SonicOS 7

Switch Network

Administration Guide

SONICWALL®

Contents

1

Overview

Topics:

- Pre-Plan: Before Adding a Switch
- Physical View: Enabling the Switch
- List View: Setting Up Ports
- Overview: Checking Switch Details

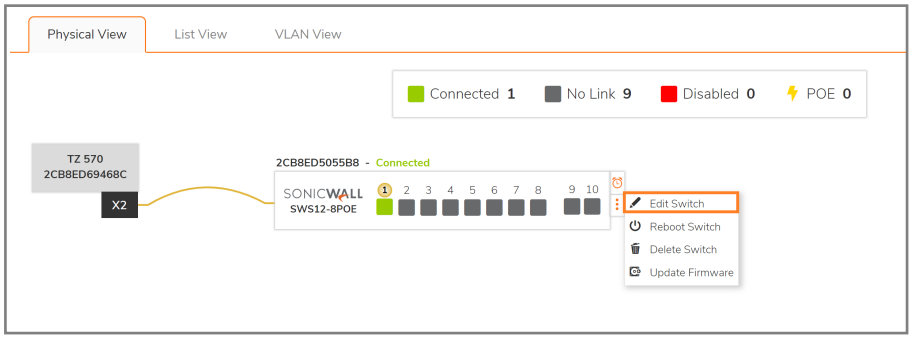
Before Adding a Switch

- Be sure to first register your Switch on MySonicWall.
- Consider the firewall/switch topology to be implemented. Refer to or the *Switch Getting Started Guide* available at https://www.sonicwall.com/support/technical-documentation
- 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 default management IP address. Refer to Connecting the Switch Management Port to a Firewall.
- The firewall interface linking to the Switch interface must have the **Enable Auto-Discovery of SonicWall Switches** option enabled. Edit the firewall interface and enable this option on the **Advanced** screen of the **Edit Interface** dialog.
- 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.
- If the management link between the switch and firewall is isolated from data traffic, the switch must configured at a static IP address.
- 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.

- 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.

Enabling the Switch

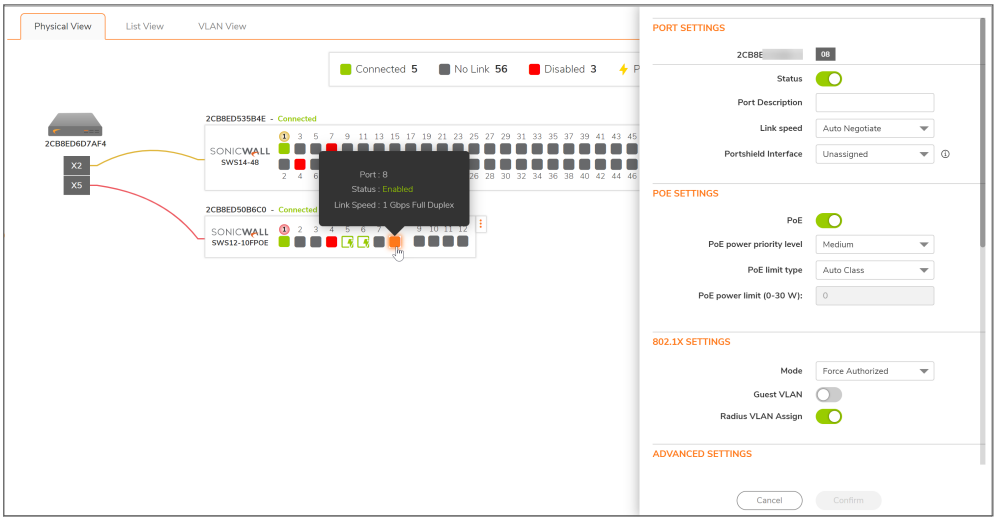
If the Switch is offline, navigate to **DEVICE > Switch Network > Overview** and click on 3 dot menu of the Switch which is off-line and then click on Edit Switch to bring up the Switch configuration dialog box. Check if the Switch configuration details are correct including: IP address, serial number, and Switch Management interface.



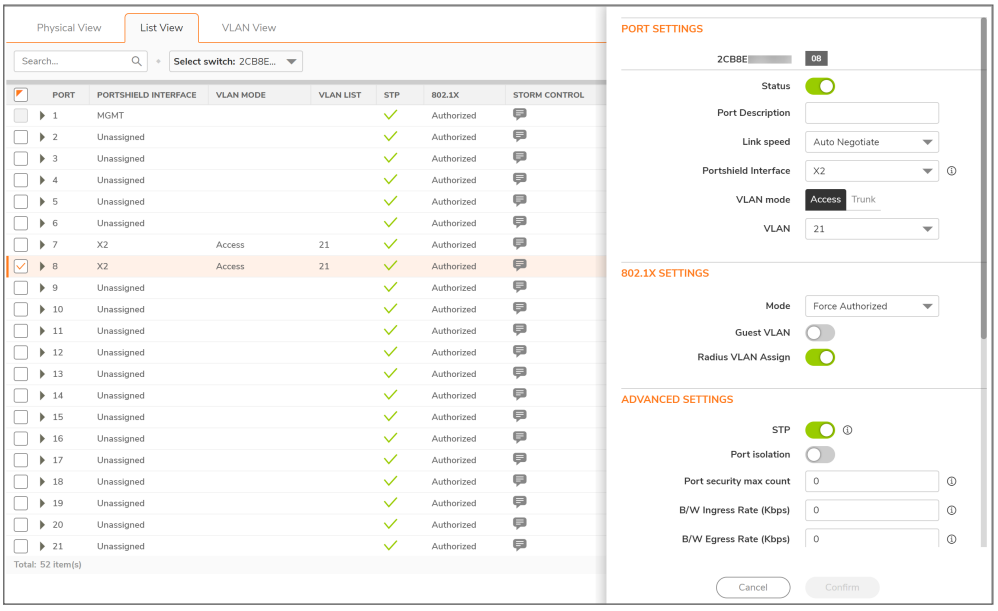
Setting Up Ports

To configure specific ports:

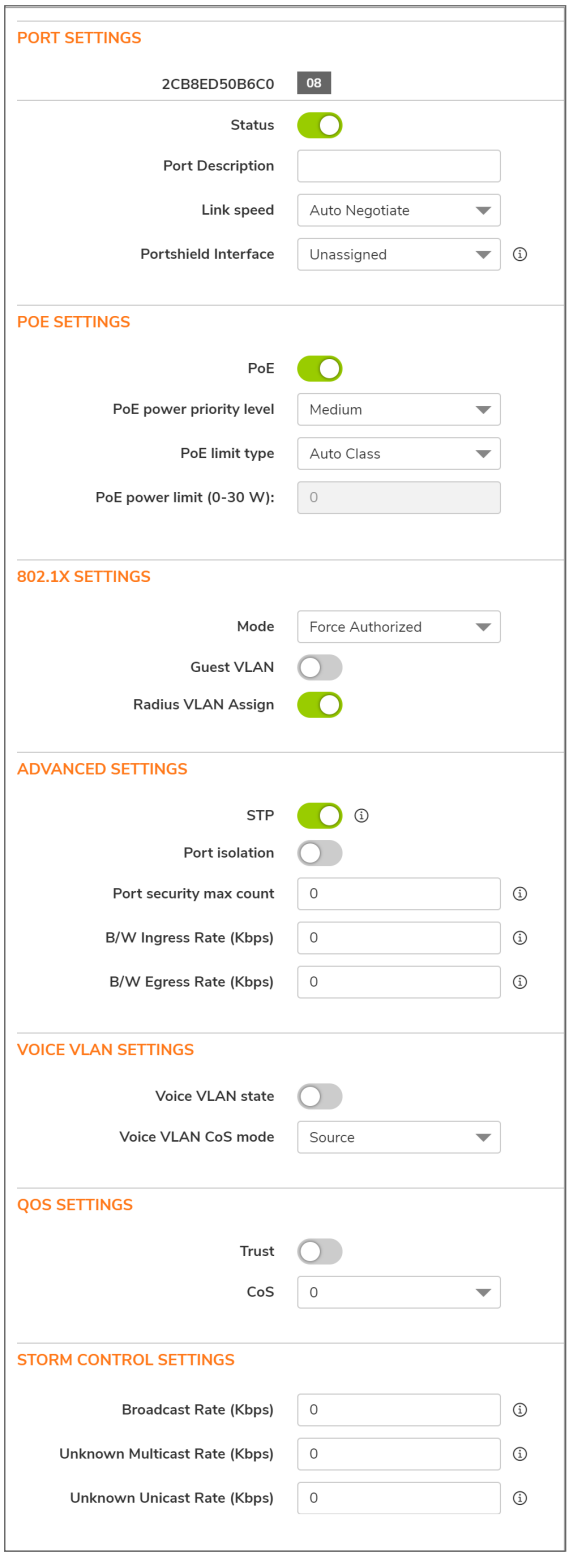
1. Navigate to **DEVICE > Switch Network > Overview**.
2. Do one of the following:
   - Click on the desired port in the **Physical View**.



   - Click on **List View**, select the desired port and then click the **Edit port** pencil icon.



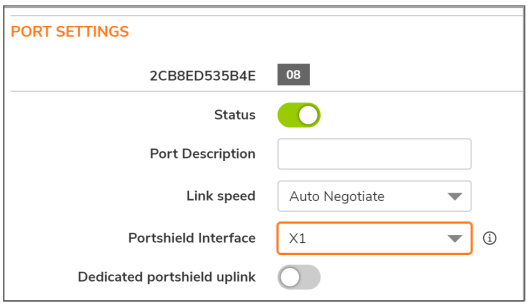
The port setup dialog for the specific port is displayed at the right of the screen.



3. Configure the following options for the port:

   PORT SETTINGS:

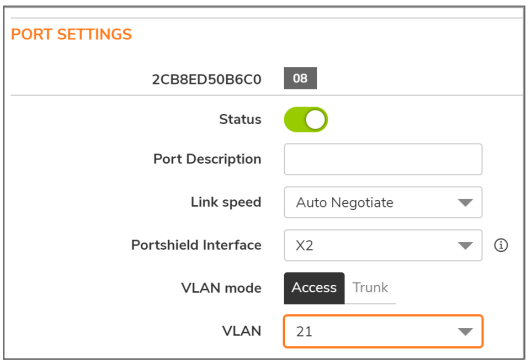
   - **Status** - Enable or disable by clicking the slider.
   - **Port Description** - Enter a description for this port.
   - **Link speed** - Default is **Auto Negotiate**. Selections also include **1000 Mbps Full Duplex**, **100 Mbps Full Duplex**, **100 Mbps Half Duplex**, **10 Mbps Full Duplex**, and **10 Mbps Half Duplex**.
   - **Portshield Interface** - Set this option to portshield the Switch port to a firewall interface. **Unassigned** by default. Selections include **Any** and **X0-Xn**.
   - **Dedicated portshield uplink** - This option appears if **PortShield Interface** is set to a firewall interface in any zone. Enable or disable by clicking the slider.



   - **VLAN Mode** - This option appears if **PortShield Interface** is set to an interface that is configured with a VLAN Sub-Interface. Default is **Access**.

     Select **Access** if the port transmits data on a specific VLAN.

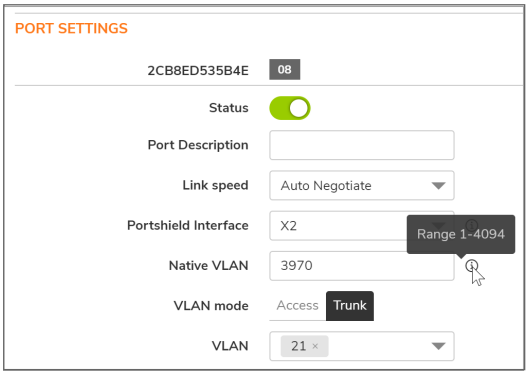
     Select **Trunk** for a port that can carry traffic for multiple VLANs. Port Trunking allows you to assign physical links to one logical link that functions as a single, higher-speed link, providing dramatically increased bandwidth. Use Port Trunking to bundle multiple connections and use the combined bandwidth as if it were a single larger “pipe”.



   - **Native VLAN** - The **Native VLAN** field appears when **Trunk** is selected for **VLAN mode**. Enter a number between 1 and 4094 in the **Native VLAN** field to assign the port's Native VLAN (Port VLAN ID).

     The Native VLAN option allows you to specify the Switch Port VLAN ID for traffic that does not carry a VLAN tag, which can help with SonicWave provisioning. A packet received on a given Switch port is assigned that port’s Native VLAN ID and is then forwarded to the port that corresponds to the packet’s destination address. If the Native VLAN of the port that received

the packet is different from the Native VLAN of the port that is to transmit the packet, the Switch will drop the packet.



- **VLAN** - The **VLAN** field appears in conjunction with **VLAN mode**. Select **Unassigned** or the number of a VLAN Sub-Interface associated with the firewall interface selected in **PortShield Interface**.

POE SETTINGS: Ports on a PoE enabled Switch can provide power to connected devices with Power over Ethernet.

- **PoE** - Enable or disable Power over Ethernet on this port by clicking the slider.
- **PoE power priority level** - Default is **Medium**. Selections also include **Critical**, **High** and **Low**. If several devices are connected and they exceed the Switch PoE capacity, the priority level determines which ports get powered.
- **PoE limit type** - Default is **Auto Class**, which uses a Device Discovery Protocol to discover attached devices and learn their classification. You can also select **User Defined**.
- **PoE power limit (0-30 W)** - This field is disabled if **Auto Class** is selected above. When **User Defined** is selected, enter a value between 0 and 30 for the port power limit in watts.

  Each SonicWall Switch model has a different total power budget:

  - SWS12-8POE - 55 Watts (supports IEEE802.3 af only)
  - SWS12-10FPOE - 130 Watts (IEEE802.3 af and at)
  - SWS14-24FPOE - 410 Watts (IEEE802.3 af and at)
  - SWS14-48FPOE - 730 Watts (IEEE802.3 af and at)

802.1X SETTINGS: IEEE 802.1X defines authentication controls for users or devices trying to connect to a port that accesses a LAN or WLAN.

- **Mode** - Default is **Force Authorized**. Selections also include **Auto** and **Force Unauthorized**.
- **Guest VLAN** - Enable or disable by clicking the slider. Default is disabled.
- **Radius VLAN Assign** - Enable or disable by clicking the slider. The user's identity based on their credentials or certificate can be confirmed by a RADIUS server. The RADIUS server takes care of the VLAN assignment for the Switch port.

ADVANCED SETTINGS:

- **STP** - Enable or disable by clicking the slider. Spanning Tree Protocol (STP) must be enabled on the Switch before configuring port STP settings. STP prevents loops when you have redundant paths in your network.
- **Port isolation** - Enable or disable by clicking the slider. Enable to isolate the port.

- **Port security max count** - Default is **0**, which disables port security. Range is 0-256. This is the maximum number of MAC addresses that can be learned on the port. Network security can be increased by limiting access on a specific port to users with specific MAC addresses.
- **B/W Ingress Rate (Kbps)** - Default is **0**, which disables ingress bandwidth control. Allowed values are multiples of 16 between 0 and 1,000,000.
- **B/W Egress Rate (Kbps)** - Default is **0**, which disables egress bandwidth control. Allowed values are multiples of 16 between 0 and 1,000,000.

VOICE VLAN SETTINGS:

- **Voice VLAN state** - Enable or disable by clicking the slider.
- **Voice VLAN CoS mode** - Default is **Source**. Selections for the Class of Service mode include **Source** or **All**.

QOS SETTINGS: Quality of Service allows certain traffic types, such as voice or video streaming, to be prioritized.

- **Trust** - Enable or disable Trust mode for incoming packets by clicking the slider. Enable this to classify traffic based on the IEEE 802.1p standard (using the 8 CoS priority tags).
- **CoS** - Select the CoS priority to set the priority for packets entering on this port. Default is **0**. Range is 0-7 for Class of Service tags, with 0 (background) and 1 (best effort) the lowest priority and 7 the highest priority in the traffic forwarding queue.

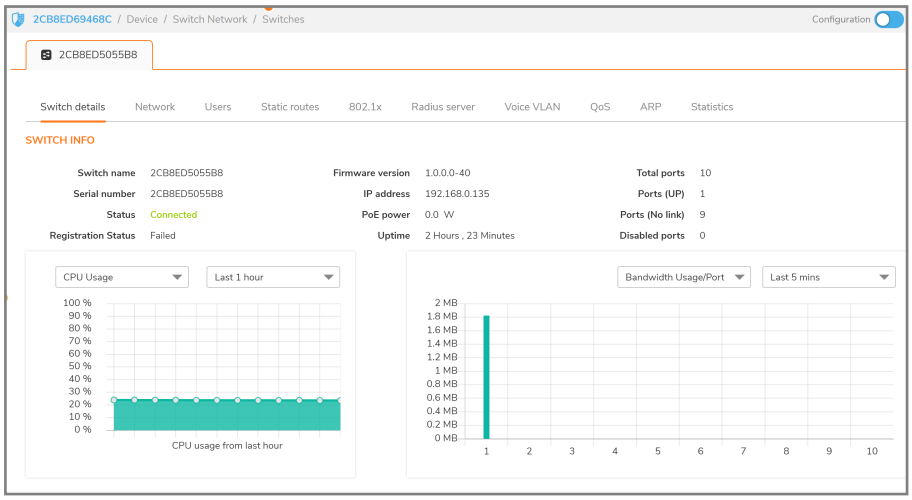
STORM CONTROL SETTINGS: Storm Control limits the amount of Broadcast, Unknown Multicast, and Unknown Unicast frames accepted and forwarded by the Switch. Storm Control can be enabled per port by defining the packet type and the rate of packet transmission. The Switch discards the frames when the rate exceeds the defined rate.

- **Broadcast Rate (Kbps)** - Default is **0**, which disables port broadcast. Allowed values are multiples of 16 between 0 and 1,000,000.
- **Unknown Multicast Rate (Kbps)** - Default is **0**, which disables port unknown multicast. Allowed values are multiples of 16 between 0 and 1,000,000.
- **Unknown Unicast Rate (Kbps)** - Default is **0**, which disables port unknown unicast. Allowed values are multiples of 16 between 0 and 1,000,000.

4. Click **Confirm** to save and apply your changes, or click **Cancel** to exit the edit dialog without saving.

Checking Switch Details

Navigate to **DEVICE > Switch Network > Switches > Switch Details** to get a summary on Switches connected to the firewall.



2

Managing from a Firewall

Topics:

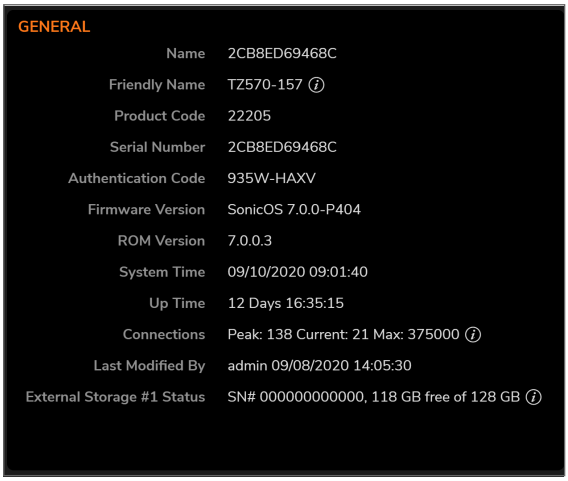
Adding a Switch to a Firewall with Zero-Touch

IMPORTANT: IMPORTANT: Please register your Switch before trying to add it to a firewall.

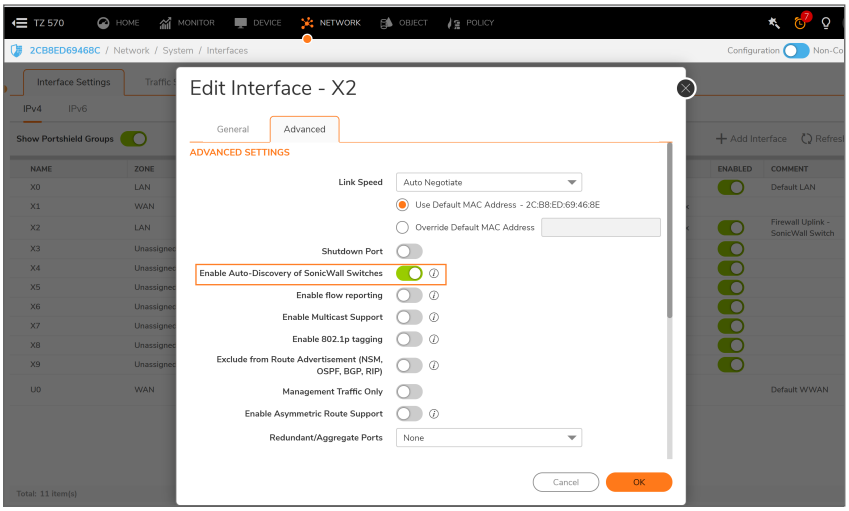
NOTE: In order for the firewall to sense the presence of the Switch, the firewall must be setup to add Switches with Zero-Touch.

To prepare the firewall:

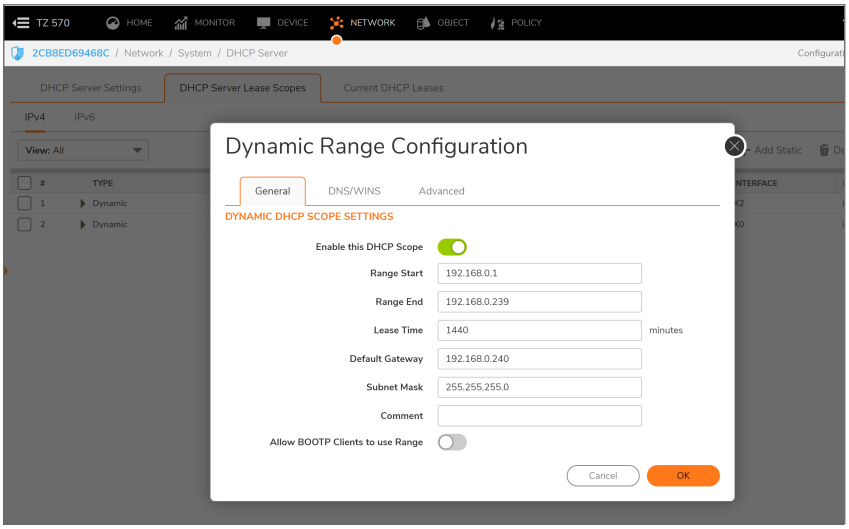
1. Navigate to **HOME > Dashboard > System > General** and check that the firewall **Firmware Version** is at the most recent level.



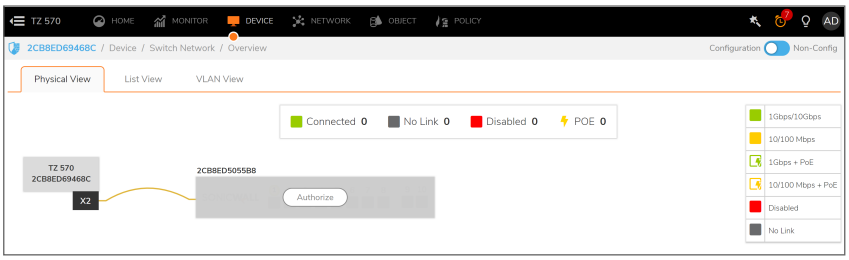
2. Select an interface on the firewall to connect to the Switch. Navigate to **NETWORK > System > Interface > Interface Settings** and select an interface, then click on the pencil icon.
3. In the **Edit Interface** dialog box, select the **Advanced** tab and enable the **Enable Auto-Discovery of SonicWall Switches** option, then click **OK**.
4. Connect the Switch to the selected firewall interface.



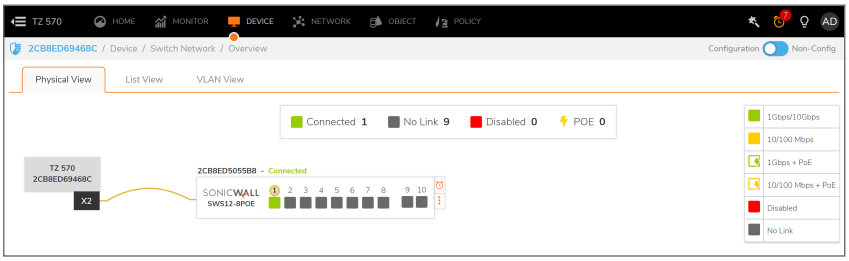
5. Navigate to **NETWORK > System > DHCP Server** and verify that the lease scope is correct for the switch attached to the selected interface.



6. Navigate to **DEVICE > Switch Network > Overview**. Click on **Authorize** button to add the Switch to firewall:



7. The network topology will now appear on the display at **Overview > Physical View**.



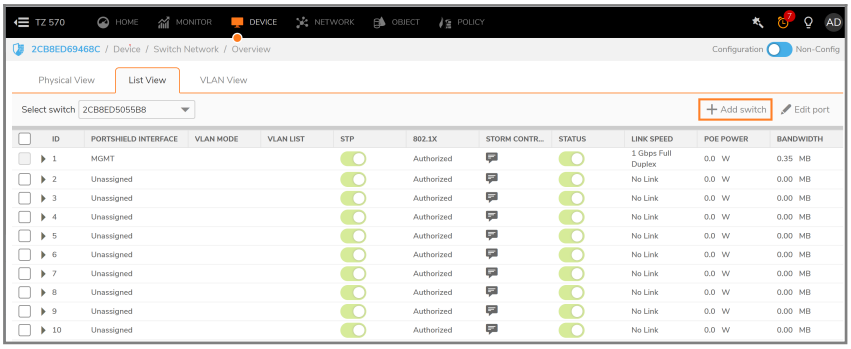
Adding a Switch to a Firewall Manually

1. Connect a port on the SonicWall Switch to an available port on the firewall. Use a CAT5e or CAT6 cable (that is, RJ45 to RJ45) when connecting to an RJ45 port, or use a fiber optic cable when connecting to a supported SFP interface.

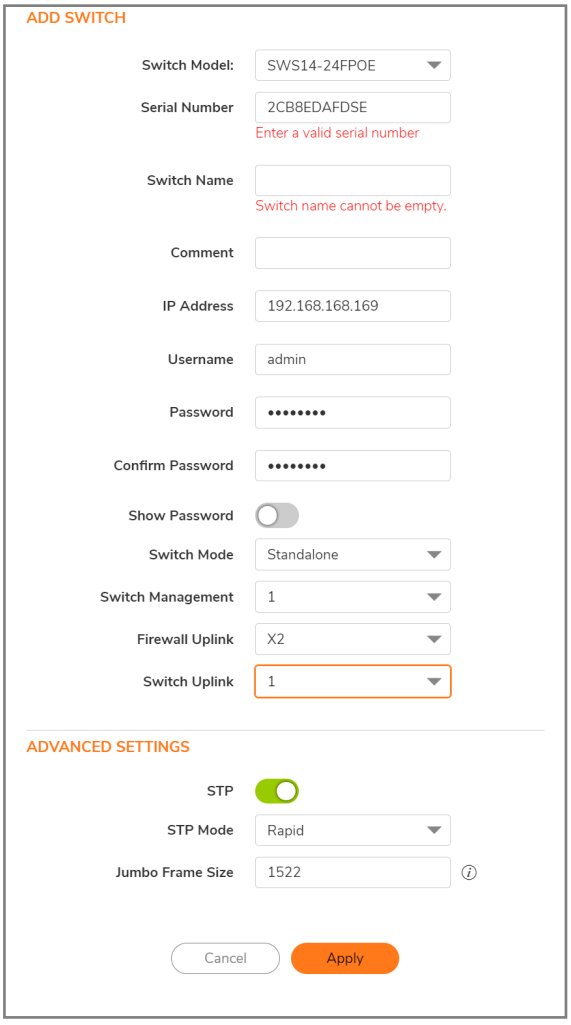
NOTE: When adding a Switch manually, first check that it is configured to factory defaults. This can be ensured by depressing the reset switch button for 10 seconds or more. The Switch can also be factory defaulted from the Switch Local UI, or the Command Line Interface accessible through the console 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. Log into the SonicOS management interface and navigate to **DEVICE > Switch Network > Overview> List View**. Click on **Add Switch** as shown below.



The **ADD SWITCH** dialog appears:



3. In the **Add Switch** dialog box, populate the following fields:

- **Switch Model** - Select the SWS model from the drop-down list.
- **Serial Number** - Type in the serial number, found on the label on the bottom of the Switch.
- **Switch Name** - Enter a descriptive name for the Switch.

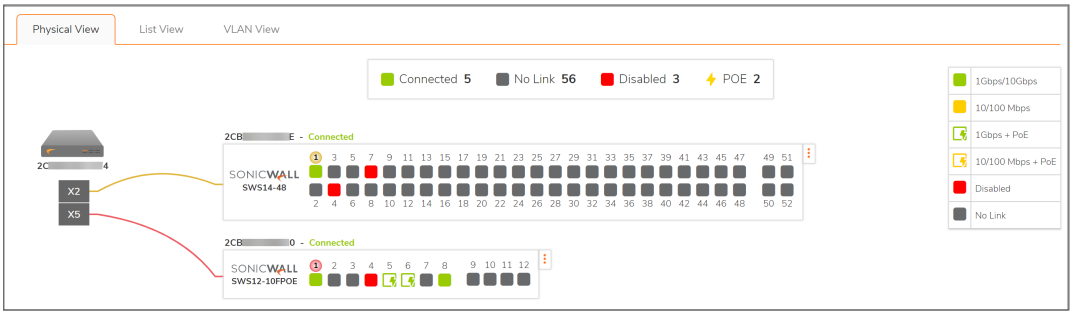
- **Comment** - Enter a comment. A comment is required when adding a Switch.
- **IP Address** - Enter the IP address of the Switch. Default is 192.168.168.169.
- **User Name** - Default is *admin*.
- **Password** - Default is *password*.
- **Switch Mode** - Select **Standalone** for a single Switch, and **Daisy-chain** for one of multiple Switches connected to the same port.
- **Switch Management** - Select the number of the Switch port that is connected to the firewall for management of the Switch.
- **Firewall Uplink**: Select the interface on the firewall that is connected to the Switch.
- **Switch Uplink**: Select the number of the Switch port that is connected to the firewall.

> **NOTE:** The Firewall Uplink interface and the Switch Uplink port are physically connected to each other. Refer to **About Uplink Interfaces** in the Configuring Basic Topologies section.

Under **ADVANCED SETTINGS**, configure Spanning Tree and Jumbo Frame size settings:

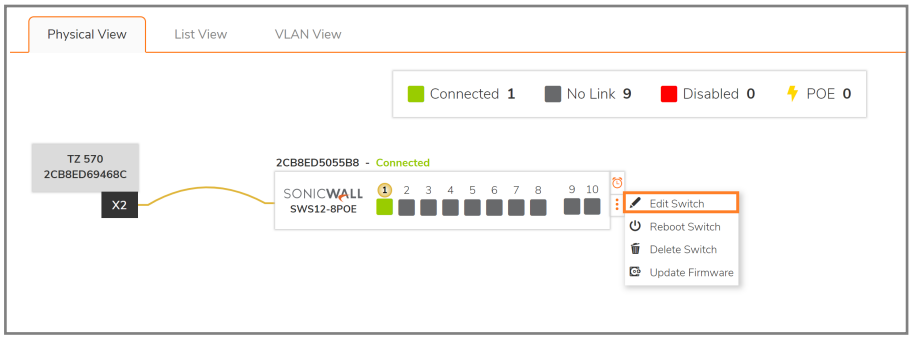
- **STP** - Enable or disable Spanning Tree Protocol by clicking the slider.
- **STP Mode** - Select **Rapid** or **Multiple**. Default is **Multiple**.
- **Jumbo Frame Size** - Enter a value between 1522 and 10240. Default is 1522. The default is the maximum standard transmission unit size in bytes. Frame sizes larger than this are jumbo.

4. Click **Apply**.
5. Go to **Overview > Physical View**, the new Switch will appear graphically with the ports linking the Switch and the firewall indicated.



Changing the Switch Configuration

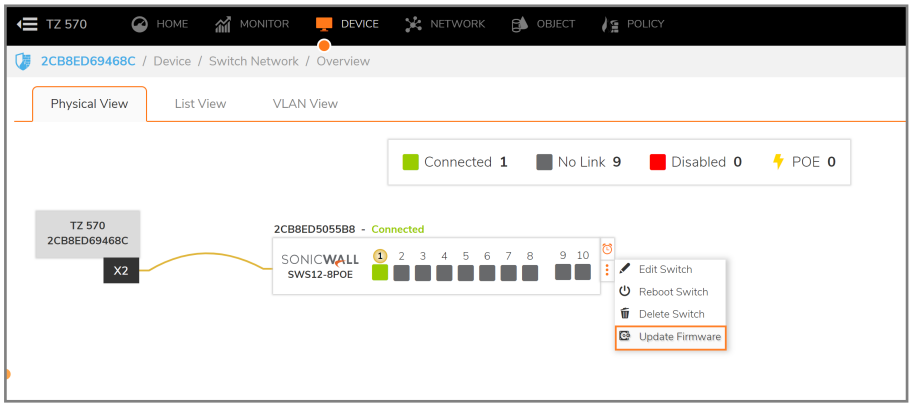
To edit the Switch Configuration, click on the three-dot menu and select **Edit Switch**.



The edit switch dialog box will come up:

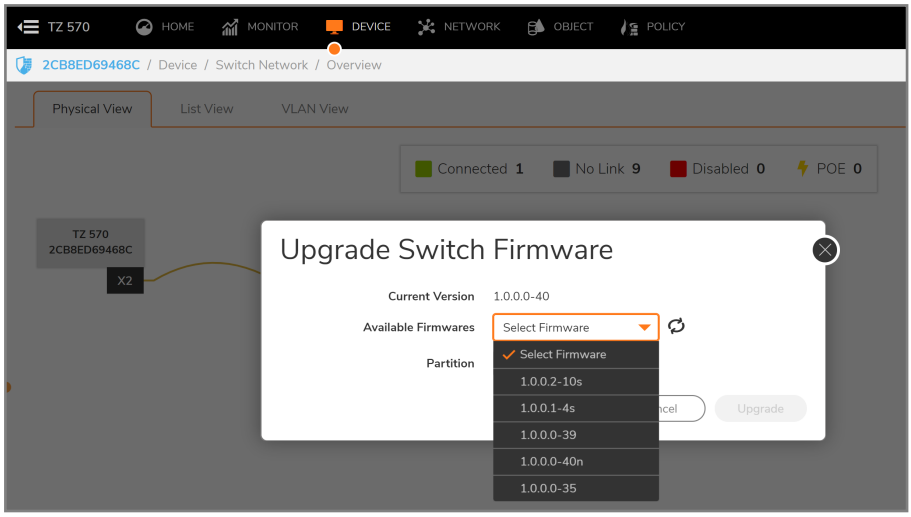
Upgrading Firmware

To upgrade firmware, go to **Overview > Physical View** and click the three dot icon to the right of the switch graphic.



Click on the refresh icon to see if any new updates are available.

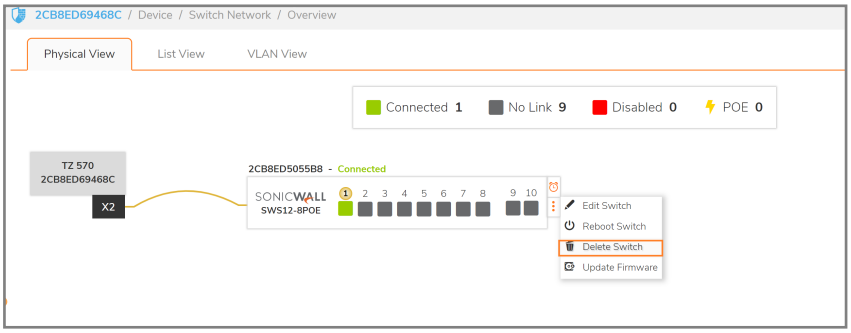
Look to see if new firmware is available. If yes, then select it and click on upgrade.



Shutting Down the Switch

To remove a Switch from a firewall:

1. Navigate to **Device > Switch Network > Overview**.
2. Click on the **Delete Switch**.



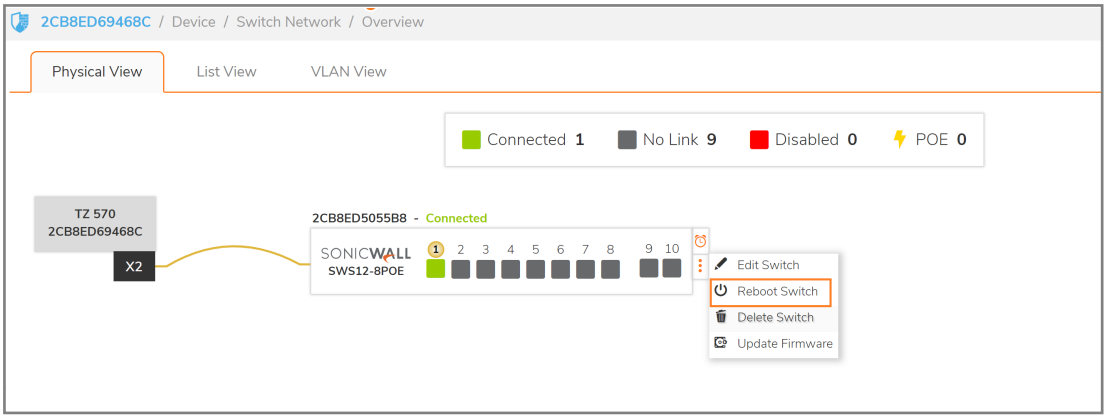
Restarting the Switch

To reboot the switch:

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

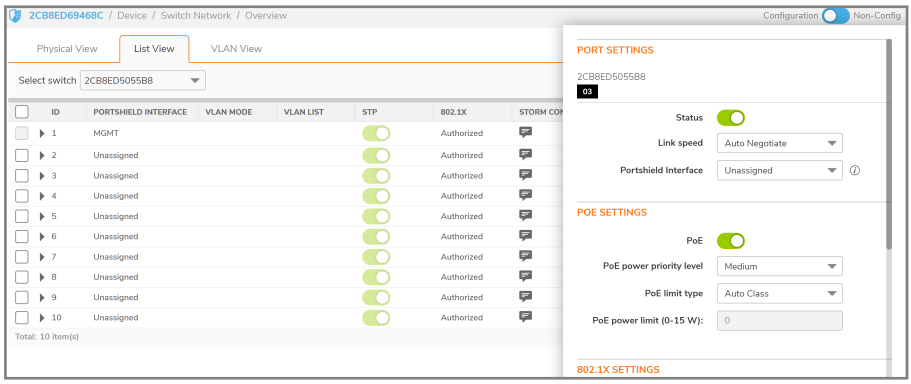
OR

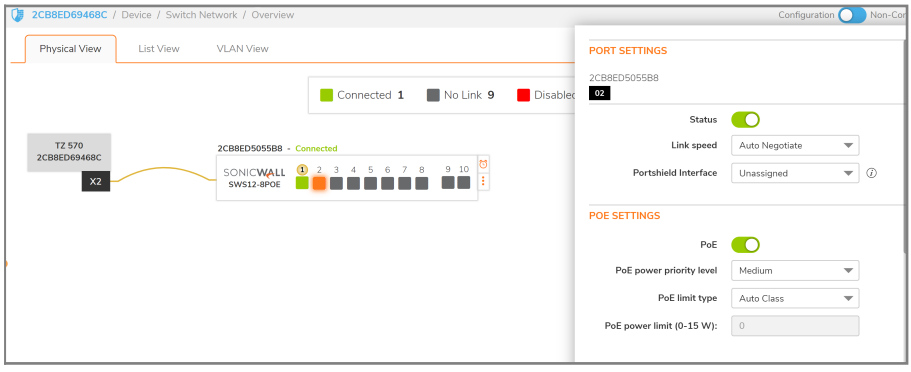
1. Click on the 3 dot menu on the Switch image on the **Overview** page and click on **Reboot Switch**.



Setting Up PoE

To set up PoE limits per port, navigate to **Device > Switch Network > 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 Medium. 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.

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.

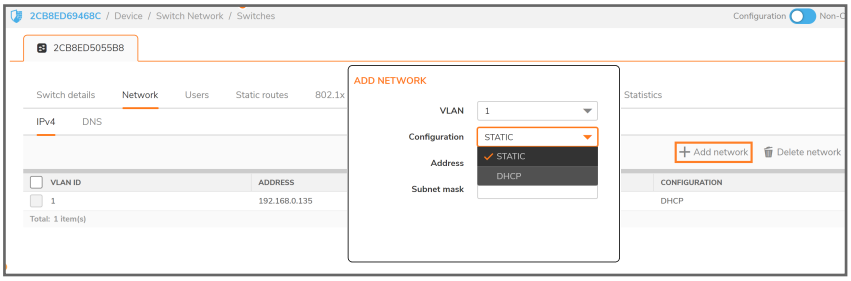
Each VLAN in a network has an associated VLAN ID, which appears in the IEEE 802.1Q tag in the Layer 2 header of packets transmitted on a VLAN. The IEEE802.1Q specification establishes a standard method for tagging Ethernet frames with VLAN membership information. The key for IEEE802.1Q to perform its 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 **DEVICE > Switch Network > Switches > Network**.
2. Click on **Add Network**.

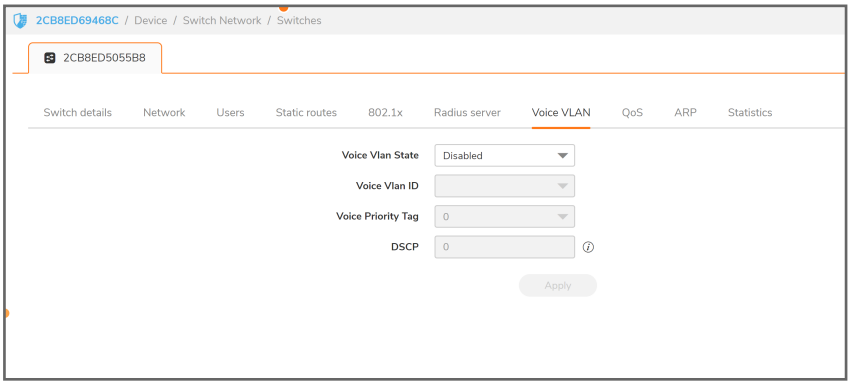


3. Define **VLAN ID, Address, Subnet Mask** and choose address assignment method: **Static** or **DHCP**.
4. Click on **OK**.

Configuring Voice VLAN:

NOTE: Voice VLANs can be enabled/disabled per port in the **DEVICE > Switch Network > Switches > Voice VLAN** display.

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



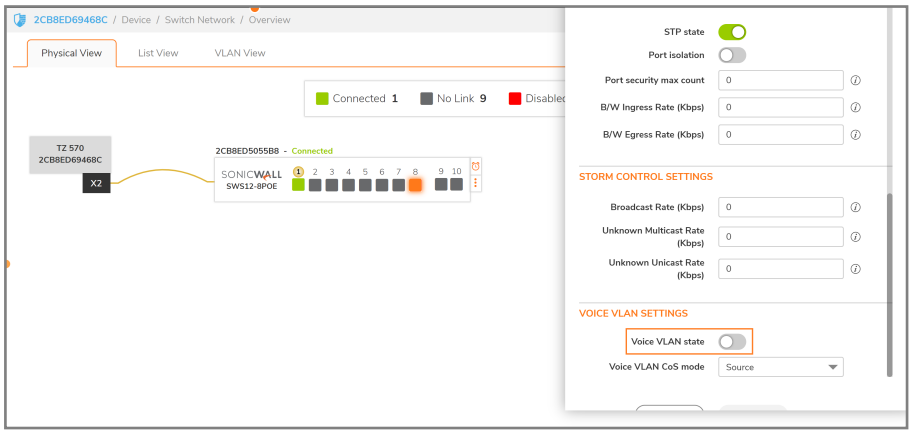
2. Set up a voice VLAN by moving the state from Disabled to Auto and set the other parameters before clicking on Accept as it appears at the bottom of the display.
    - **Voice Vlan ID** — identifies LAN.
    - **Voice Priority Tag** — determines priority among active voice streams.
    - **Differentiated 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.

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:

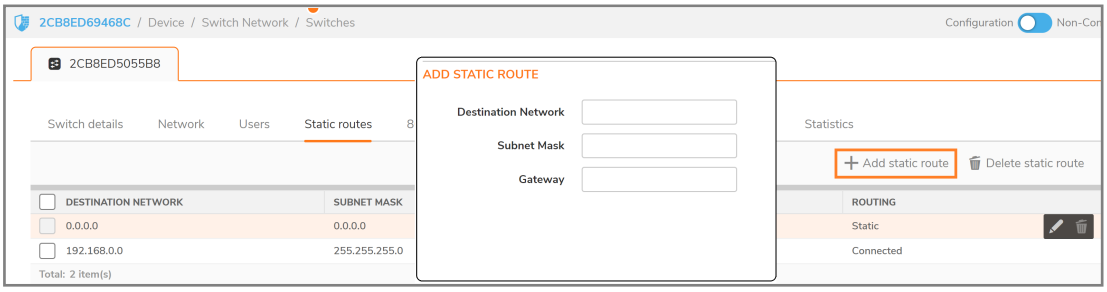
Go to **DEVICE > Switch Network > Overview** and click on the port. When the sideband display appears, scroll to Voice VLAN state as shown below.



Adding Static Routes

To add a static route to a Switch:

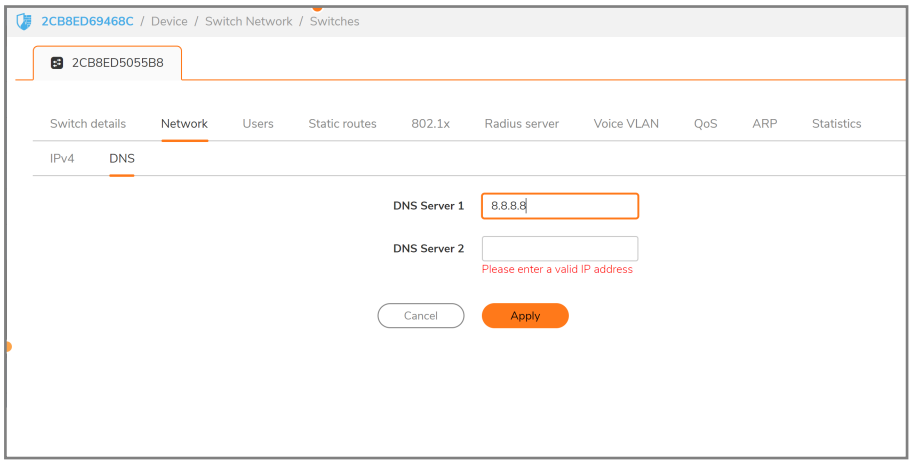
1. Navigate to **DEVICE > Switch Network > Switches** then select **Static Routes** and click on **Add Static Route**.



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 **DEVICE > Switch Network > Switches** and select **Network**, then click on **DNS**.

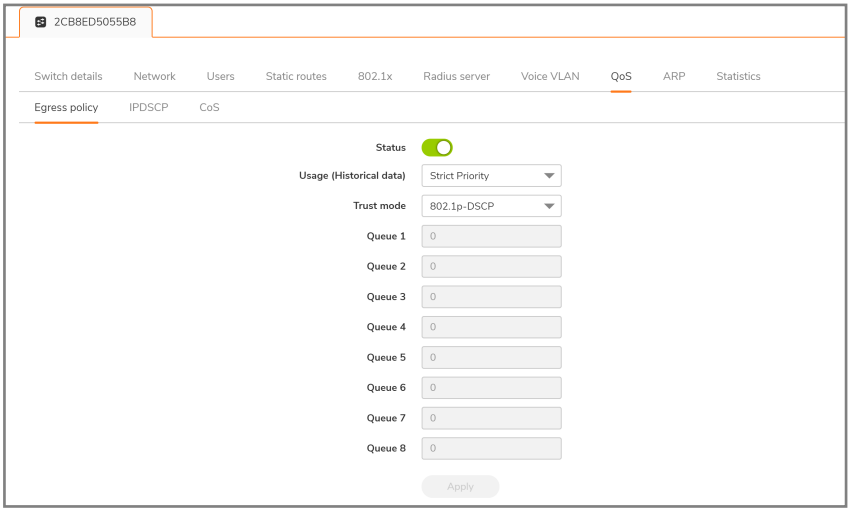


Setting Up QoS

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:

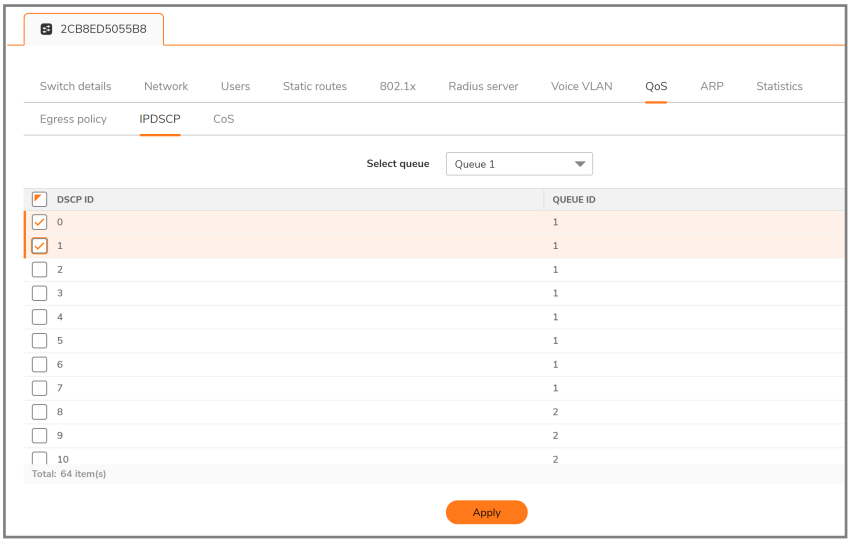
1. Navigate to **DEVICE > Switch Network > Switches** and click on **QoS**.



2. Set Egress Policy.

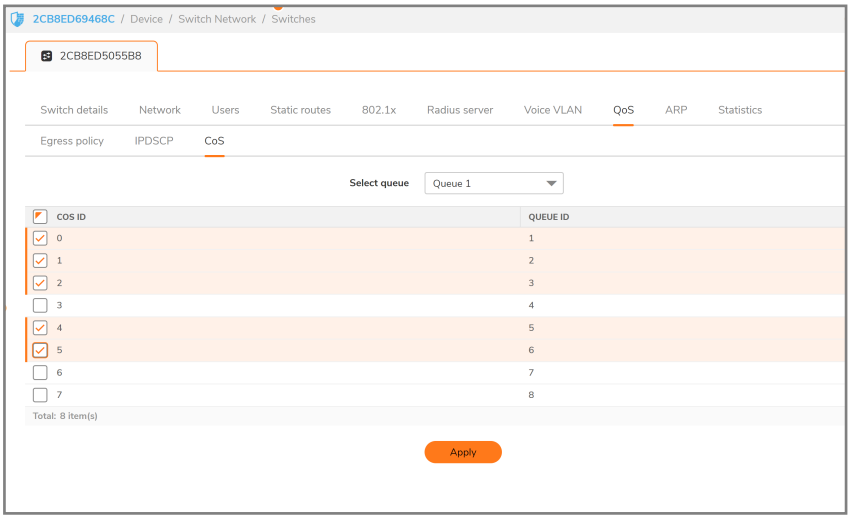
   The first screen details Egress Policy which applies for all approaches to packet and traffic classification.In the preceding UI screen, the State slider determines whether QoS is enabled (to the right) or disabled (to the left). Scheduling method can be set as Strict Priority based on Queue number or 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.



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

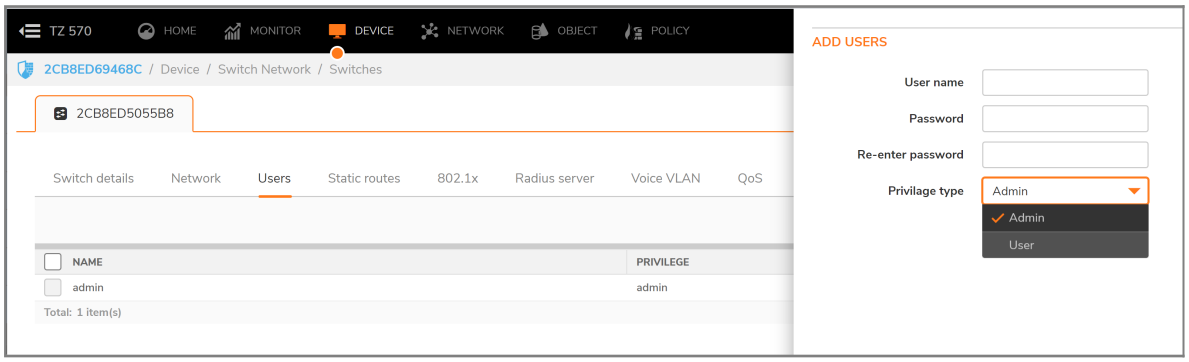
   In the CoS (Class of Service) screen, the CoS priority tag values, where 0 is the lowest and 7 is the highest are related to eight traffic priority queues from 1 to 8, where one is the lowest priority and eight is the highest priority.



Setting Up Users

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

Users with "user level privileges" are limited to Non-Configuration Mode.

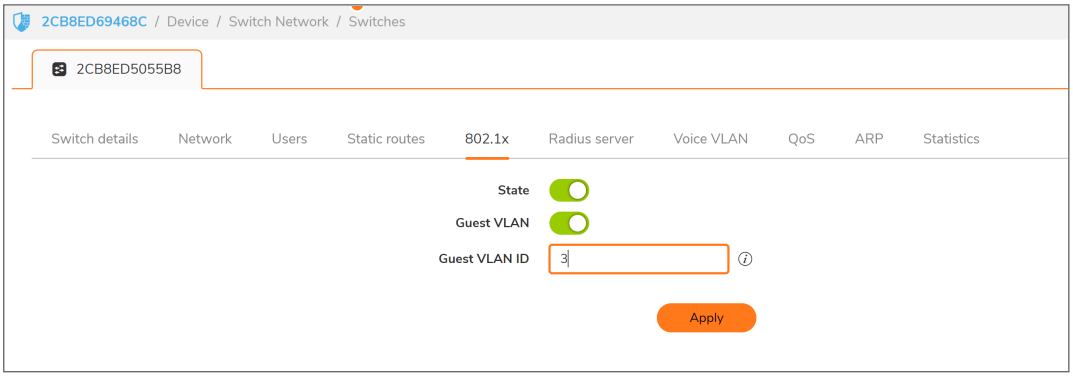


Setting Up 802.1X Authentication

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.

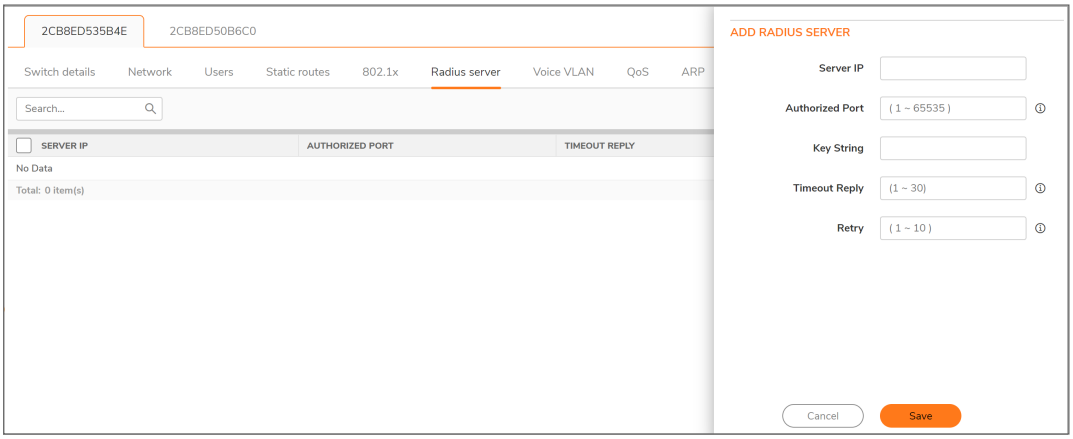
To enable 802.1 Authentication:

1. Go **DEVICE > Switch Network > 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 RADIUS server:

1. In **DEVICE > Switch Network > Switches** click on **Radius server**. In the **Radius server** screen, click on **+Add**.
2. To enable the Radius server, set the **Authorized Port** to 1812.



Daisy-Chaining Switches

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

- Standalone mode — Up to eight Switches can interface to a single firewall over separate ports.
- Daisy Chain mode — Up to eight Switches can be supported in multiple configurations with one level of chaining. For example:

- 4 Switches in standalone mode with one Switch connected to each in daisy chain mode.
- 6 Switches in standalone mode with two more Switches connected separately to any two of them in daisy chain mode.
- 7 Switches in standalone mode and one Switch connected to any one of them in daisy chain mode.

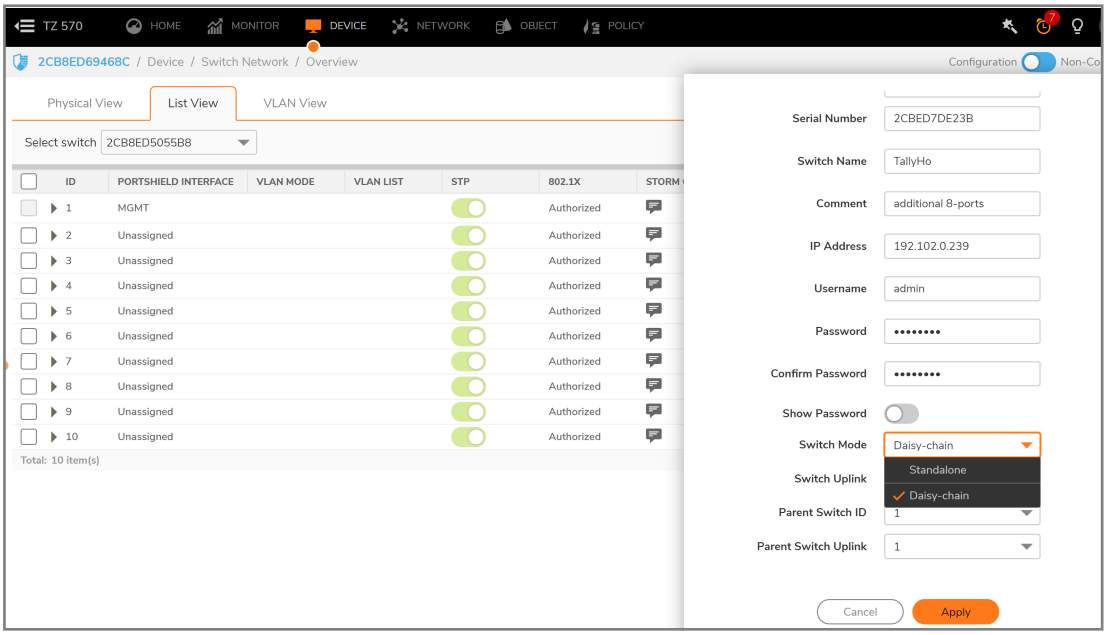
NOTE: Switches may be added into daisy-chained configurations manually or by using Zero-Touch.

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 **Device | Switch Network > 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 it. Then determine which ports to use to connect the additional Switch.
2. Go to **Device | Switch Network > 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 **Network > DHCP Server**.
   - Switch Mode — Select Daisy-chain.
   - Parent Switch ID — The Switch ID will be 1 if the child Switch is connected to the Switch which was added first to the firewall.
   - 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 **DEVICE | Switch Network > Switches** and click on **Physical View**. The new Switch will appear graphically with the ports linking the Switch and the firewall indicated.

Connecting Access Points

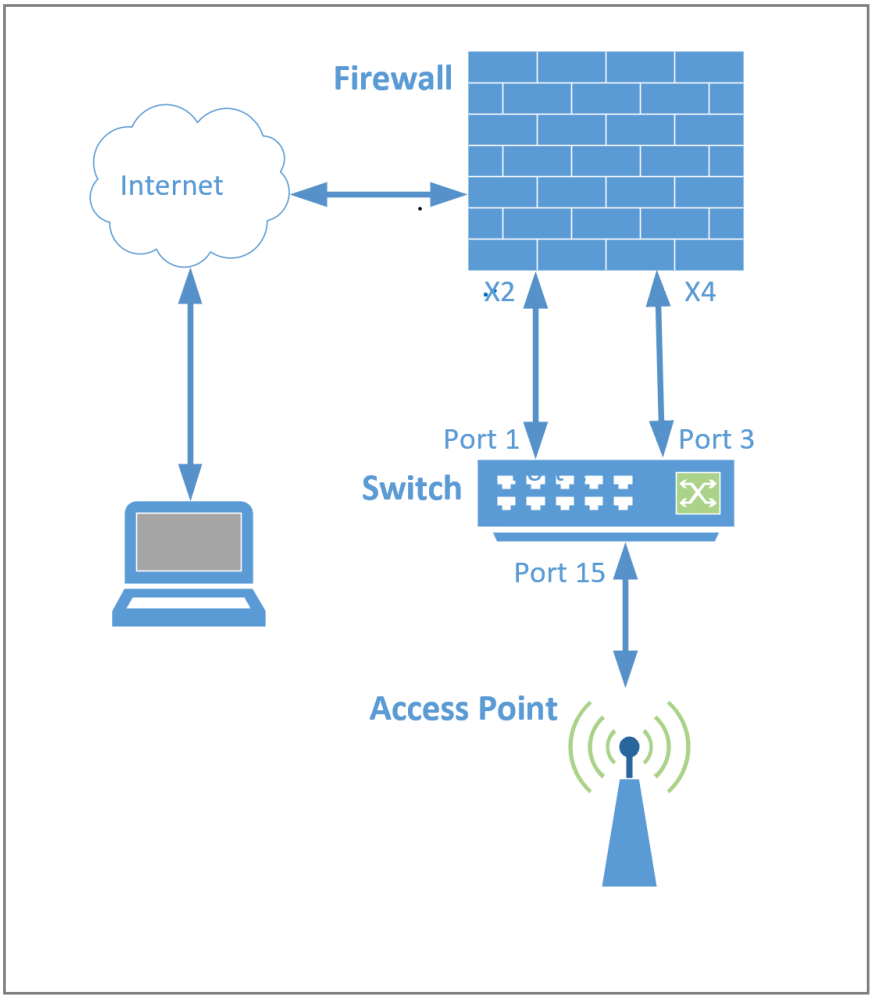
With the firewall user interface, administrators may manage SonicWave access points connected to Switches. Adding access points to a Switch involves three steps beyond making the physical connection.

- 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 see Adding a Switch to a Firewall with Zero-Touch.
2. Add the Switch.
3. Configure X4 in WLAN zone with VLANs.
4. Connect Switch Port 3 to X4 interface.
5. In the firewall GUI, navigate to **DEVICE | Switch Network > Switches**, 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 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.
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 a Link to SonicWall Access Points.

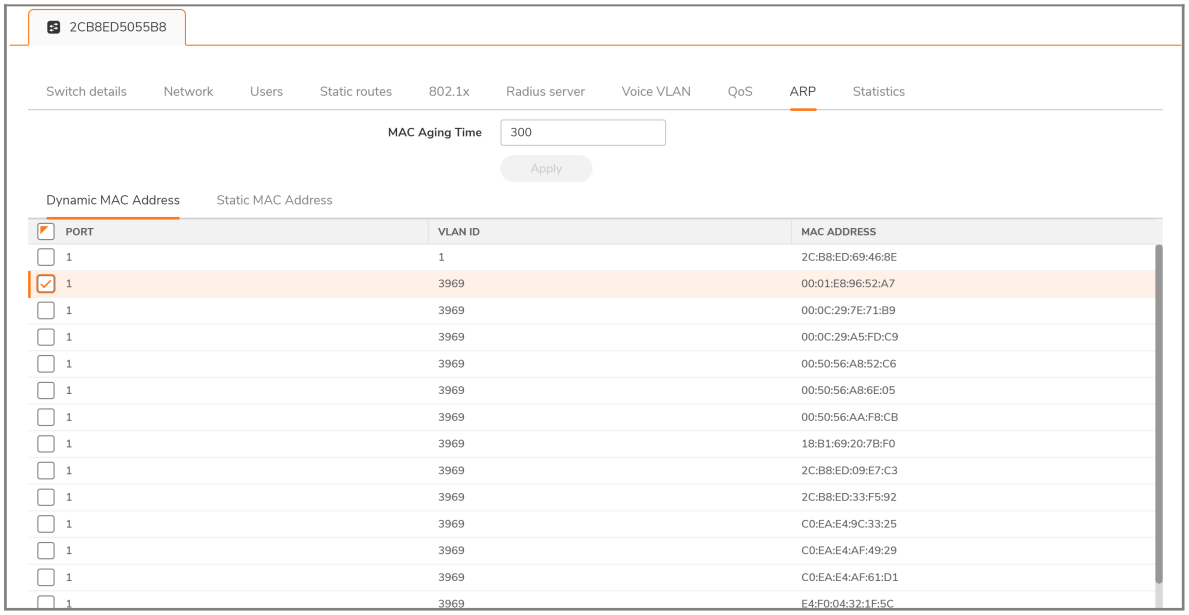
9. Connect a WiFi client and check that it gets an IP address from in the X4 Portshield lease-hold.

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 **Device > Switch Network > Switches** and then click on **ARP**.

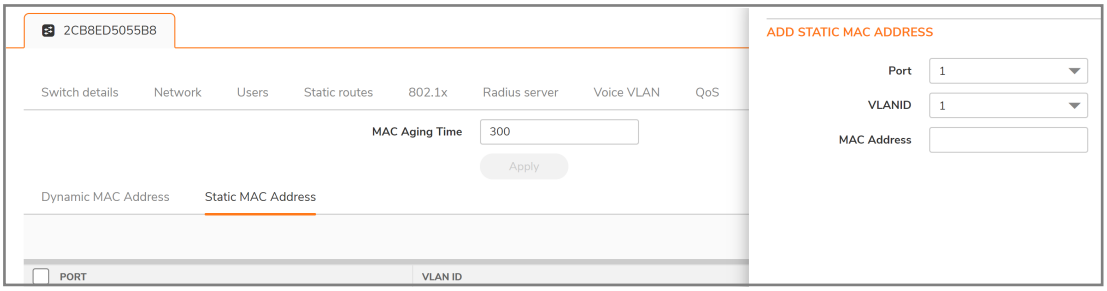


To set MAC Aging Time:

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 630; The default value is 300 seconds. Disabling MAC aging is not supported. 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.

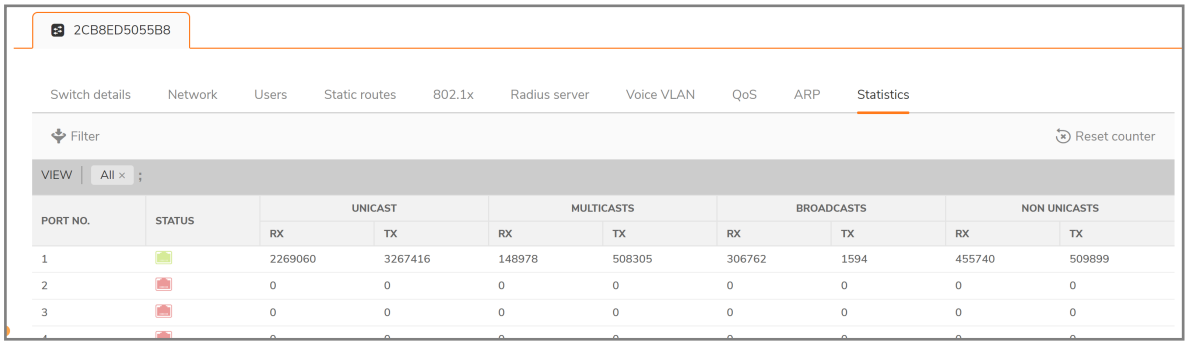
To Check Dynamic MAC Address Learning:

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 **DEVICE | Switch Network > Switches > Statistics**.

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



3

Configuring Switch Topologies

Topics:

Configuring Basic Topologies

About Topologies

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

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 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).

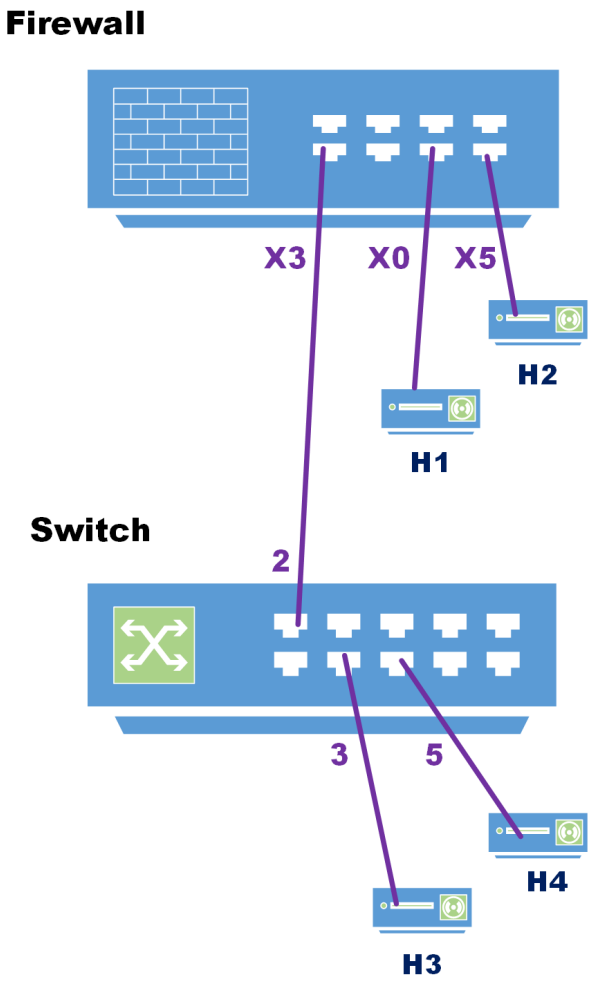
The advantage of such a deployment option is to separate a set of firewall/Switch ports that are not being used for management traffic. The disadvantage is that a high amount of data traffic can penalize forwarding of management traffic as the same link is shared for both types of traffic.

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). 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 as described in:

- Before Adding a Switch
- Adding a Switch to a Firewall with Zero-Touch
- Adding a Switch to a Firewall Manually

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 configured 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.

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. Configure 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 should include this.
2. Add the Switch to the network as described in Adding a Switch to a Firewall Manually by navigating to **DEVICE | Switch Network > Overview > List 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.
    c. Click **Apply** to save the configuration.
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.

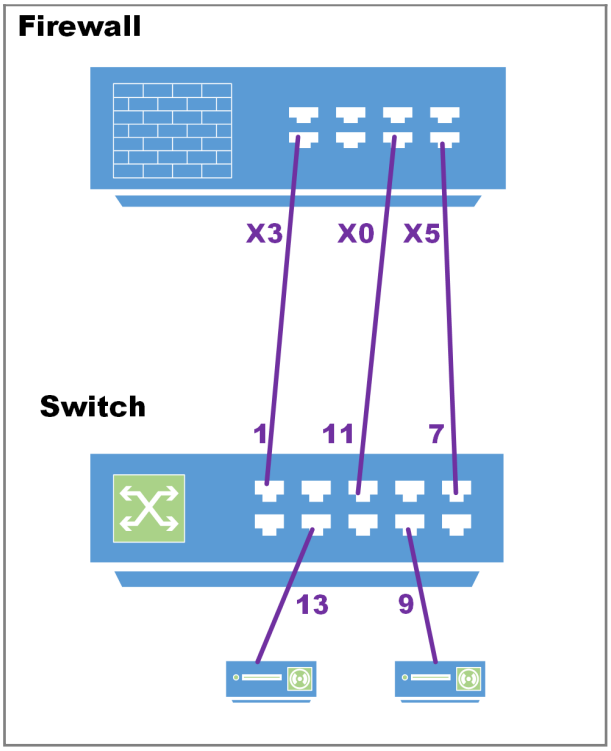
ⓘ **NOTE:** In this example, there is no common uplink to carry the PortShield traffic for the rest of the firewall interfaces (excluding X0 and X5 for which dedicated links are set up).

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

The diagram, 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.
2. To set up a link as a dedicated uplink without management traffic, in the Add Switch dialog box set **Firewall Uplink** and **Switch Uplink** to **None**.
3. In the **DEVICE | Switch Network > Overview > Physical View** or **List View**, enable the Switch port for the dedicated link.
4. Once the Switch port is enabled, go to Switch Port Settings as described in Setting Up Ports. Set portshields to support dedicated uplinks. In this example, port 7 is portshielded to X5.

Configuring a Hybrid System with Common and Dedicated Uplinks

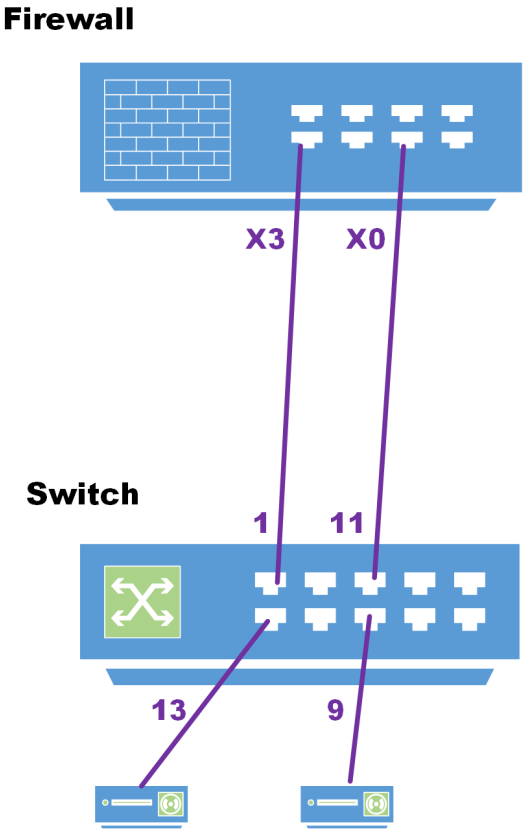
This configuration allows a combination of common and dedicated uplinks to be set up between the firewall and the Switch. The dedicated uplinks are used to carry PortShield traffic corresponding to the connected firewall interface. The common uplink is used to carry PortShield traffic for the remaining 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.
2. Configure the uplink as described inConfiguring a Dedicated Uplink.

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.

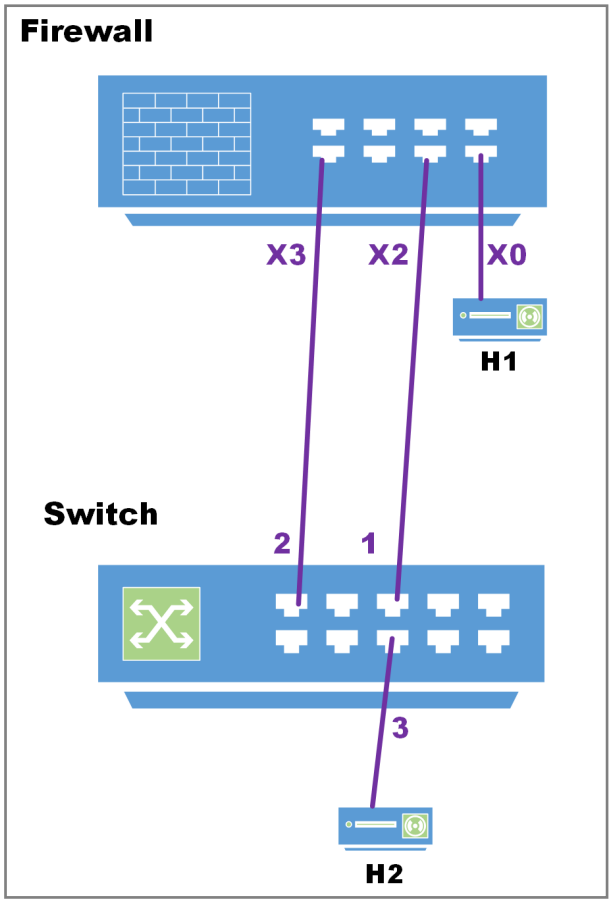
Isolated Link Topology shows an isolated link setup of a firewall with a Switch:

- 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 **DEVICE | Switch Network > Overview > List View** 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 High Availability

Topics:

- Configuring HA and PortShield With a Common Uplink
- Configuring HA and PortShields With Dedicated Uplink(s)
- Configuring HA Using One Switch Management Port
- Configuring HA Using Two Switch Management Ports

Configuring HA and PortShields With Dedicated Uplinks

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.

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

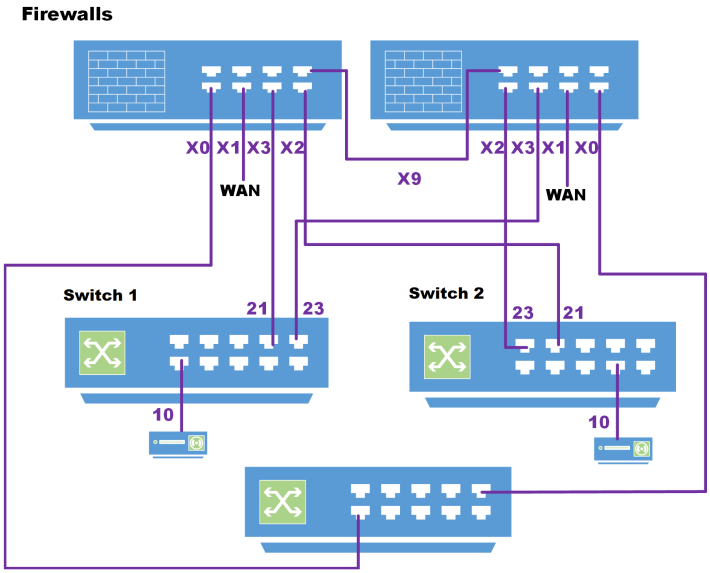
- Configuring HA Using One Switch Management Port
- Configuring HA Using Two Switch Management Ports

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

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:

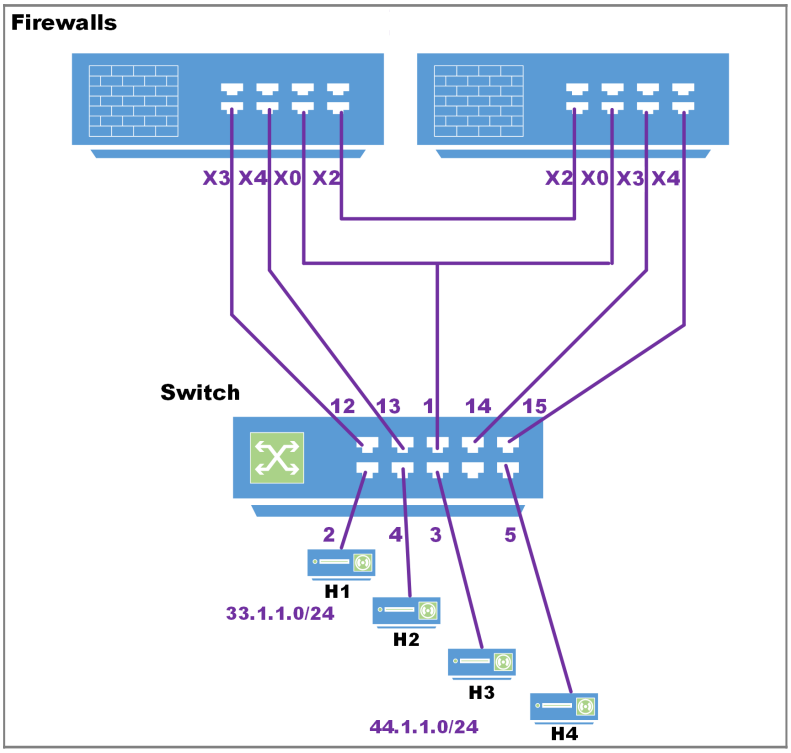
- The firewall interfaces, X3 and X4, on the primary unit are connected to ports 12 and 13 on the Switch.
- X3 and X4 are configured as PortShield hosts.
- Similarly, the firewall interfaces X3 and X4 on the secondary unit are connected to ports 14 and 15 on the Switch.
- Ports 12 and 14 on the Switch 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:

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

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

   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

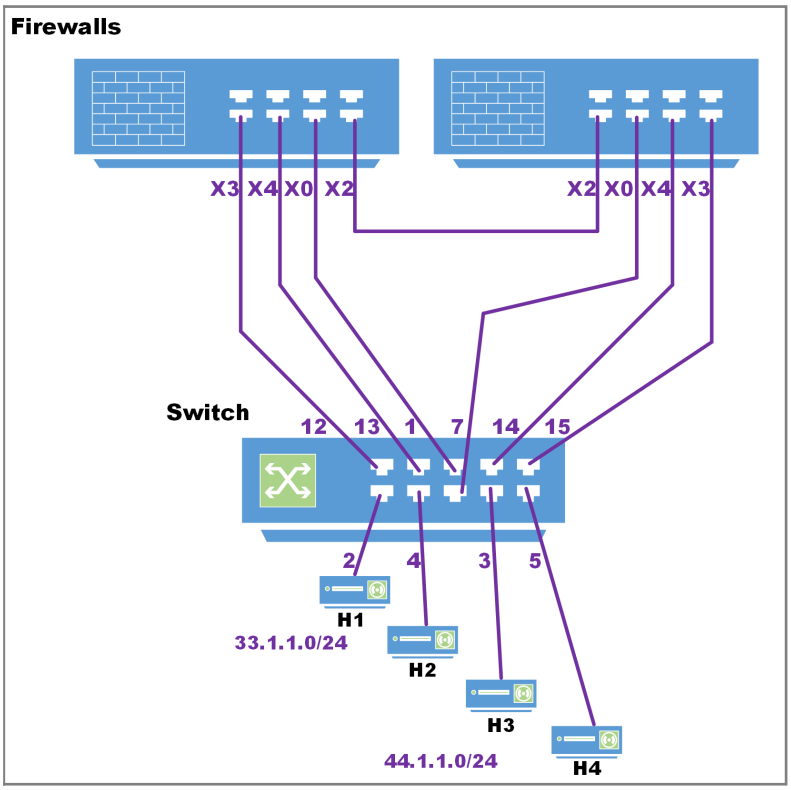
You can connect X0 of the primary and secondary firewalls directly to the ports on the Switch. In this case, two Switch ports are used on the Switch for management traffic.

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:

IMPORTANT: 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 **DEVICE | Switch Network > Overview** pages for the two Switch management port configuration.
    b. Set **Firewall and Switch Uplink** options to **None**.

    NOTE: Define one as Primary and the other as Secondary.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.
3. Click **ADD**.

Configuring VLANs With Dedicated Uplinks

Topics:

- Prerequisites for VLAN Support
- Configuring a Dedicated Uplink for VLANs

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:

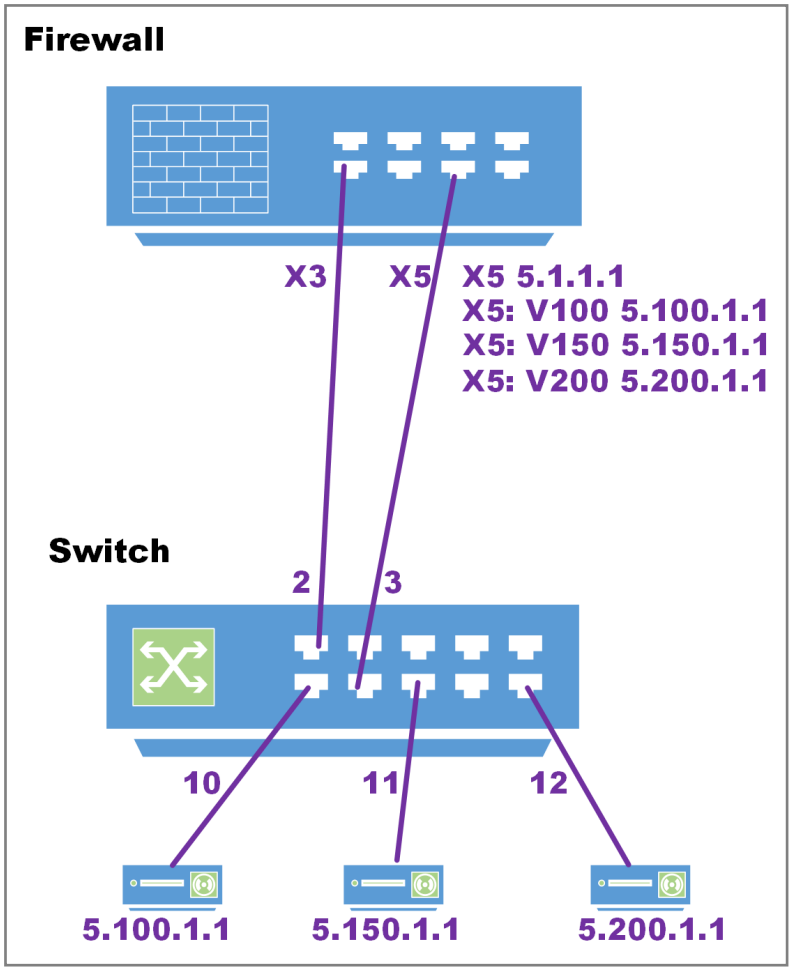
- Dedicated Uplink for VLAN Topology
- Configuring a Dedicated Uplink for a VLAN

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 Configuring a Dedicated Uplink:

1. Add the Switch and set up the data uplink as described in Adding a Switch to a Firewall Manually
2. Configure the options as described in Configuring a Dedicated Uplink to except ensure to select the Dedicated Uplink option.
3. Navigate to **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.

   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 2T

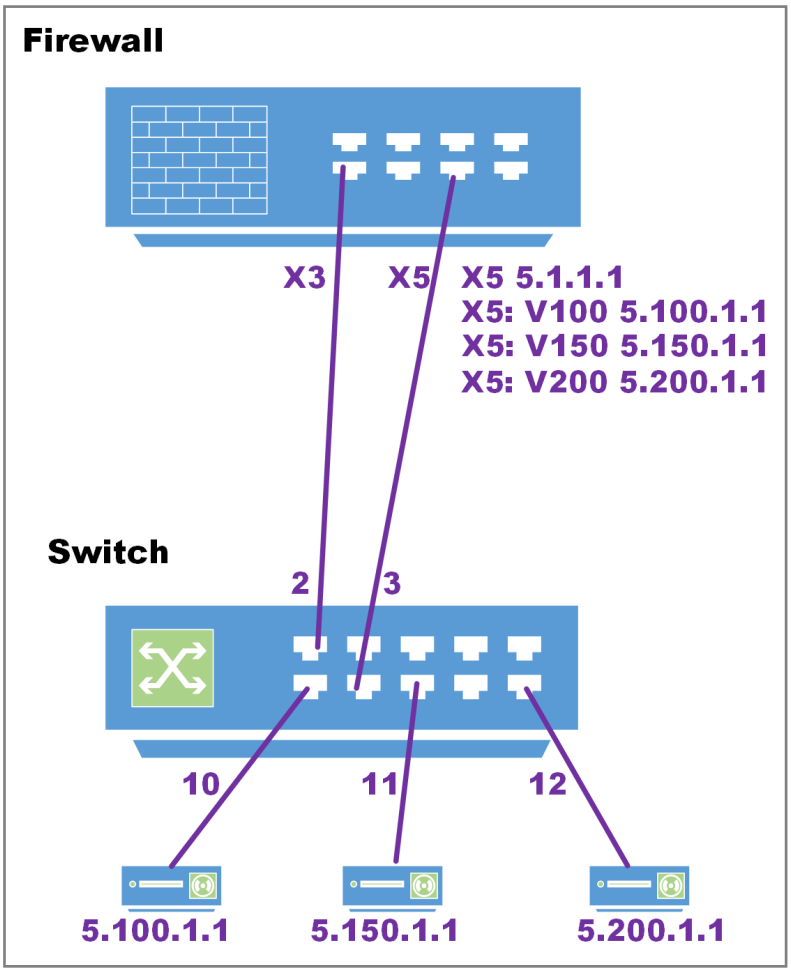
Configuring a Link to SonicWall Access Points

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.

CONNECTING TO ACCESS POINT



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.
2. Connect access points to Switch as described in Connecting Access Points.
3. Configure the uplinks as described in Configuring VLANs With Dedicated Uplinks.
4. Ensure that all SonicWall access points are connected to Switch ports configured in the PortShield group of the dedicated link.

SonicWall Support

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

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

The Support Portal enables you to:

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

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

About This Document

NOTE: A NOTE icon indicates supporting information.

IMPORTANT: An IMPORTANT icon indicates supporting information.

TIP: A TIP icon indicates helpful information.

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

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

SonicOS Switch Network Administration Guide
Updated - April 2021
Software Version - 7
232-005349-10 Rev C

End User Product Agreement

To view the SonicWall End User Product Agreement, go to: https://www.sonicwall.com/legal/end-user-product-agreements/.

Open Source Code

SonicWall Inc. is able to provide a machine-readable copy of open source code with restrictive licenses such as GPL, LGPL, AGPL when applicable per license requirements. To obtain a complete machine-readable copy, send your written requests, along with certified check or money order in the amount of USD 25.00 payable to "SonicWall Inc.", to:

General Public License Source Code Request
Attn: Jennifer Anderson
1033 McCarthy Blvd
Milpitas, CA 95035