VIMAR

Manuel de l'installateur

01945-01946

Web Server By-me

HOME AUTOMATION

by-me home automation

Contrat de licence Vimar avec l'utilisateur final

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

Sommaire

Sommaire

Sommaire

Pré-requis

P.1 COMPATIBILITÉ AVEC LES NAVIGATEURS WEB

Pour l'accès au **Web Server,** il est possible d'utiliser les navigateurs web suivants :

- Apple Safari (ver. 5,1 ou supérieure)
- Google Chrome (ver. 14 ou supérieure)

Le Web Server Vimar By-web n'est pas compatible avec le navigateur Microsoft Internet Explorer.

P.2 COMPATIBILITÉ AVEC LES SYSTÈMES D'EXPLOITATION

La complète compatibilité avec les diverses distributions de Linux n'est pas garantie.

P.3 COMPATIBILITÉ AVEC LES SYSTÈME BY-ME

Le tableau suivant présente toutes les versions de logiciel et d'équipement de la centrale By-me et du logiciel de configuration EasyTool Professional compatibles avec le Web Server.

Web Server	EasyTool Professional	Centrale By-me	Centrale 3 modules	Multimedia Video Touch Screen 10in P		
				Cod. 21553	Cod. 21553.1	Cod. 21553.2
01945 - ver. 2.2 01946 - ver. 2.2	ver. 2.12	ver. 5.1 ou supérieure	ver. 1.0 ou supérieure	ver. 1.4.01	ver. 4.0.05	ver. 5.0.xx

P.3.1 VERSION MINIMALE DU LOGICIEL WEB STATION DE STATION KNX SERVEUR DE GESTION (ARTICLE 01546

Si une station météo KNX est configurée dans l'installation, utiliser une version logicielle 1.15 ou suivante du serveur Internet.

P.4 PRÉ-REQUIS POUR L'ACCÈS À DISTANCE

Pour utiliser le Web Server à distance, il est nécessaire que :

- **l'adresse IP** (statique ou dynamique) **soit publique.**
- **certains paramètres du router puissent être modifiés.**

P.5 COMPATIBILITÉ AVEC LES SYSTÈME BY-ALARM

Le tableau suivant présente les versions SW et FW des central By-alarm compatibles avec le Serveur.

Serveur Internet	Centrale By-alarm	
(art. 01945-01946)	Art. 01700	Art. 01703
Version 1.20 ou suivantes	1.0 ou suivantes	1.0 ou suivantes

ATTENTION : Avant d'effectuer toute opération de configuration du Serveur, télécharger la version mise à jour du logiciel depuis la section Logiciel de produit du site www.vimar.com

1. Installation

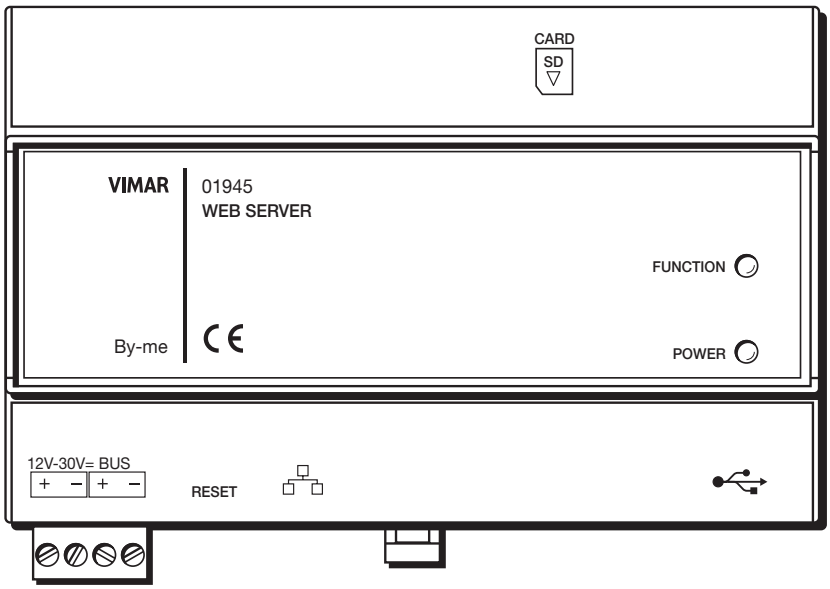
1.1 Montage et branchements art. 01945 (pour l'art. 01946, les références sont analogues).

Le Web Server est conçu pour être monté sur de guide DIN standard. Pour le correct fonctionnement du Web Server, il est nécessaire de prévoir les branchements suivants :

- Alimentation 12V CC en branchant l'alimentateur art. 01830 par l'intermédiaire du connecteur fourni en dotation.
- Bus By-me avec le connecteur fourni en dotation.
- Réseau LAN avec le câble cat. 5 ou supérieure et connecteur RJ45 standard.

Le voyant frontal identifié sous le nom « ALIMENTATION » signale la présence de l'alimentation, tandis que le voyant « FONCTION » reste normalement éteint hormis indication d'opérations particulières en cours.

Le Web Server met également à disposition les ports suivants :
- Fente SD : disponible pour des applications futures
- Port USB : disponibles pour des applications futures



REMARQUE : le branchement au bus **By-me** n'est pas indispensable pour la configuration du **Web Server**, cependant il reste recommandé car, en son absence, il est impossible d'en vérifier le fonctionnement correct.

L'art. 01946 peut contrôler jusqu'à 64 dispositifs By-me (centrale art. 21509 incluse). Seuls les dispositifs dotés d'une borne BUS + - peuvent être pris en compte.

Le Web Server (art. 01945-01946) peut gérer au maximum 1 module de contrôle des charges art. 01455.

1.1.1 Gestion de la carte SD par le Web Server

Le Web Server dispose d'une fente permettant l'insertion d'une carte mémoire SD.
La fente est de type « push-push ».

Caratteristiche SD card compatibili

Tipi SD card compatibili: SD, SDHC.
Tipo formattazione: FAT32

Insertion de la carte SD

1. Couper l'alimentation électrique du Web Server.
2. Insérer la carte SD dans la fente du Web Server prévue à cet effet, avec le versant indiqué sur l'étiquette du dispositif selon les indications de la fente.

   La carte doit être enfoncée jusqu'à ce qu'elle s'encastre dans la fente.
3. Restaurer l'énergie électrique du Web Server.

IMPORTANT : si la carte SD est insérée avec le Web Server sous tension, elle ne pourra pas être utilisée sur le Web Server.

Retrait de la carte SD

Pour extraire la carte SD dans le serveur, procéder comme suit :

1. Couper l'alimentation électrique du Web Server.
2. Appuyer sur la carte SD jusqu'à ce qu'elle se débloque de la fente et l'extraire.
3. Restaurer l'énergie électrique du Web Server.

1.1.2 Touche de RÉINITIALISATION

La touche de RÉINITIALISATION permet d'effectuer les opérations suivantes :

- Restauration des configurations réseau par défaut
- Restauration complète des données usine : paramètres réseau et configuration.

1.1.2.1 Restauration des paramètres réseau par défaut

Ce paramètre permet de restaurer les données de configuration réseau du Web Server aux valeurs d'usine.

Adresse IP : 192.168.0.110

Passerelle : 192.168.0.4

Masque de réseau : 255.255.255.0

ATTENTION : Une fois cette procédure appliquée, il ne sera plus possible de l'annuler.

La procédure prévoit les étapes suivantes :

1) Appuyer sur la touche RÉINITIALISATION et la maintenir enfoncée pendant 10 secondes. Le voyant « fonction » commencera à clignoter, indiquant l'accès au mode de configuration.
2) Relâcher la touche RÉINITIALISATION.
3) Appuyer sur la touche RÉINITIALISATION et la maintenir enfoncée pendant environ 1 seconde (**dans tous les cas moins de 4 secondes**). Quelques instants plus tard, le voyant cesse de clignoter et la procédure de réinitialisation des paramètres de réseau commence.

1.1.2.2 Restauration complète des données usine

Ce paramètre permet de restaurer toutes les données de configuration du Web Server aux valeurs d'usine (configuration des paramètres de réseau, données relatives
au système, informations utilisateur, historique du système Economiseur d'énergie).

ATTENTION : Une fois cette procédure appliquée, il ne sera plus possible de l'annuler.

La procédure prévoit les étapes suivantes :

1) Appuyer sur la touche RÉINITIALISATION et la maintenir enfoncée pendant 10 secondes. Le voyant « fonction » commencera à clignoter, indiquant l'accès au mode de configuration.
2) Relâcher la touche RÉINITIALISATION.
3) Appuyer sur la touche RÉINITIALISATION et la maintenir enfoncée pendant environ 5 secondes. Quelques instants plus tard, le voyant cesse de clignoter et la procédure de réinitialisation des paramètres de configuration.

1.2 Connexion par réseau

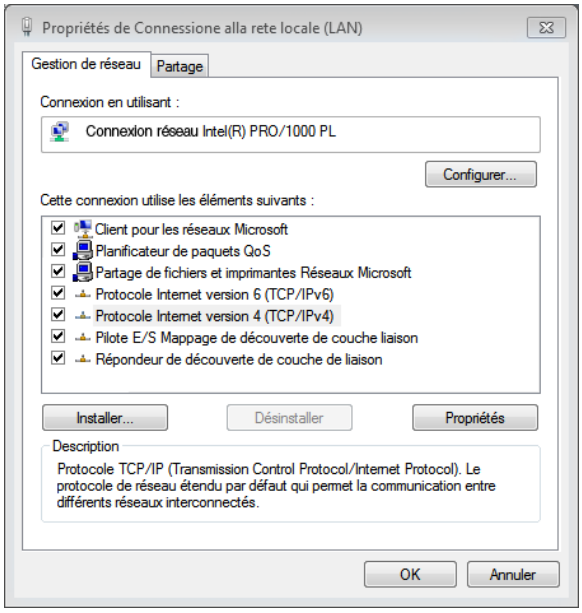
La configuration et l'utilisation du **Web Server** prévoient un branchement au réseau domestique ou professionnel.

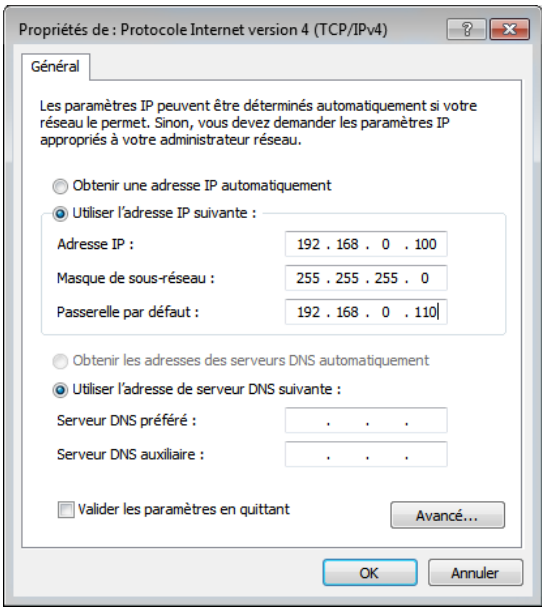
Les paramètres de réseau du Web Server devront être configurés en fonction de la configuration du réseau LAN dans lequel il doit être inséré.

Pour la première configuration du **Web Server,** tout comme en cas d'absence de réseau durant la phase d'installation, il est nécessaire de procéder comme indiqué ci-après :

- Brancher le **Web Server** au PC en utilisant un câble de réseau ethernet (droit, straight through) ou croisé (crossover).
- Accéder aux paramètres de réseau du PC, comme illustré dans la documentation du système d'exploitation.
- Modifier les paramètres du protocole de communication TCP/IP (version 4) relative au port LAN auquel est relié le **Web Server**, et configurer manuellement les paramètres suivants :
  - Adresse IP : 192.168.0.100
  - Masque de réseau : 255.255.255.0
  - Passerelle prédéfinie : 192.168.0.110
- Enregistrer et patienter jusqu'à ce que les nouveaux paramètres deviennent effectifs. Si cela est demandé, redémarrer le système.

Les figures ci-dessous montrent, à titre d'exemple, les fenêtres de configuration du réseau pour un PC équipé du système d'exploitation Windows 7.

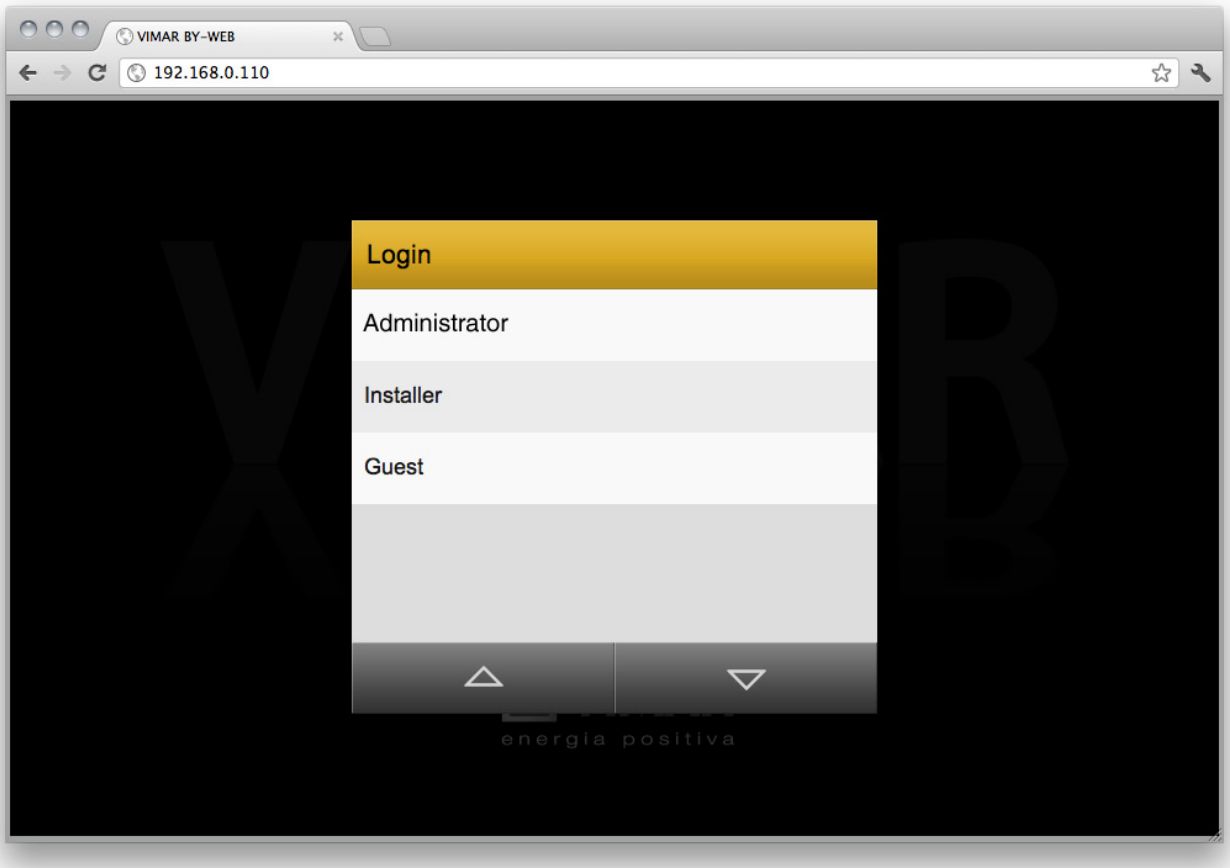




Une fois cette opération terminée, ouvrir un navigateur internet et saisir les informations suivantes dans la barre d'adresse :

http://192.168.0.110

Si la configuration du réseau est correcte, la page de bienvenue suivante s'affichera :



Si les paramètres de réseau par défaut du Web Server ne sont pas compatibles avec la configuration du réseau LAN dans lequel il doit être inséré, après y avoir accédé, comme décrit ci-dessus :

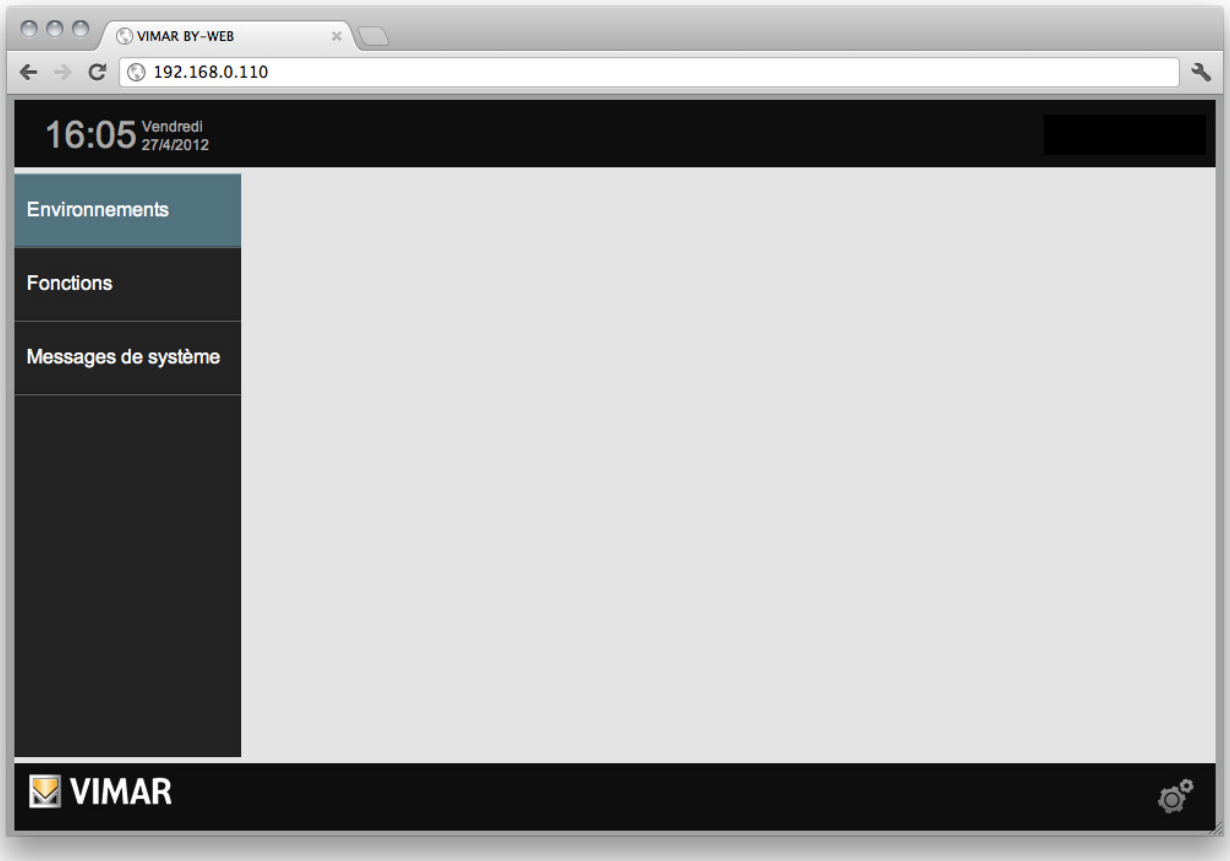
1. Modifier les paramètres de réseau du Web Server en fonction de la configuration du réseau LAN
2. Restaurer la configuration réseau du PC à l'originale.

1.3 Accès

Le Web Server propose les utilisateurs prédéfinis suivants :

UTILISATEUR	MOT DE PASSE	DESCRIPTION
Administrator	**admin**	Utilisateur administrateur du système domotique.
Installer	**poweruser**	Utilisateur dédié à l'installation et à la configuration du Web Server. Ce dernier possède les droits pour effectuer toutes les opérations sur le système mais ne peut pas modifier les droits des autres utilisateurs.
Guest	**guest**	Utilisateur de base pour connexions depuis un PC. Ce dernier peut visualiser le statut du système, naviguer dans le pages du Web Server et effectuer des commandes de base sur le système domotique.

Pour configurer la supervision du système By-me, il est nécessaire de sélectionner l'utilisateur « installateur » dans la liste et de saisir le mot de passe correspondant (lequel pourra être modifié par la suite). Une fois le chargement terminé, la page-écran principale du Web Server s'affichera :

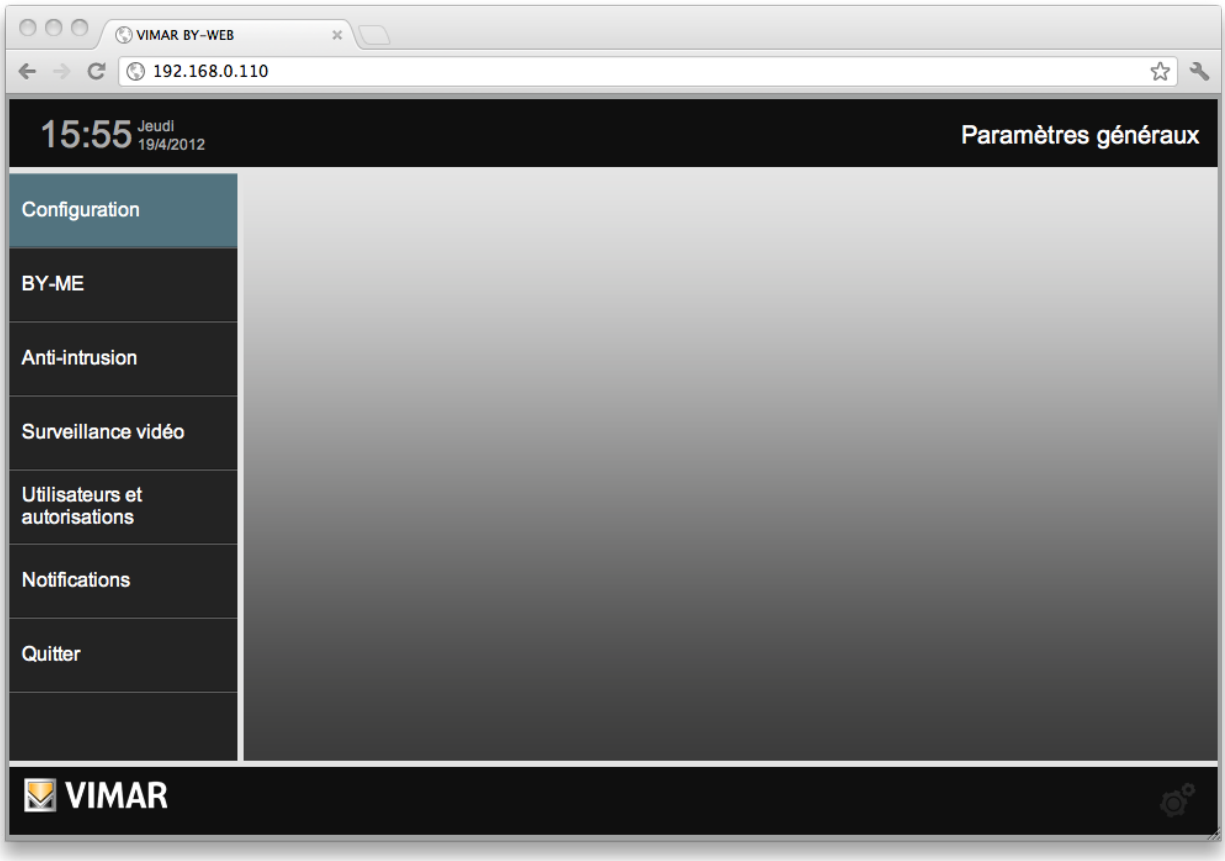


NOTE: Pour des raisons de sécurité, il est conseillé aux usagers Administrateur, Installateur et Guest de modifier le mot de passe fourni par défaut.

2. Paramètres généraux

2.1 Avant-propos

Le **Web Server** peut être configuré et personnalisé depuis la section prévue à cet effet PARAMÈTRES GÉNÉRAUX, accessible en sélectionnant « Paramètres généraux » dans le menu déroulant visible en appuyant sur la touche en bas à droite de la page. La page suivante s'affiche :



Le menu disponible sur la gauche permet d'accéder aux sections suivantes :

CONFIGURATION	Paramètres à caractère général sur le **Web Server** et opérations d'entretien.
BY-ME	Configuration de la supervision du système **By-me**.
ANTI-INTRUSION	Modifier le nom des Découpages
SURVEILLANCE VIDÉO	Configuration des caméras vidéo IP.
UTILISATEURS ET AUTORISATIONS	Configuration des utilisateurs autorisés à utiliser le **Web Server** et autorisations relatives.
NOTIFICATIONS	Configuration des notifications par courrier électronique suite aux alarmes SAI.
QUITTER	Retour à la page principale du **Web Server**.

Dans les pages spécifiques de configuration des différents aspects du **Web Server**, un clavier est toujours disponible dans la partie inférieure de la page et propose une ou plusieurs des touches suivantes :

	RETOUR Permet de revenir à la page précédente ou au menu principal de configuration
	VERS LE HAUT Permet de faire défiler le contenu de la page vers le haut, lorsque la hauteur disponible de la page est dépassée
	VERS LE BAS Permet de faire défiler le contenu de la page vers le bas, lorsque la hauteur disponible de la page est dépassée
	CONFIRMER Si présente, cette touche permet d'enregistrer les modifications effectuées sur la page. Sur les pages où cette touche n'est pas disponible, les éventuelles modifications sont instantanément enregistrées sans besoin de confirmation.
	AJOUTER/ INSÉRER Si présente, cette touche permet – en fonction des cas – de créer un nouvel élément dans une liste (ex : création d'un nouvel environnement), ou encore d'ajouter des éléments corrélés à celui courant en utilisant le moteur de recherche (ex : ajout de dispositifs dans l'environnement courant)

Les paragraphes suivants illustrent dans le détail les fonctions disponibles dans la section « CONFIGURATION » des PARAMÈTRES GÉNÉRAUX. Les autres sections seront approfondies dans les chapitres suivants.

2.2 Langue

2.2.1 Configuration de la langue au premier démarrage

Lors du premier démarrage du Web Server, et après chaque opération de « Réinitialisation de la configuration usine », une fenêtre de configuration de la langue s'ouvrira. Il est dans tous les cas possible de modifier la langue utilisée par le Web Server ultérieurement en utilisant le menu consacré décrit au chapitre suivant.

2.2.2 Configuration de la langue du menu

Cette page permet de modifier la langue du Web Server.
Pour accéder aux PARAMÈTRES GÉNÉRAUX, sélectionner le menu CONFIGURATION puis l'option LANGUE.
Cette page propose un menu déroulant permettant de sélectionner la langue du Web Server, une fois la langue de préférence sélectionnée, appuyer sur la touche de confirmation située en bas à droite. Après un court instant, la nouvelle langue sélectionnée sera chargée dans le Web Server.
En revanche, si la touche de sortie située en bas à gauche est enfoncée durant la phase de sélection de la langue, la modification ne sera pas prise en compte et le logiciel reviendra à la page de Paramètres généraux.

2.3 Réseau

Dans cette page, il est possible de configurer les paramètres réseau du Web Server; cette opération est nécessaire pour :

1. Modifier les paramètres réseau du serveur web, si ceux configurés en usine ne sont pas compatibles avec la configuration du réseau LAN sur lequel il doit être installé.
2. Terminer la procédure de gestion des certificats SSL du serveur web, introduite à partir de la version 1.12 du logiciel du Web Server.

IMPORTANT : cette procédure exige que le Web Server dispose d'une connexion Internet. Si le Web Server ne dispose pas d'une connexion Internet, il utilisera alors le certificat SSL fourni par les versions précédentes du logiciel de Web Server.

Pour ce faire, même s'il n'est pas indispensable de modifier les paramètres réseau du serveur web configurés en usine, il sera cependant toujours nécessaire de confirmer la configuration du réseau en appuyant sur la touche .

REMARQUES:
Les versions 2.5 et 2.6 disposent des mises à jour dans la gestion de la communication protégée HTTPS, conformément aux directives actuellement en vigueur. Plus particulièrement, le certificat CA de Vimar mis à jour est disponible, il est possible de gérer la création du certificat TLS mis à jour du serveur Internet et de mettre à jour le protocole TLS à la version 1.2.
Il est donc conseillé de mettre à jour le serveur Internet à la version 2.6.

En mettant à jour le serveur Internet à la version 2.5, qui comporte des nouveautés importantes sur la gestion des certificats TLS, il est nécessaire de confirmer les paramètres de réseau du serveur Internet (avec le serveur connecté à Internet) de sorte qu'il puisse actualiser son certificat TLS et télécharger le certificat CA de Vimar à la toute dernière version.

La version 2.6 du logiciel du serveur Internet dispose désormais des automatismes et des procédures automatiques pour la mise à jour du certificat TLS du serveur Internet et du certificat CA de Vimar. Suivre les procédures pour mettre à jour le plus tôt possible lesdits certificats pour la gestion de la connexion protégée HTTPS. La version 2.6 met également à disposition la nouvelle version firmware pour les serveurs Internet moins récents. Cette version dispose du protocole TLS à la version 1.2, ainsi que l'exigent les dernières directives.

Paramètres généraux

Avant de décrire la procédure de saisie des paramètres, il est utile de faire un petit récapitulatifs sur la façon dont fonctionne un réseau.

- L'accès à distance au Web Server est effectué via Internet.
- Chaque nœud Internet (hôte) est individualisé de façon univoque par un numéro (IPv4 32 bit - IPv6 128 bit), appelé communément Adresse IP. Exemple d'adresse IPv4 : 190 230 140 122
- Pour faciliter l'individualisation des nœuds Internet, un système permettant d'associer une chaîne alphanumérique aux adresses a été créé.

  IP : DNS (Domain Name System)

  Par exemple :
  Adresse IP : 213 178 196 136
  Nom DNS : www.vimar.com
- Bien évidemment, pour accéder à un nœud IP, il est nécessaire de connaître l'adresse ou le nom DNS associé
- L'attribution d'une adresse IP à un hôte peut être :

  - statique : l'adresse est attribuée de façon permanente

  - dynamique : l'adresse attribuée n'est pas toujours la même.

  L'exemple type est celui de l'adressage fourni par les fournisseurs de service Internet auquel les utilisateurs privés font référence pour l'accès à Internet. L'adresse est généralement attribuée à chaque connexion (dans certains cas, elle peut même être modifiée à l'intérieur d'une même session)
- Pour permettre l'accès aux nœuds Internet auxquels l'adresse est attribuée dynamiquement, des services se sont développés, permettant de créer une association dynamique entre le nom DNS (attribué à un utilisateur) et l'adresse IP. Ces services prennent le nom de DNS dynamiques (DDNS, Dynamic DNS)
- De nombreux routers ADSL actuellement disponibles sur le marché supportent automatiquement les services DDNS d'un ou plusieurs fournisseurs. Les routers envoient l'adresse IP actualisée suite à l'attribution ou modification de l'adresse IP par le fournisseur de service internet, au fournisseur DDNS.
- Habituellement, la configuration d'un DNS dynamique sur un router supportant ce type de technologie prévoit les étapes suivantes :
  1. Création d'un compte auprès du fournisseur DNS dynamique choisi (ex : DynDNS.org)
  2. Dans le menu de configuration Internet du router, sélectionner l'utilisation du DNS dynamique (Dynamic DNS, DDNS)
  3. Sélectionner le fournisseur DNS dynamique parmi ceux gérés par le router (généralement par le biais d'un menu déroulant)
  4. Saisir les données de configuration fournies par le fournisseur de DNS dynamique dans les champs correspondants.
- Pour l'accès à distance au serveur Internet, la configuration suivante est nécessaire:
  - Configuration de l'adresse IP du serveur Internet dans le réseau LAN. Le Web Server dispose d'une configuration par défaut de cette adresse. En cas de nécessité de modifier cette adresse, accéder au Web Server en utilisant l'adresse prédéfinie et la modifier depuis la page de configuration relative.
  - Configuration du NAT sur le routeur. Cette configuration, à effectuer sur le router, sert à dire au router que les demandes à distances effectuées sur le port https doivent être adressées à l'adresse LAN identifiant le Web Server. Pour effectuer ces configurations, consulter le manuel d'instructions du router.
  - Vérifier l'ouverture du port https sur le routeur ADSL (port 443) et, si la gestion à distance de la configuration et du diagnostic du système By-alarm avec le logiciel By-alarm manager est prévue, exécuter aussi l'ouverture du port du routeur cartographié sur le port du logiciel By-alarm manager pour l'accès au serveur Internet

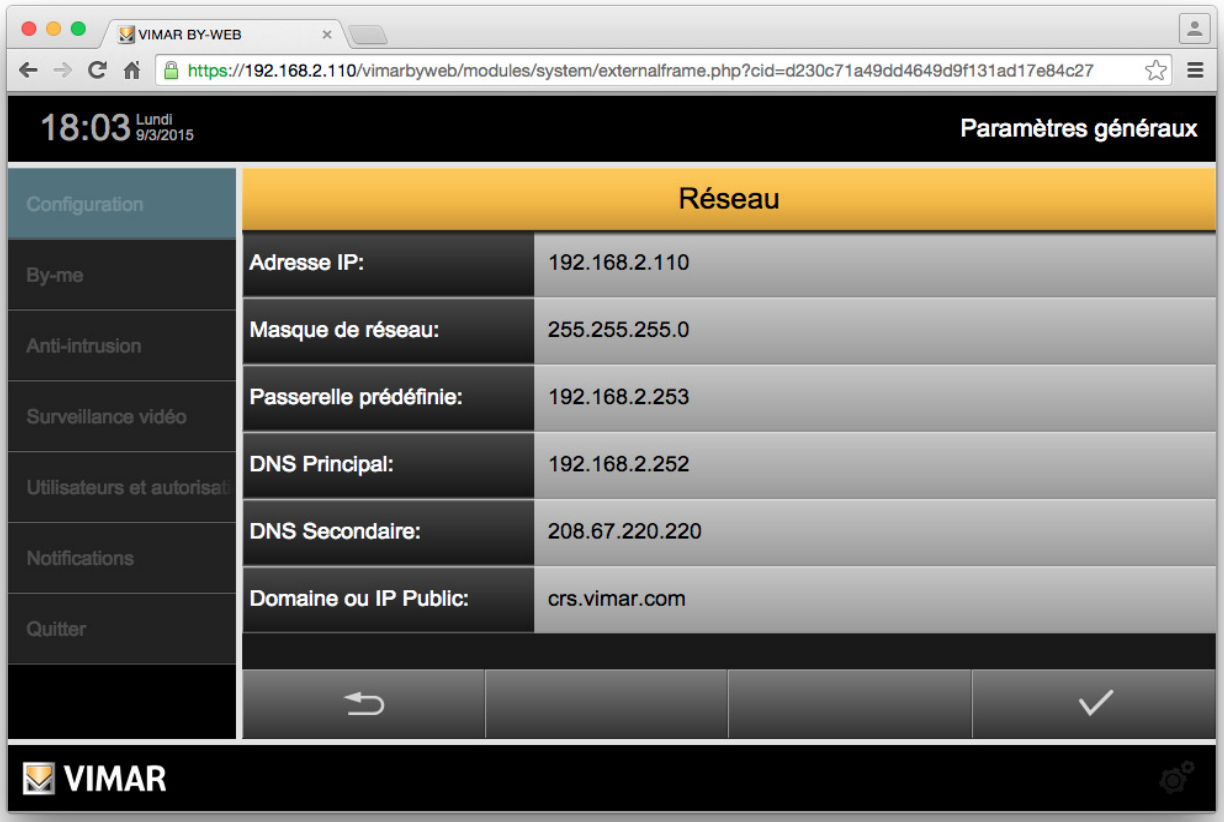
    NOTE: si le port 443 de l'interface extérieure du routeur est déjà utilisé par d'autres services, il est possible d'utiliser un autre port (s'il est libre) à associer au port 443 du serveur Internet (non modifiable) par création d'un réglage du port forwarding sur le routeur.

    IMPORTANT: pour des raisons de sécurité, configurer le routeur pour que seuls les ports 443 du serveur Internet soient accessibles de l'extérieur du réseau LAN (HTTPS) idem pour le port choisi pour la configuration à distance de la centrale By-alarm (s'il y en a une dans l'installation).
  - Si on utilise des systèmes DNS dynamique, exécuter les configurations suivantes.
- Le Web Server utilise le protocole HTTPS permettant d'augmenter la sécurité de la connexion à distance entre l'utilisateur et le Web Server. Le protocole utiliser un port spécifique (le 443) lequel doit être ouvert sur le router.
- Le Web Server peut également être utilisé si le fournisseur de service Internet assigne une adresse dynamique.
- Le Web Server gère, de base, le service de DNS dynamique proposé par DynDNS.
  Dans ce cas, procéder aux configurations relatives sur les pages consacrées aux Web Server.
  En cas d'utilisation d'un router gérant, de base, le service de DNS dynamique choisi par l'utilisateur, procéder aux configurations nécessaires sur le router.

Paramètres généraux

Saisir les informations suivantes dans les champs correspondants :

ADRESSE IP	Adresse attribuée au Web Server, caractérisée par 4 chiffres séparés par un point. L'adresse doit être valide et univoque à l'intérieur du réseau LAN, sous peine de ne pouvoir communiquer avec le Web Server.
MASQUE DE RÉSEAU	Indiquer le masque de réseau utilisé par le propre réseau LAN, sauf indication particulière, saisir « 255,255,255,0 ».
PASSERELLE PRÉDÉFINIE	En présence d'un router ou autre dispositif mettant le réseau LAN en communication avec d'autres réseaux ou avec Internet, spécifier son adresse dans ce champ. Dans le cas contraire, indiquer la même adresse que celle attribuée au Web Server. **NOTA BENE**: Pour utiliser le Web Server à distance, il est indispensable de configurer l'adresse IP du routeur dans le champ Passerelle prédéfinie.
DNS PRINCIPAL DNS SECONDAIRE	Spécifier l'adresse des serveurs DNS principal et secondaire, nécessaires aux fonctions du Web Server nécessitant un accès internet. Saisir les adresses fournies par le fournisseur de service Internet ; en laissant ces champs vides, le Web Server utilisera des valeurs valides dans la plupart des configurations.
DOMAINE OU IP PUBLIQUE	Pour accéder à distance au serveur web 01945-01946, il est nécessaire de configurer également le « Domaine ou IP publique » du serveur web. En présence d'une adresse IP publique statique, cette valeur peut être saisie directement. En présence d'une adresse IP dynamique et avec gestion via DNS dynamique, il sera alors nécessaire de saisir le domaine. Le domaine est la partie de texte comprise entre le protocole et le port d'accès. Exemple : Si l'URL d'accès à distance est « https://example.dyndns.org:4123 », le domaine d'accès à distance à saisir est : « example.dyndns.org »

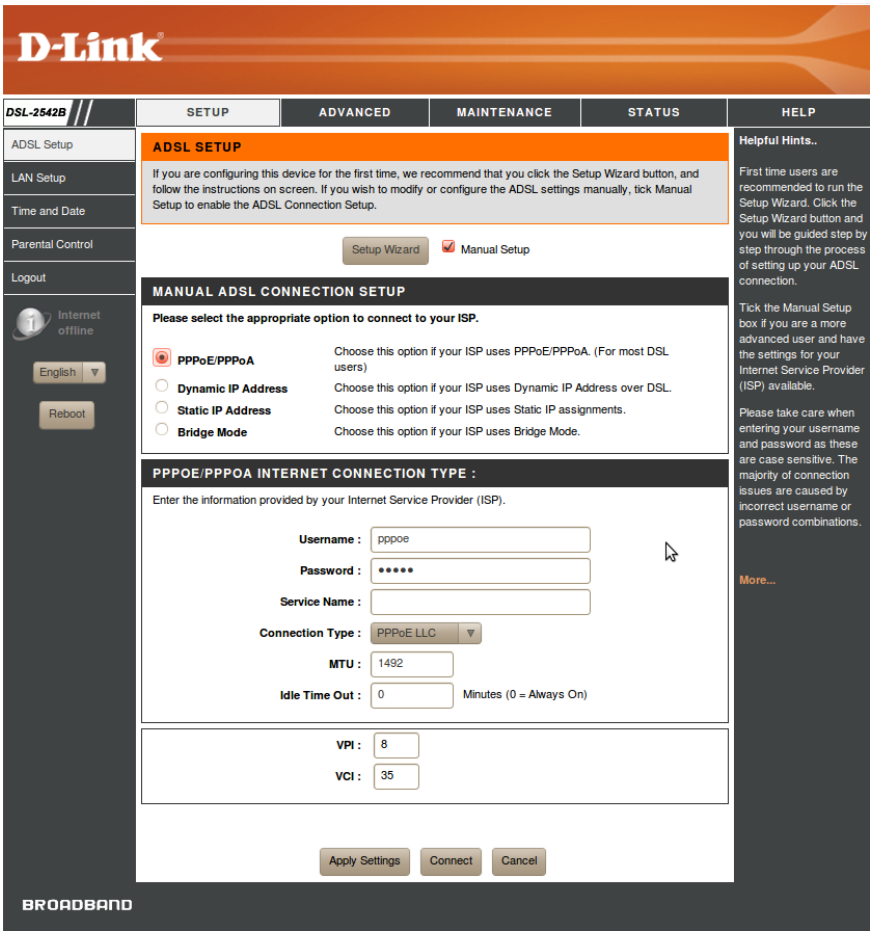


EXEMPLE DE CONFIGURATION DU ROUTER.

L'exemple suivant illustre les opérations à effectuer pour configurer correctement le router (ouverture des ports, configuration port forwarding, etc.)

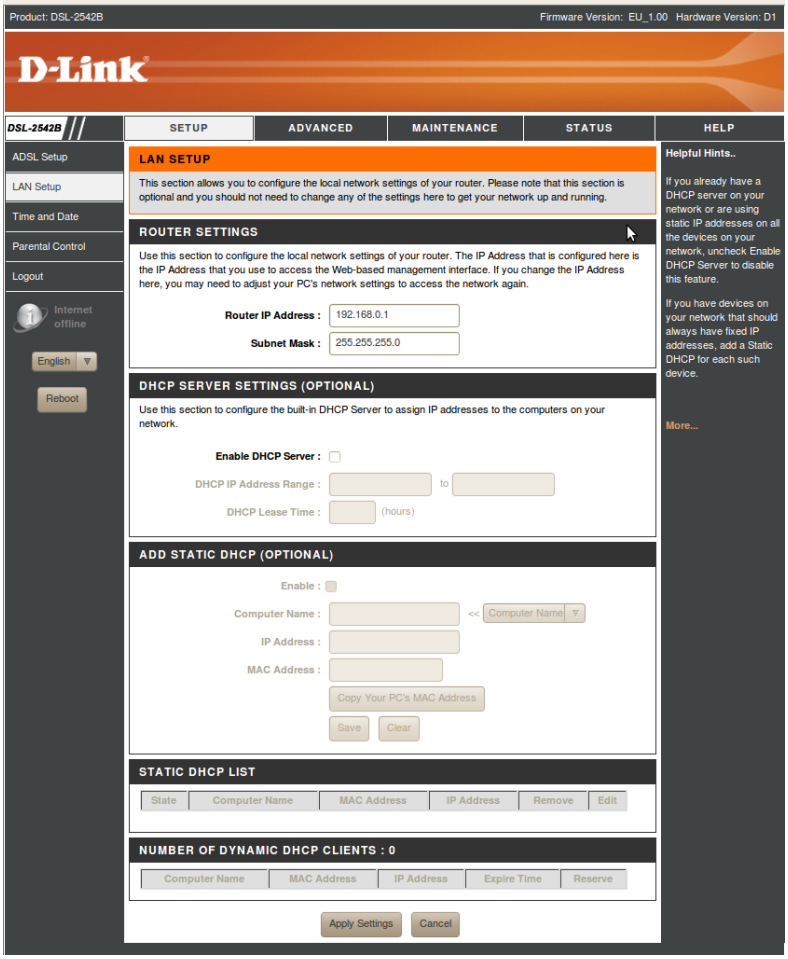
Bien entendu, les pages-écran proposées seront différentes en fonction du router utilisé, cependant les options et les paramètres sont les mêmes ou dans tous les cas très semblables.

- CONFIGURATION WAN



La page-écran du router ci-dessus correspond aux paramètres de la WAN (interface de réseau « externe » du router, vers le monde Internet). Ces paramètres dépendent du fournisseur de services Internet de l'utilisateur et **NE DOIVENT PAS ÊTRE MODIFIÉES !!**

- CONFIGURATION LAN

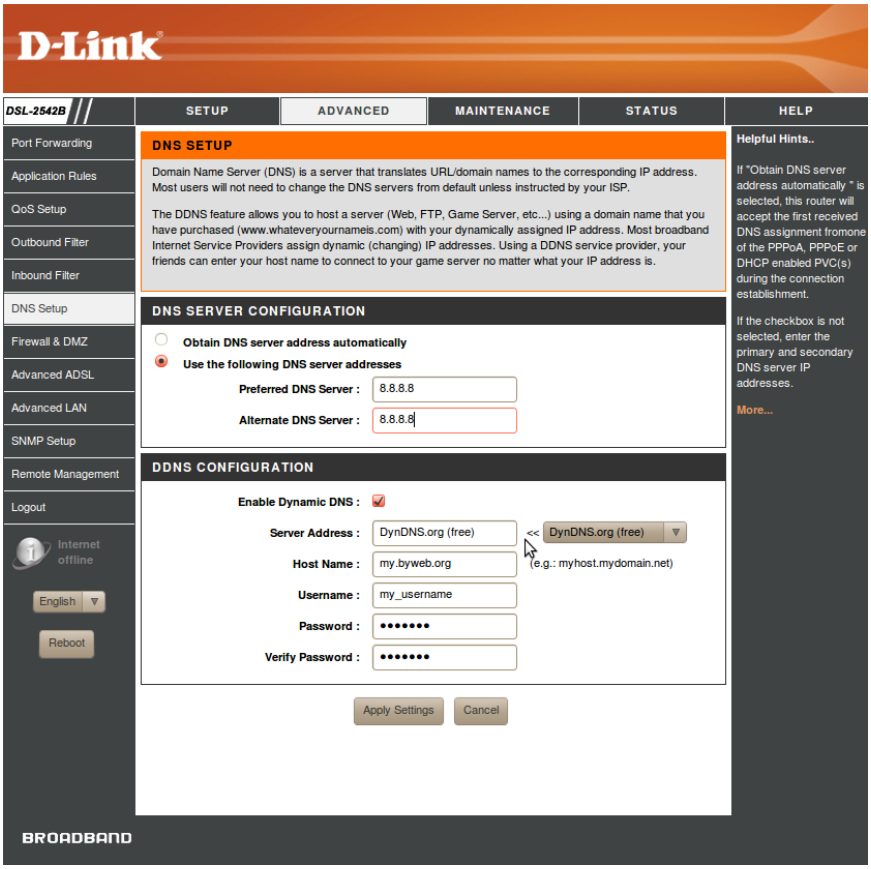


Ce image représente la page-écran du router relative aux paramètres de la LAN (interface de réseau « interne » du router, celui du réseau local de l'utilisateur). Ces paramètres dépendent de la structure du réseau LAN et **NE DOIVENT PAS ÊTRE MODIFIÉES !!**

Dans cet exemple, le router a l'adresse IP (LAN) : **192.168.0.1.**

IMPORTANT : afin de permettre d'établir la connexion à distance avec le Web Server, il est nécessaire que le router et le Web Server se trouvent dans le même sous-réseau.

- DYNDNS



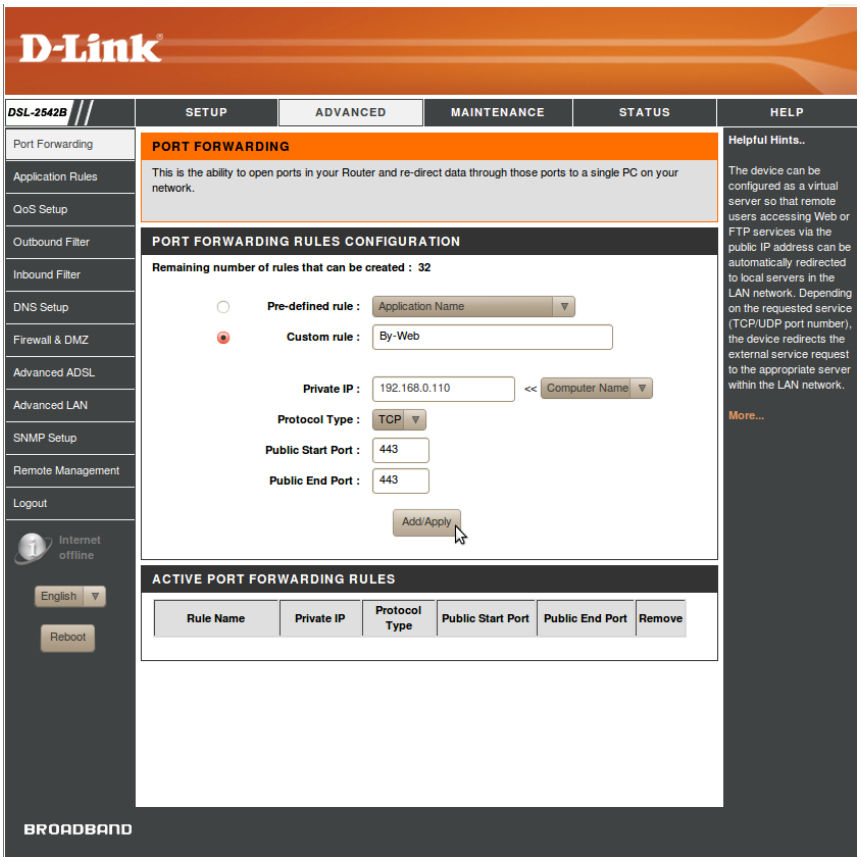
Cette image représente la page-écran du router relative aux paramètres du DNS et l'éventuelle utilisation des services de DNS dynamique (par exemple DynDNS).

REMARQUE : les valeurs saisies dans le champ DNS et DNS alternatif sont purement indicatives et non obligatoires.
Les données saisies pour la gestion de DynDNS sont purement indicatives et représentent les données fournies par l'utilisateur au moment de l'inscription sur DynDNS.

Concernant la page-écran ci-dessus, les données devant être saisies pour la configuration du service de DNS dynamique « DynDNS » (dans la section « CONFIGURATION DDNS » sur la figure) sont les suivantes :

- **Adresse du serveur** : choix du service de DNS dynamique (le router utilisé dans l'exemple dispose d'un menu déroulant dans lequel il possible de procéder à la sélection)
- **Nom de l'hôte** : il s'agit de l'adresse url utilisée pour individualiser l'utilisateur sur Internet.
  Cette information est saisie durant l'inscription sur le site du fournisseur de service de DNS dynamique et associée de façon dynamique à l'adresse IP de l'interface externe (WAN) du router de l'utilisateur.
- **Nom de l'utilisateur** : le nom de l'utilisateur est saisi par l'utilisateur durant son inscription sur le site du fournisseur de service de DNS dynamique.
- **Mot de passe** : le mot de passe est saisi par l'utilisateur durant son inscription sur le site du fournisseur de service de DNS dynamique.

- PORT FORWARDING



Cette image représente la page-écran du router correspondant aux paramètres du port forwarding, dans lequel a été créée une règle pour l'accès à distance au Web Server Vimar (le nom de la règle « By-Web » est indicatif et non-obligatoire) :

- adresse du Web Server (ici, l'adresse utilisée est celle par défaut) : 192.168.0.110
- ouverture du port 443 (nécessaire pour l'accès au Web Server)

2.4 Mise à jour

Cette page permet d'actualiser la version du logiciel présent dans le Web Server.

Pour cela, suivre la procédure indiquer ci-après :

1. Accéder au menu de configuration en utilisant l'icône  et sélectionner l'option **Configuration -> Mise à jour**
Co mparer la fenêtre de mise à jour du logiciel dans laquelle est indiquée la version actuelle du logiciel du Web Server.
2. Appuyer sur la touche «**Sélectionner fichier** » (ou « **parcourir** », en fonction de la mention utilisée par le navigateur) et sélectionner le pack d'installation fourni, lequel doit être présent dans le PC utilisé pour accéder au Web Server
3. Passer à la page-écran suivante en appuyant sur la touche «**Confirmation**»
4. Sélectionner l'option «**Ajouter fichier** »
5. Appuyer sur la touche **« Actualiser logiciel** » La procédure peut prendre plusieurs minutes.
6. Une fois la procédure de mise à jour terminée, le redémarrage du Web Server est demandé. Appuyer sur la touche «**Redémarrer maintenant** ».
7. Patienter environ 2 minutes avant de rallumer le Web Server (procéder au rafraîchissement de la page sur le navigateur).

Après le redémarrage, le chargement du fichier XML du système pourrait être demandé par le Serveur Web.

REMARQUE: en cas d'apparition de messages d'erreur sur l'écran, merci de contacter le service clients Vimar.

IMPORTANTE: La version 2.6 présente de nouvelles fonctions et mises à jour importantes relatives à la gestion de la connexion protégée HTTPS entre le serveur Internet et les clients qui permettent d'accéder au serveur Internet.
Il est conseillé de vérifier la version du logiciel qu'utilise le serveur Internet et, s'il n'est pas encore actualisé sur la version 2.6, il est conseillé de procéder à la mise à jour le plus rapidement possible.
En cas de serveurs internet dont la version matérielle est moins récente, pour procéder à d'importantes mises à jour pour la gestion de la connexion protégée HTTPS, après l'avoir actualisé à la version 2.6, le serveur internet présentera un message contenant les indications pour procéder à la « Firmware Upgrade » (mise à jour du microprogramme) ; cette procédure est décrite au chapitre suivant.
Pour les informations supplémentaires concernant les versions 2.5 et 2.6 du logiciel du serveur Internet, consulter le chapitre « Mises à jour importantes faisant partie des versions 2.5 et 2.6 du logiciel du serveur Internet pour la gestion de la connexion protégée HTTPS » de ce manuel.

2.5 Firmware Upgrade

La version 2.6 du logiciel du serveur Internet dispose de la fonction « Firmware Upgrade » (mise à jour du microprogramme du serveur Internet) qui permet de mettre à jour le système d'exploitation du serveur Internet lorsque les paquets traditionnels de mise à jour ne le permettent pas.

La procédure de mise à jour du microprogramme ne remplace pas la procédure de « mise à jour logiciel » qui passe par le téléchargement de paquets de mise à jour disponibles sur le site Internet de Vimar, et elle permettra de gérer certaines exigences spécifiques.

S'il est connecté à Internet, le serveur procède régulièrement à un contrôle sur la disponibilité d'une nouvelle version microprogramme : si une nouvelle version est disponible, il informera l'utilisateur à travers un message et lui demandera de lancer la procédure de « Firmware upgrade » décrite ci-après.

La procédure de mise à jour du microprogramme peut être lancée à partir de la page dédiée à laquelle on accède en appuyant sur le bouton « Firmware Upgrade » du menu « Setup » de la section « Paramètres généraux » (pour les utilisateurs disposant des identifiants pour accéder à la section en question).

IMPORTANT : La mise à jour du firmware du serveur Internet est une procédure qui ne peut être effectuée que lorsque le serveur est connecté à Internet ; le serveur Internet affiche des messages signalant qu'il n'arrive pas à accéder à Internet.

En accédant à la page de « Firmware Upgrade » le serveur Internet, s'il est connecté à Internet, vérifie la disponibilité d'un nouveau microprogramme:

- S'il n'y a aucune nouvelle version disponible, la fenêtre affiche : Version firmware actuelle et Version firmware disponible. Pour les serveurs Internet dont le microprogramme n'a jamais été mis à jour et pour lesquels aucune nouvelle version n'est disponible, les messages suivants s'affichent : NO VERSION et NO AVAILABLE VERSION.
  REMARQUE : pour les serveurs Internet dont le microprogramme n'a jamais été mis à jour et pour lesquels aucune nouvelle version n'est disponible, les messages suivants s'affichent : NO VERSION et NO AVAILABLE VERSION (c'est le cas des serveurs Internet plus récents produits par Vimar).
- Si une nouvelle version du microprogramme est disponible:
  - Le champ avec la version microprogramme actuelle se distinguera de celui avec la version microprogramme disponible.
  - Un texte s'affiche avec les consignes à respecter pour que la procédure de mise à jour soit effectuée correctement.
  - Le champ « Mise à jour Firmware » s'affiche ; appuyer sur « Marche » pour lancer la procédure de mise à jour du microprogramme.

IMPORTANT : si la procédure de « Firmware Upgrade » devait s'interrompre, le serveur Internet pourrait ne plus être accessible. Il sera nécessaire de faire appel au service d'assistance Vimar.
La procédure de « Firmware Upgrade » prévoit les passages suivants, qu'il faut respecter pour obtenir la mise à jour correcte du microprogramme :

1. **Exporter la base de données du serveur Internet (création d'une copie de sauvegarde de la base de données du serveur Internet).**
   À partir de la version 2.6 du logiciel du serveur Internet, cette procédure fait une copie de sauvegarde des données du Monitorage de l'énergie, enregistrées sur la mémoire FLASH du serveur Internet.
2. **Réarmer les données d'origine de la base de données du serveur Internet. Cette opération est fondamentale et doit être effectuée correctement pour ne pas compromettre le fonctionnement du serveur Internet.**
3. **Lancer la procédure de « Firmware Upgrade » en appuyant sur le bouton « Marche » qui se trouve à droite du champ « Mise à jour Firmware ».**
4. **Une fois la procédure de « Firmware Upgrade » terminée, importer sur le serveur Internet la copie de la base de données créée au point 1.**

IMPORTANT : pour porter à terme correctement la procédure de mise à jour firmware, respecter les consignes ci-après. Le non-respect de ces consignes pourrait compromettre le fonctionnement du serveur Internet.

- **NE PAS couper le courant au serveur Internet pendant la procédure de « Firmware Upgrade ».**
- **NE PAS interrompre la connexion Internet pendant la procédure de « Firmware Upgrade ».**
- **NE PAS quitter la page du navigateur pendant la procédure de « Firmware Upgrade »**

La procédure de mise à jour Firmware pourrait durer une heure : la durée de l'opération dépend également de la qualité de la connexion Internet.

Si vous avez lancé la procédure de mise à jour firmware sans que le serveur soit connecté à Internet, la procédure n'aura pas lieu et un message s'affichera. Durant la procédure de mise à jour firmware, une page noire contenant une barre d'avancement s'affiche.

En cas d'erreur durant la procédure de mise à jour, le serveur Internet signale le problème et vous devrez contacter le service d'assistance Vimar.

Remarque : après avoir mis à jour le microprogramme, il pourrait s'avérer nécessaire de supprimer des données de la chronologie du navigateur Google Chrome (consulter la documentation du navigateur pour procéder à cette opération) ; effectuer cette opération, par exemple, si après la mise à jour du microprogramme et après avoir remis en marche le serveur Internet, la page avec le logo Vimar s'affiche mais la fenêtre d'accès du serveur Internet n'apparaît pas au bout de quelques secondes, ou encore dans d'autres situations présentant des anomalies au niveau de la présentation graphique des pages du serveur Internet.

2.6 Base de données

Cette page permet de travailler sur la base de données du **Web Server**, contenant la configuration du projet de supervision. Il est possible d'effectuer les opérations suivantes, en sélectionnant l'option correspondante dans la liste :

EXPORTER	Cette fonction permet d'exporter une copie de sauvegarde de la base de données et de l'enregistrer sur le PC afin de la charger successivement sur le même ou sur un autre **Web Server**.
IMPORTER	Cette fonction permet de charger une copie de sauvegarde précédemment enregistrée sur le PC depuis le même ou depuis un autre **Web Server**.
RESTAURER	Cette fonction permet de restaurer la configuration usine de la base de données du **Web Server**. **Remarque** : cette opération ne réinitialisera pas l'adresse IP originale du **Web Server**.

Remarque : Jusqu'à la version 2.5 (comprise) du logiciel du serveur Internet, les opérations d'exportation et d'importation de la base de données n'interviennent pas sur les données du Monitorage de l'énergie enregistrées sur la mémoire FLASH du serveur Internet.

À partir de la version 2.5, les opérations d'exportation et d'importation de la base de données du serveur Internet concernent également les données du monitorage de l'énergie enregistrées sur la mémoire FLASH du serveur Internet.

Une fois la fonction désirée sélectionnée, utiliser la touche CONFIRMER située sur le clavier pour démarrer la procédure. Celle-ci peut nécessiter plusieurs minutes, durant lesquelles il est important de ne pas effectuer d'autres opérations sur le **Web Server** et de ne pas fermer la fenêtre du navigateur.

2.7 Fonds d'écran

Les commandes suivantes sont proposées :

EXPORTER	Cette commande permet d'enregistrer, sur PC, une copie de sauvegarde des images utilisées en fonds d'écran sur le Web Server. Procédure : 1. Sélectionner « Exporter ». 2. Appuyer sur la touche de confirmation ✓ . 3. Une fois la phase de traitement du serveur web terminée (durant laquelle un message s'affiche à l'écran), le fichier sera enregistré sur le PC selon la modalité configurée dans les paramètres du navigateur concernant le téléchargement de fichiers (voir la documentation du navigateur utilisé).
IMPORTER	Cette commande permet de charger une copie de sauvegarde des fonds d'écran, précédemment enregistrée sur PC. Procédure : 1. Sélectionner « Importer ». 2. Appuyer sur la touche « Sélectionner fichier ». La fenêtre de navigation du système s'affiche à l'écran. 3. Sélectionner le fichier de sauvegarde des fonds d'écran précédemment enregistré sur le PC (comme décrit dans la procédure « Exporter ») et appuyer sur la touche « Ouvrir ». 4. Appuyer sur la touche de confirmation ✓ .

2.8 Gestion de la carte mémoire SD

Le serveur web dispose d'une fente permettant l'insertion de cartes SD. Certaines fonctions nécessitent la présence du Web Server et une activation correcte de la carte mémoire SD (ex : messages vidéo).
Si, au moment du démarrage du serveur web, une carte SD fonctionnante est présente, celle-ci sera automatiquement détectée et validée par le serveur web.
Pour être utilisée par le Web Server, la carte mémoire SD doit être correctement insérée et activée par le serveur web.
La page « Gestion de la carte mémoire SD » permet de vérifier la présence de la carte mémoire, son état d'activation, avec présence des commandes d'activation et de désactivation.

CARTE MÉMOIRE PRÉSENTE	Indique la présence de la carte SD dans la fente du serveur web : États possibles : • Non : la carte SD n'est pas insérée dans la fente du serveur web, ou est insérée mais non détectée par le serveur web (carte mémoire SD non compatible ou endommagée). • Oui : la carte mémoire est correctement insérée dans la fente du serveur web et détectée par le serveur web.
ACTIVER	Permet d'activer une carte SD insérée dans le serveur web et actuellement non activée. Pour activer la carte mémoire, appuyer sur « ... ».
DÉSACTIVER	Permet de désactiver une carte SD insérée et activée dans le serveur web. Cette opération est nécessaire avant de retirer la carte SD du serveur Web sans avoir préalablement éteint le serveur web. Pour désactiver la carte mémoire, appuyer sur « ... ».

2.9 Date / heure

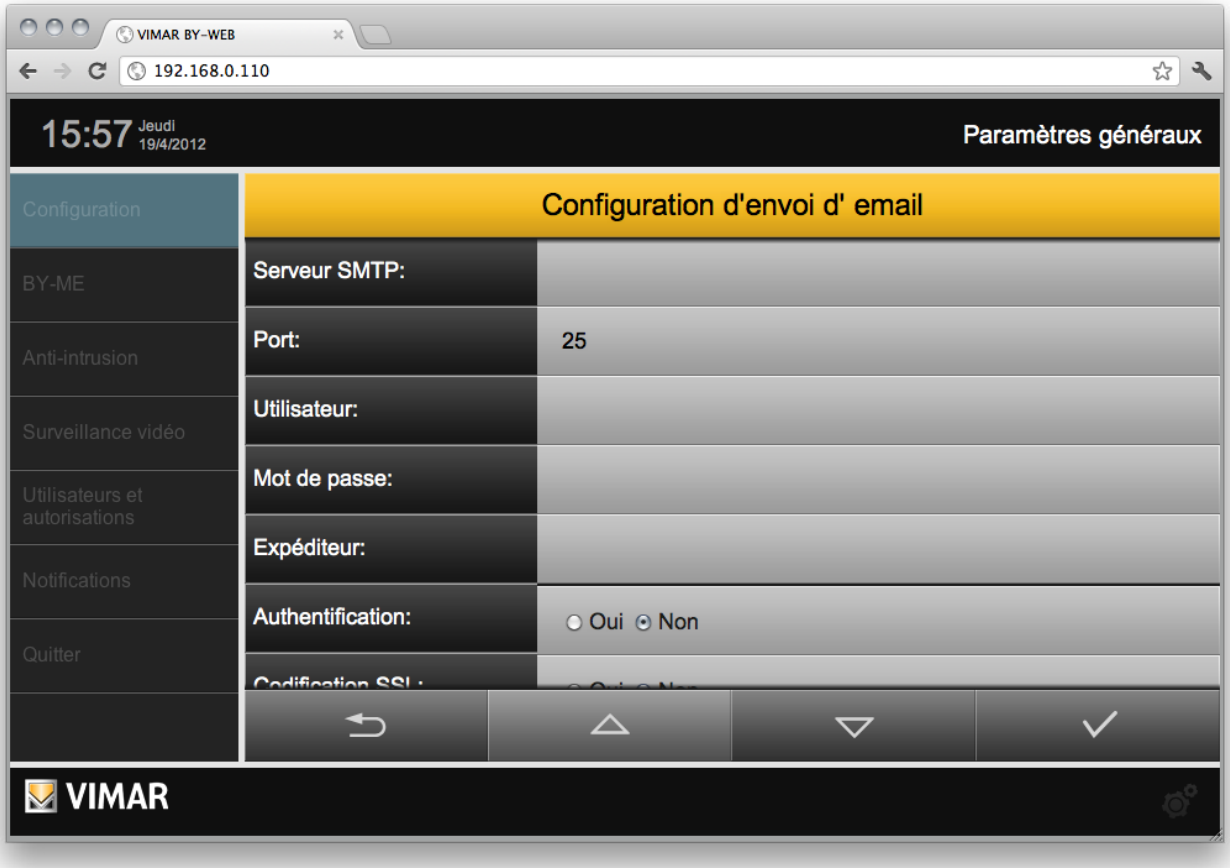
Cette page permet de configurer les paramètres du Web Server suivants relatifs à l'horloge du système :

HEURE	Cette fonction permet de configurer l'heure du système du Web Server.
DATE	Cette fonction permet de configurer la date du système du Web Server.
FUSEAU HORAIRE	Cette fonction permet de sélectionner le fuseau horaire du Pays ou de la région dans lequel/laquelle est installé le Web Server.

2.10 Email

Cette page permet de configurer les paramètres nécessaires à l'envoi des notifications des évènements d'alarme du Système anti-intrusion (SAI) par courrier électronique.

Attention : il est nécessaire que le système SAI soit correctement installé,fonctionnant et que la configuration du Web Server ait été correctement exécutée.



Plus particulièrement, la page permet de configurer les paramètres suivants (consulter le propre fournisseur de poste électronique pour connaître les valeurs à spécifier) :

SERVEUR SMTP	Adresse du serveur de poste électronique utilisé pour l'envoi de messages.
PORT	Port utilisé pour la connexion au serveur SMTP.
UTILISATEUR	Compte (généralement l'adresse email complète) avec lequel accéder au serveur SMTP.
MOT DE PASSE	Mot de passe avec lequel effectuer l'accès au serveur SMTP.
EXPÉDITEUR	Spécifier l'adresse email à utiliser en qualité d'expéditeur des messages, en cas de doute, saisir à nouveau l'adresse de poste électronique spécifiée en qualité d' « UTILISATEUR ».
AUTHENTIFICATION	Spécifier si le serveur SMTP nécessite une authentification.
CODIFICATION SSL	Préciser si le serveur SMTP nécessite ou non une codification SSL.

IMPORTANT : Le serveur Internet permet d'utiliser des serveurs SMTP qui prévoient un accès à travers un *Nom d'utilisateur* et un *Mot de Passe*. Pour utiliser le serveur SMTP Google Gmail, consultez le chapitre 14 « Utilisation du service SMTP de Google Gmail pour l'envoi des mails de notification du serveur Internet » de ce manuel.

2.11 DYNDNS

Cette page permet de configurer le client DNS dynamique intégré dans le Web Server ; cette fonction permet d'accéder au système domotique par internet même en absence d'une adresse IP publique statique. Pour cela, il est nécessaire d'effectuer les opérations préliminaires suivantes :

- Ouvrir une fenêtre du navigateur à l'adresse WWW.DYNDNS.ORG
- Créer un nouveau compte en suivant les indications fournies sur le site.
- Sur le panneau principal du propre compte à peine créer, sélectionner l'option « AJOUTER SERVICES HÔTE »
- Insérer le nom à attribuer au système et choisir une des extensions disponibles. Puis choisir « HÔTE AVEC ADRESSE IP » comme typologie.
- Insérer le nouveau service dans le panier et finaliser la création (gratuite) du domaine dynamique. Exemple : « nomdomaine » comme nom, « dyndns.org » comme extension.

Une fois cette opération terminée, paramétrer les paramètres suivants, dans la page de configuration de réseau du Web Server à la section consacrée au DNS dynamique :

NOM DE L'UTILISATEUR	L'utilisateur avec lequel le compte a été créé sur DYNDNS.ORG.
MOT DE PASSE	Mot de passe nécessaire pour accéder au propre compte DYNDNS.ORG.
NOM DU DOMAINE	Le nom attribué précédemment au propre domaine, avec son extension et sans indications de protocole, exemple : **nomdomaine.dyndns.org**

REMARQUE : le client DNS dynamique intégré avec le Web Server fonctionne uniquement avec les comptes créés sur le site WWW.DYNDNS.ORG

Une fois tous les paramètres de configuration saisis, enregistrer la configuration en appuyant sur la touche CONFIRMATION. En cas de modification de l'adresse IP du Web Server, celui-ci résultera dès lors disponible à la nouvelle adresse, en patientant le temps nécessaire pour de redémarrage des services de réseau.

De plus, si le client DNS dynamique a été configuré, une procédure automatique de mise à jour périodique du domaine avec la propre adresse IP publique sera exécutée.
A chaque fois que l'adresse IP sera modifiée par le fournisseur de service Internet, l'association entre le nom de domaine et l'adresse IP sera actualisée lors de la mise à jour successive permettant ainsi l'accès à distance (la mise à jour peut prendre plusieurs minutes).

2.12 ByWeb Tools

Cette page fournit la description de ByWeb Tools de Vimar ainsi que sa procédure d'installation. Cette même page est présentée par le Serveur Web, le cas échéant et automatiquement, en cas d'importation du fichier de projet By-me et en cas de visualisation de flux vidéo RTSP.

3. Configuration By-me

3.1 Activités préliminaires

Afin que le Web Server puisse gérer le système By-me, il est nécessaire d'effectuer des configurations impliquant le système By-me et le Web Server lui-même.

Pour terminer la configuration, IL EST NÉCESSAIRE d'utiliser le logiciel EasyTool Professional LT ou EasyTool Professional.

IMPORTANT : La procédure recommandée prévoit l'utilisation d'EasyTool Professional tant pour la configuration du système By-me que pour celle du Web Server, comme décrit ci-après.

3.1.1 Configuration du système avec Easytool Professional

La procédure prévoit les étapes suivantes :

- Configurer tous les dispositifs du système avec EasyTool Professional
- Configurer toutes les interfaces évoluées (Écran tactile, GSM…) en utilisant EasyTool Professional
- Configurer le Web Server en utilisant EasyTool Professional.

Remarque: La configuration du Web Server à l'intérieur d'EasyTool Professional, si nécessaire, procède à l'ouverture des routers du système By-me en mode automatique.

- Après avoir configuré l'intégralité du système, télécharger la base de données en Centrale.
- Après avoir configuré l'intégralité du système et toujours à l'aide d'EasyTool Professional, créer le fichier XML et l'importer dans le Web Server, en utilisant la section de configuration prévue à cet effet.

Attention: Lors de chaque nouvelle modification de la structure du système By-me, effectuée à l'aide d'EasyTool Professional, il est nécessaire de charger la nouvelle base de données dans la Centrale et de procéder à nouveau aux opérations de création du fichier XML avec importation de ce dernier dans le Web Server.

3.1.2 Configuration du système par le biais de la Centrale

La procédure prévoit les étapes suivantes :

- Configurer les dispositifs du système, incluant le Web Server en utilisant la centrale By-me.
- Effectuer l'opération d'Authentification si le système est équipé du système anti-intrusion

IMPORTANT: cette opération n'est pas nécessaire lorsque le Web Server est configuré avec EasyTool Professional

- Ouvrir les routers manuellement depuis la Centrale.
- Configurer la base de données de la Centrale à l'intérieur d'EasyTool Professional LT/EasyTool Professional
- Avec EasyTool Professional, LT/EasyTool Professional, créer le fichier XML et l'importer dans le Web Server.

Remarque: Lors de chaque nouvelle modification de la structure du système By-me, effectuée par le biais de la Centrale, il est nécessaire de charger la nouvelle base de données dans EasyTool Professional LT/EasyTool Professional et de procéder à nouveau aux opérations de création du fichier XML avec importation de ce dernier dans le Web Server. Si l'installateur ajoute de nouveaux groupes depuis la Centrale, il devra faire attention, le cas échéant, à ouvrir manuellement les routeurs.

3.2 Configuration

Une fois l'importation du projet XML terminée, il est nécessaire d'effectuer la procédure de « Configuration » du **Web Server** sur la Centrale ou sur EasyTool Professional, tout comme c'est le cas pour les autres dispositifs du système By-me (grâce à laquelle l'adresse physique est attribuée au Web Server).

Pour cela, procéder comme suit :

- Accéder à l'administration de **By-web**, sélectionner l'option «BY-ME» dans le menu principal puis « Configuration ».
- Un message pop-up s'affiche décrivant les opérations à effectuer depuis le **Web Server**.
- Une fois la configuration correctement effectuée, appuyer sur la touche de confirmation du message.

Durant l'ouverture du message pop-up, le **Web Server** est en mode de programmation. Éviter de configurer les autres dispositifs **By-me** car le **Web Server** pourrait répondre aux messages envoyés par la Centrale et empêcher le bon déroulement de ces opérations.

3.3 Importation d'un projet By-me

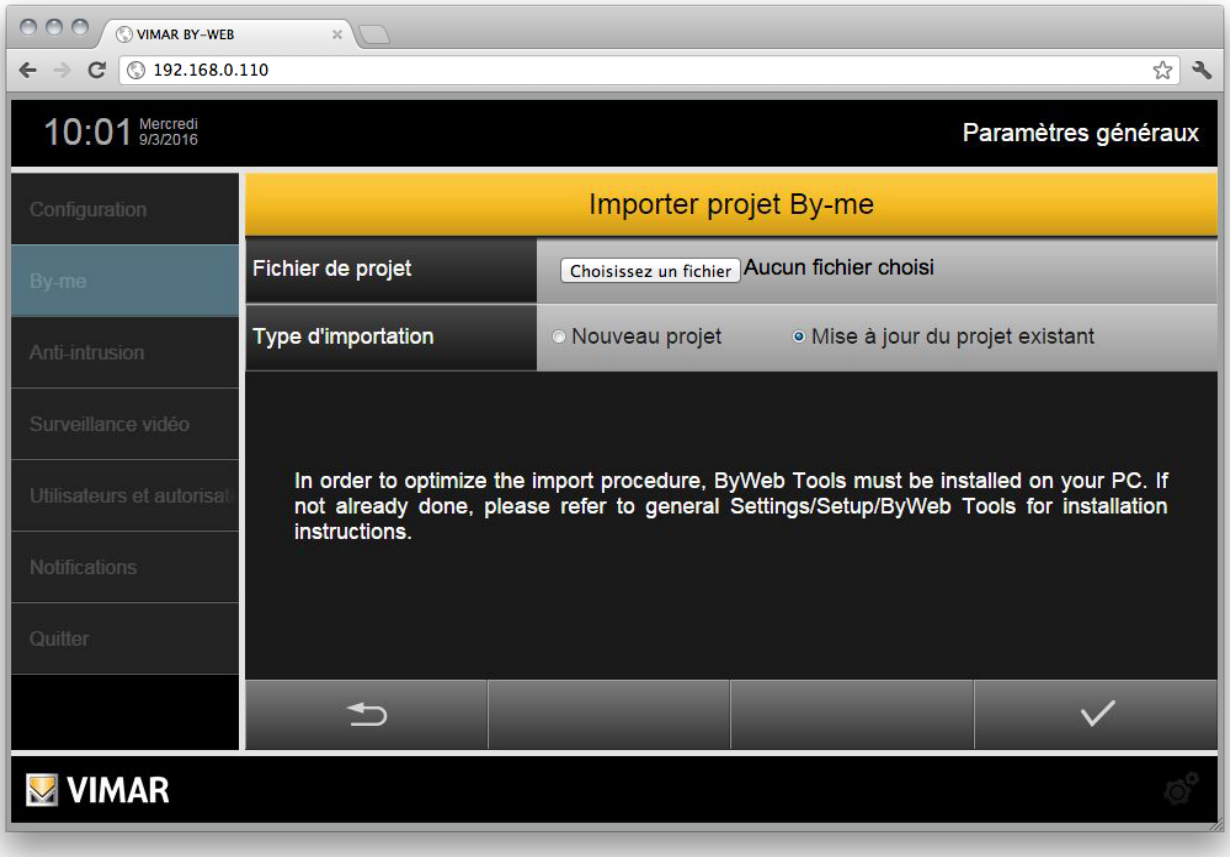
Accéder à la zone RÉGLAGES GÉNÉRAUX, sélectionner « By-me » depuis le menu principal et « Importer XML ».

Cette procédure permet de fournir les données du système By-me au Serveur Web.

Le Serveur Web, outre la procédure d'importation standard, prévoit une nouvelle procédure permettant de réduire les temps d'importation et impliquant l'utilisation de l'applet ByWeb Tools de Vimar.

Pour des informations sur l'installation de ByWeb Tools, voir le chapitre 12. ByWeb Tools de Vimar de ce manuel.

Si ByWeb Tools a déjà été installé, et que les conditions préalables sont remplies, le Serveur Web affichera la page illustrée ci-dessous. Dans le cas contraire, avant d'afficher cette page, une page contenant la description de ByWeb Tools s'affichera avec les instructions d'installation sur l'ordinateur à partir duquel l'importation est effectuée, avec la possibilité de démarrer l'installation de ByWeb Tools ou de procéder à l'importation selon la procédure standard.



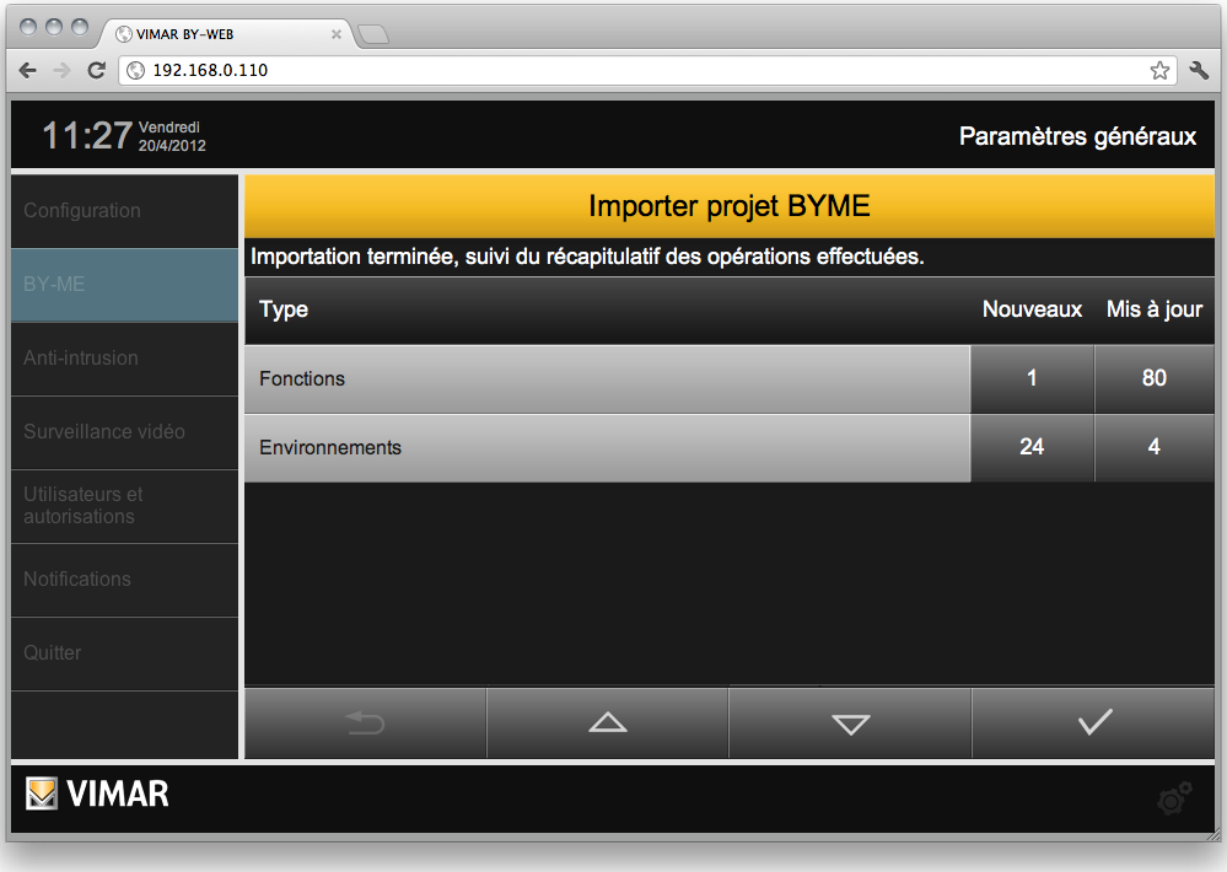
Cliquer sur la touche « Sélectionner fichier » ou « Parcourir » (en fonction du navigateur) et sélectionner sur l'ordinateur le fichier de projet XML précédemment exporté depuis EasyTool Professional LT/EasyTool Professional.

Dans le cas où un projet a déjà été importé précédemment dans le **Web Server**, il est nécessaire de spécifier si le nouveau fichier doit être considéré comme une mise à jour du précédent (dans ce cas, sélectionner « mise à jour du projet existant ») ou comme un nouveau projet. Dans ce dernier cas, tous les dispositifs **By-me** seront éliminés du **Web Server** avant de procéder à l'importation.

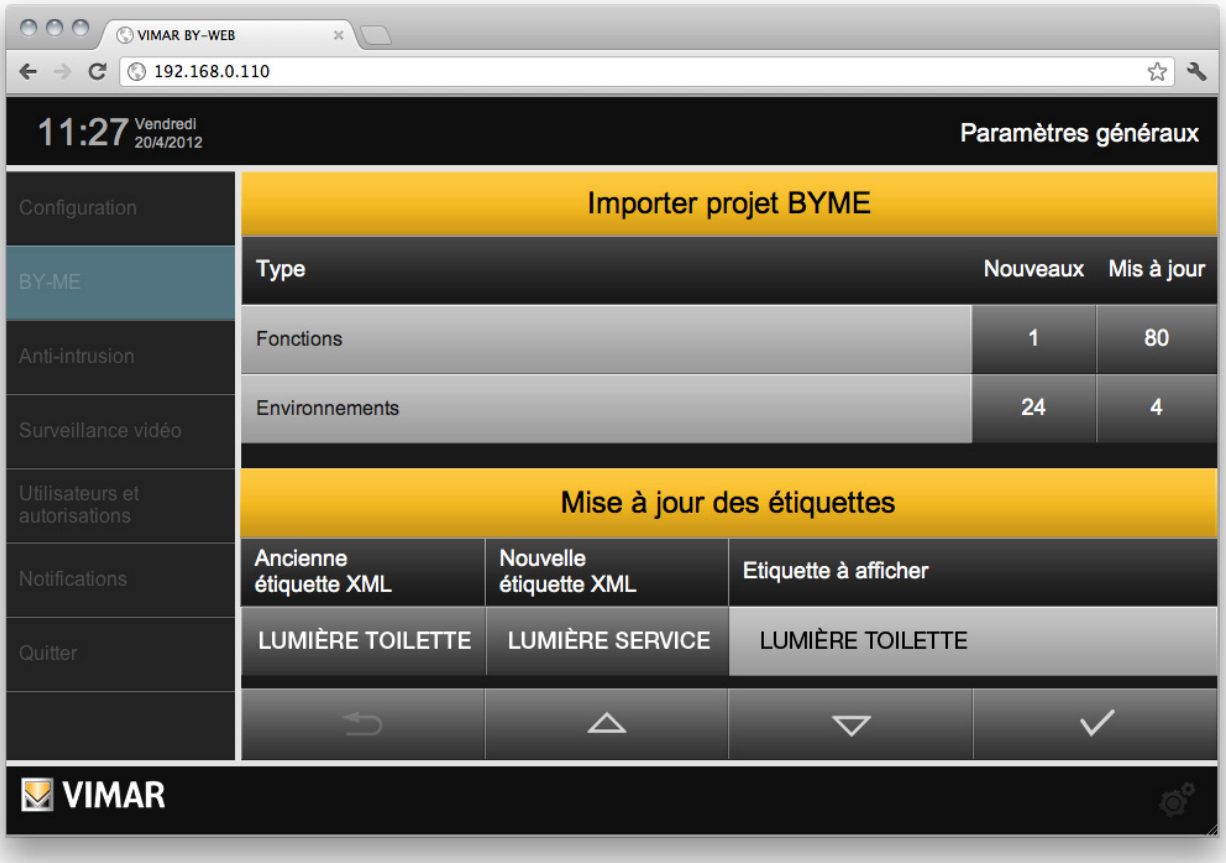
Une fois le type d'importation spécifié, cliquer sur la touche de confirmation en bas à droite et patienter jusqu'à la fin de la procédure.
L'opération peut prendre plusieurs minutes en fonction des dimensions du projet, durant lesquelles il est recommandé de n'effectuer aucune opération et de ne pas fermer la fenêtre du navigateur, sous peine de dysfonctionnement du **Web Server**.

Si le projet du système By-me prévoit l'utilisation de Master Group, le Serveur Web affichera une page permettant de choisir le représentant de visualisation de l'état de chaque Master Group.

Une fois la procédure terminée, un récapitulatif des opérations effectuées s'affiche sur l'écran :



En cas de mise à jour d'un projet existant, le Web Server détectera les éventuels dispositifs dont le nom a été modifié par rapport à la version précédente avec présentation d'une liste de ces différences, comme illustré dans la figure ci-dessous :



Il suffit de cliquer sur l'onglet Nouvelle ou Précédente pour le configurer automatiquement dans l'espace de droite, lequel sera le nom effectivement utilisé dans les pages du Web Server. Il est en outre possible de spécifier un onglet complètement personnalisé différent de celui présent dans le fichier XML.

Une fois cette opération terminée, confirmer le récapitulatif et les éventuelles modifications effectuées sur les noms en utilisant la touche de confirmation en bas à droite. Le Web Server est ainsi prédisposé pour la gestion du nouveau projet. Dans ce cas également, l'opération peut nécessiter plusieurs minutes durant lesquelles il est recommandé de n'effectuer aucune autre opération sur la page.

Une fois le processus terminé, l'utilisateur est automatiquement dirigé vers la page de gestion des environnements.

IMPORTANT : Ne pas importer les fichiers XML du système By-me simultanément sur plusieurs serveurs Internet à partir d'un même ordinateur.

3.4 Environnements

Si le projet XML importé contient des informations relatives à l'emplacement des dispositifs dans l'environnement, ces derniers seront automatiquement créés dans le Web Server. En sélectionnant l'option « Environnements » dans le menu « By-me » de la zone de configuration, il est possible de personnaliser la liste, définissant ainsi les pages graphiques dans lesquelles l'utilisateur pourra gérer les dispositifs du système domotique.

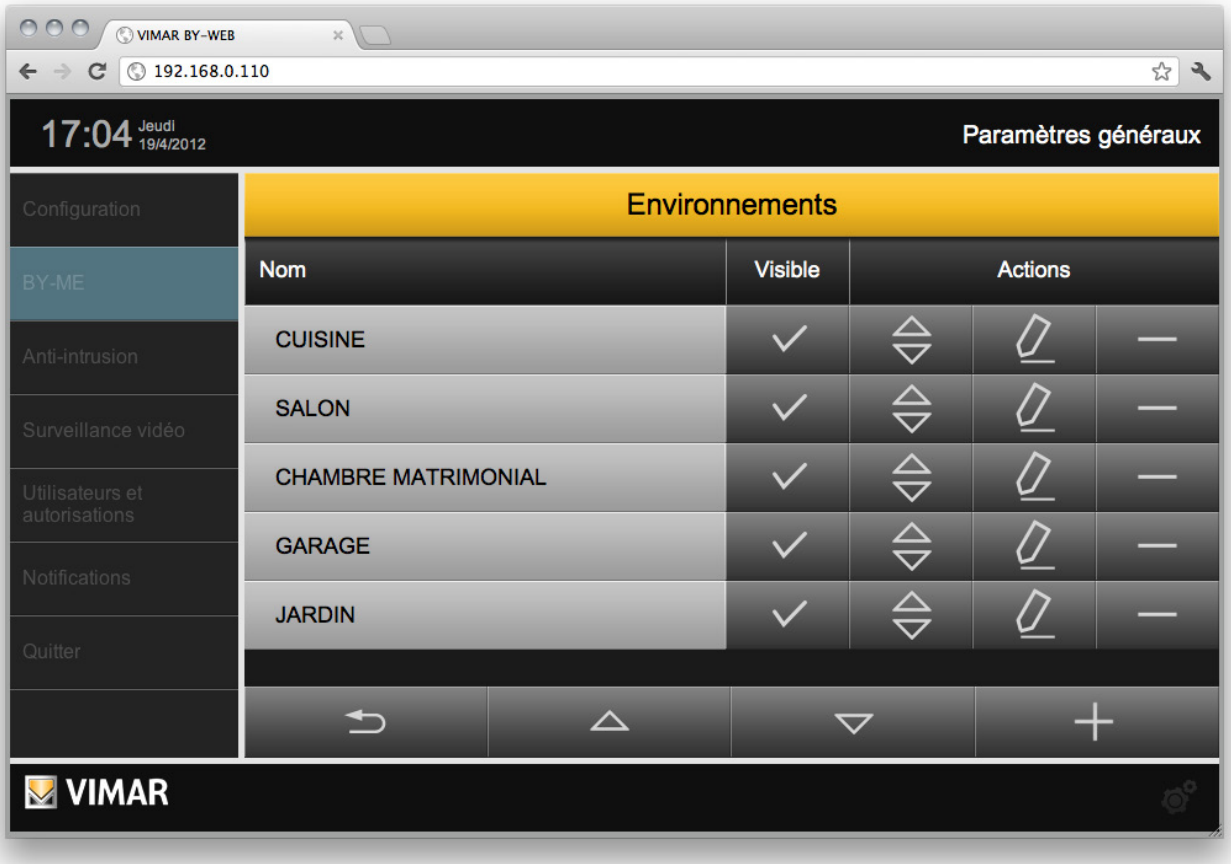
L'installateur peut modifier le nom des environnements existants directement depuis la page principale, mais également spécifier si ceux-ci doivent être visibles ou non par l'utilisateur final (en sélectionnant ou non la case correspondante).

La liste permet en outre d'effectuer les opérations suivantes sur chacun des éléments proposés :

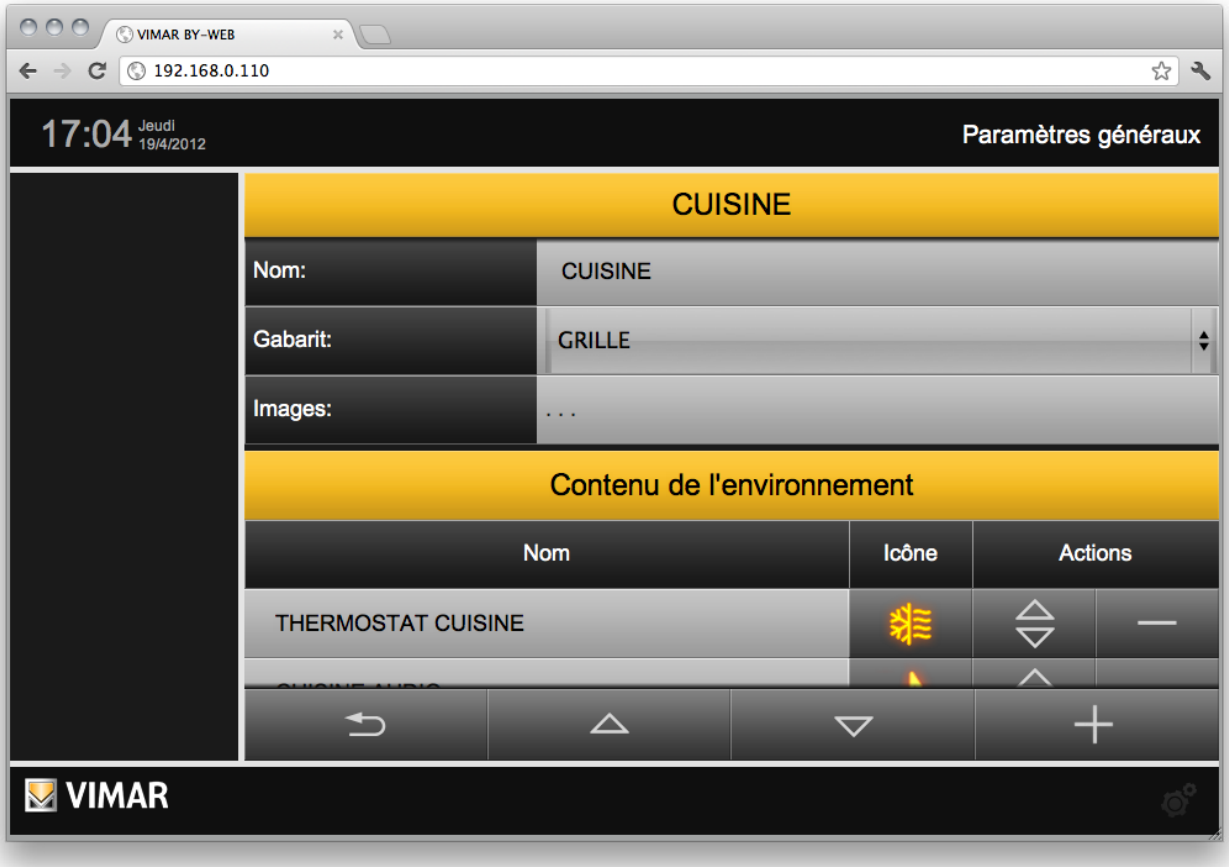
	MODIFICATION DE L'ORDRE En faisant glisser cette touche, il est possible de modifier l'ordre d'affichage des environnements dans le menu relatif du Web Server.
	MODIFIER Permet d'accéder à la fiche détaillée de l'environnement, comme mieux décrit ci-après.
	SUPPRIMER Éliminer l'environnement du Web Server. Cette opération, sur confirmation préalable de l'installateur, ne pourra plus être annulée. **Remarque** : les dispositifs éventuellement présents dans l'environnement ne seront pas supprimés mais simplement retirés de l'environnement éliminé. Ces derniers seront encore visibles dans les autres environnements les contenant, tout comme dans les pages de fonctions respectives.

REMARQUE : la modification des paramètres ci-dessus est effectuée en temps réel à chaque saisie du mot « ENTRÉE » (dans le cas de fenêtre de texte), à chaque changement de la sélection d'un menu déroulant ou en sélectionnant un autre point de la page après avoir modifié une valeur. L'utilisation de touche d'enregistrement ou de confirmation n'est pas nécessaire.

Il est également possible de créer de nouveaux environnements en utilisant la touche « AJOUTER » disponible sur le clavier inférieur. Les nouveaux environnements sont provisoirement insérés en bas de la liste, leur emplacement peut cependant être modifié en utilisant la touche « MODIFIER ORDRE ».



La touche « MODIFIER » permet d'accéder à la fiche détaillée de l'environnement :



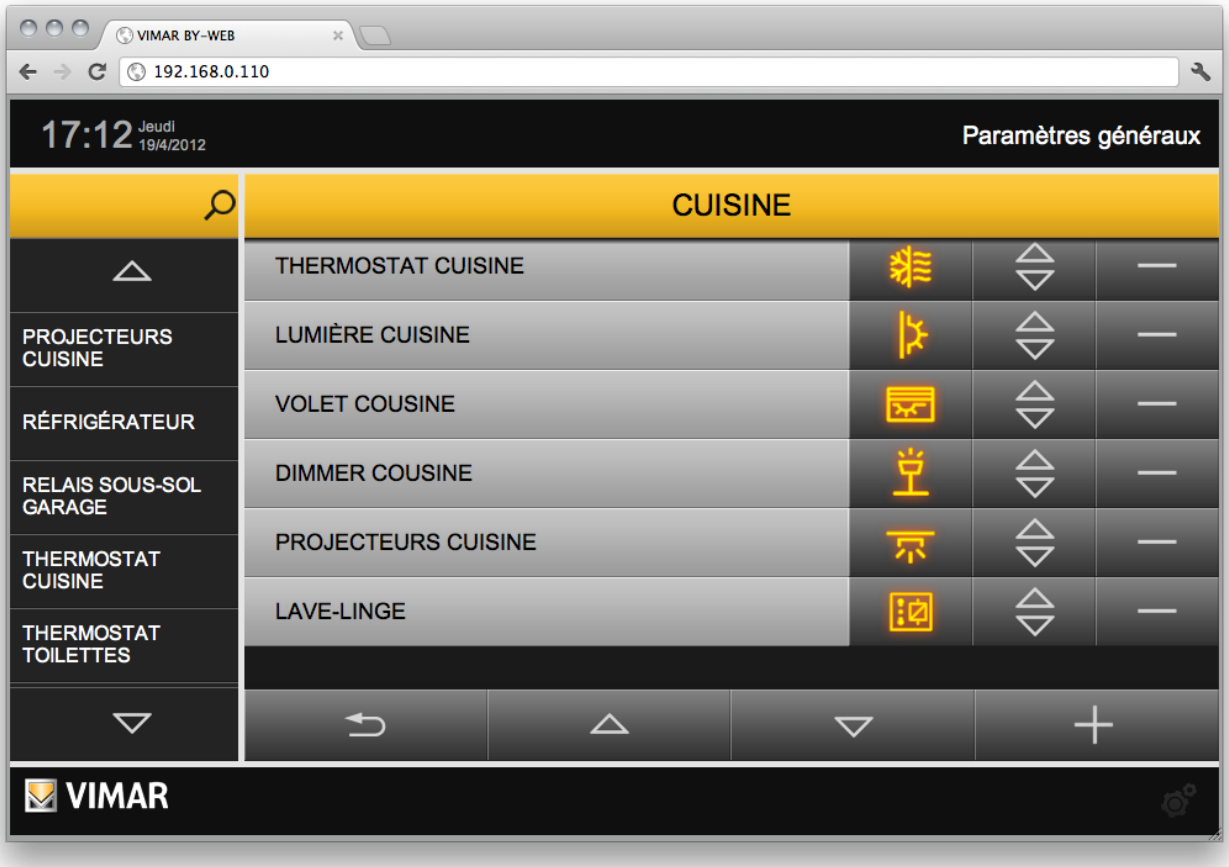
La première partie de cette page permet de :

- Configurer le nom de l'environnement qui sera utilisé dans le menu Environnements du Web Server.
- Visualiser la description associée à l'environnement, comme configurée dans le projet XML (pour des environnements créés durant l'importation).
- Spécifier si l'environnement pourra être visualisé par l'utilisateur sous forme de GRILLE (tableau contenant les dispositifs) ou sous forme de CARTE (dispositifs positionnés librement sur une image de fond).
- Associer une image à l'environnement, laquelle sera visualisée sur la partie latérale de la page de l'Environnement en cas d'affichage en GRILLE, ou utilisée comme fond en cas d'affichage en mode CARTE.

  En cliquant sur la touche de sélection de l'image, une fenêtre pop-up s'ouvrira, dans laquelle il sera possible de sélectionner une image déjà présente dans le Web Server, ou d'en charger une nouvelle (en utilisant la touche « AJOUTER ») en la sélectionnant dans le PC.

  IMPORTANT : Concernant les images de fond, ne pas charger d'image dont la largeur dépasse 800 pixels. Concernant les images en mode d'affichage GRILLE, les dimensions des images ne doivent pas dépasser 120 pixels x 425 pixels (largeur x hauteur)

- Valider la protection de la pièce par un code PIN et définir le code PIN correspondant. Par défaut, le paramètre « Accès avec PIN » est programmé sur « Non ». En configurant sur « Oui » le paramètre « Accès avec PIN », les champs de saisie et la confirmation du PIN (code numérique pouvant compter de 4 à 6 chiffres) s'affichent.



La seconde partie de la page (identifiée par le titre « CONTENU DE L'ENVIRONNEMENT ») permet en revanche de définir les dispositifs devant être visualisés dans la page de l'environnement prédéfini. Si l'environnement a été créé en phase d'importation du projet XML, la liste contiendra les éléments du projet associés à l'environnement courant, sinon la liste sera initialement vide.

De façon analogue à la procédure de la liste des environnements, décrite précédemment, la liste des dispositifs permet de :

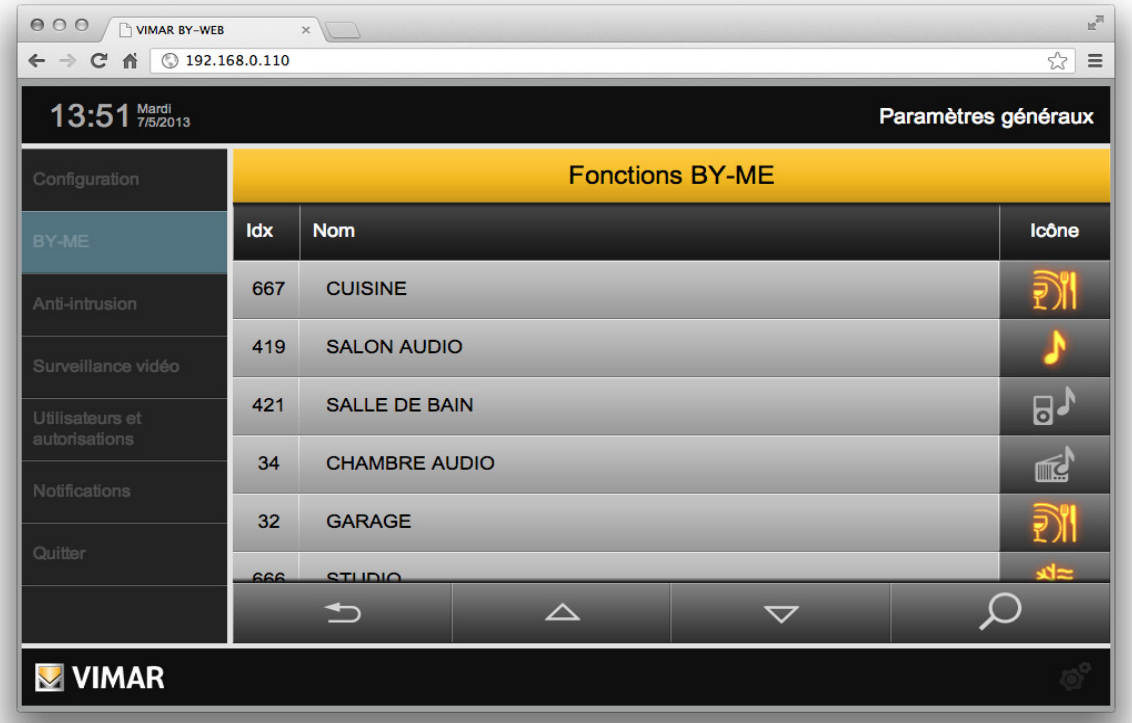
- Modifier le nom des dispositifs par rapport à celui attribué en phase d'importation du projet XML.
- Personnaliser l'icône d'identification du dispositif : en cliquant sur la touche contenant l'aperçu de l'icône actuelle, une fenêtre pop-up proposant les icônes disponibles s'affichera sur l'écran (la liste dépend du type de fonction choisie). En sélectionnant une image, celle-ci sera assignée au dispositif et le message pop-up sera automatiquement fermé.
- Modifier l'ordre du dispositif dans l'environnement, en le faisant glisser vers le haut ou le bas de la liste.

  Remarque : l'ordre n'a pas d'importance dans le cas d'un affichage de l'environnement en mode CARTE car la disposition de chaque dispositif sera définie lors d'une phase successive.
- Éliminer le dispositif de l'environnement en cours, sur confirmation.

La liste des dispositifs peut être consultée en utilisant les touches de défilement vertical disponibles sur le clavier situé dans la partie inférieure. En utilisant la touche « AJOUTER », il est en outre possible d'insérer d'autres dispositifs dans l'environnement en cours. En appuyant sur cette touche, un moteur de recherche s'affichera sur le côté de la page (dans l'espace normalement occupé par le menu principal), proposant une liste de tous les dispositifs présents dans le projet, filtrables en utilisant un ou plusieurs mots clé à insérer dans la case de texte initiale. Il suffit de faire glisser, un par un, les dispositifs à ajouter à l'environnement en cours, dans la position prédéfinie de la liste des dispositifs, pour créer la combinaison.
Pour quitter la page détaillée de l'environnement, appuyer sur la touche « RETOUR » disponible sur le clavier situé dans la partie inférieure de la page.

3.5 Fonctions BY-ME

En sélectionnant « Fonctions BY-ME » dans le sous-menu « BY-ME » du menu « Paramètres généraux », la liste de tous les périphériques (groupes) du système BY-ME s'affichera.



La liste des périphériques permet de:

- Modifier le nom des périphériques par rapport à celui défini durant le processus d'importation du projet XML: modifier directement le champ de texte.
- Personnaliser l'icône d'identification du périphérique: en cliquant sur la touche contenant l'aperçu de l'icône actuelle, une fenêtre pop-up proposant les icônes disponibles s'affichera sur l'écran (la liste dépend du type de fonction choisie). En sélectionnant une image, celle-ci sera assignée au dispositif et le message pop-up sera automatiquement fermé.
- Définir les paramètres spécifiques du dispositif ou de l'objet graphique correspondant sur le serveur Internet : pour certains dispositifs, la page qui s'ouvre en cliquant sur le bouton présentant l'icône du dispositif affiche des icônes qu'il est possible de choisir pour le dispositif et d'autres réglages, décrits aux chapitres suivants et qui concernent :
  - Configuration réinitialisation automatique des valeurs min/max de la station météo KNX.
  - Gestion personnalisée du comportement du widget du dispositif.

En utilisant la touche de Recherche/filtre située en bas à droite de la liste, il est possible d'afficher les périphériques dont le nom dispose de la chaîne désirée. Cette fonction est utile pour accélérer l'identification des périphériques spécifiques dans le cas où la liste des dispositifs est particulièrement.

ATTENTION: Seules les commandes à encastrer (art. 01480, 01481, 01482, 01485, 01486 et 01487) peuvent disposer d'une fonction de pression courte/longue qui permet de modifier la dynamique de l'actionneur tem¬porisé configuré dans le même groupe (de monostable temporisé à bistable ou l'inverse).

3.5.1 Configuration réinitialisation automatique des valeurs min/max de la station météo KNX

1. Accéder à la section "Configurations générales".
2. Sélectionner la rubrique "Fonctions By-me" du sous menu "By-me".
3. Identifier les lignes de la liste relative aux stations météo présents dans l'installation.

> **Note**: pour faciliter cette opération utiliser le bouton de Recherche/filtre présent dans la partie inférieure droite de la liste en utilisant, pour la recherche, une chaine de texte qui identifie les stations météo (ex. s'il y a deux stations météo: "Station météo 1" et "Station météo 2", pour la recherche utiliser le texte "météo" ou "Station météo")

4. Pour chaque station météo pour laquelle on souhaite modifier la configuration de la réinitialisation automatique des valeurs min/max suivre les étapes suivantes:
5. Appuyer sur l'icône correspondante à la station météo. Une fenêtre relative à la station météo apparait.
6. Pour activer la réinitialisation automatique des valeurs min/max de la température et maximum de la vitesse du vent, activer la rubreique "Activer réinitialisation périodique min/max" (Opération confirmée avec l'apparition d'un message d'avertissement qui rappelle que les valeurs min/max seront réinitialisées tous les jours à 0h00).

La procédure pour désactiver cette fonction se différencie de celle d'activation seulement avec le point 6) , où il faut désactiver la rubrique "Activer réinitialisation périodique min/max (L'opération de désactivation de la réinitialisation automatique est confirmée par l'apparition d'un message d'avertissement).

3.5.2 Gestion personnalisée du comportement du widget du dispositif

Certains dispositifs et certaines configurations permettent de modifier le comportement du widget du dispositif par rapport à la configuration prédéfinie sur le serveur Internet. Ceci permet de répondre à certaines exigences spécifiques de supervision des dispositifs du système By-me afin de pouvoir choisir comment doit se comporter le widget du dispositif quant à l'affichage de l'état du dispositif et à l'envoi de la commande au dispositif.

Pour définir ce réglage, sur les dispositifs et les configurations qui le prévoient, accéder à la page « Fonctions By-me » en appuyant sur l'icône du dispositif concerné : la partie inférieure de la page affiche la configuration « Gestion personnalisée ».

Le menu déroulant correspondant permet de définir le comportement du widget du dispositif en sélectionnant une des options possibles :

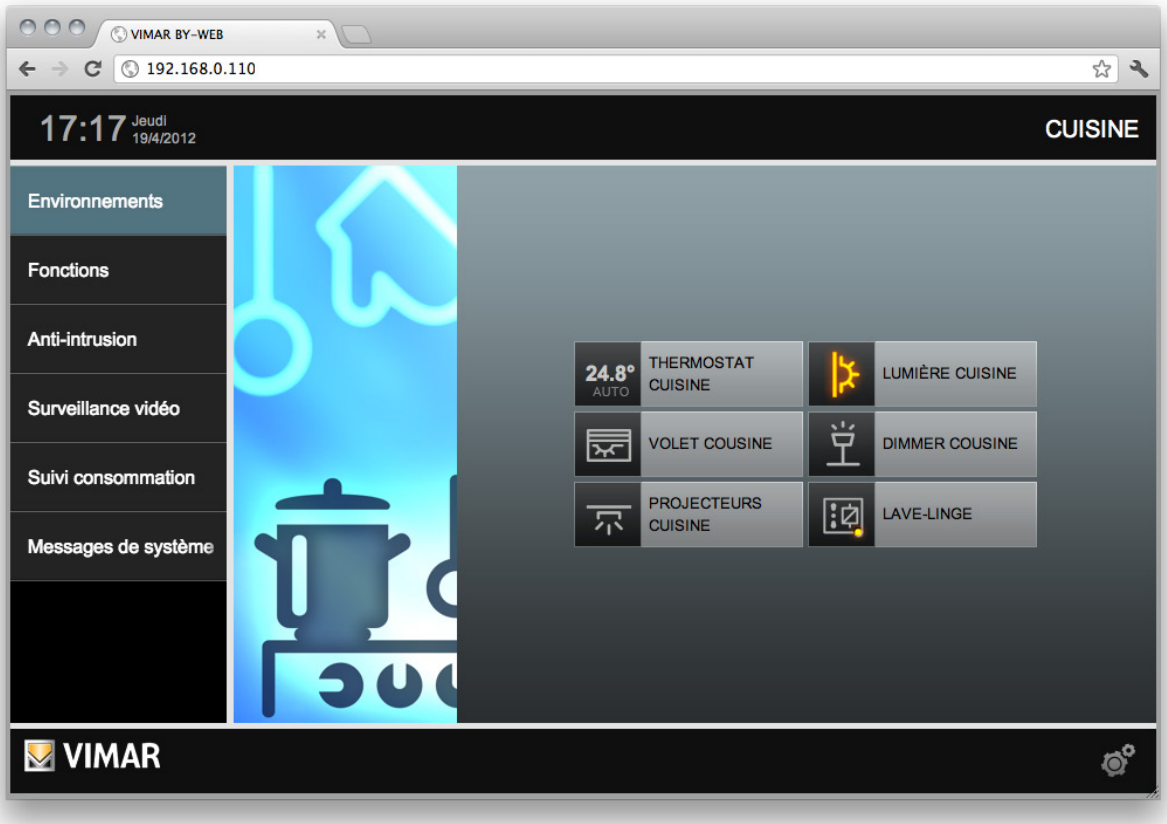
Rubriques du menu	Description
---	Aucun réglage personnalisé. Le widget se comportera tel qu'il a été défini sur le serveur Internet pour le dispositif concerné et selon la configuration du système.
État seulement	Le widget du dispositif permet uniquement d'afficher l'état mais ne permet pas d'envoyer la commande au dispositif.
Commande seulement	Le widget du dispositif permet uniquement d'envoyer la commande mais ne permet pas d'afficher l'état du dispositif.
État + Commande	Le widget du dispositif permet d'afficher l'état et d'envoyer la commande au dispositif.

3.6 Navigation par environnements

Une fois la personnalisation des environnements terminée, le Web Server peut être utilisé pour la supervision du système By-me, mais également pour les fonctions relatives à l'automation et à la diffusion sonore. Avec la touche « QUITTER » dans menu principal de l'espace de configuration, il est possible de revenir à la page-écran initiale.

Dans le menu principal, toujours disponible dans la partie gauche de la page, l'utilisateur final a la possibilité de naviguer à l'intérieur des environnements précédemment configurés dans l'option « ENVIRONNEMENTS ». En appuyant sur cette touche, un sous-menu contenant la liste des environnements disponibles s'ouvrira. Si le nombre d'environnements dépasse la hauteur maximum disponible sur la page, deux touches de défilement vertical seront alors proposées.

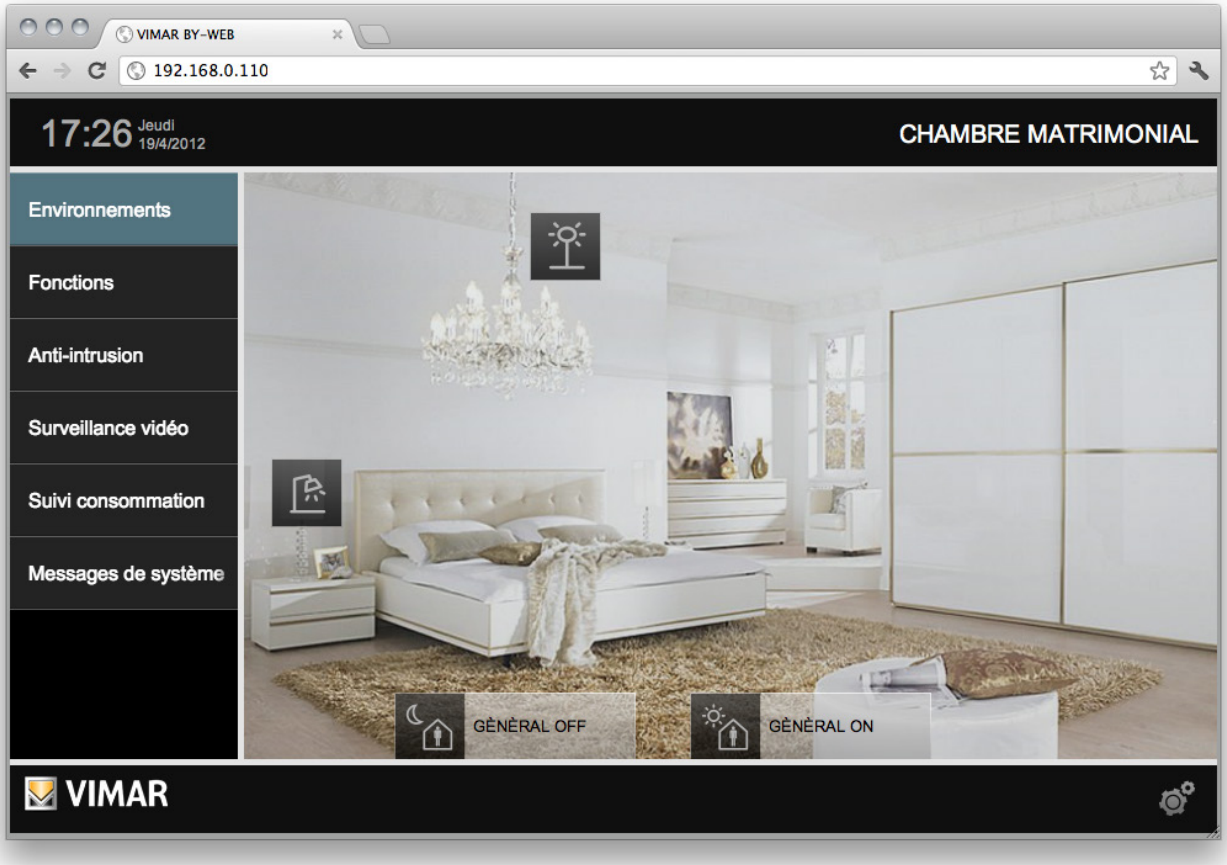
En sélectionnant un environnement dans la liste, son contenu sera chargé dans la partie principale de la page. En cas d'affichage en mode GRILLE, les dispositifs associés à l'environnement seront présentés dans un tableau, chacun d'eux caractérisés par une touche composée d'une icône, représentant le statut actuel du dispositif et par le nom identifiant. Les dispositifs seront automatiquement disposés dans la zone utile en fonction de l'ordre précédemment configuré. Si le nombre de dispositifs dépasse le nombre admissible de la zone utile de la page, ces derniers seront répartis sur plusieurs pages, et il sera possible d'y accéder en utilisant les touches de défilement proposées dans la partie inférieure de la page-écran.



Configuration By-me

En cas d'affichage en mode CARTE, l'environnement sera proposé initialement avec toutes les icônes, représentatives des fonctions domotiques associées à l'environnement, superposées en haut à gauche, ceci car les dispositifs nécessitent encore d'être positionnés sur la page. Pour ce faire, sélectionner l'option « PERSONNALISER PAGE » dans le menu contextuel activable en utilisant la touche en bas à droite de la page-écran. Puis, à l'aide de la souris, faire glisser ces touches dans la position désirée pour composer un affichage optimal pour l'utilisateur.

Si la protection via PIN (code numérique) est validée pour la pièce sélectionnée, une fenêtre permettant de saisir le code numérique PIN s'affiche. Pour afficher la page de la pièce, saisir le code PIN et appuyer sur OK. Si le code PIN est incorrect, un message signalant que le PIN n'est pas valide s'affiche.



En cliquant sur les icones, la partie de la touche contenant le nom s'affichera en alternance. S'il est choisi de la masquer en permanence, le nom du dispositif ne sera plus visible par l'utilisateur final, sauf durant les opérations de commande sur le dispositif.

Durant la phase de personnalisation de la page, le menu principal est remplacé par une liste complète des dispositifs appartenant à l'environnement. Cette liste permet de modifier directement le nom des dispositifs (la modification sera immédiatement visible sur les touches présentes sur la page, à chaque pression de la touche ENTRÉE ou en cas de sélection d'un autre élément de la page).

Une fois la personnalisation de la page terminée, il sera nécessaire d'enregistrer les modifications de façon permanente. Pour cela, utiliser la touche de CONFIRMATION située dans la partie inférieure de la page. À l'inverse, s'il est souhaité quitter la page sans enregistrer les modifications, appuyer sur la touche RETOUR : la page reviendra à son statut d'affichage précédent, sur demande de confirmation.

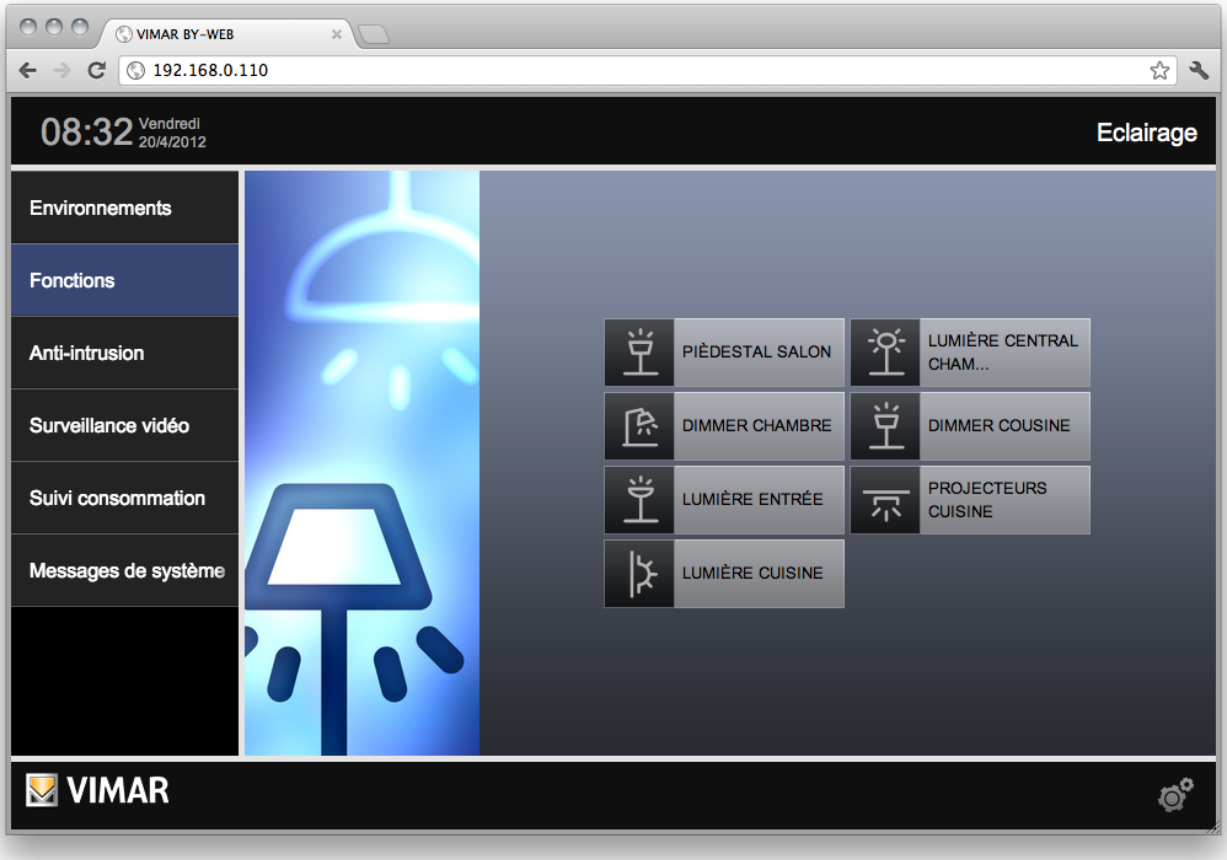
Pour plus de détails sur la gestion des différentes typologies de dispositif, consulter le MANUEL DE L'UTILISATEUR.

3.7 Navigation par fonctions

Comme précédemment expliqué pour les environnements, il est possible de visualiser et de gérer les dispositifs du système By-me en naviguant dans le Web Server par fonctions, en utilisant l'option spécifique du menu principal. Dans ce cas les dispositifs seront proposés uniquement avec un affichage en mode GRILLE, avec subdivisions conformément aux typologies suivantes :

LUMIÈRES	Lumières, gradateur, relais de façon général.
STORES	Stores (avec et sans gestion des lamelles), ouvertures et automations.
CLIMAT	Thermostats (avec ou sans gestion des évaporateurs à ventilation forcée).
SCÉNARIOS	Scénarios configurés en Centrale By-me.
AUDIO	Diffusion sonore.
PROGRAMMES DES ÉVÈNEMENTS	Programmes des évènements configurés en Centrale By-me.

Pour plus de détails sur la gestion des différentes typologies de dispositif, consulter le MANUEL DE L'UTILISATEUR.



REMARQUE : À la différence de la procédure par environnements, les images représentatives des différentes fonctions, visualisées à côté de la liste des dispositifs, ne peuvent être personnalisées.

IMPORTANT : Si un élément est présent UNIQUEMENT dans des pièces que l'usager ne peut pas voir, ce même élément n'apparaîtra pas non plus sur la page des fonctions. Si un élément est présent dans une pièce protégée par un PIN, il ne sera pas visible sur la page des fonctions.
Si un élément est présent dans plusieurs pièces, certaines étant protégées par un PIN et d'autres pas, l'élément résultera visible UNIQUEMENT dans les pièces protégées par un PIN.

4. Configuration anti-intrusion

4.1 Le système anti-intrusion By-alarm

4.1.1 Introduction

Pour intégrer le système By-alarm au système d'automatisation By-me, il doit y avoir un serveur Internet 01945/01946 dans le système By-me, avec une version logicielle 1.19 ou suivante et une centrale By-alarm (art. 01700 ou art. 01703) avec une interface réseau Ethernet (art. 01712).

NOTE: pour faciliter la présentation, les chapitres suivants se réfèrent aux paramètres de réseau (adresse IP, port IP) de la centrale By-alarm et notamment aux paramètres réseau de l'interface Ethernet (art. 01712) de la centrale By-alarm.

Le serveur Internet et la centrale By-alarm doivent être intégrés au même réseau LAN.

Si le système By-me ne comporte pas de système anti-intrusion By-me (aucun groupe configuré dans l'application anti-intrusion sur la centrale By-me ni dans la gestion des alarmes techniques), le serveur Internet affiche le menu de configuration du système anti-intrusion By-alarm qui sera décrit dans les paragraphes suivants, auquel on accède par l'onglet Anti-intrusion dans la page Paramètres généraux et qui comporte les options suivantes.

- Importation XML
- Configuration
- Évènements By-me
- Bridge By-alarm Manager

NOTE: pour configurer la centrale By-alarm, se référer à la centrale By-alarm (art. 01700, art. 01703).

4.1.2 Importation XML

Le serveur Internet 01945/01946 acquiert les informations du système By-alarm grâce au fichier XML généré par le logiciel By-alarm Manager qui contient les informations sur la configuration de la centrale By-alarm (art. 01700, art. 01703).
Se référer à la documentation du système By-alarm pour générer le fichier XML.
La page Importation configuration By-alarm, accessible par l'onglet Importation XML, comporte les deux options suivantes :

- Fichiers de configuration : appuyer sur Sélectionner le fichier puis sélectionner le fichier XML généré par le logiciel By-alarm Manager.
- Type d'importation

  Sélectionner l'option Nouveau projet avant d'importer le fichier XML, le serveur Internet efface toutes les données de configuration du système By-alarm.

  Si on sélectionne l'option Mise à jour du projet existant, le serveur Internet importe le fichier XML, conserve les parties qui n'ont pas été modifiées lors de la précédente importation et modifie uniquement les autres.

  Pour exécuter l'importation, appuyer sur le bouton de validation, pour annuler l'importation, appuyer sur le bouton Retour.

NOTE: l'importation peut durer quelques minutes selon la dimension du système By-alarm.

4.1.3 Configuration

La page Configuration centrale By-alarm contient les paramètres qui permettent au serveur Internet d'accéder à la centrale By-alarm avec les options suivantes.

- **Adresse IP** : adresse IP de la centrale By-alarm Adresse IP utilisée par le serveur Internet pour communiquer avec la centrale By-alarm.

  Cette donnée est configurée automatiquement pendant l'importation automatique du fichier XML de l'installation By-alarm mais peut aussi être gérée dans la page du serveur Internet.
- **Port TCP By-me** : port IP de communication de la centrale By-alarm (elle doit correspondre à la configuration exécutée sur la centrale By-alarm). Port utilisé par le serveur Internet pour communiquer avec la centrale By-alarm.

  Cette donnée est configurée automatiquement pendant l'importation automatique du fichier XML de l'installation By-alarm mais peut aussi être gérée dans la page du serveur Internet.
- **Port TCP By-alarm** : port IP de communication de la centrale By-alarm permettant de gérer la fonction bridge pour l'accès à distance/LAN à la centrale By-alarm avec le logiciel By-alarm Manager (il doit correspondre à la configuration exécutée sur la centrale By-alarm).

  Cette donnée est configurée automatiquement pendant l'importation automatique du fichier XML de l'installation By-alarm mais peut aussi être gérée dans la page du serveur Internet.
- **PIN système** : code PIN permettant l'authentification de l'accès du serveur Internet à la centrale By-alarm (6 caractères numériques).

  Pour exécuter l'importation, appuyer sur le bouton de validation, pour annuler l'importation, appuyer sur le bouton Retour.

4.1.4 Évènements By-me

Grâce au serveur Internet, les commandes de l'installation d'automatisation By-me peuvent être exécutées en fonction des évènements générés par le système By-alarm.

Les commandes à exécuter sont les suivantes.
- Commandes des actionneurs (ON/OFF)
- Activation des scénarios
- Envoi de la commande de Protection/Rétablissement de l'état précédent pour les thermostats du système By-me équipés.

Les évènements du système By-alarm qui peuvent être utilisés dans ce but sont les suivants.
- Passage des découpages à un état déterminé.
- Passage des zones à un état déterminé.
- Envoi d'une Commande By-me par la centrale By-alarm dirigée vers le système By-me. Une configuration spéciale de la centrale By-alarm permet d'associer l'envoi d'une commande By-me à la pression d'un bouton de radiocommande du système By-alarm. Il est possible de configurer jusqu'à 32 commandes By-me différentes.

Pour la configuration des évènements, entrer dans la page Paramètres généraux/Anti-intrusion/Évènements By-me qui se présente comme une liste divisée en trois parties.
- **Découpages By-alarm** : cette page présente les découpages configurés dans le système By-alarm auxquels il est possible d'associer des commandes By-me.
- **Découpages By-alarm** : cette page présente les découpages configurés dans le système By-alarm auxquels il est possible d'associer les commandes By-me.
- **Commandes By-me** : cette page contient les 32 éléments du type Commandes By-me configurés dans le système By-alarm auxquels il est possible d'associer les commandes By-me.

Priorité de l'état des découpages et des zones pour la gestion des évènements By-me
(fonction valide uniquement pour les versions du serveur web allant de la 1.19 à la 1.26 comprises)

IMPORTANT : la gestion avec priorité des états des secteurs et des zones du système By-alarm de la part du serveur web est valable pour les versions du serveur web allant de la 1.19 à la 1.26 comprises : pour les versions du serveur web 1.27 et suivantes, la gestion des états des secteurs et des zones permet d'utiliser indépendamment les états possibles prévus par le système By-alarm.
Un découpage ou une zone peut présenter au même moment plusieurs états.
Exemple : une zone du système By-alarm peut être en même temps ouverte et en alarme. Cette situation peut se présenter à l'ouverture d'une zone quand le découpage auquel elle appartient est activé. La gestion des évènements By-me basée sur l'état des découpages et des zones du système By-alarm suit les priorités d'état décrites dans les tableaux suivants.
Au moment du changement d'état d'un découpage ou d'une zone définissant un évènement By-me, le serveur Internet gère la situation en priorité.

NOTE: certains états peuvent s'exclure, ils ont donc été regroupés dans un même niveau de priorité. Par exemple, une zone ne peut prendre qu'un seul état d'activation (OFF, ON, INT, PAR), ces états ont donc la même priorité.

Plus l'index numérique est haut plus la priorité est élevée.

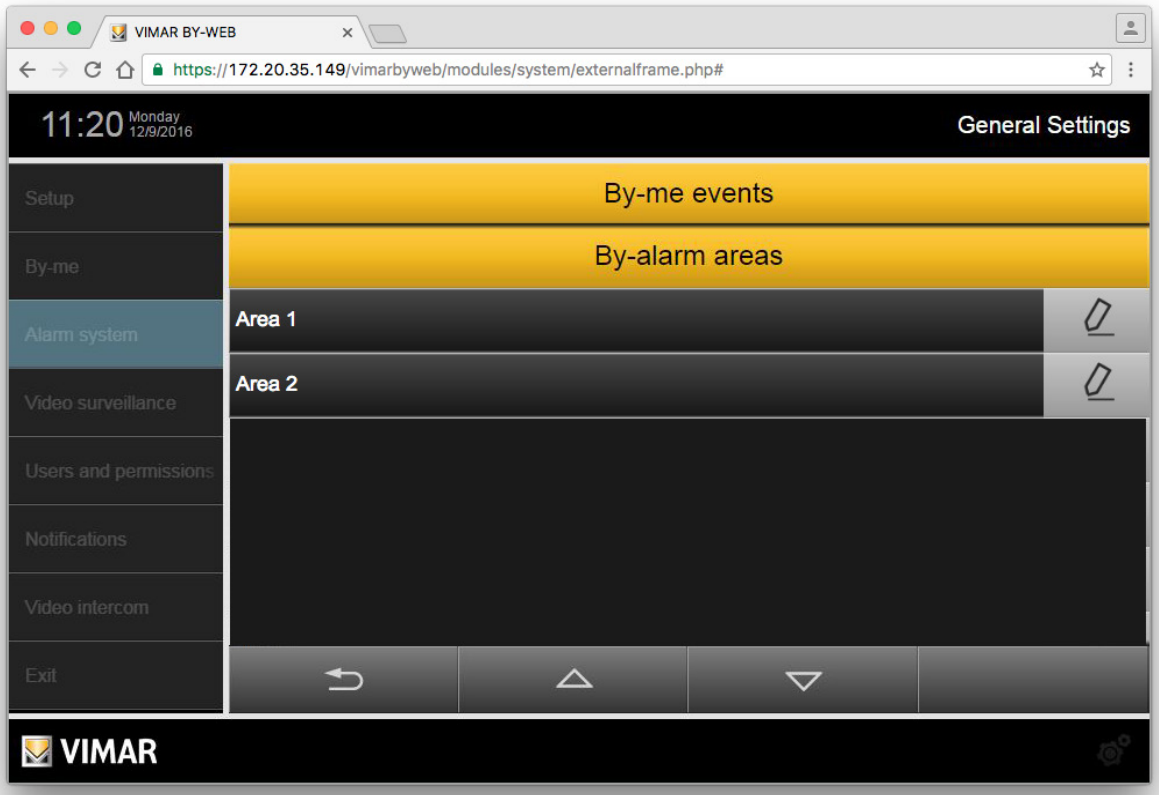
Priorité liée à l'état du découpage	Description de l'état
1	OFF
	ON
	INT
	PAR
2	Mémoire alarmes
3	Alarme

Priorité liée à l'état de la zone	Description de l'état
1	Fermée
	Ouverte
2	Masquée
3	Mémoire alarmes
4	Alarme
5	Modifiée
6	Exclue

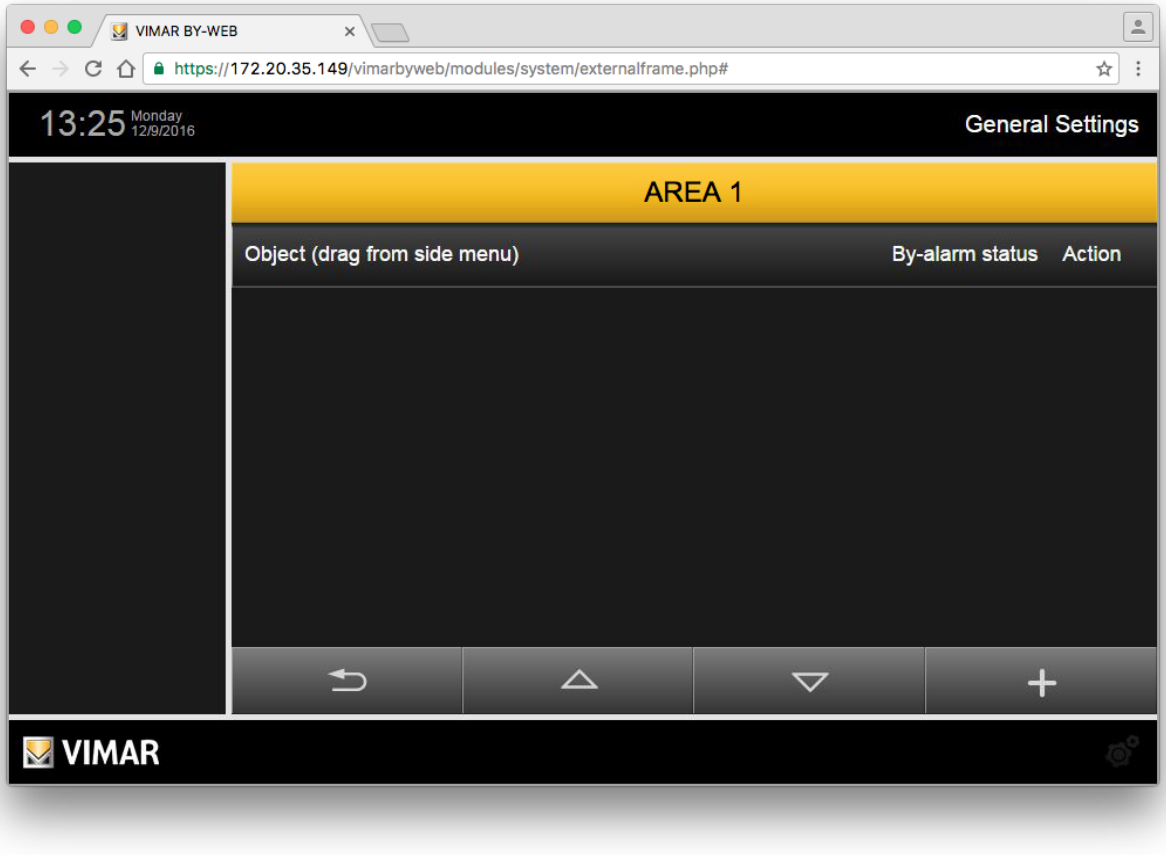
Exemple 1 : si une zone qui appartient à un découpage actif est ouverte, elle est en même temps en état ouvert (priorité 1) et en alarme (priorité 4) dans le système By-alarm. Si deux évènements By-me ont été créés et associés aux états d'ouverture et d'alarme de cette zone, le serveur Internet exécute les commandes prévues pour l'état qui a la priorité la plus élevée, c'est-à-dire pour l'état d'alarme de la zone (priorité 4 par rapport à la priorité 1 de l'état d'ouverture).

Exemple 2 : si on crée un évènement associé à l'état OFF d'un découpage qui est désactivé (OFF) suite à une alarme, l'évènement créé n'est pas géré parce que le découpage est passé simultanément de l'état OFF à l'état mémoire alarme qui a la priorité sur l'état OFF. L'évènement créé est géré quand la zone est OFF sans état d'alarme.

4.1.4.1 Évènements By-me associés à l'état d'alarme des découpages By-alarm



Quand on appuie sur le bouton de modification situé à gauche de chaque ligne, on accède à la page des évènements du découpage sélectionné.
Initialement, la page ne présente aucun évènement.


VIMAR BY-WEB
https://172.20.35.149/vimarbyweb/modules/system/externalframe.php#
13:25 Monday 12/9/2016
General Settings
AREA 1
Object (drag from side menu)
By-alarm status
Action
VIMAR

Configuration anti-intrusion

Les opérations qui peuvent être exécutées dans la page des évènements associés à un découpage spécifique sont les suivants et sont décrits dans les paragraphes ci-dessous.

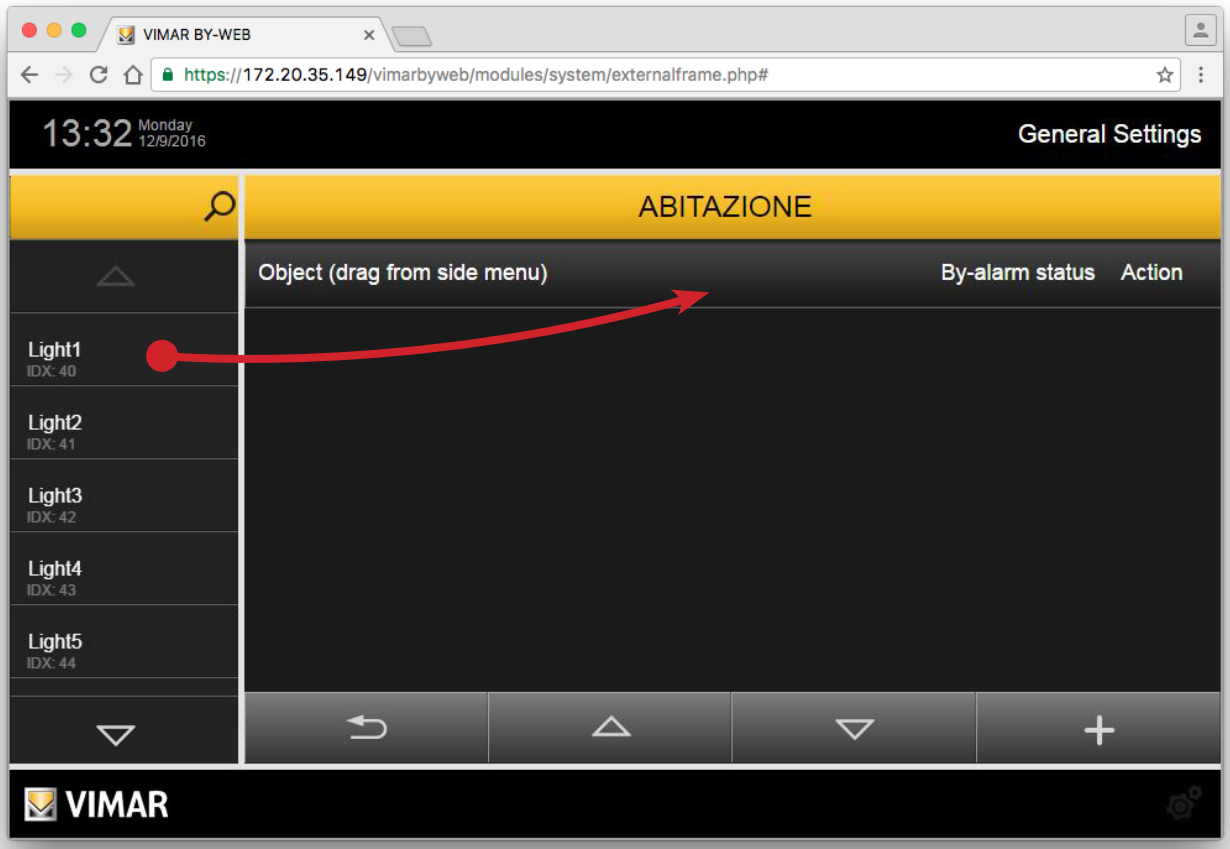
- Création d'un évènement
- Affichage de la configuration des évènements préalablement créés
- Modification d'un évènement préalablement créé
- Suppression d'un évènement préalablement créé

Création d'un évènement

Pour ajouter un évènement associé un découpage du système By-alarm, procéder de la façon suivante.

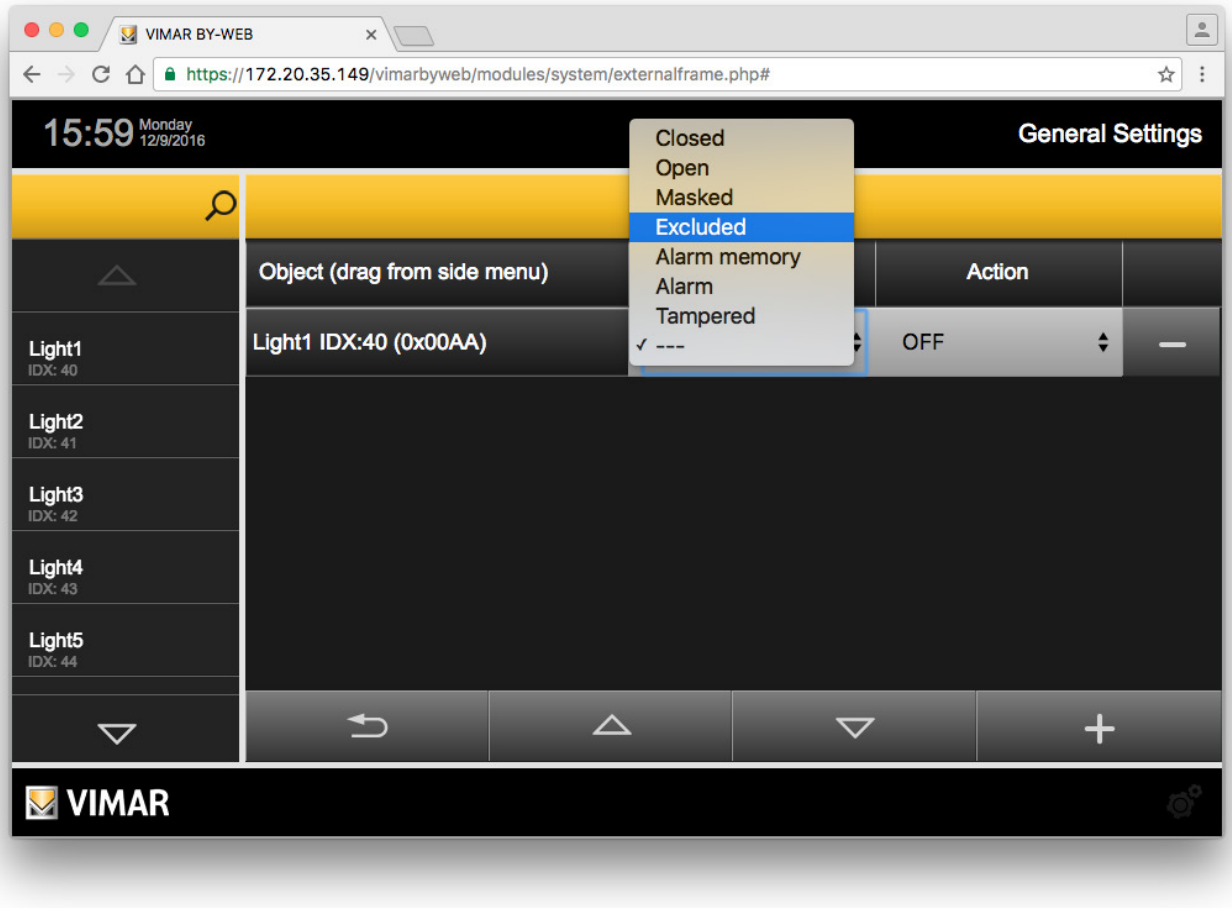
1. Appuyer sur le bouton + en bas et à droite de la page pour ajouter un évènement à la liste.
2. La colonne de gauche affiche la liste des dispositifs qui peuvent être commandés par le serveur Internet après un évènement du système By-alarm.

   Cliquer-glisser l'objet de la liste dans la colonne latérale sur la barre grise Objet, en haut de la fenêtre (cliquer-glisser depuis le menu latéral). Si l'objet est déplacé par cliquer-glisser dans une autre zone de la fenêtre, l'évènement n'est pas créé.



3. Une ligne est créée pour représenter l'évènement, son nom qui n'est pas modifiable coïncide avec la description de l'objet commandé. Avant de devenir opérationnel, l'évènement doit être configuré en suivant les indications ci-dessous.
   Appuyer sur le bouton dans la colonne État By-alarm pour sélectionner l'état du découpage qui déclenche l'envoi de la commande By-me. Sélectionner --- pour ne pas associer d'évènement (dans ce cas, la gestion de l'évènement spécifique est inhibée).
   Appuyer sur le bouton de la colonne Action pour sélectionner la valeur de la commande qui doit être déclenchée par l'évènement By-alarm sélectionné.

   NOTE: les modifications décrites ne nécessitent pas de confirmation et sont enregistrées par le serveur Internet automatiquement.



4. Appuyer sur le bouton Retour pour sortir de la page ou pour répéter les opérations préalablement décrites à partir du point 1 et ajouter des dispositifs commandés à associer au même évènement.

Affichage de la configuration des évènements préalablement créés.

La page des évènements associés au découpage contient la liste de tous les évènements configurés.

Chaque ligne de la liste représente un évènement et donne les informations suivantes.

- Objet : nom permettant d'identifier l'objet à commander (actionneur ON/OFF, thermostat ou scénario)
- État de la zone du système By-alarm à laquelle la commande de l'objet By-me doit être associée
- Action : commande à envoyer à l'objet

Modification d'un évènement préalablement créé

Pour modifier la configuration d'un évènement, trouver la ligne correspondante dans la liste et modifier les paramètres.

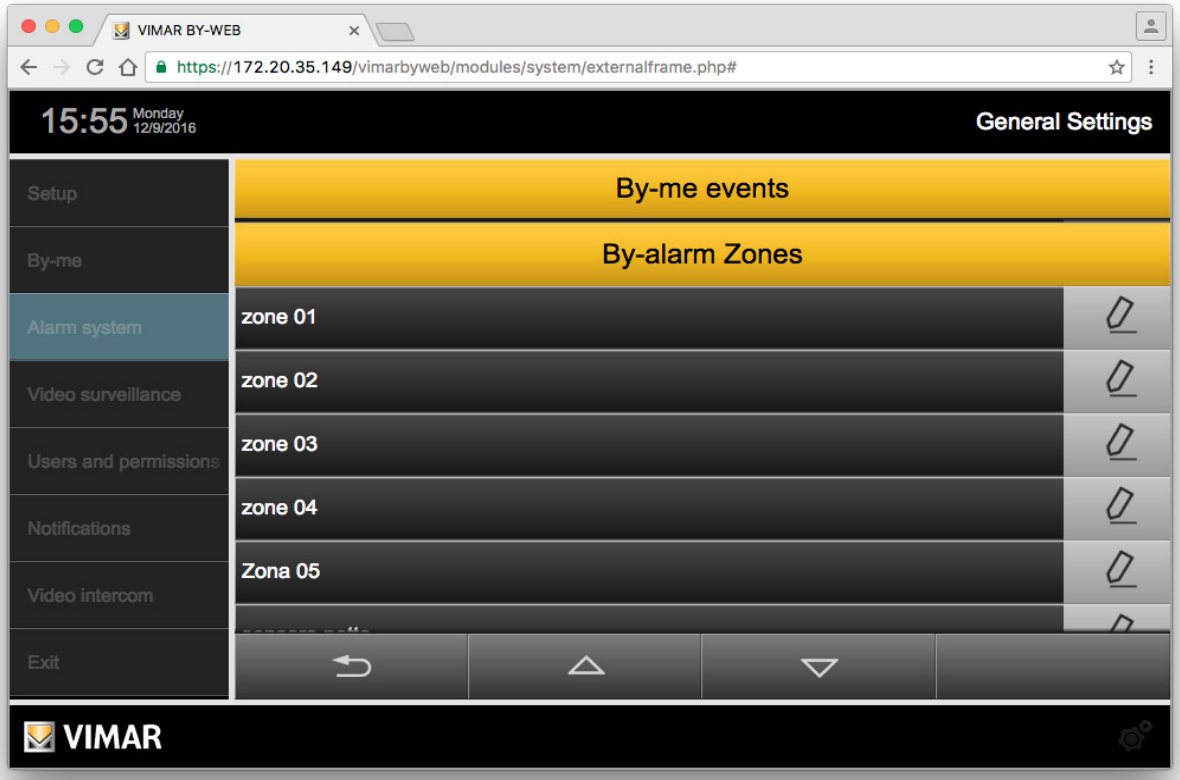
NOTE: les modifications décrites ne nécessitent pas de confirmation et sont enregistrées par le serveur Internet automatiquement.

Suppression d'un évènement préalablement créé

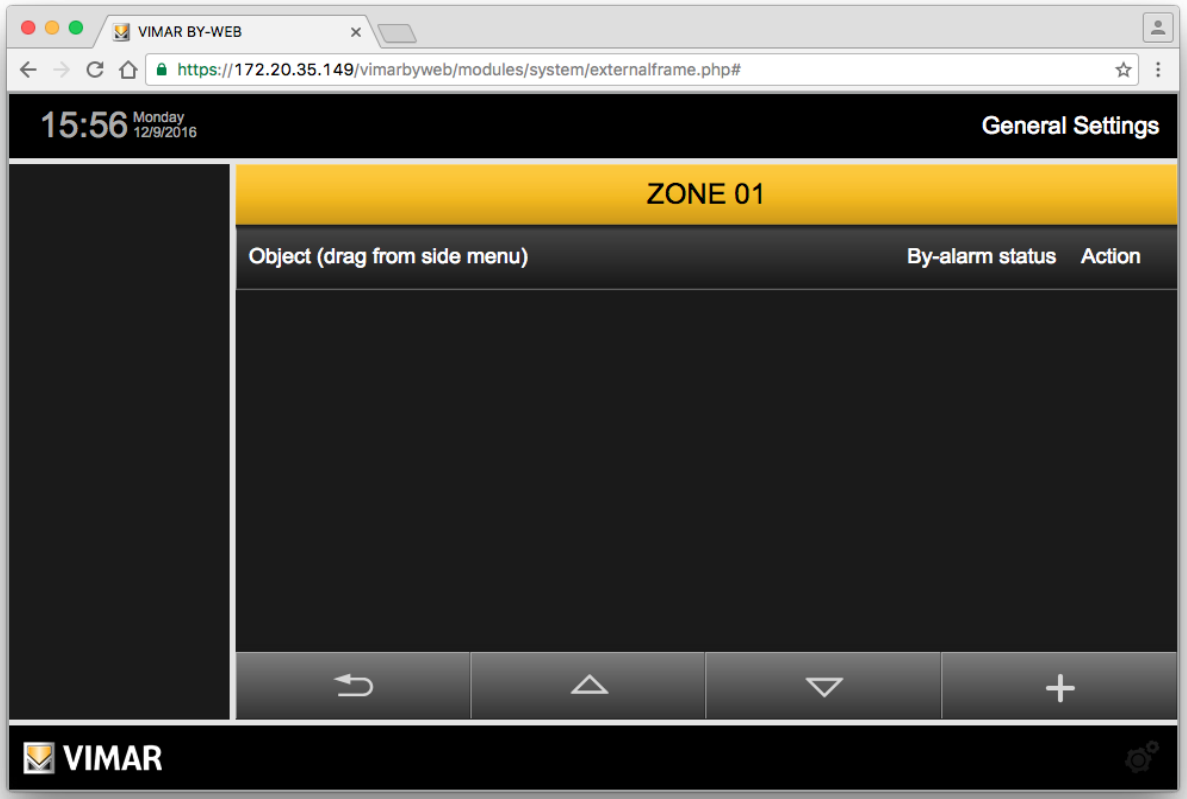
Pour supprimer de la liste un évènement préalablement créé lié à une zone spécifique, appuyer sur le bouton - à droite de la ligne qui représente l'évènement, dans la page qui contient la liste des évènements associés à ce découpage.

L'opération se termine par une fenêtre de validation.

4.1.4.2 Évènements By-me associés à l'état des zones By-alarm



Quand on appuie sur le bouton de modification situé à gauche de chaque ligne, on accède à la page des évènements de la zone sélectionnée.
Initialement, la page ne présente aucun évènement.


VIMAR BY-WEB
https://172.20.35.149/vimarbyweb/modules/system/externalframe.php#
15:56 Monday 12/9/2016
General Settings
ZONE 01
Object (drag from side menu)
By-alarm status
Action
VIMAR

Les opérations qui peuvent être exécutées dans la page des évènements associés à une zone spécifique sont les suivants et sont décrits dans les paragraphes ci-dessous

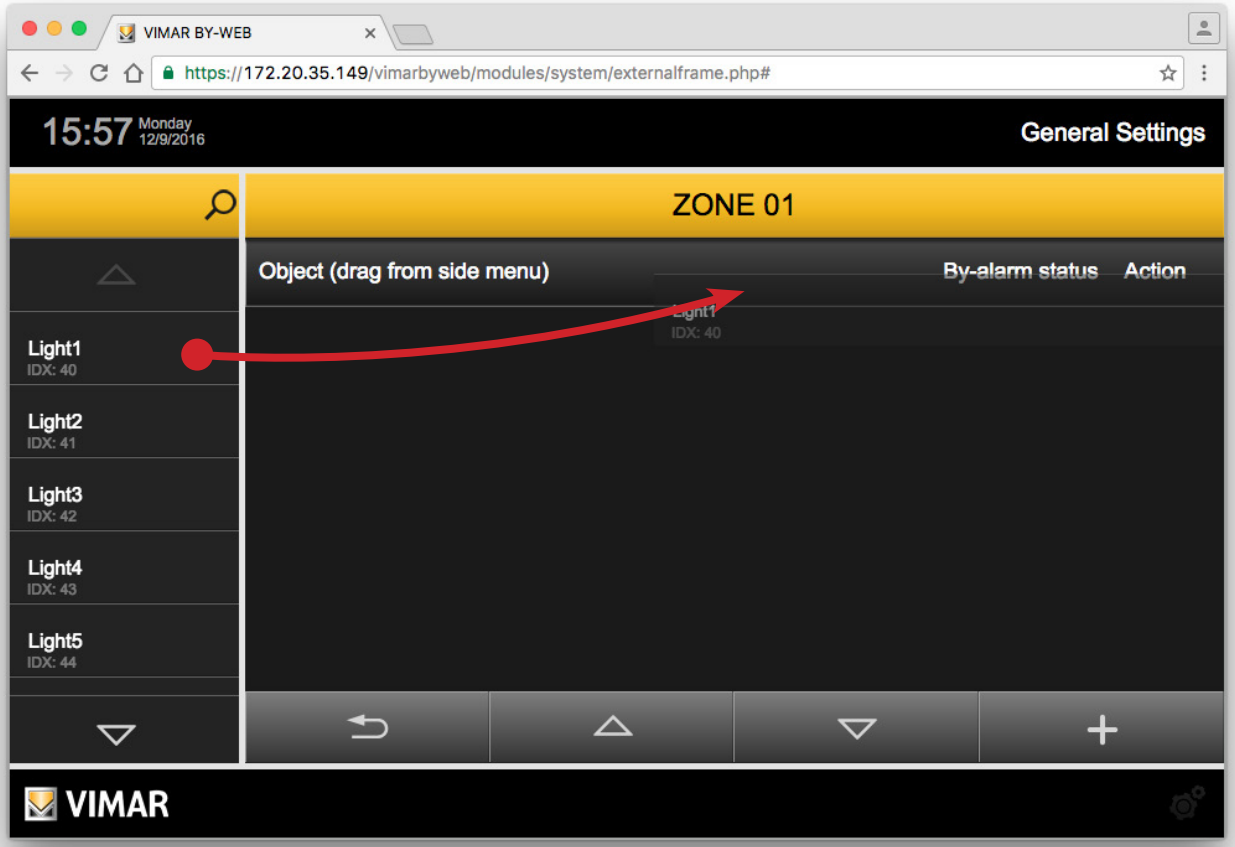
- Création d'un évènement
- Affichage de la configuration des évènements préalablement créés
- Modification d'un évènement préalablement créé
- Suppression d'un évènement préalablement créé

Création d'un évènement

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

1. Appuyer sur le bouton + en bas et à droite de la page pour ajouter un évènement à la liste.
2. La colonne de gauche affiche la liste des dispositifs qui peuvent être commandés par le serveur Internet après un évènement du système By-alarm.

   Cliquer-glisser l'objet de la liste dans la colonne latérale sur la barre grise Objet, en haut de la fenêtre (cliquer-glisser depuis le menu latéral). Si l'objet est déplacé par cliquer-glisser dans une autre zone de la fenêtre, l'évènement n'est pas créé.

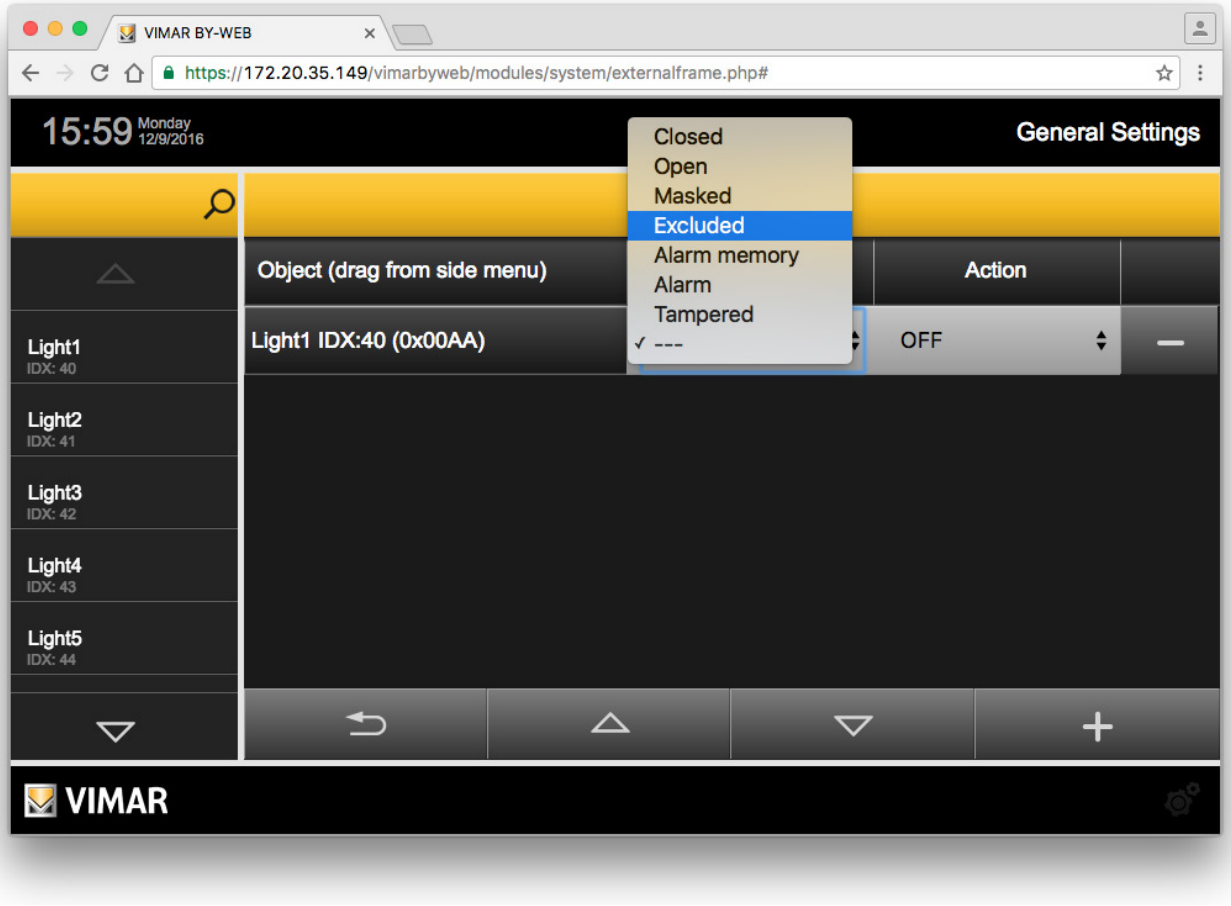


3. Une ligne est créée pour représenter l'évènement, son nom qui n'est pas modifiable coïncide avec la description de l'objet commandé. Avant de devenir opérationnel, l'évènement doit être configuré en suivant les indications ci-dessous.

   Appuyer sur le bouton dans la colonne État By-alarm pour sélectionner l'état de la zone qui déclenche l'envoi de la commande By-me Sélectionner -- pour ne pas associer d'évènement (dans ce cas, la gestion de l'évènement spécifique est inhibée).

   Appuyer sur le bouton de la colonne Action pour sélectionner la valeur de la commande qui doit être déclenchée par l'évènement By-alarm sélectionné.

   NOTE: les modifications décrites ne nécessitent pas de confirmation et sont enregistrées par le serveur Internet automatiquement.



4. Appuyer sur le bouton Retour pour sortir de la page ou pour répéter les opérations préalablement décrites à partir du point 1 et ajouter des dispositifs commandés à associer au même évènement.

Affichage de la configuration des évènements préalablement créés.

La page des évènements associés à la zone spécifique contient la liste de tous les évènements configurés.

Chaque ligne de la liste représente un évènement et donne les informations suivantes.

- Objet : nom permettant d'identifier l'objet à commander (actionneur ON/OFF, thermostat ou scénario)
- État de la zone du système By-alarm auquel la commande de l'objet By-me doit être associée.
- Action : commande à envoyer à l'objet

Modification d'un évènement préalablement créé

Pour modifier la configuration d'un évènement, trouver la ligne correspondante dans la liste et modifier les paramètres.

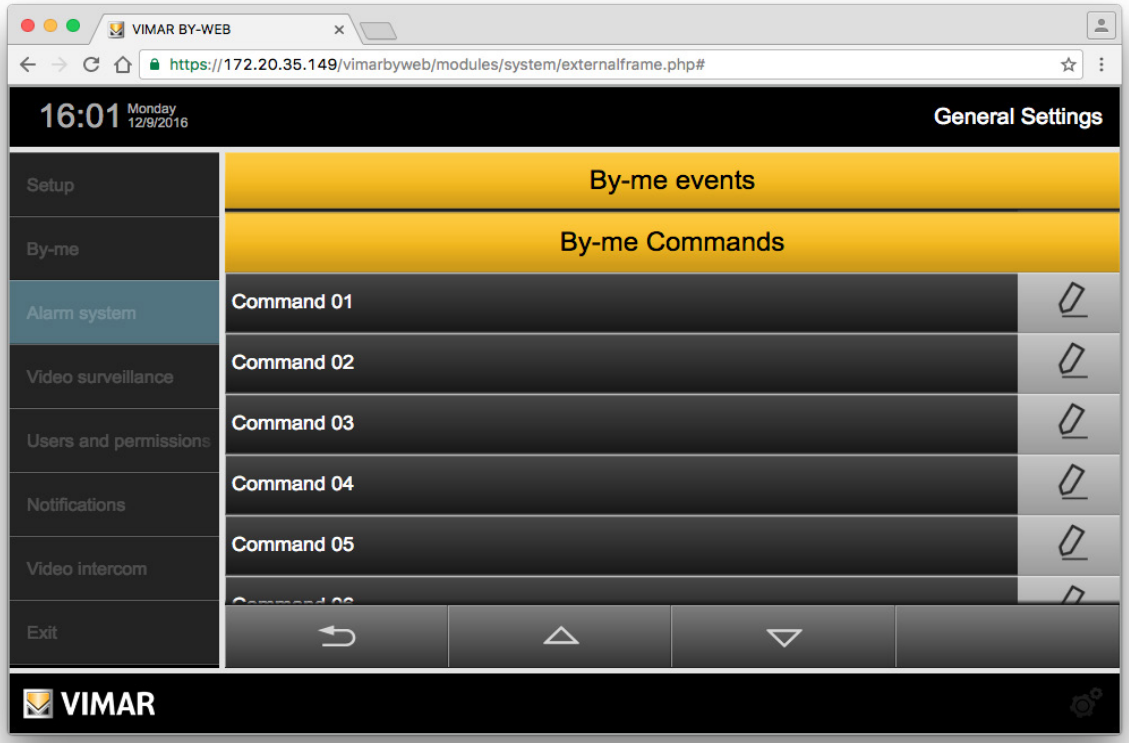
NOTE: les modifications décrites ne nécessitent pas de confirmation et sont enregistrées par le serveur Internet automatiquement.

Suppression d'un évènement préalablement créé

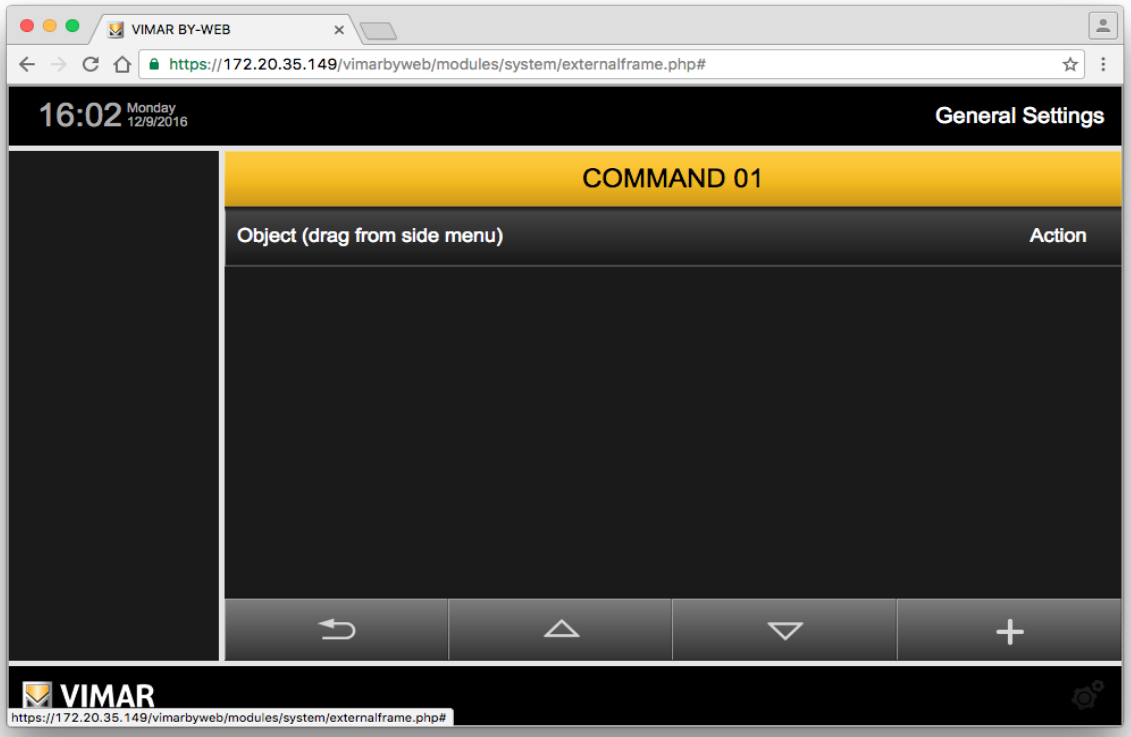
Pour supprimer de la liste un évènement préalablement créé pour une zone spécifique, appuyer sur le bouton - à droite de la ligne qui représente l'évènement, dans la page qui contient la liste des évènement associés à la zone.
L'opération se termine par une fenêtre de validation.

4.1.4.3 Évènements By-me associés aux commandes By-me

En plus de l'envoi des commandes d'activation à l'installation By-me, après certains changements d'état des découpages et des zones de l'installation By-alarm, il est possible d'envoyer des commandes d'activation à l'installation By-me en appuyant sur un bouton de radiocommande du système By-alarm. Cette fonction est possible grâce à la gestion des commandes By-me par la centrale By-alarm (art. 01700, art. 01702) équipée d'une interface de réseau Ethernet (art. 01712) avec un serveur Internet (art. 01945, art. 01946). Ce chapitre décrit la configuration des commandes By-me dans le serveur Internet. Se référer à la documentation du système By-alarm pour la description de la configuration des commandes By-me dans le système By-alarm.



Quand on appuie sur le bouton de modification situé à gauche de chaque ligne, on accède à la page des évènements pour la commande By-me sélectionnée. Initialement, la page ne présente aucun évènement.


VIMAR BY-WEB
https://172.20.35.149/vimarbyweb/modules/system/externalframe.php#
16:02 Monday 12/9/2016
General Settings
COMMAND 01
Object (drag from side menu)
Action
VIMAR
https://172.20.35.149/vimarbyweb/modules/system/externalframe.php#

Configuration anti-intrusion

Les opérations qui peuvent être exécutées dans la page des évènements associés à une zone spécifique sont les suivants et sont décrits dans les paragraphes ci-dessous.

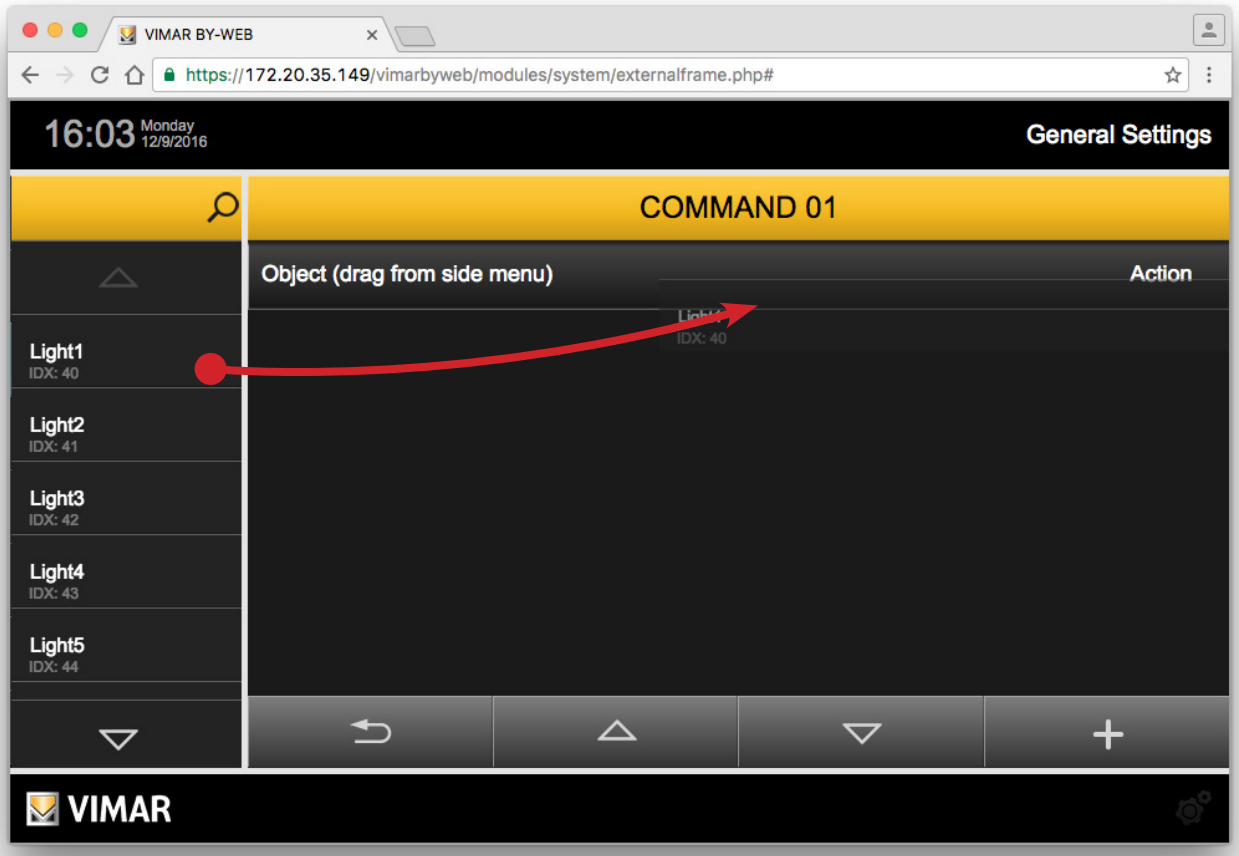
- Création d'un évènement
- Affichage de la configuration des évènements préalablement créés
- Modification d'un évènement préalablement créé
- Suppression d'un évènement préalablement créé

Création d'un évènement

Pour ajouter un évènement associé à une commande By-me du système By-alarm, procéder de la façon suivante.

1. Appuyer sur le bouton + en bas et à droite de la page pour ajouter un évènement à la liste.
2. La colonne de gauche affiche la liste des dispositifs qui peuvent être commandés par le serveur Internet après un évènement du système By-alarm.

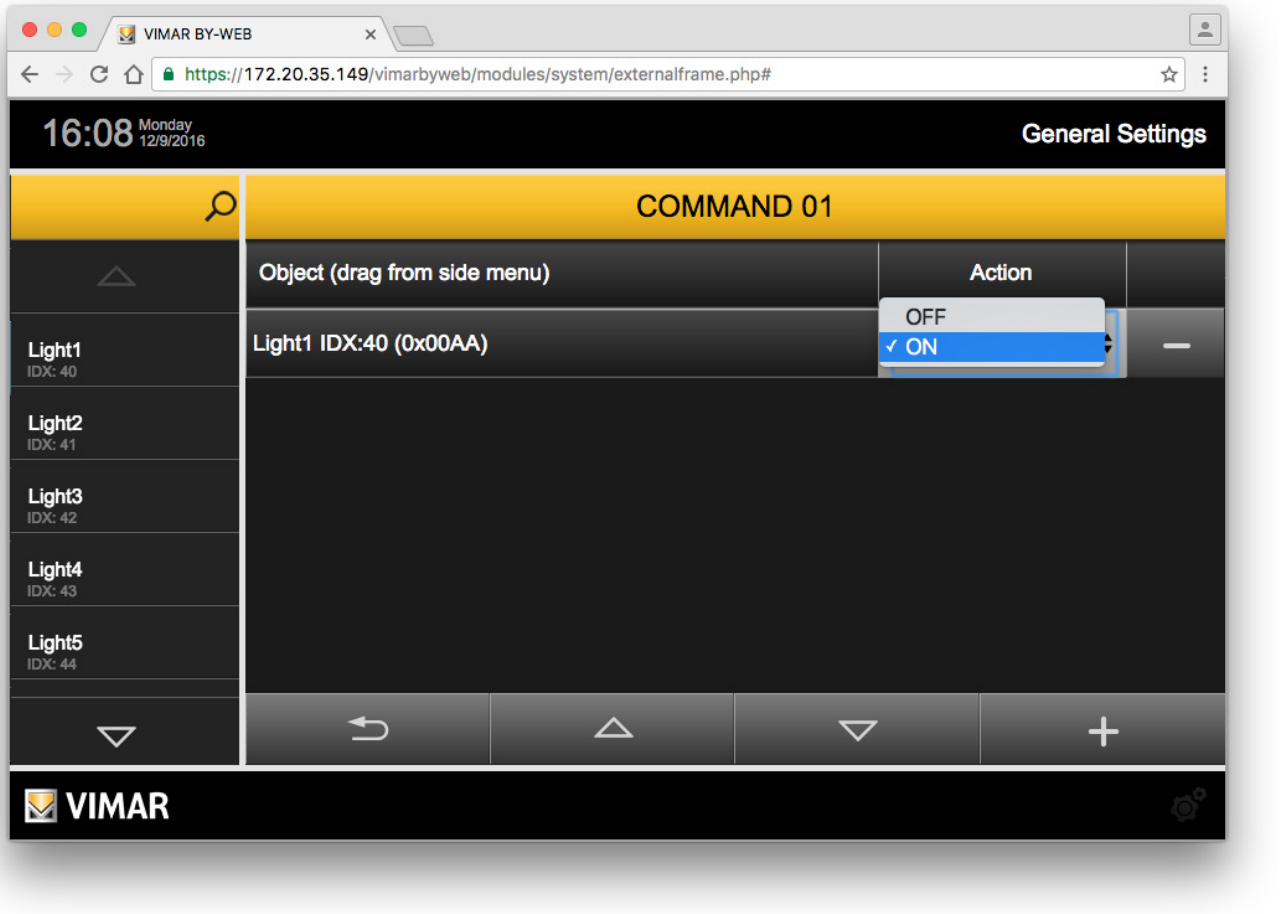
   Cliquer-glisser l'objet de la liste dans la colonne latérale sur la barre grise Objet, en haut de la fenêtre (cliquer-glisser depuis le menu latéral). Si l'objet est déplacé par cliquer-glisser dans une autre zone de la fenêtre, l'évènement n'est pas créé.



3. Une ligne est créée pour représenter l'évènement, son nom qui n'est pas modifiable coïncide avec la description de l'objet commandé. Avant de devenir opérationnel, l'évènement doit être configuré en suivant les indications ci-dessous.

Appuyer sur le bouton de la colonne Action pour sélectionner la valeur de la commande qui doit être déclenchée par l'évènement By-alarm sélectionné.

NOTE: les modifications décrites ne nécessitent pas de confirmation et sont enregistrées par le serveur Internet automatiquement.



4. Appuyer sur le bouton Retour pour sortir de la page ou pour répéter les opérations préalablement décrites à partir du point 1 et ajouter des dispositifs commandés à associer au même évènement.

Affichage de la configuration des évènements préalablement créés.

La page des évènements associés à la commande By-me sélectionnée contient la liste des évènements configurés.

Chaque ligne de la liste représente un évènement et donne les informations suivantes.

- Objet : nom permettant d'identifier l'objet à commander (actionneur ON/OFF, thermostat ou scénario)
- Action : commande à envoyer à l'objet

Modification d'un évènement préalablement créé

Pour modifier la configuration d'un évènement, trouver la ligne correspondante dans la liste et modifier les paramètres.

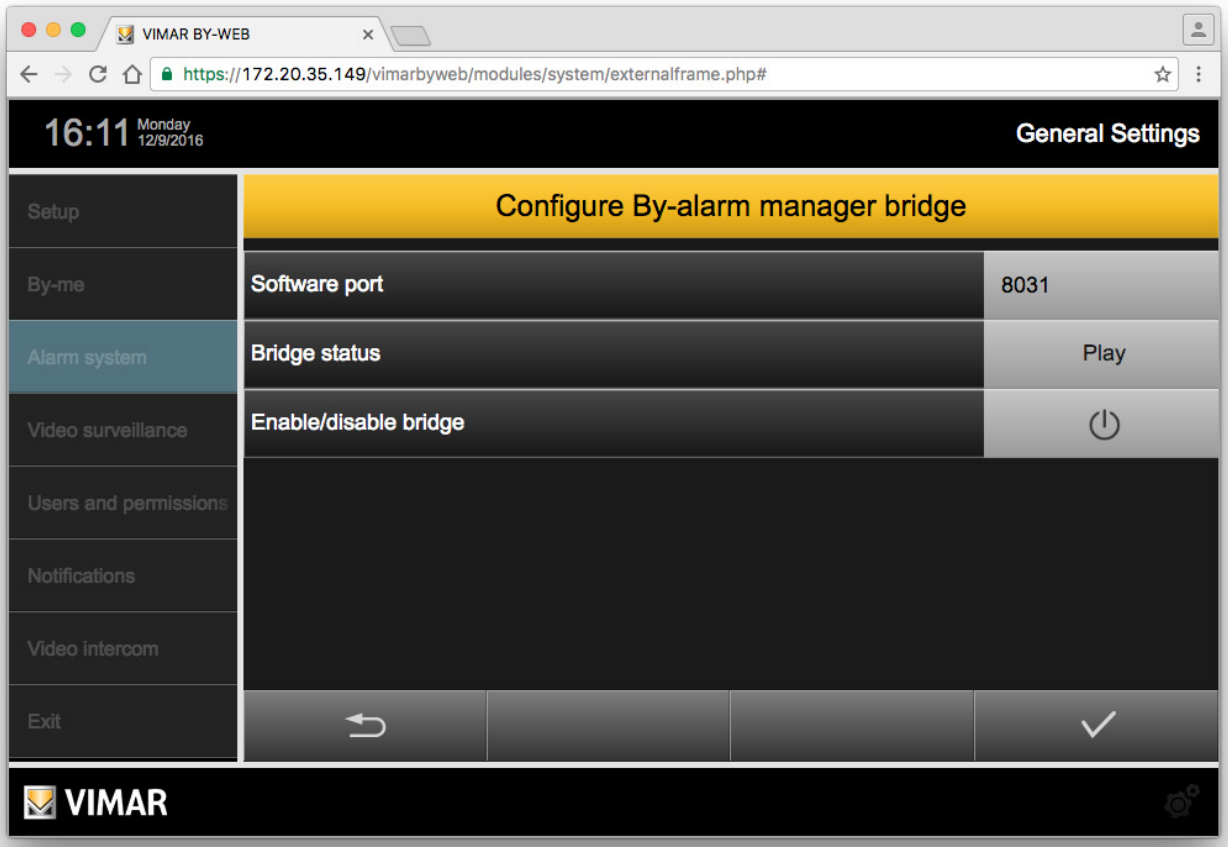
NOTE: les modifications décrites ne nécessitent pas de confirmation et sont enregistrées par le serveur Internet automatiquement.

Suppression d'un évènement préalablement créé

Pour supprimer de la liste un évènement préalablement créé pour une commande By-me spécifique, appuyer sur le bouton - à droite de la ligne qui représente l'évènement, dans la page qui contient la liste des évènements associés à cette commande.
L'opération se termine par une fenêtre de validation.

4.1.5 Bridge By-alarm Manager

Paramétrer et activer cette fonction avant d'utiliser le logiciel By-alarm Manager pour la gestion du système By-alarm, à distance ou par LAN, avec le serveur Internet comme bridge et une connexion HTTPS protégée par un certificat SSL.
Pour la description de la fonction, se référer au chapitre 4.1.5.1 Fonction bridge du serveur Internet.



La page Configuration bridge By-alarm Manager comporte trois champs :

- Port du logiciel : port IP utilisé par le logiciel By-alarm Manager afin de communiquer avec le serveur Internet pour la fonction bridge. Définir le port du serveur Internet et utiliser cette valeur comme paramètre dans la fenêtre du logiciel By-alarm Manager pour la connexion à la centrale By-alarm avec le bridge géré par le serveur Internet.
- État bridge : indique l'état de fonctionnement du bridge.
  - Play : la fonction bridge est active.
  - Stop : la fonction bridge est désactivée.
- Activer/désactiver bridge : activation et désactivation de la fonction. L'état d'activation est affiché dans le champ État bridge.

Appuyer sur le bouton de validation pour confirmer les données saisies ou sur le bouton Retour pour sortir de la page sans sauvegarder les données saisies.

4.1.5.1 Fonction bridge du serveur Internet

S'il y a un serveur Internet dans l'installation By-alarm (01945 ou 01946) et que la centrale By-alarm (art. 01700, art. 01703) est équipée d'une interface de réseau Ethernet (art. 01712), il est possible d'utiliser le logiciel By-alarm Manager avec une connexion de réseau HTTPS et la centrale By-alarm.
Cette fonction est prévue pour une connexion locale (le PC sur lequel est installé By-alarm manager est relié au réseau LAN auquel est reliée la centrale By-alarm) ou pour une connexion à distance par Internet qui permet d'effectuer les opérations de configuration et de diagnostic à distance du logiciel By-alarm manager.
Les chapitres suivants décrivent les deux cas, connexion locale et connexion à distance entre le logiciel By-alarm manager et la centrale By-alarm avec les fonctions bridge du serveur Internet.

Connexion locale entre By-alarm Manager et la centrale By-alarm

La figure suivante est un schéma des flux d'information entre le logiciel By-alarm manager et la centrale By-alarm pour une connexion locale.

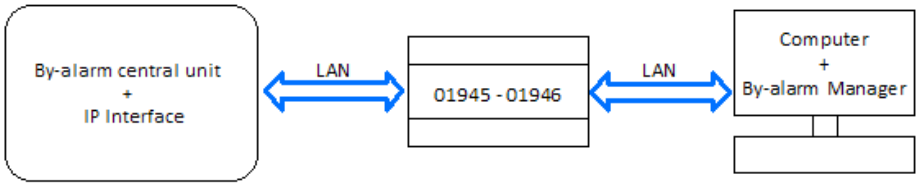


Figure 1 - Connexion locale entre By-alarm Manager et la centrale By-alarm

Avant la première connexion, il nécessaire d'exécuter les étapes de configuration suivantes.

1. Configurer sur la centrale By-alarm le port pour la fonction bridge. Port TCP By-alarm (se référer à la documentation de la centrale By-alarm).
2. Sur le serveur Internet, configurer le champ Port TCP By-alarm dans la page Anti-intrusion/Configuration de la rubrique Paramètres généraux. Cette valeur doit coïncider avec celle qui a été configurée au point 1.
3. Sur le serveur Internet, configurer le champ Port du logiciel dans la page Anti-intrusion/Bridge By-alarm manager, rubrique Paramètres généraux. Cette valeur doit être saisie dans la page de configuration des paramètres de connexion du logiciel By-alarm manager avec le serveur Internet.

Pour exécuter la connexion, procéder de la façon suivante.

1. Sur le serveur Internet, activer la fonction bridge avec le bouton Activer/désactiver bridge de la p age Anti-intrusion/Bridge By-alarm manager, rubrique Paramètres généraux.
   Il est possible de vérifier dans le champ État bridge de cette page l'activation de la fonction : vérifier que l'état est Play.
2. Ouvrir le logiciel By-alarm manager, se connecter à la centrale By-alarm, saisir les paramètres suivants comme paramètres de CONNEXION SUR LE RÉSEAU LOCAL.
   a. Adresse locale : adresse IP du serveur Internet
   b. Port TCP : port configuré sur le serveur Internet au point 3.

   Après la configuration avec By-alarm manager, il est possible de désactiver la fonction bridge du serveur Internet.

Connexion à distance entre By-alarm Manager et la centrale By-alarm

La figure suivante est un schéma des flux d'information entre le logiciel By-alarm manager et la centrale By-alarm pour une connexion à distance.

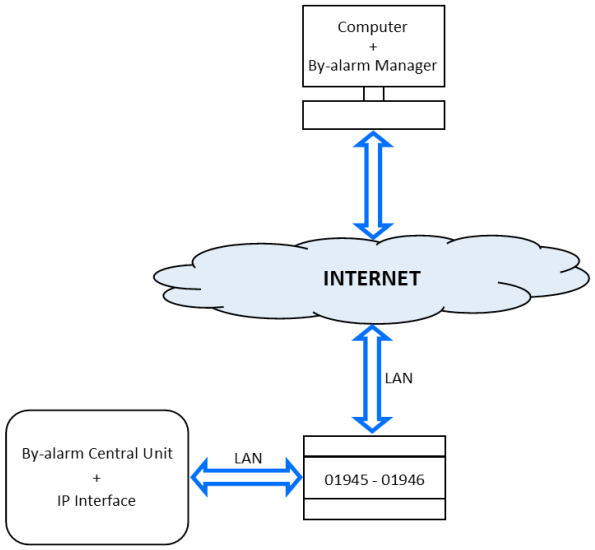


Figure 2 - Connexion à distance entre By-alarm Manager et la centrale By-alarm

Avant la première connexion, il nécessaire d'exécuter les étapes de configuration suivantes.

1. Configurer sur la centrale By-alarm le port pour la fonction bridge. Port TCP By-alarm (se référer à la documentation de la centrale By-alarm).
2. Sur le serveur Internet, configurer le champ Port TCP By-alarm dans la page Anti-intrusion/Configuration de la rubrique Paramètres généraux. Cette valeur doit coïncider avec celle qui a été configurée au point 1.
3. Sur le serveur Internet, configurer le champ Port du logiciel dans la page Anti-intrusion/Bridge By-alarm manager, rubrique Paramètres généraux. Cette valeur doit être saisie dans la page de configuration des paramètres de connexion du logiciel By-alarm manager avec le serveur Internet.
4. Sur le routeur ADSL, exécuter l'ouverture du port externe qui doit être cartographié en réglant le port forwarding sur le port utilisé par le serveur Internet pour la connexion avec By-alarm manager.

Le réglage du port forwarding à créer sur le routeur ADSL doit associer le port extérieur à la paire suivante (vérifier que le port n'est pas déjà utilisé par d'autres applications/services) : adresse IP du serveur Internet (sur LAN) et Port du logiciel, page Anti-intrusion/Bridge By-alarm manager, option Paramètres généraux du serveur Internet.

Pour exécuter la connexion, procéder de la façon suivante.

1. Sur le serveur Internet, activer la fonction bridge avec le bouton Activer/Désactiver bridge, page Anti-intrusion/Bridge By-alarm manager, option Paramètres généraux.
   Il est possible de vérifier dans le champ État bridge de cette page l'activation de la fonction : vérifier que l'état est Play.
2. Ouvrir le logiciel By-alarm manager et se connecter à la centrale By-alarm, saisir les paramètres suivants comme paramètres de CONNEXION INTERNET.
   a. Adresse locale : URL du serveur Internet (DNS)/adresse IP interface extérieure du routeur correspondant à l'adresse IP du serveur Internet.
   b. Port TCP : port extérieur du routeur correspondant au port configuré sur le routeur au point 4 ci-dessus.

Après la configuration avec By-alarm manager, il est possible de désactiver la fonction bridge du serveur Internet.

4.2 Le système anti-intrusion By-me

4.2.1 Avant-propos

Si le système dispose de la fonction de gestion du système anti-intrusion SAI, toutes les informations nécessaires pour la configuration du Web Server sont déjà présentes dans le projet XML exporté depuis la Centrale, sans devoir effectuer d'autres opérations.
Certaines opérations sont cependant nécessaires pour procéder à la correcte communication entre la Centrale SAI et le Web Server, comme illustré ci-après.

4.2.2 Modification des découpages

La page « DÉCOUPAGES » de la section « ANTI-INTRUSION » de l'administration permet de modifier le nom attribué en Centrale aux découpages présents dans le projet ; modifier simplement le nom puis fermer la page en utilisant la touche de retour à la page principale de l'administration.

5. Configuration de la télésurveillance

5.1 Avant-propos

Il est possible de visualiser, dans la page du **Web Server**, le flux vidéo d'une ou plusieurs caméras vidéo IP (maximum 32) répondant aux requis suivants :

Fabricant	Requis d'équipement	Conditions préalables pour l'installation du logiciel	Requis de navigateur
Axis	Tous les modèles de caméra vidéo IP		Tout navigateur supporté par le dispositif.
ELVOX	Gère toutes les caméras IP et serveurs vidéo ELVOX	VideoLAN VLC Vimar ByWeb Tools**	
Générique Mjpeg*	Dispositif capable de gérer le format Mjpeg		Tout navigateur capable d'afficher le format Mjpeg
Mobotix	Tous les modèles de caméra vidéo IP	VideoLAN VLC Vimar ByWeb Tools**	Tout navigateur capable de lire le format MJPEG
Gestion d'un flux RTSP générique *	Dispositifs capables de gérer le flux RTSP		

* Le fonctionnement correct des flux vidéo de tous les dispositifs disponibles sur le marché n'est pas garanti (caméras vidéo, serveur vidéo…).

** Pour l'installation de Vimar ByWeb Tools, voir le chapitre 12. ByWeb Tools de Vimar de ce manuel.

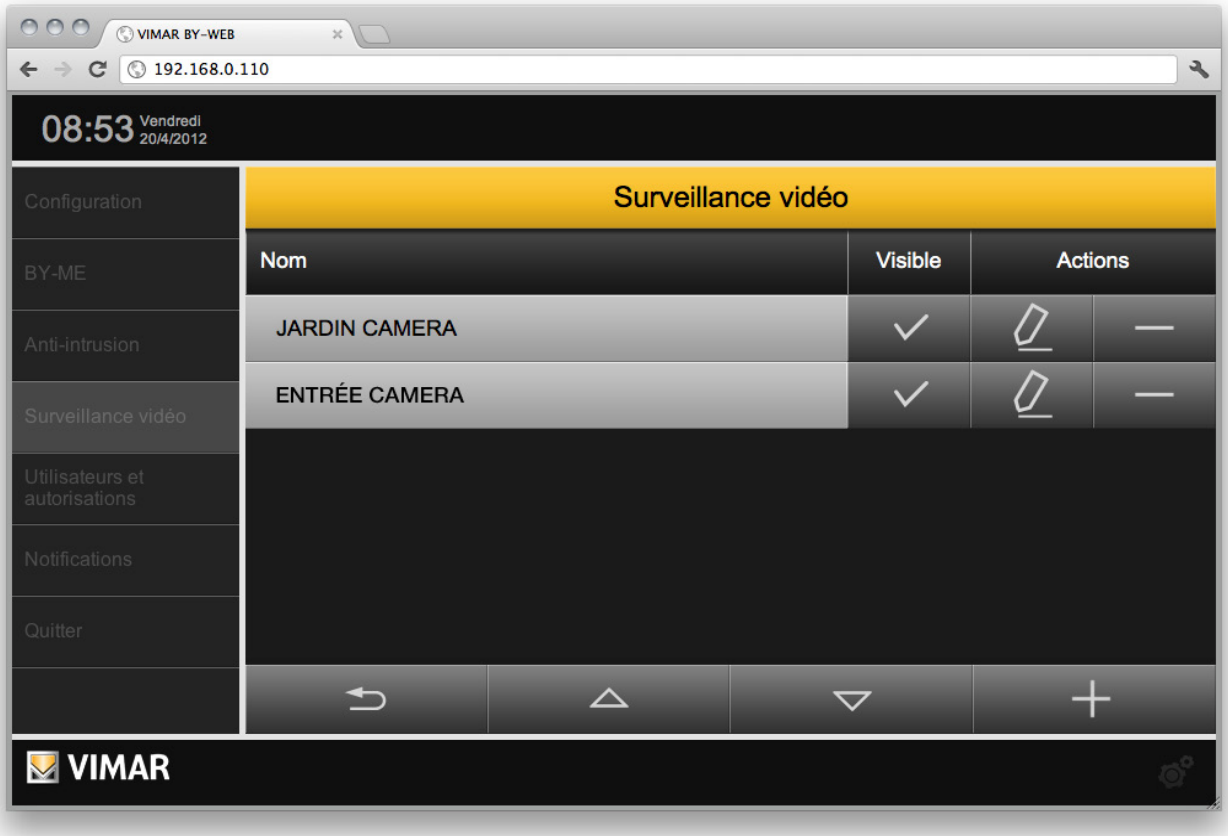
5.2 Configuration d'une caméra vidéo IP.

En sélectionnant l'option « TÉLÉSURVEILLANCE » dans le menu principal de a zone RÉGLAGES GÉNÉRAUX, il est possible de configurer les caméras vidéo IP présentes dans le système, à condition que celles-ci répondent aux requis précédemment énumérés. La liste des caméras vidéo est initialement vide, pour ajouter une nouvelle caméra vidéo, appuyer sur la touche « AJOUTER » disponible sur le clavier situé en bas de la page (comme expliqué précédemment dans le cadre de la création de nouveaux environnements).

Une fois la nouvelle caméra vidéo affichée dans la liste, il est possible d'en modifier immédiatement le nom dans la case de texte prévue à cet effet. Les touches suivantes sont également disponibles :

	MODIFICATION DE L'ORDRE En faisant glisser cette touche, il est possible de modifier l'ordre d'affichage des télécaméras dans le menu relatif du **Web Server**.
	MODIFIER Permet d'accéder à la fiche détaillée de la télécaméra, comme mieux décrit ci-après.
	SUPPRIMER Supprime la télécaméra du **Web Server**. Cette opération, sur confirmation préalable de l'installateur, ne pourra plus être annulée.

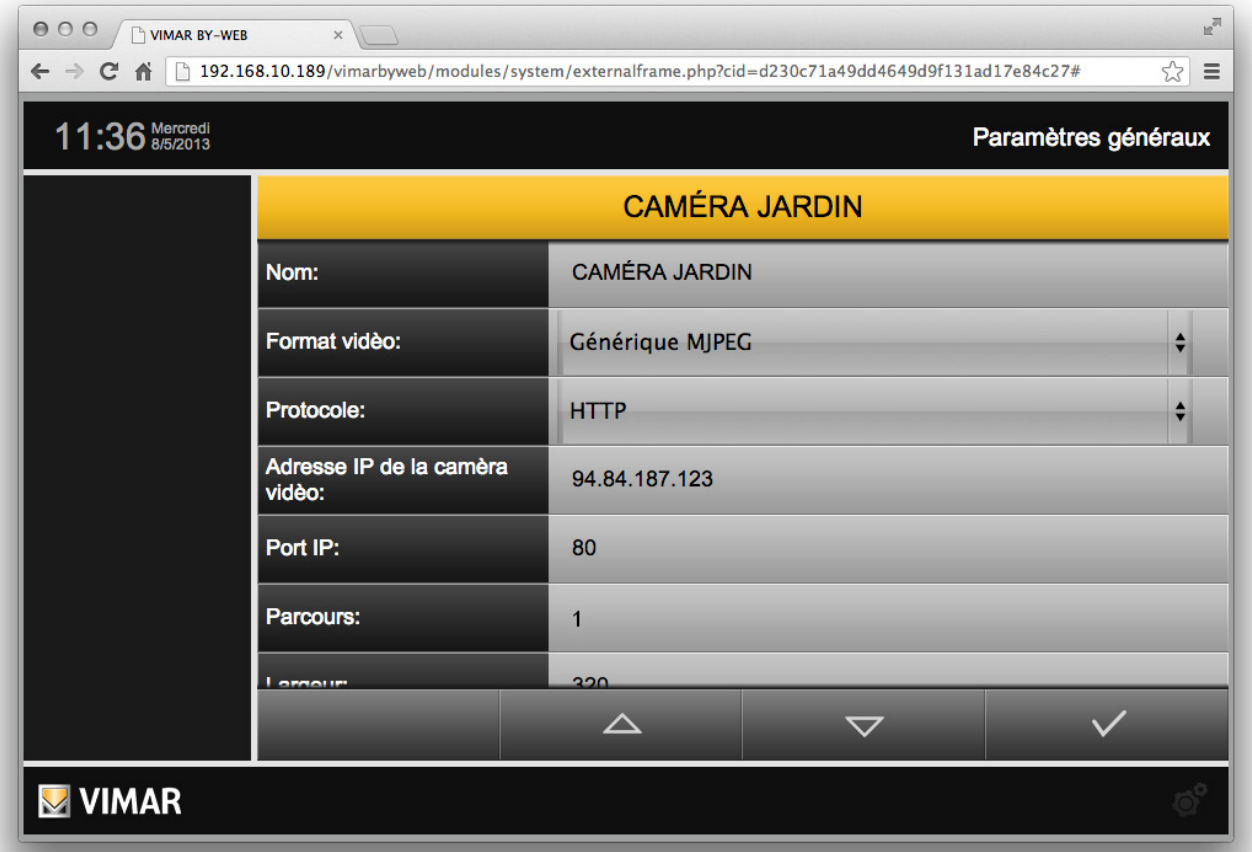
Configuration de la télésurveillance



Avec la touche « MODIFIER », il est possible d'accéder à la fiche détaillée de la caméra vidéo dans laquelle personnaliser les paramètres suivants: *(Tous les champs ne sont pas présents pour chaque format vidéo).*

NOM	Nom associé à la caméra vidéo, visible dans le menu « TÉLÉSURVEILLANCE » par les utilisateurs.
FORMAT VIDÉO	Sélectionner une des formats possibles proposés en fonction du fabricant de la caméra vidéo et de sa typologie.
PROTOCOLE	Protocole utilisé pour accéder à la caméra.
ADRESSE IP	Adresse IP en réseau local attribuée à la caméra vidéo IP. **REMARQUE**: il n'est pas nécessaire de saisir le protocole utilisé (http, https, rtsp)
PORT IP	Port IP sur lequel afficher le flux vidéo de la caméra.
PARCOURS	Chaîne représentant le parcours à suivre jusqu'à la caméra.
CANAL	En cas de caméras vidéo ou serveurs vidéo avec plusieurs canaux, spécifier le numéro du canal à visualiser. Prédéfini : 1.
FLUX	Il est possible de choisir entre Flux principal et Flux secondaire.
IDENTIFIANT	Nom de l'utilisateur utilisé pour la connexion aux caméras.
MOT DE PASSE	Mot de passe utilisé pour la connexion à la caméra.
LARGEUR	Largeur en pixels de la fenêtre dans laquelle seront visualisées les images vidéo en provenance de la caméra. Consulter la documentation de la caméra vidéo et sa configuration pour connaître les différentes valeurs possibles à saisir dans ce champ.
HAUTEUR	Hauteur en pixels de la fenêtre dans laquelle seront visualisées les images vidéo en provenance de la caméra. Consulter la documentation de la caméra vidéo et sa configuration pour connaître les différentes valeurs possibles à saisir dans ce champ.
Activer le proxy HTTPS pour les connexions à distance :	En activant cette fonction, les images de la caméra vidéo IP seront élaborées par le proxy interne du Web Server (et codifiées par SSL).

REMARQUE : pour les formats vidéos et RTSP générique et MJPEG générique, l'URL d'accès à la caméra est construit par le Web Server de la façon suivante : adresse IP: port IP/parcours.



Une fois la saisie des paramètres de fonctionnement terminée, revenir à la page de télésurveillance en utilisant la touche « RETOUR » du clavier. Configurer les éventuelles autres caméras vidéo en suivant la même procédure.

5.2.1 Fonction Proxy des caméras vidéo IP

Les caméras vidéo IP disposent d'une fonction proxy, créant un « tunnel » dans le port 443 en cas d'accès à distance, véhiculant ainsi sur le Web Server, les images vidéo des caméras IP disponibles en réseau local sur un nombre équivalent d'adresses IP. Ainsi, l'installateur n'a plus besoin d'ouvrir plus d'un port IP sur le routeur ADSL (ou similaire).

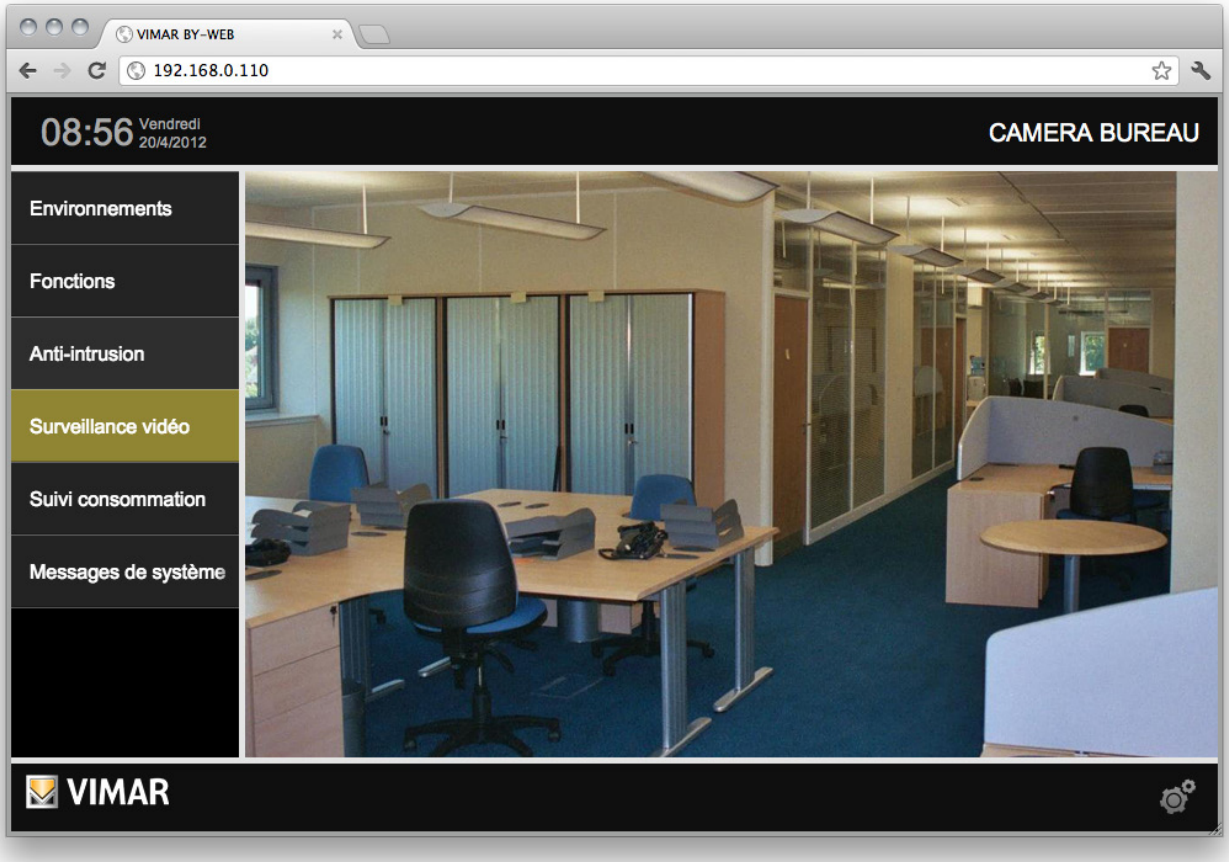
La configuration de la fonction proxy est totalement automatique et « transparente » : lors de la sauvegarde d'une télécaméra, la règle proxy correspondante est créée dans le fichier de configuration du Web Server, laquelle est rappelée en cas d'accès à la page de ladite caméra vidéo avec allumage à distance (en réseau local, le flux prélevé depuis l'adresse IP de la caméra vidéo est directement visualisé).

Si cette fonction n'est pas activée, il reste dans tous les cas possible de visualiser la caméra vidéo IP à distance sans utiliser la codification SSL du proxy du Web Server, rendant donc nécessaire l'ouverture d'un port supplémentaire sur le router pour l'accès à distance à la télécaméra IP (utiliser cette fonction par exemple si la caméra IP ne dispose pas déjà d'une codification SSL interne et si une connexion internet très rapide, type fibre optique, est disponible).

REMARQUE: Avec les formats vidéo Elvox et RTSP générique, la fonction Proxy est absente.
Pour accéder à distance à la caméra par l'intermédiaire du Web Server, il est nécessaire de créer des règles d'accès au routeur appropriées.

5.3 Visualisation des télécaméras

Les télécaméras IP configurées dans le **Web Server** sont accessibles pour les utilisateurs à travers l'option correspondante proposée dans le menu principal de navigation. Le menu secondaire contient la liste des caméras vidéo dans l'ordre défini précédemment. En sélectionnant une des options disponibles, il sera possible d'accéder aux images vidéo relatives.



Pour plus de détails, consulter le MANUEL DE L'UTILISATEUR.

6. Economiseur d’énergie

6.1 Avant-propos

ECONOMISEUR D’ÉNERGIE est une fonction de By-Web destinée à la surveillance et à l’analyse des consommations énergétiques du système domotique. La lecture périodique des compteurs de puissance consommée et produite permet au système d’élaborer une série de statistiques en fonction des paramètres de configuration, et donc à l’utilisateur de disposer d’une synthèse sous forme graphique et de tableau fournissant les informations utiles pour un usage plus conscient et responsable de l’énergie.

Si le système dispose d’un dispositif de production d’électricité, l’indicateur de consommation de la section ECONOMISEUR D’ÉNERGIE indique la quantité d’énergie effectivement consommée par les charges du système (il est supposé que le système a été construit conformément aux prescriptions de Vimar : la sonde (les sondes en présence de trois phases) de l’appareil de mesure de la consommation doit être située immédiatement en aval du compteur d’échange d’électricité avant toute dérivation).

En cas de surveillance de la consommation d’une ligne triphasée, l’indicateur de consommation indique la somme des consommations des trois phases.

En cas de surveillance de la production d’une ligne triphasée, l’indicateur de production indique la somme des productions des trois phases.

Le système By-me permet aussi de mesurer la consommation des charges unitaire (ou groupes de charges) comme cela est décrit dans le chapitre Charges Unitaires. Le système By-me permet aussi d’afficher et de sauvegarder les données fournies par l’interface compteur d’impulsions de Vimar (pour la gestion des compteurs de d’autres parties qui ont des impulsions comme ampleur de sortie), comme cela est décrit dans le chapitre Compteur d’impulsions.

Pour les configurations qui concernent le economiseur d’énergie, aller à la Section “Configurations générales”-> “By-me”-> “Economiseur d’énergie”. La page de configuration est divisée en deux sections principales: dans la première il y a les configurations de consommation et de production au niveau du système (Monitoring énergie) et dans la deuxième section il y a les configurations des compteurs unitaires et des compteurs d’impulsions (Compteurs et compteurs d’impulsions). L’autorisation du monitoring énergie s’effectue dans la section AUTORISER ECONOMISEUR D’ÉNERGIE.

Le données collectées par ECONOMISEUR D’ÉNERGIE doivent être considérées comme indicatives et ne correspondent pas nécessairement aux consommations enregistrées par le fournisseur du contrat d'énergie.

6.2 Consommation électrique

6.2.1 Configuration générale

La page « ECONOMISEUR D’ÉNERGIE » de la section « By-me » de l'administration permet d'en configurer les paramètres de fonctionnement. Ces derniers dépendent principalement du type de contrat énergétique du système. Ainsi, afin de saisir correctement les informations demandées, il est recommandé de se munir d'une facture ou autre type de document fourni par le fournisseur du contrat d'énergie.

Lors du premier accès, la fonction ECONOMISEUR D’ÉNERGIE est inactive; en autorisant la case de sélection correspondante (de la section “AUTORISER MONITORING ÉNERGIE”), la page sur laquelle il est possible de configurer toutes les fonctions liées au monitoring de l’énergie s’affiche. Pour accéder à la page de configuration de la “Consommation d’énergie”, sélectionner la section correspondante.

Les paramètres de configuration suivants sont prévus:

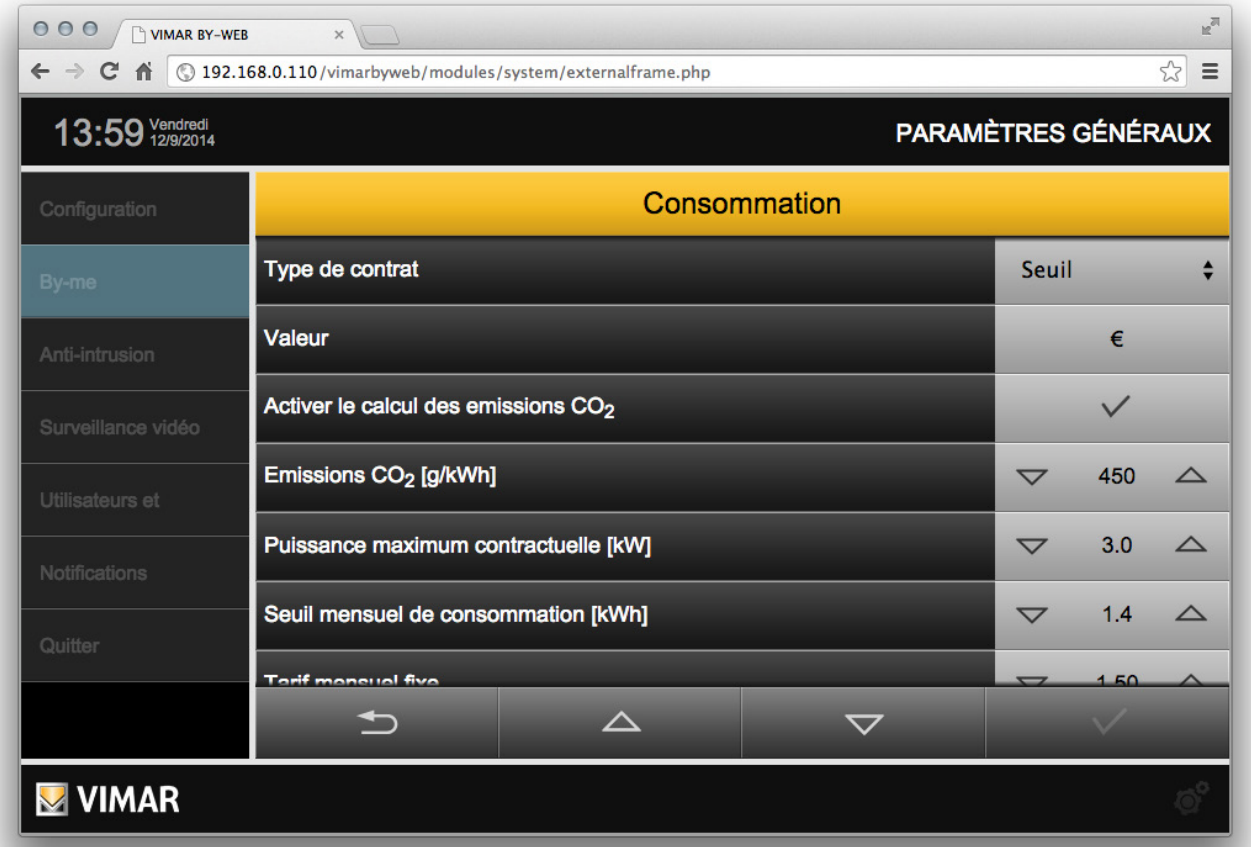
TYPE DE CONTRAT	Il est possible de configurer une des typologie de contrat suivantes : • CRÉNEAUX HORAIRE : contrat avec un ou plusieurs créneaux horaire au cours de la journée correspondant à différents tarifs. • SEUIL : contrat à tarif fixe jusqu'à une consommation donnée, puis tarif applicable au consommations supplémentaires. En fonction du choix du contrat, les sections successives de la page s'activeront ou non.
VALEUR	Spécifier la valeur à utiliser lors de l'affichage des coûts.
ACTIVER LE CALCUL DES ÉMISSIONS DE CO2	Spécifier s'il est souhaité visualiser les informations relatives à l'émission de gaz de serre.
ÉMISSIONS CO2	Si le calcul des émissions est activé, il est possible de spécifier la quantité de gaz de serre émis par kWh d'énergie consommée.
PUISSANCE MAXIMUM CONTRACTUELLE	Valeur maximum d'absorption autorisée par le gestionnaire.

REMARQUE : les modifications effectuées sont instantanément enregistrées et restent disponibles pour ECONOMISEUR D’ÉNERGIE . Il n'est donc pas nécessaire d'effectuer des opérations de sauvegarde une fois les paramètres requis saisis, mais de quitter la page en appuyant sur la touche « RETOUR » .

6.2.2 Contrats à seuil

En cas de contrat à SEUIL, les paramètres suivants sont également demandés :

SEUIL MENSUEL DE CONSOMMATION	Valeur maximum de consommation énergétique outre laquelle est prévu un coût majeur au tarif contractuel de base.
TARIF MENSUEL FIXE	Coût fixe mensuel en absence de dépassement du seuil.
Coût KWH AU-DELÀ DU SEUIL	Tarif appliqué aux consommations dépassant le seuil mensuel.



6.2.3 Contrats à créneaux horaires

En cas de contrats à CRÉNEAUX HORAIRES certaines sections spécifiques de configuration sont activées, elles permettent de configurer tous les paramètres nécessaires pour que le Web Server puisse fournir les données des consommations et des coûts en fonction de son propre contrat.

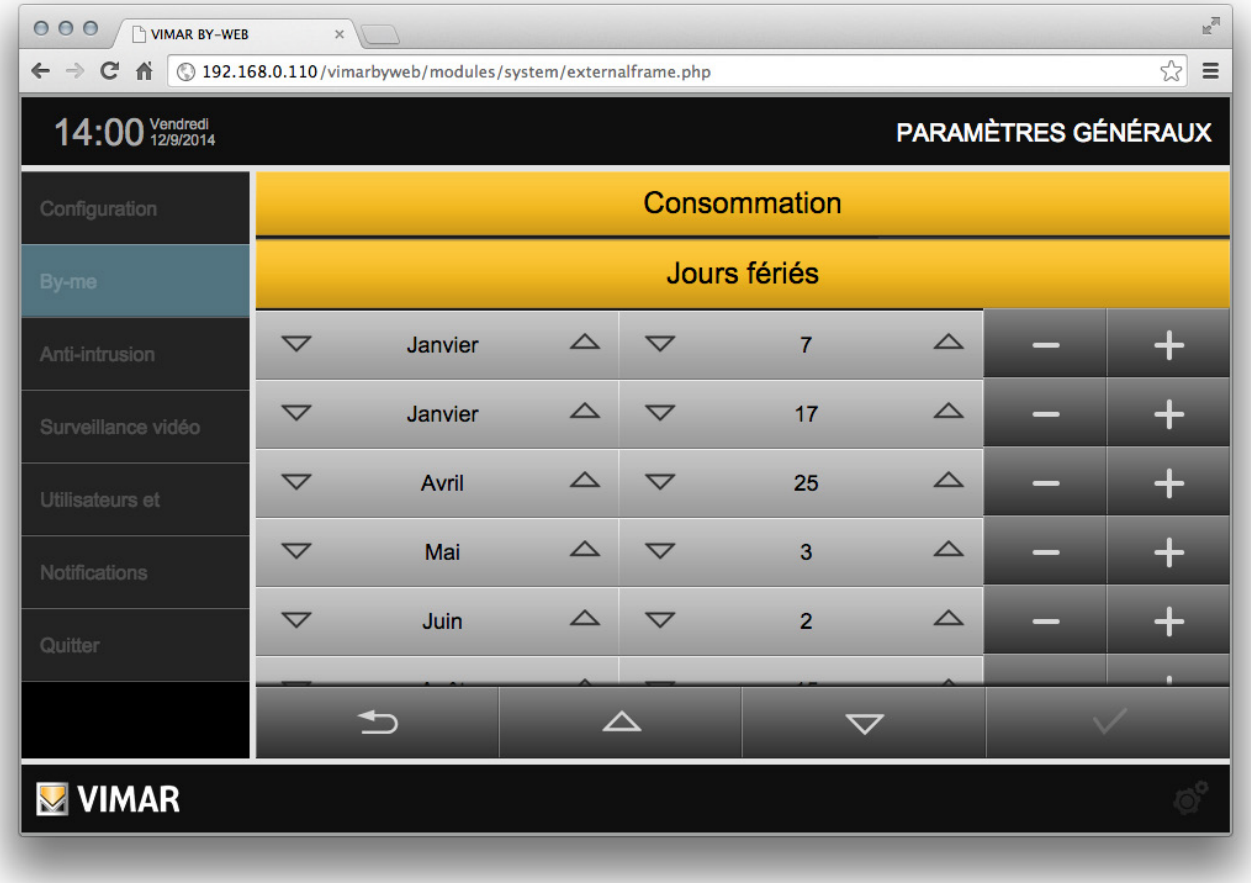
6.2.3.1 Créneaux horaires

La section CRÉNEAUX HORAIRES permet d'établir le nombre de créneaux horaires (minimum une heure, jusqu'à un maximum de trois jours) prévus dans le contrat de fournitures d'énergie électrique.
Utiliser la case de sélection en correspondance de chaque créneau horaire pour l'activer, et ensuite, configurer le tarif correspondant (en saisissant une valeur numérique à partir du clavier, après avoir sélectionnée le champ des données, ou les boutons d'augmentation/diminution).

6.2.3.2 Jours fériés

Cette section permet de configurer une série de dates durant l'année, correspondant à des jours fériés. Pour modifier un jour férié existant, utiliser les touches de défilement pour modifier le mois et le jour, ou sur la touche « AJOUTER » pour insérer une nouvelle date suite à celle sélectionnée. La touche « SUPPRIMER » permet d'éliminer un jour férié de la liste.

REMARQUE : il est indispensable de conserver au moins un jour férié dans la liste, c'est pourquoi le système ne permet pas d'éliminer la dernière ligne de la liste.



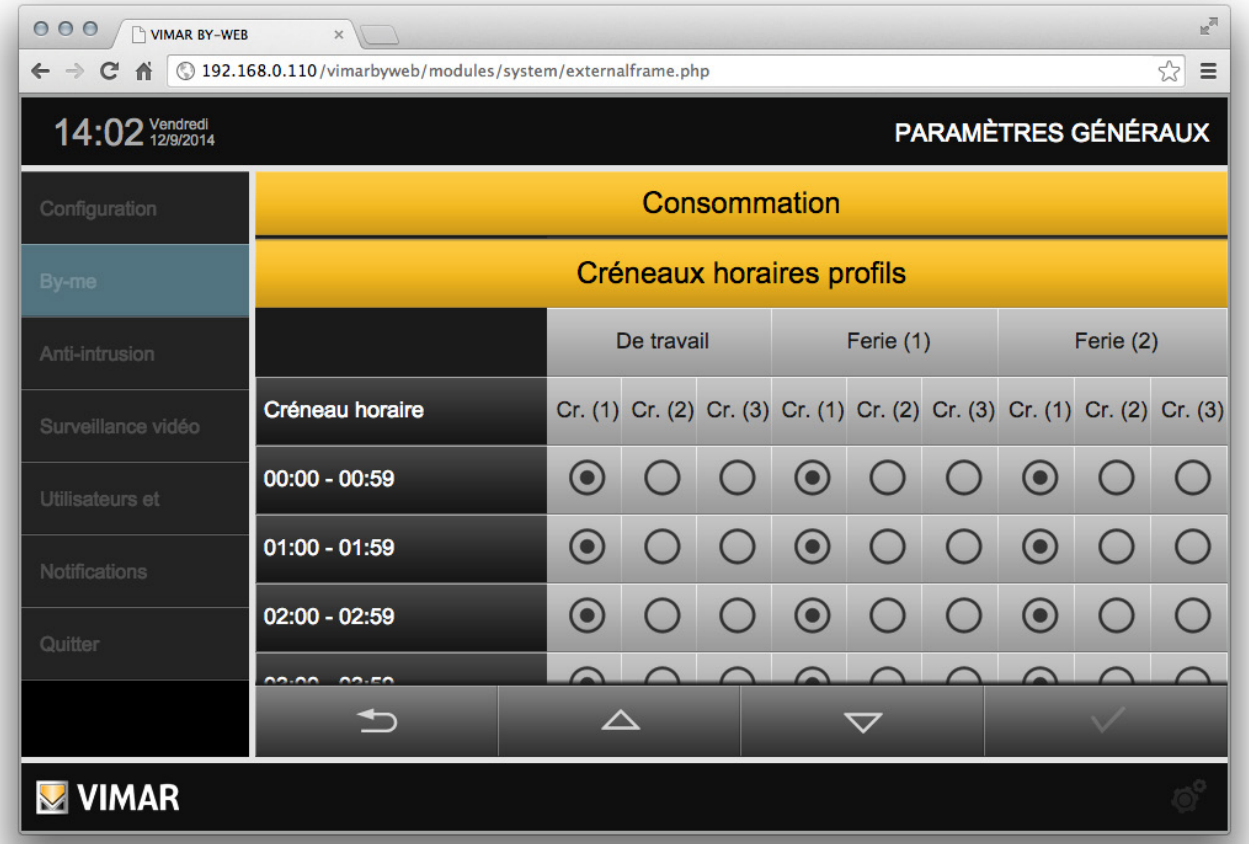
6.2.3.3 Profil des jours de la semaine

Cette section permet d'associer un profil horaire différent à chaque jour de la semaine, avec la possibilité de choisir entre « OUVRABLE », « FÉRIÉ 1 » et « FÉRIÉ 2 ». Utiliser les touches de sélection pour associer chaque jour de la semaine à un profil différent, pour lequel il sera ensuite possible de définir un tarif horaire.

REMARQUE : les jours fériés sont automatiquement associés au profil « FÉRIÉ 2 ».

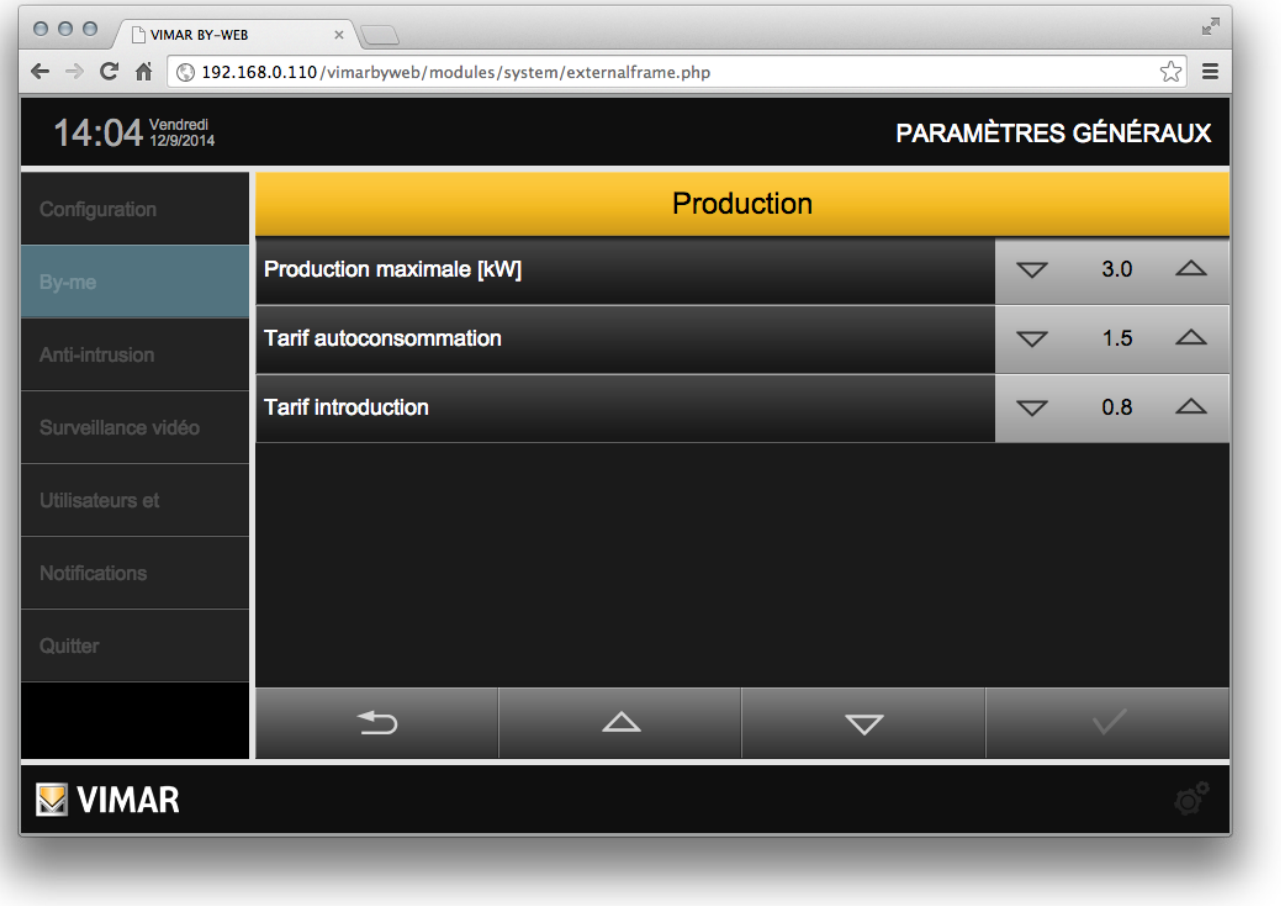
6.2.3.4 Créneaux horaire profils

Cette section permet de définir pour chaque profil (et donc pour chaque jour de la semaine et/ou jours fériés), le tarif de référence relatif à chaque heure. Dans ce cas également, utiliser les touches de sélection pour associer le tarif de référence à chaque horaire, pour chacun des profils.



6.3 Production d’énergie

Pour accéder à la page de configuration de la “Production d’énergie”, sélectionner la section correspondante.



Les paramètres de configuration suivants qui permettent de gérer les différents types de contrats sont prévus:

PRODUCTION MAXIMALE [kWh]	C’est la valeur prévue dans le contrat
TARIF AUTOCONSOMMATION	Représente la valeur prévue dans le contrat pour l’énergie produite par le système qui est consommée par le système lui-même.
TARIF INJECTION	Représente la valeur prévue dans le contrat pour l'énergie produite par le système qui n'étant pas consommée par le système est injectée dans le réseau de distribution.

REMARQUE : les valeurs peuvent être modifiées en utilisant les icônes “augmentation”/”diminution” ou en modifiant le champ numérique.

Important: les calculs économiques effectués par le Web Server sont indicatifs.

6.4 Compteur charges unitaires

Le système By-me permet de mesurer et de sauvegarder les données de consommation des charges unitaires (ou groupes de charges) associés à des compteurs indépendants.

Pour mesurer les consommations des charges unitaires (ou d'un groupe de charges alimentés par la même ligne électrique) il faut utiliser un le compteur d'un des dispositifs Vimar suivants: 01450, 01451, 01455, 01456, 14537, 19537, 20537.

Important: pour gérer, par le Web Server, les compteurs en objet, il faut insérer une carte SD dans le Web Server.

La configuration de ces compteurs est exportée de ETPro dans le fichier XML de configuration. Après l'importation dans le Web Server du fichier XML généré par ETPro, les sections des compteurs "unitaires" configurés seront présents dans la section "Compteurs et compteur d'impulsions" de la page "Monitoring énergie" ("Configurations générales"-> "By-me"->"Monitoring énergie") . En sélectionnant l'icône de modification de l'élément, correspondant à un compteur, il est possible d'accéder à la page qui permet de modifier le texte de la description.

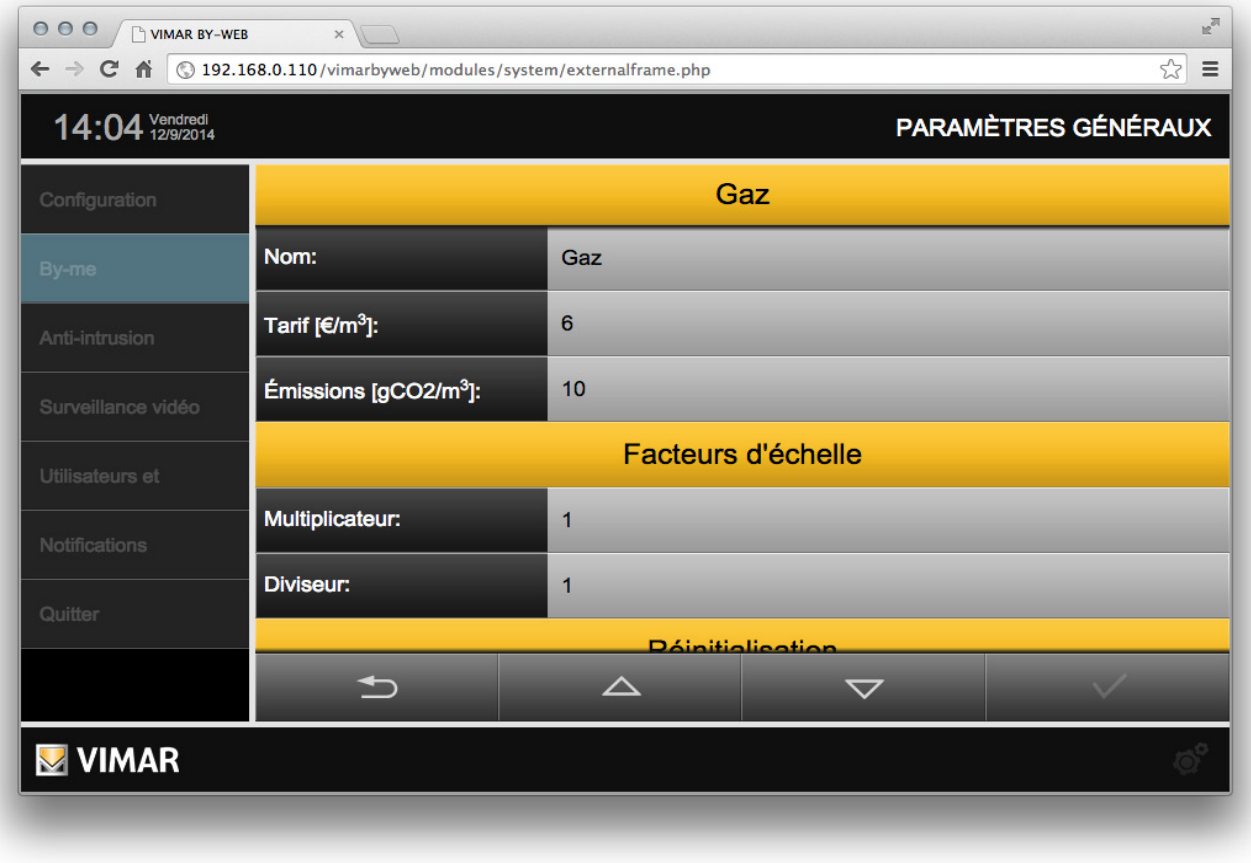
REMARQUE : le tarif pour le calcul du coût associé à la consommation de la charge est celui prévu dans la configuration de la consommation d'énergie électrique (qui tient compte des éventuels créneaux horaires prévus dans le contrat).

6.5 Compteur d'impulsions

Le système By-me permet de contrôler et sauvegarder les données de consommation des compteurs connectés au système By-me par les interfaces compteurs d'impulsions de Vimar (art. 01452 - Interface compteur d'impulsions).

Important: pour gérer, par le Web Server, les compteur en objet, il faut insérer une carte SD dans le Web Server.

La configuration des ces compteurs est exportée de ETPro dans le fichier XML de configuration. Après l'importation dans le Web Server du fichier XML généré par ETPro, les sections des compteurs "unitaires" configurés seront présents dans la section "Compteurs et compteur d'impulsions" de la page "Monitoring énergie" ("Configurations générales"-> "By-me"->"monitoring énergie"). En sélectionnant l'icône de modification de l'élément, correspondant à un compteur d'impulsions, il est possible d'accéder à la page de configuration du Web Server.



Ci-dessous la description des paramètres de configuration prévus par le Web Server.

NOM	Description du compteur, peut être modifier en écrivant le texte désiré.
TARIF [€/m3]	Tarif prévu pour une unité de grandeur mesurée
INJECTION [gCO2/m3]	Valeur de CO2 par unité de grandeur mesurée
Facteurs d'échelle	Les deux facteurs d'échelle (Multiplicateur et Diviseur) prévus par l'interface compteur d'impulsions pour le compteur en question, sont lus par le Web Server directement par l'interface compteur d'impulsions et ne peuvent pas être modifiés par le Web Server.
Réinitialisation: Valeur	À partir du Web Server il est possible de configurer une certaine valeur au compteur d'impulsions. La valeur doit être avec l'unité de mesure prévue par le compteur (ex. m3, litres, ...) et configurée dans l'interface compteur d'impulsions.

7. Utilisateurs et autorisations

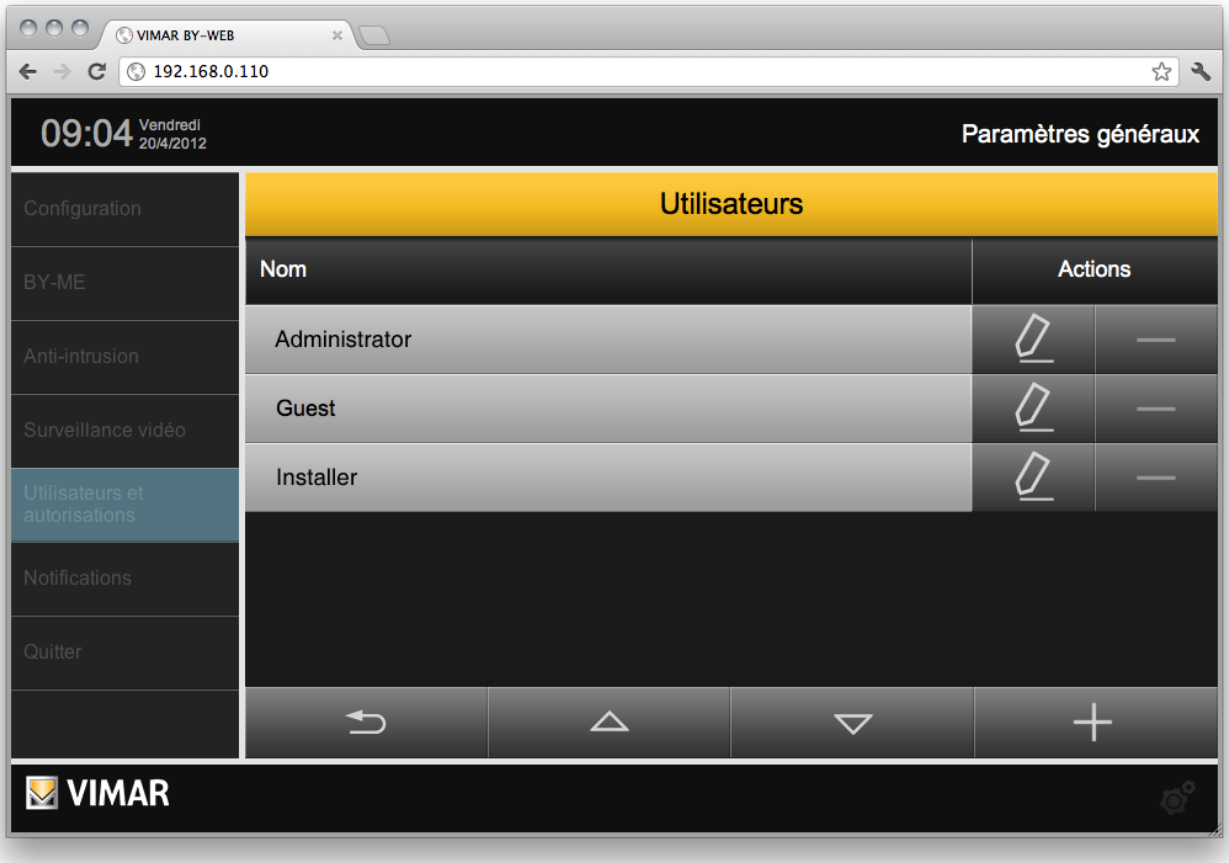
7.1 Avant-propos

By-web permet de configurer les différents compte d'accès à la supervision ainsi que de spécifier les droits conférés. La gestion des utilisateurs et des autorisations s'articulent autour de 3 aspects :

GROUPES UTILISATEURS	Ils représentent les groupes d'utilisateurs homogènes d'autorisations de visualisation et d'exécution des opérations sur By-Web. Prédéfinis : administrateurs, installateurs, utilisateurs.
UTILISATEURS	Les véritables comptes d'accès à By-web. Ils peuvent appartenir à un ou plusieurs groupes, sur héritage des autorisations.
AUTORISATIONS	Les droits de visualisation et d'exécution des opérations pour les différents groupes utilisateurs.

7.2 Utilisateurs

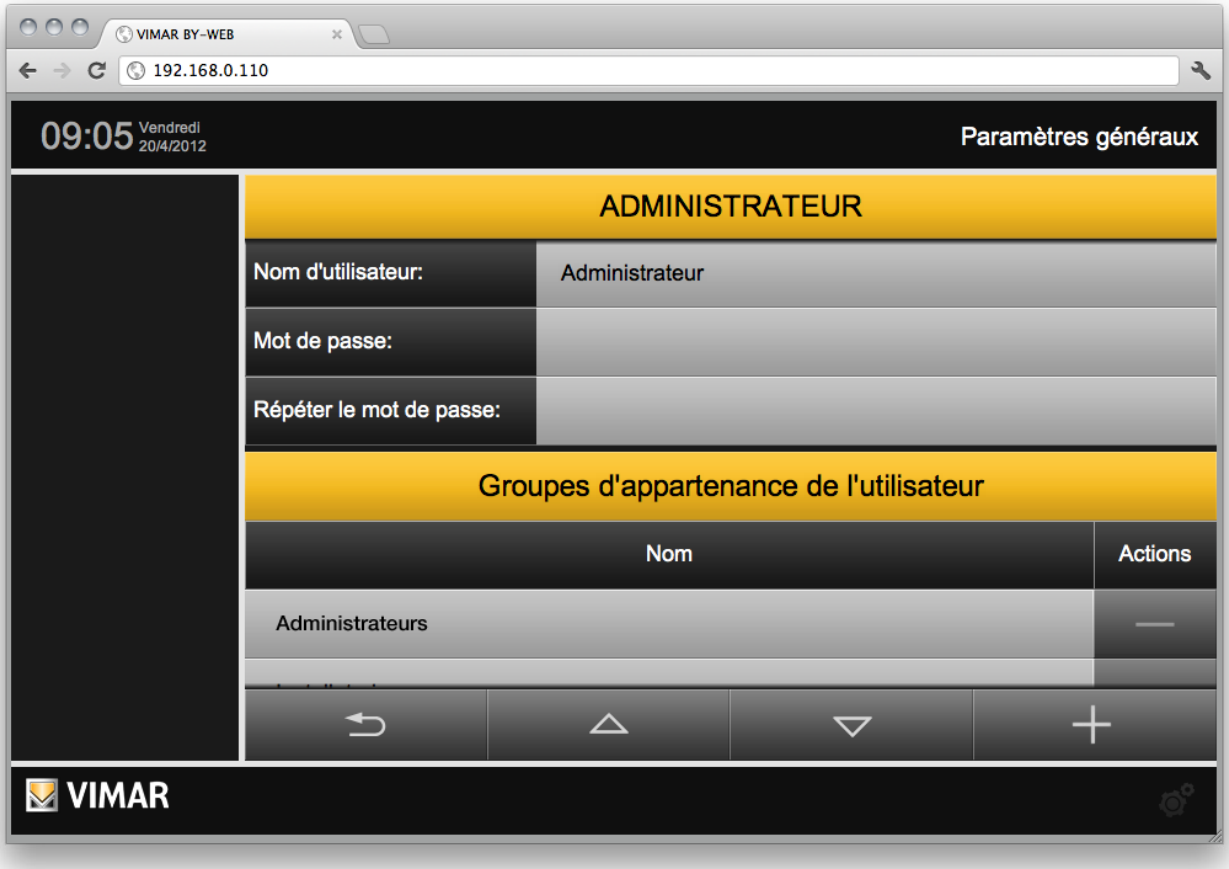
La page « UTILISATEURS » du menu « UTILISATEURS ET AUTORISATIONS » de l'administration permet de configurer les comptes d'accès à By-Web. La figure suivante illustra la page visualisée lors du premier accès, avec les paramètres usine :



Il est possible de créer de nouveaux utilisateurs en utilisant la touche AJOUTER en bas à droite. Dans ce cas, une ligne s'ajoutera à la liste et il sera possible d'indiquer une description associée au nouvel utilisateur (ex : « Martin »).

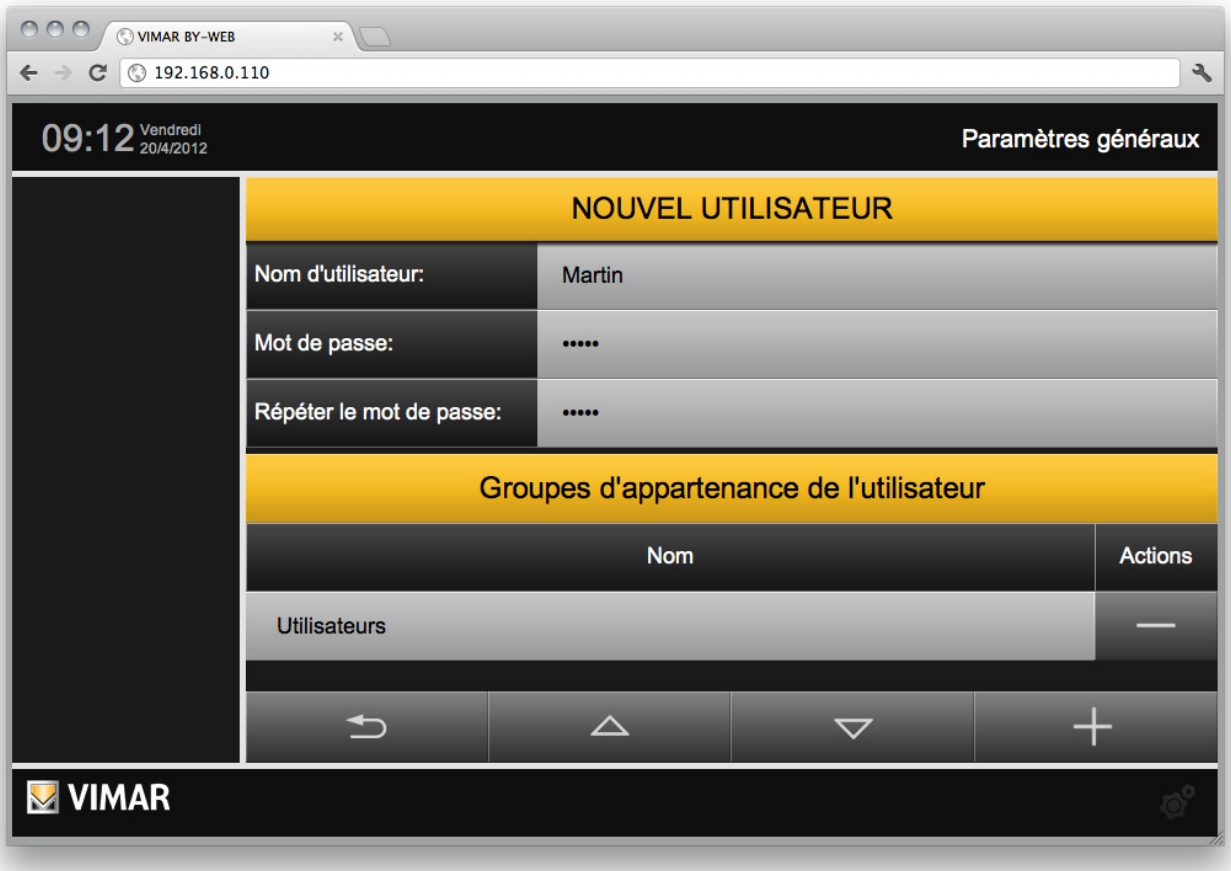
Utilisateurs et autorisations

En utilisant la touche de modification correspondant à un utilisateur, on accède à sa fiche, dans laquelle il sera possible de personnaliser les attributs :



Pour chaque utilisateur, il est nécessaire de spécifier le NOM D'UTILISATEUR - univoque pour chaque utilisateur du système, et le MOT DE PASSE. Ce dernier doit être saisi à deux reprises pour des raisons de sécurité.

La partie inférieure de la page (« GROUPES D'APPARTENANCE DE L'UTILISATEUR ») permet de définir les groupes auxquels l'utilisateur doit être associé. En utilisant la touche AJOUTER, il est possible de faire glisser les groupes concernés dans cette portion de la page en les sélectionnant dans la partie gauche de la page-écran :



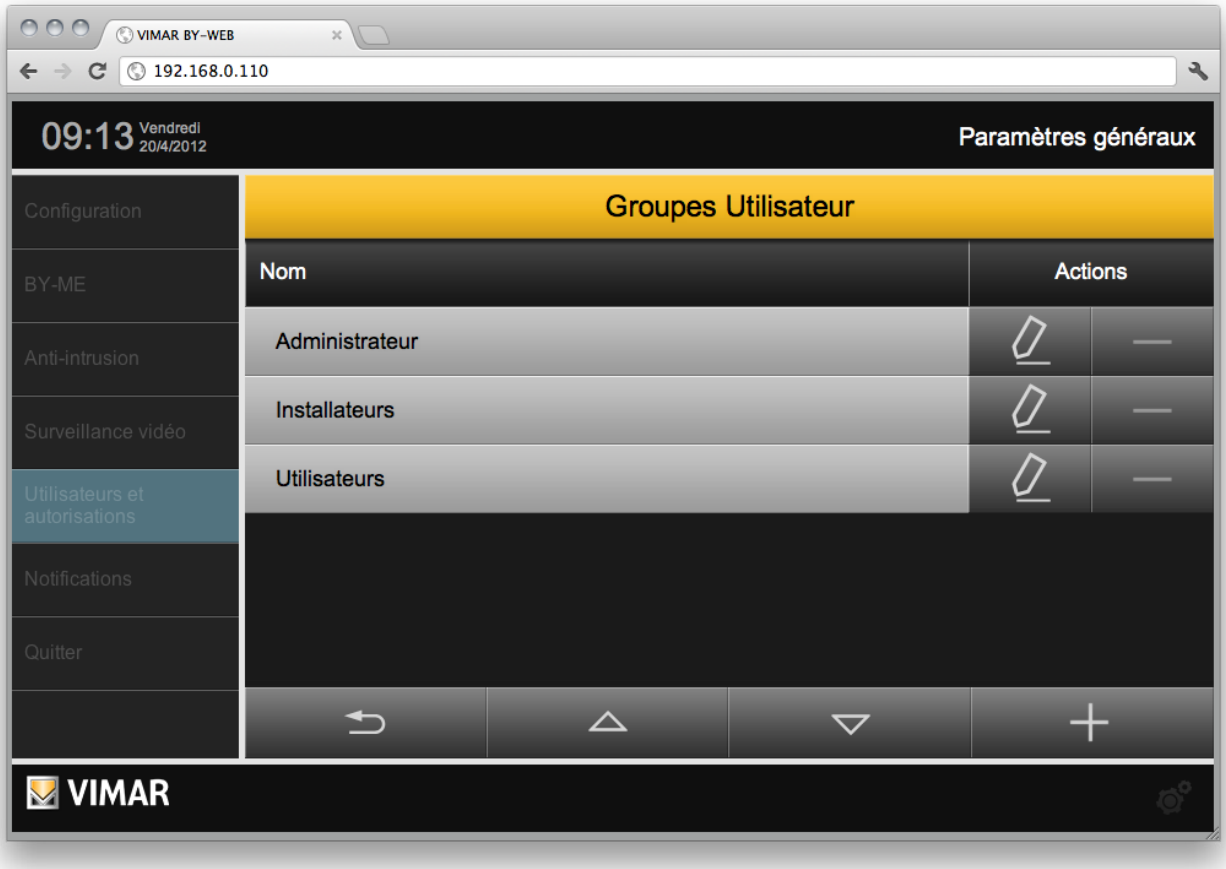
L'utilisateur héritera des autorisations de tous les groupes auxquels il appartient. Il est possible, à tout moment, d'éliminer une association entre un utilisateur et un groupe, ou encore d'éliminer définitivement l'utilisateur en appuyant sur la touche SUPPRIMER.

REMARQUE : il n'est pas possible d'éliminer les utilisateurs prédéfinis et leur association à des groupes prédéfinis. Il est simplement consenti d'en modifier le nom et les autorisations d'accès.

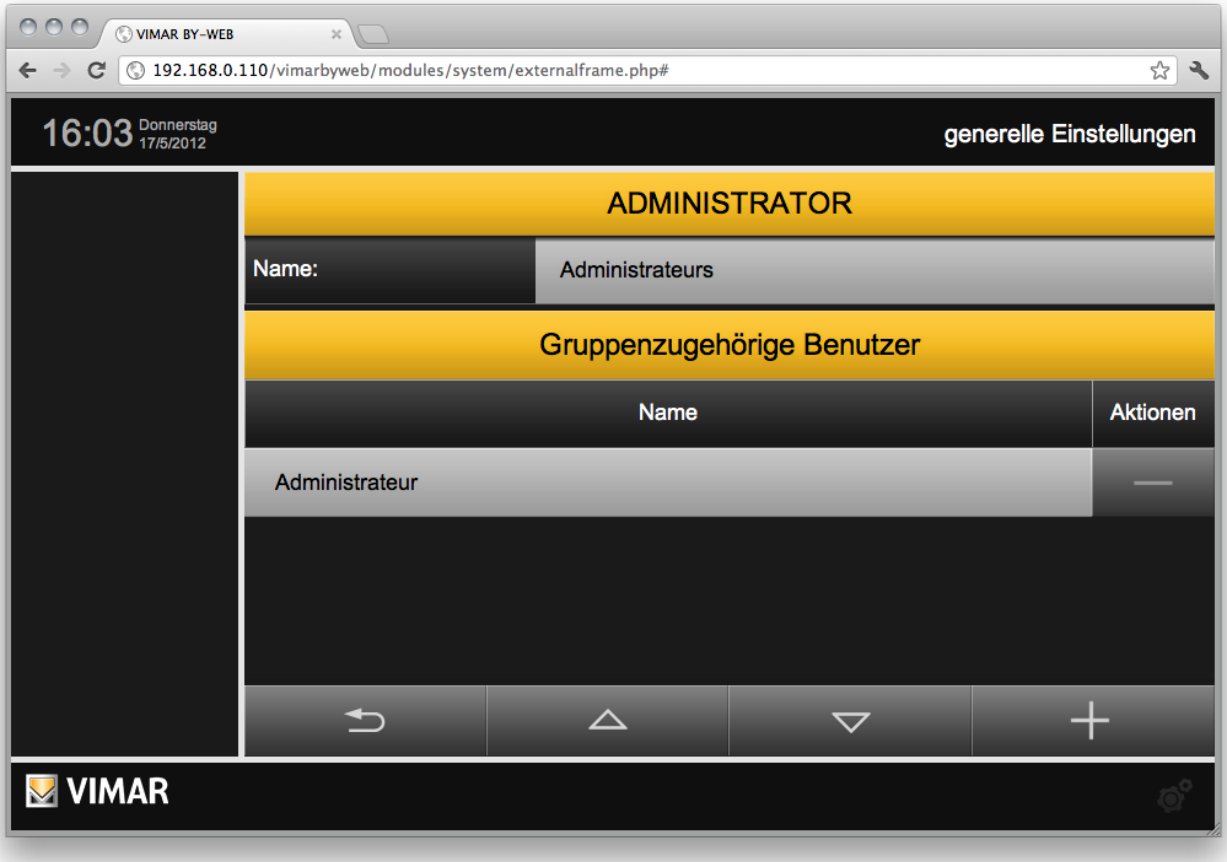
7.3 Groupes utilisateur

La page « GROUPES » de la section « UTILISATEUR ET AUTORISATIONS » de l'administration permet de gérer les groupes utilisateurs. De même que pour les utilisateurs, cette page permet de créer de nouveaux groupes ou de modifier ceux existant.

Avec la touche AJOUTER, il est possible de créer un nouveau groupe utilisateur. La description peut être directement modifiée dans la liste, simplement en éditant la description prédéfinie.



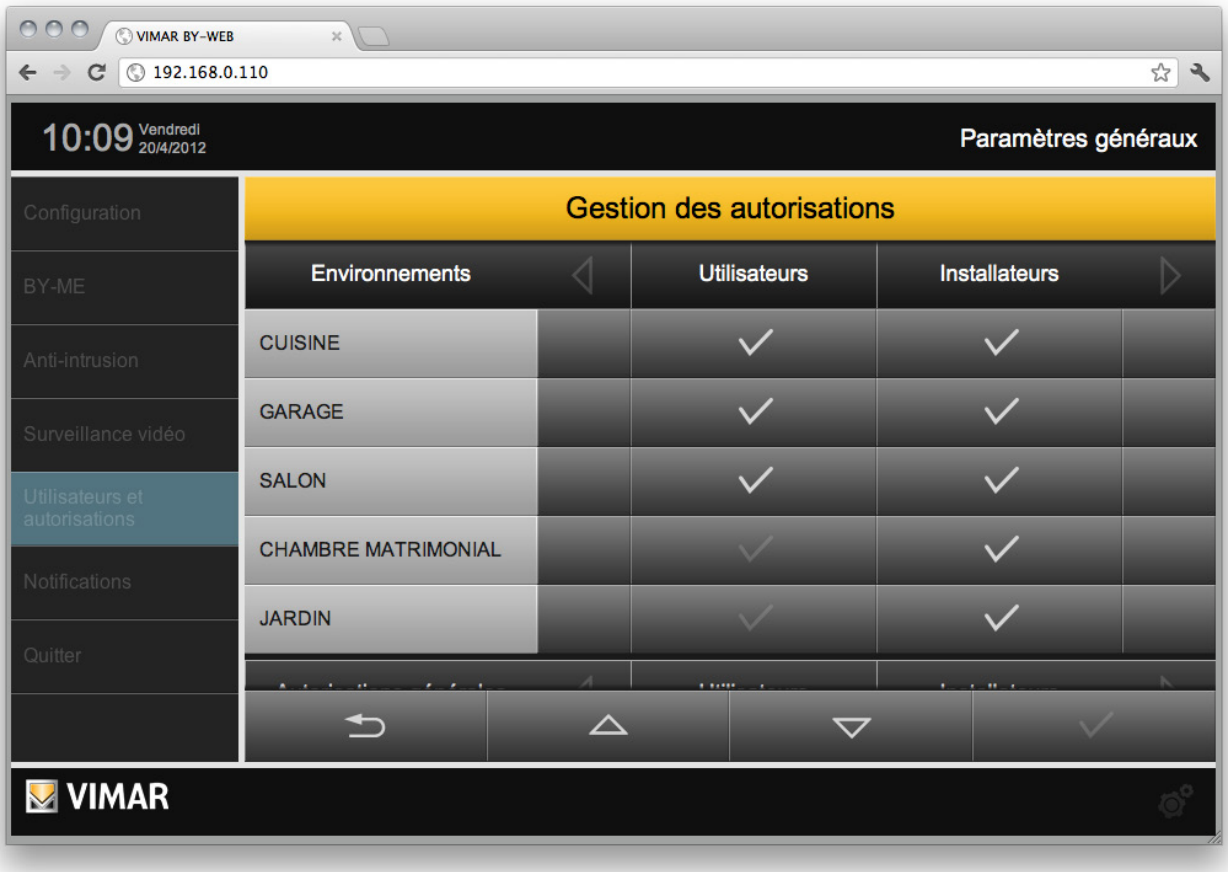
En appuyant sur la touche « MODIFIER », on accède à la fiche du groupe utilisateur :



Cette page permet uniquement de modifier la description du groupe (si cela n'a pas déjà été effectué depuis la liste des groupes) et d'associer les utilisateurs à ce même groupe, opération similaire à celle effectuée depuis la fiche de chaque utilisateur unique.

7.4 Autorisations

La page « AUTORISATIONS » permet de spécifier pour chaque groupe utilisateur, les autorisations relatives à la visualisation des environnements et à l'exécution de certaines opérations. La page se présente comme illustré dans la figure ci-après :



La première partie est constituée d'un tableau contenant la liste de tous les environnements présents dans le projet, répartis en lignes, et les groupes utilisateurs dans les colonnes. En cliquant sur les cases de sélection, il est possible d'activer ou de désactiver les différents groupes utilisateurs et d'accéder aux environnements correspondants. Lors de la création, les environnements sont visibles par tous les groupes utilisateurs.

REMARQUE : il n'est pas possible de modifier les autorisations du groupe ADMINISTRATEURS, lequel possède les droits d'accès à tous les environnements, les droits pour effectuer toutes les opérations ainsi que la possibilité d'accéder à la section de configuration UTILISATEURS ET AUTORISATIONS.

La partie inférieure de la page permet de définir les droits d'exécution conférés à un groupe utilisateur. Plus particulièrement, By-Web prévoit les droits suivants :

AFFICHER LE STATUT SAI SANS PIN	Permet de visualiser le statut du système anti-intrusion avant de saisir le code PIN valide.
OPÉRATIONS DE NIVEAU 1	Accès aux fenêtres pop-up de configuration des thermostats et des évènements, apprentissages des scénarios, configuration de la mémoire de la radio FM.
OPÉRATIONS DE NIVEAU 2	Accès aux fenêtres pop-up de configuration de la programmation temporelle des thermostats et des évènements.
NIVEAU 1 TECHNICIEN	Accès à la fenêtre de configuration du régulateur climatique. Permet de modifier les valeurs de consigne du mode courant du régulateur climatique.
NIVEAU 2 TECHNICIEN	Accès à la fenêtre de configuration du mode de fonctionnement et de la programmation temporelle du régulateur climatique.

Également dans ce cas, utiliser les cases de sélection pour habiliter ou non les différents groupes utilisateurs à l'exécution des actions correspondantes. Les utilisateurs sans droits spécifiques ne pourront pas effectuer les opérations correspondantes, sauf utilisation de l'autorisation d'un autre utilisateur (appartenant à un groupe disposant des autorisations nécessaires) en utilisant la fenêtre de connexion prévue à cet effet.

7.4.1 Niveaux et fonctions

NIVEAU 0 (PAR DÉFAUT) :

- Visualisation du statut/commande des actionneurs
  Statut + commande : actionneurs relais, actionneurs stores, actionneurs gradateur (tous les dispositifs faisant partie des fonctions Éclairage, Stores)
- Visualisation du statut des thermostats
  Statut des thermostats. Visualisation des icônes des thermostats dans les fenêtres des environnements et des fonctions. (en cliquant sur l'icône, la fenêtre pop-up s'affiche, demandant la « promotion ») à un niveau disposant de privilèges supérieurs.
- Activation des scénarios
- Visualisation des télécaméras IP

NIVEAU 1 :

- Utilisation des fonctions d'Economiseur d'énergie
- Thermostat, configuration des modalités de fonctionnement
  Modes de fonct. (OFF, OFF à temps, MANUEL, PROGRAMMÉ,…), point de consigne des diverses modalités. De fait, ce niveau permet d'ouvrir la fenêtre pop-up de thermostat et d'effectuer tous les réglages visibles dans la fenêtre pop-up, SAUF la configuration du programme horaire, lequel prévoit l'ouverture d'une fenêtre pop-up spéciale. Sur demande de modification du programme horaire, une fenêtre pop-up s'affiche sur l'écran pour demander la promotion au niveau supérieur.
- Configuration des événements
- Lecture/Pause évènement
- Apprentissage scénario
- Contrôle des charges, Configuration du mode « ON forcée
- Syntonisation FM, Configuration de la mémoire de stations
- Modifier la disposition des Widgets par pièce avec la fonction «Carte

NIVEAU 2 :

- Thermostat, Paramètres avancés
- Programme horaire hebdomadaire, fenêtre pop-up de config. climat (changement de saison, changement de l'unité de mesure)
- Évènements, Paramètres avancés, Temporisation (programme hebdomadaire, cyclique,…)

NIVEAU 0 TECHNICIEN :

- Affichage de l'état des régulateurs climatiques
  Affichage des icônes des régulateurs climatiques dans les fenêtres de Pièces et Fonctions En cliquant avec la souris sur l'icône, une fenêtre apparaîtra demandant une « autorisation » d'accéder à un niveau de privilèges supérieur.
  Ce niveau est assigné par défaut au groupe « Utilisateurs ».

NIVEAU 1 TECHNICIEN :

- Régulateur climatique, configuration du mode saisonnier et du point de consigne.
  Point de consigne des modes Confort et Economy (si configurés comme modes courants). Ce niveau permet d'ouvrir la fenêtre du régulateur climatique, d'accéder à la fenêtre de réglage du mode saisonnier (si prévu par le système) et de modifier les points de consigne du mode courant (si Confort ou Economy). En cas de demande de modification du programme horaire ou de la modalité de fonctionnement (Auto, Confort, Economy, Off), la fenêtre contextuelle d'autorisation d'accès vers un niveau supérieur s'affichera.

NIVEAU 2 TECHNICIEN :

- Régulateur climatique, configuration du mode de fonctionnement et du programme horaire.
  Ce niveau permet d'accéder à la fenêtre de réglage du mode de fonctionnement (Auto, Confort, Economy, Off) et à celle de configuration du programme horaire (avec points de consigne relatifs).

7.4.2 Technique de « promotion» à des niveaux d'autorisation supérieurs

Lorsqu'un utilisateur souhaite accéder à une fonction non autorisée par son niveau d'autorisation, une fenêtre pop-up s'affichera sur l'écran pour demander l'insertion d'une autorisation (mot de passe). Si le mot de passe d'un utilisateur disposant de l'autorisation adéquate pour accéder à la fonction est inséré, il sera alors procédé à la « promotion » du niveau de l'utilisateur.

Une fois l'opération terminée et l'utilisateur revenu à la fenêtre de départ, les droits de ce dernier seront restaurés.

7.4.3 Association Groupes-Autorisations

Groupes	0	1	2	0 Technicien	1 Technicien	2 Technicien	Environnement {1}	Environnement {2}	....	Environnement n°
Administrateurs	X	X	X	X	X	X	X	X	X	X
Installateurs	X	X	X	X	X	X	X	X	X	X
Utilisateurs	X			X			X	X	X	X
....	....	....	....	....	....	....	....	....	....	....

Pour les groupes autres que le groupe Administrateurs, il reste dans tous les cas possible de modifier les autorisations associées.

7.4.4 Groupe Administrateurs

Le groupe ***Administrateurs*** possède tous les droits et ces derniers ne peuvent lui être retirés. Ce groupe n'apparaît pas dans la liste des autorisations (étant donné l'impossibilité d'effectuer des modifications d'autorisation dans ce groupe).

Il est cependant visible dans la liste des groupes dans la fenêtre de création des utilisateurs, pour l'association utilisateur/groupes.

Le niveau 2 (avancé) est associé par défaut au groupe ***Administrateur*** et ne peut être modifié.

Le groupe ***Administrateurs*** est le seul groupe disposant de tous les droits de gestion « administrative » (gestion utilisateurs) du Web Server.

Le niveau 2 technicien (avancé) est associé par défaut au groupe ***Administrateurs*** et ne peut pas être modifié.

7.4.5 Groupe Installateurs

Le groupe ***Installateurs*** possède les droits d'administration du groupe ***Administrateurs*** **SAUF** ceux relatifs à la gestion des utilisateurs. Il est possible de modifier le niveau d'autorisation de ce groupe et la liste des environnements visibles par le groupe.

Le niveau 2 (avancé) est associé par défaut au groupe ***Installateurs*** mais peut être modifié.

Le niveau 2 technicien (avancé) est associé par défaut au groupe ***Installateurs*** mais peut être modifié.

7.4.6 Groupe Utilisateurs

Le groupe ***Utilisateurs*** possède très peu d'autorisations d'administration : outre la modification de la langue et la configuration date/heure.

Il est possible de modifier le niveau d'autorisation de ce groupe et la liste des environnements visibles par le groupe.

Le niveau 0 (base) est associé par défaut au groupe ***Utilisateurs*** mais peut être modifié.

Le niveau 0 technicien (basic) est associé par défaut au groupe ***Utilisateurs*** mais peut être modifié.

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

Pour l'association du Multimedia Touch 10 avec les Web Server (code 01945-01946), consulter le manuel de l'installateur du Multimedia Touch 10.

Lors de l'association entre le Web Server et le Multimedia Touch 10, un utilisateur spécifique au Multimedia Touch 10 sera créé. Son nom peut être défini par l'utilisateur, et permet au Multimedia Touch 10 de procéder à la connexion automatique à chaque lancement de l'application domotique. Cet utilisateur peut être utilisé UNIQUEMENT par le Multimedia Touch 10.

Pour éliminer correctement cet utilisateur du Web Server (élimination de l'association entre Multimedia Touch 10 et Web Server) il faut obligatoirement effectuer la Réinitialisation de la configuration d'origine de la configuration du Web Server par le menu de configuration du Multimedia Touch 10".

Dans le menu de configuration du Web Server il existe aussi la possibilité d'afficher la liste de Multimedia Touch 10 configurés dans le Web Server et éventuellement les éliminer de cette liste. Pour cela aller à la page "Configurations générales"->"By-me"-> "Multimedia Touch 10" et appuyer sur le bouton "-" de l'utilisateur Multimedia Touch 10 à éliminer du Web Server (à utiliser UNIQUEMENT s'il est impossible d'utiliser la procédure d'élimination prévue de la configuration du Multimedia Touch 10.

Pour modifier les privilèges de l'utilisateur prédéfini du VST10, il suffit d'accéder au Web Server à l'aide d'un navigateur depuis un PC, de se connecter en qualité d'**Administrateur** et d'accéder aux PARAMÈTRES GÉNÉRAUX, depuis le menu déroulant, UTILISATEURS ET AUTORISATIONS, sélectionner AUTORISATIONS et modifier les privilèges du groupe relatif au Multimedia Touch 10.

Il n'est pas consenti de procéder à la configuration des Paramètres généraux du Web Server depuis le Multimedia Touch 10.

NOTE: Il est uniquement possible de modifier la langue du Web Server depuis le Multimedia Touch 10.

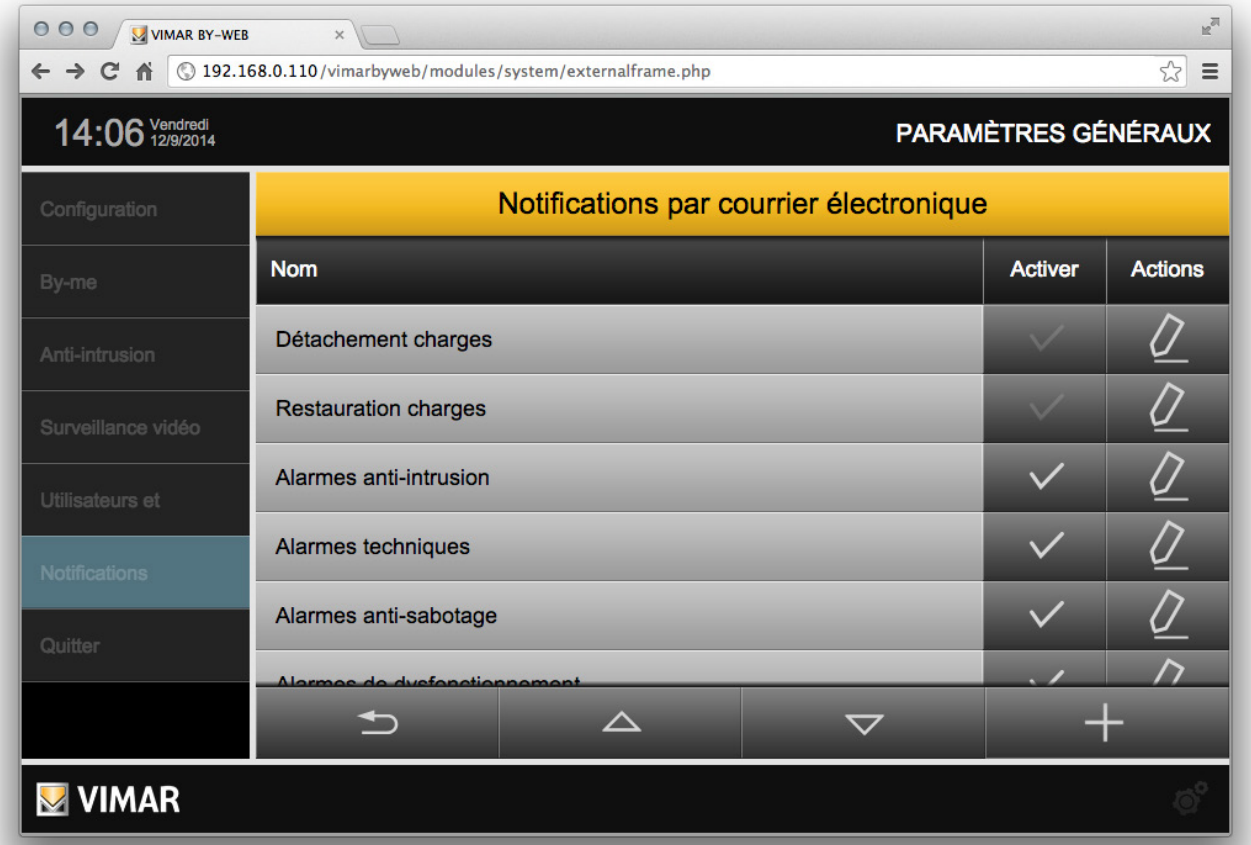
À partir de la version du logiciel 1.4.08, l'écran tactile vidéo multimédia 10 pouces propose une section consacrée à la gestion des caméras.

Si un Multimedia Touch 10 équipé de cette version (ou supérieure) se connecte à un Web Server avec la version 1.5 (ou supérieure), l'option « Surveillance vidéo » ne figurera pas au menu principal car la gestion des caméras se fait à partir de la section spécifique de l'application du Multimedia Touch 10.

L'option « Surveillance vidéo » s'affiche en revanche en cas de connexion au Web Server d'un client autre que Multimedia Touch 10.

9. Notifications par e-mail

La page “AVERTISSEMENTS” du menu administration (“Configurations générales->”Avertissements”) permet de configurer les avertissements par poste électronique à la suite d’évènements particuliers gérés par le Web Server.



Pour chaque type d’évènement géré par le Web Server une ligne dans le tableau de la page de configuration est prévue.

Pour chaque type d’évènement il est possible d’activer la réception d’avertissement par e-mail et accéder à la page de configuration.

Pour chaque type d’évènement il est possible de définir un groupe de destinataires spécifique, objet de l’e-mail et texte de l’e-mail.

Ci-dessous la liste de types d’évènements qu’il est possible associer de manière indépendante à la réception d’un avertissement par e-mail:

Type d’évènement	Description
Détachement charges	Informe du détachement de la première charge de la part du dispositif de contrôle des charges. Le système de contrôle des charges est entré en action à cause d’une consommation supérieure au seuil configuré. **Note**: tale funzionalità prevede che nell’impianto sia presente un dispositivo di controllo carichi e che sia correttamente configurato nel Web Server.
Restauration charges	Informe de la reprise de la dernière charge de la part du dispositif de contrôle des charges. Le système de contrôle des charges a remis en marche toutes les charges précédemment détachées: les consommations sont rentrées dans la limite du seuil configuré. **Note**: cette fonction prévoit que dans le système il y ait un dispositif de contrôle des charges et qu’il soit correctement configuré dans le Web Server.
Alarmes anti-intrusion	Informe d’une alarme de type “Intrusion” de la part du système anti-intrusion By-me. **Note**: cette fonction prévoit que dans le système il y ait un dispositif anti-intrusion et qu’il soit correctement configuré dans le Web Server.
Notification des états By-alarm	Notification des évènements d’état envoyés sur la centrale du système anti-intrusion By-alarm.
Notification des découpages By-alarm	Notification des passages d’état activation/alarme des découpages. Il est possible de configurer les passages d’état qui doivent être notifiés pour chaque découpage configuré dans le système By-alarm.

Notifications par e-mail

Alarmes techniques	Informe d'une alarme de type "Technique" de la part du système By-me. **Note**: cette fonction est disponible uniquement si elle est prévue par le système By-me et si elle est correctement configurée dans le Web Server.
Alarmes anti-sabotage	Informe d'une alarme de type "Tamper" de la part du système anti-intrusion By-me. **Note**: cette fonction prévoit que dans le système il y ait un dispositif anti-intrusion et qu'il soit correctement configuré dans le Web Server.r.
Alarmes de dysfonctionnement	Informe d'une alarme de type "Dysfonctionnement du dispositif" de la part du système anti-intrusion By-me. **Note**: cette fonction prévoit que dans le système il y ait un dispositif anti-intrusion et qu'il soit correctement configuré dans le Web Server.
Avertissements vidéophone	Informe sur la réception d'un nouveau message vidéo. **Note**: cette fonction est disponible si dans le système il y a au moins un Multimedia Touch 10, connecté au système vidéophone 2 fils et si le Multimedia Touch 10 a été correctement configuré dans le Web Server (voir le chapitre du manuel sur les messages vidéo).
Notificaciones acerca de eventos de cambio de estado de objetos de 1 bit	Es posible recibir notificaciones por email relacionadas con el paso a un estado predeterminado de los objetos de 1 bit, pertenecientes a la categoría "Automatización" o a la de los objetos de integración KNX (1 bit). **Note**: esta función se ha introducido a partir de la versión 2.1 del software del Web Server. Para la configuración de estas notificaciones, consulte el apartado "Notificaciones acerca de eventos de cambio de estado de objetos de 1 bit".

Pour chaque points reporté dans le tableau précédent les icônes suivantes sont disponibles:

	Permet d'activer l'avertissent: activer/désactiver par "toggle" L'activation est illustrée avec l'icône:  Désactivé  Activé
	En appuyant sur le bouton on accède à la page de configuration des paramètres pour l'envoi des emails d'avertissements liés à l'évènement: • Adresse/s de destination (séparer les adresses avec «;») • Adresse/s en copie (séparer les adresses avec «;») • Objet du message • Texte du message **Note**: le détail de l'avertissement, si prévu, sera mis à la suite du texte d'avertissement automatique dans cette page, nous vous conseillons donc de saisir un texte générique qui identifie le message de poste électronique provenant du système By-me à la suite de l'évènement. La configuration des Notifications des découpages anti-intrusion By-alarm comporte d'autres champs de configuration : se référer au chapitre suivant Notification des découpages anti-intrusion By-alarm.

Notifications des états By-alarm

Le serveur web permet de notifier via e-mail les évènements d'état suivants envoyés par la centrale By-alarm :

- Modifier état des secteurs
- Tamper centrale
- Absence tension centrale
- Batterie faible
- Batterie absente
- Absence ligne PSTN
- Absence ligne GSM
- Jamming ligne GSM
- Tamper claviers (si au moins un clavier est en alarme Tamper)
- Tamper du module entrées (si au moins une extension est en alarme Tamper)
- Tamper du module sorties (si au moins une extension est en alarme Tamper)
- Tamper zones (si au moins une zone est en alarme Tamper)
- Tamper activateurs (si au moins un activateur est en alarme Tamper)
- Batterie des dispositifs radio faible (si au moins un dispositif présente la batterie faible)
- Absence de communication avec la centrale

Notifications par e-mail

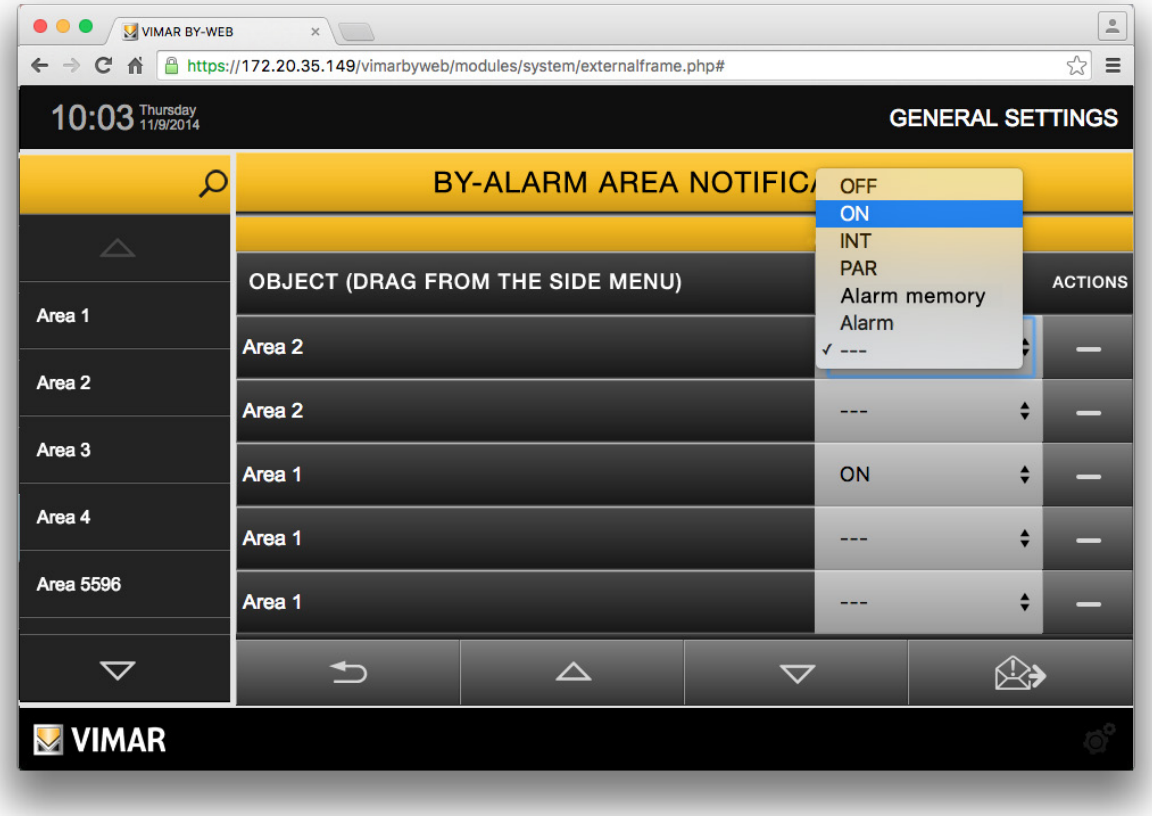
Notification des découpages By-alarm

Le serveur Internet permet une notification flexible des changements d'état spécifiques par mail pour chaque découpage configuré, de la façon suivante.

1. Saisir les données nécessaires à l'envoi par mail : destinataire, copie à, objet, texte.
2. Cliquer-glisser de la colonne de gauche sous la ligne OBJET (CLIQUER-GLISSER DEPUIS LE MENU LATÉRAL) le découpage dont on souhaite notifier un état spécifique ; une ligne s'affiche dans la liste en bas de la page.
3. Sélectionner le bouton de la ligne correspondant à la colonne CONDITION. Un menu déroulant s'affiche qui permet de sélectionner l'état à notifier par mail.

Les états possibles sont les suivants.

a. OFF
b. ON
c. INT
d. PAR
e. Mémoire alarmes
f. Alarme
g. ---



Il est possible de supprimer une ligne associée à un découpage après l'avoir créée en appuyant sur le bouton "-" situé à droite de la ligne.

Notificaciones acerca de eventos de cambio de estado de objetos de 1 bit

El Web Server permite notificar por email el paso a un estado predeterminado de un objeto de 1 bit (perteneciente a la categoría “Automatización” o a la de los objetos de integración KNX), con la posibilidad de configurar el texto que describe la notificación.
Con el procedimiento de configuración que se describe a continuación se crea una asociación entre una notificación email y el paso a un estado específico de un objeto de 1 bit.
Por ejemplo, si se desea que el Web Server envíe un email de notificación cuando un objeto de 1 bit pasa al estado 1 (por ejemplo, notificación de apertura de la puerta) y también cuando vuelve al estado 0 (por ejemplo, al cerrar la puerta), deben crearse dos notificaciones distintas, con los textos y la condición correspondientes.

La configuración incluye los pasos siguientes:

1. Para crear una nueva notificación, pulse el botón “+” situado abajo a la derecha de la ventana “Notificaciones por correo electrónico”: se crea así una nueva línea en la lista de notificaciones con el nombre “Nueva notificación email”.

   Es posible editar el nombre de la notificación colocando el cursor en el campo “Nombre” de la línea correspondiente y tecleando el texto.

   Después de la creación, la notificación está desactivada: para activarla, pulse el botón “v” (Activar/Desactivar) de la línea correspondiente.
2. Pulse el botón de edición, de la línea correspondiente, para acceder a la página de configuración de la notificación.
3. Introduzca los datos necesarios para el envío del email: Destinatario, posible CC, Asunto, texto descriptivo del evento notificado.
4. Arrastre, desde la columna de la izquierda hasta la parte de la página debajo de la línea “OBJETO (ARRASTRAR DEL MENÚ LATERAL”) el objeto cuyo estado específico desea notificar; aparece una línea en el listado de la parte inferior de la página.

   Note: para cada notificación creada es posible asociar solo un objeto de 1 bit (de las categorías descritas previamente).

   Es posible eliminar el objeto introducido pulsando el botón “-” en la parte derecha de la línea.
5. Configure el estado del objeto que desea notificar, mediante el menú desplegable “Condición” en la línea del objeto arrastrado.
6. Después de completar la configuración de la notificación, es posible enviar un email de prueba pulsando el botón abajo a la derecha (prueba envío email).

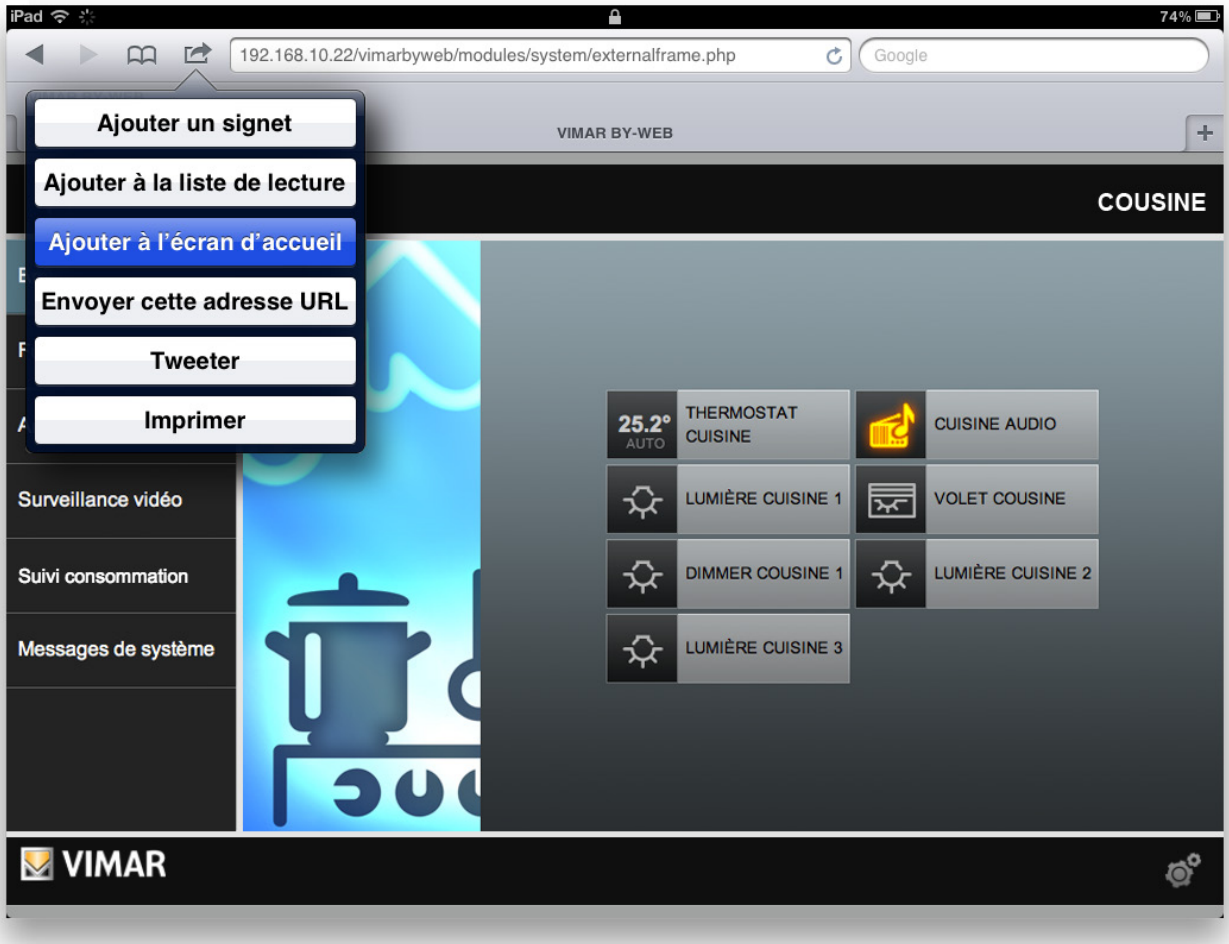
Para eliminar una notificación, pulse el botón “-” situado abajo a la derecha de la ventana “Notificaciones por correo electrónico”.
Para activar o desactivar una notificación, utilice el botón “v” (Activar/Desactivar) de la línea correspondiente.

10. Mobile

En cas d'utilisation du Web Server depuis des dispositifs mobiles ou depuis le 21553.2, il est possible d'accéder uniquement à certaines fonctions du menu Paramètres généraux.
Le menu s'affiche intégralement mais la majeure partie des fonctions sont grisées et ne peuvent être sélectionnées. Il est cependant possible d'utiliser les menus CONFIGURATION et la fonction QUITTER.
Depuis le menu déroulant CONFIGURATION, il est possible d'accéder à la page-écran pour sélectionner la langue du Web Server (voir chapitre 2.2), les autres options ne sont pas disponibles.

10.1 Ajouter à Accueil

La fonction AJOUTER À ACCUEIL permet de créer un lien direct à la page web du Web Server.
Une icône sur la page d'ACCUEIL sera créée. Lors de son activation, la page du Web Server s'affichera dans une fenêtre du navigateur.
Pour créer l'icône avec le lien, procéder comme suit :
1. Ouvrir le navigateur Safari.
2. Saisir l'adresse IP du Web Server (ex : pour l'accès depuis LAN, l'adresse par défaut est http://192.168.0.110).
3. Appuyer sur la touche des options située en haut à gauche et sélectionner l'option « Ajouter à Accueil » depuis le menu déroulant.



Une fois ces simples opérations effectuées, une fenêtre pop-up s'affiche, dans la laquelle il est possible de modifier le nom de l'application. Puis, appuyer sur la touche Entrée du clavier virtuel.

L'application créée s'affiche sur la page-écran Accueil du dispositif mobile , appuyer sur l'icône pour activer la communication avec le Web Server.

11. ByWeb Tools de Vimar

11.1 Avant-propos

ByWeb Tools est un pack logiciel de Vimar permettant les fonctions suivantes :

- Réduction de la durée de la procédure d'importation du fichier XML du système, en utilisant une procédure d'importation spécifique prévoyant l'exécution d'une application Vimar spécifique sur l'ordinateur à partir duquel l'opération est effectuée.
- Affichage de flux vidéo RTSP des caméras IP de surveillance vidéo configurées sur le Serveur Web.
  Il est nécessaire d'installer ByWeb Tools sur tous les ordinateurs à partir desquels il est accédé au Serveur Web et sur lesquels il est désiré utiliser l'une ou les deux fonctions décrites.

Il est nécessaire d'installer ByWeb Tools sur tous les ordinateurs à partir desquels il est accédé au Serveur Web et sur lesquels il est désiré utiliser l'une ou les deux fonctions décrites.

ByWeb Tools est disponible pour les systèmes d'exploitation suivants : Microsoft Windows.

Le pack d'installation de ByWeb Tools de Vimar est téléchargeable directement sur le Serveur Web, par conséquent aucune connexion Internet n'est nécessaire.

11.2 Conditions préalables

Avant de procéder à l'installation de ByWeb Tools de Vimar, vérifier d'avoir au préalable installé les logiciels suivants :

- JAVA de Oracle (Version 8) : requis pour l'importation du projet By-me. Si seule fonction de visualisation des flux vidéo RTSP est désirée, l'installation de JAVA n'est pas nécessaire.
- VLC de VideoLAN : requis pour la visualisation des flux vidéo RTSP. Si seule la fonction relative à l'importation du projet du système est désirée, l'installation de VLC n'est pas nécessaire.

S'il est procédé à l'installation de ByWeb Tools sans avoir installé les logiciels mentionnés ci-dessus, et qu'il est procédé ultérieurement à l'installation de ces derniers, ByWeb Tools devra être réinstallé.

IMPORTANT : Il est nécessaire de disposer de privilèges d'administrateur sur l'ordinateur sur lequel sera installé ByWeb Tools.
Pour le bon fonctionnement de ByWeb Tools, il est nécessaire que le Serveur Web dispose des certificats SSL adaptés. Si cela n'est pas déjà fait, enregistrer à nouveau les paramètres de réseau du Serveur Web en vous assurant qu'il est connecté à internet (Paramètres généraux/Setup/Réseau).

11.3 Installation

L'installation de ByWeb Tools peut être lancée des différentes manières suivantes :

- Demande d'installation automatique (par le biais d'un message d'avertissement), si celle-ci n'a pas encore été effectuée, au démarrage de la procédure d'importation du fichier XML du système (également en cas de mise à jour du logiciel du Serveur Web, la réimportation du fichier XML de système enregistré sur le Serveur Web est nécessaire durant la dernière importation du fichier XML de système).
- Demande d'installation automatique (par le biais d'un message d'avertissement), si celle-ci n'a pas encore été effectuée, lors de la demande de visualisation d'une caméra IP de surveillance vidéo fournissant un flux vidéo RTSP (ex. caméras vidéo IP Elvox).

12. Intégration des dispositifs KNX dans le système By-me

12.1 Préambule

Le système By-me ayant de nombreux points communs avec la structure KNX, l'interaction entre les deux systèmes peut être réalisée sans interface physique.

Certaines fonctions des dispositifs KNX peuvent être transposées dans le système By-me (avec les dispositifs et les interfaces utilisateur évolués, notamment les écrans tactiles et les serveurs Internet).

Sur le plan physique et électrique, les dispositifs By-me et KNX peuvent être reliés au même câble bus mais ils conservent leur propres formats d'adressage ainsi que des outils et des modes de configuration différents.

Concernant l'adressage, il est possible de convertir les formats avec le logiciel EasyTool Professional.

Pour la configuration du système KNX, utiliser le logiciel ETS de KNX, pour le système By-me, le logiciel EasyTool Professional.

La possibilité de configurer l'intégration des dispositifs KNX dans le système By-me est disponible à partir de la version 2.10 d'EasyTool Professional.

L'intégration des deux systèmes est basée sur le partage des données dans un format spécifique et sur les adresses de groupe ; les données partagées se réfèrent à des fonctions précises des dispositifs physiques (température mesurée par un thermostat, commande ON/OFF d'un relai, etc.).

Les serveur Internet permet de gérer deux macro catégories d'objets ou de fonctions à intégrer.

- Les fonctions simples ou générales
- Les fonctions composées:
  - Relai
  - Variateur
  - Store
  - Store vénitien

12.2 Les fonctions simples

Les fonctions simples du dispositif KNX identifiées par des objets de communication KNX sont transférées dans le système By-me en tant que fonctions simples.

La liste ci-dessous indique les objets de communication KNX gérés par le serveur Internet (se référer à la documentationKNX pour la description des datapoint types (DPT) du système KNX).

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]
9.006 DPT_Value_Pres [Pa]
9.007 DPT_Value_Humidity [%]
9.008 DPT_Value_AirQuality [ppm]
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

Intégration des dispositifs KNX dans le système By-me

Dans les fenêtres du serveur Internet, chaque objet de communication est représenté par des éléments graphiques. Le mode d'interaction avec l'utilisateur qui varie en fonction du type de donnée est précisé par le flag de communication sélectionné.

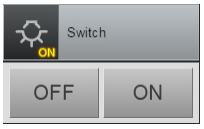
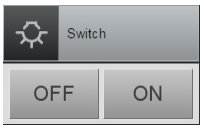
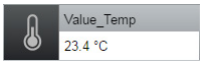
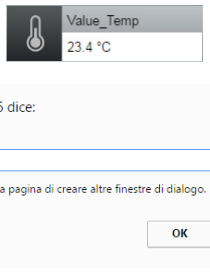
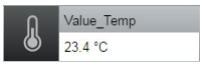
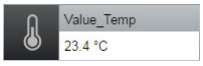
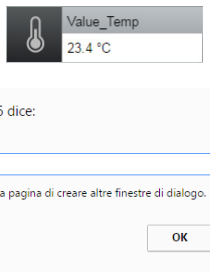
Le mode d'intégration est commandé par les trois flag de communication suivants.

- **Read.** Un objet graphique représentant une adresse de groupe avec ce flag de communication correspond à l'affichage d'un état ou d'une valeur numérique envoyée par le dispositif au serveur Internet. Pour certains types de données, le statut de l'icône de l'objet graphique est affiché.
- **Write.** Un objet graphique représentant une adresse de groupe avec ce flag de communication indique qu'il est possible d'envoyer une commande ou une valeur numérique du serveur Internet vers le dispositif.
  Remarque: le statut des boutons d'envoi des commandes (ON/OFF, etc.) n'est pas affiché ; les boutons s'activent quelques secondes quand on les touche pour valider la pression.
  Quand on appuie sur la zone blanche du widget, une fenêtre pop-up s'ouvre pour la saisie des données numériques sur le clavier.
- **Transmit.** Un objet graphique représentant une adresse de groupe avec ce flag de communication correspond à l'affichage d'un état ou d'une valeur numérique envoyée par le dispositif au serveur Internet.

Chaque adresse de groupe à intégrer doit avoir au moins un flag de communication sur trois sélectionné.

Les objets graphiques qui représentent les adresses de groupe à intégrer changent en fonction du type de donnée représentée.

Le tableau ci-dessous en donne quelques exemples.

DPT	Objet graphique fermé	Objet graphique ouvert	Flag de communication		
			R	W	T
1.001 DPT_Switch			✓	✓	✓
1.001 DPT_Switch		PAS de commande	✓		✓
1.001 DPT_Switch	 PAS de statut sur l'icône			✓	
9.001 DPT_Value_Temp [°C]			✓	✓	✓
9.001 DPT_Value_Temp [°C]		PAS de commande	✓		✓
9.001 DPT_Value_Temp [°C]	 PAS de lecture de la valeur			✓	

IMPORTANT: Le serveur Internet exécute un contrôle des données numériques saisies sur le clavier, si la valeur saisie sort de l'intervalle prévu ou si elle ne respecte pas la syntaxe (saisie de caractères non autorisés), la donnée est ignorée.

12.3 Les fonctions composées

Le serveur Internet contient des objets graphiques spécifiques pour certains dispositifs physiques simples et d'usage courant qui facilitent son utilisation : les fonctions simples (associées à un objet de communication KNX) sont regroupées en un seul objet graphique qui représente le dispositif physique.

Les fonctions composées gérées par le serveur Internet sont les suivantes.

- Relai
- Variateur
- Store avec point de consigne en pourcentage
- Store vénitien avec point de consigne en pourcentage

Relai

L'objet composé Relai regroupe les fonctions simples suivantes.

- Commande (ON/OFF)
- Statut ON/OFF

L'élément graphique qui représente cet objet composé est celui des actionneurs By-me, il a le même fonctionnement.

Variateur

L'objet composé Variateur regroupe les fonctions simples suivantes.

- Commande (ON/OFF)
- Statut ON/OFF
- Réglage de la luminosité (en pourcentage)
- Statut de la luminosité (en pourcentage)

L'objet graphique qui représente cet objet composé est celui des actionneurs de variateurs By-me, il a le même fonctionnement.

Store avec point de consigne en pourcentage

L'objet composé Store regroupe les fonctions simples suivantes.

- Mouvement haut/bas
- Stop
- Réglage de la position du store (en pourcentage)
- Statut de la position du store (en pourcentage)

L'objet graphique qui représente cet objet composé est celui des actionneurs de store By-me, il a le même fonctionnement.

Store avec point de consigne en pourcentage

L'objet composé Store vénitien regroupe les fonctions simples suivantes.

- Mouvement haut/bas
- Stop
- Réglage de la position du store (en pourcentage)
- Statut de la position du store (en pourcentage)
- Réglage de la position des lamelles (en pourcentage)
- Réglage par paliers de la position des lamelles dans les deux directions
- Statut de la position des lamelles (en pourcentage)

L'élément graphique qui représente cet objet composé est celui des actionneurs de stores vénitiens By-me avec le même fonctionnement.

12.4 Configuration

L'intégration des deux systèmes est basée sur le partage des données dans un format spécifique et sur les adresses de groupe.

Pour la configuration, utiliser le logiciel EasyTool Professional et le logiciel ETS de KNX ; pour consulter leur mode d'emploi détaillé, se référer à la documentation correspondante.

Après avoir configuré les groupes à intégrer (avec le logiciel EasyTool Professional), exporter le fichier XML et l'importer dans le serveur Internet.

Les groupes à intégrer sont enregistrés dans la fonction **Éclairage** du menu **Fonctions** sur le serveur Internet, ils peuvent être ajoutés aux pièces sélectionnées.

12.5 Intégration du gateway ME-AC-KNX-1-V2 Intesis pour la gestion des climatiseurs Mitsubishi

12.5.1 Préambule

Le serveur Internet 01945-01946 gère les principales fonctions des climatiseurs Mitsubishi compatibles avec le gateway ME-AC-KNX-1-V2 Intesis.

NOTE: pour toute information sur le gateway Intesis, consulter la documentation Intesis.

Pour permettre au serveur Internet 01945-01946 Vimar de gérer une unité interne de climatisation Mitsubishi :

- Chaque unité interne Mitsubishi doit être reliée à un gateway ME-AC-KNX-1-V2 Intesis compatible. Chaque gateway doit être spécialement configuré dans le logiciel ETS de KNX.
- Il faut d'abord créer dans le logiciel EasyTool Professional de Vimar un objet d'intégration KNX pour chaque unité interne Mitsubishi puis le configurer spécialement.
- Après la configuration par EasyTool Professional, le fichier de configuration XML doit être exporté puis importé dans le serveur Internet.

Comme l'indique le chapitre 13.4 Configuration, la gestion du gateway Intesis (un dispositif KNX) par le serveur Internet 01945-01946 est basée sur le partage des données entre le système KNX et le système By-me de Vimar par les adresses de groupe.

Les fonctions des climatiseurs Mitsubishi qui peuvent être gérées par le serveur Internet 01945-01946 sont les suivantes :

- affichage de l'état et commande ON/OFF
- affichage de la température ambiante
- affichage et configuration du setpoint de température
- affichage de l'état et configuration du mode de fonctionnement
- affichage de l'état et configuration de la vitesse du fancoil
- affichage de l'état et configuration de la position des lamelles.
- affichage de l'état d'erreur de l'unité interne Mitsubishi.
- affichage du code d'erreur de l'unité interne Mitsubishi (en présence d'une erreur).

IMPORTANT : la disponibilité de certaines fonctions et leur plage de réglage dépendent du modèle d'unité interne et de la procédure de configuration exécutée, comme on le verra dans les chapitres suivants.

12.5.2 Procédure de configuration

La gestion du gateway ME-AC-KNX-1-V2 Intesis par le serveur Internet 01945-01946 est basée sur le partage des données entre le système KNX et le système By-me de Vimar avec les adresses de groupe.

Pour chaque unité interne Mitsubishi, exécuter les opérations suivantes :

1. avec le logiciel ETS de KNX, configurer le gateway Intesis relié à l'unité interne Mitsubishi, lui attribuer des adresses de groupe qui ne sont pas déjà utilisées dans le système By-me.
2. Dans le logiciel EasyTool Professional de Vimar, créer un objet d'intégration KNX de type Mitsubishi et le configurer en attribuant les adresses de groupe précédemment créées dans le logiciel ETS de KNX aux objets de communication correspondants pour intégrer les deux systèmes.

   IMPORTANT : le serveur Internet ne peut gérer QUE les objets de communication auxquels on a attribué une adresse de groupe correcte.

   Les objets de communication auxquels aucune adresse de groupe n'a été associée ne sont pas inclus dans le fichier exporté depuis le logiciel puis importé dans le serveur Internet.

Après avoir configuré les groupes à intégrer (avec le logiciel EasyTool Professional de Vimar), exporter le fichier XML. Importer le fichier XML dans le serveur Internet.

Les chapitres suivants décrivent en détails les étapes de la configuration.

Les versions du programme d'application ETS de la passerelle ME-AC-KNX-1-V2 d'Intesis

La version actuellement disponible du programme d'application de la passerelle ME-AC-KNX-1-V2 d'Intesis est la 1.0. La version précédente était la 0.8.

Les deux versions 0.8 et 1.0 sont différentes du point de vue des valeurs et des paramètres de configuration ETS, ce qui implique une gestion différente de la part du serveur Internet et d'EasyTool Professional pour la phase de configuration.

- La gestion de la version 0.8 du logiciel d'application ETS de la passerelle ME-AC-KNX-1-V2 d'Intesis a été introduite dans la version 2.11 d'EasyTool Professional et dans la version 2.2 du logiciel du serveur Internet 01945/01946.

  Il est toujours recommandé d'utiliser les versions les plus récentes d'EasyTool Professional disponibles et du logiciel du serveur Internet.
- La gestion de la version 1.0 du logiciel d'application ETS de la passerelle ME-AC-KNX-1-V2 d'Intesis a été introduite dans la version 2,14.1 d'EasyTool Professional et dans la version 2.9 du logiciel du serveur Internet 01945/01946.

Les procédures de configuration, pour la gestion de la passerelle d'Intesis avec les deux versions du programme d'application ETS, seront décrites plus bas dans les chapitres correspondants du fait de la différence entre les deux versions. L'utilisation d'une procédure de configuration non correcte, en ce qui concerne la version du programme d'application ETS de la passerelle d'Intesis, risque de compromettre l'intégration.

12.5.3 Configuration KNX du gateway Intesis (avec version 0.8 du programme d'application ETS)

12.5.3.1 Configuration des paramètres du gateway ME-AC-KNX-1-V2 (avec version 0.8 du programme d'application ETS) dans le projet KNX

Après avoir ajouté le dispositif ME-AC-KNX-1-V2 au projet KNX, configurer les paramètres du dispositif suivants.

- General->AC unit type: dans le menu en arborescence, sélectionner le modèle de climatiseur Mitsubishi relié au portail concerné. Ce paramètre est très important car les fonctions et les valeurs admissibles dépendent du modèle d'unité interne.
- General->Virtual temperature control: Sélectionner NON.
- General->Mode object type [1 byte]: dans le menu en arborescence, sélectionner l'option Both (20.105 and enumerated). Les datapoint suivants sont maintenant disponibles :
  - CO 1-Mode (énumération) en lecture et en transmission. Ce datapoint est utilisé par le serveur Internet pour mettre à jour l'état du mode de fonctionnement de l'unité interne
  - o CO 49-HVAC Mode (dpt 20.105) en lecture, transmission et écriture. Ce datapoint est utilisé par le serveur Internet pour définir le mode de fonctionnement de l'unité interne.
- Objects Display->Show Increase/Decrease Bits : sélectionner Yes. Ce paramètre active les datapoint pour la configuration par augmentation/diminution de la vitesse du fancoil, de la position des lamelles et du setpoint de température. Après avoir configuré ce paramètre sur Yes, pour chacune des valeurs présentées ci-dessus, définir le type de valeur à utiliser en suivant les descriptions ci-après : sélectionner DPT_Step 1.007 (0=Dec/1=Inc) pour les objets de communication « Fan Speed [+/-] » et « Setpoint Temperature [+/-] ». Par contre, pour l'objet de communication « Vane [+/-] », sélectionner DPT_Step 1.008 (0=Up/1=Down).

12.5.3.2 Attribution des adresses de groupe aux datapoint du gateway ME-AC-KNX-1-V2 (avec version 0.8 du programme d'application ETS) dans le projet KNX

Après la configuration des paramètres, activer les datapoint, leur attribuer les adresses de groupe des datapoint suivants. Ne pas choisir des adresses de groupe déjà utilisées dans le système By-me. Exécuter avec le logiciel EasyTool Professional un contrôle préalable des adresses déjà utilisées dans le système By-me (le logiciel EasyTool Professional permet de visualiser les adresses au format KNX 2 niveaux, KNX 3 niveaux et By-me).

Le tableau suivant indique aussi les datapoint nécessaires à la gestion par le serveur Internet et ceux qui peuvent être ignorés, si on ne souhaite pas que la fonction correspondante soit gérée par le serveur Internet.

CO	Nom de l'objet de communication	Remarques
0	On/Off [1 bit]	**NÉCESSAIRE** Envoi de la commande ON/OFF à l'unité interne et réception des informations sur son état d'activation.
1	Mode [1 byte]	**NÉCESSAIRE** Lecture et réception par le serveur Internet de l'état du mode de fonctionnement.
3	Fan [1 byte]	**NÉCESSAIRE[1]** Lecture et réception par le serveur Internet de l'état de la vitesse du fancoil. Sans cet objet de communication, le serveur Internet ne peut pas gérer la vitesse du fancoil.
5	Vane [1 byte]	**NÉCESSAIRE[1]** Lecture et réception par le serveur Internet de la position des lamelles. Sans cet objet de communication, le serveur Internet ne peut pas gérer la position des lamelles.
7	Set Temperature [2 byte]	**NÉCESSAIRE[1]** Lecture et réception par le serveur Internet de l'état du setpoint de température. Sans cet objet de communication, le serveur Internet ne peut pas gérer le setpoint de température.
8	Ambient temperature [2 byte]	Lecture et réception par le serveur Internet de l'état de la température ambiante.
9	Error [1 bit]	**NÉCESSAIRE** Visualisation et gestion par le serveur Internet des erreurs de communication entre le gateway Intesis et l'unité interne et des disfonctionnements de l'unité interne.
10	Error Code [2 byte]	**NÉCESSAIRE** Affichage par le serveur Internet du code d'erreur envoyé par l'unité interne. Remarque : pour connaître la signification du code d'erreur numérique, se référer à la documentation technique Intesis.
24	Fan Speed [+/-] [1 bit]	Configuration de la vitesse du fancoil par le serveur Internet.
30	Vane [+/-] [1 bit]	Configuration de la position des lamelles par le serveur Internet.
38	Set temperature [+/-] [1 bit]	Configuration par le serveur Internet du setpoint de température.
49	HVAC Mode [1 byte]	Configuration par le serveur Internet du mode de fonctionnement.

[1] Si le modèle d'unité interne possède cette fonction.

Après les opérations décrites ci-dessus, télécharger les configurations exécutées sur les gateway Intesis.

12.5.4 Création et configuration des objets d'intégration KNX pour les gateway Intesis (avec version 0.8 du programme d'application ETS) dans EasyTool Professional

Pour la gestion des climatiseurs Mitsubishi (à travers la passerelle ME-AC-KNX-1-V2 d'Intesis version 0.8 du programme d'application), utiliser la version 2.14.1 (ou suivante) de EasyTool Professional.

Pour que le serveur Internet 01945-01946 puisse gérer les gateway KNX Intesis dans le système By-me, il faut d'abord créer et configurer dans Easy Tool Professional les objets d'intégration KNX correspondants en suivant la procédure ci-dessous.

Dans le projet EasyTool Professional qui sera exporté vers le serveur Internet, effectuer les opérations suivantes pour chaque gateway Intesis.

1. Créer un nouveau groupe KNX : Configure->Integrate third party KNX->New KNX Group.

   Attribuer une description à ce groupe KNX, sélectionner la fonction Mitsubishi 0.8 ou Mitsubishi No Fan Mode 0.8, selon les modes de fonctionnement disponibles dans l'unité interne Mitsubishi concernée.

   En particulier :

   a. sélectionner l'option Mitsubishi 0.8 si l'unité interne possède tous les modes de fonctionnement : HEAT, DRY, COOL, FAN, AUTO.

   b. Sélectionner l'option Mitsubishi No Fan Mode 0.8 si l'unité interne ne possède pas le mode FAN et peut gérer les modes de fonctionnement : HEAT, DRY, COOL, AUTO.

2. Terminer la création du groupe KNX en appuyant sur le bouton Enregistrer. L'Explorer Tree Window d'EasyTool Professional affiche le nouveau groupe KNX sous le nœud KNX.

   L'utilisateur peut ensuite créer d'autres groupes KNX ou appuyer sur le bouton Fermer dans la fenêtre Nouveau groupe KNX afin de configurer le groupe KNX qui vient d'être créé.

3. Sélectionner le groupe KNX qu'on vient de créer et lancer sa configuration. La fenêtre principale visualise la fiche du groupe et la liste des fonctions objet auxquelles une adresse de groupe doit être attribuée.
   Il est possible de modifier le format de l'adresse de groupe dans le menu Outils->Format adresses KNX.

4. Attribuer les adresses de groupe aux fonctions objet. Utiliser les adresses de groupe attribuées par ETS aux objets de communication du gateway Intesis à associer au groupe KNX configuré.

   Attribuer AU MOINS toutes les adresses NÉCESSAIRES décrites au chapitre 13.5.3.2 Attribution des adresses de groupe aux datapointdu gateway ME-AC-KNX-1-V2 dans le projet KNX.

   Il est conseillé d'attribuer des adresses de groupe à toutes les fonctions gérées par le serveur Internet.

   Les fonctions objet auxquelles aucune adresse de groupe n'a été attribuée ne peuvent pas être gérées par le serveur Internet.

   Le tableau suivant donne les correspondances entre les objets de communication ETS et les fonctions objets d'EasyTool Professional :

ETS		EasyTool Professional
CO	**Nom de l'objet de communication**	**Fonction objet**
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 : les flag RWT sont prédéfinis pour chaque fonction objet.

5. Après avoir terminé la création des groupes KNX associés à tous les gateway Intesis à gérer et les avoir configurés, exporter le projet vers le serveur Internet.
6. Le fichier de projet exporté depuis EasyTool Professional doit être ensuite importé dans le serveur Internet 01945-01946.

12.5.5 La configuration KNX de la passerelle d'Intesis (version 1.0 du programme d'application ETS)

12.5.5.1 Réglage des paramètres de la passerelle ME-AC-KNX-1-V2 (version 1.0 du programme d'application ETS) dans le projet KNX

Après avoir ajouté le dispositif ME-AC-KNX-1-V2 dans le projet KNX, configurer les paramètres ci-après du dispositif (seuls les paramètres concernant l'intégration prévue sont mentionnés ici) :

- General->Enable object "Error Code (2 byte) : Sélectionner ce paramètre pour afficher l'objet de communication Status_Error Code. Pour la description des codes d'erreur, consulter le tableau faisant partie de la documentation d'Intesis.
- Mode Configuration-> Indoor unit has FAN mode : régler sur Yes si l'unité interne Mitsubishi dispose du mode de fonctionnement FAN (Ventilation). Dans le cas contraire, régler sur No.
- Fan Speed Configuration->Fan is accessible in indoor unit (see docum. For your indoor unit) : régler sur Yes si le dispositif Mitsubishi dispose du réglage de la vitesse du ventilateur de l'unité interne. Dans le cas contraire, régler sur No.
  Après avoir réglé ce paramètre sur Yes, une liste de réglages s'affiche pour la gestion de la vitesse du ventilateur.
- Fan Speed Configuration->Available fanspeeds in Indoor Unit (see docum. For your indoor unit) : régler le nombre de vitesses du ventilateur sur l'unité interne Mitsubishi.
- Fan Speed Configuration->Indoor unit has AUTO fan speed (see docum. for your indoor unit) : régler sur Yes si l'unité interne Mitsubishi dispose du mode de réglage automatique de la vitesse du ventilateur. Dans le cas contraire, régler sur No.
- Fan Speed Configuration->Enable use of +/- object for Fan Speed: régler sur Yes. En réglant sur Yes, le choix du type de datapoint à utiliser s'affiche :
  - DPT type for +/- Fan Speed object : sélectionner 0-Decrease/1-Increase [DPT_1.007].
- Fan Speed Configuration->Enable "Fan Speed Man/Auto" objects (for Control and Status): régler sur Yes si l'unité interne Mitsubishi dispose du mode de réglage automatique de la vitesse du ventilateur. Dans le cas contraire, régler sur No.
- Vanes Up-Down Configuration->Indoor unit has U-D Vanes (see docum. for your indoor unit) : régler sur Yes si l'unité interne Mitsubishiprévoit la gestion de la position des lamelles. Dans le cas contraire, régler sur No. En réglant sur Yes, une liste de réglages relative à la gestion de la position des lamelles s'affiche.
- Vanes Up-Down Configuration->Available positions in Indoor Unit (see docum. for your indoor unit): sélectionner le nombre de positions des lamelles.
- Vanes Up-Down Configuration->Indoor unit has AUTO Vanes U-D: régler sur Yes si l'unité interne Mitsubishi dispose du réglage automatique (AUTO) de la position des lamelles : dans ce cas, un nouveau paramètre s'affiche pour la validation du réglage de la position des lamelles Automatique ou Manuel.
- Vanes Up-Down Configuration->Enable "Vanes U-D Man/Auto" objects (for Control and Status): ce paramètre s'affiche si le précédent a été réglé sur Yes et il permet de valider (en les affichant dans la liste des objets de communication) les objets de communication pour la validation et le statut de la gestion manuelle ou automatique de la position des lamelles.
- Vanes Up-Down Configuration->Enable "Vanes U-D Swing" objects (for control and status): en réglant sur Yes, les objets de communication sont validés pour le réglage et le statut du mode swing de la position des lamelles.
- Vanes Up-Down Configuration->Enable use of +/- object for Vanes U-D: régler sur Yes. En réglant sur Yes, le choix du type de datapoint à utiliser s'affiche :
  - Vanes Up-Down Configuration->DPT type for +/- Vanes U-D object : sélectionner 0-UP/1-Down (DPT_1.008).
- Temperature Configuration->Enable use of +/- obj for Sepoint Temp : Régler sur Yes. Après avoir réglé ce paramètre sur Yes, un nouveau paramètre s'affiche pour choisir le type de datapoint à utiliser.
- Temperature Configuration->DPT type for +/- Sept Temp object: Sélectionner 0-Decrease/1-Increase (DPT_1.007).

12.5.5.2 Attribution des adresses de groupe aux valeurs de la passerelle ME-AC-KNX-1-V2 (version 1.0 du programme d'application ETS) dans le projet KNX

Après avoir configuré les paramètres, en validant les datapoint nécessaires, attribuer les adresses de groupe aux datapoint suivants. Se rappeler que les adresses de groupe à utiliser ne doivent pas encore avoir été utilisées dans le système

By-me. Procéder à un contrôle préliminaire, en utilisant le logiciel EasyTool Professional, des adresses déjà utilisées sur le système By-me (se rappeler que le logiciel EasyTool Professional permet d'afficher les adresses aux formats KNX 2 niveaux, KNX 3 niveaux et By-me).

Le tableau ci-après regroupe les datapoint nécessaires à la gestion complète prévue par le serveur Internet.

Certains modèles d'unité interne Mitsubishi pourraient ne pas disposer de toutes les fonctions que le serveur Internet est en mesure de gérer.

Il est également possible d'exclure certaines fonctions de la gestion à travers le serveur Internet de l'unité interne Mitsubishi (dans ce cas, il ne sera pas nécessaire d'associer une adresse de groupe au datapoint dans la configuration ETS et sur la page correspondante de configuration de l'objet d'intégration KNX d'ETPro).

CO	Nom objet de communication	Remarques
0	Control_On/Off [DPT_1.001]	Permet d'envoyer la commande On/Off à l'unité interne.
1	Control_Mode [DPT_20.105]	Permet de définir le mode de fonctionnement : Auto, Heat, Cool, Fan (si disponible sur le modèle d'unité interne), Dry.
11	Control_Fan Speed Man/Auto [DPT_1.002]	Permet de valider le mode de réglage automatique ou manuel de la vitesse du ventilateur.
16	Control_Fan Speed -/+ [DPT_1.007]	Permet de régler la vitesse du ventilateur en mode manuel.
19	Control_Vanes U-D Man/Auto [DPT_1.002]	Permet de valider le mode de réglage automatique ou manuel de la position des lamelles.
25	Control_Vanes U-D Swing [DPT_1.002]	Permet de valider le mode de réglage Swing de la position des lamelles.
26	Control_Vanes U-D +/- [DPT_1.008]	Permet de définir la position des lamelles.
28	Control_Setpoint Temperature -/+ [DPT_1.007]	Permet de régler le point de consigne de température.
46	Status_On/Off [DPT_1.001]	Permet de lire et de recevoir l'état On/Off de l'unité interne.
47	Status_Mode [DPT_20.105]	Permet au serveur Internet de lire et de recevoir l'état du mode de fonctionnement : Auto, Heat, Cool, Fan (si disponible sur le modèle d'unité interne), Dry.
55	Status_Fan Speed [DPT_5.010]	Permet au serveur Internet de lire et de recevoir le statut de la vitesse du ventilateur, en mode manuel.
57	Status_Fan Speed Man/Auto [DPT_1.002]	Permet au serveur Internet de lire et de recevoir le statut de validation du mode de réglage automatique ou manuel de la vitesse du ventilateur.
63	Status_Vanes U-D [DPT_5.010]	Permet au serveur Internet de lire et de recevoir le statut de la position des lamelles, en mode manuel.
65	Status_Vanes U-D Man/Auto [DPT_1.002]	Permet au serveur Internet de lire et de recevoir le statut de validation du mode de réglage automatique ou manuel de la position des lamelles.
71	Status_Vanes U-D Swing [DPT_1.002]	Permet au serveur Internet de lire et de recevoir le statut de validation du mode de réglage Swing de la position des lamelles.
73	Status_AC Setpoint Temperature [DPT_9.001]	Permet au serveur Internet de lire et de recevoir la valeur actuelle du point de consigne de température.
74	Status_AC Return Temperature [DPT_9.001]	Permet au serveur Internet de lire et de recevoir la valeur actuelle de la température ambiante mesurée par l'unité interne.
75	Status_error/Alarm [DPT_1.005]	Permet au serveur Internet d'afficher et de gérer les erreurs de communication entre la passerelle et l'unité interne ou les dysfonctionnements de l'unité interne.
76	Status_Error Code [8.001]	Permet au serveur Internet d'afficher le code d'Erreur qu'a envoyé l'unité interne. Remarque : Pour la signification du code numérique d'erreur, consulter la documentation technique d'Intesis.

Après avoir complété les opérations décrites, télécharger les réglages effectués sur les passerelles Intesis.

12.5.6 La création et la configuration des objets d'Intégration KNX pour les passerelles Intesis (version 1.0 du programme d'application ETS) via EasyTool Professional

Pour la gestion des climatiseurs Mitsubishi (à travers la passerelle ME-AC-KNX-1-V2 d'Intesis version 1.0 du programme d'application), utiliser la version 2.14.1 (ou suivante) de EasyTool Professional.

Pour que le serveur Internet 01945-01946 puisse gérer les passerelles KNX d'Intesis dans le système By-me, il est nécessaire de créer et de configurer dans EasyTool Professional les objets d'intégration KNX correspondants, en se conformant à la procédure décrite ci-après.

Dans le projet EasyTool Professional, qui devra être exporté pour le serveur Internet, prévoir les opérations suivantes pour chaque passerelle Intesis :

1. Créer un Nouveau Groupe KNX : Configurer->Intégration systèmes tiers KNX->Nouveau Groupe KNX
   Attribuer une description au groupe KNX, sélectionner, comme Fonction, la rubrique « Mitsubishi 1.0 » ou « Mitsubishi No Fan Mode 1.0 » en fonction des modes de fonctionnement disponibles sur l'unité interne Mitsubishi à gérer.

   En particulier :
   a. Sélectionner la rubrique « Mitsubishi 1.0 » si l'unité interne à gérer prévoit tous les modes de fonctionnement : HEAT, DRY, COOL, FAN, AUTO.
   b. Sélectionner la rubrique « Mitsubishi No Fan Mode 1.0 » si l'unité interne à gérer ne prévoit pas la modalité FAN, c'est-à-dire qu'elle est en mesure de gérer les modes de fonctionnements suivants : HEAT, DRY, COOL, AUTO.
2. Compléter la création du groupe KNX en appuyant sur le poussoir Enregistrer. L'ExplorerTree Window d'EasyTool Professional affiche le nouveau groupe KNX sous le nœud KNX.
   Il est possible de créer d'autres groupes KNX ou d'appuyer sur le poussoir « Fermer » de la fenêtre « Nouveau Groupe KNX » pour procéder à la configuration du groupe KNX créé.
3. Sélectionner le groupe KNX créé pour procéder à la configuration. L'espace de travail principal présente la fiche du groupe, avec la liste des Fonctions objet auxquels attribuer l'adresse correspondante de groupe.
   Se rappeler qu'il est possible de modifier le format de l'adresse de groupe à partir du menu Instruments->Format adresses KNX.
4. Attribuer les adresses de groupe aux Fonctions objet en utilisant les adresses de groupe préalablement attribuées via ETS aux objets de communication correspondants de la passerelle Intesis que l'on souhaite associer au groupe KNX en cours de configuration.
   Il est conseillé d'attribuer les adresses de groupe à toutes les fonctions que le serveur Internet est en mesure de gérer.
   Les fonctions objet ne présentant aucune adresse de groupe associée ne seront pas gérées par le serveur Internet.
   Ci-après, le tableau présentant les correspondances entre les objets de communication d'ETS et les Fonctions objet d'EasyTool Professional :

ETS		EasyTool Professional
CO	Nom objet de communication	Fonction objet
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)

REMARQUE : chaque fonction objet dispose déjà des flag RWT correctement prédéfinis.

5. Après avoir complété la création des groupes KNX associés à toutes les passerelles Intesis à gérer, et après les avoir configurés correctement, exporter le projet pour le serveur Internet.
6. Le fichier de projet exporté par EasyTool Professional doit être ensuite importé sur le serveur Internet 01945-01946.

13. Mises à jours importantes faisant partie des versions 2.5 et 2.6 du logiciel du serveur Internet pour la gestion de la connexion protégée HTTPS

13.1 Avant-propos

Les versions 2.5 et 2.6 du logiciel du serveur Internet 01945/01946 présentent d'importantes améliorations/mises à jour concernant la gestion de la communication protégée HTTPS entre le serveur Internet et les clients qui permettent d'accéder au serveur (navigateur, appli By-web pour dispositifs mobiles) afin de répondre aux toutes dernières dispositions en la matière.

Les modifications concernent :

1. Mise à jour du certificat TLS du serveur Internet et du certificat CA de Vimar.
2. Mise à jour du protocole TLS à la version 1.2.

La mise à jour à la version 2.5 du logiciel du serveur Internet permet à tous les serveurs Internet de mettre à jour le certificat TLS et le certificat CA de Vimar.

Par contre, la mise à jour du protocole TLS à la version 1.2 s'effectue automatiquement avec la mise à jour à la version 2.5 sur les serveurs Internet plus récents. Pour les moins récents, lancer une procédure dédiée et qui sera disponible après la mise à jour à la version 2.6 du logiciel du serveur Internet 01945/01946, selon la description ci-après.

Par conséquent, il est conseillé, si possible, de mettre à jour le serveur Internet directement à la version 2.6.

Le dépassement de la date limite du certificat CA du serveur Internet, l'impossibilité à mettre à jour le certificat TLS ou l'utilisation d'une version de protocole TLS précédente à la 1.2 ne permettent pas aux clients qui donnent accès au serveur Internet d'assurer une « connexion fiable » (navigateur pour ordinateur et appli By-web pour dispositifs mobiles).

La connexion cryptée entre serveur Internet et client est toujours garantie, mais des messages expliquant que la connexion n'est pas fiable pourraient s'afficher.

Il est donc nécessaire de mettre à jour le plus tôt possible les serveurs Internet à la version 2.6 (pour les serveurs les plus récents, il suffit de passer à la version 2.5) et de suivre les indications qui s'affichent et qui seront également décrites dans le manuel, afin de mettre à jour les composants de la connexion protégée HTTPS.

Rappelons que pour vérifier l'état des composants du serveur Internet nécessaires à la gestion de la connexion protégée HTTPS, il est possible d'accéder à la page « Instruments pour développeurs » de Google Chrome et de sélectionner le tab « Security ».

REMARQUE : Après la mise à jour du certificat ou du protocole TLS, pour que Google Chrome actualise l'état de l'indicateur de sécurité de la connexion HTTPS, il pourrait s'avérer nécessaire de relancer Google Chrome.

13.2 La version 2.5 du logiciel du serveur Internet 01945/01946

La version 2.5 comprend les nouvelles fonctions suivantes relatives à la connexion protégée HTTPS :

1. Gestion de la mise à jour du certificat TLS du serveur Internet et téléchargement du nouveau certificat CA.
   Cette fonction est disponible pour toutes les révisions matérielles du serveur Internet 01945/01946 de Vimar.
2. Mise à jour du protocole TLS à la version 1.2, exclusivement sur les versions matérielles les plus récentes (03 et 04) du serveur Internet 01945/01946 de Vimar.
3. Introduction d'un mécanisme automatique pour le contrôle périodique de la date limite du certificat CA et de la disponibilité éventuelle d'un nouveau certificat CA.

13.2.1 Opérations nécessaires après la mise à jour à la version 2.5

Après la mise à jour à la version 2.5, un message demande de télécharger le nouveau certificat CA depuis le serveur Internet et de l'installer sur les clients.

Avant de procéder à cette opération, mettre à jour les certificats TLS du serveur Internet, selon les explications suivantes :

1. S'assurer que le serveur est connecté à Internet. S'il n'est pas connecté à Internet, il ne sera pas possible de mettre à jour son certificat TLS ni de télécharger le nouveau certificat CA.
2. Accéder à la page des réglages de réseau du serveur Internet en suivant le parcours : « Paramètres généraux » -> « Réseau ». Appuyer sur le bouton pour confirmer l'opération qui permet de modifier les paramètres du réseau.
3. Après avoir appuyé sur le bouton pour confirmer les paramètres de réseau, une fenêtre s'ouvre avec un message qui demande de confirmer l'opération qui permet de modifier les paramètres du réseau. Confirmer l'opération qui permet de modifier les paramètres du réseau.
4. Un message annonce le démarrage de la procédure de mise à jour des certificats TLS si le serveur est connecté à Internet. Confirmer le message.
5. Si le serveur est connecté à Internet, il commencera par la mise à jour du certificat TLS et à télécharger le tout dernier certificat CA, il relancera les services (après avoir notifié un message) pour rendre les modifications disponibles. Une fois l'opération terminée, il affichera la page d'accueil du serveur Internet.
   Si le serveur n'est pas connecté à Internet, il ne sera pas possible de créer les nouveaux certificats TLS et un message d'erreur sur la mise à jour des certificats TLS s'affichera.
6. Après la mise à jour du certificat TLS et le téléchargement du certificat CA actualisé sur le serveur Internet, il faudra télécharger le certificat CA depuis le serveur Internet et l'installer sur les clients qui donnent accès au serveur Internet.

13.2.2 Mise à jour du protocole TLS à la version 1.2

Nous l'avons déjà dit, la mise à jour du protocole TLS à la version 1.2 est automatique durant la mise à jour du logiciel à la version 2.5, uniquement pour les serveurs Internet 01945/01946 équipés du matériel à la version 03 et 04. Pour les versions matérielles précédentes, la mise à jour du protocole TLS à la version 1.2 nécessite une procédure dédiée de « mise à jour microprogramme » disponible à la version 2.6 du logiciel du serveur Internet.

13.2.2 Contrôle automatique depuis le serveur Internet sur la disponibilité d'un nouveau certificat CA et sur la date limite du certificat CA embarqué sur le serveur Internet.

Après la mise à jour du logiciel du serveur Internet à la version 2.5 (ou suivantes), celui-ci procèdera une fois par semaine aux contrôles suivants :

- Si le serveur est connecté à Internet, il vérifiera si Vimar pourra disposer d'un nouveau certificat CA et s'il le trouve, il le téléchargera sur le serveur Internet avec le nouveau certificat TLS.
- Si le serveur n'est pas connecté à Internet, il vérifiera la date de validité du certificat CA embarqué et affichera un message si la date d'expiration est proche.

13.3 La version 2.6 du logiciel du serveur Internet 01945/01946

La version 2.6 du logiciel du serveur Internet a été améliorée et présente de nouvelles fonctions relatives à la mise à jour des certificats TLS et du protocole TLS à la version 1.2, par rapport à la version 2.5 précédente.

Les nouveautés principales sont résumées ci-après:

1. Installation de la fonction « Firmware upgrade » qui permet de mettre à jour le système d'exploitation du serveur Internet.
   Dans le cas spécifique, conformément à la nécessité d'actualiser les composants pour réaliser la connexion protégée HTTPS, cette nouvelle fonction permet de mettre à jour le protocole TLS (à la version 1.2) des serveurs Internet en disposant de matériel de la version précédente à la 03.
   La procédure de mise à jour du microprogramme du serveur Internet est décrite au chapitre « Mise à jour du microprogramme du serveur Internet (Firmware Upgrade) » de ce manuel.

2. Introduction de certains automatismes servant à guider les opérations de mise à jour des certificats TLS et du protocole TLS :
   - Après avoir mis à jour le logiciel du serveur Internet à la version 2.6, si le serveur est doté d'un matériel d'une version précédente à la 03, un message signale la disponibilité d'une nouvelle version du microprogramme (absolument nécessaire pour mettre à jour le protocole TLS). Pour mettre à jour le microprogramme, suivre les indications qui s'affichent et qui sont également signalées au chapitre correspondant de ce manuel. Attention, la procédure de « Firmware Upgrade » est possible uniquement si le serveur Internet est connecté à Internet.
     Pour le moment, il n'est pas nécessaire de mettre à jour le microprogramme des serveurs Internet disposant de matériel à la version 03 et 04 mais elle reste à prévoir pour les exigences futures ; par conséquent, ces serveurs n'afficheront encore aucun message sur la disponibilité d'un nouveau microprogramme.
   - Après la mise à jour du logiciel du serveur Internet à la version 2.6, un message signale la nécessité de mettre à jour les certificats. En confirmant, la procédure démarrera automatiquement. Attention, l'opération aura lieu correctement uniquement si le serveur Internet est connecté à Internet.

14. Utilisation du service SMTP de Google Gmail pour l'envoi des mails de notification du serveur Internet

14.1 Avant-propos

Pour envoyer des notifications par e-mail, le serveur Internet doit pouvoir se connecter à un serveur SMTP qui lui permette d'y accéder après avoir saisi un *Nom d'utilisateur* et un *Mot de passe*.

Pour utiliser le service SMTP de Google Gmail, il faut avoir un compte de courrier électronique Google Gmail.

Si vous utilisez le service SMTP de Google Gmail, sachez que Google a modifié la gestion de la sécurité des accès aux comptes Gmail. De ce fait, à partir du 30 mai 2022, vous ne pourrez plus vous authentifier sur un compte Gmail à travers vos Nom d'Utilisateur et Mot de passe habituels (la possibilité de les utiliser, en validant la fonction « Autoriser applis moins sûres », terminera elle aussi le 30 mai 2022).

La référence est la suivante : https://support.google.com/accounts/answer/6010255

Google prévoit une procédure de configuration spécifique, à effectuer sur le compte Google Gmail et qui sera encore utilisable après le 30 mai 2022 ; elle permettra au serveur Internet de se connecter au service SMTP de Google Gmail pour envoyer les mails de notification.
Cette procédure, prévue par Google, permet de créer des mots de passe spéciaux appelés « mots de passe pour les applis », qui permettent au serveur Internet d'accéder au service SMTP du compte Google Gmail du client. Les chapitres qui suivent décrivent la procédure permettant de créer des « mots de passe pour applis » dans la section d'administration du propre compte Google Gmail et d'utiliser ces applis pour configurer le serveur Internet.

IMPORTANT : rappelons que le service de notification via e-mail est subordonné à l'utilisation d'un service SMTP de tiers que Vimar n'est pas en mesure de garantir. Vimar n'est donc pas en mesure de garantir les temps de validité de cette solution pour le futur.

14.2 Création d'un « mot de passe pour les applis » sur Google Gmail

La création d'un « *mot de passe pour applis* » se fait en deux étapes :

1. La première étape, nécessaire pour pouvoir passer à la suivante, consiste à valider la « vérification en deux passages » (appelée également « *authentification à deux facteurs* ») du propre compte Google Gmail (ou au moins du compte Google Gmail que vous souhaitez utiliser pour envoyer les mails de notification du serveur Internet).
2. La deuxième étape, possible si la première a été effectuée correctement, consiste à créer le « mot de passe pour les applis » qui sera utilisé par le serveur Internet.

14.2.1 Valider la « *vérification en deux passages* » pour accéder au compte Google Gmail

L'utilisation de la vérification en deux passages permet d'augmenter le niveau de sécurité du compte Google Gmail.

Pour valider la « vérification en deux passages » afin d'accéder au compte Google Gmail, procédez de la façon suivante :

1. Accédez au compte Google que vous souhaitez utiliser pour envoyer des mails à partir du serveur Internet.
2. Sélectionnez la rubrique « Sécurité » sur le panneau de navigation.
3. Sélectionnez « Vérification en deux passages » à la section « Accéder à Google » ➡ Commencer.
4. Suivez les passages qui s'affichent à l'écran.

Consultez la documentation officielle de Google : https://support.google.com/accounts/answer/185839

Après avoir validé la vérification en deux passages, complétez un deuxième passage pour vérifier votre propre identité au moment de l'accès. Pour mieux protéger votre compte, Google demandera de compléter un deuxième passage spécifique.

14.2.2 Création du « mot de passe pour les applis » pour le serveur Internet

Après avoir validé la « Vérification en deux passages » du compte Google que vous souhaitez utiliser pour envoyer le mail à partir du serveur Internet, créez un « mot de passe pour l'appli » pour le serveur Internet.

Remarque : si l'utilisateur dispose de plusieurs serveurs Internet (ou d'autres dispositifs/applis) nécessitant l'accès à un compte Gmail, il est conseillé de créer un « mot de passe pour les applis » dédié à chaque dispositif. Ceci permettra, par exemple, d'empêcher l'accès au compte d'un dispositif indépendamment des autres dispositifs, en éliminant du compte Google le « mot de passe pour les applis » spécifique.

Pour créer un « Mot de passe pour les applis » pour le serveur Internet, procédez de la façon suivante :

1. Accédez au compte Google que vous souhaitez utiliser pour envoyer des mails à partir du serveur Internet.
2. Sélectionnez la rubrique « Sécurité » sur le panneau de navigation.
3. Sélectionnez la rubrique « Mot de passe pour les applis » à la section « Accès à Google » (cette rubrique sera disponible uniquement si la rubrique « Vérification en deux passages » est validée (ON)).
4. La liste des mots de passe pour les applis préalablement créés s'affiche (au départ, la liste résulte vide).
5. Pour le champ « Sélectionner Appli », sélectionnez la rubrique « Courrier ».
6. Pour le champ « Sélectionner dispositif », sélectionnez la rubrique « Autre (nom personnalisé) ».
7. Pour le champ « nom dispositif », saisissez un nom au choix qui identifie le serveur Internet précis pour lequel vous voulez créer le « mot de passe pour les applis ».
8. Appuyez sur le bouton « Générer » : un pop-up s'affiche. La rubrique « Votre mot de passe pour l'appli pour le dispositif » présente un champ contenant le mot de passe créé (16 caractères). Ce mot de passe permettra au serveur Internet d'accéder au compte Google Gmail pour envoyer des mails de notification.
9. Copiez le mot de passe pour pouvoir le saisir dans le champ prévu à cet effet dans la fenêtre de configuration du serveur Internet (faire référence au chapitre 14.3 suivant : Configuration du serveur Internet).

Pour créer le « Mot de passe pour les applis » de Google, consultez la documentation officielle de Google :

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

Utilisation du service SMTP de Google Gmail

14.3 Configuration du serveur Internet

Après avoir créé un « mot de passe pour applis » pour le compte Google Gmail que vous souhaitez utiliser pour envoyer des mails de notification du serveur Internet, remplissez la page de configuration dédiée au serveur Internet.

Par rapport au passé, le mot de passe que le serveur Internet doit utiliser pour accéder au service SMTP de Google Gmail ne sera plus le mot de passe du compte Gmail de l'usager, mais il s'agira désormais du « mot de passe pour les applis » qui a été créé pour le serveur Internet à partir du compte Gmail de l'usager.

Remarque : si l'utilisateur dispose de plusieurs serveurs Internet (ou d'autres dispositifs/applis) nécessitant l'accès à un compte Gmail, il est conseillé de créer un « mot de passe pour les applis » dédié à chaque dispositif.

Le tableau ci-après présente les données que vous devez saisir sur la page de configuration d'envoi de mails du serveur Internet pour notifier correctement les mails à partir du compte Google Gmail.

Champ	Description champ	Valeur (pour le compte Google Gmail)
Serveur SMTP	Adresse du serveur de courriel utilisée pour envoyer les messages.	smtp.gmail.com
Port	Port utilisé pour la connexion au serveur SMTP.	465
Utilisateur	Adresse e-mail du compte Gmail utilisé pour envoyer les mails depuis le serveur Internet	Ex. : yyy.zzz@gmail.com
Mot de passe	« Mot de passe pour les applis » (16 caractères) créé par le compte Google Gmail pour le serveur Internet. Important : le serveur Internet n'accèdera plus au service SMTP de Google à travers le mot de passe du compte Google à partir du 30 mai 2022.	Ex : aaaabbbbccccdddd
Expéditeur	Précisez l'adresse e-mail à utiliser comme expéditeur des messages. Normalement, l'adresse saisie dans le champ « Utilisateur ».	Ex. : yyy.zzz@gmail.com
Authentification	Précisez si le serveur SMTP exige l'authentification.	Oui
Chiffrage SSL	Précisez si le serveur SMTP exige ou nom le chiffrage SSL.	Oui

CE

01945-01946 IFR 27 2206

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