▷ COMPREHENSIVE INTERNET SECURITY™

SonicWALL Secure Wireless Solution

SonicPoint and SonicPoint G Getting Started Guide

SONICWALL

SonicPoint and SonicPoint G Getting Started Guide

The SonicWALL SonicPoint and SonicPoint G provide secure wireless access to your network, managed from your SonicWALL TZ 170 Series or PRO Series security appliance running SonicOS Enhanced.

This *SonicPoint Getting Started Guide* supports both the SonicPoint and the SonicPoint G:

- The SonicPoint provides 802.11a (5.0 GHz radio band) and 802.11b/g (2.4 GHz radio band) wireless connections. The SonicPoint can be managed by a SonicWALL security appliance running SonicOS Enhanced 2.5 or higher.
- The SonicPoint G provides 802.11b/g (2.4 GHz radio band) wireless connections, and provides detachable antennas. The SonicPoint G can be managed by a SonicWALL security appliance running SonicOS Enhanced 3.2, or higher.

The *SonicPoint Getting Started Guide* provides instructions for setting up your SonicPoint, configuring your SonicWALL security appliance to manage the SonicPoint and support secure WiFiSec connections from wireless clients. After you complete this guide, refer to the *SonicOS Enhanced Administrator's Guide* and the *SonicWALL Secure Wireless Solution Guide for* more detailed information.

Note: *The latest versions of the SonicPoint Getting Started Guide, SonicPoint Administrator's Guide, SonicWALL Secure Wireless Solution Guide, SonicOS Enhanced Administrator's Guide, and all other SonicWALL product documentation are available on the SonicWALL Web site at <http://www.sonicwall.com/support/documentation.html>.*

SonicPoint

SonicPoint G

Before You Begin

Check Package Contents

- One SonicWALL SonicPoint
- One SonicPoint Getting Started Guide
- One SonicPoint Regulatory Statement
- One SonicWALL Services insert card
- One SonicPoint Resource CD
- One Ethernet cable
- One 12 volt, 1.66 amp DC power supply
- One power cord*
- One mounting plate
- One wall mount kit
- Two detachable antennas (SonicPoint G only)

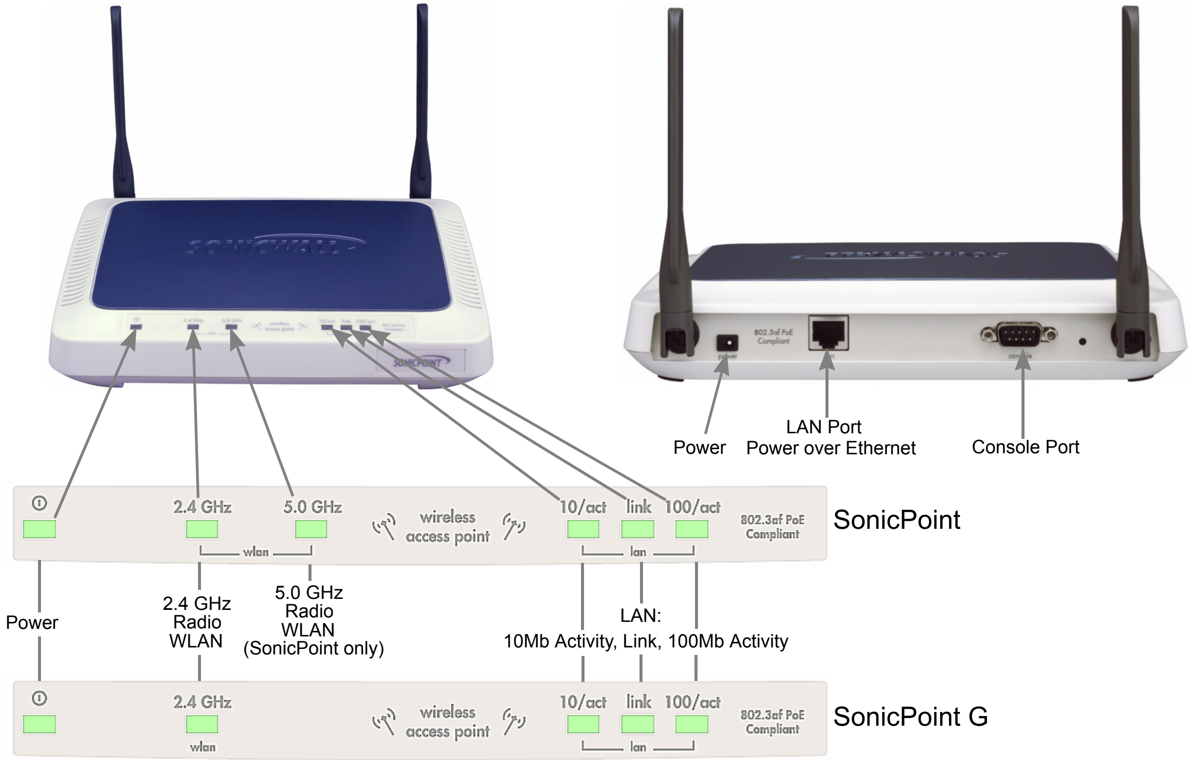
**A power cord is included only with units shipped to North America.*

Any Items Missing?

If any items are missing from your package, contact:

SonicWALL Support
Web: <http://www.sonicwall.com/support/>
E-mail: customer_service@sonicwall.com

Overview of the SonicWALL SonicPoint Hardware



Front Panel

The front panel of the SonicPoint has the following LEDs (from left to right):

- **Power** - Blinks when the device is powering up. After the SonicPoint is powered up, the Power LED turns steady.
- **WLAN 2.4 GHz Radio** - Blinks at a constant rate when the SonicPoint is ready to receive traffic, and blinks at a variable rate while transferring data with connected 802.11g/b stations.
- **WLAN 5.0 GHz Radio** - (SonicPoint only) Blinks at a constant rate when the SonicPoint is ready to receive traffic, and blinks at a variable rate while transferring data with connected 802.11a stations.
- **LAN 10/act** - Blinks to indicate 10Mb LAN activity.
- **LAN link** - Shines steadily to indicate physical layer connectivity.
- **LAN 100/act** - Blinks to indicate 100Mb LAN activity.

Back Panel

The back panel of the SonicPoint has the following three connections:

- **Power** - Connect the 12.0 volt DC power supply connector to the power port, if you are not using an 802.3af Power over Ethernet (PoE) Injector.
- **LAN / PoE** - Connect to your SonicWALL security appliance with a straight-through Ethernet cable. If you are not using the 12.0 volt DC power supply, connect the SonicWALL PoE Injector to the SonicPoint LAN port.
- **Console** - To display bootup and diagnostic messages through the command-line interface (CLI), connect one end of an RS-232 serial cable to the SonicPoint console port and the other end to your work station.

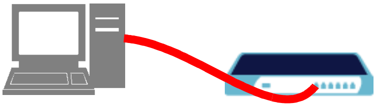
What You Need to Get Connected

- A SonicWALL SonicPoint
- A SonicWALL TZ 170 Series or PRO Series security appliance running:
    - SonicOS Enhanced 2.5 or higher to manage a SonicPoint
    - SonicOS Enhanced 3.1.3.x, 3.2, or higher to manage a SonicPoint G
- An active Internet connection if you are using a SonicWALL TZ 170 Series security appliance
- An interface on the SonicWALL security appliance configured as part of a Wireless zone, for example the default, WLAN
- A location selected for placement of your SonicPoint. You can mount the SonicPoint on any surface, on the wall, or the ceiling. For mounting instructions, refer to the *SonicPoint Regulatory Statement* included in your SonicPoint package
- SonicWALL Global VPN Client (GVC) or SonicWALL Global Security Client (GSC) running on your wireless clients

SonicPoint Setup Procedures

Setting up your SonicPoint consists of procedures in three categories:

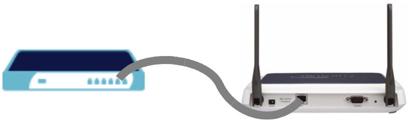
Configuring Your SonicWALL Security Appliance



Because you manage a SonicPoint from a SonicWALL security appliance running SonicOS Enhanced, you first configure the wireless settings on the SonicWALL security appliance. These settings include radio settings, the number of SonicPoints deployed, and security settings. This guide instructs you to set up WiFiSec security. For other security options, refer to the *SonicWALL Secure Wireless Solution Guide*.

When the SonicWALL security appliance detects a connection to a SonicPoint, it automatically provisions the SonicPoint with the settings you configure in these steps.

Setting Up Your SonicPoint



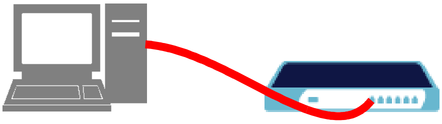
After you configure your SonicWALL security appliance, you can physically set up and register your SonicPoint.

Setting Up Secure Wireless Connections

When your SonicPoint is set up, you can configure your wireless clients to communicate with it.

Note: *This guide provides instructions to set up your SonicPoint in managed mode. The SonicPoint can also operate in stand-alone mode, refer to the SonicWALL SonicPoint Administrator's Guide for instructions on using stand-alone mode.*

Configuring Your SonicWALL Security Appliance



Configuring your SonicWALL TZ 170 Series or PRO Series security appliance to manage SonicPoints consists of the following procedures:

- “Configuring a Wireless Zone Interface” on page 5
- “Configuring the Default SonicPoint Profile” on page 7

1 Configuring a Wireless Zone Interface

SonicOS Enhanced running on a SonicWALL security appliance provides you with a Wireless zone type. SonicOS automatically searches for SonicPoints connected to a Wireless zone and configures them with the default profile for that zone. By default, SonicOS only allows traffic from a SonicPoint to pass through a Wireless zone.

SonicOS Enhanced offers a default Wireless zone called “WLAN”. This guide instructs you on using the default WLAN zone.

Note: *You can create custom Wireless zones to manage different levels of security. When you create the new zone, select **Wireless** for the **Zone Type**. For instructions on creating custom zones, refer to the SonicOS Enhanced Administrator’s Guide.*

Configuring a WLAN Zone Interface

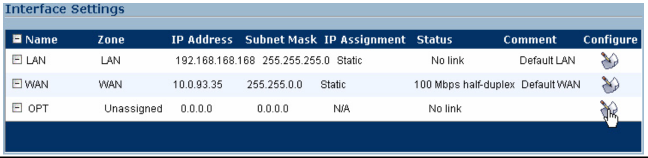
To configure an interface on the WLAN zone:

1. With a Web browser, connect to your SonicWALL security appliance and open the SonicOS management interface.
2. Click Network in the left-navigation menu.
3. In the **Network > Interfaces** page, select a port or interface to assign to the WLAN zone.

- SonicWALL TZ 170 Series: **OPT**
- SonicWALL PRO 1260: **OPT**
- SonicWALL PRO 2040: **X2** - **X3**
- SonicWALL PRO 3060 though PRO 5060: **X2** - **X5**
- SonicWALL PRO 5060 Fiber: **F1** - **F2**, **X2** - **X3**

4. Click the edit icon for the interface you select.

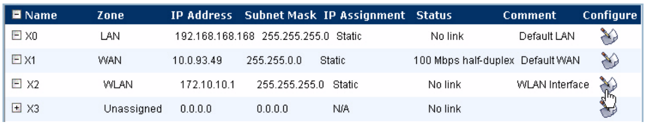
TZ 170 Series
PRO 1260
OPT:



Interface Settings

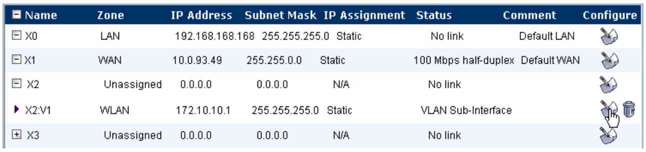
Name	Zone	IP Address	Subnet Mask	IP Assignment	Status	Comment	Configure
⊟ LAN	LAN	192.168.168.168	255.255.255.0	Static	No link	Default LAN	
⊟ WAN	WAN	10.0.93.35	255.255.0.0	Static	100 Mbps half-duplex	Default WAN	
⊟ OPT	Unassigned	0.0.0.0	0.0.0.0	N/A	No link		

PRO Series
X2 - **X5**:



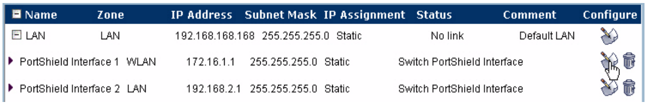
Name	Zone	IP Address	Subnet Mask	IP Assignment	Status	Comment	Configure
⊟ X0	LAN	192.168.168.168	255.255.255.0	Static	No link	Default LAN	
⊟ X1	WAN	10.0.93.49	255.255.0.0	Static	100 Mbps half-duplex	Default WAN	
⊟ X2	WLAN	172.10.10.1	255.255.255.0	Static	No link	WLAN Interface	
⊞ X3	Unassigned	0.0.0.0	0.0.0.0	N/A	No link		

PRO 4060
PRO 5060
VLAN:



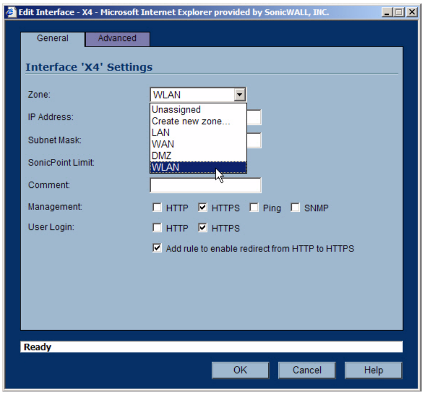
Name	Zone	IP Address	Subnet Mask	IP Assignment	Status	Comment	Configure
⊟ X0	LAN	192.168.168.168	255.255.255.0	Static	No link	Default LAN	
⊟ X1	WAN	10.0.93.49	255.255.0.0	Static	100 Mbps half-duplex	Default WAN	
⊟ X2	Unassigned	0.0.0.0	0.0.0.0	N/A	No link		
▸ X2:V1	WLAN	172.10.10.1	255.255.255.0	Static		VLAN Sub-Interface	
⊞ X3	Unassigned	0.0.0.0	0.0.0.0	N/A	No link		

PRO 1260
PortShield:



Name	Zone	IP Address	Subnet Mask	IP Assignment	Status	Comment	Configure
⊟ LAN	LAN	192.168.168.168	255.255.255.0	Static	No link	Default LAN	
▸ PortShield Interface 1	WLAN	172.16.1.1	255.255.255.0	Static		Switch PortShield Interface	
▸ PortShield Interface 2	LAN	192.168.2.1	255.255.255.0	Static		Switch PortShield Interface	

5. In the **Edit Interface** window, select **WLAN** from the **Zone** list.



Edit Interface - X4 - Microsoft Internet Explorer provided by SonicWALL, INC.

Interface 'X4' Settings

Zone: WLAN

IP Address:

Subnet Mask:

SonicPoint Limit:

Comment:

Management: ☐ HTTP ☑ HTTPS ☐ Ping ☐ SNMP

User Login: ☐ HTTP ☑ HTTPS

☑ Add rule to enable redirect from HTTP to HTTPS

Ready

6. Enter an IP address range and netmask for the interface in the **IP Address** and **Subnet Mask** field. For example, an IP address range of 172.32.16.1 and a subnet of 255.255.255.0.

7. In the **SonicPoint Limit** field, select the number of SonicPoints you will attach to this interface. That way you can select an appropriate subnet mask.

8. Click OK.

Use this interface when you connect a SonicPoint to your SonicWALL security appliance. Then the SonicPoint is automatically connected to the Wireless zone.

Note: *You can assign several interfaces to the same Wireless zone.*

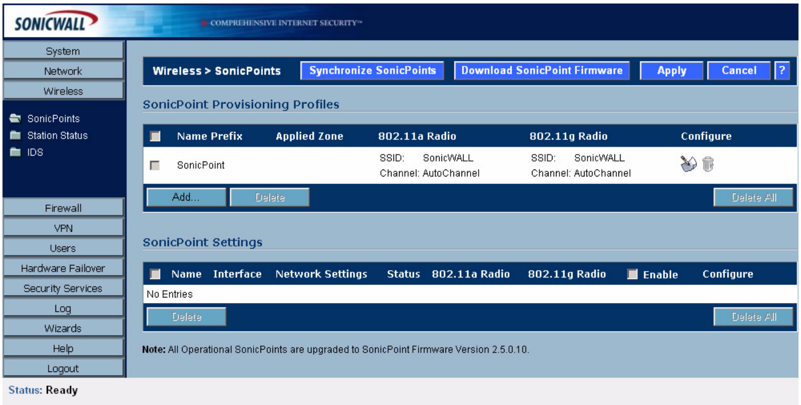
2 Configuring the Default SonicPoint Profile

The SonicPoint Profile contains the configuration that SonicOS applies to all SonicPoints connected to a Wireless (default: **WLAN**) zone. SonicOS applies the settings in the SonicPoint Profile when it first detects a SonicPoint.

Note: *To reapply the settings in a SonicPoint Profile, delete the individual SonicPoint from **SonicPoint Settings** table in the **SonicPoint > SonicPoints** page, then let the SonicWALL security appliance detect the SonicPoint again and apply the settings.*

To configure the default SonicPoint Profile:

1. In the management interface of your SonicWALL security appliance, click on **SonicPoint** in the left-navigation menu, and then click on **SonicPoints**.



SonicPoint Provisioning Profiles

□	Name Prefix	Applied Zone	802.11a Radio	802.11g Radio	Configure
□	SonicPoint		SSID: SonicWALL Channel: AutoChannel	SSID: SonicWALL Channel: AutoChannel	

SonicPoint Settings

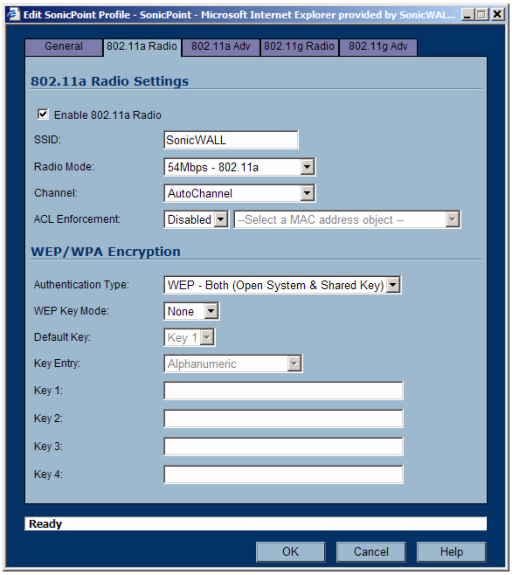
□	Name	Interface	Network Settings	Status	802.11a Radio	802.11g Radio	□ Enable	Configure
No Entries								

Note: All Operational SonicPoints are upgraded to SonicPoint Firmware Version 2.5.0.10.

Status: Ready

2. In the **SonicPoint Provisioning Profiles** list, select the default **SonicPoint** profile and click the edit icon .

3. In the **Edit SonicPoint Profiles** window, configure the radio settings and the Service Set Identifiers (SSIDs) of the SonicPoints in the WLAN zone. You should at least set the SSIDs in the **802.11a Radio** (SonicPoint only) tab and the **802.11g Radio** tab to a recognizable value, for example: "*MyCorp Wireless Network*".


Edit SonicPoint Profile - SonicPoint - Microsoft Internet Explorer provided by SonicWAL...
General
802.11a Radio
802.11a Adv
802.11g Radio
802.11g Adv
OK
Cancel
Help

802.11a Radio Settings

☑ Enable 802.11a Radio

SSID: SonicWALL

Radio Mode: 54Mbps - 802.11a

Channel: AutoChannel

ACL Enforcement: Disabled --Select a MAC address object --

WEP/WPA Encryption

Authentication Type: WEP - Both (Open System & Shared Key)

WEP Key Mode: None

Default Key: Key 1

Key Entry: Alphanumeric

Key 1:

Key 2:

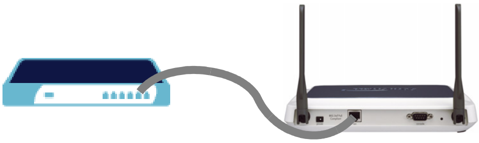
Key 3:

Key 4:

Ready

Note: *You can add additional profiles and assign them to different Wireless zones. Refer to the SonicOS Enhanced Administrators Guide.*

Setting Up Your SonicPoint



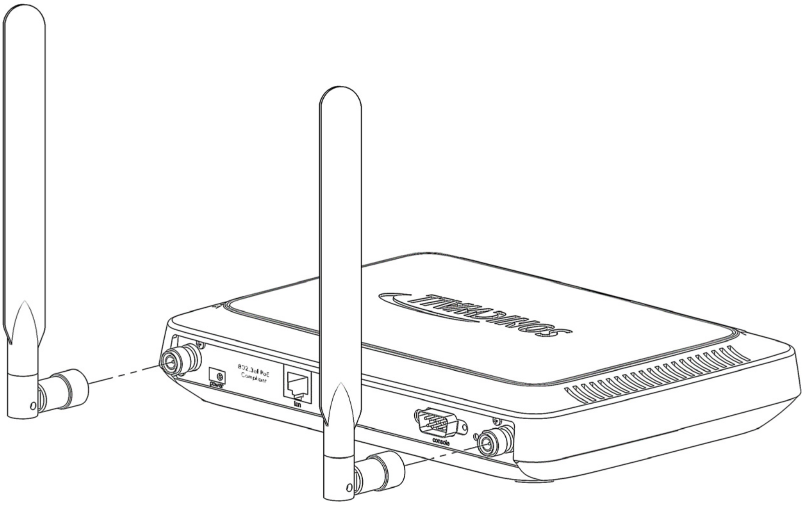
Setting up your SonicPoint consists of the following procedures:

- "Installing the Antennas (SonicPoint G Only)" on page 9
- "Applying Power to the SonicPoint" on page 10
- "Connecting the SonicPoint" on page 11

3

Installing the Antennas (SonicPoint G Only)

The SonicPoint G comes with detachable antennas, which you must install. Remove the antennas from the bag and place one on each connector. Finger tighten the fittings.



Note: *The SonicPoint G is authorized to use a dipole antenna with 4dBi or less. Only use antennas provided by SonicWALL; otherwise your authority to use this unit may be revoked. Be aware of the regulations in your area before using other antennas with the SonicPoint G.*

Adjusting the Antennas

You can adjust the antennas for best radio reception. In most cases, the antennas should be pointing straight up and perpendicular to the box. Start from that position, and move them until you notice better reception. Certain areas, such as the areas directly below the SonicPoint, have weaker reception.

4 Applying Power to the SonicPoint

You have two options for applying power to the SonicPoint:

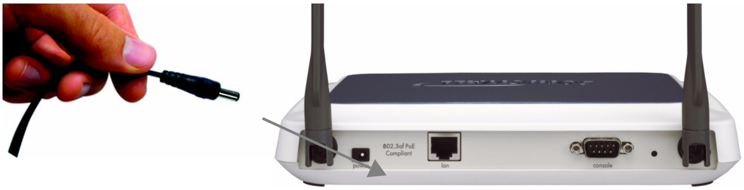
- “Option 1: Using the SonicWall Power Supply” on page 10
- “Option 2: Applying Power with a Power over Ethernet Injector” on page 10

Option 1: Using the SonicWall Power Supply

Attach the power supply to the power cord. Plug the power adapter into the SonicPoint and plug the other end into a power outlet.

The **Power** LED turns green when power is applied to the SonicPoint.

▲ **Warning:** *Only use a SonicWALL-approved 12V, 1.66A power supply.*

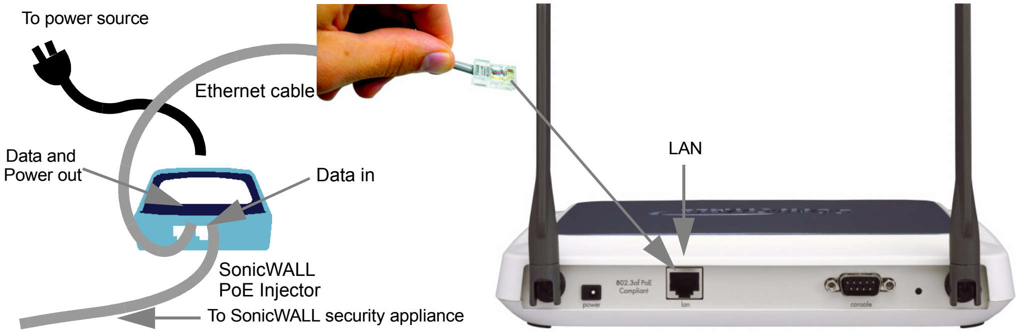


Option 2: Applying Power with a Power over Ethernet Injector

If you are using the SonicWALL Power over Ethernet (PoE) Injector or any standard 802.3af PoE injector, you do not need to plug a separate power cord into the SonicPoint. The SonicPoint has the option of receiving power through the Ethernet cable inserted into its LAN port for enhanced deployment flexibility.

Note: *For more information on the SonicWALL PoE Injector, visit <http://www.sonicwall.com/products>.*

1. Plug the power cord of the SonicWALL PoE injector into the power outlet.
2. Connect an Ethernet cable to the **Data and Power out** port on the SonicWALL PoE injector and connect the other end of the cable to the **LAN** port on the back of your SonicPoint.



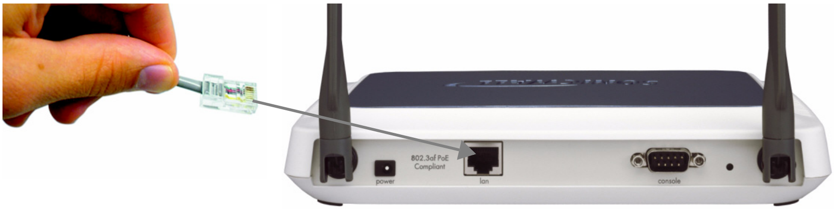
5

Connecting the SonicPoint

If you are not using a SonicWALL PoE Injector, connect one end of an Ethernet cable to the WLAN zone interface that you created earlier on the SonicWALL security appliance and the other end of the cable to either the **LAN** port on the SonicPoint, or any Layer 2 hub or switch.

If you are using a SonicWALL PoE Injector, connect one end of the Ethernet cable to the WLAN zone interface that you created earlier and the other end of the cable to the **Data in** port on the SonicWALL PoE Injector. Connect the **Data and Power out** port on the SonicWALL PoE Injector to the **LAN** port on your SonicPoint.

The **link** LED lights up to indicate an active connection.

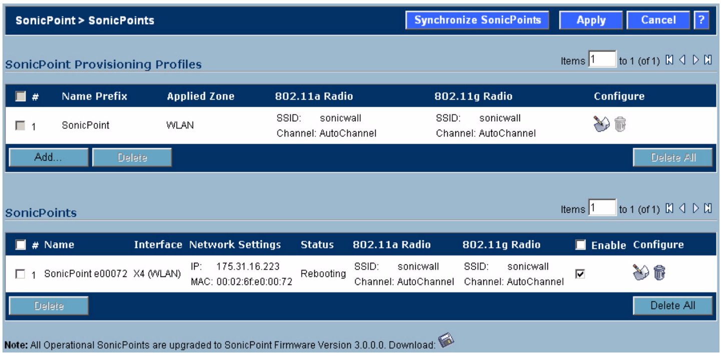


Note: *It takes approximately one minute for the SonicWALL security appliance to auto-provision the SonicPoint. At the end of this process, your SonicPoint is configured with the settings in the default SonicPoint provisioning profile.*

Your SonicPoint should automatically display in the list on the **Wireless > SonicPoints** page of the management interface for the SonicWALL security appliance managing the SonicPoint. If it does not:

- Check that the SonicPoint is properly connected to the SonicWALL security appliance.
- Make sure the interface the SonicPoint is connected to is configured as part of a Wireless zone (WLAN by default).

- Click the **Synchronize SonicPoints** button near the top-right corner of the page to refresh the display.



SonicPoint Provisioning Profiles — Items 1 to 1 (of 1)

☐ #	Name Prefix	Applied Zone	802.11a Radio	802.11g Radio	Configure
☐ 1	SonicPoint	WLAN	SSID: sonicwall Channel: AutoChannel	SSID: sonicwall Channel: AutoChannel	

SonicPoints — Items 1 to 1 (of 1)

☐ #	Name	Interface	Network Settings	Status	802.11a Radio	802.11g Radio	☐ Enable	Configure
☐ 1	SonicPoint e00072	X4 (WLAN)	IP: 175.31.16.223 MAC: 00:02:6f:e0:00:72	Rebooting	SSID: sonicwall Channel: AutoChannel	SSID: sonicwall Channel: AutoChannel	☑	

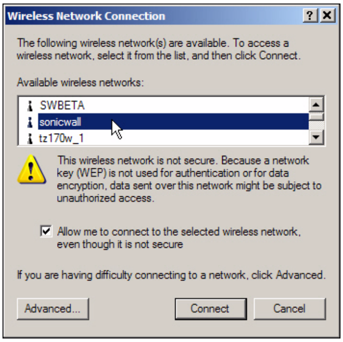
Note: All Operational SonicPoints are upgraded to SonicPoint Firmware Version 3.0.0.0. Download:

6 Testing the SonicPoint Radio

Once you have connected the SonicPoint, you should be able to establish a connection with a computer that has an 802.11 a, b, or g wireless card.

Note: *This step tests your ability to connect wirelessly to the SonicPoint. At this stage you may not be able to connect to the your network or Internet.*

Make sure the wireless card on your computer can detect the SSID you configured of your SonicPoint. Your wireless client may automatically detect and display the SonicPoint's SSID in a list of available wireless networks or you may need to manually configure your wireless connection with the SonicPoint's SSID.



The following wireless network(s) are available. To access a wireless network, select it from the list, and then click Connect.

Available wireless networks:

- SWBETA
- sonicwall
- tz170w_1

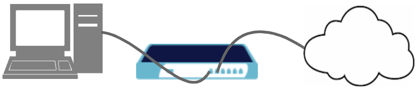
This wireless network is not secure. Because a network key (WEP) is not used for authentication or for data encryption, data sent over this network might be subject to unauthorized access.

☑ Allow me to connect to the selected wireless network, even though it is not secure

If you are having difficulty connecting to a network, click Advanced.

7

Registering Your SonicPoint



Once you have powered up your SonicPoint, you can register it at mySonicWALL.com. Registering your SonicPoint provides you with access to SonicWALL technical support for the device.

You register a SonicPoint on mySonicWALL.com as a child device to the registered SonicWALL security appliance with which you are managing the SonicPoint. Therefore, you must have a mySonicWALL.com account already set up and have your SonicWALL security appliance registered before you can register your SonicPoint.

Note: *mySonicWALL.com registration information is not sold or shared with any other company.*

To register your SonicPoint:

1. In your Web browser, log into your account at <https://www.mySonicWALL.com>.
2. In the list of registered products, click on the link for the SonicWALL security appliance you are using to manage the SonicPoint.
3. At the bottom of the **Service Management** page under the **Child Product Type** heading, click the **SonicPoint** link.
4. In the **My Product - Associated Products** page, enter the serial number of the SonicPoint. You can also enter a friendly name, which mySonicWALL.com uses to communicate with you about the SonicPoint.
5. Click **Register**, and your SonicPoint is registered and associated with the SonicWALL security appliance you are using to manage it.

Setting Up Secure Wireless Connections

Setting up your secure wireless network includes the following procedures:

- “Enabling Secure Wireless Connections” on page 14
- “Connecting Wireless Clients to the SonicPoint” on page 19

8

Enabling Secure Wireless Connections

Enabling a secure wireless connection through your SonicPoint involves the following configuration steps in the management interface of your SonicWALL security appliance and on the wireless clients:

- “Verifying WiFiSec Enforcement is Enabled on the WLAN Zone” on page 14
- “Enabling the WLAN GroupVPN Policy on Your Wireless Zone” on page 15
- “Configuring Users with Authenticated Access to the GroupVPN Policy” on page 17

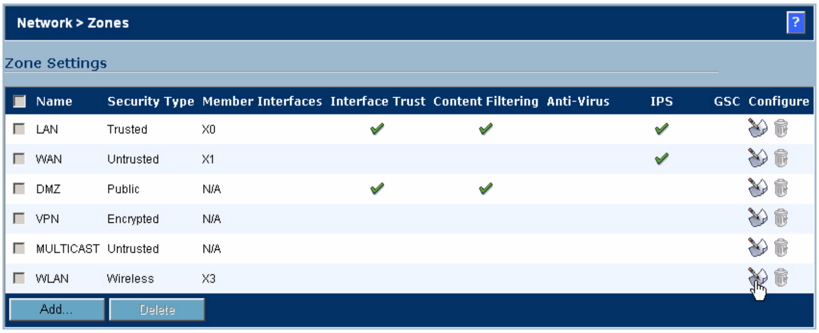
Verifying WiFiSec Enforcement is Enabled on the WLAN Zone

WiFiSec is a security protocol that uses IPSec VPN over the wireless connection to maintain security. WiFiSec enforcement is enabled by default on the WLAN zone.

Note: *By following these steps, your SonicPoint provides the highest level of wireless security possible. If you do not want to enable WiFiSec for wireless client connections, you can disable WiFiSec enforcement in step 4 of this procedure.*

To verify WiFiSec is enforced on the WLAN zone:

1. In the management interface of your SonicWALL security appliance, click on **Network** in the left-navigation menu, and then click on **Zones** under **Network**.
2. In the list of zones on the **Network > Zones** page, click the edit icon in the same line as your Wireless zone.

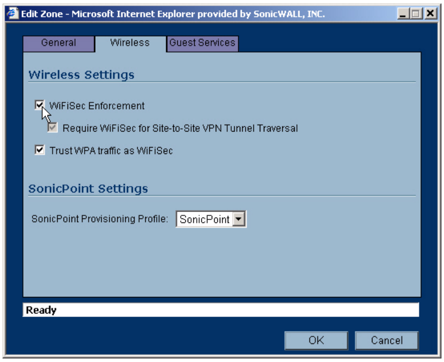


Network > Zones

Zone Settings

□ Name	Security Type	Member Interfaces	Interface Trust	Content Filtering	Anti-Virus	IPS	GSC	Configure
□ LAN	Trusted	X0	✓	✓		✓		
□ WAN	Untrusted	X1				✓		
□ DMZ	Public	N/A	✓	✓				
□ VPN	Encrypted	N/A						
□ MULTICAST	Untrusted	N/A						
□ WLAN	Wireless	X3						

3. In the **Edit Zone** window, click the **Wireless** tab.
4. In the **Wireless** tab, verify that the **WiFiSec Enforcement** box is checked and click OK.



Edit Zone - Microsoft Internet Explorer provided by SonicWALL, INC.

Wireless Settings

☑ WiFiSec Enforcement

☑ Require WiFiSec for Site-to-Site VPN Tunnel Traversal

☑ Trust WPA traffic as WiFiSec

SonicPoint Settings

SonicPoint Provisioning Profile: SonicPoint

Ready

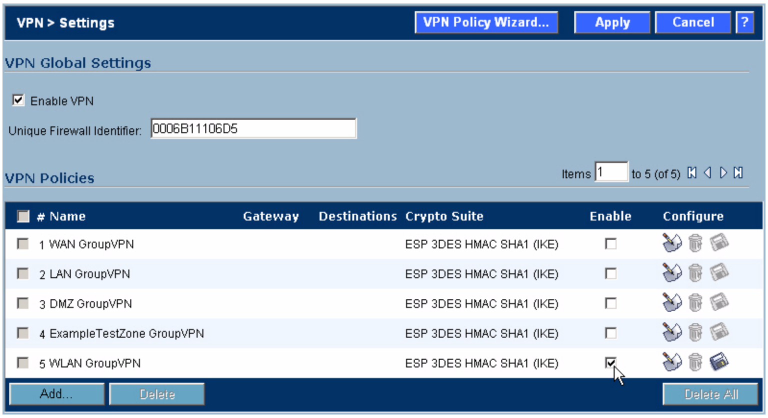
Enabling the WLAN GroupVPN Policy on Your Wireless Zone

Enabling the default **WLAN GroupVPN** policy on your Wireless zone allows wireless clients to securely access your network using SonicWALL Global VPN Client (GVC) or SonicWALL Global Security Client (GSC).

Note: *For instructions on adding a GroupVPN Policy to a custom zone, refer to the SonicOS Enhanced Administrator's Guide.*

To enable the WLAN GroupVPN policy:

1. In the management interface of your SonicWALL security appliance, click on **VPN** in the left-navigation menu, and then click on **Settings** under **VPN**.
2. In the list of VPN policies on the **VPN > Settings** page, check the box under **Enable** for the WLAN GroupVPN policy and click Apply.



VPN > Settings

VPN Global Settings

☑ Enable VPN

Unique Firewall Identifier: 0006B11106D5

VPN Policies

Items 1 to 5 (of 5)

□ # Name	Gateway	Destinations	Crypto Suite	Enable	Configure
□ 1 WAN GroupVPN			ESP 3DES HMAC SHA1 (IKE)	□	
□ 2 LAN GroupVPN			ESP 3DES HMAC SHA1 (IKE)	□	
□ 3 DMZ GroupVPN			ESP 3DES HMAC SHA1 (IKE)	□	
□ 4 ExampleTestZone GroupVPN			ESP 3DES HMAC SHA1 (IKE)	□	
□ 5 WLAN GroupVPN			ESP 3DES HMAC SHA1 (IKE)	☑	

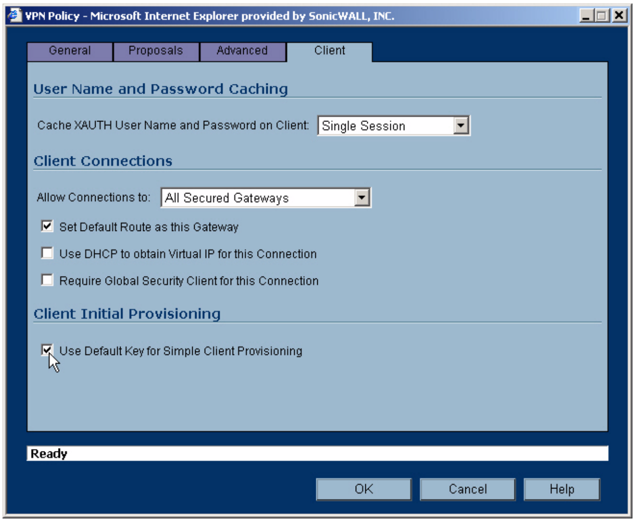
To make connecting wireless clients to your secure wireless network easier, you can specify that all SonicWALL GVC or SonicWALL GSC connections use the default shared secret value, generated by the SonicWALL security appliance. If you do not configure the **WLAN GroupVPN** policy with this setting, wireless clients are prompted for the shared secret value, which they must enter before establishing a WiFiSec connection.

Making Client Configuration Easier

You can enable the WLAN GroupVPN policy to automatically download the shared secret to SonicWALL GVC or SonicWALL GSC clients to make client configuration easier:

1. In the list of VPN policies on the **VPN > Settings** page, click the edit icon in the same line as your **WLAN GroupVPN** policy.
2. In the **VPN Policy** window, click on the **Client** tab.

3. In the **Client** page, check the **Use Default Key for Simple Client Provisioning** checkbox and click OK.


VPN Policy - Microsoft Internet Explorer provided by SonicWALL, INC.
General
Proposals
Advanced
Client
OK
Cancel
Help

User Name and Password Caching

Cache XAUTH User Name and Password on Client: Single Session

Client Connections

Allow Connections to: All Secured Gateways

☑ Set Default Route as this Gateway

□ Use DHCP to obtain Virtual IP for this Connection

□ Require Global Security Client for this Connection

Client Initial Provisioning

☑ Use Default Key for Simple Client Provisioning

Ready

Configuring Users with Authenticated Access to the GroupVPN Policy

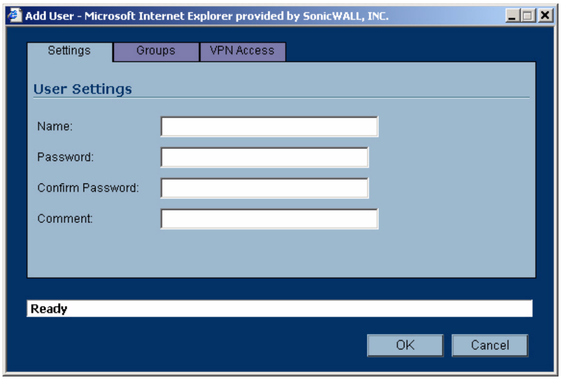
You can configure authenticated VPN access for individual users or configure VPN access for a group using the SonicWALL security appliance's local user's database or using an external RADIUS server.

Note: *For more information on configuring the SonicWALL security appliance to use RADIUS for authenticating VPN clients, refer to the SonicOS Enhanced Administrator's Guide.*

To add an individual user to the SonicWALL security appliance's local user database for VPN access:

1. In the management interface of your SonicWALL security appliance, click on **Users** in the left-navigation menu, and then click on **Local Users** under **Users**.
2. In the **Users > Local Users** page, click **Add User**.

3. In the **Add User** window:



- **Settings**: Enter the **Name** and **Password** of the user
- **Group**: Select the groups the user should belong to. The user automatically has any VPN access configured for the group.
- **VPN Access**: Select the networks, subnets, and IP addresses the user should have access to when connected via GroupVPN. For example, All WAN IP, WLAN Subnets, LAN Primary Subnets, and WLAN RemoteAccess Networks.

4. Click OK.

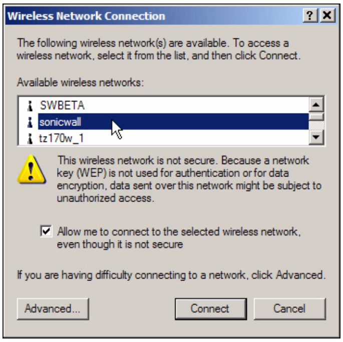
9 Connecting Wireless Clients to the SonicPoint

For wireless clients to connect to your WLAN zone, they need:

- A wireless network card installed and configured for the SonicPoint's SSID
- SonicWALL Global VPN Client (GVC) or SonicWALL Global Security Client (GSC) installed and configured for a secure wireless connection

Connecting to the SonicPoint Wireless Network

You connect to the wireless network according to the requirements of your client operating system. Your wireless client may automatically detect and display the SonicPoint's SSID in a list of available wireless networks or you may need to manually configure your wireless card with the SonicPoint's SSID.



The following wireless network(s) are available. To access a wireless network, select it from the list, and then click Connect.

Available wireless networks:

- SWBETA
- sonicwall
- tz170w_1

This wireless network is not secure. Because a network key (WEP) is not used for authentication or for data encryption, data sent over this network might be subject to unauthorized access.

☑ Allow me to connect to the selected wireless network, even though it is not secure

If you are having difficulty connecting to a network, click Advanced.

Establishing Secure Wireless Connections

Note: *If you disabled WiFiSec, you do not need to follow this procedure. See Procedure 8, **"Enabling Secure Wireless Connections" on page 14** for instructions on enabling and disabling WiFiSec.*

For a wireless client to securely connect to the SonicPoint using WiFiSec, the SonicWALL GVC or SonicWALL GSC must be installed and configured. Installing and configuring SonicWALL GVC involves the following procedures:

- Installing the SonicWALL GVC or SonicWALL GSC Using the **Setup Wizard**
- Creating an Office Gateway Connection Profile Using the **New Connection Wizard**
- Establishing a WiFiSec VPN Connection Via the SonicPoint Using the **WLAN GroupVPN** Policy

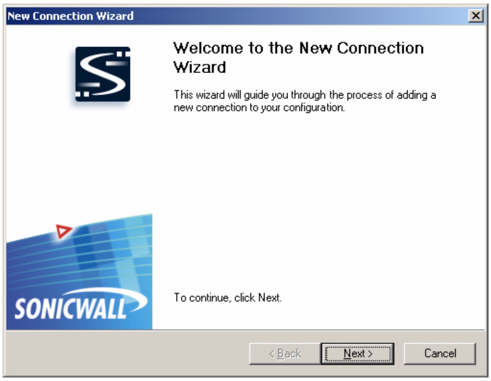
Installing the SonicWALL GVC or SonicWALL GSC using the **Setup Wizard**

If necessary, install the SonicWALL GVC. It is available either as the standalone SonicWALL GVC or as the SonicWALL GVC component of SonicWALL GSC. Follow the instructions in the **Setup Wizard** to install SonicWALL GVC or SonicWALL GSC.

Note: *For complete product documentation on SonicWALL GVC or SonicWALL GSC, visit the SonicWALL Web site at <http://www.sonicwall.com/support/documentation.html>.*

To create an Office Gateway connection profile using the **New Connection Wizard**:

1. In your Windows Start Menu, Choose **Start > Programs > SonicWALL Global VPN Client**. The first time you open SonicWALL GVC, the **New Connection Wizard** automatically launches.



Welcome to the New Connection Wizard

This wizard will guide you through the process of adding a new connection to your configuration.

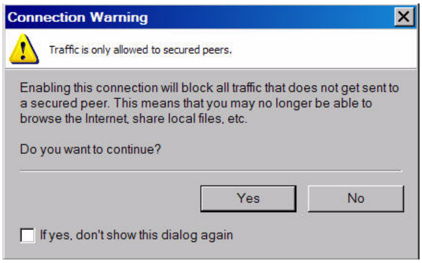
To continue, click Next.

   If the **New Connection Wizard** does not display, click the **New Connection Wizard** icon on the far left side of the toolbar to launch it. Click **Next**.

2. In the **Choose Scenario** page, select **Office Gateway**. Click **Next**.
3. In the **Completing the New Connection Wizard** page select any of the following options:
   - Select **Create a desktop shortcut to this connection**, if you want to create a shortcut icon on your desktop for this VPN connection.
   - Select **Enable this connection when the program is launched**, if you want to automatically establish this VPN connection when you launch the SonicWALL Global VPN Client.
4. Click **Finish.** The new VPN connection policy appears in the **SonicWALL Global VPN Client** window.

To establish a WiFiSec VPN connection through the SonicPoint using the **WLAN GroupVPN** policy:

1. In the **SonicWALL Global VPN Client** window, double-click the **Office Gateway** profile. The **Connection Warning** dialog box is displayed, which informs you that all traffic that is not going to the secured VPN gateway will be blocked.



Connection Warning

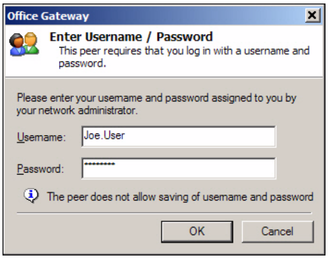
Traffic is only allowed to secured peers.

Enabling this connection will block all traffic that does not get sent to a secured peer. This means that you may no longer be able to browse the Internet, share local files, etc.

Do you want to continue?

□ If yes, don't show this dialog again

2. Click **Yes** to continue.
3. In the **Enter Username/Password** dialog box, enter the authentication credentials for the user configured on the SonicWALL security appliance's local user database for access to the **WLAN GroupVPN**.



Office Gateway

Enter Username / Password

This peer requires that you log in with a username and password.

Please enter your username and password assigned to you by your network administrator.

Username: Joe.User

Password: ********

The peer does not allow saving of username and password

4. Click OK. You now have secure wireless access to all the networks, subnets, and addresses you assigned the user access.

SonicPoint Radio Frequencies and Bands

The SonicPoint supports:

Radio Frequency Bands

802.11a	802.11b/g
5.15-5.35 GHz	2.412 - 2.462 GHz (US, Canada, Taiwan)
5.25-5.35 GHz (Taiwan)	2.412 - 2.472 GHz (Europe ETSI)
5.725-5.825 GHz	2.412 - 2.484 GHz (Japan)
5.725-5.825 GHz (Taiwan)	
5.725-5.825 GHz no turbo (Korea)	

Radio Operating Channels

802.11a (SonicPoint only)	802.11b/g
US & Canada: 12 CHs (FCC)	US & Canada: 1 CH~11CH (FCC)
Europe: 19 CHs	Europe: 1 CH~13CH (ETSI)
Japan: 4 CHs	Japan: 14 CHs
Singapore: 12 CHs	
Taiwan: 7 CHs	

Dynamic Frequency Selection (DFS) is supported.

Cable Connections

All Ethernet and RS232 (Console) cables are designed for intra-building connection to other equipment. Do not connect these ports directly to communication wiring or other wiring that exits the building where the SonicWALL is located.

Power Supply Information

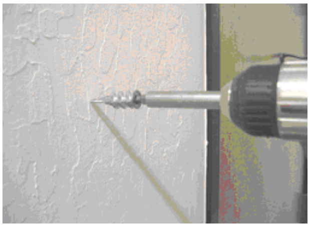
If the power supply is missing from your SonicWALL product package, please contact SonicWALL Technical Support at 408-752-7819 for a replacement. This product should only be used with a UL listed power supply marked “Class 2” or “LPS”, with an output rated 12 VDC, minimum 1.66 A.

Mounting the SonicPoint

Wall Mounting the SonicPoint

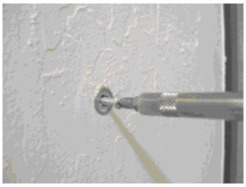
Follow the instructions below to mount the SonicPoint on the wall.

1. Using the mounting plate as a template, mark the places to insert the mounting anchors.
2. Using a #2 Phillips screw driver, press the tip of the anchor into the marked places on the hollow wall.

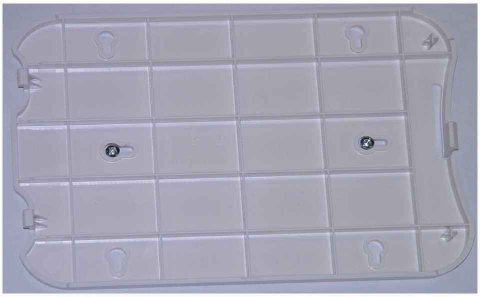


3. Turn the screwdriver clockwise until the anchor is flush with the wall. Repeat for the second anchor.

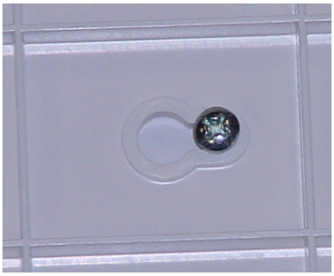
4. Insert a #6 x 11/4" pan head Phillips self-tapping screw into each anchor leaving a gap for the mounting plate.



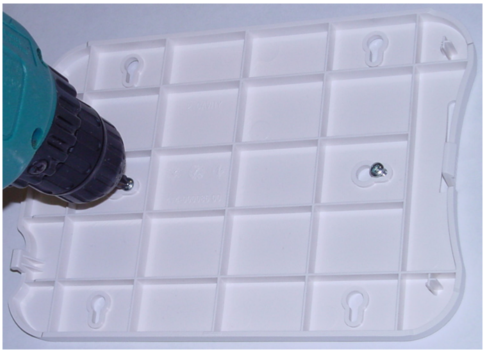
5. Hang the mounting plate on the screws. Use the middle row of mounting holes.



6. Slide the plate down to the narrowest part of the keyhole so that the mounting plate rests on the screws.



7. Tighten the mounting screws to secure the mounting plate.

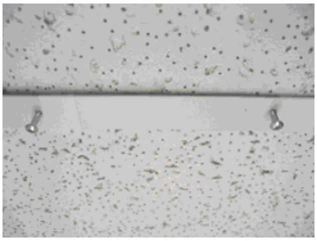


8. Snap the SonicPoint onto the mounting plate.

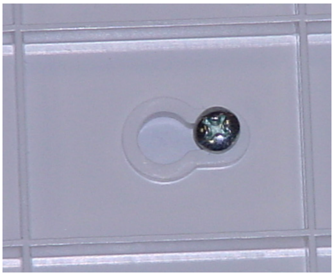
Mounting Models the SonicPoint on the Ceiling

1. Locate a metal support to hang the SonicPoint.
2. Using the mounting plate as a template, mark the places to insert the mounting anchors.
3. Drill two holes for #6 x 1-1/4” screws in the marked location.

4. Install the #6 x 1-1/4” self-tapping screws leaving a slight gap for the mounting plate.



5. Hang the mounting plate on the screws.
6. Slide the plate down to the narrowest part of the keyhole so that the mounting plate rests on the screws.



7. Tighten the mounting screws to secure the mounting plate.

8. Snap the SonicPoint onto the mounting plate.

Copyright Notice

Trademarks

Notes

SonicWALL,Inc.
1143 Borregas Avenue T: 408.745.9600 www.sonicwall.com
Sunnyvale,CA 94089-1306 F: 408.745.9300

P/N 232-000799-00
Rev B 05/05