

Vimar end-user license contract

Vimar end-user license contract

VIMAR SPA located in Marostica (VI), Viale Vicenza n. 14 (<https://www.vimar.com>), sole owner of the software named "Software Web Server", through this contract grants the license of use of the aforementioned program.

VIMAR SPA shall not be held liable for any damage caused by improper use of the aforementioned software, in particular for direct or indirect damage to persons, property, and/or animals due to economic loss that may occur as a result of the use of the software.

VIMAR SPA reserves the right to make any changes to improve the function of the aforementioned software without advance notice. It is prohibited to modify, translate, adapt, or create applications based on the aforementioned software, without previous written consent from VIMAR.

The user must verify the suitability of the program to his needs, and interpret the results to verify the consequences of the choices of design made.

All risks concerning the results and performance of the program are assumed by the user.

VIMAR SPA holds the exclusive property right of the software.

Unauthorized duplication of the program is prohibited.

It is expressly forbidden to modify, translate, fit, change, disassembly in any way or to create by-products from the software.

The user is to be held responsible not to eliminate any information of the software relevant to the Copyright.

The software are protected under the Copyright laws in force in Italy and foreseen by the International treaties, therefore, any activity realized in contrast with what is stated above, will be prosecuted at the right place.

Microsoft, Windows, Vista, Xp, Seven, Media Center, Internet Explorer are registered trademarks of the Microsoft Corporation in the United States and/or other countries.

Apple, Mac, Mac OS, iMac, MacBook, iPhone, iPod Touch, iPad, Safari are trademarks of Apple Inc., registered in the U.S. and other countries.

Mozilla, Firefox are registered trademarks of Mozilla.

Google Chrome is a trademark of Google Inc.

Linux is a registered trademark of Linus Torvalds in the United States and/or other countries.

VIMAR SPA
Viale Vicenza, 14
36063 Marostica VI - Italy
<https://www.vimar.com>

INDEX

Prerequisites	6
P.1 WEB BROWSER COMPATIBILITY	6
P.2 OPERATING SYSTEM COMPATIBILITY	6
P.3 BY-ME SYSTEM COMPATIBILITY	6
P.3.1 Minimum web software version Weather station KNX management server (Art. 01546)	6
P.4 REQUIREMENTS FOR REMOTE ACCESS	6
P.5 COMPATIBILITY WITH THE BY-ALARM SYSTEM	6
1. Installation	7
1.1 Mounting and connections	7
1.1.1 Management of SD card by the Web Server	7
1.1.2 RESET button	8
1.1.2.1 Restoring the network settings to default	8
1.1.2.2 Fully restore the factory settings	8
1.2 Connecting via Network	9
1.3 Access	11
2. General settings	12
2.1 Introduction	12
2.2 Language	13
2.2.1 Setting the language at first start	13
2.2.2 Setting the language from the menu	13
2.3 Network	13
2.4 Updates	19
2.5 Firmware Upgrade	20
2.6 Database	21
2.7 Backgrounds	22
2.8 SD Memory Management	22
2.9 Date / Time	22
2.10 Email	23
2.11 DYNDNS	24
2.12 ByWeb Tools	24
3. By-me configuration	25
3.1 Getting Started	25
3.1.1 System configuration using EasyTool Professional	25
3.1.2 System configuration using the control unit	25
3.2 Configuration	25
3.3 Importing the By-me project	26
3.4 Environments	29
3.5 BY-ME Functions	32
3.5.1 Configuring the automatic reset of the min/max values of the KNX weather station	32
3.5.2 Device widget customized behaviour management	33
3.6 Browsing by environments	33
3.7 Browsing by functions	35

INDEX

4. Alarm System configuration	36
4.1 The By-alarm intrusion detection alarm system	36
4.1.1 Introduction	36
4.1.2 Import XML	36
4.1.3 Configuration	36
4.1.4 By-me Events	37
4.1.4.1 By-me Events linked to the states of By-alarm areas	38
4.1.4.2 By-me Events linked to the states of By-alarm areas	41
4.1.4.3 By-me events linked to By-me commands	44
4.1.5 By-alarm Manager Bridge	47
4.1.5.1 The bridge feature of the Web Server	48
4.2 The Alarm System By-me	49
4.2.1 Introduction	49
4.2.2 Changing partializations	49
5. Setting up the video surveillance	50
5.1 Introduction	50
5.2 Setting up an IP camera	50
5.2.1 IP cameras Proxy Function	52
5.3 Viewing the cameras	53
6. Energy monitoring	54
6.1 Introduction	54
6.2 Power consumption	55
6.2.1 General settings	55
6.2.2 Contracts with variable threshold	56
6.2.3 Contracts at hourly rates	56
6.2.3.1 Hourly rates	56
6.2.3.2 Holidays	57
6.2.3.3 Profile of week days	58
6.2.3.4 Profiles times frames	59
6.3 Electricity production	60
6.4 Individual loads measurement	61
6.5 Pulse-counter	61
7. Users and authorisations	62
7.1 Introduction	62
7.2 Users	62
7.3 User Groups	65
7.4 Authorizations	67
7.4.1 Levels and functionality	68
7.4.2 The technique of "promotion" to higher authorization levels	69
7.4.3 Groups-Permissions Association	69
7.4.4 The Administrators Group	69
7.4.5 The Installers Group	69
7.4.6 The Users Group	69
8. Multimedia Touch 10 (cod. 21553 or 21553.1 or 21553.2)	70
9 Notifications by email	71

INDEX

10. Mobile	75
10.1 Add To Home	75
11. ByWeb Tools by Vimar	76
11.1 Introduction	76
11.2 Requirements	76
11.3 Installation	76
12. Integration of KNX devices in the By-me system	77
12.1 Introduction	77
12.2 Single functions	77
12.3 Compound functions	79
12.4 Configuration	79
12.5 Integration of the gateway ME-AC-KNX-1-V2 of Intesis for the management of Mitsubishi air-conditioners	80
12.5.1 Premessa	80
12.5.2 The configuration procedure	80
12.5.3 The KNX configuration of the Intesis (with version 0.8 of the ETS application programme) gateway	81
12.5.3.1 Setting the gateway ME-AC-KNX-1-V2 (with version 0.8 of the ETS application programme) parameters in the KNX project	81
12.5.3.2 Setting the gateway ME-AC-KNX-1-V2 (with version 0.8 of the ETS application programme) parameters in the KNX project	81
12.5.4 Creation and configuration of KNX integration objects for the gateway Intesis (with version 0.8 of the ETS application programme) through EasyTool Professional	82
12.5.5 The KNX configuration of the Intesis (with version 1.0 of the ETS application programme) gateway	83
12.5.5.1 Setting the gateway ME-AC-KNX-1-V2 (with version 1.0 of the ETS application programme) parameters in the KNX project	83
12.5.5.2 Setting the gateway ME-AC-KNX-1-V2 (with version 1.0 of the ETS application programme) parameters in the KNX project	84
12.5.6 Creation and configuration of KNX integration objects for the gateway Intesis (with version 1.0 of the ETS application programme) through EasyTool Professional	85
13 The significant upgrades introduced in versions 2.5 and 2.6 of the web server software for the management of the HTTPS protected connection	86
13.1 Premessa	86
13.2 Version 2.5 of the web server software 01945/01946	86
13.2.1 Operations to be completed before upgrading to version 2.5	86
13.2.2 Upgrade of the TLS protocol to version 1.2	86
13.2.3 The automatic check performed by the web server on the availability of a new CA certificate and on the expiry of the CA certificate on board the web server.	87
13.3 Version 2.6 of the web server software 01945/01946	87
14 Using the Google Gmail SMTP service to send web server e-mail notifications	88
14.1 Introduction	88
14.2 Creating a “password for Apps” on Google Gmail	88
14.2.1 Enabling the “two-step verification” to access the Google Gmail account	88
14.2.2 Creating the “password for Apps” for the web server	88
14.3 Web server configuration	89

Prerequisites

Prerequisites

P.1 WEB BROWSER COMPATIBILITY

To access the Web Server you can use the following web browsers:

- Apple Safari (version 5.1 or above)
- Google Chrome (version 14 or above)

The Vimar By-Web Web Server is not compatible with browser Microsoft Internet Explorer.

P.2 OPERATING SYSTEM COMPATIBILITY

Full compatibility with various Linux distributions is not guaranteed.

P.3 BY-ME SYSTEM COMPATIBILITY

The following table reports versions of SW and FW of the By-me control unit and EasyTool Professional configuration software compatible with the Web Server.

Web Server	EasyTool Professional	By-me control unit	3 modules control unit	Multimedia Video Touch Screen 10in P		
				Code 21553	Code 21553.1	Code 21553.2
01945 - ver. 2.6 01946 - ver. 2.6	ver. 2.12	ver. 5.1 or later	ver. 1.0 or later	ver. 1.4.01	ver. 4.0.05	ver. 5.0.xx

P.3.1 MINIMUM WEB SOFTWARE VERSION WEATHER STATION KNX MANAGEMENT SERVER (ART. 01546)

If a KNX weather station is configured in the installation, you need to use a web server software version of 1.15 or later.

P.4 REQUIREMENTS FOR REMOTE ACCESS

To access the web server remotely:

- **The IP address (static or dynamic) must be public.**
- **there has to be the possibility to change some parameters of the router.**

P.5 COMPATIBILITY WITH THE BY-ALARM SYSTEM

The following table gives the SW and FW versions of the By-alarm control panels compatible with the Web Server.

Web Server	By-alarm control panel	
	Art. 01700	Art. 01703
(art. 01945-01946)	Art. 01700	Art. 01703
Ver 1.20 or later	1.0 or later	1.0 or later

ATTENTION: Before performing any Web Server configuration, download the updated software from the Product Software section on website www.vimar.com

Installation

1. Installation

1.1 Mounting and connections

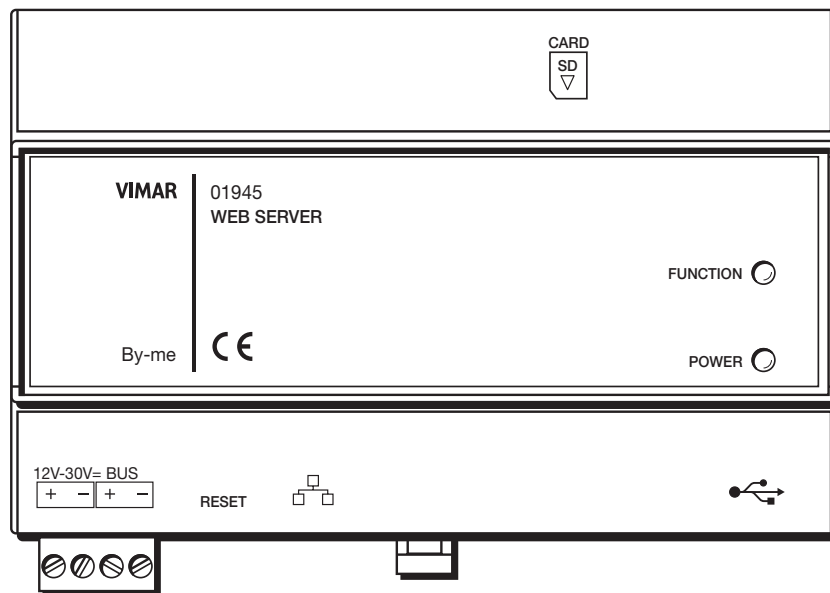
The Web Server is designed to be mounted on standard DIN rail. For the correct operation of the Web Server it is necessary to provide the following connections:

- 12V DC power supply by connecting, through a special terminal provided, the power supply art. 01830.
- By-me bus using the special terminal provided
- LAN network via cable via cat. 5 or higher and standard RJ45 connector

The front LED marked as "POWER" indicates the presence of power, while the "FUNCTION" LED is normally off, except to point out special operations in progress.

The Web Server also provides the following ports:

- SD Slot: available for future applications
- USB Slot: available for future applications



NOTE: connection to the By-me bus is not essential to the configuration of the Web Server; however, it is preferable because in its absence is not possible to check its correct operation.

Art. 01946 can manage up to 64 By-me devices (control panel art. 21509 included). The devices to be counted are only all those with a + - BUS terminal.

The Web Server (art. 01945-01946) can support a maximum of 1 load control module art. 01455.

1.1.1 Management of SD card by the Web Server

The Web Server has a slot for inserting an SD memory card. The slot is a "push-push" type.

SD card compatibility characteristics

Compatible SD cards: SD, SDHC.
Format: FAT32

Inserting the SD card

The procedure for inserting the SD card in the Web Server is as follows:

1. Disconnect the power supply to the Web Server
2. Insert the SD card into the dedicated slot on the Web Server, with the direction indicated on the label on the device. The card must be pushed into the docked position in the slot.
3. Reconnect electrical power to the Web Server

IMPORTANT: If the SD card is inserted with the Web Server powered on, it will not be usable on the Web Server.

Removing the SD card

The procedure for removing the SD card from the Web Server is as follows:

1. Disconnect the power supply to the Web Server
2. Push the SD card in to release the card from dock and proceed with the extraction of the SD card .
3. Reconnect electrical power to the Web Server

Installation

1.1.2 RESET button

The RESET button allows you to do the following:

- Restore the network settings to default
- Fully restore the factory settings: network settings and configuration.

1.1.2.1 Restoring the network settings to default

This setting resets to factory defaults the following data on the network configuration of the web server.

IP Address: 192.168.0.110

Gateway: 192.168.0.4

Netmask: 255.255.255.0

ATTENTION: Once executed, the procedure cannot be undone.

The procedure involves the following steps:

- 1) Hold down the RESET button for 10 seconds. The LED "function" begins to flash, indicating it has entered into configuration mode.
- 2) Release the RESET button
- 3) Hold down the RESET button for 1 second (**and in any case less than 4 seconds**).
After a few seconds the LED stops flashing and the recovery process of the network parameters begins.

1.1.2.2 Fully restore the factory settings

This setting resets to factory defaults all configuration data of the web server (network parameters settings, system data, user data, Energy Monitoring system history).

ATTENTION: Once executed, the procedure cannot be undone.

The procedure involves the following steps:

- 1) Hold down the RESET button for 10 seconds. The LED "function" begins to flash, indicating it has entered into configuration mode.
- 2) Release the RESET button
- 3) Hold down the RESET button for at least 5 seconds. After a few seconds the LED stops flashing and the recovery process of the configuration parameters.

Installation

1.2 Connecting via Network

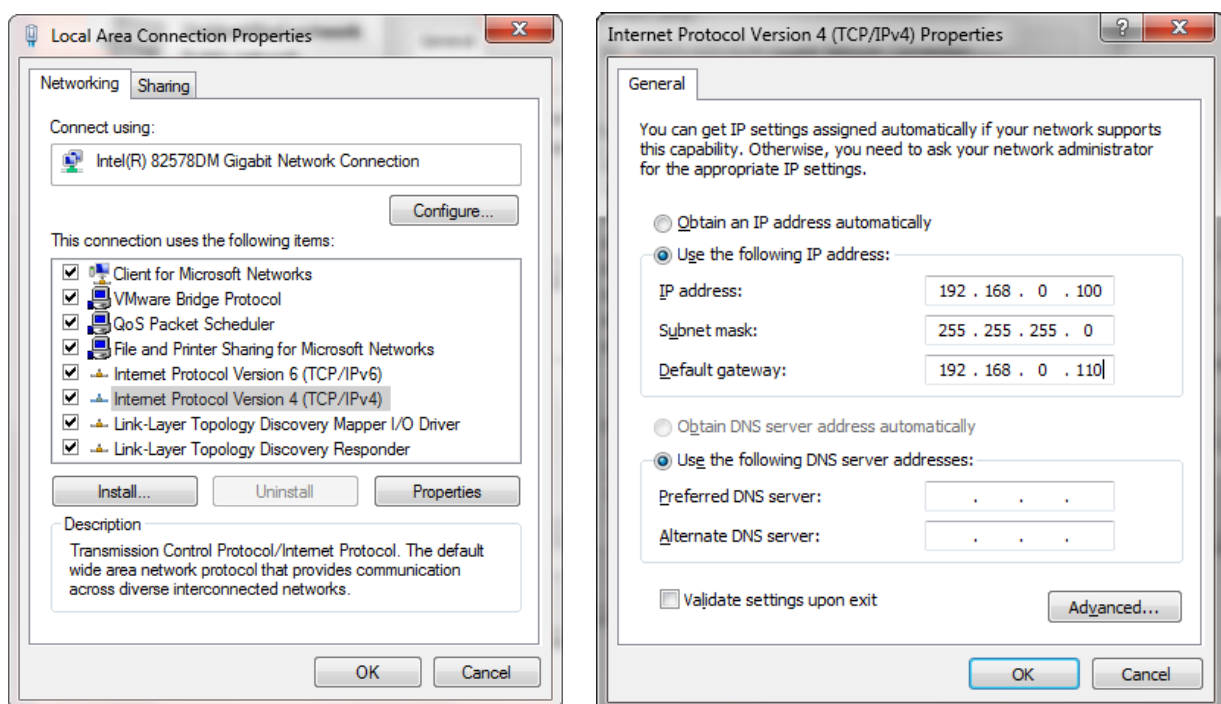
The configuration and use of the **Web Server** include a link to your home or business.

The network parameters of the **Web Server** will be set according to the configuration of the LAN which must host it.

For the initial configuration of the **Web Server**, as well as in the absence of a network during installation, you must proceed as follows:

- Connect the **Web Server** to the PC through a Ethernet straight through or crossover Ethernet cable
- Access to the network configurations of the PC, as shown in the documentation for your operating system
- Change the settings of the TCP/IP (version 4) communication protocol relating to the LAN port that is connected to the **Web Server**, and manually set the following parameters:
 - IP Address: 192.168.0.0.100
 - Netmask: 255,255,255.0
 - Default gateway: 192.168.0.110
- Save and wait for the new settings to take effect. If required, restart the system.

The following figures show, for example, the network configuration windows for a PC with Windows 7 operating system.

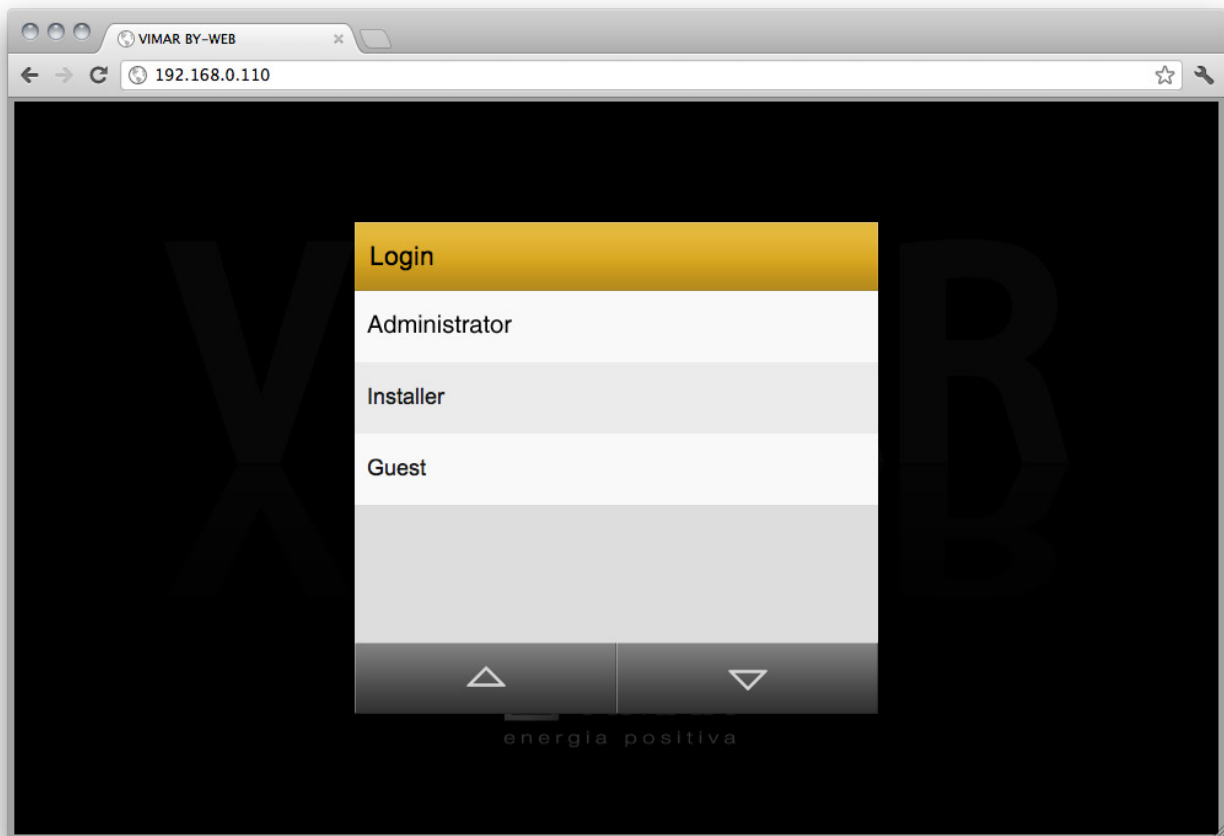


After these operations, open an Internet browser and type in the address bar, as follows:

<https://192.168.0.110>

Installation

If the network configuration is correct, you will see the following welcome page:



If the default network settings of the Web Server are not compatible with the configuration of the LAN which must host it, after accessing it as described above:

1. Change the network settings of the Web Server based on the configuration of the LAN
2. Restore the network configuration of the PC to the factory defaults

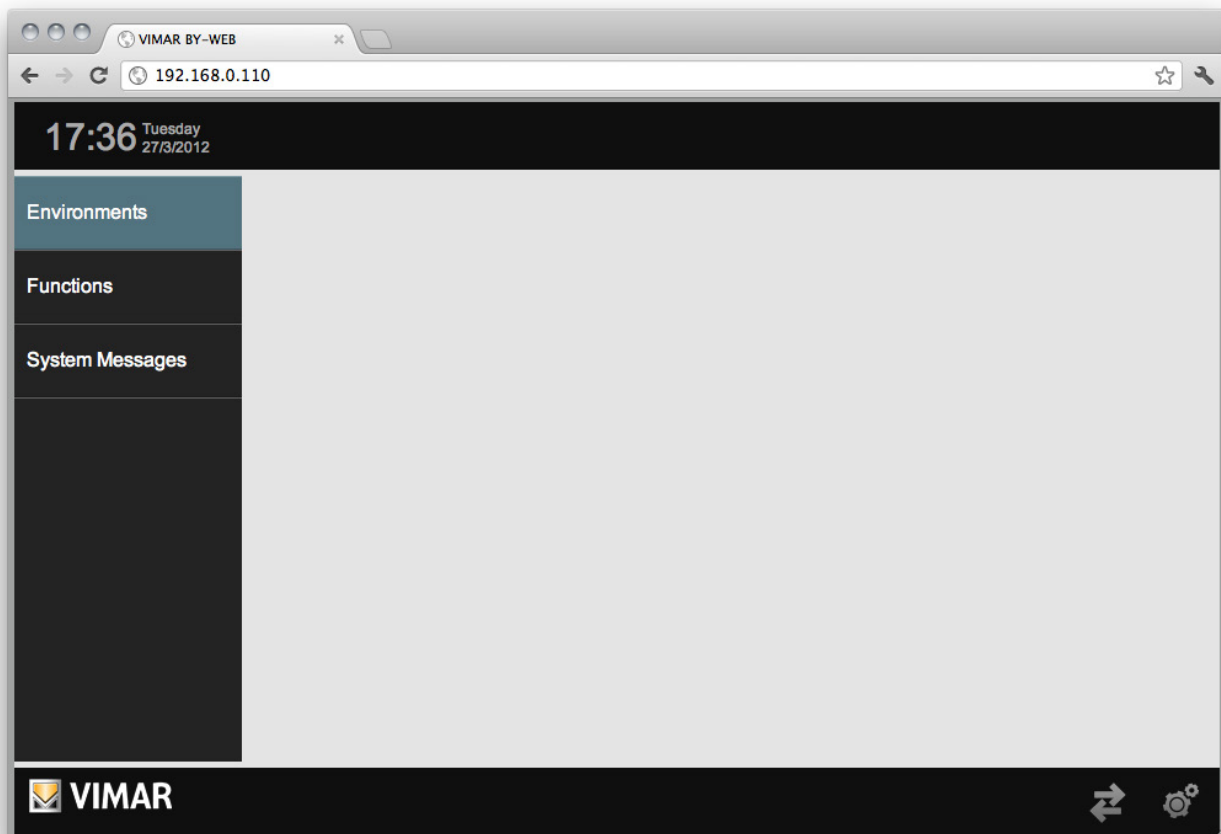
Installation

1.3 Access

The Web Server has the following users preset by default:

USER	PASSWORD	DESCRIPTION
Administrator	admin	Home automation system administrator user.
Installer	poweruser	User dedicated to installing and configuring the Web Server. He has the rights to perform any operation on the system, but cannot edit the rights of other users.
Guest	guest	Basic user for connections from the PC. Has the rights to view the status of the system, browse the pages of the Web Server and perform basic commands on the home automation system.

To configure the supervision of the **By-me** system, you must then select the "Installer" user from the list and type in the corresponding password (which can be changed later); after it's been loaded you'll view the following **Web Server** main screen:



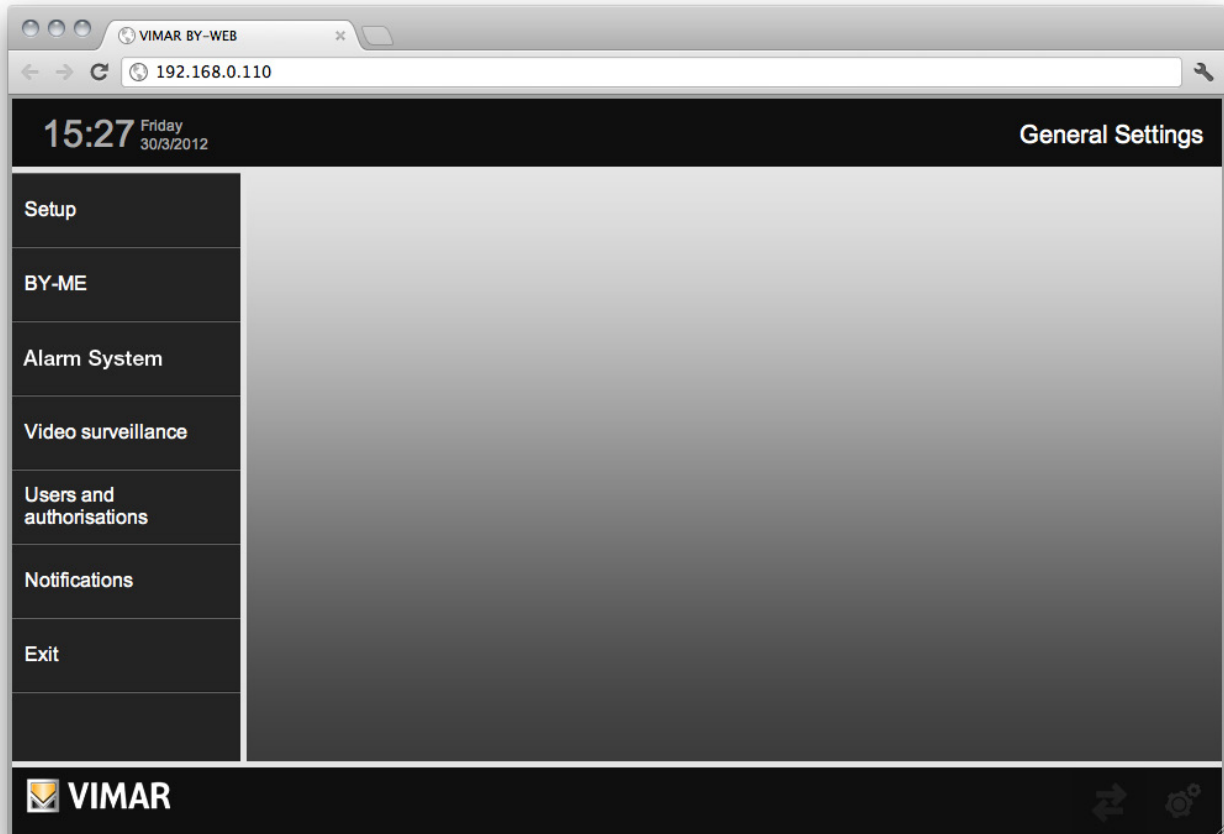
NOTE: For security reasons, we recommend that you change the default password of the Administrator, Installer and Guest users.

General settings

2. General settings

2.1 Introduction

The Web Server can be configured and customized through a special section of GENERAL SETTINGS, accessible by selecting "General Settings" from the popup menu displayed by pressing the button on bottom right of the page. The following page is displayed:








The available menu on the left provides access to the following sections:

SETUP	General settings on the Web Server , and maintenance.
BY-ME	Configuring the supervision of the By-me system.
ALARM SYSTEM	Changing the name of the Partializations
VIDEO SURVEILLANCE	Configuration of the IP cameras
USERS AND AUTHORISATIONS	Setting up authorized users to use the Web Server and related permits.
NOTIFICATIONS	Configuring notifications by e-mail after SAI alerts.
EXIT	Return to the main page of the Web Server .

General settings

Within the specific configuration pages of the various aspects of the **Web Server**, it is always available at the bottom a button panel containing one or more of the following buttons:

	BACK Allows you to return to the previous page or the settings main menu
	SCROLL UP Allows you to scroll up the page, if it exceeds the available height
	SCROLL DOWN Allows you to scroll down the page, if it exceeds the available height
	CONFIRM Where available, allows you to save your changes on the page. On pages where it is not present, any changes are saved instantly without the need of confirmation.
	ADD / ENTER Where available, allows - as appropriate - to create a new item in a list (e.g.: creation of a new environment), or add items related to the current through the search engine (e.g. addition of devices the current environment)

The following paragraphs describe in particular the functions available in the "SETUP" section of GENERAL SETTINGS; other sections will be explored in subsequent chapters.

2.2 Language

2.2.1 Setting the language at first start

When you first start the Web Server, and after every "restore to factory settings" operation a dialog opens for setting the language. You can still change the language used by the Web Server later, from the appropriate menu described in the next chapter.

2.2.2 Setting the language from the menu


From this page you can only change the language of the Web Server. To access the Web Server language management, from the GENERAL SETTINGS page select the SETUP menu and then select LANGUAGE. This page contains a drop down menu that lets you choose the language of the Web Server, once selected your preferred language, you must press the confirm button on bottom right. After a second, the Web Server is reloaded with the new language of choice. If, however, when choosing the language, you press the exit button on bottom left, the change is not applied and you will return to the General Settings page.

2.3 Network

Through this page you can set network parameters of the **Web Server**; this operation is required for:

1. Editing web server network settings, if the factory settings are not compatible with the target LAN configuration.
2. Finishing the management process for web server SSL certificates, introduced by web server software version 1.12.

Important: This process requires an Internet connection for the web server. If an Internet connection is not available, the web server will use the SSL certificate provided by previous software versions of the web server.

For such purpose, even if it is not required to edit the factory network settings of the web server, you should confirm network connection anyway, by pressing the  button.

NOTE: In versions 2.5 and 2.6, upgrades have been introduced in the management of the HTTPS protected communication, according to the directives currently in force. In particular, the upgraded CA certificate by Vimar has been made available, the creation of the upgraded TLS certificate of the web server and the upgrade of the TLS protocol to version 1.2 has been managed. We therefore recommend you upgrade the web server to version 2.6.

If you upgrade the web server to version 2.5, in which significant improvements have been introduced for the management of TLS certificates, it is important that you confirm the network settings of the web server (with the web server connected to the Internet), so that the web server can upgrade its TLS certificate and download the most up-to-date CA certificate by Vimar.

In version 2.6 of the web server software, some automations and automatic procedures have been introduced for the upgrade of the web server TLS certificate and of the CA certificate by Vimar. Follow the procedures to upgrade the aforementioned certificates as soon as possible for the management of the HTTPS protected connection. With version 2.6, the new firmware version is also available for less recent web servers, which upgrades the TLS protocol to version 1.2, as required by recent directives.

General settings

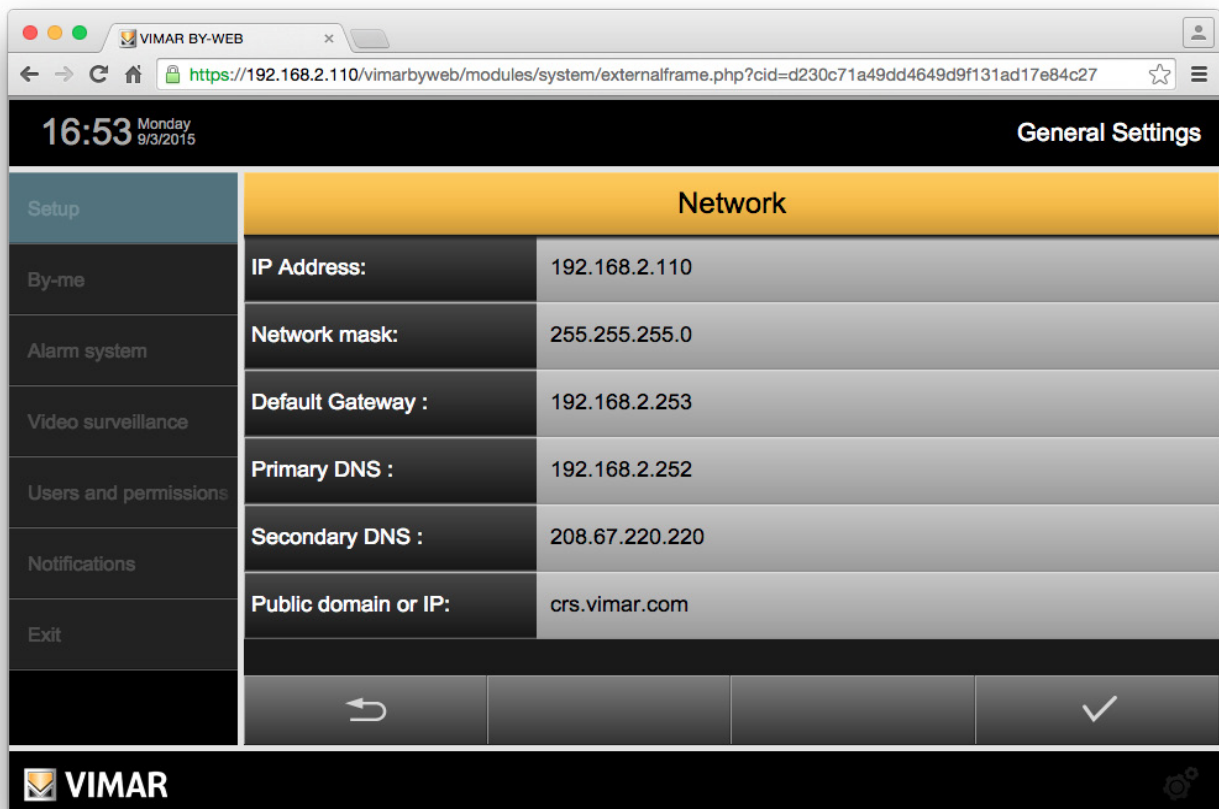
Before describing the procedure for entering the parameters, let's make a small summary of how a network works.

- Remote access to the web server is via the Internet.
 - Each Internet node (host) is uniquely identified by a number (32-bit IPv4, 128-bit IPv6), commonly called IP address.
Example of IPv4 address: 190.230.140.122
 - To make the identification of Internet nodes more easy, it was created a system for associating an alphanumeric string to the IP addresses: DNS (Domain Name System)
For example:
IP Address: 213.178.196.136
DNS Name: www.vimar.com
 - Obviously, for access to an IP node, you must know the address or DNS name associated with it
 - Assigning an IP address to a host can be:
 - static: the address is assigned permanently
 - dynamic: the address assigned is not always the same.A typical example is provided by Internet Service Providers addressing referenced by private users for internet access. The address is typically assigned with each connection (in some cases can also be edited within the same session)
 - To enable access to Internet nodes whose address is dynamically assigned, have been developed services that help create an association between dynamic DNS name (assigned to a user) and IP address. These services are called Dynamic DNS (DDNS Dynamic DNS)
 - Many of the ADSL routers on the market today have native DDNS services support for one or more providers. The router sends the updated IP address to the DDNS after it's been assigned or after the Internet Service Provider has changed the IP address.
 - Typically, configuring a dynamic DNS on a router that supports this technology involves the following steps:
 1. Creating an account on the dynamic DNS provider chosen (e.g. DynDNS.org)
 2. From the Internet configuration menu of the router select the option for Dynamic DNS (Dynamic DNS, DDNS)
 3. Select the Dynamic DNS provider among those managed by the router (typically via a drop down menu)
 4. Type the data provided by dynamic DNS providers in the appropriate fields.
 - For remote access to the Web Server, the following settings are required:
 - Configuration of the IP address of the Web Server in the LAN. The web server has a default configuration of that address. If you need to change that address, access the web server using the default address and change it from the configuration pages. This configuration, to be performed on the router, is need to tell the router that the remote requests on the https port should be addressed to the same LAN address identifying the web server. For this setting, refer to the instruction manual of your router.
 - Configuration of the NAT on the router
 - Check the opening of the https port on the ADSL router (port 443) and, if remote management of the configuration and diagnostics of the By-alarm system via the By-alarm manager software is envisaged, open also the router port that will be mapped in the port used by the By-alarm manager software to access the Web Server.
- NOTE:** If the port 443 of the external interface of the router is already being used by other services, you can use a different port (if not used) but this must be linked to port 443 on the web server (this cannot be changed) by creating a port forwarding rule in the router.
- IMPORTANT:** For safety reasons, configure the router so that only ports 443 (HTTPS) of the web server and the port defined for a remote configuration of the By-alarm control panel (if present in the system) are accessible from outside the LAN.
- If you use dynamic DNS systems, make the relevant configurations
 - The web server uses the HTTPS protocol to increase security of the remote connection between the user and the web server. The protocol uses a specific port (443) to be opened on the router
 - The web server can be used even if the ISP assigns a dynamic IP address.
 - The web server runs natively the dynamic DNS service offered by DynDNS. In this case, carry out the appropriate settings on the pages of the web server. If you use a router that manages the dynamic DNS service chosen by the user natively, set the necessary configurations on the router.

General settings

Enter the following information in the appropriate fields:

IP ADDRESS	Address assigned to the Web Server , characterized by 4 numbers separated by periods. The address must be valid and unique within the LAN, otherwise unable to communicate with the Web Server .
NETWORK MASK	Enter the network mask used by your LAN; unless special requirements, indicate "255.255.255.0".
DEFAULT GATEWAY	In the presence of a router or other device that puts the LAN into communication with other networks or the Internet, enter its address in this field. Otherwise, indicate the same address assigned to the Web Server . NOTE: To use the Remote Web Server, the IP address of the router must be set in the Default Gateway.
PRIMARY DNS SECONDARY DNS	Specify the address of the primary and secondary DNS servers, which are necessary for the functions of Web Server that require internet access. Enter the addresses provided by your ISP; if you these fields blank, the Web Server will use values valid for most configurations.
DOMAIN OR PUBLIC IP	If you want to remotely access to web server 01945-01946, you must set up web server "Domain or Public IP" as well. If you have a static public IP address, you may enter such value. If you have a dynamic IP address and use a dynamic management based on DNS, you must enter the domain. The domain is the part of text included between the protocol and the access port. I.e. if remote access URL is "https://example.dyndns.org:4123", enter this remote access domain - "example.dyndns.org"



The screenshot shows a web browser window with the URL <https://192.168.2.110/vimarbyweb/modules/system/externalframe.php?cid=d230c71a49dd4649d9f131ad17e84c27>. The page title is "General Settings" and the time is 16:53 on Monday, 9/3/2015. The "Network" section is highlighted in yellow. The configuration details are as follows:

Setup	Network	
By-me	IP Address:	192.168.2.110
Alarm system	Network mask:	255.255.255.0
Video surveillance	Default Gateway :	192.168.2.253
Users and permissions	Primary DNS :	192.168.2.252
Notifications	Secondary DNS :	208.67.220.220
Exit	Public domain or IP:	crs.vimar.com

At the bottom of the interface, there is a navigation bar with a back arrow, a checkmark, and the VIMAR logo.

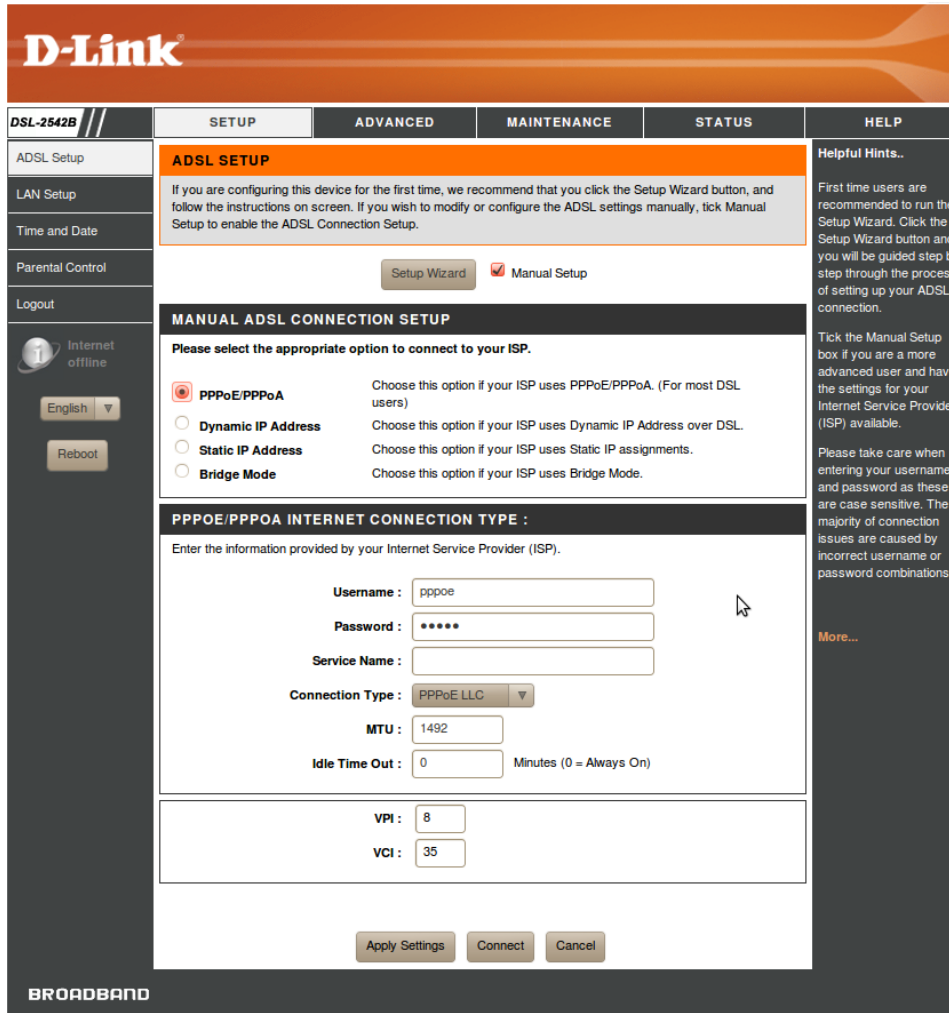
General settings

EXAMPLE OF ROUTER SETTING.

The following example illustrates the steps for setting up the router (opening ports, setting the port forwarding, etc..)

Obviously, the screens will be different depending on the router but the options and parameters used are typically always the same or very similar.

- WAN CONFIGURATION



D-Link

DSL-2542B // SETUP ADVANCED MAINTENANCE STATUS HELP

ADSL Setup
LAN Setup
Time and Date
Parental Control
Logout

Internet offline
English
Reboot

ADSL SETUP

If you are configuring this device for the first time, we recommend that you click the Setup Wizard button, and follow the instructions on screen. If you wish to modify or configure the ADSL settings manually, tick Manual Setup to enable the ADSL Connection Setup.

Setup Wizard Manual Setup

MANUAL ADSL CONNECTION SETUP

Please select the appropriate option to connect to your ISP.

PPPoE/PPPoA Choose this option if your ISP uses PPPoE/PPPoA. (For most DSL users)

Dynamic IP Address Choose this option if your ISP uses Dynamic IP Address over DSL.

Static IP Address Choose this option if your ISP uses Static IP assignments.

Bridge Mode Choose this option if your ISP uses Bridge Mode.

PPPOE/PPPOA INTERNET CONNECTION TYPE :

Enter the information provided by your Internet Service Provider (ISP).

Username : pppoe
Password : *****
Service Name :
Connection Type : PPPoE LLC
MTU : 1492
Idle Time Out : 0 Minutes (0 = Always On)

VPI : 8
VCI : 35

Apply Settings Connect Cancel

BROADBAND

Helpful Hints..

First time users are recommended to run the Setup Wizard. Click the Setup Wizard button and you will be guided step by step through the process of setting up your ADSL connection.

Tick the Manual Setup box if you are a more advanced user and have the settings for your Internet Service Provider (ISP) available.

Please take care when entering your username and password as these are case sensitive. The majority of connection issues are caused by incorrect username or password combinations.


More...

The routers screen above is the one with the WAN settings ("external" network interface of the router towards the Internet world); these settings depend on the Internet Service Provider of the user and **MUST NOT BE CHANGED!!**

General settings

- LAN CONFIGURATION

Product: DSL-2542B Firmware Version: EU_1.00 Hardware Version: D1



DSL-2542B	SETUP	ADVANCED	MAINTENANCE	STATUS	HELP																		
ADSL Setup LAN Setup Time and Date Parental Control Logout Internet offline English ▼ Reboot	<div style="background-color: #f08080; padding: 5px; border: 1px solid black;"> LAN SETUP This section allows you to configure the local network settings of your router. Please note that this section is optional and you should not need to change any of the settings here to get your network up and running. </div> <div style="background-color: #333; color: white; padding: 5px; border: 1px solid black;"> ROUTER SETTINGS Use this section to configure the local network settings of your router. The IP Address that is configured here is the IP Address that you use to access the Web-based management interface. If you change the IP Address here, you may need to adjust your PC's network settings to access the network again. </div> <div style="padding: 5px; border: 1px solid black;"> Router IP Address : <input type="text" value="192.168.0.1"/> Subnet Mask : <input type="text" value="255.255.255.0"/> </div> <div style="background-color: #333; color: white; padding: 5px; border: 1px solid black;"> DHCP SERVER SETTINGS (OPTIONAL) Use this section to configure the built-in DHCP Server to assign IP addresses to the computers on your network. </div> <div style="padding: 5px; border: 1px solid black;"> Enable DHCP Server : <input type="checkbox"/> DHCP IP Address Range : <input type="text"/> to <input type="text"/> DHCP Lease Time : <input type="text"/> (hours) </div> <div style="background-color: #333; color: white; padding: 5px; border: 1px solid black;"> ADD STATIC DHCP (OPTIONAL) </div> <div style="padding: 5px; border: 1px solid black;"> Enable : <input type="checkbox"/> Computer Name : <input type="text"/> << (Computer Name) ▼ IP Address : <input type="text"/> MAC Address : <input type="text"/> <input type="button" value="Copy Your PC's MAC Address"/> <input type="button" value="Save"/> <input type="button" value="Clear"/> </div> <div style="background-color: #333; color: white; padding: 5px; border: 1px solid black;"> STATIC DHCP LIST </div> <table border="1" style="width: 100%; border-collapse: collapse; margin-top: 5px;"> <thead> <tr> <th>State</th> <th>Computer Name</th> <th>MAC Address</th> <th>IP Address</th> <th>Remove</th> <th>Edit</th> </tr> </thead> <tbody> <tr> <td colspan="6" style="text-align: center;">NUMBER OF DYNAMIC DHCP CLIENTS : 0</td> </tr> <tr> <td></td> <td>Computer Name</td> <td>MAC Address</td> <td>IP Address</td> <td>Expire Time</td> <td>Reserve</td> </tr> </tbody> </table> <div style="text-align: center; margin-top: 5px;"> <input type="button" value="Apply Settings"/> <input type="button" value="Cancel"/> </div>				State	Computer Name	MAC Address	IP Address	Remove	Edit	NUMBER OF DYNAMIC DHCP CLIENTS : 0							Computer Name	MAC Address	IP Address	Expire Time	Reserve	Helpful Hints.. If you already have a DHCP server on your network or are using static IP addresses on all the devices on your network, uncheck Enable DHCP Server to disable this feature. If you have devices on your network that should always have fixed IP addresses, add a Static DHCP for each such device. More...
State	Computer Name	MAC Address	IP Address	Remove	Edit																		
NUMBER OF DYNAMIC DHCP CLIENTS : 0																							
	Computer Name	MAC Address	IP Address	Expire Time	Reserve																		

This image shows the router screen with the LAN settings ("internal" network interface of the router, the one of the user's local network); these settings depend on the structure of the LAN of the user and **MUST NOT BE CHANGED!!**

In this example, the router has the (LAN) IP address: **192.168.0.1**.

IMPORTANT: in order to connect remotely to the Web Server, it is necessary that the router and the Web Server are on the same subnet.

General settings

- DYNDNS



D-Link

DSL-2542B // SETUP ADVANCED MAINTENANCE STATUS HELP

DNS SETUP

Domain Name Server (DNS) is a server that translates URL/domain names to the corresponding IP address. Most users will not need to change the DNS servers from default unless instructed by your ISP.

The DDNS feature allows you to host a server (Web, FTP, Game Server, etc...) using a domain name that you have purchased (www.whateveryournameis.com) with your dynamically assigned IP address. Most broadband Internet Service Providers assign dynamic (changing) IP addresses. Using a DDNS service provider, your friends can enter your host name to connect to your game server no matter what your IP address is.

DNS SERVER CONFIGURATION

Obtain DNS server address automatically

Use the following DNS server addresses

Preferred DNS Server : 8.8.8.8

Alternate DNS Server : 8.8.8.8

DDNS CONFIGURATION

Enable Dynamic DNS :

Server Address : DynDNS.org (free) << DynDNS.org (free) (e.g.: myhost.mydomain.net)

Host Name : my.byweb.org

Username : my_username

Password : ••••••

Verify Password : ••••••

Apply Settings Cancel

BROADBAND

Internet offline

English

Reboot

Helpful Hints..

If "Obtain DNS server address automatically" is selected, this router will accept the first received DNS assignment from one of the PPPoA, PPPoE or DHCP enabled PVC(s) during the connection establishment.

If the checkbox is not selected, enter the primary and secondary DNS server IP addresses.

More...

This image shows the screen of the router on the DNS settings and the possible use of dynamic DNS services (e.g. DynDNS).

NOTE: The values entered in DNS and Alternate DNS are purely indicative and not binding.

The data for the management of DynDNS are indicative only and represent the data provided by the user when registering on DynDNS.

With reference to the screen above, the data that must be entered for the configuration of the dynamic DNS service "DynDNS" (in the "DDNS CONFIGURATION" section in the figure) are the following:

- **Server Address:** choice of the dynamic DNS service (the routers used in the example has a drop down menu through which you can make the choice)
- **Host Name:** is the url used to locate the user on the Internet.
It is the data entered by the user during registration on the site of the dynamic DNS service provider and which is dynamically associated with the IP address of the external interface (WAN) of the user's router.
- **Username:** username entered by the user during registration on the site of the dynamic DNS service provider
- **Password:** password entered by the user during registration on the site of the dynamic DNS service provider

General settings

- PORT FORWARDING



D-Link

DSL-2542B // SETUP ADVANCED MAINTENANCE STATUS HELP

PORT FORWARDING

This is the ability to open ports in your Router and re-direct data through those ports to a single PC on your network.

PORT FORWARDING RULES CONFIGURATION

Remaining number of rules that can be created : 32

Pre-defined rule : Application Name
 Custom rule : By-Web

Private IP : 192.168.0.110 << Computer Name

Protocol Type : TCP

Public Start Port : 443

Public End Port : 443

Add/Apply

ACTIVE PORT FORWARDING RULES

Rule Name	Private IP	Protocol Type	Public Start Port	Public End Port	Remove
-----------	------------	---------------	-------------------	-----------------	--------

Helpful Hints...
The device can be configured as a virtual server so that remote users accessing Web or FTP services via the public IP address can be automatically redirected to local servers in the LAN network. Depending on the requested service (TCP/UDP port number), the device redirects the external service request to the appropriate server within the LAN network.

More...

Internet offline
English
Reboot

BROADBAND


This image shows the screen of the router with the port forwarding settings, where a rule for remote access to Vimar web server has been created (the name of the "By-Web" rule is indicative and not binding):

- address of the web server (here the default address is used): 192.168.0.110
- opening of port 443 (required for access to the web server)

2.4 Updates

This page allows you to upgrade your version of the software inside the Web Server.

To do this, proceed as follows.

1. Access the configuration menu using the icon  and select **Setup -> Update**
The software Update window appears that displays the current software version of the Web Server.
2. Press the button "**Choose File**" (or "**browse**", depending on your browser) and select the installation package received, which must be present in the PC used to access the Web Server
3. Go to the next screen by pressing "**Confirm**"
4. Select "**Add File**"
5. Press the "**Update Software**" button The installation procedures may require Several minutes.
6. At the end of the update process you will need to restart your Web Server by pressing "**Restart Now**".
7. Wait about 2 minutes to log back in to the Web Server (refresh the page in the browser).

After restart, the web server might request to load the XML system file.

NOTA: in case of occurrence of error messages on the screen, please contact customer support Vimar.

IMPORTANT: In version 2.6 significant functions and upgrades have been introduced concerning the management of the HTTPS protected connection between the web server and the clients used to access the web server.
We recommend you check the current software version of the web server and, if you have not yet upgraded to version 2.6, we recommend you perform this upgrade as soon as possible.
For web servers with less recent hardware revisions, to make certain important upgrades for the management of the HTTPS protected connection, after performing the upgrade to version 2.6, the web server will display a warning message with instructions on performing the "Firmware Upgrade" procedure; this procedure is described in the following chapter.
For additional information about versions 2.5 and 2.6 of the web server software, please refer to the chapter entitled "The significant upgrades introduced in versions 2.5 and 2.6 of the web server software for the management of the HTTPS protected connection" in the manual herein.

General settings

2.5 Firmware Upgrade

A "Firmware Upgrade" function (upgrade of the web server firmware) was introduced in version 2.6 of the web server software, which allows you to perform upgrades to the web server operating system which cannot be performed using the usual software upgrade packages.

The firmware upgrade procedure does not replace the "software upgrade" procedure performed by loading in the web server the upgrade packages available on the Vimar website, and it will be used to manage specific upgrade requirements.

If connected to the Internet, the web server performs a regular check for the availability of a new firmware version for the web server: in the event that it detects the availability of a new firmware version, it will present the user with a warning message, prompting the launch of the "Firmware upgrade" procedure, as described below.

The firmware upgrade procedure can be launched from the dedicated page, which can be accessed using the "Firmware Upgrade" button in the "Setup" menu of the "General settings" section (for users who have the credentials to access the aforementioned section).

IMPORTANT: The web server firmware upgrade is a procedure that can only be performed if the web server is connected to the Internet; the web server displays the warning messages if it cannot access the Internet.

By accessing the "Firmware Upgrade" page, if the web server is connected to the Internet, it performs a check for the availability of a new firmware:

- If a new firmware version is not available, the window displays: Current firmware version and firmware version available. For web servers which have never undergone a firmware upgrade and for which no new firmware version is available, the following texts will be displayed: NO VERSION and NO AVAILABLE VERSION.

NOTE: for web servers which have never undergone a firmware upgrade and for which no new firmware version is available, the following texts will be displayed: NO VERSION and NO AVAILABLE VERSION (this is the case of the most recent web servers produced by Vimar).

- If a new firmware version is available:
 - The field with the current firmware version will differ from the one with the firmware version available.
 - A warning text is displayed, with the important rules that need to be respected for the upgrade procedure to be performed successfully.
 - The "Firmware Upgrade" field is displayed, with the "Start" push button to launch the firmware upgrade procedure.

IMPORTANT: if the "Firmware Upgrade" procedure is interrupted, the web server may no longer be accessible, and you should request support from Vimar.

The "Firmware Upgrade" procedure envisages the following steps, which must be respected for the firmware upgrade to be successful:

1. **Perform an export of the web server database (creation of a backup copy of the web server database).**
From version 2.6 of the web server software, this procedure also performs a backup of the Energy Monitoring data stored in the internal FLASH memory of the web server.
2. **Restore the web server database to the factory data. This is a vital step and failure to perform it could compromise the operation of the web server.**
3. **Start the "Firmware Upgrade" procedure by pressing the "Start" push button situated to the right of the "Firmware Upgrade" field.**
4. **Once the "Firmware Upgrade" procedure is complete, import the copy of the database you created in previous point 1 into the web server.**

IMPORTANT: you need to respect the following rules for the firmware upgrade procedure to be successful. Failure to respect the following rules could compromise the operation of the web server.

- Do NOT cut off the electricity supply to the web server during the "Firmware Upgrade" procedure.
- Do NOT cut off the Internet connection to the web server during the "Firmware Upgrade" procedure.
- Do NOT exit the browser page during the "Firmware Upgrade" procedure

The Firmware upgrade procedure may take up to an hour: the length of the procedure also depends on the speed of your Internet connection.

If the firmware upgrade procedure has been launched without the web server being able to access the Internet, the firmware upgrade procedure may not be performed and a warning message will be displayed.

During the firmware upgrade procedure, a black screen is displayed with a upgrade procedure progress bar.

In the event of an error during the upgrade procedure, the error will be signalled by the web server and you will need to contact Vimar for support.

NOTE: after a firmware upgrade, you may need to delete the Google Chrome browser history data (please refer to the browser documentation to do this); perform this operation, for instance, if after the firmware upgrade procedure and after restarting the web server, the page with the Vimar logo is displayed, but the web server login window fails to appear within ten seconds or so, or in other circumstances in which there are anomalies in the graphic presentation of the web server pages.

General settings

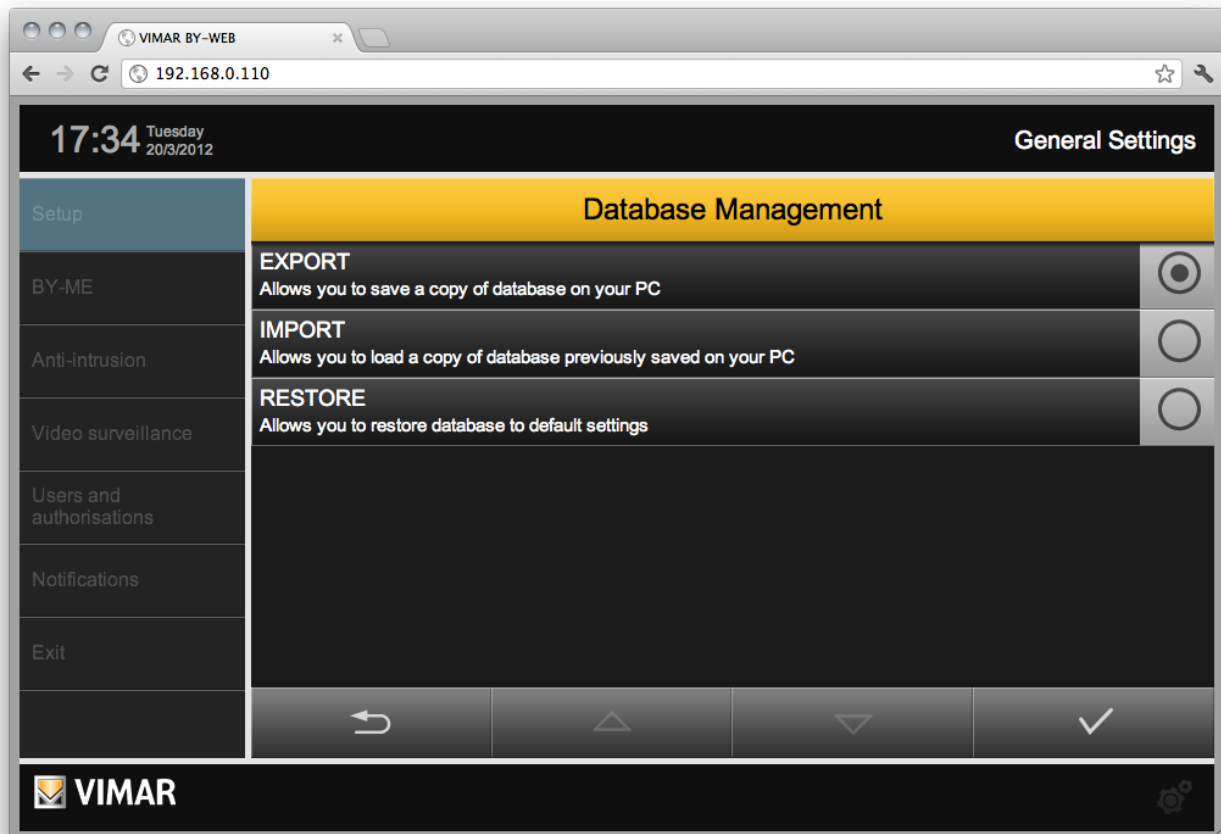
2.6 Database

This page allows you to operate on the **Web Server** database, which contains the configuration of the supervising project; you can do the following by selecting the corresponding item from the list:

EXPORT	It allows you to export a backup of the database and save it on your PC in order to load it later on the same or a different Web Server .
IMPORT	It allows you to load a backup of the database previously saved on your PC from the same or a different Web Server .
RESTORE	It allows you to restore the Web Server database to its defaults. Note: this does not restore the original IP address of the Web Server .

NOTE: up to version 2.5 (included) of the web server software, the database importing and exporting operations do not affect the Energy Monitoring data saved in the internal FLASH memory of the web server.
Starting with version 2.5, the web server database importing and exporting operations also concern the energy monitoring data saved in the internal FLASH memory of the web server.

After selecting the desired item, use the ENTER button available from the button panel to start the procedure, which can take several minutes, during which it is important neither to perform any other operation on the **Web Server**, nor close the browser window.



General settings

2.7 Backgrounds

The following commands are available:

EXPORT	<p>Saves a backup copy of web server background images in the PC. Procedure:</p> <ol style="list-style-type: none"> 1. Select "Export". 2. Press the confirmation button ✓. 3. After the processing phase done by the web server (where a warning message appears), the file will be saved in the PC according to browser settings for file download (refer to your browser documentation).
IMPORT	<p>Loads a backup copy of backgrounds, previously saved in the PC. Procedure:</p> <ol style="list-style-type: none"> 1. Select "Import". 2. Press "Select file" button. The system navigation window appears. 3. Select the background images backup file previously saved in the PC (as described on "Export" procedure) and press "Open" button. 4. Press the confirmation button ✓.

2.8 SD Memory Management

The web server has one slot for SD memory cards. Some features of the web server require a SD memory card correctly activated (i.e. video messages).

If there is an operating SD memory card at the web server start up, this will be automatically discovered and activated by the web server.

In order to be used by the web server, a SD memory card must be correctly inserted and activated by the web server.

The "SD Memory Management" page allows you to verify if a SD memory card is present and its activation status, with activation/deactivation controls.

MEMORY AVAILABLE	<p>Shows the presence status of a SD memory card inside the web server slot: Possible statuses:</p> <ul style="list-style-type: none"> • No: a SD memory card is not inserted into the web server slot, or it has been inserted but not discovered by the web server (non compatible or damaged SD memory card). • Yes: a SD memory card is correctly inserted into the web server slot and it is correctly discovered by the web server.
ACTIVE	<p>Enables a SD memory card inserted into the web server and currently inactive. To activate a SD memory card, press "...".</p>
INACTIVE	<p>DEACTIVATES A SD MEMORY CARD INSERTED AND ACTIVATED INTO THE WEB SERVER. THIS OPERATION IS REQUIRED BEFORE REMOVING A SD MEMORY CARD FROM THE WEB SERVER WITHOUT SHUTTING DOWN THE WEB SERVER FIRST. TO DEACTIVATE A SD MEMORY CARD, PRESS "...".</p>

2.9 Date / Time

This page allows you to set the following **Web Server** parameters for the system clock:

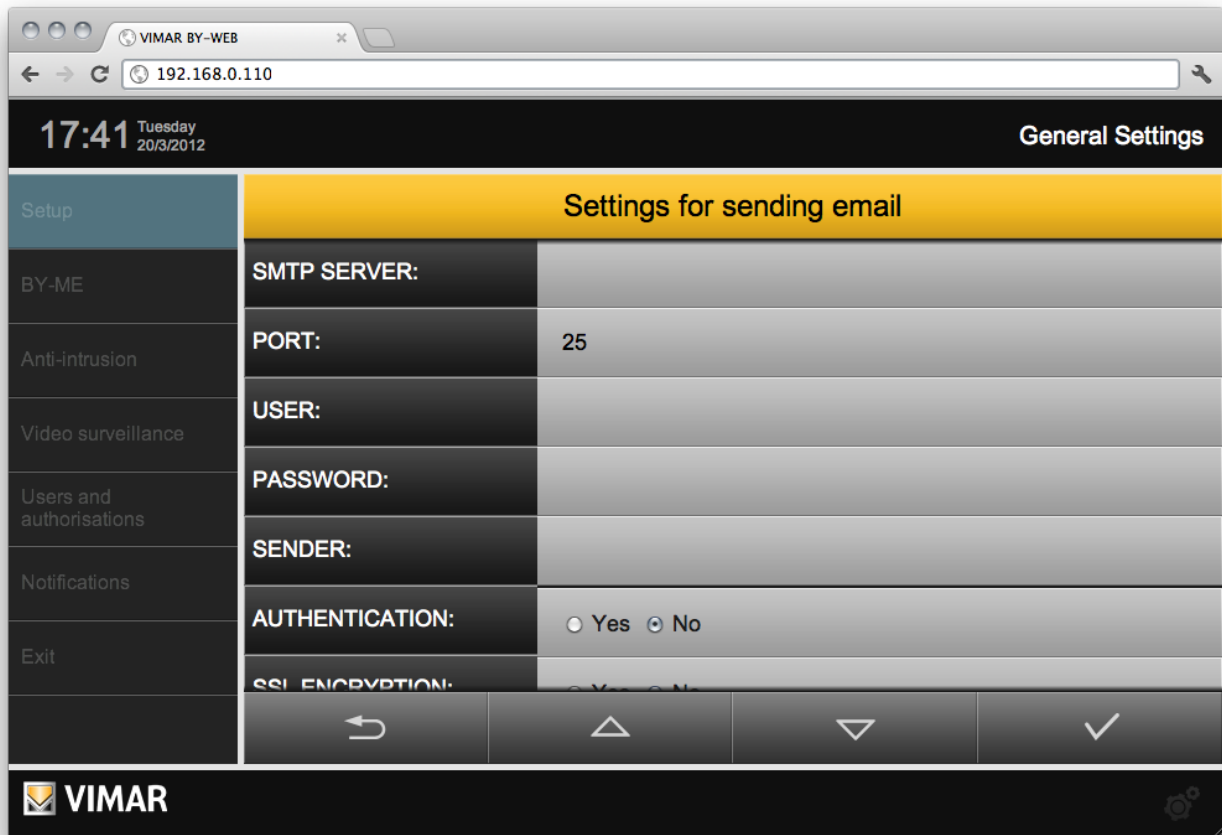
TIME	Allows you to set the system time of the Web Server .
DATE	Allows you to set the system date of the Web Server .
TIME ZONE	Allows you to select the time zone of the country or region in which you installed the Web Server .

General settings

2.10 Email

This page allows you to set the parameters required for sending alarm notifications of the Alarm System (SAI) by email.

Warning: it is necessary that the SAI system is properly installed and working, and that the web server has been properly configured.



In particular, the page allows you to set the following parameters (consult your email provider to find out what values to specify):

SMTP SERVER	Address of the mail server used for sending messages.
PORT	Port used to connect to the SMTP server.
USER	Account (usually the full email address) with which to logon to the SMTP server.
PASSWORD	Password to login to the SMTP server.
SENDER	Specify the email address to be used to send the messages; if in doubt, re-enter the email address specified as "USER".
AUTHENTICATION	Specify if the SMTP server requires authentication.
SSL ENCRYPTION	Specify if the SMTP server requires SSL encryption.

IMPORTANT: The web server makes it possible to use SMTP servers that envisage access via a *Username* and a *Password*. To use the Google Gmail SMTP server, please refer to chapter 14 "Using the Google Mail SMTP service to send web server e-mail notifications" in this manual.

General settings

2.11 DYNDNS

This page allows you to set up the dynamic DNS client embedded in **Web Server**; this feature allows you to access the Internet through your home automation system even in the absence of a static public IP address. To do this you must do the following:

- Open a browser window on WWW.DYNDNS.ORG
- Create a new account by following the instructions on the site
- From the main panel of your newly created account, select "ADD HOST SERVICES"
- Enter a name for the system and choose one of the available extensions; then click "HOST WITH IP ADDRESS" as a type
- Insert the new service in the cart and finalize your (free) creation of the dynamic domain. Example: "domainname" as the name, "dyndns.org" as the extension.

Once completed, set the network configuration page of the **Web Server** with the following parameters, from the Dynamic DNS section:

USER NAME	Username of the DYNDNS.ORG account.
PASSWORD	Password required to access your DYNDNS.ORG account.
DOMAIN NAME	The name previously assigned to the domain, including the extension and devoid of any protocol indications; for example: domainname.dyndns.org

NOTE: The dynamic DNS client integrated with the Web Server works only with the accounts created on WWW.DYNDNS.ORG

Once finished entering the configuration parameters, save by the special CONFIRM button. If you changed the IP address of the **Web Server**, from now on it will be available at the new address, after waiting for the time necessary to restart the network services.

Configuring the dynamic DNS client, also starts an automatic periodic refresh of the domain with its own public IP address; each time the IP address is changed by the internet provider, the next update will be update the association between domain and IP address, allowing remote access (the update may take several minutes).

2.12 ByWeb Tools

This page provides the description of ByWeb Tools by Vimar and the corresponding installation procedure. The same page is shown by the Web server if needed, automatically if the project file By-me is imported and in case of RTSP video streaming.

By-me configuration

3. By-me configuration

3.1 Getting Started

In order for the Web Server to handle the By-me system, it is necessary to change the configurations involving the By-me system and the Web Server itself.

To complete the configuration YOU MUST use the EasyTool Professional software or use the LT EasyTool Professional software.

IMPORTANT: The recommended procedure requires the use of EasyTool Professional for the configuration of both the By-me system and the Web Server, as described below.

3.1.1 System configuration using EasyTool Professional

The procedure involves the following steps:

- Configure all devices in the system through EasyTool Professional
- Configure all the evolved interfaces (Touch Screen, GSM...) through EasyTool Professional
- Configure the Web Server via EasyTool Professional.

Note: The configuration of the Web Server within EasyTool Professional, if necessary, automatically opens the router in the By-me system

- After configuring the entire system, download the database to the Control unit
- After configuring the whole system, create, still through EasyTool Professional, the xml file and import it into the Web Server, using the appropriate configuration section

Attention: With every change in the structure of the By-me system, performed with the aid of EasyTool Professional, you must load the new database into the control unit and keep creating the xml file and importing it into the Web Server.

3.1.2 System configuration using the control unit

The procedure involves the following steps:

- Configure the system devices, including the Web Server, through the By-me control unit
- Execute the authentication if the system is equipped with the alarm system

IMPORTANT: this step is not necessary when the Web Server is configured using EasyTool Professional

- Open the router manually from the Control unit
- Import the Control unit database to EasyTool Professional LT/EasyTool Professional
- Through EasyTool Professional LT/EasyTool Professional create the xml file and import it into the Web Server

Note: With every change in the structure of the By-me system, performed with the aid of the control unit, you must load the new database into EasyTool Professional LT/EasyTool Professional and keep creating the xml file and importing it into the Web Server. If the installer adds new groups from the Control unit, the router must be opened manually, if necessary.

3.2 Configuration

Once completed the XML project import, you must carry out the "Configuration" of the **Web Server** on the control unit or EasyTool Professional, as with other devices of the By-me system (by which the physical address is assigned to the Web Server).

To do this, proceed as follows:

- Access the **By-web** administration page, select the "BY-ME" from the main menu and then "Configuration"
- A popup is displayed, that describes the steps performed from the **Web Server**.
- After completing the configuration successfully, press the confirm button from the popup.

During the opening of the popup, the **Web Server** is in programming mode; avoid configuring other **By-me** devices, as the **Web Server** might respond to messages sent from the control unit and prevent the completion of these operations.

By-me configuration

3.3 Importing the By-me project

Access the GENERAL SETTINGS, select "By-me" from the main menu and, after opening the sub-menu, "Import XML".

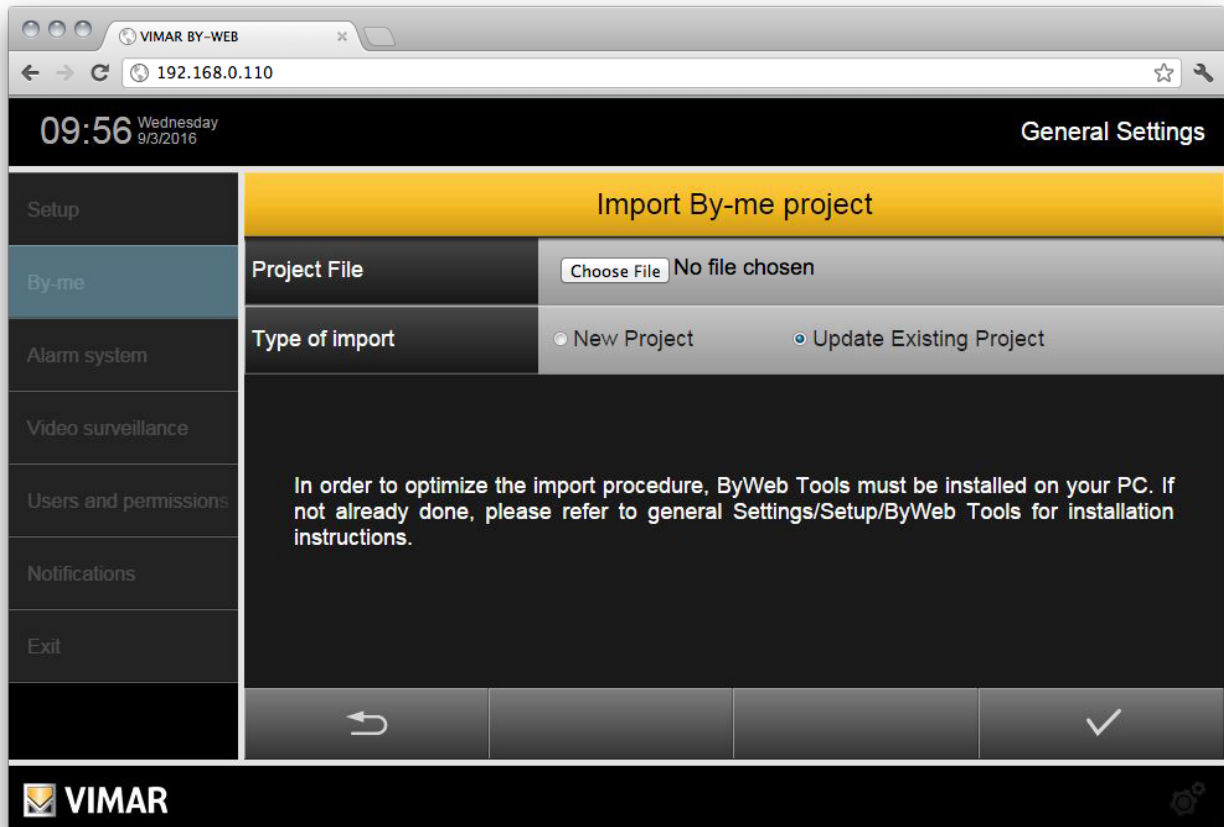
Through this procedure, the Web Server is provided with the By-me system data.

In addition to the standard import procedure, the Web Server provides for a new procedure to reduce the import times that involves the use of the ByWeb Tools applet by Vimar.

For information about the installation of ByWeb Tools refer to chapter 12. ByWeb Tools by Vimar of this manual.

If ByWeb Tools has already been installed and the minimum requirements are met, the Web Server shows the following page.

Otherwise, before showing that page, another page is displayed with the description of ByWeb Tools and the instructions for installation on the computer from which the import is taking place, with the ability to start the installation of ByWeb Tools or to proceed with the import by following the standard import procedure.



Click on the "choose file" or "browse" button (depending on the browser) and select the XML project file on your PC previously imported from EasyTool Professional LT/EasyTool Professional.

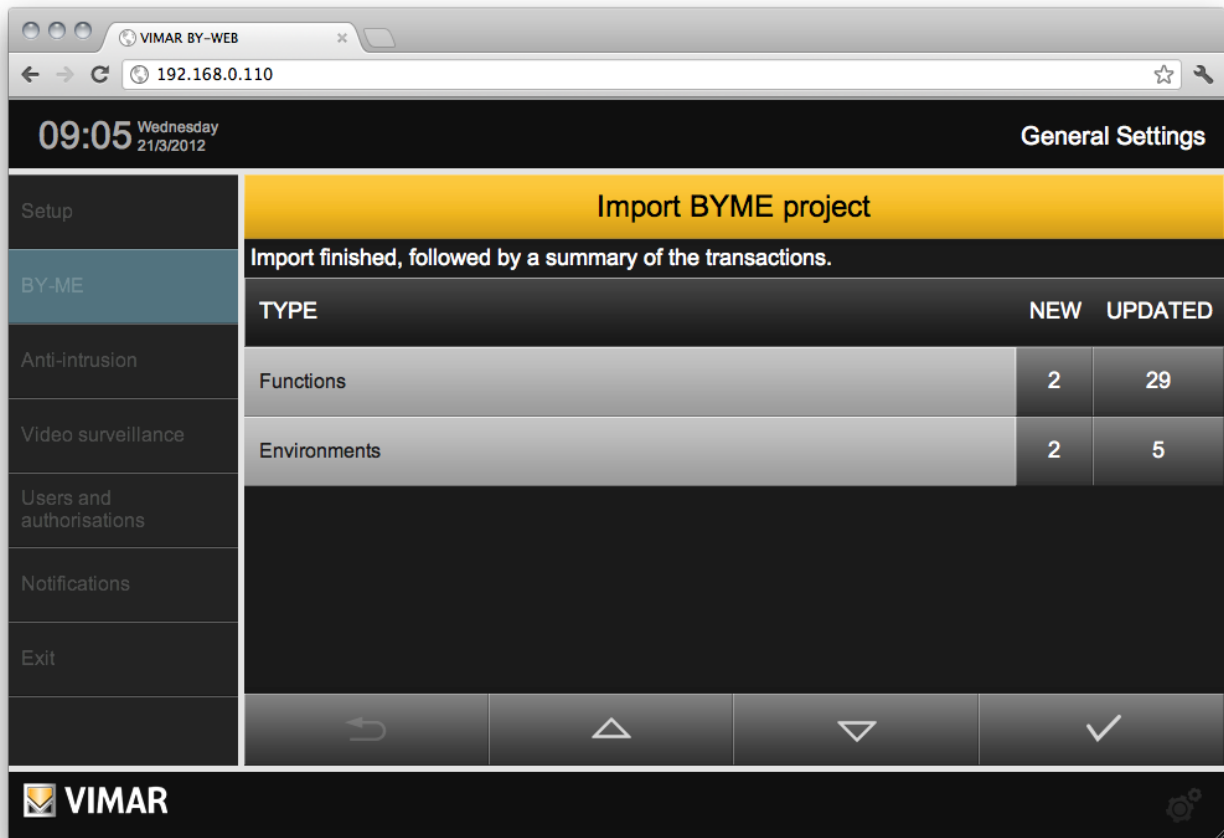
In case you have already imported a project into the **Web Server**, you must specify whether the new file should be considered as an update of the previous one (in this case, select "update existing project"), or a new project; in this case all the **By-me** devices will be removed from the **Web Server** before proceeding with the import.

After you specifying the type of import, click the Confirm button at the bottom right and wait for the completion of the procedure; the operation may take several minutes depending on the size of the project, during which it is recommended neither to do any other operations, nor to close the browser window, to avoid serious malfunction of the **Web Server**.

If the **By-me** system project involves the use of Master Group, the **Web Server** displays a page for choosing the representative for displaying the status of each Master Group.

By-me configuration

After the procedure, a summary of the operations carried out is displayed:



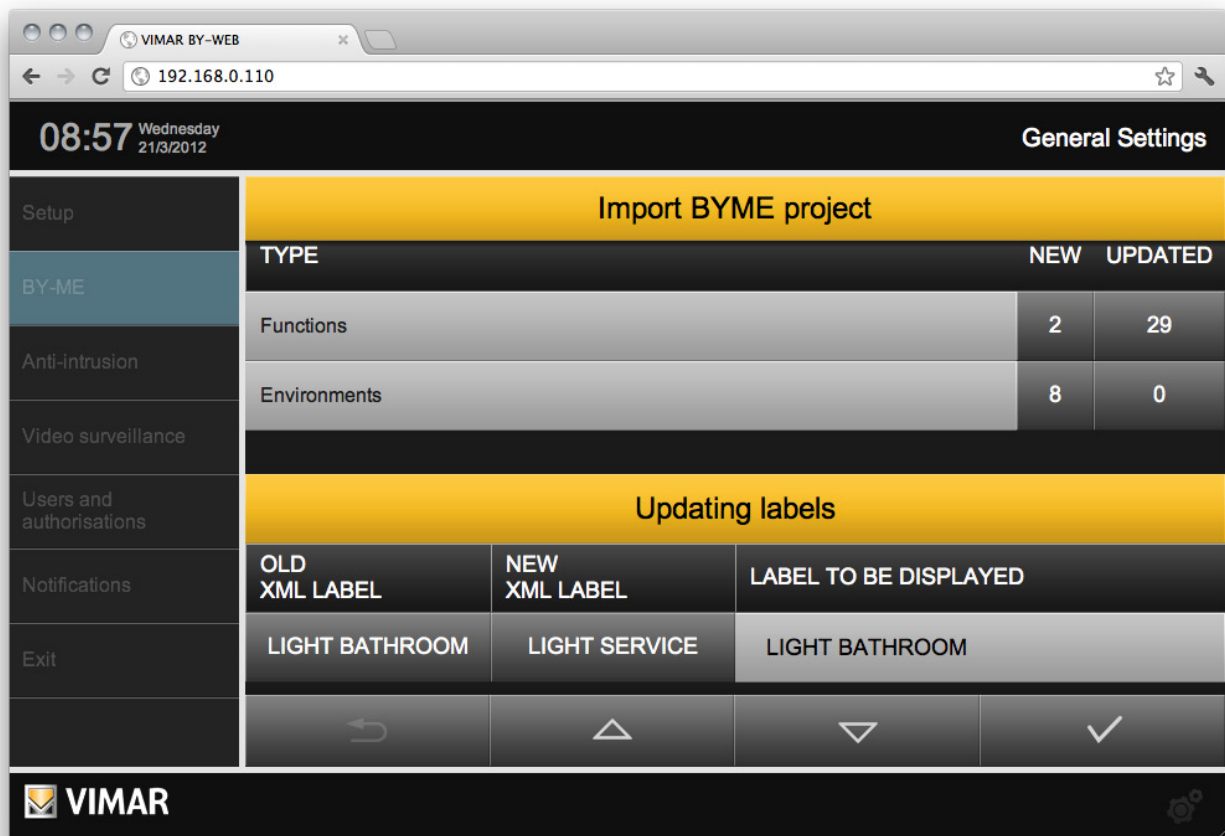
The screenshot shows a web browser window titled 'VIMAR BY-WEB' with the address '192.168.0.110'. The page displays the time '09:05 Wednesday 21/3/2012' and 'General Settings'. A navigation menu on the left includes 'Setup', 'BY-ME', 'Anti-intrusion', 'Video surveillance', 'Users and authorisations', 'Notifications', and 'Exit'. The main content area is titled 'Import BYME project' and contains the message 'Import finished, followed by a summary of the transactions.' Below this is a table with the following data:

TYPE	NEW	UPDATED
Functions	2	29
Environments	2	5

At the bottom of the interface, there is a VIMAR logo and a set of navigation icons: a back arrow, an up arrow, a down arrow, and a checkmark.

In the case of updating an existing project, the **Web Server** detects any devices whose name has changed since the previous version, and displays a list of these differences, as shown in the following example:

By-me configuration



Import BYME project		
TYPE	NEW	UPDATED
Functions	2	29
Environments	8	0

Updating labels		
OLD XML LABEL	NEW XML LABEL	LABEL TO BE DISPLAYED
LIGHT BATHROOM	LIGHT SERVICE	LIGHT BATHROOM

Simply click on the new or previous label to automatically set it in the space on the right, which is the name that will be used in the pages of the **Web Server**; you can also specify a completely different custom label from that present in the XML file.

After this, confirm the summary and any changes to the names through the confirmation button at the bottom right. The **Web Server** is then prepared to manage the new project; even in this case, this may take several minutes, during which it is recommended not to perform any other operation on the page.

Once this process is complete, you are automatically redirected to the environment management page.




IMPORTANT: do not import the By-me system XML files on more than one web server, simultaneously, from the same PC.

By-me configuration

3.4 Environments

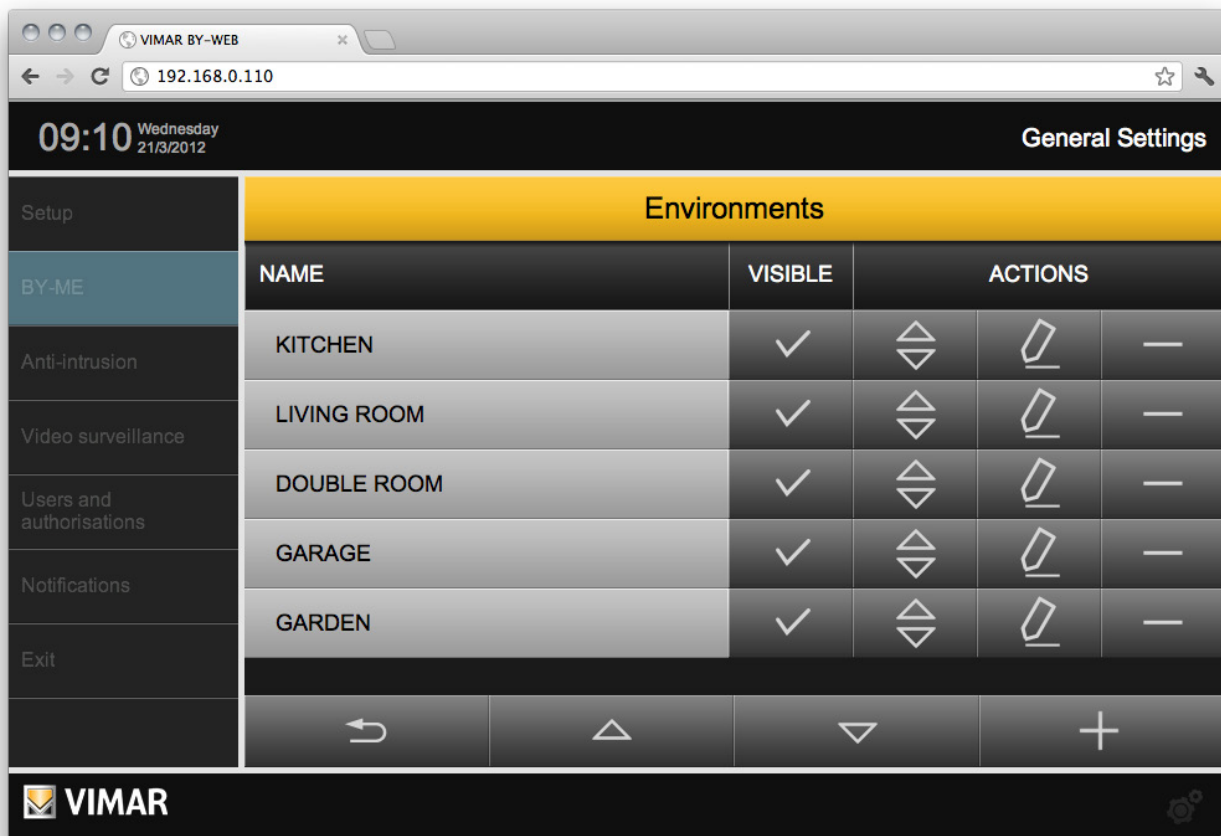
If the imported XML project contains the information on the location of the devices environment, they are automatically created within the **Web Server**. By selecting "environments" from the "**By-me**" menu of the settings you can customize this list, thus defining the graphic pages where the user can manage the devices in the home automation system.




















The installers can change the name of the existing environments directly from the main page; they can also specify whether or not they should be visible to the end user (selecting the appropriate box); from the list, the following operations can also be performed on each entry:

	<p>CHANGE ORDER Drag this button to change the display order of the environments in the corresponding Web Server menu.</p>
	<p>EDIT Allows access to the environment details, as described below.</p>
	<p>DELETE Deletes the environment from the Web Server. This operation, subject to confirmation by the installer, cannot be subsequently canceled. Note: Devices that may be present in the environment are not deleted, only removed from the deleted environment; they are still visible in any other environments that contain them, as well as in their function pages.</p>

NOTE: these parameters are changed in real time whenever "ENTER" is pressed (in the case of text boxes), when the selection of a drop-down menu is changed or selecting another location on the page after changing a value. No need for pressing any buttons to save or confirm.

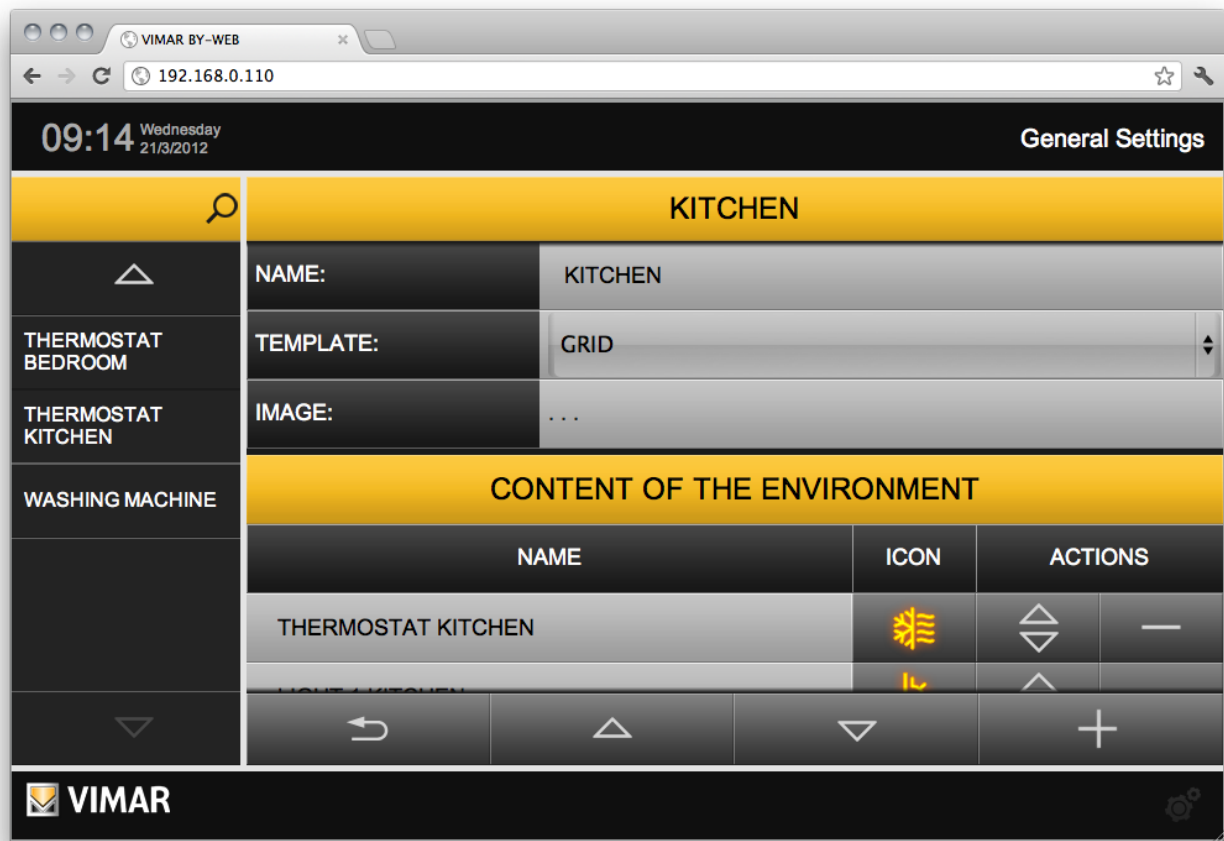
You can also create new environments by using the "ADD" button available in the lower panel; the new environments are temporarily placed at the bottom of the list, after which they can be moved by clicking the "CHANGE ORDER" button.



Setup		Environments			
BY-ME	NAME	VISIBLE	ACTIONS		
Anti-intrusion	KITCHEN	✓			
Video surveillance	LIVING ROOM	✓			
Users and authorisations	DOUBLE ROOM	✓			
Notifications	GARAGE	✓			
Exit	GARDEN	✓			
					

By-me configuration

The "EDIT" button displays the detail tab of the environment:



The first part of this page allows you to:

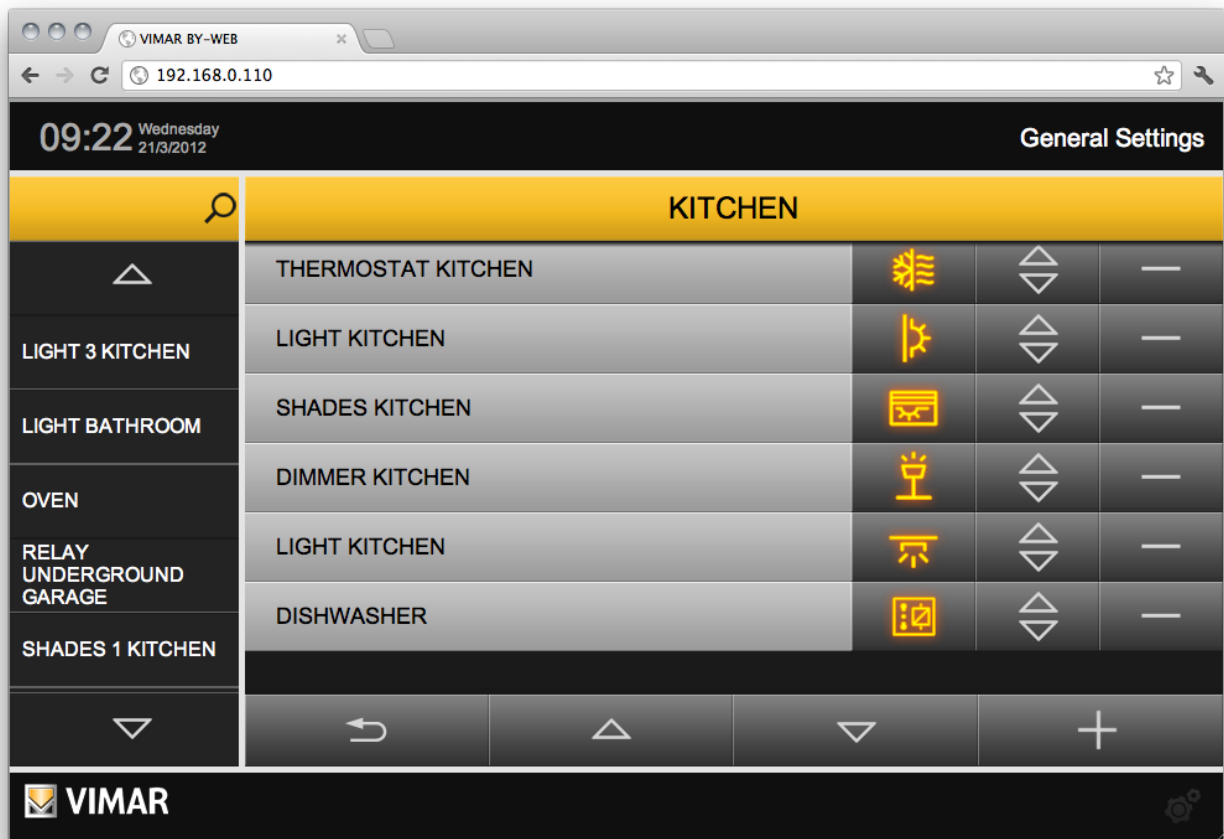
- Set the environment name that will appear in the environments menu of the **Web Server**.
- View the description associated with the environment, as set in the XML project (for environments created during the import).
- Specify if the environment is to be displayed to the user as a GRID (table containing the devices) or MAP (devices placed freely on a background image).
- Associate an image to the environment itself, which appears on the side of the environment page, in the case of GRID display, or used as a background for the MAP display.

Simply clicking on the image selection opens a popup window, which lets you select an image already present on the **Web Server**, or load a new one (through the "ADD" button) by selecting it from your PC.

IMPORTANT: For background images do not load images wider than 800 pixels. For images displayed on the grid, the images must be no larger than 120 pixels x 425 pixels (width x height).

- Enable protection with the PIN code of the room and set the relevant PIN code. By default the "Access with PIN" parameter is set to "No". Setting the "Access with PIN" parameter" to "Yes" displays the fields for entering and confirming the PIN (numerical code with a number of digits between 4 and 6)

By-me configuration



The second part of the page (identified by the title "ENVIRONMENT CONTENT"), instead, allows to determine which devices should be displayed on the page of the selected environment; if the environment has been created while importing the XML project, the list already contains project elements associated with the current environment, otherwise the list is initially empty.

In a similar way to what happens in the list of environments, described previously, the list of the devices allows to:

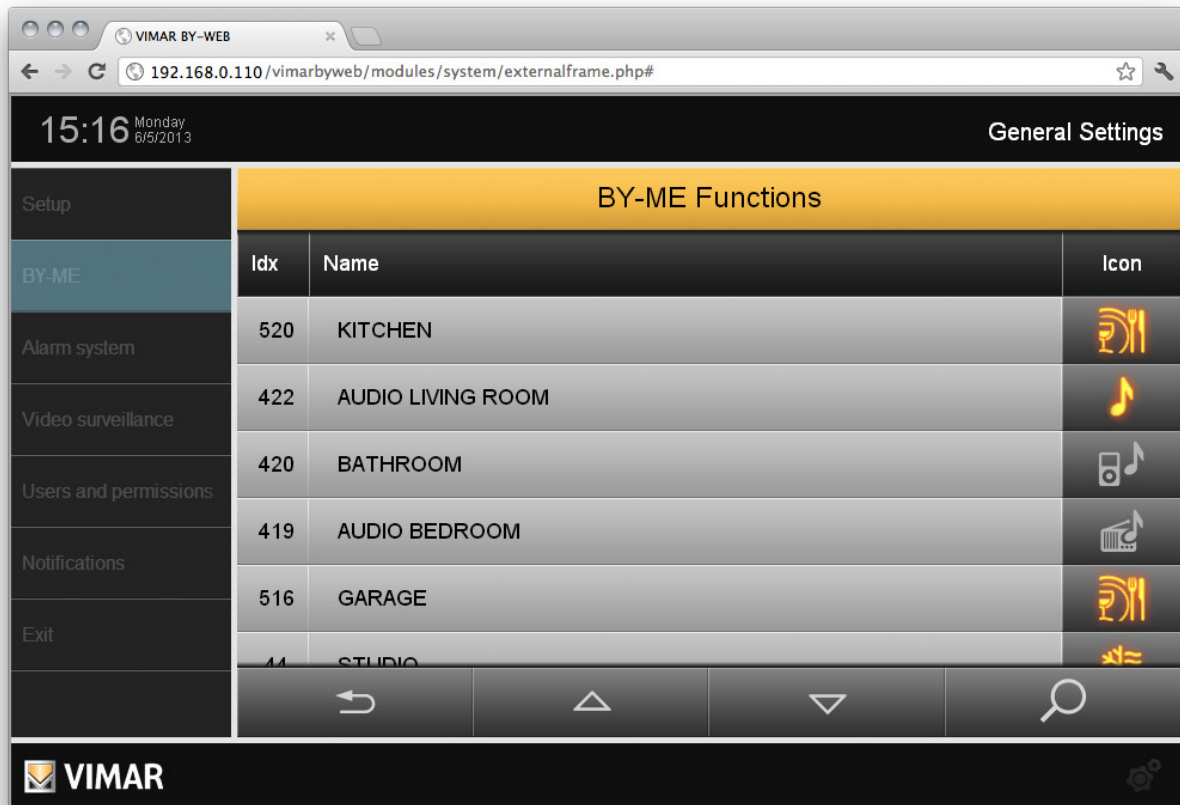
- Change the name of the devices, compared to that set when importing the XML project.
- Customize the identification icon of the device: clicking on the button containing a preview of the current icon opens a popup that shows the possible icons you (the list depends on the type of selected feature), selecting an image it is assigned to the device and the popup is closed automatically.
- Change the order of the device within the environment, dragging it to the top or bottom of the list.
Note: the order is not influential in the case of MAP display of the current environment, since the arrangement will be established for each device in the next phases.
- Remove the device from the current environment, to be confirmed.

The device list can be consulted through the vertical scroll buttons found in the bottom panel; using the "ADD" button is also possible to add other devices the current environment. Pressing the button displays (in the space usually occupied by the main menu) a search engine on the side, showing a list of all devices in the project, that can be filtered through one or more keywords to be inserted in the initial text box; you can simply drag the devices you want to ADD to the current environment one by one, to the chosen position within the device list, to create the pairing. To exit the environment detail page, use the "BACK" button from the lower panel.

By-me configuration

3.5 BY-ME Functions

By selecting "BY-ME Functions" from the "BY-ME" submenu in "General Settings", you will see a list of all the devices (units) in the BY-ME system.



From the list of devices you can:

- Change the name of the devices, compared to that set when importing the XML project: edit the text field directly.
- Customize the identification icon of the device: clicking on the button containing a preview of the current icon, opens a popup window showing the possible icons (the list depends on the type of selected feature). Selecting an image assigns it to the device and the popup window is closed automatically.
- Set specific parameters of the device or related graphic object on the Web Server: for certain devices, the page that opens when the device icon button is clicked allows you to select the icon representing the device and to make various other settings as described in the following chapters, concerning:
 - KNX Weather Station min/max values automatic reset setting.
 - Device widget customized behaviour management.

Using the Search/filter button at the bottom right of the list, you can view the devices whose name includes the string you want. This function is useful to speed up the identification of specific devices, in the case where the list of devices is particularly long.

CAUTION: For the flush-mounted controls only (art. 01480, 01481, 01482, 01485, 01486 and 01487), the function of pressing the button briefly or holding it down dynamically change the behaviour of the timer actuator (from monostable timed to bistable or vice versa) configured in the same group.

3.5.1 Configuring the automatic reset of the min/max values of the KNX weather station

Apart from allowing the manual reset of the max/min temperature and max wind speed (refer to the user manual), the Web server also allows to automatically reset these max/min values every day at midnight.

To enable this automatic feature, proceed as follows.

1. Navigate to the "General Settings" section.
2. Select "Functions By-me" from the "By-me" submenu.
3. Look for rows in the list relating to the weather stations in the system.

NOTE: To facilitate this operation, use the Search/filter button at the bottom right of the list by using a text string that identifies the weather stations for the search (eg. if there are two weather stations: "Weather Station 1" and "Weather Station 2", for the search use text "weather" or "Weather Station")

4. For each weather station whose min/max values automatic reset you want to set, perform the following steps.
5. Press the icon corresponding to the weather station. A weather station window appears.
6. To activate the automatic reset of the min/max temperature and maximum wind speed, enable "Enable min/max periodic reset" (This operation is confirmed by the appearance of a warning message reminding that the min/max values will be reset every day at 00:00).

The difference between disabling and enabling this function is given by point 6), where "Enable min/max periodic reset" is disabled (Also the disabling of the automatic reset is confirmed by the appearance of a message alert).

By-me configuration

3.5.2 Device widget customized behaviour management

For several devices and in specific system configurations, device widget behaviour can be modified with respect to the default settings provided by the web server.

This possibility allows a response to various specific supervision requirements of By-me system devices, making it possible to decide on the behaviour of the device widget in relation to device status display and command transmission to the device.

To make this setting, for compatible devices and system configurations, access the "By-me Functions" page, pressing the icon of the device in question: the "Custom management" setting appears at the bottom of the page.

You can set up the behaviour of the device widget by selecting one of the available options in the drop-down menu:

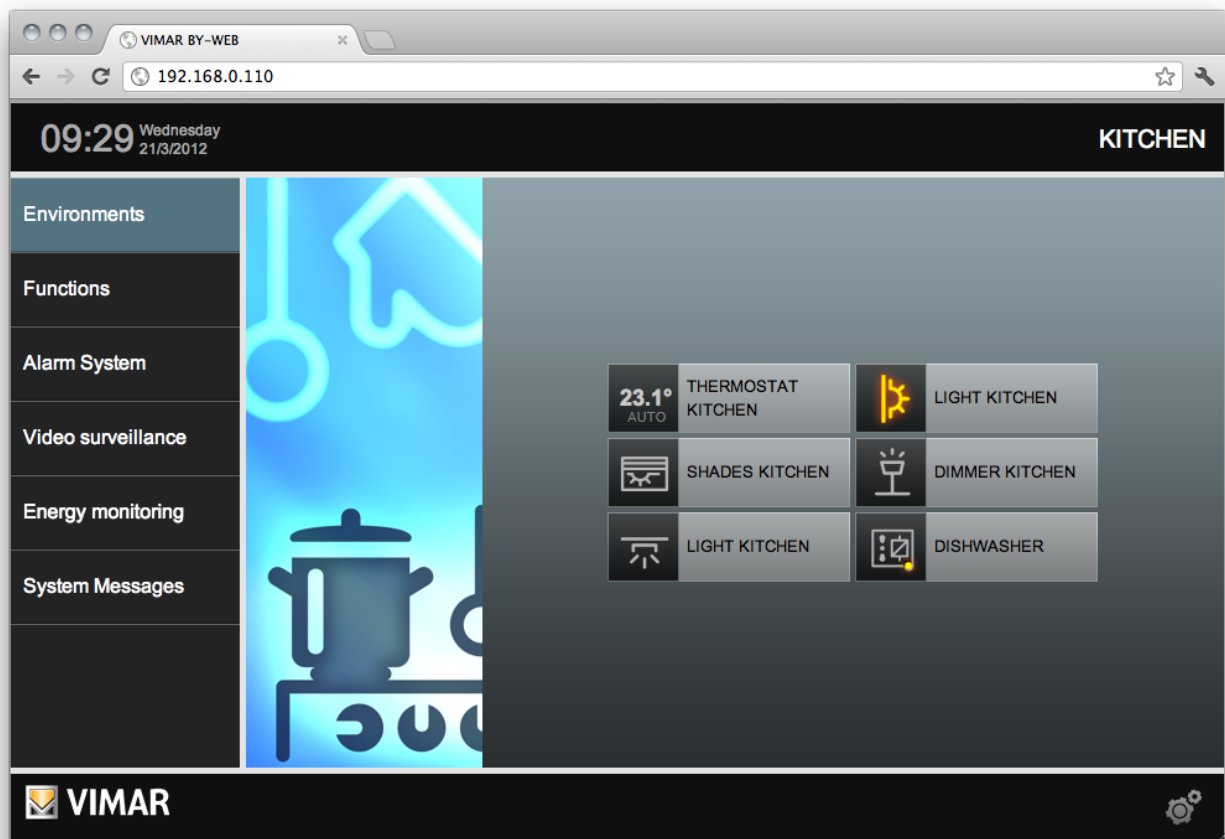
Menu option	Description
---	No customized setting. The widget behaves as envisaged by the web server for the device and system configuration in question.
State only	The device widget allows status display only and does not allow the command to be transmitted to the device.
Command only	The device widget only allows the command to be transmitted but does not allow device status display.
State + Command	The device widget allows both status display and also command transmission to the device.

3.6 Browsing by environments

After customizing the environments, the **Web Server** can be used for the supervision of the **By-me** system, at least for functions related to automation and sound system. Through the "EXIT" button in the main menu of the settings you can return to the home screen.

Through the main menu, always available on the left side of the page, the end user can browse the environments previously configured through the "ENVIRONMENTS" entry; pressing this button will open a sub-menu that contains the list of available environments. If the number of applications exceeds the maximum height available on the page, two vertical scroll buttons are shown.

Selecting an environment from the list, loads its contents in the main part of the page; in the case of GRID display, the devices associated with the environment are shown in the table, each characterized by a button composed of an icon, which represents the current status of the device itself, and by the identification name. The devices are automatically arranged in the order previously set; where the number of devices exceeds the maximum permissible number for each page, they are placed on several pages, accessible through the sliding buttons shown on the bottom of the screen.

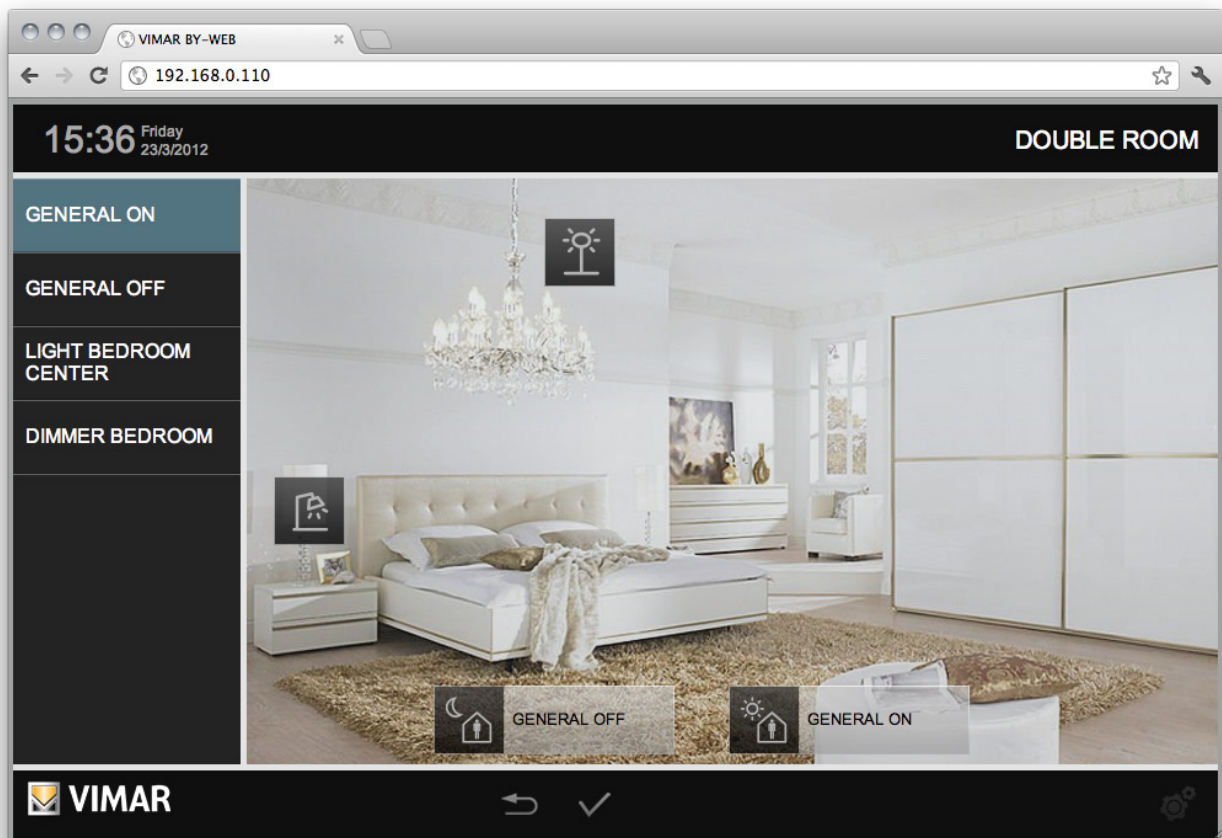


In case of MAP display, the environment is initially presented with all the icons, representing the home automation functions associated with the environment, superimposed on top left, as it is still necessary to place the devices on the page; for this purpose, select "CUSTOMIZE PAGE" from the context menu which can be activated by clicking the button at the bottom right of the screen.

By-me configuration

At this point, drag such buttons with the mouse to the desired position to obtain the best display for the user.

If PIN protection (numeric code) is enabled for the selected room, a window will appear for entering the PIN code number. To display the room page, enter the PIN code and press the OK push button. If the PIN code is the wrong one, an invalid PIN alert message will be displayed.



Double clicking on the icons shows and hides alternately the part of the button containing the name; if you choose to keep hidden, the name of the device will not be visible to the end user, except during command operations on the device itself.

During the customization of the page, the main menu is replaced by a complete list of devices in the environment; through such list you can edit the name of the devices themselves (the change is immediately reflected on the buttons on the page, each time you press the ENTER button, or you select another item on the page).

Once you finish customizing the page, you must save your changes permanently; for this purpose use the CONFIRM button at the bottom of the page. Conversely, if you want to exit without saving the changes, use the BACK button: the page returns to its previous state after confirmation.

For more details on the management of different types of device, see the USER'S GUIDE.

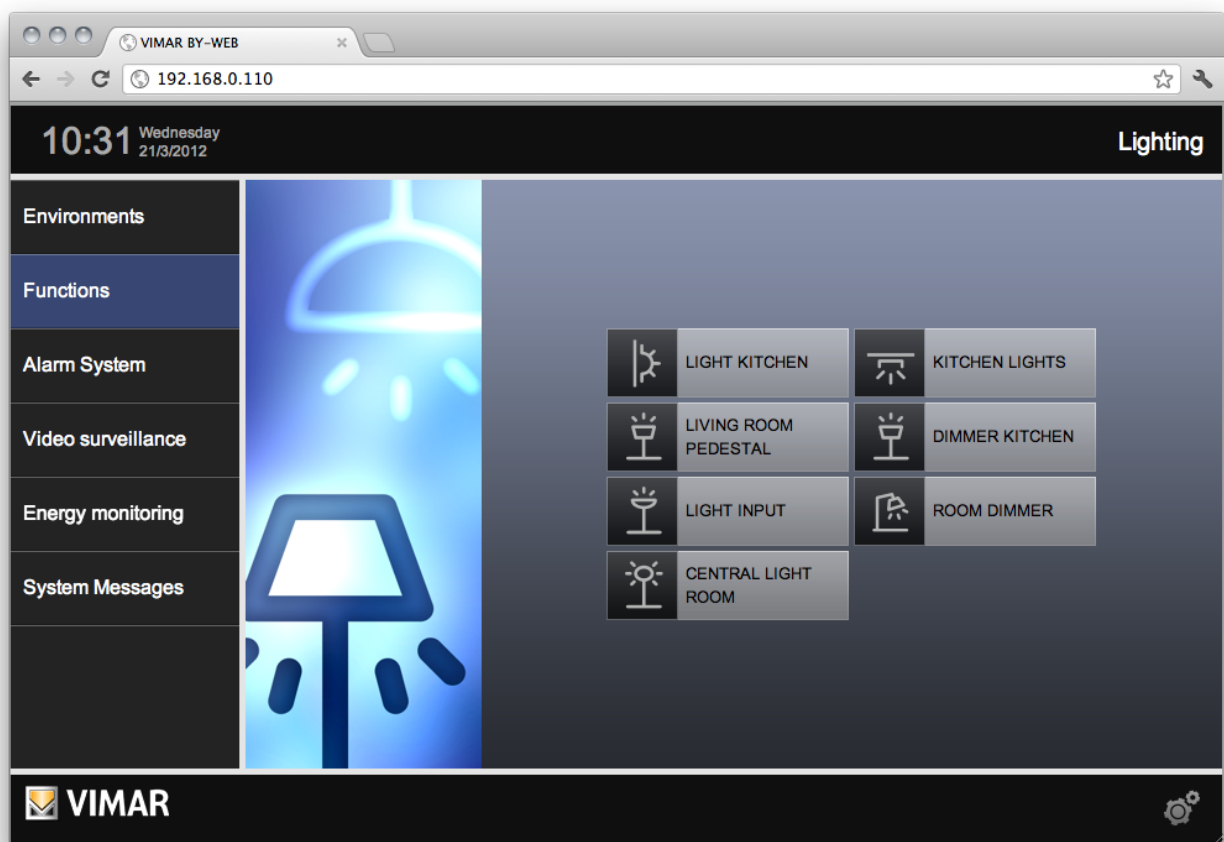
By-me configuration

3.7 Browsing by functions

Similar to what seen for the environments, you can view and manage devices in the By-me system, browsing the Web Server by functions, through the appropriate main menu item; in this case, the devices are shown only in GRID display, divided into the following types:

LIGHTS	Lights, dimmers, relays in general.
SHUTTERS	Shutters (with and without slat management), gates and automation.
CLIMATE	Thermostats (with and without fancoil management).
SCENARIOS	Scenarios configured at the By-me control unit level.
AUDIO	Sound System.
EVENT PROGRAMS	Event programs configured at the By-me control unit level.

For more details on the management of different types of device, see the USER'S GUIDE.



NOTE: in contrast to what happens for the environments, the representative images of the different functions, displayed on the side of the correspondent lists of devices, cannot be customized.

IMPORTANT: If an object is present ONLY in rooms that are not visible to the current user, it is not visible to the user in function view either.
 If an object is present in a room protected by PIN, it is not visible in function view.
 If an object is present in multiple rooms, some protected by PIN and others not protected by PIN, then the object is visible ONLY in the rooms protected by PIN.

Alarm System configuration

4. Alarm System configuration

4.1 The By-alarm intrusion detection alarm system

4.1.1 Introduction

For the integration of the By-alarm system with the By-me automation system there must be a Web Server 01945/01946 in the By-me system, with software version 1.19 or later and the By-alarm control panel (art. 01700 or art. 01703) equipped with its own Ethernet network interface (art. 01712).

NOTE: For the sake of simplicity, in the following chapters, reference is made to the network parameters (IP address, IP ports) of the By-alarm control panel, meaning, more precisely, the Ethernet network interface parameters (art. 01712) of the By-alarm control panel.

The Web Server and By-alarm control panel must be in the same LAN.

If the By-me system does not contain the By-me intrusion detection alarm system (the By-me control panel contains no configured group in the Intrusion detection alarm system application, so no groups for managing technical alarms), the Web Server will display the configuration menu of the By-alarm intrusion detection alarm system, which will be described in the following subsections, accessed from "Intrusion detection alarm system" in the "General Settings" section, and which includes the following items:

- Import XML
- Configuration
- By-me events
- By-alarm Manager Bridge

NOTE: For setting the configuration parameters of the By-alarm control panel, please refer to the documentation of the By-alarm control panel (Art. 01700, Art. 01703).

4.1.2 Import XML

The Web Server 01945/01946 acquires information on the By-alarm system via the XML file generated by the By-alarm Manager software, which contains information on the configuration of the By-alarm control panel (Art. 01700, Art. 01703).

Refer to the documentation of the By-alarm system for generating the XML file.

The "Importing By-alarm configuration" page, accessible via "Import XML", contemplates the following two items:

- Configuration file: press "Choose file" to select the XML file generated with the By-alarm Manager software.
- Import type.

By selecting "New project", before importing the XML file, the Web Server will delete any data there might be about the configuration of the By-alarm system.

By selecting "Update existing project", the Web Server will import the XML file while preserving the parts that have not been changed from the previous import and changing only the parts that have been changed.

NOTE: The import procedure may take several minutes, depending on the size of the By-alarm system.

4.1.3 Configuration

The "By-alarm control panel configuration" page contains the settings to allow the Web Server to access the By-alarm control panel, and it includes the following items:

- **IP address:** IP address of the By-alarm control panel. This is the IP address that the Web Server uses to communicate with the By-alarm control panel.
This is set automatically when you import the XML file of the By-alarm system, but it can also be set from the page of the Web Server.
- **By-me TCP port:** IP port for By-alarm control panel communications (it must match the setting in the By-alarm control panel). This is the port that the Web Server uses to communicate with the By-alarm control panel.
This is set automatically when you import the XML file of the By-alarm system, but it can also be set from the page of the Web Server.
- **By-alarm TCP port:** IP port for By-alarm control panel communications to manage the "bridge" feature for remote/LAN access to the By-alarm control panel via the By-alarm Manager software (it must match the settings in the By-alarm control panel).
This is set automatically when you import the XML file of the By-alarm system, but it can also be set from the page of the Web Server.
- **System PIN:** PIN code for authenticating Web Server access to the By-alarm control panel (6 digits).

To proceed with the import, press the Confirm push button; otherwise, to cancel the import procedure, press the "Back" push button.

Alarm System configuration

4.1.4 By-me Events

Via the Web Server you can run commands in the By-me automation system according to the events generated by the By-alarm system.

The following commands can be run:

- Actuator control (ON/OFF)
- Scenario activation
- Sending the "Protection"/"Restore previous state" command for thermostats in the By-me system that require it.

The By-alarm system events that can be used to create events are the following:

- Switching to a particular area status.
- Switching to a particular zone status.
- Sending a "By-me command" from the By-alarm control panel to the By-me system. By appropriately configuring the By-alarm control panel, sending a By-me command by the control panel can be linked to pushing a push button on the By-alarm system transmitters. You can configure up to 32 different By-me commands.

For configuring events, go to the "General settings"/"Intrusion detection alarm system"/"By-me Events" page, which looks like a list divided into three sections:

- **By-alarm Areas:** this section shows the areas that are configured in the By-alarm system, to which By-me commands can be linked.
- **By-alarm Zones:** this section shows the zones that are configured in the By-alarm system, to which By-me commands can be linked.
- **By-me Commands:** this section shows the 32 "By-me command" elements that are configured in the By-alarm system, to which By-me commands can be linked.

Priorities of the area and zone statuses in By-me event management (valid only for web server versions between 1.19 and 1.26, inclusive)

IMPORTANT: Priority management of the area and zone statuses of the By-alarm system, by the Web Server, applies to Web Server versions between 1.19 and 1.26 (inclusive); for Web Server versions 1.27 and later, area and zone status management allows independent use of the possible statuses envisaged by the By-alarm system.

It is possible for an area or a zone of the By-alarm system to have more than one state at the same time.

Example: a zone of the By-alarm system can be open and in alarm mode at the same time. This is the case of opening a zone when the area to which it belongs is armed.

In By-me events management, based on the states of the areas and zones of the By-alarm system, priorities are determined on the states, as described in the tables below.

Upon a change in the state of an area or zone used to define a By-me event, the Web Server manages the condition with higher priority.

NOTE: Some states are mutually exclusive and so are grouped into one priority level. For example, an area can take one arming state (OFF, ON, INT, PAR) and then these states are assigned the same priority.

Regarding the notation used to indicate the priority, a higher numerical index corresponds to a higher priority.

Area status priority	Status description
1	OFF
	ON
	INT
	PAR
2	Alarm memory
3	Alarm

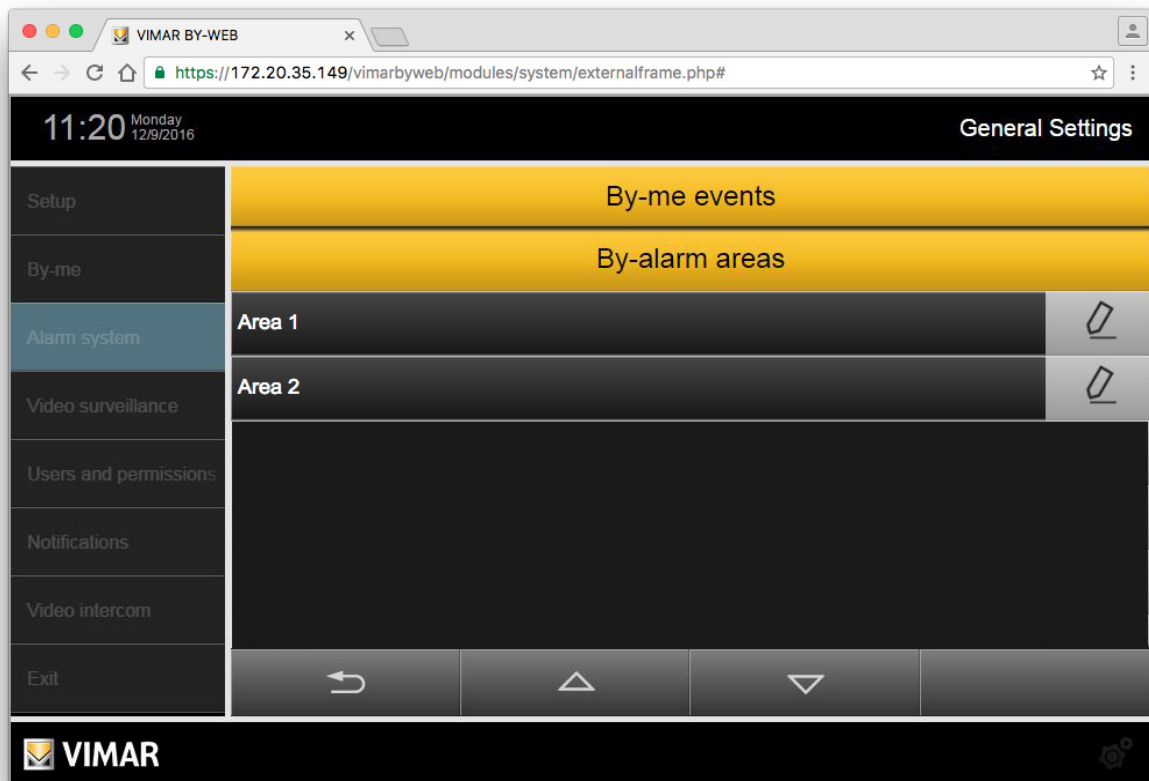
Zone status priority	Status description
1	Closed
	Open
2	Masked
3	Alarm memory
4	Alarm
5	Tampered
6	Excluded

Example 1: If a zone, which belongs to an armed area, is opened, it will simultaneously take the status of "open" (priority 1) and "alarm" (priority 4) in the By-alarm system. If you have created two separate By-me events, linked to the states of "open" and "alarm" for that zone, the web server will run the commands for the state with the highest priority and then those for the alarm status (priority 4 with respect to priority 1 of the open state) of the zone.

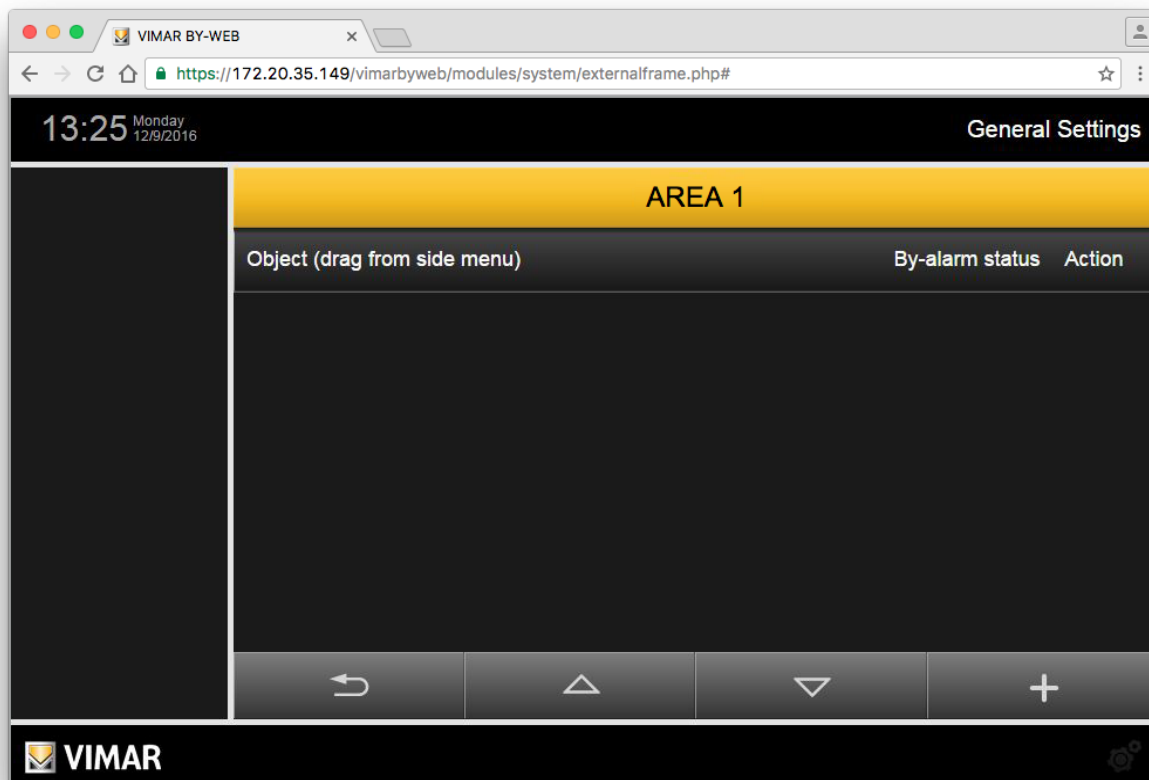
Example 2: If I create an event linked to the OFF status of an area, and that area, starting from an alarm state is disabled (OFF), the created event will not be managed because the area has simultaneously gone into the OFF status and into the "Alarm memory" status and the latter has a higher priority than the OFF status. In other words the created event will be managed when the area goes into the OFF status not coming from an alarm condition.

Alarm System configuration

4.1.4.1 By-me Events linked to the states of By-alarm areas



Pressing the Edit push button at the left of each row takes you to the events page of the selected area. Initially the page has no events.



Alarm System configuration

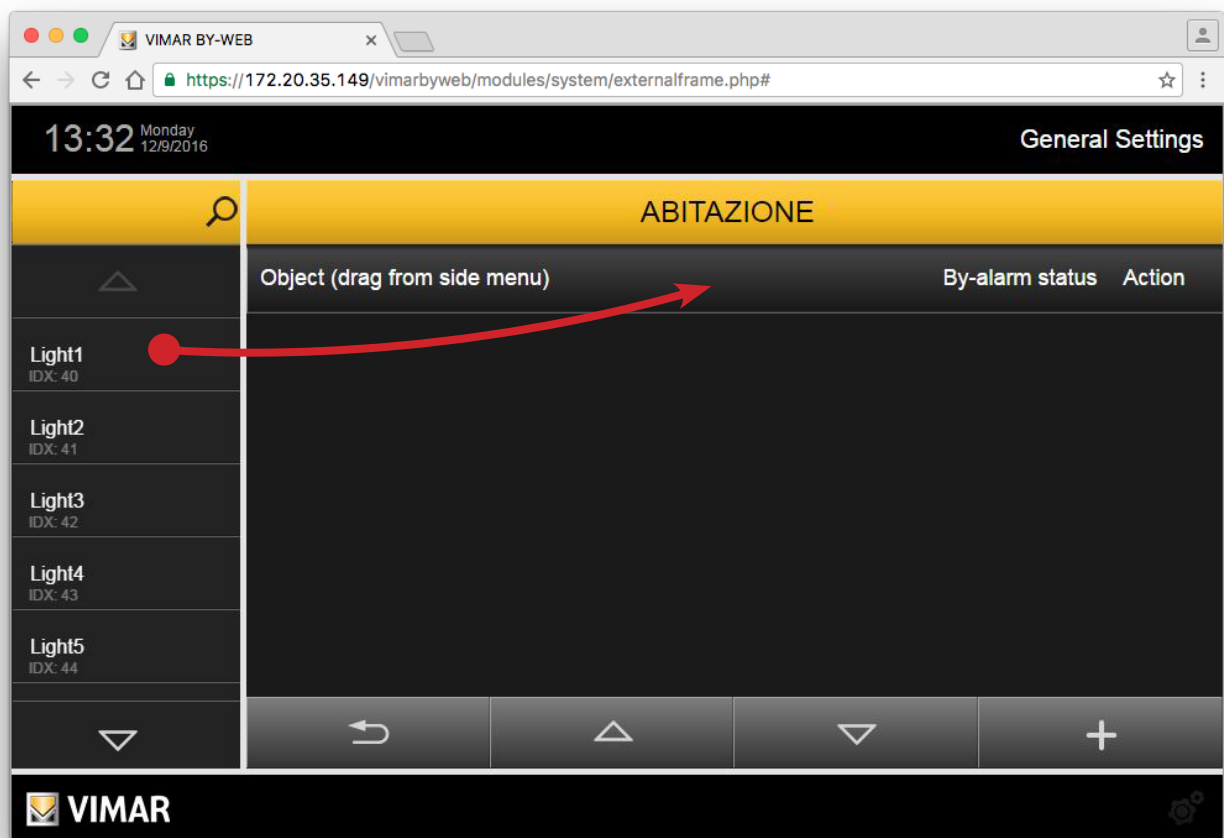
The operations that can be carried out from the events page linked to a specific area are as follows and are described in the following subsections:

- Creating an event.
- Displaying the configuration of previously created events.
- Editing a previously created event.
- Deleting a previously created event.

Creating an event

To add an event linked to an area of the By-alarm system, proceed as follows:

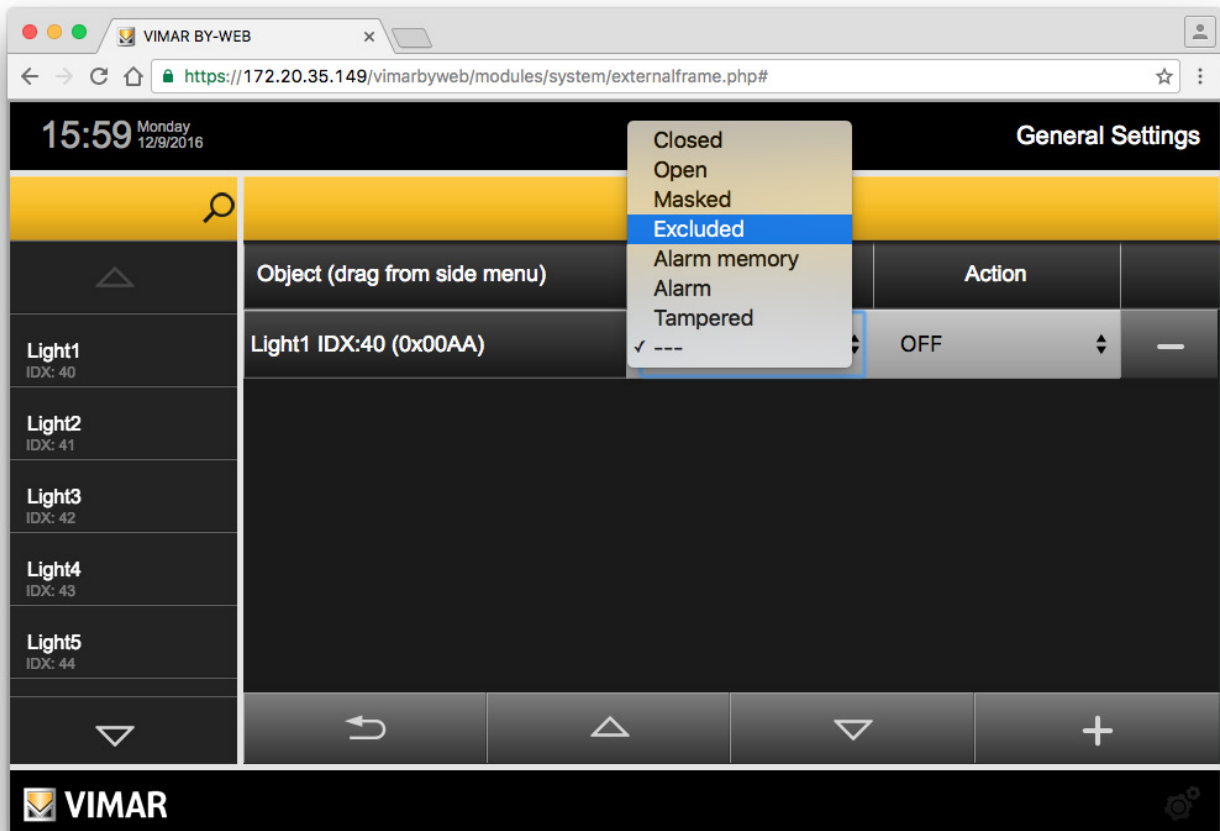
1. Press the "+" push button at the bottom right of the page to add an event to the list.
2. The left side column shows the list of devices that can be controlled by the Web Server following the occurrence of an event of the By-alarm system.
Drag the desired object from the list of the side column to the grey "Object (Drag from the side menu)" bar at the top of the workspace.
If the object is dragged to a different area of the workspace, the event will not be created.



Alarm System configuration

- A row is created representing the created event, whose name (not editable) matches the description of the controlled object. Before becoming operative, the event must be configured, as described below.
Press the push button on the "By-alarm status" column to choose the state of the area when the By-me command is sent. Select "--" so as not to link any events (in this case, management of the specific event is inhibited).
Press the "Action" column push button to select the value of the command that is to be sent when the selected By-alarm event occurs.

NOTE: These changes do not require confirmation and are stored by the Web Server automatically.



- Press the "Back" button to exit the page or repeat the operations described above, from point 1. to add additional devices to be controlled, linked to the same event.

Displaying the configuration of previously created events

The page of events linked to the specified area contains a list of all the configured events. Each row in the list represents an event and provides the following information:

- Object: name identifying the object that is to be controlled (ON/OFF actuator, thermostat or scenario).
- State of the By-alarm system area that is to be linked to the command to the By-me object.
- Action: command to be sent to the object.

Editing a previously created event

To change the configuration of an event, locate the corresponding row in the list and edit its parameters.

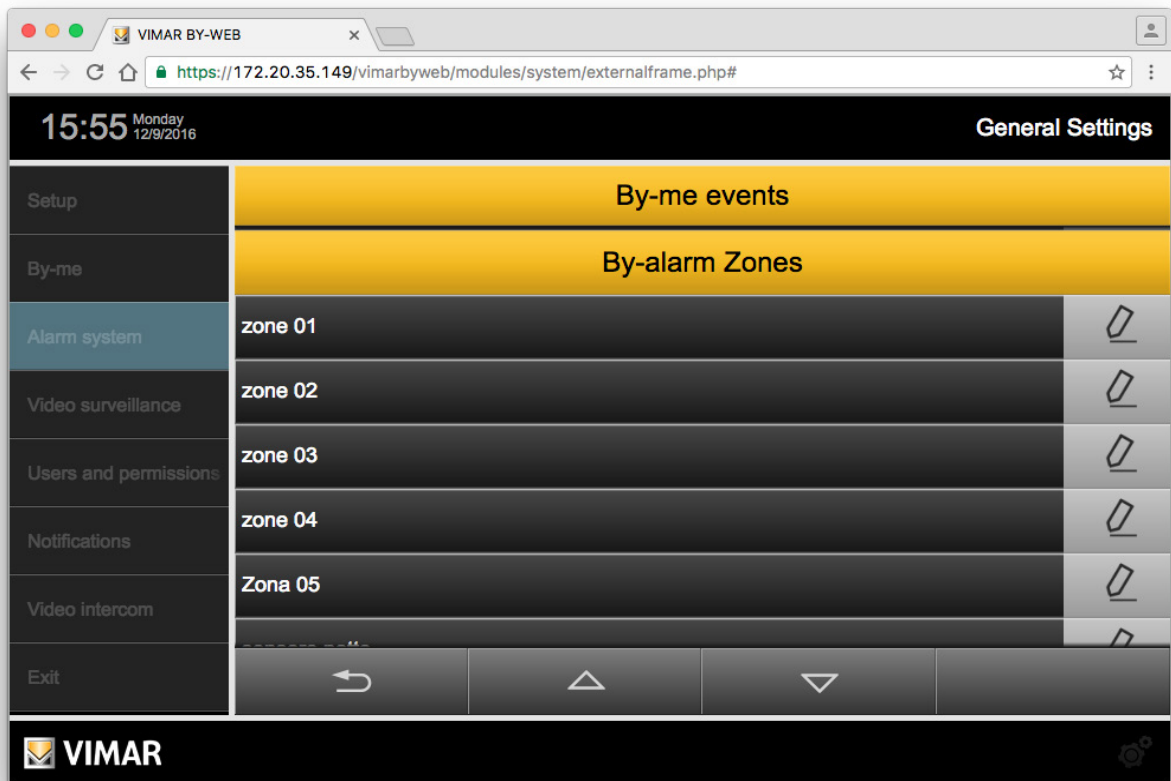
NOTE: These changes do not require confirmation and are stored by the Web Server automatically.

Deleting a previously created event

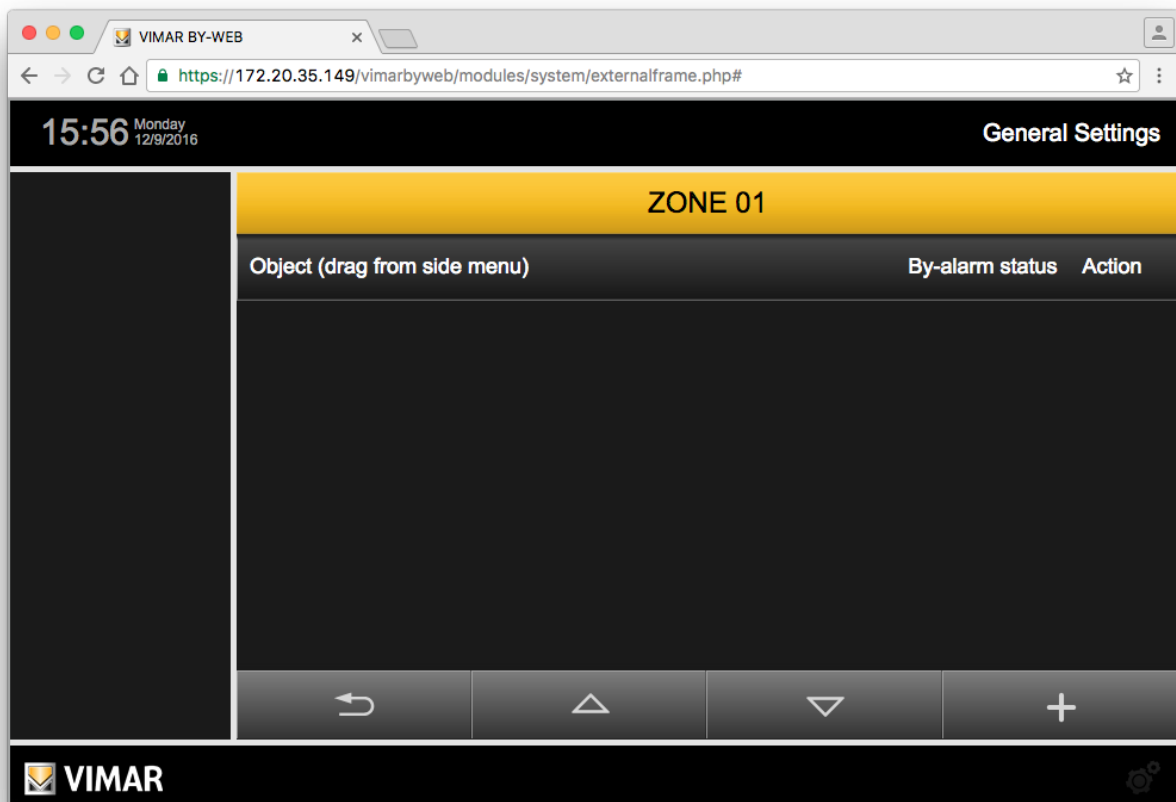
To remove an event previously created for a specific Area from the list, after entering the page with the list of events linked to that area, press the "-" push button on the right of the row representing the event. The operation involves a confirmation window.

Alarm System configuration

4.1.4.2 By-me Events linked to the states of By-alarm areas



Pressing the Edit push button at the left of each row takes you to the events page of the selected zone. Initially the page has no events.



Alarm System configuration

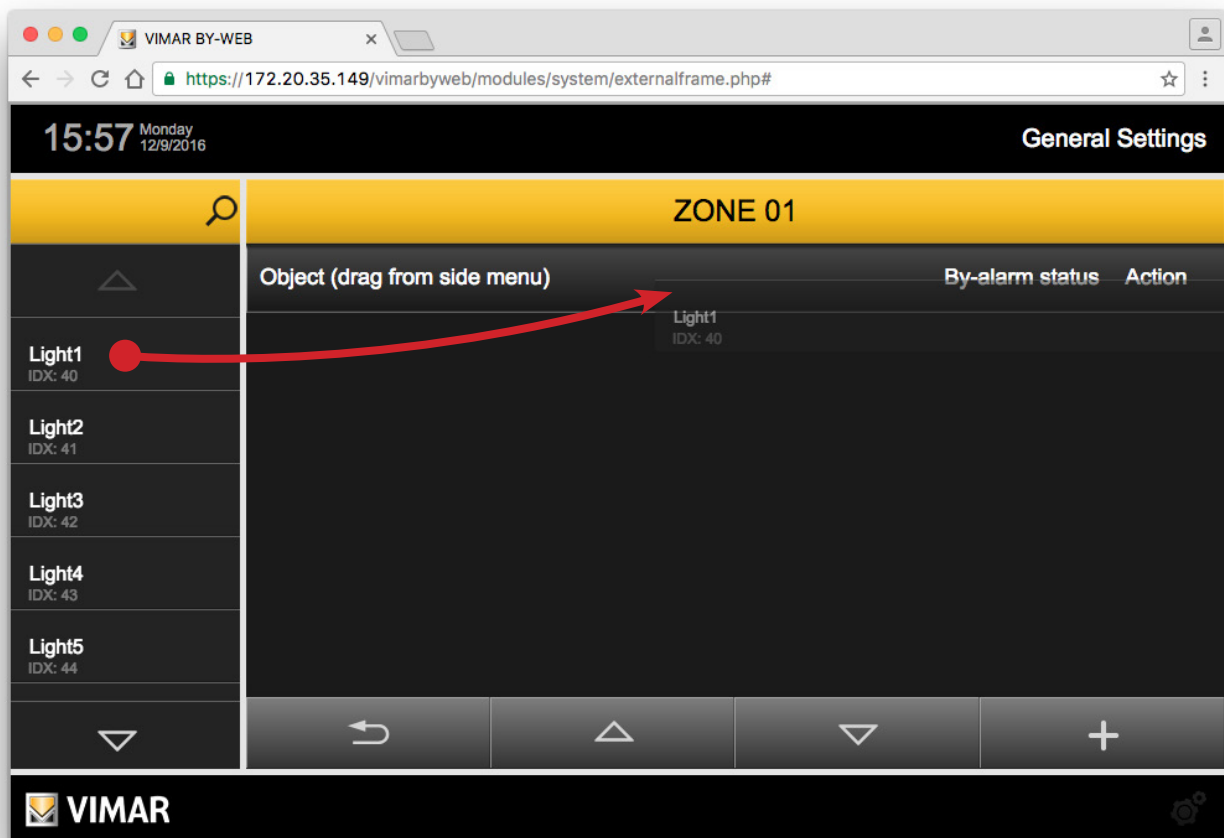
The operations that can be carried out from the events page linked to a specific zone are as follows and are described in the following subsections:

- Creating an event.
- Displaying the configuration of previously created events.
- Editing a previously created event.
- Deleting a previously created event.

Creating an event

To add an event linked to a zone of the By-alarm system, proceed as follows:

1. Press the "+" push button at the bottom right of the page to add an event to the list.
2. The left side column shows the list of devices that can be controlled by the Web Server following the occurrence of an event of the By-alarm system.
Drag the desired object from the list of the side column to the grey "Object (Drag from the side menu)" bar at the top of the workspace.
If the object is dragged to a different area of the workspace, the event will not be created.



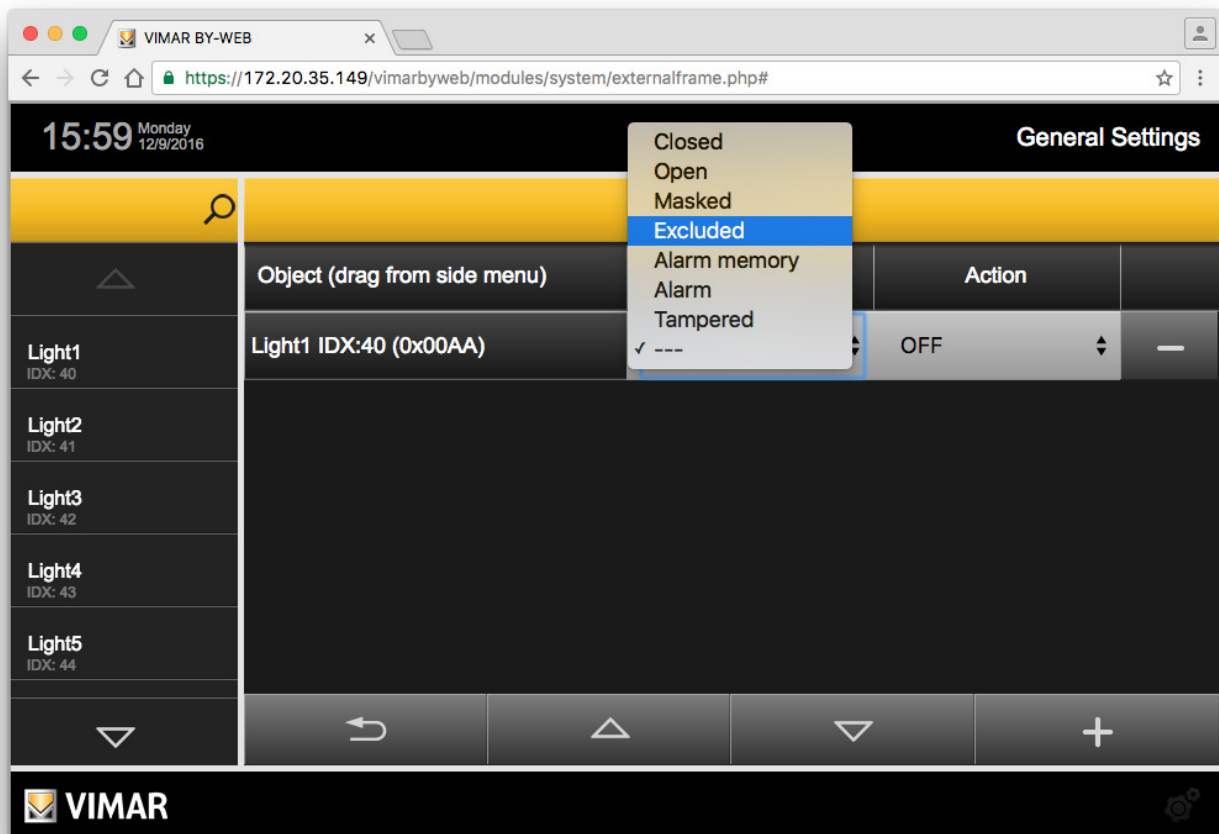
3. A row is created representing the created event, whose name (not editable) matches the description of the controlled object. Before becoming operative, the event must be configured, as described below.

Press the push button on the "By-alarm status" column to choose the state of the zone when the By-me command is sent. Select "--" so as not to link any events (in this case, management of the specific event is inhibited).

Press the "Action" column push button to select the value of the command that is to be sent when the selected By-alarm event occurs.

NOTE: These changes do not require confirmation and are stored by the Web Server automatically.

Alarm System configuration



4. Press the "Back" button to exit the page or repeat the operations described above, from point 1. to add additional devices to be controlled, linked to the same event.

Displaying the configuration of previously created events

The page of events linked to the specified zone contains a list of all the configured events. Each row in the list represents an event and provides the following information:

- Object: name identifying the object that is to be controlled (ON/OFF actuator, thermostat or scenario).
- State of the By-alarm system zone that is to be linked to the command to the By-me object.
- Action: command to be sent to the object.

Editing a previously created event

To change the configuration of an event, locate the corresponding row in the list and edit its parameters.

NOTE: These changes do not require confirmation and are stored by the Web Server automatically.

Deleting a previously created event

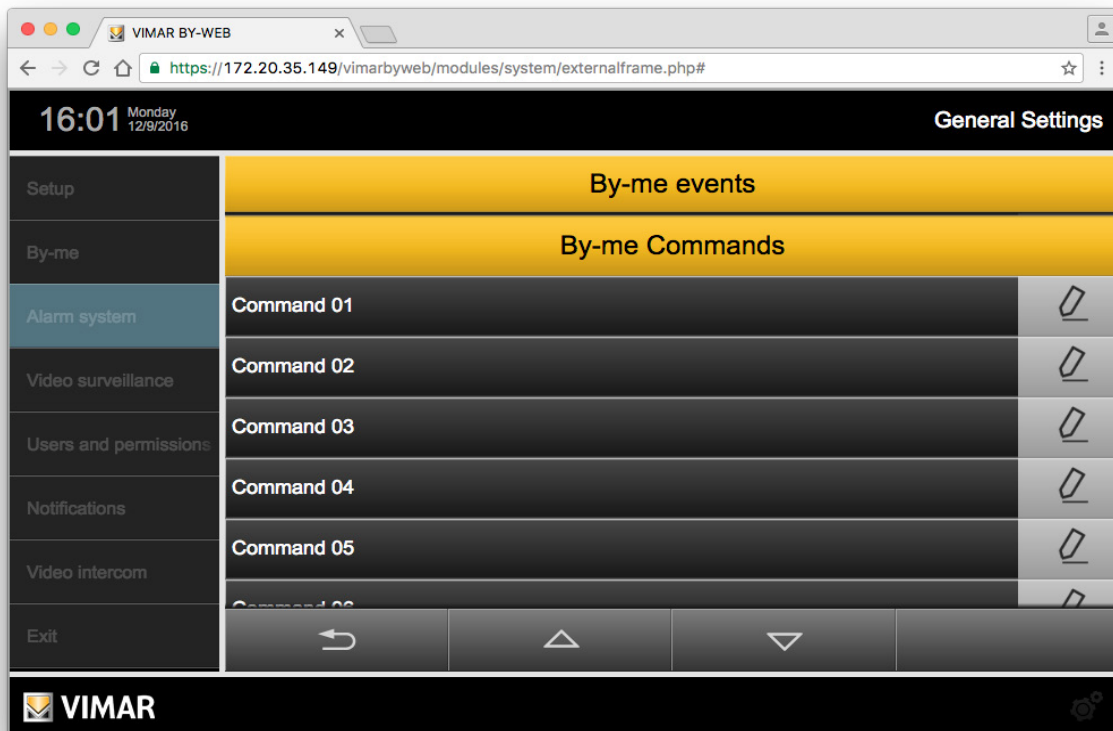
To remove an event previously created for a specific zone from the list, after entering the page with the list of events linked to that zone, press the "-" push button on the right of the row representing the event. The operation involves a confirmation window.

Alarm System configuration

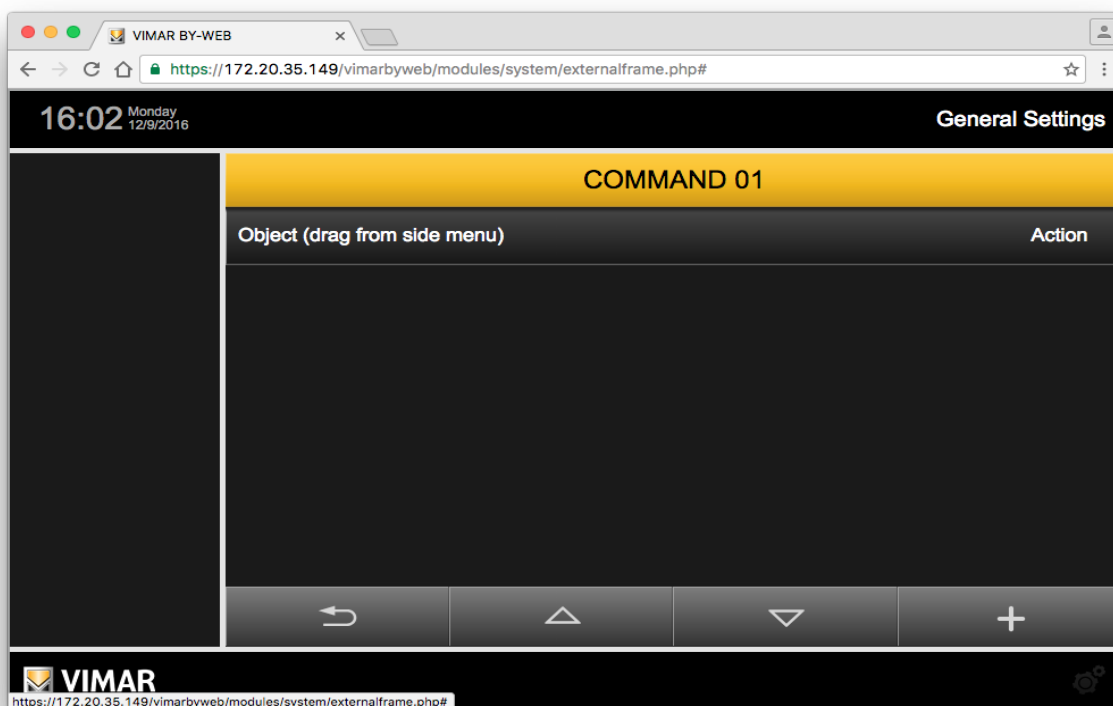
4.1.4.3 By-me events linked to By-me commands

Besides being able to send actuation commands in the By-me system following specific changes in status of the By-alarm system areas and zones, you can send actuation commands in the By-me system by pressing push buttons on the By-alarm system transmitters.

This feature is made possible by the management of the "By-me Commands" by the By-alarm control panel (art. 01700, art. 01702), equipped with an Ethernet interface (art. 01712) and by the Web Server (art. 01945, art. 01946). This chapter describes the configuration for managing By-me commands in the Web Server. Please refer to the By-alarm system documentation for a description of the configuration of the By-me commands in the By-alarm system.



Pressing the Edit push button at the left of each row takes you to the events page of the selected By-me command. Initially the page has no events



Alarm System configuration

The operations that can be carried out from the events page linked to a specific zone are as follows and are described in the following subsections:

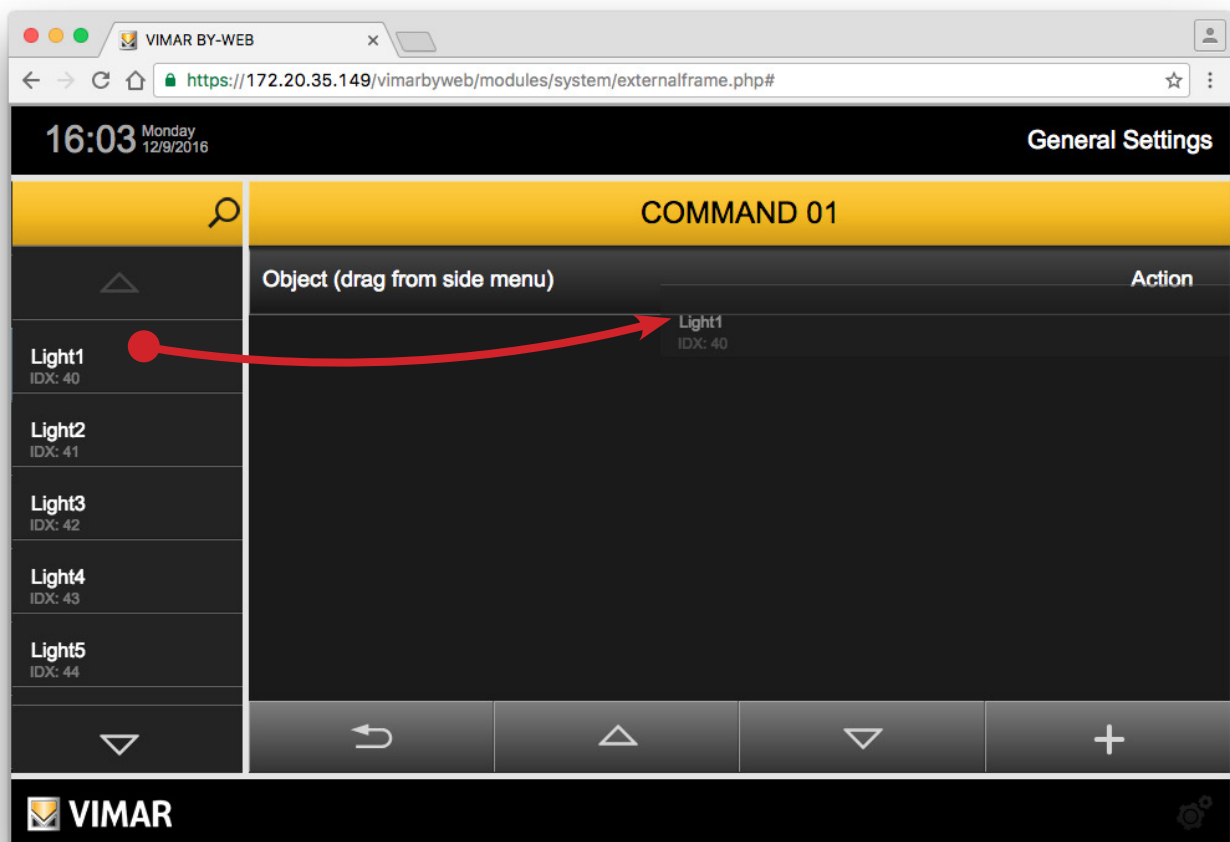
- Creating an event.
- Displaying the configuration of previously created events.
- Editing a previously created event.
- Deleting a previously created event.

Creating an event

To add an event linked to a By-me command of the By-alarm system, proceed as follows:

1. Press the "+" push button at the bottom right of the page to add an event to the list.
2. The left side column shows the list of devices that can be controlled by the Web Server following the occurrence of an event of the By-alarm system.

Drag the desired object from the list of the side column to the grey "Object (Drag from the side menu)" bar at the top of the workspace. If the object is dragged to a different area of the workspace, the event will not be created.

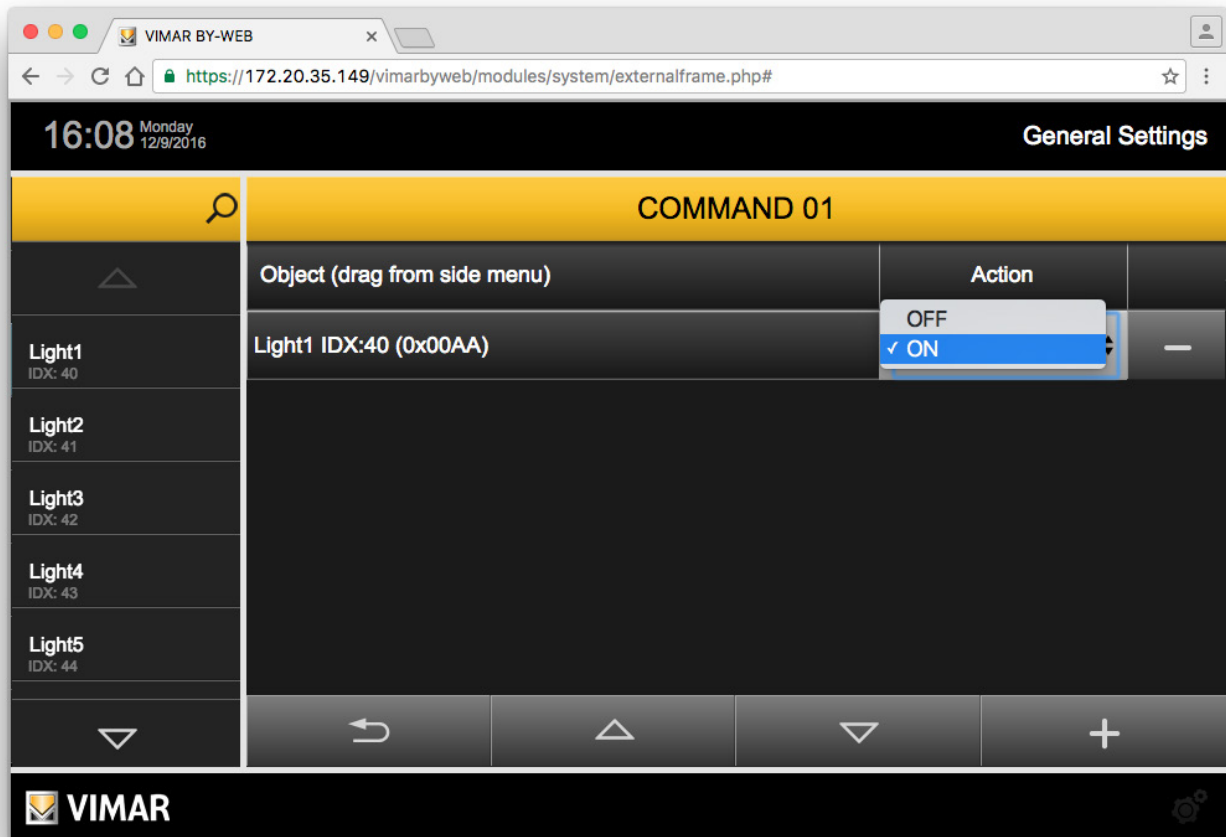


3. A row is created representing the created event, whose name (not editable) matches the description of the controlled object. Before becoming operative, the event must be configured, as described below.

Alarm System configuration

Press the "Action" column push button to select the value of the command that is to be sent when the selected By-alarm event occurs.

NOTE: These changes do not require confirmation and are stored by the Web Server automatically.



4. Press the "Back" button to exit the page or repeat the operations described above, from point 1. to add additional devices to be controlled, linked to the same event.

Displaying the configuration of previously created events

The page of events linked to the selected By-me command contains a list of all the configured events.

Each row in the list represents an event and provides the following information:

- Object: name identifying the object that is to be controlled (ON/OFF actuator, thermostat or scenario).
- Action: command to be sent to the object.

Editing a previously created event

To change the configuration of an event, locate the corresponding row in the list and edit its parameters.

NOTE: These changes do not require confirmation and are stored by the Web Server automatically.

Deleting a previously created event

To remove an event previously created for a specific By-me command from the list, after entering the page with the list of events linked to that By-me command, press the "-" push button on the right of the row representing the event.

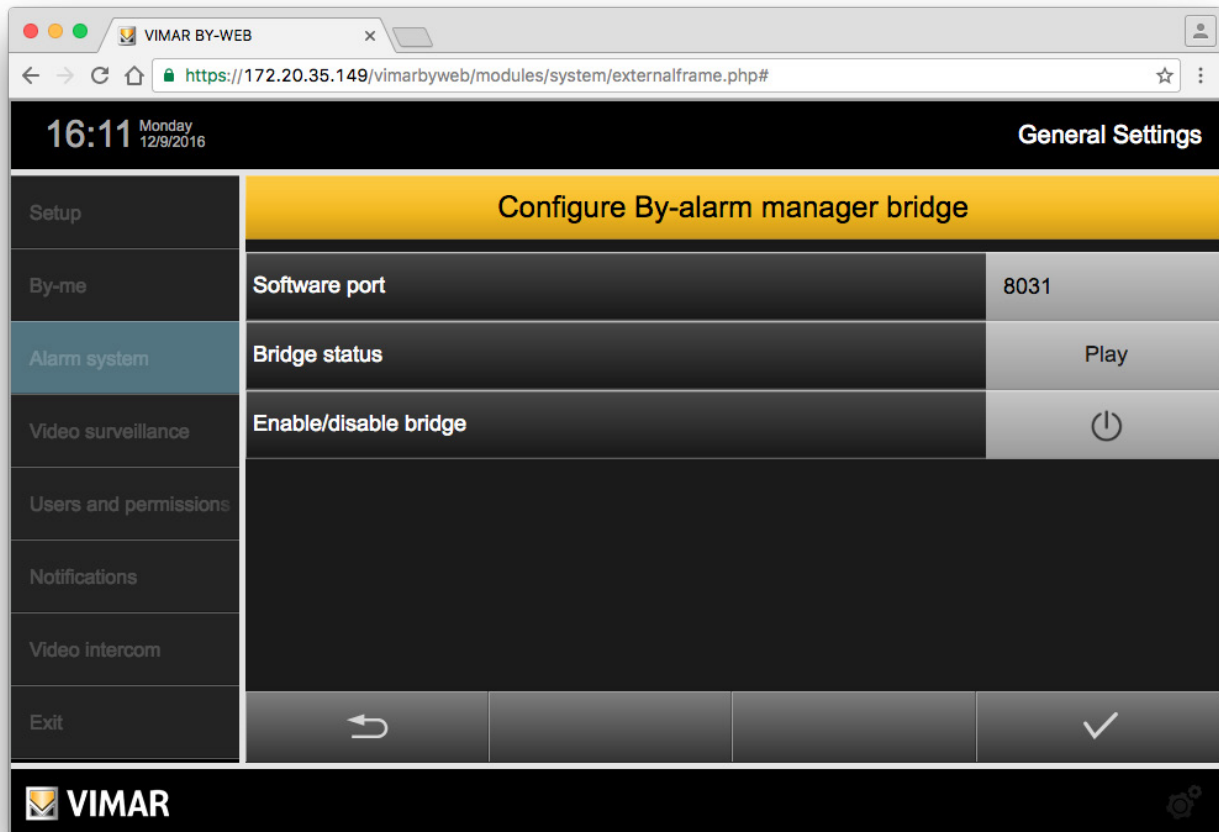
The operation involves a confirmation window.

Alarm System configuration

4.1.5 By-alarm Manager Bridge

Set and enable this feature if you want to use the By-alarm Manager software, to manage the By-alarm system, remotely or over a LAN, using the Web Server as a bridge and taking advantage of an HTTPS connection protected by an SSL certificate.

For a description of the feature, see chapter 4.1.5.1 The bridge feature of the Web Server.



The "Configuring By-alarm Manager bridge" page has three fields:

- Software port: this is the IP port used by the By-alarm Manager software for communicating with the Web Server for the bridge feature. Set the port in the Web Server and use the port value set as a parameter in the By-alarm Manager software window for connecting to the By-alarm control panel via the bridge managed by the Web Server.
- Bridge status: gives an indication of the operating status of the bridge:
 - Play: the bridge feature is on.
 - Stop: the bridge feature is off.
- Enable/disable bridge: used to enable or disable this feature. The activation status is provided by the "Bridge status" field.

Press the Confirm button to confirm the data entered, or the "Back" button to exit the page without saving any data entered.

Alarm System configuration

4.1.5.1 The bridge feature of the Web Server

If the By-alarm system contains the Web Server (01945 or 01946) and the By-alarm control panel (art. 01700, art. 01703) is equipped with its own Ethernet interface (art. 01712), you can use the By-alarm Manager software using an HTTPS network connection with the By-alarm control panel.

This feature is contemplated both for a local connection (the PC on which By-alarm manager is installed is connected to the LAN to which the By-alarm control panel is connected) and for a remote connection over the Internet, making it possible, in the latter case, to perform configuration and diagnostic operations (contemplated by the By-alarm manager software) remotely.

The following chapters describe the two cases of local and remote connection between the By-alarm manager software and the By-alarm control panel, using the bridge feature of the Web Server.

Local connection between By-alarm Manager and By-alarm control panel

The following figure schematically shows the flow of information between the By-alarm manager software and the By-alarm control panel in the case of a local connection.

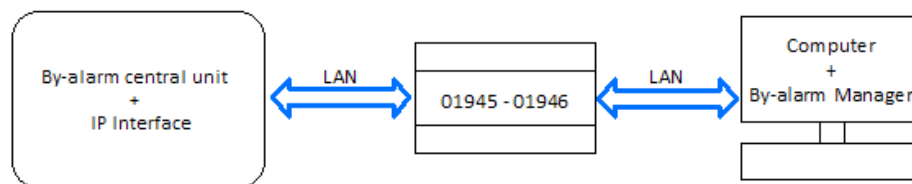


Figure 1 - Local connection between By-alarm Manager and By-alarm control panel

Before you make the first connection you must have performed the following configuration steps:

1. Configure the port for the bridge feature in the By-alarm control panel: By-alarm TCP port (refer to the documentation of the By-alarm control panel).
2. On the Web Server, configure the "By-alarm TCP port" on the Intrusion detection alarm system/Configuration page of the General settings section. This value must match the one set in point 1.
3. On the Web Server, configure the "Software port" on the "Intrusion detection alarm system/By-alarm manager bridge" page of the General settings section. This is the value that must be set on the page for setting the parameters for connecting the By-alarm manager software with the Web Server.

To make the connection, proceed as follows:

1. On the Web Server, enable the bridge feature with the Bridge enable/disable push button on the "Intrusion detection alarm system/By-alarm manager bridge" page of the General settings section.
In the "Bridge status" field on the same page you can check the activation status of this feature: verify that the status is "Play".
2. Open the By-alarm manager software and connect to the By-alarm control panel, setting as parameters for LOCAL NETWORK CONNECTION:
 - a. Local address: IP address of the Web Server
 - b. TCP port: the port set on the Web Server at point 3.

After completing the configuration settings via By-alarm manager you can disable the bridge feature of the Web Server.

Alarm System configuration

Remote connection between By-alarm Manager and By-alarm control panel

The following figure schematically shows the flow of information between the By-alarm manager software and the By-alarm control panel in the case of a remote connection.

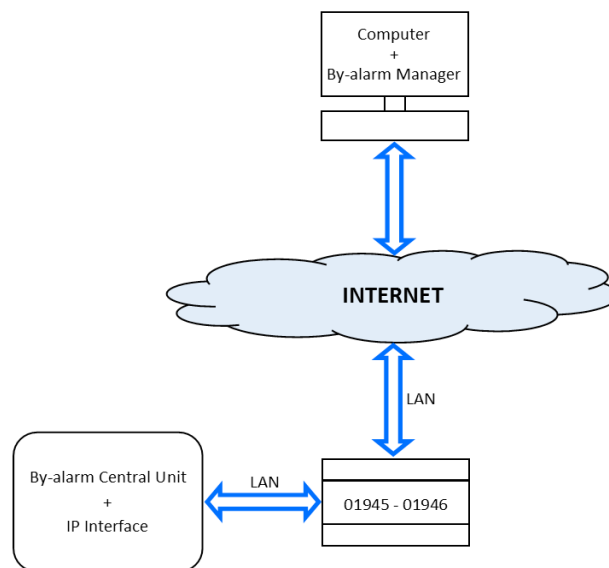


Figure 2 - Remote connection between By-alarm Manager and By-alarm control panel

Before you make the first connection you must have performed the following configuration steps:

1. Configure the port for the bridge feature in the By-alarm control panel: By-alarm TCP port (refer to the documentation of the By-alarm control panel).
2. On the Web Server, configure the "By-alarm TCP port" on the Intrusion detection alarm system/Configuration page of the General settings section. This value must match the one set in point 1.
3. On the Web Server, configure the "Software port" on the "Intrusion detection alarm system/By-alarm manager bridge" page of the General settings section. This is the value that must be set on the page for setting the parameters for connecting the By-alarm manager software with the Web Server.
4. On the ADSL router, open the external port that must then be mapped, using the port forwarding rule, to the Web Server port used by the Web Server for the connection with the By-alarm manager software.

The port forwarding rule, to be created in the ADSL router, must link the desired external port (make sure the port is not already used by other applications/services) to the pair: IP Address of the Web Server (on the LAN) and "Software port" on the "Intrusion detection alarm system/By-alarm manager bridge" page of the General settings section of the Web Server.

To make the connection, proceed as follows:

1. On the Web Server, enable the bridge feature with the Bridge enable/disable push button on the "Intrusion detection alarm system/By-alarm manager bridge" page of the General settings section. In the "Bridge status" field on the same page you can check the activation status of this feature: verify that the status is "Play".
2. Open the By-alarm manager software and connect to the By-alarm control panel, setting as parameters for INTERNET CONNECTION:
 - a. Local address: URL of the web server (DNS)/IP Address of the external interface of the router, corresponding to the IP address of the Web Server.
 - b. TCP port: External port of the router corresponding to the router port set in the previous point 4.

After completing the configuration settings via By-alarm manager you can disable the bridge feature of the Web Server.

4.2 The Alarm System By-me

4.2.1 Introduction

If the system provides the management of the intrusion detection systems SAI, the XML project exported from the control unit already has all the information necessary to configure the Web Server, without any further steps to take. However, some operations are necessary to initiate proper communication between the SAI central and the **Web Server**, illustrated below.

4.2.2 Changing partializations

The "PARTIALIZATIONS" page of the "ALARM SYSTEM" section allows the administration to change the name assigned to the central partializations in the project; simply change the name and, when finished, close the page with the appropriate button to return to the main administration page.

Setting up the video surveillance

5. Setting up the video surveillance

5.1 Introduction

From the **Web Server** pages, you can view the of the video stream of one or more IP cameras (up to a maximum of 32) meeting the following requirements:

Builder	Hardware Requirements	Software requirements	Browser Requirements
Axis	All models of IP camera		Any browser supported by the device.
ELVOX:	It manages all the IP cameras and the ELVOX video server	VideoLAN VLC Vimar ByWeb Tools**	
Generic Mjpeg*	A device that can handle the Mjpeg format		Any browser that can display the MJPEG format
Mobotix	All models of IP camera		Any browser supporting the MJPEG format
Managing a generic RTSP stream *	Devices supporting the RTSP stream	VideoLAN VLC Vimar ByWeb Tools**	




* We cannot guarantee proper operation of these video streams for all the available devices (cameras, video servers...).

** For the installation of Vimar ByWeb Tools refer to chapter 12. ByWeb Tools by Vimar of this manual.

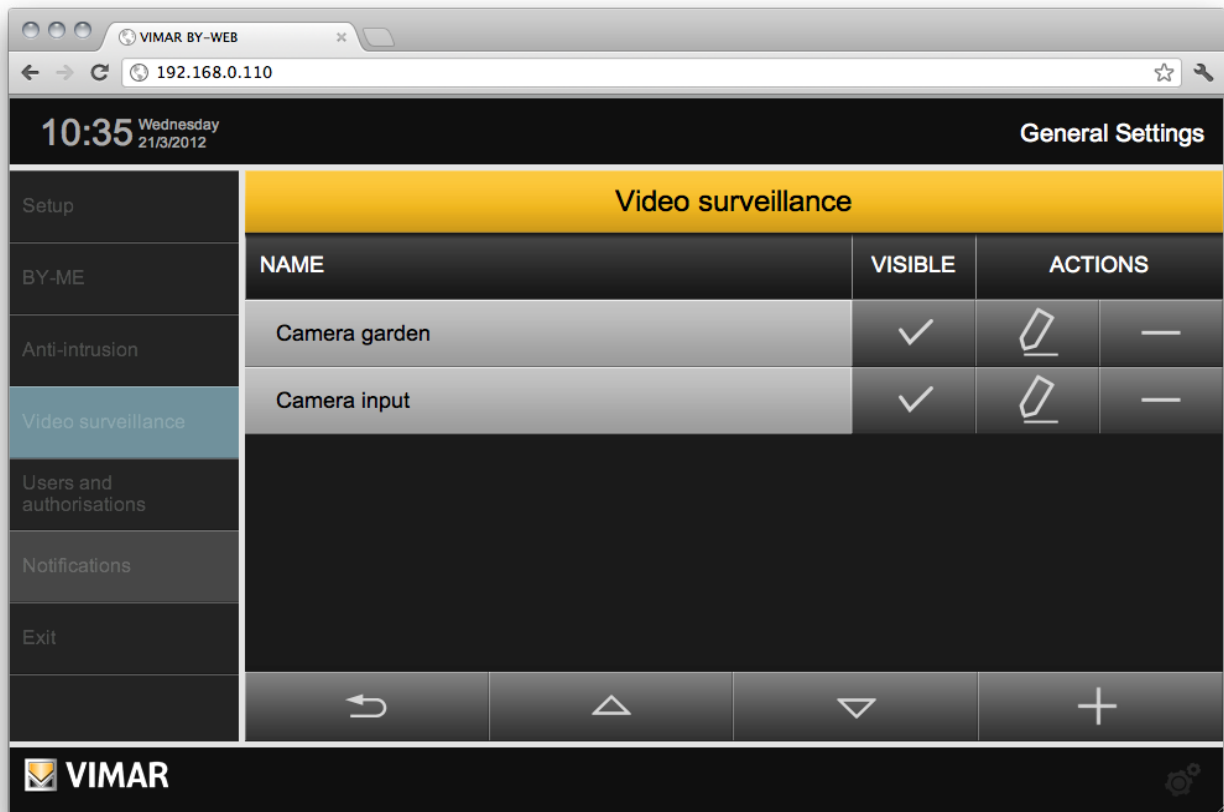
5.2 Setting up an IP camera

By selecting "VIDEO SURVEILLANCE" from the main menu of the GENERAL SETTINGS, you can configure the IP cameras in the system, provided that they meet the requirements listed above. Initially, the list of cameras is empty, to add a new camera use the "ADD" button available in the panel at the bottom of the page (similar to what we saw earlier to create new environments).

Once the new camera appears in the list, you can instantly change its name through the appropriate text box; the following buttons are also available:

	<p>CHANGE ORDER Drag this button to change the display order of the cameras in the corresponding Web Server menu.</p>
	<p>EDIT Allows access to the camera details, as described below.</p>
	<p>DELETE Deletes the camera from the Web Server. This operation, subject to confirmation by the installer, cannot be subsequently canceled.</p>

Setting up the video surveillance

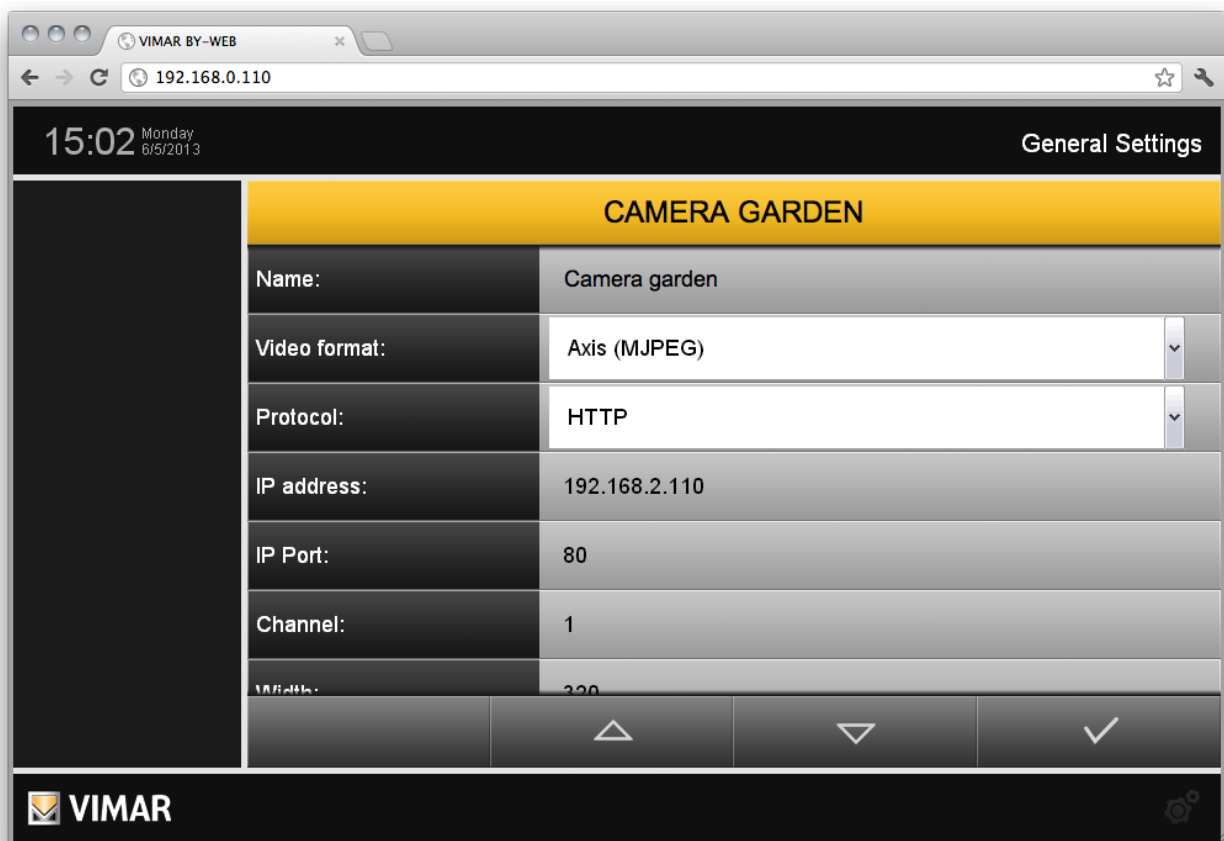


Through the "CHANGE" button, you can access the details of the camera, from which to customize the following parameters:
(Not all fields are present for every video format).

NAME	Name associated with the camera, visible by the users in the "VIDEO SURVEILLANCE" menu.
VIDEO FORMAT	Choose one of the possible formats, depending on the manufacturer of the camera and its type.
PROTOCOL	Protocol used to access the video camera.
IP ADDRESS	Local network IP address assigned to the IP camera. NOTE: it is not necessary to type the used protocol (http, https, rtsp)
IP PORT	IP port on which you can view the camera video stream.
PATH	String representing the path to reach the camera.
CHANNEL	In the case of cameras or video servers with more than one channel, specify the channel number to display. Default: 1.
FLOW	It is possible to choose between Primary and Secondary Flow.
USER	The user data required to log in to the cameras.
PASSWORD	The password required to log in to the cameras.
WIDTH	Width in pixels of the window that displays the camera video stream. Refer to the documentation of the camera and its configuration, to get the possible values to be entered in this field.
HEIGHT	Height in pixels of the window that displays the camera video stream. Refer to the documentation of the camera and its configuration, to get the possible values to be entered in this field.
Enables HTTPS proxy for remote connections:	Enabling this feature allows the IP camera images to be processed by the internal proxy of the Web Server (and coded by SSL).

NOTE: For Generic RTSP and Generic MJPEG video formats, the URL to access the camera is created from Web Server as follows:
IP address: IP port / path.

Setting up the video surveillance



After completing the entry of operating parameters, return to the video surveillance page through the "BACK" button. Configure any other cameras following the same procedure.

5.2.1 IP cameras Proxy Function

A proxy function available for the IP cameras, creates a "tunnel" on port 443 in case of remote access, conveying IP cameras video streams, available on the local network IP addresses, via the Web Server. In this way, the installer doesn't have to open more than one IP port on the ADSL (or similar) router.

The configuration of the proxy function is totally automatic and "transparent": saving a camera, creates the correspondent proxy rule in the configuration file of the Web Server, prompted in case of access to that camera page when accessing remotely (on local network the stream picked up by the IP address of the camera is displayed directly).

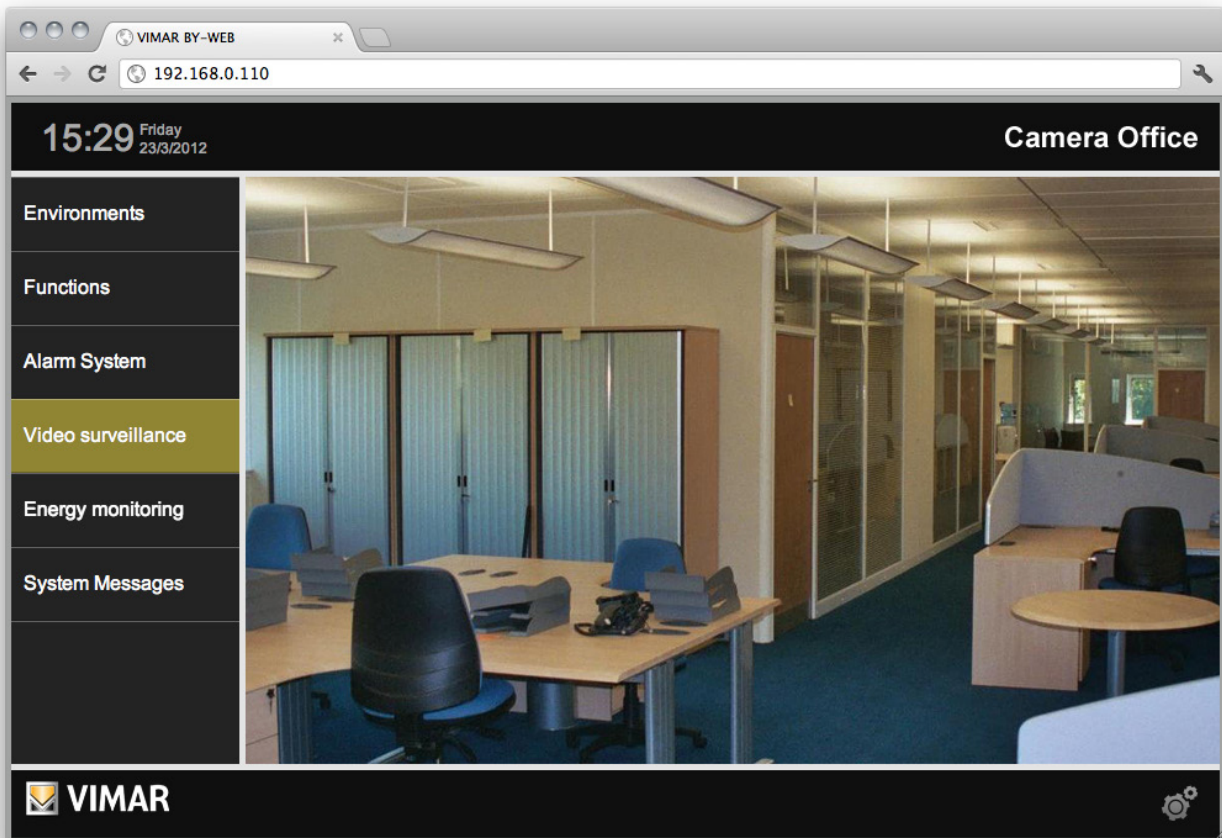
If this feature is not enabled, you can still view the IP camera remotely using the SSL encryption of the Web Server proxy after opening of an additional port on the router for remote access to the IP camera (use this feature, for example, if the IP camera already uses an internal SSL encryption and you have a very fast internet connection, such as optical fiber).

NOTA: For the Elvox and Generic RTSP video formats, the Proxy function is not present.
To remotely access the camera via the Web Server, you must create the appropriate access rules on the router.

Setting up the video surveillance

5.3 Viewing the cameras

IP cameras configured in the **Web Server** are accessible to users through the appropriate main menu; the sub-menu contains the list of cameras in the order established previously; selecting one of the available entries shows the corresponding video stream in specific section of the page.



For more details , see the USER'S GUIDE.

Setting up the video surveillance

6. Energy monitoring

6.1 Introduction

ENERGY MONITORING is a function of By-web intended for the monitoring and analysis of energy consumption of the home automation system. Through the periodic reading of the meters which measure the power consumed and produced, the system generates a series of statistics (based on the configuration parameters) which provide the user with graph and table summaries intended to provide useful information for a more conscious and responsible use of energy.

If the system includes a component which produces electricity, the load indicator of the Energy Monitoring section shows the electricity effectively consumed by the system loads (assuming that the system has been set up according to the Vimar specifications: the probe (probes for three-phase) of the power consumption meter must be located immediately downstream of the electricity exchange meter, before any derivation).

If it is monitoring consumption on a three-phase line, the load indicator reports the sum of the loads of the three phases.

If it is monitoring production on a three-phase line, the production indicator reports the sum of the production of the three phases.

The By-me system also allows to monitor the consumption of individual loads (or groups of loads), as described in the Chapter Individual loads.

The By-me system also allows to display and store the data provided by the Vimar pulse counter interface (for the management of third-party counters that have pulses as output quantity), as described in chapter Pulse counter.

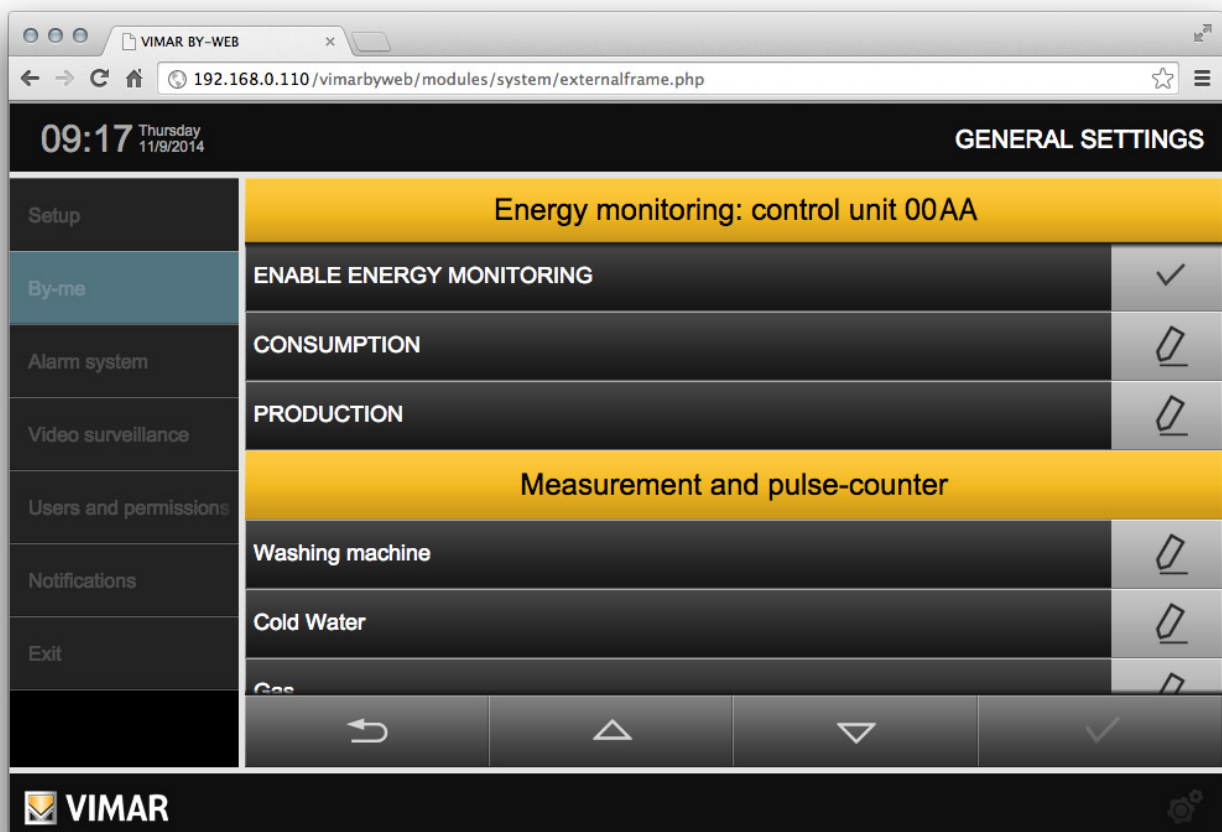
For settings relating to the Energy monitoring, go to "General Settings" -> "By-me" -> "Energy monitoring."

The configuration page is divided into two main sections: the first groups the consumption and production settings at the plant level (Energy monitoring), while the second groups individual meters and pulse counters settings (Meters and pulse counters). Energy monitoring is enabled by selecting "ENABLE ENERGY MONITORING": if disabled, the settings for this feature do not appear.

For settings relating to the Energy monitoring, go to "General Settings" -> "By-me" -> "Energy monitoring."

The configuration page is divided into two main sections: the first groups the consumption and production settings at the plant level (Energy monitoring), while the second groups individual meters and pulse counters settings (Meters and pulse counters). Energy monitoring is enabled by selecting "ENABLE ENERGY MONITORING": if disabled, the settings for this feature do not appear.

The data collected by Energy Monitoring are indicative and not necessarily equivalent to the consumption registered by the supplier of the energy contract.



The screenshot shows the VIMAR BY-WEB interface on a mobile device. The browser address bar displays '192.168.0.110/vimarbyweb/modules/system/externalframe.php'. The page title is 'GENERAL SETTINGS'. The main content area is titled 'Energy monitoring: control unit 00AA'. It features a sidebar menu on the left with items: Setup, By-me, Alarm system, Video surveillance, Users and permissions, Notifications, and Exit. The main content area has a yellow header for 'Energy monitoring: control unit 00AA'. Below this, there are three rows of settings: 'ENABLE ENERGY MONITORING' with a checkmark icon, 'CONSUMPTION' with an edit icon, and 'PRODUCTION' with an edit icon. A second yellow header section is titled 'Measurement and pulse-counter'. Below it are three rows of settings: 'Washing machine' with an edit icon, 'Cold Water' with an edit icon, and 'Gas' with an edit icon. At the bottom of the screen, there is a navigation bar with icons for back, home, search, and refresh. The VIMAR logo is visible in the bottom left corner of the interface.

Energy monitoring

6.2 Power consumption

6.2.1 General settings

The ENERGY MONITORING page in the "By-me" section of the administration allows you to set the operating parameters; they depend largely on the type of energy contract of the system, and consequently for proper compilation it is desirable to have a bill or other documentation from the electricity provider.

On first access the ENERGY MONITORING function is disabled; enabling the corresponding check box (under "ENABLE ENERGY MONITORING"), shows the page where all the functions related to energy monitoring can be configured. To access the "Energy consumption" setup page, select the corresponding entry.

The following configuration parameters are provided:

TYPE OF CONTRACT	You can set one of the following types of contract: <ul style="list-style-type: none">• TIME FRAMES: contract with one or more time frames throughout the day, which corresponds to a different rate.• THRESHOLD: fixed cost contract with up to a certain consumption, and rates for any excess consumption. Depending on the choice of contract, subsequent sections of the page may be enabled.
CURRENCY	Specify the currency to be used to display the costs.
ENABLE CALCULATION OF CO2 EMISSIONS	Specify if you want to view greenhouse gases data or not.
CO2 EMISSIONS	In the event that the emissions calculation of is enabled, allows you to specify the amount of greenhouse gases emitted per kWh of energy consumed.
CONTRACT MAXIMUM POWER	Maximum consumption allowed by the operator.

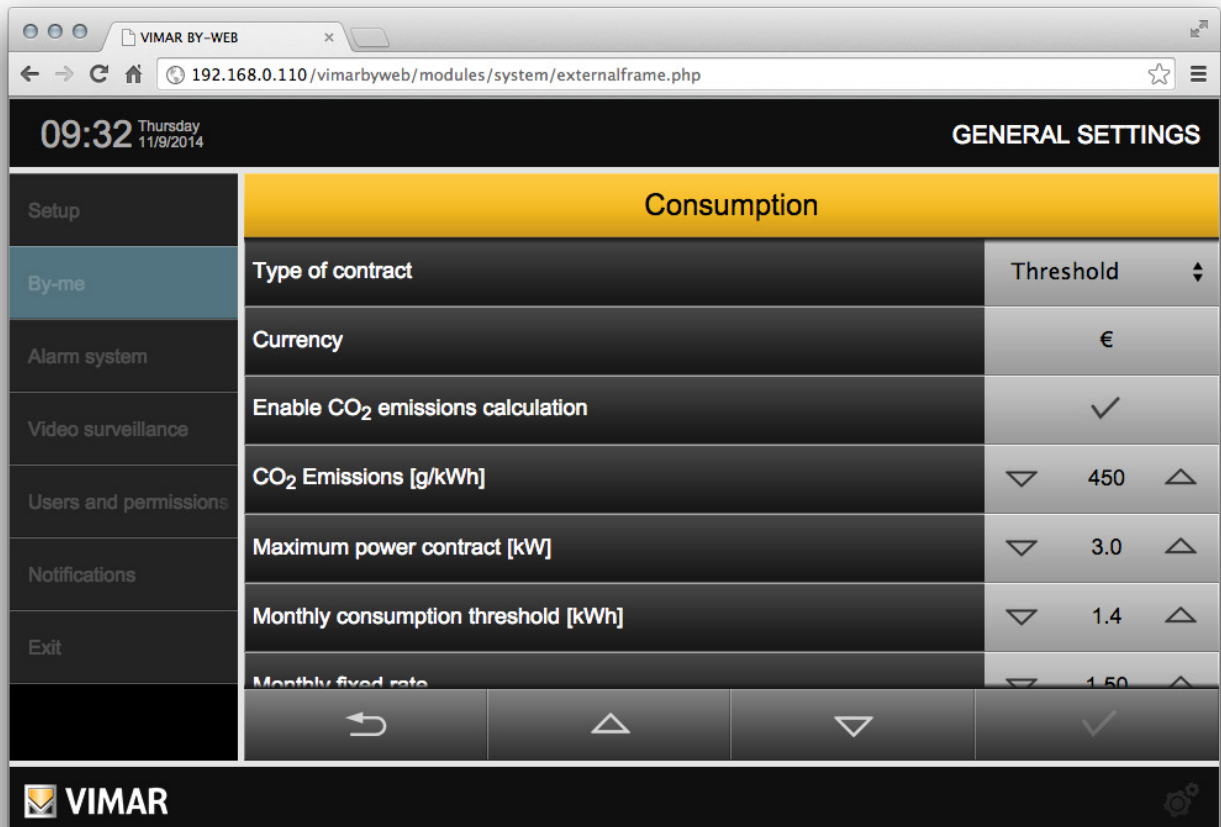
NOTE: The changes made are instantly saved and made available to ENERGY MONITORING ; you do not need to save at the end, but leave the page via the "BACK" button when you are finished setting the parameters required.

Energy monitoring

6.2.2 Contracts with variable threshold

In case of THRESHOLD contract, the following parameters are also required:

MONTHLY CONSUMPTION THRESHOLD	Maximum power consumption beyond which there is an extra cost compared to the basic contract rate.
MONTHLY FIXED RATE	Monthly costs without exceeding the threshold.
COST PER kWh OVER THRESHOLD	Rate applied to the monthly consumption exceeding the threshold.



The screenshot displays the 'Consumption' configuration page in the VIMAR BY-WEB interface. The page is titled 'GENERAL SETTINGS' and 'Consumption'. The sidebar menu includes 'Setup', 'By-me', 'Alarm system', 'Video surveillance', 'Users and permissions', 'Notifications', and 'Exit'. The main content area shows the following configuration fields:

Field	Value	Threshold
Type of contract		
Currency	€	
Enable CO ₂ emissions calculation	✓	
CO ₂ Emissions [g/kWh]	450	
Maximum power contract [kW]	3.0	
Monthly consumption threshold [kWh]	1.4	
Monthly fixed rate	1.50	

The bottom of the screen shows the VIMAR logo and a navigation bar with back, up, down, and confirm buttons.

6.2.3 Contracts at hourly rates

In case of TIME FRAME contracts, specific configuration sections are enabled, which allow you to set all the parameters required so that the Web Server can provide consumption and cost data, according to the energy contract.

6.2.3.1 Hourly rates

The TIME FRAMES section allows to determine how many time frames (at least one, up to a maximum of 3) are covered by the electricity supply contract.

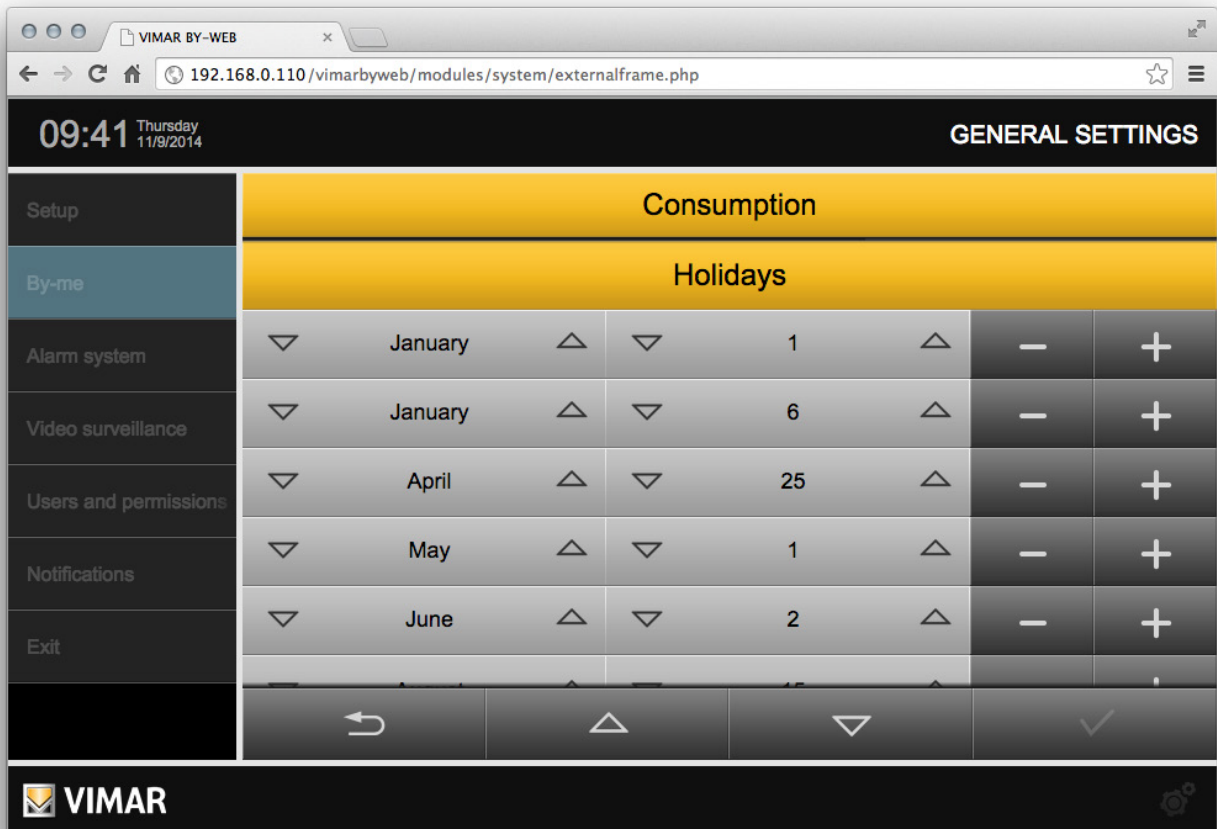
Use the selection box corresponding to each time frame to enable it, and then set the corresponding rate (using a numerical value from the keyboard, after selecting the data field, or through the increase/decrease buttons).

Energy monitoring

6.2.3.2 Holidays

This section allows you to set a series of dates throughout the year, to be considered public holidays. To edit an existing holiday, simply use the scroll buttons to change the month and day, while the "ADD" button allows to insert a new date after the selected one. The "DELETE" button removes a holiday from the list.

NOTE: You must keep at least one holiday in the list, which is why the system does not allow the cancellation of the last line of this list.



The screenshot shows the VIMAR web interface. The browser address bar displays '192.168.0.110/vimarbyweb/modules/system/externalframe.php'. The top status bar shows the time '09:41' and date 'Thursday 11/9/2014'. The page title is 'GENERAL SETTINGS'. A navigation menu on the left includes 'Setup', 'By-me', 'Alarm system', 'Video surveillance', 'Users and permissions', 'Notifications', and 'Exit'. The main content area is titled 'Consumption' and 'Holidays'. It contains a table with the following data:

Month	Day	Control
January	1	- +
January	6	- +
April	25	- +
May	1	- +
June	2	- +

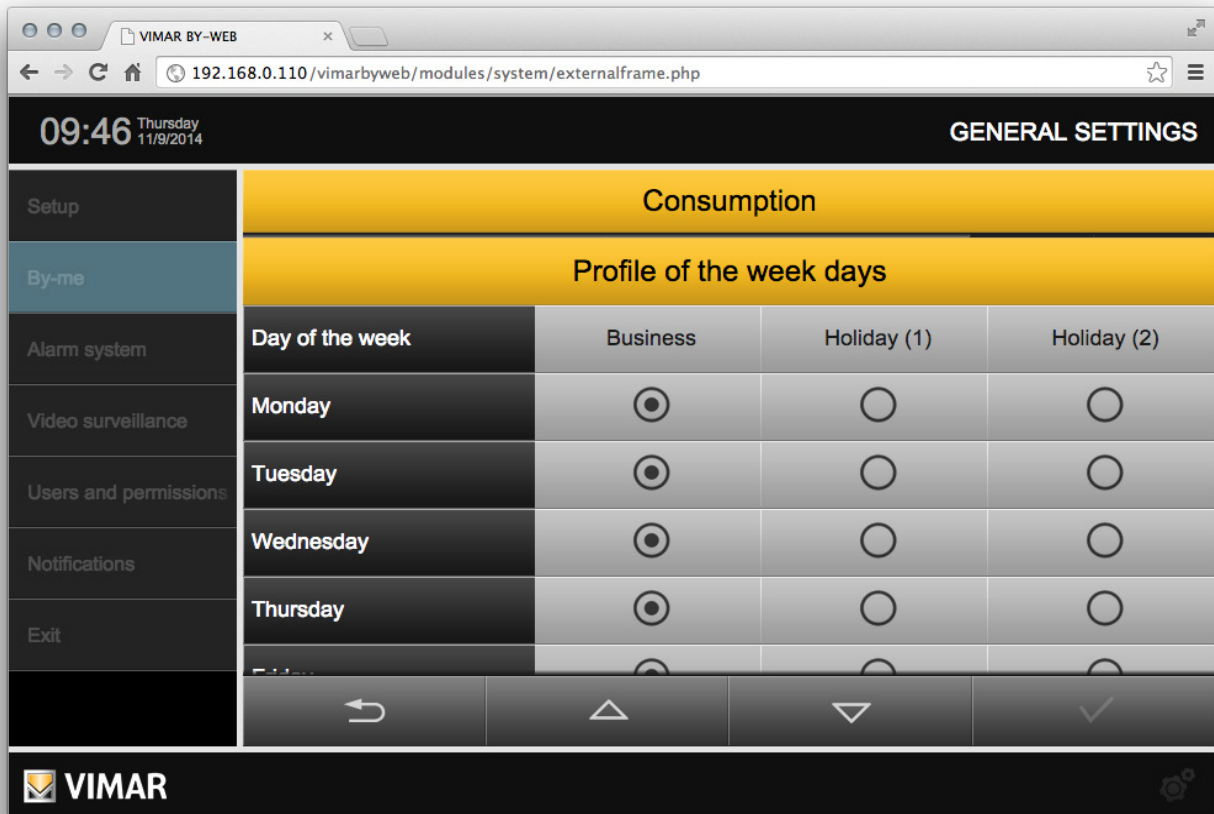
At the bottom of the interface, there are navigation buttons: a back arrow, an up arrow, a down arrow, and a checkmark. The VIMAR logo is visible in the bottom left corner.

Energy monitoring

6.2.3.3 Profile of week days

This section allows you to associate a different time profile to each day of the week, choosing between "WORK", "HOLIDAY 1" and "HOLIDAY 2". Use the selection buttons to associate each weekday to a different profile, whose hourly rate profile you can then determine.

NOTE: the holidays are automatically assigned to profile "HOLIDAY 2".



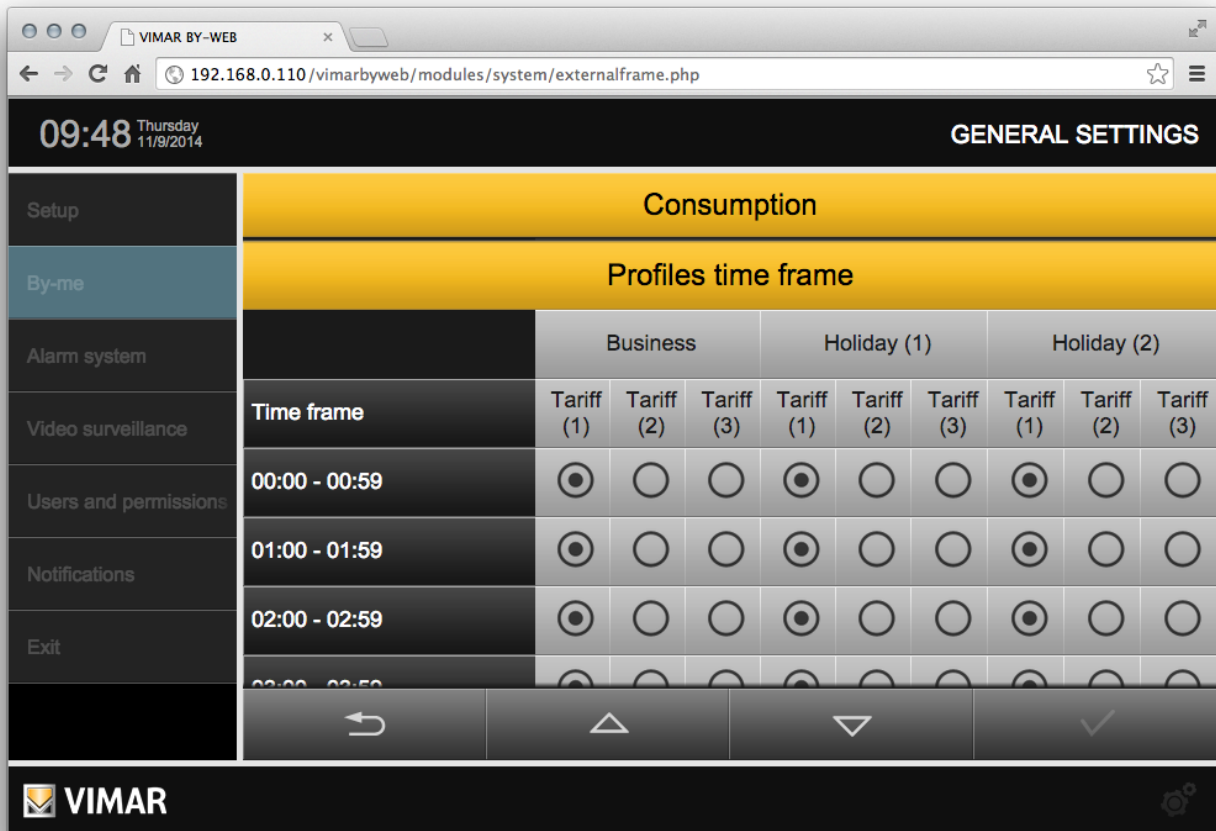
The screenshot shows the VIMAR BY-WEB interface. The browser address bar displays the URL: 192.168.0.110/vimarbyweb/modules/system/externalframe.php. The top status bar shows the time 09:46 and the date Thursday 11/9/2014. The page title is GENERAL SETTINGS. The main content area is titled 'Consumption' and 'Profile of the week days'. A table allows selecting a profile for each day of the week.

Day of the week	Business	Holiday (1)	Holiday (2)
Monday	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Tuesday	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Wednesday	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Thursday	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Friday	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Energy monitoring

6.2.3.4 Profiles times frames

This section allows you to determine for each profile (and thus, for each day of the week and/or holiday) the reference price for each hour; even in this case, use the selection buttons to associate each zone, for each of the profiles, with the rate of reference.



The screenshot shows the 'Profiles time frame' configuration screen in the VIMAR BY-WEB interface. The browser address bar shows the URL: 192.168.0.110/vimarbyweb/modules/system/externalframe.php. The top status bar displays the time 09:48 and the date Thursday 11/9/2014. The page title is 'GENERAL SETTINGS'.

The main content area is divided into a left sidebar and a main table. The sidebar contains the following menu items: Setup, By-me (highlighted), Alarm system, Video surveillance, Users and permissions, Notifications, and Exit.

The main table is titled 'Consumption' and 'Profiles time frame'. It has the following structure:

Time frame	Business			Holiday (1)			Holiday (2)		
	Tariff (1)	Tariff (2)	Tariff (3)	Tariff (1)	Tariff (2)	Tariff (3)	Tariff (1)	Tariff (2)	Tariff (3)
00:00 - 00:59	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
01:00 - 01:59	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
02:00 - 02:59	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
03:00 - 03:59	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

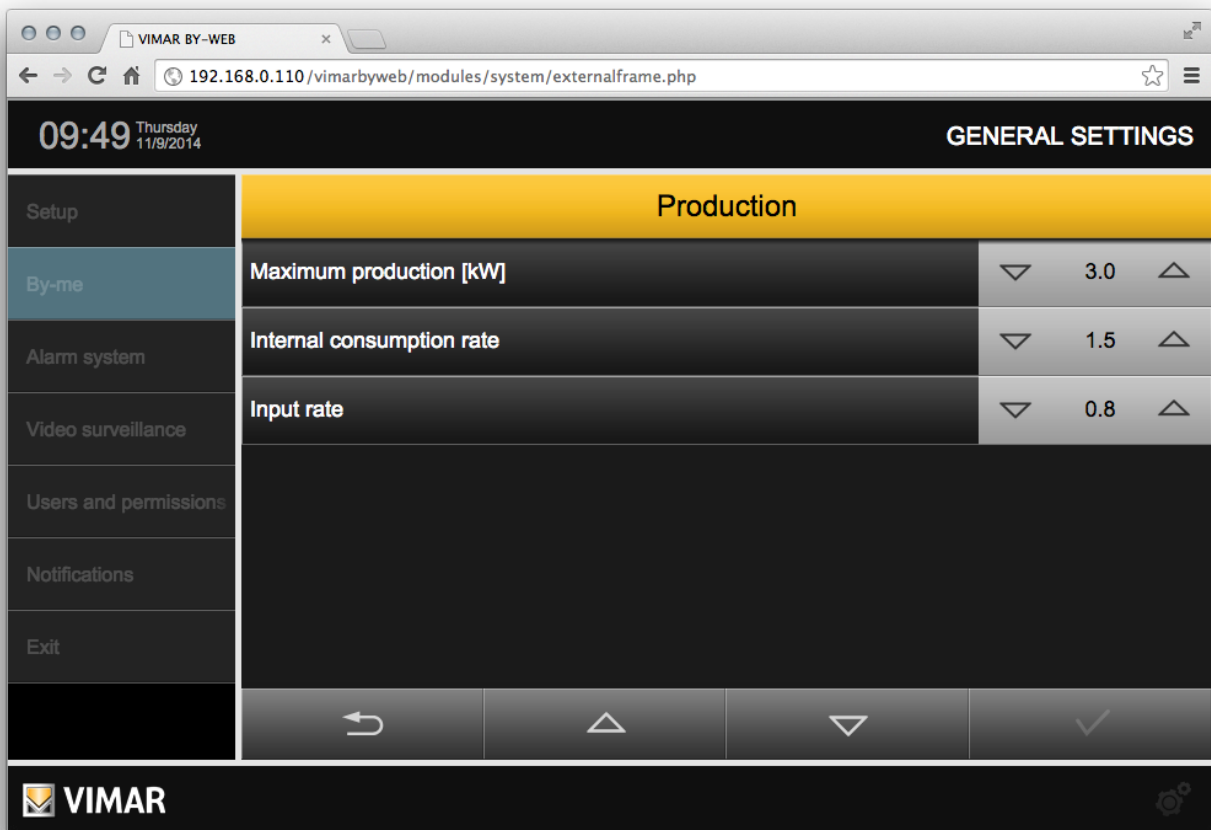
At the bottom of the table, there are four navigation buttons: a back arrow, an up arrow, a down arrow, and a checkmark.

The VIMAR logo is visible in the bottom left corner of the interface.

Energy monitoring

6.3 Electricity production

To access the "Electricity production" setup page, select the corresponding entry.



The following configuration parameters are provided, which allow to manage the different types of contract provided:

MAXIMUM POWER [KW]	Is the expected value of the contract
INTERNAL CONSUMPTION RATE	Represents the value of the contract, for the energy produced by the plant that is used by the system.
INPUT RATE	Represents the value of the contract, for the energy produced by the plant that, not being used by the plant is input into the distribution network.

Note: The values can be changed using the "increase"/"decrease" icons or by directly editing the numeric field.

Important: the economic calculations made by the Web Server must be considered approximate.

Energy monitoring

6.4 Individual loads measurement

The By-me system allows to monitor and store the individual loads (or groups of loads) consumption data associated with independent meters.

To monitor the consumption of a single load (or group of loads supplied from the same power sub-line) a meter of one of the following Vimar devices must be used: 01450, 01451, 01455, 01456, 14537, 19537, 20537.

Important: To manage these meters via the Web Server, it is necessary to insert an SD card into the Web Server.

The configuration of these meters is exported from ETPro in the configuration XML file. After importing the Web Server's XML file generated by ETPro, in the "Meters and pulse counters" section of the "Energy monitoring" page ("General Settings" -> "By-me" -> "Energy monitoring") the "individual" meters configured will be shown.

Selecting the icon for editing the item corresponding to a meter, gives access to a page where the descriptive text can be edited.

Note: The rate for the calculation of the cost associated with the load consumption is the one provided for in the electricity consumption settings (which takes into account the possible time periods specified in the contract).

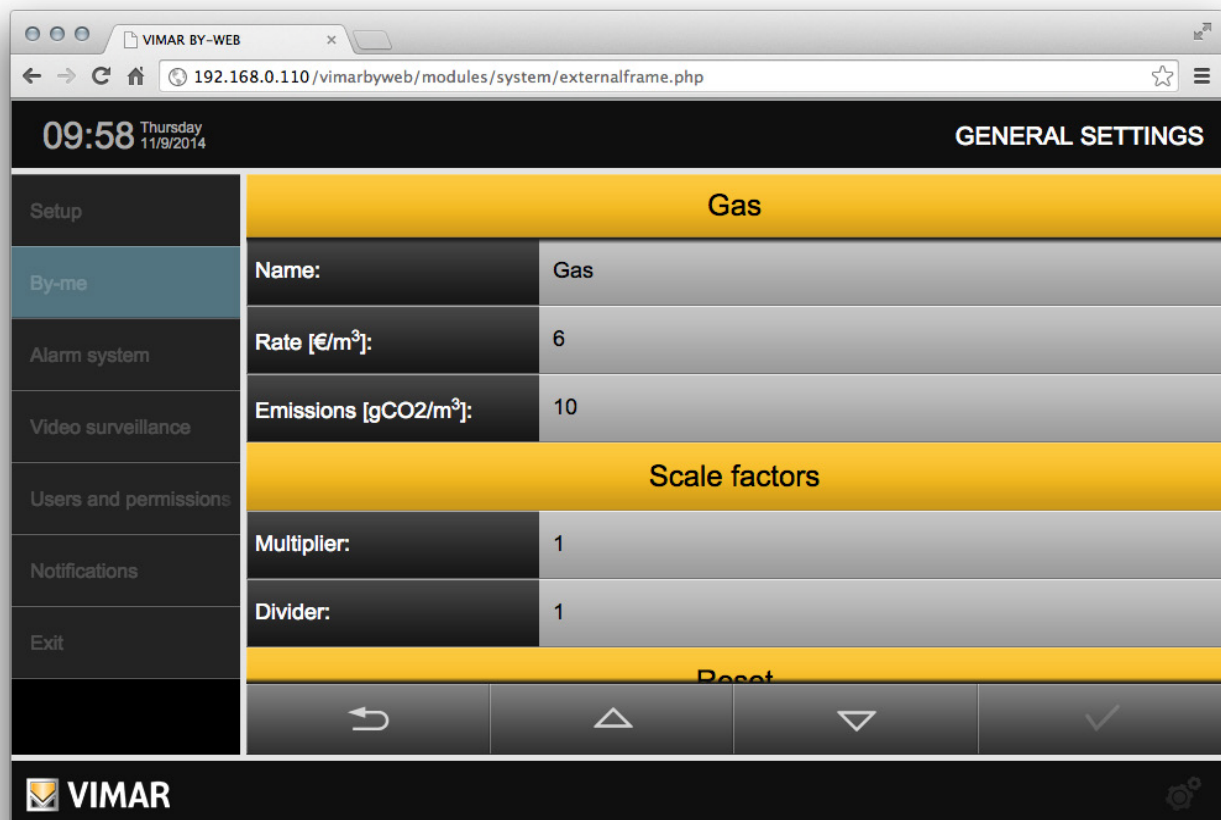
6.5 Pulse-counter

The By-me system allows to track and store data related to the consumption of counters connected with the By-me system through the Vimar pulse counter interfaces (P/N 01452 - Pulse counter interface).

Important: To manage these meters via the Web Server, it is necessary to insert an SD card into the Web Server.

The configuration of these meters is exported from ETPro in the configuration XML file. After importing the Web Server's XML file generated by ETPro, in the "Meters and pulse counters" section of the "Energy monitoring" page ("General Settings" -> "By-me" -> "Energy monitoring") the "pulse counters" configured will be shown.

Selecting the icon for editing the item corresponding to a pulse counter, gives access to the Web Server configuration page.



Below is a description of the configuration parameters provided by the Web Server:

NAME	Description of the counter, editable by typing the desired text
RATE [€/m³]	Expected rate per measured quantity
INPUT [gCO₂/m³]	CO ₂ per quantity measured
Scale factors	The two scale factors (Multiplier and Divider) provided by the pulse counter interface for the specific counter, are read by the Web Server directly from the pulse counter interface and cannot be changed by the Web Server.
Reset: Value	From Web Server, a particular value can be set for the pulse counter. The value is to be understood in the unit of measurement provided for the counter (e.g. m ³ , liters,...) and set from the pulse counter interface.

Users and authorisations

7. Users and authorisations

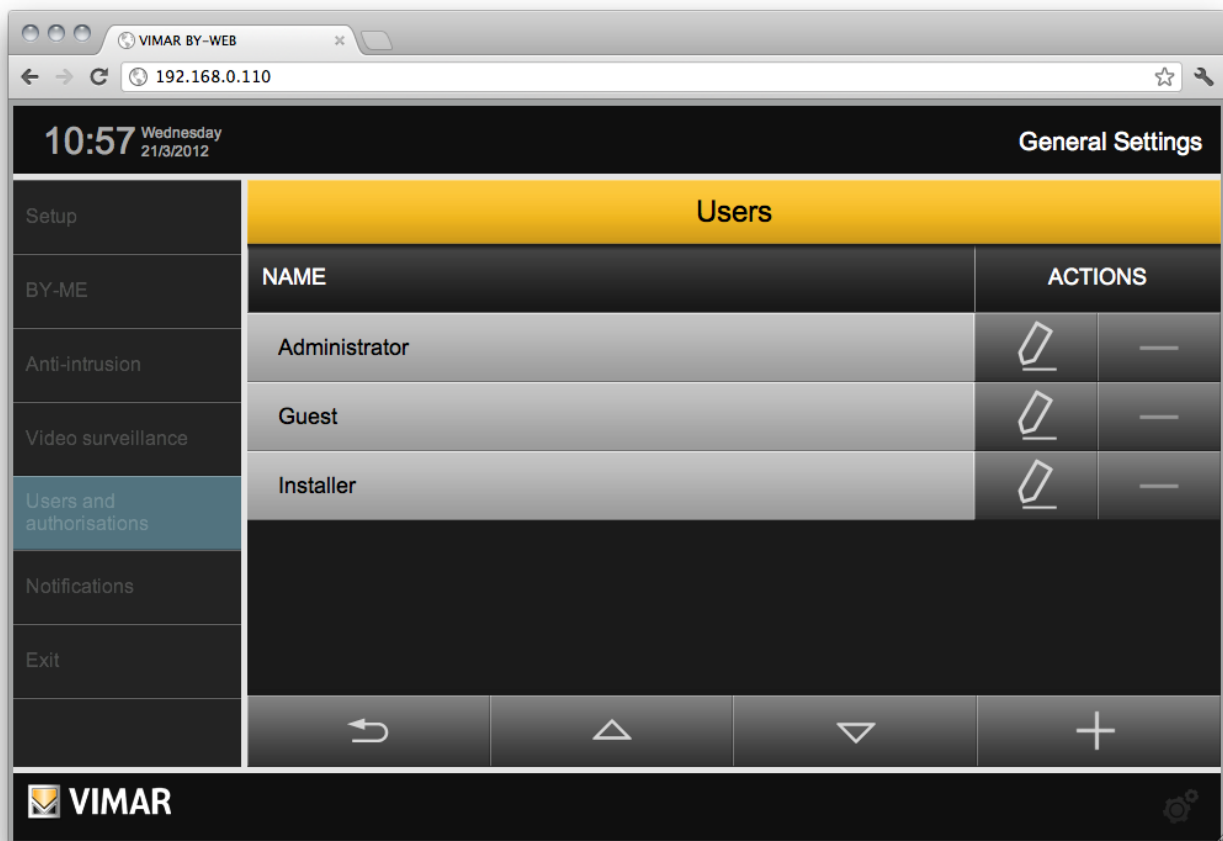
7.1 Introduction

By-Web allows you to configure multiple accounts for access to supervision and to specify what rights they should have. Users and permissions management is divided into 3 aspects:

USER GROUPS	Represent homogeneous groups of users allowed to view and perform operations on By-web. Default: administrators, installers and users.
USERS	The actual account to access By-Web. They can belong to one or more groups, inheriting their permissions.
AUTHORISATIONS	The rights to view and perform operation for different user groups.

7.2 Users

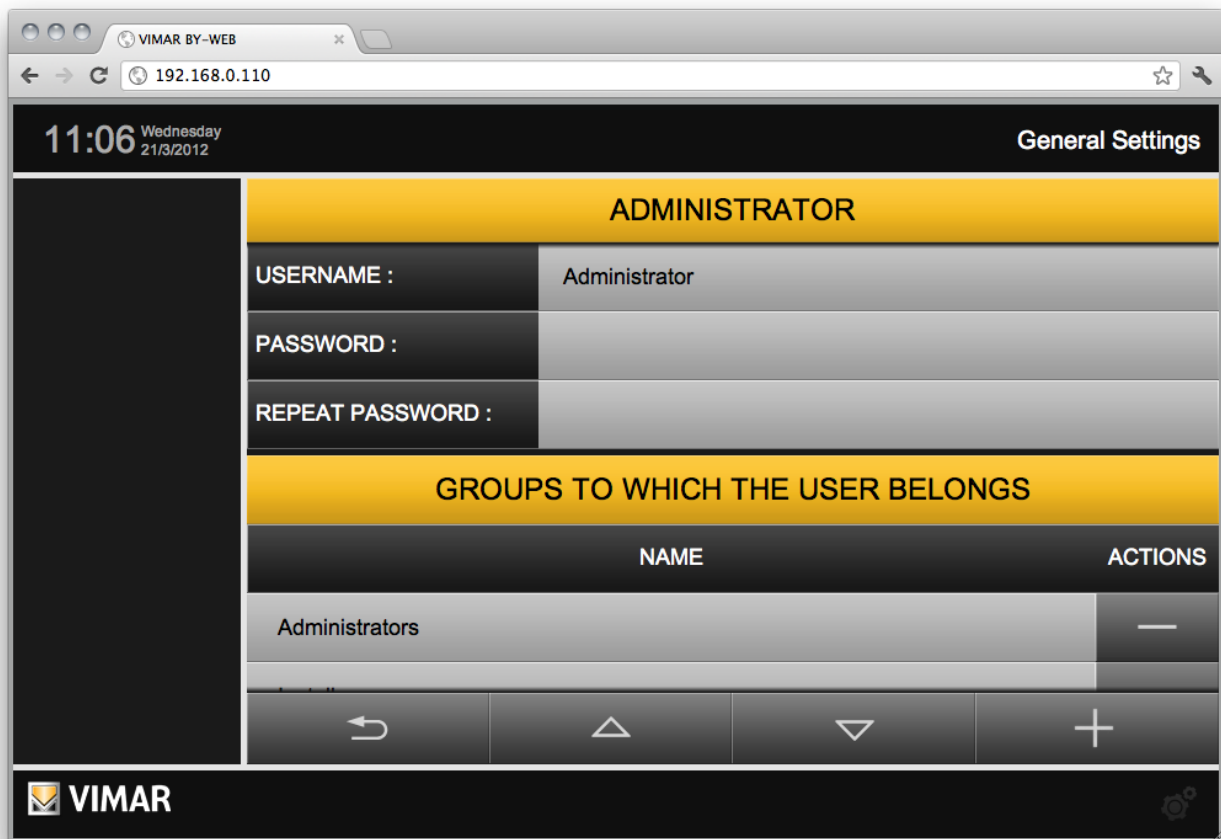
The page "USER" in the "USERS AND AUTHORIZATIONS" menu of the administration allows you to configure the By-web login accounts. The following figure shows how the page looks the first time, with the factory settings:



You can create new users using the ADD button at the bottom right; in this case, a row is added to the list, and you can specify the description associated with the new user (e.g. "Mark").

Using the edit button in correspondence of a user, you can access his tab, through which it is possible to customize his attributes:

Users and authorisations



11:06 Wednesday 21/3/2012 General Settings

ADMINISTRATOR

USERNAME : Administrator

PASSWORD :

REPEAT PASSWORD :

GROUPS TO WHICH THE USER BELONGS

NAME	ACTIONS
Administrators	—

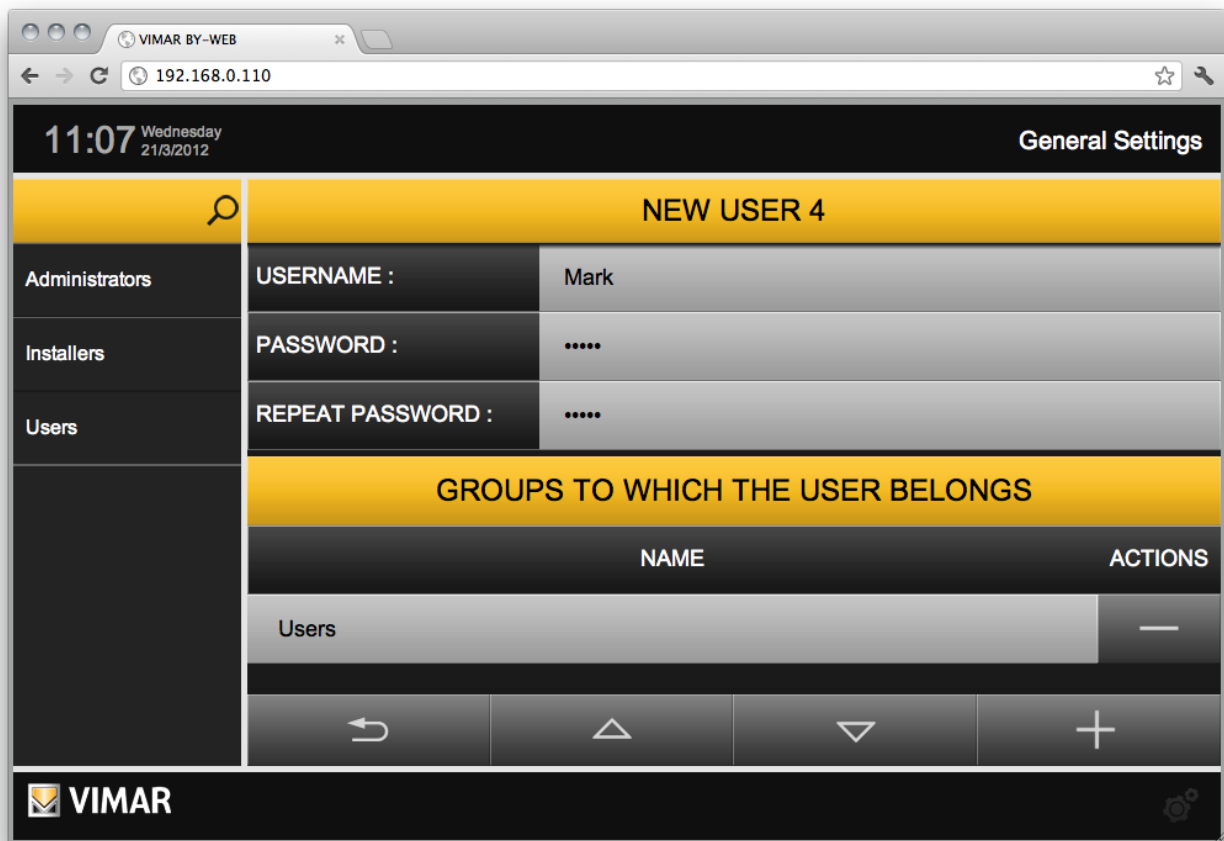
↶
▲
▼
+

 **VIMAR** ⚙️

Each user must specify USERNAME, which must be unique for all users of the system, and PASSWORD, which must be entered twice for safety reasons.

The bottom of the page ("GROUP TO WHICH THE USER BELONGS") allows to determine which groups should be associated with the user; through the ADD button you can drag the desired groups to this portion of the paper, selecting them on the left side the screen:

Users and authorisations



11:07 Wednesday 21/3/2012 General Settings

NEW USER 4

Administrators **USERNAME :** Mark


Installers **PASSWORD :**

Users **REPEAT PASSWORD :**

GROUPS TO WHICH THE USER BELONGS

NAME	ACTIONS
Users	—

Navigation: ↶ ▲ ▼ +

 **VIMAR**

Users inherit the permissions of all the groups they belong to. You can at any time remove the association between a user and a group, or permanently delete the user, through the appropriate DELETE buttons.

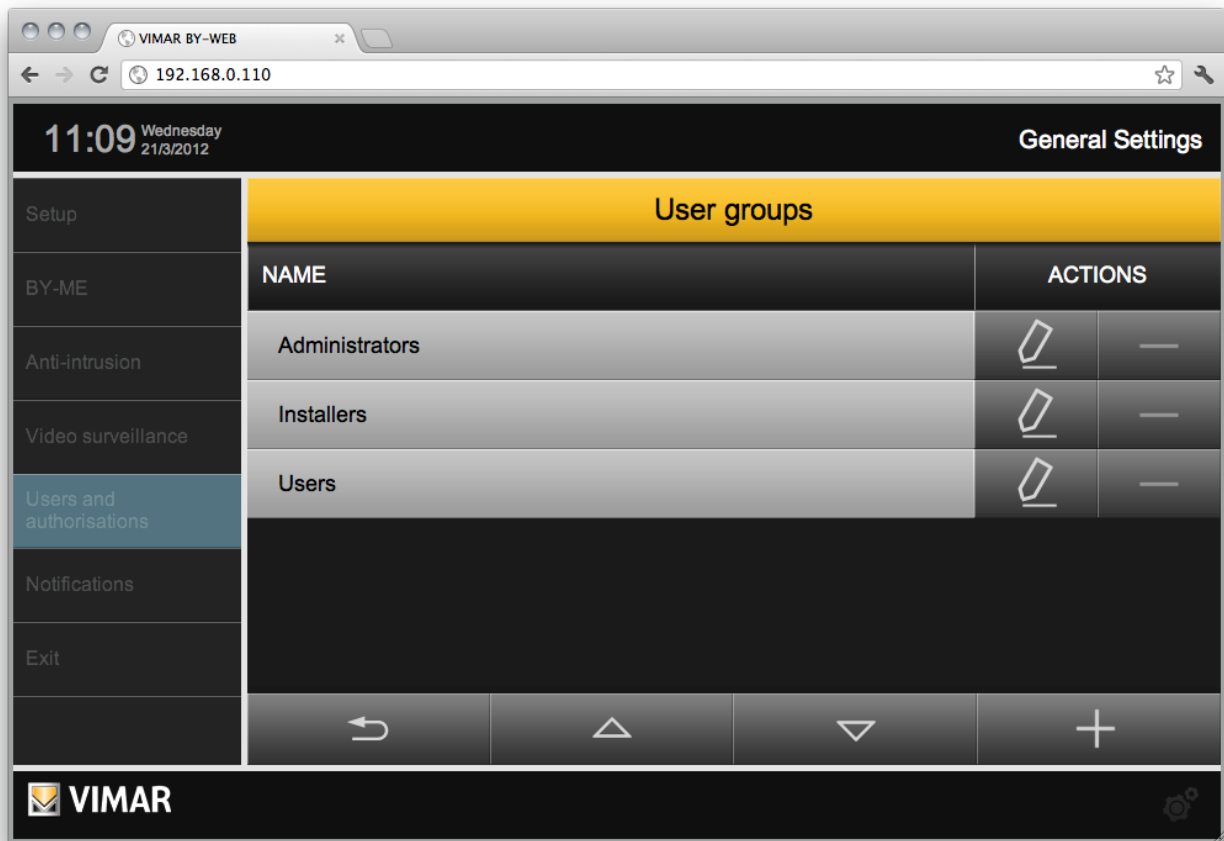
NOTE: You cannot delete default users and their association to the default groups; you can only edit the name and login credentials.

Users and authorisations







7.3 User Groups

The page "GROUPS" in the "USERS AND AUTHORIZATIONS" sections of the administration allows you to manage user groups; similar to that seen for users, this page allows you to create new groups or edit existing ones.

Using the ADD button, you can create a new user group, the description can be modified directly in the list, just by editing the default description.



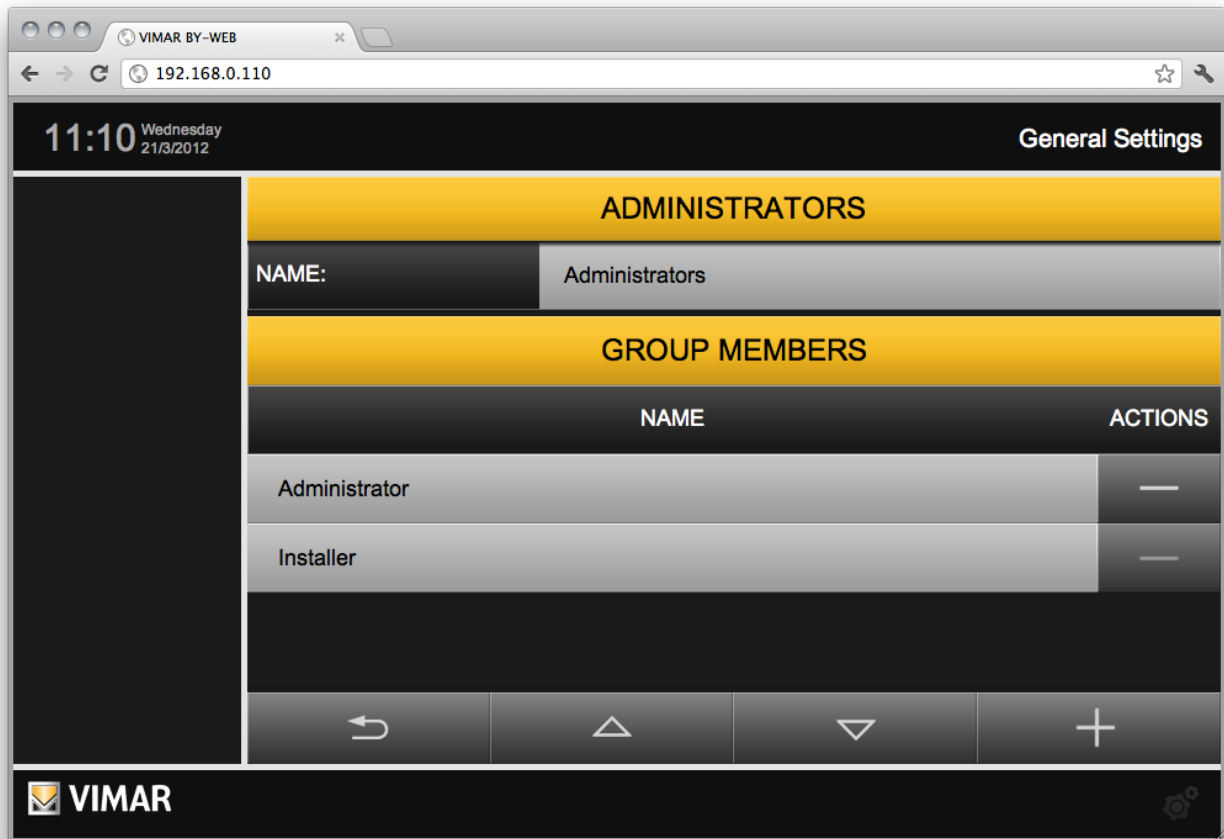
The screenshot shows the VIMAR BY-WEB administration interface. The browser address bar displays '192.168.0.110'. The top navigation bar includes the time '11:09', the date 'Wednesday 21/3/2012', and the 'General Settings' link. A sidebar on the left contains navigation options: Setup, BY-ME, Anti-intrusion, Video surveillance, Users and authorisations (highlighted), Notifications, and Exit. The main content area is titled 'User groups' and contains a table with the following data:

NAME	ACTIONS
Administrators	 
Installers	 
Users	 

At the bottom of the interface, there is a navigation bar with icons for back, home, forward, and a plus sign for adding new items. The VIMAR logo is visible in the bottom left corner.

Users and authorisations

The "EDIT" button displays the tab of the user group:

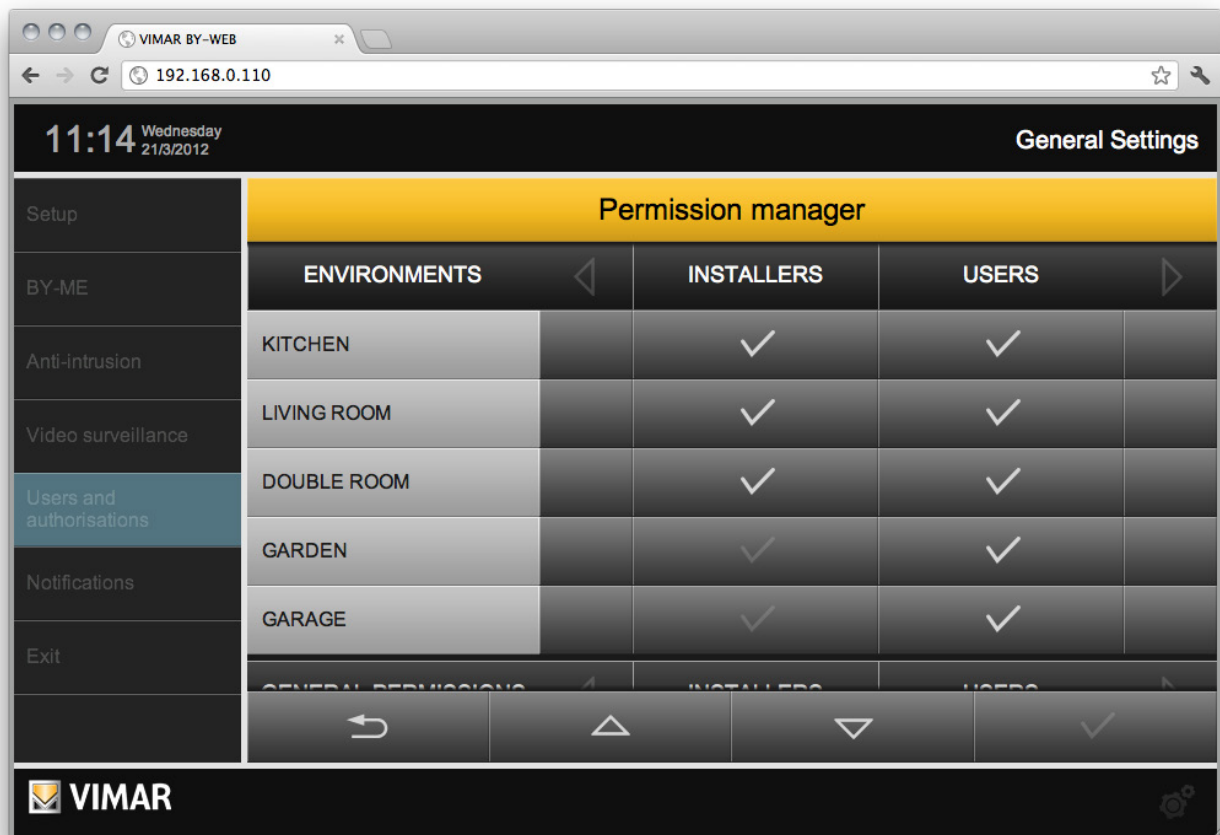


This page only allows you to change the description of the group (if not done from the list of groups) and to associate users with the group; this operation is similar to what can be done from individual users tabs.

Users and authorisations

7.4 Authorizations

The page "AUTHORIZATIONS" allows you to specify, for each of the user groups, the different authorizations to view the environments and perform certain operations. The page looks as shown below:



The first part consists of rows in a table containing a list of all environments in the project, and in the columns of user groups. By clicking on the checkboxes you can enable or disable the different user groups to access the corresponding environments; when created, the environments are visible by all user groups.

NOTE: You cannot change the permissions of the ADMINISTRATORS group, which owns the rights to access all environments and perform all operations, as well as the ability to access the USERS AND AUTHORIZATIONS configuration section.

The bottom of the page allows you to determine which execution rights are granted to user groups, in particular, By-Web provides the following rights:

SEE SAI STATUS WITHOUT PIN	It allows you to view the status of the alarm system before typing a valid PIN.
LEVEL 1 OPERATIONS	Access to the popup configuration of thermostats and events, learning of scenarios, setting the FM radio memory.
LEVEL 2 OPERATIONS	Access to the configuration popup for time scheduling of thermostats and events.
TECHNICAL LEVEL 1	Access to the climate controller configuration popup. Allows editing of the current mode setpoints of the climate controller.
TECHNICAL LEVEL 2	Access to the operating mode configuration popup and to the time programming of the climate controller.

Also in this case, use the checkboxes to enable or disable the various user groups when performing the corresponding actions. Users without specific permission cannot perform the corresponding operations, unless entering the credentials of another user (belonging to a group that has the required authorizations) through a special login window.

Users and authorisations

7.4.1 Levels and functionality

LEVEL 0 (DEFAULT):

- Actuators status/command display
Status + command: relay actuators, shutters actuators, dimmer actuators (all the devices that are part of the Lighting, Shutters functions)
- Thermostats status display
Thermostats status. Display of the thermostat icons in the environments and functions window. (clicking with the mouse on the icon, a popup appears for the "promotion" request) to a level with higher privileges.
- Scenarios activation
- IP Camera Display

LEVEL 1:

- Using the functionality of Energy Monitoring
- Thermostat, Operating mode setting
Operating mode. (OFF, OFF time, MANUAL, PROGRAMMED,...), setpoint of the various modes. In fact, this level can open the popup of the thermostat and carry out all the visible settings in the popup EXCEPT for the time programming setting, which opens a dedicated popup. At the request of the time programming the popup appears for promotion to higher level.
- Setting the Events
- Play/Pause event
- Scenario learning
- Load Control, Setting "Forced ON" mode
- FM tuner, setting station memory
- Edit Widget arrangement for environments with "Map" features

LEVEL 2:

- Thermostat, Advanced Settings
- Weekly time schedule, climate config popup (change season, change unit of measure)
- Events, Advanced settings, timer (weekly, cyclical program,...)

TECHNICAL LEVEL 0:

- Climate controllers status display
Display of the climate controllers icons in the environments and functions windows. (Clicking with the mouse on the icon, a popup appears for the "promotion" request) to a level with higher privileges.
This level is assigned by default to the "Users" group.

TECHNICAL LEVEL 1:

- Climate controller, setting of seasonal mode and setpoint.
Comfort and Economy modes setpoint (if set as current modes). In fact, this level allows to open the popup of the climate controller, to access to the seasonal mode setting popup (if provided by the system) and to change the setpoint of the current mode (whether it is Comfort or Economy). At the request of the time programming or operating mode change (Auto, Comfort, Economy, Off) the popup appears for promotion to the higher level.

TECHNICAL LEVEL 2:

- Climate controller, setting of operating mode and time programming.
This level provides access to the operating mode setting popup (Auto, Comfort, Economy, Off) and to the time programming the setting popup (with the relative setpoints).

Users and authorisations

7.4.2 The technique of "promotion" to higher authorization levels

When a user tries to access a function not granted by his permission level, he is prompted with a pop-up window for entering credentials (passwords). If you enter the password of a user who has permission to access the function, the "promotion" of the user level takes place.

After completing the operation and return to the initial window, the user gets back his permission.

7.4.3 Groups-Permissions Association

Groups	0	1	2	0 Technical	1 Technical	2 Technical	Environment 1	Environment 2	...	No Environment
Administrators	X	X	X	X	X	X	X	X	X	X
Installers	X	X	X	X	X	X	X	X	X	X
Users	X			X			X	X	X	X
....

For groups other than Administrators group can still modify the associated permissions.

7.4.4 The Administrators Group

The **Administrators** group has all permissions and these cannot be removed. This group does not appear in the list of groups for assigning permissions (since in any case the permissions of this group cannot be changed).

It is still visible in the list of groups in the users creation dialog, for the association users/groups.

The **Administrators** group is associated by default with level 2 (advanced) and cannot be changed.

The **Administrators** group is the only group that has all the permissions of the "administrative" management (user management) of the web server.

The **Administrators** group is associated by default with technical level 2 (advanced) and cannot be changed.

7.4.5 The Installers Group

The **Installers** group has the permission of administration of the **Administrators** group **EXCEPT** for those relating to user management. You can change the permissions of this group and the list of environments which the group can view.

The **Installers** group is associated by default with level 2 (advanced), but it can still be changed.

The **Installers** group is associated by default with technical level 2 (advanced), but it can still be changed.

7.4.6 The Users Group

The **Users** group has very few administrative permissions: it can only change the language and set the date/time.

You can change the permissions of this group and the list of environments which the group can view.

The **Users** group is associated by default with level 0 (basic), but it can still be changed.

The **Users** group is associated by default with technical level 0 (basic), but it can still be changed.

Multimedia Touch 10

8. Multimedia Touch 10 (cod. 21553 or 21553.1 or 21553.2)

For associating Multimedia Touch 10 of the Web Server (code 01945-01946) refer to the Multimedia Touch 10 installer manual.

Upon the association between Web Server and Multimedia Touch 10 a specific user is created for the Multimedia Touch 10, whose name can be defined by the user, allowing the Multimedia Touch 10 to log in automatically each time the home automation application is launched. This user can ONLY be used by Multimedia Touch 10.

To properly remove this user from the Web Server (elimination of the association between Multimedia Touch 10 and Web Server), the Vimar Web Server configuration must be Restored to Factory Settings from the configuration menu of the Multimedia Touch 10".

From the Web Server configuration menu there is still a chance to see the list of Multimedia Touch 10 configured in the web server and remove them from the list as needed. To do this, go to "General settings" -> "By-me" -> "Multimedia Touch 10" and press the "-" button of the Multimedia Touch 10 user to be removed from the Web Server (to be used ONLY if the removal procedure laid down in the configuration of the Multimedia touch 10 cannot be used).

To change the Multimedia Touch default user privileges, access the Web Server with a Browser from a PC, login as **Administrator** and access the GENERAL SETTINGS from the USERS AND AUTHORIZATIONS drop down menu, select AUTHORIZATIONS and change the privileges of the group related to the Multimedia Touch.

The Web Server General Settings cannot be configured from the Multimedia Touch 10, is only allowed to change the language of the Web Server.

NOTE: from the Multimedia Touch 10 you can only change the language of the Web Server
--

Starting from software version 1.4.08, the Multimedia Video Touch Screen 10in has a section dedicated to the management of the cameras.

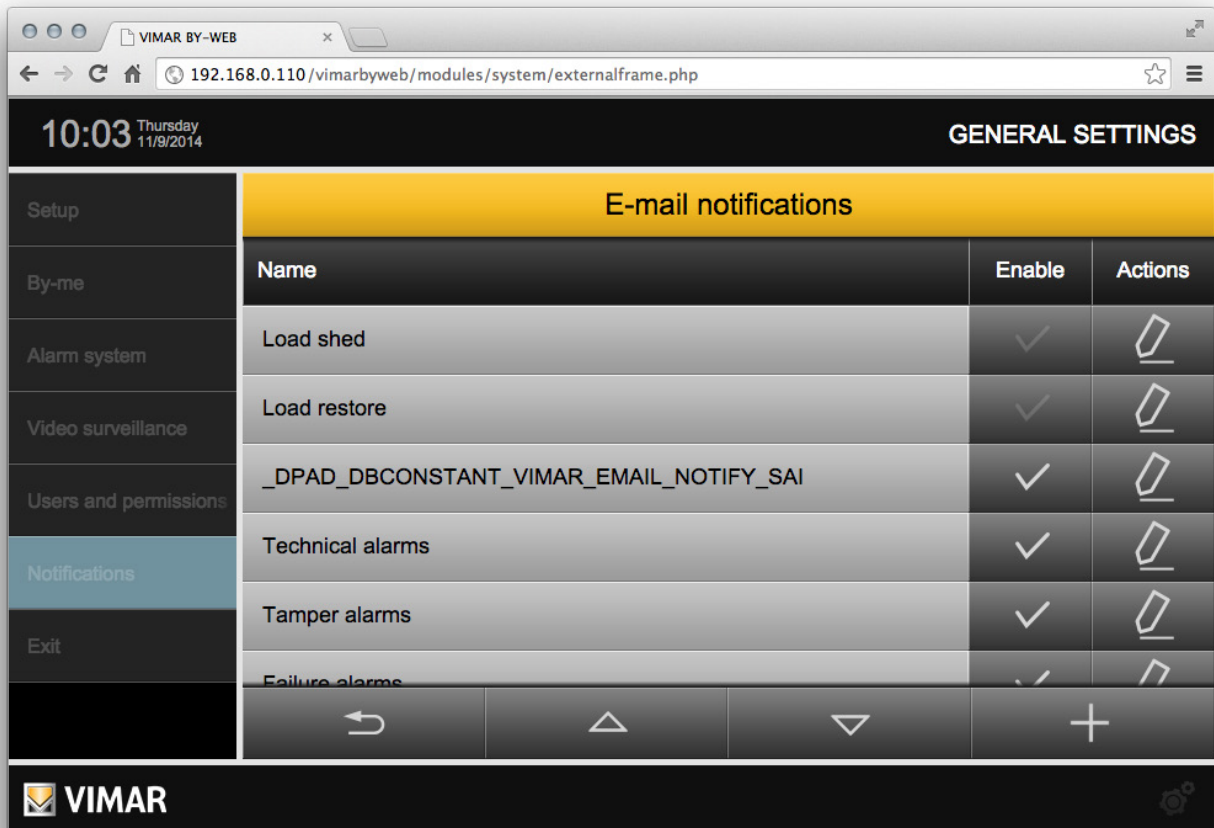
If a Multimedia Touch 10 provided with that version (or later) connects to a Web Server with version 1.5 (or later), the main menu does not display the "video surveillance" entry, because the camera management takes place from the special section of the Multimedia Touch 10 application.

The "Video surveillance" menu entry is still displayed if you access the web server from a client other than the Multimedia Touch 10.







Multimedia Touch 10

9 Notifications by email

The page "NOTIFICATIONS" of the administration menu ("General settings " -> "Notifications" allows to set email notifications as a result of certain events handled by the Web Server.



The screenshot shows a web browser window with the URL `192.168.0.110/vimarbyweb/modules/system/externalframe.php`. The page title is "GENERAL SETTINGS" and the time is 10:03 Thursday 11/9/2014. The main content area is titled "E-mail notifications" and contains a table with the following data:

Name	Enable	Actions
Load shed	<input checked="" type="checkbox"/>	
Load restore	<input checked="" type="checkbox"/>	
_DPAD_DBCONSTANT_VIMAR_EMAIL_NOTIFY_SAI	<input checked="" type="checkbox"/>	
Technical alarms	<input checked="" type="checkbox"/>	
Tamper alarms	<input checked="" type="checkbox"/>	
Failure alarms	<input checked="" type="checkbox"/>	

Each type of event handled by the Web Server has a corresponding row in the table of the configuration page.

For each event type, it is possible to enable email notification and access the configuration page.

For each event type, it is possible to define a specific group of recipients, email subject, and email message.



Below is the list of the event types that can be associated, independently, with an email notification:

Event type	Description
Discontinued loads	Notification of the first discontinued load by the load control device. The load control device is intervened due to a consumption above the set threshold. Note: This feature requires that the system includes a load control device and that it is correctly configured in the Web Server.
Loads reset	Notification of the reset of the last load by the load control device. The load control system has restored all the previously discontinued loads: consumption is back within the set threshold. Note: This feature requires that the system includes a load control device and that it is correctly configured in the Web Server.
Intruder Alarm	Notification of the occurrence of an "intrusion" alarm by the intrusion detection system By-me. Note: This feature requires that the system includes the Vimar intrusion detection system and that it is correctly configured in the Web Server.
By-alarm status notifications	Notification of state events sent by the control panel of the By-alarm intrusion detection alarm system.
By-alarm area notifications	Notification of changes in status of activation/alarm of the areas. You can configure which changes in status must be notified for each of the areas configured in the By-alarm system.

Notifications by email

<p>Technical alarms</p>	<p>Notification of the occurrence of a "technical" alarm by the By-me system.</p> <p>Note: This feature is available only if provided by the By-me system and if it has been correctly configured on the Web Server.</p>
<p>Tamper alarms</p>	<p>Notification of the occurrence of a "tamper" alarm by the intrusion detection system By-me.</p> <p>Note: This feature requires that the system includes the Vimar intrusion detection system and that it is correctly configured in the Web Server.</p>
<p>Malfunction alarms</p>	<p>Notification of the occurrence of a "Device malfunction" alarm by the intrusion detection system By-me.</p> <p>Note: This feature requires that the system includes the Vimar intrusion detection system and that it is correctly configured in the Web Server.</p>
<p>Video Intercom notifications</p>	<p>Notification of a new video message.</p> <p>Note: This feature is available if the system is provided with at least one Multimedia Touch 10, connected to the 2-wire video intercom system and the Multimedia Touch 10 has been appropriately configured in the web server (see the chapter of this manual on video messages).</p>
<p>Notifications of state change events relating to 1 bit objects</p>	<p>It is possible to receive e-mail notifications of the passage from a pre-set state of 1 bit objects, belonging to the "Automation" category or the KNX integration objects category (1 bit).</p> <p>Note: this function is introduced from version 2.1 of the Web Server software onwards. To configure these notifications, refer to the chapter on "Notifications of state change events relating to 1 bit objects".</p>

Each entry in the above table corresponds to the following icons:

	<p>Allows to enable this notification: Enable/disable via "toggle". The enable status is shown by the icon:</p> <p><input type="checkbox"/> Disabled</p> <p><input checked="" type="checkbox"/> Enabled</p>
	<p>Press the button to access the parameter configuration page for sending email notifications related to the specific event:</p> <ul style="list-style-type: none"> • Destination address(es) (separate multiple addresses by ";") • CC address(es) (separate multiple addresses by ";") • Subject of the message. • Text of the message <p>Note: the detail of the notification, if provided, will be appended to the text set in this page, so you may want to insert a generic text that identifies the email as coming from the By-me system after the specific event.</p> <p>In the case of setting the "By-alarm intrusion detection alarm system area notifications", there are additional configuration fields: refer to the next chapter "By-alarm intrusion detection alarm system area notifications".</p> <p>When setting "Notifications of state change events relating to 1 bit objects", there are other configuration fields: refer to the following chapter, "Notifications of state change events relating to 1 bit objects".</p>

By-alarm status notifications

The Web Server enables e-mail notification of the following status events sent by the By-alarm control panel:

- Area status change
- Control panel tamper
- No mains on control panel
- Low battery
- No battery
- No PSTN line
- No GSM line
- GSM line jamming
- Keypad tamper (if at least one keypad is in Tamper alarm status)
- Input module tamper (if at least one expansion is in Tamper alarm status)
- Output module tamper (if at least one expansion is in Tamper alarm status)
- Zone tamper (if at least one zone is in Tamper alarm status)
- Inserter tamper (if at least one inserter is in Tamper alarm status)
- Radio devices battery low (if at least one device has a low battery)
- No control panel communication

Notifications by email

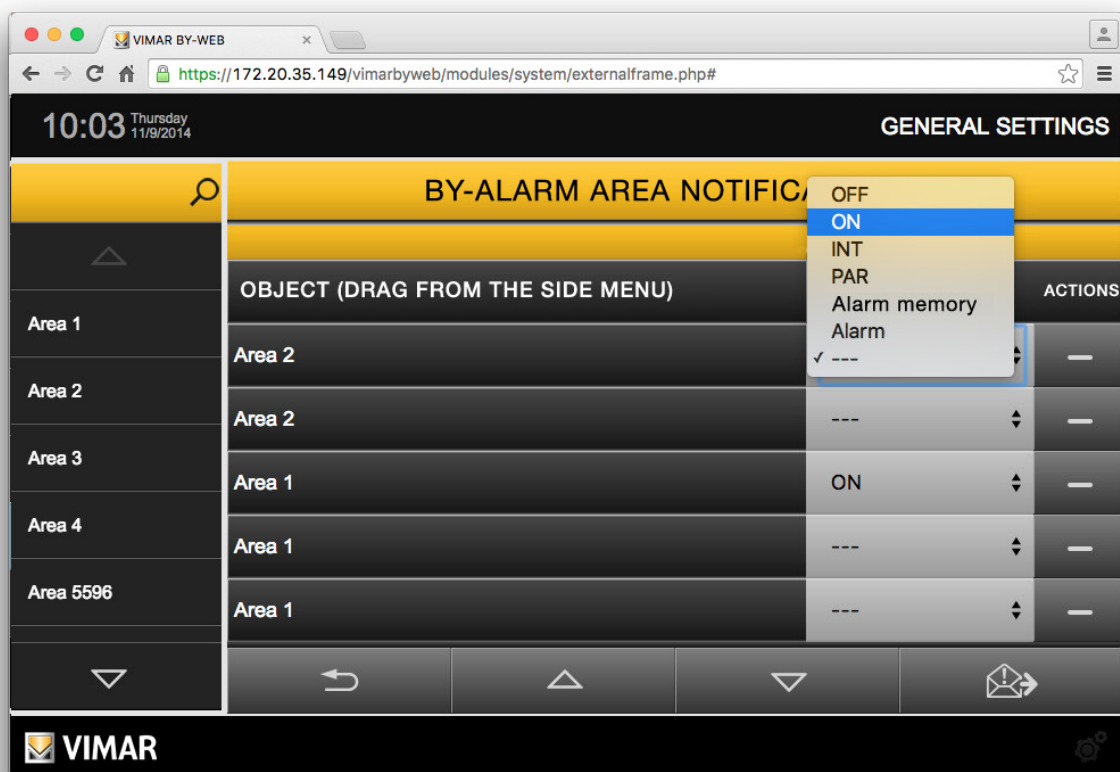
By-alarm area notifications

The Web Server enables, flexibly and for each configured area, notifying the specific state changes by email, as described below:

1. Enter the data needed to send the email: Addressee, CC if any, Subject, and any text.
2. Drag the area for which you want to notify a specific status from the left column to the part of the page under the "OBJECT (DRAG FROM THE SIDE MENU)" row; a row will appear in the list at the bottom of the page.
3. Select the push button of the row corresponding to the "CONDITION" column. A drop-down menu will appear for selecting the state for which you would like to be notified via email.

The following states are possible:

- a. OFF
- b. ON
- c. INT
- d. PAR
- e. Alarm memory
- f. Alarm
- g. ---



You can delete a previously created row, linked to an area, by pressing the "-" button located on the right side of the row.

Notifications by email

Notifications of state change events relating to 1 bit objects

The Web Server can be used to notify by e-mail of the passage from a pre-set state of a 1 bit object (belonging to the "Automation" category or the KNX integration objects category), and set the descriptive text of the notification.

The configuration procedure described below creates an association between an e-mail notification and the passage from a specific state of a 1 bit object.

E.g. If you want the Web Server to send a notification e-mail when a 1 bit object passes to state 1 (e.g. door opening notification) and when it returns to state 0 (e.g. door closing), you must create two separate notifications, with the corresponding condition and texts.

The configuration involves the following steps:

1. To create a new notification, press "+" in the bottom right-hand corner of the "notifications via e-mail" window: a new row is created in the list of notifications, called "New email notification".

It is possible to edit the notification name by positioning the cursor in the name field of the corresponding row and editing the text.

After creating the notification, it is disabled: to enable the notification, press "v" (Enable/Disabled) in the corresponding row.

2. Press the edit button on the corresponding row to access the notification settings page.
3. Enter the data needed to send the e-mail: Recipient, any CC, Subject, descriptive text of the notified event.
4. Drag the object for which you want to notify a specific status from the left column to the part of the page under the "OBJECT (DRAG FROM THE SIDE MENU" row; a row will appear in the list at the bottom of the page.

Note: only one 1-bit object can be associated to each created notification (in the previously described categories).

The object can be deleted by pressing "-" to the right of the row.

5. Set the state of the object you wish to notify using the drop-down "Condition" menu in the row of the dragged object.
6. Having configured the notification, it is possible to send a test e-mail by pressing the button in the bottom right-hand corner (e-mail send test).

To delete a notification press "-" to the right of the notification row in the "Notifications via e-mail" page.

To enable or disable a notification use "v" (Enable/Disable) in the corresponding row.

Mobile

10. Mobile

If you use the Web Server from mobile devices or VTS 10 you can only access certain functions of the General Settings menu.

The menu is displayed in full, but most of the features are greyed out and are not selectable, you can still use the SETUP and EXIT menus.


From the SETUP drop down menu you can access the screen to choose the Web Server language (see section 2.2), the other options are not available.

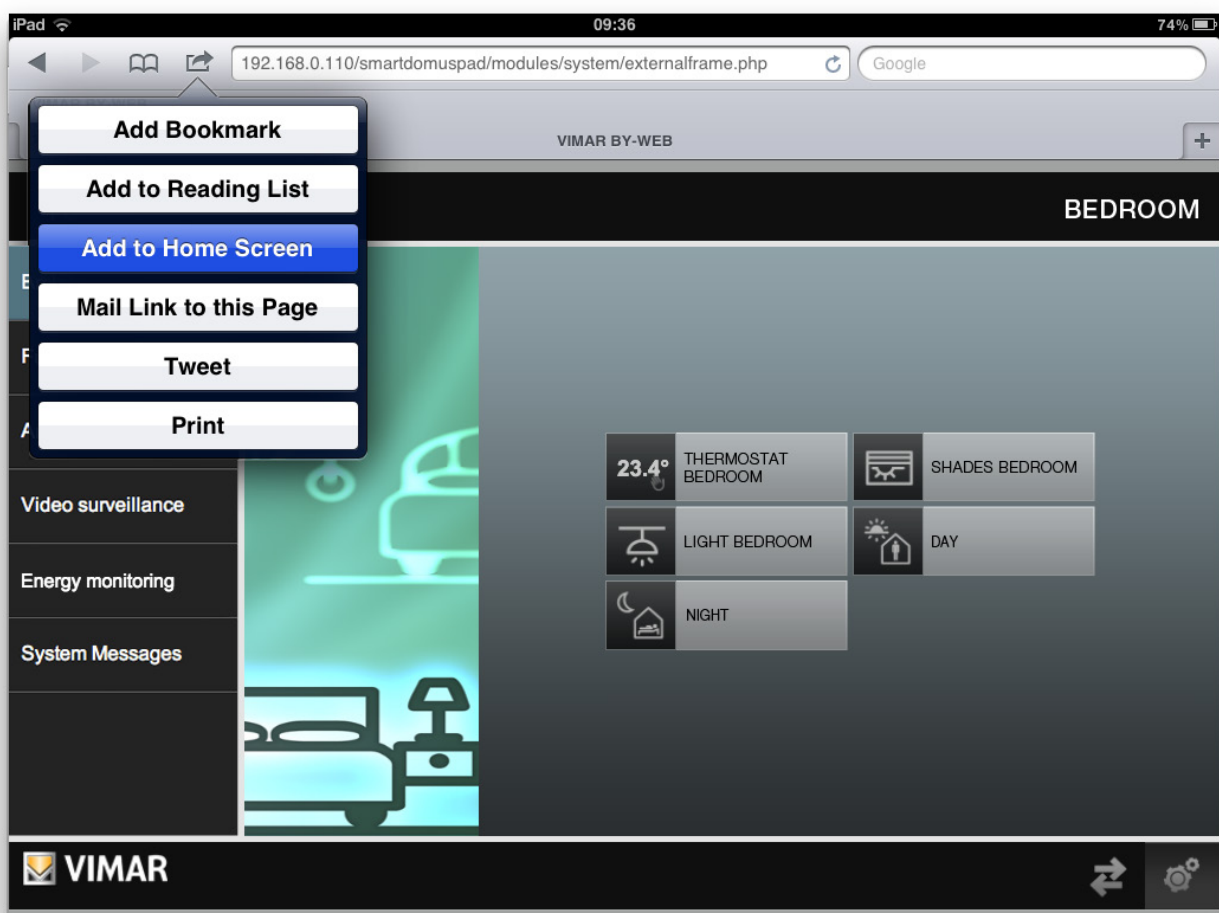
10.1 Add To Home

The ADD TO HOME feature creates a direct link to the Web Server web page.

It creates an icon on the HOME page, which displays the Web Server page in a browser window.

To create the icon with the link, follow these steps:

1. Open the Safari browser.
2. Type the IP address of the Web Server (e.g. for access over the LAN, the default address is <http://192.168.0.110>).
3. Press the options button on top  left and select "Add to Home" from the drop-down menu.



Following these simple steps you will see a popup where you can change the application name to be displayed; then you must press the Enter button on the virtual keyboard.

The created application is displayed on the Home screen of the mobile device, pressing the icon  starts the communication with the Web Server.

ByWeb Tools by Vimar

11. ByWeb Tools by Vimar

11.1 Introduction

ByWeb Tools Vimar is a software package that provides the following features:

- Reduction in the duration of the XML system file import process, by using a specific import procedure that involves running a dedicated Vimar application on the operating computer.
- Display of the RTSP video streams from the IP Video Surveillance cameras configured on the Web server.

ByWeb Tools must be installed on all computers from which the web server is accessed and where one or both of the features described are going to be used.

ByWeb Tools is available for the following operating systems: Microsoft Windows.

The installation package By-web Tools by Vimar can be downloaded directly from the web server and, therefore, an internet connection is not required.

11.2 Requirements

Before proceeding with the installation of ByWeb Tools by Vimar, make sure the following software packages have been previously installed:

- JAVA by Oracle (Version 8): necessary for the import of the By-me project. To display RTSP video streams only, there is no need to install JAVA.
- VLC by VideoLAN: necessary for viewing the RTSP video streams. For importing the system project only, there is no need to install VLC.

If ByWeb Tools is installed without installing the above software, if the above software is installed later, ByWeb Tools must be reinstalled.

IMPORTANT: Administrator privileges are required on the computer where ByWeb Tools will be installed.

For proper functioning of ByWeb Tools the Web Server must include the correct SSL certificates. If not already done so, save the Web Server network parameters again, making sure that it is connected to the Internet (General Settings/Setup/Network).

11.3 Installation

The installation of ByWeb Tools can be started in the following ways:

- Automatic installation request (via warning message), if not yet carried out, at the start of the XML system file import (even in the case of web server software upgrade, if the XML system file saved on the web server during the last import of the XML system file needs to be re-imported).
- Automatic installation request (via warning message), if not yet carried out, at the viewing request of the IP video surveillance camera that provides an RTSP video stream (e.g. IP cameras by Elvox).

Integration of KNX devices in the By-me system

12. Integration of KNX devices in the By-me system

12.1 Introduction

The By-me system has much in common with the KNX structure and, thanks to this feature, you can make the two systems interact without using physical interfaces.

This enables making certain features of KNX devices available in the By-me system (for devices and advanced user interfaces such as touchscreens and Web Servers).

Although from a physical/electrical point of view By-me and KNX devices can be connected to the same cable bus, the two systems have their own addressing formats and different tools and methods for configuration.

In terms of addressing you can still make a conversion between the different formats and the EasyTool Professional software lets you make such conversions.

From the point of view of the configuration, for the KNX system you need to use the ETS software of KNX, while the By-me system is configurable via EasyTool Professional.

The ability to make the required configuration for the integration of KNX devices in the By-me system has been available since version 2.10 of EasyTool Professional.

The integration of the two systems is based on sharing data, with a specific format, using the group addresses; the shared data refer to certain features of the physical devices (e.g. temperature measured by a thermostat, ON/OFF control of a relay, etc.).

The Web Server enables managing two broad categories of objects (or functions) of integration:

- Single (or generic) functions.
- Compound functions:
 - Relay
 - Dimmer
 - Roller shutter
 - Roller shutter with slats

12.2 Single functions

The single function of the KNX device, identified through its KNXcommunication object, is "shown" in the By-me system as a single function.

The types of KNX communication objects managed by the Web Server are listed below (refer to the KNX documentation for a description of the datapoint types (DPT) of the KNX system).

ID, DPT	
1.001 DPT_Switch	
1.002 DPT_Bool	
1.003 DPT_Enable	
1.004 DPT_Ramp	
1.005 DPT_Alarm	
1.006 DPT_BinaryValue	
1.007 DPT_Step	
1.008 DPT_UpDown	
1.009 DPT_OpenClose	
1.010 DPT_Start	
1.011 DPT_State	
1.012 DPT_Invert	
1.013 DPT_DimSendStyle	
1.014 DPT_InputSource	
1.015 DPT_Reset	
1.100 DPT_HeatCool	
5.001 DPT_Scaling	
5.010 DPT_Value_1_Ucount	
6.010 DPT_Value_1_Count	
7.001 DPT_Value_2_Ucount	
7.006 DPT_TimePeriodMin	
8.001 DPT_Value_2_Count	
9.001 DPT_Value_Temp [°C]	
9.002 DPT_Value_Tempd [K]	
	9.003 DPT_Value_Tempa [K/h]
	9.004 DPT_Value_Lux [Lux]
	9.005 DPT_Value_Wsp [m/s]
	9.007 DPT_Value_Humidity [%]
	9.008 DPT_Value_AirQuality [ppm]
	9.006 DPT_Value_Pres [Pa]
	9.010 DPT_Value_Time1 [s]
	9.011 DPT_Value_Time2 [ms]
	9.020 DPT_Value_Volt [mV]
	9.021 DPT_Value_Curr [mA]
	12.001 DPT_Value_4_Ucount
	13.001 DPT_Value_4_Count
	9.024 DPT_Power [kW]
	14.056 DPT_Value_Power [W]
	20.102 DPT_HVACMode
	20.107 DPT_ChangeoverMode

Integration of KNX devices in the By-me system

In the Web Server windows, each communication object is represented by graphical objects that, regardless of the data type, are characterized by a different way of interacting with the user depending on the set communication flag.

The method of integration involves managing the following three communication flags:

- **Read.** The graphical object that represents a group address with this communication flag provides for displaying a state or a numerical value that is sent by the device and received by the Web Server. Some data types provide for displaying the status in the icon of the graphical object.
- **Write.** The graphical object that represents a group address with this communication flag provides for sending a command or a numerical value from the Web Server to the device.

Note: The push buttons for sending commands (such as ON/OFF) do not display the status; when pressed, they are highlighted, for a few seconds, to give feedback.

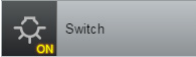
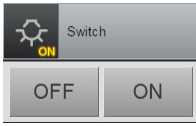
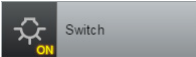
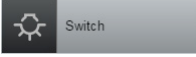


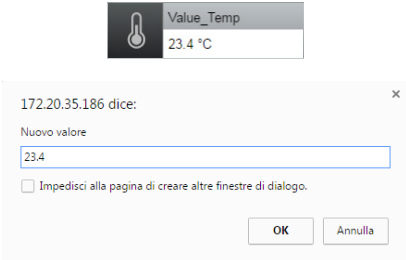


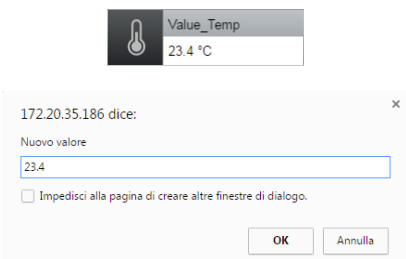
For entering numerical data, on pressing the white area of the widget you'll see a pop-up window for entering the data via the numeric keypad.

- **Transmit.** The graphical object that represents a group address with this communication flag provides for displaying a state or a numerical value that is sent by the device and received by the Web Server.

Each integration group address must have at least one of the three communication flags set (even all of them can be set).

The graphical objects that represent the integration group addresses differ depending on the type of data they represent.

The following table shows some examples of what has just been described.

DPT	Closed graphical object	Open graphical object	Communication flag		
			R	W	T
1.001 DPT_Switch			✓	✓	✓
1.001 DPT_Switch		NO command	✓		✓
1.001 DPT_Switch	 NO status on icon			✓	
9.001 DPT_Value_Temp [°C]			✓	✓	✓
9.001 DPT_Value_Temp [°C]		NO command	✓		✓
9.001 DPT_Value_Temp [°C]	 NO value reading			✓	

IMPORTANT: The Web Server checks the numerical data entered via the keyboard: if the entered value is "out of range" or if the syntax is not respected (such as entering characters that are not allowed), the data is ignored.

Integration of KNX devices in the By-me system

12.3 Compound functions

The Web Server makes provision for specific graphical objects for some simple and commonly used physical devices, for ease of use: the single functions (associated with the relevant KNX communication object) are grouped into a single graphical object that represents the physical device.

The compound functions managed by the Web Server are:

- Relay
- Dimmer
- Roller shutter with percentage setpoint
- Roller shutter with slats with percentage setpoint

Relay

The "relay" compound object groups the following single functions:

- ON/OFF command
- ON/OFF status

The graphical object representing this compound object is the one used for the By-me actuators and has the same operation.

Dimmer

The "dimmer" compound object groups the following single functions:

- ON/OFF command
- ON/OFF status
- Setting brightness value (percentage value)
- Brightness value status (percentage value)

The graphical object representing this compound object is the one used for the By-me dimmers and has the same operation.

Roller shutter with percentage setpoint

The "Roller Shutter" compound object groups the following single functions:

- Up/Down movement
- Stop
- Setting roller shutter position (percentage value)
- Roller shutter position status (percentage value)

The graphical object representing this compound object is the one used for the By-me roller shutter actuators and has the same operation.

Roller shutter with slats with percentage setpoint

The "Roller Shutter with slats" compound object groups the following single functions:

- Up/Down movement
- Stop
- Setting roller shutter position (percentage value)
- Roller shutter position status (percentage value)
- Setting slat position (percentage value)
- Setting, in increments in both directions, the position of the slats.
- Slat position status (percentage value)

The graphical object representing this compound object is the one used for the By-me roller shutter with slats actuators and has the same operation.

12.4 Configuration

The integration of the two systems is based on sharing data, with a specific format, using the group addresses.

To make the configuration you need to use the EasyTool Professional software and the ETS software of KNX; for all the details on usage please refer to the respective documentation.

After completing the configuration of all the integration groups (using the EasyTool Professional software), export the XML file for the Web Server and proceed to import the XML file on the Web Server.

All the integration groups are included in the "Lighting" function of the "Functions" menu of the Web Server and can be added to the rooms you want.

Integration of KNX devices in the By-me system

12.5 Integration of the gateway ME-AC-KNX-1-V2 of Intesis for the management of Mitsubishi air-conditioners

12.5.1 Premessa

The Web Server 01945-01946 is able to manage the main features of Mitsubishi air conditioners compatible with the Intesis gateway ME-AC-KNX-1-V2 .

Note: For information regarding the gateway of Intesis refer to the documentation of Intesis.

In order for the Web Server 01945-01946 by Vimar to manage a Mitsubishi indoor air-conditioning unit:

- Each Mitsubishi internal unit to be managed must be connected to a Intesis gateway ME-AC-KNX-1-V2 and must be compatible with it. Each gateway must be appropriately configured using the software ETS of KNX.
- Through the EasyTool Professional software of Vimar it is necessary to create a KNX integration object for each Mitsubishi internal unit and it must be appropriately configured.
- After completing the configuration through EasyTool Professional, it is necessary to export the XML configuration file that must be subsequently imported into the Web Server.

As already described in chapter 13.4 Configuration, also the management of the gateway Intesis (which is a KNX device) by the web server 01945-01946, is based on data sharing between the KNX system and the By-me system of Vimar through the group addresses.

The features of the Mitsubishi air conditioners that the Web Server 01945-01946 can manage are the following:

- Status and ON/OFF control displaying.
- Room temperature displaying.
- Temperature setpoint displaying and setting.
- Operating mode and status setting displaying.
- Fancoil speed status displaying and setting.
- Slats position status displaying and setting.
- Displays the Mitsubishi indoor unit error status.
- Displays the Mitsubishi indoor unit error code (in the event of an error).

IMPORTANT: The availability of some features and the relative setting range depends on the internal conditioning unit model and on how the configuration procedure was carried out, as described in the following chapters.

12.5.2 The configuration procedure

The management of the Intesis gateway ME-AC-KNX-1-V2 by the web server by 01945-01946, is based on data sharing of between the KNX system and the Vimar By-me system through the group addresses.

For each Mitsubishi internal unit to be managed, the following operations must be performed:

1. Through the ETS software of KNX configure the gateway of Intesis connected to the Mitsubishi internal unit, assigning group addresses that have not already been used by the By-me system.
2. Through the EasyTool Professional software of Vimar, create a Mitsubishi KNX integration object and configure it assigning the group addresses previously created through the ETS software of KNX to the corresponding communication objects for integration of the two systems.

IMPORTANT: The web server is able to manage ONLY the communication objects to which a correct group address has been assigned. Communication objects to which no group address is associated are not exported to the file to be imported from the web server.

After completing the configuration of all the integration groups (using the EasyTool Professional software of Vimar), export the XML file for the Web Server and proceed to import the XML file on the Web Server.

The above mentioned configuration phases are described in detail in the following chapters.

The versions of the ETS application programme of the Intesis ME-AC-KNX-1-V2 gateway

The currently available version of the application programme of the Intesis ME-AC-KNX-1-V2 gateway is 1.0. The previous version was 0.8.

The two versions 0.8 and 1.0 are different, in terms of the datapoints and ETS configuration parameters, and this means a different management by the web server and EasyTool Professional for the configuration phase.

- The management of version 0.8 of the ETS software of the Intesis ME-AC-KNX-1-V2 gateway was introduced in version 2.11 of EasyTool Professional and in version 2.2 of the web server 01945/01946 software.
In any case use the most recent available versions of EasyTool Professional and the web server software.

- The management of version 1.0 of the ETS software of the Intesis ME-AC-KNX-1-V2 gateway was introduced in version 2.14 of EasyTool Professional and in version 2.9 of the web server 01945/01946 software.

The configuration procedures to manage the Intesis gateway with the two different versions of the ETS application programme will be described below in specific chapters, due to the differences between the two versions. Using an incorrect configuration procedure, in relation to the Intesis gateway ETS application programme, will cause the integration to malfunction.

Integration of KNX devices in the By-me system

12.5.3 The KNX configuration of the Intesis gateway (with version 0.8 of the ETS application programme)

12.5.3.1 Setting the gateway ME-AC-KNX-1-V2 (with version 0.8 of the ETS application programme) parameters in the KNX project

After adding the ME-AC-KNX-1-V2 device to the KNX project it is necessary to configure the following parameters of the device:

- **General->AC unit type:** Select from the drop-down menu the correct model of Mitsubishi air conditioner connected to the specific gateway.
This is an important setting because the features and their permissible values depend on the specific model of internal unit.
- **General->Virtual temperature control:** Set to NO.
- **General->Mode object type [1 byte]:** Select the "Both (20.105 and enumerated)" option from the drop-down menu. In this way the following datapoint are made available:
 - CO 1-Mode (enumerative), in reading and transmission. This datapoint is used by the Web Server to update the operating mode status of the internal unit.
 - CO 49-HVAC Mode (dpt 20.105), in reading, transmission, and writing. This datapoint is used by the web server for setting the operating mode of the internal unit.
- **Objects Display->Show Increase/Decrease Bits:** Set to Yes. This parameter enables the datapoint for setting by increasing/decreasing the fancoil speed, of the slats position and temperature setpoint . Having set this parameter to Yes, for each of the above presented datapoints, the datapoint type to use must be set, as described below: select DPT_Step 1.007 (0=Dec/1=Inc) for the communication objects "Fan Speed [+/-]" and "Setpoint Temperature [+/-]", while for the communication object "Vane [+/-]" select DPT_Step 1.008 (0=Up/1=Down).

12.5.3.2 Setting the gateway ME-AC-KNX-1-V2 (with version 0.8 of the ETS application programme) parameters in the KNX project

After having carried out the configuration of the parameters, enabling the necessary datapoint, proceed with the assignment of the group addresses of the following datapoint. It should be remembered that the group addresses to be used must be addresses that have not already been used in the By-me system. Perform a preliminary check, using the EasyTool Professional software, of the addresses already used by the By-me system (it should be remembered that the EasyTool Professional software allows to view the addresses in the 2-level KNX, 3-level KNX and By-me formats).

The following table also shows the datapoint that are necessary for management by the Web Server and those that can be ignored, in case it is desired that the related feature is not managed by the Web Server.

CO	Communication object name	Notes
0	On/Off [1 bit]	NECESSARY It allows to send the ON/OFF command to the internal unit and to receive information on its activation status.
1	Mode [1 byte]	NECESSARY It allows the web server to read and receive the operating mode status.
3	Fan [1 byte]	NECESSARY¹ It allows the web server to read and receive the fancoil speed status. In the absence of this communication object, the web server will not be able to manage the fancoil speed.
5	Vane [1 byte]	NECESSARY¹ It allows the web server to read and receive the slat position status. In the absence of this communication object, the web server will not be able to manage the slats position.
7	Set Temperature [2 byte]	NECESSARY¹ It allows the web server to read and receive the status of the temperature setpoint . In the absence of this communication object, the web server will not be able to manage the temperature setpoint .
8	Ambient temperature [2 byte]	It allows the Web Server to read and receive the room temperature status.
9	Error [1 bit]	NECESSARY It allows the Web Server to display and manage communication errors between gateway Intesis and the internal unit or internal unit malfunctions.
10	Error Code [2 byte]	NECESSARY It allows the web server to display the Error code sent by the internal unit. Note: For the meaning of the numerical error code, refer to the technical documentation of Intesis.
24	Fan Speed [+/-] [1 bit]	It allows the web server to set the fancoil speed.
30	Vane [+/-] [1 bit]	It allows the web server to set the slats position.
38	Set temperature [+/-] [1 bit]	It allows the web server to set the temperature setpoint .
49	HVAC Mode [1 byte]	It allows the web server to set the operation mode.

¹ If the internal unit model provides this functionality.

After completing the operations described, download the settings made in the gateway Intesis.

Integration of KNX devices in the By-me system

12.5.4 Creation and configuration of KNX integration objects for the gateway Intesis (with version 0.8 of the ETS application programme) through EasyTool Professional

To manage Mitsubishi air conditioners (via the Intesis gateway ME-AC-KNX-1-V2 with version 0.8 of the application programme) use version 2.14.1 (or higher) of EasyTool Professional.

In order to allow the Intesis gateway KNX to be managed by the Web Server 01945-01946 in the By-me system, the corresponding KNX integration objects must be created and configured in Easy Tool Professional, following the procedure described below.

In the EasyTool Professional project to be exported for the Web Server, for each gateway Intesis it is necessary:

1. Create a New KNX Group: Configure->Integrate third party KNX->New KNX Group
Assign a description to the KNX group, select, as Functionality, "Mitsubishi 0.8" or "Mitsubishi No Fan Mode 0.8" according to the operating modes available on the Mitsubishi internal unit that you want to manage.
Specifically:
 - a. Select "Mitsubishi 0.8" if the internal unit to be managed includes all the operating modes: HEAT, DRY, COOL, FAN, AUTO.
 - b. Select "Mitsubishi No Fan Mode 0.8" if the internal unit to be managed does not provide the FANmode, i.e. it is able to manage the following operating modes: HEAT, DRY, COOL, AUTO.
2. Complete KNX group creation by pressing the Save button. The new KNX group appears in the Explorer Tree Window of EasyTool Professional under the KNX node.
It is possible to proceed with the creation of other KNX groups or press the "Close" button of the "New KNX Group" window to proceed with the configuration of the KNX group created.
3. Select the KNX group created to proceed with the configuration. The group tab appears in the main work area with the list of Object Functions to which the related group address must be assigned.
It should be remembered that it is possible to change the format of the group address from the Tools-> KNX address Format menu.
4. Assign group addresses to the object functions, using the group addresses previously assigned through ETS to the corresponding communication objects of the gateway Intesis which is intended to associate with the KNX group that is being configured.
Dovranno essere assegnati ALMENO tutti gli indirizzi NECESSARI descritti nel capitolo 13.5.3.2 Assegnazione degli indirizzi di gruppo ai datapoint del gateway ME-AC-KNX-1-V2 nel progetto KNX.
AT LEAST all the NECESSARY addresses described in chapter 13.5.3.2 Assigning group addresses to the datapoint of the gateway ME-AC-KNX-1-V2 in the KNX project must be assigned.
It is advisable to assign group addresses to all the features that can be managed by the web server.
The object functions to which a group address is not associated will not be managed by the web server.
Here following there is the table with the correspondences between the ETScommunication objects and the EasyTool Professional Functions object:

ETS		EasyTool Professional
CO	Communication object name	Object function
0	On/OFF [1 bit]	Set On/OFF – DPT_Switch (1.001)
1	Mode [1 byte]	Get Mode
3	Fan [1 byte]	Get fan speed
5	Vane [1 byte]	Get vane
7	Set Temperature [2 byte]	Setpoint temperature – DPT_Value_Temp (9.001)
8	Ambient temperature [2 byte]	Get ambient temperature – DPT_Value_Temp (9.001)
9	Error [1 bit]	Get error state – DPT_Switch (1.001)
10	Error Code [2 byte]	Get error code – DPT_Value2_Ucount (7.001)
24	Fan Speed [+/-] [1 bit]	Set fan speed – DPT_Step (1.007)
30	Vane [+/-] [1 bit]	Set vane – DPT_Step (1.008)
38	Set temperature [+/-] [1 bit]	Setpoint increase/decrease – DPT_Step (1.007)
49	HVAC Mode [1 byte]	Set HVAC Mode

NOTE: the correct flag RWT settings are already preset for each object function.

5. After completing the creation of the KNX groups associated with all the gateway Intesis to be managed, and having appropriately configured them, export the project to the web server.
6. The project file exported from EasyTool Professional must subsequently be imported into the web server 01945-01946.

Integration of KNX devices in the By-me system

12.5.5 The KNX configuration of the Intesis gateway (with version 1.0 of the ETS application programme)

12.5.5.1 Setting the parameters of the gateway ME-AC-KNX-1-V2 (with version 1.0 of the ETS application programme) in the KNX project

Having added the ME-AC-KNX-1-V2 device in the KNX project, the following parameters must be configured in the device (only the parameters concerning the integration in question are shown):

- **General->Enable object "Error Code (2 byte):** Select this parameter to display the communication object Status_Error Code. For the description of the error codes, refer to the table in the Intesis documentation.
- **Mode Configuration-> Indoor unit has FAN mode:** set to Yes if the Mitsubishi indoor unit has the operating mode FAN (ventilation). Otherwise set to No.
- **Fan Speed Configuration->Fan is accessible in indoor unit (see docum. For your indoor unit):** set to Yes if the Mitsubishi device has the indoor unit fan speed setting. Otherwise set to No. Having set this parameter to Yes a list of settings appears for managing the fan speed.
- **Fan Speed Configuration->Available fan speeds in Indoor Unit (see docum. For your indoor unit):** set the number of fancoil speeds of the Mitsubishi indoor unit.
- **Fan Speed Configuration->Indoor unit has AUTO fan speed (see docum. for your indoor unit):** set to Yes if the Mitsubishi indoor unit has an automatic fan speed settings mode. Otherwise set to No.
- **Fan Speed Configuration->Enable use of +/- object for Fan Speed:** set to Yes. Set to Yes, the choice of type of datapoint to use is displayed: DPT type for +/- Fan Speed object: select 0-Decrease/1-Increase [DPT_1.007].
- **Fan Speed Configuration->Enable "Fan Speed Man/Auto" objects (for Control and Status):** set to Yes if the Mitsubishi indoor unit has an automatic fan speed settings mode. Otherwise set to No.
- **Vanes Up-Down Configuration->Indoor unit has U-D Vanes (see docum. for your indoor unit):** set to Yes if the Mitsubishi indoor unit has vane position management. Otherwise set to No. Set to Yes, a list of vane position management settings is displayed.
- **Vanes Up-Down Configuration->Available positions in Indoor Unit (see docum. for your indoor unit):** select the number of vane positions.
- **Vanes Up-Down Configuration->Indoor unit has AUTO Vanes U-D:** set to Yes if the Mitsubishi indoor unit has an automatic vane position setting (AUTO): in this case, a new parameter appears for enabling the Automatic or Manual vane position settings.
- **Vanes Up-Down Configuration->Enable "Vanes U-D Man/Auto" objects (for Control and Status):** this parameter appears if the previous one was set to Yes and is used to enable the communication objects (making them visible in the communication objects list) for the automatic or manual vane position settings or status.
- **Vanes Up-Down Configuration->Enable "Vanes U-D Swing" objects (for control and status):** set to Yes, the communication objects are enabled for the settings and status of the vane position swing mode.
- **Vanes Up-Down Configuration->Enable use of +/- object for Vanes U-D:** set to Yes. Set to Yes, the choice of type of datapoint to use is displayed: Vanes Up-Down Configuration->DPT type for +/- Vanes U-D object: select 0-UP/1-Down (DPT_1.008).
- **Temperature Configuration->Enable use of +/- obj for Setpoint Temp:** Set to Yes. Having set the parameter to Yes a further parameter is displayed for choosing the type of datapoint to use.
- **Temperature Configuration->DPT type for +/- Sept Temp object:** Select 0-Decrease/1-Increase (DPT_1.007).

Integration of KNX devices in the By-me system

12.5.5.2 Assigning group addresses to the ME-AC-KNX-1-V2 gateway datapoints (with version 1.0 of the ETS application programme) in the KNX project

After configuring the parameters, enabling the necessary datapoints, proceed with the assignment of the group addresses of the following datapoints. It should be remembered that the group addresses to be used must be addresses that have not already been used in the By-me system. Run an initial check using the EasyTool Professional software, of the addresses already used by the By-me system (remember that the EasyTool Professional software can be used to display the addresses in formats KNX 2 levels, KNX 3 levels and By-me).

The following table also shows the datapoints necessary for the complete management by the Web Server.

Some Mitsubishi indoor unit models may not have all the functions that can be managed by the Web Server.

It is also possible to exclude some functions from the Web Server management of the Mitsubishi indoor unit (in this case it is not necessary to associate a group address to the datapoint in the ETS configuration and in the related configuration page of the EPro KNX integration object).

CO	Communication object name	Notes
0	Control_On/Off [DPT_1.001]	Used to send the On/Off command to the indoor unit.
1	Control_Mode [DPT_20.105]	Used to set the operating modes: Auto, Heat, Cool, Fan (where available in the indoor unit model), Dry.
11	Control_Fan Speed Man/Auto [DPT_1.002]	Used to enable the automatic or manual fan speed setting mode.
16	Control_Fan Speed +/- [DPT_1.007]	Used to set the fan speed in manual mode.
19	Control_Vanes U-D Man/Auto [DPT_1.002]	Used to enable the automatic or manual vane position setting mode.
25	Control_Vanes U-D Swing [DPT_1.002]	Used to enable the Swing vane position settings mode.
26	Control_Vanes U-D +/- [DPT_1.008]	Used to set the vane position.
28	Control_Setpoint Temperature +/- [DPT_1.007]	Used to set the temperature setpoint.
46	Status_On/Off [DPT_1.001]	Used to read and receive the indoor unit On/Off status.
47	Status_Mode [DPT_20.105]	Allows the Web Server to read and receive the operating mode status: Auto, Heat, Cool, Fan (where available in the indoor unit model), Dry.
55	Status_Fan Speed [DPT_5.010]	Allows the Web Server to read and receive the fan speed status, in manual mode.
57	Status_Fan Speed Man/Auto [DPT_1.002]	Allows the Web Server to read or receive the fan speed automatic or manual settings mode enabling status
63	Status_Vanes U-D [DPT_5.010]	Allows the Web Server to read and receive the vane position status, in manual mode.
65	Status_Vanes U-D Man/Auto [DPT_1.002]	Allows the Web Server to read or receive the vane position speed automatic or manual settings mode enabling status.
71	Status_Vanes U-D Swing [DPT_1.002]	Allows the Web Server to read or receive the vane position Swing settings mode enabling status.
73	Status_AC Setpoint Temperature [DPT_9.001]	Allows the Web Server to read and receive the current temperature setpoint value.
74	Status_AC Return Temperature [DPT_9.001]	Allows the Web Server to read and receive the current room temperature value measured by the indoor unit.
75	Status_error/Alarm [DPT_1.005]	Allows the Web Server to display and manage communication errors between the Intesis gateway and the indoor unit or indoor unit malfunctions.
76	Status_Error Code [8.001]	Allows the Web Server to display the Error code sent by the indoor unit. Note: For the meaning of the numerical error code, refer to the technical documentation of Intesis.

After completing the operations described, download the settings made in the gateway Intesis.

Integration of KNX devices in the By-me system

12.5.6 Creation and configuration of KNX integration objects for the gateway Intesis (with version 1.0 of the ETS application programme) through EasyTool Professional

To manage Mitsubishi air conditioners (via the Intesis gateway ME-AC-KNX-1-V2 with version 1.0 of the ETS application programme) via EasyTool Professional.

In order to allow the Intesis gateway KNX to be managed by the Web Server 01945-01946 in the By-me system, the corresponding KNX integration objects must be created and configured in Easy Tool Professional, following the procedure described below.

In the EasyTool Professional project to be exported for the Web Server, for each gateway Intesis it is necessary:

1. Create a New KNX Group: Configure->Integrate third party KNX->New KNX Group
Assign a description to the KNX group, select, as Functionality, "Mitsubishi 1.0" or "Mitsubishi No Fan Mode 1.0" according to the operating modes available on the Mitsubishi internal unit that you want to manage.

Specifically:

- a. Select "Mitsubishi 1.0" if the internal unit to be managed includes all the operating modes: HEAT, DRY, COOL, FAN, AUTO.
 - b. Select "Mitsubishi No Fan Mode 1.0" if the internal unit to be managed does not provide the FANmode, i.e. it is able to manage the following operating modes: HEAT, DRY, COOL, AUTO.
2. Complete the KNX group creation by pressing the Save button. In the ExplorerTree Window in EasyTool Professional the new KNX group appears under the KNX node.
It is possible to proceed with the creation of other KNX groups or press the "Close" button of the "New KNX Group" window to proceed with the configuration of the group created.
 3. Select the KNX group created to proceed with the configuration. The group tab appears in the main work area with the list of Object Functions to which the related group address must be assigned.
Remember that it is possible to change the format of the group address in the menu Tools->KNX address format.
 4. Assign group addresses to the object functions, using the group addresses previously assigned through ETS to the corresponding communication objects of the Intesis gateway which is to be associated with the KNX group being configured.

It is advisable to assign group addresses to all the features that can be managed by the Web Server.

The object functions to which a group address is not associated will not be managed by the Web Server.

The following table shows the correspondences between the ETS communication objects and the EasyTool Professional Functions:

ETS		EasyTool Professional
CO	Communication object name	Object function
0	Control_On/Off [DPT_1.001]	Set On/Off - DPT_Switch (1.001)
1	Control_Mode [DPT_20.105]	Set HVAC mode - DPT_HVACContrMode (20.105)
11	Control_Fan Speed Man/Auto [DPT_1.002]	Set fan speed Man/Auto - DPT_Bool (1.002)
16	Control_Fan Speed +/- [DPT_1.007]	Set fan speed - DPT_Step (1.007)
19	Control_Vanes U-D Man/Auto [DPT_1.002]	Set vane Man/Auto - DPT_Bool (1.002)
25	Control_Vanes U-D Swing [DPT_1.002]	Set vane Swing - DPT_Bool (1.002)
26	Control_Vanes U-D +/- [DPT_1.008]	Set vane - DPT_UpDown (1.008)
28	Control_Setpoint Temperature +/- [DPT_1.007]	Setpoint increase/decrease - DPT_Step (1.007)
46	Status_On/Off [DPT_1.001]	Get On/Off - DPT_Switch (1.001)
47	Status_Mode [DPT_20.105]	Get HVAC mode - DPT_HVACContrMode (20.105)
55	Status_Fan Speed [DPT_5.010]	Get fan speed - DPT_Value_1_Ucount (5.010)
57	Status_Fan Speed Man/Auto [DPT_1.002]	Get fan speed Man/Auto - DPT_Bool (1.002)
63	Status_Vanes U-D [DPT_5.010]	Get vane - DPT_Value_1_Ucount (5.010)
65	Status_Vanes U-D Man/Auto [DPT_1.002]	Get vane Man/Auto - DPT_Bool (1.002)
71	Status_Vanes U-D Swing [DPT_1.002]	Get vane Swing - DPT_Bool (1.002)
73	Status_AC Setpoint Temperature [DPT_9.001]	Setpoint temperature - DPT_Value_Temp (9.001)
74	Status_AC Return Temperature [DPT_9.001]	Get ambient temperature - DPT_Value_Temp (9.001)
75	Status_error/Alarm [DPT_1.005]	Get error state - DPT_Alarm (1.005)
76	Status_Error Code [8.001]	Get error code - DPT_Value_2_Count (8.001)

NOTE: the correct flag RWT settings are already preset for each object function.

5. After completing the creation of the KNX groups associated with all the gateway Intesis to be managed, and having appropriately configured them, export the project to the web server.
6. The project file exported from EasyTool Professional must subsequently be imported into the web server 01945-01946.

The upgrades of the HTTPS protected connection in versions 2.5 and 2.6

13 The significant upgrades introduced in versions 2.5 and 2.6 of the web server software for the management of the HTTPS protected connection

13.1 Premessa

In versions 2.5 and 2.6 of the web server software 01945/01946, significant improvements/upgrades have been introduced in the management of the HTTPS protected communication between the web server and the clients used to access the web server (web browser, By-web App for mobile devices), to accommodate the latest provisions on the subject.

The changes concern:

1. Upgrade of the web server TLS certificate and of the CA certificate by Vimar.
2. Upgrade of the TLS protocol to version 1.2.

As from the upgrade to version 2.5 of the web server software, all web servers will be able to perform the upgrade of the TLS certificate and of the CA certificate by Vimar.

The upgrade of the TLS protocol to version 1.2, on the other hand, occurs automatically with the upgrade to version 2.5 in the most recent web servers, whereas for less recent versions, a dedicated procedure needs to be launched, which is available after the upgrade to version 2.6 of the web server software 01945/01946, as described in detail below.

So, if possible, we recommend you upgrade the web server directly to version 2.6.

The expiry of the web server CA certificate, the failure to upgrade the TLS certificate or the use of a TLS protocol version prior to 1.2 lead to the failed recognition of a "secure connection" by clients used to access the web server (browser for PC and By-web App for mobile devices). The encrypted connection between the web server and the client is always guaranteed in all cases, but some warning messages may appear, informing you that the connection is not entirely secure.

It is therefore necessary to upgrade the web servers to version 2.6 as soon as possible (for more recent web servers, the upgrade to version 2.5 is sufficient) and follow the instructions displayed by the web server, and which will be described in the manual, to upgrade the components of the HTTPS protected connection.

Please remember that to check the status of the web server components necessary for the management of the HTTPS protected connection, you can access the "Web developer tools" page in Google Chrome and select the "Security" tab.

NOTE: After the upgrades of the certificate or of the TLS protocol, you may need to restart Google Chrome for Google Chrome to upgrade the status of the security indicator for the HTTPS connection.

13.2 Version 2.5 of the web server software 01945/01946

Version 2.5 includes the following new functions concerning the HTTPS protected connection:

1. Management of the web server TLS certificate upgrade and downloading the new CA certificate.

This function is available for all the hardware revisions of the web server 01945/01946 by Vimar.

2. Upgrade of the TLS protocol to version 1.2, only for the most recent hardware revisions (03 and 04) of web server 01945/01946 by Vimar.
3. Introduction of an automatic mechanism for the routine checking of the CA certificate expiry and the possible availability of a new CA certificate.

13.2.1 Operations to be completed before upgrading to version 2.5

After upgrading to version 2.5, a warning message will be displayed, prompting you to download the new CA certificate from the web server and install it in the clients.

Before you do this, proceed with the upgrade of the TLS certificates of the web server, as described below:

1. Check the web server is connected to the Internet. If the web server is not connected to the Internet, you will be unable to upgrade the TLS certificate of the web server and download the new CA certificate into the web server.
2. Access the network settings page of the web server, following the path below: "General settings"->"Network". Press the push button to confirm the change to the network settings.
3. After you have pressed the push button to confirm the network settings, a window will appear with a message prompting you to confirm the change to the network settings. Confirm the change to the network settings.
4. A TLS certificate upgrade procedure launch message will appear if the web server is connected to the Internet. Confirm the message.
5. If the web server is connected to the Internet, it will proceed with the TLS certificate upgrade operations and download the most recent CA certificate, then restart the services (notified by a warning message) to make the changes effective. When the operation is complete, the home page of the web server will be displayed.
If the web server is not connected to the Internet, the new TLS certificates cannot be created and a TLS certificate upgrade error message will be displayed.
6. After you have upgraded the TLS certificate and downloaded the upgraded CA certificate into the web server, you need to download the CA certificate from the web server and install it in the clients used to access the web server.

13.2.2 Upgrade of the TLS protocol to version 1.2

As mentioned earlier, the upgrade of the TLS protocol to version 1.2 is performed automatically during the software upgrade to version 2.5 only for web servers 01945/01946 equipped with hardware revision 03 and 04. For previous hardware revisions, the TLS protocol upgrade to version 1.2 must be performed using a dedicated "firmware upgrade" procedure which is available in version 2.6 of the web server software.

The upgrades of the HTTPS protected connection in versions 2.5 and 2.6

13.2.3 The automatic check performed by the web server on the availability of a new CA certificate and on the expiry of the CA certificate on board the web server.

After the software upgrade of the web server to version 2.5 (or subsequent versions), the web server will perform the following checks every week:

- If the web server is connected to the Internet, it will perform a check for the availability from Vimar of a new CA certificate and if it finds one, it will download it into the web server together with the new TLS certificate.
- If the web server is not connected to the Internet, it will perform a check on the expiry date of the CA certificate that is "on board" and if the expiry date is soon, it will display a warning message.

13.3 Version 2.6 of the web server software 01945/01946

In version 2.6 of the web server software, further improvements and new functions have been introduced concerning the upgrade of the TLS certificates and the upgrade of the TLS protocol to version 1.2, with respect to previous version 2.5.

The main novelties are summarised below:

1. Addition of the "Firmware upgrade" function, with which upgrades to the web server operating system can be performed.
Specifically, with reference to the need to upgrade the components for the creation of the HTTPS protected connection, this new function makes it possible to upgrade the TLS protocol (to version 1.2) of the web servers with a hardware revision prior to 03.
The web server firmware upgrade procedure is described in the chapter entitled "Web server Firmware Upgrade" in the manual herein.
2. Introduction of certain automations to guide the TLS certificate and TLS protocol upgrade operations:
 - After the web server software has been upgraded to version 2.6, if the web server is equipped with a hardware revision prior to 03, a warning message is displayed, notifying the availability of a new firmware version (which specifically is required for the TLS protocol upgrade). To perform the firmware upgrade, follow the instructions displayed and provided in the dedicated chapter of the manual herein. Remember that the "Firmware Upgrade" procedure can only be performed if the web server is connected to the Internet.
Web Servers equipped with hardware revision 03 and 04 do not currently require a firmware upgrade, but it is nevertheless envisaged for possible future needs; in these web servers, therefore, no warning message will currently be displayed as to the availability of new firmware.
 - After the web server software has been upgraded to version 2.6, a warning message will be displayed as to the need to perform the upgrade of the certificates; once you confirm this message, the procedure will automatically be launched. Remember that the correct completion of this procedure can only occur if the web server is connected to the Internet.

Using the Google Gmail SMTP service

14. Using the Google Gmail SMTP service to send web server e-mail notifications

14.1 Introduction

In order to send e-mail notifications, the web server must be able to connect to an SMTP server that grants access via a *Username* and a *Password*. In order to use the Google Gmail SMTP service, a Google Gmail account must be available.

If you are using the Google Gmail SMTP service, due to changes made by Google in managing security of access to Gmail accounts, from 30th May 2022 users will no longer be able to log in to Gmail accounts using only their Username and Password (the possibility of using them, by enabling the feature “Enable less secure Apps”, will end on 30th May 2022).

The reference is as follows: <https://support.google.com/accounts/answer/6010255>

However, Google envisages a specific configuration procedure, to be carried out on the Google Gmail account which will remain valid also after 30th May 2022, which will allow the web server to connect to the Google Gmail SMTP service to send e-mail notifications.

This procedure, envisaged by Google, allows you to create specific passwords referred to as “passwords for Apps”, which enable the web server to access the SMTP service of the customer’s Google Gmail account. The following chapters describe the procedure for the creation of “passwords for Apps” from the administrator section of your Google Gmail account and the use of these Apps for the web server configuration.

IMPORTANT: remember that the e-mail notification service is dependent upon the use of a third-party SMTP service which Vimar cannot guarantee. Vimar therefore cannot guarantee the validity times of this solution in future.

14.2 Creating a “password for Apps” on Google Gmail

The creation of a “password for Apps” envisaged two steps:

1. The first step, which is necessary in order to move on to the next step, consists in enabling the “two-step verification” (also referred to as “two-factor authentication”) in your Google Gmail account (or in any case in the Google Gmail account you intend to use to send the web server e-mail notifications).
2. The second step, which depends on the successful completion of the first, consists in the genuine creation of the “password for Apps” which will be used by the web server.

14.2.1 Enabling the “two-step verification” to access the Google Gmail account

Using the two-step verification allows you to increase the degree of security of the Google Gmail account.

To enable the “two-step verification” to access the Google Gmail account, follow the steps set out below:

1. Access the Google account you wish to use to send e-mails from the web server.
2. In the navigation panel, select the “Security” item.
3. In the “Accessing Google” section, select “Two-step verification” ➔ Start.
4. Follow the steps shown on the screen.

Please refer to the official Google documentation: <https://support.google.com/accounts/answer/185839>

After you have activated the two-step verification, you will need to complete a second step to verify your identity at the time of access. To protect your account more, Google will ask you to complete a specific second step.

14.2.2 Creating the “password for Apps” for the web server

Once you have enabled the “two-step verification” for the Google account you intend to use to send e-mails via web server, you will need to create a “password for Apps” for the web server.

N.B.: if the user has more than one web server (or other devices/Apps) requiring access to a Gmail account, we recommend you create a “password for Apps” dedicated to each device. This will, for instance, allow you to inhibit access to the account by a device independently from other devices, by removing the specific “password for Apps” from the Google account.

To create a “Password for Apps” for the web server proceed as follows:

1. Access the Google account you wish to use to send e-mails from the web server.
2. In the navigation panel, select the “Security” item.
3. In the “Accessing Google” section, select the “Password for Apps” item (this item will only be available if the “Two-step verification” item is enabled (ON)).
4. The list of passwords for Apps created previously is shown (initially the list is empty).
5. In the “Select App” field, select the “Mail” item.
6. In the “Select device” field, select the “Other (customised name)” item.
7. In the “device name” field, enter a name of your choice that identifies the specific web server for which you are creating the “password for Apps”.
8. Press the “Generate” button: a pop-up message appears. Under the “Your password for the App for the device” item is a field with the password created (16 characters). This is the password that will allow the web server to access the Google Gmail account to send e-mail notifications.
9. Copy the password so you can paste it into the dedicated field in the web server configuration window (please refer to chapter 14.3 below: Web server configuration).

To create the “Password for Apps” for Google, please refer to the official Google documentation:

<https://support.google.com/accounts/answer/185833>

Using the Google Gmail SMTP service

14.3 Web server configuration

Once you have created a “password for Apps” for the Google Gmail account you wish to use to send e-mail notifications from the web server, you need to fill in the dedicated web server configuration page.

In fact, the novelty compared to the past lies in the fact that the password the web server needs to use to access the Google Gmail SMTP service will no longer be the same password as the user’s Gmail account password, but will instead be the “password for Apps” which was created for the web server from the user’s Gmail account.

N.B.: if the user has more than one web server (or other devices/Apps) requiring access to a Gmail account, we recommend you create a “password for Apps” dedicated to each device.

Below is a table with the details that need to be entered in the web-server e-mail sending configuration page for the correct e-mail notification from a Google Gmail account.

Field	Field description	Value (for Google Gmail account)
SMTP Server	E-mail server address used to send messages.	smtp.gmail.com
Port	Port used for connection to the SMTP server.	465
User	E-mail address of the Gmail account used to send e-mails via the web server	E.g.: yyy.zzz@gmail.com
Password	“Password for Apps” (16 characters) created from the Google Gmail account for the web server. Important: web server access to the Google SMTP service made using the password of the Google account will no longer work from 30 th May 2022.	E.g.: aaaabbbbccccdddd
Sender	Specify the e-mail address to use as the message sender. Typically the address entered in the “User” field.	E.g.: yyy.zzz@gmail.com
Authentication	Specify whether the SMTP server requires authentication.	Yes
SSL encryption	Specify whether the SMTP server requires SSL encryption or not.	Yes



01945-01946 IEN 27 2206



VIMAR

Viale Vicenza, 14
36063 Marostica VI - Italy
www.vimar.com