

SonicWALL TZ 150 Wireless Security Appliance Getting Started Guide

The SonicWALL® TZ 150 Wireless is a total security platform for both your wired and wireless network, delivering true layered security by integrating gateway anti-virus, intrusion prevention and content filtering capabilities for small networks in an easy-to-use, low cost platform.

This *Getting Started Guide* provides instructions for basic installation and configuration of the *SonicWALL TZ 150 Wireless*. After you complete this guide, up to 10 computers on your Local Area Network (LAN) will have secure Internet access.

Note: For complete documentation, refer to the [SonicOS Standard Administrator's Guide on the SonicWALL Resource CD](#) or at: <http://www.sonicwall.com/us/support.html>.

Before You Begin

Check Package Contents

- One SonicWALL TZ 150 Wireless security appliance
- One SonicWALL TZ 150 Wireless Getting Started Guide
- One SonicOS Standard 3.1 Release Notes
- One Ethernet cable
- One 12V, 1.66A power supply
- One SonicWALL Resource CD, which contains product documentation and software utilities.

Any Items Missing?

If any items are missing from your package, contact:

SonicWALL Support

Web: <http://www.sonicwall.com/support/>

E-mail: customer_service@sonicwall.com

SonicWALL TZ 150 Wireless Configuration

This Getting Started Guide covers the following procedures. Procedures 1 through 6 are required for initial configuration of your SonicWALL TZ 150 Wireless security appliance.

- | | | |
|----|--|---------|
| 1 | Collect Required Information | page 3 |
| 2 | Applying Power to the SonicWALL TZ 150 Wireless | page 4 |
| 3 | Connecting the SonicWALL TZ 150 Wireless | page 5 |
| 4 | Accessing the Management Interface | page 7 |
| 5 | Using the SonicWALL Setup Wizard | page 9 |
| 6 | Registering Your SonicWALL TZ 150 Wireless | page 20 |
| 7 | Activating SonicWALL Security Services | page 25 |
| 8 | Connecting Wireless Clients to the SonicWALL TZ 150 Wireless | page 29 |
| 9 | Connecting Computers to Your SonicWALL TZ 150 Wireless | page 33 |
| 10 | Wall Mounting the SonicWALL TZ 150 Wireless | page 36 |

What You Need to Begin

- A computer to use as a management station for initial configuration of the SonicWALL TZ 150 Wireless
- An Internet connection
- A Web browser for accessing the SonicWALL TZ 150 Wireless's Web-based management interface. The Web browser must support Java and HTTP uploads. Internet Explorer 5.0 or higher or Netscape Navigator 4.7 or higher are recommended.

1

Collect Required Information

Internet Service Provider (ISP) Information

Collect the following information about your Internet service:

If you connect via	You probably use	Please record
Cable modem, DSL with a router	DHCP	You do not need to provide any Internet connection information.
Home DSL	PPPoE	User Name: _____ Password: _____ Note: Your ISP may require your user name in the format: <i>name@ISP.com</i>
T1, Static broadband, Cable or DSL with a static IP	Static IP	IP Address: _____ Subnet Mask: _____ Default Gateway (Router Address): _____ Primary DNS: _____ Secondary DNS (optional): _____
Dial in to a server	PPTP	Server Address: _____ User Name: _____ Password: _____

Note: If you are not using one of the network configurations above, refer to the SonicOS Standard Administrator's Guide available on the SonicWALL Resource CD and on the Web at:

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

Other Information

SonicWALL Management Interface


To access the SonicWALL TZ 150 Wireless Web-based management interface. These are the default settings, which you can change:



User Name: admin

Password: password

2

Applying Power to the SonicWALL TZ 150 Wireless

1. Plug the power supply into back of the security appliance  and into an appropriate power outlet.

The Power LED  on the front panel lights up green when you plug in the SonicWALL TZ 150 Wireless. The Test LED  may light up and may blink while the appliance performs a series of diagnostic tests. When the Test light is no longer lit, the security appliance is ready for configuration.



If the Test LED remains lit after the SonicWALL TZ 150 Wireless has booted, Restart the security appliance.

For more trouble shooting information, refer to the *SonicOS Standard Administrator's Guide* available on the SonicWALL Resource CD and on the Web at:

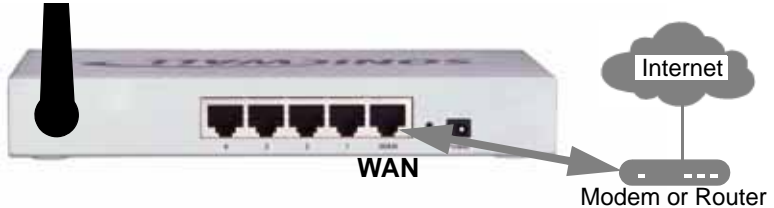
<http://www.sonicwall.com/us/support.html>

3

Connecting the SonicWALL TZ 150 Wireless

Connecting the Ethernet Cables

Connect the WAN Cable



1. Connect one end of an Ethernet cable to your Internet connection, such as a DSL modem or cable modem.
This cable may already be connected between your computer and your modem. If so, disconnect it from your computer, and leave it connected to the Internet.
2. Connect the other end of the cable to the **WAN** port on the back of your SonicWALL TZ 150 Wireless.

The **WAN** LEDs on the front panel light up indicating an active connection.



Connect the LAN Cable



1. Connect one end of another Ethernet cable to the computer you are going to use to manage the SonicWALL TZ 150 Wireless.
2. Connect the other end of the cable to port # 1 on the back of your SonicWALL TZ 150 Wireless.

The port # 1 LEDs on the front panel light up indicating an active connection.



4

Accessing the Management Interface

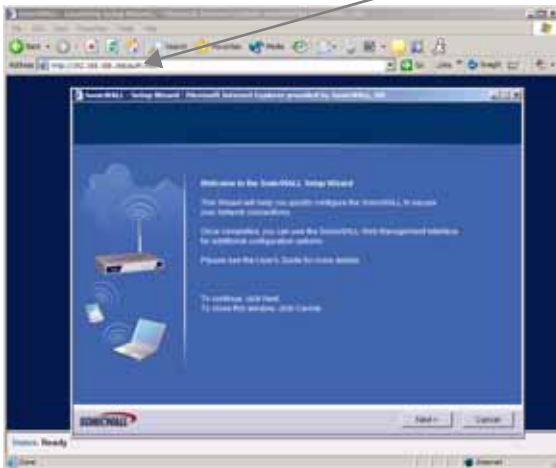
To access the Web-based management interface of the SonicWALL TZ 150 Wireless:

1. On the computer you have connected to port # 1, Start your Web browser.

Alert: Turn off pop-up blocking software before accessing the SonicWALL management interface.

Your Web browser must support Java and HTTP uploads. Internet Explorer 5.0 or higher or Netscape Navigator 4.7 or higher are recommended.

2. Enter **http://192.168.168.168** in the **Location** or **Address** field.



3. The **SonicWALL Setup Wizard** launches and guides you through the configuration and setup of your SonicWALL TZ 150 Wireless.

If the SonicWALL Setup Wizard Does Not Appear

If you cannot connect to the SonicWALL TZ 150 Wireless or the **Setup Wizard** does not display, verify the following configurations:

- Did you correctly enter the SonicWALL TZ 150 Wireless management IP address in your Web browser?
- Is your computer running pop-up blocking software?
- Are the Local Area Connection settings on your computer set to obtain an IP address dynamically (DHCP)? see Procedure 7, “Connecting Computers to Your SonicWALL TZ 150 Wireless” on page 33 for instructions on changing your Local Area Connection settings.
- Do you have the Ethernet cable connected to your computer and to port **1** on your SonicWALL TZ 150 Wireless?
- Some browsers may not launch the **Setup Wizard** automatically. In this case, log into SonicWALL TZ 150 Wireless using “**Admin**” as the user name and “**password**” as the password. After you log in, click the **Wizards** button on the **System > Status** page. Select **Setup** to begin configuring your SonicWALL TZ 150 Wireless.

5

Using the SonicWALL Setup Wizard

The SonicWALL **Setup Wizard** provides user-guided instructions for configuring your SonicWALL TZ 150 Wireless.

Note: Make sure you have any required ISP information to complete the configuration before using the **Setup Wizard**. See the list of required information in Procedure 1, “Collect Required Information” on page 3.

Tip: If you do not know what type of Internet connection you have, contact your ISP. In addition, the SonicWALL **Setup Wizard** will attempt to detect your connection settings. You will see what is automatically selected in Setup Wizard page 4, **WAN Network Mode**

Welcome - Click **Next** to begin.

1. **Deployment Scenario** - select the wireless deployment scenario that best matches your deployment requirements. Clicking on the deployment scenario link displays a diagram of the deployment to show how the scenario is best used.



Select **Office Gateway**, which is a commonly used wireless deployment for LAN and WLAN to Internet connectivity.



2. **Change Password** - Change the administrative password. This is the password for the **admin** account.

Old Password	Should be populated with the default password, <i>password</i> .
New Password	Enter your new password.
Confirm	Re-enter your new password.

Note: Keep your new password in a safe place. If you lose your password, you will have to reset the SonicWALL TZ 150 Wireless to factory settings, losing your configuration. For instructions on resetting your SonicWALL TZ 150 Wireless, See the [SonicOS Standard Administrator's Guide](#) available on the SonicWALL Resource CD and on the Web at:

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

Click **Next**.

3. **Change Time Zone** - Change the **Time Zone** setting to your local time zone.

Time Zone	Select the time zone for your location from the list.
Automatically adjust clock for daylight saving time	Check this if you live in an area that observes Daylight Savings Time.

Click **Next**.

Note: *It is important that you set the time zone correctly before you register your SonicWALL TZ 150 Wireless.*

4. **WAN Network Mode** - The **Setup Wizard** automatically detects most networking modes. If it does not detect the networking mode, you may have a Static IP Address. See Procedure 1, "Collect Required Information" on page 3.

Confirm the selection or select the correct type of network connection for your network.

Static IP	Select Static IP if you want to give the SonicWALL TZ 150 Wireless a specific, unchanging IP address.
DHCP	Select DHCP if your ISP assigns your computer a dynamic IP Address. DHCP is commonly used with cable modems.
PPPoE	Select PPPoE if your ISP requires a username and password to establish a connection and assign a dynamic address. PPPoE is commonly used with DSL modems.
PPTP	Select PPTP if you dial into a specific server and log into a VPN to establish a connection. With PPTP, you can have either a static or dynamic IP Address.

Click on the yellow link for a networking type to see a definition.

Click **Next**.

5. **WAN Network Mode** - The second WAN network mode page configures your WAN settings for the selection you made in the previous page.

WAN Network Mode: NAT Enabled (Static IP)

SonicWALL WAN IP Address	Enter a single, static IP address. This must be in the correct address range for your ISP.
WAN Sub-net Mask	Enter the subnet mask for your network, for example, 255.255.255.0.
Gateway (Router) Address	Enter the IP address of your internet gateway.
DNS Server Address	Enter the IP address of the DNS server for your network.
DNS Server Address #2 (optional)	You can enter a secondary, back-up DNS server to use if the first one fails.

Click **Next**.

WAN Network Mode: NAT with DHCP Client

You do not need to enter any WAN networking settings. The network settings are provisioned automatically from a DHCP server.

Click **Next**.

WAN Network Mode - NAT with PPPoE Client

Obtain an IP Address Automatically	Select this if your ISP assigns you a dynamic IP address.
Use the following IP Address	Select this if your ISP has assigned you a static IP address, and enter the address.
PPPoE User Name	Enter the user name for your Internet account. The username usually includes “@” and the domain name, for example, <i>joe.user@ispgate-way.net</i> .
PPPoE Password	Enter the password for your internet account.
Inactivity Disconnect (minutes)	Check this box if you want the SonicWALL TZ 150 Wireless to disconnect from the Internet if there is no traffic for the number of minutes you enter.

Click **Next**.

WAN Network Mode: NAT with PPTP Client

PPTP Server IP Address	Enter the address of the server you are connecting to.
PPTP User Name	Enter your network user name.
PPTP Password	Enter your network password.
Obtain an IP Address Automatically	Select this if the server assigns you a dynamic IP address.
Use the following IP Address	Check this if you have been given a static IP address, and fill in the following three fields.
SonicWALL WAN IP Address	Enter the static IP address for your connection.
WAN/DMZ Subnet Mask	Enter the subnet mask for your connection.
Gateway (Router) Address	Enter the address of your Internet Gateway.

Click **Next**.

6. **LAN Settings** - The LAN Settings page configures your LAN interface. These settings apply to all twenty-four LAN ports.

SonicWALL LAN IP Address	Accept the default IP address or enter a new IP address of the LAN interface.
LAN Subnet Mask	Accept the default, or enter a subnet mask for your LAN.
Enable Windows Networking Support	Leave this option checked if you plan to have more than one Windows computer, Windows Networking allows them to communicate with each other. If you have only one Windows computer or have computers with other operating systems, Windows Networking has no effect.

By default, your SonicWALL TZ 150 Wireless is configured with a LAN network IP address, **192.168.168.168**, and subnet mask, **255.255.255.0**, that will work well for most installations. In most cases, leave the default LAN IP address and subnet mask unchanged.

Note: *The LAN IP address is the address you will use to access the SonicWALL TZ 150 Wireless management interface.* !

Click **Next**.

7. **LAN DHCP Settings** - The LAN DHCP Settings page allows you to select whether or not to use the DHCP Server in the SonicWALL TZ 150 Wireless to automatically distribute IP addressing information to computers and other network devices on your LAN.

Enable DHCP Server on LAN	Leave checkbox checked to use the DHCP server in the SonicWALL TZ 150 Wireless. Do not use select this option if you already have a DHCP server on your network, or if you want to require your network clients to have static IP addresses.
LAN Address Range	If you enabled the DHCP Server, enter a range of IP addresses in the same subnet as the LAN IP address. Leave the default range unchanged if you accepted the default LAN IP address and subnet mask settings in the previous page.

Click **Next**.

8. **WLAN 802.11b/g Settings** - The WLAN 802.11b/g Settings page allows you to configure your wireless network settings.

SSID	Enter a unique name your wireless clients will use to identify the SonicWALL TZ 150 Wireless connection.
Radio Mode	Select which radio transmission standard you want to use. The default, Mixed , works for most office and home settings.
Country Code	Select the country where you are deploying this SonicWALL TZ 150 Wireless
Channel	Select the broadcast channel you want the SonicWALL TZ 150 Wireless to use. The default, AutoChannel automatically detects the channel with the least interference to use.

Click **Next**.

9. **WiFiSec** - WiFiSec is a security standard that uses an IPSec VPN to secure wireless network connections. The WiFiSec page allows you to create a first VPN user to connect securely to your wireless network. WiFiSec is disabled by default.

User Name	Enter a user name for the VPN user.
Password	Enter a unique password for the user.
Confirm Password	Re-enter the password.

- 10.

Click **Next**.

Note: You add additional users in the **Users> Settings** page in the SonicWALL TZ 150 Wireless security appliance's Management Interface. See the SonicOS Standard Administrator's Guide for instructions.

11. **Wireless Guest Services** - Wireless Guest services allow guest users to connect through your wireless network to the internet without any access to your network.

Enable Wireless Guest Services	Check to enable Wireless Guest Services on your network.
Account Name	Enter the account name your guest users must use to log into Wireless Guest Services.
Account Password	Enter a password for the guest account.
Confirm Password	Re-enter the password
Account Lifetime	Specify how long this account may exist before you need to regenerate it.
Session Lifetime	Specify how long a guest user may be logged in.
Comment	A brief description of the guest account.

Click **Next**.

12. **SonicWALL Configuration Summary** - Displays your network configuration information.



Setup Wizard Complete - your SonicWALL TZ 150 Wireless is now successfully configured for LAN, Wireless, and Internet access. Click **Restart** to complete the configuration process.

13. Test your connection: After the SonicWALL TZ 150 Wireless reboots, open a Web browser, and go to <http://www.sonicwall.com>

If you can view the SonicWALL home page, you have configured everything correctly.

If you cannot view the SonicWALL home page try a second URL. If you still cannot view a Web page, return to procedure 4, "Accessing the Management Interface" on page 7, log in as "admin" with your administrative password, and click on the Wizards button in the top right corner of the management interface to restart the wizard.

6

Registering Your SonicWALL TZ 150 Wireless

Once you've established your Internet connection, it is recommended you register your SonicWALL security appliance at mySonicWALL.com. Registering your SonicWALL security appliance provides the following benefits:

- Try a FREE 30-day trial of SonicWALL's Gateway Anti-Virus, Anti-Spware and Intrusion Prevention Service, Content Filtering Service, Enforced-Client Anti-Virus/Anti-Spyware.
- Activate SonicWALL security services
- Access SonicOS firmware updates
- Get SonicWALL technical support

Alert: *The **Time Zone** and **DNS** settings on your SonicWALL TZ 150 Wireless must be set correctly before registering your security appliance. See Step 5, "Using the SonicWALL Setup Wizard" on page 9 for instructions on setting the Time Zone and DNS settings.*

Before You Register

You need a mySonicWALL.com account to register the SonicWALL TZ 150 Wireless. You can create a new mySonicWALL.com account directly from the SonicWALL management interface.

Alert: *Make sure the DNS and Time settings on your SonicWALL TZ 150 Wireless are correct when you register the device. Configure Time settings in the **System > Time** page. Configure DNS settings in the **Edit Interface** window from the **Network > Interfaces** page.*

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

Creating a mySonicWALL.com Account

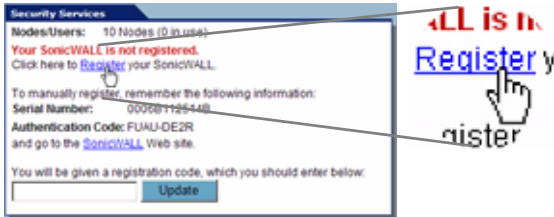
Creating a mySonicWALL.com account is fast, simple, and FREE. Simply complete an online registration form in the SonicWALL TZ 150 Wireless management interface.

If you already have a mysonicWALL.com account, go to “Registering Your SonicWALL TZ 150 Wireless” on page 23 to register your appliance.

1. If you are not logged into the SonicWALL TZ 150 Wireless management interface log in with the username **admin** and the administrative password you set in the **Setup Wizard**.
2. If the **System > Status** page is not displaying in the management interface, click **System** in the left-navigation menu, and then click **Status**.



3. On the **System > Status** page, in the **Security Services** section, click the **Register** link in **Your SonicWALL is not registered**. **Click here to Register your SonicWALL**.



4. In the **mySonicWALL.com Login** page, click the **here** link in “**If you do not have a mySonicWALL account, please click here to create one.**” The mySonicWALL.com account form is displayed.



5. In the **MySonicWall Account** page, enter in your information in the **Account Information, Personal Information** and **Preferences** fields. All fields marked with an asterisk (*) are required fields.
- Note:** Remember your username and password to access your mySonicWALL.com account.
6. Click **Submit** after completing the **MySonicWALL Account** form.
7. When the mySonicWALL.com server has finished processing your account, you will see a page saying that your account has been created. Click **Continue**.

Congratulations. Your mySonicWALL.com account is activated. Now you need to log into mySonicWALL.com to register your SonicWALL TZ 150 Wireless.

Registering Your SonicWALL TZ 150 Wireless

1. If you are not logged into the SonicWALL TZ 150 Wireless management interface, log in with the username **admin** and the administrative password you set in the **Setup Wizard**.
2. If the **System > Status** page is not displaying in the management interface, click **System** in the left-navigation menu, and then click **Status**.



3. On the **System > Status** page, in the **Security Services** section, click the **Register** link. The **mySonicWALL.com Login** page is displayed.

A screenshot of the mySonicWALL.com Login page. The page has a light blue background. At the top, the text "mySonicWALL.com Login" is displayed. Below this, there is a paragraph of text explaining the service. At the bottom of the page, there are two input fields: "User Name:" and "Password:". Below these fields is a blue "Submit" button.

4. Enter your mySonicWALL.com account username and password in the **User Name** and **Password** fields, then click **Submit**.
5. The next several pages inform you about SonicWALL's Security Services. Click **Continue** on each page.
6. At the top of the **Product Survey** page, enter a "friendly name" for your SonicWALL security appliance in the **Friendly Name** field. The friendly name allows you to easily identify your SonicWALL security appliance in your mySonicWALL.com account.
7. Please complete the Product Survey. SonicWALL uses this information to further tailor services to fit your needs.

Note: SonicWALL Product Survey information is not sold or shared with any other company.

8. Click **Submit**.
9. When the mySonicWALL.com server has finished processing your registration, you will see a page informing you that your SonicWALL TZ 150 Wireless appliance is registered. Click **Continue**, and the **System > Licenses** page is displayed showing the available security services. You can activate the services from this page now or at any time in the future.

Congratulations

Your SonicWALL TZ 150 Wireless is now fully operational.

You can continue with this Getting Started Guide to:

- Activate SonicWALL Security Services.
- Set up computers on your network
- Mount your SonicWALL TZ 150 Wireless on a wall or to any vertical surface

7

Activating SonicWALL Security Services

When you register your SonicWALL TZ 150 Wireless, you are eligible for a Free Trial of the SonicWALL Security Services:

- **Gateway Anti-Virus/Anti-Spyware/Intrusion Prevention Service** - Provides real-time protection for all hosts behind your SonicWALL from viruses, spyware, worms and application-layer attacks using deep packet inspection to detect and prevent malicious content before it can reach hosts on your network
- **Enforced Client Anti-Virus/Anti-Spyware** - protects hosts on your network from viruses by enforcing the use of client-based Anti Virus software
- **Premium Content Filtering Service** - Enhances productivity by limiting access to objectionable Web content

At the end of your free trial period, the services will automatically expire unless you purchase a subscription from your reseller or at <https://www.mySonicWALL.com>.

Activate the SonicWALL Security Services

If your SonicWALL management interface is displaying the **Manage Services Online** table on the **System > Licenses** page, skip to Step 5.

1. Log in to your SonicWALL management interface.
2. In the left-navigation menu, click **System** and then **Licenses**.
3. Near the bottom of the **System > Licenses** page, under **Manage Security Services Online**, click the link: **For Free Trials, Click Here**.
4. Log in with your mySonicWALL.com account name and password, if prompted.
5. In the **Manage Services Online** table, click **Try** in the **Free Trial** column for **Gateway Anti-Virus**.

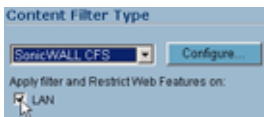
- In the SonicWALL Gateway Anti-Virus page, click **Continue**. Your Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service free trial is now activated.
- In the **Manage Services Online** table, click **Try** in the **Free Trial** column for **Enforced-Client Anti-Virus/Anti-Spyware** and for **CFS Premium Service** to activate the Complete Anti-Virus and Content Filtering Service (CFS) free trials.

Your SonicWALL Security Service free trials are now activated. You must now enable each service on your SonicWALL security appliance. Use the following instructions to configure each service with its default values. For complete configuration instructions, see the administrative guides available on your SonicWALL Resource CD and on the Web at:

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

Enabling Premium Content Filtering Service

- Select the **Security Services > Content Filter** page in the SonicWALL management interface.
- Select the **LAN** checkbox to apply the filter to all computers on your LAN interface.



- Click **Configure**, select the categories to block in the **URL List** tab, and click **OK**.
- Click **Apply** in the top-right corner of the page.

Enabling Enforced Anti-Virus/Anti-Spyware Service

1. Select the **Security Services > Enforced Client Anti-Virus/Anti-Spyware** page in the SonicWALL management interface.
2. Select the **Enable Anti-Virus** checkbox.



3. Click **Apply** in the top-right corner of the page.

Users on your network will be prompted to download the SonicWALL Anti-Virus client.

Enabling Intrusion Prevention Service

1. Select the **Security Services > Intrusion Prevention** page in the SonicWALL management interface.
2. In the **IPS Global Settings** section, click the **Enable IPS on Interface** checkbox, and check the **WAN** and **LAN** interface check boxes.



3. In the **Signature Groups** table, select **Prevent All** for **High Priority** attacks.
4. Click **Apply** in the top-right corner of the page.

Enabling Gateway Anti-Virus Service

1. Select the **Security Services > Gateway Anti-Virus** page in the SonicWALL management interface.
2. In the **Gateway Anti-Virus Global Settings** section, click the **Enable Gateway Anti-Virus on Interface** checkbox, and check the **WAN** and **LAN** interface boxes.



3. Click **Apply** in the top-right corner of the page.

Enabling Anti-Spyware Service

1. Select the **Security Services > Anti-Spyware** page in the SonicWALL management interface.
2. In the **Gateway Anti-Spyware Global Settings** section, click the **Enable Anti-Spyware** checkbox.
3. Select which interfaces you want to apply Anti-Spyware service on, You can select any combination of **WAN, LAN, and OPT**.
4. For best protection from spyware, select the **Prevent All** checkbox for High, Medium, and Low danger levels. This will block all spyware that can be detected.



5. Click **Apply** in the top-right corner of the page.

8

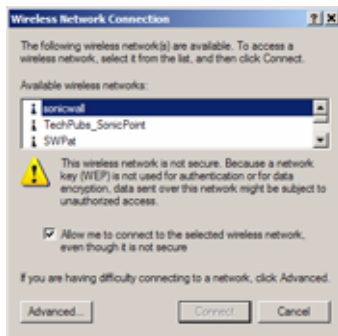
Connecting Wireless Clients to the SonicWALL TZ 150 Wireless

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

- A wireless network card installed and configured for the SonicWALL TZ 150 Wireless' SSID
- SonicWALL GVC installed and configured for a secure wireless connection

Connecting to the Wireless Network

You connect to the wireless network according to the requirements of your client operating system. Your wireless client may automatically detect and display the SonicWALL TZ 150 Wireless' SSID in a list of available wireless networks or you may need to manually configure your wireless card with the SonicWALL TZ 150 Wireless' SSID.



Establishing Secure Wireless Connections

For a wireless client to securely connect to the SonicWALL TZ 150 Wireless using WiFiSec, the SonicWALL Global VPN Client (GVC) must be installed and configured, and WiFiSec must be enabled. Installing and configuring SonicWALL GVC involves the following procedures:

- “Installing the SonicWALL GVC Using the Setup Wizard” on page 30
- “Creating an Office Gateway Connection Profile Using the New Connection Wizard” on page 31
- “Establishing a WiFiSec VPN Connection Using the WLAN GroupVPN Policy” on page 32

Installing the SonicWALL GVC Using the Setup Wizard

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

Note: SonicWALL GVC is free to use for WiFiSec secured wireless connections. For remote VPN access through a WAN port, you must have a GVC Client License. For complete product documentation on SonicWALL GVC, see your Resource CD or visit the SonicWALL Web site at

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

Tip: You can download the latest GVC installer at SonicWALL’s product Web site at

<http://help.mysonicwall.com/applications/vpnclient>.

Creating an Office Gateway Connection Profile Using the New Connection Wizard

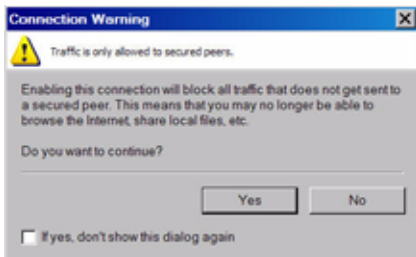
1. In your Windows Start Menu, Choose **Start > Programs > SonicWALL Global VPN Client**. The first time you open SonicWALL GVC, the **New Connection Wizard** automatically launches.



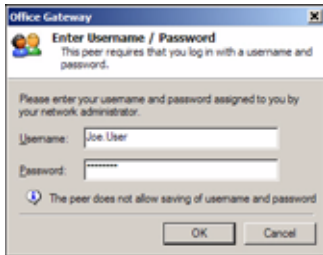
- If the **New Connection Wizard** does not display, click the **New Connection Wizard** icon on the far left side of the toolbar to launch it. Click **Next**.
2. In the **Choose Scenario** page, select **Office Gateway**. Click **Next**.
 3. In the **Completing the New Connection Wizard** page select any of the following options:
 - Select **Create a desktop shortcut to this connection**, if you want to create a shortcut icon on your desktop for this VPN connection.
 - Select **Enable this connection when the program is launched**, if you want to automatically establish this VPN connection when you launch the SonicWALL Global VPN Client.
 4. Click **Finish**. The new VPN connection policy appears in the **SonicWALL Global VPN Client** window.

Establishing a WiFiSec VPN Connection Using the WLAN GroupVPN Policy

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



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

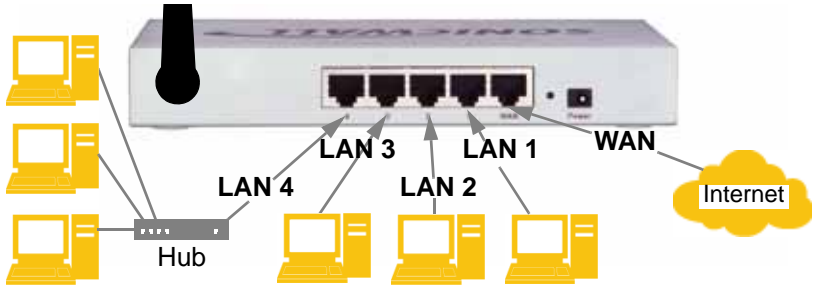


4. Click **OK**. You now have secure wireless access to all the networks, subnets, and addresses you assigned the user access.

9

Connecting Computers to Your SonicWALL TZ 150 Wireless

You can attach up to ten computers to your SonicWALL TZ 150 Wireless.



Configuring DHCP IP Addressing

Complete the following section based on your operating system in order to configure your management computer to obtain an IP address automatically (using DHCP addressing):

Note: *If you are not using DHCP, refer to the [SonicOS Standard Administrator's Guide](#) available on the SonicWALL Resource CD and on the SonicWALL's Documentation Web Site at:*

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

Windows Vista

1. From the **Start** menu, right-click **Network** and select **Properties**.
2. In the **Tasks** menu, click **Manage network connections**, the Network Connections windows displays.
3. Right-click on your **Local Area Connection** and select **Properties**.
4. In the list, double-click **Internet Protocol Version 4 (TCP/IP)**.
5. Select **Obtain an IP address automatically** and **Obtain a DNS address automatically**.
6. Click **OK**, and then click **OK** again for the settings to take effect.

Windows XP

1. From the **Start** menu, highlight **Connect To** and then select **Show All Connections**.
2. Right-click on your **Local Area Connection** and select **Properties**.
3. In the list, double-click **Internet Protocol (TCP/IP)**.
4. Select **Obtain an IP address automatically** and **Obtain a DNS address automatically**.
5. Click **OK**, and then click **OK** again for the settings to take effect.

Windows 2000

1. From your Windows **Start** menu, select **Settings**.
2. Open **Network and Dial-up Connections**.
3. Click **Properties**.

4. Highlight **Internet Protocol (TCP/IP)** and click **Properties**.
5. Select **Obtain an IP address automatically** and **Obtain a DNS address automatically**.
6. Click **OK** for the settings to take effect.

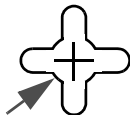
Wall Mounting the SonicWALL TZ 150 Wireless

You can mount your SonicWALL TZ 150 Wireless on a wall or any vertical surface. Use the template on the next page as a guide for placing the mounting screws.

1. Using the template on the next page, attach two screws to the surface where you want to mount the security appliance.
The mounting screws should have a head between 3/16" and 1/4" in diameter.
The mounting screws should stick approximately 1/8" out from the surface.
2. Slide the slots in the back of the SonicWALL TZ 150 Wireless over the heads of the mounting screws and then slide the security appliance down to secure it in place.

SonicWALL TZ 150 Wireless Mounting Template

Align front
corner here

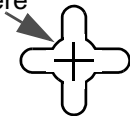


Attach mounting screw here

Considerations for Mounting the SonicWALL TZ 150 Wireless

- Mount in a location away from direct sunlight and sources of heat. A maximum ambient temperature of 104° F (40° C) is recommended.
- Route cables away from power lines, fluorescent lighting fixtures, and sources of noise such as radios, transmitters, and broadband amplifiers
- Ensure that no water or excessive moisture can enter the unit.
- Allow unrestricted airflow around the unit and through the vents on the side of the unit. A minimum of 1 inch (25.44mm) clearance is recommended.

Attach mounting screw here



SonicWALL TZ 150 Wireless Security Appliance Regulatory Statement and Safety Instructions

Regulatory Model/Type	Product Name
APL15-054	TZ 150 Wireless

Note: Detailed regulatory information can be found in the electronic file, “SonicWALL_TZ_150_Wireless_Regulatory_Statement.pdf,” located on the SonicWALL Resource CD provided with the unit or on the SonicWALL Web site: <<http://www.sonicwall.com>>.

Cable Connections

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

Power Supply Information

If you need to order a power supply for your SonicWALL TZ 150 Wireless, please contact SonicWALL Technical Support at 408-752-7819 for a replacement. This product should only be used with a UL listed power supply marked “Class 2” or “LPS”, with an output rated 12 VDC, minimum 1.66 A.

Considerations for Mounting

See the “SonicWALL TZ 150 Wireless Mounting Template” on page 37.

North American Authorized Channels

SonicWALL declares that the APL15-054 (FCC ID: QWU-054) (IC: 4408A-054) when sold in US or Canada is limited to CH1~CH11 by specified firmware controlled in the USA.

Glossary of Networking Terms

- **Default Gateway** - A device on an internetwork that forwards packets to another network.
- **DHCP** - Dynamic Host Configuration Protocol allocates IP addresses to computers on the network automatically without assigning a computer a static (fixed) IP address.
- **DNS** - A Domain Name System is a hierarchical naming system that resolves a domain name with its associated IP address. A DNS server looks up the name of a computer and finds the corresponding IP address. This allows users to access hosts using friendly text-based names instead of IP addresses. These names are called fully qualified domain names (FQDN).
- **IP Address** - An Internet Protocol Address is a thirty-two bit number that identifies a computer or other resource on the Internet or on any TCP/IP network. The number is usually expressed as four numbers from 0 to 255 separated by periods, for example, 172.16.31.254.
- **LAN** - A Local Area Network is typically a group of computers located at a single location, and is commonly based on the Ethernet architecture.
- **NAT** - Network Address Translation is an internet standard that allows your local network to use private IP addresses, which are not recognized on the Internet. The IP address used for the router is the only routable IP address. The computers behind the NAT can access the Internet through the router, but Internet users cannot access the computers behind the router.
- **Packet** - A unit of information transmitted over the internet or within any TCP/IP network. Packets have a header, which contains information about the source, destination, and protocol to be used for the data, and a body, which contains the data being transmitted.
- **PPPoE** - The Point to Point Protocol over Ethernet supports the transmission of network packets over an analog phone line.
- **Private IP Address** - An IP address for a resource in your network that is not known or published outside the zone (for example LAN) where it is located.

- **Public IP Address** - An IP address for a resource in your network that is published outside your network to the WAN.
- **Router** - A device that routes data between networks through IP address information in the header of the IP packet. A router forwards packets to other routers until the packets reach their destination. The Internet is the largest example of a routed network.
- **Subnet** - A portion of a network. Each subnet within a network shares a common network address and is uniquely identified by a subnetwork number.
- **Subnet Mask** - A 32-bit number used to separate the network and host sections of an IP address. A subnet mask subdivides an IP network into smaller pieces. An example of a subnet mask might be 255.255.255.248 for subnet with only eight IP addresses.
- **TCP/IP** - Transmission Control Protocol/Internet Protocol is the basic communication protocol of the Internet. It supports sending information in packets, and identifies each device with a unique numeric IP address.
- **VPN** - A Virtual Private Network is a virtual network that encrypts data and sends it privately over the Internet to protect sensitive information.
- **WAN** - A Wide Area Network is a geographically distributed network composed of multiple networks joined into a single large network. The Internet is a global WAN.

Copyright Notice

© 2007 SonicWALL, Inc.

All rights reserved.

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

Specifications and descriptions subject to change without notice.

Trademarks

SonicWALL is a registered trademark of SonicWALL, Inc.

Microsoft Windows 98, Windows Vista, Windows 2000, Windows XP, Windows Server 2003, Internet Explorer, and Active Directory are trademarks or registered trademarks of Microsoft Corporation.

Netscape is a registered trademark of Netscape Communications Corporation in the U.S. and other countries. Netscape Navigator and Netscape Communicator are also trademarks of Netscape Communications Corporation and may be registered outside the U.S.

Adobe, Acrobat, and Acrobat Reader are either registered trademarks or trademarks of Adobe Systems Incorporated in the U.S. and/or other countries.

Firefox is a trademark of the Mozilla Foundation.

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

Notes

FCC Statement

This equipment has been tested and found to comply with the limits for a class digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does not cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.

- Increase the separation between the equipment and receiver.

- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

- Consult the dealer or an experienced radio/ TV technician for help.

To assure continued compliance, any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

FCC Radiation Exposure Statement

This equipment complies with FCC RF radiation exposure limits set forth set forth in an uncontrolled environment. This equipment should be installed and operated with a minimum distance 20 cm between the radiator and your body.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

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

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

The antennas used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter.

This equipment marketed in USA is restricted by firmware to only operate on 2.4G channel 1-11.

Notes

Canada Statement

Operation is subject to the following two conditions:

- 1) This device may not cause interference and
- 2) This device must accept any interference, including interference that may cause undesired operation of the device.

Europe – EU Declaration of Conformity

This device complies with the essential requirements of the R&TTE Directive 1999/5/EC. The following test methods have been applied in order to prove presumption of conformity with the essential requirements of the R&TTE Directive 1999/5/EC:

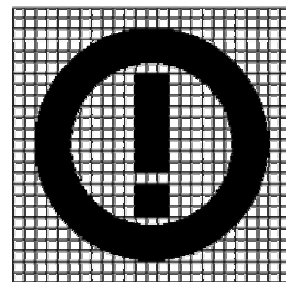
- EN 60950-1: 2001
Safety of Information Technology Equipment
- EN 50392: 2004
Generic standard to demonstrate the compliance of electronic and electrical apparatus with the basic restrictions related to human exposure to electromagnetic fields (0 Hz - 300 GHz)
- EN 300 328 V1.7.1 (2006-10)
Electromagnetic compatibility and Radio spectrum Matters (ERM); Wideband transmission systems; Data transmission equipment operating in the 2,4 GHz ISM band and using wide band modulation techniques; Harmonized EN covering essential requirements under article 3.2 of the R&TTE Directive
- EN 301 489-17 V1.2.1 (2002-08) and EN 301 489-1 V1.5.1 (2004-11)
Electromagnetic compatibility and Radio spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 17: Specific conditions for 2,4 GHz wideband transmission systems and 5 GHz high performance RLAN equipment













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






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

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

CE 0560



 Český [Czech]	<i>Netgear Inc.</i> tímto prohlašuje, že tento <i>Prosafé Wireless ADSL Modem VPN Firewall Router</i> je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/ES.
 Dansk [Danish]	Undertegnede <i>Netgear Inc.</i> erklærer herved, at følgende udstyr <i>Prosafé Wireless ADSL Modem VPN Firewall Router</i> overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
 Deutsch [German]	Hiermit erklärt <i>Netgear Inc.</i> , dass sich das Gerät <i>Prosafé Wireless ADSL Modem VPN Firewall Router</i> in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG befindet.
 Eesti [Estonian]	Käesolevaga kinnitab <i>Netgear Inc.</i> seadme <i>Prosafé Wireless ADSL Modem VPN Firewall Router</i> vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
 English	Hereby, <i>Netgear Inc.</i> , declares that this <i>Prosafé Wireless ADSL Modem VPN Firewall Router</i> is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
 Español [Spanish]	Por medio de la presente <i>Netgear Inc.</i> declara que el <i>Prosafé Wireless ADSL Modem VPN Firewall Router</i> cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.
 Ελληνική [Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ <i>Netgear Inc.</i> ΔΗΛΩΝΕΙ ΟΤΙ <i>Prosafé Wireless ADSL Modem VPN Firewall Router</i> ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ.
 Français [French]	Par la présente <i>Netgear Inc.</i> déclare que l'appareil <i>Prosafé Wireless ADSL Modem VPN Firewall Router</i> est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE.
 Italiano [Italian]	Con la presente <i>Netgear Inc.</i> dichiara che questo <i>Prosafé Wireless ADSL Modem VPN Firewall Router</i> è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
Latviski [Latvian]	Ar šo <i>Netgear Inc.</i> deklarē, ka <i>Prosafé Wireless ADSL Modem VPN Firewall Router</i> atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lietuvių [Lithuanian]	Šiuo <i>Netgear Inc.</i> deklaruoja, kad šis <i>Prosafé Wireless ADSL Modem VPN Firewall Router</i> atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
 Nederlands [Dutch]	Hierbij verklaart <i>Netgear Inc.</i> dat het toestel <i>Prosafé Wireless ADSL Modem VPN Firewall Router</i> in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG.
 Malti [Maltese]	Hawnhekk, <i>Netgear Inc.</i> , jiddikjara li dan <i>Prosafé Wireless ADSL Modem VPN Firewall Router</i> jikkonforma mal-ftiġġiet essenzjali u ma provvedimenti oħrajn rilevanti li hemm fid-Direttiva 1999/5/EC.
 Magyar [Hungarian]	Alulírott, <i>Netgear Inc.</i> nyilatkozom, hogy a <i>Prosafé Wireless ADSL Modem VPN Firewall Router</i> megfelel a vonatkozó alapvető követelményeknek és az 1999/5/EC irányelv egyéb előírásainak.

<p> Polski [Polish]</p>	<p>Niniejszym <i>Netgear Inc.</i> oświadcza, że <i>Prosafe Wireless ADSL Modem VPN Firewall Router</i> jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.</p>
<p> Português [Portuguese]</p>	<p><i>Netgear Inc.</i> declara que este <i>Prosafe Wireless ADSL Modem VPN Firewall Router</i> está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.</p>
<p> Slovensko [Slovenian]</p>	<p><i>Netgear Inc.</i> izjavlja, da je ta <i>Prosafe Wireless ADSL Wireless ModemVPN Firewall Router</i> v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES.</p>
<p>Slovensky [Slovak]</p>	<p><i>Netgear Inc.</i> týmto vyhlasuje, že <i>Prosafe Wireless ADSL Modem VPN Firewall Router</i> spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.</p>
<p> Suomi [Finnish]</p>	<p><i>Netgear Inc.</i> vakuuttaa täten että <i>Prosafe Wireless ADSL Modem VPN Firewall Router</i> tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.</p>
<p> Svenska [Swedish]</p>	<p>Härmed intygar <i>Netgear Inc.</i> att denna <i>Prosafe Wireless ADSL Modem VPN Firewall Router</i> står i överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.</p>