

SonicPoint-Ne / SonicPoint-Ni Getting Started Guide

**SonicWALL® ECLASS**

**SONICWALL®**

DYNAMIC SECURITY FOR THE GLOBAL NETWORK™

# SonicWALL SonicPoint-Ne / SonicPoint-Ni

## Getting Started Guide

This *Getting Started Guide* provides instructions for basic installation and configuration of the SonicWALL SonicPoint-Ne / SonicPoint-Ni wireless appliances in single-unit or distributed wireless deployments.

### Setup

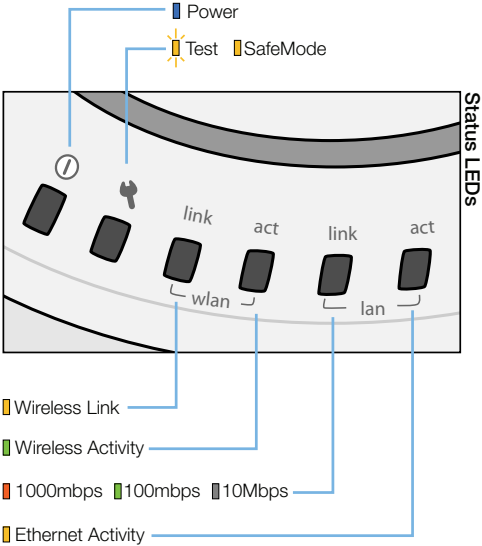
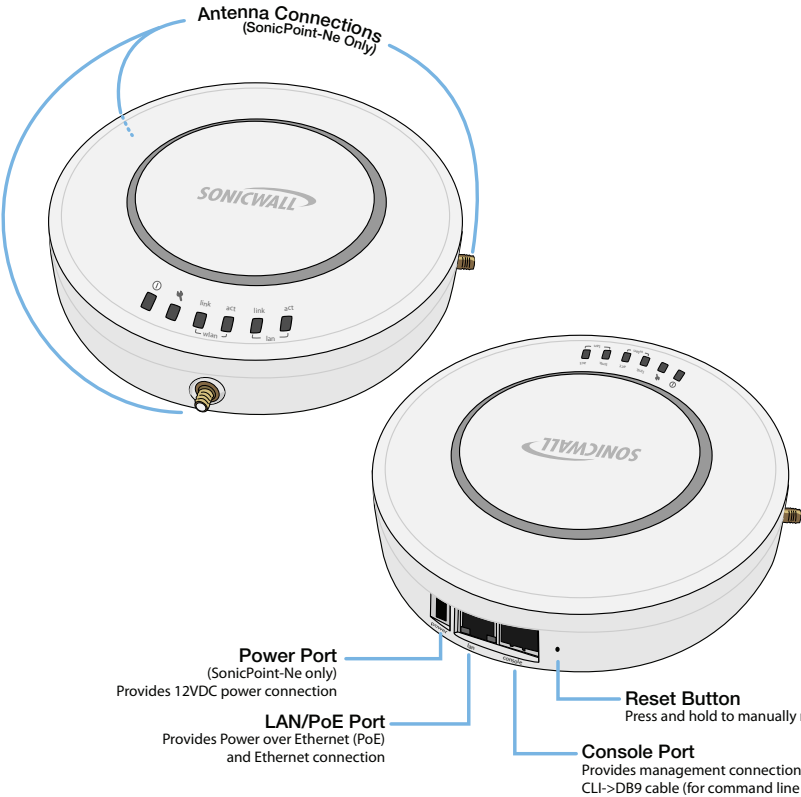
Step	Procedure	Est. Time
1	<a href="#">Before You Begin</a> - page 3	5
2	<a href="#">Introduction to Secure Wireless</a> - page 7	10
3	<a href="#">Registering Your Appliance</a> - page 13	10
4	<a href="#">Configuring Your UTM Appliance for Wireless</a> - page 17	15
5	<a href="#">Setting Up Your SonicPoint</a> - page 23	20

### Additional Configuration and Information

[Support and Training Options](#) - page 31

[Product Safety and Regulatory Information](#) - page 37

# SonicPoint Top Panel / Status LEDs



In this Section:

This section provides a basic checklist of materials and information you will need before you begin.

- [\*Check Package Contents\*](#) - page 4
- [\*What You Need to Begin\*](#) - page 5

## Check Package Contents

Before continuing, ensure that your SonicPoint package contains the following materials:

SonicPoint-Ne Appliance Checklist	SonicPoint-Ni Appliance Checklist
<ul style="list-style-type: none"><li><input type="checkbox"/> This Getting Started Guide Document</li><li><input type="checkbox"/> SonicPoint-Ne Appliance</li><li><input type="checkbox"/> Mounting Kit (Ceiling Braces, Anchor and Screw Kit)</li><li><input type="checkbox"/> Front LED/Logo Cover Plate</li><li><input type="checkbox"/> Antennas (3)</li><li><input type="checkbox"/> Power Adaptor<sup>a</sup></li></ul>	<ul style="list-style-type: none"><li><input type="checkbox"/> This Getting Started Guide Document</li><li><input type="checkbox"/> SonicPoint-Ni Appliance</li><li><input type="checkbox"/> Mounting Kit (Ceiling Braces, Anchor and Screw Kit)</li><li><input type="checkbox"/> Front LED/Logo Cover Plate</li></ul>

*a. The included power cord is intended for use in North America only.*

### Any Items Missing?

If any of the items corresponding to your product are missing from the package, **please contact SonicWALL support.**

A listing of the most current support documents are available online at:

[<http://www.sonicwall.com/us/support.html>](http://www.sonicwall.com/us/support.html)

## What You Need to Begin

The SonicWALL SonicPoint-Ne/Ni security appliances are centrally managed by SonicWALL NSA E-Class appliances. For more information on deploying this SonicPoint with SonicWALL NSA series and TZ series platforms, contact your local SonicWALL sales representative for the supported SonicOS releases. SonicPoints receive auto-firmware updates from the central gateway SonicWALL, this device supports SonicOS 5.6.0.3 or higher releases.

In addition to the above SonicOS firmware and hardware requirements, ensure that your network deployment includes:

- An 802.3af compliant PoE injector or PoE-capable switch (*optional when using the SonicPoint-Ne*)
- An active Internet connection
- A configured interface on the SonicWALL security appliance set to a zone type of “wireless”
- A location selected for placement of your SonicPoint such as a wall or ceiling
- Clients capable of 802.11n wireless communications<sup>1</sup>

---

1. Although clients with 802.11a/b/g hardware are supported, the presence of these legacy clients within range of your network may affect the connection speed of your 802.11n clients.



## In this Section:

This section contains excerpts from the *SonicWALL Secure Wireless Network Integrated Solutions Guide*. The content is meant to provide a brief introduction to Radio Frequency (RF) technology as it pertains to different deployment scenarios.

- [Wireless RF Introduction](#) - page 8
- [Placing Access Points](#) - page 10
- [SonicWALL Wireless Firewalling](#) - page 12

## Wireless RF Introduction

There are currently four widely adopted standards for 802.11 wireless network types: a, b, g, and n. Although 802.11n is the newest and highest capacity standard, each of the four standards has its own strengths and weaknesses. This section provides overviews of these standards.

The following section provides a brief overview of RF technologies:

- [Frequency Bands and Channels](#) - page 8
- [802.11 Comparison Chart](#) - page 8
- [Radio Frequency Barriers](#) - page 9
- [RF Interference](#) - page 9

### Frequency Bands and Channels

To allow multiple separate wireless networks in a shared and confined space, the RF medium is divided into channels. For devices in the 5GHz range (802.11a), this means the possibility of up to 23 discrete channels. For devices using the 2.4GHz range (802.11b, 802.11g), the wireless space is limited to a maximum of 14 *overlapping* channels. As a result of these overlapping channels, 2.4GHz technology provides only a total of three discrete channels.

The newer 802.11n technology does not fit into either of these categories, as it is capable of using both 2.4GHz and 5GHz, but is limited to 14 overlapping channels for backward compatibility.

## 802.11 Comparison Chart

The following table compares signal characteristics as they apply to the current 802.11 standards:

	802.11a	802.11b	802.11g	802.11n
# of Channels in USA	23	11	11	11
# of Channels in EU	23	13	13	13
# of Channels in Japan	15	14	14	14
Frequency Band	5GHz	2.4GHz	2.4GHz	2.4/5GHz
Max. Data Rate	54Mbps	11Mbps	54Mbps	150Mbps 300Mbps <sup>a</sup>
Radius (Range)	90ft/25m	120ft/ 35m	120ft/ 35m	300ft/90m

a. Full 300Mbps throughput is possible only in environments free from 2.4Ghz interference.



**Note:** Although 802.11b/g/n standards provide between 11 and 14 channels, only 3 of those channels are fully discrete (non-overlapping) channels.

For more information on this topic, refer to the *SonicWALL Secure Wireless Networking Integrated Solutions Guide*.

## Radio Frequency Barriers

Determining the location of RF barriers can be a painful part of the placement process, but keep in mind that they can be used beneficially in an attempt to block signals where you do not want coverage.

The following tables list some common RF barrier types:

Barrier Type	RF Signal Blocking
Open air	Very Low
Glass, drywall, cube partitions	Low
Stone floors and walls (brick/marble/granite)	Medium
Concrete, security glass, stacked books/paper	High
Metal, metal mesh (chicken wire), re-enforced concrete, water	Very High
Faraday cage	Extremely High

## RF Interference

RF interference from home, office, and medical equipment is a common source of frustration in wireless deployments from the smallest home office to the largest multi-building campus.

The following table lists several common sources of RF interference:

Interference Source	Possible RF Interference	Band(s) Affected
2.4GHz phones	Entire range (hundreds of feet)	802.11b/g/n
Bluetooth devices	Within 30 feet	802.11b/g/n
Microwave oven <sup>a</sup>	Within 10-20 feet	802.11b/g/n
Scientific and medical equipment	Short distance, varies	802.11b/g/n
Off-network access points	Entire range	All
RF reflective objects	Long-range wireless bridging	All

*a. Most newer model microwave ovens have sufficient shielding to negate possible RF interference.*

## Placing Access Points

Physical placement of an access point has a measurable effect on who can and cannot access your wireless signal. The following sections provide an overview of wireless access point placement, signal strength, and signal direction in common wireless deployment situations:

- [Making Hardware Decisions](#) - page 10
- [Solutions to RF Interference and Barriers](#) - page 11



---

**Tip:** For the latest SonicPoint wireless deployment information from **switching recommendations to site survey**, see the SonicWALL SonicPoint Deployment Best Practices Guide at:  
<<http://www.sonicwall.com/us/support.html>>

---

## Making Hardware Decisions

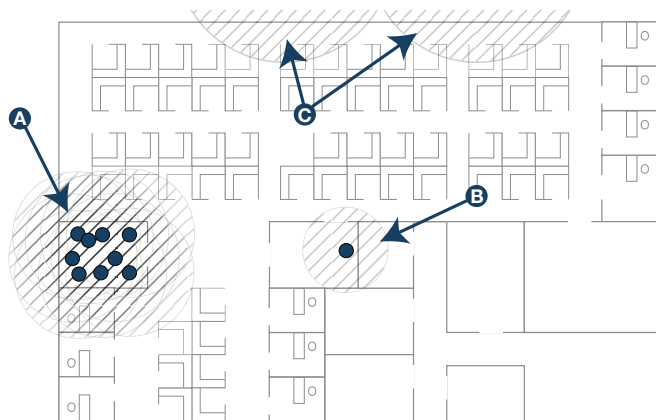
The first decision in hardware is the access point. While access point technology (802.11a/b/g/n) is one factor in determining your placement, based on distance served and bandwidth needed, taking note of other hardware-based factors is just as important.

Some of the more important hardware decisions include:

- **Number of access points versus user density** – If too many users are serviced by a single access point, maximum transfer rates are reached and that 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 to and how are you securing that cable. Is your PoE switch able to power all access points?
- **Hubs / Switches / UTM** – Your wireless deployment has to tie back into your UTM appliance and LAN resources at some point. What speed is needed for your Ethernet connection to accommodate the number of access points you are installing? Also consider where your key networking devices are deployed and how they will connect efficiently with your wireless appliances.
- **Upgrade your Ethernet connections for 802.11n** – In most cases, 802.11n wireless hardware requires more bandwidth than a single (or even dual) 10/100 Ethernet connection can handle. Gigabit Ethernet connectivity between the WLAN and the LAN is required to take full advantage of 802.11n speed.
- **Power up that PoE for 802.11n** – Part of your wireless network planning should include verifying that your PoE equipment is 802.3af compliant, and that a full 15 watts of power can be supplied to each SonicPoint.

## Solutions to RF Interference and Barriers

These days, finding an environment with no RF interference or noise is nearly impossible. Only if you are setting up an office in a secluded redwood grove can you count on RF interference to be a non-issue. Even then, the redwood trees might just be among those fitted with high-gain cellular antennas, an all-too-common occurrence today. Regardless, you should expect to deal with some level of signal interference in your deployment.



### Location A – Rogue access points or wireless test lab

- **Problem** – Wireless product test labs and other (non-malicious) rogue access points are problems in many Wi-Fi deployments.
- **Solution** – Either eliminate all rogue access points, or force their owners to use a set channel that does not overlap with your distributed wireless solution.

### Location B – Spectrum noise for 2.4 GHz and 5 GHz

- **Problem** – Your phone system is partially wireless and uses the 2.4GHz spectrum.
- **Solution** – Give VoIP a try. VoIP will work in tandem *with* your wireless network, instead of against it. For more on SonicWALL VoIP implementation and capabilities, refer to the *Configuring VoIP* SonicOS feature module available at: <http://www.sonicwall.com/us/support.html>

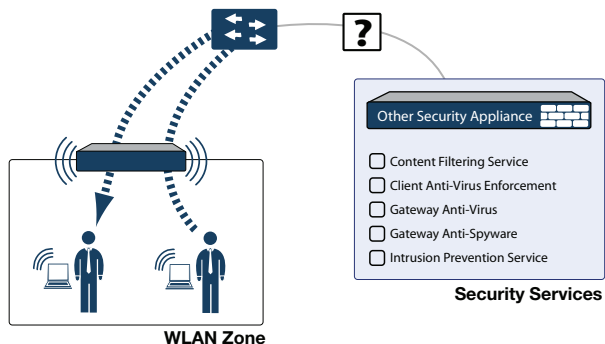
### Location C – Off-network access points

- **Problem** – Your neighbors need wireless, too! Unfortunately, only a few sheets of drywall separate you.
- **Solution** – Overpowering your neighbors with high-gain antennas is an option, but not a particularly neighborly one. Instead, you could simply use a different channel for wireless access points bordering this wall and ensure that your neighbors do the same. Performance in some dual-channel wireless devices may take a hit, but it is better than dropped connections—or unhappy neighbors.

## SonicWALL Wireless Firewalling

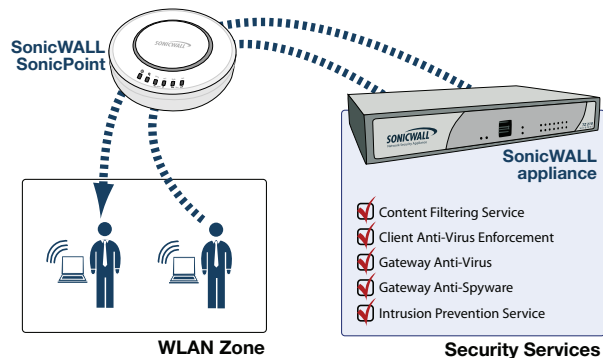
When a wireless device uses an access point to communicate with a device on another subnet or on a completely different network, traffic between the devices is forced to traverse the network gateway. This traversal enables Unified Threat Management (UTM) services to be enforced at the gateway.

Standard practice for wireless firewalling (where one wireless client is communicating with another) bypasses many of the critical UTM security services. The illustration below shows the standard practice for wireless firewalling.



Many security products on the market share this potential vulnerability when two users connected by a common hub or wireless access point wish to exchange data.

SonicWALL addresses this security shortcoming by managing the SonicPoint access points from the UTM appliance. This allows complete control of the wireless space, including zone enforcement of security services and complete firewalling capabilities, as shown in the illustration below.



In this Section:

This section provides instructions for registering your SonicWALL SonicPoint appliance.

- [Creating a MySonicWALL Account](#) - page 14
- [Registering and Licensing Your Appliance on MySonicWALL](#) - page 14
- [Using SonicWALL UTM Security Services for Wireless Clients](#) - page 15



---

**Note:** *Registration is an important part of the setup process and is necessary to receive the full benefits of SonicWALL security services, firmware updates, and technical support.*

---

## Creating a MySonicWALL Account

A MySonicWALL account is required for product registration. If you already have an account, continue to the *Registering and Licensing Your Appliance on MySonicWALL* section.

To create a MySonicWALL account:

1. In your browser, navigate to [www.mysonicwall.com](http://www.mysonicwall.com).
2. In the login screen, click the *Not a registered user?* link.

3. Complete the Registration form and click **Register**.
4. Verify that the information is correct and click **Submit**.
5. In the screen confirming that your account was created, click **Continue**.

## Registering and Licensing Your Appliance on MySonicWALL

You must register your SonicWALL security appliance on MySonicWALL to enable full functionality.

To register your SonicPoint, perform the following tasks:

1. Login to your MySonicWALL account. If you do not have an account, you can create one at [www.mysonicwall.com](http://www.mysonicwall.com).
2. Enter the serial number of your product in the **REGISTER A PRODUCT** field and click the **Next** button.
3. Type a friendly name for the appliance, select the **Product Group** if any, type the authentication code into the appropriate text boxes, and then click **Register**.
4. On the Product Survey page, fill in the requested information and then click **Continue**.
5. To pair your SonicPoint with a SonicWALL UTM appliance, navigate to the **Service Management** page by clicking on the device you wish to pair with your SonicPoint.
6. Scroll to the **Associated Products** section and click the *SonicWALL SonicPoint* link to associate your SonicPoint with the appliance.

## Using SonicWALL UTM Security Services for Wireless Clients

Any security services you purchased for your SonicWALL UTM appliance can also be applied to wireless clients. Simply enable the security services on the WLAN zone or on a custom wireless zone, and your wireless traffic will be protected along with your wired traffic.

**If you have not yet purchased a security service subscription** for your SonicWALL UTM appliance, please speak with a sales representative or visit [www.mysonicwall.com](http://www.mysonicwall.com) to register for free trials.

- To try a Free Trial of a service, click **Try** in the Service Management page.
- To purchase a product or service, click **Buy Now** in the Service Management page.

Status - Gateway AV/Anti-Spyware/Intrusion Prevention

Product Name: My TZ 210  
Serial Number: 0017C5288E1C  
Activation Status: Enabled  
Expiration Date: 10 Dec 2008

BACK

Renew Service

Enter an Activation Key and Submit or Click the Shopping cart to buy Activation keys online. Select "Upgrade" to increase licenses and "Renew" to extend current expiration date.

Multiple activations can be performed by adding keys for the same service separated by a comma.

Activation Key:

BUY SUBMIT

If you recently purchased security services, you will receive an activation key. This key is emailed to you after online purchases, or is on the front of the certificate that was included with your purchase.

To activate existing licenses:

1. Log into [mysonicwall.com](http://mysonicwall.com) and navigate to the **My Products** page.
2. Select the registered product you want to manage.
3. Locate the product on the Service Management page and click **Enter Key** in that row.

SERVICE BUNDLES			
Service Name	Info	Status	Options
Client/Server Anti-Virus Suite	30	-	<a href="#">Enter Key</a>
Comprehensive Gateway Security Suite	30	-	<a href="#">Enter Key</a>

4. In the Activate Service page, type or paste your key into the **Activation Key** field and then click **Submit**.

When activation is complete, MySonicWALL displays an activation screen with service status and expiration information.

Gateway AV/Anti-Spyware/Intrusion Prevention 30 Expiry: 11 Jun 2009

You have successfully registered your SonicWALL appliance, and now you need to enable UTM security services on the SonicWALL appliance itself. SonicWALL UTM security services are not enabled by default.



---

# Configuring Your UTM Appliance for Wireless

4

In this Section:

This section provides instructions for configuring the SonicWALL UTM appliance to connect with your SonicWALL SonicPoint.

- [An Introduction to Zones and Interfaces](#) - page 18
- [Configuring Wireless Access](#) - page 18

## An Introduction to Zones and Interfaces

Zones split a network infrastructure into logical areas, each with its own set of usage rules, security services, and policies. Most networks include multiple definitions for zones, including those for trusted, untrusted, public, encrypted, and wireless traffic.

Some basic (default) zone types include:

**WAN** - Untrusted resources outside your local network

**LAN** - Trusted local network resources

**WLAN** - Local wireless network resources originating from SonicWALL wireless enabled appliances

**DMZ** - Local network assets that must be accessible from the WAN zone (such as Web and FTP servers)

**VPN** - Trusted endpoints in an otherwise untrusted zone (such as the WAN)

The security features and settings configured for the zones are enforced by binding a zone to one or more physical interfaces (such as, X0, X1, or X2) on the SonicWALL UTM appliance.

The X1 and X0 interfaces are preconfigured as WAN and LAN respectively. The remaining ports (X2-X6) are also LAN ports by default. However, these ports can be configured to meet the needs of your network, either by using basic zone types (WAN, LAN, WLAN, DMZ, VPN) or configuring a custom zone type to fit your network requirements (for example: Gaming Console Zone, Wireless Printer Zone, Wireless Ticket Scanner Zone).

## Configuring Wireless Access

This section describes how to configure SonicPoints with a SonicWALL UTM appliance.

SonicWALL SonicPoints are wireless access points specially engineered to work with SonicWALL UTM appliances. Before you can manage SonicPoints in the management interface, perform the following steps:

- [Configuring Provisioning Profiles](#) - page 19
- [Configuring a Wireless Zone](#) - page 21
- [Configuring the Network Interface](#) - page 22

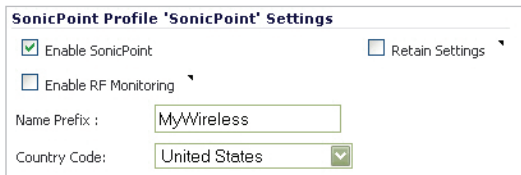
## Configuring Provisioning Profiles

SonicPoint Profile defines settings that can be configured on a SonicPoint, such as radio SSIDs, and channels of operation.

These profiles make it easy to apply basic settings to a wireless zone, especially when that zone contains multiple SonicPoints. When a SonicPoint is connected to a zone, it is automatically provisioned with the profile assigned to that zone. If a SonicPoint is connected to a zone that does not have a custom profile assigned to it, a default profile is used.

To add a new profile:

1. Navigate to the **SonicPoint > SonicPoints** page in the SonicOS interface.
2. Click **Add SonicPoint** below the list of SonicPoint provisioning profiles.
3. The Add/Edit SonicPoint Profile window displays.



SonicPoint Profile 'SonicPoint' Settings

☒ Enable SonicPoint ☐ Retain Settings

☐ Enable RF Monitoring

Name Prefix :

Country Code:

### Settings Tab

1. Select **Enable SonicPoint**.
2. Enter a **Name Prefix** to be used internally as the first part of the name for each SonicPoint provisioned.
3. Select the **Country Code** for the area of operation.

### 802.11n Radio Tab

1. Select **Enable Radio**.
2. Optionally, select a schedule for the radio to be enabled from the drop-down list. The most common work and weekend hour schedules are pre-populated for selection.
3. Select a **Radio Mode** to dictate the radio frequency band(s). The default setting is **2.4GHz 802.11n/g/b Mixed**.
4. Enter an **SSID**. This is the access point name that will appear in clients' lists of available wireless connections.
5. Select a **Primary Channel** and **Secondary Channel**. You may choose AutoChannel unless you have a reason to use or avoid specific channels.
6. Under **WEP/WPA Encryption**, select the **Authentication Type** for your wireless network. SonicWALL recommends using **WPA2** as the authentication type.
7. Fill in the fields specific to the authentication type that you selected. The remaining fields change depending on the selected authentication type.

8. Optionally, under **ACL Enforcement**, select **Enable MAC Filter List** to enforce Access Control by allowing or denying traffic from specific devices. Select a MAC address object group from the **Allow List** or **Deny List** to automatically allow or deny traffic to and from all devices with MAC addresses in the group. The Deny List is enforced before the Allow List.

**802.11n Radio Settings**

☒ Enable Radio Always on

Mode: 2.4GHz 802.11n/g/b Mixed

SSID: MyWireless

Radio Band: Auto

Primary Channel: Auto

Secondary Channel: Auto

☐ Enable Short Guard Interval

☐ Enable Aggregation

**Wireless Security**

Authentication Type: WPA2 - PSK

Cipher Type: AES

Group Key Interval (seconds): 86400

Password: mypassphrase12345

**ACL Enforcement** ☐ **Enable MAC Filter List**

Allow List: --Select an Address Object Group--

Deny List: --Select an Address Object Group--

## Advanced Tab

Configure the advanced radio settings for the 802.11n radio. For most 802.11n advanced options, the default settings give optimum performance. For a full description of the fields on this tab, see the *SonicOS Enhanced Administrator's Guide*.

**802.11n Advanced Radio Settings**

☐ Hide SSID in Beacon

Schedule IDS Scan: Disabled

Data Rate: Best

Transmit Power: Half (-3 dB)

Antenna Diversity: Best

Beacon Interval (milliseconds): 800

DTIM Interval: 1

Fragmentation Threshold (bytes): 2346

RTS Threshold (bytes): 2346

Maximum Client Associations: 32

Preamble Length: Long

Protection Mode: None

Protection Rate: 1 Mbps

Protection Type: CTS-only

☐ Enable Short Slot Time ☐ Allow Only 802.11g Clients to Connect

When you are finished, click **OK**.

## Configuring a Wireless Zone

You can configure a wireless zone on the **Network > Zones** page. Typically, you will configure the WLAN zone for use with SonicPoints.

To configure a standard WLAN zone:

1. On the **Network > Zones** page in the **WLAN** row, click the icon in the **Configure** column.
2. Click on the **General** tab.
3. Select the **Allow Interface Trust** setting to automate the creation of Access Rules to allow traffic to flow between the interfaces within the zone, regardless of which interfaces to which the zone is applied. For example, if the WLAN Zone has both the **X2** and **X3** interfaces assigned to it, selecting the **Allow Interface Trust** checkbox on the WLAN Zone creates the necessary Access Rules to allow hosts on these interfaces to communicate with each other.

The screenshot shows the 'General Settings' tab for a 'WLAN' zone. The 'Name' field is set to 'WLAN' and the 'Security Type' is set to 'Wireless'. Under the 'Allow Interface Trust' section, the checkbox is unchecked. Under the 'Enforce Content Filtering Service' section, the checkbox is unchecked and the 'CFS Policy' dropdown is set to an empty state. Under the 'Enable Client AV Enforcement Service' section, four checkboxes are checked: 'Enable Client AV Enforcement Service', 'Enable Gateway Anti-Virus Service', 'Enable IPS', and 'Enable Anti-Spyware Service'.

4. Select the checkboxes for the security services to enable on this zone. Typically, you would enable **Gateway Anti-Virus**, **IPS**, and **Anti-Spyware**. If your wireless clients are all running SonicWALL Client Anti-Virus, select **Enable Client AV Enforcement Service**.
5. Click on the **Wireless** Tab.
6. Select **Only allow traffic generated by a SonicPoint** to allow only traffic from SonicWALL SonicPoints to enter the WLAN Zone interface, providing maximum security.

The screenshot shows the 'Wireless Settings' and 'SonicPoint Settings' tabs. In the 'Wireless Settings' section, the 'Only allow traffic generated by a SonicPoint' checkbox is checked. The 'SSL-VPN Enforcement' checkbox is unchecked, with 'SSL-VPN server' and 'SSL-VPN service' dropdowns set to '-Select an address object-' and '-Select a service-' respectively. The 'WiFiSec Enforcement' checkbox is unchecked, with the 'WiFiSec Exception Service' dropdown set to '-Select a service-'. The 'Require WiFiSec for Site-to-Site VPN Tunnel Traversal' and 'Trust WPA / WPA2 traffic as WiFiSec' checkboxes are also unchecked. In the 'SonicPoint Settings' section, the 'SonicPoint Provisioning Profile' dropdown is set to 'MyWireless'.

7. Optionally, click the **Guest Services** tab to configure guest Internet access solely, or in tandem with secured access. For information about configuring Guest Services, see the *SonicOS Enhanced Administrator's Guide*.
8. When finished, click **OK**.

## Configuring the Network Interface

Each SonicPoint or group of SonicPoints must be connected to a physical network interface that is configured for Wireless. SonicOS by default provides a standard wireless zone (WLAN), which can be applied to any available interface.

To configure a network interface using the standard wireless (WLAN) zone:

1. Navigate to the **Network > Interfaces** page and click the **Configure** button for the interface to which your SonicPoints will be connected.



2. Select **WLAN** for the **Zone** type.
3. Select **Static** for the **IP Assignment**.
4. Enter a static **IP Address** in the field. Any private IP is appropriate for this field, as long as it does not interfere with the IP address range of any of your other interfaces.
5. Enter a **Subnet Mask**. In our example 255.255.255.0 is an appropriate mask.
6. Optionally, choose a **SonicPoint Limit** for this interface. This option helps limit resources on port-by-port basis when using SonicPoints across multiple ports.
7. Optionally, choose to allow **Management** and **User Login** mechanisms if they make sense in your deployment. Remember that allowing login from a wireless zone can pose a security threat, especially if you or your users have not set strong passwords.

In this Section:


This section describes how to connect and configure physical aspects of the SonicPoint including cabling and mounting.

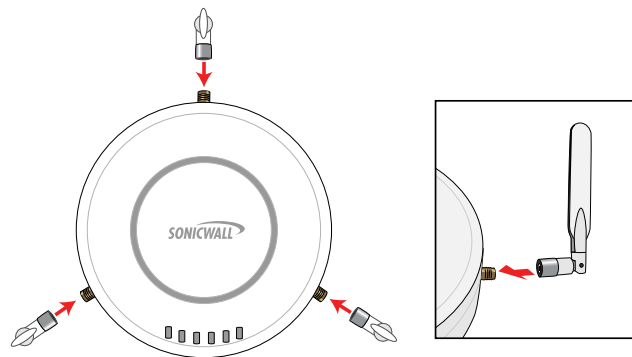
- *Installing Antennas (SonicPoint-Ne Only)* - page 24
- *Connecting Ethernet Cable* - page 24
- *Verifying Operation* - page 28
- *Verifying WAN (Internet) Connectivity* - page 28
- *Troubleshooting Tips* - page 29
- *Onboard Help System* - page 29

## Installing Antennas (SonicPoint-Ne Only)

To install the SonicPoint-Ne included antennas:

1. Remove the antennas from the bag and place one on each connector.
2. Carefully finger-tighten the fittings.
3. Adjust the antennas for optimal reception.

 **Note:** For optimal wireless coverage in most cases, the SonicPoint-Ne antennas should be oriented vertically.



The circular design of the SonicPoint aides in creating a strong tri-directional wireless signal pattern. In most cases, leaving the antennas straight up (as indicated in the illustration) will provide the best overall coverage.



**Note:** The SonicPoint-Ne 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 region before using other antennas.

## Connecting Ethernet Cable

The illustration on the following page depicts the SonicPoint within a typical network deployment.

### Ethernet Cabling: SonicPoint-Ne vs SonicPoint-Ni

While the SonicPoint-Ne may be powered with either the included external power adaptor or through Power over Ethernet (PoE), **the SonicPoint-Ni must be powered using Power over Ethernet (PoE).**

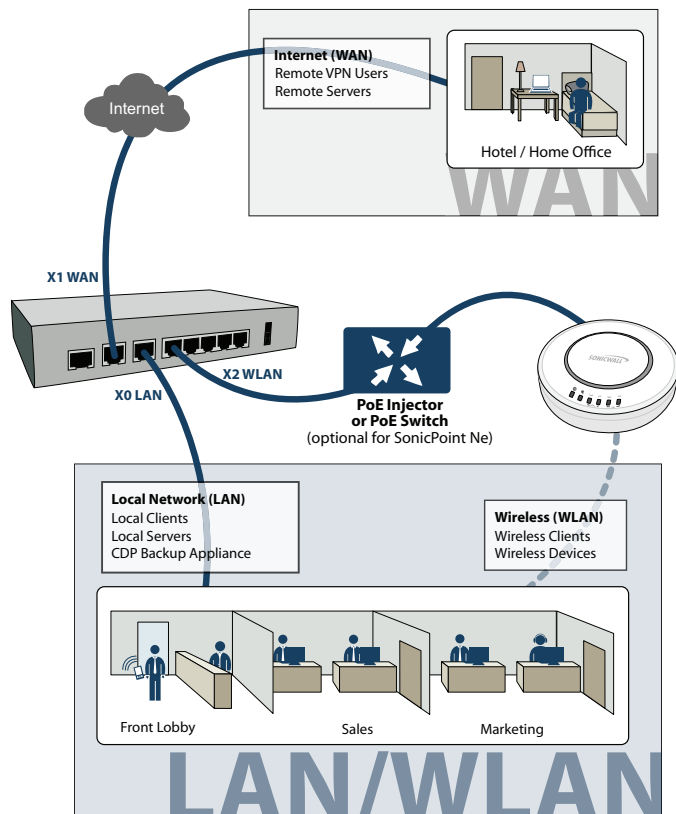
Both SonicPoint appliances should be cabled with CAT5, CAT5e, or CAT6 Ethernet cabling. In addition, the SonicPoint-Ni will not function unless the Ethernet connection to its LAN port is powered either by using the SonicWALL PoE line injector (sold separately), or by using a third-party 802.3af compliant PoE powered switch. For more information on the SonicWALL PoE injector, visit:

[http://www.sonicwall.com/us/products\\_solutions.html](http://www.sonicwall.com/us/products_solutions.html)

## Connecting the PoE Cable

If your deployment uses a SonicWALL PoE injector, read and comply with instructions provided with the PoE first, then complete the following steps:

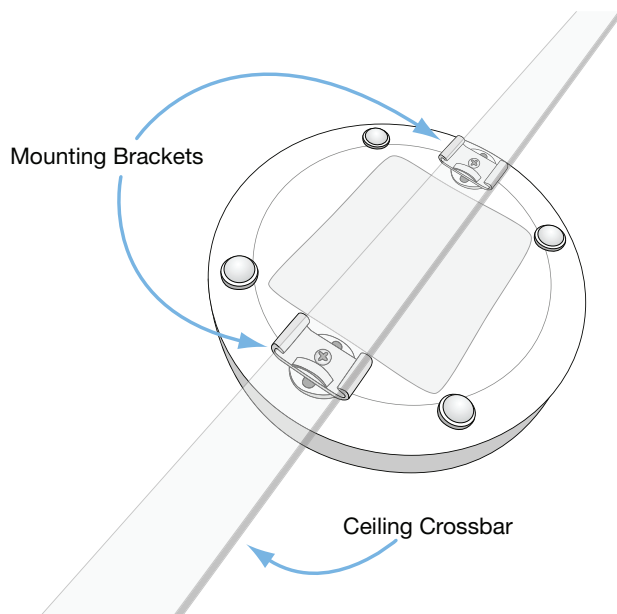
1. Plug the power cord of the SonicWALL PoE injector into the power outlet.
2. Using Ethernet cable (not included), connect the **Data in** port on the SonicWALL PoE Injector to the **WLAN** zone interface that you created earlier.
3. Using Ethernet cable, connect the **Data and Power out** port on the SonicWALL PoE injector to the **LAN** port on the back of your SonicPoint.
4. Wait for the **link** LED to illuminate. This indicates an active connection. It takes approximately one minute for the SonicWALL security appliance to auto-provision.



## Mounting Using Ceiling Brackets

To mount the SonicPoint to a crossbar between ceiling panels using included brackets:

1. Using the 3/8" screws, screw in the brackets to the underside of the SonicPoint, making sure both brackets are parallel.
2. (Optional) Attach the front LED/logo cover plate to the top of the SonicPoint and if necessary, rotate it to the desired position (See *Mounting Using Anchor Screws* section, on page 27 for illustration).
3. Supporting the SonicPoint in one hand, clip the edge of each bracket over the edge of the ceiling crossbar. Make sure the SonicPoint is securely attached to the crossbar before releasing the device.

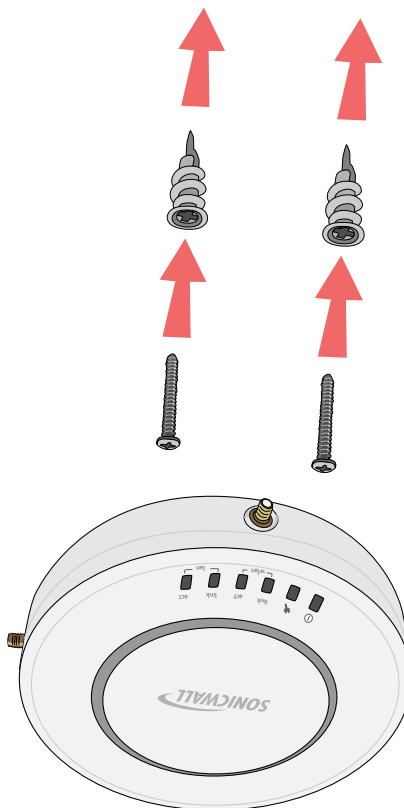


## Mounting Using Anchor Screws

To mount the SonicPoint using included anchor screws:

1. On the mounting surface, mark the location to make two screw holes. The marks should be horizontally parallel to each other.
2. Drill the holes to accommodate the metal anchor screws.
3. Screw the anchor screws into the holes to their full depth.
4. Insert the 5/8" screws into the anchors, and screw them in deep enough to leave minimal space between the screw heads and the wall surface.
5. (Optional) Attach the front LED/logo cover plate to the top of the SonicPoint and if necessary, rotate it to the desired position.
6. Supporting the SonicPoint in your hands, securely fit the underside slots of the SonicPoint onto the screw heads.

See also, [Product Safety and Regulatory Information](#) - page 37



## Verifying Operation

To verify that the SonicPoint is provisioned and operational, navigate to the **SonicPoint > SonicPoints** page in the SonicOS management interface. The SonicPoint displays an “operational” status in the **SonicPoint** table:

SonicPoint /

### SonicPoints

View Style:

Items 1 to 2 (of 2)

#### SonicPointN Provisioning Profiles

#	Name Prefix	Applied Zone	802.11n Radio	802.11n Channel	Configure
1	MySonicPoint-N	MyWirelessZone	SSID: MySonicPoint-N Mode: 2.4GHz 802.11n/g/b Mixed	Band: Auto Channel: AutoChannel	<input type="button" value="Configure"/> <input type="button" value="Delete"/>
2	SonicPointN1	WLAN	SSID: sonicwall-604C Mode: 2.4GHz 802.11n/g/b Mixed	Band: Auto Channel: AutoChannel	<input type="button" value="Configure"/> <input type="button" value="Delete"/>

#### SonicPoints

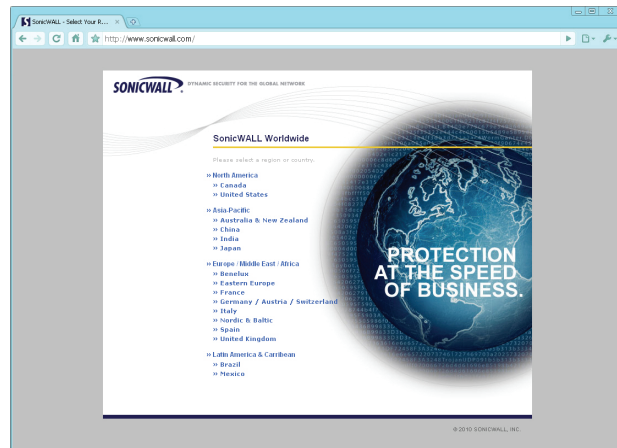
Items 1 to 1 (of 1)

#	Name	Interface	Network Settings	Status	802.11n Radio	802.11n Channel	Enable	Configure
1	SonicPointN2ef3ae	X3 (MyWirelessZone)	IP: 10.10.40.253 MAC: 00:17:C5:2e:53:ae	Operational	SSID: MySonicPoint-N Mode: 2.4GHz 802.11n/g/b Mixed	Band: Auto Channel: AutoChannel Radio: Enabled (Active)	<input checked="" type="checkbox"/>	<input type="button" value="Configure"/> <input type="button" value="Delete"/>

## Verifying WAN (Internet) Connectivity

Complete the following steps to confirm your Internet connectivity:

1. Disconnect a client computer from any other network connections (LAN, 3G, and more).
2. Connect the client computer to the wireless access point by selecting the appropriate SSID.
3. Launch your Web browser.
4. Enter “http://www.sonicwall.com” in the address bar and press **Enter** on the keyboard. The SonicWALL website displays. If you are unable to browse to a website, see “Troubleshooting Tips” on page 29.



## Troubleshooting Tips

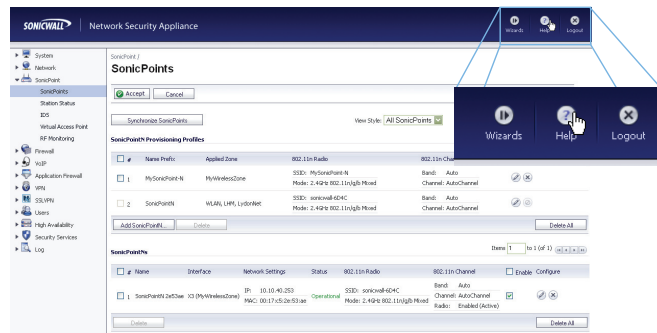
If the SonicPoint locates a peer SonicOS device, the two units perform an encrypted exchange and the profile assigned to the relevant wireless zone is used to automatically configure (provision) the newly added SonicPoint unit.

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

- **Make sure the SonicPoint is connected** to an interface that is configured as part of a Wireless zone. Either the default WLAN zone, or a custom zone with type set to “wireless” is required.
- **Click the Synchronize SonicPoints button.** This is located in the SonicOS management interface on the SonicPoint > SonicPoints page and forces the SonicWALL appliance, if connected, to download a new SonicPoint image from the SonicWALL back-end server.
- **Ensure that the SonicPoint is connected to a 802.3af compliant PoE powered Ethernet connection.** If using PoE to power your SonicPoint appliance, keep in mind that a PoE-capable switch or PoE injector is required.
- **Verify that your PoE switch/injector is rated** to deliver at least 15 watts of power to each port. Some older PoE devices do not provide sufficient power to properly run current generation 802.11n devices across multiple ports. Check with your PoE manufacturer for 802.3af support, or use a SonicWALL PoE injector.

## Onboard Help System

All SonicWALL network security appliances include an onboard help system with help topics that are relevant to each area of the management interface. To access SonicPoint help, click the Help icon in the upper right-hand corner of the SonicOS management interface while you are on a SonicPoint page.





In this Section:

This section provides overviews of customer support and training options for SonicWALL appliances.

- [\*Customer Support\*](#) - page 32
- [\*Knowledge Base\*](#) - page 32
- [\*User Forums\*](#) - page 33
- [\*Training\*](#) - page 34
- [\*Related Documentation\*](#) - page 35
- [\*SonicWALL Secure Wireless Network Integrated Solutions Guide\*](#) - page 36

## Customer Support

SonicWALL offers telephone, email and Web-based support to customers who have a valid Warranty or who purchased a Support Contract. Please review our Warranty Support Policy for product coverage. SonicWALL also offers a full range of consulting services to meet your needs, from our innovative implementation services to traditional statement of work-based services.

For further information, visit:

<http://www.sonicwall.com/us/support.html>

## Knowledge Base

The Knowledge Base allows users to search for SonicWALL documents based on the following types of search tools:

- Browse
- Search for keywords
- Full-text search

For further information, navigate to the **Support > Knowledge Portal** page at:

<http://www.mysonicwall.com/>

## User Forums

The SonicWALL User Forums are a resource that provide users the ability to communicate and discuss a variety of security and appliance subject matters. The following categories are available for users:

- Content Security Manager topics
- Continuous Data Protection topics
- Email Security topics
- Firewall topics
- Network Anti-Virus topics
- Security Services and Content Filtering topics
- SonicWALL GMS and Viewpoint topics
- SonicPoint and Wireless topics
- SSL VPN topics
- TZ 210 / Wireless WAN - 3G Capability topics
- VPN Client topics
- VPN site-to-site and interoperability topics

For further information, visit:  
<<https://forum.sonicwall.com/>>

Comprehensive Internet Security™

Welcome, amendoza@sonicwall.com.  
You last visited: 01-01-1970 at 12:00 AM  
Private Messages: Unread 0, Total 0.

SonicWALL Forums

User CP FAQ Calendar New Posts Search Quick Links KnowledgePortal Log Out

Forum	Last Post	Threads	Posts
<b>Firewalls</b> firewall related topics			
 <b>Network</b> Networking related topics.	 by thevnon Today 10:56 PM	4,538	19,051
 <b>VPN</b> VPN site to site and interoperability topics	 by mdominquez@marlinengineering.com Today 08:52 PM	1,973	6,800
 <b>VPN Client</b> VPN Client related topics	 by mdominquez@marlinengineering.com Today 02:44 PM	1,795	8,366
 <b>SonicPoint / Wireless</b> SonicPoint and wireless related topics	 by idement@shetm.com Today 08:26 PM	536	2,492
 <b>SGMS / Viewpoint</b> SGMS and Viewpoint related topics	 by indcenter Today 08:36 PM	756	2,650
 <b>Security Services</b> All IPS, Gateway Anti-Virus, Anti Spyware, Client AV, Application Firewall, and Content Filtering topics	 by Huegel_admin Today 09:41 AM	1,062	4,316
 <b>Network Anti-Virus</b> Network Anti-Virus related topics	 by templeiv@yahoo.com 07-20-2008 01:56 AM	225	1,028
 <b>TZ 190 / Wireless WAN</b> 3G Capability on the new TZ 190	 by jameswright72 Today 07:38 PM	113	461
 <b>Misc</b> Miscellaneous topics relating to SonicWALL firewalls	 by PAWELD Today 02:21 PM	1,112	4,047
<b>SonicWALL SSL-VPN</b> SSL-VPN Topics			
 <b>SSL-VPN 4000</b> SSL-VPN 4000 related topics	 by johnt@alaskabilingservices.com Today 08:02 PM	58	253

## Training

SonicWALL offers an extensive sales and technical training curriculum for Network Administrators, Security Experts, and SonicWALL Medallion Partners who need to enhance their knowledge and maximize their investment in SonicWALL Products and Security Applications. SonicWALL Training provides the following resources for its customers:

- E-Training
- Instructor-Led Training
- Custom Training
- Technical Certification
- Authorized Training Partners

For further information, visit:

[<http://training.sonicwall.com/>](http://training.sonicwall.com/)

WORLDWIDE | NORTH AMERICA

SEARCH

Log in to MySonicWALL

**SONICWALL** PROTECTION AT THE SPEED OF BUSINESS.™

HOME | PRODUCTS | SOLUTIONS | HOW TO BUY | SUPPORT | **TRAINING & EVENTS** | COMPANY | PARTNERS

GO BACK TO

## TRAINING & CERTIFICATION

### PRODUCT TRAINING

OVERVIEW | COURSES | CERTIFICATION | CLASS SCHEDULES | TRAINING PARTNERS

NEXT STEPS

CUSTOMER RESOURCES

- » Data Sheets
- » Phishing IQ Test
- » Podcasts
- » Product Demos
  - » Training Services Demo
- » Solution Briefs
- » Webinars
- » White Papers

PRODUCT SUPPORT

- » Online Self-Service
- » Product Training

STAY IN TOUCH

- » Contact Us
- » E-Mail Newsletters

SonicWALL offers an extensive technical training curriculum for Network Administrators, Security Experts and SonicWALL Medallion Partners who need to enhance their knowledge and maximize their investment in SonicWALL Products and Security Applications.

**COURSES & MATERIALS »**

SonicWALL provides instructor-led courses and technical eLearning modules designed to supply you with extensive technology foundations, in-depth SonicWALL-specific knowledge, in addition to online practice and an array of supplemental resources to enhance learning. [more info »](#)

**CERTIFICATION PROGRAMS »**

SonicWALL's Technical Certification programs give you confidence and improve your performance, and will immediately identify you as an expert in your field. Demonstrating your capabilities through certification will give you a key advantage whether you are a SonicWALL Medallion Partner, a Network Administrator or a Security Specialist. [more info »](#)

**CLASS SCHEDULES »**

SonicWALL instructor-led classroom training is designed to build upon the knowledge and concepts put forth in the Technical e\*Training courses. SonicWALL instructor-led classroom training is offered through SonicWALL Authorized Training Partners. If you are interested in attending SonicWALL instructor-led training, please contact a SonicWALL Authorized Training Partner. [more info »](#)

**AUTHORIZED TRAINING PARTNERS »**

SonicWALL Authorized Training Partners (ATPs) deliver a variety of educational programs to meet the many learning methods that each individual prefers. [more info »](#)

## Related Documentation

See the following related documents for more information:

- *SonicOS Enhanced Administrator's Guide*
- *SonicOS Enhanced Release Notes*
- *SonicOS Enhanced Feature Modules*
  - DPI-SSL
  - MAC-IP Anti-Spoof
  - Virtual Access Points
  - SSL VPN Remote Access
  - High Availability
  - Multiple Administrators
  - NAT Load Balancing
  - Packet Capture
  - Radio Frequency Monitoring
  - Single Sign-On
  - SSL Control
  - Secure Wireless Bridging
- *SonicWALL GMS Administrator's Guide*
- *SonicWALL GVC Administrator's Guide*
- *SonicWALL ViewPoint Administrator's Guide*
- *SonicWALL GAV Administrator's Guide*
- *SonicWALL IPS Administrator's Guide*
- *SonicWALL Anti-Spyware Administrator's Guide*
- *SonicWALL CFS Administrator's Guide*

For further information, visit:

[<http://www.sonicwall.com/us/support.html>](http://www.sonicwall.com/us/support.html)

WORLDWIDE | NORTH AMERICA SEARCH SITE MAP

SONICWALL PROTECTION AT THE SPEED OF BUSINESS.™

HOME PRODUCTS SOLUTIONS HOW TO BUY SUPPORT TRAINING & EVENTS COMPANY PARTNERS

GO BACK TO

PRODUCT REFERENCE GUIDES

SUPPORT RESOURCES

SELF-SERVE HELP

Downloads

- Firmware
- Setup Tool (PC)
- Setup Tool (Mac)
- Signatures

User Forums

Knowledge Portal

OPEN A SUPPORT CASE

Web

Telephone

Partner

REFERENCE LIBRARY

Product Guides

Technical Notes

FAQs

Release Notes

OTHER SERVICES

Support Services

Training & Certification

STAY IN TOUCH

Email Newsletters

Recently Published

#	Date	Description
1	13 Jan 2009	SonicOS Enhanced 5.1 Administrator's Guide for TZ 210 Series
2	12 Jan 2009	SonicWALL TZ 210 Series Getting Started Guide
3	12 Jan 2009	SonicOS 5.1 Dashboard Feature Module
4	22 Dec 2008	CDP 5.0 Agent Tool User's Guide
5	22 Dec 2008	CDP 5.0 Administrator's Guide

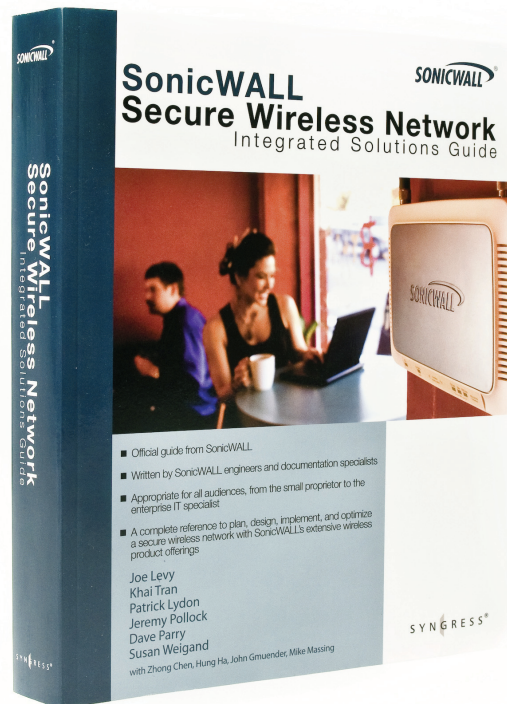
Guides for UTM / FIREWALL / VPN Products

#	Date	Description
1	10 Mar 2006	Configuring Manual Signature Updates for SonicOS 3.2 Enhanced
2	10 Mar 2006	Configuring Remotely Triggered Dial-Out in SonicOS 3.2 Enhanced
3	13 Nov 2006	Configuring Virtual Access Points for SonicOS 3.5 Enhanced
4	10 Mar 2006	Configuring VoIP for SonicOS Enhanced 3.2
5	10 Mar 2006	Configuring VoIP for SonicOS Standard 3.1
6	17 Oct 2006	Dynamic Address Objects: FQDN and MAC Address Objects in SonicOS Enhanced 3.5

## SonicWALL Secure Wireless Network Integrated Solutions Guide

Looking to go wireless? Have questions about what it takes to build a truly “secure” wireless network? Check out the SonicWALL Secure Wireless Network Integrated Solutions Guide. This book is the official guide to SonicWALL’s market-leading wireless networking and security devices.

This title is available in hardcopy at fine book retailers everywhere, or by ordering directly from Elsevier Publishing at: <http://www.elsevier.com>



In this Section:

This section provides regulatory, trademark, and copyright information.

- *Safety and Regulatory Information for the SonicWALL SonicPoint Wireless Appliance* - page 38
- *SonicWALL SonicPoint Wireless Appliance Sicherheit und gesetzliche Vorschriften* - page 39
- *FCC Part 15 Notice for the SonicWALL SonicPoint Wireless Appliance* - page 40
- *Industry Canada Notices* - page 41
- *Industrie Canada Notifications* - page 41
- *NCC Statement* - page 42
- *Copyright Notice* - page 45
- *Trademarks* - page 45

## Safety and Regulatory Information for the SonicWALL SonicPoint Wireless Appliance

Regulatory Model/Type	Product Names
APL21-06E APL21-083	SonicPoint-Ne SonicPoint-Ni

### Mounting the SonicWALL

- Mount in a location away from direct sunlight and sources of heat. A maximum ambient temperature of 104° F (40° C) is recommended.
- Route cables away from power lines, fluorescent lighting fixtures, and sources of noise such as radios, transmitters, and broadband amplifiers
- The included power cord is intended for use in North America only. For European Union (EU) customers, a power cord is not included.
- Ensure that no water or excessive moisture can enter the unit.
- Allow unrestricted airflow around the unit and through the vents on the side of the unit. A minimum of 1 inch (25.4mm) clearance is recommended.
- Consideration must be given to the connection of the equipment to the supply circuit and the effect of overloading the circuits has minimal impact on overcurrent protection and supply wiring. Appropriate consideration of equipment nameplate ratings must be used when addressing this concern.

### 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 for APL21-083

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 48 VDC, minimum 0.35 A, Tma: minimum 40 degrees C.

### Power Supply Information APL21-06E

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 1.5 A, Tma: minimum 40 degrees C.

If power is provided by the Ethernet cable plugged into the "lan" port, this is called "Power Over Ethernet" or "POE". The POE source should only be UL listed marked "Class 2" or "LPS", with an output rated 48 VDC, minimum 0.35 A, Tma: minimum 40 degrees C.

# SonicWALL SonicPoint Wireless

## Appliance Sicherheit und gesetzliche Vorschriften

### Weitere Hinweise zur Montage

- Wählen Sie für die Montage einen Ort, der keinem direkten Sonnenlicht ausgesetzt ist und sich nicht in der Nähe von Wärmequellen befindet. Die Umgebungstemperatur darf nicht mehr als 40 °C betragen.
- Führen Sie die Kabel nicht entlang von Stromleitungen, Leuchtstoffröhren und Störquellen wie Funksendern oder Breitbandverstärkern.
- Das beigelegte Netzkabel ist nur für den Betrieb in Nordamerika vorgesehen. Für Kunden in der Europäischen Union ist kein Kabel beigelegt.
- Stellen Sie sicher, dass das Gerät vor Wasser und hoher Luftfeuchtigkeit geschützt ist.
- Stellen Sie sicher, dass die Luft um das Gerät herum zirkulieren kann und die Lüftungsschlitze an der Seite des Gehäuses frei sind. Hier ist ein Belüftungsabstand von mindestens 26 mm einzuhalten.
- Vergewissern Sie sich, dass das Gerät sicher im Rack befestigt ist.

### Kabelverbindungen

Alle Ethernet- und RS232-C-Kabel eignen sich für die Verbindung von Geräten in Innenräumen. Schließen Sie an die Anschlüsse der SonicWALL keine Kabel an, die aus dem Gebäude herausgeführt werden, in dem sich das Gerät befindet.

### Informationen zur Stromversorgung APL21-083

Sollte das Netzteil nicht im Lieferumfang der SonicWALL enthalten sein, wenden Sie sich diesbezüglich an den technischen Support von SonicWALL (Tel.: +1-408-752-7819). Dieses Produkt darf nur in Verbindung mit einem nach den Normen der Underwriter Laboratories, USA als „UL-gelistet“ zugelassenen Netzteil der Kategorie „Class 2“ oder „LPS“ verwendet werden. Ausgang: 48 VDC Gleichsspannung, mind. 0,35 A, Tma: mind. 40 Grad C.

### Informationen zur Stromversorgung APL21-06E

Sollte das Netzteil nicht im Lieferumfang der SonicWALL enthalten sein, wenden Sie sich diesbezüglich an den technischen Support von SonicWALL (Tel.: +1-408-752-7819). Dieses Produkt darf nur in Verbindung mit einem nach den Normen der Underwriter Laboratories, USA als „UL-gelistet“ zugelassenen Netzteil der Kategorie „Class 2“ oder „LPS“ verwendet werden. Ausgang: 12 VDC Gleichsspannung, mind. 1,5 A, Tma: mind. 40 Grad C.

Wenn der Strom über den LAN Port eingespeist wird, bezeichnet man dies als "Power over Ethernet" oder "PoE". Die POE Quelle sollte mit UL Listed "Class 2" oder "LPS" gekennzeichnet sein, mit einer Ausgangsspannung von 48 VDC und mindestens 0.35 A, Tma: mind. 40 Grad C.

For more information regarding the following statements, please contact SonicWALL, Inc. at:  
2001 Logic Drive  
San Jose, CA 95124-3452  
1-408-745-9600

## FCC Part 15 Notice for the SonicWALL SonicPoint Wireless Appliance

NOTE: This equipment was tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy. And, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If the equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try and correct the interference using one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and the receiver.
- Connect the equipment into an outlet on a circuit different from the receiver connection.
- Consult SonicWALL for assistance.

**Caution:** Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

### Radiation Exposure Statement

This equipment complies with FCC and IC RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 centimeters (7.9 inches) between the radiator (antenna) and your body. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

### Authorized Channels

SonicWALL declares that the APL21-083 (FCC ID: QWU-083) and APL21-06E (FCC ID: QWU-06E) when sold in US is limited to CH1~CH11 by specified firmware controlled in the USA.

(1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

### Caution:

The device for the band 5470 -5725 MHz is only for indoor usage to reduce potential for harmful interference to co-channel mobile satellite systems.

The APL21-06E device has been designed to operate with an antenna having a maximum gain of 4 dBm. Antenna having a higher gain is strictly prohibited. The required antenna impedance is 50 ohms.

Dynamic Frequency Selection(DFS) is required on all Wireless LAN Mater devices (usually Access Points) and Wireless LAN Clients (usually Wireless NICs) that operate within 5470 MHz – 5725 MHz. SonicPoints that have these frequencies and channels enable in this range comply with North American and International DFS requirements. Some frequencies are blocked, and cannot be selected by the user per each specific regional approval.

Specific to the USA; at the urging of the Federal Communication Commission (FCC) user/installers should avoid operation frequencies near Terminal Doppler Weather Radar (TDWR) systems frequencies 5600-5650 MHz when installing SonicPoint within 35 km of line-of-site of TDWR sites. If TDWR is within 35 km the SonicPoint frequencies should be set to at least 30 MHz above or below any TDWR system frequency at that site. TDWR locations and specific frequencies used can be found at <<http://spectrumbridge.com/udrs/home.aspx>>.

Detailed current and background information can be found at <[http://www.wispa.org/?page\\_id=2341](http://www.wispa.org/?page_id=2341)>.

## Industry Canada Notices

### Authorized Channels

SonicWALL declares that the APL23-06E (IC: 4408A-06E) and APL23-083 (IC: 4408A-083) when sold in Canada is limited to CH1~CH11 byspecified firmware controlled in the USA.

### Operation

This device complies with RSS-210 of the Industry Canada Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

### Radiation Exposure Statement

This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

### Antenna

Under Industry Canada regulations, this radio transmitter may only operate using an antenna of a "dipole" type and maximum 4dBi at 5GHz and at 2.4Ghz (or lesser) gain approved for the transmitter by Industry Canada. To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (e.i.r.p.) is not more than that necessary for successful communication. L'impédance d'antenne requise est de 50 ohms

### Caution: (DFS band use)

(i) the device for operation in the band 5150-5250 MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems;

(ii) the maximum antenna gain permitted for devices in the bands 5250-5350 MHz and 5470-5725 MHz shall comply with the e.i.r.p. limit; and

(iii) the maximum antenna gain permitted for devices in the band 5725-5825 MHz shall comply with the e.i.r.p. limits specified for point-to-point and non point-to-point operation as appropriate.

Users should also be advised that high-power radars are allocated as primary users (i.e. priority users) of the bands 5250-5350 MHz and 5650-5850 MHz and that these radars could cause interference and/or damage to LE-LAN devices.

## Industrie Canada Notifications

### Chaînes autorisées

SonicWALL déclare que l'APL23-06E (IC : 4408A-06E) et APL23-083 (IC: 4408A-083) une fois vendu au Canada est limité à CH1~CH11 par spécifique microprogrammé aux Etats-Unis.

### Opération

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes : (1) l'appareil ne doit pas produire de brouillage, et (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

### Déclaration de l'exposition aux radiations

Cet équipement est conforme à l'exposition aux rayonnements IC limites établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 20 cm de distance entre le radiateur et votre corps.

### Antenne

Conformément à la réglementation d'Industrie Canada, le présent émetteur radio peut fonctionner avec une antenne d'un "dipole" type et d'un gain maximal 4dBi at 5GHz and at 2.4Ghz (ou inférieur) approuvé pour l'émetteur par Industrie Canada. Dans le but de réduire les risques de brouillage radioélectrique à l'intention des autres utilisateurs, il faut choisir le type d'antenne et son gain de sorte que la puissance isotrope rayonnée équivalente (p.i.r.e.) ne dépasse pas l'intensité nécessaire à l'établissement d'une communication satisfaisante. The required antenna impedance is 50 ohms.

**Attention: (utilisation de bande DFS)**

(i) les dispositifs fonctionnant dans la bande 5 150-5 250 MHz sont réservés uniquement pour une utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux;

(ii) le gain maximal d'antenne permis pour les dispositifs utilisant les bandes 5 250-5 350 MHz et 5 470-5 725 MHz doit se conformer à la limite de p.i.r.e.;

(iii) le gain maximal d'antenne permis (pour les dispositifs utilisant la bande 5 725-5 825 MHz) doit se conformer à la limite de p.i.r.e. spécifiée pour l'exploitation point à point et non point à point, selon le cas.

De plus, les utilisateurs devraient aussi être avisés que les utilisateurs de radars de haute puissance sont désignés utilisateurs principaux (c.-à-d., qu'ils ont la priorité) pour les bandes 5 250-5 350 MHz et 5 650-5 850 MHz et que ces radars pourraient causer du brouillage et/ou des dommages aux dispositifs LAN-EL.

## NCC Statement

**•第十二條**

•經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

**•第十四條**

•低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。前項合法通信，指依電信法規定作業之無線電通信。低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

依LP0002第4.7.5節規定 ”在5.25-

5.35兆赫頻帶內操作之無線資訊傳輸設備，限於室內使用”

**專業安裝警語(固定式點對點操作)**

此器材須經專業安裝並限用於固定式點對點操作。

## Declaration of Conformity

Certificate #: EU00170-A

This device is a 2.4 GHz wideband transmission system (transceiver), intended for use in all EU member states and EFTA countries, except in France and Italy where restrictive use applies.

In Italy the end-user should apply for a license at the national spectrum authorities in order to obtain authorization to use the device for setting up outdoor radio links and/or for supplying public access to telecommunications and/or network services.

This device may not be used for setting up outdoor radio links in France and in some areas the RF output power may be limited to 10 mW EIRP in the frequency range of 2454 – 2483.5 MHz. For detailed information the end-user should contact the national spectrum authority in France.

CE 0560

Application of council Directive	2004/108/EC (EMC) 2006/95/EC (LVD) 1999/5/EC (R&TTE)
Standard(s) to which conformity is declared	EN 55022:1998 +A1 +A2 Class B EN 55024:1998, +A2 EN 61000-3-2:2000, +A2 EN 61000-3-3:1995, +A2 EN 60950-1:2006, +A11:2009 National Deviations: AR, AT, AU, BE, CA, CH, CN, CZ, DE, DK, FI, FR, GB, GR, HU, IL, IN, IT, JP, KE, KR, MY, NL, NO, PL, SE, SG, SI, SK, US EN 300 328 V1.7.1:2006 EN 301 893 V1.5.1:2008 EN 301 489 V1.8.1:2008 EN 301 489-17 V2.1.1:2009a EN 50385:2002
Manufacturer/ Responsible Party	SonicWALL, Inc. 2001 Logic Drive San Jose, California 95124-3452 USA
Type of Equipment	802.11b/g/n access point
Type Numbers	APL21-06E APL21-083
May be Marketed as	SonicPoint-Ne SonicPoint-Ni

I, the undersigned, hereby declare that the equipment specified above conforms to the above Directives and Standards. Quality control procedures will ensure series production of equipment will be compliant.

<b>Signature</b> <u>/s/ Larry Wagner</u> Sr. Engineering Director	<b>Date</b> <u>05/30/10</u>
----------------------------------------------------------------------	-----------------------------

SonicWALL tímto prohlašuje, že tento APL21-083 / APL21-06E je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/ES.

Undertegnede SonicWALL erklærer herved, at følgende udstyr APL21-083 / APL21-06E overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.

Hiermit erklärt SonicWALL, dass sich das Gerät APL21-083 / APL21-06E in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG befindet.

Käesolevaga kinnitab SonicWALL seadme APL21-083 / APL21-06E vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.

Hereby, SonicWALL, declares that this APL21-083 / APL21-06E is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.

Por medio de la presente SonicWALL declara que el APL21-083 / APL21-06E cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.

ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ SonicWALL ΔΗΛΩΝΕΙ ΟΤΙ ΑΡ21-083 / ΑΡ21-06Ε ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ.

Par la présente SonicWALL déclare que l'appareil APL21-083 / APL21-06E est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE.

Con la presente SonicWALL dichiara che questo APL21-083 / APL21-06E è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.

Ar šo SonicWALL deklarē, ka APL21-083 / APL21-06E atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.

Šiuo SonicWALL deklaruoja, kad šis APL21-083 / APL21-06E atitinka esminius reikalavimus ir kitas 1999/5/EB Direktivos nuostatas.

Hierbij verklaart SonicWALL dat het toestel APL21-083 / APL21-06E in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG.

Hawnhekk, SonicWALL, jiddikjara li dan APL21-083 / APL21-06E jikkonforma mal-htigijiet essenzjali u ma provvedimenti oħrajn rilevanti li hemm fid-Direttiva 1999/5/EC.

Alulírott, SonicWALL nyilatkozom, hogy a APL21-083 / APL21-06E megfelel a vonatkozó alapvető követelményeknek és az 1999/5/EC irányelv egyéb előírásainak.

Niniejszym SonicWALL oświadczam, że APL21-083 / APL21-06E jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.

SonicWALL declara que este APL21-083 / APL21-06E está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.

SonicWALL izjavlja, da je ta APL21-083 / APL21-06E v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES.

SonicWALL týmto vyhlasuje, že APL21-083 / APL21-06E spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.

SonicWALL vakuuttaa täten että APL21-083 / APL21-06E tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.

Härmed intygar SonicWALL att denna APL21-083 / APL21-06E står i överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.

## Copyright Notice

© 2010 SonicWALL, Inc.

All rights reserved.

Under the copyright laws, this manual or the software described within, cannot be copied, in whole or part, without the written consent of the manufacturer, except in the normal use of the software to make a backup copy. The same proprietary and copyright notices must be affixed to any permitted copies as were affixed to the original. This exception does not allow copies to be made for others, whether or not sold, but all of the material purchased (with all backup copies) can be sold, given, or loaned to another person. Under the law, copying includes translating into another language or format.

Specifications and descriptions subject to change without notice.

## Trademarks

SonicWALL is a registered trademark of SonicWALL, Inc.

Microsoft Windows, Windows Vista, Windows XP, Windows Server, Internet Explorer, and Active Directory are trademarks or registered trademarks of Microsoft Corporation.

Other product and company names mentioned herein may be trademarks and/or registered trademarks of their respective companies and are the sole property of their respective manufacturers.



SonicWALL, Inc.

2001 Logic Drive

San Jose CA 95124-3452

T +1 408.745.9600

F +1 408.745.9300

[www.sonicwall.com](http://www.sonicwall.com)

**P/N 232-001795-50**

**Rev A 06/10**



**DYNAMIC SECURITY FOR THE GLOBAL NETWORK™**