



Zennio GetFace IP

Vidéo-portier IP (unité basique)

ZVP-CAM/ZVP-WOCAM

Édition du manuel : [2.32]_d
Version firmware 2.32

www.zennio.fr

SOMMAIRE

Sommaire	2
Actualisations du document	3
1 Introduction	5
2 Installation.....	7
2.1 Branchement du dispositif	7
2.2 Applications.....	10
2.2.1 Logement individuel.....	10
2.2.2 Immeuble d'appartement	11
3 Configuration.....	12
3.1 Configuration basique du Zennio GetFace IP.....	14
3.1.1 Configurations de réseau (Système)	15
3.1.2 Configuration de l'appel (Services)	16
3.1.3 Configuration des logements et unité intérieure (Répertoire)	24
3.1.4 Configuration d'interrupteurs	28
3.1.5 Configuration de la porte	30
3.1.6 Configuration des appels depuis le module de Boutons.....	34
3.1.7 Configuration du <i>tamper</i> anti-sabotage.....	34
3.1.8 Configuration d'accès avec l'écran tactile	35
3.1.9 Configuration de l'accès avec carte RFID	37
3.1.10 Configuration de l'accès avec module Bluetooth.....	40
3.1.11 Configuration de la boucle d'induction magnétique.....	47
3.2 Configurations avancées	47
3.2.1 État	47
3.2.2 Répertoire	50
3.2.3 Services.....	52
3.2.4 Hardware.....	58
3.2.5 Système	62

ACTUALISATIONS DU DOCUMENT

Version	Modifications	Page(s)
[2.32]_d	Changements en respect à l'application mobile d'accès avec le module Bluetooth.	
[2.32]_c	Indication sur la connexion à la terre sur le schéma de câblage.	
[2.32]_b	Indication sur la limitation de responsabilité par rapport à l'application ZenCom.	
[2.32]_a	<p>Changement dans l'emplacement des paramètres "Accepter appel entrant au moyen du bouton" et "Fonction du bouton pendant l'appel sortant" à l'onglet Services → Téléphone → Appels.</p> <p>Il s'élimine le paramètre "Destinataire prédéterminé" dans l'onglet E-mail → E-mail.</p> <p>Options du module Clavier inclus sur Services → Téléphone → Appels</p> <p>Changement dans la configuration d'authentification recommandée sur la API du système.</p> <p>Il s'élimine la section dédiée au module ZVP-FINGER (retiré du catalogue).</p> <p>Changements mineurs de texte.</p>	
[2.26]_a	<p>Possibilité de contrôle à distance à travers de l'application ZenCom.</p> <p>Changement dans la configuration recommandée sur la API du système.</p> <p>Bouton d'essai pour simuler un appel de marquage rapide.</p> <p>Recommandation sur l'actualisation du <i>firmware</i>.</p> <p>Possibilité de restaurer seulement certaines options de la configuration à télécharger une copie de sécurité.</p> <p>Corrections et changements mineurs.</p>	
[2.25]_a	<p>Écran → configuration du module de l'écran tactile avec icônes uniquement</p> <p>E-Mail → envoi automatique de e-mails devant des actions du système</p> <p>Option d'accepter des appels entrants au moyen du bouton de marquage rapide.</p>	

	<p>Augmentation de la sécurité grâce à l'option de choisir la version de LTS.</p> <p>Numéro virtuel de l'utilisateur → peuvent être des numéros d'entre 1 et 7 chiffres.</p> <p>Corrections et changements mineurs.</p>	
[2.24]_a	<p>Nouvelle structure de la section Répertoire → Utilisateurs. Jusqu'à 10.000 utilisateurs disponibles.</p> <p>Nouvelle structure de la section Écran → répertoire.</p> <p>Possibilité d'établir la localisation de l'utilisateur sur le répertoire dans la configuration de l'utilisateur. Groupes d'appel.</p> <p>Boutons de marquage rapide: appeler plusieurs utilisateurs.</p> <p>Possibiliter d'établir des profils de temps spécifiques (différents de ceux prédéfinis).</p>	
[2.23]_a	<p>Configuration du module lecteur d'empreintes digitales ZVP-FINGER</p> <p>Jusqu'à deux cartes par utilisateur pour accès au moyen du module ZVP-RFSMN.</p>	
[2.22]_a	<p>Nouvelle section pour la configuration de porte: Hardware / Porte.</p> <p>Corrections mineures.</p>	
[2.21]_a	<p>Rétablir l'état de la configuration prédéterminée.</p> <p>Éclaircissement sur le champ "Numéro de téléphone (ID)"</p> <p>Configuration de Automatisation.</p> <p>Configuration du courrier électronique d'accès.</p> <p>Configuration hardware du module ZVP-RFSMN</p> <p>Corrections mineures.</p>	
[2.20]_a	<p>Configuration du Module bluetooth.</p> <p>Configuration des cartes pour le module RFID depuis la section de Hardware.</p> <p>Corrections mineures.</p>	
[2.18]_b	<p>Changements mineurs de texte.</p>	

1 INTRODUCTION

Le **Zennio GetFace IP** est un visiophone (vidéo-portier) qui, en combinaison avec les écrans tactiles Zennio avec lesquels il est compatible (tels que le Z41 COM, Z70 v2, Z100, etc.), permet d'intégrer sur l'installation domotique la gestion d'**appels vidéo** entre la porte d'accès d'un environnement résidentiel (un immeuble d'appartements, une maison, une promotion urbaine avec porte d'accès commune, etc.) et l'intérieur des logements. Ou, en général, entre l'intérieur de n'importe quelle construction avec des caractéristiques analogues, comme, par exemple, un immeuble de bureaux, et sa porte d'accès.

De plus, à travers de l'application mobile **ZenCom** (*) (disponible pour Android et iOS) il est possible d'interagir avec le visiophone depuis n'importe quel lieu. Cette application permet de voir qui appelle à la porte, maintenir une conversation et inclure, ouvrir à distance depuis un dispositif mobile.

Les caractéristiques principales du Zennio GetFace IP sont:

- Caméra de résolution 1280x960 et émetteur IR pour les situations d'obscurité (modèle ZVP-CAM).
- Température de travail: Entre -40 et 60 °C.
- Humidité relative de travail: Entre 10 et 95%.
- Connecteur RJ-45 et compatibilité avec la norme Fast Ethernet.
- Permet une alimentation PoE (Power Over Ethernet) 802.3af – Classe 0 – 12.95W.
- Bouton de réinitialisation et indicateurs (jaune, rouge, vert).
- Sortie audio (Line Out).
- Sortie de relais NO/NF 30V/1A (AC/DC) pour les fonctions d'ouverture et de fermeture.

- Entrée active ou passive (-30 - 30VDC).
- Sortie active (8 ... 12VDC, I_{MAX}=400mA).
- Différents modes d'ouverture de porte.
- Contrôle à distance à travers de l'application ZenCom (*).

(*) LIMITATION DE RESPONSABILITÉ

Zennio informe à l'utilisateur de que le fonctionnement correct de ZenCom cela dépend de plusieurs facteurs parmi lesquels se distinguent les suivants:

- *ZenCom doit avoir toutes les autorisations demandées activées.*
- *ZenCom devra avoir activé un compte de l'utilisateur formée, au moins par un identificateur et un mot de passe facilité par Zennio.*
- *Les unités extérieures devront être paramétrées selon les exigences établies par Zennio (voir la documentation de chaque dispositif).*
- *Les unités extérieures doivent être enregistrées sur les serveurs ZenCom en utilisant les informations d'identifications fournies par Zennio spécifiques à chaque unité.*
- *Pour le fonctionnement correct du service, autant la(les) unité(s) extérieure(s) comme le (les) smartphones (s) doivent avoir accès à internet et il est nécessaire que ladite connexion ait au moins:*
 - *Un minimum de 10Mb/s de montée et de descente.*
 - *L'utilisation illimitées d'au moins, les protocoles et technologies suivants: SIP, SRTP, HTTPS, SDP, services de notification push de Google et Apple.*

Cependant, veuillez noter que certaines compagnies limitent certains des services requis nécessaires pour l'écosystème ZenCom. Dans ces cas, Zennio ne pourra pas se responsabiliser du fonctionnement correct de ZenCom, par conséquent, ils doivent être communiqués et gérés avec votre fournisseur de services internet. Ces limites peuvent se présenter sur n'importe quels réseaux sur lesquels se connectent les unités extérieures et les terminaux mobiles où se trouve installée l'application ZenCom.

En cas de doute, recueillir un maximum d'informations sur votre incident et contactez le service technique de Zennio (support@zennio.com).

2 INSTALLATION

2.1 BRANCHEMENT DU DISPOSITIF

Le Zennio GetFace IP dispose de différents modules optionnels qui peuvent être connectés de façon indépendante pour élargir la gamme des fonctions ou des caractéristiques du dispositif.

- Module de clavier (ZVP-KEYPAD),
- Module de 5 boutons (ZVP-NAME5),
- Écran tactile (ZVP-TOUCHD),
- Panneau d'information (ZVP-INFOP),
- Module lecteur de cartes d'accès RFID (ZVP-RFSMN),
- Module d'induction magnétique (ZVP-ILOOP),
- Module I/O (ZVP-INOUT).
- Lecteur de cartes RFID avec NFC (ZVP-RFSMN)
- Module Bluetooth (ZVP-BLUET).

Notes :

- *Après avoir connecté un module, il est nécessaire de réinitialiser le visiophone pour pouvoir accéder à sa configuration.*
- *Il est possible de vérifier à tout moment la connexion du module en accédant depuis l'interface web du produit à la rubrique Hardware → *Extendeurs* (voir les prochaines sections du document).*
- *Le vidéo-portier peut être alimenté par l'entrée d'alimentation externe de 12V ou au travers de l'entrée PoE.*
- *Si des problèmes d'accouplement du son sont observés durant l'appel, il est nécessaire de réaliser un filtre sur la réalimentation acoustique (voir section 3.2.4.1).*

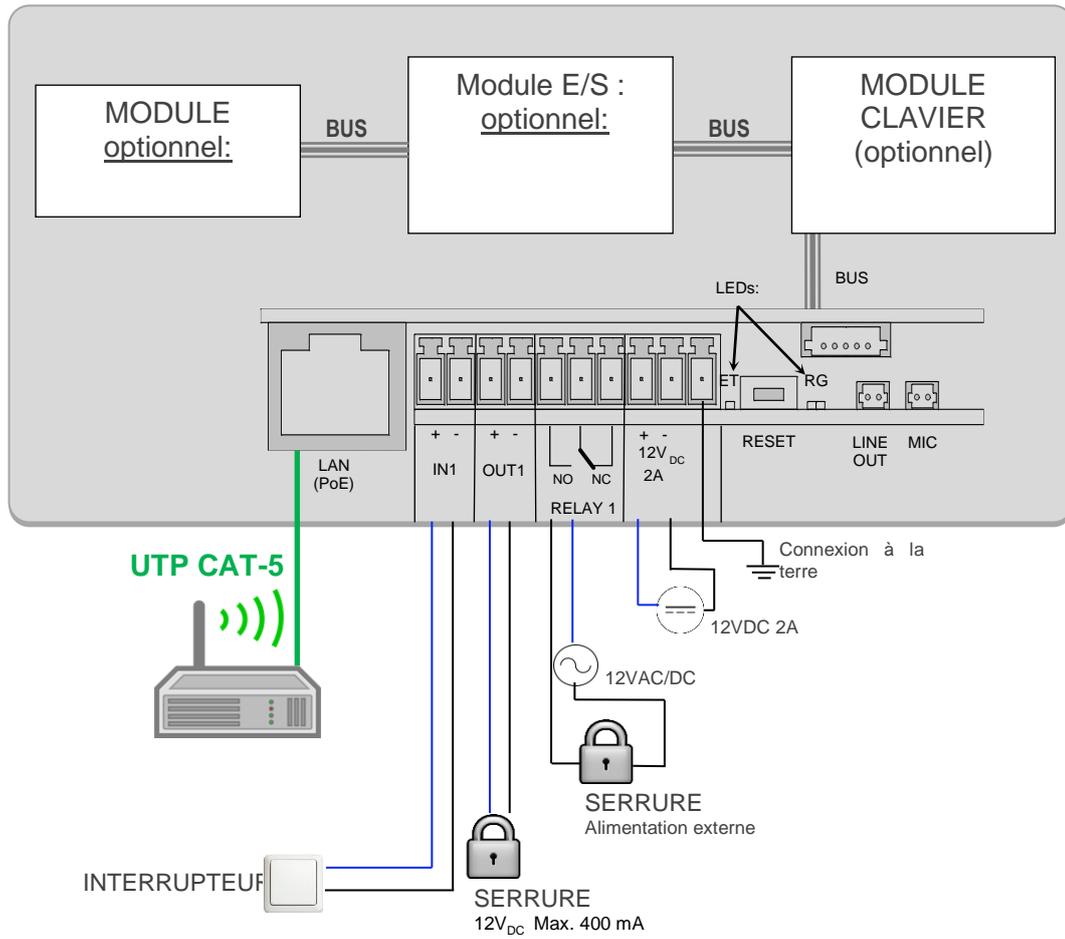


Figure 1 Câblage.

2.2 APPLICATIONS

Dans cette rubrique, les topologies de réseau les plus typiques pour l'installation du Zennio GetFace IP sont décrites.

2.2.1 LOGEMENT INDIVIDUEL

Pour un environnement résidentiel avec des logements individuels qui requièrent des systèmes totalement indépendants de visiophonie, l'installation typique sera une des 2 installations représentées dans la Figure 2, en fonction de si on désire interconnecter le Zennio GetFace IP et l'unité intérieure de Zennio directement ou bien à travers de la *box (router)* intérieur du logement (fourni, par exemple, par le fournisseur de l'accès à Internet) s'il y a lieu.

Si nécessaire, un *switch* qui augmente le nombre de connexions LAN disponibles de la *box (router)* peut être utilisé pour ainsi connecter plusieurs unités intérieures.

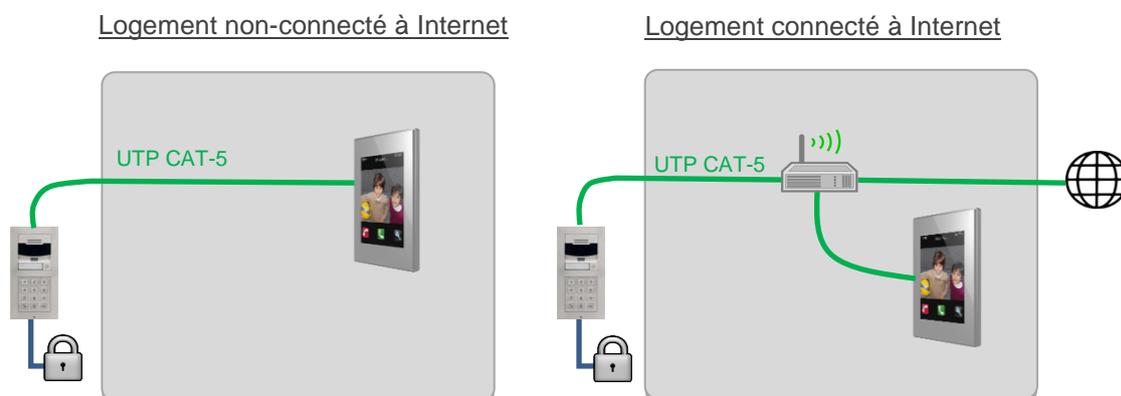


Figure 2 Installation dans un logement standard.

2.2.2 IMMEUBLE D'APPARTEMENT

Dans le câble d'un immeuble d'appartements avec un Zennio GetFace IP en commun, il faut utiliser une infrastructure en réseau communautaire (géré par un *router* coupe-feu) qui interconnecte le vidéo-portier avec chaque appartement. À leur tour, les appartements peuvent disposer ou non de leur propre box (*router*) de connexion à Internet.

La Figure 3 montre un exemple de ce type de topologie, dans laquelle on utilise l'étiquetage VLAN pour isoler le trafic entre les appartements.

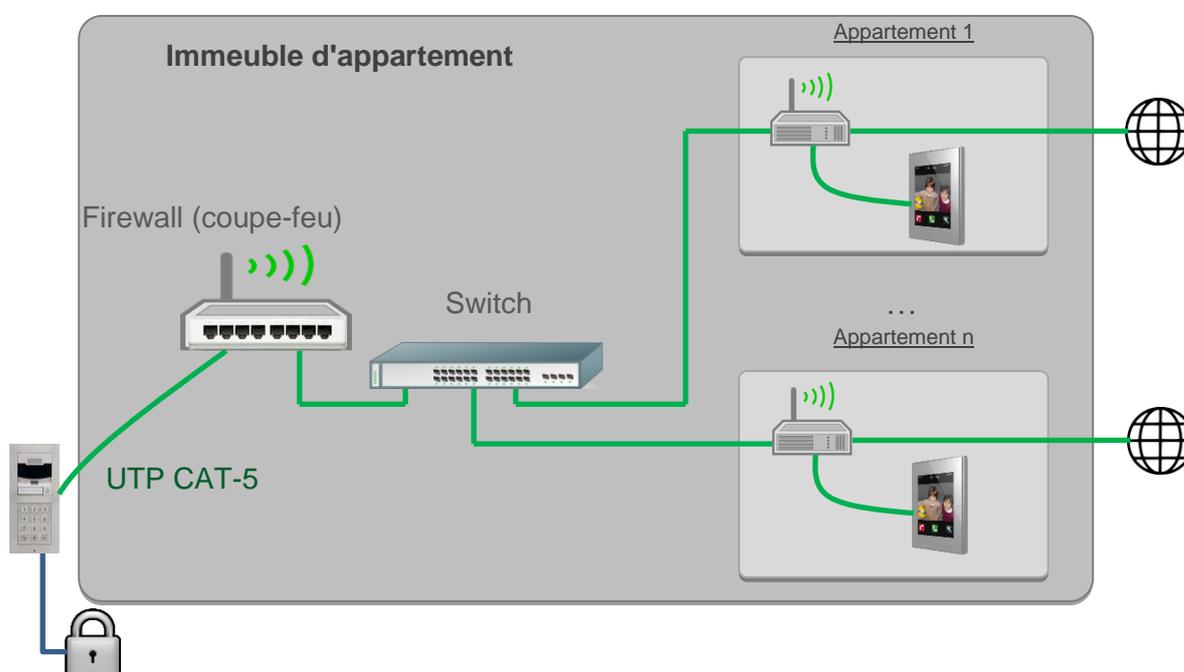


Figure 3 Installation dans un immeuble d'appartements.

Pour plus d'informations sur les caractéristiques techniques du dispositif, ainsi que sur les informations de sécurité et sur son installation, veuillez consulter le **document technique** inclu dans l'emballage original du dispositif, également disponible sur la page web. www.zennio.fr.

3 CONFIGURATION

Lorsque l'installation a été réalisée en tenant compte les applications expliquées dans la rubrique précédente, vous pouvez procéder à la configuration. La configuration a une série de paramètres nécessaires au bon fonctionnement de l'ensemble de GetFace IP avec l'unité intérieure de Zennio.

Durant les premières 30 secondes de fonctionnement (après avoir alimenté le visiophone), il faut **appuyer 5 fois le bouton de l'unité principale**, ce qui provoquera que **le dispositif annonce de vive voix son adresse IP**, au moyen de laquelle vous pourrez accéder à l'interface de configuration en utilisant un navigateur web. L'URL d'accès aura le format "**http://192.168.1.100**" (en supposant que l'IP du dispositif soit 192.168.1.100).

Par défaut, le visiophone est configuré pour fonctionner avec un serveur DHCP. S'il y a un problème de réseau ou s'il n'y a aucun serveur DHCP, le vidéo-portier prendra l'IP erronée 0.0.0.0.

Pour modifier la configuration de réseau du GetFace IP, **vous devez appuyer, rapidement, 15 fois le bouton de l'unité principale après le démarrage**, ce qui fera que le dispositif se réinitialise de nouveau automatiquement. À chaque réinitialisation, le dispositif alternera entre une IP dynamique (DHCP) et une IP statique (qui sera 192.168.1.100).

Lors de l'accès à l'interface web, **les données de session** sont sollicitées. Elles sont, **par défaut**:

- Nom d'utilisateur: **admin**
- Mot de passe: **zennio**

Note: Veuillez faire attention à bien différencier les majuscules et les minuscules.

Après le premier accès au dispositif, il est recommandé de **changer le mot de passe** depuis la rubrique **Services** → **Serveur web**. Le nouveau mot de passe devra avoir huit caractères, et inclure au moins une majuscule, une minuscule et un chiffre.

Voir l'aspect de la fenêtre principale dans la Figure 4.



Figure 4 Menu de configuration.

Notes:

- La langue par défaut de l'interface est l'anglais. Ce manuel, cependant, fera référence à la version en français.
- Au pied de chaque page de configuration, il existe un bouton pour sauvegarder les modifications réalisées. Si vous changez de page sans les sauvegarder, un message de confirmation apparaîtra pour sauvegarder ou rejeter les modifications faites.

3.1 CONFIGURATION BASIQUE DU ZENNIO GETFACE IP

À continuation, se décrit les champs les plus importants pour que le visiophone fonctionne avec l'unité intérieure de Zennio. Les paramètres qui doivent se changer en respect à la configuration par défaut, à mode de résumé, sont:

- **Numéro de TÉlÉphone (ID):** identificateur du visiophone (si on prétend l'associer avec une case concrète de l'unité intérieure de Zennio).
- **HTTP:** configuration de sécurité des services disponibles. Il peut y avoir jusqu'à 5 configurations différentes.
- **Numéro de téléphone de l'utilisateur:** Il devra contenir l'IP de chaque unité intérieure de Zennio.

Des précisions sur la façon de configurer ces champs sont indiquées dans les rubriques suivantes.

Notes:

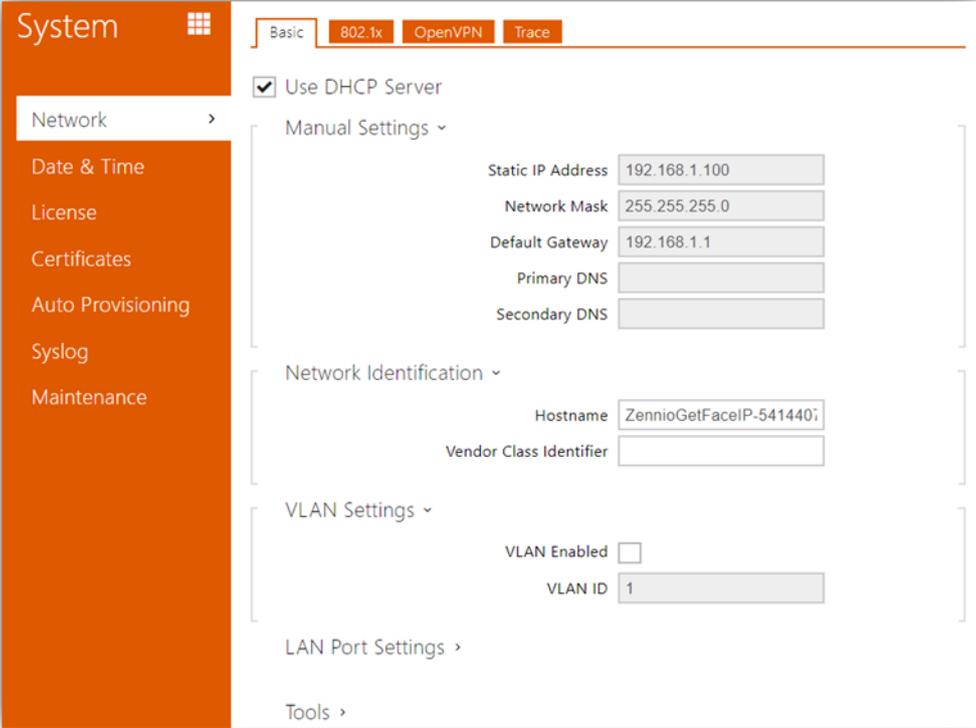
- *Les options qui ne sont pas mentionnées dans le présent document doivent être maintenues telles que par défaut.*
- *Les options qui affichent le symbole d'interdiction lorsque vous placez la souris dessus sont bloquées à cause des restrictions de licence.*
- *Il est possible de remettre le dispositif à ses valeurs de configuration prédéterminées ('hard reset'). Pour ce faire, deux options sont disponibles:*
 - *Appuyer pendant 30 secondes le bouton de reset de l'unité principale.*
 - *Depuis l'interface web, dans la section **système** → **Maintenance** → **Configuration** → **Rétablir l'état prédéterminé**.*

3.1.1 CONFIGURATIONS DE RÉSEAU (SYSTÈME)

L'onglet **Réseau** permet d'utiliser un serveur DHCP ou d'établir une configuration de réseau statique.

Note : Il existe des cas où il est obligatoire d'utiliser une IP statique:

- Dans un logement individuel avec le vidéo-portier directement connecté à l'unité intérieure du logement. Il est important de s'assurer que le masque de réseau des deux éléments est le même et que leurs IPs sont différentes, bien qu'appartenant au même rang.
- Lorsque le visiophone est dans un réseau différent de celui de l'unité intérieure de Zennio (selon le cas). Dans ce cas il sera nécessaire, en plus, d'activer dans le programme d'application de l'unité intérieure sur ETS le paramètre **L'unité extérieure est sur un réseau différent**, et introduire la même adresse IP fixe qui a été configuré sur l'interface web.



The screenshot displays the 'System' configuration page for a Zennio device. The left sidebar contains navigation options: Network, Date & Time, License, Certificates, Auto Provisioning, Syslog, and Maintenance. The main content area is titled 'System' and has tabs for 'Basic', '802.1x', 'OpenVPN', and 'Trace'. The 'Basic' tab is active, showing the following settings:

- Use DHCP Server
- Manual Settings:
 - Static IP Address: 192.168.1.100
 - Network Mask: 255.255.255.0
 - Default Gateway: 192.168.1.1
 - Primary DNS: (empty)
 - Secondary DNS: (empty)
- Network Identification:
 - Hostname: ZennioGetFaceIP-541440
 - Vendor Class Identifier: (empty)
- VLAN Settings:
 - VLAN Enabled:
 - VLAN ID: 1
- LAN Port Settings: (empty)
- Tools: (empty)

Figure 5 Système.

3.1.2 CONFIGURATION DE L'APPEL (SERVICES)

3.1.2.1 TÉLÉPHONE

Dans cet onglet les fonctions basiques de l'appel vidéo:

SIP

SIP est un protocole de transmission utilisé pour la téléphonie IP. Vous pouvez établir jusqu'à 2 profils SIP. Chaque profil doit être configuré en adéquation avec le réseau de travail. Les paramètres suivants de configuration permettent à l'unité extérieure de Zennio de se connecter avec le Zennio GetFace IP.

- **Identifiant de l'interphone:** paramètres de configuration qui définissent le profil du vidéo-portier. Voir section 3.1.3.1.
 - **Nom d'affichage:** nom identifiant le vidéo-portier et qui apparaîtra dans la page initiale de l'interface web.
 - **Numéro de téléphone (identifiant):** identificateur alpha-numérique du vidéo-portier. Cette valeur devra coïncider avec le paramètre ETS **ID du visiophone** de la case de l'unité intérieure de Zennio avec lequel vous voulez associer le visiophone. Ce champ est obligatoire dans le cas où l'unité extérieure et intérieure sont sur différents réseaux. Il sera aussi nécessaire dans le cas de vouloir différencier plusieurs visiophones sur différentes cases d'une même unité intérieure.

Notes:

- Le champ **Afficher le nom** n'admet pas les caractères > ni <.
- Le champ **Numéro de téléphone (identifiant)** aura une valeur alphanumérique de 10 caractères maximum. *Il n'admet pas non plus les caractères @ · ni d'autres types de caractères spéciaux, même si les caractères de ponctuation basiques sont permis.*

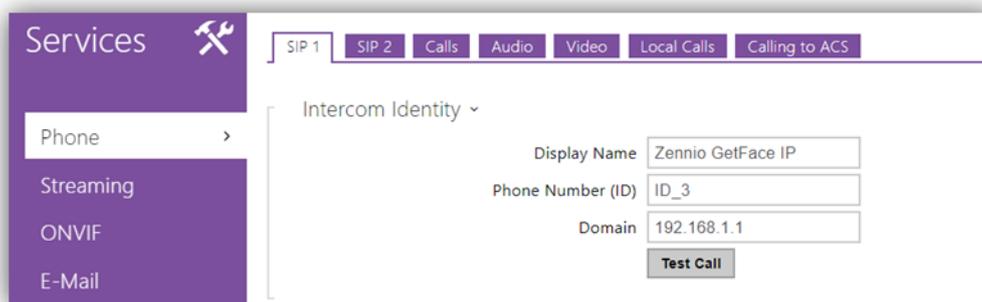


Figure 6 SIP

APPELS

L'onglet **Appels** permet de configurer les paramètres concernant les appels.

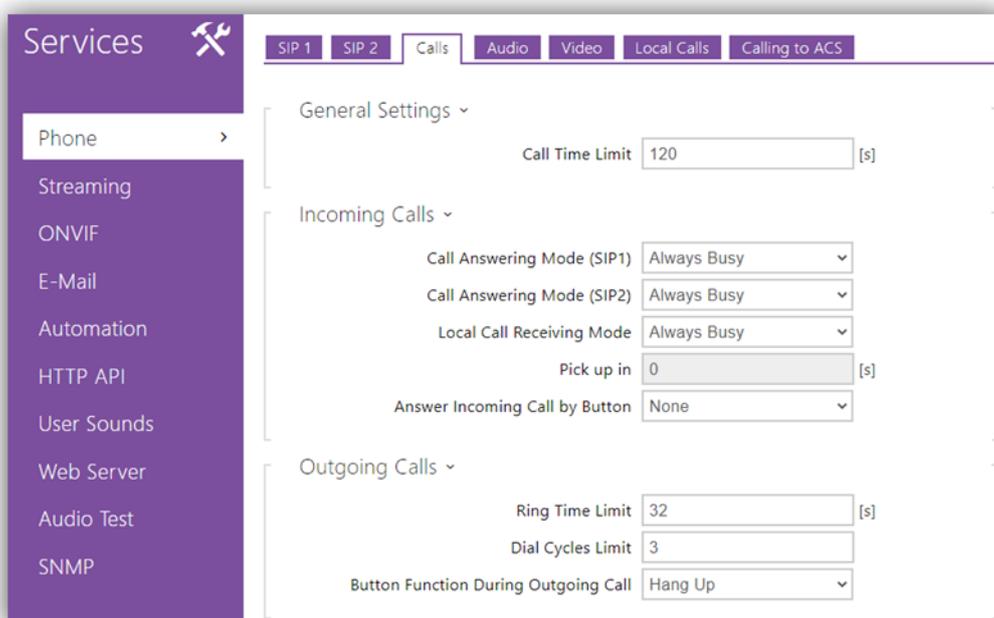


Figure 7 Appels.

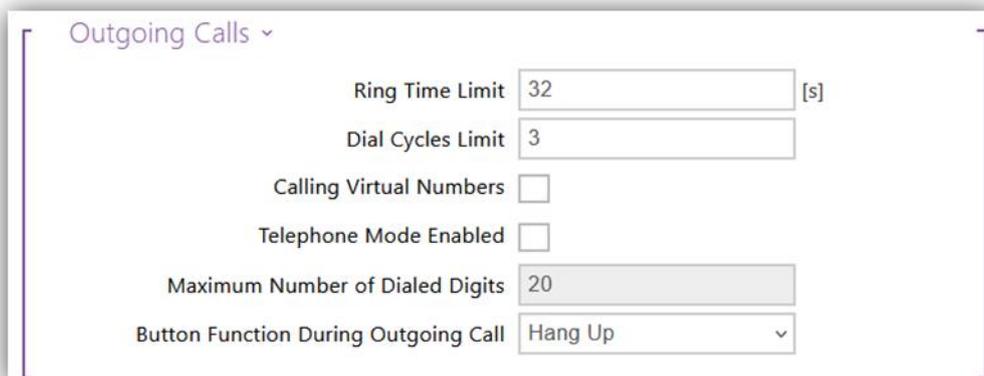
En premier lieu, sur **Options générales** il est possible de configurer un **temps limites d'appel**, lequel définit la durée de l'appel. Passé ce temps, l'appel se coupera automatiquement. Le Zennio GetFace IP avertira de la fin de l'appel en émettant un bip 10 secondes avant de couper. Dans ce cas, l'appel pourra être prolongé en appuyant simplement sur un bouton de l'écran tactile (ZVP-TOUCHD) ou du module de clavier (ZVP-KEYPAD), s'ils ont été configurés.

Dans la rubrique **Appels entrants** vous pourrez paramétrer la réponse du vidéo-portier lors d'un appel entrant. Parce que les appels se produisent en général dans une seule direction, ce paramètre aura par défaut la valeur "Toujours occupé". Il se permet aussi d'accepter des appels entrants au moyen du bouton de marquage rapide choisit. S'il a été choisit 'Aucun' cette fonctionnalité est désactivée.

Dans la rubrique **Appels sortants** vous définirez les durées des appels sortants:

- La **Limite de durée de la sonnerie** est le temps maximum que l'appel durera sans qu'il y ait de réponse. Il est conseillé que cette limite soit supérieure à 20 secondes.
- La **limite de cycles d'appel** sert à éviter que l'appel se bloque lorsque l'utilisateur n'est pas joignable et son substitut ai le même numéro de téléphone dans le répertoire téléphonique.
- **Fonction du bouton pendant l'appel**: définit la fonction du bouton de marquage rapide durant l'appel. Cela ne concerne que le bouton au moyen duquel vous avez initié l'appel. Il est recommandé de configurer ce bouton de façon à ce qu'il n'ait aucune fonction durant l'appel pour éviter de raccrocher l'appel par erreur.

De plus, si se connecte le module de clavier, il apparaît deux options supplémentaires:



The screenshot shows a configuration window titled "Outgoing Calls" with a dropdown arrow. It contains the following settings:

Ring Time Limit	32	[s]
Dial Cycles Limit	3	
Calling Virtual Numbers	<input type="checkbox"/>	
Telephone Mode Enabled	<input type="checkbox"/>	
Maximum Number of Dialed Digits	20	
Button Function During Outgoing Call	Hang Up	▼

Figure 8 Appels – Options avec le module de clavier.

- **Appel aux numéros virtuels:** permet d'appeler les utilisateurs du répertoire téléphonique en pianotant son numéro virtuel.
- **Mode téléphonique habilité:** permet de faire des appels aux numéros de téléphone marqués au moyen du clavier numérique.

AUDIO

L'onglet **Audio** contient les paramètres de configuration de la sortie audio. Cet onglet contient les rubriques suivantes:

- **Codecs audio: Services → Téléphone → Audio.** Il est souhaitable d'assigner la priorité maximale au codec G.722, tel qu'indiqué dans la Figure 9.

CODEC	ENABLED	PRIORITY
PCMU	<input checked="" type="checkbox"/>	2
PCMA	<input checked="" type="checkbox"/>	3
L16 / 16 kHz	<input type="checkbox"/>	4
G.729	<input type="checkbox"/>	5 (lowest)
G.722	<input checked="" type="checkbox"/>	1 (highest)

Figure 9 Audio.

● **Paramètres de qualité de transmission:**

- **Valeur de la qualité du service DSCP (QoS):** définit la priorité des paquets RTP dans le réseau. La valeur établie sera envoyée dans le champ ToS (type de service) de l'entête du paquet IP.
- **Compensation du jitter:** définit la capacité du buffer (mémoire tampon) pour compenser l'effet *jitter* dans la transmission des paquets audio. Plus la capacité est grande, meilleure sera la robustesse de la transmission. Nonobstant, le retard du son pourra aussi être plus grand.

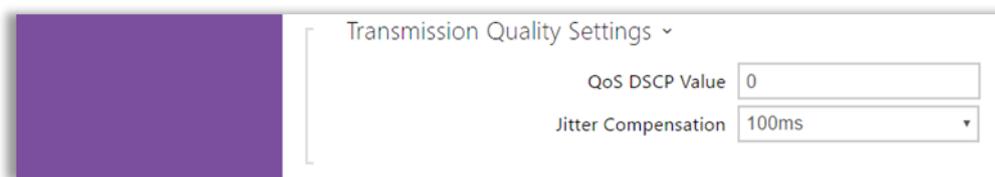


Figure 10 Paramètres de qualité de transmission.

VIDÉO

L'onglet **Vidéo** contient les paramètres de configuration de la sortie vidéo.

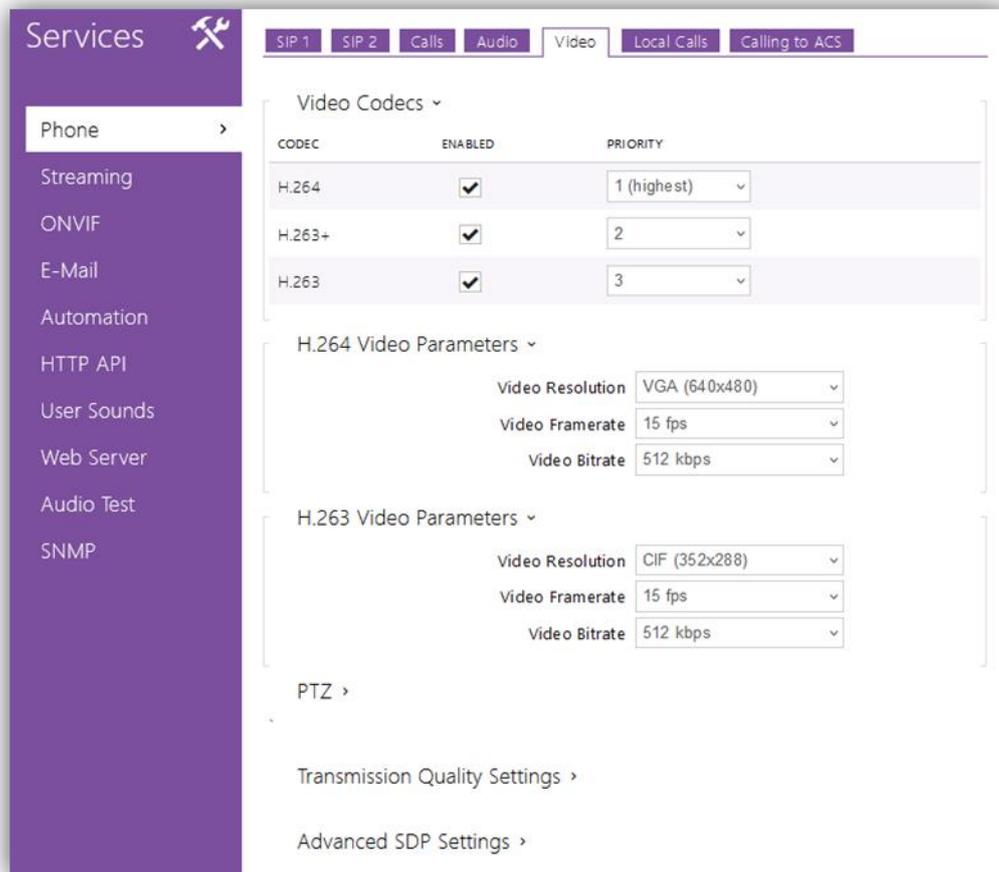


Figure 11 Vidéo.

- **Codecs vidéo**: pour améliorer la fluidité de la source vidéo, il est recommandé de changer la résolution vidéo H.264. Cette modification peut être réalisée dans **Services** → **Téléphone** → **Vidéo** comme on peut l'observer dans la Figure 11:

3.1.2.2 HTTP API

Cette rubrique permet de contrôler les fonctions IP via HTTP.

SERVICES

Cet onglet permet la configuration des services, le protocole de transport et le mode d'authentification pour chaque service (pour configurer les services avancés, voir la section 3.2.3). De plus, il sera nécessaire de paramétrer l'**API¹ de système**, l'**API d'interrupteur** et l'**API de caméra**.

Pour ce faire, ces paramètres doivent être configurés comme indiqué ci-après, dans **Services → API HTTP → Services**.

- **API de système:** "Protégé (TLS)" et avec authentification "Digest".
- **API d'interrupteur:** "Protégé (TLS)" et avec authentification "Digest".
- **API de caméra:** "Non-protégé (TCP)". Si on veut pouvoir utiliser une prévisualisation de la caméra, il est nécessaire de paramétrer l'authentification comme "Aucun".

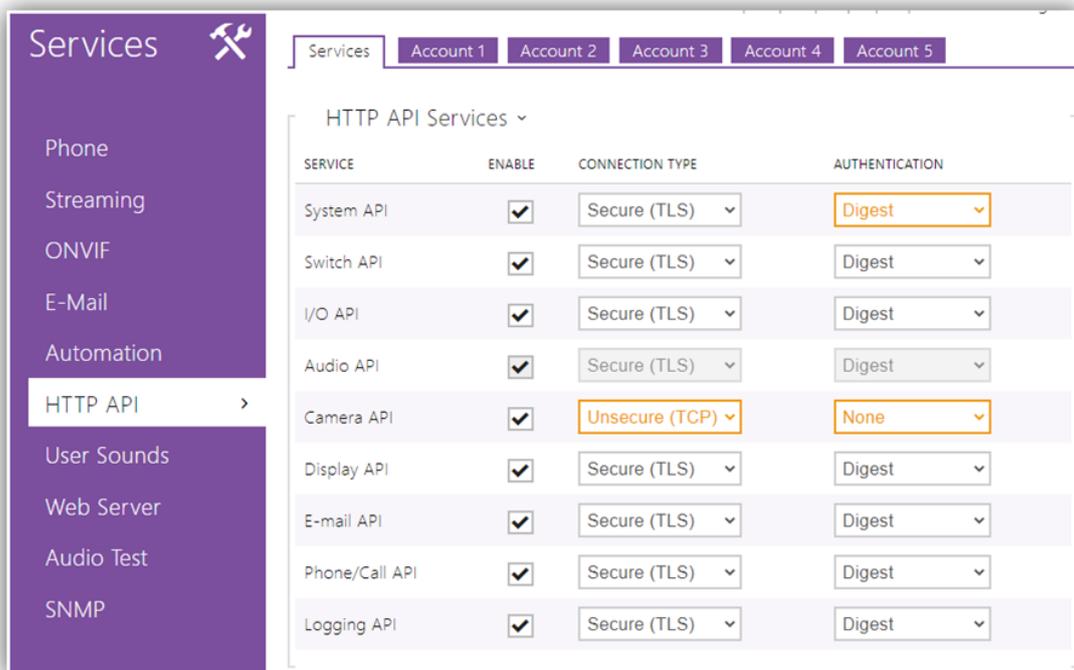


Figure 12 Services API HTTP.

¹ API: *Application Programming Interface*.

COMPTE

Les onglets **Compte n** permettent d'établir des profils de configuration d'utilisateur qui restreignent certaines actions au moyen des données d'utilisateur et mot de passe. On peut établir au maximum cinq comptes avec utilisateur et mot de passe et appliquer des privilèges d'accès, que ce soit un accès de surveillance et/ou de contrôle. Ces comptes permettent d'avoir un plus grand niveau de sécurité, car ils exigent une authentification avec l'unité intérieure de Zennio.

Si l'unité intérieure est configurée sous ETS avec un nom d'utilisateur et un mot de passe au travers du paramètre **Méthodes d'ouverture**, il faudra établir une configuration analogue dans l'onglet **Comptes** pour permettre l'ouverture de la serrure.

Il faudra aussi activer la case **Accès à l'interrupteur**. Dans le cas contraire la communication entre les dispositifs n'aura pas lieu. Si on n'utilise pas cette configuration, les champs d'utilisateur et mot de passe devront rester en blanc dans les deux dispositifs.

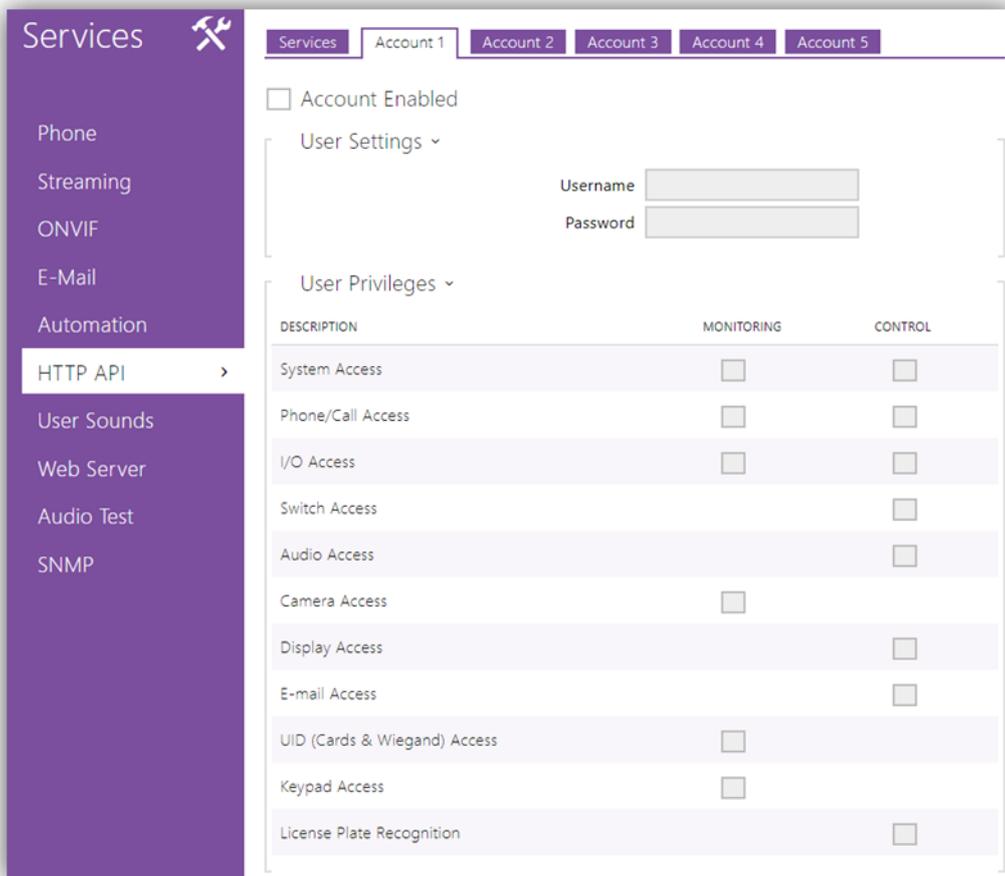


Figure 13 Compte API HTTP.

Note : La limite de la taille autant pour l'utilisateur comme pour le mot de passe est de 10 caractères. Cette limite est donnée par les champs d'ETS correspondants dans l'unité intérieure de Zennio, qui sont limités à 10 bytes (y compris les caractères spéciaux qui occupent plus de 1 byte, dans ce cas il est possible que se permettent moins de 10).

3.1.3 CONFIGURATION DES LOGEMENTS ET UNITÉ INTÉRIEURE (RÉPERTOIRE)

Dans le menu **Répertoire**, les logements connectés au vidéo-portier seront configurés. Il sera possible de configurer les onglets suivants:

3.1.3.1 UTILISATEURS

Dans **répertoire**→**Utilisateurs** il faut créer, au minimum, autant d'utilisateurs comme de logements susceptibles d'être appelés depuis le visiophone. Il est possible de créer jusqu'à 10 000 utilisateurs.

Dans chacun d'eux, le **Numéro de téléphone** correspondant à l'IP de l'unité intérieure Zennio associée doit être défini.

Pour le même utilisateur, il sera possible d'activer autant de numéros de téléphone d'utilisateurs qu'il y a d'unités intérieures dans l'appartement, en activant pour ce faire la fonction **Appel en parallèle au numéro suivant**.

Si un logement dispose de plus de trois unités intérieures de Zennio, on pourra réaliser des appels en parallèle à tous si plus d'un utilisateur est défini par logement. Dans ce cas, non seulement il faudra activer la fonction **Appel en parallèle au numéro suivant**, mais aussi la fonction **Appel en parallèle du délégué suivant**. En résumé, un logement peut avoir plusieurs utilisateurs assignées, mais toutes les unités intérieures d'un utilisateur doivent appartenir au même logement.

Exemple :

Le **format** doit être:

• **Sip**: *identifiant_non_pertinent@IP_de_unité_intérieur_Zennio*

Un exemple valable serait: **sip:555@192.168.1.101**, en supposant que 192.168.1.101 est la direction IP de l'unité intérieure.

Note : Si on ajoute un clavier numérique au vidéo-portier (ZVP-KEYPAD) ou un écran tactile (ZVP-TOUCHD), dans le champ **Numéro virtuel** on indiquera le numéro à marquer depuis le clavier pour faire l'appel.

Pour accéder à la configuration de chaque utilisateur, il faut les ajouter individuellement en appuyant sur le bouton , après lequel la page se charge pour remplir les données de l'utilisateur:

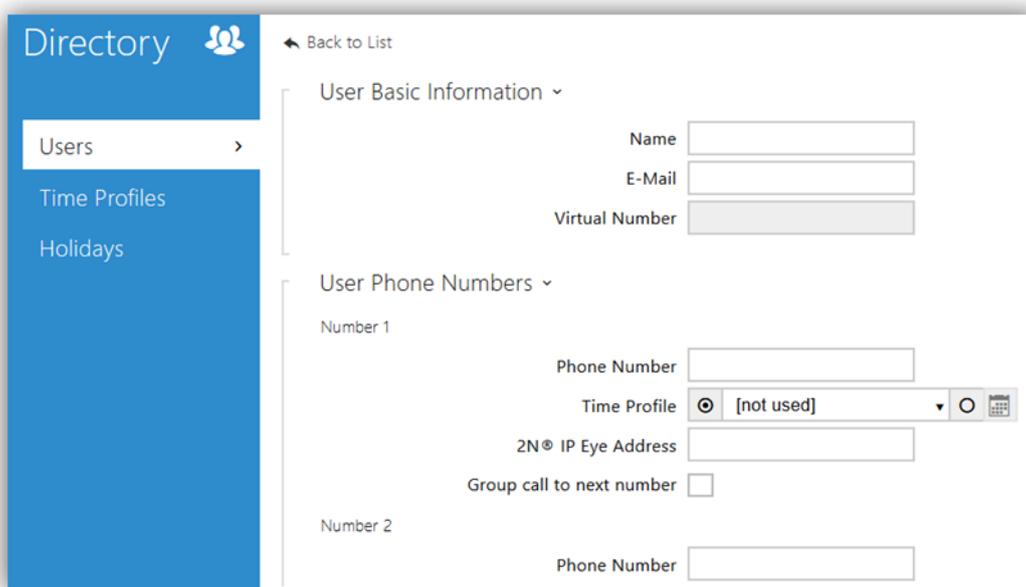


Figure 14 Utilisateurs.

Dans l'onglet **Utilisateurs**, les paramètres suivants sont définis:

- **Nom**, qui identifie le logement ou le propriétaire.
- **Photographie**: seulement disponible si le module Touch Display est connecté (ZVP-TOUCH).
- **E-mail** mail électronique de contact (optionnel; voir section 3.2.3.1).
- **Numéro virtuel**: numéro qui sera utilisé pour appeler l'utilisateur au moyen du clavier numérique. Il doit avoir entre 1 et 7 chiffres. Seulement pour le module ZVP-KEYPAD ou pour le module tactile display (ZVP-TOUCHD).

Note : ce champ est activé tant que l'option "appel vers des numéros virtuels" dans l'onglet de Services → Téléphone → Appels (voir section 3.1.2.1).

- **Ajout à l'écran:** uniquement pour le module Touch Display (ZVP-TOUCH).
 - **Localisation dans le répertoire:** établit le dossier dans lequel va se trouver l'utilisateur sur l'écran Touch Display. Peuvent se créer jusqu'à quatre sous dossiers.
 - **Groupe d'appel:** nom du groupe qui apparaîtra sur l'écran Touch Display. À appuyer sur le nom du groupe, il se réalisera un appel à tous les utilisateurs du groupe en même temps.

- **Liste des numéros de téléphone de l'utilisateur:**
 - **Numéro de téléphone:** chaîne de caractères avec le format décrit plus haut.
 - **Profil horaire:** fourchette des heures auxquelles la réception d'appels est permise. Il est possible de choisir un profil de ceux prédéfinis (voir section 3.2.2.1) ou en établir un spécifique en sélectionnant le bouton sur la gauche du calendrier.
 - **Appel en parallèle au numéro suivant:** case à activer si on souhaite appeler un autre numéro en parallèle (c'est-à-dire, s'il y a plusieurs unités intérieures Zennio dans le même logement).
 - **Remplaçant de l'utilisateur:** utilisateur auquel les appels doivent être redirigés dans le cas où l'utilisateur actuel n'est pas disponible. De plus, si on active la fonction **Appel en parallèle du délégué suivant**, l'appel sera dirigé en parallèle vers l'utilisateur et le remplaçant. Cette option peut être utilisée lorsqu'il existe plus de trois unités intérieures dans le même logement.

- **Réglage de l'accès:** (simple par défaut) permet de combiner des cartes RFID avec des codes d'accès pour ouvrir la porte (uniquement avec les modules ZVP-KEYPAD, ZVP-RFSMN ou ZVP-TOUCHD). Peuvent être établis des profils de temps pour ce type d'accès, différents pour chaque sens (entrée ou sortie).

- **Codes de l'utilisateur:** code privé de l'utilisateur pour l'ouverture de l'interrupteur. Plusieurs profils horaires peuvent être définis pour limiter son utilisation. Seulement pour le module ZVP- KEYPAD..

Note : *l'interrupteur correspondant doit être activé dans **Hardware** → **Interrupteurs** (voir section 3.1.4).*

- **Cartes de l'utilisateur:** Identifiant de la carte d'accès de l'utilisateur et profil horaire qui sera activé. Il est permis deux cartes par utilisateur. Seulement pour le module ZVP- RFSMN. Voir section 3.1.9.

3.1.4 CONFIGURATION D'INTERRUPTEURS

Dans **Hardware** → **Interrupteurs** il est possible de configurer l'ouverture de serrures électriques associées au Zennio GetFace IP pour pouvoir les contrôler depuis l'unité intérieure de Zennio (jusqu'à trois serrures électriques). Pour la connexion de la serrure au Zennio GetFace IP veuillez voir la section 2 et le document technique du dispositif.

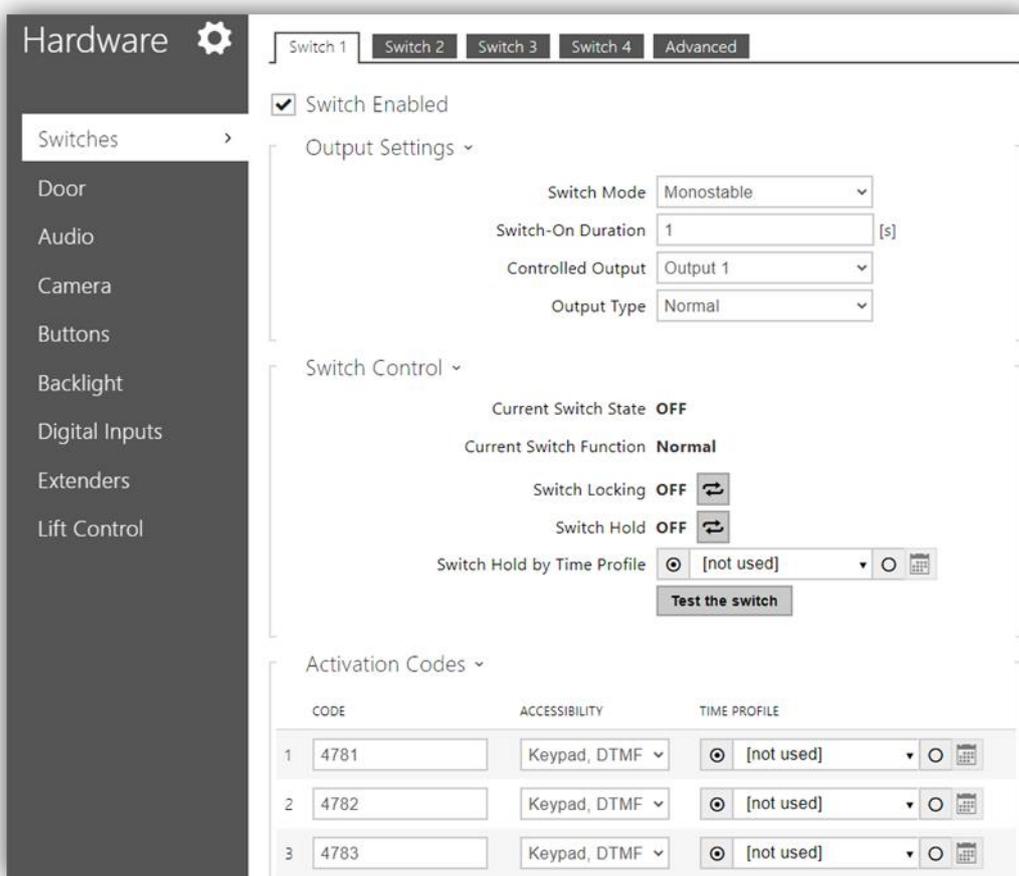


Figure 15 Interrupteurs.

En ce qui concerne la configuration, il est nécessaire de cocher la case d'activation de l'interrupteur située dans la partie supérieure de la page, puis de paramétrer les options de la page en fonction de la serrure dont vous disposez.

- **Paramètres de base** des interrupteurs:
 - **Mode des interrupteurs:** permet de choisir le type d'ouverture (**monostable**, s'il doit se désactiver automatiquement après un certain temps; ou **bistable**, s'il doit se désactiver manuellement).
 - **Durée d'enclenchement:** retard pour l'interrupteur monostable.
 - **Sortie Contrôlée:** on peut choisir s'il s'agit d'un relais ou d'une sortie électrique. En cas de sélection de l'option Aucun, l'interrupteur pourra être contrôlé avec des commandes HTTP.
 - **Type de sortie:** le fonctionnement de la sortie peut être sélectionné entre les types suivants:
 - **Normal:** on active la sortie pour réaliser l'ouverture.
 - **Inverse:** on désactive la sortie pour faire l'ouverture.
 - **Sécurité:** la sortie fonctionne de façon inversée mais on dispose d'un relais de sécurité contrôlé au moyen d'une séquence d'impulsions spécifique (il faut utiliser le module ZVP-ACSR).
 - **Profil horaire** qui sera appliqué à l'interrupteur. Il est possible de choisir l'un des préfixes (voir section 3.2.2.1) ou un spécifique.
- **Codes d'activation:** codes qui permettront d'activer les interrupteurs depuis le clavier (si on dispose des modules ZVP-KEYPAD ou ZVP-TOUCHD). On peut leur appliquer des profils horaires d'activation des codes (voir section 3.2.2.1).
 - **Distinguer les codes d'activation/désactivation**, dans le cas des interrupteurs bistables.
- **Synchronisation:** active la synchronisation des interrupteurs de sorte que, lorsque l'un d'eux est activé, après un retard paramétrable, un autre interrupteur soit activé.

3.1.5 CONFIGURATION DE PORTE

Dans **Hardware** → **Porte** se regroupe la configuration des paramètres pour la gestion de l'ouverture de la porte et les règles d'accès.

PORTE

Dans cet onglet se configurent des aspects généraux de la porte, qui s'appliqueront toujours, sans différencier entre accès d'arrivée ou de sortie.

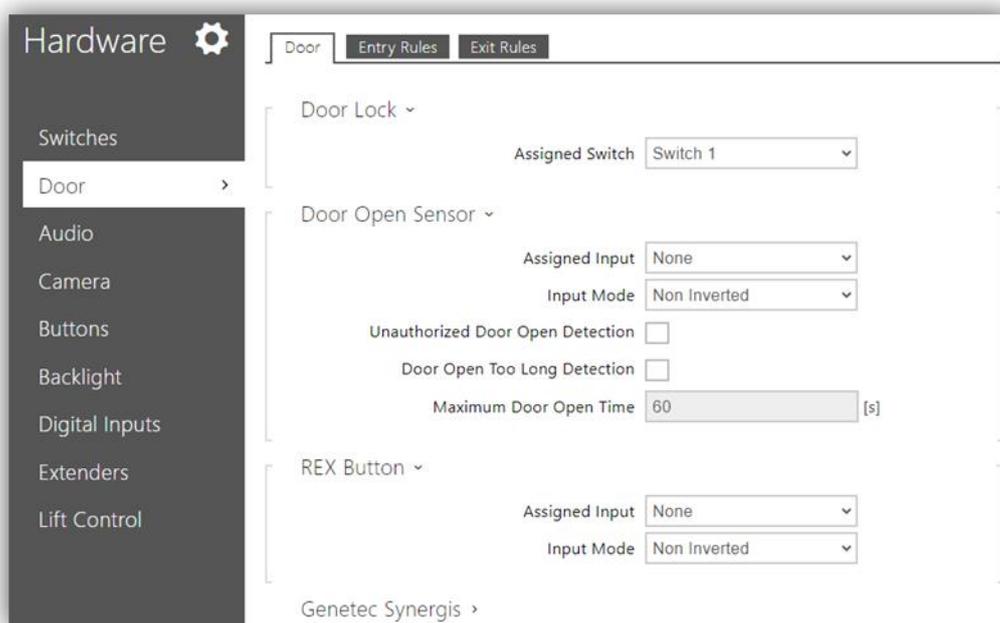


Figure 16 Porte.

- **Fermeture de la porte:** se désigne l'interrupteur à contrôler. La configuration de cet interrupteur s'explique dans la section suivante.
- **Capteur d'ouverture de la porte:** établit une entrée pour visualiser l'état de la porte. Il est possible de détecter une ouverture non autorisée de la porte ainsi qu'une ouverture prolongée (le temps limite est paramétrable).
- **Bouton de sortie REX,** on définit quelle entrée du GetFace IP sera utilisée comme bouton de sortie, de sorte que la sortie associée à la porte sera activée lorsque cette entrée est activée. Cette fonction peut être intéressante si on désire avoir un bouton poussoir intérieur qui puisse agir sur l'ouverture de la porte.

RÈGLES POUR ENTRER / SORTIR

Dans ces deux onglets se configurent les mêmes paramètres, en différenciant si l'accès est d'arrivée ou de sortie.

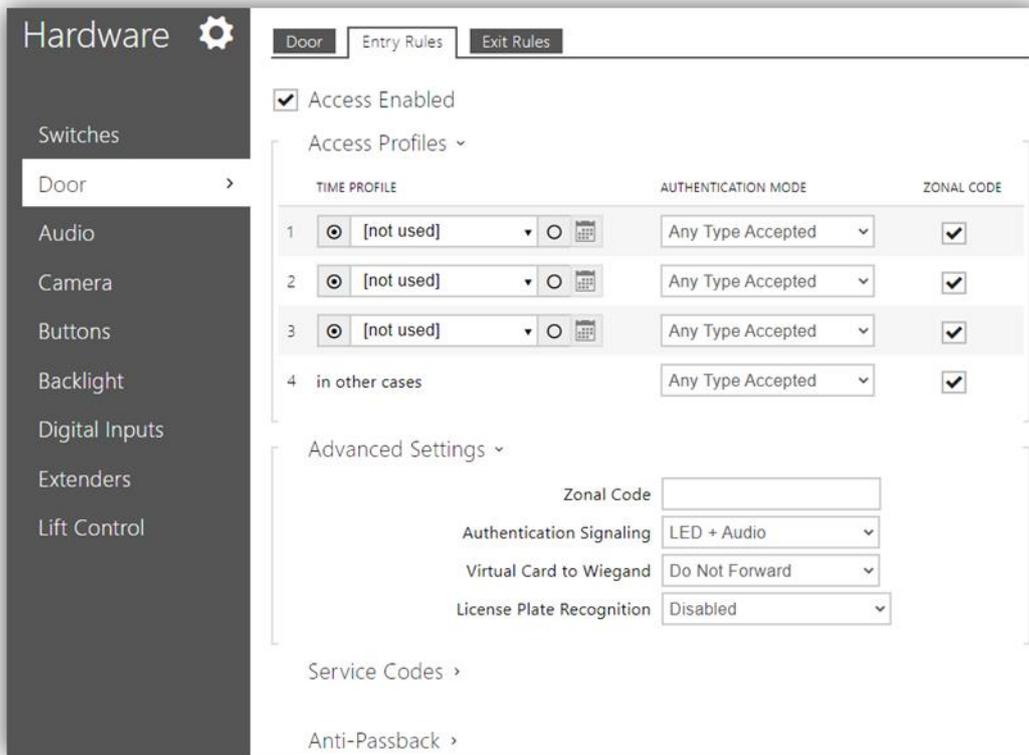


Figure 17 Port. Règles pour entrer / sortir.

- **Profil d'accès:** s'associent les profils de temps, configurés dans **Répertoire** → **Profils de temps**, ou spécifiques, avec les modes d'authentification disponibles et si s'accepte le Code de zone pour chaque cas.
- **Configuration avancée:** se configure le **Code de zone** et se pourra déterminer sa signalisation sonore à authentifier un accès et si se renvoi l'ID de la carte virtuel à un groupe de sorties Wiegand.

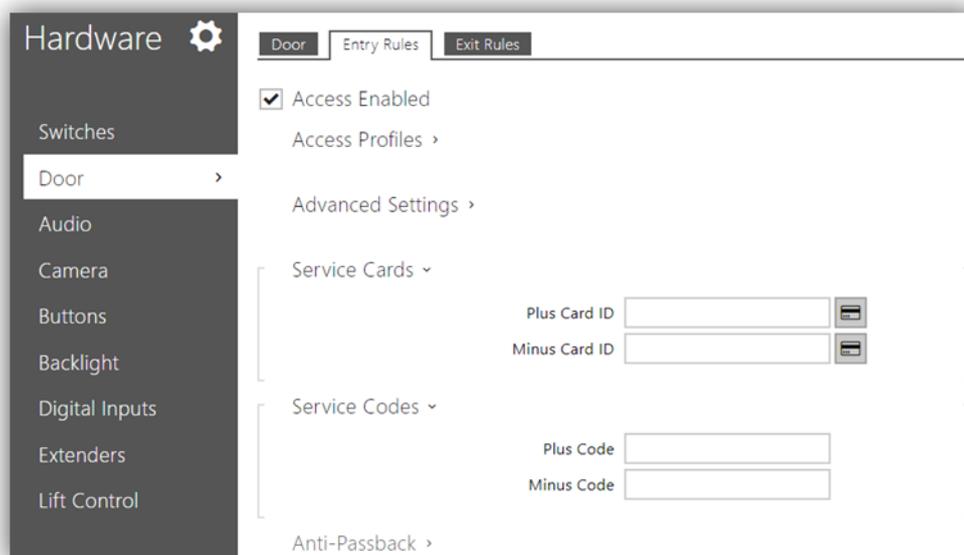


Figure 18 Cartes et codes de service.

- **Cartes de service:** se déterminent les IDs des cartes qui serviront pour ajouter des cartes de visiteurs (qui seront créés automatiquement comme nouveaux utilisateurs). Pour cela il est nécessaire le module lecteur de cartes (ZVP-RFSMN).

- Une fois introduit l'ID des cartes de ajouter et éliminer, il suffit de:
 - Approcher une d'entre elles du lecteur, sera averti par deux tonalités.
 - Approcher la carte de l'utilisateur que l'on désire ajouter ou éliminer, il s'indiquera avec trois tonalités.
- Les cartes d'utilisateurs ajoutées se garderont comme nouveaux utilisateurs avec nom "*!Visiteur #n*", ou n sera l'ID de la carte.

Vous pouvez créer autant de cartes de visiteurs qu'il y a d'utilisateurs libres (jusqu'à 10.000).

- **Codes de service:** se déterminent les codes qui serviront pour ajouter des codes utilisateur. Pour cette fonctionnalité il est nécessaire le module de clavier numérique (ZVP-KEYPAD) ou le module Touch Display (ZVP-TOUCHD).

- s'utilisera ces codes pour ajouter ou éliminer les codes qui se garderont comme nouveaux utilisateurs avec nom "!Visiteur #n", ou n sera le code assigné.
- Le code doit tenir un minimum de 2 caractères, mais il est recommandé d'utiliser des codes d'au moins 4 caractères.
- Les pas pour ajouter/éliminer un code seront:
 - Introduire code d'ajouter/éliminer à appuyer la touche clé  (ZVP-KEYPAD) ou *Ouvrir porte* (ZVP-TOUCHD).
 - Si s'ajoute un nouveau code d'utilisateur, introduire le numéro de l'interrupteur à contrôler et appuyer sur la touche clé ou *Ouvrir porte*.
 - Introduire un code à ajouter ou à éliminer et appuyer sur la touche clé ou *Ouvrir porte*.

Après chacun de ces pas, sera notifié sonore et visuellement si le pas a été réalisé avec succès.

Pourront s'introduire autant de codes comme il y a d'utilisateurs libres (10.000).

Exemple pour s'inscrire: Si le "Code d'ajout" est 1111, pour ajouter le code 1234 associé à l'ouverture de la serrure 1, il faudra suivre les pas suivants (1111  1  1234 ):

- Introduisez le Code d'ajout (1111).
- Appuyez sur la touche de la clé .
- Introduisez l'interrupteur à contrôler : 1, 2 ou 3 (1).
- Appuyez sur la touche de la clé .
- Introduisez le Nouveau code (1234).
- Appuyez sur la touche de la clé .

Exemple pour se désinscrire: Si le Code d'élimination est 0000, pour dés inscrire le code 1234, il se procédera de la façon suivante (0000  1234 ):

- Introduisez le Code d'élimination (0000).

- Appuyez sur la touche de la clé .
- Introduisez le code pour vous désinscrire (1234).
- Appuyez sur la touche de la clé .

3.1.6 CONFIGURATION DES APPELS DEPUIS LE MODULE DE BOUTONS

Dans **Hardware** → **Boutons**, les boutons sont associés aux utilisateurs à appeler, dans le cas d'avoir des modules de boutons (référence ZVP-NAME5).

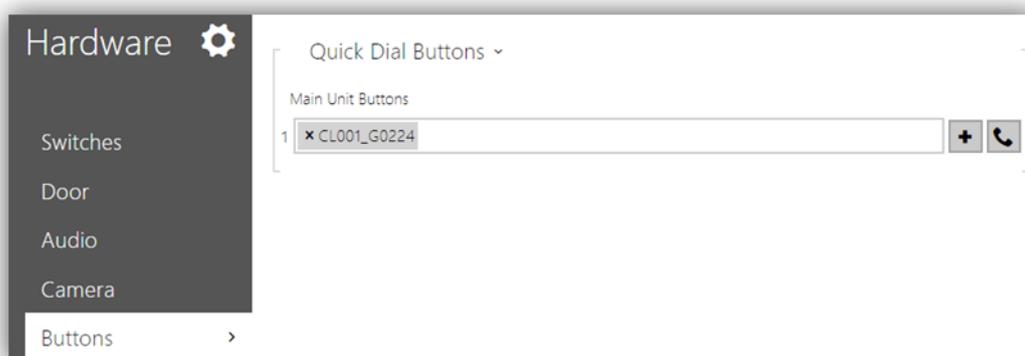


Figure 19 Boutons.

Dans boutons de numérotation rapide apparaîtront tous les boutons de numérotation directe disponibles. Ces boutons sont groupés en modules de cinq boutons (jusqu'à un maximum de 29 modules) en plus de celui intégré par défaut dans le vidéo-portier. Chaque bouton peut-être configurer pour que se réalise un appel à un ou plusieurs utilisateurs de ceux configurés sur le répertoire (voir la section 3.1.3.1). En appuyant sur l'icône  il est possible de simuler un appui sur le bouton et réaliser un appel pour vérifier que la configuration est correcte.

3.1.7 CONFIGURATION DU TAMPER ANTI-SABOTAGE

L'**interrupteur de sabotage** ne requiert aucune configuration additionnelle. La fonction de cet accessoire est d'avertir lorsque le vidéo-portier est en train d'être manipulé. C'est pour cette raison qu'on le connecte à une entrée KNX ou d'un autre système de supervision. Le contact sera fermé lorsque le cadre du Zennio GetFace IP est installé et, par contre, le contact sera ouvert lorsque le cadre est retiré (Voir section 3.2.4.4).

3.1.8 CONFIGURATION D'ACCÈS AVEC L'ÉCRAN TACTILE

Le module d'écran tactile ou Touch Display (ZVP-TOUCH) permet de réaliser des appels et d'activer la serrure. Pour configurer ce module, il est nécessaire d'accéder à la rubrique de l'interface web **Hardware→Écran**.

ÉCRAN

Dans cet onglet, on définit les paramètres de base de configuration:

- **Visualiser le répertoire téléphonique:** permet d'activer un répertoire ordonné des utilisateurs sur le Touch Display.
- **Clavier pour la saisie:** active le type de clavier pour la saisie.

Note : pour activer le clavier qui permet de réaliser des appels à utilisateurs avec le **Numéro virtuel** il faut habilitier l'option **Appel aux numéros virtuels** dans l'onglet de Services → Téléphone → Appels (voir section 3.1.2.1).

- **Langue:** établit la langue principale des contrôles sur l'écran.
- **Donner préférence aux icônes sur le texte:** si s'active cette option, le module écran montrera seulement les icônes.
- **Mode d'économie d'énergie:** active le mode économie d'énergie, sur lequel se réduit la luminosité de l'écran.

RÉPERTOIRE

Dans cet onglet, on établit l'aspect du répertoire qui apparaîtra sur l'écran du Touch Display. Il est possible de distribuer les utilisateurs par dossiers, avec un maximum de quatre sous dossiers.

Pour ajouter un nouveau dossier il faut appuyer sur le bouton . Une fois les dossiers créés, les utilisateurs configurés dans l'annuaire peuvent y être inclus en cliquant sur le bouton qui apparaît lorsqu'il se trouve sur le dossier correspondant. Prenez en compte que les dossiers qui ne contiennent pas d'utilisateurs (dans leur propre niveau ou sous-niveaux) ne seront pas enregistrés.

Il est aussi possible d'assigner les utilisateurs au dossier depuis l'onglet de **Répertoire** → **Utilisateurs**, dans la configuration du propre utilisateur. De plus, dans cet onglet peuvent se créer des **groupes d'appel** pour appeler en même temps à tous les utilisateurs qui appartiennent au même groupe. Sur la figure suivante, un exemple de groupe d'appel est *Logement 1* auquel appartient l'utilisateur 1 et Utilisateur 2 (voir la section 3.1.3.1 pour plus de détails).

Note : *un même utilisateur ne peut être dans deux dossiers différents avec le même nom. Pour cela il est nécessaire de mettre des noms différents à l'aide des groupes configurables dans l'onglet Répertoire (voir la section 3.1.3.1 pour plus de détails).*

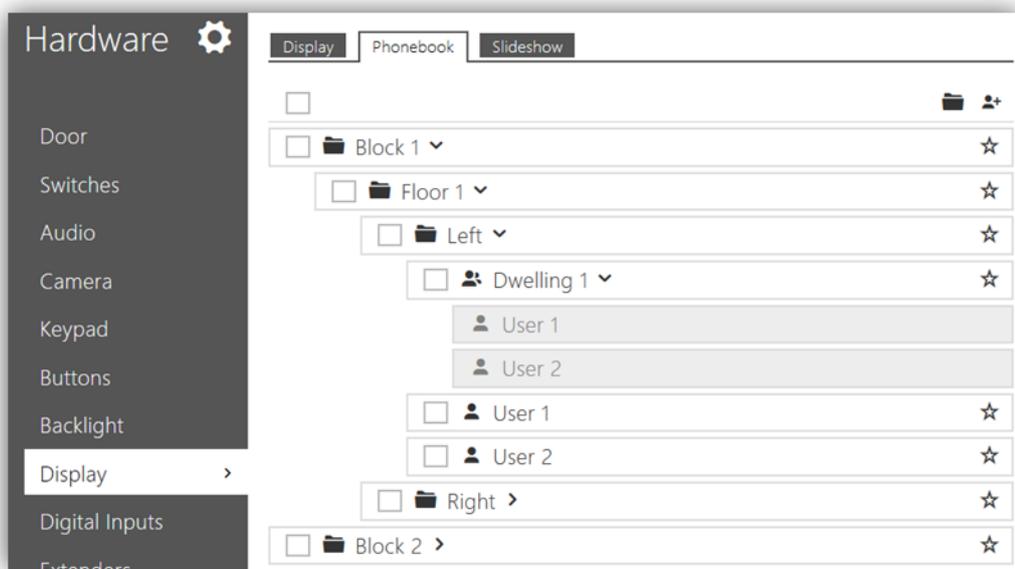


Figure 20 Écran - Répertoire.

Par ailleurs, lorsque les utilisateurs sont ajoutés, il est possible de les réordonner en appuyant sur le bouton . Les dossiers ne peuvent être déplacés, si se sélectionne un dossier et se pressionne  les utilisateurs dans ce dossier se déplaceront.

Pour éliminer un utilisateur ou dossier pressionner le bouton .

PRÉSENTATION

Le module Touch Display permet d'afficher un écran de veille ou un diaporama personnalisé après un certain temps sans utilisation. Pour ce dernier, il est possible de télécharger jusqu'à 8 images depuis votre PC. Ensuite, il est possible de les réorganiser en déplaçant avec la souris chaque image jusqu'à la position désirée. Les images seront adaptées à la résolution du Touch Display automatiquement.

Il est possible de configurer:

- **Délai d'attente pour l'activation de la présentation de l'écran de veille:** temps en secondes qui doit passer sans manipulation sur le Touch Display pour que l'écran de veille apparaisse.
- **Intervalle de transition:** temps entre images de la présentation de l'écran de veille.

3.1.9 CONFIGURATION DE L'ACCÈS AVEC CARTE RFID

Le module ZVP-RFSMN permet la lecture de cartes d'accès RFID. Il est possible de configurer différents types de cartes:

- **Cartes assignées aux utilisateurs déjà créées** (jusqu'à deux cartes par utilisateur).
- **Cartes de visiteurs**, qui s'ajoutent au moyen des cartes de service (voir **Carte de service** dans la section 3.1.4).
- **Cartes de service:** Une pour enregistrer les cartes des visiteurs et une autre pour les annuler (voir **Cartes de service** dans la section 3.1.4).

L'attribution des cartes d'utilisateurs déjà créées, se fait depuis l'écran de configuration de l'utilisateur (**Répertoire → Utilisateurs**):

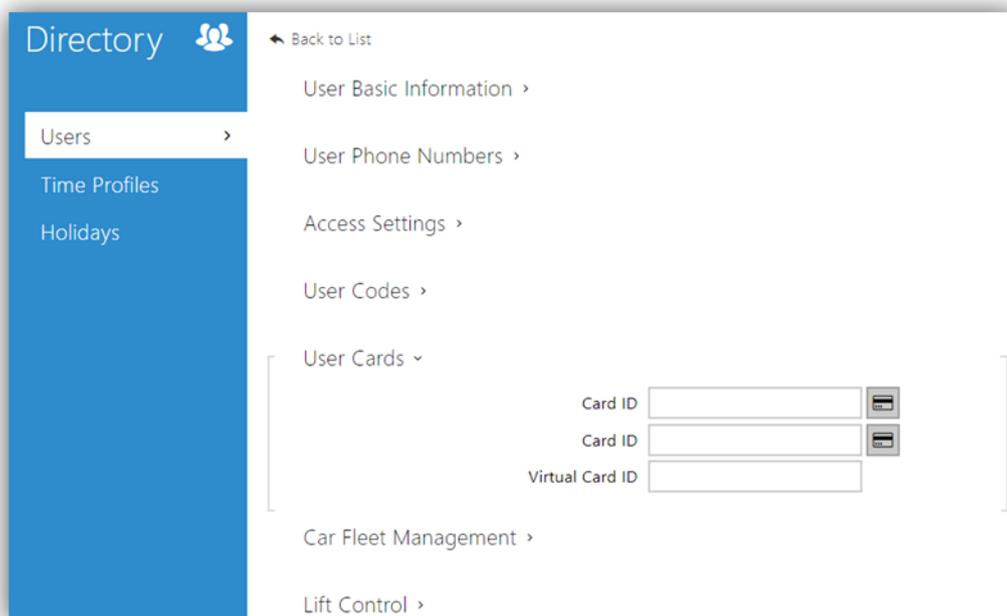


Figure 21 Utilisateurs - Cartes de l'utilisateur.

Pour introduire l'identificateur des cartes il existent deux options:

- **En automatisant le processus au moyen du lecteur de cartes RFID pour PC (ZVP-RFUSB).** Pour cela il est nécessaire d'installer le contrôleur du lecteur, disponible sur www.zennio.fr. En appuyant sur le bouton , le champ sera automatiquement rempli avec le code de la carte qui passe par le lecteur (le lecteur allumera une led verte lorsque la carte est insérée).
- Si vous ne disposez pas du lecteur de cartes RFID pour PC, il est possible de faire les assignations manuellement. Pour ajouter une nouvelle carte, il sera nécessaire de connaître son Identifiant. Pour le connaître, il est possible de passer la carte par le module du lecteur (ZVP-RFSMN), ce qui fera qu'elle apparaisse dans **État→Registre d'accès**:

	TIME	CARD ID	CARD TYPE	DESCRIPTION
1	24/08/2017 14:46:49	804C80DA1D5C04	MIFARE DESFire	(user #1)
2	24/08/2017 14:46:44	804C80DA1D5C04	MIFARE DESFire	(user #1)
3	24/08/2017 14:46:30	804C80DA1D5C04	MIFARE DESFire	Access denied
4	24/08/2017 14:46:29	804C80DA1D5C04	MIFARE DESFire	Access denied
5	24/08/2017 14:46:22	80518B1A3E2704	MIFARE DESFire	!Visitor #11 (user #11)
6	24/08/2017 14:46:07	804C80DA1D5C04	MIFARE DESFire	!Visitor #12 (user #12)

Figure 22 Registre d'accès.

À l'entrée du registre on peut voir son ID qui peut être copié pour configurer la carte sans besoin d'un lecteur USB externe.

L'**ID de la carte virtuelle** sera celui qui s'enverra aux dispositifs Wiegand.

On peut leur appliquer des profils horaires pour la configuration d'accès de la carte (voir section 3.2.2.1). Si le profil de temps n'est pas configuré, il faut s'assurer que dans la section **d'utilisateurs** → **Configuration d'accès** se sélectionne le profil d'accès **[sans utilisation]**.

D'autre part, dans la section **Hardware** → **Extensions** apparaîtront des options à configurer pour le module, une fois qu'il est connecté:

- **Nom du module:** établit le nom qui apparaîtra dans le registre pour les évènements relationnés avec ce module.
- **Porte:** établit la direction (sans utilisation / sortie) ou se permet l'accès.
- **Interrupteur associé:** établit quel interrupteur activera après s'authentifier à travers de ce module.
- **Type de carte permise:** établit les types de cartes supportées par le module.
- **Renvoyer à la sortie Wiegand:** établit un groupe de sorties Wiegand auxquels se renverront tous les ID de carte virtuelle configurés

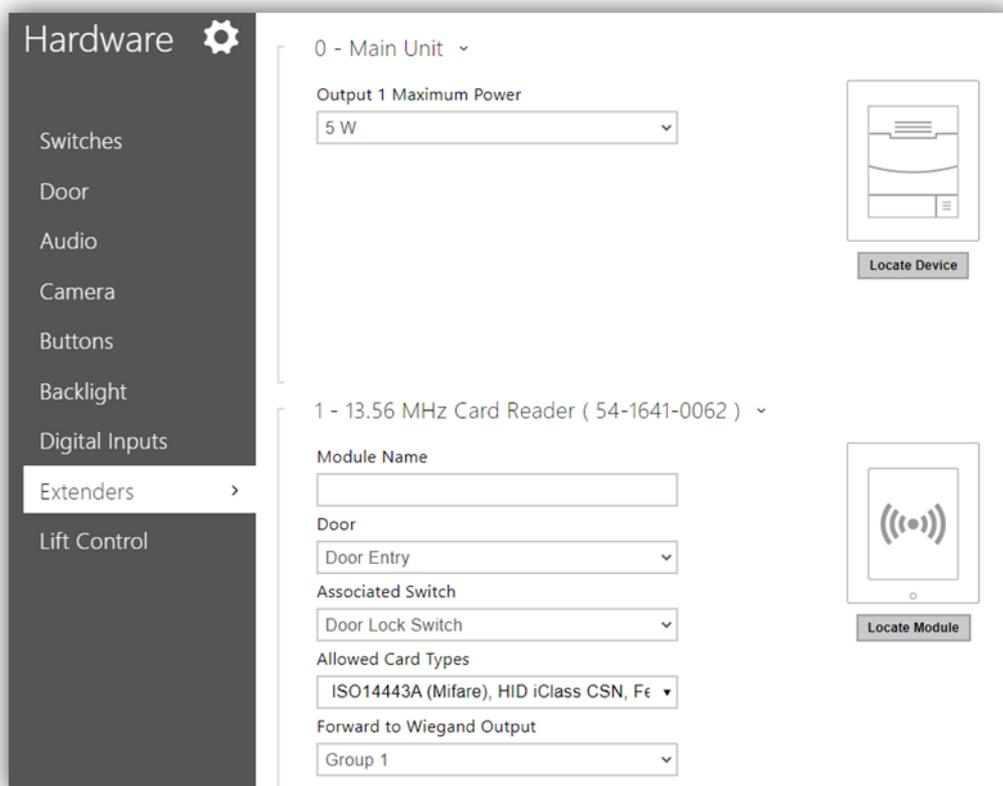


Figure 23 Configuration hardware du module lecteur de carte NFC.

3.1.10 CONFIGURATION DE L'ACCÈS AVEC MODULE BLUETOOTH

Le module **ZVP-BLUET** offre une forme sûre et commode d'ouvrir les portes en utilisant une application et un dispositif mobile qui dispose du Bluetooth. Consultez la section du module [ZVP-BLUET](#) de la web de Zennio pour obtenir l'application mobile correspondante.

L'utilisation de ce module est très simple, il suffit seulement de le connecter au GetFace IP et **l'appairer** avec un dispositif mobile. Pour motifs de sécurité, toute la communication Bluetooth est **cryptée**. Pour cela s'utilisent plusieurs clés nécessaires pour que l'authentification soit correcte et se permet l'ouverture des portes.

3.1.10.1 PROCÉDURE D'APPAIRAGE

Le procès d'appairage consiste à transmettre les données d'accès d'un utilisateur de GetFace IP à un dispositif mobile.

L'appairage se réalise à travers d'un numéro PIN. Cela s'obtient dans l'interface web de GetFace IP dans la section **directoire** → **Utilisateurs** → **Clé mobile d'utilisateur** et s'introduit dans l'application mobile.

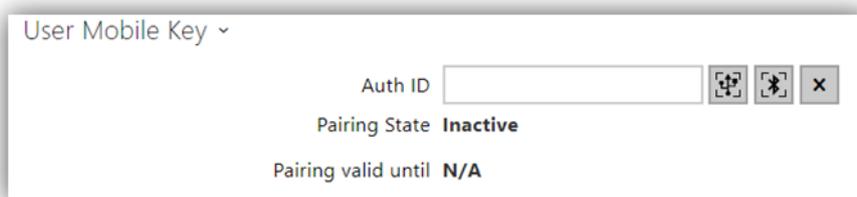


Figure 24 Clé mobile de l'utilisateur

Liste des **paramètres**:

- **Auth ID**: identifiant unique d'utilisateur/dispositif mobile. Se génère automatiquement pendant l'appairage. Peut se transmettre à autre utilisateur ou copier à autre vidéo portier dans le Même emplacement (pour connaître plus de détails de l'emplacement voir la section 3.1.10.2).
- **État de l'appairage**: indique l'état actuel de l'appairage (N'est pas actif, En attente de l'appairage, Appairé ou PIN expiré).
- **Appairage valide jusqu'à**: date et heure jusqu'à ce que le PIN généré soit valide.

Les pas pour réaliser l'**appairage** sont:

1. Cliquer sur le bouton de Bluetooth  pour commencer l'appairage pour l'utilisateur sélectionné.
2. Se génère automatiquement l'identifiant dans Auth ID et se montre une fenêtre de dialogue en indiquant le numéro PIN

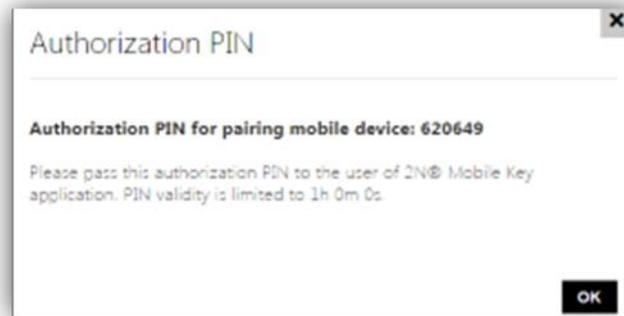


Figure 25 Fenêtre pour indiquer le numéro PIN.

3. Chercher le lecteur Bluetooth adéquat dans la section "Dispositifs" de l'application et appuyer "Appairer de nouveaux dispositifs". Le changement de section se réalise depuis le bouton  du coin supérieur gauche.

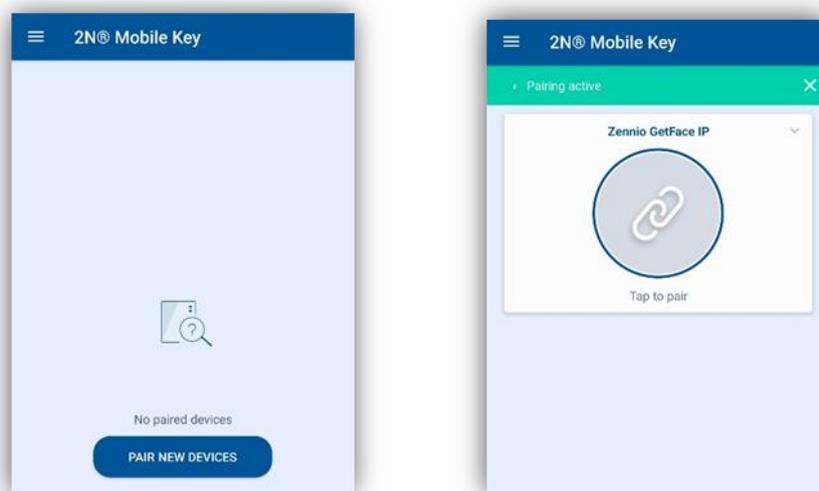


Figure 26 Recherche de dispositifs

4. Introduite le PIN obtenu dans le pas 2

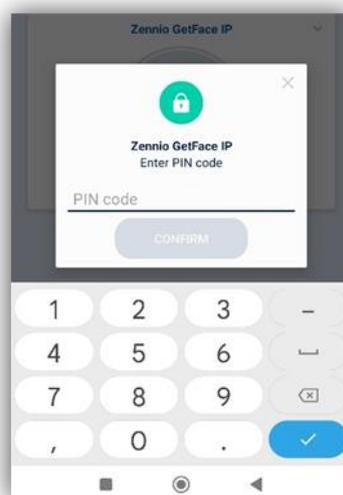


Figure 27 introduction du numéro PIN

5. Lorsque l'appairage se termine, il se montrera "L'appairage s'est réalisé avec succès".

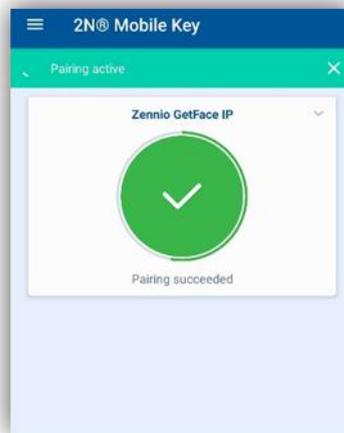


Figure 28 Dispositif appairé

Dans l'appairage, se transmet l'information suivante au dispositif mobile:

- Identificateur d'emplacement (voir section 3.1.10.2 pour plus de détails).
- Clé de chiffrement d'emplacement (voir section 3.1.10.2 pour plus de détails).
- Identificateur de l'utilisateur (Auth ID).

Une fois appairés, lorsque le mobile se trouve dans le rayon de détection du module, apparaîtra dans l'application et simplement en appuyant sur le bouton la porte s'ouvrira, comme se montre sur la figure suivante:

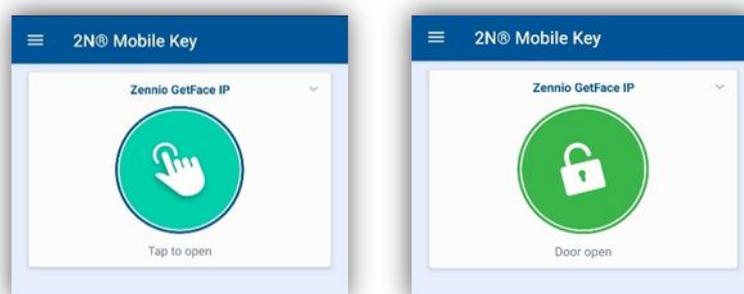


Figure 29 Processus d'authentification et d'ouverture

3.1.10.2 AUTRES CONFIGURATIONS

Dans la section **Services** → **Mobile Key** se dispose de plusieurs aspects en relation avec l'interaction de l'application mobile:

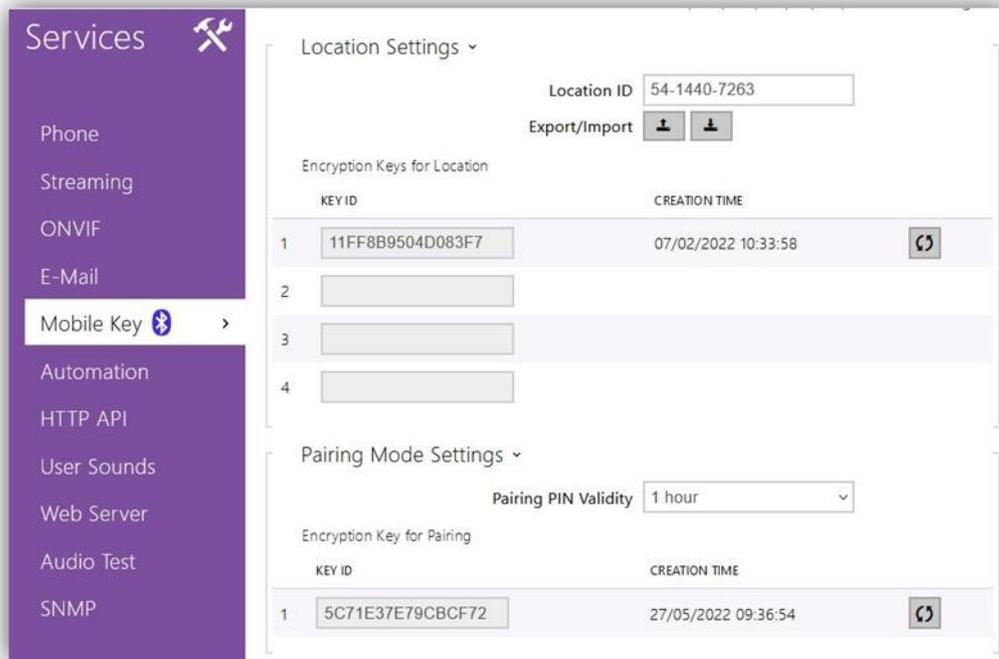


Figure 30 Configuration de l'emplacement et du mode d'appairage

Comme il a déjà été commenté, la communication Bluetooth entre l'application mobile et le vidéo portier est cryptée. Pour cela se dispose d'une clé primaire et jusqu'à trois secondaires, valides pour un emplacement déterminé. La clé primaire se génère automatiquement avec la première mise en marche du vidéo portier et se transmet au dispositif mobile pendant l'appairage.

Il est possible d'exporter/importer les clés d'encryptage et l'identificateur de l'emplacement à d'autres vidéo portiers. Les vidéo portiers avec la même localisation et clés d'encryptage forment ce qui s'appelle un **emplacement**. Dans un emplacement il est possible de copier d'un vidéo portier à l'autre l'identificateur d'un utilisateur (Auth ID) et il ne sera pas nécessaire de l'appairer.

Configuration de l'emplacement:

- **Emplacement ID:** identificateur unique de l'emplacement dans lequel la clé d'encryptage sera valide.
- **Exporter:** créer une archive avec l'emplacement et clés d'encryptage actuelles pour importer dans d'autres vidéo portiers et former un emplacement.
- **Importer:** pour importer une archive avec l'emplacement et clés d'encryptage qui a été exporté depuis un autre vidéo portier.

Les options pour les clés d'encryptage de l'emplacement sont:

- **Restaurer la clé primaire** : la clé primaire actuelle passe à être la première clé secondaire et les clés secondaires se déplacent d'une position vers le bas (s'il y a 3 positions, la plus ancienne s'élimine).
- **Effacer la clé primaire/ secondaire** : s'efface la clé correspondante.

Si la clé gardée dans un dispositif mobile est une des clés secondaires, il se permet l'accès et après un accès valide, s'actualise la clé sur le dispositif primaire.

Si la clé gardée dans un dispositif mobile ne coïncide avec aucune des clés (primaire ou secondaires) l'accès ne sera pas permis.

Important: Dans le cas de perte ou de vol d'un dispositif mobile avec l'information d'accès, procéder de la manière suivante:

- Éliminer l'Authentification ID (voir section 3.1.10.1) pour éviter l'accès.
- Restaurer la clé primaire (optionnelle) pour éviter l'utilisation non permise de la clé gardée dans le dispositif mobile.

Configuration du mode d'appairage.

- **Période de validité:** temps pendant lequel le numéro PIN est valide et l'utilisateur peut s'appairer
- **Clé d'appairage:** indique la clé d'appairage actuelle et donne l'option de la régénérer.

3.1.10.3 OPTIONS DE HARDWARE

Dans la section **Hardware** → **Extensions** apparaîtront des options à configurer pour le module, une fois qu'il est connecté:

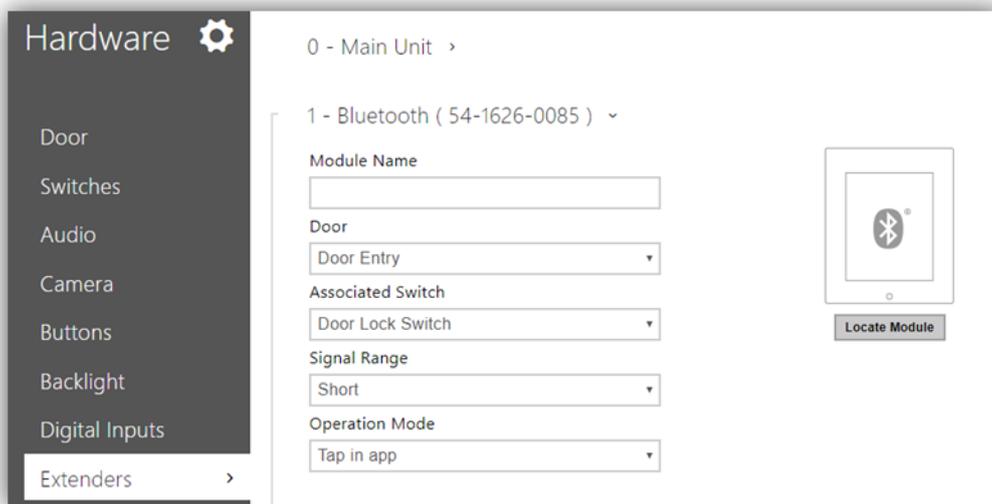


Figure 31 Configuration hardware du module Bluetooth

- **Nom du module:** établit le nom qui apparaîtra dans le registre pour les évènements relationnés avec ce module.
- **Porte:** établit la direction (Arrivée / sortie) ou se permet l'accès.
- **Interrupteur associé:** établit quel interrupteur activera après s'authentifier à travers de ce module.

Note : L'option 'Personnalisé' n'a pas de fonctionnalité.

- **Portée du signal:** établit l'échelle maximum du module Bluetooth pour localiser des dispositifs mobiles.
- **Mode de fonctionnement:** méthode d'authentification avec le mobile:
 - Un appui sur l'application: la vérification et ouverture de porte se réalise dans l'application depuis le dispositif mobile.

3.1.11 CONFIGURATION DE LA BOUCLE D'INDUCTION MAGNÉTIQUE

Le module ZVP-ILOOP est un module conçu pour les personnes avec des problèmes d'audition. Permet la transmission d'un signal audio directement vers une prothèse auditive au moyen d'une boucle magnétique. De plus, il montre des signaux visuels de grande taille pour améliorer la communication.

Pour configurer ce module, il faut accéder à la rubrique **Hardware** → **Extensions** et ajuster la puissance du signal à la valeur désirée.

3.2 CONFIGURATIONS AVANCÉES

Ces champs ne sont pas nécessaires pour le fonctionnement de l'installation, mais cette information est fournie pour le cas où l'utilisateur voudrait configurer des fonctions additionnelles.

3.2.1 ÉTAT

L'onglet **État** montre toute l'information d'état qui concerne le Zennio GetFace IP. Il se décompose dans les rubriques suivantes:

3.2.1.1 DISPOSITIF

Elle montre l'information la plus utile du produit, dont le numéro de version du hardware, du firmware et du logiciel de démarrage, ainsi que le **Nom du produit**, son **Numéro de série**, le **Temps de fonctionnement** et le type **Source d'alimentation**. Il se montre aussi le bouton **Localiser le dispositif**. À cliquer sur le dispositif il se reproduira un son court e fera clignoter tous ses indicateurs lumineux.

La partie **Caractéristiques de l'appareil** indique si l'unité basique dispose d'une caméra et les caractéristiques des modules.

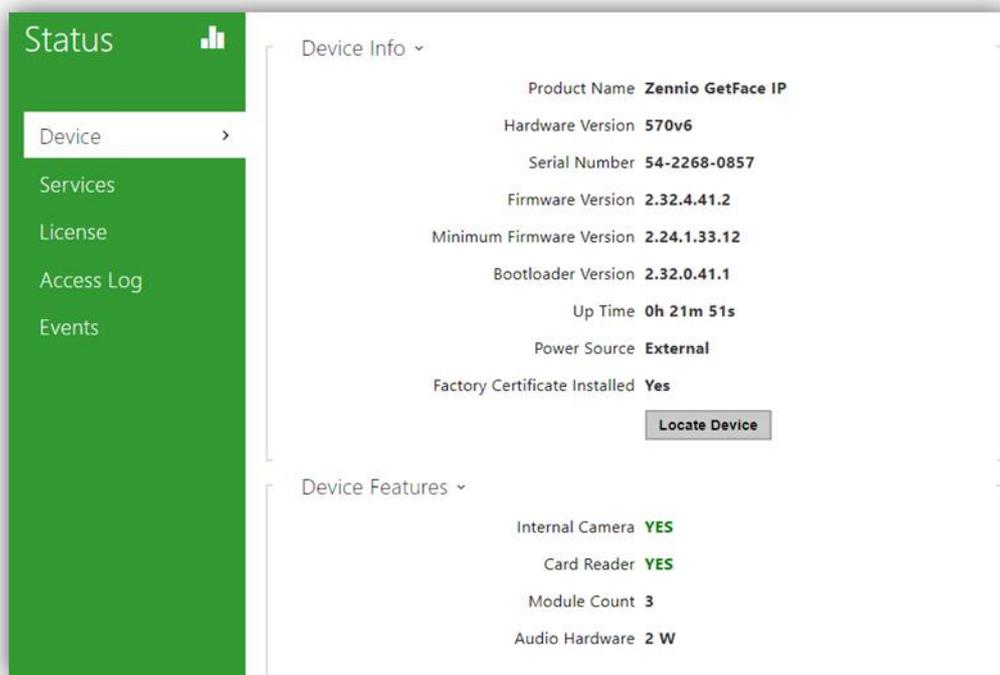


Figure 32 Appareil.

3.2.1.2 SERVICES

Elle montre l'information basique concernant le réseau du dispositif et l'état de ses services.

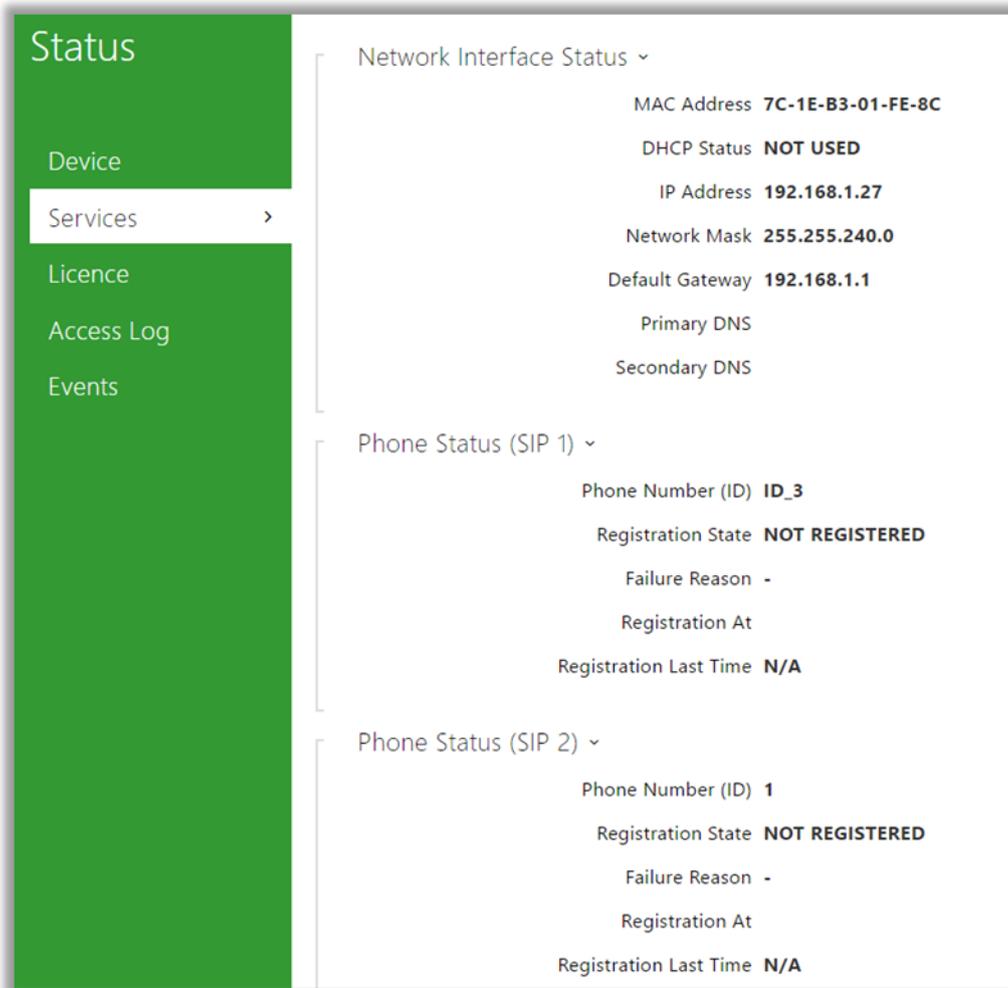
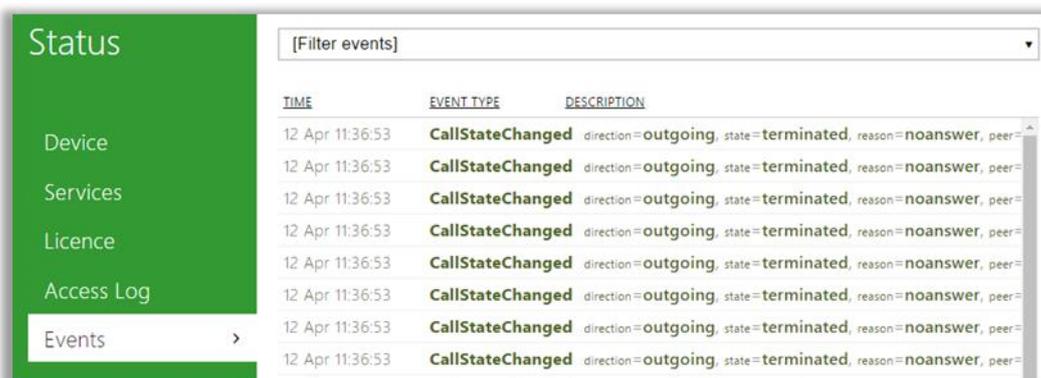


Figure 33 Services.

3.2.1.3 ÉVÉNEMENTS :

Elle montre, par ordre chronologique, un registre avec les derniers évènements produits.



TIME	EVENT TYPE	DESCRIPTION
12 Apr 11:36:53	CallStateChanged	direction=outgoing, state=terminated, reason=noanswer, peer=
12 Apr 11:36:53	CallStateChanged	direction=outgoing, state=terminated, reason=noanswer, peer=
12 Apr 11:36:53	CallStateChanged	direction=outgoing, state=terminated, reason=noanswer, peer=
12 Apr 11:36:53	CallStateChanged	direction=outgoing, state=terminated, reason=noanswer, peer=
12 Apr 11:36:53	CallStateChanged	direction=outgoing, state=terminated, reason=noanswer, peer=
12 Apr 11:36:53	CallStateChanged	direction=outgoing, state=terminated, reason=noanswer, peer=
12 Apr 11:36:53	CallStateChanged	direction=outgoing, state=terminated, reason=noanswer, peer=
12 Apr 11:36:53	CallStateChanged	direction=outgoing, state=terminated, reason=noanswer, peer=

Figure 34 Évènements.

3.2.2 RÉPERTOIRE

Dans le menu **Répertoire**, les logements connectés au vidéo-portier sont configurés. Comme fonctions avancées, on peut configurer les rubriques suivantes:

3.2.2.1 PROFILS HORAIRES

Les profils horaires permettent de limiter l'utilisation des cartes RFID et les codes numériques. En particulier, il est possible de définir des fourchettes de temps pour lesquelles:

- Les appels reçus par un utilisateurs sont bloqués.
- L'accès avec des cartes RFID est bloqué.
- L'ouverture de la porte est bloquée.

Il est possible de configurer jusqu'à 20 profils différents avec différents horaires activés pour chaque jour de la semaine. Les paramètres à configurer sont les suivants:

- Nom du profil (optionnel).
- **Feuille horaire du profil** pour chaque jour de la semaine, fériés inclus.

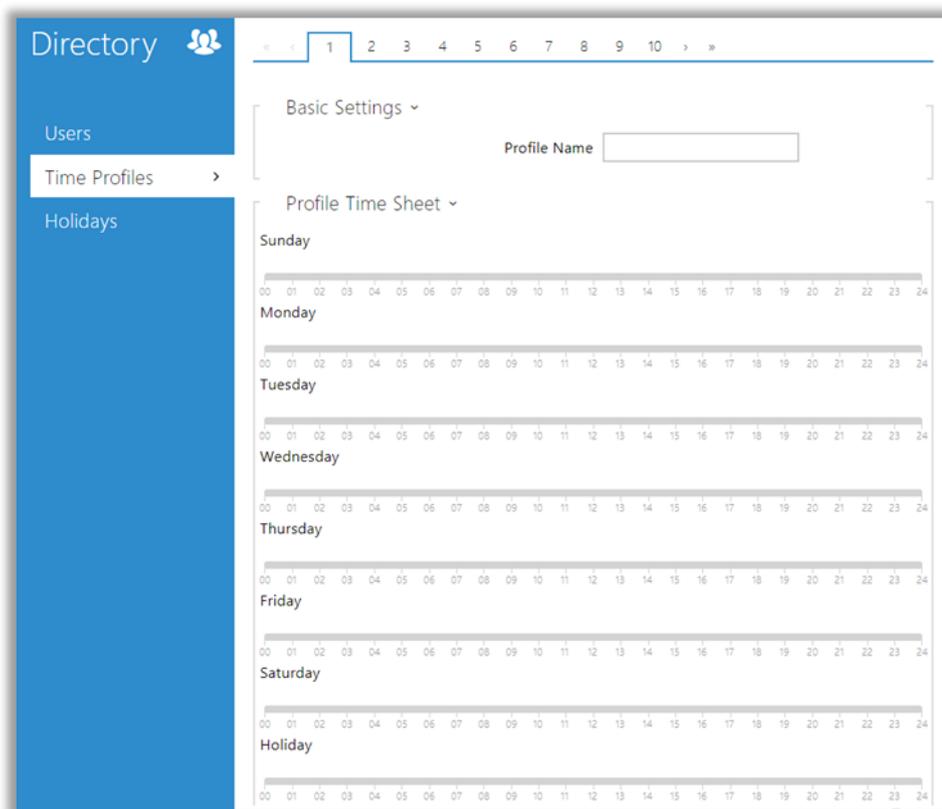


Figure 35 Profils horaires.

3.2.2.2 VACANCES

Dans cette rubrique, on peut configurer le calendrier des jours fériés fixes (annuels) et variables dans le but de définir des profils horaires en fonction de la date.

*Avec un seul clic sur une date la case se marque en vert, ce qui indique qu'il s'agit d'un **jour férié fixe**. En cliquant une seconde fois sur cette case, elle passera à être considérée comme **jour férié variable**, ce qui est indiqué par la couleur bleue. Un troisième clic annulerait la configuration de jour férié.*

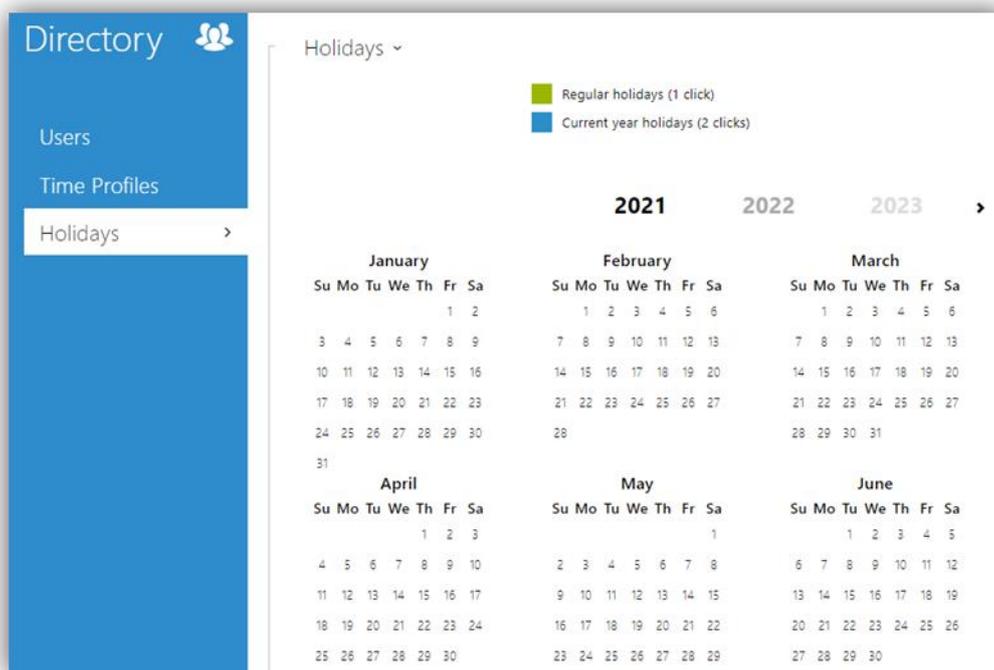


Figure 36 Vacances.

3.2.3 SERVICES

Le menu **Services** permet les fonctions avancées suivantes:

3.2.3.1 E-MAIL

Il peut s'envoyer un courrier électronique aux utilisateurs du GetFace IP Zennio avec information sur les appels (perdus ou acceptés) si se dispose de connexion à internet (il est aussi possible d'envoyer une information sur les accès si le module ZVP-RFSMN est connecté). Si, en plus, le vidéo-portier est équipé d'une caméra, il est possible de joindre automatique une ou plusieurs photos prises lors de l'appel ou de la sonnerie.

Le vidéo-portier envoie des courriels à tous les utilisateurs dont l'adresse e-mail est incluse dans la liste des utilisateurs. Si le paramètre E-mail de la liste des utilisateurs est vide, les courriels seront envoyés à l'adresse mail du destinataire par défaut.

SMTP

Permet la configuration du serveur SMTP:

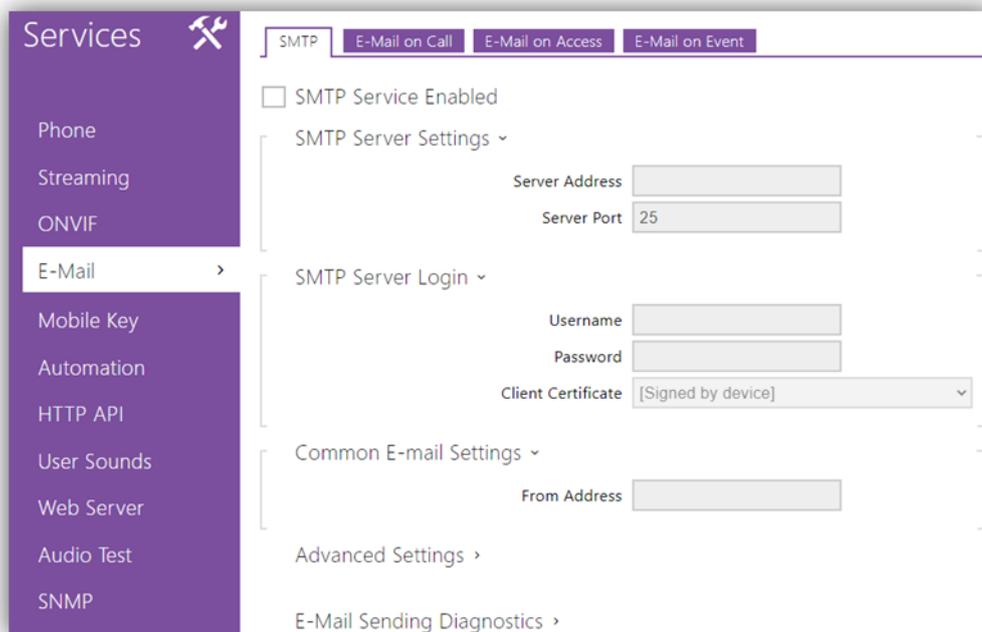


Figure 37 SMTP.

- **Paramètres du serveur SMTP:** définit l'adresse et le port du serveur SMTP auquel seront envoyés les courriels.
- **Connexion au serveur SMTP:** permet d'introduire un nom d'utilisateur valable pour initier une session si le serveur SMTP requiert une autorisation; sinon, le champ doit rester en blanc. Il est aussi possible d'indiquer un **certificat d'utilisateur** et un **mot de passe** pour chiffrer la communication entre le vidéo-portier et le serveur SMTP.
- **Ajustes généraux de e-mail:** configure l'adresse de l'expéditeur pour tous les courriels envoyés.
- **Réglages avancés:** définit la limite du temps pour le livraison d'un courriel à un serveur SMTP qui ne serait pas disponible.

- **Diagnostics d'envoi d'E-mails:** permet d'envoyer un courriel de test vers une adresse prédéfinie dans le but de tester la fonctionnalité de la configuration d'envoi d'e-mail actuelle. Pour ce faire, il faut introduire une adresse e-mail destinataire et appuyer sur le bouton. L'état de l'envoi est affiché continuellement dans la fenêtre pour faciliter la détection de problèmes.

E-MAIL SUR L'APPEL

Montre les réglages du courriel à envoyer en cas d'appel:

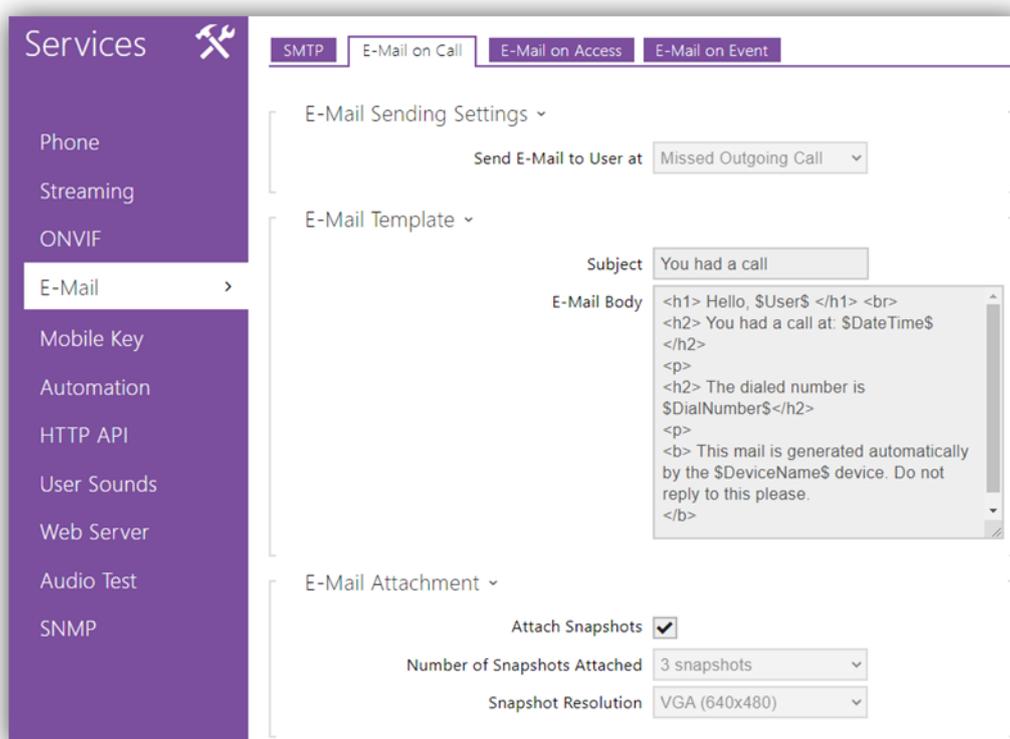


Figure 38 Appel sur E-mail.

- **Réglages d'envoi de courriers électroniques:** définit le type d'envoi
- **Modèle de E-mail:** établit le destinataire, le sujet et le corps du message.

Le vidéo-portier envoie les messages à l'adresse mail qui figure dans la liste de positions des utilisateurs. Dans le cas où ce champ serait aussi en blanc, aucun courriel ne sera envoyé.

Pour le corps du message, on peut utiliser des **étiquettes HTML**. Il est possible d'insérer des symboles spéciaux pour remplacer le nom de l'utilisateur, la date, l'heure, l'identifiant du vidéo-portier ou le numéro auquel on appelle, qui sont remplacés par les informations réelles lors de l'envoi.

- **\$User\$**: nom d'utilisateur.
 - **\$DateTime\$**: date et heure actuelle.
 - **\$DialNumber\$**: numéro pianoté.
- **Archives adjointes de e-mail**: active l'envoi d'images en pièces jointes, prises depuis le vidéo-portier durant le marquage ou l'appel. On peut choisir le nombre d'images et leur résolution.

E-MAIL D'ACCÈS

Montre les réglages du mail à envoyer en cas d'un accès: Les paramètres sont équivalents à ceux de l'onglet précédent.

E-MAIL – ÉVÉNEMENT

Montre les réglages du mail à envoyer devant différentes actions du système:

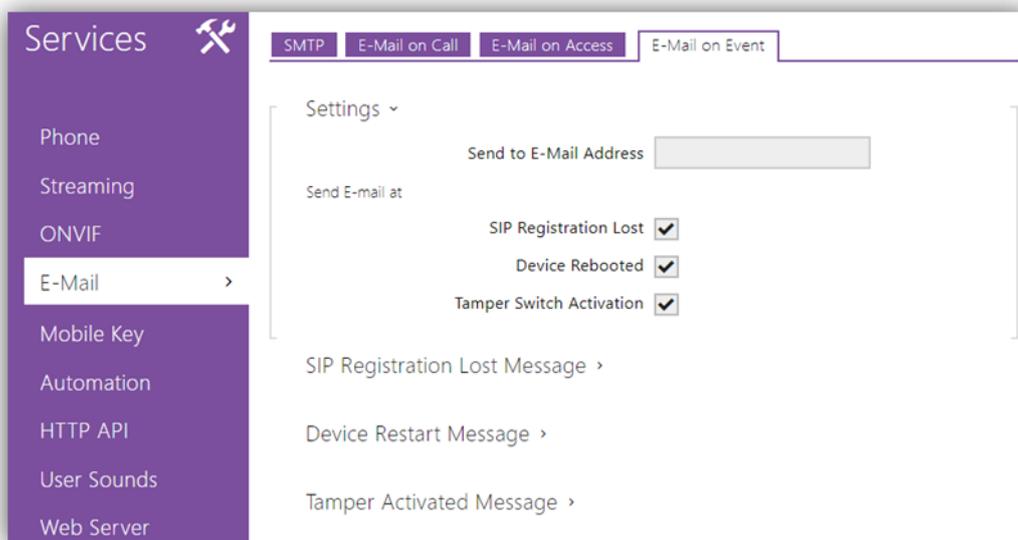


Figure 39 E-mail d'événement

- **Configuration:** permet de définir l'adresse de destination et les événements qui provoqueront l'envoi du mail d'événement. Ces événements peuvent être:
 - Perdre le registre SIP
 - Réinitialisation du dispositif.
 - Activation de l'interrupteur Tamper
- **Message dans le cas de perdre le registre SIP:** Établit l'objet de l'e-mail du message envoyé et le corps du message en cas de perte de l'enregistrement SIP. Dans le corps du mail peuvent être utilisés les symboles du format du langage HTML.
- **Message au redémarrage du dispositif:** Les paramètres sont équivalents au champ précédent.
- **Message à l'activation de l'interrupteur de sécurité:** Les paramètres sont équivalents au champ précédent.

3.2.3.2 AUTOMATISATION

L'**automatisation** permet d'associer des événements du système (appui de touches, utilisation de cartes RFID, changement d'état dans une entrée numérique, etc.) avec des actions spécifiques (activation d'une sortie numérique, reproduction de sonneries, appels, etc.). L'exécution des actions peut être limitée par des conditions sélectionnées (état du profil horaire, état d'une entrée, etc.).

On peut établir jusqu'à **cinq fonctions**, lesquels peuvent être configurées sur une interface disponible à faire un clic sur le bouton 'Éditer' de la fonction .

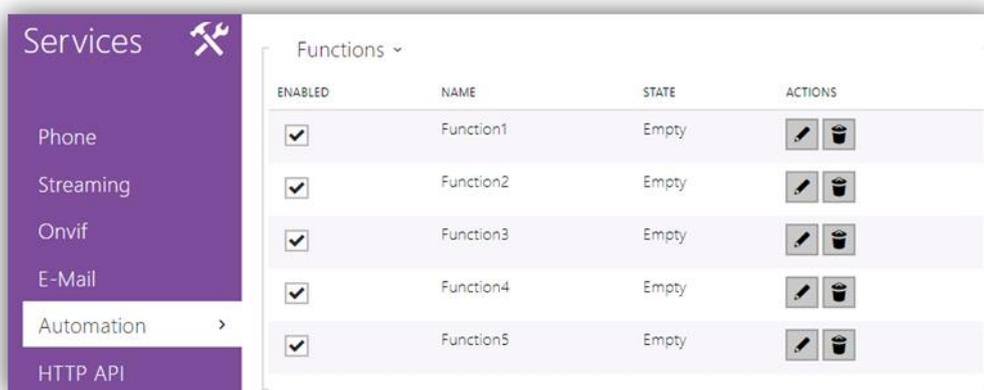


Figure 40 Automatisation.

Dans chaque fonction il faut combiner des événements, des actions et des conditions.
Peut se paramétrer un maximum de trente conditions

Note : Après le démarrage du dispositif se vérifieront automatiquement les états des entrées dans l'automatisation.

3.2.3.3 SERVEUR WEB

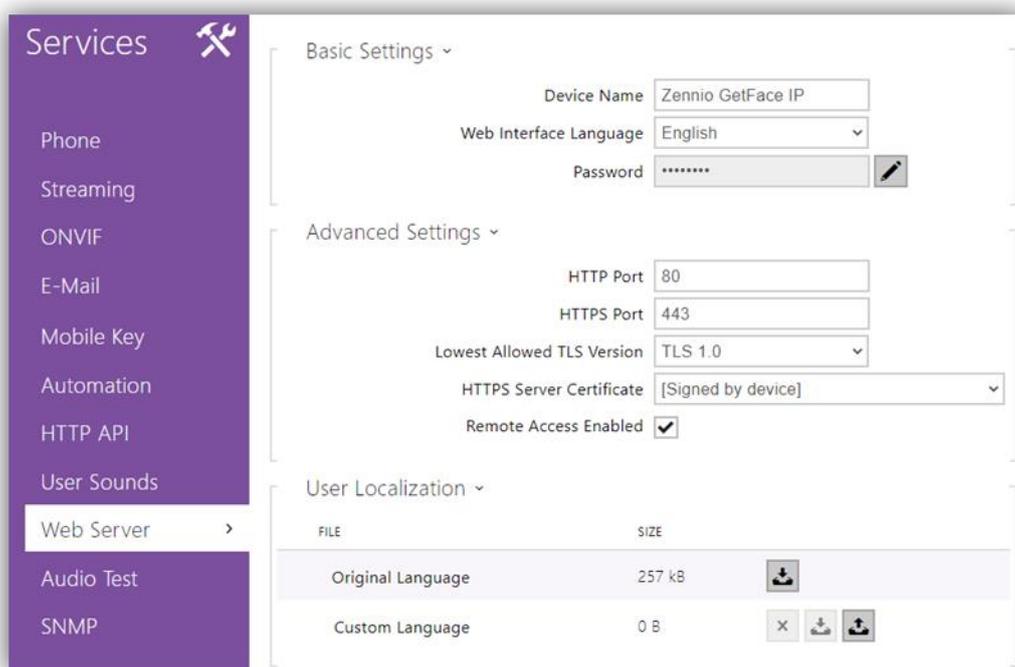


Figure 41 Serveur web.

Le nom d'utilisateur et le mot de passe de connexion de l'interface web du Zennio GetFace IP (par défaut, **admin** et **zennio** respectivement) peuvent être changé dans cette section. De la même façon, on peut changer la langue de l'interface.

3.2.4 HARDWARE

Dans le menu **Hardware**, il est possible de configurer les paramètres suivants:

3.2.4.1 AUDIO

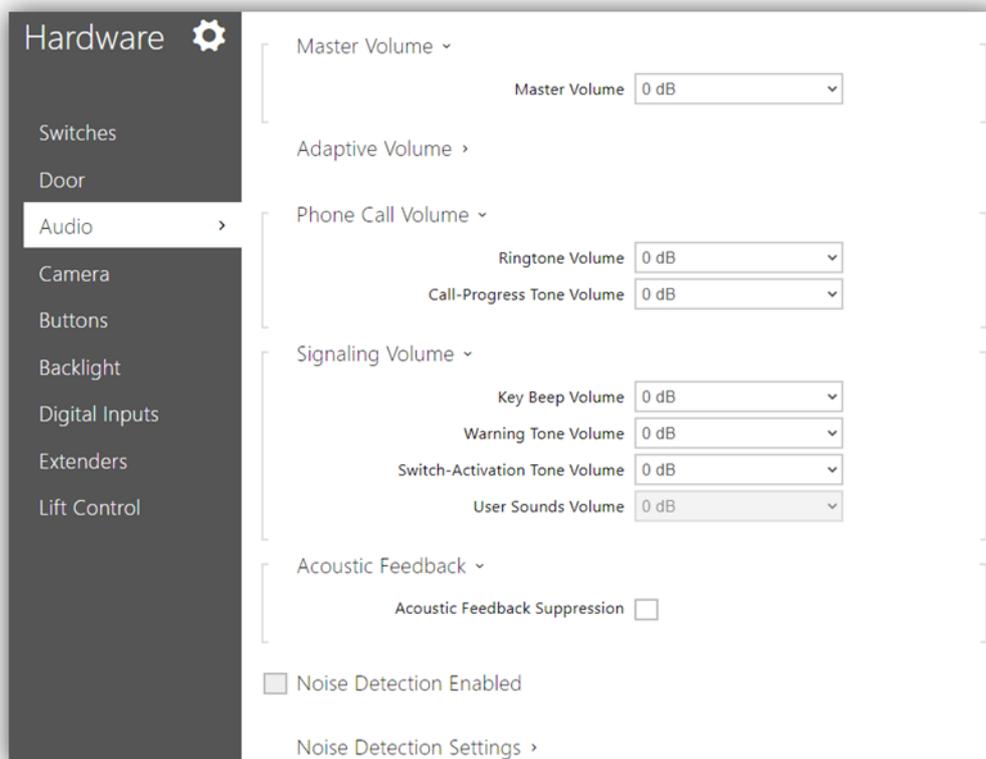


Figure 42 Audio.

- **Volume général:** intensité du volume général du dispositif. Ce paramètre affecte les appels, et les sons de signalisation.
- **Volume adaptable:** lorsque ce paramètre est activé, on peut paramétrer un **Gain maximal** et un **Seuil de sensibilité** à partir duquel on appliquera l'augmentation du volume adaptable. Qu'il soit activé ou non, il est possible d'observer le **Niveau de bruit actuel** ainsi que le **Gain adaptable actuel** du volume.

- **Volume appel téléphonique:** définit l'intensité de la sonnerie de l'appel ainsi que des sons d'appel, c'est-à-dire, les sons de marquage et de ligne occupée.
- **Volume de signalisation:** établit les valeurs d'intensité du volume des touches, des avertissements et de l'activation des interrupteurs, ainsi que les sonneries à reproduire.
- **Rétroaction acoustique:** permet de supprimer les couplages entre le haut-parleur du vidéo-portier et l'unité intérieure. Il est recommandé d'activer ce paramètre uniquement dans le cas où des problèmes de couplage du son seraient détectés.

3.2.4.2 CAMÉRA

Dans cette rubrique, on peut configurer la source de vidéo du GetFace IP ainsi que modifier les paramètres qui établissent le format de la sortie vidéo.

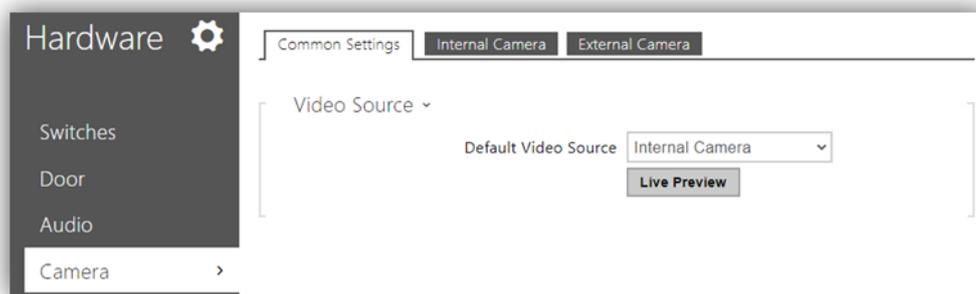


Figure 43 Caméra.

PARAMÈTRES COMMUNS

Dans cet onglet, on configure l'origine de la source vidéo. On peut y configurer une caméra **interne** (celle du Zennio GetFace IP) ou une caméra IP **externe**. Lorsque la source vidéo par défaut est choisie et que la configuration est établie, il existe la possibilité de faire une prévisualisation.

Note : Dans le cas où le dispositif ne dispose pas de caméra (modèle ZVP-WOCAM), il n'est pas possible de configurer de caméra interne.

CAMÉRA INTERNE

Dans cet onglet, on configure les paramètres de l'image de la sortie vidéo:

- **Niveau de luminosité.**
- **Saturation des couleurs.**
- **Mode caméra:** permet de réduire l'effet de la lumière solaire directe ou des sources de lumières artificielles sur l'image, en fonction du lieu où est installé le Zennio GetFace IP (en intérieur ou en extérieur).
- **Mode jour/nuit:** définit le mode jour/nuit de la caméra. On peut établir un mode unique ou d'activer une commutation automatique, en fonction du niveau de lumière de l'environnement.
- **Mode actuel:** affiche le mode jour/nuit actuel.
- **Niveau de luminosité de la LED IR:** définit le niveau de luminosité de la LED infrarouge dans une fourchette entre 0 et 100% avec des pas de 25%. Si le mode automatique est sélectionné, le Zennio GetFace IP activera l'éclairage infrarouge quand il détecte une luminosité faible et que la caméra est en marche.
- **Niveau actuel de luminosité de la LED IR:** affiche le niveau de luminosité actuel de la LED IR. Le niveau pourrait être inférieur à celui établi en cas de consommation élevée d'énergie (normalement, lorsque plusieurs extensions sont connectées –voir section 3.2.4.5– et qu'on utilise une source d'alimentation PoE).
- **Prévisualisation en direct:** permet d'avoir une prévisualisation de la caméra avec la configuration sélectionnée.

3.2.4.3 RÉTRO-ÉCLAIRAGE

Le Zennio GetFace IP permet de limiter l'intensité de l'éclairage du dispositif et de la led de signalisation en fonction du mode jour/nuit. De la même façon, dans cet onglet on peut vérifier la valeur actuelle.

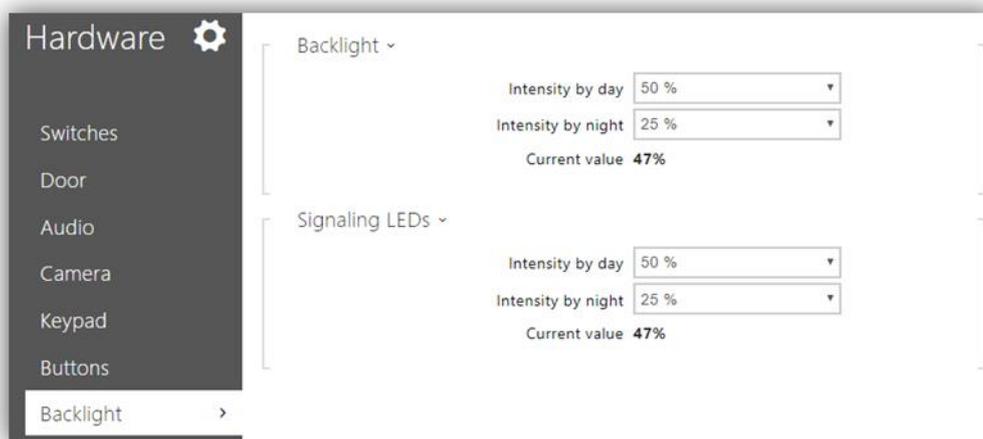


Figure 44 Rétro-éclairage

3.2.4.4 ENTRÉES LOGIQUES

Dans cet onglet, on configure les paramètres associés aux entrées logiques.

- **Contrôle d'état sécurisé:** détermine laquelle des entrées sera utilisée pour détecter l'état de sécurité, qui sera indiqué au moyen d'une led du Zennio GetFace IP. Ce paramètre peut être appliqué pour le contrôle de boutons poussoir pour ouvrir une porte. En **Mode d'entrée** on définit si l'entrée est inversée ou non.
- **Interrupteur Tamper:** détermine quel module ZVP-INOUT sera utilisé comme interrupteur de sabotage (Tamper Switch).

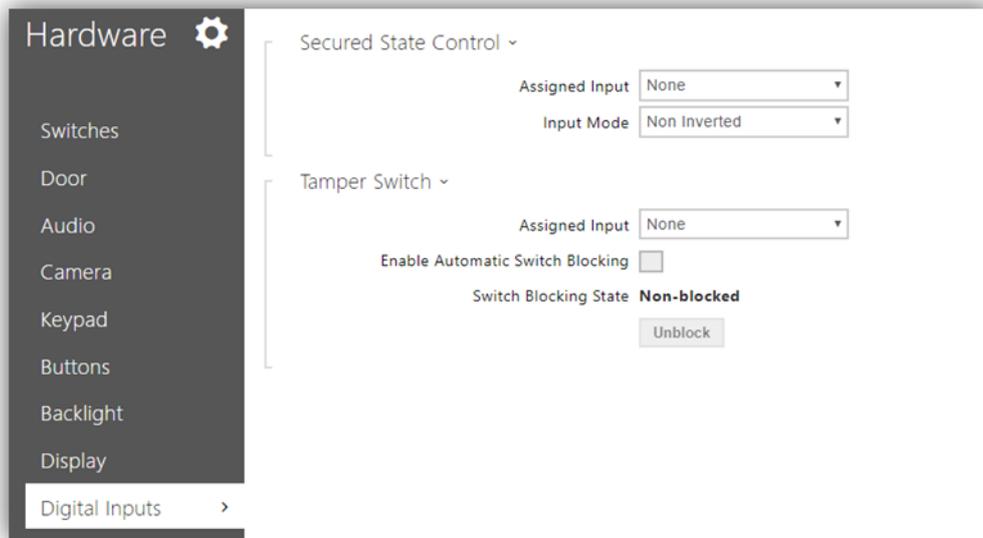


Figure 45 Entrées logiques.

3.2.4.5 PROLONGATEURS

Dans cet onglet les modules connectés à l'unité basique sont affichés. Les modules sont connectés en série, donc ils prendront une référence correspondant à la position qu'ils occupent. L'unité basique, étant un module spécial, prendra la valeur 0.

3.2.5 SYSTÈME

La configuration générale du dispositif est établie dans les onglets suivants:

3.2.5.1 RÉSEAU

Dans cet onglet, on configure les paramètres relatifs à l'interface de réseau.

BASIQUE

Le Zennio GetFace IP fonctionne par défaut avec une IP statique. Cependant, il est possible de le configurer pour qu'il fonctionne au moyen d'un **serveur DHCP**.

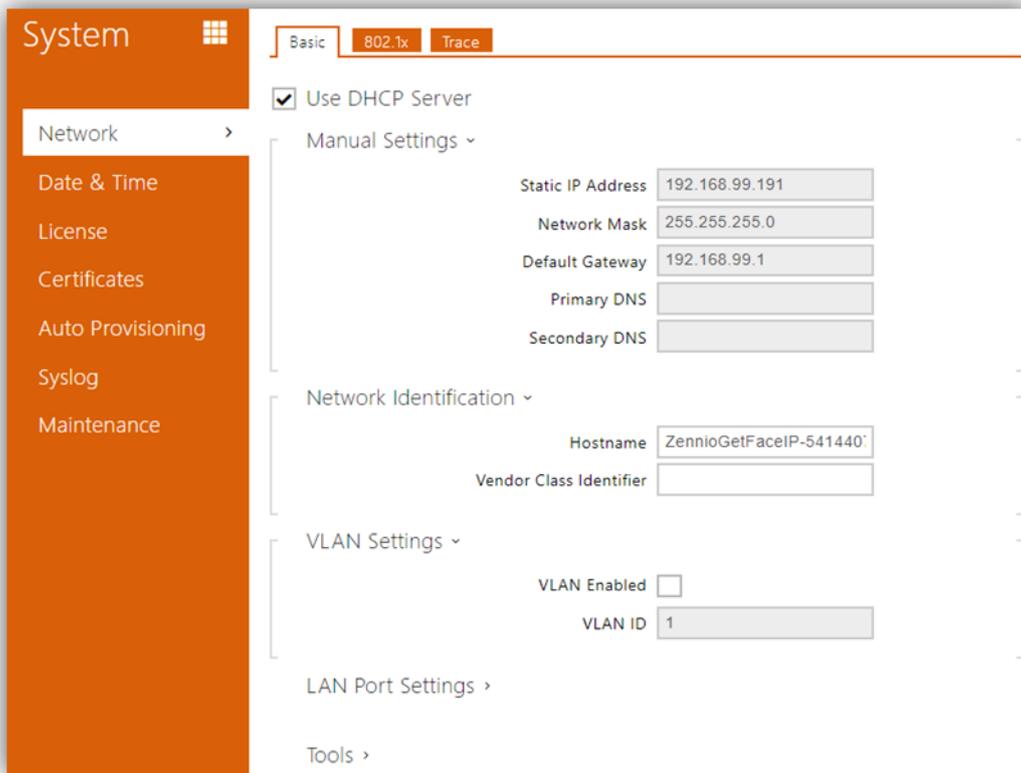


Figure 46 Système.

Avec l'option DHCP désactivée, on peut configurer:

- **Paramètres manuels:** permet de définir manuellement une IP statique, le masque de réseau et la passerelle par défaut. On peut aussi établir un serveur DNS primaire et un secondaire.
- **Identification dans le réseau:** assigne un nom de réseau au dispositif (optionnel).
- **Paramètres de VLAN:** permet d'activer un réseau virtuel (VLAN).
- **Paramètres LAN:** établit le mode de port souhaité (automatique ou semi-duplex).
- **Instruments:** permet de vérifier l'état du réseau et du dispositif ainsi que la latence des réponses.

Dans le cas d'avoir **activé le serveur DHCP**, la configuration manuelle des réglages de réseau est bloquée.

3.2.5.2 DATE ET HEURE

Dans cet onglet, on configure la date et l'heure du dispositif.

Il est possible de synchroniser la date et l'heure avec le navigateur du PC. Lorsque la synchronisation est faite, le paramètre **Zone horaire** définit le fuseau horaire du Zennio GetFace IP, de façon à être tenu en compte lors des changements d'heures d'été et d'hiver.

Il est aussi possible de définir manuellement les règles horaires au moyen du paramètre **Règle de zone horaire**.

Enfin, il est possible de définir un **serveur NTP** pour synchroniser l'heure du dispositif avec celle d'un serveur NTP Internet, dont l'URL ou l'IP devra être spécifiée.

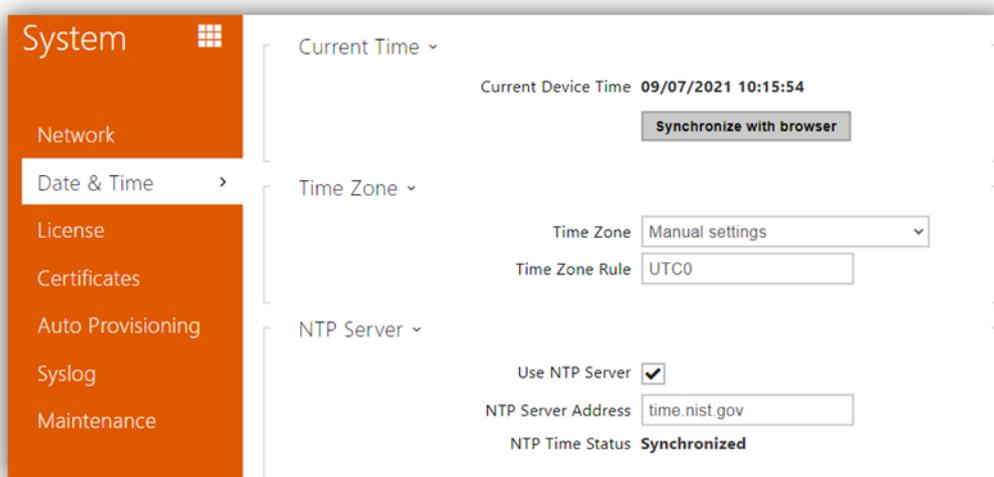


Figure 47 Date et heure.

3.2.5.3 APPROVISIONNEMENT

Il est recommandé de désactiver l'actualisation du firmware, ainsi comme de la configuration. Il est conseillé de réaliser cette actualisation manuellement pour le faire de façon contrôlée et pouvoir réaliser une copie de sécurité avant les actualisations, de manière que se gardent des configurations et n'affecte pas au fonctionnement normal de l'unité (voir section 3.2.5.4 pour plus de détails).

Pour cela, décocher les cases "d'Actualisation du firmware habilité" et "Actualisation de la configuration habilitée" dans les onglets Firmware et Configuration, respectivement.

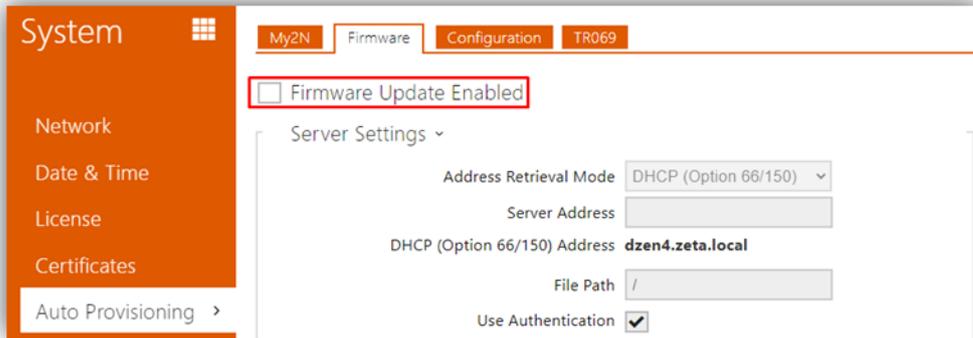


Figure 48 Approvisionnement

3.2.5.4 MAINTENANCE

Cet onglet permet de mener à bien les opérations générales de maintenance du dispositif. Il proportionne aussi une information générale sur le dispositif.

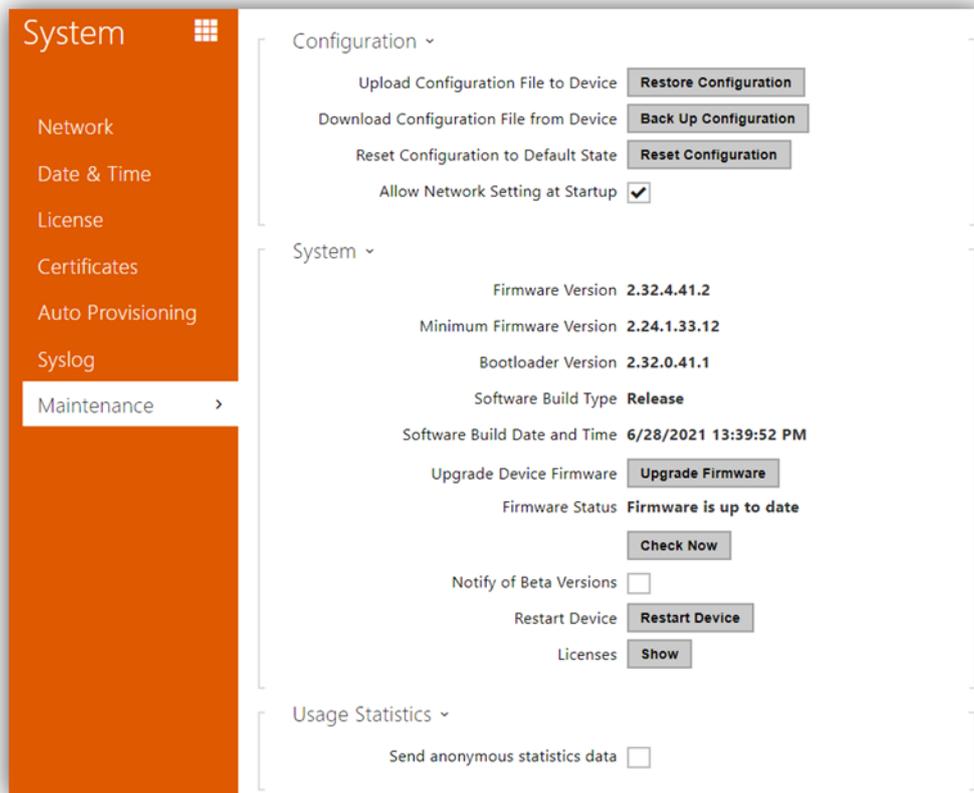


Figure 49 Maintenance

Les principales actions qui peuvent se réaliser sont:

- **Restaurer la configuration:** Charger la configuration générale depuis un fichier de sauvegarde ou *backup*.

Important : avant de restaurer la configuration il est recommandé de **réaliser une copie de sécurité de la configuration actuelle** ("Garder la configuration").

Il est possible de choisir seulement charger certaines parties de la configuration:

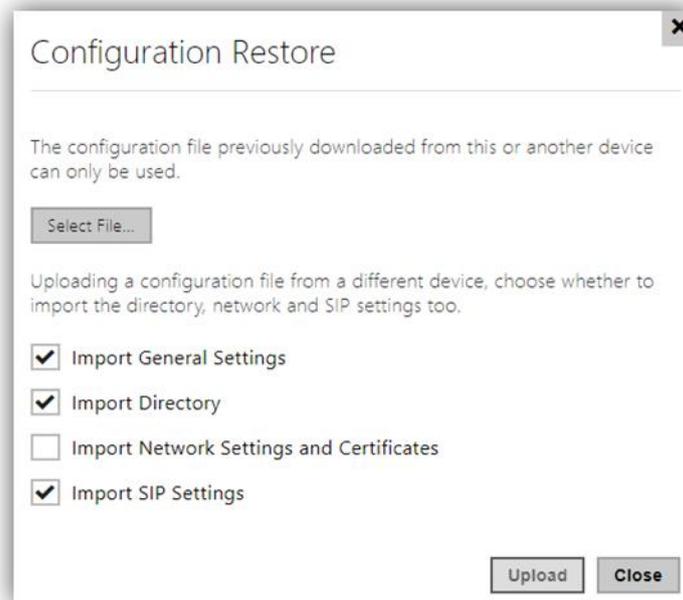


Figure 50 Restauration de la configuration.

- **Garder la configuration:** Télécharger la configuration actuelle sur un fichier de sauvegarde.
- **Rétablir la configuration** du Zennio GetFace IP aux valeurs par défaut de fabrique.
- **Actualiser le firmware** manuellement depuis une archive.

Important :

- avant d'actualiser le firmware il est recommandé de **réaliser une copie de sécurité de la configuration actuelle** ("Garder la configuration").
- Consultez Zennio avant d'actualiser le *firmware* à une version différente à celle indiquée au début de ce manuel.

Venez poser vos questions
sur les dispositifs Zennio :
<https://support.zennio.com>

Zennio Avance y Tecnología S.L.
C/ Río Jarama, 132. Nave P-8.11
45007 Toledo (Espagne).

Tél.: +33 (0)1 76 54 09 27 et +34 925 232 002.

www.zennio.fr
info@zennio.fr