

Chapter 3

Wireless Security Settings

Your wireless data transmissions can be received well beyond your walls by anyone with a compatible adapter. For this reason, use the security features of your wireless equipment. The RangeMax NEXT provides highly effective security features which are covered in detail in this chapter. Deploy the security features appropriate to your needs.

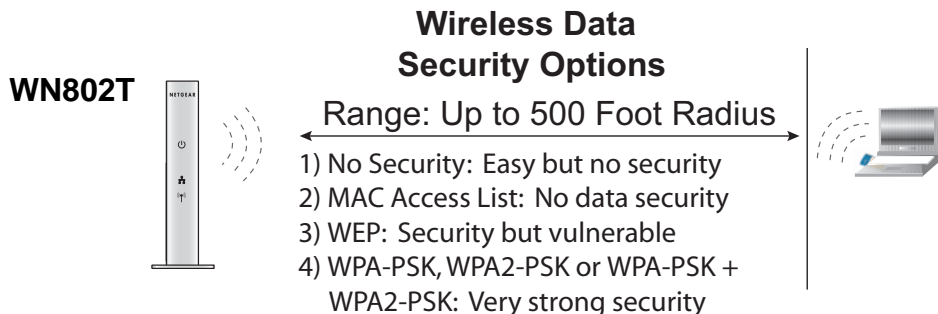


Figure 3-1

Understanding WN802T Wireless Security Options

There are several ways you can enhance the security of your wireless network:

- **Restrict Access Based on MAC address.** You can restrict access to only trusted PCs so that unknown PCs cannot wirelessly connect to the WN802T. MAC address filtering adds an obstacle against unwanted access to your network, but the data broadcast over the wireless link is fully exposed.
- **Turn Off the Broadcast of the Wireless Network Name (SSID).** If you disable broadcast of the SSID, only devices that have the correct SSID can connect. This nullifies the wireless network “discovery” feature of some products such as Windows XP, but the data is still fully exposed to a determined snoop using specialized test equipment like wireless sniffers.
- **Use WEP.** Wired Equivalent Privacy (WEP) data encryption provides data security. WEP Shared Key authentication and WEP data encryption will block all but the most determined eavesdropper.

- **Use WPA-PSK or WPA2-PSK.** Wi-Fi Protected Access (WPA) data encryption provides data security. The very strong authentication along with dynamic per frame rekeying of WPA make it virtually impossible to compromise. Because this is a new standard, wireless device driver and software availability may be limited.

WEP/WPA Settings

The WN802T Access Point is set by default “None” or no authentication. When setting up Network Authentication, bear in mind the following:

Not all wireless adapters support WPA or WPA2. Windows XP and Windows 2000 with Service Pack 3 do include the client software that supports WPA. However, client software is required on the client. Consult the product documentation for your wireless adapter and WPA or WPA2 client software for instructions on configuring WPA2 settings.

- **Network Authentication.** You can configure the RangeMax NEXT to use the types of network authentication shown in the table below.

Table 3-1. Network Authentication Types

Type	Description
None	No data encryption
WEP	Wired Equivalent Privacy using either 64-bit or 128-bit data encryption.
WPA-PSK (TKIP)	Wi-Fi Protected Access with Pre-Shared Key, uses WPA-PSK standard encryption with TKIP encryption type.
WPA2-PSK (AES)	Wi-Fi Protected Access with Pre-Shared Key, uses WPA-PSK standard encryption with AES encryption type. Only select this if all clients support WPA2.
WPA-PSK (TKIP) + WPA2-PSK (AES)	This selection allows clients to use either WPA-PSK (TKIP) or WPA2-PSK (AES).

- **Data Encryption.** The available options depend on the Network Authentication setting selected (see [Table 3-1](#) above); otherwise, the default is None. The Data Encryption settings are explained in the table below:

Table 3-1. Data Encryption Settings

Data Encryption Type	Description
None	No encryption is used.
64 bits WEP	Standard WEP encryption, using 40/64 bit encryption.

Table 3-1. Data Encryption Settings (continued)

Data Encryption Type	Description
128 bits WEP	Standard WEP encryption, using 104/128 bit encryption.
TKIP	Automatic encryption with WPA-PSK; requires passphrase
AES	Automatic encryption with WPA2-PSK; requires passphrase

- **WEP Authentication Type.** WEP can be authenticated using Open System or Automatic. If set to Open System, clients can only associate to the wireless access point by using the Open System option. If set to Automatic, clients can associate to the wireless access point using both Open System and Shared Key. Setting the Authentication Type to Automatic will detect which WEP authentication method is being used. The default is Automatic.
- Use of Passphrases and Keys are explained below:
 - **Passphrase.** To use the Passphrase to generate the WEP keys, enter a passphrase and click the Generate Keys button. You can also enter the keys directly. These keys must match the other wireless stations.
 - **Key 1, Key 2, Key 3, Key 4.** If using WEP, select the key to be used as the default key. Data transmissions are always encrypted using the default key. The other keys can only be used to decrypt received data.
 - **WPA Preshared Key Passphrase.** If using WPA-PSK, WPA2-PSK or WPA-PSK + WPA2-PSK, enter the passphrase here. All wireless stations must use the same passphrase (network key). The network key must be from 8 to 63 characters in length.

SSID and WEP/WPA Settings Setup Form

For a new wireless network, print or copy this form and fill in the configuration parameters. For an existing wireless network, the person who set up or is responsible for the network will be able to provide this information. Be sure to set the Regulatory Domain correctly as the first step.

- **SSID:** The Service Set Identification (SSID) identifies the wireless local area network. **NETGEAR** is the default WN802T SSID. However, you may customize it by using up to 32 alphanumeric characters. Write your customized SSID on the line below.

Note: The SSID in the wireless access point is the SSID you configure in the wireless adapter card. All wireless nodes in the same network must be configured with the same SSID,

- Circle the type of Security Authentication used in your wireless network, and then fill out the appropriate required encryption parameters:

WEP, WPA-PSK, WPA2-PSK, WPA-PSK + WPA2-PSK

- **WEP Encryption Type:**

Circle one: Automatic or Open System

Note: If you selected Open System, the other devices in the network will not connect unless they are set to Open System, and have the same keys in the same positions as those in the WN802T.

- **WEP Encryption Keys:**

Circle one: 64 or 128 bits. (Enter all four keys for the Key Size chosen.)

Key 1: _____

Key 2: _____

Key 3: _____

Key 4: _____

- **WPA Security Encryption for WPA-PSK, WPA2-PSK or WPA-PSK + WPA2-PSK.** Record a **Passphrase** between 8 and 63 characters:

Passphrase: _____

Use the procedures described in the following sections to configure the WN802T. Store this information in a safe place.

Configuring WEP

To configure WEP data encryption:

1. Select **WEP/WPA Settings** under the Security menu on the left navigation pane. The WEP/WPA Settings screen will display.

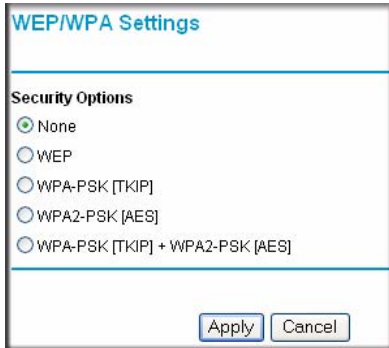


Figure 3-2

2. Check the **WEP** radio button. The WEP Security Encryption options will display. Select the **Authentication Type** from the pull-down menu. The default is Automatic.
3. Selection the Encryption Strength from the pull-down menu; either 64-bit or 128 bit.
4. You can manually or automatically program the four data encryption keys. These values must be identical on all PCs and wireless access points in your network. Choose either:
 - **Automatic** – Enter a word or group of printable characters in the Passphrase box and click the Generate button. The four key boxes will be automatically populated with key values.
 - **Manual** – Enter the number of hexadecimal digits appropriate to the encryption strength: 10 digits for 64-bit and 26 digits for 128-bit (any combination of 0-9, a-f, or A-F) Select which of the four keys will be the default.

The figure shows two screenshots of the WEP/WPA Settings page. The left screenshot shows the 'Security Encryption (WEP)' section with 'Authentication Type' set to 'Automatic' and 'Encryption Strength' set to '64bit'. The 'Security Encryption (WEP) Key' section shows a passphrase of '12345' and four keys, all with radio buttons next to them. The right screenshot shows the same page but with 'Encryption Strength' set to '128bit' and the 'Key 1' radio button selected.

Figure 3-3

5. Select the key to be used as the default key by checking the radio box. (Data transmissions are always encrypted using the default key.)

See the document “Wireless Communications” for a full explanation of each of these options, as defined by the IEEE 802.11 wireless communication standard. A link to this document on the NETGEAR website is in [Appendix B, “Related Documents.”](#)

6. Click **Apply** to save your settings.



Note: If you use a wireless computer to configure WEP settings, you will be disconnected when you click Apply. Reconfigure your wireless adapter to match the new settings or access the wireless access point from a wired computer to make any further changes.

Configuring WPA-PSK, WPA2-PSK and WPA-PSK + WPA2-PSK

Not all wireless adapters support WPA. Furthermore, client software is required on the client. Windows XP and Windows 2000 with Service Pack 3 or above include the client software that supports WPA. Nevertheless, the wireless adapter hardware and driver must also support WPA. Consult the product document for your wireless adapter and WPA client software for instructions on configuring WPA settings.

To configure WPA-PSK, WPA2-PSK or WPA-PSK + WPA2-PSK:

1. Select **WEP/WPA Settings** under the **Security** menu on the left navigation pane. The **WEP/WPA Settings** screen will display.

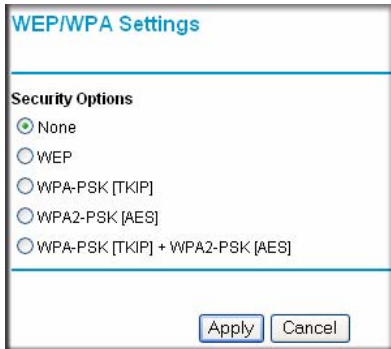
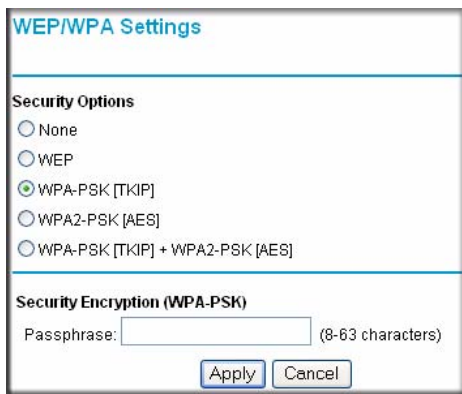


Figure 3-4

2. Select one of the following radio buttons: **WPA-PSK**, **WPA2-PSK** or **WPA-PSK + WPA2-PSK**. The Security encryption Passphrase field will display.



WEP/WPA Settings

Security Options

None

WEP

WPA-PSK [TKIP]

WPA2-PSK [AES]

WPA-PSK [TKIP] + WPA2-PSK [AES]

Security Encryption (WPA-PSK)

Passphrase: (8-63 characters)

Figure 3-5

3. Enter the preshared key **Passphrase** (Network Key).
4. Click **Apply** to save your settings.

Restricting Wireless Access by MAC Address

By default, all wireless PCs that are configured with the correct SSID are allowed access to your wireless network. For increased security, you can restrict access to your wireless network to only those trusted wireless PCs based on their MAC address.

The **Access Control List** screen lets you block the network access privilege of any specified stations to only those displayed in the Trusted **Wireless Stations** table. When you enable the **Turn Access Control On** radio box, the access point will only accept connections from those clients on the Trusted Wireless Stations access control list. This provides an additional layer of security.




Note: If configuring the WN802T from a wireless computer whose MAC address is not in the **Trusted Wireless Stations** access control list, when you select **Turn Access Control On**, you will lose your wireless connection when you click Apply. You must then access the wireless access point from a wired computer or from a wireless computer which is on the access control list to make any further changes.

To restrict access based on MAC addresses:

1. Log in to the WN802T using the default address of **http://192.168.0.233**, user name of **admin** and default password of **password**, or whatever LAN address and password you have set up.
2. Under Security on the main menu, select **Access Control**. The Access Control menu will display.

Figure 3-6

3. Check the **Turn Access Control On** radio button.
4. Click **Apply** to enable the Access Control feature.
5. The **Trusted Wireless Stations** table will display any wireless stations you have entered. If you have not entered any wireless stations this list will be empty.

	Note: If Turn Access Control On is enabled and the Access Control List is blank, then no wireless PCs will be able to connect to your wireless network
---	--

To delete an existing entry:

Check the radio button adjacent to the entry and then click **Delete**.

To set up the trusted wireless stations control list:

1. Click **Add** on the Access Control List screen. The **Wireless Card Access Setup** screen will display. The **Available Wireless Cards** table will display all available wireless PCs and their MAC addresses.

Wireless Card Access Setup

Available Wireless Cards

Device Name	MAC Address
-------------	-------------


Wireless Card Entry

Device Name:

MAC Address:

Figure 3-7

- If the wireless PC you want to add appears in the list, check its adjacent radio button and click **Add**.
 - If the PC is not displayed, make sure that it is configured correctly and click **Refresh**.
 - If no wireless PCs appear in the **Available Wireless Cards** access list, then you can manually enter the **Device Name** and **MAC Address** of the wireless PC in the appropriate fields and then click **Add**. (You can usually find the MAC address printed on the bottom of the wireless adapter.)
- Repeat these steps for each additional device you want to add to the **Trusted Wireless Stations** list.

	Note: The wireless stations must be selected and added one at a time to the Trusted Wireless Stations list.
---	---

- Click **Apply** to save your wireless access control list settings.

Now, only devices on this list will be allowed to wirelessly connect to the WN802T.