

SonicWALL Secure Wireless Solution

SonicPoint and SonicPoint G Administrator's Guide



Table of Contents

Using the SonicWALL SonicPoint	1
Supported Platforms	2
Overview of the SonicWALL SonicPoint Hardware	2
SonicPoint Registration	6
SonicPoint Overview	7
SonicPoint Features	8
SonicPoint Modes of Operation	9
Number of Subnets Supported	11
Wireless Zones: The WLAN Zone	11
SonicPoint Enforcement	12
Enabling Traffic from Non-SonicPoint Devices	12
Wireless Firewalling	14
WiFiSec Enforcement / WPA	16
Wireless Roaming	17
Roaming Within Layer 3 Boundaries	18
Roaming Across Multiple SonicWALL Interfaces	19
Guest Services	20
Inter-guest Communications	20
Dynamic Address Translation	20
Bypass Guest Authentication	20
Customizable Authentication Pages	20
SMTP Redirection	21
Enabling External Guest Services	21
MAC Filtering Using MAC Address Objects	22
SonicPoint Profiles	22
Automatic Provisioning (SDP & SSPP)	22
Hardware Failover and LAN Port Disconnect Transitions	23
Managed Mode and Stand-Alone Mode Transitions	24
SonicPoint LEDs	25
Managing SonicPoints in Managed Mode	26
Before Managing SonicPoints	26
SonicPoint Provisioning Profiles	26
Configuring a SonicPoint Profile	27
Selecting Variable Numbers of SonicPoint Access Points	31
Working with New Memory Requirements	32
Updating SonicPoint Settings	33
Edit SonicPoint settings	33
Synchronize SonicPoints	33
Enable and Disable Individual SonicPoints	33
Updating SonicPoint Firmware	33
SonicPoint States	34
Managing the SonicPoint in Stand-Alone Mode	35

Connecting to the Stand-Alone Management Interface	35
Using the SonicPoint Stand-Alone Management Interface	36
System > Status	36
.	36
System > Settings	36
.	37
System > Firmware	37
.	37
System > Restart	37
.	37
Network > Interfaces	38
Wireless > Status	38
Wireless > 802.11a Radio	39
Wireless > 802.11a Advanced	39
Wireless > 802.11g Radio	40
Wireless > 802.11g Advanced	40
Managing the SonicPoint in SafeMode	41
Resetting the SonicPoint	42
SonicPoint Radio Characteristics	43
.	44

Preface

Copyright Notice

© 2005 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.

SonicWALL is a registered trademark of SonicWALL, Inc.

Other product and company names mentioned herein may be trademarks and/or registered trademarks of their respective companies.

Specifications and descriptions subject to change without notice.

Limited Warranty

SonicWALL, Inc. warrants that commencing from the delivery date to Customer (but in any case commencing not more than ninety (90) days after the original shipment by SonicWALL), and continuing for a period of twelve (12) months, that the product will be free from defects in materials and workmanship under normal use. This Limited Warranty is not transferable and applies only to the original end user of the product. SonicWALL and its suppliers' entire liability and Customer's sole and exclusive remedy under this limited warranty will be shipment of a replacement product. At SonicWALL's discretion the replacement product may be of equal or greater functionality and may be of either new or like-new quality. SonicWALL's obligations under this warranty are contingent upon the return of the defective product according to the terms of SonicWALL's then-current Support Services policies.

This warranty does not apply if the product has been subjected to abnormal electrical stress, damaged by accident, abuse, misuse or misapplication, or has been modified without the written permission of SonicWALL.

DISCLAIMER OF WARRANTY. EXCEPT AS SPECIFIED IN THIS WARRANTY, ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS, AND WARRANTIES INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY OR CONDITION OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT, SATISFACTORY QUALITY OR ARISING FROM A COURSE OF DEALING, LAW, USAGE, OR TRADE PRACTICE, ARE HEREBY EXCLUDED TO THE MAXIMUM EXTENT ALLOWED BY APPLICABLE LAW. TO THE EXTENT AN IMPLIED WARRANTY CANNOT BE EXCLUDED, SUCH WARRANTY IS LIMITED IN DURATION

TO THE WARRANTY PERIOD. BECAUSE SOME STATES OR JURISDICTIONS DO NOT ALLOW LIMITATIONS ON HOW LONG AN IMPLIED WARRANTY LASTS, THE ABOVE LIMITATION MAY NOT APPLY TO YOU. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS, AND YOU MAY ALSO HAVE OTHER RIGHTS WHICH VARY FROM JURISDICTION TO JURISDICTION. This disclaimer and exclusion shall apply even if the express warranty set forth above fails of its essential purpose.

DISCLAIMER OF LIABILITY. SONICWALL'S SOLE LIABILITY IS THE SHIPMENT OF A REPLACEMENT PRODUCT AS DESCRIBED IN THE ABOVE LIMITED WARRANTY. IN NO EVENT SHALL SONICWALL OR ITS SUPPLIERS BE LIABLE FOR ANY DAMAGES WHATSOEVER, INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION, LOSS OF INFORMATION, OR OTHER PECUNIARY LOSS ARISING OUT OF THE USE OR INABILITY TO USE THE PRODUCT, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL, OR PUNITIVE DAMAGES HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY ARISING OUT OF THE USE OF OR INABILITY TO USE HARDWARE OR SOFTWARE EVEN IF SONICWALL OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. In no event shall SonicWALL or its suppliers' liability to Customer, whether in contract, tort (including negligence), or otherwise, exceed the price paid by Customer. The foregoing limitations shall apply even if the above-stated warranty fails of its essential purpose. BECAUSE SOME STATES OR JURISDICTIONS DO NOT ALLOW LIMITATION OR EXCLUSION OF CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

Current Documentation

Check the SonicWALL documentation Web site for that latest versions of this manual and all other SonicWALL product documentation.

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

Using the SonicWALL SonicPoint

The SonicWALL SonicPoint provides secure wireless access across your enterprise, managed from a single central SonicWALL security appliance.

This guide introduces you to the concepts involved in designing your wireless network to use SonicPoints. It also provides a guide to managing the SonicPoint, either through a SonicWALL security appliance in *Managed Mode* or on its own in *Stand-Alone Mode*.

For more detailed instructions on managing a SonicPoint in Managed Mode, see the *SonicWALL SonicOS Enhanced 2.5 Administrators Guide*.



Note: See the SonicWALL documentation Web site for up-to-date copies of this and all SonicWALL documentation:

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

This guide is divided into the following sections:

- **Supported Platforms**
- **Managing SonicPoints in Managed Mode**
- **Managing the SonicPoint in Stand-Alone Mode**
- **Managing the SonicPoint in SafeMode**
- **Resetting the SonicPoint**
- **SonicPoint Radio Characteristics**

Supported Platforms

This section provides details on the supported platforms for the SonicWALL SonicPoint hardware. The SonicWALL SonicPoint hardware includes:

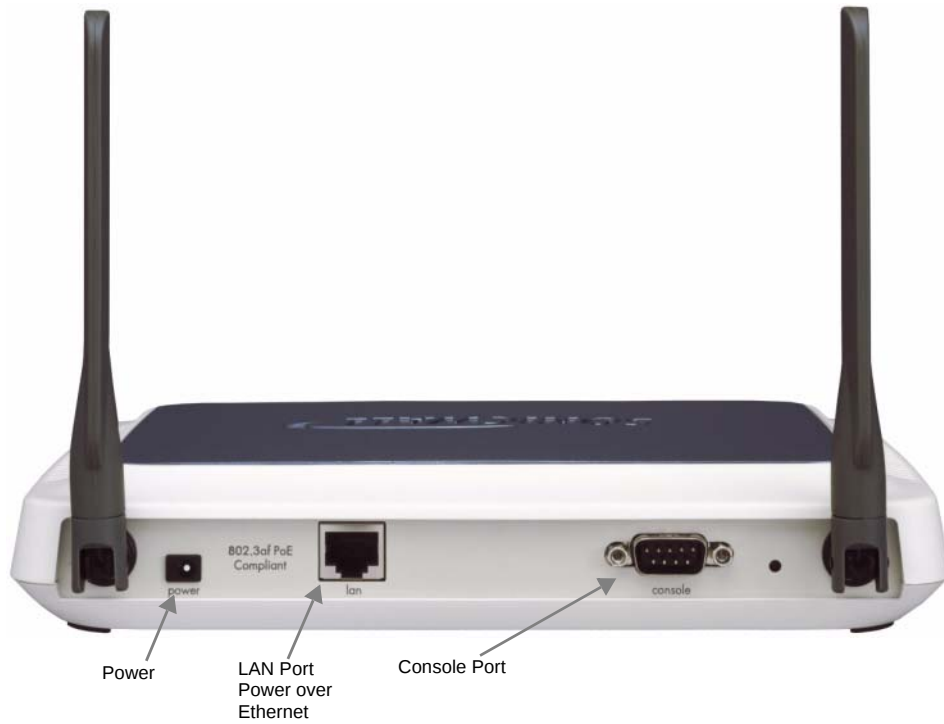
- SonicPoint (IEEE 802.11a/b/g).
- SonicPoint G (IEEE 802.11g/b).

Overview of the SonicWALL SonicPoint Hardware

The SonicPoint contains both 2.4 and 5.0 GHz Radio WLANs. The following figure details the front view of the SonicPoint.



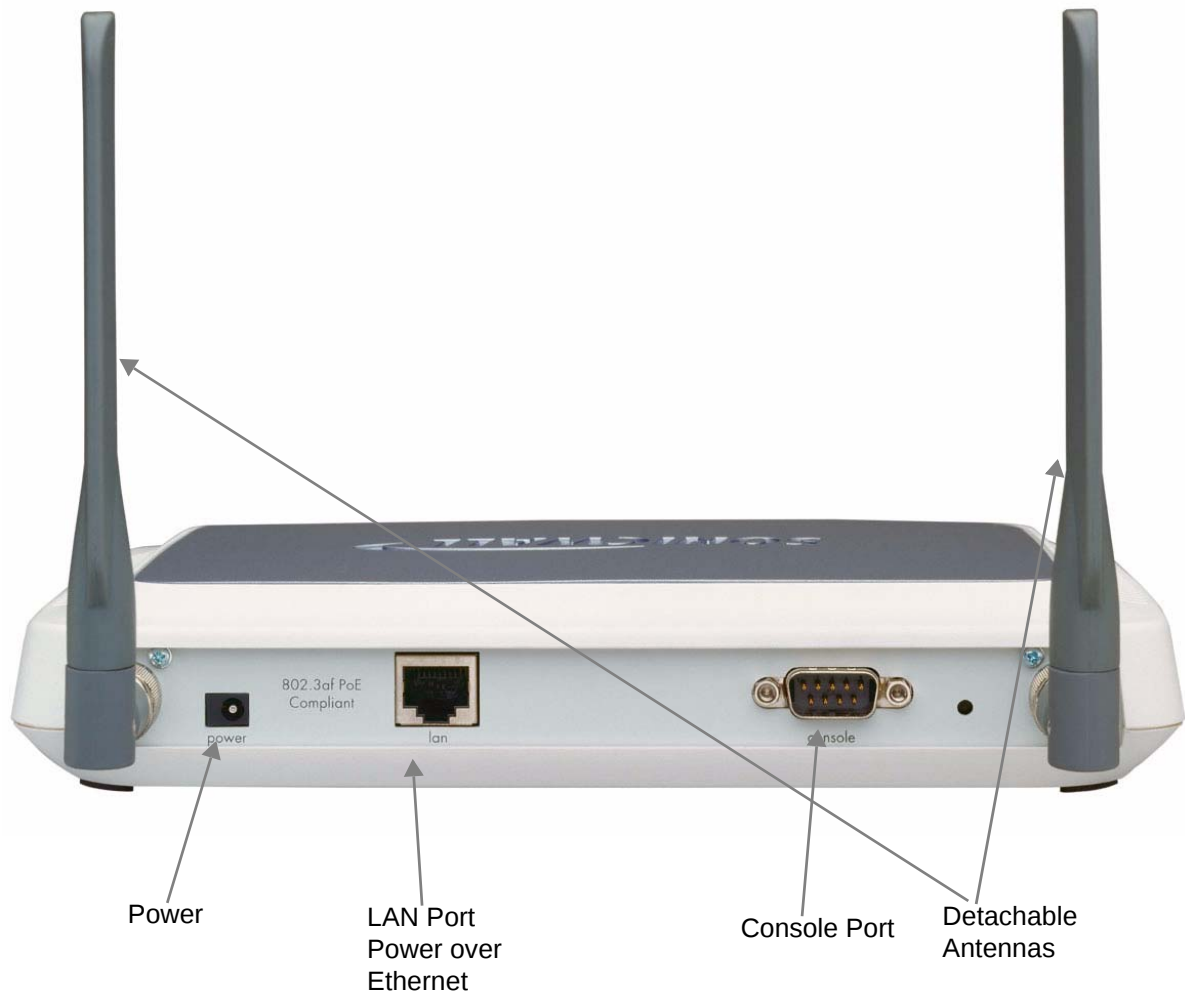
The following figure details the rear view of the SonicPoint 802.11 a/b/g.



The SonicPoint G contains only the 2.4 GHz Radio WLAN. The following figure details the front view of the SonicPoint G.



The following figure details the rear view of the SonicPoint G.



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

- **Power** - The Power LED blinks when the SonicPoint or SonicPoint G is powering up. After the SonicPoint is powered up, the Power LED turns steady.
- **WLAN 2.4 GHz Radio** - The 2.4 GHz Radio LED blinks at a constant rate when the SonicPoint is ready to receive traffic, and blinks at a variable rate while transferring data with connected 802.11g/b stations.
- **WLAN 5.0 GHz Radio** - The 5 GHz Radio LED blinks at a constant rate when the SonicPoint is ready to receive traffic, and blinks at a variable rate while transferring data with connected 802.11a stations.
- **LAN 10/act** - The LAN 10/act LED blinks to indicate 10Mb LAN activity.
- **LAN link** - The LAN link LED illuminates steadily to indicate physical layer connectivity.
- **LAN 100/act** - The LAN 100/act LED blinks to indicate 100Mb LAN activity.

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

- **Power** - Connect the 12.0 volt DC power supply connector to the power port, if you are not using the SonicWALL Power over Ethernet Injector (SonicWALL PoE Injector) through the LAN connector.
- **LAN / PoE** - To connect the SonicPoint to your SonicWALL PRO series security appliance, connect an Ethernet cable to the SonicPoint LAN port. If you are not using the 12.0 volt DC power supply, connect the SonicWALL PoE Injector to the SonicPoint LAN port.

- **Console** - To display bootup and diagnostic messages through the command-line interface (CLI), connect one end of an RS-232 serial cable to the SonicPoint console port and the other end to your work station.



Note: Note that SonicWALL does not support a non-SonicWALL antenna on both the SonicPoint G and SonicPoint a/b/g devices.

SonicPoint Registration

Registering your SonicPoint device is important because it provides you with a direct contact point with SonicWALL. Please be sure you take some time to register the device.

Registering Your SonicPoint

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

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



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

Before you register your SonicPoint, you need to have:

- A mySonicWALL.com account
- A SonicWALL security appliance running SonicOS Enhanced registered with mySonicWALL.com.
- The serial number of your SonicPoint. You can find the serial number on the sticker on the bottom of the SonicPoint.

To register your SonicPoint:

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

The Create Association page displays, showing a list of all security appliances you have registered capable of running SonicOS Enhanced 2.5 and therefore capable of managing a SonicPoint. All appliances are listed as *Governing Appliances*. A governing appliance is an appliance that manages the configuration of a child appliance.

- 6 Select the security appliance that you are managing the SonicPoint with, and click **Continue**.

The Service Management, Associated Products page displays with a summary of the SonicPoint registration and the services installed. **Extended Warranty** and **Support 8X5** are the only services applicable to the SonicPoint, and are installed and activated automatically when you register.

- 7 You can associate SonicWALL Dual Band, Long Range Wireless Cards as child products of the SonicPoint. To associate a wireless card with this SonicPoint, click on **Long Range Wireless Card** under the **Child Product Type** heading.

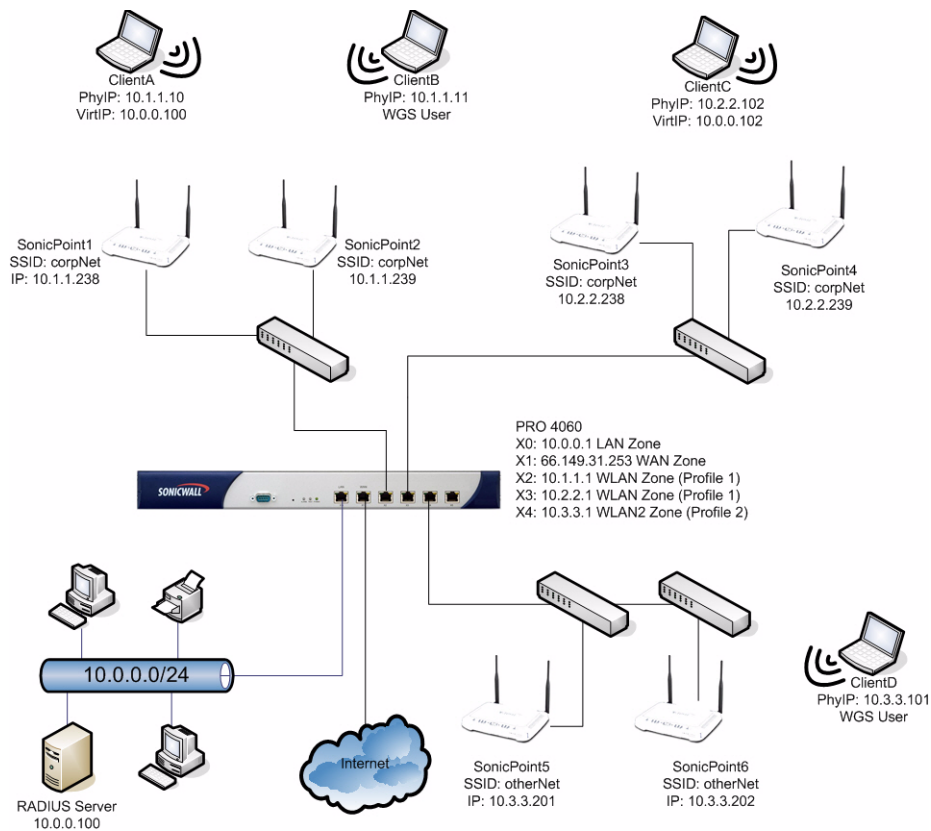
8 In the My Product - Associated Products page, enter the Serial Number and a Friendly Name for a wireless card. and click **Register**.

If the card is already registered with mySonicWALL.com and associated with another SonicWALL product (such as a SonicWALL TZ 170 Wireless), you will prompted and asked if you want to change the association of the child product. Click **Continue** to change the association to the SonicPoint.

9 Click **Logout** in the top-right corner of the mySonicWALL.com page when you are done.

SonicPoint Overview

As the proliferation of wireless networking continues, it becomes increasingly important to support more diverse, and more geographically expansive wireless network configurations. To accommodate wireless installations larger than those that can be serviced by individual SonicWALL wireless security appliances, such as the SonicWALL TZ 170 Wireless, SonicOS Enhanced 2.5 or greater and the SonicPoint work together to act as the center of a distributed wireless network. To extend the reach and intelligence of the core, up to 128 SonicPoint Access Points can be connected to a SonicWALL appliance (the total number of supported SonicPoints is platform dependent) running SonicOS Enhanced 2.5 or greater.



SonicPoint Features

Note that in this manual SonicPoint refers to both SonicPoint 802.11a/b/g and SonicPoint G. While the following table explicitly refers to each platform, the remainder of this manual refers to instances where both are appropriate, simply using the SonicPoint name. The SonicPoint offers the following capabilities:

Feature	Platform
Tri-Mode, Dual-Band, Dual-Radio 802.11a/b/g operation for simultaneous support of 802.11a and 802.11g/b clients	SonicPoint (802.11a/b/g)
Support for 802.11g/b clients	SonicPoint G
WPA and WEP Encryption with EAP-PEAP, EAP-TTLS, TKIP and AES Support	SonicPoint (802.11a/b/g), SonicPoint G
802.11g Turbo Mode for data rates up to 108 Mbps	SonicPoint G
802.11a/g Turbo Modes for data rates up to 108 mbit	SonicPoint (802.11a/b/g)
802.11d compliance	SonicPoint (802.11a/b/g), SonicPoint G
802.3af Power over Ethernet	SonicPoint (802.11a/b/g), SonicPoint G
Managed Mode and Stand-Alone Modes of operation	SonicPoint (802.11a/b/g), SonicPoint G
Rogue Access Point Discovery and BSSID/MAC Address Object Authorization	SonicPoint (802.11a/b/g), SonicPoint G
Safe Mode for recovery	SonicPoint (802.11a/b/g), SonicPoint G

Because of the high throughput capabilities of the SonicPoint, aggregate SonicPoints have the potential to exhaust the capacity of Fast Ethernet interfaces on the security appliance. The following table illustrates—per platform—the maximum number of SonicPoints per interface, and the total recommended number of SonicPoints per appliance:

Managing Security Appliance	Wireless Zone Assignable Interfaces	Recommended # of SonicPoints per WLAN Interface	Recommended # of SonicPoints per Security Appliance
SonicWALL TZ Series 170 Series	1 Fast Ethernet	2 SonicPoints	2 SonicPoints
SonicWALL PRO Series 1260	1 Fast Ethernet*	4 SonicPoints	8 SonicPoints
SonicWALL PRO Series 2040	2 Fast Ethernet	4 SonicPoints	8 SonicPoints
SonicWALL PRO Series 3060	4 Fast Ethernet	8 SonicPoints	16 SonicPoints
SonicWALL PRO Series 4060	4 Fast Ethernet	16 SonicPoints	32 SonicPoints
SonicWALL PRO Series 5060	4 Fast/Gig Ethernet	32 SonicPoints	64 SonicPoints

** Any of the 22 assignable interfaces can be a Port Shield interface, but the restriction of eight total SonicPoint devices for the entire device still applies.*

SonicPoint Modes of Operation

SonicPoint devices can operate in two modes, namely, Stand-Alone Mode and Managed Mode. The mode of operation is automatically selected by the SonicPoint depending on its environment. When the SonicPoint starts up, it will announce itself using SDP (SonicWALL Discovery Protocol) Advertisement broadcasts. If it has a layer 2 attachment to a Wireless Zone interface on a SonicWALL (for example, connected directly, using a hub, or using a switch) the security appliance and the SonicPoint will negotiate a peer-relationship, and the SonicPoint will enter Managed Mode. Once a peer relationship has been established, a SonicPoint will remain wedded to its peered SonicWALL so as to prevent conflicts in the event of multiple SonicWALL security appliances sending SDP on a single segment. The peering can be manually broken from the SonicOS GUI, and peer relationships can also be imposed using manual synchronization from the SonicOS GUI.

If the SonicPoint cannot discover or be discovered by a security appliance within 5 seconds of startup, it will reboot into Stand-Alone Mode. When operating in Stand-Alone Mode, the SonicPoint will assume a default IP address of **192.168.1.20**, a default username of **admin**, and a default password of **password**. SonicPoints maintain their Stand-Alone and Managed Mode configurations separately so that they do not conflict with, or overwrite one another.

SonicPoints will dynamically transition from one mode to the other in response to environmental changes. For example, if a SonicPoint starts in Stand-Alone Mode, but is then plugged into a Wireless Zone, it will respond to SDP Discovery packets from the security appliance and will transition to Managed Mode. Alternatively, if the SonicPoint is operating in Managed Mode and it loses its connection with the security appliance for 6 minutes, it will transition to Stand-Alone Mode. The SonicPoint reboots when it changes operating modes. Rebooting takes approximately 1 minute.

When operating in Stand-Alone Mode, the SonicPoint will function much like a conventional Access Point, configurable using its integrated Web-based GUI. The SonicPoint Stand-Alone UI has been modeled after the SonicOS UI, but it does not precisely match the SonicPoint configuration interface within SonicOS. Like other generation-four SonicWALL devices, the SonicPoint features SafeMode to

facilitate recovery from compromised states of operation. When the SonicPoint is operating in SafeMode, it will be possible to upload a new firmware image using FTP. This is different from SonicOS devices which use an HTTP POST for firmware uploads. Under normal conditions, it will not be necessary to manually update firmware using with FTP on the SonicPoint. SonicPoint firmware is embedded within SonicOS and updates are automatically performed while operating in Managed Mode as part of the auto-provisioning process.

Operating in Managed Mode requires L2 connectivity to a security appliance interface assigned to a Wireless Zone. The Wireless Zone type has certain unique characteristics:

- Additional configuration tabs for 'Wireless' and 'Guest Services'. The 'Wireless' and 'Guest Services' tabs have the following default settings:
 - ♦ WiFiSec Enforcement Enabled.
 - ♦ Require WiFiSec for Site-to-Site VPN Tunnel Traversal.
 - ♦ Trust WPA traffic as WiFiSec.
 - ♦ SonicPoint Provisioning Profile set to 'SonicPoint.'
 - ♦ Wireless Guest Services Disabled.
- Enforces that all traffic that enters the zone arrive from a SonicPoint. All other traffic will be dropped (i.e. traffic from wired network systems, or wireless traffic originating from a non-SonicPoint device). You cannot use a third-party wireless Access Point device in a Wireless Zone.
- The only Zone type on which SDP and SSPP operate.
- The only Zone type on which Guest Services, and WiFiSec enforcement is available.
- The size of the subnet mask will vary with the number of SonicPoint devices available. For more details on this, see the following section.
- A DHCP scope will be activated on Wireless Zones, and based on the platform, the top range of addresses will be reserved for SonicPoints. Refer to the table on page 3 for platform specific numbers.
- The IP Address assigned to the Wireless Zone interface may not conflict with the SonicPoint address reservations described above (for example, for a /24 subnet on a PRO4060, the assigned address must be .238 or below).
- The WLAN GroupVPN (the default Wireless Zone) will NOT be activated by default, due to the fact that an interface must first be added to correctly auto-create Access Rules. The WLAN GroupVPN must be manually activated, and upon activation will employ the following WiFiSec optimized default settings:
 - ♦ HTTP and HTTPS Management using this SA Enabled.
 - ♦ Require authentication of VPN clients using XAUTH.
 - ♦ User Group for XAUTH Users set to Trusted Users.
 - ♦ Cache XAUTH User Name and Password on Client set to Single Session.
 - ♦ Allow Connections to All Secured Gateways.
 - ♦ Set Default Route as this Gateway.



Note: *In SonicOS Enhanced, WLAN is the default instance of the Wireless zone type. You can modify the WLAN zone or create a new zone of the Wireless type.*

When in Managed Mode, operating parameters for SonicPoint units will be controlled by the peered SonicWALL security appliance. If a security appliance discovers a SonicPoint for which it has no stored configuration, it will consider that SonicPoint to be unprovisioned, and it will use the Zone's assigned SonicPoint Profile to auto-provision the SonicPoint. This can occur in the following cases:

- The SonicPoint had never been previously provisioned.
- The SonicPoint had been provisioned, but was manually deleted using the SonicOS GUI.
- The SonicPoint was provisioned by one security appliance, and then moved to a different security appliance that contains no stored configuration for that SonicPoint.

As part of the provisioning process, the security appliance will store the configuration for that SonicPoint, and will push the configuration to the SonicPoint using SSPP (SonicWALL Simple Provisioning Protocol). Upon receiving the configuration, the SonicPoint will update its configuration, will reboot to affect the changes, and will enter an *operational* state. While still peered with the same security appliance, changes to that SonicPoint's configuration will only be possible using the SonicOS GUI, and must be performed at the unit (as opposed to the Profile) level.

While in Managed Mode, the SonicPoint will report its state to the security appliance using SDP packets. A full description of SonicPoint state information can be found in the 'SonicPoint States' section of this document. Also included in the SDP packets sent by *operational* SonicPoint devices is a checksum value for its configuration. If the security appliance determines from the checksum that there is a disagreement between its configuration checksum for that SonicPoint and that SonicPoint's advertised checksum, it will engage an encrypted SSPP channel with that SonicPoint, and will send it the proper configuration. The SonicPoint will then reboot to assume the corrected configuration.

It is important to note that changing a SonicPoint Profile on the security appliance will not update operational SonicPoint units. This is by design, so as to allow Profiles to be added, deleted, and modified with interrupting network operation. SonicPoint Profiles will only affect an unprovisioned SonicPoint device, that is, a SonicPoint for which security appliance has no stored configuration. Changing the configuration on an operational SonicPoint requires modification to that SonicPoint's settings (under *Wireless > SonicPoints > SonicPoint Settings*). Alternatively, it is possible to delete the SonicPoint peering from the SonicOS GUI, thus forcing a new auto-provisioning process using the appropriate SonicPoint Profile.

Number of Subnets Supported

The following table indicates the size of a subnet allowed depending on the number of SonicPoint devices available.

SonicPoints per Interface	Maximum Subnet Mask	Total Usable IP Addresses	Available Client IP Addresses
No SonicPoints	30 bits - 255.255.255.252	2	2
2 SonicPoints	29 bits - 255.255.255.248	6	3
4 SonicPoints	29 bits - 255.255.255.248	6	1
8 SonicPoints	28 bits - 255.255.255.240	14	5
16 SonicPoints	27 bits - 255.255.255.224	30	13
32 SonicPoints	26 bits - 255.255.255.192	62	29

Wireless Zones: The WLAN Zone

The Wireless Zone type has been added to existing Zone types (Trusted, Untrusted, Public, Encrypted, Multicast) to provide support to SonicPoint Access Points. The default Wireless Zone instance will be the "WLAN Zone."

Interfaces assigned to a Wireless Zone will have the following important and unique characteristics:

- **SonicPoint Enforcement:** As traffic passes from wireless clients through a SonicPoint, the SonicPoint will tag the traffic so that it will be identifiable by a Wireless Zone interface. If the Wireless Zone interface receives traffic that has not been appropriately tagged, it will discard the traffic.
- **Wireless Firewalling:** The next-generation of the Inter-client Communications. The ability to apply firewall Access Rules and Security Services to all wireless client traffic, even client-to-client traffic through a single or multiple SonicPoints.

- **WiFiSec Enforcement:** The ability to require that all traffic that enters into a Wireless Zone interface be either IPSec traffic, WPA traffic, or both.
- **Guest Services:** Guest Services will only be available on interfaces belonging to a Wireless Zone. Recent Guest Services enhancements include Profiles for automated account generation, customizable post-authentication landing page, SMTP Redirection, and the integration of Guest Services accounts and local user accounts and groups.
- **SonicPoint Profiles:** The ability to define profiles containing the complete set of SonicPoint parameters that can be assigned to a Wireless Zone, and inherited by any connected SonicPoint.
- **Automatic SonicPoint Provisioning:** Utilizing the newly developed SonicWALL Discovery Protocol (SDP) and SonicWALL Simple Provisioning Protocol (SSPP) SonicPoints will be automatically updated with the latest firmware and configurations by their managing SonicWALL appliance.
- **NAT Policy Enforcement:** A Wireless zone can only be configured with NAT enabled. When you create a Wireless zone, or assign an interface to the WLAN zone, SonicOS automatically creates a NAT policy for it.

SonicPoint Enforcement

SonicPoint Enforcement is automatically enabled on all Wireless Zones, but can be overridden by deselecting the enforcement option in the wireless portion of the configuration environment for the WLAN zone in SonicOS 3.0 and greater. The enforcement feature requires that any traffic that enters into a Wireless Zone be delivered using a SonicPoint. When not overridden, traffic cannot pass from an industry-standard Access Point, or even from a wired host through a Wireless Zone. Therefore, only SonicPoints should be connected to Wireless Zone interfaces, either directly or through a switch or hub. Layer 2 connectivity between SonicPoints and the managing SonicWALL appliance is required.

Wireless Zone interfaces will automatically recognize when a SonicPoint has been connected using the SonicWALL Discovery Protocol (SDP). SDP will then conjoin the SonicPoint to the SonicOS Enhanced enabled SonicWALL PRO Series security appliance or SonicWALL TZ Series security appliance that first discovered it, making it its peer (to protect against the event of a SonicPoint being on an L2 segment with more than one PRO). Once peered, SDP will negotiate encryption parameters and will determine the configuration state of the SonicPoint. If the configuration state is validated by the PRO, the SonicPoint will immediately enter into an operational state.

Whenever the operating system on the SonicPoint is out of sync with the OS on the PRO-series device, the SonicWALL PRO Series security appliance uses the SonicWALL Simple Provisioning Protocol (SSPP) and reconfigures the SonicPoint as needed. For example, if you upgrade the firmware in the PRO-series device to a newer version. The SonicWALL PRO Series security appliance automatically detects that the SonicPoint is out of sync and provisions the SonicPoint with updated firmware.

Enabling Traffic from Non-SonicPoint Devices

In prior versions of SonicOS Enhanced, when an interface was assigned to a Wireless Zone, that interface would only accept traffic that arrived through a SonicPoint. This provided the benefit of ensuring that all wireless communications were secure. To accommodate the need to integrate SonicPoints into existing networks where SonicPoint devices would be installed on the same physical segment as existing wireless nodes, administrator control has been provided over the application of SonicPoint Enforcement. SonicOS Enhanced 3.1 for SonicPoint now provides an option that provides two options for the device:

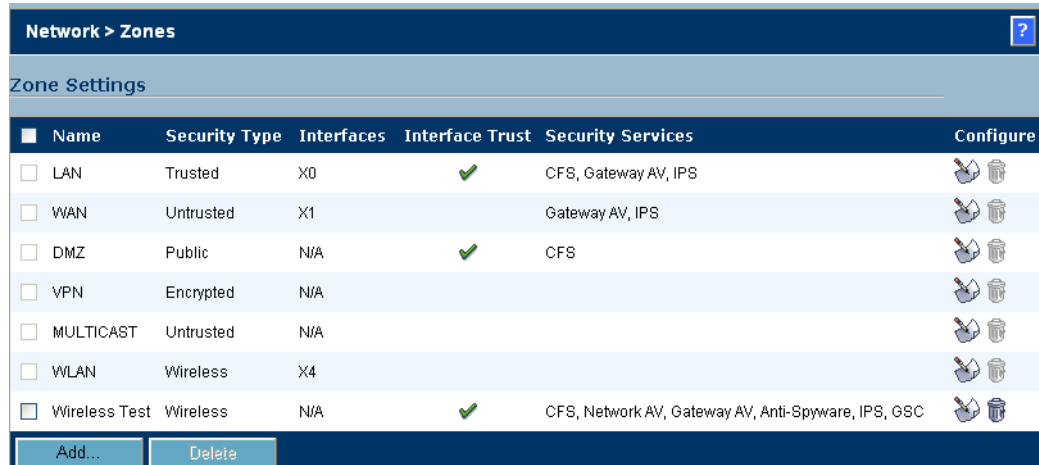
- it allows traffic only generated by a SonicPoint device.
- it allows traffic generated by a non-SonicWALL access point device.

To accommodate the need to integrate SonicPoints into existing networks where SonicPoints would be installed on the same physical segment as existing wired nodes, administrator control has been provided over the application of SonicPoint enforcement. By default, this option is enabled, providing the same behavior as previous SonicOS releases. Deselecting this option allows for all the interfaces in that Wireless Zone to accept either SonicPoint-sourced traffic, as well as traffic sourced from any other host. Packets will continue to be tagged as they pass through the SonicPoint.

Providing the ability to allow traffic from another device is a new feature that gives you great flexibility because:

To configure this option, perform the following steps:

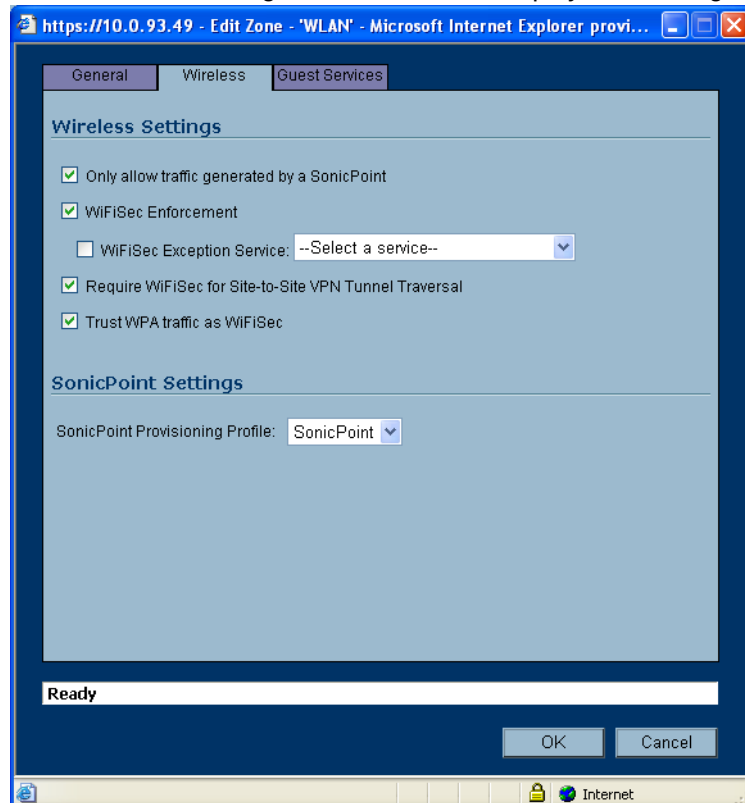
- 1 Log into the SonicWALL security device that is managing the SonicPoint device.
- 2 Go to the Zones page under the Network > Zones location.



The screenshot shows the 'Network > Zones' page in the SonicWALL management interface. It features a table with columns: Name, Security Type, Interfaces, Interface Trust, Security Services, and Configure. The table lists several zones: LAN, WAN, DMZ, VPN, MULTICAST, WLAN, and Wireless Test. The WLAN zone is highlighted, and its 'Configure' icon is visible.

Name	Security Type	Interfaces	Interface Trust	Security Services	Configure
LAN	Trusted	X0	✓	CFS, Gateway AV, IPS	
WAN	Untrusted	X1		Gateway AV, IPS	
DMZ	Public	N/A	✓	CFS	
VPN	Encrypted	N/A			
MULTICAST	Untrusted	N/A			
WLAN	Wireless	X4			
Wireless Test	Wireless	N/A	✓	CFS, Network AV, Gateway AV, Anti-Spyware, IPS, GSC	

- 3 In the WLAN Zone, click on the Configure icon. SonicOS displays the Configure dialog box.



- 4 Click on the Wireless tab. By default, the Only allow traffic generated by a SonicPoint checkbox is enabled.

- 5 Click on this checkbox to deselect the option. By deselecting Only allow traffic generated by a SonicPoint, you are allowing for all the interfaces in this wireless zone to accept traffic that originates either from a SonicPoint or other device.
- 6 The SonicPoint device can now receive traffic from a non-WLAN device.

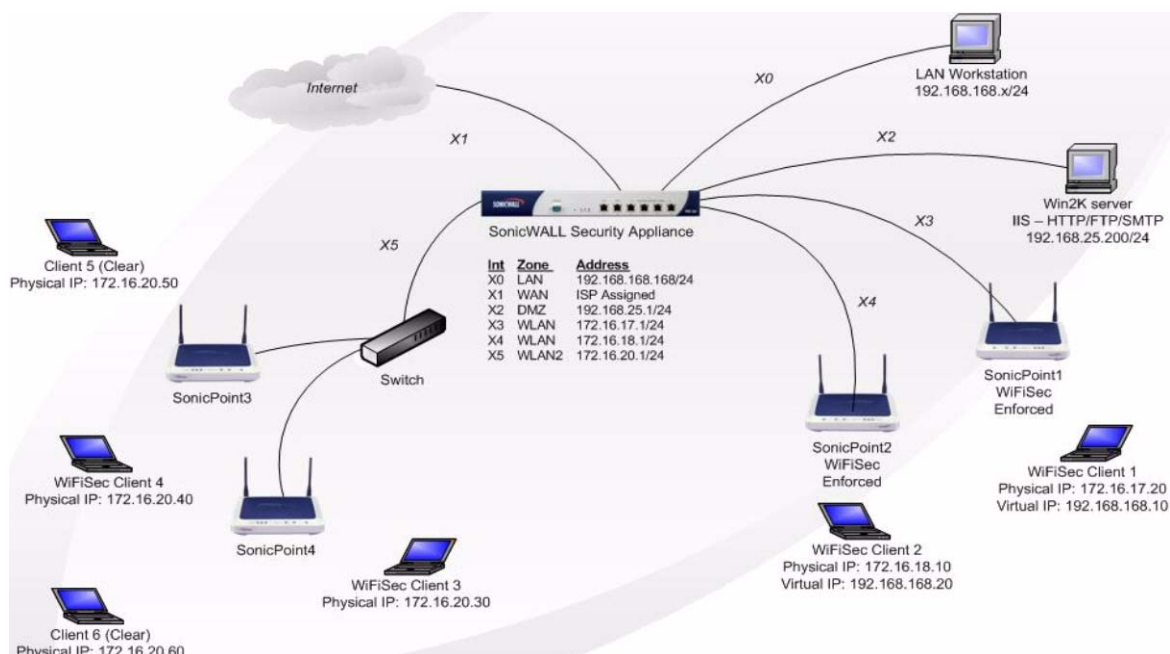
Wireless Firewalling

Some high-end wireless Access Points provide the ability to control wireless Inter-client Communications, meaning they can allow or disallow wireless clients connected to that particular Access Point from communicating with each other. These Access Points, however, generally cannot directly control a wireless client's communication with a remote host, such as a wired client, an Internet host, or even a wireless client associated with another Access Point.

The Inter-client communication control feature on the SonicWALL TZ Series 170 Wireless took this control a step further by consolidating the Access Point, Secure Wireless Gateway and the Firewall into a single unit--providing full firewall Access Rule applicability to all wireless traffic on that individual unit.

Wireless Firewalling within the Secure Wireless Solutions/Architecture provides this same level of granular control, only in a highly scalable, distributed fashion. It is a function of a design innovation wherein all traffic that enters the wireless interfaces on a SonicPoint is forwarded back to the managing SonicWALL security appliance where it can be processed by firewall Access Rules, NAT Policies, and Security Services. While in Managed Mode, Wireless Firewalling allows no direct communication between an affected wireless client and any other host, whether connected to the same or a different SonicPoint, or whether wireless or wired; all traffic must traverse the firewall. This can be used, for example, for the following application:

- To control access for all wireless inter-client communications.
- To control access for certain wireless client communications with other wireless clients.
- To control access for wireless client communications with wired hosts, or Internet hosts.
- To control access using Service Objects.



Access Rules for Wireless clients are controlled using Zone based intersections and applicable Address Objects. Consider the following examples from the illustration above (Address Objects used are generalized by subnet, and can be made more specific):

Address Object	Type	Address	Netmask	Bound to Zone
192.168.168.0	Network	192.168.168.0	255.255.255.0	VPN
172.16.17.0	Network	172.16.17.0	255.255.255.0	VPN
172.16.18.0	Network	172.16.18.0	255.255.255.0	VPN
172.16.20.0	Network	172.16.20.0	255.255.255.0	VPN

From Host	To Host	From Zone	To Zone	Source Address Object	Destination Address Object
Client 1	Client 2	VPN	VPN	192.168.168.0	192.168.168.0
Client 3	Client 4	VPN	VPN	172.16.20.0	172.16.20.0
Client 2	Client 3	VPN	VPN	192.168.168.10	172.16.20.0
Client 5	Client 6	WLAN2	WLAN2	WLAN2 Subnets	WLAN2 Subnets
Client 6	LAN Workstation	WLAN2	LAN	WLAN2 Subnets	LAN Subnets

Default levels of trust for Wireless Zones are as follows:

From Zone	To Zone Type	Action
Trusted	Wireless	Allow
Untrusted	Wireless	Deny
Public	Wireless	Deny
Wireless	Trusted	Deny
Wireless	Untrusted	Allow
Wireless	Public	Allow
Wireless	Wireless	Interface Trust
Wireless (custom)	Wireless	Deny
Encrypted (WiFiSec)	Trusted	Allow
Encrypted (WiFiSec)	Untrusted	Allow
Encrypted (WiFiSec)	Public	Allow
Encrypted (WiFiSec)	Wireless	Allow

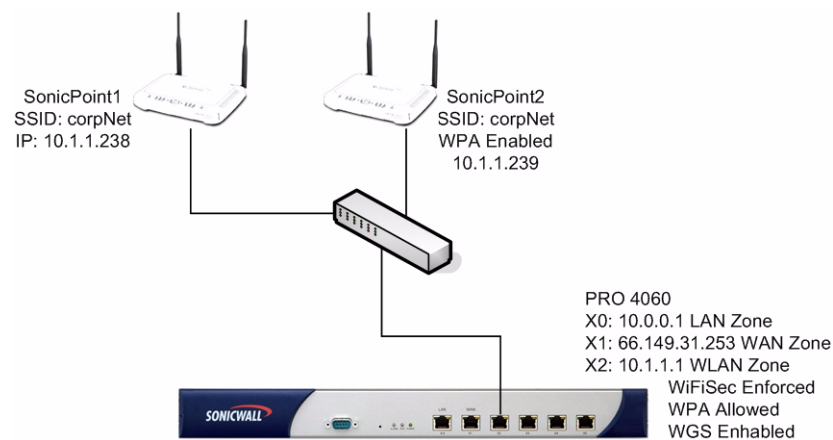
WiFiSec clients are terminated at the 'WLAN GroupVPN' (or custom Wireless Zone GroupVPN) are associated with the VPN (Encrypted) Zone. By default, the 'WLAN GroupVPN' enables the 'Set Default Route as this Gateway' option (see page 5 for default settings), but VPN Access must still be

assigned at the User or Group level (such as to 'WLAN RemoteAccessNetworks', which is effectively '0.0.0.0' or 'Any') for access to the Internet and trusted resources.

Access types not covered by the default levels of trust (such as WiFiSec to WiFiSec) will require custom Access Rules, and changes to the above default behaviors can be made more or less restrictive by modifying the default rules.

WiFiSec Enforcement / WPA

As introduced on the SonicWALL TZ 170 Wireless, WiFiSec Enforcement is the ability to require that all traffic that traverse the wireless network be IPSec (VPN) traffic. We will be able to enforce the same level of security with the Secure Wireless Solutions/Architecture by providing WiFiSec Enforcement at the Zone level; all non-guest wireless clients connected to SonicPoints attached to an interface belonging to a Zone on which WiFiSec is enforced will be required to use the strong security of IPSec. The VPN connection will terminate at the "WLAN GroupVPN", which can be configured independently of "WAN GroupVPN" or other Zone GroupVPN instances.



Sensitive to the fact that WPA (WiFi Protected Access) provides security rivaling that of WiFiSec, albeit in a more complicated and less versatile fashion, administrators enabling WiFiSec Enforcement on a Wireless Zone will have the option to accept WPA as an allowable alternative to IPSec. Both WPA-PSK (Pre-shared key) and WPA-EAP (Extensible Authentication Protocol using an external 802.1x/EAP capable RADIUS server) will be supported on SonicPoints.

Consider the above example where there are two SonicPoints connected to the WLAN Zone where WiFiSec is enforced. SonicPoint1 does not have WPA enabled, but WPA is enabled and is 'Trusted as WiFiSec' (meaning it has been allowed as an acceptable alternative to WiFiSec) on SonicPoint2. Non-Guest clients that are connected to SonicPoint1 will have to use IPSec to communicate through the X2 interface on the PRO, or the traffic will be dropped at the interface. Guest clients will be able to associate with SonicPoint1, and use Guest Services. Because WPA is enabled on SonicPoint2, clients connecting to SonicPoint2 *must* use WPA, since WPA is an all-or-nothing technology. This means that Guest clients will either have to have WPA credentials, or they will not be able to associate with SonicPoint2. Once a client provides WPA credentials and successfully associates with SonicPoint2, as traffic passes from SonicPoint2 to the X2 interface, SonicPoint2 will tag the packets as having been transmitted using WPA. The X2 interface will recognize these tags, and will accept the traffic, even if it is not IPSec.

The all-or-nothing restriction of WPA, along with the added complexity of having to maintain an external EAP capable directory service, is perhaps the greatest drawbacks of WPA as compared to WiFiSec. Take, for example, a wireless network wishing to simultaneously offer Guest Services to visiting users and encryption enforcement for access to trusted resources. This combination of differentiated access could easily be afforded by SonicPoint1 using WiFiSec, but Guest users connecting to SonicPoint2 would require the WPA pre-shared key or a previously created EAP account, effectively defeating the extemporaneous and dynamic nature of Guest Services.

WiFiSec Enforcement and the *Trust WPA Traffic as WiFiSec* settings are only available on Wireless Zones. Because Wireless Zones only accept SonicPoint traffic, only SonicPoints can provide this feature; it is not possible to provide this security feature with any other WPA-capable OTS Access Point.

Wireless Roaming

As wireless clients move through a distributed wireless network, it is necessary to support roaming from one SonicPoint to another in as non-interruptive a manner as possible. The SonicWALL Secure Wireless Solutions/Architecture was designed such that client connections, even across multiple SonicPoint Access Points, traverse a single point--whether it is the physical interface on the SonicOS device, or a Virtualized Adapter using the Global VPN Client (GVC). This method helps to ensure that even as a client moves through the wireless network in nomadic fashion that applications will experience minimal if any interruption, providing a virtually seamless wireless client experience.

Roaming decisions are made by the wireless client, and are done so in a non-prescribed fashion, meaning that different wireless client card vendors can implement different types of roaming decision algorithms. Generally, the roaming process involves the following components:

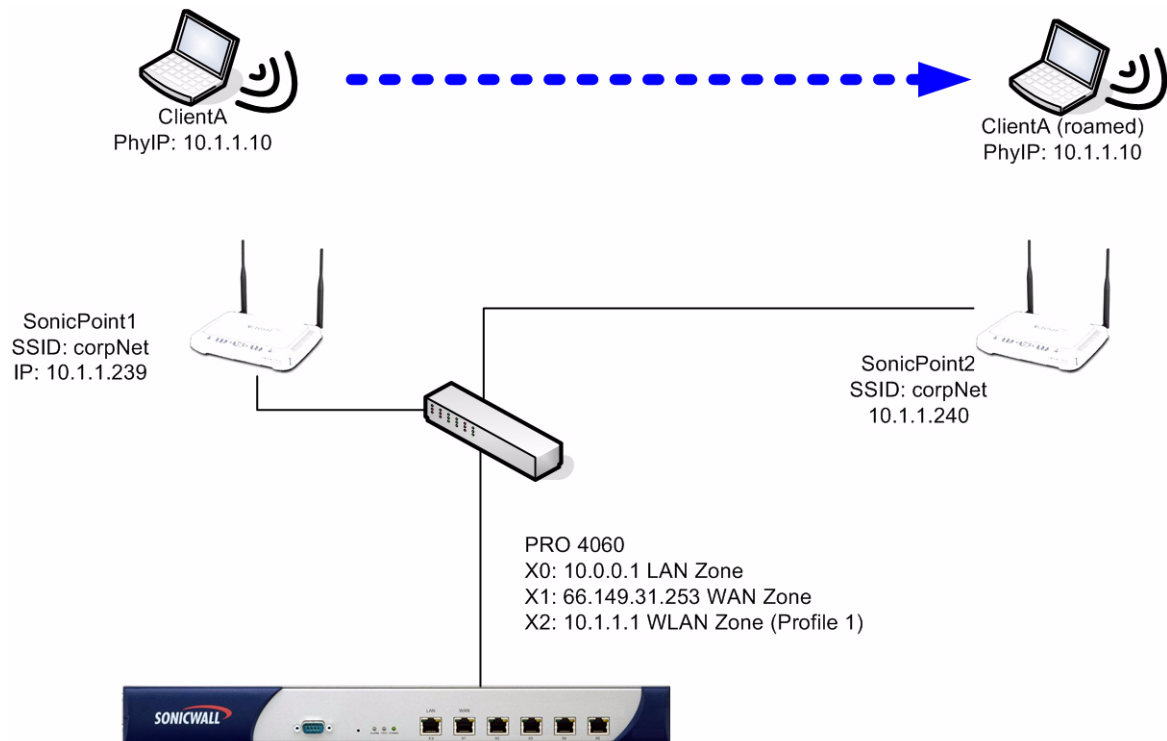
- The client decides to roam: When the wireless device moves or the signal strength changes for some reason, the client enters into a roaming state based on such factors as signal strength, missed beacons, or acknowledgements, the client will enter into a roaming state.
- The client determines where to roam: Once the client has decided to roam, it must then decide where to roam to. Finding an eligible Access Point to roam to is accomplished using some sort of scanning technique, either active or passive, and the scan may be performed either preemptively (before the decision to roam) or reactively (after the decision to roam). The scanning technique employed may or may not affect the client's ability to send and receive data during the scanning process. This varies from vendor to vendor. Some clients cleverly employ power-saving to make this process more seamless--they signal the Access Point to which they're attached that they are entering a Power-Save Mode before starting the scanning process. The client and Access Point then attempt to queue data for the "sleeping" client. During this respite, the client performs its scan. When the client finds a new Access Point, it wakes up, and exchanges queued data with the Access Point.
- The client roams: by de-associating with the old access point, and re-associating with the new access point. Layer 2 connectivity is severed and re-established during this process.
- The client's applications resume: Layer 3 (and higher) communications can resume after layer 2 connectivity is restored. The effect this has on the continuity of the application depends on whether the application is connection-oriented (such as a telnet or SSH session), or stateless (such as Web-browsing). Connection-oriented applications will generally be interrupted by roaming while stateless applications will exhibit no ill-effects. Many client-server applications, such as a Microsoft Outlook client connection to an Exchange Server, use higher layer logic to automatically re-establish the client-server connection after layer 2/3 connectivity is restored, and these will operate with relative seamlessness.

There are many factors that can affect the roaming process, and the effect it will have on the user application. For example, using WPA introduces additional latency as a result of the 4-way handshake that must occur during association or re-association with the new Access Point. Latency can introduce a significant amount of interruption, especially to connection-oriented or streaming/multimedia applications.

Roaming from one Access Point to another can occur across different boundaries, within the same layer 2 segment, across layer 2 segments, and across layer 3 segments. Generally, remaining within the same layer 2 segment while roaming presents the least potential for interruption, crossing layer 2 segments presents more, and crossing layer 3 segments presents the most.

Roaming Within Layer 3 Boundaries

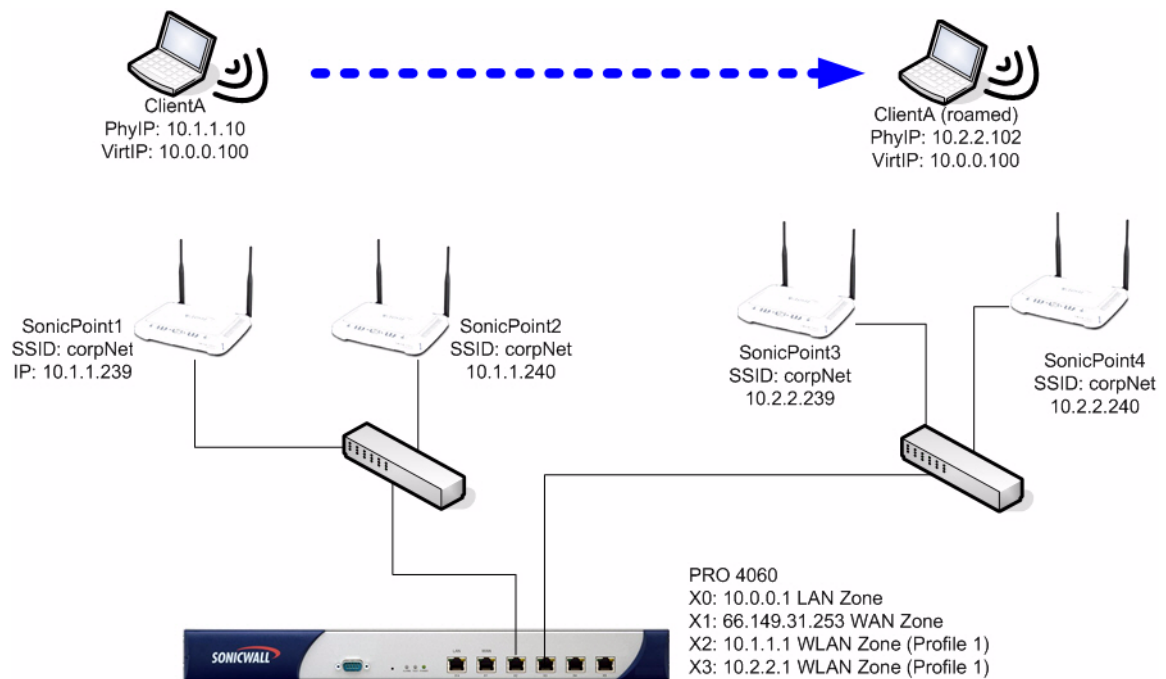
In configurations where a single SonicPoint or multiple SonicPoints are connected to a single interface on a SonicWALL security appliance, roaming (under most circumstances) will be seamless to the user since the client connection is terminated at the security appliance's interface rather than at the individual SonicPoint. Consider the following configuration:



In the above configuration, the WLAN Zone has Wi-FiSec enforced, but the 'WLAN GroupVPN' does not have 'Use DHCP to obtain Virtual IP for this Connection' enabled. ClientA associates with SonicPoint1, and received a DHCP lease of 10.1.1.10. All wireless traffic entering SonicPoint1 traverses the X2 interface. As ClientA moves through the network, the wireless client adapter will at some point make a decision to roam to SonicPoint2. Upon doing so, the wireless client adapter will preserve the same DHCP lease (10.1.1.10) and in most cases, there should be no perceptible interruption to traffic.

Roaming Across Multiple SonicWALL Interfaces

If it becomes necessary or desirable to span a contiguous network of SonicPoints across multiple interfaces on a SonicWALL security appliance, the effects of roaming across L3 boundaries can be mitigated by using the GVC with the Virtual Adapter option:



The illustration above depicts a wireless client (ClientA) associated with SonicPoint1. SonicPoint1 is attached to SonicWALL PRO Series security appliance port X2 occupying address space 10.1.1.x/24. A DHCP Server is active on X2, and has provided a lease of 10.1.1.10 to ClientA. ClientA has a WiFiSec connection to the PRO, and a Virtual Adapter lease of 10.0.0.100 from the X0 (LAN) scope.

As ClientA moves from SonicPoint1 to SonicPoint2, both of which use the same SSID (corpNet), roaming occurs within the same L2 segment. When ClientA re-associates, the physical adapter IP address (10.1.1.10) will remain the same, as will the Virtual Adapter address (10.0.0.100). The GVC client will automatically re-establish the WiFiSec connection, and all but the most sensitive connection-oriented applications will continue without perceptible interruption.

If ClientA continues to move through the distributed wireless network, roaming from SonicPoint2 to SonicPoint3, roaming will cross both L2 and L3 boundaries. When ClientA associates with SonicPoint3, the physical adapter IP address will change to a lease from the scope on the X3 interface (for example, 10.2.2.102), but the Virtual Adapter address will remain the same (10.0.0.100). Through the use of the GVC with the Virtual Adapter, the roaming process can be made significantly less interruptive.

Guest Services

Guest Services are designed to provide guest users with wireless access to public resources, such as the Internet, or a number of “walled-garden” (explicitly allowed) sites. Adding to the capabilities of WGS on the SonicWALL TZ Series 170 Wireless, the Guest Services feature on the SonicOS Enhanced offers:

- Profiles to allow for template based account generation.
- Bulk Account generation to create multiple accounts at once.
- Limited Admin access to Guest Services management pages.
- Integration of Guest Services user accounts into the Local User/Group account structure.

Guest Services controls on SonicOS Enhanced 2.5 will be integrated into the Zone configuration pages, and will be uniquely configurable on every Wireless Zone instance. In other words, it will be possible to provide WGS on a user created “Working Zone” while not providing guest access on the default “WLAN Zone”, or to provide one set of Guest Services options on one Wireless Zone, and a completely different set of options on another.

In addition to providing the ability to accept wired traffic, disabling SonicPoint enforcement has the additional benefit of being able to provide Wireless Guest Services to wired hosts. All features of Wireless Guest Services will function for wired guests exactly as they do for wireless guests, including authentication page redirection and Lightweight Hotspot Messaging (LHM) and DAT.

Inter-guest Communications

The option to enable inter-guest communications allows for Guest Services users to communicate with each other for the purpose of peer-to-peer networking, WiFi VoIP communications, gaming, etc. Inter-guest communications controls occur at the Wireless Gateway layer, below the Firewall Access Rules, and will not manifest itself in the Access Rule table. If IP addresses are known or predictable, it will still be possible to create Access Rules to further control Guest user traffic. DAT (Dynamic Address Translation) Guest users will not be able to communicate with each other, regardless of Inter-guest Communication settings.

Dynamic Address Translation

Dynamic Address Translation allows for Guest clients to use any IP addressing scheme and DNS settings rather than requiring them to reside on a pre-scribed L3 subnet. This allows for statically addressed guests to use Guest Services without having to reconfigure their client settings.

Bypass Guest Authentication

Bypass Guest Authentication can be enabled for the “All MAC Addresses” address object, providing un-authenticated Guest Services access to all users, or MAC Addresses can be specified (individually as a group) to provide unauthenticated Internet access to certain Stations. This is useful in providing Internet access to pre-defined users, or to devices that lack the ability to authenticate (such as WiFi-SIP VoIP phones, or other browser-less wireless networking devices).

Customizable Authentication Pages

It is possible to define either an external URL or text/html-based header and footer information the authentication page for users authenticating on a Wireless Zone interface rather than presenting the default SonicWALL auth.html authentication page. This allows for the sort of customizability required for hotspot, business, or hospitality environments. It is also now possible to define a post-authentication page, that is, a page to which the user will be automatically redirected after successful authentication. This can be used to present such things as usage policy information or custom portal pages.

SMTP Redirection

In a hotspot or hospitality environment, users with variously configured SMTP settings will visit, and will expect the same network experience as they have at home or at work. An obstacle to this sort of transparency is the fact that many ISP's only allow connections to their SMTP servers from source IP addresses that fall into their own ranges of IP addresses. This security mechanism, or the much more prevalent (although unfortunately not yet ubiquitous) prevention of SMTP relaying will prevent hotspot users from sending e-mail using SMTP when connecting from the IP address of the hotspot provider.

To solve this problem, SMTP Redirection intercepts and translates all outbound SMTP (TCP port 25) traffic to a server that can be defined by the hotspot operator. This server is then be used to send outbound e-mail for all hotspot visitors, regardless of their client software configurations.



Note: The potential for using this sort of arrangement for spamming must be mitigated by anti-spam software running on the mail server, or on some security (anti-spam) gateway or appliance.

Enabling External Guest Services

In addition to providing the ability to accept non-SonicWALL wireless traffic, disabling SonicPoint enforcement has the additional benefit of being able to provide Wireless Guest Services (WGS) to wired hosts. All features of WGS function for wired guests exactly as they do for wireless guests, including authentication page redirection and Lightweight Hotspot Messaging, and DAT.

To configure guest services for wireless, click on the Enable External Guest Authentication checkbox. This enables external authentication if you are configuring from a centralized point if you want all remote sites to connect to one central management server.,



Note: For more details, see *Lightweight Hotspot Messaging* documentation available on

http://www.sonicwall.com/support/sohotzw_documentation.html

MAC Filtering Using MAC Address Objects

MAC filtering has long been used by wireless Access Points as a rudimentary form of security. Although easily thwarted, MAC filters still provide a fair first layer of defense in the area of wireless security. To make the application of MAC filters fit better within the framework of SonicOS Enhanced and the Secure Wireless Solution/Architecture, MAC Address Objects and Groups will be introduced in SonicOS Enhanced 2.5, allowing for MAC Addresses, or Groups of MAC Addresses to be defined and applied to SonicPoints. MAC Filters can be applied in either an “Allow” or a “Deny” fashion, wherein Allowed MAC Filters will define the list of MAC addresses that can connect (denying all others), and Deny MAC Filters will define the list of MAC addresses that cannot connect (allowing all others).

Changes to MAC Filter settings, or the MAC Filter Objects or Groups themselves will take effect immediately on all affected SonicPoints.

SonicPoint Profiles

SonicPoint Profiles provide a scalable and highly automated method of configuring and provisioning multiple SonicPoints across a Secure Wireless Solution/Architecture. SonicPoint Profile definitions will include all of the settings that can be configured on a SonicPoint, such as radio settings for the 2.4GHz and 5GHz radios, including SSID's, encryption settings, MAC filters, channels of operation, etc. Once defined, profiles can be applied at the Zone level in a fully flexible fashion, meaning that one Wireless Zone can use one profile, while a different Wireless Zone uses another.

Automatic Provisioning (SDP & SSPP)

The SonicWALL Discovery Protocol (SDP) is a layer 2 protocol employed by SonicPoints and devices running SonicOS Enhanced 2.5 and higher. SDP is the foundation for the automatic provisioning of SonicPoint units using the following messages:

- **Advertisement:** SonicPoint devices without a peer will periodically and on startup announce or advertise themselves using a broadcast. The advertisement will include information that will be used by the receiving SonicOS device to ascertain the state of the SonicPoint. The SonicOS device will then report the state of all peered SonicPoints, and will take configuration actions as needed.
- **Discovery:** SonicOS devices will periodically send discovery request broadcasts to elicit responses from L2 connected SonicPoint units.
- **Configure Directive:** A unicast message from a SonicOS device to a specific SonicPoint unit to establish encryption keys for provisioning, and to set the parameters for and to engage Configuration Mode.
- **Configure Acknowledgement:** A unicast message from a SonicPoint to its peered SonicOS device acknowledging a Configure Directive.
- **Keepalive:** A unicast message from a SonicPoint to its peered SonicOS device used to validate the state of the SonicPoint.

If using the SDP exchange the SonicOS device ascertains that the SonicPoint requires provisioning or a configuration update (such as on calculating a checksum mismatch, or when a firmware update is available), the Configure directive will engage a 3DES encrypted, reliable TCP based SonicWALL Simple Provisioning Protocol (SSPP) channel. The SonicOS device will then send the update to the SonicPoint using this channel, and the SonicPoint will restart with the updated configuration. State information will be provided by the SonicPoint, and will be viewable on the SonicOS security appliance throughout the entire discovery and provisioning process.

As part of the provisioning process, SonicOS will assign the discovered SonicPoint device a unique name, and it will record its MAC address and the interface and Zone on which it was discovered. It can also automatically assign the SonicPoint an IP address, if so configured, so that the SonicPoint can communicate with an authentication server for WPA-EAP support. SonicOS will then use the profile associated with the relevant Zone to configure the 2.4GHz and 5GHz radio settings.

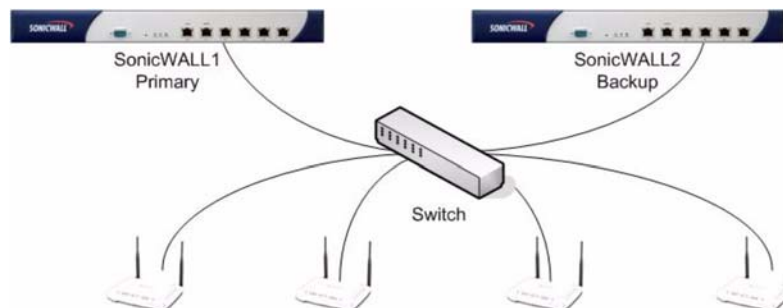
Modifications to profiles will not affect units that have already been provisioned and are in an operational state. Configuration changes to operational SonicPoint devices can occur in two ways:

- **through manual configuration changes:** Appropriate when a single, or a small set of changes are to be affected, particularly when that individual SonicPoint requires settings that are different from the profile assigned to its Zone.
- **through un-provisioning:** Deleting a SonicPoint unit effectively un-provisions the unit, or clears its configuration and places it into a state where it will automatically engage the provisioning process anew with its peer SonicOS device. This technique is useful when the profile for a Zone is updated or changed, and the change is set for propagation. It can be used to update firmware on SonicPoints, or to simply and automatically update multiple SonicPoint units in a controlled fashion, rather than changing all peered SonicPoints at once, which can cause service disruptions.

Hardware Failover and LAN Port Disconnect Transitions

While in Managed Mode, two additional SonicPoint transitions have been defined to help provide uninterrupted connectivity and high availability. The first such transition is specific to configurations wherein two SonicWALL appliances are paired in a Hardware Failover Mode. The following is a brief explanation of Hardware Failover (HF) concepts which will be useful in understanding the integration of SonicPoints into HF scenarios:

- **Primary:** Describes the principal *hardware* unit itself. The *Primary* identifier is a manual designation, and is not subject to conditional changes. Under normal operating conditions, the *Primary* hardware unit operates in an *Active* role.
- **Backup:** Describes the subordinate *hardware* unit itself. The *Backup* identifier is a relational designation, and is assumed by a unit when paired with a *Primary* unit. Under normal operating conditions, the *Backup* unit operates in an *Idle* Mode. Upon failure of the *Primary* unit, the *Backup* unit will assume the *Active* role.
- **Active:** Describes the operative condition of a hardware unit. The *Active* identifier is a logical *role* that can be assumed by either a *Primary* or *Backup* hardware unit.
- **Idle:** Describes the passive condition of a hardware unit. The *Idle* identifier is a logical *role* that can be assumed by either a *Primary* or *Backup* hardware unit. The *Idle* unit assumes the *Active* role in the event of determinable failure of the *Active* unit.



In the illustration, if the *Primary* unit fails and the *Backup* unit becomes *Active*, SonicWALL2 will broadcast a special SDP message informing all SonicPoints to drop their existing peering relationship with SonicWALL1, and to immediately re-peer with SonicWALL2. The SonicPoint configurations will already be synchronized as a result of the HF state-synchronization, and wireless service will be restored in parallel with the failover.

To appreciate the LAN Port Disconnect transition, consider what happens with a regular off-the-shelf access point in the event of a loss of LAN connectivity, for example, as a result of being physically disconnected or due to a faulty cable--once the Access Point loses its LAN link, it can no longer pass traffic from the wireless segment to the wired segment, but since its radio remains operational, all the associated clients remain associated--even if there is another fully connected and operation Access Point that can service them. The wireless clients are effectively stranded until some manual remedial action is taken.

If a SonicPoint loses LAN connectivity to its peered SonicWALL security appliance, that SonicPoint will immediately send disassociation messages to all associated clients, and will not accept subsequent association requests, forcing the clients to roam to the next available SonicPoint. The moment the LAN link is restored, the SonicPoint will begin to accept associations, allowing clients to roam back as their card's roaming logic decides. In conjunction with the AutoChannel feature, which allows SonicPoints to determine the best channel of operation based upon their environment, overlapping SonicPoints can easily be deployed to provide uninterrupted coverage.

Managed Mode and Stand-Alone Mode Transitions

Managed Mode requires that the SonicPoint be connected to a Wireless Interface of a SonicWALL appliance running SonicOS Enhanced 2.5 or greater. When a SonicPoint is in Managed Mode, it senses if a security appliance is present using the SonicWALL Discovery Protocol (SDP). Immediately after a boot, if a security appliance is not detected, the SonicPoint will reboot after a short time interval (~5 seconds) into Stand-Alone Mode. If a security appliance is initially detected (resulting in Managed Mode) but then becomes unavailable (such as it is powered off, or physically disconnected from the SonicPoint), the SonicPoint will poll at a longer interval (~6 minutes), and then revert into Stand-Alone Mode.

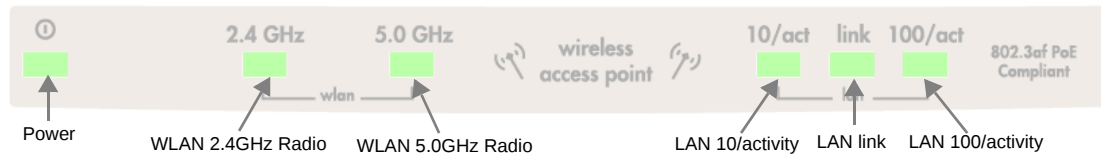
If for any reason a SonicPoint unexpectedly reboots while in Managed Mode, it will reboot into Managed Mode, unless the unexpected reboot occurred while attempting to upload firmware; in this case it will reboot into SafeMode. This fail-safe measure is achieved by setting the flash boot ROM pointer to the SafeMode image at the start of every firmware upgrade process, and setting it back to the Firmware image only after verifying that the image update completed successfully. Once entering into SafeMode through this course, if the SonicPoint is still connected to the SonicWALL security appliance, it will automatically attempt to upgrade firmware again.

Failing to sense a security appliance using SDP for a time interval greater than 6 minutes, a SonicPoint in Managed Mode will reboot into Stand-Alone Mode. In Stand-Alone Mode, the SonicPoint acts like a normal off-the-shelf access point. The SDP protocol continues to run while in Stand-Alone Mode, so if a SonicWALL PRO Series security appliance is ever sensed, the SonicPoint will automatically reboot into Managed Mode.

- The SonicPoint maintains separate Managed Mode and Stand-Alone Mode configurations so that neither conflicts with nor overwrites the other.
- When SafeMode is engaged (in all versions of SonicOS except for 3.1), either manually or automatically, both Managed Mode and Stand-Alone Mode configurations are restored to Factory Defaults. Currently if the SonicPoint device runs SonicOS 3.1, you can enable wired and non-SonicPoint access points on wireless zones.
- Restoring factory defaults with the Reset Switch only restores Factory Defaults for that mode of operation, such as depressing the Reset Switch for 5 seconds while in Managed Mode will only reset the Managed Mode configuration, but the Stand-Alone configuration will be left intact.

SonicPoint LEDs

The SonicPoint has six LEDs:



The SonicPoint G has five LEDs



- **Power** - The power LED is controlled directly by the 12.0 Volt DC power using power supply connector (power port) or the 802.3af Power over Ethernet (PoE) through the LAN connector. The power LED has the following behavior:

SonicPoint State	Power LED
Power off	off
Power on, SonicPoint ready	on, steady
Booting	blinking
Reboot to managed or Standalone Mode	flash three times (flash is a very short flash of light--0.25 seconds on and 0.25 seconds off)
Reboot to Safe Mode	Blink three times (blink is a slightly longer blink--0.5 seconds on and 0.5 seconds off)

- **WLAN 2.4 GHz Radio** - The 2.4 GHz Radio LED is controlled by the wireless radio. The LED blinks at a constant rate when the SonicPoint is ready to receive traffic using the 2.4 GHz radio (802.11b/g), and blinks at a variable rate when transferring data.
- **WLAN 5.0 GHz Radio** - (Only appears on the SonicPoint) The 5 GHz Radio LED is controlled by the wireless radio. The LED blinks at a constant rate when the SonicPoint is ready to receive traffic using the 5 GHz radio (802.11a), and blinks at a variable rate when transferring data.
- **LAN 10/activity** - The LAN 10/act LED is controlled by the network interface. It blinks to indicate 10mbit activity.
- **LAN Link** - The LAN Link LED is controlled by the network interface. It lights to indicate connectivity.
- **LAN 100/activity** - The LAN 100/act LED is controlled by the network interface. It blinks to indicate 100mbit activity.

Managing SonicPoints in Managed Mode

SonicWALL SonicPoints are wireless access points specially engineered to work with a SonicWALL security appliance running SonicOS Enhanced 2.5 or newer to provide wireless access throughout your enterprise. In Managed Mode, you use the Management Interface of the security appliance to manage the SonicPoint.

Use the Wireless section of the Management Interface to manage the SonicPoints connected to your security appliance.

Before Managing SonicPoints

Before you can manage SonicPoints in the Management Interface, you must first set up the security appliance:

- Configure your SonicPoint Provisioning Profiles.
- Configure a Wireless zone.
- Assign profiles to wireless zones. This step is optional. If you do not assign a default profile for a zone, SonicPoints in that zone will use the first profile in the list.
- Assign one or more interfaces to the Wireless zone.
- Attach the SonicPoints to the interfaces in the Wireless zone.
- Test the SonicPoints.

The screenshot displays the SonicWALL Management Interface. On the left is a navigation menu with options: System, Network, Wireless, SonicPoints, Station Status, IDS, Firewall, VPN, Users, Hardware Failover, Security Services, Log, Wizards, Help, and Logout. The main content area is titled 'Wireless > SonicPoints' and includes buttons for 'Synchronize SonicPoints', 'Apply', 'Cancel', and a help icon. Below this, there are two sections: 'SonicPoint Provisioning Profiles' and 'SonicPoints'. The 'SonicPoint Provisioning Profiles' section shows a table with one profile named 'SonicPoint' applied to the 'WLAN' zone. The 'SonicPoints' section shows a table with one SonicPoint named 'SonicPoint e00072' connected to the 'X3 (WLAN)' interface. A note at the bottom states: 'Note: All Operational SonicPoints are upgraded to SonicPoint Firmware Version 2.5.0.1. Download: [icon]'. The status at the bottom left is 'Status: Ready'.

#	Name Prefix	Applied Zone	802.11a Radio	802.11g Radio	Configure
1	SonicPoint	WLAN	SSID: TechPubs_SonicPoint Channel: AutoChannel	SSID: TechPubs_SonicPoint Channel: AutoChannel	[icon]

#	Name	Interface	Network Settings	Status	802.11a Radio	802.11g Radio	Enable	Configure
1	SonicPoint e00072	X3 (WLAN)	IP: 172.4.4.239 MAC: 00:02:6f:e0:00:72	Operational	SSID: TechPubs_SonicPoint Channel: AutoChannel	SSID: TechPubs_SonicPoint Channel: AutoChannel	☒	[icon]

SonicPoint Provisioning Profiles

SonicPoint Provisioning Profiles provide a scalable and highly automated method of configuring and provisioning multiple SonicPoints across a Secure Wireless Solution/Architecture. SonicPoint Profile definitions include all of the settings that can be configured on a SonicPoint, such as radio settings for the 2.4GHz and 5GHz radios, SSID's, and channels of operation.

Once you have defined a SonicPoint profile, you can apply it to a Wireless zone. Each Wireless zone can be configured with one SonicPoint profile. Any profile can apply to any number of zones. Then, when a SonicPoint is connected to a zone, it is automatically provisioned with the profile assigned to that zone.

Configuring a SonicPoint Profile

You can add any number of SonicPoint profiles.

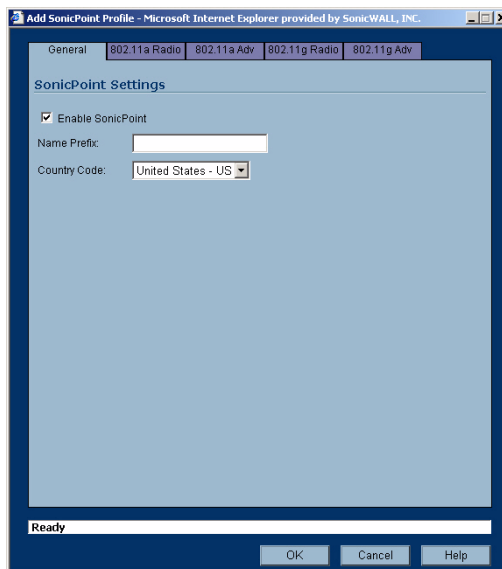
To configure a SonicPoint provisioning profile:

- 1 To add a new profile click **Add** below the list of SonicPoint provisioning profiles

To edit an existing profile, select the profile and click the edit icon  in the same line as the profile you are editing.

- 2 In the **General** tab of the Add Profile window, specify:

- ♦ **Enable SonicPoint:** Check this to automatically enable each SonicPoint when it is provisioned with this profile.
- ♦ **Name Prefix:** Enter a prefix for the names of all SonicPoints connected to this zone. When each SonicPoint is provisioned it is given a name that consists of the name prefix and a unique number, for example: "SonicPoint 126008."
- ♦ **Country Code:** Select the country where you are operating the SonicPoints. The country code determines which regulatory domain the radio operation falls under.



- 3 In the **802.11a** tab, Configure the radio settings for the 802.11a (5GHz band) radio:

- ♦ **Enable 802.11a Radio:** Check this to automatically enable the 802.11a radio bands on all SonicPoints provisioned with this profile.



Note: 802.11a radio settings only apply to the SonicPoint with 802.11a/b/g.

- ♦ **SSID:** Enter a recognizable string for the SSID of each SonicPoint using this profile. This is the name that will appear in clients' lists of available wireless connections.



Note: If all SonicPoints in your organization share the same SSID, it is easier for users to maintain their wireless connection when roaming from one SonicPoint to another.

- ♦ **Radio Mode:** Select the speed of the wireless connection. You can choose **54 Mbps** or **108 Mbps (Turbo)** Mode. If you choose Turbo Mode, all users in your company must use wireless access cards from the same manufacturer.
- ♦ **Channel:** Select the channel the radio will operate on. The default is **AutoChannel**, which automatically selects the channel with the least interference. Use AutoChannel unless you have a specific reason to use or avoid specific channels.
- ♦ **ACL Enforcement:** Select this to enforce Access Control by allowing or denying traffic from specific devices. Select an address object from the list of MAC address objects.

- ♦ **Authentication Type:** Select the method of authentication for your wireless network. You can select **WEP - Both (Open System & Shared Key)**, **WEP - Open System**, **WEP - Shared Key**, **WPA - PSK**, or **WPA - EAP**.
- ♦ **WEP Key Type:** Select the size of the encryption key.
- ♦ **Default Key:** Select which key in the list below is the default key, which will be tried first when trying to authenticate a user.
- ♦ **Key Entry:** Select whether the key is alphanumeric or hexadecimal.
- ♦ **Key 1 - Key 4:** Enter the encryptions keys for WEP encryption. Enter the most likely to be used in the field you selected as the default key.

4 In the **802.11a Advanced** tab, configure the performance settings for the 802.11a radio. For most 802.11a advanced options, the default settings give optimum performance.

- ♦ **Hide SSID in Beacon:** Check this option to have the SSID broadcast as part of the wireless beacon, rather than as a separate broadcast.
- ♦ **Schedule IDS Scan:** Enables you to schedule a an Intrusion Detection scan at a specific time. The choices are:
 - Disabled.
 - Create new schedule.
 - Work Hours.
 - M-T-W-TH-F 08:00 to 17:00.
 - After Hours.
 - M-T-W-TH-F 17:00 to 24:00.
 - SU-S 00:00 to 25:00.
 - Weekend.
- ♦ **Data Rate:** Select the speed at which the data is transmitted and received. **Best** automatically selects the best rate available in your area given interference and other factors. You can select: **Best, 6 Mbps, 9 Mbps, 12 Mbps, 18 Mbps, 24 Mbps, 36 Mbps, 48 Mbps, or 54 Mbps.**
- ♦ **Transmit Power:** Select the transmission power. Transmission power effects the range of the SonicPoint. You can select: **Full Power, Half (-3 dB), Quarter (-6 dB), Eighth (-9 dB), or Minimum.**

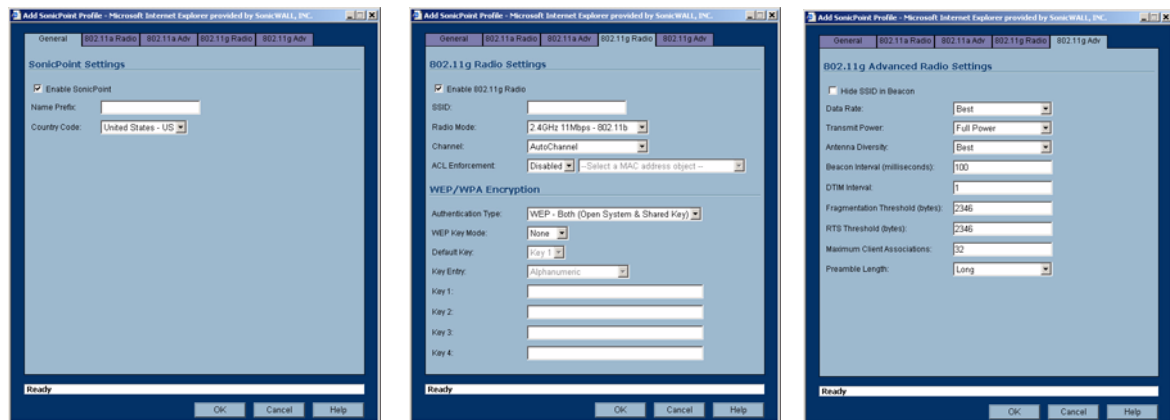
- ♦ **Antenna Diversity:** The **Antenna Diversity** setting determines which antenna the SonicPoint uses to send and receive data. You can select
 - **Best:** This is the default setting. When **Best** is selected, the SonicPoint automatically selects the antenna with the strongest, clearest signal. In most cases, **Best** is the optimal setting.
 - **1:** Select **1** to restrict the SonicPoint to use antenna 1 only. Facing the rear of the SonicPoint, antenna 1 is on the left, closest to the power supply.
 - **2:** Select **2** to restrict the SonicPoint to use antenna 2 only. Facing the rear of the SonicPoint, antenna 2 is on the right, closest to the console port.
 - ♦ **Beacon Interval (milliseconds):** Enter the number of milliseconds between sending out a wireless beacon.
 - ♦ **DTIM Interval:** Enter the interval in milliseconds.
 - ♦ **Fragmentation Threshold (bytes):** Enter the number of bytes of fragmented data you want the network to allow.
 - ♦ **RTS Threshold (bytes):** Enter the number of bytes.
 - ♦ **Maximum Client Associations:** Enter the maximum number of clients you want the SonicPoint to support on this radio at one time.
 - ♦ **Preamble Length:** (802.11g Adv) Establishes the style of the preamble which indicates the starting point and ending point of the frame. The preamble can be Long or Short. The Short type helps optimize performance. The default value is Long.
 - ♦ **CCK OFDM Power Delta:** (802.11g Adv) Enables you to control the power difference between a SonicPoint g and b client. CCK indicates greater power and OFDM indicates lesser power. You can specify three values for this field: 0 dBm, 1 dBm, and 2 dBm.
 - ♦ **Protections Fields:** These settings are appropriate when you allow both the SonicPoint b and g clients to be present at the same time. Since g clients transmit at a high rate, the b clients (that operate at a slower rate) cannot understand the traffic sent by a g client. It creates the problem of the b client not knowing when the media is clear to send traffic. You select a protection method to solve this issue. The g clients need to send CTS or CTS-RTS traffic at a slow rate (1 Mbps, 2 Mbps up to 11 Mbps) so that b clients can understand the traffic. The three protection methods are:
 - **Protection Mode:** (802.11g Adv).
 - **Protection Rate:** (802.11g Adv).
 - **Protection Type:** (802.11g Adv).
 - ♦ **Enable Short Slot Time:** (802.11g Adv) Enables short slot burst performance to address delays required in the MAC layer for radio transmission.
 - ♦ **Allow Only 802.11g Clients to Connect:** (802.11g Adv) Enables only the SonicPoint G clients to connect to the network.
- 5 Configure the settings in the **802.11g Radio** and **802.11g Advanced** tabs. These settings affect the operation of the 802.11g radio bands. The SonicPoint has two separate radios built in. Therefore, it can send and receive on both the 802.11a and 802.11g bands at the same time.
- The settings in the **802.11g Radio** and **802.11g Advanced** tabs are similar to the settings in the **802.11a Radio** and **802.11a Advanced** tabs. Follow the instructions in step 3 and step 4 in this procedure to configure the 802.11g radio.

When a SonicPoint unit is first connected and powered up, it will have a factory default configuration (IP Address 192.168.1.20, username: admin, password: password). Upon initializing, it will attempt to find a SonicOS device with which to peer. If it is unable to find a peer SonicOS device, it will enter into a Stand-Alone Mode of operation with a separate stand-alone configuration allowing it to operate as a standard Access Point.

If the SonicPoint does locate, or is located by a peer SonicOS device, using the SonicWALL Discovery Protocol, an encrypted exchange between the two units will ensue wherein the profile assigned to the relevant Wireless Zone will be used to automatically configure (provision) the newly added SonicPoint unit.

SonicPoint Settings							
Name	Interface	Network Settings	Status	802.11a Radio	802.11g Radio	Enable	Configure
☐ SonicPoint e00072	X3 (WLAN)	IP: 192.168.67.239 MAC: 00:02:8f:e0:00:72	Operational	SSID: TechPubs SonicPoint Channel: AutoChannel	SSID: TechPubs SonicPoint Channel: AutoChannel	☒	
							

As part of the provisioning process, SonicOS will assign the discovered SonicPoint device a unique name, and it will record its MAC address and the interface and Zone on which it was discovered. It can also automatically assign the SonicPoint an IP address, if so configured, so that the SonicPoint can communicate with an authentication server for WPA-EAP support. SonicOS will then use the profile associated with the relevant Zone to configure the 2.4GHz and 5GHz radio settings.



Modifications to profiles will not affect units that have already been provisioned and are in an operational state. Configuration changes to operational SonicPoint devices can occur in two ways:

- using manual configuration changes: Appropriate when a single, or a small set of changes are to be affected, particularly when that individual SonicPoint requires settings that are different from the profile assigned to its Zone.
- using un-provisioning: Deleting a SonicPoint unit effectively un-provisions the unit, or clears its configuration and places it into a state where it will automatically engage the provisioning process anew with its peer SonicOS device. This technique is useful when the profile for a Zone is updated or changed, and the change is set for propagation. It can be used to update firmware on SonicPoints, or to simply and automatically update multiple SonicPoint units in a *controlled* fashion, rather than changing all peered SonicPoints at once, which can cause service disruptions.

Selecting Variable Numbers of SonicPoint Access Points

SonicOS 3.1 Enhanced supports the selection of a variable number of SonicPoint access points. Previously you could only set Class C or greater networks on your subnet. SonicPoint access points. Now you can select four different amounts. This provides you with the flexibility to create a subnetwork that is appropriate for the amount of devices you have.

The indiscriminating addressing requirement sometimes proved unnecessary or disruptive.

To configure a number of SonicPoint access points, perform the following steps:

- 1 Log into the SonicWALL security appliance that is managing the SonicPoint device.
- 2 Go to the Interfaces page under the Network > Interfaces location.

Name	Zone	IP Address	Subnet Mask	IP Assignment	Status	Comment	Configure
X0	LAN	192.168.168.168	255.255.255.0	Static	No link	Default LAN	
X1	WAN	10.0.93.49	255.255.0.0	Static	100 Mbps half-duplex	Default WAN	
X2	Unassigned	0.0.0.0	0.0.0.0	N/A	No link		
X3	Unassigned	0.0.0.0	0.0.0.0	N/A	No link		
X3/V1	DMZ	10.100.9.1	255.255.255.0	Static	VLAN Sub-interface		
X4	WLAN	172.10.99.1	255.255.255.0	Static	100 Mbps full-duplex		
X5	Unassigned	0.0.0.0	0.0.0.0	N/A	No link		

- 3 Click on the Configure icon of the WLAN interface. SonicOS displays the Configure screen.

Interface 'X4' Settings

Zone: WLAN

IP Address: 172.10.99.1

Subnet Mask: 255.255.255.0

SonicPoint Limit: 16 SonicPoints

Comment:

Management: ☐ Ping ☐ SNMP ☐ SSH

User Login:

☒ Add rule to enable redirect from HTTP to HTTPS

Ready

OK Cancel Help

- 4 Make sure the Zone listbox has the WLAN zone selected.
- 5 You can provide any subnet mask size you want. Previously, you could only configure subnet masks in the range of 255.255.255.0 to 255.255.255.255.

- 6 Click on the SonicPoint Limit listbox and select one of the options that indicates the number of SonicPoints:
 - ♦ No SonicPoints.
 - ♦ 2 SonicPoints.
 - ♦ 4 SonicPoints.
 - ♦ 8 SonicPoints.
 - ♦ 12 SonicPoints.
- 7 Check one of the checkboxes in the Management region to indicate a management type you want to use.

Working with New Memory Requirements

As SonicWALL devices began to evolve, the company provided different versions of ROM to accommodate varying levels of memory requirements. Beginning with SonicOS Enhanced 3.1, the SonicWALL TZ Series 170, SonicWALL TZ Series 170W, and SonicWALL TZ Series 170SPW now run the SonicPoint image at startup for distribution to connected SonicPoint devices, regardless of which ROM version is present. The image is downloaded from software.sonicwall.com, and is DSA signed with an embedded SHA1 hash to ensure integrity.

You can change the default path for SonicPoint image retrieval by performing the following steps:

- 1 Log into the SonicWALL security appliance that is managing the SonicPoint device.
- 2 Navigate to the System > Administration page.
- 3 From the Download URL section of the page, change the path of the SonicPoint image retrieval point in the SonicPoint Download URL (<http://>) field. Make sure the last character in the path is a forward slash (/).



Note: Note that the filename of the SonicPoint image is embedded within SonicOS. You can verify the embedded filename at the bottom of the SonicPoint > SonicPoints page.

- 4 After downloading the SonicPoint image from mysonicwall.com, verify that the name is exactly as it appears on the SonicPoint > SonicPoints page.
- 5 Place the image on the file system of the Web server in the path specified on the System > Administration page.
 - ♦ Assuming your Web server is a Microsoft IIS Server, create a directory called sonicpoint in your default Web site path. Place the file in this directory. Make sure anonymous access is allowed and that no IP restrictions are in place which might prevent the SonicWALL from retrieving the file.
 - ♦ Assuming your Web server is a Red Hat server, create a directory called sonicpoint in the default document root directory and place the file in this directory. Make sure no authentication or access restrictions are in place which could prevent the SonicWALL from retrieving the file.

Updating SonicPoint Settings

You can change the settings of any individual SonicPoint listed on the Wireless > SonicPoints page.

Edit SonicPoint settings

To edit the settings of an individual SonicPoint:

- 1 Under SonicPoint Settings, click the Edit icon  in the same line as the SonicPoint you want to edit.
- 2 In Edit SonicPoint screen, make the changes you want. The Edit SonicPoint screen has the following tabs:

- ◆ **General.**
- ◆ **802.11a Radio.**
- ◆ **802.11a Advanced.**
- ◆ **802.11g Radio.**
- ◆ **802.11g Advanced.**

The options on these tabs are the same as the Add SonicPoint Profile screen. See [Configuring a SonicPoint Profile](#) for instructions on configuring these settings.

- 3 Click **OK** to apply these settings.

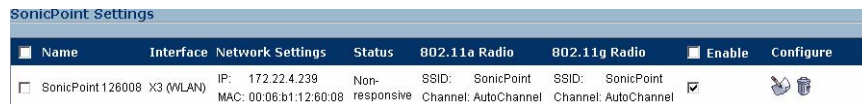
Synchronize SonicPoints

Click **Synchronize SonicPoints** at the top of the Wireless > SonicPoints page to update the settings for each SonicPoint reported on the page. When you click **Synchronize SonicPoints**, SonicOS polls all connected SonicPoints and displays updated settings on the page.

Enable and Disable Individual SonicPoints

You can enable or disable individual SonicPoints on the Wireless > SonicPoints page:

- 1 Check the box under Enable to enable the SonicPoint, uncheck the box to disable it.



Name	Interface	Network Settings	Status	802.11a Radio	802.11g Radio	Enable	Configure
☐ SonicPoint 126008	X3 (WLAN)	IP: 172.22.4.239 MAC: 00:06:b1:12:60:08	Non-responsive	SSID: SonicPoint Channel: AutoChannel	SSID: SonicPoint Channel: AutoChannel	☒	 

- 2 Click **Apply** at the top of the Wireless > SonicPoints page to apply this setting to the SonicPoint.

Updating SonicPoint Firmware

SonicOS Enhanced 2.5 (or greater) contains an image of the SonicPoint firmware. When you connect a SonicPoint to a security appliance running SonicOS Enhanced 2.5 (or greater), the appliance checks the version of the SonicPoint's firmware, and automatically updates it, if necessary.

You can manually update the SonicPoint's firmware as well:

- 1 In the SonicOS Management Interface, on the Wireless > SonicPoints page, click the download firmware icon  at below the list of SonicPoints to download a copy of the firmware appropriate to the version of SonicOS to your workstation desktop.
- 2 Place the firmware file in an FTP-enabled directory on your computer or on an FTP Server.
- 3 Connect to your SonicPoint in Stand-Alone Mode. See [Managing the SonicPoint in Stand-Alone Mode](#) for instructions.

- 4 In the Stand-Alone Management Interface, on the System > Firmware page, enter the IP address or path of the location of the firmware file.
- 5 Enter the username and password for the FTP site, and click **Upload New Firmware**.

SonicPoint States

SonicPoint devices can function in and report the following states:

- **Initializing:** The state when a SonicPoint starts up and advertises itself using SDP prior to it entering into an operational or Stand-Alone Mode.
- **Operational:** Once the SonicPoint has peered with a SonicOS security appliance and has its configuration validated, it will enter into a operational state, and will be ready for clients.
- **Provisioning:** If the SonicPoint configuration requires an update, the SonicOS security appliance will engage an SSPP channel to update the SonicPoint. During this brief process it will enter the provisioning state.
- **Safe Mode:** Safe Mode can be engaged by depressing the reset button, or from the SonicOS peer device. Placing a SonicPoint into Safe Mode returns its configuration to defaults, disables the radios, and disables SDP. The SonicPoint must then be rebooted to enter either a stand-alone, or some other functional state.
- **Non-Responsive:** If a SonicOS security appliance loses communications with a previously peered SonicPoint, it will report its state as non-responsive. It will remain in this state until either communications are restored, or the SonicPoint is deleted from the SonicOS device's table.
- **Updating Firmware:** If the SonicOS security appliance detects that it has a firmware update available for a SonicPoint, it will use SSPP to update the SonicPoint's firmware.
- **Over-Limit:** By default, up to 16 SonicPoint devices can be attached to each Wireless Zone interface on a SonicOS device. If more than 16 units are detected, the over-limit devices will report an over-limit state, and will not enter an Operational Mode. The number can be reduced from 16 as needed.
- **Rebooting:** After a firmware or configuration update, the SonicPoint will announce that it is about to reboot, and will then do so.
- **Firmware failed:** If a firmware update fails, the SonicPoint will report the failure, and will then reboot.
- **Provision failed:** In the unlikely event that a provision attempt from a SonicOS security appliance fails, the SonicPoint will report the failure. So as not to enter into an endless loop, it can then be manually rebooted, manually reconfigured, or deleted and re-provisioned.
- **Stand-Alone Mode:** If a SonicPoint security appliance cannot find or be found by a SonicOS security appliance to peer with, it will enter a Stand-Alone Mode of operation. This will engage the SonicPoint's internal GUI (which is otherwise disabled) and will allow it to be configured as a conventional Access Point. If at any time it is placed on the same layer 2 segment as a SonicOS security appliance that is sending Discovery packets, it will leave Stand-Alone Mode, and will enter into a Managed Mode. The Stand-Alone Mode configuration will be retained.

Managing the SonicPoint in Stand-Alone Mode

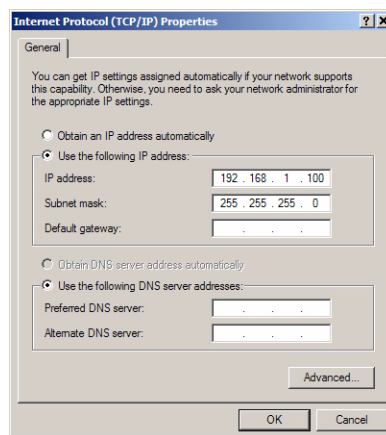
The SonicPoint runs in Stand-Alone Mode whenever it is not physically connected (directly or using a hub or switch) to a Wireless zone on a SonicWALL security appliance running SonicOS Enhanced 2.5 or newer. Stand-Alone Mode allows the SonicPoint to function as a standard wireless access point.

In Stand-Alone Mode, the SonicPoint has a management interface that is very similar to the Wireless section of the SonicOS Enhanced 2.5 Management Interface. Once connected, the settings you can manage in Stand-Alone Mode are the same as the Wireless settings you manage in the SonicOS Management Interface.

Connecting to the Stand-Alone Management Interface

- 1 Configure your management station. If you are connecting to the LAN port on the SonicPoint directly from your management station or through only the PoE injector, you need to configure the Local Area Connection on your management station.

- ♦ **IP address:** 192.168.1.100.
- ♦ **Netmask:** 255.255.255.0.

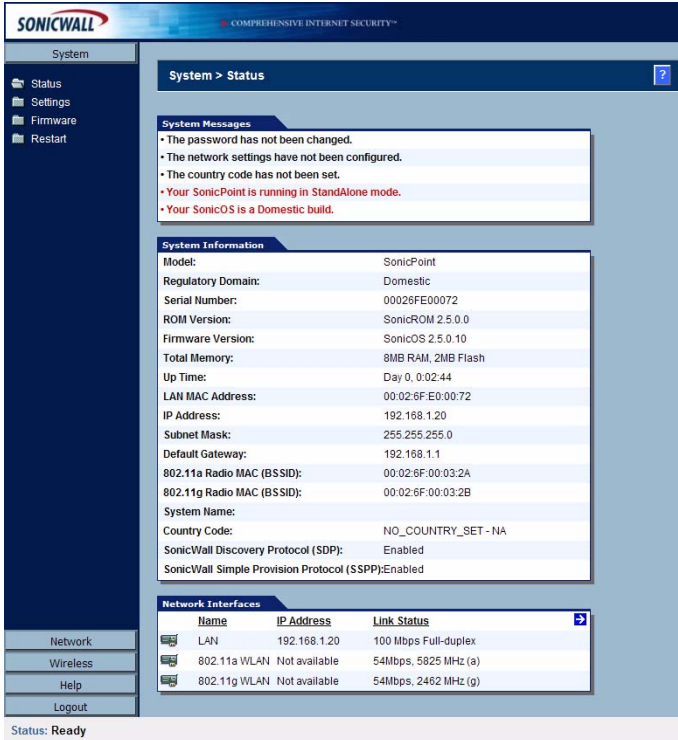


- 2 Connect to the SonicPoint.
 - ♦ Connect directly to the LAN port of the SonicPoint with a crossover cable or regular cat. 5 Ethernet cable.
 - ♦ Connect to the LAN port of the SonicPoint through the PoE injector with a regular cat. 5 Ethernet cable.
 - ♦ If the SonicPoint is connected to a port in a SonicWALL security appliance and the port is not in a Wireless zone, you can connect to it through the security appliance provided there are rules to allow HTTP management traffic between the zone your management station is in and the zone the SonicPoint is in.
- 3 Start your Web browser and direct it to the default management IP address for the SonicPoint, **192.168.1.20**.

Using the SonicPoint Stand-Alone Management Interface

Because the stand-alone Management Interface mirrors the Wireless section of the SonicOS Management Interface, see [Managing SonicPoints in Managed Mode](#) for instructions on managing the SonicPoint in Stand-Alone Mode.

System > Status



System > Status

System Messages

- The password has not been changed.
- The network settings have not been configured.
- The country code has not been set.
- Your SonicPoint is running in StandAlone mode.
- Your SonicOS is a Domestic build.

System Information

Model:	SonicPoint
Regulatory Domain:	Domestic
Serial Number:	00026FE00072
ROM Version:	SonicROM 2.5.0.0
Firmware Version:	SonicOS 2.5.0.10
Total Memory:	8MB RAM, 2MB Flash
Up Time:	Day 0, 0:02:44
LAN MAC Address:	00:02:6F:E0:00:72
IP Address:	192.168.1.20
Subnet Mask:	255.255.255.0
Default Gateway:	192.168.1.1
802.11a Radio MAC (BSSID):	00:02:6F:00:03:2A
802.11g Radio MAC (BSSID):	00:02:6F:00:03:2B
System Name:	
Country Code:	NO_COUNTRY_SET - NA
SonicWall Discovery Protocol (SDP):	Enabled
SonicWall Simple Provision Protocol (SPP):	Enabled

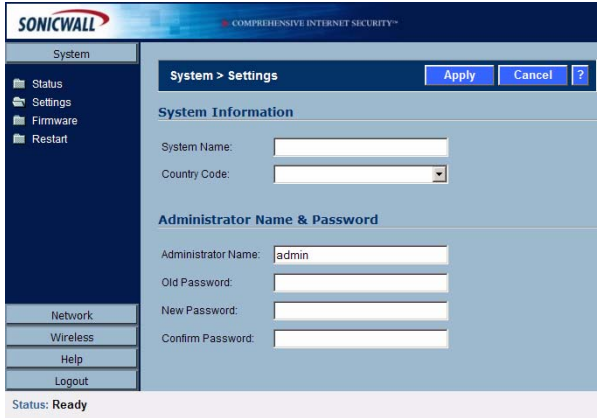
Network Interfaces

Name	IP Address	Link Status
LAN	192.168.1.20	100 Mbps Full-duplex
802.11a WLAN	Not available	54Mbps, 5825 MHz (a)
802.11g WLAN	Not available	54Mbps, 2462 MHz (g)

Status: Ready

Provides a view of operating parameters on the SonicPoint, and provides quick links to the Network Interface settings.

System > Settings



System > Settings

System Information

System Name:

Country Code:

Administrator Name & Password

Administrator Name:

Old Password:

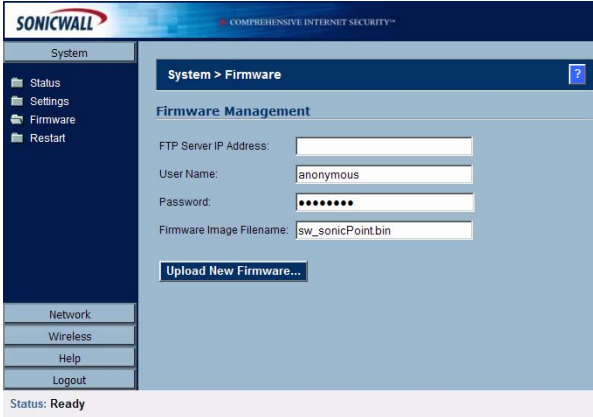
New Password:

Confirm Password:

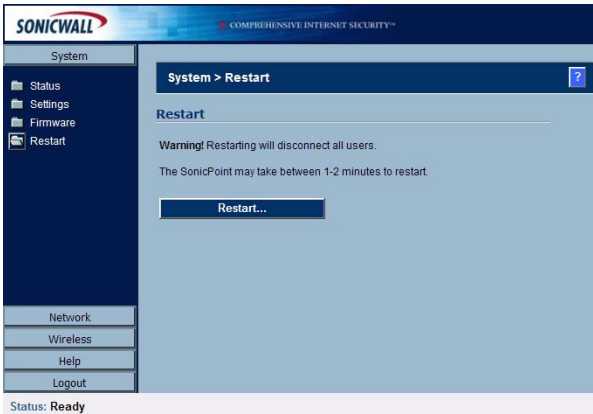
Status: Ready

Allows for the System Name, Country Code, and administrative information to be configured.

System > Firmware

	Provides an interface to upload new firmware using FTP. Requires access to an external FTP server hosting a SonicPoint Firmware image. SonicPoint firmware can be downloaded from a SonicOS Enhanced 2.5 or greater SonicOS security appliance from the 'Wireless > SonicPoints' page, or from www.mysonicwall.com
---	---

System > Restart

	UI based restarting of the SonicPoint.
--	---

Network > Interfaces

The screenshot shows the SonicWall SonicPoint Administrator's Guide interface. The left sidebar contains a tree view with 'System', 'Network', 'Interfaces', 'Wireless', 'Help', and 'Logout'. The main content area is titled 'Network > Interfaces' and includes 'LAN Settings' with the following fields:

IP Address:	192.168.1.20
Subnet Mask:	255.255.255.0
Gateway:	192.168.1.1

Buttons for 'Apply', 'Cancel', 'Reboot', and a help icon are located at the top right of the configuration area. The status bar at the bottom indicates 'Status: Ready'.

Configuration of LAN IP, netmask, and default gateway.

Wireless > Status

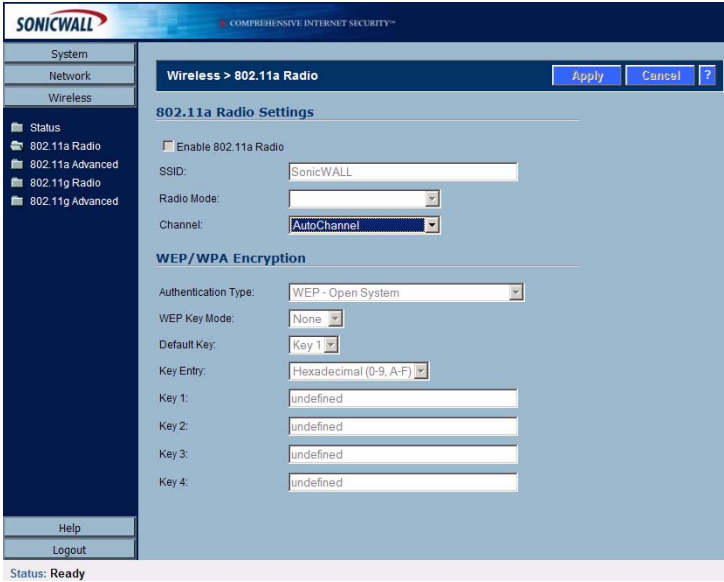
The screenshot shows the SonicWall SonicPoint Administrator's Guide interface. The left sidebar contains a tree view with 'System', 'Network', 'Wireless', 'Status', '802.11a Radio', '802.11a Advanced', '802.11g Radio', '802.11g Advanced', 'Help', and 'Logout'. The main content area is titled 'Wireless > Status' and includes a 'Site Survey' button. Below this, there are sections for 'Sonic Point Status', '802.11a Radio Settings', and '802.11g Radio Settings'. A 'Station Status' table is displayed with the following columns:

Station	MAC Address	Authenticated	Associated	Association Id
---------	-------------	---------------	------------	----------------

The status bar at the bottom indicates 'Status: Ready'.

View statistics for both radios, and associated Station status.

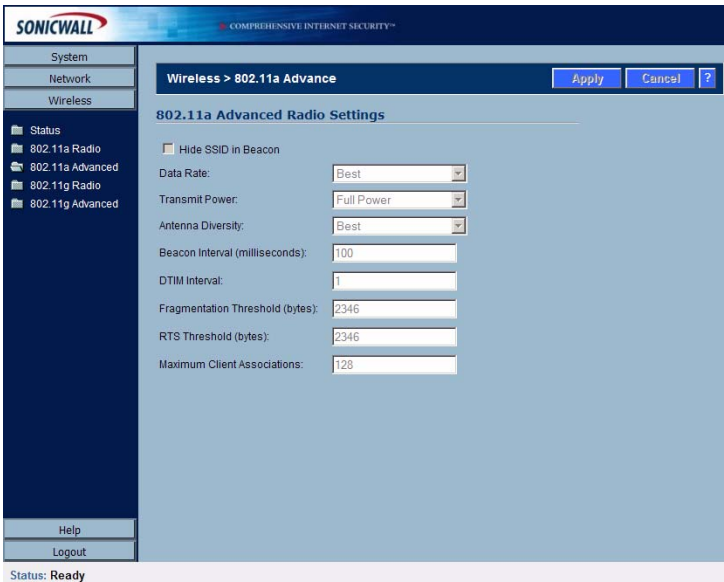
Wireless > 802.11a Radio



The screenshot shows the SonicWALL web interface for configuring 802.11a radio settings. The left sidebar contains a tree view with 'Status', '802.11a Radio', '802.11a Advanced', '802.11g Radio', and '802.11g Advanced'. The main content area is titled '802.11a Radio Settings' and includes an 'Enable 802.11a Radio' checkbox, an SSID field set to 'SonicWALL', a 'Radio Mode' dropdown, and a 'Channel' dropdown set to 'AutoChannel'. Below this is a 'WEP/WPA Encryption' section with an 'Authentication Type' dropdown set to 'WEP - Open System', a 'WEP Key Mode' dropdown set to 'None', a 'Default Key' dropdown set to 'Key 1', a 'Key Entry' dropdown set to 'Hexadecimal (0-9, A-F)', and four 'Key' input fields (Key 1 through Key 4), all of which are currently empty. At the bottom left are 'Help' and 'Logout' buttons, and at the bottom right is a 'Status: Ready' indicator.

802.11a (5GHz) Radio settings

Wireless > 802.11a Advanced



The screenshot shows the SonicWALL web interface for configuring advanced 802.11a radio settings. The left sidebar contains a tree view with 'Status', '802.11a Radio', '802.11a Advanced', '802.11g Radio', and '802.11g Advanced'. The main content area is titled '802.11a Advanced Radio Settings' and includes a 'Hide SSID in Beacon' checkbox, a 'Data Rate' dropdown set to 'Best', a 'Transmit Power' dropdown set to 'Full Power', an 'Antenna Diversity' dropdown set to 'Best', a 'Beacon Interval (milliseconds)' input field set to '100', a 'DTIM Interval' input field set to '1', a 'Fragmentation Threshold (bytes)' input field set to '2346', an 'RTS Threshold (bytes)' input field set to '2346', and a 'Maximum Client Associations' input field set to '128'. At the bottom left are 'Help' and 'Logout' buttons, and at the bottom right is a 'Status: Ready' indicator.

Advanced 802.11a (5GHz) Radio settings

Wireless > 802.11g Radio

The screenshot displays the SonicWall SonicPoint Administrator's Guide interface. The left sidebar shows a navigation tree with 'Wireless' selected, and '802.11g Radio' highlighted. The main content area is titled 'Wireless > 802.11g Radio' and contains the '802.11g Radio Settings' section. The settings include: 'Enable 802.11g Radio' (checked), 'SSID' (SonicWALL), 'Radio Mode' (2.4GHz 54 Mbps - 802.11g), 'Channel' (AutoChannel), 'WEP/WPA Encryption' (WEP - Open System), 'WEP Key Mode' (None), 'Default Key' (Key 1), 'Key Entry' (Hexadecimal (0-9, A-F)), and four 'Key' fields (Key 1, Key 2, Key 3, Key 4) all set to 'undefined'. The status at the bottom is 'Ready'.

802.11g/b (2.4GHz) Radio settings

Wireless > 802.11g Advanced

The screenshot displays the SonicWall SonicPoint Administrator's Guide interface. The left sidebar shows a navigation tree with 'Wireless' selected, and '802.11g Advanced' highlighted. The main content area is titled 'Wireless > 802.11g Advance' and contains the '802.11g Advanced Radio Settings' section. The settings include: 'Hide SSID in Beacon' (unchecked), 'Data Rate' (Best), 'Transmit Power' (Full Power), 'Antenna Diversity' (Best), 'Beacon Interval (milliseconds)' (100), 'DTIM Interval' (1), 'Fragmentation Threshold (bytes)' (2346), 'RTS/CTS Threshold (bytes)' (2346), 'Maximum Client Associations' (128), 'Preamble Length' (Short), 'Protection Mode' (Auto), 'Protection Rate' (11 Mbps), 'Protection Type' (CTS-only), 'Enable Short Slot Time' (checked), and 'Allow Only 802.11g Clients to Connect' (unchecked). The status at the bottom is 'Ready'.

Advanced 802.11g/b (2.4GHz) Radio settings

Managing the SonicPoint in SafeMode

The SafeMode image provides a fail-safe mechanism for the firmware upload process as performed from either the stand-alone GUI using FTP, or using automatic updates performed by a SonicOS security appliance using SonicWALL Discovery Protocol (SDP) and SonicWALL Simple Provisioning Protocol (SSPP). In the event of firmware image corruption, the SonicPoint will automatically enter into SafeMode, the configuration (both Stand-Alone and Managed) will be restored to factory defaults, and a new firmware image can be uploaded using FTP.

SonicPoint SafeMode

Your SonicPoint is now running in SafeMode.

SafeMode will allow you to view your basic SonicPoint settings and upload a new firmware image.

System Information	
Product Name:	SonicPoint
Regulatory Domain:	Domestic
Serial Number:	00026FE0009B
ROM Version:	SonicROM 2.5.0.0
SafeMode Firmware Version:	SonicOS 2.5.0.6
LAN MAC Address:	00:02:6F:E0:00:9B
IP Address:	192.168.1.20
Subnet Mask:	255.255.255.0
Default Gateway:	192.168.1.1
802.11a Radio MAC (BSSID):	00:02:6F:00:03:7C
802.11g Radio MAC (BSSID):	00:02:6F:00:03:7D
SonicWall Discovery Protocol (SDP):	Enabled
SonicWall Simple Provision Protocol (SSPP):	Enabled

Firmware Management

FTP Server IP Address:

User Name:

Password:

Firmware Image Filename:

Status: Ready.



Note: An FTP server hosting the SonicPoint firmware image is required for this process. The SonicPoint firmware is embedded in SonicOS Enhanced version 2.5 and later, and can be retrieved from the SonicOS GUI using the download  link at bottom of the **Wireless > SonicPoints** page. After successfully uploading the new firmware image to the SonicPoint using FTP, the ROM pointer will be updated, and the SonicPoint will reboot using the new firmware image. The default IP address of the Safe Mode (and Stand-Alone) GUI is 192.168.1.20. Safe Mode does not require a login, while Stand-Alone Mode employs a default username of 'admin' and a password of 'password'.

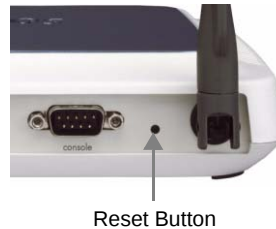
The SafeMode firmware image is stored on the SonicPoint flash file system with the internal file name "/fl/swsm1". The SafeMode image is installed during manufacturing, and provides a fail-safe mechanism if the normal firmware image becomes corrupt or crashes immediately after boot, or fails to upgrade.

In SafeMode, the SonicWALL Discovery Protocol (SDP) and SonicWALL Simple Provisioning Protocol (SSPP) allow the SonicPoint device to be managed using an Interface that is a member of a Wireless zone of a SonicWALL PRO family appliance running SonicOS 2.5 or higher. Simply connect a cable between the SonicPoint LAN and the PROs Wireless Interface. The SonicWALL PRO Series security appliance will automatically upgrade the SonicPoint SonicOS Firmware Image if necessary, and the SonicWALL PRO Series security appliance will provision the SonicPoint's configuration to work in the network environment of the PRO. The SonicPoint will then reboot and run the SonicOS Firmware Image if the firmware upgrade and provision is successful. If firmware upgrade fails, it will reboot into SafeMode.

In addition to simple provisioning by a PRO, a SonicPoint running in SafeMode runs a Web server where a user may upload firmware and view basic settings. While similar to the SonicWALL PRO Series security appliance and SonicWALL TZ Series security appliance family SafeMode features, the SafeMode Web Management utility of a SonicPoint only allows the uploading of firmware. Upon successfully uploading a SonicOS Firmware Image, the SonicPoint will reboot and run the SonicOS Firmware Image.

Resetting the SonicPoint

The SonicPoint has a reset switch inside a small hole in the back of the unit, next to the console port.



You can reset the SonicPoint at any time by pressing the reset switch with a straightened paper-clip, a tooth pick, or other small, straight object.

The reset button resets the configuration of the mode the SonicPoint is operating in to the factory defaults. It does not reset the configuration for the other mode. Depending on the mode the SonicPoint is operating in, and the amount of time you press the reset button, the SonicPoint behaves in one of the following ways:

- Press the reset button for **at least three seconds**, and **less than eight seconds** with the SonicPoint operating in Managed Mode to reset the Managed Mode configuration to factory defaults and reboot the SonicPoint.
- Press the reset button for **more than eight seconds** with the SonicPoint operating in Managed Mode to reset the Managed Mode configuration to factory defaults and reboot the SonicPoint in SafeMode.
- Press the reset button for **at least three seconds**, and **less than eight seconds** with the SonicPoint operating in Stand-Alone Mode to reset the Stand-Alone Mode configuration to factory defaults and reboot the SonicPoint.
- Press the reset button for **more than eight seconds** with the SonicPoint operating in Stand-Alone Mode to reset the Stand-Alone Mode configuration to factory defaults and reboot the SonicPoint in SafeMode.

SonicPoint Radio Characteristics

Each SonicPoint contains two separate radios, a 2.4GHz radio for 802.11b and 802.11g, and 5GHz radio for 802.11a. Since the radios are fully distinct, each SonicPoint can simultaneously host 802.11g/b and 802.11a clients, providing the highest level of wireless client compatibility.

SonicPoints support data rates of 6 to 54 Mbps in 802.11a and 802.11g modes, and up to 11 Mbps in 802.11b mode. Turbo Modes are also available in 802.11a and 802.11g modes, providing data rates of up to 108 Mbps.

Depending on the regulatory domain, the 5GHz 802.11a radio supports a maximum of 47 channels, with channel frequencies from 5130MHz to 5825MHz, non-contiguously. In 802.11a Static Turbo Mode, available only within the FCC regulatory domain, it supports 5 channels, with channels frequencies of 5210, 5250, 5290, 5760, and 5800MHz. In 802.11a Dynamic Turbo Mode, also available only within the FCC regulatory domain, it supports and additional 5 channels, with channel frequencies of 5200, 5240, 5280, 5765, and 5805MHz.

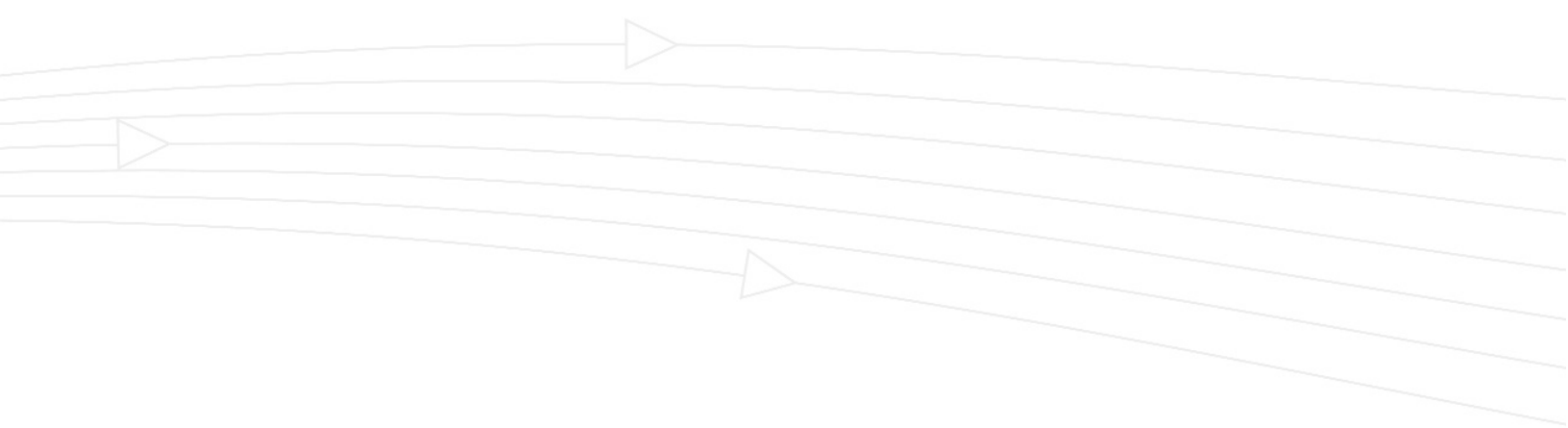
The 2.4Ghz 802.11g/b radio supports a maximum of 14 channels, depending on the regulatory domain, with a frequency range of 2412MHz to 2484MHz. The FCC regulatory domain also allows the channel frequency of 2437MHz to be used for either Static or Dynamic Mode Turbo 802.11g operation.



Note: Regulatory domain information is configured on the SonicPoint during the manufacturing process. When a SonicPoint operated in Stand-Alone Mode, radio configuration options will be limited to those allowed by the programmed regulatory domain. While operating in Managed Mode, the SonicPoint will advertise its regulatory domain to the managing SonicWALL security appliance using SDP, and the SonicWALL will only allow for radio configuration options appropriate to the advertised regulatory domain.

Frequency Band	802.11a: 5.15~5.25GHz, 5.25~5.35GHz, 5.725~5.825GHz 802.11b/g: 2.412~2.462GHz(US) 2.412~2.484GHz(Japan) 2.412~2.472GHz(Europe ETSI) 2.457~2.462GHz(Spain) 2.457~2.472GHz(France)
Modulation Technology	802.11a/g: OFDM (64-QAM, 16-QAM, QPSK, BPSK) 802.11b: DSSS (DBPK, DQPSK, CCK)

Operating Channels	802.11a: 12 for FCC 11 for Europe 4 for Japan 4 for Singapore 4 for Taiwan 802.11b/g: 11 for FCC 14 for Japan 13 for Europe 2 for Spain 4 for France
Receive Sensitivity (typical)	802.11a: -82dBm @ 6Mbps -81dBm @ 9Mbps -79dBm @ 12Mbps -78dBm @ 18Mbps -75dBm @ 24Mbps -72dBm @ 36Mbps -70dBm @ 48Mbps -68dBm @ 54Mbps 802.11b/g: -91dBm @ 1Mbps -90dBm @ 2Mbps -89dBm @ 5.5Mbps -84dBm @ 6Mbps -82dBm @ 9Mbps -87dBm @ 11Mbps -79dBm @ 12Mbps -77dBm @ 18Mbps -75dBm @ 24Mbps -73dBm @ 36Mbps -70dBm @ 48Mbps -68dBm @ 54Mbps
Transmit Output Power (Typical)	802.11a: Up to 20dBm = Up to 100mw 802.11g: Up to 21dBm = Up to 126mw 802.11b: Up to 23dBm = Up to 200mw



SonicWALL, Inc.

1143 Borregas Avenue
Sunnyvale, CA 94089-1306

T: 408.745.9600
F: 408.745.9300

www.sonicwall.com

© 2005 SonicWALL, Inc. SonicWALL is a registered trademark of SonicWALL, Inc. Other product and company names mentioned herein may be trademarks and/or registered trademarks of their respective companies. Specifications and descriptions subject to change without notice.

P / N 232-000797-00
Rev B 05/05

