

3 Configuring Wireless on the SOHO TZW

The SOHO TZW uses a wireless protocol called IEEE 802.11b, commonly known as Wi-Fi, and sends data via radio transmissions. Wi-Fi transmission speed is usually faster than broadband connection speed, but it is slower than Ethernet.

The SonicWALL SOHO TZW combines three networking components to offer a fully secure wireless firewall: an 802.11b Access Point, a secure wireless gateway, and a stateful firewall with flexible NAT and VPN termination and initiation capabilities. With this combination, the SOHO TZW offers the flexibility of wireless without compromising network security.

Typically, the SOHO TZW is the access point for your wireless LAN and serves as the central access point for computers on your LAN. In addition, it shares a single broadband connection with the computers on your network. Since the SOHO TZW also provides firewall protection, intruders from the Internet cannot access the computers or files on your network. This is especially important for an “always-on” connection such as a cable modem or T1 line that is shared by computers on a network.

However, wireless LANs are vulnerable to “eavesdropping” by other wireless networks which means you should establish a wireless security policy for your wireless LAN. Wired Equivalent Privacy, WEP, should not be used as your only security policy.

On the SOHO TZW, wireless clients connect to the Access Point layer of the firewall. Instead of bridging the connection directly to the wired network, wireless traffic is first passed to the Secure Wireless Gateway layer where the client is required to be authenticated via User Level Authentication. Access to Wireless Guest Services (WGS) and Access Control Lists (ACL) are managed by the SOHO TZW. It is also at this layer that the SOHO TZW has the capability of enforcing WiFiSec, and IPSec-based VPN overlay for wireless networking. As wireless network traffic successfully passes through these layers, it is then passed to the VPN-NAT-Stateful firewall layer where WiFiSec termination, address translation, and access rules are applied. If all of the security criteria is met, then wireless network traffic can then pass via one of the following Distribution Systems (DS):

- LAN
- WAN
- Wireless Client on the WLAN
- VPN tunnel

Considerations for Using Wireless Connections

- **Mobility** - if the majority of your network is laptop computers, wireless is more portable than wired connections.
- **Convenience** - wireless networks do not require cabling of individual computers or opening computer cases to install network cards.
- **Speed** - if network speed is important to you, you may want to consider using Ethernet connections rather than wireless connections.
- **Range and Coverage** - if your network environment contains numerous physical barriers or interference factors, wireless networking may not be suitable for your network.
- **Security** - wireless networks have inherent security issues due to the unrestricted nature of the wireless transmissions. However, the SOHO TZW is a firewall and has NAT capabilities which provides security, and you can use WEP to secure data transmissions.

Recommendations for Optimal Wireless Performance

- Place the SOHO TZW near the center of your intended network. This can also reduce the possibility of eavesdropping by neighboring wireless networks.
- Minimize the number of walls or ceilings between the SOHO TZW and the receiving points such as PCs or laptops.
- Try to place the TZW in a direct line with other wireless components. Best performance is achieved when wireless components are in direct line of sight with each other.
- Building construction can make a difference on wireless performance. Avoid placing the TZW near walls, fireplaces, or other large solid objects. Placing the TZW near metal objects such as computer cases, monitors, and appliances can affect performance of the unit.
- Metal framing, UV window film, concrete or masonry walls, and metallic paint can reduce signal strength if the TZW is installed near these types of materials.
- Installing the TZW in a high place can help avoid obstacles and improve performance for upper stories of a building.
- Neighboring wireless networks and devices can affect signal strength, speed, and range of the SOHO TZW. Also, devices such as cordless phones, radios, microwave ovens, and televisions may cause interference on the TZW.

Adjusting the SOHO TZW Antennas

The antennas on the SOHO TZW can be adjusted for the best radio reception. Begin with the antennas pointing straight up, and then adjust as necessary. Note that certain areas, such as the area directly below the SOHO TZW, get relatively poor reception. Pointing the antenna directly at another wireless device does not improve reception. Do not place the antennas next to metal doors or walls as this can cause interference.

Wireless Guest Services (WGS)

With your SOHO TZW, you can provide wireless guest services to wireless-equipped users who are not part of your corporate network, for example, a consultant or a sales person. You can offer authenticated wireless users access to the Internet through your SOHO TZW while preventing them from accessing your corporate LAN, or allowing them access to specific resources on the LAN and unencrypted access to the Internet.

When WGS is active, wireless clients can authenticate and associate with the Access Layer of the SonicWALL. When a Web browser is launched, the wireless user is prompted to provide a user name and password to gain access to WGS. The browser is redirected to the HTTP (unencrypted) management address of the SOHO TZW, but the user name and password is not transmitted. Instead, a secure hash is transmitted rendering the information useless to anyone “eavesdropping” on the network. After authentication, WGS is tracked and controlled by the client MAC address as well as Account and Session lifetimes.

In order to take advantage of Wireless Guest Services, you must provide a guest with a user name and password which they use to authenticate themselves using HTTP and a Web browser, creating a secure HTTP session. For more information on configuring Wireless Guest Services, see page X, Configuring Wireless Guest Services.

Easy ACL (Access Control Lists)

802.11 wireless networking protocol provides native MAC address filtering capabilities. When MAC address filtering occurs at the 802.11 layer, wireless clients are prevented from authenticating and associating with the wireless access point. Since data communications cannot occur without authentication and association, access to the network cannot be granted until the client has given the network administrator the MAC address of their wireless network card.

The SOHO TZW uses its WGS to overcome this limitation by moving MAC address filtering to the Secure Wireless Gateway layer. This allows wireless users to authenticate and associate with the Access Point layer of the SonicWALL, and be redirected to the WGS by the Secure Wireless Gateway where the user authenticates and obtains WLAN to WAN access.

Easy ACL is an extension of WGS that simplifies the administrative burden of manually adding MAC addresses to the ACL. Users can add themselves to the ACL by providing a user name and password assigned to them by the SonicWALL administrator. WGS must be enabled on the SOHO TZW before Easy ACL can be implemented.

WiFiSec Enforcement

Enabling WiFiSec Enforcement on the SonicWALL enforces the use of IPSec-based VPN for access from the WLAN to the LAN, and provides access from the WLAN to the WAN independent of WGS. Access from one wireless client to another is configured on the **Wireless>Advanced** page where you can disable or enable access between wireless clients.

WiFiSec uses the easy provisioning capabilities of the SonicWALL Global VPN client making it easy for experienced and inexperienced administrators to implement on the network. The level

of interaction between the Global VPN Client and the user depends on the WiFiSec options selected by the administrator. WiFiSec IPsec terminates on the WLAN/LAN port, and is configured using the Group VPN Security Policy including noneditable parameters specifically for wireless access.

- **Apply NAT & Firewall Rules** - On
- **Forward Packets to Remote VPNs** - On
- **Default LAN Gateway** - <management IP Address> if left unspecified
- **VPN Terminated at the LAN/WLAN** - to differentiate between VPN Security Associations terminated at the WAN port.

Configuring Your Wireless Network

You can use the Wireless Wizard to quickly and easily set up your wireless network. Log into the SOHO TZW, and click **Wireless** on the menu bar. Click Wireless Wizard to launch the wizard and begin the configuration process.

Welcome to the SonicWALL Wireless Configuration Wizard



1. When the Wireless Wizard launches, the **Welcome** page is displayed. Click **Next** to continue configuration.

WLAN Network Settings

The screenshot shows a web browser window titled "SonicWALL Wireless Configuration Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.". The page is titled "WLAN Network" and contains the following text and fields:

Review the WLAN network settings for your SonicWALL.

The WLAN IP Address and subnet mask specify the WLAN network.

Enable WLAN

WLAN IP Address:

WLAN Subnet Mask:

At the bottom, there is a SonicWALL logo and three buttons: "< Back", "Next >", and "Cancel".

2. Select **Enable WLAN** to activate the wireless feature of the SOHO TZW. Use the default IP address for the WLAN or choose a different private IP address. The default value works for most networks. Click **Next** to continue.

Alert! You cannot use the same private IP address range as the LAN port of the SOHO TZW.

WLAN 802.11b Settings

The screenshot shows a web browser window titled "SonicWALL Wireless Configuration Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.". The page is titled "WLAN 802.11b Settings" and contains the following text and fields:

Configure the SSID and channel settings for your SonicWALL.

The Service Set ID (SSID) serves as the primary identifier for your wireless network. The SSID may be up to 32 alphanumeric characters long and is case sensitive.

Select the the desired channel of operation for your SonicWALL.

SSID:

Channel:

At the bottom, there is a SonicWALL logo and three buttons: "< Back", "Next >", and "Cancel".

3. Enter a unique identifier for the SOHO TZW in the SSID field. It can be up to 32 alphanumeric characters in length and is case-sensitive. The default value is the serial number of the appliance.

WLAN Security Settings

The screenshot shows the 'WLAN Security Settings' page in the SonicWALL Wireless Configuration Wizard. The page title is 'SonicWALL Wireless Configuration Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.'. The main heading is 'WLAN Security Settings' with the instruction 'Optimize the WLAN security capabilities of your SonicWALL.'. Below this, it says 'Select one of the following security modes for your SonicWALL.'. There are three radio button options: 1. 'WiFiSec VPN Security' (selected) - Enforce IPSec VPN Technology over all wireless connections to provide the highest level of security with SonicWALL's Global VPN. 2. 'WEP + Stealth Mode' - Caution! WEP is a flawed security mechanism and is offered purely for compatibility with existing wireless security standards. Stealth mode hides the WLAN from conventional means of detection. 3. 'Connectivity' - Caution! This mode offers no encryption or access controls and allows unrestrained wireless access to the device. At the bottom, there is a SonicWALL logo and three buttons: '< Back', 'Next >', and 'Cancel'.

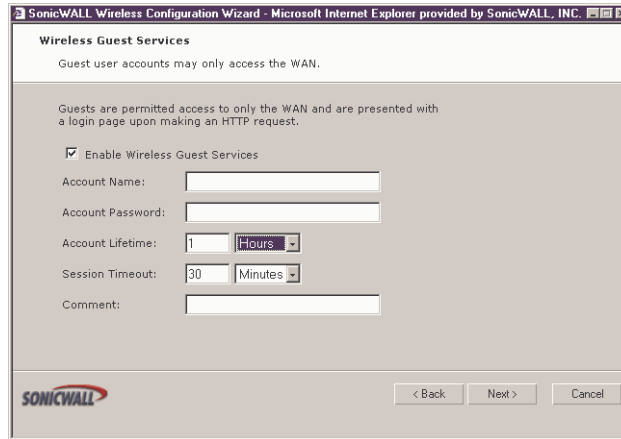
4. Select the desired security setting for the SOHO3 TZW. WiFiSec is the most secure and enforces IPSec over the wireless network. If you have an existing wireless network and want to use the SOHO TZW, select **WEP + Stealth Mode**.

WiFiSec - VPN Client User Authentication

The screenshot shows the 'WiFiSec - VPN Client User Authentication' page in the SonicWALL Wireless Configuration Wizard. The page title is 'SonicWALL Wireless Configuration Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.'. The main heading is 'WiFiSec - VPN Client User Authentication' with the instruction 'Configure the user settings for client WiFiSec connections.'. Below this, it says '1 of 1 users have VPN Client access privileges.' and there is a checkbox labeled 'Give all users VPN Client privileges.' which is currently unchecked. There is a section for creating a new user with VPN client access privileges, with fields for 'User Name:' and 'Password:'. At the bottom, there is a note: 'Note: Manage users from the Objects > Users page.' and a SonicWALL logo. At the very bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

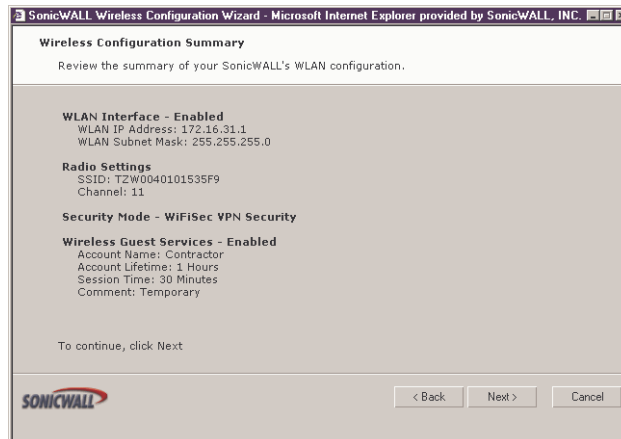
5. Select **Give all users VPN Client privileges** if all wireless clients use the SonicWALL Global VPN Client software. Create a new user with VPN Client privileges by typing a user name and password in the **User Name** and **Password** fields.

Wireless Guest Services



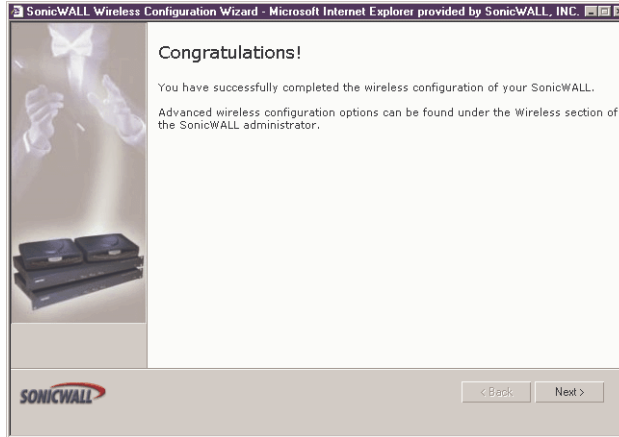
6. **Enable Wireless Guest Services** is selected by default. You can create guest wireless accounts to grant access to the WAN only. If you enable Wireless Guest Services, type a name for the account in the **Account Name** field, and a password in the **Account Password** field. The **Account Lifetime** is set to one hour by default, but you can enter a value and then select **Minutes**, **Hours**, or **Days** to determine how long the guest account is active. Determine how long the connection can be inactive before disconnecting and enter the value in the **Session Timeout** field. Select **Minutes**, **Hours**, or **Days**. Any comments about the connection can be entered in the **Comment** field.

Wireless Configuration Summary



7. Review your wireless settings for accuracy. If you want to make changes, click **Back** until the settings are displayed. Then click **Next** until you reach the **Summary** page.

Congratulations!



8. Congratulations! You have successfully configured your WLAN port on the SOHO TZW.

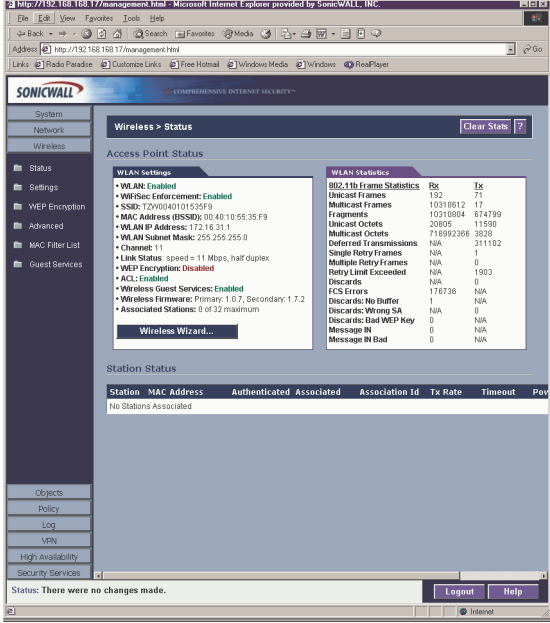
Configuring Additional Wireless Features

The SonicWALL SOHO TZW has the following features available:

- **WiFiSec Enforcement** - an IPsec-based VPN overlay for wireless networking
- **WEP Encryption** - configure Wired Equivalent Privacy (WEP) Encryption
- **Beaconing and SSID Controls** - manage transmission of the wireless signal.
- **Wireless Client Communications** - configure wireless client settings.
- **Advanced Radio Settings** -
- **MAC Filtering** - use MAC addresses for allowing access or blocking access to the SOHO TZW.
- **Wireless Guest Services** - configure limited access accounts for non-employees.

To begin configuring advanced features on the SOHO TZW, log into the management interface, and click **Wireless**. The Status page is displayed and contains information relating to the WLAN connection.

Access Point Status



The screenshot shows the SonicWALL management interface in Internet Explorer. The browser address bar shows <http://192.168.168.17/management.html>. The page title is "SonicWALL Comprehensive Internet Security". The left sidebar contains navigation options: System, Network, Wireless, Status, Settings, WEP Encryption, Advanced, MAC Filter List, and Guest Services. The main content area is titled "Wireless > Status" and includes a "Clear State" button. Below this, there is an "Access Point Status" section with two panels: "WLAN Settings" and "WLAN Statistics".

WLAN Settings:

- WLAN: Enabled
- WiFiSec Enforcement: Enabled
- SSID: DVW04D018455F0
- MAC Address (BSSID): 00:40:10:55:35:F9
- WLAN IP Address: 172.16.31.1
- WLAN Subnet Mask: 255.255.255.0
- Channel: 11
- Link Status: speed = 11 Mbps, half duplex
- WEP Encryption: Disabled
- ACL: Enabled
- Wireless Guest Services: Enabled
- Wireless Firmware: Primary: 0.7, Secondary: 1.7.2
- Associated Stations: 0 of 32 maximum

WLAN Statistics:

802.11b Frame Statistics	Rx	Tx
Unicast Frames	192	71
Multicast Frames	10310612	17
Fragments	10310604	674799
Unicast Octets	20805	11580
Multicast Octets	718992368	3838
Deferred Transmissions	N/A	311102
Single Retry Frames	N/A	1
Multiple Retry Frames	N/A	0
Retry Limit Exceeded	N/A	1903
Discards	N/A	0
FCS Errors	176736	N/A
Discards: No Buffer	1	N/A
Discards: Wrong SA	N/A	0
Discards: Bad WEP Key	0	N/A
Message IN Bad	0	N/A

Station Status:

Station	MAC Address	Authenticated	Associated	Association Id	Tx Rate	Timeout	Power
No Stations Associated							


At the bottom of the page, there is a status message: "Status: There were no changes made." and buttons for "Logout" and "Help".

WLAN Settings	Value
WLAN:	Enabled or Disabled
WiFiSec:	Enabled or Disabled
SSID:	Network Identification Information
MAC Address:	Serial Number of the SOHO TZW
WLAN IP Address:	IP address of the WLAN port
WLAN Subnet Mask:	Subnet information
Channel	Channel Number selected for transmitting wireless signal
Link Status:	Network speed in mbps, full or half duplex
WEP Encryption:	Enabled or Disabled
ACL:	Enabled or Disabled
Wireless Guest Services	Enabled or Disabled
Wireless Firmware:	
Associated Stations:	Number of clients associated with the SOHO TZW

WLAN Statistics

Station Status

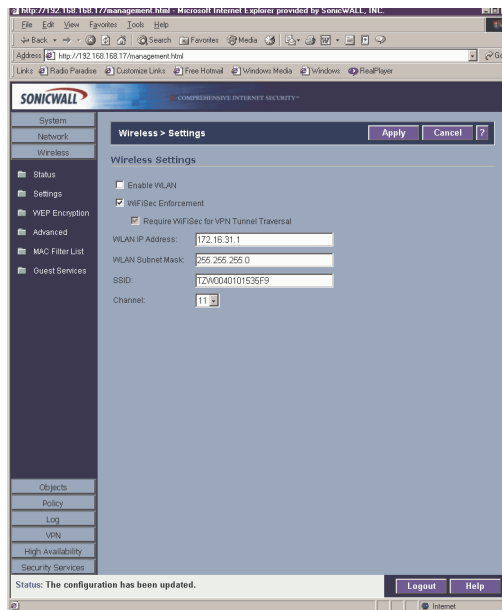
The **Station Status** table displays information about wireless connections associated with the SOHO TZW.

Station	MAC Address	Authenticated	Associated	Association ID	Tx Rate	Timeout	Power Mgmt	Configure
1 - Laura's Laptop	00:20:ED:41:07:6B	Authenticated	Associated	9	2 Mbps	295s	Disabled	

- **Station** - the name of the connection used by the MAC address
- **MAC Address** - the wireless network card MAC address
- **Authenticated** - status of 802.11b authentication
- **Associated** - status of 802.11b association
- **Association ID** - assigned by the SonicWALL
- **Tx Rate** - in Mbps
- **Timeout** - number of seconds left on the session
- **Power Mgmt** - if power management is enabled on your wireless network card, the setting is displayed here.
- **Configure** - delete the entry or add the entry to the MAC Filter List.

Wireless>Settings

On the **Wireless Settings** page, you can enable or disable the WLAN port by selecting or clearing the **Enable WLAN** checkbox.



WiFiSec Enforcement

Select **WiFiSec Enforcement** to use IPSec-based VPN for access from the WLAN to the LAN, and also provide access from the WLAN to WAN independent of Wireless Guest Services. When WiFiSec Enforcement is selected, a second check box, **Require WiFiSec for VPN Tunnel Traversal** is selected by default. When **Require WiFiSec for VPN Tunnel Traversal** is selected, any wireless traffic destined for a remote network with a VPN tunnel is secured by WiFiSec. If **WiFiSec Enforcement** is not selected, you can select or clear the **Require WiFiSec for VPN Tunnel Traversal** checkbox.

Deployment Scenario for WiFiSec and VPN Tunnel Traversal

A site-to-site VPN tunnel is configured between Site 1 and Site 2, both sites using a SOHO TZW, and Site 1 has a wireless client on the LAN. When the wireless client at Site 1 attempts to send data to Site 2 over the VPN tunnel, all data is encrypted between the wireless client, the SOHO TZW at Site 1, and then over the Internet to Site 2.

Insert Graphic Here

To configure the WLAN Settings, log into the SonicWALL, and click **Wireless**, then **Settings**.

1. Select **Enable WLAN** to allow wireless communication over the WLAN port.
2. Select **WiFiSec Enforcement** to encrypt all traffic over the WLAN. If you choose not to enforce WiFiSec on your network, clear the check box. You can then select or clear the **Require WiFiSec for VPN Tunnel Traversal** check box.
3. Type the IP address of the WLAN in the **WLAN IP Address** field or use the default IP address. The default IP address is acceptable for most networks.
4. Type the subnet mask in the **WLAN Subnet Mask** field.
5. Type a name for the SSID in the **SSID** field or use the default value which is SonicWALL.
6. Select a channel from the Channel list. The most frequently used channels are 1, 6, and 11. Channel 11 is considered to be the optimal channel for wireless networking.

Wireless>WEP Encryption

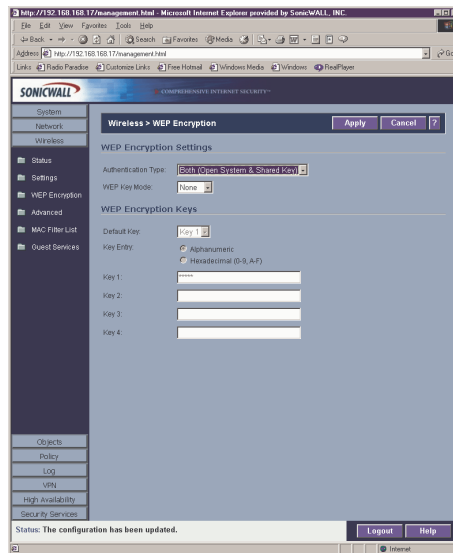
WEP (Wired Equivalent Protocol) can be used to protect data as it is transmitted over the wireless network, but it provides no protection past the SonicWALL. It is designed to provide a minimal level of protection for transmitted data, and is not recommended for network deployments requiring a high degree of security.

WEP Encryption Settings

Open-system authentication is the only method required by 802.11b. In open-system authentication, the SonicWALL allows the wireless client access without verifying its identity. Shared-key authentication uses WEP and requires a shared key to be distributed to wireless clients before authentication is allowed.

The SOHO TZW provides the option of using Open-system, Shared-key, or both when WEP is used to encrypt data.

To configure WEP on the SonicWALL, log into the SonicWALL and click **Wireless**, then **WEP Encryption**.



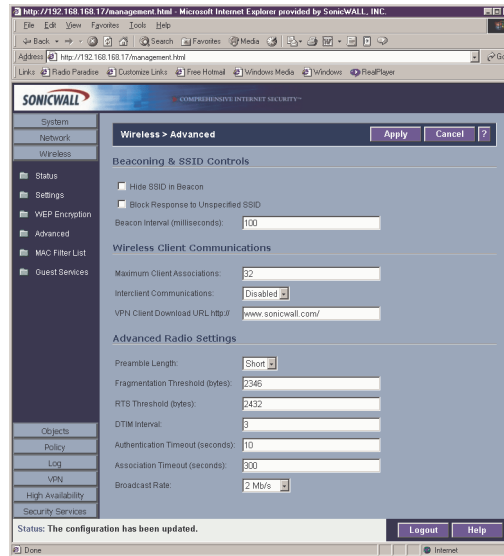
1. Select the authentication type from the **Authentication Type** list. **Both (Open System & Shared Key)** is selected by default.
2. Select 64-bit or 128-bit from the **WEP Key Mode**. 128-bit is considered more secure than 64-bit. This value is applied to all keys. 64-bit keys are 5 characters long and 128-bit keys are 13 characters in length.

WEP Encryption Keys

3. Select the key number, 1,2,3, or 4, from the **Default Key** menu.
4. Select the key type to be either **Alphanumeric** or **Hexadecimal**.

Wireless>Advanced

To access Advanced configuration settings for the SOHO TZW, log into the SonicWALL, click **Wireless**, and then **Advanced**.



Beaming & SSID Controls

1. Select **Hide SSID in Beacon**.
2. Select **Block Response to Unspecified SSID**
3. Type a value in milliseconds for the **Beacon Interval**. Decreasing the interval time makes passive scanning more reliable and faster because Beacon frames announce the network to the wireless connection more frequently.

Wireless Client Communications

1. Enter the number of clients to associate with the SHO3 TZW in the **Maximum Client Associations** field.
2. If you do not want wireless clients communicating to each other, select **Disabled** from the **Interclient Communications** menu. If you want wireless clients communicating with each other, select **Enabled**.
3. Guests on the wireless network can download the SonicWALL Global VPN Client to install on their computer or laptop. Type the URL location for the software in the **VPN Client Download URL http://** field.

Advanced Radio Settings

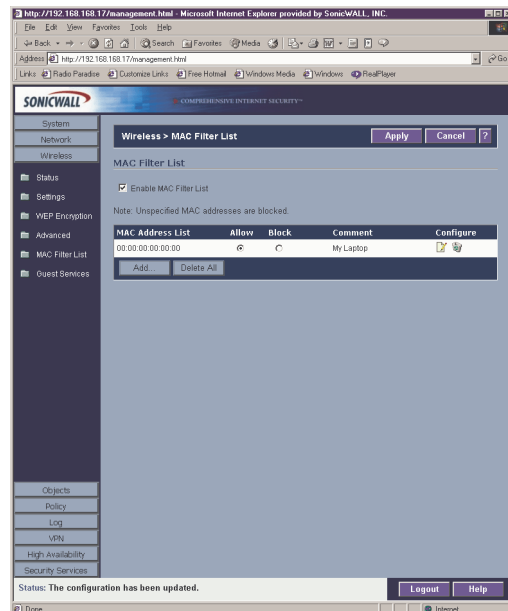
Advanced Radio Settings	
Preamble Length:	Short
Fragmentation Threshold (bytes):	2346
RTS Threshold (bytes):	2432
DTIM Interval:	3
Authentication Timeout (seconds):	10
Association Timeout (seconds):	300
Broadcast Rate:	2 Mb/s

1. Select **High** from the **Transmit Power** menu to send the strongest signal on the WLAN.
2. Select **Short** or **Long** from the **Preamble Length** menu. **Short** is recommended for efficiency and improved throughput on the wireless network.
3. The **Fragmentation Threshold (bytes)** is 2346 by default. Increasing the value means that frames are delivered with less overhead but a lost or damaged frame must be discarded and retransmitted.
4. The **RTS Threshold (bytes)** is 2432 by default. If network throughput is slow or a large number of frame retransmissions is occurring, decrease the RTS threshold to enable RTS clearing.
5. The default value for the **DTIM Interval** is 3. Increasing the DTIM Interval value allows you to conserve power more effectively.
6. The Authentication process times out after 10 seconds by default. If your network is very busy, you can increase the timeout by increasing the number of seconds in the **Authentication Timeout (seconds)** field.
7. The Association Timeout (seconds) is 300 seconds by default. If your network is very busy, you can increase the timeout by increasing the number of seconds in the **Authentication Timeout (seconds)** field.
8. Broadcast Rate?

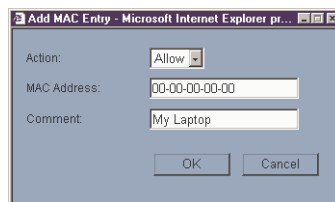
Wireless>MAC Filter List

Wireless networking provides native MAC filtering capabilities which prevents wireless clients from authenticating and associating with the SOHO TZW. If you enforce MAC filtering on the WLAN, wireless clients must provide you with the MAC address of their wireless networking card.

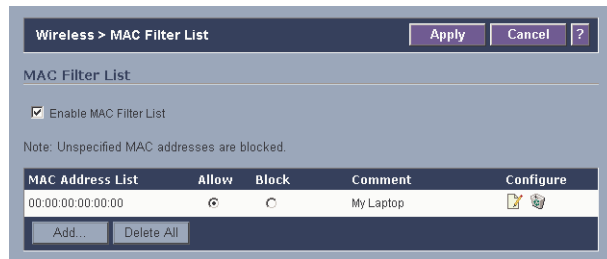
To set up your MAC Filter List, log into the SonicWALL, and click **Wireless**, then **MAC Filter List**.



1. Click **Add** to add a MAC address to the **MAC Filter List**.



2. Select **Allow** from the **Action** menu to allow access to the WLAN. To deny access, select Block.
3. Type the MAC address in the **MAC Address** field. The two character groups should be separated by a hyphen.
4. Type a name or comment in the **Comment** field. The **Comment** field can be used to identify the source of the MAC address.
5. Click **OK** to add the MAC address.

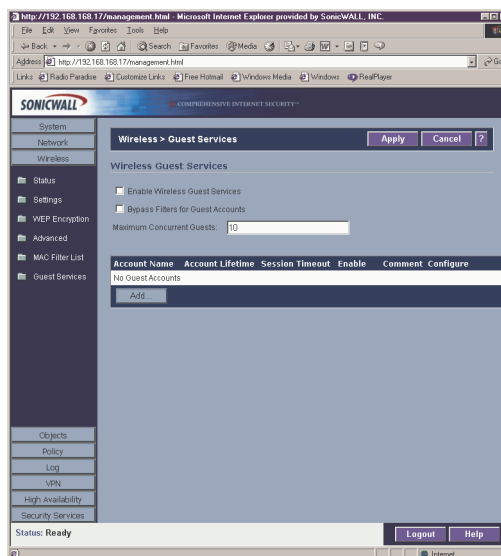


Once the MAC address is added to the **MAC Address List**, you can select **Allow** or **Block** next to the entry. For example, if the user with the wireless card is not always in the office, you can select **Block** to deny access during the times the user is offsite.

Click on the Notepad icon under **Configure** to edit the entry. Click on the Trashcan icon to delete the entry. To delete all entries, click **Delete All**.

Wireless>Guest Services

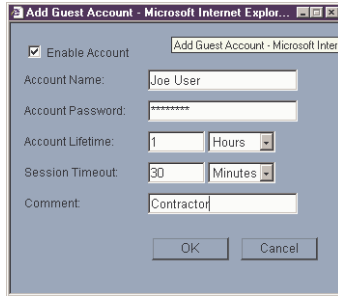
Wireless Guest Services allow you to create access accounts for temporary use that allow wireless clients to connect from the WLAN to the WAN. To configure Wireless Guest Services, log into the SonicWALL, and click **Wireless**, then **Guest Services**.



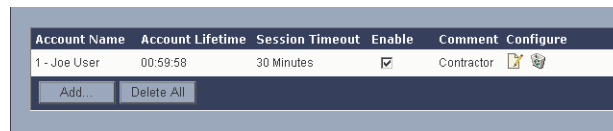
1. Select **Enable Wireless Guest Services**.
2. If your Guest Accounts are associated with the **Users** feature of the SonicWALL, you can select **Bypass Filters for Guest Accounts**. See the Users, page X, Chapter X, Objects, for information on configuring User Level Access.



TIP! You can have Wireless Guest Accounts without configuring User Level Access. Wireless Guest Accounts are considered more temporary than permanent.

3. Type the number of wireless clients that can use the same Guest Account in the **Maximum Concurrent Guests** field.
4. To add a Guest Account, click **Add**.



5. **Enable Account** is selected by default.
6. Enter a name for Guest Account in the **Account Name** field. In the example above, it is "Joe User".
7. Enter a password in the **Account Password** field.
8. Configure the **Account Lifetime** by entering a value in the field, and then selecting **Minutes, Hours, or Days**.
9. Configure the **Session Timeout** by entering a value in the field, and then selecting **Minutes, Hours, or Days**.
10. Enter any comments in the **Comment** field, and click **OK** to add the Guest Account. Guest Account information is displayed in the **Guest Account** table.



Account Name	Account Lifetime	Session Timeout	Enable	Comment	Configure
1 - Joe User	00:59:58	30 Minutes	<input checked="" type="checkbox"/>	Contractor	 

To disable a Guest Account, clear the **Enable** check box in the Guest Account entry line. To edit an existing Guest Account, click on the Notepad icon under **Configure**. To delete a Guest Account, click the Trashcan icon under **Configure**. To delete all Guest Accounts, click **Delete All**.