SonicOS 7

Access Points

Administration Guide

SONICWALL®

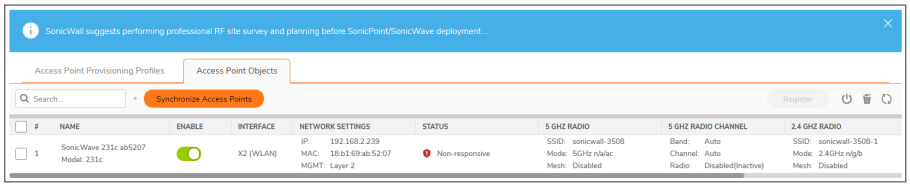
Contents

1

Settings

The most effective way to provision wireless access points is let the SonicOS firewall automatically detect the access points and use one of the default profiles. SonicOS includes four default profiles, one for each generation of SonicWall access points: SonicPointN, SonicPointNDR, SonicPointACe/ACi/N2, and SonicWave. 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 **Device > Access Points > Settings** page displays informational messages and shows the firmware version for operational access points.



The access point profiles are displayed in the **Access Point Provisioning Profiles** tab. You can edit each profile or add a new profile.

The **Access Point Objects** tab displays the settings for connected access points, and provides Edit icons to edit them or perform other actions.

NOTE: When wireless LAN is disabled, all Access Points and Wireless related pages disappear. Wireless Zone is removed from zone type. And any existing WLAN zones or objects are not editable anymore.

Topics:

Synchronize Access Points

Click **Synchronize Access Points** at the top of the **Device > Access Points > Settings** 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. SonicOS 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.

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). Upon initializing, the unit attempts to find a SonicOS device with which to peer. When a SonicOS device starts up, it also searches for access points through the SonicWall Discovery Protocol. If the access point and a peer SonicOS 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, SonicOS 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. SonicOS 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:

- Through 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.
- Through 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 SonicOS 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

On the **Device > Access Points > Settings** page, 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/432i/432o/224w/231c/231o. SonicPoint ACs are supported on appliances running SonicOS 6.2.2 and newer, while SonicWave devices are supported on SonicOS 6.5 and newer.

Navigate to **Device > Access Points > Settings** page. The four default SonicOS profiles are listed along with any custom profiles you've developed under the **SonicPoint/SonicWave Provisioning Profiles** section. To modify any of the default provisioning profiles, hover on the profile and click the **Edit** icon, and make the appropriate changes.

IMPORTANT: Because creating or modifying the SonicPoint/SonicWave Provisioning Profiles are 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 New Profile** option has several screens where similar settings are grouped. The procedures are grouped to match those screens.

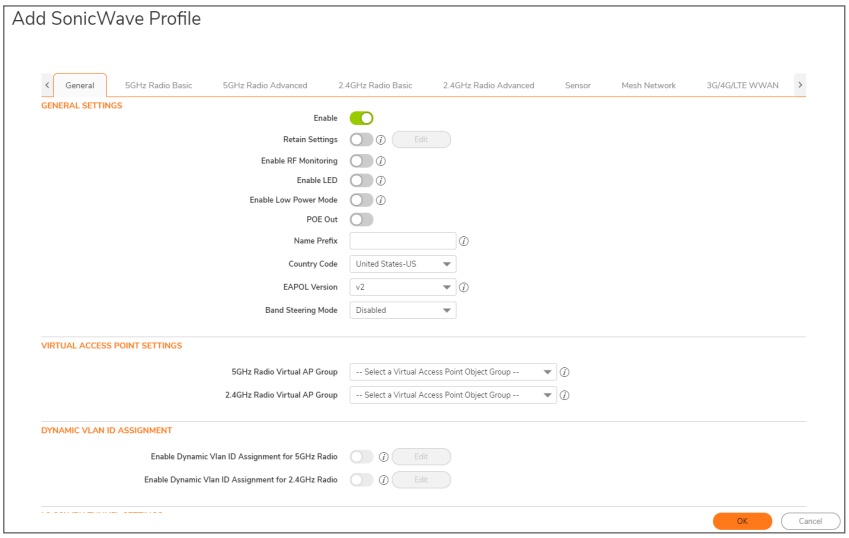
Topics:

Adding/Editing a Provisioning Profile - Getting Started

To add a new provisioning profile:

1. Navigate to **Device > Access Points > Settings > Access Point Provisioning Profiles** page.
2. In the **Add New Profile** drop-down, select the type of profile you want to build. For an example, **SonicWave Profile** was selected.

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



General Settings for Provisioning Profiles

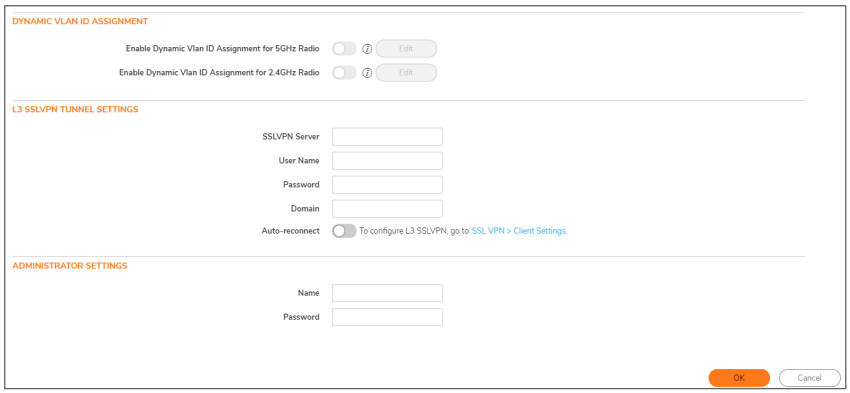
To configure the options on the General screen:

1. Set the **SonicWave Settings**.

Option	Action
Enable	When selected, enables the SonicWave access point. By default, this option is enabled.
Retain Settings	When selected, retains the customized until the next time the unit is rebooted. **Edit** option is enabled and the Retain Settings dialog is displayed. You can customize which settings needs to be retained.
Enable RF Monitoring	When selected, enables wireless RF-threat, real-time monitoring and management.
Enable LED	When selected, turns on the SonicWave LEDs. If left unchecked, which is the default, the LEDs stay off.
Enable Low Power Mode	When selected, allows the SonicWave to operate in a low power mode because of the power source not being standard 802.3at 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**.

2. 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.

3. Scroll down to see the other General Settings.



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

   To enable the options under **Dynamic VLAN ID Assignment**, you need create a WLAN zone under **Object > Match Objects > Zones** and VLAN interface under **Network > System > VLAN Translation**.

5. Configure the **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. Select the **Auto-Reconnect** option to enable it.
   f. If you want to configure Layer 3 SSLVPN, click **SSL VPN > Client Settings** and define the appropriate settings.

6. Set the **Administrator Settings**:

   a. Type in the user **Name** of the network administrator.
   b. Type in the **Password** for the network administrator.

5GHz/2.4GHz Radio Basic Settings for Provisioning Profiles

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.If a VAP group was selected in the General settings, however, a different options display.

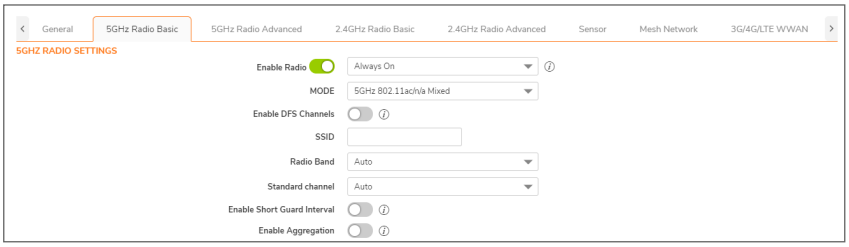
The following topics describe settings on the **5GHz/2.4GHz Radio Basic** screens:

Topics:

Radio Settings

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

1. Click on **5GHz Radio Basic** or **2.4GHz Radio Basic**.



2. Select **Enable Radio** to enable the radio bands automatically on all access points provisioned with this profile. This option is selected by default.
3. 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**.
4. Select your preferred radio mode from the **Mode** drop-down menu:

RADIO MODE CHOICES

5GHz Radio Basic	2.4GHz 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 (2.4GHz 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 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 5GHz/2.4GHz 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.

5. 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 SonicPoints or SonicWaves in your organization share the same SSID, it is easier for users to maintain their wireless connection when roaming from one access point to another.

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

   NOTE: When **Mode = 5GHz 802.11a Only**, the **Radio Band** option 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 the radio 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 the radio 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 the 5GHz Radio 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**.)

7. 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 drop-down menu.
	Wide - 80 MHz Channel	Select **Auto** or one of the radio channels in the **Channel** drop-down menu.
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** drop-down menu.
	Wide - 80 MHz Channel	Select **Auto** or one of the radio channels in the **Channel** drop-down menu.

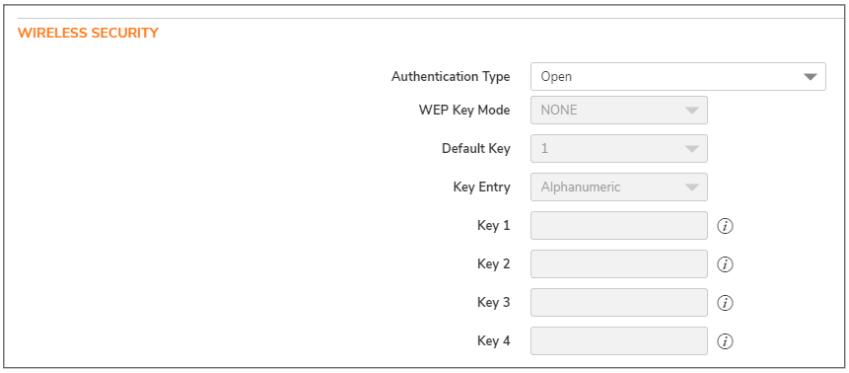
8. Select **Enable Short Guard Interval** to enable it. This allows you to increase the radio data rate by shortening the guard interval. Be sure the wireless client can support this to avoid compatibility issues.
9. Select **Enable Aggregation** to enable it. This allows you to increase the radio throughput by sending multiple data frames in a single transmission. Be sure the wireless client can support this to avoid compatibility issues.

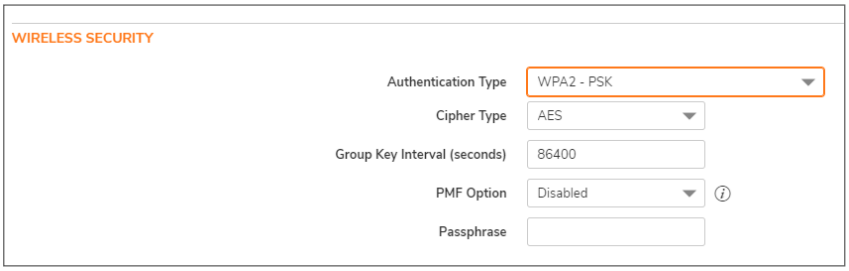
Wireless Security

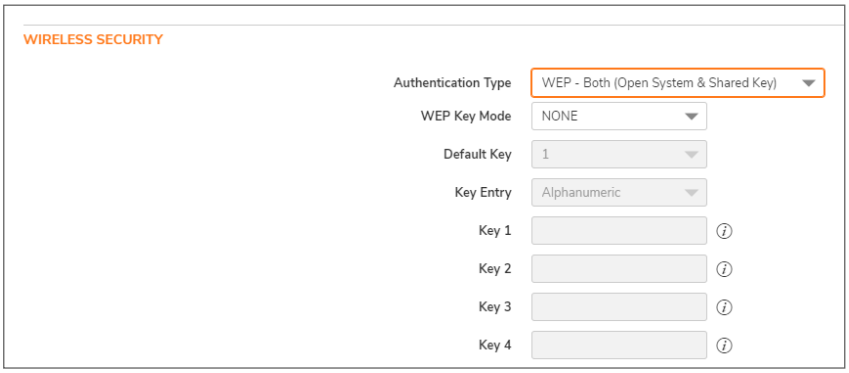
NOTE: The SonicOS interface is context-sensitive. If a VAP Group was selected in the **General** screen, the **Wireless Security** section is hidden and you can skip this section.

To set the Wireless Security options:

1. Scroll down to the **Wireless Security** section. The options vary depending on the selected **Authentication Type**.







To configure Wireless Security:

1. 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. If a **WPA2 - EAP** option is selected, the **Radius Server Settings** section is displayed.

2. Define the remaining settings, using the following tables 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.	• In **Default Key** field, select the default key (the key that is tried first). **Key 1** is the default. • In the **Key Entry** field, choose whether the key is **Alphanumeric** or **Hexadecimal (0-9, A-F)**. • 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.	• In **Default Key** field, select the default key (the key that is tried first). **Key 1** is the default. • In the **Key Entry** field, choose whether the key is **Alphanumeric** or **Hexadecimal (0-9, A-F)**. The **Hexadecimal** option is the default. • 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	• Select **Cipher Type** from the drop-down menu. Options are **AES** (default), **TKIP**, or **Auto**.

	Description
Authentication Type	**Settings**
	• Set the **Group Key Interval** in seconds. The default is **86400**. • For SonicWave, select the **PMF Option** from the drop-down menu. See Protected Management Frames (PMF Option). • Define the **Passphrase** for the public shared key.
WPA2 - EAP	• For SonicWave, select the **Authentication Balance Method** from the drop-down menu. See About Local Radius Servers and EAP Authentication Balancing. • Select **Cipher Type** from the drop-down menu. Options are **AES** (default), **TKIP**, or **Auto**. • Set the **Group Key Interval** in seconds. The default is **86400**. • For SonicWave, select the **PMF Option** from the drop-down menu. See Protected Management Frames (PMF Option).
WPA2 - AUTO - PSK	• Select **Cipher Type** from the drop-down menu. Options are **AES** (default), **TKIP**, or **Auto**. • Set the **Group Key Interval** in seconds. The default is **86400**. • For SonicWave, select the PMF Option from the drop-down menu. See Protected Management Frames (PMF Option). • Define the **Passphrase** for the public shared key.
WPA2 - AUTO - EAP	• For SonicWave, select the **Authentication Balance Method** from the drop-down menu. See About Local Radius Servers and EAP Authentication Balancing. • Select **Cipher Type** from the drop-down menu. Options are **AES** (default), **TKIP**, or **Auto**. • Set the **Group Key Interval** in seconds. The default is **86400**. • For SonicWave, select the **PMF Option** from the drop-down menu. See Protected Management Frames (PMF Option).

Protected Management Frames (PMF Option)

When **Authentication Type** is set to any **WPA2** option, the **PMF Option** setting is available. The **PMF Option** setting is supported for SonicWave profiles starting in SonicOS 6.5.2. This feature supports the IEEE 802.11w-2009 amendment to the IEEE 802.11 standard for protection of wireless management frames. It is also known as the Protected Management Frames (PMF) standard.

You can select one of the following settings from the **PMF Option** drop-down menu under **Wireless Security**:

- **Disabled** – The service is not enabled. Clients connect without PMF.
- **Enabled** – The service is optional for wireless clients. Clients can connect with or without PMF, based on client settings.
- **Required** – Clients must have PMF enabled to connect.

While the 802.11i amendment protects **data** frames, management frames such as authentication, de-authentication, association, dissociation, beacons, and probes are used by wireless clients to initiate and tear down sessions for network services. Unlike data traffic, which can be encrypted to provide a level of confidentiality, these frames must be heard and understood by all clients and therefore must be transmitted as open or unencrypted. While these frames cannot be encrypted, they must be protected from forgery to protect the wireless medium from attacks. For example, if an attacker obtains the MAC address of a client, it can send a disassociation request to the client in the name of an AP, or send a re-association request to an AP in the name of the client. The client is logged off in either situation.

The 802.11w amendment applies to a set of robust **management** frames that are protected by the Protected Management Frames (PMF) service. These include Disassociation, De-authentication, and Robust Action frames. 802.11w protects only specific management frames and does not affect the communication between access points and clients. 802.11w can only take effect when both access points and clients have 802.11w enabled.

802.11w provides the following benefits:

Confidentiality	Encrypts Unicast management frames:
	Uses same PTK as for data frames
	Protects the previously unencrypted frame header through additional authentication data (AAD)
	Extended AES-CCM to handle Unicast management frames
	Separate Receive Sequence Counter (RSC) for replay protection
Group addressed frame protection	Broadcast/Multicast Integrity Protocol (BIP) protects the integrity of broadcasts and multi casts, prevents replay attacks, and protects clients from spoofing broadcast/multicast attacks. For Broad-/Multi casts Management Frames:
	Uses new Integrity Group Temporal Key (IGTK) received during WPA key handshake
	New Algorithm: Broadcast Integrity Protocol (BIP)
	New Information Element: Management MIC IE with Sequence Number + Cryptographic Hash (AES128-CMAC-based)
Connection protection	Security Association (SA) Query can prevent clients from going offline caused by spoofing re-association requests.

About Local Radius Servers and EAP Authentication Balancing

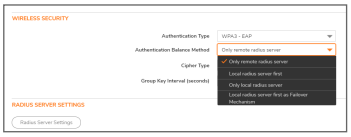
This feature is introduced in SonicOS 6.5.2. It allows local SonicWave access points to provide local radius authentication service within selected SonicWaves and integrates with corporate directory services,

including native LDAP systems and Active Directory. In this scenario, the SonicWave provides EAP authentication for clients and functions as both the authenticator and authentication server simultaneously. LDAP cache and TLS cache are supported for fast performance when reconnecting.

To configure this feature, you need:

- An interface in the WLAN zone with one or more local RADIUS servers configured in the subnet; these are the SonicWave local RADIUS servers
- WLAN zone configured with the **Enable Local Radius Server** option selected on the **Radius Server** screen; this option controls whether this feature is enabled or not.
- SonicWave profile with the following settings on the **Radio Basic** screen(s):
    - One of the **WPA2 - EAP** types selected for **Authentication Type**

      The **Radius Server Settings** section is displayed where you can configure the local RADIUS server settings. See Configuring Radius Server Settings for details.
    - One of the **Local Radius Server** options selected for **Authentication Balance Method**.

      Local radius server first – With this option selected, when a client tries to authenticate, a local RADIUS server is used first. If the authentication fails, the authentication request is sent to the remote RADIUS server.

      Only remote radius server – Only use the remote RADIUS server for authentication.

      Only local radius server – Only use the local RADIUS server for authentication.

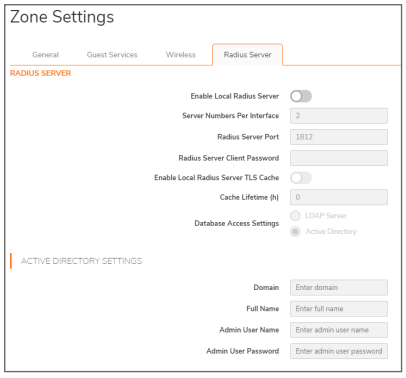
      Local radius server As Failover Mechanism – When the remote RADIUS server is down, the local RADIUS server are used automatically.
    - NAT policy, Access Rule, Address Group, RADIUS pool - automatically configured.

When you enable a local radius server on a SonicWave, a NAT policy and access rule are automatically created. The SonicOS NAT module has failover and load balance methods, so a Radius server pool is supported. Additional SonicWaves with a local radius server configured can be added to this pool. More than one local radius server provides a failover mechanism and optimizes network performance.

The **Enable Local Radius Server** option and other settings are configured in the **Radius Server** screen available when configuring the **WLAN zone**, configured from the **Object > Match Objects > Zones** page. This screen provides options for setting the number of RADIUS servers per interface, the server port, the client password, the TLS cache, and LDAP or Active Directory access settings. When you enable a local radius server on a SonicWave, the configured RADIUS server port and client password are used on that SonicWave.

ⓘ **NOTE:** The SonicWave DNS server must be able to resolve the name of the LDAP server or Active Directory server domain.

The **Server Numbers Per Interface** option controls the number of local RADIUS servers under one specific interface in this zone. Increasing this value means more SonicWaves can be add to the RADIUS pool. The minimum value is 1, and the maximum is equal to maximum number of SonicWaves per interface in a WLAN Zone. Because the number configured for the option can be smaller than the number of connected SonicWaves, the specific SonicWaves configured as local radius servers is not fixed.



When the **Enable Local Radius Server TLS Cache** option is enabled, the client and the server can cache TLS session keys and use these to reduce the delay in time between an authentication request by a client and the response by the RADIUS server. Clients can also perform a fast reconnect. When enabled, you can set the **Cache Lifetime** option to the number of hours that cached entries are saved. The cache lifetime can be a number between one hour and 24 hours.

When the security appliance powers up, if **Enable Local Radius server** is enabled on the WLAN zone, an address object, the Radius Pool, a NAT policy, and an access rule should be created. The Radius Pool name is a combination of the interface name plus “Radius Pool,” for example, X2 Radius Pool. A new address object is automatically created for the SonicWave acting as a Radius server, which is named with the interface name and MAC address of the SonicWave, for example, *X2 18:b1:69:7b:75:2e*. This address object is added to the RADIUS Pool if seats are available.

If **Enable Local Radius server** is disabled, the SonicWave address object, Radius pool, NAT policy, and access rule are removed, and a **Delete** command by restApi is sent to the SonicWaves which are in the Radius pool to make the local Radius server go down.

If the WLAN zone is edited, the NAT policy and access rule are removed and re-created. The radius pool always exists unless **Enable Local Radius server** is disabled.

If the interface changes, the NAT policy, access rule, and radius pool are removed and created again if the interface is still bound to the WLAN Zone.

Configuring Radius Server Settings

If you selected either **WPA2 - EAP** or **WPA2 - AUTO - EAP** in the **Wireless Security** section, the **Radius Server Settings** section appears for configuration of 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. Click **Radius Server Settings**. The Radius Server Settings dialog displays. The options displayed on this dialog depend on the type of SonicPoint/SonicWave.

2. In the **Retries** field, enter the number times, from 1 to 10, the firewall attempts to connect before it fails over to the other Radius server.
3. In the **Retry Interval** field enter the time, from 0 to 60 seconds, to wait between retries. The default number is 0 or no wait between retries.

4. 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

5. 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

6. 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**
   - **SSID** – When the SSID option is selected, both the RADIUS authentication message and RADIUS accounting message carry the access point SSID.
7. To send the NAS IP address to the RADIUS Server, enter the address in the **NAS IP Addr** field.
8. 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 SonicOS. 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. Toggle the option to **Enable MAC Filter List**. When the MAC filter list is enabled, the other settings are also enabled so you can set them.
2. In the **Allow List**, select an option from the drop-down menu. This identified which MAC addresses you allow to have access.

   Choose **Create MAC Address Object Group** if you want to create a new address object group made up of those you want to have access. Refer to *SonicOS Policies* for information.
3. In the **Deny** List, select an option from the drop-down menu. This identified which MAC addresses that you deny access to.

   Choose **Create MAC Address Object Group** if you want to create a new address object group made up of those who should not have access. Refer to *SonicOS Policies* for information.
4. Toggle the option to **Enable MIC Failure ACL Blackist**.
5. 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.

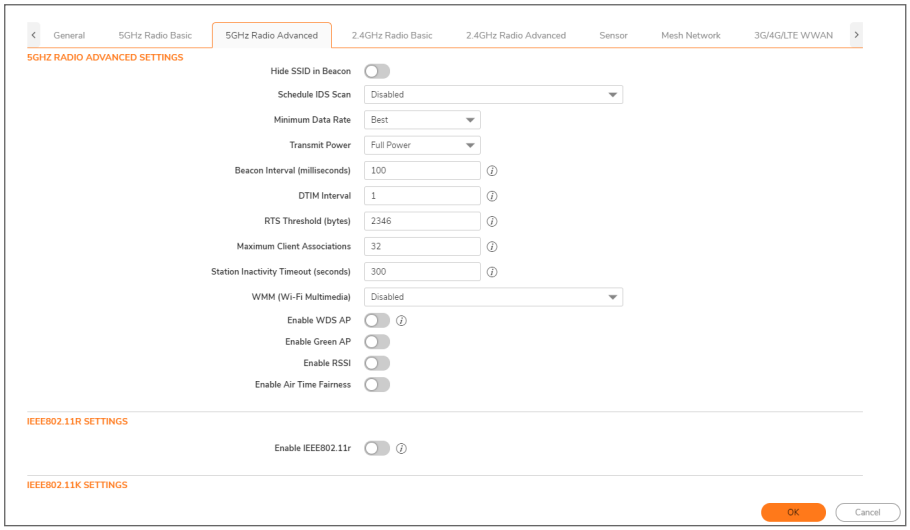
To allow wireless access control:

1. Toggle the option to **Enable Remote MAC Access Control**.
2. Click **Configure**.
3. If not already configured, set up the RADIUS Server(s) as described in Configuring Radius Server Settings.
4. 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 **5GHz Radio Advanced** screen has the same options as the **2.4GHz Radio Advanced** screen, plus other options. The screens are similar across the different access point models. Differences are noted in the procedure where needed.



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

1. Click **5GHz Radio Advanced** or **2.4GHz Radio Advanced** as needed.
2. Toggle the option 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.
3. 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.
4. 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.
5. 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**
6. 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.

7. 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.
8. 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).
9. 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).
10. 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).
11. 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**.
12. 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.
13. If you are configuring the **2.4GHz Radio Advanced** screen settings, define the following settings which 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
Protection Type	Select from the drop-down menu: • CTS Only (default) • RTS-CTS

Enable Short Slot Time	Select to allow clients to disassociate and reassociate 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.

14. 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.
    - A previously configured WMM profile
15. Toggle the option 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.
16. 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, 5GHz Radio and 2.4GHz Radio.
17. 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.
18. If configuring a SonicWave or SonicPoint ACe/ACi/N2 profile, select **Enable RSSI** to enable a RSSI threshold. Clients with signal strengths below the threshold are disassociated by the access point so that they are associated to a closer access point. This option is not selected by default.
19. If **Enable RSSI** is selected, enter the threshold value as a negative number into the **RSSI Threshold (dBm)** field. The default is -95 dBm. For more information about RSSI thresholds, see Configuring the RSSI Treshold.
20. If configuring a SonicWave device, toggle the option to **Enable Air Time Fairness**.

    This feature is disabled by default. If enabled, it steers the traffic for devices that can use the 5GHz band to that band because it usually has less traffic and less interference. If the signal strength or signal conditions are better on the 2.4GHz band, traffic is steered to that band. The intention is to use both bands in the most effective manner.
21. Under **IEEE802.11r Settings**, select **Enable IEEE802.11r** to enable secure, fast roaming. If **Enable IEEE802.11r** is selected, you can select the other options:
    - **Enable FT over DS** – enable fast transition over DS
    - **Enable IEEE802.11r Mix Mode** – enable fast transition in mixed mode

    For more information about these options, see Configuring IEEE802.11r Settings for Secure Fast Roaming.
22. Under **IEEE802.11k Settings**, select **Enable Neighbor Report** to enable collection of information about neighboring access points. This option is not selected by default. See Configuring IEEE802.11k Settings for Dynamic Radio Management for more information.
23. Under **IEEE802.11v Settings**, select **Enable BSS Transition Management** to enable the access point to request a voice client to transition to a specific access point if the client sends a query to the access point. This option is not selected by default. See Configuring IEEE802.11v Settings for Dynamic Environment Management for more information.

24. Under **IEEE802.11v Settings**, select **Enable WNM Sleep Mode** to enable a non-access point station to signal to an access point that it is sleeping for a specified time. This option is not selected by default. See Configuring IEEE802.11v Settings for Dynamic Environment Management for more information.

Configuring the RSSI Treshold

In areas large enough to require multiple access points to provide good WiFi coverage across the whole area, one would expect a WiFi client to detect and move to the closest access point. Unfortunately, many WiFi clients tend to hang on to the original access point they associated with, rather than moving to a nearby access point that would generally be a better choice for them. This is referred to as sticky behavior and results in a low RSSI (Received Signal Strength Indicator) and a high SNR (Signal-to-Noise Ratio). The farther away from the original access point the client moves, the weaker its RSSI gets and the worse its SNR gets. Retransmissions occur, dynamic rate-shifting happens, and the client communicates at a much lower data-rate. A lower data-rate consumes more air-time to transfer the same information, resulting in higher channel utilization. Ideally, the client would roam to the closest access point, and the resulting RF space would be better for everyone.

Beginning in SonicOS 6.5.2, RSSI thresholds are supported. When the client reaches a certain RSSI level from the perspective of the access point, the access point disassociates from the client and the client then associates to a closer access point. The RSSI threshold is configurable.

RSSI measurements represent the relative quality of a received signal on a device after any possible loss at the antenna and cable level. The higher the RSSI value, the stronger the signal. When measured in negative numbers, the number that is closer to zero usually means better signal. As an example, -50 dBm is a pretty good signal, -75 dBm is fairly reasonable, and -100 dBm is no signal at all.

Configuring IEEE802.11r Settings for Secure Fast Roaming

Many deployed implementations of IEEE 802.11 WiFi have effective ranges of only a few hundred meters, so, to maintain communications, devices in motion need to hand-off from one access point to another. In an automotive environment, this could easily result in a hand-off every five to ten seconds.

Hand-offs are already supported under the existing standard. The fundamental architecture for hand-offs is identical for 802.11 with and without 802.11r: the mobile device is entirely in charge of deciding when to hand-off and to which access point it wishes to hand-off. In the early days of 802.11, hand-off was a much simpler task for the mobile device. Only four messages were required for the device to establish a connection with a new access point (five if you count the optional “I'm leaving” message [deauthentication and disassociation packet] the client could send to the old access point). However, as additional features were added to the standard, including 802.11i with 802.1X authentication and 802.11e or WMM with admission control requests, the number of messages required went up dramatically. During the time these additional messages are being exchanged, the mobile device's traffic, including that from voice calls, cannot proceed, and the loss experienced by the user could amount to several seconds. Generally, the highest amount of delay or loss that the edge network should introduce into a voice call is 50 ms.

802.11r undoes the added burden that security and quality of service added to the hand-off process and restores it to the original four-message exchange. In this way, hand-off problems are not eliminated, but at least are returned to the status quo.

The primary application currently envisioned for the 802.11r standard is voice over IP (VOIP) through mobile phones designed to work with wireless Internet networks, instead of (or in addition to) standard cellular networks.

Configuring IEEE802.11k Settings for Dynamic Radio Management

The **IEEE802.11k Settings** section of the 5GHz or 2.4GHz Radio Advanced screen provides the **Enable Neighbor Report** option. Enabling this option makes the access point collect radio measurements, as defined by the IEEE802.11k amendment to the 802.11 standard.

The Neighbor Report request is sent from a client to an access point. The access point returns a Neighbor Report report containing information about neighboring access points that are known candidates for the client to reassociate with (should the client choose to do so). Therefore, the Neighbor Report request/report pair enables the client to collect information about the neighboring access points of the access point it is currently associated to, and this information might be used as identification of potential candidates for a new point of attachment while roaming.

The benefits of the neighbor/request report are:

- **Speeds up scanning** – Instead of the client engaging in time-consuming scanning activity (either actively probing for access points or passively listening to every channel for beacons), the client can instead narrow its list to the known available neighbors. This is especially useful in high-density environments where multiple WLANs can be heard by the client
- **Reduces client power consumption** – The time taken by scanning (especially active scanning) also consumes battery power for the client. As the neighbor report provides information before roaming, less power might be consumed
- **More efficient use of WLAN air time** – Active scanning is not only time consuming from the perspective of client resources (such as CPU, memory, radio), it's also air-time consuming. For example, a client that is not neighbor-aware likely engages in so-called wildcard probe requests (some clients burst these). In this scenario, typically every access point that hears the probe request generates a probe response. In other words, for a single client, N number of access points generate N probe responses. If multiple clients engage in wildcard probing, then the RF environment can quickly become polluted with management traffic simply because the clients are not using neighbor request. This has a negative impact for the entire WLAN.

Configuring IEEE802.11v Settings for Dynamic Environment Management

802.11v refers to the IEEE802.11 Wireless Network Management (Amendment 8). This is an amendment to the IEEE 802.11 standard to allow configuration of client devices while connected to wireless networks. Stations that support WNM (Wireless Network Management) can exchange information with each other (access points and wireless clients) to improve their performance of the wireless network. 802.11v allows client devices to exchange information about the network topology, including information about the RF environment, making each client network aware, facilitating overall improvement of the wireless network.

Stations use WNM protocols to exchange operational data so that each station is aware of the network conditions, allowing stations to be more cognizant of the topology and state of the network. WNM protocols

provide a means for stations to be aware of the presence of collocated interference, and enable stations to manage RF parameters based on network conditions.

In addition to providing information on network conditions, WNM also provides a means to exchange location information, provide support for multiple BSSID capability on the same wireless infrastructure, support efficient delivery of group addressed frames, and enable a WNM-Sleep mode in which a STA can sleep for long periods without receiving frames from the AP.

BSS Max idle period management has been supported by SonicWall SonicPoints. SonicWave supports two more WNM services to improve the performance of wireless network:

- **Enable BSS transition management** – Enables an access point to request a voice client to transition to a specific access point, or suggest a set of preferred access points to a voice client, because of network load balancing or BSS termination. This helps the voice client identify the best access point to which that client should transition to as that client roams.

  The BSS Transition capability can improve throughput, data rates and QoS for the voice clients in a network by shifting (through transition) the individual voice traffic loads to more appropriate points of association within the ESS.

  802.11v BSS Transition Management Request is a suggestion given to the client. The client can make its own decision whether to follow the suggestion or not.

  BSS Transition Management uses these frame types:

  - **Query** – A Query frame is sent by the voice client that supports BSS Transition Management requesting a BSS transition candidate list to its associated access point, if the associated access point indicates that it supports the BSS transition capability.
  - **Request** – An access point that supports BSS Transition Management responds to a BSS Transition Management Query frame with a BSS Transition Management Request frame.
  - **Response** – A Response frame is sent by the voice client back to the access point, informing whether it accepts or denies the transition.
- **WNM-Sleep mode** – An extended power-save mode for non-access point stations whereby a non-access point station need not listen for every delivery traffic indication message (DTIM) Beacon frame, and does not perform group temporal key/integrity group temporal key (GTK/IGTK) updates.

  WNM-Sleep mode enables a non-access point station to signal to an access point that it is sleeping for a specified time. This enables a non-access point station to reduce power consumption and remain associated while the station has no traffic to send to or receive from the access point.

  IMPORTANT: If the WNM-Sleep mode is enabled and the station supports WNM-Sleep mode, update the station to avoid Key Reinstallation Attack.

Sensor Settings for WIDP in Provisioning Profiles

In the Sensor screen, you can enable or disable Wireless Intrusion Detection and Prevention (WIDP) mode. In SonicOS 6.5.3 and higher, SonicWave appliances can function as both an access point and as a sensor to detect any unauthorized access point connected to a SonicWall network.

In earlier releases, access point or virtual access point functionality is disabled if this option is selected.

To configure the Sensor screen options:

1. Select **Enable WIDP sensor** to have the access point operate as a WIDP sensor. This option is not selected by default.
2. 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**.

Mesh Network Settings for Provisioning Profiles

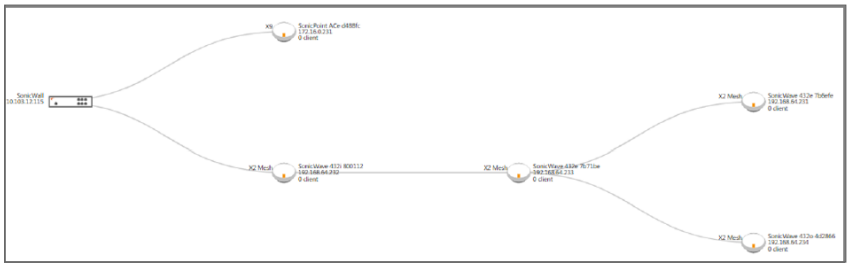
This features provides a scalable secure wireless network infrastructure across large coverage areas. You can utilize this feature to deploy and manage SonicWave access points.

Topics:

Setting Up a Mesh Network

To set up a mesh network:

1. Enable mesh in the SonicWave profile for your firewall as described in Enabling a Multi-hop Mesh Network.
2. Connect each SonicWave to this firewall by an Ethernet cable.
3. When a SonicWave's state becomes operational, disconnect the cable from that appliance.
4. Keep one SonicWave connected to the firewall.
5. Move the disconnected SonicWave to its designated location.
6. Power up all the SonicWaves.
7. To view the network, navigate to **Device > Access Points > Topology View**.

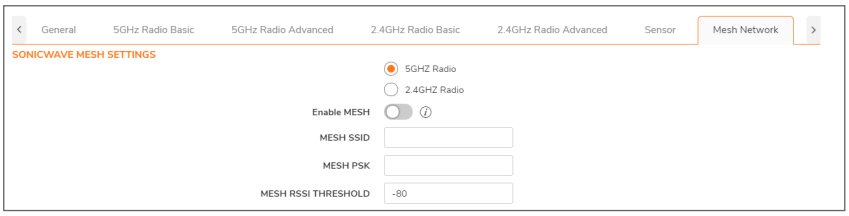


Enabling a Multi-hop Mesh Network

To enable multi-hop mesh networks:

1. Navigate to **Device > Access Points > Settings** page.
2. Click **Access Point Provisioning Profiles**.
3. Click on the **Edit** icon for the SonicWave profile. The **Edit SonicWave** Profile dialog displays.

4. Click **Mesh Network**.



5. Choose the radio to be used for the mesh network:
   - **5GHZ Radio**
   - **2.4GHZ Radio**
6. To enable the radio band Mesh on the SonicPointAC, select **Enable Mesh**.
7. Enter the SSID for the WLAN network in **Mesh SSID**.
8. Enter the preshared key in **Mesh PSK**.
9. Enter the threshold in **Mesh RSSI Threshold**. The default is set as **-80**.
10. Click **OK**.

Active/Active Clustering Full Mesh

An Active/Active Clustering Full-Mesh configuration is an enhancement to the Active/Active Clustering configuration option and prevents any single point of failure in the network. All firewall and other network devices are partnered for complete redundancy. Full-Mesh ensures that there is no single point of failure in your deployment, whether it is a device (security appliance/switch/router) or a link. Every device is wired twice to the connected devices. Active/Active Clustering with Full-Mesh provides the highest level of availability possible with high performance; see below table.

IMPORTANT: The routers in the security appliance's upstream network should be preconfigured for Virtual Router Redundancy Protocol (VRRP).
Full Mesh deployments require that Port Redundancy is enabled and implemented.

BENEFITS OF ACTIVE/ACTIVE CLUSTERING FULL MESH

No Single Point of Failure in the Core Network	In an Active/Active Clustering Full-Mesh deployment, there is no single point of failure in the entire core network, not just for the security appliances. An alternative path for a traffic flow is always available in case there are simultaneous failures of switch, router, security appliance on a path, thus providing the highest levels of availability.
Port Redundancy	Active/Active Clustering Full-Mesh utilizes port redundancy in addition to HA redundancy within each Cluster Node, and node level redundancy within the cluster. With port redundancy, a backup link takes over in a transparent manner if the primary port fails. This prevents the need for device level failover.

3G/4G/LTE WWAN Settings for Provisioning Profiles

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

This features 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 connected, the SonicWave acts as a WWAN device for the firewall and provides WAN access.

When configuring the modem for the first time, you can use the wizard to take advantage of the auto-discovery features for this option.

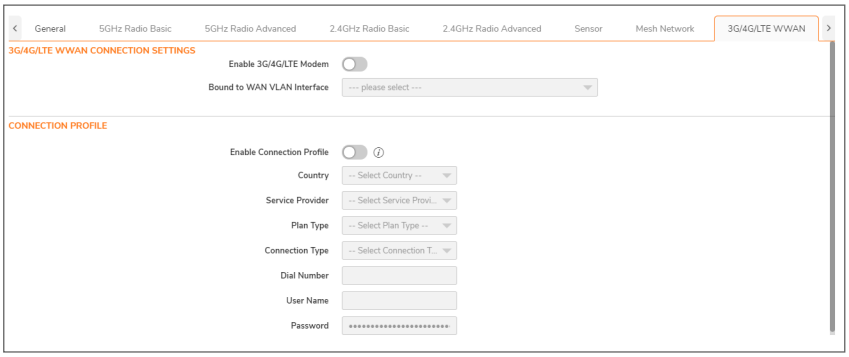
Topics:

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

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



2. Toggle the option to **Enable 3G/4G/LTE modem**.
3. 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 >System > Interfaces** section in *SonicOS 6.5 System Setup*.

   NOTE: When building a VLAN interface, set the zone to WAN zone and the parent interface to the physical interface the access point is connected to.
   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**.
4. In the **Connection Profile** section, toggle the option to **Enable Connection Profile**.

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

5. In the **Country** field, select the country where the access point is deployed.
6. Select the **Service Provider** from the drop-down menu.
7. Select the **Plan Type** from the drop-down menu. Depending on the selection, other fields are auto-populated.
8. If needed, add the **User Name** and **User Password** to the appropriate fields.
9. When all settings on the screen are done, click **OK**.

Using the 3G/4G/LTE WWAN Wizard

To configure the modem using the wizard:

1. Click **3G/4GLTE WWAN**.
2. Scroll to the bottom and click **3G/4G/LTE WIZARD**.
3. Click **Next**.
4. Choose a **VLAN Interface** from the drop-down menu, or toggle the option to **Create a New VLAN Interface**.

   If you opt to create a new VLAN interface, the remaining fields become active. Provide the data requested.

   NOTE: If you set **IP Assignment to DHCP**, the IP Address, Subnet Mask, and Default Gateway fields are hidden.
5. Click **Next**.
6. In the **Country** field, select the country where the access point is deployed.
7. Select the **Service Provider** for the drop-down menu.
8. Select the **Plan Type** from the drop-down menu. Depending on the selection, other fields are auto-populated.
9. If needed, add the **User Name** and **User Password** to the appropriate fields.
10. Click **Next**.
11. Click **Next** again to apply the settings.

Configuring Load Balancing among Multiple USB Modems

When multiple SonicPoint/SonicWaves and multiple 3G/4G modems (at least two of each) are available, load balancing can be performed among these multiple pairs of SonicPoint/SonicWaves and modems.

To configure load balancing using multiple 3G/4G modems:

1. Assign a unique VLAN to each pair of SonicPoint/SonicWaves and 3G/4G modems, manually or by using the 3G/4G/LTE Wizard.
2. Add these VLAN interfaces to a load balancing group on the **Network > System > Failover & LB**. See the *SonicOS System Setup* administration documentation for more information.

Bluetooth LE Settings for Provisioning Profiles

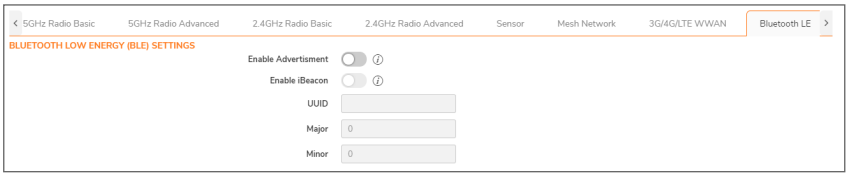
SonicWave series are equipped with Bluetooth Low Energy (BLE) functionality, which is a subset of classic Bluetooth. BLE enables smart phones, tablets, SonicWall mobile applications, and other devices, such as

other SonicWaves, to easily connect to the SonicWave access point, especially when in close proximity to an appliance with iBeacon enabled. BLE also provides location estimation.

iBeacon is a protocol developed by Apple. Various vendors make iBeacon-compatible BLE devices that broadcast their identifier to nearby portable electronic devices. The technology enables smart phones, tablets, and other devices to perform actions when in close proximity to an iBeacon.

To enable and configure Bluetooth Low Energy settings:

1. Navigate to **Device > Access Points > Settings** page.
2. Click **Access Point Provisioning Profiles**.
3. Click the **Edit** icon for SonicWave. The **Edit SonicWave Profile** dialog displays.
4. Click **Bluetooth LE**.



5. To enable BLE advertisement, select **Enable Advertisement**. This option is not selected by default. When this option is enabled, the **Enable iBeacon** option becomes available.

   ⓘ | **NOTE:** Enabling BLE advertisement might affect or interfere with the 2.4G radio frequencies.
6. To enable iBeacon so that BLE devices broadcast their identifiers, select **Enable iBeacon**. This option is not selected by default. The subordinate fields become available.
7. Complete the fields:

   - **UUID** – Enter the 36-characters of the UUID. For example: *51b9d455-6a32-426c-b5cc-524181c24df3*
   - **Major** – Enter the significant identity in the same geographical group. The range is 0 to 65535; the default is 0.
   - **Minor** – Enter the secondary identity in the same geographical group. The range is 0 – 65535; the default is 0.

   ⓘ | **TIP:** Use different UUIDs to distinguish different geographical groups and major and minor options to distinguish areas within the geographical group. For example, you deploy several SonicWave appliances with BLE in one building, and you set the same UUID for these SonicWave appliances. The SonicWave appliances on the same floor have the same Major number, but have different Minor numbers in different places on the same floor. In this way, your mobile device is close to a SonicWave appliance and its location.
8. Click **OK**.

Deleting 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 **Access Point Provisioning Profiles** section on the **Device > Access Points > Settings** page:

- Delete a single access point profile by:
  1. Hover on the access point profile and click **Delete**. A confirmation message appears.
  2. Click **OK**.
- Delete one or more access point profiles by:
  1. Select the checkbox next to the name(s) of the access points to be deleted.
  2. Click **Delete** icon . A confirmation message appears.
  3. Click OK.

Product Specific Configuration Notes

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

Managing Access Points

The SonicPoint / SonicWave Objects section displays the settings for connected access points, and provides icons to edit them or perform other actions.

The table displays the configured values for the access points, including:

Column	Description
#	Row reference number
Name	Name of access point
Interface	Firewall interface number and zone to which the access point is connected
Network Settings	Access point IP address, MAC address, and management designation
Status	Operational, Non-responsive, or other access point states
5GHz Radio	Access point SSID (MSSID) name for this radio, frequency and 802.11 protocols
5GHz Radio Channel	Band setting, channels, and state of radio such as enabled and active
2.4GHz Radio	Access point SSID (MSSID) name for this radio, frequency and 802.11 protocols
2.4GHz Radio Channel	Band setting, channels, and state of radio such as enabled and active
3G/4G/LTE	Enabled/disabled state of 3G, 4G, or LTE and binding information
Enable	Selected if the access point is enabled
SSH	Button for SSH access to the access point

Topics:

Deleting Access Point Objects

You can delete individual access points or groups of access points from the **Access Point Objects** section on the **Device > Access Points > Settings** page:

- Delete a single object by:
  1. Hover on the and click **Delete** icon. A confirmation message appears.
  2. Click **OK**.
- Delete one or more objects by:
  1. Select the checkbox next to the objects to be deleted.
  2. Click on **Delete** icon. A confirmation message appears.
  3. Click **OK**.

Rebooting Access Point Objects

You can reboot individual access points or groups of access points from the **Access Point Objects** section on the **Device > Access Points > Settings** page:

- Reboot a single object by:
  1. Check the checkbox next to the name of the access point to be rebooted.
  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**.

Modifying Access Point Objects

An access point object can be modified from the **Device > Access Points > Settings** page.

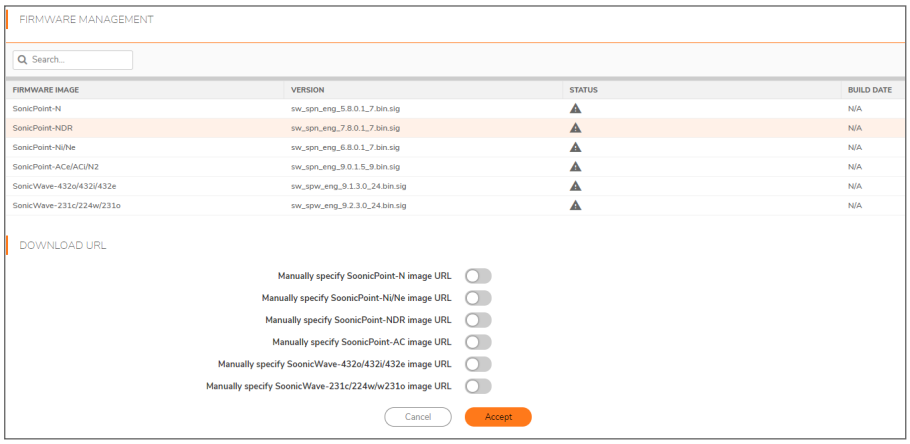
1. Hover on the object which you want to modify and click the Edit icon.
2. Changes the settings you want to modify.
3. Click **OK** to save the new settings.

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

2

Firmware Management

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



Topics:

- About Firmware Management
- Obtaining the Latest SonicWall Firmware
- Downloading Firmware from a Specific URL
- Uploading Firmware to an Access Point

About Firmware Management

The **Firmware Management** table displays the status of the current access point firmware images, and provides buttons to obtain new firmware and upload it to the access points.

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.

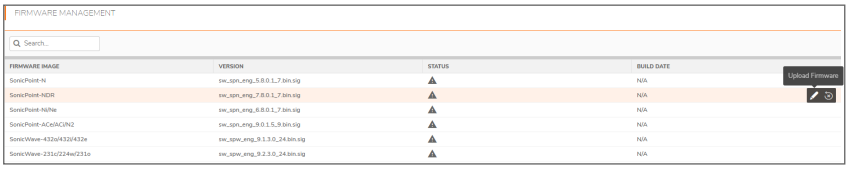
Status	Initially, all firmware status is *Need Download*. If a different firmware image is uploaded to the firewall buffer, it changes to a check mark indicating *Ready*.
Build Date	Displays the date that the uploaded firmware was created.
Action	Provides two icons: • **Upload Firmware** – Click to upload 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** – 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.

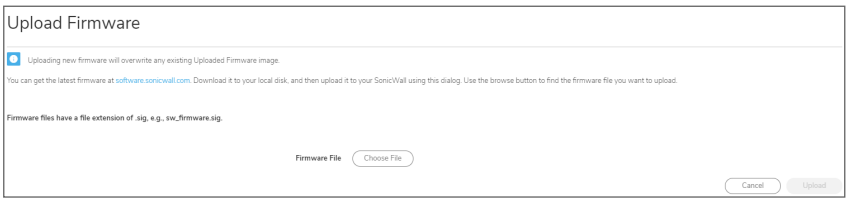
Obtaining the Latest SonicWall Firmware

To obtain the latest firmware version from SonicWall:

1. Navigate to **Device > Access Points > Firmware Management** page.
2. In the Firmware Management table, hover on the desired access point and click **Edit**(Upload Firmware) icon.



3. In the **Upload Firmware** dialog box, click the **software.sonicwall.com** link.



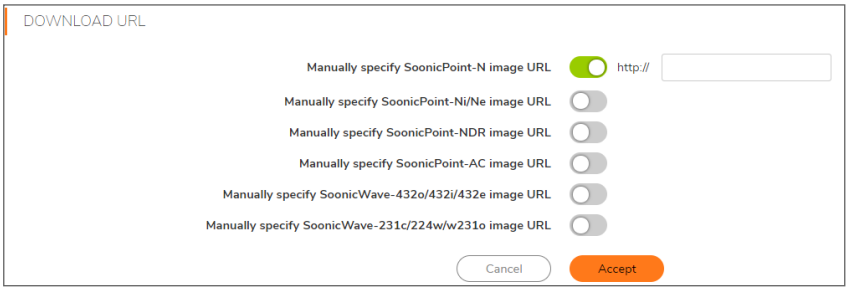
4. The file, for example *sw_firmware.sig*, is saved to your default location, such as your *Downloads* folder.

Downloading Firmware from a Specific URL

You can manually specify a URL location and download a firmware image from it for use on your access point.

To specify a URL for the image:

1. Navigate to **Device > Access Points > Firmware Management**.
2. Scroll to **Download URL** section.
3. Toggle the option for the type of image to be downloaded. A field becomes available.



4. Enter the URL of the image's location in the field.

5. Click **Accept**. The file is saved to the firewall buffer.

Uploading Firmware to an Access Point

You can upload any locally saved firmware image file to an access point. The saved file can be an official SonicWall firmware version, or a firmware image downloaded from a manually specified URL.

To upload a firmware image to an access point:

1. Do one of the following to obtain the firmware image and save it on your local workstation:
   - Download an official SonicWall version as described in Obtaining the Latest SonicWall Firmware.

     This procedure leaves you in the **Upload Firmware** dialog after saving the image file to your local computer.
   - Download a firmware image from a manually specified URL as described in Downloading Firmware from a Specific URL.
2. If you want to upload a firmware image, click Upload Firmware under Action in the row for the desired access point type to open the Upload Firmware dialog box. If you downloaded the image file using the link to software.sonicwall.com, the dialog is already open.
3. In the **Upload Firmware** dialog, click **Browse**, navigate to the saved image and select it. The **Upload Firmware** dialog now displays the firmware image name.
4. In the **Upload Firmware** dialog, click **Upload**.

The firmware image is uploaded to the buffer on your security appliance. While uploading, the *Status* indicates the percentage of the upload.

When the upload completes, the *Version* column displays the new firmware version. If the access point is connected, the firmware version is automatically pushed to it and the *Status* changes to a check mark, indicating that the firmware image is *Ready*, and the *Build Date* shows the date that the image was created. The access point is now running the new firmware.

5. To clear the downloaded firmware from the buffer, click **Reset Firmware**. The **Status** indicator and **Build Date** return to the default display.

3

Floor Plan View

On the **Device > Access Points > Floor Plan View** page, the SonicOS user interface allows a more visual approach to managing large numbers of SonicWave and SonicPoint devices. You can also track physical location and real-time status.

The Floor Plan View feature is an add-on to the existing wireless access point management suite in SonicOS. 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 FPMV 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 below shows a sample of a typical floor plan view.

Topics:

- Managing the Floor Plans
- Managing Access Points

Managing the Floor Plans

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

Navigate to **Device > Access Points > Floor Plan View** page and click (Floorplan List) icon in the upper left corner and select the floor plan which needs to be displayed.

Creating a Floor Plan

To create a floor plan:

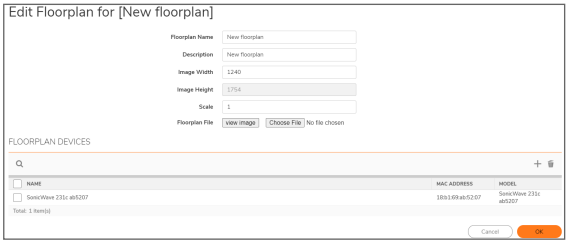
1. Navigate to **Device > Access Points > Floor Plan View** page.
2. Click on + icon. The **Add New Floor Plan** dialog is displayed.

3. Fill in the fields describing the plan.
4. Click **OK**.

Editing a Floor Plan

To edit a floor plan:

1. Navigate to **Device > Access Points > Floor Plan View** page.
2. Click on the **Edit** icon. The Edit Floor Plan dialog is displayed.



3. Change the fields as needed.
4. Click **OK**.

To edit a plan in the list:

1. Navigate to **Device > Access Points > Floor Plan View** page.
2. Click (Floorplan List) icon.
3. Select the check box of the Floor Plan which you want to edit and click **Edit** icon.The Edit Floor Plan dialog is displayed.
4. Change the fields as needed.
5. Click **OK**.

Set Measuring Scale

You need to set a measuring scale to show the relationship of real distance (feet) and the pixels that make up the picture of the floor plan. You can use this value to help estimate the RF coverage.

To set the measuring scale:

1. Navigate to **Device > Access Points > Floor Plan View** page.
2. Hover on the (Measure distance and areas) icon on the left bottom of the page and click create a new measurement option.
3. Start creating a measurement by adding points to the map and click **Finish measurement**.

Managing Access Points

Access Point status is displayed with color:

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

Topics:

- Available Devices
- Added Access Points
- Removing Access Points
- Export Image

Available Devices

The access points that are available for deployment are shown in the Devices Available list. The list typically appears in the upper right corner. You can close it by clicking on the X in the corner. To show the list, click **Access Points > Floor Plan View > Floor Plan Info**.

You can drag-and-drop these access points to the floor plan and place them where you want them. Be sure to SAVE PLAN when done.

ⓘ | **NOTE:** Access points that are already added to a floor plan do not show in this panel.

Added Access Points

The access points that have been deployed are shown in the Added Access Points list. The list typically appears in the upper left corner, but you can drag-and-drop it anywhere. You can close it by clicking on the X in the corner.

You can drag-and-drop these access points to different places on the floor plan, or you can delete them from the plan. Be sure to SAVE PLAN when done.

ⓘ | **NOTE:** Access points that are already added to a floor plan do not show in this panel.

Removing Access Points

To remove all access points:

1. Navigate to **Device >Access Points > Floor Plan View**.
2. Click on **More** option.
3. Select **Remove All Added Access Points of the Current FloorPlan**.

Export Image

To export the floor plan images:

1. Navigate to **Device > Access Points > Floor Plan View** page.
2. Click on **More** option.
3. Select **Export as Image** and choose the image format.
4. 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.

4

Station Status

The **Station Status** page reports on the statistics of each Access Point.

The table lists entries for each wireless client connected to each Access Point. The sections of the table are divided by Access Point. Under each Access Point displays the list of all clients currently connected to it.

Click the **Refresh** button in the top left corner to refresh the list.

5

Intrusion Detection Services

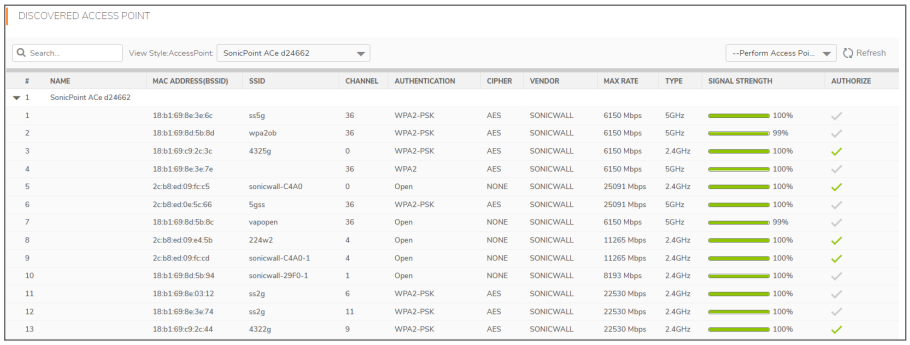
Rogue devices have emerged as one of the most serious and insidious threats to wireless security. In general terms, a device is considered rogue when it has not been authorized for use on the network. The convenience, afford-ability and availability of non-secure access points, and the ease with which they can be added to a network creates an 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 doesn't 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 **Device > 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 Point** Table and entities that are displayed on the **IDS** page.

Table Column or Entity	Description
Entity	
Refresh	Refreshes the screen to display the most current list of access points in your network.

Scan All	Initiates an operation to call all access points and identify connected devices.
View Style: Access Point	If you have more than one access point, you can select an individual access point from the **Access Point** drop-down menu or **All Access Points** if you want to see all of them.
Discovered Access Points Table	
Access Point	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.
Authentication	The authentication type.
Cipher	The cipher mode.
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:

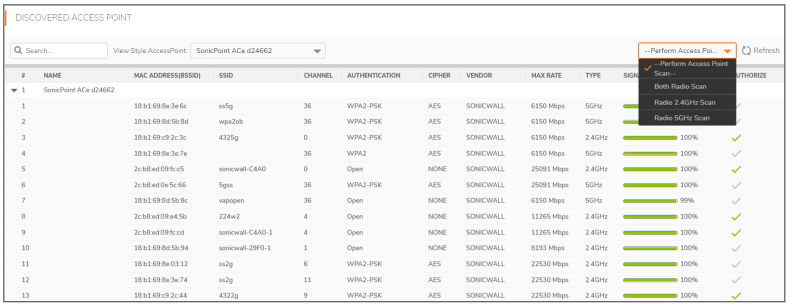
- Non-persistent, stateless protocols (such as HTTP) should not exhibit any ill-effects.
- Persistent connections (protocols such as FTP) are impaired or severed.
- WiFiSec connections should automatically re-establish and resume with no noticeable interruption to the client.

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 **Device > Access Points > IDS** page.
2. In the **View Style: Access Point** drop-down menu (at the top of the table), select **All Access Points** to scan all devices or choose a specific access point to scan only one device.

3. At the top of the table:
    - If you are scanning all access points, click **Scan All**.
    - If you are scanning only access point, select the access point from **View Style: Access Point** drop-down and choose one of the options in the drop-down menu for **--Perform Access Point Scan--** : **Both Radio Scan**, **Radio 2.4GHz scan** or **Radio 5GHz scan**.



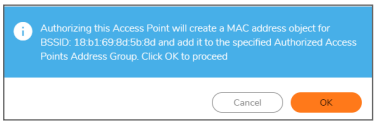
4. Confirm that you want to perform the scan.

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 **Device > Access Points > IDS**page.
2. Click the **Edit** icon in the **Authorize** column for the access point you want to authorize. A confirmation dialog is displayed.



3. Click **OK**.
4. Verify that authorization was successful by checking that the access point's MAC address was added. (Refer to the *SonicOS System Setup* for more information).

6

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.**

SonicOS Wireless Intrusion Detection and Prevention is based on SonicPoint and SonicWave access points cooperating with a SonicWall gateways. This feature turns your access points into dedicated WIDP sensors that detect unauthorized access points connected to a SonicWall network. This includes detection of KRACK Man-in-the-Middle access points.

△ **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 Points address object group.

Topics:

Enabling Wireless IDP on a Profile

You can enable wireless intrusion detection and prevention on an access point profile, including setting a schedule for scanning. For more information about access point profiles, refer to **Creating/Modifying Provisioning Profiles** of **Access Points > Settings** page.

To enable Wireless IDP scanning on an access point profile:

1. Navigate to **SonicPoint/SonicWave Provisioning Profiles** section of the **Device > Access Points > Settings** page.
2. Click the **Edit** icon for the appropriate profile.
3. Click **Sensor**.

   ⓘ **TIP:** The **Sensor** screen is the same for all SonicPoint or SonicWave 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

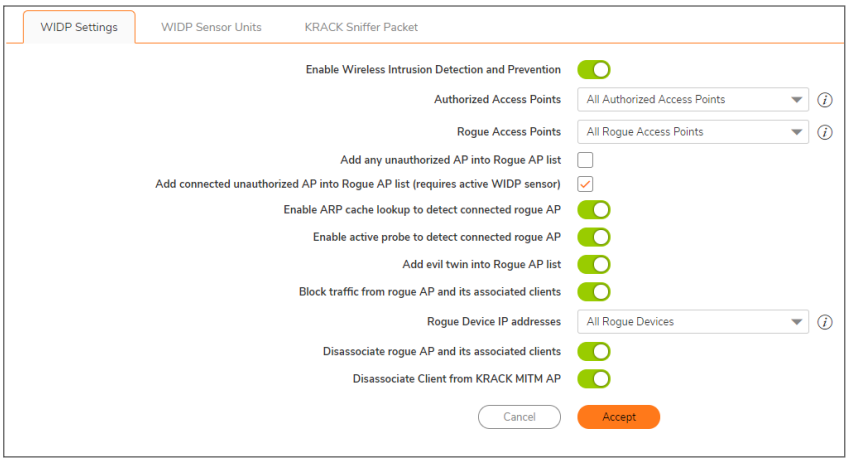
   CAUTION: When Advanced IDP scanning is enabled on a SonicPoint/SonicWave radio, its access point functions are disabled and any wireless clients are disconnected.

6. Click **OK**.

Configuring Wireless IDP Settings

To configure Wireless IDP settings:

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



2. Select **Enable Wireless Intrusion Detection and Prevention** to enable the appliance to search for rogue access points, including KRACK Man-in-the-Middle 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 **Device > 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've 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 **Accept** to save your changes.

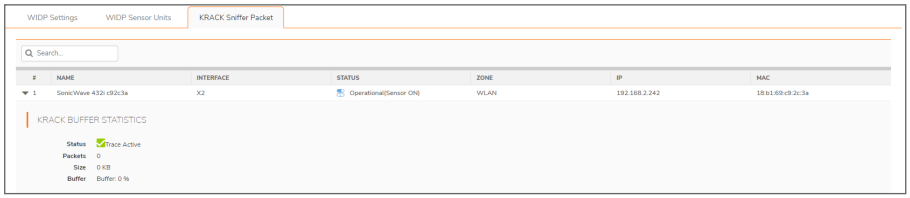
Viewing KRACK Sniffer Packets

When the **Enable Wireless Intrusion Detection and Prevention** option is enabled, the SonicWave periodically scans the wireless environment looking for a KRACK Man-in-the-Middle access point and any clients interacting with it. **KRACK** is the acronym for **Key Reinstallation Attack**.

The KRACK MITM attack clones the real access point on a different channel with the same MAC address as the real access point. When a KRACK MITM access point is detected, the SonicWave opens a monitoring interface on the same channel as the KRACK MITM, and sniffs the packets on the channel for a period of time. If a wireless client is associated with the MITM access point and the **Disassociate Client from KRACK MITM AP** option is enabled, the client is disassociated from the MITM access point. Log messages are reported in the **Monitor > Logs > System** Logs page when any of the following events occur:

- KRACK MITM access point is detected
- Client is detected communicating with the MITM access point
- Client is disassociated from the MITM access point

Because the sniffing is done during the KRACK detection process, the captured packets are saved in the buffer of the SonicWave. The below image shows the KRACK sniffer results from SonicWaves.



To analyze the KRACK process, click **Download**icon for a SonicWave to export the packet data to the file *krackSniffer_[SonicWave name].cap*, where *[SonicWave name]* is the name of the SonicWave. Then open the file and view it using Wireshark or another PCAP analyzer tool.

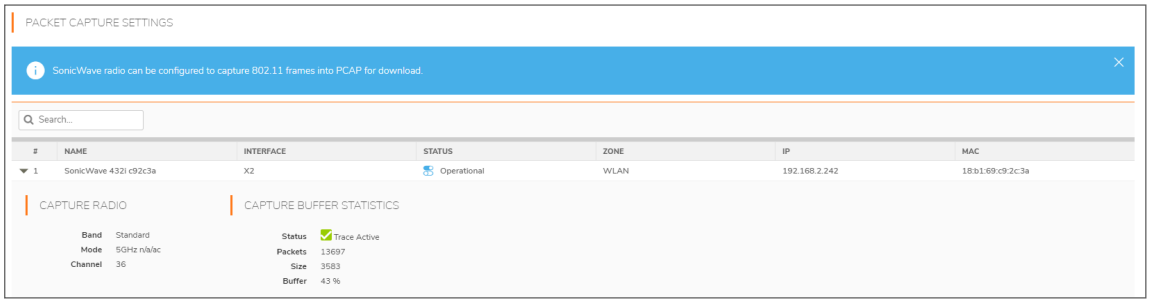
7

Packet Capture

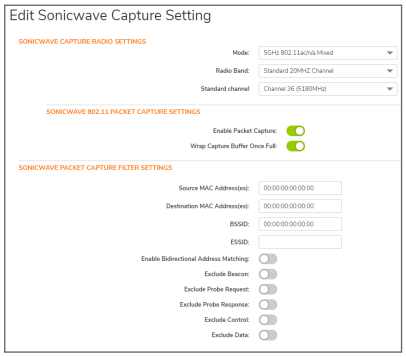
The **Device > Access Points > Packet Capture** feature provides an in-depth type of wireless troubleshooting that you can use to gather wireless data from a client site and output into a readable file. This feature is supported for SonicWave access points.

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 **Packet Capture** page shows the status of the SonicWave, the number of packets captured, and the size of the packet buffer. At the right, hover on the SonicWave 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** icon for the SonicWave you want to configure.



To capture the data for one of configured SonicWave radios, click Download for that row on the **Packet Capture** page. The capture file is named with the format, "*wirelessCapture_[SW name].cap,*" where *SW name* is the SonicWave name. Wireshark™ can be used to read the file.

8

Virtual Access Points

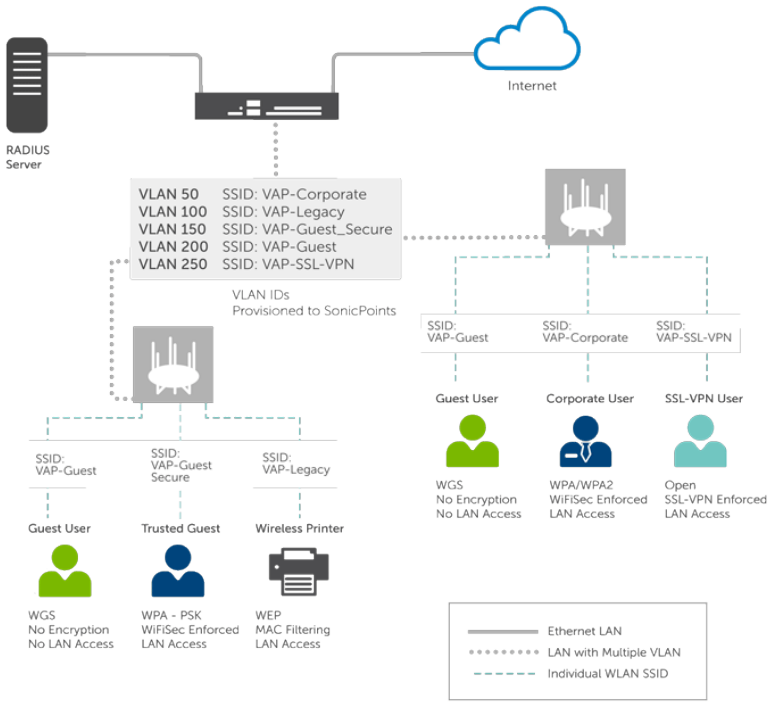
NOTE: Virtual access points are supported when using wireless access points along with SonicWall NSA appliances.

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.

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.

Topics:

- Before Configuring VAPs
- Access Point VAP Configuration Task List
- Virtual Access Point Profiles
- Virtual Access Points
- Virtual Access Point Groups

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

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 APs 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 the **Device > Access Points > Settings** page. Then click the **Edit** icon for the **SonicPoint/SonicWave Provisioning Profiles > General Settings: Enable** option to enable VAP.
- 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 below table 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:	
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 you do not care about because they are not even on your LAN.	Disable all SonicWall security services.
	Your Configurations:	

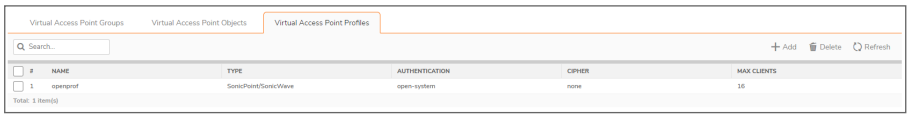
Access Point VAP Configuration Task List

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 **Object > Match Objects > Zones** in *SonicOS System Setup*.
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 > System > Interfaces** in *SonicOS System Setup*.
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 > System > DHCP Server** in *SonicOS System Setup*.
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 Point 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 **Device > Access Points > Settings** page.

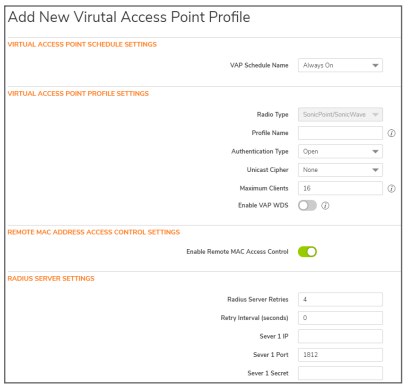
Virtual Access Point Profiles

A Virtual Access Point Profile allows you to pre-configure 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 **Device > 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** icon.

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



Topics:

- Virtual Access Point Schedule Settings
- Virtual Access Point Profile Settings
- ACL Enforcement
- Remote MAC Address Access Control Settings

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 **Device > Access Points > Virtual Access Point**.
2. Select **Add** if creating a new profile, or select a Virtual Access Point Profile and click on the **Edit** icon if editing an existing profile.
3. In the **VAP Schedule Name** field, select the schedule you want from the options in the drop-down menu.

Virtual Access Point Profile Settings

To set the Virtual Access Point Profile settings:

1. Navigate to the **Device > Access Points > Virtual Access Point**.
2. Select **Add** if creating a new profile, or select a Virtual Access Point Profile and click on the **Edit** icon if editing an existing profile.
3. 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 menu. 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 preshared key for authentication.
WPA2-EAP	Best security used with trusted corporate wireless clients. Transparent authentication with Windows login. Supports fast-roaming feature. Uses extensible authentication protocol.
WPA2-AUTO-PSK	Tries to connect using WPA2 security, if the client is not WPA2 capable, the connection defaults to WPA.Uses preshared 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 setting appear on the page depending upon which option 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.
- **Both** or **Shared**, refer to WEP Encryption Settings for information on the settings.
- an option requiring a preshared key (PSK), refer to WPA-PSK > WPA2-PSK Encryption Settings for information on the settings.
- an option using the extensible authentication protocol (EAP), refer to Radius Server and Radius Accounting for information on the settings.

ACL Enforcement

Each virtual access point can support an individual Access Control List (ACL) to provide more effective authentication control. The wireless ACL feature works in tandem with the wireless MAC Filter List currently available on SonicOS. Using the ACL Enforcement 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: • **Create new Mac Address Object Group...** • **All MAC Addresses** ⓘ **NOTE:** It is recommended that the **Allow List** be set to **All MAC Addresses**. • **Default SonicPoint/SonicWave ACL Allow Group** • 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**. • **Create new Mac Address Object Group...** • **No MAC Addresses**

	• **Default SonicPoint/SonicWave ACL Deny Group** ⓘ **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**.

Option	Description
Enable Remote MAC Access Control	Select the option 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

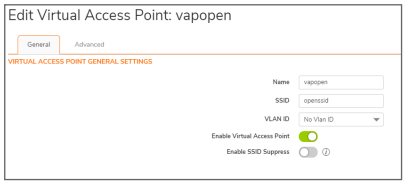
The VAP Settings feature allows for setup of general VAP settings. SSID and VLAN ID are configured through VAP Settings. virtual access points are configured from the **Device > Access Points > Virtual Access Point** page.

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

Topics:

- General Tab
- Advanced Tab

General Tab

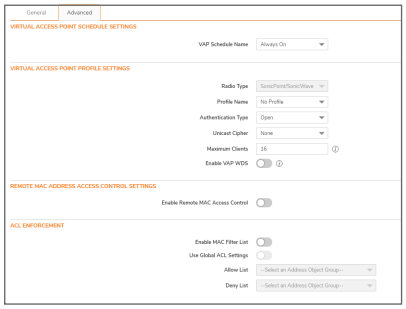


Set the following features on the General tab.

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 can 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.
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	Toggle this option to enable. Dynamic VLAN can only be enabled when the authentication type is set to EAP.

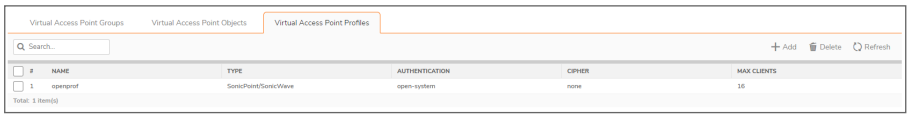
Advanced Tab



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 Point Profiles for complete authentication and encryption configuration information.

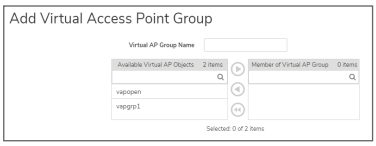
Virtual Access Point Groups

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 **Device > Access Points > Virtual Access Point** page.



To add a virtual access point group:

1. Navigate to the **Device > Access Points > Virtual Access Point** page.
2. Select **Add** if creating a new profile, or select a Virtual Access Point Profile and click on the **Edit** icon if editing an existing profile.



3. 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 **Right Arrow** to move it to the **Member of Virtual AP Group** list.
5. Select an object and use the **Left Arrow** to remove objects from the group.
6. Click **Accept** to save your settings.

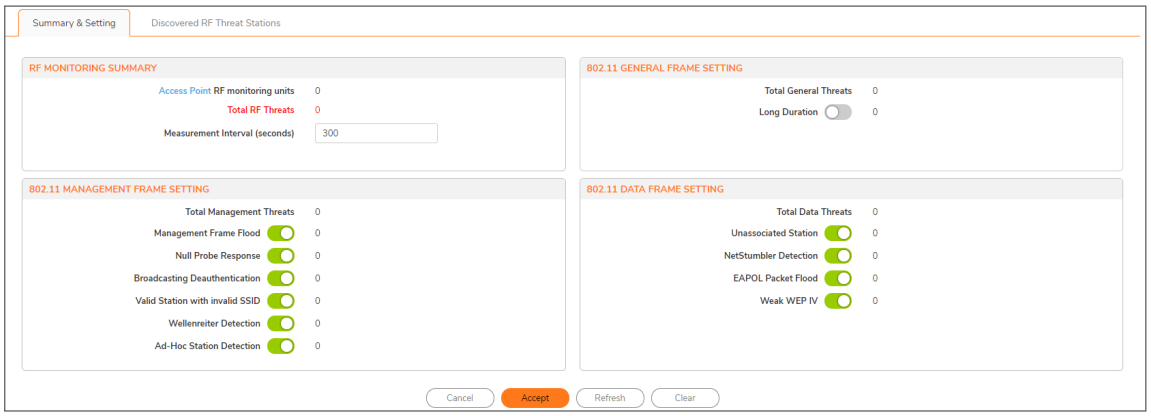
9

RF Monitoring

Radio Frequency (RF) technology used in today's 802.11-based wireless networking devices poses an attractive target for intruders. If left un-managed, 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.

SonicOS RF Monitoring provides real-time threat monitoring and management of SonicPoint radio frequency traffic. In addition to its real-time threat monitoring capabilities, SonicOS 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 **Device > 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.

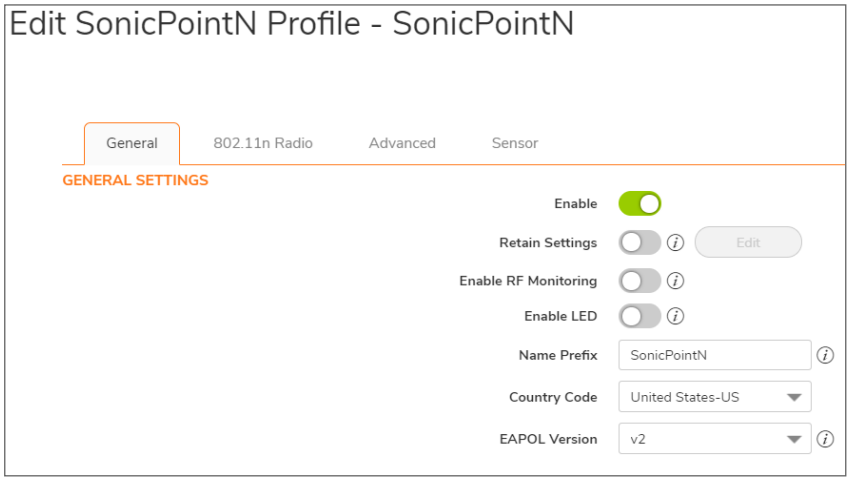


Topics:

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 **Device > Access Points > Settings** page.
2. Click the **Edit** icon on the profile you want to update (or S**elect SonicPoint/SonicWave Type** from the **Add New Profile** drop-down menu if creating a new profile).
3. Select the **Enable** option in the **General Settings** group.

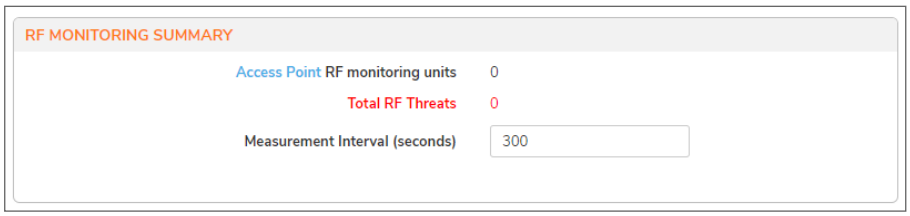


For more information on setting up profiles, refer to *Creating/Modifying Provisioning Profiles* in the *SonicOS Connectivity* administration documentation.

RF Monitoring Summary

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

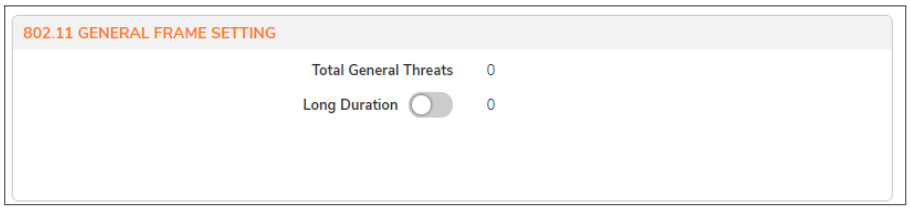
It also shows, in red, how many RF threats have been identified and the **Measurement Interval** setting. You can reset the Measurement Interval by typing a new number into the field. The default value is **300** seconds. Be sure to click **Accept** to save the settings.



By clicking on the **Access Point** link, you are navigated to the **Device > Access Points > Settings** page to edit profile or object settings.

802.11 General Frame Setting

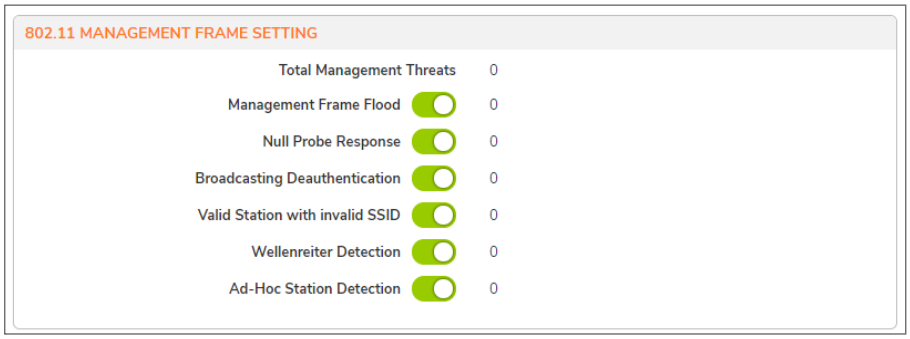
The **802.11 General Frame Setting** panel displays the total number of general threats and the option to enable long duration.



Selecting the **Long Duration** option and clicking **Accept** 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.

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.



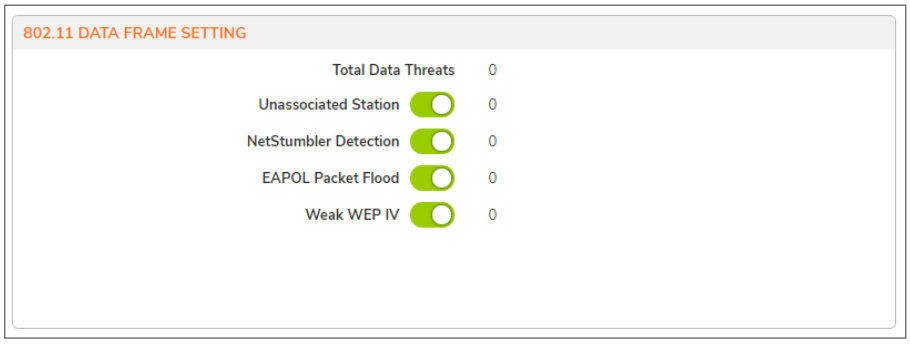
To enable any of the settings, toggle the radio button for that option. By default, all are enabled. Click **Accept** to save the settings. The below table describes the settings.

Name	Description
Total Management Threats	Displays the total number of management threats.
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.

Name	Description
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 may 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.

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.



To enable any of the settings, toggle the radio button for that option. Click **Accept** to save the settings. By default, **Unassociated Station** option is not enabled; the others are enabled. The below table describes the settings.

Name	Description
Total Data Threats	Displays the total number of data threats.

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.

Discovered RF Threat Stations

The **Discovered RF threat stations** tab displays information about discovered RF threat stations. It can either show all discovered threat stations or only those on the Watch List Group, depending on what you select from the **View Style: Station** drop-down menu.

The below table describes the data displayed in the Threat Stations table.

Name	Description
Items	Displays the total number of logged threats. Use the arrow buttons to navigate through pages if applicable.
View Style: Station	Selects the type of stations displayed in the list of entries: • **All Discovered Stations** • **Only Stations in Watch List Group**
#	Reference number for the entry.
MAC Address	Sorts the entries by MAC Address. This is the physical address of the RF threat station.
Type	Sorts the entries by the type of wireless signal received from the threat station.
Vendor	Sorts the entries by vendor. This is the manufacturer of the threat station (determined by MAC address).

Name	Description
RSSI	Sorts the entries by the received signal strength as reported by the SonicPoint. This entry, along with the **Sensor** entry, can be helpful in triangulating the actual physical position of the RF threat device.
Rate	Sorts the entries by transfer rate (Mbps) of the threat station.
Encrypt	Sorts the entries by wireless signal encryption on the threat station, **None**, or **Encrypted**.
RF Threat	Sorts the entries by RF threat (occurs in the latest time).
Update Time	Sorts the entries by the time this log record was created/updated.
Sensor	Sorts the entries by the ID of the SonicPoint which recorded this threat. This entry, along with the **RSSI** entry, can be helpful in triangulating the actual physical position of the RF threat device.
Comment	Displays a text box to add comments about the threat.
Configure	Configures a watch list for discovered stations.

TIP: It is possible to find approximate locations of RF Threat devices by using logged threat statistics. For more practical tips and information on using the RF Management threat statistics, see Practical RF Monitoring Field Applications.

Adding a Threat Station to the Watch List

The RF Monitoring Discovered Threat Stations Watch List feature allows you to create a watch list of threats to your wireless network. The Watch List is used to filter results in the **Discovered RF Threat Stations** list.

To add a station to the watch list:

1. Navigate to the **Device > Access Points > RF Monitoring** page and select **Discovered RF Threat Stations** tab.
2. Click the **Edit** icon that corresponds to the threat station you wish to add to the watch list. A confirmation dialog displays.
3. Click **OK** to add the station to the watch list.
4. If you have accidentally added a station to the watch list, or would otherwise like a station removed from the list, click the **Delete** icon that corresponds to the threat station you wish to remove.

   TIP: After you have added one or more stations to the watch list, you can filter results to see only these stations in the real-time log by choosing **Only Stations in Watch List Group** from the **View Style** drop-down menu.
5. Click **Accept**.

Practical RF Monitoring Field Applications

This section provides an overview of practical uses for collected RF Monitoring data in detecting WiFi 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 may have more than one hardware device at their disposal.

Topics:

Using Sensor ID to Determine RF Threat Location

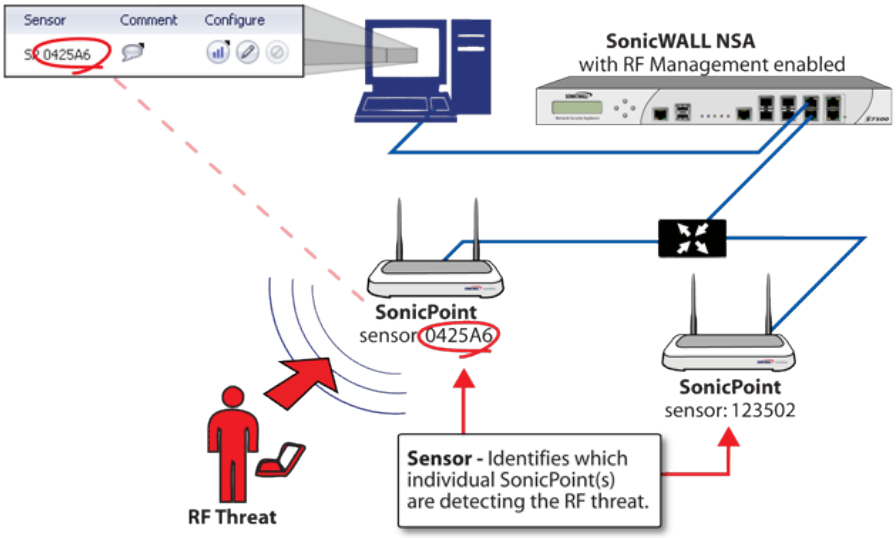
In the **Discovered RF Threat Stations** table, the Sensor field indicates which access point is detecting the particular threat. Using the sensor ID and MAC address of the access point allows you to easily determine the location of the access point that is detecting the threat.

ⓘ **TIP:** For this section in particular (and as a good habit in general), you may find it helpful to keep a record of the locations and MAC addresses of your access points.

1. Navigate to the **Device > Access Points > RF Monitoring** page.
2. In the **Discovered RF Threat Stations** table, locate the **Sensor** for the SonicPoint/SonicWave that is detecting the targeted RF threat and record the number.
3. Navigate to the **Device > Access Points > Settings** page.
4. In the **SonicPoint/SonicWave Objects** table, locate the access point that matches the Sensor number you recorded in *Step 2*.
5. Record the **MAC address** for this access point.
6. Use the MAC address to find the physical location of the access point.

   The RF threat is likely to be in the location that is served by this access point.

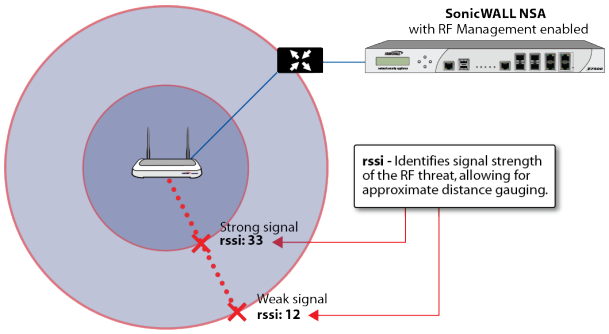
USING SENSOR ID TO DETERMINE RF THREAT LOCATION



Using RSSI to Determine RF Threat Proximity

This section builds on what was learned in the Using Sensor ID to Determine RF Threat Location. In the **Discovered RF Threat Stations** table, the **RSSI** field indicates the signal strength at which a particular access point is detecting an RF threat.

USING RSSI TO DETERMINE RF THREAT PROXIMITY



The **RSSI** field allows you to easily determine the proximity of an RF threat to the access point that is detecting that threat. A higher RSSI number generally means the threat is closer to the access point.

ⓘ **IMPORTANT:** Remember that walls serve as barriers for wireless signals. While a very weak RSSI signal may mean the RF threat is located very far from the access point, it may also indicate a threat located nearby, but outside the room or building.

1. Navigate to the **Device > Access Points > RF Monitoring** page.
2. In the **Discovered RF Threat Stations** table, locate the **Sensor** and **RSSI** for the access point that is detecting the targeted RF threat and record the number.
3. Navigate to the **Device > Access Points > Settings** page.

4. In the **SonicPoint/SonicWave Objects** table, locate the access point that matches the Sensor number you recorded in *Step 2*.
5. Record the **MAC address** for this SonicPoint/SonicWave.
6. Use the MAC address to find the physical location of the SonicPoint/SonicWave.

   A high RSSI usually indicates an RF threat that is closer to the SonicPoint/SonicWave. A low RSSI can indicate obstructions or a more distant RF threat.

10

RF Analysis

RF Analysis is a feature that helps you understand how wireless channels are utilized by the managed SonicWall access points and all other neighboring wireless access points. This section describes how to use the RF Analysis feature in SonicWall SonicOS to help best utilize the wireless bandwidth with wireless access point appliances.

NOTE: SonicWall RF Analysis can analyze third-party access points and include these statistics in the RF data as long as at least one SonicWall access point is present and managed through the SonicWall firewall.

Choosing RF Analysis

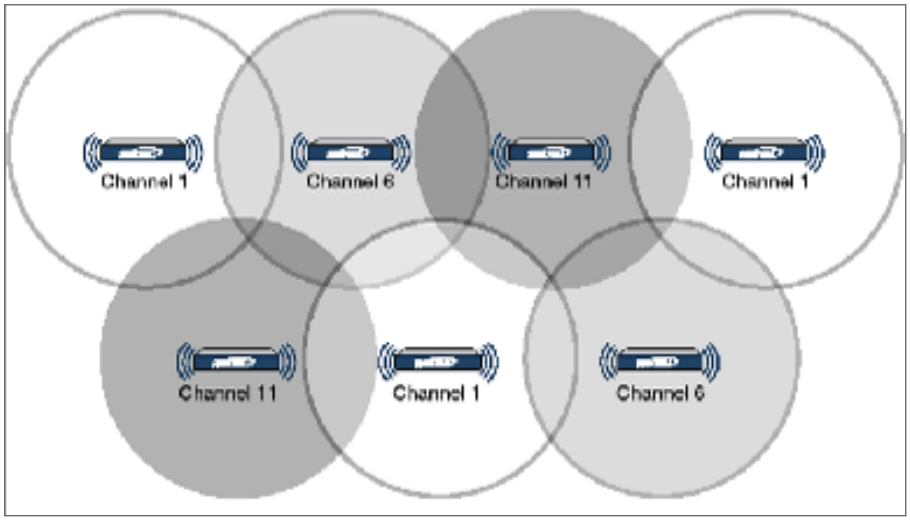
Deploying and maintaining wireless infrastructure can be a daunting task for the network administrator. Wireless issues, such as low performance and poor connectivity are issues that wireless network administrators often face, but ironically, these issues can usually be resolved simply analyzing and properly tuning radio settings.

RFA is a tool that brings awareness to these potential wireless issues. The two main issues that RFA deals with are overloaded channels and SonicWall access point interference with adjacent channels. RF Analysis calculates an RF score for each operational access point and displays the data in a way that allows you to identify access points operating in poor RF environment.

The RF Environment

The IEEE 802.11 specified that devices use ISM 2.4 GHz and 5 GHz bands, and most of the currently deployed wireless devices use the 2.4 GHz band. Because each channel occupies 20 MHz wide spectrum, only three channels out of the 11 available are not overlapping. In the United States, channels 1, 6, and 11 do not overlap. In most cases, these are the three channels used when deploying a large number of SonicWall access points.

SONICPOINT MANUAL CHANNEL SELECTION



The whole 2.4GHz band is segmented into three separate channels 1, 6, and 11. To achieve this ideal scenario, two factors are necessary: channel allocation and power adjustment. In most scenarios, it is best to assign neighboring SonicPoints to different channels. SonicPoint transmit power should also be watched carefully, as it needs to be strong enough for nearby clients to connect, but not so powerful that causes interference to other SonicPoints operating within the same channel.

Using RF Analysis on SonicWall Access Points

RF Analysis uses scores, graphs, and numbers to assist users to discover and identify potential or existing wireless problems.

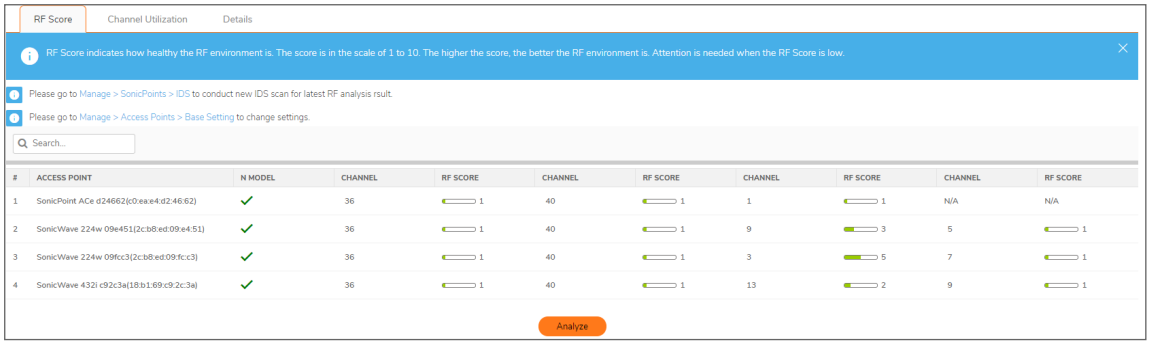
Although the best case scenario is to have the smallest number of access points working in the same channel at any given time, in the real world it is difficult to maintain that, especially when deploying many access points. Also, because the ISM band is free to the public, other devices outside of your control could be operating in that band.

Topics:

- Understanding the RF Score
- Channel Utilization Graphs and Information
- Viewing Overloaded Channels
- RFA Highly Interfered Channels

Understanding the RF Score

RF score is a calculated number on a scale of 1-10 that is used to represent the overall condition for a channel. The higher the score, the better the RF environment is. Low scores indicate that attention is needed.



SonicWall wireless drivers report signal strength in RSSI, this number is used in the preliminary RF score equation to get a raw score on a scale of 1 to 100:

*rfaScore100 = 100-((rssiTotal-50)*7/10))*

*Simplified: rfaScore100 = -0.7*rssiTotal + 135;*

The final score is based on this rfaScore100:

- If the RFA score is greater than 96, it is reported as 10.
- If the RFA score is less than 15, it is reported as 1.
- All other scores are divided by 10 to make them fall into the 1-10 scale.

In the SonicOS interface, the RF Score is displayed for the channel that is being used by the SonicWall access points.

NOTE: This feature depends on the knowledge of what channel SonicPoint is operating in. If the channel number is unknown, RF Score is going to be not available.

Channel Utilization Graphs and Information

Searching for a way to show how a channel is utilized for all connected SonicPoints resulted in channel utilization graphs:

Two color bars are displayed for each channel. The number on the top of each color bar indicates the number of SonicWall access points that detects the particular issue in that channel. SonicWall access points complete an IDS scan on all available channels upon boot-up, and RF Analysis analyzes these scan results to identify possible issues for each channel.

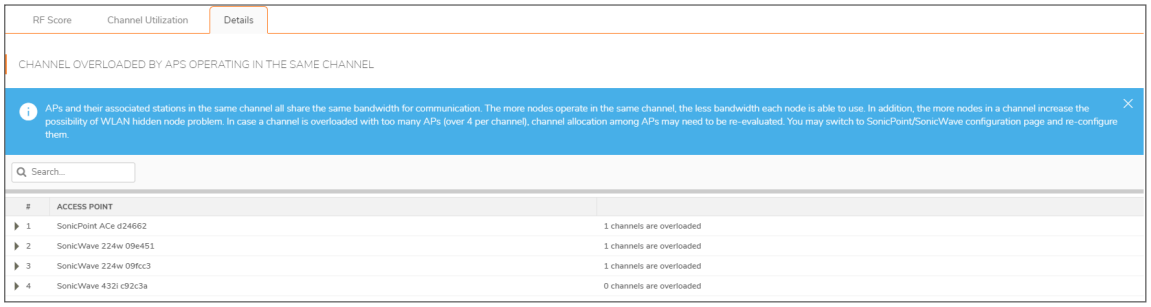
For example: If 10 SonicWall access points are connected, and 6 of these decide that channel 11 is overloaded, the number on the top of purple color bar is 6; if 8 SonicWall access points decide that channel 6 is highly interfered, the number on the top of the cyan color bar is 8. Zero is shown for channels no issues.

NOTE: Channels 12, 13, 14 are shown, but in some countries these channels are not used. These channels are still monitored, however, because it is possible for a wireless cracker to set up a wireless jammer in channel 12, 13, or 14 to launch a denial-of-service attack to lower channels.

Viewing Overloaded Channels

RF Analysis gives a warning when it detects more than four active access points in the same channel. No matter how strong its signal strength is, RF Analysis marks the channel as overloaded.

OVERLOADED CHANNELS



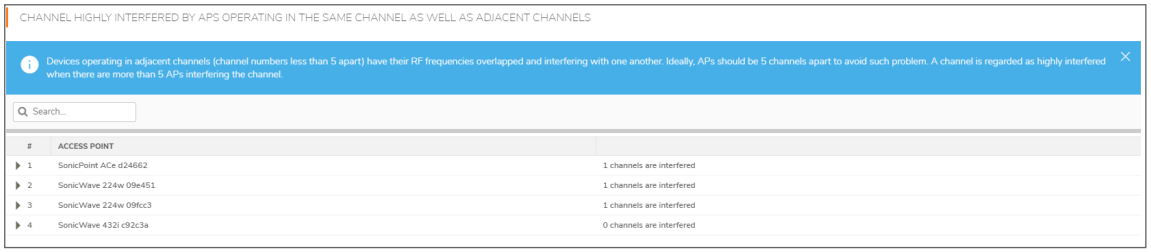
Information about each discovered access point includes: SSID, MAC, signal strength, and channel. Two values are shown for signal strength: dBm and percentage value.

RFA Highly Interfered Channels

Access points working in the same channel can create interference, as access points working in adjacent channels (channel number less than five apart) can also interfere with each other.

RFA delivers a warning when it detects that around a certain SonicPoint, there are more than five active APs in the channels that are less than five apart. No matter how strong their signal strength is, RFA marks the channel as highly interfered.

HIGHLY INTERFERED CHANNELS



Information about each discovered AP includes: SSID, MAC, signal strength, and channel. Two values are shown for signal strength: dBm and percentage value.

11

RF Spectrum

Widespread use of Wi-Fi devices, Bluetooth wireless technology, and security cameras has resulted in increased spectral interference that causes performance degradation. SonicOS provides:

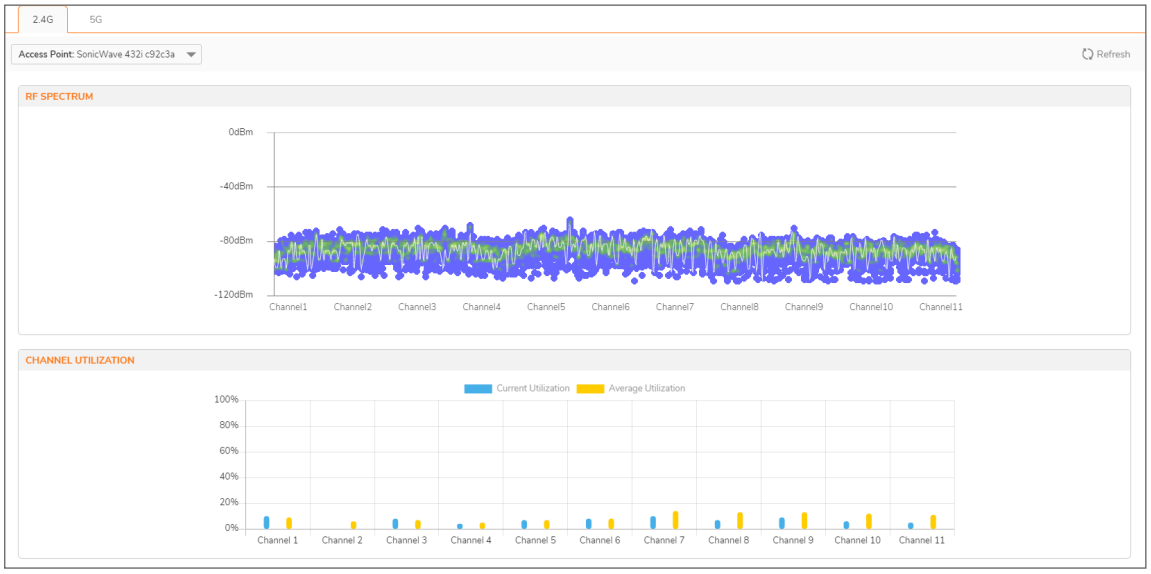
- Automated RF-channel interference detection.
- Power tools to troubleshoot at deeper layers of the RF environment and adjust radio settings accordingly.

To help you troubleshoot problems, navigate to the **Device > Access Points > RF Spectrum** page.

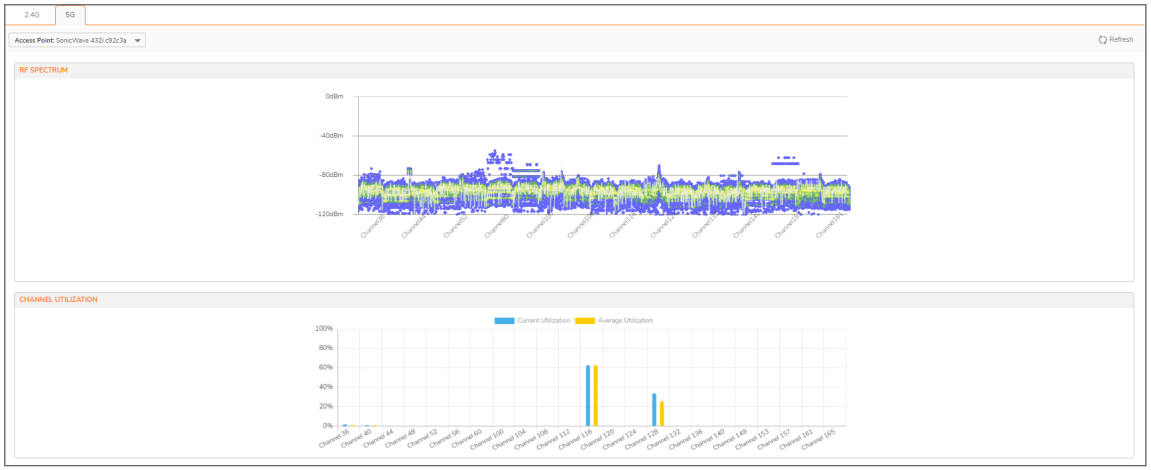
To monitor RF-channel interference:

1. Select the bandwidth you would like to monitor, 2.4G or 5G.
2. Select the access point you would to analyze for performance degradation or interference detection from the **Access Point** drop-down menu.

2.4G EXAMPLE



5G EXAMPLE

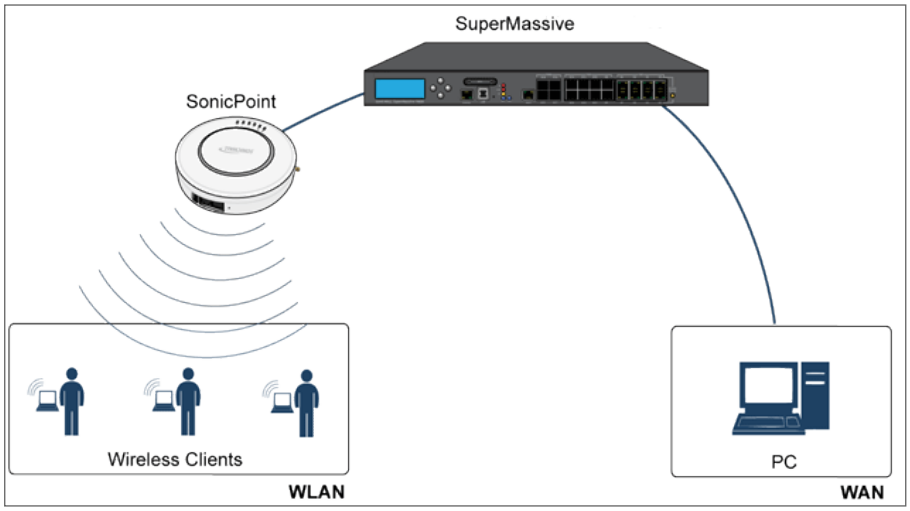

2.4G
5G
Refresh
RF SPECTRUM
0dBm
-40dBm
-80dBm
-120dBm
CHANNEL UTILIZATION
Current Utilization
Average Utilization
100%
80%
60%
40%
20%
0%

12

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:



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

Topics:

Supported Platforms

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

- SonicWall TZ Series
- SonicWall NSA Series
- SonicWall E-Class NSA 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 in 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.

Name	Description
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.
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.

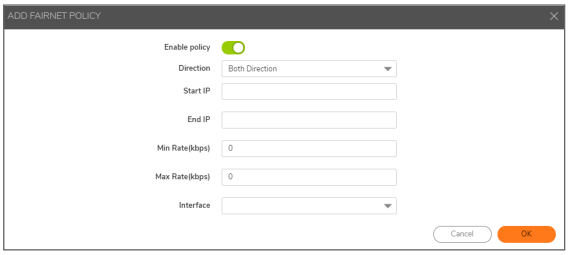
Name	Description
Enable	Enables the selected FairNet policy when the box is checked.
Configure	Edits existing FairNet policies when the **Edit** icon is clicked. Deletes the specific FairNet policy when the **Delete** icon is clicked.
Add	Adds a FairNet policy for an IP address or range of addresses. Displays the **Add Fairnet Policy** dialog.
Delete	Deletes the selected FairNet policies.
Accept	Applies the latest configuration settings.
Cancel	Cancels any changed configuration settings.

Configuring FairNet

This section contains an example FairNet configuration.

To configure FairNet to provide more bandwidth in both directions:

1. Navigate to the **Device > Access Points > FairNet** page.
2. Click **Add** icon. The **Add Fairnet Policy** dialog is displayed.



3. Toggle **Enable Policy** option. This is selected by default.
4. From the **Direction** drop-down menu, select **Both Direction** option. This applies the policy to clients uploading content and downloading content. This is selected by 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 **OK**. The FairNet Policy is added to the FairNet Policies table.
11. In the **FairNet Policies** table, enable the FairNet policy.
12. Click **Accept**.

13

Wi-Fi Multimedia

SonicOS 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.

SonicWall Wireless Cloud Management Support is also available for SonicWave access points. You no longer need to connect a SonicWave to your central firewall to manage it. You can deploy it standalone by connecting it to your network. The appliance provides wireless services that you can manage through the cloud on our new mobile application.

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 "backoff" periods for each Access Category. The WMM backoff 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 backoff periods. A range of time that specifies the random backoff 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 9 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

WMM Access Category (AC)	WMM AC Designation (informative)	CWMin	CWMax	AIFS
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 **Object > Services > Service Objects** page. Refer to *SonicOS Policies* for more information.

At least one access rule should be added on the **Policy > Rules and Policies > 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 **Adding Rule** window. In the **Traffic Shaping** tab of the **Adding 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 *SonicOS Policies* for more information.

Configuring Wi-Fi Multimedia Parameters

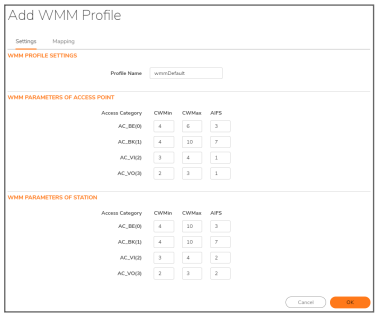
By default, a single WMM profile is configured on the SonicWall security appliance with the parameters set to the values on the 802.11e standard.

Topics:

Configuring WMM

To customize the WMM configuration:

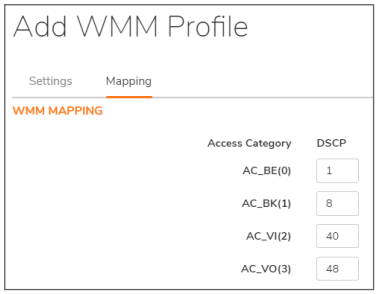
1. Navigate to the **Device > Access Points > Wi-Fi Multimedia** page.
2. To modify the a WMM profile, click the **Edit** icon for that profile. Or, to create a new WMM profile, click **Add** icon.



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 the Wi-Fi Multimedia Access Categories table.

> **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** tab 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 **Policy > Rules and Policies > Access Rules** > **Adding Rule** > **Traffic Shaping** tab.
7. Click **OK**.

Creating a WMM Profile for an Access Point

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

For more details, see Configuring WMM.

Deleting WMM Profiles

To delete a single WMM Profile, click the **Delete** icon in the profile's Configure column.

To delete multiple WMM Profiles, check the boxes next to the profiles to delete, and then click **Delete** icon on the top of the table.

14

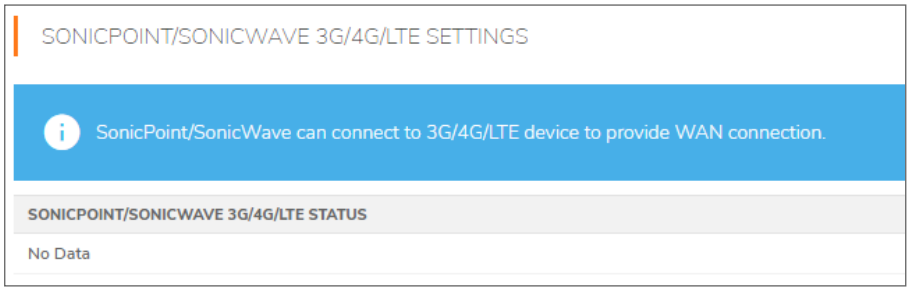
3G/4G/LTE WWAN

If you have a 3G/4G/LTE device connected to one of your access points, the **Device > Access Points > 3G/4G/LTE WWAN** page offers monitoring information on that device.

The first panel provides connectivity data and modem status, and the second panel shows a graphical representation of the device's signal strength.

Click **Refresh** to refresh the data in panels.

If no 3G/4G/LTE device is detected on one of your access points, you get the following message on the **Device > Access Points > 3G/4G/LTE WWAN** page:



15

Bluetooth LE Devices

SonicWave 432 and 200 series appliances now support Bluetooth Low Energy (BLE), a wireless personal area network technology that provides considerably reduced power consumption and cost while maintaining a similar communication range to standard Bluetooth appliances. Bluetooth Low Energy (BLE) is a subset of classic Bluetooth that enables smart phones, tablets, SonicWall mobile applications, and other devices, such as other SonicWaves, to easily connect to the SonicWave access point, especially when in close proximity to an iBeacon appliance. BLE also provides location estimation and an easier SonicWave configuration.

ⓘ **NOTE:** IBeacon is a protocol developed by Apple. Various vendors make iBeacon-compatible BLE devices that broadcast their identifier to nearby portable electronic devices. The technology enables smart phones, tablets, and other devices to perform actions when in close proximity to an iBeacon.

Viewing BLE Scanned Data

The **Device > Access Points > Bluetooth LE** page displays information about nearby Bluetooth Low Energy (BLE) devices. You can control the display by selecting a single SonicWave or **All Access Points** from the Access Point drop-down menu at the top of the page.

The table below displays information scanned from nearby BLE devices. The columns provide the following information, if available:

Column	Description
#	Reference number for the table row.
Access Point Name	Name of the access point (the SonicWave) scanning the BLE device.
Device Name	Name of the BLE device.
MAC Address	Unique hardware address of the device.
Vendor	Device manufacturer.
RSSI	Received signal strength indicator for the BLE device, expressed as a negative number (dB). Higher numbers (closer to zero) indicate stronger signals.
UUID	Proximity UUID, unique identifier of the BLE device. Exactly 36 hex characters and hyphens. Must not be set to all zeros.

Column	Description
Major	The significant identity within the group of BLE devices. Valid values are 0 - 65535. 0x0000 = unset.
Minor	The secondary identity within the group of BLE devices. Valid values are 0 - 65535. 0x0000 = unset.
Power	Power level of the BLE device in dBm. This is the measured power of the scanned devices, which is calculated by averaging multiple RSSI samples in a process corresponding to that defined by Apple.

16

Radio Resource Management

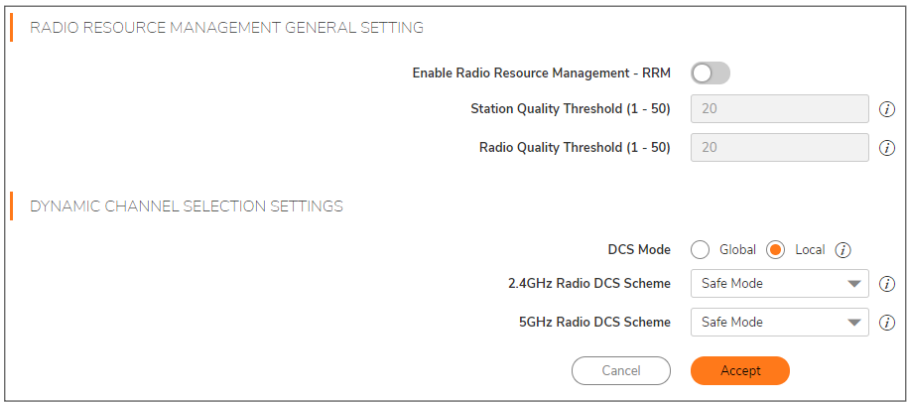
This section describes the settings available for Radio Resource Management and Dynamic Channel Selection in SonicOS.

NOTE: Radio Resource Management is supported on SonicWall access points that have a dedicated scan radio, including SonicWave 231c, 231o, 432e, 432i, and 432o. The RRM feature is not supported on SonicWave 224w or on SonicPoints.

Topics:

Configuring Radio Resource Management

Radio Resource Management settings are available on the **Device > Access Points > Radio Resource Management** page.



RADIO RESOURCE MANAGEMENT GENERAL SETTINGS

Option Name	Description
Enable Radio Resource Management - RRM	Enable this option to activate the settings for **Station Quality Threshold** and **Radio Quality Threshold**. This option is disabled by default.

Option Name	Description
Station Quality Threshold (1-50)	Health index to track and assess the status of wireless client connections, from 1 to 50. A higher index value means the wireless station is connected with higher data rate and less packet drop. Wireless clients will be disconnected if station quality drops below the configured threshold. • Minimum value = 1 • Maximum value = 50 • Default value = 20
Radio Quality Threshold (1-50)	Health index to track and assess the status of radio band utilization, which varies between 1 and 50. A higher index value means radio band utilization is lower with less packet drop. The radio transmit power will be lowered if the radio quality drops below the configured threshold. • Minimum value = 1 • Maximum value = 50 • Default value = 20

To configure Radio Resource Management settings:

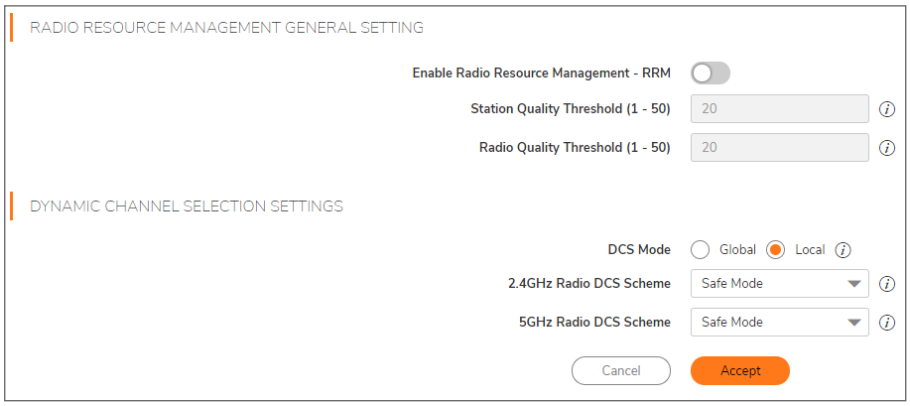
1. Navigate to the **Device > Access Points > Radio Resource Managemen**t page.
2. Select the **Enable Radio Resource Management - RRM** option to enable this feature.
3. For **Station Quality Threshold (1-50)**, enter a value between 1 and 50 or accept the default setting of 20.

   A higher index value means the wireless station is connected with higher data rate and less packet drop. Wireless clients will be disconnected if station quality drops below the configured threshold.
4. For **Radio Quality Threshold (1-50)**, enter a value between 1 and 50 or accept the default setting of 20.

   A higher index value means radio band utilization is lower with less packet drop. The radio transmit power will be lowered if the radio quality drops below the configured threshold.
5. Click **Accept**.

Configuring Dynamic Channel Selection

Dynamic Channel Selection settings are available on the **Device > Access Points > Radio Resource Management** page.



DYNAMIC CHANNEL SELECTION SETTINGS

Option Name	Description
DCS Mode	**DCS Mode** supports two settings for automatic channel selection: • **Global Mode** – Firewall assigns proper channel for all SonicWaves according to information received from all SonicWaves. • **Local Mode** – SonicWave finds the best channel according to the information from itself.
2.4GHz Radio DCS Scheme **5GHz Radio DCS Scheme**	2.4GHz or 5GHz Radio DCS Scheme options are: • **Safe Mode** – SonicWaves switch to a better channel only without clients connected. This is conservative mode. • **Steady Mode** – SonicWaves seek a better channel periodically in the background. This is moderate mode. • **Swift Mode** – SonicWaves switch to a better channel as soon as noise/interference becomes high on the current channel. This is aggressive mode. **Safe Mode** is the default.

To configure Dynamic Channel Selection settings:

1. Navigate to the **Device > Access Points > Radio Resource Management** page.
2. For **DCS Mode**, select either **Global** or **Local**.

   If **Global** is selected, the firewall assigns the proper channel for all SonicWaves according to information received from all SonicWaves. If **Local** is selected, each SonicWave finds the best channel according to the information from itself.

3. For **2.4GHz Radio DCS Scheme**, select one of the following:
    - **Safe Mode**

      SonicWaves switch to a better channel only without clients connected. This is conservative mode.
    - **Steady Mode**

      SonicWaves seek a better channel periodically in the background. This is moderate mode.
    - **Swift Mode**

      SonicWaves switch to a better channel as soon as noise/interference becomes high on the current channel. This is aggressive mode.
4. For **5GHz Radio DCS Scheme,**, select one of the following:
    - **Safe Mode**

      SonicWaves switch to a better channel only without clients connected. This is conservative mode.
    - **Steady Mode**

      SonicWaves seek a better channel periodically in the background. This is moderate mode.
    - **Swift Mode**

      SonicWaves switch to a better channel as soon as noise/interference becomes high on the current channel. This is aggressive mode.
5. Click **Accept**.

17

SonicWall Support

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

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

The Support Portal enables you to:

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

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

About This Document

NOTE: A NOTE icon indicates supporting information.

IMPORTANT: An IMPORTANT icon indicates supporting information.

TIP: A TIP icon indicates helpful information.

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

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

SonicOS Access Points Administration Guide
Updated - January 2021
Software Version - 7
232-005322-10 Rev B

End User Product Agreement

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

Open Source Code

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

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