

1. FIRMWARE LICENSE INFORMATION.

The Vimar access point contains third party firmware subject to the GNU General Public License conditions. The firmware was made available and can be modified and distributed under GNU General Public License conditions.

2. SOURCE CODE AVAILABILITY.

The firmware source code (including programming scripts) subject to the GNU General Public License is available upon request and can be downloaded from www.vimar.com.

3. NETWORK SAFETY.

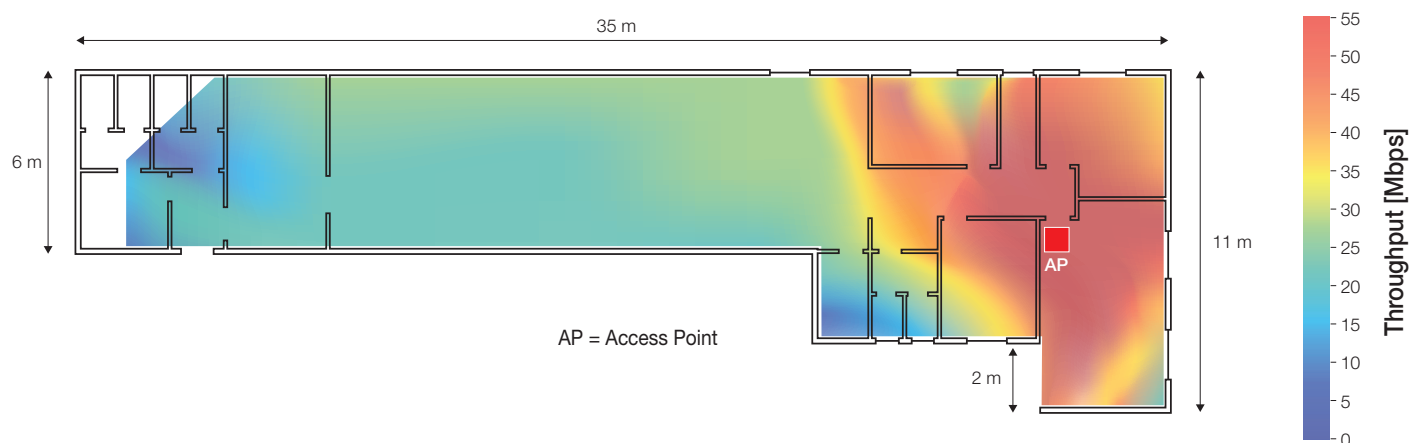
The access point is a device designed to be connected via network interfaces to the local network to communicate information and data. It is the user's responsibility to establish a secure communication between the access point and the local network and/or other networks (and to monitor them regularly).

All actions (for example, installing a firewall and/or anti virus software, adopting authentication procedures, data encryption etc.) to ensure security and protect the device, the network, the system and the interface against any kind of security violation, unauthorized access, interference, infiltration attempts, loss of information and/or theft of data or information are the responsibility of the user.

Vimar SpA declines all responsibility for damages and/or losses associated with security violations, infiltration attempts, unauthorized access, interference, loss of information and/or theft of data or information.

4. ACCESS POINT INSTALLATION.

- The Access Point can be installed at a height of between 30 and 240 cm.
- The performance levels of the device are not particularly affected by the type of material of the cover plate installed.
- The quality of coverage depends on both the type of setting and on the position in which the device is installed.
- Connectivity can be used on a surface of approximately 150-200 m² keeping in mind the fact that the coverage extension is naturally characterised by a drop in performance levels as the distance increases (see figure below).



- If installation is appropriate, two storeys of a building/home may even be covered.

5. FIRST SETUP.

The configurator device (PC, tablet or smartphone) connected to the access point is used to configure the system; this device must be set up with a static IP address. Once the configuration is completed, the pages are displayed at the address: <http://192.168.1.225>.

5.1 Cable connection .

In the event the access point is connected via LAN to the configurator device (ETH1 or ETH2 connection), set the TCP/IP parameters as follows:

- IP static in the subnet 192.168.1.x
x = number between 2 and 254 different from the address used by the access point (225 by default)
- Subnet mask 255.255.255.0

5.2 Wireless connection .

Activate the access point WiFi radio by briefly pressing the button (front or remote); the LED will blink for about 1 to 10 seconds and will stay on until the initialization phase has been completed.

To connect from the configurator device WiFi interface, use the following default parameters:

- SSID: "VIMAR_AP"
- WPA2 key: "password" (we recommend changing the default password immediately, replacing it with a personal one).

Set the TCP/IP parameters as follows:

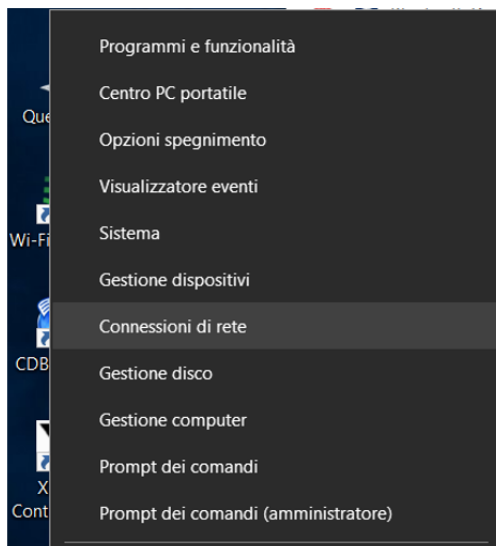
- IP static in the subnet 192.168.1.x
x = number between 2 and 254 different from the address used by the access point (225 by default)
- Subnet mask 255.255.255.0

5.3 Example of configuration from PC Windows.

Because the default access point does not supply the user network address, the PC's WiFi interface needs to be configured assigning a fixed address that belongs to the same device subnet.

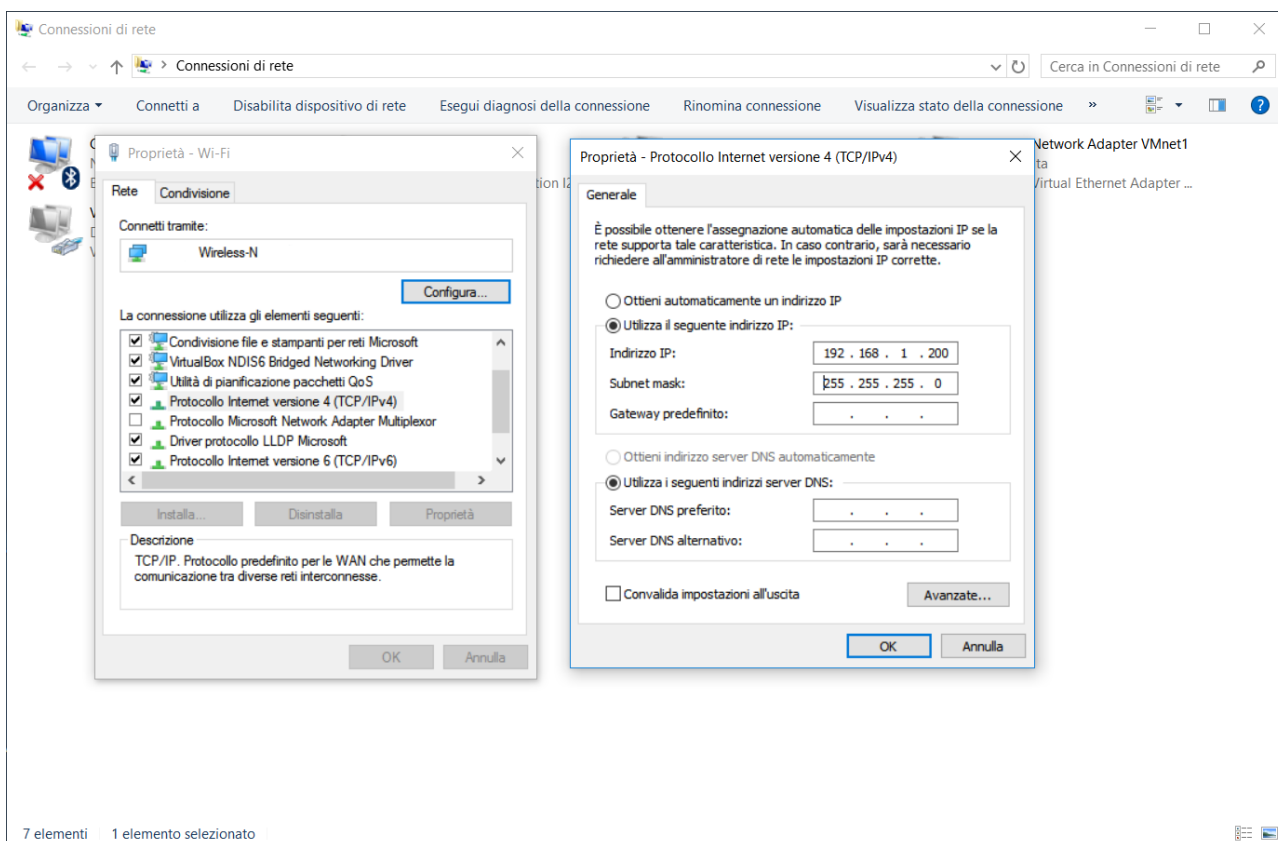
To configure the static IP on a PC with Windows 10, proceed as follows:

- Right click the mouse to select  → "Network connections".

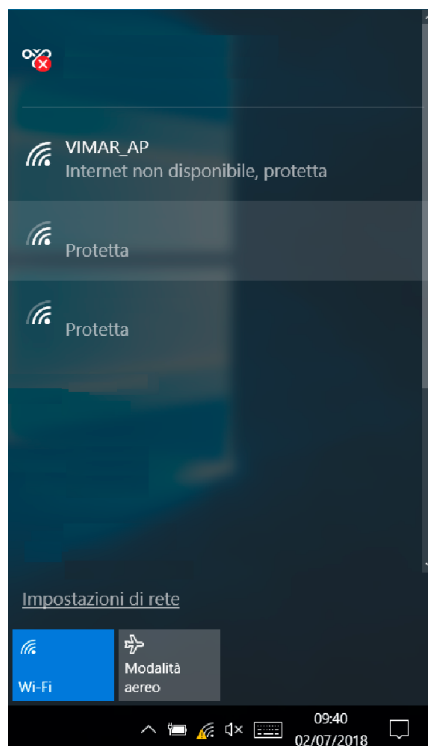


- On the page "Network connections", select the interface you want to use to configure the access point (in this case the WiFi interface) by right clicking the mouse and selecting "Properties".
- On the page "Properties", right click to select the option "Internet Protocol version 4 (TCP/IPv4)" and set a fixed address in the subnet IP network assigned to the access point that is different from the one assigned to the same access point.


By default, the access point IP is 192.168.1.225 and so it is set to 192.168.1.200 for the PC and 255.255.255.0 for the mask.



- Activate the access point search on the PC and select the device with SSID "VIMAR_AP" (SSID by default), using the password "password".



- Display the configuration page on the access point browser by entering the device IP as the URL and set password.
By default the IP 192.168.1.225 and the username is "admin" with password "admin".



Authorization Required

Please enter your username and password.

Username

Password


N.B. The SSID corresponds to the "network name" (that can be selected by the user) while the BSSID corresponds to the MAC address of the access point or network device in general (unique number written by the Vendor).

6. CONFIGURATION BY OPERATION TYPE.

Here we outline the procedures in detail for the three types of operation (SWITCH, BRIDGE and EXTENDER), that can be configured through the browser interface, with which the access point can be used.

• Login

The access point configuration page, accessible through the browser at the address set in "Advanced settings -> LAN IP", requires the login:



Authorization Required

Please enter your username and password.

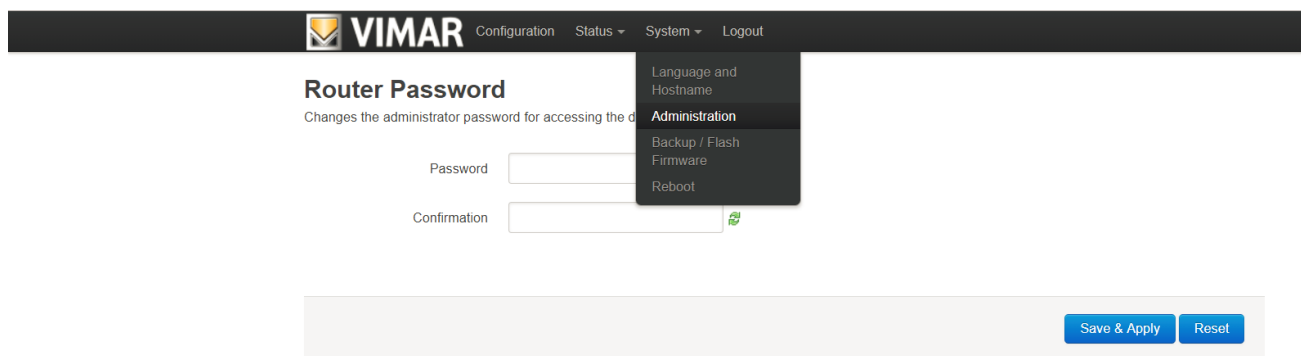
Username

Password

• Password

To change the system password, proceed as follows:

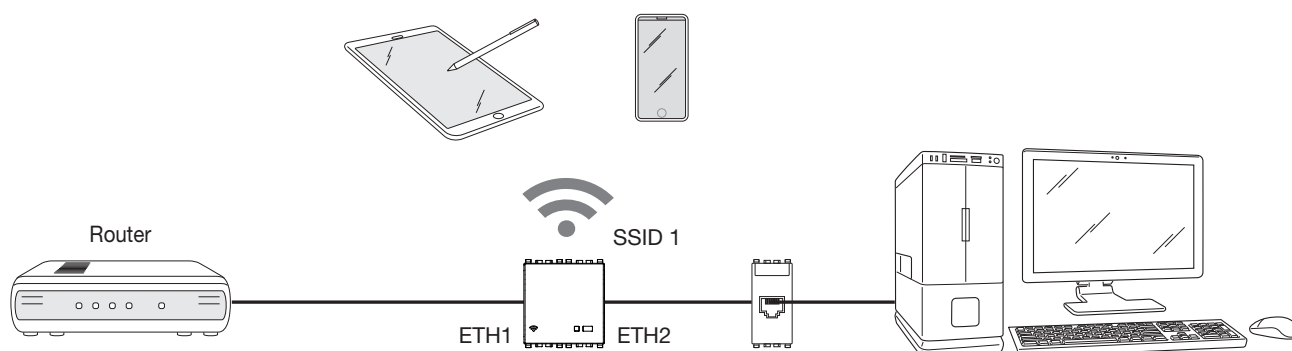
- select "System -> Password"



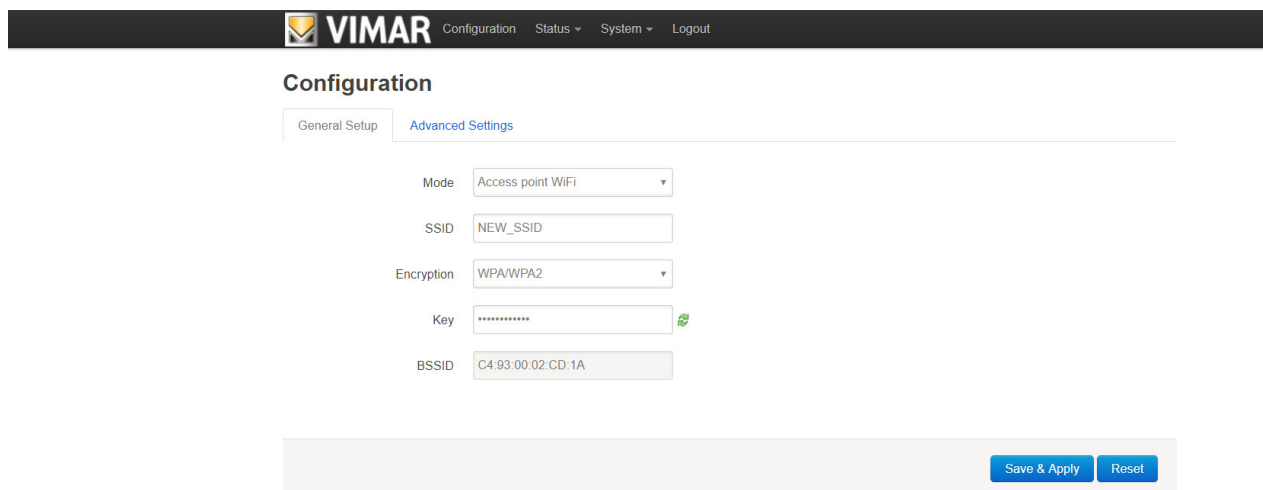
- set the new password and confirm using "Save & Apply".

6.1 WiFi Access Point (SWITCH)

This configuration implements a WiFi network that starts from a wired network connection.



Select "Configuration" and "Access point WiFi" mode; we recommend changing the password and setting up a personalized SSID as needed.



Select "Save & Apply" to confirm.

In the case of a Wireless network configuration, the connection will not be made until the system has completed the changes and the new settings have been activated. When the WiFi signal is active, the interface BSSID of the access point is displayed in the field "MAC Address" and the LED stays on.

In the advanced settings, the key parameter is "Radio Power" which varies between 0 and 20 dBm (20 dBm maximum signal capacity).

It is also possible to select the WiFi users who can connect to the network; this is particularly useful in the case of "Cable network extension" as the maximum transmission speed is reserved only for this extension, preventing other users from connecting by activating the "MAC-Address Filter" in "Advanced Settings".

Configuration
Status ▾
System ▾
Logout

Configuration

General Setup
Advanced Settings

MAC-Address Filter
disable ▾

Channel
auto ▾

Transmit Power
20 dBm ▾

Radio Channel Width
20MHz ▾

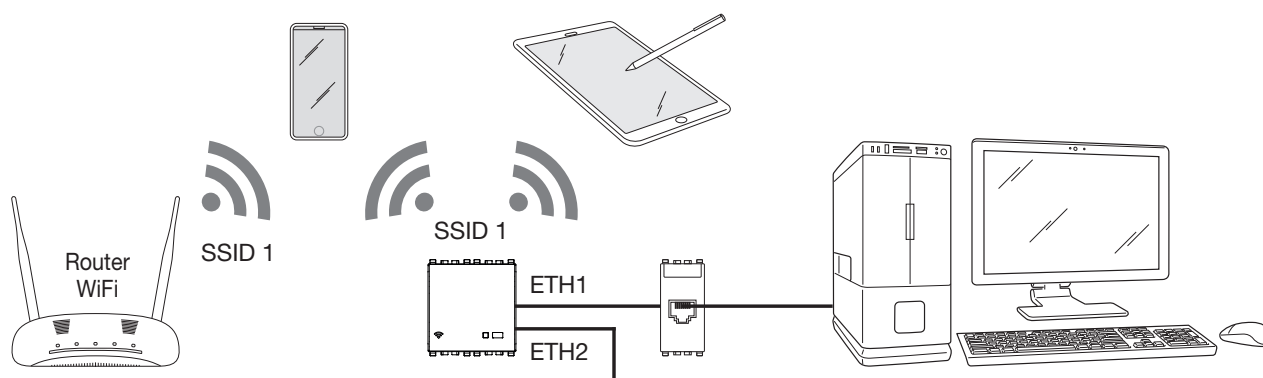
IPv4 address
192.168.1.225

IPv4 netmask
255.255.255.0

Save & Apply
Reset

6.2 WiFi network extension (BRIDGE)

This configuration extends the WiFi network coverage using the access point as a signal "repeater".



In this case, it is necessary to set the home router SSID, the security type and the password in the wireless device being extended.

The configuration is confirmed by selecting "Save & Apply"; if the operation is successful, the BSSID of the access point used to extend the WiFi network is shown in the "Connected" field.

Configuration
Status ▾
System ▾
Logout

Configuration

General Setup
Advanced Settings

Mode
WiFi network extension ▾

SSID
VIMAR_AP

Encryption
WPA/WPA2 ▾

Key

Connected
C4:93:00:09:7A:F2

Save & Apply
Reset

In the advanced settings, the key parameter is "Radio Power" which varies between 0 and 20 dBm (20 dBm maximum signal capacity).

We recommend keeping the radio channel width at 20 MHz to obtain a more stable connection with the access point being used to extend the WiFi network.

Configuration

[General Setup](#)
[Advanced Settings](#)

WLAN IPv4 settings DHCP

Connect to this MAC

MAC-Address Filter disable

Transmit Power 20 dBm

Radio Channel Width 20MHz

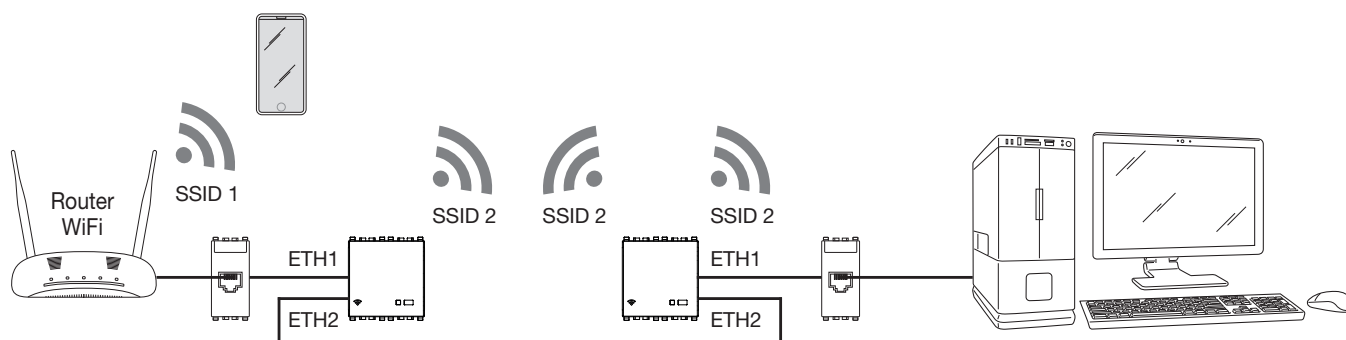
IPv4 address 192.168.1.225

IPv4 netmask 255.255.255.0

[Save & Apply](#)
[Reset](#)

6.3 WiFi network extension (BRIDGE)

This configuration extends the wired network to an area that the cable and/or wireless network cannot reach directly.



To achieve this configuration, two access points must be used:

- the first, connected to the LAN network, is configured in "Access point WiFi" mode;
- the second is configured in "Extension of the wired network" mode.

Then set the **SSID**, the **security** type and the **password** for the access point connected to the LAN network.

The configuration is confirmed by selecting "Save & Apply"; if the operation is successful, the BSSID of the access point to which it is connected is displayed in the "Connected" field.

It is also possible to enable the Wireless signal repeater by selecting "Enable WiFi repeater"; in this case, the maximum transmission speed available to extend the radio signal is reduced (by up to half).

Configuration

[General Setup](#)
[Advanced Settings](#)

Mode Wired network extension

SSID VIMAR_AP

Encryption WPA/WPA2

Key *****

WiFi repeater enable ☐

Connected C4:93:00:09:7A:F2

[Save & Apply](#)
[Reset](#)

In the advanced settings, in addition to the parameter “Radio Power”, the “Radio channel width” must be set, aligning the setting with the access point it is connected to. In the event of more than one network with the same SSID, using the option “Connect to this MAC” it is possible to force the BSSID of the WiFi network you want to connect to.

In this case, it is vital that the option “LAN IP” is set at a different address from the one used for the connected access point; if this is not the case, when “Save and Apply” is selected, once the connection is established, there will be a duplicated address resulting in difficulties accessing the configuration page of both devices.

Configuration Status ▾ System ▾ Logout

Configuration

General Setup
Advanced Settings

Connect to this MAC

Transmit Power

20 dBm ▾

Radio Channel Width

20MHz ▾

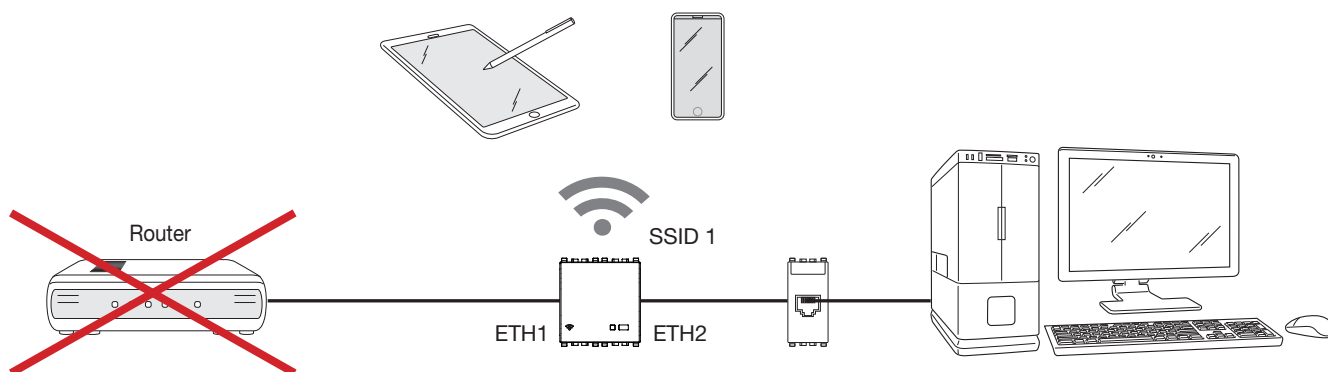
IPv4 address

IPv4 netmask

Save & Apply
Reset

7. OPERATION AS A WiFi Access Point - Temporary DHCP server activation.

When the system is configured as a WiFi Access Point (see para. 6.1), the DHCP server function can be temporarily enabled. This service can be used when the router is not available in the system and you wish to configure devices that require the assignment of an IP address in the local network.



7.1 Service characteristics.

The IP range assigned is: 192.168.1.100 - 192.168.1.150 with Lease Time of 30 minutes.

The DHCP server function is available in the Access point with fw ver. 1.1.0 and later; in the event of previous fw versions, during the upgrade do not select “Maintain settings”.

If the DHCP server function is not used, the system does not need to be upgraded.

7.2 Service activation.

To activate the service, follow the procedure below:

1. Power the Access point; if it is already powered, cut off and restore the power supply. Once this is done, you have to complete the procedure within 180 s.
2. Wait for approximately 30 s to restart and hold down the front push button between 2 and 5 s; the LED flashes quickly.
If the push button is pressed without being released after 5 s the LED returns to its normal operating status (on or off depending on the status of the WiFi) whereas if it is pressed continuously (total time of 10 s) the device reset is activated.
3. While the LED flashes, release the push button and then press it again.
4. Repeat step 3; you have entered DHCP server active mode and the LED flashes slowly for a few seconds (0.5 s on, 0.5 s off).
If another active DHCP server is detected in the network, the procedure is interrupted and the LED flashes in “warning” mode (50 ms on, 500 ms off) to indicate that the DHCP server has not been activated.
5. Once you have activated the service, switch off all the devices connected to the network and then back on again so that they are assigned a new valid IP address.

Caution: Do not activate the DHCP service in operating modes other than WiFi Access Point.

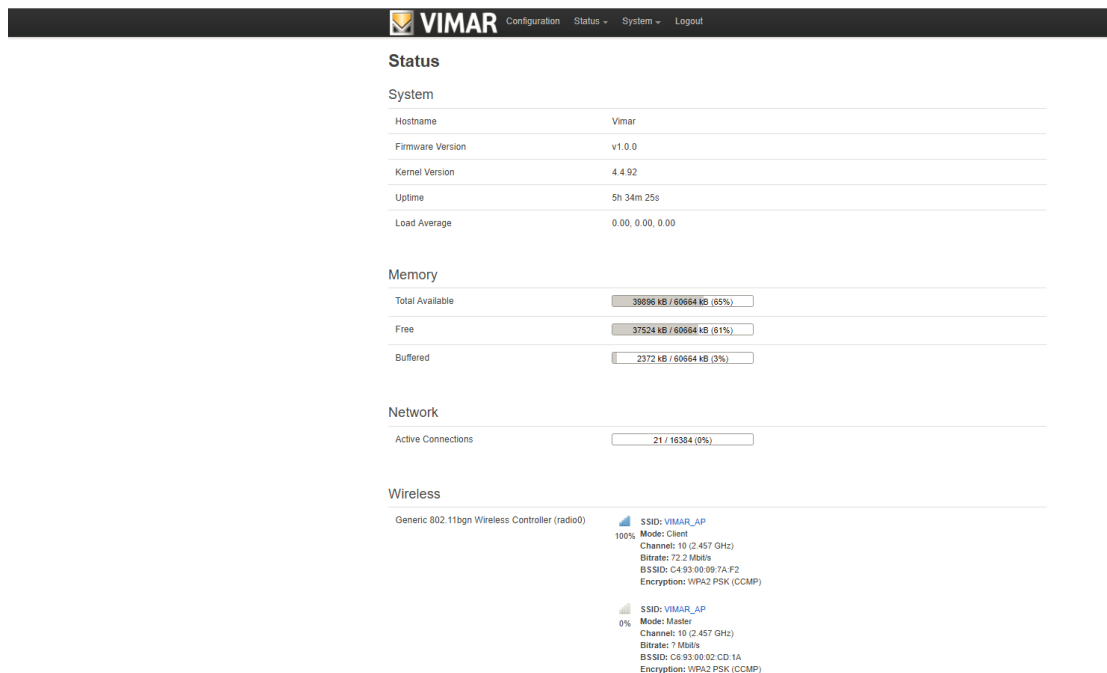
7.3 Service deactivation.

The service is deactivated:

- automatically after 10 h;
- if the Access point is switched off and back on again;
- if another active DHCP server is detected in the network during the activation phase.

8. STATUS.

Select “State -> Panoramic” to display that status of the network interfaces, any users connected and the system firmware version.



The screenshot shows the VIMAR Status page with a navigation bar at the top containing 'Configuration', 'Status', 'System', and 'Logout'. The main content area is titled 'Status' and is divided into four sections: System, Memory, Network, and Wireless.

System

Hostname	Vimar
Firmware Version	v1.0.0
Kernel Version	4.4.92
Uptime	5h 34m 25s
Load Average	0.00, 0.00, 0.00

Memory

Total Available	38896 KB / 60664 KB (65%)
Free	37524 KB / 60664 KB (61%)
Buffered	2372 KB / 60664 KB (3%)

Network

Active Connections	21 / 16384 (0%)
--------------------	-----------------

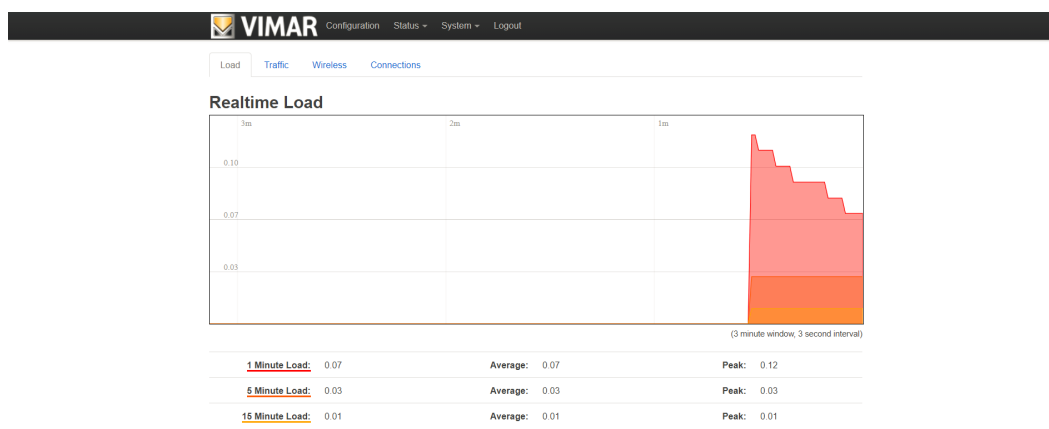
Wireless

Generic 802.11bgn Wireless Controller (radio0)

SSID: VIMAR_AP
Mode: Client
Channel: 10 (2.457 GHz)
Bitrate: 72.2 Mbit/s
BSSID: C4:93:00:09:7A:F2
Encryption: WPA2 PSK (CCMP)

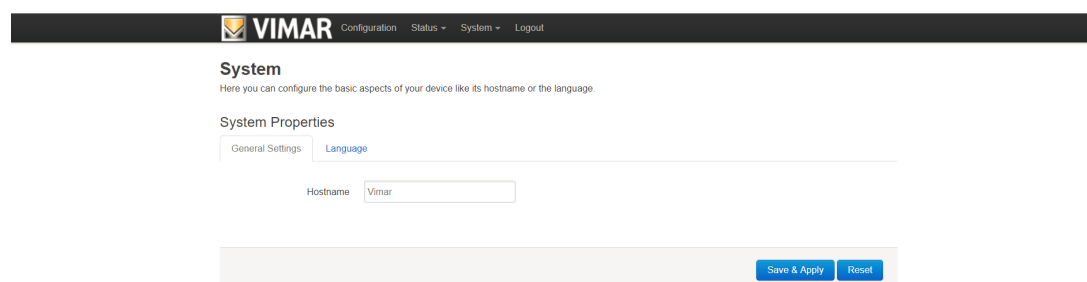
SSID: VIMAR_AP
Mode: Master
Channel: 10 (2.457 GHz)
Bitrate: 7 Mbit/s
BSSID: C6:93:00:02:CD:1A
Encryption: WPA2 PSK (CCMP)

Select “State -> Graphics” to display the data traffic trend transiting in the access point.



9. SYSTEM.

Select “System -> Language and Hostname” to set the page display and device name language.



The screenshot shows the VIMAR System page with a navigation bar at the top containing 'Configuration', 'Status', 'System', and 'Logout'. The main content area is titled 'System' and contains a sub-section 'System Properties' with a 'Language' tab selected. Below the tab, there is a form for setting the Hostname, which is currently set to 'Vimar'. At the bottom right, there are buttons for 'Save & Apply' and 'Reset'.

System

Here you can configure the basic aspects of your device like its hostname or the language.

System Properties


General Settings | **Language**

Hostname:

[Save & Apply](#) [Reset](#)

Select “System -> Password” to modify the password to access the configuration pages (see chap. 6).

Select “System -> Save data/Update Firmware” to update the device firmware, save the configuration or download a different one and reset the access point to the factory default.


Configuration Status ▾ System ▾ Logout

Flash operations

Backup / Restore

Click “Generate archive” to download a tar archive of the current configuration files. To reset the firmware to its initial state, click “Perform reset” (only possible with squashfs images).

Download backup: Generate archive

Reset to defaults: Perform reset

To restore configuration files, you can upload a previously generated backup archive here.

Restore backup: Choose File No file chosen Upload archive...

Flash new firmware image


Upload a sysupgrade-compatible image here to replace the running firmware. Check “Keep settings” to retain the current configuration (requires a compatible firmware image).

Keep settings: ☒

Image: Choose File No file chosen Flash image...

9.1 Updating the firmware

1. Download the compressed file containing the new firmware Image by article code from the www.vimar.com website.
2. Extract the file containing the configuration image in .bin format, the .txt file contains release notes and the MD5SUM signature needed to verify the accuracy of the code downloaded.
3. Download the firmware Image as illustrated in the figure on the next page; the text file attached sets out the option to keep the settings.


Configuration Status ▾ System ▾ Logout

Flash operations

Backup / Restore

Click “Generate archive” to download a tar archive of the current configuration files. To reset the firmware to its initial state, click “Perform reset” (only possible with squashfs images).

Download backup: Generate archive

Reset to defaults: Perform reset

To restore configuration files, you can upload a previously generated backup archive here.

Restore backup: Choose File No file chosen Upload archive...


Flash new firmware image

Upload a sysupgrade-compatible image here to replace the running firmware. Check “Keep settings” to retain the current configuration (requires a compatible firmware image).

Keep settings: ☐

Image: Choose File vimar-xx195-v1.0.0.bin Flash image...

Caution: always check that the MD5 value corresponds to the value in the .txt file distributed with the .bin file.


Configuration Status ▾ System ▾ Logout

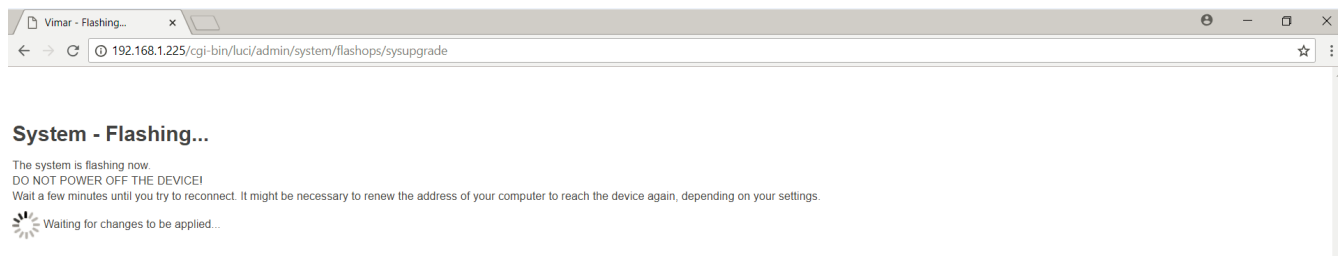
Flash Firmware - Verify

The flash image was uploaded. Below is the checksum and file size listed, compare them with the original file to ensure data integrity. Click “Proceed” below to start the flash procedure.

- Checksum
MD5: 023a8d450890eb7636aa30022285e288
SHA256: 250fb88e2a8468f880cc1c05aa4672e9a68055a49678f672ae9a3b0d0800f164
- Size: 3.63 MB (15.62 MB available)
- Note: Configuration files will be erased.

Cancel Proceed

5. Lastly, select “Continue” to launch the update.
During this stage, it is vital not to interrupt the power supply.



N.B.: During the update, in order to prevent damage or malfunctions, the system must be protected against interference or interruptions to the power supply.

A firmware update is recommended only when the system is experiencing technical problems.

Vimar SpA shall not be liable in any way to guarantee the product in the event:

- non-original firmware or firmware other than that downloaded from the Vimar site is downloaded;
- it is found that the firmware is corrupted as a result of an incorrect procedure.

10. RESET THE FACTORY CONFIGURATION OF THE WiFi ACCESS POINT.

To restore the device to the factory configuration:

- within 3 minutes from when the device is connected to the power supply and after the start up phase (about 30 s), press the button (front or remote) for at least 10 s until the LED blinks;
- release the button.

The access point will restart in about 30 s.