule from the list:
    - **Once**- This options allows the selection of one schedule profile defined by setting the **Start** and **End** date and time.



    - **Recurring**-This option allows the configuration of a recurring entry with up to seven entries defined. Select the day and time for each schedule. Each profile allows scheduling up to seven entries.



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



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 provides the list of configurable Layer 2 switching capabilities. Utilize these features to configure the Switch to your preferences.

Topics:

- Port Settings
- Spanning Tree Protocol
- Loopback Detection
- Link Aggregation
- Port Mirror
- Jumbo Frames
- MAC Address Table
- Link Layer Discovery Protocol
- IGMP Snooping
- Multicast Filtering
- Quality of Service
- Remote Network Monitoring
- Port Statistics

Port Settings

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

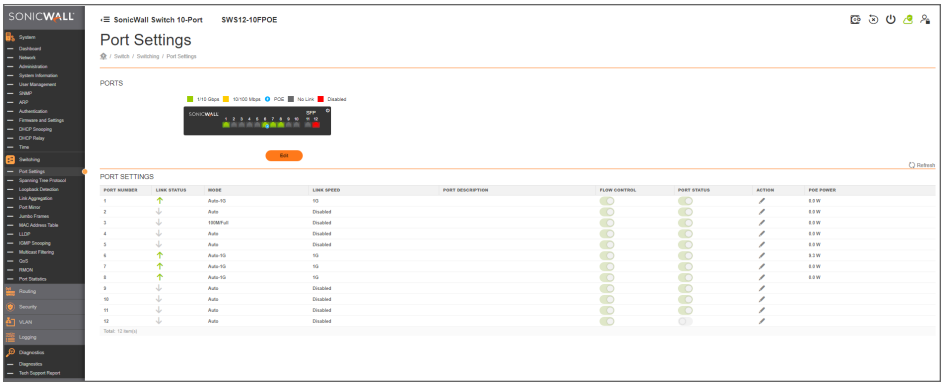
- Port Settings
- Quality of Service
- PoE
- Security
- ACL Binding
- Advanced

Port Settings

Use this screen to view and configure Switch port settings. The Port Settings feature allows for the configuration of the ports on the Switch in order to find the best balance of speed and flow control. To access the page, in the **Ports** image, select the port to configure and click **Edit**.

Status	Enables or disables the interfaces.
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.
STP	By default STP is not available. After creating a MST instance, STP states can be modified for individual ports.

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 the settings of the peer port to be the same in order to connect.
Port Description	Add a port description using up to 127 characters.



Native VLAN

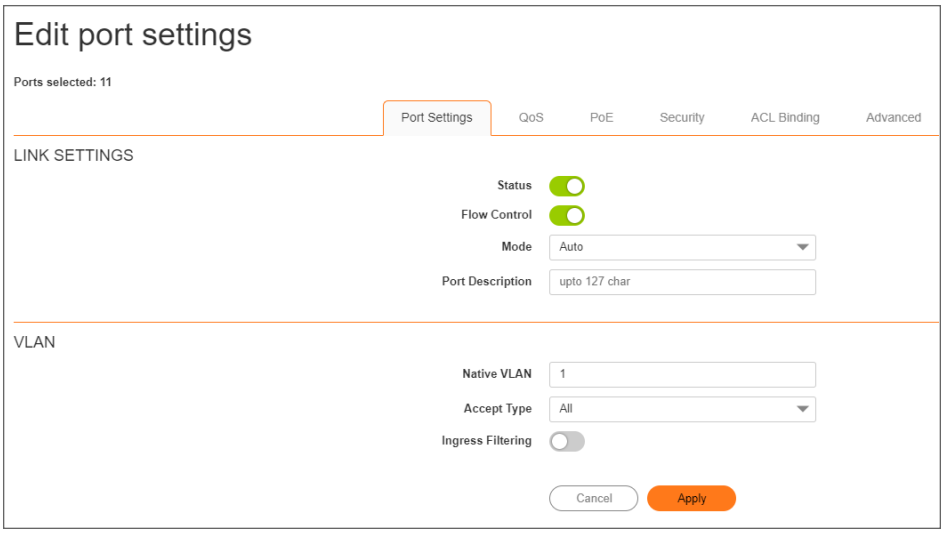
When an Untagged packet enters a Switch port, the Native VLAN (Port VLAN ID) will be attached to the untagged packet and forward frames to a VLAN specified VID part of the Native VLAN. A packet received on a given port would be assigned that port's Native VLAN and then be forwarded to the port that corresponded 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.
- The default Native VLAN requires change, 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 the port to handle tagged frames. Select Enabled or Disabled from the list. • Enabled: tagged frames are discarded if VLAN ID does not match the NATIVE VLAN of the port. • Disabled: All frames are forwarded in accordance with the IEEE 802.1Q VLAN.

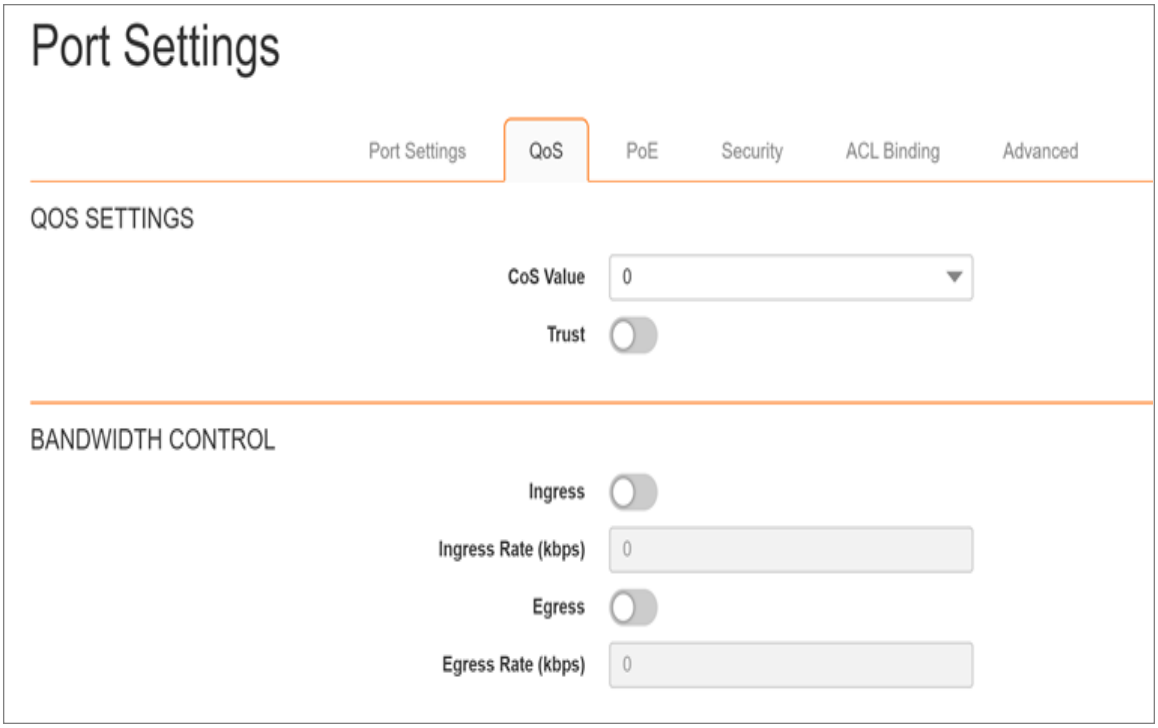


Click **Apply** to update the system settings.

QoS Settings

Configure the QoS port settings for the Switch by selecting a port and choosing 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.



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.

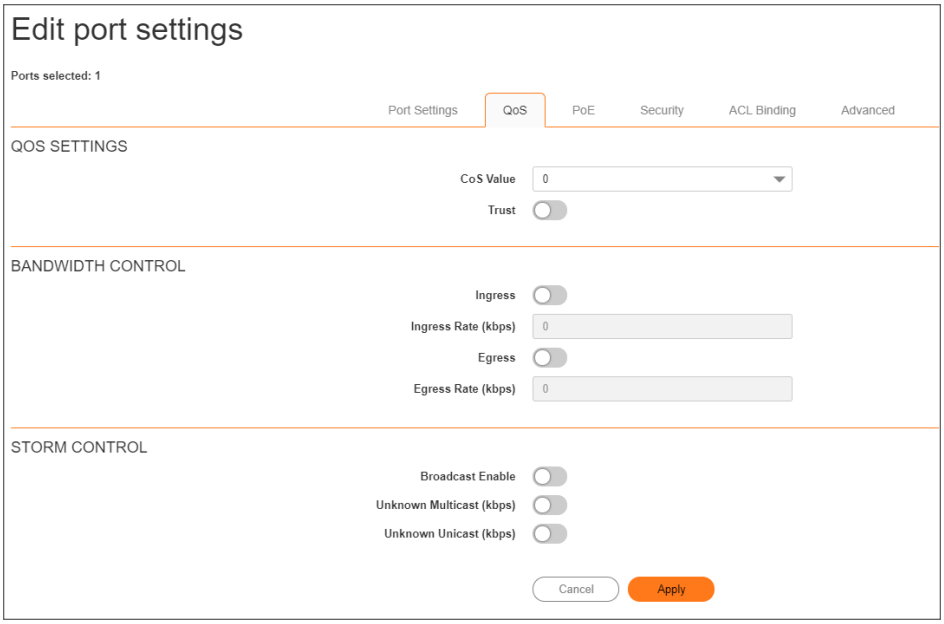
Ingress	Select to **Enable** or **Disable** ingress on the interface.
Ingress Rate	Enter the ingress rate in kilobits per second. The Gigabit Ethernet ports have a maximum speed of 1000000 kilobits per second.
Egress	Select from the drop down box to **Enable** or **Disable** egress on the interface .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

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.



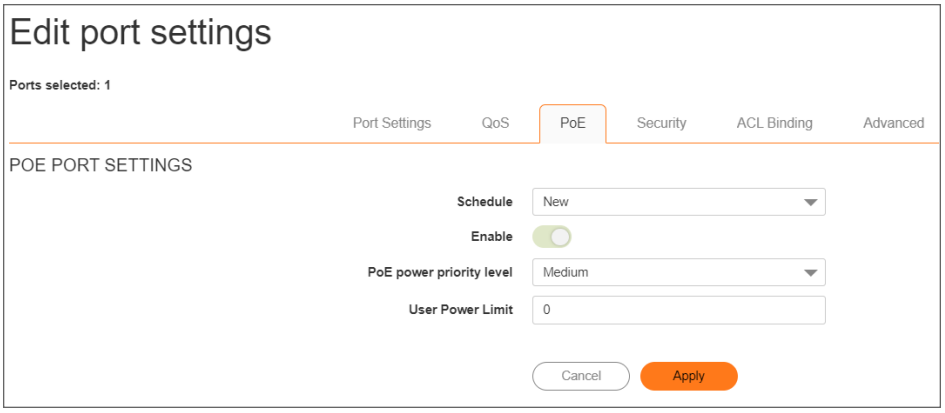
Click **Apply** to save the changes to the system.

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

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



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 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.

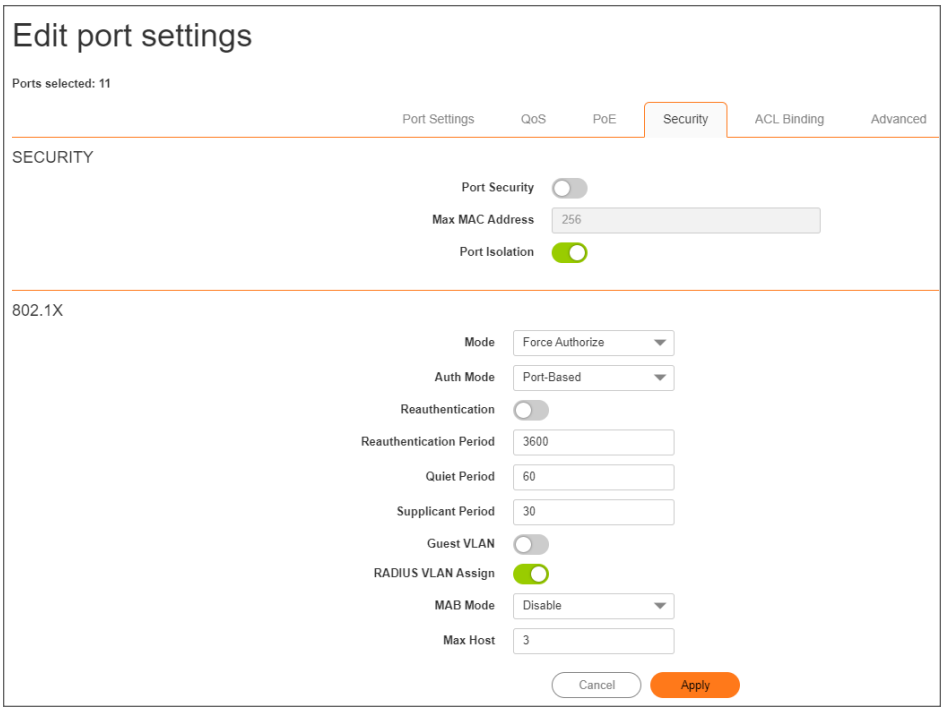
Settings	Description
PoE power priority level	This setting establishes the power priority level for the port. When the port priority level is set to high, that port is prioritized to receive power. The following priority levels are available: • Low • Medium • High • Critical The default priority level is Low.
User Power Limit	This setting sets the maximum amount of power that can be delivered by a port.The maximum power limit is 31.

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 an unauthorized device from accessing the network according to the MAC address.

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



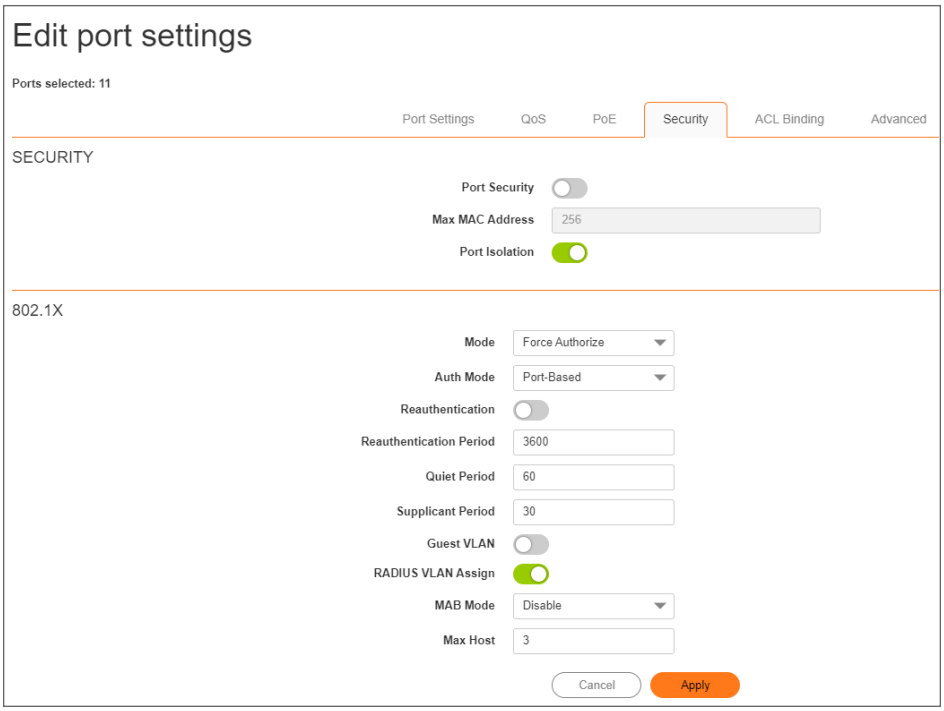
Click **Apply** to save the changes to the system.

802.1X

This section allows the configuration of the 802.1x port settings. 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 to elapse for the Reauthentication period, Quiet Period, and Supplicant Period. After this, enter the Max number of times for the Switch to retransmit and EAP request. Finally, choose to Enable or Disable the VLAN ID.

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 mode	**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. Up to 10 can be added. The default value is 3.

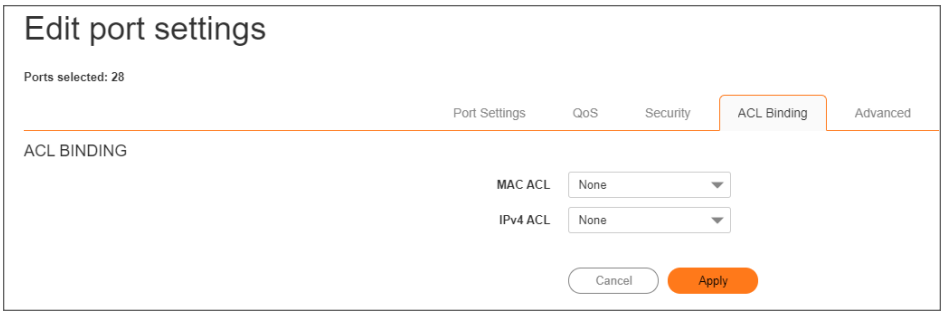


Click **Apply** to accept the changes or **Cancel** to discard them.

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.

MAC ACL	Select the MAC ACL as defined in the Security, ACL Management section.
IPv4 ACL	Select the IPv4 ACL as defined in the Security, ACL Management section.



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

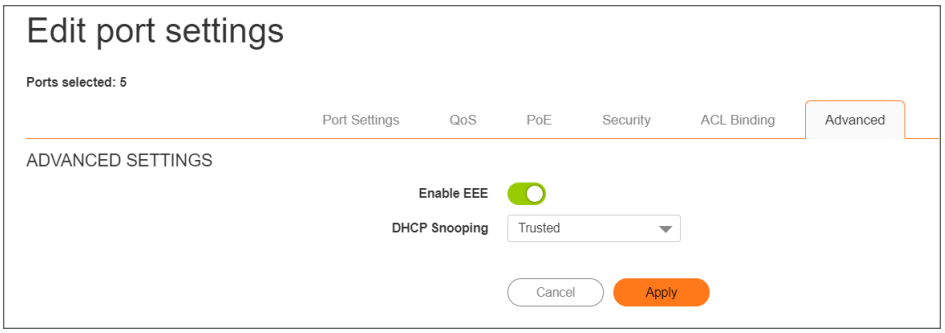
Advanced

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 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 Advanced 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.



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 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.

STP is a Layer 2 protocol that runs on Switches. 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.

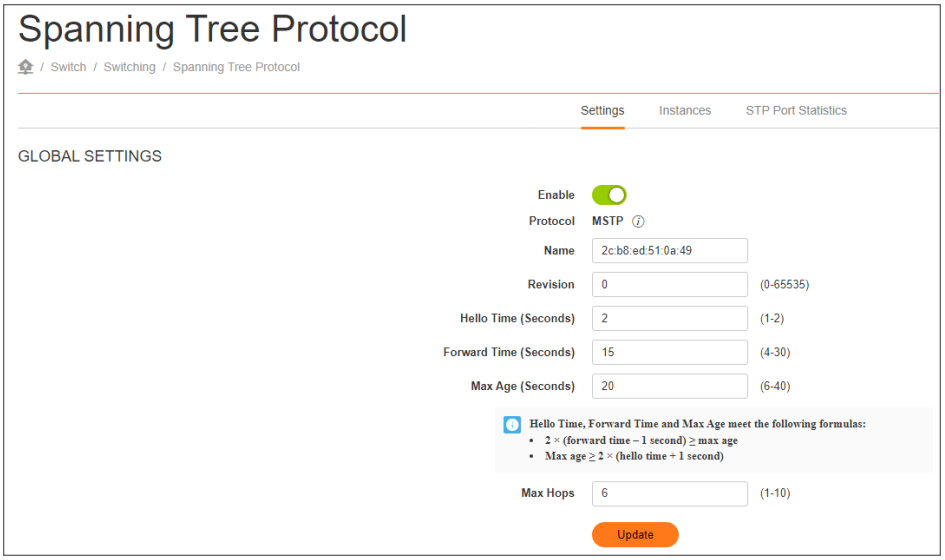
MSTP defined in IEEE 802.1s, enables multiple VLANs to be mapped to reduce the number of spanning-tree instances needed to support a large number of VLANs. If there is only one VLAN in the network, a single STP works appropriately.

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.



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 a 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). The default is 15 seconds.
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 the following formula: 2*(Forward Time -1 second) ≥ Max Age Max Age ≥ 2*(Hello Time + 1 second).
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 6.

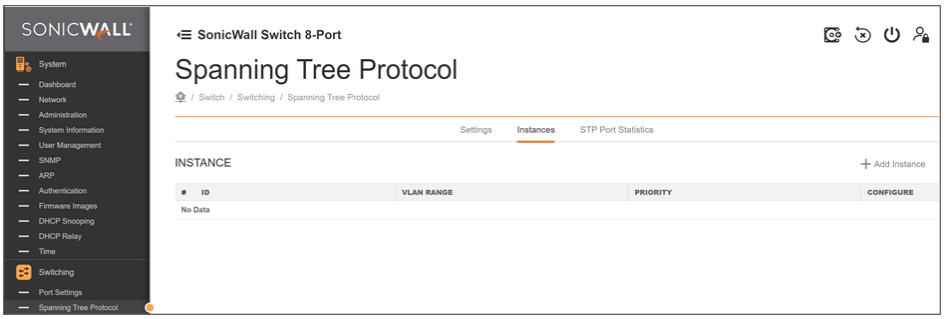
Select whether to enable or disable the Spanning Tree function for the Switch and click **Update** to update the system settings.

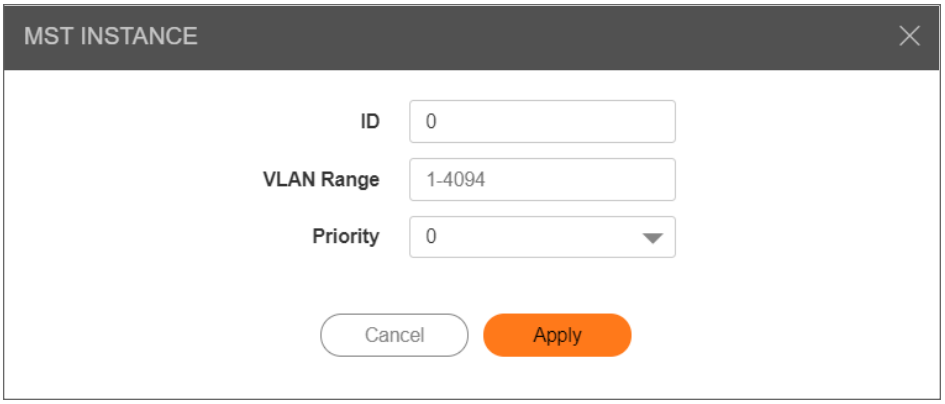
MST Instance Settings

Multiple Spanning Tree Protocol (MSTP) enables the grouping of multiple VLANs with the same topology requirements into one 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 CST.

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





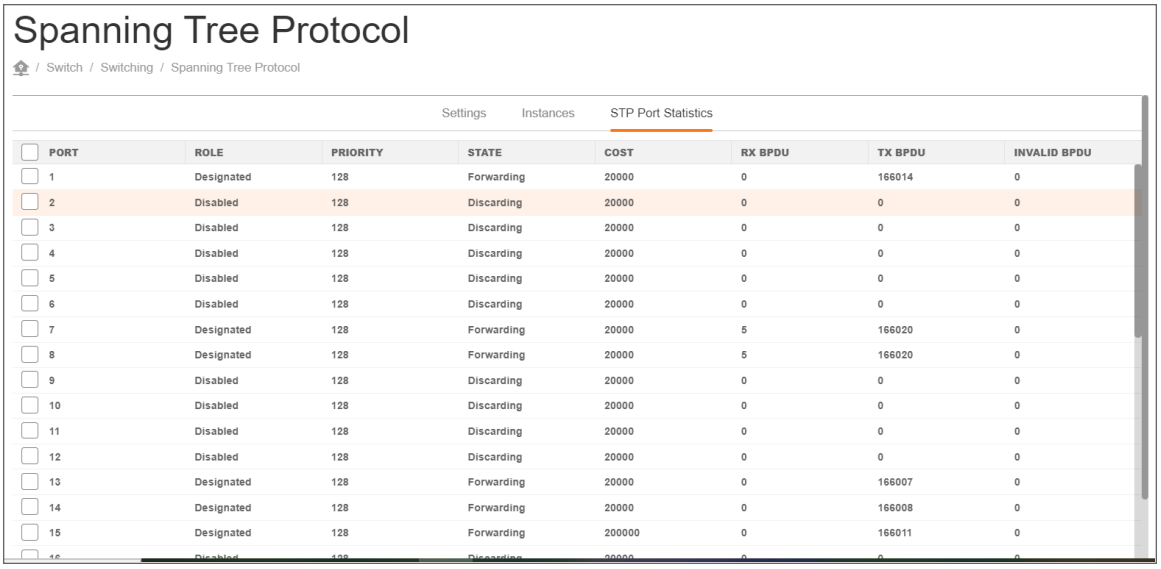
ID	Displays the ID of the MST group that is created. A maximum of 15 groups can be set for the Switch.
VLAN Range	Enter the VLAN ID range from for the configured VLANs to associate with the MST ID. The VLAN ID number range is from 1 to 4094.
Priority	Select the bridge priority value for the MST. When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

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.

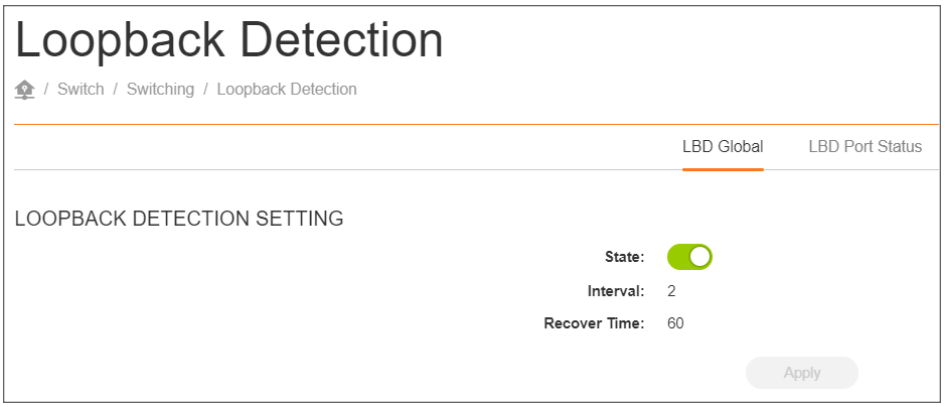


Port	Displays the port for which statistics are displayed.
Role	Displays the designated (connected port link status) or disabled ports (no connection).
Priority	Displays the priority value of the port (0-240 with multiples of 16). Default priority is 128.
State	Displays the forwarding or discarding or 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.



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

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.

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

Link Aggregation Control Protocol (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.

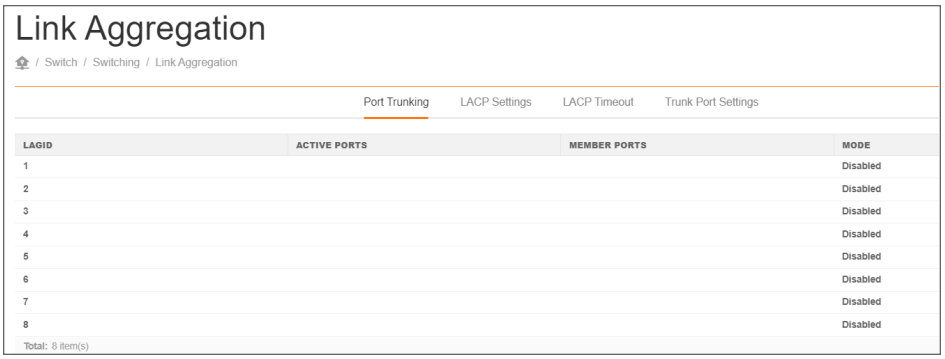
Port Trunking

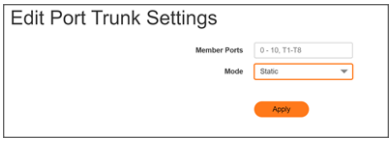
Port Trunking allows you to assign physical links to one logical link that functions as a single, higher-speed link, providing dramatically increased bandwidth. Use Port Trunking to bundle multiple connections and use the combined bandwidth as if it were a single larger "pipe".

ⓘ | **IMPORTANT:** Trunk Mode must be enabled to 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 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 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. 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.



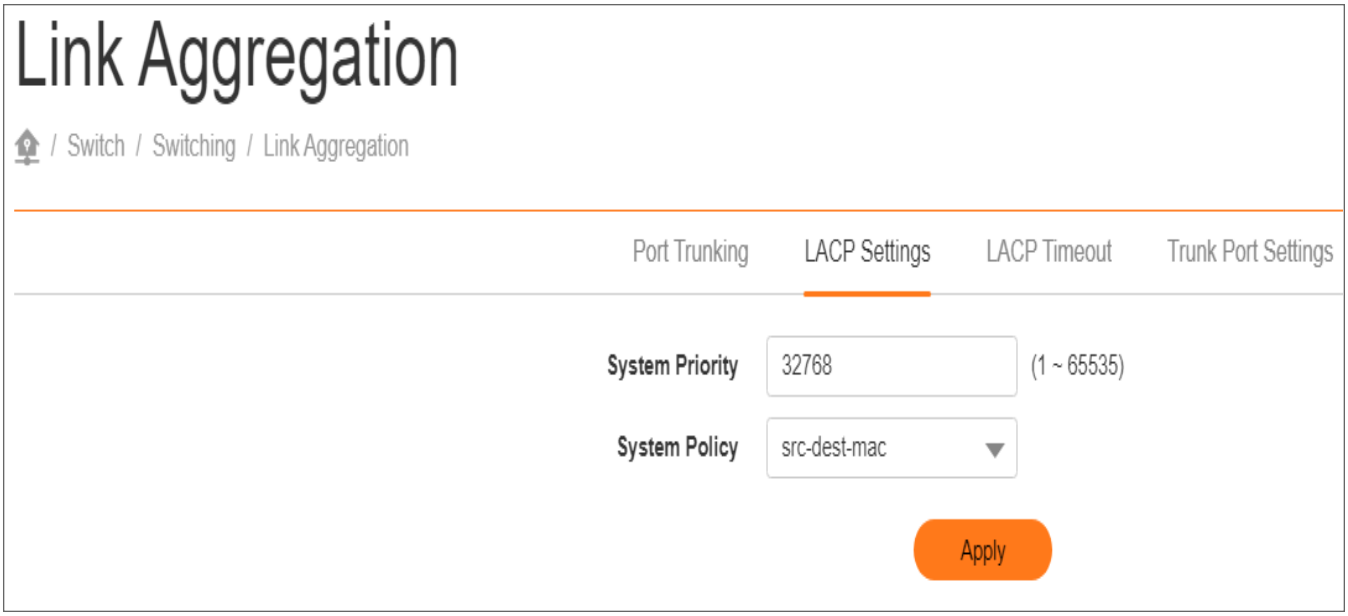


Click **Apply** to accept the changes or **Cancel** to discard them.

Link Aggregation Control Protocol Settings

Assign a system priority to run with Link Aggregation Control Protocol (LACP) and it becomes 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, 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.

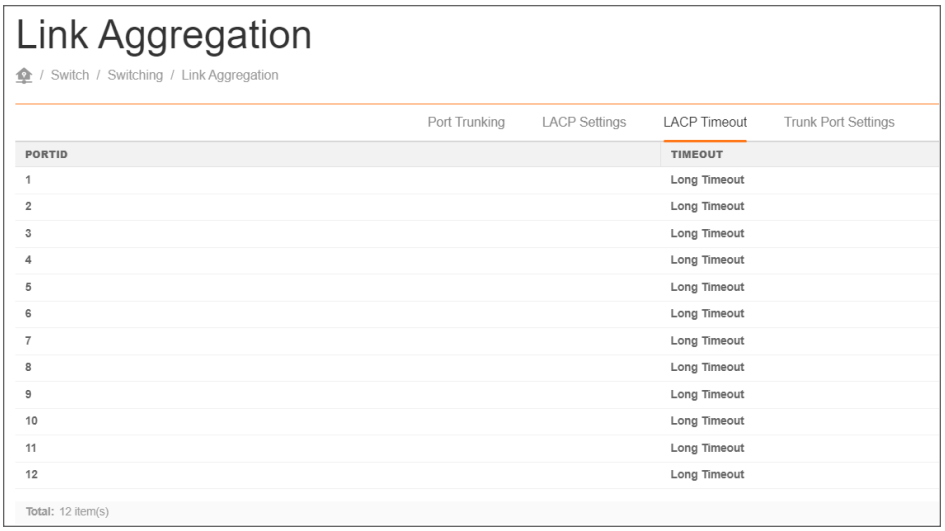


Click **Apply** to update the system settings.

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.

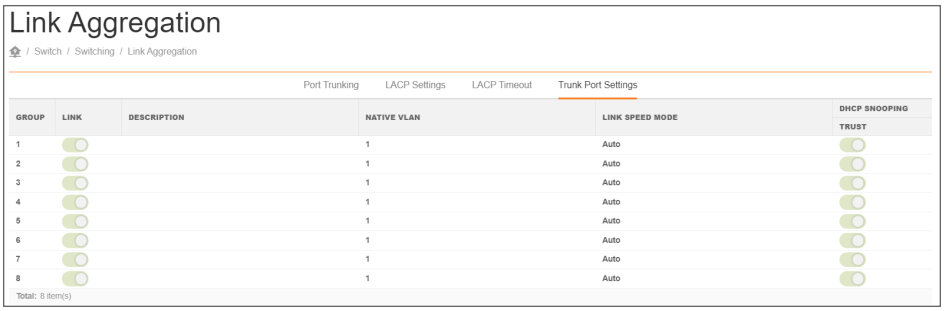
Timeout	Select the administrative LACP timeout. Long - The LACP PDU will be sent for every 30 seconds, and the LACP timeout value is 90 seconds. Short - The LACP PDU will be sent every second. The timeout value is 3 seconds.



Trunk Port Settings

Create one logical link or trunk by aggregating multiple links and configuring port trunking. The trunk link functions as a high-speed link to provide increased bandwidth.

A trunk group is a set of up to eight ports configured as members of the same port trunk.



Link	Enable or disable the link status
Description	Enter a description for this port.
Native VLAN	The Native VLAN field appears when Trunk is selected for VLAN mode. Enter a number between 1 and 4094 in the Native VLAN field to assign the port's Native VLAN (Port VLAN ID). The Native VLAN option allows you to specify the Switch Port VLAN ID for traffic that does not carry a VLAN tag, which can help with SonicWave provisioning. A packet received on a given Switch port is assigned that port's Native VLAN ID and is then forwarded to the port that corresponds 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.

Mode	Select the speed and the duplex mode of the Ethernet connection on this port. The default is Auto Negotiate. Other options are: • 1000 Mbps Full • 100 Mbps Full • 100 Mbps Half • 10 Mbps Full • 10 Mbps Half
DHCP Snooping trust	Enable or disable Trust mode for incoming packets.

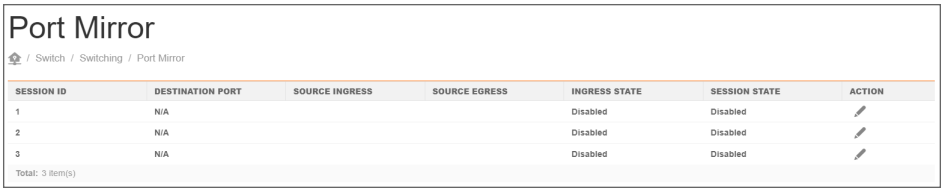
Editing a Trunk Port Setting

To edit a trunk port setting:

1. In the **Link Aggregation > Trunk Port Setting** table, hover on the trunk port to edit and click **Edit** icon.
2. Make the necessary changes and click **Apply** to save the settings.

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. Monitor traffic passing through the mirrored ports by connecting to the mirror destination port.



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.

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 addresses 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.

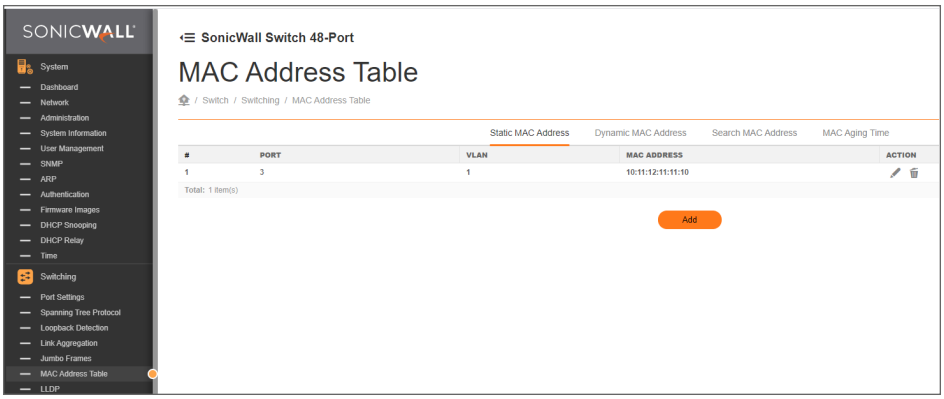
Static MAC Address

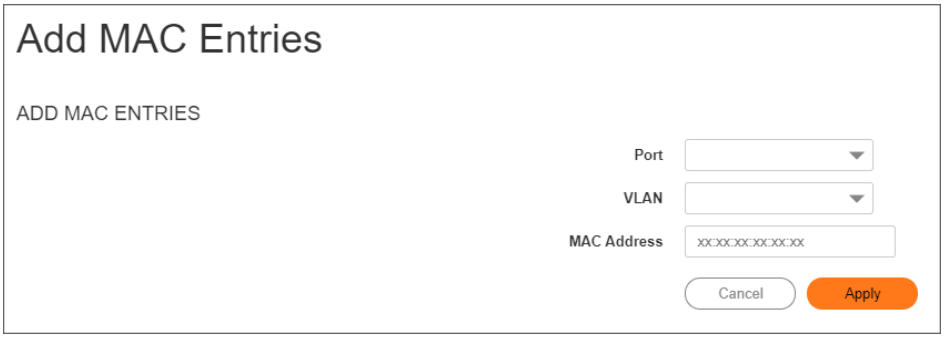
The address table lists the destination MAC address, the associated VLAN ID, and port number associated with the address. When a Static MAC Address is specified, it sets the MAC address to a VLAN or port and makes the entry in its forwarding table. These entries are then used to forward packets through 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 **Add** on the **MAC Address Table** section.

Port	Select the port where the MAC address 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.





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

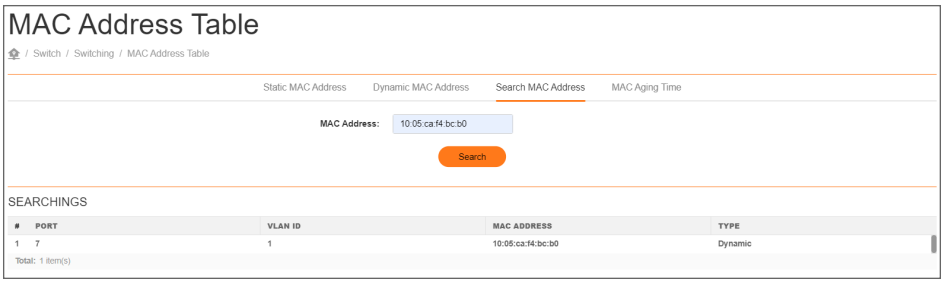
Dynamic MAC Address

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.

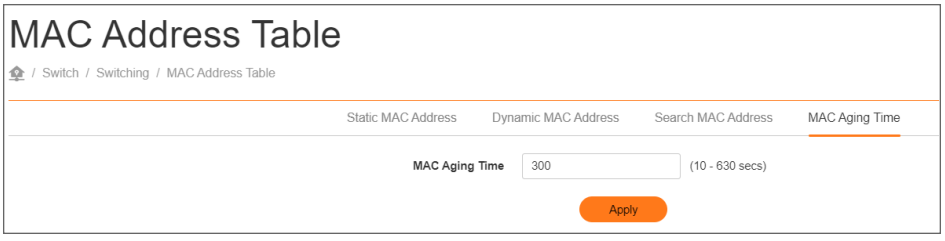
Search MAC Address

Search for a MAC Address using the **Search** field.



MAC Aging Time

The **MAC Aging Time** specifies the time before an entry ages and is discarded from the MAC address table. The range is from 10 to 630; The default value is 300 seconds. Disabling MAC aging is not supported. This age specification applies to all VLANs.



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

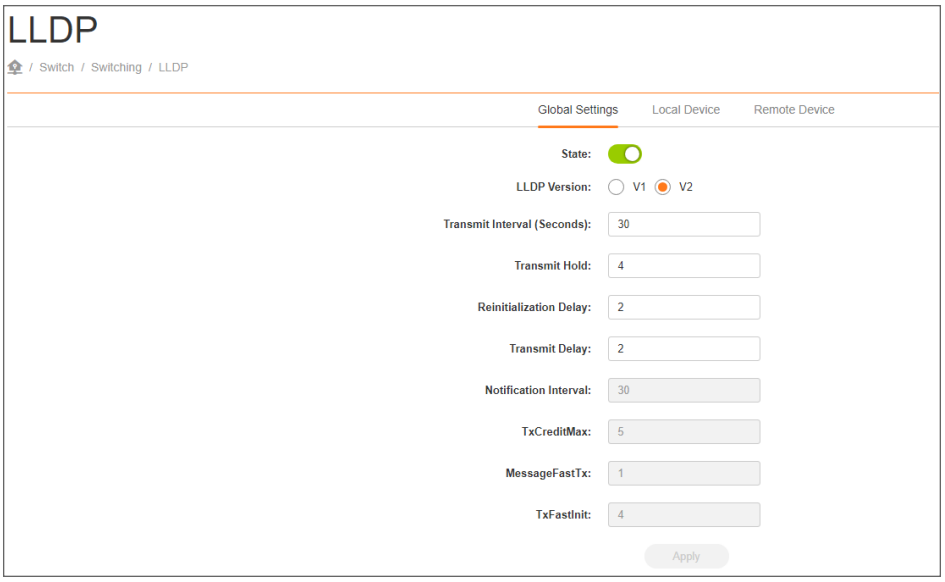
system topology and detect faulty configurations on the LAN. LLDP is essentially a neighbor discovery protocol that uses Ethernet connectivity to advertise information to devices on the same LAN and store information about the network. The information transmitted in LLDP advertisements flow in one direction 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.

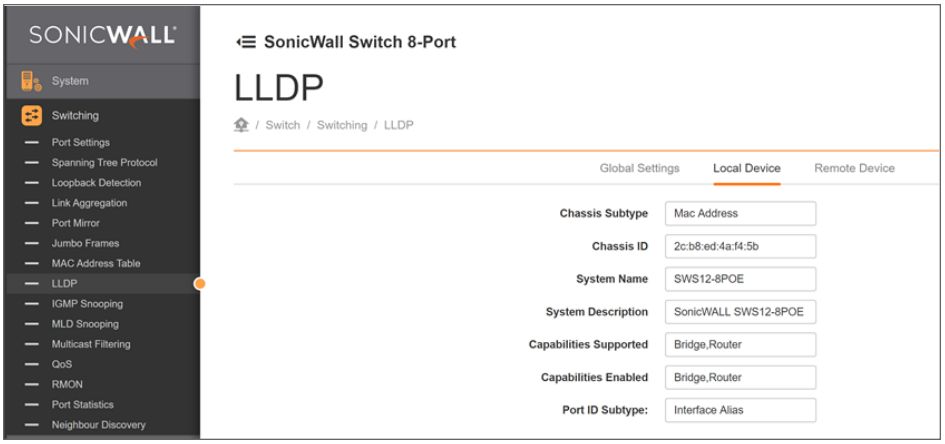
State	Select Enabled or Disabled to activate LLDP for the Switch.
LLDP Version	Select the required LLDP version. By deafult V2 is selected.
Transmission Interval	Enter the interval at which LLDP advertisement updates are sent. The default value is 30. The range is from 5-32767.
Transmit Hold	Enter the 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.
Notification Interval	It is the time interval in which the local system generates a notification-event. In the specific interval, generating more than one notification-event is not possible. It is fixed value and unchangeable.
TxCreditMax	It is the maximum number of consecutive LLDPDUs that can be transmitted at any time. It is fixed value and unchangeable.
MessageFastTx	It is the interval at which LLDP frames are transmitted on behalf of this LLDP agent during a fast transmission period. It is fixed value and unchangeable.
TxFastInit	It is the value used to initialize the TxFast variable which determines the number of transmissions that are made in fast transmission mode. It is fixed value and unchangeable.



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.

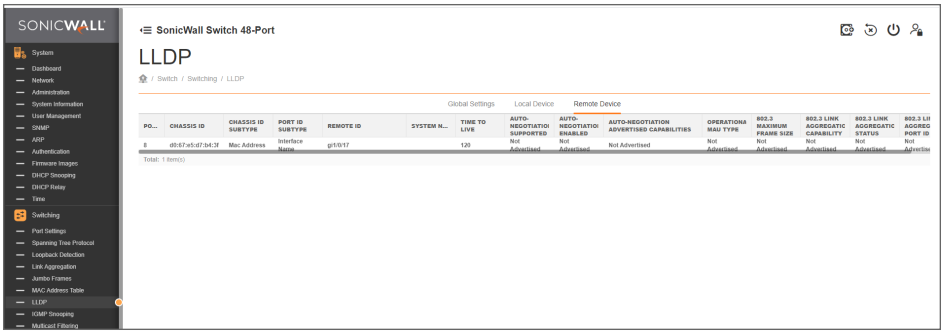
Chassis Subtype	Displays the chassis ID type.
Chassis ID	Displays the chassis ID of the device transmitting the LLDP frame.
System Name	Displays the administratively assigned device name.
System Description	Describes the device.
Capabilities Supported	Describes the device functions.
Capabilities Enabled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



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. Here you can view detailed LLDP information for for devices connected to the switch.

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.



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

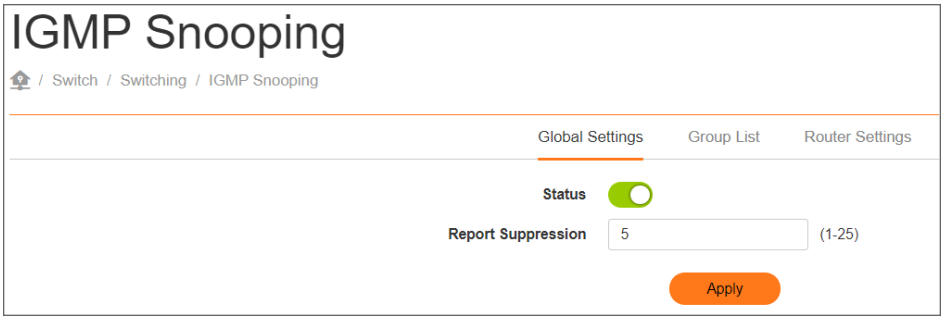
server does not have to establish a separate connection with each client. It merely broadcasts its service to the network, and any host that wishes to receive the multicast register with their local multicast Switch.

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.

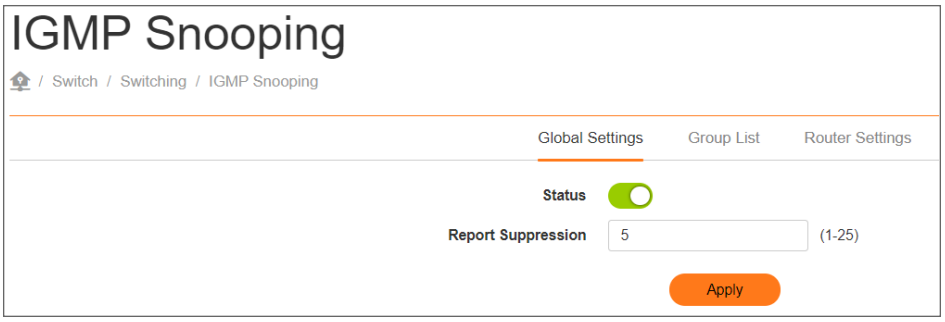
IGMPv1	Defined in RFC 1112. An explicit join message is sent to the Switch, but a timeout is used to determine when hosts leave a group.
IGMPv2	Defined in RFC 2236. Adds an explicit leave message to the join message so that Switch can more easily determine when a group has no interested listeners on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



Global Settings

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

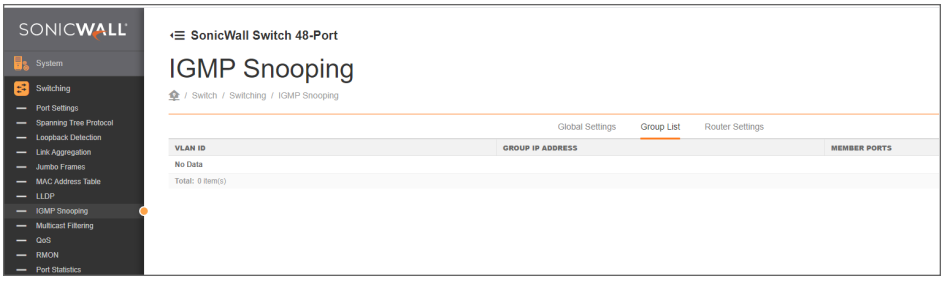
Status	Select to Enable or Disable IGMP Snooping on the Switch. The switch snoops all IGMP packets it receives to determine which segments should receive packets directed to the group address when enabled.
Report Suppression	The Report Suppression feature limits the amount of membership reports the member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



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

Group List

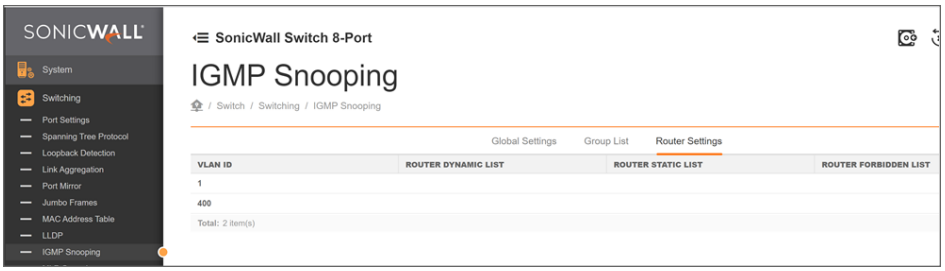
The Group List displays **VLAN ID**, **Group IP Address**, and **Members Port** in the IGMP Snooping List.



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

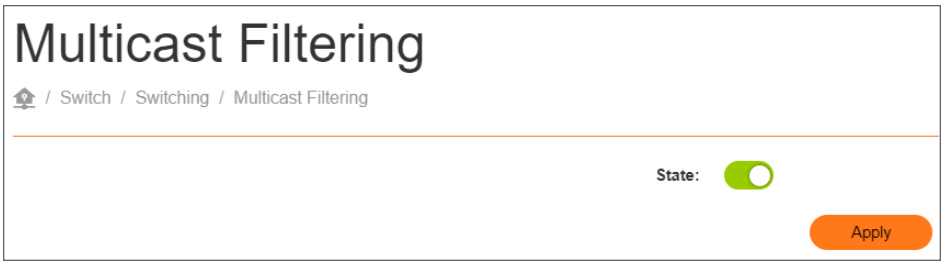


Click **Apply** to accept the changes or **Cancel** to discard them.

Multicast Filtering

Multicast Filtering is used to filter multicast packets destined for devices that are not members of IGMP groups. To know more about IGMP group membership refer to the IGMP Snooping section.

If Multicast Filtering is enabled but IGMP snooping is disabled, all the multicast packets are dropped.



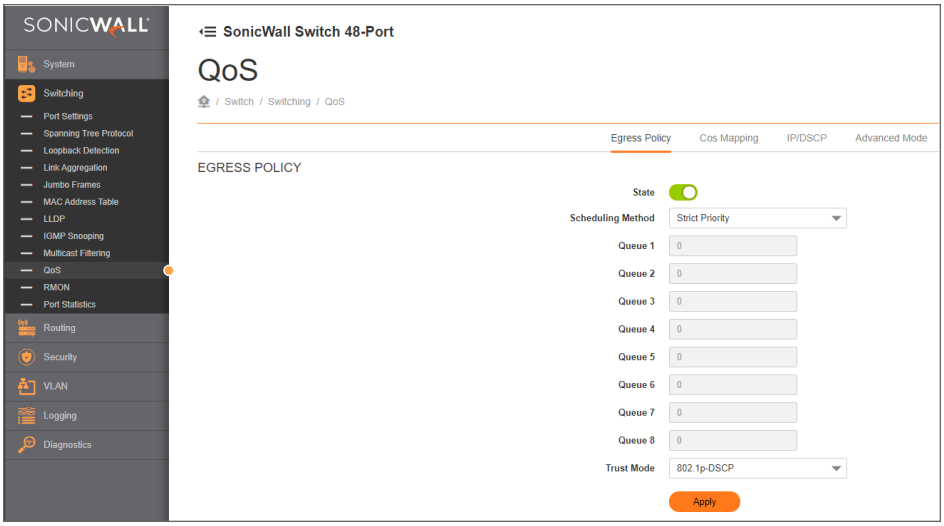
Select whether to enable or disable the Multicast Filtering function.

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. Traffic, 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.

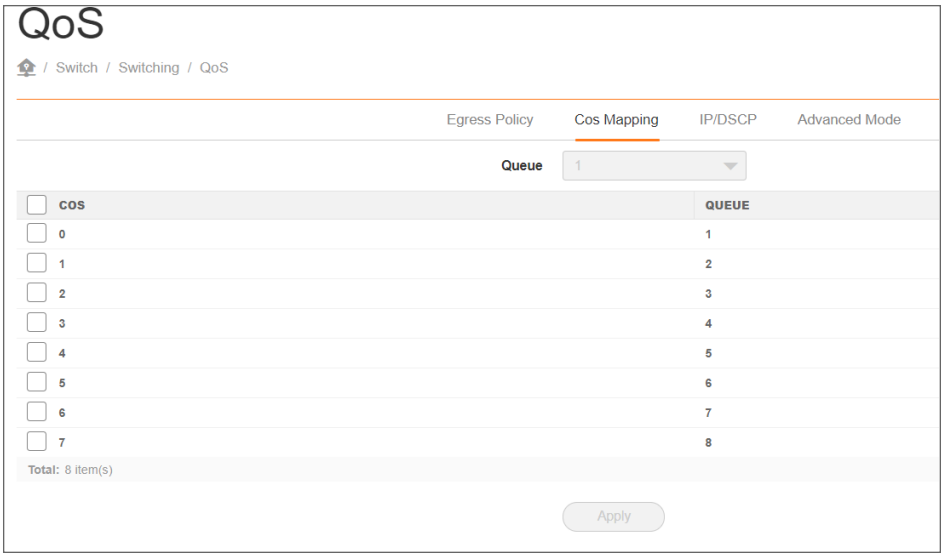
Trust Mode	Select which packet fields to use for classifying packets entering the Switch. • DSCP – Classify traffic based on the DSCP (Differentiated Services Code Point) tag value. • 1p–Classify traffic based on the 802.1p. The eight priority tags that are specified in IEEE802.1p are from 1 to 8.



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.

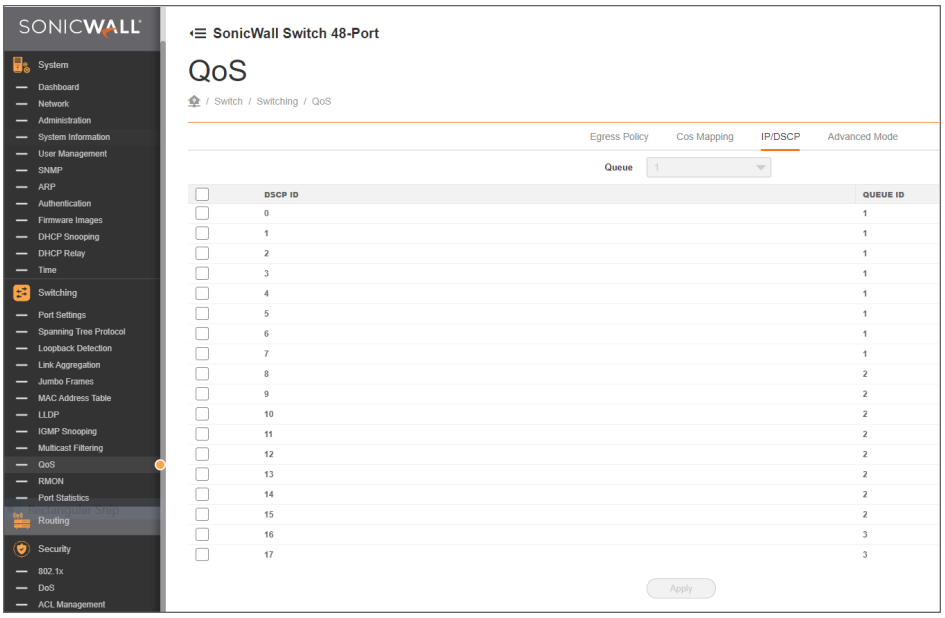


Click **Apply** to save the changes to the system.

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.



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

Advanced Mode

Add and configure the details pertaining to Class and Policy Mappings and view the details under the **Advanced Mode** tab.

Topics:

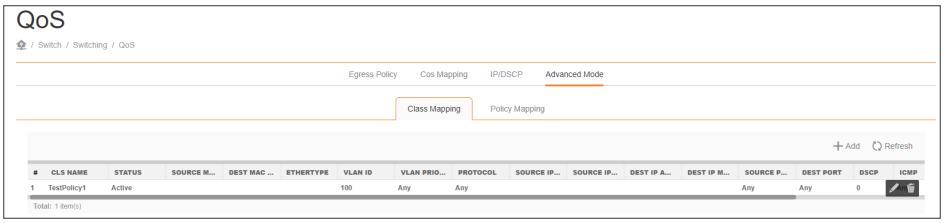
- Class Mapping
- Policy Mapping

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.

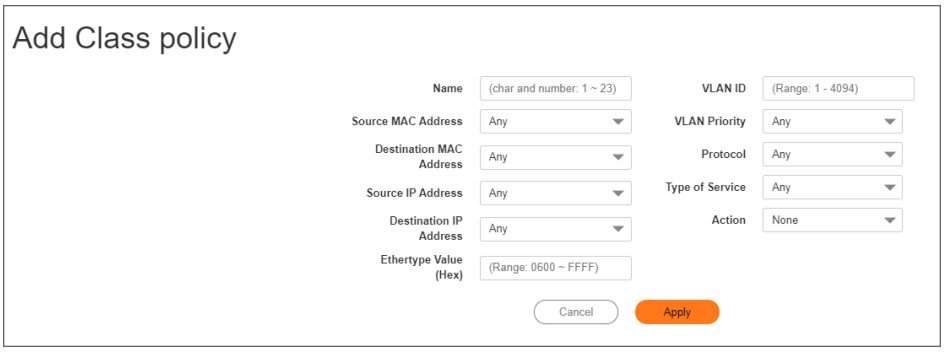


Adding a Class Policy

Under Class Mapping, the details of class policies can be added or configured. Click **Add** to add a new class policy.

Name	Enter the name for the class policy. Using up to 23 alphanumeric characters.
Source MAC Address	Select the Source MAC Address from the drop-down. • Selecting **User Defined** option allows the definition of a 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 the definition of a 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 the definition of a Source IP Address. In the Source IP Mask field, enter the required value. ⓘ **NOTE:** The same IP address can be used for both the source and destination in the configuration.
Destination IP Address	Select the Destination IP Address from the drop-down. • Selecting **User Defined** option allows the definition of a 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 the definition of a 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 the definition of 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 the definition of the VLAN Priority. The VLAN ID Priority range is from 0 to 7. • Selecting **DSCP to match** option allows the definition of the DSCP value. The range is from 0-63.



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 desired class policy and click **Edit** icon.
2. Make the necessary changes and click **Apply** to save the settings.

Deleting a Class Policy

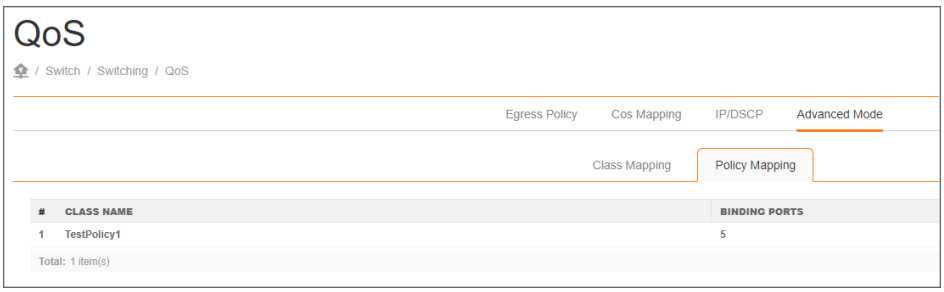
To delete a class policy:

1. In the **Class Mapping** table, hover on desired class policy 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.



Editing a Policy Mapping

To edit a policy mapping:

1. In the **Policy Mapping** table, hover on desired class policy and click **Edit** icon.
2. Make the necessary changes and click **Apply** to save the settings.

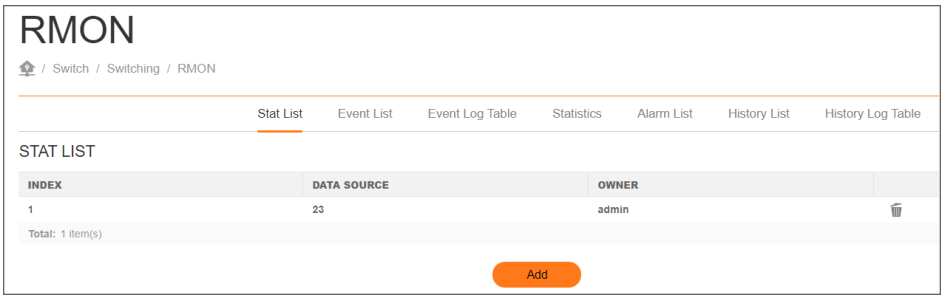
Remote Network Monitoring

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.



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.

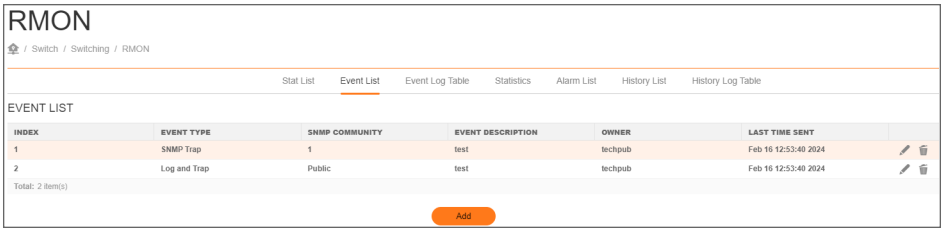
To delete Stats Data:

1. Click **Delete** icon on the stat list which is to be deleted.
   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.

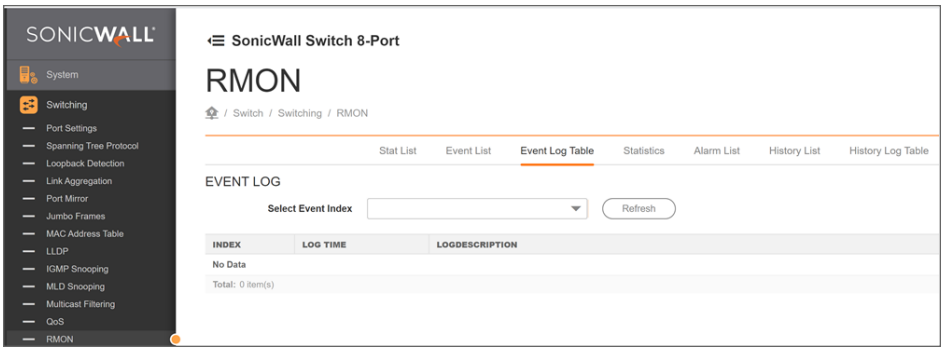
Index	Enter the entry number for Event.
Event Type	Select the event type. • Log – The event is a log entry. • SNMP Trap – The event is a trap. • Log and Trap – The event is both a log entry and a trap.
SNMP Community	Enter the community to which the event belongs created in **System > SNMP > Community**.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



Event Log Table

View specific Event logs for the Switch in the Event Log Table. Choose an Event log to view from the drop-down list.

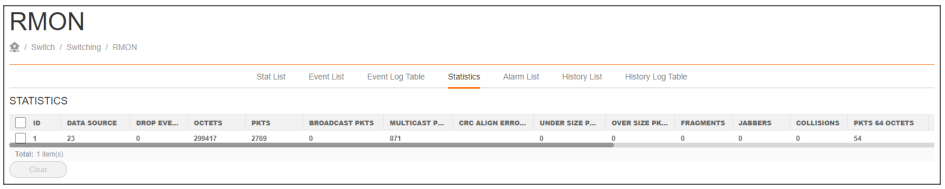
Select the index of the Event Log from the list.



Statistics

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

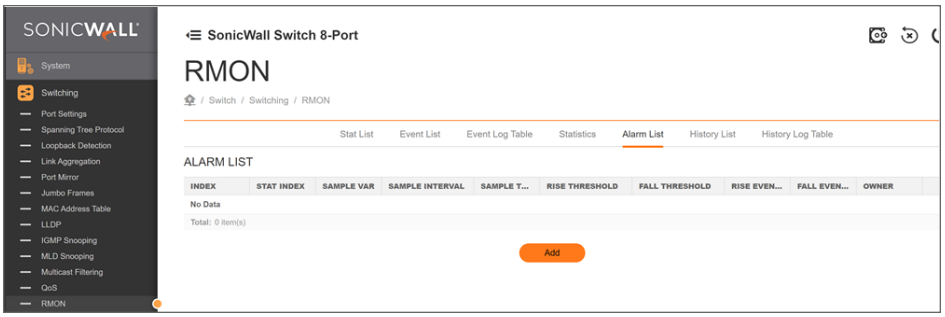
ID	Shows the specific port for which RMON statistics are displayed.
Data Source	Displays the data source from which the data is collected.
Drop Event	Displays the number of dropped events that have occurred on the port.
Octets	Displays the sample number from which the statistic taken.
Pkts	Displays the 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.



Alarm List

Configure Network alarms to occur when a network problem is detected. To add an alarm, click the Add button and select the alarm from the drop-down boxes.

Index	Enter the entry number for the History Log Table.
Sample Stat	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.

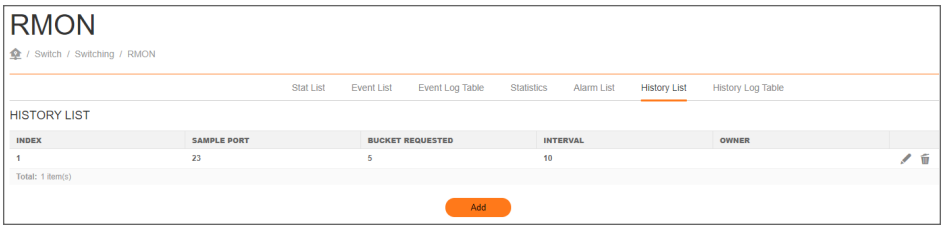


History List

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

Click Add to create the History List.

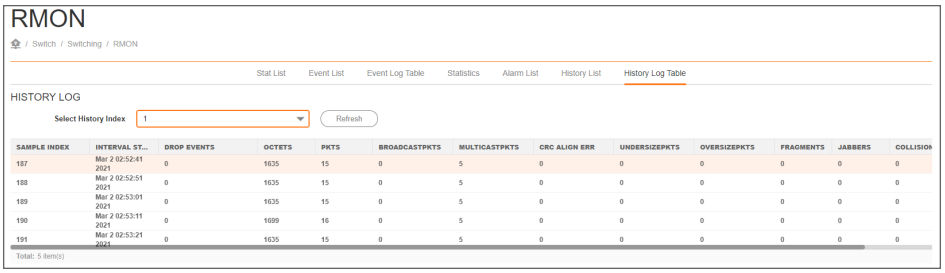
Index	Enter the entry number for the History Log Table.
Sample Port	Select the port from which the history samples were taken.
Bucket Requested	Enter the number of samples to be saved. The range is from 1- 50.
Interval	Enter the time that samples are taken from the ports. The field range is from 1-3600.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



History Log Table

View the History Index for the History Logs available on the Switch within the History Log Table. Select a History Index to view from the drop-down box.

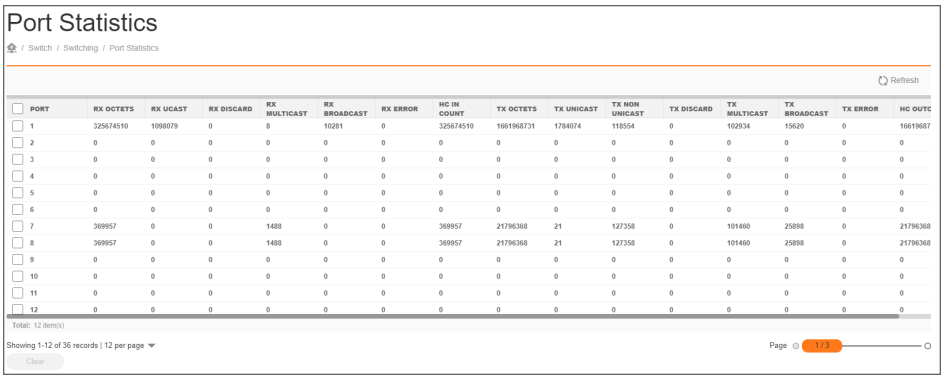
Sample Index	Displays the index value for the sample which is collected on the port for a particular interval of time.
Interval Start	Displays the starting time for the sample collected on the port.
Drop Events	Displays the number of dropped events that have occurred on the port.
Octets	Displays the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



Port Statistics

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

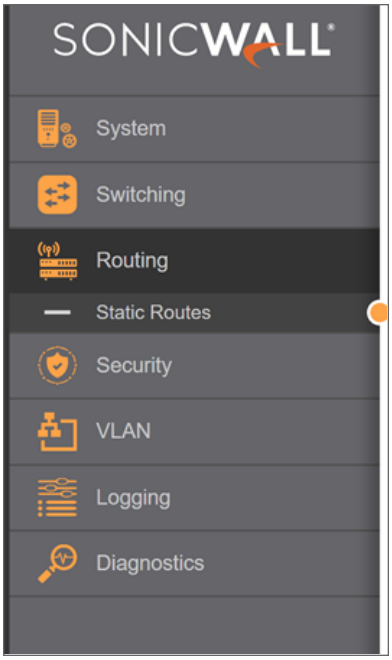
Port	Displays the port for which statistics are displayed.
RX OCTETS	Displays the number of all packets received on the port.
RX UCAST	Displays the number of non-Unicast packets received on the port.
RX NON UCAST	Displays the number of non-Unicast packets received on the port.
RX DISCARD	Displays the 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 non-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.



ⓘ | **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.

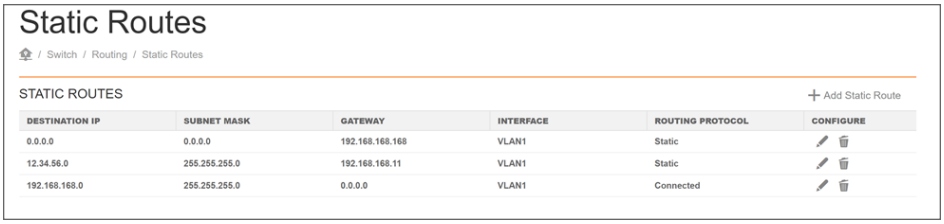


Static Routes

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.



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

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 MAC Authentication Bypass (MAB) is an access control technique which uses the MAC address of a device to determine what kind of network access should be provided to hosts. For MAB authentication mechanism, the switch will transmit an Access-Request message to the RADIUS server, with the 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 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

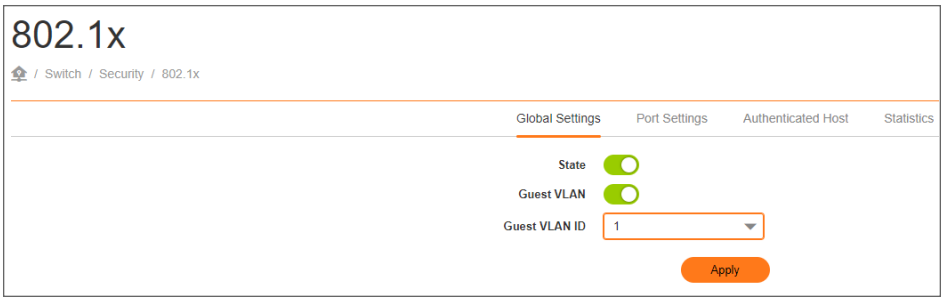
1. For MAB authentication mechanism, the switch will transmit an Access-Request message with the host source MAC address as user and password. In the RADIUS server configuration, the format of the MAC address should be 12 hexadecimal digits, all lowercase and no punctuation.
2. If the host source MAC address is saved as a 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**, the host will be authenticated with EAP by default. If the host does not support EAP, 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 to **802.1X Mode 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 802.1x Guest VLAN and RADIUS VLAN assignment are disabled.)
9. In **MAC-based** mode, host information will be cleared after configuring the max host number. Hosts that have passed authentication will have to be authenticated again.
10. Host information will be cleared after authentication mode, link status or MAB mode has changed.
11. **MAC Based** mode does not support MAB hybrid mode.(**MAC-Based** mode can only be enabled when 802.1x MAB is mab_mode or disabled.)
12. Max host count is only effective when using **MAC-based authentication** mode.

Global Settings

Within Global Settings, 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 from the list.

State	Select whether authentication is Enabled or Disabled on the Switch.

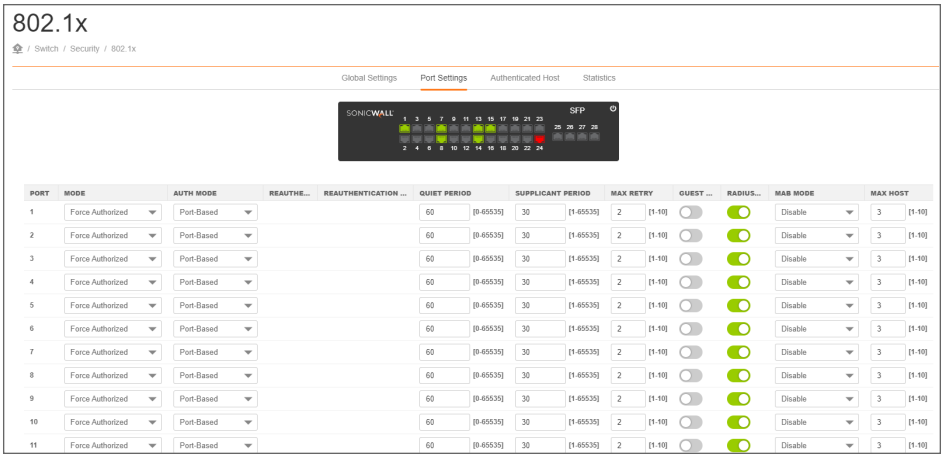
Guest VLAN	Select whether Guest VLAN is Enabled or Disabled on the Switch. The default is Disabled.
Guest VLAN ID	Select the guest VLAN ID from the list of currently defined VLANs.



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.

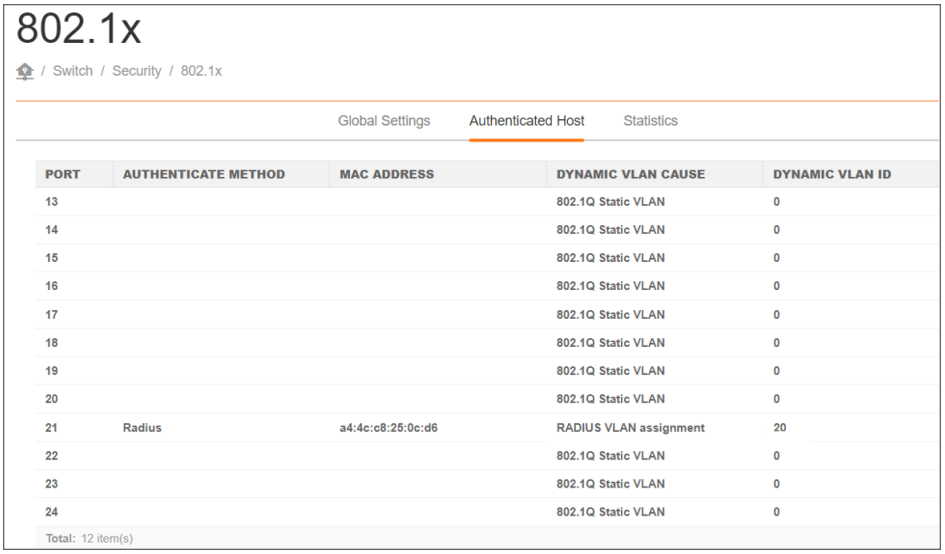


Port	Displays the ports for which the 802.1X information is displayed
Mode	Select the Auto or Force UnAuthorized or Force Authorized mode from the list.
AuthMode	Select the Port-Based or MAC-Based from the list.
Reauthentication	Displays whether port reauthentication is Enabled or Disabled.
Reauthentication 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.



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

Statistics

The **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.

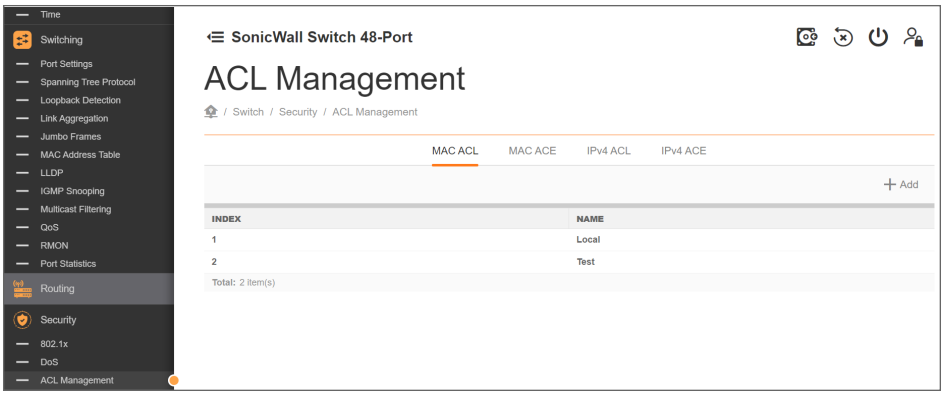
State: Enable or disable DoS to prevent the switch from DoS attacks

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

ACL Management

Access Control List (ACL) allows the definition of the criteria required to allow or block access to the network or specific resources. ACLs can provide basic security for access to the network by controlling whether packets are

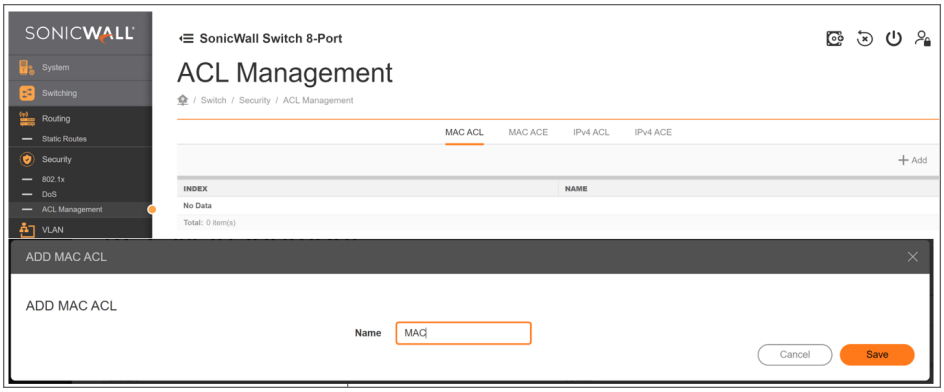
forwarded or blocked at the Switch ports. ACLs are filters to classify data packets according to a particular content in the packet header, such as the source address, destination address, source port number, destination port number, and more. Packet classifiers identify flows for more efficient processing. 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.



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. Up to 32 alphanumeric characters can be used.

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

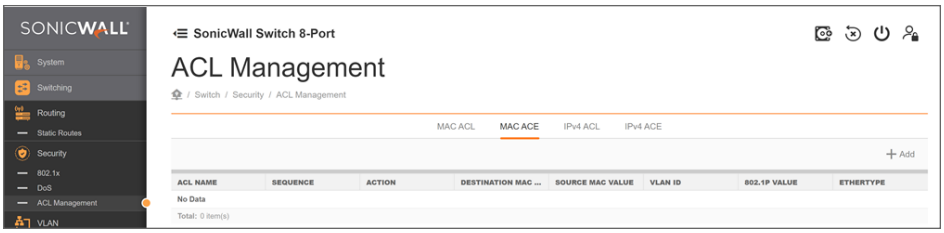


Click **Save** to accept the changes or **Cancel** to discard them.

MAC-Based ACE

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

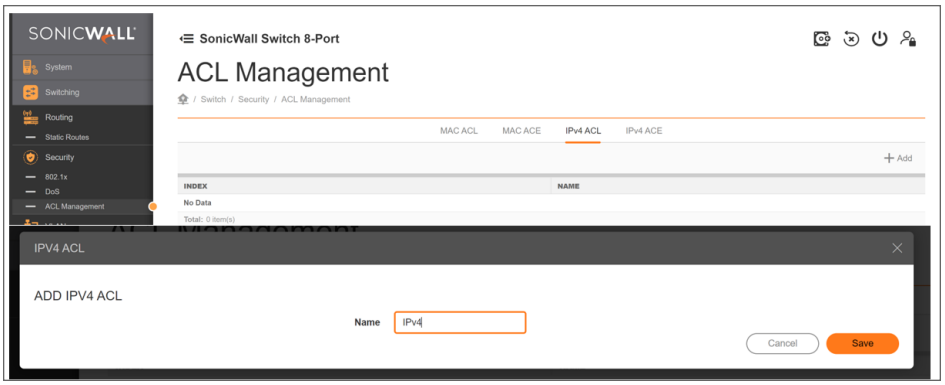
ACL Name	Select the ACL from the list.
Sequence	Enter the sequence number which signifies the order of the specified ACL relative to other ACLs assigned to the selected interface. The valid range is from 1-2147483646, 1 being processed first.
Action	Select what action taken if a packet matches the criteria. • 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.



IPv4 ACL

Allows the IP Based ACL to be defined.

Index	Displays the current number of ACLs.
Name	Enter the IP based ACL name, using up to 32 alphanumeric characters.



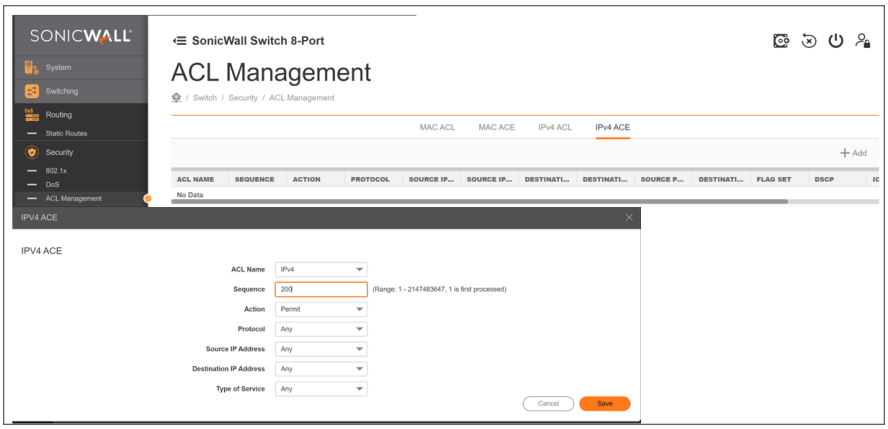
Click **Save** to accept the changes or **Cancel** to discard them.

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. The range is from 0-255. • 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.



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

After creating the MAC or IPv4ACL, 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.

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 network traffic. A VLAN is 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

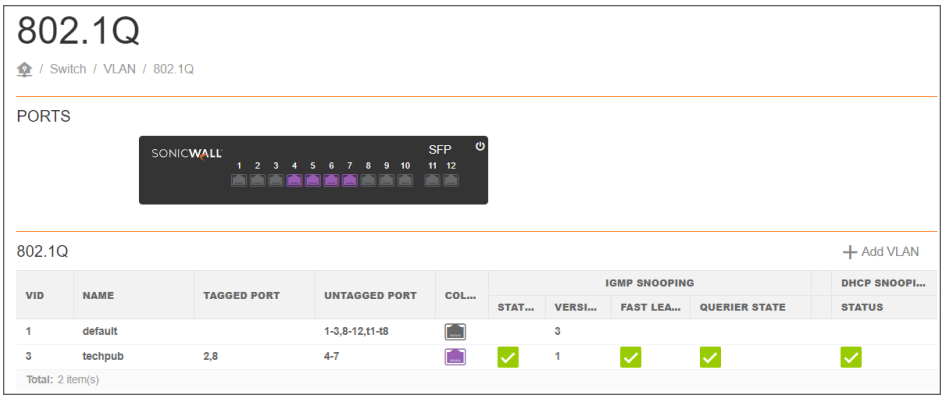
802.1Q

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 an 802.1Q VLAN configuration, ports are then configured 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 2-4094. ⓘ | **NOTE:** VLAN 1 is created by default.
Name	Enter the VLAN name, using 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 port-based VLANs are enabled, then 802.1Q VLAN is disabled.

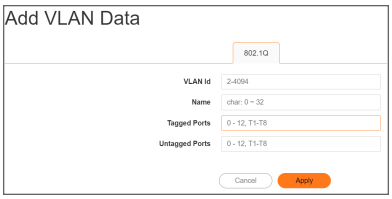
ⓘ | **NOTE:** The Switch's default setting is to assign all ports to a single 802.1Q VLAN(VID 1). Please keep this in mind when configuring the VLAN settings for the Switch.



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

1. Click the Add VLAN button.
2. Enter the VID and name in the VID and Name text boxes.

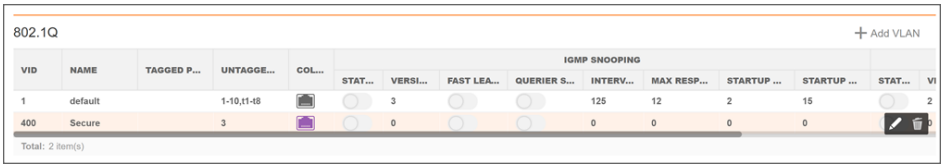
3. Enter the tagged Ports as required.
4. Enter the Untagged Ports as required.



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 to remove and entry. A confirmation dialog is displayed.

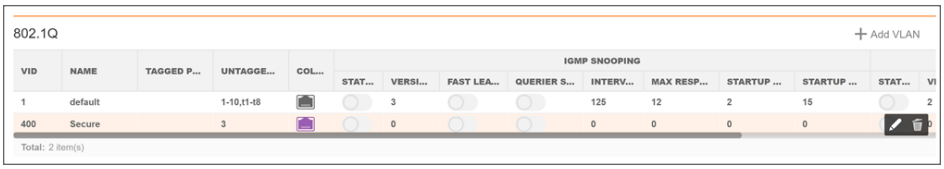


2. Click **Confirm** to continue or **Cancel** to abort the changes.
   ⓘ | **NOTE:** Any port associated with this VLAN will be reset to the default VLAN (VLAN 1).

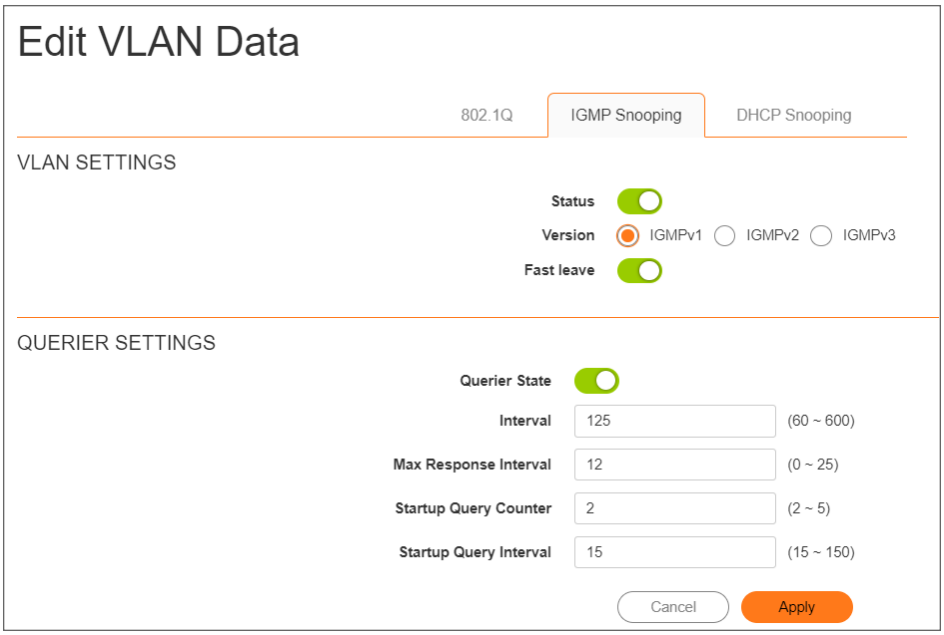
Configuring IGMP Snooping Settings

To edit an item in the 802.1Q list, and configure IGMP Snooping settings follow the below steps:

1. Click the  edit button in the row.



2. Click on the **IGMP Snooping** tab and select the required VLAN and Querier settings.



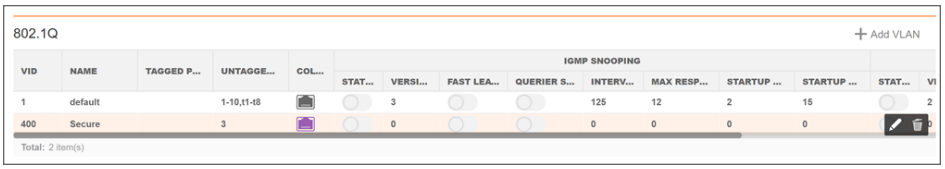
Status	Enable or Disable IGMP Snooping
Version	Select the operating version of the IGMP snooping Switch for a specific VLAN.
Fast leave	Enable or disable Fast leave to remove the port information from a multicast group entry immediately after fast leave message is received.
Querier State	Enable or Disable Querier State
Interval	Enter the time interval at which the IGMP snooping queries are sent by the Switch when configured as querier on a VLAN. The value range is between 60 to 600 seconds.
Max Response Interval	Enter the maximum response code inserted in general queries sent to host. The unit of the response code is tenth of second. This value ranges between 0 and 25.
Startup Query Counter	Enter the maximum number of general query messages sent out on Switch startup when the Switch is configured as a querier. This value ranges between 2 and 5.
Startup Query Interval	Enter the time interval between the IGMP snooping query messages sent by the Switch, during startup of the querier election process. This time interval ranges between 15 and 150 seconds and should be less than or equal to query interval divided by four.

3. Click **Apply**.

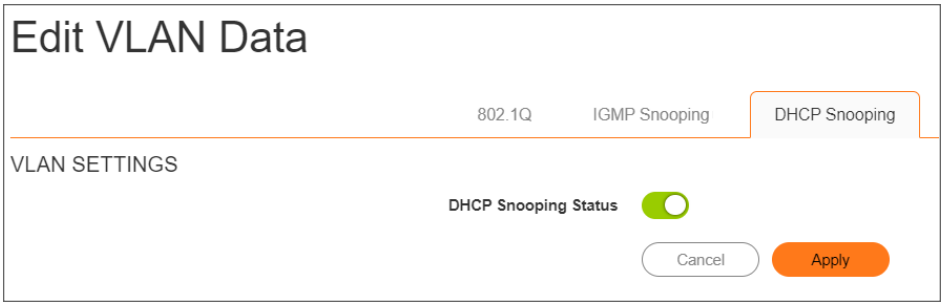
Configuring DHCP Snooping Status

To edit an item in the 802.1Q list, and configure DHCP Snooping status follow the below steps:

1. Click the  edit button in the row.



2. Click on the **DHCP Snooping** tab and select the required VLAN and Querier settings.



3. Enable or disable the **DHCP Snooping Status**.
4. Click **Apply**.

Configuring Access and Trunks using Standalone access

A trunk port is a specific type of network switch that allows data to flow across a network node for multiple virtual local area networks (VLANs). It can pass numerous VLANs and VLAN traffic through it. Usually, a switch's uplink port is configured as a trunk. Trunk ports are also used to extend a network, connecting VLANs with the same VLAN ID that is configured on multiple switches. These may also be referred to as a tagged port.

An access port is a switch port dedicated to a specific network. It transports traffic to and from only the specified VLAN allotted to it. Unlike a trunk port, it will not deliver exclusive identifying tags (802.1Q or ISL tags) because the VLAN intended for it is pre-assigned. These may also be referred to as an untagged port.

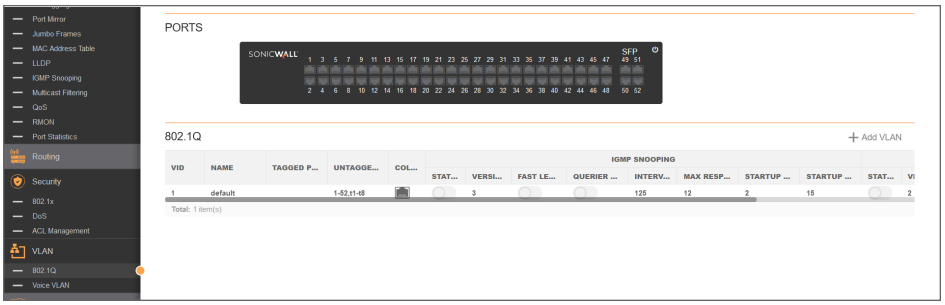
Usually, an access port has only a single VLAN set up on the interface, and it carries traffic for that VLAN. If the VLAN for an access port is not configured, the interface can carry traffic using only the default VLAN, which is usually VLAN 1 (native VLAN).

It is possible to configure Ethernet interfaces as access or trunk ports, but they cannot function simultaneously as both types of ports.

To configure Trunk and access ports on a SonicWallSwitch while using in Standalone configuration:

By default, all the ports of the SonicWall Switch are a part of the Native VLAN 1. So, by default, the configurations will be that all the ports are untagged in the native VLAN.

Create a new VLAN and make a few ports part of it. Use one port as an uplink port that connects to the upstream firewall or router with new VLAN configurations and other VLAN configurations. To accomplish this, configure some ports as access ports of the new VLAN and the uplink port as the trunk port, which also passes the new VLAN traffic along with the other VLAN traffic. Consider the following example:



1. Go to **VLAN > 802.1Q**.
2. Click **Add VLAN**.
    a. Enter the VLAN ID, for example 2.
    b. Enter the Name. For example, Data traffic
    c. Under tagged port, enter the port number to pass traffic for multiple VLANs. For example, 48.
    d. In Untagged ports, enter the port numbers to accept traffic for only a single VLAN. For example, 1-20.
    e. Click Apply.

Ports 1-20 are part of VLAN 2, and port 48 is part of the trunk port that passes VLAN 2 traffic.

To make VLAN 2 pass to a downstream device along with other VLANs through port 30, add port 30 in the tagged ports of VLAN 2.

1. Go to **VLAN > 802.1Q**.
2. Hover over the VLAN ID, and click the  edit icon to edit VLAN ID 2.
3. Under tagged port, enter the port number 30 to pass traffic for multiple VLANs. For example, 48,30.
4. In Untagged ports, enter the port numbers to accept traffic for only a single VLAN. For example, 1-20.
5. Click Apply.

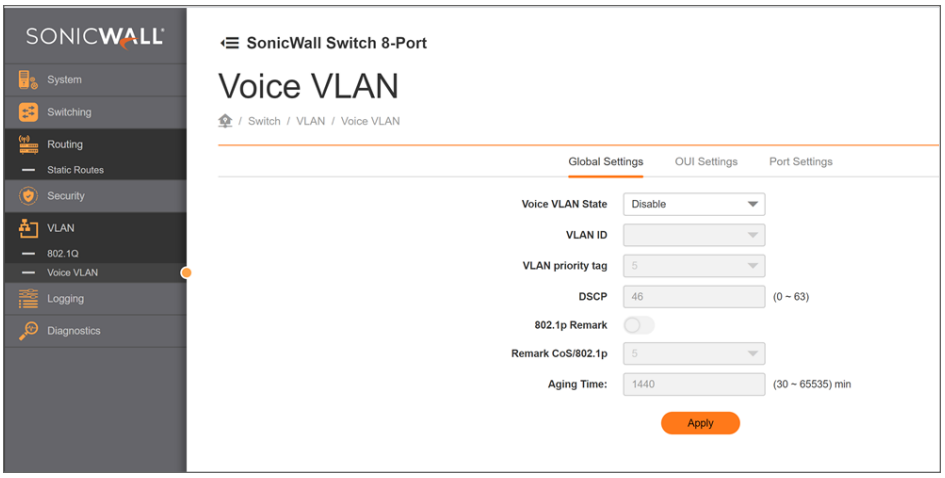
Port 30 also acts as a trunk port. VLAN 2 is tagged along with all the other tagged VLANs.

ⓘ **TIP:** Many VLANs can be tagged on a single port, but only one VLAN can be untagged on a port. That means a port can be a trunk port and pass as many VLANs as it is tagged in, but it can be an access port of only a particular VLAN.

Voice VLAN

Enhance the Voice over IP (VoIP) service by configuring ports to carry VoIP traffic from IP phones on a specific VLAN. Voice VLAN provides QoS to VoIP, ensuring that the Voice VLAN traffic is processed with the appropriate QoS priority if the switch processor is in high contention.

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.



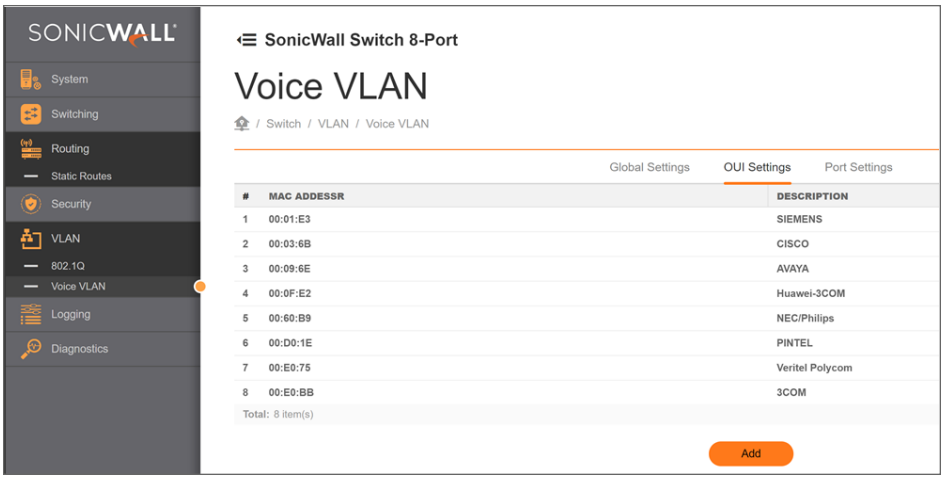
Click **Apply** to update the system settings.

OUI Settings

The switch 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 or 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. 00:01:E3 - Assigned to Siemens IP Phones. 00:03:6B - Assigned to Cisco IP Phones. 00:09:6E - Assigned to Avaya IP Phones. 00:0F:E2 - Assigned to Huawei-3COM 00:60:B9 - Assigned to NEC/Philips IP Phones. 00:D0:1E - Assigned to Pintel IP Phones. 00:E0:75 - Assigned to Veritel IP Phones. 00:E0:BB - Assigned to 3COM 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.



Port Settings

Voice VLAN provides QoS to VoIP, ensuring that the quality of voice does not deteriorate if the switch resources are in contention. Hover over the required Port ID, and click the  edit icon to edit the port settings.

Port ID	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 create and post-event notification messages in response to events, faults, or errors occurring on the platform and changes in configuration or other occurrences across an IP network to Syslog servers or local to the device. A syslog server can collect the event messages, providing robust support for users to monitor network operations 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

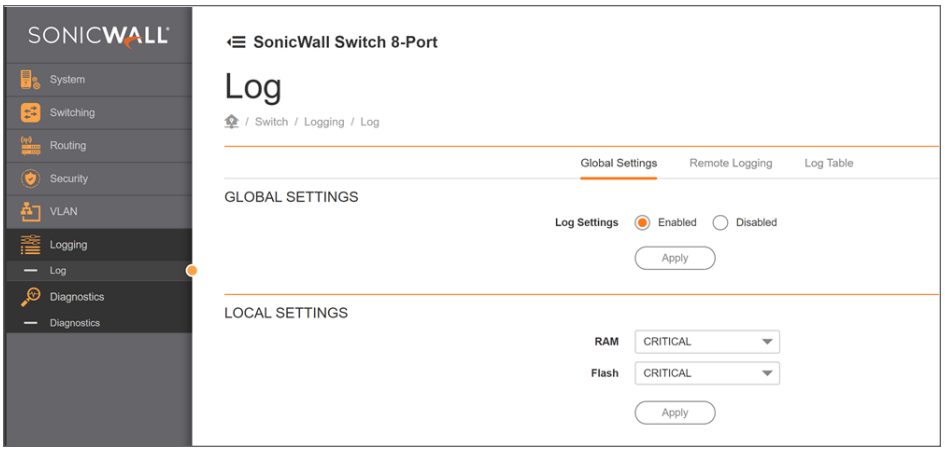
the syslog server. Refer to the documentation of your syslog program for details. The following table describes the syslog severity levels.

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

Enable or Disable the **Log settings** for the switch within the **Global Settings** option.

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



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

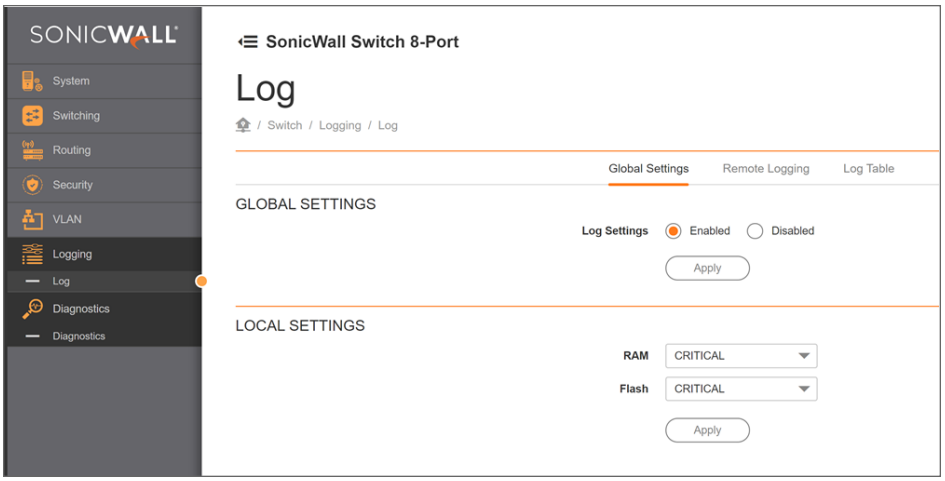
Local Settings

The Switch supports log output to two locations, Flash and RAM. The information stored in the system's RAM log will be lost after the Switch is rebooted or powered off, whereas the information stored in the System Flash will be retained 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 Error is selected for the logging level, the logged messages include Error, Critical, Alert, and Emergency.

RAM	Log stored in RAM. Will only be erased after system reset.
Flash	Log erased after reboot or power off

Refer to Logging for severity level details.



EMERGENCY	If the Switch is not functioning properly, an emergency log message is saved to the specified logging location.

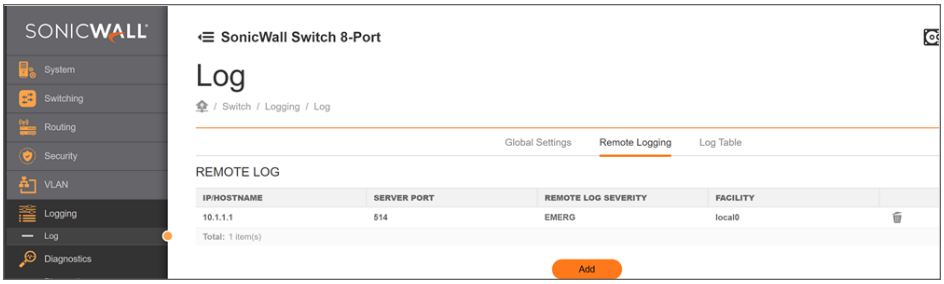
ALERT	If there is a serious Switch malfunction, then all Switch features are down.
CRITICAL	A critical log is saved if a critical Switch malfunction occurs.
ERROR	If triggered, a device error has occurred.
WARNING	The device is functioning, but an operational problem has occurred.
NOTICE	This will provide information about the Switch.
INFO	This will provide information about the Switch.
DEBUG	This will provide a debugging message.

Click **Apply** to accept the changes.

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 administrator 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 of the host configured for syslog.
Server Port	Specify the port on the host to which syslog messages are sent.
Remote Log Severity	Refer to severity level table Logging section. Logs with the selected severity level and all logs of greater severity are sent to the host. For example, if Error is selected, the logged messages include Error, Critical, Alert, and Emergency
Log 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.

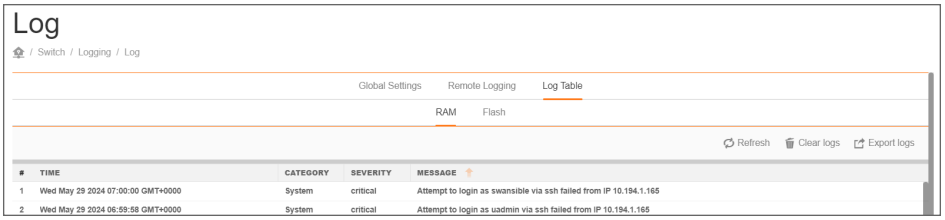


Click **Apply** to accept the changes or **Cancel** to discard them.

Log Table

From the Log Table the log history can be viewed and deleted. Select the log location in RAM or Flash to view.

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.
Refresh	Click **Refresh** to refresh the log data.
Clear logs	Click **Clear logs** to clear the buffered log in the memory Diagnostics.
Export logs	Click **Export logs**. Log data downloads automatically to a local machine as a *.log* file. For example, the downloaded file name is SWS12- 10FPOE_v1.2.1.x-xram.log



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

Diagnostics

This section provides you the configuration information for the following:

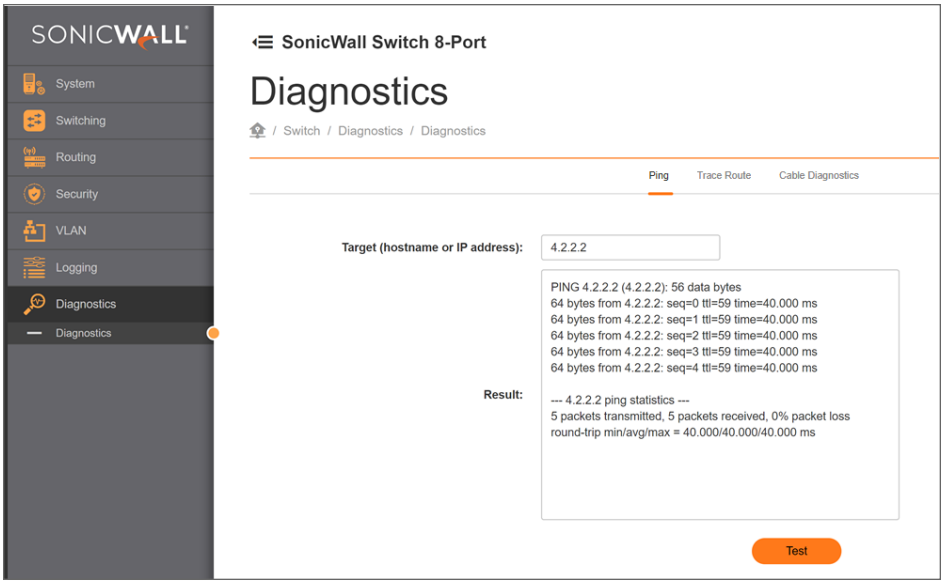
- Ping
- Trace Route
- Cable Diagnostics
- Tech Support Report

Ping

The Packet Internet Groper (Ping)Test allows you to verify connectivity to remote hosts. The test operates by sending Internet Control Message Protocol (ICMP) request packets to the tested host and waiting for an ICMP response. In the process, it measures the time from transmission to reception and records any packet loss. With this diagnostic tool, a ping request is sent to a specified IPv4 address to check whether the switch can communicate with a particular network host.

Test parameters can be varied by entering the data in the appropriate boxes. To verify accuracy of the test, it is recommended to run multiple tests in case of a test fault or user error.

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



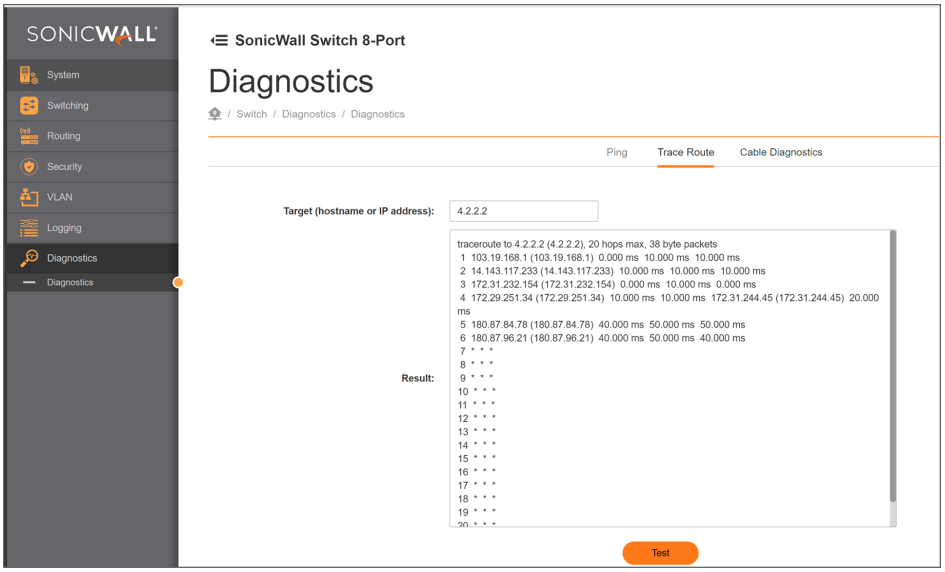
Trace Route

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

In testing, it will tell 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 hostname of the station to trace the route.
Result	Displays the trace route results.

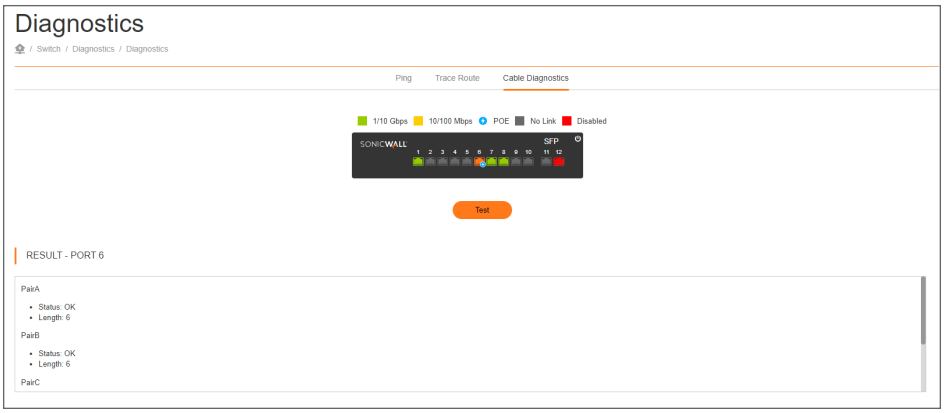
Click **Test** to initiate the trace route.



Cable Diagnostics

The Cable Diagnostics feature helps identify any connectivity problems with cabling and provides information about where errors may have occurred. The tests utilize Time Domain Reflectometry (TDR) technology to assess the quality of a copper cable connected to a port. TDR works by detecting cable faults through the transmission and analysis of a signal sent through the cable. However, it's important to note that TDR may yield different results based on the status of the port, and these results must be interpreted accordingly.

- Select any port and click **Test** to initiate the cable diagnostics. The result of the port is displayed.
- The result displays the local pair's status and length of the cable.



Tech Support Report

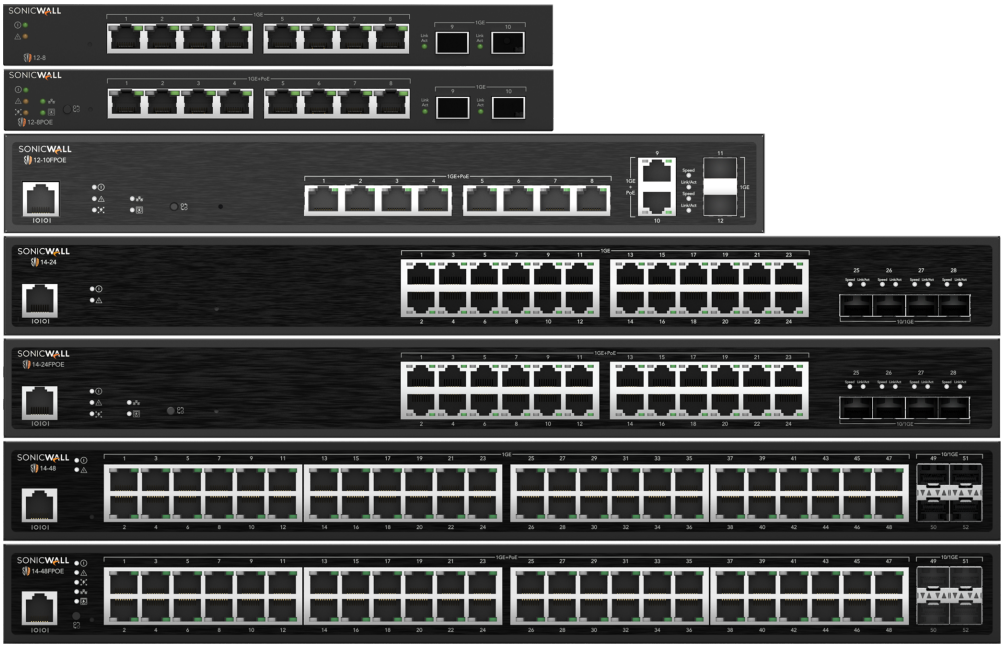
To download required tech support files:

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

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

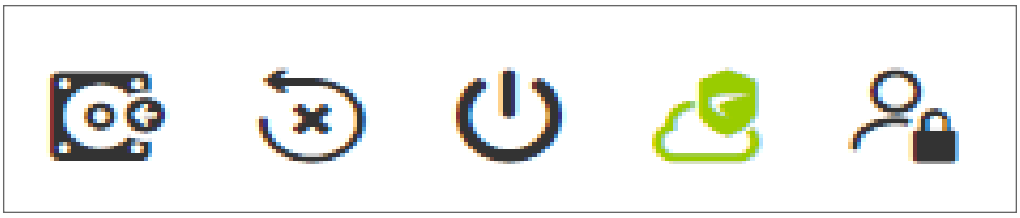
3

System Maintenance



The maintenance bar provides maintenance functions, including upgrading firmware, resetting the configuration to factory default standards, rebooting the device, resetting cloud management, and logging out of the interface.

The following represents the Maintenance Menu bar:



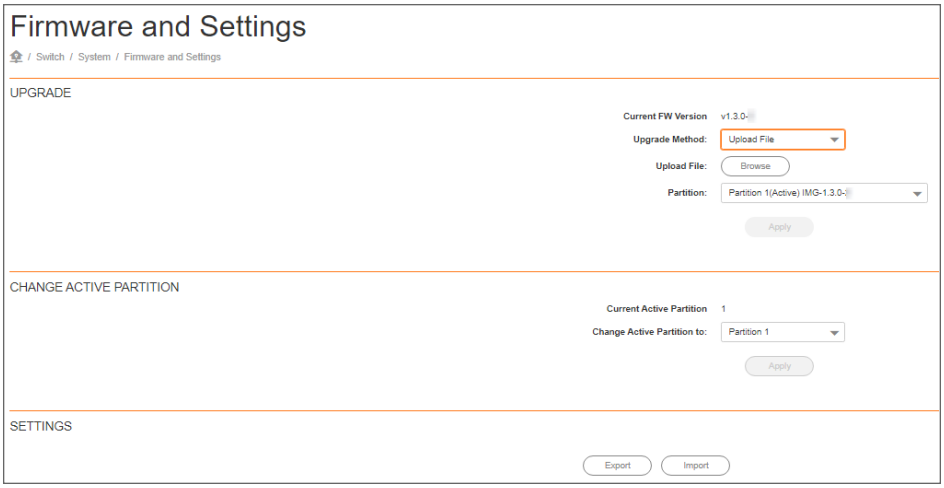
Upgrading

Firmware can be upgraded using two methods

- Upload
- SonicWall Cloud Server

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 of the 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.



A prompt displays to confirm the Firmware Upgrade.

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

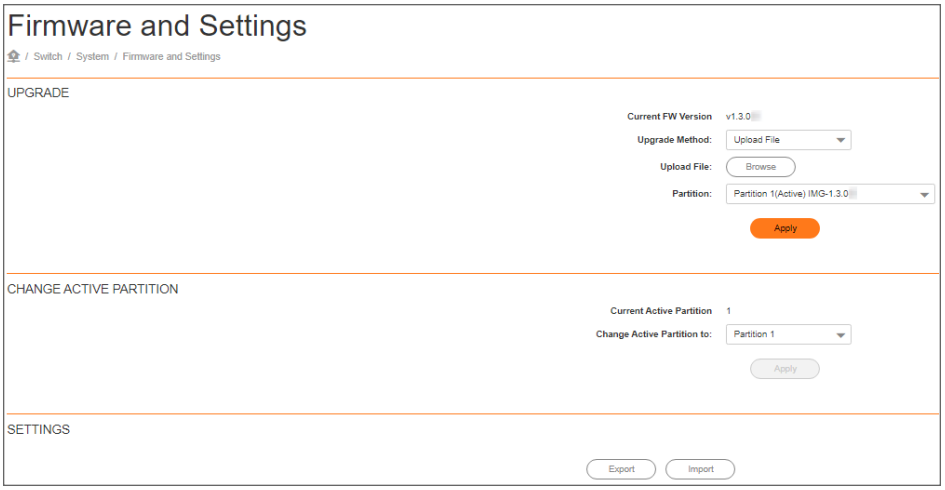
Follow this procedure to upgrade the Firmware using SonicWall Cloud Server method:

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 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.



Resetting

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

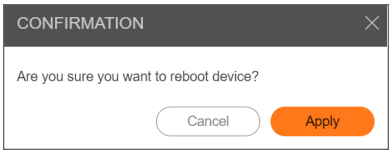
Follow this procedure to reset the Switch back to factory default settings:

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

Rebooting

Follow this procedure to reboot the Switch:

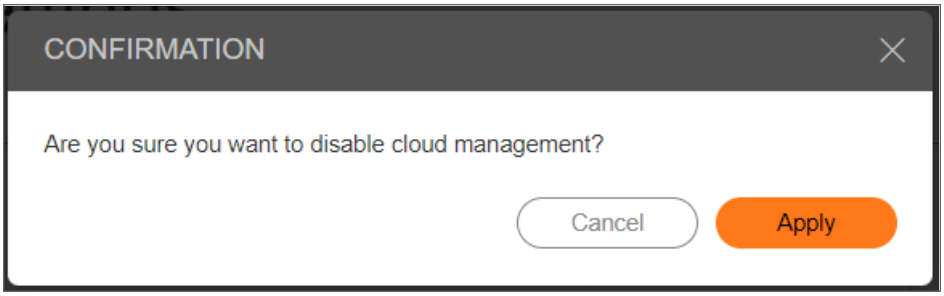
1. Click  to start the reboot process.
2. When a prompt displays, click **Apply** to confirm the reboot process or **Cancel** to quit the procedure.



Cloud Management

Follow this procedure to disable or enable cloud management:

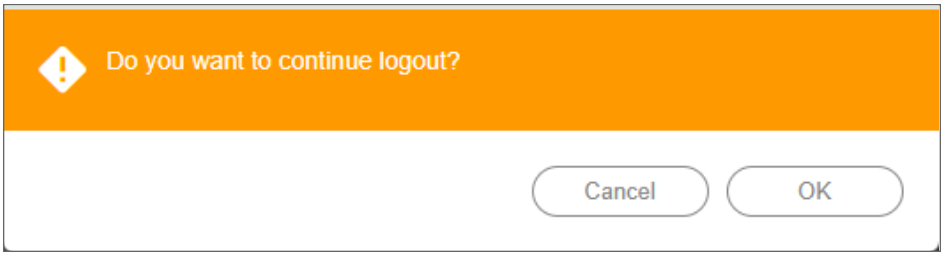
1. Click  icon in the Maintenance menu bar.
2. When a prompt displays, click **Apply** to disable cloud management.
   If cloud management has already been disabled, the prompt will ask to enable cloud management.



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.

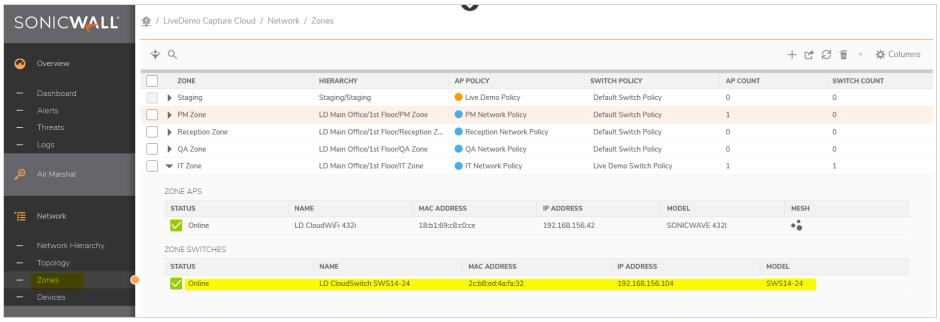


You are logged out from the Switch application.

Switch Troubleshooting

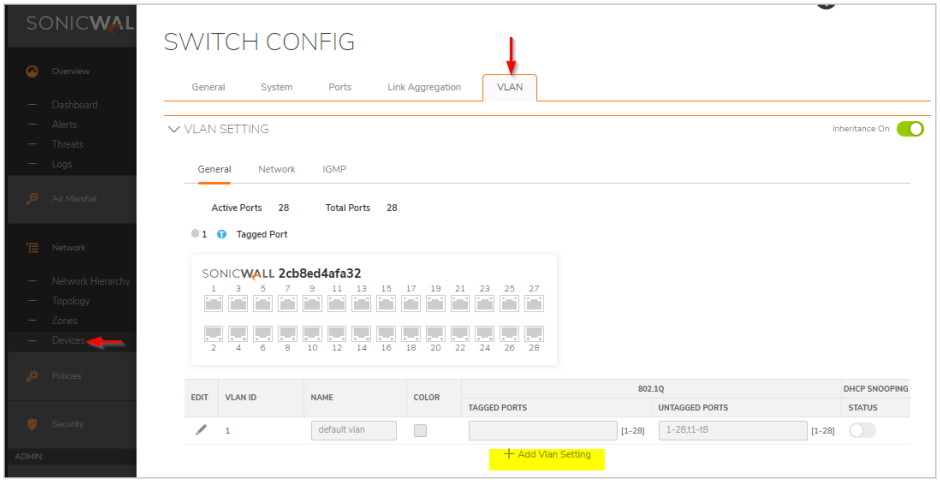
Steps to create VLAN from WNM on the switch

- 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.**

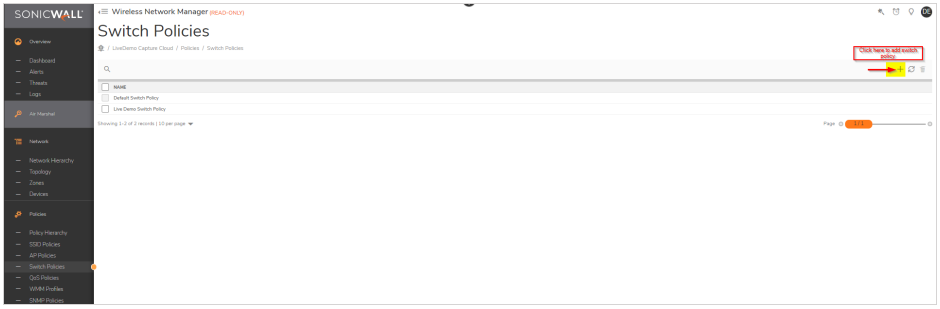


- Navigate to **Network > Devices > Switches > edit > VLAN**.

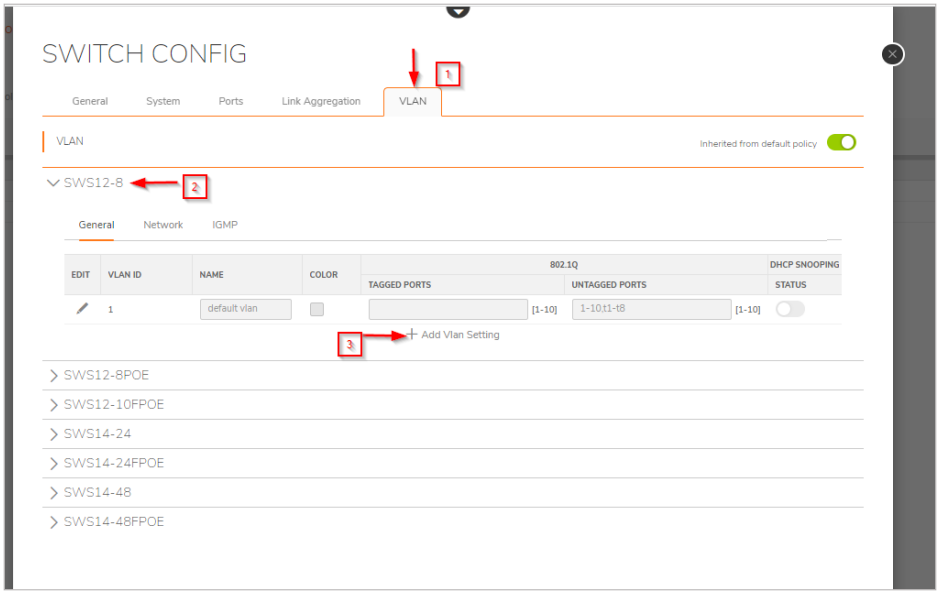
  ⓘ | **NOTE:** This only applies to a single switch or switches not using a Switch Policy.



- There is more than 1 Switch then make use of switch policies, for this Navigate to **Policies > Switch Policies**, Click on **Add**.



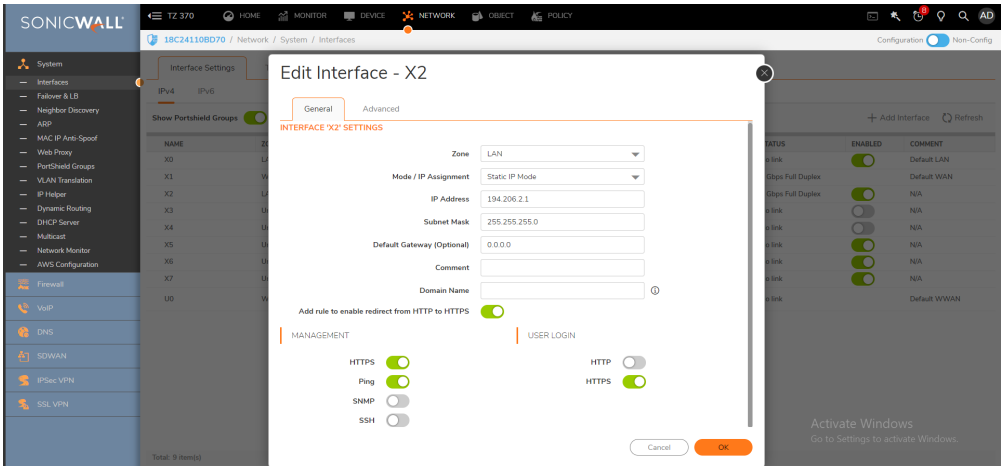
- Go to **VLAN**, select the switch model to add the VLAN, Click on **Add VLAN settings**.



Communication flow between Firewall and Switch before it gets authenticated

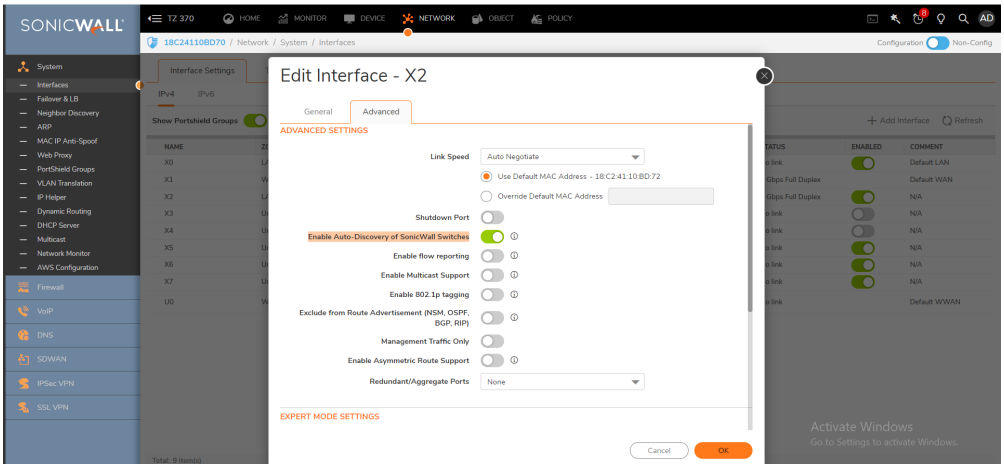
IMPORTANT: If switch **Auto-Discovery** is not working when a third party switch is in the middle between SW firewall and SW switch. where LLDP packets are not forwarded, the switch can be added manually.

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

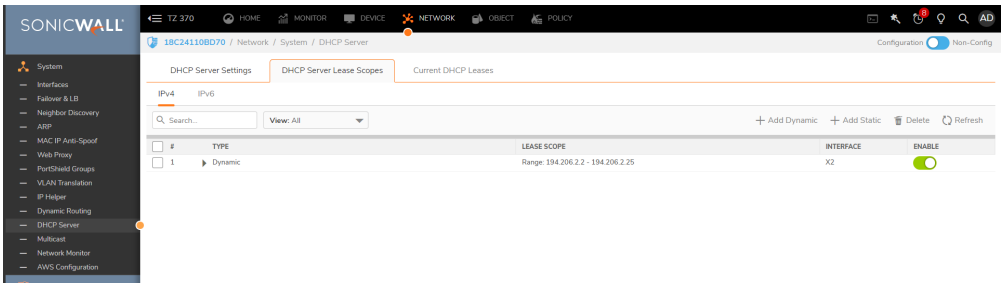


In the same interface edit and go to **Advanced** tab and enable the toggle button **Enable Auto-Discovery of SonicWall Switches**.

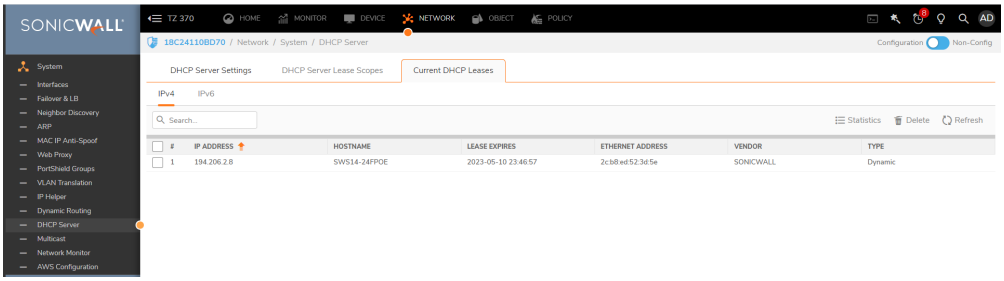
ⓘ | **NOTE:** Max of eight switches can be added to the firewall.



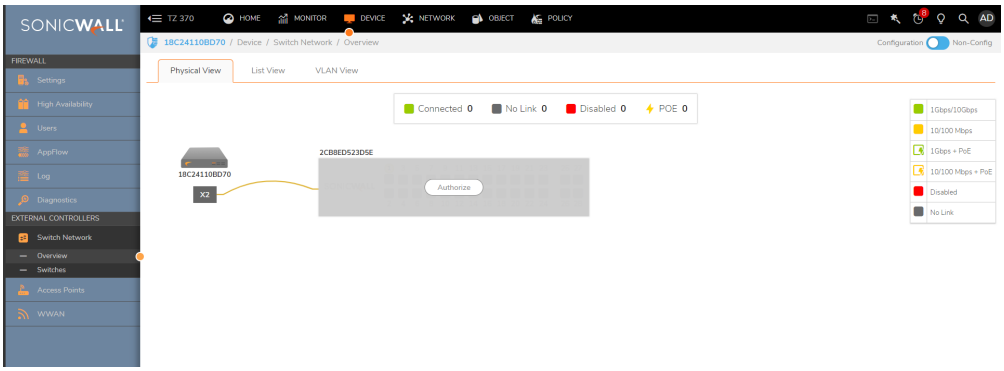
Now, check and confirm if the **DHCP Server lease scopes** setting is enabled for that interface.



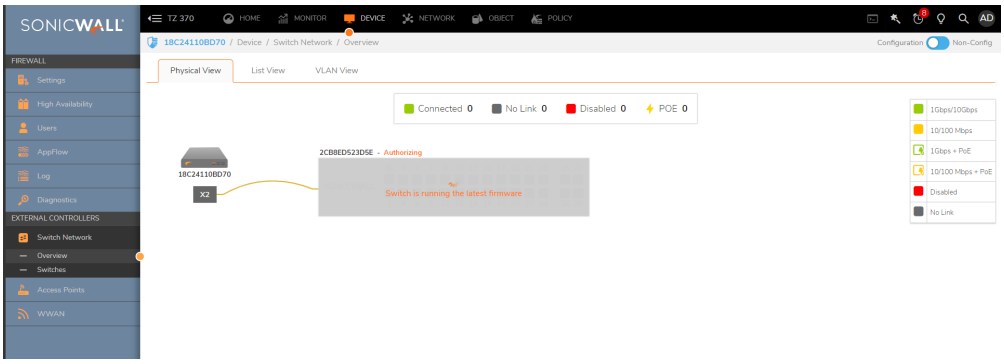
Once the switch gets an IP from the interface (X2) check and confirm from the **Current DHCP Leases** tab.



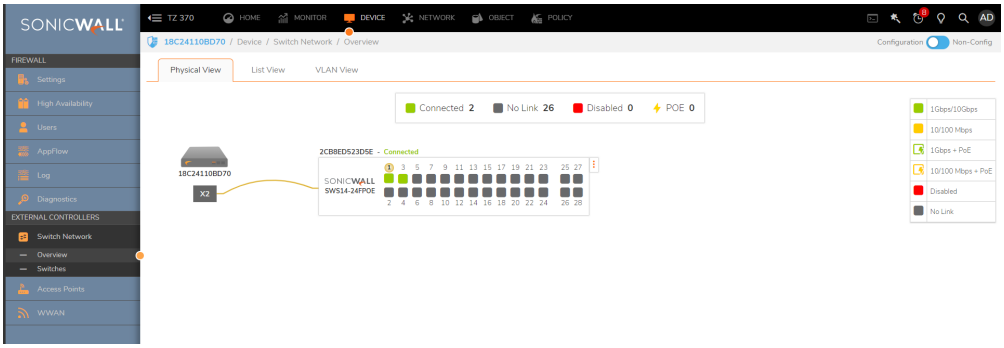
Navigate to **External Controllers> Overview>Physical View** and check for switch getting authorized.



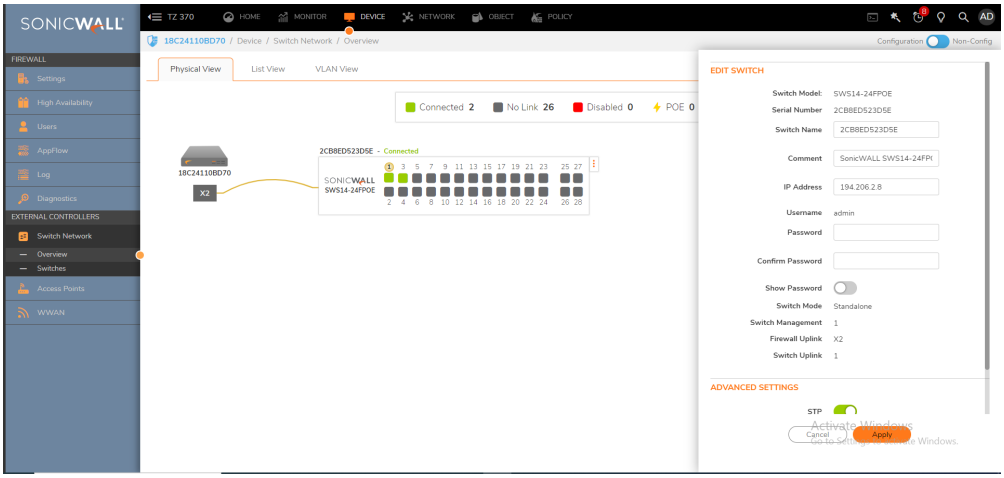
Click on **authorize** button



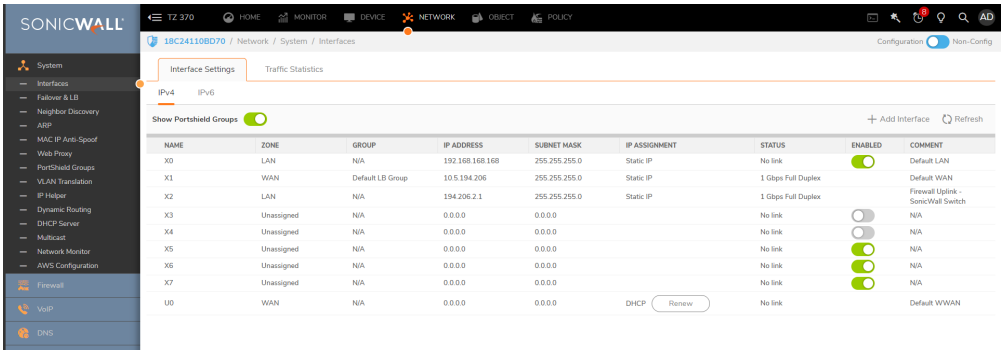
After completing authorization the switch gets added successfully.



Now, you can edit the Switch configuration.



you can view the X2 interface comment section.



View the Switch CLI information

```
SWS14-24# show system information
Firmware Version                    : 1.3.0-2
Switch Name                         : SWS14-24
System Contact                      : Default Contact
System Location                     : Default Location
Logging Option                      : Console Logging
Login Authentication Mode           : Local
Config Save Status                  : Not Initiated
Remote Save Status                  : Not Initiated
Config Restore Status               : Successful
Traffic Separation Control          : none
Serial Number                       : 2CB8ED516F4F
Loader Version                      : 03.01.05
Protocol Version                    : 3.01.468
MAC Address                         : 2c:b8:ed:51:6f:4f
System Uptime                       : 5 days, 10 hours, 23 mins

SWS14-24#
```

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 after factory resetting the switch.
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

5

SonicWall Support

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

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

The Support Portal enables you to:

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

About This Document

Switch Administration Guide
Updated - September 2024
232-005592-00 Rev H

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