Parameter	Defaults	Description
Stateful Packet Inspection	Enabled	This option allows you to select different application types that are using dynamic port numbers. If you wish to use Stateful Packet Inspection (SPI) for blocking packets, click on the Yes radio button in the "Enable SPI and Anti-DoS firewall protection" field and then check the inspection type that you need, such as Packet Fragmentation, TCP Connection, UDP Session, FTP Service and TFTP Service. It is called a "stateful" packet inspection because it examines the contents of the packet to determine the state of the communication; i.e., it ensures that the stated destination computer has previously requested the current communication. This is a way of ensuring that all communications are initiated by the recipient computer and are taking place only with sources that are known and trusted from previous interactions. In addition to being more rigorous in their inspection of packets, stateful inspection firewalls also close off ports until a connection to the specific port is requested. When particular types of traffic are checked, only the particular type of traffic initiated from the internal LAN will be allowed. For example, if the user only checks FTP Service in the Stateful Packet Inspection section, all incoming traffic will be blocked except for FTP connections initiated from the local LAN.
When hackers attempt to enter your network, we can alert you by email		
Your E-mail Address		Enter your email address.
SMTP Server Address		Enter your SMTP server address (usually the part of the email address following the "@" sign).
POP3 Server Address		Enter your POP3 server address (usually the part of the email address following the "@" sign).
User Name		Enter your email account user name.

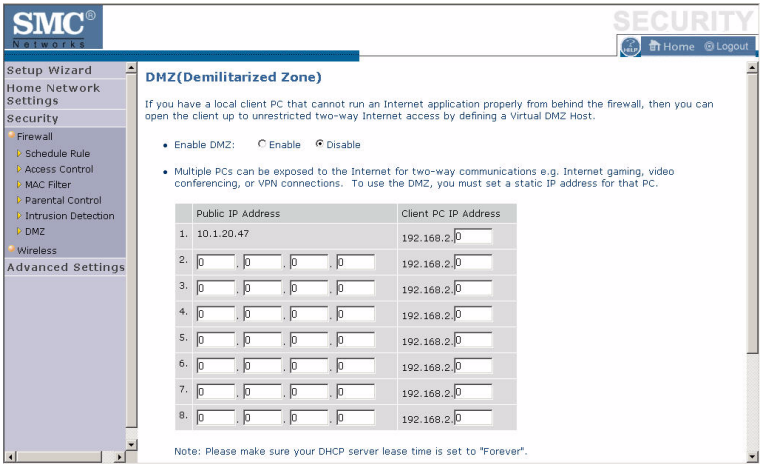
Parameter	Defaults	Description
Password		Enter your email account password.
Connection Policy		
Fragmentation half-open wait	10 secs	Configures the number of seconds that a packet state structure remains active. When the timeout value expires, the router drops the unassembled packet, freeing that structure for use by another packet.
TCP SYN wait	30 secs	Defines how long the software will wait for a TCP session to reach an established state before dropping the session.
TCP FIN wait	5 secs	Specifies how long a TCP session will be managed after the firewall detects a FIN-exchange.
TCP connection idle timeout	3600 secs (1 hour)	The length of time for which a TCP session will be managed if there is no activity.
UDP session idle timeout	30 secs	The length of time for which a UDP session will be managed if there is no activity.
DoS Detect Criteria		
Total incomplete TCP/UDP sessions HIGH	300 sessions	Defines the rate of new unestablished sessions that will cause the software to *start* deleting half-open sessions.
Total incomplete TCP/UDP sessions LOW	250 sessions	Defines the rate of new unestablished sessions that will cause the software to *stop* deleting half-open sessions.
Incomplete TCP/UDP sessions (per min.) HIGH	250 sessions	Maximum number of allowed incomplete TCP/UDP sessions per minute.
Incomplete TCP/UDP sessions (per min.) LOW	200 sessions	Minimum number of allowed incomplete TCP/UDP sessions per minute.
Maximum incomplete TCP/UDP sessions number from same host	10 sessions	Maximum number of incomplete TCP/UDP sessions from the same host.

Parameter	Defaults	Description
Incomplete TCP/UDP sessions detect sensitive time period	300 msecs	Length of time before an incomplete TCP/UDP session is detected as incomplete.
Maximum half-open fragmentation packet number from same host	30 sessions	Maximum number of half-open fragmentation packets from the same host.
Half-open fragmentation detect sensitive time period	1 sec	Length of time before a half-open fragmentation session is detected as half-open.
Flooding cracker block time	300 secs	Length of time from detecting a flood attack to blocking the attack.

Note: We do not recommend modifying the default parameters shown above.

Click **Save Settings** to proceed, or **Cancel** to change your settings.

DMZ

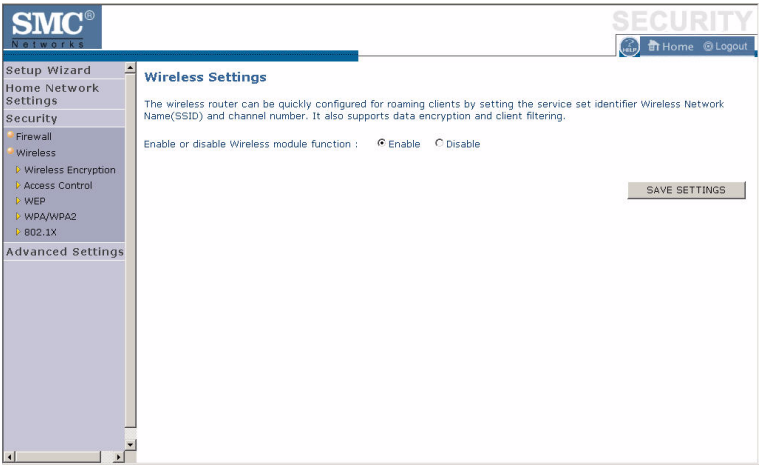


If you have a client PC that cannot run an Internet application properly from behind the firewall, you can open the client up to unrestricted two-way Internet access. Enter the IP address of a DMZ (Demilitarized Zone) host on this screen. Adding a client to the DMZ may expose your local network to a variety of security risks, so only use this option as a last resort.

Wireless

The Barricade can be quickly configured for roaming clients by setting the Service Set Identifier (SSID) and channel number. It supports data encryption and client filtering.

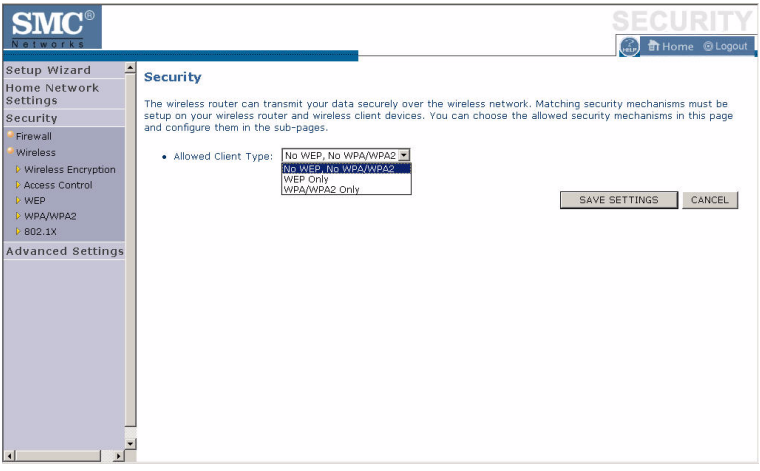
To use the wireless feature, check the **Enable** check box and click **Save Settings**.



To begin configuring your wireless security settings, click **Wireless Encryption**.

Wireless Encryption

The Barricade can transmit your data securely over a wireless network. Matching security mechanisms must be set up on your Barricade and your wireless client devices. Select the most suitable security mechanism from the drop-down list on this screen.

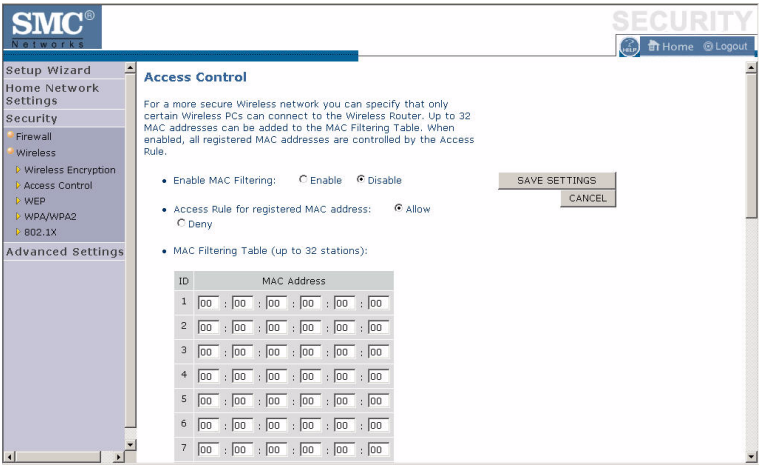


Parameter	Description
No WEP, No WPA/WPA2	Disables all wireless security. To make it easier to set up your wireless network, we recommend enabling this setting initially. By default, wireless security is disabled.
WEP Only	Once you have your wireless network in place, the minimum security we recommend is to enable the legacy security standard, Wired Equivalent Privacy (WEP). See "WEP" on page 4-45.
WPA/WPA2 Only	For maximum wireless security, you should enable the WPA/WPA2 option. See "WPA/WPA2" on page 4-47.

Click **Save Settings** to proceed, or **Cancel** to change your settings.

Access Control

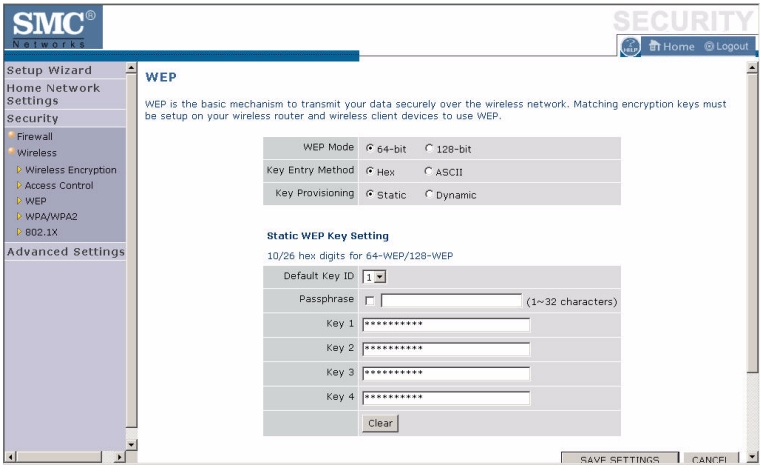
For a more secure wireless network you can specify that only certain wireless clients can connect to the Barricade. Up to 32 MAC addresses can be added to the MAC Filtering Table. When enabled, all registered MAC addresses are controlled by the Access Rule.



By default, this MAC filtering feature is disabled.

WEP

WEP is the basic mechanism to transmit your data securely over a wireless network. Matching encryption keys must be set up on your Barricade and and each of your wireless client devices.



Parameter	Description
WEP Mode	Select 64-bit or 128-bit key to use for encryption.
Key Entry Method	Select hexadecimal (Hex) or ASCII for the key entry method.
Key Provisioning	Select Static if there is only one fixed key for encryption. If you want to select Dynamic, you need to enable 802.1X function first.
Default Key ID	Choose which key to use as default.
Passphrase	Check the Passphrase check box to generate a key automatically.
Key 1~4	The Barricade supports up to 4 keys. You select the default key.

You may automatically generate encryption keys or manually enter the keys. To generate the key automatically with passphrase, check the **Passphrase** box, and enter a string of characters. Select the default key from the drop-down menu. Click **APPLY**.

Note: The passphrase can consist of up to 63 alphanumeric characters.

Hexadecimal Keys

A hexadecimal key is a mixture of numbers and letters from A-F and 0-9. 64-bit keys are 10 digits long and can be divided into five two-digit numbers. 128-bit keys are 26 digits long and can be divided into 13 two-digit numbers.

ASCII Keys

There are 95 printable ASCII characters:

!"#$%&'()*+,-./0123456789:;<=>?

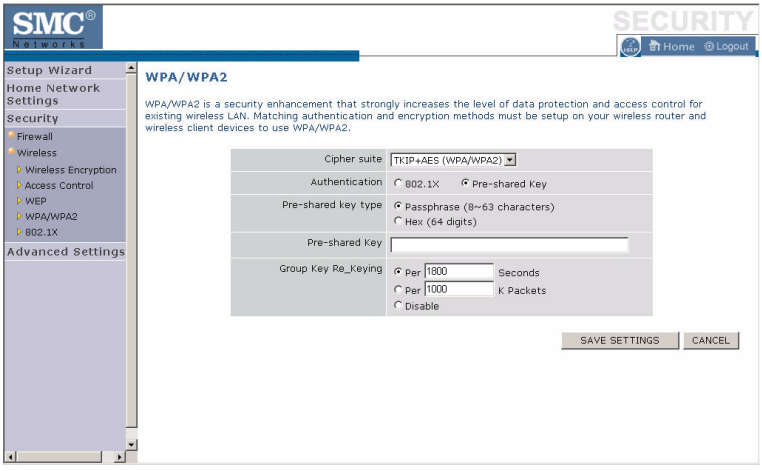
@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_

`abcdefghijklmnopqrstuvwxyz{|}~

Having selected and recorded your key, click **Save Settings** to proceed, or **Cancel** to go back.

WPA/WPA2

WPA/WPA2 is a security enhancement that strongly increases the level of data protection and access control for existing wireless LAN. Matching authentication and encryption methods must be set up on your Barricade and wireless client devices to use WPA/WPA2. To use WPA, your wireless network cards must be equipped with software that supports WPA. A security patch from Microsoft is available for free download (for XP only).



Parameter	Description
Cipher Suite	The security mechanism used in WPA for encryption. Select TKIP+AES (WPA/WPA2) or AES WPA2 Only.
Authentication	Select 802.1X or Pre-shared Key for the authentication method. - 802.1X: for the enterprise network with a RADIUS server. - Pre-shared key: for the SOHO network environment without an authentication server.
Pre-shared key type	Select the key type to be used in the Pre-shared Key.
Pre-shared Key	Type the key here.
Group Key Re_Keying	The period of renewing the broadcast/multicast key.

WPA

WPA addresses all known vulnerabilities in WEP, the original, less secure 40 or 104-bit encryption scheme in the IEEE 802.11 standard. WPA also provides user authentication, since WEP lacks any means of authentication. Designed to secure present and future versions of IEEE 802.11 devices, WPA is a subset of the IEEE 802.11i specification.

WPA replaces WEP with a strong new encryption technology called Temporal Key Integrity Protocol (TKIP) with Message Integrity Check (MIC). It also provides a scheme of mutual authentication using either IEEE 802.1X/Extensible Authentication Protocol (EAP) authentication or pre-shared key (PSK) technology. The passphrase can consist of up to 32 alphanumeric characters.

WPA2

Launched in September 2004 by the Wi-Fi Alliance, WPA2 is the certified interoperable version of the full IEEE 802.11i specification which was ratified in June 2004. Like WPA, WPA2 supports IEEE 802.1X/EAP authentication or PSK technology. It also includes a new advanced encryption mechanism using the Counter-Mode/CBC-MAC Protocol (CCMP) called the Advanced Encryption Standard (AES).

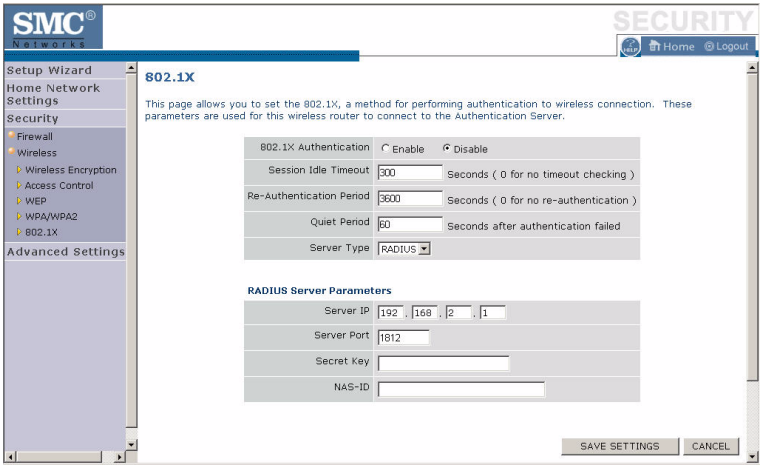
WPA and WPA2 Mode Types

	WPA	**WPA2**
Enterprise Mode	Authentication: IEEE 802.1X/EAP	Authentication: IEEE 802.1X/EAP
	Encryption: TKIP/MIC	Encryption: AES-CCMP
SOHO Mode	Authentication: PSK	Authentication: PSK
	Encryption: TKIP/MIC	Encryption: AES-CCMP

Click **Save Settings** to proceed, or **Cancel** to change your settings.

802.1X

If 802.1X is used in your network, then you should enable this function for the Barricade. This screen allows you to set the 802.1X parameters. 802.1X is a method of authenticating a client wireless connection. Enter the parameters below to connect the Barricade to the Authentication Server.



Parameter	Description
802.1X Authentication	Enable or disable the authentication function.
Session Idle Timeout	This is the time (in seconds) that a session will sit inactive before terminating. Set to 0 if you do not want the session to timeout. (Default: 300 seconds)
Re-Authentication Period	The interval time (in seconds) after which the client will be asked to re-authenticate. For example, if you set this to 30 seconds, the client will have to re-authenticate every 30 seconds. Set to 0 for no re-authentication. (Default: 3600 seconds)
Quiet Period	This is the interval time (in seconds) for which the Barricade will wait between failed authentications. (Default: 60 seconds)
Server Type	Sets the authentication server type.
Server IP	Set the IP address of your RADIUS server.

Parameter	Description
Server Port	Set the connection port that is configured on the radius server.
Secret Key	The 802.1X secret key used to configure the Barricade.
NAS-ID	Defines the request identifier of the Network Access Server.

The use of IEEE 802.1X offers an effective framework for authenticating and controlling user traffic to a protected network, as well as dynamically varying encryption keys. 802.1X ties EAP (Extensible Authentication Protocol) to both the wired and wireless LAN media and supports multiple authentication methods, such as token cards, Kerberos, one-time passwords, certificates, and public key authentication.

Click **Save Settings** to proceed, or **Cancel** to change your settings.

Advanced Settings

To configure the advanced settings such as NAT, Maintenance, System settings and UPnP, click **Advanced Settings**.

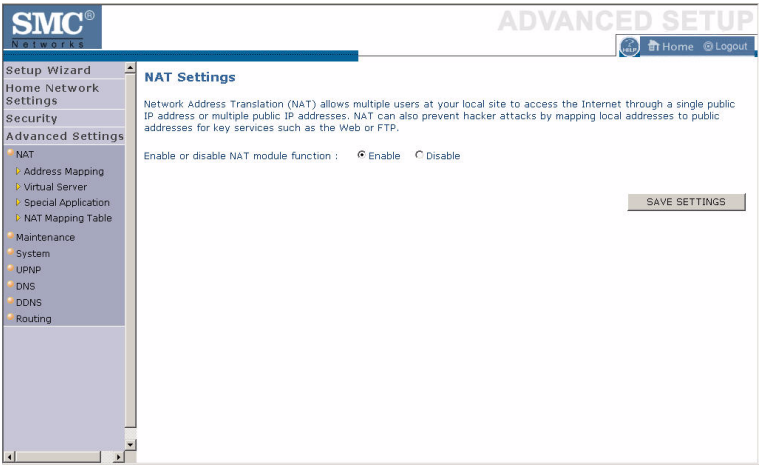
Note: Changing some of the device settings in the Advanced Settings mode may cause the Barricade to become unresponsive.

The Barricade's advanced management interface contains 6 main menu items as described in the following table.

Menu	Description
NAT	Shares a single ISP account with multiple users, sets up virtual servers.
Maintenance	Allows you to backup, restore, reset, and upgrade the Barricade's firmware.
System	Sets the local time zone, the password for administrator access, the IP address of a PC that will be allowed to manage the Barricade remotely, and the IP address of a Syslog Server.
UPnP	Universal Plug and Play (UPnP) allows for simple and robust connectivity between external devices and your PC.
DNS	Sets the IP address of a Domain Name Server.
DDNS	Dynamic DNS provides users on the Internet with a method to tie their domain name to a computer or server.
Routing	Sets routing parameters and displays the current routing table.

NAT

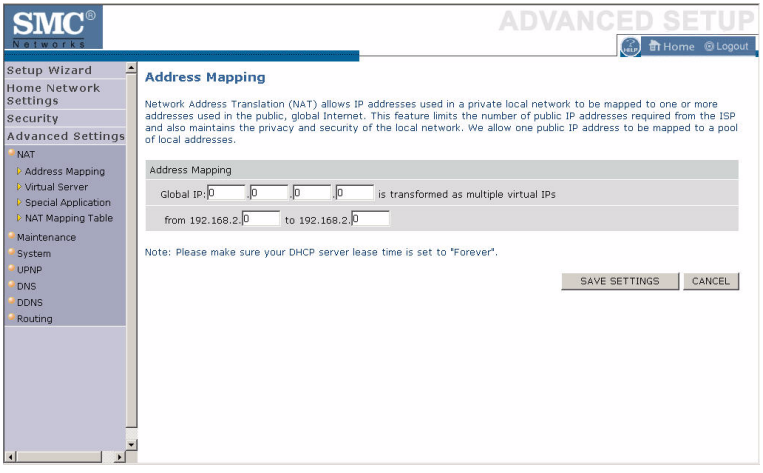
The first menu item in the Advanced Settings section is Network Address Translation (NAT). This process allows all of the computers on your home network to use one IP address. Using the NAT capability of the Barricade, you can access the Internet from any computer on your home network without having to purchase more IP addresses from your ISP.



To use the NAT feature, check the **Enable** radio button and click **Save Settings**.

Address Mapping

Network Address Translation (NAT) allows IP addresses used in a private local network to be mapped to one or more addresses used in the public, global Internet. This feature limits the number of public IP addresses required from the ISP and also maintains the privacy and security of the local network. We allow one public IP address to be mapped to a pool of local addresses.



Click **Save Settings** to proceed, or **Cancel** to change your settings.