

LAN

This page allows you to modify the device's LAN settings.

Wireless-N Pocket AP/Router AP Router Mode

[Status](#) [LAN](#) [DHCP](#) [Schedule](#) [Log](#) [Monitor](#) [Language](#)

You can enable the Broadband routers DHCP server to dynamically allocate IP Addresses to your LAN client PCs. The broadband router must have an IP Address for the Local Area Network.

LAN IP

IP address :

IP Subnet Mask :

802.1d Spanning Tree :

DHCP Server

DHCP Server :

Lease time :

Start IP :

End IP :

Domain name :

DNS Servers

DNS Servers Assigned by DHCP Server _____

LAN IP

IP address :

IP Subnet Mask :

802.1d Spanning Tree : ▼

LAN IP

IP address:	The LAN IP Address of this device.
IP Subnet Mask:	The LAN Subnet Mask of this device.
802.1d Spanning Tree:	When Enabled, the Spanning Tree protocol will prevent network loops in your LAN network.

DHCP Server

DHCP Server :	Enabled ▾
Lease time :	Forever ▾
Start IP :	192.168.0.100
End IP :	192.168.0.200
Domain name :	etr9350

DHCP Server	
DHCP Server:	The DHCP Server automatically allocates IP addresses to your LAN devices.
Lease Time:	The duration of the DHCP server allocates each IP address to a LAN device.
Start / End IP:	The range of IP addresses of the DHCP server will allocate to LAN devices.
Domain name:	The domain name for this LAN network.

DNS Servers

DNS Servers Assigned by DHCP Server

First DNS Server

Second DNS Server

From ISP
User-Defined
DNS Relay
None

Two DNS servers can be assigned for use by your LAN devices.
There are three modes available.

DNS Servers	
From ISP:	The DNS server IP address is assigned from your ISP.
User-Defined:	The DNS server IP address is assigned manually.
DNS Relay:	LAN clients are assigned the device's IP address as the DNS server. DNS requests are relayed to the ISP's DNS server.

DHCP

This page shows the status of the DHCP server and also allows you to control how the IP addresses are allocated.

Wireless-N Pocket AP/Router AP Router Mode

Status LAN DHCP Schedule Log Monitor Language

DHCP Client Table

This DHCP Client Table shows client IP address assigned by the DHCP Server

IP address	MAC address	Expiration Time
192.168.0.100	00:1A:4D:49:1E:3A	Forever
192.168.0.101	00:0C:F6:5C:06:14	Forever

Refresh

You can assign an IP address to the specific MAC address

Enable Static DHCP IP

IP address	MAC address
<input type="text"/>	<input type="text"/>

Add Reset

Current Static DHCP Table :

NO.	IP address	MAC address	Select
-----	------------	-------------	--------

The DHCP Client Table shows the LAN clients that have been allocated an IP address from the DHCP Server

DHCP Client Table

This DHCP Client Table shows client IP address assigned by the DHCP Server

IP address	MAC address	Expiration Time
192.168.0.100	00:1A:4D:49:1E:3A	Forever
192.168.0.101	00:0C:F6:5C:06:14	Forever

Refresh

DHCP Client Table	
IP address:	The LAN IP address of the client.
MAC address:	The MAC address of the client's LAN interface.
Expiration Time:	The time that the allocated IP address will expire.
Refresh:	Click this button to update the DHCP Client Table.

Enable Static DHCP IP

IP address	MAC address
<input type="text" value="192.168.0.155"/>	<input type="text" value="000AF43C1516"/>
<input type="button" value="Add"/>	<input type="button" value="Reset"/>

Current Static DHCP Table :

NO.	IP address	MAC address	Select
1	192.168.0.150	00:0C:C6:3C:06:17	<input type="checkbox"/>

You can also manually specify the IP address that will be allocated to a LAN client by associating the IP address with its MAC address.

Type the IP address you would like to manually assign to a specific MAC address and click **Add** to add the condition to the Static DHCP Table.

Schedule

This page allows you to schedule times that the Firewall and Power Saving features will be activated / deactivated.

Click **Add** to create a Schedule entry.

Wireless-N Pocket AP/Router
AP Router Mode ▾

Status
LAN
DHCP
Schedule
Log
Monitor
Language

You can use the Schedule page to Start/Stop the Services regularly. The Schedule will start to run, when it get GMT Time from Time Server. Please set up the Time Server correctly in Toolbox. The services will start at the time in the following Schedule Table or it will stop.

Enabled Schedule Table (up to 8)

NO.	Description	Service	Schedule	Select
1	schedule 01	Firewall	From 08:00 to 20:00---Mon, Wed, Fri	<input type="checkbox"/>
2	schedule 02	Power Saving	From 21:00 to 23:30---Mon, Tue, Wed, Thu, Fri, Sat, Sun	<input type="checkbox"/>

Add
Edit
Delete Selected
Delete All

Apply
Cancel

Schedule Description :	<input type="text" value="schedule 01"/>
Service :	<input checked="" type="checkbox"/> Firewall <input type="checkbox"/> Power Saving
Days :	<input type="checkbox"/> Every Day <input checked="" type="checkbox"/> Mon <input type="checkbox"/> Tue <input checked="" type="checkbox"/> Wed <input type="checkbox"/> Thu <input checked="" type="checkbox"/> Fri <input type="checkbox"/> Sat <input type="checkbox"/> Sun
Time of day :	<input type="checkbox"/> All Day (use 24-hour clock) From <input type="text" value="8"/> : <input type="text" value="0"/> To <input type="text" value="20"/> : <input type="text" value="0"/>

Schedule	
Schedule Description:	Assign a name to the schedule.
Service:	The service provides for the schedule.
Days:	Define the Days to activate or deactivate the schedule.
Time of day:	Define the Time of day to activate or deactivated the schedule. Please use 24-hour clock format.

Log

This page displays the system log of the device. When powered down or rebooted, the log will be cleared.

Wireless-N Pocket AP/Router
AP Router Mode ▾

Status
LAN
DHCP
Schedule
Log
Monitor
Language

View the system operation information.

```

day 1 02:01:25 [SYSTEM]: WLAN, start LLTD
day 1 02:01:25 [SYSTEM]: WLAN, LLTD Stopping
day 1 02:01:25 [SYSTEM]: UPnP, Stopping
day 1 02:01:24 [SYSTEM]: NET, start Firewall
day 1 02:01:24 [SYSTEM]: NET, start NAT
day 1 02:01:24 [SYSTEM]: NET, stop Firewall
day 1 02:01:24 [SYSTEM]: NET, stop NAT
day 1 02:01:24 [SYSTEM]: SCHEDULE, stop Power Save
day 1 02:01:24 [SYSTEM]: SCHEDULE, Schedule Stopping

```

Log	
Save:	Save the log to a file.
Clear:	Clears the log.
Refresh:	Updates the log.

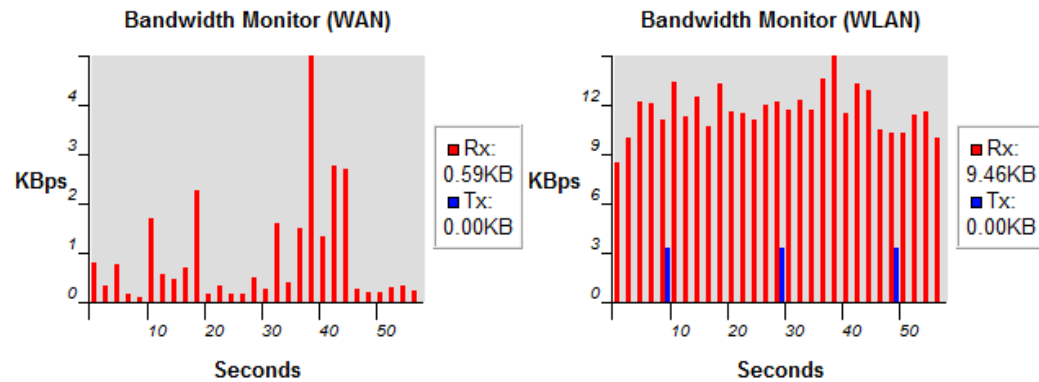
Monitor

This page shows a histogram of the WAN and Wireless LAN traffic. The information is automatically updated every five seconds.

Wireless-N Pocket AP/Router AP Router Mode ▾

[Status](#) | [LAN](#) | [DHCP](#) | [Schedule](#) | [Log](#) | **Monitor** | [Language](#)

You can monitor the bandwidth in different interface. This page will refresh in every five seconds.



Language

This page allows you to change the Language of the User Interface.



You can select other language in this page.

Multiple Language :

- Choose your language
- English
- Traditional Chinese
- Simplified Chinese

8.2.2 Internet

The Internet section allows you to manually set the WAN type connection and its related settings.

Status

This page shows the current status of the device's WAN connection.

Wireless-N Pocket AP/Router AP Router Mode ▾

[Status](#) | [Dynamic IP](#) | [Static IP](#) | [PPPoE](#) | [PPTP](#) | [L2TP](#) | [3G](#)

View the current internet connection status and related information.

WAN Settings

Attain IP Protocol	Dynamic IP Address
IP address	10.0.174.29
Subnet Mask	255.255.254.0
Default Gateway	10.0.175.254
MAC address	00:02:6F:5F:A9:1E
Primary DNS	10.0.200.101
Secondary DNS	10.0.200.102

Dynamic IP Address

The IP Address is allocated automatically. However some ISP's will also recognize the MAC address and will reject connections if the MAC address does not match.

If your ISP has recorded the MAC address of your computer's Ethernet LAN card, please connect only the computer with the authorized MAC address, and click the **Clone MAC Address** button.

This will replace the AP Router MAC address to the computer MAC address. The correct MAC address is used to initiate the connection to the ISP.

Wireless-N Pocket AP/Router AP Router Mode ▾

Status Dynamic IP Static IP PPPoE PPTP L2TP 3G

You can select the type of the account you have with your ISP provider.

Hostname :	<input type="text"/>
MAC address :	<input type="text" value="000000000000"/> <input type="button" value="Clone MAC"/>
DNS Servers	
DNS Servers Type	From ISP ▾
First DNS Server	<input type="text" value="10.0.200.101"/>
Second DNS Server	<input type="text" value="10.0.200.102"/>

Dynamic IP Address	
Hostname:	This is optional. Only required if specified by ISP
MAC address:	The MAC Address that is used to connect to the ISP.
DNS Servers	
Two DNS servers can be assigned for use by your LAN devices. There are two modes available.	
From ISP:	LAN devices are assigned the DNS server IP address of your ISP.
User-Defined:	Set the DNS server IP address manually.

Static IP Address

If your ISP Provider has assigned you a fixed IP address, enter the assigned IP address, Subnet mask, Default Gateway IP address, and Primary DNS and Secondary DNS (if available) of your ISP provider.

Wireless-N Pocket AP/Router AP Router Mode ▾

[Status](#) [Dynamic IP](#) [Static IP](#) [PPPoE](#) [PPTP](#) [L2TP](#) [3G](#)

You can select the type of the account you have with your ISP provider.

IP address:	<input type="text"/>
IP Subnet Mask :	<input type="text"/>
Default Gateway :	<input type="text"/>
Primary DNS :	<input type="text"/>
Secondary DNS :	<input type="text"/>

PPP over Ethernet

ISP requires an account username and password.

Wireless-N Pocket AP/Router		AP Router Mode ▾				
Status	Dynamic IP	Static IP	PPPoE	PPTP	L2TP	3G
You can select the type of the account you have with your ISP provider.						
Login :	<input type="text" value="username"/>					
Password :	<input type="password" value="••••••••"/>					
Service Name	<input type="text" value="ISP"/>					
MTU :	<input type="text" value="1492"/>	(512<=MTU Value <=1492)				
Authentication type :	Auto ▾					
Type :	Keep Connection ▾					
Idle Timeout :	<input type="text" value="10"/>	(1-1000 Minutes)				
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>						

PPP over Ethernet (PPPoE)	
Username:	Username assigned to you by the ISP
Password:	Password for this username.
Service:	You can assign a name for this service. (Optional)
MTU:	The maximum size of packets. Do not change unless mentioned by the ISP.
Authentication type	Select whether the ISP uses PAP or CHAP methods for authentication. Select Auto if unsure.
Type:	You can choose the method that the router maintains connection with the ISP. Keep Connection: The device will maintain a constant connection with the ISP. Automatic Connection: The device will only initiate connection to the ISP when there is an Internet connection request made from a LAN device. Manual Connection: The user will need to manually connect to the ISP by clicking the Connect button.
Idle Timeout:	When the connection type is Automatic Connection , when Internet traffic is idle, then the device will automatically disconnect from the ISP. Please specify the Idle time in minutes.

Point-to-Point Tunneling Protocol (PPTP)

PPTP is used by some ISPs.

Wireless-N Pocket AP/Router
AP Router Mode ▾

Status
Dynamic IP
Static IP
PPPoE
PPTP
L2TP
3G

You can select the type of the account you have with your ISP provider.

WAN Interface Settings :

WAN Interface Type :

Hostname :

MAC address :

PPTP Settings :

Login :

Password :

Service IP address :

Connection ID : (Optional)

MTU : (512<=MTU Value <=1492)

Type :

Idle Timeout : (1-1000 Minutes)

Point-to-Point Tunneling Protocol (PPTP)

WAN Interface Type:	Select whether the ISP is set to Static IP or will allocate Dynamic IP addresses.
Hostname:	This is optional. Only required if specified by ISP

MAC address:	The MAC Address that is used to connect to the ISP.
Login:	Username assigned to you by the ISP
Password:	Password for this username.
Service IP Address:	The IP Address of the PPTP server.
Connection ID:	This is optional. Only required if specified by ISP
MTU:	The maximum size of packets. Do not change unless mentioned by the ISP.
Type:	<p>You can choose the method that the router maintains connection with the ISP.</p> <p>Keep Connection: The device will maintain a constant connection with the ISP.</p> <p>Automatic Connection: The device will only initiate connection to the ISP when there is an Internet connection request made from a LAN device.</p> <p>Manual Connection: The user will need to manually connect to the ISP by clicking the Connect button.</p>
Idle Timeout:	<p>When the connection type is Automatic Connection, when Internet traffic is idle, then the device will automatically disconnect from the ISP.</p> <p>Please specify the Idle time in minutes.</p>

Layer-2 Tunneling Protocol (L2TP)

L2TP is used by some ISPs.

Wireless-N Pocket AP/Router AP Router Mode ▾

[Status](#) [Dynamic IP](#) [Static IP](#) [PPPoE](#) [PPTP](#) [L2TP](#) [3G](#)

You can select the type of the account you have with your ISP provider.

WAN Interface Settings :

WAN Interface Type :

Hostname :

MAC address :

L2TP Settings :

Login :

Password :

Service IP address :

MTU : (512<=MTU Value <=1492)

Type :

Idle Timeout : (1-1000 Minutes)

Layer-2 Tunneling Protocol (L2TP)	
WAN Interface Type:	Select whether the ISP is set to Static IP or will allocate Dynamic IP addresses.
Hostname:	This is optional. Only required if specified by ISP
MAC:	The MAC Address that is used to connect to the ISP.
Login:	Username assigned to you by the ISP
Password:	Password for this username.
Service IP Address:	The IP Address of the PPTP server.
MTU:	The maximum size of packets. Do not change unless mentioned by the ISP.
Type:	<p>You can choose the method that the router maintains connection with the ISP.</p> <p>Keep Connection: The device will maintain a constant connection with the ISP.</p> <p>Automatic Connection: The device will only initiate connection to the ISP when there is an Internet connection request made from a LAN device.</p> <p>Manual Connection: The user will need to manually connect to the ISP by clicking the Connect button.</p>
Idle Timeout:	<p>When the connection type is Automatic Connection, when Internet traffic is idle, then the device will automatically disconnect from the ISP.</p> <p>Please specify the Idle time in minutes.</p>

Mobile 3G

Please ensure your 3G USB card is connected to the TRAVEL ROUTER and has an active USIM card inserted.

Wireless-N Pocket AP/RouterAP Router Mode ▾

StatusDynamic IPStatic IPPPPoEPPTPL2TP**3G**

You can select the type of the account you have with your ISP provider.

Pin Code :	<input style="width: 100%;" type="text"/>
APN Code :	<input style="width: 100%;" type="text"/>
Dial Number :	<input style="width: 100%;" type="text"/>
Username :	<input style="width: 100%;" type="text"/>
Password :	<input style="width: 100%;" type="text"/>
Type :	Keep Connection ▾
Idle Timeout :	<input style="width: 50px;" type="text" value="10"/> (1-1000 Minutes)

Mobile 3G	
Pin Code:	Enter the Pin code for your USIM card if required.
APN Code:	Enter the APN code for the network provider
Dial Number:	Only required if specified by ISP
User Name:	Account Username. Only required if specified by ISP
Password:	Account Password. Only required if specified by ISP
Type:	<p>You can choose the method that the router maintains connection with the ISP.</p> <p>Keep Connection: The device will maintain a constant connection with the ISP.</p> <p>Automatic Connection: The device will only initiate connection to the ISP when there is an Internet connection request made from a LAN device.</p> <p>Manual Connection: The user will need to manually connect to the ISP by clicking the Connect button.</p>
Idle Timeout:	<p>When the connection type is Automatic Connection, when Internet traffic is idle, then the device will automatically disconnect from the ISP.</p> <p>Please specify the Idle time in minutes.</p>

8.2.3 Wireless

The Wireless section allows you to configure the Wireless settings.

Status

This page shows the current status of the device's Wireless settings.

Wireless-N Pocket AP/Router AP Router Mode ▾

[Basic](#) | [Advanced](#) | [Security](#) | [Filter](#) | [WPS](#) | [Client List](#) | [Policy](#)

This page allows you to define SSID, and Channel for the wireless connection. These parameters are used for the wireless stations to connect to the Access Point.

Radio :	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Mode :	AP ▾
Band :	2.4 GHz (B+G+N) ▾
Enable SSID#:	2 ▾
SSID1 :	EnGenius5FA6E8
SSID2 :	EnGenius5FA6E8_2
Auto Channel :	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Channel :	11 ▾

Basic	
Radio:	Enable or Disable the device's wireless signal.
Mode:	Select between Access Point or Wireless Distribution System (WDS) modes.
Band:	Select the types of wireless clients that the device will accept. eg: 2.4 Ghz (B+G) Only 802.11b and 11g clients will be allowed.
Enable SSID#:	Select the number of SSID's (Wireless Network names) you would like. You can create up to 4 separate wireless networks.
SSID#	Enter the name of your wireless network. You can use up to 32 characters.
Auto Channel:	When enabled, the device will scan the wireless signals around your area and select the channel with the least interference.
Channel:	Manually select which channel the wireless signal will use.
Check Channel Time:	When Auto Channel is Enabled, you can specify the period of the device will scan the wireless signals around your area.

Wireless Distribution System (WDS)

Using WDS to connect Access Point wirelessly, and in doing so extend a wired infrastructure to locations where cabling is not possible or inefficient to implement.

Note that compatibility between different brands and models is not guaranteed. It is recommended that the WDS network be created using the same models for maximum compatibility.

Also note that all Access Points in the WDS network needs to use the same Channel and Security settings.

To create a WDS network, please enter the MAC addresses of the Access Points that you want included in the WDS. There can be a maximum of four access points.

Radio :	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Mode :	WDS ▾
Band :	2.4 GHz (B+G+N) ▾
Enable SSID#:	2 ▾
SSID1 :	EnGenius5FA6E8
SSID2 :	EnGenius5FA6E8_2
Channel :	11 ▾
MAC address 1 :	000000000000
MAC address 2 :	000000000000
MAC address 3 :	000000000000
MAC address 4 :	000000000000
WDS Data Rate :	300M ▾
Set Security :	Set Security

Advanced

This page allows you to configure wireless advance settings. It is recommended the default settings are used unless the user has experience with these functions.

Wireless-N Pocket AP/Router AP Router Mode ▾

Basic **Advanced** Security Filter WPS Client List Policy

These settings are only for more technically advanced users who have a sufficient knowledge about wireless LAN. These settings should not be changed unless you know what effect the changes will have on your Broadband router.

Fragment Threshold :	<input type="text" value="2346"/>	(256-2346)
RTS Threshold :	<input type="text" value="2347"/>	(1-2347)
Beacon Interval :	<input type="text" value="100"/>	(20-1024 ms)
DTIM Period :	<input type="text" value="1"/>	(1-255)
N Data rate :	<input type="text" value="Auto"/>	
Channel Bandwidth :	<input checked="" type="radio"/> Auto 20/40 MHZ <input type="radio"/> 20 MHZ	
Preamble Type :	<input type="radio"/> Long Preamble <input checked="" type="radio"/> Short Preamble	
CTS Protection :	<input checked="" type="radio"/> Auto <input type="radio"/> Always <input type="radio"/> None	
Tx Power :	<input type="text" value="100 %"/>	

Advanced	
Fragment Threshold:	<p>Specifies the size of the packet per fragment. This function can reduce the chance of packet collision.</p> <p>However when this value is set too low, there will be increased overheads resulting in poor performance.</p>
RTS Threshold:	<p>When the packet size is smaller than the RTS Threshold, then the packet will be sent without RTS/CTS handshake which may result in incorrect transmission.</p>
Beacon Interval:	<p>The time interval that the device broadcasts a beacon. This beacon is used to synchronize all wireless clients on the network.</p>
DTIM Period:	<p>A Delivery Traffic Indication Message informs all wireless clients that the access point will be sending Multi-casted data.</p>
N Data Rate:	<p>You can limit the transfer rates between the device and wireless clients. Each Modulation Coding Scheme (MCS) refers to a specific transfer speed.</p>
Channel Bandwidth:	<p>Set whether each channel uses 20 or 40Mhz. To achieve 11n speeds, 40Mhz channels must be used.</p>
Preamble Type:	<p>A preamble is a message that helps access points synchronize with the client.</p> <p>Long Preamble is standard based so increases compatibility. Short Preamble is non-standard, so it decreases compatibility but increases performance.</p>
CTS Protection:	<p>When Enabled, the performance is slightly lower however the chances of packet collision is greatly reduced.</p>
Tx Power:	<p>Set the power output of the wireless signal.</p>

Security

This page allows you to set the wireless security settings.

Wireless-N Pocket AP/Router

AP Router Mode ▾

Basic Advanced **Security** Filter WPS Client List Policy

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

SSID Selection :	EnGenius5FA6E8 ▾
Broadcast SSID :	Enable ▾
WMM :	Enable ▾
Encryption :	Disable ▾

Enable 802.1x Authentication

Apply Cancel

Security	
SSID Selection:	Select the SSID that the security settings will apply to.
Broadcast SSID:	If Disabled, then the device will not be broadcasting the SSID. Therefore it will be invisible to wireless clients.
WMM:	WiFi Multi-Media is a Quality of Service protocol which prioritizes traffic in the order according to voice, video, best effort, background. Note that in certain situations, WMM needs to be enabled to achieve 11n transfer speeds.
Encryption:	<p>The encryption method to be applied. You can choose from WEP, WPA pre-shared key or WPA RADIUS.</p> <ul style="list-style-type: none"> • Disabled - no data encryption is used. • WEP - data is encrypted using the WEP standard. • WPA-PSK - data is encrypted using the WPA-PSK standard. This is a later standard than WEP, and provides much better security than WEP. If all your Wireless stations support WPA-PSK, you should use WPA-PSK rather than WEP. • WPA2-PSK - This is a further development of WPA-PSK, and offers even greater security, using the AES (Advanced Encryption Standard) method of encryption. • WPA-RADIUS - This version of WPA requires a Radius Server on your LAN to provide the client authentication according to the 802.1x standard. Data transmissions are encrypted using the WPA standard. <p>If this option is selected:</p> <ul style="list-style-type: none"> • This Access Point must have a "client login" on the Radius Server. • Each user must have a "user login" on the Radius Server. • Each user's wireless client must support 802.1x and provide the login data when required. • All data transmission is encrypted using the WPA standard. Keys are automatically generated, so no key input is required.

IEEE 802.1x is an authentication protocol. Every user must use a valid account to login to this Access Point before accessing the wireless LAN. The authentication is processed by a RADIUS server. This mode only authenticates users by IEEE 802.1x, but it does not encrypt the data during communication.

Enable 802.1x Authentication

RADIUS Server IP address :	<input type="text"/>
RADIUS Server port :	<input type="text" value="1812"/>
RADIUS Server password :	<input type="text"/>

802.1x Authentication

RADIUS Server IP Address:	The IP Address of the RADIUS Server
RADIUS Server port:	The port of the RADIUS Server.
RADIUS Server password:	The RADIUS Server's password.

WEP Encryption:

WEP Encryption	
Authentication Type:	Please ensure that your wireless clients use the same authentication type.
Key Length:	<p>Select the desired option, and ensure the wireless clients use the same setting.</p> <ul style="list-style-type: none"> • 64 Bit - data is encrypted, using the default key, before being transmitted. You must enter at least the default key. For 64 Bit Encryption, the key size is 10 chars in HEX (0~9 and A~F). • 128 Bit - data is encrypted, using the default key, before being transmitted. You must enter at least the default key. For 128 Bit Encryption, the key size is 26 chars in HEX (0~9 and A~F).
Default Key:	Select the key you wish to be the default. Transmitted data is ALWAYS encrypted using the Default Key; the other Keys are for decryption only. You must enter a Key Value for the Default Key .
Encryption Key #:	Enter the key value or values you wish to use. Only the Key selected as Default is required. The others are optional.

Encryption :	WEP ▾
Authentication type :	<input checked="" type="radio"/> Open System <input type="radio"/> Shared Key <input type="radio"/> Auto
Key Length :	128-bit ▾
Key type :	ASCII (13 characters) ▾
Default key :	Key 1 ▾
Encryption Key 1 :	1234567890123
Encryption Key 2 :	*****
Encryption Key 3 :	*****
Encryption Key 4 :	*****

WPA Pre-Shared Key Encryption:

Encryption :	WPA pre-shared key ▾
WPA type :	<input checked="" type="radio"/> WPA(TKIP) <input type="radio"/> WPA2(AES) <input type="radio"/> WPA2 Mixed
Pre-shared Key type :	Passphrase ▾
Pre-shared Key :	1234567890

WPA Pre-Shared Key Encryption	
Authentication Type:	Please ensure that your wireless clients use the same authentication type.
WPA type:	Select the WPA encryption you would like. Please ensure that your wireless clients use the same settings.
Pre-shared Key Type:	Select whether you would like to enter the Key in HEX or Passphrase format.
Pre-shared Key:	Wireless clients must use the same key to associate the device. If using passphrase format, the Key must be from 8 to 63 characters in length.

WPA RADIUS Encryption:

Encryption :	WPA RADIUS ▾
WPA type :	<input checked="" type="radio"/> WPA(TKIP) <input type="radio"/> WPA2(AES) <input type="radio"/> WPA2 Mixed
RADIUS Server IP address :	<input type="text"/>
RADIUS Server port :	1812
RADIUS Server password :	<input type="text"/>

WPA RADIUS Encryption	
WPA type:	Select the WPA encryption you would like. Please ensure that your wireless clients use the same settings.
RADIUS Server IP address:	Enter the IP address of the RADIUS Server
RADIUS Server Port:	Enter the port number used for connections to the RADIUS server.
RADIUS Server password:	Enter the password required to connect to the RADIUS server.

Filter

This page allows you to create filters to control which wireless clients can connect to this device by only allowing the MAC addresses entered into the Filtering Table.

Wireless-N Pocket AP/Router
AP Router Mode ▾

Basic
Advanced
Security
Filter
WPS
Client List
Policy

For security reason, the Access Point features MAC Address Filtering which only allows authorized MAC Addresses to associate with the Access Point.

Enable Wireless Access Control

Description	MAC address
Notebook2	00ABC710722

MAC Address Filtering Table :

NO.	Description	MAC address	Select
1	Notebook1	00:0C:C6:3C:06:17	<input type="checkbox"/>

Wireless Filter	
Enable Wireless Access Control:	<p>Tick the box to Enable Wireless Access Control.</p> <p>When Enabled, only wireless clients on the Filtering Table will be allowed.</p>
Description:	Enter a name or description for this entry.
MAC address:	Enter the MAC address of the wireless client that you wish to allow connection.
Add:	Click this button to add the entry.
Reset:	Click this button if you have made a mistake and want to reset the MAC address and Description fields.
MAC Address Filtering Table	
Only clients listed in this table will be allowed access to the wireless network.	
Delete Selected:	Delete the selected entries.
Delete All:	Delete all entries
Reset:	Un-tick all selected entries.

Wi-Fi Protected Setup (WPS)

WPS feature is following the Wi-Fi Alliance WPS standard and it eases the set up of security-enabled Wi-Fi networks in the home and small office environment.

It reduces the user steps required to configure a network and supports two methods that are familiar to most consumers to configure a network and enable security.

Wireless-N Pocket AP/Router AP Router Mode

[Basic](#) [Advanced](#) [Security](#) [Filter](#) [WPS](#) [Client List](#) [Policy](#)

WPS : Enable

WPS Button : Enable

Wi-Fi Protected Setup Information

WPS Current Status : Configured Release Configuration

Self Pin Code : 62686488

SSID : 123

Authentication Mode : WPA2 pre-shared key

Passphrase Key :

WPS Via Push Button : Start to Process

WPS via PIN : Start to Process

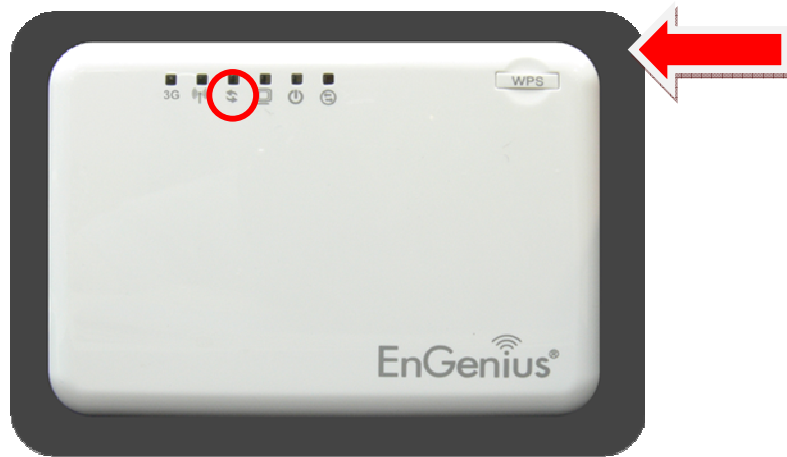
Wi-Fi Protected Setup (WPS)	
WPS:	Tick to Enable the WPS feature.
WPS Button:	Tick to Enable the WPS push button.
Wi-Fi Protected Setup Information	
WPS Current Status:	Shows whether the WPS function is Configured or Unconfigured . Configured means that WPS has been used to authorize connection between the device and wireless clients.
SSID:	The SSID (wireless network name) used when connecting using WPS.
Authentication Mode:	Shows the encryption method used by the WPS process.
Passphrase Key:	This is the passphrase key that is randomly generated during the WPS process. It is required if wireless clients that do not support WPS attempts to connect to the wireless network.
WPS Via Push Button:	Click this button to initialize WPS feature using the push button method.

Initializing WPS Feature

There are two methods to initialize the WPS feature. They are the Push Button and Pin code methods.

1. WPS Push Button Method

Push the WPS button on the TRAVEL ROUTER device. The WPS LED light will start to flash to indicate that the WPS process is ready.



While the WPS LED is flashing on the TRAVEL ROUTER, press the WPS button on your wireless client. This could either be a physical hardware button, or a software button in the utility.

