Manuel de Configuration des Interphones IP 2N

v.2.43

www.2n.com

Contenu:

1. Vue d'ensemble du produit

Les **Interphones IP 2N** peuvent intelligemment remplacer les sonnettes de porte traditionnelles, les platines à boutons poussoirs et haut-parleur ou tout autre interphone filaire dans les bâtiments équipés du câblage adéquat. Nos portiers offrent des services plus avancés et plus étendus que les interphones résidentiels standard. L'installation est très simple. Il vous suffit de connecter l'interphone au réseau local à l'aide d'un câble UTP et de définir les paramètres nécessaires.

Grâce au protocole SIP intégré, l'interphone peut utiliser tous les services VoIP : renvoi d'appel en absence (vers un autre bureau, une messagerie vocale ou un téléphone cellulaire) ou bien transfert d'appel (du secrétariat vers l'interlocuteur souhaité par le visiteur, par exemple).

Les interphones sont équipés d'un nombre programmable de boutons de numérotation rapide pour des appels vers les utilisateurs dont les numéros figurent dans la liste de contacts. Chacun de ces utilisateurs peut se voir assigner jusqu'à 3 numéros pouvant être composés en parallèle ou bien de manière séquentielle. Grâce à une feuille de temps intégrée, il est possible de configurer chacun des numéros de manière à ce que la personne appelée soit toujours joignable et/ou que les appels vers les numéros de téléphone sélectionnés puissent être restreints selon des plages horaires configurables.

Certains des **Interphones IP 2N** peuvent être équipés de claviers numériques pouvant être utilisés pour les codes de déverrouillage ou bien pour composer un numéro de poste précis.

Les **Interphones IP 2N** permettent aux utilisateurs du réseau local de visualiser la zone située devant la caméra via un flux vidéo. Grâce au support complet d'ONVIF, les interphones 2N peuvent faire partie intégrante du système de surveillance vidéo de votre établissement.

Les **Interphones IP 2N** peuvent être équipés d'un lecteur de carte RFID pour le contrôle d'accès et deviennent ainsi un élément clé de vos systèmes de surveillance ou de contrôle d'accès au bâtiment.

Les **Interphone IP 2N** sont équipés de commutateurs à relais (et, il est possible d'ajouter d'autres relais supplémentaires), qui commande la serrure électrique ou un autre équipement connecté à l'interphone. Quand et comment il s'active, tout cela peut être programmées de manière très flexible : il peut être activé par un code, une carte RFID, automatiquement par un appel, en appuyant sur une touche…etc. Il est toujours recommandé d'utiliser le Relais de sécurité 2N® (Part No. 9159010) pour accroître la sécurité.

Les symboles et pictogrammes suivants sont utilisés dans le mode d'emploi.

Risque d'accident

- **Respectez toujours** ces consignes pour écarter un risque d'accident.

Avertissement

- **Respectez toujours** ces consignes pour éviter d'endommager l'appareil.

Observation

- **Observation importante.** Le non-respect des consignes peut entraîner un dysfonctionnement de l'appareil.

Conseil

- **Informations utiles** pour un fonctionnement ou un réglage plus facile et plus rapide.

Note

- Procédés et conseils pour profiter de manière efficace des caractéristiques de l'appareil.

2. Guide express pour la configuration de base

Paramètres de connexion réseau (LAN)

Vous devez connaître l'adresse IP de l'Interphone pour pouvoir vous connecter avec succès à son interface de configuration. **L'Interphone 2N** est configuré par défaut pour récupérer automatiquement une adresse IP depuis u, serveur DHCP. Ainsi, si vous êtes connecté à un réseau disposant d'un serveur DHCP, votre interphone se verra directement attribué une adresse IP. L'adresse IP de l'interphone peut être trouvée dans l'état du serveur DHCP (selon l'adresse MAC indiquée sur la plaque de production), ou bien elle vous sera communiquée par la fonction vocale de l'interphone. Pour cela, reportez-vous au manuel d'installation de votre modèle.

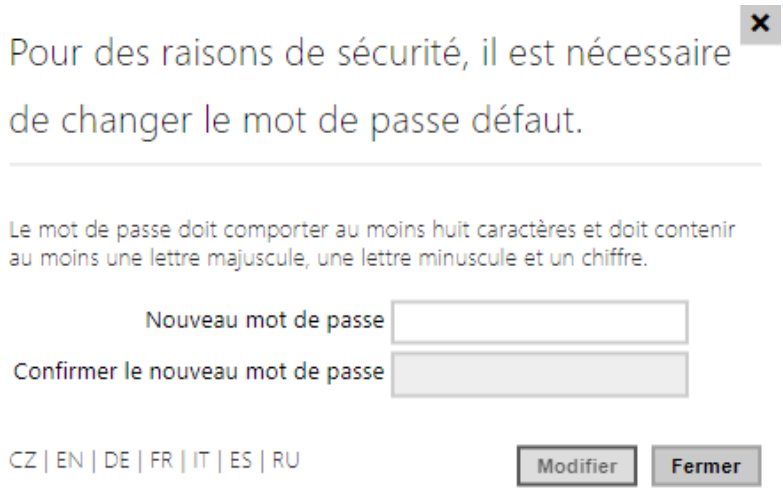
S'il n'y a pas de serveur DHCP sur votre réseau local, utilisez les boutons d'interphone pour définir le mode d'adresse IP statique. Reportez-vous pour cela au manuel d'installation de votre modèle. Votre Interphone prendra alors l'adresse IP **192.168.1.100**. Utilisez-la pour votre première connexion puis changez-la si nécessaire.

Maintenant, entrez l'adresse IP de l'interphone dans votre navigateur préféré. Nous vous recommandons d'utiliser les dernières versions de Chrome, Firefox ou Internet Explorer 9+, car **l'interphone IP 2N** n'est pas totalement compatible avec les versions de navigateur antérieure.

Utilisez le nom **admin** et le mot de passe **2n** (mot de passe par défaut) pour votre première connexion à l'interface de configuration.

Nous vous recommandons de changer le mot de passe pour plus de sécurité.

L'Interphone vous demandera de le changer à la première connexion. Le mot de passe doit contenir au moins 8 caractères dont au moins une lettre majuscule, une lettre minuscule et un nombre.



Choisissez un mot de passe dont vous vous souviendrez ou notez-le quelque part car si vous l'oubliez, il vous faudra réinitialiser l'appareil aux paramètres d'usine (pour cela, référez-vous au manuel d'installation de votre interphone) et vous perdrez toute configuration existante.

Conseil

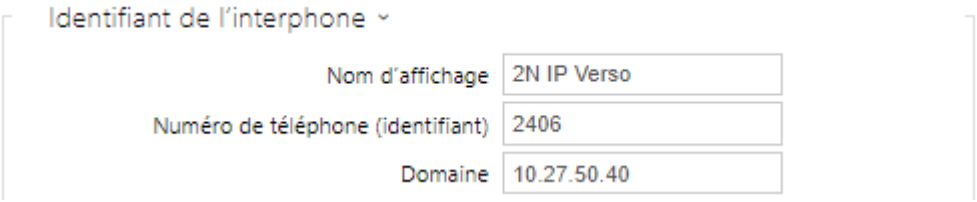
- FAQ : Adresse IP – Comment obtenir l'adresse IP d'un Interphone IP 2N

Mise à jour du Firmware

Nous vous recommandons également de mettre à jour le firmware de votre interphone lors de votre première connexion. Pour obtenir la dernière version, référez-vous au site internet 2N : www.2n.cz. Pour passer au nouveau firmware, pressez le bouton de **Mise à jour Firmware** dans la section **Système / Maintenance**. L'Interphone se redémarrera pendant la mise à jour et seulement après, le processus de mise à jour sera complété. La mise à jour complète prend environ 30 secondes.

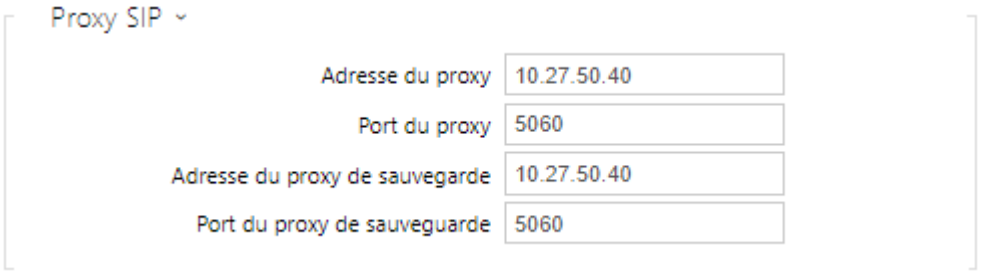
Paramètres de connexion à un Serveur SIP

Définissez les paramètres suivants dans le menu **Services / Téléphone / SIP** pour permettre à votre interphone de passer des appels et d'être accessible au sein de votre infrastructure VoIP.

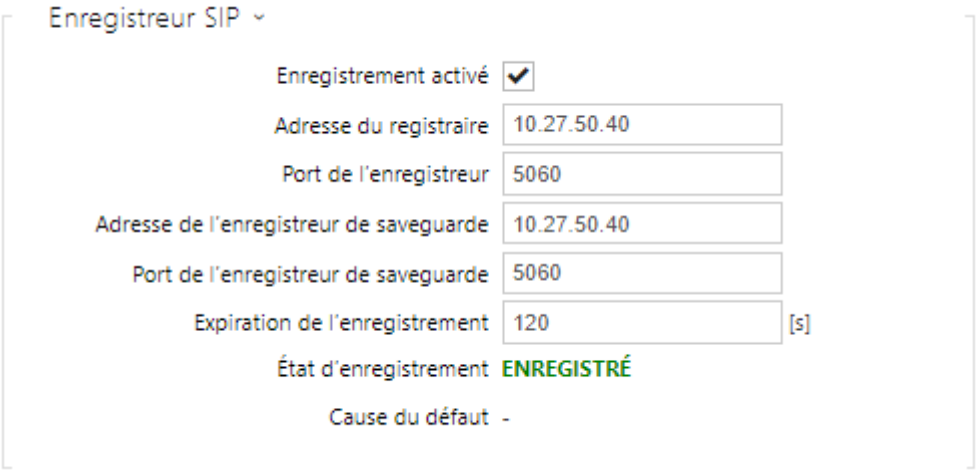


- **Nom d'affichage** – définissez le nom à afficher sur le téléphone de correspondant, dans la fenêtre de connexion et sur la page de démarrage de l'interface Web.
- **Numéro de téléphone (ID)** – définissez le numéro de téléphone de l'interphone (ou un autre ID unique composé de caractères et de chiffres) pour identifier l'interphone de manière unique dans les journaux d'appels et les enregistrements.
- **Domaine** – définissez le nom de domaine du service avec lequel l'interphone est enregistré. En règle générale, cette adresse est équivalente à l'adresse du proxy SIP ou du registrar. Si vous n'utilisez pas de proxy SIP dans votre installation d'interphonie, entrez l'adresse IP de l'interphone.
- **Appel d'essai** – affichez une fenêtre de dialogue vous permettant de faire un test d'appel vers un numéro de téléphone sélectionné, voir ci-dessous.

Si vous utilisez un serveur SIP (Proxy, Registrar), définissez les adresses pour les éléments de réseau suivants :



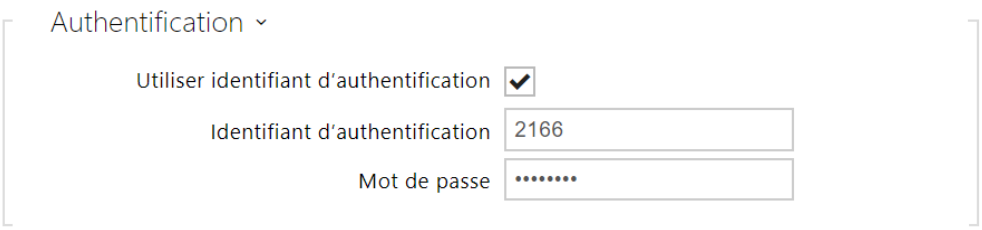
- **Adresse du proxy** – définissez l'adresse IP du proxy SIP ou le nom de domaine.
- **Port du proxy** – définissez le port du proxy SIP (généralement 5060).
- **Adresse du proxy de sauvegarde** – définissez l'adresse IP du proxy SIP ou le nom de domaine à utiliser lorsque le proxy principal ne répond pas aux requêtes.
- **Port du Proxy de sauvegarde** – définissez le port du proxy SIP (généralement 5060).



- **Enregistrement activé** – activez l'enregistrement de l'Interphone pour le registrar SIP défini.
- **Adresse du registrar** – définissez l'adresse IP ou le nom de domaine du registrar SIP.
- **Port du registrar** – définissez le port du registrar SIP (généralement 5060).
- **Adresse du registrar de sauvegarde** – définissez l'adresse IP ou le nom de domaine du registrar SIP à utiliser lorsque le registrar principal ne répond pas aux requêtes.
- **Port du registrar de sauvegarde** – définissez le port de registrar SIP de sauvegarde (généralement 5060).
- **Expiration de l'enregistrement** – définissez l'expiration de l'enregistrement, qui affecte le réseau et la charge du bureau d'enregistrement SIP, en fonction des exigences d'enregistrement régulièrement envoyées. Le registrar SIP peut modifier la limite d'expiration sans vous en informer.
- **Etat d'enregistrement** – affiche l'état actuel d'enregistrement (non enregistré, enregistrement, enregistré…).

- **Cause du défaut** – affiche le motif de l'échec de la dernière tentative d'enregistrement : la dernière réponse d'erreur du registrar, par exemple. 404 introuvable.

Si votre serveur SIP requiert l'authentification de l'équipement terminal, entrez les paramètres suivants :

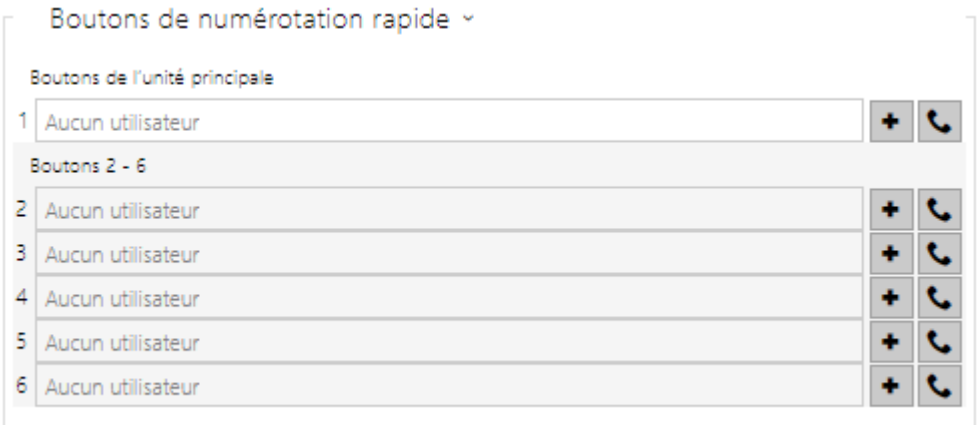


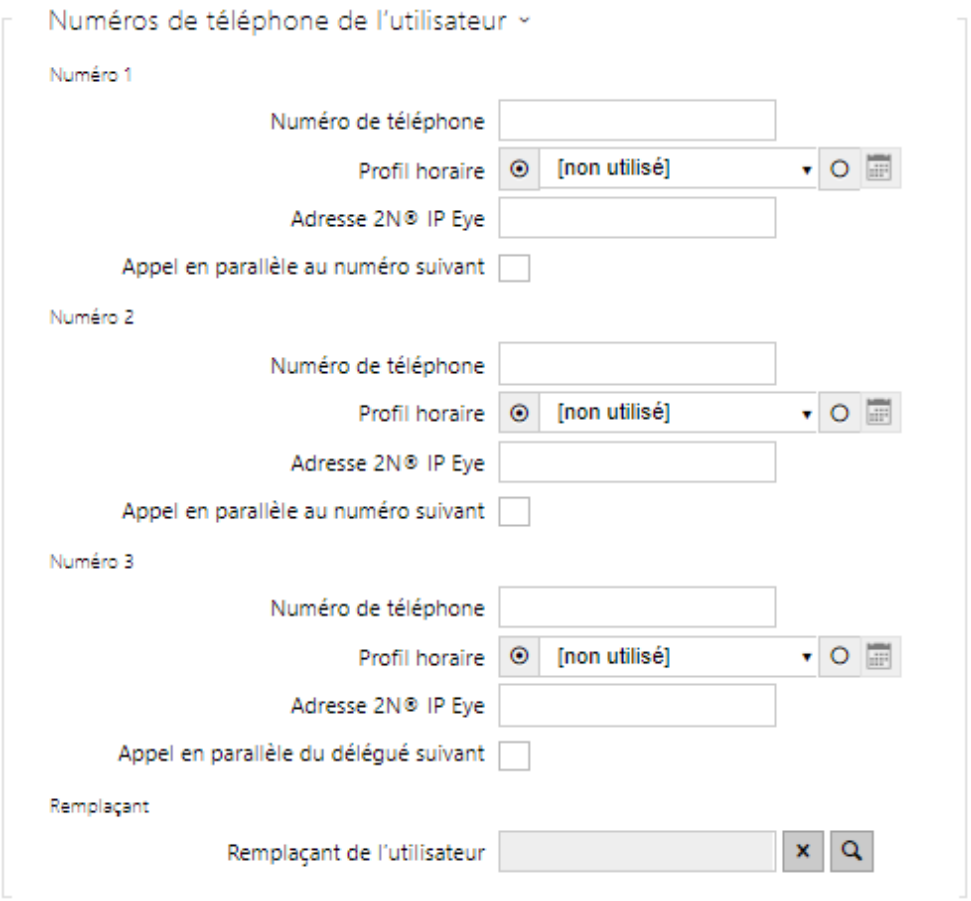
- **Mot de passe** – entrez le mot de passe pour identifier l'Interphone.

Paramétrage des boutons d'appel rapide

Tous les modèles **d'interphones IP 2N** sont équipés de boutons de numérotation rapide. Si vous appuyez sur l'un des boutons, un appel sera lancé vers le numéro de téléphone attribué à l'utilisateur présent dans la liste de contact.

Dans la section **Hardware / Boutons**, est affiché la liste de tous les boutons potentiellement disponibles sur le modèle d'Interphone. Dans certains modèles d'interphone (**2N® IP Vario**, **2N® IP Verso**), la liste des boutons est divisée en groupes de 8 ou de 5 correspondants aux modules d'extension des boutons. Cliquez sur  , sélectionnez l'utilisateur puis appuyez sur ajouter pour ajouter un nouvel utilisateur dans le champ d'édition du bouton. Pour rechercher un utilisateur dans la liste, utilisez le champ de texte intégral pour rentrer le nom. Il est possible d'attribuer plusieurs utilisateurs pour un même bouton d'appel.

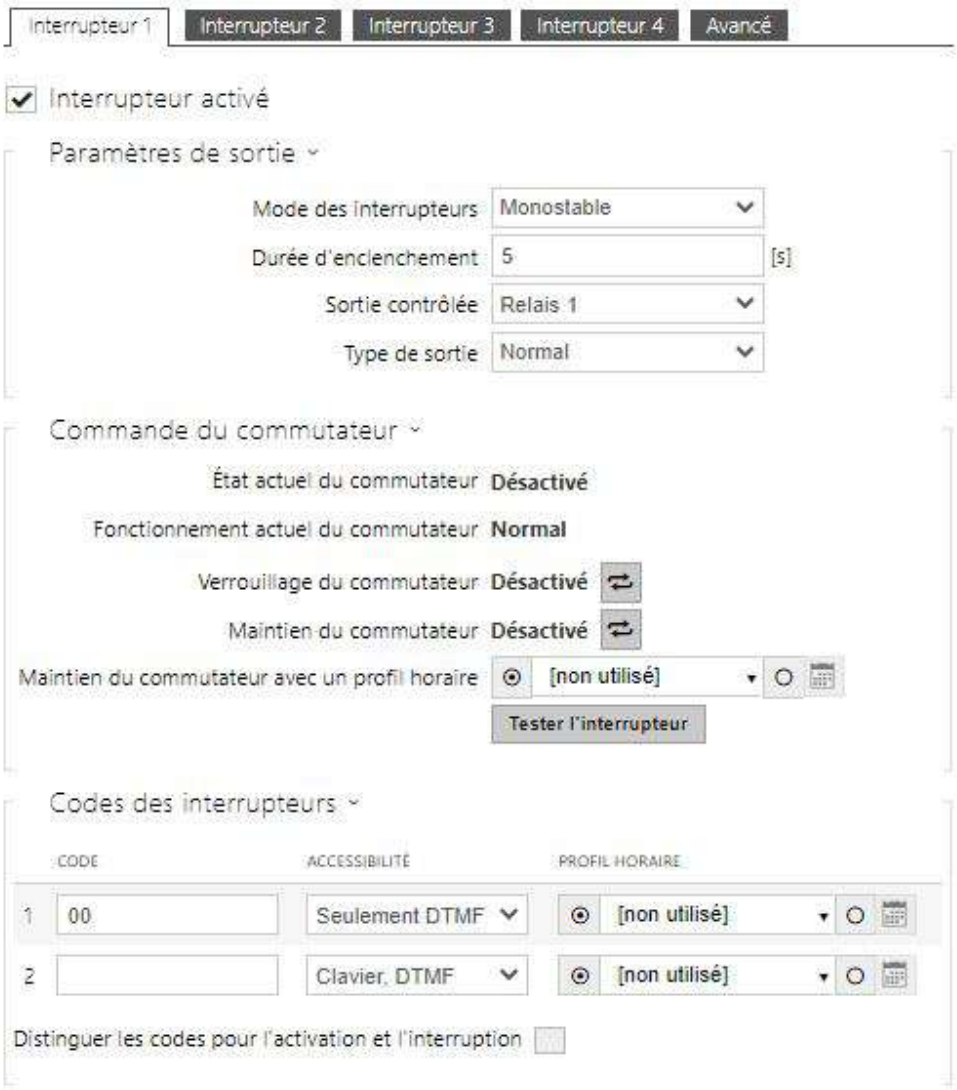




Vous pouvez également utiliser **l'interphone IP 2N** avec un ou plusieurs téléphones IP sans serveur SIP. Utilisez l'appel direct SIP pour les appels sortants et entrez l'adresse SIP du téléphone appelé (sip :phone_number@phone_ip_address) au lieu du numéro d'extension.

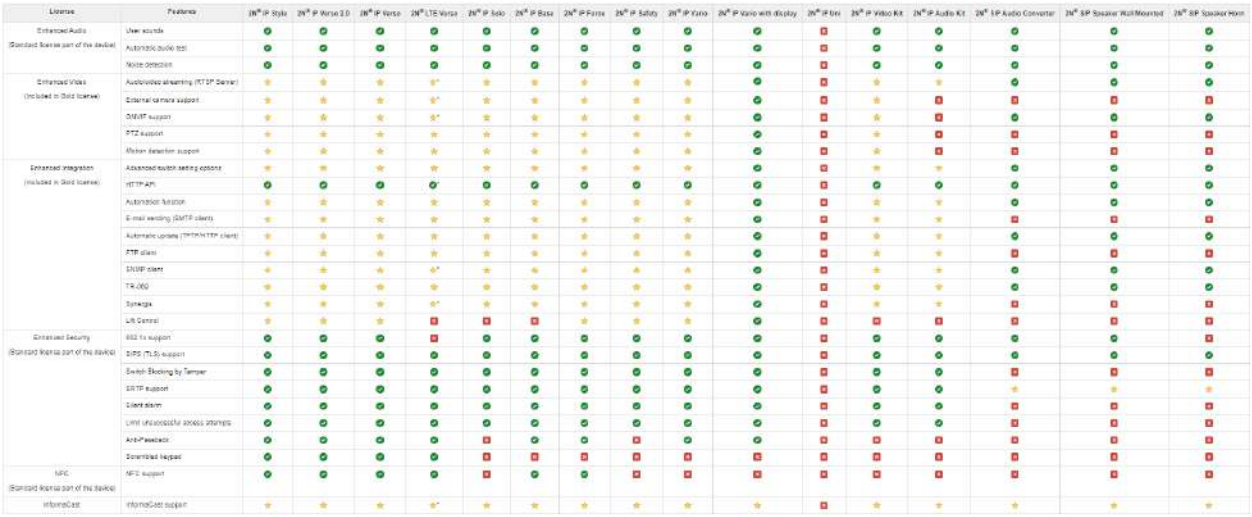
Réglage des interrupteurs de déverrouillage électrique

Une serrure électrique peut être connectée aux **interphones IP 2N** et contrôlée par un code du clavier numérique de l'interphone ou un code du clavier du téléphone IP (DTMF) pendant un appel. Connectez la serrure électrique comme indiqué dans le manuel d'installation de votre modèle d'interphone.



Activez l'interrupteur en cochant le paramètre Interrupteur activé dans la section **Hardware / Interrupteur / Interrupteur 1**, réglez la sortie de l'interphone contrôlée par l'interrupteur c'est à dire celle à laquelle la gâche électrique ou la ventouse est connectée. Définissez maintenant un ou plusieurs codes d'activation pour la commutation du verrouillage électrique des portes.

3. Différents modèles et fonctionnalités sous licences



✅ – Fonctionnalité native
⭐ – Fonctionnalité sous licence à acheter séparément

❌ – Indisponibles

*) La disponibilité du service dépend de la configuration réseau du fournisseur de téléphonie mobile.

> ⚠ **Observation**
>
> - Les licences ne s'appliquent pas aux Etats-Unis, Canada, Mexique, Caraïbes, Amérique Centrale et Amérique du Sud.

3.1 Différence de modèle

Ce manuel est valable pour tous les membres de la famille **d'interphones IP 2N**. Par conséquent, certaines des fonctionnalités qu'il décrit ne sont disponibles que dans certains modèles d'interphone IP 2N ou doivent être activées avec une clé de licence valide. Cette section fournit une courte liste des différences entre les modèles et les licences qui affectent les options de configuration. Si une fonction n'est pas disponible dans tous les modèles, il y a une note dans la sous-section respective et une référence à cette section.

Le tableau ci-dessous donne un aperçu des propriétés et des fonctions de tous les modèles **d'interphone IP 2N**.

Modèle d'Interphone	2N® IP Style	2N® IP Verso 2.0	2N® IP Verso	2N® IP Base	2N® IP Solo	2N® IP Vario	2N® IP Force	2N® IP Safety	2N® IP Uni	2N® IP Audio Kit	2N® IP Video Kit
Numéro de référence.	9157...	91552...	9155…	9156...	91553...C	9137….	9151…	9152…	9153…	9154…	9154…C
Processeur Artpec-7	Oui		Non								
Caméra Intégrée	Oui		Au choix	Oui		Au choix		Non			
Résolution de la caméra	2560 x 1920	1920 x 1440	1280 x 960			640 x 480	640 x 480 ou 1280 x 960				
Support Caméra Analogue Externe	Non										Oui
Support Caméra IP Externe	Oui								Non		Oui
Lecteur de carte RFID interne	Oui	En option			Non	En option		Non			
Ecran d'affichage	Oui	En option		Non		En option		Non			

Modèle d'Interphone	2N® IP Style	2N® IP Verso 2.0	2N® IP Verso	2N® IP Base	2N® IP Solo	2N® IP Vario	2N® IP Force	2N® IP Safety	2N® IP Uni	2N® IP Audio Kit	2N® IP Video Kit
Interrupteurs supplémentaires	Oui	Non	En option						Non		
Nombre de boutons sur l'unité principale	0	1		1 ou 2	1	1, 3 ou 6	1, 2 ou 4	1	1 ou 2	jusqu'à 16 boutons externes programmables	
Module d'extension de boutons	0	jusqu'à 145		Non		jusqu'à 48	Non				
Clavier numérique	Oui	En option		Non		En option		Non			
Entrée logique	Oui					En option			Non	2	
Codec audio Large bande(L16, G.722)	Oui								Non		Oui
Puissance de l'amplificateur	4 W	2 W				150 mW	10 W			10 W	
Gain du microphone réglable	Non									Oui	
Puissance de sortie étendue de l'amplificateur (10W)	Non						Oui		Non	Non	

Modèle d'Interphone	2N® IP Style	2N® IP Verso 2.0	2N® IP Verso	2N® IP Base	2N® IP Solo	2N® IP Vario	2N® IP Force	2N® IP Safety	2N® IP Uni	2N® IP Audio Kit	2N® IP Video Kit
Commutateur d'autoprotection	Oui	En option		Oui		Non	En option		Oui	Non	
Nombre d'utilisateurs possible	10 000								2	16	
Utilisateur remplaçant	Oui								Non	Oui	
Nombre d'interrupteurs contrôlables	4			2	4				1	4	
Nombre de codes universels	10			2	10				2	10	
Nombre de profils utilisateurs	20										
JPEG HTTP video	Oui							Non			Oui
Support **2N® IP Eye**	Oui							Non			Oui
Mode Téléphone	Oui			Non		Oui		Non		Oui	

Certaines fonctions **des interphones IP 2N** sont disponibles uniquement sous licences (voir la sous-section Licence).

3.2 Fonctionnalités sous licences

Licences de fonctionnalité

Pour une utilisation courante de l'interphone IP 2N, les licences de base qui sont déjà incluses avec l'appareil en usine sont suffisantes. Les interphones 2N IP peuvent être complétés par des fonctions supplémentaires, qui nécessitent une licence payante.

Types de licences

Certaines fonctionnalités des **Interphones IP 2N** ne sont pas disponibles jusqu'à ce qu'une clé de licence valide soit entrée (voir la sous-section Licences). Voici les types de licences disponibles:

- NFC (fait partie de l'appareil)
- Enhanced Audio (fait partie de l'appareil)
- Enhanced Security (fait partie de l'appareil)
- Gold (Part No. 9137909)
- InformaCast (Part No. 9137910, Axis Part No. 01381-001)

Note

- La licence InformaCast permet l'utilisation du protocole SingleWire InformaCast.

Les portiers **2N® IP Style, Verso**, **Base**, **Solo**, **Vario**, **Force**, **Safety** et les **Audio Kit** et **Video Kit** supportent les fonctions liées aux licences. Aucune licence n'est disponible pour le modèle **2N® IP Uni**.

Conseil

- Référez-vous à la section 3. Différents modèles et fonctionnalités sous licences

Le tableau ci-dessous liste les fonctionnalités devant être activées par les clés de licence correspondant aux licences mentionnées ci-dessus. Les licences peuvent être combinées arbitrairement.

Fonction	Enhanced Audio	Enhanced Video	Enhanced Integration	Enhanced Security	NFC	InformaCast	IP intercoms Lift module license	Licence
Sons personnalisables	•							fait partie de l'appareil
Test automatique boucle audio	•							fait partie de l'appareil
Détection de bruit	•							fait partie de l'appareil
Flux Audio/video (Serveur RTSP)		•						GOLD
Support Caméra IP Externe		•						GOLD
Support ONVIF		•						GOLD
Fonctionnalité PTZ		•						GOLD
Détection de mouvement		•						GOLD
Options avancées du Contrôle des Interrupteurs			•					GOLD
HTTP API (voir notes ci-dessous)			•					fait partie de l'appareil
Fonctionnalités d'Automatisation			•					GOLD

Fonction	Enhanced Audio	Enhanced Video	Enhanced Integration	Enhanced Security	NFC	InformaCast	IP intercoms Lift module license	Licence
Envoi d'E-mail (Serveur SMTP)			•					GOLD
Mise à jour automatique (Client TFTP/ HTTP)			•					GOLD
Client FTP			•					GOLD
Client SNMP			•					GOLD
TR-069			•					GOLD
Support 802.1x				•				fait partie de l'appareil
Support SIPS (TLS)				•				fait partie de l'appareil
Support SRTP				•				fait partie de l'appareil
Alarme silencieuse				•				fait partie de l'appareil
Limite des tentatives d'accès non-autorisées				•				fait partie de l'appareil

Fonction	Enhanced Audio	Enhanced Video	Enhanced Integration	Enhanced Security	NFC	InformaCast	IP intercoms Lift module license	Licence
Blocage des Interrupteurs				•				fait partie de l'appareil
Clavier Brouillé				•				fait partie de l'appareil
Support NFC					•			fait partie de l'appareil
Support InformaCast						•		InformaCast
Anti-passback				•				fait partie de l'appareil
Genetec Synergis			•					GOLD
Contrôle de l'ascenseur							•	GOLD
IP relais			•					GOLD

Quels autres produits suivent ce schéma de licences ?

Les produits **2N® SIP Audio Converter**, **2N® SIP Speaker** et **2N® SIP Speaker Horn** intègre une licence GOLD par défaut et la seule amélioration possible est donc la licence InformaCast.

Comment se procurer les licences ?

Les licences sont générées par 2N en fonction du numéro de série de l'appareil. Après avoir décidé de la licence que vous souhaitez, vous devez récupérer le numéro de série de votre unité et contacter votre distributeur pour obtenir la clé de licence.

La licence elle-même est fournie sous forme de clé alphanumérique. Elle peut donc être facilement envoyée par courrier électronique et copiée-collée dans l'interphone.

Les licences ne sont pas limitées dans le temps. Une fois que vous avez une licence, vous l'avez pour de bon.

Pour activer la licence, vous devez vous connecter à l'interface Web de l'interphone et coller la clé de licence dans le champ Système / Licence. Lorsque vous cliquez sur Enregistrer, les fonctionnalités sous licence sont immédiatement activées.

Les licences peuvent être téléchargées automatiquement dans le menu Système / Licence.

Conseil

FAQ: Les licences pour les Interphones IP 2N – Comment les obtenir ?

Puis-je avoir un licence de démo ?

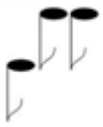
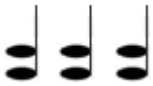
Oui, il existe une option pour une période de licence Gold d'essai de 800 heures au cours de laquelle vous pouvez essayer les fonctionnalités sous licence. Par défaut, cette démo est désactivée – activez-la via l'interface Web de votre interphone dans le menu Système / Licence. Un compte à rebours indique le temps restant après lequel toutes les fonctionnalités sous licence seront à nouveau désactivées.

Il n'y a pas de licence d'essai pour la licence InformaCast.

4. Signalisation du statut opérationnel

Les **Interphones IP 2N** génèrent des sons pour signaler la commutation et les modifications des états de fonctionnement. Chaque changement d'état se voit attribuer un type de tonalité différent. Voir le tableau ci-dessous pour la liste des signaux.

> **Note**
>
> - *La signalisation de certains des états mentionnés ci-dessous peut être modifiée; reportez-vous à la sous-section Sons utilisateurs.*

Tones	Significations
	**Signalisation confirmant le prolongement de l'appel. Les appels sont limités dans le temps sur les Interphone IP 2N** pour des raisons de sécurité (protection contre le blocage). Référez-vous la sous section Divers pour plus de détails.
	**Application Interne** lancée. L'application interne est lancée à la mise sous tension ou au redémarrage de **l'interphone IP 2N**. Un lancement réussi est signalé par cette combinaison de tonalités.
	**Connecté au LAN, Adresse IP** attribuée à l'interphone IP 2N. Une connexion réussie au réseau local est signalée par cette combinaison de tonalités.
	**Déconnecté du LAN, adresse IP perdue** Cette combinaison de tonalités signale la déconnexion du câble UTP de l'unité 2N.
	**Numéro de téléphone invalide ou code d'activation de commutateur invalide** Les **Interphone IP 2N** permettent à l'utilisateur de composer un numéro de poste directement à l'aide du clavier ou d'entrer le code de déverrouillage de la porte. Un code invalide est signalé par cette séquence de tonalités.

	**Réinitialisation par défaut des paramètres réseau** À la mise sous tension, un délai de 30 s est défini pour la saisie du code de réinitialisation par défaut. Reportez-vous à la sous-section Configuration du périphérique du Manuel d'installation de votre interphone IP 2N pour plus de détails.
	Signalisation de fin d'appel **L'interphone IP 2N** permet à l'utilisateur de définir un délai de fin d'appel pour éviter le blocage d'appels. Appuyez sur une touche de votre téléphone VoIP pour prolonger la durée de l'appel pendant ce délai. Le paramètre de délai d'attente a pour but d'éviter le blocage d'appels (sur un répondeur par exemple).
	**Connecté au Téléphone IP** Cette tonalité courte signale la connexion réussie entre un téléphone VoIP et **l'interphone IP 2N**.

5. Configuration de l'Interphone

Se connecter à l’interface de configuration web

L’appareil est configuré à l’aide de l'interface de configuration web. Vous devez connaître l’adresse IP ou le nom de domaine de l’appareil pour y accéder. L’appareil doit être connecté au réseau IP local et doit être alimenté.

Nom de domaine

Il est possible de se connecter à l’appareil en saisissant le nom de domaine au format hostname.local (par ex. 2NIPStyle-00000001.local). Le hostname du nouvel appareil se compose du nom de l’appareil et de son numéro de série. Les formats des noms des appareils dans hostname sont indiqués ci-dessous. Le numéro de série est saisi dans le nom de domaine sans trait d’union. Le hostname peut être modifié ultérieurement dans la section Système > Réseau.

Appareil 2N	Nom de l’appareil dans Hostname
2N IP Verso	2NIPVerso
2N IP Verso 2.0	2NIPVerso20

Appareil 2N	Nom de l’appareil dans Hostname
2N LTE Verso	2NLTEVerso
2N IP Style	2NIPStyle
2N IP One	2NIPOne
2N IP Vario	2NIPVario
2N IP Base	2NIPBase
2N IP Force	2NIPForce
2N IP Safety	2NIPSafety
2N IP Solo	2NIPSolo
2N IP Uni	2NIPUni

Se connecter à l’aide d’un nom de domaine présente l’avantage d’utiliser l’adresse IP dynamique de l’appareil. Tandis que l’adresse IP dynamique change, le nom de domaine reste le même. Des certificats signés par une autorité de certification de confiance peuvent être générés pour un nom de domaine.

Ecran de démarrage

L'écran de démarrage est une page d'accueil présentant une vue d'ensemble des différentes sections lors de la connexion à l'interface Web de l'interphone. Utilisez la flèche de retour dans le coin supérieur gauche des autres pages de l'interface Web pour retourner sur ce menu à tout moment. L'entête de cette page indique le nom du modèle de l'Interphone (référez-vous aux paramètres d'affichage du nom dans la section **Services / Téléphone / SIP**). Vous pouvez utiliser le menu situé dans le coin supérieur droit de l'interface web pour sélectionner la langue. Vous pouvez vous déconnecter à l'aide du bouton Déconnexion situé dans le coin supérieur droit de la page, consulter l'aide à l'aide de l'icône représentant un point d'interrogation ou utiliser la bulle pour faire part de vos commentaires.

L'écran de démarrage est également le premier niveau du menu de navigation rapide (cliquez sur une vignette) vers les sections de configuration de l'interphone. Certaines vignettes affichent également l'état des services sélectionnés.

Menu de configuration

La configuration de **l'Interphone IP 2N** s'effectue à travers 5 sections : **État**, **Répertoire**, **Hardware**, **Services** et **Système**, lesquelles intègrent des sous-menus comme indiqué ci-dessous :

État

- **Appareil** – informations essentielles sur l'Interphone
- **Services** – informations sur les services actifs et leurs statuts
- **Licences** – etat actuel des licences et fonctionnalités disponibles sur l'Interphone
- **Registre d'accès** – affiche les 10 derniers enregistrements d'accès
- **Enregistrements des appels** – affiche les 20 derniers appels effectués
- **Événements** – affiche les 500 derniers événements enregistrés par le dispositif

Répertoire

- **Utilisateurs** – paramétrage des numéros de téléphone des utilisateurs, des identifiants (cartes, digicodes…) et autorisation d'accès.
- **Profils horaires** – plages horaires programmables
- **Vacances** – paramétrage des vacances et jours fériés

Services

- **Téléphone** – téléphone et paramètres SIP
- **Contrôle de l'accès** – définition des règles d'entrée et de sortie
- **Streaming** – flux audio/video (ONVIF, RTSP, Multicast, etc.)
- **E-mail** – envoi d'email et paramètres SMTP
- **Automatisation** – automatisme flexibles de l'Interphone adaptés en fonction du besoin de l'utilisateur
- **API HTTP** – paramètres d'autorisation HTTP API
- **Sons de l'utilisateur** – paramètres et téléchargement de Sons utilisateurs
- **Serveur web** – serveur Web et paramètres du mot de passe d'accès
- **Test audio** – test automatique de la boucle audio
- **SNMP** – paramètres SNMP

Appel

- **Paramètres généraux** – paramètres des appels entrants et sortants
- **Composition** – Paramétrage des boutons d'appel rapide
- **SIP 1** – paramètres complets du compte SIP

- **SIP 2** – paramètres complets du compte SIP
- **Appels locaux** – définir les appels locaux, y compris les connexions et les paramètres vidéo et audio
- **Crestron** – paramètres de connexion avec les appareils Crestron

Hardware

- **Interrupteurs** – déverrouillage électrique, éclairage, temporisation etc.
- **Audio** – audio, signalisation, contrôle du volume, paramètres du microphone...etc.
- **Caméra** – paramètres de la Caméra Interne et de la caméra IP externe
- **Keypad** – paramétrage des boutons du clavier
- **Boutons** – boutons d'appel rapide
- **Rétroéclairage** – réglage de l'intensité de rétroéclairage
- **Ecran** – paramètres de l'écran tactile
- **Lecteur de cartes** – lecteur de carte, interface Wiegand
- **Entrées logiques** – réglage des entrées logiques
- **Extendeurs** – différents modules d'extension du **2N® IP Verso**
- **Ascenseur** – réglages de l'accès aux différents étages par l'ascenseur

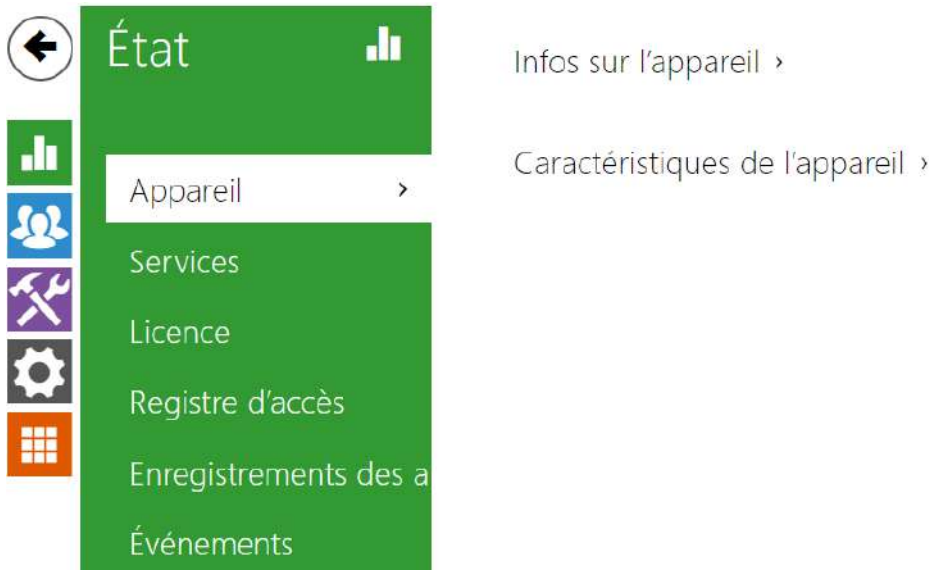
Système

- **Réseau** – paramètres de connexion au réseau local, 802.1x, Capture de paquet
- **Date et heure** – paramètres de l'heure et de la zone horaire
- **Fonction** – paramètres des fonctions de test
- **Licences** – paramètres des licences et activation de la licence d'essai
- **Certificats** – paramètres de certificats et clés privées
- **Provisioning** – mise à jour automatique Firmware et Configuration
- **Syslog** – paramètres d'envoi de message syslog
- **Maintenance** – sauvegarde et restauration de la configuration, mise à jour firmware

Observation

OBSERVATION
Afin d'assurer le bon fonctionnement et la garantie des résultats, nous recommandons fortement une vérification de la version du firmware du produit ou de l'installation au cours du processus d'installation. Le client prend en considération le fait que le produit ou l'installation peut atteindre les rendements garantis et être pleinement opérationnel conformément aux instructions du producteur en utilisant la version la plus récente du produit ou de l'installation, qui a été testée pour une interopérabilité totale. Les versions les plus récentes sont disponibles sur le site https://www.2n.com/cs_CZ/, ou des fonctionnalités spécifiques, en fonction de leur capacité technique, permettent une mise à jour dans l'interface de configuration. Si le client était amené à utiliser une autre version du produit ou de l'installation que la plus récente ou la version que le fabricant a jugée incompatible avec certaines versions des produits des installations d'autres fabricants ou le produit ou l'installation d'une manière incompatible avec les instructions du fabricant, les lignes directrices, le manuel ou la recommandation ou en conjonction avec des produits ou des installations inappropriés des autres producteurs, il est conscient de toutes les limitations potentielles de la fonctionnalité d'un tel produit ou d'une telle installation et de toutes les conséquences connexes. Si le client était amené à utiliser une version autre que la version la plus récente du produit ou de l'installation, ou la version qui a été déterminée par le fabricant comme étant incompatible avec certaines versions des produits des installations d'autres fabricants ou le produit ou l'installation dans un manière incompatible avec les instructions du fabricant, les directives, le manuel ou la recommandation ou en association avec des produits ou des installations inappropriés des autres fabricants, il accepte que la société 2N TELEKOMUNIKACE décline toute responsabilité quant à la limitation de la fonctionnalité d'un tel produit, ni à aucun dommage, perte ou dommage lié à une telle limitation potentielle de fonctionnalité.

5.1 État

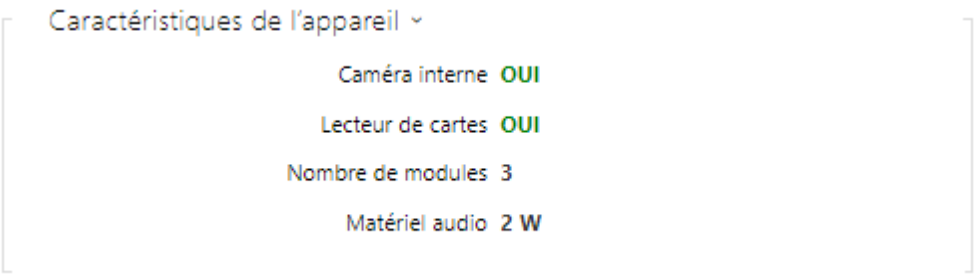


Le menu **État** vous permet d'accéder au statut ainsi qu'à d'autres informations de l'appareil. Son menu est divisé en 5 sections : **Appareil**, **Services**, **Registre d'accès** et **Événements**.

Appareil

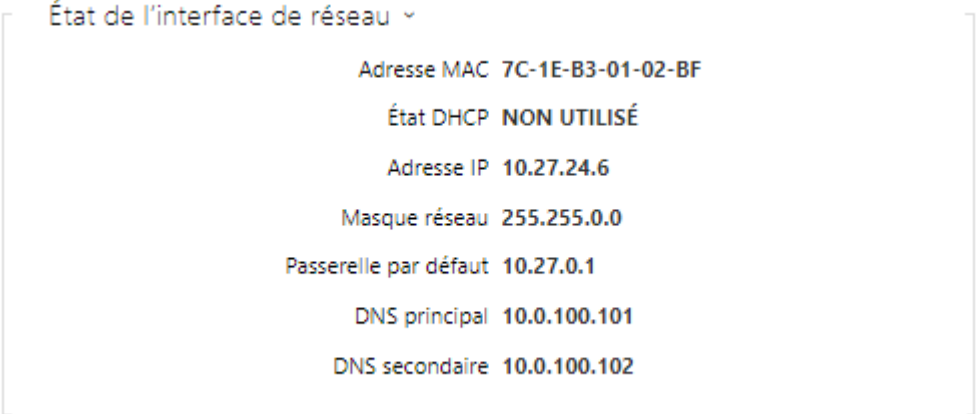
L'onglet appareil vous donnera des informations sur le modèle de l'interphone, son numéro de série, sa version firmware, son alimentation...etc.

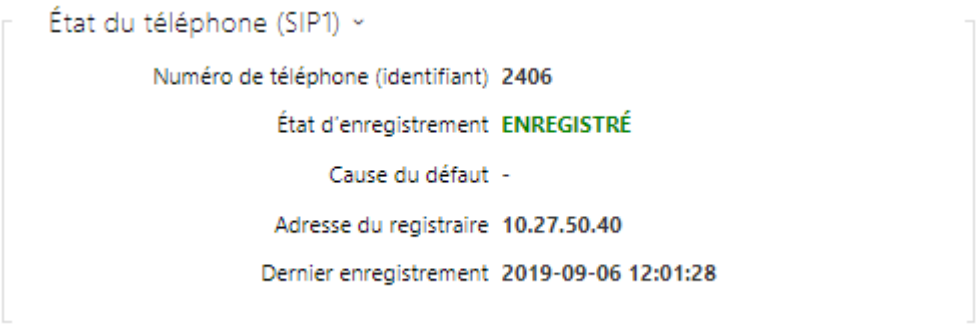
- **Un certificat d'usine est installé** – spécifie le certificat utilisateur et la clé privée utilisés pour vérifier l'autorisation de l'interphone à communiquer avec le serveur de dispositifs de parties tierces.
- **Localiser l'appareil** – signalisation visuelle et acoustique d'un appareil. La signalisation visuelle n'est possible que si l'appareil est équipé d'un rétroéclairage de contrôle disponible sur les modèles suivants (**2N® IP Style, 2N® IP Verso**, **2N® IP Solo**, **2N® IP Base**, **2N® IP Vario**, **2N® IP Force**, **2N® IP Safety** et **2N® IP Uni**). Si l'appareil n'intègre pas de haut-parleur par défaut (**2N® IP Audio Kit** et **2N® IP Video Kit**), assurez-vous qu'un haut-parleur externe est connecté pour la signalisation acoustique.

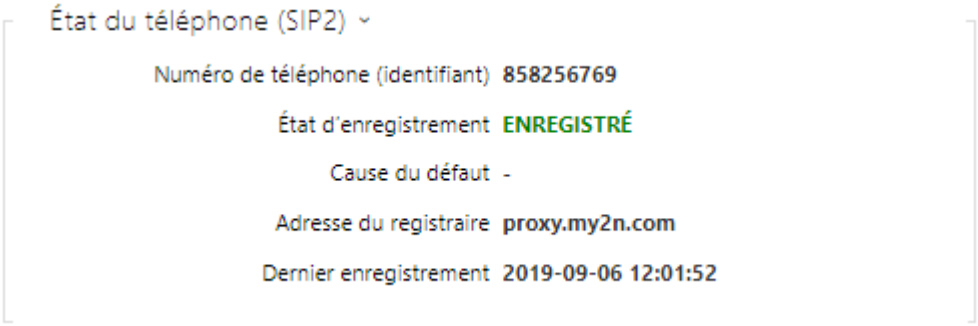


Services

L'onglet **Services** affiche l'état de l'interface réseau et des services sélectionnés.







Registre d'accès

L'onglet **Registre d'accès** affiche les 10 derniers enregistrements de cartes RFID badgées sur le lecteur de l'appareil. Chaque enregistrement comprend l'heure de passage de la carte, son identifiant, son type et sa description (validité, propriétaire de la carte, etc.).

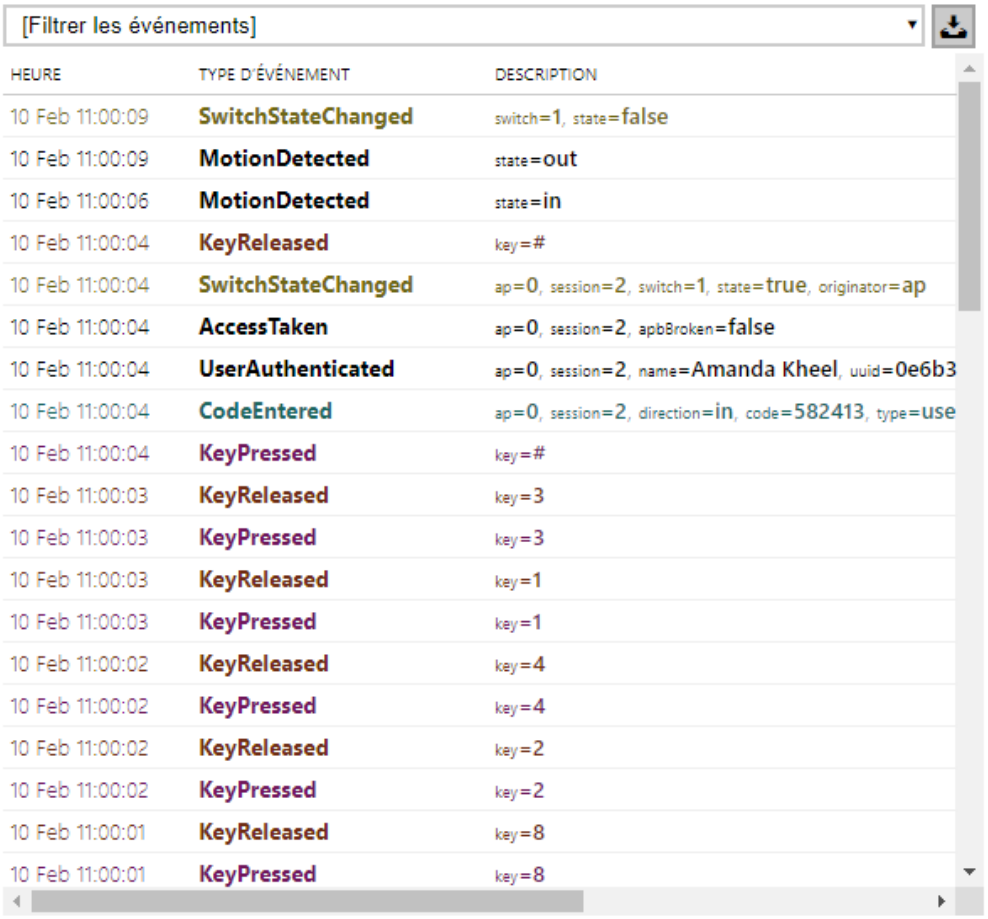
	HEURE	IDENTIFIANT DE LA CARTE	TYPE DE CARTE	DESCRIPTION
1	06/05/2020 12:22:12	45FF7C1E	ISO14443A (Mifare)	Franta Vomáčka, Valid
2	06/05/2020 12:21:21	45FF7C1E	ISO14443A (Mifare)	Franta Vomáčka, Valid
3	06/05/2020 12:13:47	45FF7C1E	ISO14443A (Mifare)	Invalid
4	06/05/2020 12:12:40	45FF7C1E	ISO14443A (Mifare)	Franta Vomáčka, Valid
5	06/05/2020 12:12:11	45FF7C1E	ISO14443A (Mifare)	Franta Vomáčka, Valid
6	06/05/2020 12:10:18	45FF7C1E	ISO14443A (Mifare)	Franta Vomáčka, Valid
7	06/05/2020 12:09:37	45FF7C1E	ISO14443A (Mifare)	Franta Vomáčka, Valid
8	06/05/2020 12:05:24	45FF7C1E	ISO14443A (Mifare)	Franta Vomáčka, Valid
9	06/05/2020 12:03:21	45FF7C1E	ISO14443A (Mifare)	Invalid
10	04/05/2020 13:12:16	4BCFF143	ISO14443A (Mifare)	Invalid

Enregistrements des appels

Les journaux d'appels affichent un aperçu de tous les appels effectués. Chaque appel contient des informations sur le type de contact, l'ID de l'appelé/l'appelant, la date et l'heure de l'appel, sa durée et son statut (entrant, sortant, manqué, décroché ailleurs, bouton de sonnerie). Le champ de recherche permet une recherche en texte intégral dans le nom des appels. La case à cocher est utilisée pour marquer tous les enregistrements pour une suppression en masse. L'enregistrement d'appel sélectionné peut également être supprimé séparément à l'aide de la touche  . La vue d'ensemble affiche les 20 derniers enregistrements, classés de l'appel le plus récent au plus ancien.

Événements

L'onglet **Événements** affiche les 500 derniers événements enregistrés. Chaque événement contient l'heure et la date, le type d'événement et une description spécifiant l'événement. Les événements peuvent être filtrés par type dans un menu déroulant, au-dessus du journal des événements.



-  – pressez ce bouton pour exporter les évènements enregistrés vers un fichier CSV.

Evénements	Signification
AccessLimited	Evènement généré après 5 tentatives d'accès erronées (Carte, code, empreinte digitale…). Le module d'accès se bloque alors pendant 30 secondes même si un identifiant valide est rentré.
ApiAccessRequested	L'événement lorsqu'une requête a été envoyée à /api/accesspoint/grantaccess avec le résultat "success" : true.
AccessTaken	Carte badgée dans une zone Anti-passback.
AudioLoop Test	Généré après le test audio indiquant le résultat du test.

Evénements	Signification
CallSessionStateChanged	Evénement décrivant la direction / l'état de l'appel, l'adresse, le numéro de session et le numéro de séquence d'appel.
CallStateChanged	Lorsque le statut de l'appel change (sonnerie, connecté, terminé), il indique également la direction (entrant, sortant) et l'identification de l'autre partie ou du compte SIP.
CardHeld	Indique qu'une carte RFID a été maintenue plus de 4 secondes sur le lecteur.
CardEntered	Indique qu'une carte RFID a été badgée.
CodeEntered	Généré chaque fois qu'un code se terminant par * est entré sur le clavier numérique.
DeviceState	Indication de l'état du périphérique, démarrage de l'appareil, par exemple.
DoorOpenTooLong	Détection d'une porte ouverte trop longtemps, réglages dans Hardware / Porte / Porte.
DoorStateChanged	Détection d'une porte ouverte / fermée. Les réglages peuvent être effectués dans la section Hardware / Porte / Porte.
DtmfEntered	Recevoir un code DTMF en cours d'appel ou localement en dehors d'un appel.
DtmfPressed	Saisir un code DTMF en cours d'appel ou localement en dehors d'un appel.
DtmfSent	Envoyer un code FTMF en cours d'appel ou localement en dehors d'un appel.
FingerEntered	Autorisation d'une empreinte digitale.
InputChanged	Signale un changement d'état de l'entrée logique.
KeyPressed	Généré chaque fois que vous appuyez sur une touche (les chiffres du clavier numérique sont 0, 1, 2 …, 9 et les touches de numérotation rapide sont %1,%2 …).

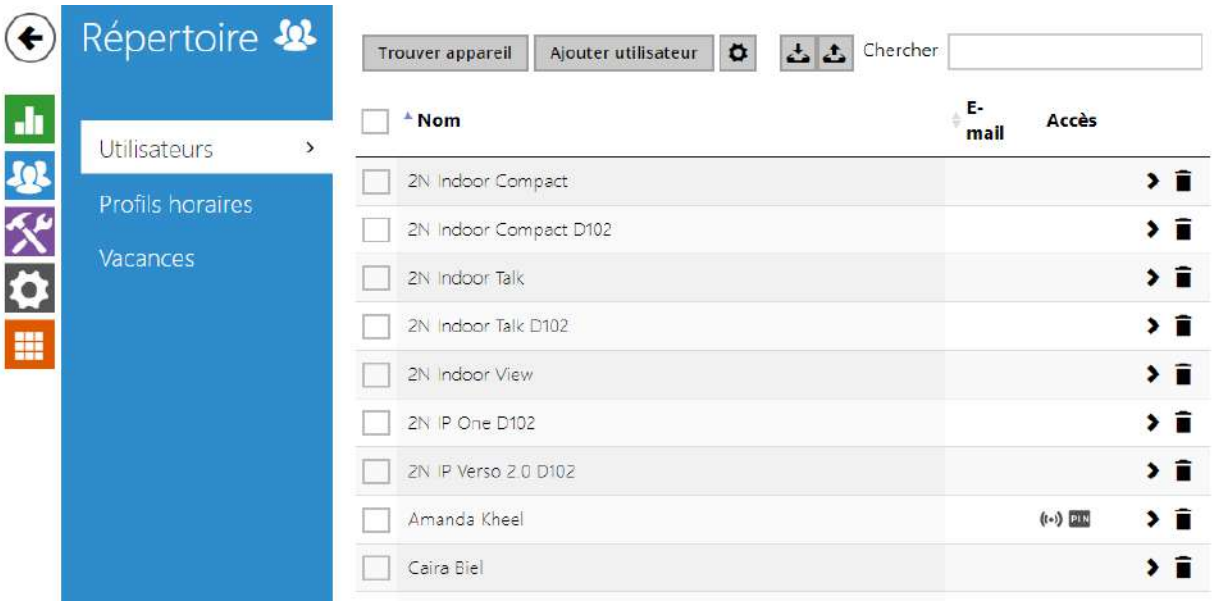
Evénements	Signification
KeyReleased	Généré chaque fois que vous relâchez un bouton (les chiffres du clavier numérique sont 0, 1, 2 …, 9 et les boutons de numérotation rapide sont %1, %2 …).
LiftFloorsEnabled	Accès à un étage d'ascenseur activé.
LiftStatusChanged	Détection de connexion / déconnexion du module de contrôle d'ascenseur.
LoginBlocked	Evénement généré après 3 connexions incorrectes sur l'interface Web. Contient des informations sur l'adresse IP.
MobKeyEntered	Autorisation d'une clé d'accès Bluetooth.
MotionDetected	Généré après la détection d'un mouvement, les réglages peuvent être effectués dans Hardware / Caméra / Caméra interne.
NoiseDetected	Généré après la détection d'un bruit, réglage dans la section Hardware / Audio.
OutputChanged	Signale un changement d'était de la sortie logique
RegistrationStateChanged	Modification de l'état d'enregistrement du proxy SIP.
RexActivated	Evénement généré lors de l'activation de l'entrée défini pour le bouton de sortie.
SilentAlarm	Evénement d'alarme silencieuse généré chaque fois qu'un code supérieur d'un chiffre au code correct est entré. Avec le code d'accès 123, le code d'alarme silencieuse est 124. Ou, chaque fois qu'un doigt ,désigné pour l'activation de l'alarme silencieuse, est placé sur le module de lecteur d'empreinte digitale.
SwitchesBlocked	Interrupteurs bloqués par une tentative d'accès non valide.

Evénements	Signification
SwitchOperationChanged	Modification du fonctionnement de l'interrupteur (signale l'état de verrouillage ou de maintien de l'interrupteur, le démarrage et le redémarrage de la minuterie ou sa fin - passage au maintien permanent).
SwitchStateChanged	Changement d'état de l'interrupteur, paramétrable dans Hardware / Interrupteurs.
TamperSwitchActivated	Signale l'activation du Commutateur d'autoprotection – ouverture du cadre de l'appareil. Assurez-vous d'avoir configuré la fonctionnalité Commutateur d'autoprotection dans la section Entrée logique.
UnauthorizedDoorOpen	Indication d'ouverture non autorisée de la porte, paramètres dans Hardware / Porte / Porte.
UserAuthenticated	Signale une authentification utilisateur et l'ouverture de la porte.
UserRejected	Rejet d'un utilisateur.
VirtualInput	Changement de l'entrée virtuelle.
VirtualOutput	Changement de la sortie virtuelle.
CallSessionStateChanged	Informe sur la phase de l'appel en cours (création, jonction, sonnerie, connexion, fin).

5.2 Répertoire

Cette section regroupe les onglets suivants :

5.2.1 Utilisateurs



La liste des utilisateurs est l'une des parties cruciales de la configuration de l'interphone. Il contient des informations utilisateurs utiles pour des fonctionnalités de l'interphone telles que la numérotation rapide, le déverrouillage des portes par carte RFID / code, les e-mails d'appels manqués…etc.

La liste d'Utilisateurs contient jusqu'à 10 000 utilisateurs (variable selon les modèles **d'interphone IP 2N**). Elle regroupe les utilisateurs pouvant être appelés via les boutons d'appel et les utilisateurs à qui l'on a attribué une carte RFID, un code d'accès...etc.

Si un lecteur de carte externe est connecté à l'interphone via l'interface Wiegand, l'ID de la carte est réduit à 6 ou 8 caractères pour la transmission (variable selon les paramètres de transmission). Si vous appliquez une carte sur le lecteur, vous recevrez un identifiant complet, qui est généralement plus long (8 caractères ou plus). Les 6 ou 8 derniers caractères sont toutefois identiques. Ceci est utile pour comparer les identifiants de carte avec la base de données de l'interphone : si les identifiants à comparer ont des longueurs différentes, ils sont comparés à partir de la fin et la correspondance doit être trouvée à partir de 6 caractères au moins. S'ils ont des longueurs identiques, tous les caractères sonte comparés. Cela garantit la compatibilité mutuelle des lecteurs internes et externes.

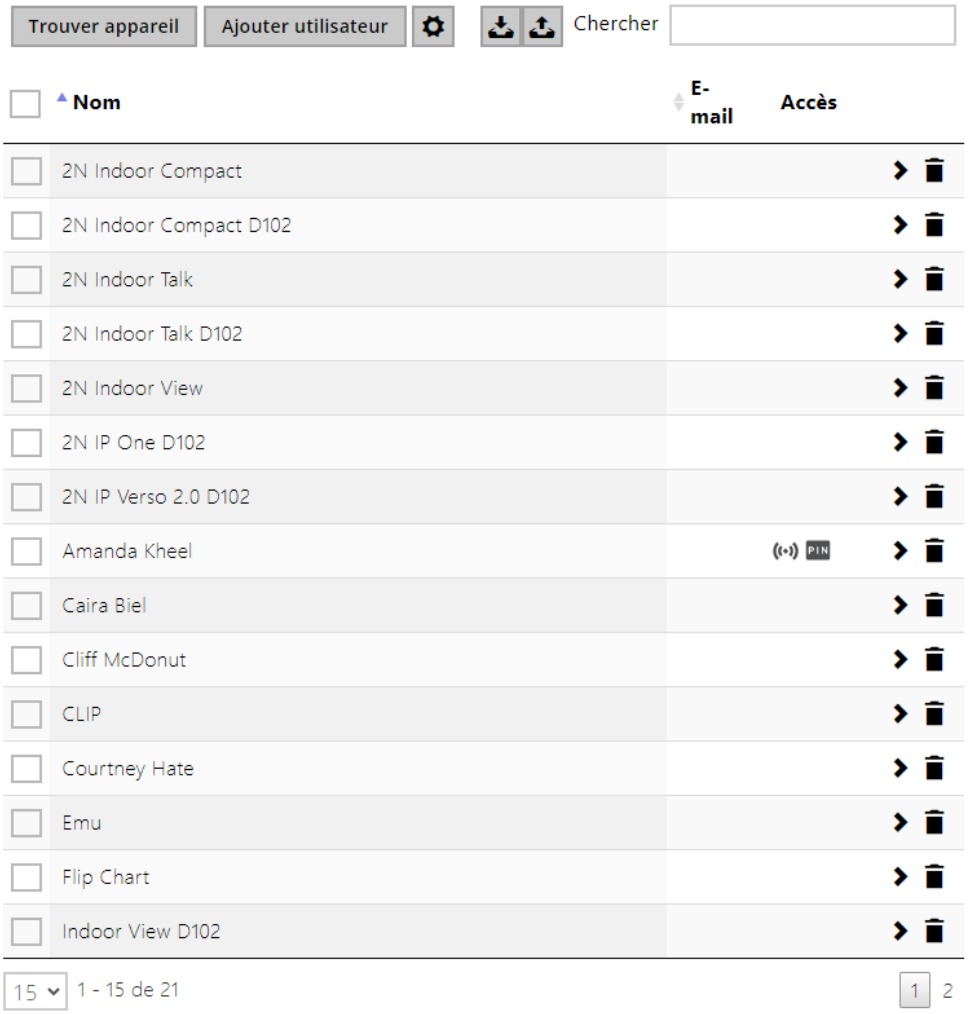
Toutes les cartes badgées sur le lecteur ou via l'interface Wiegand sont enregistrées. Reportez-vous au menu **Etat / Registre d'accès** pour retrouver les 10 dernières cartes badgées qui comprend l'ID, le type de carte, l'heure de passage de la carte et d'autres informations si nécessaire. Sur les petites installations, vous pouvez entrer les cartes directement sur le lecteur et les retrouver dans le registre d'accès. Double-cliquez pour sélectionner l'ID de la carte et appuyez sur CTRL + C. Maintenant que vous avez copié l'ID de la carte, vous pouvez le coller avec CTRL + V dans n'importe quel champ de configuration de l'interphone.

Une fois que la carte a été lue par le lecteur, elle est comparée à la base de données de l'interphone. Si l'ID de la carte correspond à l'une des cartes de la base de données, l'action appropriée sera exécutée : activation de l'interrupteur (déverrouillage de la porte, etc.). Pour modifier le numéro de l'interrupteur à activer, utilisez le paramètre Interrupteur dans le menu **Hardware / Lecteur de carte** (modèles **2N® IP Base**, **Vario**, **Force**) ou le paramètre Interrupteur dans le menu **Hardware / Module Lecteur de carte**. (Modèle **2N® IP Verso**).

Utilisez la section **Hardware / Boutons** pour assigner les utilisateurs à des boutons d'appel. Vous pouvez modifier les paramètres de l'utilisateur et des boutons si nécessaire. La plupart des **interphones IP 2N** sont équipés d'un ou de plusieurs boutons d'appel. Reportez-vous au manuel d'installation de votre modèle d'interphone pour connaître le nombre de boutons d'appel et les options d'extension.

Avertissement

- Il est déconseillé de modifier le répertoire d'un périphériques géré par **2N® Access Commander** via l'interface Web de ce périphérique. En raison de la synchronisation avec **2N® Access Commander**, les modifications apportées au répertoire via l'interface Web seront perdues.



La fonction Recherche dans le répertoire fonctionne en texte intégral par noms d'utilisateur, numéros de téléphone et adresses électroniques.
Un nouvel Utilisateur est ajouté à l'aide du bouton situé au-dessus du tableau. Vous pouvez également rechercher un appareil sur votre réseau local et cet appareil ajouter ensuite au répertoire en tant que nouveau contact.

Cliquez sur pour accéder à la page d'un utilisateur. Cliquez sur pour modifier l'affichage des colonnes. L'affichage par défaut propose : le nom de l'utilisateur, son adresse email et le type d'identifiant d'accès qui lui est attribué. Appuyez sur pour retirer un utilisateur de la liste et supprimer ses informations. Les icones vous indiquent les types d'identifiant d'accès attribués à l'utilisateur. La position de l'utilisateur dans la liste est triée par ordre alphabétique.

Vous pouvez exporter/importer un fichier CSV contenant une liste d'utilisateurs depuis/vers l'appareil à l'aide de l'icône / . Si le répertoire est vide, un fichier avec l'en-tête uniquement (en anglais) est exporté et peut servir de modèle pour l'importation d'utilisateurs. Si un fichier vide contenant uniquement l'en-tête est importé et que l'option **Remplacer le répertoire** est sélectionnée, le répertoire entier est supprimé. S'il y a des utilisateurs dans le répertoire, ils sont tous exportés, à l'exception des types spéciaux d'utilisateurs. L'importation vous permet de télécharger jusqu'à 10 000 utilisateurs, en fonction du type d'appareil.

Observation

- Les utilisateurs spéciaux, par exemple ceux créés par le service **My2N** ou le système **2N Access Commander**, ne font pas partie de l'exportation du carnet d'adresses.
- Lors de l'édition d'un fichier CSV à l'aide de Microsoft Excel, il faut enregistrer le fichier au format CSV UTF-8 (avec des séparateurs).

Les informations des fiches utilisateurs sont les suivantes :

- **Nom** – paramètre obligatoire pour identifier un utilisateur.
- **Photographie** – il est possible d'inclure la photo de l'utilisateur. Cliquez sur le bouton de sélection pour ajouter un photo depuis un dossier ou bien prenez une photo directement depuis la caméra de l'appareil. Les formats de photo supportés sont .jpg, .png et .bmp. Cette fonction est disponible uniquement sur les modèles d'Interphones équipés d'un écran tactile : **2N® IP Verso** et **2N® IP Vario**.

Observation

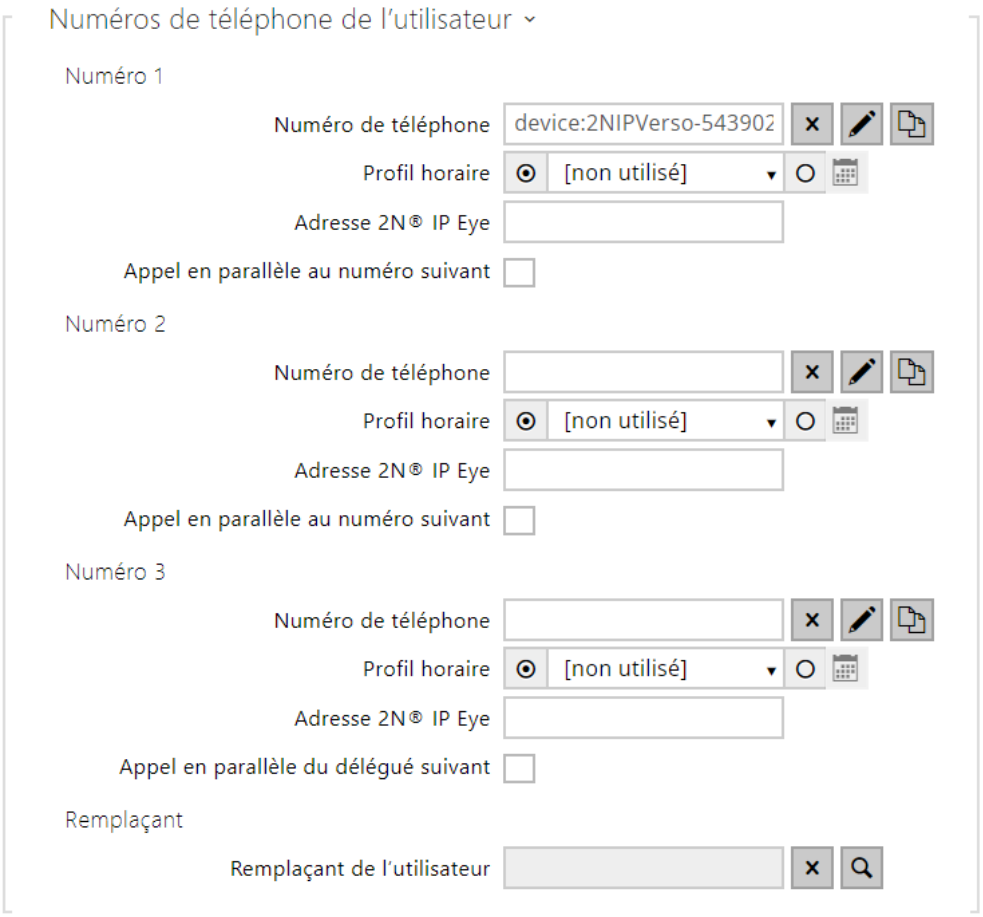
- Si la section de l'image ne remplit pas tout l'espace de la fenêtre de recadrage, l'image résultante sera centrée sur **2N® IP Style**.

- **E-Mail** – adresse électronique de l'utilisateur pour l'envoi des informations sur les appels manqués. Vous pouvez entrer plusieurs adresses électroniques séparées par des virgules.
- **Numéro virtuel** – un numéro qui peut être utilisé pour appeler l'utilisateur à l'aide d'un clavier numérique. Les numéros virtuels n'ont pas de rapport avec les numéros de téléphone de l'utilisateur. Ils peuvent former un tout autre plan de numérotation qui est indépendant des numéros de téléphone et permet ainsi de cacher les numéros de téléphone des utilisateurs. Cette fonction peut être utilisée particulièrement dans les installations où le nombre de touches ne suffit pas pour une sélection abrégée. L'arrivant entre un numéro virtuel sur le clavier numérique et appuie sur la touche *. Si vous utilisez ce mode d'appel de l'utilisateur, il convient de placer près de l'interphone un répertoire bien ordonné des noms des utilisateurs et de leurs numéros virtuels, y compris un simple mode d'emploi. La fonction des numéros virtuels peut être enclenchée dans le menu **Services / Téléphone / Appels / Appels sortants** à l'aide du paramètre **Appel de numéros virtuels**. Le numéro peut contenir de 1 à 7 chiffres.

- **Emplacement dans le répertoire** – c'est dans le répertoire de base que les utilisateurs peuvent être ajoutés directement. Ce répertoire ne peut pas être supprimé ou renommé et un utilisateur peut être ajouté dans 5 sous-groupes maximum.
- **Groupe d'appel** – entrez un nom de groupe d'utilisateurs à afficher dans l'annuaire. En appelant le groupe, vous pourrez faire sonner tous ses utilisateurs en même temps. Une fois que l'un des appels est décroché, les autres appels se termineront automatiquement.

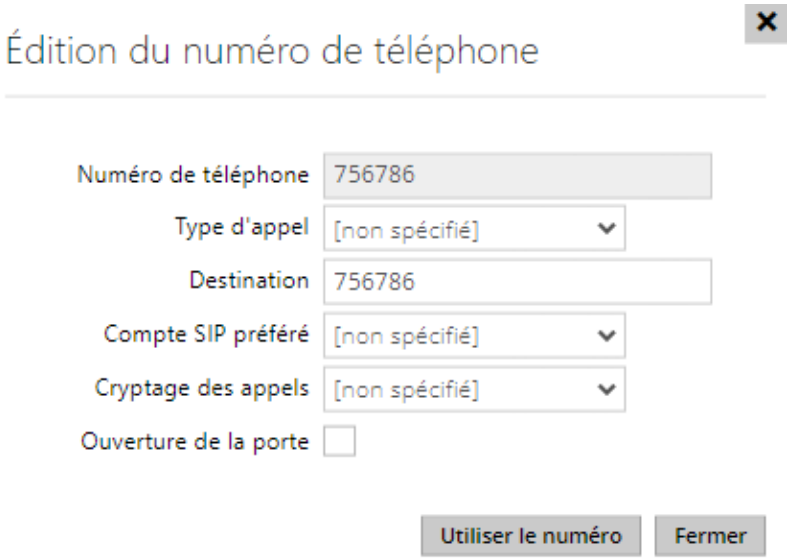
Observation

- Les caractères <, > et / ne sont pas autorisés pour le nom, la position dans le répertoire et les paramètres de groupes d'appel.



Chaque utilisateur de la liste peut se voir attribuer jusqu'à trois numéros de téléphone. Au cas où l'utilisateur est inaccessible sur un numéro, le numéro suivant sera composé automatiquement après un délai de sonnerie programmable. Activez l'option "Appel parallèle vers le numéro suivant" pour permettre la composition simultanée de plusieurs numéros. La validité du numéro de téléphone peut également être limitée selon des plages horaires.

- **Numéro de téléphone** – entrez le numéro de téléphone du poste vers lequel l'appel doit être acheminé. Entrez sip:[utilisateur_id@]domaine[:port] pour un appel SIP Direct, ex : sip:200@192.168.22.15 ou sip:nom@entreprise. Pour les appels locaux vers les Interphones IP 2N et les postes de réception, entrez device:nom de l'appareil. Définissez ce nom dans l'appareil respectif. Pour les appels vers Crestron, entrez: RAVA:device_nom. Dans le cas d'appel via un serveur SIP, entrez **/1** ou **/ 2** derrière le numéro d'extension d'un poste pour préciser via quel compte SIP l'appel sera routé (compte 1 ou 2). Entrez /**S** ou /**N** pour forcer un appel crypté ou non crypté. Entrez /**B** pour enclencher le déverrouillage sur rappel. Vous pouvez combiner la sélection du compte, le cryptage et le déverrouillage sur rappel, ex : /1S, /1B, etc. Il est possible d'aller jusqu'à 255 caractères.
  Les réglages détaillés du numéro de téléphone peuvent être effectués dans l'édition, qui s'ouvre en appuyant  .



  - **Type d'appel** – définit le schéma dans l'URI de la destination appelée. Lorsque vous sélectionnez Sans schéma, l'URI est complété par les données des paramètres du compte SIP. Utilisez d'autres paramètres pour un appel SIP direct (sip:), un appel local 2N (device:), un appel vers un appareil Crestron (rava:) ou un appel vers un système de gestion vidéo tel que AXIS Camera Station (vms:).
  - **Destination** – définit des autres parties de l'URI de la destination appelée. Il contient généralement un numéro, une adresse IP, un domaine, un port ou un identifiant de l'appareil. Un astérisque (*) est saisi pour les appels vers le VMS.
  - **Compte SIP préféré** – le compte SIP numéro 1 ou numéro 2 est préféré pour les appels.
  - **Cryptage des appels** – vous pouvez configurer le cryptage obligatoire des appels ou un appel sans cryptage.
  - **Ouverture de la porte** – à l'aide du rappel automatique.

- **Profil horaire** – attribuez un profil horaire à chaque numéro de téléphone pour définir la plage horaire sur laquelle le numéro est joignable. Si le profil est inactif, le numéro de téléphone n'est pas utilisé et le numéro de téléphone suivant sera composé s'il est défini.
- **Adresse 2N® IP Eye** – définissez l'adresse IP du PC de manière à recevoir un message UDP pour chaque appel vers le numéro de téléphone d'un utilisateur actif. L'application **2N® IP Eye** affichera alors le flux vidéo de la caméra de l'Interphone sur le PC de l'utilisateur dans le cas ou son poste IP n'est pas équipé d'un écran. Entrez l'adresse sous ce format : domaine[:**port1**][:**port2**], ex : poste.entreprise.com ou 192.168.22.111. Les paramètres du **port1** et du **port2** sont optionnels et sont utilisés dans le cas d'un NAT (Network Address Translation) entre le PC et l'Interphone et les adresses doivent être conformes au routeur ou à un autre appareil opérant le NAT. Les paramètres du port1 (valeur par défaut : 8003) définissent le port de destination pour les messages UDP envoyés vers **2N® IP Eye**. Les paramètres du port2 (valeur par défaut : 80) définissent le port de destination pour la communication HTTP entre l'interphone et **2N® IP Eye**.

Note

- *La fonction 'Adresse IP Eye' est disponible selon les modèles **d'interphones de la gamme 2N.***
- *Sans la licence Intégration Améliorée, il n'est possible de contrôler l'interrupteur du portier que pendant un appel. Durant un appel vers un utilisateur ayant une adresse **2N® IP Eye** correctement renseignée, aucune licence n'est nécessaire pour contrôler le déverrouillage depuis l'application.*

Conseil

- FAQ: 2N® IP Eye – Comment configurer un Interphone IP 2N

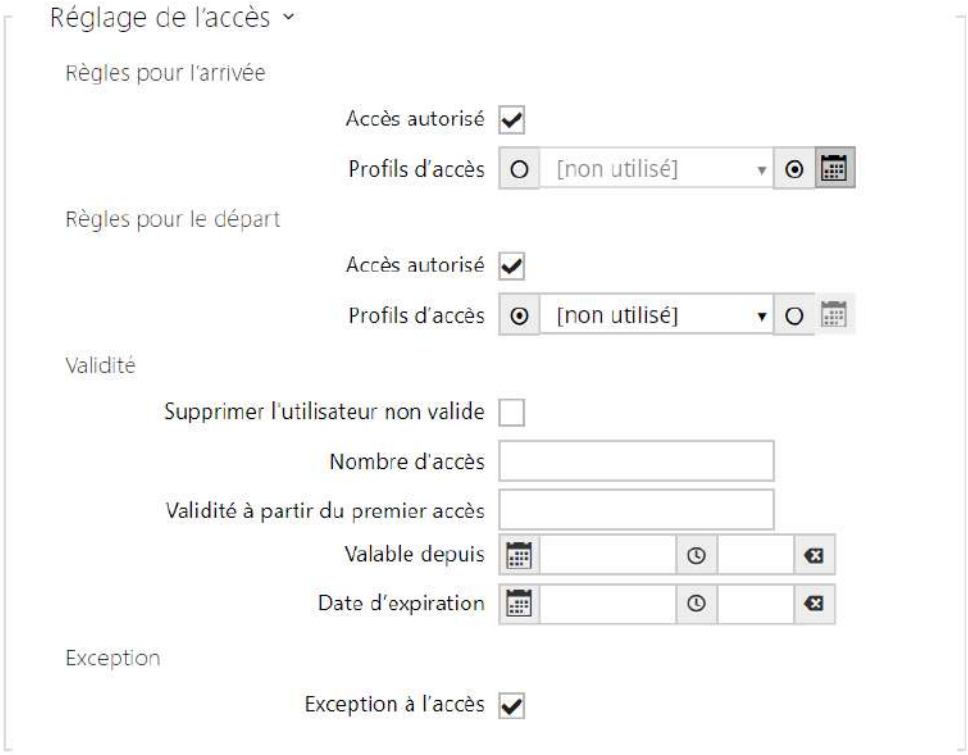
Conseil

- Vidéo Tutoriel Applications, logiciel pour les Interphones IP – 2N® IP Eye

- **Appel en parallèle au numéro suivant** – activez les appels de groupe, c'est-à-dire appeler simultanément plusieurs numéros de téléphone. Vous pouvez appeler les deux premiers numéros, les deux derniers ou bien les trois numéros en parallèle. Répondre à un appel mettra automatiquement fin aux autres appels.
- **Appel en parallèle vers le remplaçant** – permet d'appeler un utilisateur secondaire dans le cas ou aucun des 3 numéros de l'utilisateur n'a répondu à l'appel. Si la fonction "Appel en parallèle au numéro suivant" est cochée après le troisième numéro de l'utilisateur, le premier numéro d'appel de l'utilisateur remplaçant sonnera en même temps et ainsi de suite. Le nombre total maximal d'appels pouvant être composés en parallèle est de 16, ce qui peut se produire lorsque des appels de groupe et plusieurs numéros attribués à une touche de numérotation rapide sont utilisés simultanément.

- **Remplaçant de l'utilisateur** – sélectionnez un utilisateur vers lequel l'appel sera acheminé en cas d'inaccessibilité. Entrez le numéro de poste de l'utilisateur ou utilisez le bouton de recherche. Le nombre total maximal d'appels pouvant être composés en parallèle est de 16, ce qui peut se produire lorsque des appels de groupe et plusieurs numéros attribués à une touche de numérotation rapide sont utilisés simultanément.

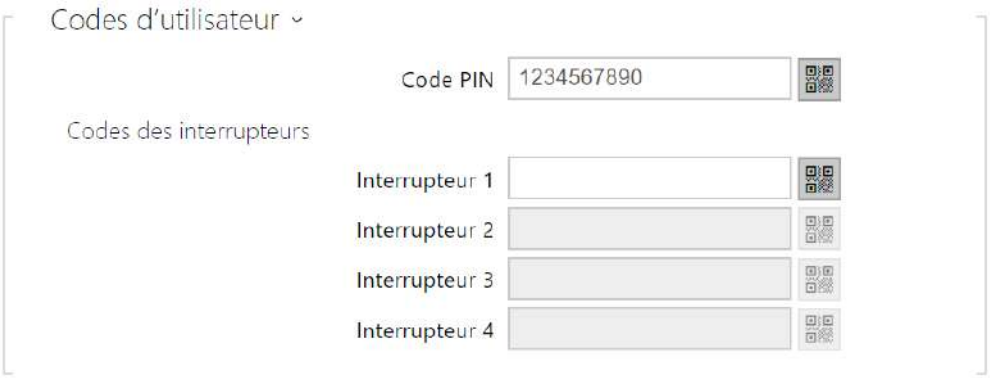
> **Note**
>
> - *La fonction remplaçant de l'utilisateur est disponible selon les modèles d'interphones utilisés.*



- **Règles pour l'arrivée**
  - **Accès autorisé** – il autorise l'authentification à ce point d'accès.
  - **Profils d'accès** – sélectionnez l'un des profils prédéfinis dans la section **Répertoire / Profils horaires** ou bien définissez le profil temporel manuellement.
- **Règles pour le départ**
  - **Accès autorisé** – il autorise l'authentification à ce point d'accès.
  - **Profils d'accès** – sélectionnez l'un des profils prédéfinis dans la section **Répertoire / Profils horaires** ou bien définissez le profil temporel manuellement.
- **Validité**
  - **Supprimer l'utilisateur non valide** – sélectionnez si l'utilisateur est supprimé du dispositif une fois qu'il est invalide (c'est-à-dire qu'il a dépassé sa période de validité

ou que le nombre de ses accès autorisés est de 0).
- **Nombre d'accès** – définissez le nombre d'accès autorisés pour cet utilisateur. Laissez vide pour définir un nombre indéfini d'accès.
- **Validité à partir du premier accès** – définissez le temps pendant lequel l'utilisateur sera valide à partir de sa première autorisation réussie. Laissez vide pour aucune période de validité relative. La validité relative peut raccourcir la période de validité mais ne la prolongera jamais. Le temps est réglé au format HH:MM, par exemple, 06:09.
- **Valable depuis** – paramétrez la date et l'heure du début de validité. Laissez vide pour que le début ne soit pas restreint. Le Valid From doit précéder le Valid To.
- **Date d'expiration** – paramétrez la date et l'heure de fin de validité. Laissez vide pour que la fin ne soit pas restreinte. Valide jusqu'au doit être après Valide depuis.

- **Exception à l'accès** – autorisez cet utilisateur à contourner les règles de blocage d'accès et anti-retour.

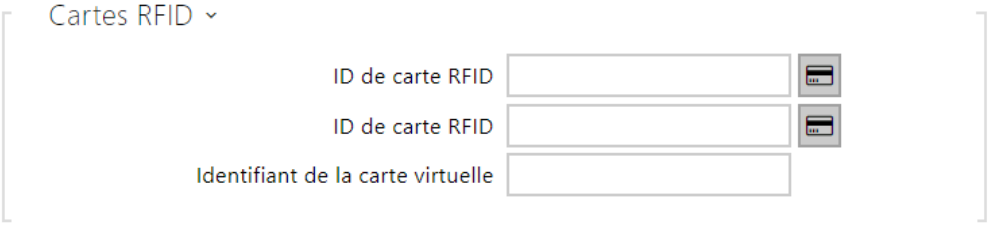


Chaque utilisateur peut se voir attribuer son propre code QR / code numérique privé pour activer l'interrupteur. Les codes Interrupteurs des utilisateurs peuvent être combinés de manière arbitraire avec les codes interrupteurs universel définis dans la section **Hardware | Interrupteurs**. Si les codes sont identiques aux codes déjà définis dans la configuration de l'interphone, le pictogramme apparaitra sur les codes en conflit.

- **Code PIN** – définissez le numéro d'identification personnel de l'utilisateur. Le code doit contenir au moins deux caractères.
  - – génère une image du code QR. Pour des raisons de sécurité, les codes contenant moins de 4 chiffres ne peuvent pas être saisis en scannant le code QR. Les codes ne doivent contenir que des chiffres. Si l'authentification est requise à l'aide d'un code QR hexadécimal, ce code doit être converti au format décimal avant d'être saisi.
- **Interrupteur 1–4** – définissez un code d'activation de commutateur d'utilisateur privé: jusqu'à 16 caractères, chiffres compris entre 0 et 9 uniquement. Le code doit comporter au

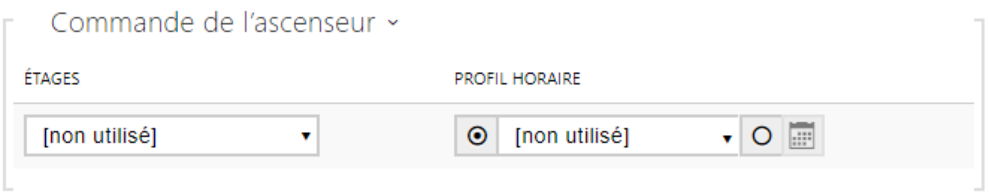
moins 2 caractères. Le code doit inclure au moins deux caractères de déverrouillage de la porte via le clavier de l'interphone et au moins un caractère de déverrouillage de la porte via DTMF.

-  – génère une image du code QR. Pour des raisons de sécurité, les codes contenant moins de 4 chiffres ne peuvent pas être saisis en scannant le code QR. Les codes ne doivent contenir que des chiffres. Si l'authentification est requise à l'aide d'un code QR hexadécimal, ce code doit être converti au format décimal avant d'être saisi.

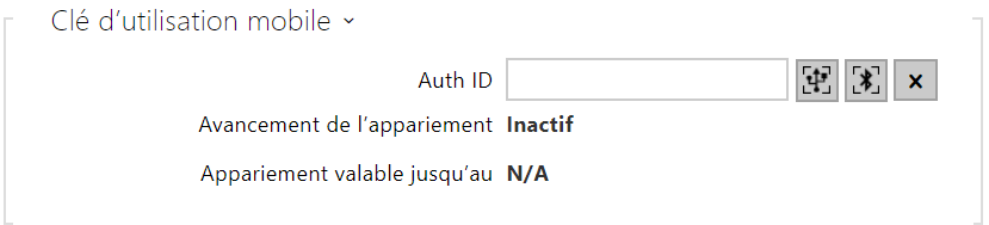


Chacun des utilisateurs de l'interphone peut se voir attribuer deux cartes RFID d'accès.

- **ID de carte RFID** – il vous permet de définir l'ID des carte d'accès de l'utilisateur. Chaque utilisateur peut se voir assigner jusqu'à deux cartes d'accès. L'ID de la carte d'accès est une séquence de 6–32 caractères comprise entre 0–9, A–F. Lorsqu'une carte valide est badgée sur le lecteur, l'interrupteur associé au lecteur de carte est activé. Si le mode Double authentification est activé, l'interrupteur ne peut être activé qu'en utilisant à la fois une carte et une seconde méthode (Empreinte Digital, Code numérique ou Clé d'accès Bluetooth).
- **Identifiant de la carte virtuelle** – il vous permet de définir l'ID de la carte d'accès virtuelle de l'utilisateur. Chaque utilisateur peut avoir une seule carte virtuelle attribuée. Il s'agit d'une séquence de 6–32 caractères comprise entre 0–9, A–F. Une fois l'utilisateur authentifié via le lecteur Bluetooth / biométrique, l'identifiant de la carte virtuelle est envoyé vers un appareil tiers intégré à l'interphone IP 2N via Wiegand.



- **Étages** – sélectionnez les étages accessibles par l'utilisateur dans le cas d'un Contrôle d'accès dans l'ascenseur.
- **Profil horaire** – sélectionnez un ou plusieurs profils horaires à appliquer. Définissez les profils horaires dans la section **Répertoire / Profils horaires**.
  - marquer la sélection à partir des profils prédéfinis ou du réglage manuel d'un profil temporel.
  - paramétrez un profil horaire.



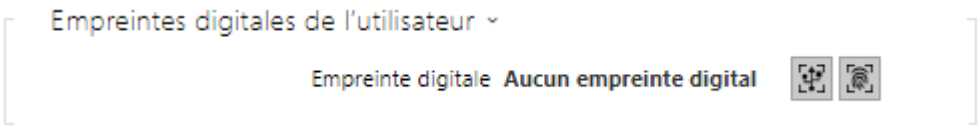
- **Authentification ID** – définissez un identifiant unique d'appareil mobile / d'utilisateur. La valeur du paramètre est automatiquement générée pour le jumelage. Vous pouvez déplacer l'ID d'authentification vers un autre utilisateur ou le copier sur un autre appareil au même emplacement.
- **Etat du jumelage** – état actuel du jumelage (Inactif, En attente de jumelage, PIN expiré ou Jumelage effectué).
- **Jumelage valable jusqu'au** – date et heure de la fin de la validité du code confidentiel d'autorisation généré.
  - jumelage via Lecteur USB
  - jumelage via l'appareil
  - effacer l'ID

Jumelage via le module Bluetooth de l'Interphone

Pour jumeler le Smartphone d'un utilisateur :

1. Cliquez sur pour démarrer le jumelage de l'utilisateur.
2. Une fenêtre de dialogue avec le code PIN va s'afficher.
3. Sélectionnez le lecteur depuis l'application **2N® Mobile Key** et appuyez le bouton pour démarrer le jumelage.
4. Rentrez le code généré.
5. Le jumelage est terminé.

Référez-vous à la section 5.4.5 Clé Mobile pour les détails de configuration de l'application **2N® Mobile Key**.

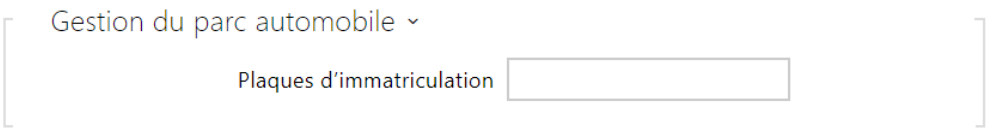


- **Empreintes digitales** – affiche le nombre d'empreintes digitales définies ; Vous pouvez définir jusqu'à 2 empreintes digitales différentes par utilisateur. Cette section ne s'affiche que si le module lecteur biométrique est disponible.
  - enrôlement via lecteur USB
  - enrôlement via le lecteur biométrique

Observation

- La capacité du lecteur biométrique est de 2000 empreintes par lecteur.

Une procédure détaillée relative à la façon de charger les empreintes digitales des utilisateurs est décrite dans le sous-chapitre 5.2.1.1 Configuration des empreintes digitales de l'utilisateur.



L'interphone 2N IP permet d'utiliser les immatriculations reconnues des véhicules envoyées dans une requête HTTP par les caméras de la société AXIS équipées de l'application complémentaire VaxALPR sur api/lpr/licenseplate (pour de plus amples informations, consulter le manuel API HTTP pour les interphones IP).
Si la fonction est activée, une fois réceptionnée une requête HTTP valide, l'événement sera enregistré dans l'historique sous l'événement LicensePlateRecognized.

L'image envoyée dans le cadre d'une requête HTTP (par ex. une partie de la photo ou la photo entière de la scène lors de la détection de la plaque d'immatriculation) sera enregistrée. Les cinq dernières photos sont stockées dans la mémoire de l'équipement, qui peut être lue à partir de l'équipement à l'aide d'une requête HTTP envoyée à api/lpr/image et sont disponibles dans le système **2N® Access Commander**.

Pour un fonctionnement adéquat, il est conseillé que chaque plaque d'immatriculation soit affectée à une seule entrée dans le répertoire. En cas de plaques d'immatriculation multiples, il n'est pas possible d'attribuer catégoriquement une entrée dans le répertoire qui a la plaque d'immatriculation configurée (la première entrée correspondant à la plaque d'immatriculation donnée configurée est sélectionnée et ses règles d'accès sont mises en œuvre).

- **Plaques d'immatriculation** – définit les immatriculations des véhicules de l'enregistrement donné dans le répertoire. Il est possible d'attribuer plusieurs immatriculations séparées par des virgules (20 maximum) dans un enregistrement. Les immatriculations saisies sont utilisées pour la fonction de reconnaissance des plaques d'immatriculation à partir de l'image de la caméra externe (pour de plus amples informations, voir le manuel d'interopérabilité). Une immatriculation peut comporter 10 caractères au maximum. La longueur de la chaîne spécifiée est limitée à 255 caractères.

- **Étages** – sélectionnez les étages accessibles par l'utilisateur dans le cas d'un Contrôle d'accès dans l'ascenseur.
- **Profil horaire** – sélectionnez un ou plusieurs profils horaires à appliquer. Définissez les profils horaires dans la section **Répertoire / Profils horaires**.
  -  marquer la sélection à partir des profils prédéfinis ou du réglage manuel d'un profil temporel.
  -  paramétrez un profil horaire.

5.2.1.1 Paramètres de connexion des appels

Pour appeler d'autres appareils terminaux sur des réseaux IP, vous devez attribuer l'appareil à un contact dans le Répertoire.

Connexion aux appareils 2N au réseau local

1. Assurez-vous que la fonction Appels locaux est autorisée sur les deux appareils 2N.
2. Cliquez sur le bouton **Trouvez appareil** au-dessus du tableau. Dans la liste, cochez l'appareil auquel vous souhaitez vous connecter. Après l'ajout de l'appareil, l'édition de l'utilisateur nouvellement ajouté s'ouvre.
3. Dans l'édition, vous pouvez modifier les informations de base sur l'utilisateur ou gérer ses options d'accès. Si vous allez composer des appels à l'aide du clavier numérique, configurez un numéro virtuel pour l'utilisateur.
4. Une fois enregistré, le contact apparaît dans le répertoire téléphonique sur l'écran de l'appareil. Si vous allez composer des appels à l'aide d'un bouton sur l'appareil, vous devez attribuer l'utilisateur à un bouton de numérotation rapide dans Hardware > Buttons, voir 5.3.5 Tlačítka.
5. Pour qu'un appel aboutisse, le service Appels locaux doit être autorisé sur l'appareil 2N appelé.

Connexion à d'autres appareilse

1. Créez un nouveau contact en cliquant sur le bouton **Ajouter utilisateur** au-dessus du tableau ou ouvrez le détail d'un contact existant.
2. Cliquez sur l'icône du crayon  à côté du paramètre Numéro de téléphone pour ouvrir l'édition du numéro de téléphone.
3. Sélectionnez le type d'appel dans le menu d'édition :

- *SIP* pour un appel effectué via SIP,
- *rava* pour les appels avec Creston,
- *vms* pour les appels avec Axis Camera Station,
- *device* pour les appels avec un appareil 2N local.

- Dans le champ Destination, entrez l'adresse de la destination de l'appel vers laquelle l'appel doit être acheminé.
  Remplissez l'URI SIP sous la forme *nom_utilisateur@hôte* ou l'adresse IP de destination (par exemple : *johana@255.0.255.0* ou *johana@calls.2N.com*). Pour les appels locaux, remplissez l'ID de l'appareil 2N appelé, voir Appels locaux dans 5.4.1 Téléphone.
- Dans l'édition, vous pouvez modifier les informations de base sur l'utilisateur ou gérer ses options d'accès. Si vous allez composer des appels à l'aide du clavier numérique, configurez un numéro virtuel pour l'utilisateur.

- Une fois enregistré, le contact apparaît dans le répertoire téléphonique sur l'écran de l'appareil. Si vous allez composer des appels à l'aide d'un bouton sur l'appareil, vous devez attribuer l'utilisateur à un bouton de numérotation rapide dans Hardware > Buttons, voir 5.3.5 Boutons.
- Pour qu'un appel aboutisse, le service qui achemine l'appel doit être autorisé sur l'appareil appelé.

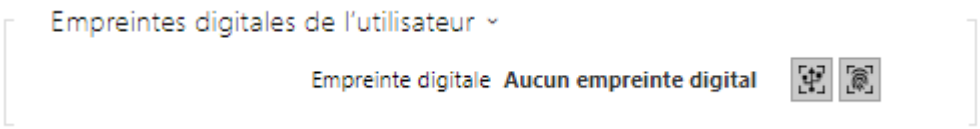
Conseil

- Chaque utilisateur peut se voir attribuer jusqu'à trois numéros de téléphone. Si l'utilisateur ne répond pas au premier numéro de téléphone, l'appel est transféré au numéro suivant. Vous pouvez également configurer des appels vers plusieurs numéros de téléphone en même temps. Pour appeler simultanément plusieurs numéros de téléphone d'un même utilisateur, cochez la case *Appeler en groupe* entre les numéros de téléphone donnés.
- Si tous les numéros de téléphone de l'utilisateur ne sont pas disponibles, vous pouvez faire en sorte que l'appel soit transféré au Remplaçant.
- Les utilisateurs peuvent être regroupés en groupes d'appel. Le nom du groupe d'appel apparaît dans le répertoire téléphonique sur l'écran de l'appareil. Vous pouvez attribuer un groupe d'appel à une touche de numérotation rapide. Si un appel de groupe sortant doit être terminé par le premier refus de l'un des utilisateurs appelés, vous devez configurer cette fonction dans Services > Téléphone > Appels, voir 5.4.1 Téléphone.

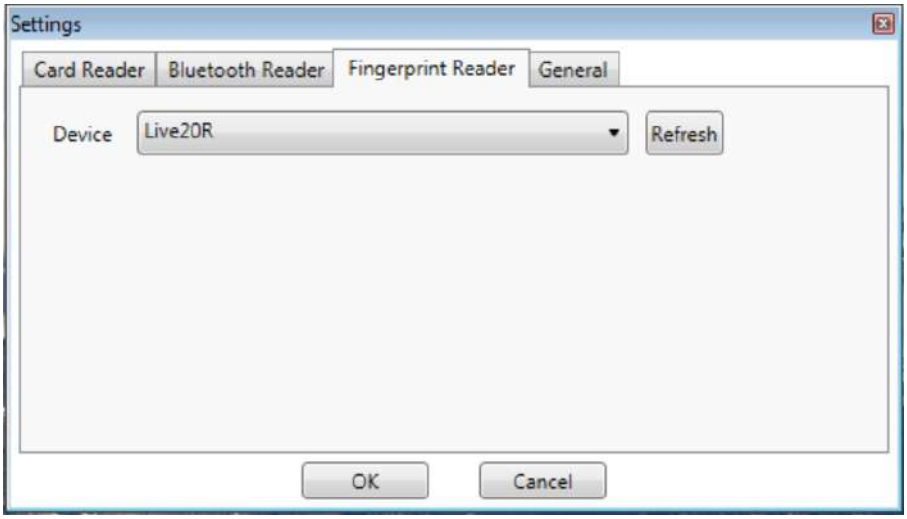
5.2.1.2 Configuration des empreintes digitales de l'utilisateur

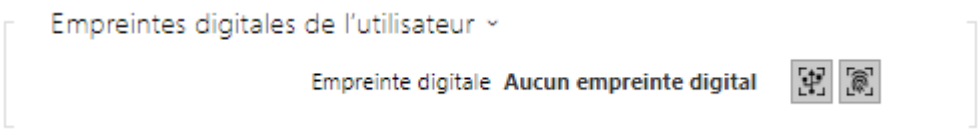
Pour enregistrer des empreintes digitales, utilisez le lecteur d'empreintes digitales du **2N® IP Verso** (référence 9155045) ou bien un lecteur d'empreintes digitales USB externe (référence 9137423E), procédez comme ceci :

1a) Pour enrôler une empreinte digitale depuis le lecteur biométrique du **2N® IP Verso**, cliquez sur  dans la fiche utilisateur. Enregistrez l'empreinte depuis le module dans l'interface Web à la section Répertoire / Utilisateur.



1b) Pour enrôler une empreinte digitale depuis un lecteur USB externe, utilisez le **2N® IP USB Driver** et sélectionnez le lecteur dans les paramètres. Cliquez sur OK pour confirmer. Pour enregistrer une nouvelle empreinte, cliquez sur  . Enregistrez l'empreinte depuis le lecteur USB dans l'interface Web à la section Répertoire / Utilisateur.





2) Cliquez sur l'un de ces deux boutons pour enregistrer une empreinte.

Vous pouvez enregistrer jusqu'à deux empreintes par utilisateur.

3) Cliquez sur le bouton pour démarrer le scan de l'empreinte.

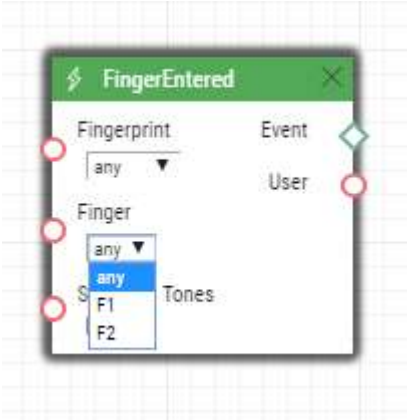
4) Placez le doigt sélectionné sur un lecteur USB externe. Cette procédure est répétée trois fois pour plus de précision.

Répétez le processus si une incohérence se produit pendant la lecture des empreintes digitales.

5) Si la numérisation des empreinte digitale est réussie, cliquez sur OK pour confirmer les paramètres.

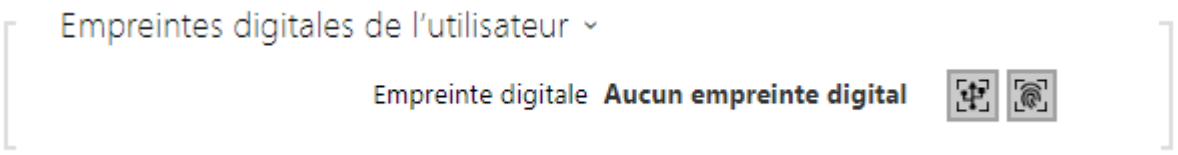
Pour définir la fonction de l'empreinte digitale, cliquez sur l'icone :

- Ouvrir la porte
- Alarme silencieuse, configurable seulement si la fonction ouverture de porte est définie (permet de signaler une ouverture de porte sous la contrainte).
- Automatisation F1 – générez l'évènement FingerEntered dans l'interface d'automatisation. F1 permet d'identifier le premier doigt
- Automation F2 – générez l'évènement FingerEntered dans l'interface d'automatisation. F2 permet d'identifier le deuxième doigt.



Cliquez sur ENREGISTRER ET QUITTER pour confirmer l’enregistrement des empreintes digitales et des fonctions sélectionnées.

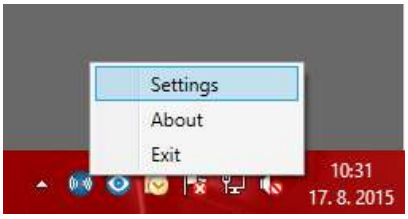
6) Vous pouvez vérifier les paramètres dans la fiche utilisateur



5.2.1.3 Lecteur de carte RFID USB

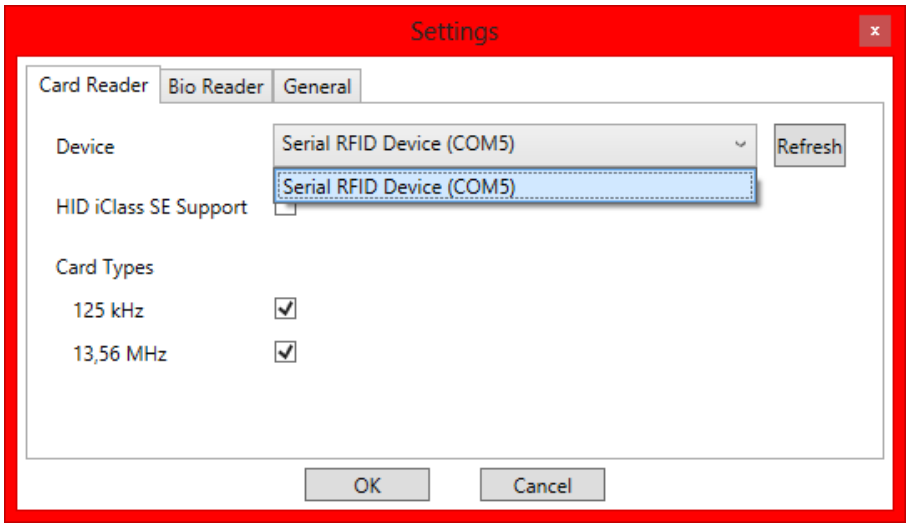
Il est possible de lire l'ID de la carte via un lecteur de carte RFID externe. La procédure est la suivante :

1. Rendez vous dans **2N IP USB Driver**

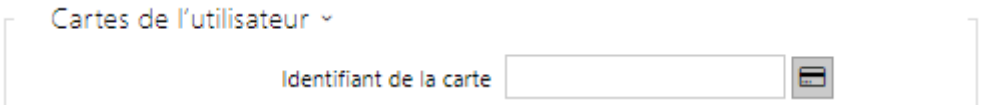


Cliquez sur Settings

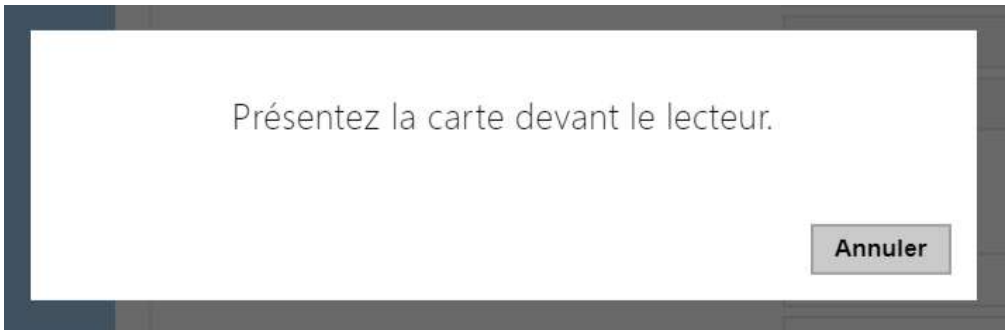
2. Configurez le port COM pour le lecteur connecté.



3. Cliquez sur le bouton Lire depuis l'interface Web de l'Interphone.



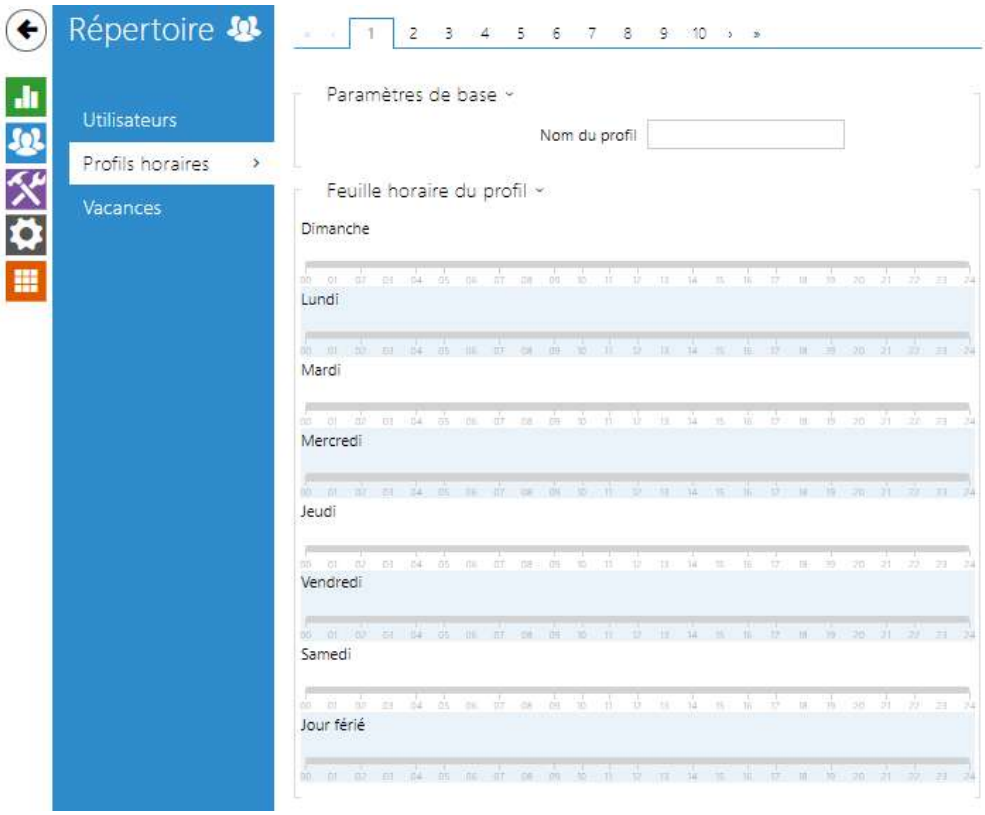
4. Badgez la carte sur le lecteur.



5. L'identifiant de la carte a été reconnu.

N'oubliez pas de sauvegarder la configuration.

5.2.2 Profils horaires



Certaines fonctionnalités de l'interphone, telles que les appels sortants, l'accès par carte RFID ou code numérique, peuvent être définies selon des plages horaires. Attribuez un profil temporel à ces fonctions pour définir quand les fonctions doivent être disponibles. Les profils temporels peuvent répondre aux exigences suivantes :

- bloquer tous les appels destinés à un utilisateur sélectionné au-delà de l'intervalle de temps défini
- bloquer les appels vers des numéros de téléphone d'un utilisateurs sélectionnés au-delà de l'intervalle défini
- bloquer l'accès RFID pour un utilisateur au-delà de l'intervalle de temps défini
- bloquer l'accès au digicode d'un utilisateur au-delà de l'intervalle de temps défini
- blocage du commutateur au-delà de l'intervalle de temps défini

Chaque profil horaire définit la disponibilité de la fonction via un calendrier hebdomadaire. Il suffit de définir De–À et de spécifier les jours de la semaine pour la disponibilité. Les **Interphones IP 2N** vous permettent de définir jusqu'à 20 profils horaires (selon le modèle d'interphone) pouvant être affectés aux fonctions souhaitées. Référez-vous à la section Utilisateurs, carte d'accès et paramètres des interrupteurs.

Les profils horaires sont définis non seulement à l'aide de la feuille de temps hebdomadaire, mais également manuellement à l'aide de codes d'activation / désactivation spéciaux que vous pouvez attribuer aux utilisateurs après votre arrivée au bureau ou avant de quitter votre bureau, par exemple. Entrez les codes d'activation / désactivation à l'aide du clavier numérique de votre interphone ou de votre téléphone IP (pendant l'appel vers l'interphone).

Référez-vous à la section **Répertoire / Profil horaire** pour paramétrer les plages horaires.

Liste des paramètres

- **Nom du profil** – entrez un nom de profil. Ce paramètre est facultatif et vous aide à rechercher des éléments dans la liste des profils horaires et à sélectionner plus facilement des profils dans les paramètres d'interrupteur, de carte et de numéro de téléphone.

Définissez le profil de temps actif dans une semaine. Un profil est actif lorsque l'heure actuelle tombe dans les intervalles définis.

Si un jour est marqué comme jour férié (voir **Répertoire** → **Vacances**), la dernière ligne du tableau (vacances) est appliquée quel que soit le jour de la semaine.

Assurez-vous que les paramètres en temps réel sont corrects (reportez-vous à la sous-section Date et heure) pour que cette fonctionnalité fonctionne correctement.

Note

- *Vous pouvez définir n'importe quel nombre d'intervalles de temps par jour : 8:00–12:00, 13:00–17:00, 18:00–20:00, par exemple.*
- *Pour que le profil horaire soit valide toute la journée, entrez un intervalle quotidien : 00:00–24:00.*

5.2.3 Vacances

Ici, vous pouvez sélectionner les jours fériés (y compris le dimanche). Vous pouvez leur attribuer des intervalles de temps différents de ceux des jours ouvrables dans les profils horaires.

Vous pouvez définir des vacances pour les 10 prochaines années (cliquez sur le numéro de l'année en haut de l'écran pour sélectionner une année). L'écran affiche le calendrier pour toute l'année en cours. Un calendrier s'affiche pour vous permettre de sélectionner / désélectionner un jour férié. Les jours fériés fixes (annuelles) sont marquées en vert et les vacances variables (valables pour l'année en question uniquement) sont en bleu. Cliquez une fois sur une date pour sélectionner un jour férié fixe, cliquez deux fois pour sélectionner un jour férié variable et cliquez pour la troisième fois pour supprimer le jour férié de la liste.

5.3 Appel

L'appel est la fonction de base de l'interphone – il vous permet d'établir une connexion avec d'autres appareils finaux dans les réseaux IP. Les **Interphones IP 2N** supportent le SIP ouvert et sont compatibles et certifiés avec les fabricants leaders de PBX SIP et d'équipement de téléphonie IP (CISCO, Avaya, Broadsoft, etc.).

Nos interphones prennent en charge jusqu'à cinq appels en parallèle : 1 appel sortant et jusqu'à 4 appels entrants. Un seul des appels peut être **actif** – le flux audio est interconnecté avec le microphone et le haut-parleur et le flux vidéo avec la caméra. Les autres appels sont toujours **inactifs** – le microphone et le haut-parleur sont mis en sourdine, l'interphone reçoit les codes DTMF afin que l'interlocuteur puisse contrôler l'interphone (activer / désactiver les profils, les utilisateurs, les interrupteurs etc.).

En général, les interphones sont utilisés pour les appels sortants et les appels entrants sont inactifs - le microphone et le haut-parleur sont en mode sourdine. Cependant, vous pouvez configurer votre interphone pour que les appels entrants soient actifs et sonnent, voir 5.3.1

Paramètres généraux. Appuyez sur les touches * et # du clavier numérique pour répondre et mettre fin à un appel entrant.

Les **Interphones IP 2N** utilisent les protocoles **G.711**, **L16**, **G.722** et **G.729** pour crypter ou compresser les flux audio et les Codecs **H.263** ou **H.264** pour la compression de flux vidéo. Les codecs à large bande L16 et G.722 sont disponibles dans certains modèles **d'interphone IP 2N** uniquement. Choisissez vos codecs préférentiels dans l'onglet Audio ou Vidéo.

Explication des termes de téléphonie IP

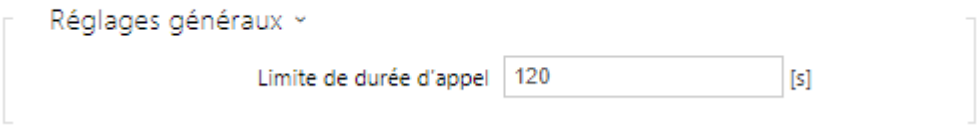
- **SIP (Session Initiation Protocol)** – c'est un protocole de transmission d'appel téléphonique utilisé dans la téléphonie IP. Il est principalement utilisé pour établir, terminer et renvoyer les appels entre deux appareils SIP (l'interphone et un autre téléphone IP, dans ce cas). Les appareils SIP peuvent établir des connexions directement entre eux (appel direct SIP) ou, généralement, via un ou plusieurs serveurs : SIP Proxy et SIP Registrar.
- **Proxy SIP** – c'est un serveur de réseau IP responsable du routage des appels (transfert d'appel vers une autre entité plus proche de la destination). Il peut y avoir une ou plusieurs unités proxy SIP entre les utilisateurs.
- **Registrar SIP** – c'est un serveur de réseau IP responsable de l'enregistrement des utilisateurs dans une certaine section du réseau. En règle générale, l'enregistrement d'un périphérique SIP est nécessaire pour qu'un utilisateur puisse être accessible aux autres sur un certain numéro de téléphone. SIP Registrar et SIP Proxy sont souvent installés sur un même serveur.
- **RTP (Real-Time Transport Protocol)** – est un protocole définissant le format de paquet standard pour la transmission audio et vidéo sur les réseaux IP. L'interphone IP 2N utilise le protocole RTP pour la transmission de flux audio et vidéo pendant un appel. Les paramètres de flux (numéros de port, protocoles et codecs) sont définis et négociés via le protocole SDP (Session Description Protocol).

Les **interphone IP 2N** supportent trois types de signalisation SIP :

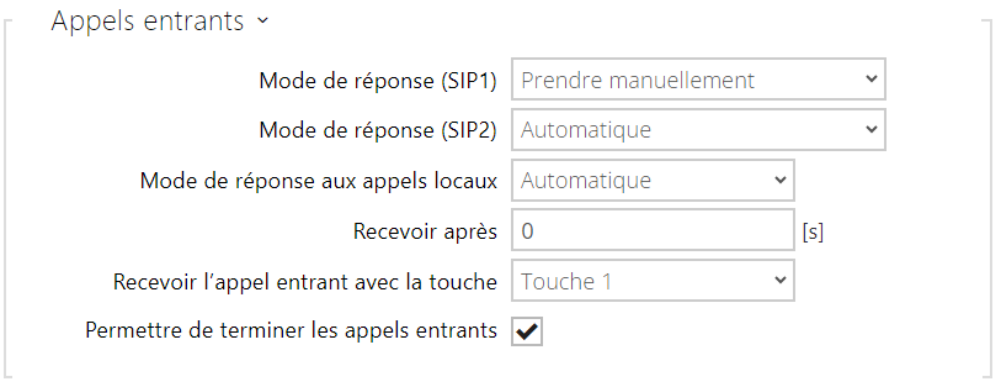
- via le protocole **User Datagram Protocol (UDP)**, qui est la méthode de signalisation non sécurisée la plus fréquemment utilisée
- via le protocole **Transmission Control Protocol (TCP)**, qui est une méthode de signalisation non sécurisée moins fréquente, mais recommandée
- via le protocole **Transaction Layer Security (TLS)**, où les messages SIP sont protégés contre la surveillance et la modification par des tiers (sauf le modèle **2N® IP Uni**)

Voici les onglets que vous pouvez trouver dans cette section :

5.3.1 Paramètres généraux



- **Limite de la durée d'appel** – fixer la limite de durée d'appel après laquelle un appel est automatiquement terminé. L'interphone signale la fin de l'appel avec un bip sonore 10 secondes avant la fin. Saisir n'importe quel caractère DTMF dans l'appel (# sur votre téléphone IP, par ex.) pour prolonger la durée d'appel. Si la durée de l'appel est définie sur 0 et que le SRTP n'est pas utilisé, l'appel n'est pas limité dans le temps.

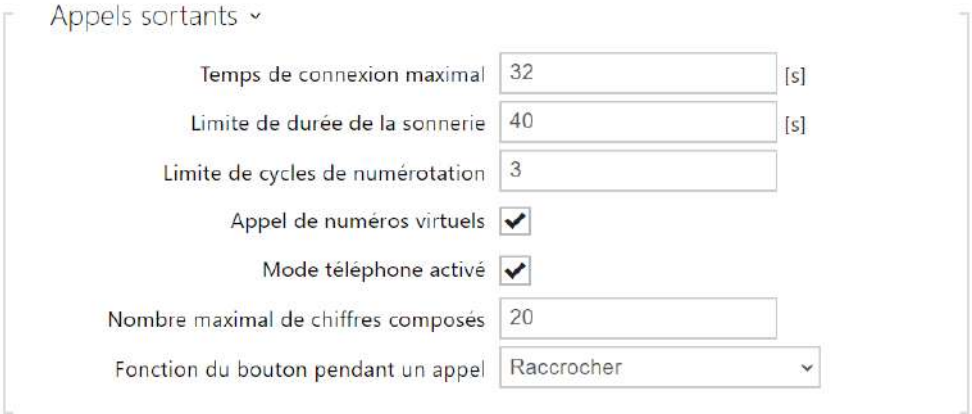


- **Mode de réponse (SIP1, SIP2)** – définissez la manière dont l'interphone va recevoir les appels entrants. Les 3 options suivantes sont possibles :
  - **Toujours occupé** – l'interphone rejette tous les appels entrant.
  - **Prendre manuellement** – l'interphone signale les appels entrants et l'utilisateur y répond à l'aide d'un bouton sur le clavier numérique.
  - **Automatique** – l'interphone répond automatiquement aux appels entrants. Vous pouvez définir séparément le mode de réception des appels pour chaque compte SIP.
  - **Automatique (DTMF uniquement)** – l'interphone répond automatiquement aux appels entrants seulement si un DTMF hors connexion à un microphone et un haut-parleur est reçu.
  - **Automatique (caché)** – l'interphone décroche automatiquement un appel entrant, sans afficher l'identité de l'appelant ni aucun signe d'accompagnement de décrochage d'appel.
- **Mode de réponse aux appels locaux** – définissez la manière dont l'interphone va recevoir les appels entrants. Les 3 options suivantes sont possibles :
  - **Toujours occupé** – l'interphone rejette tous les appels entrant.

  - **Prendre manuellement** – l'interphone signale les appels entrants et l'utilisateur y répond à l'aide d'un bouton sur le clavier numérique.
  - **Automatique** – l'interphone répond automatiquement aux appels entrants. Vous pouvez définir séparément le mode de réception des appels pour chaque compte SIP.
  - **Automatique (caché)** – l'interphone décroche automatiquement un appel entrant, sans afficher l'identité de l'appelant ni aucun signe d'accompagnement de décrochage d'appel.
- **Recevoir après** – le temps après lequel l'appel est automatiquement pris en mode de réponse automatique aux appels. Si l'un des **Modes de messagerie vocale** est activé sur un appareil prenant en charge la messagerie vocale, l'appel sera pris après ce délai et le message sélectionné sera lu en mode de réponse automatique et manuel. Si cette valeur est 0, le message est lu immédiatement. Commun à tous les comptes SIP.
- **Recevoir l'appel entrant avec la touche** – permet de prendre un appel entrant avec la touche choisie de sélection rapide. En réglant sur « Aucun », la fonction est désactivée.

> **Observation**
>
> - La fonction Accepter un appel entrant avec une touche n'est pas affichée sur les modèles **2N® IP Force** et **2N® IP Vario** avec un clavier. Un appel entrant peut être accepté pour ces modèles en utilisant la touche marquée d'un combiné vert sur le clavier, sans configuration préalable requise.

- **Permettre de terminer les appels entrants** – permet aux utilisateurs de rejeter ou de terminer un appel à l'aide de l'interphone. Lorsque la fonction est désactivée, la touche du combiné de rejet ou de fin d'appel ne fonctionne pas et l'icône de rejet ou de fin d'appel n'apparaît pas sur l'écran. L'appel peut encore être interrompu en démarrant un nouvel appel sortant à partir de l'interphone.



- **Temps de connexion maximal** – Définit le temps de connexion maximal pour les appels sortants après lequel ils sont automatiquement terminés. Si les appels sont acheminés vers le réseau GSM via des passerelles GSM, il est conseillé de définir une valeur d'une durée supérieure à 20 s.

- **Limite de la durée de sonnerie** – réglez le paramètre d'appel sortant et la limite de temps de sonnerie après laquelle les appels doivent automatiquement prendre fin. Si les appels sont dirigés vers le réseau GSM via des passerelles GSM, il est recommandé de configurer une valeur supérieure à 20 secondes. Valeur minimale: 1 s, valeur maximale: 600 s. Définissez 0 pour désactiver ce paramètre.
- **Limite de cycles de numérotation** – fixez le nombre maximal des cycles de numérotation du remplaçant de l'utilisateur si l'utilisateur appelé selon sa position dans le répertoire téléphonique est inaccessible. Cette fonction permet d'éviter une impasse si le remplaçant de l'utilisateur est réglé sur la même valeur dans le répertoire téléphonique. Les options relatives aux limites des cycles d'appels sont indiquées dans le sous-chapitre 5.4.1.1 Limite des cycles d'appels.
- **Mettre fin aux appels de groupe dès le premier rejet** – permet à l'appareil de mettre fin à tous les appels d'un appel de groupe sortant si l'une des destinations appelées rejette l'appel.
- **Appel de numéros virtuels** – permet l'appel de numéros virtuels d'utilisateurs définis.
- **Mode de numérotation étage et appartement** – autorise les appels par étages et par l'appartements. Dans ce mode, entrez le numéro virtuel attribué à l'utilisateur via le clavier numérique. Disponible uniquement sur le modèle **2N® IP Vario**. Entrez le code d'étage / appartement correspondant au numéro virtuel de l'utilisateur. Le code peut inclure des chiffres et des lettres A–F.
- **Mode téléphone activé** – activer l'option pour mettre en place les appels directement vers les numéros de téléphone composés via le clavier numérique de l'interphone. Saisir la séquence de touches du numéro de téléphone pour la mise en place de l'appel.

Conseil

- Procédez de la sorte sur les modèles **2N® IP Force** et **2N® IP Vario** : pressez **numéro_téléphone** (ou numéro_téléphone pour le **2N® IP Verso**). Si vous ne pressez pas la touche (ou pour le modèle **2N® IP Verso**) comme touche finale, le numéro composé sera confirmé automatiquement après expiration de la durée disponible pour la composition comme si vous aviez pressé la touche (ou pour le **2N® IP Verso**).

- **Nombre maximal de chiffres composés** – paramétrer le nombre maximal de chiffres d'un numéro de téléphone dans le mode Téléphonie. Si cette limite est atteinte, le numéro est composé automatiquement sans appuyer sur *.
- **Fonction du bouton pendant un appel** – définit la fonction de la touche de numérotation rapide lors d'un appel sortant. Vous pouvez seulement paramétrer le bouton qui a émis l'appel.

- **Port RTP de départ** – réglez le port RTP local de départ dans l'intervalle de la longueur de 64 ports à utiliser pour les transmissions audio et vidéo. La valeur par défaut est 4900 (c.-à-d. que l'intervalle utilisée est 4900-4963). Ce paramètre n'est défini que pour le compte 1 mais s'applique aux deux comptes SIP.
- **Délai d'attente RTP** – définir le paquet RTP de flux audio recevant un délai d'attente lors d'un appel. Si la limite est dépassée (les paquets RTP ne sont pas transmis), l'appel est coupé par l'interphone. Réglez le paramètre sur 0 pour désactiver cette fonction. Ce paramètre n'est défini que pour le compte 1 mais s'applique aux deux comptes SIP.
- **Journalisation du protocole SIP avancée** – permet d'écrire des informations plus détaillées sur la téléphonie SIP dans le syslog (pour le dépannage uniquement).

5.3.1.1 Limite des cycles d'appels

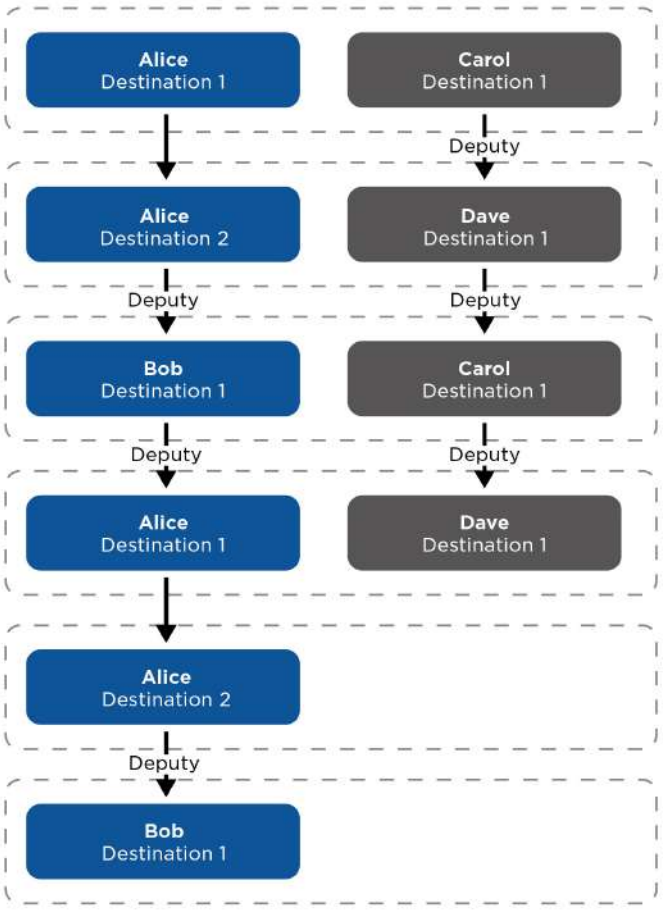
Ce paramètre définit le nombre maximal d'appels consécutifs passés vers le poste d'appel (destination) lorsque, en cas d'indisponibilité, un cycle d'appel de représentants est déterminé (l'exemple le plus simple d'un cycle d'appel consiste à se paramétrer soi-même comme un représentant, deux utilisateurs configurés en tant que représentants mutuels en est un autre exemple).

Exemple 1

L'algorithme résout d'abord les ramifications du schéma indépendamment les unes des autres. Dans l'exemple ci-dessous, les utilisateurs Alice et Carol sont configurées sous une seule touche (en appuyant sur la touche, deux appels parallèles sont réalisés en une fois). La limite du cycle d'appel est définie sur 2. Alice a deux numéros de téléphone (poste d'appel), les autres utilisateurs n'ont qu'un seul poste d'appel. Les représentants sont configurés comme suit :

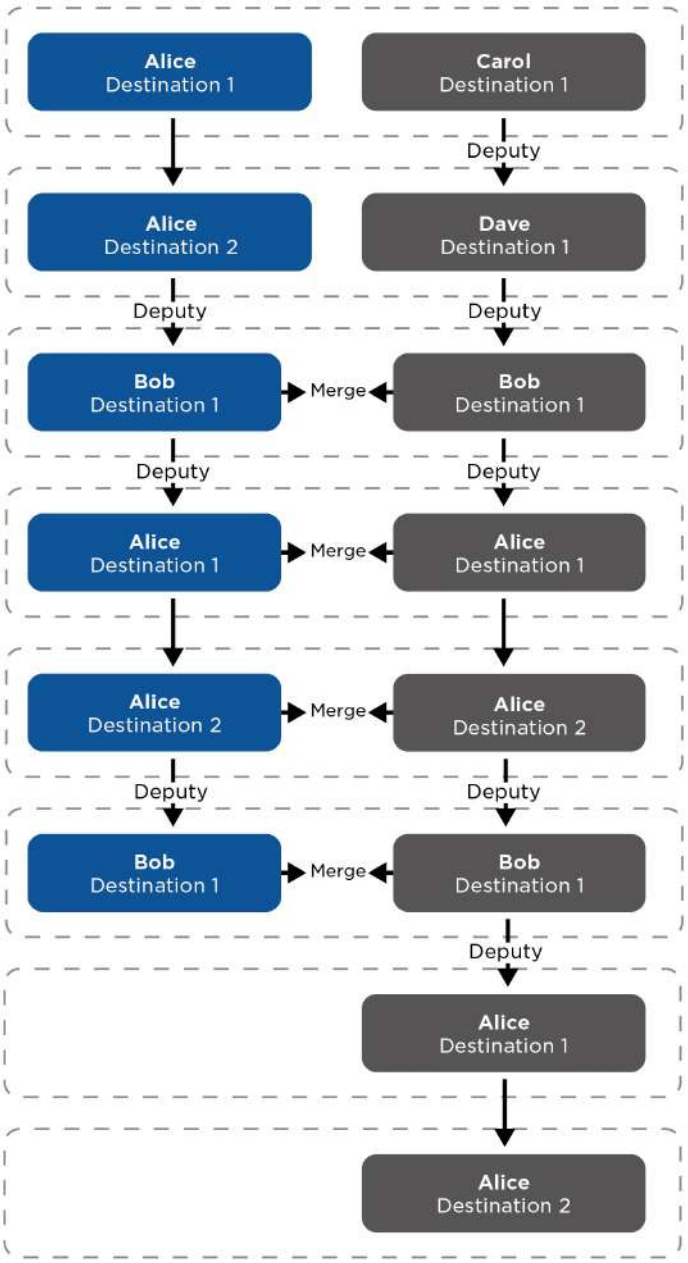
- Alice est la représentante de Bob
- Bob est le représentant d'Alice
- Carol est la représentante de Dave
- Dave est le représentant de Carol

Le schéma d'appel résultant est le suivant (lorsque l'appel n'est ni décroché, ni refusé) :



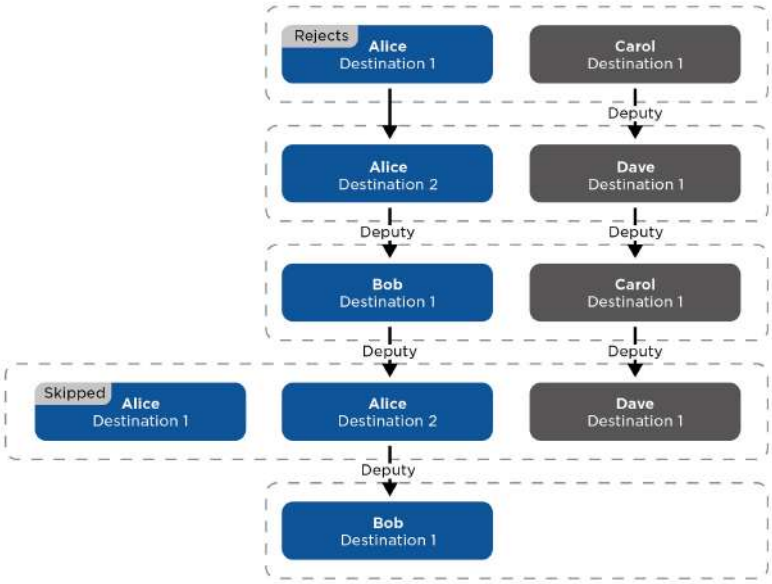
Exemple 2

Prenons l'exemple précédent et interchangeons les représentants Dave et Bob. Il y a une jonction entre les deux ramifications (à partir de l'étape 3, un seul appel a lieu). On peut également voir sur le graphique qu'Alice est finalement appelée trois fois. La limite du cycle d'appel s'applique de fait séparément à chaque ramification. Alice n'est en fait appelée que deux fois sur la ramification bleue et également seulement deux fois sur la ramification violette.



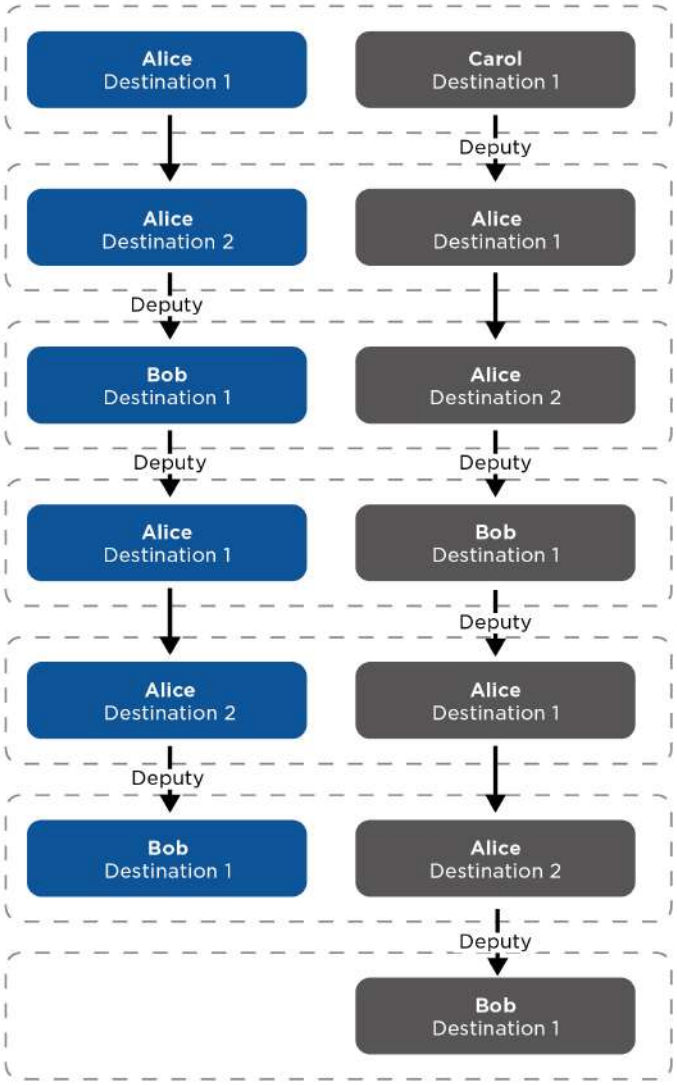
Exemple 3

Prenons la configuration de l'exemple 1 et considérons qu'Alice refuse l'appel de son premier poste. L'algorithme ignore alors cette destination (l'utilisateur a activement refusé l'appel et il ne sert à rien de l'appeler de nouveau). Le refus des appels de différents postes d'appel permet de modifier dynamiquement les groupes d'appel dans les étapes individuelles. Le fait d'ignorer un poste d'appel qui a refusé un appel s'applique à toutes les ramifications, quelle que soit celle pour laquelle l'appel a été refusé.



Exemple 4

Il peut arriver que deux postes d'appel d'un même utilisateur soient appelés simultanément. Ceci peut se faire en paramétrant un schéma similaire à l'image ci-dessous, mais cela peut également être fait en ignorant les destinations qui ont précédemment refusé l'appel.

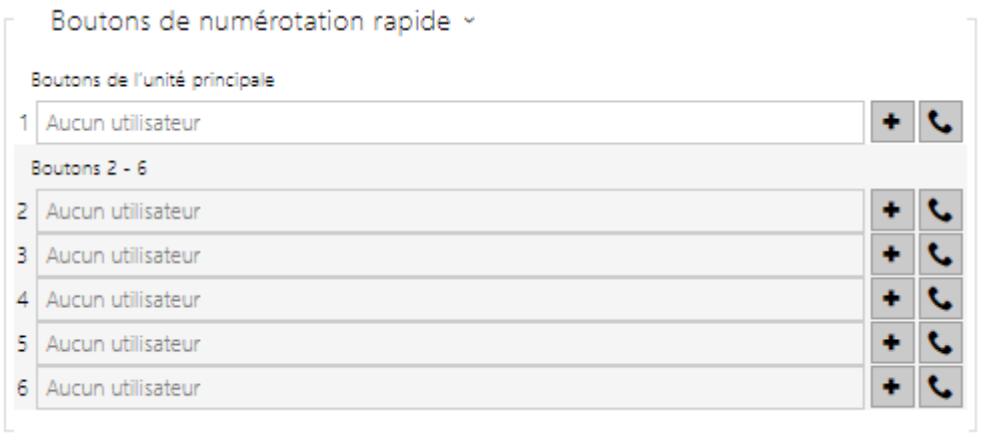


5.3.2 Composition

Boutons de numérotation rapide

Attribuez les utilisateurs du **Répertoire > Utilisateurs** aux boutons de numérotation rapide. Par défaut, tous les boutons disponibles sont attribués aux utilisateurs répertoriés. Un bouton non affecté peut être utilisé pour l'automatisation ou l'activation d'un interrupteur, par exemple. Sur le modèle **2N® IP Base**, sélectionnez tout d'abord le nombre de boutons souhaités (1 ou 2) dans la section **Hardware > Extendeur**.

- **Effacer les affectations des boutons** – toutes les touches associées aux utilisateurs seront supprimées.



Affiche la liste de tous les boutons d'interphone potentiellement disponibles. La liste inclut ceux qui sont physiquement absents. Sur certains modèles (**2N® IP Vario**, **2N® IP Verso**), a liste des boutons est divisée en groupes de 8/5 éléments correspondant aux modules d'extension des boutons. Cliquez sur  pour attribuer un ou plusieurs utilisateurs au bouton choisi. Pour rechercher un utilisateur dans la liste, utilisez le champ de texte intégral et le nom de l'utilisateur. Un bouton de numérotation rapide peut être partagé par plusieurs utilisateurs.

Cliquez sur  pour générer un appel de test sans avoir à presser manuellement le bouton. Une fenêtre de dialogue s'affiche avec des informations détaillées sur l'appel en cours (utilisateur, direction de l'appel, état, raison et heure du dernier événement).

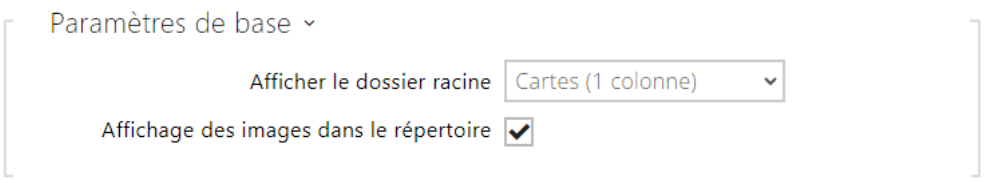
Note

- Jusqu'à 16 utilisateurs peuvent être attribués à un bouton de numérotation.

- Le nombre total maximal de numéros pouvant être composés en parallèle est de 16, ce qui peut se produire lorsque des appels de groupe et plusieurs numéros attribués à une touche de numérotation rapide sont utilisés simultanément.

Afficher le répertoire

Cet onglet vous permet de configurer une liste d'utilisateurs structurée. Vous pouvez créer pratiquement n'importe quel nombre de groupes et affecter n'importe quel nombre d'utilisateurs à chacun de ces groupes. Il n'est pas possible d'affecter un utilisateur plus d'une fois dans un même groupe mais un utilisateur peut faire partie de plusieurs groupes différents.



- **Afficher le dossier racine** – Permet de choisir l'affichage du dossier racine du répertoire sur l'écran d'accueil de l'équipement. Il est possible de choisir l'affichage en cartes (avec une image plus grande) ou l'affichage de la liste classique des éléments (l'affichage des images dans la liste des éléments est alors contrôlé par le paramètre Afficher les images). Les paramètres ne prendront effet que lorsque l'utilisateur naviguera vers une autre partie de l'interface graphique (par exemple vers Recherche).
- **Affichage des images dans le répertoire** – Vous permet de choisir d'afficher ou non les images dans l'affichage du répertoire à l'écran lorsqu'elles sont affichées dans une liste d'éléments.

Les dossiers et les utilisateurs créés sont affichés sur la gauche. Cliquez sur pour ajouter un nouveau dossier. Cliquez sur pour supprimer un groupe ou un utilisateur du répertoire. Cliquez sur pour renommer un groupe. Cliquez sur pour déplacer un utilisateur de la liste principale vers un dossier.

Les utilisateurs affectés au groupe sélectionné sont affichés sur la droite. Cliquez sur pour ajouter un utilisateur à un groupe. L'utilisateur restera dans la liste principale après avoir été assigné au groupe. La touche permet de mettre en surbrillance à l'écran le premier élément du groupe. Cliquez sur pour le supprimer.

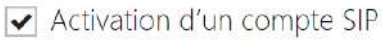
Les groupes et les utilisateurs sont classés par ordre alphabétique sur l'écran. Cliquez sur pour leur assigner une priorité. Les éléments du répertoire ont 8 priorités possibles. La priorité 1 place l'élément en tête de liste, l'absence de priorité le place en fin de liste. Si plusieurs éléments ont la même priorité, ils sont regroupés et triés par ordre alphabétique.

Caution

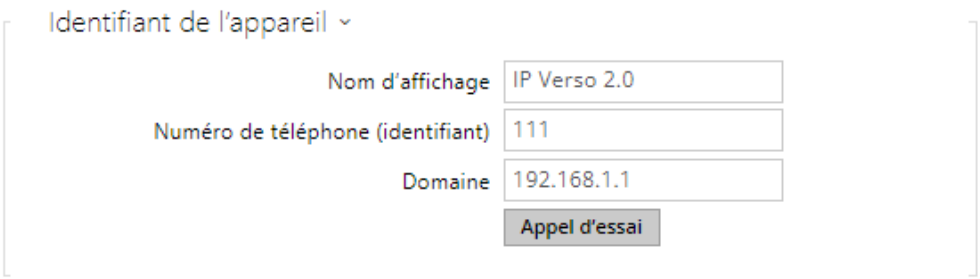
N'oubliez pas de sauvegarder les changements sur le répertoire.
Les modifications apportées aux paramètres (affichage des photos, dossier racine, contenu, etc.) sont effectives une fois accédé au menu de recherche ou de numérotation.

5.3.3 SIP 1 / SIP 2

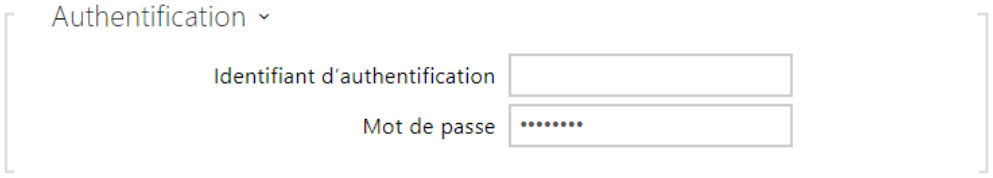
Les interphones IP 2N permettent la configuration de deux comptes SIP indépendants. Ainsi, l'interphone peut être enregistré sous deux numéros de téléphone, avec deux échanges SIP différents, etc. Les deux comptes SIP traitent les appels entrants de manière équivalente. Les appels sortants sont principalement traités par le compte SIP 1 ou si le compte SIP 1 n'est pas enregistré (par exemple, en raison d'une erreur d'échange SIP), par le compte SIP 2. Sélectionnez le numéro de compte pour les numéros de téléphone inclus dans l'annuaire afin de spécifier le compte à utiliser pour les appels sortants (exemple : **2568/1** – les appels vers l'extension 2568 passent par le compte SIP 1, **sip:1234@192.168.1.1/2** les appels SIP Uri par le compte SIP 2).



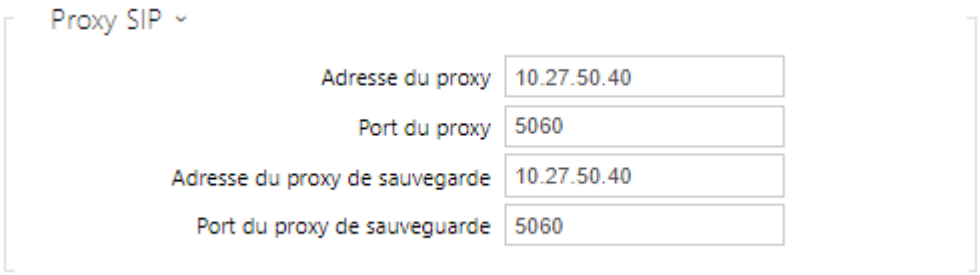
- **Activation d'un compte SIP** – permet d'utiliser un compte SIP pour les appels. Si le compte n'est pas autorisé, l'utiliser pour passer des appels sortants ou recevoir des appels entrants est impossible.



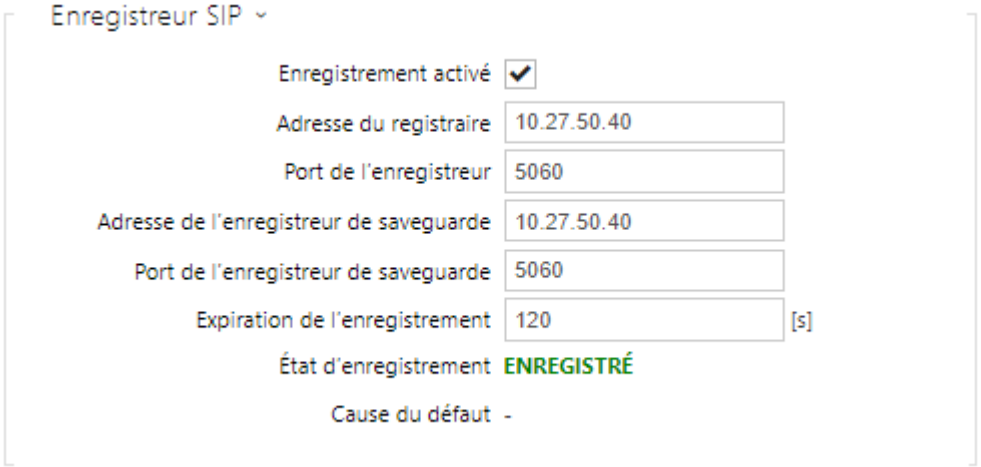
- **Nom d'affichage** – paramétrez le nom à afficher sur le téléphone de la personne appelée.
- **Numéro de téléphone (identifiant)** – paramétrer le numéro de téléphone de l'interphone (ou un autre identifiant unique comprenant des lettres et des chiffres). Ensemble avec le domaine, ce numéro représente un identifiant unique de l'interphone lors d'appels et d'enregistrements.
- **Domaine** – paramétrer le nom de domaine du service avec lequel l'interphone est enregistré. Normalement, il est identique au proxy SIP ou à l'adresse du registrar.
- **Appel d'essai** – affiche une boîte de dialogue avec la possibilité d'effectuer un appel test au numéro de téléphone sélectionné, voir ci-dessous :



- **Identifiant d'authentification** – autre ID utilisateur utilisé pour authentifier l'appareil. Le numéro de téléphone (ID) sera utilisé dans le cas où ce paramètre est vide.
- **Mot de passe** – saisissez le mot de passe pour l'authentification. Ce paramètre est uniquement appliqué si votre PBX nécessite une authentification.



- **Adresse du proxy** – paramétrez l'adresse IP ou le nom de domaine du proxy SIP.
- **Port du proxy*** – paramétrez le port du proxy SIP. L'appareil utilise le port par défaut selon la couche transport (5060 ou 5061) ou le port obtenu du DNS si le paramètre est vide ou défini sur 0.
- **Adresse du proxy de sauvegarde** – l'adresse IP ou le nom de domaine du proxy SIP de sauvegarde. L'adresse sera utilisée en cas où le proxy principal ne répond pas aux requêtes.
- **Port du proxy de sauvegarde*** – paramétrez le port du proxy SIP de sauvegarde. L'appareil utilise le port par défaut selon la couche transport (5060 ou 5061) ou le port obtenu du DNS si le paramètre est vide ou défini sur 0.



- **Enregistrement activé** – activez l'enregistrement de l'interphone avec l'enregistreur SIP paramétré.
- **Adresse du registrar** – paramétrez l'adresse IP ou le nom de domaine du registrar SIP.
- **Port du registrar*** – paramétrez le port du registrar SIP. L'appareil utilise le port par défaut selon la couche transport (5060 ou 5061) ou le port obtenu du DNS si le paramètre est vide ou défini sur 0.

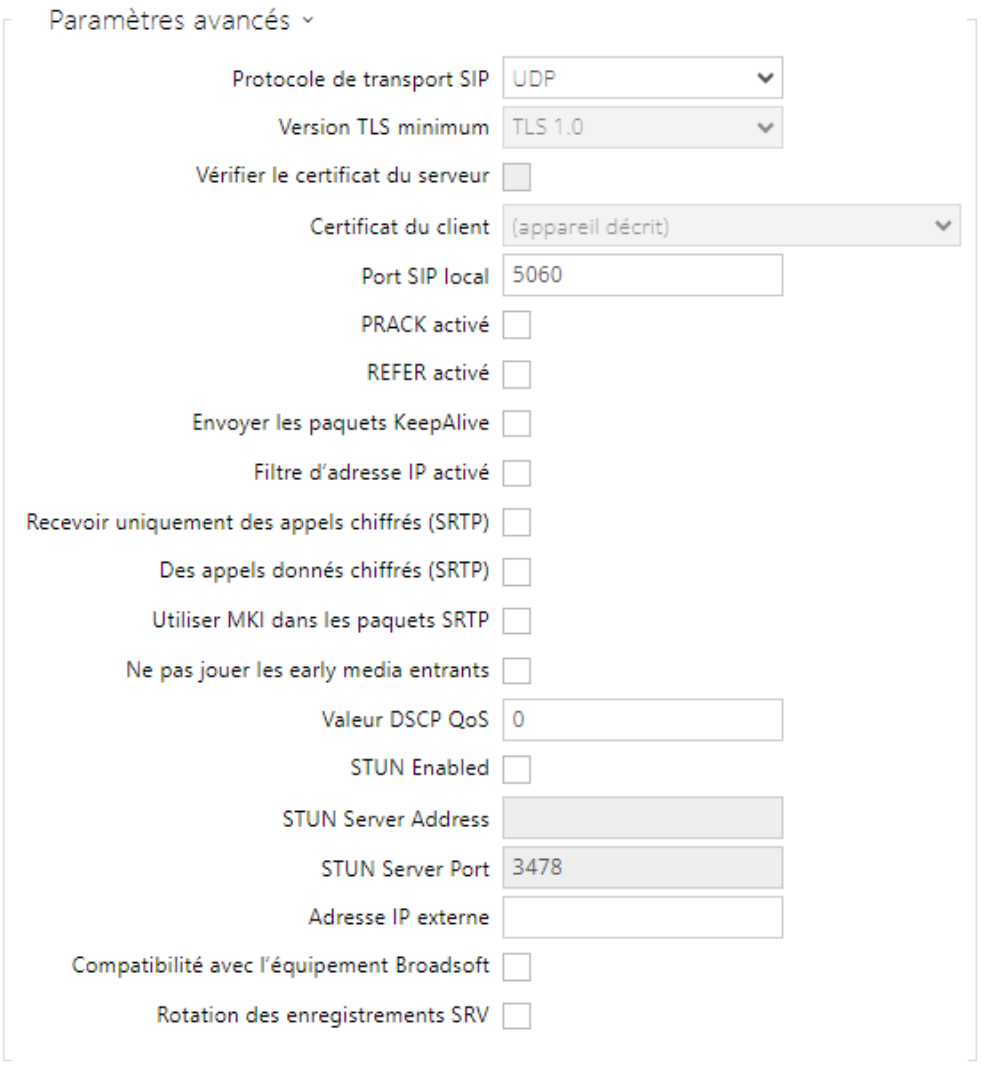
- **Adresse du registrar de sauvegarde** – l'adresse IP ou le nom de domaine du registrar SIP de sauvegarde. L'adresse sera utilisée en cas où le registrar principal ne répond pas aux requêtes.
- **Port du registrar de sauvegarde*** – paramétrez le port du registrar SIP de sauvegarde. L'appareil utilise le port par défaut selon la couche transport (5060 ou 5061) ou le port obtenu du DNS si le paramètre est vide ou défini sur 0.
- **Expiration de l'enregistrement** – définissez l'expiration d'enregistrement, qui affecte la charge du réseau et du registrar SIP par des demandes d'enregistrements envoyées régulièrement. Le registrar SIP peut modifier la limite d'expiration sans vous en informer.
- **État d'enregistrement** – affiche l'état actuel de l'enregistrement (Non-enregistré, Enregistré, En cours d'enregistrement...etc.).
- **Cause du défaut** – affiche le motif de l'échec de la dernière tentative d'enregistrement: la dernière réponse d'erreur du registrar, par ex : 404 introuvable.

Conseil

- Pour définir le proxy sortant, indiquez l'adresse du proxy sortant dans les paramètres d'adresse de proxy et d'adresse du registrar. Domaine = adresse du registraire.

Observation

- Si le **paramètre*** est laissé vide ou si la valeur du paramètre est 0, le port par défaut est utilisé en fonction du protocole de transport sélectionné (5060 pour TCP ou UDP, 5061 pour TLS).



- **Protocole de transport SIP** – définissez le protocole de communication SIP : UDP (par défaut), TCP ou TLS.
- **Version TLS minimum** – définissez la version TLS minimale, autorisée pour la connexion à l'appareil.
- **Vérifier le certificat du serveur** – vérifie le certificat public du serveur ACS vis à vis des certificats CA enregistrés dans l'appareil.
- **Certificat du client** – spécifie le certificat client et la clef privée au moyen desquels est vérifiée l'autorisation de l'interphone à communiquer avec le serveur ACS.

- **Port SIP local** – définissez le port local à utiliser pour la signalisation SIP. Ce paramètre n'est appliqué qu'après un redémarrage de l'interphone. La valeur par défaut est 5060.
- **PRACK activé** – activez la méthode PRACK pour une confirmation fiable des messages SIP avec des codes de 101 à 199.
- **REFER activé** – activez le renvoi d'appel via la méthode REFER.
- **Envoi de paquets de supervision** – déterminez si, pendant les appels, l'interphone doit envoyer périodiquement des demandes d'option SIP pour connaître l'état de la station appelée (pour détecter un échec de station, par exemple).
- **Filtre d'adresse IP activé** – activez le blocage de réception de paquets SIP provenant d'adresses autres que celles du proxy SIP et du registrar SIP. L'objet principal de cette fonction est d'améliorer la sécurité des communications et d'éliminer les appels téléphoniques non autorisés.
- **Recevoir uniquement les appels cryptés (SRTP)** – il règle la restriction des appels reçus sur ce compte sur des appels chiffrés avec le protocole SRTP. Les appels non cryptés seront rejetés. Dans le même temps, le TLS est recommandé comme protocole de transport SIP pour une sécurité accrue.
- **Appels sortants cryptés (SRTP)** – les appels sortants devront être cryptés avec le protocole SRTP . En même temps, pour accroitre la sécurité, nous vous recommandons d'utiliser le TLS comme un protocole de transport SIP.
- **Utiliser MKI dans les paquets SRTP** – permet d'utiliser MKI (Master Key Identifier), qui est requis par la contrepartie pour identifier la clé principale lors de la rotation de plusieurs clés dans les paquets SRTP.
- **Ne pas jouer les Early media entrants** – il empêche la lecture des flux audio entrant avant le décrochage du téléphone (early media) envoyé par certaines centrales ou par certains appareils. Au lieu de cela, la sonnerie locale standard sera jouée.
- **Valeur DSCP QoS** – définissez la priorité de paquets SIP dans le réseau. La valeur programmée est envoyée dans le champ TOS (Type of Service) de l'en-tête du paquet IP. La valeur est saisie sous forme de nombre décimal.

Tip

Valeurs DSCP QoS recommandées			
	QoS décimale	**QoS hexadécimale**	**Qos DSCP décimale (ToS)**
Signalisation	24 / 26	18 / 1A	96 / 104
Audio	46	2E	184
Vidéo	40	28	160

- **STUN activé** – activez la fonctionnalité STUN pour le compte SIP. L'adresse et les ports acquis à partir du serveur STUN configuré seront utilisés dans les en-têtes SIP et la négociation des médias SDP.

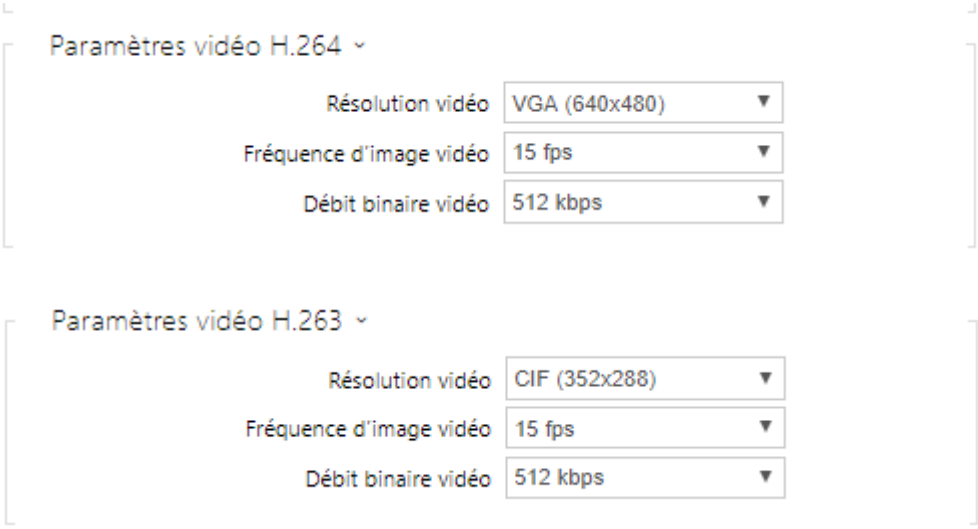
- **Adresse du serveur STUN** – définissez l'adresse IP du serveur STUN qui sera utilisé pour ce compte SIP.
- **Port du serveur STUN** – définissez le port du serveur STUN qui sera utilisé pour ce compte SIP.
- **Adresse IP externe** – configurez l'adresse IP publique ou le nom d'hôte du routeur auquel votre interphone est connecté. Si l'adresse IP de l'interphone est une adresse publique, laisser ce champ vide.
- **Compatibilité avec l'équipement Broadsoft** – Définit le mode de compatibilité avec les panneaux de commande Broadsoft. Dans ce mode, lorsque l'interphone reçoit une nouvelle invitation (re-invite) de la centrale, il répond au lieu du menu complet en répétant le dernier SDP envoyé avec les codecs actuellement utilisés.
- **Rotation des enregistrements SRV** – Permet la rotation des enregistrements SRV pour le proxy SIP et le registraire. Il s'agit d'une méthode alternative de basculement vers des serveurs de sauvegarde en cas de défaillance ou d'indisponibilité des serveurs principaux.

Observation

- Pour utiliser la requête DNS NAPTR / SRV, il convient d'annuler le paramètre de port pour Proxy/Registrar.

Vidéo

- Activez / désactivez l'utilisation des codecs vidéo pour les configurations d'appel et définirssezleurs priorités.



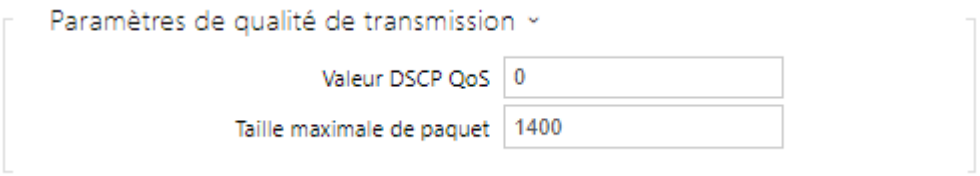
- **Résolution vidéo** – réglez la résolution vidéo pour les appels téléphoniques.
- **Fréquence d'image vidéo** – réglez la fréquence d'image vidéo pour les appels téléphoniques.
- **Débit binaire vidéo** – réglez le débit binaire du flux vidéo pour les appels téléphoniques.

- **PTZ** – activez la fonction PTZ (Pan-Tilt-Zoom) pour contrôler la zone d'affichage de la caméra pendant l'appel via DTMF (la licence **GOLD** sera nécessaire) depuis le clavier numérique de votre téléphone IP. Cliquez sur la touche * pour activer / désactiver le mode PTZ. La signification des touches de téléphone IP en mode PTZ est la suivante :

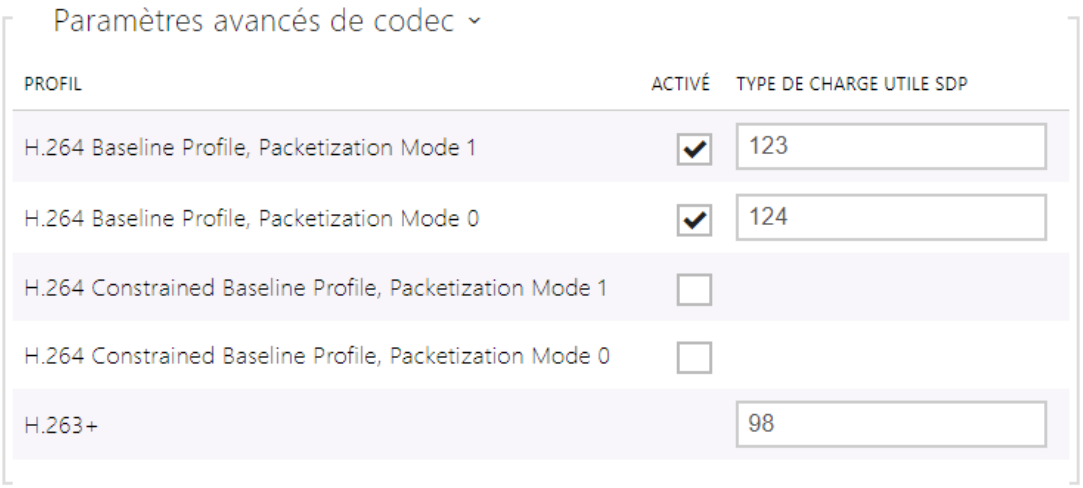
Touche du Poste IP	Fonction du mode PTZ
*	Activer/Désactiver le PTZ
1	Zoomer
3	Dézoomer
2	Déplacer la zone de Zoom vers le haut
4	Déplacer la zone de Zoom vers la gauche
6	Déplacer la zone de Zoom vers la droite
8	Déplacer la zone de Zoom vers le bas
5	Retourner aux paramètres de base

- **Mode PTZ et Face Zooming** – permet d'activer la fonction PTZ (Pan-Tilt-Zoom) ou Face Zooming, qui vous permet d'ajuster la vue de la caméra affichée pendant un appel. Lorsque vous sélectionnez *Face Zooming* , la caméra fait un zoom sur le visage de l'utilisateur qui se tient près de l'appareil. Lorsque vous sélectionnez *Face Zooming – inclinaison uniquement*, la découpe de l'image de la caméra n'est décalée que pour prendre le visage.

> **Observation**
>
> - La fonction Face Zooming est disponible uniquement sur les modèles équipés du processeur ARTPEC-7 de la société Axis.



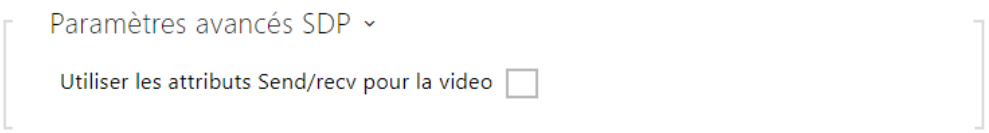
- **Valeur DSCP QoS** – définissez la priorité des paquets RTP dans le réseau. La valeur programmée est envoyée dans le champ TOS (Type of Service) de l'en-tête du paquet IP. La valeur est saisie sous forme de nombre décimal. Les valeurs de QoS recommandées pour la signalisation, l'audio et la vidéo sont indiquées dans le tableau ci-dessus.
- **Taille maximale des paquets** – déterminez la limite de la taille des paquets vidéo RTP à envoyer.



La liste des paramètres avancés du codec peut varier selon le type de l'appareil.

- **H.264 Baseline Profile, Packetization Mode 1**
- **H.264 Baseline Profile, Packetization Mode 0**
- **H.264 Main Profile, Packetization Mode 1**
- **H.264 Main Profile, Packetization Mode 0**
- **H.264 High Profile, Packetization Mode 1**
- **H.264 High Profile, Packetization Mode 0**
- **H.264 Constrained Baseline Profile, Packetization Mode 1**
- **H.264 Constrained Baseline Profile, Packetization Mode 0**
  - **Activé** – permet le mode de mise en paquet et règle le type de charge utile pour chaque codec. Le type de charge utile sera sélectionné automatiquement s'il ne peut pas être réglé manuellement.
  - **Type De Charge Utile SDP** – paramétrer le type de charge utile pour le codec vidéo H.264 (mode 1 de mise en paquet). Vous pouvez définir une valeur comprise entre 96 et 127, éventuellement 0 pour ne pas offrir cette variante de codec.

- **H.263+**
  - **Type De Charge Utile SDP** – paramétrer le type de charge utile pour le codec vidéo H.263+. Définir une valeur comprise entre 96 et 127, ou 0 pour désactiver ce type de codec.



- **Utiliser les attributs Send/recv pour la video** – avant, le réglage était désigné comme Compatiblité avec les téléphones Polycom. Ce réglage sert à garantir la compatibilité avec certains périphériques tiers (Polycom/Cisco et d'autres encore). Si ce régime était éteint, l'interphone envoile le signal send/recv à la place de send/only dans le message SDP ou dans le menu du codec vidéo.

Conseil

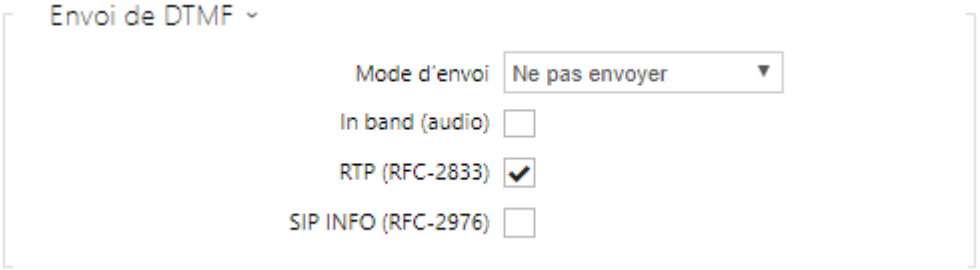
Pour activer la fonction de prévisualisation vidéo sur les postes de téléphonie **Grandstream GXV 3275** (video transmise via Early Media), aucune configuration n'est nécessaire. Vérifiez auprès de votre fournisseur d'IP PBX si cette fonctionnalité est supportée.
Pour activer la fonction de prévisualisation vidéo sur les postes de téléphonie **Gigaset Maxwell 10** (video transmise via des images jpg) il est nécessaire de paramétrer le **Type de connexion** en **Non sécurisé** et l'**Authentification** en **Aucune** dans la section **HTTP API / Camera API**.

- **Autoriser la vidéo entrante** – si ce mode est activé, l'interphone affichera pendant l'appel la vidéo de l'autre partie, si celle-ci en donne l'autorisation.
- **Rapport de forme de la video entrante** – définit le format d'image préféré de la vidéo entrante affichée sur l'écran. Lorsqu'un format d'image différent de l'original est sélectionné, la vidéo est recadrée de manière à remplir la largeur de l'écran dans le nouveau format d'image.
- **Afficher la vidéo sortante** – Choisit si l'interphone affiche un aperçu de la vidéo envoyée lors de l'appel.

Audio

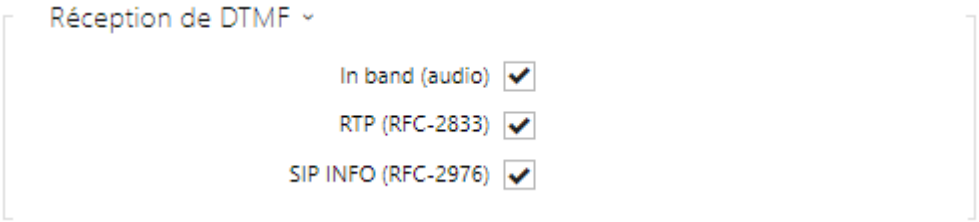
- Activez / désactivez l'utilisation de codecs audio pour les configurations d'appel et définir leurs priorités. Les codecs à large bande L16 et G.722 sont disponibles dans certains modèles d'interphone uniquement. Le codec G.729 est disponible pour tous les interphones IP 2N.

L'onglet ci-dessous vous aide à définir le mode d'envoi des caractères DTMF à partir de l'interphone. Vérifiez les options de réception DTMF et les paramètres du destinataire de l'appel pour un fonctionnement optimal.

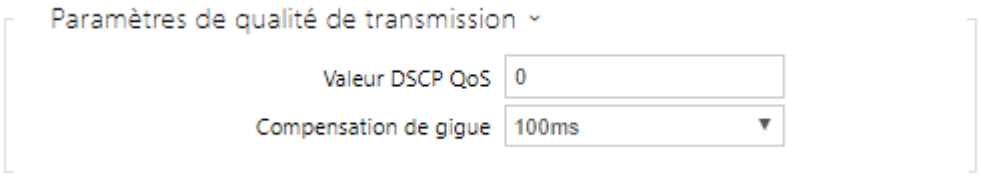


- **Mode d'envoi** – définissez s'il est possible d'envoyer une trame DTMF pendant un appel en appuyant sur les touches 0 à 9, * et # du pavé numérique de l'interphone. Paramétrez le mode d'envoi pour les appels entrants/sortants/tous les appels.
- **In band (audio)** – activez l'envoi de la double tonalité DTMF classique dans la bande audio.
- **RTP (RFC-2833)** – activez l'envoi de DTMF via RTP conformément au RFC-2833.
- **SIP INFO (RFC-2976)** – activez l'envoi de DTMF via messages SIP INFO conformément au RFC-2976.

L'onglet ci-dessous vous aide à définir comment les caractères DTMF doivent être reçus par l'interphone. Vérifiez les options de réception DTMF et les paramètres du destinataire de l'appel pour un fonctionnement optimal.



- **In-Band (Audio)** – activez la réception de la double tonalité DTMG classique dans la bande audio.
- **RTP (RFC-2833)** – activez la réception de DTMF via RTP conformément au RFC-2833.
- **SIP INFO (RFC-2976)** – activez la réception de DTMF via messages SIP INFO conformément au RFC-2976.

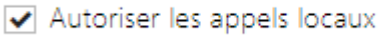


- **Valeur QoS DSCP** – paramétrez la priorité des paquets audio RTP sur le réseau. La valeur programmée est envoyée dans le champ TOS (Type of Service) de l'en-tête du paquet IP. La valeur est saisie sous forme de nombre décimal. Les valeurs de QoS recommandées pour la signalisation, l'audio et la vidéo sont indiquées dans le tableau ci-dessus.
- **Compensation de la gigue** – paramétrez la capacité tampon pour la compensation de gigue dans les transmissions de paquets audio. Une capacité supérieure améliore la résistance de transmission aux dépens d'une plus grande chambre d'écho.

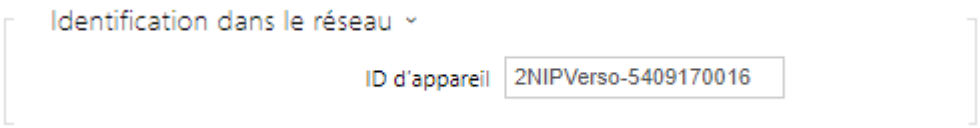
5.3.4 Appels locaux

Cet onglet contient les paramètres de connexion des Moniteurs de réception 2N à l'interphone. Le paramètre principal est la clé d'accès qui sécurise la connexion et vous permet de créer plusieurs groupes indépendants d'interphones et de Moniteurs 2N au sein du réseau local. Il contient également les paramètres de transmission vidéo.

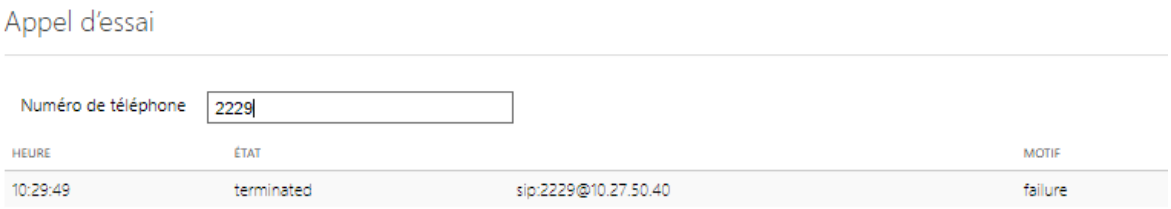
Configuration

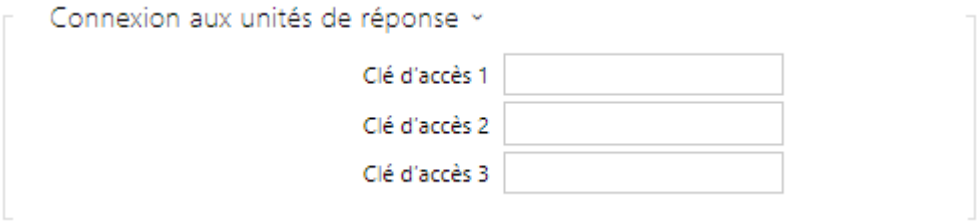


- **Autoriser les appels locaux** – activez les appels entre appareils 2N sur le réseau local. Lorsque cette fonction est désactivée, les autres appareils LAN ne peuvent pas localiser ces périphériques, c'est-à-dire ne peuvent pas appeler les Moniteurs sous le format :device_ID format.



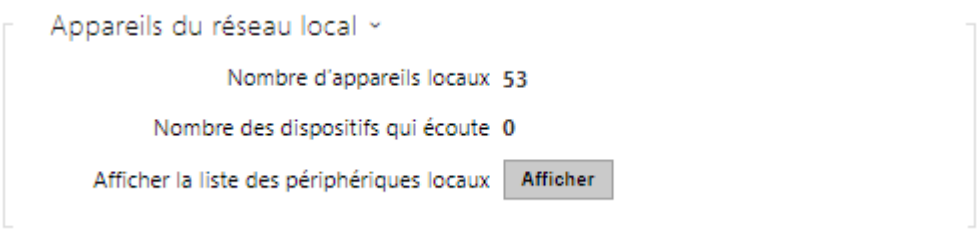
- **ID d'appareil** – configurez l'identification de l'appareil pour qu'elle apparaisse dans la liste des équipements locaux de tous les appareils 2N du même réseau local. En paramétrant le numéro de téléphone de l'utilisateur dans ces équipements avec la valeur **device:ID_de l'équipemen**t, il sera possible de rediriger l'appel vers ce moniteur.
- **Appel d'essai** – affiche une boîte de dialogue avec la possibilité d'effectuer un appel test au numéro de téléphone sélectionné, voir ci-dessous :



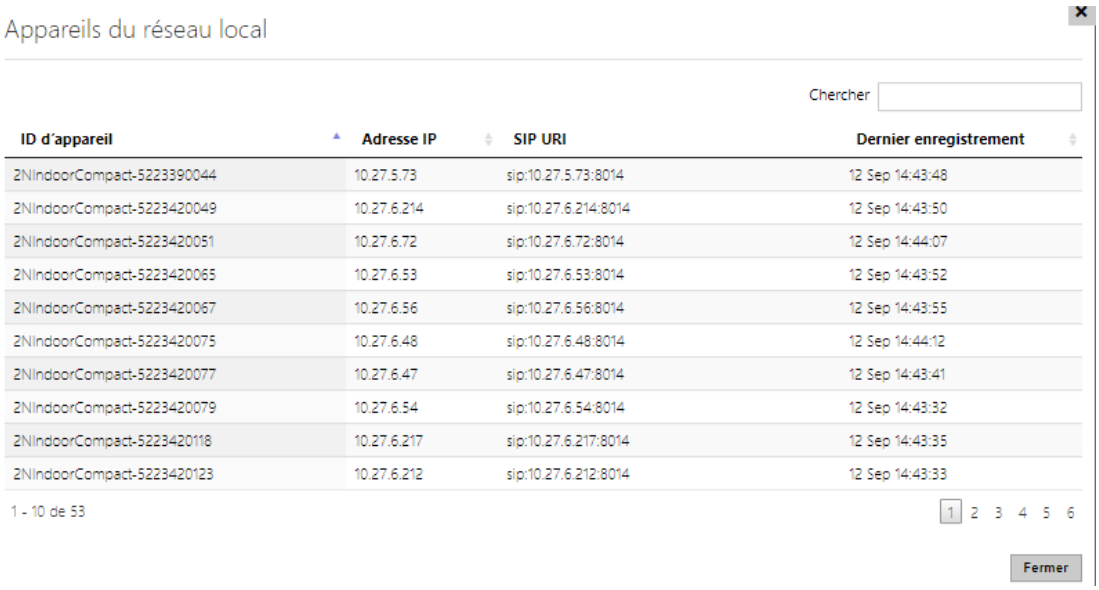


- **Clé d'accès 1–3** – définissez la clé d'accès à partager avec l'interphone et les Moniteurs 2N. Si les touches d'accès ne correspondent pas dans le Moniteur et dans l'Interphone 2N, celui-ci ne peut pas appeler le Moniteur et le Moniteur ne peut pas recevoir la vidéo de l'interphone. Vous pouvez affecter jusqu'à trois touches d'accès à chaque interphone et ainsi devenir membre de trois groupes de Moniteur 2N indépendants maximum. La longueur de la clé d'accès est limitée à 63 caractères.

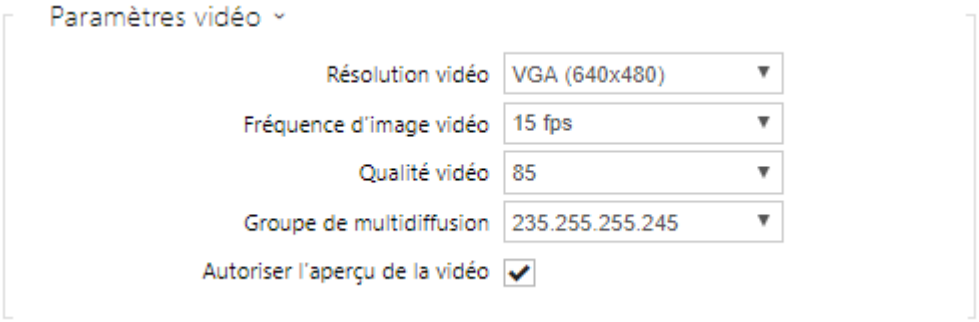
> **Note**
>
> La clé d'accès ne peut pas être utilisé avec les **2N® Indoor Touch** avec un firmware version 2 ou 3. Il doit être utiliser avec la version 4 ou supérieure.



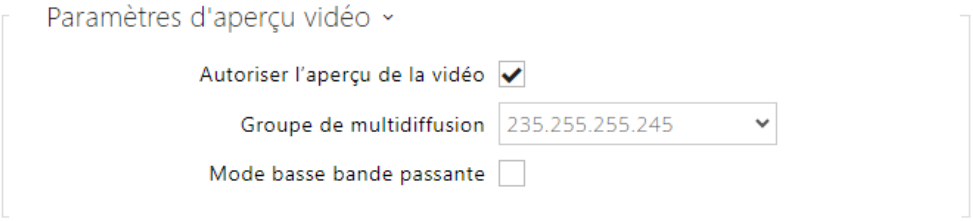
- **Nombre d'appareils locaux** – affiche le nombre actuel de Moniteur 2N locaux connectés à l'interphone, c'est-à-dire enregistrés avec l'interphone.
- **Nombre d'appareil ayant accès à la vidéo/audio** – affiche le nombre actuel de Moniteurs 2N visionnant les flux vidéo depuis l'interphone.
- **Afficher la liste des périphériques locaux**– accédez à la liste des Moniteurs 2N.



Video



- **Résolution vidéo** – réglez la définition de la vidéo diffusée vers les Moniteurs 2N.
- **Fréquence d'image vidéo** – réglez la fréquence d'image de la vidéo envoyée vers les Moniteurs 2N.
- **Qualité vidéo** – réglez la qualité du flux vidéo MJPEG envoyé vers les Moniteurs 2N.



- **Autoriser la prévisualisation de la vidéo** – autorise la diffusion de la prévisualisation vidéo en multicast sur les Moniteurs.
- **Groupe Multicast** – définissez l'adresse multicast sur laquelle le flux vidéo de l'interphone sera envoyé. Choisissez l'une des 8 adresses prédéfinies, ou choisissez le mode où l'interphone sélectionne l'adresse automatiquement.
- **Mode basse bande passante** – réduit la qualité du flux de prévisualisation vidéo pour économiser la bande passante.

- **PTZ** – activez la fonction PTZ (Pan-Tilt-Zoom) pour contrôler la zone d'affichage de la caméra pendant l'appel via DTMF (la licence **GOLD** sera nécessaire) depuis le clavier

numérique de votre téléphone IP. Cliquez sur la touche * pour activer / désactiver le mode PTZ. La signification des touches de téléphone IP en mode PTZ est la suivante :

Touche du Poste IP	Fonction du mode PTZ
*	Activer/Désactiver le PTZ
1	Zoomer
3	Dézoomer
2	Déplacer la zone de Zoom vers le haut
4	Déplacer la zone de Zoom vers la gauche
6	Déplacer la zone de Zoom vers la droite
8	Déplacer la zone de Zoom vers le bas
5	Retourner aux paramètres de base

- **Mode PTZ et Face Zooming** – permet d'activer la fonction PTZ (Pan-Tilt-Zoom) ou Face Zooming, qui vous permet d'ajuster la vue de la caméra affichée pendant un appel. Lorsque vous sélectionnez *Face Zooming* , la caméra fait un zoom sur le visage de l'utilisateur qui se tient près de l'appareil. Lorsque vous sélectionnez *Face Zooming – inclinaison uniquement*, la découpe de l'image de la caméra n'est décalée que pour prendre le visage.

> **Observation**
>
> - La fonction Face Zooming est disponible uniquement sur les modèles équipés du processeur ARTPEC-7 de la société Axis.

- **Autoriser la vidéo entrante** – si ce mode est activé, l'interphone affichera pendant l'appel la vidéo de l'autre partie, si celle-ci en donne l'autorisation.
- **Rapport de forme de la video entrante** – définit le format d'image préféré de la vidéo entrante affichée sur l'écran. Lorsqu'un format d'image différent de l'original est sélectionné, la vidéo est recadrée de manière à remplir la largeur de l'écran dans le nouveau format d'image.

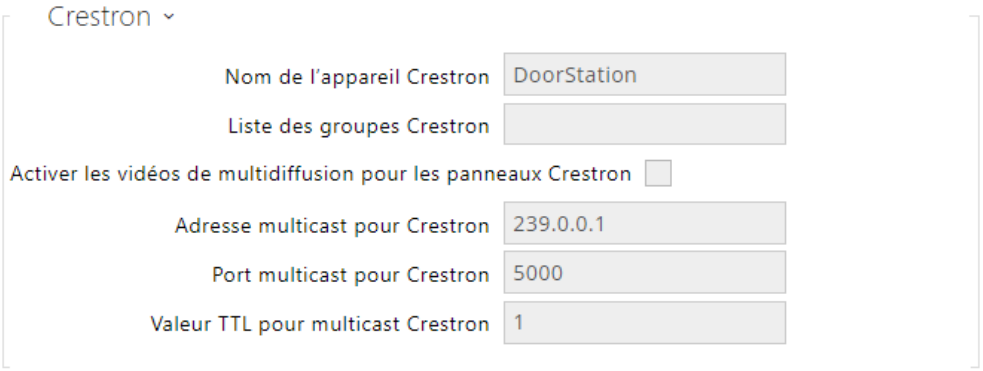
- **Afficher la vidéo sortante** – choisit si l'interphone affiche un aperçu de la vidéo envoyée lors de l'appel.

Audio

- **Compensation de la gigue** – paramétrez la capacité tampon pour la compensation de gigue dans les transmissions de paquets audio. Une capacité supérieure améliore la résistance de transmission aux dépens d'une plus grande chambre d'écho.

5.3.5 Crestron

- **Autoriser Crestron Network Discovery** – activez l'identification de l'interphone IP 2N au sein du réseau Crestron.



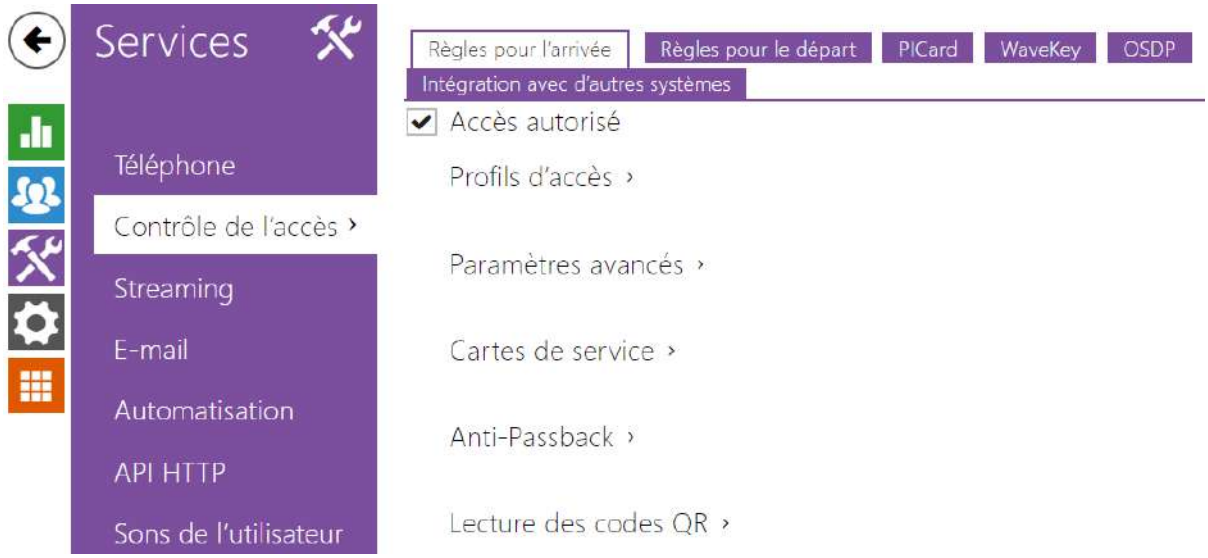
- **Nom de l'appareil Crestron** – nom de l'appareil.
- **Liste des groupes Crestron** – sélectionnez la liste des groupes Crestron avec une virgule entre chaque.
- **Activer la vidéo en multicast pour les appareils Crestron** – permet à plusieurs appareils Crestron de recevoir la même vidéo et d'économiser ainsi la capacité de transmission du réseau local.
- **Adresse multicast pour Crestron** – adresse de multidiffusion à utiliser pour la vidéo en multicast avec des appareils Crestron.
- **Port multicast pour Crestron** – port multicast qui sera utilisé pour la vidéo avec les appareils Crestron.
- **Valeur TTL pour le multicast Crestron** – valeur TTL (Time To Live) qui sera utilisée pour diffuser la vidéo en mode Early media pour les appareils Crestron.

5.4 Services

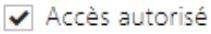
Voici les différents onglets que vous pourrez trouver dans cette section :

5.4.1 Contrôle de l’accès

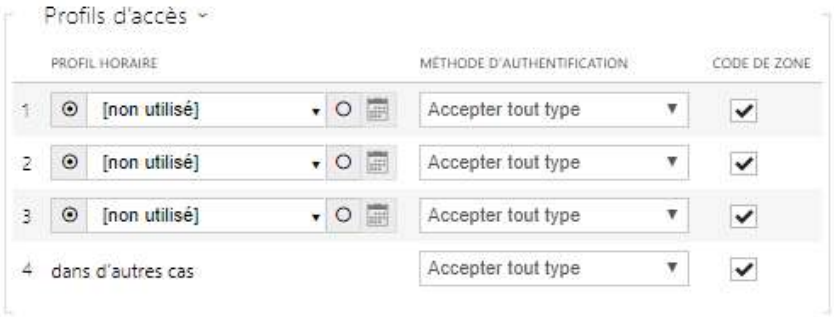
Le service Contrôle d’accès sert à gérer les accès et la façon dont l’authentification des utilisateurs est vérifiée.



Règles pour l’arrivée



- **Accès autorisé** – il permet n’importe quel accès d'un côté particulier de la porte (arrivée, départ). Si l’accès n’est pas autorisé, la porte ne peut pas être ouverte de ce côté.

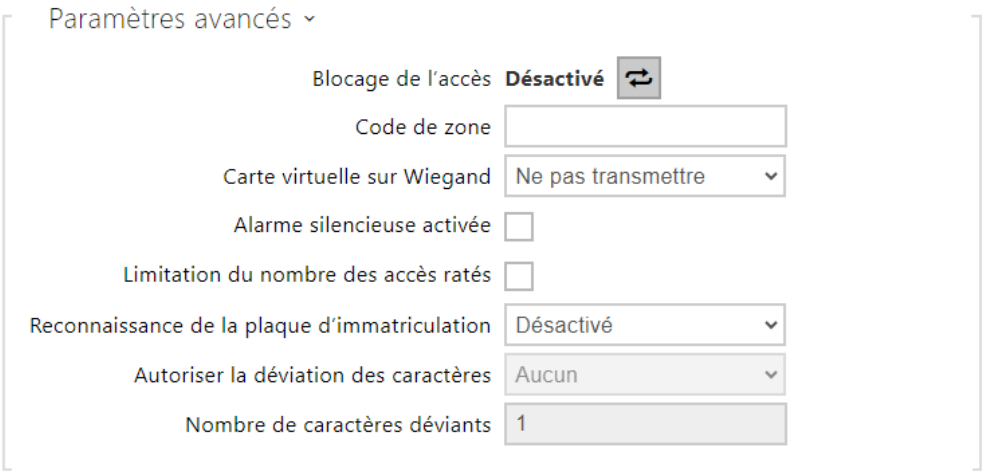


- **Profil horaire** – choisissez un ou plusieurs profils horaires à appliquer. Définissez les profils horaires dans la section **Répertoire / Profils horaires**.
  -  sélectionnez l'un des profils prédéfinis ou définissez manuellement le profil temporel pour un élément donné.
- **Méthode d’authentification** – il définit la méthode d’authentification pour la plage horaire renseignée à cette ligne, y compris la possibilité d’authentification multiple pour

une sécurité renforcée. En choisissant l'option "Accès refusé" on peut complètement interdire l'accès.
- **Code de zone** – il autorise un code de zone pour combiner le profil temporel et la méthode d'authentification pour cette ligne. Le code de zone peut alors être utilisé à la place du code PIN de l'utilisateur.

Observation

- Si le profil horaire n'est pas défini, le mode d'authentification est ignoré sur la ligne donnée.



- **Blocage de l'accès** – affiche le statut du blocage de l'accès : Activé / Désactivé. Utilisable de le cas de scénario d'évacuation ou de confinement.
- **Code de zone** – il vous permet d'entrer un code de zone numérique à l'interrupteur. Le code doit contenir au moins deux caractères, mais nous vous recommandons d'utiliser au moins quatre caractères.
- **Carte virtuelle sur Wiegand** – elle permet de choisir la sortie Wiegand à laquelle le numéro de carte virtuelle de l'utilisateur sera envoyé après son authentification réussie. On peut l'utiliser avec n'importe quelle authentification, y compris les codes, les empreintes digitales...Etc.
- **Alarme silencieuse activée** – pour chaque code d'accès, nous attribuons un code virtuel dont le numéro augmente d'une unité par rapport au numéro du code d'accès de l'utilisateur. Ce code est destiné à activer une alarme silencieuse en cas d'ouverture de porte sous la contrainte. Par exemple, si le code d'accès est 0000, le code pour activer l'alarme silencieuse est 0001. La longueur du code doit rester la même. Cela veut dire que par exemple pour le code d'accès 9999, l'alarme silencieuse est 0000 etc. L'action effectuée en cas d'activation de l'alarme silencieuse peut être réglée dans la section **Services / Automatisation**.

Observation

- Si l'alarme silencieuse n'est pas activé, l'utilisateur qui rentre le second code ne déclenchera pas l'alarme mais l'accès lui sera refusé.

- **Limite du nombre de tentative d'accès invalide** – il permet de limiter le nombre de tentatives d'authentification invalide. Après cinq tentatives d'accès invalide (code numérique incorrect, carte invalide, etc.), le module d'accès sera bloqué pendant trente secondes même si l'authentification est valide par la suite.
- **Reconnaissance de la plaque d'immatriculation** – sélectionne le scénario après reconnaissance de la plaque d'immatriculation du véhicule.

Observation

- Pour un fonctionnement adéquat, il est conseillé que chaque plaque d'immatriculation soit affectée à une seule entrée dans le répertoire. En cas de plaques d'immatriculation multiples, il n'est pas possible d'attribuer catégoriquement une entrée dans le répertoire qui a la plaque d'immatriculation configurée (la première entrée correspondant à la plaque d'immatriculation donnée configurée est sélectionnée et ses règles d'accès sont mises en œuvre).

  - **Desactivé**
  - **Ouverture du signe** – La porte sera ouverte si la plaque d'immatriculation enregistrée dans l'annuaire correspond à un droit réel d'entrée ou de sortie. L'ouverture d'une porte (ou d'une barrière, etc.) après la détection d'une plaque d'immatriculation valide **fonctionne indépendamment** des autres méthodes d'authentification paramétrées dans les Profils d'accès.
  - **Multifacteur avec la plaque** – cette option n'est disponible que lorsque la fonction bêta Authentification multifactorielle des plaques d'immatriculation est activée. Active le blocage permanent de l'accès et désactive définitivement la méthode d'authentification à l'aide de Bluetooth (WaveKey). Une fois la plaque d'immatriculation chargée, une exception temporaire de 60 secondes sera accordée à l'utilisateur avec la plaque d'immatriculation chargée, et la fonction WaveKey sera activée pour cette période. L'accès ne sera accordé qu'à l'utilisateur dont la plaque d'immatriculation est chargée et qui s'authentifie avec une autre méthode d'authentification (code WaveKey/QR) dans un délai de 60 secondes. Les utilisateurs bénéficiant d'une exception permanente sont autorisés à accéder pendant toute la durée du blocage de l'accès permanent, mais seulement dans les 60 secondes suivant l'enregistrement de la plaque d'immatriculation, ils peuvent également s'authentifier à l'aide de WaveKey.
    Chaque plaque d'immatriculation supplémentaire acceptée annule l'exception temporaire précédente et si un utilisateur possède une plaque d'immatriculation nouvellement acceptée, une exception temporaire est attribuée à cet utilisateur.

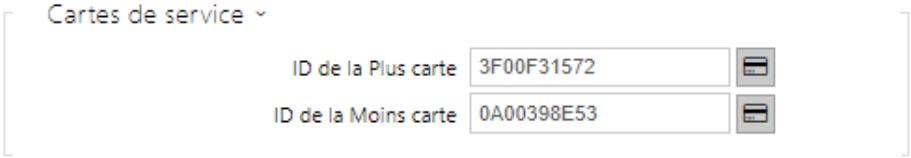
- **Tolérer un écart de caractères** – permet de déterminer si un écart est toléré dans la plaque d'immatriculation du véhicule. Il est possible de choisir entre une tolérance zéro, une tolérance depuis le début, une tolérance depuis la fin ou une tolérance tant depuis le début que depuis la fin. Lors de la sélection de la tolérance des caractères des deux côtés, un écart de caractères depuis le début est d'abord toléré lors de la lecture de la plaque d'immatriculation et, si la plaque n'est pas reconnue, un écart depuis la fin est toléré lors de la lecture suivante.
- **Nombre d'écarts de caractères** - permet de déterminer si un écart d'un ou deux caractères est toléré. L'écart des caractères se réfère au début et/ou à la fin en fonction du paramètre **Tolérer un écart de caractères**. L'appareil ne tolère aucun écart lors de la première lecture de la plaque d'immatriculation. Ce n'est que s'il ne reconnaît pas la plaque d'immatriculation enregistrée dans le répertoire qu'il tolérera un écart d'un caractère dans les directions définies ci-dessus lors de la lecture suivante. Si même ainsi l'appareil n'identifie pas la plaque d'immatriculation dans le répertoire, il tolérera un écart de deux caractères lors de la lecture suivante.

L'appareil permet d'utiliser les plaques d'immatriculation des véhicules reconnues envoyées dans la requête HTTP par les caméras de la société AXIS équipées de l'application complémentaire VaxALPR sur api/lpr/licenseplate (voir le manuel de l'API HTTP pour les interphones IP)

Si la fonction est activée, une fois réceptionnée une requête HTTP valide, l'événement sera enregistré dans l'historique sous l'événement LicensePlateRecognized. L'image envoyée dans le cadre d'une requête HTTP (par ex. une partie de la photo ou la photo entière de la scène lors de la détection de la plaque d'immatriculation) sera enregistrée. Les cinq dernières photos sont stockées dans la mémoire de l'équipement, qui peut être lue à partir de l'équipement à l'aide d'une requête HTTP envoyée à api/lpr/image et sont disponibles dans le système **2N Access Commander**.

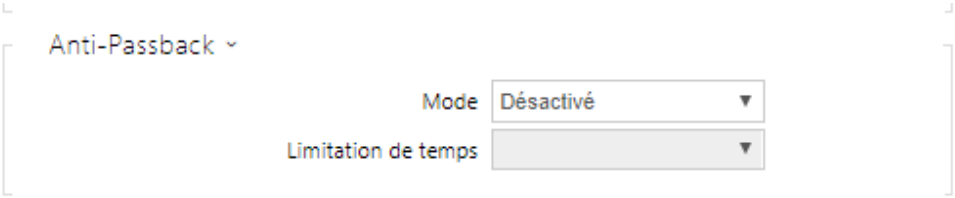
Avertissement

- La réinitialisation du logiciel d'usine ou le téléchargement d'une configuration différente ne modifiera pas les paramètres de blocage d'accès. Seule une réinitialisation matérielle des paramètres d'usine à l'aide du bouton Reset de l'appareil permet de rétablir les paramètres par défaut.
  - Le relais de sécurité augmente la sécurité de l'installation contre les abus grâce à une réinitialisation matérielle.



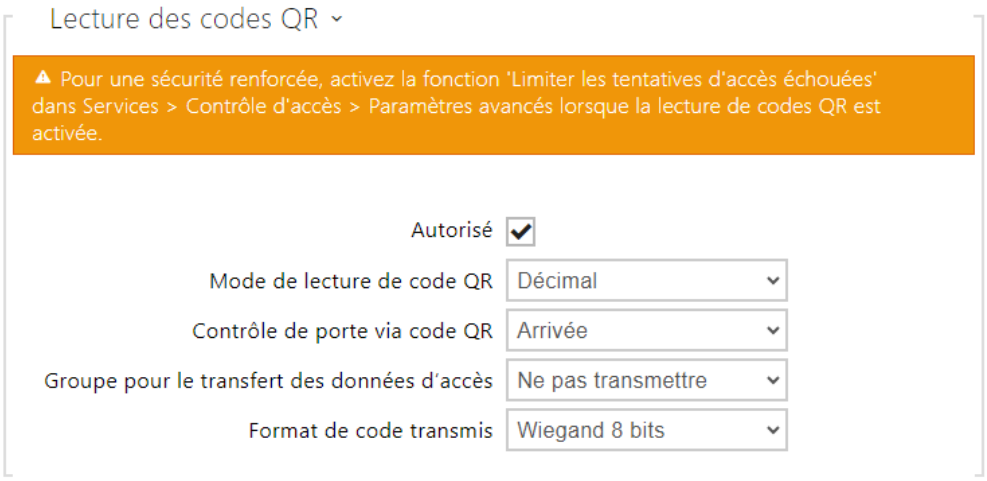
Les cartes plus / moins sont utilisées pour l'administration des cartes utilisateurs. Lorsqu'une carte plus est badgée sur le lecteur de carte, toute autre carte badgée est ajoutée au Répertoire en tant que nouvel utilisateur auquel une carte d'accès a été attribuée. L'utilisateur ! Visiteur #carte_ID est automatiquement créé dans l'appareil. Lorsqu'une carte moins est badgée sur le lecteur de carte, toute autre carte badgée et son utilisateur seront supprimées du Répertoire.

- **ID de la Plus carte** – ID de la carte de service destinée à ajouter dans la liste des cartes utilisateurs. L'ID de la carte est une séquence de 6–32 caractères de l'ensemble 0–9, A–F.
- **ID de la Moins carte** – ID de la carte de service destinée à enlever de la liste des cartes utilisateurs. L'ID de la carte est une séquence de 6–32 caractères de l'ensemble 0–9, A–F.



L'Anti-Passback est une fonctionnalité de sécurité qui empêche les utilisateurs d'utiliser leurs cartes d'accès ou d'autres identifiants pour entrer de nouveau dans une zone sans l'avoir quitté (par exemple, pour empêcher les utilisateurs de partager des cartes).

- **Mode** – activez / désactivez le mode Anti-Passback :
  - **Désactivé** – la fonctionnalité est désactivée par défaut, ce qui permet à l'utilisateur d'utiliser la carte d'accès ou un autre identifiant pour entrer de nouveau dans une zone sans la quitter.
  - **Modéré** – l'utilisateur est autorisé à utiliser la carte d'accès ou un autre identifiant pour entrer de nouveau dans une zone sans la quitter. Un nouvel enregistrement de type UserAuthenticated sera créé dans la section **UserAuthenticated** avec le paramètre *apbBroken*=***true***.
  - **Strict** – l'utilisateur n'est pas autorisé à utiliser la carte d'accès ou un autre identifiant pour entrer de nouveau dans une zone sans la quitter au préalable. Un nouvel enregistrement de type UserAuthenticated sera créé dans la section **UserRejected** avec le paramètre *apbBroken*=***true***.
- **Limite de temps** – sélectionnez un délai d'anti-passback pendant lequel l'utilisateur ne peut pas entrer à nouveau dans une zone en utilisant la méthode d'authentification donnée (carte, code, etc.) dans le même sens.

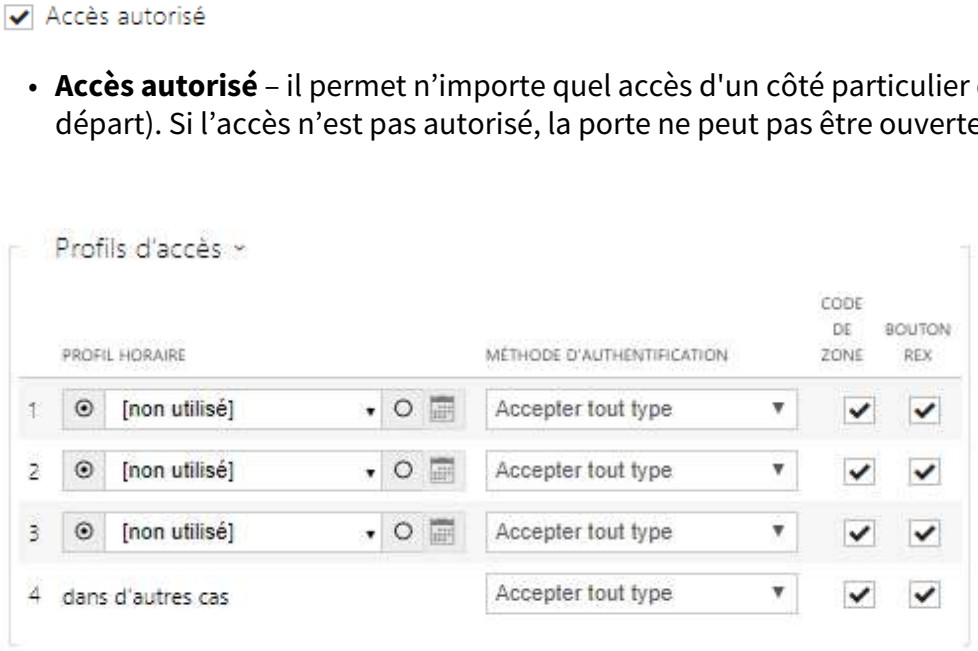


- **Autorisé** – active/désactive la lecture des codes QR à l'aide de la caméra du dispositif. Si la lecture des codes QR est activée, les codes PIN et les codes individuels des interrupteurs de plus de dix chiffres peuvent être saisis en pointant le code QR vers la caméra du dispositif.
- **Mode de lecture de code QR** – Le dispositif stocke toujours des codes décimaux. En mode décimal, les codes scannés doivent correspondre aux codes de 4 à 15 chiffres stockés dans le dispositif. En mode hexadécimal, les codes sont convertis en décimal après la numérisation et comparés aux codes décimaux stockés, en ignorant les zéros initiaux. Plage hexadécimale acceptée : de 1000 à FFFFFFFF.
- **Commandes des portes par code QR** – Autorise ou interdit la commande des portes en lisant le code QR.
- **Groupe pour le transfert des données d'accès** - vous permet de définir un groupe auquel tous les codes d'accès utilisateur reçus seront transférés.
- **Format de code transmis** – sélectionnez un format 4 bits ou 8 bits (sécurité supérieure) pour les codes à transmettre.

Observation

- Pour que la lecture des codes QR fonctionne bien, n'utilisez pas la fonction de confidentialité en même temps.
- Pour plus de sécurité, limitez le nombre de tentatives d'accès ratées dans le bloc Paramètres avancés ci-dessus.
- La fonction de lecture de codes QR est disponible uniquement sur les modèles équipés du processeur ARTPEC-7 de la société Axis.

Règles pour le départ

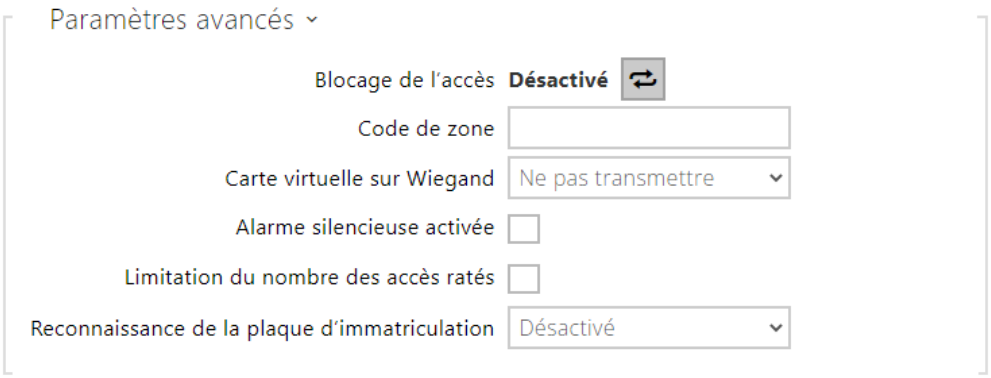


- **Accès autorisé** – il permet n'importe quel accès d'un côté particulier de la porte (arrivée, départ). Si l'accès n'est pas autorisé, la porte ne peut pas être ouverte de ce côté.

- **Profil horaire** – choisissez un ou plusieurs profils horaires à appliquer. Définissez les profils horaires dans la section **répertoire / profils horaires**.
  - sélectionnez l'un des profils prédéfinis ou définir manuellement le profil temporel pour un élément donné.
- **Méthode d'authentification** – il définit la méthode d'authentification pour la plage horaire définie à cette ligne, y compris la possibilité d'authentification multiple pour une sécurité renforcée. En choisissant l'option "Accès refusé" on peut complètement interdire l'accès.
- **Code de zone** – il autorise un code de zone pour combiner le profil temporel et la méthode d'authentification pour cette ligne. Le code de zone peut alors être utilisé à la place du code PIN de l'utilisateur.
- **Bouton de sortie (REX)** – activez la fonction du bouton de sortie pour le profil horaire sélectionné. Définissez l'entrée du bouton de sortie dans la section **Hardware / Porte**.

Observation

- Si le profil horaire n'est pas défini, le mode d'authentification est ignoré sur la ligne donnée.



- **Blocage de l'accès** – affiche le statut du blocage de l'accès : Activé / Désactivé. Utilisable de le cas de scénario d'évacuation ou de confinement.
- **Code de zone** – il vous permet d'entrer le code de zone numérique de l'interrupteur. Le code doit contenir au moins deux caractères, mais nous vous recommandons d'utiliser au moins quatre caractères.
- **Carte virtuelle sur Wiegand** – elle permet de choisir la sortie Wiegand à laquelle le numéro de carte virtuelle de l'utilisateur sera envoyé après son authentification réussie. On peut l'utiliser avec n'importe quelle authentification, y compris les codes, les empreintes digitales…Etc.
- **Alarme silencieuse activée** – pour chaque code d'accès, nous attribuons un code virtuel dont le numéro augmente d'une unité par rapport au numéro du code d'accès de l'utilisateur. Ce code est destiné à activer une alarme silencieuse en cas d'ouverture de porte sous la contrainte. Par exemple, si le code d'accès est 0000, le code pour activer l'alarme silencieuse est 0001. La longueur du code doit rester la même. Cela veut dire que

par exemple pour le code d'accès 9999, l'alarme silencieuse est 0000 etc. L'action effectuée en cas d'activation de l'alarme silencieuse peut être réglée dans la section **Services / Automatisation**.

Observation

- Si l'alarme silencieuse n'est pas activé, l'utilisateur qui rentre le second code ne déclenchera pas l'alarme mais l'accès lui sera refusé.

- **Limite du nombre de tentative d'accès invalide** – il permet de limiter le nombre de tentatives d'authentification invalide. Après cinq tentatives d'accès invalide (code numérique incorrect, carte invalide, etc.), le module d'accès sera bloqué pendant trente secondes même si l'authentification est valide par la suite.
- **Reconnaissance de la plaque d'immatriculation** – sélectionne le scénario après reconnaissance de la plaque d'immatriculation du véhicule.

Observation

- Pour un fonctionnement adéquat, il est conseillé que chaque plaque d'immatriculation soit affectée à une seule entrée dans le répertoire. En cas de plaques d'immatriculation multiples, il n'est pas possible d'attribuer catégoriquement une entrée dans le répertoire qui a la plaque d'immatriculation configurée (la première entrée correspondant à la plaque d'immatriculation donnée configurée est sélectionnée et ses règles d'accès sont mises en œuvre).

  - **Desactivé**
  - **Ouverture du signe** – La porte sera ouverte si la plaque d'immatriculation enregistrée dans l'annuaire correspond à un droit réel d'entrée ou de sortie. L'ouverture d'une porte (ou d'une barrière, etc.) après la détection d'une plaque d'immatriculation valide **fonctionne indépendamment** des autres méthodes d'authentification paramétrées dans les Profils d'accès.
  - **Multifacteur avec la plaque** – cette option n'est disponible que lorsque la fonction bêta Authentification multifactorielle des plaques d'immatriculation est activée. Active le blocage permanent de l'accès et désactive définitivement la méthode d'authentification à l'aide de Bluetooth (WaveKey). Une fois la plaque d'immatriculation chargée, une exception temporaire de 60 secondes sera accordée à l'utilisateur avec la plaque d'immatriculation chargée, et la fonction WaveKey sera activée pour cette période. L'accès ne sera accordé qu'à l'utilisateur dont la plaque d'immatriculation est chargée et qui s'authentifie avec une autre méthode d'authentification (code WaveKey/QR) dans un délai de 60 secondes. Les utilisateurs bénéficiant d'une exception permanente sont autorisés à accéder pendant toute la durée du blocage de l'accès permanent, mais seulement dans les 60 secondes suivant l'enregistrement de la plaque d'immatriculation, ils peuvent également s'authentifier à l'aide de WaveKey.

Chaque plaque d'immatriculation supplémentaire acceptée annule l'exception temporaire précédente et si un utilisateur possède une plaque d'immatriculation nouvellement acceptée, une exception temporaire est attribuée à cet utilisateur.

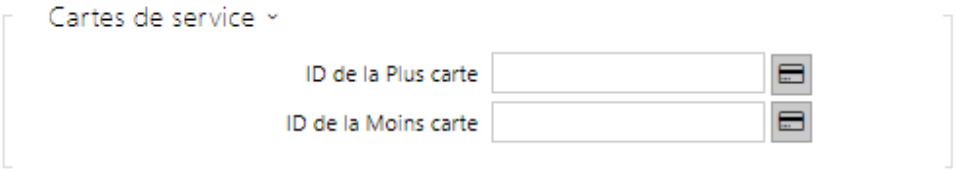
- **Tolérer un écart de caractères** – permet de déterminer si un écart est toléré dans la plaque d'immatriculation du véhicule. Il est possible de choisir entre une tolérance zéro, une tolérance depuis le début, une tolérance depuis la fin ou une tolérance tant depuis le début que depuis la fin. Lors de la sélection de la tolérance des caractères des deux côtés, un écart de caractères depuis le début est d'abord toléré lors de la lecture de la plaque d'immatriculation et, si la plaque n'est pas reconnue, un écart depuis la fin est toléré lors de la lecture suivante.
- **Nombre d'écarts de caractères** - permet de déterminer si un écart d'un ou deux caractères est toléré. L'écart des caractères se réfère au début et/ou à la fin en fonction du paramètre **Tolérer un écart de caractères**. L'appareil ne tolère aucun écart lors de la première lecture de la plaque d'immatriculation. Ce n'est que s'il ne reconnaît pas la plaque d'immatriculation enregistrée dans le répertoire qu'il tolérera un écart d'un caractère dans les directions définies ci-dessus lors de la lecture suivante. Si même ainsi l'appareil n'identifie pas la plaque d'immatriculation dans le répertoire, il tolérera un écart de deux caractères lors de la lecture suivante.

L'appareil permet d'utiliser les plaques d'immatriculation des véhicules reconnues envoyées dans la requête HTTP par les caméras de la société AXIS équipées de l'application complémentaire VaxALPR sur api/lpr/licenseplate (voir le manuel de l'API HTTP pour les interphones IP)

Si la fonction est activée, une fois réceptionnée une requête HTTP valide, l'événement sera enregistré dans l'historique sous l'événement LicensePlateRecognized. L'image envoyée dans le cadre d'une requête HTTP (par ex. une partie de la photo ou la photo entière de la scène lors de la détection de la plaque d'immatriculation) sera enregistrée. Les cinq dernières photos sont stockées dans la mémoire de l'équipement, qui peut être lue à partir de l'équipement à l'aide d'une requête HTTP envoyée à api/lpr/image et sont disponibles dans le système **2N Access Commander**.

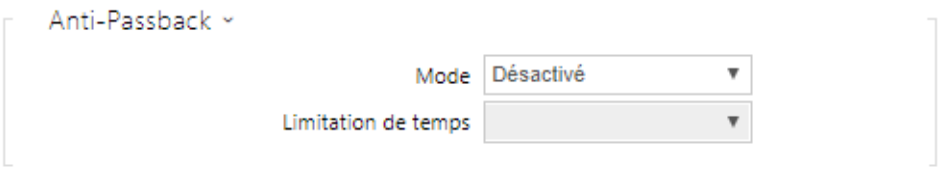
Avertissement

- La réinitialisation du logiciel d'usine ou le téléchargement d'une configuration différente ne modifiera pas les paramètres de blocage d'accès. Seule une réinitialisation matérielle des paramètres d'usine à l'aide du bouton Reset de l'appareil permet de rétablir les paramètres par défaut.
  - Le relais de sécurité augmente la sécurité de l'installation contre les abus grâce à une réinitialisation matérielle.



Les cartes plus / moins sont utilisées pour l'administration des cartes utilisateurs. Lorsqu'une carte plus est badgée sur le lecteur de carte, toute autre carte badgée est ajoutée au Répertoire en tant que nouvel utilisateur auquel une carte d'accès a été attribuée. L'utilisateur! Visiteur #carte_ID est automatiquement créé dans l'appareil. Lorsqu'une carte moins est badgée sur le lecteur de carte, toute autre carte badgée et son utilisateur seront supprimées du Répertoire.

- **ID de la Plus carte** – ID de la carte de service destiné à ajouter dans la liste des cartes utilisateurs. L'ID de la carte est une séquence de 6–32 caractères de l'ensemble 0–9, A–F.
- **ID de la Moins carte** – ID de la carte de service destiné à enlever de la liste des cartes utilisateurs. L'ID de la carte est une séquence de 6–32 caractères de l'ensemble 0–9, A–F.



L'Anti-Passback est une fonctionnalité de sécurité qui empêche les utilisateurs d'utiliser leurs cartes d'accès ou d'autres identifiants pour entrer de nouveau dans une zone sans l'avoir quitté (par exemple, pour empêcher les utilisateurs de partager des cartes).

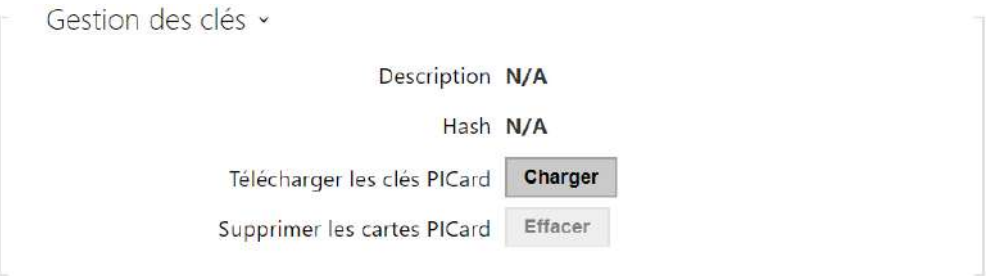
- **Mode** – activer / désactiver le mode Anti-Passback :
  - **Désactivé** – la fonctionnalité est désactivée par défaut, ce qui permet à l'utilisateur d'utiliser la carte d'accès ou un autre identifiant pour entrer de nouveau dans une zone sans la quitter.
  - **Modéré** – l'utilisateur est autorisé à utiliser la carte d'accès ou un autre identifiant pour entrer de nouveau dans une zone sans la quitter. Un nouvel enregistrement de type UserAuthenticated sera créé dans la section **UserAuthenticated** avec le paramètre *apbBroken*=***true***.
  - **Strict** – l'utilisateur n'est pas autorisé à utiliser la carte d'accès ou un autre identifiant pour entrer de nouveau dans une zone sans la quitter au préalable. Un nouvel enregistrement de type UserAuthenticated sera créé dans la section **UserRejected** avec le paramètre *apbBroken*=***true***.
- **Limite de temps** – sélectionnez un délai d'anti-passback pendant lequel l'utilisateur ne peut pas entrer à nouveau dans une zone en utilisant la méthode d'authentification donnée (carte, code, etc.) dans le même sens.

PICard

La technologie 2N PICardpermet de crypter les données de connexion sur les cartes d'accès. Pour lire les données de connexion, les dispositifs 2N doivent avoir accès aux clés correspondantes générées par l'application 2N PICard Commander. Celles-ci peuvent ensuite être importées dans 2N Access Commanderu, qui assure la distribution à tous les dispositifs 2N pris en charge.

Observation

- Les appareils sur lesquels les cartes dotées de la technologie PICard chargée peuvent être lues sont énumérés dans le manuel de configuration de 2N PICard Commander.



- **Description** – nom pour la clé de cryptage qui a été créée.
- **Hash** – identificateur numérique du projet.
- **Télécharger les clés PICard** – en sélectionnant un fichier clé et en saisissant un mot de passe valide, la clé PICard sera téléchargée.
- **Supprimer les cartes PICard** – supprime les clés PICard téléchargées

WaveKey

Les **interphones IP 2N** équipés du module Bluetooth permettent l'authentification des utilisateurs via l'application **2N Mobile Key** disponible sur les appareils iOS 12 ou version ultérieure (iPhone 4s ou version ultérieure) ou Android 6.0 Marshmallow ou version ultérieure (téléphones compatibles Bluetooth 4.0 Smart).

Identifiant de l'utilisateur (ID d'authentification)

L'application **2N Mobile Key** s'authentifie avec un identifiant unique du côté de l'interphone : L'**ID d'Authentification** (nombre de 128 bits) est générée aléatoirement pour chaque utilisateur et associée à l'utilisateur de l'interphone et à son appareil mobile.

Note

- L'ID d'authentification généré ne peut pas être enregistré dans plus d'un appareil mobile. Cela signifie que l'ID d'authentification identifie de manière unique un seul appareil mobile et son utilisateur.

Vous pouvez définir et modifier la valeur de l'ID d'authentification pour chaque utilisateur dans la section Clé mobile du répertoire de l'interphone. Vous pouvez déplacer l'ID d'authentification vers un autre utilisateur ou le copier dans un autre interphone. En supprimant la valeur de l'ID d'authentification, vous pouvez bloquer l'accès de l'utilisateur.

Clé crypté pour la localisation

2N Mobile Key – communique toujours avec l'Interphone de manière cryptée. **2N Mobile Key** ne peut pas authentifier un utilisateur sans connaître la clé de chiffrement. La clé de chiffrement principale est automatiquement générée lors du premier lancement de l'interphone et peut être générée manuellement à tout moment. Avec l'ID d'authentification, la clé de chiffrement principale est transmise au périphérique mobile pour le jumelage.

Vous pouvez exporter / importer les clés de cryptage et l'identifiant d'emplacement vers d'autres interphones. Les interphones avec des noms d'emplacement et des clés de cryptage identiques forment ce que l'on appelle des emplacements. Dans un emplacement, un appareil mobile est couplé une seule fois et s'identifie avec un identifiant d'authentification unique (c'est-à-dire qu'un identifiant d'authentification d'utilisateur peut être copié d'un interphone à un autre dans un emplacement).

Jumelage

Le jumelage signifie la transmission de données d'accès utilisateur à un appareil mobile personnel de l'utilisateur. Les données d'accès utilisateur ne peuvent être enregistrées que sur un seul appareil mobile, c'est-à-dire qu'un utilisateur ne peut pas avoir deux appareils mobiles pour s'authentifier, par exemple. Toutefois, les données d'accès des utilisateurs peuvent être sauvegardées dans plusieurs emplacements d'un même appareil mobile (c'est-à-dire que l'appareil mobile sert de clé pour plusieurs emplacements simultanément).

Pour associer un utilisateur à un appareil mobile, utilisez la page de cet utilisateur dans le répertoire de l'interphone. Physiquement, vous pouvez associer un utilisateur localement à l'aide du module Bluetooth USB connecté à votre PC ou à distance à l'aide d'un module Bluetooth intégré dans l'interphone. Le résultat des deux méthodes de jumelage est le même.

Les données suivantes sont transmises à un appareil mobile pour le jumelage :

- Identifiant d'emplacement
- Clé crypté de l'emplacement
- Identification d'authentification de l'utilisateur

Clé de chiffrement pour le jumelage

Une clé de chiffrement autre que celle utilisée pour la communication après le jumelage est utilisée en mode jumelage pour des raisons de sécurité. Cette clé est générée automatiquement au premier lancement de l'interphone et peut être générée à tout moment par la suite.

Administration de la clé cryptée

L'interphone peut conserver jusqu'à 4 clés de chiffrement valides : 1 primaire et 3 secondaires. Un appareil mobile peut utiliser l'une des 4 clés pour le cryptage de la communication. Les clés de chiffrement sont entièrement contrôlées par l'administrateur du système. Il est recommandé que les clés de cryptage soient régulièrement mises à jour pour des raisons de sécurité, en particulier en cas de perte d'un appareil mobile ou de fuite de la configuration de l'interphone.

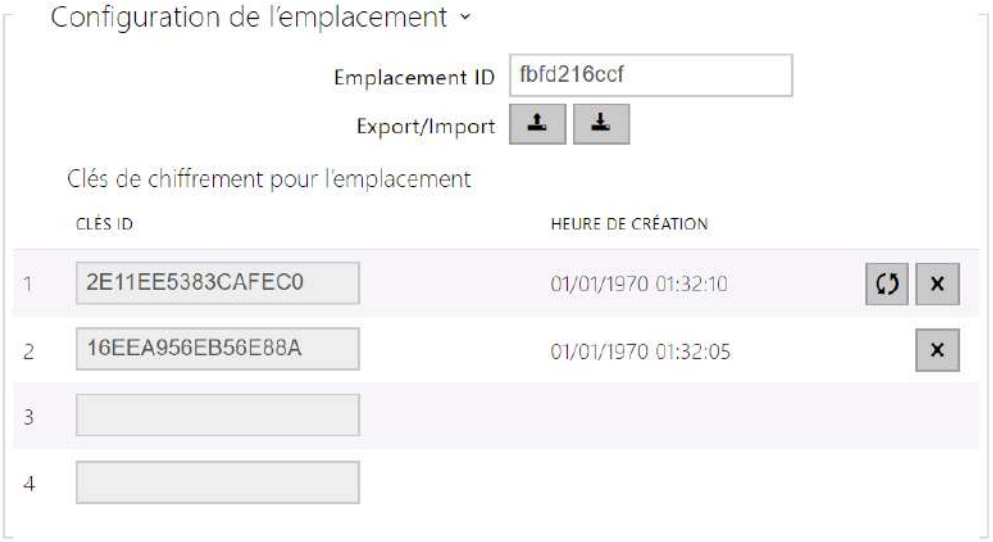
Note

- Les clés de chiffrement sont générées automatiquement au premier lancement de l'interphone et sauvegardées dans le fichier de configuration de l'interphone. Nous vous recommandons de générer à nouveau les clés de chiffrement manuellement avant la première utilisation pour renforcer la sécurité.

La clé primaire peut être générée à tout moment. Ainsi, la clé primaire d'origine devient la première clé secondaire, la première clé secondaire devient la deuxième clé secondaire et ainsi de suite. Les clés secondaires peuvent être supprimées à tout moment.

Lorsqu'une clé est supprimée, les utilisateurs de l'application **2N Mobile Key** qui utilisent toujours cette clé ne pourront pas s’authentifier à moins d’avoir mis à jour les clés de chiffrement de leurs appareils mobiles avant leur suppression. Les clés de l'appareil mobile sont mises à jour à chaque utilisation de l'application **2N Mobile Key**.

Liste des paramètres



- **Emplacement ID** – identificateur incontestable de l'emplacement, dans lequel prévaut le set de clés de chiffrement réglées.
- **Export** – appuyez sur ce bouton pour exporter l'ID d'emplacement et les clés de chiffrement actuelles dans un fichier. Par la suite, le fichier exporté peut être importé sur un autre appareil.
- **Import** – appuyez sur ce bouton pour importer l'ID d'emplacement et les clés de chiffrement actuelles à partir d'un fichier exporté depuis un autre interphone.
- **Restaurer la clé primaire** – en générant une nouvelle clé de cryptage principale vous supprimez la plus ancienne clé secondaire. Ainsi, l'utilisateur de l'application **2N Mobile Key** qui utilisent toujours cette clé ne pourront pas s'authentifier à moins d'avoir mis à jour les clés de chiffrement de leurs appareils mobiles avant leur suppression. Les clés de l'appareil mobile sont mises à jour à chaque utilisation de l'application **2N Mobile Key**.
- **Effacer la clé primaire** – efface la clé primaire pour empêcher l'authentification des utilisateurs qui utilisent encore cette clé.
- **Effacer la clé secondaire** – les utilisateurs de **2N Mobile Key** qui utilisent toujours cette clé ne pourront pas s'authentifier à moins d'avoir mis à jour les clés de chiffrement de leurs appareils mobiles avant leur suppression. Les clés de l'appareil mobile sont mises à jour à chaque utilisation de l'application **2N Mobile Key**.

- **Validité du code confidentiel de jumelage** – durée de validité du code confidentiel d’autorisation pour le jumelage d'un appareil mobile de l’utilisateur avec l’interphone.

Conseil

- En cas de perte d'un téléphone portable avec données d'accès, procédez comme ceci :

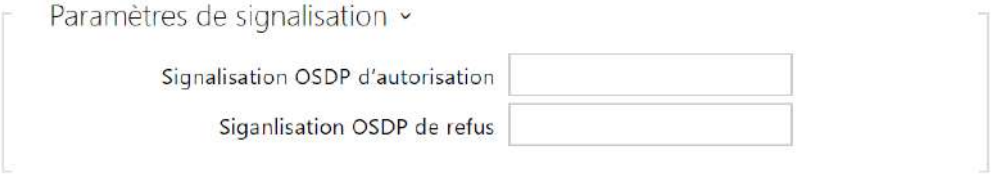
1. Supprimez la valeur de l'identifiant d'authentification de la clé mobile pour bloquer le téléphone perdu et éviter les utilisations non-autorisées.
2. Générez à nouveau la clé de cryptage principale (éventuellement) pour éviter toute utilisation abusive de la clé de cryptage stockée sur le périphérique mobile.

Avertissement

- Avec la mise à niveau vers la version 2.30, il y aura également une mise à niveau des modules bluetooth. Lors de la mise à niveau vers la version 2.29 et inférieure, ils peuvent mal fonctionner.

OSDP

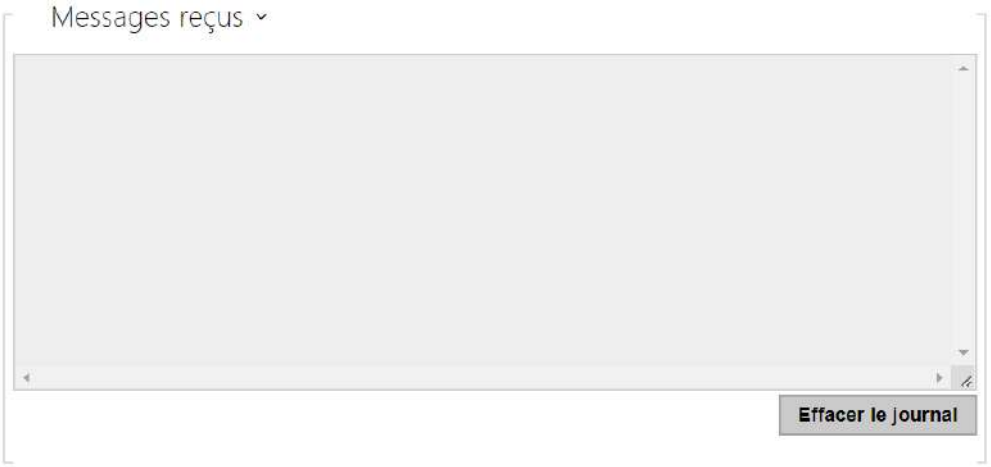
Le protocole OSDP assure une communication sécurisée pour l'envoi de données d'accès telles que l'ID de la carte d'accès ou le code PIN entre le dispositif OSDP connecté (panneau de commande, contrôleur de porte) et **l'interphone IP 2N**. L'objectif est de permettre d'activer la signalisation sur **l'interphone IP 2N** en fonction de la réponse de la contrepartie à la définition de signalisation de la carte envoyée.



- **Signalisation OSDP d'autorisation** – chaîne de définition pour la signalisation d'autorisation d'accès.
- **Siganlisation OSDP de refus** – chaîne de définition pour la signalisation de refus d'accès.

Observation

- Si la même définition est insérée dans les deux paramètres, l'évaluation se fera avec des expressions audiovisuelles qui correspondront au cas où l'accès autorisé et l'accès non autorisé seraient utilisés pour l'accès en succession rapprochée.



La fenêtre Messages reçus permet de récupérer la chaîne de définition. En présentant la carte d'accès au lecteur d'interphone IP 2N, la définition de signalisation OSDP de l'appareil de la contrepartie est affichée pour un accès autorisé ou non autorisé.

Le message reçu s'affiche avec les données temporelles au format :

13:46:39] led(0,0,0,0,0,0,0,0,1,1,1,2,2)
13:46:39] buz(0,2,1,1,1)
13:46:42] led(0,0,0,0,0,0,0,0,1,1,1,1,1)
13:46:42] buz(0,1,0,0,0)

Une partie (sans indication de l'heure) est utilisée comme chaîne de définition et sa longueur ne doit pas dépasser 255 caractères, par exemple : led(0,0,0,0,0,0,0,0,1,1,1,1,1) ou buz(0,2,1,1,1). Lors de l'évaluation de la correspondance de l'autre côté, l'appareil répond par une signalisation correspondante. Toute partie de la définition peut être remplacée par « * », cette partie sera interprétée comme n'importe quel contenu du message (par exemple, il est possible d'obtenir que la signalisation soit activée pour tout allumage de la LED 0 sur l'appareil, indépendamment des autres paramètres du message).

- **Effacer le journal** – efface l'enregistrement du message reçu.

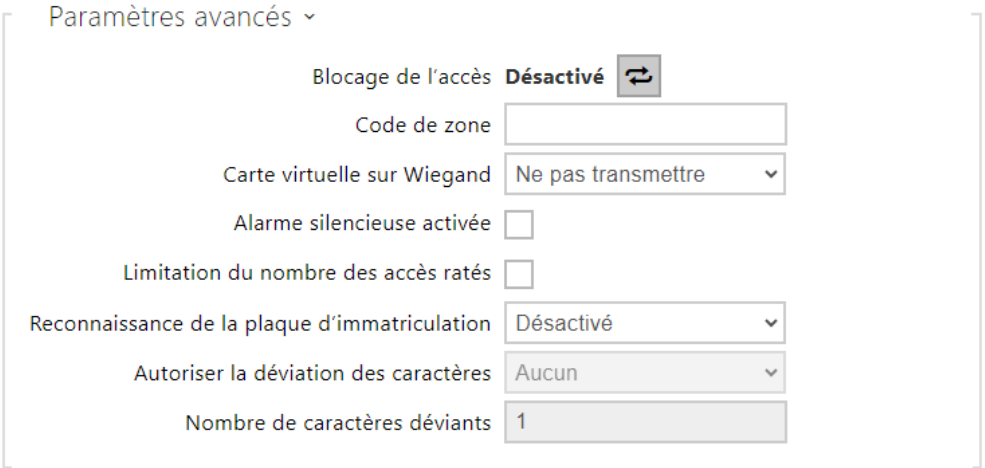
Observation

- Pour un bon fonctionnement, il convient que le paramètre Porte/Non utilisé soit défini dans la section Matériel/Modules d'extension pour le lecteur de cartes et le clavier. L'interphone IP 2N confirme le chargement de la carte par un bip sonore, après évaluation le dispositif répond par la signalisation correspondante.

Intégration avec d’autres systèmes

- **Autorisé** – il autorise la connexion avec le système de sécurité tiers Genetec Synergis.
- **Adresse du serveur Synergis** – Adresse IP du serveur Synergis ou nom de domaine.
- **Nom d’utilisateur** – authentification de l'utilisateur.
- **Mot de passe** – mot de passe d'authentification.
- **Format** – définit le format de lecture des cartes pour l’envoi de l’identifiant de la carte à Genetec Synergis.
- **Transférer les codes** – indique s’il faut transférer les codes attribués. Les codes peuvent avoir un maximum de 6 chiffres et il convient d’appuyer sur la touche de confirmation à la fin.
- **État de connexion** – affiche l'état actuel de la connexion au serveur Synergis ou une description de l'état d'erreur si nécessaire.
- **Cause du défaut** – affiche le motif de l'échec de la dernière tentative de connexion au serveur Synergis – le dernier message d'erreur, 404 Not Found, par exemple.

Onglet Avancé



- **Mode de compatibilité** – la prise en charge des anciens modes de lecture des cartes. Il n'est pas recommandé de l'utiliser en combinaison avec des cartes PICard. Si ce mode est désactivé, les numéros de carte doivent correspondre exactement pour que l'autorisation réussisse.

5.4.2 Streaming

Les **interphones IP 2N** fournissent plusieurs méthodes de streaming audio / vidéo ; se référer au tableau ci-dessous :

Méthode de transmission	Description
JPEG/HTTP	Transmission d'image JPEG statique. Reportez-vous à l'onglet JPEG ci-dessous.
MJPEG/HTTP	Une série d'images JPEG consécutives, la méthode Server Push - multipart / x-mixed-replace. Reportez-vous à l'onglet JPEG ci-dessous.
RTSP + RTP/UDP	RTSP avec flux audio et vidéo RTP / UDP distincts. Pris en charge à la fois de l'audio (G.711) et de la vidéo (H.264, H.263, MPEG-2 et MJPEG). Reportez-vous à l'onglet RTSP ci-dessous.
RTP/RTSP	Tunneling RTP via RTSP. Pris en charge à la fois de l'audio (G.711) et de la vidéo (H.264, H.263, MPEG-2 et MJPEG). Reportez-vous à l'onglet RTSP ci-dessous.
RTP/RTSP/HTTP	Tunneling RTSP via HTTP. Pris en charge à la fois de l'audio (G.711) et de la vidéo (H.264, H.263, MPEG-2 et MJPEG). Reportez-vous à l'onglet RTSP ci-dessous.

Méthode de transmission	Description
RTP/UDP-Multicast	Multicast de paquets RTP non contrôlés. Pris en charge de l'audio (G.711) uniquement. Reportez-vous à l'onglet Multicast ci-dessous.

Explication des termes

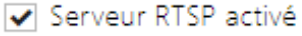
- **RTP (Real-Time Transport Protocol)** – c'est un protocole définissant le format des paquets standard pour la transmission audio / vidéo via les réseaux IP. Les **interphone IP 2N** utilisent ce protocole pour le streaming audio / vidéo. Le protocole de transport RTP est soit UDP, soit RTSP et HTTP.
- **RTSP (Real-Time Streaming Protocol)** – c'est un protocole réseau pour le contrôle en continu du serveur (contrôle de la configuration, du lancement et de l'arrêt des flux audio / vidéo).
- **HTTP (Hypertext Transfer Protocol)** – il aide à transmettre pratiquement tous les contenus et est principalement utilisé par les navigateurs Internet pour la communication entre serveurs Web. Les **interphones IP 2N** utilisent le protocole HTTP pour transmettre des images JPEG statiques ou des flux MJPEG via HTTP Server Push.
- **IP Multicast** – c'est un moyen d'envoyer en parallèle des paquets IP d'une source vers plusieurs destinations via le réseau IP. Les **interphones IP 2N** utilisent la diffusion multicast IP pour envoyer et recevoir des flux audio.
- **ONVIF (Open Network Video Interface Forum)** – c'est un ensemble de spécifications de recherche, de configuration et d'administration des caméra vidéo pour le réseau IP. Les **interphones IP 2N** sont compatibles ONVIF et supportent pleinement ONVIF Profile T et Profile S.
- **JPEG** – c'est une méthode standard de compression avec perte d'images.
- **MJPEG** – c'est un format de codage de flux vidéo dans lequel chaque image est compressée séparément par JPEG. Le codage MJPEG produit une vidéo de haute qualité à un débit nettement supérieur à celui des méthodes mentionnées ci-dessous.
- **H.263** – c'est une norme de compression de flux vidéo utilisée dans les télécommunications. Contrairement à MJPEG, le format H.263 utilise les différences entre les images consécutives et fournit un niveau de compression considérablement plus élevé au détriment de la qualité du flux vidéo.
- **H.263+** – il est semblable au H.263, mais prend en charge une méthode de mise en paquets de flux de bits différente.
- **MPEG-4 part 2** – est une norme de compression de flux vidéo utilisée principalement dans des domaines autres que les télécommunications, mais souvent prise en charge par les systèmes de caméra vidéo et de surveillance vidéo IP. Dans les **interphones IP 2N**, le niveau de compression et la qualité d'image sont comparables à ceux de la norme H.263.

- **H.264** – c'est une norme de compression de flux vidéo. Par rapport au H.263 et au MPEG-4, H.264 offre un niveau de qualité de flux vidéo à peu près identique, mais un demi-débit. Ce type de compression est parfois appelé MPEG-4, partie 10.
- **G.711** – est l'une des normes de transmission audio les plus courantes dans les télécommunications. Il utilise la fréquence d'échantillonnage de 8 kHz et les données sont compressées à l'aide de la compression logarithmique.

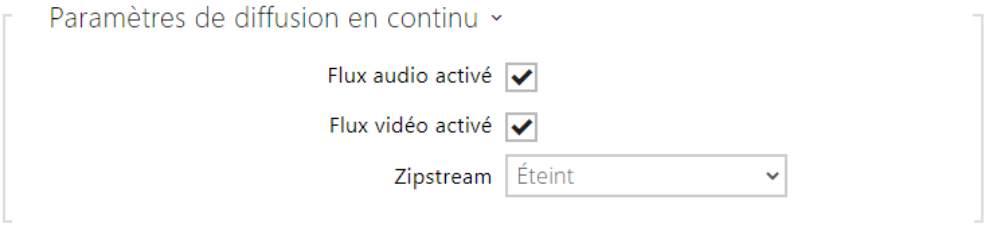
Liste des paramètres

ONVIF/RTSP

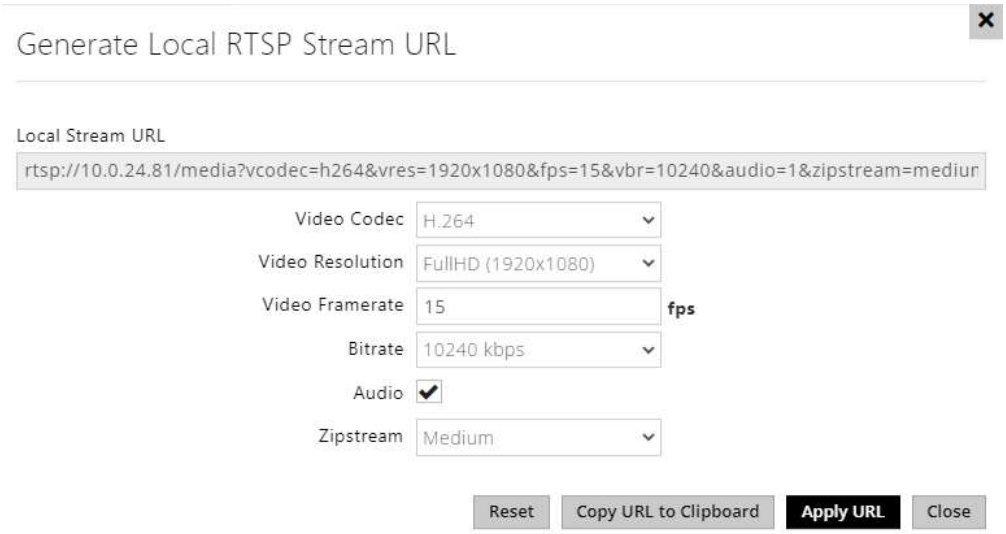
Les **interphones IP 2N** intègrent un serveur RTSP, qui peut être configuré dans cet onglet. Le serveur RTSP permet le streaming audio / vidéo. Vous pouvez choisir la méthode de transmission des données, la méthode / les paramètres de compression vidéo et d'autres paramètres associés à la sécurité et à la qualité de la transmission.



- **Serveur RTSP activé** – activez la fonction serveur RTSP sur l'interphone.



- **Flux audio activé** – activez l'offre de flux audio tout en établissant une connexion avec le serveur RTSP. Si la diffusion audio n'est pas autorisée, l'audio ne sera pas transmis via des profils de diffusion fixes ou via un flux URL local.
- **Flux vidéo activé** – activez l'offre de flux vidéo tout en établissant une connexion avec le serveur RTSP. Si la diffusion vidéo n'est pas autorisée, la vidéo ne sera pas transmise via des profils de diffusion fixes ou via un flux URL local.
- **Zipstream** – sélectionne le niveau de compression Zipstream initial (pour H.264). AXIS Zipstream préserve tous les détails légaux importants dont vous avez besoin tout en réduisant les besoins de transfert et de stockage de données de 50 % en moyenne. La compression Zipstream n'est disponible que pour les appareils équipés du processeur Artpec-7 et pour le codec H.264.
- **URL local du flux** – indique la dernière URL de flux générée et enregistrée pour le client RTSP. L'édition et la génération de l'URL du flux local peuvent être effectuées dans la boîte de dialogue qui s'ouvre en cliquant sur l'icône du crayon  .

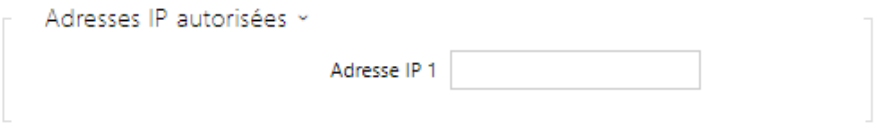


- **Codec vidéo** – sélection des codecs vidéo disponibles
- **Résolution vidéo** – sélection des résolutions vidéo possibles
- **Fréquence d'image vidéo** – paramètres de la fréquence d'images (1 à 30 fps, la valeur maximale possible pour le codec vidéo MJPEG est de 15 fps).
- **Bitrate** – sélection du débit binaire disponible
- **Audio** – autoriser la transmission audio
- **Zipstream** (disponible uniquement pour H.264) – paramètre du zipstream de l'URL du flux local qui a la priorité sur la valeur spécifiée dans **les Paramètres de diffusion en continu**.

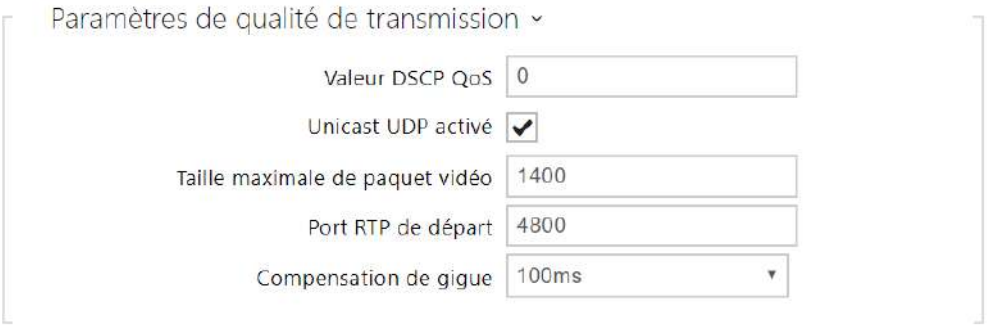
Le nombre de flux RTSP est limité à 4 flux parallèles. Ce nombre inclut les deux flux audio sans canal de retour vidéo et audio dirigé vers l'interphone.

Assurez-vous de définir au moins un compte d'utilisateur et le niveau d'accès approprié (conformément aux spécifications ONVIF et au système de gestion des messages utilisés) pour obtenir la fonctionnalité ONVIF complète. Sans cela, seul les fonctionnalités de base sont disponibles.

- **Nom** – définissez le nom de l'utilisateur pour l'accès à ONVIF.
- **Mot de passe** – définissez le mot de passe d'accès ONVIF.
- **Niveau d'accès à Onvif** – définissez le niveau d'accès ONVIF de l'utilisateur (Utilisateur, Operateur, Administrateur).



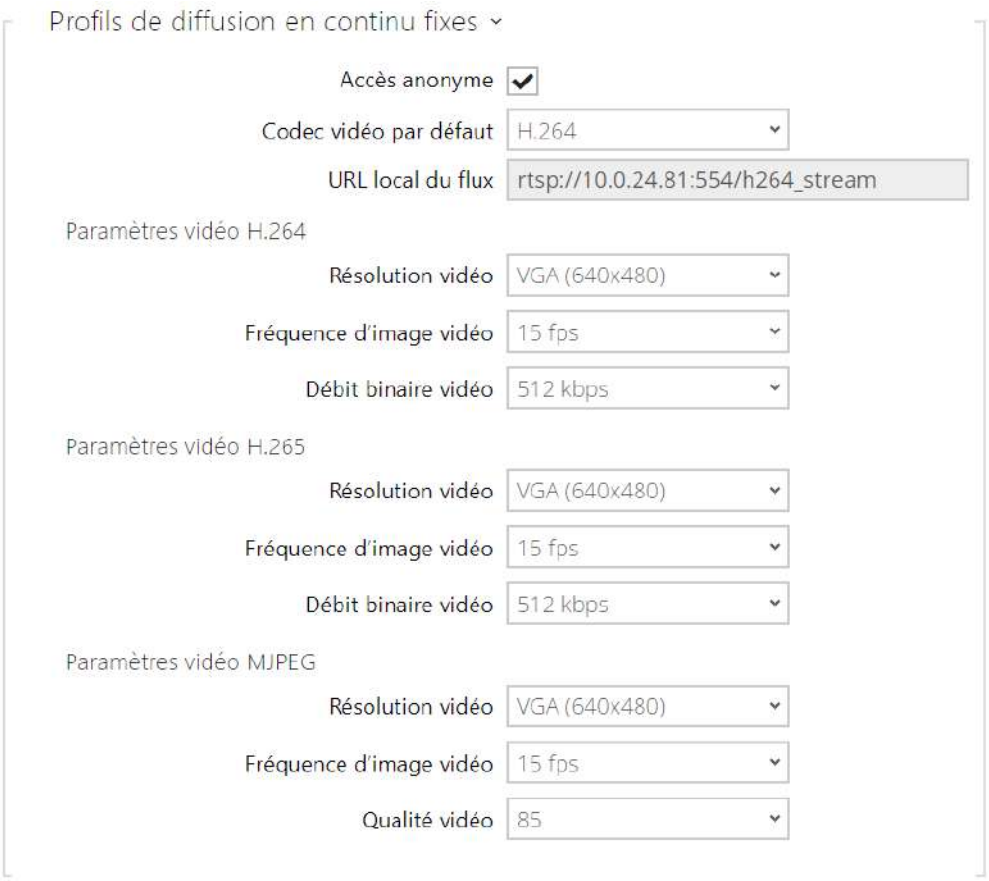
- **Adresse IP 1–4** – définir au maximum 4 adresses IP autorisées à partir desquelles vous pouvez vous connecter au serveur RTSP. Si aucun des quatre champs n'est rempli, une adresse IP quelconque peut être utilisée pour se connecter.



- **Valeur DSCP QoS** – définissez la priorité de paquets audio/vidéo RTP dans le réseau. La valeur programmée est envoyée dans le champ TOS (Type of Service) de l'en-tête du paquet IP.
- **Unicast UDP activé** – activez l'envoi de flux audio/vidéo via RTP/UDP. Si ce mode est éteint, les données de flux audio/vidéo sont uniquement envoyées via RTP/RTSP.
- **Taille maximale de paquet** – définissez la taille maximale des paquets vidéo à envoyer via le protocole RTP / UDP.
- **Port RTP de départ** – réglez le port RTP local de départ dans l'intervalle de la longueur de 60 ports à utiliser pour les transmissions audio et vidéo. La valeur par défaut est 4800 (c.-à-d. que l'intervalle utilisée est 4800–4863).
- **Compensation de gigue** – paramétrez la capacité tampon pour la compensation de gigue dans les transmissions de paquets audio. Une capacité supérieure améliore la résistance de transmission aux dépens d'une plus grande chambre d'écho.

Conseil

- FAQ: VLC Player – Comment visualiser la vidéo des interphones IP 2N depuis le serveur RTSP
- FAQ: VLC Player – Comment enregistrer la vidéo des interphones IP 2N



Note

- ONVIF media 1 ne prend pas en charge le profil H.265.

- **Accès anonyme** – enable access to the original RTSP server streams without user authentication. If this field is unselected, the RTSP client must authenticate itself as one of the ONVIF users while accessing the server.
- **Codec vidéo par défaut** – paramètre par défaut du codec vidéo proposé lors de la diffusion en continu via RTSP.
- **Local Stream URL** – affiche l'URL locale du flux en fonction de la sélection du codec

- **Résolution vidéo** – définissez la résolution d'image par défaut pour la diffusion RTSP en continu.
- **Fréquence d’image vidéo** – définissez la fréquence d'images vidéo par défaut pour la diffusion RTSP en continu.
- **Débit binaire vidéo** – définissez le débit binaire vidéo par défaut pour la diffusion RTSP en continu.
- **Qualité vidéo** – paramétrez le niveau de compression vidéo de 10 (qualité faible, débit binaire le plus bas) à 99 (excellente qualité, débit binaire le plus élevé).

JPEG

Configurez ici le moyen le plus simple de récupérer le streaming vidéo : JPEG / HTTP et MJPEG / HTTP. Envoyez la requête d'adresse GET suivante pour télécharger des images à partir de l'interphone :

http://ip_adresse_interphone/api/camera/snapshot?width=**W**&height=**H**

ou (pour MJPEG, HTTP Server Push):

- http://ip_adresse_interphone/api/camera/snapshot?width=**W**&height=**H**&fps=**N**

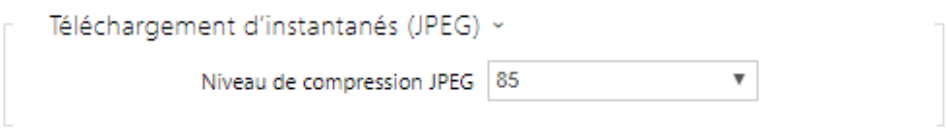
où W et H spécifient la résolution de l'image (résolutions supportées : 160 x 120, 320 x 240, 640 x 480, 176 x 144, 322 x 272, 352 x 288, 1280 x 960 – (seulement pour les modèles équipés d'une caméra 1 Mega Pixel). N correspond au nombre d'instantanés par seconde (1 à 10).

Le tableau suivant indique le nombre maximal de flux MJPEG / HTTP simultanés dans lesquels le débit des images sortantes utilisant le niveau de compression JPEG par défaut n'est pas réduit.

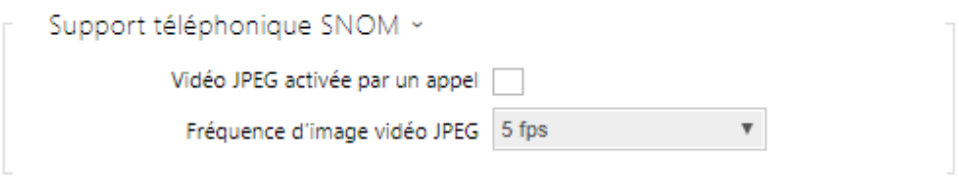
Type d'interphone	Résolution	Nombre de flux
Force/Vario	640 x 480	15
Force HD	640 x 480	15
Force HD	1280 x 960	3
Verso	640 x 480	8
Verso	1280 x 960	2

Note

- *La méthode HTTP Server Push avec le contenu multipart / x-mixed-replace n'est pas prise en charge par tous les navigateurs Internet. Testez la fonction dans le navigateur Firefox, par exemple.*



- **Niveau de compression JPEG** – réglez le niveau de compression JPEG (de 1 à 99). 85 est la valeur recommandée. Ce paramètre affecte la taille et la qualité de l'image.

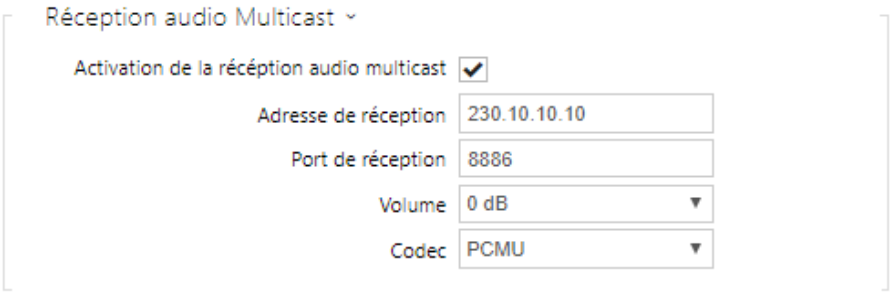


Certains téléphones IP (SNOM 820/870) ne prennent pas en charge les appels vidéo mais peuvent télécharger et afficher des instantanés JPEG à partir de l'adresse IP prédéfinie pendant un appel. Nos interphones supportent cette fonctionnalité : définissez les paramètres dans cet onglet.

- **Vidéo JPEG activée par un appel** – activez le téléchargement d'instantanés pris par la caméra lors d'un appel avec les téléphones Snom 820/870.
- **Fréquence d'image vidéo JPEG** – réglez la fréquence d'image ou les périodes pour le téléchargement d'instantanés pris par la caméra avec les téléphones Snom 820/870.

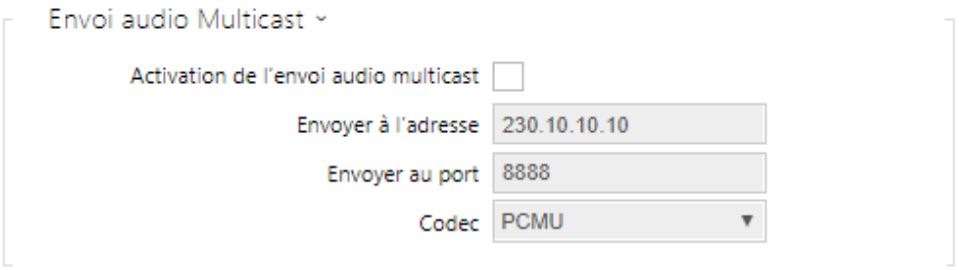
Multicast

Les **interphones IP 2N** vous permettent de diffuser des signaux audio (provenant du microphone ou d'une autre entrée audio de l'interphone) via des paquets RTP envoyés vers l'adresse multicast, de recevoir des flux audio au même format et de les lire via le haut-parleur intégré ou une autre sortie audio de l'interphone. Le flux audio est codé selon la loi G.711.



- **Activation de la réception audio multicast** – paramétrez le port de destination pour le flux audio. Le flux audio reçu est également diffusé lors d'un appel actif et les sons des deux sources sont mélangés.
- **Adresse de réception** – paramétrez l'adresse IP MultiCast pour recevoir des paquets RTP MultiCast.
- **Port de réception** – paramétrez le port local pour recevoir des paquets RTP MultiCast.
- **Volume** – paramétrez le volume de diffusion du flux audio reçu.

- **Codec** – définissez le codec audio pour le décodage de paquets RTP : PCMU, PCMA, G.722, L.16. Les codecs haut débit G.722 et L16 sont disponibles dans certains modèles d'interphone uniquement.



- **Activation de l'envoi audio multicast** – activez l'envoi de paquets RTP à l'adresse et au port MultiCast sélectionnés.
- **Envoyer à l'adresse** – paramétrez l'adresse IP MultiCast de destination pour le flux audio.
- **Envoyer au port** – paramétrez le port de destination pour le flux audio.
- **Codec** – définissez le codec audio pour le décodage de paquets RTP : PCMU, PCMA, G.722, L.16. Les codecs haut débit G.722 et L16 sont disponibles dans certains modèles d'interphone uniquement.

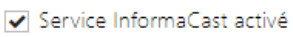
InformaCast

Les **interphones IP 2N** prennent en charge le protocole de streaming audio InformaCast qui vous aide à configurer un flux audio (unicast / multicast RTP / UDP codé avec la loi G.711) entre l'interphone et un serveur InformaCast ou tout autre client InformaCast.

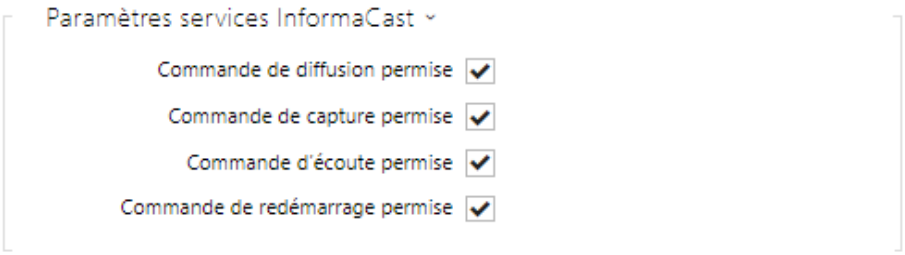
Lorsque vous activez ce service, les serveurs InformaCast sont automatiquement trouvés sur le réseau local via le serveur SLP et l'interphone est automatiquement enregistré avec eux. Le serveur InformaCast auprès duquel l'interphone est enregistré peut envoyer les commandes de configuration du flux audio à l'interphone.

- **Diffusion** – l'interphone reçoit le son du serveur InformaCast et le lit via un haut-parleur intégré.
- **Capture** – l'interphone enregistre l'audio via un microphone interne et l'envoie au serveur InformaCast.
- **Ecoute** – l'interphone reçoit l'audio d'un autre client InformaCast.

L'interphone prend en charge l'enregistrement simultané de 4 serveurs InformaCast au maximum et la configuration de 6 flux audio parallèles au maximum.



- **Service InformaCast activé** – activez le service InformaCast sur votre interphone.

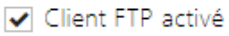


- **Commande de diffusion** – activez la commande de diffusion pour mettre en place l'envoi d'un flux audio à l'interphone par le serveur InformaCast.
- **Commande de capture** – activez la commande de capture pour mettre en place l'envoi d'un flux audio à l'interphone par le serveur InformaCast.
- **Commande d'écoute permise** – activez la commande d'écoute pour mettre en place l'envoi d'un flux audio à l'interphone par un autre client InformaCast.
- **Commande de redémarrage permise** – activez la commande de redémarrage pour permettre au serveur InformaCast de redémarrer l'interphone.

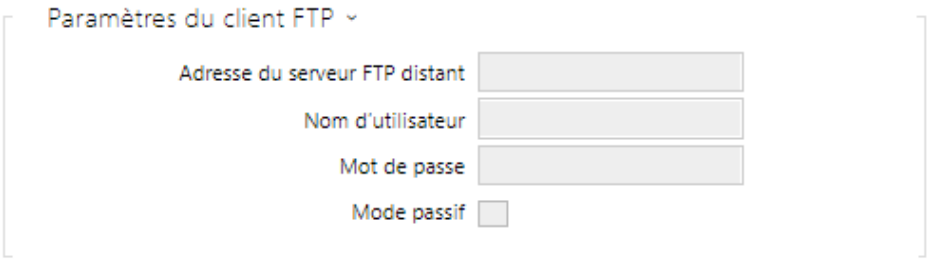
FTP

Définissez ici l'accès au serveur FTP (S) où les images de caméras internes / externes peuvent être stockées au format JPEG et sous la résolution sélectionnée. Le nom de fichier de l'image comprend la date et l'heure de la prise de vue.

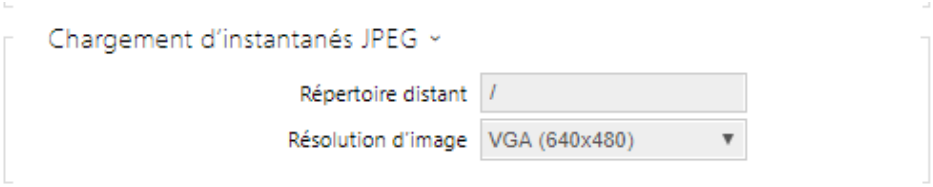
Les images sont stockées sur le serveur FTP soit automatiquement (périodiquement ou au début de l'appel), soit via l'automatisation en utilisant l'Action **UploadSnapshotToFTP**.



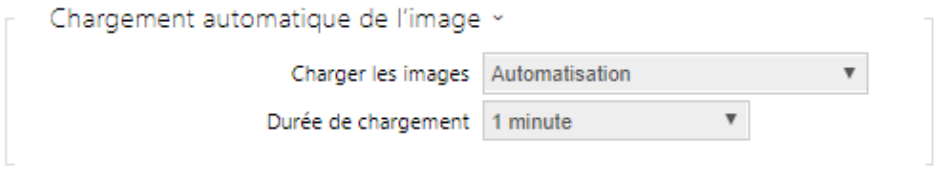
- **Client FTP activé** – activez l'enregistrement des images de la caméra sur le serveur FTP.



- **Adresse du serveur FTP distant** – définissez l'adresse du serveur FTP dans ftp://ip_adresse ou ftps://ip_adresse format.
- **Nom d'utilisateur** – définissez le nom d'utilisateur du serveur FTP. Ce paramètre est obligatoire si le serveur FTP requiert une authentification de l'utilisateur.
- **Mot de passe** – définissez un mot de passe pour l'utilisateur du serveur FTP mentionné ci-dessus.
- **Mode passif** – Paramétrez le mode passif pour les transferts (comme un navigateur WWW).



- **Répertoire distant** – définissez le répertoire du serveur FTP dans lequel les images de la caméra doivent être enregistrées.
- **Résolution d'image** – définissez la résolution des images.

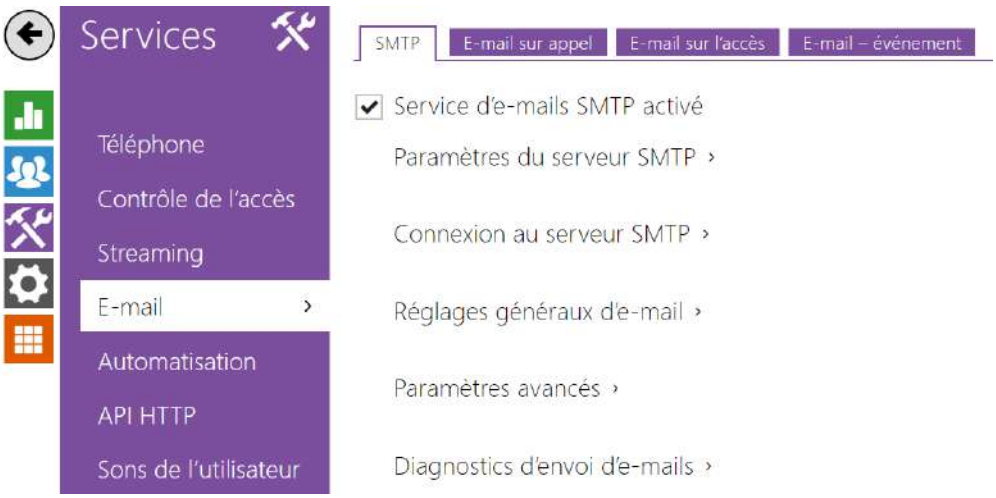


- **Charger les images** – permet de régler l'envoi automatique des images sur le serveur FTP en début d'appel, éventuellement périodiquement ou à la fin de la durée établie. L'envoi automatique d'une image peut être éteint (option Automatisation), ensuite il reste possible d'envoyer des images au moyen de l'action automatique UploadSnapshotToFtp.

- **Durée de chargement** – définit la période de l'envoi automatique des images à FTP lors du réglage du paramètre **Envoi des images** à la valeur **Périodiquement**. La période peut être comprise entre 10 secondes et 30 minutes.

Cliquez sur **Appliquer et tester** pour enregistrer la configuration actuelle du serveur FTP, charger l'image de la caméra et enregistrer l'image sur le serveur FTP. La fenêtre ci-dessus affiche les détails de la communication avec le serveur FTP lors de la sauvegarde.

5.4.3 E-Mail



Pour informer les utilisateurs de l'interphone de tous les appels manqués et / ou passés avec succès, vous pouvez configurer **l'interphone IP 2N** pour envoyer un courrier électronique après chaque appel. Il vous est possible de personnaliser l'objet de l'e-mail et le texte du message. Si votre interphone est équipé d'une caméra, vous pouvez également joindre de manière automatique un ou plusieurs instantanés pris pendant l'appel ou la sonnerie.

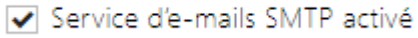
L'interphone peut envoyer des courriers électroniques à tous les utilisateurs dont les adresses de messagerie valides sont renseignées dans le répertoire. Si le paramètre **E-Mail** de la liste d'utilisateurs est vide, les e-mails sont envoyés à l'adresse électronique par défaut.

Vous pouvez également envoyer des emails depuis l'interface d'Automatisation en utilisant l'action **Action.SendEmail**.

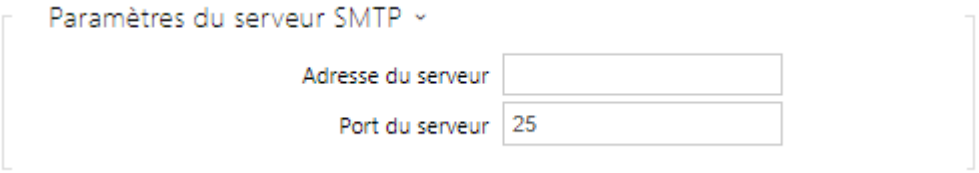
Note

- *La fonction de courriel n’est disponible qu’avec la licence Gold.*

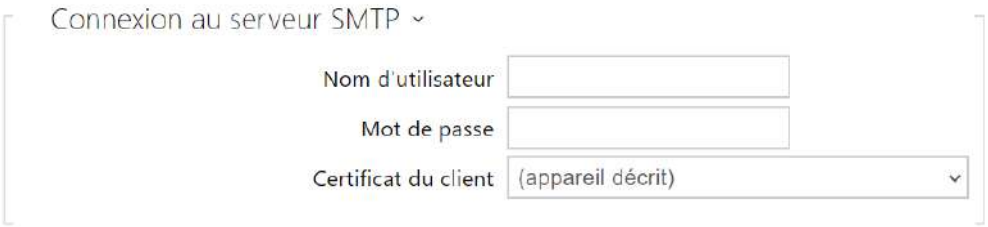
SMTP



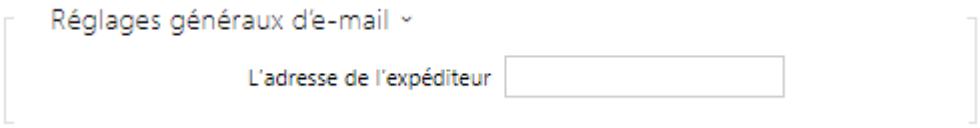
- **Service d'e-mails SMTP activé** – activer/désactiver l'envoi d'e-mails à partir de l'interphone.



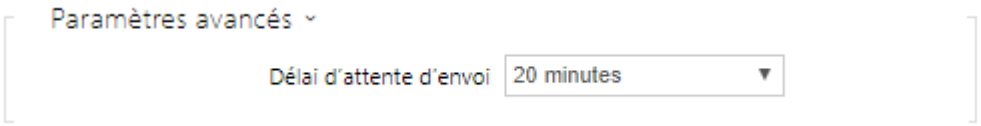
- **Adresse du serveur** – paramétrez l'adresse du serveur SMTP auquel les e-mails doivent être envoyés.
- **Port du serveur** – précisez le port du serveur SMTP. Modifiez la valeur uniquement si le paramètre du serveur SMTP ne répond pas à la norme. La valeur de référence du port SMTP est 25.



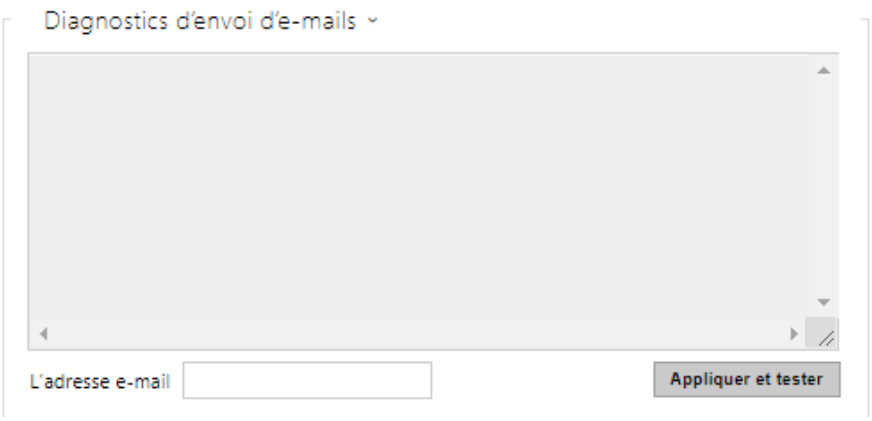
- **Nom d'utilisateur** – si le serveur SMTP nécessite une authentification, ce champ doit contenir un nom valide pour la connexion au serveur. Sinon, vous pouvez laisser le champ vide.
- **Mot de passe** – saisissez le mot de passe de connexion du serveur SMTP.
- **Certificat du client** – spécifiez le certificat client et la clé privée pour le dispositif – cryptage de communication du serveur SMTP. Sélectionner l'un des trois jeux de certificats d'utilisateur et de clés privées (se référer à la partie Certificats) ou conserver le paramètre **SelfSigned** grâce auquel le certificat est automatiquement généré lors du premier allumage de l'appareil.



- **L’adresse de l’expéditeur** – définissez l'adresse de l'expéditeur pour tous les courriels sortants à partir de l'interphone.



- **Délai d'attente pour l'envoi** – définissez le délai d'envoi d’un e-mail vers un serveur SMTP inaccessible.



Cliquez sur **Appliquer et Tester** pour envoyer un e-mail de test à l’adresse définie dans le but de tester la fonctionnalité du paramètre d’envoi d’e-mail. Entrez l'adresse e-mail de destination dans le champ Adresse e-mail de test et appuyez sur le bouton. L'état d'envoi du courrier électronique est affiché en permanence dans la fenêtre pour vous permettre de détecter un problème de configuration, le cas échéant, sur l'interphone ou sur un autre élément du réseau. Une photo est toujours jointe au courrier électronique, même dans les modèles sans caméra où l’image est envoyée avec N / A.

E-Mail sur appel

Définissez l'envoi d'e-mails lors d'appels sortants sur cet onglet.

- **Envoyer un e-mail à l'utilisateur lors** – définissez l'envoi d'un e-mail en cas d'appel sortant effectué / manqué. Les options suivantes sont disponibles
  - **N'importe quel appel sortant** – un email sera envoyé pour n'importe quel appel sortant.
  - **Appel sortant manqués** – un email sera envoyé pour les appels sortant manqués.
  - **Jamais** – aucun n'email n'est envoyé en cas d'appel sortant.

> **Note**
>
> - Les E-mail peuvent être envoyé depuis l'interface d'Automatisation.

- **Objet du message** – définissez l'objet de l'e-mail envoyé.
- **Corps du message** – modifier le texte à envoyer. Utiliser le langage de formatage HTML dans le texte. Il est possible d'insérer des symboles spéciaux pour remplacer le nom d'utilisateur, la date et l'heure, l'identifiant de l'interphone ou le numéro appelé ; ces symboles seront remplacés par les valeurs correspondantes avant l'envoi. Des symboles spéciaux pour remplacer la date et l'heure, l'identification de l'interphone et le numéro composé peuvent être utilisés. Des symboles spéciaux pour la date et l'heure et pour identifier l'interphone peuvent être utilisés. Ces symboles seront remplacés par les valeurs

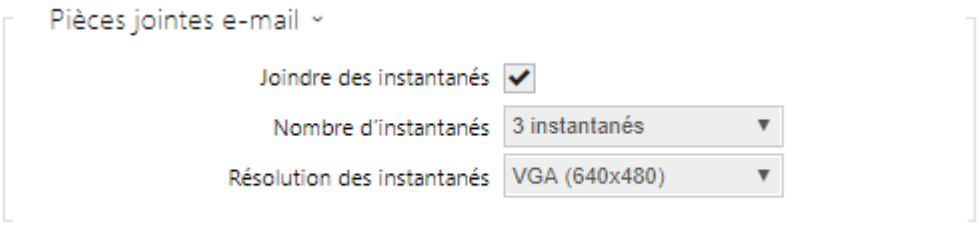
réelles avant d'envoyer le message. La liste des symboles de substitution rencontrés dans le modèle est récapitulée dans le tableau à la fin du présent chapitre.

Corps du message

```
<p>Hello <b>$User$</b>
</p>
<p>You had a call on: <b>$DateTime$</b>
  <br>The number dialed was: <b>$DialNumber$</b>
</p>
<p>This e-mail message is generated automatically by device: <b>$DeviceName$</b>. Do
not reply to this message.
</p>
```

Observation

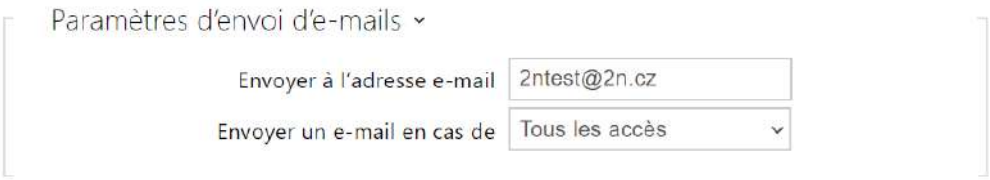
- Si l'appel est passé à plusieurs utilisateurs, l'espace réservé pour le nom de l'utilisateur appelé $User$ est vide.



- **Joindre des instantanés** – permet l'envoi d'une pièce jointe comprenant une ou plusieurs photos prises depuis la caméra de l'interphone pendant une sonnerie ou un appel.
- **Nombre d'instantanés** – réglez le nombre d'instantanés à joindre à un message envoyé par e-mail.
- **Résolution des instantanés** – définissez la résolution de l'instantané pour les images à envoyer.

E-mail sur l'accès

Définissez qu'un e-mail doit être envoyé à chaque fois qu'une carte RFID est rentré sur le lecteur de carte et / ou un clé d'accès Mobile sur le lecteur Bluetooth et / ou un empreinte digitale sur le lecteur Biométrique.



- **Envoyer à l'adresse e-mail** – paramètres de l'adresse e-mail de l'administrateur.
- **Paramètres d'envoi d'e-mails** – définissez l'envoi d'e-mail. Les options suivantes sont disponibles :
  - **Ne pas envoyer d'e-mail** – l'e-mail ne sera pas envoyé.
  - **Tous les accès** – un e-mail sera envoyé pour toutes les tentatives d'accès (valides / invalides).
  - **Accès refusés** – un e-mail sera envoyé seulement si l'accès est refusé.

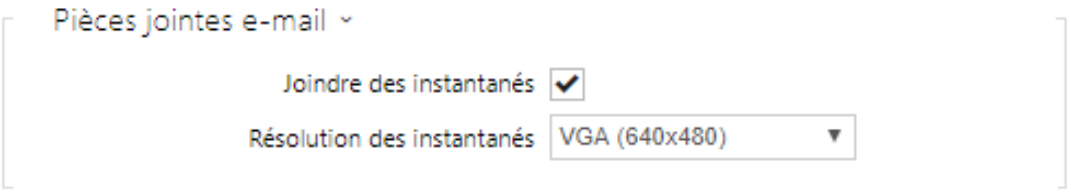
- **Objet du message** – définit l'objet de l'e-mail envoyé.
- **Corps du message** – modifier le texte à envoyer. Utiliser le langage de formatage HTML dans le texte. Il est possible d'insérer des symboles spéciaux pour remplacer le nom d'utilisateur, la date et l'heure, l'identifiant de l'interphone ou le numéro appelé ; ces symboles seront remplacés par les valeurs correspondantes avant l'envoi. Des symboles spéciaux pour remplacer la date et l'heure, l'identification de l'interphone et le numéro composé peuvent être utilisés. Des symboles spéciaux pour la date et l'heure et pour identifier l'interphone peuvent être utilisés. Ces symboles seront remplacés par les valeurs réelles avant d'envoyer le message. La liste des symboles de substitution rencontrés dans le modèle est récapitulée dans le tableau à la fin du présent chapitre.

Corps du message

```
<p>Hello,
</p>
<p>User <b>$User$</b> generated a new access event on device <b>$DeviceName$</b> (IP:
<b>$Ip4Address$</b>)
</p>
<ul>
  <li>Authentication Type: <b>$AuthIdType$</b>
  </li>
  <li>Authentication ID: <b>$AuthId$</b>
  </li>
  <li>Validity: <b>$AuthIdValid$</b>
  </li>
  <li>Reason: <b>$AuthIdReason$</b>
  </li>
  <li>Direction: <b>$AuthIdDirection$</b>
  </li>
  <li>Date/Time: <b>$DateTime$</b>
  </li>
</ul>
<p>This e-mail message is generated automatically by device: <b>$DeviceName$</b>. Do
not reply to this message.
</p>
```

Observation

- Une syntaxe étendue peut être utilisée pour les espaces réservés $AuthIdType$ et $AuthIdValid$ afin de remplacer les valeurs dans différentes langues. $AuthIdValid|Valid=valid|Invalid=invalid$
  - En cas de valeur $AuthId$ invalide, la première moitié de l'ID est masquée, par ex. : ******11188, **********792d9044158891fa, etc .
  - En cas de valeur $AuthId$ valide, l'intégralité de l'ID **** est masquée.
- Si la valeur dans l'espace réservé est introuvable dans la chaîne, la valeur par défaut est utilisée directement.



- **Joindre des instantanés** – autorise l'envoi d'une pièce jointe avec un ou plusieurs clichés de la caméra pris après l'activation du commutateur d'autoprotection.

- **Résolution des instantanés** – paramétrez la résolution des instantanés pour l'envoi d'images.

E-mail – événement

Configurez l'envoi d'un e-mail à chaque fois que la connexion SIP est perdue, que l'appareil se redémarre ou que le commutateur d'autoprotection s'active sur l'appareil.

Envoyer à l'adresse e-mail – définissez l'envoi d'e-mail. Les options suivantes sont disponibles :

- **Perte de l'enregistrement SIP**
- **Redémarrer l'appareil**
- **Activation de l'interrupteur de protection**

Message en cas de perte de l'enregistrement SIP – définissez le message à envoyer à l'adresse e-mail spécifiée chaque fois que l'enregistrement SIP est perdu.

- **Objet du message** – définit l'objet de l'e-mail envoyé.
- **Corps du message** – modifier le texte à envoyer. Utiliser le langage de formatage HTML dans le texte. Il est possible d'insérer des symboles spéciaux pour remplacer le nom d'utilisateur, la date et l'heure, l'identifiant de l'interphone ou le numéro appelé ; ces symboles seront remplacés par les valeurs correspondantes avant l'envoi. Des symboles spéciaux pour remplacer la date et l'heure, l'identification de l'interphone et le numéro composé peuvent être utilisés. Des symboles spéciaux pour la date et l'heure et pour identifier l'interphone peuvent être utilisés. Ces symboles seront remplacés par les valeurs réelles avant d'envoyer le message. La liste des symboles de substitution rencontrés dans le modèle est récapitulée dans le tableau à la fin du présent chapitre.

Corps du message

```
<p>Hello,
</p>
<p>SIP account <b>$SipAccountNumber$</b> of device <b>$DeviceName$</b> (IP:
<b>$Ip4Address$</b>) got unregistered on <b>$DateTime$</b>
</p>
<p>This e-mail message is generated automatically by device: <b>$DeviceName$</b>. Do
not reply to this message.
</p>
```

Observation

- Si la valeur dans l'espace réservé est introuvable dans la chaîne, la valeur par défaut est utilisée directement.

Message lors du redémarrage de l'appareil – définissez le message à envoyer à l'adresse e-mail spécifiée à chaque redémarrage de l'appareil.

- **Objet du message** – définit l'objet de l'e-mail envoyé.
- **Corps du message** – modifier le texte à envoyer. Utiliser le langage de formatage HTML dans le texte. Il est possible d'insérer des symboles spéciaux pour remplacer le nom d'utilisateur, la date et l'heure, l'identifiant de l'interphone ou le numéro appelé ; ces symboles seront remplacés par les valeurs correspondantes avant l'envoi. Des symboles spéciaux pour remplacer la date et l'heure, l'identification de l'interphone et le numéro composé peuvent être utilisés. Des symboles spéciaux pour la date et l'heure et pour identifier l'interphone peuvent être utilisés. Ces symboles seront remplacés par les valeurs réelles avant d'envoyer le message. La liste des symboles de substitution rencontrés dans le modèle est récapitulée dans le tableau à la fin du présent chapitre.

Corps du message

```
<p>Hello,
</p>
<p>Device <b>$DeviceName$</b> (IP: <b>$Ip4Address$</b>) rebooted on <b>$DateTime$</b>
</p>
<ul>
  <li>Reason: <b>$RebootReason$</b>
  </li>
  <li>Uptime: <b>$UpTime$</b>
  </li>
  <li>Firmware version: <b>$SoftwareVersion$</b>
  </li>
  <li>Build date: <b>$BuildTime$</b>
  </li>
</ul>
<p>This e-mail message is generated automatically by device: <b>$DeviceName$</b>. Do
not reply to this message.
</p>
```

Observation

- Si la valeur dans l'espace réservé est introuvable dans la chaîne, la valeur par défaut est utilisée directement.

Message lors de l'activation du commutateur de sécurité – définissez le message à envoyer à l'adresse e-mail spécifiée à chaque fois que le commutateur d'autoprotection est activé.

- **Objet du message** – définit l'objet de l'e-mail envoyé.
- **Corps du message** – modifier le texte à envoyer. Utiliser le langage de formatage HTML dans le texte. Il est possible d'insérer des symboles spéciaux pour remplacer le nom d'utilisateur, la date et l'heure, l'identifiant de l'interphone ou le numéro appelé ; ces symboles seront remplacés par les valeurs correspondantes avant l'envoi. Des symboles spéciaux pour remplacer la date et l'heure, l'identification de l'interphone et le numéro composé peuvent être utilisés. Des symboles spéciaux pour la date et l'heure et pour identifier l'interphone peuvent être utilisés. Ces symboles seront remplacés par les valeurs réelles avant d'envoyer le message. La liste des symboles de substitution rencontrés dans le modèle est récapitulée dans le tableau à la fin du présent chapitre.

- **Joindre des images à partir de la caméra** – autorise l'envoi d'une pièce jointe avec un ou plusieurs clichés de la caméra pris après l'activation du commutateur d'autoprotection.
- **Nombre d'images jointes** – définissez le nombre d'instantanés à joindre dans l'e-mail.
- **Résolution des instantanés** – paramétrez la résolution des instantanés pour l'envoi d'images.

Corps du message

```
<p>Hello,
</p>
<p>Tamper switch of device <b>$DeviceName$</b> (IP: <b>$Ip4Address$</b>) was
activated on <b>$DateTime$</b>
</p>
<p>This e-mail message is generated automatically by device: <b>$DeviceName$</b>. Do
not reply to this message.
</p>
```

Observation

- Si la valeur dans l'espace réservé est introuvable dans la chaîne, la valeur par défaut est utilisée directement.

Observation

- Le nom du symbole de substitution $DeviceName$ est directement lié à la valeur du paramètre *Nom de l'équipement* dans la section Services / Serveur web / Paramétres de base. Nous vous recommandons d'utiliser un nom définissant clairement l'équipement dont il s'agit.

Liste des symboles de substitution

Occurrence	Symbole de substitution	Description
Toujours	$DateTime$	date et heure actuelles
	$DeviceName$	nom de l'équipement
	$Ip4Address$	adresse IP de l'équipement
	$SoftwareVersion$	version du micrologiciel
	$BuildTime$	date et heure d'établissement
	$UpTime$	période d'exploitation de l'équipement

Occurrence	Symbole de substitution	Description
Fonction du cas spécifique	$User$	nom de l'utilisateur
	$RebootReason$	raison du redémarrage
	$DialNumber$	numéro appelé, entrant ou sortant
	$SipAccountNumber$	numéro de compte SIP
	$AuthId$	ID d'authentification
	$AuthIdDirection$	direction (sortie/entrée)
	$AuthIdType$	type d'identification
	$AuthIdValid$	valide, invalide
	$AuthIdReason$	raison du rejet

Vue d'ensemble des symboles de substitution dans les événements

Symbole de substitution / Fonction	E-mail sur l'accès	E-mail sur appel	E-mail sur perte de l'enregistrement SIP	E-mail sur redémarrer l'appareil	E-mail sur activation de l'interrupteur de protection	E-mail sur envoi de diagnostic	Automatisation
$DateTime$	*	*	*	*	*	*	*
$DeviceName$	*	*	*	*	*	*	*
$Ip4Address$	*	*	*	*	*	*	*
$SoftwareVersion$	*	*	*	*	*	*	*
$BuildTime$	*	*	*	*	*	*	*
$UpTime$	*	*	*	*	*	*	*

Symbole de substitution / Fonction	E-mail sur l'accès	E-mail sur appel	E-mail sur perte de l'enregistrement SIP	E-mail sur redémarrer l'appareil	E-mail sur activation de l'interrupteur de protection	E-mail sur envoi de diagnostic	Automatisation
$User$	*	*				*	*
$RebootReason$				*			
$DialNumber$		*				• (envoie de l'« E-mail de test »)	CallStateChanged
$SipAccountNumber$			*				
$AuthId$	*						CardEntered, CardHeld
$AuthIdDirection$	*						CardEntered, CardHeld
$AuthIdType$	*						CardEntered, CardHeld
$AuthIdValid$	*						CardEntered, CardHeld
$AuthIdReason$	*						

5.4.4 Automatisation

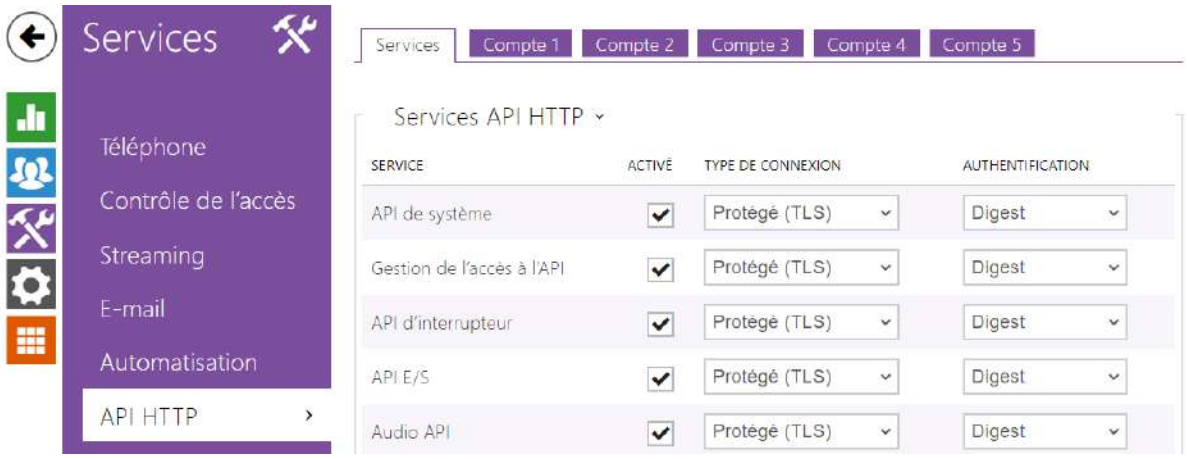
Les **Interphones IP 2N** offrent des options de réglage très flexibles pour répondre aux besoins variables des utilisateurs. Il existe des situations dans lesquelles les paramètres de configuration standards (modes commutateur ou appel, par exemple) sont insuffisants. Il s'agit de l'interface d'**Automatisation**, une interface programmable spéciale pour les applications nécessitant des interconnexions complexes avec des systèmes tiers ou des fonctionnalités automatiques personnalisables pour améliorer le confort et/ou la sécurité.

Référez-vous au Manuel d'Automatisation pour découvrir les possibilités et les détails de la configuration.

> **Note**
>
> - *La fonction Automatisation est disponible uniquement avec la licence Gold.*

5.4.5 API HTTP

HTTP API est une interface d'application conçue pour le contrôle de certaines fonctionnalités des **interphones IP 2N** via HTTP. Il permet d'intégrer facilement nos appareils à des systèmes tiers, tels que la domotique, les systèmes de sécurité et de surveillance, les solutions d'Hypervision...etc.



Services

HTTP API offre les services suivants :

- **API de système** – permet les modifications de configuration de l'interphone, les informations d'état et les mises à jour.
- **Gestion de l'accès à l'API** – permet de gérer les accès et la façon dont l'authentification des utilisateurs est vérifiée.
- **API d'interrupteur** – permet le contrôle et la surveillance de l'état des interrupteurs, par ex. ouverture de la porte, etc.
- **API E/S** – permet le contrôle et la surveillance des entrées / sorties logiques de l'interphone.
- **API Audio** – permet un contrôle de la lecture audio et la surveillance du microphone.
- **API de la Caméra** – permet le contrôle et la surveillance des images de la caméra.
- **API de l'Ecran** – permet le contrôle de l'écran tactile et la surveillance des informations utilisateurs.
- **API E-mail** – permet l'envoi d'e-mails à des utilisateurs.
- **API du téléphone/appel** – assure le contrôle et la surveillance des appels entrants / sortants.
- **API de enregistrement** – permet la lecture et l'enregistrements des événements.
- **API d'automatisation** – permet de configurer les exigences de communication et d'autorisation sécurisées/non sécurisées.

Définissez le protocole de transport (**HTTP** ou **HTTPS**) et la méthode d'authentification (**Aucune**, **Basic** ou **Digest**) pour chaque fonctionnalité. Créez jusqu'à cinq comptes d'utilisateur

(avec leur propre nom d'utilisateur et mot de passe) dans la configuration de l'**API HTTP** pour un contrôle d'accès détaillé des services et des fonctions.

Définissez les méthodes d'authentification pour les demandes à envoyer à l'interphone pour chaque service. Si l'authentification requise n'est pas exécutée, la demande sera rejetée. Les demandes sont authentifiées via un protocole d'authentification standard décrit par **RFC-2617**. Les trois méthodes d'authentification suivantes sont disponibles :

- **Aucune** – aucune authentification n'est requise. Dans ce cas, ce service est complètement non sécurisé sur le réseau local.
- **Basic** – l'authentification de base est requise selon **RFC-2617**. Dans ce cas, le service est protégé par un mot de passe transmis dans un format ouvert. Nous vous recommandons donc de combiner cette option avec **HTTPS** dans la mesure du possible.
- **Digest** – l'authentification Digest est requise selon **RFC-2617**. C'est l'option par défaut et la plus sécurisée des trois méthodes énumérées ci-dessus.

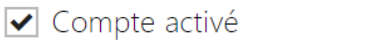
Référez vous au Manuel HTTP API pour découvrir les fonctionnalités et les détails de configuration.

Conseil

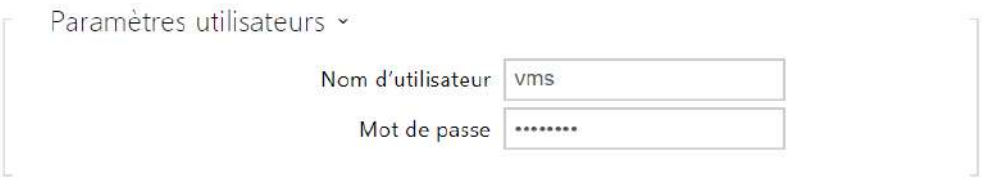
- Pour la fonction de Prévisualisation Vidéo sur le Téléphone IP Gigaset Maxwell 10, il est nécessaire (dans la section **HTTP API**) de passer l'**API de la Caméra** en **Non sécurisé** et le mode **d'Authentification** en **Aucune**.

Compte 1–5

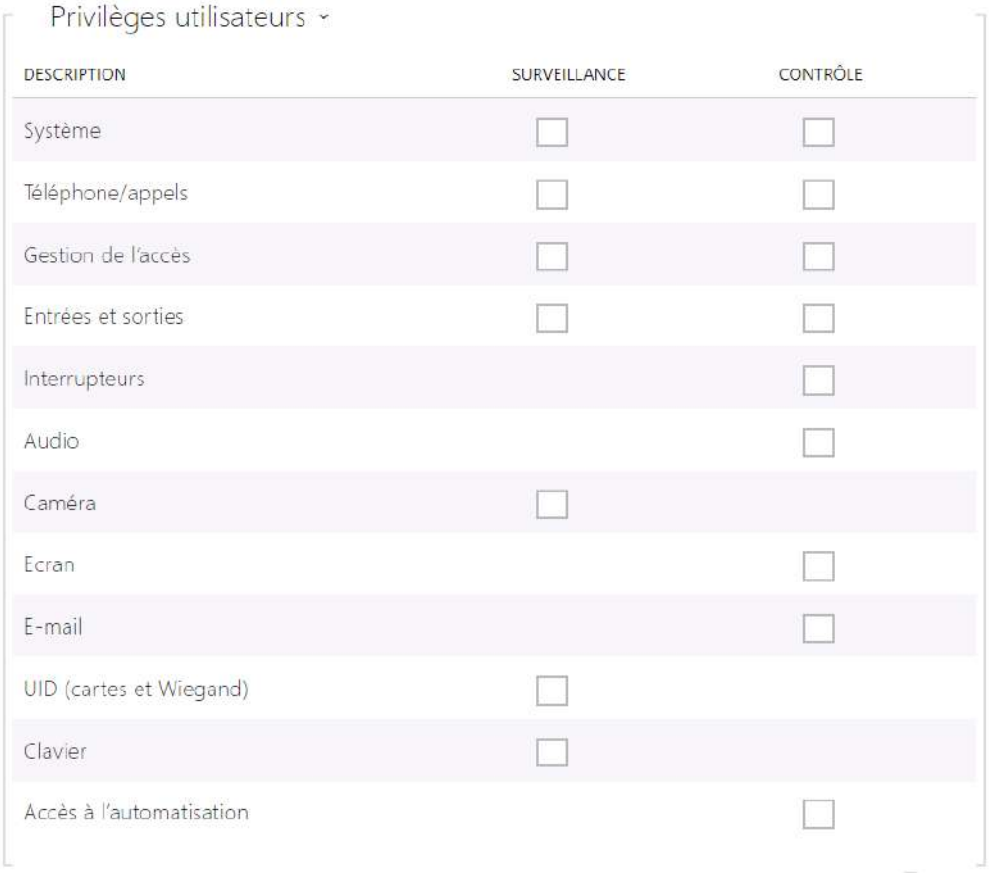
L’interphone 2N IP permet de gérer jusqu'à cinq comptes d'utilisateurs qui sont destinés à l'accès aux services **HTTP API**. Le compte d'utilisateur comprend le nom et le mot de passe de l'utilisateur ainsi qu'un tableau des droits d'accès de l'utilisateur aux différents services de **HTTP API**.



- **Compte activé** – autorise ce compte d’utilisateur.



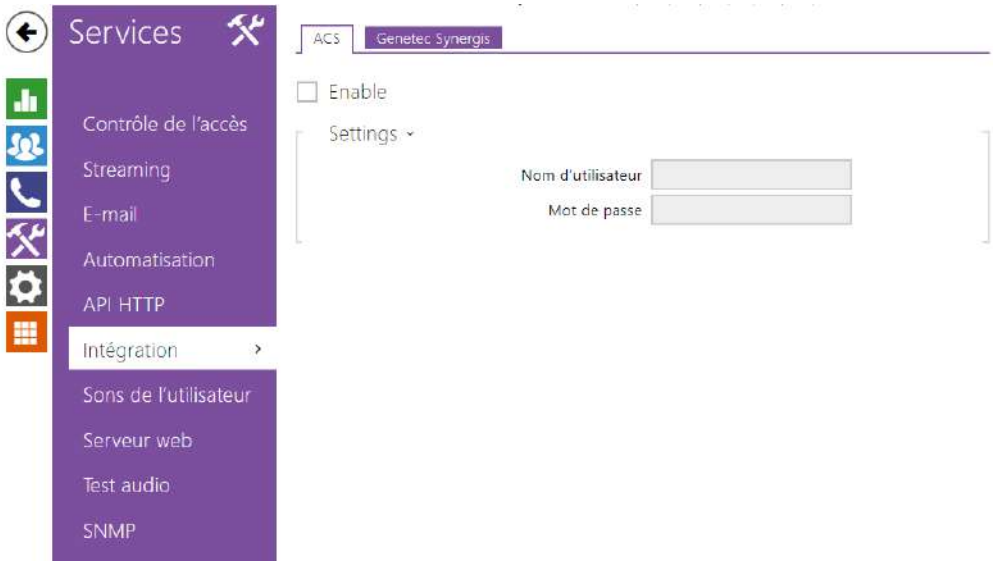
- **Nom d’utilisateur** – saisir le nom d’utilisateur pour l’authentification de HTTP API.
- **Mot de passe** – saisir le mot de passe d’authentification de HTTP API.



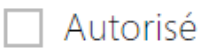
À l'aide du tableau des droits d'accès on peut gérer les privilèges du compte d'utilisateur pour les différents services.

5.4.6 Integration

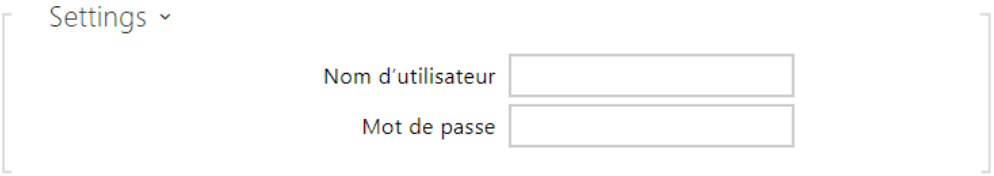
Le service Intégration permet à l'appareil de se connecter avec les systèmes de tierces parties.



Onglet ACS

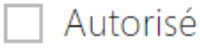


- **Autorisé** –autorise la fonction d'appel à Axis Camera Station (ACS). Un URI particulier est utilisé pour les appels sur ACS sous la forme vms : *.

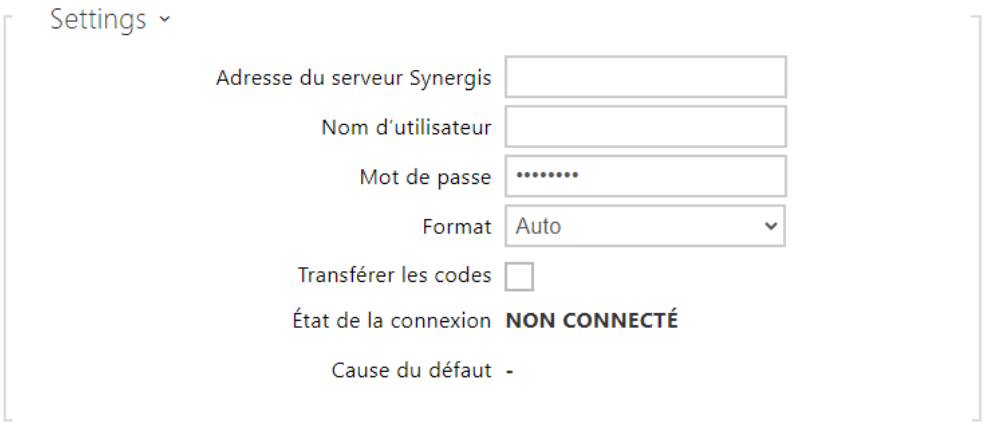


- **Nom d'utilisateur** – nom d'utilisateur pour l'authentification des appels à ACS.
- **Mot de passe** – mot de passe pour l'authentification des appels à ACS.

Onglet Genetec Synergis

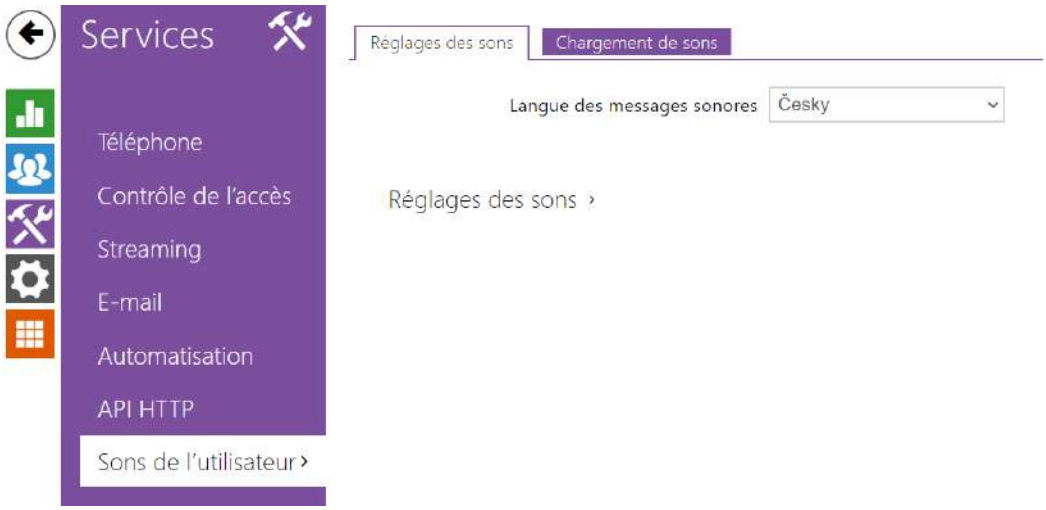


- **Autorisé – autorise la connexion avec le système de sécurité externe Genetec Synergis.**



- **Adresse du serveur Synergis** – adresse IP ou nom de domaine. du serveur Synergis.
- **Nom d'utilisateur** – nom d'utilisateur utilisé lors de l'authentification.
- **Mot de passe** – mot de passe utilisé lors de l'authentification.
- **Format** - format des codes envoyés.
- **Transmettre les codes** –configure s'il faut transmettre les codes demandés. Les codes peuvent avoir un maximum de 6 chiffres et il convient d'appuyer sur la touche de confirmation à la fin.

5.4.7 Sons Utilisateurs



Les **interphones IP 2N** fournissent une signalisation standard des états de fonctionnement par séquences de tonalités ; reportez-vous à la sous-section Signalisation des états de fonctionnement. Si les tonalités de signalisation standard ne répondent pas à vos exigences, vous pouvez les modifier et les personnaliser.

L'interphone vous permet de modifier la signalisation sonore pour les états suivants :

a. **Sonnerie avant de répondre à un appel**
b. **Sonnerie**

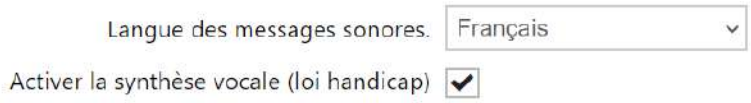
c. **Tonalité Correspondant occupé**
d. **Appel raccroché**
e. **Numéro invalide**
f. **Saisie invalide**
g. **Activation de l'interrupteur**

Vous pouvez soit mettre complètement en sourdine les sons mentionnés ci-dessus, les remplacer par l'un des dix sons prédéfinis, ou tout simplement enregistrer votre propre fichier son dans l'interphone. Le fichier son doit avoir le format WAV et utiliser le codage PCM avec une fréquence d'échantillonnage de 8/16 kHz et une résolution d'échantillonnage de 8/16 bits. Assurez-vous que la taille du fichier ne dépasse pas 256 Ko dans les **Interphones IP 2N** et 2048 kB dans le Haut-parleur **2N® SIP Horn**.

Fréquence	Bits d'échantillonnage	Durée du son	Qualité
16 kHz	16-bit	jusqu'à 8 s	1 (Top)
16 kHz	8-bit	jusqu'à 16 s	2
8 kHz	16-bit	jusqu'à 16 s	3 (combinaison non-recommandée)
8 kHz	8-bit	jusqu'à 32 s	4 (basse)

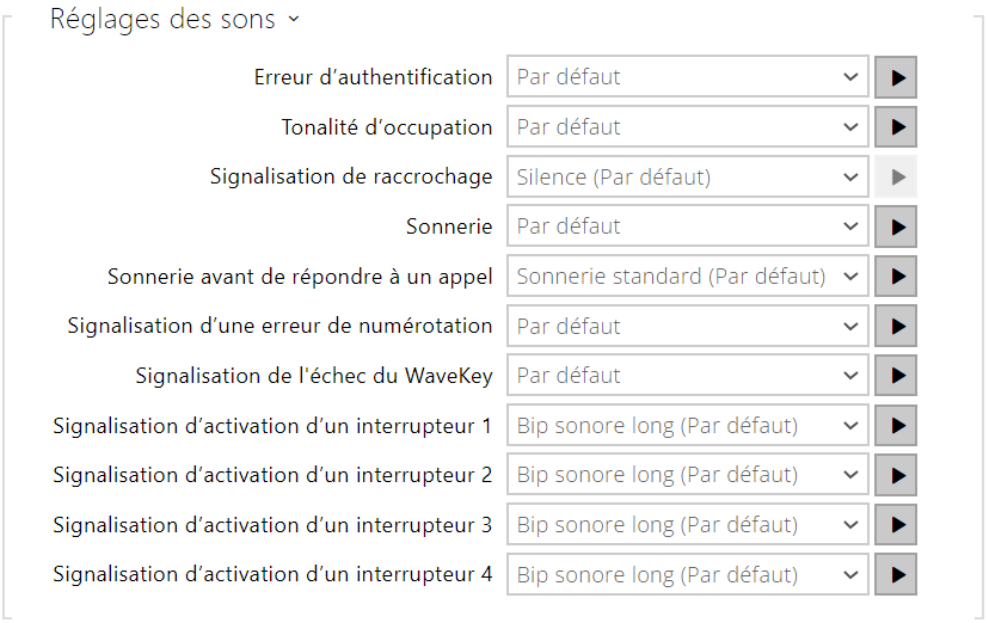
Vous pouvez également jouer les sons enregistrés via l'Automatisation à l'aide de l'action **PlayUserSound** et, en option, à l'aide du haut-parleur de l'interphone directement pendant l'appel.

Liste des Paramètres



- **Langue des messages sonores –** sélectionne la langue pour les messages sonores de l'intercom. Si un fichier pour lequel une traduction est disponible est remarqué pour l'événement donné, le message sera enregistré dans la langue choisie. S'il n'y a pas de traduction disponible, un son en anglais ou linguistiquement neutre sera enregistré.
- **Activer la synthèse vocale (loi handicap)** – Aux fins de conformité à la législation des régions francophones, il est possible d'activer la signalisation vocale en français pour les personnes à mobilité réduite pour les actions suivantes : établissement d'appel, connexion d'appel et déverrouillage des portes.

Classement des sons



- **Erreur d'authentification** – définit le son joué lorsque l'accès est refusé.
- **Tonalité d'occupation** – paramétrer le son de la tonalité d'occupation (joué si l'appelé est occupé).
- **Signalisation de raccrochage** – paramétrer le son à diffuser lorsqu'un appel prend fin.
- **Sonnerie** – paramétrer le son à jouer lorsque l'appelé est en train de sonner.La sonnerie PBX est préférée à la sonnerie de l'interphone définie ici.
- **Sonnerie avant de répondre à un appel** – paramétrer le son à diffuser avant de répondre à un appel entrant (sonnerie de l'interphone).
- **Signalisation d'une erreur de numérotation** – paramétrer le son à diffuser lorsqu'un bouton de numérotation rapide est appuyé mais que la position correspondante dans le répertoire téléphonique n'est pas programmée.
- **Signalisation de l'échec du WaveKey** – définit le son qui sera joué si aucun téléphone n'a ouvert la porte pendant la période de recherche.
- **Signalisation d'activation d'un interrupteur 1–4** – paramétrer le son à générer lorsqu'un interrupteur 1–4 est activé. Spécifiez les détails de signalisation pour chaque interrupteur; reportez-vous à la sous-section Interrupteurs.

Observation

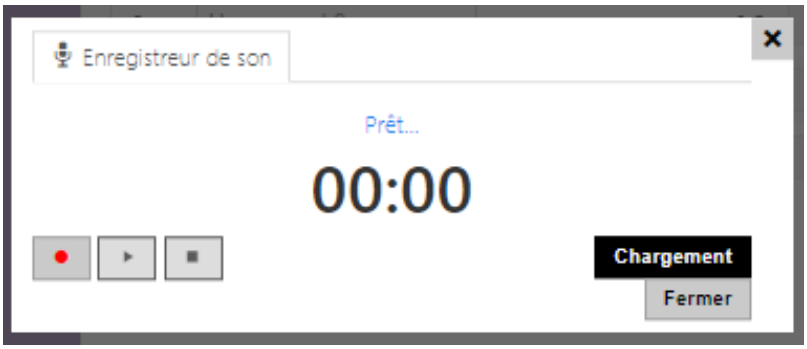
- Si le son attribué ne peut pas être lu, cela signigie soit que le son est réglé sur "Silence".

Téléchargement de sons

Vous pouvez enregistrer jusqu'à 10 fichiers son utilisateur dans l'interphone et leur attribuer un nom pour plus de commodité.

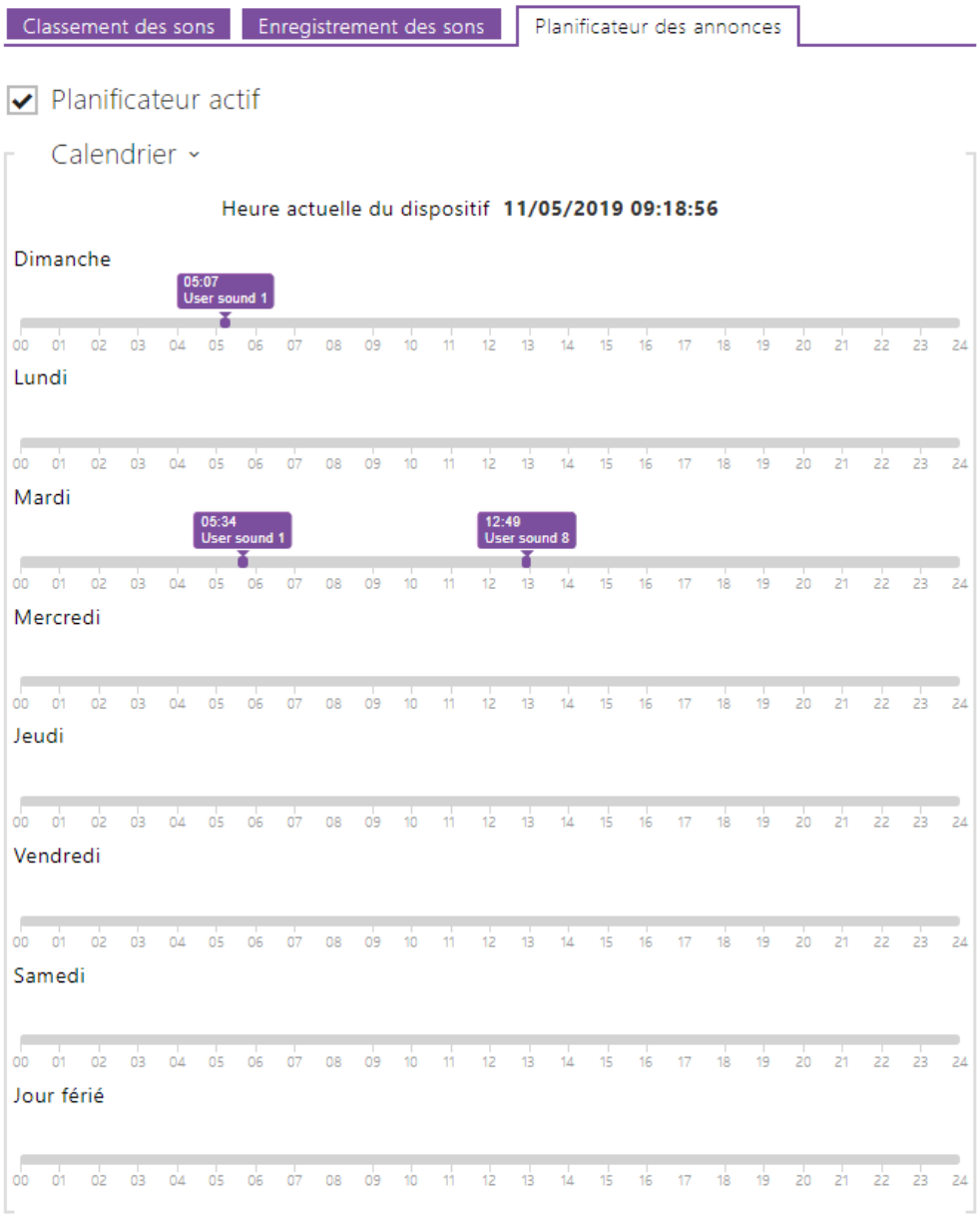
Appuyez sur pour télécharger un fichier son sur l'interphone. Sélectionnez un fichier sur votre PC via une fenêtre de dialogue et appuyez sur **Chargement**. Appuyez sur pour effacer un fichier. Appuyez sur pour rejouer le fichier son (localement sur votre PC). Appuyez sur pour enregistrer un fichier audio directement depuis le microphone de votre ordinateur.

Vous pouvez enregistrer un fichier son en utilisant le microphone de votre ordinateur. Appuyez sur pour démarrer l'enregistrement et sur pour le stopper. Appuyez sur pour jouer le son enregistré. Cliquez sur **Chargement** pour enregistrer le son dans l'Interphone.



Planificateur d'annonces

Le planificateur d'annonces vous aide à jouer des sons de manière récurrente à une heure prédéfinie. Vous pouvez définir des jours dans une semaine pendant lesquels le son doit être joué. Cliquez sur l'axe de temps du jour requis pour ajouter un son. Pendant l'ajout, définissez l'heure exacte, sélectionnez le son que vous souhaitez jouer et réglez le volume. L'onglet **Planificateur d'annonces** est seulement disponible sur les Haut-parleurs **2N SIP Audio**.



- **Planificateur actif** – activez la lecture des sons utilisateurs prédéfinis comme vous l'avez programmé.

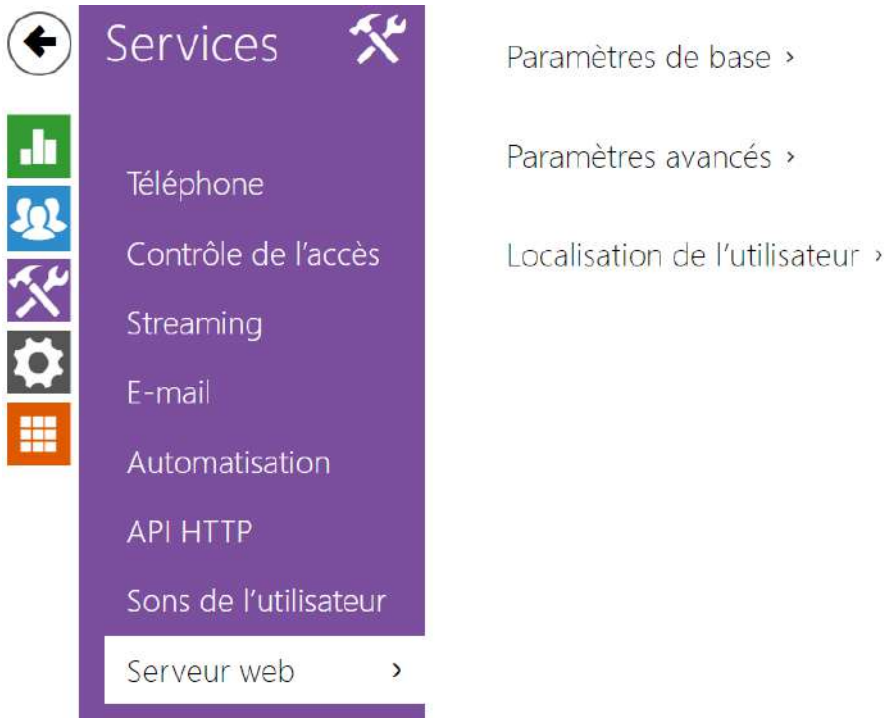
Conseil

- Référez vous à ce lien https://wiki.2n.cz/hip/inte/latest/en/10-media-applications/audacity pour plus de détails.

Note

- La fonction d'enregistrement de son n'est pas disponible dans les navigateurs qui ne prennent pas en charge la norme WebRTC (Internet Explorer, par exemple).

5.4.8 Serveur web



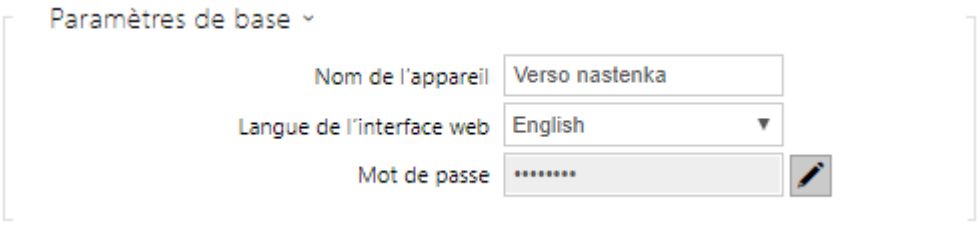
Vous pouvez configurer votre **interphone IP 2N** à l'aide d'un navigateur standard qui accède au serveur Web intégré. Utilisez le protocole **HTTPS** sécurisé pour la communication entre le navigateur et l'interphone. Après avoir accédé à l'interphone, entrez le nom d'utilisateur et le mot de passe. Le nom d'utilisateur et le mot de passe par défaut sont **admin** et **2n** respectivement. Nous vous recommandons de changer le mot de passe par défaut dès que possible.

La fonction Serveur Web est également utilisée par les fonctionnalités suivantes sur l'interphone :

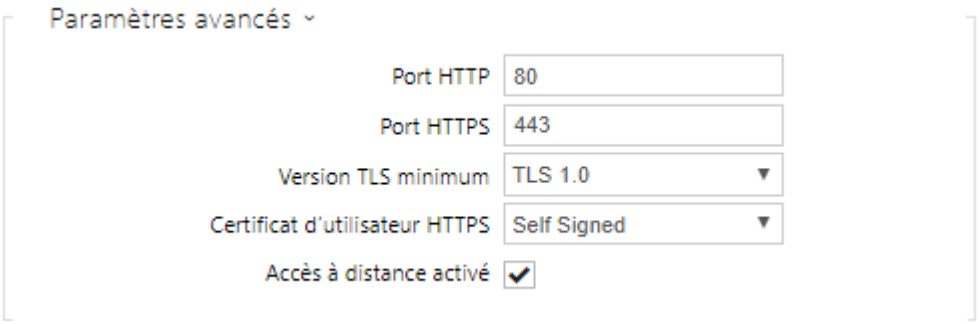
a. JPEG Snapshots Télécharger / vidéo MJPEG ; voir Streaming.
b. Protocole ONVIF pour le streaming vidéo, voir Streaming.
c. Commandes HTTP pour le contrôle des Interrupteurs, reportez-vous à la sous-section Interrupteur.
d. Event.HttpTrigger dans **Automatisation**, référez vous au Manuel concerné.

Le protocole HTTP non sécurisé peut être utilisé pour les cas de communication spéciaux.

Liste des Paramètres

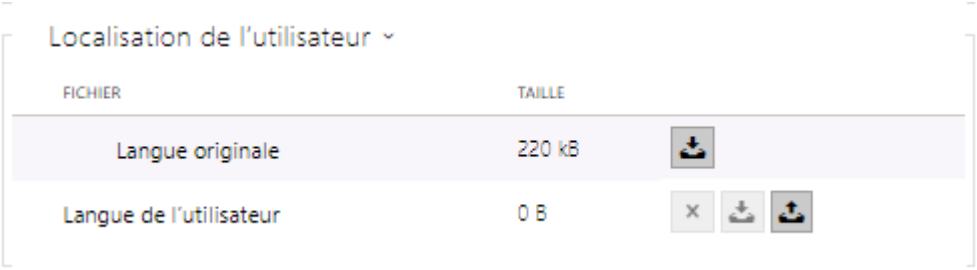


- **Nom de l’appareil** – définissez le nom de l'appareil à afficher dans le coin supérieur droit de l'interface Web, dans la fenêtre de connexion et dans d'autres applications si nécessaire (scanner réseau, etc.).
- **Langue de l’interface web** – paramétrez la langue de l’utilisateur pour la connexion au serveur web d’administration. Utiliser les boutons de la barre d’outils supérieure pour modifier la langue provisoirement.
- **Mot de passe** – paramétrez le mot de passe d’accès à l’interphone. Appuyez sur pour modifier le mot de passe. Le mot de passe composé de 8 caractères doit comporter au moins une lettre minuscule, une lettre majuscule et un chiffre.



- **Port HTTP** – paramétrez le port du serveur web pour la communication HTTP. Le paramétrage du port ne sera appliqué qu'après le redémarrage de l'Interphone.
- **Port HTTPS** – il définit le port de communication du serveur Web pour la communication à l’aide du protocole HTTPS sécurisé. Le paramétrage du port ne sera appliqué qu'après le redémarrage de l'Interphone.
- **Version TLS minimum** – définissez la version TLS minimale, autorisée pour la connexion à l’appareil.
- **Certificat d’utilisateur HTTPS** – spécifiez le certificat d’utilisateur et la clé privée pour le serveur HTTP du dispositif – cryptage de communication du navigateur web de l’utilisateur. Sélectionner l’un des trois jeux de certificats d’utilisateur et de clés privées (se

reporter à la partie Certificats) ou conserver le paramètre **SelfSigned**, grâce auquel le certificat automatiquement généré lors du premier allumage du dispositif est utilisé.
- **Accès à distance activé** – activez l'accès à distance au serveur web du dispositif à partir d'adresses IP Off-LAN.

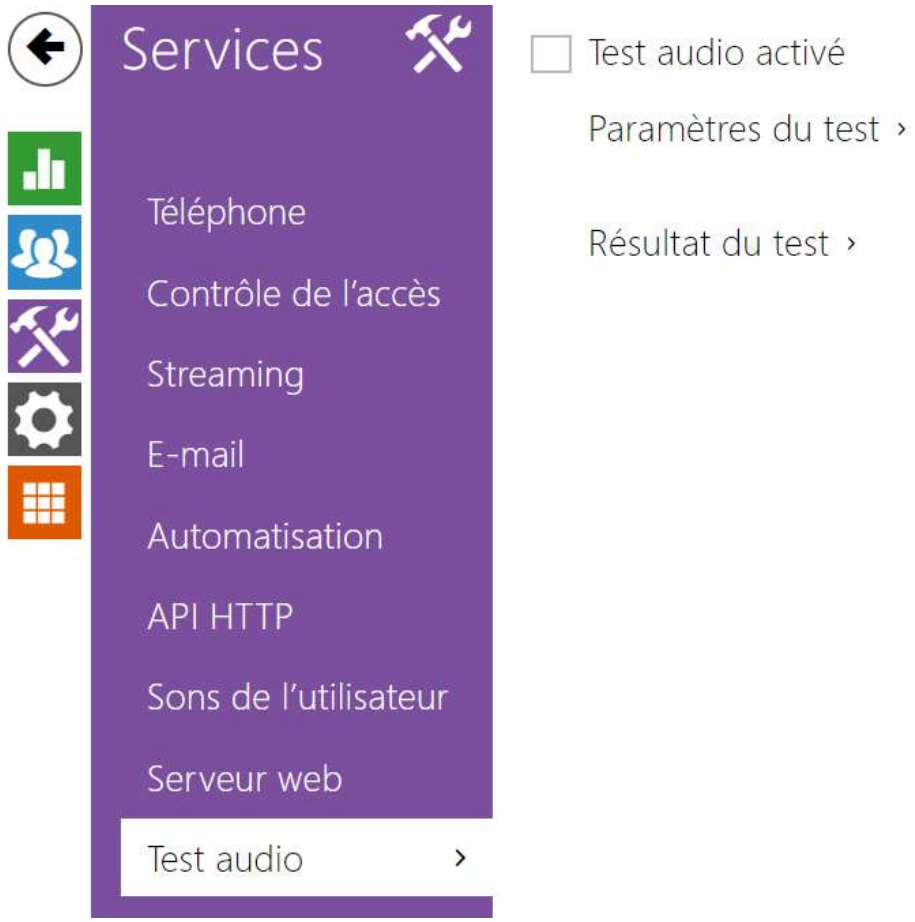


- **Langue originale** – téléchargez le fichier original contenant tous les textes de l'interface utilisateur en anglais. Le format de fichier est XML; voir ci-dessous.
- **Langue de l'utilisateur** – enregistrez, chargez et supprimez, si nécessaire, un fichier utilisateur contenant vos propres traductions de texte d'interface utilisateur.

```
<?xml version="1.0" encoding="UTF-8"?>
<strings language="English" languageshort="EN">
  <!-- Global enums-->
  <s id="enum/error/1">Invalid value!</s>
  <s id="enum/bool_yesno/0">NO</s>
  <s id="enum/bool_yesno/1">YES</s>
  <s id="enum/bool_user_state/0">ACTIVE</s>
  <s id="enum/bool_user_state/1">INACTIVE</s>
  <s id="enum/bool_profile_state/0">ACTIVE</s>
  <s id="enum/bool_profile_state/1">INACTIVE</s>
  ..
  ..
  ..
</strings>
```

Pendant la traduction, modifiez uniquement la valeur des éléments **<s>**. Ne modifiez pas les valeurs **id**. Le nom de langue spécifié par l'attribut de langue de l'élément <strings> sera disponible dans les sélections du paramètre de langue de l'interface Web. L'abréviation du nom de langue spécifié par l'attribut **languageshort** de l'élément **<strings>** sera incluse dans la liste des langues située dans le coin supérieur droit de la fenêtre et sera utilisée pour un changement rapide de langue.

5.4.9 Test audio

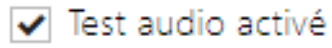


Les **interphones IP 2N** vous permettent d'effectuer des tests périodiques du haut-parleur et du microphone intégrés. À des fins de test, le haut-parleur intégré génère un ou plusieurs bips brefs. Le microphone intégré reçoit la tonalité générée et le test réussit si la tonalité est détectée correctement. Le test prend environ 4 secondes. Si le test échoue (ce qui peut être dû à un niveau de bruit ambiant extrême, par exemple), un nouveau test est effectué en 10 minutes. Le résultat du dernier test peut être affiché dans l'interface de confirmation interphone ou traité par l'interface d'**Automatisation**.

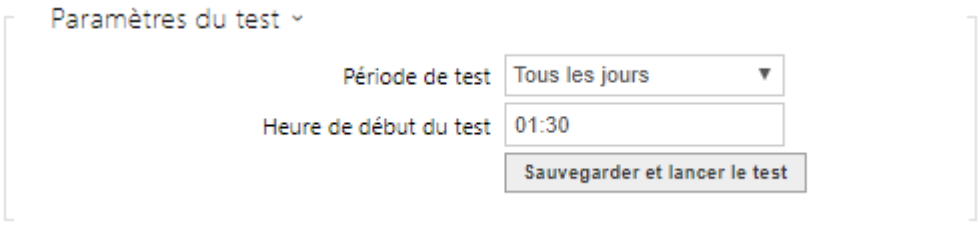
Note

- *Un appel est en cours au début du test audio, le test audio est mis en attente jusqu'à la fin de l'appel. Le test audio sera effectué dès que l'appel sera terminé.*

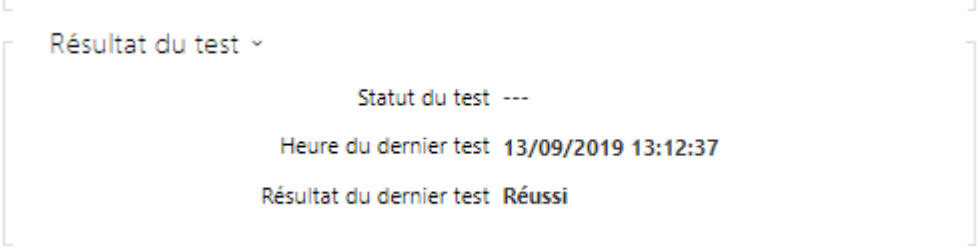
Liste des Paramètres



- **Test audio activé** – activez l'exécution automatique du test audio.

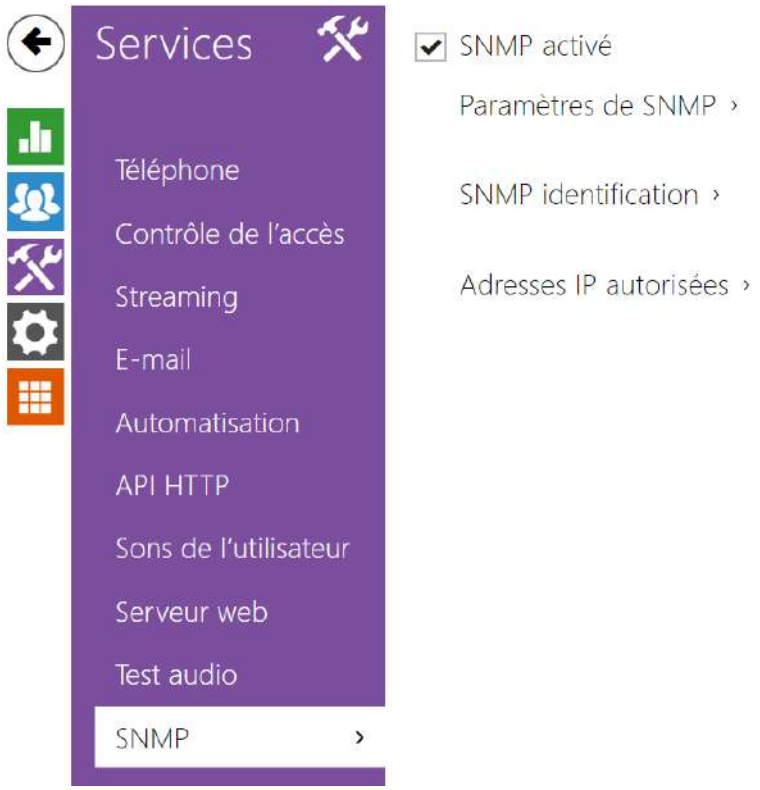


- **Période de test** – il permet de définir la période d'exécution du test. Le test peut être exécuté automatiquement une fois par jour ou une fois par semaine.
- **Heure de début du test** – il permet de définir l'heure à laquelle le test doit être régulièrement effectué. Vous pouvez régler l'heure au format HH : MM. Nous vous recommandons de régler l'heure à laquelle une utilisation minimale de l'interphone est attendue.
- **Sauvegarder et lancer le test** – appuyez sur le bouton pour démarrer et enregistrer le test immédiatement, quels que soient les paramètres actuels.



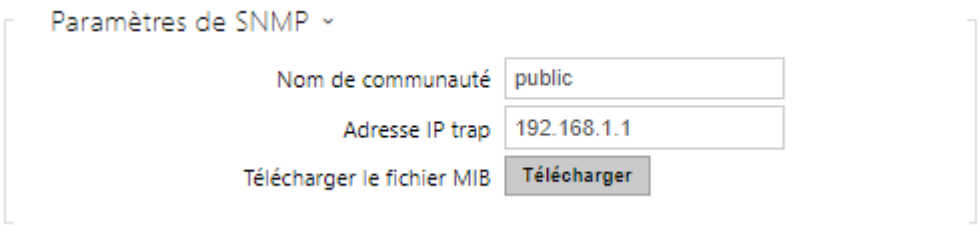
- **Statut du test** – ce paramètre affiche le statut actuel du test.
- **Heure du dernier test** – ce paramètre affiche l'heure du dernier test effectué.
- **Résultat du dernier test** – ce paramètre affiche le résultat du dernier test effectué.

5.4.10 SNMP



Les **interphones IP 2N** intègrent une fonctionnalité de supervision d'interphone à distance via le protocole SNMP. L'agent SNMP intégré devient disponible lorsque la clé de licence Gold ou Integration améliorée est ajoutée. Les interphones supportent la version 2c du SNMP.

Liste des Paramètres

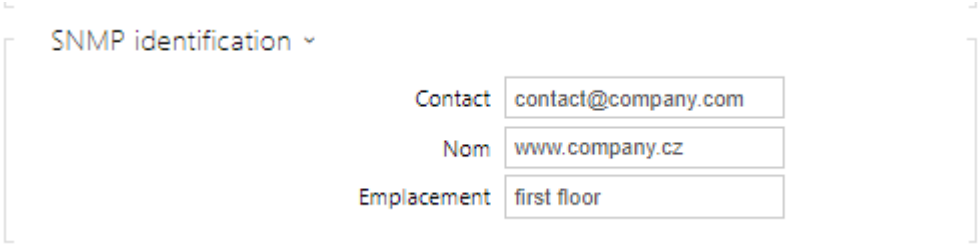


- **Nom de communauté** – chaîne de texte représentant la clé d'accès aux objets de la table MIB.
- **Adresse IP Concept d'interruptions** – il s'agit de l'adresse IP à laquelle les concepts d'interruptions SNMP sont envoyés.

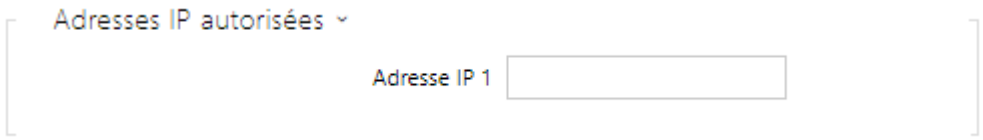
Note

- Les concepts d'interruptions ne sont pas supportés sur la version actuel de l'interphone. Les **Interphones IP 2N** fonctionnent sur le principe demande – messages de réponse.

- **Télécharger le fichier MIB** – téléchargez la définition MIB actuelle à partir d'un périphérique.



- **Contact** – permet d’entrer le contact de l’administrateur du dispositif (par ex. nom, e-mail, etc.).
- **Nom** – entrez le nom du dispositif.
- **Emplacement** – permet d’entrer la description de l’emplacement du dispositif (par ex. 1er étage).

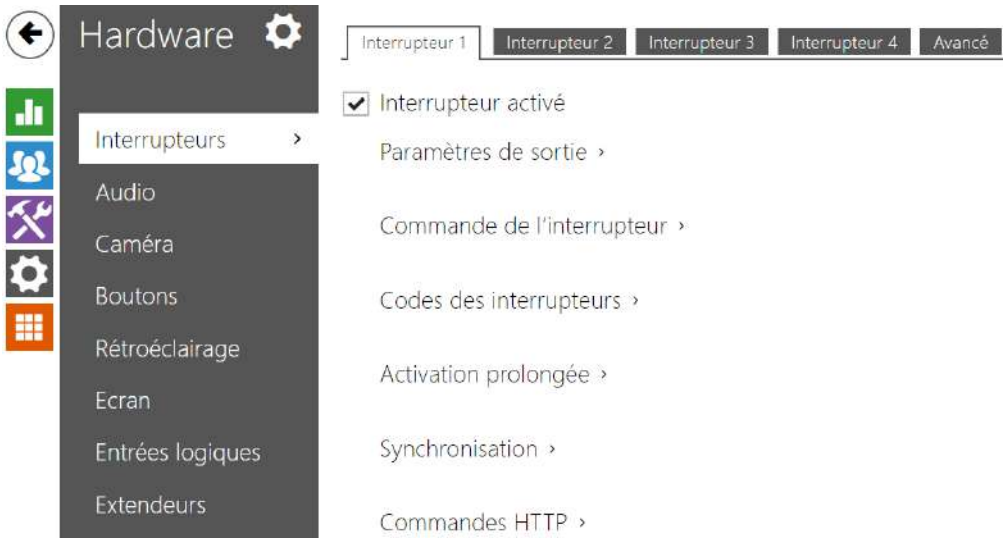


- **Adresse IP** – entrez jusqu'à 4 adresses IP valides pour l'accès à l'agent SNMP afin de bloquer l'accès à partir d'autres adresses. Si le champ est vide, vous pouvez accéder au périphérique à partir de n'importe quelle adresse IP.

5.5 Hardware

Voici les onglets que vous pouvez trouver dans cette section :

5.5.1 Interrupteurs



Les Interrupteurs permettent un contrôle très souple et efficace des périphériques liés à l'interphone tels que les serrures électriques, l'éclairage, des dispositifs de signalisation, de sonnerie...etc.

Les **Interphones IP 2N** vous permettent de configurer jusqu'à 4 interrupteurs indépendants selon les modèles.

Un interrupteur peut être activé par :

- la saisie d'un code valide sur le clavier de l'Interphone ou bien la réception d'une trame DTMF valide pendant un appel,
- le passage d'une carte valide sur le lecteur RFID de l'interphone,
- un délai prédéfini après l'activation d'un premier interrupteur (ex : option SAS),
- un appel entrant ou sortant,
- un bouton d'appel pressé *),
- le passage dans une certaine plage horaire*),
- la réception d'une commande http depuis un autre dispositif IP *),
- l'interface d'automatisation en utilisant l'action **"ActivateSwitch"** *).

L'activation de l'interrupteur peut être bloquée sur certaines plages horaires spécifiques si nécessaire.

> **Note**
>
> - Les options marquées d'un *) nécessitent leurs licences actives respectives..

Verrouillage et pression de l'interrupteur
Les conditions de commutation des interrupteurs peuvent être modifiées à l'aide de deux fonctions. Il s'agit des fonctions de verrouillage et d'enclenchement de l'interrupteur. Si l'interrupteur est verrouillé, il se trouve en permanence « désactivé » et ne peut être manipulé tant qu'il reste verrouillé (la priorité du verrouillage est supérieure à celle de l'enclenchement - si l'interrupteur est verrouillé et enclenché simultanément, le verrouillage l'emporte). Si l'interrupteur est enclenché, il se trouve en permanence « commuté » et ne peut être manipulé tant qu'il est enclenché.
Le verrouillage et l'enclenchement peuvent être entre autre gérés avec les profils horaires.Il n'est pas recommandé d'utiliser un profil horaire aux fins de verrouillage (la commande de verrouillage du profil horaire existe dans l'équipement du fait de la compatibilité dédiée), l'interrupteur étant déverrouillé une fois écoulé le délai défini, même si l'interrupteur a été manuellement verrouillé.
Le paramètre **Fonctionnement actuel de l'interrupteur** affiche la combinaison réelle de ces deux fonctions (Normal - verrouillage et enclenchement désactivés ; Enclenchement - verrouillage désactivé et enclenchement activé ; Verrouillé - verrouillage activé, les réglages de l'enclenchement ne sont pas pris en compte).
Une fois redémarré, l'équipement vérifie si le verrouillage ou l'enclenchement sont impactés par le profil horaire. Si tel est le cas, la fonction correspondante est activée ou désactivée eu égard au paramétrage du profil horaire. Si tel n'est pas le cas, le dernier état de verrouillage avant l'arrêt de l'équipement est défini, ou l'enclenchement est défini sur l'état inactif (l'interrupteur n'est pas enclenché).

Si un interrupteur s'active, vous pouvez :

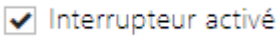
- activer n'importe quelle sortie de l'Interphone (Relais, Sortie active)
- activer la sortie qui contrôle le **Relais de sécurité de l'Interphone**
- envoyer une commande http vers un autre appareil IP ou bien un autre Interphone IP 2N

Les Interrupteurs peuvent fonctionner en mode Monostable ou Bistable. En mode monostable, il sera automatiquement désactivé après une temporisation programmable. En mode Bistable, l'interrupteur s'activera et aura besoin d'une seconde activation pour revenir en mode non actif.

L'interrupteur signal sont état par :

- Un bip programmable ou un son prédéfini et personnalisable.
- Un indicateur LED, si disponible selon le modèle de l'Interphone.
- Un pictogramme d'ouverture de porte si disponible selon le modèle de l'Interphone.

Interrupteurs 1–4



- **Interrupteur activé** – activez / désactivez l'interrupteur de manière général. Lorsqu'il est désactivé, l'interrupteur ne peut être activé par aucun des codes disponibles (y compris les codes des utilisateurs), bouton d'appel ou de numérotation rapide.

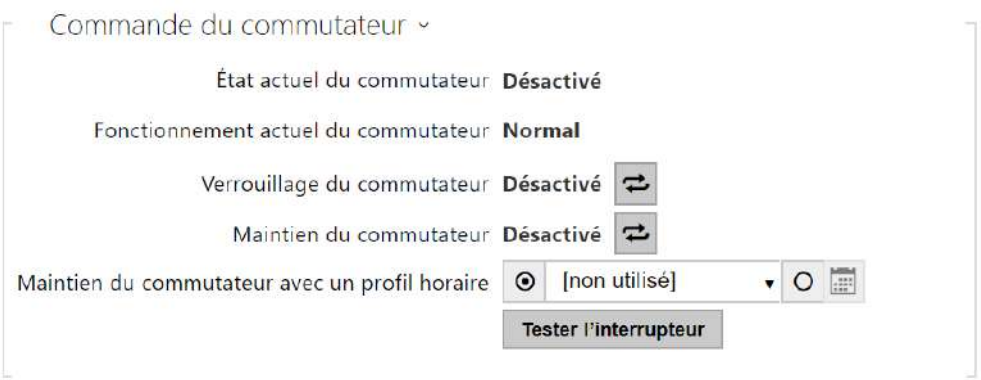
- **Modes des interrupteurs** – paramétrez le mode monostable/bistable pour l'interrupteur. En mode monostable, l'interrupteur est automatiquement désactivé après le temps de commutation réglé. En mode bistable, l'interrupteur est activé par la première activation et désactivé par la deuxième.
- **Durée d'enclenchement** – paramétrez la durée de temporisation pour un interrupteur monostable. Cette valeur n'est pas appliquée en mode bistable.
- **Sortie contrôlée** – attribuez une sortie électrique à l'interrupteur. Sélectionnez l'une des sorties disponibles sur le dispositif : relais, sortie 12V, sortie relais supplémentaire (module E/S). En sélectionnant **Aucun**, l'interrupteur ne contrôlera aucune sortie électrique, mais pourra contrôler des équipements tiers via des commandes HTTP.
- **Type de sortie** – si le **Relais de sécurité** est utilisé, régler le type de sortie sur **Sécurité**. En mode **Sécurité**, la sortie fonctionne en mode inversé, c.-à-d. qu'elle reste fermée et contrôle le **Relais de sécurité IP 2N®** en utilisant une séquence d'impulsions électriques spécifiques. Si vous utilisez le mode inversé (c'est-à-dire que la porte est verrouillée lorsque la tension est appliquée), définissez le type de sortie **inversée**. Si plusieurs interrupteurs sont réglés sur la même sortie mais ont des types différents de sortie, ils seront commandés conformément à la priorité suivante : 1. sécurité, 2. inverse, 3. normal.

Note

- ***2N® IP Vario*** *– assurez-vous de régler l'alimentation interne et le relais de l'interrupteur sur la configuration.* ***2N® IP Force*** *– le relais de sécurité est connecté au + et – du terminal PORTE.*
- *Une valeur d'activation de l'interrupteur supérieure à 1 s peut être définie pour le type de sortie de* ***sécurité****. Une valeur égale ou supérieure à 0,1 s peut être définie pour les types de sortie* ***normaux*** *et* ***inversés****.*

Sécurité

- La sortie 12V est utilisée pour connecter la serrure. Toutefois, si l'unité (2N IP Interkom, 2N Access Unit) se trouve à un endroit (coque du bâtiment) où il existe un risque d'intrusion dans l'établissement, il est fortement recommandé d'utiliser le Relais de sécurité 2N (Part No. 9159010) pour sécuriser l'installation au maximum.

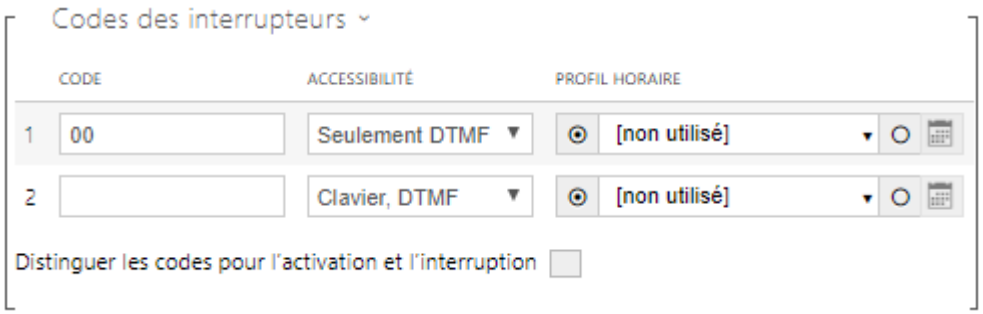


- **État actuel du commutateur** – affiche l'état actuel du commutateur (activé ou désactivé).
- **Fonctionnement actuel du commutateur** – Affiche le fonctionnement actuel du commutateur.
  - **Normal** : le commutateur n'est pas verrouillé ni maintenu.
  - **Maintenu** : le commutateur est maintenu mais pas verrouillé.
  - **Verrouillé** : le commutateur est verrouillé (dans ce cas, le verrouillage prime sur le maintien).
- **Verrouillage du commutateur** – activé : le commutateur est en permanence en position 0 et ne peut pas être commandé tant qu'il n'est pas déverrouillé. Désactivé : le commutateur n'est pas verrouillé.

- **Maintien du commutateur** – activé : le commutateur est en permanence en position 0 et ne peut pas être commandé tant qu'il n'est pas déverrouillé. Désactivé : le commutateur n'est pas verrouillé.
- **Maintien du commutateur avec un profil horaire** – permet d'attribuer un profil horaire prédéfini à l'interrupteur ou de définir manuellement un profil horaire permettant à l'interrupteur de se fermer. Si le profil horaire attribué n'est pas actif, il est alors possible d'activer le commutateur en apposant une carte RFID valide, en passant un appel, en entrant un code ou en utilisant le bouton de numérotation rapide.
- **Bouton "Tester l'interrupteur"** – activez l'interrupteur manuellement pour tester son bon fonctionnement. Ex : activation d'une serrure électrique ou d'un autre appareil connecté.

Observation

- Si l'interrupteur est verrouillé et que l'équipement est éteint puis rallumé, l'interrupteur restera verrouillé après la mise sous tension de l'équipement. L'interrupteur se comporte de la même manière s'il est désactivé puis activé.
- Si l'interrupteur est enclenché et que l'équipement est éteint puis rallumé, l'interrupteur ne sera pas enclenché après la mise sous tension. L'interrupteur n'est enclenché après la mise sous tension de l'équipement que si le profil horaire d'enclenchement de l'interrupteur est paramétré et que ce profil est actif au moment de la mise sous tension de l'équipement. L'interrupteur se comporte de la même manière s'il est désactivé puis activé.



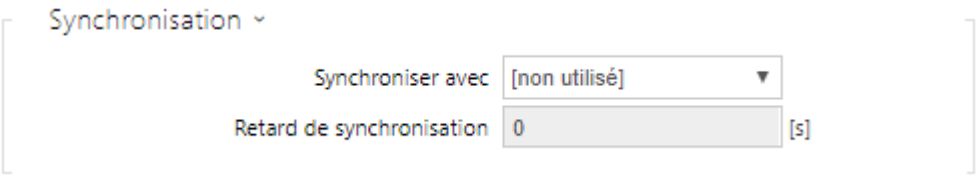
Le tableau ci-dessus comprend une liste de codes universels qui vous permettent d'activer les interrupteurs à partir du clavier du téléphone ou de l'interphone. Vous pouvez définir jusqu'à 10 codes universels pour chaque interrupteurs (en fonction du modèle d'interphone utilisé).

- **Code** – il permet d'entrer un code numérique pour activer l'interrupteur. Le code doit contenir au moins deux caractères pour déverrouiller la porte en utilisant le clavier de l'interphone et au moins un caractère pour déverrouiller la porte en utilisant une trame DTMF depuis le clavier du téléphone. Nous recommandons d'utiliser au moins 4 caractères. Les codes 00 et 11 ne sont pas acceptés depuis le clavier numérique, ils sont réservés à l'ouverture de porte par DTMF. Pour ce code, vous devez confirmer le code avec la touche *. Les codes peuvent contenir au maximum 16 caractères.
- **Accessiblité** – bloquez la saisie du code d'activation de l'interrupteur sur le clavier numérique de l'interphone ou sur votre téléphone.
- **Profil horaire** – attribuez un profil temporel au code de l'interrupteur pour contrôler sa validité.
- **Distinguer les codes pour l'activation et l'interruption** – définissez un mode de code d'interrupteur dans lequel les codes impairs (1, 3 ….) sont utilisés pour l'activation de l'interrupteur et les codes pairs (2, 4 …) servent à la désactivation de l'interrupteur. Ce mode ne peut être utilisé que si l'interrupteur est réglé sur le mode bistable.

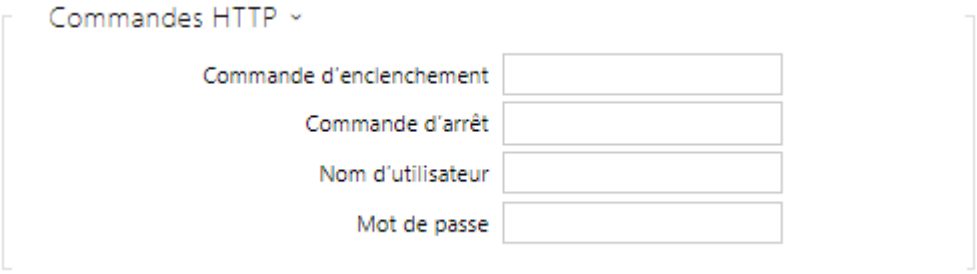
- **Activation par appel** – activez l'activation de l'interrupteur par un appel sortant, par exemple. Pendant un appel sortant, le commutateur est activé après la réception du message SIP 180. Dans le cas du mode bistable de l'interrupteur, l'interrupteur est actif pendant toute la durée de l'appel. Dans le cas du mode monostable, l'interrupteur est activé au début de l'appel et désactivé après la période de temporisation définie.
- **Activation par bouton de numérotation rapide** – attribuez à l'interrupteur un bouton de numérotation rapide. L'interrupteur est activé à chaque fois que le bouton est pressé.

Note

- *L'activation de l'interrupteur par un bouton d'appel est disponible avec la licence Gold.*



- **Synchroniser avec** – paramétrez la synchronisation de l'interrupteur pour activer automatiquement un autre interrupteur après un délai prédéfini. Déterminez le délai dans le paramètre de **Délai de synchronisation**.
- **Délai de synchronisation** – définissz l'intervalle de temps entre l'activations synchronisées de deux interrupteurs. Le paramètre ne sera pas appliqué si la fonction **Synchroniser** avec est désactivée.



- **Commande d'enclenchement** – paramétrez la commande http à envoyer vers un dispositif tiers (Web Relais, Haut-parleur SIP 2N, autres Interphones...etc.) lors de l'activation de l'interrupteur. La commande est envoyée via HTTP (demande GET). La commande doit être sous ce format http://ip_adresse/chemin. Par exemple http://192.168.1.50/relay1=on.
- **Commande d'arrêt** – paramétrez la commande http à envoyer vers un dispositif tiers (Web Relais, Haut-parleur SIP 2N, autres Interphones...etc.) lors de la désactivation de l'interrupteur. La commande est envoyée via HTTP (demande GET). La commande doit être sous ce format : http://ip_adresse/chemin. Par exemple http://192.168.1.50/relay1=off.
- **Nom d'utilisateur** – saisissez le nom d'utilisateur pour l'authentification du dispositif externe (relais WEB, par exemple). Ce paramètre est uniquement obligatoire si le dispositif externe nécessite une authentification.
- **Mot de passe** – saisissez le mot de passe d'authentification du dispositif externe (relais WEB, par exemple). Ce paramètre est uniquement obligatoire si le dispositif externe nécessite une authentification.

Conseil

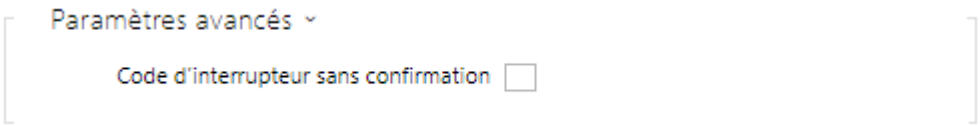
Les commandes HTTP n'ajoutent pas de codage d'URL. Si, par exemple, vous entrez http://10.27.24.6/message.cgi?action=9%3A%2F, voici ce qui est envoyé :http://10.27.24.6/message.cgi?action=9%3A%2F.
Pour inclure le codage d'URL, entrez, par exemple : http://10.27.24.6/message.cgi?action=9%253A%252F et voici ce qui sera envoyé : http://10.27.24.6/message.cgi?action=9%253A%252F.

Conseil

Avec le relais IP déporté 2N, **référence : 9137410E**, les commandes suivantes sont utilisées :
Activer l'interrupteur – http://ip_address/state.xml?relayState=1 (ex : http://192.168.1.10/state.xml?relayState=1)
Pour activer l'interrupteur pendant une durée prédéfinie (la valeur par défaut est 1,5 s) – http://ip_address/state.xml?relayState=2 (ex : http://192.168.1.10/state.xml?relayState=2)
Pour désactiver l'interrupteur – http://ip_address/state.xml?relayState=0 (ex : http://192.168.1.10/state.xml?relayState=0)

Avec le relais IP déporté 2N, **référence 9137411E**, les commandes suivantes sont utilisées (remplacez le symbole X par le numéro de relais)
Activer l'interrupteur – http://ip_address/state.xml?relayState=1 (ex : http://192.168.1.10/state.xml?relayState=1)
Pour activer l'interrupteur pendant une durée prédéfinie (la valeur par défaut est 1,5 s) – http://ip_address/state.xml?relayXState=2 (ex : http://192.168.1.10/state.xml?relay1State=2)
Pour désactiver l'interrupteur – http://ip_address/state.xml?relayXState=0 (ex : http://192.168.1.10/state.xml?relay1State=0)

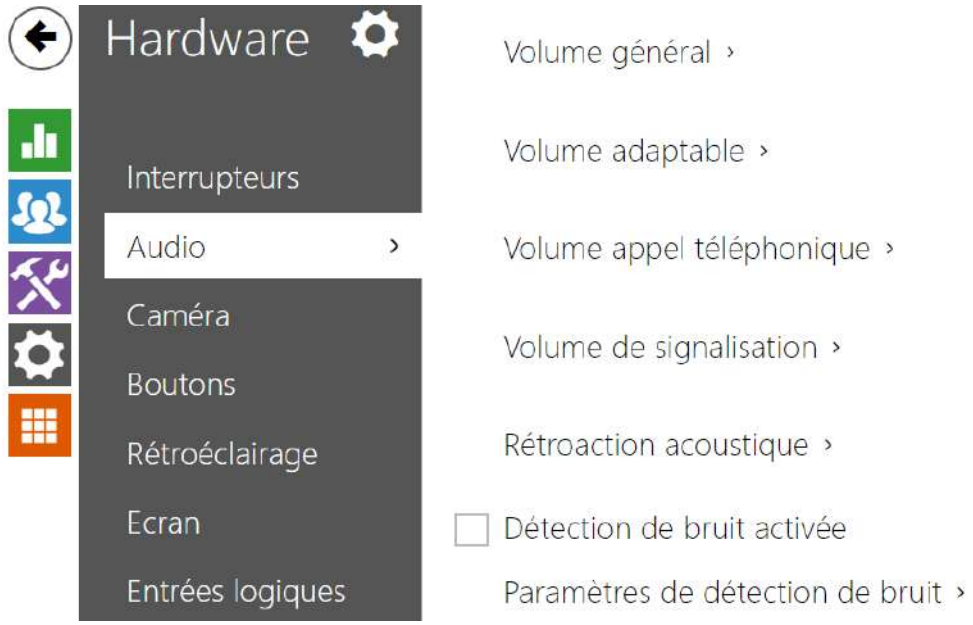
Avancé



- **Code d'interrupteur sans confirmation** – activez l'option pour activer le premier code de l'interrupteur répertorié à partir du téléphone sans confirmation avec *. Lorsque cette case est cochée, le premier code ne nécessite pas de confirmation par *. Ce paramètre ne s'applique pas aux autres codes d'interrupteur répertoriés et à l'activation via le clavier numérique, ceux-ci doivent toujours être confirmés par *. Le code d'interrupteur Legacy vous permet de conserver la compatibilité avec les modèles d'interphone 2N antérieurs. Dans le cas d'un mode bistable d'interrupteur, l'interrupteur est actif pendant toute la durée de l'appel.

- **Alimentation maximale sortie 1** – définit la valeur maximale de la puissance de la sortie 1.

5.5.2 Audio

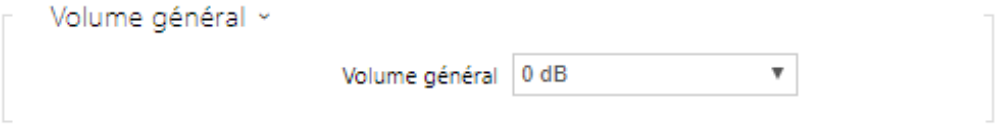


Tous les modèles **d'interphone IP 2N** sont équipés d'une sortie haut-parleur ou d'un amplificateur de puissance à laquelle un haut-parleur externe peut être connecté. Définissez le contrôle du volume des appels téléphoniques et des états dans cette section de configuration. Définissez le **Volume général** pour contrôler le volume principal de l'appareil: volume des appels, tonalités de signalisation...etc. Réglez ce paramètre en fonction du niveau de bruit ambiant. Si le niveau de bruit n'est pas constant, utilisez le mode adaptable pour augmenter le volume principal temporairement en fonction du niveau de bruit ambiant.

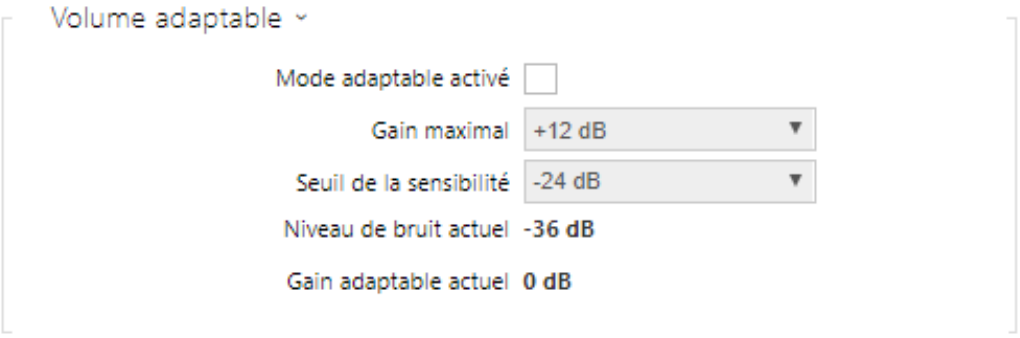
Modèles	Volume général
IP Style	−12 dB .. +8 dB (2 x 4 W)
IP Vario	−10 db .. +0 dB (150 mW)
Force/Safety 1W	−12 dB .. +6 dB (1 W)
Force/Safety 10W	−12 dB .. +20 dB (10 W)
IP Uni	−12 dB .. +6 dB (1 W)
IP Verso	−8 dB .. +8 dB (2 W)
IP Solo	−8 dB .. +4 dB (2 W)

Modèles	Volume général
IP Base	−8 dB .. +8 dB (2 W)
Audio/Video Kit	−10 dB .. +10 dB
SIP Speaker	−10 dB .. +10 dB
SIP Speaker Horn	−16 dB .. +16 dB

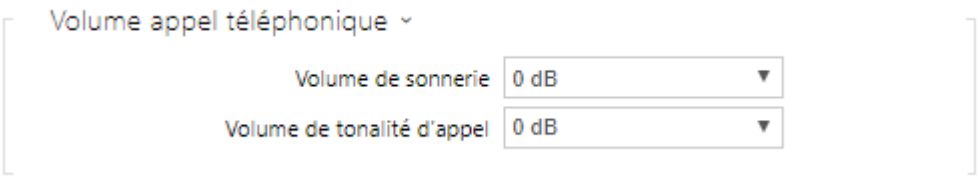
Liste des paramètres



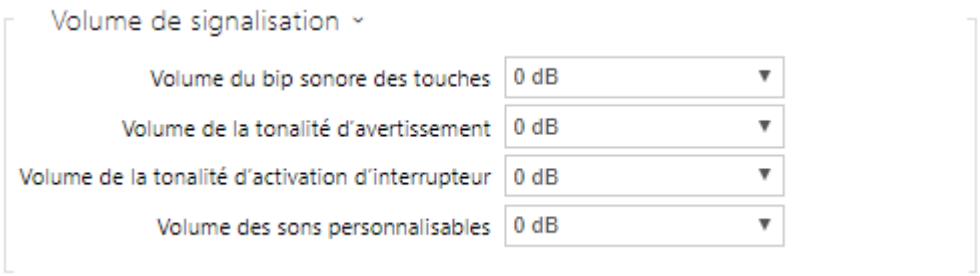
- **Volume général** – paramétrez le volume général pour tout le système. Ce paramètre affecte le volume des appels téléphoniques et de toutes les tonalités de signalisation.



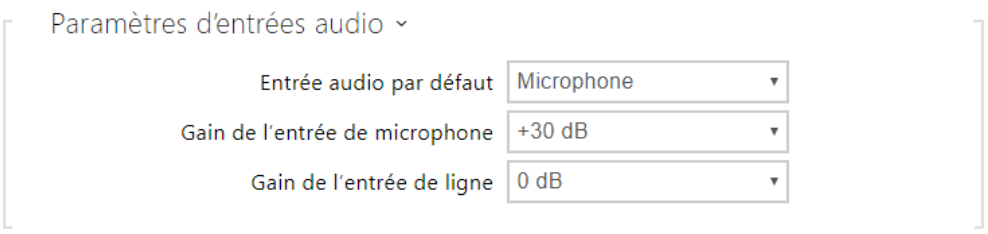
- **Volume adaptable** – activez le mode de volume adaptable avec lequel le volume du haut-parleur est ajusté automatiquement en fonction du niveau de bruit sur le site où est installé l'interphone.
- **Gain maximal** – réglez le gain maximum à appliquer au volume principal en mode adaptable.
- **Seuil sensibilité** – réglez le seuil de bruit ambiant auquel le gain adaptable est appliqué.
- **Niveau de bruit** – affiche le niveau de bruit ambiant en temps réel.
- **Gain adaptable actuel** – affiche le gain adaptable en temps réel du volume principal. La valeur est déterminée par la différence entre le niveau de bruit actuel et le seuil de sensibilité et ne dépasse jamais la valeur du gain maximal.



- **Volume de sonnerie** – paramétrez le volume de sonnerie des appels entrants.
- **Volume de tonalité d'appel** – paramétrez le volume de numérotation, de sonnerie et de tonalité d'occupation. Si les tonalités de progression d'appel sont automatiquement générées par le PBX, ce paramètre ne sera pas appliqué.



- **Volume du bip sonore des touches** – paramétrez le volume de bip sonore des touches. Les valeurs du volume sont relatives vis-à-vis du volume général paramétré.
- **Volume de la tonalité d'avertissement** – paramétrez le volume des tonalités d'avertissement et de signalisation décrites dans la section "Signalisation d'états opérationnels". Les valeurs du volume sont relatives vis-à-vis du volume général paramétré.
- **Volume de la tonalité d'activation des interrupteurs** – paramétrez le volume de la tonalité d'activation des interrupteurs. Les valeurs de volume sont relatives vis-à-vis du volume général paramétré.
- **Volume des sons personnalisables** – paramétrez le volume des sons personnalisables. Les valeurs du volume sont relatives vis-à-vis du volume général paramétré.

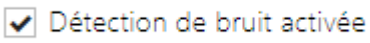


- **Entrée Audio par défaut** – définissez l'entrée audio par défaut (microphone, entrée de ligne ou entrée de module audio) à utiliser pour les appels téléphoniques et la diffusion audio.
- **Gain d'entrée du microphone** – paramétrez le gain d'entrée du microphone.
- **Gain d'entrée de ligne** – définissez le gain d'entrée de ligne indépendamment de la valeur de gain du microphone.

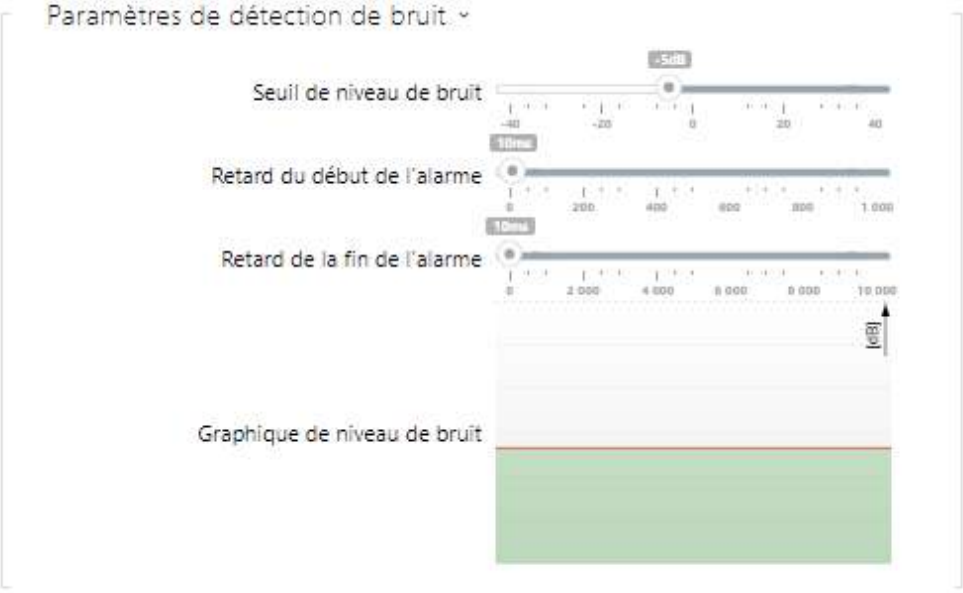
Conseil

Seul les modèles **2N® SIP Speaker Horn**, **2N® IP Audio Kit** et **2N® IP Video Kit** permettent de configurer le gain du microphone.
Le paramètre de gain d'entrée microphone / ligne est connecté au niveau du signal d'entrée et au type d'installation du microphone externe. La plage de gain (0 à 39 dB pour une entrée microphone et −6 dB à 24 dB pour une entrée ligne) devrait être suffisante pour la plupart des installations. Définissez une valeur pour assurer une bonne audibilité et éliminer les retours acoustiques excessifs avec des volumes de haut-parleurs élevés, avec une saturation du signal sur l'entrée microphone / ligne et donc une détérioration de l'annulation d'écho acoustique (AEC).

- **Suppression de la rétroaction acoustique** – définissez la suppression automatique du retour acoustique (généralement un sifflement) entre le haut-parleur de l'interphone et le combiné du téléphone s'il est situé à proximité immédiate de l'interphone. Ce mode est désactivé par défaut.

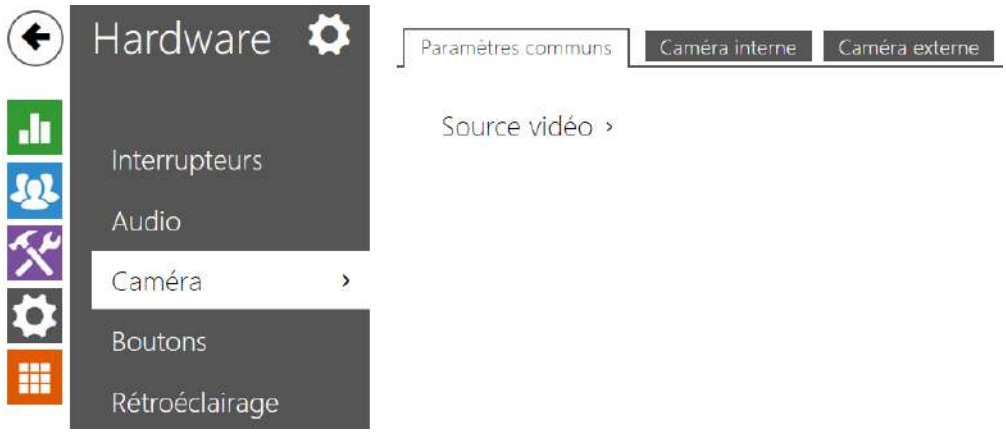


- **Détection de bruit activée** – activer la détection automatique du bruit ambiant au delà ou d'un certain seuil paramétrable. La détection d'un bruit anormalement élevé par rapport au seuil programmé apparait comme ceci dans l'Interface d'automatisation **"Event.NoiseDetected"** vous pouvez lui affecter une action automatique de votre choix.



- **Seuil du niveau de bruit** – définissez le seuil de bruit du microphone pour le réglage de l'alarme.
- **Retard du début de l'alarme** – définissez l'intervalle de temps pendant lequel le signal doit être supérieur au seuil pour déclencher l'alarme.
- **Retard de la fin de l'alarme** – définissez l'intervalle de temps pendant lequel le signal doit être inférieur au seuil pour arrêter l'alarme.
- **Graphique du niveau de bruit** – affichez l'historique du niveau de bruit ambiant en dB. La ligne rouge désigne le seuil au delà duquel l'alarme peut s'activer.

5.5.3 Caméra



Ce menu est uniquement disponible dans les modèles **d'interphone IP 2N** équipés d'une caméra interne ou pouvant être connectés à une caméra externe. Le signal de la caméra peut être transmis directement pendant l'appel depuis le vidéophone, envoyé par courrier électronique, via ONVIF / RTSP vers un autre appareil (un dispositif de vidéosurveillance, par exemple), ou simplement téléchargé via HTTP à partir de l'interphone au format JPEG.
Les sources de signal vidéo suivantes peuvent être utilisées :

- une caméra intégrée interne ou une caméra analogique externe (**2N® IP Video Kit** seulement).
- une caméra IP externe standard prenant en charge le flux RTSP avec les codecs MJPEG (résolution maximale de 640 x 480) ou H.264 (résolution maximale du profil de ligne de base de 640 x 480). Le nombre d'images par seconde recommandé est de 15 images par seconde dans les deux cas. Des taux de trame plus élevés peuvent entraîner des effets indésirables (flux moins fluide).

Le menu Caméra vous aide à définir des paramètres tels que la luminosité, la saturation des couleurs et les données de connexion à une caméra IP externe, le cas échéant. Référez-vous aux sections **Services / Téléphone, Services** / **Streaming** et **Services** / **E-Mail** pour les paramètres d'appel vidéo / streaming.

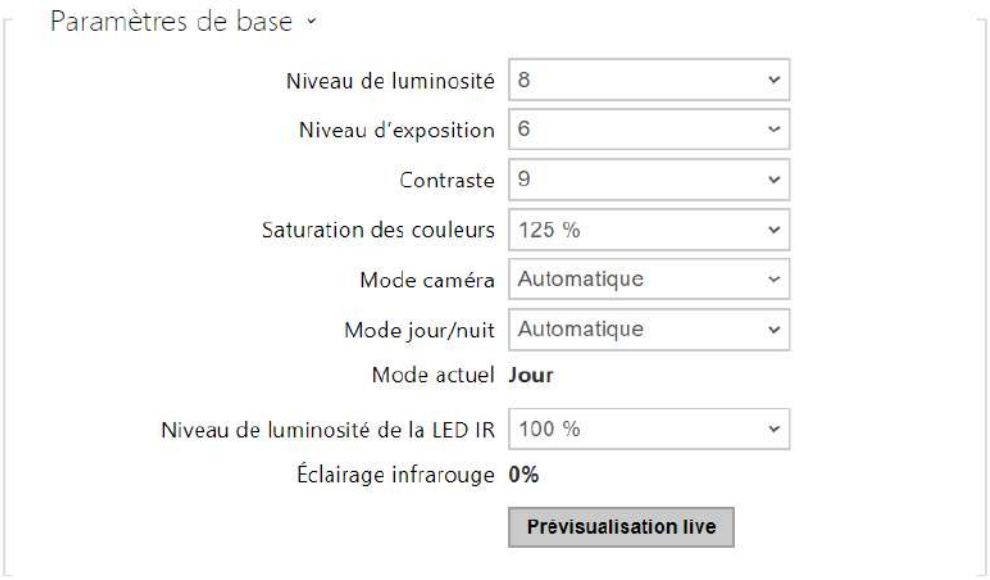
Paramètres de base

- **Source vidéo par défaut** – paramétrez la source de signal vidéo par défaut. Sélectionnez une caméra interne (ou une caméra analogique connectée à l'interphone) ou une caméra IP externe. Le changement de la source de signal vidéo par défaut est appliqué au flux RTSP et à l'API HTTP. Dans l'application **2N® IP Eye** il est nécessaire d'activer

manuellement la caméra externe, même en l'absence de caméra interne dans l'appareil. Si aucune caméra interne n'est connectée à l'interphone, seule la caméra IP externe peut être sélectionnée. Si la caméra externe n'est pas connectée ou configurée correctement, N / A s'affiche sur un fond bleu.

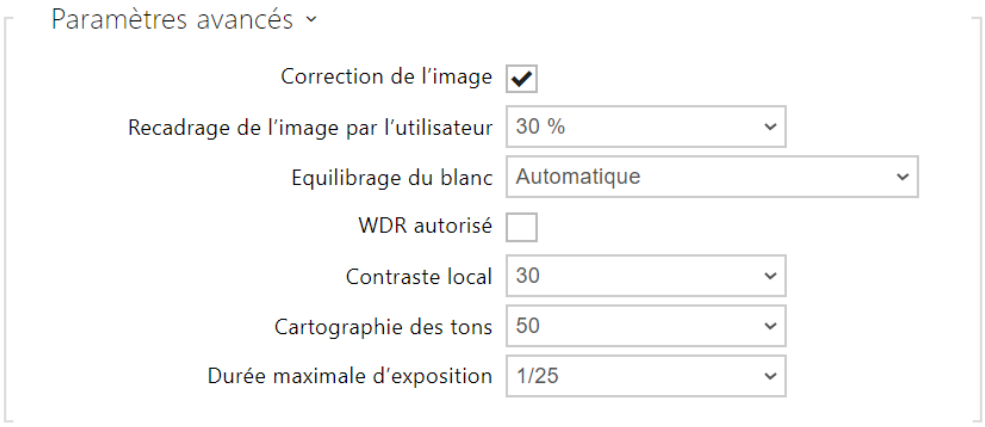
- **Prévisualisation live** – affiche la fenêtre de visualisation en direct de la caméra de l'interphone IP 2N.

Caméra interne



- **Niveau de luminosité** – paramétrez le niveau de luminosité de l'image de la caméra.
- **Niveau d'exposition** – définit le niveau d'exposition de l'image (des valeurs plus élevées signifient que l'appareil préfère un temps d'exposition plus long).
- **Contraste** - définit le contraste de l'image de la caméra.
- **Saturation des couleurs** – paramétrez la saturation des couleurs de l'image de la caméra.
- **Mode caméra** – permet de régler différents régimes d'enregistrement de l'image selon l'installation actuelle de l'interphone (utilisation en intérieur et à l'extérieur). En cas d'installation à l'intérieur, il est possible de choisir entre différents modes de suppression du clignotement de l'image causé par une source de lumière artificielle. En cas d'installation à l'extérieur, le régime de suppression de la lumière solaire directe peut être réglé.
- **Taux de la fréquence d'image automatique décroissante** – permet une diminution automatique de la fréquence d'images dans des conditions d'éclairage dégradées afin d'améliorer la qualité de l'image.
- **Découpage d'image** – l'angle de la caméra du modèle **2N® IP Force** vous permet de numériser la plus grande surface possible. Utilisez ce paramètre pour activer le rognage automatique des images de la caméra afin d'éliminer la vue (parfois gênante) de la trame interphone. Si vous avez besoin d'un angle de vue maximum, désactivez cette fonction. Ce paramètre n'est disponible que sur le modèle **2N® IP Force**.

- **Mode jour/nuit** – paramétrez le mode jour/nuit de la caméra. Les options sont automatiques (contrôlées par le niveau de lumière ambiante) ou en mode jour ou nuit de façon permanente.
- **Mode actuel** – affiche le mode de caméra actuellement sélectionné (jour / nuit). En mode jour, la caméra utilise un filtre anti-infrarouge et l'éclairage infrarouge est désactivé. En mode nuit. En mode nuit, le filtre suppresseur d'infrarouge est désactivé et l'éclairage par infrarouge est allumé.
- **Niveau de luminosité de la LED IR** – permet de régler le niveau de luminosité de la LED infrarouge dans une plage comprise entre 0 et 100% avec plusieurs niveaux disponibles. L'éclairage infrarouge est automatiquement activé en mode nuit. Les réglages du niveau de luminosité de la LED IR sont uniquement disponibles sur les modèles **2N® IP Style, 2N® IP Verso** et **2N® IP Force** équipés de la caméra HD.
- **Niveau actuel de luminosité de la LED IR** – affiche le pourcentage actuel de niveau de luminosité de la LED IR. Le niveau peut être automatiquement réduit en dessous de la valeur définie afin que la consommation électrique maximale ne puisse pas être dépassée (généralement, lorsque plusieurs extensions sont connectées et que l'alimentation PoE est utilisée).
- **Prévisualisation live** – affiche la fenêtre de visualisation en direct de la caméra de l'interphone IP 2N.

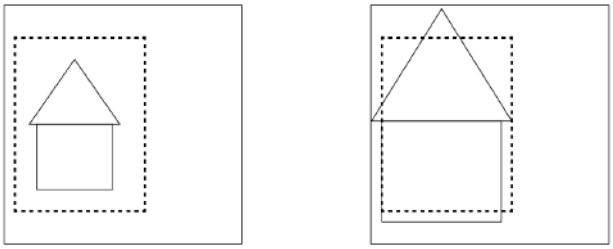


Le groupe de fonctions Paramètres avancés est valable pour les modèles 2N IP de l'interphone **2N® IP Style**.

- **Correction de l'image** – définit la correction numérique (alignement) de l'image de la caméra interne de l'appareil.
- **Recadrage de l'image par l'utilisateur** – définit le recadrage centré par défaut de l'image (les bords sont recadrés uniformément).
- **Equilibrage du blanc** – le réglage de l'équilibrage fixe du blanc en fonction de la source de lumière dominante convient si l'équilibrage automatique du blanc ne suffit pas (une variante d'équilibrage du blanc mal sélectionnée entraîne une palette de couleurs de l'image indésirable).
- **WDR autorisé** – WDR (Wide Dynamic Range) doit être activé s'il y a des endroits à la fois très sombres et très illuminés sur la scène. WDR garantit la visibilité de toute la scène.
- **Contraste local** – la définition d'un niveau plus élevé permet d'accentuer le contraste de l'interface entre les parties claires et sombres de la scène.
- **Cartographie des tons** – la définition d'un niveau plus élevé permet d'accentuer l'image et d'améliorer la visibilité (l'image peut alors avoir des couleurs dénaturées).
- **Durée maximale d'exposition** – définit la durée maximale d'exposition et de création d'une image particulière. Lorsque davantage de lumière est disponible, l'obturateur peut ne pas être ouvert en permanence et l'appareil photo définit alors automatiquement une durée d'exposition actuelle plus courte.

Precaución

- Après avoir modifié le paramètre ***Découpage de la scène par l'utilisateur*** sur un appareil équipé d'un processeur ARTPEC-7, il convient de vérifier la délimitation de la zone de détection de mouvement et de la zone de confidentialité, qui changent dans l'espace, cf. l'illustration.



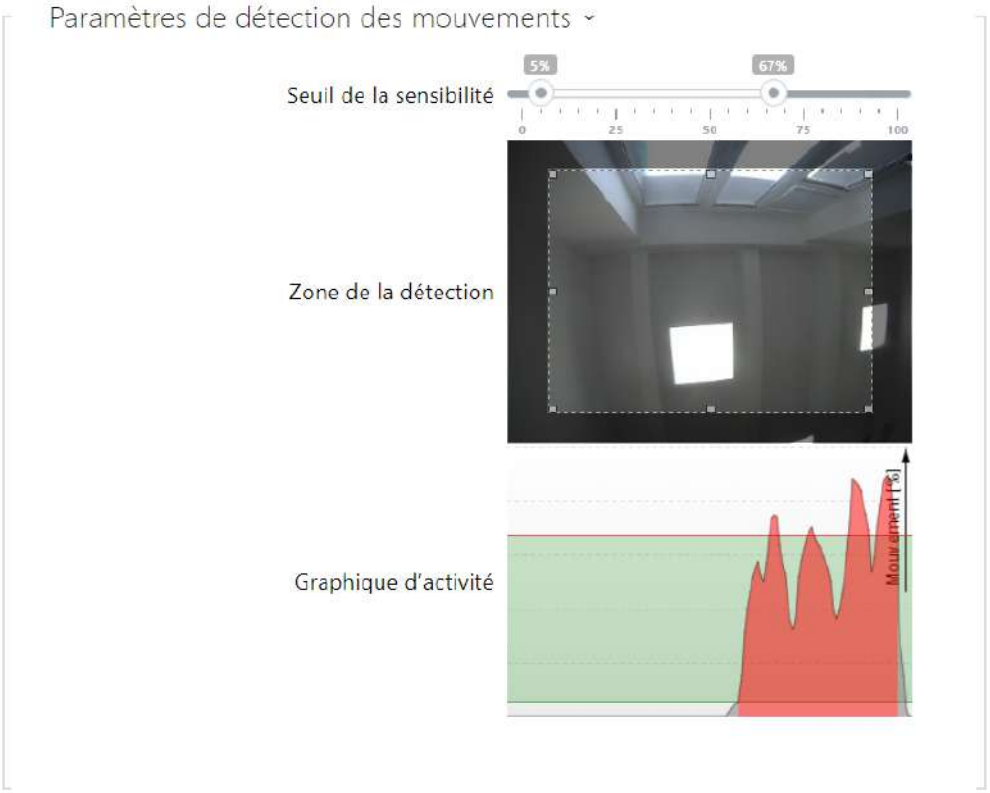
Nota

- *Ce paramètre est uniquement disponible sur les modèles équipés d'une entrée de caméra analogique externe.*

- **Entrée Video** – choisissez l'une des entrées de caméra analogiques. Vous pouvez modifier l'entrée par automatisation via Action.SetCameraInput pendant l'opération.
- **Video standard** – définissez le standard vidéo pour la caméra connectée. Modifiez la valeur uniquement si la détection automatique du standard vidéo ne fonctionne pas correctement (valeur automatique).

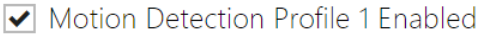
- **Détection de mouvement** – permet d'activer la détection automatique de mouvement à partir de l'image de la caméra interne. Le mouvement est détecté par la surveillance d'un changement de luminosité dans la section d'image sélectionnée dans le temps. Lorsque

des objets se déplacent dans la plage de la caméra, la partie sélectionnée de l'image détecte une activité, qui peut être exprimée en pourcentage. Si l'activité dépasse la limite supérieure, un mouvement est détecté et indiqué jusqu'à ce que l'activité chute sous la limite inférieure. Sélectionnez les seuils de sensibilité et la zone de détection en fonction des exigences et des conditions du site d'installation.



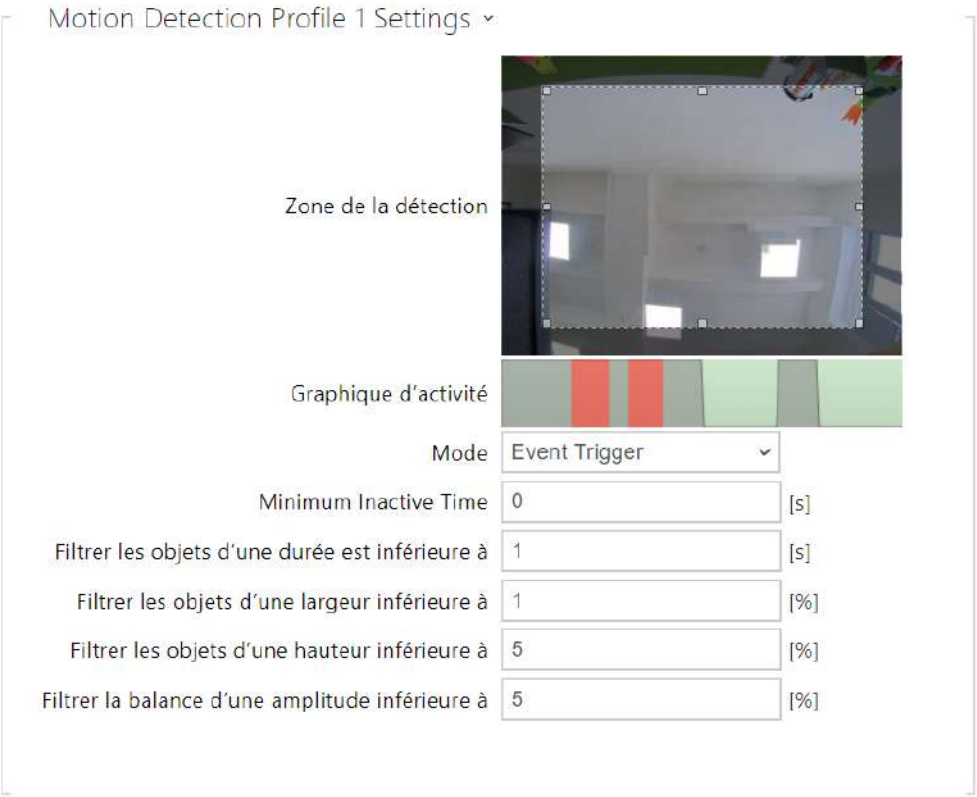
- **Seuil de sensibilité** – définissez les limites inférieure et supérieure de sensibilité et d'hystérésis pour l'algorithme de détection de mouvement.
- **Zone de détection** – définissez la zone de détection rectangulaire dans l'image.
- **Graphique d'activité** – affichez l'historique d'activité (changements de luminosité de l'image), y compris les seuils de sensibilité supérieur / inférieur.

Détection de mouvement et protection de la confidentialité pour les appareils équipés du processeur ARTPEC-7



- **Détection de mouvement – profil 1/2 activée** – permet d'activer la détection automatique de mouvement à partir de l'image de la caméra interne. Le mouvement est détecté en suivant la variation de la composante de luminosité dans une partie sélectionnée de l'image au fil du temps. Lorsque les objets dans le cadre de la caméra se

déplacent, certaines parties de l'image changent. Si l'activité dépasse le seuil de sensibilité supérieur, un mouvement est indiqué. Le mouvement est indiqué jusqu'à ce que l'activité tombe en dessous du seuil de sensibilité inférieur.



- **Zone de la détection** – définissez la zone de détection rectangulaire dans l'image.
- **Graphique d'activité** – Affiche l'historique de l'activité détectée sur la ligne de temps. Le vert signifie qu'il n'y a pas de mouvement, le gris signifie qu'un mouvement est détecté mais ne remplit pas les conditions, le rouge signifie qu'un mouvement est détecté et remplit les conditions.
- **Mode** - le mode de déclenchement d'événements est conçu pour générer de courts événements de détection de mouvement pour des actions telles que par ex. l'enregistrement d'images. Le mode d'enregistrement est conçu pour générer des événements plus longs, par ex. pour l'enregistrement à l'aide d'ONVIF.
- **Temps minimal d'inactivité** – définit le temps minimal entre deux événements de détection de mouvement. Cela permet d'éviter que de nombreux événements ne se produisent en succession rapide.
- **Filtrer les objets d'une durée est inférieure à** – définit la durée minimale requise en secondes au cours de laquelle le mouvement doit être détecté en continu pour qu'un événement de détection du mouvement soit rapporté. La gamme de réglage est de 1 à 5 s, 0 est interdit par ce filtre. Le mouvement doit également satisfaire aux autres conditions définies dans cette section.
- **Filtrer les objets d'une largeur inférieure à** – définit la largeur minimale des objets par rapport à la largeur totale de l'image de la caméra que l'objet détecté doit avoir pour

qu'un événement soit rapporté. La gamme de réglage est de 1 à 100 %, 0 est interdit par ce filtre. Le mouvement doit également satisfaire aux autres conditions définies dans cette section.

- **Filtrer les objets d'une hauteur inférieure à** – définit la hauteur minimale des objets par rapport à la hauteur totale de l'image de la caméra que l'objet détecté doit avoir pour que l'événement soit rapporté. La gamme de réglage est de 1 à 100 %, 0 est interdit par ce filtre. Le mouvement doit également satisfaire aux autres conditions définies dans cette section.
- **Filtrer la balance d'une amplitude inférieure à** – définit l'amplitude minimale devant être dépassée des objets oscillants par rapport à la largeur ou la hauteur totale de l'image de la caméra, pour permettre de détecter l'objet (le paramètre n'a aucun effet sur les objets fixes). La gamme de réglage est de 0 à 20 %, 0 est interdit par ce filtre. Le mouvement doit également satisfaire aux autres conditions définies dans cette section.

Precaución

- Pour les appareils équipés d'un processeur ARTPEC-7, les objets en mouvement sont évalués même en dehors de la zone active, y compris les filtres définis (si le ***Recadrage de l'image utilisateur*** est utilisé, les objets seront évalués même dans les parties de l'image qui sont recadrées et l'utilisateur ne les voit pas dans l'aperçu). Les objets qui entrent dans la zone active déclenchent ensuite un événement de détection de mouvement. Par exemple, si le filtre temporel est réglé sur 5 s, un objet qui se déplace en dehors de la zone active pendant 10 s déclenchera un événement de détection de mouvement immédiatement après être entré dans la zone active car il a déjà rempli la condition de filtre en dehors de la zone active. L'objet continue d'être détecté même lorsqu'il quitte la zone active et déclenche un événement dès qu'il revient dans la zone active (à condition qu'il ne quitte pas complètement la zone d'image de la caméra et ne soit pas « oublié »).

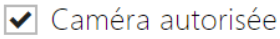
- **Protection de la vie privée autorisée** – active la fonction de confidentialité qui masque une partie de l'image avec la couleur ou la mosaïque sélectionnée.

- **Mode couverture** – règle la couleur ou la mosaïque de la zone couverte.
- **Rugosité de la mosaïque** – définit la rugosité de la mosaïque dans le domain de la protection de la vie privée.
- **Domaine de la protection de la vie privée** – domaine de la protection de la vie privée - définit la position et la taille de la zone de confidentialité.

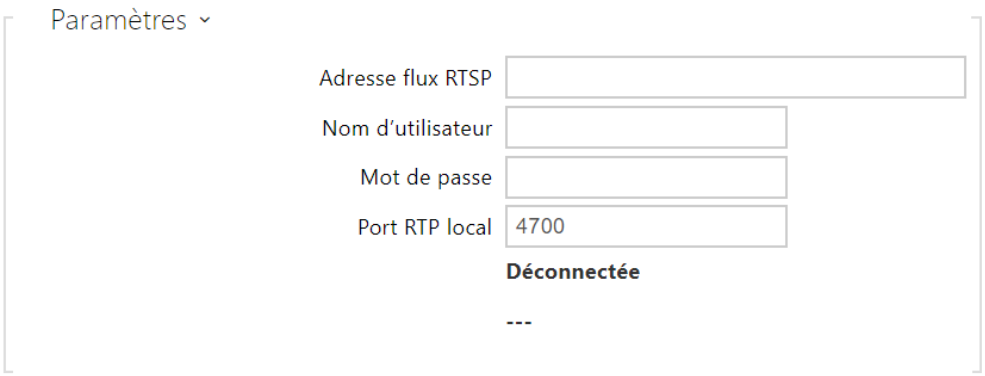
Observation

- La protection de la confidentialité peut limiter le fonctionnement d'autres fonctions, telles que la lecture des codes QR ou la détection de mouvement. Nous ne recommandons pas d'utiliser la protection de la confidentialité en même temps que ces fonctions.

Caméra externe



- **Caméra autorisée** – activez le téléchargement par flux RTSP depuis la caméra IP externe. Remplir l'adresse de flux RTSP valide ou le nom d'utilisateur et le mot de passe pour que la fonction fonctionne bien.



- **Adresse flux RTSP** – entrez l'adresse du flux RTSP de la caméra IP : rtsp://camera_ip_address/param1=x&param2=y, voir le tableau des paramètres ci-dessous. Les paramètres sont spécifiques au modèle de caméra IP sélectionné. Si vous choisissez un autre interphone **IP 2N** pour la caméra externe, entrez : http://ip_address/mjpeg_stream ou http://ip_address/h264_stream.

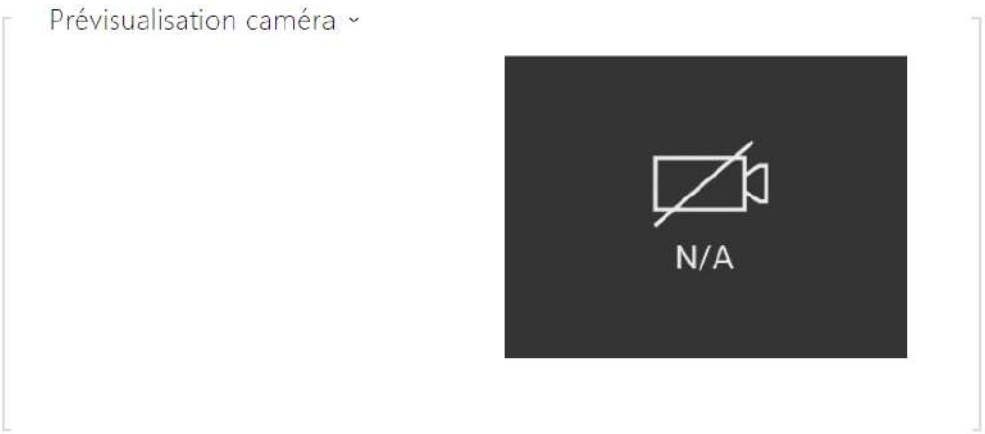
paramètre	description	exemple / valeurs
vcodec	Codec vidéo	vcodec=h264 pour le codec H.264 vcodec=mjpeg pour le codec MJPEG
vres	Résolution vidéo	vres=1920x1080 pour FullHD
fps	Fréquence d'image vidéo	fps=15 (1 à 30 fps, la valeur maximale possible pour le codec vidéo MJPEG est de 15 fps.)
vbr	Débit binaire	vbr=768 pour 768 kbps
audio	Audio	• audio=1 (activé) • audio=0 (désactivé)
zipstream	Zipstream (disponible uniquement pour H.264)	• zipstream=off (désactivé) • zipstream=low • zipstream=medium • zipstream=high • zipstream=higher

- **Nom d'utilisateur** – entrez le nom d'utilisateur pour l'authentification de la caméra IP externe. Ce paramètre est uniquement obligatoire si la caméra IP externe nécessite une authentification.

- **Mot de passe** – entrez le mot de passe d'authentification de la caméra IP externe. Ce paramètre est uniquement obligatoire si la caméra IP externe nécessite une authentification.
- **Port RTP local** – définissez le port UTP local pour la réception du flux RTP.

Consejo

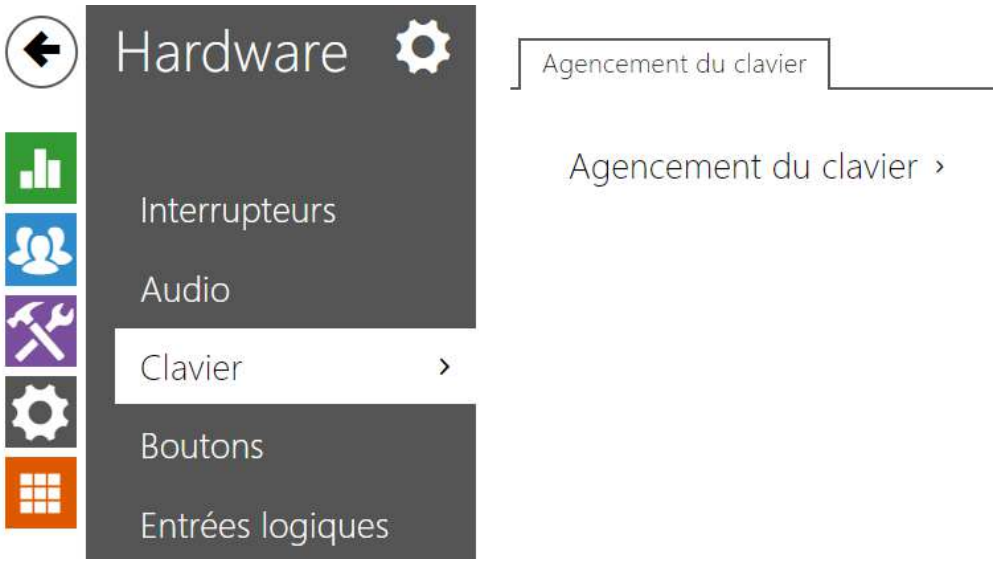
- FAQ: Caméra externe – Comment intégrer une caméra dans l'interphone IP 2N



La fenêtre Prévisualisation de la caméra affiche l'image en temps réel reçue depuis une caméra externe. Si la caméra externe n'est pas connectée ou configurée correctement, N / A s'affiche sur un fond bleu.

La Communication de la caméra IP externe affiche la communication RTSP avec la caméra IP externe sélectionnée, y compris les défaillances et les états d'erreur, le cas échéant.

5.5.4 Clavier



Cette section de configuration vous aide à définir les fonctions du clavier numérique et du bouton de numérotation rapide. Les **Interphones IP 2N** vous permettent de :

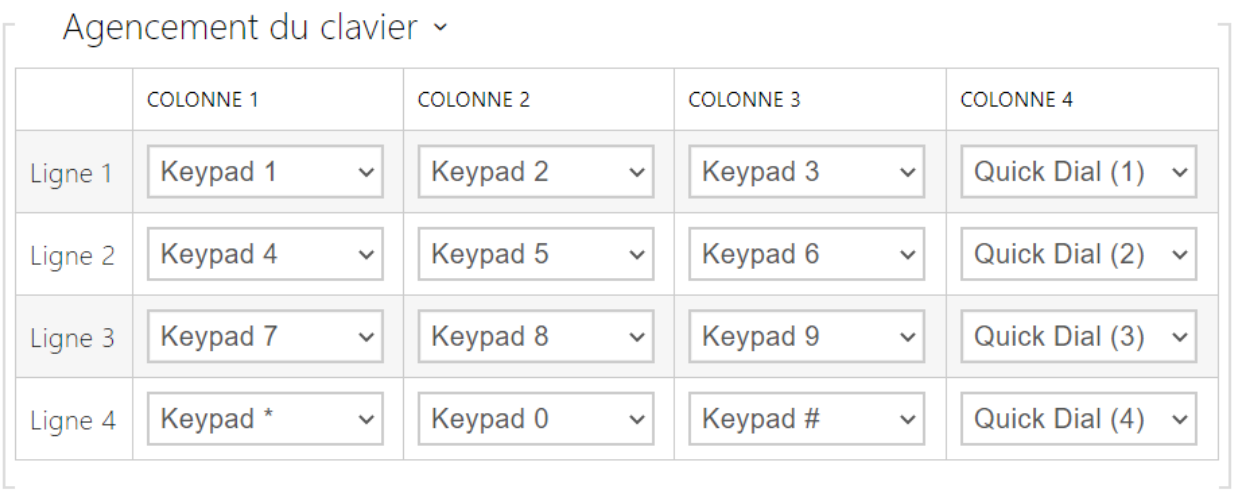
- utiliser le clavier numérique pour passer un appel en saisissant le numéro virtuel de l'utilisateur,
- utiliser le pavé numérique pour composer le numéro d'un poste,
- utilisez le clavier numérique pour entrer le code d'accès pour le déverrouillage de la porte, par ex.,
- définir la fonction #,
- définir le délai d'attente pour la saisie des codes et des numéros de téléphone,
- régler la fonction des boutons et des touches du poste connecté sur les modèles **2N® IP Audio/Video Kit**.

Agencement du clavier

Les modèles **2N® IP Audio Kit** et **2N® IP Video Kit** sont équipés de huit terminaux pour un maximum de 16 boutons externes ou d'un clavier. Les fonctions peuvent être définies pour chaque bouton séparément.

Les boutons et leurs paramètres sont disposés dans une matrice de 4 colonnes X 4 lignes (voir le schéma ci-dessous).

Le schéma ci-dessous montre les paramètres de bouton par défaut.



Vous pouvez affecter une fonction à chaque position de la matrice : les touches du pavé numérique 0 à 9, *, # ou l'une des touches de numérotation rapide 1–16.

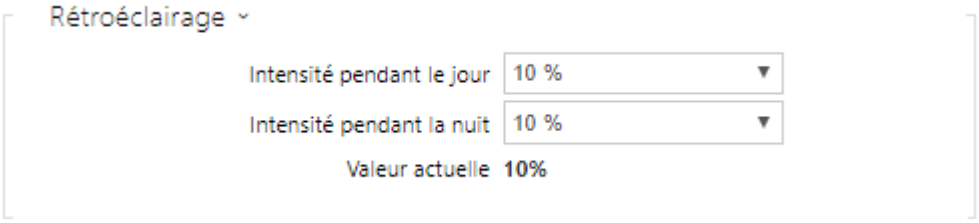
5.5.5 Rétroéclairage

Cette section vous permet de contrôler le niveau de rétroéclairage des étiquettes d'identification, des boutons et la luminosité des voyants de signalisation.

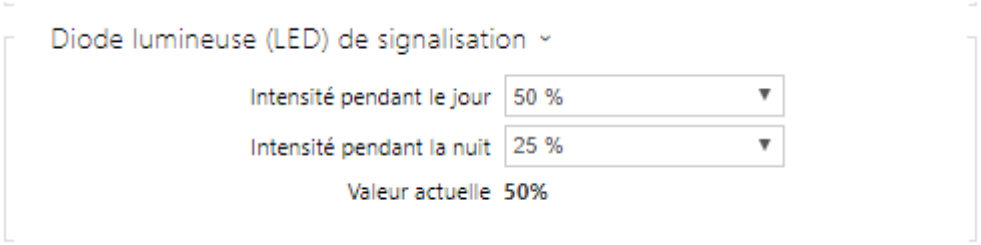
S'il est équipé d'un capteur de niveau de lumière ambiante, l'interphone choisit automatiquement le niveau de rétroéclairage approprié dans la plage de valeurs définie. Les interphones sélectionnés vous permettent de contrôler la luminosité du rétro-éclairage des étiquettes de nom (boutons) et des voyants de signalisation (pictogrammes lumineux). Reportez-vous au tableau ci-dessous :

Propriétés/ Modèles	2N® IP Style	2N® IP Verso/ LTE Verso	2N® IP Solo	2N® IP Base	2N® IP Vario	2N® IP Force	2N® IP Safety	2N® IP Uni	2N® IP Audio Kit	2N® IP Video Kit
Contrôle du niveau de rétroéclairage	**Oui**			**Oui**	**Oui**				Non	

Propriétés/ Modèles	2N® IP Style	2N® IP Verso/ LTE Verso	2N® IP Solo	2N® IP Base	2N® IP Vario	2N® IP Force	2N® IP Safety	2N® IP Uni	2N® IP Audio Kit	2N® IP Video Kit
Capteur de niveau de lumière ambiante	**Oui**			Non	Non				Non	
Contrôle du niveau de rétroéclairage des LED et des boutons indépendants	**Oui**			**Oui**	Non				Non	



Les paramètres établis dans le groupe Rétroéclairage sont valables pour le rétroéclairage de l'unité principale, des boutons et des modules d'ajout.



Le paramétrage du groupe de signalisation LED est valable pour les voyants LED de signalisation des modules d'extension **2N® IP Verso**.

- **Intensité pendant le jour** – définissez la valeur de luminosité du rétroéclairage pendant le jour. La valeur est donnée en pourcentage de la luminosité maximale possible des LED.
- **Intensité pendant la nuit** – définissez la valeur de luminosité du rétroéclairage pendant la nuit. La valeur est donnée en pourcentage de la luminosité maximale possible des

LED. Si les paramètres Luminosité pendant le jour et Luminosité pendant la nuit sont réglés sur une seule et même valeur, le niveau de lumière ambiante est ignoré.
- **Valeur actuelle** – affiche la valeur actuelle de l'intensité de la LED sélectionnée automatiquement en fonction du niveau de lumière du jour ambiant.

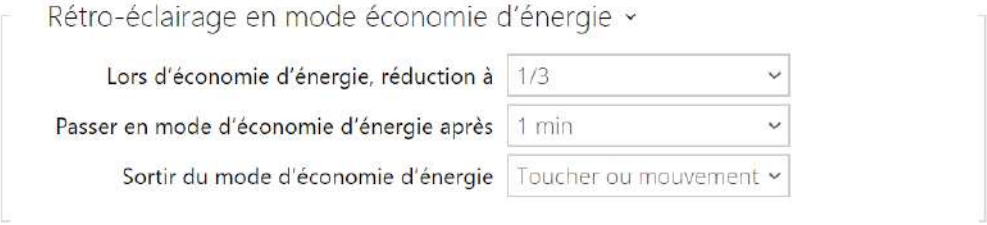
Note

- Les paramètres d'intensité de la luminosité affectent la fonction, la consommation d'énergie et l'apparence générale de votre appareil. Si le niveau de luminosité ambiante est faible, une valeur élevée de rétroéclairage des boutons peut éblouir les personnes se tenant devant l'interphone et, en général, augmenter la consommation électrique de l'appareil. En revanche, une valeur d'intensité de LED faible peut entraîner, si l'interphone est exposé au soleil, un contraste plus faible de la LED et des problèmes d'identification de l'état de la LED.

Paramètres du rétro-éclairage de l'écran de l'interphone 2N® IP Style

Le paramétrage des groupes Rétro-éclairage et Rétro-éclairage en mode d'économie d'énergie est valable pour le rétro-éclairage de l'écran et du voyant LED ambiant.

- **Intensité en mode actif le jour** – définit la valeur maximale de la luminosité du rétro-éclairage le jour (la valeur est contrôlée par le capteur de lumière ambiante). La valeur est indiquée en pourcentage de luminosité maximale possible.
- **Intensité en mode actif la nuit** – définit la valeur maximale de la luminosité du rétro-éclairage la nuit (la valeur est contrôlée par le capteur de lumière ambiante). La valeur est indiquée en pourcentage de luminosité maximale possible.
- **Valeur actuelle** – affiche la valeur de l'intensité du rétro-éclairage réellement sélectionnée automatiquement en fonction du niveau de lumière ambiante réellement détecté.



- **Lors d'économie d'énergie, réduction à** – Le niveau de rétroéclairage diminue lorsque l'appareil passe en mode inactif.
- **Passer en mode d'économie d'énergie après** – Définit la durée pendant laquelle l'équipement est inactif (à savoir la durée pendant laquelle l'équipement n'interagit pas) au-delà de laquelle il passe automatiquement en mode d'économie d'énergie. La valeur est indiquée en secondes dans une envergure comprise entre 1 et 600.
- **Sortir du mode d'économie d'énergie** – définit les modes d'interaction qui peuvent être utilisés pour sortir du mode d'économie d'énergie. Il est possible de choisir entre le contact tactile sur l'écran et le contact tactile ou la détection du mouvement. L'équipement sort de plus toujours du mode d'économie d'énergie au cours de l'authentification de l'utilisateur, d'un appel entrant et d'autres états de fonctionnement.

Le paramétrage du groupe de signalisation LED est valable pour les voyants LED de signalisation (rétro-éclairage du lecteur **2N® IP Style**).

- **Intensité pendant le jour** – il définit la valeur de luminosité des LED de signalisation pendant le jour. La valeur est donnée en pourcentage de la luminosité maximale possible des LED.
- **Intensité pendant la nuit** – il définit la valeur de luminosité des LED de signalisation pendant la nuit. La valeur est donnée en pourcentage de la luminosité maximale possible des LED. Si les paramètres Luminosité pendant le jour et Luminosité pendant la nuit sont réglés sur une seule et même valeur, le niveau de lumière ambiante est ignoré.
- **Valeur actuelle** – affiche la valeur de l'intensité du voyant LED réellement sélectionnée automatiquement en fonction du niveau de lumière ambiante réellement détecté.

5.5.6 Ecran

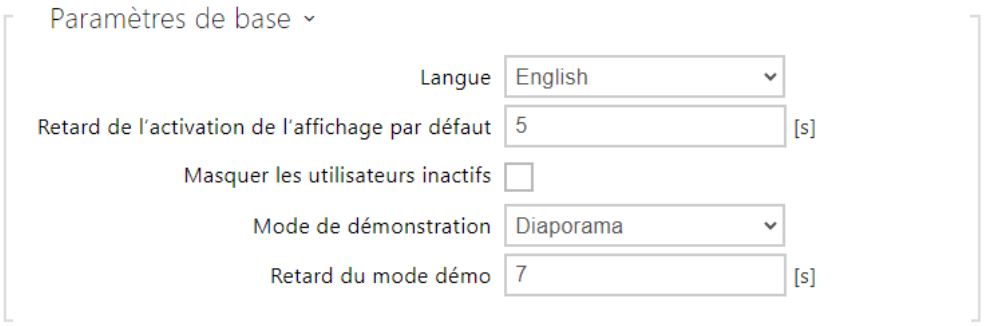
Certains modèles d'Interphone (**2N® IP Vario**, **2N® IP Verso**) peuvent être équipés d'un écran LCD couleur. L'état de l'appareil est affiché (progression de l'appel, ouverture de la porte, etc.) et les modes suivants sont disponibles :

Ecran – active les paramètres d'affichage et de langue pour le **2N® IP Vario** et les paramètres de base et de langue pour le **2N® IP Verso**.

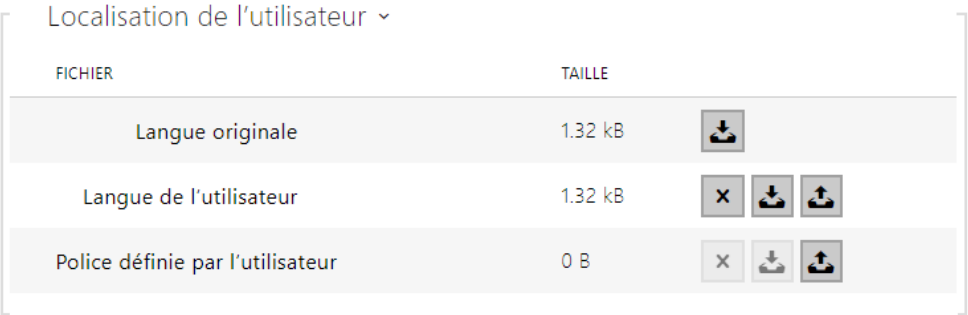
Répertoire – affiche une liste configurable d'utilisateurs. Utilisez les boutons du clavier numérique (flèches) pour parcourir la liste des utilisateurs. Vous pouvez créer de nombreux groupes et de nombreux utilisateurs qui pourront être répartis dans ces groupes.

Diaporama – affiche un diaporama d'images enregistrées après un temps d'inactivité prédéfini. Le temps avant l'affichage automatique peut être configuré.

Ecran (seulement sur le modèle 2N® IP Vario)



- **Langue** – définissez la langue des textes affichés à l'écran. Unes des langues prédéfinies peut être sélectionnée : anglais, tchèque, allemand, italien, français, espagnol, russe, finnois, danois, polonais, néerlandais, portugais, turc, norvégien, suédois ou une langue personnalisée (custom).
- **Retard de l'activation de l'affichage par défaut** – définissez le temps d'inactivité maximum de l'écran (c'est-à-dire pendant lequel l'écran n'est pas utilisé) au delà duquel le mode Répertoire rebascule sur le menu si celui-ci est configuré, ou bien, sur la fenêtre affichant le logo 2N par défaut.
- **Masquer les utilisateurs inactifs** – si cette option est cochée, l'utilisateur dont le profil temporel est actif ce qui l'empêche d'être contacté, est automatiquement masqué.
- **Mode de démonstration** – définit si l'équipement passe en mode de démonstration lorsqu'il est inactif. Il est possible de choisir un autre comportement en mode de démonstration (Désactivé, Diaporama).
- **Temporisation de l'activation du mode de démonstration** – définit l'intervalle de temps d'inactivité de 1 à 600 secondes après lequel l'appareil passe en mode démonstration. Il y a toujours un délai fixe de 15 secondes avant que l'appareil ne retourne à la page d'accueil.



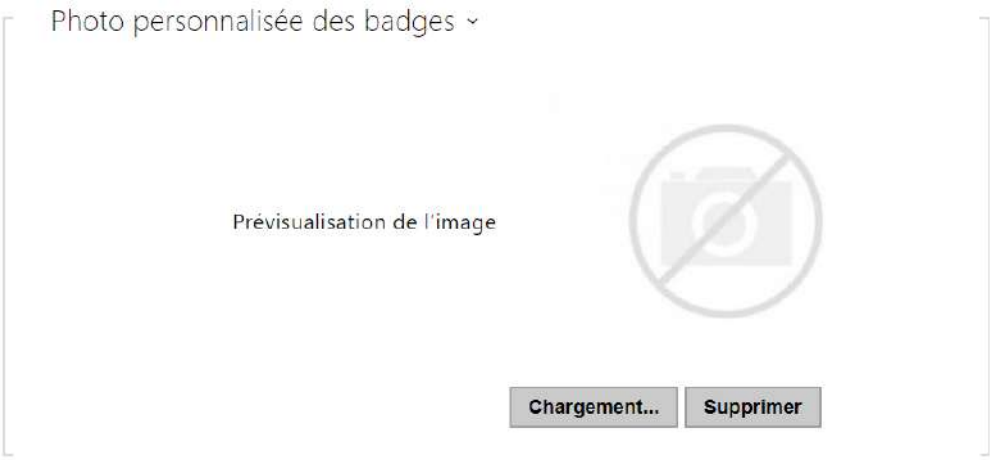
- **Langue originale** – téléchargez le modèle de fichier de localisation pour sa traduction. C'est un fichier XML avec tous les textes à afficher.
- **Langue de l'utilisateur** – enregistrez, supprimez et chargez un fichier de localisation de votre choix.
- **Police définie par l'utilisateur** – enregistrez, supprimez et chargez votre propre police pour que les textes soient affichés. Conservez le format TTF et assurez-vous que le fichier ne dépasse pas 4 Mo.

Note

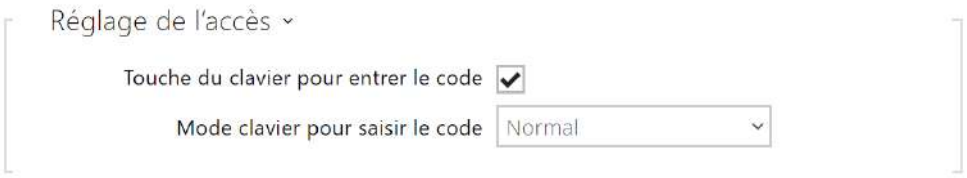
Si aucune des langues prédéfinies ne vous convient, procédez comme indiqué ci-dessous :

- Téléchargez le fichier de langue d'origine (**anglais**).
- Modifiez le fichier en utilisant un éditeur de texte (remplacez les textes en anglais par les textes dans votre langue).
- Rechargez le fichier de localisation modifié sur l'interphone.
- Définissez les **paramètres de langue** | **Langue à personnaliser**.
- Vérifiez et corrigez si nécessaire les textes sur l'écran de l'interphone.

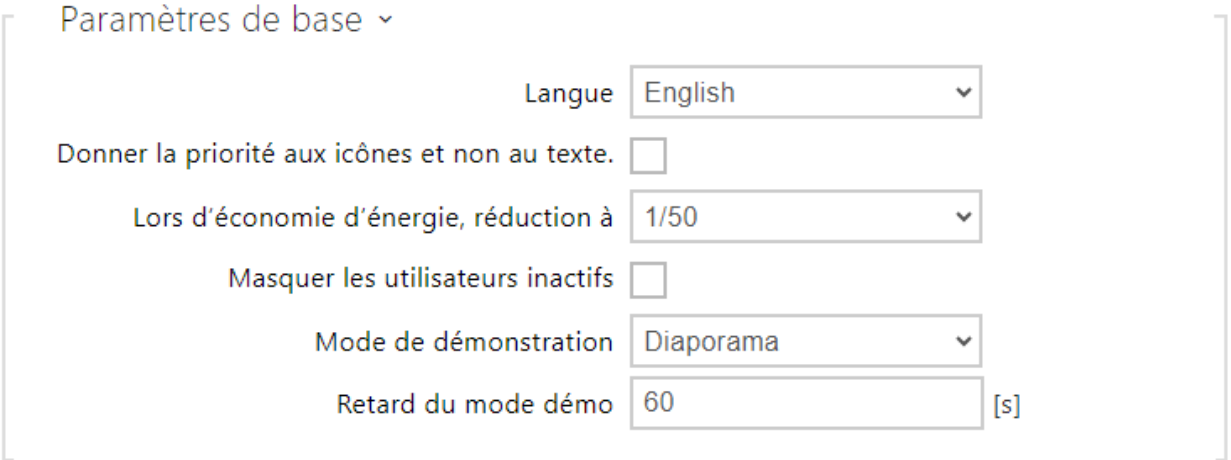
Si vous n'aimez pas l'aspect graphique par défaut des étiquettes de nom, téléchargez un arrière-plan de votre choix sur l'interphone. Assurez-vous que la résolution de l'image est de 320 x 240 pixels. Téléchargez vos étiquettes de nom sur l'interphone pour remplacer les étiquettes de nom d'origine. Les assignations utilisateur originales restent toutefois les mêmes.



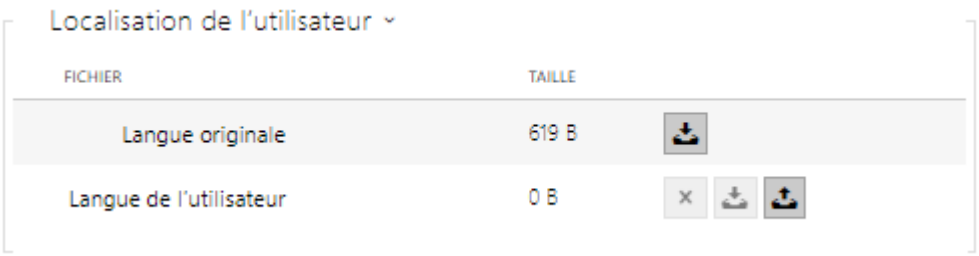
Ecran (seulement sur le modèle 2N® IP Verso)



- **Touche du clavier pour entrer le code** – active l'affichage du clavier à l'écran pour saisir les codes numériques.
- **Mode clavier pour saisir le code** – définit le mode clavier à l'écran pour saisir les codes numériques. Les modes sont le clavier normal ou le clavier avec des touches mélangées pour plus de sécurité. Le paramètre s'applique également au clavier pendant l'authentification multiple.



- **Langue** – définissez la langue des textes affichés sur l'écran. Unes des langues prédéfinies peut être sélectionnée : anglais, tchèque, allemand, italien, français, espagnol, russe, finnois, danois, polonais, néerlandais, portugais, turc, norvégien, suédois ou une langue personnalisée (custom).
- **Donner la priorité aux icônes et non au texte** – les icônes à l'écran seront préférées au texte.
- **Lors d´économie d'énergie** – activez le mode économie d'énergie avec lequel la luminosité de l'écran est réduite. Si aucun événement ne se produit pendant le délais d'activation de l'écran du diaporama, le mode économie d'énergie a bien été activé. Définissez 0 dans le délai d'activation de l'écran Diaporama pour désactiver le mode économie d'énergie. Tout mouvement devant la caméra d'interphone ou tout événement d'affichage (tel que l'activation du verrouillage de la porte ou le toucher de l'écran) rétablit toute la luminosité de l'écran.
- **Masquer les utilisateurs inactifs** – si cette option est cochée, l'utilisateur dont le profil temporel est actif ce qui l'empêche d'être contacté, est automatiquement masqué.
- **Mode de démonstration** – définit si l'équipement passe en mode de démonstration lorsqu'il est inactif. Il est possible de choisir un autre comportement en mode de démonstration (Désactivé, Diaporama).
- **Retard du mode démo** – définit l'intervalle de temps d'inactivité de 1 à 600 secondes après lequel l'appareil passe en mode démonstration. Il y a toujours un délai fixe de 15 secondes avant que l'appareil ne retourne à la page d'accueil.

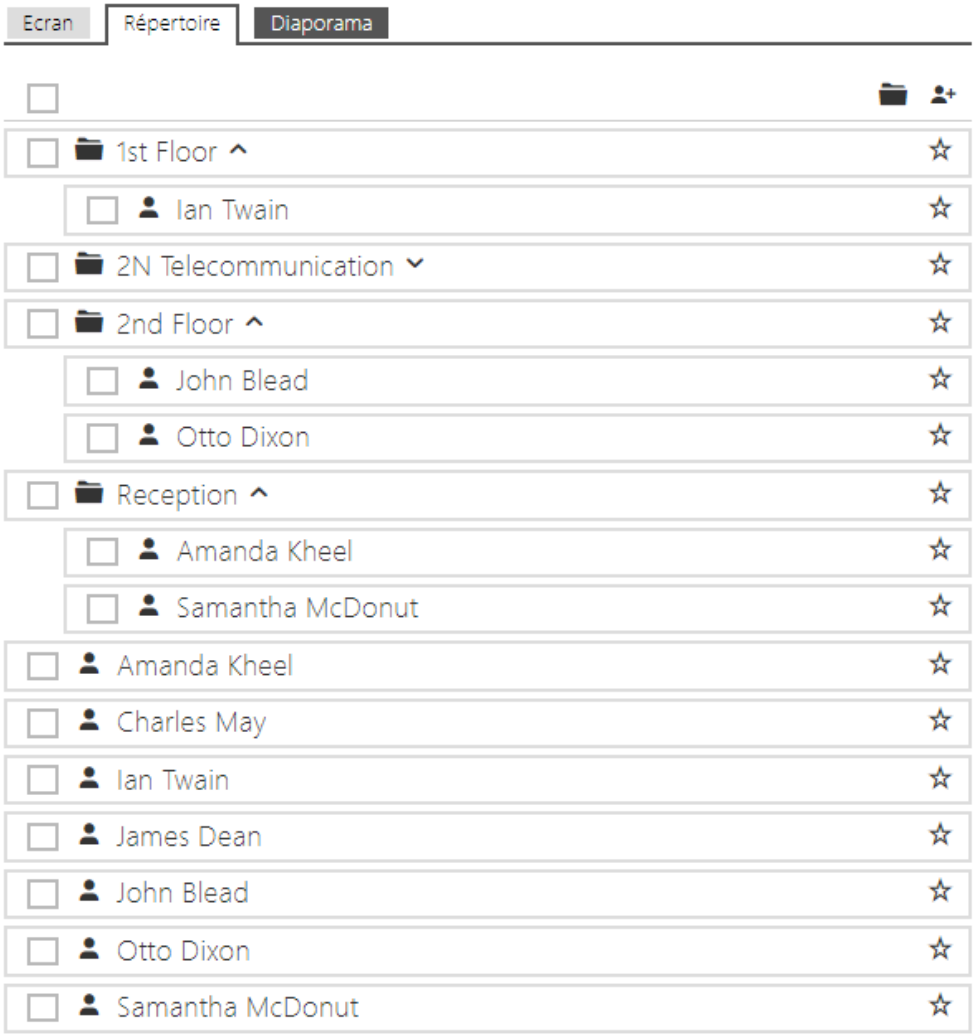


- **Langue originale** – téléchargez le modèle de fichier de localisation pour sa traduction. C'est un fichier XML avec tous les textes à afficher.
- **Langue de l'utilisateur** – enregistrez, supprimez et chargez un fichier de localisation de votre choix.

ⓘ Si aucune des langues prédéfinies ne vous convient, procédez comme indiqué ci-dessous :
- Téléchargez le fichier de langue d'origine (**anglais**).
- Modifiez le fichier en utilisant un éditeur de texte (remplacez les textes en anglais par les textes dans votre langue).

- Rechargez le fichier de localisation modifié sur l'interphone.
- Définissez les **paramètres de langue** | **Langue à personnaliser**.
- Vérifiez et corrigez si nécessaire les textes sur l'écran de l'interphone.

Répertoire (pour les modèles 2N® IP Verso et 2N® IP Vario)



Cet onglet vous permet de configurer une liste d'utilisateurs structurée. Vous pouvez créer pratiquement n'importe quel nombre de groupes et affecter n'importe quel nombre d'utilisateurs à chacun de ces groupes. Il n'est pas possible d'affecter un utilisateur plus d'une fois dans un même groupe mais un utilisateur peut faire partie de plusieurs groupes différents.

Les dossiers et les utilisateurs créés sont affichés sur la gauche. Cliquez sur pour ajouter un nouveau dossier. Cliquez sur pour supprimer un groupe ou un utilisateur du répertoire. Cliquez sur pour renommer un groupe. Cliquez sur pour déplacer un utilisateur de la liste principale vers un dossier.

Les utilisateurs affectés au groupe sélectionné sont affichés sur la droite. Cliquez sur pour ajouter un utilisateur à un groupe. L'utilisateur restera dans la liste principale après avoir été assigné au groupe. Cliquez sur pour le supprimer.

Les groupes et les utilisateurs sont classés par ordre alphabétique sur l'écran. Cliquez sur pour leur assigner une priorité. Les éléments du répertoire ont 8 priorités possibles. La priorité 1 place l'élément en tête de liste, l'absence de priorité le place en fin de liste. Si plusieurs éléments ont la même priorité, ils sont regroupés et triés par ordre alphabétique.

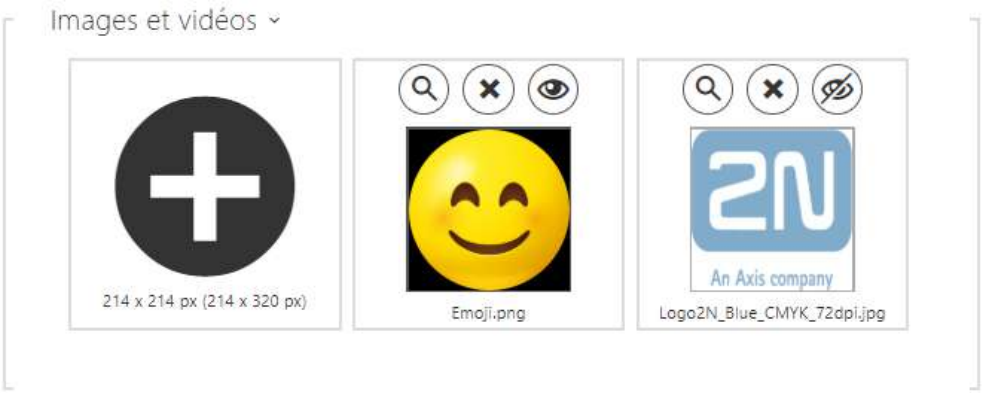
Caution

- N'oubliez pas de sauvegarder les changements sur le répertoire.

Diaporama sur les modèles 2N® IP Verso

La liste des images et des vidéos affichées en mode présentation est définie sur cet onglet. Jusqu'à 8 images/vidéos peuvent être téléchargées, qui défilent séquentiellement avec un délai défini.

- **Intervalle de transition** – définissez le temps d'affichage de chaque image avant de passer à l'image suivante.
- **Profil horaire** – choisissez un ou plusieurs profils horaires à appliquer. Définissez les profils horaires dans la section **Répertoire / Profils horaires**.
  - sélectionnez l'un des profils prédéfinis ou définissez manuellement le profil temporel pour un élément donné.



La résolution des images/vidéos téléchargées devrait être de 214 x 214 ou 214 x 320 pixels pour une taille maximale de 2 MB. Les autres tailles seront automatiquement ajustées à la résolution de l'écran.

Cliquez sur l'icone pour visualiser l'image chargée, appuyez sur pour effacer l'image et cliquez sur pour cacher une image ou une vidéo sur l'écran de l'appareil. L'affichage peut être conditionné par un profil temporel en cliquant sur une icône variable de l'image ou de la vidéo. Si le profil temporel n'est pas actif, la présentation ne contiendra pas de contenu conditionné par le profil temporel. Dans le même cas, la présentation contiendra toujours un contenu qui n'est pas conditionné par le profil temporel. Si aucune image n'est chargée, le mode Diaporama ne sera jamais activé.

Tip

- Pour cacher le texte “Toucher pour démarrer” sur l'écran du **2N® IP Verso**, chargez une image de résolution 214 x 320 pixels.

Observation

- Les versions FW inférieures à 2.35 ne peuvent pas télécharger de vidéos avec une résolution de 214 x 320.

Diaporama sur les modèles 2N® IP Vario

Cet onglet vous aide à configurer une liste d’images à afficher en mode Diaporama. Téléchargez jusqu'à 8 images à afficher avec un délai prédéfini.

- **Intervalle de transition** – définissez le temps d'affichage de chaque image avant de passer à l'image suivante.

La résolution des images enregistrées devrait être de 320 x 240 pixels. Les autres tailles seront automatiquement ajustées à la résolution de l'écran.

Cliquez sur l'icone pour visualiser l'image chargée, appuyez sur pour effacer l'image et cliquez sur pour cacher une image ou une vidéo sur l'écran de l'appareil.

Si aucune image n'est chargée, le mode Diaporama ne sera jamais activé.

Observation

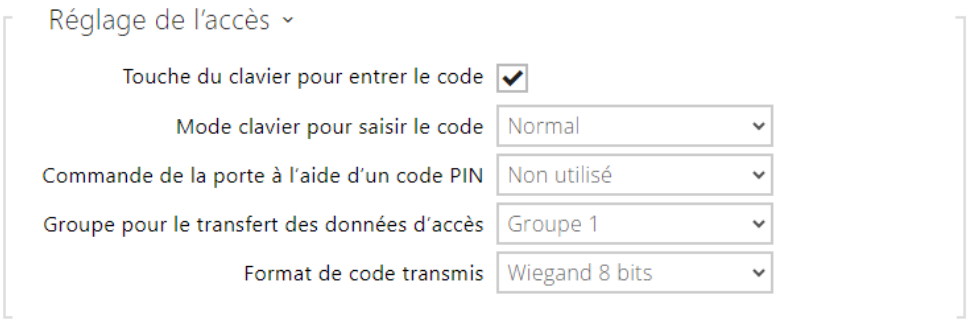
- L'écran du **2N® IP Vario** ne supporte que les images

5.5.6.1 Ecran 2N® IP Style

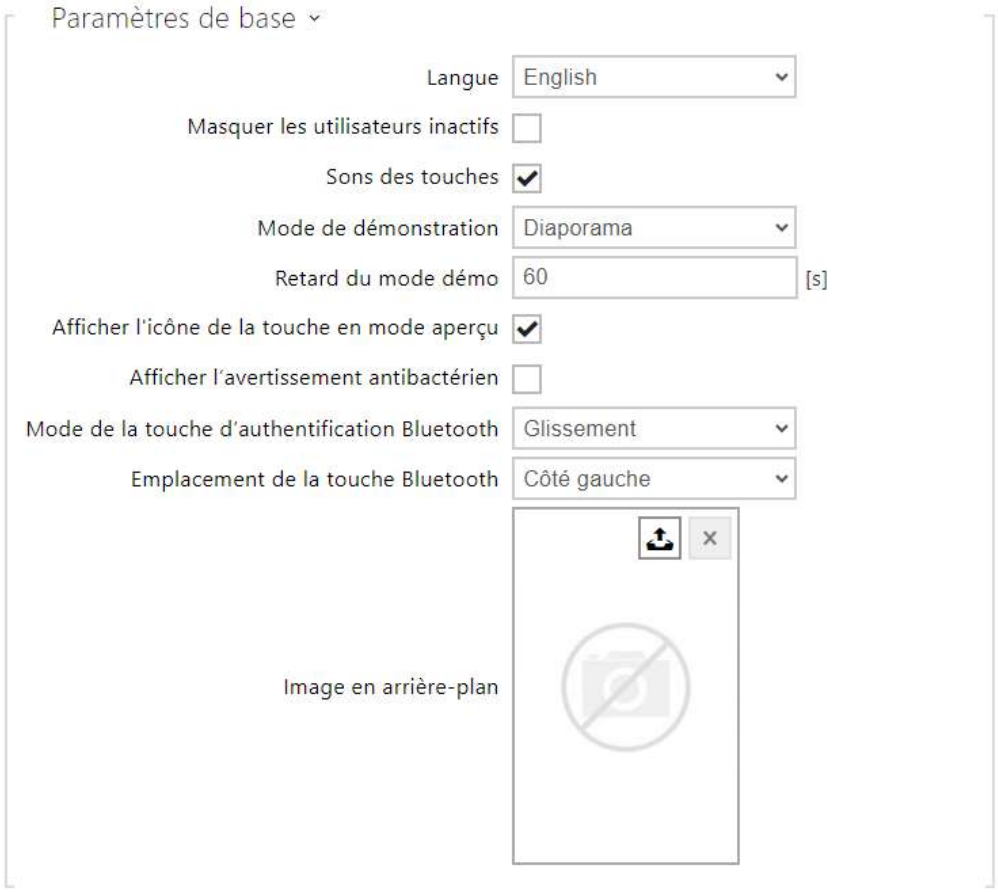
Interphone 2N IP - **2N® IP Style** est doté d'un écran LCD couleur 10'' avec une résolution de 800 x 1280. L'état de l'appareil est affiché (progression de l'appel, ouverture de la porte, etc.) et les modes suivants sont disponibles :

- **Affichage** – affiche le répertoire contenant les utilisateurs pouvant être contactés et un clavier numérique pour l'accès avec un code.
- **Diaporama** – après une période d'inactivité définie, une présentation peut être affichée à l'écran sous forme d'un ensemble d'images téléchargées. Le temps avant l'affichage automatique peut être configuré.
- **Logo** – après une période d'inactivité définie, le logo téléchargé dans la configuration de l'appareil peut être affiché à l'écran.
- **Adresse** – après une période d'inactivité définie, l'écran peut afficher l'adresse et le numéro de la maison ou un autre identifiant de localisation.
- **Date et heure** – permet le paramétrage des données, de l'heure et des conditions météorologiques.
- **Message d'accueil** – permet de définir le message qui s'affiche à l'écran après une authentification réussie.

Ecran



- **Touche du clavier pour entrer le code** – active l'affichage du clavier à l'écran pour saisir les codes numériques.
- **Mode clavier pour saisir le code** – définit le mode clavier à l'écran pour saisir les codes numériques. Les modes sont le clavier normal ou le clavier avec des touches mélangées pour plus de sécurité. Le paramètre s'applique également au clavier pendant l'authentification multiple.
- **Commande de la porte à l'aide d'un code PIN** – autorise ou interdit le contrôle de la porte en entrant un code PIN à partir de l'écran.
- **Groupe pour le transfert des données d'accès** - vous permet de définir un groupe auquel tous les codes d'accès utilisateur reçus seront transférés.
- **Format de code transmis** – sélectionnez un format 4 bits ou 8 bits (sécurité supérieure) pour les codes à transmettre.



- **Langue** – définissez la langue des textes affichés sur l'écran. Unes des langues prédéfinies peut être sélectionnée : anglais, tchèque, allemand, italien, français, espagnol, russe, finnois, danois, polonais, néerlandais, portugais, turc, norvégien, suédois ou une langue personnalisée (custom).
- **Masquer les utilisateurs inactifs** – si cette option est cochée, l'utilisateur dont le profil temporel est actif ce qui l'empêche d'être contacté, est automatiquement masqué.
- **Sons des touches** – active la signalisation sonore des touches sur l'écran
- **Mode de démonstration** – définit si l'équipement passe en mode de démonstration lorsqu'il est inactif. Il est possible de choisir un autre comportement en mode de démonstration (Désactivé, Diaporama, Logo, Adresse, Date et heure).
- **Retard du mode démo** – définit le temps d'inactivité après lequel l'équipement passe en mode de démonstration dans une envergure comprise entre 1 et 600 secondes.

Observation

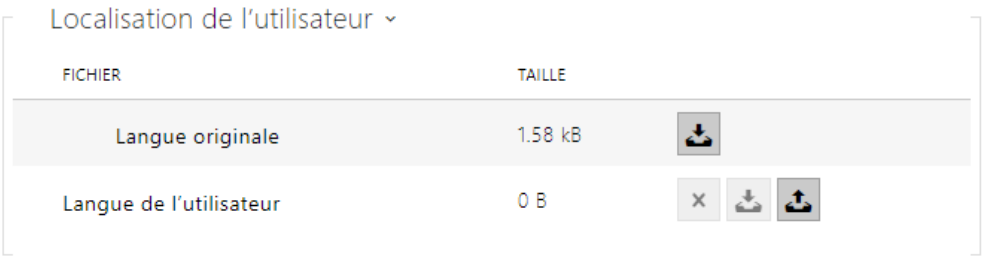
- L'équipement dispose d'une option fixe d'affichage de l'écran d'accueil après 60 secondes d'inactivité. Une fois ce délai écoulé, le temps défini dans le présent paramètre entame un décompte puis le dispositif passe en mode de démonstration.

- Après 2 minutes d'inactivité, l'économiseur d'écran se déclenche sur l'appareil **2N® IP Style,** pendant lequel la luminosité de l'écran est alternativement réduite et augmentée à intervalles de 20 secondes. L'économiseur est interrompu par une touche sur l'écran, une tentative d'accès, un appel entrant, une notification sur l'écran ou une détection de mouvement, même si la fonction de détection de mouvement n'est pas autorisée. Si l'économiseur d'écran fonctionne en arrière-plan du mode démonstration, le fait de quitter l'économiseur d'écran en le touchant fera également passer l'appareil à la page d'accueil.

- **Autoriser l´icône de la touche en mode de démonstration** – autorise l´affichage de l´icône de la touche (main pulsée) en mode de démonstration.
- **Afficher l'avertissement antibactérien** – permet d'afficher l'information sur la couche antibactérienne appliquée sur l'écran (accessoire optionnel pour 2N® IP Style) pendant le temps où l'appareil est en mode démonstration.
- **Mode de la touche d'authentification Bluetooth** – définit si le bouton d'activation de l'authentification Bluetooth est activé par glissement ou par toucher. Les paramètres ne prendron effet que lorsqu'aucun téléphone équipé de l'application Mobile Key ne se trouvera à proximité de **2N® IP Style**.
  - **Glissement** – pour fermer le verrou, faire glisser la touche de gauche à droite sur l'écran.
  - **Contact** – appuyer sur la touche pour enclencher le verrou.
- **Emplacement de la touche Bluetooth** – définit l'emplacement du bouton d'authentification Bluetooth (WaveKey). Les paramètres ne prendront effet que lorsqu'aucun téléphone équipé de l'application Mobile Key ne se trouvera à proximité d'IP Style.
- **Image en arrière-plan** – permet de télécharger une image en arrière-plan (utilisée sur des affichages divers à l'écran). Le fichier doit être une image avec une résolution d'au moins 800 x 1280 pixels. Les images en haute résolution seront réduites.

Caution

- Les modifications de l'affichage du dossier racine apparaissent à l'écran une fois accédé au menu de recherche ou de numérotation.
- Pour modifier l'emplacement et le mode d'authentification de la touche Bluetooth à l'écran, déconnecter tous les équipements disponibles avec l'authentification Bluetooth ou les mettre hors de portée de **2N® IP Style**.



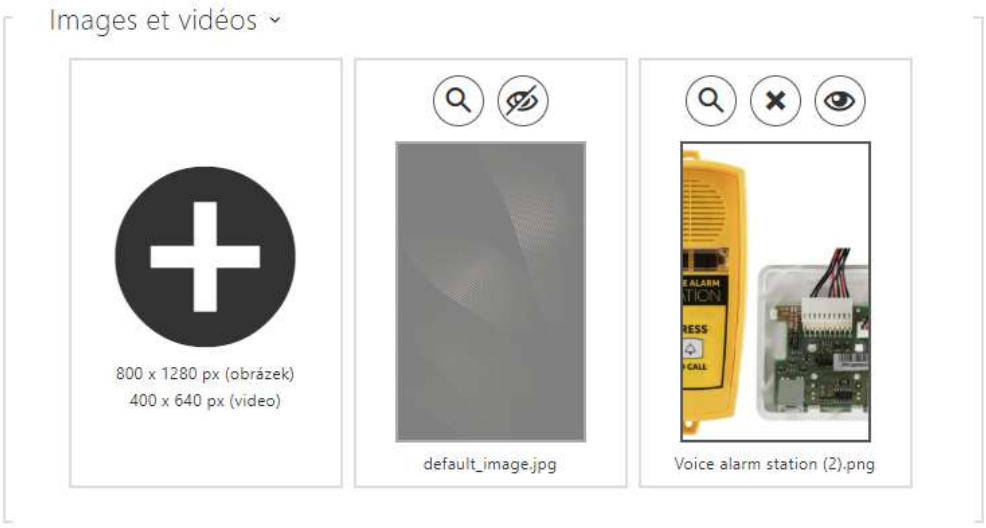
- **Langue originale** – téléchargez le modèle de fichier de localisation pour sa traduction. C'est un fichier XML avec tous les textes à afficher.
- **Langue de l'utilisateur** – enregistrez, supprimez et chargez un fichier de localisation de votre choix.

> ⓘ Si aucune des langues prédéfinies ne vous convient, procédez comme indiqué ci-dessous :
>
> - Téléchargez le fichier de langue d'origine (**anglais**).
> - Modifiez le fichier en utilisant un éditeur de texte (remplacez les textes en anglais par les textes dans votre langue).
> - Rechargez le fichier de localisation modifié sur l'interphone.
> - Définissez les **paramètres de langue** | **Langue à personnaliser**.
> - Vérifiez et corrigez si nécessaire les textes sur l'écran de l'interphone.

Diaporama

Cet onglet vous aide à configurer une liste d'images à afficher en mode Diaporama. Jusqu'à 14 images/vidéos peuvent être téléchargées, qui défilent séquentiellement avec un délai défini.

- **Intervalle de transition** – définissez le temps d'affichage de chaque image avant de passer à l'image suivante.
- **Profil horaire** – choisissez un ou plusieurs profils horaires à appliquer. Définissez les profils horaires dans la section **Répertoire / Profils horaires**.
  - sélectionnez l'un des profils prédéfinis ou définissez manuellement le profil temporel pour un élément donné.



Assurez-vous que la résolution de l'image est de 800 x 1280 pixels pour le **2N® IP Style**. Les autres tailles seront automatiquement ajustées à la résolution de l'écran.

Les fichiers vidéo doivent avoir une résolution de 400 x 640 px, une taille maximale de 7 MB et un framerate maximal de 24 fps.

Cliquez sur l'icône pour visualiser l'image chargée, appuyez sur pour effacer l'image et cliquez sur pour cacher une image ou une vidéo sur l'écran de l'appareil. L'affichage peut être conditionné par un profil temporel en cliquant sur une icône variable de l'image ou de la vidéo. Si le profil temporel n'est pas actif, la présentation ne contiendra pas de contenu conditionné par le profil temporel. Dans le même cas, la présentation contiendra toujours un contenu qui n'est pas conditionné par le profil temporel. Si aucune image n'est chargée, le mode Diaporama ne sera jamais activé.

Observation

- Les échantillons « Diaporama » n'apparaissent à l'écran qu'en autorisant le mode donné dans le menu Matériel / Affichage / Affichage.

Logo

Permet de télécharger un logo pour le mode démo. Une image avec une résolution supérieure à 800 x 1 280 pixels sera réduite. Un plus petit fichier restera petit et n'occupera pas toute la surface. Les images en format PNG avec un arrière-plan transparent sont elles aussi prises en charge.

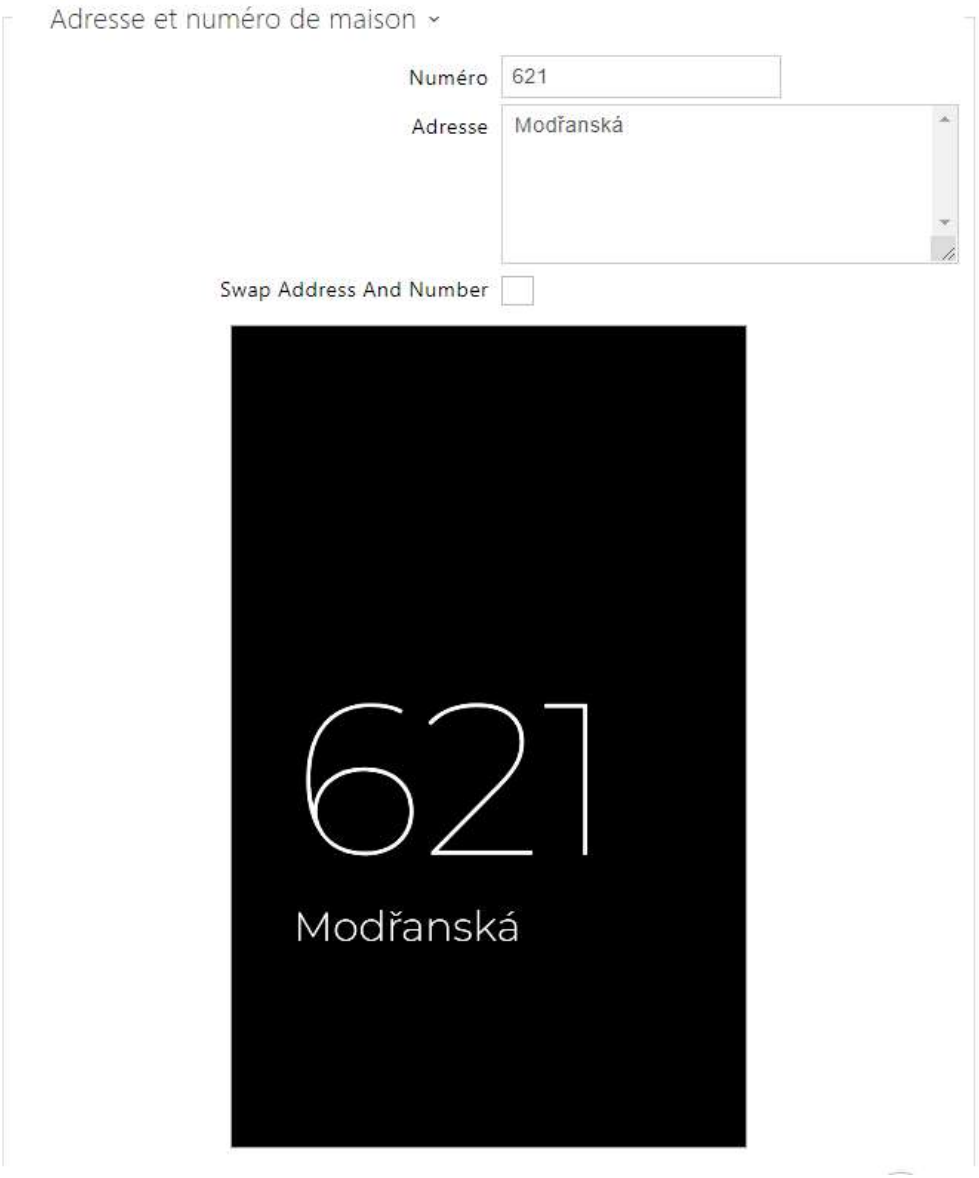

Logo du mode de démonstration

Observation

- La démonstration « Logo » n'apparaît à l'écran qu'en autorisant le mode donné dans le menu Matériel / Affichage / Affichage.

Adresse

Permet de définir une adresse ou un autre identifiant du domicile pour le mode de démonstration qui sera affiché à l'écran lorsque l'équipement est inactif.



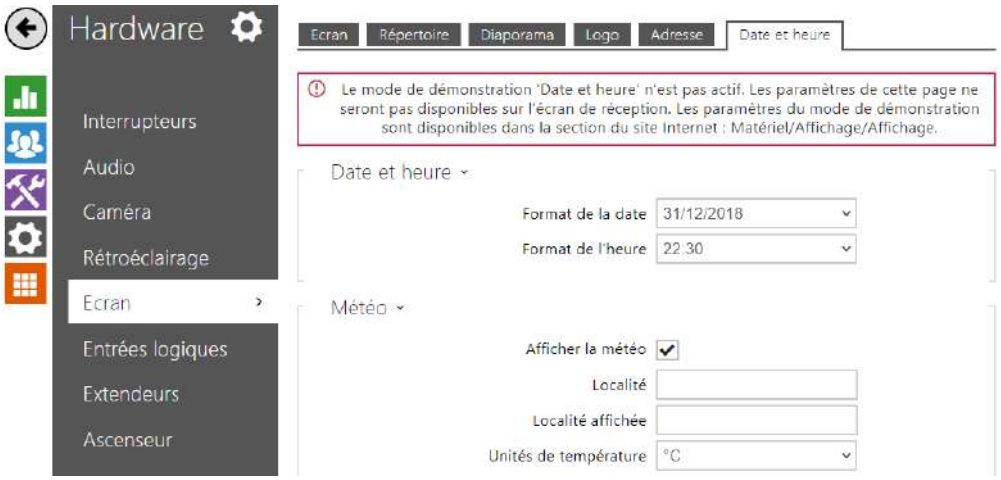
- **Numéro** – permet de saisir le numéro de maison ou toute autre identification conforme aux habitudes locales. S’affiche en mode de démonstration lorsque l’option Adresse est sélectionnée.
- **Adresse** – permet de saisir l’adresse, le nom du bâtiment, etc. affichés en mode de démonstration lorsque l’option Adresse est sélectionnée.
- **Intervertir l’adresse et le numéro** – échange l’ordre dans lequel les numéros et les adresses sont affichés.

Observation

- La démonstration « Adresse » n'apparaît à l'écran qu'en autorisant le mode donné dans le menu Matériel / Affichage / Affichage.

Date et heure

Permet le paramétrage des données, de l'heure et des conditions météorologiques.



- **Format de la date** – configuration du format de la date affichée sur l'écran de l'appareil.
- **Format de l'heure** – configuration du format de l'heure affichée sur l'écran de l'appareil.

Météo

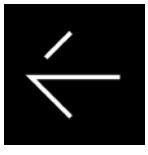
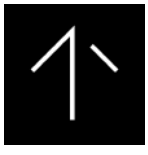
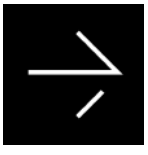
- **Afficher la météo** – sur l'écran de l'appareil s'afficheront les informations relatives à la météo actuelle.
- **Localité** – localité dans laquelle se trouve l'appareil pour les prévisions météorologiques. Quand elle n'est pas remplie, la localité définie est utilisée automatiquement.
- **Localité affichée** – localité affichée sur l'écran Si elle n'est pas remplie, la localité s'affiche selon la prévision météorologique.
- **Unités de température** – choix de l'unité de température affichée sur l'écran Possibilités en °C ou °F.

Message d'accueil

	
Image personnaliseé	Message textuel

Permet de définir le message qui s'affiche à l'écran après une authentification réussie.

- **Mode écran d'accueil** – sélectionnez le type de contenu du message d'accueil.
- **L'heure d'affichage** – définit la durée pendant laquelle l'appareil affiche le message d'accueil.
- **Icône** – sélectionnez l'icône du message d'accueil textuel :

 Info	 Observation	 Accès interdit
 Flèche vers la gauche	 Flèche vers le haut	 Flèche vers la droite

		
Flèche pour tourner à gauche	Flèche vers le bas	Flèche pour tourner à droite

- **Titre du message** – définit le titre du message d'accueil textuel.
- **Corps du message** – définit le corps du message d'accueil textuel.
- **Confirmation** – définit si le message d'accueil textuel comporte un bouton de confirmation "OK".
- **Télécharger une image personnalisée** – permet de télécharger une image qui sera affichée comme le message d'accueil. L'image doit avoir une résolution de 800 x 1280 px et être au format JPEG ou PNG.

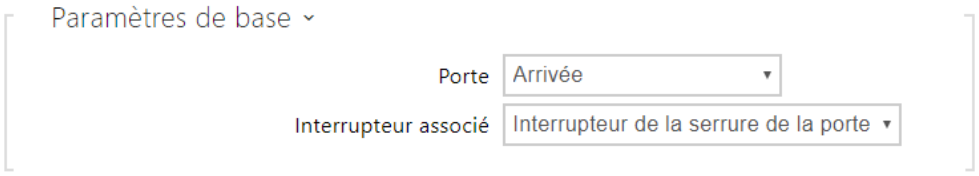
5.5.7 Lecteur de carte

Cette onglet est disponible sur les modèle **2N® IP Base**, **2N® IP Vario** et **2N® IP Force**. Sur le modèle **2N® IP Verso** seule l'option permettant de limiter les tentatives d'accès infructueuses est configurée ici. Les autres options de lecteur de carte seront configurées dans le menu **Extendeurs**.

Le lecteur de carte vous aide à contrôler efficacement l'accès à votre bâtiment à l'aide de cartes RFID sans contact. Les types de carte pris en charge dépendent du modèle de lecteur de carte utilisé.

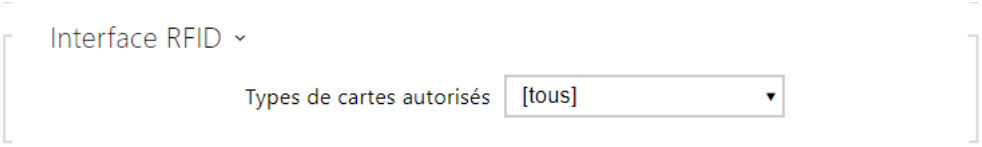
Les lecteurs de carte du **2N® IP Vario** et du **2N® IP Force** sont d'équipés d'une interface Wiegand en Entrée / Sortie. La direction de l'interface Wiegand est configurable. En mode saisie, l'interface peut être utilisée pour la connexion de lecteurs de cartes externes, de lecteurs d'empreintes digitales, de lecteurs de données biométriques…etc. En mode sortie, l'interface permet de connecter l'interphone à un dispositif de contrôle d'accès tiers, il vous est alors possible d'envoyer les identifiants des cartes badgés sur le lecteur vers un Contrôleur de porte par exemple.

Paramètres de base



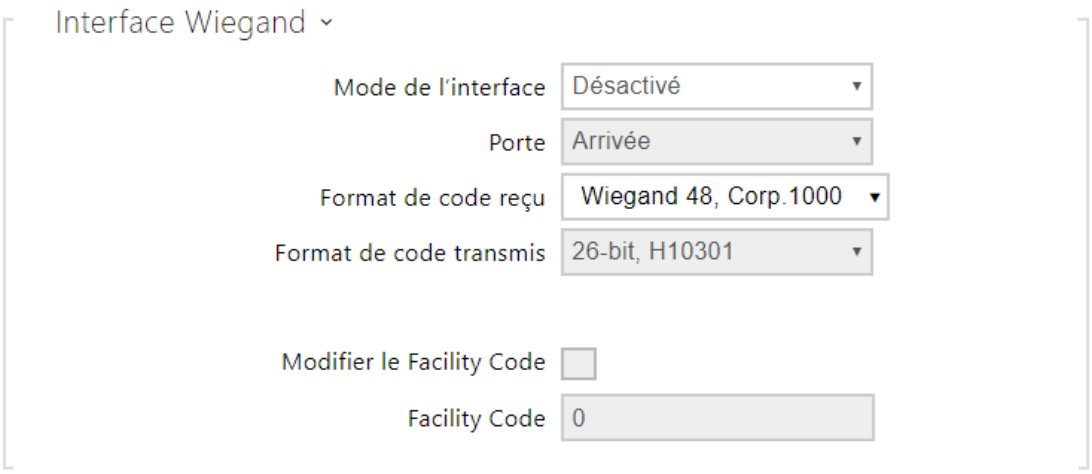
- **Porte** – définissez la direction du lecteur (Arrivée, Départ). Cela permet de gérer le temps de présence par exemple.
- **Interrupteur associé** – définissez l'interrupteur à activer après la lecture d'une carte RFID valide. La valeur définie n'est pas appliquée lorsqu'une carte d'utilisateur valide est badgée sur le lecteur et que le mode d'authentification double est activé. Dans ce cas, un code d'activation numérique est requis pour activer l'interrupteur.

RFID Interface



- **Types de cartes autorisés** – sélectionnez un ou plusieurs types de cartes à accepter. Si aucune sélection n'est effectuée, tous les types de cartes prises en charge sont acceptés.

Interface Wiegand

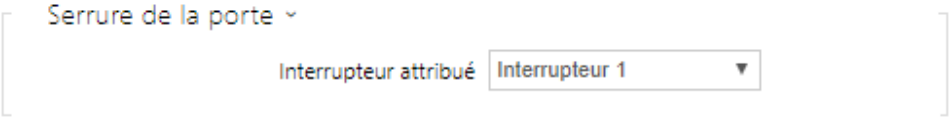


- **Mode de l'interface** – activez la fonction Wiegand et réglez le mode Entrée / Sortie. Les identifiants des cartes badgées sur le lecteur de carte interne sont toujours renvoyés vers Wiegand OUT.
- **Porte** – définissez la direction du lecteur (Arrivée, Départ). Cela permet de gérer le temps de présence par exemple.
- **Format de code reçu** – définissez le format des codes à recevoir (Wiegand 26, 32, 37 et RAW).
- **Format de code transmis** – définissez le format des codes à transmettre (Wiegand 26, 32, 37 et RAW).
- **Modifier le Facility Code** – définissez la première partie du code via Wiegand. Ceci s'applique au Wiegand en sortie pour le format de code 26 bits. Contactez votre fournisseur de système de sécurité pour savoir si ce code est demandé.
- **Facility Code** – définissez l'emplacement de l'interphone IP 2N dans le système de sécurité. Entrez une valeur décimale pour l'emplacement (0–255).

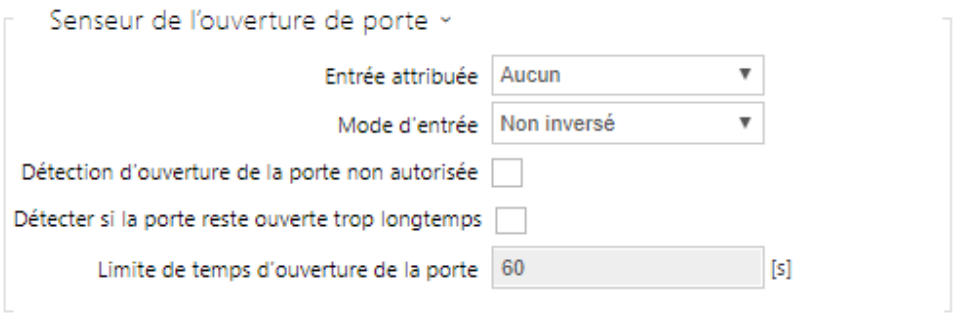
5.5.8 Entrées logiques

Dans cette section de configuration, définissez les paramètres associés aux entrées logiques et leurs interconnexions avec d'autres fonctionnalités de l'interphone. Les entrées logiques sont disponibles sur certains modèles d'interphone ou lorsqu'un équipement approprié est installé (équipés d'un lecteur).

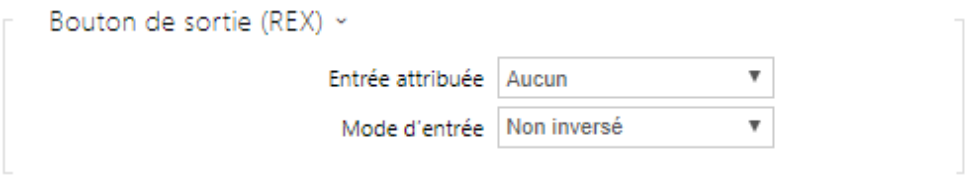
Porte



- **Interrupteur attribué** – il vous permet de sélectionner un interrupteur conçu pour contrôler la serrure électromagnétique de la porte. L'état de l'interrupteur est lié à la signalisation de déverrouillage de la porte (pictogramme de porte vert, voyant vert).

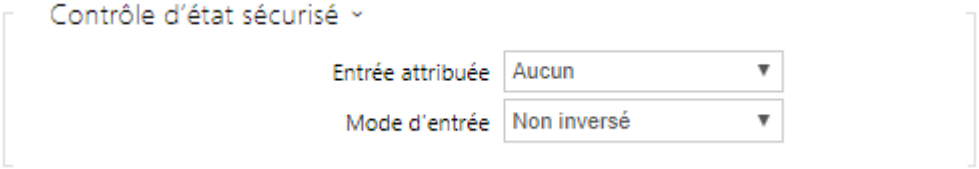


- **Entrée attribuée** – permet de sélectionner une des entrées logiques (éventuellement aucune entrée) pour la détection de portes ouvertes.
- **Mode d'entrée** – permet de régler le statut (la polarité) de l'entrée. Inversé ou Non inversé.
- **Détection d'ouverture de la porte non autorisée** – détecter l'ouverture de la portes lorsque le verrou est fermé.
- **Détecter si la porte reste ouverte trop longtemps** – détecter si la porte reste ouverte trop longtemps.
- **Limite de temps d'ouverture de la porte** – durée maximale de l'ouverture de porte.



- **Entrée attribuée** – permet de définir l'une des entrées logiques (ou pas d'entrée) pour que celle-ci fonctionne comme bouton de sortie. L'activation de l'entrée du bouton de sortie entraine l'activation de l'interrupteur sélectionné. La durée et la méthode d'activation sont définies par les paramètres de l'interrupteur sélectionné.
- **Mode d'entrée** – permet de régler le statut (la polarité) de l'entrée : Inversé ou Non inversé.

Sécurité



- **Entrée attribuée** – définissez l'une (ou aucune) des entrées logiques pour la détection de l'état sécurisé. L'état sécurisé est ensuite signalisé par une LED sur l'interphone, dont l'emplacement peut varier selon le type d'interphone.
- **Mode d'entrée** – réglez le mode d'entrée actif (polarité).

Note

- *La signalisation d'état sécurisé est généralement utilisée avec un PBX de sécurité connecté à l'une des entrées logiques de l'interphone. Le fil provenant du PBX est connecté à l'interphone directement ou via un module d'extension. L'emplacement de la LED d'état sécurisée est variable en fonction du type d'interphone :*

  *Les interphones **2N® IP Vario** (91371…U) sont équipés d'une LED rouge située au milieu des étiquettes de nom rétroéclairées.*
  *Les interphones **2N® IP Force** sont équipés d'une LED rouge située dans la fenêtre du lecteur de carte intégré.*
  *Les interphones **2N® IP Verso** sont équipés d'un pictogramme cadenas rouge dans le coin supérieur gauche du module de base.*

Les modèles équipés d'un commutateur d'autoprotection permettent la détection de l'ouverture de l'interphone par la force **TamperSwitchActivated**. Les événements sont enregistrés dans un journal d'évènement et lus via l'API HTTP (voir le manuel de **l'API HTTP**).

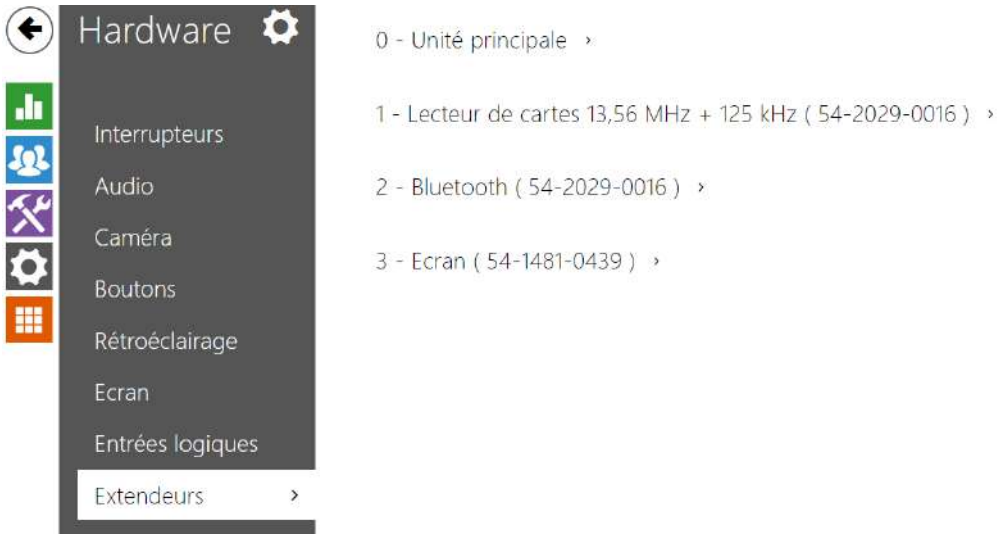
Si la fonction d'autoprotection est activée, tous les interrupteurs seront automatiquement bloqués. Le blocage reste actif même après le redémarrage de l'appareil. Chaque port peut être contrôlé via l' **Automatisation**. Pressez le bouton de déblocage ou effectuez un redémarrage usine pour débloquer les interrupteurs.

- **Entrée attribuée** – sélectionnez l'entrée logique à laquelle le commutateur d'autoprotection doit être connecté. L'évènement **TamperSwitchActivated** signal l'activation de l'autoprotection.
- **Autoriser le blocage automatique des interrupteurs** – l'activation du commutateur d'autoprotection bloque les interrupteurs pendant une durée de 30 minutes.
- **État du blocage des interrupteurs** – permet de connaitre le statut des interrupteurs.

Déclencheurs

- **Déclencheur des actions utilisateur 1, 2**
  - **Entrée attribuée** – permet de sélectionner une entrée logique qui remplira la fonction d'une action utilisateur. Si la fonction est activée, l'événement UserActionActivated est inscrit sur la liste des événements du dispositif avec le paramètre state=in (la désactivation de la fonction est indiquée par state=out). Sur la base de cet événement, les systèmes supérieurs par exemple peuvent déclencher une alarme, verrouiller l'ensemble du bâtiment ou effectuer une toute autre action.
  - **Mode d'entrée** – détermine si l'action utilisateur sera évaluée sur la base de la valeur inverse de l'entrée assignée ou de la valeur normale.

5.5.9 Extendeurs



Les interphones **2N® IP Verso** et **2N® IP Style** peuvent être étendus grâce à des modules dits d'extension connectés à l'unité d'interphonie de base via le bus VBUS. Les modules suivants sont disponibles :

- Module 5 boutons
- Module Clavier mécanique
- Module Info
- Module Lecteur de carte

- Bluetooth
- Module E/S (Entrée / Sortie)
- Module Wiegand
- Module OSDP
- Module Boucle auditive
- Module Ecran tactile
- Module Lecteur biométrique
- Module Clavier capacitif
- Module Clavier capacitif & Lecteur RFID 125 kHz, 13.56 MHz
- Module Bluetooth & Lecteur RFID 125 kHz, 13.56 MHz
- Module Clavier capacitif & Bluetooth & Lecteur RFID 125 kHz, 13.56 MHz

Les modules sont interconnectés en chaîne. Chaque module a son numéro en fonction de sa position dans la chaîne (le premier module porte le numéro 1). L'unité de base est un type spécial de module (Module maître) et porte le numéro 0.

Il est possible de configurer chaque module séparément. Chaque paramètre est spécifique au type de module concerné.

Observation

- Le module connecté n'est pas détecté automatiquement. Redémarrez l'appareil pour visualiser le module connecté dans la liste des modules d'extension.
- Si les versions du firmware du module à connecter et de l'unité principale ne sont pas compatibles, le module ne sera pas détecté. Il est donc nécessaire de mettre à jour le firmware de l'appareil après avoir connecté les modules. Vous pouvez mettre à jour le firmware à l'aide de l'interface web de l'appareil dans la partie Système > Maintenance.

Observation

- Assurez-vous de configurer les modules remplacés. La configuration est liée au numéro de série du module.

Note

- *Les modules d'extension sont affichés dans l'ordre correspondant à leur interconnexion. Les modules connectés plus loin de l'unité de base sont énumérés ci-dessous. Si plusieurs modules du même type sont connectés à un seul interphone, il peut s'avérer difficile d'attribuer un paramètre à un module particulier (ex : bloc de boutons). Dans ce cas, identifiez les modules connectés à l'aide du bouton* ***Localiser le module****. Le module clignotera brièvement plusieurs fois lorsque vous appuierez sur le bouton.*

Observation

- Après avoir connecté le module avec Lecteur de cartes à un appareil sur lequel sont chargées des clés **2N® PICard**, vous devez jumeler le module avec l'appareil. Sans jumelage, le module de lecteur n'aura pas d'accès aux clés de lecture et ne sera pas en mesure de lire des cartes cryptées. Le jumelage du module se fait à l'aide du bouton **Jumeler le module.**

Observation

- Le nom du module doit être unique.
- Les modules sur lesquels il n'est pas possible de configurer de nom peuvent être identifié par leur position <module_position>.

Conseil

- Le passage du curseur de la souris sur l'image du module affiche les informations de base sur sa fabrication et son logiciel.

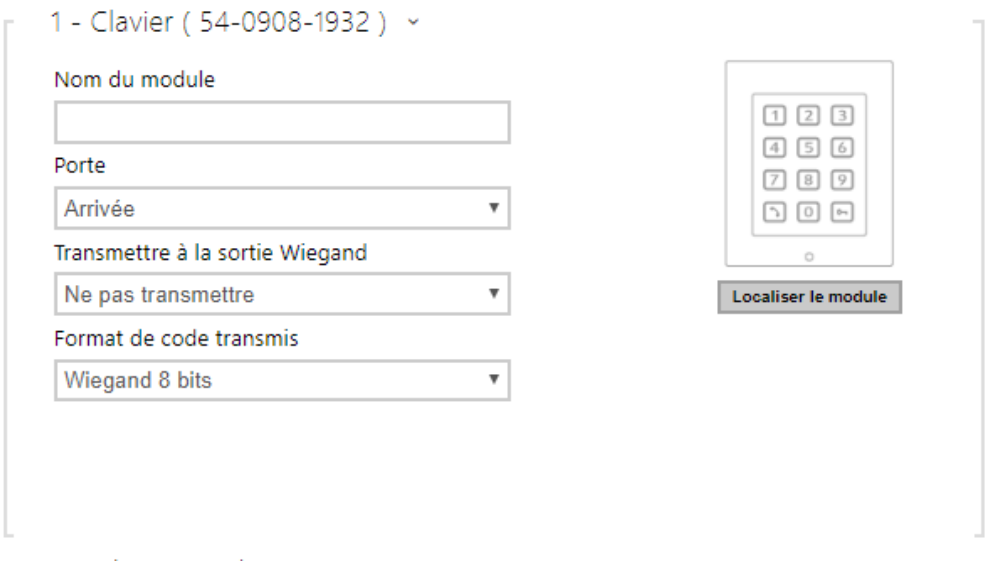
Configuration de l'Unité de base

- **Localiser l’appareil** – signalisation optique et acoustique d'un appareil. Remarque : la signalisation optique n'est possible que si l'appareil est équipé d'un rétroéclairage de contrôle (Verso, Base, Vario, Force, Safety et Uni). Si aucun haut-parleur n'est intégré à l'appareil, assurez-vous qu'un haut-parleur externe est connecté (Kit audio et kit vidéo) pour utiliser la signalisation sonore.

Configuration du Module Boutons

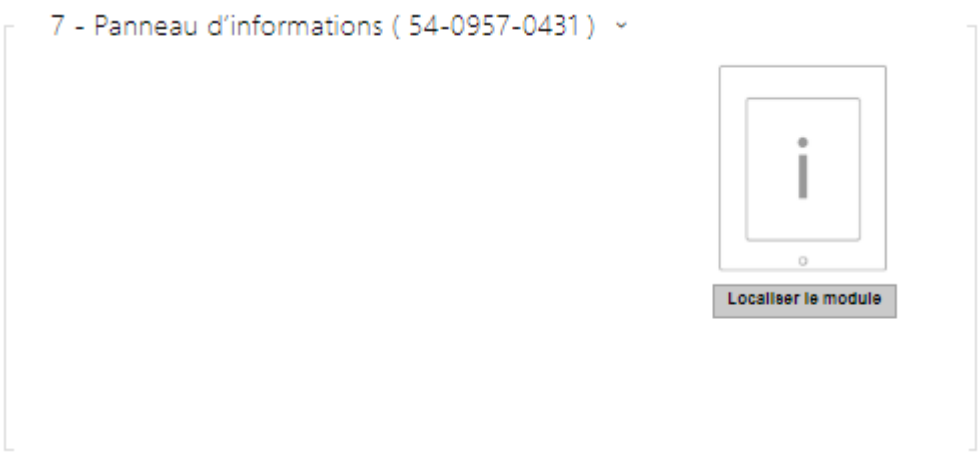
- **Fonctions des boutons** – assignez la position des utilisateurs aux boutons.

Configuration du Module Clavier



- **Nom du module** – définissez le nom du module pour l'enregistrement des événements à partir du clavier.
- **Porte** – définissez la direction du lecteur (Entrée / Sortie), pour le système de présence par exemple.
- **Transmettre à la sortie Wiegand** – définissez le groupe de sorties Wiegand auxquelles toutes les touches pressées doivent être transférées.
- **Format de code transmis** – sélectionnez un format 4 bits ou 8 bits (sécurité supérieure) pour les codes à transmettre.

Configuration Module Info



- aucun paramétrage n'est nécessaire sur ce module

Configuration Module Lecteur de cartes 125 kHz

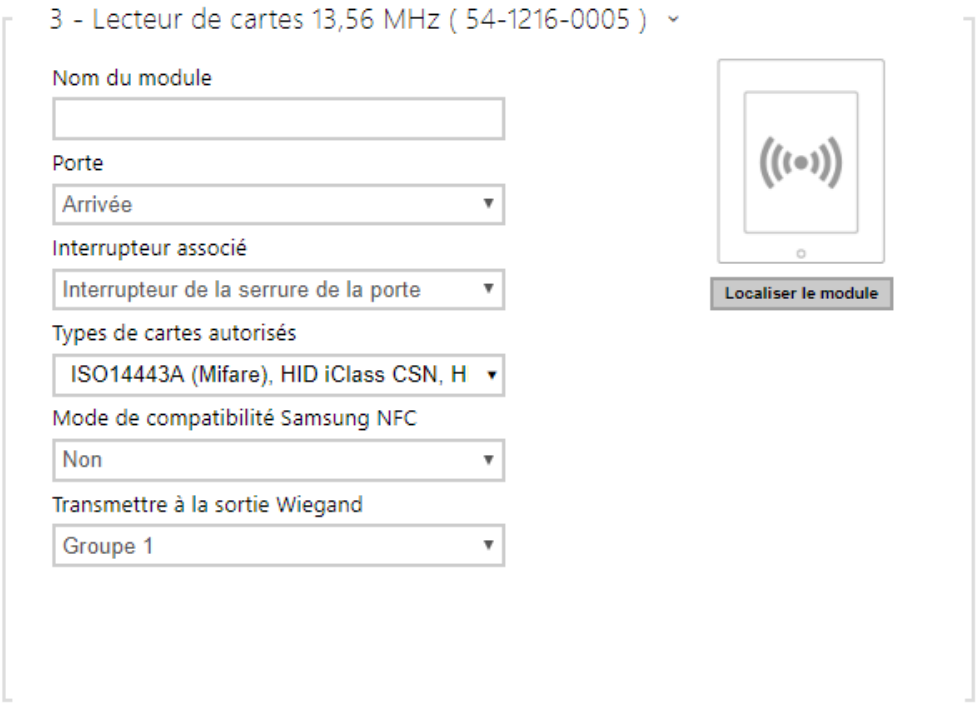
- **Nom du module** – définissez le nom du module pour le journal d'accès.
- **Porte** – définissez la direction du lecteur (entrée ou sortie) pour le système de présence.
- **Interrupteur associé** – réglez l'interrupteur pour qu'il soit activé après l'authentification de l'utilisateur via ce module. Si vous définissez l'interrupteur de verrouillage de porte et les règles d'authentification spécifiées dans Hardware / Porte.

- **Types de cartes autorisés** – définissez le type de carte pouvant être lu par le lecteur. Le lecteur de carte ne prend en charge qu'un seul type de carte à la fois.
- **Transmettre à la sortie Wiegand** – définissez un groupe de sorties Wiegand auxquelles tous les ID de cartes RFID reçus seront renvoyés.

Conseil

- Pour accélérer la lecture de la carte, il est recommandé de sélectionner les types de carte utilisés par l'utilisateur dans les paramètres du module.

Configuration Module Lecteur de cartes 13,56 MHz

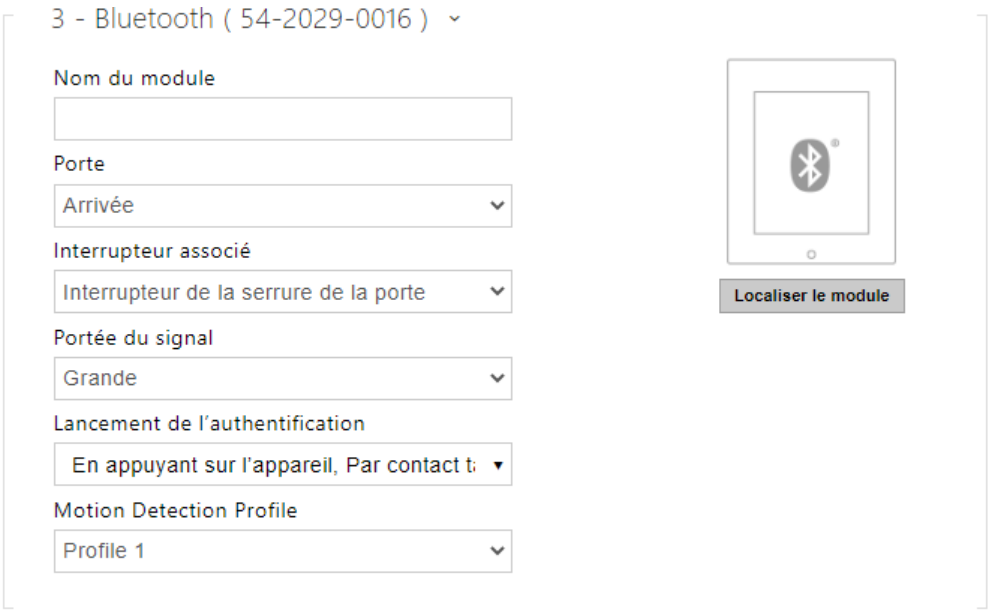


- **Nom du module** – définissez le nom du module pour le journal d'accès.
- **Porte** – définissez la direction du lecteur (entrée ou sortie) pour le système de présence.
- **Interrupteur associé** – réglez l'interrupteur pour qu'il soit activé après l'authentification de l'utilisateur via ce module. Si vous définissez l'interrupteur de verrouillage de porte et les règles d'authentification spécifiées dans Hardware / Porte.
- **Types de cartes autorisés** – définissez le type de carte pouvant être lu par le lecteur. Le lecteur de carte ne prend en charge qu'un seul type de carte à la fois.
- **Mode de compatibilité Samsung NFC** – activez la compatibilité NFC avec les Smartphones Samsung.
- **Transmettre à la sortie Wiegand** – définissez un groupe de sorties Wiegand auxquelles tous les ID de cartes RFID reçus seront renvoyés.

Conseil

- Pour accélérer la lecture de la carte, il est recommandé de sélectionner les types de carte utilisés par l'utilisateur dans les paramètres du module.

Configuration Module Bluetooth



- **Nom du module** – définissez le nom du module pour le journal d'accès. Le nom du module est utilisé lors de l'enregistrement des événements du module Bluetooth.
- **Porte** – définissez la direction du lecteur (entrée ou sortie) pour le système de présence.
- **Interrupteur associé** – réglez l'interrupteur pour qu'il soit activé après l'authentification de l'utilisateur via ce module. Si vous définissez l'interrupteur de verrouillage de porte et les règles d'authentification spécifiées dans Hardware / Porte.
- **Portée du signal** – définit la portée du signal (la valeur 5 représente la portée la plus longue, la valeur 1 la plus courte), c'est-à-dire la distance sur laquelle le module Bluetooth continuera à communiquer avec le téléphone portable. Lors de la mise en place, il est recommandé de tester la portée réelle du signal, qui dépend de plusieurs facteurs (notamment la disposition spatiale de l'installation, le téléphone portable utilisé et sa position).
- **Lancement de l'authentification** – définissez la méthode d'authentification pour un téléphone portable :
  - **Par contact tactile dans l'application** – l'authentification est effectuée en appuyant sur une icône dans l'application installée sur un Smartphone.
  - **En appuyant sur l'appareil** – appuyez sur le lecteur de carte muni d'un Smartphone doté de la clé **2N® Mobile Key** pour confirmer l'authentification.

  - **Détection des mouvements** – l'authentification sera déclenchée par la détection de mouvement en présence d'un téléphone avec l'application **2N® Mobile Key** jumelée.
- **Profil de détection de mouvement** – définit le profil de détection de mouvement que le module d'authentification par un téléphone portable doit suivre.

Configuration Module E / S

- **Nom du module** – définissez le nom du module Entrée / Sortie pour les spécifications des Evènements SetOutput, GetInput et InputChanged dans **l'interface d'Automatisation**.

Configuration Module Wiegand

Le module Wiegand est équipé d'interfaces d'entrée et de sortie Wiegand indépendantes les unes des autres, dotées de paramètres distincts et pouvant recevoir et envoyer des codes simultanément. L'entrée Wiegand vous aide à connecter des équipements tels que des lecteurs de cartes RFID, des lecteurs biométriques, etc. Avec la sortie Wiegand, vous pouvez connecter l'interphone au système de Contrôle d'accès de votre bâtiment, par exemple (pour envoyer des identifiants de cartes RFID ou des codes reçus sur n'importe quelle entrée Wiegand). Le **2N® Wiegand Isolator** est également équipé d'une entrée logique et d'une sortie logique, contrôlables via l'interface d'automatisation.

- **Nom du module** – définissez le nom du module Entrée / Sortie pour les spécifications des Evènements SetOutput, GetInput and InputChanged dans **l'interface d'Automatisation**.
- **Porte** – définissez la direction du lecteur (entrée ou sortie) pour le système de présence.
- **Interrupteur associé** – réglez l'interrupteur pour qu'il soit activé après l'authentification de l'utilisateur via ce module. Si vous définissez l'interrupteur de verrouillage de porte et les règles d'authentification spécifiées dans Hardware / Porte.
- **Format de code reçu** – définissez le format du code à recevoir (Wiegand 26, 32, 37 et RAW).
- **Sortie groupe Wiegand** – assignez la sortie Wiegand à un groupe auquel les codes des lecteurs de cartes connectés ou des entrées Wiegand peuvent être renvoyés.
- **Format de code transmis** – définissez le format du code à transmettre (26 bit, 32 bit, 37 bit, Format RAW, 35 bit, Corp. 1000, 48 bit, Corp. 1000 et Auto).
- **Modifier le Facility Code** – définissez la première partie du code via Wiegand. Ceci s’applique au Wiegand OUT pour le format de code 26 bits. Contactez votre fournisseur de système de sécurité pour savoir si le code d'installation est demandé.
- **Facility Code** – définissez l'emplacement du périphérique IP 2N dans le système de sécurité. Entrez une valeur décimale pour l'emplacement (0–255).

Configuration OSDP Wiegand

Le module OSDP est équipé d'une interface (entrée/sortie) OSDP (RS-485).Grâce à l'interface OSDP, l'interphone 2N IP peut être connecté, par exemple, au système de sécurité d'un bâtiment, au panneau de configuration (il est possible d'envoyer l'ID des cartes RFID attachées au lecteur RFID connecté, éventuellement les codes PIN).

- **Nom du module** – définit le nom du module. Le nom du module est utilisé pour spécifier une entrée ou une sortie dans les paramètres **Automation**.
- **Groupe pour le transfert des données d'accès** – affecte la sortie OSDP à un groupe auquel les codes des lecteurs de cartes connectés peuvent être transférés, éventuellement les entrées OSDP.
- **Format de code transmis** – définit le format des codes transmis.
- **Adresse OSDP** – adresse du module OSDP dans la plage 0-126 sur la ligne OSDP.
- **Débit en bauds** – réglage de la vitesse de communication en fonction du dispositif connecté.
- **Clé de chiffrement** – clé personnalisée pour la communication chiffrée.
- **Mode** – pour le réglage à distance de la clé de chiffrement sur la périphérie, si cette option est possible, le mode d'installation peut être utilisé. Après réception de la clé de chiffrement, passage automatique en mode normal. Un clignotement rapide de la LED de signalisation sur le module OSDP indique le mode d'installation.

- **Appliquer le chiffrement** – définir le chiffrement imposé uniquement pour les communications chiffrées.

> **Observation**
>
> - Si la communication du dispositif OSDP se fait en clair après que le chiffrement imposé a été défini, cette communication sera refusée.

Configuration Module Boucle auditive

- **Nom du module** – définit le nom du module. Le nom du module est utilisé lors de l'enregistrement des événements de la boucle d'induction.
- **Alimentation maximale** – définissez la puissance maximale de transmission de l'antenne de la boucle auditive. Une puissance de transmission plus élevée signifie une porté plus grande, mais moins de puissance pour les autres fonctionnalités de l'interphone. La valeur par défaut est 0,25 W dans des circonstances normales.

Configuration Module Ecran tactile

- **Nom du module** – définissez le nom du module pour le journal d'évènements.
- **Porte** – définissez la direction de l'écran (entrée ou sortie) pour le système de présence.
- **Groupe pour le transfert des données d'accès** - vous permet de définir un groupe auquel tous les codes d'accès utilisateur reçus seront transférés.
- **Format de code transmis** – sélectionnez un format 4 bits ou 8 bits (sécurité supérieure) pour les codes à transmettre.

Configuration Module Lecteur biométrique

- **Nom du module** – définissez le nom du module pour le journal d'évènements.
- **Porte** – définissez la direction du lecteur (entrée ou sortie) pour le système de présence.

- **Interrupteur associé** – réglez l'interrupteur pour qu'il soit activé après l'authentification de l'utilisateur via ce module. Si vous définissez l'interrupteur de verrouillage de porte et les règles d'authentification spécifiées dans Hardware / Porte.
- **Sunlight Sensitivity Mode** – en l'activant, on évite que le lecteur ne se comporte mal lorsqu'il est exposé à la lumière directe du soleil. Pour modifier les paramètres, l'appareil doit être redémarré. Le mode peut causer une réduction de la sensibilité de lecture.

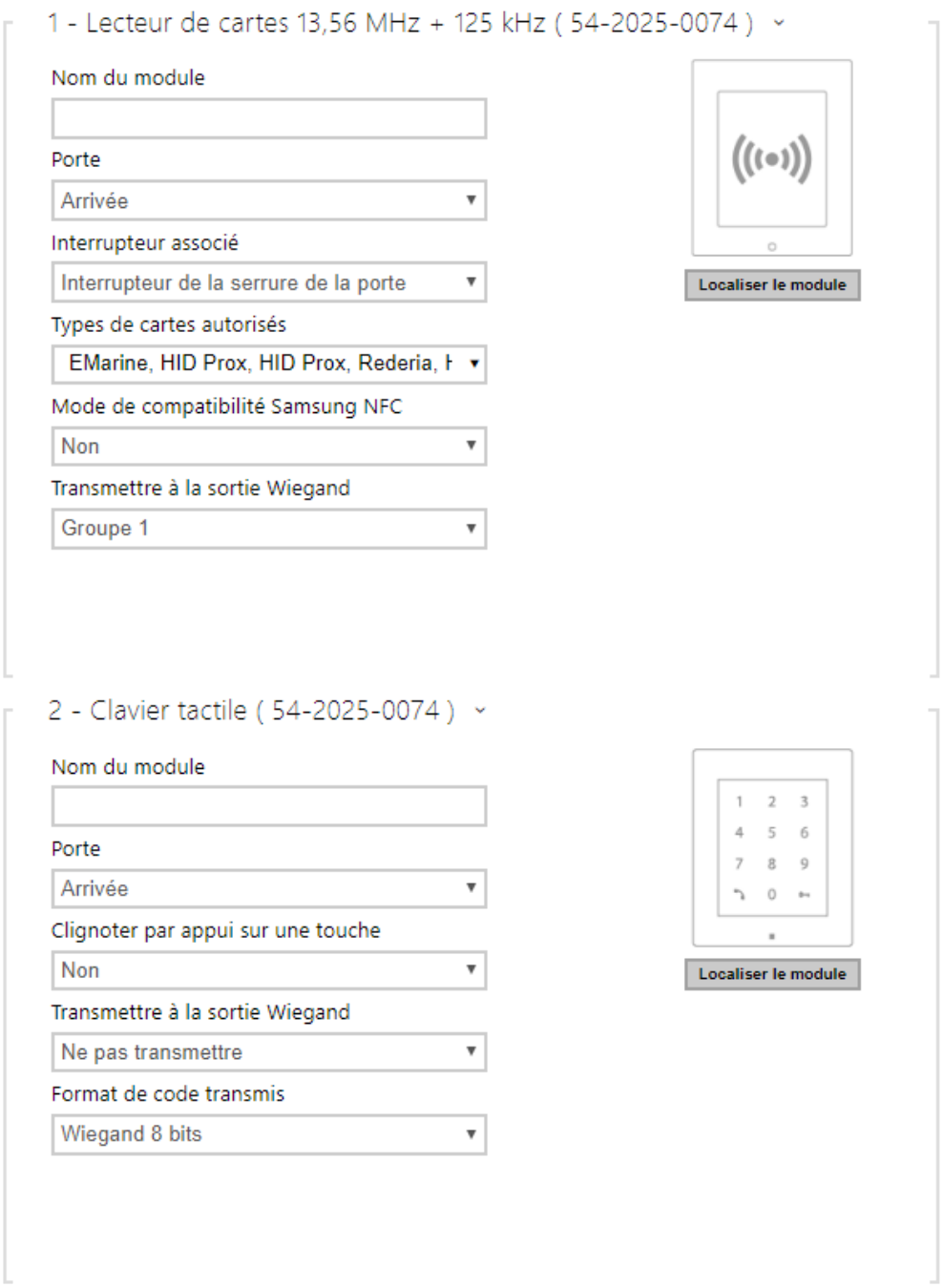
Observation

- Chaque fois que le lecteur d’empreintes digitales est déconnecté, les empreintes digitales de l’utilisateur seront masquées dans le profil de l’utilisateur après le redémarrage. Cette section affiche le nombre d'empreintes digitales d'utilisateurs téléchargées dans la mémoire de l'interphone. Une fois qu'un lecteur d'empreintes digitales est reconnecté, les empreintes digitales de l'utilisateur seront à nouveau affichées.

Configuration Module Clavier capacitif

- **Nom du module** – définissez le nom du module pour le journal d'évènements**.**
- **Porte** – définissez la direction du clavier (entrée ou sortie) pour le système de présence.
- **Clignotement par pression sur les boutons** – activez la signalisation sur le clavier pour les environnements bruyants où les signaux acoustiques sont difficiles à entendre.
- **Transmettre à la sortie Wiegand** – définissez le groupe de sorties Wiegand auxquelles toutes les touches pressées doivent être transmises.
- **Format de code transmis** – sélectionnez un format 4 bits ou 8 bits (sécurité supérieure) pour les codes à transmettre.

Configuration Module Clavier capacitif & Lecteur de carte RFID 125 kHz, 13,56 MHz



Lecteur de carte 13.56 MHz (125 kHz) (numéro de série)

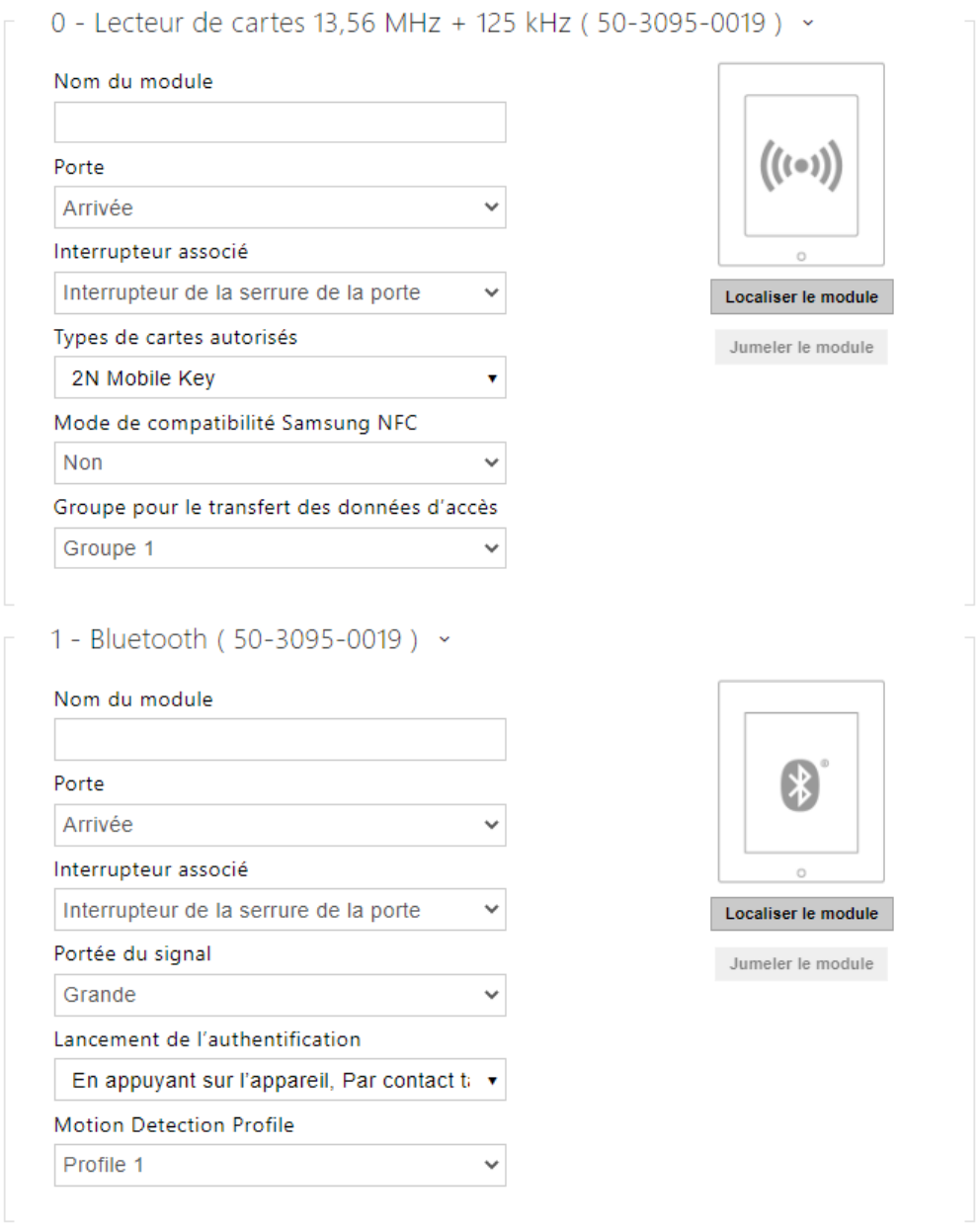
- **Nom du module** – définissez le nom du module pour le journal d'accès.
- **Porte** – définissez la direction du lecteur (entrée ou sortie) pour le système de présence.

- **Interrupteur associé** – réglez l'interrupteur pour qu'il soit activé après l'authentification de l'utilisateur via ce module. Si vous définissez l'interrupteur de verrouillage de porte et les règles d'authentification spécifiées dans Hardware / Porte.
- **Types de cartes autorisés** – définissez le type de carte pouvant être lu par le lecteur. Le lecteur de carte ne prend en charge qu'un seul type de carte à la fois.
- **Mode de compatibilité Samsung NFC** – activez la compatibilité NFc avec les Smartphones Samsung.
- **Transmettre à la sortie Wiegand** – définissez un groupe de sorties Wiegand auxquelles tous les ID de cartes RFID reçus seront renvoyés.

Clavier capacitif (numéro de série)

- **Nom du module** – définissez le nom du module pour l'enregistrement des événements à partir du clavier.
- **Porte** – définissez le nom du module pour le journal d'accès.
- **Clignotement par pression sur les boutons** – activez la signalisation sur le clavier pour les environnements bruyants où les signaux acoustiques sont difficiles à entendre.
- **Transmettre à la sortie Wiegand** – définissez le groupe de sorties Wiegand auxquelles toutes les touches pressées doivent être transmises.
- **Format de code transmis** – sélectionnez un format 4 bits ou 8 bits (sécurité supérieure) pour les codes à transmettre.

Configuration Module Bluetooth & Lecteur de carte RFID125 kHz, 13,56 MHz / 2N IP Style



Lecteur de carte 13.56 MHz (125 kHz)

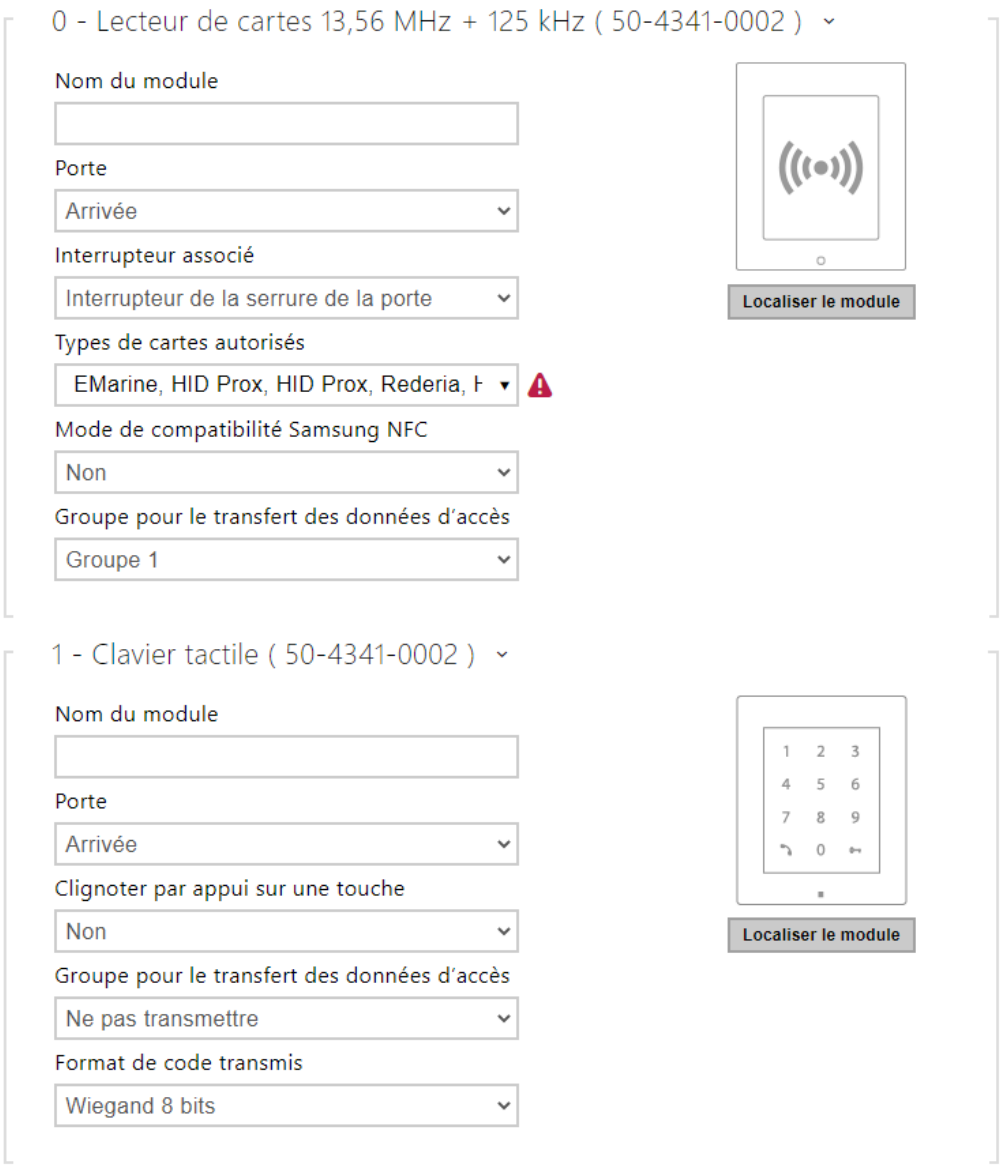
- **Nom du module** – définissez le nom du module pour le journal d'accès.
- **Porte** – définissez la direction du lecteur (entrée ou sortie) pour le système de présence.
- **Interrupteur associé** – réglez l'interrupteur pour qu'il soit activé après l'authentification de l'utilisateur via ce module. Si vous définissez l'interrupteur de verrouillage de porte et les règles d'authentification spécifiées dans Hardware / Porte.

- **Types de cartes autorisés** – définissez le type de carte pouvant être lu par le lecteur. Le lecteur de carte ne prend en charge qu'un seul type de carte à la fois.
- **Rétroéclairage du symbole RFID** (pour IP Style uniquement) – permet d'activer ou de désactiver le rétroéclairage du symbole RFID sur l'appareil.
- **Mode de compatibilité Samsung NFC** – activez la compatibilité NFC avec les Smartphones Samsung.
- **Transmettre à la sortie Wiegand** – définissez un groupe de sorties Wiegand auxquelles tous les ID de cartes RFID reçus seront renvoyés.

Bluetooth

- **Nom du module** – définissez le nom du module pour le journal d'accès. Le nom du module est utilisé lors de l'enregistrement des événements du module Bluetooth.
- **Porte** – définissez la direction du lecteur (entrée ou sortie) pour le système de présence.
- **Interrupteur associé** – réglez l'interrupteur pour qu'il soit activé après l'authentification de l'utilisateur via ce module. Si vous définissez l'interrupteur de verrouillage de porte et les règles d'authentification spécifiées dans Hardware / Porte.
- **Portée du signal** – définit la portée du signal (la valeur 5 représente la portée la plus longue, la valeur 1 la plus courte), c'est-à-dire la distance sur laquelle le module Bluetooth continuera à communiquer avec le téléphone portable. Lors de la mise en place, il est recommandé de tester la portée réelle du signal, qui dépend de plusieurs facteurs (notamment la disposition spatiale de l'installation, le téléphone portable utilisé et sa position).
- **Lancement de l'authentification** – définir la méthode d'authentification pour un téléphone portable :
    - **Par contact tactile dans l'application** – l'authentification est effectuée en appuyant sur une icône dans l'application installée sur un Smartphone.
    - **En appuyant sur l'appareil** – appuyez sur le lecteur de carte muni d'un Smartphone doté de la clé **2N® Mobile Key** pour confirmer l'authentification.
    - **Détection des mouvements** – l'authentification sera déclenchée par la détection de mouvement en présence d'un téléphone avec l'application **2N® Mobile Key** jumelée.
- **Profil de détection de mouvement** – définit le profil de détection de mouvement que le module d'authentification par un téléphone portable doit suivre.

Configuration Module Clavier capacitif & Bluetooth & Lecteur de carte RFID 125 kHz, 13,56 MHz, NFC



Lecteur de carte 13.56 MHz (125 kHz) (numéro de série)

- **Nom du module** – définissez le nom du module pour le journal d'accès.
- **Porte** – définissez la direction du lecteur (entrée ou sortie) pour le système de présence.
- **Interrupteur associé** – réglez l'interrupteur pour qu'il soit activé après l'authentification de l'utilisateur via ce module. Si vous définissez l'interrupteur de verrouillage de porte et les règles d'authentification spécifiées dans Hardware / Porte.
- **Types de cartes autorisés** – définissez le type de carte pouvant être lu par le lecteur. Le lecteur de carte ne prend en charge qu'un seul type de carte à la fois.
- **Mode de compatibilité Samsung NFC** – activez la compatibilité NFC avec les Smartphones Samsung.
- **Groupe pour le transfert des données d'accès** - vous permet de définir un groupe auquel tous les codes d'accès utilisateur reçus seront transférés.

Clavier capacitif (numéro de série)

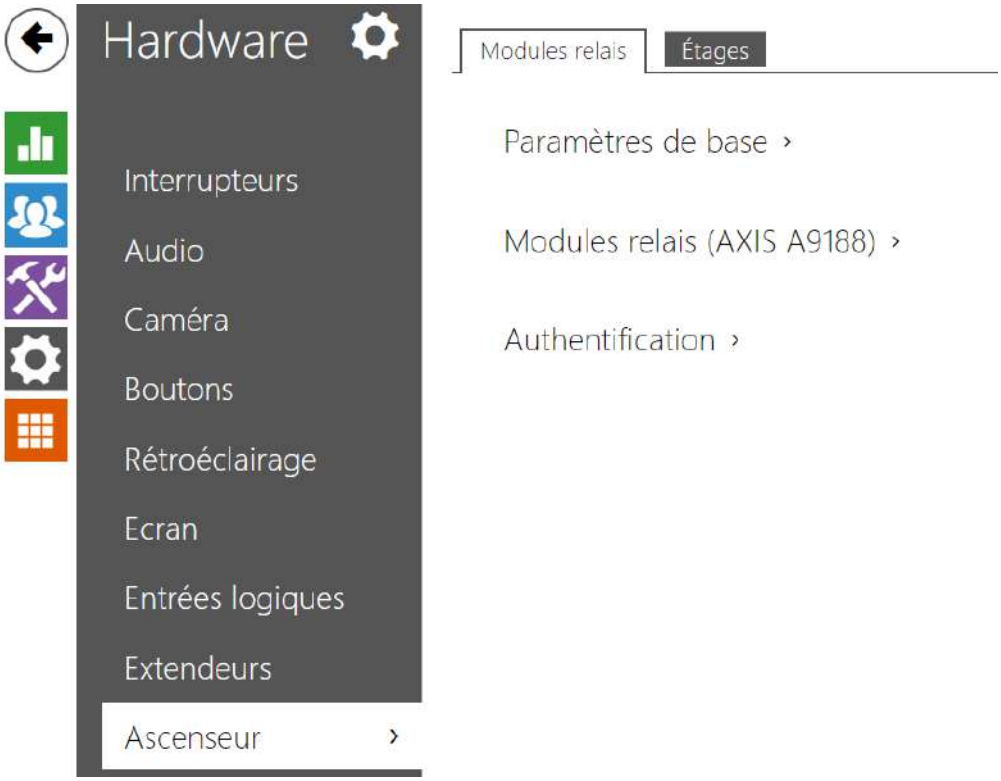
- **Nom du module** – définissez le nom du module pour le journal d'accès.
- **Porte** – définissez la direction du lecteur (entrée ou sortie) pour le système de présence.
- **Clignotement par pression sur les boutons** – activez la signalisation sur le clavier pour les environnements bruyants où les signaux acoustiques sont difficiles à entendre.
- **Groupe pour le transfert des données d'accès** - vous permet de définir un groupe auquel tous les codes d'accès utilisateur reçus seront transférés.
- **Format de code transmis** – sélectionnez un format 4 bits ou 8 bits (sécurité supérieure) pour les codes à transmettre.

Bluetooth

- **Nom du module** – définissez le nom du module pour le journal d'accès.
- **Porte** – définissez la direction du lecteur (entrée ou sortie) pour le système de présence.
- **Interrupteur associé** – réglez l'interrupteur pour qu'il soit activé après l'authentification de l'utilisateur via ce module. Si vous définissez l'interrupteur de verrouillage de porte et les règles d'authentification spécifiées dans Hardware / Porte.

- **Portée du signal** – définit la portée du signal (la valeur 5 représente la portée la plus longue, la valeur 1 la plus courte), c'est-à-dire la distance sur laquelle le module Bluetooth continuera à communiquer avec le téléphone portable. Lors de la mise en place, il est recommandé de tester la portée réelle du signal, qui dépend de plusieurs facteurs (notamment la disposition spatiale de l'installation, le téléphone portable utilisé et sa position).
- **Lancement de l'authentification** – définir la méthode d'authentification pour un téléphone portable. Un, une combinaison de deux ou les trois.
  - **Par contact tactile dans l'application** – l'authentification est effectuée en appuyant sur une icône dans l'application installée sur un Smartphone.
  - **En appuyant sur l'appareil** – appuyez sur le lecteur de carte muni d'un Smartphone doté de la clé **2N® Mobile Key** pour confirmer l'authentification.
  - **Détection des mouvements** – l'authentification sera déclenchée par la détection de mouvement en présence d'un téléphone avec l'application **2N® Mobile Key** jumelée.

5.5.10 Ascenseur

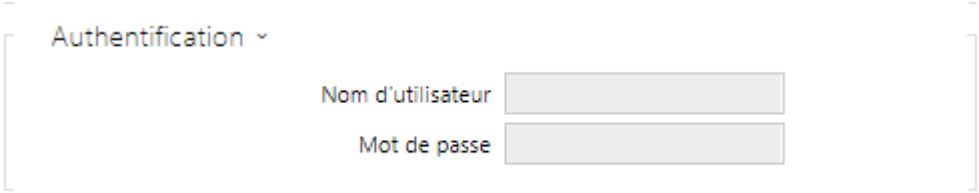


Afin de pouvoir contrôler l'accès aux étages par l'ascenseur, connectez le module relais AXIS A9188 à l'interphone IP 2N (**2N® IP Style**, **2N® IP Verso**, **2N® LTE Verso**, **2N® IP Force**, **2N® IP Safety**, **2N® IP Vario**). Jusqu'à 8 modules relais peuvent être connectés à un interphone IP 2N, chacun pouvant contrôler jusqu'à 8 étages, soit un total de 64.

Modules relais

- **Durée d'enclenchement** – paramètrez le temps d'activation du module du relais (entre 1 et 600 secondes).

- **Activé** – affiche l'activation / désactivation du module relais AXIS A9188 utilisé pour la commande d'ascenseurs jusqu'à 8 étages.
- **Adresse IP** – adresse IP du module AXIS A9188.
- **État** – affiche l'état de connexion du module AXIS A9188 (Erreur / Accès refusé / Prêt / Hors ligne).
- **Numéro de série** – numéro de série du module AXIS A9188.



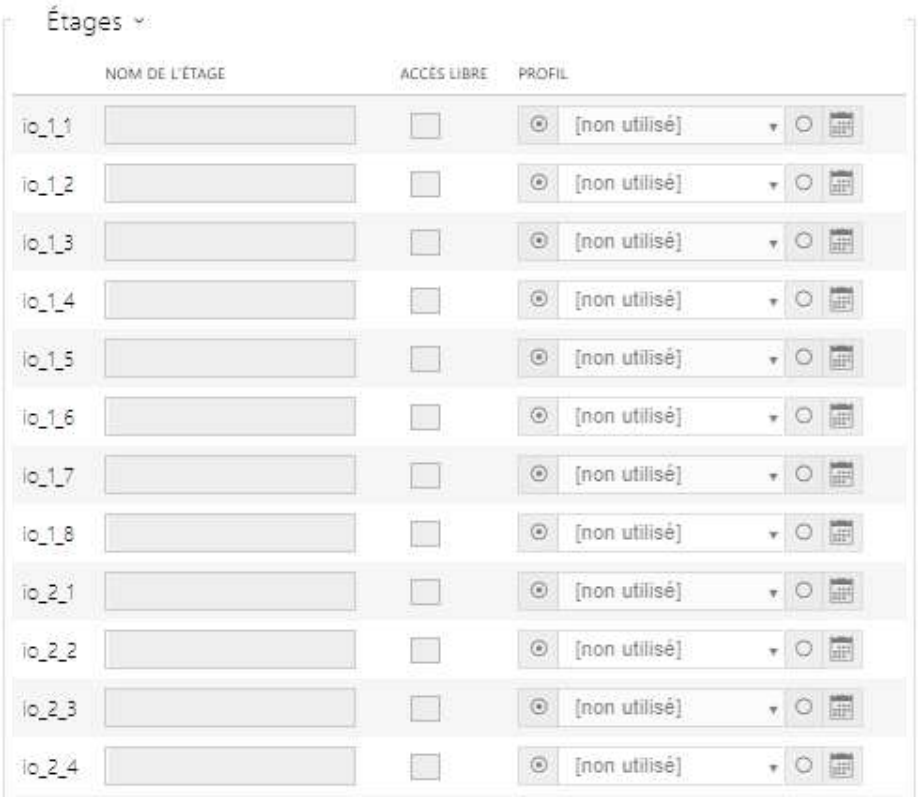
- **Nom d'utilisateur** – authentification du périphérique externe. Ce paramètre n'est obligatoire que si le périphérique externe requiert une authentification.

- **Mot de passe** – entrez le mot de passe d'authentification du périphérique externe (relais WEB, par exemple). Ce paramètre n'est obligatoire que si le périphérique externe requiert une authentification.

Observation

- Vous n'avez besoin que d'un nom d'utilisateur et d'un mot de passe d'authentification pour tous les modules.

Étages



- **Nom de l'étage** – définissez le nom des étages.
- **Accès libre** – activez l'accès permanent à l'étage sans aucune authentification.
- **Profil** – choisissez un ou plusieurs profils horaires à appliquer. Définissez les profils horaires dans la section Répertoire / Profils horaires.
  -  marquez la sélection à partir de profils prédéfinis ou du réglage manuel d'un profil temporel pour l'élément donné.
  -  définissez un profil temporel pour l'élément donné.

Conseil

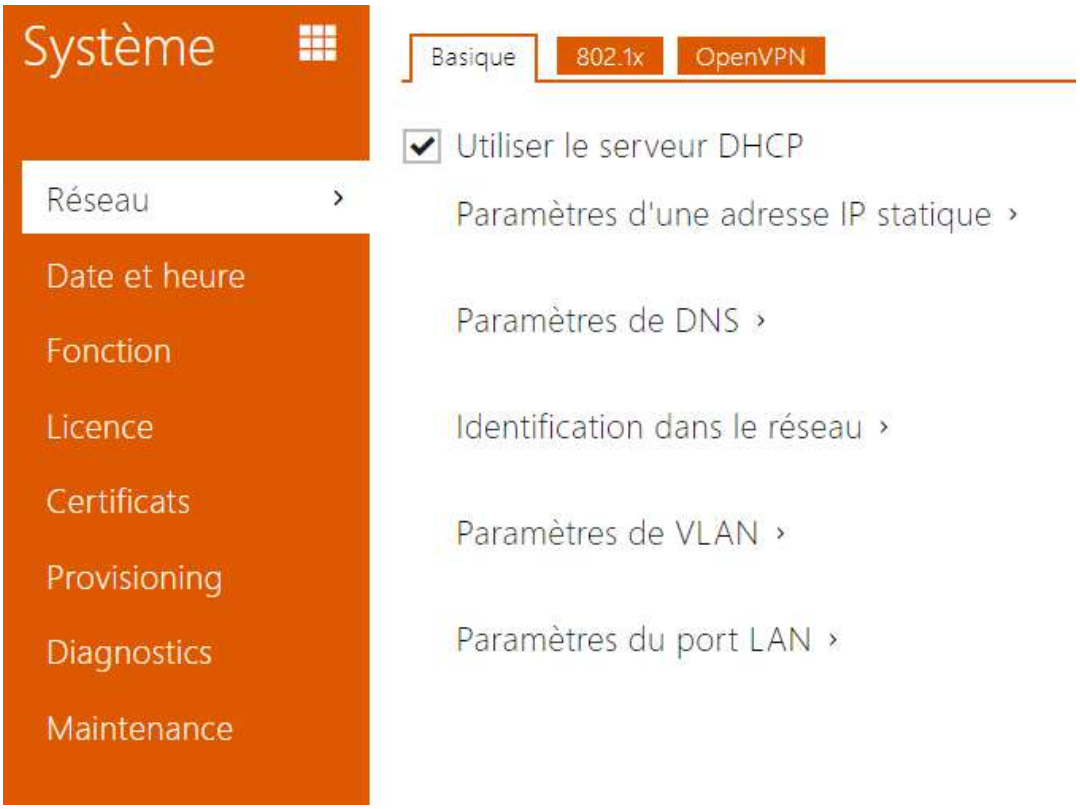
Certificat pour le module AXIS A9188

1. Retrouvez le module relais AXIS A9188 dans votre LAN en utilisant le scanner AXIS IP Utility.
2. Entrez l'identifiant.
3. Sélectionnez Préférences / Configuration additionnel du périphérique dans le menu.
4. Une nouvelle fenêtre de configuration de périphérique s'affiche.
5. Sélectionnez Options système / Sécurité / Certificats.
6. Cliquez sur *Créer un certificat auto-signé* pour créer un certificat.
7. Remplissez tous les champs obligatoires et cliquez sur OK pour confirmation.
8. Accédez à Options système / Sécurité / HTTPS.
9. Sélectionnez le certificat dans un menu contextuel et appuyez sur Enregistrer pour le sauvegarder.
10. Passez à l'interface Web de l'interphone IP 2N, rendez-vous dans la section Hardware / Ascenseur. Entrez les données de connexion et l'adresse IP du module AXIS.
11. READY est affiché sur le module relais si la connexion a réussi.

5.6 Système

Voici les différents onglets que vous pourrez trouver dans cette section :

5.6.1 Réseau



Comme les **interphones IP 2N** sont connectés au réseau local, assurez-vous que son adresse IP a été correctement définie ou obtenue depuis le serveur DHCP du réseau local. Configurez l'adresse IP et DHCP dans la sous-section Réseau.

Conseil

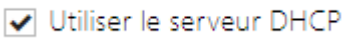
- *Pour connaître l'adresse IP actuelle de votre interphone, utilisez le **2N® Network Scanner**, qui est téléchargeable gratuitement sur le site www.2n.com, ou appliquez les étapes décrites dans le manuel d'installation de l'interphone correspondant : l'interphone peut vous communiquer son adresse IP via une fonction vocale.*

Si vous utilisez un serveur RADIUS et la vérification basée sur 802.1x pour les équipements connectés, vous pouvez faire en sorte que l'Interphone utilise l'authentification EAP-MD5 ou EAP-TLS. Définissez cette fonction dans l'onglet 802.1x.

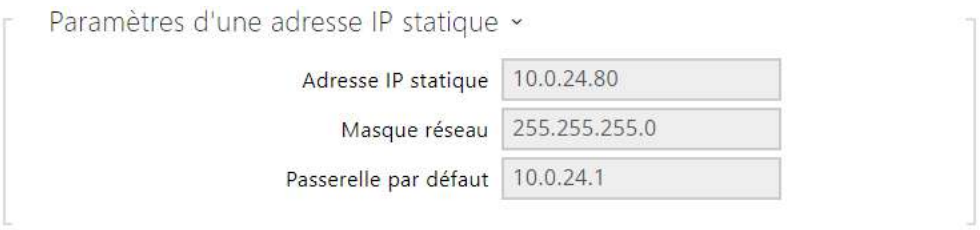
L'onglet Trace vous permet de lancer la capture des paquets entrants et sortants sur l'interface réseau de l'interphone. Le fichier contenant les paquets capturés peut être téléchargé pour le traitement sur Wireshark, par exemple. (www.wireshark.org).

Listes des Paramètres

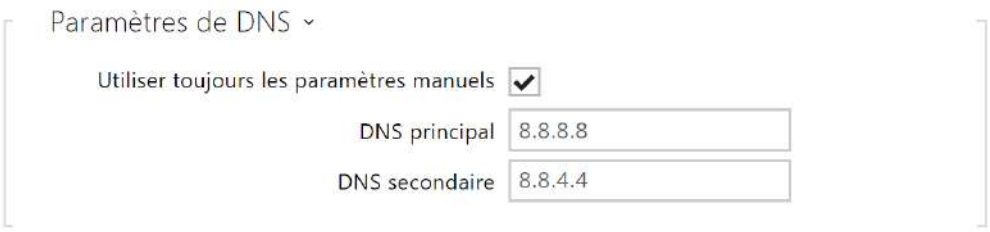
Basique



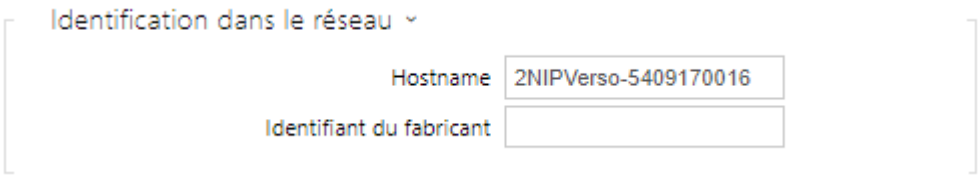
- **Utiliser le serveur DHCP** – activez l'obtention automatique de l'adresse IP à partir du serveur LAN DHCP. Si le serveur DHCP n'est pas disponible ou n'est pas accessible sur votre LAN, paramétrer le réseau manuellement.



- **Adresse IP statique** – l'Adresse IP statique de l'appareil est utilisée selon les paramètres mentionnés ci-dessous si le paramètre Utiliser le serveur DHCP est désactivé.
- **Masque réseau** – masque réseau.
- **Passerelle par défaut** – adresse de la passerelle par défaut, qui permet de communiquer avec l'équipement Off-LAN.

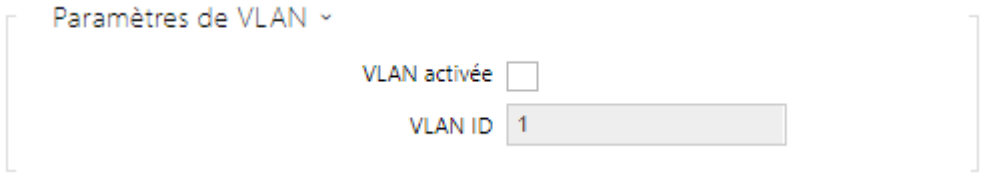


- **DNS principal** – l'adresse du serveur DNS principal pour la traduction de noms de domaines en adresses IP. En cas de réinitialisation sur les réglages d'usine, le serveur DNS principal sera défini sur 8.8.8.8.
- **DNS secondaire** – l'adresse du serveur DNS secondaire, qui est utilisée si le DNS principal n'est pas accessible. En cas de réinitialisation sur les réglages d'usine, le serveur DNS principal sera défini sur 8.8.4.4.

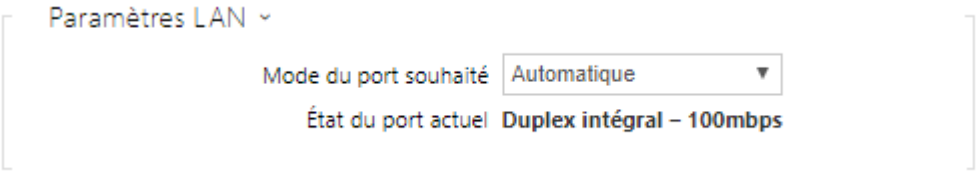


- **Nom d'hôte** – définissez l'identification du réseau de l'interphone IP 2N.
- **Identifiant du fabricant** – définissez l'identifiant de classe du fournisseur sous la forme d'une chaîne de caractères pour l'option DHCP 60.

- **WS-Discovery activé** – Activer la fonction WS-Discovery, qui permet à d'autres clients ONVIF de rechercher un dispositif compatible sur le LAN. Activer la fonction pour utiliser votre interphone en tant que dispositif compatible avec ONVIF.

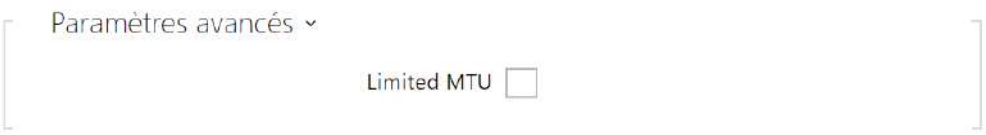


- **VLAN activée** – activez le support du réseau local virtuel (VLAN 802.1q comme recommandé). Pour un fonctionnement optimal, il est également nécessaire de définir l'ID du réseau virtuel.
- **VLAN ID** – ID du réseau virtuel sélectionné dans une plage 1–4094. L'appareil va accepter uniquement les paquets ayant cet identifiant. Un mauvais réglage peut entraîner une perte de connexion et la nécessité de réinitialiser l'appareil aux valeurs d'usine.



- **Mode de port requis** – définissez le port de l'interface réseau par défaut (Automatique ou Half Duplex – 10 Mbps). Cela permet de réduire la vitesse de transmission à 10 mbps si l'infrastructure du réseau utilisée (câblage) ne peut pas supporter 100 Mbps.

- **État du port actuel** – état actuel du port de l'interface réseau (Half-duplex ou Full-duplex : 10 Mbps ou 100 Mbps).

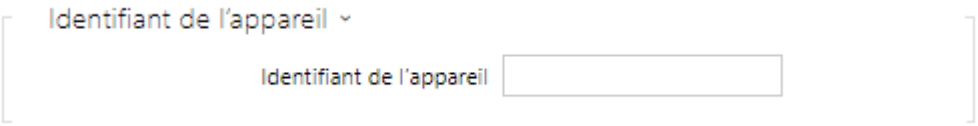


- **MTU réduit** – active la prise en charge du MTU (Maximum Transmission Unit) réduit pour le bon fonctionnement du dispositif sur les réseaux qui ne prennent en charge qu'un MTU réduit.

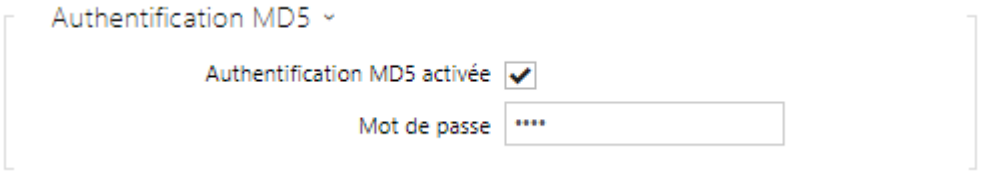
802.1x

Observation

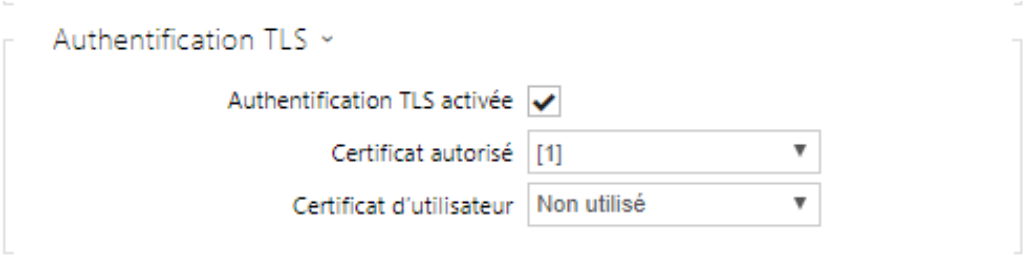
- Les modifications apportées aux paramètres d'authentification prendront effet après le redémarrage de l'appareil.



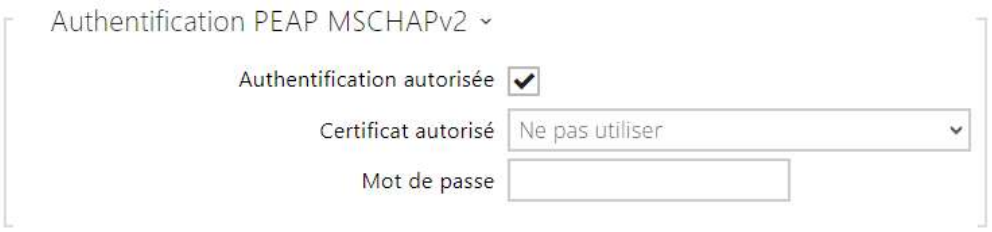
- **Identifiant de l'appareil** – nom d'utilisateur (identifiant) pour l'authentification via EAP-MD5 et EAP-TLS.



- **Authentification MD5 activée** – activez l'authentification des périphériques réseau via le protocole 802.1x EAP-MD5. Si votre réseau ne supporte pas 802.1x, n'activez pas cette fonction. Si vous le faites, l'interphone deviendra inaccessible.
- **Mot de passe** – renseignez le mot de passe d'accès pour l'authentification EAP-MD5.



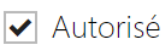
- **Authentification TLS activée** – activez l'authentification de l'appareil du réseau via le protocole 802.1x EAP-MD5. Si votre réseau ne supporte pas le 802.1x, n'activez pas cette fonction. Si vous le faites, l'interphone deviendra inaccessible.
- **Certificat autorisé** – spécifiez les certificats autorisés pour la vérification de la validité du certificat du serveur public RADIUS. Sélectionnez l'un des trois types de certificats; se reporter au chapitre sur les Certificats. Si aucun certificat autorisé n'est inclus, la vérification du certificat public RADIUS ne peut être effectuée.
- **Certificat d'utilisateur** – spécifiez le certificat d'utilisateur et la clé privée pour vérifier si le dispositif est autorisé à communiquer sur le LAN via le port de l'élément du réseau sécurisé par le protocole 802.1x. Sélectionner l'un des trois types de certificats ; se reporter au chapitre sur les Certificats.



- **Authentification autorisée** – autorise l'utilisation de l'authentification de l'appareil sur le réseau à l'aide du protocole 802.1x PEAP MSCHAPv2. Si votre réseau ne supporte pas 802.1x, n'activez pas cette fonction. Sinon, l'appareil devient inaccessible.
- **Certificat autorisé** – spécifie le certificat de l'autorité de certification pour la vérification de la validité du certificat public du serveur RADIUS S'il n'est pas spécifié, le certificat public du serveur RADIUS ne peut pas être vérifié.
- **Mot de passe** – utilisé pour l'authentification à l'aide de la méthode PEAP MSCHAPv2.

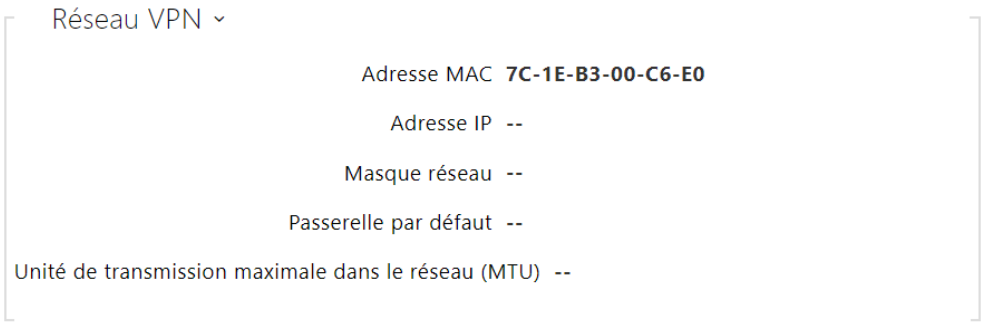
Open VPN

Vous pouvez utiliser OpenVPN pour connecter le périphérique à un autre réseau.



- **Autorisé** – activation du réseau privé virtuel (VPN).

- **Interface par défaut** – en cas d'autorisation, l'ensemble du trafic réseau sortant est dirigé en dehors du masque de réseau local vers l'interface VPN.
- **Adresse du serveur** – définissez l'adresse du serveur OpenVPN.
- **Port du serveur** – définissez le Port du serveur OpenVPN.
- **Certificat autorisé** – spécification d'un ensemble de certificats d'organismes de certification pour la validation d'un certificat de serveur public OpenVPN. Sélectionner l'un des trois types de certificats; se reporter au chapitre sur les Certificats. Si le certificat de l'organisme de certification n'est pas présenté, le certificat du serveur public OpenVPN n'est pas vérifié.
- **Certificat du client** – spécification d'un ensemble de certificats du client à des fins de vérification de l'identité du client par le serveur OpenVPN. Sélectionnez l'un des trois types de certificats; se reporter au chapitre sur les Certificats. Si le certificat du client n'est pas présenté, l'identité du client OpenVPN n'est pas vérifiée.
- **État** – affiche l'état de la connexion OpenVPN. Connecté / Déconnecté.
- **Erreur** – affiche, le cas échéant, le type d'erreur de connexion OpenVPN.
- **Start** – connectez le périphérique à OpenVPN.
- **Stop** – déconnectez le périphérique à OpenVPN.



- **Réseau VPN** – affiche les informations de base sur le VPN.

Conseil

- Référez-vous à la section FAQ sur les détails du paramétrage du serveur et client OpenVPN.

5.6.2 Date et Heure

Si vous contrôlez la validité des numéros de téléphone, des codes d'activation de verrouillage et des profils similaires, assurez-vous que la date et l'heure internes de l'interphone sont correctement définies.

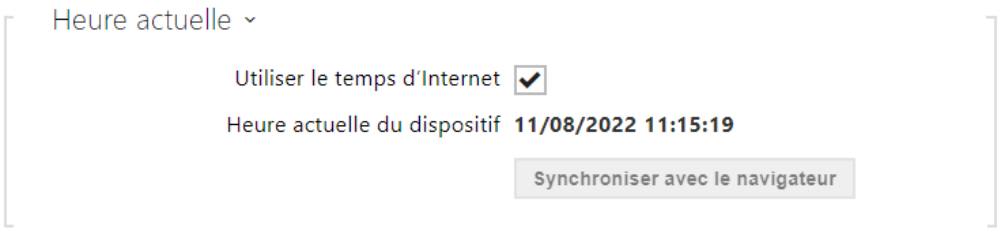
La plupart des modèles d'**Interphones IP 2N** sont équipés d'une horloge de secours en temps réel pouvant résister à plusieurs jours de pannes de courant. S'il n'est pas équipé de cette fonction, l'interphone perd les données en temps réel en cas de panne de courant (ou de redémarrage). Par conséquent, si l'interphone est mis sous tension après une période assez longue (après l'installation d'un nouvel interphone, par exemple), l'heure est définie sur la valeur par défaut et doit être réinitialisée. Vous pouvez à tout moment synchroniser l'heure de l'interphone avec l'heure d'Internet en cochant la fonction **Utiliser l'heure réelle d'Internet** ou avec l'heure actuelle de votre PC à l'aide du bouton **Synchroniser dans le navigateur**.

Note

- *L'interphone n'a pas besoin des valeurs de date et heure actuelles pour sa fonction de base. Cependant, veillez à définir ces valeurs lorsque vous appliquez des profils de temps et affichez l'heure des événements répertoriés (Syslog, utilisation de carte RFID, évènements téléchargés via **HTTP API**, etc.).*

Pour une précision et une fiabilité maximales, nous recommandons de toujours utiliser la fonction **Utiliser l'heure réelle d'Internet**. Dans des conditions de fonctionnement normales, l'appareil peut afficher un retard ou une avance de l'ordre de ±2 minutes/mois.

Liste des Paramètres

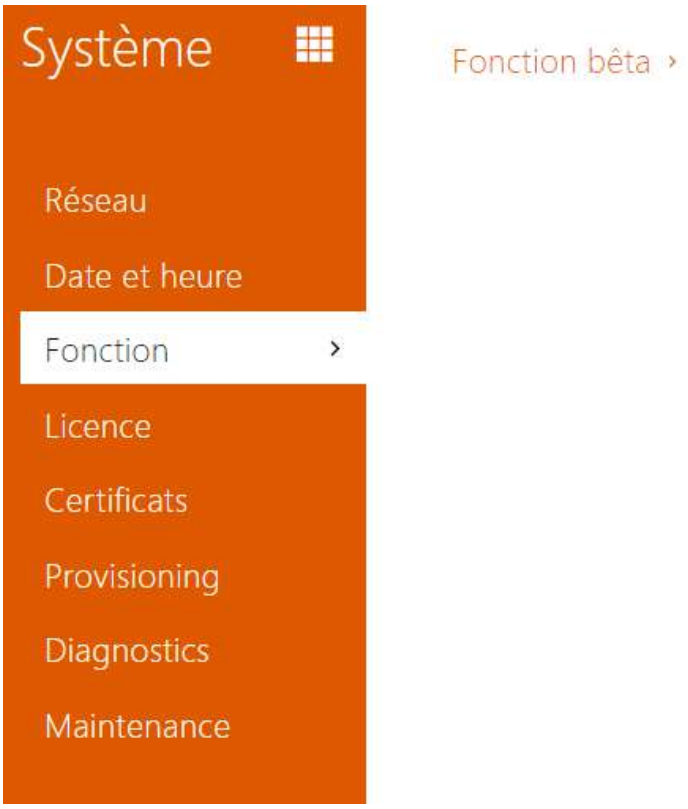


- **Utiliser le temps d'Internet** – Activer l'utilisation du serveur NTP pour la synchronisation de l'heure du dispositif.
- **Synchroniser avec le navigateur** – appuyez sur le bouton pour synchroniser la valeur temporelle de l'interphone avec la valeur temporelle de votre ordinateur.

- **Détection automatique** – définit si le fuseau horaire sera détecté automatiquement depuis le service My2N. Si la détection automatique est désactivée, le réglage dans le paramètre de sélection manuelle (fuseau horaire sélectionné manuellement ou Règle personnalisée) est utilisé.
- **Fuseau horaire détecté** – affiche le fuseau horaire détecté automatiquement. Affiche N/A si le service n'est pas disponible ou s'il est désactivé.
- **Sélection manuelle** – il définit la zone horaire pour l'emplacement d'installation de l'appareil. Paramètres déterminent le décalage temporel et les transitions de l'heure d'été et d'hiver.
- **Règle personnalisée** – si le dispositif est installé sur un site qui ne figure pas parmi les paramètres de zone horaire, configurer la règle de zone horaire manuellement. Cette règle s'applique uniquement si la zone horaire est réglée sur Manuel.

- **Adresse du serveur NTP** – paramétrez l’adresse IP / le nom de domaine du serveur NTP utilisé pour la synchronisation de l’heure de votre dispositif. Ni l’adresse IP du serveur ni le nom de domaine ne peuvent être définis lorsque la fonction **Utiliser l’heure d’Internet** est désactivée.
- **État du NTP** – affiche l'état de la dernière tentative de synchronisation de l'heure locale via le serveur NTP (Non synchronisé, Synchronisé, Erreur).

5.6.3 Fonction



Affiche une liste de fonctions bêta publiées qui sont destinées à être testées par les utilisateurs. La liste indique :

- nom de la fonction,
- état de la fonction indiquant si la fonction est lancée ou arrêtée,
- action pour lancer ou arrêter la fonction.

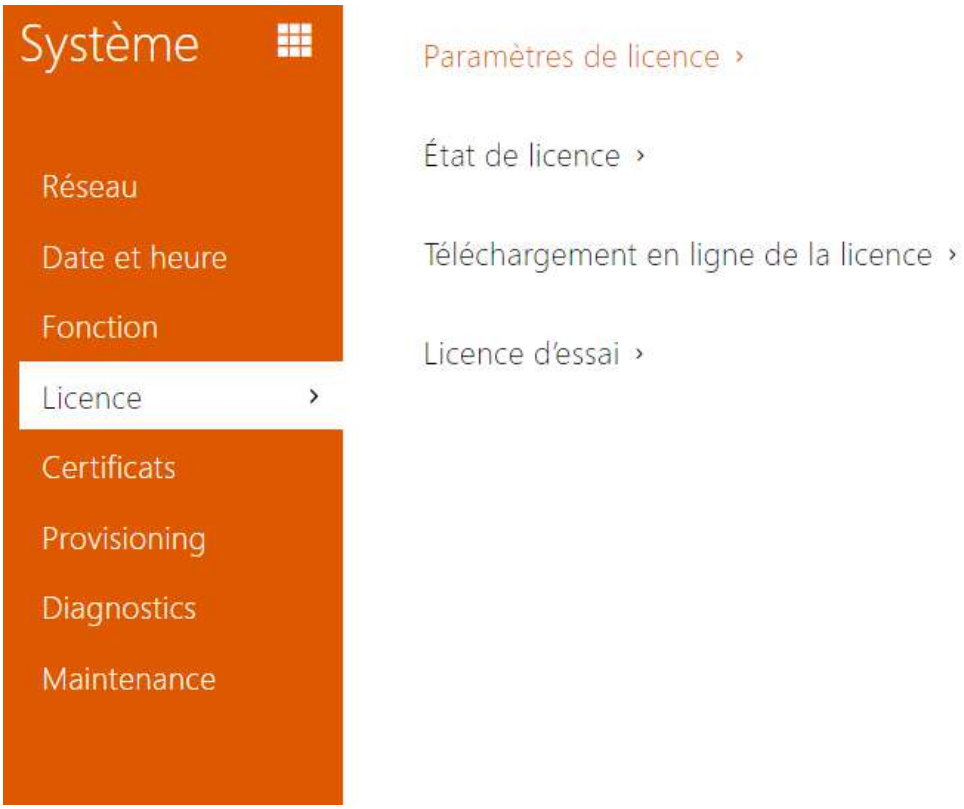
La fonction ne sera lancée ou arrêtée qu'après le redémarrage de l'appareil. Tant que l'appareil n'est pas redémarré, la demande de changement d'état peut être annulée à l'aide de l'action **Annuler**.

Note

- Les fonctions de test ne sont pas garanties et la société 2N TELEKOMUNIKACE a.s. n'est pas responsable des limitations fonctionnelles et de tout dommage éventuel résultant des limitations fonctionnelles des fonctions bêta. Les fonctions bêta sont fournies à des fins de test uniquement.

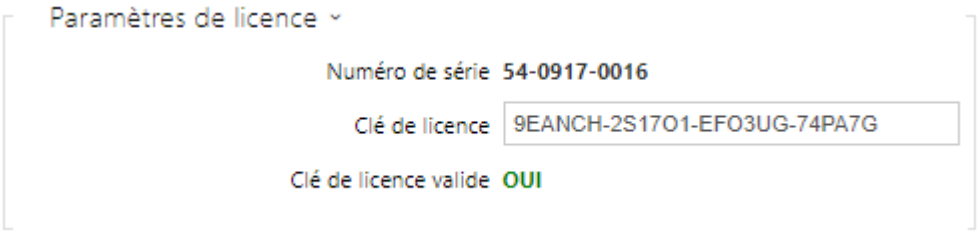
Nom de la fonction bêta	Description
Fichier de configuration protégé par un mot de passe	Cette fonction permet de crypter le fichier de configuration avec un mot de passe lors de sa sauvegarde (voir 5.5.8 Maintenance). Lors du téléchargement du fichier de configuration sur l'appareil, le mot de passe qui sécurise le fichier de configuration sera demandé. Si le mot de passe ne correspond pas, le fichier de configuration ne sera pas téléchargé sur l'appareil.
Authentification multifactorielle des plaques d'immatriculation	Lorsque cette fonction est activée, l'option Multifacteur apparaît dans la section Services > Contrôle d'accès > Règles pour l'arrivée > Paramètres avancés > Reconnaissance des plaques d'immatriculation. L'accès n'est autorisé qu'après la combinaison d'au moins deux méthodes d'authentification, en fonction des paramètres des règles d'accès. Lorsque la plaque d'immatriculation est reconnue, il est nécessaire d'introduire une autre méthode d'authentification dans un délai de 60 secondes.
Noise Cancelling	Cette fonction supprime le bruit ambiant du microphone lorsque la voix est détectée.

5.6.4 Licences

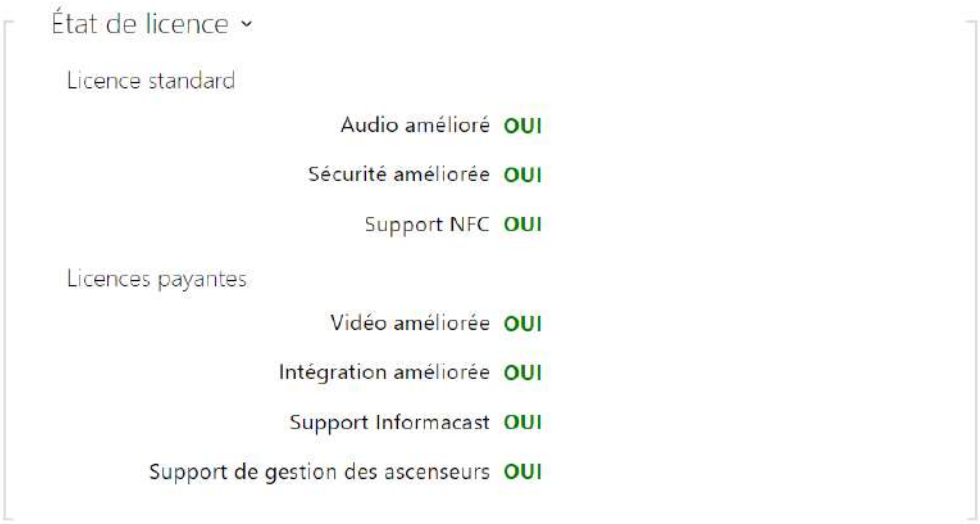


Certaines fonctionnalités des **interphones IP 2N** sont disponibles avec une clé de licence valide uniquement. Reportez-vous à la sous-section **Différents modèles et fonctionnalités sous licences** pour obtenir la liste des options de licence pour votre interphone.

Liste des Paramètres



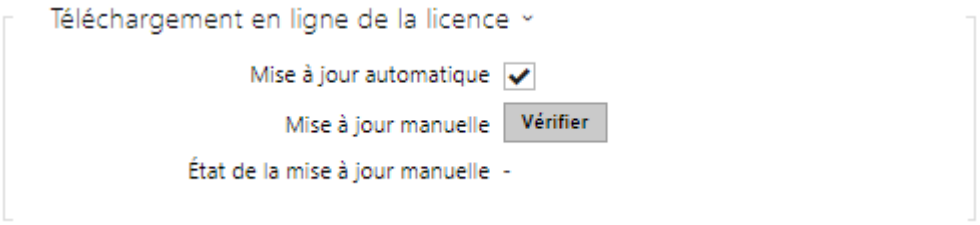
- **Numéro de série** – affiche le numéro de série de l'appareil pour lequel la licence est valide.
- **Clé de licence** – saisissez la clé de licence valide.
- **Clé de licence valide** – vérifiez si la clé de licence utilisée est valide.



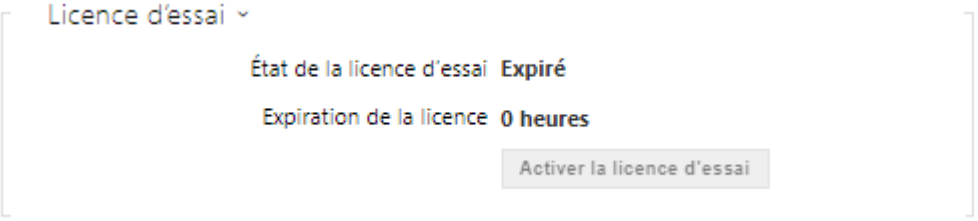
- **Licence standard** – affiche la liste des licences qui sont incluses avec le dispositif en usine.
  - **Audio améliorée** – vérifiez si les fonctions activées par la licence Audio amélioré sont disponibles.
  - **Securité améliorée** – vérifiez si les fonctions activées par la licence Sécurité améliorée sont disponibles.
  - **Support NFC** – vérifiez si le support d'identification d'utilisateur NFC est disponible.
- **Licences payantes** – affiche une liste des licences disponibles après la saisie d'une clé de licence valide
  - **Vidéo améliorée** – vérifiez si les fonctions activées par la licence Vidéo améliorée sont disponibles.
  - **Intégration améliorée** – vérifiez si les fonctions activées par la licence Intégration améliorée sont disponibles.
  - **Support InformaCast** – vérifiez si le support InformaCast est disponible.
  - **Support de commande de l'ascenseur** – vérifiez si les fonctions activées par la licence de Contrôle du Module Ascenseur sont disponibles.

Conseil

- Aperçu des licences et de leurs fonctions



- **Mise à jour automatique** – activez la mise à jour automatique de la clé de licence à partir du serveur de licences 2N.
- **Mise à jour manuelle** – demande manuelle de vérification de la disponibilité d'une licence.
- **État de la mise à jour manuelle** – en cours, actualisé, non-spécifié.

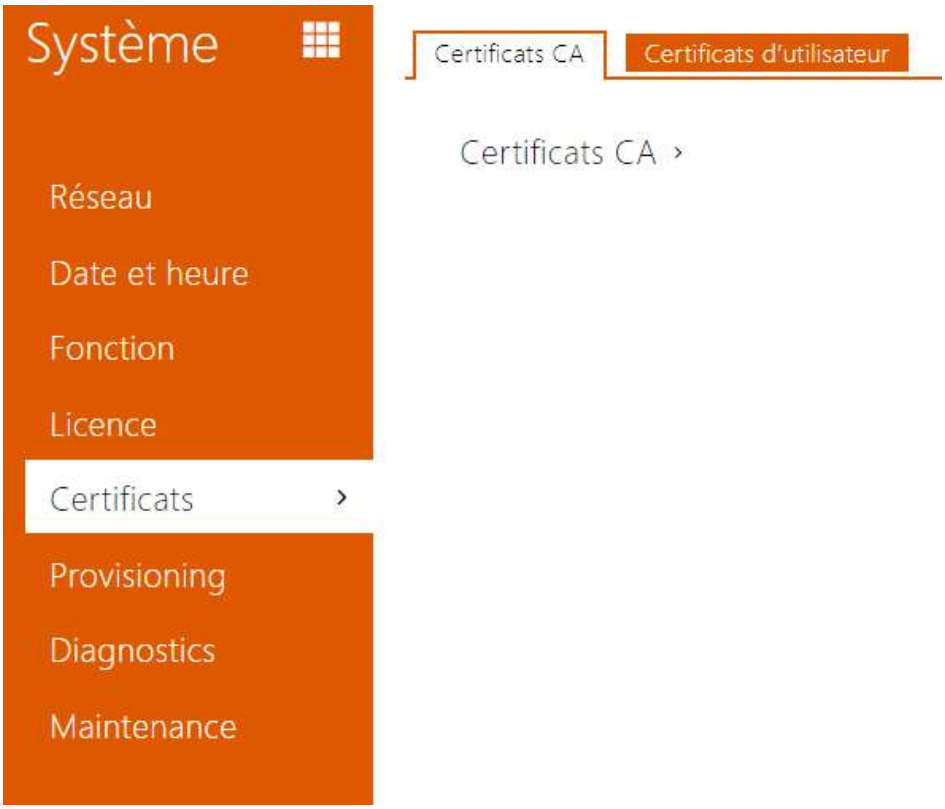


- **État de la licence d'essai** – vérifiez l'état de la licence d'essai (non activé, activé, expiré).
- **Expiration de la licence** – vérifiez le temps restant de la validité de la licence d'évaluation. 1 heure est déduite automatiquement du temps restant de la licence à chaque redémarrage et réinitialisation aux paramètres d'usine; sinon ce temps n'est affecté d'aucune façon.

Observation

- La réinitialisation logicielle ne supprime pas la clé de licence et entraîne le redémarrage de l'appareil. Si elle est désactivée avant la réinitialisation du logiciel, la mise à jour automatique de la licence est automatiquement activée et une requête est envoyée au serveur de licences. Si la mise à jour automatique de la licence est activée, la requête au serveur de licences est envoyée comme prévu.
- La réinitialisation matérielle supprime la clé de licence et le redémarrage ultérieur de l'appareil dans un laps de temps aléatoire génère une requête auprès du serveur de licences.
- Intervalle entre les demandes – de 1 à 100 minutes après le début, puis dans les 8 heures sous licence d'essai ou dans les 8 heures suivantes pendant 7 jours après le redémarrage, avec une licence illimitée.

5.6.5 Certificats



Certains services réseau des **interphones IP 2N** utilisent le protocole TLS (Transaction Layer Security) pour la communication avec d'autres périphériques LAN afin d'empêcher des tiers de surveiller et / ou de modifier le contenu de la communication. Une authentification unilatérale ou bilatérale basée sur des certificats et des clés privées est nécessaire pour établir des connexions via TLS.

Les services d'interphone suivants utilisent le protocole TLS :

a. Serveur Web (HTTPS)
b. E-mail (SMTP)
c. 802.1x (EAP-TLS)
d. SIPs

Les **interphones 2N IP** ermettent simultanément de télécharger des ensembles de certificats d'autorités de certification, aux fins de vérification de l'identité de l'équipement avec lequel l'interphone communique, et de télécharger des certificats personnels et des clés privées, servant au cryptage de la communication.

L'un des trois ensembles de certificats disponibles peut être affecté à chaque service requérant un certificat. Référez vous aux sous sections **Serveur Web**, **E-mail** et **Streaming**. Les certificats peuvent être partagés par ces services.

- **L'interphone IP 2N** accepte les formats de certificat DER (ASN1) et PEM.
- **L’interphone 2N IP** prend en charge le cryptage AES, DES et 3DES.
- **L’interphone 2N IP** prend en charge les algorithmes :
    - RSA jusqu’à une taille de clé de 2048 bits pour les certificats téléchargés par l’utilisateur ; en interne jusqu’à une taille de clé 4096 bits (lors de la connexion - certificats intermédiaires et homologues)
    - Courbes elliptiques

Observation

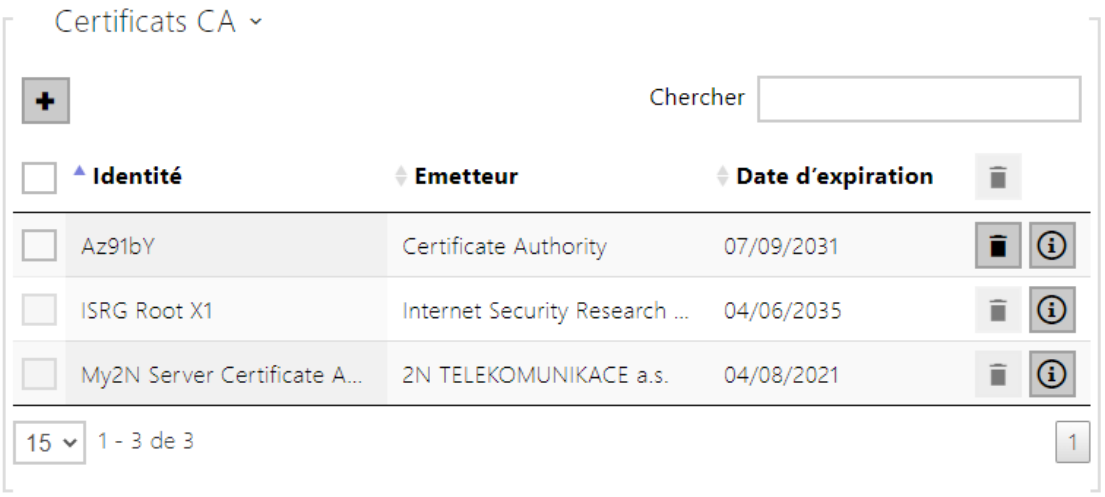
- Les certificats CA doivent utiliser le format X.509 v3.

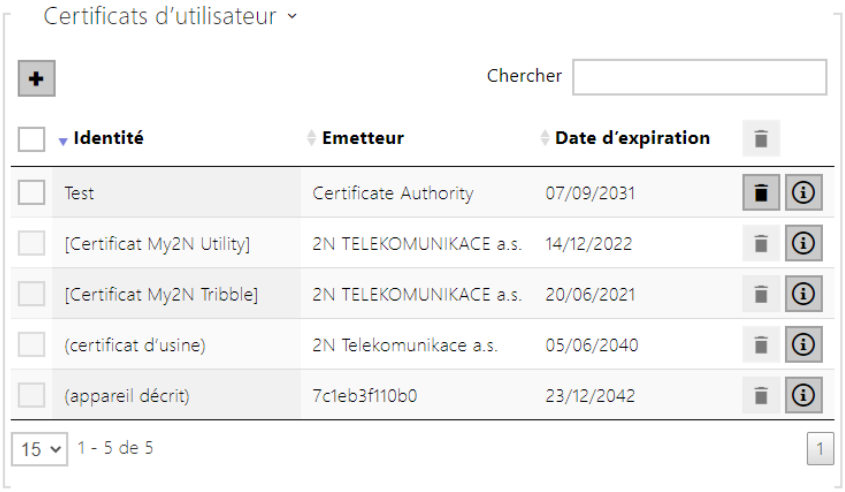
Lors de la première mise sous tension, l'interphone génère automatiquement le **certificat** et la **clé privée auto-signés** pour le **Serveur Web** et les **services de messagerie**, sans vous obliger à charger un certificat et une clé privée.

Note

- *Si vous utilisez le certificat auto-signé pour le chiffrement du serveur Web de l'interphone - communication entre navigateurs, la communication est sécurisée, mais le navigateur vous avertit qu'il est incapable de vérifier la validité du certificat de l'Interphone.*

L'aperçu actuel des certificats téléchargés des autorités de certification et des certificats personnels est affiché dans deux onglets :





Appuyez sur  pour charger un certificat enregistré sur votre PC. Vous pouvez remplir l'ID du certificat dans la boîte de dialogue pour identifier le certificat lorsque vous le sélectionnez, le modifiez ou le supprimez. L'ID peut comporter un maximum de 40 caractères et peut contenir des caractères alphabétiques minuscules et majuscules, des chiffres et des caractères '_' et '-'. L'ID n'est pas obligatoire. Sélectionnez le fichier de certificat (ou clé privée) dans la fenêtre de dialogue et cliquez sur **Charger**. Appuyez sur le bouton  pour effacer le certificat de l'appareil. Appuyez sur  pour affichez les informations relatives au certificat.

Observation

- Après la mise à jour du micrologiciel ou un redémarrage, l'équipement remplace le certificat **Self signed** par un nouveau. Il faut comparer et vérifier que le certificat affiché sur l'équipement est identique à celui du site Internet.

Observation

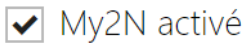
- Notez qu'un certificat avec une clé RSA privée de plus de 2048 bits peut être rejeté et le message suivant s'affiche **Le fichier de clé privée / mot de passe n'a pas été accepté par l'appareil**!
- Pour les certificats basés sur des courbes elliptiques, utilisez uniquement les courbes secp256r1 (ou prime256v1, également appelée NIST P-256) et secp384r1 (ou NIST P-384).

5.6.6 Provisioning

Les **interphones IP 2N** vous permettent de mettre à jour le firmware et la configuration manuellement ou automatiquement à partir d'un stockage sur un serveur TFTP / HTTP que vous avez sélectionné selon des règles prédéfinies.

Vous pouvez configurer manuellement l'adresse du serveur TFTP et HTTP. Les **interphones IP 2N** prennent en charge l'identification automatique de l'adresse du serveur DHCP local (option 66).

My2N



- **My2N activé** – activez la connexion à My2N ou à un autre serveur ACS.

- **Numéro de série** – affiche le numéro de série de l'équipement pour lequel le code My2N est en vigueur.

- **My2N Security Code** – affiche le code d'activation de l'application complète.
- **Générer un nouveau** – le code de sécurité My2N actuel sera invalidé et un nouveau sera créé.

Affiche les informations relatives à l'état de la connexion de l'équipement à My2N.

- **My2N ID** – identifiant unique de la société créée via le portail My2N.

Firmware

Utilisez l'onglet **Firmware** pour définir le téléchargement automatique du firmware à partir d'un serveur que vous avez défini. L'interphone compare périodiquement le fichier du serveur avec son fichier de firmware actuel et, si le fichier du serveur est ultérieur, il met automatiquement à jour le firmware et se redémarre (environ 30 s). Par conséquent, nous vous recommandons la mise à jour lorsque le trafic de l'interphone est très faible (la nuit, par exemple).

Les Interphones IP 2N recherchent les formats de fichier suivants :

1. **MODEL**-firmware.bin – firmware de l'Interphone
2. **MODEL**-common.xml – configuration commune pour tous les interphones d'un modèle
3. **MODEL**-**MACADDR**.xml – configuration spécifique pour un interphone

MODEL dans le nom du fichier spécifie la désignation technique de l'interphone 2N IP ou du dispositif audio 2N IP :

1. **hipv – 2N® IP Vario**
2. **hipf – 2N® IP Force**
3. **hipsf – 2N® IP Safety**
4. **hipak – 2N® IP Audio Kit**
5. **hipvk – 2N® IP Video Kit**
6. **hipve – 2N® IP Verso**

7. **verso2 – 2N® IP Verso 2.0**
8. **au – 2N Access Unit**
9. **aug2 – 2N Access Unit 2.0**
10. **aum – 2N Access Unit M**
11. **hipso – 2N® IP Solo**
12. **hipba – 2N® IP Base**
13. **sac – 2N® SIP Audio Converter**
14. **sassh – 2N® SIP Speaker Horn**
15. **ss – 2N® SIP Speaker**
16. **style – 2N® IP Style**

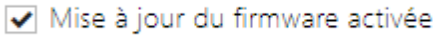
MACADDR est l'adresse MAC de l'interphone au format 00-00-00-00-00-00. Recherchez l'adresse MAC sur la plaque de production de l'interphone ou dans l'onglet **État** de l'interphone via l'interface Web.

Exemple :

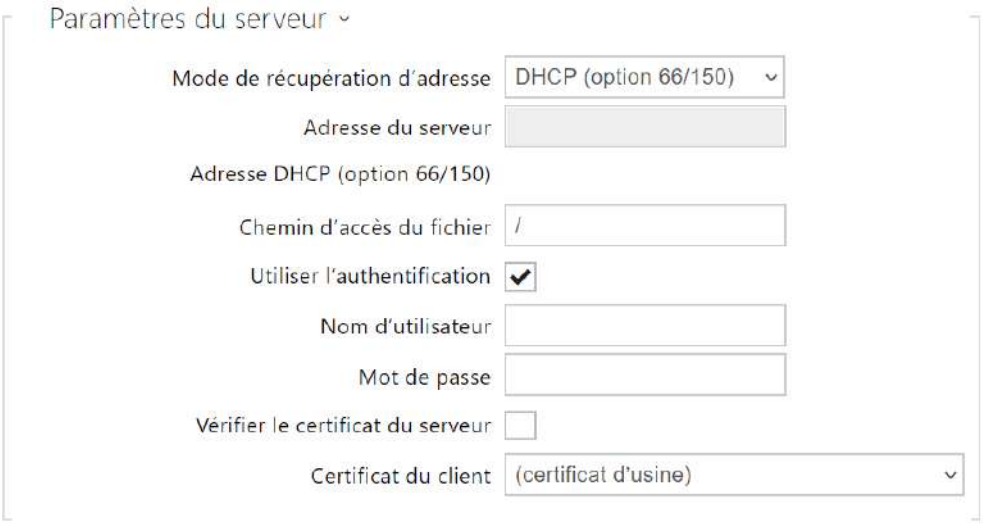
2N® IP Vario avec l'adresse MAC 00-87-12-AA-00-11 télécharge les fichiers suivants à partir du serveur TFTP :

- hipv-firmware.bin
- hipv-common.xml
- hipv-00-87-12-aa-00-11.xml

Liste des Paramètres



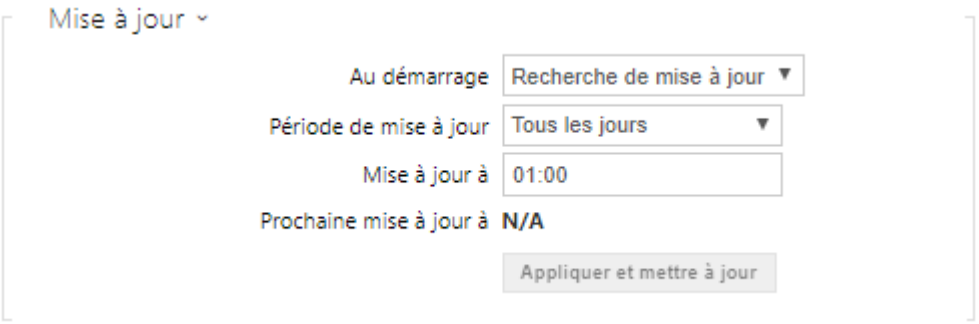
- **Mise à jour du firmware activée** – activez la mise à jour automatique du firmware / de la configuration à partir du serveur TFTP / HTTP.



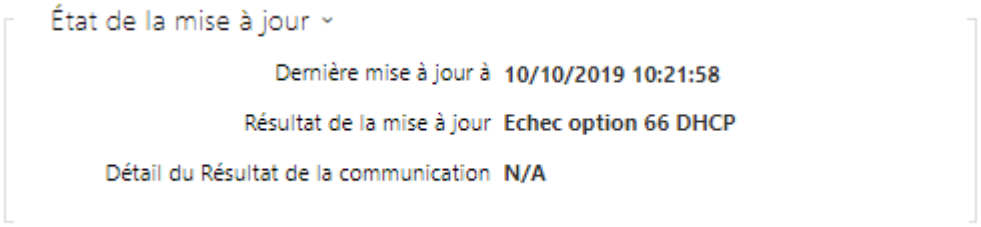
- **Mode de récupération d'adresse** – définissez si l'adresse du serveur TFTP/HTTP doit être saisie manuellement ou via une valeur récupérée automatiquement à partir du serveur DHCP utilisant l'option 66.
- **Adresse du serveur** – saisissez manuellement l'adresse du serveur TFTP (tftp://ip_adresse), HTTP (http://ip_adresse) ou HTTPS (https://ip_adresse).
- **Adresse DHCP (Option 66/150)** – vérifiez l'adresse du serveur récupérée via l'option DHCP 66 ou l'option DHCP 150.
- **Chemin d'accès du fichier** – définissez le chemin d'accès au dossier des fichiers firmware. Saisissez / pour rechercher model-firmware.bin (modèle spécifique) dans le dossier racine du serveur. Consultez la barre latérale (?) pour plus de détails sur les modèles, etc.
- **Utiliser l'authentification** – activez l'authentification pour l'accès au serveur HTTP.
- **Nom d'utilisateur** – entrez le nom d'utilisateur pour l'authentification du serveur.
- **Mot de passe** – entrez le mot de passe pour l'authentification du serveur.
- **Vérifier le certificat du serveur** – définit une liste des autorités de certifications pour vérifier la validité du certificat public du serveur ACS.
- **Certificat du client** – définit le certificat client et la clé privée qui autorise l'interphone à communiquer avec le serveur ACS.

Note

- L'interphone contient le certificat d'usine, un certificat signé utilisé pour l'intégration de British Telecom, par exemple.



- **Au démarrage** – activez la vérification et, si possible, mettez à jour l'exécution à chaque démarrage de l'interphone.
- **Période de mise à jour** – il définit la période de mise à jour. Définissez une mise à jour automatique pour qu'elle se produise toutes les heures, tous les jours, toutes les semaines ou tous les mois, ou définissez la période manuellement.
- **Mise à jour à** – définissez l'heure de mise à jour au format HH : MM pour la mise à jour périodique à une heure de faible trafic. Le paramètre n'est pas appliqué si la période de mise à jour est définie sur une valeur inférieure à 1 jour.
- **Prochaine mise à jour à** – définissez l'heure de la prochaine mise à jour.



- **Dernière mise à jour à** – heure de la dernière mise à jour.
- **Résultat de la mise à jour** – résultat de la dernière mise à jour. Les options suivantes sont disponibles : L'option DHCP 66 a échoué, le firmware est à jour, la connexion au serveur a échoué, En cours d'exécution …, Fichier non trouvé.
- **Détail du Résultat de la communication** – code d'erreur de communication avec le serveur ou le code d'état du protocole TFTP / HTTP.

Result	Description
Adresse du serveur Invalide	L'adresse du serveur est invalide.

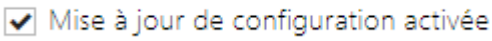
Result	Description
Protocole non supporté	Le protocole n'est pas supporté. Seul HTTP (s) et TFTP sont pris en charge.
Chemin de fichier invalide	L'emplacement du fichier de provisionnement n'est pas valide.
L'option DHCP 66 a échoué	L'adressage du serveur via DHCP Option 66 ou 150 a échoué.
Nom de domaine invalide	Le nom de domaine du serveur n'est pas valide en raison d'une configuration incorrecte ou de l'indisponibilité du serveur DNS.
Serveur non trouvé	Le serveur HTTP / TFTP demandé ne répond pas.
L'authentification a échoué	Les informations d'identification HTTP ne sont pas valides.
Fichier non trouvé	Le fichier n'a pas été trouvé sur le serveur.
Demande en attente…	La demande de provisioning est en file d'attente.
En cours…	La mise à jour est en cours.
Fichier invalide	Le fichier à télécharger est corrompu ou d'un type incorrect.
Firmware à jour	La tentative de mise à jour du firmware révèle que la dernière version du firmware a été chargée.
Mise à jour Réussi	La mise à jour de la configuration / du firmware a réussi. Avec la mise à jour du firmware, l'appareil sera redémarré dans quelques secondes.
Erreur interne	Une erreur non spécifiée s'est produite lors du téléchargement du fichier.

Configuration

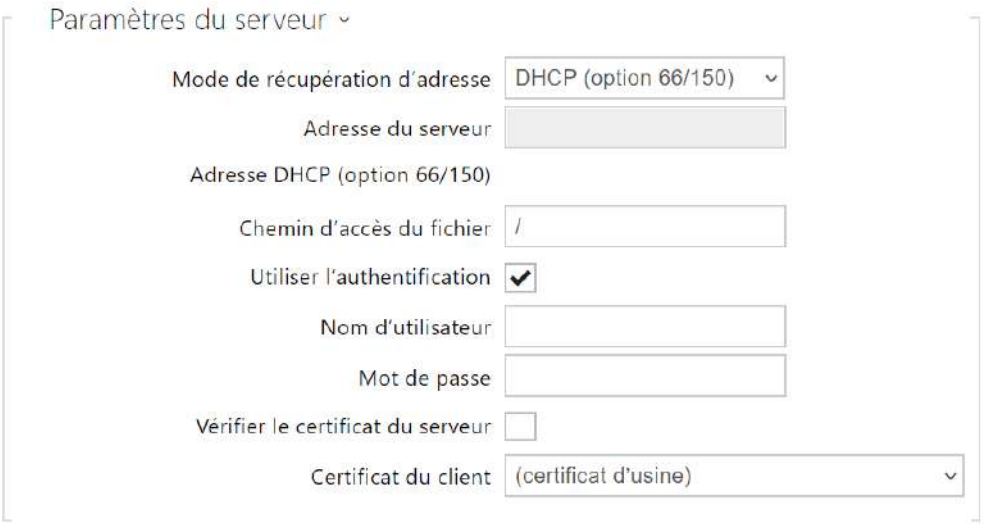
Utilisez l'onglet **Configuration** pour télécharger la configuration automatique à partir du serveur que vous avez défini. L'interphone télécharge périodiquement un fichier du serveur et est reconfiguré sans être redémarré.

Note

- *La fonction d'affichage est interrompue pendant quelques secondes dans les modèles **2N® IP Vario** équipés de ce type d'affichage lors de la reconfiguration. Par conséquent, nous vous recommandons de mettre à jour l'interphone lorsque le trafic est très faible (la nuit, par exemple).*



- **Mise à jour de configuration activée** – activez la mise à jour automatique du firmware / de la configuration à partir du serveur TFTP / HTTP.

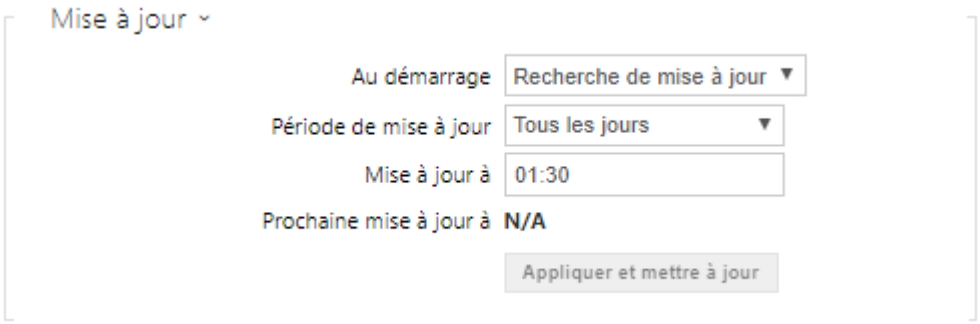


- **Mode de récupération d'adresse** – définissez si l'adresse du serveur TFTP/HTTP doit être saisie manuellement ou si une valeur récupérée automatiquement à partir du serveur DHCP utilisant l'option 66 doit être utilisée.
- **Adresse du serveur** – saisissez manuellement l'adresse du serveur TFTP (tftp://ip_adresse), HTTP (http://ip_adresse) ou HTTPS (https://ip_adresse).
- **Adresse DHCP (Option 66/150)** – vérifiez l'adresse du serveur récupérée via l'option DHCP 66 ou l'option DHCP 150.
- **Chemin d'accès du fichier** – définissez le repertoire ou le préfixe du firmware / de la configuration sur le server. L'Interphone attend un fichier XhipY_firmware.bin, XhipY-common.xml et XhipY-MACADDR.xml, où X est le préfixe spécifié et Y spécifie le modèle de l'interphone.

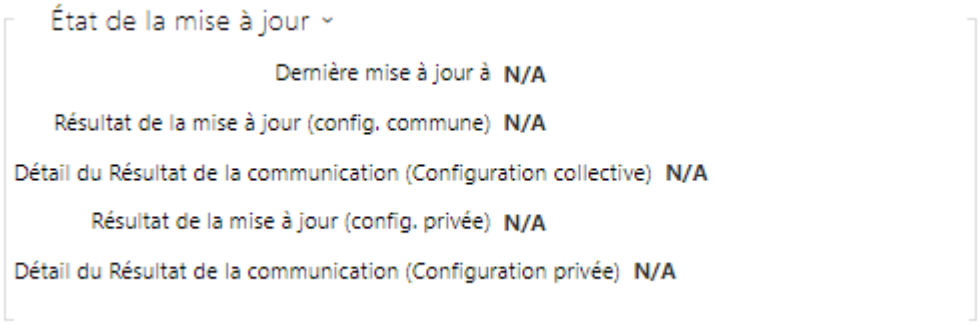
- **Utiliser l'authentification** – activez l'authentification pour l'accès au serveur HTTP.
- **Nom d'utilisateur** – entrez le nom d'utilisateur pour l'authentification du serveur.
- **Mot de passe** – entrez le mot de passe pour l'authentification du serveur.
- **Vérifier le certificat du serveur** – définit une liste des autorités de certifications pour vérifier la validité du certificat public du serveur ACS.
- **Certificat du client** – définit le certificat client et la clé privée qui autorise l'interphone à communiquer avec le serveur ACS.

Note

- L'interphone contient le certificat d'usine, un certificat signé utilisé pour l'intégration de British Telecom, par exemple.



- **Au démarrage** – activez la vérification et, si possible, mettez à jour l'exécution à chaque démarrage d'interphone.
- **Période de mise à jour** – définissez la période de mise à jour. Définissez une mise à jour automatique pour qu'elle ait lieu toutes les heures / tous les jours / toutes les semaines / tous les mois ou définissez la période manuellement.
- **Mise à jour à** – définissez l'heure de mise à jour au format HH : MM pour la mise à jour périodique à une heure de faible trafic. Le paramètre n'est pas appliqué si la période de mise à jour est définie sur une valeur inférieure à 1 jour.
- **Prochaine mise à jour à** – définissez l'heure de mise à jour suivante.



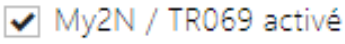
- **Dernière mise à jour à** – heure de la dernière mise à jour.
- **Résultat de la mise à jour (config. commune)** – résultat de la dernière mise à jour. Les options suivantes sont disponibles: L'option DHCP 66 a échoué, le firmware est à jour, la connexion au serveur a échoué, En cours d'exécution …, Fichier non trouvé.
- **Détail du Résultat de la communication (Configuration collective)** – code d'erreur de communication avec le serveur ou code d'état TFTP / HTTP.
- **Résultat de la mise à jour (config. privée)** – la configuration privée suit la mise à jour de la configuration commune. Le périphérique avec une configuration privée est identifié par son adresse MAC. Le dernier résultat de la mise à jour privée effectuée est affiché. Les options suivantes sont disponibles: L'option DHCP 66 a échoué, le firmware est à jour, la connexion au serveur a échoué, En cours d'exécution …, Fichier non trouvé.
- **Détail du Résultat de la communication (Configuration privée)** – code d'erreur de communication avec le serveur ou code d'état TFTP / HTTP.

My2N / TR069

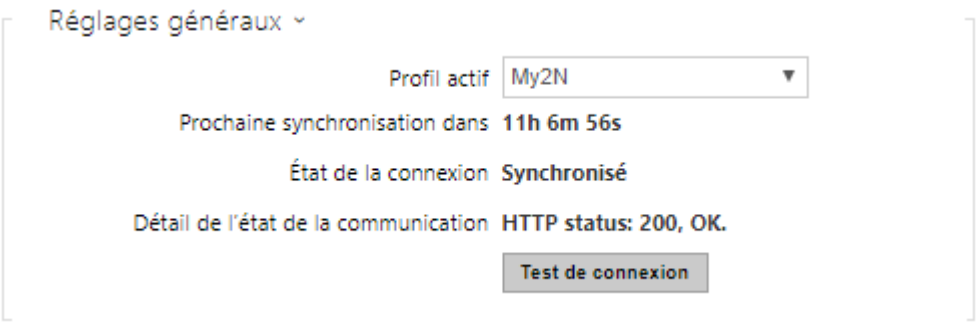
Utilisez cet onglet pour activer et configurer la gestion d'interphone à distance via le protocole TR-069. Le TR-069 vous aide à configurer de manière fiable les paramètres d'interphone, à mettre à jour et à sauvegarder la configuration et / ou à mettre à niveau le firmware du périphérique.

Le protocole TR-069 est utilisé par le service cloud My2N. Assurez-vous que le TR-069 est activé et que le profil Actif est défini sur My2N pour que votre interphone se connecte régulièrement à My2N pour la configuration.

Cette fonction vous aide à connecter l'interphone à votre ACS (serveur de configuration automatique). Dans ce cas, la connexion à My2N sera désactivée dans l'interphone.



- **My2N / TR069 activé** – activez la connexion à My2N ou à un autre serveur ACS.

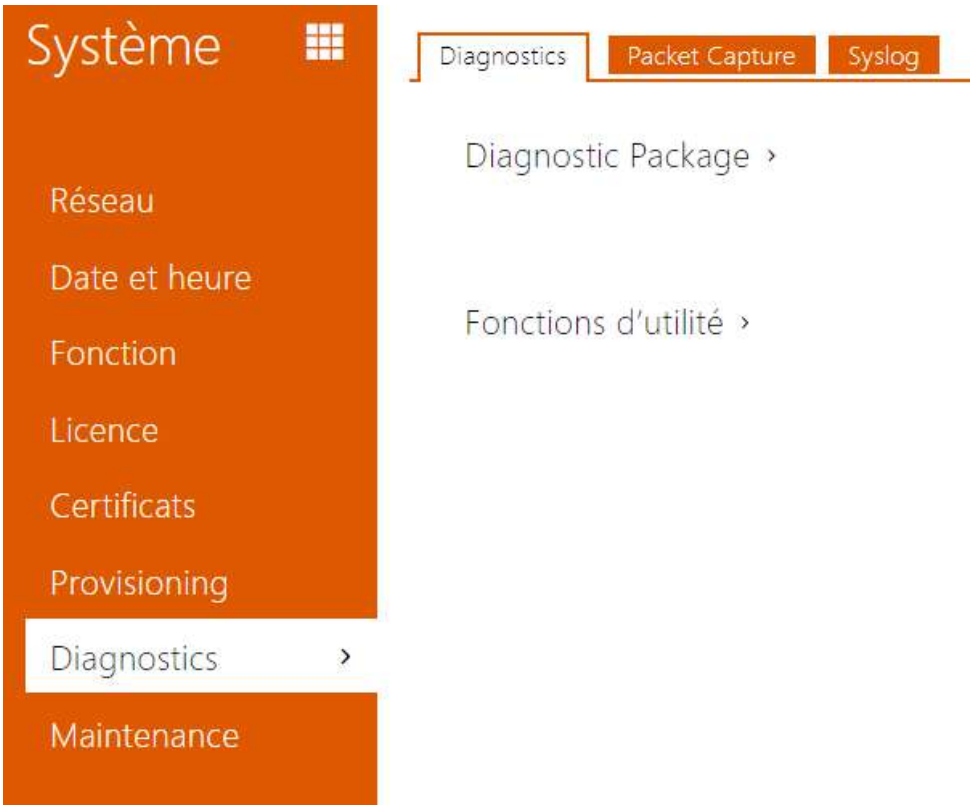


- **Profil actif** – sélectionnez l'un des profils prédéfinis (du serveur ACS) ou choisissez vos propres paramètres et configurer manuellement la connexion au serveur ACS.
- **Prochaine synchronisation dans** – affiche la période après laquelle l'interphone doit contacter un ACS distant.
- **État de la connexion** – affiche l'état actuel de la connexion ACS ou la description de l'état d'erreur si nécessaire.
- **Détail de l'état de la communication** – code d'erreur de communication avec le serveur ou code d'état du protocole HTTP.
- **Test de connexion** – testez la connexion TR069 en fonction du profil défini, voir le profil Actif. Le résultat du test est affiché dans l'état de la connexion.

- **Adresse du serveur ACS** – définissez l'adresse ACS au format suivant : ipadresse[: port], 192.168.1.1:7547, par exemple.
- **Nom d'utilisateur** – définissez le nom d'utilisateur pour l'authentification de l'interphone lors de la connexion au serveur ACS.
- **Mot de passe** – définissez le mot de passe pour l'authentification de l'interphone lors de la connexion au serveur ACS.

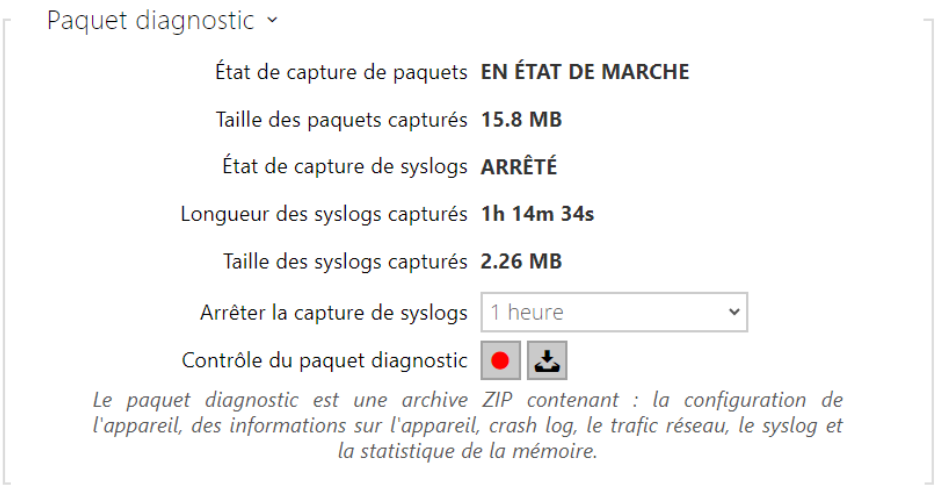
- **Vérifier le certificat du serveur** – définit une liste des autorités de certifications pour vérifier la validité du certificat public du serveur ACS. Si le certificat de l'autorité de certification n'est pas indiqué, le certificat public du serveur ACS n'est pas vérifié.
- **Certificat du client** – définit le certificat client et la clé privée qui autorise l'interphone à communiquer avec le serveur ACS. Sélectionner l'un des trois types de certificats ; se reporter au chapitre sur les Certificats.
- **Vérification périodique** – activez l'enregistrement périodique de l'interphone dans l'ACS.
- **Intervalle de vérification** – définissez l'intervalle d'enregistrement périodique de l'interphone dans le système ACS s'il est activé par le paramètre **Vérification périodique**.

5.6.7 Diagnostic



Diagnostic

L'interface permet de commencer à capturer des logs de diagnostic, qui peuvent ensuite être téléchargés et envoyés à l'Assistance technique. Les logs de diagnostic capturés permettent d'identifier et de résoudre les problèmes rapportés. Les logs contiennent des informations sur l'appareil, sa configuration, le trafic réseau, le crash log et la statistique de la mémoire.

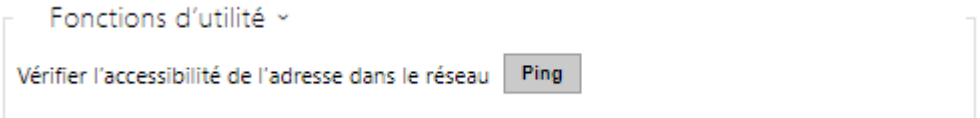


- **État de capture de paquets** – indique si la capture de paquets est lancée dans l'onglet Capture de paquets.
- **Taille des paquets capturés** – indique le nombre de paquets capturés.
- **État de capture de syslogs** – indique si la capture des messages syslog est lancée dans l'onglet Syslog.
- **Longueur des syslogs capturés** – indique la durée pendant laquelle les messages syslog sont capturés dans l'onglet Syslog.
- **Taille des syslogs capturés** – indique le nombre de messages syslog capturés.
- **Arrêter la capture de syslogs** – définit la période pendant laquelle les données seront capturées.

La capture est lancée à l'aide du bouton d'enregistrement  . Lorsque l'on appuie à nouveau sur le bouton d'enregistrement, la capture redémarre et recommence à fonctionner. Le fichier contenant les paquets capturés peut être téléchargé à l'aide du bouton  .

Observation

- Le lancement de la capture de données de diagnostic redémarre la capture de paquets si elle est déjà en cours d'exécution.



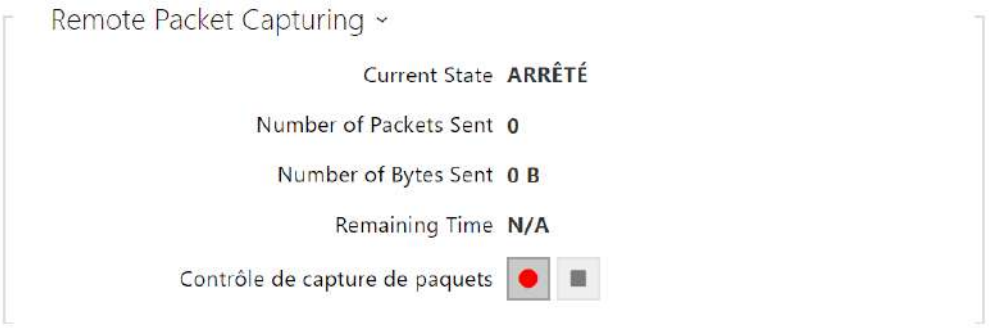
- **Vérifier l'accessibilité de l'adresse dans le réseau** – vérifiez l'accessibilité de l'adresse réseau via la commande Ping dans les systèmes d'exploitation standard. Appuyez sur Ping

pour afficher une boîte de dialogue, entrez l'adresse IP / le nom de domaine, puis cliquez sur Ping pour envoyer les données de test à cette adresse. Si l'adresse IP / le nom de domaine sélectionné n'est pas valide, un avertissement s'affiche et Ping reste inactif jusqu'à ce que l'adresse IP donnée devienne valide.
La progression de la fonction et le résultat sont également affichés dans la boîte de dialogue. Échec signifie : soit l'inaccessibilité de l'adresse IP donnée dans les 10 secondes, soit l'impossibilité de traduire le nom de domaine en une adresse. Si une réponse valide est reçue, l'adresse IP d'où provient la réponse et le temps d'attente de la réponse en millisecondes sont affichés.
Réappuyez sur Ping pour envoyer une autre requête à la même adresse.

Capture de paquets

Dans l'onglet Capture de paquets, vous pouvez lancer la capture des paquets entrants et sortants sur l'interface réseau d'interphone. Les paquets capturés peuvent être stockés soit localement dans la mémoire tampon de l'appareil, dont la taille dépend de l'appareil, soit à distance sur l'ordinateur de l'utilisateur, dont la limitation ne concerne que le temps de stockage indiqué et l'espace disque disponible. Le fichier contenant les paquets capturés peut être téléchargé et traité ultérieurement, par exemple à l'aide de l'application Wireshark (www.wireshark.org).

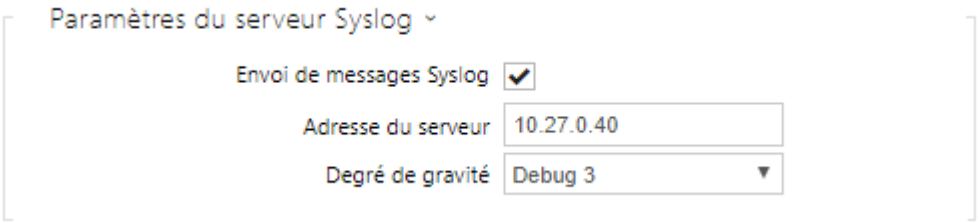
Une fois que la mémoire tampon est pleine durant la capture locale, les paquets stockés les plus anciens sont automatiquement copiés. Lors de la capture locale des paquets, nous recommandons de réduire le débit binaire du flux vidéo à une valeur inférieure à 512 kbps. Appuyez sur  pour démarrer,  pour arrêter et  pour télécharger le fichier de capture des paquets.



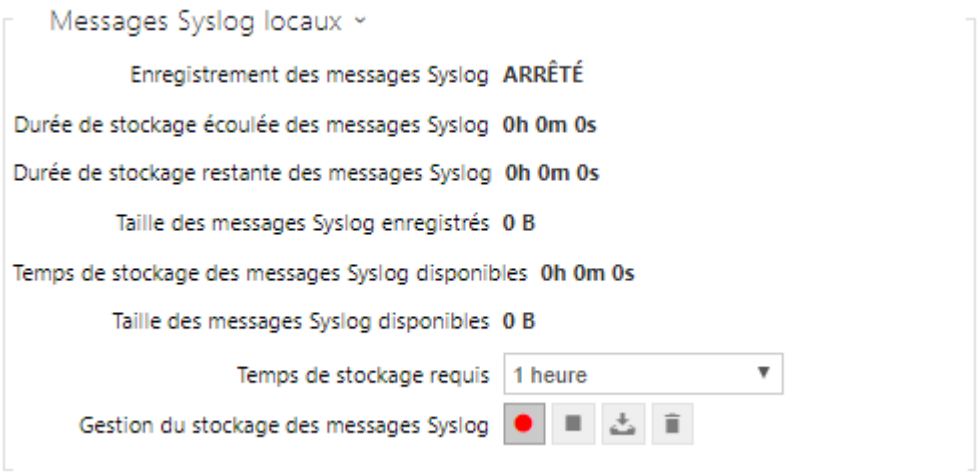
Vous pouvez lancer la capture à distance en appuyant sur le bouton . Il convient de spécifier le temps (s) durant lequel les paquets entrants et sortants doivent être capturés. Une fois la valeur de temps définie expirée, le fichier contenant les paquets capturés sera automatiquement téléchargé sur le PC de l'utilisateur. Arrêter la capture est possible à l'aide du bouton .

Syslog

Les **interphones IP 2N** vous permettent d'envoyer au serveur Syslog des messages système contenant des informations pertinentes sur les états des périphériques et les processus d'enregistrement, d'analyse et d'audit. Il n'est pas nécessaire de configurer ce service pour un fonctionnement classique de l'interphone.

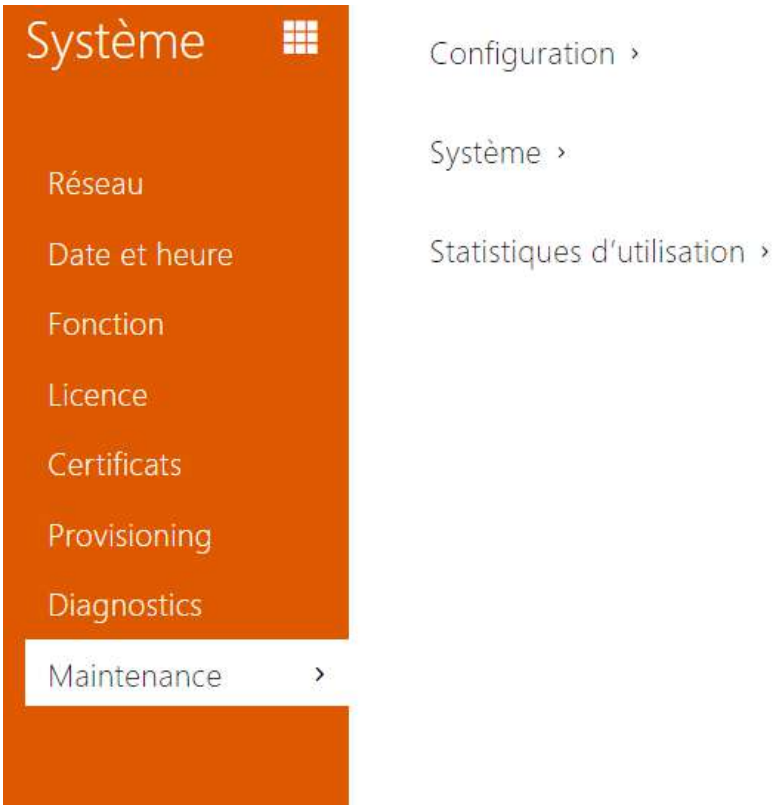


- **Envoi de messages Syslog** – activez l'envoi de messages système au serveur Syslog. Assurez-vous que l'adresse du serveur est bien paramétrée.
- **Adresse du serveur** – définissez l'adresse IP[:port] ou MAC du serveur sur lequel l'application s'exécute pour capturer les messages syslog.
- **Degré de gravité** – réglez le degré de gravité des messages à envoyer. (Erreur, Avertissement, Notification, Info, Debug 1–3). Le réglage du niveau n'est recommandé que pour faciliter le dépannage du service de support technique.



Présentation générale des messages syslog locaux.

5.6.8 Maintenance



Utilisez ce menu pour gérer la configuration de votre interphone et le firmware. Vous pouvez sauvegarder et réinitialiser tous les paramètres, mettre à jour le firmware et / ou réinitialiser les paramètres par défaut ici.

- **Restaurer la configuration** – restaurez la configuration d'une sauvegarde précédente. Appuyez sur le bouton pour afficher une fenêtre de dialogue vous permettant de sélectionner et de télécharger le fichier de configuration sur l'interphone. Avant de télécharger le fichier sur l'appareil, vous pouvez choisir d'appliquer les paramètres généraux, d'importer le répertoire, d'importer les paramètres réseau et les certificats ou de configurer la connexion à SIP à partir du fichier de configuration.

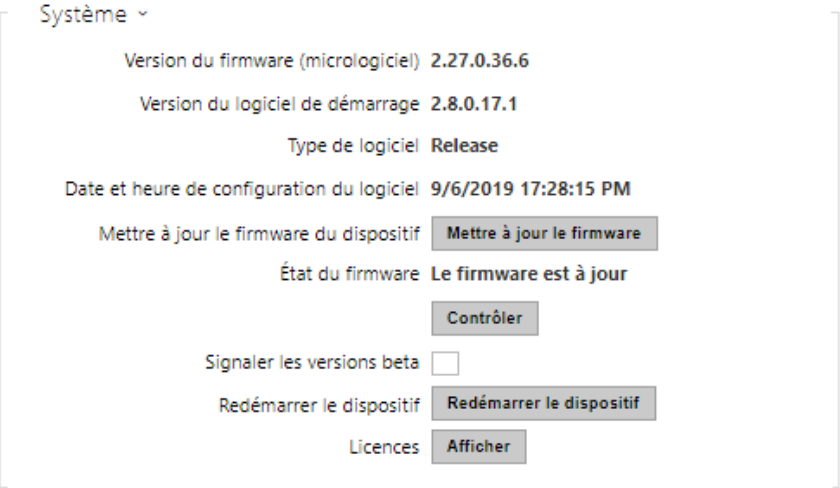
- **Enregister config**. – sauvegardez la configuration actuelle complète de votre interphone. Appuyez sur le bouton pour télécharger le fichier de configuration sur votre ordinateur.

> ⚠ **Observation**
>
> - *Traitez le fichier avec prudence, car la configuration de l'interphone peut inclure des informations délicates telles que les numéros de téléphone des utilisateurs et les codes d'accès.*

- **Réinitialiser la configuration** – réinitialisez les valeurs par défaut pour tous les paramètres d'interphone, à l'exception des paramètres réseau. Utilisez le cavalier correspondant ou appuyez sur Réinitialiser pour réinitialiser tous les paramètres d'interphone; reportez-vous au manuel d'installation de votre interphone.

> ⚠ **Observation**
>
> - *La réinitialisation d'état par défaut supprime la clé de licence, le cas échéant. Par conséquent, nous vous recommandons de le copier sur un autre stockage pour une utilisation ultérieure.*
> - *La clé de licence n'est pas supprimée dans le cas d'une réinitialisation matérielle HW (c'est-à-dire une réinitialisation à l'aide du bouton sur l'appareil), si la fonction de mise à jour automatique (Système/Licence) est activée, qui met à jour la clé de licence à partir du serveur de licences 2N. Une réinitialisation logicielle rétablit tous les paramètres à l'état d'usine, à l'exception des certificats et des paramètres réseau.*

- **Activer les paramètres réseau après la mise sous tension** – activez la restauration des paramètres du réseau par défaut en composant une séquence de boutons de numérotation rapide après le redémarrage du dispositif, tel que décrit dans la partie Configuration du Manuel d'installation de votre modèle respectif.



Note

- La fonctionnalité, la fiabilité et la sécurité de l'appareil dépendent du firmware installé.. La mise à jour régulière du firmware à la version actuelle fait partie des conditions d'utilisation du produit. Les erreurs qui peuvent être causées par l'utilisation d'une version obsolète du firmware ne peuvent pas faire l'objet d'une réclamation. Le firmware actuel met en œuvre les expériences des clients et les exigences dans le domaine de la sécurité des données personnelles.

- **Mettre à jour le firmware** – pour mettre à jour le firmware de votre interphone, appuyez sur le bouton pour afficher une fenêtre de dialogue vous permettant de sélectionner et de télécharger le fichier du firmware sur l'interphone. L'interphone sera automatiquement redémarré et un nouveau firmware sera alors disponible. La procédure complète de mise à jour dure moins d'une minute. Référez-vous au site www.2n.com. pour la dernière version FW de votre interphone. La mise à niveau du firmware n'affecte pas la configuration car l'interphone vérifie le fichier pour empêcher le téléchargement d'un fichier erroné ou corrompu.

Avertissement

- Les rétrogradations du firmware sur les appareils à processeur Artpec provoquent une réinitialisation d'usine qui perd toute la configuration, y compris les clés de licence. Nous vous recommandons de sauvegarder votre configuration et d'enregistrer la clé de licence valide avant de rétrograder.

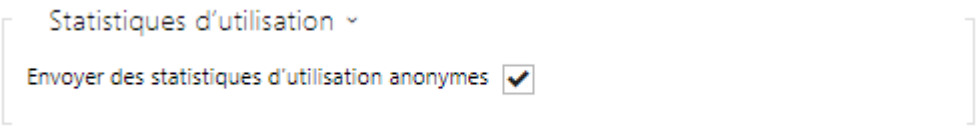
- **Contrôle** – vérifiez en ligne si une nouvelle version du firmware est disponible. Si tel est le cas, téléchargez la nouvelle version du firmware et une mise à niveau automatique du périphérique suivra.

- **Redémarrer le dispositif** – redémarrez l'interphone. Le processus prend environ 30 s. Lorsque l'interphone a obtenu l'adresse IP au redémarrage, la fenêtre de connexion s'affiche automatiquement.

Observation

- L'écriture de changement de configuration de l'interphone prend 3 à 15 s, en fonction de la taille de la configuration. Ne redémarrez pas l'interphone pendant ce processus.

- **Afficher** – cliquez sur Afficher pour afficher une fenêtre de dialogue comprenant une liste des licences utilisées et des logiciels tiers, ainsi qu'un lien CLUF.



- **Envoyer des statistiques d'utilisation anonymes** – permettre l'envoi de données statistiques anonymes sur l'utilisation de l'appareil au fabricant. Aucune information aussi délicate que les mots de passe, codes d'accès ou numéros de téléphone n'est incluse. Cette information aide 2N TELEKOMUNIKACE a.s. améliorer la qualité, la fiabilité et les performances du logiciel. Votre participation est volontaire et vous pouvez annuler cet envoi à tout moment.

5.7 Ports Utilisés

Services	Port	Protocoles	Direction	Activé par défaut	Configurable	Paramètres
802.1x	–	–	In/Out	non	non	–
DHCP	68	UDP	In/Out	oui	non	–
DNS	53	TCP/ UDP	In/Out	oui	non	–
Echo (device discovery)*	8002	UDP	In/Out	oui	non	–
FTP	21	TCP	Out	non	non	–
2N IP Eye	8003	UDP	Out	non	non	–
HTTP	80	TCP	In/Out	oui	oui	5.4.8 Web server

Services	Port	Protocoles	Direction	Activé par défaut	Configurable	Paramètres
HTTPS	443	TCP	In/Out	oui	oui	5.4.8 Web server
Multicast audio	22222	UDP	Out	non	oui	5.4.2 Streamování
Multicast audio for ICU protocol	8006	UDP	Out	oui	non	–
Multicast video for ICU protocol	8008	UDP	Out	oui	non	–
Multicast video (wide) for ICU protocol	8016	UDP	In/Out	oui	non	–
NTP client	123	UDP	In/Out	oui	non	–
ONVIF	80, 443, 3702	TCP/ UDP	In/Out	non	non	–
RTP+RTCP ports (SIP)	4900+ (range of 64 ports)	UDP	In/Out	non	oui	5.4.1 Téléphone
RTP+RTCP ports (caméra externe)	4800+ (range of 64 ports)	UDP	In/Out	non	oui	5.4.2 Streamování
RTSP client	554	UDP	In/Out	non	oui	5.4.1 Téléphone
RTSP server	554	UDP	In/Out	non	non	–
SingleWire Commands	80	TCP	In/Out	oui	non	–

Services	Port	Protocoles	Direction	Activé par défaut	Configurable	Paramètres
SingleWire Communication	8081	TCP	Out	oui	non	–
SLP	427	UDP	In/Out	oui	non	–
SingleWire Media	20000+	UDP	In	oui	non	–
SIP	5060, 5062	TCP/ UDP	In/Out	non	oui	5.4.1 Téléphone
SIPS	5061	TCP	In/Out	non	oui	5.4.1 Téléphone
SMTP	25	TCP	Out	non	oui	5.4.3 E-Mail
Syslog	514	UDP	Out	non	non	–
TFTP	69	UDP	Out	oui	non	–
My2N Knocker	443	TCP	Out	oui	non	–
My2N Tribble Tunnel	443	TCP	Out	oui	non	–
SNMP Agent	161	UDP	In/Out	oui	non	–
SNMP Trap	162	UDP	Out	oui	non	–
SSDP	1900	UDP	In/Out	oui	non	–
SDDP	1902	UDP	In/Out	oui	non	–
Multicast receiver (Automation)	4433	UDP	In	non	non	–
WS-Discovery	3702	UDP	In/Out	oui	non	–

Services	Port	Protocoles	Direction	Activé par défaut	Configurable	Paramètres
CIP Client (Crestron)	41794	UDP	In/Out	non	non	–
Sitechannel (ICU protocol)	8004	UDP	In/Out	oui	non	–

Echo – il s'agit d'un protocole propriétaire pour la découverte de l'interphone dans le réseau. Utilisé dans les applications: **2N® IP Network Scanner**, **2N® IP Eye**, **2N® Access Commander**.

6. Informations supplémentaires

Voici les différents onglets que vous pourrez trouver dans cette section :

6.1 Dépannage

Vous trouverez les problèmes le plus souvent traités sur le site faq.2n.cz.

6.2 Directives, lois et réglementations

2N® IP Interkom est en accord avec les directives et réglementations suivantes:

- 2014/35/UE relative au matériel électrique destiné à être employé dans certaines limites de tension
- 2014/30/UE relative à la compatibilité électromagnétique
- 2011/65/UE relative à la limitation de l'utilisation de certaines substances dangereuses dans les équipements électriques et électroniques
- 2012/19/UE relative aux déchets d'équipements électriques et électroniques

Industry Canada

Cet appareil de classe B est conforme aux exigences de la norme canadienne ICES/NMB-003.

FCC

Cet équipement est certifié en conformité avec les exigences relatives aux appareils numériques de classe B en vertu de la partie 15 des règles de la FCC.

REMARQUE: Le but de ces exigences est d'établir une protection raisonnable contre les interférences nuisibles des ondes dans les installations résidentielles. Cet appareil génère, utilise, et peut émettre de l'énergie haute fréquence, et peut interférer de manière nuisible avec les communications radio s'il n'est pas installé et utilisé conformément aux instructions.

Il n'est cependant pas possible de garantir qu'aucune interférence ne se produira dans telle ou telle installation particulière. Si cet équipement provoque des interférences nuisibles à la réception de la radio ou de la télévision (ce qui peut être déterminé en allumant puis éteignant l'appareil) son utilisateur peut essayer de corriger les interférences en mettant en œuvre les mesures suivantes:

- Rediriger ou déplacer l'antenne ou la ligne de réception
- Accroitre la distance entre l'appareil et le récepteur

- Relier l’équipement à une prise branchée sur un circuit différent de celui auquel le récepteur est connecté.
- Avoir recours à un vendeur ou à un technicien radio/TV spécialisé

Les changements ou modifications de l’appareil qui n’ont pas été explicitement approuvés par l’instance responsable de sa conformité aux normes peuvent entraîner une annulation du droit de l’utilisateur à utiliser cet équipement.

6.3 Instructions générales et précautions

Avant d'utiliser ce produit, veuillez lire attentivement ce mode d'emploi et suivez les consignes et les recommandations qui y figurent.

Si le produit est utilisé d'une manière autre que celle spécifiée dans ce mode d'emploi, ceci peut entraîner un dysfonctionnement, un endommagement ou une destruction du produit.

Le fabricant n'est pas responsable d'un quelconque dommage causé par une utilisation du produit d'une manière autre que celle spécifiée dans ce mode d'emploi, c'est-à-dire en cas d'utilisation incorrecte et de non-respect des recommandations et des avertissements.

Toute utilisation ou branchement du produit autre que ceux indiqués dans le mode d'emploi est considéré comme incorrect et le fabricant décline toute responsabilité quant aux conséquences d'un tel acte.

Le fabricant n'est pas responsable d'un endommagement ou d'une destruction du produit causé par un emplacement ou une installation inapproprié, une utilisation incorrecte ou une utilisation du produit non conforme à ce mode d'emploi.

Le fabricant décline toute responsabilité en cas de dysfonctionnement, endommagement ou destruction du produit causé par un remplacement de pièces non professionnel ou par l'utilisation de pièces de rechange non originales.

Le fabricant n'est pas responsable d'une perte ou d'un endommagement du produit causé par une catastrophe naturelle ou par l'effet d'autres conditions naturelles.

Le fabricant n'est pas responsable d'un endommagement du produit survenu lors de son transport.

Le fabricant ne fournit aucune garantie pour la perte ou la corruption de données.

Le fabricant décline toute responsabilité en cas de dommages directs ou indirects causés par une utilisation du produit non conforme à ce mode d'emploi ou par une défaillance du produit due à une utilisation du produit non conforme à ce mode d'emploi.

Lors de l'installation et de l'utilisation du produit, les dispositions légales ou les dispositions des normes techniques pour les installations électriques doivent être respectées. Le fabricant décline toute responsabilité en cas d'endommagement ou de destruction du produit ou de préjudice causé au client en cas de manipulation du produit non conforme aux normes mentionnées.

Le client est tenu d'assurer à ses frais la protection logicielle du produit. Le fabricant décline toute responsabilité en cas de dommages causés par une protection insuffisante.

Le client est tenu de changer immédiatement après l'installation le mot de passe d'accès au produit. Le fabricant n'est pas responsable des dommages causés dans le cadre de l'utilisation du mot de passe d'accès d'origine.

Le fabricant n'est pas non plus responsable des surcoûts encourus par le client à cause d'appels à des numéros à tarification majorée.

Traitement des déchets électriques et des accumulateurs usagés

Les appareils électriques et accumulateurs usagés n'ont pas leur place dans les déchets municipaux. Leur mauvaise élimination peut causer des dommages à l'environnement!

Déposez les appareils électriques domestiques arrivés en fin de vie et les accumulateurs usagés retirés de l'appareil dans les déchetteries spécialisés ou remettez-les au vendeur ou au fabricant qui assurera leur traitement écologique. La reprise est gratuite et n'est pas soumise à l'achat d'un autre produit. Les appareils remis doivent être complets.

N'incinérez pas les accumulateurs, ne les démontez pas et ne les court-circuitez pas.