# SonicOS 7

# Internal Wireless

## Administration Guide

SONICWALL®

# Contents


**Wireless Overview** ..... **4**
Device Support ..... 5
Compliance ..... 5
FCC U-NII New Rule Compliance ..... 5
RED Compliance ..... 6
Considerations for Using Wireless Connections ..... 6
Recommendations for Optimal Wireless Performance ..... 6
Adjusting the Antennas ..... 7
Wireless Node Count Enforcement ..... 7
About MAC Address Filtering ..... 7

**Status** ..... **8**
WLAN Settings ..... 8
WLAN Statistics ..... 10
WLAN Activities ..... 10
Station Status ..... 11

**Settings** ..... **12**
Access Point ..... 12
Access Point Wireless Settings ..... 13
Wireless Virtual Access Point ..... 16
Wireless WDS Station ..... 17
Wireless Settings ..... 17
Advanced Radio Settings ..... 18
Access Point & WDS Station ..... 18
Access Point & WDS Station Wireless Settings ..... 19
Wireless Virtual Access Point ..... 20
Station Setting ..... 20

**Security** ..... **21**
About Authentication ..... 21
Configuring the WEP Settings ..... 23
Configuring WPA3/WPA2/WPA PSK Settings ..... 24
Configuring WPA3/WPA2/WPA EAP Settings ..... 25

**Advanced** ..... **27**
Beaconing and SSID Controls ..... 28

Green Access Point ..... 28
Advanced Radio Settings ..... 29
Configurable Antenna Diversity ..... 31

**MAC Filter List** ..... **32**
Deployment Considerations ..... 32
Configuring MAC Filter List ..... 32

**IDS - Wireless Intrusion Detection Service** ..... **34**
Access Point IDS ..... 34
Rogue Access Points ..... 34
Configuring IDS Settings ..... 35
Discovered Access Points ..... 36
Authorizing Access Points on Your Network ..... 37

**Virtual Access Point** ..... **38**
Wireless Virtual AP Configuration Task List ..... 39
Virtual Access Point Profiles ..... 40
Virtual Access Point Schedule Settings ..... 41
Virtual Access Point Profile Settings ..... 41
ACL Enforcement ..... 44
Virtual Access Point Objects ..... 45
VAP General Settings ..... 45
VAP Advanced Settings ..... 46
Virtual Access Point Groups ..... 46
Enabling the Virtual Access Point Group ..... 47

**SonicWall Support** ..... **48**
About This Document ..... 49

3

# Wireless Overview

Only SonicWall wireless security appliances (TZ wireless platforms) display the pages under **DEVICE | Internal Wireless** for configuring wireless settings on the appliance.

The SonicWall wireless security appliances support wireless protocols IEEE 802.11a, 802.11ac, 802.11b, 802.11g, and 802.11n and send data through radio transmissions. These transmissions are commonly known as Wi-Fi or wireless. The SonicWall wireless security appliance combines three networking components to offer a fully secure wireless firewall: an Access Point, a secure wireless gateway, and a stateful firewall with flexible NAT and VPN termination as well as initiation capabilities. With this combination, the wireless security appliance offers the flexibility of wireless without compromising network security.

Typically, the wireless security appliance is the access point for your wireless LAN and serves as the central access point for computers on your LAN. In addition, it shares a single broadband connection with the computers on your network. Because the wireless security appliance also provides firewall protection, intruders from the Internet cannot access the computers or files on your network. This is especially important for an “always-on” connection such as a DSL or T1 line that is shared by computers on a network.

However, wireless LANs are vulnerable to “eavesdropping” by other wireless networks, which means you should establish a wireless security policy for your wireless LAN. On the wireless security appliance, wireless clients connect to the Access Point layer of the firewall. Instead of bridging the connection directly to the wired network, wireless traffic is first passed to the Secure Wireless Gateway layer where the client is required to be authenticated through User Level Authentication. Wireless access to Guest Services and MAC Filter Lists are managed by the wireless security appliance. If all of the security criteria are met, then wireless network traffic can then pass through one of the following distribution systems:

- LAN
- WAN
- Wireless Client on the WLAN
- DMZ or other zone
- VPN tunnel

See the following topics for more information about using SonicWall wireless security appliances.

**Topics:**


- Device Support
- Compliance
- Considerations for Using Wireless Connections
- Adjusting the Antennas
- Wireless Node Count Enforcement
- About MAC Address Filtering


See the following topics for information about using the SonicOS 7 **Internal Wireless** web management pages.


- Status
- Settings
- Security
- Advanced
- MAC Filter List
- IDS - Wireless Intrusion Detection Service
- Virtual Access Point


# Device Support

Internal Wireless functionality and settings are supported on the following wireless network security appliances (firewalls) running SonicOS 7:

- TZ270W
- TZ370W
- TZ470W
- TZ570W

# Compliance

The wireless devices are required to comply with various requirements for sale and use of these devices in specific areas. For the latest information about regulatory approvals and restrictions for SonicWall wireless devices, see the Technical Documentation pages for your product at https://www.sonicwall.com/support/technical-documentation. Each device has a unique regulatory document that provides the relevant information.

# FCC U-NII New Rule Compliance

FCC U-NII (Unlicensed –National Information Infrastructure) New Rule (Report and Order ET Docket No. 13-49) is supported on TZ series wireless appliances. To comply with FCC New Rules for Dynamic Frequency Selection (DFS), a TZ wireless appliance detects and avoids interfering with radar signals in DFS bands.

# RED Compliance

The Radio Compliance Directive (RED) is supported on the TZ series wireless appliances. RED (2014/53/EU) sets essential requirements for safety and health, electromagnetic compatibility and the efficient use of the radio spectrum.

# Considerations for Using Wireless Connections

When evaluating wireless versus wired connections, consider the advantages and disadvantages give your infrastructure and environment:

| | |
|---|---|
| **Mobility** | Is your network mostly used by laptop computers, tablets or smartphones? Wireless is more portable than wired connections. |
| **Convenience** | Wireless networks do not require cabling to individual computers or opening computer cases to install network cards. |
| **Speed** | If highest network speed is important to you, you might want to consider using Ethernet connections rather than wireless connections. |
| **Range and Coverage** | If your network environment contains numerous physical barriers or interference factors, wireless networking might not be suitable for your network. |
| **Security** | Wireless networks have inherent security issues because of the unrestricted nature of the wireless transmissions. However, the wireless security appliance is a firewall and has NAT capabilities which provides security, and you can use WPA or WPA2 to secure data transmissions. |

# Recommendations for Optimal Wireless Performance

SonicWall recommends the following for optimal wireless performance:

- Place the wireless security appliance near the center of your intended network. This reduces the possibility of eavesdropping by neighboring wireless networks.
- Minimize the number of walls or ceilings between the wireless security appliance and the receiving points such as PCs or laptops.
- Try to place the wireless security appliance in a direct line with other wireless components. Best performance is achieved when wireless components are in direct line of sight with each other.
- Building construction can affect wireless performance.
    - Avoid placing the wireless security appliance near walls, fireplaces, or other large solid objects.
    - Placing the wireless security appliance near metal objects such as computer cases, monitors, and appliances can affect performance of the unit.

    - Metal framing, UV window film, concrete or masonry walls, and metallic paint can reduce signal strength if the wireless security appliance is installed near these types of materials.
- Installing the wireless security appliance in a high place can help avoid obstacles and improve performance for upper stories of a building.
- Neighboring wireless networks and devices can affect signal strength, speed, and range of the wireless security appliance.
- Devices such as cordless phones, radios, microwave ovens, and televisions might cause interference on the wireless security appliance.

# Adjusting the Antennas

The antennas on the wireless security appliance can be adjusted for the best radio reception. Begin with the antennas pointing straight up, and then adjust as necessary. Note that certain areas, such as the area directly below the wireless security appliance, get relatively poor reception. Pointing the antenna directly at another wireless device does not improve reception. Do not place the antennas next to metal doors or walls as this can cause interference.

ⓘ | **NOTE:** Be sure to connect antennas to the appliance before enabling the wireless radio.

# Wireless Node Count Enforcement

Users connecting to the WLAN or connecting through the SonicWall GroupVPN are not counted toward the node enforcement on the SonicWall wireless network appliance. Only users on the LAN and non-Wireless zones are counted toward the node limit.

The Station Status table lists all the wireless nodes connected.

# About MAC Address Filtering

The SonicWall wireless security appliance networking protocol provides native MAC address filtering capabilities. When MAC address filtering is enabled, filtering occurs at the 802.11 layer and wireless clients are prevented from authenticating and associating with the wireless access point. Because data communications cannot occur without authentication and association, access to the network cannot be granted until the client has given the network administrator the MAC address of their wireless network card.

1

# Status

The **DEVICE | Internal Wireless > Status** page provides status information for the wireless network, including wireless radio status and client station information.

**NOTE:** The **Internal Wireless > Status** page applies only to wireless platforms. See Device Support for the list of supported platforms. The pages in the **Internal Wireless** menu group vary depending on the **Radio Role** selected on the **Internal Wireless > Settings** page.

The **Internal Wireless > Status** page displays these tables:

- WLAN Settings
- WLAN Statistics
- WLAN Activities

## WLAN Settings

In the **Internal Wireless > Status** page, the **WLAN Settings** table lists the configuration information for the built-in radio. All configurable settings in the **WLAN Settings** table provide hyperlinks to their respective pages for configuration.

**NOTE:** The displayed settings vary depending on the **Radio Role** selected on the **Internal Wireless > Settings** page.

**WLAN SETTINGS**

| WLAN Settings | Value |
|---|---|
| WLAN | **Enabled (Active)** or **Disabled (Inactive)**; click the **Edit** link to open the **Internal Wireless > Settings** page to configure this setting. |
| SSID | Service Set Identifier for wireless network identification; click the **Edit** link to open the **Internal Wireless > Settings** page to configure this setting. |
| Primary BSSID | MAC address / serial number of the wireless security appliance |
| Primary IP Address | IP address of the wireless interface |
| Primary Subnet Mask | Netmask of the wireless subnet; this designates the network portion of the IP address |

| | |
|---|---|
| Regulatory Domain | **FCC - North America** for domestic appliances<br>**MKK - Japan** for Japanese appliances<br>**ETSI - Europe** for international appliances |
| Channel | Channel number selected for transmitting wireless signal; click the **Edit** link to open the **Internal Wireless > Settings** page to configure this setting. |
| Radio Tx Rate | Wireless data transmission rate, Best or one of a dozen possible values in Mbps; click the **Edit** link to open the **Internal Wireless > Advanced** page to configure this setting. |
| Radio Tx Power | Current power level of the radio signal transmission, Full Power or one of several other settings; click the **Edit** link to open the **Internal Wireless > Advanced** page to configure this setting. |
| Primary Security | Encryption settings for user authentication to the wireless radio, or Disabled; click the **Edit** link to open the **Internal Wireless > Security** page to configure this setting. |
| MAC Filter List | Indicates whether a custom Allow list and/or Deny list of client wireless devices (MAC addresses) is Enabled or Disabled. Click the **Edit** link to open the **Internal Wireless > MAC Filter List** page to configure this setting. |
| Wireless Guest Services | Enabled or Disabled. Guest Services can be enabled or disabled under **Object > Zones**, by editing the zone and updating the settings on the Guest Services screen of the dialog. |
| Intrusion Detection | Enabled or Disabled. Click the **Edit** link to open the **Internal Wireless > IDS** page to configure this setting. |
| Wireless Firmware | Firmware version on the radio card. |
| Associated Stations | Number of clients associated to the wireless security appliance, and the maximum number of supported wireless associations for this appliance. |
| Radio Mode | Current mode of the radio signal transmission, including:<br>• Type – **2.4GHz** or **5GHz** radio frequency band<br>• Protocol – **802.11 a, b, g, n, ac,** or a combination indicated by '/'<br>• **Mixed** or **Only – Mixed** if multiple protocols are supported by the radio, **Only** if the radio mode is configured to connect only to devices using a specific single protocol<br>Click the **Edit** link to open the **Internal Wireless > Settings** page to configure this setting. |

# WLAN Statistics

In the **Internal Wireless > Status** page, the **WLAN Statistics** table lists all of the traffic sent and received between the appliance wireless radio and the wireless client devices. The **Wireless Statistics** column lists the kinds of traffic recorded, the **Rx** column lists received traffic, and the **Tx** column lists transmitted traffic.

**WLAN STATISTICS**

| Wireless Statistics | Rx/TX |
|---|---|
| Good Frames | Number of allowed frames received and transmitted. |
| Bad Frames | Number of frames that were dropped. |
| Good Bytes | Total number of bytes in the good frames. |
| Management Frames | Number of management frames received and transmitted. |
| Control Frames | Number of control frames received and transmitted. |
| Data Frames | Number of data frames received and transmitted. |

# WLAN Activities

In the **Internal Wireless > Status** page, the **WLAN Activities** table summarizes the history of wireless client connections to the SonicWall wireless security appliance.

**WLAN ACTIVITIES**

| Wireless Activities | Value |
|---|---|
| Associations | Number of wireless clients that have connected to the wireless security appliance. |
| Disassociations | Number of wireless clients that have disconnected from the wireless security appliance. |
| Reassociations | Number of wireless clients that were previously connected that have re-connected. |
| Authentications | Number of wireless clients that have been authenticated. |
| Deauthentications | Number of authenticated clients that have disconnected. |
| Discards Packets | Number of discarded packets. |

# Station Status

In the **Internal Wireless > Status** page, the Station Status screen displays information about wireless client devices currently associated with the wireless security appliance.

### STATION STATUS

| Wireless Information | Description |
|---|---|
| **Station** | The name of the wireless client device |
| **MAC Address** | The hardware address of the wireless network card on the client device |
| **Vendor** | The vendor who manufactured the client station |
| **SSID** | The service set identifier of the wireless radio to which the client station is connected |
| **Authenticated** | Status of the client authentication |
| **Associated** | Status of the wireless association between the client station and the SonicWall wireless appliance |
| **AID** | Association ID, assigned by the security appliance |
| **Signal** | Strength of the radio signal |
| **Connect Rate** | Speed of the connection between client station and wireless appliance, generally in Mbps |
| **Timeout** | Number of seconds left in the session |
| **Configure** | Options for controlling the client station:<br>•  - allow the station to connect to the security appliance and add it to the Allow MAC Filter List.<br>•  - block the station from connecting to the security appliance and add it to the Deny MAC Filter List.<br>• - logout and disassociate the station from the security appliance. |

# Settings

You can set up the Wireless Radio Mode of your wireless appliance as an access point, a wireless distribution system (WDS) station, or as an access point and a WDS station.

***To configure the Wireless Radio Mode for the 802.11 wireless antenna:***

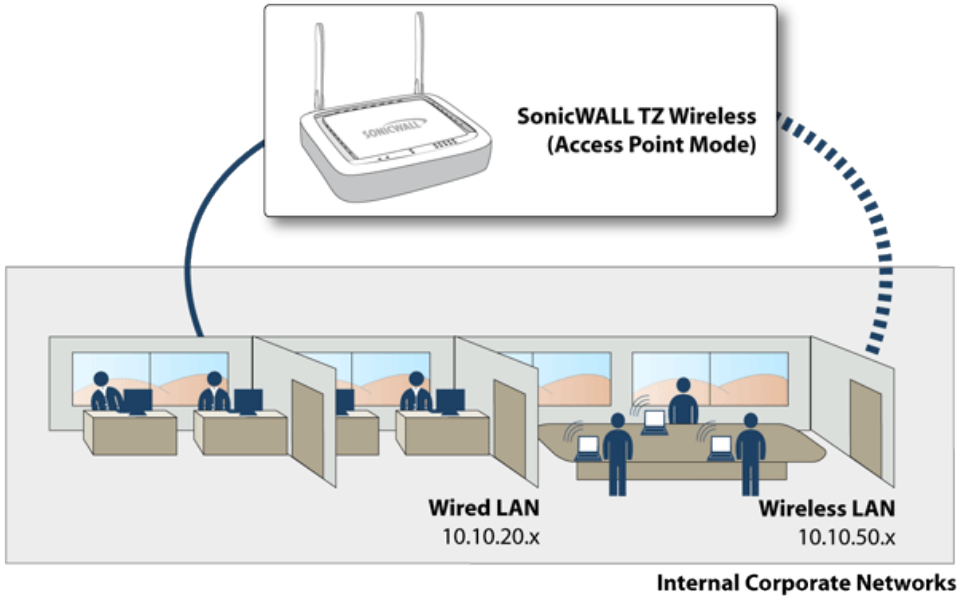
1. Navigate to **DEVICE | Internal Wireless > Settings**.
2. Choose the **Radio Role** you want your wireless appliance to perform.
   ⓘ | **IMPORTANT:** Changing from one mode to the other drops clients and might require a reboot.
   ⓘ | **NOTE:** The options on the page change depending on which **Radio Role** you choose.

The following sections describe how to configure your device for each **Radio Role** option:

- Access Point
- Wireless WDS Station
- Access Point & WDS Station

# Access Point

Selecting **Access Point** for the **Radio Role** configures the SonicWall wireless security appliance as an Internet/network gateway for wireless clients as shown in the following figure:



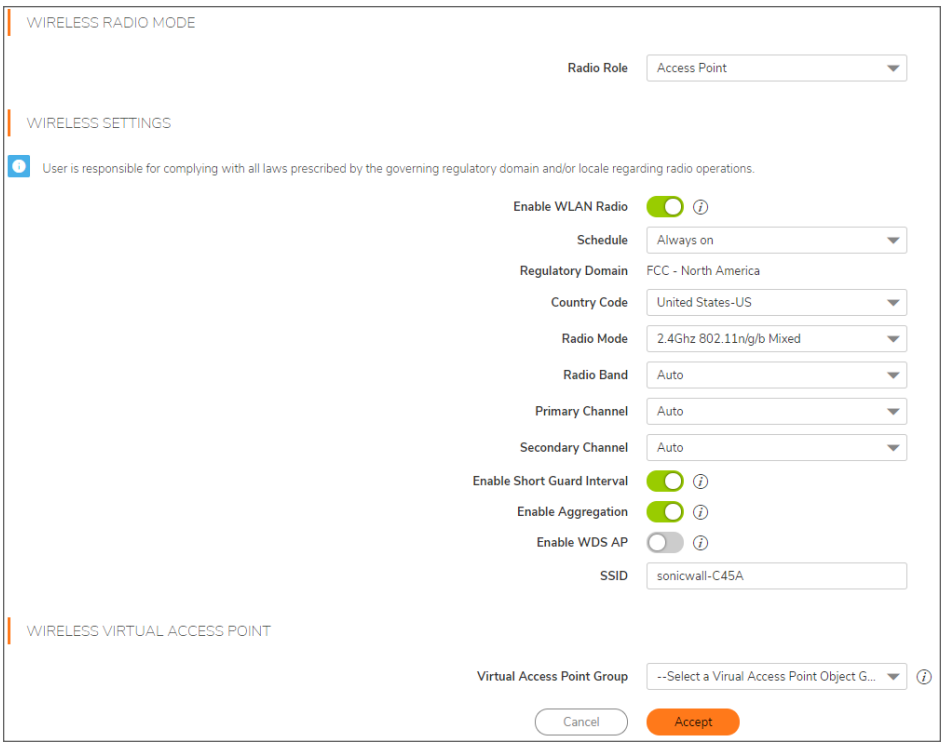
**Topics:**

- Access Point Wireless Settings
- Wireless Virtual Access Point

# Access Point Wireless Settings

**IMPORTANT:** When setting up the wireless appliance as an access point, you are responsible for complying with all laws prescribed by the governing regulatory domain and/or locale regarding radio operations.

1. Navigate to **DEVICE | Internal Wireless > Settings**.
2. In the **Radio Role** field, chose **Access Point** from the drop-down menu.




3. Toggle **Enable WLAN Radio** option to enable it. This provides clean wireless access to your mobile users. The WLAN radio is disabled by default.
4. In the **Schedule** field, select the time that WLAN radio is active from the drop-down menu. The Schedule list displays the schedule objects you create and manage in the **OBJECT | Match Objects > Schedules** page. The default value is **Always on**.
5. In the **Country Code** field, select the country in which the appliance is being used. The country code determines which regulatory domain the radio operation falls under.

6. In the **Radio Mode** field, select your preferred radio mode from the drop-down menu. The wireless security appliance supports the following modes:

   **TIP:** For optimal throughput speed solely for 802.11n clients, SonicWall recommends the **802.11n Only** radio mode. Use the **802.11n/g/b Mixed** radio mode for multiple wireless client authentication compatibility.

   - 802.11n/a/ac Mixed - Select this mode if 802.11a, 802.11ac, and 802.11n clients access your wireless network.
   - 802.11ac Only - Select this mode if only 802.11ac clients access your wireless network.

| Radio Mode | Definition |
|---|---|
| **2.4GHz 802.11n/g/b Mixed** | Supports 802.11b, 802.11g, and 802.11n clients simultaneously. If your wireless network comprises multiple types of clients, select this mode. |
| **2.4GHz 802.11n Only** | Allows only 802.11n clients access to your wireless network. 802.11a/b/g clients are unable to connect under this restricted radio mode. |
| **2.4GHz 802.11g/b Mixed** | Supports 802.11g and 802.11b clients simultaneously. If your wireless network comprises both types of clients, select this mode. |
| **2.4GHz 802.11g Only** | If your wireless network consists only of 802.11g clients, select this mode for increased 802.11g performance. You might also select this mode if you wish to prevent 802.11b clients from associating. |
| **5GHz 802.11n/a Mixed** | Select this mode if 802.11a and 802.11n clients access your wireless network. |
| **5GHz 802.11n Only** | Select this mode if only 802.11n clients access your wireless network. |
| **5GHz 802.11a Only** | Select this mode if only 802.11a clients access your wireless network. |
| **5GHz 802.11n/a/ac Mixed** | Select this mode if 802.11a, 802.11n, and 802.11ac clients access your wireless network. |
| **5GHz 802.11ac Only** | Select this mode if you want to provide improved throughput. |

The remaining options in the Wireless Settings section might change, depending on which **Radio Mode** you selected.

### Topics:

- 802.11n Wireless Settings
- 802.11a/b/g Wireless Settings
- 802.11ac Wireless Settings

# 802.11n Wireless Settings

When the **Radio Mode** field is configured for a mode that supports 802.11n only or a mixed mode that includes 802.11n, set following options:

ⓘ | **NOTE:** The options you see could vary slightly, depending on the on the type of appliance being configured.

| | | |
|---|---|---|
| **Radio Band** | Sets the band for the 802.11n radio. | |
| | **Auto** | Allows the appliance to automatically detect and set the optimal channel for wireless operation based on signal strength and integrity. This is the default setting. |
| | **Standard - 20 MHz Channel** | Specifies that the 802.11n radio uses only the standard 20 MHz channel. When this option is selected, the **Standard Channel** drop-down menu is displayed. |
| | **Standard Channel** | Is set to **Auto**, by default, which allows the appliance to set the optimal channel based on signal strength and integrity. You can select a single channel within the range of your regulatory domain. Selecting a specific a channel can also help the appliance avoid interference with other wireless networks in the area. |
| | **Wide - 40 MHz Channel** | Specifies that the 802.11n radio uses only the wide 40 MHz channel. When this option is selected, the **Primary Channel** and **Secondary Channel** drop-down menus are displayed. |
| | **Primary Channel** | Set to **Auto** by default, or you can specify a specific primary channel. |
| | **Secondary Channel** | The configuration of this drop-down menu is controlled by your selection for the primary channel:<br>• If the primary channel is set to Auto, the secondary channel is also set to Auto.<br>• If the primary channel is set to a specific channel, the secondary channel is set to the optimum channel to avoid interference with the primary channel. |
| **Enable Short Guard Interval** | | Enable this to have a higher Tx/Rx rate if supported. It applies only to 802.11ac/n mode. |
| **Enable Aggregation** | | Enables 802.11n frame aggregation, which combines multiple frames to reduce overhead and increase throughput. It applies only to 802.11ac/n mode. |
| **Enable WDS AP** | | Allows the WDS client to connect to this access point. |

| | |
|---|---|
| **SSID** | Is filled with a default value of **sonicwall-** plus the last four characters of BSSID; for example, *sonicwall-C587*. The SSID can be changed to any alphanumeric value with a maximum of 32 characters. |

**TIP:** The **Enable Short Guard Interval** and **Enable Aggregation** options can slightly improve throughput. They both function best in optimum network conditions where users have strong signals with little interference. In networks that experience less than optimum conditions (interference, weak signals, and so on), these options could introduce transmission errors that eliminate any efficiency gains in throughput.

## 802.11a/b/g Wireless Settings

When the **Radio Mode** field is configured for a mode that supports 802.11a only, 802.11g/b mixed, 802.11a only, or 802.11g only, set the following option displays:

| | |
|---|---|
| **Channel** | Allows the appliance to automatically detect and set the optimal channel for wireless operation based on signal strength and integrity. This is the default setting. You can select a single channel within the range of your regulatory domain. |
| **Enable WDS AP** | Allows the WDS client to connect to this access point. |
| **SSID** | Is filled with a default value of **sonicwall-** plus the last four characters of BSSID; for example, *sonicwall-C587*. The SSID can be changed to any alphanumeric value with a maximum of 32 characters. |

## 802.11ac Wireless Settings

When the wireless radio is configured for 802.11ac only, these options display:

- **Radio Band** drop-down menu – Sets the band for the 802.11ac radio which also allows support Band Wide-80 MHz Channel.
- **Channel** drop-down menu – Select a channel:
  - **Auto** – Allows the wireless security appliance to automatically detect and set the optimal channel for wireless operation based upon signal strength and integrity. **Auto** is the default channel setting, and it displays the selected channel of operation to the right. Alternatively, an operating channel within the range of your regulatory domain can be explicitly defined.
  - Specific channel.

# Wireless Virtual Access Point

If using wireless virtual access points, select a **Virtual Access Point Group** from the drop-down menu in the **Wireless Virtual Access Point** section. Or you can select a VAP group previously defined.

When done with all Access Point settings, click **Accept** to save the settings.

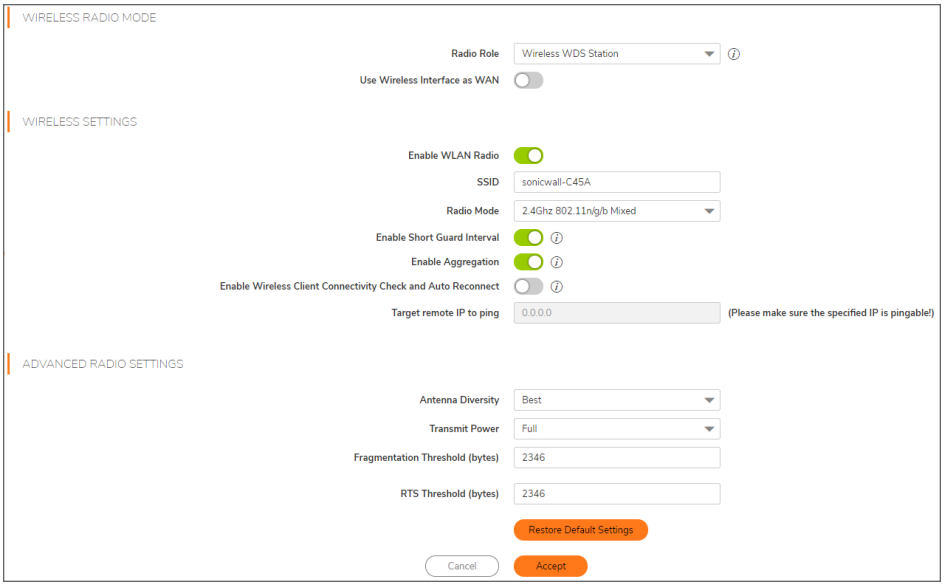
# Wireless WDS Station

The wireless appliance provides Internet/network access to another SonicWall wireless device or access point. Selecting **Wireless WDS Station** as the Radio Role allows secure network communications between physically separate locations, without the need for long and costly Ethernet cabling runs.

ⓘ | **NOTE:** The appliance cannot be used as a Wireless WDS Station if a wireless virtual access point is in use.

# Wireless Settings

1. Navigate to **DEVICE | Internal Wireless > Settings**.
2. In the **Radio Role** field, choose **Wireless WDS Station** from the drop-down menu.




3. Toggle **Wireless Interface as WAN** option to use wireless interface as WAN. The default value is not enabled.
4. Under the Wireless Settings section, toggle **Enable WLAN Radio** option to enable it. In Wireless WDS Station mode, after the radio is enabled, it acts as a client instead of an access point and does not provide wireless access to the client. The WLAN radio is disabled by default.
5. Select the following options:

| | |
|---|---|
| **SSID** | Is filled with a default value of **sonicwall-** plus the last four characters of BSSID; for example, *sonicwall-C587*. The SSID can be changed to any alphanumeric value with a maximum of 32 characters. |

| | |
|---|---|
| **Enable Short Guard Interval** | Enable this to have a higher Tx/Rx rate if supported. It applies only to 802.11ac/n mode. |
| **Enable Aggregation** | Enables 802.11n frame aggregation, which combines multiple frames to reduce overhead and increase throughput. It applies only to 802.11ac/n mode. |
| **Enable Wireless Client Connectivity Check and Auto Reconnect** | Periodically checks the wireless client connectivity by pinging a user-defined IP address. In case of lost connection, performs an auto-reconnection. |
| **Target remote IP to ping** | If you enabled the connectivity check previously, enter a remote IP address to ping.<br>ⓘ \| **IMPORTANT:** Make sure the specified IP address is pingable. |

# Advanced Radio Settings

To set the Advanced Radio Settings:

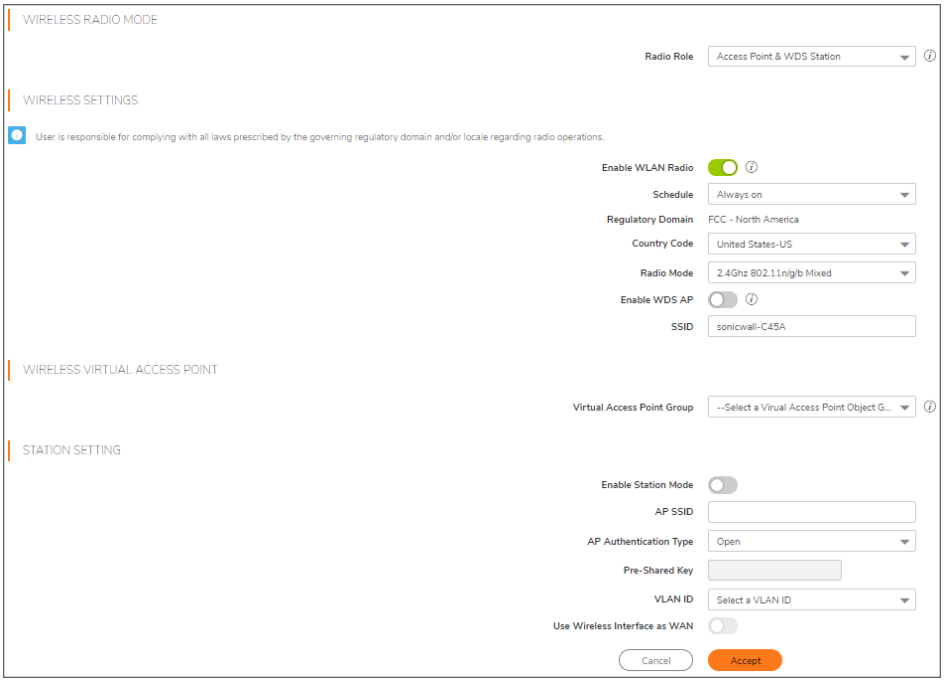
1. Set the **Antenna Diversity**. The default value is **Best**.
2. Select the **Transmit Power** from the drop-down menu:
   - **Full Power** sends the strongest signal on the WLAN. For example, select **Full Power** if the signal is going from building-to-building.
   - **Half (-3 dB)** is recommended for office-to-office within a building.
   - **Quarter (-6 dB)** is recommended for short distance communications.
   - **Eighth (-9 dB)** is recommended for shorter distance communications.
   - **Minimum** is recommended for very short distance communications.
3. Specify the **Fragmentation Threshold (bytes)**. The minimum value can be **256** and the maximum is **2346**. The default is set to the maximum.
4. Set the **RTS Threshold (bytes)**. The minimum is **1** and the maximum is **2346**, which also the default.
5. Click **Accept** to save the settings.
   ⓘ | **NOTE:** You can click **Restore Default Settings** to return to the factory default settings.

# Access Point & WDS Station

When two or more hosts have to be connected with one another over the 802.11 protocol, and the distance is too long for a direct connection to be established, a wireless repeater is used to bridge the gap.

SonicWall wireless security appliances have access point and bridge mode. While in **Access Point & WDS Station** mode, one virtual access point is created as station and can connect to another access point. Other virtual access points works as normal access points. That is to say the unit configured as an **Access Point &**

**WDS Station** works in repeater mode. In this mode, we can also set the virtual interface which the station virtual access point used as a WAN interface.




# Access Point & WDS Station Wireless Settings

**IMPORTANT:** When setting up the wireless appliance as an access point and station, you are responsible for complying with all laws prescribed by the governing regulatory domain and/or locale regarding radio operations.

1. Navigate to **DEVICE | Internal Wireless > Settings**.
2. In the **Radio Role** field, select **Access Point & WDS Station** from the drop-down menu.
3. Toggle **Enable WLAN Radio** to enable it. This provides clean wireless access to your mobile users. The WLAN radio is enabled by default.
4. In the **Schedule** field, select the time that WLAN radio is active from the drop-down menu. The Schedule list displays the schedule objects you create and manage in the **OBJECT | Match Objects > Schedules** page in addition to the system-supplied options. The default value is **Always on**.
5. In the **Country Code** field, select the country in which the appliance is being used. The country code determines which regulatory domain the radio operation falls under.
6. In the **Radio Mode** field, select your preferred radio mode from the drop-down menu.
7. Toggle **Enable WDS AP** option to enable it. This allows the WDS client to connect to this device as an access point.

8. Validate that the **SSID** field is filled in correctly. It is given a default value of **sonicwall-** plus the last four characters of the BSSID; for example, *sonicwall-C587*. The SSID can be changed to any alphanumeric value with a maximum of 32 characters.
9. Click **Accept** to save the settings.

# Wireless Virtual Access Point

If using wireless virtual access points, select a **Virtual Access Point Group** from the drop-down menu in the Wireless **Virtual Access Point** section. Or you can select a VAP group previously defined.

When done with all Access Point settings, click **Accept** to save the settings.

# Station Setting

To configure the station settings:

1. In the **DEVICE | Internal Wireless > Settings** page, with the **Radio Role** set to **Access Point & WDS Station**, scroll down to the **STATION SETTING** section.
2. Toggle **Enable Station Mode** to enable it.
3. Enter the **AP SSID** in the field provided. This is the access point name that users will see when connecting.
4. Select the **AP Authentication Type** from the drop-down menu. Choose from:
    - **OPEN**
    - **WPA2-AUTO-PSK**
    - **WPA3-PSK**
5. If a WPA authentication type is selected, type in a **Pre-Shared Key**.
6. Select a **VLAN ID** from the drop-down menu. To appear in the list, the VLAN ID must already have been created. The VLAN allows the internal wireless radio to identify which traffic belongs to this subnet. You can create VLAN interfaces in the **NETWORK | System > Interfaces** page by clicking **Add Interface** at the top of the **Interface Settings** screen.
7. Toggle **Use Wireless Interface as WAN** to enable access outside your local network. This option changes the wireless interface to a WAN zone interface that can provide WAN access.
8. Click **Accept** to save the settings.

2

# Security

On the **DEVICE | Internal Wireless > Security** page, you configure the authentication and encryption settings for your wireless appliances. Different options are shown depending on the type of authentication you select.

**Topics:**


- About Authentication
- Configuring the WEP Settings
- Configuring WPA3/WPA2/WPA PSK Settings
- Configuring WPA3/WPA2/WPA EAP Settings


## About Authentication

The authentication types are described in the following table:

**AUTHENTICATION TYPES**

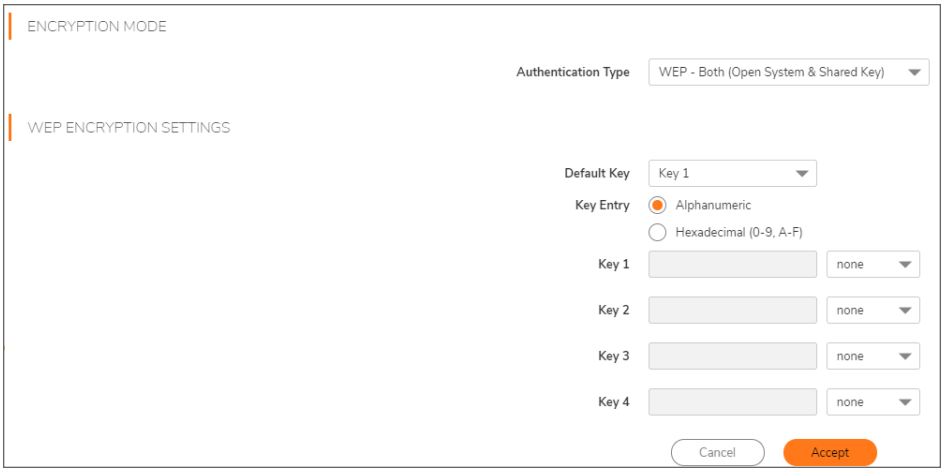
| Type | Features and use |
|---|---|
| WEP (Wired Equivalent Protocol) | • Protects data over wireless networks<br>• Provides no protection past the SonicWall appliance<br>• Provides minimum protection for transmitted dat<br>• Uses a static key for encryption<br>• Useful for older legacy devices, PDAs, wireless printers<br>• Not recommended for deployments needing a high degree of security |

| Type | Features and use |
| --- | --- |
| WPA (Wi-Fi Protected Access) | • Good security (uses TKIP)<br>• For use with trusted corporate wireless clients<br>• Transparent authentication with Windows log-in<br>• No client software needed in most cases<br>• Requires a separate authentication protocol, such as RADIUS to authenticate the users<br>• Uses a dynamic key<br>ⓘ **NOTE:** This option is only visible when it has been enabled on the diagnostics page. |
| WPA2 (Wi-Fi Protected Access, v2) | • Best security (uses AES)<br>• For use with trusted corporate wireless clients<br>• Transparent authentication with Windows log-in<br>• Client software install might be necessary in some cases<br>• Supports 802.11i WPA/WPA2 EAP authentication mode<br>• No backend authentication needed after first log-in (allows for faster roaming)<br>• Supports two protocols for storing and generating keys: PSK (Pre-Shared Key) and EAP (Extensible Authentication Protocol)<br>ⓘ **NOTE:** EAP support is only available in Access Point Mode (selected on the **DEVICE \| Internal Wireless > Settings** page). EAP support is not available in Bridge Mode. |
| WPA2-AUTO | • Tries to connect using WPA2 security<br>• If the client is not WPA2 capable, the connection defaults to WPA |
| WPA3 | • WPA3 is a WFA security standard for personal and enterprise networks<br>• It improves Wi-Fi security by using modern security algorithms and stronger cipher suites.<br>• Supports the following protocols for storing and generating keys: PSK (Pre-Shared Key), EAP (Extensible Authentication Protocol), and OWE (opportunistic wireless encryption) |
| WPA3/WPA2 | • Tries to connect using WPA3 security<br>• If the client is not WPA3 capable, the connection defaults to WPA2 |

| Type | Features and use |
|---|---|
| WPA3-EAP-192B | • The 192-bit security mode offered by WPA3-Enterprise ensures the right combination of cryptographic tools are used and sets a consistent baseline of security within a WPA3 network.<br>• Uses extensible authentication protocol. |

# Configuring the WEP Settings

The options shown in the below image can be set when one of the WEP options is selected for the **Authentication Type**.




To configure the wireless appliance for WEP authentication:

1. Navigate to **DEVICE | Internal Wireless > Security** page.
2. Select the appropriate authentication type from the **Authentication Type** drop-down menu.
   - **WEP - Both (Open System & Shared Key)** (default): The Default Key assignments are not important as long as the identical keys are used in each field.
   - **Open**: In open-system authentication, the firewall allows the wireless client access without verifying its identity. All Web Encryptions Settings are grayed out an cannot be selected.
   - **WEP -Shared key**: Uses WEP and requires a shared key to be distributed to wireless clients before authentication is allowed. If Shared Key is selected, then the Default Key assignment is important.
3. From the **Default Key** drop-down menu, select which key is the default key: **Key 1**, **Key 2**, **Key 3**, or **Key**.
4. From the **Key Entry** options, select if your keys are **Alphanumeric** or **Hexadecimal (0-9, A-F)**.

5. Enter up to four keys in the designated fields. For each key, select whether it is **64 bit**, **128 bit**, or **152 bit**. The higher the bit number, the more secure the key is. Refer to the following table to see how many characters each type of key requires.

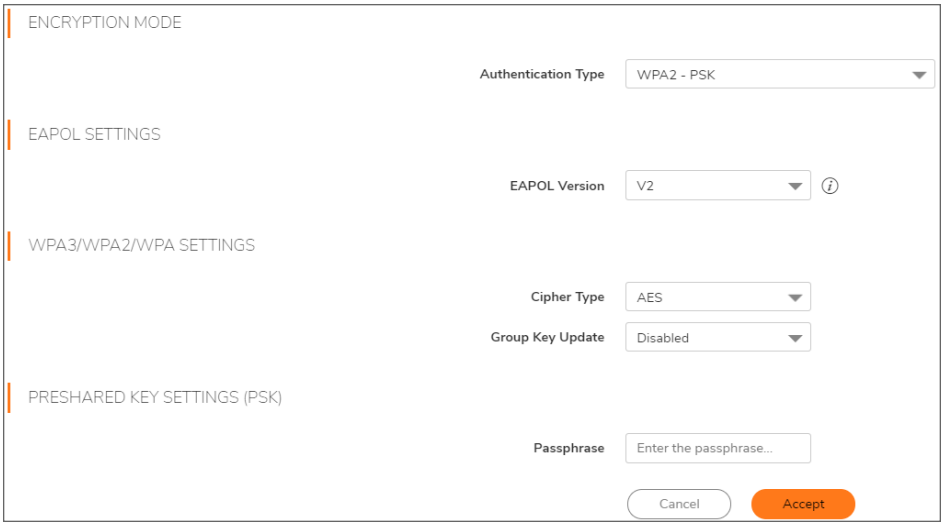
**KEY TYPES**

| Key Type | WEP - 64-bit | WEP - 128-bit | WEP - 152-bit |
|---|---|---|---|
| Alphanumeric | 5 characters | 13 characters | 16 characters |
| Hexadecimal (0-9, A-F) | 10 characters | 26 characters | 32 characters |

6. Click **Accept**.

# Configuring WPA3/WPA2/WPA PSK Settings

The settings shown in he below image can be defined when one of the WPA PSK options is selected for the **Authentication Type**.



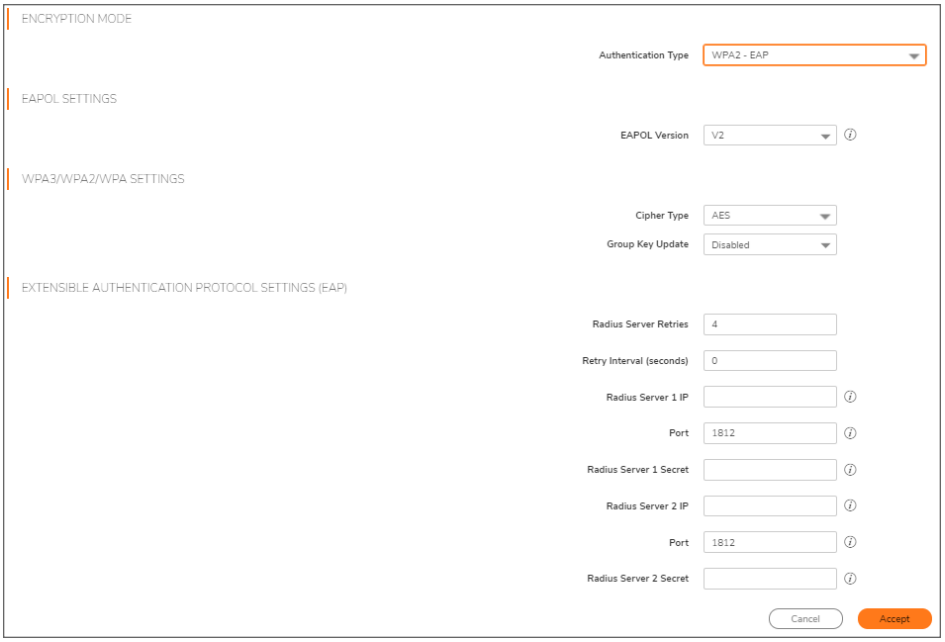

To configure wireless appliance for WPA authentication with a preset shared key:

1. Navigate to the **DEVICE | Internal Wireless > Security** page.
2. Select the appropriate authentication type from the **Authentication Type** drop-down menu.
   - **WPA2 - PSK** : Connects using WPA2 and a preset authentication key.
   - **WPA2 - Auto - PSK** : Automatically tries to connect using WPA2 and a preset authentication key, but falls back to WPA if the client is not WPA2-capable.
   - **WPA3 - PSK** : Connects using WPA3 and a preset authentication key.
   - **WPA3/WPA2 - PSK** : Automatically tries to connect using WPA3 and a preset authentication key, but falls back to WPA2 if the client is not WPA3-capable.

3. Select the **EAPOL Version** setting from the drop-down menu:
    - **V2** (default)—Selects version 2. This provides better security than version 1, but might not be supported by some wireless clients.
    - **V1**—Selects version 1 of the protocol.
4. In **WPA3/WPA2/WPA Settings** section, specify these settings:
    - **Cipher Type**—Select TKIP. *Temporal Key Integrity Protocol (TKIP)* is a protocol for enforcing key integrity on a per-packet basis, but it is less secure and has lower throughput. AES and AUTO are also Cipher type options.
    - **Group Key Update**—Specifies when the SonicWall security appliance updates the key. Select **By Timeout** to generate a new group key after an interval specified in seconds; this is the default. Select **Disabled** when using a static key.
    - **Interval**—If you selected **By Timeout** in the **Group Key Update** field, enter the number of seconds before WPA automatically generates a new group key. The default is **86400** seconds. If you selected **Disabled** for **Group Key Update**, this option is not displayed.
5. In the **Passphrase** field, enter the passphrase from which the key is generated.
6. Click **Accept** to save and apply your settings.

# Configuring WPA3/WPA2/WPA EAP Settings

The settings shown in the below image can be defined when one of the WPA EAP options is selected for the **Authentication Type**.



***To configure wireless appliance for WPA authentication:***

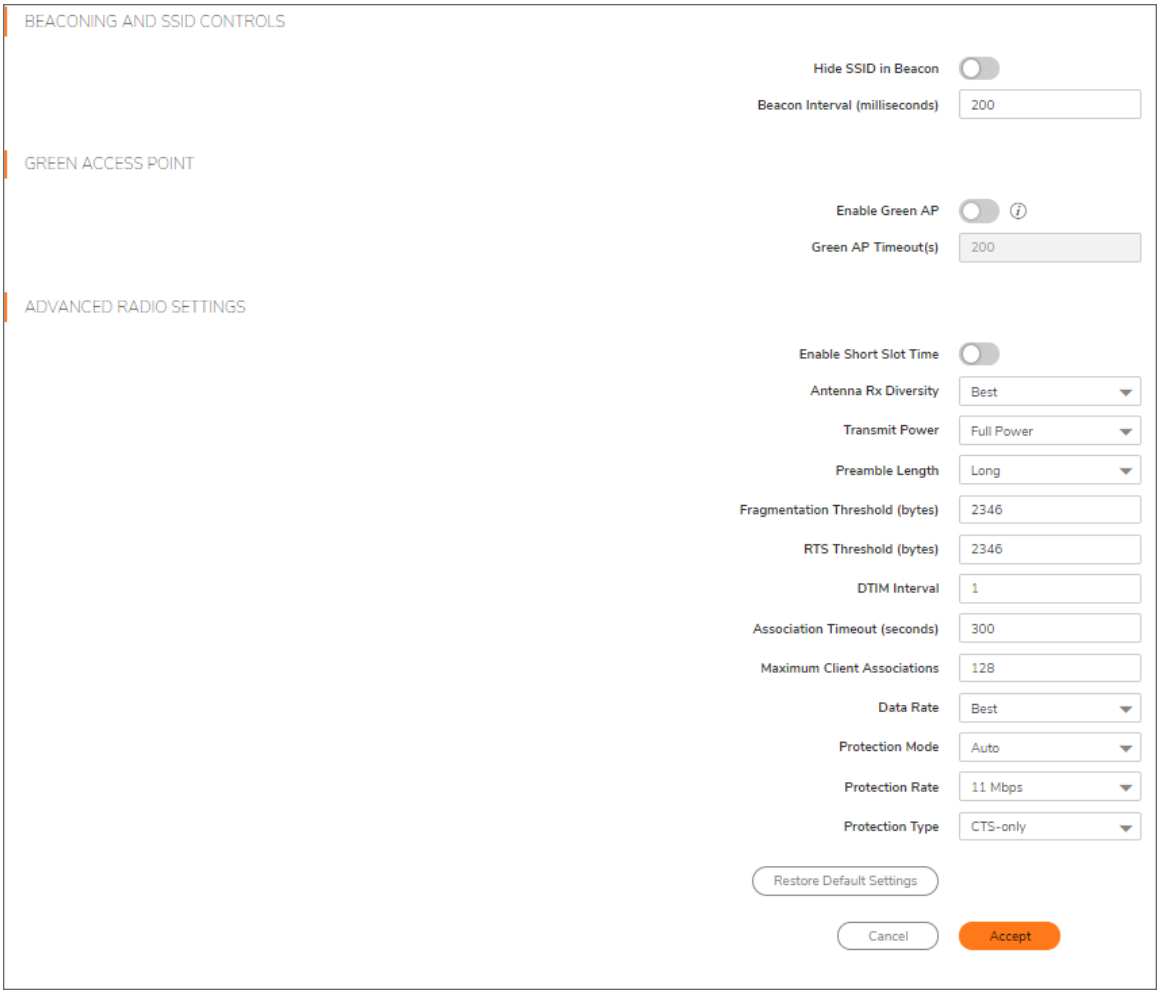
1. Navigate to **DEVICE | Internal Wireless > Security** page.
2. Select the appropriate authentication type from the **Authentication Type** drop-down menu.
   - **WPA2 - EAP** : Connects using WPA2 and an extensible authentication protocol.
   - **WPA2 - Auto - EAP** : Automatically tries to connect using WPA2 and an extensible authentication protocol, but falls back to WPA if the client is not WPA2-capable.
   - **WPA3 - EAP** : Connects using WPA3 and an extensible authentication protocol.
   - **WPA3/WPA2 - EAP** : Automatically tries to connect using WPA3 and a preset authentication key, but falls back to WPA2 if the client is not WPA3-capable.

     ⓘ **NOTE:** EAP support is available when the **Radio Role** includes **Access Point** mode, but not when **Radio Role** is set to **Wireless WDS Station** alone.
3. Select the EAPOL Version setting from the drop-down menu:
   - **V1**—Selects the extensible authentication protocol over LAN version 1.
   - **V2**—Selects the extensible authentication protocol over LAN version 2. This provides better security than version 1, but might not be supported by some wireless clients.
4. In **WPA3/WPA2/WPA Settings** section, specify these settings:
   - **Cipher Type**—Select TKIP. *Temporal Key Integrity Protocol (TKIP)* is a protocol for enforcing key integrity on a per-packet basis, but it is less secure and has lower throughput. AES and AUTO are also Cipher type options.
   - **Group Key Update**—Specifies when the SonicWall security appliance updates the key. Select **By Timeout** to generate a new group key after an interval specified in seconds; this is the default. Select **Disabled** when using a static key.
   - **Interval**—If you selected **By Timeout** in the **Group Key Update** field, enter the number of seconds before WPA automatically generates a new group key. The default is **86400** seconds. If you selected **Disabled** for **Group Key Update**, this option is not displayed.
5. In the **Extensible Authentication Protocol Settings (EAP)** section, specify these settings:
   - **Radius Server Retries**—Enter the number of authentication retries the server attempts. The default is 4.
   - **Retry Interval (seconds)**—Enter the delay the server is to wait between retries. The default is 0 (no delay).
   - **Radius Server 1 IP and Port**—Enter the IP address and port number for your primary RADIUS server.
   - **Radius Server 1 Secret**—Enter the password for access to the primary RADIUS server.
   - **Radius Server 2 IP and Port**—Enter the IP address and port number for your secondary RADIUS server, if you have one.
   - **Radius Server 2 Secret**—Enter the password for access to the secondary RADIUS server.
6. Click **Accept** to apply your WPA3/WPA2 EAP settings.

3

# Advanced

On the **DEVICE | Internal Wireless > Advanced** page, you can customize a range of features for your wireless appliance. This page is only accessible when the firewall is acting as an access point.



**Topics:**


- Beaconing and SSID Controls
- Green Access Point
- Advanced Radio Settings
- Configurable Antenna Diversity


# Beaconing and SSID Controls

To configure the Beaconing and SSID Controls:

1. Navigate to the **DEVICE | Internal Wireless > Advanced** page.
2. Toggle **Hide SSID in Beacon** option, which suppresses broadcasting of the SSID name and disables responses to probe requests. Enabling this option helps prevent your wireless SSID from being seen by unauthorized wireless clients. This setting is disabled by default.
3. Type a value, in milliseconds, for the **Beacon Interval**. Decreasing the interval time makes passive scanning more reliable and faster because Beacon frames announce the network to the wireless connection more frequently. The default interval is 200 milliseconds.
4. Click **Accept** to apply your changes. Click **Restore Default Settings** to return to the default settings.

# Green Access Point

A "green" access point uses power efficiently to reduce wasteful energy consumption and help protect the environment.

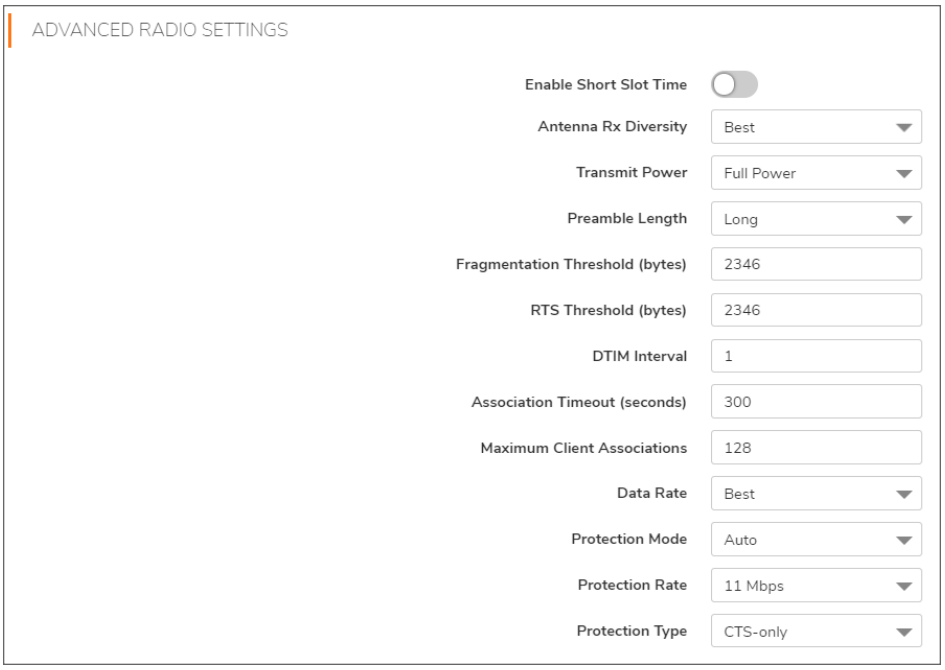
To configure power efficiency:

1. To increase power efficiency, toggle the **Enable Green AP** option on the **DEVICE | Internal Wireless > Advanced** page. This setting is disabled by default.
2. In the **Green AP Timeout(s)** field, enter the number of seconds to wait after no clients are associated

before entering power saving mode. The range is 20 to 65535. The default is 20 seconds.

3. Click **Accept** to apply your changes. Click **Restore Default Settings** to return to the default settings.

# Advanced Radio Settings




To configure advanced radio settings:

1. Toggle the **Enable Short Slot Time** option on the **DEVICE | Internal Wireless > Advanced** page to increase performance if you do not expect 802.11b traffic. 802.11b is not compatible with a short slot time. This setting is disabled by default.
2. From the **Antenna Rx Diversity** drop-down menu, select which antenna the wireless security appliance uses to send and receive data. For more information about antenna diversity, refer to Configurable Antenna Diversity. The default is **Best**.
3. From the **Transmit Power** drop-down menu, select:
    - **Full Power** to send the strongest signal on the WLAN. For example, select **Full Power** if the signal is going from building-to-building.
    - **Half (-3 dB)** is recommended for office-to-office within a building.
    - **Quarter (-6 dB)** is recommended for shorter distance communications.
    - **Eighth (-9 dB)** is recommended for shorter distance communications.
    - **Minimum** is recommended for very short distance communications.

4. From the **Preamble Length** drop-down menu, select **Short** or **Long**. Short is recommended for efficiency and improved throughput on the wireless network, but is not supported by 802.11b. The default is **Long**.
5. Specify the **Fragmentation Threshold (bytes)**. The minimum is 256; the maximum is 2346, and the default is **2346**.

   You can fragment wireless frames to increase reliability and throughput in areas with RF interference or poor wireless coverage. Lower threshold numbers produce more fragments. Increasing the value means that frames are delivered with less overhead, but a lost or damaged frame must be discarded and retransmitted.
6. Specify the request-to-send (RTS) threshold in the **RTS Threshold (bytes)** field. The minimum is 1, the maximum is 2347, and the default is **2346**.

   This field sets the threshold for a packet size (in bytes) at which a RTS is sent before packet transmission. Sending an RTS ensures that wireless collisions do not take place in situations where clients are in range of the same access point, but might not be in range of each other. If network throughput is slow or a large number of frame retransmissions is occurring, decrease the RTS threshold to enable RTS clearing.
7. Specify the DTIM (Delivery of Traffic Indication Message) interval in the **DTIM Interval** field. The minimum is 1, the maximum is 256, and the default is **1**.

   For 802.11 power-save mode clients of incoming multicast packets, the DTIM interval specifies the number of beacon frames to wait before sending a DTIM. Increasing the DTIM Interval value allows you to conserve power more effectively.
8. Enter the number of seconds for client association in the **Association Timeout (seconds)** field. The default is **300** seconds, and the allowed range is from 60 to 36000 seconds. If your network is very busy, you can increase the timeout by increasing the number of seconds in this field.
9. Enter the **Maximum Client Associations** for each access point using this profile. The minimum value is 1; the maximum is 128, and the default is **128**. This setting limits the number of stations that can connect wirelessly at one time.
10. From the **Data Rate** drop-down menu, select the speed at which the data is transmitted and received. **Best** automatically selects the best rate available in your area given interference and other factors. Or you can manually select a data rate from the options that range from **1 Mbps** to **54 Mbps**.
11. From the **Protection Mode** drop-down menu, select the protection mode: **None**, **Always**, or **Auto**.

    Protection can decrease collisions, particularly where you have two overlapping access points. However, it can slow down performance. **Auto** is probably the best setting, as it engages only in the case of overlapping access points.
12. Choose the **Protection Rate** from the drop-down menu: **1 Mbps**, **2 Mbps**, **5 Mbps**, or **11 Mbps**. The protection rate determines the data rate when protection mode is on. The slowest rate offers the greatest degree of protection, but also the slowest data transmission rate.
13. From the **Protection Type** drop-down menu, select the type of handshake used to establish a wireless connection: **CTS-only** (default) or **RTS-CTS**.

    ⓘ | **NOTE:** 802.11b traffic is only compatible with **CTS**.
14. Click **Accept** to apply your changes. Click **Restore Default Settings** to return to the default settings.

# Configurable Antenna Diversity

The wireless SonicWall security appliances employ dual 5 dBi antennas running in diversity mode. The default implementation of diversity mode means that one antenna acts as a transmitting antenna, and both antennas act as potential receiving antennas. As radio signals arrive at both antennas on the secure wireless appliance, the strength and integrity of the signals are evaluated, and the best received signal is used. The selection process between the two antennas is constant during operation to always provide the best possible signal. To allow for external (higher gain uni-directional) antennas to be used, antenna diversity can be disabled.

The **Antenna Rx Diversity** setting determines which antenna the wireless security appliance uses to send and receive data. **Best** is the default setting, and is currently the only option on SonicWall TZ270W, TZ370W, TZ470W and TZ570W. When **Best** is selected, the wireless security appliance automatically selects the antenna with the strongest, clearest signal.

4

# MAC Filter List

Wireless networking provides native MAC filtering capabilities that prevent wireless clients from authenticating and associating with the wireless security appliance. If you enforce MAC filtering on the WLAN, wireless clients must provide you with the MAC address of their wireless networking card. The SonicOS wireless MAC Filter List allows you to configure a list of clients that are allowed or denied access to your wireless network. Without MAC filtering, any wireless client can join your wireless network if they know the SSID and other security parameters, thus allowing them to “break into” your wireless network.

**Topics:**


- Deployment Considerations
- Configuring MAC Filter List


## Deployment Considerations

Consider the following when deploying the MAC Filter List:

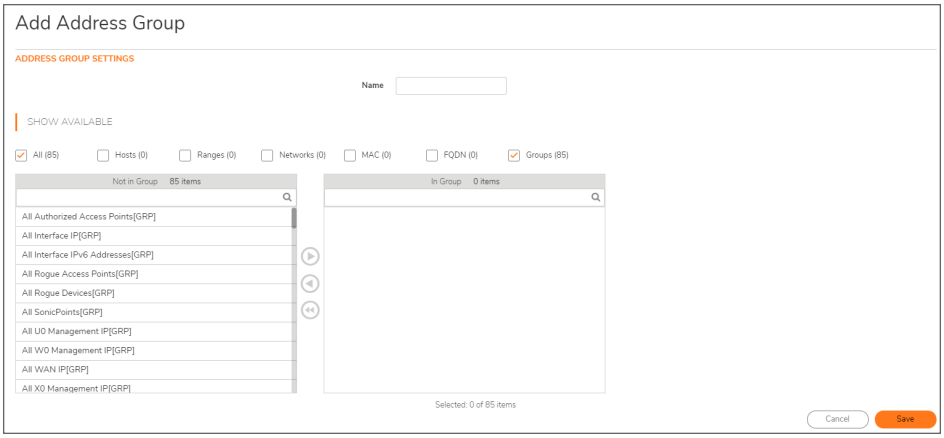
- The MAC Filter List can be enabled on the **DEVICE | Internal Wireless > MAC Filter List** page if a virtual access point (VAP) group is not configured. If a VAP group is configured, the MAC Filter function needs to be enabled on the VAP object.
- The virtual access point can configure its MAC Filter List or inherit global settings configured on the **DEVICE | Internal Wireless > MAC Filter List** page.

## Configuring MAC Filter List

To configure the MAC Filter List:

1. Navigate to the **DEVICE | Internal Wireless > MAC Filter List** page.
2. Click **Enable MAC Filter List**. This setting is disabled by default.
3. From the **Allow List** drop-down menu, select the address group you want to allow: **All MAC Addresses** (default), **Default ACL Allow Group**, or a group you created.

4. From the **Deny List** drop-down menu, select the address group you want to deny: **No MAC Addresses** (default), **Default ACL Deny Group**, or a group you created.
5. If you want to add new address objects to the allow and deny lists, select **Create New MAC Address Object Group...** from either the **Allow List** or **Deny List** drop-down menu.




   a. In the **Name**: text field, enter a name for the new group.
   b. In the left column, select the group(s) or individual address object(s) you want to allow or deny. You can use **Ctrl+click** to select more than one item at a time.
   c. Click the **Right Arrow** to add the items to the group.
   d. Click **Save**. The address displays in the drop-down menu for selection.
6. Click **Accept**.

5

# IDS - Wireless Intrusion Detection Service

Wireless Intrusion Detection Services (IDS) greatly increase the security capabilities of the SonicWall wireless security appliances. They enable recognition of, and countermeasures against, Rogue Access Points. This is the most common type of illicit wireless activity.

## Access Point IDS

When the **Radio Role** of the wireless security appliance is set to **Access Point** mode, Rogue Access Point detection, by default, acts in a passive mode (passively listening to other Access Point Beacon frames only on the selected channel of operation).

A **Scan** momentarily changes the Radio Role to allow the wireless security appliance to perform an active scan, and might cause a brief loss of connectivity for associated wireless clients. While in Access Point mode, the **Scan** function should only be scheduled when no clients are actively associated, or if the possibility of client interruption is acceptable.

## Rogue Access Points

Rogue Access Points have emerged as one of the most serious and insidious threats to wireless security. In general terms, an access point is considered rogue when it has not been authorized for use on a network. The convenience, affordability and availability of non-secure access points, and the ease with which they can be added to a network creates a easy environment for introducing rogue access points. The real threat emerges in a number of different ways, including unintentional and unwitting connections to the rogue device, transmission of sensitive data over non-secure channels, and unwanted access to LAN resources. While this doesn't represent a deficiency in the security of a specific wireless device, it is a weakness to the overall security of wireless networks.

The security appliance can alleviate this weakness by recognizing rogue access points potentially attempting to gain access to your network. It does this in two ways: active scanning for access points on all 2.4Ghz and 5GHz channels, and passive scanning (while in Access Point mode) for beaconing access points on a single channel of operation.

See also:

- Configuring IDS Settings
- Discovered Access Points

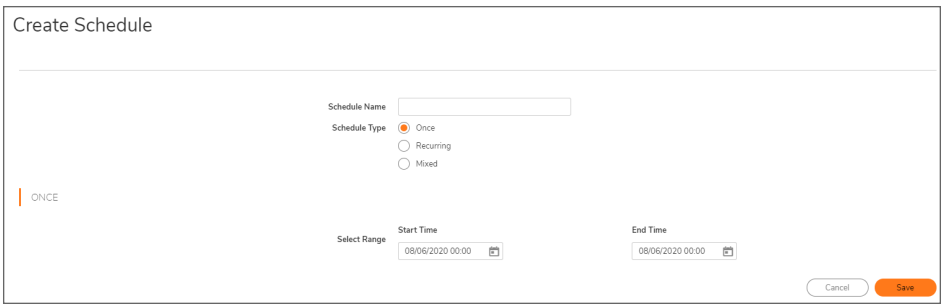
# Configuring IDS Settings

To schedule when to run an IDS scan, choose an option from the **Schedule IDS Scan** drop-down menu:

- **Disabled** - This is the default. IDS scans do not take place when Disabled is selected.
- **Create New Schedule** - The **Add Schedule** dialog displays and you can create a custom scheduled as described later in this section.
- **Work Hours**
- **M-T-W-TH-F 08:00 to 17:00**
- **After Hours**
- **SU-SA 00:00 to 24:00**
- **M-T-W-TH-F 17:00 to 24:00**
- **M-T-W-TH-F 00:00 to 08:00**
- **Weekend Hours**
- **AppFlow Report Hours**
- **SU-M-T-W-TH-F-SA 00:00 to 24:00**
- **App Visualization Report Hours**
- **TSR Report Hours**
- **SU-M-T-W-TH-F-SA 00:00 to 00:01**
- **Cloud Backup Hours**
- **SU-M-T-W-TH-F-SA 02:00 to 03:00**
- **Guest Cycle Quota Update**
- **SU-M-T-W-TH-F-SA 00:00 to 00:15**

To create a new schedule:

1. In the **Schedule IDS Scan** field, select **Create New Schedule**.




2. Type a descriptive name into the **Schedule Name** field.
3. Select **Once**, **Recurring**, or **Mixed** for the **Schedule Type**:
    - With **Once**, you schedule a one-time event and only **Start Time** and **End Time** fields are active.
        - In the **Once** section, use the drop-down menus to schedule the start and end times for your IDS scan.
    - With **Recurring**, the display changes to show the fields needed to schedule a recurring event.
        - Under **Select Day**, choose the **Day(s)** for your scan. You can also enable **Select All**.
        - Enter a **Start Time**, using 24-hour format
        - Enter a **Stop Time**, using 24-hour format
        - Click **Add** to add those parameters to the **Schedule List**.
        - To delete an item from the list, click the **Delete this Schedule** button on the item's row. Click the **Delete All** button at the top to clear the **Schedule List**.
    - With **Mixed**, you schedule a mixed event and all fields for **Once** and **Recurring** are active.
4. Click **Save** to add this schedule to the **Schedule IDS Scan** drop-down list.

# Discovered Access Points

Active scanning occurs when the wireless security appliance starts up and any time **Scan** is clicked at the top of the table on the **DEVICE | Internal Wireless > IDS > Discovered Access Points** screen. The appliance scans the environment and identifies other wireless devices in the vicinity. The Note above the table displays the number of Access Points found and the time, in days, hours, minutes, and seconds, since the last scan.

To refresh the entries in the Discovered Access Points table, click **Refresh**. To do an immediate scan, click **Scan**.

**IMPORTANT:** The **Scan** feature causes a brief disruption in service when operating in Access Point Mode. This interruption manifests itself as follows:

- Non-persistent, stateless protocols (such as HTTP) should not exhibit any ill-effects.
- Persistent connections (protocols such as FTP) are impaired or severed.

If this is a concern, wait to use **Scan** at a time when no clients are active or until the potential for disruption becomes acceptable.

The table on the **Discovered Access Points** page displays information on every access point (including wireless TZ appliances) that can be detected by the wireless security appliance:

| Field | Description |
|---|---|
| MAC Address (BSSID) | The MAC address of the radio interface of the detected access point. |
| SSID | The radio SSID of the access point. |
| Channel | The radio channel used by the access point. |
| Authentication | The type of authentication. |
| Cipher | The cipher used. |
| Vendor | The manufacturer of the access point. |
| Signal Strength | The strength of the detected radio signal. |
| Max Rate | The fastest allowable data rate for the access point radio. |
| Authorize | Click the edit icon in the **Authorize** column to add the access point to the address object group of authorized access points. |

# Authorizing Access Points on Your Network

Access Points detected by the wireless security appliance are regarded as rogues until they are identified to the wireless security appliance as authorized for operation. To authorize an access point, click the **Authorize** icon.

6

# Virtual Access Point

A Virtual Access Point (VAP) is a multiplexed representation of a single physical access point—it presents itself as multiple discrete access points. To wireless LAN clients, each virtual access point appears to be an independent physical access point, when actually only one physical access point exists. Virtual access points allow you to control wireless user access and security settings by setting up multiple custom configurations on a single physical interface. Each of these custom configurations acts as a separate (virtual) access point and can be grouped and enforced on a single internal wireless radio.

The benefits of using the VAP includes:

- **Radio Channel Conservation**—Prevents building overlapped infrastructures by allowing a single physical access point to be used for multiple purposes to avoid channel collision problem. Multiple providers are becoming the norm within public spaces such as airports. Within an airport, for example, it might be necessary to support an FAA network, one or more airline networks, and perhaps one or more wireless ISPs. However, in the US and Europe, 2.4GHz networks can only support three usable (non-overlapping) channels, and in France and Japan only one channel is available. After the channels are utilized by existing access points, additional access points interfere with each other and reduce performance. VAPs conserve channels by allowing a single network to be used for multiple purposes.
- **Wireless LAN Infrastructure Optimization**—Shares the same Wireless LAN infrastructure among multiple providers, rather than building an overlapping infrastructure, to lower down the capital expenditure for installation and maintenance of your WLANs.

**Topics:**

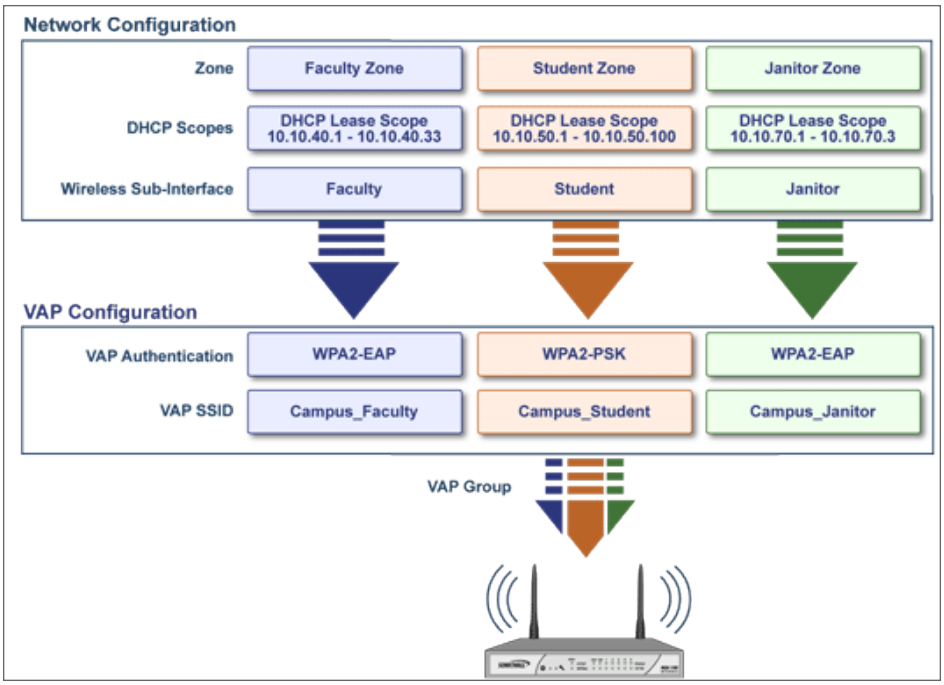

- Wireless Virtual AP Configuration Task List
- Virtual Access Point Profiles
- Virtual Access Point Objects
- Virtual Access Point Groups
- Enabling the Virtual Access Point Group

# Wireless Virtual AP Configuration Task List

A Wireless VAP deployment requires several steps to configure. The following section provides a brief overview of the steps involved:

1. **Network Zone** - The network zone is the backbone of your VAP configuration. Each zone you create has its own security and access control settings, and you can create and apply multiple zones to a single physical interface using wireless subnets. For more information on network zones, refer to the section **OBJECT | Match Objects > Zones** in *SonicOS 7 Match Objects* administration guide.
2. **Wireless Interface** - The W0 interface (and its WLAN subnets) represent the physical connections between your SonicWall network security appliance and the internal wireless radio. Individual zone settings are applied to these interfaces and forwarded to the wireless radio. For more information on wireless interfaces, refer to the section on **NETWORK | System > Interfaces** in the *SonicOS 7 System* administration guide.
3. **DHCP Server** - The DHCP server assigns leased IP addresses to users within specified ranges, known as Scopes. The default ranges for DHCP scopes are often excessive for the needs of most wireless deployments, for instance, a scope of 200 addresses for an interface that only uses 30. Because of this, DHCP ranges must be set carefully in order to ensure the available lease scope is not exhausted. For more information on setting up the DHCP server, refer to the section on **NETWORK | System > DHCP Server** in the *SonicOS 7 System* administration guide.
4. **Virtual Access Point Profiles** - The VAP Profile feature allows for creation of wireless configuration profiles which can be easily applied to new wireless Virtual Access Points as needed. Refer to Virtual Access Point Profiles for more information.
5. **Virtual Access Point** - The VAP Objects feature allows for setup of general VAP settings. SSID and wireless subnet name are configured through VAP Settings. Refer to Virtual Access Point Objects for more information.
6. **Virtual Access Point Group** - The VAP Group feature allows for grouping of multiple VAP objects to be simultaneously applied to a single internal wireless radio. Refer to Virtual Access Point Groups for more information.

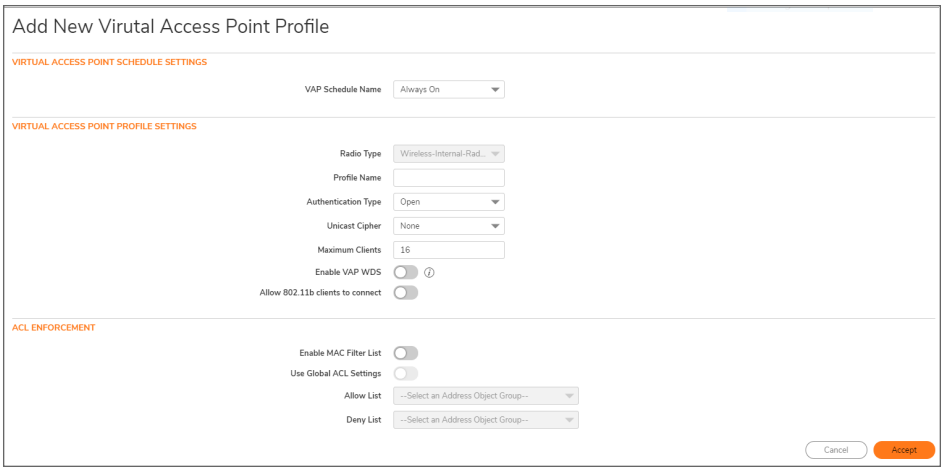
7. **Assign VAP Group to Internal Wireless Radio**- The VAP Group is applied to the internal wireless radio and made available to users through multiple SSIDs. Refer to Enabling the Virtual Access Point Group for more information.




# Virtual Access Point Profiles

A Virtual Access Point Profile allows you to pre-configure and save access point settings in a profile. VAP Profiles allows settings to be easily applied to new Virtual Access Points. Virtual Access Point Profiles are configured from the **DEVICE | Internal Wireless > Virtual Access Point > Virtual Access Point Profiles**. Select the profile name and click the **Edit** icon or click **Add** to create a new Virtual Access Point Profile. Click **Accept** when done.

ⓘ **TIP:** This feature is especially useful for quick setup in situations where multiple virtual access points share the same authentication methods.




**Topics:**


- Virtual Access Point Schedule Settings
- Virtual Access Point Profile Settings
- ACL Enforcement


# Virtual Access Point Schedule Settings

Each Virtual Access Point can have its own schedule associated with it and by extension each profile can have a set schedule defined for it as well.

To associate a schedule with a Virtual Access Point Profile:

1. Navigate to **DEVICE | Internal Wireless > Virtual Access Point > Virtual Access Point Profiles**.
2. Click **Add** if creating a new profile, or select a Virtual Access Point Profile and click on the **Edit** icon if editing an existing profile.
3. In the **VAP Schedule Name** field, select the schedule you want from the options in the drop-down menu.

# Virtual Access Point Profile Settings

To set the Virtual Access Point Profile Settings:

1. Navigate to **DEVICE | Internal Wireless > Virtual Access Point > Virtual Access Point Profiles**.
2. Click **Add** if creating a new profile, or select a Virtual Access Point Profile and click on the **Edit** icon if editing an existing profile.
3. In the **Virtual Access Point Profile Settings** group, set the **Radio Type**. It is set to **Wireless-Internal-Radio** by default. Retain this default setting if using the internal radio for VAP access; it is currently the only supported radio type.

4. In the **Profile Name** field, type a friendly name for this Virtual Access Point profile. Choose something descriptive and easy to remember as you apply this profile to new VAPs.
5. Select the **Authentication Type** from the drop-down menu. Choose from these options:

| Authentication Type | Definition |
|---|---|
| Open | No authentication is specified. |
| Shared | A shared key is used to authenticate WEP encryptions settings. |
| Both | If no shared key is configured, it is same as an open network.<br>If shared key is configured, it means open authentication with encrypted data traffic. |
| WPA2-PSK | Best security used with trusted corporate wireless clients. Transparent authentication with Windows login. Supports fast-roaming feature. Uses pre-shared key for authentication. |
| WPA2-EAP | Best security used with trusted corporate wireless clients. Transparent authentication with Windows login. Supports fast-roaming feature. Uses extensible authentication protocol. |
| WPA2-AUTO-PSK | Tries to connect using WPA2 security, if the client is not WPA2 capable, the connection defaults to WPA. Uses pre-shared key for authentication. |
| WPA2-AUTO-EAP | Tries to connect using WPA2 security, if the client is not WPA2 capable, the connection defaults to WPA. Uses extensible authentication protocol. |
| WPA3-OWE | WPA3 is a WFA security standard for personal and enterprise networks. It improves Wi-Fi security by using modern security algorithms and stronger cipher suites. Uses opportunistic wireless encryption. |
| WPA3-PSK | WPA3 is a WFA security standard for personal and enterprise networks. It improves Wi-Fi security by using modern security algorithms and stronger cipher suites. Uses pre-shared key for authentication. |
| WPA3-EAP | WPA3 is a WFA security standard for personal and enterprise networks. It improves Wi-Fi security by using modern security algorithms and stronger cipher suites. Uses extensible authentication protocol. |
| WPA3/WPA2-PSK | Tries to connect using WPA3 security, if the client is not WPA3 capable, the connection defaults to WPA2. Uses pre-shared key for authentication. |
| WPA3/WPA2-EAP | Tries to connect using WPA3 security, if the client is not WPA3 capable, the connection defaults to WPA2. Uses extensible authentication protocol. |
| WPA3-EAP-192B | The 192-bit security mode offered by WPA3-Enterprise ensures the right combination of cryptographic tools are used and sets a consistent baseline of security within a WPA3 network. Uses extensible authentication protocol. |

The **Unicast Cipher** field is auto-populated based on what authentication type you selected.

ⓘ | **NOTE:** Different setting appear on the page depending upon which option you select.

6. In the **Maximum Clients** field, type in the maximum number of concurrent client connections permissible for this virtual access point.

7. Toggle the **Enable VAP WDS** (Wireless Distribution System) option to enable it. By default, this option is not selected.
8. Toggle the **Allow 802.11b clients to connect** option to enable it. By default, this option is not selected.

   Depending on the **Authentication Type** selected, an additional section with options is added to the Add/Edit Virtual Access Point Profile page.

   - If you selected Both or Shared, refer to WEP Encryption Settings for information on the settings.
   - If you selected an option requiring a pre-shared key (PSK), refer to WPA-PSK / WPA2-PSK Encryption Settings for information on the settings.
   - If you selected an option using the extensible authentication protocol (EAP), refer to RADIUS Server Settings for information on the settings.

# WEP Encryption Settings

If you selected **Both** or **Shared** in **Authentication Type** drop-down menu during the creation of Virtual Access Point Profile, the section **WEP Encryption Settings** appears. WEP settings are commonly shared by virtual access points within a common physical access point.

In the **Encryption Key** field, select **Key 1**, **Key 2**, **Key 3** or **Key 4** from the drop-down menu.

# WPA-PSK / WPA2-PSK Encryption Settings

The **WPA/WPA2-PSK Encryption Settings** section appears when one of the following options for **Authentication Type** is selected in a Virtual Access Point Profile:

- **WPA2-PSK**
- **WPA2-AUTO-PSK**
- **WPA3-PSK**
- **WPA3/WPA2-PSK**

When any of these authentication types are selected, a preshared key is used for authentication. Fill in the values in the following fields:

| Field Name | Description |
|---|---|
| **Pass Phrase** | Type in the shared passphrase users need to enter when connecting with PSK-based authentication. |
| **Group Key Interval** | Type in the time period for which a Group Key is valid. The default value is 86400 seconds. Setting too low of a value can cause connection issues. |

## RADIUS Server Settings

The **RADIUS Server Settings** section appears when one of the following options for **Authentication Type** is selected in a Virtual Access Point Profile:

- **WPA2-EAP**
- **WPA2-AUTO-EAP**
- **WPA3-EAP**
- **WPA3/WPA2-EAP**

When any of these authentication types are selected, an external 802.1x/EAP capable RADIUS server is used for key generation and authentication. Fill in the values in the following fields:

| Field Name | Description |
|---|---|
| **Radius Server Retries** | Enter the number times a user can try to authenticate before access is denied. The default is 4. |
| **Retry Interval (seconds)** | Enter the time period during which retries are valid. The default is 0. |
| **Server 1 IP** | Input the IP address of the primary RADIUS authentication server. |
| **Server 1 Port** | Input the port on which your primary RADIUS authentication server communicates with clients and network devices. The default port is 1812. |
| **Server 1 Secret** | Enter the secret passcode for your primary RADIUS authentication server. |
| **Server 2 IP** | Input the IP address of your backup RADIUS authentication server. |
| **Server 2 Port** | Input the port on which your backup RADIUS authentication server communicates with clients and network devices. The default port is 1812. |
| **Server 2 Secret** | Enter the secret passcode for your backup RADIUS authentication server. |
| **Group Key Interval** | Input the time period (in seconds) during which the group key is enforced. The default value is 86400. |

# ACL Enforcement

Each Virtual Access Point can support an individual Access Control List (ACL) to provide more effective authentication control. The Wireless ACL feature works in tandem with the wireless MAC Filter List currently available on SonicOS. Using the ACL Enforcement settings, users are able to enable or disable the MAC Filter List, configure the Allow List, and configure the Deny list.

Each VAP can have its own MAC Filter List settings or use the global settings. In Virtual Access Point (VAP) mode, each VAP of this group shares the same MAC Filter List settings.

To enable MAC Filter List enforcement:

1. Toggle **Enable MAC Filter List** option to enable it. When the MAC filter list is enabled, the other settings are also enabled so you can set them.

2. Toggle **Use Global ACL Settings** option to enable it. This associates the Virtual Access Point with the already existing MAC Filter List settings for the SonicWall network security appliance. Note you cannot edit the Allow or Deny Lists with this option enabled.
3. In the **Allow List**, select an address object group from the drop-down menu. This identifies the MAC addresses of the devices allowed to access the virtual access point.

   Choose **Create MAC Address Object Group** if you want to create a new address object group containing MAC addresses of the devices that are allowed access. Refer to the *SonicOS 7 Match Objects* administration guide for information on how to create an address object group.
4. In the **Deny List**, select an address object group from the drop-down menu. This identifies the MAC addresses of the devices denied access to the virtual access point.

   Choose **Create MAC Address Object Group** if you want to create a new address object group containing MAC addresses of the devices that are denied access. Refer to the *SonicOS 7 Match Objects* administration guide for information on how to create an address object group.
5. Click **Accept** when done.

# Virtual Access Point Objects

Virtual Access Point general and advanced settings are available on the **DEVICE | Internal Wireless > Virtual Access Point > Virtual Access Point Objects** page. You can set the SSID, VLAN ID, schedule, profile, authentication type, maximum clients and other settings when adding or editing a VAP Object.

# VAP General Settings

To define the Virtual Access Point General settings:

1. Navigate to the **DEVICE | Internal Wireless > Virtual Access Point > Virtual Access Point Objects** page.
2. To edit an existing virtual access point, click the **Edit** icon for that access point. To create a new access point, click on **Add**.
3. On the **General** screen, in the **Name** field, create a friendly name for the access point.
4. In the **SSID** field, type in a unique name. This name is a unique identifier attached to the packet header. It is case sensitive and can be up to 32 alphanumeric characters. The SSID is seen when users look for a Wi-Fi connection.

5. Select the **VLAN ID** from the drop-down menu. To appear in the list, the VLAN ID must already have been created. The VLAN allows the internal wireless radio to identify which traffic belongs to this subnet. You can create VLAN interfaces in the **NETWORK | System > Interfaces** page by clicking **Add Interface** at the top of the **Interface Settings** screen.
6. Toggle **Enable Virtual Access Point** option to enable it.
7. Toggle **Enable SSID Suppress** option if you do not want your SSID to be seen by unauthorized wireless clients. When enabled, it suppresses the broadcasting of the SSID name and disables responses to probe requests.
8. Click **Accept**.

# VAP Advanced Settings

The **Advanced** settings screen provides schedule settings, authentication and encryption settings, and other settings for this virtual access point. The options are the same as those you define for a Virtual Access Point Profile.

To define the Virtual Access Point Advanced settings:

1. Navigate to the **DEVICE | Internal Wireless > Virtual Access Point > Virtual Access Point Objects** page.
2. To edit an existing virtual access point, click the **Edit** icon for that access point. To create a new access point, click on **Add**.
3. Click **Advanced**.
4. In the **Virtual Access Point Schedule Settings** section, set the schedule for when this VAP is active and available.
5. In the **Virtual Access Point Profile Settings** section, choose a **Profile Name** from the drop-down menu. All the settings for that profile are auto-filled from the profile.
6. If you do not want to use a profile, leave the Profile Name set to **No Profile** and fill in the remaining fields as described in Virtual Access Point Profiles.
7. Click **Accept**.

# Virtual Access Point Groups

The Virtual Access Point Groups feature allows multiple VAP objects to be grouped and simultaneously applied to your internal wireless radio. Virtual Access Point Groups are configured on the **DEVICE | Internal Wireless > Virtual Access Point > Virtual Access Point Groups** page.

ⓘ **NOTE:** Multiple virtual access points need to be set up before you can create a Virtual Access Point Group. If you have only one access point, it is automatically added to the default group Internal AP Group.

To create a Virtual Access Point Group:

1. Navigate to the **DEVICE | Internal Wireless > Virtual Access Point > Virtual Access Point Groups** page.
2. To edit an existing virtual access point group, click the **Edit** icon for that group, or to add a new group click **Add**.
3. To add an object to the group, select the object you want to add from the **Available Virtual AP Objects** list and click the right arrow.
4. To delete an object from the group, select the object you want to delete from the **Member of Virtual AP Group** list and click the left arrow.
5. Click **Accept** when done.

# Enabling the Virtual Access Point Group

After your virtual access points are configured and added to a VAP group, that group must be applied to the internal wireless radio and made available to the users.

To make the group available:

1. Navigate to the **DEVICE | Internal Wireless > Virtual Access Point** page.
2. In the **Virtual Access Point Groups** screen, click the triangle icon to expand the Internal AP Group or other group which you want to enable.
3. Click **Edit** icon in the row for the VAP and select **Enable Virtual Access Point** in the Edit dialog.
4. Click **Accept** to update the configuration.

7

# 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 Internal Wireless Administration Guide
Updated - July 2021
Software Version - 7
232-005336-10 Rev C

Copyright © 2021 SonicWall Inc. All rights reserved.

The information in this document is provided in connection with SonicWall and/or its affiliates' products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, SONICWALL AND/OR ITS AFFILIATES ASSUME NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL SONICWALL AND/OR ITS AFFILIATES BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF SONICWALL AND/OR ITS AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SonicWall and/or its affiliates make no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. and/or its affiliates do not make any commitment to update the information contained in this document.

For more information, visit https://www.sonicwall.com/legal.

## End User Product Agreement

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

## Open Source Code

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

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