SonicPoint-N Dual Radio Getting Started Guide

SonicWALL® E-CLASS

SONICWALL®

DYNAMIC SECURITY FOR THE GLOBAL NETWORK™

SonicWALL SonicPoint-N Dual Radio Getting Started Guide

This SonicWALL *Getting Started Guide* provides the network administrator with setup instructions for creating an enterprise-class secure wireless network with the SonicPoint-N Dual Radio appliance, all in about 60 minutes. More than just the basics, this guide provides a concise overview of both general wireless deployment concepts and specific network configurations.

Setup

Step	Procedure	Est. Time
1	*Before You Begin* - page 3	5
2	*Introduction to Secure Wireless* - page 7	10
3	*Registering Your Appliance* - page 11	10
4	*Configuring the Wireless Zone and Interface* - page 13	15
5	*Setting Up Your SonicPoint* - page 17	20

Additional Configuration and Information

- *Optimizing Wireless with RF Analysis* - page 23
- *Support and Training Options* - page 27
- *Product Safety and Regulatory Information* - page 31

Before You Begin 1

In this Section:

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

Check Package Contents

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

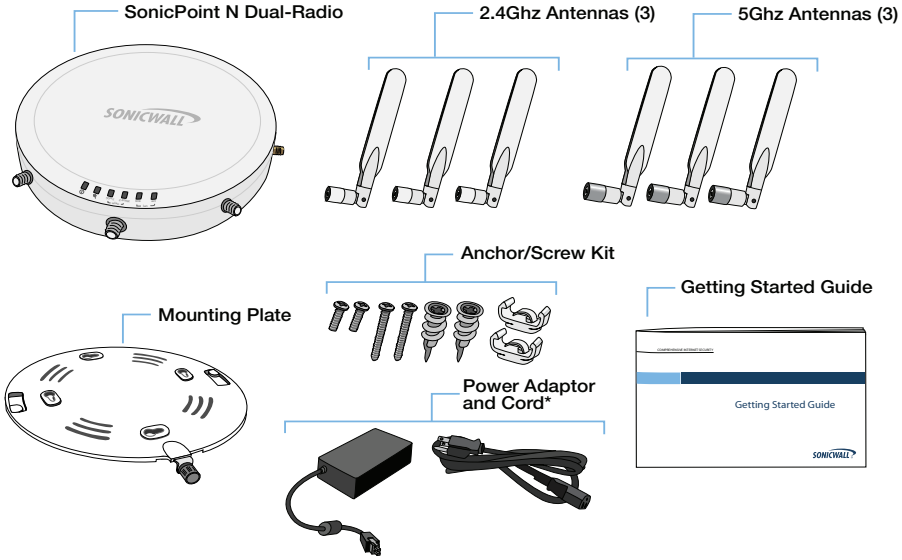
- ☐ SonicPoint-N Dual Radio Appliance
- ☐ Six (6) Antennas (2.4 GHz x 3), (5GHz x 3)
- ☐ Mounting Plate
- ☐ Anchor Kit (Screw Kit, Ceiling Braces)
- ☐ This *Getting Started Guide*
- ☐ Power Adaptor and Cord*

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

Missing Items?

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*>



What You Need to Begin

This page provides basic network hardware and software prerequisites as a baseline for SonicPoint-N Dual Radio deployments. More specific requirements are detailed in the remainder of this guide.

Hardware / Firmware Requirements

The SonicWALL SonicPoint-N Dual Radio security appliances are centrally managed and require a **SonicWALL NSA E-Class appliance running SonicOS 5.6.3.1 or higher** firmware to function properly.

Note: *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.*

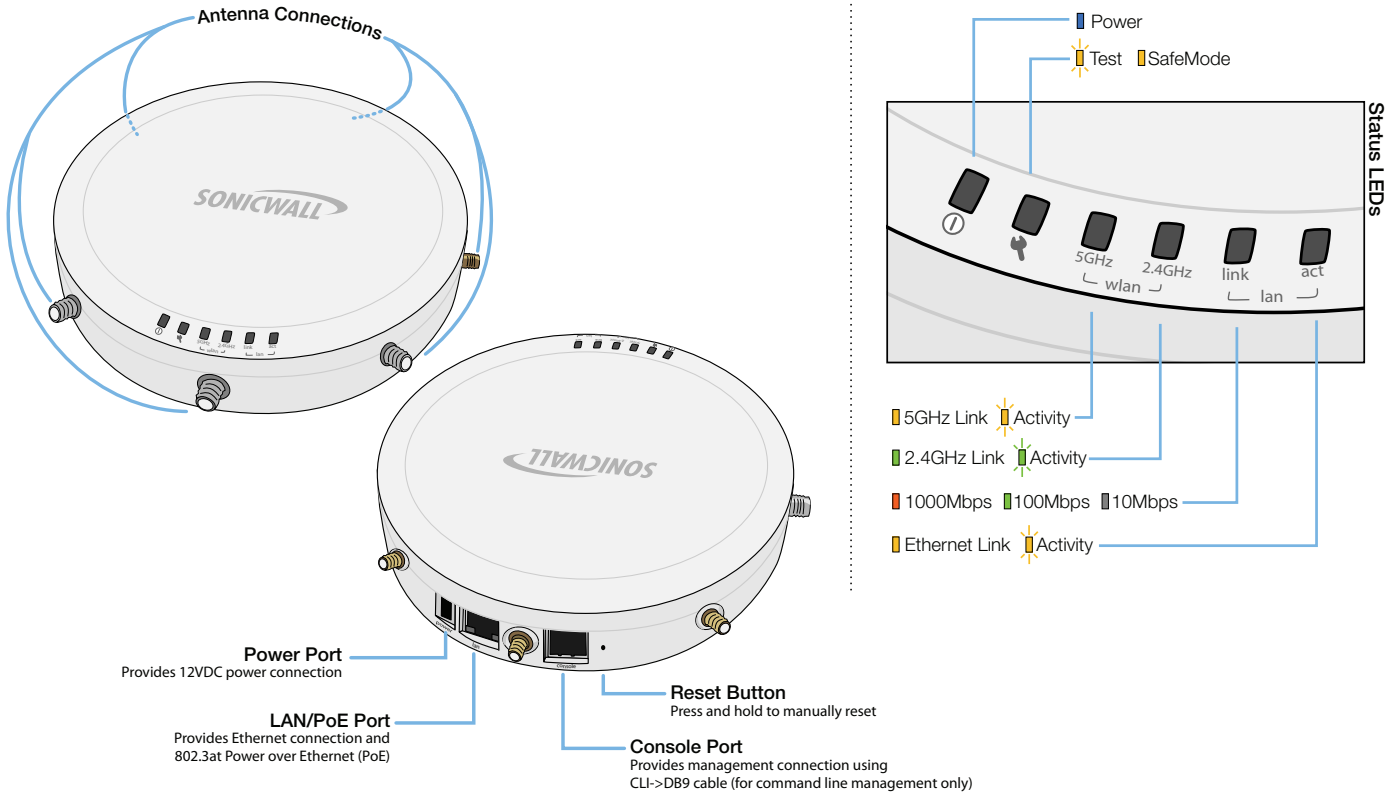
Network Deployment Requirements

- An active broadband Internet connection
- At least one free network interface on the SonicWALL security appliance, configured with a zone type of “WLAN”
- A single point placement or distributed wireless placement plan for your SonicPoint(s)
- Wireless clients capable of 802.11n wireless communications[1]
- A network infrastructure capable of sustaining 802.11n data rates to the number of clients you intend to support
- An 802.3at compliant PoE injector or PoE-capable switch (if powering your deployment using PoE)

Note: *For more network deployment recommendations and tips, see the Hardware Decisions section, on page 9.*

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.

Ports and Status LEDs



Introduction to Secure Wireless 2

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

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:

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
Radius (Range)	90ft/25m	120ft/ 35m	120ft/ 35m	300ft/90m

Radio Frequency Barriers

The following tables list some common RF barrier types:

Barrier Type	RF Signal Blocking
Open air	Very Low
Glass, drywall, cubicle partitions	Low
Stone floors and walls (brick/marble/granite)	Medium
Concrete, security glass, stacked books/paper	High
Metal, metal mesh, reinforced concrete, water	Very High

RF Interference

The following table lists several common interference sources:

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[a]	Within 10-20 feet	802.11b/g/n
Scientific and medical equipment	Short distance, varies	802.11b/g/n
Other wireless devices	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.*

Access Points and Network Design

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:

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>*

Hardware Decisions

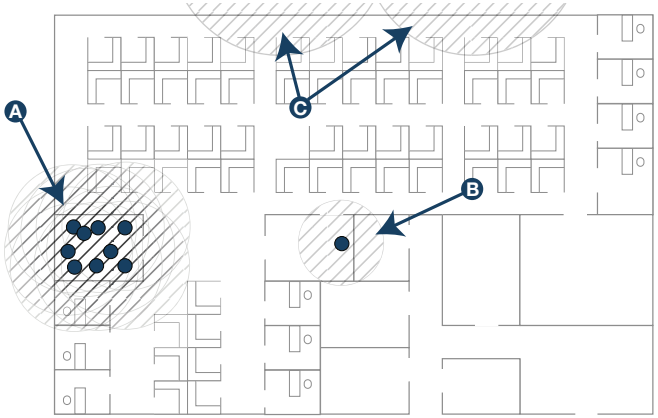
The first decision in hardware is the access point. While access point technology (802.11a/b/g/n) is one factor in determining your placement, based on distance served and bandwidth needed, taking note of other hardware-based factors is just as important.

Some hardware factors to take into consideration:

- **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 / Security Appliance** – Your wireless deployment has to tie back into your SonicWALL security 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.
- **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 Over Ethernet (PoE)** – Part of your wireless network planning should include verifying that your PoE equipment is 802.3at compliant, and that full 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 or 5GHz 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.

Registering Your Appliance 3

In this Section:

This section provides instructions for registering your SonicWALL SonicPoint appliance.

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

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:

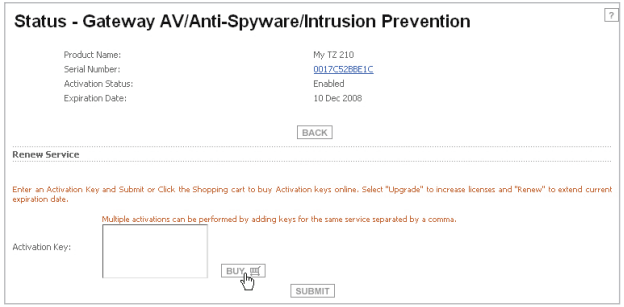
1. Login to your MySonicWALL account. If you do not have an account, you can create one at www.mysonicwall.com.
2. Enter the serial number of your product in the **REGISTER A PRODUCT** field and click the **Next** button.
3. Type a friendly name for the appliance, select the **Product Group** if any, 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 security 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 Security Services for Wireless Clients

Any security services you purchased for your SonicWALL security 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 security appliance, please speak with a sales representative or visit *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.



Configuring the Wireless Zone and Interface 4

In this Section:

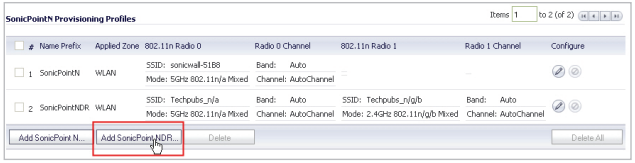
SonicWALL SonicPoints are wireless access points specially engineered to work with SonicWALL security appliances. This section provides instructions for configuring the SonicWALL security appliance to recognize and connect with your SonicWALL SonicPoint(s).

Configuring Provisioning Profiles

SonicPoint profiles make it easy to apply basic settings to multiple SonicPoints within a wireless 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 NDR** below the list of SonicPoint provisioning profiles. The Add/Edit SonicPoint Profile window displays.



General Tab

1. Select **Enable SonicPoint**.
2. Enter a **Name Prefix**. This prefix is used as an internal reference to identify each SonicPoint provisioned, but is not a part of the public SSID, which is configured later.
3. Select the **Country Code** for the area of operation (*for countries outside of North American only.*)
4. Choose the desired **EAPOL Version**. Version 2 of the protocol is more secure, but less compatible with older network devices.

802.11n Radio 0/1 Tabs (5GHz Radio / 2.4 GHz Radio)

Radios are configured in their respective tabs. To configure both Radio 0 and Radio 1:

1. Select **Enable Radio**.
2. Optionally, select a schedule for the radio to be enabled from the drop-down list.
3. Select a **Radio Mode** to dictate the radio frequency band(s). The default setting for Radio 0 is **5GHz 802.11 n/g/b Mixed**, the default for Radio 1 is **2.4GHz 802.11n/g/b Mixed**.
4. Enter an **SSID** to identify this network to wireless clients.
5. Select a **Radio Band** for this radio. You may choose to keep the default setting, Auto, unless you have reason to manually select a Band.
6. Select a **Primary Channel** and **Secondary Channel**. You may choose to keep the default setting, Auto, unless you have a reason to use or avoid specific channels.
7. Under **WEP/WPA Encryption**, select the **Authentication Type** for your wireless network. Using **WPA2** provides the most secure connection.
8. The remaining fields change depending on the selected authentication type. Refer to the *SonicOS Administrator's Guide* for details on the multiple wireless security authentication types available.
9. Optionally, under **ACL Enforcement**, select **Enable MAC Filter List** and choose an address object group from the **Allow List** or **Deny List** to allow or deny traffic to and from all devices with MAC addresses in the group.

Radio 0/1 (5Ghz/2.4GHz) Advanced Tabs

Configure the advanced radio settings for each 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 Administrator's Guide*. When you are finished, click **OK**.

Note: ***If one or more of your SonicPoints were connected to the SonicWALL appliance before a provisioning profile was created, the default profile is used.*** *To re-apply new provisioning profile settings, delete all devices from the SonicPointNs table on the* ***SonicPoint > SonicPoints*** *page. This action reboots the devices so they may assume the correct assigned profile.*

Configuring a Wireless Zone

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

To configure a standard WLAN zone:

1. On the **Network** > **Zones** page in the **WLAN** row, click the icon in the **Configure** column. The Edit Zone - WLAN window displays.

2. Click on the **General** tab.
3. The **Allow Interface Trust** option allows traffic to flow between multiple WLAN-zoned interfaces. It is common to select this option when SonicPoints are connected to multiple physical interfaces.
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.
7. If you configured a custom **SonicPoint N Provisioning Profile** in the previous section, select it from the drop down list, otherwise you may keep the default profile selected.
8. 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 Administrator's Guide*.
9. When finished, click **OK**.

Configuring the Network Interface

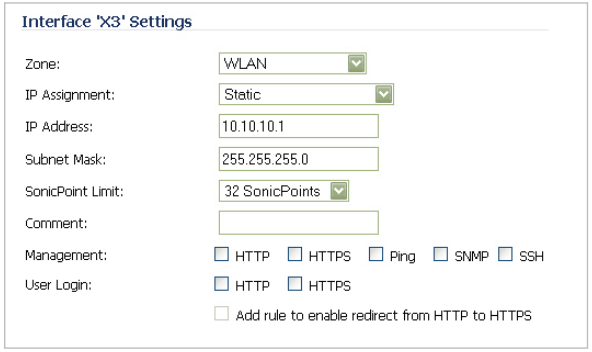
Each SonicPoint or group of SonicPoints must be connected to a physical network interface configured for Wireless. By default, SonicOS provides a standard wireless zone (WLAN), which can be applied to any available interface.

General Tab

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** (automatically generated in most cases). In our example, 255.255.255.0 is an appropriate subnet mask.
6. 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, you may choose to allow **Management** and **User Login** mechanisms to allow wireless clients to log into the SonicWALL management interface. Enabling these options is not common for most wireless networks. If you must do so, first ensure that you have a strong password.



Advanced Tab

1. Select a **Link Speed** to manually limit the port speed, or keep the default setting of Auto Negotiate for best-effort.
2. Configure a custom MAC address using the **Override Default MAC Address** option if necessary for your deployment, or choose to **Use Default MAC Address** assigned by SonicWALL. This setting should not be changed unless your deployment requires it.
3. Optionally, choose to **Enable Multicast Support**.
4. Optionally, choose to **Enable 802.1p tagging** for QoS support.

Setting Up Your SonicPoint 5

In this Section:

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

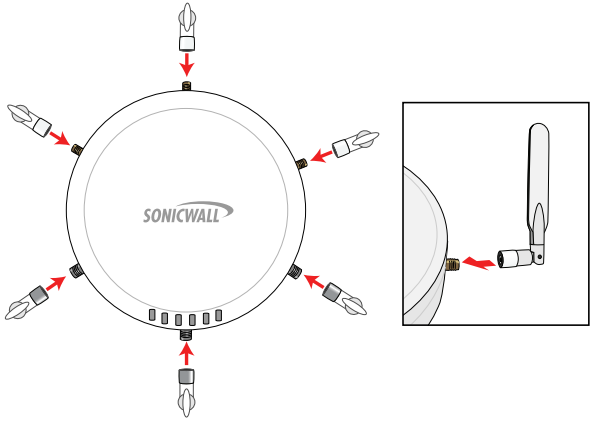
Installing Antennas

To install the SonicPoint-N Dual Radio included antennas:

1. Remove the six (6) antennas from the bag and place each on the appropriate connector, keeping in mind that two antenna/connector types exist.
2. Carefully finger-tighten the fittings.

Note: *The proper antennas will fit easily into the appropriate connection. Never force an antenna onto a connector.*

3. Adjust the antennas for reception, keeping in mind that orienting the antennas vertically provides optimal wireless coverage in most cases.



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

Note: *The antennas provided by SonicWALL are designed to provide optimal signal strength and coverage within the confines of regulatory laws. Only use the antennas provided by SonicWALL with this appliance.*

Connecting Ethernet Cable

To connect the SonicPoint to your network:

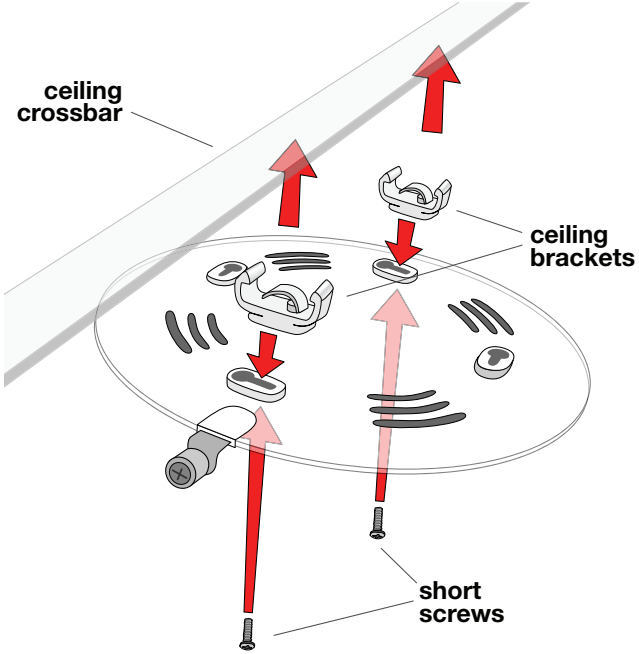
1. Using CAT5, CAT5e, or CAT6 cabling, connect the “lan” port of the SonicPoint to the interface you previously configured on the SonicWALL security appliance.
2. Optionally, SonicPoints may be powered by using the SonicWALL **802.11at PoE** line injector (sold separately), or by using a third-party 802.3at compliant PoE switch.

Note: If using a PoE switch/injector to power the SonicPoint, ensure that the switch/injector is 802.11at compliant and rated to deliver at least 25.5 watts. Always read and comply with instructions and warnings provided with the PoE before connecting the device to your SonicPoint.

Mounting Using Ceiling Brackets

To mount the SonicPoint to a crossbar between ceiling panels:

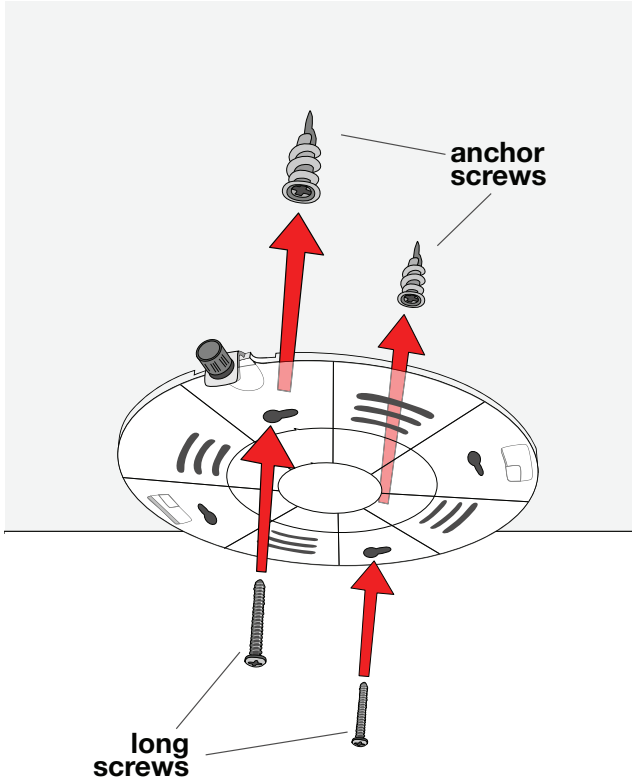
1. Using the short screws, screw in the brackets to the underside of the SonicPoint, mounting plate, making sure both brackets are parallel.
2. Supporting the SonicPoint in one hand, clip the edge of each bracket over the edge of the ceiling crossbar. Make sure the SonicPoint is securely attached to the crossbar before releasing the device.
3. Place the SonicPoint onto the mounting plate so the locking screw lines up with the ‘unlock’ position.
4. Turn the SonicPoint clockwise until the locking screw lines up with the ‘lock’ position on the SonicPoint.
5. Push the mounting screw in and turn clockwise until firm.



Mounting Using Anchor Screws

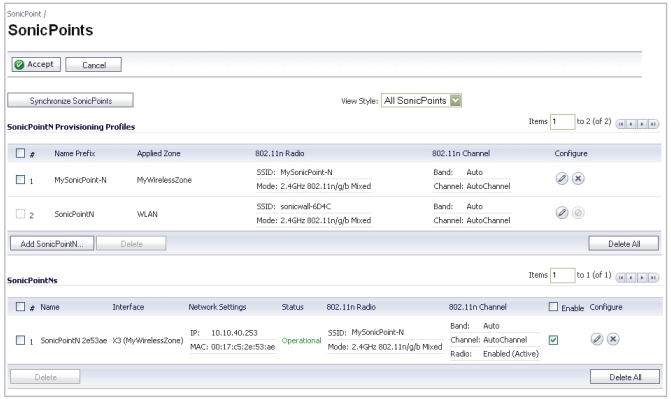
To mount the SonicPoint using the plate and anchor screws:

1. Remove the mounting plate from the bottom of the SonicPoint and place the plate on the location where you wish to mount the SonicPoint.
2. Using a pencil, mark the location of two of the locking screw holes. The holes you mark should be directly across from each other, not adjacent to each other.
3. Screw the larger anchor screws into the locations you marked until the face of the screw is flush with the surface.
4. Screw the long screws into the anchors, leaving enough space between the screw head and the anchor surface to fit the mounting plate underneath.
5. Place the mounting plate over the screws and turn to lock. The plate should fit snugly after turning. Tighten the screws if needed.
6. Place the SonicPoint onto the mounting plate so the locking screw lines up with the ‘unlock’ position.
7. Turn the SonicPoint clockwise until the locking screw lines up with the ‘lock’ position on the SonicPoint.
8. Push the mounting screw in and turn clockwise until firm.



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:



Verifying WAN (Internet) Connectivity

Complete the following steps to confirm your Internet connectivity:

1. Disconnect a client computer from any other network connections (LAN, Wireless, 3G, etc...)
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 22.

Troubleshooting Tips

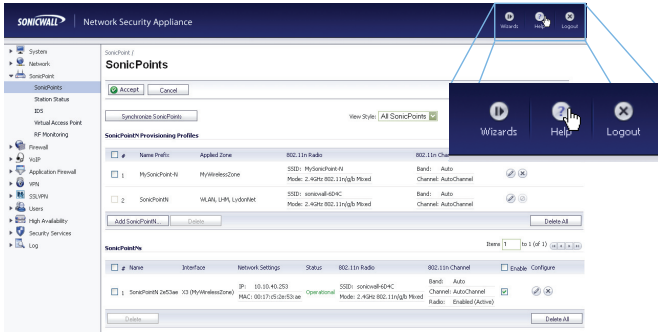
If the SonicPoint locates a peer SonicOS device, the two units perform an encrypted exchange and the profile assigned to the relevant wireless zone is used to automatically configure (provision) the newly added SonicPoint unit.

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 802.3at compliant PoE** if using PoE to power your SonicPoint appliance.
- **Verify that your PoE switch/injector is rated to deliver at least 25.5 watts** of power to each port. Some older PoE devices do not provide sufficient power to properly run current generation dual radio 802.11n devices across multiple ports. Check with your PoE manufacturer for 802.3at support, or use a SonicWALL 802.3at 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.



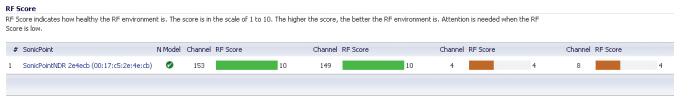
Optimizing Wireless with RF Analysis 6

In this Section:

This section describes how to monitor, adjust, and optimize your wireless network using the RF Analysis features built into the SonicOS management interface **SonicPoint > RF Analysis** panel.

Using the Wireless RF Score

The RF Score is a calculated number on a scale of 1-10 which is used to represent the overall condition for a channel. A high channel RF score (depicted in green) indicates a better quality RF environment.



SonicWALL wireless drivers report signal strength in RSSI, this number is used in the below equation to get a raw score on a scale of 1 to 100.

Preliminary RF Score Formula:

rfaScore100 = 100-((rssiTotal-50)*7/10))
simplified: rfaScore100 = -0.7*rssiTotal + 135

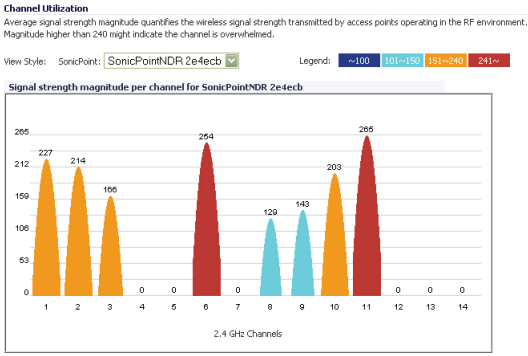
The Final (1-10) RF Analysis Score:

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

Note: *This feature depends on the knowledge of what channel a SonicPoint is operating in. If the channel number is unknown, RF Score is not shown.*

Channel Utilization

The channel utilization graph shows how channels are being utilized for each SonicPoint.

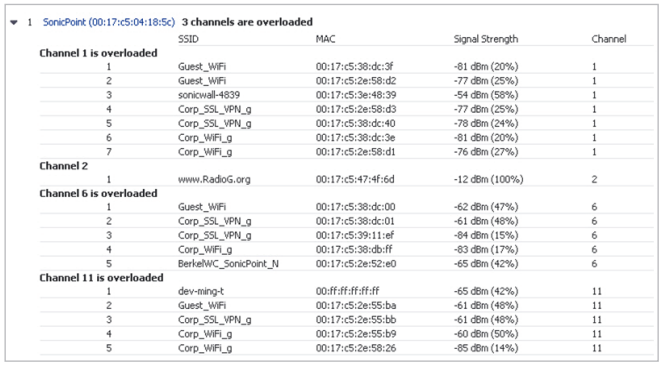


The number on the top of each color bar indicates the average signal strength magnitude each SonicPoint detects for the indicated channel. High magnitudes (greater than 240) are shown in red and generally indicate that the corresponding channel is overloaded.

Note: *Although some channels are not used in all countries, they are still shown, as it is possible for a wireless cracker to launch denial of service attacks to adjacent channels.*

Viewing Overloaded Channels

RF Analysis shows devices operating in each channel. A warning is displayed when it detects more than four active APs in the same channel, regardless of how strong the signal strength is.



1 SonicPoint (00:17:c5:04:18:5c) **3 channels are overloaded**

	SSID	MAC	Signal Strength	Channel
Channel 1 is overloaded				
1	Guest_WiFi	00:17:c5:38:dc:3f	-81 dBm (20%)	1
2	Guest_WiFi	00:17:c5:2e:58:d2	-77 dBm (25%)	1
3	sonicwall-4839	00:17:c5:3e:48:39	-54 dBm (58%)	1
4	Corp_SSL_VPN_g	00:17:c5:2e:58:d3	-77 dBm (25%)	1
5	Corp_SSL_VPN_g	00:17:c5:38:dc:40	-78 dBm (24%)	1
6	Corp_WiFi_g	00:17:c5:38:dc:3e	-81 dBm (20%)	1
7	Corp_WiFi_g	00:17:c5:2e:58:d1	-76 dBm (27%)	1
Channel 2				
1	www.RadioG.org	00:17:c5:47:4f:6d	-12 dBm (100%)	2
Channel 6 is overloaded				
1	Guest_WiFi	00:17:c5:38:dc:00	-62 dBm (47%)	6
2	Corp_SSL_VPN_g	00:17:c5:38:dc:01	-61 dBm (48%)	6
3	Corp_SSL_VPN_g	00:17:c5:39:11:ef	-84 dBm (15%)	6
4	Corp_WiFi_g	00:17:c5:38:db:ff	-83 dBm (17%)	6
5	BerkelWC_SonicPoint_N	00:17:c5:2e:52:e0	-65 dBm (42%)	6
Channel 11 is overloaded				
1	dev-ming-t	00:ff:ff:ff:ff:ff	-65 dBm (42%)	11
2	Guest_WiFi	00:17:c5:2e:55:ba	-61 dBm (48%)	11
3	Corp_SSL_VPN_g	00:17:c5:2e:55:bb	-61 dBm (48%)	11
4	Corp_WiFi_g	00:17:c5:2e:55:b9	-60 dBm (50%)	11
5	Corp_WiFi_g	00:17:c5:2e:58:26	-85 dBm (14%)	11

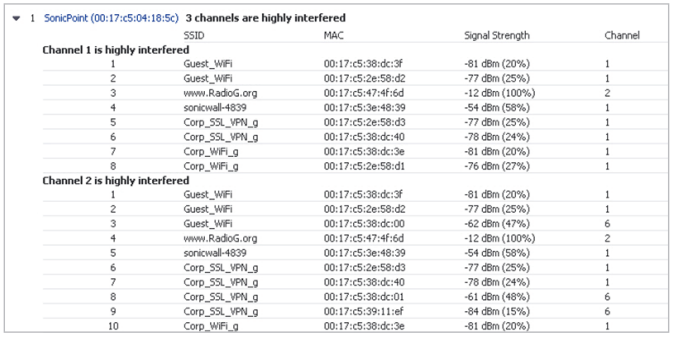
Information about each discovered access point includes: SSID, MAC, signal strength, and channel. Two values are shown for signal strength: dBm and percentage value, where higher numbers indicate stronger signals.

RFA Highly Interfered Channels

Access points working in adjacent channels (less than 5 channels apart) can also interfere with each other.

The RF Analysis feature displays a warning when a SonicPoint appliance detects more than five active access points nearby operating in adjacent channels.

Again, regardless of the signal strength from interfering access points, RF Analysis marks the channel as highly interfered.



1 SonicPoint (00:17:c5:04:18:5c) **3 channels are highly interfered**

	SSID	MAC	Signal Strength	Channel
Channel 1 is highly interfered				
1	Guest_WiFi	00:17:c5:38:dc:3f	-81 dBm (20%)	1
2	Guest_WiFi	00:17:c5:2e:58:d2	-77 dBm (25%)	1
3	www.RadioG.org	00:17:c5:47:4f:6d	-12 dBm (100%)	2
4	sonicwall-4839	00:17:c5:3e:48:39	-54 dBm (58%)	1
5	Corp_SSL_VPN_g	00:17:c5:2e:58:d3	-77 dBm (25%)	1
6	Corp_SSL_VPN_g	00:17:c5:38:dc:40	-78 dBm (24%)	1
7	Corp_WiFi_g	00:17:c5:38:dc:3e	-81 dBm (20%)	1
8	Corp_WiFi_g	00:17:c5:2e:58:d1	-76 dBm (27%)	1
Channel 2 is highly interfered				
1	Guest_WiFi	00:17:c5:38:dc:3f	-81 dBm (20%)	1
2	Guest_WiFi	00:17:c5:2e:58:d2	-77 dBm (25%)	1
3	Guest_WiFi	00:17:c5:38:dc:00	-62 dBm (47%)	6
4	www.RadioG.org	00:17:c5:47:4f:6d	-12 dBm (100%)	2
5	sonicwall-4839	00:17:c5:3e:48:39	-54 dBm (58%)	1
6	Corp_SSL_VPN_g	00:17:c5:2e:58:d3	-77 dBm (25%)	1
7	Corp_SSL_VPN_g	00:17:c5:38:dc:40	-78 dBm (24%)	1
8	Corp_SSL_VPN_g	00:17:c5:38:dc:01	-61 dBm (48%)	6
9	Corp_SSL_VPN_g	00:17:c5:39:11:ef	-84 dBm (15%)	6
10	Corp_WiFi_g	00:17:c5:38:dc:3e	-81 dBm (20%)	1

Support and Training Options 7

In this Section:

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

Related Documentation

SonicWALL's documentation reference library <*http://www.sonicwall.com/us/support.html*> provides digital downloads of all available print and web-based documentation for the SonicWALL product line.

- *SonicOS Administrator's Guide*
- *SonicOS Release Notes*
- *SonicOS Feature Modules:*
  - DPI-SSL
  - MAC-IP Anti-Spoof
  - Virtual Access Points
  - SSL VPN Remote Access
  - High Availability
  - NAT Load Balancing
  - Packet Capture
  - Radio Frequency Monitoring
  - Single Sign-On
  - SSL Control
  - Secure Wireless Bridging

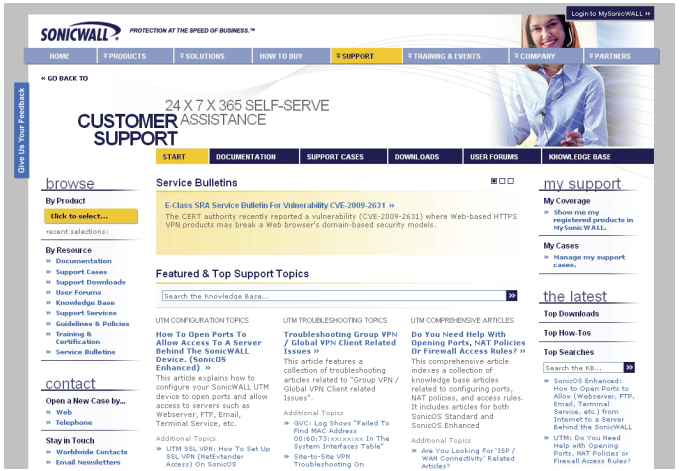
SonicWALL Secure Wireless Network Integrated Solutions Guide

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*>

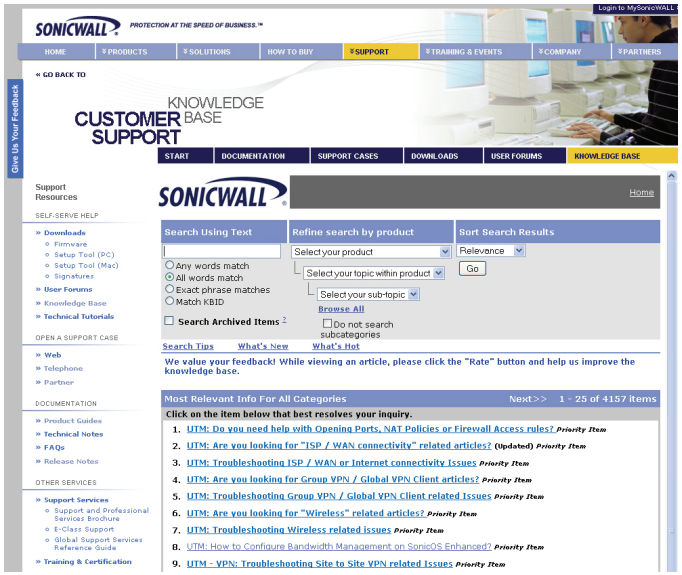
Customer Support

SonicWALL Customer Support <*http://www.sonicwall.com/us/support.html*> 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.



Knowledge Base

The Knowledge Base <*http://www.mysonicwall.com/*> allows users to browse or search for SonicWALL support documents.



User Forums

The SonicWALL User Forums <*https://forum.sonicwall.com/*> are a resource that provide users the ability to communicate and discuss a variety of security and appliance subject matters.

Training

SonicWALL's Training Program <*http://training.sonicwall.com/*> 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.

Product Safety and Regulatory Information 8

In this Section:

This section provides regulatory, trademark, and copyright information.

Safety and Regulatory Information for the SonicWALL SonicPoint Wireless Appliance

Regulatory Model/Type	Product Names
APL23-081	SonicPoint-N Dual Radio

Mounting the SonicWALL

- Mount in a location away from direct sunlight and sources of heat. A maximum ambient temperature of 104º F (40º 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 (25.44mm) clearance is recommended.
- Consideration must be given to the connection of the equipment to the supply circuit and the effect of over-loading 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 APL23-081

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, 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 beigefügte Netzkabel ist nur für den Betrieb in Nordamerika vergesehen. Für Kunden in der Europäischen Union ist kein Kabel beigefügt.
- 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 APL23-081

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. 1,66 A, Tma: mind. 40 Grad C.

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

FCC

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 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.

United States of America Authorized Channels
SonicWALL declares that the APL23-081 (FCC ID: QWU-081) when sold in US is limited to CH1~CH11 by specified firmware controlled in the USA.

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.

Caution:

This device is for indoor usage to reduce potential for harmful interference to co-channel systems.

The APL23-081 device has been designed to operate with an antenna having a maximum gain of 4dBi at 5GHz and 3dBi at 2.4Ghz. 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*>.

Industry Canada Notices

SonicWALL declares that the APL23-081 (IC: 4408A-081) when sold in Canada is limited to CH1~CH11 by specified firmware controlled in the USA.

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.

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.

Under Industry Canada regulations, this radio transmitter may only operate using an antenna of a “dipole” type and maximum 4dBi at 5GHz and 3dBi 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

SonicWALL déclare que l'APL23-081 (IC : 4408A-081) une fois vendu au Canada est limité à CH1~CH11 par spécifique microprogrammé aux Etats-Unis.

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.

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.

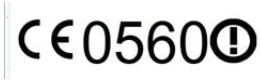
Conformément à la réglementation d'Industrie Canada, le présent émetteur radio peut fonctionner avec une antenne d'un “dipole” type et d'un gain maximal 4dBi at 5GHz and 3dBi at 2.4Ghz (ou inférieur) approuvé pour l'émetteur par Industrie Canada. Dans le but de réduire les risques de brouillage radioélectrique 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.



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.

Declaration of Conformity

Certificate #: EU00190-A

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	802.11a/b/g/n access point
Type Numbers	APL23-081
May be Marketed as	SonicPoint-N Dual Radio

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.

Signature /s/ Larry Wagner Sr. Engineering Director	**Date** 1/21/11

SonicWALL tímto prohlašuje, že tento APL23-081 je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/ES.

Undertegnede SonicWALL erklærer herved, at følgende udstyr APL23-081 overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.

Hiermit erklärt SonicWALL, dass sich das Gerät APL23-081 in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG befindet.

Käesolevaga kinnitab SonicWALL seadme APL23-081 vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.

Hereby, SonicWALL, declares that this APL23-081 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 APL23-081 cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.

ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ SonicWALL ΔΗΛΩΝΕΙ ΟΤΙ APL23-081 ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ.

Par la présente SonicWALL déclare que l'appareil APL23-081 est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE.

Con la presente SonicWALL dichiara che questo APL23-081 è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.

Ar šo SonicWALL deklarē, ka APL23-081 atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.

Šiuo SonicWALL deklaruoja, kad šis APL23-081 atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.

Hierbij verklaart SonicWALL dat het toestel APL23-081 in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG.

Hawnhekk, SonicWALL, jiddikjara li dan APL23-081 jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 1999/5/EC.

Alulírott, SonicWALL nyilatkozom, hogy a APL23-081 megfelel a vonatkozó alapvetõ követelményeknek és az 1999/5/EC irányelv egyéb elõírásainak.

Niniejszym SonicWALL oświadcza, że APL23-081 jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.

SonicWALL declara que este APL23-081 está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.

SonicWALL izjavlja, da je ta APL23-081 v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES.

SonicWALL týmto vyhlasuje, že APL23-081 spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.

SonicWALL vakuuttaa täten että APL23-081 tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.

Härmed intygar SonicWALL att denna APL23-081 står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.

Copyright Notice

Trademarks

SonicWALL, Inc.

2001 Logic Drive
San Jose CA 95124-3452

T +1 408.745.9600
F +1 408.745.9300

www.sonicwall.com

P/N 232-001939-50
Rev A 01/11

DYNAMIC SECURITY FOR THE GLOBAL NETWORK™