SonicWall® Global Management System Access Points

Administration

SONICWALL®

Contents

1

Using the Access Points Dashboard

For SonicWave and SonicPoint AC devices, **Access Points > Dashboard** uses charts and graphs to visualize the data related to the access points that are a part of your infrastructure. You can display both real-time status and historical status, as well as each client's rate, OS type and host name. It also displays status of the SonicWave and SonicPoint devices and provides information to help with monitoring and problem diagnosis.

Topics:

Feature Limitations

SonicWave and SonicPoint AC device status is displayed on when the device is managed by a SonicWall firewall. Both the firewall and the access point needs to be functional or no valid data can be exchanged. SonicWave access points retain a seven-day history of the dashboard data at all times. However, because of memory limitations, SonicPoint AC devices lose all history data when they are rebooted.

Access Point Snapshot

Two graphs are shown in the **Access Point Snapshot** section of the **Access Points > Dashboard**:

Access Point Online/Offline

The **Access Point Online/Offline** graph shows a quick status of the access points in the infrastructure. The data is presented as a pie chart; online is green, busy is yellow, and offline is red. At the bottom of the chart, the number of access points and the status is also listed.

Client Associations

The **Client Associations** chart shows the number of clients associated with each access point in the configuration. When users are connected, the number of users are shown in bar chart form.

Real-Time Bandwidth

NOTE: Only SonicPoint ACe/ACi/N2 and SonicWave devices support the **Real-Time Bandwidth** feature.

A graph showing the bandwidth being used of the selected access point is displayed in the **Real-Time Bandwidth** section of the **Access Points > Dashboard**.

To select the refresh interval, select the interval period from the drop-down menu by the chart title. Options are: **1 minute**, **2 minutes**, **5 minutes**, **10 minutes**, and **60 minutes**.

To change the access point being displayed, go to the **Access Point** drop-down menu and select a different device. The chart updates with the data for that access point.

Client Report

NOTE: Only SonicPoint ACe/ACi/N2 and SonicWave devices support the **Client Report** feature.

Two graphs are shown in the **Client Report** section of the **Access Points > Dashboard**:

- OS Type
- Top Clients

OS Type

The type and version number of the operating system running on the device.

Top Clients

The **Top Clients** chart shows the clients who are using the most bandwidth. By going to the **TOP** field and selecting a number from the drop-down menu, you can show the top 5, top 10, top 15 or top 20 consumers for bandwidth. The values for both transmitting and receiving data are shown for the top users.

Real-Time Client Monitor

A graph showing the client connection details is displayed in the **Real-Time Client Monitor** section of the **Access Points > Dashboard**. This provides the detail for each user connected through the access points. You can see MAC address, hostname, OS type, volume of traffic being received (Rx) and the volume of traffic being transmitted (Tx).

2

Access Points SonicPoints

The most effective way to provision wireless access points is to let the GMS firewall automatically detect the access points and use one of the default profiles. GMS includes four default profiles, one for each generation of SonicWall access points: SonicWave 432e/432i/432o, SonicPointACe/ACi/N2, SonicPoint NDR/Ne/Ni and SonicPoint N. These can be used as is, or they can be customized to suit your configuration. You can also build new profiles based on the type of SonicWall access point you have. The basic settings for the access point profile is configured at **Access Points > SonicPoints**.

Topics:

Provisioning Overview

SonicPoint/SonicWave Provisioning Profiles provide a scalable and highly automated method of configuring and provisioning multiple access points across a Distributed Wireless Architecture. SonicPoint/SonicWave Profile definitions include all of the settings that can be configured on a SonicWall access point, such as radio settings for the 2.4GHz and 5GHz radios, SSID's, and channels of operation.

After you have defined a access point profile, you can apply it to a wireless zone. Each wireless zone can be configured with one access point profile. Any profile can apply to any number of zones. Then when an access point is connected to a zone, it is automatically provisioned with the profile assigned to that zone.

When an access point is first connected and powered up, it has a factory default configuration (IP address: `192.168.1.20`, username: `admin`, password: `password`). After initializing, the unit attempts to find a GMS device with which to peer. When a GMS device starts up, it also searches for access points through the SonicWall Discovery Protocol. If the access point and a peer GMS device find each other, they communicate through an encrypted exchange where the profile assigned to the relevant wireless zone is used to automatically provision the newly added access point unit.

As part of the provisioning process, GMS assigns the discovered access point a unique name and records its MAC address, the interface, and zone on which it was discovered. If part of the profile, it can also automatically assign an IP address so that the access point can communicate with an authentication server for WPA-EAP support. GMS then uses the profile associated with the relevant zone to configure the 2.4GHz and 5GHz radio settings.

Note that changes to profiles do not affect units that have already been provisioned and are in an operational state. Configuration changes to operational access points can occur in two ways:

- **Via manual configuration changes**

  This option is the best choice when a single, or a small set of changes are to be made, particularly when that individual access point requires settings that are different from the profile assigned to its zone.

- **Via un-provisioning**

  Deleting an access point effectively un-provisions the unit. It clears its configuration and places it into a state where it automatically engages the provisioning process anew with its peer GMS device. This technique is useful when the profile for a zone is updated or changed, and the change is set for propagation. It can be used to update firmware on access points, or to simply and automatically update multiple access points in a *controlled* fashion, rather than changing all peered access points at the same time, causing service disruptions.

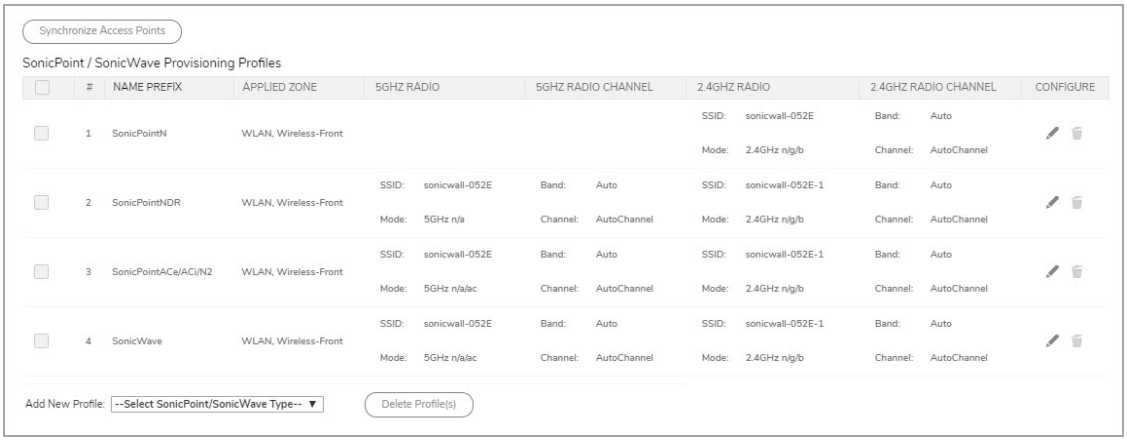
Creating/Modifying Provisioning Profiles

At **Access Points > SonicPoints**, you can configure and manage the provisioning profiles as well as the individual objects. You can add any number of profiles.

NOTE: *SonicPoint AC* refers to SonicPoint ACe/ACi/N2; *SonicPoint* refers to all SonicPoint devices. *SonicWave* refers to SonicWave 432e/i/o. SonicWave devices are supported on GMS 9.3 and newer.

1 Navigate to the **Access Points > SonicPoints** page. The four default GMS profiles are listed along with any custom profiles you have developed under the **SonicPoint/SonicWave Provisioning Profiles** section.

2 To modify any of the default provisioning profiles, click the **Edit** icon, and make the appropriate changes.



IMPORTANT: Because creating or modifying the **SonicPoint/SonicWave Provisioning Profiles** is very similar across all access point types, this section reviews how to add a new profile for a SonicWave device. Significant differences in the general process are noted and described in more detail later in this section.

NOTE: The SonicWall-provided provisioning profiles cannot be deleted so the corresponding **Delete** icon is grayed out and not active.

The **Add a New Profile** option has several windows where similar settings are grouped. The procedures are grouped to match those windows.

Topics:

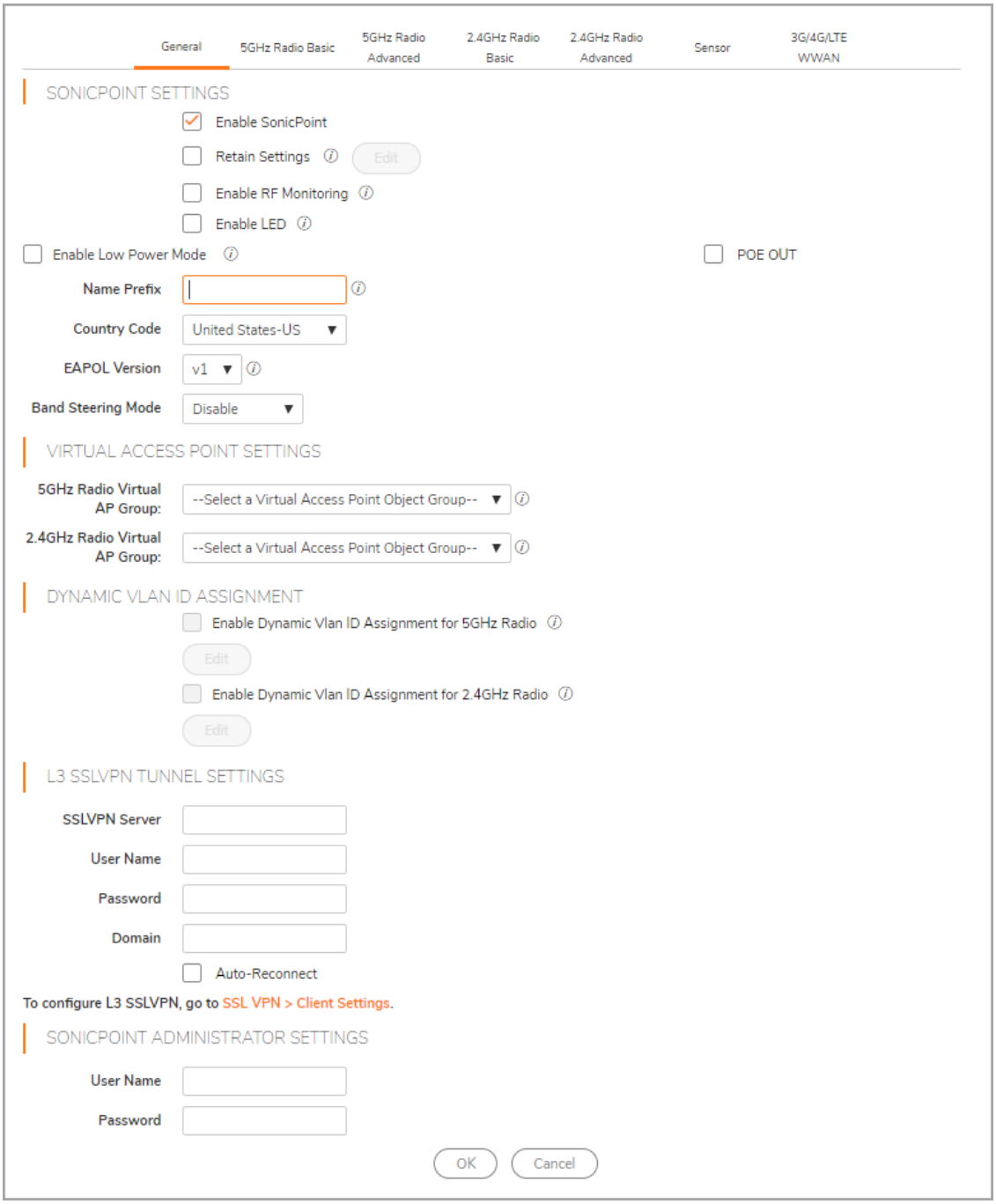
- Product Specific Configuration Notes

To access a new provisioning profile:

1 Navigate to the **Access Points > SonicPoints** page.

2 From the **Add a New Profile** drop-down menu, under the **SonicPoint/SonicWave Provisioning Profiles** section, select the type of profile you want to build. For this example SonicPoint SonicWave Profile was selected.

NOTE: To modify an existing profile, click the **Edit** icon for profile you want to update.



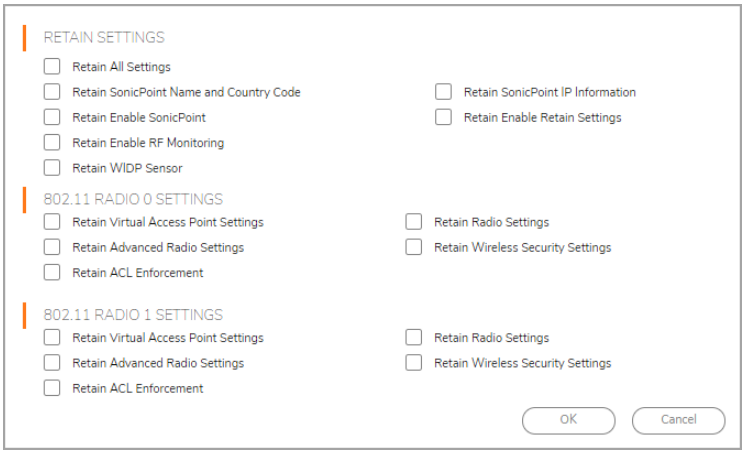
General Settings for Provisioning Profiles

To set the options on the General group:

1 Navigate to the **Access Points > SonicPoints** page.

2 Click the **Edit** icon in the **Configure** column.

3 Set the **SonicWave Settings**.

Option	Action
Enable SonicPoint	When checked, enables the SonicPoint access point. Default is checked.
Retain Settings	When checked, retains the customized until the next time the unit is rebooted. The **EDIT** button is enabled so you can customize which settings should be retained. 
Enable RF Monitoring	When checked, enables wireless RF-threat, real-time monitoring and management.
Enable LED	When checked, turns on the SonicWave LEDs. If left unchecked, which is the default, the LEDs stay off.
Enable Low Power Mode	When checked, the SonicWave operates in low power mode for when the power source is not the standard 802.3at PoE.
PoE Out	Click to provide an out-going power source from the PoE.
Name Prefix	Type the prefix used for the name in the field provided.
Country Code	From the drop-down menu, select the country code for the country in which the access point is deployed.
EAPOL Version	Select EAPoL version from the drop-down menu. Note that V2 provides the better security.
Band Steering Mode	Select the band steering mode from the drop-down menu. Options include: **Disable**, **Auto**, **Prefer 5GHz**, or **Force 5GHz**.

4 Set the **Virtual Access Point Settings**:

a For **5GHz Radio Virtual AP Group**, select a Virtual Access Point object group from the drop-down menu.

b For **2.4GHz Radio Virtual AP Group**, select a Virtual Access Point object group from the drop-down menu.

5 Scroll down to see the other General Settings.

6 Set the **Dynamic VLAN ID Assignment**.

> **NOTE:** To enable the options under Dynamic VLAN ID Assignment, you need to create a WLAN zone and VLAN interface under **Network > Interfaces.**

7 Configure the **L3 SSLVPN Tunnel Settings**:

   a Type in the **SSLVPN Server** name or IP address in the field provided.

   b Type the **User Name** for the SSLVPN server in the field provided.

   c Type the **Password** to authenticate on the SSLVPN server.

   d Type the **Domain** name in the field provided.

   e Check the box to enable **Auto-Reconnect**.

   f If you want to configure Layer 3 SSLVPN, follow the link to **Connectivity | SSL VPN > Client Settings** and define the appropriate settings.

8 When at the GlobalView, set the SonicPoint Administrator Settings:

   a Type in the **User Name** of the network administrator.

   b Type in the **Password** for the network administrator.

9 Click **OK**.

5GHz Radio Basic Settings for Provisioning Profile

The basic settings for 5GHz Radio and 2.4GHz Radio across the different types of access points are similar and have only a few differences. These differences are noted in the steps.

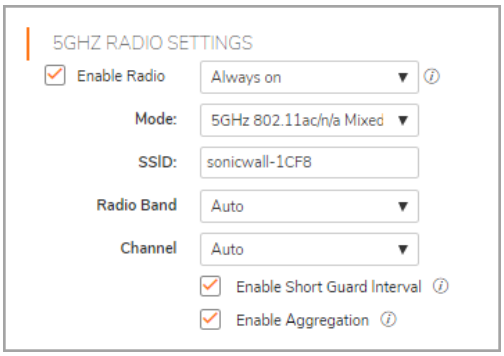
Radio Settings

To configure 5GHz Radio/2.4 GHz Radio Basic Settings:

1 Navigate to the **Access Points > SonicPoints** page.

2 Click the **Edit** icon in the **Configure** column.

3 Select the **5GHz Radio Basic** or **2.4 GHz Radio Basic** option.



4 Check **Enable Radio** to enable the radio bands automatically on all access points provisioned with this profile. This option is selected by default.

5 From the **Enable Radio** drop-down menu, select a schedule for when the radio is on or create a new schedule. The default is **Always on**.

6 Select your preferred radio mode from the **Mode** drop-down menu:

Radio Mode Choices

5GHz Radio Basic	2.4 GHz Radio Basic	Definition
5GHz 802.11n Only	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.
5GHz 802.11n/a Mixed	2.4GHz 802.11n/g/b Mixed (SonicPoint AC/NDR default)	Supports 802.11a and 802.11n (5GHz Radio) or 802.11b, 802.11g, and 802.11n (2.4 GHz Radio) clients simultaneously. If your wireless network comprises multiple types of clients, select this mode.
5GHz 802.11a Only (SonicPoint NDR default)		Select this mode if only 802.11a clients access your wireless network.
	2.4GHz 802.11g Only	If your wireless network consists only of 802.11g clients, you might 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 802.11ac/n/a Mixed (SonicWave and SonicPoint AC default)		Supports 802.11ac, 802.11a, and 802.11n (5GHz Radio) clients simultaneously. If your wireless network comprises multiple types of clients, select this mode.
5GHz 802.11ac Only		Allows only 802.11ac clients access to your wireless network. Other clients are unable to connect under this restricted radio mode.

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

For optimal throughput for 802.11ac clients, SonicWall recommends the **802.11ac Only** radio mode. Use the **802.11ac/n/a Mixed** radio mode for multiple wireless client authentication compatibility.

NOTE: The available **802.11n 5 GHz/2.4 GHz Radio Settings** options change depending on the mode selected. If the wireless radio is configured for a mode that:

- Supports 802.11n, the following options are displayed: **Radio Band**, **Primary Channel**, **Secondary Channel**, **Enable Short Guard Interval**, and **Enable Aggregation**.
- Does not support 802.11n, only the **Channel** option is displayed.

7 In the **SSID** field, enter a recognizable string for the SSID of each access point using this profile. This is the name that appears in clients' lists of available wireless connections.

TIP: If all SonicPoint ACs or NDRs in your organization share the same SSID, it is easier for users to maintain their wireless connection when roaming from one SonicPoint AC/NDR to another.

8 Select a radio band from the **Radio Band** drop-down menu:

NOTE: When **Mode** = **5GHz 802.11a Only**, the Radio Band options is not available.

- **Auto** - Allows the appliance to automatically detect and set the optimal channel for wireless operation based on signal strength and integrity. If selected for one, both the **Primary Channel** and **Secondary Channel** should set to **Auto**. This is the default setting.
- **Standard - 20MHz Channel**—Specifies that Radio 0 uses only the standard 20MHz channel.
- **Wide - 40MHz Channel**—Available when any mode except **5GHz 802.11a Only** is selected for the **Radio Band**. It specifies that Radio 0 uses only the wide 40MHz channel.
- **Wide - 80MHz Channel**—Available only when **5GHz 802.11ac/n/a Mixed** or **5GHz 802.11ac only** is selected for the **Radio Band**, specifies that Radio 0 uses only the wide 80MHz channel.(Not available when the **Mode** is **5GHz 802.11n Only**, **5GHz 802.11n/a Mixed**, or **5GHz 802.11a Only**.)

9 Select the channel or channels based on the Mode and Radio Band options chosen:

Mode	Radio Band	Channel
5GHz 802.11n Only	Auto	The **Primary Channel** and **Secondary Channel** fields default to **Auto**.
	Standard - 20 MHz Channel	Select **Auto** or one of the radio channels specified in the **Standard Channel** drop-down menu.
	wide - 40 MHz Channel	Select **Auto** or one of the radio channels in the **Primary Channel**. The **Secondary Channel** is automatically defined as **Auto**.
5GHz 802.11n/a Mixed	Auto	The **Primary Channel** and **Secondary Channel** fields default to **Auto**.
	Standard - 20 MHz Channel	Select **Auto** or one of the radio channels specified in the **Standard Channel** drop-down menu.
	Wide - 40 MHz Channel	Select **Auto** or one of the radio channels in the **Primary Channel**. The **Secondary Channel** is automatically defined as **Auto**.
5GHz 802.11a Only	(no option)	Select **Auto** or one of the radio channels specified in the **Channel** drop-down menu.
5GHz 802.11ac/n/a Mixed	Auto	The **Channel** field defaults to **Auto**.
	Standard - 20 MHz Channel	Select **Auto** or one of the radio channels specified in the **Channel** drop-down menu.
	Wide - 40 MHz Channel	Select **Auto** or one of the radio channels in the **Channel** field.
	Wide - 80 MHz Channel	Select **Auto** or one of the radio channels in the **Channel** field.

Mode	Radio Band	Channel
5GHz 802.11ac Only	Auto	The **Channel** field defaults to **Auto**.
	Standard - 20 MHz Channel	Select **Auto** or one of the radio channels specified in the **Channel** drop-down menu.
	Wide - 40 MHz Channel	Select **Auto** or one of the radio channels in the **Channel** field.
	Wide - 80 MHz Channel	Select **Auto** or one of the radio channels in the **Channel** field.

10 Check the box to **Enable Short Guard Interval**. This allows you to increase the radio data rate by shortening the guard interval. Be sure the wireless client can support this to avoid compatibility issues. (Option is not available for **Mode** = **5HGz 802.11ac only**.)

11 Check the box to **Enable Aggregation**. This allows you to increase the radio throughput by sending multiple data frames in a single transmission. Be sure the wireless client can support this to avoid compatibility issues. (Option is not available for **Mode** = **5HGz 802.11ac only**.)

Wireless Security

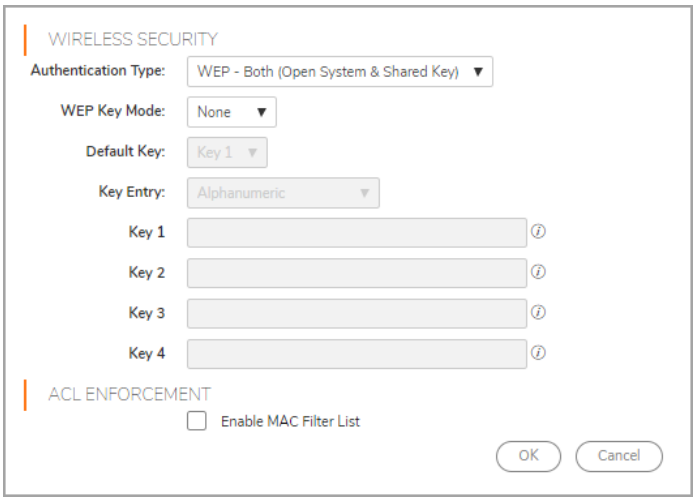
NOTE: The GMS interface is context-sensitive. If a VAP Group was selected in on the General page, the Wireless Security section is hidden and you can skip this section.

To set the Wireless Security options:

1 Navigate to the **Access Points > SonicPoints** page.

2 Click the **Edit** icon in the **Configure** column.

3 Scroll down to the **Wireless Security** section.



To configure Wireless Security:

1 Navigate to the **Access Points > SonicPoints** page.

2 Click the **Edit** icon in the **Configure** column.

3 In the **Wireless Security** section, select the **Authentication Type** from the drop-down menu.

NOTE: The options available change with the type of configuration you select.

4 Define the remaining settings to using the following table as a reference:

WEP Settings for Wireless Security

	WEP Description	
Authentication Type	**WEP Key Mode**	**Settings**
WEP (Wired Equivalent Privacy) is standard for Wi-Fi wireless network security. Open system uses and exchange of information to authenticate and then encrypts the data. Shared keys uses a shared secret key to authenticate.		
WEP - Both (Open System & Shared Key)	**WEP Key Mode** = **None**	Remaining settings are grayed out and cannot be selected.
	WEP Key Mode = **64 bit**, **128 bit** or **152 bit** The number of bits indicates the key strength of the WEP key.	1 In **Default Key** field, select the default key (the key that is tried first). **Key 1** is the default. 2 In the **Key Entry** field, choose whether the key is **Alphanumeric** or **Hexadecimal (0-9, A-F)**. 3 In the fields for Key 1, Key 2, Key 3, and Key 4 enter encryption keys that are used when transferring data.
WEP - Open System		Remaining settings are grayed out and cannot be selected.
WEP - Shared Key	**WEP Key Mode** = **64 bit**, **128 bit** or **152 bit** The default is **152 bit**.	1 In **Default Key** field, select the default key (the key that is tried first). **Key 1** is the default. 2 In the **Key Entry** field, choose whether the key is **Alphanumeric** or **Hexadecimal (0-9, A-F)**. The **Hexadecimal** option is the default. 3 In the fields for Key 1, Key 2, Key 3, and Key 4 enter encryption keys that are used when transferring data.

WPA2 Settings for Wireless Security

	Description
Authentication Type	**Settings**
WPA and WPA2 (Wi-Fi Protected Access) are newer protocols for protecting wireless devices. Selecting one of the **WPA2 - AUTO** options allows the WPA protocol to be used if a device is not enabled for WPA2.	
WPA2 - PSK	1 Select **Cipher Type** from the drop-down menu. Options are **AES** (default), **TKIP**, or **Auto**. 2 Set the **Group Key Interval** in seconds. The default is **86400**. 3 Define the **Passphrase** for the public shared key.
WPA2 - EAP	1 Select **Cipher Type** from the drop-down menu. Options are **AES** (default), **TKIP**, or **Auto**. 2 Set the **Group Key Interval** in seconds. The default is **86400**.

WPA2 Settings for Wireless Security (Continued)

	Description
Authentication Type	**Settings**
WPA2 - AUTO - PSK	1 Select **Cipher Type** from the drop-down menu. Options are **AES** (default), **TKIP**, or **Auto**. 2 Set the **Group Key Interval** in seconds. The default is **86400**. 3 Define the **Passphrase** for the public shared key.
WPA2 - AUTO - EAP	1 Select **Cipher Type** from the drop-down menu. Options are **AES** (default), **TKIP**, or **Auto**. 2 Set the **Group Key Interval** in seconds. The default is **86400**.

Radius Server Settings

If you selected either **WPA2 - EAP** or **WPA2 - AUTO - EAP** in the **Wireless Security** section, the **Radius Server** Settings section appears. This feature uses a RADIUS server to generate authentication keys. The server has to be configured for this and for communicating with the SonicWall appliance.

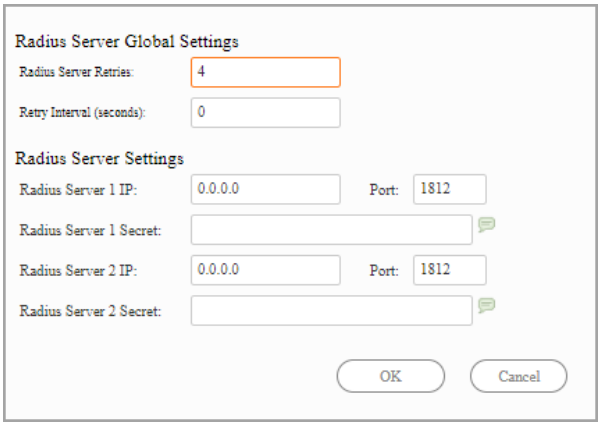
To configure RADIUS Server Settings:

1 Navigate to the **Access Points > SonicPoints** page.

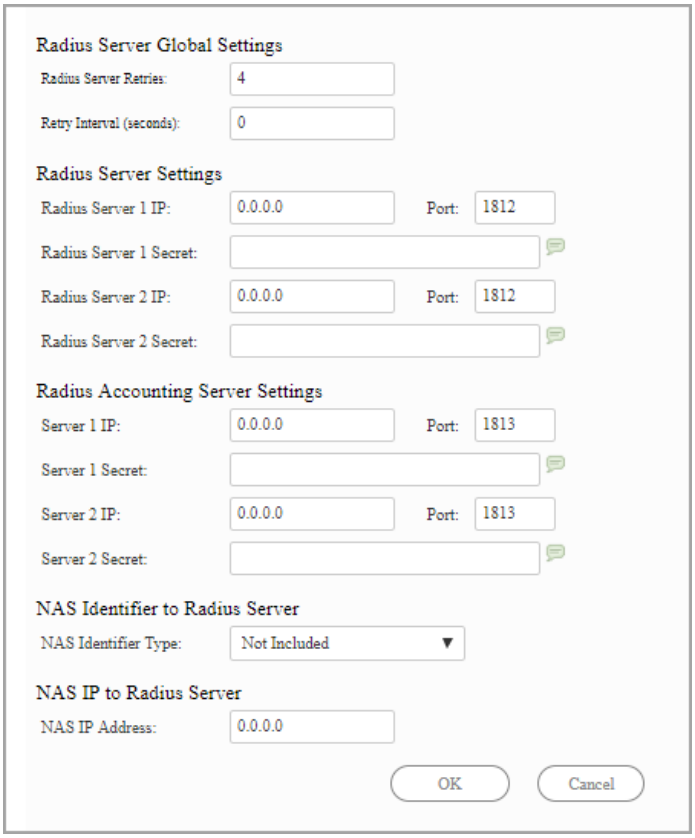
2 Click the **Edit** icon in the **Configure** column.

3 Click **Configure**. The **Radius Server Settings** dialog displays. The options displayed on this dialog depend on the type of SonicPoint.

SonicPointNDR or SonicPoint N



SonicPoint ACe/ACi/N2 - SonicWave



4 In the **Radius Server Retries** field, enter the number of times, from 1 to 10, the firewall attempts to connect before it fails over to the other Radius server.

5 In the **Retry Interval (seconds)** field enter the time, from 0 to 60 seconds, to wait between retries. The default number is **0** or no wait between retries.

6 Define the **Radius Server Settings** as described in the following table:

RADIUS Authentication Server Settings

Option	Description
Server 1 IP	The name/location of your RADIUS authentication server.
Server 1 Port	The port on which your RADIUS authentication server communicates with clients and network devices. The default port is **1812**.
Server 1 Secret	The secret passcode for your RADIUS authentication server.
Server 2	The name/location of your backup RADIUS authentication server.
Server 2 Port	The port on which your backup RADIUS authentication server communicates with clients and network devices. The default port is **1812**.
Server 2 Secret	The secret passcode for your backup RADIUS authentication server.

7 If you are using a Radius server to track usage for charging, set up the Radius Accounting Server:

RADIUS Accounting Server Settings

Option	Description
Server 1 IP	The name/location of your RADIUS accounting server.
Server 1 Port	The port on which your RADIUS authentication server communicates with clients and network devices.
Server 1 Secret	The secret passcode for your RADIUS authentication server.
Server 2	The name/location of your backup RADIUS authentication server.
Server 2 Port	The port on which your backup RADIUS authentication server communicates with clients and network devices.
Server 2 Secret	The secret passcode for your backup RADIUS authentication server.

8 To send the NAS identifier to the RADIUS server, select the type from the **NAS Identifier Type** drop-down menu:

- **Not Included** (default)
- **SonicPoint's Name**
- **SonicPoint's MAC Address**

9 To send the NAS IP address to the RADIUS Server, enter the address in the **NAS IP Addr** field.

10 Click **OK**.

ACL Enforcement

Each access point can support an Access Control List (ACL) to provide more effective authentication control. The ACL feature works in tandem with the wireless MAC Filter List currently available on GMS. Using the ACL Enforcement feature, users are able to enable or disable the MAC Filter List, set the Allow List, and set the Deny list.

To enable MAC Filter List enforcement:

1 Navigate to the **Access Points > SonicPoints** page.

2 Click the **Edit** icon in the **Configure** column.

3 Check the box to **Enable MAC Filter List**. When the MAC filter list is enabled, the other settings are also enabled so you can set them.

4 In the **Allow List**, select an option from the drop-down list. This identified which MAC addresses you allow to have access.

5 In the **Deny List**, select an option from the drop-down list. This identified which MAC addresses that you deny access to.

6 Check the box to **Enable MIC Failure ACL Blacklist**.

7 Set a **MIC Failure Frequency Threshold** based on number of times per minute. The default is **3**.

Remote MAC Address Access Control Settings

This option allows you to enforce radio wireless access control based on the MAC-based authentication on the RADIUS Server.

To allow wireless access control:

1 Navigate to the **Access Points > SonicPoints** page.

2 Click the **Edit** icon in the **Configure** column.

3 Check the box to **Enable Remote MAC Access Control**.

4 Click **Configure**.

5 If not already configured, set up the RADIUS Server(s) as described in Radius Server Settings.

6 Click **OK**.

5GHz/2.4GHz Radio Advanced Settings for Provisioning Profiles

These settings affect the operation of the radio bands. The SonicPoint/SonicWave has two separate radios built in. Therefore, it can send and receive on both bands at the same time.

The **2.4GHz Radio Advanced** view has the same options as the **5GHz Radio Advanced** view plus other options. The tabs are similar across the different access point models so follow this procedure for both. Differences are noted in the procedure where necessary.

To configure the 5GHz Radio/ 2.4GHz Radio Advanced settings:

1 Navigate to the **Access Points > SonicPoints** page.

2 Click the **Edit** icon in the **Configure** column.

3 Click **5GHz Radio Advanced** or **2.4GHz Radio Advanced** as needed.

4 Check the box if you want to **Hide SSID in Beacon.** This allows the SSID to send null SSID beacons in place of advertising the wireless SSID name. Sending null SSID beacons forces wireless clients to know the SSID to connect. This option is unchecked by default.

5 From the **Schedule IDS Scan** drop-down menu, select a schedule for the IDS (Intrusion Detection Service) scan.

Select a time when there are fewer demands on the wireless network to minimize the inconvenience of dropped wireless connections. You can create your own schedule by selecting **Create new schedule** or disable the feature by selecting **Disabled**, the default.

> **NOTE:** IDS offers a wide selection of intrusion detection features to protect the network against wireless threats. This feature detects attacks against the WLAN Infrastructure that consists of authorized access points, the RF medium, and the wired network. An authorized or valid-AP is defined as an access point that belongs to the WLAN infrastructure. The access point is either a SonicPoint, a SonicWave, or a third-party access point.

6 From the **Data Rate** drop-down menu, select the speed at which the data is transmitted and received. **Best** (default) automatically selects the best rate available in your area, given interference and other factors.

7 From the **Transmit Power** drop-down menu, select the transmission power. Transmission power effects the range of the SonicPoint.

- **Full Power** (default)
- **Half (-3 dB)**
- **Quarter (-6 dB)**

- **Eighth (-9 dB)**
- **Minimum**

8 If you are configuring a SonicPoint NDR: from the **Antenna Diversity** drop-down menu, select **Best** (default).

The **Antenna Diversity** setting determines which antenna the access point uses to send and receive data. When **Best** is selected, the access point automatically selects the antenna with the strongest, clearest signal.

9 In the **Beacon Interval (milliseconds)** field, enter the number of milliseconds between sending wireless SSID beacons. The minimum interval is 100 milliseconds (default); the maximum is 1000 milliseconds.

10 In the **DTIM Interval** field, enter the DTIM interval in milliseconds. The minimum number of frames is 1 (default); the maximum is 255.

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 (Delivery Traffic Indication Message).

11 If you are configuring a SonicPointNDR: in the **Fragmentation Threshold (bytes)** field, enter the number of bytes of fragmented data you want the network to allow.

The fragmentation threshold limits the maximum frame size. Limiting frame size reduces the time required to transmit the frame and, therefore, reduces the probability that the frame is corrupted (at the cost of more data overhead). Fragmented wireless frames increase reliability and throughput in areas with RF interference or poor wireless coverage. Lower threshold numbers produce more fragments. The minimum is 256 bytes, the maximum is 2346 bytes (default).

12 In the **RTS Threshold (bytes)** field, enter the threshold for a packet size, in bytes, at which a request to send (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. The minimum threshold is 256 bytes, the maximum is 2346 bytes (default).

13 In the **Maximum Client Associations** field, enter the maximum number of clients you want each access point using this profile to support on this radio at one time. The minimum number of clients is 1, the maximum number is 128, and the default number is **32**.

14 In the **Station Inactivity Timeout (seconds)** field, enter the maximum length of wireless client inactivity before the access point ages out the wireless client. The minimum period is 60 seconds, the maximum is 36000 seconds, and the default is **300** seconds.

15 If you are configuring the **2.4GHz Radio Advanced** view settings, define the following settings that are specific to that window; otherwise skip to the next step.

Options	Settings
Preamble Length	Select from the drop-down menu: • **Long** (default) • **Short**
Protection Mode	Select from the drop-down menu: • **None** • **Always** • **Auto**
Protection Rate	Select from the drop-down menu: • **1 Mbps** (default) • **2 Mbps** • **5 Mbps** • **11 Mbps**

Options	Settings
Protection Type	Select from the drop-down menu: • **CTS Only** (default) • **RTS-CTS**
Enable Short Slot Time	Select to allow clients to disassociate and re-associate more quickly. Specifying this option increases throughput on the 802.11n/g wireless band by shortening the time an access point waits before relaying packets to the LAN.
Do not allow 802.11b Clients to Connect	Select if you are using Turbo G mode and, therefore, are not allowing 802.11b clients to connect. Specifying this option limits wireless connections to 802.11g and 802.11n clients only.

16 From the **WMM (Wi-Fi Multimedia)** drop-down menu, select whether a WMM profile is to be associated with this profile:

- **Disabled** (default)
- **Create new WMM profile**. Refer to Configuring Wi-Fi Multimedia for more details.
- A previously configured WMM profile

17 Check the box to **Enable WDS AP**. It allows a wireless network to be expanded using multiple access point without the traditional requirement for a wired backbone to link them.

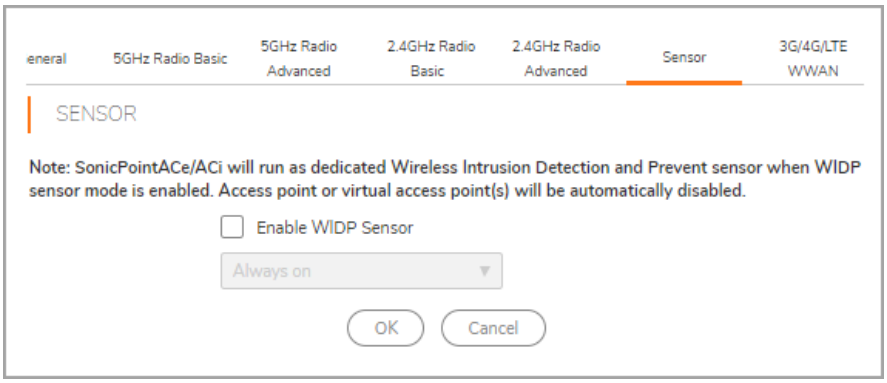
18 Select **Enable Green AP** to allow the access point radio to go into sleep mode. This saves power when no clients are actively connected. The access point immediately goes into full power mode when any client attempts to connect to it. Green AP can be set on each radio independently, Radio 0 (5GHz) and Radio 1 (2.4GHz).

19 In the **Green AP Timeout(s)** field, enter the transition time, in seconds, that the access point waits while it has no active connections before it goes into sleep mode. The transition values can range from 20 seconds to 65535 seconds with a default value of **20** seconds.

20 If configuring a SonicWave device, check the box to **Enable Air Time Fairness**.

This feature is disabled by default. If enabled, it steers the traffic for devices that can use the 5 GHz band to that band because it usually has less traffic and less interference. If the signal strength or signal conditions are better on the 2.4 GHz band, traffic is be steered to that band. The intention is to use both bands in the most effective manner.

Sensor



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

IMPORTANT: If this option is selected,access point or Virtual Access Point functionality is disabled automatically.

To configure the Sensor tab:

1 Navigate to the **Access Points > SonicPoints** page.

2 Click the **Edit** icon in the **Configure** column.

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

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

Manually Configuring the 3G/4G/LTE WWAN Profile

NOTE: If you are not configuring a modem, you can skip this section.

This feature provides another wireless WAN solution for firewall appliances that use wireless access points like SonicWave devices. You can plug a USB modem device into the SonicWave and it does the dial-up operation and connects to the Internet. After connecting, the SonicWave acts as a WWAN device for the firewall and provides WAN access.

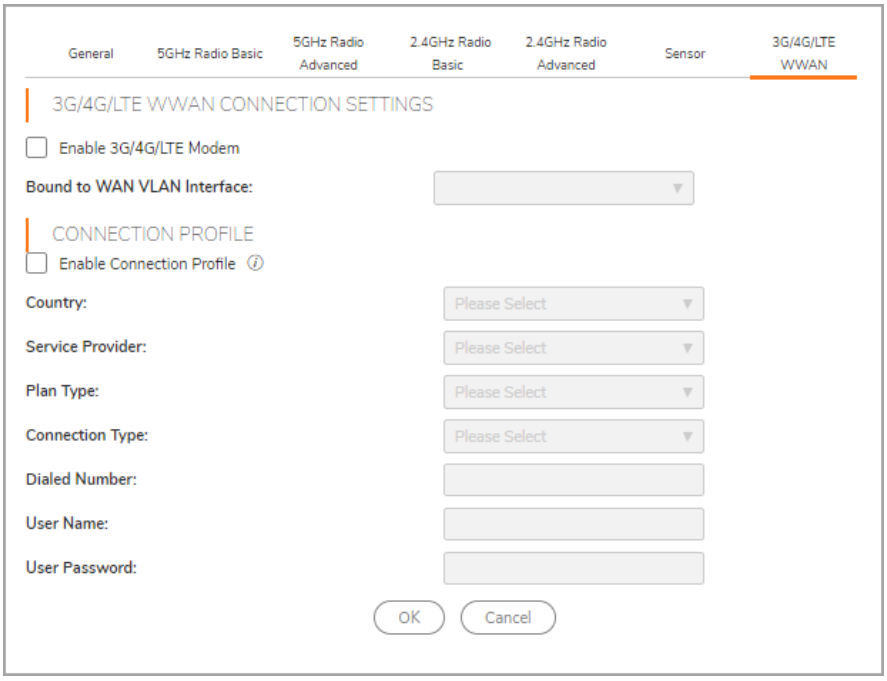
You can manually configure the 3G/4G/LTE WWAN profile or manually make changes by using the following procedure.

To manually configure the modem as a WWAN:

1 Navigate to the **Access Points > SonicPoints** page.

2 Click the **Edit** icon in the **Configure** column.

3 Click **3G/4GLTE WWAN**.



4 Check the box to **Enable the 3G/4G/LTE Modem**.

5 Select a VLAN interface from the **Bound to WAN VLAN Interface** drop-down menu.

If no interfaces are listed in the drop-down menu, you need to define one. Refer to the **Network > Interfaces** section.

NOTE: When building a VLAN interface, set the zone to WAN zone and the parent interface to the physical interface to which the access point is connected.

For 3G USB modems, set the IP Assignment to Static and assign a private IP address to it. Leave the gateway and DNS server fields blank.

For 4G and QMI modems, set the IP Assignment to DHCP.

6 In the **Connection Profile** section, check the box to **Enable Connection Profile**.

NOTE: Some traditional 3G/4G modems need connection profiles for dial-up.

7 In the **Country** field, select the country where the access point is deployed.

8 Select the **Service Provider** for the drop-down menu.

9 Select the **Plan Type** from the drop-down menu. Depending on the selection, other fields are auto-populated.

10 Select the **Connection Type** based on associations with the **Plan Type** from the drop-down menu.

11 If needed, add the **User Name** and **User Password** to the appropriate fields.

12 For an LTE modem, enter the **APN** value.

When all settings on the Profile page are complete, be sure to click **OK**.

Configuring Bluetooth Low Energy Settings

The Bluetooth Low Energy (BLE) settings feature allows you to use iBeacon compatible devices to communicate with other devices in the proximity.

To manually configure Bluetooth Low Energy settings:

1. Navigate to the **Access Points > SonicPoints** page.
2. Click the **Edit** icon in the **Configure** column.
3. Click the **Bluetooth LE** tab.
4. Check **Enable iBeacon.**
5. Enter Universally Unique Identifier (**UUID**), **Major**, and **Minor** parameters.
6. Click **OK**.
7. Enter a description and click **Accept**.

Product Specific Configuration Notes

SonicPoint configuration process varies slightly depending on whether you are configuring a single-radio (SonicPoint N) or a dual radio (SonicPoint AC and SonicPoint NDR) devices.

Managing Access Points

Topics:

Synchronize Access Points

Click **SYNCHRONIZE ACCESS POINTS** at the top of the **Access Points > SonicPoints** page to issue a query from the SonicWall appliance to the WLAN Zone. All connected access points report their current settings and statistics to the appliance. GMS also attempts to locate the presence of any newly connected access points that are not yet registered with the firewall.

NOTE: The button polls the access points, but does not push configuration to them.

Delete Access Point Profiles

NOTE: You cannot delete the predefined profiles; you can only delete those you add.

You can delete individual profiles or groups of profiles from the **SonicPoint/SonicWave Provisioning Profiles** section on the **Access Points > SonicPoints** page:

To delete a single access point profile:

1 Clicking **Delete**. A confirmation message appears.

2 Click **OK**.

To delete one or more access point profiles:

1 Selecting the checkbox next to the name(s) of the access points to be deleted. **DELETE** becomes active.

2 Click **DELETE**. A confirmation message appears.

3 Click **OK**.

To delete all profiles:

1 Select the checkbox next to the **#** in the column heading. **Delete All** becomes active.

2 Click **DELETE ALL**. A confirmation message appears.

3 Click **OK**.

Delete SonicPoint/SonicWave Objects

You can delete individual access points or groups of access points from the **SonicPoint/SonicWave Objects** section on the **Access Points > SonicPoints** page:

To delete a single object:

1 Clicking **Delete** for that object. A confirmation message appears.

2 Click **OK**.

To delete one or more objects:

1 Selecting the checkbox next to the objects to be deleted. **DELETE** becomes active.

2 Click **DELETE**. A confirmation message appears.

3 Click **OK**.

To delete all objects:

1 Select the checkbox next to the **#** in the column heading. **DELETE ALL** becomes active.

2 Click **DELETE ALL**. A confirmation message appears.

3 Click **OK**.

Reboot SonicPoint/SonicWave Objects

You can reboot individual access points or groups of access points from the **SonicPoint/SonicWave Objects** section on the **Access Points > SonicPoints** page:

To reboot a single object:

1 Check the checkbox next to the name of the access point to be rebooted. **REBOOT** becomes active.

2 Click **REBOOT**. A confirmation message displays.

3 Select the type of reboot:

- **reboot** (default) – Reboots to the configured profile settings.
- **reboot to factory default** – Reboots to factory default settings.

CAUTION: Selecting this option overwrites the access point profiles with factory default values.

4 Click **OK**.

To reboot all objects:

1 Click **REBOOT ALL**.

2 Select one of the following:

- **reboot** (default) – Reboots to the configured profile settings.
- **reboot to factor default**

CAUTION: Selecting this option overwrites the access point profiles with factory default values.

3 Click **OK** to apply to reboot the access points or **Cancel** to close the window without rebooting.

Modify SonicPoint/SonicWave Objects

To modify and an access point object:

1 Navigate to the **Access Points > SonicPoints** page.

2 Click **Edit** for the object you want to modify.

3 Changes the settings you want to modify.

4 Click **OK** to save the new settings.

NOTE: New SonicPoint/SonicWave access points are added automatically when network appliance performs an auto-discovery process.

3

Firmware Management

The **Access Points > Firmware Management** page provides a way to obtain the latest SonicPoint/SonicWave firmware and update an access point with it.

About Firmware Management

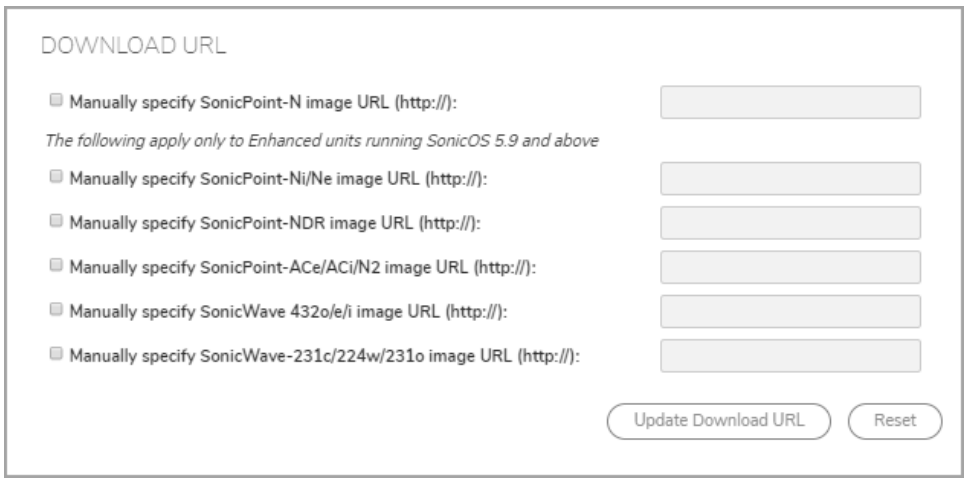
The **Firmware Management** table displays the status of the current access point firmware images, and provides options to update firmware and upload it to the access points. After clicking the **Update SonicPoint Firmware Status Information** link, if updated information is available, the following displays:

Column	Description
Firmware Image	Displays the type of access point for the firmware image.
Version	Displays the firmware version supported by the firewall that the access point needs to match. When a new version of AP firmware is available and supported by the firewall, then the **Version** entry displays it and the access point is automatically updated to it after connecting.
Status	Initially, all firmware status is Need Download. If a different firmware image is uploaded to the firewall buffer, it changes to a check mark indicating *Ready*.
Build Date	Displays the date that the uploaded firmware was created.
Action	Provides two buttons: • **Upload Firmware** button – Click to upload the downloaded firmware to the firewall buffer. As previously described for **Version**, a new, supported AP firmware is automatically pushed to the access point. To push the firmware to an access point that is already in operational status, you must use an internal setting. Contact SonicWall Support for information about using internal settings. • **Reset Firmware** button – Click to remove the downloaded firmware image from the buffer.

The Download URL section of the page provides a way to download access point firmware images from a specific location over HTTP. This allows you to load alternate firmware, such as a version provided by SonicWall Support which is not yet officially released.

Download URL

This is now on **Access Points | Firmware Management**. Scroll to the **Download URL** section.



The **Download URL** section provides fields for specifying the URL address of a site for downloading the SonicPoint images. SonicOS Enhanced 5.0 and higher does not contain an image of the SonicPoint firmware. If your SonicWall appliance has Internet connectivity, it automatically downloads the correct version of the SonicPoint image from the SonicWall server when you connect a SonicPoint device. If your SonicWall appliance does not have Internet access, or has access only through a proxy server, you must manually specify a URL for the SonicPoint firmware. You do not need to include the `http://` prefix, but you do need to include the filename at the end of the URL. The filename should have a `.bin` extension.

CAUTION: It is imperative that you download the corresponding SonicPoint image for the SonicOS firmware version that is running on your SonicWall network security appliance. The MySonicWall.com Web site provides information about the corresponding versions. When upgrading your SonicOS firmware, be sure to upgrade to the correct SonicPoint image.

To download an image:

1. Select the type of image or images to download by clicking on the appropriate checkbox and entering the image download location in the associated field:
   - **Manually specify SonicPoint-N image URL (http://)**
   - **Manually specify SonicPoint-Ni/Ne image URL (http://)**
   - **Manually specify SonicPoint-NDR image URL (http://)**
   - **Manually specify SonicPoint-ACe/ACi/N2 image URL (http://)**
   - **Manually specify SonicWave- 432o/e/i image URL (http://)**
   - **Manually specify SonicWave-231c224w/231o image URL (http://)**
2. Click **Update Download URL.**

4

Viewing Station Status

Station Status allows you to view status and individual statistics for all SonicPoint devices connected to the currently selected SonicWall firewall appliance.

The **Access Points > Station Status** page reports on the statistics of each SonicPoint.

The table lists entries for each wireless client connected to each SonicPoint. The sections of the table are divided by SonicPoint. Under each SonicPoint, is the list of all clients currently connected to it.

Click **Refresh SonicPoint Station Status Information from Firewall** at the top to refresh the list.

By default, the page displays up to the first 50 entries found. Click the First Page, Previous Page, Next Page, and Last Page icons to navigate if you need to view more than 50 entries.

Each SonicPoint device reports for both radios, and for each station, the following information to its GMS peer:

- **Station** – The state of the station. States can include:
  - **None** – No state information yet exists for the station.
  - **Authenticated** – The station has successfully authenticated.
  - **Associated** – The station is associated.
  - **Joined** – The station has joined the ESSID.
  - **Connected** – The station is connected (joined, authenticated or associated).
  - **Up** – An Access Point state, indicating that the Access Point is up and running.
  - **Down** – An Access Point state, indicating that the Access Point is not running.
- **MAC Address** – The client's (Station's) hardware address.

Additional Info

You can see the following additional information by mousing over the green comment bubble in the right column.

- **Associations** – Total number of Associations since power up.
- **Disassociations** – Total number of Disassociations.
- **Reassociations** – Total number of Reassociations.
- **Authentications** – Number of Authentications.
- **Deauthentications** – Number of Deauthentications.
- **Good Frames Received** – Total number of good frames received.
- **Good Frames Transmitted** – Total number of good frames transmitted.
- **Error in Receive Frames** – Total number of error frames received.
- **Error in Transmit Frames** – Total number of error frames transmitted.
- **Discarded Frames** – Total number of frames discarded. Discarded frames are generally a sign of network congestion.

- **Total Bytes received** – Total number of bytes received.
- **Total Bytes Transmitted** – Total number of bytes transmitted.
- **Management Frames Received** – Total number of Management frames received. Management Frames include:
    - Association request
    - Association response
    - Re-association request
    - Re-association response
    - Probe request
    - Probe response
    - Beacon frame
    - ATIM message
    - Disassociation
    - Authentication
    - De-authentication
- **Management Frames Transmitted** – Total number of Management frames transmitted.
- **Control Frames Received** – Total number of Control frames received. Control frames include:
    - **RTS** – Request to Send
    - **CTS** – Clear to Send
    - **ACK** – Positive Acknowledgment
- **Control Frames Transmitted** – Total number of Control frames transmitted.
- **Data Frames Received** – Total number of Data frames received.
- **Data Frames Transmitted** – Total number of Data frames transmitted.

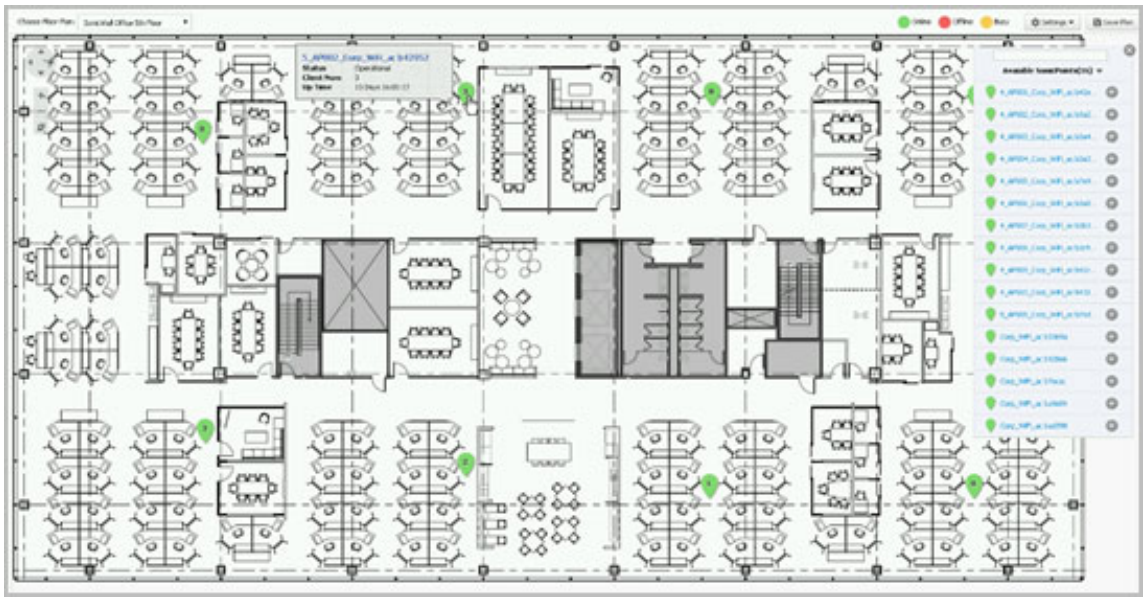
5

Access Points Floor Plan View

On the **Access Points > Floor Plan View**, the in GMS user interface allows a more visual approach to managing large numbers of SonicWave and SonicPoint devices. You can also track their physical locations and real-time statuses.

The Floor Plan View feature is an add-on to the existing wireless access point management suite in GMS. It provides a real-time picture of the actual wireless radio environment and improves your ability to estimate the wireless coverage of new deployments. The FPV also provides a single point console to check access point statistics, monitor access point real-time status, configure access points, remove access points and even show the access point RF coverage from the consolidated the context menu.

The figure that follows shows a sample of a typical floor plan view.



The Floor Plan View feature has a number of ways to view, add, and edit floor plans. The most common are described in this section.

Topics:

Selecting a Floor Plan

When you choose the **Access Points > Floor Plan View** page, the title of the floor plan being displayed is shown in the drop-down menu. To see a different floor plan, select a different floor plan from the **Floor Plans** drop-down menu.

Creating a Floor Plan

To create a floor plan:

1 Navigate to **Access Points > Floor Plan View**.

2 Click the **Settings** icon **> Manage Floor Plans**.

3 Select **Add New**.

4 Enter the name of your Floor Plan.

5 Click **Create**.

Editing a Floor Plan

There are different ways to edit floor plans; these are the most common.

To edit floor plan being displayed:

1 Navigate to **Access Points > Floor Plan View**.

2 Click the **Settings** icon **> Manage Floor Plans**.

3 Select **Edit**.

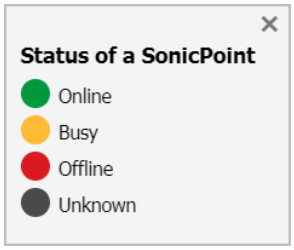
4 Change the fields as needed.

5 Click **Update**.

6 Click **Close**.

Managing Access Points

Access Point status is displayed using color.



The individual access points can be managed on the **Floor Plan View**.

Topics:

- Exporting an Image

Exporting an Image

To export the floor plan images:

1 Navigate to **Access Points > Floor Plan View**.

2 Click the **Settings** icon.

3 Select **Export as**.

4 Then choose whether you want it saved in **JPEG**, **PNG**, or **PDF** format.

5 Save the file where you can access it later.

Context Menu

You can use your mouse to activate various context menus:

- When you mouse over an active access point on the floor plan, a pop-up displays access point information, including ID, status, number of clients, and up time.
- By clicking on the access point, the RF coverage is displayed.
- By double-clicking the access point, the Real-Time Monitoring window appears.
- By right-clicking the access point, a context menu appears. It has options to edit, show statistics, monitor status and so forth.

6

Configuring SonicPoint Intrusion Detection Services

Rogue devices have emerged as one of the most serious and insidious threats to wireless security. In general terms, a device is considered rogue when it has not been authorized for use on the 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 devices. The real threat emerges in a number of different ways:

- Unintentional and unwitting connections to the rogue device
- Transmission of sensitive data over non-secure channels
- Unwanted access to LAN resources

While this does not represent a deficiency in the security of a specific wireless device, it is a weakness to the overall security of wireless networks.

Intrusion Detection Services (IDS) greatly increase the security capabilities of the firewall because it helps the appliance recognize and take countermeasures against the most common types of illicit wireless activity. IDS reports on all access points the firewall can find by scanning the 802.11a, 802.11g, and 802.11n radio bands on the access points.

The **Access Points > IDS** page reports on all devices detected by the firewall and its associated access points, and provides the ability to authorize legitimate devices.

The following table describes the **Discovered Access Points** Table and entities that are displayed on the **Access Points > IDS** page.

Discovered Access Points Table Components

Table Column or Entity	Description
Entity	
Scan All button	Initiates an operation to call all access points and identify connected devices.
Discovered Access Points	
SonicPoint	The access point name: shows only when **All SonicPoints** is selected in the **View Style: Access Point** drop-down menu.
MAC Address (BSSID)	The MAC address of the radio interface of the detected access point.
SSID	The radio SSID of the device.
Type	The radio band being used by the device: 2.4 GHz or 5 GHz.
Channel	The radio channel used by the device.
Manufacturer	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	When the Edit icon is clicked, the device is added to the address object group of authorized devices.

Topics:

Scanning Access Points

Active scanning occurs when the security appliance starts up. When you request a scan after start-up, the wireless clients are interrupted for a few seconds. The scan can effect traffic in the following ways:

- Non-persistent, stateless protocols (such as HTTP) should not exhibit any ill-effects.
- Persistent connections (protocols such as FTP) are impaired or severed.
- WiFiSec connections should automatically re-establish and resume with no noticeable interruption to the client.

CAUTION: Clicking Scan All causes all active wireless clients to be disconnected while the scan is performed. If service interruption is a concern, you should not request a scan while the SonicWall security appliance is in Access Point mode. Wait until no clients are active or a short interruption in service is acceptable.

To perform a scan:

1. Navigate to the **Access Points > IDS** page.
2. At the bottom of the table:
   - If you are scanning all access points, click **Scan All**.

     You can optionally choose one of the options in the drop-down menu for **--Perform SonicPoint Scan--**: **Scan Both Radios**, **Scan 802.11n Radio (5GHz)** or **Scan 802.11n Radio (2.4GHz)**.
3. Confirm that you want to perform the scan (wireless clients will be disconnected) by clicking **OK**.

Authorizing Access Points

Access Points that the security appliance detects are regarded as rogue access points until the security appliance is configured to authorize them for operation.

To authorize an access point:

1. Navigate to the **Access Points > IDS** page.
2. Click the **Edit** icon in the **Authorize** column for the access point you want to authorize. A pop-up displays.
3. Click **OK**.
4. Verify that authorization was successful by checking that the access point's MAC address was added.

7

Configuring Advanced IDP

Advanced Intrusion Detection and Prevention (IDP), or Wireless Intrusion Detection and Prevention (WIDP), monitors the radio spectrum for presence of unauthorized devices (intrusion detection) and to take countermeasures automatically (intrusion prevention) according to administrator settings. When Advanced IDP is enabled on an access point, the radio functions as a dedicated IDP sensor.

CAUTION: When Advanced IDP is enabled on a SonicWall access point radio, its access point functions are disabled and any wireless clients are disconnected.

GMS Wireless Intrusion Detection and Prevention is based on SonicPoint and SonicWave access points cooperating with SonicWall gateways. This feature turns your access points into dedicated WIDP sensors that detect unauthorized access points connected to a SonicWall network.

CAUTION: A SonicPoint N configured as a WIDP sensor cannot function as an access point.

When an access point is identified as a rogue access point, its MAC address is added to the All Rogue Access.

Configuring Advanced IDP is a two-part process:

- Enabling Advanced IDP on a Profile
- Configuring Advanced IDP

Enabling Advanced IDP on a Profile

The following is a checklist for enabling the Advanced IDP feature. More more information on access point profiles, refer to Creating/Modifying Provisioning Profiles.

To enable Advanced IDP scanning on an access point profile:

1 Navigate to the **Access Points > SonicPoints** page.

1 Scroll down to the **SonicPoint/SonicWave Provisioning Profiles** section.

2 Click the **Edit** icon for the appropriate profile.

3 Click **Sensor**.

TIP: The **Sensor** tab is the same for all SonicPoint N profiles.

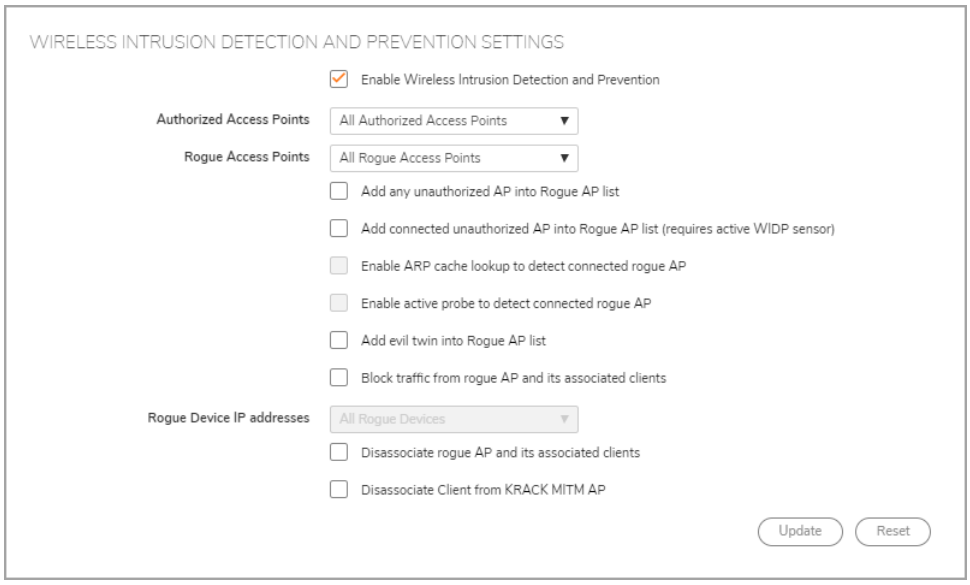
4 Select **Enable WIDP Sensor**. The drop-down menu becomes active.

5 In the drop-down menu, select the appropriate schedule for IDP scanning, or select **Create new schedule** to create a custom schedule.

CAUTION: When Advanced IDP scanning is enabled on a SonicPoint/SonicWave radio, its access point functions are disabled and any wireless clients are disconnected.

6 Click **OK**.

Configuring Advanced IDP



To configure Advanced IDP:

1 Navigate to the **Access Points > Advanced IDP** page.

2 Select **Enable Wireless Intrusion Detection and Prevention** to enable the appliance to search for rogue access points. This option is not selected by default, so when selected, the other options become active.

> **NOTE:** All detected access points are displayed in the **Discovered Access Points** table on the **Access Points > IDS** page, and you can authorize any allowed access points.

3 For **Authorized Access Points**, select the Address Object Group to which authorized Access Points are assigned. By default, this is set to **All Authorized Access Points**.

> **NOTE:** For SonicPoint Ns, no access point mode Virtual Access Point (VAP) is created. One station mode VAP is created, which is used to do IDS scans, and to connect to and send probes to unsecured access points.

4 For **Rogue Access Points**, select the Address Object Group to which unauthorized Access Points are assigned. By default, this is set to **All Rogue Access Points**.

5 Select one of the following two options to determine which access points are considered rogue (only one can be enabled at a time):

- **Add any unauthorized AP into Rogue AP list** automatically assigns all detected unauthorized access points—regardless if they are connected to your network—to the Rogue list.
- **Add connected unauthorized AP into Rogue AP list** assigns unauthorized devices to the Rogue list only if they are connected to your network. The following options determine how IDP detects connected rogue devices; both can be selected:
  - **Enable ARP cache search to detect connected rogue AP** – Advanced IDP searches the ARP cache for clients' MAC addresses. When one is found and the AP it is connected to is not authorized, the AP is classified as rogue.
  - **Enable active probe to detect connected rogue AP** – The SonicPoint/SonicWave connects to the suspect device and sends probes to all LAN, DMZ and WLAN interfaces of the firewall. If the firewall receives any of these probes, the AP is classified as rogue.

6 Select **Add evil twin into Rogue AP list** to add devices to the rogue list when they are not in the authorized list, but have the same SSID as a managed access point.

7 Select **Block traffic from rogue AP and its associated clients** to drop all incoming traffic that has a source IP address that matches the rogue list. From the **Rogue Device IP addresses** drop-down menu, either:

- Select **All Rogue Devices** (default) or an address object group you have created.
- Create a new address object group by selecting **Create New IP Address Object Group**. The **Add Address Object Group** window displays.

8 Select **Disassociate rogue AP and its clients** to send de-authentication messages to clients of a rogue device to stop communication between them.

9 Select **Disassociate Client from KRACK MITM AP** to enable the KRACK prevention function. When enabled, the SonicWave periodically checks for KRACK Man-in-the-Middle access points and actively disassociates the client from the KRACK MITM access point when it detects a client associated to it.

10 Click **Update** to save your changes.

8

Access Points Packet Capture

The **Access Points > Packet Capture** feature provides an in-depth type of wireless troubleshooting that you can use to gather wireless data from a client site and output into a readable file. This feature is supported for SonicWave access points.

NOTE: Because the antenna of the scan radio is 1x1, some data frames cannot be captured by the scan radio because of hardware restrictions.

The capture view on the **Access Points > Packet Capture** page shows the status of the SonicWave, the number of packets captured, and the size of the packet buffer. At the right, the **Configure** column provides buttons you can click to configure the capture settings for each SonicWave.

You can configure the mode, band and channel settings in the configuration dialog, allowing you to capture wireless packets in a specific channel. You can configure up to five source and destination MAC addresses. Click **Edit** for the SonicWave you want to configure.

Edit the configuration as necessary.

9

Configuring Virtual Access Points

NOTE: Virtual access points are supported when using wireless access points along with SonicWall NSA appliances.

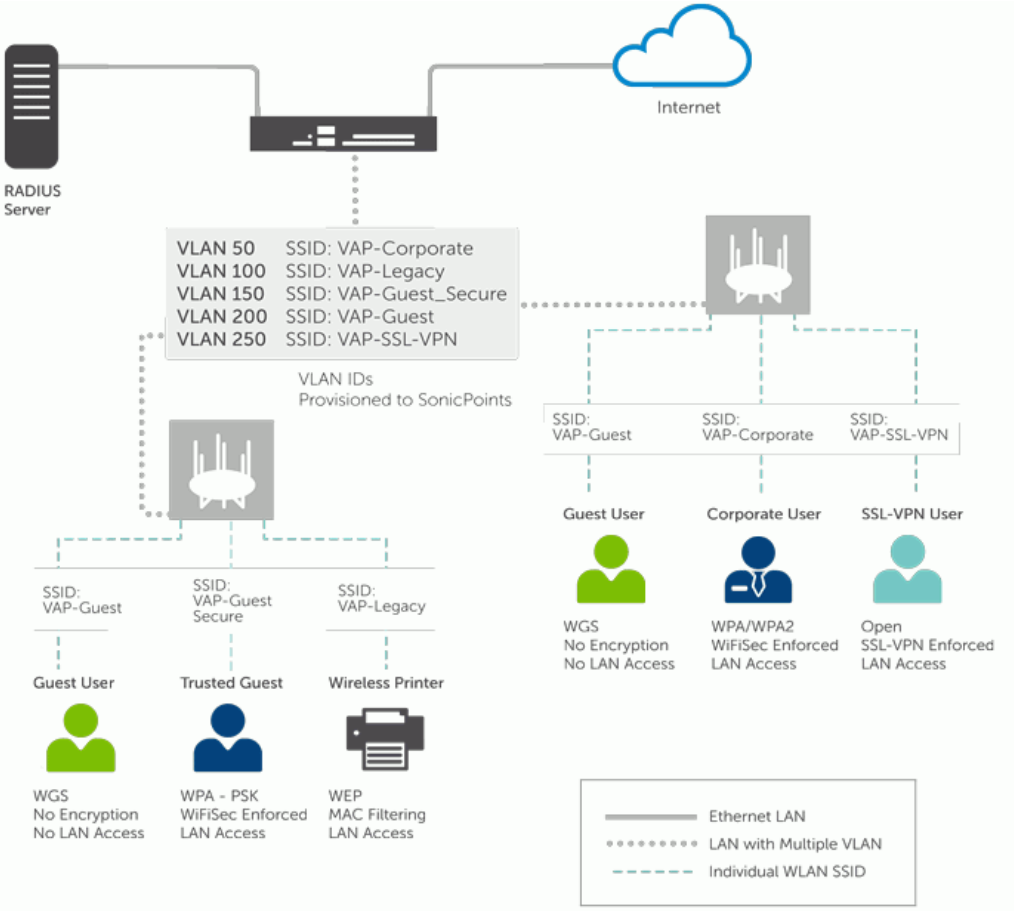
A Virtual Access Point (VAP) is a multiplexed representation of a single physical access point—it presents itself as multiple discrete access points. To wireless LAN clients, each virtual access point appears to be an independent physical access point, when actually only one physical access point exists. VAPs 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 SonicWall VAP feature is in compliance with the IEEE 802.11 standard for the media access control (MAC) protocol layer that includes a unique Basic Service Set Identifier (BSSID) and Service Set Identified (SSID). This segments the wireless network services within a single radio frequency footprint on a single physical access point.

VAPs 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 single or multiple physical access points simultaneously.

Topics:

Virtual Access Point Configuration



VAPs afford the following benefits:

- Each VAP can have its own security services settings (for example, GAV, IPS, CFS, and so on).
- Traffic from each VAP can be easily controlled using access rules configured from the zone level.
- Separate Guest Services or Lightweight Hotspot Messaging (LHM) configurations can be applied to each, facilitating the presentation of multiple guest service providers with a common set of access points.
- Bandwidth management and other access rule-based controls can easily be applied.

Before Configuring VAPs

Before configuring your virtual access points, you need to have in understanding of what your options are and what you can do.

Topics:

- Determining Your VAP Needs
- Determining Security Configurations
- Sample Network Definitions
- Determining Security Configurations
- VAP Configuration Worksheet

Determining Your VAP Needs

When deciding how to configure your VAPs, begin by considering your communication needs, particularly:

- How many different classes of wireless users do I need to support?
- How do I want to secure these different classes of wireless users?
- Do my wireless client have the required hardware and drivers to support the chosen security settings?
- What network resources do my wireless users need to communicate with?
- Do any of these wireless users need to communicate with other wireless users?
- What security services do I wish to apply to each of these classes or wireless users?

Determining Security Configurations

After understanding your security requirements, you can then define the zones (and interfaces) and VAPs that provide the most effective wireless services to these users. The following are examples of ways you can define certain types of users.

- **Corp Wireless** – Highly trusted wireless zone. Employs WPA2-AUTO-EAP security. WiFiSec (WPA) Enforced.
- **WEP & PSK** – Moderate trust wireless zone. Comprises two virtual access points and subinterfaces, one for legacy WEP devices (for example, wireless printers, older hand-held devices) and one for visiting clients who use WPA-PSK security.
- **Guest Services** – Using the internal Guest Services user database.
- **LHM** – Lightweight Hotspot Messaging enabled zone, configured to use external LHM authentication-back-end server.

Sample Network Definitions

The following list shows one possible way you and configure your virtual access points to ensure proper access:

- **VAP #1, Corporate Wireless Users** – A set of users who are commonly in the office, and to whom should be given full access to all network resources, providing that the connection is authenticated and secure. These users already belong to the network's Directory Service, Microsoft Active Directory, which provides an EAP interface through IAS – Internet Authentication Services.
- **VAP#2, Legacy Wireless Devices** – A collection of older wireless devices, such as printers, PDAs and hand-held devices, that are only capable of WEP encryption.
- **VAP#3, Visiting Partners** – Business partners, clients, and affiliated who frequently visit the office, and who need access to a limited set of trusted network resources, as well as the Internet. These users are not located in the company's Directory Services.
- **VAP# 4, Guest Users** – Visiting clients to whom you wish to provide access only to untrusted (for example, Internet) network resources. Some guest users are provided a simple, temporary username and password for access.
- **VAP#5, Frequent Guest Users** – Same as Guest Users, however, these users have more permanent guest accounts through a back-end database.

Prerequisites

Before configuring your virtual access points, be aware of the following:

- Each SonicWall access point must be explicitly enabled for virtual access point support. To verify, navigate to **Access Points > SonicPoints.** Then click the **Edit** icon for the **SonicPoint/SonicWave Provisioning Profiles > General Settings**: **Enable SonicPoint/SonicWave** checkbox and enabling either Radio A or G.
- Access points must be linked to a WLAN zone on your SonicWall network security appliance to provision the access points.
- When using VAPs with VLANs, you must ensure that the physical access point discovery and provisioning packets remain untagged (unless being terminated natively into a VLAN subinterface on the firewall).
- You must also ensure that VAP packets that are VLAN tagged by the access point are delivered unaltered (neither un-encapsulated nor double-encapsulated) by any intermediate equipment, such as a VLAN capable switch, on the network.
- Be aware that maximum access point restrictions apply and differ based on your SonicWall security appliance.

VAP Configuration Worksheet

The VAP Configuration Worksheet provides some common VAP setup questions and solutions along with a space for you to record your own configurations.

VAP Configuration Worksheet

Questions	Examples	Solutions
How many different types of users do I need to support?	Corporate wireless, guest access, visiting partners, wireless devices are all common user types, each requiring their own VAP	Plan out the number of different VAPs needed. Configure a zone and VLAN for each VAP needed
	Your Configurations:	
How many users does each VAP need to support?	A corporate campus has 100 employees, all of whom have wireless capabilities	The DHCP scope for the visitor zone is set to provide at least 100 addresses
	A corporate campus often has a few dozen wireless capable visitors	The DHCP scope for the visitor zone is set to provide at least 25 addresses
	Your Configurations:	

VAP Configuration Worksheet (Continued)

Questions	Examples	Solutions
How do I want to secure different wireless users?	A corporate user who has access to corporate LAN resources.	Configure WPA2-EAP
	A guest user who is restricted to only Internet access.	Enable Guest Services but configure no security settings.
	A legacy wireless printer on the corporate LAN.	Configure WEP and enable MAC address filtering.
	Your Configurations:	
What network resources do my users need to communicate with?	A corporate user who needs access to the corporate LAN and all internal LAN resources, including other WLAN users.	Enable Interface Trust on your corporate zone.
	A wireless guest who needs to access Internet and should not be allowed to communicate with other WLAN users.	Disable Interface Trust on your guest zone.
	Your Configurations:	
What security services to I wish to apply to my users?	Corporate users who you want protected by the full SonicWall security suite.	Enable all SonicWall security services.
	Guest users who do not require your attention because they are not on your LAN.	Disable all SonicWall security services.
	Your Configurations:	

Access Point VAP Configuration Task List

An access point VAP deployment requires several steps to configure. The following section provides a brief overview of the steps involved.

1. **Network Zone** - The 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 by way of VLAN subinterfaces. For more information on network zones, refer to the section on **Network > Zones**.
2. **Interface (or VLAN Subinterface)** - The Interface (X2, X3, and so on...) represents the physical connection between your SonicWall network security appliance and your physical access points. Your individual zone settings are applied to these interfaces and then forwarded to your access points. For more information on wireless interfaces, refer to the section on **Network > Interfaces**.

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 access points, 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 > DHCP Server**.

4 **Virtual Access Point Profiles** - The **Virtual Access Point Profile** feature allows for creation of access point configuration profiles, which can be easily applied to new virtual access points as needed. Refer to **Virtual Access Points Profiles** for more information.

5 **Virtual Access Point Objects** - The **Virtual Access Point Objects** feature allows for setup of general VAP settings. SSID and VLAN ID are configured through VAP Settings. Refer to **Virtual Access Points** for more information.

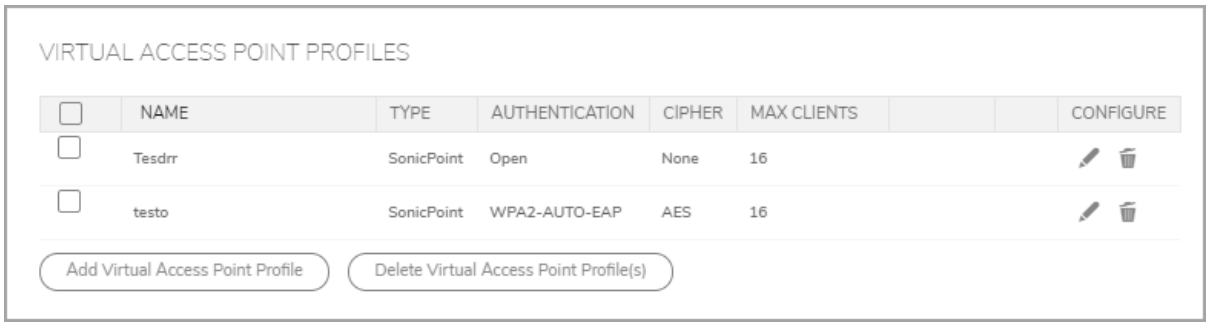
6 **Virtual Access Point Groups** - The **Virtual Access Point Groups** feature allows grouping of multiple virtual access point objects to be simultaneously applied to your access points.

7 **Assign Virtual Access Group to Access Point Provisioning Profile Radio**- The Provisioning Profile allows a VAP Group to be applied to new access points as they are provisioned.

8 **Assign WEP Key (for WEP encryption only)** - The Assign WEP Key allows for a WEP Encryption Key to be applied to new access points as they are provisioned. WEP keys are configured per-access point, meaning that any WEP-enabled virtual access points assigned to a physical access point must use the same set of WEP keys. Up to 4 keys can be defined, and WEP-enabled VAPs can use these 4 keys independently. WEP keys are configured on individual physical access points or on Access Point Profiles from the **Access Points > SonicPoints** page.

Virtual Access Points Profiles

A Virtual Access Point Profile allows you to preconfigure and save access point settings in a profile. Virtual Access Point Profiles allows settings to be easily applied to new virtual access points. Virtual Access Point Profiles are configured from the **Virtual Access Point Profiles** section of the **Access Points > Virtual Access Point** page.



To configure an existing VAP profile, click the **Edit** icon for that profile. To add a new VAP profile, click **Add Virtual Access Point Profile**.

NOTE: Options displayed change depending on your selection of other options.

Topics:

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 the **Access Points > Virtual Access Point** page.
2. Select **Add Virtual Access Point** if creating a new profile, or select a Virtual Access Point Profile and click on the **Edit** icon if editing an existing profile.
3. On the Advanced view, 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 the **Wireless > Virtual Access Point** page.
2. Select **Add Virtual Access Point Profile** if creating a new profile, or select a Virtual Access Point Profile and click on the **Edit** icon if editing an existing profile.
3. Set the **Radio Type**. It is set to **SonicPoint/SonicWave** by default if using the access points as virtual access points (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 list. Choose from these options:

Authentication Type	Definition
Open	No authentication is specified; unsecured access.
Shared	A shared key is used to authenticate and ensure basis security.
Both	Unsecured, shared access.
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.

Authentication Type	Definition
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.

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

NOTE: Different settings might appear on the page depending upon which options you select.

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 **Open**, refer to Radius Server and Radius Accounting on RADIUS settings.
- 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 and Radius Accounting for information on the settings.

WEP Encryption Settings

If you selected **Both** or **Shared** in Step 5 of the prior procedure, the section called **WEP Encryption Settings** appears. WEP settings are commonly shared by virtual access points within a common physical access point.

To set the encryptions settings:

1. In the **Encryption Key** field, select **Key 1**, **Key 2**, **Key 3** or **Key 4** from the drop-down list.
2. Go to Radius Server and Radius Accounting to set up the RADIUS settings, if you kept Remote MAC Access Control enabled.

WPA-PSK > WPA2-PSK Encryption Settings

If you selected an option in Step 5 that requires a pre-shared key—**WPA2-PSK** or **WPA2-AUTO-PSK**—the section called **WPA/WPA2-PSK Encryption Settings** appears. When these settings are defined, a preshared key is used for authentication.

To set the encryptions settings:

1. Input a password in the **Pass Phrase** field.
2. Go to Radius Server and Radius Accounting to set up the RADIUS settings, if you kept Remote MAC Access Control enabled.

Radius Server and Radius Accounting

You can set up a RADIUS server for any of the options selected in Step 5. When these settings are defined, an external 802.1x/EAP capable RADIUS server is used for key generation and authentication. Input values in the following fields:

To set the Radius Server Settings:

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.
RADIUS Server 1 IP	Input the name/location of the RADIUS authentication server.
Server 1 Port	Input the port on which your primary RADIUS authentication server communicates with clients and network devices.
RADIUS Server 1 Secret	Enter the secret passcode for your primary RADIUS authentication server.
RADIUS Server 2 IP	Input the name/location 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.
RADIUS Server 2 Secret	Enter the secret passcode for your backup RADIUS authentication server.

To set the Radius Accounting Server Settings:

Field Name	Description
Server 1 IP	Enter the IP address for the first RADIUS server.
Server 1 Port	Input the port on which your primary RADIUS accounting server communicates with clients and network devices.
Server 1 Secret	Enter the secret passcode for your primary RADIUS accounting server.
Server 2 IP	Enter the IP address for the backup RADIUS server.
Server 2 Port	Input the port on which your backup RADIUS accounting server communicates with clients and network devices.
Server 2 Secret	Enter the secret passcode for your backup RADIUS accounting server.
NAS Identifier Type	Select the NAS Identifier Type from the drop-down menu. Options include: **Not Included** (default), **SonicPoint's Name** and **SonicPoint's MAC Address**.
NAS IP Address	Input the NAS system IP address.
Group Key Interval	The time period, in seconds, for which a group key is valid and after which the group key is forced to be updated. The default is **86400** seconds (24 hours).

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 GMS. Using the ACL Enforcement feature, users are able to enable or disable the MAC Filter List, set the Allow List, and set the Deny list.

Each VAP can have its own MAC Filter List settings or use the global settings. When the global settings are enabled, the SonicWave, SonicPoint-N/SonicPointNDR/SonicPoint Ni/Ne, the SonicPoint, or SonicPoint-N appliance uses these settings by default. In Virtual Access Point (VAP) mode, each VAP of this group shares the same MAC Filter List settings.

ACL Enforcement Settings

Option	Description
Enable MAC Filter List	Enforces Access Control by allowing or denying traffic from specific devices. By default, this option is not selected and all options in this section are dimmed and unavailable.
Use Global ACL Settings	Uses global ACL settings. **NOTE:** ACL support per virtual access point is only supported by SonicPointN. If one virtual access point is used by SonicPoint/SonicWave, global ACL configuration is applied by default.
Allow List	Select a MAC address group to automatically allow traffic from all devices with the MAC addresses listed in a particular group: • **All MAC Addresses** **NOTE:** It is recommended that the **Allow List** be set to **All MAC Addresses**. • **Default SonicPoint ACL Allow Group** • **Default Global ACL Allow Group** • **GMS Addresses** • Custom MAC Address Object Groups that you developed
Deny List	Select a MAC address group from the drop-down menu to automatically deny traffic from all devices with MAC address in the group. **NOTE:** The **Deny List** is enforced before the **Allow List**. • **No MAC Addresses** • **Default SonicPoint ACL Deny Group** • **Default Global ACL Deny Group** • **Default ACL Deny Group** • **GMS Addresses** **NOTE:** It is recommended that the **Deny List** be set to **Default SonicPoint/SonicWave ACL Deny Group**. • Custom MAC Address Object Groups that you developed

Remote MAC Address Access Control Settings

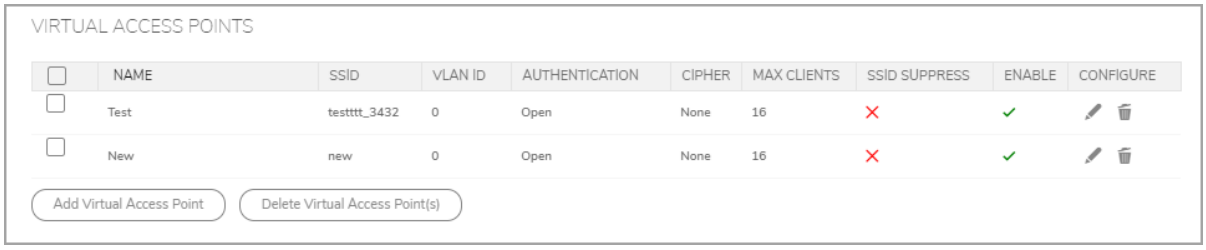
NOTE: This section is not displayed if **WPA2-EAP/WPA2-AUTO-EAP** is selected for **Authentication Type**.

Remote MAC Address Access Control Settings

Option	Description
Enable Remote MAC Access Control	Check the box to enforce radio wireless access control based on MAC-based authentication policy in a remote Radius server. By default, this option is not selected. **NOTE:** If you selected other than **WPA2-EAP/WPA2-AUTO-EAP** for **Authentication Type**, selecting **Enable Remote MAC Access Control** displays the **Radius Server Settings** section.

Virtual Access Points

The VAP Settings feature allows for setup of general VAP settings. SSID and VLAN ID are configured through VAP Settings. virtual access points are configured from the **Access Point > Virtual Access Point** page.

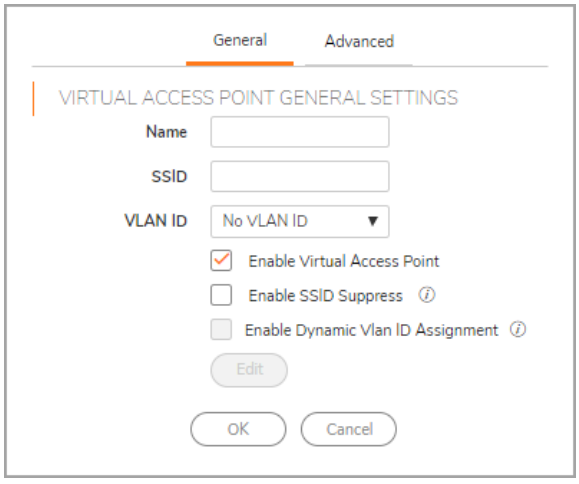


To configure an existing VAP, click the **Edit** icon for that virtual access point. To add a new VAP, click **Add Virtual Access Point**.

Topics:

- General Panel
- Advanced Panel

General Panel



Set the following features on the **General** panel.

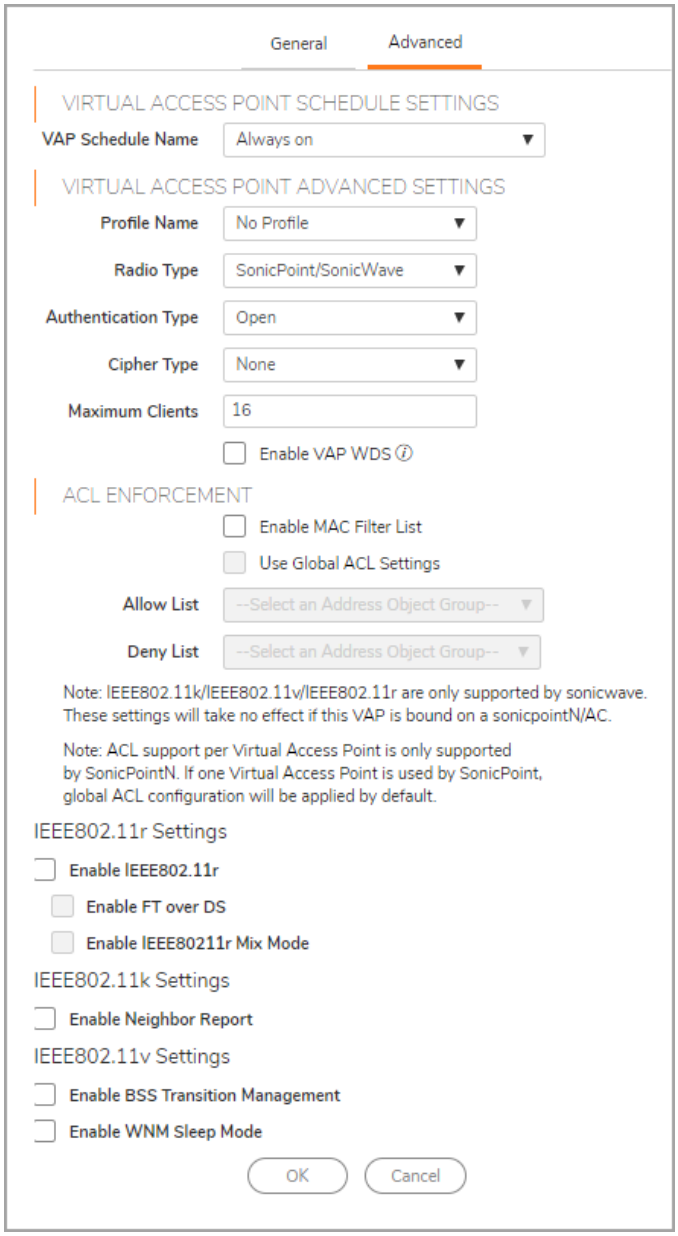
Virtual Access Point General Settings

Feature	Description
Name	Create a friendly name for your VAP.
SSID	Enter an SSID name for the access points using this VAP. This name appears in wireless client lists when searching for available access points.
VLAN ID	When using platforms that support VLAN, you might optionally select a VLAN ID to associate this VAP with. Settings for this VAP are inherited from the VLAN you select.
Enable Virtual Access Point	Enables this VAP. This option is selected by default.

Virtual Access Point General Settings (Continued)

Feature	Description
Enable SSID Suppress	Suppresses broadcasting of the SSID name and disables responses to probe requests. Check this option if you do not wish for your SSID to be seen by unauthorized wireless clients. This option is not selected by default.
Enable Dynamic VLAN ID Assignment	Check to enable. Dynamic VLAN can only be enabled when the authentication type is set to EAP.

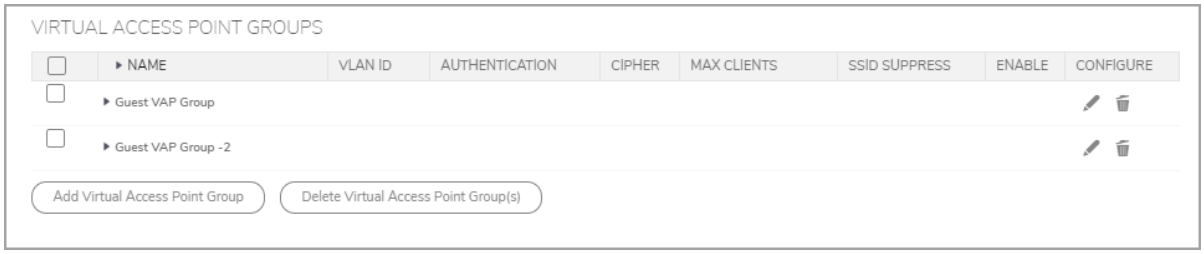
Advanced Panel



Advanced settings allows you to configure authentication and encryption settings for a specific virtual access point. Choose a **Profile Name** to inherit these settings from a user-created profile. As the **Advanced** tab of the **Add/Edit Virtual Access Point** window is the same as **Add/Edit Virtual Access Point Profile** window, see Virtual Access Points Profiles for complete authentication and encryption configuration information.

Virtual Access Point Groups

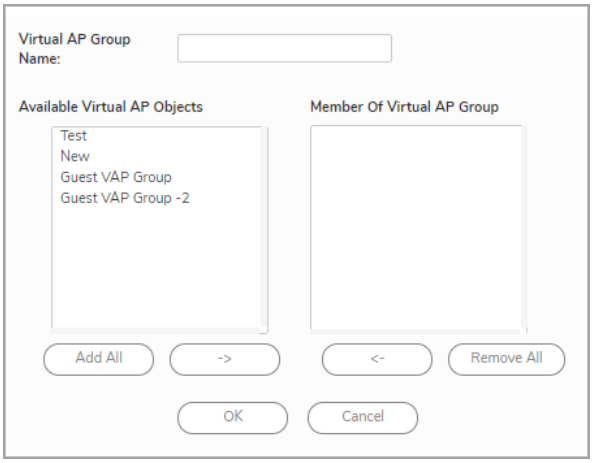
The Virtual Access Point Groups feature is available on SonicWall NSA appliances. It allows for grouping of multiple VAP objects to be simultaneously applied to your access points. Virtual Access Point Groups are configured from the **Access Points > Virtual Access Point** page.



Add a virtual access point group:

1 Select **Access Points > Virtual Access Point**.

2 Select **Add Group** if creating a new profile, or select a Virtual Access Point Profile and click on the **Edit** icon if editing an existing profile.



3 Enter the **Virtual AP Group Name** in the field provided.

4 Select the objects you want to add from the **Available Virtual AP Objects** list and click the **Left Arrow** to move it to the **Member of Virtual AP Group** list.

Or, click **ADD ALL** to add all the objects to the group.

5 Select an object and use the **Right Arrow** or **REMOVE ALL** to remove objects from the group.

6 Click **OK** to save your settings.

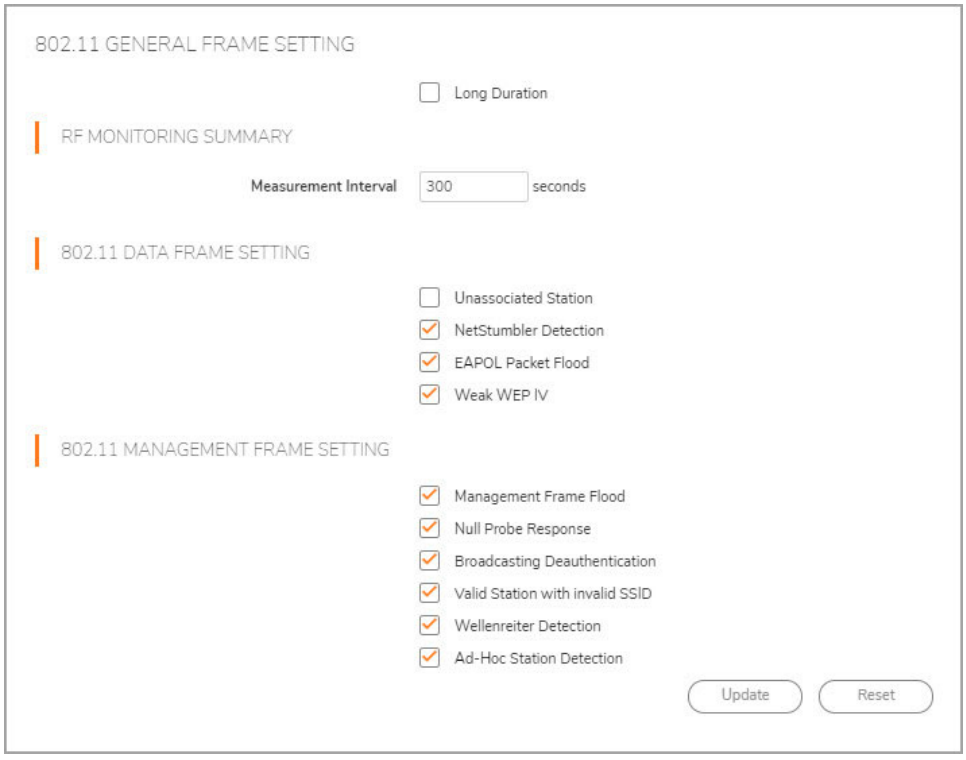
10

Configuring RF Monitoring

Radio Frequency (RF) technology used in today's 802.11-based wireless networking devices poses an attractive target for intruders. If left unmanaged, RF devices can leave your wireless (and wired) network open to a variety of outside threats, from Denial of Service (DoS) to network security breaches. To help secure your SonicWall wireless access points, SonicWall helps detect threats without interrupting the current operation of your wireless or wired network.

SonicWall RF Monitoring provides real-time threat monitoring and management of SonicPoint radio frequency traffic. In addition to its real-time threat monitoring capabilities, SonicWall RF monitoring provides a system for centralized collection of RF threats and traffic statistics that offer a way to easily manage RF capabilities directly from the SonicWall security appliance gateway.

The **Access Points > RF Monitoring** page provides a central location for selecting RF signature types, viewing discovered RF threat stations, and adding discovered threat stations to a watch list.



Topics:

Prerequisites

For RF Monitoring to be enforced, you must enable the RF Monitoring option on all available access points. The easiest way to do that is to update the access point profile and then apply that profile to the applicable access points.

To find the RF Monitoring option:

1. Navigate to the **Access Points > SonicPoints** page.
2. Click the **Edit** icon on the profile you want to update (or **Select SonicPoint/SonicWave Type** from the **Add New Profiles** drop-down menu if creating a new profile).
3. Check the box to **Enable RF Monitoring** in the **General** window.

For more information on setting up profiles, refer to Creating/Modifying Provisioning Profiles.

802.11 General Frame Setting

The 802.11 General Frame Setting panel displays the option to enable long duration.

Checking the box enables **Long Duration**. Wireless devices share airwaves by dividing the RF spectrum into 14 staggered channels. Each device reserves a channel for a specified (short) duration, and during the time that any one device has a channel reserved, other devices know not to broadcast on this channel. Long Duration attacks exploit this process by reserving many RF channels for very long durations, effectively stopping legitimate wireless traffic from finding an open broadcast channel. By default, this option is not specified.

RF Monitoring Summary

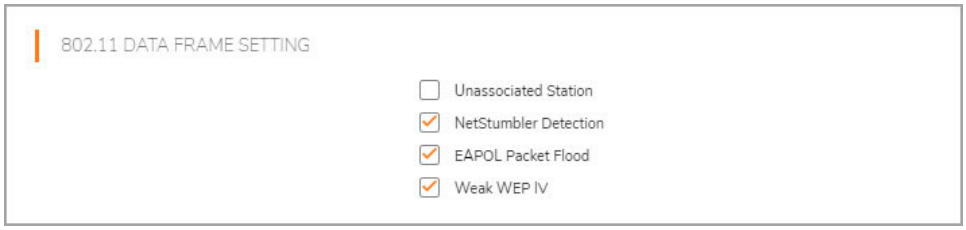
The **RF Monitoring Summary** displays data about the access points that have been configured for RF monitoring.

It shows how many RF threats have been identified and the **Measurement Interval** setting. You can reset the **Measurement Interval** by type a new number into the field. The default value is **300** seconds. Be sure to click **Update** to save the settings.

By clicking the **Access Point** link, you are taken to the **Access Points > SonicPoints** page to edit profile or object settings.

802.11 Data Frame Setting

The **802.11 Data Frame Setting** panel is used to configure your data frame settings and displays the number of threats for each setting.



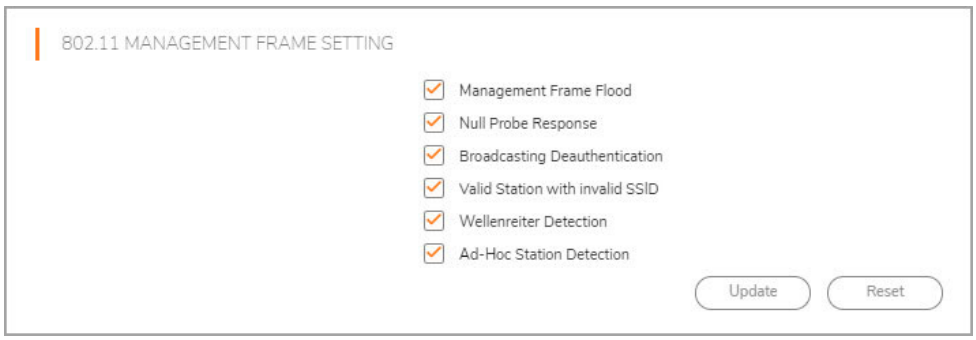
Check the boxes to enable any of these options. Click **Update** to save the settings. By default, **Unassociated Station** is not selected; the others are enabled. The following table describes the **Data Frame Settings**.

802.11 Data Frame Settings

Name	Description
Unassociated Station	A wireless station attempts to authenticate prior to associating with an access point, the unassociated station can create a DoS by sending a flood of authentication requests to the access point while still unassociated.
NetStumbler Detection	Typically used to locate both free Internet access as well as interesting networks. NetStumbler interfaces with a GPS receiver and mapping software to automatically map out locations of wireless networks. NetStumbler is also used by attackers to retrieve information from surrounding wireless networks.
EAPOL Packet Flood	Extensible Authentication Protocol over LAN (EAPOL) packets are used in WPA and WPA2 authentication mechanisms. As these packets, like other authentication request packets, are received openly by wireless access points, a flood of these packets can result in DoS to your wireless network.
Weak WEP IV	WEP security mechanism uses your WEP key along with a randomly chosen 24-bit number known as an Initialization Vector (IV) to encrypt data. Network attackers often target this type of encryption because some of the random IV numbers are weaker than others, making it easier to decrypt your WEP key.

802.11 Management Frame Setting

The **802.11 Management Frame Setting** panel is used to configure your management frame settings and displays the number of threats for each setting.



Check the box to enable any of these options, and by default, all are enabled. Click **Update** to save the settings. The following table describes the **Management Frame Settings**.

802.11 Management Frame Setting

Name	Description
Management Frame Flood	This variation on the DoS attack attempts to flood wireless access points with management frames (such as association or authentication requests) filling the management table with bogus requests.
Null Probe Response	When a wireless client sends out a probe request, the attacker sends back a response with a Null SSID. This response causes many popular wireless cards and devices to stop responding.
Broadcasting Deauthentication	This DoS variation sends a flood of spoofed de-authentication frames to wireless clients, forcing them to constantly de-authenticate and subsequently re-authenticate with an access point.
Valid Station with invalid SSID	In this attack, a rouge access point attempts to broadcast a trusted station ID (ESSID). Although the BSSID is often invalid, the station can still appear to clients as though it is a trusted access point. The goal of this attack is often to gain authentication information from a trusted client.
Wellenreiter Detection	Wellenreiter is a popular software application used by attackers to retrieve information from surrounding wireless networks.
Ad hoc Station Detection	Ad hoc stations are nodes that provide access to wireless clients by acting as a bridge between the actual access point and the user. Wireless users are often tricked into connecting to an Ad hoc station instead of the actual access point, as they might have the same SSID. This allows the Ad hoc station to intercept any wireless traffic that connected clients send to or receive from the access point.

Practical RF Monitoring Field Applications

This section provides an overview of practical uses for collected RF Monitoring data in detecting Wi-Fi threat sources. When using RF data to locate threats, keep in mind that wireless signals are affected by many factors.

- Signal strength is not always a good indicator of distance.

  Obstructions such as walls, wireless interference, device power output, and even ambient humidity and temperature can affect the signal strength of a wireless device.

- A MAC Address is not always permanent.

  While a MAC address is generally a good indicator of device type and manufacturer, this address is susceptible to change and can be spoofed. Also, originators of RF threats might have more than one hardware device at their disposal.

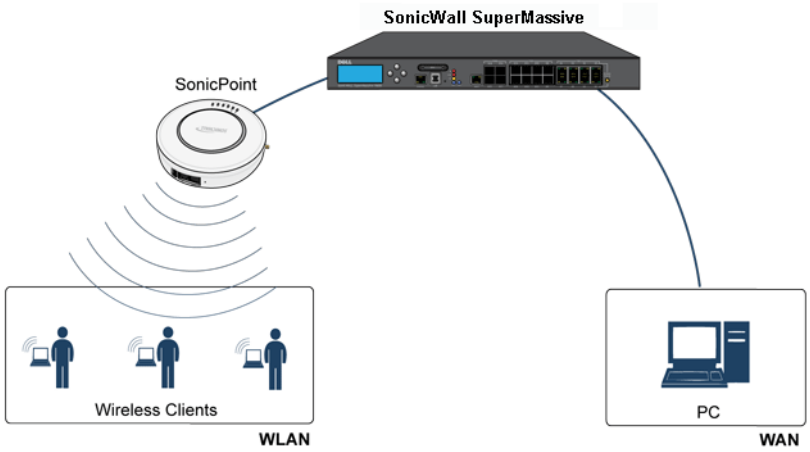
11

Configuring Fairnet

The FairNet feature provides an easy-to-use method for network administrators to control the bandwidth of associated wireless clients and make sure it is distributed fairly between them. Administrators can configure the FairNet bandwidth limits for all wireless clients, specific IP address ranges, or individual clients to provide fairness and network efficiency.

This is an example of typical FairNet topology:

Typical FairNet Topology



To deploy the FairNet feature, you must have a laptop or PC with an IEEE802.11b/g/n wireless network interface controller.

Topics:

- Supported Platforms
- FairNet Features
- Management Interface Overview
- Configuring FairNet

Supported Platforms

The FairNet feature is currently supported on the following appliance models:

- SonicWall TZ Series
- SonicWall NSA Series
- SonicWall E-Class NSA Series
- SonicWall SuperMassive Series

FairNet Features

The Distributed Coordination Function (DCF) provides timing fairness for each client to access a medium with equal opportunity. However, it cannot guarantee the per-station data traffic fairness among all wireless clients. The FairNet feature is implemented on top of the existing 802.11 DCF to guarantee fair bandwidth among wireless clients regardless of the number and direction of flows.

The traffic control feature decides if packets are queued or dropped (for example, if the queue has reached some length limit, or if the traffic exceeds some rate limit). It can also decide which order packets are sent (for example, to give priority to certain ones), and it can delay the sending of packets (for example, to limit the rate of outbound traffic). After traffic control has released a packet for sending, the device driver picks it up and emits it on the network.

Management Interface Overview

The components of the FairNet display are described in the following table.

FairNet Interface Components

Name	Description
Buttons and checkboxes	
Add New Fairnet Policy	Adds a FairNet policy for an IP address or range of addresses. Displays the **Add Fairnet Policy** dialog.
Delete Fairnet Policy(s)	Deletes the selected FairNet policies.
Update	Applies the latest configuration settings.
Reset	Cancels any changed configuration settings.
Checkboxes	
Enable FairNet	Enables the FairNet feature.
FairNet Policies	In the **FairNet Policies** table header: Selects or deselects all the policies in the **FairNet Polices** table. Individual policies can also be selected from the policies list.
Fairnet Policies Table Columns	
Direction	Displays the direction for each policy. The directions include: • Uplink • Downlink • Both
Start IP	Displays the start point for the IP address range.
End IP	Displays the end point for the IP address range.
Min Rate (kbps)	The minimum bandwidth that clients are guaranteed. Minimum rate is 1 Kbps.
Max Rate (kbps)	The maximum bandwidth that clients are guaranteed. Maximum rate is 54000 Kbps.
Interface	Displays the interface to which the FairNet policy applies. This is the interface on the managing firewall that the access point is connected to.
Enable	Enables the selected FairNet policy when the box is checked.
Configure	Edits existing FairNet policies when the **Edit** icon is clicked. Deletes the specific FairNet policy when the **Delete** icon is clicked.

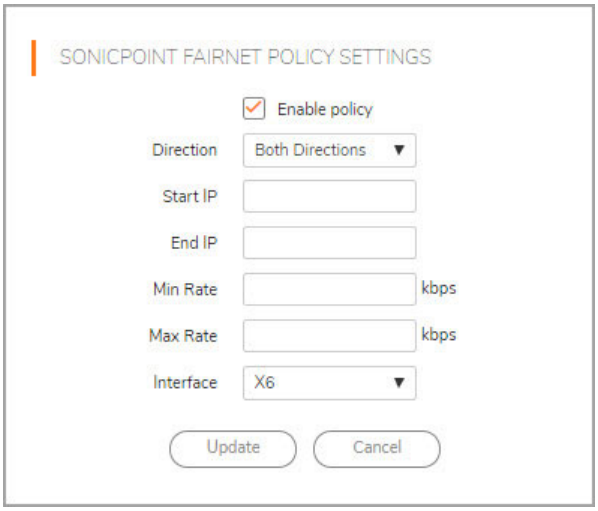
Configuring FairNet

This section contains an example FairNet configuration.

To configure FairNet to provide more bandwidth in both directions:

1 Navigate to the **Access Points > FairNet** page.

2 Click **Add New FairNet Policy**.



3 Check **Enable policy**. This is checked by default.

4 From the **Direction** drop-down menu, select **Both Directions**. This applies the policy to clients uploading content and downloading content. This is the default.

5 In the **Start IP** field, enter the starting IP address (for example, `172.16.29.100`) for the FairNet policy.

6 In the **End IP** field, enter the ending IP address (for example, `172.16.29.110`) for the FairNet policy.

TIP: The IP address range must be on a subnet that is configured for a WLAN interface.

7 In the **Min Rate (kbps)** field, enter the minimum bandwidth for the FairNet policy. The minimum and default is 100Kbps, and the maximum is 300Mbps (300,000Kbps).

8 In the **Max Rate (kbps)** field, enter the maximum bandwidth for the FairNet policy. The minimum and default is 100Kbps, and the maximum is 300Mbps (300,000Kbps), although a typical setting is 20Mbps.

9 From the **Interface** drop-down menu, select the interface (for example, `X2`) that the access point is connected to.

10 Click **Update** and the FairNet Policy is added to the **FairNet Policies** table.

11 Click **Enable FairNet**.

12 Click **Update**.

Your SonicWall FairNet policy is now configured.

12

Configuring Wi-Fi Multimedia

GMS access points support Wi-Fi Multimedia (WMM) to provide a better Quality of Service (QoS) experience on bandwidth-intensive applications such as VoIP, VoIP on Wi-Fi phones, and multimedia traffic on wireless IEEE 802.11 networks.

WMM is a Wi-Fi Alliance interoperability certification based on the IEEE 802.11e standard that prioritizes traffic according to four Access Categories:

- **Voice**—highest priority
- **Video**—second priority
- **Best effort**—third priority (intended for applications like email and Internet surfing)
- **Background**—fourth priority (intended for applications that are not latency sensitive, such as printing)

NOTE: WMM does not provide guaranteed throughput.

Topics:

WMM Access Categories

Each Access Category has its own transmit queue. Traffic is assigned to the appropriate Access Category based on type of service (ToS) information that is provided by either the application or the firewall. SonicWall security appliances assign ToS either through access rules or VLAN tagging.

The following table shows how the WMM Access Categories map to 802.1D user priorities.

Wi-Fi Multimedia Access Categories

Priority	User Priority (Same as 802.1D user priority)	802.1D designation	WMM Access Category (AC)	WMM AC Designation (informative)
Lowest	1	BK	AC_BK	Background
	2	—	AC_BK	Background
	0	BE	AC_BE	Best Effort
	3	EE	AC_BE	Best Effort
	4	CL	AC_VI	Video
	5	VI	AC_VI	Video
	6	VO	AC_VO	Voice
Highest	7	NC	AC_VO	Voice

WMM prioritizes traffic through a process known as Enhanced distributed channel access (EDCA). It prioritizes traffic by defining a different range of "back-off" periods for each Access Category. The WMM back-off periods are defined by two parameters:

- **Arbitration Inter-Frame Space (AIFS)** – The time interval between the wireless channel becomes idle and when the AC can begin negotiating access to the channel.
- **Contention Window (CW)** – The range of possible values for the random back-off periods. A range of time that specifies the random back-off period. The CW is defined by a minimum and maximum value:
  - **Minimum contention window size (CWMin)** – The initial upper limit of the length of the CW. The AC waits for a random time between 0 and CWMin before attempting to transmit. Higher priority AC with higher priority is assigned a shorter CWMin.
  - **Maximum contention window size (CWMax)** – The upper limit of the CW. If a collision occurs, the AC doubles the size of the CW, up to the CWMax, and attempts to transmit again. The CWMax must be larger than the CWMin.

Higher priority ACs are generally given lower values for AIFS, CWMin, CWMax.

NOTE: The unit of measure for AIFS, CWMin, and CWMax is multiples of the slot time for the 802.11 standard that is being used. For 802.11b, one slot is 20 microseconds. For 802.11a and 802.11g, one slot is nine microseconds.

Separate WMM parameters are configured for the access points and for the station (the SonicWall security appliance). The following tables show the default WMM parameters for the access points and SonicWall security appliances.

Default WMM Parameters for Access Points

WMM Access Category (AC)	WMM AC Designation (informative)	CWMin	CWMax	AIFS
AC_BE(0)	Best Effort	4	6	3
AC_BK(1)	Background	4	10	7
AC_VI(2)	Video	3	4	1
AC_VO(3)	Voice	2	3	1

Default WMM Parameters for SonicWall Security Appliances

WMM Access Category (AC)	WMM AC Designation (informative)	CWMin	CWMax	AIFS
AC_BE(0)	Best Effort	4	10	3
AC_BK(1)	Background	4	10	7
AC_VI(2)	Video	3	4	2
AC_VO(3)	Voice	2	3	2

Assigning Traffic to Access Categories

WMM requires the access points to implement multiple queues for multiple priority access categories. To differentiate traffic types, the access point relies on either the application or the firewall to provide type of service (TOS) information in the IP data. SonicWall security appliances assign traffic to WMM Access Categories through two methods:

- Specifying Firewall Services and Access Rules
- VLAN Tagging

Specifying Firewall Services and Access Rules

Services using a certain port can be prioritized and put into a proper transmit queue. For example, UDP traffic sending to port 2427 can be regarded as a video stream. Add a custom service on the **Firewall > Service Objects** page.

At least one access rule should be added on the **Firewall > Access Rules** page for the new service. For example, when such a service happens from a station on the LAN zone to a wireless client on the LAN zone to a wireless client on the WLAN zone, an access rule can be configured in the **General** tab of the **Add Rule** window. In the **QoS** tab of the **Add Rule** window, an explicit DSCP value is defined.

Later, when packets are sent to the access point through the firewall using UDP protocol with destination port 2427, their TOS fields are set according to the QoS setting in the access rule.

VLAN Tagging

Prioritization is possible in VLAN over virtual access point because the SonicWave, SonicPoint N and ACs allow a virtual access point to be configured to connect with a VLAN by using same VLAN ID. You can set priority for VLAN traffic through a firewall access rule.

The firewall access rule is similar to setting priority for a UDP service destined to a port such as 2427, but is configured with a VLAN (VLAN over VAP) interface, such as WLAN Subnets, as the **Source** and **Destination** is a WLAN-to-WLAN rule. Refer to **Firewall > Access Rules** for more information.

Configuring Wi-Fi Multimedia Parameters

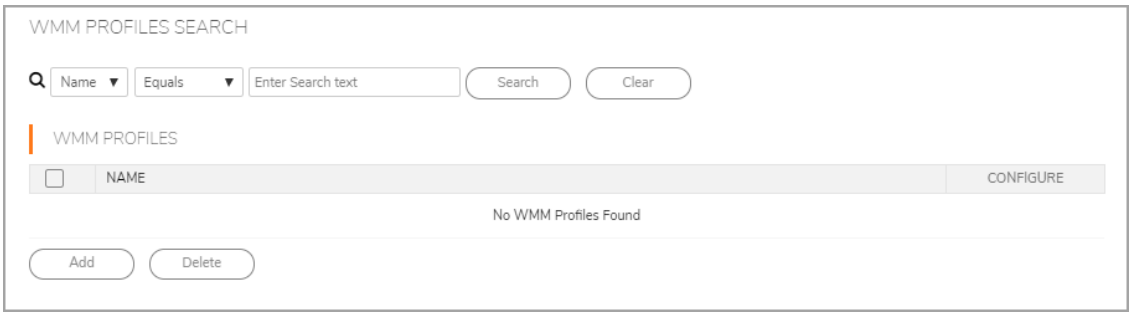
By default, a single WMM profile is configured on the SonicWall security appliance with the parameters set to the values on the 802.11e standard.

Topics:

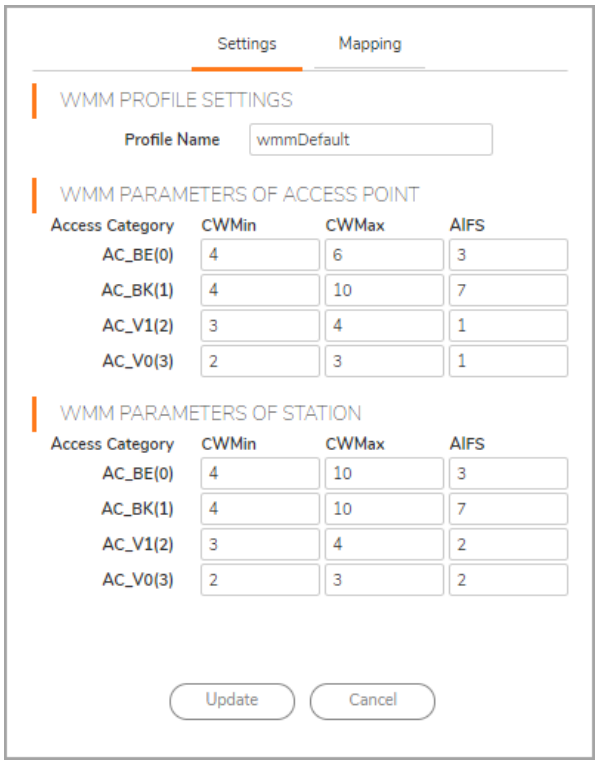
Configuring WMM

To customize the WMM configuration:

1 Navigate to the **Access Points > Wi-Fi Multimedia** page.



2 To modify the a WMM profile, click the **Edit** icon for that profile. Or, to create a new WMM profile, click **Add**.

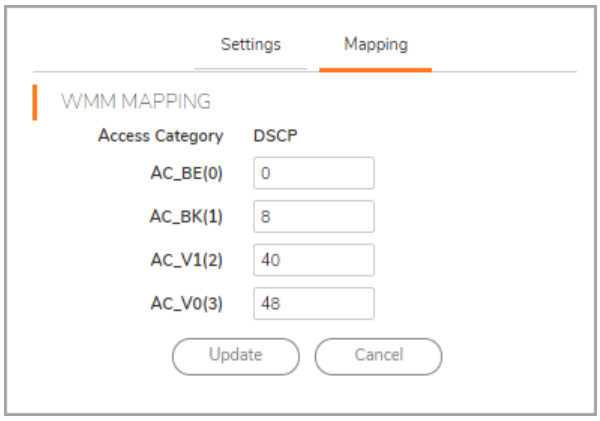


3 For a new WMM profile, enter a **Profile Name**. The default name is **wmmDefault**.

4 Modify the parameters to customize the WMM profile; the default WMM parameter values are auto-populated in the window. For information about these categories, see Wi-Fi Multimedia Access Categories.

NOTE: When configuring the WMM profile, you can configure the size of the contention window (CWMin/CWMax) and the arbitration interframe space (AIFS) number when creating a WMM profile. These values can be configured individually for each priority, AC_BK, AC_BE, AC_VI, and AC_VO on the access point (SonicPointN) and for the station (firewall).

5 Click the **Mapping** panel to customize how the Access Categories are mapped to DSCP values.



6 Map priority levels to DSCP values. The default DSCP values are as same as the ones in **Firewall > Access Rules, QoS** mapping.

7 Click **Update**.

Creating a WMM Profile for an Access Point

The **Access Points > Wi-Fi Multimedia** view provides a way to configure WMM profiles, including parameters and priority mappings.

You can also create a WMM profile or select an existing WMM profile when configuring a SonicWave, SonicPoint N or a SonicPoint AC Profile from the **Access Points > SonicPoints** page. The **Configuration** window provides a **WMM (Wi-Fi Multimedia)** drop-down menu on the **Advanced/Radio 0/1 Advanced** tabs.

Selecting **Create New WMM Profile…** from the **WMM (Wi-Fi Multimedia)** drop-down menu displays the **Add Wlan WMM Profile** Window.

Deleting WMM Profiles

To delete a single WMM Profile:

1. Navigate to the **Access Points > Wi-Fi Multimedia** page.
2. Click the **Delete** icon in the profile's **Configure** column.

To delete multiple WMM Profiles:

1. Navigate to the **Access Points > Wi-Fi Multimedia** page.
2. Check one or more boxes next to the profiles to delete or the leftmost checkbox next to the **Name** column to delete all profiles.
3. Click **Delete**.

13

SonicWall Support

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

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

The Support Portal enables you to:

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

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

About This Document

Legend

NOTE: A NOTE icon indicates supporting information.

IMPORTANT: An IMPORTANT icon indicates supporting information that may need a little extra attention.

TIP: A TIP 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.

Global Management System Access Points Administration
Updated - October 2020
Software Version - 9.3
232-005123-00 Rev B