USER GUIDE

Dual band Access Point
802.11a/b/g

legrand®
www.legrand.fr

Contents

Introduction

The Access Point's Back Panel

The Access Point's port (where an uplink network cable is connected) is located on the Access Point's back panel, the power is supplied by power over Ethernet (802.3af standard).

The Access Point's Front Panel

User port: This **LAN** (Local Area Network 100 base T) port allows to connect other Ethernet network devices, such as a computer, a hub, switch, router, printer, etc.

Reset Button: This button has two uses:
Short press will reboot the AP
Long press (more than 5 seconds) will reset the AP to its factory defaults (blue Leds will flash)

Green Power LED: The Power LED lights up when the Access Point is powered on.

Blue Radio LEDs: The radio LED light up when the radio is active.

1.1 / HOW TO ACCESS THE WEB-BASED INTERFACE

1. You have a computer running Windows XP

Check if the UPnP protocol is activated on your computer. Otherwise follow this procedure:

- Click on the Start Menu->Settings->Control Panel
- Click “Add or Remove Programs” in Control Panel.
- Click “Add/Remove Windows Components”.
- In the Components list, select the Networking Services entry, and then click Details.
- Make sure the Universal Plug and Play check box is selected. And click on OK, then Next until the installation is complete.

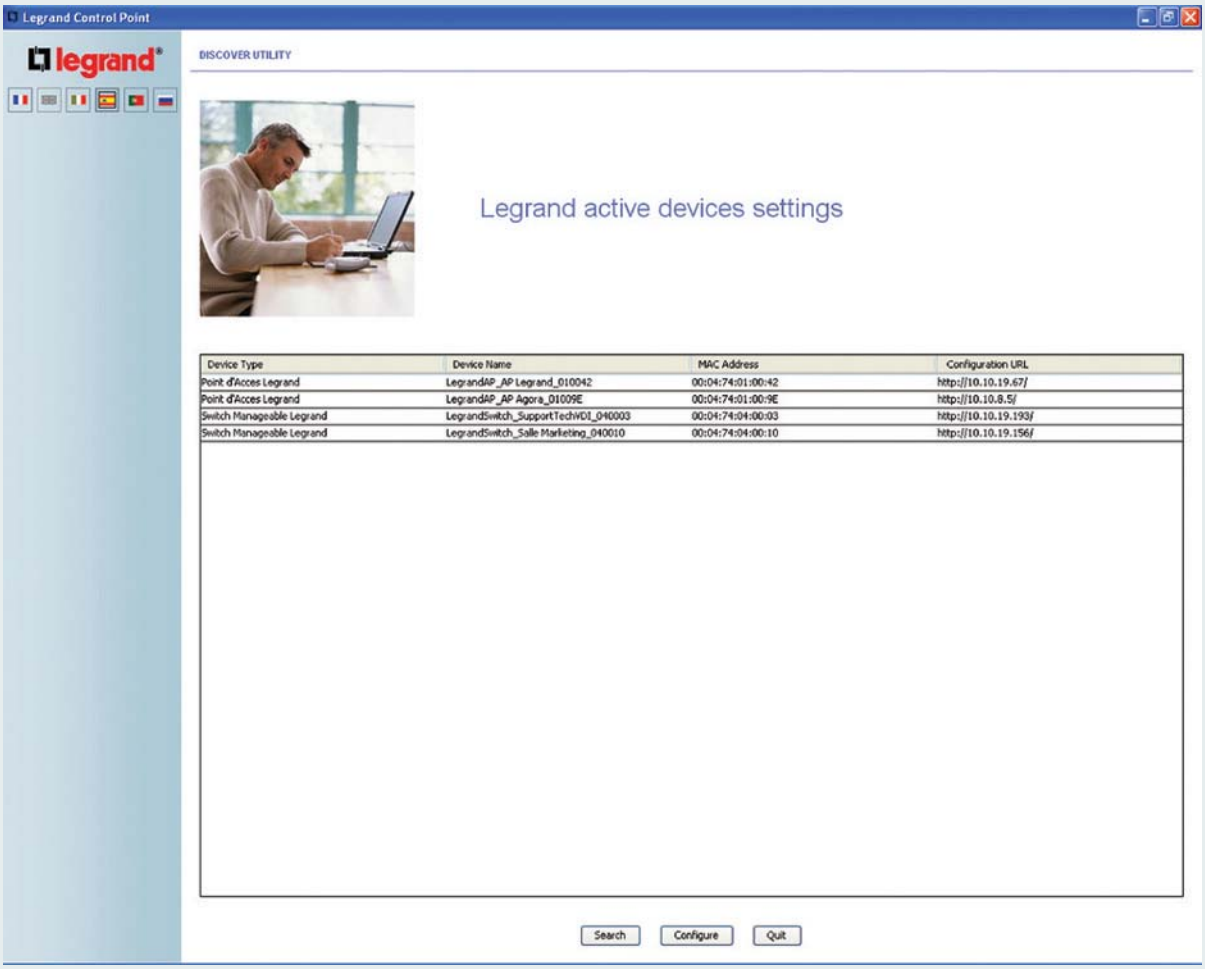
UPnP is now activated on your computer, when clicking on the Network Neighbourhood icon on your desktop, a window will display the Legrand Access Points discovered using UPnP.

Double click on one Access point to access the web configuration interface.

2. You have a computer running a different Windows version, MAC, Linux, Unix or other

Use the CD ROM to launch the *Legrand Control point* discovery utility.
Insert **THE CD-ROM SUPPLIED WITH THE ACCESS POINT**. This CD provides the tools needed to configure your wireless network.

The main menu will be displayed automatically on your screen. If the main menu does not appear automatically, browse the contents of the CD-ROM and doubleclick on the file “setup.exe”.



The list will show you all the Legrand Access Points in your installation.

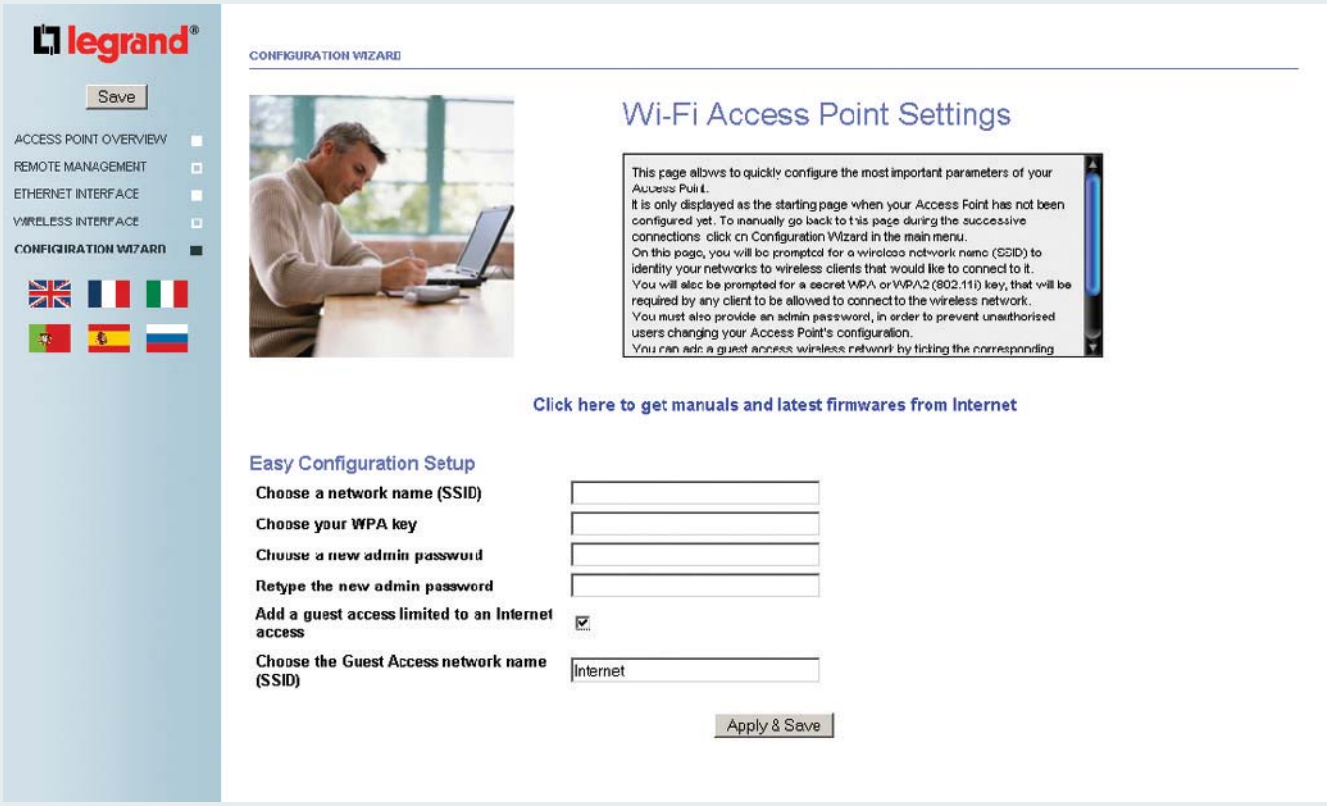
Select one Access Point and click on connect to access the web configuration interface.

1.2 / CONFIGURATION PASSWORD INPUT

On the first connection to the management web interfaces, or after a full reset, no password will be prompted to configure the Access Point; it is highly recommended to protect your Legrand Access Point using a password, in which case access to the management web interfaces will be subject to prior authentication. The Login will then be “**admin**”, and the password will have to match with the one previously configured.

Caution
Depending on your webbrowser, a “Remember my password” dialog box may be presented to you when the management web interfaces are password-protected. Enabling this option means your browser will fill in the password automatically for you for all subsequent connections to the management web interfaces.
Do not check the option **Remember my password** if other people have access to your PC, or they could modify the Access Point configuration without having to provide the configuration password.

1.3 / CONFIGURATION WIZARD



This page offers a quick access to the main security features of your Access Point.

First enter the **network name (SSID)** of your choice.
In the field choose **your WPA Key** select a wireless key (at least 8 characters long), this will have to be entered on all wireless devices to connect to the wireless network.
In the field **choose a new admin password** enter the password of your choice.
This password will be required to modify the configuration of your Access Point.
Click on **Apply & Save** to update and save this configuration.

By using this quick setup page, your Access Point is configured with the **Static WPA or WPA2** encryption method (using the key provided).

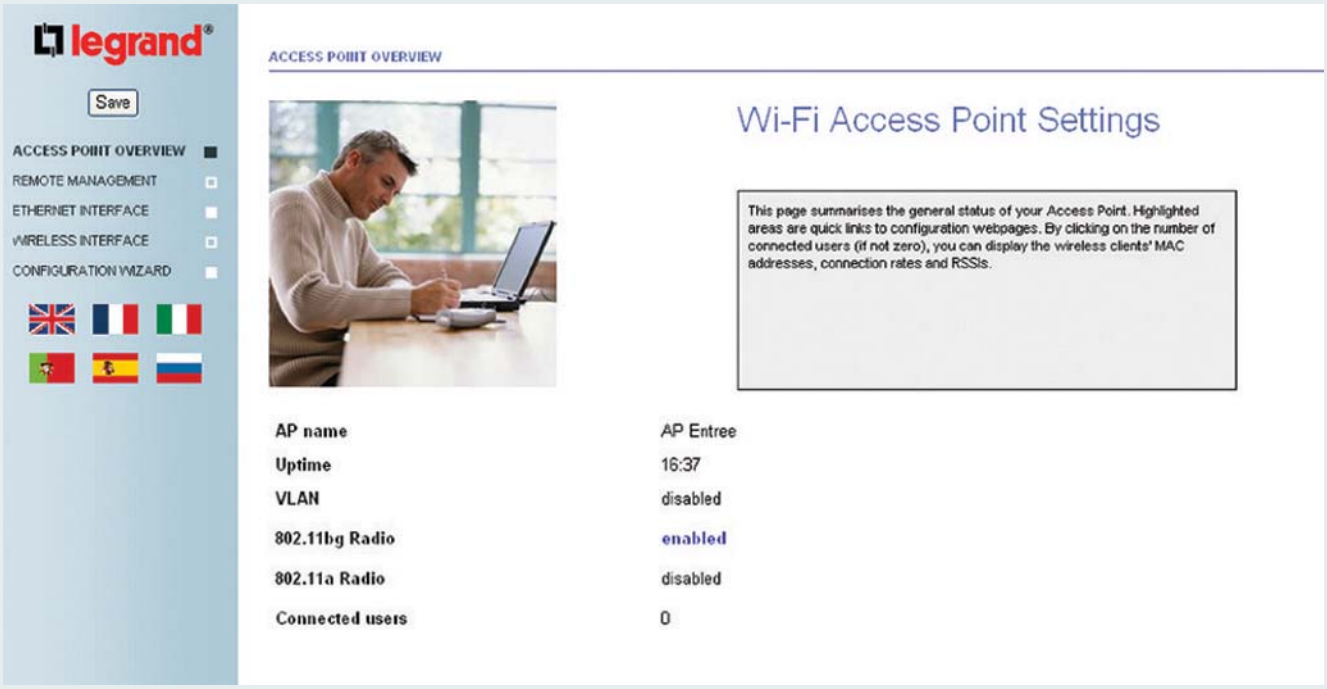
When you tick **Add a guest access limited to an Internet access**, you can define a nonsecure wireless network but this network will only enable access to the Internet.

Use the **Choose the Guest Access network name (SSID)** field to give a name to your limited-access network.

When your configuration is done, the connection between your computer and the Access Point will be interrupted.
In order to restore your computer's wireless connectivity, you will need to apply the same encryption and key to your PC's wireless connection settings.

At this stage your AP is secured and ready to use, if you need to modify advanced parameters use the left menu of the web interface.

1.4 / ACCESS POINT OVERVIEW



The screen provides an overview of the Legrand AP main information.

AP Name	This name will identify your Access Point (i.e. it is shown in the discovery utility)
Uptime	Shows how long the Legrand AP has been running since its last reboot/power on
VLAN	Status of VLAN trunking Enabled/Disabled
802.11bg Radio	Status of the 2.4GHz band radio Enabled/Disabled
802.11a Radio*	Status of the 5GHz band radio Enabled/Disabled
Connected Users	List of currently connected Wireless clients

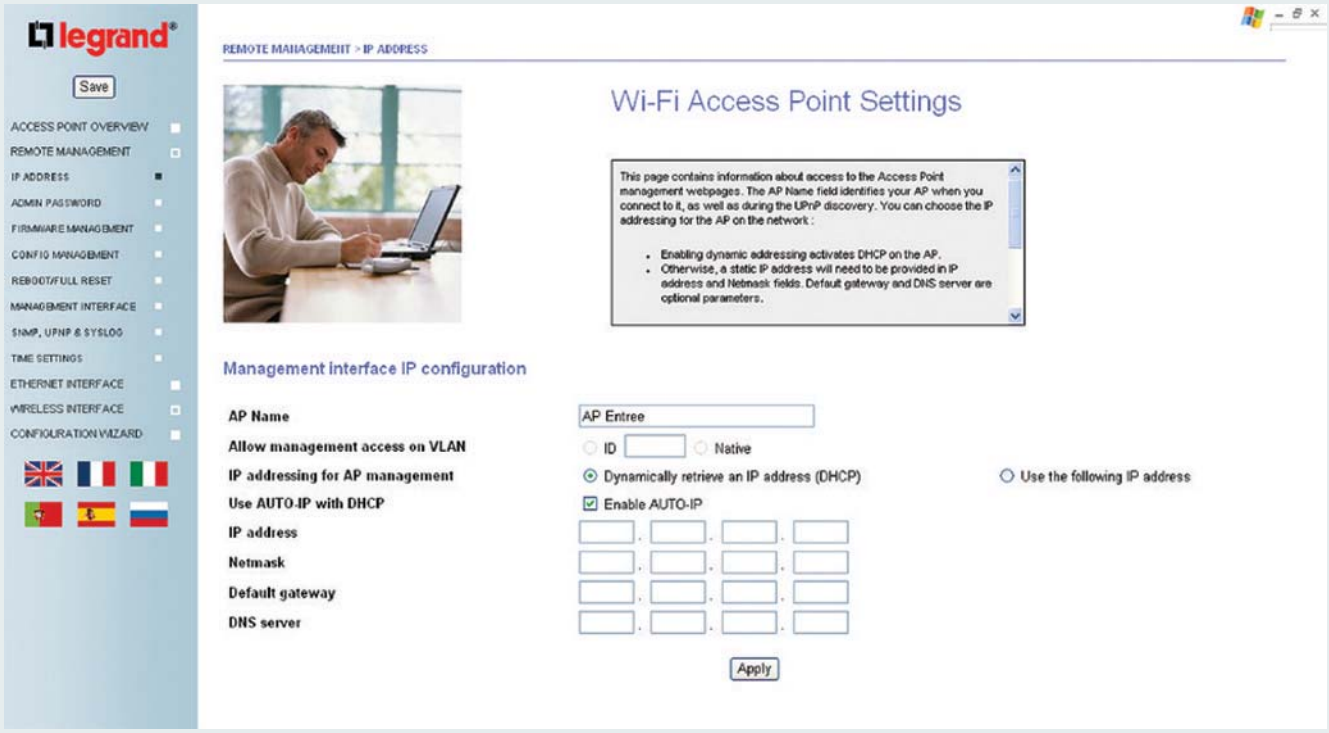
Definition of RUNNING CONFIGURATION & STARTUP CONFIGURATION

In each configuration web interface, changes have to be activated using the "**Apply**" button. This will make the changes effective on the Access Point.
In order to store the settings for the next reboot you have to press the **Save** button.

This allows the user to test the configuration (making changes and pressing the **Apply** buttons on the relevant pages), and only to press the **Save** button when the configuration is satisfactory.
All the settings that are active while the **Save** button is pressed will survive a reboot.

** Only for Dual band Access point.*

1.5 / IP ADDRESS



AP Name

This name will help you to identify your Access Point.

Allow management access on VLAN

All management/configuration access to the AP can be restricted to a specific VLAN on the uplink port.
By default, VLANs are disabled, and access to the management interface is allowed from any interface.
If needed, one VLAN on the uplink port can be selected as the only way to access the management interface (VLANs must first be enabled to do so, see the Ethernet Interface section).

Note: *if VLANs are enabled you can restrict management/configuration access to a specific VLAN ID or to the native VLAN.*

Dynamically retrieve an IP address (DHCP)

You can either use Dynamic (DHCP) or Static (use the following IP address) IP addressing for the AP management.
By default or after a full reset, the Access Point is set to use DHCP.

Enable AUTO-IP

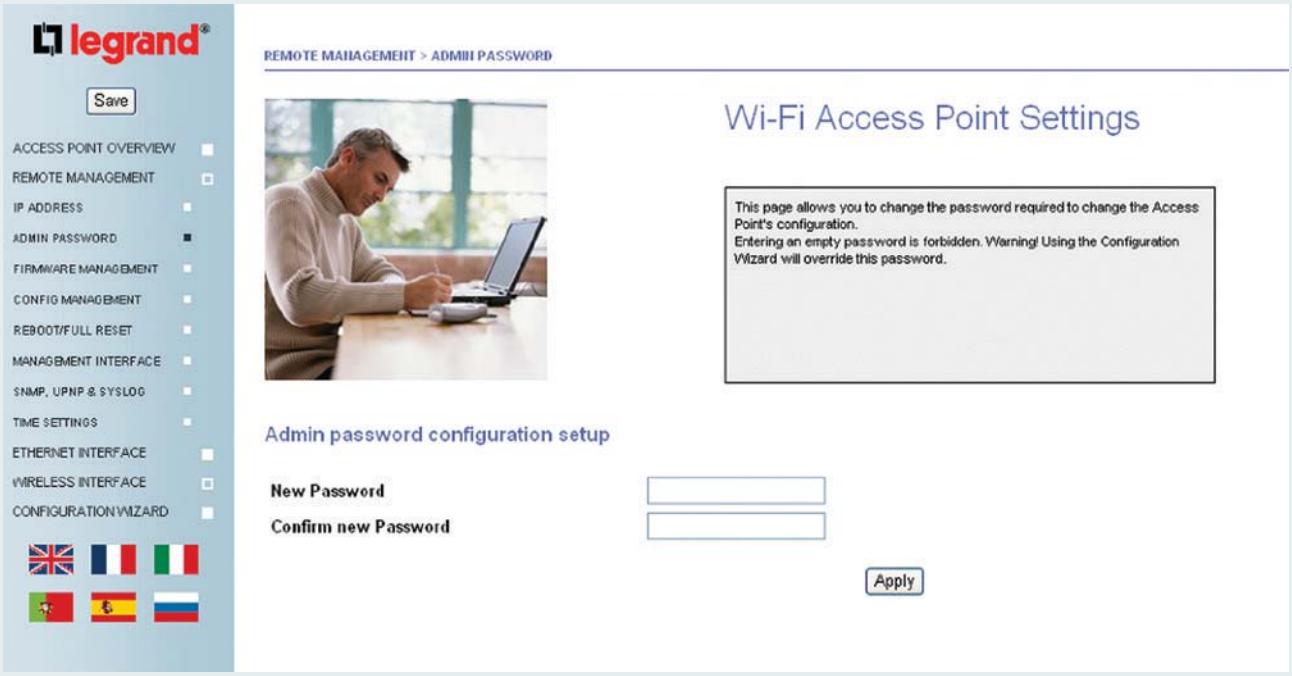
If Enable Auto-IP is checked, the AP will fall back to Auto-IP addressing mode (169.254.0.0/16) if no DHCP server can be found on the network.

Use the following IP address

(An IP address must be unique in your network. **Netmask, Default Gateway and DNS Server,** values can be safely copied from a computer already configured with static IP addressing in your network)
IP Address: Type in the static IP address for your Access Point.
Netmask: Type in the IP Netmask for your network.
Default Gateway: Type in the default gateway IP address (used for any traffic beyond the local network).
DNS Server: Type in your DNS IP address (optional).

After changing settings on this page, click the **Apply** button to validate your changes and click the **Save** button to keep your changes for future reboots.

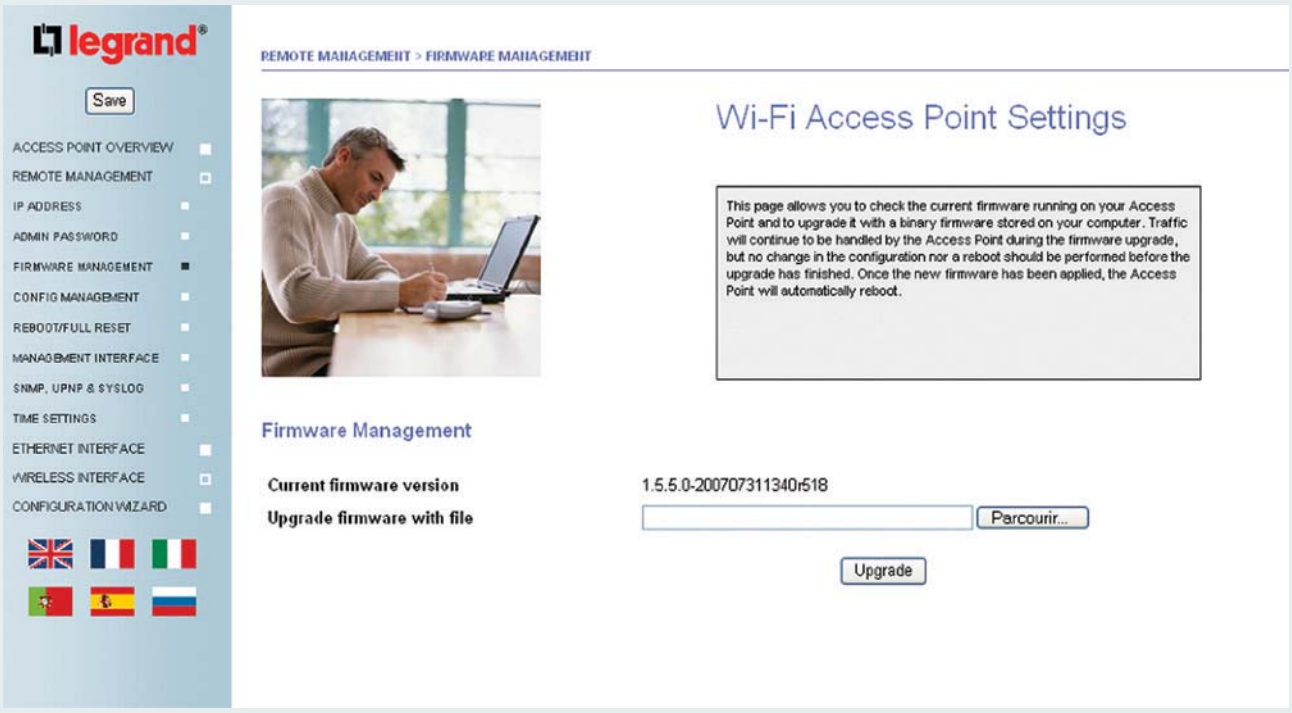
1.6 / ADMINISTRATION PASSWORD



This page allows you to change the Access Point's configuration password.
Enter the new password into the two fields, and click the **Apply** button to apply your changes.

Important:
Restoring the Access Point's factory defaults will erase your Password settings. No password will be prompted for the web interface after a factory defaults reset.

1.7 / FIRMWARE MANAGEMENT

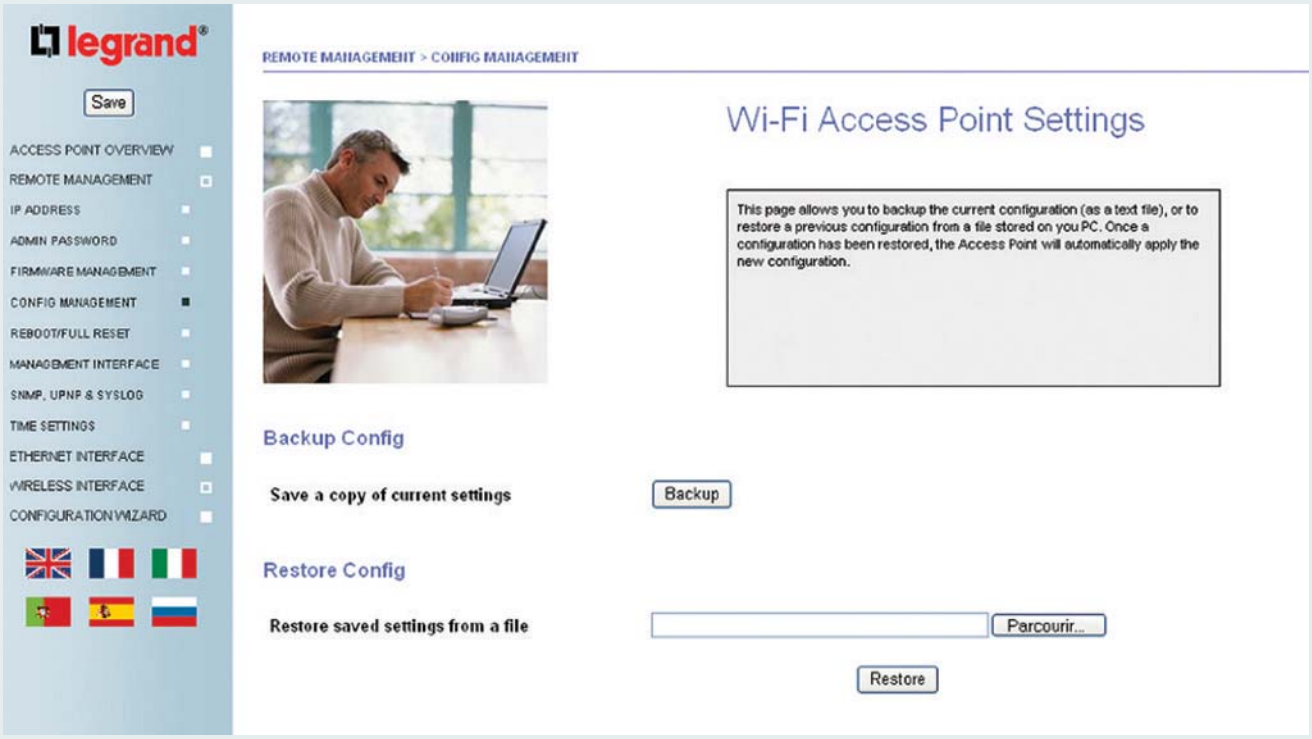


The field **Current firmware version** shows the firmware version running on your Legrand AP.

The firmware upgrade webpage displays the Access Point's current firmware version. Before upgrading the Access Point's firmware, be sure to download the latest firmware from Legrand website *http://www.wifi.legrandelectric.com.*
Press the **Browse** button to select a firmware file on your computer.

Then, click the **Upgrade** button to upgrade the firmware.
This process takes about 5 or 6 minutes.

Note: When upgrading the firmware, you must not interrupt the Web browser or power down your Access Point.

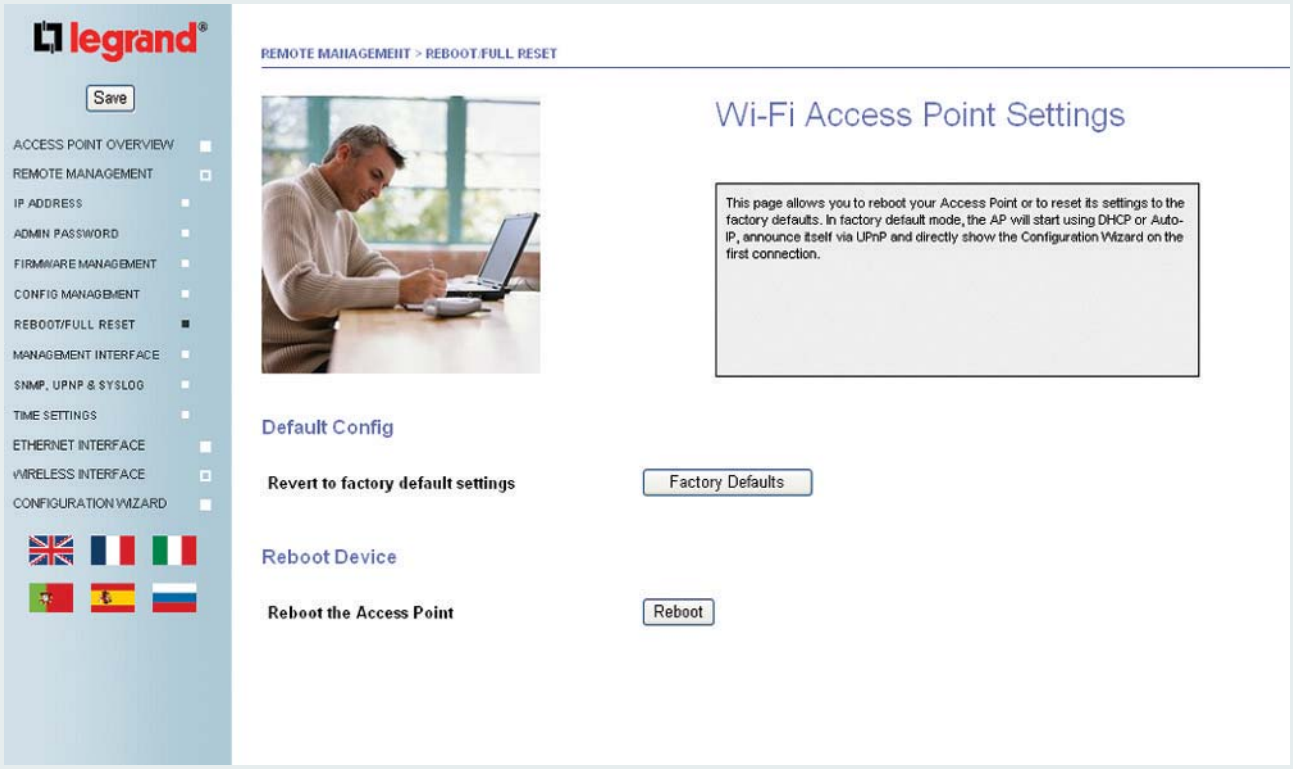


Saving and Retrieving the Configuration

The Access Point settings are stored on the AP.
This configuration can be backed up on the administrator's computer as a text file (**Backup** button).

At a later stage, this file can then be restored to the AP from the user's computer (click on **Browse** to locate the file, then on the **Restore** button).

1.9 / REBOOT / FULL RESET



Default Config

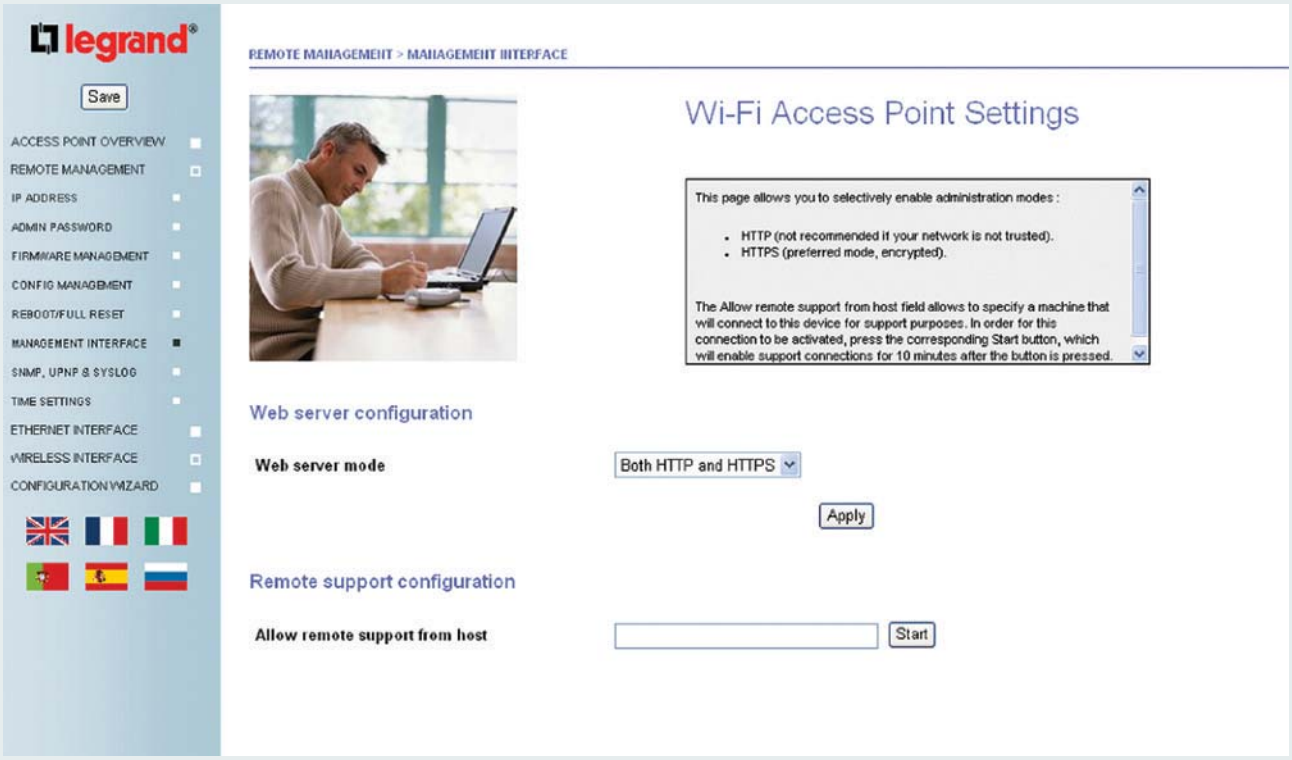
To restore the Access Point's factory default settings, click the **Factory Defaults** button (this is equivalent to performing a long press on the reset button.

Reboot Device

Click on this button to reboot the AP.
Any changes since the last **Save** will be lost, all wireless connections will be terminated during the reboot (this is equivalent to performing a short press on the reset button).

Important:
Restoring the Access Point's factory defaults will erase all of your settings (Password, Security Encryption, Wireless and LAN settings, etc.), and replace them with the factory defaults (see Administration password section).

1.10 / MANAGEMENT INTERFACE



This page allows you to control the enabling/disabling of various methods to configure the Access Point:

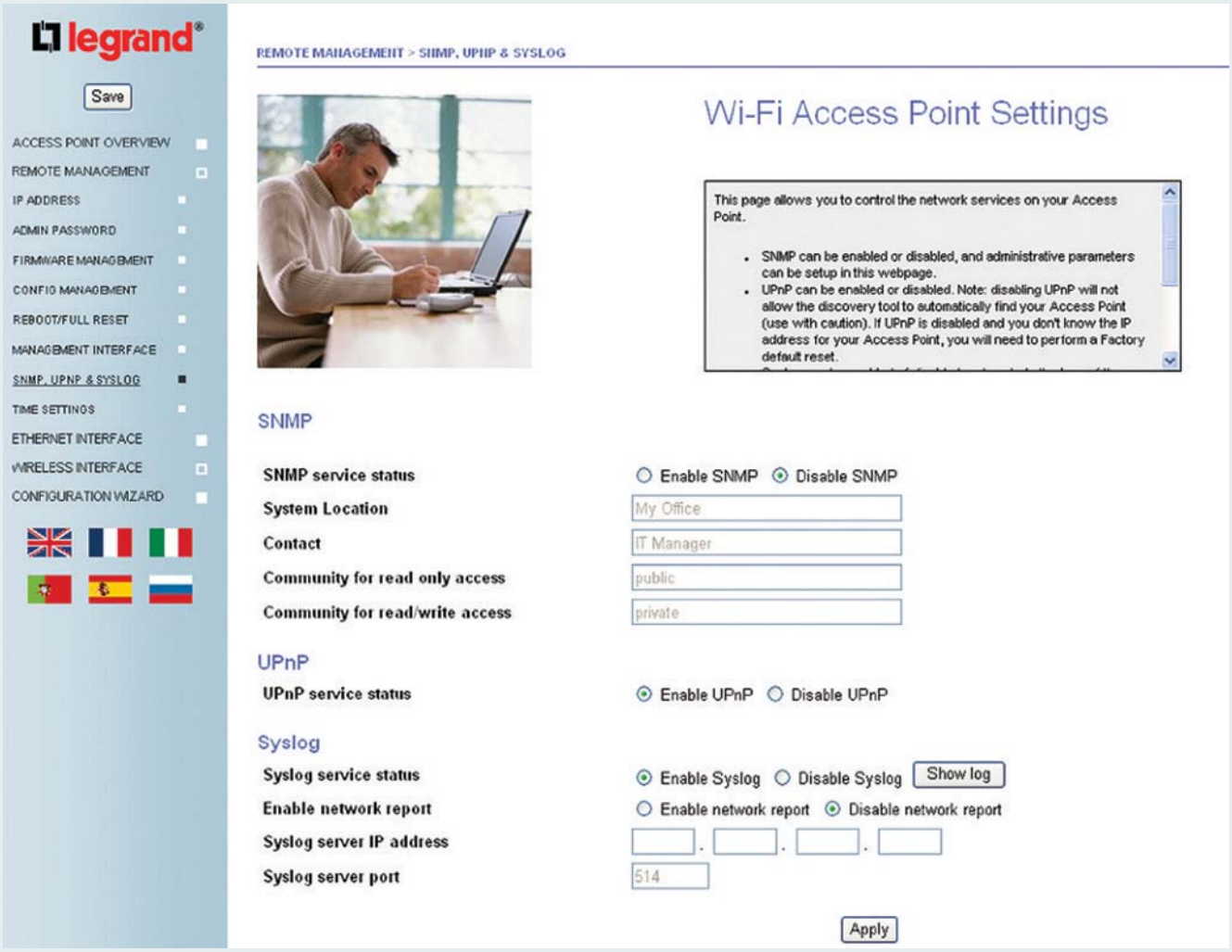
HTTP only: enables management via the web management interface (standard unencrypted HTTP communication).

HTTPS only: enables management only via a secured web management interface (SSL encrypted HTTP communication).

HTTP or HTTPS: enables management via either HTTP or HTTPS.

The **Allow remote support from host** field allows to specify a machine that will connect to this device for support purposes. In order for this connection to be activated, press the corresponding Start button, which will enable support connections for 10 minutes after the button is pressed.

1.11 / SNMP, UPNP & SYSLOG



SNMP

To enable SNMP (remote network monitoring), click on **Enable SNMP**. **Disable SNMP** will be selected by default (after a factory default reset).
In the **System Location** and **Contact** fields, specify a location and administration contact details that will be displayed by the remote SNMP console.
The **Community for read only access** and **Community for read/write access** settings allow controlling SNMP access respectively in read and read/write to the AP.

UPnP

To allow the AP to announce itself to the network using **UPnP**, select **Enable UPnP**. By default, the UPnP is enabled to allow you to use **Legrand Control Point Discovery Utility.**

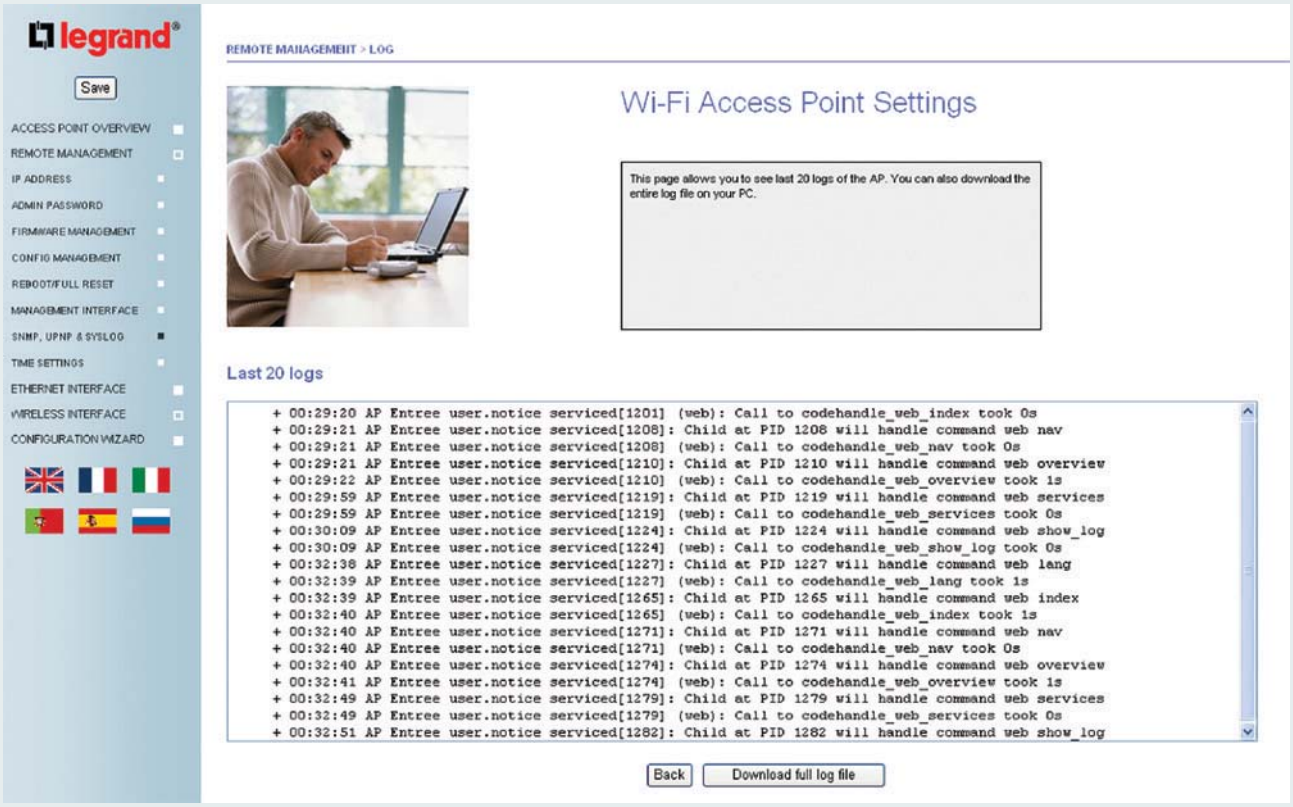
Syslog

To enable system logging, click the **Enable Syslog** button (enabled by default).
If you have chosen to remotely monitor the Access Point's system logs, check **enable Network Report** and select the monitoring equipment machine's IP address and UDP port in the field **Syslog Server IP Address** and **Syslog Server Port respectively**.

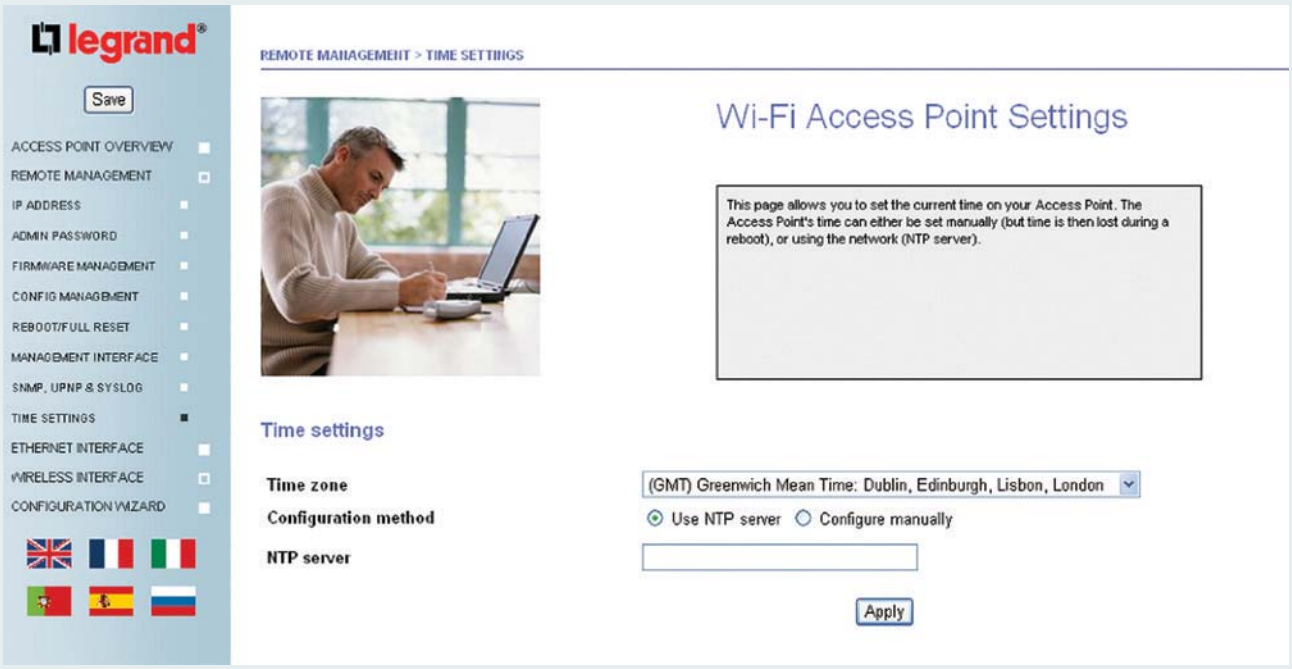
After changing settings on this page, click the **Apply** button to validate your changes and click the **Save** button to save your changes for future reboots.

Show Log

Click the **Show Log** button to see the 20 last logs or click **Download full log file** button to retrieve all logs (see below) since the last reboot.



1.12 / TIME SETTINGS



Time Zone

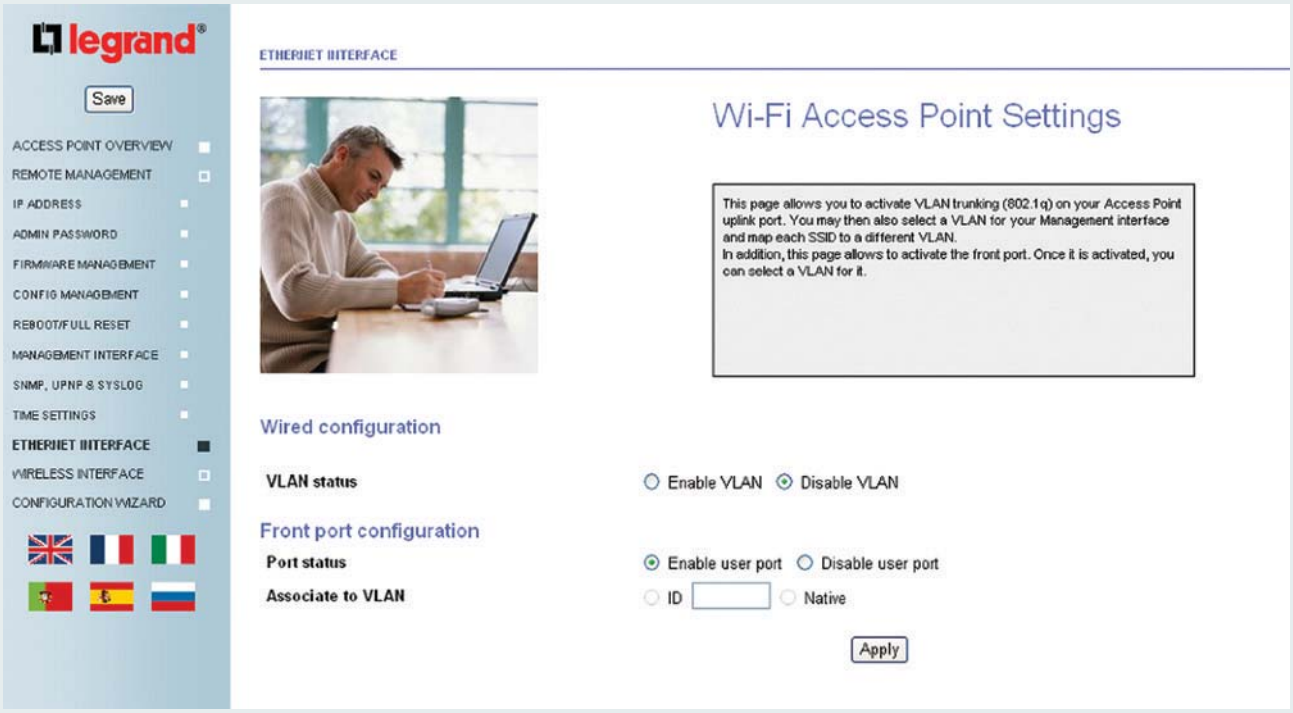
In the menu change the time zone where your AP is located.
If your location does not appear in this list, select a location in the same time zone.
The default is GMT.

Configuration method

You can choose between two modes to adjust the time on your AP: **Use NTP server or Manually**.
- If you select **Use NTP server**, the Legrand AP will automatically sync to UTC/GMT time from the NTP server of your choice in the field **NTP server**.
Over time, a device's clock is prone to drift. The Network Time Protocol (NTP) is one way to ensure your clock stays accurate.
- If you select **Manually**, you will need to manually adjust the current date/time (See figure on next page). However, in this case the time will be lost after a reboot.

After changing settings on this page, click the **Apply** button to validate your changes and click the **Save** button to save your changes for future reboots.

1.13 / ETHERNET INTERFACE



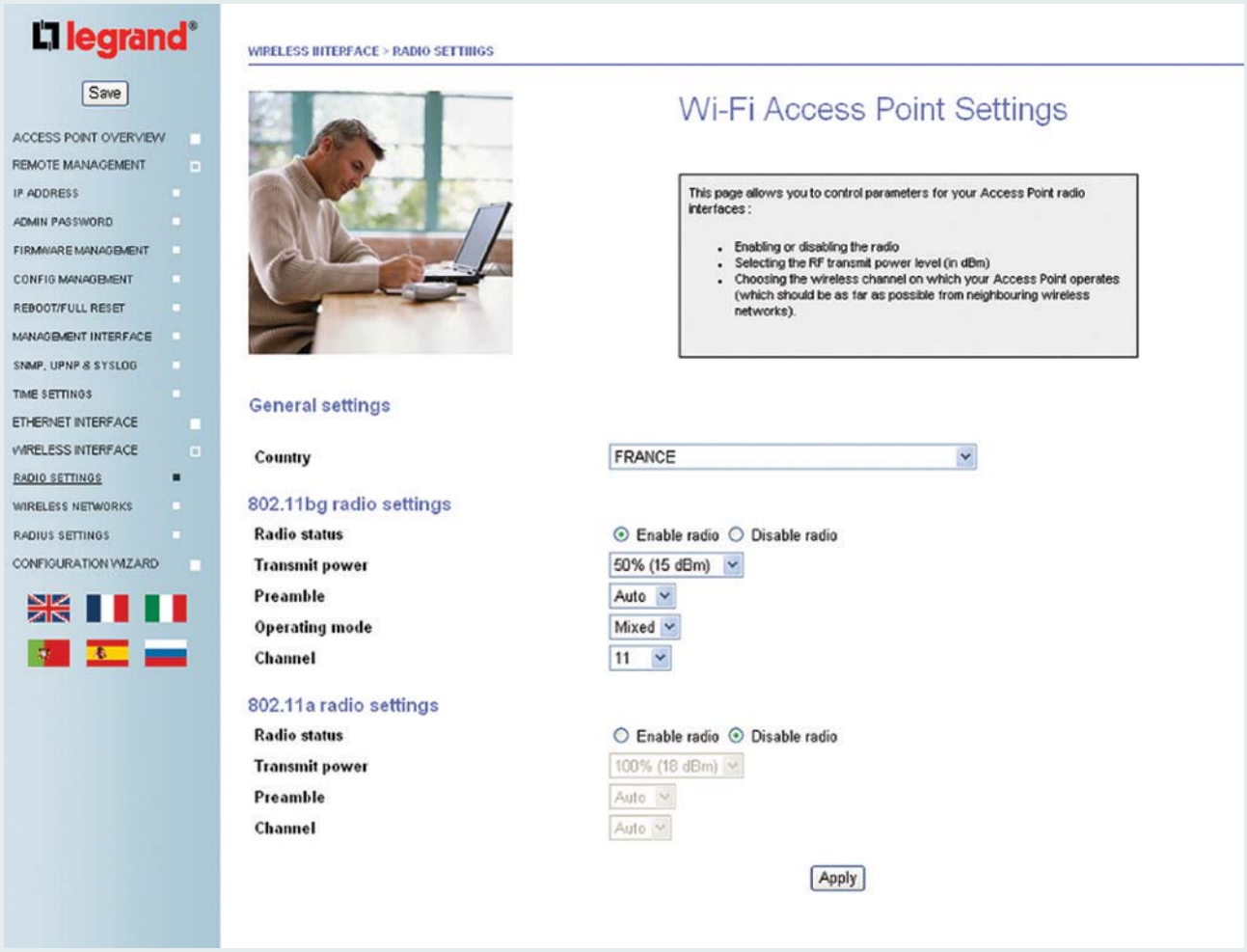
By selecting **Enable VLAN**, you can activate 802.1q VLAN trunking on the uplink Ethernet interface.
The default value is **Disable VLAN**, which will not use any VLAN tagging on the uplink interface.
In order to achieve a sufficient security level, VLANs should be used to isolate traffic when several network names (SSIDs) are activated on the same radio.

Selecting **Enable User Port** activate the front Ethernet port.

Associate to VLAN: If the front Ethernet port is associated to a VLAN you can restrict the traffic from/to the front Ethernet port to a specific VLAN ID or to the native VLAN.

After changing settings on this page, click the **Apply** button to validate your changes and click the **Save** button to save your changes for future reboots.

1.14 / RADIO SETTINGS



The Legrand AP integrates two wireless radios* in order to create two overlaid networks (802.11b/g on 2.4GHz and 802.11a on 5 GHz).
Each radio can be enabled/disabled independently (**Radio status** field).

The following settings are available for each radio:
- The radio **transmit power** can be adjusted on each radio (**Transmit power** field).
- The **preamble** type can be adjusted using the Preamble Field (recommended value **Auto**).

The b/g radio can act as an 802.11 b only, an 802.11g only or an 802.11b/g mixed (default) network.
The **Operating mode** allows to select the compatibility mode for the 2.4GHz radio.

Note: The available channels supported by the wireless products depend on the country (regulation) where they are installed.
For example, Channels 1 to 11 are supported in the U.S. and Canada, Channels 1 to 13 in Europe and Australia and 1 to 14 in Japan.

** Only for Dual band Access point.*

802.11b/g Radio Frequency Channels

Channel	Frequency
1	2.412 GHz
2	2.417 GHz
3	2.422 GHz
4	2.427 GHz
5	2.432 GHz
6	2.437 GHz
7	2.442 GHz
8	2.447 GHz
9	2.452 GHz
10	2.457 GHz
11	2.462 GHz
12	2.467 GHz
13	2.472 GHz
14	2.484 GHz

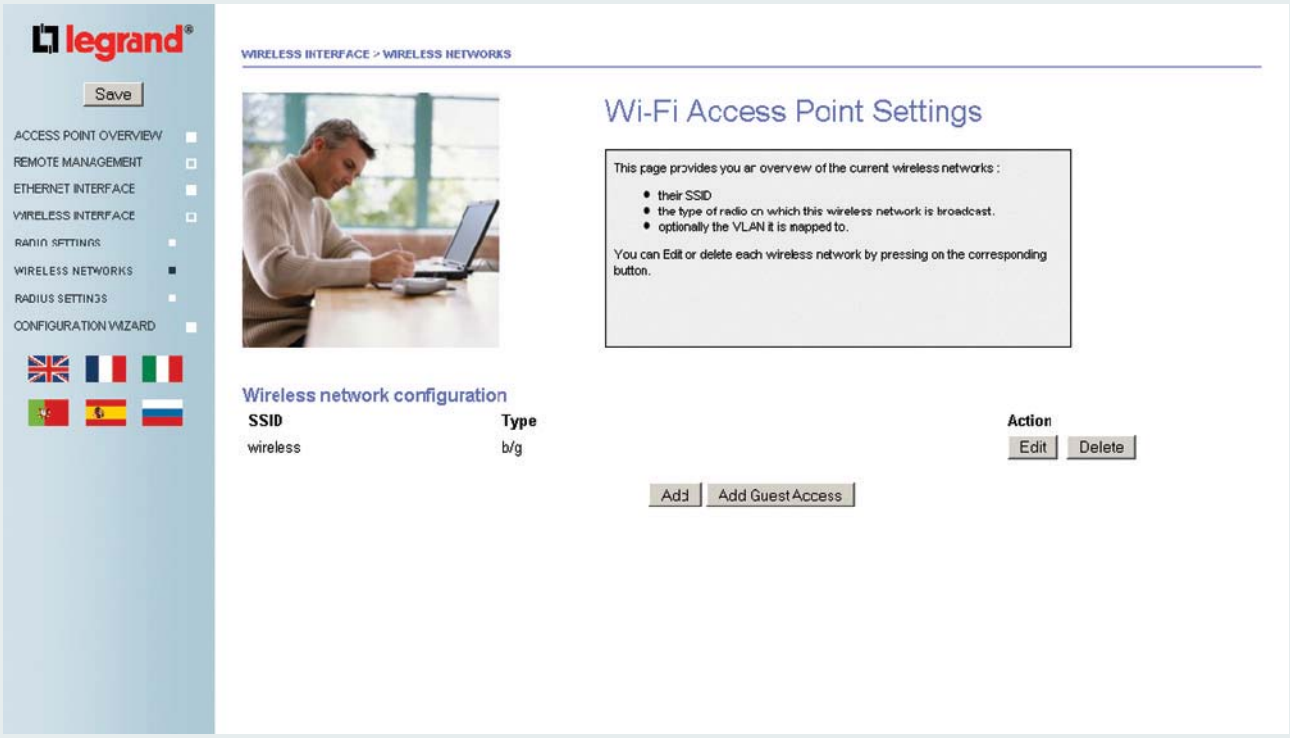
802.11a Wireless Channels

Channel	Frequency
36	5.180 GHz
40	5.200 GHz
44	5.220 GHz
48	5.240 GHz
52	5.260 GHz
56	5.280 GHz
60	5.300 GHz
64	5.320 GHz

In a wireless network, it is the AP that selects the channel on which all radio transmissions will be performed.

After changing settings on this page, click the **Apply** button to validate your changes and click the **Save** button to save your changes for future reboots.

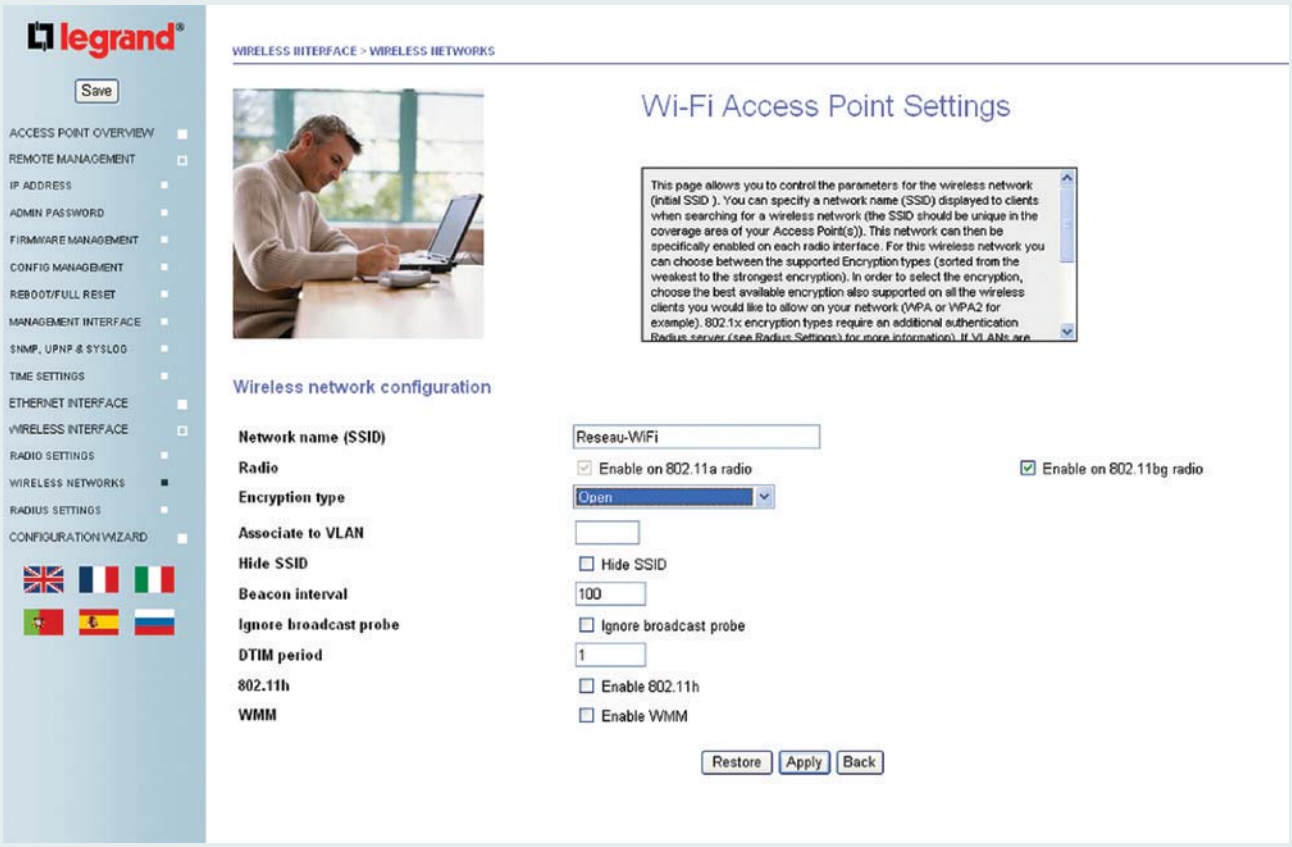
1.15 / WIRELESS NETWORK



This page shows you the list of **SSIDs** already configured.

The **Edit** button allows you to modify the corresponding SSID configuration.
The **Delete** button allows you to erase the corresponding **SSID**.
The **Add** button allows you to add a new **SSID** as described on the next pages.

You can use the **Add Guest Access** button to add your guests to a network that will only enable them to connect to the Internet. Only one guest-access wireless network can be created.



Network name (SSID)

The **SSID** is also known as the wireless network name.
The characters in this field are case sensitive.

Radio

In this field, you can select which radio this SSID will be assigned to.
Possible choices are 802.11a only, 802.11bg only or 802.11a + 802.11bg.

Encryption type

choose your authentication method from the following (from the lowest to the highest security level):

1. OPEN
2. STATIC WEP
3. WEP with 802.1x
4. STATIC WPA
5. STATIC WPA with 802.1x
6. STATIC WPA2
7. WPA with 802.1x
8. STATIC WPA or WPA2
9. WPA or WPA2 with 802.1x

Associate to VLAN
If VLANs are enabled, you can restrict the traffic from/to this SSID to a specific VLAN ID.

Hide SSID
Check the field **Hide SSID** to prevent the AP from broadcasting the SSID for this network.
Note: *this will force the users to manually enter the SSID for this wireless network on their computers, and may even prevent some wireless clients from connecting. This field is unchecked by default.*

Beacon Interval
Specifies how much time elapses between two beacon frames sent from the AP.
The default value should be suitable for most installations.

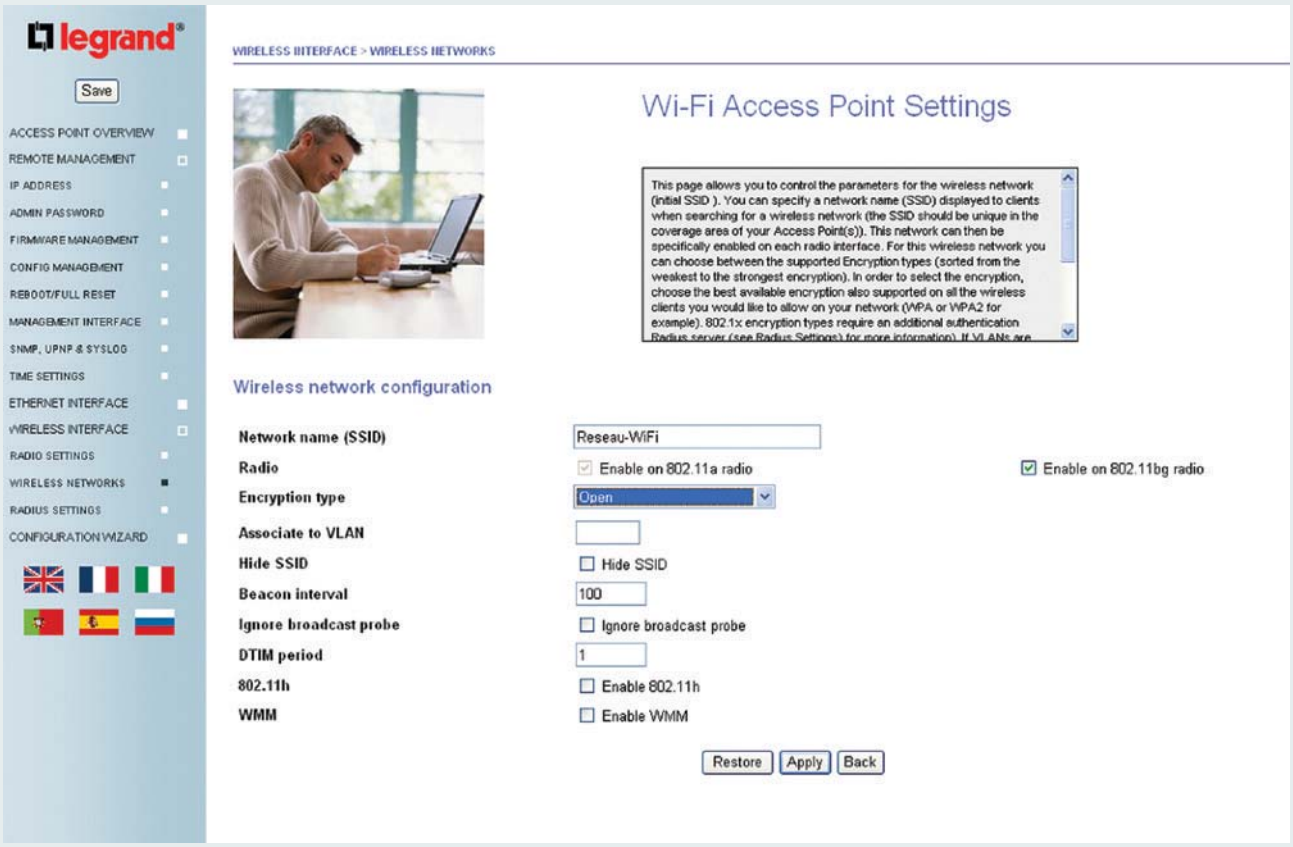
Ignore Broadcast probe requests
enable this option to prevent the AP from responding to broadcast scanning from wireless equipments (this can make the wireless network less visible to scanning tools).

DTIM period (Delivery Traffic Indication Message)
Specifies every how many beacons a DTIM indication will be included (allows equipments in power save mode to wake up).
The default value of 1 should be suitable for most installations.

802.11h
Check this option to make the AP comply with the IEEE 802.11h standard (radar avoidance and power saving regulation for Europe).
The remaining Wireless Network fields depend on the type of encryption selected and are detailed per encryption type in the sections below.

WMM
Check this option to activate Quality of service, which is developed by the WiFi alliance as a subset of 802.11e standard called the Wi-Fi Multimedia (WMM) specification.

1.15.1 / WIRELESS NETWORK / SECURITY/Open

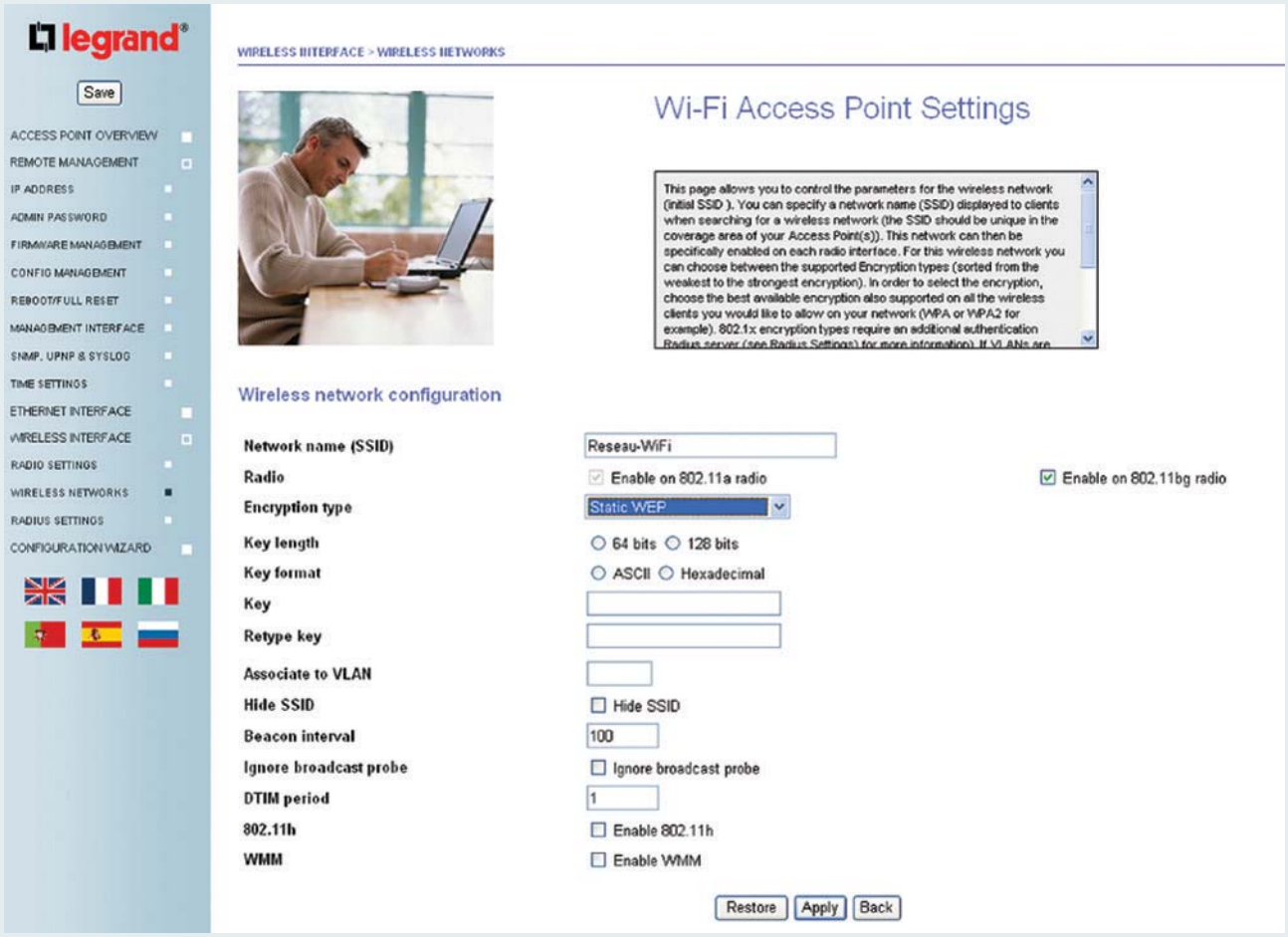


Encryption type

Select Open.

In this mode, any equipment is allowed to connect to your wireless network.
Your network will not be protected by any security or encryption.

1.15.2 / WIRELESS NETWORK / SECURITY/STATIC WEP



Encryption type

Select Static WEP.

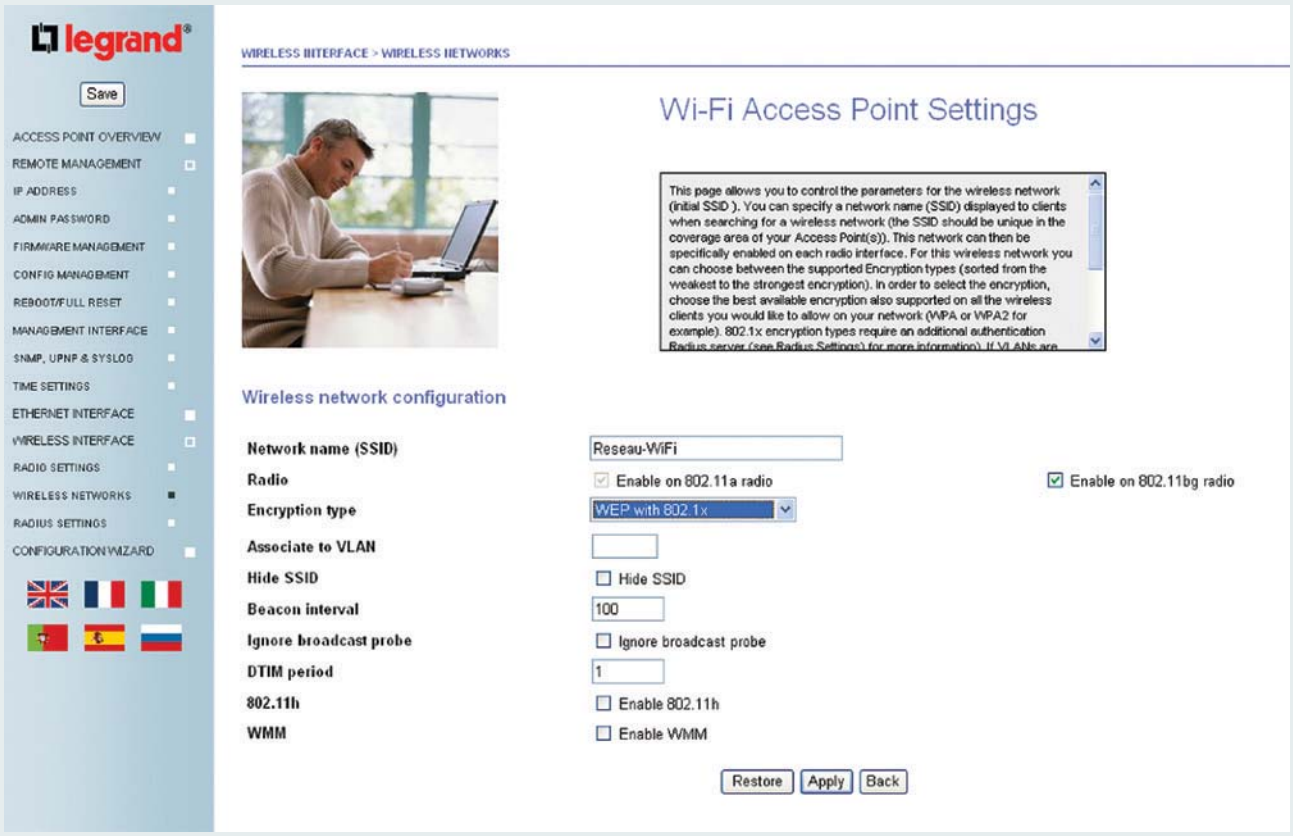
Key

Enter the WEP Key encrypting the data on your wireless network.
WEP keys can be 64 or 128bits long and can be entered as ASCII or in hexadecimal format.
The length of the keys will thus be:

- 10 hexadecimal digits for 64-bit keys
- 5 ASCII characters for 64-bit keys
- 26 hexadecimal digits for 128-bit keys
- 13 ASCII characters for 128-bit keys

You will need to enter this WEP key on each equipment that will connect to your wireless network.

1.15.3 / WIRELESS NETWORK / SECURITY/WEP with 802.1x

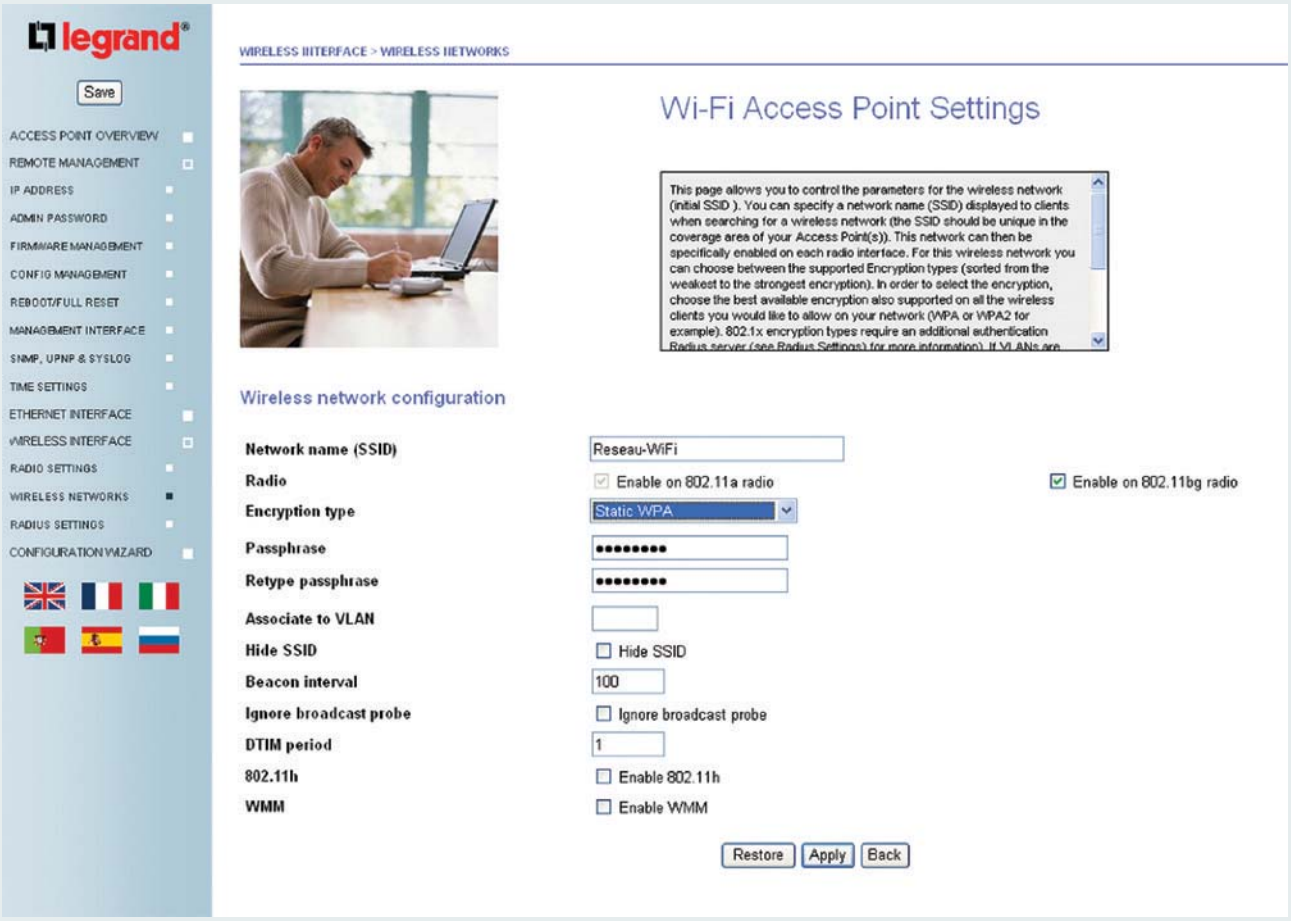


Encryption type

Select WEP with 802.1x.

Use WEP as an encryption mode and 802.1x (Radius authentication) as the station authentication protocol.
No key needs to be provided in this encryption mode, as the key will be dynamically provided by an external Radius server (See Radius section).

1.15.4 / WIRELESS NETWORK / SECURITY/STATIC WPA



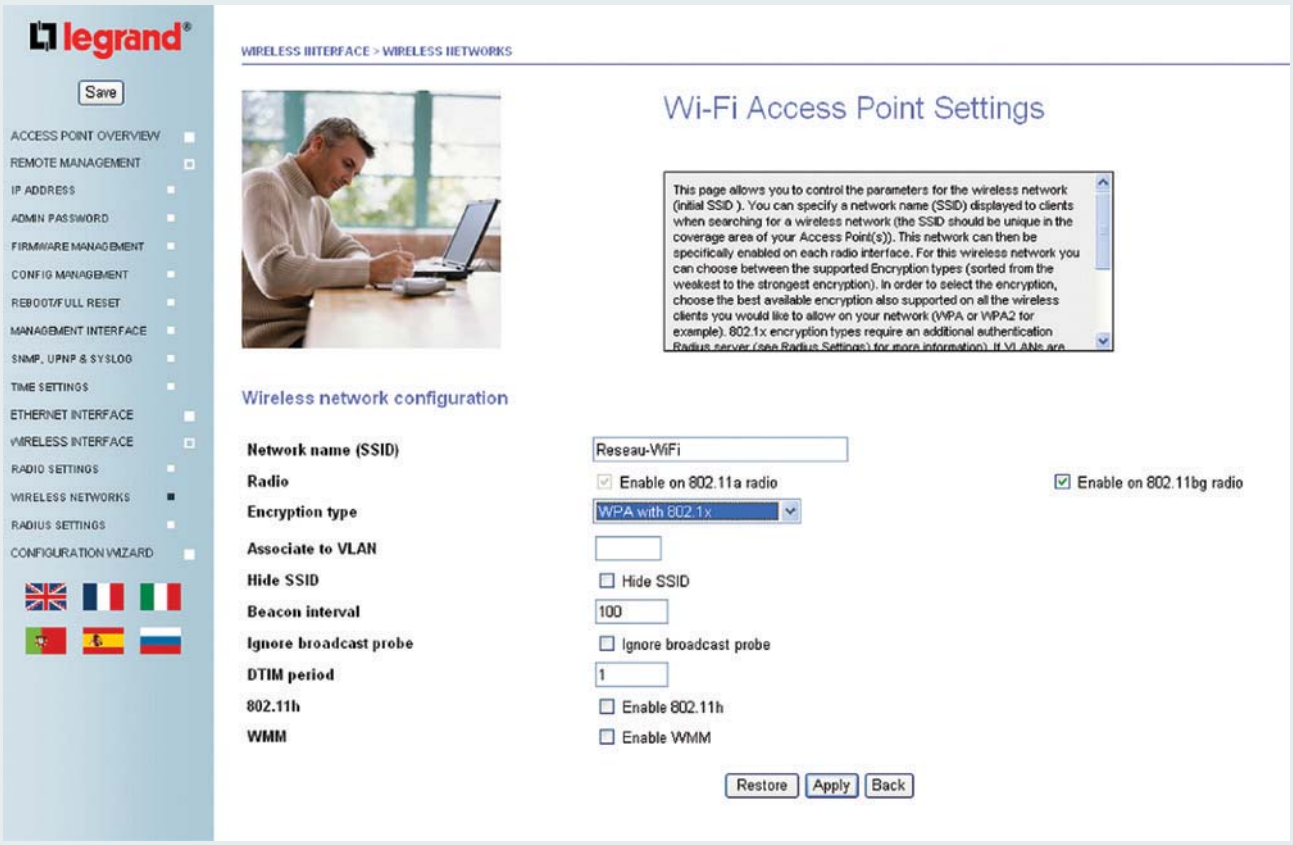
Encryption type

Select Static WPA.

This encryption is stronger than WEP, and also called WPA-PSK (based on RC4+TKIP). The key is provided as a passphrase of at least 8 characters.

You will need to enter this WPA passphrase on each equipment that will connect to your wireless network.

1.15.5 / WIRELESS NETWORK / SECURITY WPA with 802.1x

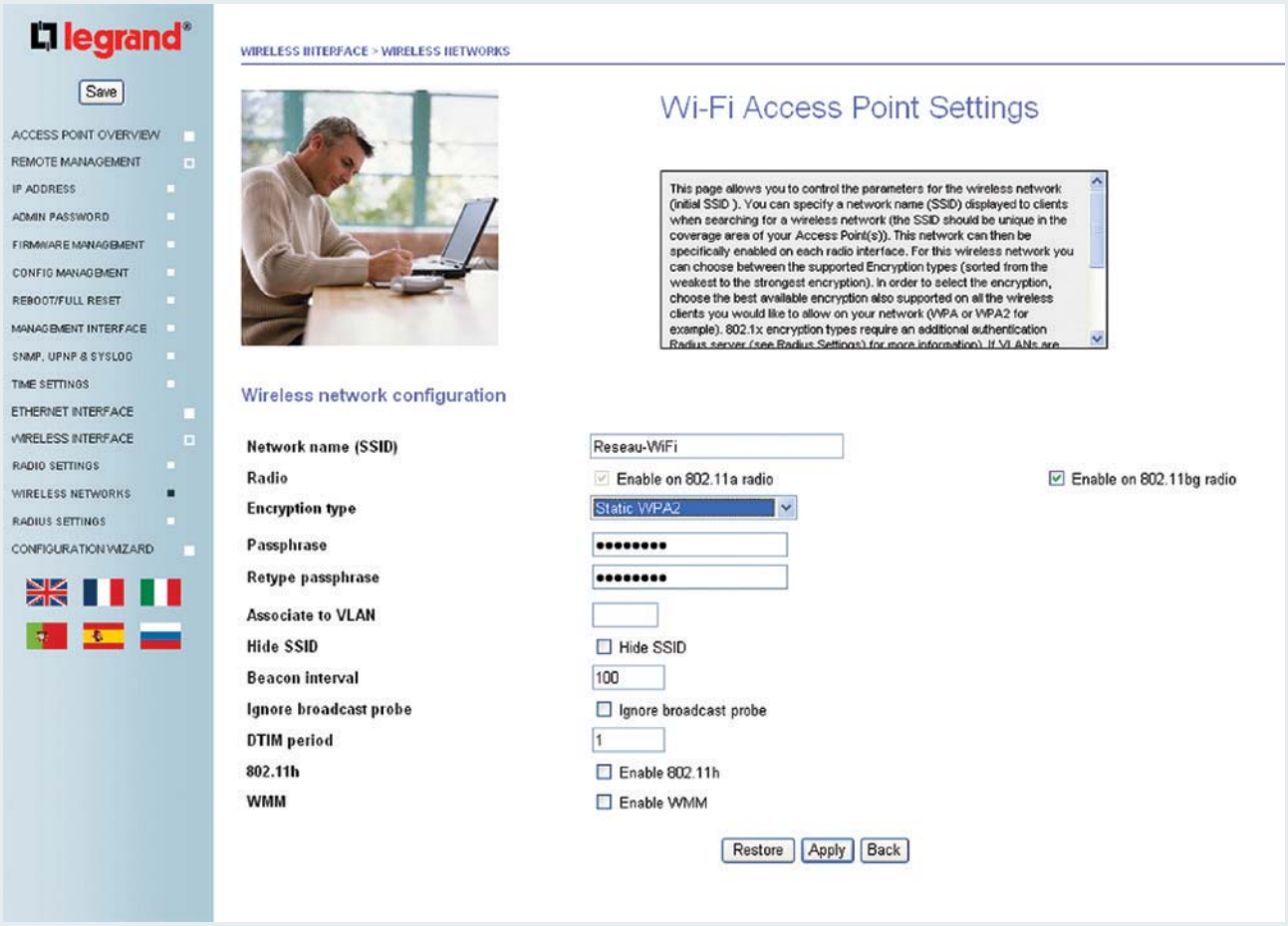


Encryption type

Select encryption WPA with 802.1x.

Use WPA as an encryption mode and 802.1x (Radius authentication) as the station authentication protocol.
No key needs to be provided in this encryption mode, as the key will be dynamically provided by an external Radius server (See Radius section).

1.15.6 / WIRELESS NETWORK / SECURITY/STATIC WPA2



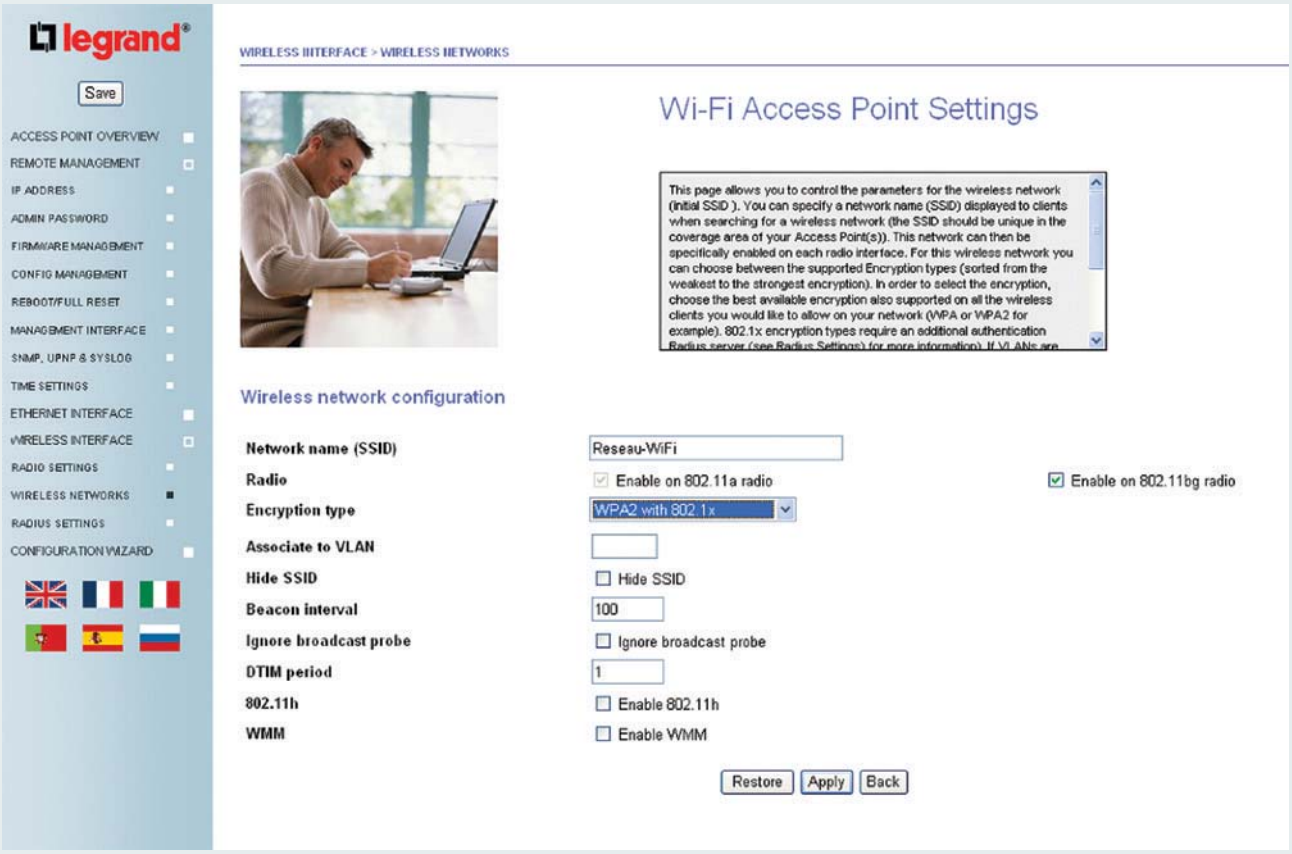
Encryption type

Select static WPA2.

This encryption is stronger than WEP and WPA, and also called WPA2-PSK or 802.11i-PSK (based on AES and CCMP). The key is provided as a passphrase of at least 8 characters.

You will need to enter this WPA2 passphrase on each equipment that will connect to your wireless network.

1.15.7 /WIRELESS NETWORK / SECURITY/WPA2 with 802.1x

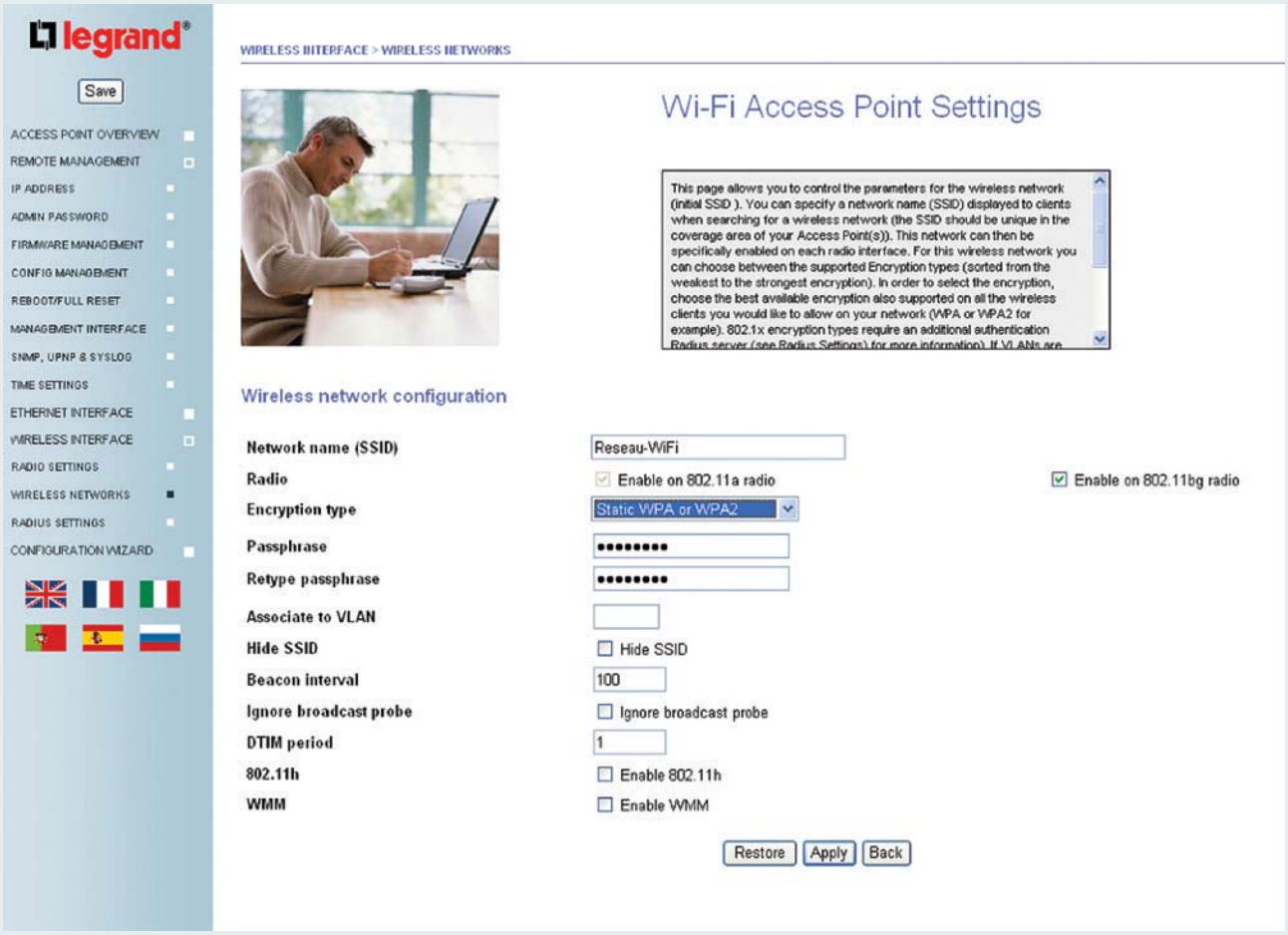


Encryption type

Select WPA2 with 802.1x.

Use WPA2 as an encryption mode and 802.1x (Radius authentication) as the station authentication protocol.
No key needs to be provided in this encryption mode, as the key will be dynamically provided by an external Radius server (See Radius section).

1.15.7 / WIRELESS NETWORK / SECURITY/STATIC WPA OR WPA2

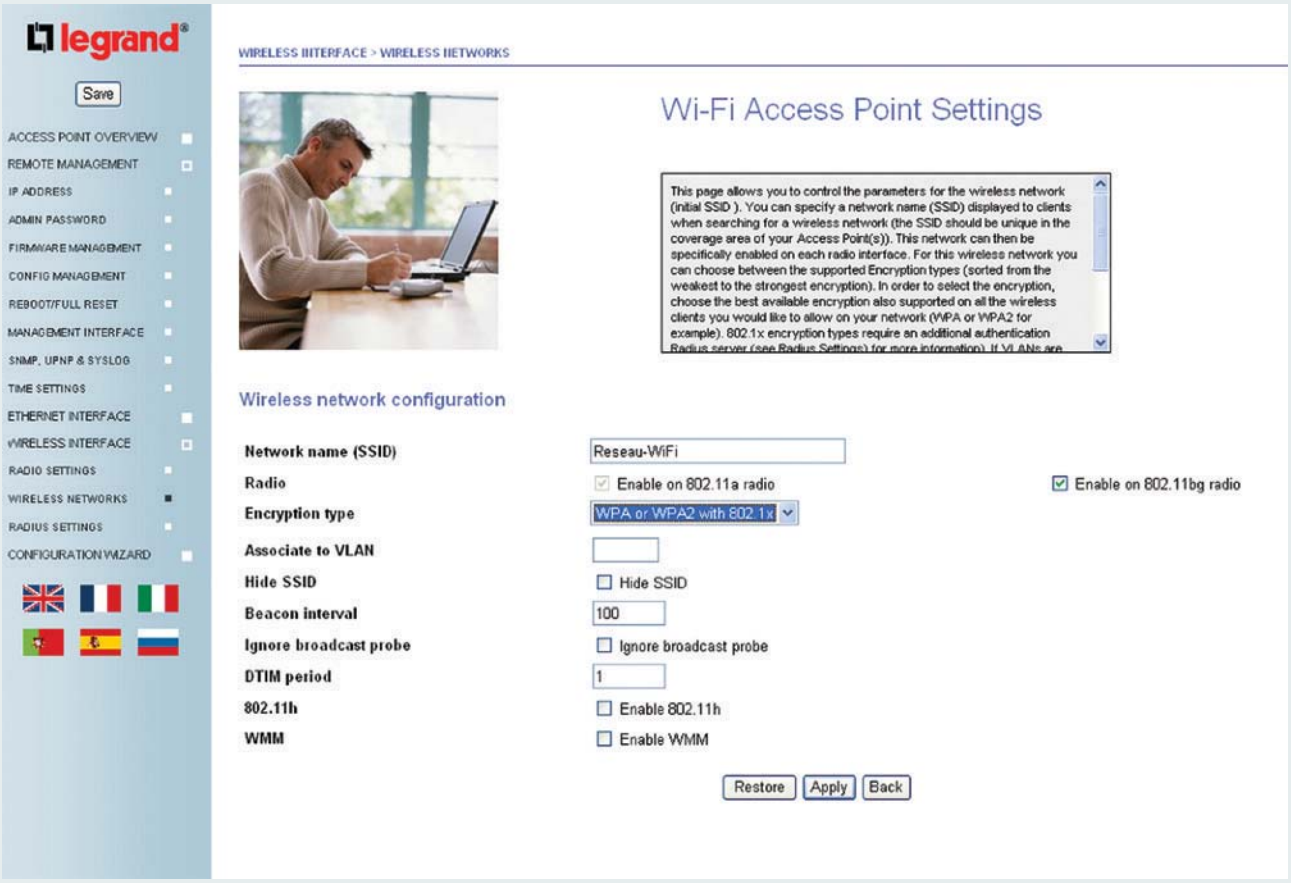


Encryption type

Select Static WPA or WPA2.

Using this mode, mixed WPA and WPA2 (802.11i) clients will be allowed to connect to the wireless network.

1.15.8 / WIRELESS NETWORK / SECURITY/WPA or WPA2 with 802.1x



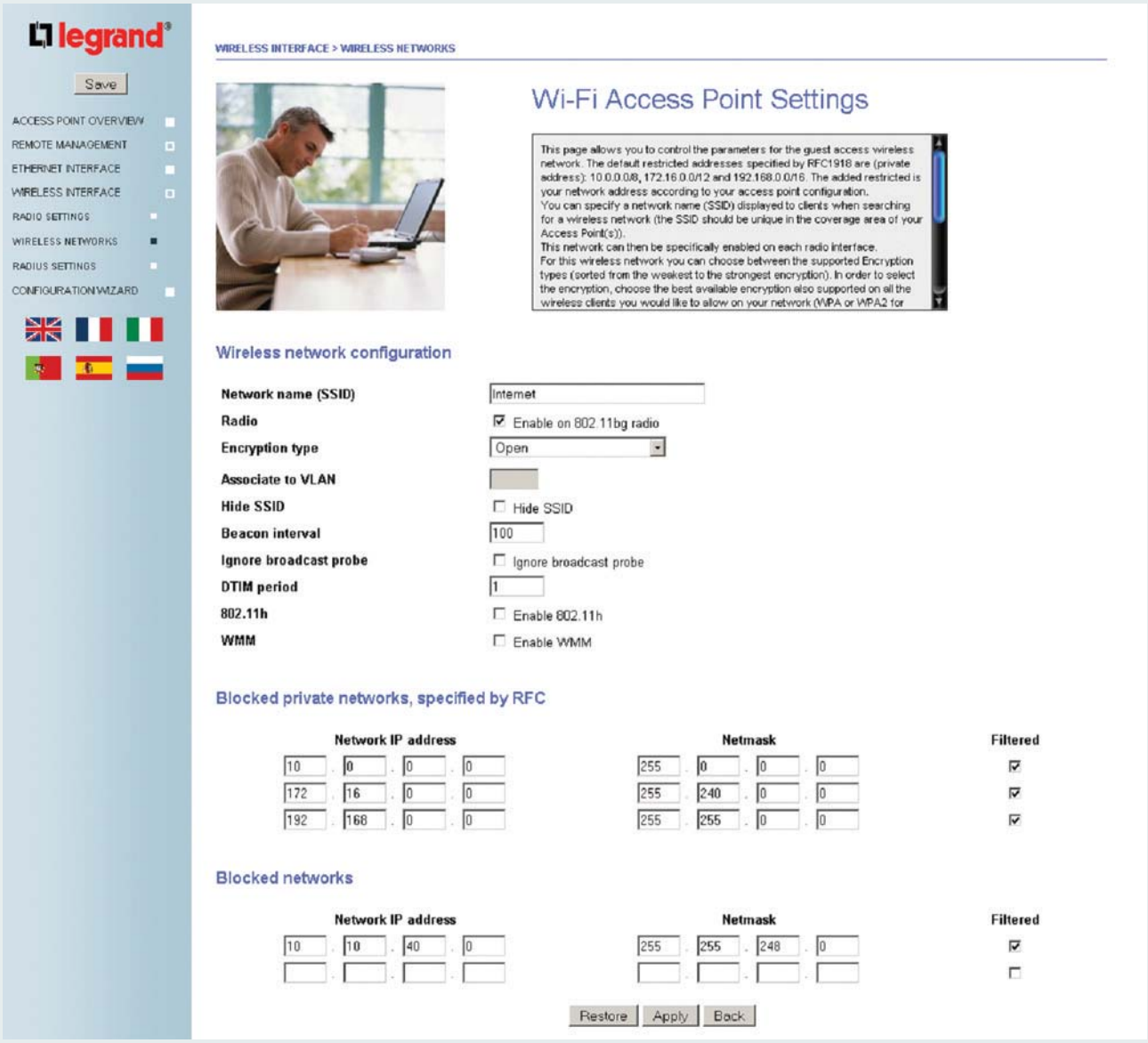
Encryption type

Select encryption WPA or WPA2 with 802.1x.

Use WPA or WPA2 as an encryption mode and 802.1x (Radius authentication) as the station authentication protocol.
No key needs to be provided in this encryption mode, as the key will be dynamically provided by an external Radius server (See Radius section).

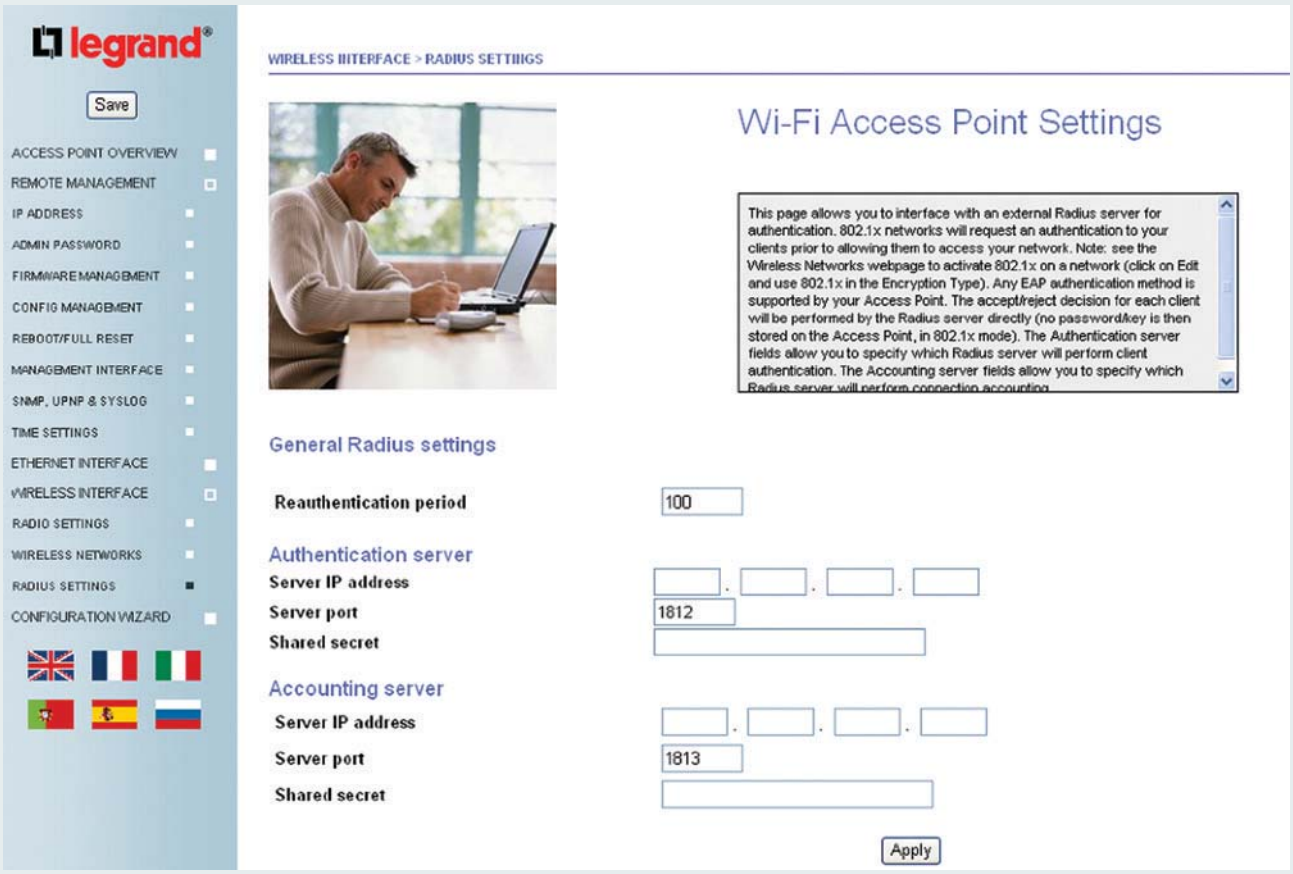
Using this mode, mixed WPA and WPA2 (802.11i) clients will be allowed to connect to the wireless network.

1.15.9 / WIRELESS NETWORK / GUEST ACCESS



In addition to the conventional wireless network parameters described above, this page also lets you configure the networks to which people connected to this SSID will not have access. By default, the private networks described in the RFC1918 are filtered automatically.
You have the option of setting a further 4 networks for filtering. The network hosting the access point is automatically uncovered and pre-completed..

1.16 / RADIUS SETTINGS



The Radius webpage allows your AP to delegate authentication to a remote Radius server (using 802.1x port-based authentication).

Reauthentication period
In this field, you can specify every how many seconds a wireless client will have to reauthenticate.

Authentication Server IP address
This is the IP address of the Radius server used for 802.1x client authentication.

Authentication Server port
Using this field, you can specify the authentication port on the radius server.

Authentication Shared secret
This field contains the shared secret between the Wireless Access Point and the radius server to secure Radius communications.

Accounting Server IP address
This is the IP address of the server managing wireless clients accounting.

Accounting Server port
Using this field, you can specify the accounting port on the accounting server.

Accounting Shared secret
This field contains the shared secret between the Wireless Access Point and the accounting server.

After changing settings on this page, click the **Apply** button to validate your changes and click the **Save** button to save your changes for future reboots.

RESTORING THE FACTORY DEFAULT CONFIGURATION

Using the Reset Button

If an issue with your Access Point's configuration prevents you from connecting back to its management interface, a factory default reset will be needed.
To restore the factory default configuration settings, use the Default Reset button on the front of the wireless access point.
This reset button has two functions:
• **Reboot.** After a short press on the button, the Wireless Access Point will reboot (restart). This has the same effect as power cycling the AP or pressing the Reboot button in the Reboot/Full reset menu.
• **Reset to Factory Defaults.** If the reset button is pressed and held for more than 5 seconds, the Blue LEDs will flash shortly and the AP will reboot with its factory default configuration.

Default Factory Settings

When you start the first configuration of your Legrand Access Point, the default factory settings will be set as shown below.

Password	None
Access Point Name	AP Legrand
IP address	DHCP then auto-IP
VLANs	Disabled
11a Network Name (SSID)	Legrand
11g Network Name (SSID)	Legrand
Broadcast Network Name (SSID)	Enabled
802.11a Radio Frequency Channel	Auto
802.11g Radio Frequency Channel	Auto
Security mode	(no WEP, no WPA, no WPA2)
NTP	Disabled
SNMP	Disabled
Syslog	Disabled
Radius Settings	None
UPnP	Enabled

SPECIFICATIONS

Standards	IEEE 802.11a, IEEE 802.11g, IEEE 802.11b, IEEE 802.3af
Internet Ports	One 10/100 RJ-45 Port for connection to the backbone network (uplink port)
LAN	One 10/100 RJ-45 Switched Ports
Reset Button	One reboot/full reset button
Cabling	UTP type CAT 5 Ethernet Cable or better
LEDs	Power, DMZ, Internet, Ethernet (1, 2, 3, 4)
Dimensions	3.55" x 1.77" x 2.36"
(W x H x D)	(90 mm x 45 mm x 60 mm)
Weight	0.19 lbs. (90 g)
Power supply	Power over Ethernet (802.3af)
Certifications	CE
Operating Temperature	5 °C to 40 °C (41 °F to 104 °F)
Storage Temperature	-20 °C to 70 °C (-4 °F to 158 °F)
Operating Humidity	10 % to 85 % Non-Condensing
Storage Humidity	5 % to 90 % Non-Condensing

GLOSSARY

100BASE-T
IEEE 802.3 specification for 100 Mbps Ethernet over twisted pair wiring.

802.1x
802.1x defines port-based network access control used to provide authenticated network access and automated data encryption key management. The IEEE 802.1x draft standard offers an effective framework for authenticating and controlling user traffic to a protected network, as well as dynamically varying encryption keys. 802.1x uses a protocol called EAP (Extensible Authentication Protocol).

802.11a
IEEE specification for wireless networking at 54 Mbps using orthogonal frequency division multiplexing (OFDM) technology and operating in the unlicensed radio spectrum at 5GHz.

802.11b
IEEE specification for wireless networking at 11 Mbps using direct-sequence spread-spectrum (DSSS) technology and operating in the unlicensed radio spectrum at 2.4GHz.

802.11g
IEEE specification for wireless networking at 54 Mbps using orthogonal frequency division multiplexing (OFDM) technology and operating in the unlicensed radio spectrum at 2.4GHz. 802.11g is backwards compatible with 802.11b.

802.11i
IEEE 802.11i, also known as WPA2, is an amendment to the 802.11 standard specifying security mechanisms for wireless networks.

a

AP
Access Point

c

Centrino
Chipset developed by Intel for mobile computing, especially laptops. They incorporate builtin wireless adapters.

Channel
Subdivision of the Wi-Fi band 13 channels are available in France in the 2.4 GHz band.

Configuration password
Password needed to change the Legrand Access Point configuration (channel, SSID, encryption). The configuration password is requested when you connect to the management interface.

d

DHCP (Dynamic Host Configuration Protocol)
An Ethernet protocol specifying how a centralized DHCP server can assign network configuration to multiple clients. The assigned information includes IP addresses, DNS addresses, and gateway (router) addresses.

e

Encryption
Encoding of information exchanged between two wireless equipments to make them unintelligible to any other equipment that is not aware of the encryption key/passphrase.

ESSID (also called SSID)
The Extended Service Set Identification (ESSID) is a thirty-two character (maximum) alphanumeric key identifying the wireless local area network.

Ethernet
The 802.3 IEEE standard network protocol that specifies communication s over twisted pairs.

f

Firmware
Sofware that is written onto the flash memory of the Access Point. It is retained even when the device is turned off.

g

Gateway
A local device, usually a router, that connects hosts on a local network to other networks.

h

Hexadecimal key

Representation in hexadecimal format (computing) of the network key. Used only with WEP.
Some Wi-Fi adapters only allow the input of a network key in its hexadecimal format.
With WEP 64-bit encryption, the hexadecimal key is represented by 10 characters within the range 0 to 9 or a to f.
When WEP 128-bit encryption is used, the hexadecimal key is represented by 26 characters within the range 0 to 9 or a to f.

i

IP/ Internet Protocol

Internet Protocol is the main internetworking protocol used in the Internet.

IP Address

A four-byte number uniquely defining each host on a network, usually written in dotted-decimal notation with periods separating the bytes (for example, 134.177.244. 57).

m

MAC address

The Media Access Control address is a unique 48-bit identifier hardware address assigned to every network interface card according to the template xx:xx:xx:xx:xx:x x (with x=character within the range 0 to 9 or a to f).

Mbps

Megabits per second.

n

Netmask

Combined with the IP address, the IP Subnet Mask allows a device to know which other addresses are local to it, and which must be reached through a gateway or router.
A number that explains which part of an IP address comprises the network address and which part is the host address on that network. It can be expressed in dotted-decimal notation or as a number appended to the IP address.

Network key

Code enabling the encryption and decryption of the information exchanged between devices.

o

Open system

Mode for wireless communication without encryption.

r

RADIUS
Short for Remote Authentication Dial-In User Service, RADIUS is an authentication system.
Using RADIUS, you must enter your user name and password or certificates before gaining access to a network. This information is passed to a RADIUS server, which checks that the information is correct, and then authorizes access.

S

Securing a Wi-Fi network
Adding encryption to Wi-Fi communications

Shared KeyShared key =Pre-shared Key (PSK) = network key

SSID
See ESSID.

u

Upgrade
To replace existing software or firmware with a newer version.

W

WEPs
Wired Equivalent Privacy is a data encryption protocol for 802.11 wireless networks.
All wireless nodes and access points on the network are configured with a 64-bit or 128-bit Shared Key for data encryption.

Wi-Fi
A Commercial brand certifying interoperability for 802.11a/b/g wireless devices.

DECLARATION CE DE CONFORMITE

Nous déclarons que les produits satisfont aux dispositions de :
We declare that the products satisfy the provisions of :

La Directive 1999/5/CE du Parlement européen et du Conseil du 9 mars 1999 "R & TTE"

Sous réserve d'une utilisation conforme à sa destination et/ou d'une installation conforme aux normes en vigueur et/ou aux recommandations du constructeur

On condition that they are used in the manner intended and/or in accordance with the current installation standards and/or with the manufacturer's recommendations

La libération des canaux est sous la responsabilité de chaque pays. L'administrateur réseaux sans fil doit configurer le pays. Ainsi les canaux seront automatiquement en conformité avec les dispositions du pays

Channel availability depends on local country regulations. The wireless LAN system administrator must choose the correct country of operation. Channels are then automatically configured to comply with specified country's regulations.

Ces dispositions sont assurées pour la directive 1999/5/CEE par la conformité aux normes suivantes :
These provisions are ensured for directive 1999/5/CEE by conformity to the following standards:

EN 301 489-17

EN 301 489-1

EN 60669-2-1

EN 60950

EN 300 328

EN 301 893

LEGRAND SNC
World headquarters:
128, av. du Maréchal-de-Lattre-de-Tassigny
87045 Limoges Cedex - France
tél. : 05 55 06 87 87 +
télex : 580048 F
fax : 05 55 06 88 88

Technical support:
0810484848

07 8503 362 D