Basic Wireless Configuration and Security

This quick start guide provides basic wireless configuration information for the ProSafe Wireless-N 8-Port Gigabit VPN Firewall FVS318N. For information about more complicated wireless features, and for complete configuration steps, see the *Reference Manual*. This quick start guide contains the following sections:

- *Default Wireless Settings*
- *Wireless Equipment Placement and Range Guidelines*
- *Configure the Country of Operation*
- *Configure WPA+WPA2 with PSK Security*
- *Configure Wi-Fi Protected Setup for Easy Configuration of Wireless Clients*
- *Test Wireless Connectivity*
- *For More Information*

> ***Note:*** For more information about the topics covered in this guide, visit the FVS318N support website at *http://support.netgear.com*. You will also find the *Reference Manual* at the support website.

Default Wireless Settings

The default wireless settings should work well for most wireless networks, but you do need to configure the country of operation and wireless security. These are the default settings:

Table 1. Default wireless settings

Item	Description
Wireless radio	Enabled
Region	Nonconfigurable; set for the region in which you purchased the wireless VPN firewall.

Table 1. Default wireless settings (continued)

Item	Description
Country	The selection is limited to the countries in the region in which you purchased the wireless VPN firewall. The default settings are: • Africa. Algeria • Asia. Azerbaijan • Europe. Albania • Middle East. Bahrain • North America, Latin America, and The Caribbean. United States • Oceania. Australia
Operating frequency	Nonconfigurable: Set at 2.4 GHz
Default security profile	default1
Default network name (SSID)	FVS318N_1
Broadcast SSID	Enabled
Security	Open
Encryption	None
Authentication	None
Transmission rate	Best[1]
Default transmit power	Full
802.11 wireless mode	802.11ng (this is the default for most countries)
802.11b/g/n radio frequency channel	Auto
802.11n channel spacing	20 MHz
Beacon interval	100 ms
DTIM interval	2
RTS threshold	2346 bytes
Fragmentation threshold	2346 bytes
Preamble mode	Long
Protection mode	None
Power save	Disabled

1. The maximum wireless signal rate derived from IEEE Standard 802.11 specifications. The actual throughput varies. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, lower actual data throughput rate.

Wireless Equipment Placement and Range Guidelines

The range of your wireless connection can vary significantly based on the location of the wireless VPN firewall. The latency, data throughput performance, and notebook power consumption of wireless adapters also vary depending on your configuration choices.

> ***Note:*** Failure to follow these guidelines can result in significant performance degradation or inability to wirelessly connect to the wireless VPN firewall. For complete performance specifications, see the Data Sheet at *http://www.netgear.com/images/FVS318N_DS_23Aug1118-36060.pdf*.

For best results, place your wireless VPN firewall according to the following general guidelines:

- Near the center of the area in which your wireless devices will operate.
- In an elevated location such as a high shelf where the wirelessly connected devices have line-of-sight access (even if through walls).
- Away from sources of interference, such as computers, microwaves ovens, and 2.4-GHz cordless phones.
- Away from large metal surfaces or water.
- Placing the antennas in a vertical position provides the best side-to-side coverage. Placing the antennas in a horizontal position provides the best up-and-down coverage.
- If you are using multiple wireless access points such as the wireless VPN firewall, it is better if access points use different radio frequency channels to reduce interference. The recommended channel space between adjacent access points is five channels (for example, use channels 1 and 6, or 6 and 11, or 1 and 11).
- The time it takes to establish a wireless connection can vary depending on both your security settings and placement. WEP connections can take slightly longer to establish. Also, WEP encryption can consume more battery power on a notebook computer.

Configure the Country of Operation

The region of operation is nonconfigurable; it is set for the region in which you purchased the wireless VPN firewall. The selection of the country is limited to the countries in the region in which you purchased the wireless VPN firewall.

➢ **To configure the country settings:**

1. Select **Network Configuration > Wireless Settings > Radio Settings**. The Radio Settings screen displays:

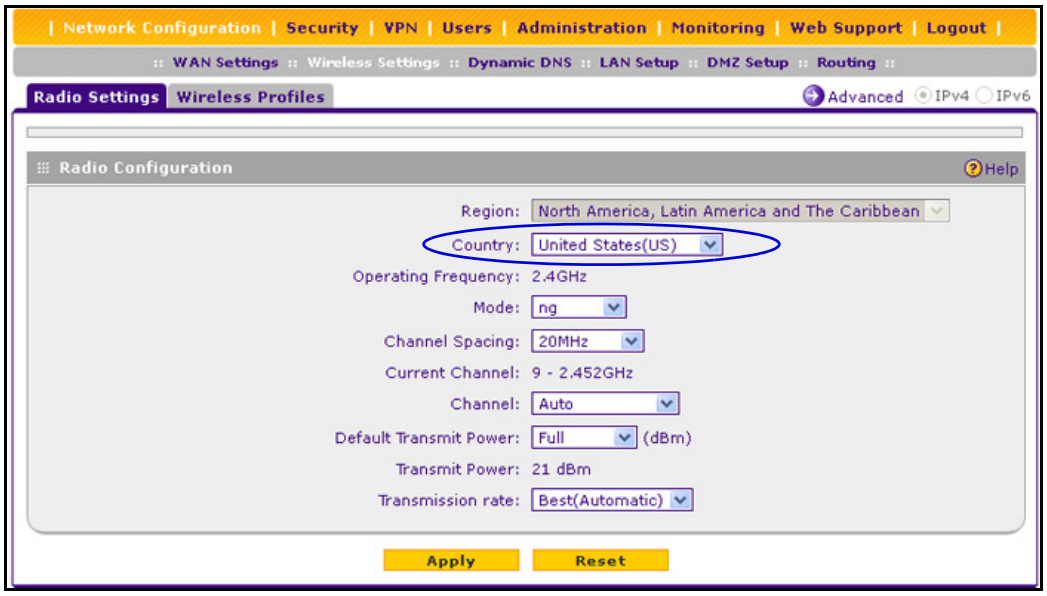

Figure 1.

2. Specify the country by making a selection from the Country drop-down list.
3. Click **Apply** to save your settings. The wireless VPN firewall reboots.

Note: Other wireless settings that you can configure on the Radio Settings screen are explained in the “Configure the Basic Radio Settings” section in Chapter 4, “Wireless Configuration and Security,” of the *Reference Manual*.

Configure WPA+WPA2 with PSK Security

NETGEAR recommends that you configure wireless authentication and encryption to secure your wireless traffic. WPA+WPA2 with a pre-shared key (PSK) is easy to configure and should work well in most situations. However, if your network uses 802.11n devices only, configure WPA2 to enable the 802.11n devices to function at full speed.

➢ **To configure WPA+WPA2 with PSK security for the default1 wireless profile:**

1. Select **Network Configuration > Wireless Settings > Wireless Profiles**. The Wireless Profiles screen displays. (The following figure shows some examples.)

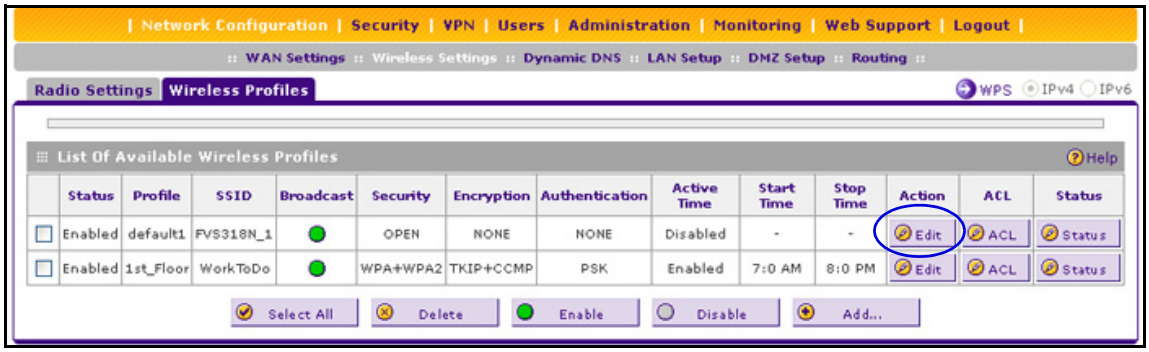

Figure 2.

2. Click the **Edit** button in the Action column for the default1 wireless profile. The Edit Wireless Profiles screen displays (see the figure on the next page).
3. From the Security drop-down list, select **WPA+WPA2**.

   The Encryption drop-down list automatically selects TKIP+CCMP, which is the default encryption setting for WPA+WPA2.
4. From the Authentication drop-down list, select **PSK**.
5. In the WPA Password field, enter a password (also referred to as a pre-shared key) of at least 8 characters long.
6. Click **Apply** to save your settings.

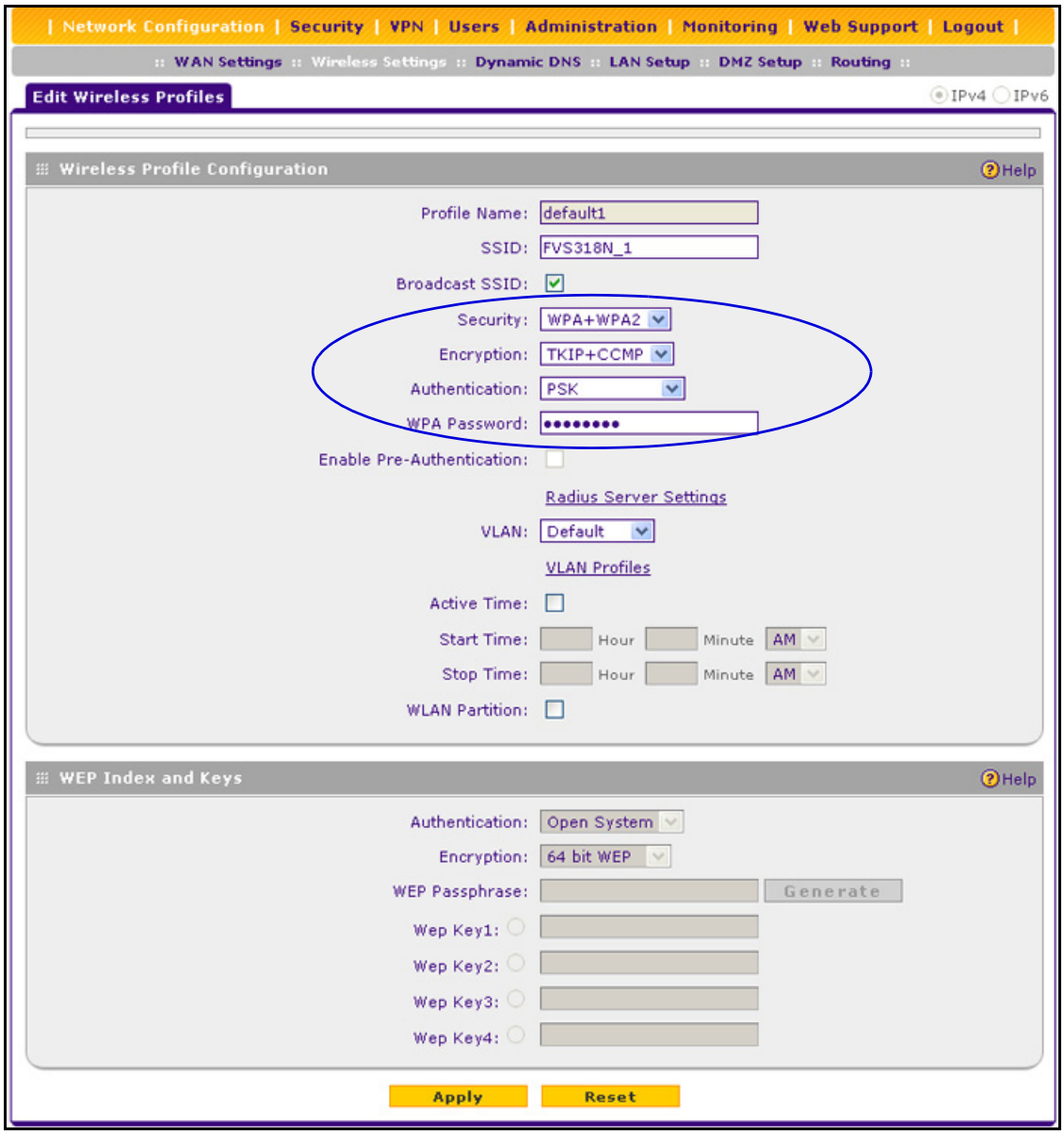

Figure 3.

Note: For other types of security (WEP, WPA, WPA2, RADIUS authentication) and for the other wireless settings that you can configure on the Add Wireless Profiles and Edit Wireless Profiles screens, see the “Configure and Enable Wireless Profiles” section in Chapter 4, “Wireless Configuration and Security,” of the *Reference Manual*.

Configure Wi-Fi Protected Setup for Easy Configuration of Wireless Clients

Push 'N' Connect using Wi-Fi Protected Setup™ (WPS) allows you to connect computers to a secure wireless network with WPA or WPA2 wireless security. The wireless VPN firewall automatically sets security for each computer or device that uses WPS to join the wireless network. To use WPS, make sure that your wireless devices are Wi-Fi certified and support WPS. NETGEAR products that use WPS call it Push 'N' Connect.

You can use a WPS button or the wireless router interface method to add wireless computers and devices to your wireless network. For a list of other Wi-Fi-certified products available from NETGEAR, go to *http://www.wi-fi.org*.

➢ **To enable WPS and initiate the WPS process on the wireless VPN firewall:**

1. Select **Network Configuration > Wireless Settings > Wireless Profiles**. The Wireless Profiles screen displays (see *Figure 2* on page 5).
2. On the Wireless Profiles screen, to the right of the Wireless Profiles tab, click the **WPS** option arrow. The WPS screen displays:

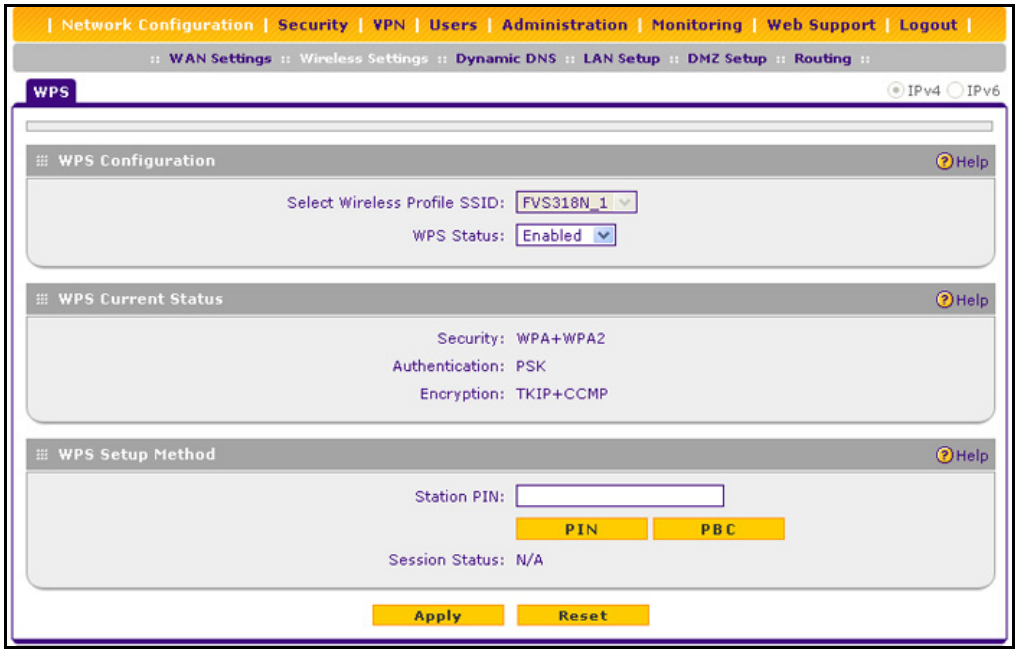

Figure 4.

3. From the Select Wireless Profile SSID drop-down list, select the name of the SSID for which you want to enable WPS, for example, FVS318N_1 (the default SSID). The wireless profile with which the SSID is associated needs to be configured for WPA, WPA, or WPA+WPA2 security in order to be displayed as a selection in the drop-down list.
4. From the WPS Status drop-down list, select **Enabled** to enable the WPS feature.
5. Click **Apply** to save your changes.

Note: The Security, Authentication, and Encryption fields are nonconfigurable fields that are for information only.

6. In the WPS Setup Method section of the screen, use *one* of the following methods to initiate the WPS process for a wireless device:
   - PIN method:
     a. Collect the pin of the wireless device.
     b. In the Station PIN field, enter the pin.
     c. Click the **PIN** button.
   - Push button configuration (PBC) method:
     a. Click the **PBC** button.
     b. Within 2 minutes, press the **WPS** button on your wireless device to enable the device to connect to the wireless VPN firewall, or follow the WPS instructions that came with the device.

   With either method, the wireless VPN firewall tries to communicate with the wireless device, set the wireless security for the wireless device, and allow it to join the wireless network.

Note: There is no physical WPS push button on the wireless VPN firewall.

Test Wireless Connectivity

After you have configured the wireless VPN firewall as explained in the previous sections, test your wireless clients for wireless connectivity before you place the wireless VPN firewall at its permanent position.

➢ **To test for wireless connectivity:**

1. Configure the 802.11g/n wireless clients so that they all have the same SSID that you have configured on the wireless VPN firewall, for example, FVS318N_1 (the default SSID). Make sure that the wireless mode on the wireless VPN firewall supports the wireless capacity of the wireless clients.
2. Verify that your wireless clients have a link to the wireless VPN firewall.
3. Verify network connectivity by using a browser such as Internet Explorer 7.0 or later or Mozilla Firefox 4.0 or later to browse the Internet, or check for file and printer access on your network.

If you have trouble connecting to the wireless VPN firewall, try to connect without security by selecting **OPEN** from the Security drop-down list on the Edit Wireless Profiles screen (see the previous figure) for the profile that you are using.

For More Information

Chapter 4, “Wireless Configuration and Security,” of the *Reference Manual* provides information about the following wireless topics:

- Configuring the basic radio settings
- Wireless data security options
- Wireless security profiles, including information about restricting wireless access by MAC address
- Configuring advanced radio settings