

USER GUIDE



Dual band Access Point
802.11a/b/g/n

Contents

1.1 / HOW TO ACCESS THE WEB-BASED INTERFACE	p. 4
1.2 / ENTERING THE CONFIGURATION PASSWORD	p. 5
1.3 / CONFIGURATION WIZARD	p. 6
1.4 / ACCESS POINT OVERVIEW	p. 7
1.5 / IP ADDRESS	p. 8
1.6 / ADMINISTRATION PASSWORD	p. 9
1.7 / FIRMWARE MANAGEMENT	p. 10
1.8 / CONFIGURATION MANAGEMENT	p. 11
1.9 / REBOOT/FULL RESET	p. 12
1.10 / MANAGEMENT INTERFACE	p. 13
1.11 / SNMP, UPnP & SYSLOG	p. 14
1.12 / TIME SETTINGS	p. 16
1.13 / ETHERNET INTERFACE	p. 18
1.14 / RADIO SETTINGS	p. 19
1.15 / WIRELESS NETWORKS	p. 21
1.15.1 / WIRELESS NETWORK/SECURITY/Open	p. 24
1.15.2 / WIRELESS NETWORK/SECURITY/Static WEP	p. 25
1.15.3 / WIRELESS NETWORK/SECURITY/WEP with 802.1x	p. 26
1.15.4 / WIRELESS NETWORK/SECURITY/Static WPA	p. 27
1.15.5 / WIRELESS NETWORK/SECURITY/Static WPA with 802.1x	p. 28
1.15.6 / WIRELESS NETWORK/SECURITY/Static WPA2	p. 29
1.15.7 / WIRELESS NETWORK/SECURITY/WPA2 with 802.1x	p. 30
1.15.8 / WIRELESS NETWORK/SECURITY/Static WPA or WPA2	p. 31
1.15.9 / WIRELESS NETWORK/SECURITY/WPA or WPA2 with 802.1x	p. 32
1.16 / WIRELESS NETWORK/GUEST ACCESS	p. 33
1.17 / RADIUS SETTINGS	p. 34
GLOSSARY	p. 36

Introduction

Rear Panel of the Access Point (AP)

The port to which an uplink network cable is connected is located on the rear panel of the Access Point. The power is supplied via twisted pair cable (Power over Ethernet standard IEEE 802.3af).

Front panel of the Access Point

LED (PWR): The power LED lights when the Access Point is powered on.

LED (WLAN): The LED blinks when the radio is activated.

Reset button: This button has two uses:

- A short press reboots the AP
- A long press (more than 5 seconds) resets the AP (to factory defaults)

Before configuring your device, please download the latest firmware from the following website : <http://www.wifi.legrandelectric.com> and update your device with this firmware.

1.1 / HOW TO ACCESS THE WEB-BASED INTERFACE

1. If your computer is operating with Windows

- XP

Check that the UPnP protocol is activated on your computer. If it is not, follow this procedure:

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

UPnP is now activated on your computer. When you click on the Network Neighbourhood icon on your desktop.

- Vista/7

- Click on Start
- Click on Computer
- Click on Network

A window opens displaying the Legrand AP detected using UPnP.

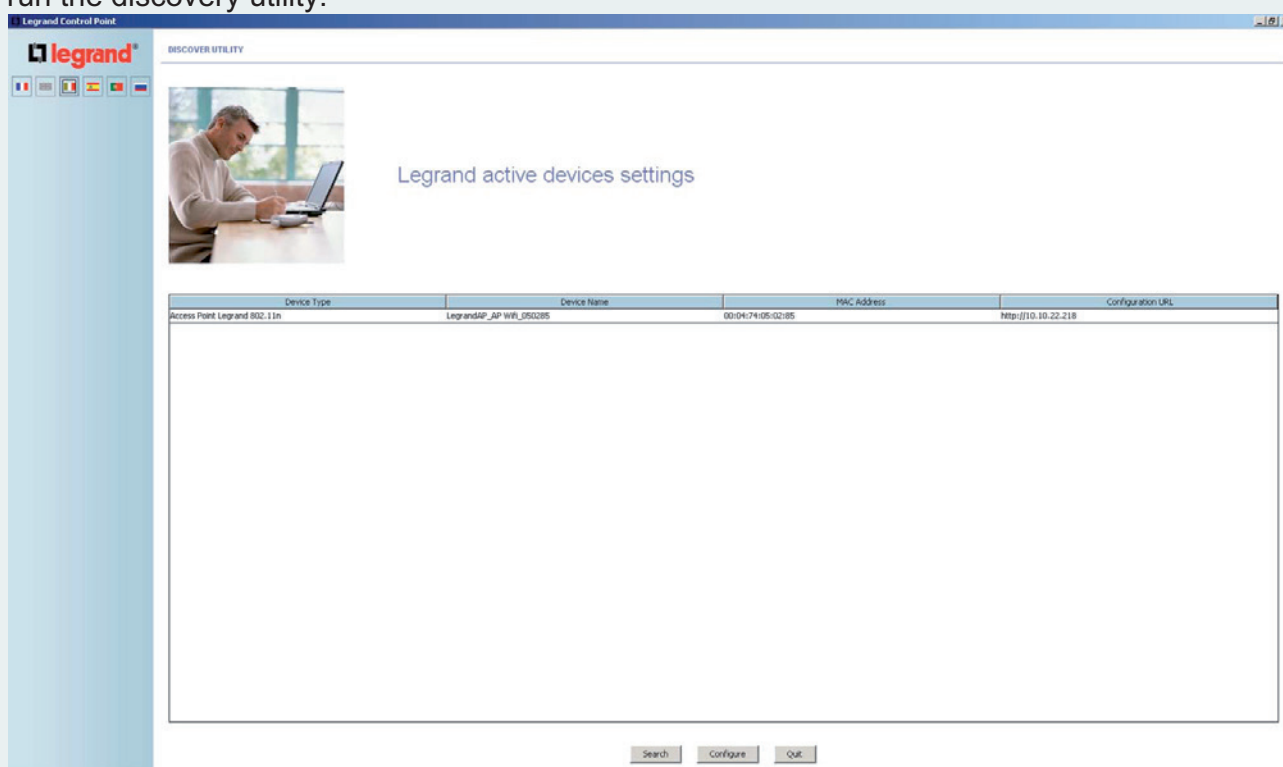
Double-click on one of the Access Points to access the web configuration interface.

2. If your computer is operating with another version of Windows or with MAC, Linux, Unix or another operating system

Use the CD-ROM to launch the Legrand Control Point discovery utility.

Insert the **CD-ROM SUPPLIED WITH THE ACCESS POINT (AP)**. This CD provides the tools you need to configure your wireless network.

The main menu will be displayed automatically on the screen. If the main menu does not open automatically, browse the contents of the CD-ROM using the Windows Explorer, then double-click on the index.html. From your web browser, click on "Launch Legrand Control Point from the CD" to run the discovery utility.

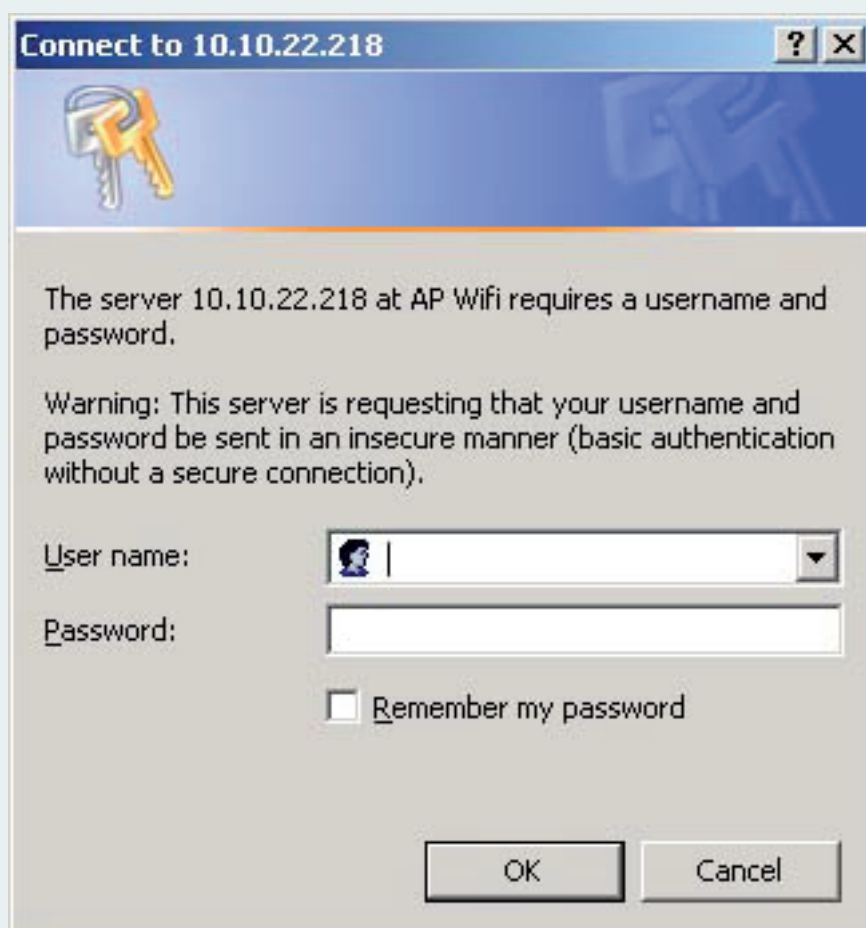


The list shows all the Legrand Access Points in your installation.

Select an Access Point and click on "Connect" to access the web configuration interface.

1.2 / ENTERING THE CONFIGURATION PASSWORD

The first time you connect to the management web interfaces, or following a full reset, you will not be asked to enter a password to configure the Access Point. It is strongly recommended that you password protect your Legrand Access Point, as this will make access to the management web interfaces 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 the web browser you use, a **Remember my password** dialogue box may appear if the management web interfaces are password-protected. Enabling this option means your browser will fill in the password automatically for you each time you subsequently connect to the management web interfaces.

Do not check this option if other people have access to your PC, as they could modify the Access Point configuration without having to provide the configuration password.

1.3 / CONFIGURATION WIZARD

CONFIGURATION WIZARD

Wi-Fi Access Point Settings

This page allows to quickly configure the most important parameters of your Access Point. It is only displayed as the starting page when your Access Point has not been configured yet. To manually go back to this page during the successive connections, click on Configuration Wizard in the main menu. On this page, you will be prompted for a wireless network name (SSID) to identify your networks to wireless clients that would like to connect to it. You will also be prompted for a secret WPA or WPA2 (802.11i) key, that will be required by any client to be allowed to connect to the wireless network. You must also provide an admin password, in order to prevent unauthorised users changing your Access Point's configuration. You can add a guest access wireless network by ticking the corresponding

[Click here to get manuals and latest firmwares from Internet](#)

Easy Configuration Setup

Choose a network name (SSID)

Choose your WPA key

Choose a new admin password

Retype the new admin password

AP Name

Add a guest access limited to an Internet access ☐

Apply

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

First enter your chosen network name (**Choose a network name (SSID)**).

In the **Choose your WPA key** field, select a wireless key (at least 8 characters long). This will have to be entered on all wireless devices to be connected to the wireless network.

In the **Choose a new admin password** field, enter your chosen password.

This password will be required to modify the configuration of your Access Point.

Click on **Apply & Save** to update and save this configuration.

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

AP name

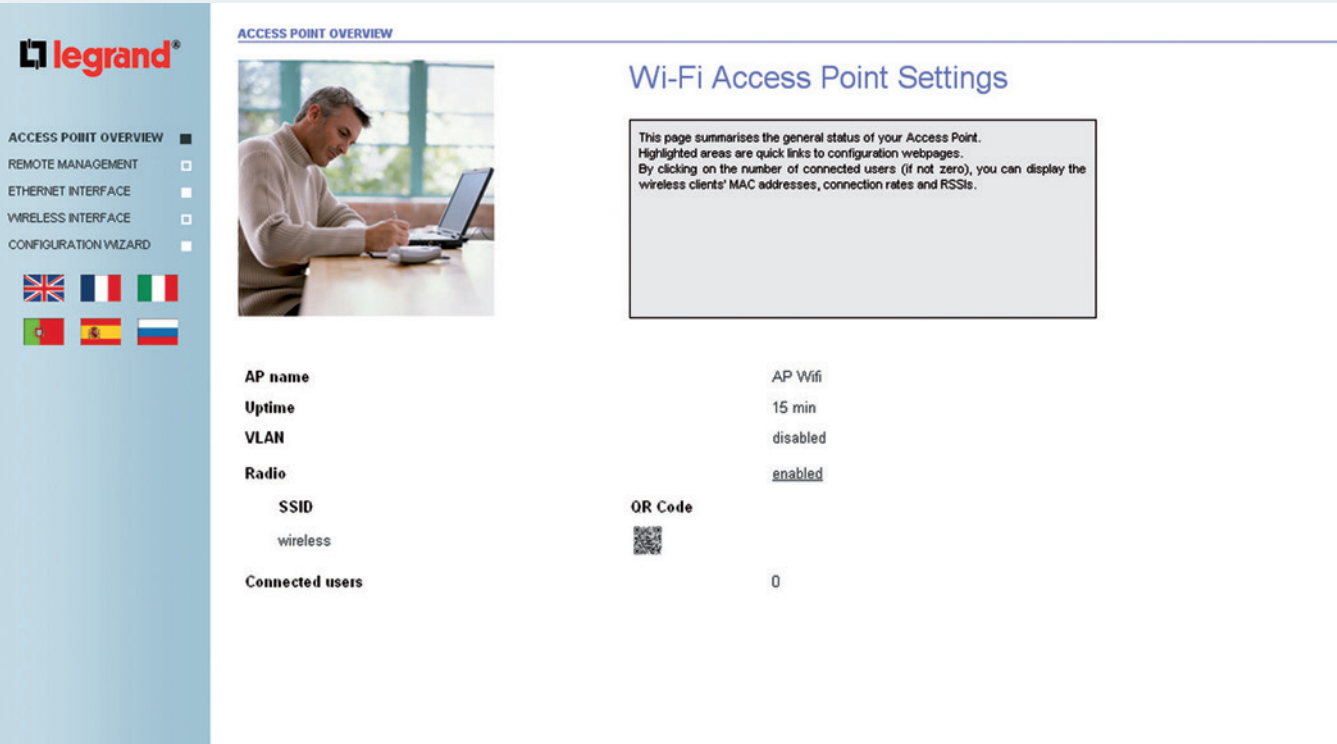
This name will help you to identify your Access Point.

When you select **Add a guest access limited to an Internet access**, you can define an open (hotspot) wireless network which will only provide access to the Internet. Enter the name of this limited-access network in the **Choose the guest access network name (SSID)** field.

When your configuration is complete, 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.

Your AP is now secure and ready to use. If you need to modify the advanced settings use the web interface menu.

1.4 / ACCESS POINT OVERVIEW



The screen gives an overview of the main information on the Legrand AP.

AP name	This name will identify your Access Point (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)
Radio	Status of the radio (Enabled/Disabled)
Connected users	Number of wireless clients currently connected

The detailed list of client PCs connected to the radio can be displayed by clicking on the number of connected users.

1.5 / IP ADDRESS

- ACCESS POINT OVERVIEW ☐
- REMOTE MANAGEMENT ☐
- IP ADDRESS ☒
- ADMIN PASSWORD ☐
- FIRMWARE MANAGEMENT ☐
- CONFIG MANAGEMENT ☐
- REBOOT/FULL RESET ☐
- MANAGEMENT INTERFACE ☐
- UPNP & SYSLOG ☐
- TIME SETTINGS ☐
- ETHERNET INTERFACE ☐
- WIRELESS INTERFACE ☐
- CONFIGURATION WIZARD ☐

REMOTE MANAGEMENT > IP ADDRESS

Wi-Fi Access Point Settings

This page contains information about access to the Access Point management webpages.
The AP Name field identifies your AP when you connect to it, as well as during the UPnP discovery.

You can choose the IP addressing for the AP on the network :

- Enabling dynamic addressing activates DHCP on the AP.
- Otherwise, a static IP address will need to be provided in IP address and Netmask fields. Default gateway and DNS server are optional parameters.

Management interface IP configuration

AP Name

AP Wifi

Allow management access on VLAN

☐ ID ☐ Native

IP addressing for AP management

☒ Dynamically retrieve an IP address (DHCP) ☐ Use the following IP address

☒ Use AUTO-IP with DHCP

☐ ID ☐ Native

☒ Dynamically retrieve an IP address (DHCP) ☐ Use the following IP address

☒ Enable AUTO-IP

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 necessary, one VLAN on the uplink port can be selected as the only way to access the management interface (for this, the VLANs must first be enabled, 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 use either Dynamic (DHCP) or Static (use the next IP address) IP addressing to manage the AP.

By default or after a full reset, the Access Point is set to use DHCP.

Toggle AUTO-IP in the absence of DHCP
If **Toggle AUTO-IP in the absence of DHCP** is selected, the AP returns to automatic 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. **The 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: Enter the static IP address for your Access Point.

Netmask: Enter the IP Netmask for your network.

Default gateway: Enter the default gateway IP address (used for any traffic beyond the local network)

DNS server: Enter your DNS IP address (optional).

After you have changed the settings on this page, click on **Apply** to confirm your changes.

1.6 / ADMINISTRATION PASSWORD

- ACCESS POINT OVERVIEW
- REMOTE MANAGEMENT
- IP ADDRESS
- ADMIN PASSWORD
- FIRMWARE MANAGEMENT
- CONFIG MANAGEMENT
- REBOOT/FULL RESET
- MANAGEMENT INTERFACE
- UPNP & SYSLOG
- TIME SETTINGS
- ETHERNET INTERFACE
- WIRELESS INTERFACE
- CONFIGURATION WIZARD

REMOTE MANAGEMENT > ADMIN PASSWORD

Wi-Fi Access Point Settings

This page allows you to change the password required to change the Access Point's configuration.

Entering an empty password is forbidden. Warning! Using the Configuration Wizard will override this password.

Admin password configuration setup

New Password

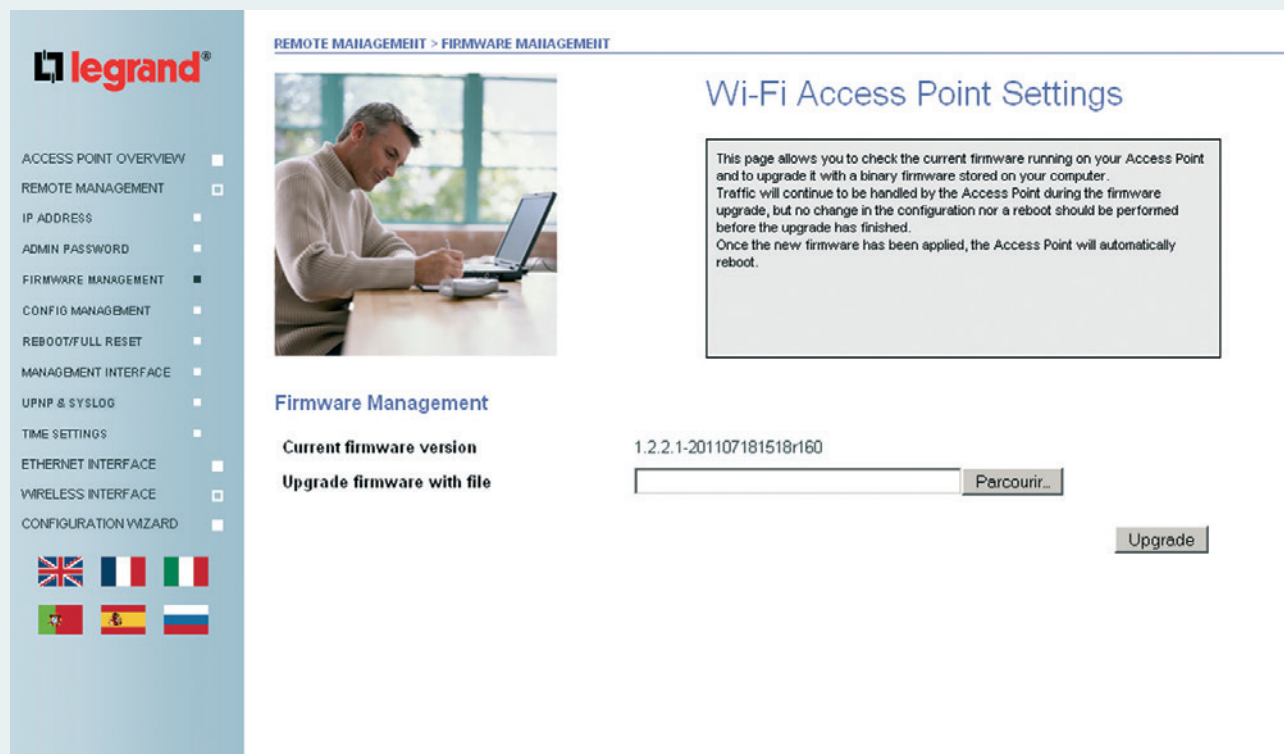
Confirm new Password

This page enables you to change the Access Point's configuration password. Enter the new password in both fields, and click on **Apply** to confirm the changes.

Important:

If you restore the Access Point's factory defaults your password settings will be erased. No password will be required for the web interface after a factory default reset.

1.7 / FIRMWARE MANAGEMENT



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

The firmware upgrade web page shows the current firmware version on the Access Point. Before upgrading the firmware on the Access Point, download the latest version from <http://www.wifi.legrandelectric.com>.

Press **Browse** to select a firmware file on your computer.

Then click on **Upgrade** to upgrade the firmware.

This takes a few minutes.

Note: When upgrading the firmware, do not interrupt the Web browser and do not power down your Access Point.

1.8 / CONFIGURATION MANAGEMENT

REMOTE MANAGEMENT > CONFIG MANAGEMENT

Wi-Fi Access Point Settings

This page allows you to backup the current configuration (as a text file), or to restore a previous configuration from a file stored on your PC. Once a configuration has been restored, the Access Point will automatically apply the new configuration.

Backup Config
Save a copy of current settings

Restore Config
Restore saved settings from a file

Backing up and restoring the configuration

The settings of the Access Point are saved in the AP.

This configuration can be backed up on the administrator's computer as a text file, using the **Backup** button.

This file can then be restored to the AP from the user's computer at a later stage: click on **Browse** to locate the file, then on the **Restore** button.

1.9 / REBOOT/FULL RESET

- ACCESS POINT OVERVIEW ☐
- REMOTE MANAGEMENT ☐
- IP ADDRESS ☐
- ADMIN PASSWORD ☐
- FIRMWARE MANAGEMENT ☐
- CONFIG MANAGEMENT ☐
- REBOOT/FULL RESET ☒
- MANAGEMENT INTERFACE ☐
- SNMP, UPnP & SYSLOG ☐
- TIME SETTINGS ☐
- ETHERNET INTERFACE ☐
- WIRELESS INTERFACE ☐
- CONFIGURATION WIZARD ☐

REMOTE MANAGEMENT > REBOOT/FULL RESET

Wi-Fi Access Point Settings

This page allows you to reboot your Access Point or to reset its settings to the factory defaults.
In factory default mode, the AP will start using DHCP or Auto-IP, announce itself via UPnP and directly show the Configuration Wizard on the first connection.

Default Config

Revert to factory default settings

Reboot Device

Reboot the Access Point

Default Config

To restore the Access Points factory default settings, click on **Restore default settings** (this is equivalent to a long press on the reset button).

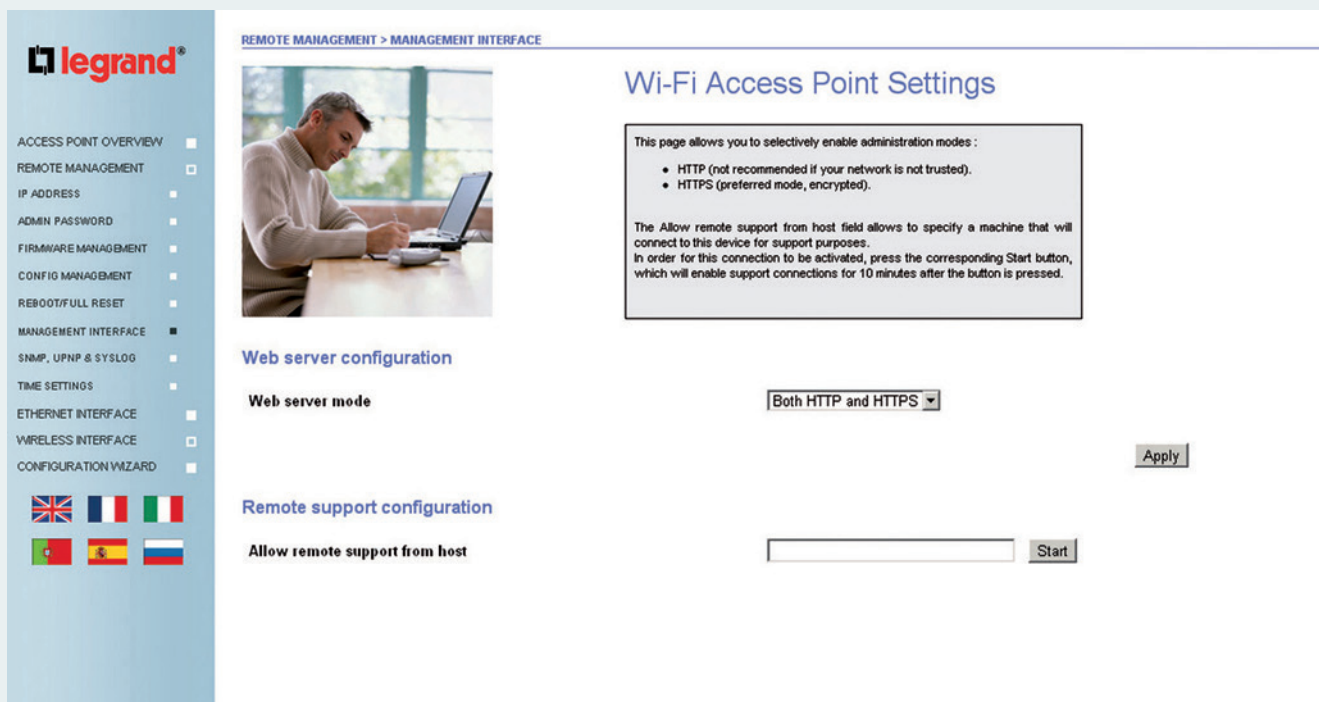
Reboot Device

Click on **Reboot** to reboot the AP.
This is equivalent to a short press on the reset button.

Important:

If you restore the Access Points factory defaults, all of your settings will be erased (password, security encryption, wireless and LAN settings, etc.) and replaced by the factory defaults (see Administration password section).

1.10 / MANAGEMENT INTERFACE



This page enables you to control the enabling/disabling of various methods of configuring the AP:

HTTPS only: enables management via a secure web management interface only (SSL encrypted HTTP transmission)

HTTP or HTTPS: enables management via HTTP or HTTPS

1.11 / SNMP, UPnP & SYSLOG

- ACCESS POINT OVERVIEW ☐
- REMOTE MANAGEMENT ☐
- IP ADDRESS ☐
- ADMIN PASSWORD ☐
- FIRMWARE MANAGEMENT ☐
- CONFIG MANAGEMENT ☐
- REBOOT/FULL RESET ☐
- MANAGEMENT INTERFACE ☐
- SNMP, UPnP & SYSLOG ☒
- TIME SETTINGS ☐
- ETHERNET INTERFACE ☐
- WIRELESS INTERFACE ☐
- CONFIGURATION WIZARD ☐

REMOTE MANAGEMENT > SNMP, UPnP & SYSLOG
Wi-Fi Access Point Settings

This page allows you to control the network services on your Access Point.

- SNMP can be enabled or disabled, and administrative parameters can be setup in this webpage.
- UPnP can be enabled or disabled. Note: disabling UPnP will not allow the discovery tool to automatically find your Access Point (use with caution). If UPnP is disabled and you don't know the IP address for your Access Point, you will need to perform a Factory default reset.
- Syslog can be enabled or disabled and controls the logs of the Access Point. If Enable network report is activated, the logs from the Access Point will be sent over the network to the machine specified in the field Syslog server IP address.

SNMP

SNMP service status ☒ Enable SNMP ☐ Disable SNMP

System Location

Contact

Community for read only access

Community for read/write access

UPnP/Bonjour

Service status ☒ Enable UPnP/Bonjour ☐ Disable UPnP/Bonjour

Syslog

Syslog service status ☒ Enable Syslog ☐ Disable Syslog Show log

Enable network report ☐ Enable network report ☒ Disable network report

Apply

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 inread and read/write to the AP.

UPnP/Bonjour

Select **Activate UPnP/Bonjour** to enable the AP to announce itself on the network using the UPnP/Bonjour protocols. By default, the protocols are activated to enable the Legrand AP detection utility to function.

By default, the UPnP is enabled to allow you to use **Legrand Control Point Discovery Utility**.

Syslog

To enable system logging, select **Enable Syslog** (enabled by default).

If you have chosen to manage the Access Points system logging remotely, select **Enable network report** and then select the IP address and UDP port of the device management machine in the **Syslog server IP address** and **Syslog server port** fields respectively. After you have changed the settings on this page, click on **Apply** to confirm your changes.

Show Log

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

- ACCESS POINT OVERVIEW
- REMOTE MANAGEMENT
- IP ADDRESS
- ADMIN PASSWORD
- FIRMWARE MANAGEMENT
- CONFIG MANAGEMENT
- REBOOT/FULL RESET
- MANAGEMENT INTERFACE
- SNMP, UPNP & SYSLOG
- TIME SETTINGS
- ETHERNET INTERFACE
- WIRELESS INTERFACE
- CONFIGURATION WIZARD

REMOTE MANAGEMENT > LOG

Wi-Fi Access Point Settings

This page allows you to see last 20 logs of the AP.
You can also download the entire log file on your PC.

Last 20 logs

```

Jan 1 00:00:07 AP Wifi user.warn : srvmgrd codehandle_telnetd: Starting telnet service
Jan 1 00:00:08 AP Wifi user.info kernel: br0: topology change detected, propagating
Jan 1 00:00:08 AP Wifi user.warn : srvmgrd : No password found in config file. No authentication requested for web interface
Jan 1 00:00:08 AP Wifi user.warn : srvmgrd : Starting httpd service
Jan 1 00:00:09 AP Wifi user.info kernel: br0: port 1(eth0) entering forwarding state
Jan 1 00:00:09 AP Wifi user.info kernel: br0: topology change detected, propagating
Jan 1 00:00:09 AP Wifi user.info kernel: br0: port 2(ath0) entering forwarding state
Jan 1 00:00:09 AP Wifi user.warn : srvmgrd : Bringing up management interface br0
Jan 1 00:00:09 AP Wifi user.warn : srvmgrd : Requesting IP address via DHCP on interface br0 (falling back to auto-IP if no answer)
Jan 1 00:00:10 AP Wifi user.warn : srvmgrd : Will launch udhcpd -b -i br0 -p /var/run/udhcpd.pid -s /etc/scripts/udhcpd/udhcpd-script -V Legrand
Jan 1 00:00:10 AP Wifi user.notice DHCP client: Got IP address 10.10.18.65
Jan 1 00:00:10 AP Wifi user.warn : srvmgrd /sbin/codehandle_mdnsd: Warning: No PID provided by PID file /var/run/mdnsd.pid
Jan 1 00:00:10 AP Wifi user.warn : srvmgrd : Enter stop_service: service_exec_path:/sbin/mdnsd service_pid: signal:15
Jan 1 00:00:11 AP Wifi user.warn : srvmgrd : Starting mdnsd service. Advertising with MAC address 00:04:74:05:02:85
Jan 1 00:00:11 AP Wifi user.warn : srvmgrd /sbin/codehandle_upnpd: Enter stop_service: service_exec_path:miniupnpd

```

[Back](#)
[Download full log file](#)

1.12 / TIME SETTINGS

Time Zone

In the menu select the time zone in which your AP is located.

If your zone does not appear in this list, select a location that is in the same time zone.

The default zone is GMT.

Configuration method

If you select Activate NTP, the Legrand access point will automatically synchronise with UTC/ GMT time using the NTP server specified in the NTP server field. In the Scheduling section, select the time ranges during which your Legrand access point will be inoperative. To do this, select the days of the week and a time range when the Wi-Fi will be activated.

- ACCESS POINT OVERVIEW
- REMOTE MANAGEMENT
- IP ADDRESS
- ADMIN PASSWORD
- FIRMWARE MANAGEMENT
- CONFIG MANAGEMENT
- REBOOT/FULL RESET
- MANAGEMENT INTERFACE
- SNMP, UPNP & SYSLOG
- TIME SETTINGS
- ETHERNET INTERFACE
- WIRELESS INTERFACE
- CONFIGURATION WIZARD

REMOTE MANAGEMENT > TIME SETTINGS

Wi-Fi Access Point Settings

This page allows you to set the current time on your Access Point. The Access Point's time will automatically be setup by the network if the NTP protocol is enabled and a NTP server is provisioned. The NTP time synchronisation is mandatory when the time scheduling feature is enabled.

Time settings

Time zone

Service status

Schedule

You must enabled NTP to use radio scheduling

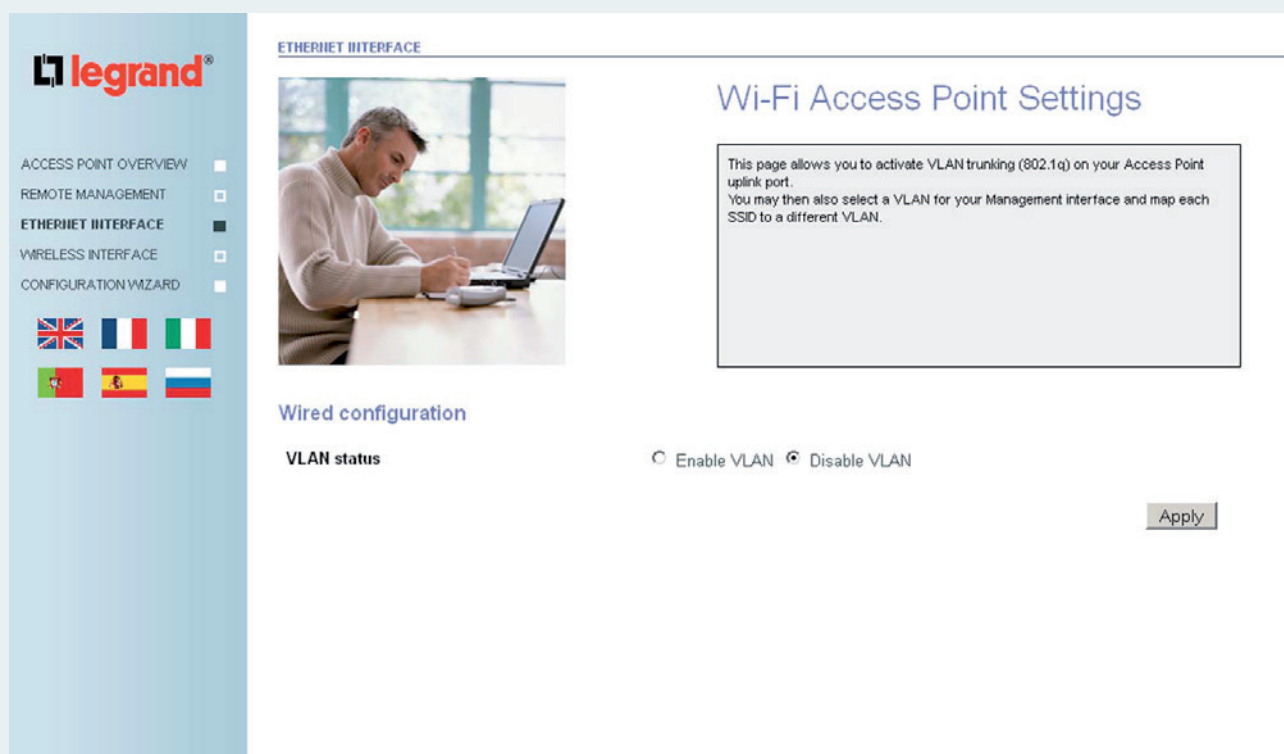
Europe/Paris

☐ Enable NTP
 ☒ Disable NTP

Apply

After you have changed the settings on this page, click on **Apply** to confirm your changes.

1.13 / ETHERNET INTERFACE



The screenshot shows the 'ETHERNET INTERFACE' configuration page. On the left is a sidebar with the Legrand logo and navigation links: ACCESS POINT OVERVIEW, REMOTE MANAGEMENT, ETHERNET INTERFACE (selected), WIRELESS INTERFACE, and CONFIGURATION WIZARD. Below these are flags for various languages. The main content area is titled 'Wi-Fi Access Point Settings' and contains a text box explaining that this page allows activating VLAN trunking (802.1q) on the uplink port. Below this, under 'Wired configuration', there is a 'VLAN status' section with two radio buttons: 'Enable VLAN' and 'Disable VLAN' (which is selected). An 'Apply' button is located at the bottom right of the configuration area.

Selecting **Enable VLAN** activates VLAN 802.1q trunking on the uplink Ethernet interface. The default is **Disable VLAN**, which means that no VLAN tagging will be used. In order to achieve an adequate security level, VLANs should be used to isolate traffic when several network names (SSIDs) are activated on the radio.

After you have changed the settings on this page, click on **Apply** to confirm your changes.

1.14 / RADIO SETTINGS

- ACCESS POINT OVERVIEW
- REMOTE MANAGEMENT
- IP ADDRESS
- ADMIN PASSWORD
- FIRMWARE MANAGEMENT
- CONFIG MANAGEMENT
- REBOOT/FULL RESET
- MANAGEMENT INTERFACE
- SNMP, UPNP & SYSLOG
- TIME SETTINGS
- ETHERNET INTERFACE
- WIRELESS INTERFACE
- RADIO SETTINGS
- WIRELESS NETWORKS
- RADIUS SETTINGS
- CONFIGURATION WIZARD

WIRELESS INTERFACE > RADIO SETTINGS

Wi-Fi Access Point Settings

This page allows you to control parameters for your Access Point radio interfaces :

- Enabling or disabling the radio
- Selecting the RF transmit power level (in dBm)
- Choosing the wireless channel on which your Access Point operates (which should be as far as possible from neighbouring wireless networks).

General settings

Country FRANCE

Radio settings

Radio status ☒ Enable radio ☐ Disable radio

Operating mode 802.11bg, 802.11n

Transmit power 100%

Preamble Short

Channel Auto

Channel width 20/40HT

Guard interval ☒ Short ☐ Long

Frame aggregation ☒ Enabled ☐ Disabled

Apply

The Legrand AP integrates a wireless radio that can operate at 2.4 GHz or 5 GHz.

The radio can be enabled/disabled (in the **Radio status** field).

The following settings are available:

- Mode is used to select the frequency band on which the radio is to operate: 802.11bg, 802.11n on 2.4 GHz and 802.11a, 802.11n on 5 GHz (in the **Mode** field).
- The radio transmission power can be adjusted on the radio (**Transmit power** field).
- The preamble type can be adjusted in the **Preamble** field (recommended value: **Auto**).

- In the **Channel** field, enter the desired radio transmission channel (recommended value: **Auto**).

- The channel width can be adjusted in the **Channel width** field (recommended value: 20/40HT).

- The guard interval can be adjusted in the **Guard interval** field (recommended value: **Short**).

- The link aggregation can be adjusted in the **Aggregation** field (recommended value: **Enabled**).

Country: Select in this field the country in which the Access Point is installed in order to comply with the local radio regulations.

Note: The available radio channels depend on the value of the "Country" field.

2.4 GHz 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

5 GHz wireless radio frequency channels

Channel	Frequency
36	5.180 GHz
38	5.190 GHz
40	5.200 GHz
42	5.210 GHz
44	5.220 GHz
46	5.230 GHz
48	5.240 GHz
52	5.260 GHz
56	5.280 GHz
60	5.300 GHz
64	5.320 GHz
100	5.500 GHz
104	5.520 GHz
108	5.540 GHz
112	5.560 GHz
116	5.580 GHz
120	5.600 GHz
124	5.620 GHz
128	5.640 GHz
132	5.660 GHz
136	5.680 GHz
140	5.700 GHz
149	5.745 GHz
153	5.765 GHz
157	5.785 GHz
161	5.805 GHz
165	5.825 GHz

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

After you have changed the settings on this page, click on **Apply** to confirm your changes.

1.15 / WIRELESS NETWORKS

legrand

ACCESS POINT OVERVIEW ☐
 REMOTE MANAGEMENT ☐
 ETHERNET INTERFACE ☐
 WIRELESS INTERFACE ☐
 RADIO SETTINGS ☐
 WIRELESS NETWORKS ☒
 RADIUS SETTINGS ☐
 CONFIGURATION WIZARD ☐

UK FR IT ES PT RU

WIRELESS INTERFACE > WIRELESS NETWORKS

Wi-Fi Access Point Settings

This page provides you an overview of the current wireless networks :

- their SSID
- the type of radio on which this wireless network is broadcast.
- optionally the VLAN it is mapped to.

You can Edit or delete each wireless network by pressing on the corresponding button.

Wireless network configuration

SSID	Type	Action
wireless	802.11bg, 802.11n	Edit Delete

This page gives you a list of the **wireless networks (SSIDs)** that are already configured.

Use the **Edit** button to modify the configurations of the corresponding SSIDs.

Use the **Delete** button to erase the corresponding **SSID**.

Use the **Add** button to add a new **SSID** (see next page).

Use the **Add Guest Access** button to add a network for your guests who will only have access to the Internet. Only one guest-access wireless network can be created (see page 33).

- ACCESS POINT OVERVIEW ☐
- REMOTE MANAGEMENT ☐
- ETHERNET INTERFACE ☐
- WIRELESS INTERFACE ☐
- RADIO SETTINGS ☐
- WIRELESS NETWORKS ☒
- RADIUS SETTINGS ☐
- CONFIGURATION WIZARD ☐

WIRELESS INTERFACE > WIRELESS NETWORKS

Wi-Fi Access Point Settings

This page allows you to control the parameters for the wireless network (initial SSID).
You can specify a network name (SSID) displayed to clients when searching for a wireless network (the SSID should be unique in the coverage area of your Access Point(s)).
This network can then be specifically enabled on each radio interface.
For this wireless network you can choose between the supported Encryption types (sorted from the weakest to the strongest encryption). In order to select the encryption, choose the best available encryption also supported on all the wireless clients you would like to allow on your network (WPA or WPA2 for example).
802.1x encryption types require an additional authentication Radius server (see

Wireless network configuration

Network name (SSID)	wireless
Encryption type	Open
Associate to VLAN	
Hide SSID	☐ Hide SSID
Beacon interval	100 ms
Ignore broadcast probe	☐ Ignore broadcast probe
DTIM period	1 ms
802.11h	☐ Enable 802.11h
WMM	☐ Enable WMM

Network name (SSID)

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

Encryption type

Choose an 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. WPA2 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

Select this box to prevent the AP from broadcasting the SSID for this network.

Note: *This will force users to enter the SSID for this wireless network manually on their computers, and may even prevent some wireless clients from connecting. By default this field is not selected.*

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

Enable this option to prevent the AP from responding to broadcast scanning from wireless devices (this makes the wireless network less visible to scanning tools).

DTIM period (Delivery Traffic Indication Message)

Specifies at what beacon frequency a DTIM indication will be included (enables devices in power save mode to wake up).

The default value of 1 should be suitable for most installations.

802.11h

Select this option to make the AP comply with the IEEE 802.11h standard (European standard on radar avoidance and power saving). The remaining wireless network fields depend on the type of encryption selected and are detailed by encryption type in the following sections.

WMM

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

1.15.1 / WIRELESS NETWORK/SECURITY/Open

- ACCESS POINT OVERVIEW ☐
- REMOTE MANAGEMENT ☐
- ETHERNET INTERFACE ☐
- WIRELESS INTERFACE ☐
- RADIO SETTINGS ☐
- WIRELESS NETWORKS ☒
- RADIUS SETTINGS ☐
- CONFIGURATION WIZARD ☐

WIRELESS INTERFACE > WIRELESS NETWORKS

This page allows you to control the parameters for the wireless network (initial SSID).

You can specify a network name (SSID) displayed to clients when searching for a wireless network (the SSID should be unique in the coverage area of your Access Point(s)).

This network can then be specifically enabled on each radio interface.

For this wireless network you can choose between the supported Encryption types (sorted from the weakest to the strongest encryption). In order to select the encryption, choose the best available encryption also supported on all the wireless clients you would like to allow on your network (WPA or WPA2 for example).

802.1x encryption types require an additional authentication Radius server (see

Wi-Fi Access Point Settings

Wireless network configuration

Network name (SSID)	wireless
Encryption type	Open
Associate to VLAN	
Hide SSID	☐ Hide SSID
Beacon interval	100 ms
Ignore broadcast probe	☐ Ignore broadcast probe
DTIM period	1 ms
802.11h	☐ Enable 802.11h
WMM	☐ Enable WMM

Encryption type

Select **Open**.

In this mode, any device 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

- ACCESS POINT OVERVIEW ☐
- REMOTE MANAGEMENT ☐
- ETHERNET INTERFACE ☐
- WIRELESS INTERFACE ☐
- RADIO SETTINGS ☐
- WIRELESS NETWORKS ☒
- RADIUS SETTINGS ☐
- CONFIGURATION WIZARD ☐

WIRELESS INTERFACE > WIRELESS NETWORKS
Wi-Fi Access Point Settings

This page allows you to control the parameters for the wireless network (initial SSID).

You can specify a network name (SSID) displayed to clients when searching for a wireless network (the SSID should be unique in the coverage area of your Access Point(s)).

This network can then be specifically enabled on each radio interface.

For this wireless network you can choose between the supported Encryption types (sorted from the weakest to the strongest encryption). In order to select the encryption, choose the best available encryption also supported on all the wireless clients you would like to allow on your network (WPA or WPA2 for example).

802.1x encryption types require an additional authentication Radius server (see

Wireless network configuration

Network name (SSID)	wireless
Encryption type	Static WEP
Key length	☐ 64 bits ☐ 128 bits
Key format	☐ ASCII ☐ Hexadecimal
Key	
Retype key	
Associate to VLAN	
Hide SSID	☐ Hide SSID
Beacon interval	100 ms
Ignore broadcast probe	☐ Ignore broadcast probe
DTIM period	1 ms
802.11h	☐ Enable 802.11h
WMM	☐ Enable WMM

Encryption type
Select **Static WEP**.

Key
Enter the WEP key to encrypt the data on your wireless network.
WEP keys can be 64 or 128 bits long and can be entered in ASCII or 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 device that will connect to your wireless network.

1.15.3 / WIRELESS NETWORK/SECURITY/WEP with 802.1x

- ACCESS POINT OVERVIEW ☐
- REMOTE MANAGEMENT ☐
- ETHERNET INTERFACE ☐
- WIRELESS INTERFACE ☐
- RADIO SETTINGS ☐
- WIRELESS NETWORKS ☒
- RADIUS SETTINGS ☐
- CONFIGURATION WIZARD ☐

WIRELESS INTERFACE > WIRELESS NETWORKS

Wi-Fi Access Point Settings

This page allows you to control the parameters for the wireless network (initial SSID).

You can specify a network name (SSID) displayed to clients when searching for a wireless network (the SSID should be unique in the coverage area of your Access Point(s)).

This network can then be specifically enabled on each radio interface.

For this wireless network you can choose between the supported Encryption types (sorted from the weakest to the strongest encryption). In order to select the encryption, choose the best available encryption also supported on all the wireless clients you would like to allow on your network (WPA or WPA2 for example).

802.1x encryption types require an additional authentication Radius server (see

Wireless network configuration

Network name (SSID)

Encryption type

Associate to VLAN

Hide SSID

Beacon interval

Ignore broadcast probe

DTIM period

802.11h

WMM

wireless

WEP with 802.1x

☐ Hide SSID

ms

☐ Ignore broadcast probe

ms

☐ Enable 802.11h

☐ Enable WMM

Restore

Apply

Back

Encryption type

Select **WEP with 802.1x**.

Use WEP as the encryption mode and 802.1x (RADIUS authentication) as the station authentication protocol.

No key is required 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

- ACCESS POINT OVERVIEW ☐
- REMOTE MANAGEMENT ☐
- ETHERNET INTERFACE ☐
- WIRELESS INTERFACE ☐
- RADIO SETTINGS ☐
- WIRELESS NETWORKS ☒
- RADIUS SETTINGS ☐
- CONFIGURATION WIZARD ☐

WIRELESS INTERFACE > WIRELESS NETWORKS

Wi-Fi Access Point Settings

This page allows you to control the parameters for the wireless network (initial SSID).

You can specify a network name (SSID) displayed to clients when searching for a wireless network (the SSID should be unique in the coverage area of your Access Point(s)).

This network can then be specifically enabled on each radio interface.

For this wireless network you can choose between the supported Encryption types (sorted from the weakest to the strongest encryption). In order to select the encryption, choose the best available encryption also supported on all the wireless clients you would like to allow on your network (WPA or WPA2 for example).

802.1x encryption types require an additional authentication Radius server (see

Wireless network configuration

Network name (SSID)	wireless
Encryption type	Static WPA
Passphrase	
Retype passphrase	
Associate to VLAN	
Hide SSID	☐ Hide SSID
Beacon interval	100 ms
Ignore broadcast probe	☐ Ignore broadcast probe
DTIM period	1 ms
802.11h	☐ Enable 802.11h
WMM	☐ Enable WMM

Encryption type
Select **Static WPA**.

This encryption, which is stronger than WEP and WPA, is also called WPA-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 WPA passphrase on each device that will connect to your wireless network.

1.15.5 / WIRELESS NETWORK/SECURITY/Static WPA with 802.1x

- ACCESS POINT OVERVIEW ☐
- REMOTE MANAGEMENT ☐
- ETHERNET INTERFACE ☐
- WIRELESS INTERFACE ☐
- RADIO SETTINGS ☐
- WIRELESS NETWORKS ☒
- RADIUS SETTINGS ☐
- CONFIGURATION WIZARD ☐

WIRELESS INTERFACE > WIRELESS NETWORKS

Wi-Fi Access Point Settings

This page allows you to control the parameters for the wireless network (initial SSID).

You can specify a network name (SSID) displayed to clients when searching for a wireless network (the SSID should be unique in the coverage area of your Access Point(s)).

This network can then be specifically enabled on each radio interface.

For this wireless network you can choose between the supported Encryption types (sorted from the weakest to the strongest encryption). In order to select the encryption, choose the best available encryption also supported on all the wireless clients you would like to allow on your network (WPA or WPA2 for example).

802.1x encryption types require an additional authentication Radius server (see

Wireless network configuration

Network name (SSID)	wireless
Encryption type	WPA with 802.1x
Associate to VLAN	
Hide SSID	☐ Hide SSID
Beacon interval	100 ms
Ignore broadcast probe	☐ Ignore broadcast probe
DTIM period	1 ms
802.11h	☐ Enable 802.11h
WMM	☐ Enable WMM

Encryption type
Select **WPA with 802.1x**.

Use WPA as the encryption mode and 802.1x (RADIUS authentication) as the station authentication protocol.
No key is required 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

- ACCESS POINT OVERVIEW ☐
- REMOTE MANAGEMENT ☐
- ETHERNET INTERFACE ☐
- WIRELESS INTERFACE ☐
- RADIO SETTINGS ☐
- WIRELESS NETWORKS ☒
- RADIUS SETTINGS ☐
- CONFIGURATION WIZARD ☐

WIRELESS INTERFACE > WIRELESS NETWORKS

Wi-Fi Access Point Settings

This page allows you to control the parameters for the wireless network (initial SSID). You can specify a network name (SSID) displayed to clients when searching for a wireless network (the SSID should be unique in the coverage area of your Access Point(s)). This network can then be specifically enabled on each radio interface. For this wireless network you can choose between the supported Encryption types (sorted from the weakest to the strongest encryption). In order to select the encryption, choose the best available encryption also supported on all the wireless clients you would like to allow on your network (WPA or WPA2 for example). 802.1x encryption types require an additional authentication Radius server (see

Wireless network configuration

Network name (SSID)	wireless
Encryption type	Static WPA2
Passphrase	
Retype passphrase	
Associate to VLAN	
Hide SSID	☐ Hide SSID
Beacon interval	100 ms
Ignore broadcast probe	☐ Ignore broadcast probe
DTIM period	1 ms
802.11h	☐ Enable 802.11h
WMM	☐ Enable WMM

Encryption type
Select **Static WPA2**.

This encryption, which is stronger than WEP and WPA, is 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 device that will connect to your wireless network.

1.15.7 / WIRELESS NETWORK/SECURITY/WPA2 with 802.1x

- ACCESS POINT OVERVIEW ☐
- REMOTE MANAGEMENT ☐
- ETHERNET INTERFACE ☐
- WIRELESS INTERFACE ☐
- RADIO SETTINGS ☐
- WIRELESS NETWORKS ☒
- RADIUS SETTINGS ☐
- CONFIGURATION WIZARD ☐

WIRELESS INTERFACE > WIRELESS NETWORKS

Wi-Fi Access Point Settings

This page allows you to control the parameters for the wireless network (initial SSID).
You can specify a network name (SSID) displayed to clients when searching for a wireless network (the SSID should be unique in the coverage area of your Access Point(s)).
This network can then be specifically enabled on each radio interface.
For this wireless network you can choose between the supported Encryption types (sorted from the weakest to the strongest encryption). In order to select the encryption, choose the best available encryption also supported on all the wireless clients you would like to allow on your network (WPA or WPA2 for example).
802.1x encryption types require an additional authentication Radius server (see

Wireless network configuration

Network name (SSID)

Encryption type

Associate to VLAN

Hide SSID

Beacon interval

Ignore broadcast probe

DTIM period

802.11h

WMM

wireless

WPA2 with 802.1x

☐
Hide SSID

ms

☐
Ignore broadcast probe

ms

☐
Enable 802.11h

☐
Enable WMM

Restore

Apply

Back

Encryption type

Select **WPA2 with 802.1x**.

Use WPA2 as the encryption mode and 802.1x (RADIUS authentication) as the station authentication protocol.

No key is required in this encryption mode, as the key will be dynamically provided by an external RADIUS server (see RADIUS section).

30

USER GUIDE FOR LEGRAND
DUAL BAND ACCESS POINT

1.15.8 / WIRELESS NETWORK/SECURITY/Static WPA or WPA2

- ACCESS POINT OVERVIEW ☐
- REMOTE MANAGEMENT ☐
- ETHERNET INTERFACE ☐
- WIRELESS INTERFACE ☐
- RADIO SETTINGS ☐
- WIRELESS NETWORKS ☒
- RADIUS SETTINGS ☐
- CONFIGURATION WIZARD ☐

WIRELESS INTERFACE > WIRELESS NETWORKS
Wi-Fi Access Point Settings

This page allows you to control the parameters for the wireless network (initial SSID).

You can specify a network name (SSID) displayed to clients when searching for a wireless network (the SSID should be unique in the coverage area of your Access Point(s)).

This network can then be specifically enabled on each radio interface.

For this wireless network you can choose between the supported Encryption types (sorted from the weakest to the strongest encryption). In order to select the encryption, choose the best available encryption also supported on all the wireless clients you would like to allow on your network (WPA or WPA2 for example).

802.1x encryption types require an additional authentication Radius server (see

Wireless network configuration

Network name (SSID)	wireless
Encryption type	Static WPA or WPA2
Passphrase	
Retype passphrase	
Associate to VLAN	
Hide SSID	☐ Hide SSID
Beacon interval	100 ms
Ignore broadcast probe	☐ Ignore broadcast probe
DTIM period	1 ms
802.11h	☐ Enable 802.11h
WMM	☐ Enable WMM

Encryption type
Select **Static WPA or WPA2**.

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

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

- ACCESS POINT OVERVIEW ☐
- REMOTE MANAGEMENT ☐
- ETHERNET INTERFACE ☐
- WIRELESS INTERFACE ☐
- RADIO SETTINGS ☐
- WIRELESS NETWORKS ☒
- RADIUS SETTINGS ☐
- CONFIGURATION WIZARD ☐

WIRELESS INTERFACE > WIRELESS NETWORKS

Wi-Fi Access Point Settings

This page allows you to control the parameters for the wireless network (initial SSID).
 You can specify a network name (SSID) displayed to clients when searching for a wireless network (the SSID should be unique in the coverage area of your Access Point(s)).
 This network can then be specifically enabled on each radio interface.
 For this wireless network you can choose between the supported Encryption types (sorted from the weakest to the strongest encryption). In order to select the encryption, choose the best available encryption also supported on all the wireless clients you would like to allow on your network (WPA or WPA2 for example).
 802.1x encryption types require an additional authentication Radius server (see

Wireless network configuration

Network name (SSID)	wireless
Encryption type	WPA or WPA2 with 802.1x
Associate to VLAN	
Hide SSID	☐ Hide SSID
Beacon interval	100 ms
Ignore broadcast probe	☐ Ignore broadcast probe
DTIM period	1 ms
802.11h	☐ Enable 802.11h
WMM	☐ Enable WMM

Encryption type

Select **WPA or WPA2 with 802.1x**.

Use WPA or WPA2 as the encryption mode and 802.1x (RADIUS authentication) as the station authentication protocol. No key is required 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 can connect to the wireless network.

1.16 / WIRELESS NETWORK/GUEST ACCESS

- ACCESS POINT OVERVIEW
- REMOTE MANAGEMENT
- IP ADDRESS
- ADMIN PASSWORD
- FIRMWARE MANAGEMENT
- CONFIG MANAGEMENT
- REBOOT/FULL RESET
- MANAGEMENT INTERFACE
- UPNP & SYSLOG
- TIME SETTINGS
- ETHERNET INTERFACE
- WIRELESS INTERFACE
- RADIO SETTINGS
- WIRELESS NETWORKS
- RADIUS SETTINGS
- CONFIGURATION WIZARD

WIRELESS INTERFACE > WIRELESS NETWORKS

Wi-Fi Access Point Settings

This page allows you to control the parameters for the guest access wireless network. The default restricted addresses specified by RFC1918 are (private address): 10.0.0.0/8, 172.16.0.0/12 and 192.168.0.0/16. The added restricted is your network address according to your access point configuration.

You can specify a network name (SSID) displayed to clients when searching for a wireless network (the SSID should be unique in the coverage area of your Access Point(s)).

This network can then be specifically enabled on each radio interface.

For this wireless network you can choose between the supported Encryption types (sorted from the weakest to the strongest encryption). In order to select the encryption, choose the best available encryption also supported on all the wireless clients you would like to allow on your network (WPA or WPA2 for

Wireless network configuration

Network name (SSID)

Encryption type Open

Associate to VLAN

Hide SSID ☐

Beacon interval 100 ms

Ignore broadcast probe ☐

DTIM period 1 ms

802.11h ☐

WMM ☐

☐ Hide SSID

☐ Ignore broadcast probe

☐ Enable 802.11h

☐ Enable WMM

Blocked private networks, specified by RFC

Network IP address	Netmask	Filtered
10 . 0 . 0 . 0	255 . 0 . 0 . 0	☒
172 . 16 . 0 . 0	255 . 240 . 0 . 0	☒
192 . 168 . 0 . 0	255 . 255 . 0 . 0	☒

Blocked networks

Network IP address	Netmask	Filtered
10 . 10 . 16 . 0	255 . 255 . 248 . 0	☒
. . .	. . .	☐

Restore Apply Back

On this page, in addition to the conventional wireless network settings described above, you can configure the IP address to which this SSID will not be permitted to access. By default, the private networks described in RFC 1918 are filtered automatically. You can then filter up to four more networks (IP address ranges). The subnetwork on which the access point is located is automatically detected and automatically filled-in .

1.17 / RADIUS SETTINGS

- ACCESS POINT OVERVIEW ☐
- REMOTE MANAGEMENT ☐
- ETHERNET INTERFACE ☐
- WIRELESS INTERFACE ☐
- RADIO SETTINGS ☐
- WIRELESS NETWORKS ☐
- RADIUS SETTINGS ☒
- CONFIGURATION WIZARD ☐

WIRELESS INTERFACE > RADIUS SETTINGS

Wi-Fi Access Point Settings

This page allows you to interface with an external Radius server for authentication.

802.1x networks will request an authentication to your clients prior to allowing them to access your network. Note: see the Wireless Networks webpage to activate 802.1x on a network (click on Edit and use 802.1x in the Encryption Type). Any EAP authentication method is supported by your Access Point.

The accept/reject decision for each client will be performed by the Radius server directly (no password/key is then stored on the Access Point, in 802.1x mode). The Authentication server fields allow you to specify which Radius server will perform client authentication. The Accounting server fields allow you to specify which Radius server will perform connection accounting.

General Radius settings

Reauthentication period

Authentication server

Server IP address . . .

Server port

Shared secret

Accounting server

Server IP address . . .

Server port

Shared secret

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 how often (in 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 port on the RADIUS server.

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' accounts.

Accounting server port

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

Shared secret

This field contains the shared secret between the wireless Access Point and the accounting server.

After you have changed the settings on this page, click on **Apply** to confirm your changes.

RESTORING THE FACTORY DEFAULT CONFIGURATION

Using the Reset button

If an issue with your Access Point's configuration prevents you from reconnecting to its management interface, a factory default reset will be needed.

To restore the factory configuration settings, use the **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 AP will reboot (restart).

This has the same effect as power cycling the AP or pressing the **Apply** button facing Reboot Access Point in the Reboot/Full reset menu.

- **Reset to factory defaults.** If the reset button is pressed and held down for more than 5 seconds, the AP will reboot in its factory configuration.

Default factory settings

When you start the initial configuration of your Legrand Access Point, the factory settings are as follows:

Password	None
Access Point Name	AP Wifi
IP Address	DHCP then auto-IP
VLANs	Disabled
Wireless network	Disabled
2.4 GHz Radio Frequency Channel	Auto
Security mode	Open
NTP	Disabled
Syslog	Disabled
Radius settings	None
UPnP/Bonjour	Enabled

SPECIFICATIONS

Standards	IEEE 802.11a, IEEE 802.11g, IEEE 802.11b, IEEE 802.11n, IEEE 802.3af
Ethernet Ports	One 10/100 RJ-45 port for connection to the backbone network (uplink port)
Reset button	One reboot/full reset button
Wiring	CAT5 UTP Ethernet cable or better
LED	Power, WLAN
Power supply	Power over Ethernet (802.3af) POE
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.

802.1x
802.1x defines the port-based network access control used to provide authenticated network access and automated management of the data encryption key. 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 54 Mbps wireless networks using orthogonal frequency division multiplexing (OFDM) technology and operating in the 5 GHz radio spectrum.

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

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

802.11i
The IEEE 802.11i standard, also known as WPA2, is an amended version of the 802.11 standard specifying security mechanisms for wireless networks.

802.11n
The IEEE 802.11n standard must enable a theoretical data rate of up to 270 Mbps or 300 Mbps to be reached in the 2.4 GHz or 5 GHz frequency bands respectively.

a

AP
Access Point

c

Channel
Subdivision of
the Wi-Fi band

Centrino
Chipset devel-
oped by Intel for
mobile comput-
ing, in particular
laptops, incorpo-
rating wireless
adaptors.

**Configuration
password**
Password need-
ed to change
the Legrand
Access Point
configuration
(channel, SSID,
encryption).
The configura-
tion password is
requested when
you connect to
the manage-
ment interface.

d

DHCP
(Dynamic Host
Configuration
Protocol)
An Ethernet pro-
tocol specifying
how a central-
ised DHCP serv-
er can assign
the network
configuration to
multiple clients.
The informa-
tion assigned
includes IP
addresses, DNS
addresses, and
gateway (router)
addresses.

e

Encryption
Encoding of
information
exchanged
between two
wireless devic-
es to make
them unintelligi-
ble to any other
device that
does not have
the encryp-
tion key/pass-
phrase.

ESSID (also
called SSID)
The Extended
Service Set
Identification
(ESSID) is a
32-character
(maximum)
alphanumeric
key which iden-
tifies the wire-
less LAN.

Ethernet
The 802.3 IEEE
standard net-
work protocol
that specifies
communication
over twisted
pairs.

f

Firmware

Software that is present in the flash memory of the Access Point. It is retained even when the device is turned off.

g

Gateway

(passerelle applicative)

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

h

Hexadecimal key

Representation in hexadecimal (computing) format of the network key; only used with WEP. Some Wi-Fi adaptors only allow the input of a network key in its hexadecimal format. In 64-bit WEP encryption, the hexadecimal key is made up of 10 characters between 0 and 9 or between A and F. In 128-bit WEP encryption, the hexadecimal key is made up of 26 characters between 0 and 9 or between A and F.

i

Internet Protocol (IP)

The Internet Protocol (IP) is the main inter-networking protocol used by the Internet.

IP Address

A four-byte number uniquely defining each host on a network, usually written in dotted decimal notation with full stops separating the bytes (for example, 134.177.244.57).

m

MAC address

The MAC address is a unique 48-bit hardware identification address assigned to each network interface card in the format xx:xx:xx:xx:xx:x (x being a character between 0 and 9 or between A and F).

Mbps

Megabits per second.

n

Netmask

Combined with the IP address, the IP Subnet Mask enables a device to know which other addresses are local to it, and which must be reached via a gateway or a 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

Wireless communication mode without encryption.

r

RADIUS

RADIUS (Remote Authentication Dial-In User Service) is an authentication system. When 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 it is correct and then authorizes access.

s

Securing a Wi-Fi network

Adding encryption to Wi-Fi communications

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

SSID
See ESSID

u

Upgrade

Replacement of existing software or firmware with a newer version.

w

WEP

WEP (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.



LEGRAND SNC
Siège social
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

Support technique :
0810484848