SonicWave

Deployment Guide

SONICWALL®

Contents

1

Deployment Scenarios Overview

Welcome to the SonicWall SonicWave Deployment Guide. This guide provides a complete description of the hardware overview and configuration, software configuration, managing the SonicWave with a SonicOS and Wireless Network Manager (WNM)

SonicWall SonicWave 600 series Wireless Access Points (APs) are based on the Wi-Fi 6 (802.11ax) standard and offer excellent performance and security. SonicWave comes with industry-validated security features, including **Content Filtering**, **Application Control**, **Capture ATP**, **Geo-IP**, **Botnet**, and **Gateway Anti-virus** (Cloud). These secure APs can be managed via the cloud using SonicWall Wireless Network Manager (WNM) or SonicWall firewalls. They also provide additional features to improve user experience while delivering the top-notch performance and security.

The SonicWave APs are easy to set up and use. They work with the SonicWave WNM, which is an intuitive, scalable, and centralized Wi-Fi network management system. It provides detailed wireless and switching analytics and offers a simple on-boarding process through the cloud. The APs also work with WiFi Planner, a tool that helps you design and deploy a wireless network more efficiently, reducing the overall cost. With RF spectrum analysis, you can find and address sources of RF interference and monitor the health of the wireless system.

ⓘ **NOTE:** When we add new SSIDs to the AP Policies on the WNM portal, the firewall assigns a random virtual IP to the SSID, pointing to the Access Point's MAC address. This virtual IP redirects users to the SonicWave's Management Page. To prevent this, disable the **Proxy Client DNS Request On Bridge Mode** option under **WNM > SSID Profiles > Advanced > DNS**.

Before deploying access points (APs), it's important to conduct an RF survey analysis. In the WNM, you can access general information and configuration options related to the radio frequencies of the access points under the **Air Marshal > RF survey** feature. In SonicOS, on the **Device > Access Points > IDS** page, you can view reports on all devices detected by the firewall and its associated access points. These reports also provide the ability to authorize legitimate devices. Additionally, the reports include the dB value, which indicates the signal strength observed by our APs from their perspective.

ⓘ **NOTE:** Most SonicWave access points include a separate radio dedicated to security, which performs rogue AP detection, passive scanning and packet capturing. In WNM, due to hardware limitations, the separate scan radio only supports 802.11ac/n/a mode; hence, there is no 802.11ax/ac/n/a mixed mode on the **WNM > Air Marshal > Packet Capture** page.

SonicWave 600 Series Deployment Considerations

Site Survey

Make sure you understand your environment and the type of deployment you need before you set up your access points (APs). Be prepared for data traffic during peak hours on your wireless network. Before you deploy your wireless network, do a site survey to figure out how many access points you need and what type of coverage to expect from your APs.

Power Requirements

It is essential to check the power compliance of your AP before connecting it to your network. The maximum power from PoE (621/641 - 802.3at) (681– 802.3bt)

AP Mounting

Access points (APs) are designed for specific use cases and environments to ensure widespread coverage. For example, an indoor AP with an integrated antenna is meant to be mounted on the ceiling in indoor office environments. This is because APs with integrated omnidirectional antennas have a 360-degree radiation pattern. Additionally, barriers such as walls, concrete, and metal partitions can cause RF blockage.

The SonicWave 600 Series are ceiling-mountable wireless access point suitable for indoor single-unit or multi-unit deployments. It is plenum rated for installation within an enclosed space such as an attic. It can also be mounted on a wall or deployed on a shelf, table, or desktop. Power over Ethernet (PoE) should be provided to power the SonicWave 600 series.

Channel Width

In high-density environments, it's important to select narrower channel widths like 20 MHz and 40 MHz. Using wider 80MHz or 160 MHz channels reduces the number of non-overlapping channels, which can lead to interference. Wider channels are better suited for low-density, high-performance needs.

In shared spaces, wireless networks use channels to divide the RF medium. The number of channels is regulated and varies by country. For devices on the 5 GHz band (802.11a/n/ac), there are up to 23 separate channels. For devices using the 2.4 GHz range (802.11b/g/n), the wireless space is limited to a maximum of 13 overlapping channels, resulting in only three discrete channels.

Data Rates

Based on how your coverage is set up, it's best to switch off data rates below 24 Mbps. This will stop the access point and client from using slow data rates, which can cause bad performance and give users a poor experience.

SonicWave 600 Series Access Points use 802.11ax/Wi-Fi 6 technology to improve performance in complex environments. 1024 QAM allows more data to pass through, and 802.11ax enhances MU-MIMO with uplink and downlink capabilities.

Zero-Touch Deployment

You can easily register your unit and set up SonicWave APs using the SonicWall SonicExpress mobile application. The APs are detected and set up automatically with Zero-Touch Deployment. You can use the SonicExpress mobile application on iOS and Android to monitor and manage networks from anywhere.

SonicWave 600 Series Deployment Scenarios

The SonicWave Access Points (AP) are easy to set up and deploy. SonicWave works well with the deployment and setup processes, making them simpler and reducing the total cost of ownership. SonicWave APs can be managed bySonicWall next-gen firewalls. SonicWall firewalls come with a wireless controller that automatically detects and sets up SonicWave APs across the network.

The firewall or SonicWall Global Management System centrally handles the management and monitoring of wireless and security, giving network administrators a single interface to manage all aspects of the network.

SonicWave 600 series are Wi-Fi 6 access points that deliver wireless performance and security that are superior to the 802.11ac standard. The benefits using Wi-Fi 6 are:

- Wi-Fi 6 access points are more efficient than Wi-Fi 5 due to the multi-user support of OFDMA, which results in lower latency.
- Additionally, Wi-Fi 6 utilizes WPA3 for advanced security features, providing more robust authentication.
- BSS coloring is used to mark traffic on a shared frequency and reduce interference, ensuring more consistent service in complex environments. Target Wake Time (TWT) allows devices to improve battery life by determining when to wake to send or receive data.
- Wi-Fi 6's MU-MIMO supports multiple users within a single network environment, enabling simultaneous data upload and download for faster network speed.

2

Wireless Access Point Placement Considerations

Physical placement of the SonicWave wireless access point has a measurable effect on who can and cannot access your wireless signal.

Access points should be kept clear of Radio Frequency (RF) interference sources. RF barriers can be circumvented by deploying multiple access points.

A site survey can help find the optimum wireless access point placement, but you need it to find usable locations.

Considerations include:

- **Number of Access Points Versus User Density** – If too many users connect to a single access point, maximum transfer rates are reached, and that access point may become a bottleneck for the whole system.
- **Bandwidth** – How much data is moving upstream and downstream for a given type of user?
- **Ethernet Cabling** – Where are you running the powered Ethernet (PoE) cable, and how are you securing that cable? Are you using a multi-gigabit 802.3at-compliant PoE injector or switch to power all access points?

  To maintain power to the SonicWave access point, the recommended maximum length of CAT5e cable from the 802.3at PoE injector to the SonicWave access point is 100 meters (333 feet).
- **Hubs / Switches** – Your wireless deployment has to tie back into your network security application and LAN resources. Consider where your crucial networking devices are deployed and how they connect efficiently with your wireless application. What speed is needed for your Ethernet connection to accommodate the number of access points you are installed? A Gigabit Ethernet interface is recommended when connecting an SonicWave access point to your SonicWall network security application.
- **Legacy Clients** – Older laptops and mobile devices might not support 802.11ac. Although clients with 802.11a/g/b hardware are supported by the SonicWave, the presence of these legacy clients within a range of your wireless network could affect the connection speed of your 802.11ac clients.

  For example, an 802.11b device authenticated to the SonicWave access point could limit all clients connected to that radio to 802.11b data rates.

Radio Frequency Barriers

Determining how to circumvent RF barriers can be challenging in the placement process. Still, RF barriers can also be used beneficially to block signals where you do not want coverage. The 5 GHz frequency is more sensitive to RF barriers. A wall that allows a 2.4 GHz wireless network to operate can block a 5 GHz one.

COMMON RF BARRIER TYPES

Barrier Type	RF Signal Blocking
Open air	Very Low
Glass, wood, drywall, cube partitions	Low
Floors and outer walls, aquariums (brick/marble/granite/water)	Medium
Concrete, security glass, wire mesh, stacked books/paper	High
Metal partitions, desks, reinforced concrete	Very High

RF Interference

Bluetooth and Wi-Fi share the same 2.4GHz frequency, which can cause radio signals to interfere with one another. Radio frequency (RF) interference from home, office, and medical equipment is a common challenge in wireless deployments.

Remember that most cell/wireless phones and Bluetooth devices only utilize the 2.4 GHz frequency when considering RF interference sources. As such, they should not cause significant interference with wireless networks operating on the 5 GHz frequency.

COMMON SOURCES OF RF INTERFERENCE

Interference Source	Possible Range	Bands Affected
2.4 GHz phones	100 feet	2.4 GHz (802.11 b/g/n)
Bluetooth devices	30 feet	2.4 GHz (802.11 b/g/n)
Microwave oven	10-20 feet	2.4 and 5 GHz, depending on shielding
Scientific and medical equipment	Short distance, varies	2.4 and 5 GHz, depending on shielding

3

Software Configuration

Configuring SonicOS for Wireless Access

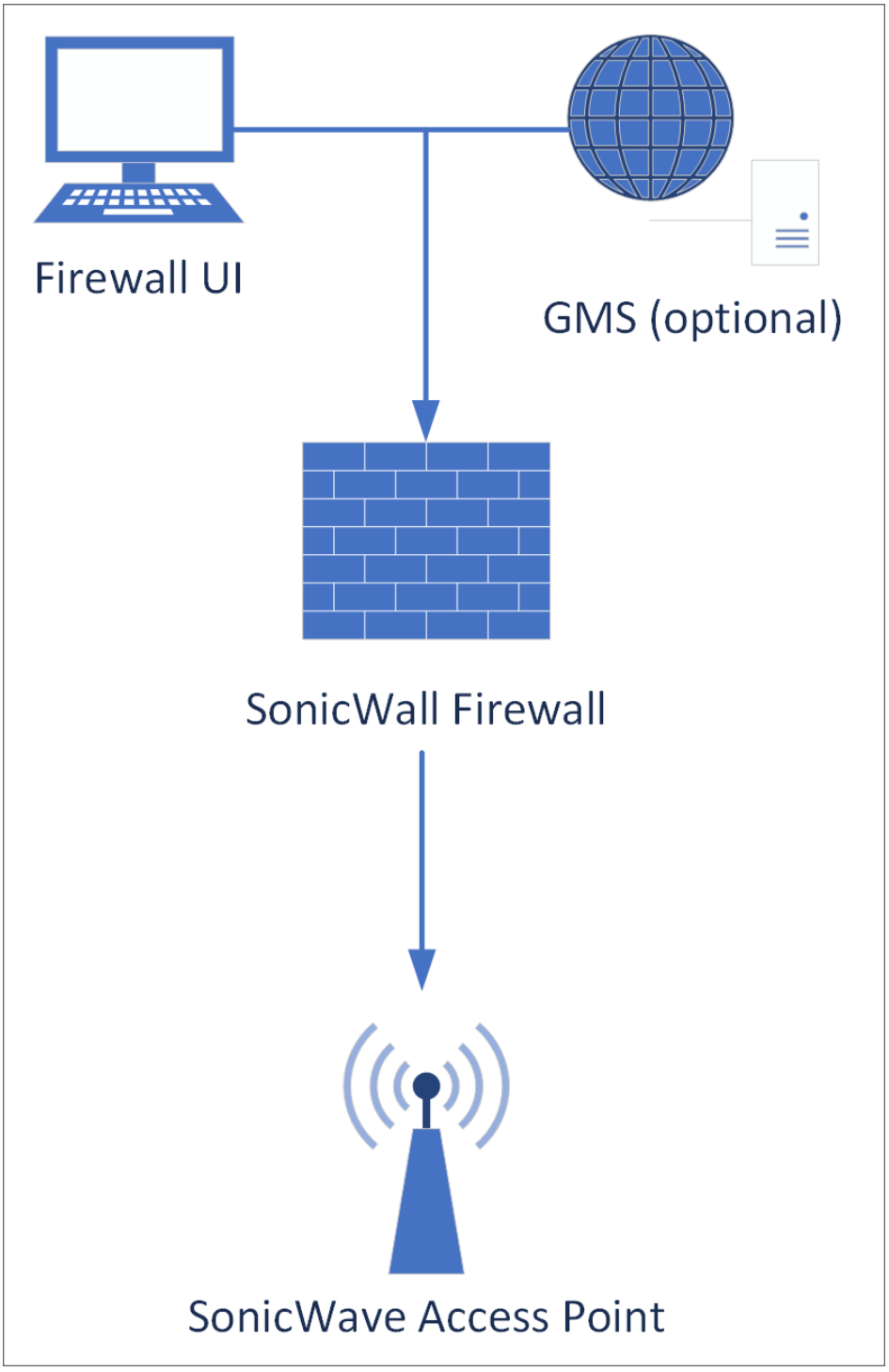
Introduction

There are two processes available for configuring SonicWave access points. The first, involves configuring the SonicWave access points from a SonicWave firewall interfacing There are two processes available for configuring. The second requires network administrators using SonicWall's WiFi Cloud Manager to deploy and manage the SonicWave access point. The following sections explore the relative advantages of these two approaches: firewall and cloud.

Firewall-based Configuration

The firewall-based approach is quick and potentially very simple. However, in a larger network environment, it could be clumsy. Changing the interface details of SonicWave access points connected to a firewall requires either using the **Console** port on the firewall or the SonicWave access point and might involve locational challenges. However, this could be necessary when you cannot establish an SSL/VPN link to the firewall. Although the firewall approach supports complex SonicWave configurations, when multiple access points in different locations are involved, the WiFi Cloud Manager option offers definite advantages.

FIREWALL-BASED CONFIGURATION

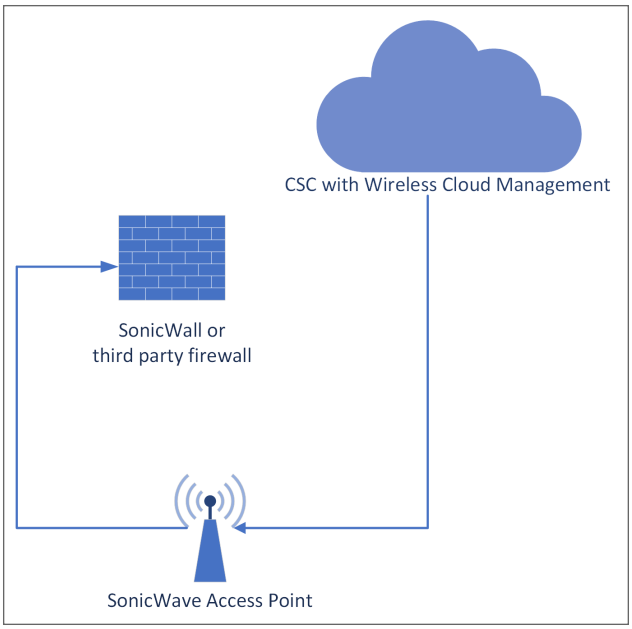


Cloud-based Configuration

WiFi Cloud Manager is offered within the Capture Security Center. With it, you can manage SonicWall access points globally regardless of their hardware environments.

Integration with other SonicWall Software provides references to manuals on WiFi Cloud Manager tools.

CLOUD-BASED CONFIGURATION



Wireless Cloud Management Overview

Wireless Cloud Management provides a simple WiFi deployment and management solution. The WiFi Cloud Manager, WiFi Planner, and WiFi Cloud Manager Mobile application are used to deploy, configure, and manage your wireless network.

Integration with other SonicWall Software provides references to the manuals of the Wireless Cloud Management tools.

- WiFi Cloud Manager
- WiFi Planner
- WiFi Cloud Manager Mobile application

WiFi Cloud Manager

WiFi Cloud Manager is an intuitive Wi-Fi network management system that simplifies Wi-Fi access, control, and troubleshooting. The Secure Wireless Cloud Management System can be deployed across multiple regions and is accessible from anywhere with an Internet connection.

You can access the WiFi Cloud Manager by clicking the **Wireless** tile from the Capture Security Center. The first time you access the WiFi Cloud Manager, you are asked to configure a wireless network hierarchy on the **Zones & Policies > Locations** page. Create your network hierarchy by adding Locations, Child Locations, and Zones under your Tenant. Additional tenants can be created from your MySonicWall (MSW) account.

After configuring the network hierarchy, you can use the wireless mobile application to add access points. Login to the application with your MSW credentials and select **Register APs** to open the QR code scanner. After scanning the QR code, the devices are registered and listed on MSW. You can change access point configurations from the **Devices** page.

WiFi Planner

The WiFi Planner is an intuitive, cloud-based, advanced wireless site survey and planning tool that enables you to assess and update your wireless network and make deployment configuration changes for an enhanced wireless user experience. The WiFi Planner is available in the WiFi Cloud Manager **Tools** menu. You can use the WiFi Planner tools to simulate a wireless deployment by creating or managing floor plans and placing/configuring/adjusting Access Points (APs).

To optimize access point placement before deployment, the WiFi planning tool provides you with comprehensive visualization of the WiFi environment, including any potential obstacles that could impact signal performance and displaying covered and non-covered zones.

WiFi Cloud Manager Mobile application

The WiFi Cloud Manager Mobile application is available for Android and iPhone devices. The mobile application SonicExpress provides a simple option for registering access points and creating a wireless mesh network. Login to the application with your MySonicWall credentials to register your access points. The mobile application allows you to scan the QR code on the back of the device or package to register the device. Registered devices application on the **MSW > Product Management > My Products** page.

Create a mesh network by selecting the **Setup Mesh** option, then follow the prompts. The application scans for devices and then asks you to connect a device to the Internet. Create or choose a profile, then enter a **Name** and **PSK** for the network. The application prompts you to only and review the network settings. Accept the settings and return to the menu. You can add access points by clicking **Add Aps** and scanning the QR code on the back of the device.

Integration with other SonicWall Software

SonicWall provides systems to help deploy, manage, and secure wireless networks:

- **Secure Mobile Access (SMA)**

  Operating on SonicWall hardware or as a virtual machine on a standard server, Secure Mobile Access provides policy-enforced SSL-VPN access and role-based privileges for mobile users.

  With the Mobile Connect application on mobile devices, mobile users can initiate a VPN connection with an SMA appliance and gain quick and appropriate access to the local network.

  For more information, go to the SonicWall technical documentation portal at: https://www.sonicwall.com/support/technical-documentation/. In the select a product box, choose **Secure Mobile Access** and then **100 series** or **1000 series**. A list of available manuals appears.

- **WiFi Cloud Manager (WCM)**

  This is a cloud-based component of SonicWall's Capture Security Center.

  WCM handles only the management plane functions of the SonicWave APs, ensuring that control and data plane functions are handled locally. Therefore, in case of an Internet outage, although there is a temporary loss in management capability, the APs continue to work. WCM can manage thousands of access points and enforce security policies at a granular level.

  Refer to details in Cloud-based Configuration for using WiFi Cloud Manager to deploy SonicWave access points.

  For more information, go to the SonicWall technical documentation portal at: https://www.sonicwall.com/support/technical-documentation/. In the select a product box, choose Secure Wireless Products. A list of available manuals appears.

- **WiFi Planner**

  A component of WiFi Cloud Manager, this planner helps make sound WiFi coverage decisions that account for different types of office spaces, floorplans, building materials, power requirements, signal strengths, channel widths and radio bands, to obtain maximum coverage with the fewest number of APs. It is ideal for new AP deployments or to ensure excellent coverage in existing wireless networks. Auto-channel assignment prevents interference in deployments on a best effort basis.

  For more information, go to the SonicWall technical documentation portal at: https://www.sonicwall.com/support/technical-documentation/. In the select a product box, choose Secure Wireless Products. The WiFi Planner User Manual will be among the listed publications.

- **SonicWall WiFi Mobile application**

  The SonicExpress (Android of iOS) mobile application provides a simple zero-touch option for registering access points as well as creating a wireless mesh network.

  Refer to details in Cloud-based Configuration for using WiFi Cloud Manager to deploy SonicWave access points.

  For more information, go to the SonicWall technical documentation portal at: https://www.sonicwall.com/support/technical-documentation/. In the select a product box, choose Secure Wireless Products. In the model box select .

4

Managing the SonicWave with a Firewall

This section provides instructions for configuring SonicOS on your SonicWall network security application to connect your SonicWave 600 series to the WLAN zone and manage it as a Layer 2 device.

ⓘ **NOTE:** For example, SonicWave 641 is connected to X14 port WLAN interface of SonicWall SonicOSNSa 2700. The access point has been configured with system default settings.

Topics:

Configuring the SonicWave Provisioning Profile

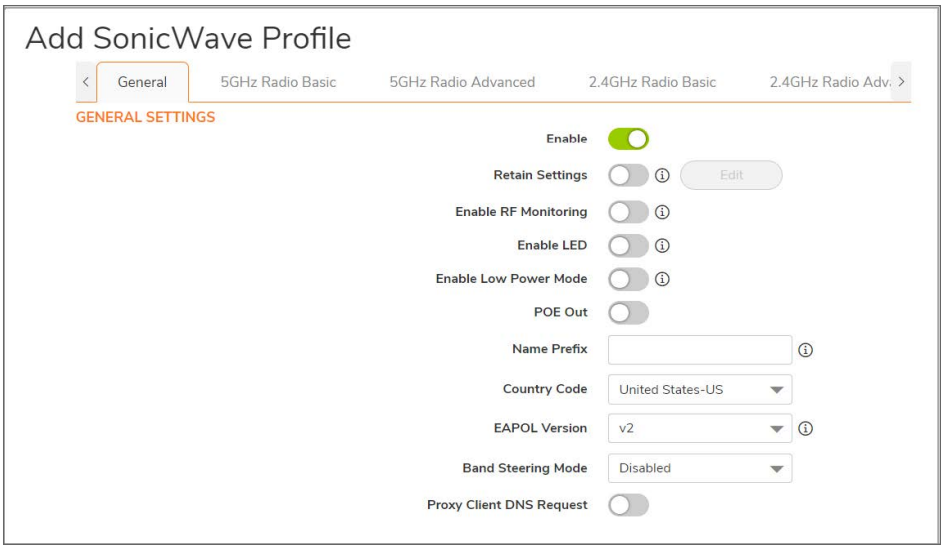
SonicWave provisioning profiles include all of the settings that can be configured on a SonicWave 600 (here 641) access point. The profile is then selected when you configure the wireless zone (WLAN by default). When your SonicWave 641 connects to that zone, it is automatically provisioned with the profile settings.

To configure the SonicWave provisioning profile:

Perquisites:

- Ensure you have performed the RF site survey and planning before SonicWave deployment.
- Ensure the two appliances have been registered in MySonicWall.

1. Log into your SonicWall firewall as an administrator (default: admin / password).
2. In SonicOS navigate to **Device > Access Points > Settings > Access Point Objects**. Initially no AP is listed .
3. To create a new profile, select **SonicWave Profile** from the **Add New Profile** drop down list.
4. In the **General** tab, the **Enable** option is activated by default.



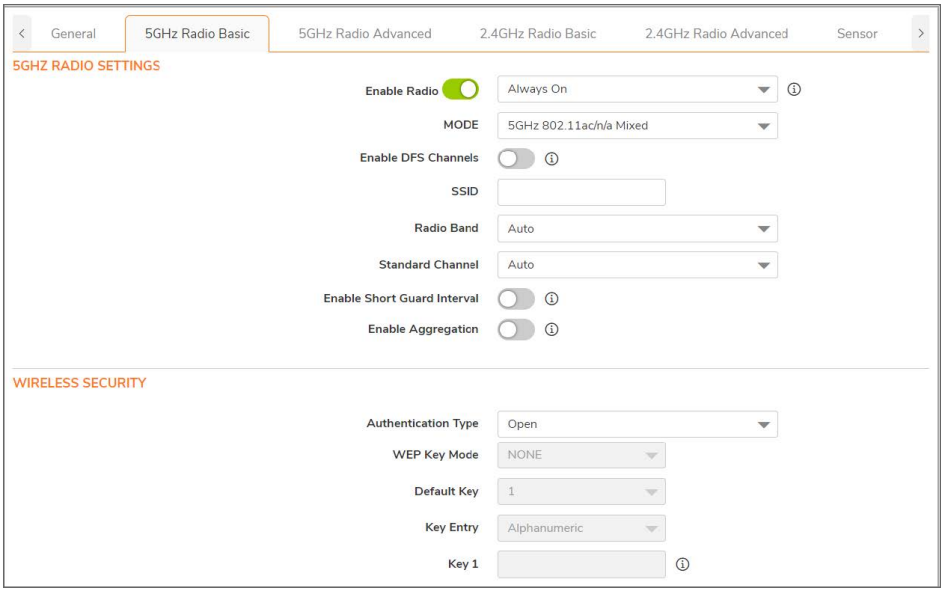
a. If adding a new profile, type a simple, descriptive name into the **Name Prefix** field to assist in identifying the SonicWave in this zone. This is the name of the provisioning profile. Each provisioned SonicWave is named with this prefix followed by a unique number. Optionally change the Name Prefix if editing the default SonicWave profile.

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

c. EAPOL Version v2 will provide better security however if we see unexpected replay counter then we can us EAPOL v1 which can be addressed by using v1.

d. Accept the defaults or configure the remaining options as necessary.

5. In the **5GHz Radio Basic** tab, select Enable Radio. This is selected by default.



a. Select a **MODE** or use the default.

b. It is advised to keep the **Enable DFS Channels** disabled.

ⓘ | NOTE:

- Dynamic Frequency Selection (DFS) is a way for wireless local area networks (WLANs) to use the 5 GHz frequency band without causing problems for radar systems. It automatically picks a frequency that won't interfere with specific radar systems. When operating in the 5 GHz band, unlicensed devices can use DFS to find out if there are radar systems on the channel they want to use. If the radar level is too high, the device moves to a different channel to avoid causing trouble for the radar systems.
- In a 5 GHz environment, not all channels within the 5 GHz band may be usable due to interference. If you are near an airport, certain 5 GHz channels may be unavailable. It is necessary to have the feature turned on that allows your APs to listen for radar or first responders using those shared frequencies. Make sure not to use those channels if they are being used.

c. Type a short, descriptive name into the **SSID** field. This is the access point name that appears in clients' lists of available wireless connections.

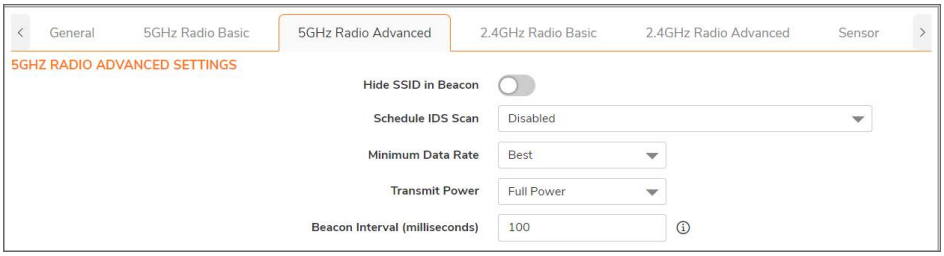
d. Under **Wireless Security**, select the **Authentication Type** for your wireless network. SonicWall recommends using **WPA2** as the authentication type if all client devices support it.

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

e. Select the **Cipher Type**. When using WPA and WPA2, SonicWall recommends **AES** for maximum security if all client devices support it.

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

6. Click **2.4GHz Radio Basic** and repeat the steps.
7. Click the **5GHz Radio Advanced** tab.



a. For most advanced options, the default settings give optimum performance.

b. Optionally select the **Hide SSID in Beacon** check box.

The SSID refers to the access point name that appears in clients' lists of available wireless connections. Hiding the SSID provides additional security because it requires the user to know the access point name before connecting.

8. Click the **2.4GHz Radio Advanced** tab and repeat the steps.
9. When finished configuring all options, click **OK**.

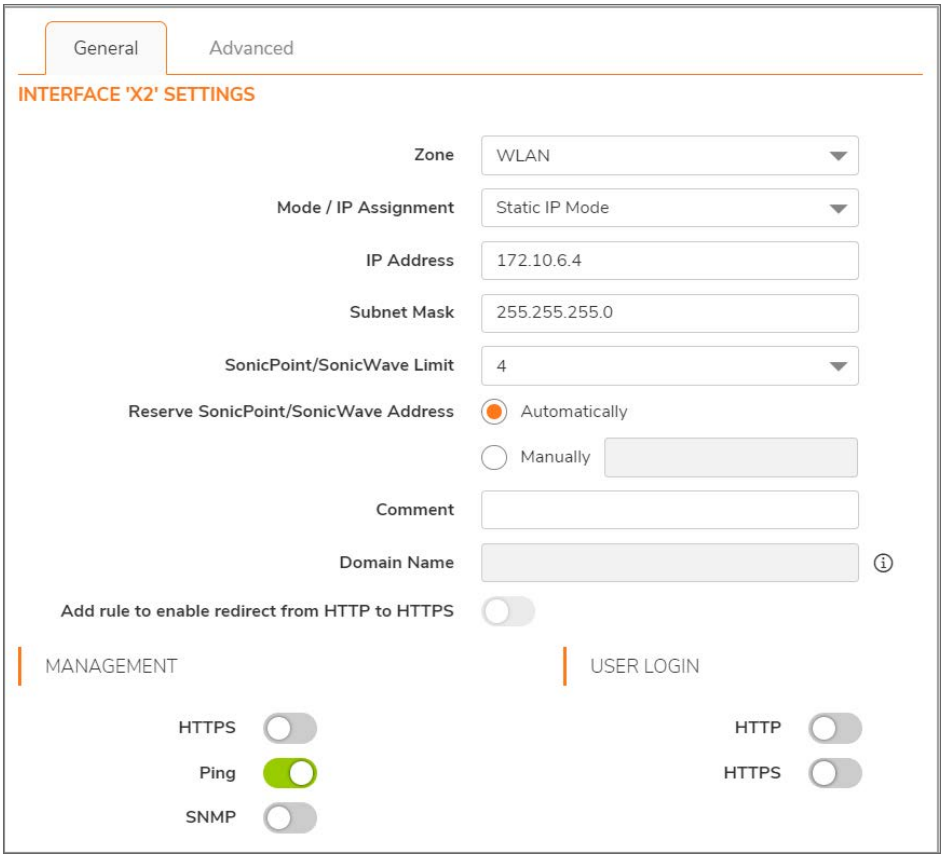
10. For information about configuring the other options and screens in the **Add/Edit SonicWave Profile** dialog, see the SonicOS Administration documentation.

Configuring the Network Interface

Each SonicWave or group of SonicWaves must be connected to a physical network interface that is configured in a wireless zone. SonicOS provides a standard wireless zone (WLAN) that can be applied to any available interface.

To configure the network interface in SonicOS:

1. Navigate to the **NETWORK** > **System** > **Interfaces** and click the **Edit** this interface icon by hovering over the interface to which your SonicWave connects.



2. Select **WLAN** or another (custom) wireless zone from the **Zone** drop-down menu. The default wireless zone is **WLAN**.
3. Select **Static IP Mode** for the **Mode/IP Assignment**.
4. In the **IP Address** field, type in any private IP address that does not interfere with the IP address range of any other interfaces on the appliance. Wireless clients are assigned an IP address in this subnet.

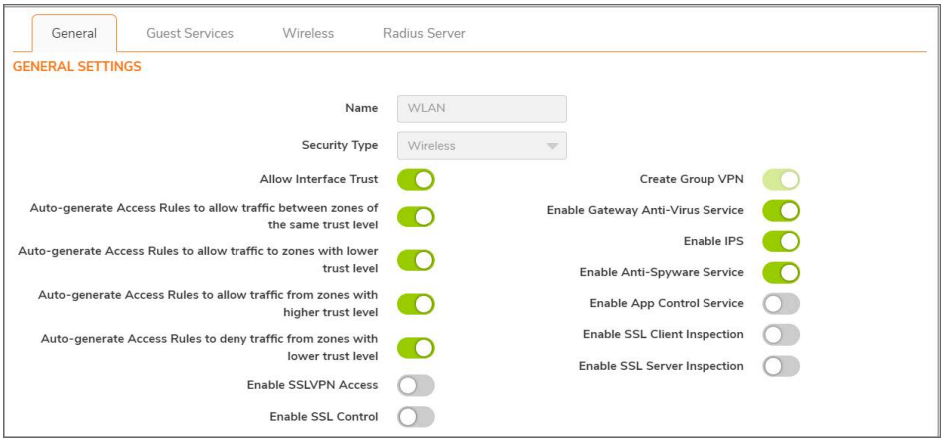
5. Enter a **Subnet Mask**. The default is 255.255.255.0.
6. Select a non-zero number for **SonicPoint/SonicWave Limit**. If 0 is selected, no access points can be discovered on this interface.
7. Use the default settings or select appropriate settings for the other fields and click **OK**.

Configuring the WLAN Zone

To configure the WLAN zone in SonicOS:

1. Navigate to **OBJECT > Match Objects > Zones**, click the **Edit** icon in the WLAN row.
2. On the **General** screen, select the **Allow Interface Trust** option to automate the creation of Access Rules to allow traffic to flow between the interfaces within the zone, regardless of the interfaces to which the zone is applied.

   For example, if the WLAN zone has both the X2 and X3 interfaces assigned to it, selecting **Allow Interface Trust** creates the necessary access rules to allow hosts on these interfaces to communicate with each other.



3. Select the check boxes to enable security services on this zone. Minimally, you would select **Enable Gateway Anti-Virus Service**, **Enable IPS**, and **Enable Anti-Spyware Service**. If your wireless clients are all running SonicWall Client Anti-Virus, select **Enable Client AV Enforcement Service**.
4. In the **Guest Services** screen, optionally configure guest Internet access. For information about Guest Services, see the SonicOS Objects Administration Guide.
5. In the **Wireless** screen under **SonicPoint/SonicWave Settings**, select the desired provisioning profile from the **SonicWave Provisioning Profile** drop-down menu. If you added a new profile in Configuring the SonicWave Provisioning Profile, select it here.

   ⓘ | **NOTE:**

   - The **Only allow traffic generated by a Sonicpoint/Sonicwave** option must be disabled to allow the sonic wave traffic to pass through the switch.

- Select **Prefer SonicPoint/SonicWave 2.4Hz Auto Channel Selection to be 1, 6 and 11** only if the preferred auto channel selection is 1, 6, or 11. In the event of environmental interference or co-channel interference, it is advisable to disable this option. Failure to do so may result in the access point switching between these three channels, potentially leading to client disconnection.

5

Deploying a SonicWave with Wireless Network Manager

This section describes registering and deploying a 600 Series SonicWave using SonicWall's Wireless Network Manager. You can leverage both Single-Pane-of-Glass (SPOG) visualization and the ZeroTouch deployment capabilities provided in the SonicWall portal.

Traditionally, a SonicWall firewall is required to act as the controller for the SonicPoint/SonicWave when deploying a wireless device. With the introduction of Wireless Network Manager, you can deploy SonicWall's wireless devices without a firewall. SonicWaves now include Capture ATP and a Content Filtering Service (CFS) to address all security concerns at the wireless LAN network level.

Licensing Requirements

The following SonicWall licenses are required to properly deploy SonicWall Wireless Network Manager.

- **Wireless Network Manager** (WNM) - Required
- **Content Filtering Service** (CFS) Premium Edition - Additional
- **Capture Advanced Threat Protection** (Capture ATP) - Additional

Registering and Deploying the SonicWave

The following steps are required to register and deploy your SonicWave using Wireless Network Manager (WNM):

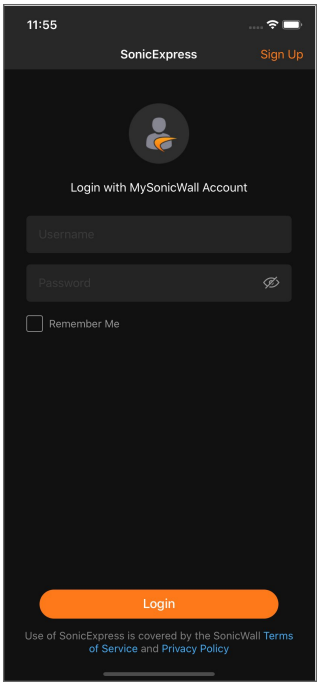
1. Register your SonicWave using an SonicExpress (Android or iOS) application.
2. Access WNM and setup a Zone and SSID.

Registering the SonicWave

ⓘ | **NOTE:** These steps are optional if you have already registered your device with MySonicWall.

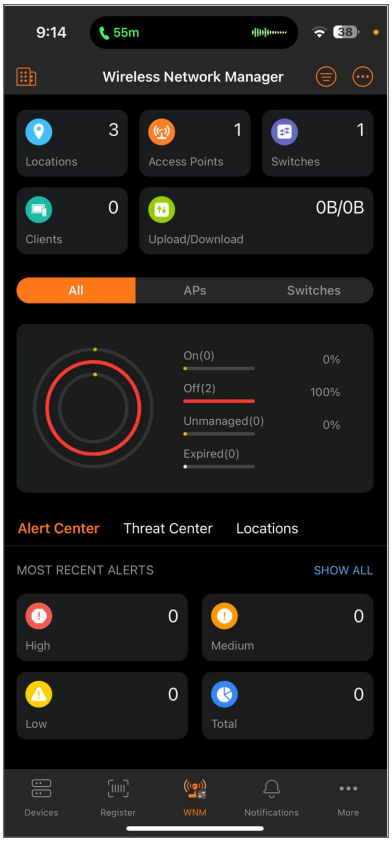
To register your SonicWave using the Wireless Network Manager:

1. Download and install the SonicExpress app from the app store for IOS devices or the Google Play store for Android devices. After installing the app, you can access all SonicWave devices associated with your account. You can also monitor and troubleshoot wireless connectivity using this application.
2. Log into the app using your MySonicWall username and password credentials.



Any SonicWave previously registered with MySonicWall appears. You can also find the option to add new SonicWave devices to your WNM directly from the application by scanning a QR code on the SonicWave or its packaging.

3. From the application **Console**, you can see a list of **Threats**, **Alerts**, **Traffic**, **Locations**, the number of SonicWave **Devices** you have, and the number of **Clients** associated with those SonicWave s.



ⓘ | **NOTE:**

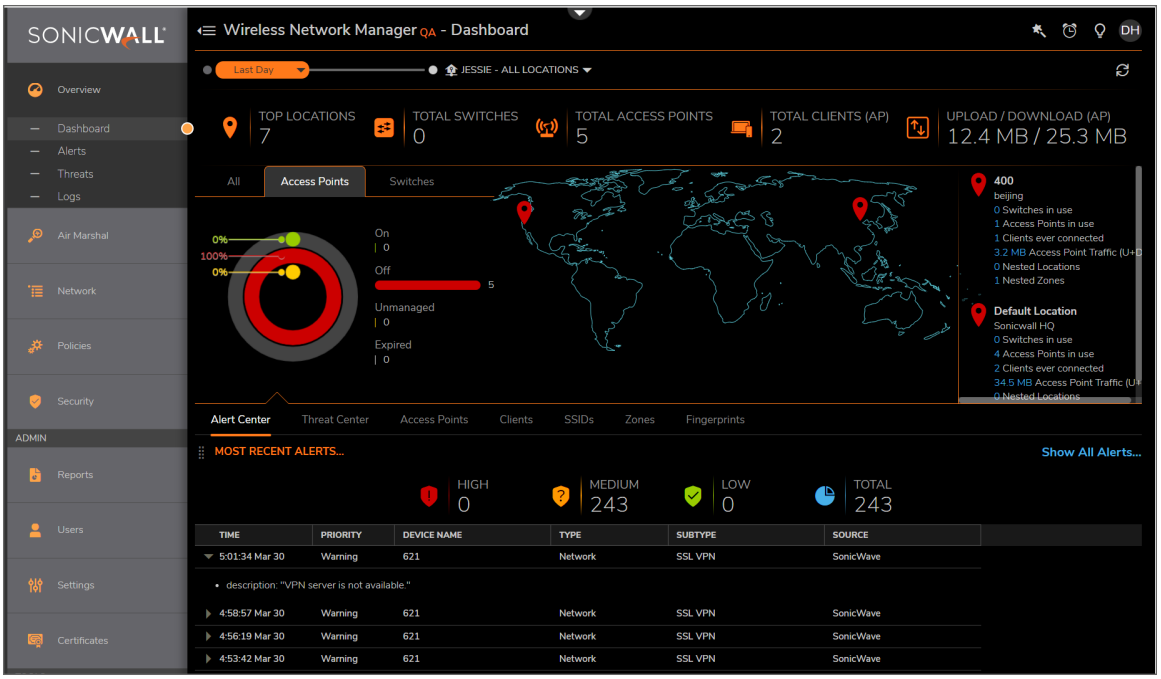
- The SonicWave firmware is not available in the MySonicWall for all the series. The standalone SonicWave does not support firmware upgrades. You can upgrade SonicWave's firmware through SonicWave, managed by the cloud management WNM, and through firewall-managed access points. For more information refer to How to upgrade SonicWaves on WNM or How to download SonicWall access point firmware?.
- The SonicWave firmware available in the firewall and WNM portal differs for each model. To update the firmware in the firewall to the latest version, you can download the latest firmware from the WNM portal and then upload the downloaded file in the firewall to upgrade to the newest version.

Accessing the Wireless Network Manager

To access the Wireless Network Manager:

1. Log into `cloud.sonicwall.com` (Capture Security Center (CSC)) using your MySonicWall credentials. Multiple tiles showing all available services and products display.

2. Click the **Wireless Network Manager** option. You are redirected to the Dashboard of the WWireless Network Manager (`wcm.sonicwall.com`).

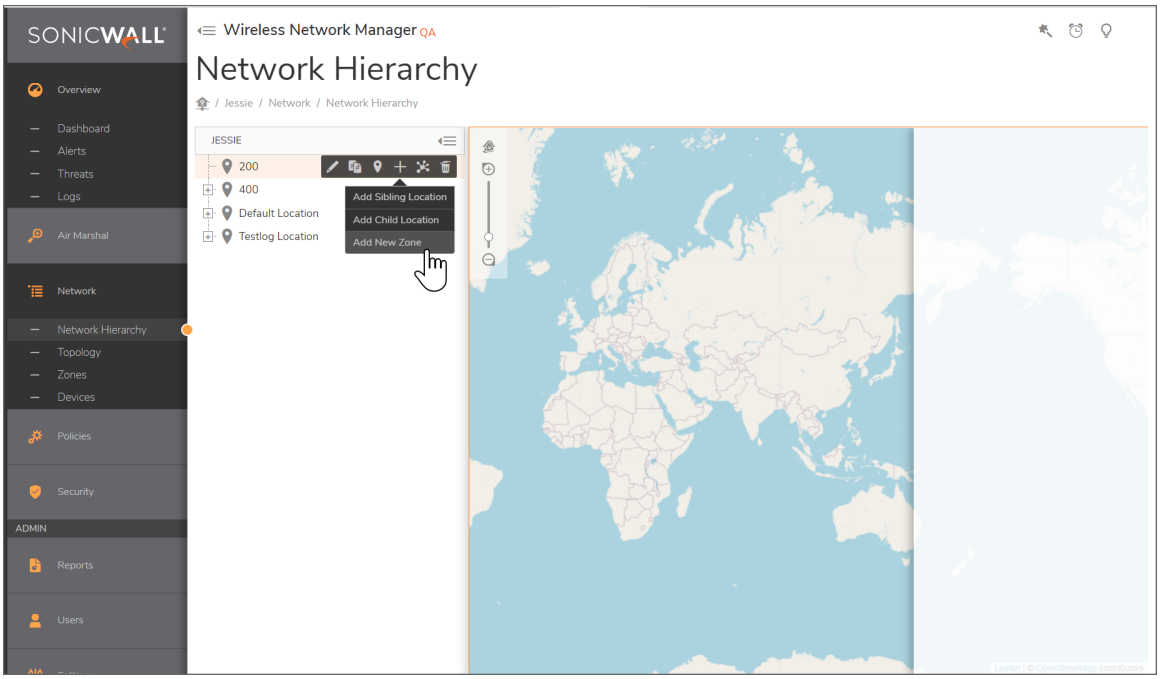


If you are deploying multiple SonicWave devices over multiple locations, you can create specific **Locations** and **Zones** unique to those devices.

Deploying with the Wireless Network Manager

To deploy a SonicWave using the Wireless Network Manager:

1. In Wireless Network Manager, navigate to **Network > Network Hierarchy**.



2. Set up a new SonicWave by first creating the **Location**(s) of your tenants and then the **Zone**(s) for those tenants.
3. To set up a **Location**, hover your mouse over the **Default Location** and click the **+ Add Location or Zone**.

   ⓘ **NOTE:** You can also hover over an existing firewall that you would like to associate with the SonicWave.

4. Choose from the options to **Add Sibling Location**, or **Add New Zone**. For this example, we chose **Add Sibling Location**.
5. In the **Location Name** field, change **New location** to `Test Lab`.
6. For the **Address**, change **location address** to your Tenant's city name.
7. Click OK.

The `Test Lab` you created should appear as a sibling to the **Default Location**.

8. Hover your mouse over the `Test Lab` location and click the **+** plus sign to **Add New Zone**.
9. For the **Zone Name**, enter `Lab Zone`.
10. For the **Description**, enter your own description of this zone to help differentiate it from other zones. This can be edited later.
11. Click **OK**.

    The `Lab Zone` you created should application as a child to your `Test Lab` in the Network Hierarchy. You will create a policy for this zone next.

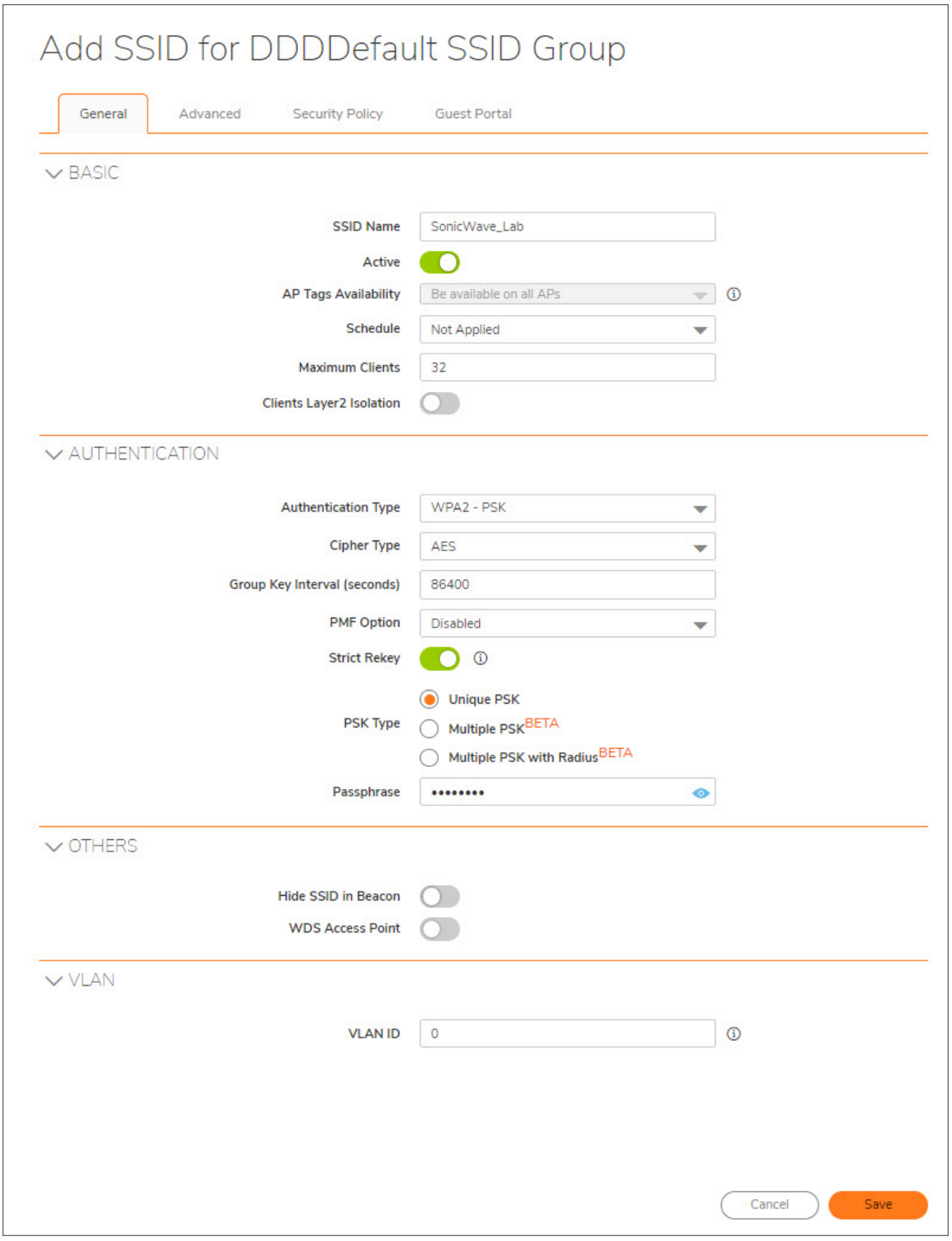
Creating a Zone Policy

Policies control the broad functionality carried out by a provisioning profile by enabling or disabling radios, band steering, channel width of the radio, transmitting power, and so on. In the **Default Policy**, the SSID data should already be configured and that is a great place to start in creating your new policies, as you will likely need to call that SSID data into your new policies. If you have yet to create a new SSID group and its associated SSIDs, continue using the default and revisit this section later.

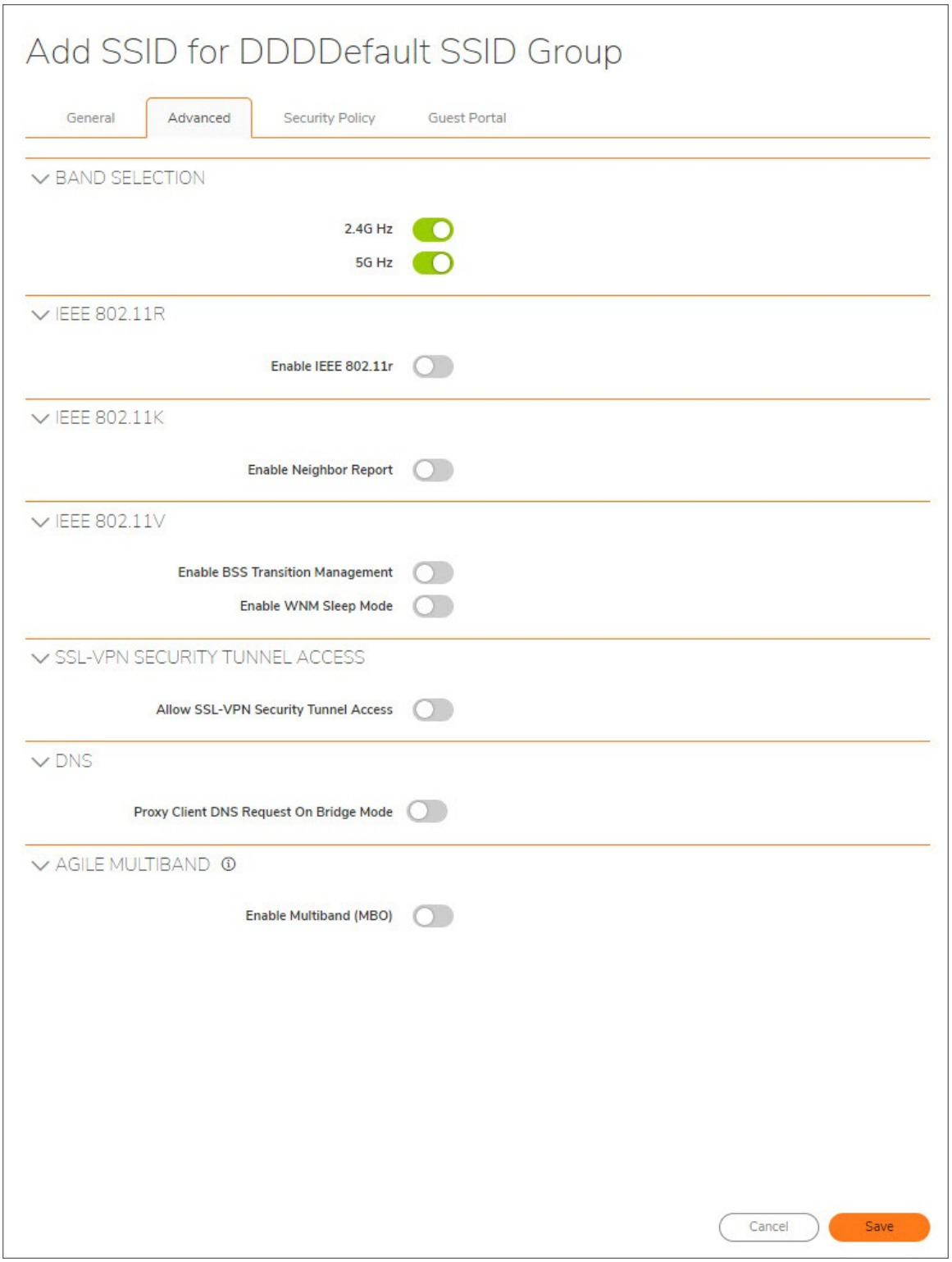
To create a Zone policy:

1. In Wireless Network Manager, navigate to **Policies > Policy Hierarchy**.
2. Hover your mouse over the **Default Policy** and click the **+ Add SSID Policy for this Policy**.

   Complete the form as follows.



3. Click the **Advanced** tab.
   Ensure the settings are as follows.

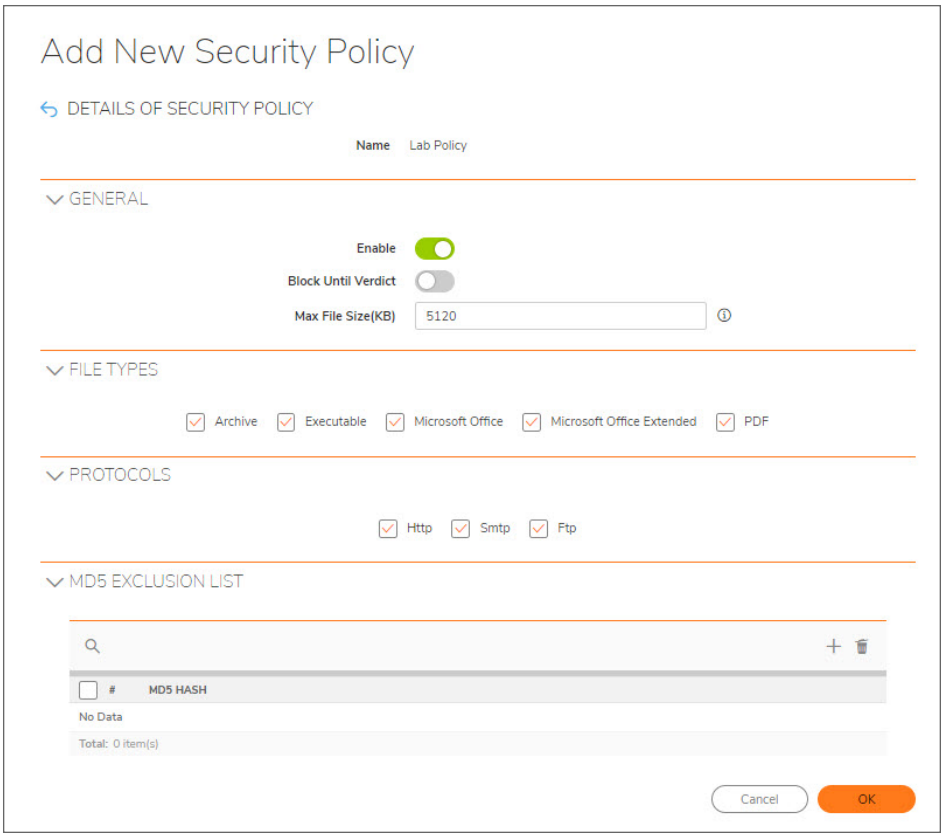

Add SSID for DDDDefault SSID Group
General
Advanced
Security Policy
Guest Portal
BAND SELECTION
2.4G Hz
5G Hz
IEEE 802.11R
Enable IEEE 802.11r
IEEE 802.11K
Enable Neighbor Report
IEEE 802.11V
Enable BSS Transition Management
Enable WNM Sleep Mode
SSL-VPN SECURITY TUNNEL ACCESS
Allow SSL-VPN Security Tunnel Access
DNS
Proxy Client DNS Request On Bridge Mode
AGILE MULTIBAND
Enable Multiband (MBO)
Cancel
Save

4. Click **Save**.

The `SonicWave_Lab` appears as a sibling to the **Default Policy**.

5. Locate and hover your mouse over the `SonicWave_Lab`.
6. Click **+Add Security Policy for this SSID**.
   The **Add New Security Policy** dialog appears.

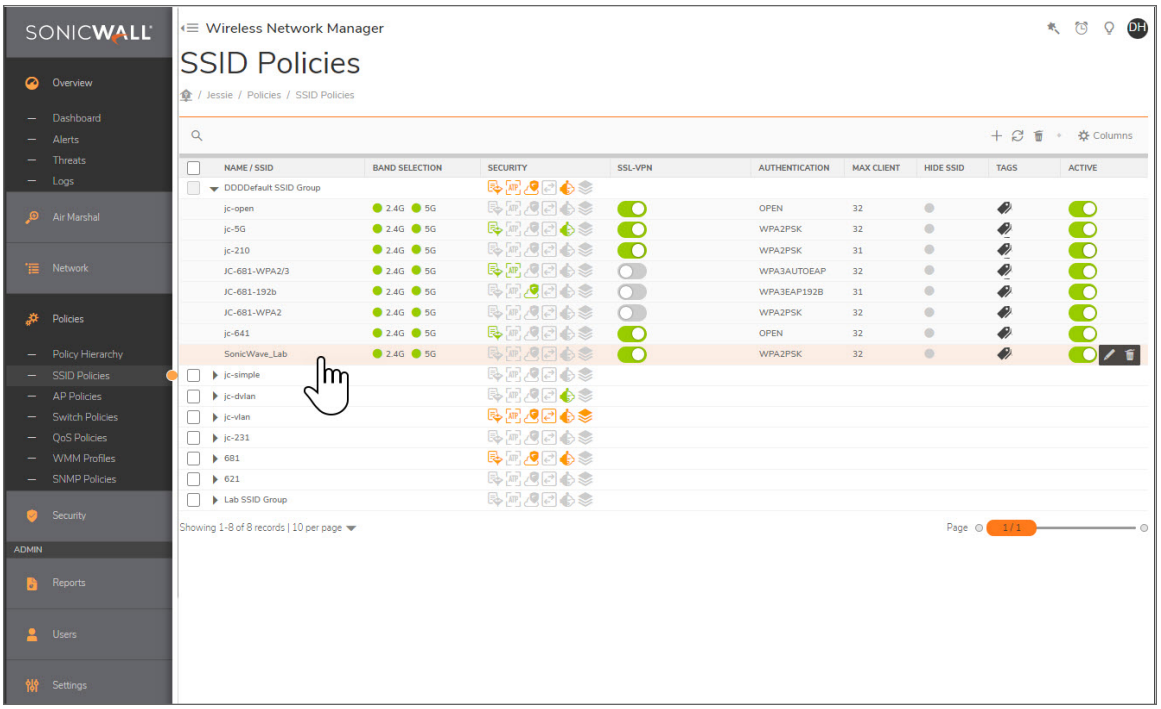
7. In the **Name** field, enter `Lab Policy`.
8. For the **Type** of policy, select a security policy appropriate for your organization.
9. Click **Next**.



10. Include any additional settings you would like to complete the policy.
11. In **Policies > Policy Hierarchy**, select the AP Policy and click on the RRM tab and configure the following settings:
    - Radio Resource Management
    - Dynamic Channel Selection
    - Client Load Balancing

> **NOTE:** Implementing Global Dynamic Channel Selection (DCS) facilitates the optimal selection of channels for SonicWave devices. Utilizing the DCS algorithm, the system leverages Radio Resource Management (RRM) to dynamically guide client devices to the access point (AP), which can provide the most robust signal strength.

12. Click **Save** when you are finished. These settings can be edited later.
13. The `SonicWave_Lab` and its associated SSID policies should appear on the **Policies > SSID Polices** page where you can complete additional configuration.



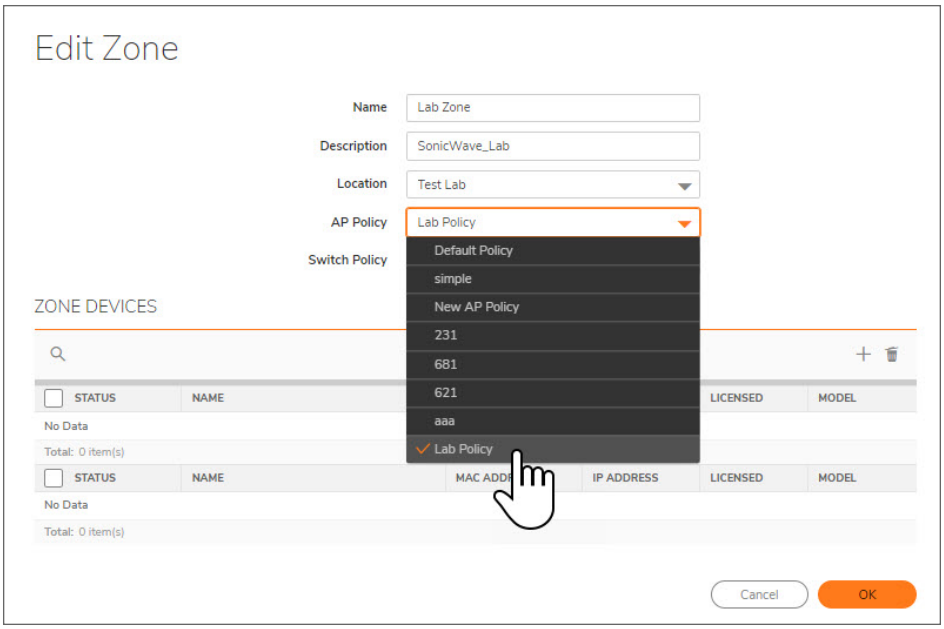
In the next section, you will link this **Policy** with the **Zone** you created earlier.

Linking the Policy to the Zone

Now that you have created a **Tenant**, a **Location**, a **Zone**, and a **Policy**, you can link them all together where they can operate using the criteria you established for each.

To link the Policy with the Zone:

1. Navigate in Wireless Network Manager to **Network > Zones**.
2. Locate the `Lab Zone` entry you created earlier and hover your mouse over the top of it.
3. Click **Edit**.
   The **Edit Zone** dialog appears.



4. For the **AP Policy**, select the `Lab Policy` you created earlier.
5. Click **OK**.

6. The **Lab Zone**, the **Hierarchy**, the **AP Policy**, and other information now appear as a completed zone/policy instance. Your client devices should begin connecting for visibility on the Dashboard where you can see its MAC address and any traffic utilized by it.

6

Using SonicPoint FairNet Bandwidth Limit Policies

The SonicPoint FairNet feature delivers an easy-to-use method for you to control the bandwidth of your associated wireless clients and make sure that bandwidth is distributed fairly between them. You can configure the SonicPoint FairNet bandwidth limits for all your wireless clients, specific IP address ranges, or individual clients to help provide them with fairness and network efficiency. FairNet guarantees a minimum amount of bandwidth to each wireless client in order to prevent disproportionate bandwidth consumption by a single user.

SonicPoint FairNet Features

The following features are included with SonicPoint FairNet:

- **Distributed Coordination Function**

  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 SonicPoint 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.

- **Traffic Control**

  The traffic control feature decides when packets are queued or dropped (for example, when the queue has reached a length limit, or when the traffic exceeds a rate limit). It can also decide in which order packets are sent (for example, to give priority to certain owners) and it can also delay the sending of packets (such as limiting the rate of outbound traffic). After traffic control has released a packet to send, the device driver picks it up and submits it to the network.

ⓘ | **NOTE:** Fairnet is unsupported on the SonicPoint Ni or Ne access points.

Configuring SonicPoint FairNet

The following is an example of a FairNet configuration.

To configure FairNet to provide more bandwidth in both directions:

1. Navigate to **DEVICE | Access Points > FairNet**.
2. Select **Enable FairNet**.
3. Click **OK**.

To create the required FairNet policy:

1. Navigate to **DEVICE | Access Points > FairNet**.
2. Click **+Add FairNet Policy**.
3. From the **Add FairNet Policy** dialog, confirm the **Enable policy** slider is green. This option is enabled by default.
4. From the **Direction** drop-down menu, select **Both Directions**. This applies the policy to clients that are both uploading and downloading content.
5. In the **Start IP** text box, enter the starting IP address (`172.16.29.100`) for the FairNet policy.
6. In the **End IP** text box, enter the ending IP address (`172.16.29.110`) for the FairNet policy.
   ⓘ | **TIP:** The IP address range must exist on a subnet that is configured for a WLAN interface.
7. In the **Min Rate(kbps)** text box, enter the minimum bandwidth (1000 Kbps) for the FairNet policy.
8. In the **Max Rate(kbps)** text box, enter the maximum bandwidth (2000 Kbps) for the FairNet policy.
9. From the **Interface** drop-down menu, select an interface (X2) to which the SonicPoint appliance is connected.
10. Click **OK**.
11. From the **FairNet Policies** list, confirm the **Enable FairNet** slider is selected green.
12. Click **Accept**.
    Your FairNet policy is now configured.

7

SonicWall Support

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

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

The Support Portal enables you to:

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

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

About This Document

NOTE: A NOTE icon indicates supporting information.

IMPORTANT: An IMPORTANT icon indicates supporting information.

TIP: A TIP icon indicates helpful information.

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

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

SonicWave Deployment Guide
Updated - August 2024
232-005825-00 Rev A

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 applicationlicable 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