Notice d'exploitation IP-GAP

Portier IP AMPHITECH

N°685 – Mars 2019

Amphitech
1, rue Robert et Sonia Delaunay
75011 Paris
Tél. SAV : +33 (0)1.43.67.96.74
Fax Service commercial : +33 (0)1.43.67.13.97

Conforme ROHS

15/NOTIC-000685D

Version logiciel

Version logiciel V.1.31.

Sommaire

Recommandations

AMPHITECH vous recommande de lire attentivement les notices fournies afin d'optimiser l'installation de votre produit.

1. Portier IP-GAP

1.1. Présentation générale

L'IP-GAP est un portier audio **ou** audio-vidéo, full-IP "mains-libres" et anti-vandales. Le produit est équipé de pictogrammes lumineux et d'une synthèse vocale pour favoriser l'accessibilité des personnes avec handicap.

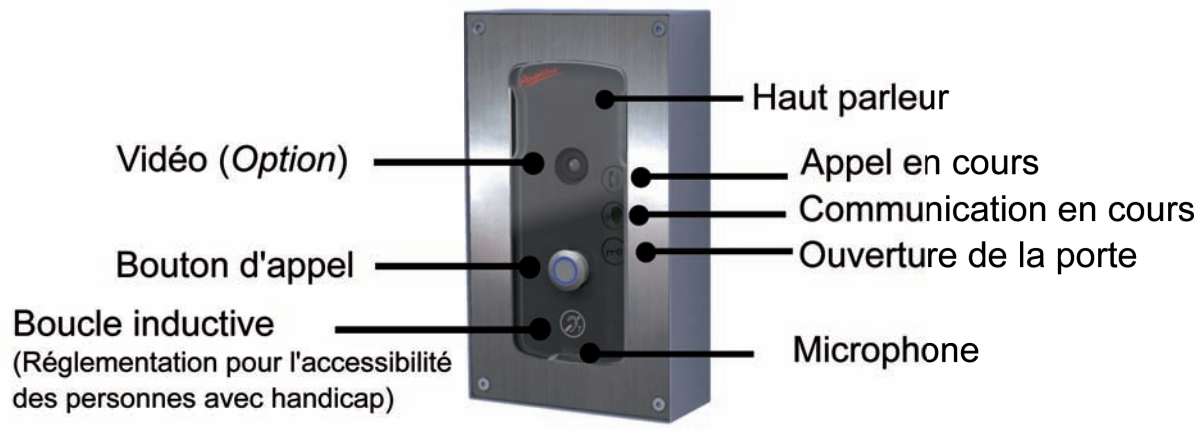
L'IP-GAP se raccorde :

- sur un réseau IP local disposant d'un serveur IP-PBX (serveur SIP) **ou**
- en mode d'appel point à point (Peer to Peer)

Le portier fonctionne avec une alimentation externe 24 VDC **ou** peut être alimenté en PoE+ *(Power over Ethernet, 802.3at)* fourni par un switch via le câble réseau.

La configuration du produit est réalisée à l'aide d'un serveur WEB. Il existe deux types de configuration :

- la configuration simplifiée  (mode assisté),
- la configuration avancée  (mode administrateur).



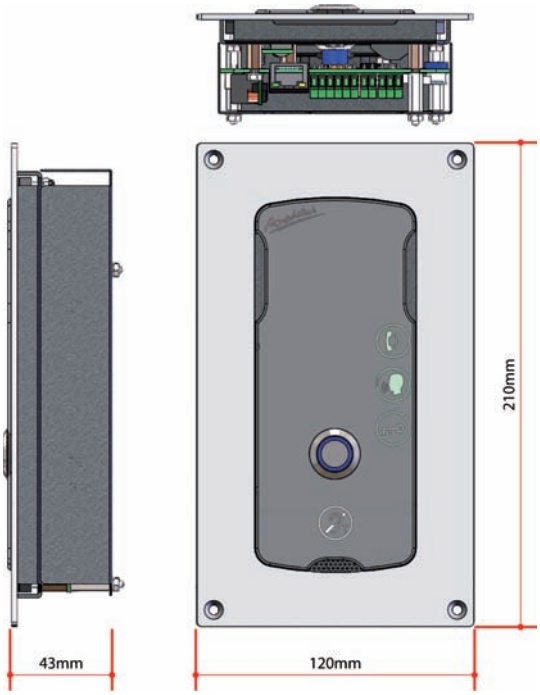
Gamme - Exemples :

VERSION SAILLIE			
			
IP-GAP 02	**IP-GAP 02V**		**Dimensions**
			
IP-GAP 12	**IP-GAP 12V**		**Dimensions**

VERSION ENCASTRÉE

IP-GAP 02

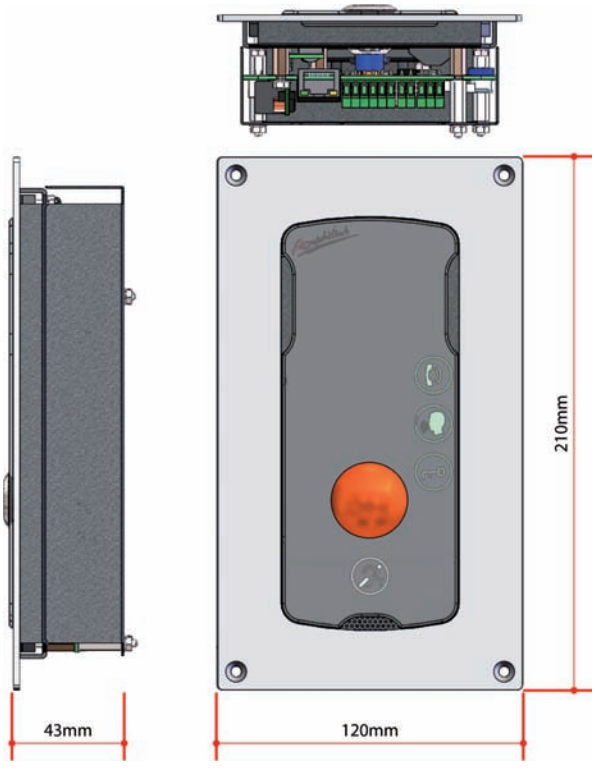
IP-GAP 02V



Dimensions

IP-GAP 12

IP-GAP 12V



Dimensions

Caractéristiques électriques

	Min	Nom	Max	Longueur (Max)	Description
Alimentation PoE+			13W		IEEE 802.3at
Alimentation secteur		24 VDC		< 5 m	Défaut secteur sur les alimentations Amphitech
Relais (pouvoir de coupure)	-	-	2A / 62,5 VA		Courant
Entrée extérieure	5 VDC		30 VDC	< 50 m	Tension
	0		500 Ohms		Contact normalement fermé
	500 Ohms		∞		Contact normalement ouvert

1.2. Caractéristiques

- 1 Bouton d'appel vers 1 ou plusieurs correspondants (via IP-PBX ou adresse IP mode Peer to Peer) - Appel cyclique en cas d'occupation ou de non réponse
- Audio, haut parleur et micro :
  - communication mains libres full duplex,
  - diffusion de messages.
- Vidéo **(V)** :
  - caméra couleur, angle de vision 90°, capteur CMOS, IR Cut Filter
  - codecs vidéo : H264, H263, H263p, VP8
  - résolution vidéo :
    - *Streaming* : QVGA 320 x 240 / 640 x 480 (accès sécurisé)
    - *En communication* : CIF 352 x 288 **ou** QCIF 176 x 144
- Boucle inductive (Réglementation pour l'accessibilité des personnes avec handicap)
- Façade inox 2.5 mm, avec ou sans vidéo :
  - IP-GAP-01, dimensions 275 x 120 mm,
  - IP-GAP-02, dimensions 210 x 120 mm,
  - IP-GAP-03, dimensions 355 x 120 mm,
  - IP-GAP-01B, dimensions 275 x 120 mm
  - IP-GAP-11, dimensions 275 x 120 mm,
  - IP-GAP-12, dimensions 210 x 120 mm,
  - IP-GAP-13, dimensions 355 x 120 mm,
  - IP-GAP-11B, dimensions 275 x 120 mm
  - anti-vandalisme IK 09 ; étanchéité IP 65
- Connexions : relais de gâche, information Prise De Ligne, extension audio

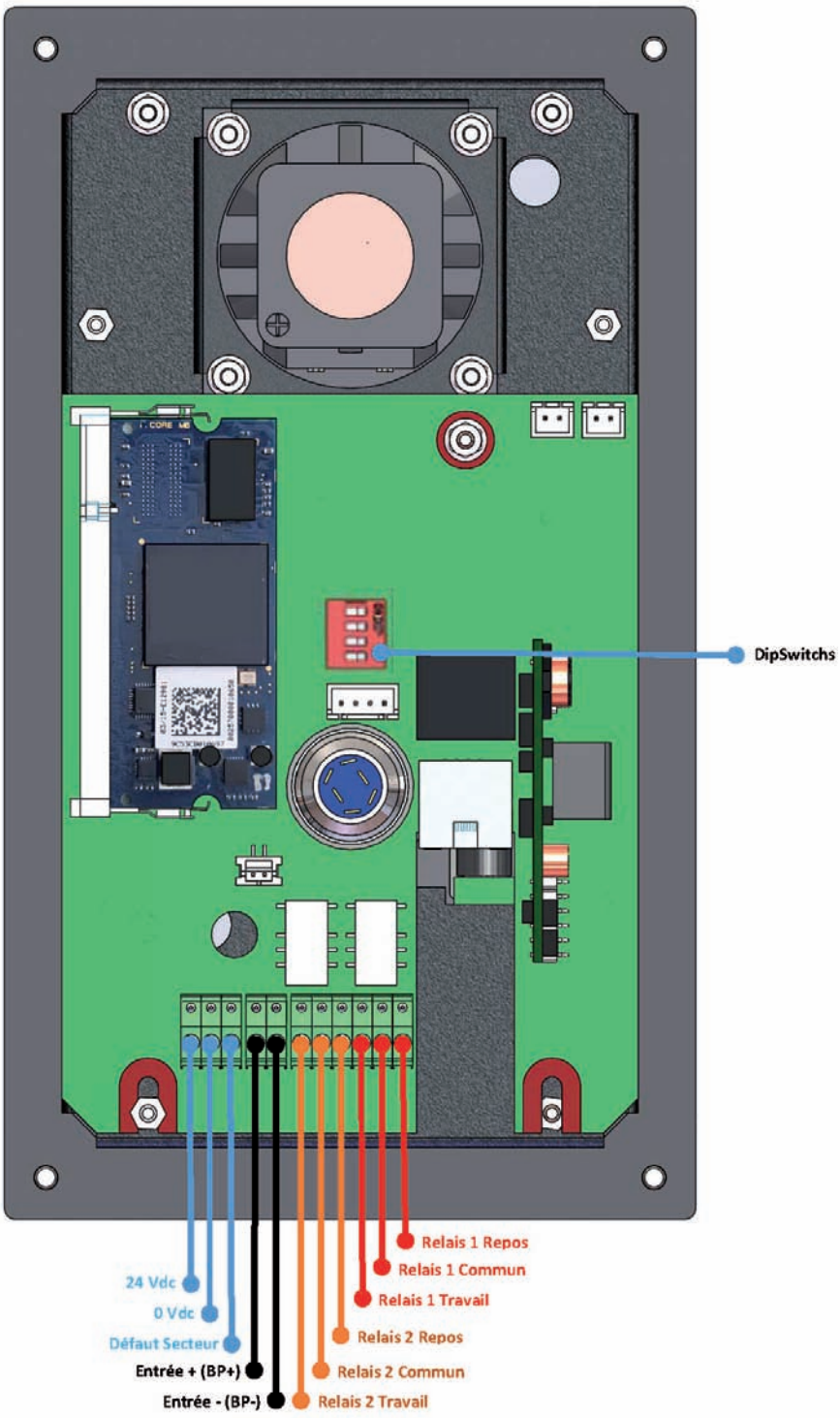
- Serveur web embarqué, sécurisé par mot de passe et connexion HTTPS
- Appel via IP-PBX et/ou adresse IP (mode Peer to Peer)
- Connexion Ethernet 10/100 base T RJ45
- Alimentation PoE+ ; Power over Ethernet : IEEE 802.3at (PoE+) **ou** Alimentation externe 24 VDC
- Réseau : DHCP ou statique
- Protocole VoIP : SIP V2 (RFC 3261).
- DTMF: RFC 2833, SIP Info (RFC 2976).
- RADIUS 802.1x (PEAP, TTLS, TLS)
- Mise à l'heure manuelle ou via serveur NTP.
- Codecs audio : G.722, G.711u, G.711a, GSM, Speex 8k, Speex 16k, Speex 32k, G.726-16, G.726-32, G.726-24, G.726-40, AAL2-G.726-16, AAL2-G.726-32, AAL2-G.726-24, AAL2-G.726-40, opus, AMR.-32
- Rapport des évènements système : fichiers téléchargeables, SYSLOG, notifications par e-mails (client smtp).
- Décroché automatique sur appel entrant.
- Éclairage de pictogrammes en fonction de l'état de l'appel
- Choix des messages vocaux à diffuser (correspondant indisponible, fin de communication, connexion réseau hors service, etc.)
- Choix de langues pour les messages vocaux : Français, Anglais, Allemand, Espagnol, Portugais
- 2 sorties relais pour la commande d'ouverture de porte ou l'information prise de ligne et le défaut d'alimentation (secteur / PoE+) ainsi que la détection défaut réseau (problème de connexion...)
- 1 entrée bouton extérieure pour activation relais Gâche ou appel de contacts
- Gestion des modes Jour / Nuit (réglage du seuil audio en mode nuit)
- Durée de communication programmable de 1 à 10 minutes
- 1 entrée défaut secteur
- 4 dipswitchs de configuration (Réseau DHCP/Statique, annonce adresse IP, retour IP usine, retour paramètres usine)
- Gestion des paramètres d'appels, temps de communication, temps d'appui bouton, délais appel sortant, volume audio…
- Visualisation en temps réel de l'état du portier (Bouton d'appel / Entrées / Sorties / Pictogrammes)
- Compatibilité ASIP Stream AMPHITECH, interface streaming vidéo (*Voir* wiki.amphitech.fr)
- Gestion téléalarme protocole SIP, envoi de messages SIP sur détection de défaut (défaut secteur, défaut bouton d'appel, défaut réseau, défaut connexion vers IP-PBX)
- Compatibilité avec le protocole DTMF GSM AMPHITECH vers l'outil de réception des appels ORA 04 et les autres centrales de télésurveillance analogiques
- API Porte, VoIP et Audio

1.3. Installation et raccordement

- Le câblage doit être réalisé avec les connecteurs débranchés
- Respecter les polarités des tensions indiquées
- Raccorder impérativement le boîtier à la terre à l'aide du fil fourni

Recommandations

Dans le cas où le cablage réseau fourni une alimentation POE+ (Power over Ethernet +) il n'est pas nécessaire d'utiliser une alimentation. Dans le cas contraire, il est impératif d'utiliser une alimentation 24 VDC. Le raccordement à la terre est obligatoire. Pour le câblage, utiliser du fil de section 0,9 mm².


DipSwitchs
Relais 1 Repos
Relais 1 Commun
Relais 1 Travail
Relais 2 Repos
Relais 2 Commun
Relais 2 Travail
24 Vdc
0 Vdc
Défaut Secteur
Entrée + (BP+)
Entrée - (BP-)

Dipswitchs - En mode normal de fonctionnement, tous les dispswitchs sont en position OFF.		
	N°1	Passage en mode DHCP :
		- Couper l'alimentation.
		- Positionner le dipswitch N°1 sur ON.
		- Rebrancher l'alimentation.
		- Après redémarrage du système, l'adresse IP est fournie par le routeur du réseau.
		- **Repositionner le dipswitch N°1 sur OFF**. Dernière adresse IP connue (DHCP ou STATIQUE)
	N°2	Diffusion de l'adresse IP au démarrage
	N°3	Retour à l'adresse IP par défaut :
		- Couper l'alimentation.
		- Positionner le dipswitch N°3 sur ON.
		- Rebrancher l'alimentation.
		- Après redémarrage du système, l'adresse IP est *192.168.0.2*
		- **Repositionner le dipswitch N°3 sur OFF.** (*Si Dipswitch 1 = ON, mode DHCP prioritaire*)
	N°4	Paramètres usine :
		- Couper l'alimentation.
		- Positionner le dipswitch N°4 sur ON.
		- Rebrancher l'alimentation.
		- Après redémarrage du système, le portier est configuré avec les paramètres par défaut.
		- **Repositionner le dipswitch N°4 sur OFF.** (*Si Dipswitch 1 = ON, mode DHCP prioritaire*)

2. Fonctionnement

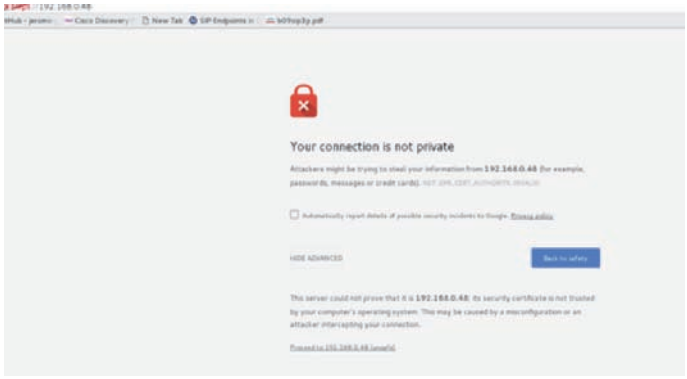
2.1. Connexion au réseau local

- Vérifier les raccordements et connecter l'alimentation si le serveur réseau ne fournit pas une alimentation POE+ (*Power over Ethernet*).
- La mise en service est réalisée avec les paramètres par défaut. L'adresse IP du portier à la livraison du produit est : 192.168.0.2
- Ouvrir un navigateur internet (Chrome, Firefox) et saisir dans la barre d'adresse http://192.168.0.2.
- A la mise en service, les pictogrammes s'allument et un bip retentit pour signaler la fin de mise en service.

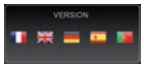
2.2. Modification de l'adresse IP

- Pour modifier l'adresse IP du portier, ouvrir l'interface de configuration à l'adresse IP par défaut http://192.168.0.2

- L'accès aux paramètres est également possible par HTTPS, cliquer sur le cadenas rouge.
- Accepter les conditions liées au mode certificat non-signé.



- Cliquer sur le drapeau correspondant pour choisir la langue



- S'identifier pour accéder aux paramètres. Saisir **login** et **password** du **profil Administrateur** puis cliquer sur pour valider. Par défaut :

Login	admin
Password	admin

- Dans le menu **Paramètres avancés,** cliquer sur **Réseau** pour ouvrir la page

Paramètres réseau :

- Saisir les nouveaux paramètres dans **Configuration réseau.**
- Cliquer sur VALIDER pour enregistrer les modifications de la page.
- Cliquer sur APPLIQUER pour appliquer les modifications.

- En mode *Statique*, le navigateur web se connecte automatiquement à la nouvelle adresse IP.

- En mode *DHCP*, l'adresse IP est attribuée par le serveur DHCP.

Pour connaître cette adresse, positionner le dipswitch N°2 sur ON puis redémarrer le portier. L'adresse IP sera énoncée par la synthèse vocale.

A la fin de la manipulation, positionner le dipswitch N°2 sur OFF.

- Si le dipswitch N°1 est positionné sur ON, il est impossible de basculer en mode *Statique*. L'information s'affiche sous forme de pop-up :

3. Configuration

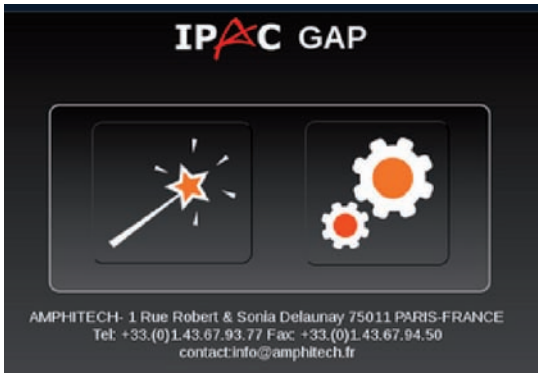
3.1. Configuration simplifiée ou Configuration avancée

- Vérifier les raccordements et connecter l'alimentation si le réseau ne fournit pas une alimentation POE+ (*Power over Ethernet, 802.3at*)
- La mise en service est réalisée avec les paramètres par défaut. L'adresse IP du portier à la livraison du produit est : 192.168.0.2
- Ouvrir un navigateur internet (Chrome, Firefox) et saisir dans la barre d'adresse http://192.168.0.2.

L'accès aux paramètres est réalisé via un HTACCES :

Login	admin
Password	admin

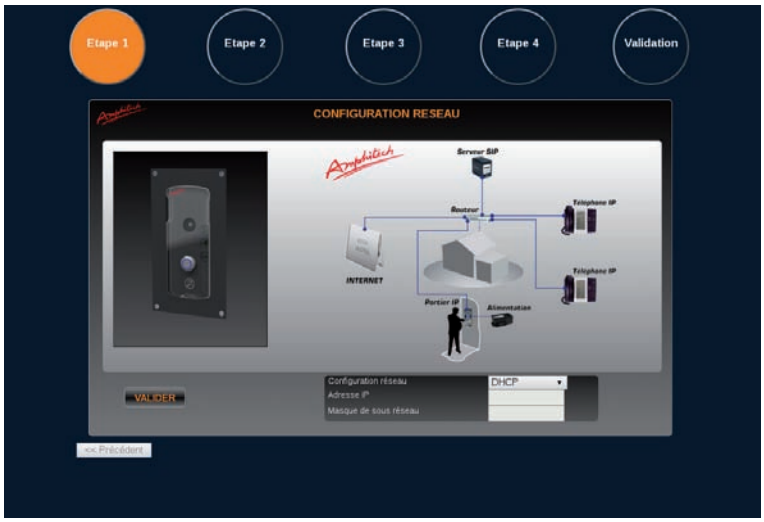
Après identification, la page suivante permet de choisir entre une configuration simplifiée et une configuration avancée.



3.2. Configuration simplifiée (Wizard)

Pour choisir la configuration simplifiée, cliquer sur l'icône  "baguette magique"

Étape 1 - Paramétrage du réseau avec visualisation du GAP IP

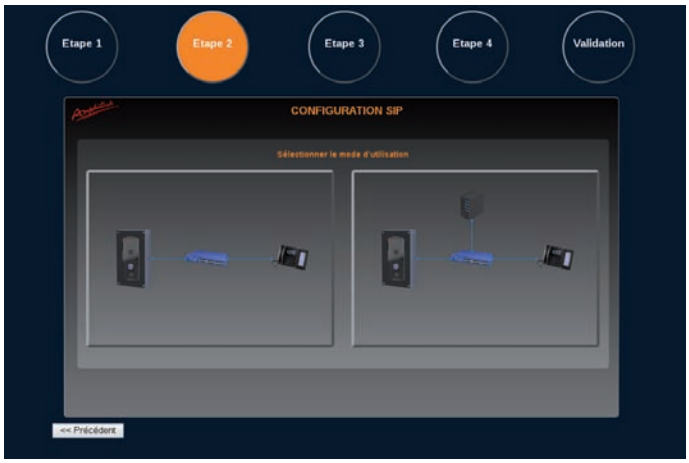


- Choisir : **Configuration réseau - Statique** ou **Dynamique** (l'adresse IP est donnée par la box Internet ou le switch du réseau disposant d'un serveur DHCP)
- En mode **Statique**, renseigner les paramètres **Adresse IP** et **Masque de sous réseau**

Cliquer sur le bouton 

pour passer à l'étape suivante :

Étape 2 - Choix Mode Peer to Peer ou Mode IPBX



Étape 3 - Mode Peer to Peer ou Étape 3 - Mode IPBX

Mode Peer to Peer

Mode IPBX

3.2.1. Mode Peer to Peer

Le mode Peer to Peer permet d'appeler de postes à postes en utilisant les adresses IP comme numéro de téléphone.

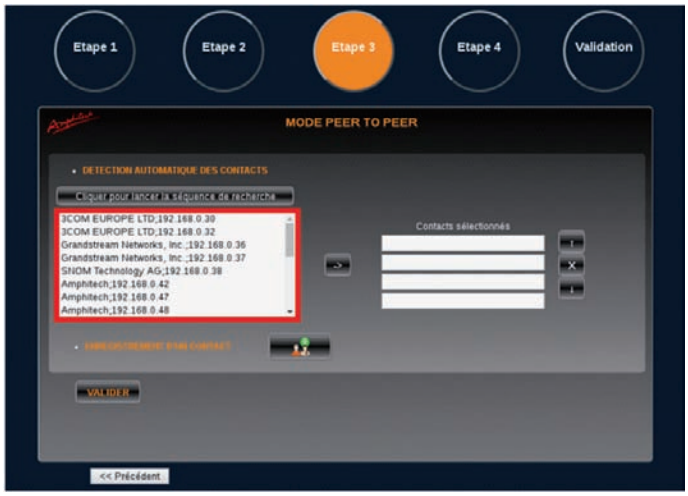
- La recherche de contacts par appui sur 

scanne le réseau à la recherche de périphériques SIP, téléphones, tablettes avec logiciel de téléphonie SIP, etc...

Attention

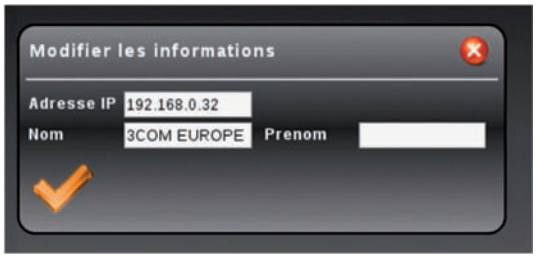
Prévenir l'administrateur réseau qu'une séquence de recherche (scan) va être effectuée sur le réseau local.

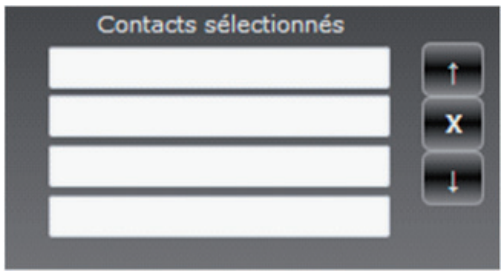
- La liste des périphériques réseaux trouvés s'affiche



- Sur sélection d'un contact dans la liste, l'appui sur 

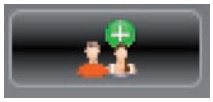
ouvre une fenêtre permettant de modifier les informations du contact sélectionné.



-L'aperçu de la liste des contacts permet de modifier l'ordre des contacts utilisés pour le mode enchaînement automatique (appel cyclique), 

à l'aide des flèches  et  .

Le bouton  permet de supprimer les contacts dans la liste.

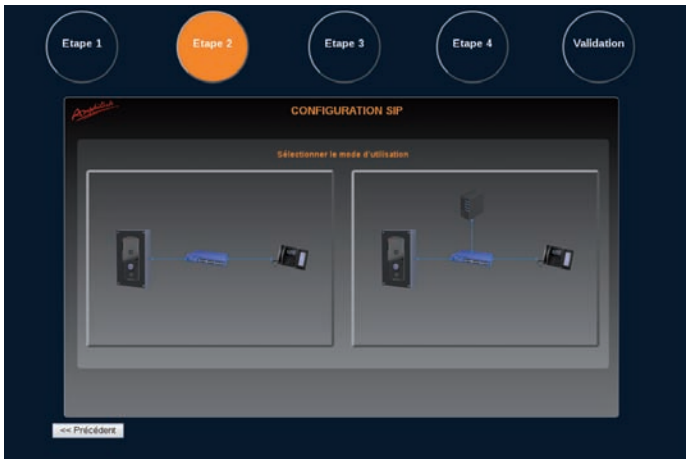
- Le bouton  permet d'ajouter manuellement un périphérique non trouvé lors de la séquence de recherche. Le numéro peut être enregistré sous forme d'adresse 192.168.xxx.xxx ou sous la forme « sip : 192.168.xxx.xxx ».

Cliquer sur le bouton 

pour passer à l'étape suivante.

3.2.2. Mode IPBX

Le mode IPBX permet de raccorder l'IP-GAP sur un réseau IP local équipé d'un serveur SIP :



- Les numéros d'appels seront attribués par le serveur SIP. L'échange du flux média (audio + vidéo) est supervisé par le serveur.

- Serveur SIP : saisir l'adresse IP de l'IP-PBX
- Nom d'utilisateur : nom nécessaire à l'enregistrement auprès de l'IP-PBX (numéro extension SIP)
- Identifiant utilisateur : habituellement identique au nom d'utilisateur
- Mot de passe : mot de passe utilisé lors de l'enregistrement auprès de l'IP-PBX
- Sur appui du bouton  la fenêtre d'ajout d'un contact s'ouvre. Remplir les champs :

- Numéro : indiquer le numéro d'appel (ex: 1000) du destinataire ou saisir l'adresse SIP complète (ex : 1000@192.168.0.252)
- Nom / Prénom : nom et prénom du contact dans la liste

- L'aperçu de la liste des contacts permet de modifier l'ordre des contacts avec les flèches  et  pour le mode enchaînement de numéro (appel cyclique).

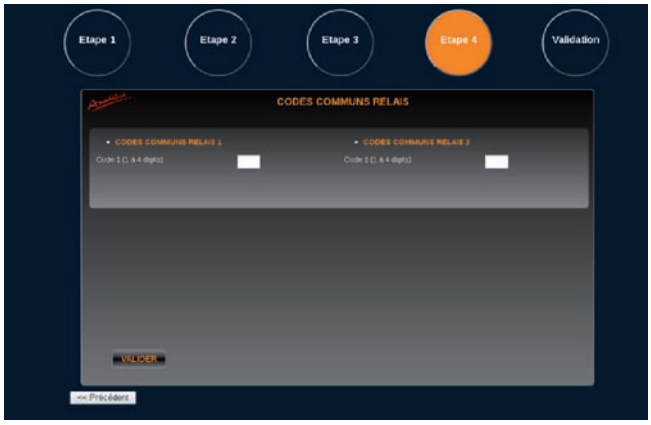
- Le bouton  permet de supprimer les contacts dans la liste  .
-

Cliquer sur le bouton  *pour passer à l'étape suivante.*

3.2.3. Codes communs relais de gâche

Étape 4 - Codes communs relais de gâche

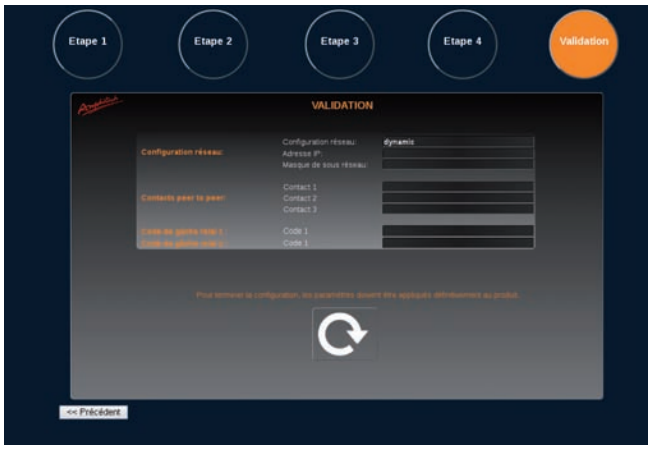
- La dernière étape permet d'ajouter un code de gâche pour les deux relais :

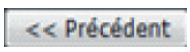


Cliquer sur le bouton  *pour passer à l'étape "Validation".*

3.2.4. Validation

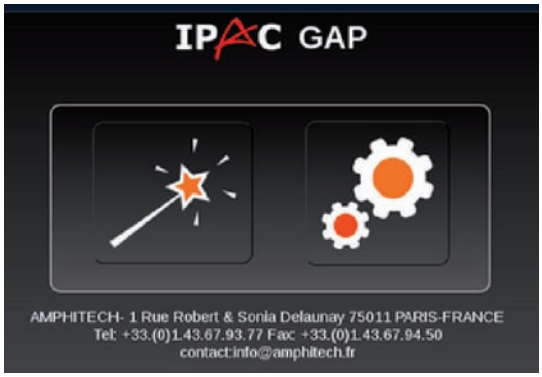
La dernière fenêtre est un écran de validation de l'ensemble des paramètres saisis sur les étapes précédentes.



- *Cliquer sur le bouton*  *pour redémarrer et sauvegarder les modifications. Le bouton*  *peut être utilisé à tout moment pour revenir aux étapes précédentes.*

3.3. Configuration avancée (administrateur)

Après identification, la page suivante permet de choisir entre la configuration simplifiée et la configuration avancée :



Cliquer sur  pour accéder à la configuration avancée.

3.3.1. Informations générales sur le produit

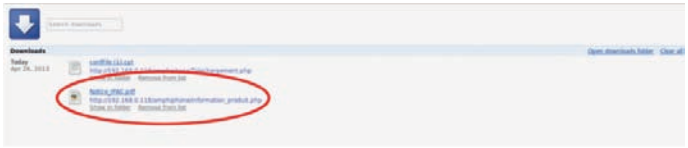
- **Informations produit** :
  - *Identité du produit* : numéro attribué au portier par l'administrateur
  - *Type de produit* : GAP
  - *Code du produit* : IP-GAP-01V
  - *Version firmware* : version logicielle du portier
  - *Version pages WEB : numéro de version actuelle des pages web*
  - *Adresse MAC* : lecture de l'adresse MAC
  - *Date et heure* : heure du système
  - *Type d'alimentation* : alimentation externe ou PoE+
  - *Température CPU* : en °C
- **Paramètres IPBX**
  - *Compte SIP* : adresse SIP du portier
  - *Status* : indication enregistrement sur IP-PBX.

- **Paramètres Peer to Peer** (appel en mode réseau "poste à poste")
  - *Adresse SIP* : par défaut en Peer to Peer *sip : ipacGap@192.168.0.2.*

    Si le mode IPBX est choisi, le champ est vide.

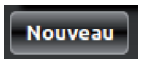
    Si l'adresse n'est plus l'adresse par défaut, *sip : ipacGap@adresse produit.*
- **Paramètres réseau** :
  - *Adresse IP* : adresse IP du produit
  - *Configuration réseau* : statique (adresse IP fixe) ou dynamique (gestion automatique des adresses IP)
  - *Masque de sous réseau* : masque de sous réseau
  - *Passerelle* : adresse IP de la Gateway (passerelle)
  - *DNS primaire* : adresse IP de la Gateway (passerelle)
  - *DNS secondaire* : adresse IP du DNS secondaire
  - *Uptime* : temps de fonctionnement depuis la mise en marche du produit
  - *Paquets et Bytes* : flux réseau vers le portier

- La touche  permet d'accéder à la notice d'exploitation du produit 

- Il est possible d'ouvrir ou de sauvegarder le fichier 

- Téléchargement local du soft ASIP STREAM, se reporter au wiki.amphitech.fr.

3.3.2. Liste des contacts

Cliquer sur 

pour créer un contact. Une fenêtre s'affiche 

avec :

- L'attribution d'un Numéro (si numéro seul, le système modifie le numéro avec la syntaxe SIP en *Sip : numéro@adresse serveur SIP*, à l'appui sur le bouton ).

- Le choix du proxy SIP pour le contact, s'il y a plusieurs comptes SIP IP-PBX.
- L'attribution d'un Nom
- L'attribution d'un Prénom
- L'enregistrement d'un contact en Peer to Peer (p2p) afin de l'utiliser comme "contact de secours" dans les contacts dédiés à l'enchaînement des numéros en mode IPBX. Dans le cas d'une panne de serveur par exemple, seul ce contact Peer to Peer sera fonctionnel.

A chaque changement de page web, cliquer sur 

pour sauvegarder les paramètres de la page.

Une fois toutes les modifications réalisées, cliquer sur 

pour redémarrer le portier.

3.3.3. Relais de télécommande

- *Configuration relais* : Gâche ou Information Prise de Ligne ou Défaut secteur ou Défaut réseau
- *Temps de maintien Gâche* : de 1 à 25 secondes
- *Temps de maintien Info Appel* : de 1 à 9 secondes ou permanent

L'information PDL s'active sur :

- l'appel sortant, de l'émission de l'appel à la fin de la tempo ou au raccroché,
- l'appel entrant, à partir du début de la sonnerie à la fin de tempo ou au raccroché.

Les deux relais peuvent être utilisés pour remonter des alertes sur :

- Problème d'alimentation secteur / PoE+ , au boot le relais 1/2 se colle (position commun-travail), sur coupure d'alimentation, le relais se décolle (position commun-repos)
- Problème Network (réseau IP) : plus de connexion réseau IP, problème d'enregistrement vers IP-PBX, le relais se colle (position commun-travail).

Important

Si le Relais 1 ou le Relais 2 sont configurés en Information PDL, Défaut secteur ou Défaut réseau, ils ne peuvent être utilisés lors d'une activation de l'entrée.

3.3.4. Code communs relais

- Possibilité d'attribuer 4 codes par relais, avec ou sans plage horaire.
- Ces codes sont activés uniquement en mode distant (DTMF).

Pour confirmer les changements de la page, cliquer sur VALIDER.

3.3.5. Plages horaires

Les 4 plages horaires peuvent être attribuées aux :

- bouton appel,
- codes d'accès,
- entrée,
- volume audio.

Chaque plage dispose de plusieurs tranches horaires. Chaque tranche horaire peut être sélectionnée 1/4 h par 1/4 h. Un double clic dans une case permet de sélectionner 1 heure entière.

Tranche horaire sélectionnée, appel autorisé

Tranche horaire non sélectionnée, appel non autorisé

Il est possible de nommer les plages horaires grâce au champ :

Pour confirmer les changements de la page, cliquer sur VALIDER.

3.3.6. Paramètres portier

- Identité
  - *Identité du produit*
  - *Adresse d'installation*: adresse physique de l'emplacement du portier.

- Options d'appel
  - *Délai de réponse sur appel entrant* : de **1 à 9 secondes, immédiat ou manuel** (appui bouton d'appel).
  - *Délai de réponse sur appel sortant* : de **10 à 60 secondes,** utilisé pour le mode cyclique (enchaînement automatique), délai entre deux numéros si destinataire occupé, introuvable ou configuré en "Ne pas déranger" (DND).
  - *Tempo de communication* : de **1 à 9 minutes ou permanent**.
  - *Fin de communication après commande d'ouverture de gâche* : oui pour obtenir la fin de communication sur fin de gâche.
  - *Temps d'appui bouton* : de **0,1 seconde à 5 secondes**, temps d'acquisition sur le **bouton d'appel** et le **bouton de commande d'ouverture de porte**.
  - *Fin de communication par appui sur le bouton* : **Oui** pour obtenir la fin de communication par appui sur le bouton du portier.

Pour confirmer les changements de la page, cliquer sur VALIDER.

3.3.7. Configuration de l'entrée

- Pour l'entrée, il est possible de configurer :
  - *État de l'entrée* : valide ou invalide.
  - *Activation relais*: Relais 1, Relais 2 ou Relais 1+2
  - *Fonction entrée* : Gâche / Appel jour (appel la liste de contact en mode jour, sauf pour le mode bouton en Gâche/ Appel, les contacts seront ceux utilisés en bouton mode nuit, voir **Mode 3 §4.2.8**
    - Bouton d'appel (fonctionnement identique à celui du bouton d'appel)
    - Gâche (Relais 1 ou Relais 2 ou Relais 1 et Relais 2)
    - Appel jour (appel de la liste de contacts en mode jour sauf pour le mode bouton en Gâche/ Appel, les contacts seront ceux utilisés en bouton mode nuit, voir **Mode 3 §4.2.8**
    - Appel d'une liste différente du bouton d'appel (l'entrée peut être utilisée comme deuxième bouton d'appel)
  - *Configuration de l'entrée* : **N**ormalement **O**uvert ou **N**ormalement **F**ermé
  - *Temps d'activation de l'entrée* : de **0,5 à 5,5 secondes**
  - *Plage horaire* : attribution d'une plage horaire

> **Important**
>
> – Si l'un des relais est configuré en **Information Prise De Ligne, Défaut alimentation ou Défaut réseau** et la fonction entrée en mode Gâche, le relais ne sera pas présent.
>
> – Si les deux relais sont configurés en **Information Prise De Ligne, Défaut alimentation ou Défaut réseau** la fonction entrée Gâche est indisponible.

Pour confirmer les changements de la page, cliquer sur VALIDER.

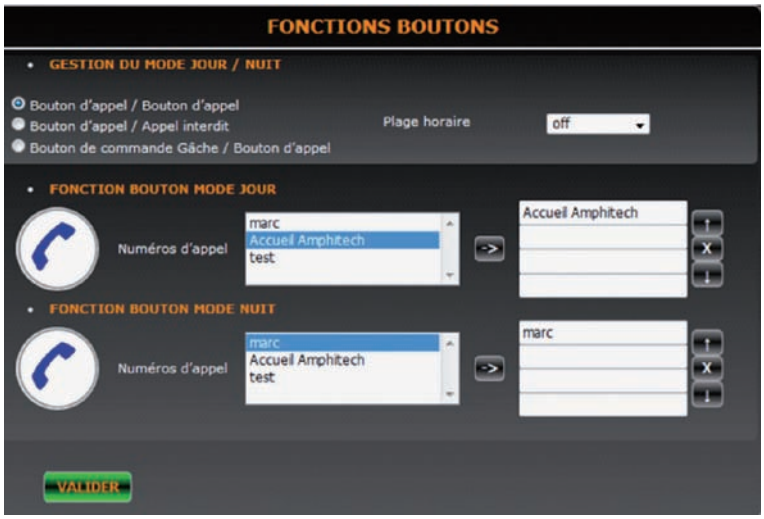
3.3.8. Configuration du bouton d'appel

A retenir

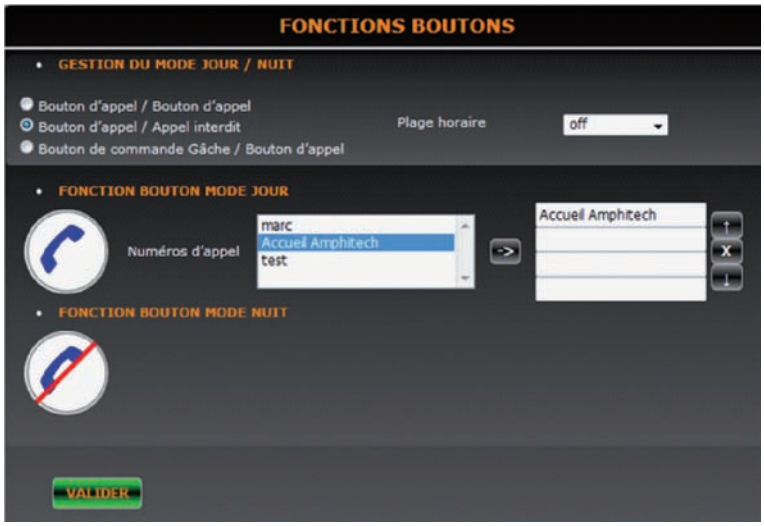
- Fonction bouton mode Jour : fonctionnement du bouton d'appel à l'intérieur des tranches horaires sélectionnées.
- Fonction bouton mode Nuit : fonctionnement du bouton d'appel en dehors des tranches horaires sélectionnées.
- Numérotation vers 1 à 4 correspondants via un IP-PBX et/ou une adresse IP.

Il existe 3 modes de fonctionnement à configurer dans l'onglet Boutons :

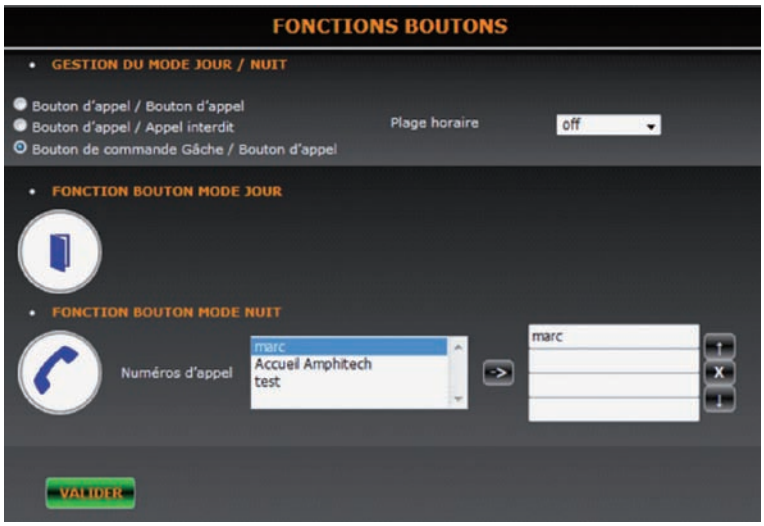
- **Mode 1** : appel de 1 à 4 correspondants le **Jour** ; appel de 1 à 4 correspondants la **Nuit** :



- **Mode 2** : appel de 1 à 4 correspondants le **Jour**, appel interdit la **Nuit** :

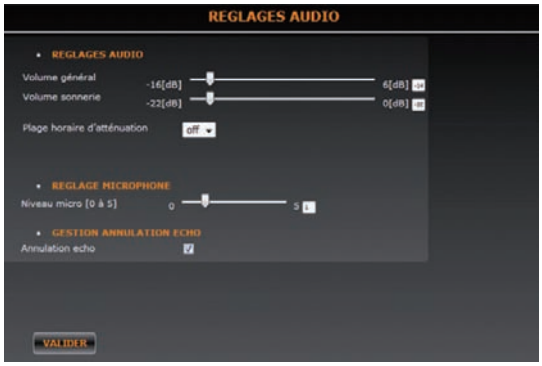


- **Mode 3** : mode commande de Gâche le **Jour** et appel de 1 à 4 correspondants la **Nuit** :



Pour confirmer les changements de la page, cliquer sur VALIDER.

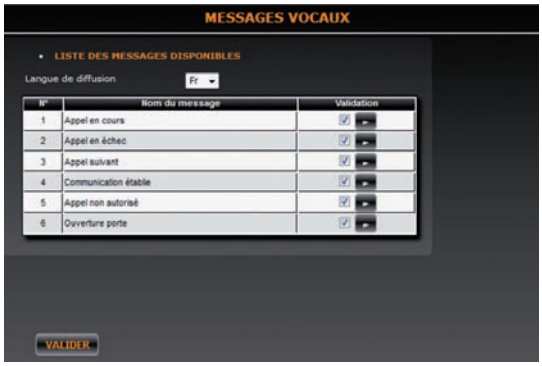
3.3.9. Réglages audio

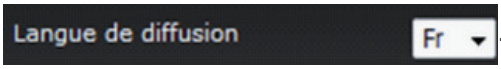


- *Volume général* : gestion des niveaux audio.
- *Volume sonnerie* : gestion du niveau sonore de la sonnerie sur appel entrant.
- *Plage horaire d'atténuation* : affectation d'une plage horaire avec atténuation (zone noire = atténuation ; zone orange = pas d'atténuation) du volume général.
- *Niveau du microphone* : gestion du niveau de sensibilité du microphone.
- *Annulation écho* : cocher pour activer.

Pour confirmer les changements de la page, cliquer sur VALIDER.

3.3.10. Messages vocaux



- La langue d'exploitation est initialisée à l'aide de l'onglet 

.

  La langue des messages vocaux est identique.
- Cocher la case  pour activer ou désactiver le message vocal.

Pour confirmer les changements de la page, cliquer sur 

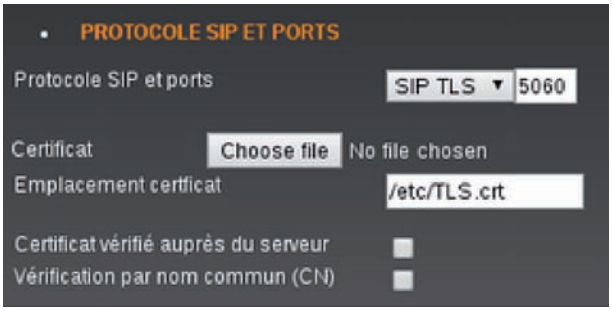
.

3.3.11. Paramètres réseau

- **Configuration réseau**
  - *Statique* : adresse IP définie par l'administrateur réseau (adresse fixe).

    ou
  - *Dynamique* : adresse IP attribuée automatiquement par un serveur DHCP.
  - *Adresse IP* : adresse IP du produit.
  - *Masque de sous réseau* : masque de sous réseau.
  - *Passerelle* : adresse IP utilisée pour accéder au WAN (*Wide Area Network*)
  - *DNS primaire* : adresse IP du premier serveur DNS.
  - *DNS secondaire* : adresse IP du second serveur DNS.
- **NAT** : 3 modes de connexion possibles à Internet :
  - *Connexion directe Internet,*
  - *Derrière NAT /Firewall - Passerelle* : connexion via un serveur NAT - Passerelle, adresse IP du serveur NAT,
  - *Derrière NAT/Firewall - Serveur STUN,* : connexion via un serveur NAT/STUN - Serveur STUN, adresse IP du serveur STUN.
  - *ICE* : permet de trouver le chemin optimum pour les appels audio-vidéo.
  - *Symmetric RTP* : flux RTP (audio/vidéo), symétrique ou non
- **Protocole SIP et Ports**
  - *SIP (TCP/UDP ou TLS)* : choix du protocole de transport SIP. *Port* : Numéro du port SIP (Par défaut 5060)

    Si le SIP TLS est activé :
    - *Certificat* : sélectionner un certificat signé ou non signé.
    - *Emplacement du certificat*: le certificat sera renommé sous TLS.crt. La validité du certificat et le nom commun du serveur contenu dans le certificat peuvent être vérifiés par le serveur.



- **Cryptage média**
  - *none :*aucun cryptage
  - *SRTP :*cryptage audio vidéo SRTP
  - *ZRTP :*cryptage audio vidéo ZRTP
- **Ports audio/vidéo**
  - Audio RTP/UDP : numéro de port.
  - Vidéo RTP/UDP : numéro de port.

Pour confirmer les changements de la page, cliquer sur VALIDER.

3.3.12. RADIUS 802.1X

Afin de protéger le réseau Ethernet filaire, nous préconisons la mise en en place d'un serveur Radius.

La norme 802.1x permet l'authentification du matériel IP avant tout accès au réseau filaire ou Wifi.

Les authentifications sont sécurisées, et les échanges se font :

- sur un chiffrement **Mode EAP** « simple » : md5 **ou** MSCHAPv2

Ces deux modes nécessitent une **identité** et un **password**.

- des modes sécurisés **EAP** : PEAP, EAP-TTLS, EAP-TLS.

En mode EAP : **PEAP** ou **TTLS** l'ensemble fonctionne sur le principe d'un **identifiant (identité)** et d'un **password** avec possibilité d'utiliser des certificats serveur / demandeur.

1. En fonction de la configuration du serveur dans chaque mode EAP il est possible de régler le protocole d'authentification **eap** (2ème phase d'authentification) :

   Pour le EAP-TTLS **Authentification eap** : PAP, MD5, CHAP, MSCHAPv2.

   Pour le EAP-PEAP **Authentification eap** : PAP, MD5, CHAP, MSCHAPv2 et TLS.

   Exemple serveur (Free Radius) :

   Dans la configuration générale d'EAP, si besoin selon votre version, remplacer la ligne

   default_eap_type = ttls

   Dans la configuration du TTLS

   ttls {

   # The tunneled EAP session needs a default

   # EAP type which is separate from the one for

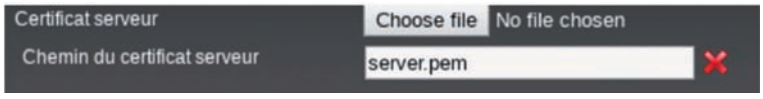
   # the non-tunneled EAP module …

   default_eap_type = md5

   }

2. Ensuite, il est possible ou non d'utiliser la vérification d'un certificat serveur dans le procédé d'authentification pour le **Mode EAP : PEAP et TTLS**. Cette nécessité de certificat se paramètre côté serveur.

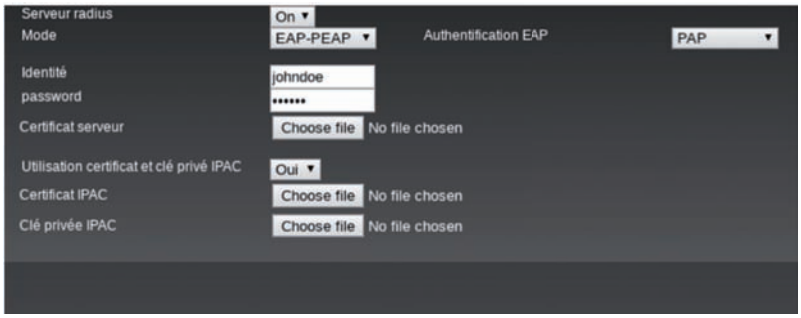
   Pour utiliser un certificat serveur auto-signé ou signé par une autorité de certification, il faut importer le certificat CA.pem dans l'IPAC. Si aucun fichier de type *.pem* n'est importé, l'IPAC ne transmettra pas le certificat au serveur (si nécessaire), et l'authentification échouera.



3. Certaines configurations de serveurs ne nécessitent pas le contrôle du certificat demandeur (IPAC) et utilisent la méthode de certificat symétrique en utilisant le certificat et la clé privée du serveur lors de la phase « Certificate server Key Exchange ».

   Or dans certaines configurations serveur il est possible de demander à l'IPAC son propre certificat ainsi que sa clé privée pour le processus d'authentification.

Si l'option « **utilisation certificat et clé privés IPAC** » est passée à « **oui** », alors :



- Ajouter manuellement un certificat et clé privé au format X.509 (auto-signé ou signé par une autorité) pour le mode EAP : PEAP ou TTLS.
- Utiliser la génération automatique de cette paire par la page web « **génération de certificat et clé privé** ».

> **Attention**
>
> Vérifier l'heure et la date de l'IPAC avant de générer un certificat.

- Utiliser le certificat et clé privé Amphitech par défaut (si aucun certificat et clé importés).

En mode EAP : **TLS**

Cette méthode nécessite une authentification mutuelle entre le serveur et le demandeur (IPAC),**Utiliser obligatoirement : certificat Serveur, clé privé pour l'IPAC, passphrase de la clé privée.**

Il n'y a plus dans ce cas d'utilisation de paire login/password, mais l'utilisation d'un **mot de passe de clé privé** (passphrase) utilisé pour générer la clé privée et le certificat pour l'IPAC (format PKI).

Il est possible de passer en mode Anonymous (plus d'identité au niveau du serveur) dans ce cas, dans la partie « identité » saisir : **anonymous**.

Dans ce cas la page web de génération de certificat et de clé privé ne peut pas être utilisée.

Le certificat émis par une PKI est sous forme d'un fichier PKCS (extension. p12) contenant :

- La clé privée

> **Attention**
>
> Le .p12 contient déja le certificat client , ne pas ajouter de certificat client IPAC.

- Le certificat associé (clé publique signée par l'autorité)

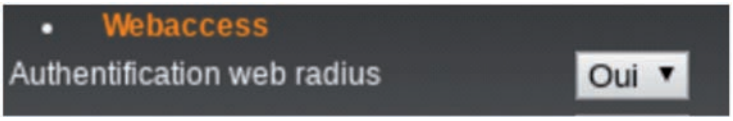
Il faudra alors remplir tous les champs de la page :

4. **Accès web par authentification serveur Radius**

   Le Serveur Radius permet aussi de gérer l'authentification des comptes (Accounting) via la méthode PAP pour accèder aux pages web de paramétrage du portier.

   La méthode initiale interne à l'IPAC permet de créer des comptes locaux d'administration et d'utilisation comme attributs :

   - **Login**
   - **Mot de passe**
   - Droits d'utilisation : **Administrateur** ou **utilisateur**

   En activant la solution 

l'authentification interne à l'IPAC fonctionnera encore si le login et le mot de passe

   correspondent, l'accès aux pages s'effectuera en fonction des droits d'utilisation du compte local.

L'authentification interne

Si le login et/ou le mot de passe ne correspondent pas à un compte interne à l'IPAC, et si la méthode RADIUS est activée, alors l'IPAC enverra une requête de demande d'authentification au serveur Radius si :

- **L'adresse IP du serveur Radius** est renseignée.
- **Le mot de passe Radius** créé pour le client IPAC lors de la création du compte client sur le serveur est renseigné.
- Les Ports d'**authentification** et de **comptabilisation** sont renseignés.

Dans tous les cas si aucun login/password ne correspond à un compte local IPAC ou sur le serveur Radius, l'authentification échouera, la connexion aux pages sera impossible.

Exemple 3.1. Exemple pour un serveur Free Radius

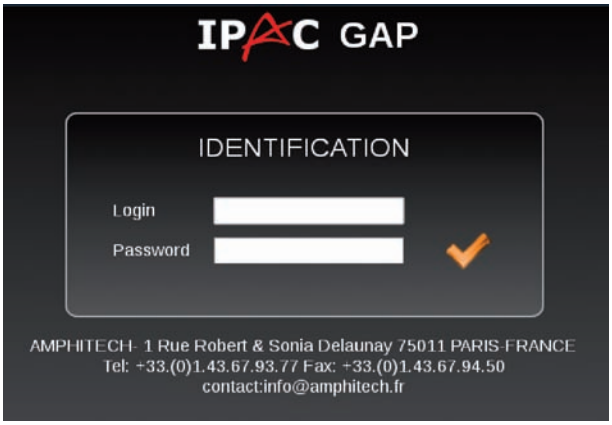
Création d'un compte client IPAC pour l'authentification (/etc/freeradius/client.conf) :

- Déclaration de l'adresse IP de l'IPAC
- Password secret (ipac1234)

```
#######################################################################
#
#  Per-socket client lists.  The configuration entries are exactly
#  the same as above, but they are nested inside of a section.
#
#  You can have as many per-socket client lists as you have "listen"
#  sections, or you can re-use a list among multiple "listen" sections.
#
#  Un-comment this section, and edit a "listen" section to add:
#  "clients = per_socket_clients".  That IP address/port combination
#  will then accept ONLY the clients listed in this section.
#
#clients per_socket_clients {
#       client 192.168.3.4 {
#               secret = testing123
#        }
#}

client 192.168.0.39 {
        secret = ipac1234
}
```

- Création d'un utilisateur (login) d'accès web (user. Conf)
  - Login : **johndoe**
  - Password : **123456789**
  - Droits d'accès : **Administrative-User** *(droit admin IPAC)* ou **Login-User** *(droit utilisateur IPAC)*

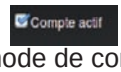
```
# #
# # Last default: shell on the local terminal server.
# #
# DEFAULT
#       Service-Type = Administrative-User

# On no match, the user is denied access.

johndoe   Cleartext-Password := "123456789"
        Service-Type = Administrative-User
```



Dans cette fenêtre d'identification du login, si l'option radius est activée, il est possible de s'authentifier soit·:

- Admin /mot de passe compte administrateur local (toujours valide).
- Login /mot de passe (compte créé localement sur l'IPAC)
- Login/ mot de passe via RADIUS, exemple : johndoe /123456789 permettant d'ouvrir la page dans ce cas Administrateur.

3.3.13. Paramètres SIP

- **Paramètres IPBX**
  - *Compte SIP x*: possibilité d'utiliser 3 comptes SIP sur différents IP-PBX **ATTENTION**: le LDAP utilise le compte SIP 1.
  - *Compte actif* : cocher la case 

pour activer l'utilisation du compte SIP. Si la case est décochée le portier passe en mode de connexion Peer to Peer.
  - *Expiration [sec]* : durée de la session avant une nouvelle demande d'enregistrement auprès de l' 'IP-PBX.
  - *Serveur SIP* : adresse IP de l'IPBX.
  - *Domaine*: indiquer le nom si le proxy se trouve dans un domaine.
  - *Port*: port d'enregistrement SIP
  - *Route*: utiliser si le routage des appels nécessite une passerelle spéciale
  - *Nom d'utilisateur*: nom d'affichage SIP, **le nom ne doit pas comprendre de caractère Espace.** Il permet de choisir en mode appel P2P un nom de contact personnalisé qui s'affichera sur le

téléphone SIP distant (lors d'un appel sortant de l'IPAC). En mode Compte SIP actif, le contact est géré par l'IP-PBX.

– *Identitifiant utilisateur* : identifiant nécessaire à l'enregistrement auprès de l'IP-PBX.

– *Identité SIP* : s'il est vide, ce champ se remplit automatiquement après un clic sur VALIDER avec les champs numero@ adresse IP serveur SIP :Port

soit

Identité SIP : numero@ adresse IP serveur SIP :Port

– *Mot de passe*: mot de passe utilisé lors de l'enregistrement auprès de l'IP-PBX.

Notification présence proxy (activation SIP PUBLISH) : oui - non

Pour confirmer les changements de la page, cliquer sur VALIDER.

3.3.14. Codecs audio

- **Choix des codecs audio** : codecs utilisés lors d'une communication vocale entre l'IP-GAP et le poste du correspondant. Pour chaque codec :
  – Déplacer le codec choisi de la liste "Disponibles" à la liste "Sélectionnés" à l'aide des fléches -> <-.
  – Utiliser les flèches ↑ ↓ pour modifier l'ordre de priorité dans la liste des codecs sélectionnés.

  Exemple 3.2. Ordre de priorité des codecs sélectionnés

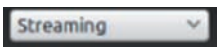
  – *Priorité 1* : opus
  – *Priorité 2* : speex16k
  – *Priorité 3* : speex8k, etc.

- **Transport DTMF** : choix des standards :
  – *RFC2833* : transmission des codes DTMF conforme à la norme RFC2833.
  – *SIP info* : transmission des codes DTMF conforme à la norme RFF2976.
  – Si aucun des 2 standards n'est sélectionné, le mode de transport est "in band".

- **Compatibilité CISCO rtcp-fb**
  – *Si la case est cochée, l'attribut média rtcp-fb dans la trame SDP n'est pas envoyé.*

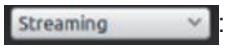
Pour confirmer les changements de la page, cliquer sur VALIDER.

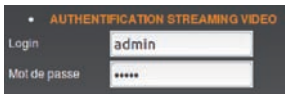
3.3.15. Paramètres vidéo

Choix du mode vidéo : il existe deux modes vidéo  ou 

- Mode  : *la vidéo est transmise uniquement durant la communication.*

  – Résolution vidéo, choisir entre les deux résolutions proposées :

- Mode  : *l'accès au mode streaming est sécurisé par un login et un mot de passe*

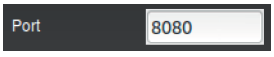


  – SnapShot (non/oui) : permet de prendre une photo au début du lancement de l'appel (par appui bouton) et de l'envoyer par Email à un destinataire (si compte Email actif). En mode vidéo, en communication, la fonction est indisponible.

  – Qualité vidéo, choisir entre les trois qualités proposées :

    - Basse : 5 images/seconde - 60% de compression
    - Moyenne : 10 images/seconde - 40% de compression
    - Haute : 15 images/seconde - 0% de compression

  – Résolution vidéo, choisir entre les deux résolutions proposées :

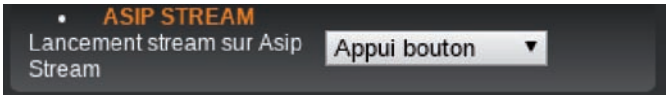
  – Port vidéo : 

  – Connexion au flux vidéo, il est possible de se connecter au flux vidéo de la caméra avec :

    http*://adresseIP:port/?action=stream*

    La visualisation du streaming est aussi réalisée sur les page web une fois le login et le mot de passe renseignés.

– **ASIP STREAM** : lancement de la vidéo sur appui bouton ou sur décroché du poste appelé.

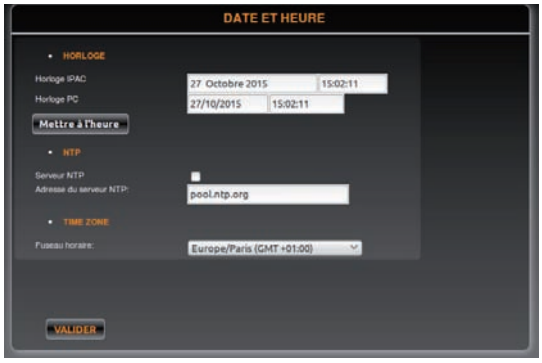


– L'onglet CODECS VIDEO n'apparaît que pour le mode vidéo en communication :

A gauche, la liste des codecs disponibles. A droite, la liste des codecs sélectionnés. L'ordre de priorité des codecs sélectionnés peut être modifié à l'aide des flèches.

Pour confirmer les changements de la page, cliquer sur VALIDER.

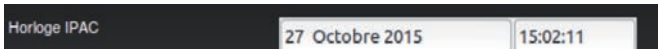
3.3.16. Date et heure



Important

La mise à l'heure du produit est importante pour la gestion des plages horaires.

- Heure actuelle de l'IP-GAP :



- Changer manuellement l'heure et la date :

- Cocher la case pour utiliser un serveur NTP et mettre à l'heure automatiquement l'IP-GAP. Renseigner une adresse de serveur NTP :

- Pour gérer le fuseau horaire et le changement automatique heure d'été/ heure d'hiver, sélectionner le fuseau dans la liste :

Pour confirmer les changements de la page, cliquer sur 

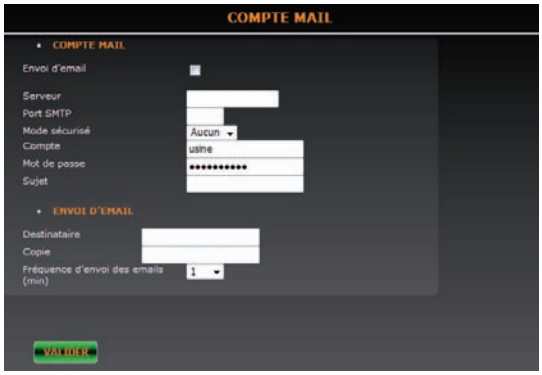
.

3.3.17. Compte mail

L'IP-GAP peut utiliser une adresse e-mail pour envoyer des rapports de fonctionnement ou d'anomalie à un destinataire. L'adresse e-mail du destinataire est modifiable dans l'onglet événements système.

Avertissement

Les comptes de messageries d'entreprises ont des règles strictes d'utilisation. Vérifier si le compte est utilisable par une application autre que celle utilisée en interne.

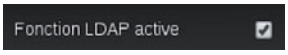


- *Envoi d'email* : cocher pour valider l'envoi d'e-mails.
- *Serveur*: saisir l'adresse du serveur d'envoi.
- *Port SMTP*: port utilisé
- *Mode sécurisé*: choisir le mode de cryptage : SSL / TLS ou clair.
- *Compte*: saisir adresse e-mail du compte émetteur.
- *Mot de passe*: saisir mot de passe du compte émetteur.
- *Sujet*: saisir l'objet.
- *Destinataire*: destinataire de l'e-mail.
- *Copie*: destinataire en copie de l'e-mail.
- *Fréquence d'envoi des e-mails*: à configurer, 1 à 30 minutes.

Pour confirmer les changements de la page, cliquer sur VALIDER

3.3.18. LDAP

Le système LDAP du portier offre la possibilité de synchroniser un répertoire stocké sur un serveur LDAP.

- Cocher la case 

pour utiliser le système LDAP. Si cette case est cochée, le répertoire du serveur sera récupéré lors du prochain redémarrage. Si cette case n'est plus cochée, le répertoire LDAP se sera plus affiché au prochain redémarrage.
- 

: saisir l'adresse IP et le port du serveur LDAP.
- *Nom d'utilisateur* : saisir le DN de l'utilisateur de connexion.
- *Mot de passe* : saisir le mot de passe.
- *Mise à jour auto des contacts LDAP* :
  - Non : pour une mise à jour à chaque redémarrage.
  - Chaque fin d'appel.
  - Toutes les 5 min, 15 min, 30 min, 45 min ou 60 min.
- *Base DN* : *Exemple* dc=pbx,dc=com, (le même que le DN de base ou d'un sous ensemble de la DN de base du serveur).
- *Nom d'attributs LDAP* : attribut du nom du contact.
- *Numéro d'attributs LDAP* : attribut du numéro d'appel du contact

Mode SIP. Si le portier est utilisé avec un serveur IP-PBX, veiller à renseigner les champs de connexion "Compte SIP" avant d'utiliser la synchronisation LDAP.

Mode P2P. Utiliser un attribut LDAP lors de la création de l'utilisateur dans le serveur et y saisir l'adresse IP. Dans le champ "Filtre numéro LDAP", utiliser ce nom d'attribut pour y récupérer l'adresse IP du contact.

Les cases  en face de chaque contact LDAP permettent de copier le contact LDAP vers la liste des contacts pour être visible dans l'attribution des boutons d'appels.

Pour prendre en compte les changements de la page, cliquer sur 

et 

pour redémarrer le portier.

3.3.19. API

1. ***API PORTE***

   Le code porte API correspond à un des codes communs RELAIS 1 ou 2. L'API porte est soumise à la plage horaire ou au type d'activation du Code commun RELAIS 1 ou 2 (local/Distant). En défaut usine USER et PASSWORD sont : admin et admin

   Dans l'exemple, l'utilisateur =toto avec mot de passe =titi.

   Le code du relais = 1234 correspond à un des 4 codes communs relais 1 ou 2.

   Authentification NONE :

   http://adresse_IP_IPAC/api/remote/?login=toto&password=titi&code=xxxx (GET)

   curl -d "code=1234&login=toto&password=titi" -X POST http://adresse_IP_IPAC/api/remote (POST)

   Authentification BASIC :

   http://toto:titi@adresse_IP_IPAC/api/remote/?code=xxxx (GET)

   curl -d "code=1234" -X POST http://toto:titi@adresse_IP_IPAC/api/remote (POST)

   Authentification DIGEST :

   http://toto:titi@adresse_IP_IPAC/api/remote/?code=xxxx (GET, mode Hashé) (GET)

   curl -d "code=1234" -X POST http://toto:titi@adresse_IP_IPAC/api/remote --digest (POST)

   Il est possible pour les méthodes GET et POST le mode « https » dans la requête à la place du « http ».

   Pour l'utilisation « https » sous CURL on ajoute - - insecure (certificat non signé)

   Attention : Le mode d'authentification est sauvegardé dans le cash de la page tout au long de l'ouverture de celle-ci.

Codes retours :

-200 OK = code OK

-403 Forbidden (mauvais code, type activation non distante)

-401 Unauthorized (plage horaire non active)

-423 LOCKED : Relais passés en PDL ou NETCUT

-480 Temporarily Unavailable (code en cours)

Exemple 3.3. Exemples Format JSON et URL Encoded :

POST:

curl -X POST -d '{"code":"1111"}' http://admin:admin@192.168.0.30/api/remote/ --digest --header "Content-Type: application/json"

POST:

curl -d "code=1111" -H "Content-Type: application/x-www-form-urlencoded" -X POST http://admin:admin@192.168.0.30/api/remote/ --digest

GET: (auth NONE/BASIC)

curl -H "Content-Type: application/x-www-form-urlencoded" http://admin:admin@192.168.0.30/api/remote/?code=1111

2. ***API VoIP***

Cette API permet de prendre le contrôle à distance de la partie téléphonie du produit.

- **Répondre à un appel entrant**

  POST:

  curl -d "type=answer" -H "Content-Type: application/x-www-form-urlencoded" -X POST http://admin:admin@192.168.0.30/api/voip/ --digest

  GET: (auth NONE/BASIC)

  curl -H "Content-Type: application/x-www-form-urlencoded" http://admin:admin@192.168.0.30/api/voip/?type=answer

- **Terminer une communication ou un appel entrant**

  POST:

  curl -d "type=terminate_all" -H "Content-Type: application/x-www-form-urlencoded" -X POST http://admin:admin@192.168.0.30/api/voip/ --digest

GET: (auth NONE/BASIC)

curl -H "Content-Type: application/x-www-form-urlencoded" http://admin:admin@192.168.0.30/api/voip/?type=terminate_all

- **Lancer un appel**

table:

Précise dans quelle table de base de donnée se situe le contact. Le format accepté est : liste – ldap – libre

id:

Précise l'index du contact dans sa base de données. Le format accepté est :

1 – 192.168.1.100 - 1000@proxy

Exemple 3.4. Exemples Format JSON et URL Encoded :

POST:

curl -d '{"type":"call","table":"libre","id":"sip:192.168.0.22"}' -H "Content-Type:

application/json" -X POST http://admin:admin@192.168.0.30/api/voip/ --digest

POST:

curl -d '{"type":"call","table":"liste","id":"4 [sip:192.168.0.22]"}' -H "Content-Type: application/json" -X

POST http://admin:admin@192.168.0.30/api/voip/ --digest

POST:

curl -d "type=call&table=libre&id=sip:192.168.0.22" -H "Content-Type: application/x-

www-form-urlencoded" -X POST http://admin:admin@192.168.0.30/api/voip/ --digest

GET: (auth NONE/BASIC)

curl -H "Content-Type: application/x-www-form-urlencoded"

http://admin:admin@192.168.0.30/api/voip/?type=call&table=libre&id=192.168.0.22 [_specify_]

3. **API AUDIO**

Cette API permet d'envoyer un fichier .WAV encodé en base64 dans l'URL, le fichier est ensuite diffusé dans le Haut-parleur du portier. (Max 1Mo)

- **Lire un fichier Wav**

  loop:

  Nombre de répétition du fichier audio. Dans le cas d'un nombre nul ou non précisé, le son sera diffusé en boucle indéfiniment. Intervalle : 0 - 9999

  Pour un fichier audio (payload.txt)

  Exemple contenu fichier payload.txt : {"type":"wav","loop" :"2","data":"UklGRmQfAABX-QVZFZm10IBAAA…..ouJiImHhA=="}

  Exemple 3.5. Exemples envoi fichier wav format Json :

  curl -X POST -d `cat payload.txt http://admin:admin@192.168.0.30/api/audio/ [_specify_] --digest --header "Content-Type: application/json" --header "Expect:"

  ou

  curl -X POST -d $(cat payload.txt) http://admin:admin@192.168.0.30/api/audio/ --digest --header "Content-Type: application/json" --header "Expect:"

- **Stopper la diffusion du fichier audio**

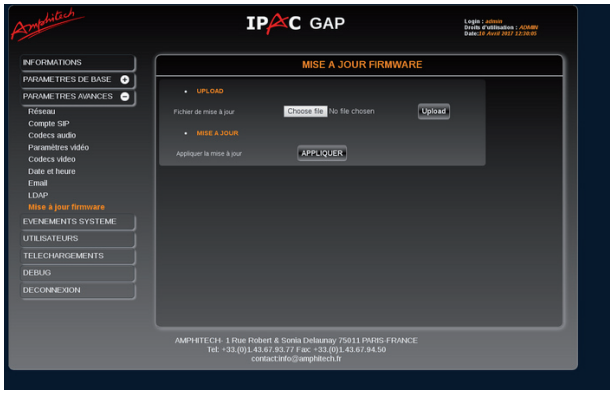
  Indique l'arrêt de la diffusion du fichier audio.

  Exemple 3.6. Exemple commande stop format URL encoded:

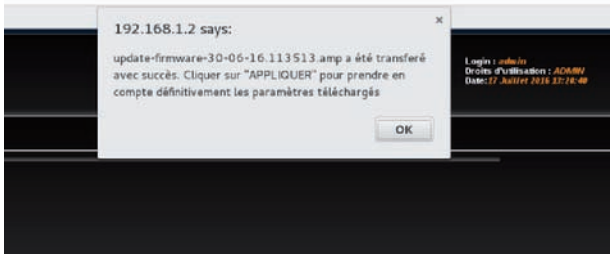
  POST: curl -d "type=wav&data=stop" -H "Content-Type: application/x-www-form-urlencoded" -X POST http://admin:admin@192.168.0.30/api/audio/ [_specify_] --digest

  GET: (auth NONE/BASIC) curl -H "Content-Type: application/x-www-form-urlencoded" http://admin:admin@192.168.0.30/api/voip/?type=wav&data=stop [_specify_]

3.3.20. Mise à jour Firmware



- Choose file permet de chercher un fichier de mise à jour .amp
- Upload permet de charger le fichier. Le fichier est vérifié par le système avant la mise à jour.



- APPLIQUER lance la procédure de mise à jour.

> **Attention**
>
> L'alimentation doit rester connectée à l'IP-GAP.

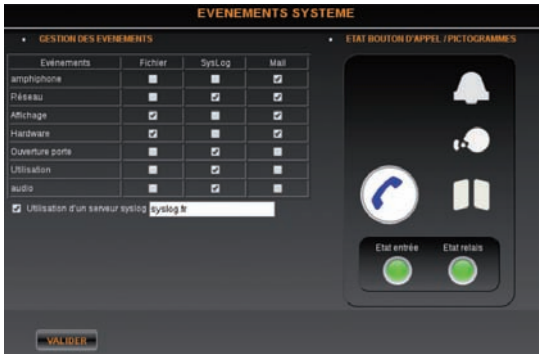
- Si la mise à jour est réussie, il est possible de revenir à la "version précédente".

- Si la mise à jour a échoué, l'accès aux pages web se fait en mode dégradé. Ce mode permet d'accéder à une version fonctionnelle ou antérieure.

Attention

Les contacts de la base de données doivent être sauvegardés. Les configurations SIP et les paramètres produits sont sauvegardés automatiquement.

3.3.21. Evénements système



- **A droite de cette fenêtre, la visualisation de l'écran du portier se fait en temps réel. Les pictogrammes "appel", "en communication" et "ouverture porte" s'allument avec la couleur définie en fonction de l'état du portier :**

Action / Etat portier	**Éclairage Pictogramme**
Appui bouton	
Communication	
Commande relais	
Pause en appel	
Réception d'appel	
Etat entrée / Etat relais = Libres	
Etat entrée / Etat relais = En fonctionnement	

Le tableau de **Gestion des événements** permet de choisir le type d'événements système pour envoi de notifications :

– *Amphiphone* : fonctionnement général de l'application.

– *Réseau* : tout ce qui concerne le réseau.

– *Affichage* : pour garder un historique de ce qui est affiché à l'écran.

– *Hardware* : les appuis boutons, les entrées, les relais, etc.

– *Ouverture de la porte* : commande d'ouverture de gâche.

– *Utilisation* : utilisation générale de l'application.

– *Audio* : volume, fichiers vocaux, etc.

- Il est possible d'utiliser un serveur Syslog pour stocker les événements d'un portier. Cocher la case et renseigner l'adresse et le port du serveur Syslog :

Pour confirmer les changements de la page, cliquer sur  .

3.3.22. Documentation technique Supervision Produit Amphitech SIP

Le produit IP Amphitech a pour but d'être connecté sur le réseau IP (Ethernet, wifi...) du client. Le système Amphitech permet en même temps de générer un appel vocal SIP, et d'envoyer des informations sous différentes formes pour identifier le type de matériel et la raison d'appel de l'appelant.

Un usagé, par action sur le bouton d'appel peut générer un appel de type Vocal. Le système Amphitech peut de manière autonome, suite à une détection d'anomalie de fonctionnement du système, émettre un appel de type technique ou test vers une centrale de télésurveillance où vers un numéro de responsable technique.

Ce système permet de s'interfacer sur des centrales d'appels SIP (réception de messages SIP) ou sur des centrales analogiques compatibles protocole GSM DTMF Amphitech.

*3.3.22.1. **Identification raison d'appel dans le Header From en mode Peer To Peer***

Raisons d'appels du produit A vers le produit B :

- Bouton Appel
- Défaut secteur / retour secteur
- Panne bouton d'appel (appui supérieur à 10 min) / fin de panne bouton d'appel
- Appel cyclique de test

Dans la méthode :**SIP INVITE** (méthode SIP de l'appelant *produit A* vers l'appelé *produit B*) on retrouvera dans le **Message Header : sip :identité_raisonAppel@adresse IP A**

- L'identité : 9 digits (de 0 à 9).
- Raison Appel (défaut usine) :

Valeurs	Raison d'appel	Type d'appel
bouton_appel	Bouton d'appel	Vocal
defautSecteur	Défaut secteur	Technique
retourSecteur	Retour secteur	Technique
retourBoutonALB	Retour bouton d'appel	Technique
panneBoutonALB	Panne bouton d'appel	Technique
test	Test cyclique	Test cyclique

- Adresse IP : adresse IP du produit A (sytème Amphitech)

Pour les raisons d'appels "Bouton d'appel" et "Test cyclique", les **valeurs** sont modifiables par les paramètres de l'application dans :

EVENEMENTS SYSTEM->Gestion appels techniques-> Gestion message Techniques P2P-> Bouton d'appel

EVENEMENTS SYSTEM->Gestion appels techniques-> Gestion message Techniques P2P-> Test Cyclique

Exemple 3.7. Exemple 1

Vue d'une trace SIP WireShark (espion protocole réseau)

*Image 1 : Trace WireShark **SIP INVITE** avec Header From contenant : l'ID_raison d'appel@adresse IP A du produit A appelant le produit B*

```
INVITE sip:192.168.0.22:5060 SIP/2.0
Via: SIP/2.0/UDP 192.168.0.33:5060;branch=z9hG4bK.FHUOzhRPQ;rport
From: <sip:000000000_bouton_appel@192.168.0.33>;tag=pMk4ZOaq~
To: sip:192.168.0.22
CSeq: 20 INVITE
Call-ID: zBtys-kw~P
Max-Forwards: 70
Supported: replaces, outbound
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, NOTIFY, MESSAGE, SUBSCRIBE, INFO,
UPDATE
Content-Type: application/sdp
Content-Length: 434
Contact: <sip:000000000_bouton_appel@192.168.0.33>;+sip.instance="<urn:uuid:fe421234-70b0-4878-ad77-
9b840cb681eb>"
User-Agent: Unknown (belle-sip/1.4.2)

v=0
o=000000000_bouton_appel 3528 3742 IN IP4 192.168.0.33
s=Talk
c=IN IP4 192.168.0.33
t=0 0
a=rtcp-xr:rcvr-rtt=all:10000 stat-summary=loss,dup,jitt,TTL voip-metrics
m=audio 7078 RTP/AVP 0 8 96 97 98 101 99 100
a=rtpmap:96 speex/8000
a=fmtp:96 vbr=on
a=rtpmap:97 speex/16000
a=fmtp:97 vbr=on
a=rtpmap:98 opus/48000
a=rtpmap:101 telephone-event/8000
a=rtpmap:99 telephone-event/16000
a=rtpmap:100 telephone-event/48000
```

Identification produit A

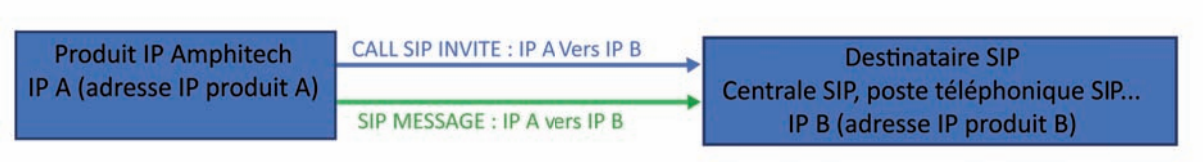
Exemple 3.8. Exemple 2

Appel de type vocal du produit B par le produit A suite à l'appui bouton sur le bouton d'appel du produit A

Côté appelé, produit B (GXV3240) affichage sur LCD :

Image 2 : ScreenShot appel entrant sur GXV3240 téléphone SIP (produit B), identification ID + raison de l'appelant du produit A

3.3.22.2. Identification raison d'appel dans un message SIP en mode Peer to Peer



Il est possible de valider l'envoi de **messages SIP** (du produit A) au même contact ou à un autre contact URI au format P2P, en même temps que l'appel vocal (méthode **SIP INVITE**) pour les raisons suivantes :

- Bouton Appel
- Défaut secteur / retour secteur
- Panne bouton d'appel (appui supérieur à 10 min) / fin de panne bouton d'appel
- Appel cyclique de test

Au format SIP MESSAGE : Text Plain

identity=000000000 ;product=product_code ;alerte=code

- **Identity** : 9 digits (de 0 à 9 avec 000000000 : défaut usine)
- **Product** :

Product code	Produit
81	IP-GAP / IPAC-200

- **Alerte**

Code	Produit
01	Bouton d'appel
04	Test cyclique
11	Retour secteur
12	Défaut secteur
17	Panne bouton d'appel
18	Retour bouton d'appel

Ci-dessous les messages reçus lors d'une raison d'appel vocal, technique ou de test cyclique vers un poste IP GRANDSTREAM GXV3240 (produit B) :

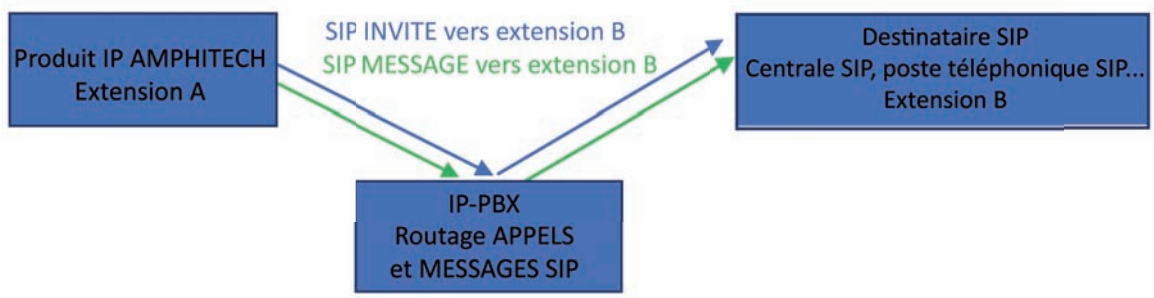
L'appelant (produit A) est identifié avec son identité + raison d'appel (*voir* §1), ainsi que la réception du message SIP (sur le produit B).

Image 3 : messages SIP reçus sur poste SIP Grandstream GXV3240

3.3.22.3. Identification raison d'appel dans un message SIP et header From en mode IP-PBX

*3.3.22.3.1. **Messages SIP***

Si le système IP (extension A) est enregistré sur un IP-PBX, l'extension A peut envoyer des **messages SIP** vers l'extension B en même temps que l'appel vocal vers l'extension B (**Méthode SIP INVITE**). L'ensemble appel SIP, et messages SIP seront relayés par l'IP-PBX (utilisation des numéros d'extensions).



Exemple : appel du GXV3240 par son numéro d'extension B (1000) à partir du numéro d'extension A (1007) du produit SIP Amphitech (info *: l'ensemble utilise un IP-PBX UCM6102*).

Image 4 : messages SIP reçus sur poste SIP Grandstream GXV3240 extension B, envoyé par l'extension A et relayé par l'IP-BX

Raisons d'appels extension A vers l'extension B

- Bouton appel
- Défaut secteur / retour secteur
- Problème d'enregistrement vers l'IP-PBX de l'extension A - Extension SIP appelée injoignable
- Panne bouton d'appel (appui supérieur à 10 min) / fin de panne bouton d'appel
- Appel cyclique de test

Au format SIP MESSAGE : Text Plain

identity=000000000 ;product=product_code ;alerte=code

- **Identity**: 9 digits (de 0 à 9 avec 000000000 :défaut usine)
- **Product :**

Product_code	Produit
81	IP-GAP / IPAC-200

- **Alerte :**

Code	Produit
01	Bouton d'appel
04	Test cyclique
11	Retour secteur
12	Défaut secteur
17	Panne bouton d'appel
18	Retour bouton d'appel
404	Problème d'enregis-trement sur IP-PBX

Le cas du **code d'alerte** « 404 » ne peut être utilisé que si le destinataire Extension B peut être joint par son adresse IP B, *Voir* §2.

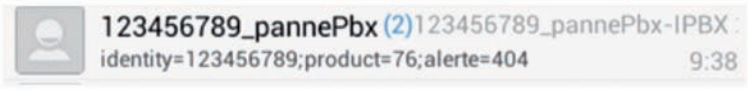
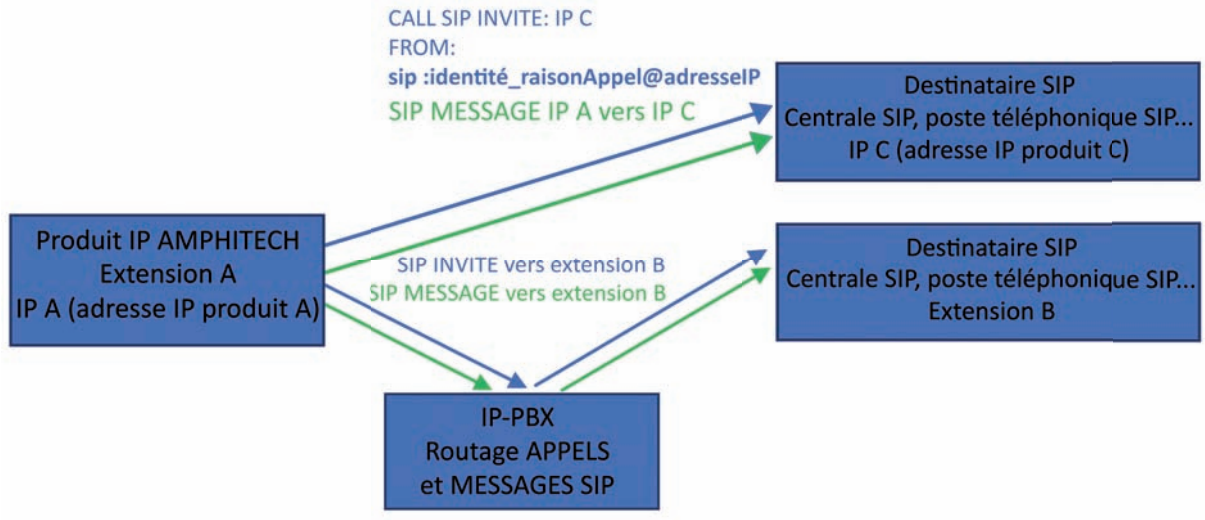


Image 5: messages SIP reçus sur poste SIP Grandstream GXV3240 extension B du problème enregis-trement IP-PBX de l'extension A. Le produit A envoie le message SIP au produit B en utilisant l'adresse IP B.

3.3.22.3.2. ***Message Header appelé en mode P2P***

Si le système IP est enregistré sur un IP-PBX, l'appel de type vocal en mode P2P (appel par adresse IP) d'un contact est toujours possible à partir du moment où l'URI appelé est au format P2P (appel par adresse IP).

L'identification du produit A vers le produit C utilisera la méthode détaillée au §1. Un autre produit C peut recevoir des **messages SIP** du produit A comme détaillé en §2 si l'extension B n'est pas accessible ou si le produit B ne peut pas utiliser la réception d'appels en P2P.



Envoi de messages SIP du produit A vers le produit C pour les raisons d'appels :

- Bouton appel
- Défaut secteur / retour secteur
- *Panne d'enregistrement vers l'IP-PBX de l'extension A*
- Panne bouton d'appel (appui supérieur à 10 min) / fin de panne bouton d'appel
- Appel cyclique de test

Dans la méthode : **SIP INVITE** on retrouvera dans le **Message Header : sip :identité_raisonAppel@adresseIP**

- L'identité : 9 digits (de 0 à 9)
- Raison Appel (défaut usine) :

Valeurs	Raison d'appel	Type d'appel
bouton_appel	Bouton d'appel	Vocal
defautSecteur	Défaut secteur	Technique
retourSecteur	Retour secteur	Technique
retourBoutonALB	Retour bouton d'appel	Technique
panneBoutonALB	Panne bouton d'appel	technique
test	Test cyclique	Test cyclique
pannePbx	*Problème d'enregistrement vers IP-PBX*	*Technique*

- Adresse IP : adresse IP du produit AMPHITECH

Pour les raisons d'appels « bouton d'appel » et « Test cyclique », les **valeurs** sont modifiables via les paramètres de l'application dans :

EVENEMENTS SYSTEM > Gestion appels techniques > Gestion messages techniques P2P > Bouton d'appel

EVENEMENTS SYSTEM > Gestion appels techniques > Gestion messages techniques P2P > Test Cyclique

3.3.22.4. Identification via PROTOCOLE DTMF de l'appelant en mode IP-PBX

3.3.22.4.1. Réception d'appel vocal

Le système SIP Amphitech appelle le centre de télésurveillance, sur décroché de la centrale, celle-ci envoie le code DTMF « C ». Lorsque le produit Amphitech reçoit ce code DTMF « C », le protocole DTMF est envoyé vers la centrale :

Étape	Centre surveillance	Dialogue ⇔	IPAC						
1		⇦	9	ab	cd	ef	ID	C	CS
2	Attente de 3 secondes								
3	Acknowledge «1»	⇨							
4		⇦	Mode Vocal « # »						
5	Mode vocal								
6	Raccrocher	⇨	Fin de communication						
7			Raccroché						

Étape 1

- Code de synchronisation "**9**"
- Code produit [**ab**]

Valeurs [ab]	Produit
81	IP-GAP / IPAC-200

- Type et raison d'appel [**cd**] :

Valeurs [cd]	Raison d'appel	Type d'appel
01	Bouton d'appel	Vocal

- Adresse du module [**ef**] : 01 (IP-GAP)
- Identité [**ID**] : 1 to 9 digits (0 to 9)
- Check sum [**CS**] : 3 digits. Checksum des paramètres 9 à C calculé avec la méthode CRC8

Étape 2

- Attente de 3 secondes : temps nécessaire au produit IP AMPHITECH pour recevoir le code DTMF.

Étape 3

- Acknowledge « **1** » : Le DTMF “1” est envoyé si le CRC calculé par la centrale est égal au CRC reçu, alors le code DTMF “C” est envoyé au produit IP AMPHITECH.

  Le code DTMF “1” est envoyé 5 fois toutes les 5 secondes tant que l’IPAC n’envoie pas le code DTMF “#”.

Étape 4

- Vocal « # » : Le code DTMF « # » est envoyé si le système IP AMPHITECH a bien recu le code DTMF “1”.

Étape 5

- La communication vocale est établie entre le système IP AMPHITECH et le centre de télésurveillance.

Étapes 6 & 7

- Le Centre de télésurveillance met fin à la communication, le système IP Amphitech raccroche.

3.3.22.4.2. Réception d'appel technique

Le système SIP Amphitech appelle le centre de télésurveillance, sur décroché de la centrale, celle-ci envoie le code DTMF « C ». Lorsque le produit AMPHITECH reçoit ce code DTMF « C », le protocole DTMF est envoyé vers la centrale :

Étape	Centre surveillance	Dialogue ⇔	IPAC						
1		⇦	9	ab	cd	ef	ID	C	CS
2	Attente de 3 secondes								
3	Acknowledge «1»	⇨							
4		⇦	Mode Vocal « # »						
5	Mode vocal								
6	Raccrocher	⇨	Fin de communication						
7			Raccroché						

Étape 1

- Code de synchronisation "**9**"
- Code produit [**ab**]

Valeurs [ab]	Produit
81	IP-GAP / IPAC-200

- Type et raison d'appel [**cd**] :

Valeurs [cd]	Raison d'appel	Type d'appel
11	Retour secteur	Technique
12	Défaut secteur	Technique
17	Défaut bouton d'appel	Technique
18	Bouton d'appel valide	Technique

- Adresse du module [**ef**] : 01 (IP-GAP)
- Identité [**ID**] : 1 to 9 digits (0 to 9)
- Check sum [**CS**] : 3 digits. Checksum des paramètres 9 à C calculé avec la méthode CRC8

Étape 2

- Attente de 3 secondes : temps nécessaire au produit IP AMPHITECH pour recevoir le code DTMF.

Étape 3

- Acknowledge « **1** » : Le DTMF “1” est envoyé si le CRC calculé par la centrale est égal au CRC reçu, alors le code DTMF “C” est envoyé au produit IP AMPHITECH.

  Le code DTMF “1” est envoyé 5 fois toutes les 5 secondes tant que l’IPAC n’envoie pas le code DTMF “#”.

Étape 4

- Vocal « # » : Le code DTMF « # » est envoyé si le système IP AMPHITECH a bien recu le code DTMF “1”.

Étape 5

- La communication vocale est établie entre le système IP AMPHITECH et le centre de télésurveillance.

Étape 6 & 7

- Le Centre de télésurveillance met fin à la communication, le système IP Amphitech raccroche.

3.3.22.4.3. Réception d'appel cyclique

Le système SIP Amphitech appelle le centre de télésurveillance, sur décroché de la centrale, celle-ci envoie le code DTMF « C ». Lorsque le produit Amphitech reçoit ce code DTMF « C », le protocole DTMF est envoyé vers la centrale :

Étape	Centre surveillance	Dialogue ⇔	IPAC						
1		⇦	9	ab	cd	ef	ID	C	CS
2	Attente de 3 secondes								
3	Acknowledge «1»	⇨							
4		⇦	Mode Vocal « # »						
5	Mode vocal								
6	Raccrocher	⇨	Fin de communication						
7			Raccroché						

Étape 1

- Code de synchronisation "**9**"
- Code produit [**ab**]

Valeurs [ab]	Produit
81	IP-GAP / IPAC-200

- Type et raison d'appel [**cd**] :

Valeurs [cd]	Raison d'appel	Type d'appel
04	Test cyclique	Test

- Adresse du module [**ef**] : 01 (IP-GAP)
- Identité [**ID**] : 1 to 9 digits (0 to 9)
- Check sum [**CS**] : 3 digits. Checksum des paramètres 9 à C calculé avec la méthode CRC8

Étape 2

- Attente de 3 secondes : temps nécessaire au produit IP AMPHITECH pour recevoir le code DTMF.

Étape 3

- Acknowledge « **1** » : Le DTMF “1” est envoyé si le CRC calculé par la centrale est égal au CRC reçu, alors le code DTMF “C” est envoyé au produit IP AMPHITECH.

  Le code DTMF “1” est envoyé 5 fois toutes les 5 secondes tant que l’IPAC n’envoie pas le code DTMF “#”.

Étape 4

- Vocal « # » : Le code DTMF « # » est envoyé si le système IP AMPHITECH a bien recu le code DTMF “1”.

Étape 5

- La communication vocale est établie entre le système IP AMPHITECH et le centre de télésurveillance.

Étape 6 & 7

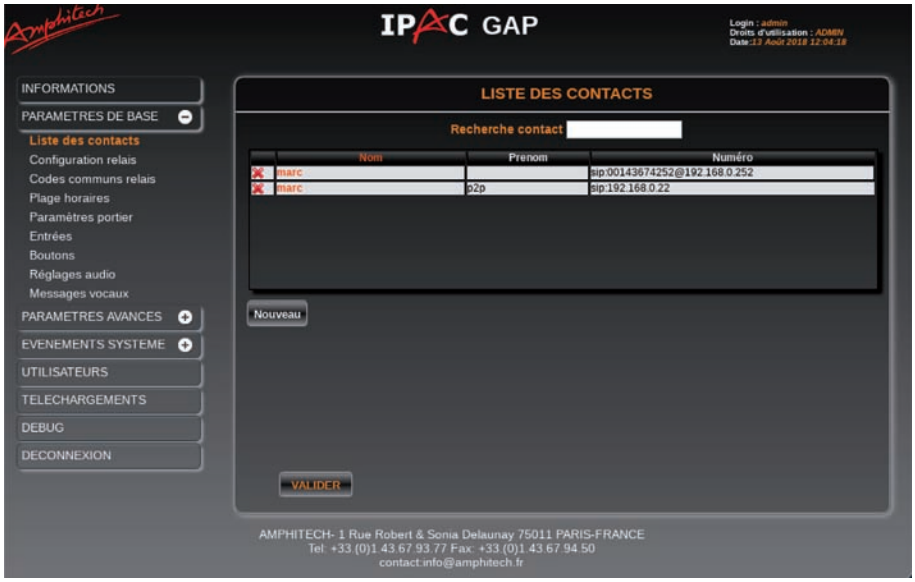
- Le Centre de télésurveillance met fin à la communication, le système IP Amphitech raccroche.

3.3.22.5. Gestion Télésurveillance IP-GAP

3.3.22.5.1. Gestion appel vocal

Création des contacts à appeler au format P2P (adresse IP) ou au format extension IP-PBX. Ces contacts pourront être utlisés pour :

- l'appel vocal (bouton d'appel)
- l'appel technique
- l'appel test cyclique



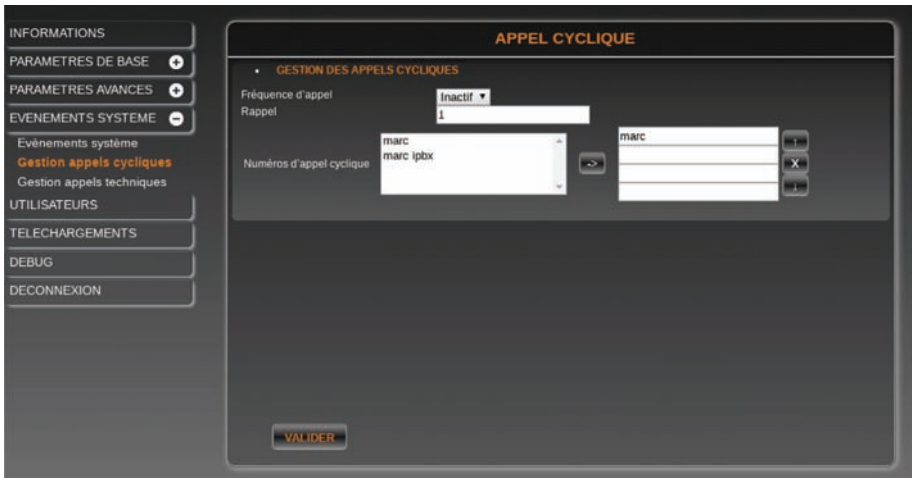
- Ajout des contacts type **vocal** sur le bouton d'appel, appel cyclique de 4 contacts possible en cas de non réponse.

3.3.22.5.2. Gestion appel test cyclique

- Ajout des contacts type **test cyclique**, appel cyclique de 4 contacts possible en cas de non réponse.
- Choix de la fréquence d'appel, tous les x jours (x de 1 à 7). Inactif = pas d'appel cyclique.

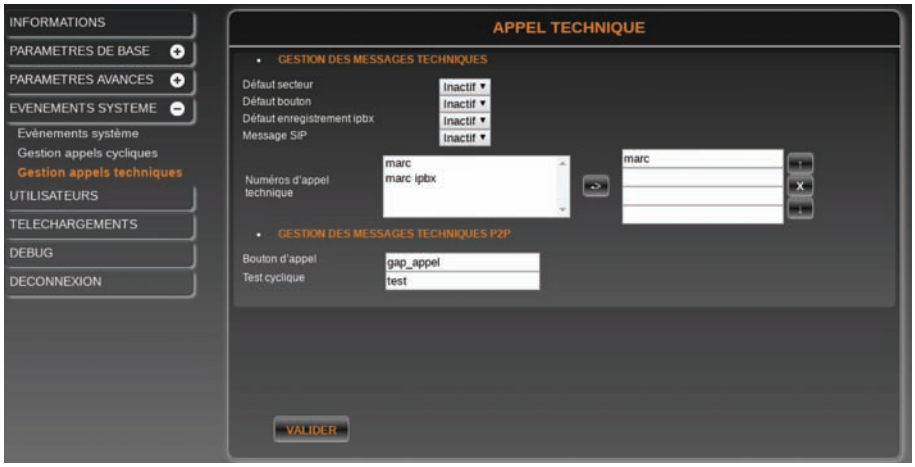
- *Rappel* : s'il n'y a pas de réponse lors du premier test, l'appel est déclenché une seconde fois *x* heures après. *x = de 1 à 24 heures*

  Si l'appel échoue la seconde fois, le prochain test sera effectué selon la fréquence d'appel choisie.



3.3.22.5.3. Gestion appels techniques

- Activation ou non des rapports (messages SIP / Message Header from) :
  - Défaut secteur / retour secteur
  - Problème bouton d'appel, bouton enfoncé (supérieur à 10 minutes) / retour bouton d'appel
  - Défaut d'enregistrement vers IP-PBX. Extension SIP appelée injoignable.
- Validation ou non de l'envoi du rapport par message SIP.
- L'appel technique peut utiliser jusqu'à 4 contacts pour utiliser le mode cyclique.

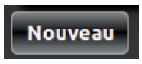


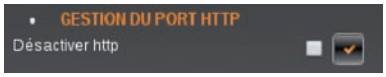
Pour l'identification en mode P2P des raisons d'appel « bouton d'appel » et « Test cyclique », les **valeurs** sont modifiables par les paramètres de l'application dans :

EVENEMENTS SYSTEM > Gestion appels techniques > Gestion messages techniques P2P > Bouton d'appel

EVENEMENTS SYSTEM > Gestion appels techniques > Gestion messages techniques P2P > Test Cyclique

3.3.23. Gestion des utilisateurs locaux

- Cliquer sur 

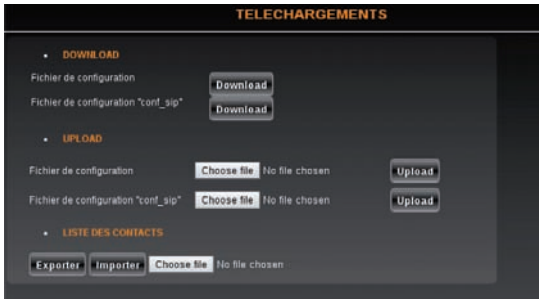
pour ajouter un nouvel utilisateur.
- Cocher la case 

pour activer la connexion automatique via HTTPS.
- Saisir le **Login**, le **Mot de passe** , définir les **Droits d'utilisation**, Administrateur ou Utilisateur et valider  :

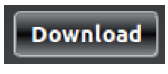
En mode utilisateur, on ne visualise que les pages web :

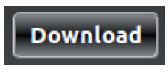
- INFORMATIONS
- PARAMETRES DE BASE
- EVENEMENTS SYSTEME (visualisation de l'écran)

3.3.24. Téléchargements



DOWNLOAD

- Fichier de configuration **"conf_user"** : Cliquer sur 

pour sauvegarder le fichier de configuration d'un portier sur votre PC.
- Fichier de configuration **"conf_sip"** : Cliquer sur 

pour sauvegarder le fichier de configuration du serveur SIP sur votre PC.

UPLOAD

- Fichier de configuration **"conf_user"** : cliquer sur 

pour sélectionner le fichier de configuration d'un portier sauvegardé sur votre PC.
- Puis sur 

pour sauvegarder le fichier de configuration sur le portier de votre choix

(même référence de portier).

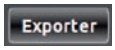
- Fichier de configuration **"conf_sip"** : cliquer sur 

pour sélectionner le fichier de configuration du serveur SIP sauvegardé sur votre PC.
- Puis sur 

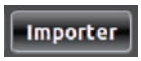
pour sauvegarder le fichier de configuration sur le portier de votre choix (même référence de portier).

LISTE DES CONTACTS

- Cliquer sur 

pour sélectionner la liste des contacts d'un portier sauvegardée sur votre PC (format CSV).
- Cliquer sur 

pour exporter une liste de contacts.
- Cliquer sur 

puis sur 

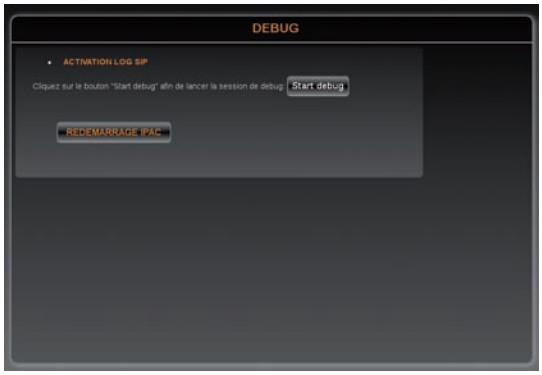
pour importer une liste des contacts.

Pour confirmer les changements de la page, cliquer sur 

.

3.3.25. Debug

En cas de dysfonctionnement, AMPHITECH peut vous demander de lancer un debug pour récupérer les informations du portier :



- Start debug pour commencer le debug.
- Réaliser la manipulation qui entraîne le dysfonctionnement.
- Appuyer sur Stop debug pour terminer l'analyse.
- Cliquer sur REDEMARRAGE IPAC pour redémarrer le portier.