SonicWall® Switch

Getting Started Guide

SONICWALL®

Contents

1

Registering Your Switch

SonicWall Switches should be registered on MySonicWall prior to using them. Select the support license for either 1 year or 3 year support, including firmware updates.

To register your Switch on MySonicWall:

1. Find the product label on the bottom surface of your Switch enclosure and make a note of the serial number and authentication code.
2. Log into your MySonicWall account. If you do not have an account, create one at: https://www.mysonicwall.com
3. Navigate to **MyWorkspace > Register Products** and go through the steps.
4. When you add a Switch at the firewall, the License Manager checks the serial number and other product information.
   For details on adding a Switch refer to Before Adding a Switch on page 23, and then either Adding a Switch to a Firewall with Zero-Touch on page 24 or Adding a Switch to a Firewall Manually on page 27.
5. To move your Switch to another firewall, simply delete it in the **Switch Controller > Overview** display and repeat the Add a Switch process on another firewall.

2

Overview

Introduction

The SonicWall Switches are designed to connect SonicWall firewalls with Access Points and IP Surveillance cameras, VoIP phones, and other PoE-Capable devices as well as other Ethernet-based networking equipment or computers. The Switch provides simple, yet powerful PoE manageability with features such as: IEEE 802.3af or IEEE 802.3at/af ports, PoE port management, voice VLAN, QoS, static routing, 802.1x authentication, and access point management.

The main applications envisioned for SonicWall Switches is in branch office scenarios where they are managed by firewalls. Application scenarios where the Switches are managed directly through their local UI are seen as less prevalent.

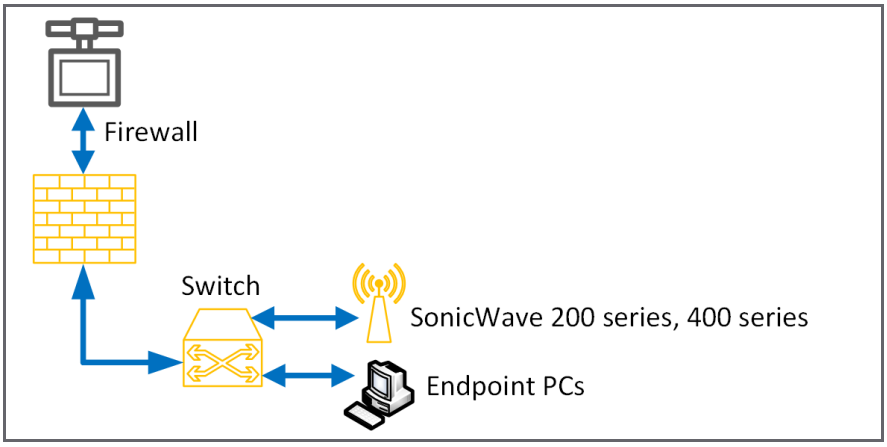
The SonicWall switches can be managed by all SonicWall firewalls running SonicOS 6.5.4.6 or higher, except NSA 2600.

NOTE: When managed through TZ model firewalls, Switches will not support Jumbo Frames.

Branch Office

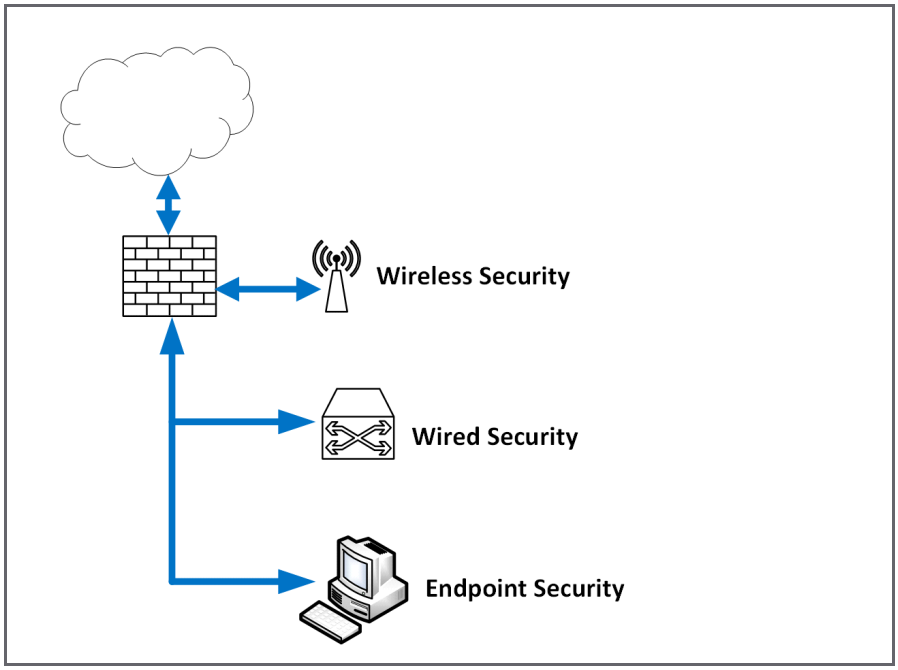
The firewall manages the Switch and wireless access points. Capture Client is installed on endpoint PCs. Typical Firewalls will be the SOHOs and TZs.

GMS or CSC-MA can manage the solution, via managing the firewall. No separate tile appears in the Capture Security Center.



The Switch segments branch offices into security domains:

- The Switch provides the **Wired Security** and also enhances port density. Use it to segment a network into different VLANs or zones.
- The Switch also supports access points, which provides **Wireless Security**. APs can connect to firewall or to the Switch.
- Capture Client provides **Endpoint Security**.



SD-WAN plays a major role in a branch solution by providing an essential software component.

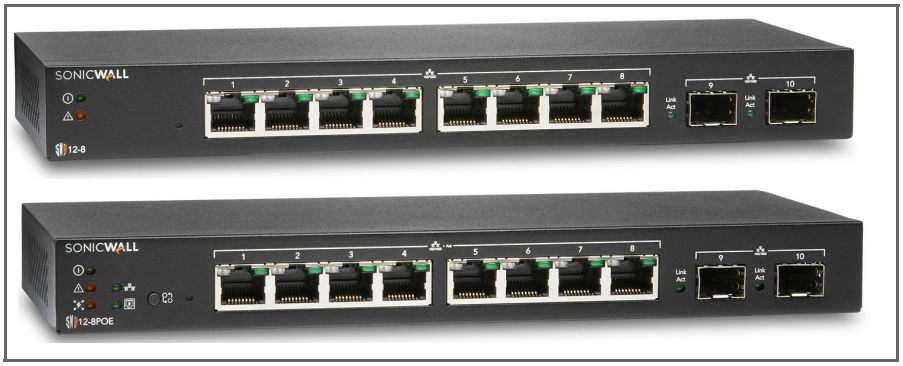
Daisy Chaining of Switches allows up to Four Switches to be concurrently managed by the firewall. Three can be daisy chained with one parent Switch, or two parent Switches sharing one child Switch.

Hardware Overview

SWS12-8 and 12-8PoE

These two Switches are distinguished by eight 1GB ports, two SFP sockets, and the use of external power supplies. The SWS12-8POE supports Power Over Ethernet (PoE) conforming to 802.3a/f as Power Sourcing Equipment (PSE). These Switches can be managed from a SonicWall firewall, WiFi Cloud Manager, or directly from on-premises or cloud based systems. From top to bottom, the models are:

- SWS12-8
- SWS12-8PoE



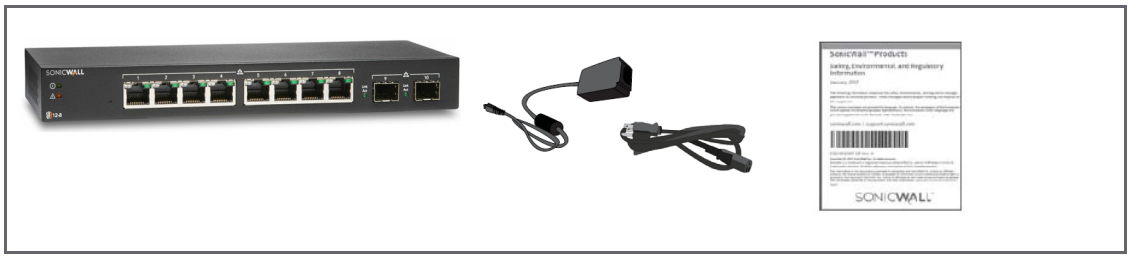
Check Package Contents

Check that your package includes:

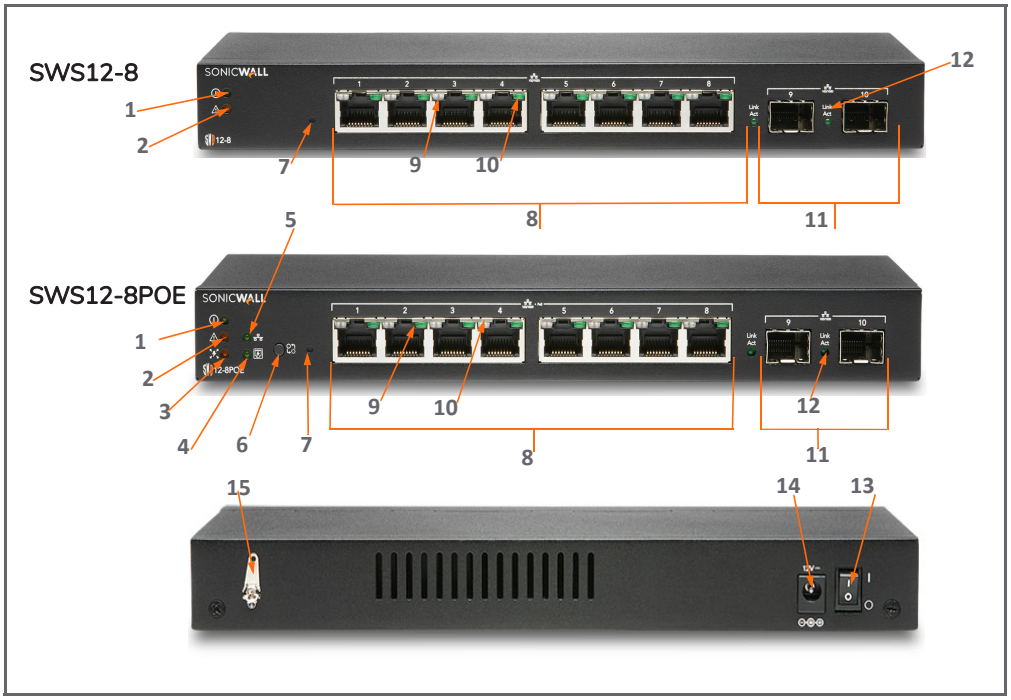
- SonicWall Switch
- 4 rubber feet
- Safety, Environmental, and Regulatory Information booklet
- Power cable and external power supply

NOTE: The included power cord is approved for use only in specific countries or regions. Before using a power cord, ensure that it is approved for use in your location.

添付の電源コードに関して：電気安全を確保するために、弊社製品にご使用いただく電源コードは必ず製品同梱の電源コードをご使用ください。この電源コードは他の製品では使用できません。



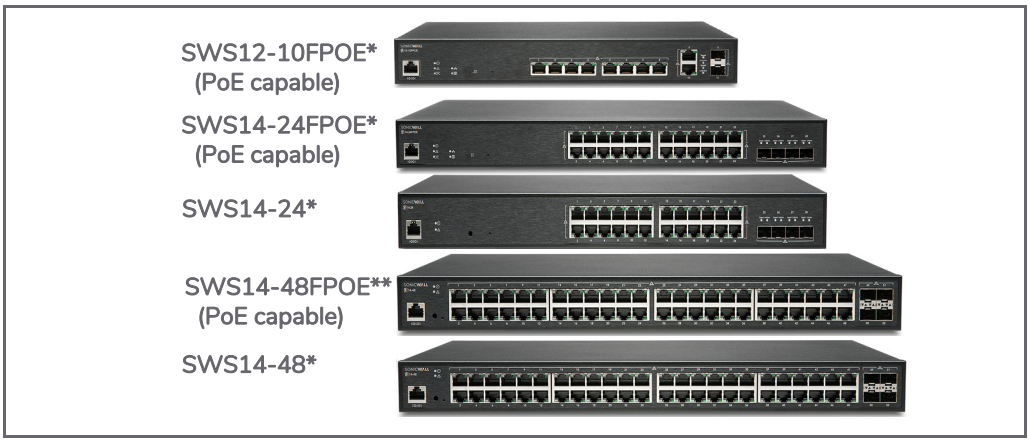
The following figure shows front and rear SWS12-8 and SWS12-8POE interface features.



1	**Power On LED**	9	**LAN Mode** (per copper port): *Off* = No link; *Amber* = active100 Mbps link; *Green* = active1 Gbps link; **PoE Mode:** *Green* = PoE OK; *Off* = no PoE current; *Amber* = PoE error
2	**Fault LED:** *Off* = normal; *Lit* = Fault	10	**Link/Act LED** (per copper port): *Off* = No link; *Lit* = link on, *Blinking Light* = packet transfer in process
3	**PoE Max LED:** *Off* = Additional PoE device may be added; *Lit* = PoE power limit exceeded	11	**SFP Ports:** Small Form Pluggable ports: 1 Gbps
4	**PoE Mode LED:** *Off* = PoE mode off; *Lit* = PoE mode on	12	**SFP Link/Act LED:** (per SFP port) *Off* = No link; *Solid Green* = active1 Gbps link; *Blinking* = packet transfer in process
5	**LAN Mode LED:** *Off* = LAN mode off; *Lit* = LAN mode on	13	On/off button
6	**LAN/PoE Mode Selector button:** Press to change between LAN and PoE LED display modes. Refer to feature 9.	14	Power input
7	**Reset button**: Press to reset the Switch to current settings. Press for 10 seconds to enter Recovery Mode. **Note:** Returns Switch to default configuration.	15	Optional connector allows connection to ground
8	**RJ45 LAN Ports:** 10/100/1000 Mbps RJ45 LAN ports		

SWS12-10FPOE, 14-24FPOE, 14-24, 14-48FPOE, 14-48

The Switch product family includes five 10, 24, and 48 port Switches with internal power supplies. Switches support Power Over Ethernet (PoE) as Powered Sourcing Equipment (PSE).



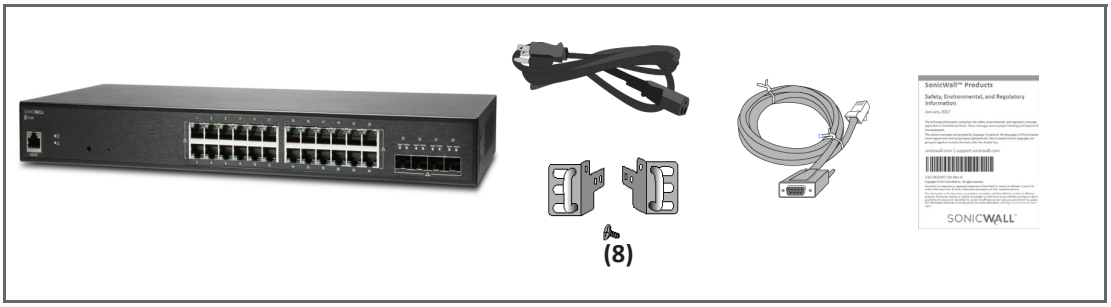
Check the Package Contents

Aside from this booklet your package includes:

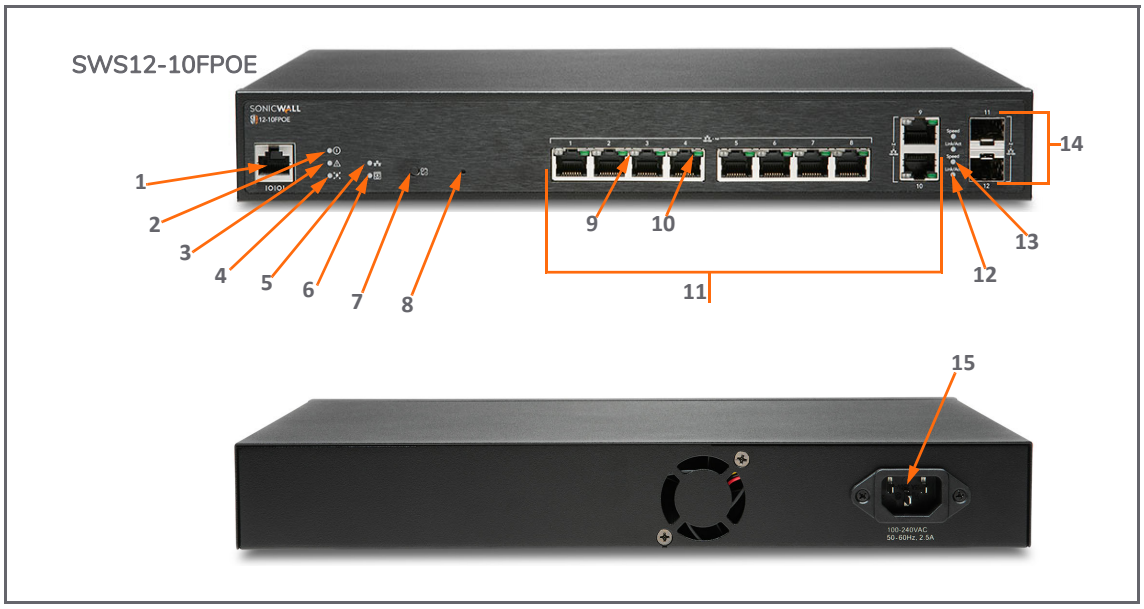
- SonicWall Switch
- 2 rack-mounting brackets with 8 screws
- Serial cable
- Safety, Environmental, and Regulatory Information booklet
- Power cable, (*in figure above) 10 A minimum provided; (**in figure above) 12 A minimum provided)

NOTE: The included power cord is approved for use only in specific countries or regions. Before using a power cord, ensure it is approved for use in your location.

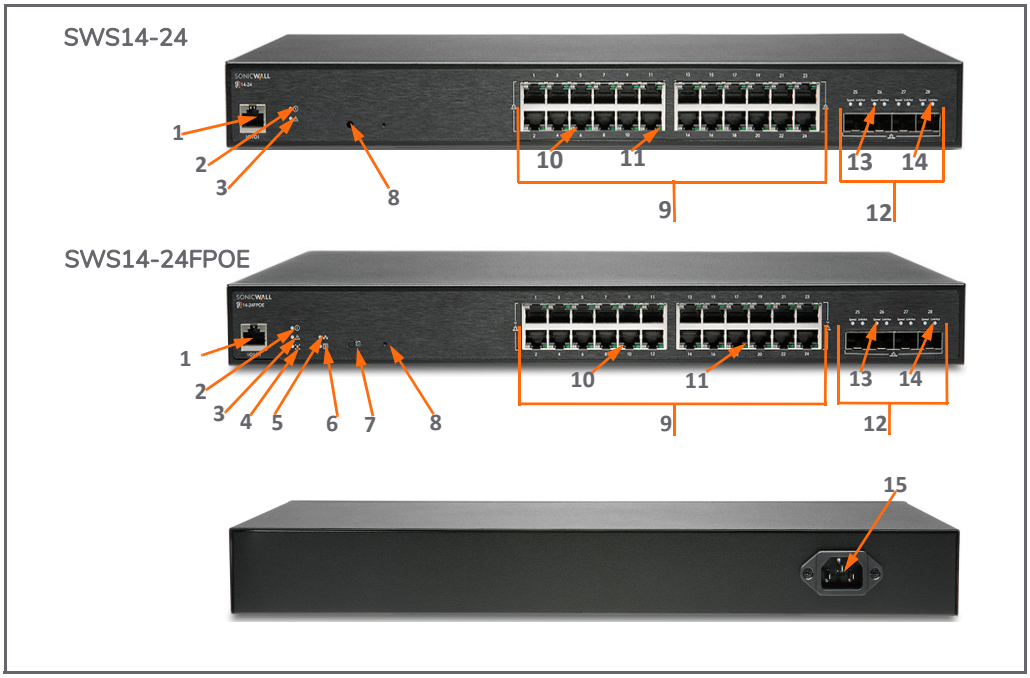
添付の電源コードに関して：電気安全を確保するために、弊社製品にご使用いただく電源コードは必ず製品同梱の電源コードをご使用ください。この電源コードは他の製品では使用できません。



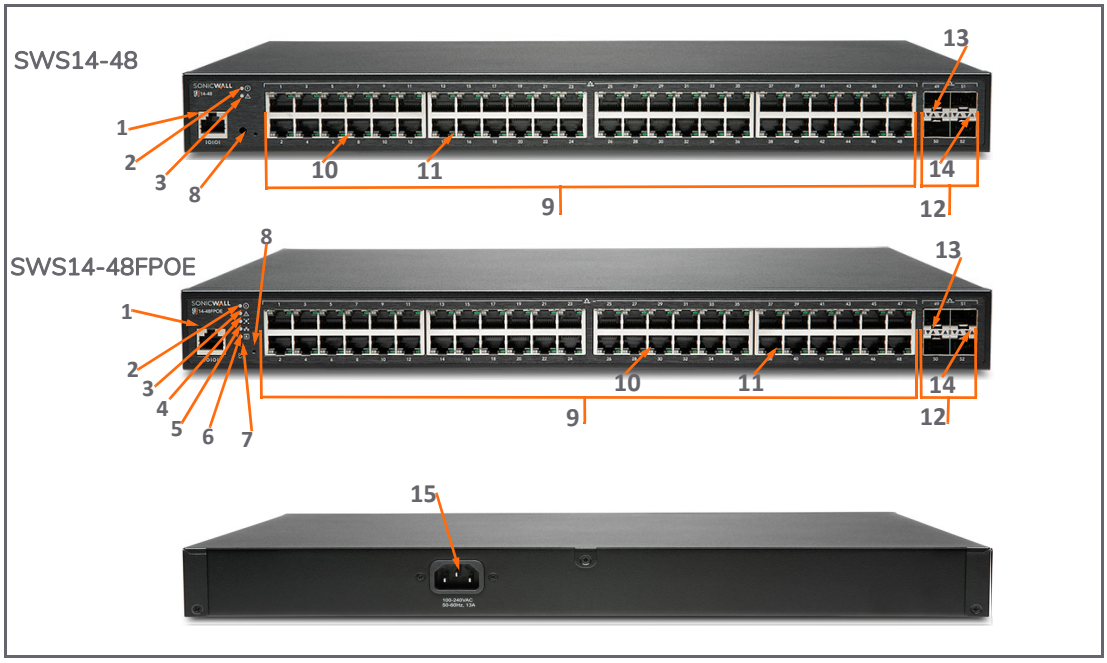
The following figures detail the front and rear panels of the SWS12-10FPOE and SWS14 Series Switches..



1	**Serial Console Port (RJ45)**	8	**Reset button:** Press to reset the Switch to current settings. Press for 10 seconds to enter Recovery mode. **Note:** Returns Switch to default configuration.
2	**Power On LED**	9	**LAN Mode** (per copper port)**:** *Off* = No link; *Amber* = active100 Mbps link; *Green* = active 1 Gbps link; **PoE Mode:** *Off* = No PoE activity; *Green* = active PoE current; *Amber* = PoE fault or overcurrent
3	**Fault LED:** *Off* = normal; *Lit* = Fault	10	**Link/Activity LED** (per copper port)**:** *Off* = No link; *Solid Light* = link on; *Blinking* = packet transfer in process
4	**PoE Max LED:** *Off* = Additional PoE device may be added; *Lit* = PoE power limit exceeded	11	**RJ45 LAN Ports:** 10/100/1000 Mbps RJ45 LAN ports
5	**LAN Mode LED:** *Off* = LAN mode off; *Lit* = LAN mode on	12	**SFP Link/Act** (per SFP port)**:** *Off* = No link; *Green* = active link; *Blinking* = packet transfer in process
6	**PoE Mode LED:** *Off* = PoE mode off; *Lit* = PoE mode on	13	**SFP Speed** (per SFP port)**:** *Off* = No traffic; *Green* = 1 Gbps
7	**LAN/PoE Mode Selector:** Press to change between LAN and PoE LED display modes. Refer to feature 9.	14	**SFP Ports:** 1 Gbps ports
		15	**AC Power Port**



1	**Serial Console Port (RJ45)**	8	**Reset button**: Press to reset the Switch to current settings. Press for 10 seconds to go to Recovery Mode. **Note:** Returns Switch to default configuration.
2	**Power On LED**	9	**RJ45 LAN Ports:** 10/100/1000 Mbps RJ45 LAN ports
3	**Fault LED:** *Off*= normal; *Lit* = Fault	10	**LAN Mode** (per copper port): *Off* = No link; *Amber* = active 100 Mbps link; *Green* = active1 Gbps link. **PoE Mode**: *Off* = No PoE; *Amber* = excess PoE current; *Green* = active PoE current
4	**PoE Max LED:** *Off* = Additional PoE device may be added; *Lit* = PoE power limit exceeded	11	**Link/Act LED** (per copper port): *Off:* No link; *Lit* = link on; *Blinking*= packet transfer in process
5	**LAN Mode LED:** *Off* = LAN mode off; *Lit* = LAN mode on	12	**SFP+ Ports** (per SFP port}: Small Form Pluggable ports: 1 or 10 Gbps ports
6	**PoE Mode LED:** *Off* = PoE mode off; *Lit* = PoE mode on	13	**SFP+ Speed LED** (per SFP+ port)**:** *Off* = no packet transfer; *Green* = 1 or 10 Gbps
7	**LAN/PoE Mode Selector:** Press to change between LAN and PoE LED display modes. Refer to feature 10.	14	**SFP+ Link/Act LED** (per SFP+ port)**:** *Off* = No link; *Green* = active link; *Blinking* = packet transfer in process
		15	**AC Power Port**



1	**Serial Console Port (RJ45)**	8	**Reset button**: Press to reset the Switch to current settings. Press for 10 seconds to go to Recovery Mode. **Note:** Returns Switch to default configuration.
2	**Power On LED**	9	**RJ45 LAN Ports:** 10/100/1000 Mbps RJ45 LAN ports
3	**Fault LED:** *Off*= normal; *Lit* = Fault	10	**LAN Mode**: (per copper port) *Off* = No link; *Amber* = active100 Mbps link; *Green* = active 1 Gbps link; **PoE Mode**: *Off* = No PoE; *Amber* = excess PoE current; *Green* = active PoE current
4	**PoE Max LED:** *Off* = Additional PoE device may be added; *Lit* = PoE power limit exceeded	11	**Link/Act LED** (per copper port): *Off* = No link; *Lit* = link on; *Blinking Light* = packet transfer in process
5	**LAN Mode LED:** *Off* = LAN mode off; *Lit* = LAN mode on	12	**SFP+ Ports:** Small Form Pluggable ports. 1 or 10 Gbps ports
6	**PoE Mode LED:** *Off* = PoE mode off; *Lit* = PoE mode on	13	**SFP+ Speed LED** (per SFP+ port)**:** *Off* = no packet transfer; *Green* = 1 or 10 Gbps
7	**LAN/PoE Mode Selector:** Press to change between LAN and PoE LED display modes. See feature 10.	14	**SFP+ Link/Act LED** (per SFP+ port)**:** *Off* = No link; *Green* = active link; *Blinking* = packet transfer in process
		15	**AC Power Port**

About PoE

The SWS12-8POE Switch complies with 802.3af power standards, while the other PoE-capable Switches support 802.at power standards. Power limitations are presented in the following specifications tables. As indicated in the table, the maximum per port power output is 15.4 Watts for the SWS12-8POE, and 30 Watts for the FPOE Switches.

All of the PoE-capable Switches (that is, those with POE of FPOE in the model designation) function as Power Sourcing Equipment (PSE), but not as Powered Devices.

For details on PoE management, see Setting Up PoE on page 40.

About SFP/SFP+

Overview

The SFP interfaces on SWS12 series Switches support only 1 Giga-bit per second (Gb/s).

The SFP+ interfaces on SWS14 series Switches support only 10 and 1 Gb/s.

NOTE: Auto-Negotiation for SFP/SFP+ ports is not currently supported. On the SWS14 Series, SFP+ ports can be manually set to 1 and 10 Gbps.

For an overview on using SFP/SFP+, refer to SonicWall 10 Gigabit Ethernet SFP+ Ports and 1 Gigabit Ethernet Ports.

For a list of third-party SFP/SFP+ modules, refer to Supported SFP and SFP+ Modules.

For a current list of SFP/SFP+ modules from SonicWall, see SonicWall SFP/SFP+ Transceiver Modules Reference Guide.

Specifications

SWS12-8 and SWS12-8POE

Specification	SWS12-8	SWS12-8POE
Regulatory Model	APL51-0E1	APL52-0E2
1 Gb RJ45	8	8
1 Gb SFP[1]	2	2
Power Supply	24W external adapter	65W external adapter
Power Input	12 VDC, 2 A	54 VDC, 1.2 A
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%

1 Contact your SonicWall sales representative for information on available SonicWall SFP/SFP+ modules and cables: https://www.sonicwall.com/customers/contact-sales/

SWS12-10 and SWS-14 Series

Specification	SWS12-10FPOE	SWS14-24	SWS14-24FPOE	SWS14-48	SWS14-48FPOE
Regulatory Models	1RK43-0E3	1RK44-0E4	1RK45-0E5	1RK46-0E6	1RK47-0E7
1 Gb RJ45	10	24	24	48	48
1 Gb SFP	2				
1 / 10 Gb SFP+[1]		4	4	4	4
Fans	1	—	2	1	3
Power Supply	180 W	25 W	480 W	60 W	900 W
Power Input	100-240 VAC; 2.5 A 50-60 Hz	100-240 VAC; 0.7 A 50-60 Hz	100-240 VAC; 7.0 A 50-60 Hz	100-240 VAC 1.5 A 50-60 Hz	100-240 VAC1 2 A 50-60 Hz
PoE Ports	10	—	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%

1.Contact your SonicWall sales representative for information on available SonicWall SFP/SFP+ modules and cables: https://www.sonicwall.com/customers/contact-sales/

3

Connecting to the Switch

This chapter details steps to connecting with the Switch Local Interface over Ethernet, or with the Switch Command Line Interface (CLI) through a serial connection to the Console Port.

Connecting over Ethernet

Follow the steps in this section to connect to the Switch Local User Interface.

1 Configure an IP address in the 192.168.168.0/24 subnet to access the Switch Local .UI

2 Now, power up the Switch and wait for it to fully boot. Connect an Ethernet cable from your system to one of the copper (RJ45) Ethernet ports on the Switch.

3 Bring up a browser and address the Switch management console: **https://192.168.168.169**

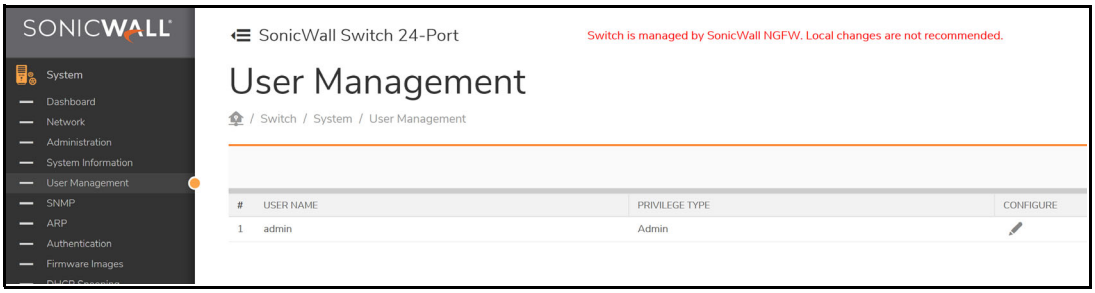
NOTE: Any browser other than Microsoft IE is recommended.

4 The Switch management console login screen now appears.

To login to the management console:

1 Enter username as admin and password as password to start a management console session for the first time.

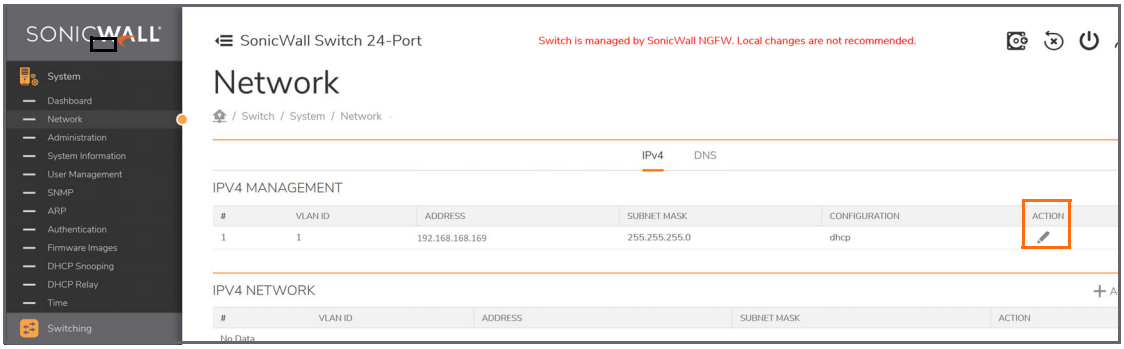
2 After logging in for the first time, go to **System>User** and click on **Configure** to change the password.



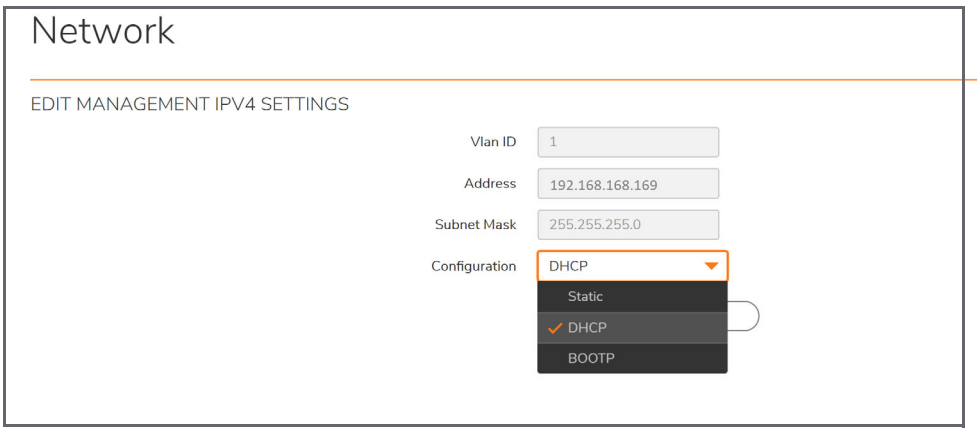
To change the password, click on the edit icon.

To add Switch to a network <u>with</u> a DHCP server:

1 Go to **System>Network** and click on **Action**.



2 In **IPV4 SETTINGS**, select **DHCP**.



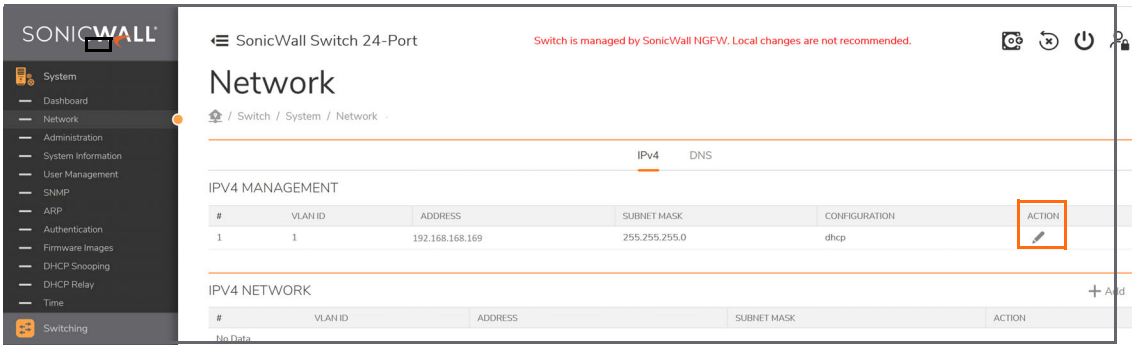
3 Click OK and then connect the Switch to your DHCP-enabled network.

4 On the DHCP server, find and write down the IP address allocated to the device. Use this IP address to access the management interface.

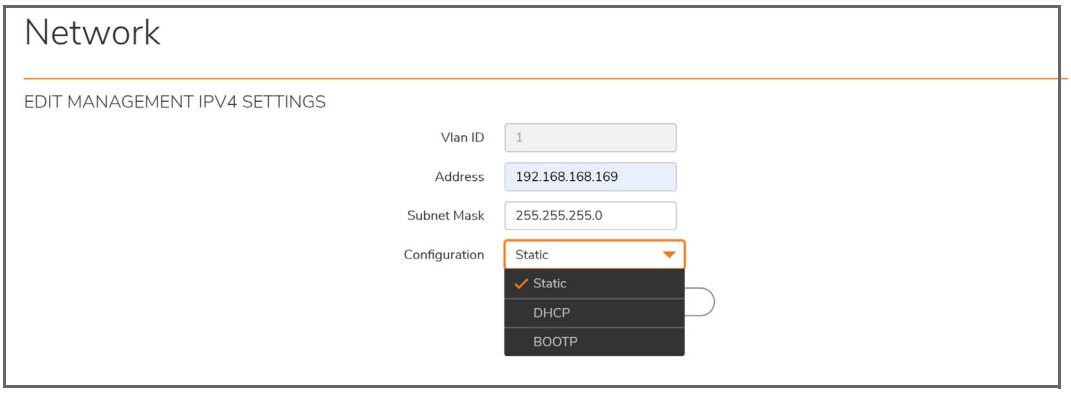
To add Switch to a network <u>without</u> a DHCP server:

1 Make sure you have set a Static IP Address on your system's Ethernet adapter. See Step 1 above.

2 After logging in, to **System>Network** and click on **Action**.



3 In **IPV4 SETTINGS**, select **Static.** Check that Address and Subnet Mask are correct.



4 Click **OK** to update the system.

When the IP is set to static, add a default route manually to access the switch from external network. Navigate to **Network > Routing** to establish a static route.

Connecting via the Console Port

Follow these steps to connect with the Command Line Interface for the switch.

NOTE: This applies only to Switches: SWS12-10FPOE, SWS14-24, SWS14-24FPOE, SWS14-48, SWS14-48FPOE.

Refer to Hardware Overview on page 7 locate the console port.

To Connect to the Console Port:

1 Locate the DB-9 to RJ45, serial cable that was shipped with the Switch and connect it from a PC to the leftmost port labeled console on the Switch.

2 For instructions on connection through the console port see:

- https://www.sonicwall.com/support/knowledge-base/how-can-i-login-to-the-appliance-using-the-command-line-interface-cli/170505641032025/

4

Upgrading the Firmware

To upgrade Switch firmware after the Switch has been integrated with firewall, the most direct approach is Via the Firewall Interface.

NOTE: On MySonicWall, firmware is available under Free Downloads for Switch firmware and under My Downloads for firewall 6.5.4.6 firmware.

For switches not managed from a firewall, two alternative approaches to upgrading firmware are:

- Via the Local UI on page 18
- .Via TFTP on page 20

Via the Firewall Interface

Within the SonicOS 6.5 GUI, navigate to **MANAGE | Switch Controller > Switches > Firmware**.

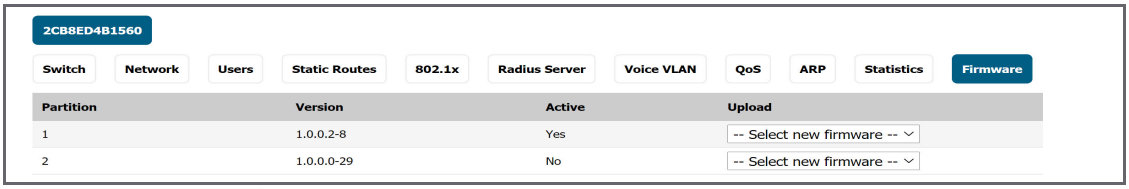
To Upgrade Switch Firmware:

NOTE: To perform this upgrade method, the Switch must connect to the internet.

1 Locate firmware upgrade options as shown below.

This feature will allow changing the active firmware image after selection here and re-booting.

New firmware can be loaded into the active or inactive partition.

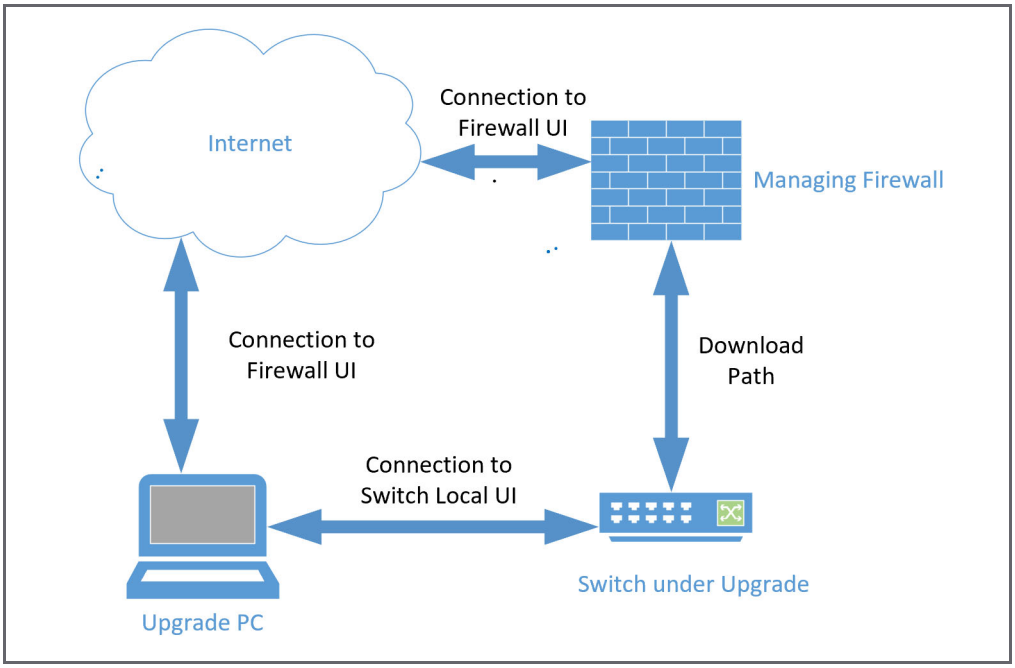


2 Click to select the most recent available firmware.

NOTE: Downloading and re-booting of the Switch may take over ten minutes. Wait for the front panel LEDs to flash, indicating the Switch has rebooted.

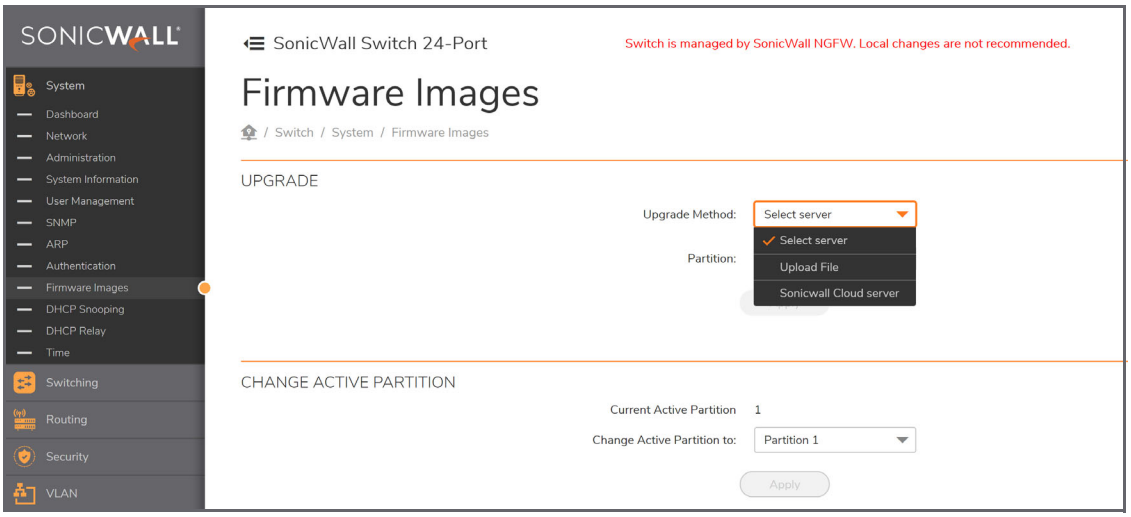
Via the Local UI

This procedure supports all SonicWall Switch models. The network setup for the upgrade is summarized in the following diagram.



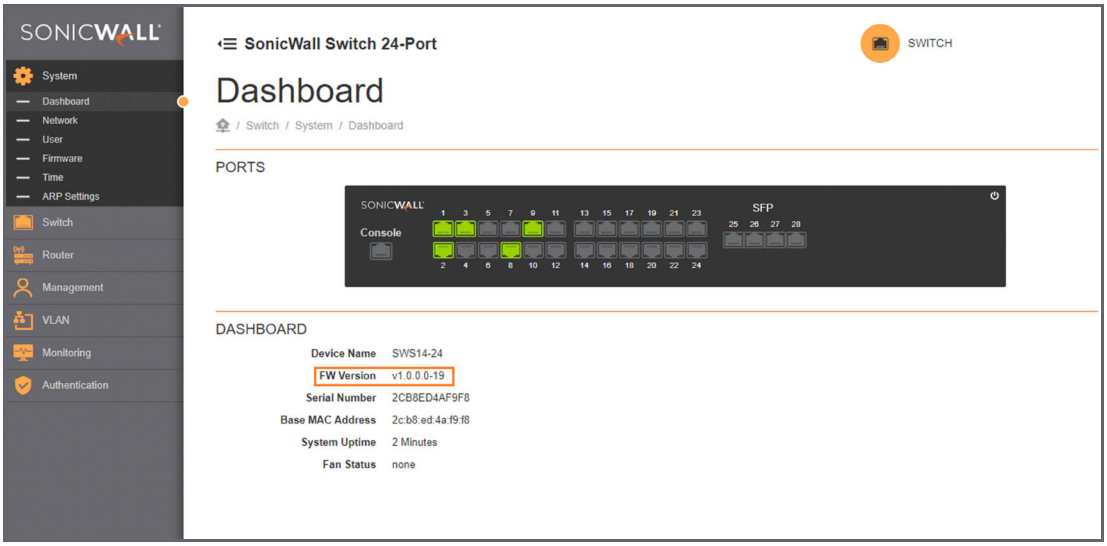
1 To connect to the Switch Local UI, refer to Connecting over Ethernet on page 15.

2 Navigate to **System > Firmware** and select upgrade details as below and click on apply.



IMPORTANT: Once the firmware upgrade begins, contact with the Switch will be lost. The upgrade process may take 5 to 10 minutes. At completion, the Switch LEDs will flash indicating a reboot.

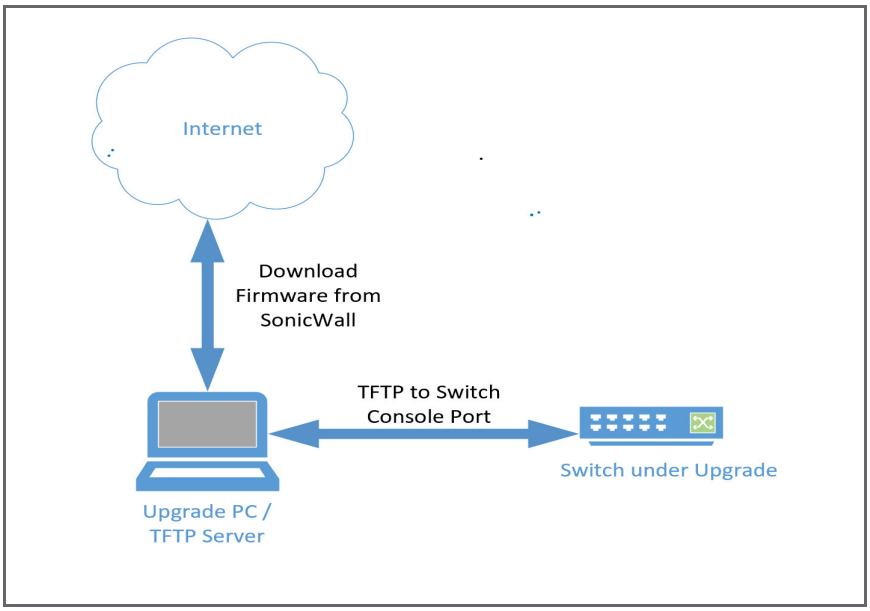
3 Once the Switch has rebooted, log back into the Switch and verify the firmware version is properly updated.



Via TFTP

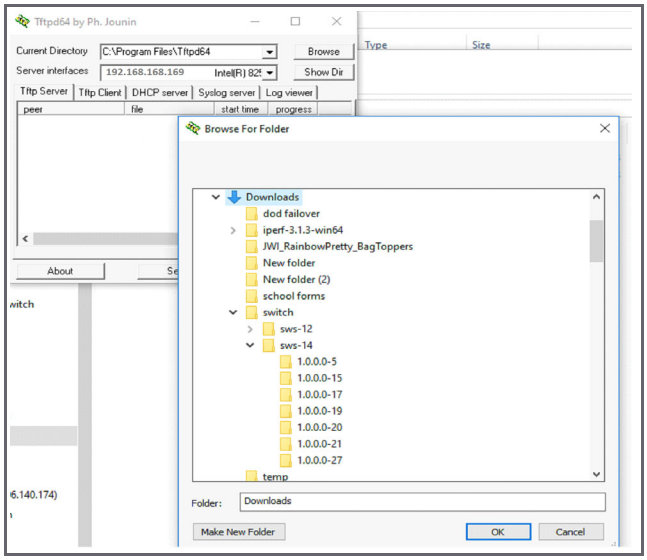
NOTE: This procedure works only with the SWS12-10FPOE and the SWS14 series Switches which include a console port.

The following diagram summarizes the network configuration.



To prepare a PC for the upgrade

1. If you do not have a TFTP server on your PC, download one. Below, we show one from: https://tftpd32.jounin.net/
2. Download the new firmware from **software.sonicwall.com**.
3. Bring up the TFTP server, note IP address and browse to the downloaded firmware.



To connect to the Switch

1 Locate the DB-9 to RJ45, serial cable that was shipped with the Switch and connect it from a PC to the leftmost port labeled console on the Switch.

2 For instructions on connection through the console port see:

- https://www.sonicwall.com/support/knowledge-base/how-can-i-login-to-the-appliance-using-the-command-line-interface-cli/170505641032025/

3 Once connected to the Command Line Interface, log in. Defaults are admin and password.

To execute the upgrade

1 At the command prompt use the IP address from TFTP server.
`firmware upgrade` ...[TFTP sever addrese/file name]...`flash:normal image` [1 or 2]

```
SWS14-24FPOE#
SWS14-24FPOE#
SWS14-24FPOE#
SWS14-24FPOE#
SWS14-24FPOE#
SWS14-24FPOE#
SWS14-24FPOE# firmware upgrade tftp://192.168.0.240/sw_SWS-14_1.0.0.0-27.imag flash:normal image 1
```

2 The flash process may take over 5 minutes. Once it completes, enter `reboot` to reboot the Switch with the new firmware revision.

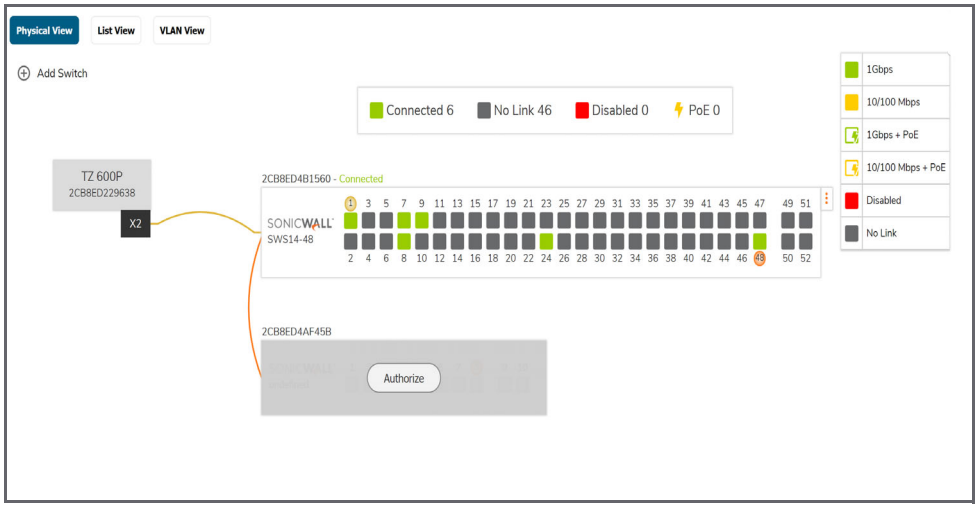
5

Configuring from the Firewall

Firewall Switch Controller UI

Starting with release 6.5.4.6, SonicOS supports firewall management of SonicWall Switches. The Switch Controller user interface consists of pages and sub-pages.

- Overview
  - Pre-Plan — Before Adding a Switch on page 23
  - Physical View — Before Adding a Switch on page 23
  - List View — Setting Up the Ports on page 37
  - VLAN View — Adding a VLAN on page 32
- Switches
  - Switch — Checking Switch Details on page 23
  - Networks — Adding a VLAN on page 32
  - Users —Setting Up Users on page 41
  - Static Routes —Adding Static Routes on page 35
  - 802.1x —Setting Up 802.1x Authentication on page 42
  - Radius Server —Setting Up 802.1x Authentication on page 42
  - Voice VLAN — Adding a VLAN on page 32
  - QoS — Setting Up QoS on page 38
  - ARP —Modifying the MAC Address Table on page 51
  - Statistics — Checking Port Statistics on page 52
  - Firmware — Changing Firmware on page 54

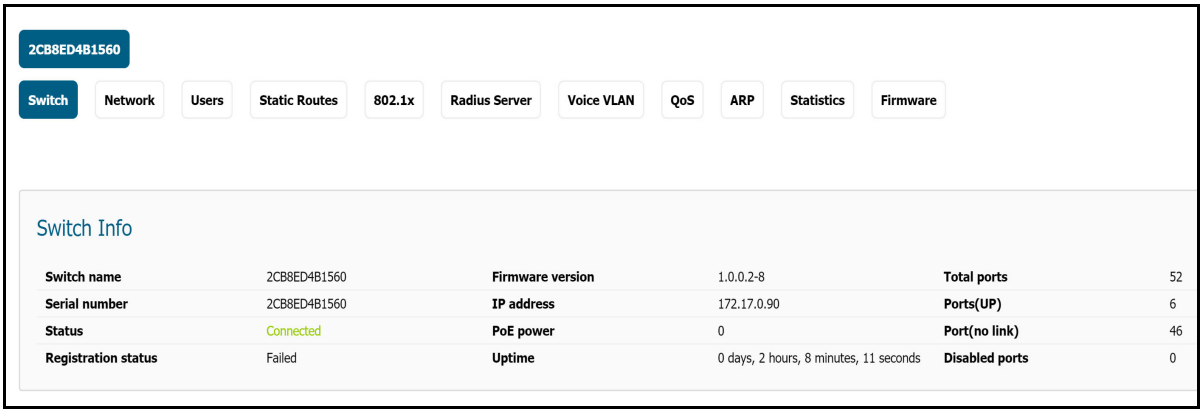


Before Adding a Switch

- Be sure to first register your Switch on MySonicWall. Refer to Registering Your Switch on page 4.
- Consider the firewall/Switch topology to be implemented. Refer to Configuring Basic Topologies on page 56.
- When adding a Switch manually, first check that it is configured to factory defaults. This can be ensured by depressing the reset Switch for 10 seconds or from the Switch Local UI, or the Command Line Interface.
- When adding a management link to a Switch manually, ensure that the DHCP lease range supports the default management IP address. Refer to Connecting the Switch Management Port to a Firewall on page 57.
- If the management link between the switch and firewall is isolated from data traffic, the switch must configured at a static IP address.
- The firewall interface linking to the Switch interface cannot be a PortShield host and no other firewall interface can be portshielded to it. The firewall interface linking to the Switch cannot be a PortShield group member, that is, it cannot be portshielded to another firewall interface.
- Switches may be added into daisy-chained configurations manually or by using Zero-Touch.
- For daisy chaining Switches, consider setting up a common link (management and data) with sufficient capacity and do not make further connections from firewall to parent switch without configuring them. Make any other connections from the firewall to the Switch when you add the Switch.
- Make any changes in the Reserved VLAN range for the firewall interface before adding the SonicWall Switch. If the Reserved VLAN range changes after connecting the Switch, then the Switch must be removed and re-added.
- Logging into switch with SSHv1 client is not supported.
- If adding Switches to a High Availability (HA) pair:
    - Switches cannot be added to HA pairs with Zero-Touch.
    - To use the Switch with HA, you must first create an HA pair, and then manually add the Switch.

Checking Switch Details

Navigate to **Switches > Switch** to get a summary on switches connected to the firewall.



Adding a Switch to a Firewall with Zero-Touch

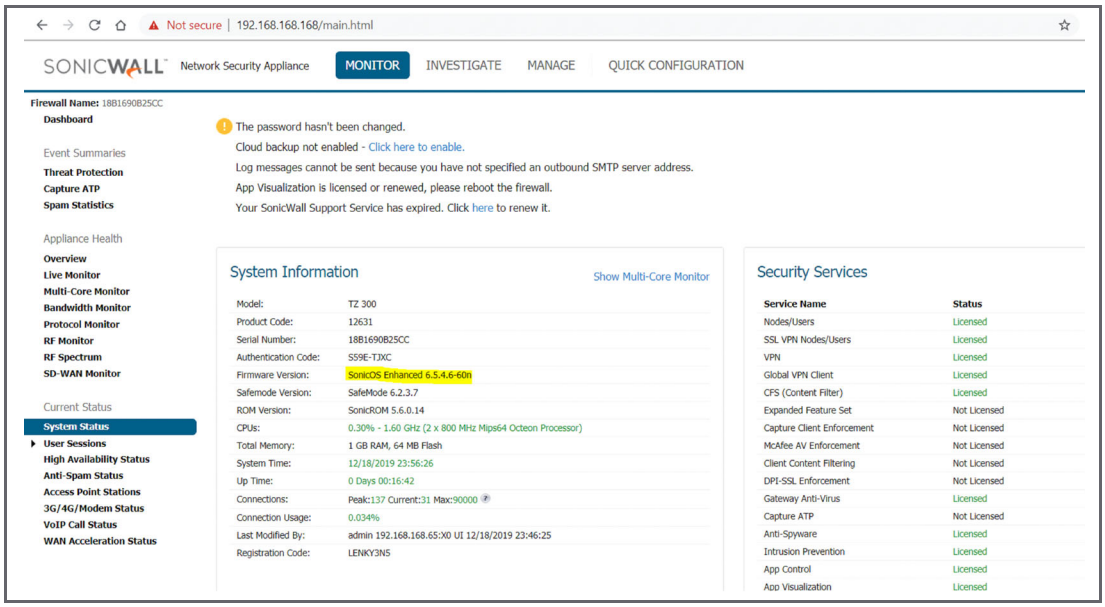
IMPORTANT: Please register your Switch before trying to add it to a firewall. See Registering Your Switch on page 4.

NOTE: In order for the firewall to sense the presence of the Switch, its firmware must be at SonicOS 6.5.4.6 or higher. The Switch should be at 1.0.0.0-19 or higher.

The firewall must be setup to add Switches with Zero Touch.

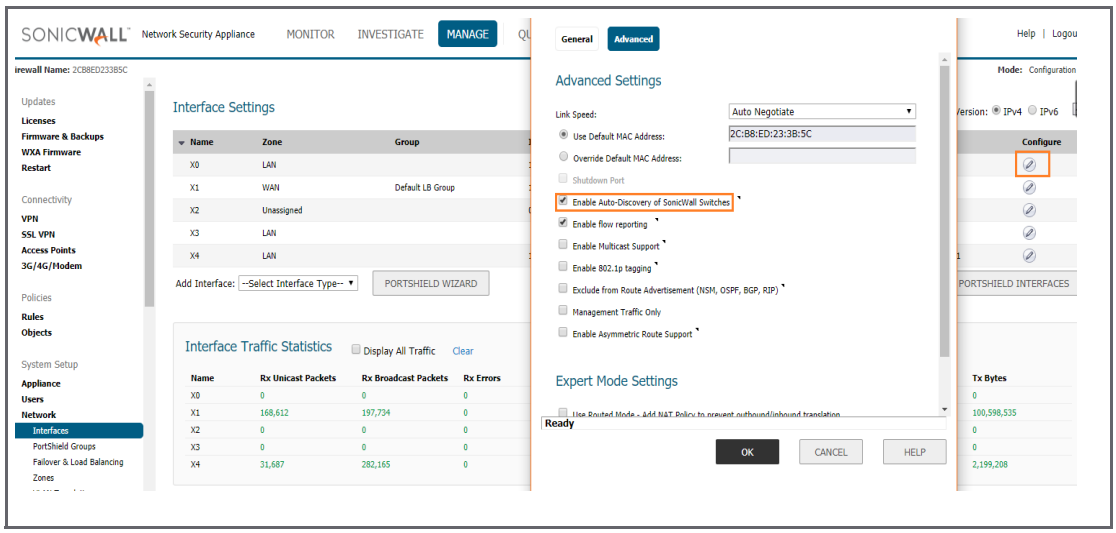
To prepare firewall:

1 Check that the firewall firmware is at the most recent level.



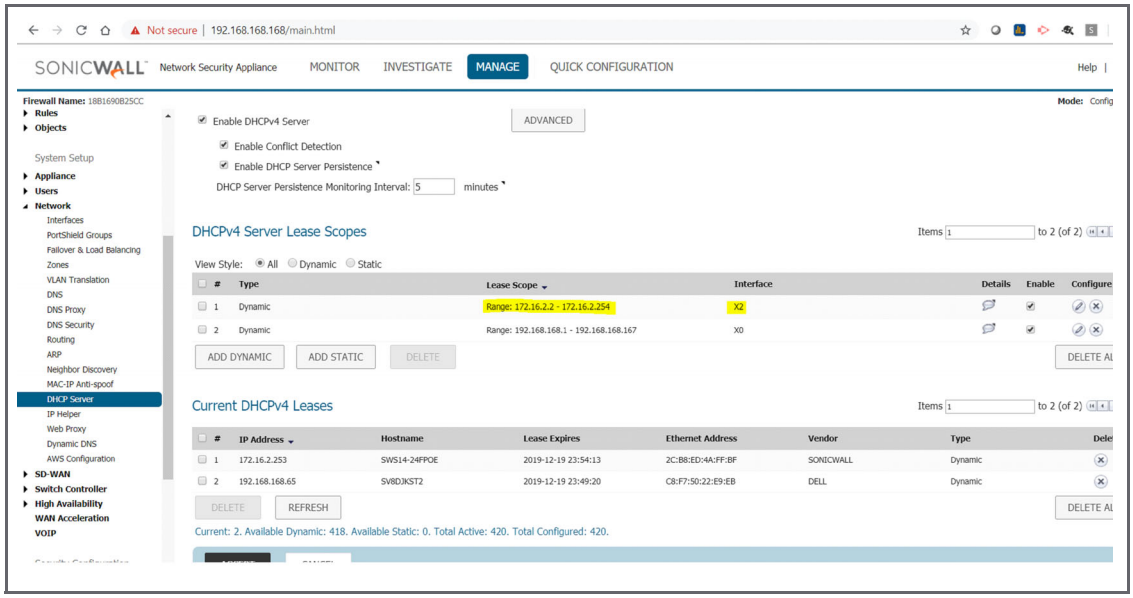
2 Select an interface on the firewall to connect to the Switch. Navigate to **Manage > Network > Interfaces** and select an interface, then click on **Configure** and select the **Advanced** tab.

Select **Enable AutoDiscovery of SonicWall Switches:**

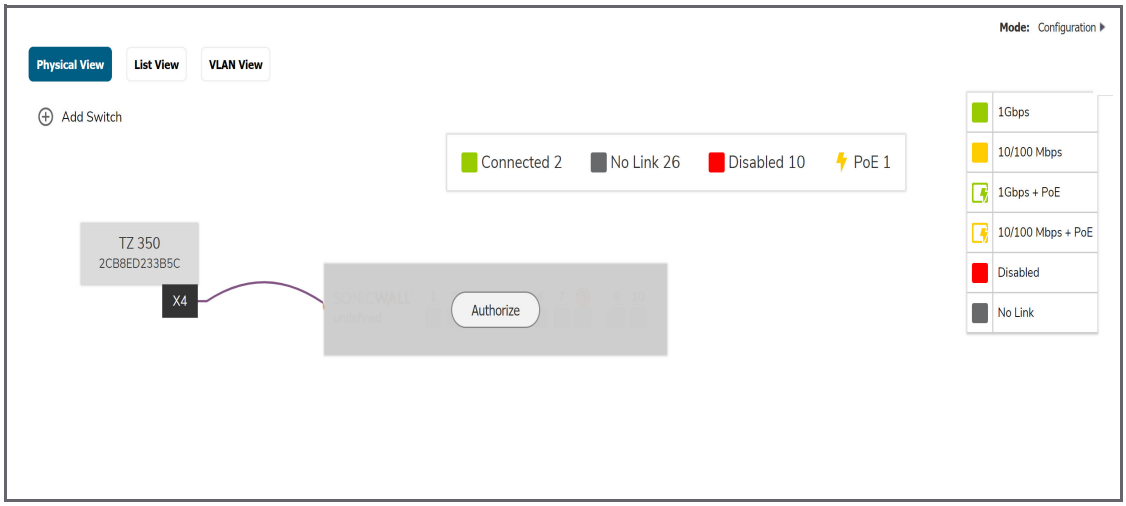


3 Connect the Switch to the selected firewall interface.

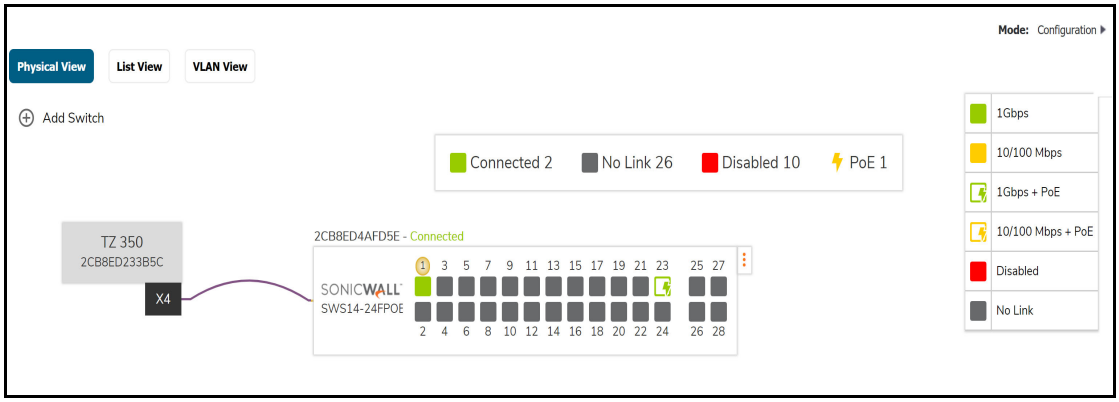
4 Navigate to **Network>DHCP Server** and verify **DHCPv4 Server Lease Scope** is enabled for the selected network.



5 Navigate to **Manage > Switch Controller > Overview**, Click on **Authorize** button to add the Switch to firewall:



6 The network topology will now appear on the **Overview.**



Adding a Switch to a Firewall Manually

IMPORTANT: Please register your Switch before trying to add it to a firewall. See Registering Your Switch on page 4.

Once an IP address is established as described in Adding a Switch to a Firewall Manually on page 27, only a few steps are necessary to set it up for management from a firewall.

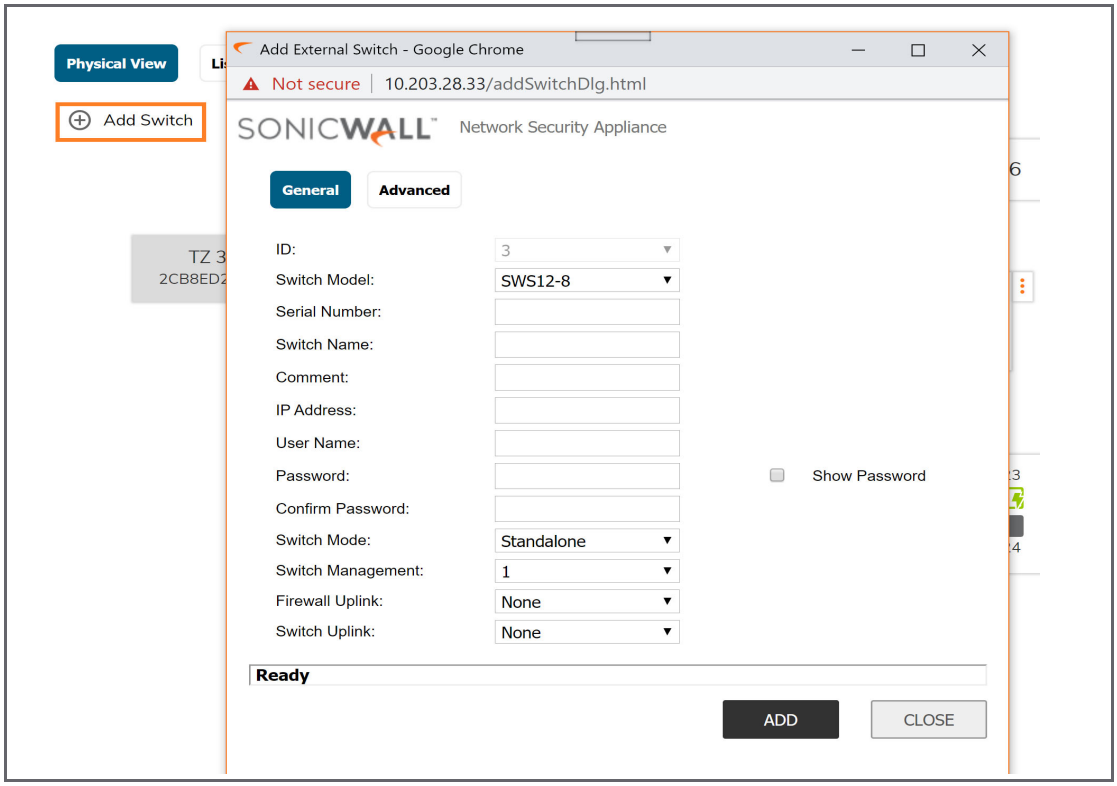
To Connect Switch to Firewall:

1 Connect an Ethernet cable (that is, RJ45 to RJ45) from a port on the Sonic Switch to an available port on the firewall.

NOTE: When adding a Switch manually, first check that it is configured to factory defaults. This can be ensured by depressing the reset switch for 10 seconds or more. The Switch can also be factory defaulted from the Switch Local UI, or the Command Line Interface accessible through the console port.

NOTE: To change the Reserved VLAN range on the firewall, do so before adding the SonicWall Switch. If the Reserved VLAN range changes after connecting the Switch, then the Switch must be removed and re-added.

2 Login to the management console and navigate to **MANAGE | System Setup > Switch Controller** and note the Switch-related pages. From Overview click on **Add Switch** as shown below.



NOTE: If the above options do not appear, check that your firewall and Switch are at the correct firmware release levels.

3 Click on **Switch** and when the Switch List appears click on **Add Switch**. The dialog box will appear:

- **ID**: The system will auto-assign a consecutive number here.

- **Switch Model**: Click on the down-pointing selection arrow and choose. Check the label on the bottom of your Switch if necessary.
- **Serial Number**: Check the label on the bottom of the Switch.
- **Switch Name**: Your choice.
- **Comment**: For optional reference.
- **IP Address:** What was established in To add Switch to a network with a DHCP server: on page 16 or, To add Switch to a network without a DHCP server: on page 17.
- **User Name**: In most test cases, Admin. To add additional users, see Setting Up Users on page 41.
- **Password:** The password is configured on the Switch.
- **Switch Mode:** The choices are **Standalone** for one Switch per port or **Daisy Chain** when multiple Switches are added such that no Switch connects with more than two others.
- **Switch Management:** Management traffic flows on this interface.
- **Firewall Uplink:** This is the port on the firewall to which the Switch will connect.
- **Switch Uplink:** This is the port on the Switch connecting to the firewall.

Click on **Advanced** to access the Spanning Tree Protocol settings:

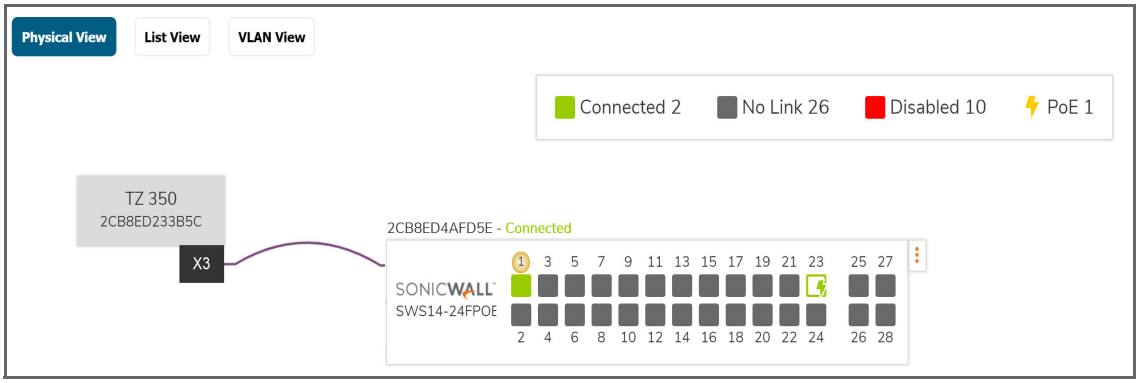
- **STP Mode**: **Rapid** or **Multiple**
- **STP State**: **Enable** or **Disabled**

  For more information on STP, see Setting Spanning Tree Protocol on page 53.
- **Jumbo Frame Size:** The default is the maximum standard transmission unit size in bytes. The default is 1522. Frame sizes larger than this are jumbo.

  NOTE: Jumbo frames are not supported on TZ model firewalls.

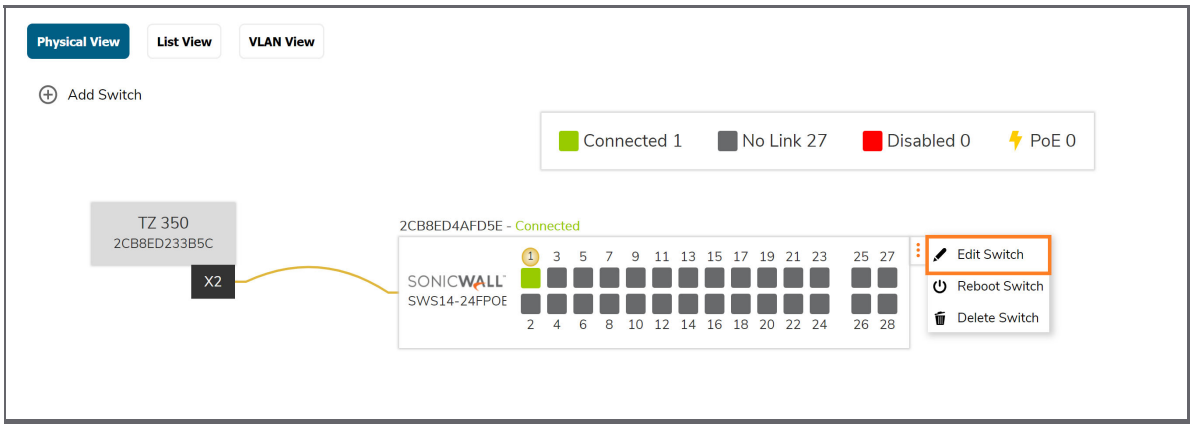
4 Once the dialog boxes are complete, click on **Add**.

5 Go to the **Overview**, the new Switch will appear graphically with the ports linking the Switch and the firewall indicated.



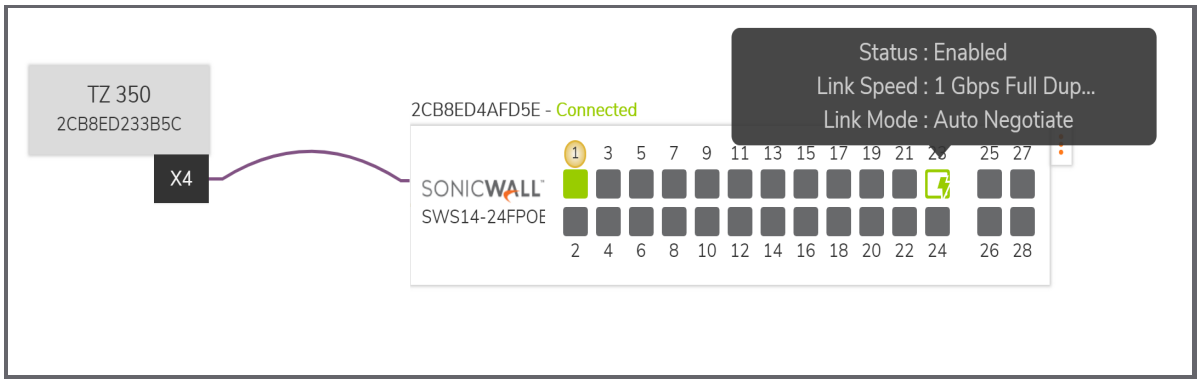
Changing the Switch Configuration

Click the “three-dot” box to the right of the switch graphic in the **Physical Overview** display and then select **Edit**.



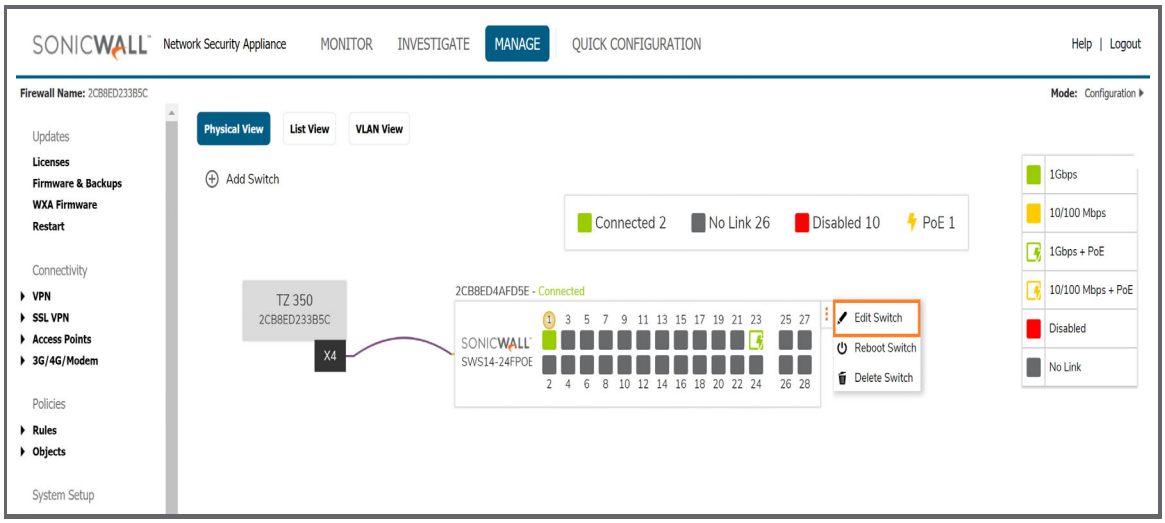
Check the Status and Link Details

Navigate to **Switch Controller > Overview** and hover over the Switch port.



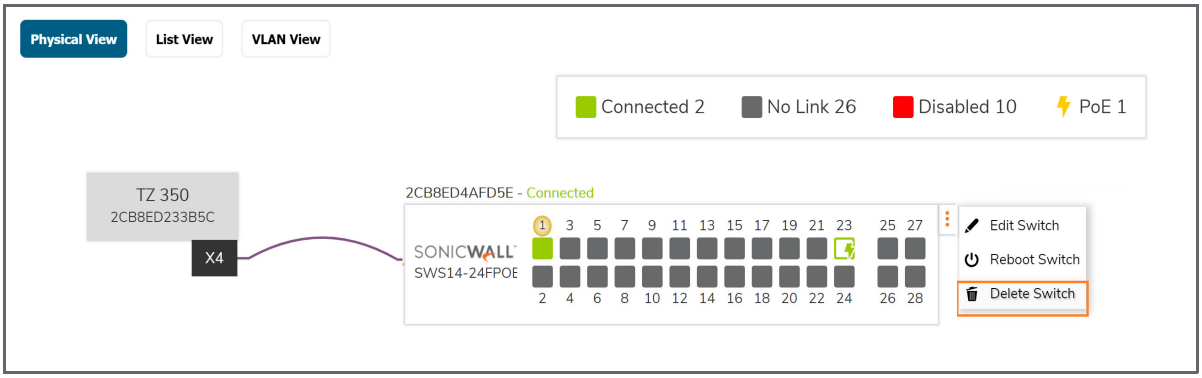
Enabling the Switch

If the firewall to Switch link is down, navigate to **Switch Controller > Overview** and click on 3 dot menu of the Switch which is off-line and then click on **Edit Switch** to bring up the Switch configuration dialog box. Check if the Switch configuration details are correct including: IP address, serial number, and Switch Management interface. This can also be done by going to **Switch Controller** > **Switches** and clicking on **Configure**. See Changing the Switch Configuration on page 29.



Shutting Down the Switch

To remove a Switch from a firewall, navigate to **Switch Controller > Overview > Physical View** and click on the **Delete Switch**. This can also be done by going to **Switch Controller** > **Switches** and clicking on **Configure**. See Changing the Switch Configuration on page 29.



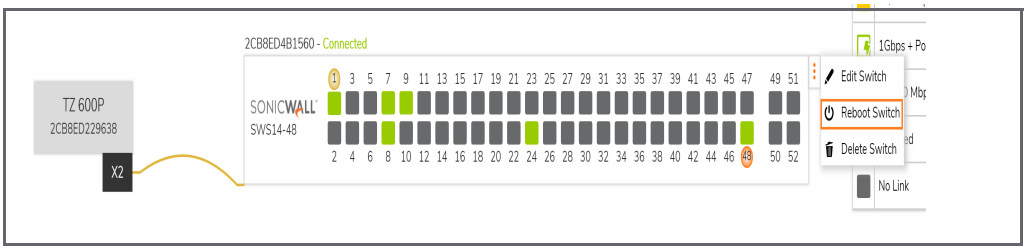
Restarting the Switch

To reboot the Switch:

1 Simply depress the recessed reset Switch on the front panel for a second.

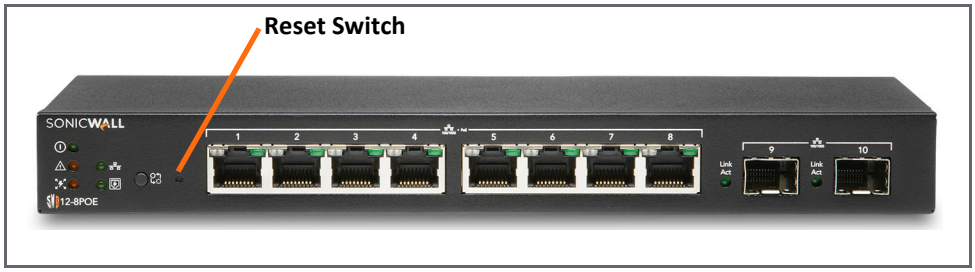
OR:

1 Click on the 3 dot menu on the Switch image on the Overview page and click on **Reboot Switch**.



To reboot the Switch to factory defaults:

1 Use a paper clip to depress the front panel reset Switch for over 10 seconds.



Adding a VLAN

A Virtual LAN (VLAN) is a group of ports that form a logical Ethernet segment on a Layer 2 Switch to provide better administration, security, and management of traffic. A VLAN is a network topology configured according to a logical scheme rather than a physical layout. When you use a VLAN, users can be grouped by logical function instead of physical location. All ports that frequently communicate with each other are assigned to the same VLAN, regardless of where their location in the network. VLANs let you logically segment your network into different broadcast domains allowing the grouping of 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, thus avoiding broadcast packets being sent to all the ports on a single Switch. A VLAN also increases network performance by limiting broadcasts to a smaller, more manageable logical broadcast domain. By limiting traffic to specific broadcast domains, VLANs improve security.

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

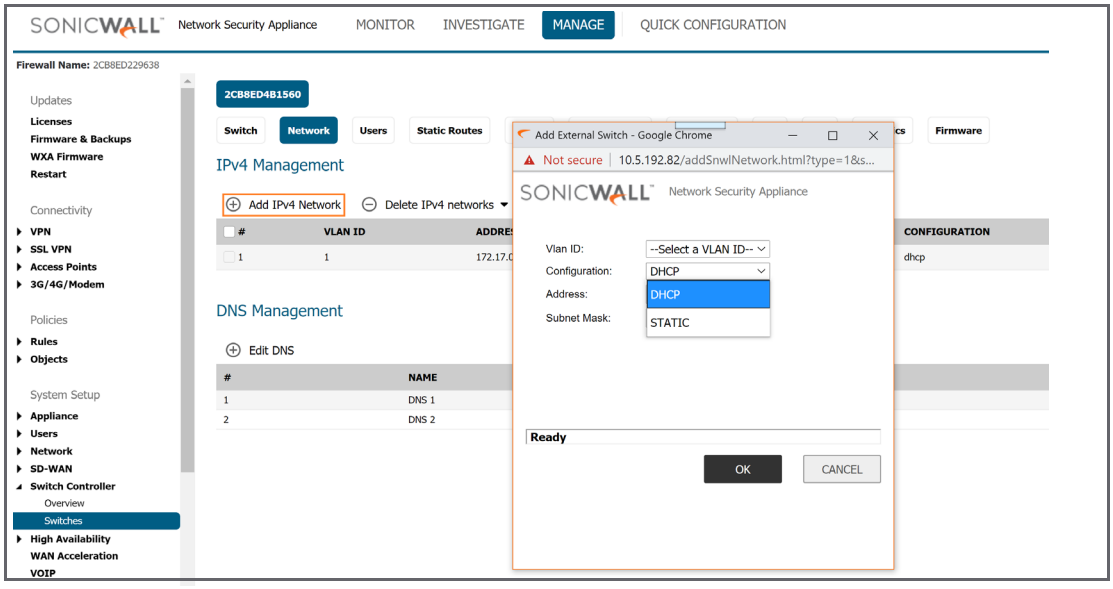
IMPORTANT: To change the Reserved VLAN range on the firewall, do so before adding the SonicWall Switch. If the Reserved VLAN range changes after connecting the Switch, then the Switch must be removed and re-added.

Adding a VLAN Interface:

Add a VLAN by adding a virtual interface under the uplink to the firewall.

1 Navigate to **Switch Controller > Switches**.

2 Click on **Add IPv4 Network**.



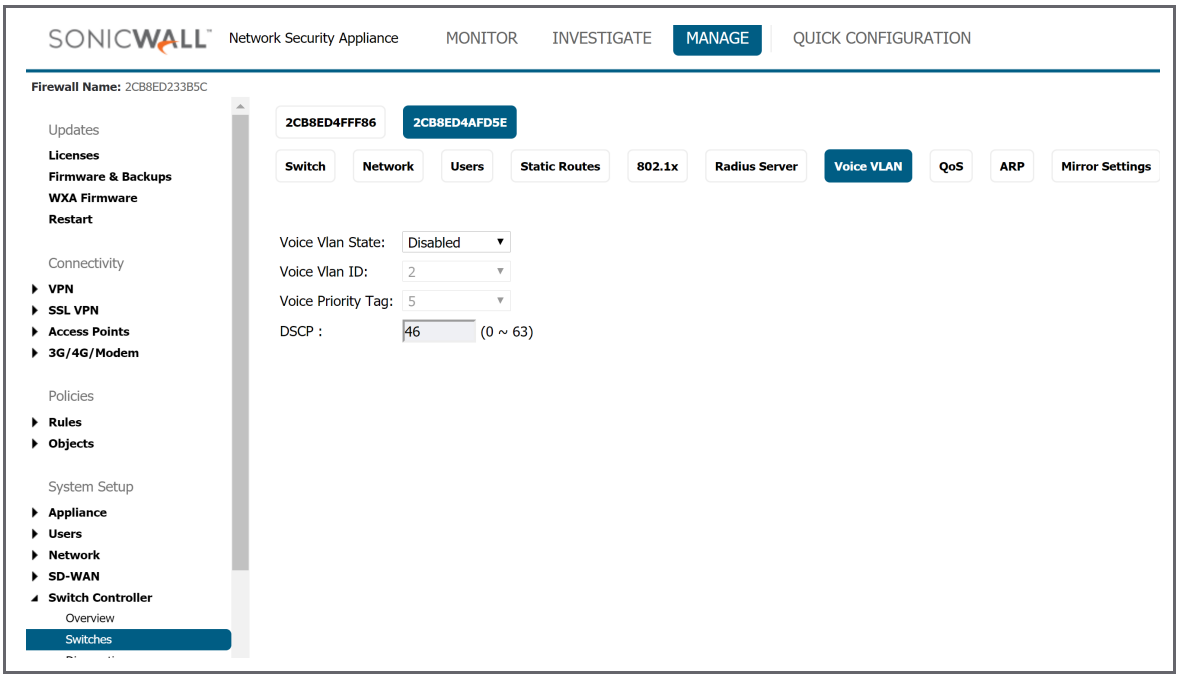
3 Define **Vlan ID**, **Address**, **Subnet Mask** and choose address assignment method: **Static** or **DHCP**.

4 Click on **OK**.

Configuring Voice VLAN:

NOTE: Voice VLANs can be enabled/disabled per port in the **Switch Controller > Overview > Physical View** display.

1 To configure a voice VLANs navigate to **Switch Controller > Switches** and then click on **Voice VLAN.**



2 Set up a voice VLAN by moving the state from **Disabled** to **Auto** and set the other parameters before clicking on **Accept** as it appears at the bottom of the display.

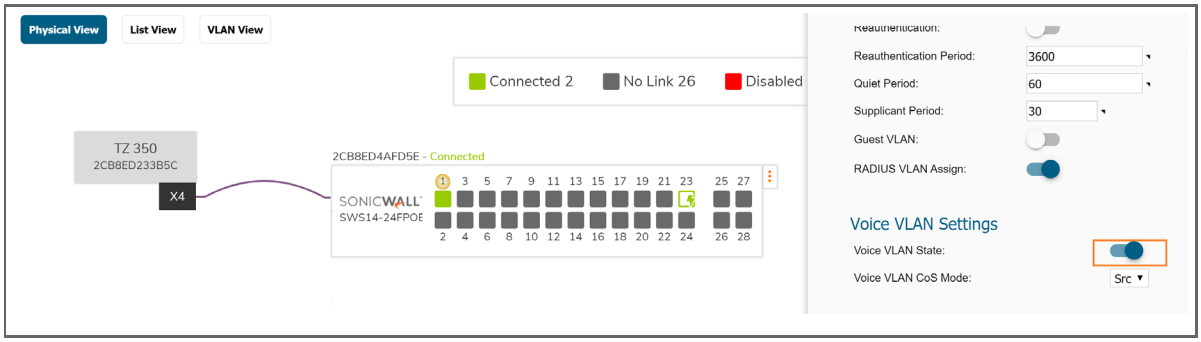
- **Voice Vlan ID —** identifies LAN.
- **Voice Priority Tag —** determines priority among active voice streams.
- **Differentiated Service Code Point —** defines QoS.

Use the Voice VLAN Settings to enable Voice traffic management and determine if Class of Service (CoS) queues will be defined for all ports or only those sourcing voice traffic. For more on CoS definition, see Setting Up QoS on page 38.

NOTE: The Switch remarks incoming voice VLAN traffic tags for voice priority and DSCP as defined by these settings.

To Enable/Disable Voice VLAN from the Physical View:

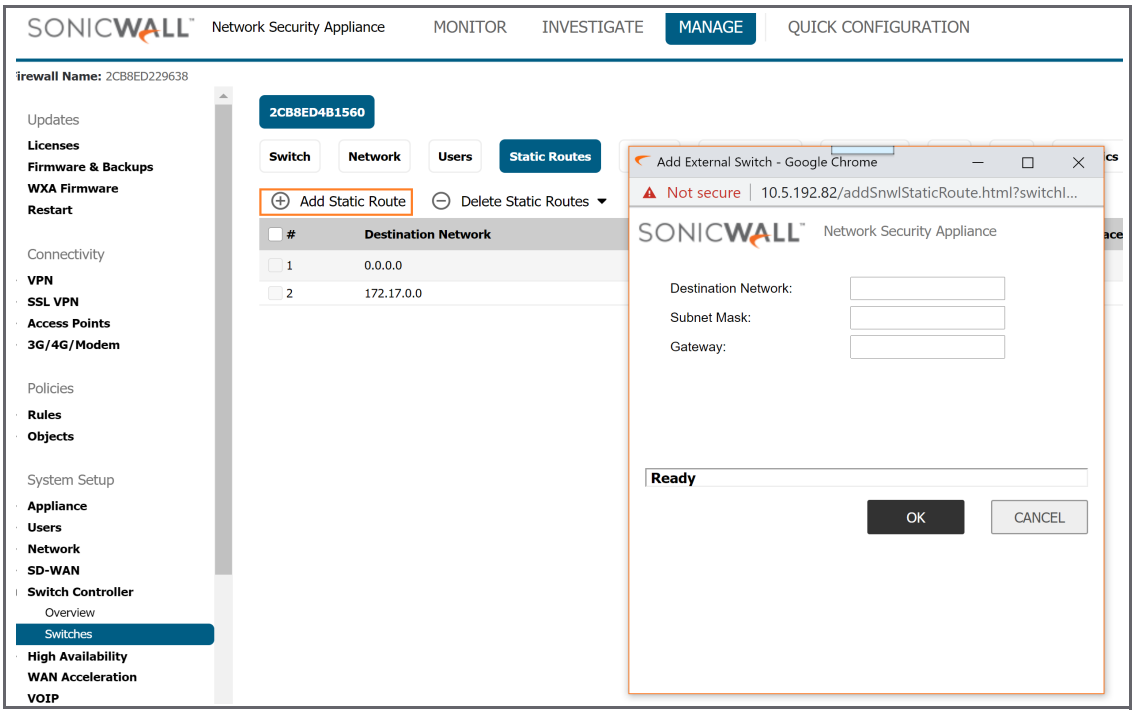
Simply go to **MANAGE > Switch Controller > Overview** and click on the port. When the sideband display appears scroll to Voice VLAN state as shown below.



Adding Static Routes

To add a static route to a Switch:

1 Navigate to **Switch Controller > Switches** then select **Static Routes** and click on **Add Static Route**.



2 Fill out the dialog box.

Destination IP address with '0' as the last octet: x.x.x.0.

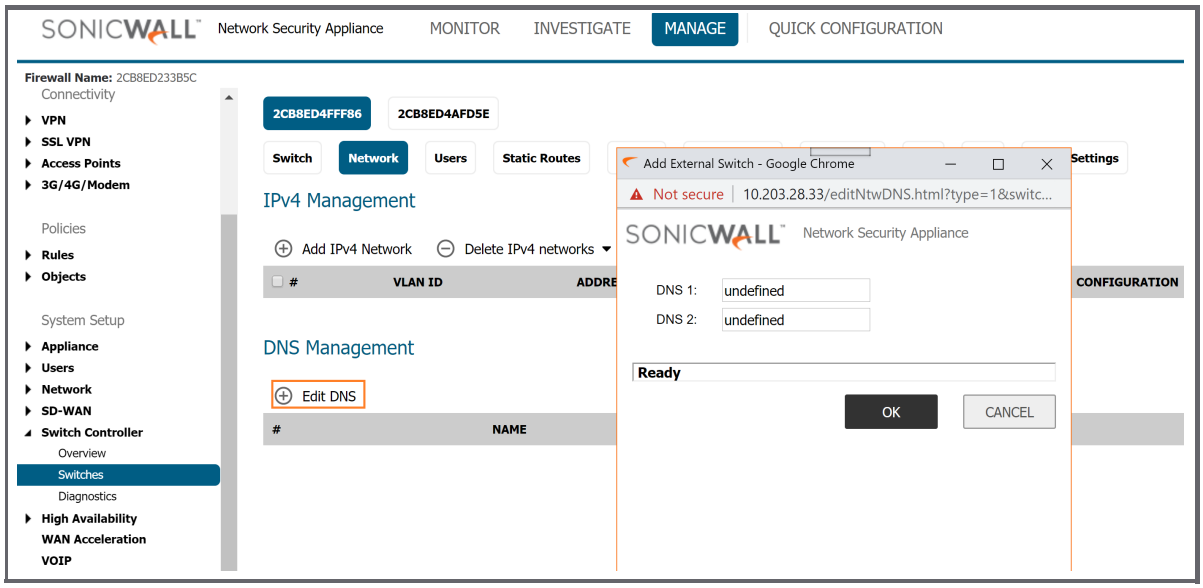
Subnet Mask for the destination.

Gateway: IP address gateway between Switch and destination.

3 Click on **OK**.

Editing DNS

To set DNS addresses go to **Switch Controller > Switches** and select **Network,** then click on **Edit DNS**.



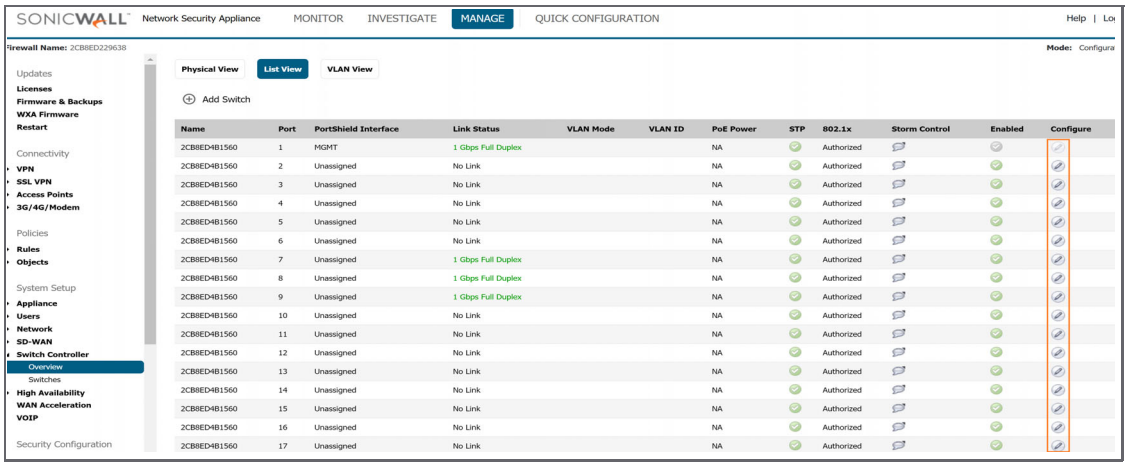
Setting Up the Ports

To configure specific ports:

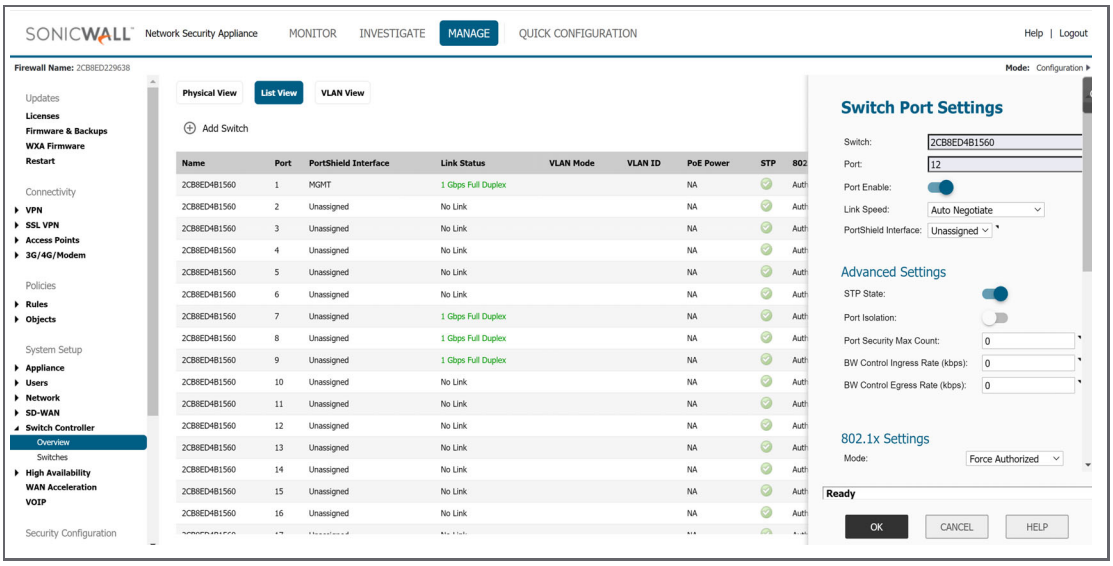
1 Go to **Switch Controller > Overview** and click on **List View**.

This can also be done from the **Physical View**.

2 When the list appears click on the edit button for the specific port.



3 The port setup dialog for the specific port will now appear to the right of the screen.

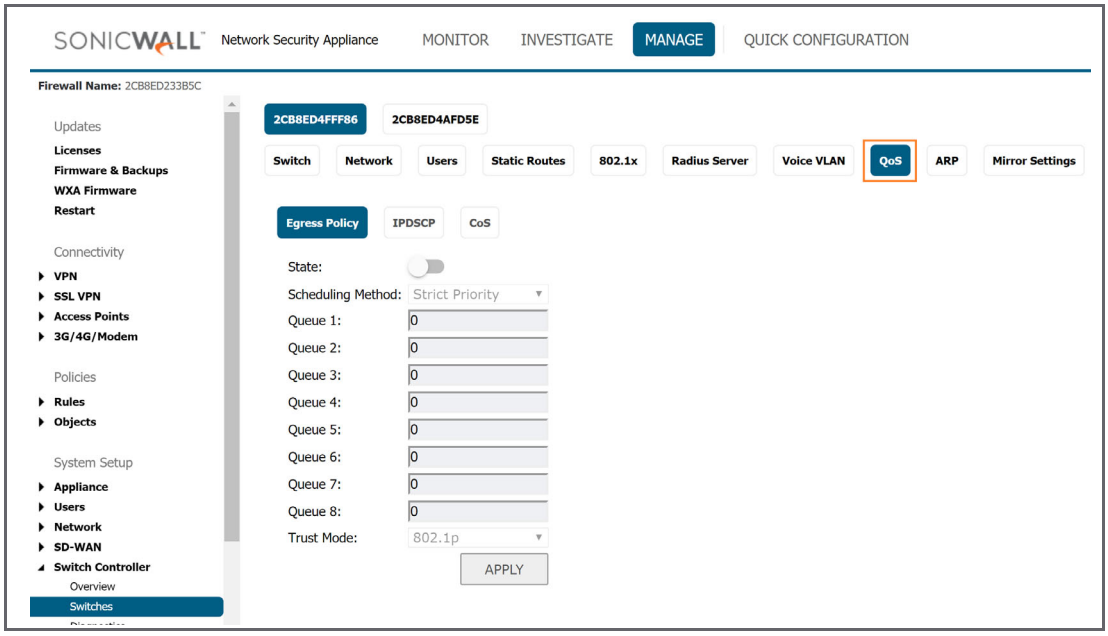


Setting Up QoS

Quality of Service (QoS) provides the ability to implement priority queuing within a network. QoS enables traffic to be prioritized, while minimizing excessive broadcast and multicast. 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.

To set up QoS for a Switch:

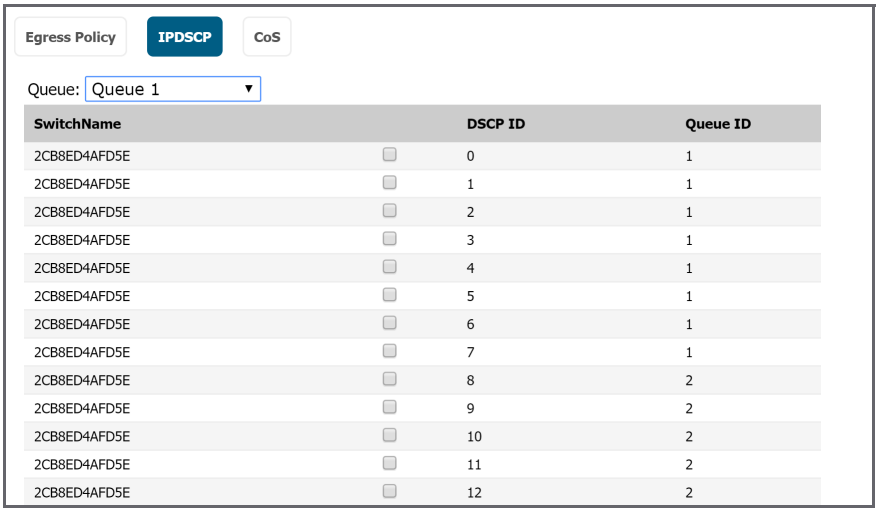
1 Navigate to **Switch Controller > Switches** and click on **QoS**.



2 Set Egress Policy.

The first screen details Egress Policy which applies for all approaches to packet and traffic classification.In the preceding UI screen, the **State** slider determines whether QoS is enabled (to the right) or disabed (to the left). Scheduling method can be set as **Strict Priority** based on Queue number or as Weighted Round Robin (**WRR**). The classification of packets can be set as 802.1p or DSCP (Differentiated Sevices Code Point), or as both.

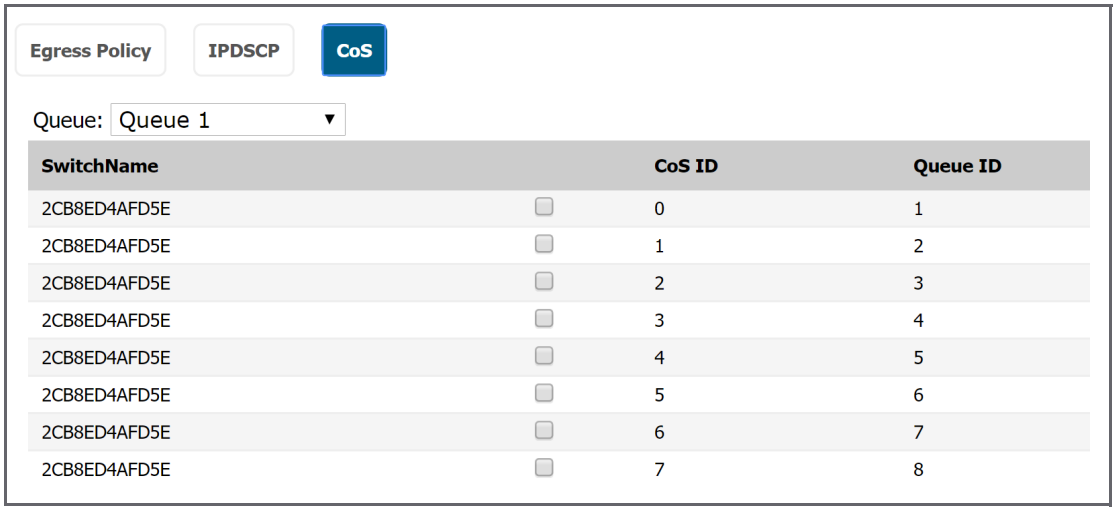
3 Select the **IPDSCP** screen to set DSCP codes to specific Queues.



SwitchName	DSCP ID	Queue ID
2CB8ED4AFD5E	0	1
2CB8ED4AFD5E	1	1
2CB8ED4AFD5E	2	1
2CB8ED4AFD5E	3	1
2CB8ED4AFD5E	4	1
2CB8ED4AFD5E	5	1
2CB8ED4AFD5E	6	1
2CB8ED4AFD5E	7	1
2CB8ED4AFD5E	8	2
2CB8ED4AFD5E	9	2
2CB8ED4AFD5E	10	2
2CB8ED4AFD5E	11	2
2CB8ED4AFD5E	12	2

4 To set class of service, click on **CoS**..

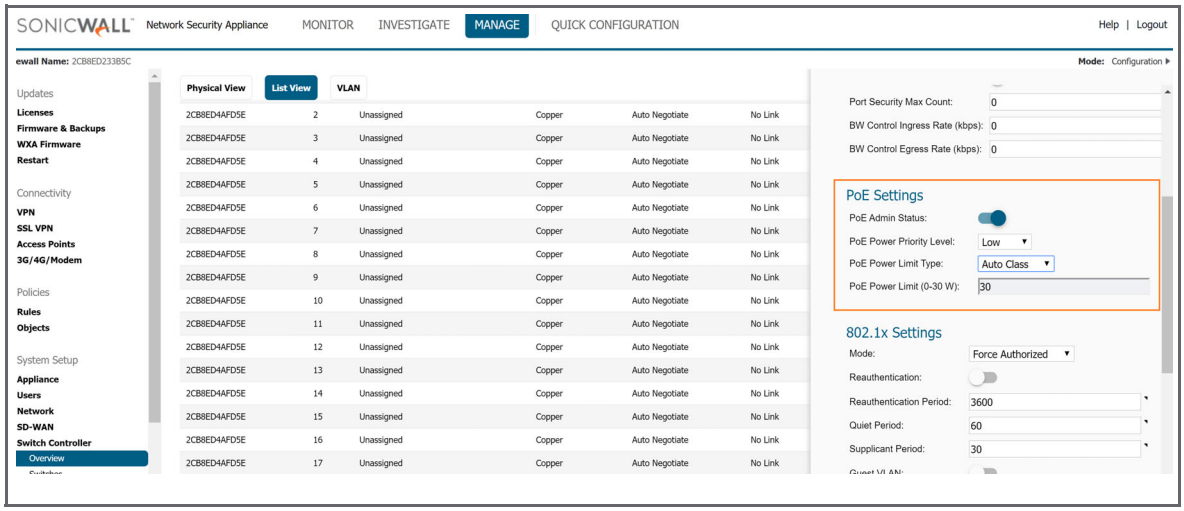
In the CoS (Class of Service) screen, the CoS priority tag values, where 0 is the lowest and 7 is the highest are related to eight traffic priority queues from 1 to 8, where one is the lowest priority and eight is the highest priority.



SwitchName		CoS ID	Queue ID
2CB8ED4AFD5E	☐	0	1
2CB8ED4AFD5E	☐	1	2
2CB8ED4AFD5E	☐	2	3
2CB8ED4AFD5E	☐	3	4
2CB8ED4AFD5E	☐	4	5
2CB8ED4AFD5E	☐	5	6
2CB8ED4AFD5E	☐	6	7
2CB8ED4AFD5E	☐	7	8

Setting Up PoE

To set up PoE limits per port, navigate to **Switch Controller > Overview** and click on **List View.** Select the click on the edit button for the port for PoE setup. Scroll down in the port configuration panel until the PoE settings appear.



The PoE+ Switches support Power over Ethernet (PoE) as defined by the IEEE 802.3af and 802.3at. The SWS12-8 PoE-enabled Switches support the -af standard and up to 15.4 Watts per port. The SWS12-10 and SWS14 series PoE-enabled Switches support the 30 Watts per port.

The Switches follow the standard PSE (Power Sourcing Equipment) pinout, whereby power is sent out over pins 1, 2, 3 and 6.

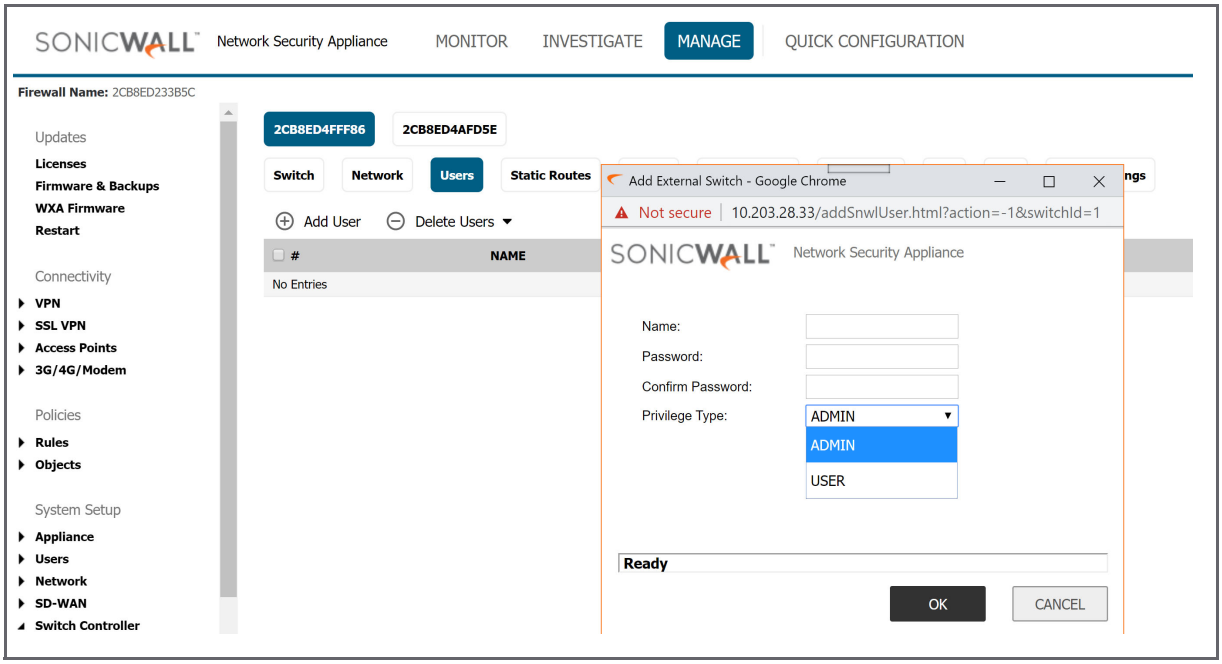
- **PoE Admin Status**
  - **Enabled -** Enables the Device Discovery protocol and provides power to the device using the PoE module. The Device Discovery Protocol lets the device discover powered devices attached to device interfaces and learns their classification.
  - **Disabled -** Disables the Device Discovery protocol and halts the power supply delivering power to the device using the PoE module.
- **PoE Priority**
  Select the port priority if the power supply is low. The field default is Low. For example, if the power supply is running at 99% usage, and port 1 is prioritized as high, but port 6 is prioritized as low, port 1 is prioritized to receive power and port 6 may be denied power. The possible field values are: 4.
  - **Low** – Sets the PoE priority level as low.
  - **Medium** – Sets the PoE priority level as medium.
  - **High** – Sets the PoE priority level as high.
  - **Critical** – Sets the PoE priority level as critical.
- **PoE Power Limit Type**
  - **Auto Class** - 15.4 or 30 W per port.
  - **User Defined** - Sets the maximum amount of power that can be delivered by a port.

    NOTE: The User Power Limit can only be implemented when the Auto Class value is set to User-Defined.

Setting Up Users

Users with different access levels, **admin** and **user**, can be defined by navigating to **Switch Controller > Switches** and clicking on **Users**.

Users are limited to Non-Configuration Mode.



Setting Up 802.1x Authentication

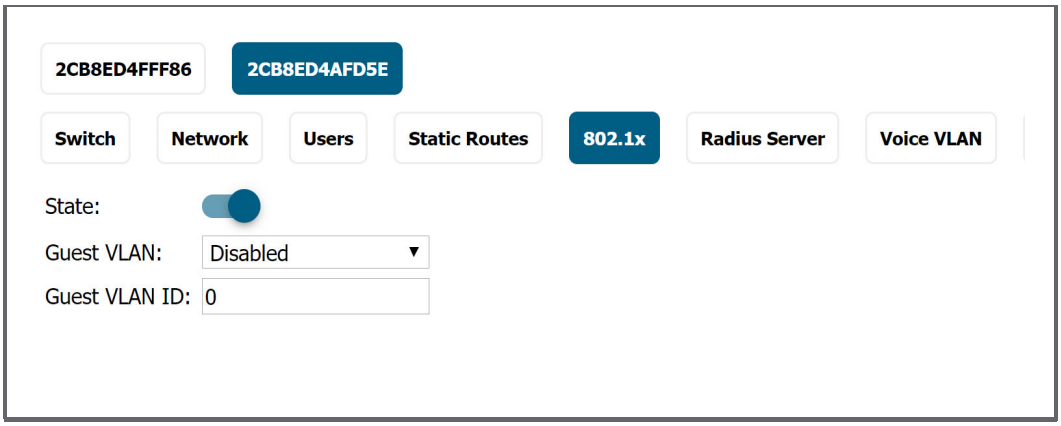
The IEEE-802.1X authentication provides a security standard for network access control with RADIUS servers and holds a network port disconnected until authentication is completed. With 802.1X authentication, the supplicant provides credentials, such as user name, password, or digital certificate to the 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.

To enable 802.1 Authentication

1 Go **MANAGE > Switch Controller > Switches** and click on 802.1 x.

2 Set the **State** slider to the right to enable authentication.
Other settings are:

- **Guest VLAN** — Select whether Guest VLAN is enabled or disabled on the Switch. The Default is disabled.
- **Guest VLAN ID** — Select the Guest VLAN from the list for currently defined VLANs.



To enable RADUIS server

1 In **MANAGE** > **Switch Controller > Switches** click on **Radius Server.** When the server list appears click on **Add Radius Server.**

2 To enable the Radius server, set the **Authorized Port** as **1812.**

Daisy-Chaining Switches

Switches can be setup with firewalls in standalone or daisy-chained configurations.

- **Standalone mode** — Up to four Switches can interface to a single firewall over separate ports.
- **Daisy Chain mode** — Up to four Switches can be supported in three configurations.
    a 1 Switch in standalone mode and three Switches connected to it in daisy chain mode.
    b 2 Switches in standalone mode and with 1 Switch connected to each in daisy chain mode.
    c 3 Switches in standalone mode and 1 Switch connected to any of the Switches in daisy chain mode.

NOTE: Switches may be added into daisy-chained configurations manually or by using Zero-Touch.

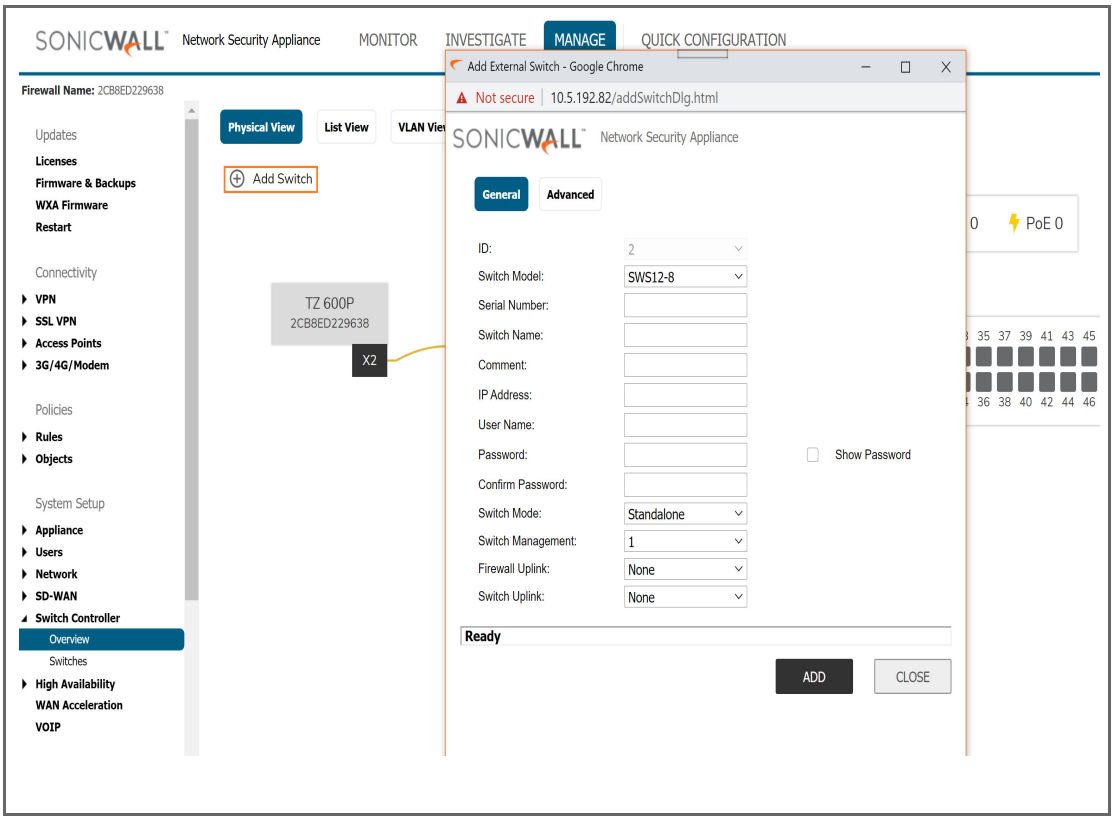
NOTE: Adding un-configured connections between the firewall and parent Switch will bring down the link between the parent Switch and a child Switch. To avoid this, configure additional links between the firewall and parent Switch before making the physical connection.

After connecting the child Switch to the parent Switch, the Switch will be visible in the **Switch Controller > Overview** page. Simply click the Authorize option and the Switch will be added in daisy chain manner.

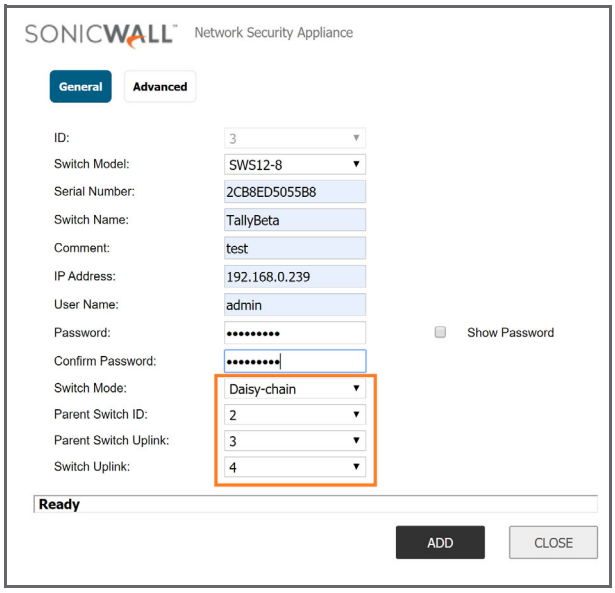
To add a Switch in daisy chain mode:

1 Select a Switch in standalone configuration to daisy-chain the additional Switch to. Then determine which ports to use to connect the additional Switch.

2 Go to **MANAGE | Switch Controller > Overview** and click on **Add Switch**.



3 When the **Add Switch** dialog box appears, make the entries outlined below.



- **IP Address —** This is an address within the leasehold of the DHCP server for Parent Switch. To identify this address range, go to **MANAGE | Network > DHCP Server.**
- **Switch Mode —** Select **Daisy-chain**.
- **Parent Switch ID —** For the ID of the parent Switch, refer to screen shot in Step 2. It is the second column in the row for this Switch.
- **Parent Switch Uplink** — Interface on parent Switch which is connected to the child Switch.
- **Switch Uplink —** This is the port through which the daisy-chained Switch connects to the Parent Switch.

4 When complete with the dialog box click on **ADD**.

NOTE: Define the first Switch connected to the firewall as **Standalone.** Setup the Switch connected to that Switch as **Daisy-chain**.

5 Navigate to **Switch Controller > Overview** and **click** on **Physical View**. The new Switch will appear graphically with the ports linking the Switch and the firewall indicated.

Connecting Access Points

With the firewall user interface, administrators may manage SonicWave access points connected to Switches.

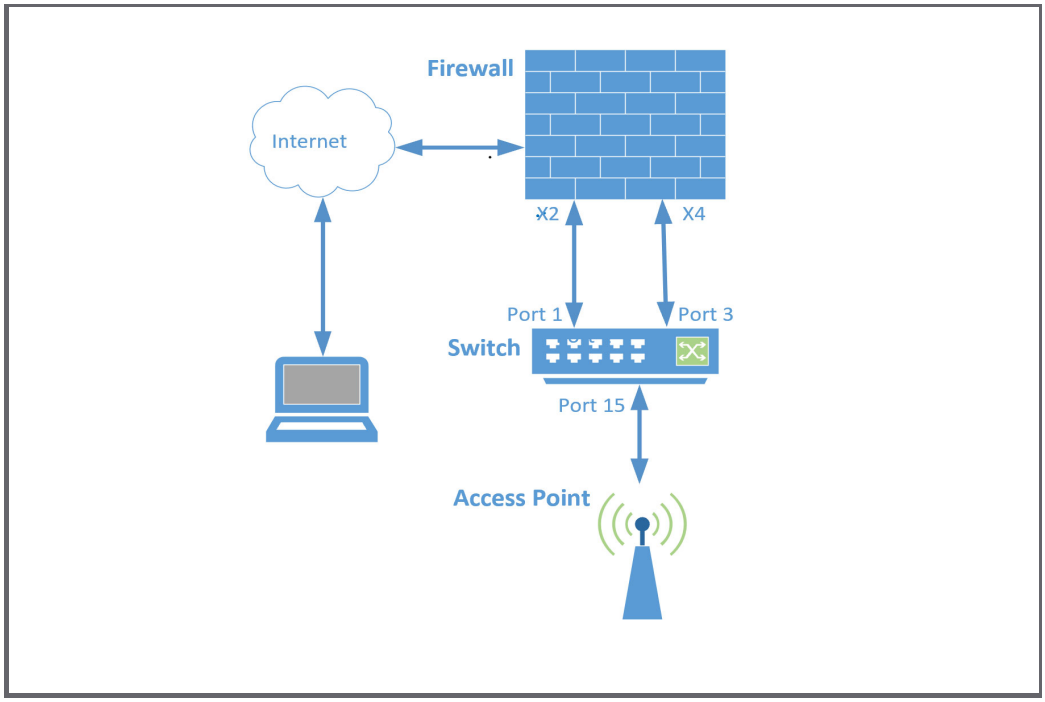
Adding access points to a Switch involves three steps beyond making the physical connection.

- Configure the network interface to the Switch supporting the access point to support the WLAN.
- Configure the WLAN zone for trust and security services.
- Configure the SonicWave access point entry for the desired radio frequency, mode, and authentication type.

The following graphic exemplifies a ***firewall — Switch — access point*** configuration.

To manage an access point through a Switch:

(this procedure refers to the following diagram)



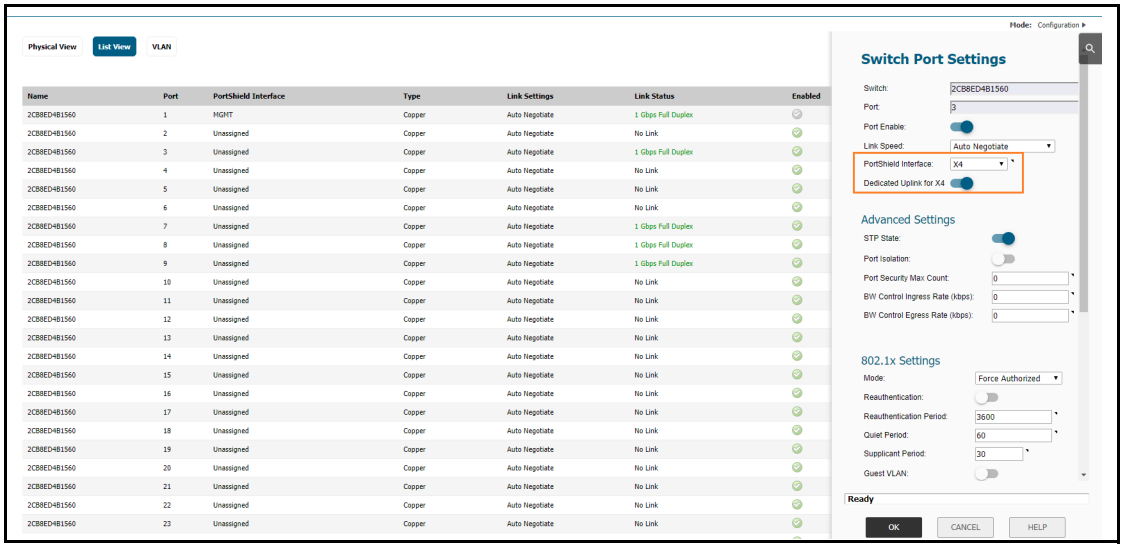
1 Connect Port-1 of Switch to X2 interface and enable auto discovery on X2 interface.
For details refer to Firewall Switch Controller UI on page 22.

2 Add the Switch.

3 Configure X4 in WLAN zone with VLANs.
Refer to Connect the SonicWave access point to port 15 on the Switch. on page 46 and To Configure the WLAN Zone: on page 47.

4 Connect Switch Port 3 to X4 interface.

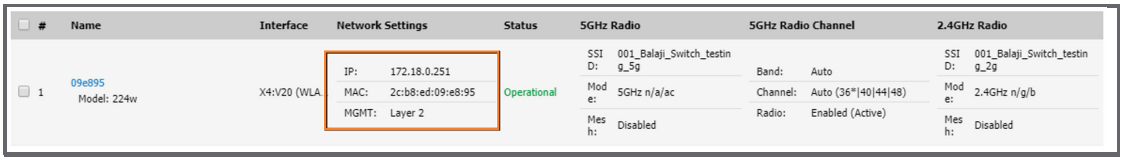
5 In the firewall GUI, navigate to **Switch Controller > Overview**, click **List View**. Click on the pencil icon to configure port 3. To create a dedicated uplink, set the **Portshield Interface** to X4, and move the **Dedicated Uplink** Switch to the right.



6 Connect the SonicWave access point to port 15 on the Switch.

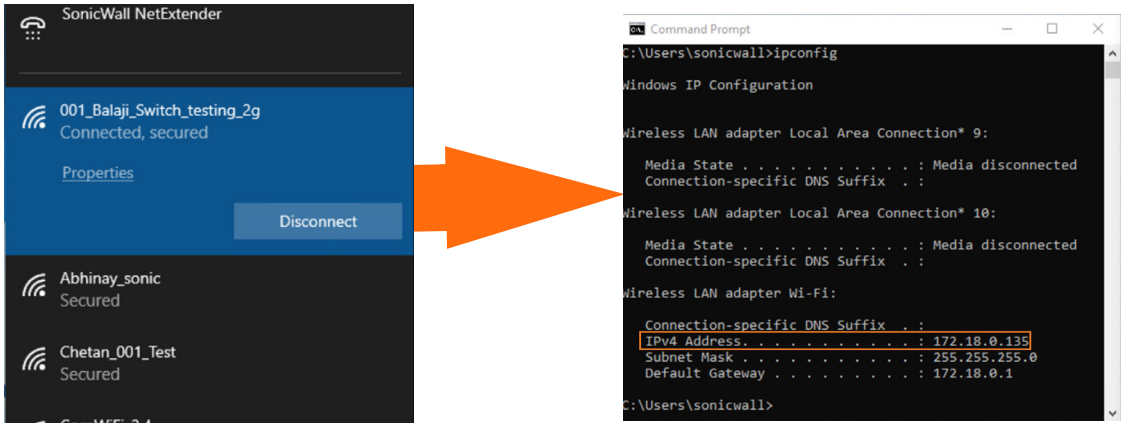
7 Go to the Switch Port Settings for port 15 (as in step 5) and set the Portshield Interface to X4.
You may instead set the port to any VLAN in the X4 interface which is in the WLAN zone, see Adding a VLAN on page 32.

8 After connecting and Port-Shielding the interface where SonicWave connected to firewall interface, verify that the Sonicwave gets an IP address from the configured network.
To do this, in the firewall GUI, go to **Access Points > Base Settings** and select **SonicWave Object.**



For details on configuring the SonicWave object, see Configuring the SonicWave Settings: on page 48.

9 Connect a WiFi client and check that it gets an IP address from in the X4 Portshield leasehold.

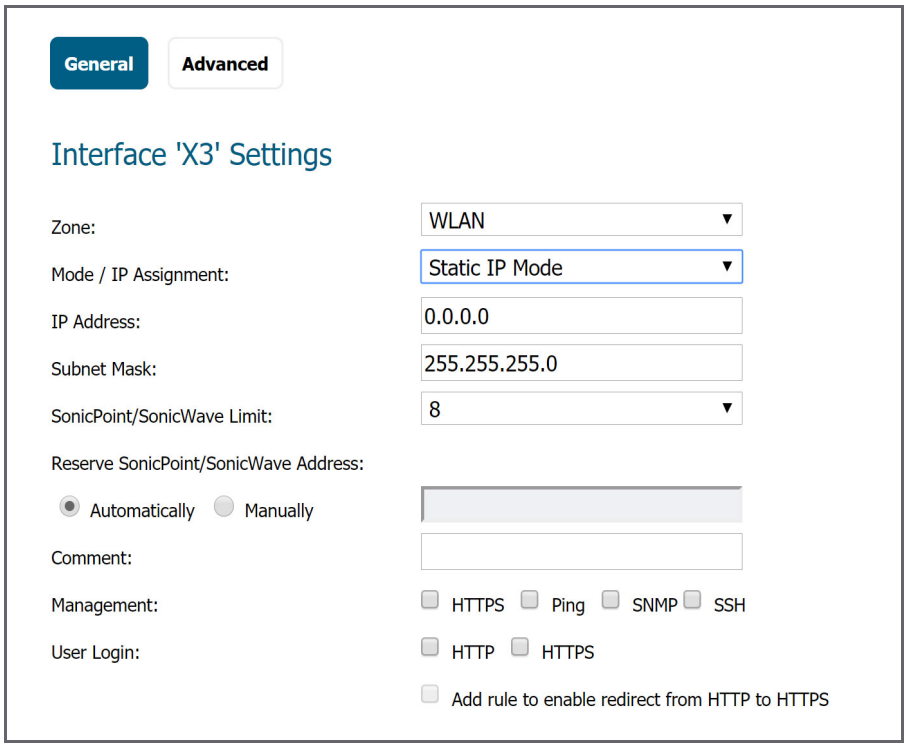


Configure the network interface to the Switch supporting the access point to support to WLAN.

1 Login to the firewall as an adminstrator and go to **MANAGE | Network > Interfaces** page and click on the configure icon for the inteface the Switch is supported on.

2 Select **WLAN** for the **Zone** type.

3 Select the **Static IP Mode** for the **Mode/IP Assignment**.



4 In the **IP Address** field, type in any private IP address that does not interfere with the IP address range of any other interfaces on the appliance.

5 Enter a **Subnet Mask**. The default is 255.255.255.0.

6 Use the default settings or select appropriate settings for the other fields and then click **OK**.

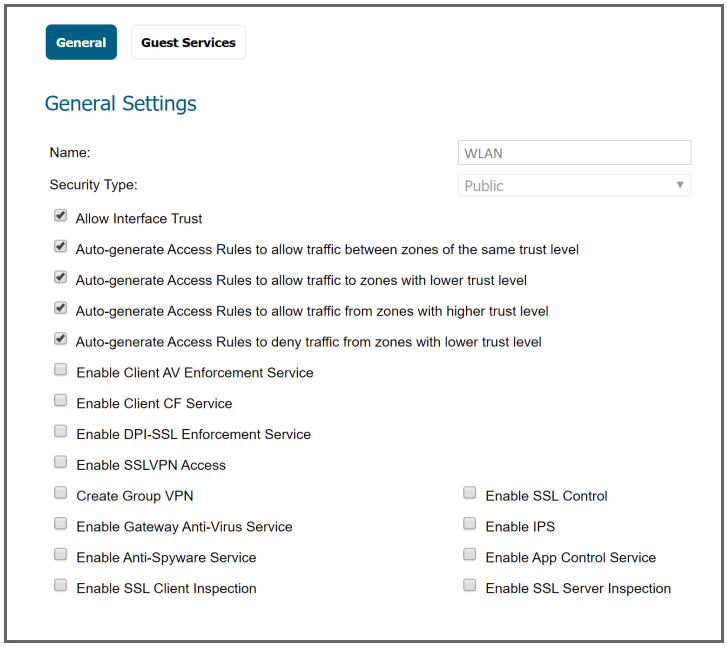
CAUTION: Allowing Management and User Login to the appliance from a wireless zone can pose a security threat if you or your users have not set strong passwords.

To Configure the WLAN Zone:

1 In the **MANAGE** view on the **System Setup | Network > Zones** page, click the **Edit** icon in the **Configure** column of the **WLAN** row.

2 On the **General** page, under **General Settings**, select the **Allow Interface Trust** option to automate the creation of Access Rules to allow traffic to flow between the interfaces within the zone, regardless of the interfaces to which the zone is applied.

For example, if the WLAN zone has both the **X1** and **X2** interfaces assigned to it, selecting **Allow Interface Trust** creates the necessary access rules to allow hosts on these interfaces to communicate with each other.



3 Select the checkboxes to enable security services on this zone. Minimally, you would select **Enable Gateway Anti-Virus Service**, **Enable IPS**, and **Enable Anti-Spyware Service**, if your wireless clients are all running **Spyware Service**. If your wireless clients are all running **SonicWall Client Anti-Virus**, select Enable Client .

4 In the **Guest Services** page, optionally configure guest Internet access. For information about Guest Services, see *SonicOS 6.5.4 Connectivity Administation* the documentation.

5 In **Wireless** under **SonicPoint/SonicWave Settings**, select **Only allow traffic generated by a SonicPoint/SonicWave** to allow only traffic from SonicPoints/SonicWaves to enter the WLAN zone interfaces, providing maximum security.

6 When finished, click **OK**.

Configuring the SonicWave Settings:

When a SonicWave AP is initially connected to an interface, the firewall uses a default provisioning profile to create a SonicWave AP entry. It can take up to five minutes for the entry to be created.

You can modify the SonicWave AP entry to configure the access point name, radio frequency mode, authentication type, and other settings specific to your SonicWave AP.

TIP: For deployments of multiple SonicWaves that need the same provisioning settings, you can create a custom provisioning profile in the upper section of **Access Points > Base Settings** page in the **MANAGE** view. In **System Setup | Network > Zones** page, you can edit the WLAN zone and specify this profile on the **Wireless** page. Any SonicWaves connecting to an interface in the WLAN zone can then be provisioned with the assigned profile.

You might want to use the new **Floor Plan View** and **Topology View** features as well. See the *SonicOS 6.5.4 Connectivity Administration* documentation for more information.

To modify the SonicWave AP entry in SonicOS:

1 In the **MANAGE** view, navigate to **Access Points > Base Settings**.

2 In the **SonicPoint/SonicWave Objects** table, click the **Configure** icon in the row for the SonicWave AP entry you wish to modify.

General page settings:

1 On the **General** page, select **Enable SonicPoint**.

2 In the **Name** field, optionally type in a new name for this SonicWave AP. The existing name is assigned by the provisioning profile based on the name prefix in the profile with a unique number appended.

This is the access point name that appears in clients' lists of available wireless connections.

3 Verify the **Country Code** for the area of operation.

4 Configure the remaining options as necessary. For more information, see the *SonicOS Connectivity Administration* documentation.

Radio 0 Basic / Radio1 Basic Settings:

1 Click **Radio 0 Basic**, or **Radio 1 Basic**.

The configuration is very similar for both Radio 0 Basic and Radio 1 Basic. The main differences are the radio frequencies:

Radio	Frequency	Default Mode
Radio 0	5 GHz	5GHz 802.11ac/n/a Mixed
Radio 1	2.4 GHz	2.4GHz 802.11n/g/b Mixed

2 Select **Enable Radio**.

3 Select a **Mode** or use the default.

4 Under Wireless Security, select the **Authentication Type** for your wireless network. SonicWall recommends using **WPA2** as the authentication type if all client devices support it.

TIP: *PSK* uses a personal passphrase for authentication, *EAP* uses an Enterprise RADIUS server.

5 Select the **Cipher Type**. When using WPA and WPA2, SonicWall recommends **AES** for maximum security.

NOTE: Older client devices might not support AES.

6 Fill in the fields specific to the authentication type that you selected. The remaining fields change depending on the selected authentication type.

7 Optionally, under **ACL Enforcement**, select **Enable MAC Filter List** to enforce Access Control by allowing or denying traffic from specific devices. Select a MAC address object group from the **Allow List** or **Deny List** to automatically allow or deny traffic to and from all devices with MAC addresses in the group. The **Deny List** is enforced before the **Allow List**.

Virtual Access Point Encryption Settings:

NOTE: This section displays only if a VAP was selected from the Radio 0 Basic/1 Virtual AP Group drop-down menu in the **Virtual Access Point Settings** section of the **General** page.

The **Virtual Access Point Encryption Settings** section of both **Radio 0 Basic** and **Radio 1 Basic** are the same for the **802.11n Radio**.

Radio 0 Advanced / Radio1 Advanced Settings:

1 Click **Radio 0 Advanced** or **Radio 1 Advanced**.

The configuration is very similar for Radio 0 Advanced and Radio 1 Advanced. For most advanced options, the default settings give optimum performance. For a full description of the fields on this page, see the *SonicOS Connectivity Administration* documentation.

2 Optionally select the **Hide SSID in Beacon** checkbox.

The *SSID* refers to the access point name that appears in clients' lists of available wireless connections.

Hiding the SSID provides additional security because it requires that you know the access point name before connecting.

3 When finished configuring all options, click **OK**.

Sensor page

On the Sensor page, enable or disable **Wireless Intrusion Detection and Prevention (WIDP) mode**.

NOTE: If this option is selected, Access Point or Virtual Access Point(s) functionality is disabled automatically.

1 Select **Enable WIDF sensor** to have the SonicWave operate as a dedicated WIDP sensor. This option is not selected by default.

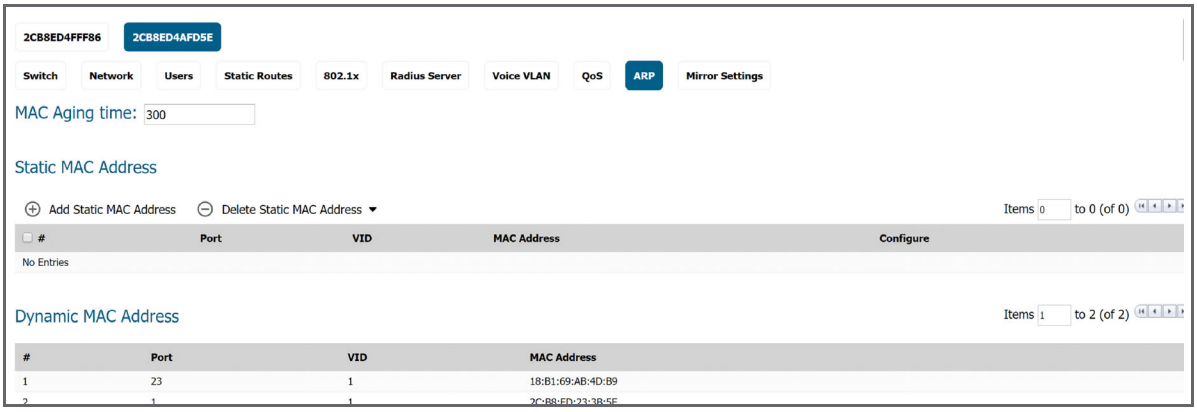
2 From the drop-down menu, select the schedule for when the SonicWave operates as a WIDP sensor or select **Create new schedule...** to specify a different time; default is **Always on**.

Modifying the MAC Address Table

The MAC address table links the MAC destination address on incoming Ethernet frames with the port closest to the destination based on learning from the transit of earlier frames. This feature allows:

- Defining MAC aging time
- Setting Static MAC table entries
- Checking Dynamic MAC entry learning

Navigate to **MANAGE > Switch Controller > Switches** and then click on **ARP**.

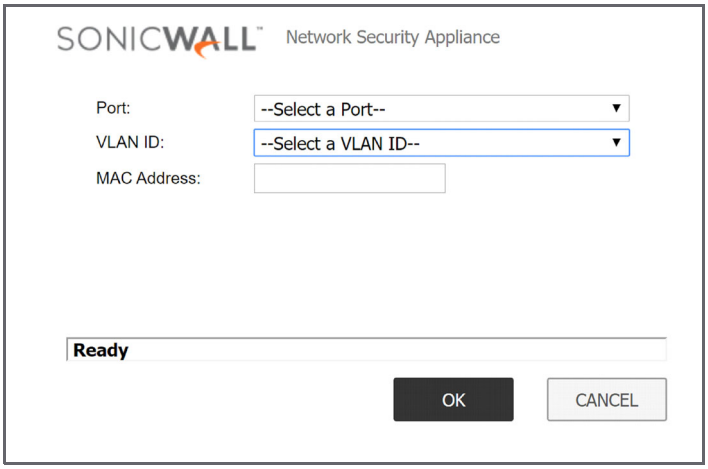


To set MAC Aging Time:

The **MAC Aging time** specifies the **time** before an entry ages and is discarded from the **MAC** address table. The range is from 0 to 1000000; The default value is 300 seconds. Entering the value 0 disables **MAC aging**. This age specification applies to all VLANs.

To add static MAC Addresses:

1 Click on **Add Static MAC Addresses** and the following dialog box will appear.



2 Select the **Port** and **VLAN ID** along with the destination MAC address and click on **OK.**

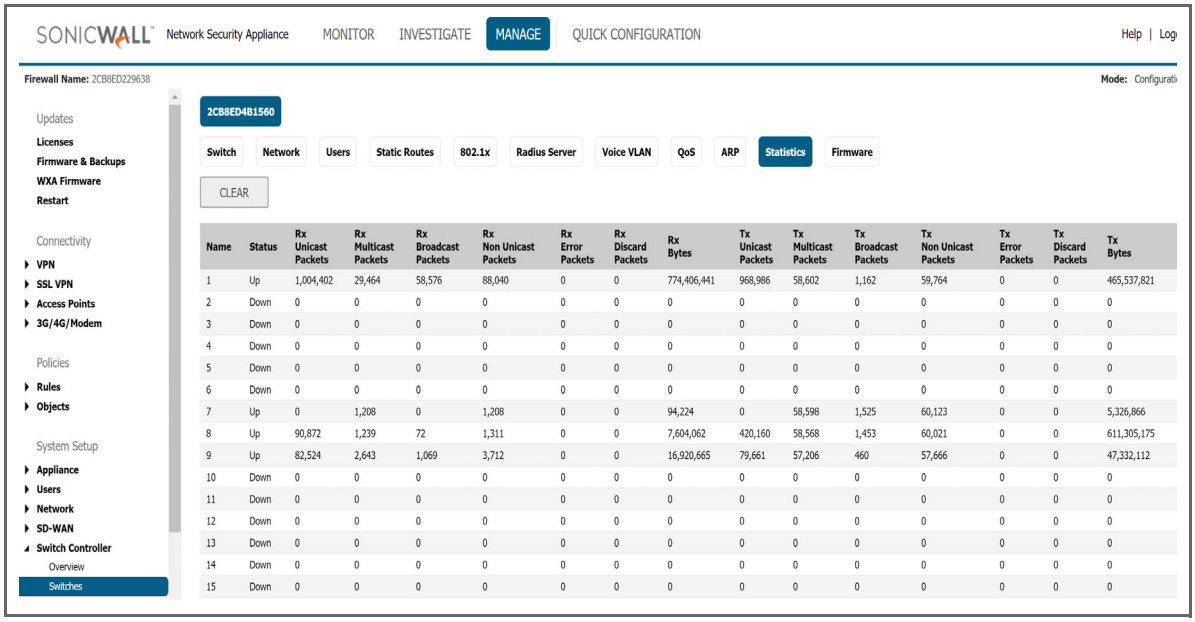
To Check Dynamic MAC Address Learning:

The dynamic MAC address table lists currently learned MAC addresses and accompanying Port and VLAN IDs. The defined **MAC Aging time** deterimines how current this information is. This table provides details on the LAN supported by the Switch.

Checking Port Statistics

The statistics table for a Switch can also be reached through **Switch Controller > Switches > Statistics**.

This table presents details on port-by-port performance.



Name	Status	Rx Unicast Packets	Rx Multicast Packets	Rx Broadcast Packets	Rx Non Unicast Packets	Rx Error Packets	Rx Discard Packets	Rx Bytes	Tx Unicast Packets	Tx Multicast Packets	Tx Broadcast Packets	Tx Non Unicast Packets	Tx Error Packets	Tx Discard Packets	Tx Bytes
1	Up	1,004,402	29,464	58,576	88,040	0	0	774,406,441	968,986	58,602	1,162	59,764	0	0	465,537,821
2	Down	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	Down	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	Down	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	Down	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	Down	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7	Up	0	1,208	0	1,208	0	0	94,224	0	58,598	1,525	60,123	0	0	5,326,866
8	Up	90,872	1,239	72	1,311	0	0	7,604,062	420,160	58,568	1,453	60,021	0	0	611,305,175
9	Up	82,524	2,643	1,069	3,712	0	0	16,920,665	79,661	57,206	460	57,666	0	0	47,332,112
10	Down	0	0	0	0	0	0	0	0	0	0	0	0	0	0
11	Down	0	0	0	0	0	0	0	0	0	0	0	0	0	0
12	Down	0	0	0	0	0	0	0	0	0	0	0	0	0	0
13	Down	0	0	0	0	0	0	0	0	0	0	0	0	0	0
14	Down	0	0	0	0	0	0	0	0	0	0	0	0	0	0
15	Down	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Setting Spanning Tree Protocol

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

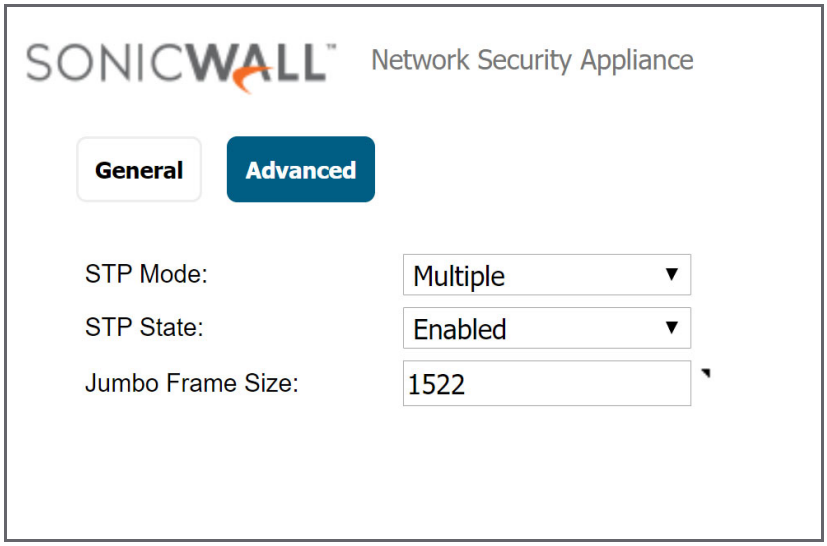
Multiple Spanning Tree Protocol (MSTP) defined in IEEE 802.1s, enables multiple VLANs to be mapped to reduce the number of spanning-tree instances needed to support a large number of VLANs. If there is only one VLAN in the network, a single STP works appropriately.

If the network contains more than one VLAN however, the logical network configured by a single STP would work, but it becomes more efficent 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.

To set Spanning Tree Protocol Configuration:

1 Navigate to **MANAGE | Switch Controller > Overview** and then click on the 3 dot menu to at the right end of the Switch graphic. When the menu appears, click on **Edit**. Then click on **Advanced**. The dialog box will appear:



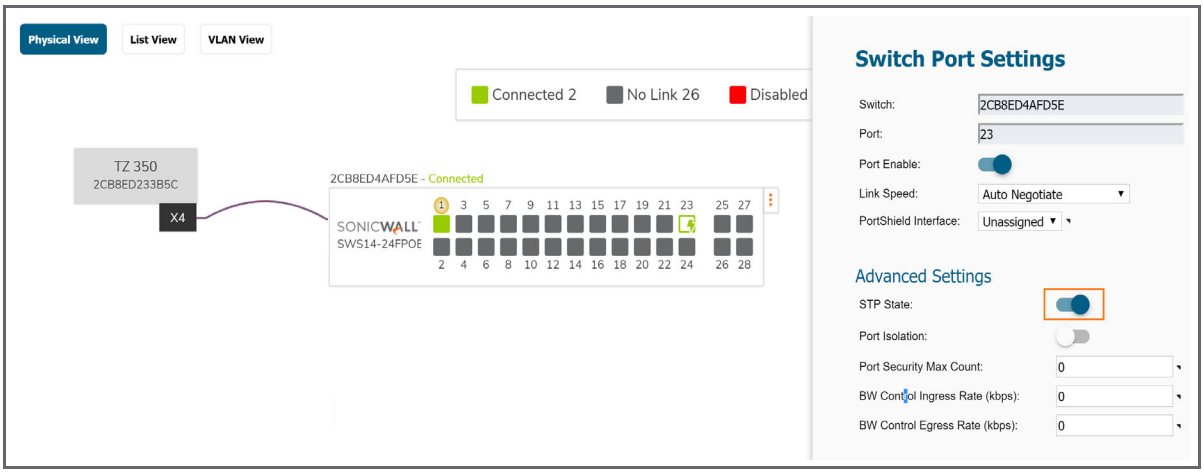
2 For the two STP entries:

- **STP Mode** — Sets the protocol version to Multiple (MSTP) or Rapid (RSTP).
- **STP State** — Enables or Disables spanning tree operation on the Switch.

3 Click on **OK**.

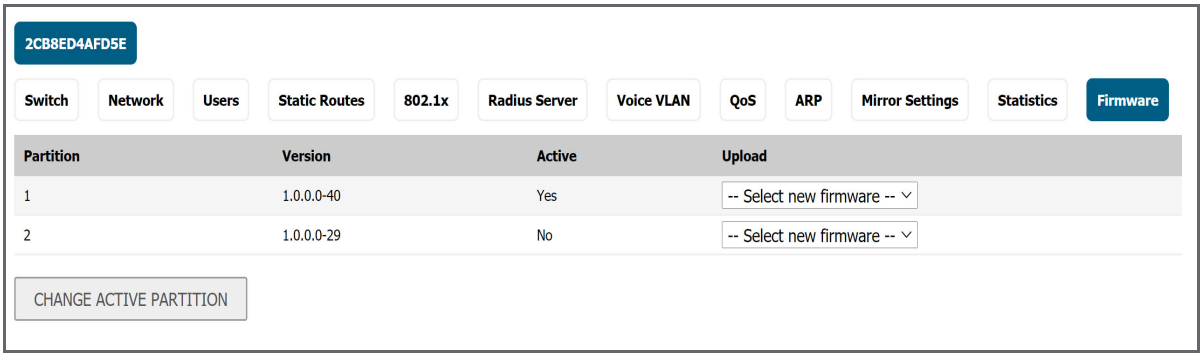
To Enable/Disable STP from Physical View:

Simply go to **MANAGE | Switch Controller > Overview** and click on the port. When the sideband display appears scroll to STP state as shown below.



Changing Firmware

Switches > Firmware enables uploading of new firmware and changing of partitions or firmware slots to boot from.



6

Configuring from Local UI

To access the Switch local user interface, refer to Connecting over Ethernet on page 15.

For a detailed description of the the Switch Local User Interface, see Switch documentaion *on* the SonicWall documentaition portal — https://www.sonicwall.com/support/technical-documentation/?language=English

7

Configuring Basic Topologies

About Topologies

Basic topologies for an SWS12- or SWS14-series Switch include:

- Common uplink configuration
- Dedicated uplink configuration
- Hybrid configuration with common and dedicated uplink(s)
- Isolated links configuration for management and data traffic
- HA and PortShield configurations with dedicated uplink(s)
- HA and PortShield configurations with common uplink(s)
- VLAN(s) with dedicated uplink(s) configuration
- Dedicated Uplinks with SonicWall Access Points

About Links

A common link carries data and management traffic. Common links carry all PortShield traffic and all the PortShield groups.

A dedicated link can carry only one PortShield group, and that group must be portshielded to the dedicated port on the SonicWall firewall.

An isolated link can carry management traffic OR data traffic, but not both at the same time. Isolated links usually have separate connections between the firewall and the Switches for management traffic and data traffic.

About Uplink Interfaces

Uplink interfaces can be viewed as “trunk” ports set up to carry tagged/untagged traffic. When a Switch is added with firewall Uplink and Switch options, the port on the firewall configured as the firewall uplink and the port on the Switch configured as the Switch uplink are set up automatically to receive/send tagged traffic for all IDV VLANs. The IDV VLAN of the tagged traffic allows the firmware to derive the PortShield host interface for the traffic.

NOTE: *IDV* — Interface Disambiguation via VLAN – The reconfiguring of ports, portshielded to firewall interfaces, on the Switch as access ports of the VLAN corresponding to the PortShield VLAN.

Criteria for Configuring an Uplink Interface

- The interface must be a physical interface; virtual interfaces are not allowed.
- The interface must connect a firewall and a Switch.
- The interface cannot be a PortShield host (some other firewall interface cannot be portshielded to it) or a PortShield group member (cannot be portshielded to another firewall interface).
- The interface cannot be a bridge primary or bridge secondary interface.
- The Switch side of the uplink interface cannot have any children (it cannot be a parent interface for children interfaces). The Firewall uplink interface can have child/ sub interfaces.

Connecting the Switch Management Port to a Firewall

The interface connected to the management port of the Switch must have an IP address from the same subnet as the Switch. For example, if the management connection between the Switch and the firewall is through X2, then X2 must have an IP address from the same subnet, such as `192.168.168.10`. The default Switch IP address is `192.168.168.169`.

All port-based configuration operations are disabled on the Switch port designated as the Switch management and Switch uplink ports. This action ensures that configuration operations on these critical ports do not lead to Switch-reachability issues jeopardizing the integration solution.

Configuring a Common Uplink

SonicWall Switches can be managed by the firewall, thereby providing a unified management option. The common uplink configuration allows a single link between the firewall and the Switch to be designated as the uplink that carries all PortShield traffic, both management and data. Both the firewall and Switch ports are configured as trunk ports for carrying tagged traffic for VLANs corresponding to all the firewall interfaces. The VLAN tag of the traffic is used to associate the traffic to the PortShield group to which it belongs through the application of IDV (Interface Disambiguation via VLAN).

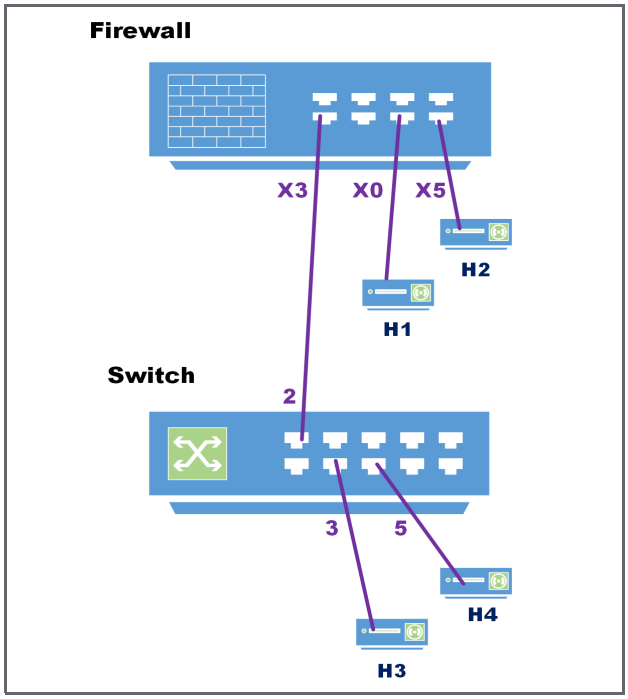
The advantage of such a deployment option is to separate a set of firewall/Switch ports that are not being used for management traffic. The disadvantage is that a high amount of data traffic can penalize forwarding of management traffic as the same link is shared for both types of traffic.

The diagram, Common Uplink Topology, shows a typical integration topology of a firewall with a SonicWall Switch:

- The firewall uplink interface is X3.
- The Switch uplink interface is 2.

This uplink between X3 on the firewall and port 2 on the Switch is a common link set up to carry PortShield traffic between H1 / H2 and H3 / H4. The uplink is also the one on which the Switch is managed by the firewall. In such a configuration, X3 is configured in the same subnet as the IP of the Switch (see Connecting the Switch Management Port to a Firewall on page 57). Also, X3 is configured as the firewall uplink.

Common Uplink Topology



To configure a common link:

A firewall-to-Switch common link can be made by adding the Switch through Zero-Touch or configuring it manually.

- Before Adding a Switch on page 23
- Adding a Switch to a Firewall Manually on page 27

Both of these options help configure a common link by selecting the proper interface.

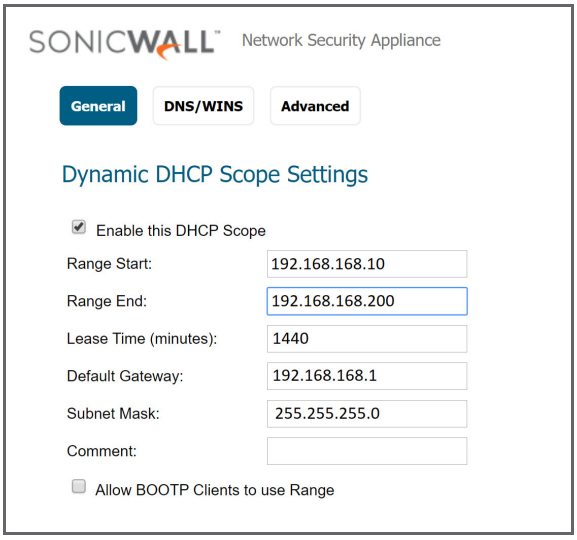
In both cases, to create a management link, DHCP on the firewall must be setup to address the IP subnet including the default IP address of the Switch management interface. For details, refer to Connecting the Switch Management Port to a Firewall on page 57.

1 Set up the firewall port X3 with the same IP subnet as the Switch management port.

   a Navigate to **Network > DHCP Server** and click on the Configure icon (pencil) for the X3 interface.

   b Setup the DHCP lease to cover the Switch management IP address.
   The default IP address for the Switch management interface is 192.168.168.169 so the range of DHCP scope settings shown in Setting DHCP Scope includes this.

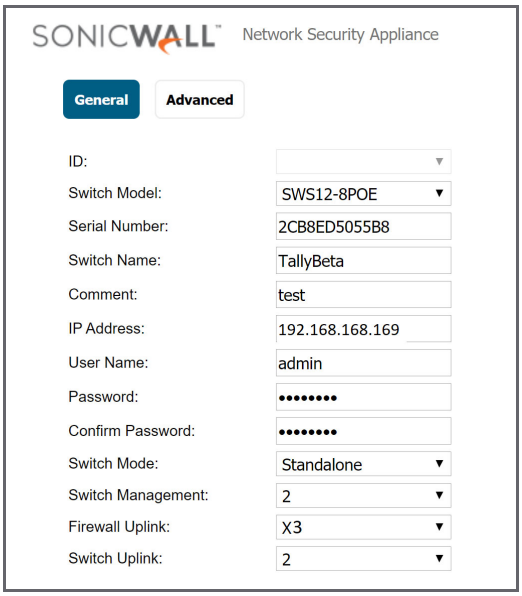
Setting DHCP Scope



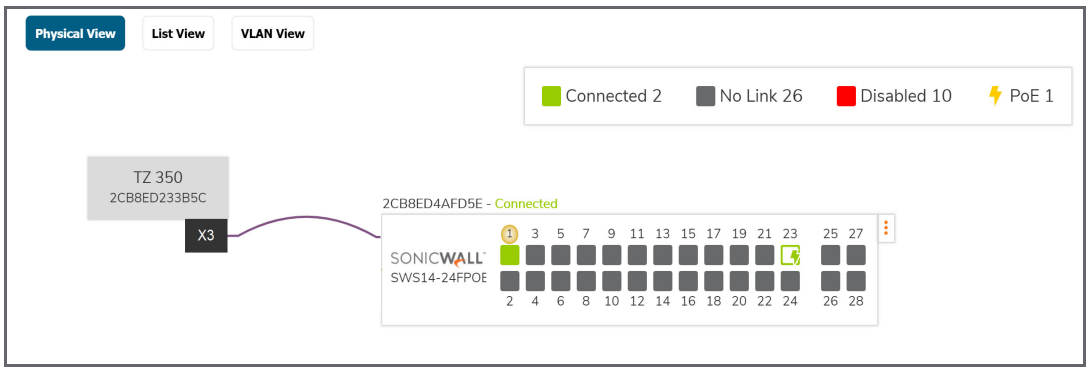
2 Add the Switch to the network as described by navigating to **MANAGE > Switch Controller > Overview**. The **Add Switch** button will appear in **Physical View**, **List View**, and **VLAN View.**

   a Click on **Add Switch**.

   b When the dialog box appears, set the **Switch Uplink** and **Switch Management** ports to 2 and the Firewall Uplink to X3.



3 In **Overview > Physical View**, a single link should now appear between the firewall and the Switch.



Configuring a Dedicated Uplink

This configuration allows a given link between the firewall and the Switch to be designated as the dedicated uplink set up to carry PortShield traffic corresponding to the connected firewall interface. The firewall and Switch ports are configured in trunk mode for the VLAN corresponding to the PortShield VLAN of the firewall interface.

This configuration can be used in deployments where a dedicated 1G link is needed for a particular firewall interface. Cases where this configuration is necessary:

- VLANs are used; for example, another Switch behind the Switch.
- There is a large volume of traffic and there needs to be a separate uplink for this traffic.

The risk associated with such a configuration is using up interfaces on the firewall fairly soon.

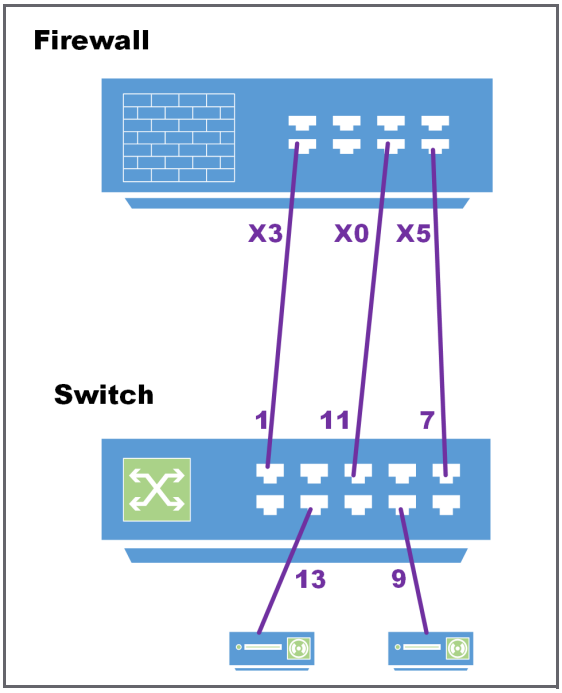
NOTE: In this example, there is no common uplink to carry the PortShield traffic for the rest of the firewall interfaces (excluding X0 and X5 for which dedicated links are set up).

IMPORTANT: For dedicated uplinks to work, the physical link must be connected before being configured.

Dedicated Uplink Topology shows a dedicated uplink setup of a firewall with a Switch. There are two dedicated uplinks in this scenario:

- The uplink between X3 on the firewall and port 1 on the SonicWall Switch is used to manage the Switch. In this configuration, X3 is configured in the same subnet as the IP of the Switch.
- In addition, there are two dedicated uplinks:
  - The uplink between X0 on the firewall and port 11 on the Switch is a dedicated link to carry all PortShield traffic for X0.
  - The uplink between X5 on the firewall and port 7 on the Switch is a dedicated link to carry all PortShield traffic for X5.

Dedicated Uplink Topology



You can configure a dedicated uplink with or without setting up the common uplink to carry all PortShield traffic for the different firewall interfaces. In both cases, the common uplink is used to manage the Switch.

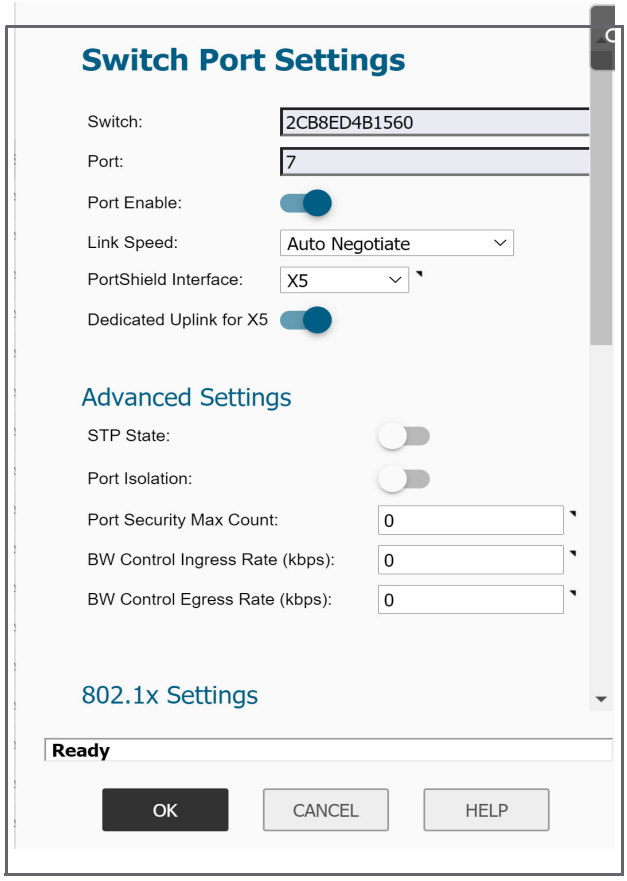
To configure a dedicated uplink topology without an common uplink:

1 Set up the Switch as described in Adding a Switch to a Firewall Manually on page 27.

2 To set up a link as a dedicated uplink without management traffic, in the Add Switch diaglog box set **Firewall Uplink** and **Switch Uplink** to **None**.

3 In the **Switch Controller > Overview** > **Physical View** or **List View**, enable the Switch port for the dedicated link.

4 Once the the Switch port is enabled, go to **Switch Port Settings** as shown below. Set portshields to support dedicated uplinks. In the dialog below, port 7 is portshielded to X5.



5 Click **OK**.

Configuring a Hybrid System with Common and Dedicated Uplink(s)

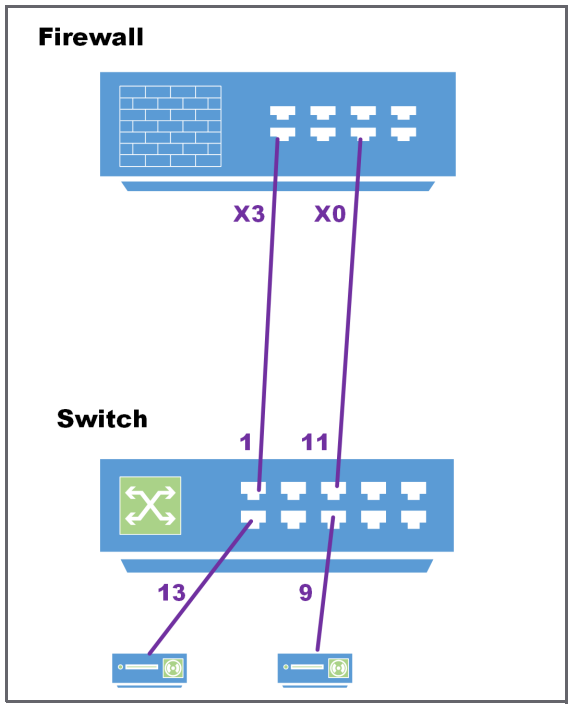
This configuration allows a combination of common and dedicated uplinks to be set up between the firewall and the Switch. The dedicated uplinks are used to carry PortShield traffic corresponding to the connected firewall interface. The common uplink is used to carry PortShield traffic for the remaining firewall interfaces (with no dedicated uplinks).

Hybrid Link Topology shows a hybrid uplink integration topology of a SonicWall firewall with a SonicWall Switch:

- The dedicated uplink between X0 on the firewall and port 11 on the Switch is set up to carry PortShield traffic for X0.
- The common link between X3 on the firewall and port 1 on the Switch carries PortShield traffic for firewall interfaces other than X0.
- Ports X0 and 11 for the dedicated uplink are trunk mode ports for the VLAN corresponding to X0. Ports X3 and 1 for the common uplink are trunk ports, and VLANs corresponding to all firewall interfaces, except X0, are added as members to this trunk to facilitate carrying the PortShield VLAN-tagged traffic.

In this configuration, the link between X3 and 1 is also used to carry management traffic between the firewall and the Switch.

Hybrid Link Topology



Setting up a hybrid configuration is done in two steps:

1 Configure a common uplink.

2 Configure the dedicated uplink.

To set up a hybrid configuration with common and dedicated uplinks:

1 Set up the Switch as described in Adding a Switch to a Firewall Manually on page 27.

2 Configure the uplink as described in Configuring a Dedicated Uplink on page 61.

Configuring Isolated Links for Management and Data Uplinks

This configuration allows separate links between the firewall and Switches to carry management traffic and data traffic. With a common link, the management traffic and data traffic run in the same uplink. If data traffic is congested, so is management traffic, which results in a delay in forwarding management traffic. If data traffic is congested, consider configuring separate links for management traffic and data traffic. Although similar to a common link configuration, the isolated management/data configuration runs separate uplinks for management traffic and data traffic. This configuration ensures that even with a high amount of data traffic, management traffic to the Switch is forwarded without being delayed.

IMPORTANT: The management port cannot be portshielded.

Isolated Link Topology shows an isolated link setup of a firewall with a Switch:

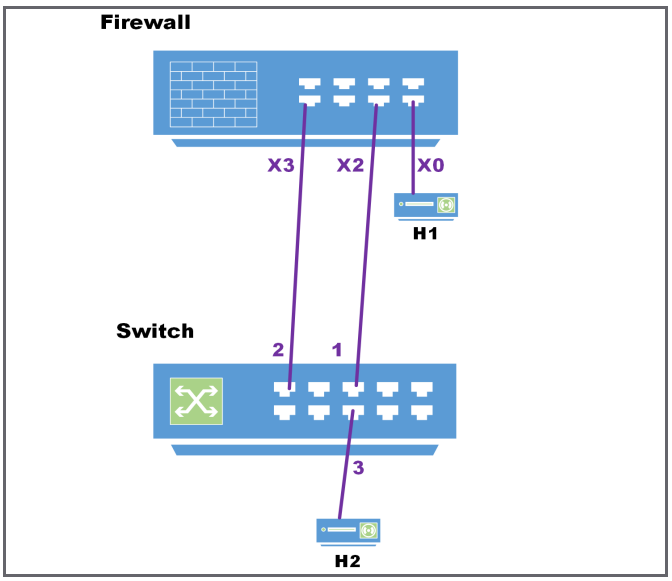
- The link between X2 on the firewall and port 1 on the Switch carries management traffic to the Switch. In such a configuration, X2 is configured in the same subnet as the IP of the SonicWall Switch.

  NOTE: When the Switch is configured with Isolated uplink the switch IP should be configured at a Static IP address.

- The link between X3 on the firewall and port 2 on the Switch is the uplink set up to carry all data traffic except managment traffic.
- The switch interfaces cannot be portshielded to X3 directly, but can be portshielded to VLAN interfaces on X3.
- Port 1 is configured as the Switch management port.
- Port 2 of the switch acts as a data uplink.
- Port 3 of the switch can be portshielded to one of the VLAN interfaces on X3.

  IMPORTANT: To change the Reserved VLAN range on the firewall, do so before adding the SonicWall Switch. If the Reserved VLAN range changes after connecting the Switch, then the Switch must be removed and re-added.

Isolated Link Topology



To set up isolated links for management and data traffic:

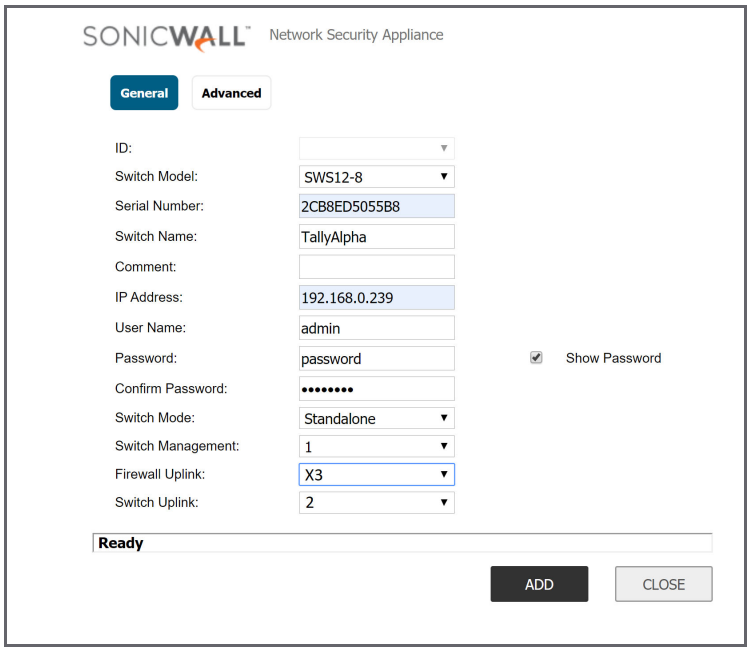
1 Connect Switch port 1 to X2 of the firewall which is configured in same subnet as the Management IP address of the Switch.

2 Connect Switch port 2 to X3 of the firewall.

3 Navigate to **Switch Controller > Overview** and click on the **Add Switch** button.

4 When a dialog box appears, enter the data requested and the following settings:

- **Switch Management** = 1
- **Firewall Uplink** = X3
- **Switch Uplink** = 2



5 When complete with configuration click on **ADD**.

Configuring HA and PortShields With Dedicated Uplink(s)

IMPORTANT: To use the Switch with HA, you must first create an HA pair, and then add the Switch.

NOTE: Switches cannot be added to HA pairs with Zero-Touch. See Adding a Switch to a Firewall Manually on page 27.

There are two ways to configure HA units with dedicated uplinks:

- Configuring HA Using One Switch Management Port on page 66
- Configuring HA Using Two Switch Management Ports on page 68

Configuring HA Using One Switch Management Port

In this configuration with PortShield functionality in HA mode, firewall interfaces that serve as PortShield hosts should be connected to the Switch on active and standby units. The PortShield members should also be connected to ports on the Switch. The link between the firewall interface serving as the PortShield host and the Switch is set up as a dedicated uplink.

HA Pair Using One Switch Management Port Topology shows a firewall HA pair with a Switch and one dedicated link:

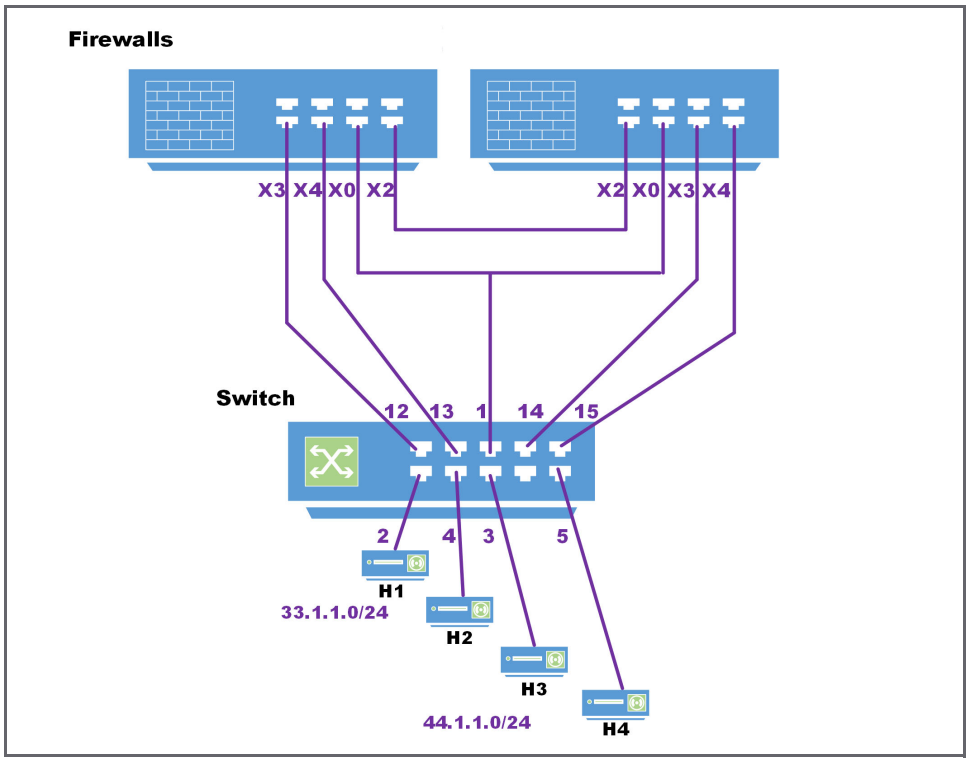
- The firewall interfaces, X3 and X4, on the primary unit are connected to ports 12 and 13 on the Switch.
- X3 and X4 are configured as PortShield hosts.
- Similarly, the firewall interfaces X3 and X4 on the secondary unit are connected to ports 14 and 15 on the Switch.
- Ports 12 and 14 on the Switch are portshielded to X3 with the dedicated uplink option enabled.
- Ports 13 and 15 on the Switch are portshielded to X4 with the dedicated uplink option enabled.
- Ports 2 and 4 are portshielded to X3.
- Ports 3 and 5 are portshielded to X4.

When the primary unit acts in active HA mode, traffic between H1 and X3 is carried over the dedicated link between X3 and 12 and traffic between H3 and X4 is carried over the dedicated link between X4 and 13.

When the secondary unit acts in active HA mode, traffic between H1 and X3 is carried over the dedicated link between X3 and 14, and traffic between H3 and X4 is carried over the dedicated link between X4 and 15.

The link between the firewall interface, X0, and port 1 on the switch, carries the management traffic to manage the Switch from the firewall. In such a configuration, X0 is configured to be in the same subnet as the Switch. Also, X0 on the primary as well as the secondary is ensured to be connected to port 1 of the Switch (for example, via a hub) so that when the secondary firewall becomes the active unit, the Switch can be managed via the link between the firewall interface X0 on the secondary and port 1 of the Switch. In such a configuration, when the Switch is provisioned, the Primary Switch Management and Secondary Switch Management are set to 1.

HA Pair Using One Switch Management Port Topology



To set up HA with one dedicated uplink:

> **NOTE:** Add Switches manually after creating the HA pair. Activating HA mode after Switches are added will not work.

1 Add the Switch and set up the data uplink.

2 Configure the options:

   a Select the management and uplinke interfaces from their respective drop-down menus and click on **Add**.

   > **NOTE:** The **Firewall Uplink** and **Switch Uplink** options are set the same in this configuration to support the redundant firewalls.

   b Set management uplinks for both Primary and Secondary firewalls to to Switch port 1 and firewall interface X0.

Configuring HA Using Two Switch Management Ports

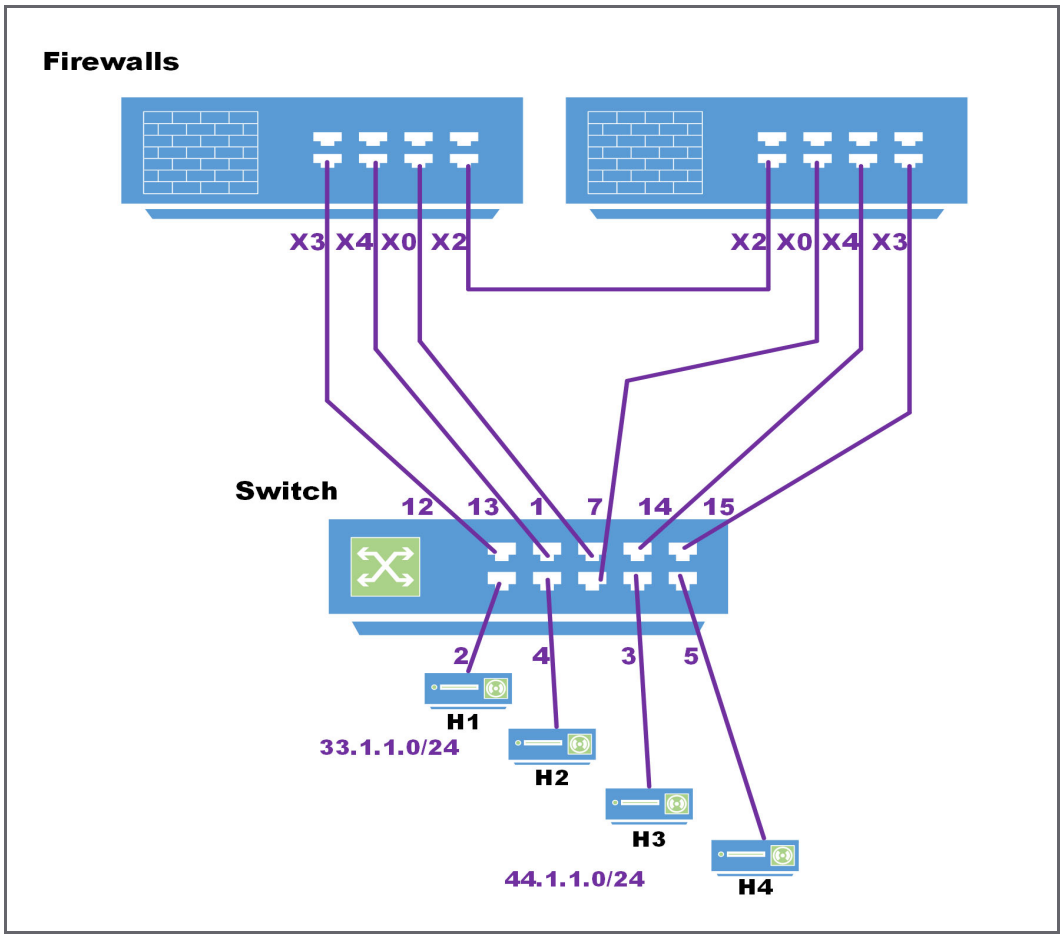
You can connect X0 of the primary and secondary firewalls directly to the ports on the Switch. In this case, two Switch ports are used on the Switch for management traffic.

HA Pair Using 2 Switch Management Ports Topology shows a firewall HA pair with a Switch and two dedicated links:

- X0 of the primary unit is connected to port 1.
- X0 of the secondary unit is connected to port 7

When the primary firewall is active, the link between X0 of the primary and port 1 of the Switch carry the management traffic. When the secondary firewall is active, the link between X0 of the secondary and port 7 of the Switch is used by the firewall to manage the Switch.

HA Pair Using 2 Switch Management Ports Topology



To set up HA with two Switch management ports:

NOTE: Add Switches manually after creating the HA pair. Activating HA mode after Switches are added will not work.

1 Add the Switch and set up the data uplink.

2 Configure the options:

a Select the **Add Switch** option from the Switch Controller > Overview pages for the two Switches. Define one as Primary and the other as Secondary.

> **NOTE:** The **Firewall Uplink** and **Switch Uplink** options are not relevant for a firewall operating in HA mode. The primary **Firewall Uplink** option and both the primary and secondary **Switch Uplink** options are set to **None**.

b Set **Firewall** and **Switch Uplink** options to None.

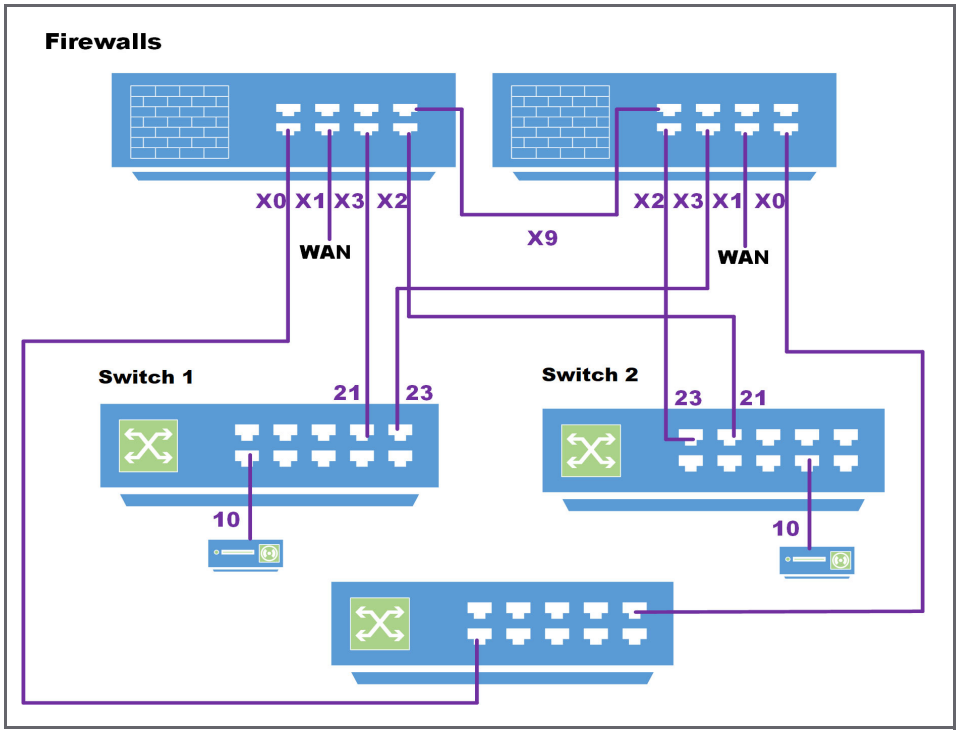
3 Click **ADD**.

Configuring HA and PortShield With a Common Uplink

In this configuration with PortShield functionality in HA mode, a link between the active/standby firewalls and the Switch serves as a common uplink to carry all the portshielded traffic. Firewall interfaces that serve as PortShield hosts are connected to a separate Switch (not necessarily a Switch) and not the same Switch connected to the active and standby units. This other Switch avoids the looping of packets for the same PortShield VLAN. The PortShield members can be connected to ports on the Switch that is controlled by the active/standby firewalls.

HA Pair Using a Common Switch Topology shows a firewall pair and two Switches. The link between X3 and Switch 1 is set up as a common uplink. Similarly, the link between X2 and Switch 2 is set up as a common uplink. The PortShield hosts X0 are connected to a different Switch (which could be a SonicWall Switch or any other vendor's Switch) to avoid looping of packets. Ports 10 on both Switch 1 and Switch 2 are portshielded to X0, and hosts connected to Ports 10 on both Switches can communicate using the common uplink.

HA Pair Using a Common Switch Topology



To set up HA with a common uplink:

> **NOTE:** Add Switches manually after creating the HA pair. Activating HA mode after Switches are added will not work.

1 Add the Switch and set up the data uplink.

2 On the **Network > Interfaces** page, configure these interfaces for both firewalls:

X0	LAN/PortShield host
X1	WAN

X2 Firewall uplink on the firewall for Switch 2

X3 Firewall uplink on the firewall for Switch 1

3 Configure common uplinks except for these ports:

Switch 1 Interfaces:	10	Host-facing interface portshielded to X0
	21	Switch uplink for the primary firewall
	23	Switch uplink for the secondary firewall
Switch 2 Interfaces:	10	Host-facing interface portshielded to X0
	21	Switch uplink for the primary firewall
	23	Switch uplink for the secondary firewall

Configuring VLAN(s) With Dedicated Uplink(s)

Topics:

Prerequisites for VLAN Support

- Support for VLANs is available on dedicated and common uplinks. For example, VLANs can be configured under firewall interfaces configured as a dedicated uplink. VLANs also can be configured under the firewall interface provisioned as the common uplink for the Switch.
- Overlapping VLANs cannot exist under appliance interfaces configured as dedicated uplinks to the same Switch because VLAN space on the Switch is global. For example, if X3 and X5 are configured for dedicated uplinks to the same Switch, VLAN 100 cannot be present under both X3 and X5. Such a configuration is rejected. If X3 and X5 are dedicated uplinks to different Switches, however, then such a configuration is accepted.
- Overlapping VLANs cannot exist under common uplink interfaces. For example, if X3 is set up as a common uplink to a Switch and VLAN 100 exists under X3, another interface that is configured as a common uplink to a second Switch, for example, X4 cannot have a VLAN 100 sub-interface.
- PortShielding of Switch interfaces to common uplink interfaces without selecting any VLANs for access/trunk configuration is not supported.

  IMPORTANT: To change the Reserved VLAN range on the firewall, do so before adding the SonicWall Switch. If the Reserved VLAN range changes after connecting the Switch, then the Switch must be removed and re-added.

Configuring a Dedicated Uplink for VLANs

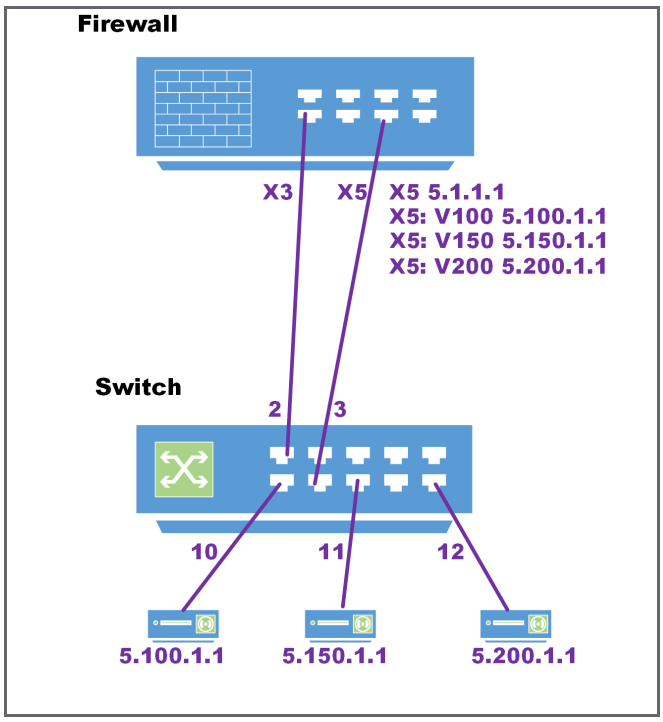
Topics:

Dedicated Uplink for VLAN Topology

In a dedicated uplink configuration, a given link between the firewall and the Switch designated as the dedicated uplink is set up to carry traffic for all VLANs configured under the firewall interface plus PortShield traffic corresponding to the firewall interface.

NOTE: VLANs must first be setup at the firewall interface.

VLAN With Dedicated Uplink Topology



- The link between X3 and port 2 on the Switch is used by the firewall to manage the Switch.
- Interface X3 is configured to be in the same subnet as the IP of the Switch.

> **NOTE:** In this example, a common uplink is not required, hence, the Switch is provisioned with the **Firewall Uplink** and **Switch Uplink** options set to **None** and **Switch Management** set to **1**.

- There are three VLAN interfaces with VLAN tags 100, 150, and 200 configured under X5.
- The link between X5 on the firewall and port 3 on the Switch is a dedicated link set up to carry traffic tagged with VLANs 100, 150, and 200 and untagged traffic for X5.

Supporting such a topology, requires this configuration:

- Port 3 is portshielded to X5 with dedicated uplink option.
- Port 10 is portshielded to X5 and configured as a trunk to carry VLAN 100.
- Port 11 is portshielded to X5 and configured as a trunk to carry VLAN 150.
- Port 12 is portshielded to X5 and configured as an access to carry VLAN 200.

Configuring a Dedicated Uplink for a VLAN

Support for VLAN(s) is achieved in a multi-step configuration process:

1 Provision the Switch. The Switch can be provisioned with the:
   - Firewall uplink and Switch uplink set to **None** if support for VLAN(s) alone is needed.
   - Common uplink option if support is needed for an common trunk interface to carry PortShield traffic for other firewall interfaces along with VLAN(s) support.

2 Configure the dedicated link by:
   a Choosing a Switch port that is connected physically to the firewall interface.

b Portshielding the port to the firewall interface.

c Choosing the dedicated link option.

3 Select the Switch port on which VLAN(s) need to be enabled.

4 Portshield the Switch port to the firewall interface.

5 Configure the required VLAN(s) under the VLAN tab.

To configure a dedicated uplink for VLANs without a common uplink:

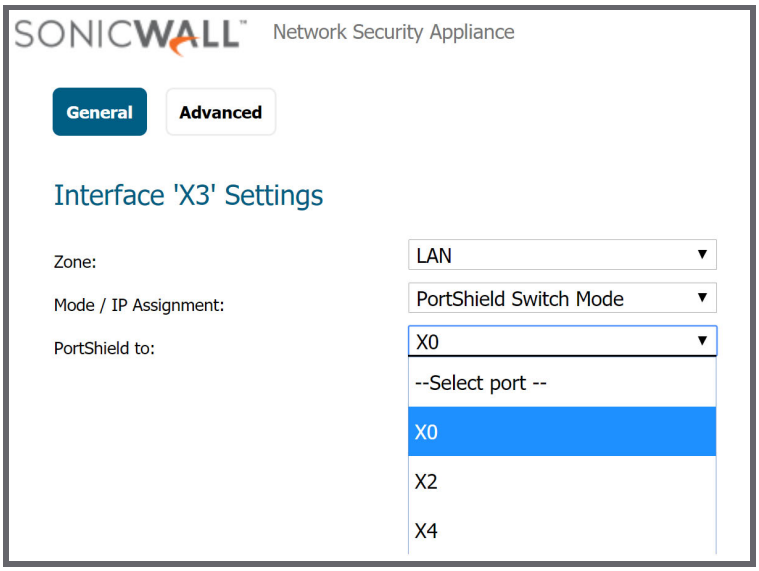
Refer to To configure a dedicated uplink topology without an common uplink: on page 62

1 Add the Switch and set up the data uplink as described in Adding a Switch to a Firewall Manually on page 27.

2 Configure the options as described in Configuring a Dedicated Uplink on page 61 except ensure to select the **Dedicated Uplink** option.

3 Navigate to **MANAGE > Network > Interfaces.**

4 In the **Interface Settings** table, click the **Configure** icon for the interface you want to configure. The **Edit Interface** dialog displays.



5 From **Zone**, select on a zone type option to which you want to map the interface. More options display.

NOTE: You can add PortShield interfaces only to **Trusted**, **Public**, and **Wireless** zones.

6 In the **Mode / IP Assignment** drop-down menu, select **PortShield Switch Mode**. The options change again.

7 From **PortShield to**, select the interface you want to map this port to. Only ports that match the zone you have selected are displayed.

8 Click **OK**.

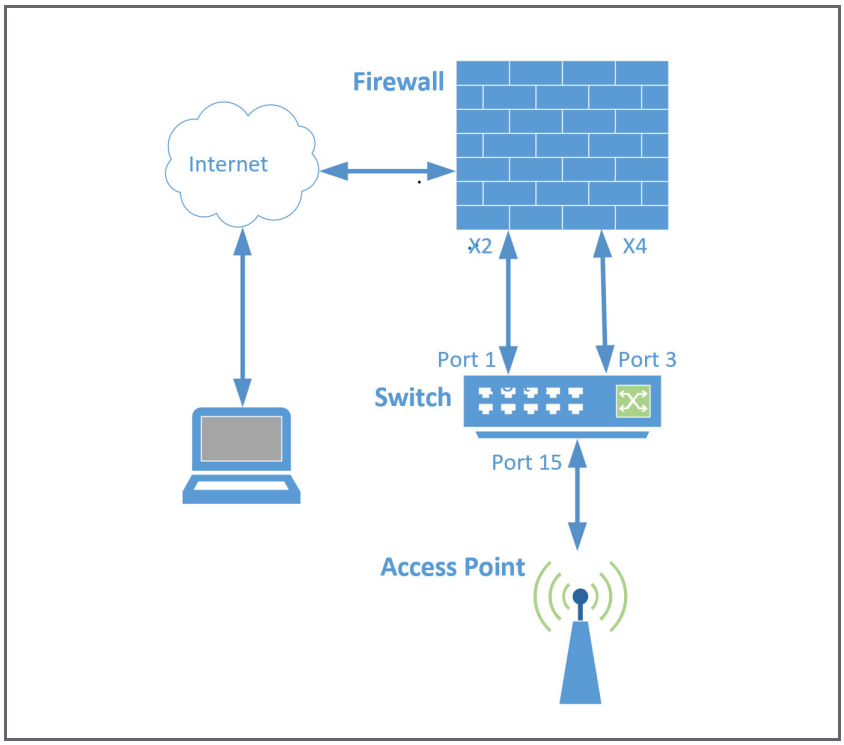
With this configuration, port 3 on the Switch carries tagged traffic for VLANs 100,150, and 200 and untagged traffic for IDV VLAN 6. Port 10 is a trunk port carrying tagged traffic for VLAN 100, Port 11 is a trunk port carrying tagged traffic for VLAN 150, and Port 12 is an access port carrying untagged traffic for VLAN 200. Ports 10, 11, and 12 are portshielded to X5 through the dedicated link between X5 and port 2.

Configuring a Dedicated Link for SonicWall Access Points

It is recommended that SonicWall access points be connected through dedicated links because access points carry several VLANS, and dedicated links pass through VLAN tunnels. The dedicated links act as trunks passing tagged traffic from the access point through the Switch to the firewall.

For non-SonicWall access points without particular management, the port in the firewall can be configured as **ANY** (LAN/WAN/DMZ, although usually LAN). In this case, the pair of ports between the firewall and the Switch must be configured as a dedicated link. Other ports on the Switch that are expected to connect to access points with RJ45 are portshielded to that dedicated port.

If the SonicWall access points are behind the firewall and are to be managed, the pair of ports on the firewall and the Switch must be configured as a dedicated link. The dedicated port on the firewall must be configured as WLAN. Other ports on the Switch that are expected to connect to SonicWall access points with RJ45 are portshielded to that dedicated port.



To configure a dedicated uplink for SonicWall Access Points:

1. Add the Switch as described with an isolated management link as described in Configuring Isolated Links for Management and Data Uplinks on page 64.
2. Connect access points to Switch as described in Connecting Access Points on page 45.
3. Configure the uplinks as described in Configuring a Dedicated Uplink for VLANs on page 72.
4. Ensure that all SonicWall access points are connected to Switch ports configured in the PortShield group of the dedicated link.

8

SonicWall Support

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

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

The Support Portal enables you to:

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

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

About This Document

Legend

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

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

IMPORTANT, NOTE, TIP, MOBILE, or VIDEO: An information icon indicates supporting information.

Switch Getting Started Guide
Released- July 2020
232-005294-00 Rev B