Notice d'exploitation IPAC 500

Portier IP AMPHITECH

N°671 – Octobre 2021

Amphitech
1, rue Robert et Sonia Delaunay
75011 Paris
Tél. SAV : +33 (0)1.43.67.96.74
www.amphitech.fr

Conforme
ROHS

15/NOTIC-000671M

Version logiciel

Version logiciel V 2.27-0.3i

Sommaire

Version logiciel **2**
Recommandations **5**
1. Portier IPAC 500 ..... **6**
1.1. DESCRIPTION **6**
1.1.1. PRÉSENTATION GÉNÉRALE **6**
1.1.2. CARACTÉRISTIQUES **9**
1.1.3. INSTALLATION ET RACCORDEMENT **12**
1.2. FONCTIONNEMENT **14**
1.2.1. PORTIER À DÉFILEMENT IPAC 500 ..... **14**
1.2.2. PORTIER BOUTONS IPAC 501/502/503 ..... **16**
1.2.3. ÉCRANS, PICTOGRAMMES ET MESSAGES VOCAUX **18**
1.3. CONFIGURATION - PAGES WEB **20**
1.3.1. CONNEXION AU RÉSEAU LOCAL **20**
1.3.2. CONFIGURATION SIMPLIFIÉE (WIZARD) **21**
2. Portiers VoIP - *Exemple*, IPAC 500 ..... **26**
2.1. CONFIGURATION AVANCÉE (ADMINISTRATEUR) **26**
2.1.1. INFORMATIONS GÉNÉRALES SUR LE PRODUIT **26**
2.1.2. LISTE DES CONTACTS IPAC 500 DÉFILEMENT **29**
2.1.3. LISTE DES CONTACTS IPAC 500 BOUTONS **31**
2.1.4. RELAIS DE TÉLÉCOMMANDE **32**
2.1.5. CODE COMMUNS RELAIS **33**
2.1.6. PLAGES HORAIRES **34**
2.1.7. PARAMÈTRES PORTIER **34**
2.1.8. CONFIGURATION DES ENTRÉES **36**
2.1.9. CONFIGURATION DES BOUTONS D'APPELS IPAC 500 BOUTONS **37**
2.1.10. RÉGLAGES AUDIO **37**
2.1.11. MESSAGES VOCAUX **38**
2.1.12. PARAMÈTRES RÉSEAU **38**
2.1.13. PARAMÈTRES SIP **40**
2.1.14. CODECS AUDIO **41**
2.1.15. PARAMÈTRES VIDÉO **42**
2.1.16. DATE ET HEURE **49**
2.1.17. COMPTE MAIL **51**
2.1.18. API **51**
2.1.19. LDAP **58**
2.1.20. RADIUS 802.1X **60**
2.1.21. ACCÈS WEB PAR AUTHENTIFICATION SERVEUR RADIUS **63**

2.1.22. GÉNÉRATION DE CERTIFICATS 65
2.1.23. LOGO D'ACCUEIL 66
2.1.24. MISE À JOUR FIRMWARE 66
2.1.25. EVÉNEMENTS SYSTÈME 67
2.1.26. GESTION DES UTILISATEURS LOCAUX 70
2.1.27. CONNEXION AU SERVEUR ASM 71
2.1.28. TÉLÉCHARGEMENTS 75
2.1.29. DEBUG 77

Recommandations

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

1. Portier IPAC 500

1.1. Description

1.1.1. Présentation générale

Le portier IPAC 500 a pour fonction le contrôle d'accès aux bâtiments. Il répond aux exigences de la réglementation sur l'accessibilité des personnes handicapées aux bâtiments collectifs ou aux bâtiments recevant du public (ERP).

L'IPAC 500 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 24-30 V **ou** peut être alimenté en PoE+ *(Power over Ethernet, 802.3at)* fourni par un switch via le câble réseau. *Préconisation câblage Cat6/Cat7 avec blindage, voir http://wiki.amphitech.fr/rj45*

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).

Figure 1.1. Détail façade

Version saillie	Version encastrée
	

Exemples

VERSION SAILLIE					
					
IPAC 500 21S	**IPAC 501 21S**	**IPAC 502 21S**	**IPAC 502 31S**	**IPAC 503 21S**	**IPAC 503 31S**

VERSION ENCASTREE					
					
IPAC 500 21E	**IPAC 501 21E**	**IPAC 502 21E**	**IPAC 502 31E**	**IPAC 503 21E**	**IPAC 503 31E**

Caractéristiques électriques

	Min	Nom	Max	Longueur (Max)	Description
Alimentation PoE+ (IEEE 802.3at)*	24 W		30W		
Alimentation secteur		24 VDC	30 VDC	< 5 m	Défaut secteur des alimentations Amphitech
	0 VDC		14 VDC		
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

** L'alimentation PoE+ (IEEE 802.3at) nécessite un port configuré en Classe 4 Type 2 sur le PSE (routeur PoE+). Catégories de câblage : http://wiki.amphitech.fr/rj45*

1.1.2. Caractéristiques

- Afficheur couleur haute résolution, haute luminosité, hauteur 67 mm, largeur 51 mm :
  - choix du contact,
  - pictogrammes,
  - messages d'informations,
  - logo ou image sur afficheur LCD.
- Clavier 12 touches alphanumériques rétro éclairées avec touche de repérage pour malvoyants :

  (selon le type d'IPAC 500)
  - composition du code d'accès,
  - numérotation abrégée,
  - numérotation libre (IPAC 50x avec clavier),
  - recherche alphanumérique,
  - surnumérotation DTMF pendant une communication (IPAC 50x avec clavier).
- Boutons rétro éclairés :
  - appel vers un numéro préenregistré **(selon le type d'IPAC 500)**,
  - déclenchement d'appel,
  - ouverture de la porte.
- Audio, haut parleur et micro :
  - communication mains libres full duplex,
  - diffusion de messages.

- Vidéo **(selon le type d'IPAC 500)** :
  - caméra couleur, ouverture 114°,
  - codecs SIP VIDÉO : H264, H263, H263p, VP8
  - résolution vidéo :

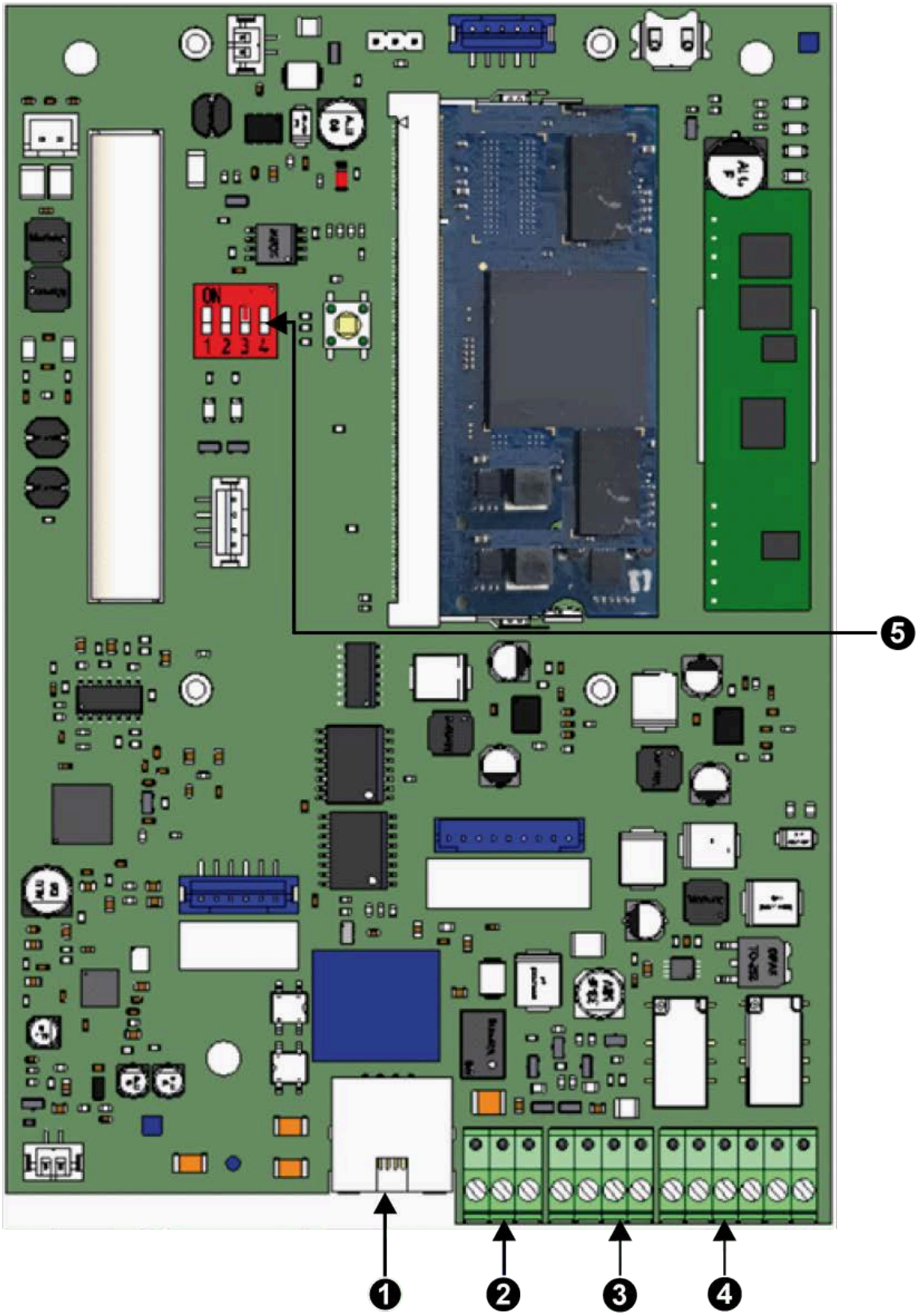
    - *Vidéo SIP* : encodage H264 en résolution 320p x 240p

    - *Serveur MjpegStreamer* : encodage MJPEG en résolution 320p x 240p

    - *Serveur RTSP* : encodage H264 ou MJPEG avec des résolutions de : 1280p x 720p / 640p x 480p / 320p x 240p
  - Certifié protocole ONVIF profil S (https://www.onvif.org/about/member-list/) - *Uniquement pour les portiers VIDÉO.*.
- Emplacement normalisé VIGIK®
- Boîtier en ZAMAK
- Façade inox 2.5 mm :
  - version saillie, dimensions 300 x 120 x 30 mm,
  - version encastrée, dimensions 350 x 154.5 x 30 mm,
  - anti-vandalisme IK 08 ; étanchéité IP 55.
- Connexions : bouton de sortie, VIGIK®, relais de gâche, information Prise De Ligne, autoprotection.
- Serveur web embarqué, sécurisé par mot de passe et protocole 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 à 30 VDC.
- Réseau : DHCP ou statique.
- Protocole VoIP : SIP V2 (RFC 3261).
- DTMF : RFC 2833, SIP Info (RFC 2976).
- RADIUS 802.1x
- Gestion de l'interface réseau VLAN
- 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,
- Gestion des évènements : rapports de fonctionnement par e-mail, fichiers, Syslog.
- De 1 à 3 boutons d'appels (IPAC501/502/503) ou bouton porte (appel cyclique en cas d'occupation ou de non réponse).
- Décroché automatique sur appel entrant.
- Choix des messages vocaux à diffuser (appel en cours, communication établie, ouverture de la porte, appel en échec, etc...).
- Choix des langues (messages audio / affichage) : Français, Anglais, Allemand, Espagnol, Portugais.
- 2 sorties relais pour la commande d'ouverture de porte ou l'information prise de ligne.

- 2 entrées contact ou tension (activation relais et discrimination d'appel).
- Gestion des plages horaires (appel contacts, bouton d’appel, relais, entrées, codes d’accès…).
- Gestion des paramètres d’appels, temps de communication, temps d’appui bouton, délais appel sortant, volume audio…
- Mise à jour des contacts par serveur LDAP
- API de gestion du produit
- Supervision via le service gratuit ASM ACCESS AMPHITECH, **connexion Internet sur le même réseau que l'IPAC 500 impérative.**

1.1.3. Installation et raccordement



❶	**Connecteur RJ45** Réseau /PoE+
❷	**Connecteur alimentation** **1** 24 V - 30 V DC **2** 0 VDC **3** Défaut 220V Uniquement avec alimentations Amphitech
❸	**Connecteur Entrée 1 et Entrée 2** **1** Entrée 1 (+) Entrée en tension de 10 à 30VDC max ou contact libre de tout potentiel pour activer l'ouverture de la porte. **2** Entrée 1 (-) **3** Entrée 2 (+) **4** Entrée 2 (-) Entrée en tension de 10 à 30VDC max ou contact libre de tout potentiel pour activer l'ouverture de la porte.
❹	**Connecteur Relais 1 et Relais 2** **1** Travail RL1 **Protections recommandées** **2** Commun RL1 **3** Repos RL1 **4** Travail RL2 **Protections recommandées** **5** Commun RL2 **6** Repos RL2
❺	**Dipswitchs - En mode normal de fonctionnement, tous les dipswitchs 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. – **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)*

Privilégier l'installation du portier dans une zone ombragée, éviter de placer le portier face au soleil pour garder une température de fonctionnement correcte (max 80°).

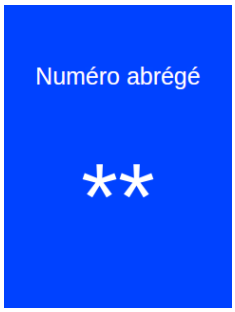
Éviter de positionner le portier sur une matière réfléchissante ou absorbant la chaleur (plaque d'acier, potelet acier, avec peinture de couleur RAL noir…).

1.2. Fonctionnement

1.2.1. Portier à défilement IPAC 500

- L'IPAC 500 dispose d'un clavier et de trois boutons utilisés pour :
  - Commander les **relais de gâche** par la saisie d'un code (1 à 4 chiffres) suivi de #.

  - Joindre un résident par la saisie * suivi du numéro abrégé attribué à chaque bouton (Exemple : *001 ou *002 ou *003) **si le clavier est configuré en mode appel abrégé**. Ces numéros "index" sont définis lors de la création du contact.



  - Appeler un contact par **numérotation libre** :

    - Soit par le numéro IPBX soit par la saisie de l'adresse IP du contact.

    - Touche # = "."

    - Touche * = correction

    - Touche Appel / Porte-étiquettes = appel

    Par défaut, les produits sont toujours configurés en "code d'accès" et "numérotation abrégée".

  - En mode **sans écran d'accueil**, le clavier peut être utilisé pour : saisir un code d'accès ou pour rechercher un contact (selon le paramétrage du portier),

- saisir un "code gâche" et pour la "numérotation abrégée",

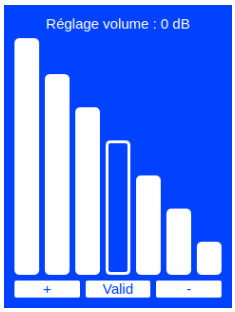
- saisir un "code gâche" et pour la "numérotation libre",

- la recherche alphabétique d'un contact et la "numérotation abrégée",

- la recherche alphabétique d'un contact et la "numérotation libre",

L'appel est lancé par appui sur le bouton "appel" ou "porte-étiquettes".

– En cours de communication, ajuster le volume d'écoute avec les boutons  et  .



– L'accès à la **liste des contacts** se fait par appui sur les deux boutons   . Il est possible d'utiliser le clavier pour la recherche alphanumérique d'un contact.

Un appui prolongé sur l'une des flèches permet d'obtenir un défilement plus rapide de la liste des contacts (disponible à partir de 15 contacts).

– Les appels pourront être lancés depuis le bouton  , après avoir sélectionné le contact.

- **Plages horaires**

  – Une plage horaire peut être attribuée à chaque contact. Cette plage horaire est propre à chaque contact.

- **Relais et entrées**

Les deux **relais** sont à configurer en télécommande ou **I**nformation **P**rise de **L**igne (les relais peuvent être mis en mode NetCut *voir* produit Netcut Amphitech). Les paramètres des deux relais sont :

– Information PDL / Gâche / NetCut,

– Temps de maintien.

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, de la sonnerie à la fin de la tempo ou au raccroché.

Important

Si le relais est configuré en Information PDL ou NetCut, la fonction commande de gâche par code d'accès n'est plus disponible.

Il est possible d'appliquer une tension ou un contact sec sur les deux **entrées**. Les paramètres des deux entrées sont :

– Valide / Invalide,

– NO / NF,

– Temps de maintien : 500 ms à 5,5 sec. par pas de 1 sec.,

– Association à une plage horaire,

– Relais 1 ou Relais 2 ou Relais 1 + Relais 2

	Configuration Relais 1	Configuration Relais 2	Entrée 1 / Entrée 2	Entrée 3
 **IPAC 500 DEFILEMENT**	Gâche	Gâche	Relais 1 / Relais 2	Relais 1
	Information PDL / Net-Cut	Gâche	Relais 2	Inactif
	Gâche	Information PDL / Net-Cut	Relais 1	Relais 1
	Information PDL / Net-Cut	Information PDL / Net-Cut	Inactif	Inactif

1.2.2. Portier boutons IPAC 501/502/503

Selon les modèles, l'IPAC 50x est équipé de :

- Un à trois boutons d'appel vers des numéros préenregistrés,

Une fois créés, les contacts sont à attribuer aux boutons d'appel. L'ordre d'enchaînement automatique des numéros peut être modifié. Les plages horaires sont attribuées aux boutons d'appel.

- Un bouton de commande d'ouverture de la porte, associé au relais 1, automatiquement configuré en mode gâche. *L'utilisation du Relais 1 en modes NetCut et Information Prise de Ligne est impossible dans le cas d'un IPAC50x en mode "ouverture porte".*

***Exemple* : Écran IPAC 503**

- Appuyer sur le bouton  pour appeler l'Accueil

- Le pictogramme "sens interdit" signifie que l'appel vers le Magasin est interdit au moment où le visiteur se présente (en dehors des plages horaires associées à l'appel vers le Magasin)
- Appuyer sur le bouton  pour commander l'ouverture de la porte.
- **Relais et entrées**

  Les deux **relais** sont à configurer en télécommande ou **I**nformation **P**rise de **L**igne ou en mode NetCut. Les paramètres des deux relais sont :

  – Information PDL / Gâche,

  – Temps de maintien,

  – Mode NetCut.

  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 moment où le portier sonne jusqu'à la fin de la tempo ou au raccroché.

> **Important**
>
> Si le relais est configuré en Information PDL ou NetCut, la fonction commande de gâche par code d'accès n'est plus disponible.

Il est possible d'appliquer une tension ou un contact sec sur les deux **entrées**. Les paramètres des deux entrées sont :

– Valide / Invalide,

– NO / NF,

– Temps de maintien : 500 ms à 5,5 sec. par pas de 1 sec.,

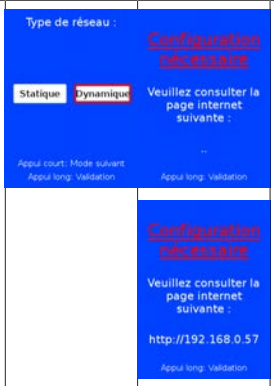
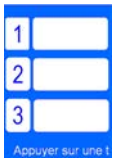
– Association à une plage horaire,

– Relais 1 ou Relais 2 ou Relais 1 + Relais 2

	Configuration Relais 1	**Configuration Relais 2**	**Entrée 1 / Entrée 2**	**Entrée 3**
 **IPAC 500 BOUTONS**	Gâche	Gâche	Relais 1 / Relais 2	Relais 1/ Appel Bouton 1
	Information PDL / Net-Cut *(PDL et NetCut : IPAC mode porte impossible)*	Gâche	Relais 2	Appel Bouton 1
	Gâche	Information PDL / Net-Cut	Relais 1	Relais 1/ Appel Bouton 1
	Information PDL / Net-Cut *PDL et NetCut IPAC : mode porte impossible)*	Information PDL / Net-Cut	Inactif	Appel Bouton 1

1.2.3. Écrans, pictogrammes et messages vocaux

- **Écrans**

	Écran	Description	Action / Utilisation	Détail / Valeur usine
1		Initialisation produit		
2		Type de fichier : Usine / OK Mode : P2P / IPBX Hardware : Désignation du portier Version : firmware IP : adresse IP actuelle		Écran qui s'affiche avant l'écran d'accueil **à chaque redémarrage** Mode de connexion par défaut : P2P
3		Choix de la langue de configuration et d'exploitation du produit, à la première mise en service ou après un retour à la configuration usine		
4		*Statique : adresse IP par défaut*192.168.0.2 *Dynamique : adresse IP fournie par le serveur DHCP*		
5		Adresse IP du produit par défaut, à la première mise en service ou après un retour à la configuration usine	Appuyer sur un des boutons du portier pour valider	Adresse IP : 192.168.0.2
6		Récaptitulatif de la configuration du réseau, à la première mise en service ou après un retour à la configuration usine		Adresse IP : 192.168.0.2 Masque : 255.255.255.0 Broadcast : 192.168.0.255 Passerelle : 192.168.0.1
7	 	Écran au repos pour l'IPAC 500 Défilement et pour l'IPAC 500 Boutons (libellés vides avant la création des contacts)		Mode de fonctionnement P2P (Peer to Peer), appel par adresse IP

- Pictogrammes et messages vocaux

  Des pictogrammes associés aux messages vocaux diffusés par le portier sont affichés sur l'écran selon l'état du portier :

  – "Appel en cours" (appel en cours ou appel sortant)

  – "Communication en cours"

  – "Ouverture de la porte" :

  - localement, par saisie du code sur le clavier,

  - par l'entrée 1 ou 2 sur contact ou tension

  - à distance, par saisie d'un code DTMF en cours de communication.

  – "Appel en échec" (contact inexistant, occupé ou en mode "Ne pas déranger, DND")

  – "Appel suivant en cours" (appel cyclique, enchaînement automatique sur le numéro suivant)

  – "Appel non autorisé" (appel en dehors de la plage horaire définie)

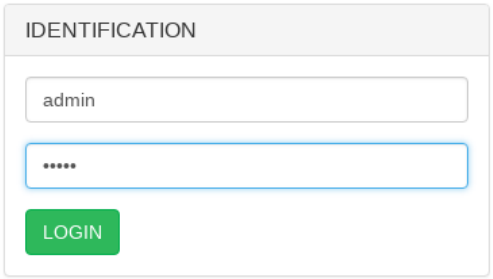
1.3. Configuration - Pages WEB

1.3.1. Connexion au réseau local

- Vérifier les raccordements et connecter l'alimentation si le serveur réseau ne fournit pas une alimentation PoE+ (*Power over Ethernet, 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. ou l'adresse DHCP trouvée et affichée par le portier lors de sa mise en route.

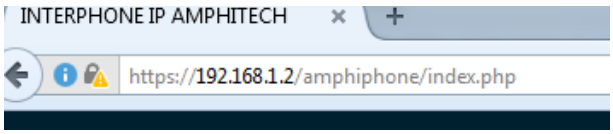
L'accès aux paramètres est réalisé via un HTACCES :

Login	admin
Password	admin

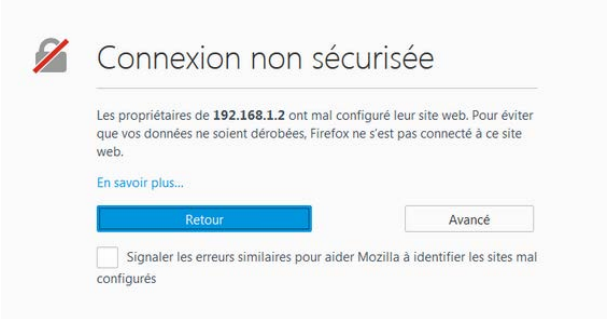


L'accès aux paramètres est également possible par HTTPS.

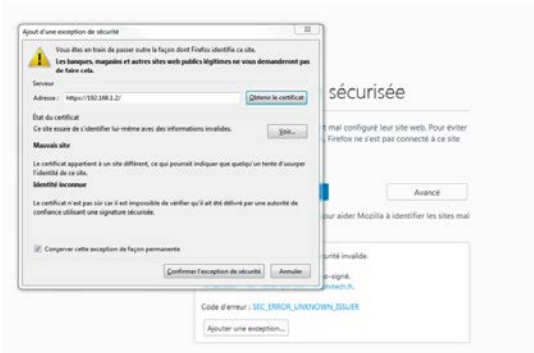
– Cliquer sur le cadenas vert pour être redirigé vers une page HTTPS.



– Selon le navigateur, accepter les règles de sécurité de certificat non connu.



– Ajouter des règles de connexion d'exception :



– Une fois connecté en HTTPS, le navigateur indique :

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

1.3.2. Configuration simplifiée (Wizard)

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

- 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 :

Choisir le mode Peer to Peer (appel point à point) ou IPBX.

1.3.2.1. 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.

ou

❶ Recherche des contacts, scan du réseau à la recherche de périphériques SIP, téléphone, tablette avec logiciel de téléphonie SIP, etc.

Attention

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

❷ Liste des périphériques réseaux trouvés.

❸ Ajout d'un périphérique SIP dans la liste des contacts avec possibilité de modifier les champs Nom, Prénom :

❹ Aperçu de la liste des contacts. Les flèches  permettent de modifier l'ordre des contacts sur l'affichage de l'écran du portier version défilement. Le bouton  permet de supprimer un contact de la liste.

❺ 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 IP 192.168.0.47 ou sous la forme sip : 192.168.0.47

Cliquer sur le bouton 

pour passer à l'étape suivante.

1.3.2.2. Mode IPBX

Le mode IPBX permet de raccorder l'IPAC 500 sur un réseau IP local équipé d'un serveur SIP :

ou

❶ Serveur SIP : saisir l'adresse IP de l'IPBX

❷ Nom d'utilisateur : nom nécessaire à l'enregistrement auprès de l'IPBX (numéro extension SIP)

❸ Identifiant utilisateur : habituellement identique au nom d'utilisateur

❹ Mot de passe : mot de passe *utilisé lors de l'enregistrement auprès de l'IPBX.*

❺ Ajout d'un contact dans la liste, 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* : Libellé affiché sur l'écran. La taille de la police est adaptée à la longueur du texte (capacité : 2 lignes de 20 caractères).

> **Note**
>
> Veiller à respecter le nombre de caractères pour rester conforme à la réglementation sur l'accessibilité des personnes handicapées aux bâtiments collectifs ou aux bâtiments recevant du public (ERP).

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

1.3.2.3. Codes communs relais de gâche

La dernière étape permet d'ajouter un code de gâche pour les relais 1 et 2 :

- *Cliquer sur le bouton* Next *pour passer à l'étape suivante* :
- *Cliquer sur le bouton* APPLIQUER *pour redémarrer et sauvegarder les modifications.*

2. Portiers VoIP - *Exemple*, IPAC 500

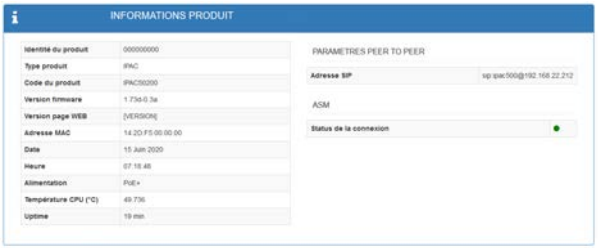
2.1. Configuration avancée (administrateur)

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

Cliquer sur l'icône pour accéder à la configuration avancée :

2.1.1. Informations générales sur le produit

Cliquer sur le bouton  pour accéder aux informations du produit.



Le bouton  permet de revenir à l'écran précédent.

- **Informations produit** :
  - *Identité du produit* : numéro attribué au portier par l'administrateur
  - *Type produit* : IPAC
  - *Code du produit* : IPAC500_xx (dénomination commerciale)
  - *Version firmware* : version logicielle du portier
  - *Version page WEB*
  - *Adresse MAC* : lecture de l'adresse MAC
  - *Date* : date du système
  - *Heure*: heure du système
  - *Alimentation* : alimentation externe ou PoE+
  - *Température CPU* : en °C
  - *Uptime* : temps de fonctionnement depuis la mise en marche du produit
  - *Mémoire disponible*: mémoire du système
  - *Mémoire RAM*
- **Paramètres IPBX**
  - *Compte SIP* : adresse SIP du portier
  - *Status* : indication enregistrement sur IPBX.
- **Paramètres Peer to Peer** (appel en mode réseau "poste à poste")
  - *Adresse SIP* : par défaut en Peer to Peer *sip : ipac500@192.168.0.2.*

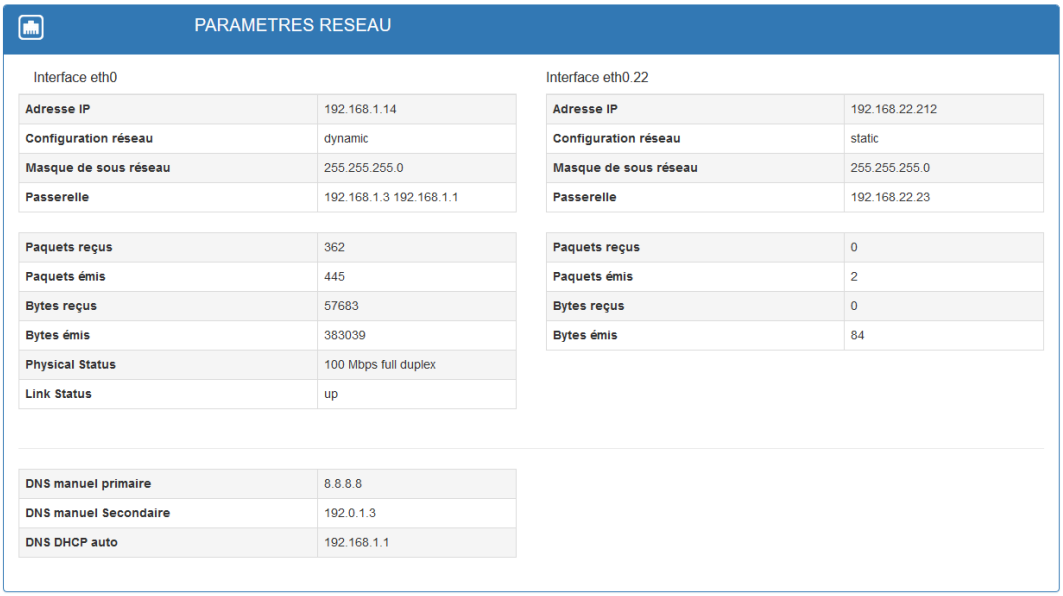
  En mode P2P, il est possible de changer le nom du contact dans les paramètres SIP.

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

  Si l'adresse n'est plus l'adresse par défaut, *sip : ipac500@adresse produit.*

  Cliquer sur le bouton 

- **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* :

  - *Manuelle* : adresse IP de la passerelle renseignée manuellement.
  - *DHCP Auto* : adresse IP de la passerelle retournée automatiquement par le réseau.

– *Paquets et Bytes émis / reçus* : flux réseau vers le portier

– *Physical Status - Statut physique* : vitesse et type de connexion réseau

– *Link Status - Statut de la connexion réseau* : UP ou Down

– *Information réseau VLAN* :

  - Id VLAN : numéro Taggue VLAN
  - Configuration VLAN : Statique ou Dynamique
  - Adresse IP VLAN
  - Masque de sous réseau Interface VLAN
  - Passerelle VLAN
  - Paquets et Bytes émis/reçus sur interface VLAN

– *DNS manuel primaire*: adresse IP de la Gateway (passerelle)

– *DNS manuel secondaire*: adresse IP du DNS secondaire

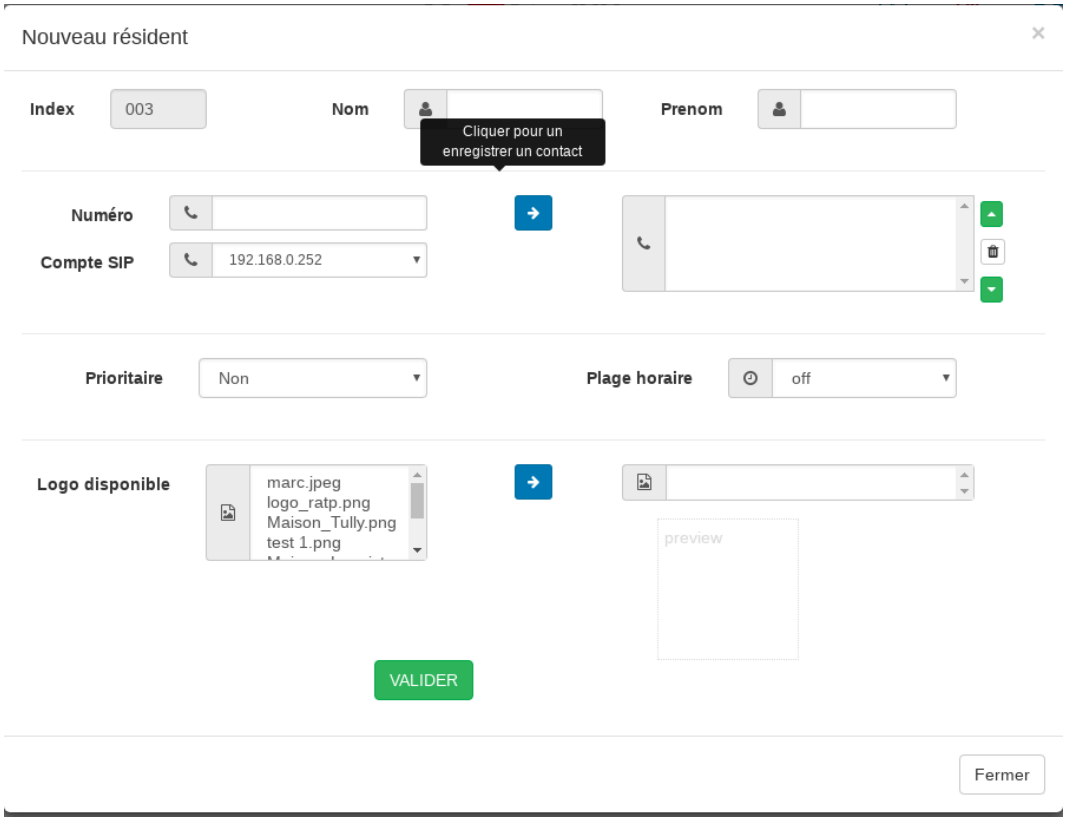
– *DNS DHCP auto*: adresse DNS retournée automatiquement par la passerelle réseau

- Lien de téléchargement de l'application AMPHITECH SIP Stream

Voir : http://wiki.amphitech.fr/notice-asipstream

2.1.2. Liste des contacts IPAC 500 Défilement

Cliquer sur  pour créer un résident. Une fenêtre s'affiche :



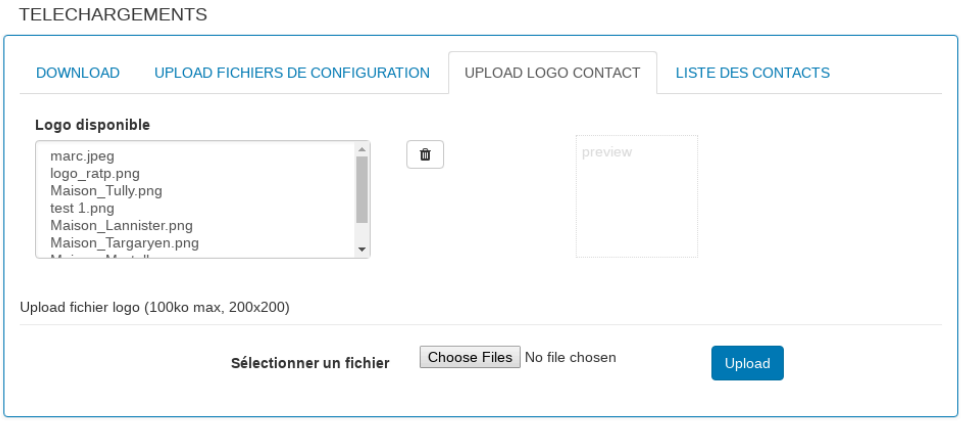
- Ajouter un « *Nom* » et un « *Prénom* ».
- Dans le champ « *Numéro* » entrer un numéro au format P2P (adresse IP) ou au format plan de numérotation IP-PBX.
- Dans le champ « *Compte SIP* » choisir l'option *Contact P2P* ou *IPBX* en sélectionnant un compte SIP valide (**déjà renseigné dans le menu SIP**). Cliquer sur  .

  Le numéro est alors ajouté dans la liste des **numéros cycliques**. Il est possible de créer jusqu'à 4 numéros cycliques par résident (renouveler l'étape précédente) :

L'ordre d'appel peut être modifié : sélectionner un numéro dans la liste puis utiliser les boutons  et  pour modifier l'ordre d'appel des numéros associés au résident.

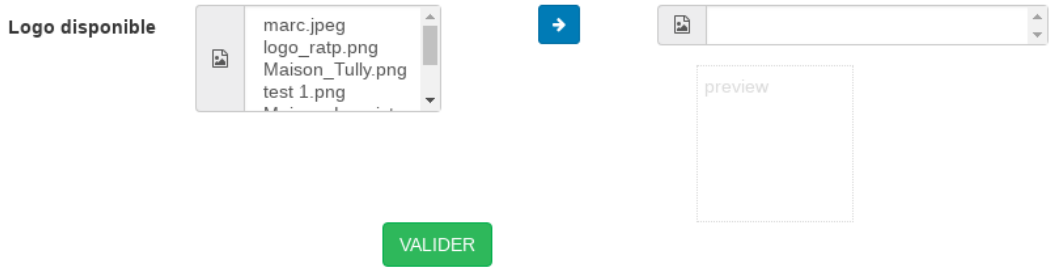
Le bouton  permet de supprimer un numéro sélectionné dans la liste.

- Si des **images** ou des **logos** ont été importés dans la mémoire de l'IPAC à partir du menu **TELECHARGEMENTS / UPLOAD LOGO CONTACT** , il est possible d'associer une image ou un logo à un résident lors de la création du contact :



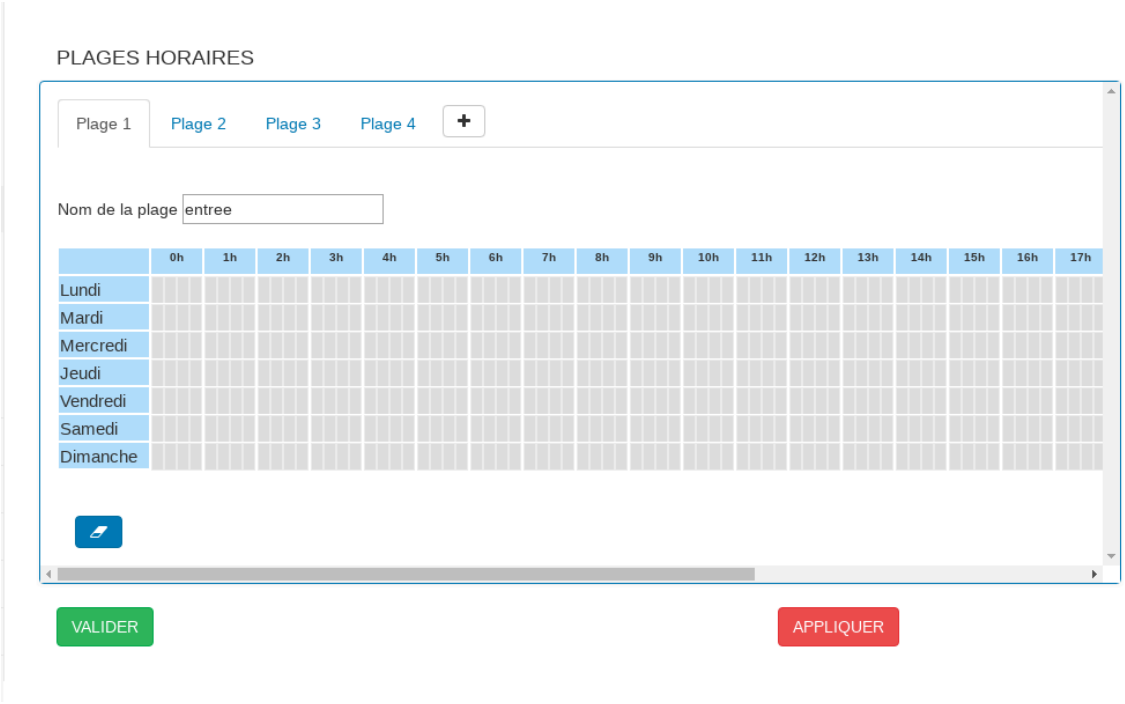
Le logo s'affichera pendant le défilement quand ce résident sera affiché dans la liste des résidents de la page d'accueil. *(Voir PARAMETRES DE BASE/Paramètres portier/ECRAN D'ACCUEIL/Timer recherche résidents)*

Ajout d'une photo à un résident :



- Une **plage horaire** peut être associée au *résident* **Plage horaire** off .

  Cette plage horaire est à créer à partir du menu **PARAMETRES DE BASE/Plages horaires**:

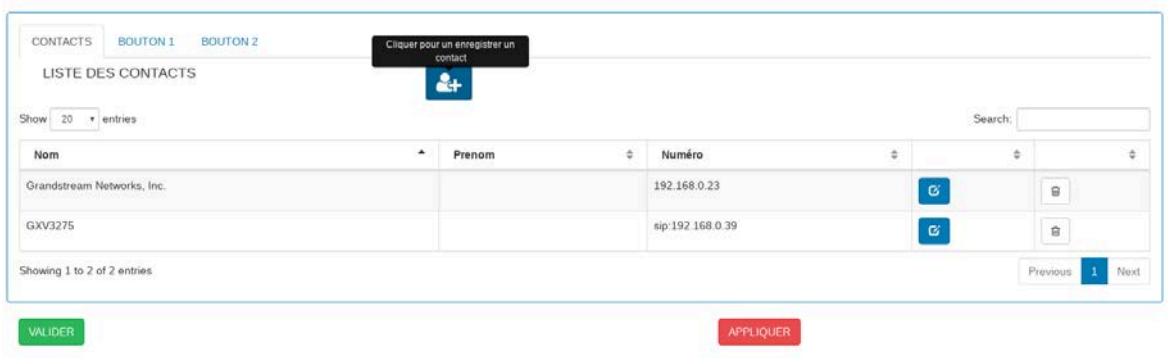


Si un des paramètres est modifié, le bouton VALIDER *s'affiche en vert et le bouton* APPLIQUER *clignote.*

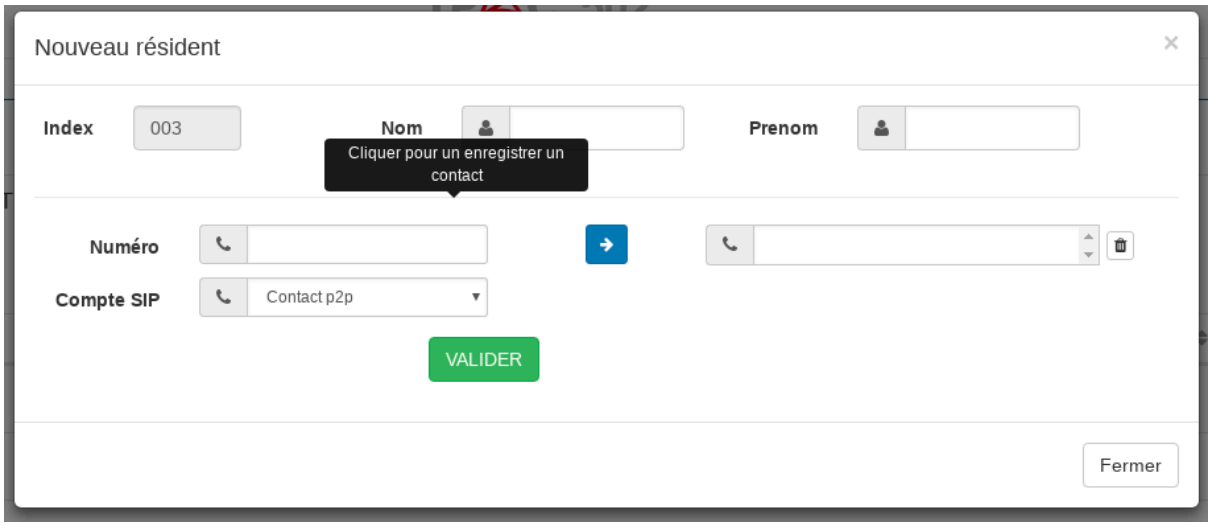
A chaque changement de page web, cliquer sur VALIDER *pour sauvegarder les paramètres de la page.*

Une fois toutes les modifications réalisées, cliquer sur APPLIQUER *pour redémarrer le portier.*

2.1.3. Liste des contacts IPAC 500 Boutons



Cliquer sur  pour créer un résident. Une fenêtre s'affiche :



- Attribuer un « *Nom* » et un « *Prénom* ».
- Saisir un numéro P2P au format adresse IP ou au format plan de numérotation IPBX.
- «*Compte SIP*» : choisir l'adresse IP de l'IPBX ou le mode Peer to Peer.
- Cliquer sur → pour valider le numéro du contact.
- Une **plage horaire** peut être associée au(x) *bouton(s) d'appel*:

- Pour les **IPAC 500 version Porte-étiquettes, l'affichage d'un logo ou d'une image est indisponible.**

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

2.1.4. Relais de télécommande

- *Configuration relais*: **Gâche** ou **Information Prise de Ligne** ou **NetCut***

Relais 1 ou Relais 2 : Le Relais 1 ou le Relais 2 surveille l'état du bouton "ouverture boîtier". Information "portier ouvert /portier fermé" par contact sec vers le produit **NetCut Amphitech** qui coupe automatiquement la connexion RJ45 entre le switch réseau et le portier en cas d'ouverture de l'IPAC 500. L'ouverture de porte par le relais 1 ou par le relais 2 en mode local (code clavier) ou distant (DTMF / API porte) ne fonctionne pas dans cette configuration.

- *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 jusqu'à la fin de la tempo ou au raccroché.

> **Important**
>
> Si les relais sont configurés en Information PDL, ils ne peuvent être utilisés pour activer les entrées.

	Configuration Relais 1	Configuration Relais 2	Entrée 1 / Entrée 2	Entrée 3
 **IPAC 500 DEFILEMENT**	Gâche	Gâche	Relais 1 / Relais 2	Relais 1
	Information PDL / NetCut	Gâche	Relais 2	Inactif
	Gâche	Information PDL / NetCut	Relais 1	Relais 1
	Information PDL / NetCut	Information PDL / NetCut	Inactif	Inactif

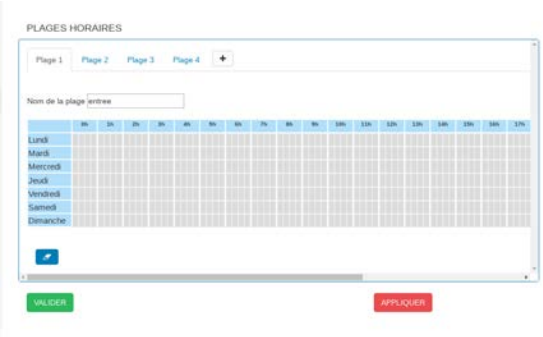
	Configuration Relais 1	Configuration Relais 2	Entrée 1 / Entrée 2	Entrée 3
 **IPAC 500 BOUTONS**	Gâche	Gâche	Relais 1 / Relais 2	Relais 1 / Appel Bouton 1
	Information PDL / NetCut *(PDL et Net-Cut : IPAC mode porte impossible)*	Gâche	Relais 2	Appel Bouton 1
	Gâche	Information PDL / NetCut	Relais 1	Relais 1 / Appel Bouton 1
	Information PDL / NetCut *(PDL et Net-Cut : IPAC mode porte impossible)*	Information PDL / NetCut	Inactif	Appel Bouton 1

2.1.5. Code communs relais

- Possibilité d'attribuer 4 codes par relais, avec ou sans plage horaire.
- Ces codes peuvent être activés en mode local (clavier) **ou** en mode distant (DTMF ou API porte) **ou** en mode local et distant.

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

2.1.6. Plages horaires



Les 4 plages horaires sont attribuées aux :

- Contacts - IPAC 500 Défilement,
- Boutons d'appels - IPAC 500 Boutons,
- Code d'accès,
- Entrées.

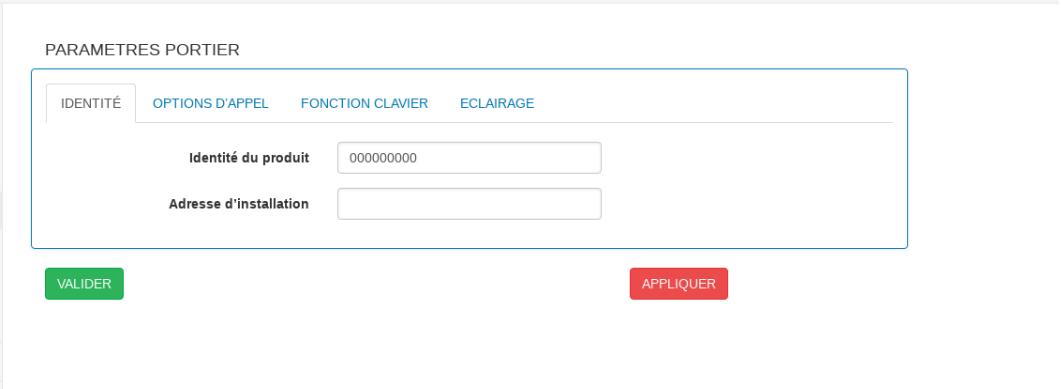
Chaque plage dispose de plusieurs tranches horaires. Chaque tranche horaire peut être sélectionnée 1/4 h par 1/4 h. Un double clic dans une case permet de sélectionner 1 heure entière.

Tranche horaire sélectionnée, appel autorisé 

Tranche horaire non sélectionnée, appel non autorisé

Pour confirmer les changements de la page, cliquer sur  .

2.1.7. Paramètres portier



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

• Onglet *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 en version IPAC Boutons, 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* : fin de communication suite à la réception de commande DTMF de la porte.

– *Temps d'appui bouton* : de **0,5 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.

– *Mode appel direct* : **Uniquement** pour les portiers à défilement : à partir de l'écran d'accueil, permet d'appeler ou non le premier contact de la liste. Dans le cas contraire, l'appui sur le bouton d'appel affiche la liste des résidents.

- Écran d'accueil - **IPAC 500 Porte-étiquettes** Onglet *Fonction clavier*

– Si le clavier est en "code d'accès", la touche * peut être activée pour utiliser la "numérotation libre".

– Touche "#" = "." pour utiliser l'appel par adresse IP.

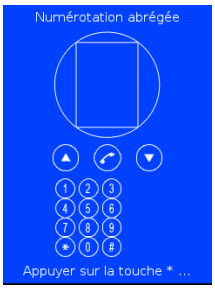
– Touche "*"= correction

– Touche Appel / porte-étiquettes = Appel

- Écran d'accueil - **IPAC 500 Défilement** Onglet *Fonction clavier*

– *Affichage écran d'accueil* : **Oui** pour afficher un message et un logo sur l'écran d'accueil ; **Non** pour utiliser les codes d'accès **ou** la recherche alphanumérique d'un contact sur le clavier.

– *Mode Instructions :* Guide d'utilisation affiché à l'écran quand le produit est au repos.



– *Message d'accueil* : La taille de la police est adaptée à la longueur du texte (capacité : 2 lignes de 20 caractères).

- En mode "avec écran d'accueil" et "Instructions", le clavier est toujours en "code d'accès".

En fonction de la configuration clavier, la touche "*" est utilisée pour : la "numérotation libre" ou 'l'appel abrégé".

- En mode sans écran d'accueil, 4 configurations possibles :

> Code gâche + "numéro abrégé"

> Code gâche + "numérotation libre"

> Recherche alphabétique + "numéro abrégé"

> Recherche alphabétique + "numérotation libre

– *Timer recherche résidents :* durée d'affichage de la liste des contacts s'il n'y a aucun appui sur une touche.

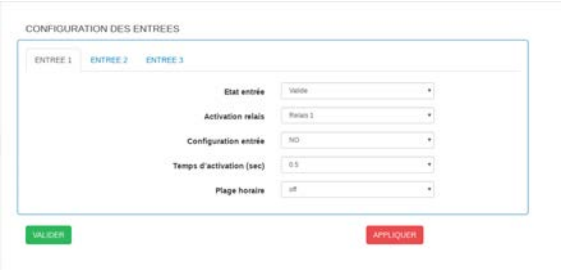
- Onglet *Eclairage*

– Gestion de l'éclairage LCD et clavier/bouton selon la plage horaire.

– Choix d'une luminosité atténuée selon la plage horaire.

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

2.1.8. Configuration des entrées



- Pour les entrées 1 et 2, il est possible de configurer :
  - *État de l'entrée* : valide ou invalide.
  - *Activation relais* : Relais 1 **ou** Relais 2 **ou** Relais 1 et Relais 2
  - *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

> **Note**
>
> Le mode *Discrimination d'appel* permet de valider un appel si et seulement si l'entrée 1 est activée (non fonctionnel avec *Plage horaire*, laisser le paramètre OFF).

	Configuration Relais 1	Configuration Relais 2	Entrée 1 / Entrée 2	Entrée 3
 **IPAC 500 DEFILEMENT**	Gâche	Gâche	Relais 1 / Relais 2	Relais 1
	Information PDL / Net-Cut	Gâche	Relais 2	Inactif
	Gâche	Information PDL / Net-Cut	Relais 1	Relais 1
	Information PDL / Net-Cut	Information PDL / Net-Cut	Inactif	Inactif

	Configuration Relais 1	Configuration Relais 2	Entrée 1 / Entrée 2	Entrée 3
 **IPAC 500 BOUTONS**	Gâche	Gâche	Relais 1 / Relais 2	Relais 1/ Appel Bouton 1
	Information PDL / Net-Cut *(PDL et NetCut : IPAC mode porte impossible)*	Gâche	Relais 2	Appel Bouton 1
	Gâche	Information PDL / Net-Cut	Relais 1	Relais 1/ Appel Bouton 1
	Information PDL / Net-Cut *(PDL et NetCut : IPAC mode porte impossible)*	Information PDL / Net-Cut	Inactif	Appel Bouton 1

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

2.1.9. Configuration des boutons d'appels IPAC 500 Boutons

La fonction bouton est définie en usine selon la version commerciale du portier.

Fonction appel

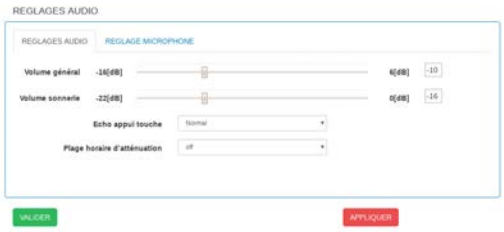
- Attribution ou non d'une plage horaire.
- Choix de 4 numéros dans la liste des contacts.
- → Pour ajouter un contact dans la liste des 4 numéros affectés au bouton d'appel afin de réaliser l'enchaînement automatique des numéros.
- ↑ ↓ Pour modifier l'ordre de l'enchaînement automatique des numéros.
- Pour supprimer un contact sélectionné dans la liste d'appel du bouton.

Fonction porte

- Il est possible d'attribuer une plage horaire au bouton pour autoriser ou interdire la commande de relais.

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

2.1.10. Réglages audio



- *Volume général* : gestion des niveaux audio.
- *Volume sonnerie* : gestion du niveau sonore de la sonnerie sur appel entrant.
- *Echo appui touche* : gestion du niveau sonore des bips (gâche et clavier).
- *Plage horaire d'atténuation* : affectation d'une plage horaire avec atténuation du volume général.
- *Réglage microphone* : gestion du niveau de sensibilité du microphone.
- *Annulation écho* : cocher pour activer.

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

2.1.11. Messages vocaux

- La langue d'exploitation est initialisée à la première mise en service. La langue des messages vocaux est identique.
- *Langue de diffusion et affichage écran* : Changement de langue pour les messages vocaux et les textes affichés à l'écran.
- Cocher la case  pour activer ou désactiver le message vocal.

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

2.1.12. Paramètres réseau

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

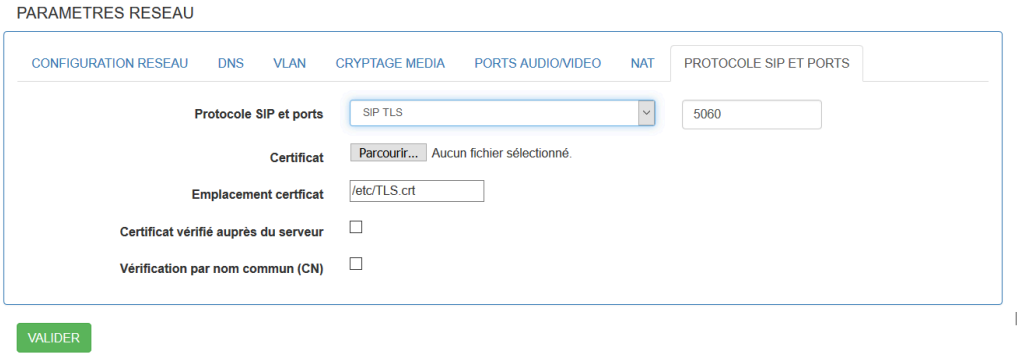
  ou

  - *Dynamique* : adresse IP attribuée automatiquement par un serveur DHCP.
  - *Adresse IP* : adresse IP du produit.
  - *Masque de sous réseau* : masque de sous réseau.
  - *Passerelle manuelle* : adresse IP utilisée pour accéder au WAN (*Wide Area Network*).
- **Bouton utilitaire PING**
  - Entrer l'adresse IP d'un matériel pour tester l'accessibilité réseau vers cette adresse.
- **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**

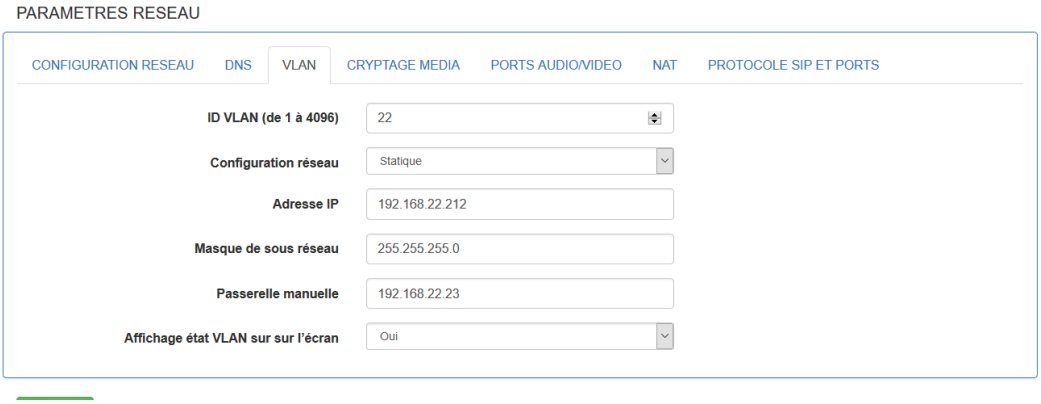
– *SIP (TCP/UDP ou TLS)* : choix du protocole de transport SIP. *Port*: Numéro du port SIP (Par défaut 5060)

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.
- **DNS**
  – *DNS manuel primaire*: adresse IP du premier serveur DNS.
  – *DNS manuel secondaire*: adresse IP du second serveur DNS.
- **VLAN**



  – *ID VLAN* : numéro du taggue VLAN (de 1 à 4096). Pour supprimer le taggue VLAN vider ce champ.
  – *Configuration réseau VLAN* : Statique ou Dynamique.
  – *Adresse IP* : à remplir si mode Statique.
  – *Masque de sous réseau :* à remplir si mode Statique.

– *Passerelle :* indiquer une adresse IP de passerelle pour accèder à un autre réseau.

–

Affichage état VLAN : indication VLAN actif sur écran du portier

Remarques

– Le portier ne peux disposer que d'une seule interface tagguée VLAN.

– Le portier peut disposer de 2 interfaces réseau, une principale et une tagguée VLAN.

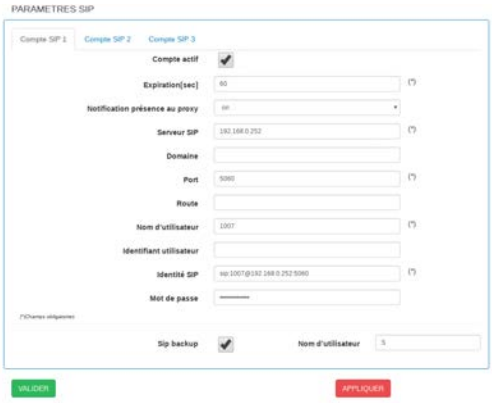
– Si une interface tagguée VLAN est activée en dynamique mais qu'aucune adresse DHCP n'est reçue, les boutons d'appels vont clignoter et l'écran affichera un "problème de connexion".

– Si l'interface VLAN est uniquement nécessaire, il faudra entrer une configuration réseau sur l'interface réseau principale en *Statique*, de manière à accéder au portier en cas de secours (exemple déplacement du portier sur un réseau non VLAN) . L'interface réseau principale sera affichée au démarrage du portier.

– Il est possible de laisser l'interface réseau principale en *Dynamique* , cependant des requêtes UDHCP seront envoyées. Ce procédé permet de réattribuer facilement une adresse IP sur le réseau principal en cas de déplacement du portier sur un réseau non taggué VLAN du même ID.

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

2.1.13. Paramètres SIP



- **Paramètres IPBX**

– *Compte SIP x* : possibilité d'utiliser trois comptes SIP sur différents IP-PBX **ATTENTION :** l'appel libre et le LDAP utilisent le compte SIP 1.

– *Compte actif* cocher la case Compte actif pour activer ou désactiver le compte SIP auprès de l'IPBX. 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'IPBX.

– *Notification présence au proxy* : valider ou non-valider l'envoi de la notification de présence, PUBLISH, dans les échanges SIP entre l'IPAC 500 et le proxy SIP.

– *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 - Compte SIP (login compte SIP)* : nom d'affichage SIP, **le nom ne doit pas comprendre de caractère Espace.**

– *Identifiant utilisateur* : identifiant nécessaire à l'enregistrement auprès de l'IPBX.

– *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'IPBX.

– *Sip backup*: cocher la case pour permettre d'utiliser le mode redondance serveur IPBX. Si l'appel du contact échoue avec le serveur IPBX qui lui est attribué, l'appel s'effectuera avec l'un des autres comptes SIP valides.

– *Nom d'utilisateur* Nom d'utilisateur S : 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.

- **Création contact SIP**: lors de la création d'un contact en *sip:xxxxxxx@sip.linphone.org* si l'IPAC 500 est enregistré sur un ou plusieurs proxy, comme le contact est en Linphone, le @proxy (configuré) ne sera pas ajouté à la suite de l'URI linphone. L'appel vers un contact Linphone sera toujours valide même si aucun proxy n'est fonctionnel **sauf** si un proxy sip linphone (pour appel l'IPAC) est configuré.

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

2.1.14. Codecs audio

- **Choix des codecs audio** : codecs utilisés lors d'une communication vocale entre l'IPAC 500 et le poste du correspondant. Pour chaque codec :

  – Déplacer le codec choisi de la liste "Disponibles" à la liste "Sélectionnés" ou inversement à l'aide des flèches et .

  – Utiliser les flèches et pour modifier l'ordre de priorité dans la liste des codecs sélectionnés.

Exemple 2.1. Ordre de priorité des codecs sélectionnés

– *Priorité 1* : PCMU

– *Priorité 2* : PCMA

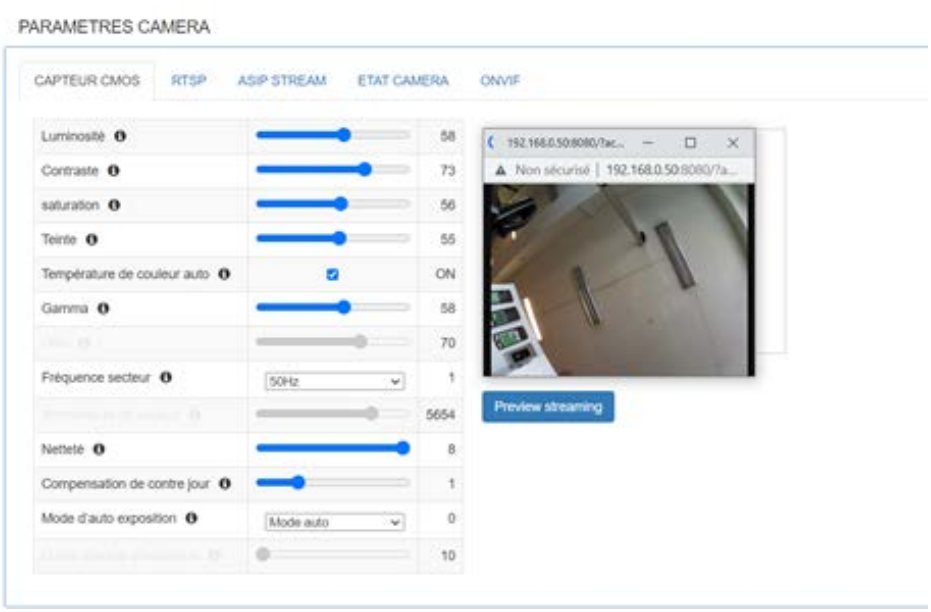
– *Priorité 3* : speex8k, etc.

- **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.*
- **Gestion de la bande passante** (flux média RTP)
  - *Mode automatique*
  - *Mode manuel* : choix des datas envoyées et reçues (kbits).

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

2.1.15. Paramètres vidéo

2.1.15.1. Capteur CMOS

- 

Cette caméra possède des réglages de capteur CMOS tels que :

- Luminosité : quantité de lumière sur l'image.
- Contraste : rapport entre luminosité maximale et luminosité minimale d'une image.
- Saturation : intensité de la coloration de l'image.
- Teinte : le réglage de la teinte permet de déplacer la couleur moyenne de l'image vers une extrémité ou l'autre du disque chromatique, c'est à dire vers le bleu ou le magenta.
- Température de couleur auto : ce paramètre permet de contrôler automatiquement le mode de calcul de la température de couleur des images du capteur. Si le paramètre est décoché, le réglage sera manuel.
- Gamma : la correction gamma consiste à appliquer un gain non linéaire à l'amplitude des pixels afin d'accentuer la différence entre les pixels clairs et les pixels sombres au voisinage d'une gamme de luminosité donnée.

- Gain : le gain est le rapport d'amplification appliqué aux signaux des pixels du capteur. Un gain faible correspond à une faible luminosité et vice-versa.
- Fréquence secteur : ce paramètre permet d'indiquer si la fréquence secteur est de 60 Hz (par exemple : Etats-Unis) ou de 50 Hz (par exemple : France) afin d'ajuster les durées d'ex permettant d'éviter un clignotement observable sur les vidéos. C'est un paramètre à prendre en compte avec un éclairage artificiel, souvent en intérieur, lorsqu'on utilise des lampes à incandescence.
- Netteté : pour augmenter artificiellement la netteté d'une image.
- Compensation de contre-jour : il s'agit de différents algorithmes utilisés pour essayer de mettre en valeur l'avant ou l'arrière-plan en fonction de la luminosité des zones centrale et périphérique de l'image. Certains de ces algorithmes sont adaptatifs et prennent en compte dans le calcul la luminosité de chaque zone de l'image afin de déterminer la correction globale.

Sans correction

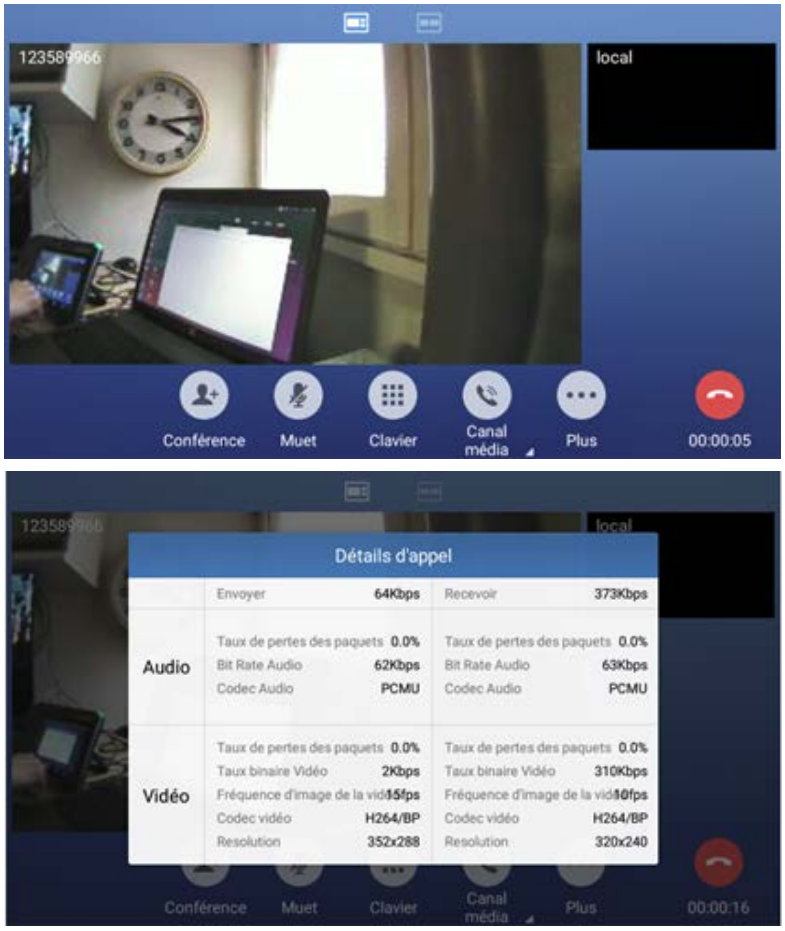
Avec correction

- Durée absolue d'ex : durée d'ex (dans le mode d'ex manuel), en multiples de 100 micro secondes.
- Bouton " Preview streaming " : permet d'ouvrir une fenêtre avec la vidéo du portier si le navigateur n'a pas pu ouvrir automatiquement la vidéo dans la fenêtre CAPTEUR CMOS.

A chaque modification de paramètres CMOS, l'image de droite dans la même fenêtre, permet de pré-visualiser le réglage effectué.

Pour prendre en compte les changements, cliquer sur VALIDER puis sur REDEMARRER .

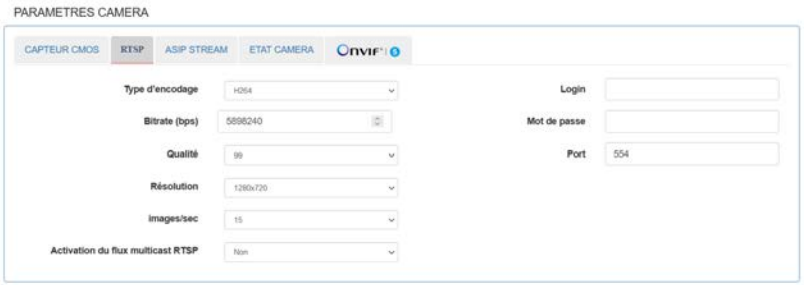
Exemple de réception vidéo sur poste SIP GXV3370 Grandstream (réception en 320p x 240p - H264 - 10 fps)



2.1.15.2. Serveur RTSP

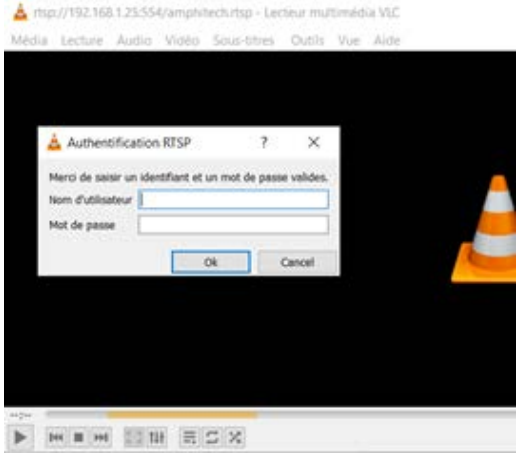
Le portier est équipé d'un serveur RTSP de manière à envoyer le flux de la caméra vers des enregistreurs réseau de vidéosurveillance. Ce flux vidéo peut être envoyé au format encodé en H264 ou en MJPEG avec différentes résolutions : 1280p x 720p, 680p x 480p, 320p x 240p.

L'onglet RTSP permet de régler :



- *Type d'encodage :* Définit le type d'encodage utilisé pour le flux RTSP (**H264** ou **MJPEG**)
- ***Si l'encodage utilisé est·:***
  - **H264** alors le réglage du BitRate sera possible (débit des données vidéos en bits/sec), de 1 à 20 000 000bps.
  - **MJPEG** alors le réglage possible sera la qualité de compression MJPEG (de 1 à 99).
- *Images /Sec :* nombre d'images par secondes.

- *Login / Mot de passe :* authentification pour ouvrir un flux RTSP.



- *Port :* Port du protocole RTSP. Par défaut, 554.
- *Activation du flux multicast RTSP* : Oui / Non - Permet d'activer le flux RTSP en multicast UDP.

  Attention : Cela peut ralentir le transfert des datas sur le réseau IP.

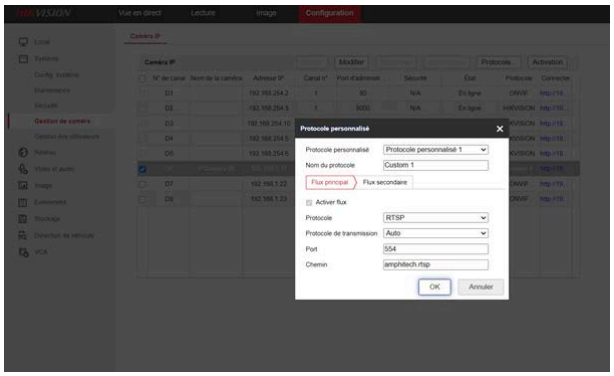
Pour prendre en compte les changements, cliquer sur VALIDER puis sur REDEMARRER.

Pour récupérer un flux RTSP, utiliser l'adresse suivante :

Rtsp://login :password@adresse_IP_Portier :portRTSP/amphitech.rtsp

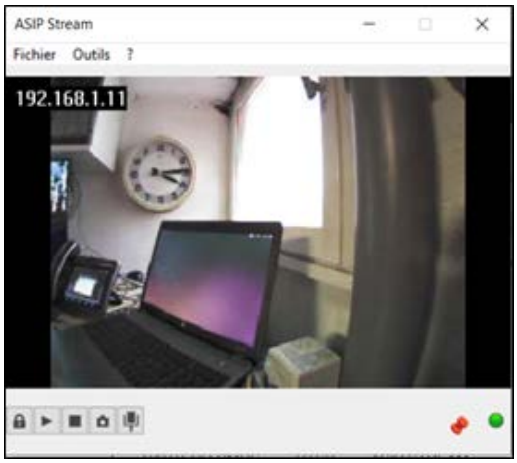
Exemple sur VLC :

Sur un enregistreur IP de vidéosurveillance (HIK-CONNECT) :



2.1.15.3. ASIP STREAM

L'onglet ASIP STREAM permet d'utiliser le lecteur vidéo qui peut être installé sur PC :



ASIP STREAM utilise la connexion au serveur MJPEG intégré au portier. Cela permet de visualiser le flux MJPEGSTREAMER de la caméra en non-stop mais aussi d'utiliser ASIP STREAM de manière à visualiser le flux vidéo de la caméra à la suite d'un appel émis depuis le portier.

Les options configurables dans le portier sont :

Lancement Stream sur ASIP STREAM :

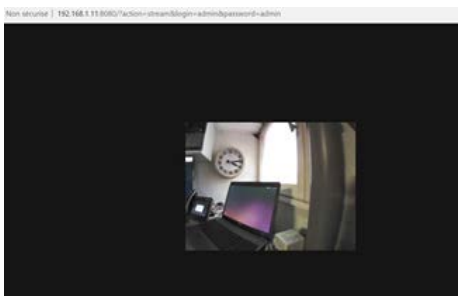
- Au décroché du distant (poste appelé).
- A l'appui sur le bouton d'appel.
- Login et mot de passe pour accèder au serveur MjpegSteamer
- Port : port de diffusion du flux MjpegStreamer

Pour accèder au flux vidéo diffusé par le serveur MjpegStreamer depuis un navigateur Web ou client MjpegStreamer, entrer l'adresse URL :

http://adresse_IP_portier:port/?action=stream&login=login&password=mot_de_passe

Exemple :

http://192.168.1.11:8080/?action=stream&login=admin&password=admin



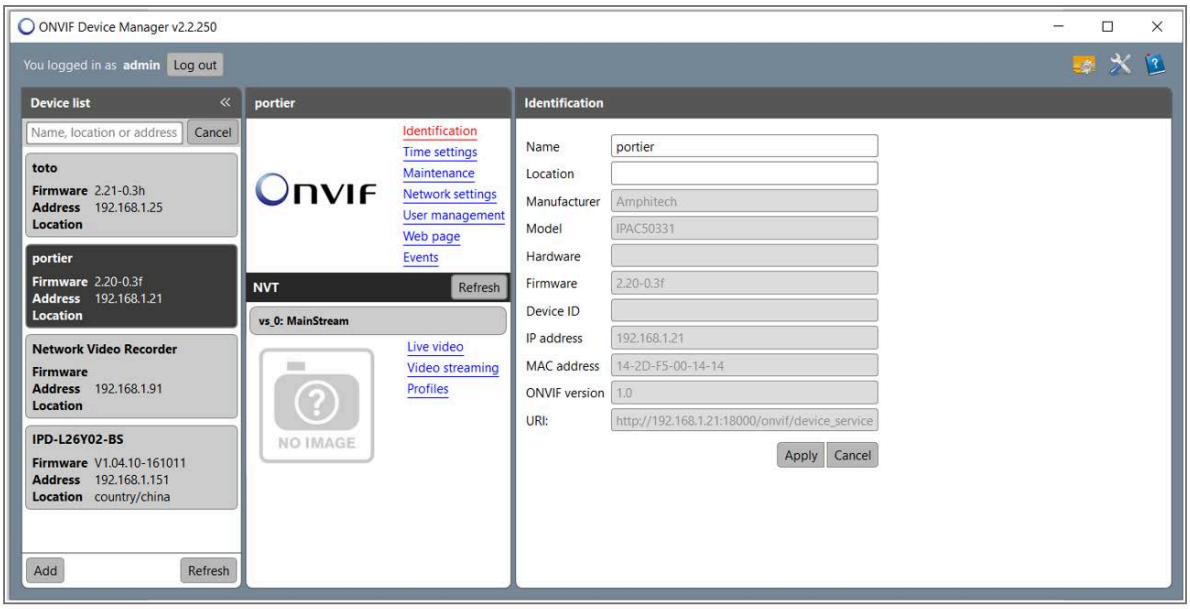
2.1.15.4. Gestion du protocole ONVIF

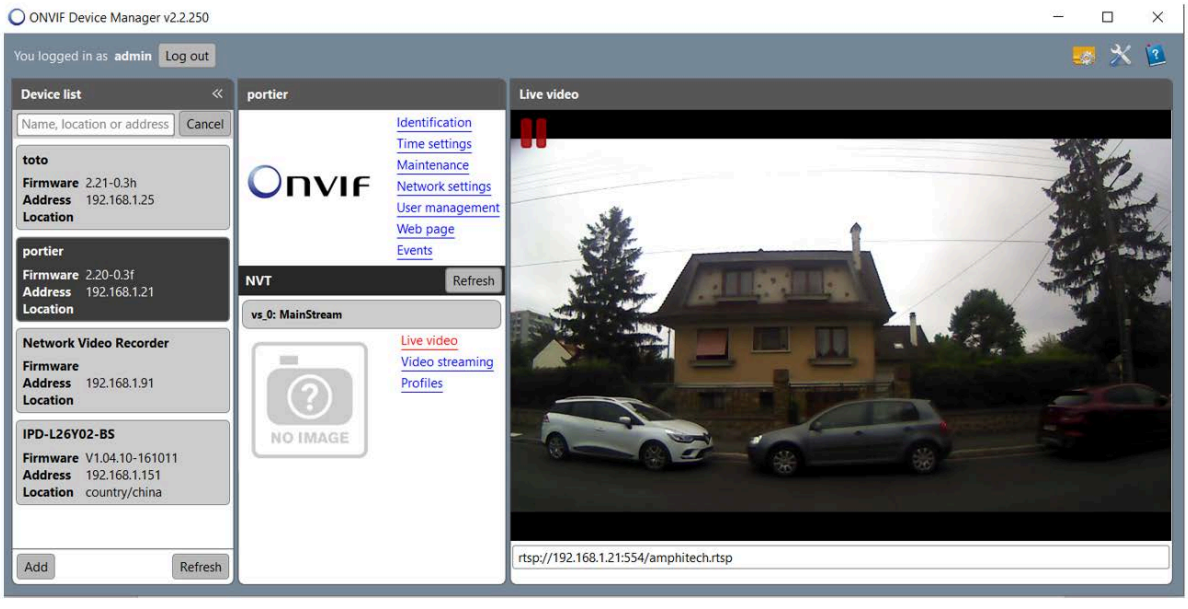
L'IPAC dispose du protocole ONVIF permettant,

- d'être détecté par des enregistreurs réseau vidéo compatible ONVIF,
- d'être détecté par l'outil ONVIF DEVICE MANAGER,
- de configurer certains paramètres du portier comme :
  - la configuration réseau,
  - la gestion de l'heure système,
  - le choix du type d'encodage RTSP, résolution, images/sec,
  - le redémarrage du portier avec les commandes de reset, etc...

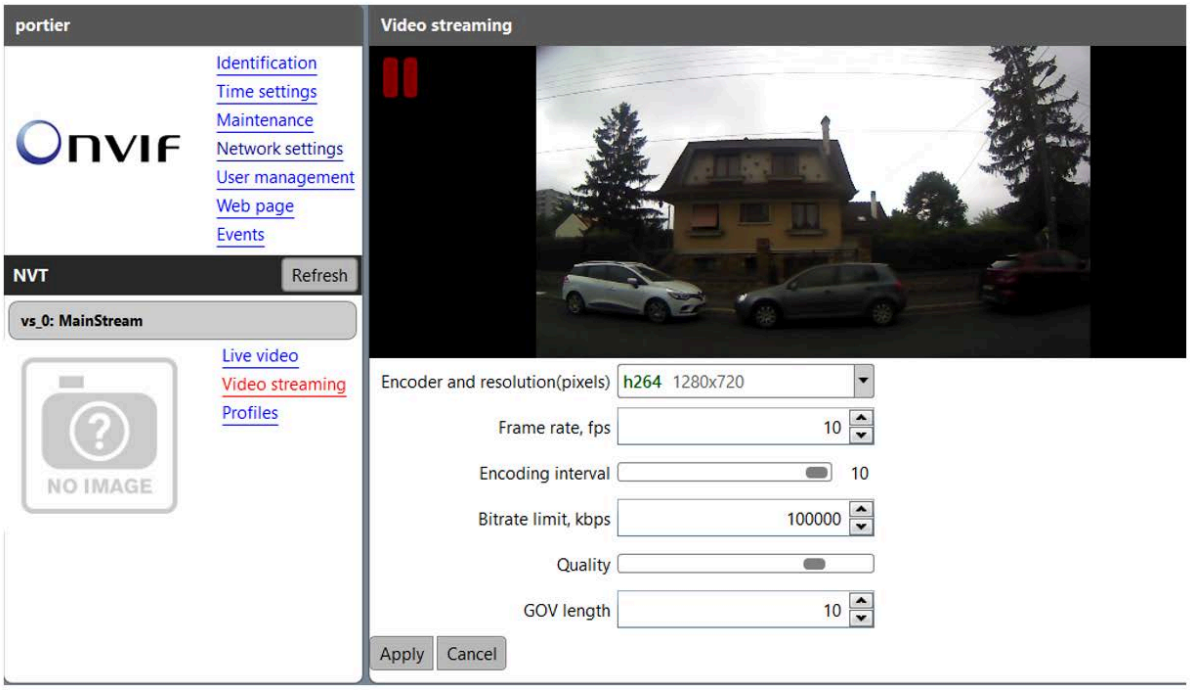
Le portier IPAC 500 avec option vidéo est certifié ONVIF Profil S (https://www.onvif.org/confor-mant-products/).

Exemple de détection du portier IPAC 500 en utilisant le protocole ONVIF sous ONVIF DEVICE MANAGER (logiciel installé sur PC)



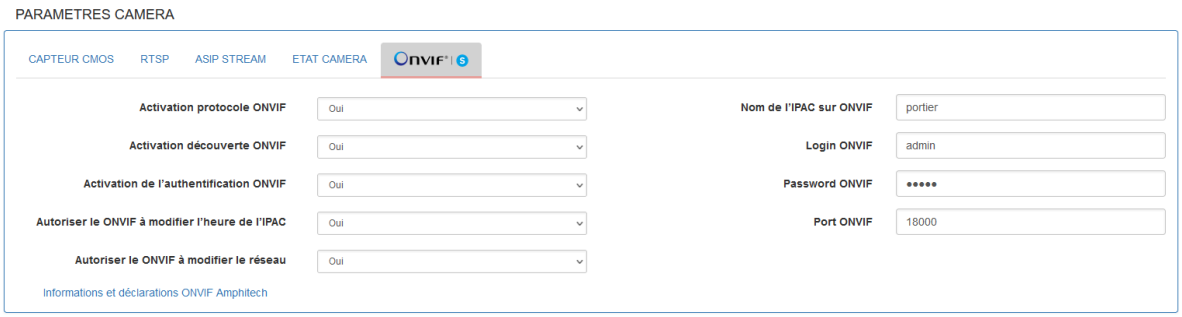


Exemple de modification du flux RTSP via ONVIF :



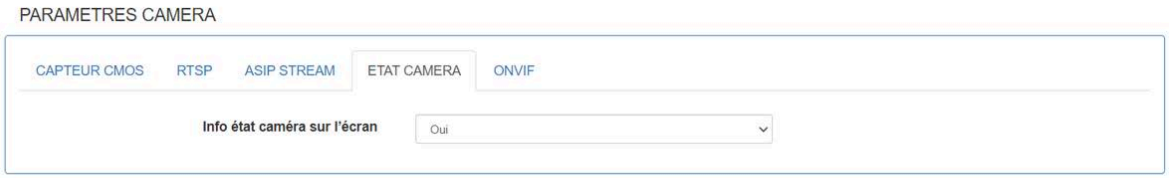
Pour activer le protocole ONVIF sur l'IPAC 500 :

A partir des pages WEB du portier, dans l'onglet *PARAMETRES AVANCES / PARAMETRES CAMERA / ONVIF*:



- *Activation protocole ONVIF* : Oui / Non - Pour activer ou ne pas activer le protocole ONVIF.
- *Activation de la découverte ONVIF* : Oui / Non - Si "Oui", permet de rendre le portier détectable avec le protocole ONVIF.
- *Activation de l'authentification ONVIF* : Oui / Non. Si "Oui", il faut créer un login et un password ONVIF.
- *Password et Login ONVIF*
- *Port ONVIF*
- *Autoriser le protocole ONVIF à modifier l'heure de l'IPAC*: Si oui, cela signifie que la mise à l'heure de l'IPAC peut se faire à partir du serveur ONVIF.
- Le protocole ONVIF peut gérer l'heure de 2 manières :
  - en activant le NTP avec l'utilisation d'un serveur NTP,
  - en synchronisant l'IPAC avec le fuseau horaire du serveur.
- *Autoriser le protocole ONVIF à modifier le réseau* : Cela veut dire que le protocole ONVIF (via un serveur) peut modifier la configuration réseau du portier (DHCP/Statique, IP, DNS, passerelle...).

2.1.15.5. Gestion de l'information de l'état de la caméra sur l'afficheur

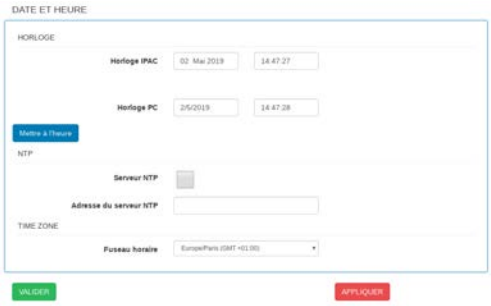


Info état de la caméra sur l'écran : Oui / Non

-  Caméra détectée
-  Streaming RTSP et MjpegStreamer valide

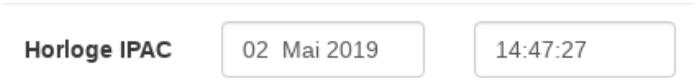
Pour prendre en compte les changements, cliquer sur VALIDER puis sur REDEMARRER.

2.1.16. Date et heure

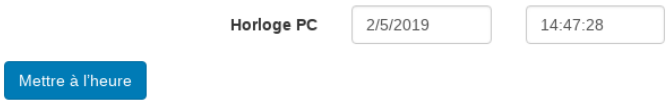


La mise à l'heure du produit est importante pour la gestion des plages horaires.

- Heure actuelle de l'IPAC 500 :



- Changer manuellement l'heure et la date :



- Cocher la case pour utiliser un serveur NTP et mettre à l'heure automatiquement l'IPAC 500 :

- 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  .

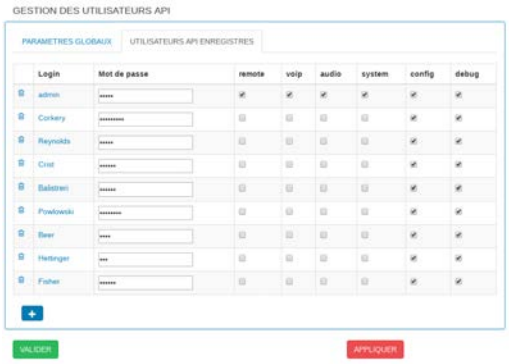
2.1.17. Compte mail

L'IPAC 500 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 **ENVOI D'EMAIL** .

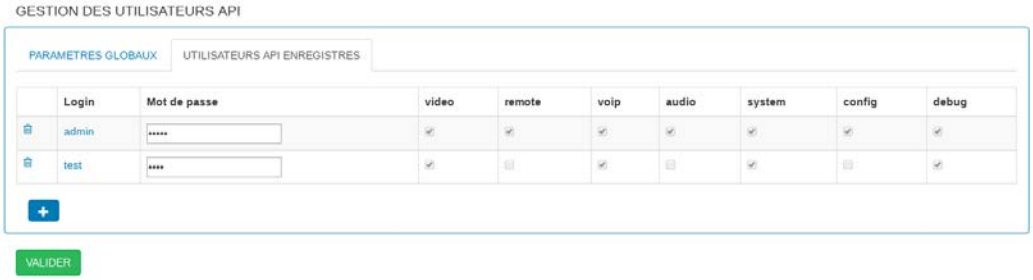
- *Envoi d'email* : cocher pour valider l'envoi d'e-mails.
- *Serveur* : saisir l'adresse du serveur d'envoi.
- *Port SMTP* : port utilisé
- *Mode sécurisé* : choisir le mode de cryptage : SSL / TLS ou clair.
- *Compte* : saisir adresse e-mail du compte émetteur.
- *Mot de passe* : saisir mot de passe du compte émetteur.
- *Sujet* : saisir l'objet.
- *Destinataire* et *Copie*: saisir les adresses mails des destinataires.
- *Fréquence d'envoi des emails* : de 1 à « x » minutes.
- *Envoi snapshot* : permet d'envoyer une photo issue de la caméra du portier suite à l'appui sur le bouton d'appel.

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

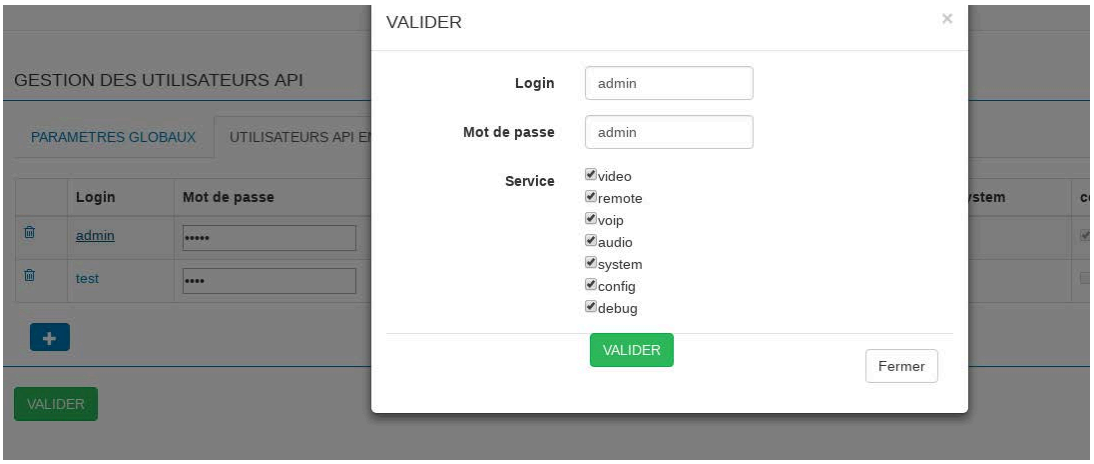
2.1.18. API



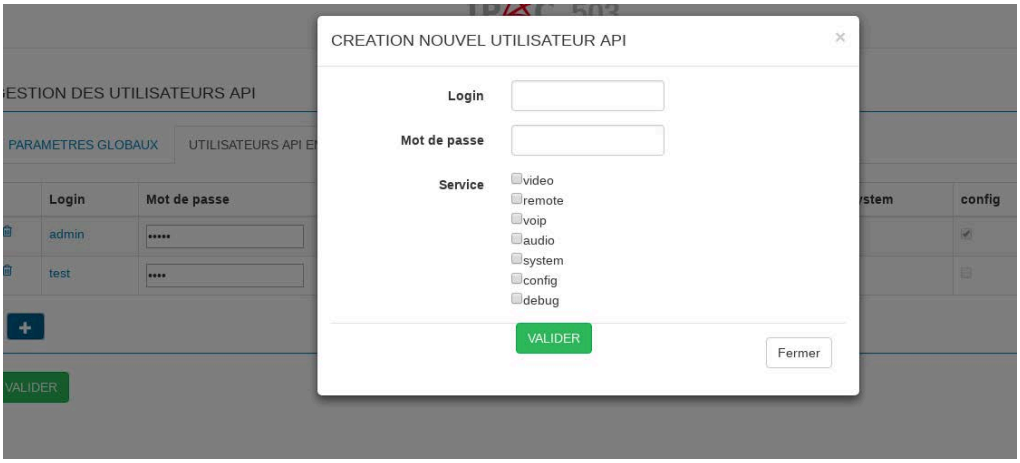
- **Paramètres globaux**
  - *Méthode GET/POST* : choix de la méthode d'envoi de l'API sur le réseau.
  - *Authentification* : type d'authentification *NONE / BASIC / DIGEST*
- **Utilisateurs API enregistrés**



  - Ajout d'un *Login* et d'un *Mot de passe* avec les attributions des API en fonction du login. Pour chaque utilisateur il est possible d'attribuer une ou plusieurs API au choix.
  - Modification des droits : cliquer sur le nom **Login** et choisir le type d'API autorisée pour le login sélectionné :



  - Ajout d'utilisateurs API :



Exemple

Ces API sont des API natives du produit, elles permettent une utilisation directe à partir d'un terminal présent sur le même réseau capable d'envoyer des requêtes de type GET et POST sous différents formats comme JSON ou URL ENCODED.

Exemple du contenu du fichier payload.txt :

{"type":"wav","loop" :"2","data":" UklGRmQfAABXQVZFZm10IBAAA…..ouJiImHhA=="}

La «value » de la clé « data » correspond à un fichier .wav converti en base64.

Exemple d'envoi d'une requête JSON contenant un fichier WAV encodé en base64:

curl -X POST -d `cat payload.txt` http://admin:admin@192.168.0.30/api/audio/ --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 commande stop formal 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/ --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

4. **API LCD**

Cette API permet d'envoyer un fichier image *(.png, .jpeg, .GIF*.). Le fichier est ensuite affiché sur l'afficheur LCD du produit *uniquement* quand le portier n'est pas en mode « communication » ou « ouverture porte ».

– **Afficher une image**

tempo:

Durée d'affichage de l'image. Dans le cas d'un nombre nul ou non précisé, l'image sera affichée indéfiniment tant que le portier est au repos.

Intervalle : 0 – 9999 sec.

Exemple d'envoi d'une requête JSON contenant un fichier png encodé en base64 :

curl -X POST -d $(cat image.b64) http://admin:admin@192.168.0.48/api/video/ --digest --header "content-type: application/json" --header "Expect:"

1. **API Porte**

Le code porte API correspond à un des codes communs Relais 1 ou Relais 2. L'API porte est soumise à la plage horaire ou au mode d'activation du code commun Relais 1 ou Relais 2 (Local/Distant). *Paramètres usine : user = admin / password = admin* .

Dans l'exemple, *user = toto / password = titi*.

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

Num = numéro relais, soit 1 = RL1, 2 = RL2 , 3 = RL1 et RL2.

Authentification NONE :

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

curl -d "code=1234&relay=num&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&relay=num (GET)

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

Authentification DIGEST :

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

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

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

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

Attention : Le mode d'authentification est sauvegardé dans le cash de la page durant toute 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)

Exemples Formats JSON et URL Encoded :

POST:

curl -X POST -d '{"code":"1111","relay":"1"}' http://admin:admin@192.168.0.30/api/remote/ --digest --header "Content-Type: application/json"

POST:

curl -d "code=1111,relay=1" -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&relay=1

2. **API VoIP**

Cette API permet de contrôler à distance 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 données 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

Exemples Formats 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

3. **API Audio**

Cette API permet d'envoyer un fichier .WAV encodé en base64 dans une URL adressée au portier, le fichier est ensuite diffusé dans le haut-parleur du portier (1 Mo max.).

– **Lire un fichier WAV**

loop:

Nombre de répétitions du fichier audio. Dans le cas d'un nombre nul ou non précisé, le son sera diffusé en boucle indéfiniment tant que le portier est au repos.

Intervalle : 0 - 9999

Pour un fichier audio (payload.txt)

Exemple du contenu du fichier payload.txt :

{"type":"wav","loop" :"2","data":" UklGRmQfAABXQVZFZm10IBAAA…..ouJiImHhA=="}

La «value » de la clé « data » correspond à un fichier .wav converti en base64.

Exemple d'envoi d'une requête JSON contenant un fichier WAV encodé en base64:

curl -X POST -d `cat payload.txt` http://admin:admin@192.168.0.30/api/audio/ --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 commande stop formal 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/ --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

4. **API LCD**

Cette API permet d'envoyer un fichier image *(.png, .jpeg, .GIF*.). Le fichier est ensuite affiché sur l'afficheur LCD du produit *uniquement* quand le portier n'est pas en mode « communication » ou « ouverture porte ».

– **Afficher une image**

tempo:

Durée d'affichage de l'image. Dans le cas d'un nombre nul ou non précisé, l'image sera affichée indéfiniment tant que le portier est au repos.

Intervalle : 0 – 9999 sec.

Exemple d'envoi d'une requête JSON contenant un fichier png encodé en base64 :

curl -X POST -d $(cat image.b64) http://admin:admin@192.168.0.48/api/video/ --digest --header "content-type: application/json" --header "Expect:"

Avec le fichier image. b64 contenant:

{"type":"img","tempo":"60","data":"iVBORw0KGgoAAAANSUhEUgAAAWQAAAEACAYAAA-CEfg…·"}

La « value » de la clé « data » correspond à une image format png convertie en base64.

– **Stopper l'affichage de l'image**

Indique l'arrêt de l'affichage de l'image.

Exemple commande stop format Json :

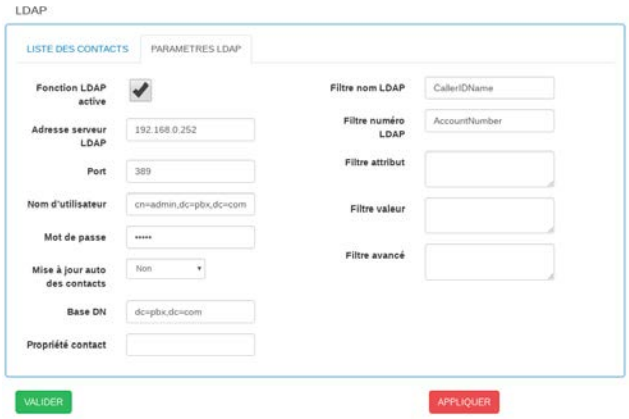
curl -X POST -d $(cat stop.txt) http://admin:admin@192.168.0.48/api/video/ --digest --header "content-type: application/json" --header "Expect:"

stop.txt :

{"type":"img","tempo":"60","data":"stop"}

2.1.19. LDAP

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



- Cocher la case **Fonction LDAP active** 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 ne sera plus affiché au prochain redémarrage.

- Adresse serveur LDAP 192.168.0.252 / Port 389 : 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.
- *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).
- *Propriété contact* : xxxyz
- *Filtre nom LDAP*: attribut du nom du contact

- *Filtre numéro LDAP* : attribut du numéro d'appel du contact
- *Filtre attribut* : permet de filtrer x attributs LDAP. *Exemple*: attribut1;attribut2;...

> **Attention**
>
> Chaque attribut doit être séparé par le caractère ;

- *Filtre valeur* : correspond aux valeurs recherchées des x attributs définis au-dessus. *Exemple* : valeurAttribut1;valeurAttribut2;...

> **Attention**
>
> Chaque valeur d'attribut doit être séparée par le caractère ; La valeur peut être une chaîne mais ne doit pas contenir de caractères ;

- *Filtre avancé*: **Si vous utilisez ce filtre, le filtre attribut et le filtre valeur ne doivent pas être utilisés.** Ce filtre permet d'utiliser des fonctions logiques ( ) ,&&, || ,== ,!= *Exemple* : ((givenName!=John)&&(physicalDeliveryOfficeName==Dorian||physicalDeliveryOfficeName==test)&&(badPwdCount==0))||(initials==JD)
- *Filtre numéro LDAP* : attribut du numéro d'appel du contact

L'attribut est une chaîne de caractères destinée à être recherchée pour chaque contact du serveur pour récupérer les entrées d'un annuaire LDAP.

Pour bénéficier des attributs "index" pour un "numéro abrégé" et des options "Prioritaire" et "Plages horaires", il faut utiliser un attribut libre sur le serveur lors de la création du contact. Saisir les informations suivantes : xxxyz

– *xxx* correspond aux 3 digits du "numéro abrégé" (commencer par 500 pour le premier contact afin d'éviter les conflits avec la table des contacts créés manuellement)

– *y* correspond à l'option "Prioritaire", 1 = Oui ; 0 = Non

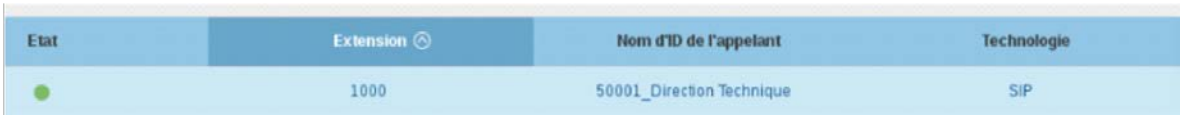
– *z* correspond à l'option "Plages horaires", 1 = Oui (Nom de la plage définie dans la liste des contacts) ; 0 = Non

Dans le champ **Propriété contact** , indiquer le nom de l'attribut libre à utiliser.

Si aucun attribut n'est disponible dans la fiche de création du contact sur le serveur, il est possible d'ajouter au nom ou au prénom "*xxxyz_prénom".*

Le système récupère alors le prénom et le nom avec le *"xxxyz_"* de manière à renseigner les informations des "numéros abrégés" et des options "Prioritaire" et "Plages horaires" dans le répertoire LDAP du produit. Dans ce cas, il n'est pas nécessaire de renseigner le champ *Propriété contact* .

Exemple de création sur un serveur OpenLDAP :



– 500 = "Numéro abrégé"

– 0 = "Non Prioritaire"

  - 1 = "Oui" (Plage horaire résidents)
- *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.

Mode SIP. Si le portier est utilisé avec un serveur IPBX, veiller à renseigner les champs de connexion « Compte SIP » avant d'utiliser la synchronisation LDAP.

Mode P2P. Utiliser un attribut LDAP libre lors de la création de l'utilisateur dans le serveur et y renseigner 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'appel.

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

et 

pour redémarrer le portier.

2.1.20. 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**.

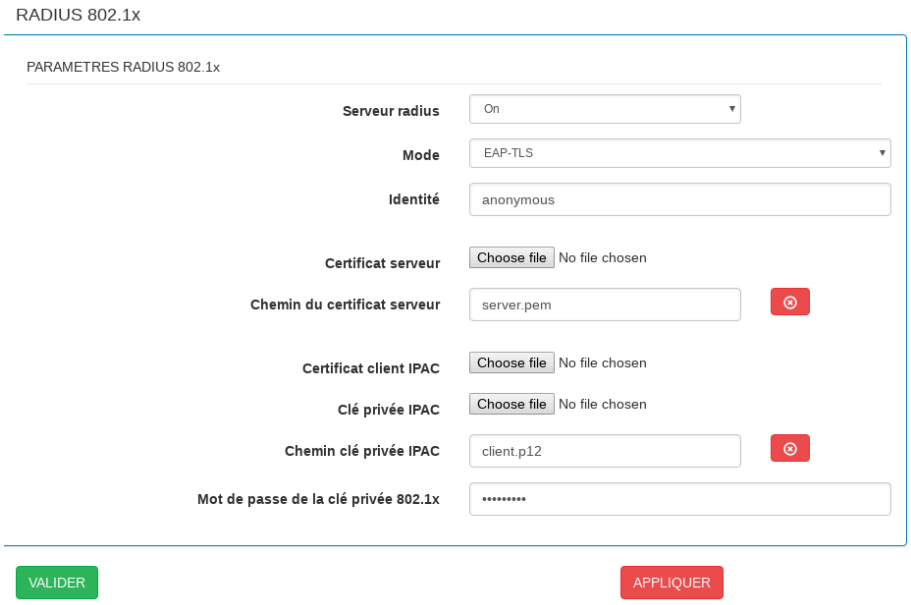
- des modes sécurisés **EAP** : PEAP, EAP-TTLS, EAP-TLS.

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

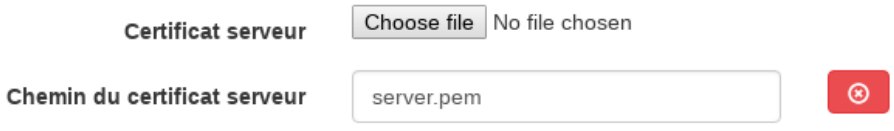
the non-tunneled EAP module …

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.

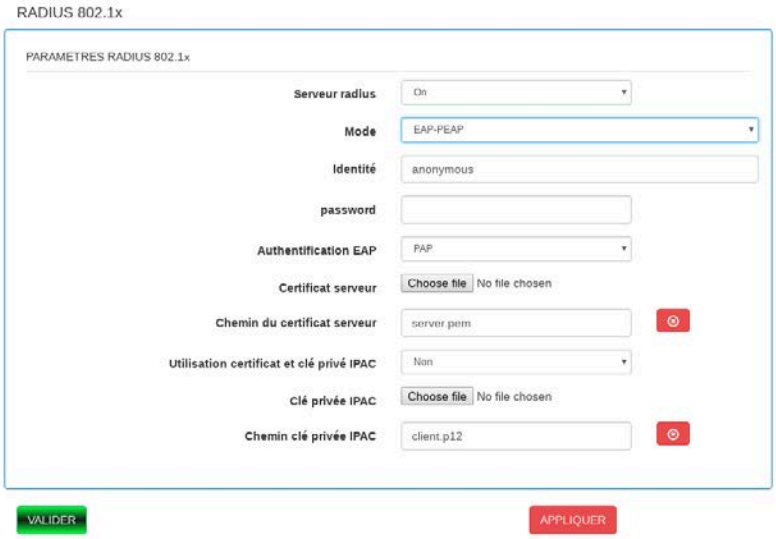
   Pour utiliser un certificat serveur auto-signé ou signé par une autorité de certification, il faut importer le certificat CA.pem dans l'IPAC. Si aucun fichier de type *.pem* n'est importé, l'IPAC ne transmettra pas le certificat au serveur (si nécessaire), et l'authentification échouera.



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).

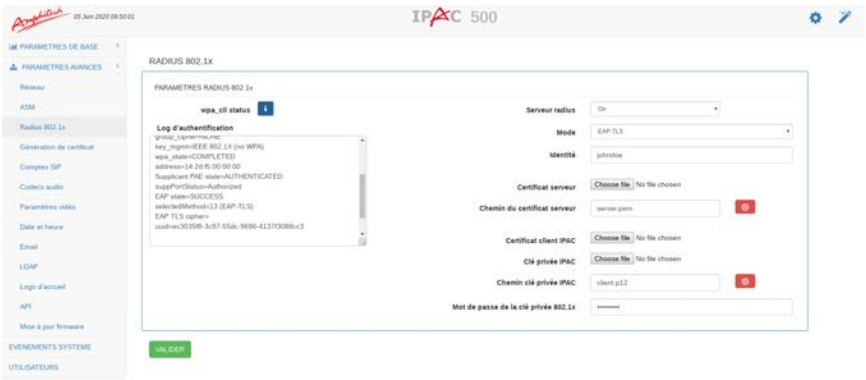
Il est possible de passer en mode Anonymous (plus d'identité au niveau du serveur) dans ce cas, dans la partie « identité » saisir : **anonymous**.

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

Il faudra alors remplir tous les champs de la page :



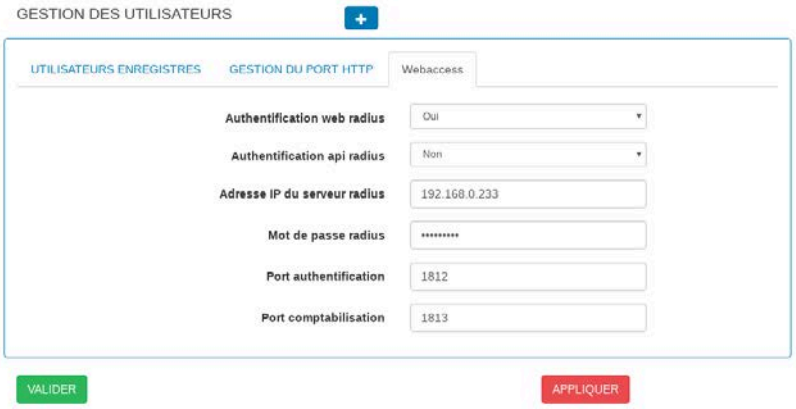
Log radius : cliquer sur le bouton "wpa_cli status", retour information d'authentification vers le serveur RADIUS.

2.1.21. Accès web par authentification serveur Radius

Le Serveur Radius permet aussi de gérer l'authentification des comptes (Accounting) via la méthode PAP pour accéder 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 avec comme attributs :

- **Login**
- **Mot de passe**
- Droit d'utilisation : **Administrateur** ou **Utilisateur**



En activant la solution **Authentification web radius** Oui :

L'authentification interne à l'IPAC fonctionnera encore, si login et mot de passe correspondent, l'accès aux pages s'effectuera en fonction des droits d'utilisation du compte local.

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** crée 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 pour un serveur Free Radius

- Déclaration de l'adresse IP du switch réseau servant d'identificateur RADIUS

  ##

  #

  # 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 = 123456789

  }

- Création d'un utilisateur (login) d'accès web /etc/user
  - Login : **johndoe**
  - Password : **pass42**
  - Droits d'accès : **Administrative-User** *(droit admin IPAC)* ou **Login-User** *(droit utilisateur IPAC)*

  # #

  # # Last default: shell on the local terminal server.

  # #

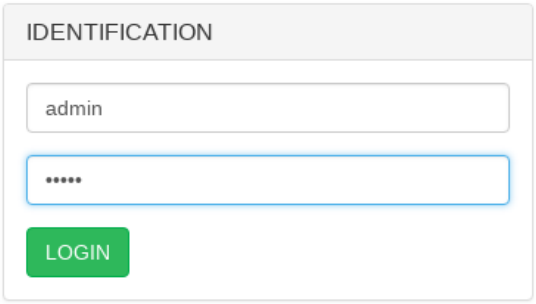
  # DEFAULT

Service-Type = Administrative-User

On no match, the user is denied access.

johndoe Cleartext-Password := "**123456789**"

Service-Type = **Administrative-User**



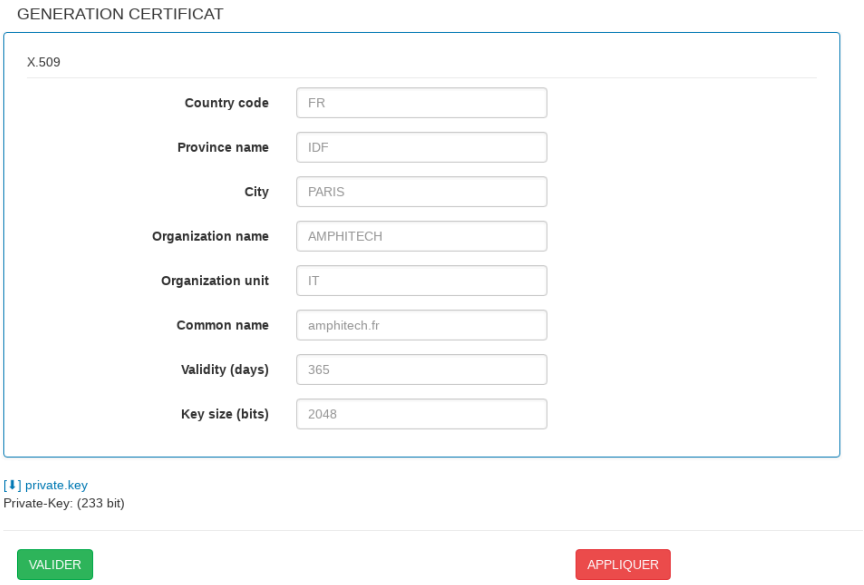
Dans cette fenêtre d'identification du login, si l'option radius est activée, il est possible de s'authentifier soit·:

– 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.

2.1.22. Génération de certificats



Le format du certificat et de la clé privée utilise le X.509. Saisir les informations personnelles dans les différents champs puis cliquer sur VALIDER . *Si les modes EAP-TLS ou TTLS sont utilisés,* le certificat et la clé privée vont être générés en fonction des informations renseignées puis intégrés dans les champs de certificats RADIUS de la page web RADIUS 802.1x.

> **Attention**
>
> Avant la génération de certificats, vérifier que la date et l'heure de l'IPAC sont correctes.

2.1.23. Logo d'accueil

- Cliquer sur 

pour importer une photo (format PNG). Le redimensionnement est automatique.

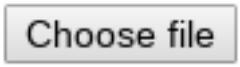
- Cliquer sur 

pour valider. Une fenêtre s'ouvre pour indiquer que le chargement s'est bien déroulé.

- *Pour confirmer les changements, cliquer sur* 

.

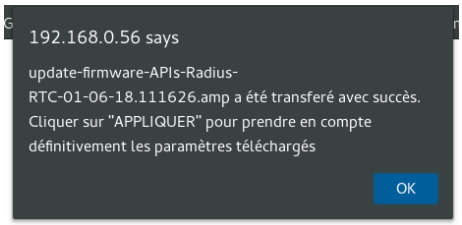
2.1.24. Mise à jour Firmware

- 

permet de chercher un fichier de mise à jour .amp

- 

permet de charger le fichier. Le fichier est vérifié par le système avant la mise à jour.



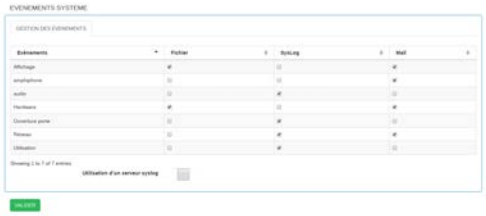
- APPLIQUER lance la procédure de mise à jour.

> **Attention**
>
> L'alimentation doit rester connectée à l'IPAC 500.

- 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 donnée doivent être sauvegardés. Les configurations SIP et les paramètres produits sont sauvegardés automatiquement.

2.1.25. Evénements système



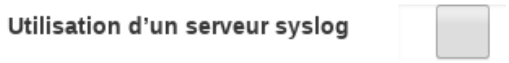
- Le tableau de **Gestion des événements** permet de choisir le type d'événements système pour envoi de notifications :
  - *Affichage* : pour garder un historique de ce qui est affiché à l'écran.
  - *Amphiphone* : fonctionnement général de l'application.
  - *Audio* : volume, fichiers vocaux, etc.
  - *Hardware* : les appuis boutons, les entrées, les relais, etc.
  - *Ouverture porte* : commande d'ouverture de gâche.
  - *Réseau* : tout ce qui concerne le réseau.
  - *Utilisation* : utilisation générale de l'application.

Tableau 2.1. Exemple de tableau des événements système

Catégorie	Sévérité	Message
AMPHIPHONE	INFORMATIONAL	"Appel de : "+ Prenom + " " + nom
AMPHIPHONE	INFORMATIONAL	"Appel établi"
AMPHIPHONE	INFORMATIONAL	"Erreur appel"
AMPHIPHONE	INFORMATIONAL	"Appel terminé"
AMPHIPHONE	INFORMATIONAL	"Com de " + numéro
AMPHIPHONE	INFORMATIONAL	"Délai de réponse dépassé"
AMPHIPHONE	INFORMATIONAL	"Lancement de l'appel: " +numéro
AMPHIPHONE	INFORMATIONAL	"Lancement de l'appel: " +numéro
AMPHIPHONE	INFORMATIONAL	"Contact non autorisé : " + numéro
AMPHIPHONE	INFORMATIONAL	"Volume diminué"
AMPHIPHONE	INFORMATIONAL	"Volume augmenté"
AMPHIPHONE	ALERT	"Boitier ouvert"
AMPHIPHONE	INFORMATIONAL	"Démarrage de l'application"
AMPHIPHONE	INFORMATIONAL	"Initialisation"
AMPHIPHONE	INFORMATIONAL	"Premier Lancement"
AMPHIPHONE	INFORMATIONAL	"Configuration de la langue"
AMPHIPHONE	INFORMATIONAL	"Affichage de la configuration réseau"
AMPHIPHONE	NOTICE	"Mode liste de résidents"
AMPHIPHONE	NOTICE	"Mode étiquettes"
AMPHIPHONE	CRITICAL	"Relais 1 incompatible avec la configuration hardware"
AMPHIPHONE	WARNING	"Mauvais code local : " + codeLocalTmp
AMPHIPHONE	INFORMATIONAL	"Code résident local : ok"
AMPHIPHONE	NOTICE	"Code local, hors plage horaire"
AMPHIPHONE	INFORMATIONAL	"Code local : ok"
AMPHIPHONE	WARNING	"Mauvais code distant : "+ codeDistantTmp
AMPHIPHONE	INFORMATIONAL	"Code résident distant : ok"
AMPHIPHONE	INFORMATIONAL	"Code distant : ok"
AUDIO	INFORMATIONAL	Lecture de "Appel en cours"
AUDIO	INFORMATIONAL	Lecture de "Communication établie"
AUDIO	INFORMATIONAL	Lecture de "Appel terminé"
AUDIO	INFORMATIONAL	Lecture de "Appel en échec"
AUDIO	INFORMATIONAL	Lecture de "Appel suivant en cours"
AUDIO	INFORMATIONAL	"Lecture du fichier audio "Appel non autorisé"
AUDIO	INFORMATIONAL	Lecture : "Ouverture de la porte"
DISPLAY	INFORMATIONAL	Affichage de "Appel en cours"

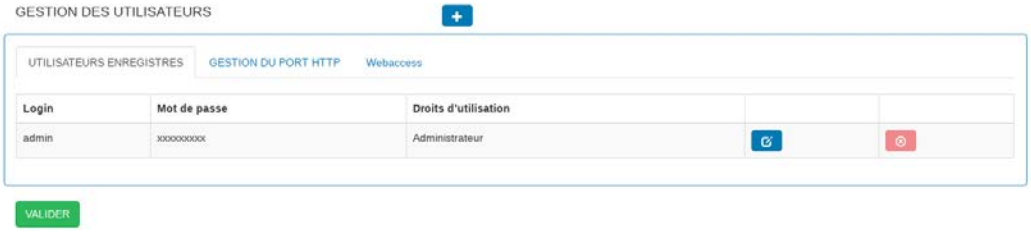
Catégorie	Sévérité	Message
DISPLAY	INFORMATIONAL	Affichage de "En communication"
DISPLAY	INFORMATIONAL	Affichage de "Appel en échec"
DISPLAY	INFORMATIONAL	Affichage de "Appel suivant en cours"
DISPLAY	INFORMATIONAL	Affichage de "Appel entrant"
DISPLAY	INFORMATIONAL	"Contact non autorisé : "+ nom
DISPLAY	INFORMATIONAL	"Mode recherche activé"
DISPLAY	INFORMATIONAL	"Mode recherche désactivé"
DISPLAY	INFORMATIONAL	"Affichage du mode code d'accès"
DISPLAY	INFORMATIONAL	"Affichage de la liste des résidents"
DISPLAY	INFORMATIONAL	"Affichage du mode numéro abrégé"
DISPLAY	INFORMATIONAL	Affichage "Ouverture de la porte"
HARDWARE	INFORMATIONAL	"Appui touche "up"
HARDWARE	INFORMATIONAL	"Appui touche "up"
HARDWARE	INFORMATIONAL	"Appui touche "down"
HARDWARE	INFORMATIONAL	"Appui touche "down"
HARDWARE	INFORMATIONAL	"Appui touche " * "
HARDWARE	INFORMATIONAL	"Appui touche "téléphone"
NETWORK	INFORMATIONAL	"IP :" + adresse IP
NETWORK	INFORMATIONAL	"Masque :"+ masque de sous reseau
NETWORK	INFORMATIONAL	"Broadcast :" + adresse de broadcast
NETWORK	INFORMATIONAL	"Passerelle :" + adresse IP passerelle
NETWORK	INFORMATIONAL	"Retour IP usine"
NETWORK	NOTICE	"Réseau Ok"
NETWORK	CRITICAL	"Problème réseau"
NETWORK	NOTICE	"Mise à jour de l'heure"
OPEN_DOOR	INFORMATIONAL	"Ouverture du relais, type : " + type
OPEN_DOOR	WARNING	"Ouverture non autorisé, relais désactivé"
OPEN_DOOR	INFORMATIONAL	"Fermeture du relais, type : "+ type
OPEN_DOOR	WARNING	"Ouverture non autorisé : voir master classe"
USE	EMERGENCY	"Problème de driver SQLite"
USE	EMERGENCY	"Problème d'ouverture base de données"
USE	EMERGENCY	"Problème table introuvable"
USE	INFORMATIONAL	"Appui sur le bouton : " + nom du bouton

- 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 VALIDER .

2.1.26. Gestion des utilisateurs locaux



- Cliquer sur + pour ajouter un nouvel utilisateur.
- Saisir le **Login**, le **Mot de passe** et définir les **Droits d'utilisation**, *Administrateur* ou *Utilisateur* :
- Dans l'onglet GESTION DU PORT HTTP , cocher la case pour activer la connexion automatique via HTTPS.

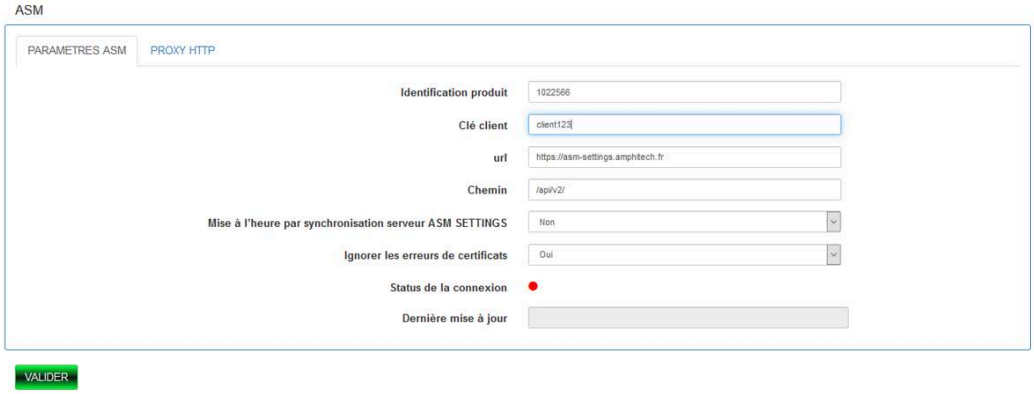
En mode utilisateur, seules les pages web suivantes sont visualisées :

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

Pour la partie WebAccess , voir 3.3.21.

2.1.27. Connexion au serveur ASM

2.1.27.1. Paramétrage du produit



Ce menu permet de se connecter à un serveur de provisionnig **ASM ACCESS** ou tiers (nécessite une connexion internet sur le réseau), en utilisant les API de gestion du produit développées par Amphitech :

- Notify.
- Events.
- Settings.

Ces requêtes permettent de :

- Mettre à jour un produit à distance (paramètres, logo, certificats radius...).
- Notifier la présence du produit.
- Activer le /les relais
- Etre informé des actions locales, de l'utilisation des codes clavier, de l'activation des relais, des appels sortants et entrants...

L'identification du produit vers le serveur utilise un modèle : Token / Id.

Les champs à remplir sont les suivants :

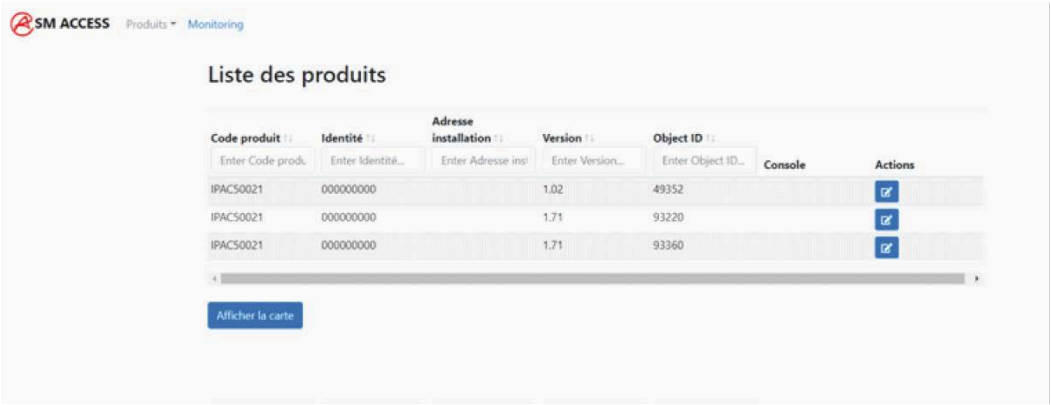
- Identification du produit : utiliser le numéro de série du produit.
- Clé client : identifiant du compte ASM ACCESS.
- URL : Adresse du serveur.
- Chemin : répertoire API Serveur.
- Mise à l'heure automatique par serveur ASM SETTINGS : Oui / Non
- Ignorer les erreurs de certificats SSL : Oui / Non
- Status connexion :
  - VERT : Connecté
  - ORANGE : Produit non activé sur le serveur
  - ROUGE: non connecté (identifiant, clé client ou adresse incorrects)
- Dernière mise à jour : horodatage de la dernière synchronisation des configurations avec le serveur.

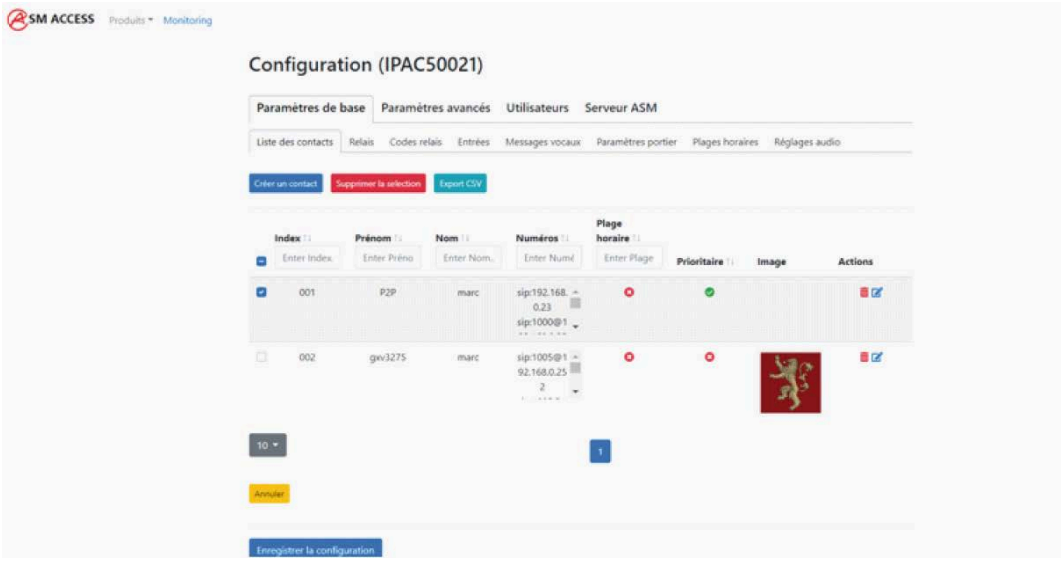
En cas d'utilisation d'un Proxy HTTP sur le réseau, utiliser les paramètres PROXY HTTP. Renseigner :

- Type de proxy.
- Adresse du serveur.
- Port.
- Login et Password si nécessaire.

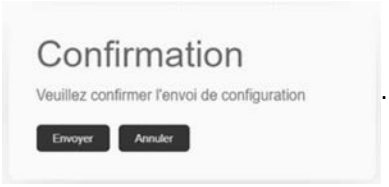
2.1.27.2. Connexion au serveur

Se connecter sur le serveur ASM ACCESS ou Créer un compte. Si les produits ont été correctement paramétrés, ils s'affichent dans la Liste des produits en « produit activé » ou « produit non activé ». Un « produit non activé » est en attente de validation (administrateur du compte).





Aprés modifications des paramètres, cliquer sur 

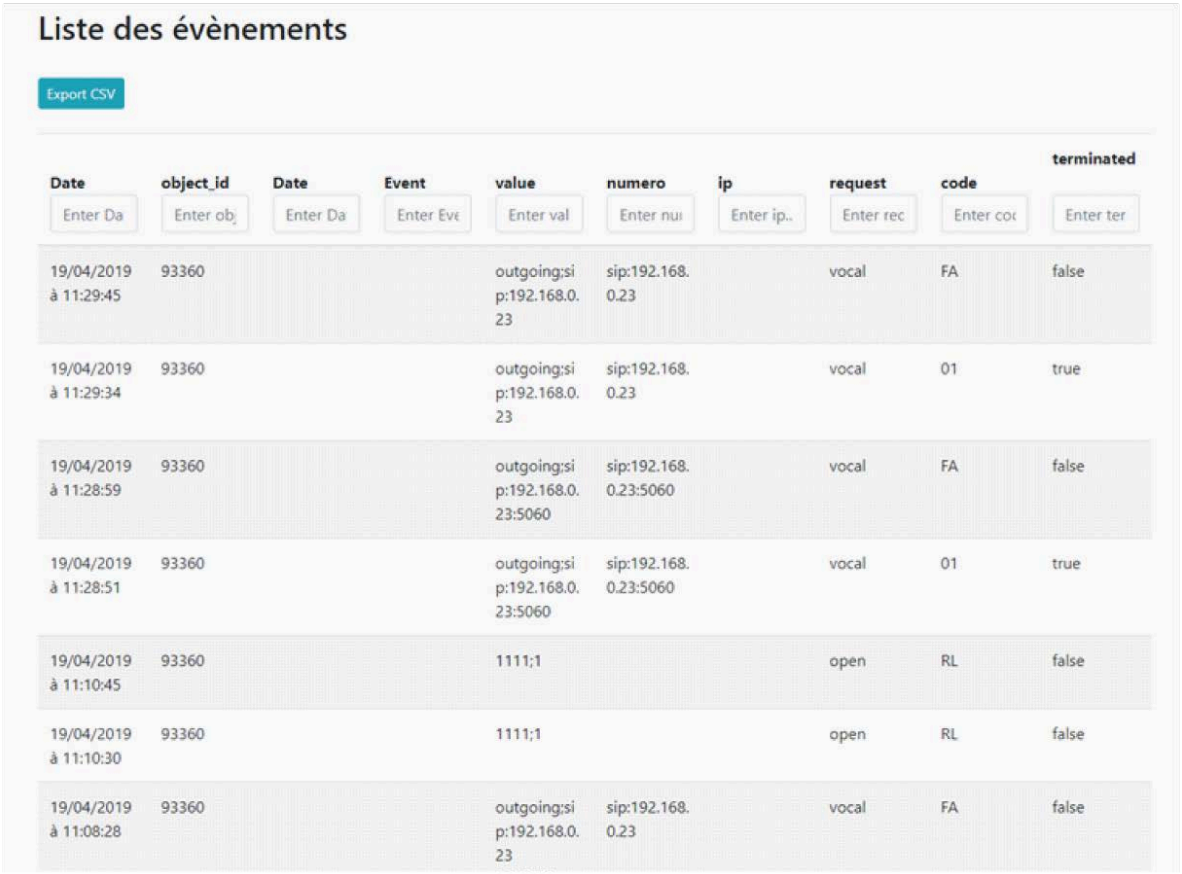
et confirmer ou non l'envoi de la configuration vers le produit 

.

A la fin de la mise à jour, un événement de redémarrage puis une alerte de mise à jour du produit avec la nouvelle configuration s'affichent :

Au redémarrage du produit, le produit renvoie ses paramètres au serveur pour vérification de synchronisation.

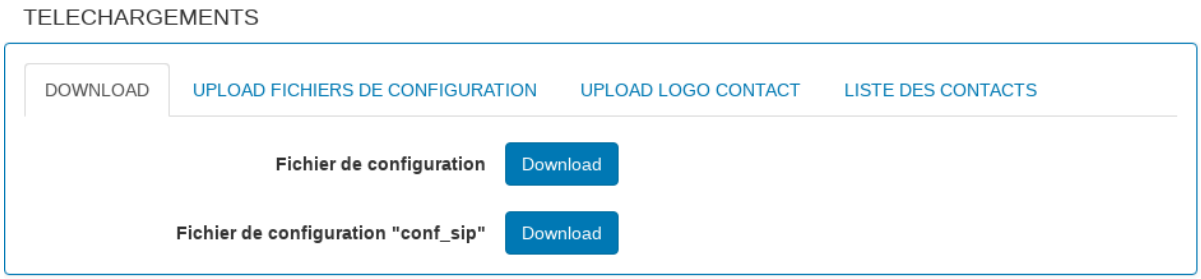
2.1.27.3. Monitoring des événements



Codes possibles `"event": "xx"`

Valeurs [xx]	Raison d'appel	request	value
01	Appel vocal sortant	Vocal ;incoming/outgoing	Num
0E	Redémarrage soft	Application	restarted
RL	Relais enclenché	open	Code ; num relais
CL	Code saisi localement au clavier	KeyBoard	code
FA	Fin d'appel vocal	Vocal ;incoming/outgoing	Num
ST	Début de stream vidéo vers ASM ACCESS	Stream ; incoming/outgoing	Adresse IP Num
FS	Fin de stream vidéo vers ASM ACCESS	Stream ; incoming/outgoing	Num

2.1.28. Téléchargements

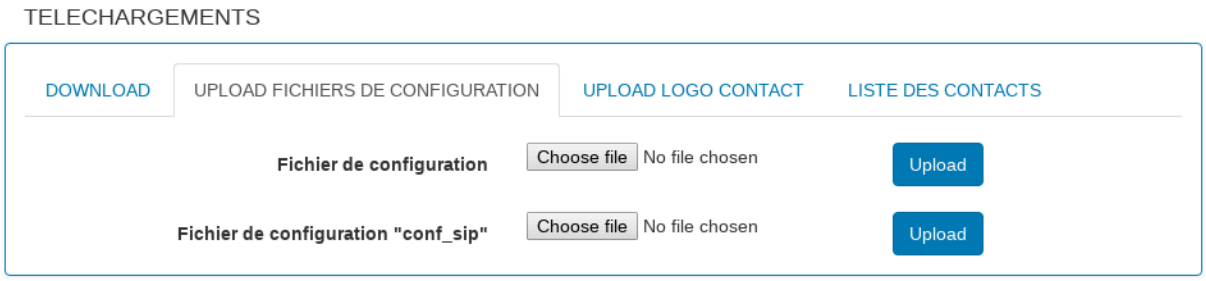


DOWNLOAD

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

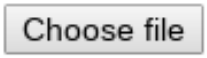
UPLOAD

UPLOAD FICHIERS DE CONFIGURATION



- Fichier de configuration **"conf_user"** : cliquer sur Choose file pour sélectionner le fichier de configuration d'un portier sauvegardé sur votre PC.
- Puis sur Upload pour sauvegarder le fichier de configuration sur le portier de votre choix (même référence de portier).
- Fichier de configuration **"conf_sip"** : cliquer sur Choose file pour sélectionner le fichier de configuration du serveur SIP sauvegardé sur votre PC.
- Puis sur Upload pour sauvegarder le fichier de configuration sur le portier de votre choix (même référence de portier).

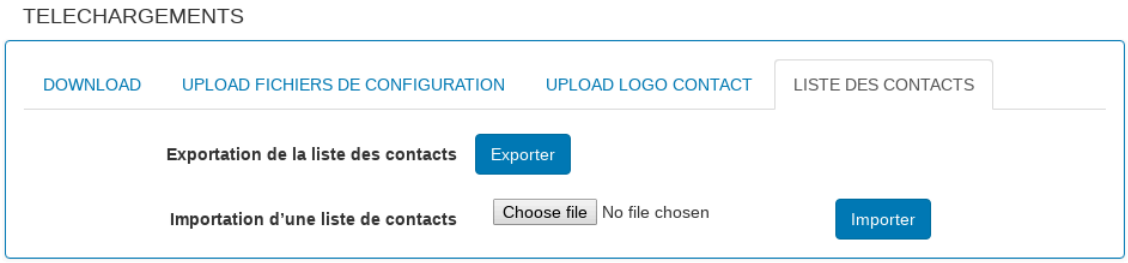
UPLOAD LOGO CONTACT

- Cliquer sur 

pour importer une image à associer à un résident.
- Cliquer sur 

pour sauvegarder l'image dans la mémoire de l'IPAC.
- Cliquer sur  pour supprimer une image sélectionnée dans la liste "Logo disponible"

LISTE DES CONTACTS



- Cliquer sur 

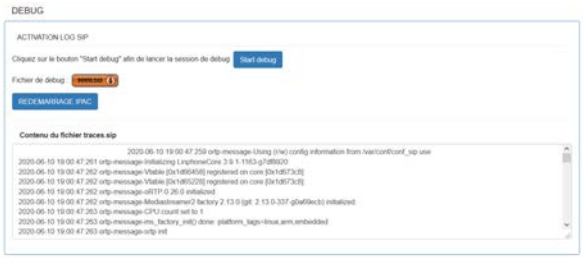
pour sélectionner la liste des contacts d'un portier sauvegardée sur votre PC (format CSV).
- Cliquer sur 

pour exporter une liste des contacts vers le portier de votre choix.
- Cliquer sur 

pour importer une liste des contacts à partir du portier de votre choix.

2.1.29. Debug

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



- Cliquer sur Start debug pour commencer le debug.
- Réaliser la manipulation qui entraîne le dysfonctionnement.
- Cliquer sur DOWNLOAD pour générer l'archive (fichier crypté) à envoyer à AMPHITECH pour analyse.

  Contenu des traces.sip : Log des traces sip (appels....) réalisés entre les appuis bouton start debug et bouton stop debug.

- Cliquer sur REDEMARRAGE IPAC pour redémarrer le portier.