Manuel de Configuration des 2N Access Unit

v.2.43

www.2n.com

Contenu:

1. Vue d'ensemble du produit

Les unités d'accès 2N comprennent **2N Access Unit, 2N Access Unit 2.0, 2N Access Unit QR et 2N Access Unit M.** Les unités d'accès 2N, associées à des logiciels supplémentaires et à des interphones IP 2N, peuvent offrir une solution de contrôle d'accès complète pour n'importe quelle installation.

Les unités d'accès 2N peuvent être utilisées comme serrure à code en combinaison avec un clavier numérique.

Les unités d'accès 2N peut aussi être équippée avec un autre lecteur de cartes RFID, afin qu'elle soit utilisée dans votre entreprise comme un composant de votre système de sécurité ou de votre système de pointage.

Les unités d'accès 2N peuvent être équipées d'un interrupteur à relais (en option, d'autres relais et sorties), qui peut être utilisé pour commander une serrure électrique ou d'autres dispositifs qui y sont connectés. Les unités d'accès peuvent être réglées de manière très flexible, par exemple en ce qui concerne le moment et la manière dont ces interrupteurs doivent être activés - par code, automatiquement, en appuyant sur un bouton, etc.

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

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.

Connexion avec le nom de domaine

Il est possible de se connecter à l’appareil en saisissant le nom de domaine au format hostname.local (par ex. 2NAccessUnitM-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 Access Unit	2NAccessUnit
2N Access Unit 2.0	2NAccessUnit20
2N Access Unit M	2NAccessUnitM
2N Access Unit QR	2NAccessUnitQR

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.

Connexion avec l'adresse IP

Entrez l'adresse IP dans votre navigateur web favori. Nous vous recommandons d'utiliser la dernière version de Chrome, Firefox ou Internet Explorer (Edge) comme l'**unité de contrôle d'accès 2N** n'est pas complètement compatible avec les version plus anciennes.

Données de connexion

Utilisez le nom "admin" et le mot de passe "2n" (i.e. mot de passe RESET par défaut) pour votre première connection à l'interface de configuration. Nous vous recommandons de changer le mot de passe par défaut dès la première connection; référez vous au paramètre MOT DE PASSE dans le menu **Services > Serveur Web**. Souvenez vous du mot de passe, ou écrivez le. Parce que si vous oubliez le mot de passe, vous allez devoir remettre à zéro l'interphone (référez vous au manuel d'installation) et donc perdre tous vos changements de configuration.

Paramètres de connexion réseau (LAN – s'applique à 2N Access Unit, 2N Access Unit 2.0 a 2N Access Unit M)

La récupération automatique de l'adresse IP depuis le serveur DHCP est choisie par défaut dans l'**unité de contrôle d'accès 2N**. C'est pourquoi, si connecté sur un réseau dans lequel est présent un serveur DHCP configuré pour attribuer automatiquement les adresses IP à tous les nouveaux appareils disponibles, l'**unité** obtiendra son adresse IP depuis le serveur DHCP. L'adresse IP de l'**unité de contrôle d'accès 2N** peut être trouvée dans les paramètres du serveur DHCP (selon l'adresse MAC donnée par la plaque de production), ou vous sera communiquée par la fonction vocale de l'**unité de contrôle d'accès 2N**; référez vous au manuel d'installation.

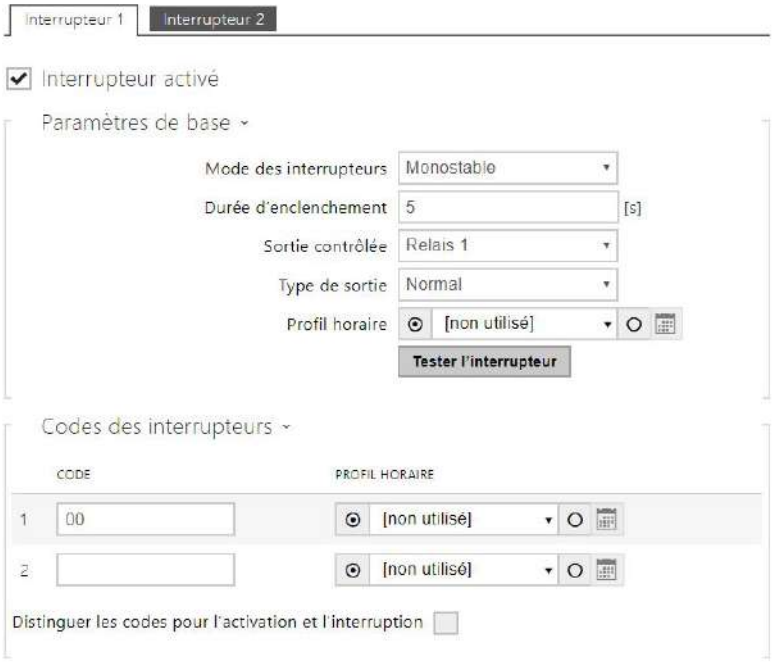
S'il n'y a pas de serveur DHCP sur votre réseau local, utilisez le bouton RESET de l'**unité de contrôle d'accès 2N** pour activer le mode adresse IP statique; référez vous au manuel d'installation. L'adresse de votre unité sera donc **192.168.1.100**. Utilisez la pour la première connection et ensuite changez la si nécessaire.

Chargement de firmware

Nous vous recommandons également de mettre à jour le firmware dès votre première connection à l'**appareil**. Référez vous à 2N.com pour la dernière version du firmware. Pressez le bouton **Mettre à jour le firmware** dans le menu **Système > Maintenance** pour charger le firmware. L'unité redémarrera pendant la mise à jour et seulement après, le processus de mise à jour sera complété. Le processus dure environ 1 minute.

Réglage des interrupteurs de déverrouillage électrique

Une gâche électrique peut être connectée à l'**Unité de contrôle d'accès 2N** et contrôlée par un code depuis le clavier numérique. Connectez la serrure électrique comme indiqué dans le manuel d'installation de votre modèle d'unité de contrôle d'accès.



Activez l'interrupteur dans le paramètre *Interrupteur activé* sur l'onglet **Hardware > Interrupteurs > Interrupteur 1**, paramètrerez la Sortie contrôlée de l'appareil sur la sortie sur laquelle est connectée la gâche électrique. Définissez maintenant un ou plusieurs codes d'activation pour la commutation du verrouillage électrique des portes.

3. Fonctionnalités sous license

Les unités d'accès 2N prennent en charge les licences standard qui sont déjà incluses dans l'appareil. Il s'agit des licences Enhanced Integration, Enhanced Security et NFC. La licence NFC ne peut être utilisée qu'avec la variante de **2N Access Unit** ou **2N Access Unit 2.0** qui comprend un lecteur de cartes de 13.56 MHz.

Le tableau ci-dessous donne un aperçu des licences et de leurs caractéristiques.

License	Features	2N Access Unit 1.0	2N Access Unit 2.0	2N Access Unit M
Enhanced Integration (Standard license part of the device)	Advanced switch setting options	✅	✅	✅
	HTTP API	✅	✅	✅
	Automation function	✅	✅	✅
	E-mail sending (SMTP client)	✅	✅	✅
	Automatic update (TFTP/HTTP client)	✅	✅	✅
	FTP client	✅	✅	✅
	SNMP client	✅	✅	✅
	TR-069	✅	✅	✅
	Synergis	✅	✅	✅
Enhanced Security (Standard license part of the device)	802.1x support	✅	✅	✅
	SIPS (TLS) support	✅	✅	✅
	Switch Blocking by Tamper	✅	✅	✅
	SRTP support	❌	❌	❌
	Silent alarm	✅	✅	✅
	Limit unsuccessful access attempts	✅	✅	✅
	Anti-Passback	✅	✅	✅
	Scrambled keypad	❌	❌	❌
NFC (Standard license part of the device)	NFC support	✅	✅	✅
Lift Control Support	Lift Control	✅	✅	✅

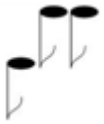
✅ – Native
⭐ – Fonctionnalité sous licence, peut être achetée
❌ – Indisponible

4. Signalisation du statut opérationnel

Les unités d'accès 2N émet des sons qui signalent les changements des statuts opérationnels. Chaque changement d'état se voit attribué 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	Signification
	**Application Interne lancée** L'application interne est lancée à la mise sous tension ou au redémarrage de l'appareil. Un lancement réussi est signalé par cette combinaison de tonalités.
	**Connecté au LAN, Adresse IP attribuee** L´appareil s'enregistre au lancement de l'application interne. 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'appareil.
	**Réinitialisation par défaut des paramètres réseaus** À la mise sous tension, un délai de 30 s est défini pour la saisie du code de réinitialisation par défaut. Reportez-vous au Manuel d'installation pour plus de détails.

5. Configuration de l’interface Web

Ecran de démarrage

L’écran de démarrage est une vue d’introduction affichée après la connection à l’interface web de l´appareil. Utilisez le bouton dans le coin en haut à gauche des pages web suivantes pour revenir à cet écran à n’importe quel moment.

Le haut de l’écran inclut le nom de l'appareil (référez vous au paramètre *Nom de l’appareil* dans l’onglet **Services > Serveur web**). 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 d’accueil est aussi le premier niveau de menu et un moyen de navigation rapide (cliquez sur un carré) pour accéder aux sections de configuration. Certaines vignettes affichent également l'état des services sélectionnés.

Menu de configuration

La configuration de l'appareil inclut 5 menus : **État, Répertoire, Hardware, Services** et **Système, lesquels** intègrent des sous menus comme indiqué ci dessous :

État

- **Appareil** – informations essentielles sur l'appareil
- **Services** – informations sur les services actifs et leurs statuts
- **Licences** – etat actuel des licences et fonctionnalités disponibles sur l'appareil
- **Registre d'accès** – liste des dix dernières cartes d'accès
- **Événements** – liste des événements

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

Hardware

- **Interrupteurs** – déverrouillage électrique, éclairage, temporisation...etc.
- **Audio** – audio, signalisation, paramètres de volume, etc.
- **Clavier** – clavier et paramètre de code d'accès
- **Rétroéclairage** – intensité du rétro éclairage
- **Lecteur de cartes** – lecteur de carte, interface Wiegand
- **Entrées logiques** – management des entrées logiques
- **Extendeurs** – paramètres des modules d'extension de l'appareil
- **Ascenseur** – réglages de l'accès aux différents étages par l'ascenseur

Services

- **Contrôle de l'accès** – définition des règles d'entrée et de sortie
- **E-mail** – envoi d'emails lors d'accès refusés par exemple
- **Mobile Key** – paramètres Bluetooth et gestion des appareils appairés
- **Automatisation** – automatismes flexibles de l'unité 2N adaptés en fonction du besoin de l'utilisateur
- **API HTTP** – paramètres d'autorisation HTTP API
- **Serveur web** – serveur Web et paramètres du mot de passe d'accès
- **SNMP** – fonctionnalité permettant la surveillance à distance sur le réseau de l'unité 2N en utilisant le protocol SNMP

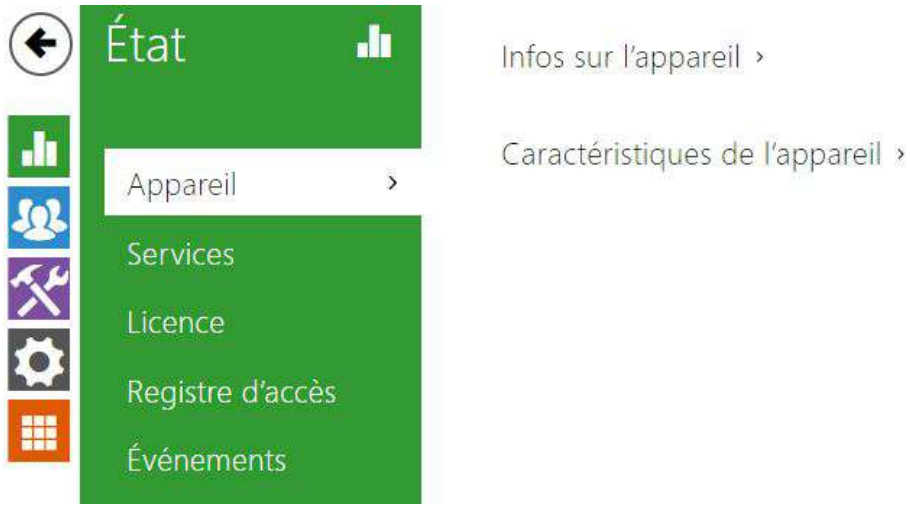
Système

- **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
- **Licence** – 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.

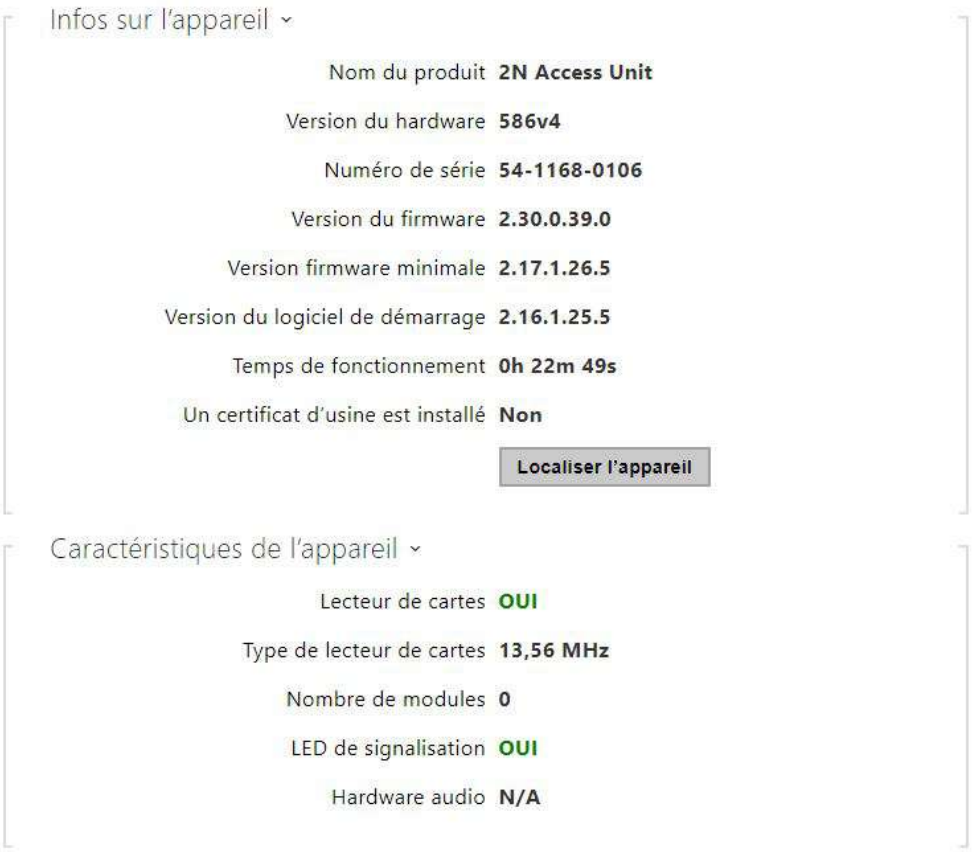
5.1 État



Le menu **État** vous permet d'accéder au statut ainsi qu'à d'autres informations de l'appareil. Son menu est divisé comme suivant :

Appareil

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



Services

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

Registre d’accès

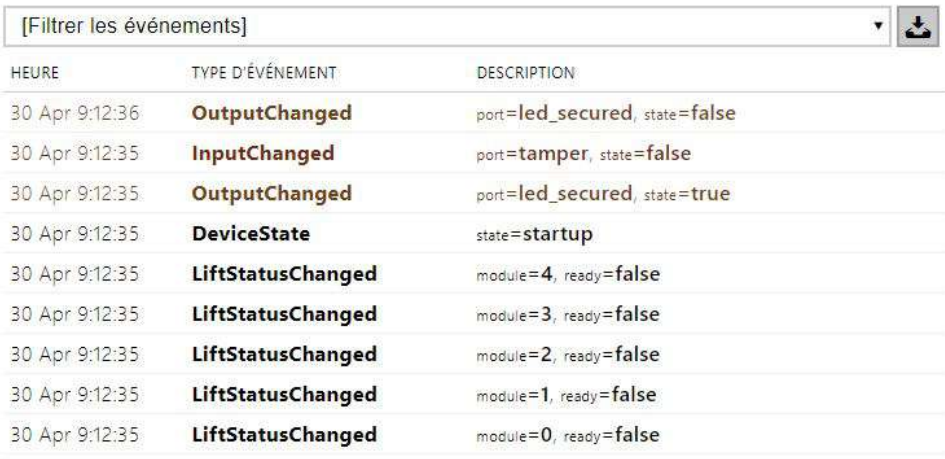
L'onglet **Registre d’accès** affiche les 10 derniers enregistrements de cartes RFID badgées sur le lecteur de l'appareil. Chaque enregistrement comprend l'heure de passage de la carte, son identifiant, son type et sa description (validité, propriétaire de la carte, etc.).


Registre d’accès

	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

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.



-  – presser ce bouton pour exporter tous les événements dans 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.
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.

Evénements	Signification
DoorStateChanged	Détection d'une porte ouverte / fermée. Les réglages peuvent être effectués dans la section Hardware / Porte / Porte.
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 …).
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.
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.

Evénements	Signification
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.
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.

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´appareil. Il contient des informations importantes sur les utilisateurs qui permettent d'exécuter des fonctions telles que l'ouverture de portes avec des cartes RFID, l'activation de serrures à code, la notification d'accès aux utilisateurs par courrier électronique, etc.

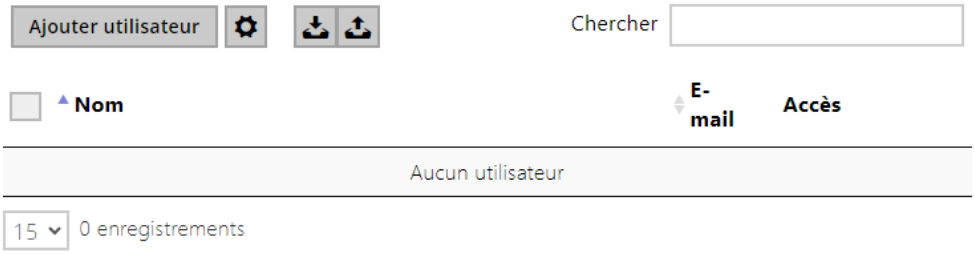
La liste d'Utilisateurs contient jusqu'à 10 000 utilisateurs - typiquement chaque utilisateur se voit assigner une position. Elle regroupe les utilisateurs à qui l'on a attribué une carte RFID, un code d'accès...etc.

Si un lecteur de carte externe est connecté à l´appareil 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´appareil : 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 sont 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´appareil.

Une fois que la carte a été lue par le lecteur, elle est comparée à la base de données de l´appareil. 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** ou le paramètre Interrupteur dans le menu **Hardware > Module Lecteur de carte**.



La fonction Recherche dans la liste des utilisateurs fonctionne en texte intégral par noms d'utilisateur et adresses électroniques. Elle recherchera toute correspondance dans le répertoire. Un nouvel Utilisateur est ajouté à l'aide du bouton situé au-dessus du tableau. Cliquez sur our 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.

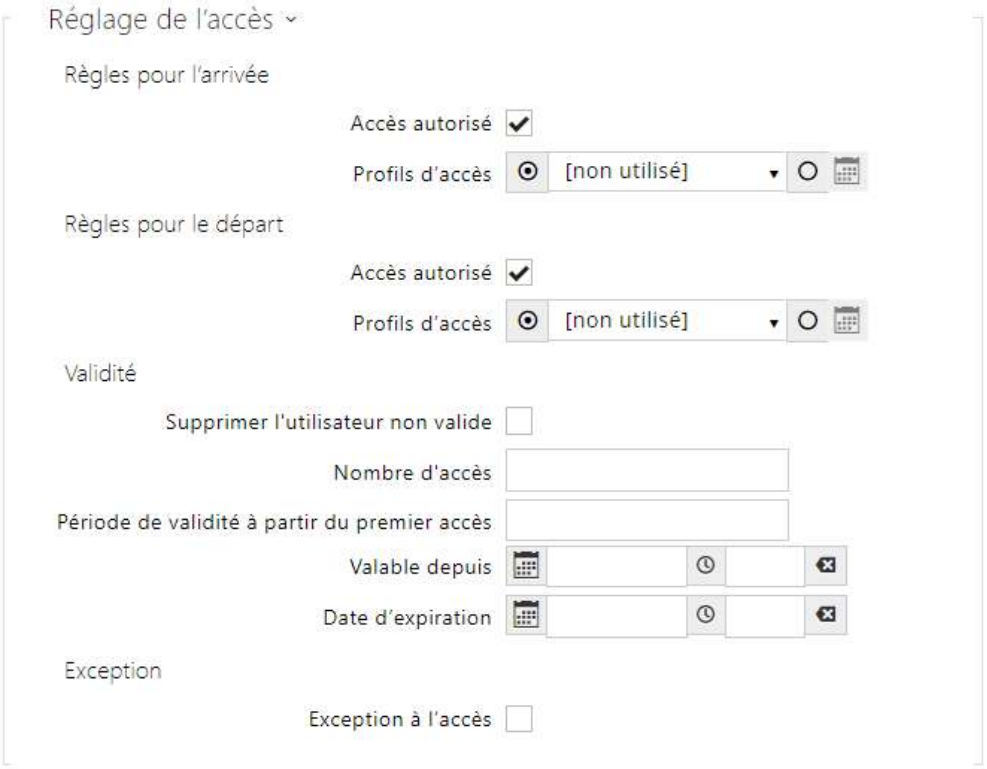
Vous pouvez exporter/importer un fichier CSV contenant une liste d'utilisateurs depuis/vers l'appareil à l'aide de l'icône / . Si le répertoire est vide, un fichier avec l'en-tête uniquement (en anglais) est exporté et peut servir de modèle pour l'importation d'utilisateurs. Si un fichier vide contenant uniquement l'en-tête est importé et que l'option **Remplacer le répertoire** est sélectionnée, le répertoire entier est supprimé. 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.
- **E-mail** – l'adresse électronique de l'utilisateur, utilisée pour l'envoi d'informations par courrier électronique, par exemple sur l'accès de l'utilisateur à l'objet ou sur l'utilisation de 2N Automation. Vous pouvez entrer plusieurs adresses électroniques séparées par des virgules des point-virgules.



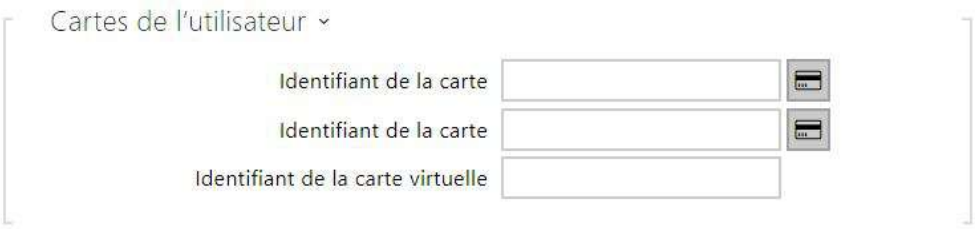
- **Règles pour l'arrivée**
  - **Accès autorisé** – il autorise l'authentification à ce point d'accès.
  - **Profils d'accès** – sélectionnez l'un des profils prédéfinis dans la section **Répertoire > Profils horaires** ou bien définissez le profil temporel manuellement.
- **Règles pour le départ**
  - **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.

  - **Période de 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 un code d'activation d'interrupteur personnel. 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'appareil, 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** – définissez un code d'activation de commutateur d'utilisateur privé : usqu'à 16 caractères, chiffres compris entre 0 et 9 uniquement. Le code doit contenir au moins deux caractères pour déverrouiller la porte en utilisant le clavier de l'appareil et au moins un caractère pour déverrouiller la porte en utilisant DTMF du téléphone.
  - 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'appareil peut se voir attribuer deux cartes RFID d'accès.

- **Identifiant de la carte** – 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. Après l'identification de l'utilisateur, l'ID de la carte virtuelle sur le lecteur Bluetooth ou biométrique est envoyé à l'interface Wiegand si la configuration (Services > Contrôle de l'accès) est réglée pour envoyer les ID à Wiegand.

Cette section ne s'affiche que lorsque le module Bluetooth est connecté.

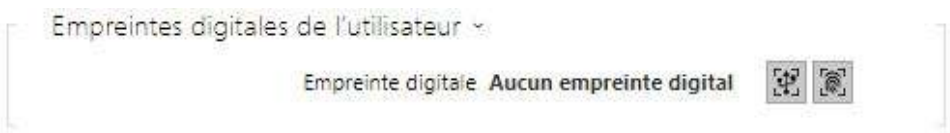
- **Auth ID** – identifiant unique WaveKey pour le contrôle d'accès. Il est enregistré sur le périphérique mobile lors du processus de couplage. L'ID d'authentification se compose de 32 caractères hexadécimaux.
- **Avancement de l'appariement** – état actuel du jumelage (Inactif, En attente de jumelage, PIN expiré ou Jumelage effectué).
- **Appariement 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'Appareil

Pour jumeler le Smartphone d'un utilisateur :

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

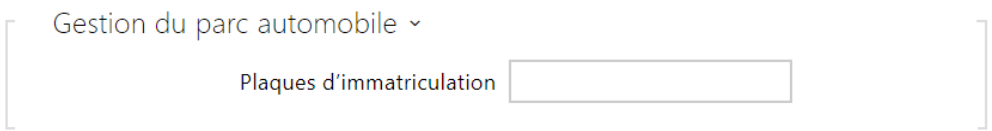


- **Empreintes digitales** – affiche le nombre d'empreintes digitales définies ; Vous pouvez définir jusqu'à 2 empreintes digitales différentes par utilisateur. Cette section ne s'affiche que si le module lecteur biométrique est disponible.
  - enrôlement via lecteur USB
  - enrôlement via le lecteur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



L´appareil 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.

- **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.

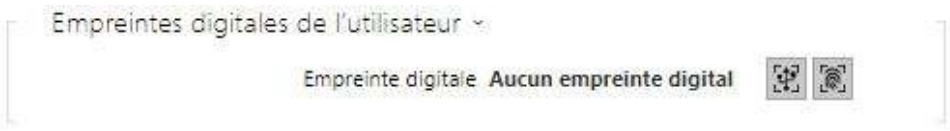
- **Étages** – sélectionnez les étages accessibles par l'utilisateur dans le cas d'un Contrôle d'accès dans l'ascenseur.

- **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.

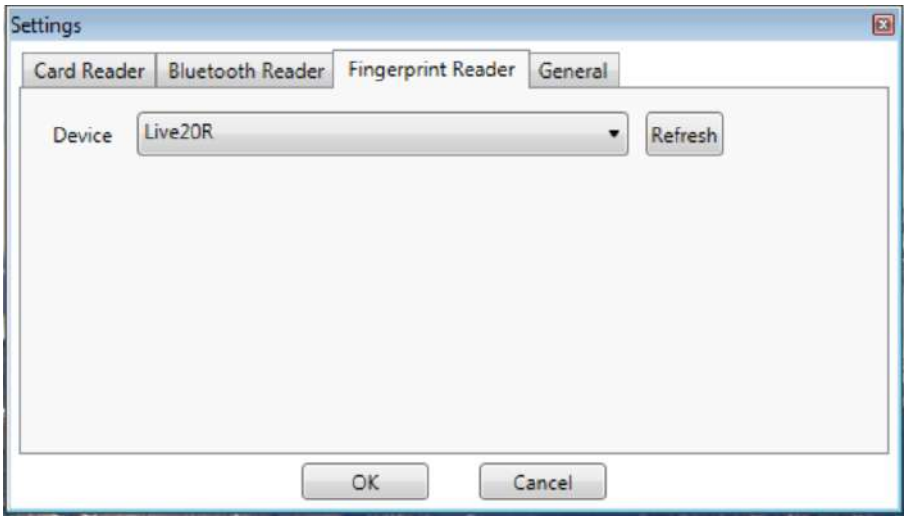
5.2.1.1 Configuration des empreintes digitales de l'utilisateur

Pour enregistrer des empreintes digitales, utilisez le lecteur **2N Access Unit Fingerprint** (référence 916019) 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 **l'unité de contrôle d'accès 2N** , utilisez l'interface web de l'utilisateur et cliquez sur . Enregistrez l'empreinte depuis le module à la section Répertoire / Utilisateurs / Empreinte digital .



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. Click Enregistrez l'empreinte depuis le module dans l'interface Web à la section Répertoire / Utilisateur.



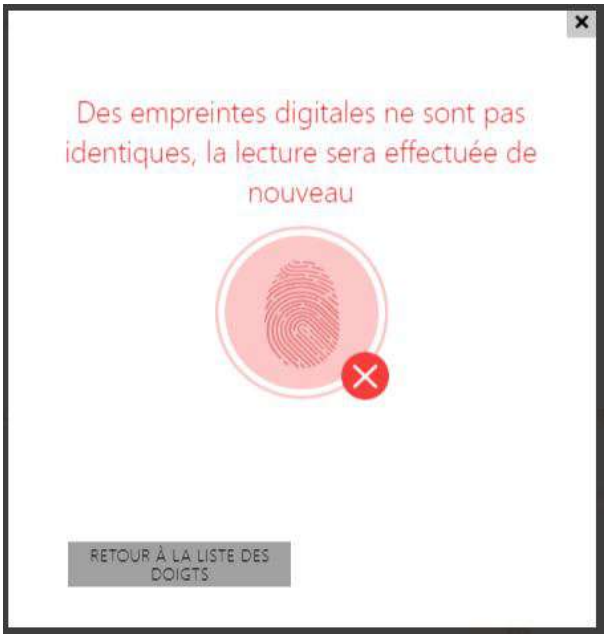
2) Cliquez sur l'un de ces deux boutons pour enregistrer une empreinte.

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.

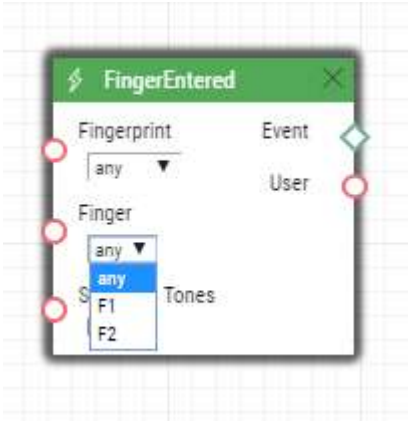
Répétez le processus si une incohérence se produit pendant la lecture des empreintes digitales.



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

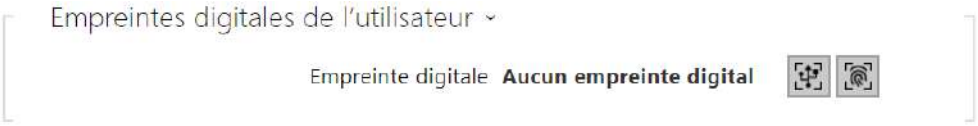
Pour définir la fonction de l'empreinte digitale, cliquez sur l'icone :

- 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.
- Automatisation 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.

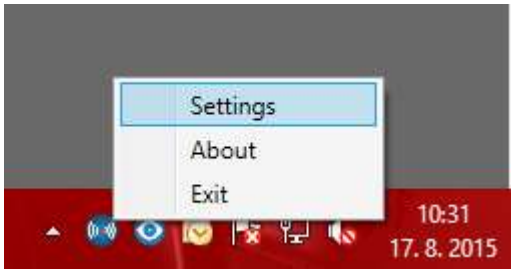
6) Vous pouvez vérifier les paramètres dans la fiche utilisateur.



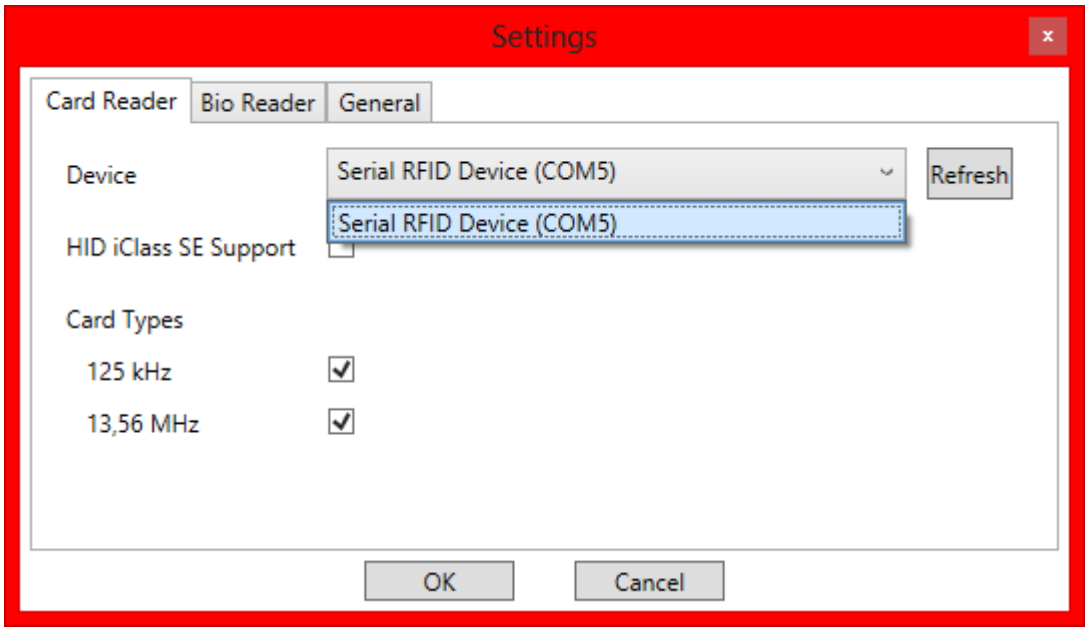
5.2.1.2 Lecteur de carte RFID USB

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

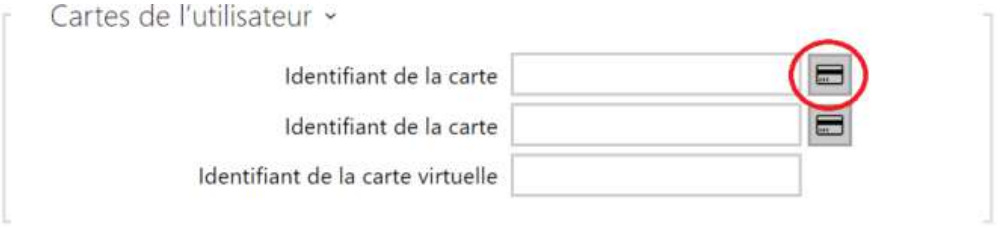
- Rendez vous dans **2N IP USB Driver**



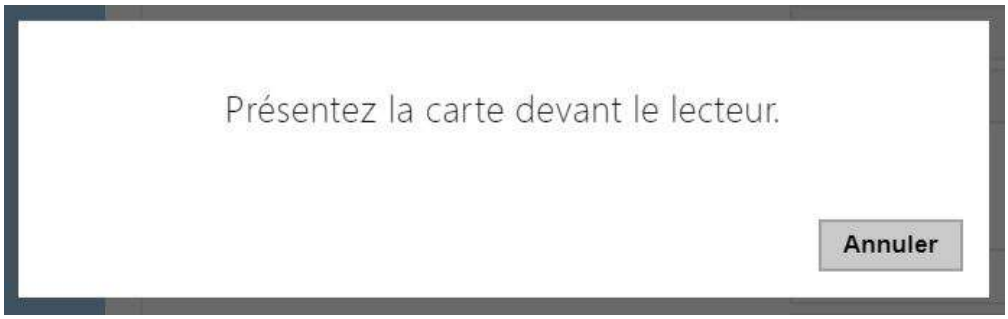
- Configurez le port COM pour le lecteur connecté.



- Pressez le bouton Lecture via l'interface web.



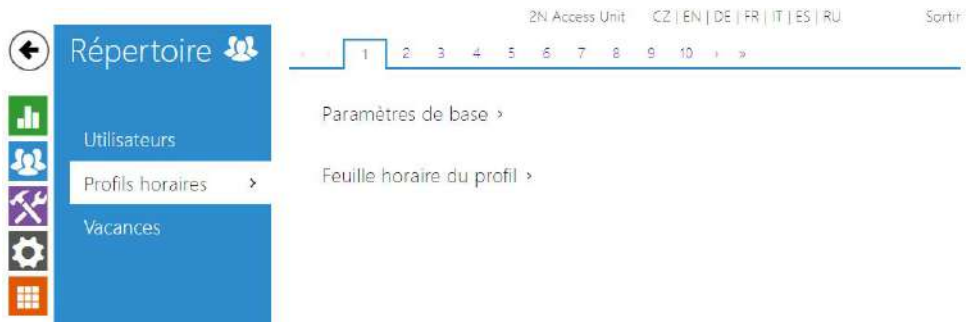
- Badgez la carte sur le lecteur.



- L'identifiant de la carte a été reconnu.

- N'oubliez pas de sauvegarder la configuration.

5.2.2 Profils horaires



Certaines fonctionnalités de l'unité de contrôle d'accès 2N, telles que l'accès par carte RFID ou code numérique par exemple, peuvent être définies selon des plages horaires en leur attribuant un **profil temporel**. 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

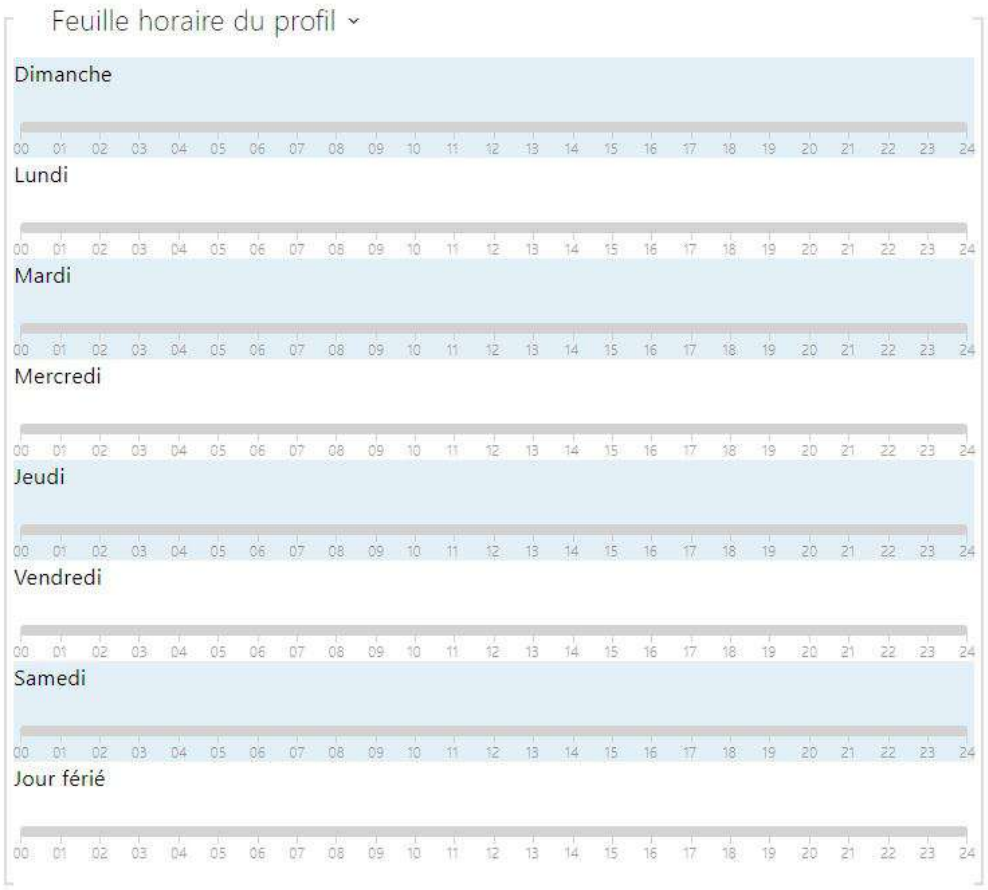
Chaque profil horaire définit la disponibilité de la fonction via un calendrier hebdomadaire. Il suffit de définir De–À et de spécifier les jours de la semaine pour la disponibilité. Les unités de contrôle d'accès 2N vous permettent de définir jusqu'à 20 profils horaires pouvant être affectés aux fonctions 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. Entrez les codes d'activation / désactivation à l'aide du clavier numérique de votre unité de contrôle d'accès 2N afin d'activer/désactiver une fonction après votre arrivée au bureau ou avant de quitter votre bureau, par exemple.

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

Liste des paramètres

- **Nom du profil** –saisissez un nom pour le profil horaire afin de pouvoir l'identifier facilement lors de sa sélection dans les interrupteurs, le contrôle d'accès, les numéros de téléphone, etc.



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.

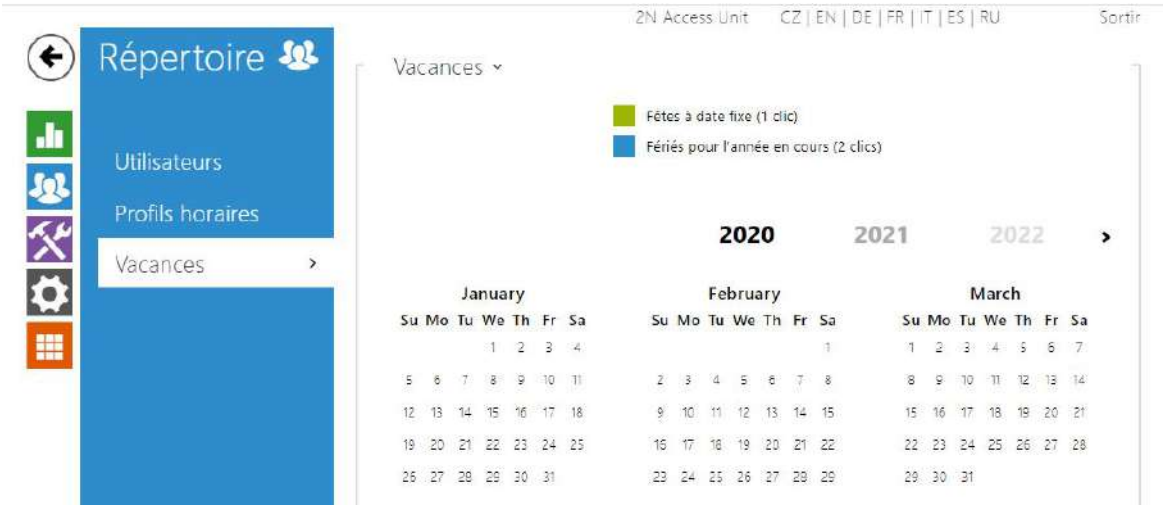
Assurez-vous que les paramètres en temps réel sont corrects (reportez-vous à la sous-section Date et heure) pour que cette fonctionnalité fonctionne correctement.

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



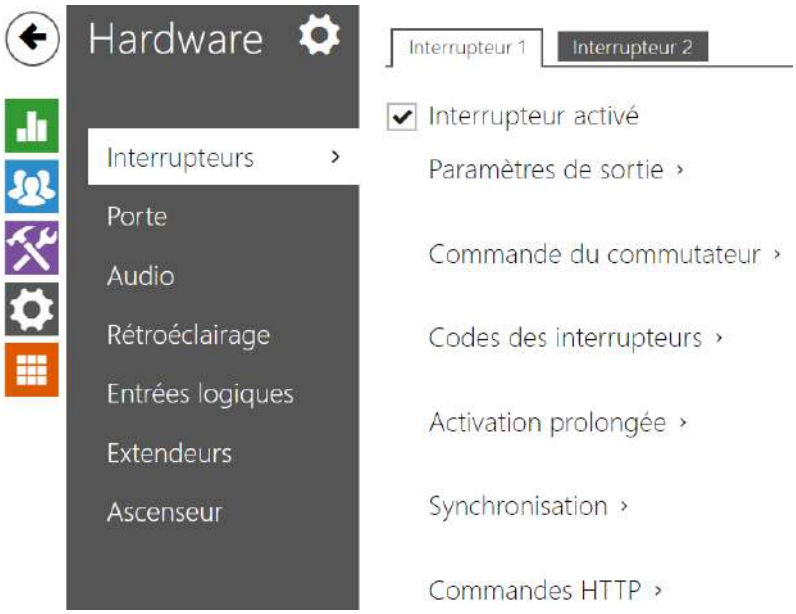
Ici, vous pouvez sélectionner les jours fériés (y compris le dimanche). Vous pouvez leur attribuer des intervalles de temps différents de ceux des jours ouvrables dans les profils horaires.

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 Hardware

Voici les onglets que vous pouvez trouver dans cette section :

5.3.1 Interrupteurs



Les Interrupteurs permettent un contrôle très souple et efficace des périphériques liés aux unités de contrôle d'accès tels que les serrures électriques, l'éclairage, des dispositifs de signalisation, de sonnerie...etc. Les unités de contrôle d'accès 2N vous permettent de configurer 2 interrupteurs indépendants.

Un interrupteur peut être activé par :

- la saisie d'un code valide sur le clavier numérique des unités de contrôle d'accès 2N,
- le passage d'une carte valide sur le lecteur RFID de l'interphone,
- un délai prédéfini après l'activation d'un premier interrupteur,
- 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 :

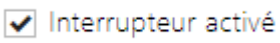
- activer n'importe quelle sortie des unités de contrôle d’accès 2N (Relais, Sortie active)
- activer la sortie qui contrôle le **Relais de sécurité 2N**
- envoyer une commande HTTP vers un autre appareil

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.

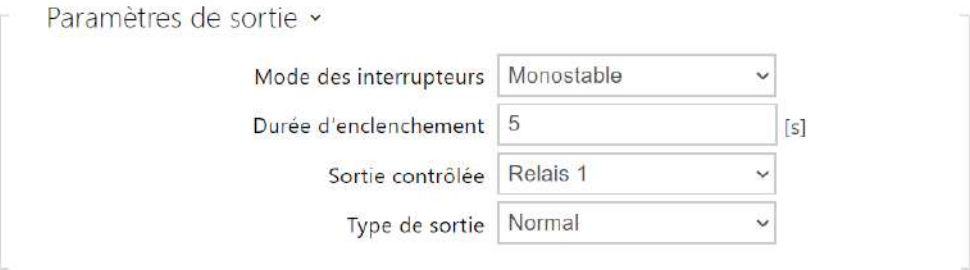
L'interrupteur signal son état par :

- un bip programmable.
- un indicateur LED si disponible sur le modèle des unités de contrôle d’accès 2N.

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.



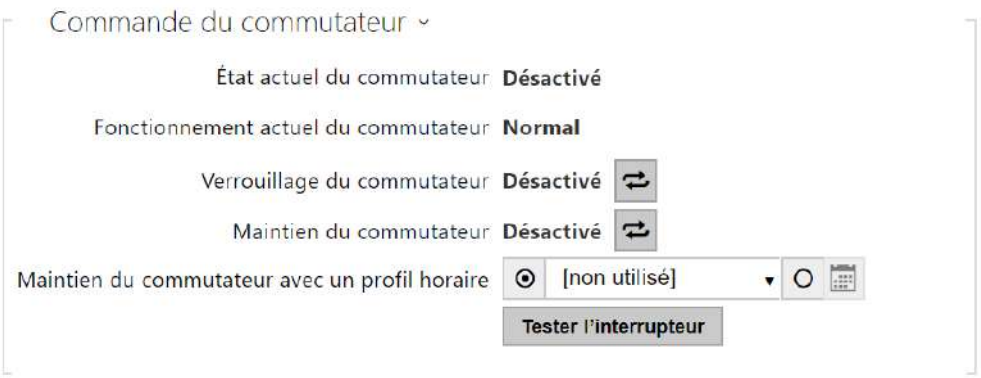
- **Modes des interrupteurs** – paramétrez le mode monostable/bistable pour l'interrupteur. En mode monostable, l'interrupteur est automatiquement désactivé après le temps de commutation réglé. En mode bistable, l'interrupteur est activé par la première activation et désactivé par la deuxième.
- **Durée 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 physique au commutateur. Choisissez l'une des sorties disponibles du dispositif : relais, sortie active, sortie d'extension. Si vous sélectionnez Aucun, le commutateur ne contrôlera aucune sortie physique mais pourra contrôler des équipements externes via des commandes HTTP.
- **Type de sortie** – si vous utilisez un relais de sécurité, réglez le type de sortie sur **Sécurité**. En mode Sécurité, la sortie fonctionne en mode inverse, c'est-à-dire qu'elle reste fermée et contrôle le module de relais de sécurité à l'aide d'une séquence d'impulsions spécifique. 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

- *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**.*

Avertissement

- La sortie 12V est utilisée pour connecter la serrure. Toutefois, si l'unité (2N IP Interphones, es unités de contrôle d'accès 2N) 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.



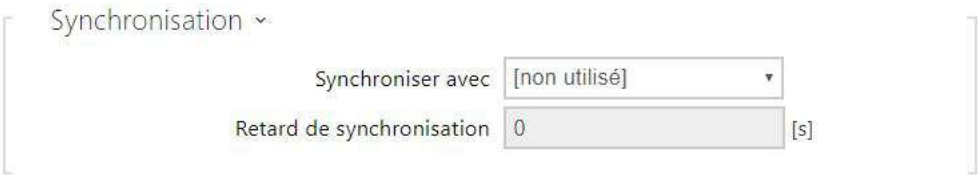
- **État actuel du commutateur** – affiche l'état actuel du commutateur (activé ou désactivé).
- **Fonctionnement actuel du commutateur** – Affiche le fonctionnement actuel du commutateur.
  - **Normal** : le commutateur n'est pas verrouillé ni maintenu.
  - **Maintenu** : le commutateur est maintenu mais pas verrouillé.
  - **Verrouillé** : le commutateur est verrouillé (dans ce cas, le verrouillage prime sur le maintien).
- **Verrouillage du commutateur** – basculer entre les états déverrouillé et verrouillé. Lorsque le commutateur est verrouillé (ON), son état logique est 0 et ne peut pas être contrôlé tant qu'il n'est pas déverrouillé.
- **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 ou en entrant un code.
- **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

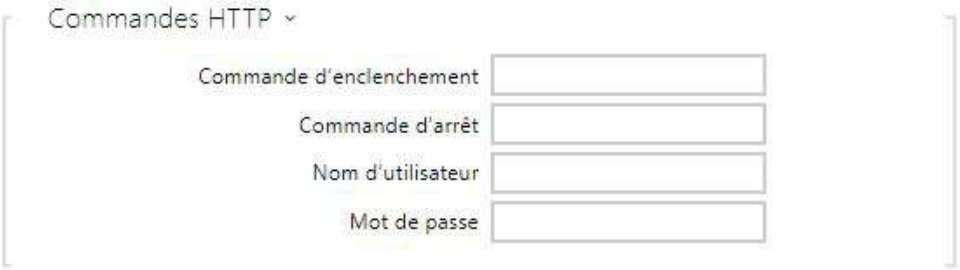
- Si l'interrupteur est verrouillé et que l'équipement est éteint puis rallumé, l'interrupteur restera verrouillé après la mise sous tension de l'équipement. L'interrupteur se comporte de la même manière s'il est désactivé puis activé.
- Si l'interrupteur est enclenché et que l'équipement est éteint 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 des'unités de contrôle d'accès 2N. Vous pouvez définir jusqu'à 10 codes universels pour chaque interrupteurs (en fonction du modèle unité utilisée).

- **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.
- **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 si les codes sur les lignes impaires (1, 3, ...) seront utilisés pour l'activation de l'interrupteur, et les codes sur les lignes paires (2, 4, ...) pour la désactivation en mode bistable.



- **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** – définissez l'URL pour la requête GET HTTP ou HTTPS envoyée lors de l'activation de l'interrupteur. La commande doit être sous ce format http://ip_adresse/chemin. Par exemple http://192.168.1.50/relay1=on.
- **Commande d'arrêt** – définissez l'URL pour la requête GET HTTP ou HTTPS envoyée lors de la désactivation de l'interrupteur. La commande doit être sous ce format http://ip_adresse/chemin. Par exemple http://192.168.1.50/relay1=on.
- **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

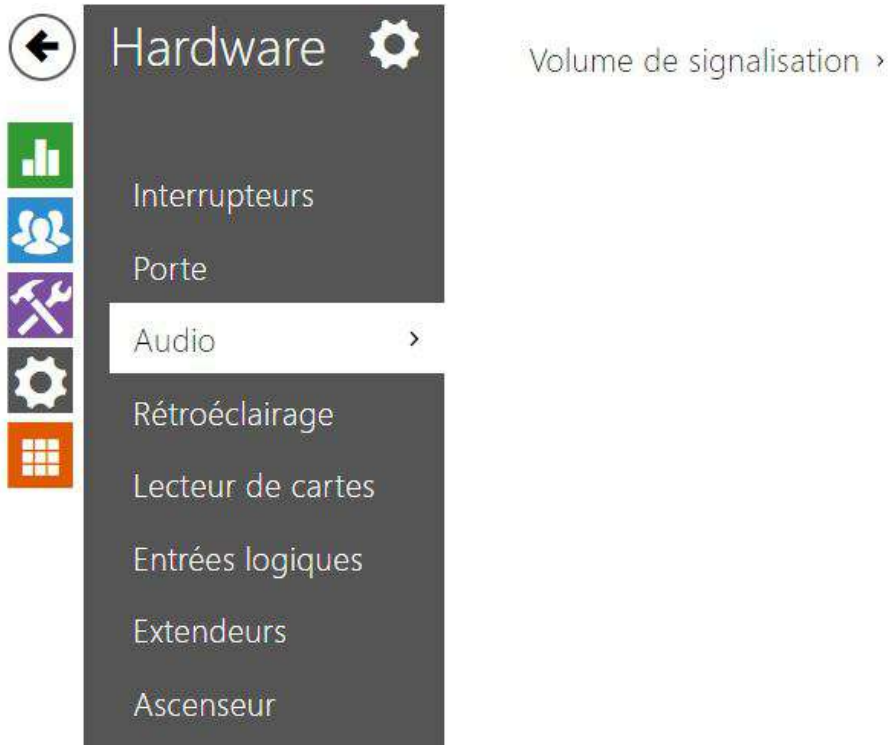
Avec le relais IP déporté 2N, **référence : 9137410E**, les commandes suivantes sont utilisées :

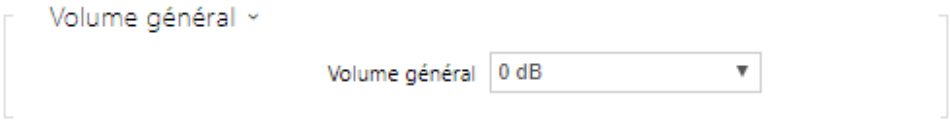
- **Activer l'interrupteur** – http://ip_address/state.xml?relayState=1 (e.g.: http://192.168.1.10/state.xml?relayState=1)
- **Pour activer l'interrupteur pendant une durée prédéfinie (la valeur par défaut est 1,5 s)** – http://ip_address/state.xml?relayState=2 (e.g.: http://192.168.1.10/state.xml?relayState=2)
- **Pour désactiver l'interrupteur** – http://ip_address/state.xml?relayState=0 (e.g.: 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?relayXState=1 (e.g.: http://192.168.1.10/state.xml?relay1State=1)
- **Pour activer l'interrupteur pendant une durée prédéfinie (la valeur par défaut est 1,5 s)** – http://ip_address/state.xml?relayXState=2 (e.g.: http://192.168.1.10/state.xml?relay1State=2)
- **Pour désactiver l'interrupteur** – http://ip_address/state.xml?relayXState=0 (e.g.: http://192.168.1.10/state.xml?relay1State=0)

Avancé

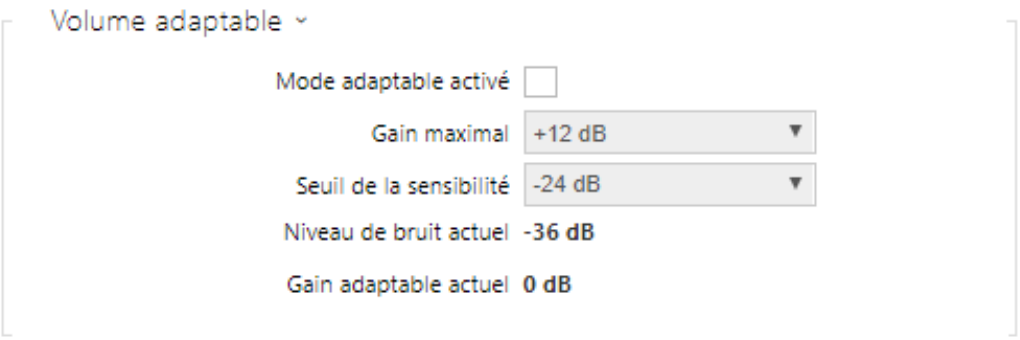
- **Alimentation maximale sortie 1** – définit la valeur maximale de la puissance de la sortie 1.

5.3.2 Audio





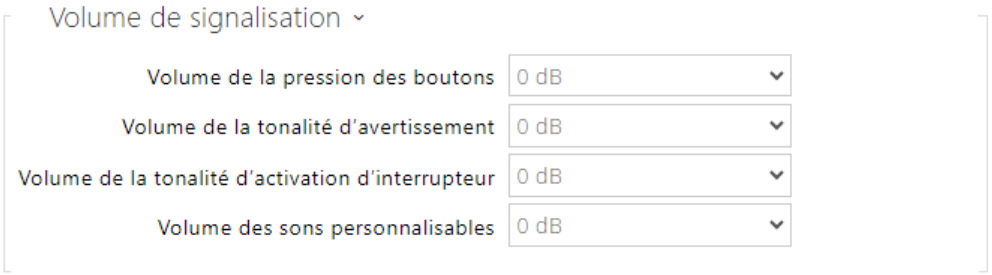
- **Volume général** – réglez le volume principal en fonction du volume d'appel souhaité, puis ajustez les volumes des autres sons au besoin. Ce paramètre affecte le volume de tous les sons.



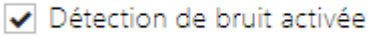
- **Volume adaptable** – activez le mode de volume adaptatif, qui augmente progressivement le volume de l'appareil en fonction de la différence entre le niveau de bruit actuel mesuré

et le seuil de sensibilité sélectionné, jusqu'à la valeur de gain maximale définie. Ce paramètre augmente également le volume principal.

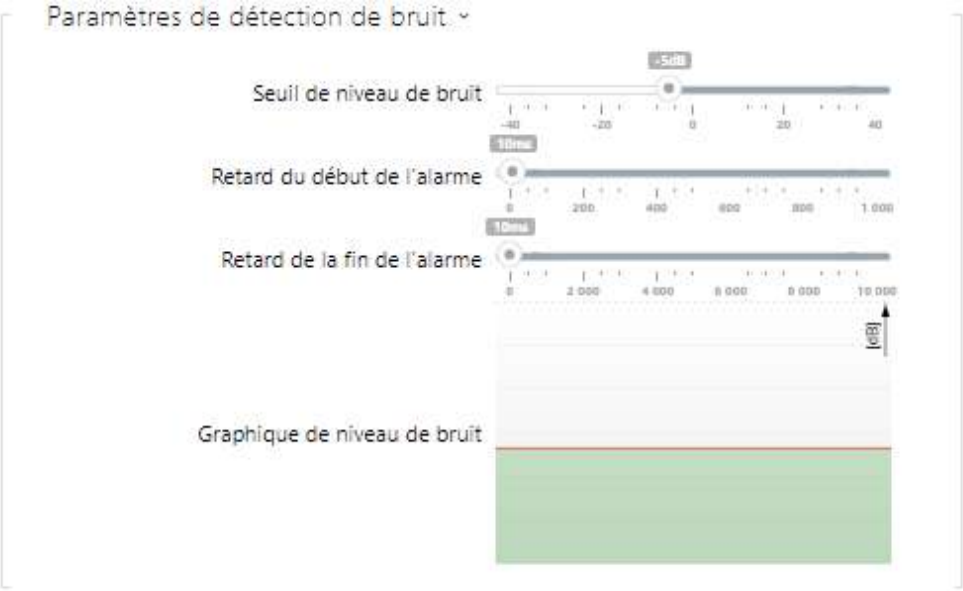
- **Gain maximal** – définissez le gain maximum qui peut être appliqué par-dessus le volume principal une fois que le niveau sonore actuel dépasse le seuil de sensibilité.
  réglez le gain maximum à appliquer au volume principal en mode adaptable.
- **Seuil sensibilité** – définissez le seuil de bruit ambiant qui détermine quand le volume commence à augmenter.
- **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 la pression des boutons** – réglez le volume de la pression des boutons. La valeur est relative au volume principal.
- **Volume de la tonalité d'avertissement** – réglez le volume des avertissements et des signaux décrits dans la section Signalisation des états opérationnels. La valeur est relative au volume principal.
- **Volume de la tonalité d'activation des interrupteurs** – réglez le volume du signal d'activation de l'interrupteur. La valeur est relative au volume principal.
- **Volume des sons personnalisables** – réglez le volume des sons d'utilisateur joués par l'automatisation. La valeur est relative au volume principal.

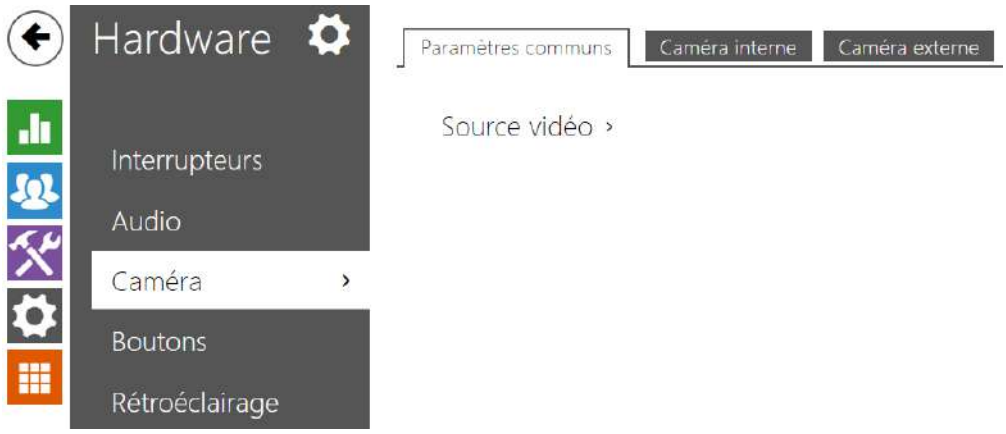


- **Détection de bruit activée** – activer la détection automatique du bruit ambiant au delà ou d'un certain seuil paramétrable. La détection d'un bruit anormalement élevé par rapport au seuil programmé apparait comme ceci dans l'Interface d'automatisation **"Event.NoiseDetected"** vous pouvez lui affecter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

5.3.3 Kamera



Ce menu est uniquement disponible dans les unités d'accès 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,
- 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).

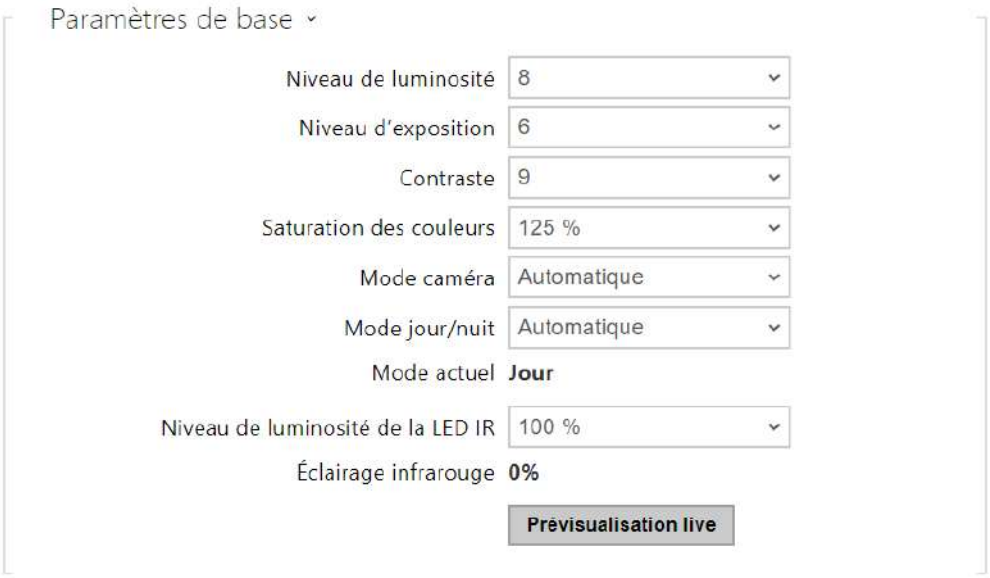
Le menu Caméra vous aide à définir des paramètres tels que la luminosité, la saturation des couleurs et les données de connexion à une caméra IP externe, le cas échéant. Référez-vous aux sections Services > Streaming et Services > E-Mail pour les paramètres d'appel vidéo / streaming.

Paramètres de base

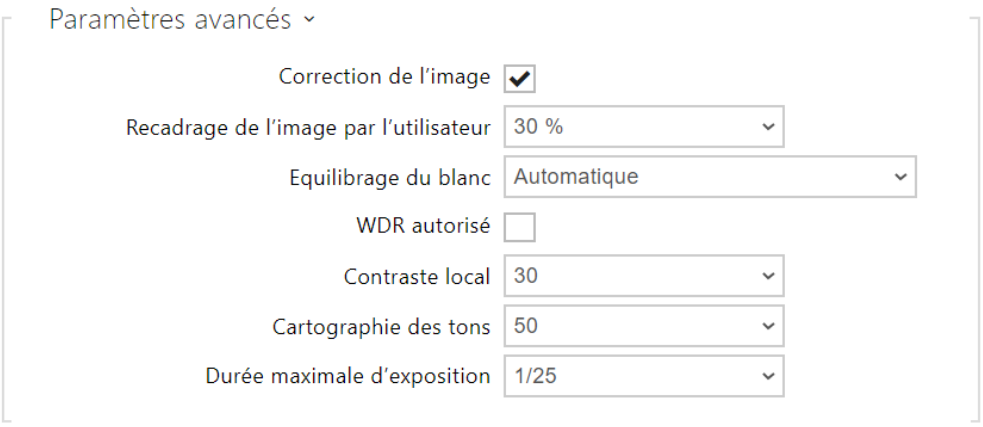
- **Source vidéo par défaut** – paramétrez la source de signal vidéo par défaut. Sélectionnez une caméra interne (ou une caméra analogique connectée à l'appareil) ou une caméra IP externe. Le changement de la source de signal vidéo par défaut est appliqué au flux RTSP

et à l'API HTTP. Dans l'application **2N IP Eye** il est nécessaire d'activer manuellement la caméra externe. 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 sélectionnée.

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

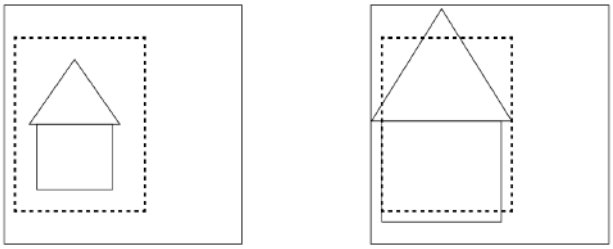


Le groupe de fonctions Paramètres avancés est valable pour les modèles d'interphones **2N IP Style** et **IP Verso 2.0**.

- **Correction de l'image** – active la correction de l'objectif fisheyed.
- **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

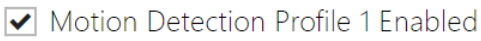
- Après avoir modifié le paramètre ***Découpage de la scène par l'utilisateur*** sur un appareil équipé d'un processeur ARTPEC-7, il convient de vérifier la délimitation de la zone de détection de mouvement et de la zone de confidentialité, qui changent dans l'espace, cf. l'illustration.



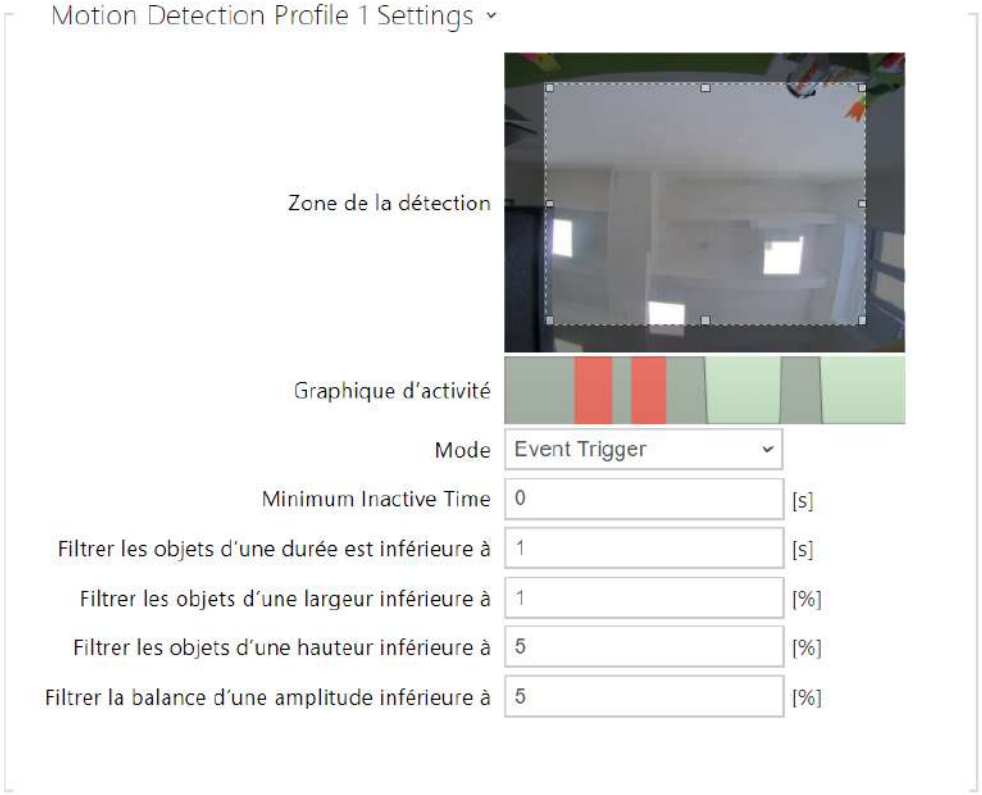
☑ Détection de mouvement activée

- **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 – 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 »).

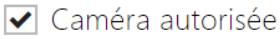
- **Protection de la vie privée autorisée** – active la fonction de confidentialité qui masque une partie de l'image avec la couleur ou la mosaïque sélectionnée.

- **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.

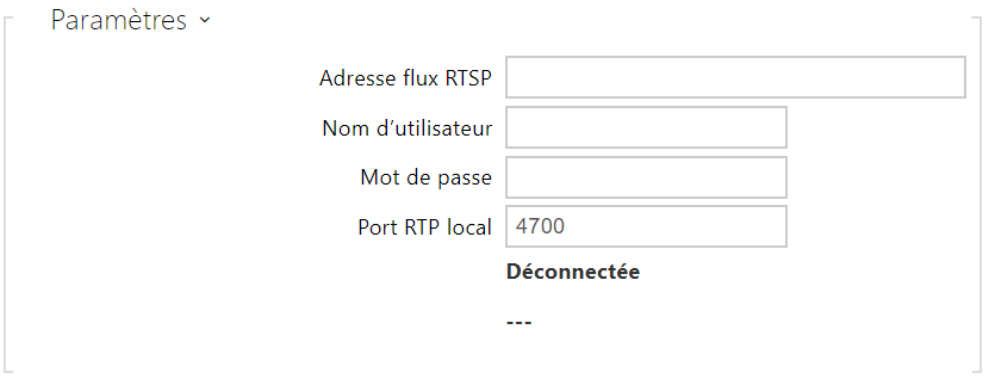
Observation

- 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.

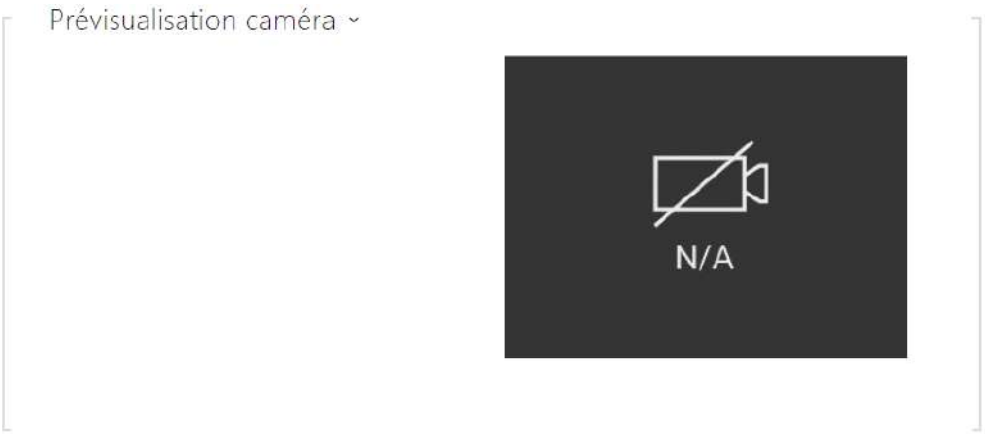
paramètre	description	exemple / valeurs
vcodec	Codec vidéo	vcodec=h264 pour le codec H.264 vcodec=mjpeg pour le codec MJPEG
vres	Résolution vidéo	vres=1920x1080 pour FullHD
fps	Fréquence d'image vidéo	fps=15 (1 à 30 fps, la valeur maximale possible pour le codec vidéo MJPEG est de 15 fps.)
vbr	Débit 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

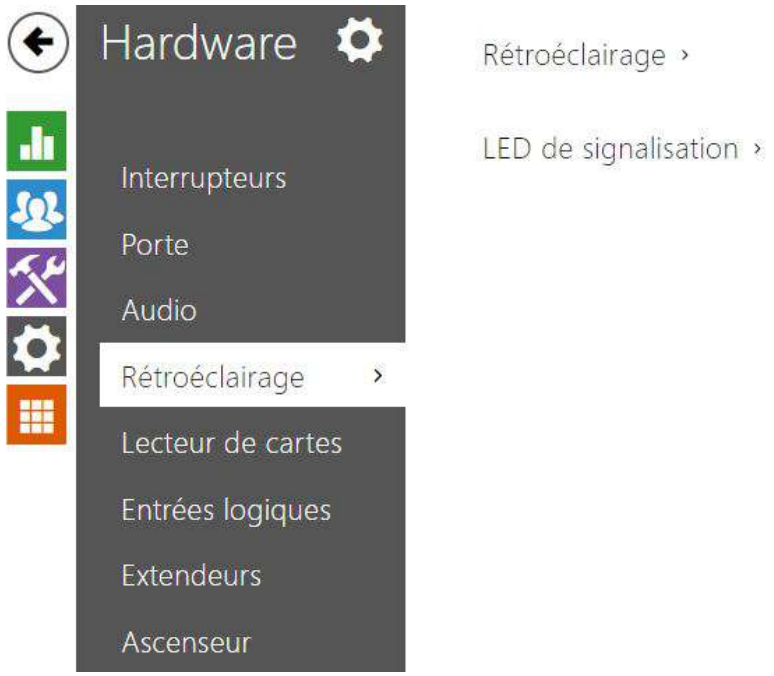
- FAQ: Caméra externe – Comment intégrer une caméra dans l'interphone IP 2N



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.

5.3.4 Rétroéclairage



Utilisez cet onglet pour paramétrer individuellement le rétro-éclairage des modules et les niveaux d'intensités des LED de signalisation.

- **Rétroéclairage** – Il définit la valeur de luminosité du rétroéclairage pendant le jour. La valeur est donnée en pourcentage de la luminosité maximale possible des LED.

- **LED de signalisation** – 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.

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’appareil et, en général, augmenter la consommation électrique de l’appareil. En revanche, une valeur d’intensité de LED faible peut entraîner, si l’appareil est exposé au soleil, un contraste plus faible de la LED et des problèmes d’identification de l’état de la LED.

5.3.4.1 Rétroéclairage (2N Access Unit QR)

Le niveau d'éclairage des LED de signalisation peut être réglé indépendamment sur cet onglet.

Si l'appareil est équipé d'un capteur de niveau de lumière ambiante, il sélectionnera automatiquement le niveau de rétroéclairage approprié dans la plage de valeurs définie. Voir les tableaux ci-dessous :

Fonctionnalité	2N Access Unit QR
Contrôle du niveau de rétroéclairage	**Oui**
Capteur de niveau de lumière ambiante	**Oui**

Les paramètres du groupe Rétro-éclairage sont valables pour le rétro-éclairage de l'unité principale et des modules additionnels.

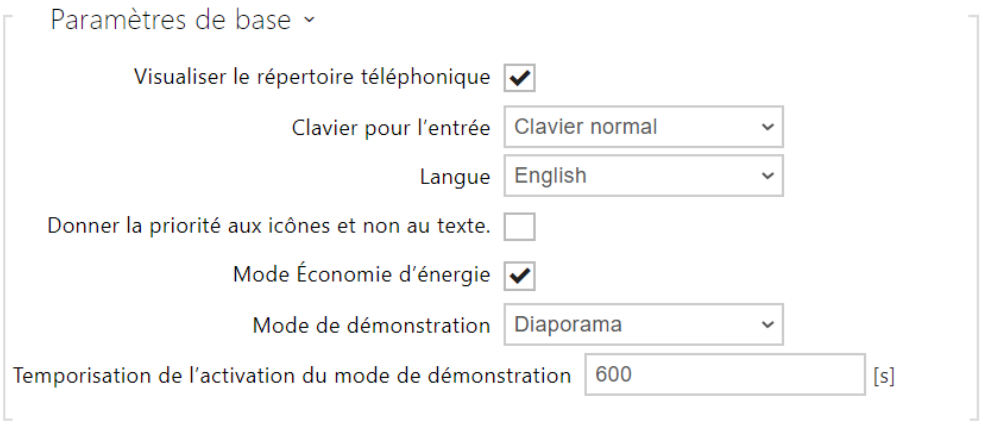
Les paramètres du bloc LED de signalisation sont valables pour les LED de signalisation des modules d'extension.

- **Intensité diurne** - définit la valeur de l'intensité du rétroéclairage pendant la journée. La valeur est exprimée en pourcentage de la luminosité maximale possible de la LED.
- **Intensité nocturne** - définit la valeur de la luminosité des DEL pendant la nuit. La valeur est exprimée en pourcentage de la luminosité maximale possible des DEL. Si l'intensité diurne et l'intensité nocturne sont réglées sur la même valeur, le niveau de lumière ambiante n'est pas pris en compte.
- **Valeur actuelle** - affiche la valeur d'intensité des DEL sélectionnée automatiquement en fonction du niveau de lumière ambiante détecté.

5.3.5 Ecran

Les systèmes d'accès 2N (modérément 2N Access Unit 2.0 et 2N Access Unit QR) peuvent être étendus avec un module d'affichage. L'écran LCD en couleur propose une fonction de clavier tactile et affiche l'état de l'équipement (par ex. l'ouverture de la porte, un refus d'accès, etc.) ou peut aussi fonctionner en mode présentation – une présentation peut s'afficher à l'écran sous la forme d'un diaporama d'images téléchargées après une période d'inactivité définie. Le temps avant l'affichage automatique peut être configuré.

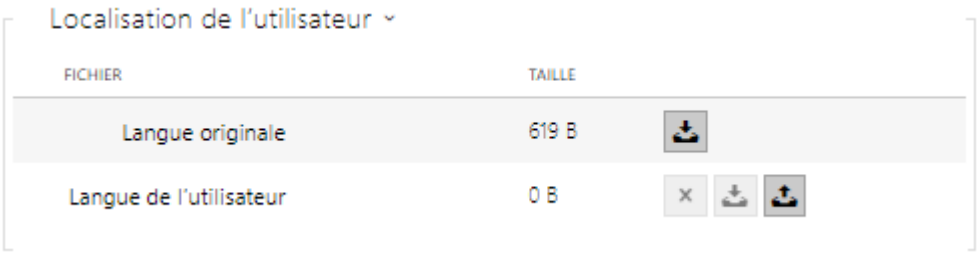
Ecran



- **Visualiser le répertoire téléphonique** – activez / désactivez l'affichage de la fonction répertoire.
- **Clavier pour l'entrée** – activez le clavier / type de clavier.
  - **Désactivé** – désactivez le clavier.
  - **Clavier normal** – activez le clavier en mode normal.
  - **Clavier mixte** – activez / désactiver le brouillage des boutons du clavier (transposition aléatoire des boutons) avant chaque nouvel affichage pour empêcher toute autre personne de regarder le code saisi (licence de sécurité renforcée requise).
- **Langue** – définissez la langue des textes affichés sur l'écran. Il est possible de sélectionner l'une des langues prédéfinies.
- **Donner la priorité aux icônes et non au texte** – les icônes à l'écran seront préférées au texte.
- **Mode 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´appareil 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.

- **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 (Présentation, Logo de la société, Adresse).
- **Temporisation de l'activation du mode de démonstration** – définit le temps d'inactivité après lequel l'équipement passe en mode de démonstration dans une envergure comprise entre 1 et 600 secondes.



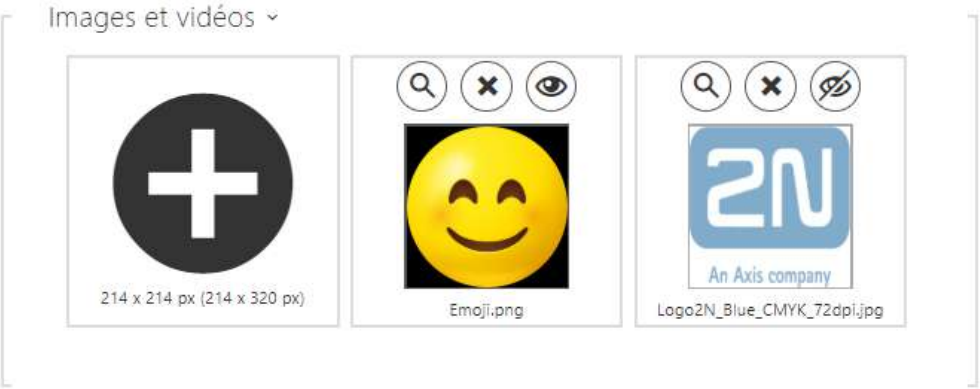
- **Langue originale** – téléchargez le modèle de fichier de localisation pour sa traduction. C'est un fichier XML avec tous les textes à afficher.
- **Langue de l'utilisateur** – enregistrez, supprimez et chargez un fichier de localisation de votre choix.

ⓘ 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´appareil.
- Définissez les **paramètres de langue** | **Langue à personnaliser**.
- Vérifiez et corrigez si nécessaire les textes sur l'écran de l´appareil.

Diaporama

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.



Assurez-vous que la résolution de l'image est de 214 x 214 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.

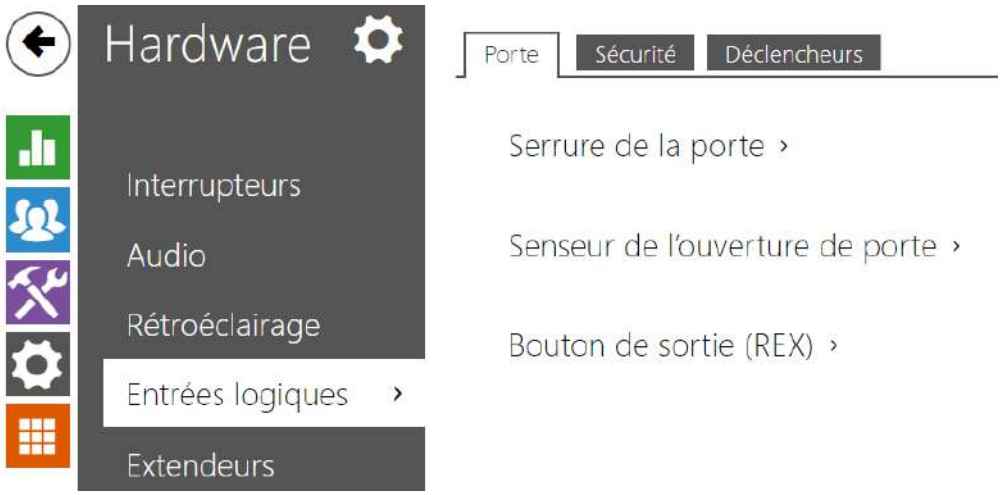
Si aucune image n'est chargée, le mode Diaporama ne sera jamais activé.

Tip

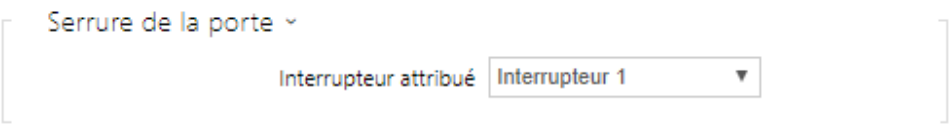
- Pour cacher le texte “Toucher pour démarrer” sur l'écran, chargez une image de résolution 214 x 320 pixels.

5.3.7 Entrées logiques

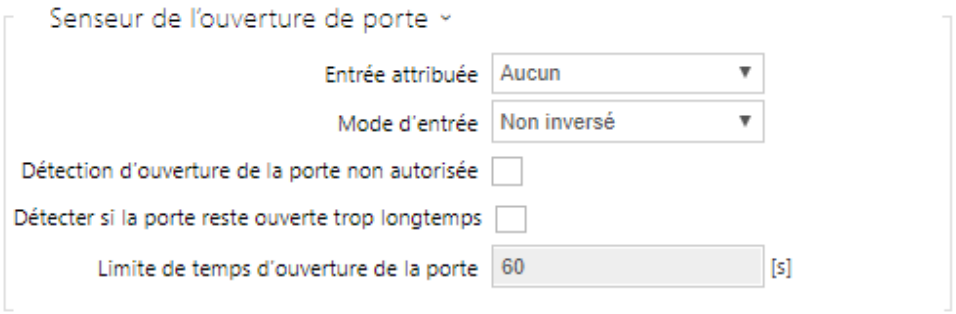
Dans cette section de configuration, définissez les paramètres associés aux entrées logiques et leurs interconnexions avec d'autres fonctionnalités de l'interphone.



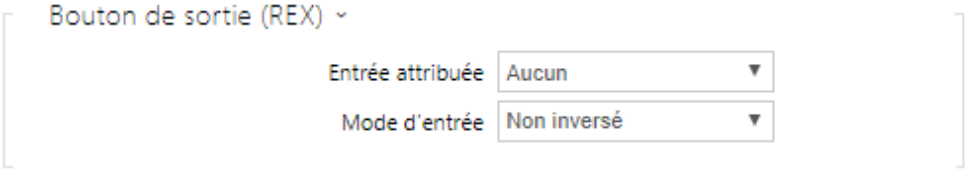
Porte



- **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).

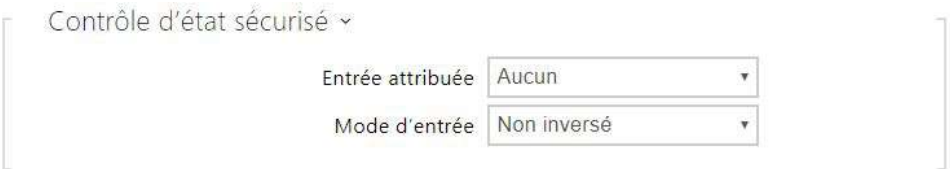


- **Entrée attribuée** – permet de sélectionner une des entrées logiques (éventuellement aucune entrée) pour la détection de portes ouvertes.
- **Mode d'entrée** – permet de régler le statut (la polarité) de l'entrée. Inversé ou Non inversé.
- **Détection d'ouverture de la porte non autorisée** – détecter 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'unité de contrôle d'accès 2N.
- **Mode d'entrée** – réglez le mode d'entrée actif (polarité).

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.

Note

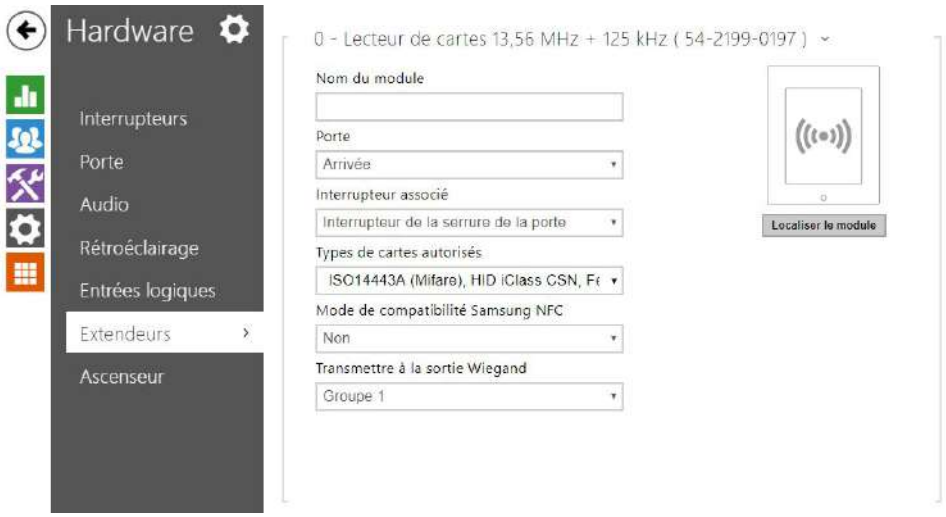
S'applique au modèle **2N Access Unit**:

- Depuis les PCB en version 599v2 et plus, tous les appareils sont équipés d'un commutateur d'auto protection optique.
- Depuis le PCB en version 599v2 et plus, l'entrée assignée est indiquée par le rétro éclairage d'un pictogramme d'un module. Dans les versions inférieures du PCB, c'est indiqué par la LED dans la partie droite du module.

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.

5.3.8 Extendeurs



2N Access Unit, 2N Access Unit 2.0 et **2N Access Unit QR** peuvent être étendues à l'aide de modules d'extension connectés via le bus VBUS. Les modules disponibles sont répertoriés dans le manuel d'installation de l'appareil. Tant qu'un module d'extension n'est pas connecté, cette section n'est pas affichée dans l'interface de configuration Web. Pour afficher la section, il est recommandé de redémarrer l'appareil après avoir connecté le module d'extension.

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 0).

Vous pouvez configurer chaque modules 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 peuvent être aussi configurés via le champ de texte, avec une série de paramètres (parameter_name=parameter_value) séparés par un point virgule. Pour l’instant seuls quelques paramètres sont disponibles. Les autres paramètres ne sont pas public car ils sont encore expérimentaux et peuvent être modifiés dans le futur.

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**.

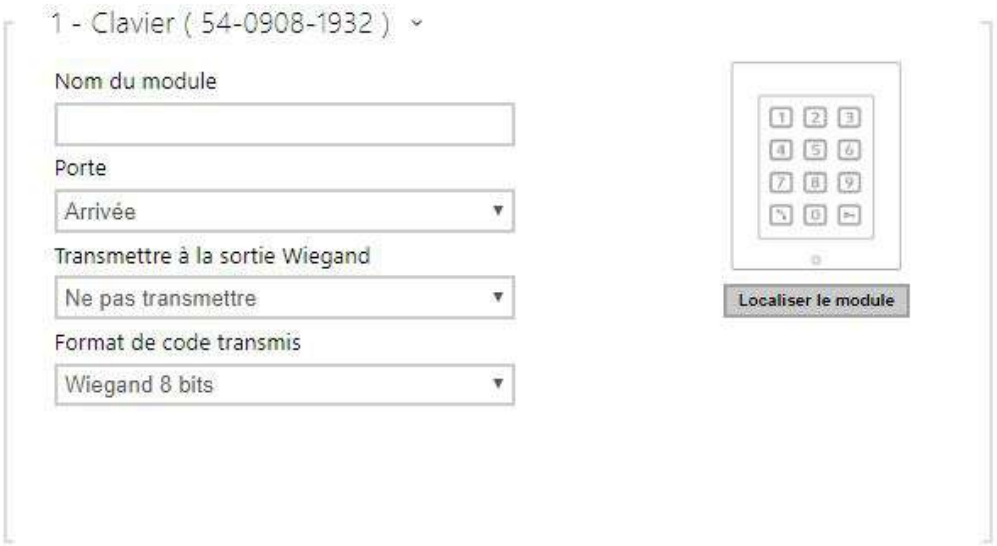
Observation

- 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 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

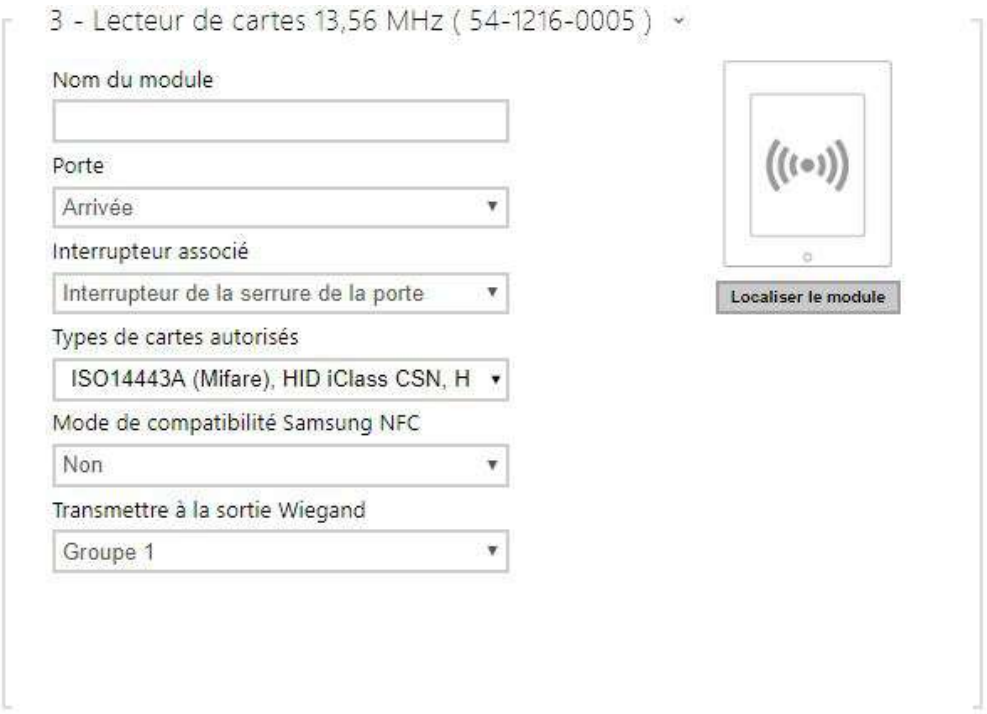
Configuration Module Lecteur de cartes 125 kHz

- **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

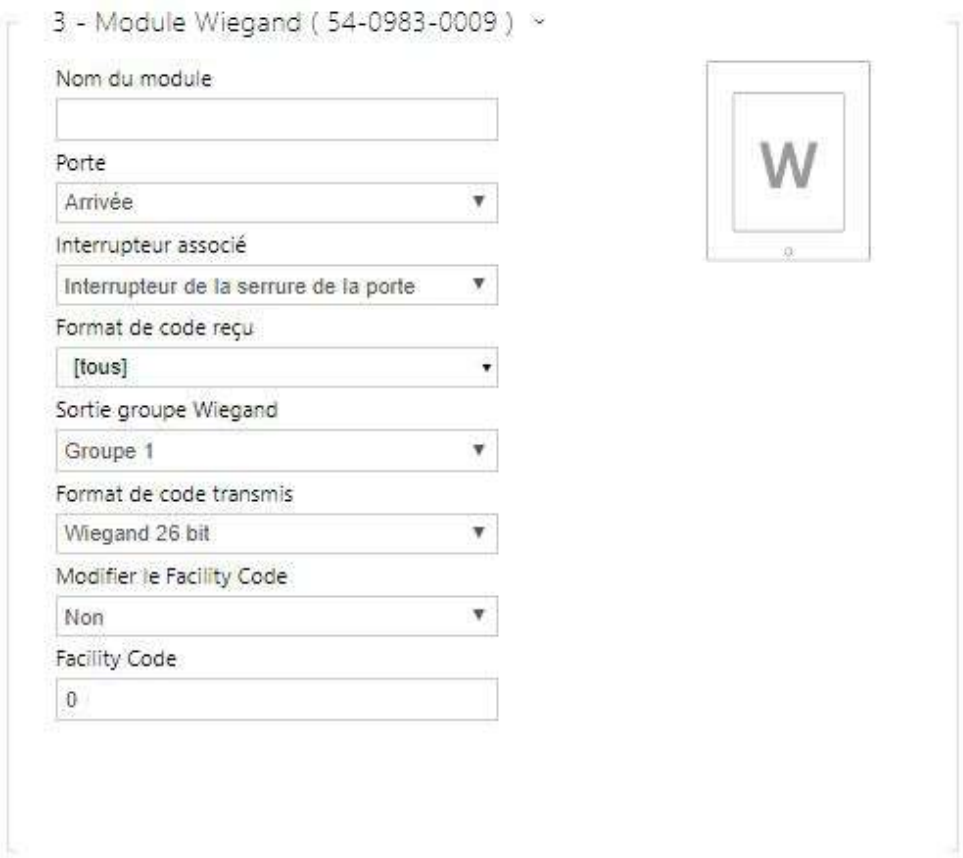
- **Nom du module** – définissez le nom du module pour le journal d'accès. Le nom du module est utilisé lors de l'enregistrement des événements du module Bluetooth.
- **Porte** – définissez la direction du lecteur (entrée ou sortie) pour le système de présence.
- **Interrupteur associé** – réglez l'interrupteur 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** – définissez la portée maximale du signal, c'est-à-dire la distance à laquelle le module Bluetooth peut communiquer avec le Smartphone :
  - **Petite** – moins de 2 m (fonctionne pour la plupart des Smartphones)
  - **Grande** – distance maximum possible (variable selon les modèles de Smartphone)
- **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.

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 ´appareil 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

- **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 portée plus grande, mais moins de puissance pour les autres fonctionnalités de l´appareil. 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.

Observation

- L'écran n'est pas supporté sur les unités de contrôle d'accès 1.0 à partir du firmware 2.27.

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.

Caution

- 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´appareil. 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 l'enregistrement des événements à partir du clavier.
- **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)

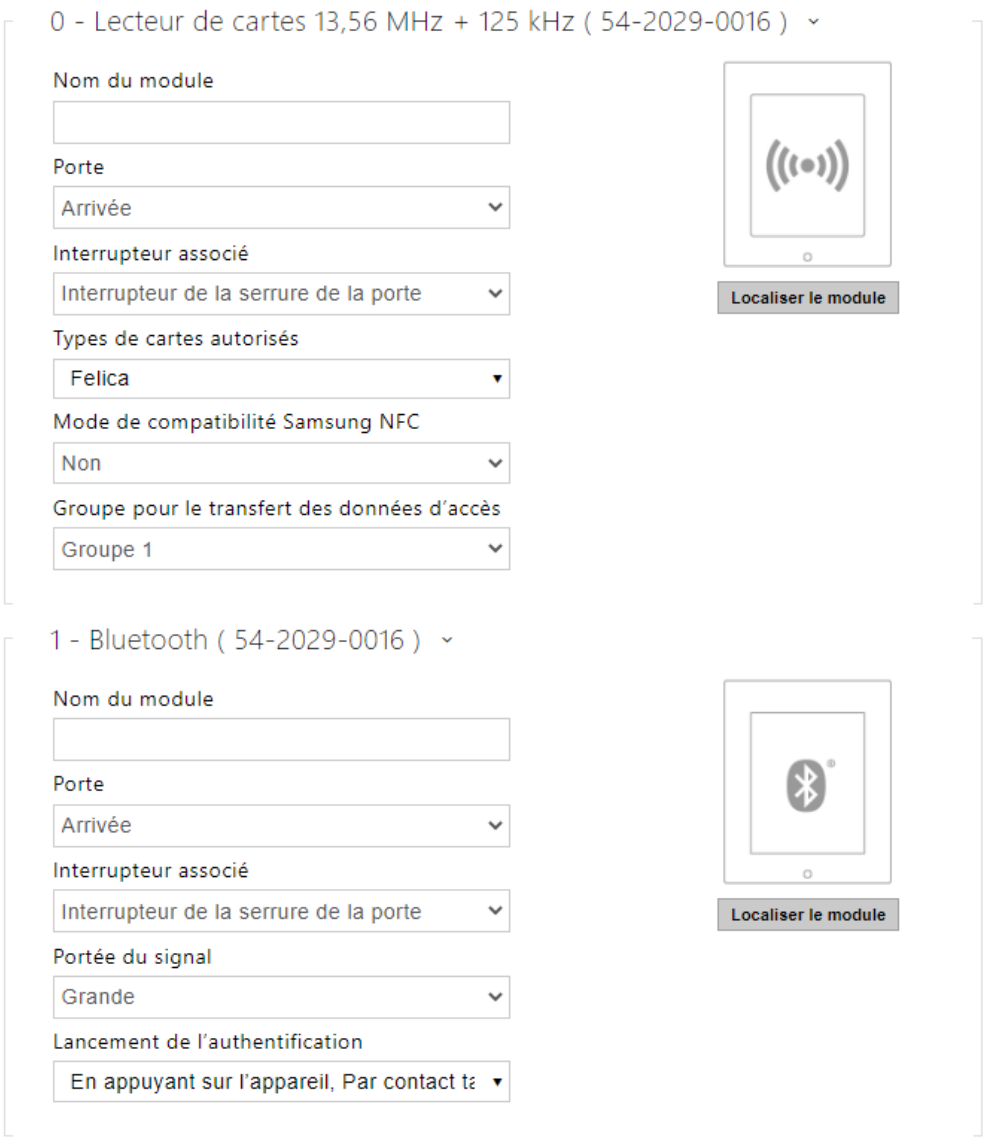
- **Nom du module** – définissez le nom du module pour le journal d'accès.
- **Porte** – définissez la direction du lecteur (entrée ou sortie) pour le système de présence.

- **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



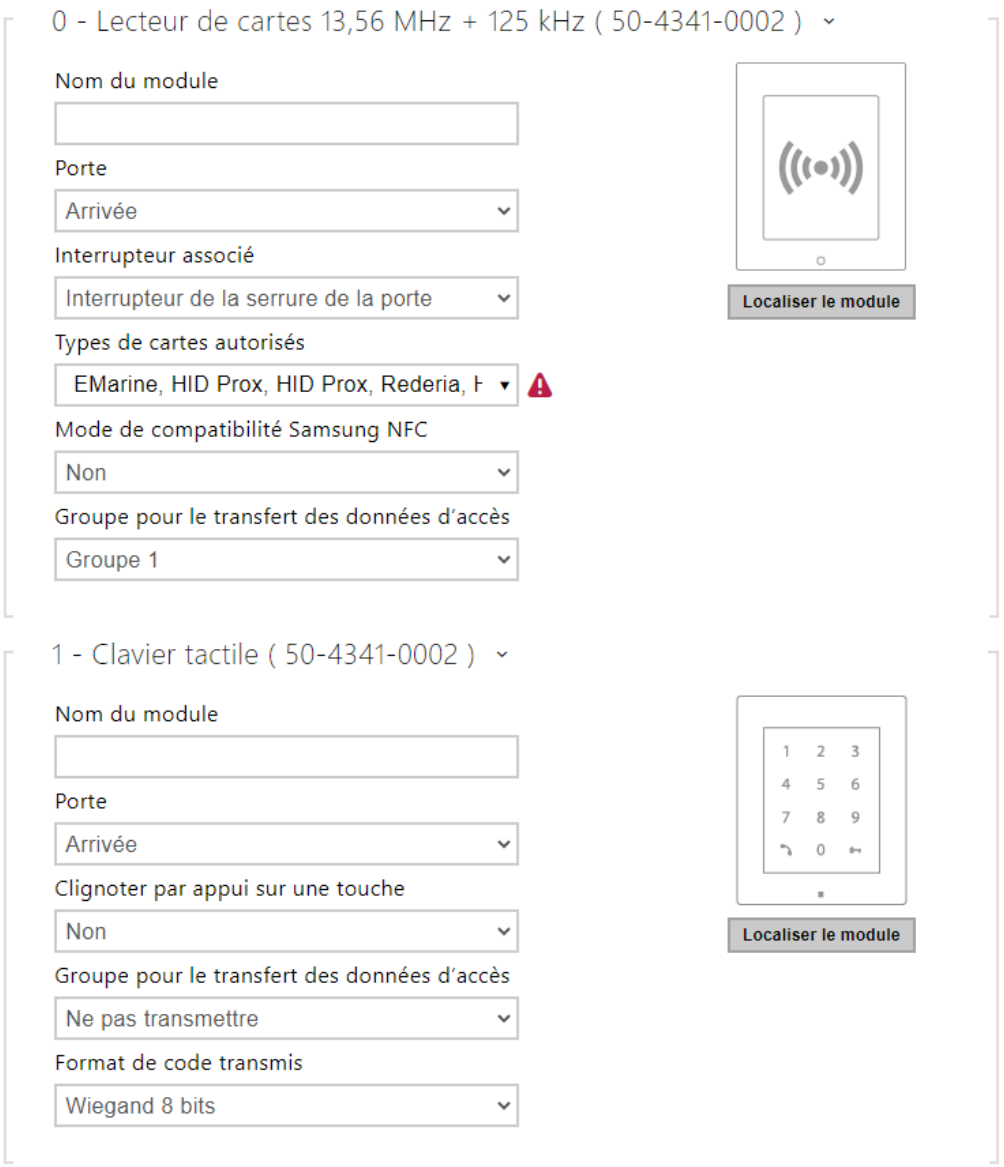
Lecteur de carte 13.56 MHz (125 kHz)

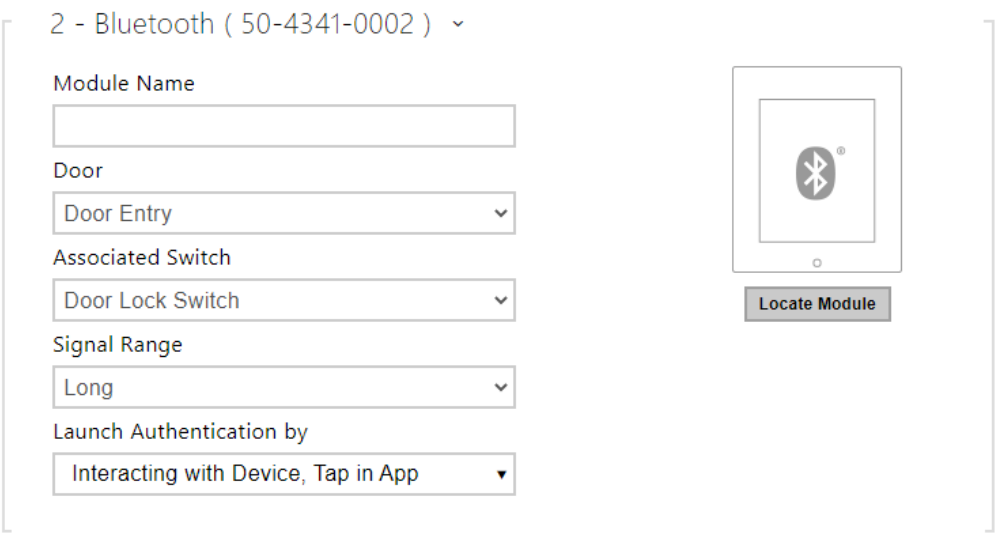
- **Nom du module** – définissez le nom du module pour le journal d'accès.
- **Porte** – définissez la direction du lecteur (entrée ou sortie) pour le système de présence.
- **Interrupteur associé** – réglez l'interrupteur pour qu'il soit activé après l'authentification de l'utilisateur via ce module. 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.
- **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** – définir la portée maximale du signal, c'est-à-dire la distance à laquelle le module Bluetooth peut communiquer avec le Smartphone :
  - **Petite** – moins de 2 m (fonctionne pour la plupart des Smartphones)
  - **Grande** – distance maximum possible (variable selon les modèles de Smartphone)
- **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.

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)

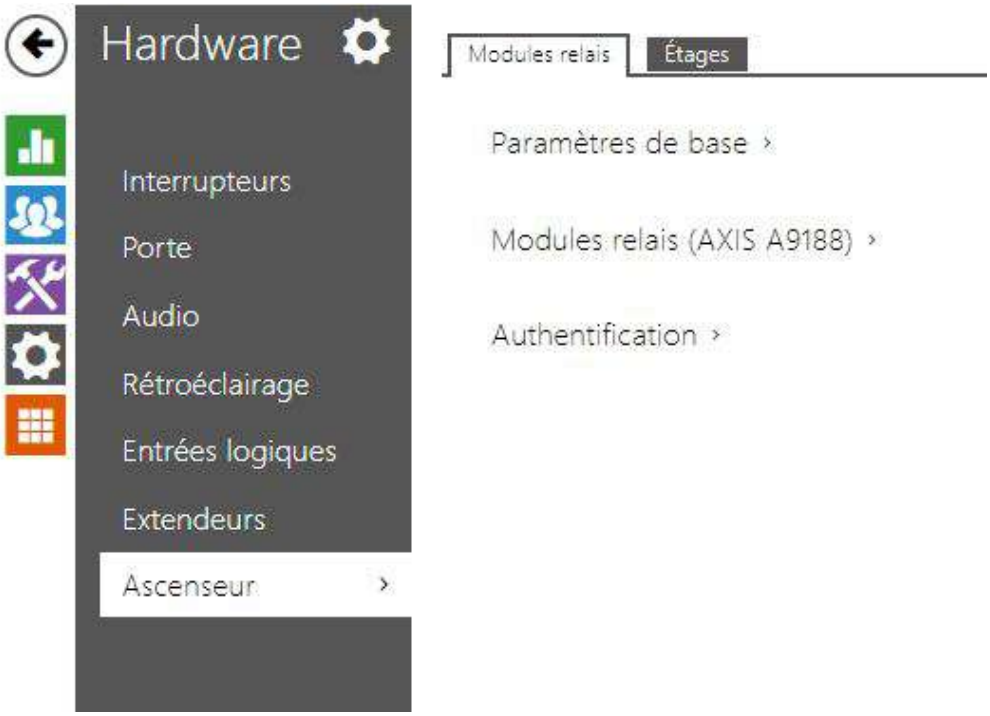
- **Nom du module** – définissez le nom du module pour le journal d'accès.
- **Porte** – définissez la direction du lecteur (entrée ou sortie) pour le système de présence.
- **Clignotement par pression sur les boutons** – activez la signalisation sur le clavier pour les environnements bruyants où les 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** – définir la portée maximale du signal, c'est-à-dire la distance à laquelle le module Bluetooth peut communiquer avec le Smartphone :
  - **Petite** – moins de 2 m (fonctionne pour la plupart des Smartphones)
  - **Grande** – distance maximum possible (variable selon les modèles de Smartphone)
- **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.

5.3.9 Ascenseur

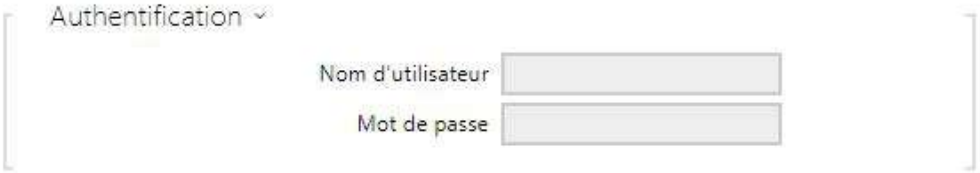


En connectant le module relais AXIS A9188 au dispositif, l'accès aux différents étages d'un bâtiment peut être contrôlé à l'aide de l'ascenseur. Un maximum de 5 de ces modules de relais peut être connecté à un appareil, chaque module contrôlant 8 étages, pour un total de 64 étages.

Modules relais

- **Durée d'enclenchement** – paramètres 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

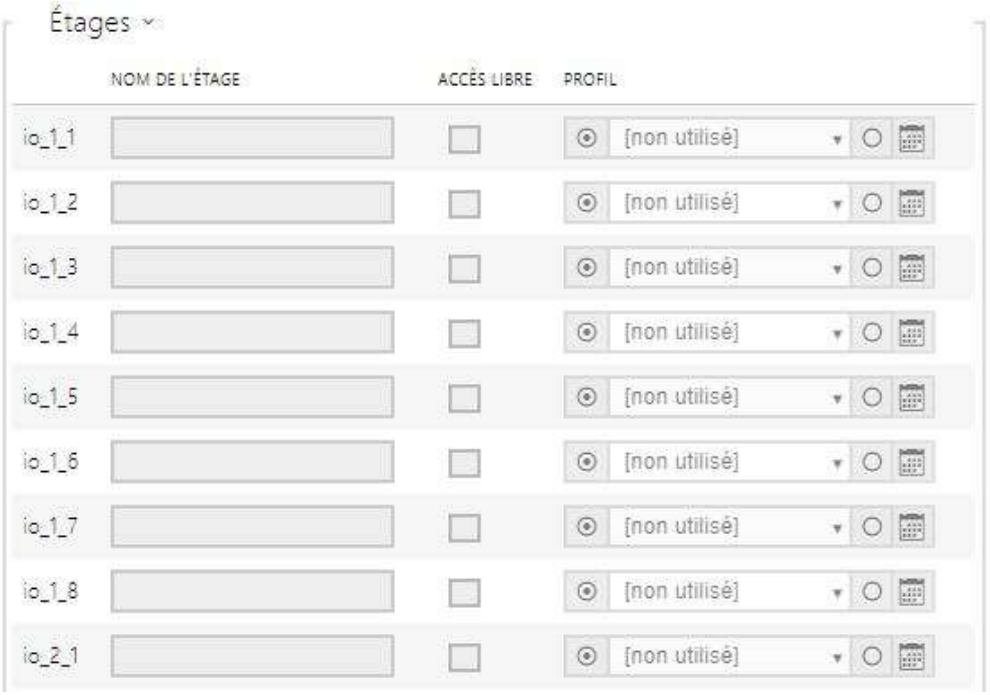


- **Nom d'utilisateur** – authentification du périphérique externe. Ce paramètre n'est obligatoire que si le périphérique externe requiert une authentification.
- **Mot de passe** – entrez le mot de passe d'authentification du périphérique externe (relais WEB, par exemple). Ce paramètre n'est obligatoire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

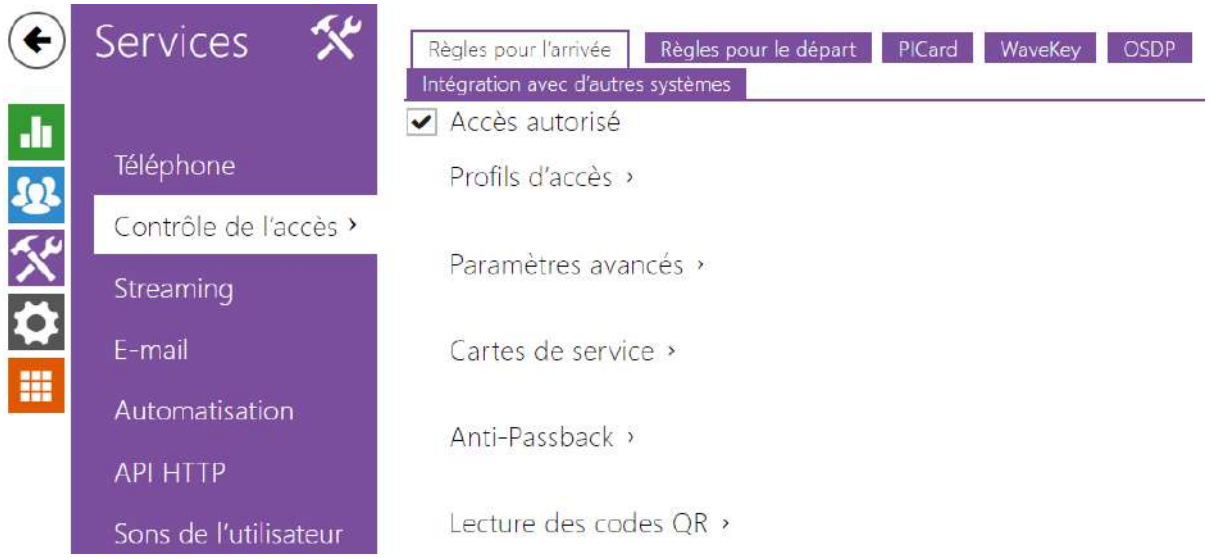
1. Retrouvez le module relais AXIS A9188 dans votre LAN en utilisant le scanner AXIS IP Utility.
2. Entrez l'identifiant.
3. Sélectionnez Préférences > Configuration additionnel du périphérique dans le menu.
4. Une nouvelle fenêtre de configuration de périphérique s’affiche.
5. Sélectionnez Options système > 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'appareil, 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.

5.4 Services

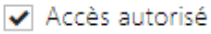
Voici les onglets que vous pouvez trouver dans cette section :

5.4.1 Contrôle de l’accès

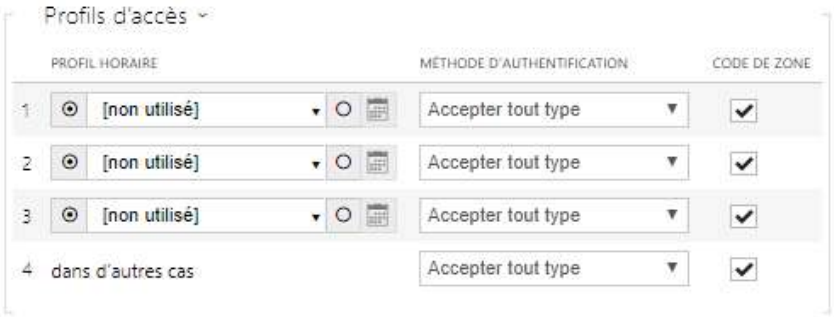
Le service Contrôle d’accès sert à gérer les accès et la façon dont l’authentification des utilisateurs est vérifiée.



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 des profils globaux dans Répertoire > Profils temporels.
  -  profil temporel individuel pour cet élément particulier.
- **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.), l´unité d'accès 2N 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.

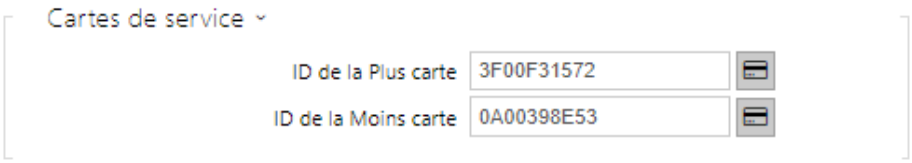
- **Nombre d'écarts de caractères** - permet de déterminer si un écart d'un ou deux caractères est toléré. L'écart des caractères se réfère au début et/ou à la fin en fonction du paramètre **Tolérer un écart de caractères**. L'appareil ne tolère aucun écart lors de la première lecture de la plaque d'immatriculation. 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

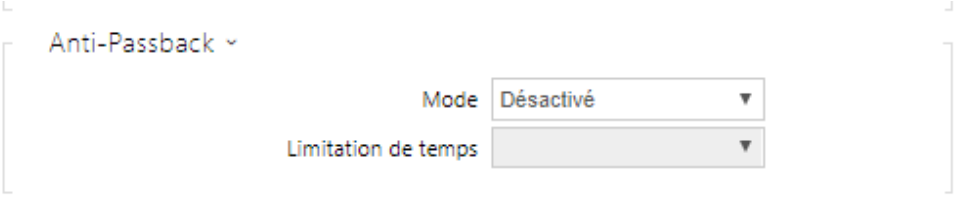
- La réinitialisation du logiciel d'usine ou le téléchargement d'une configuration différente ne modifiera pas les paramètres de blocage d'accès. Seule une réinitialisation matérielle des paramètres d'usine à l'aide du bouton Reset de l'appareil permet de rétablir les paramètres par défaut.
  - Le relais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

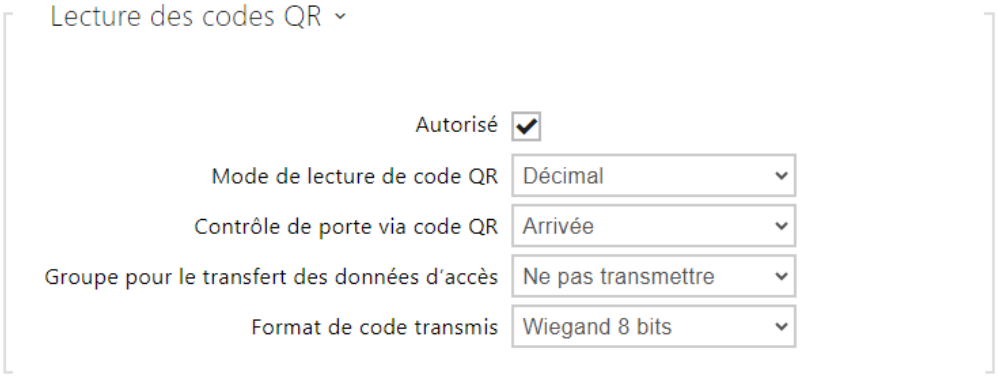
- **ID de la Plus carte** – ID de la carte de service destinée à ajouter dans la liste des cartes utilisateurs. L'ID de la carte est une séquence de 6–32 caractères de l'ensemble 0–9, A–F.

- **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 Services > Contrôle de l'accès 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 **UserRejected** sera créé dans la section Services > Contrôle de l'accès 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.



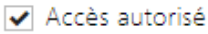
- **Autorisé** – active/désactive la lecture des codes QR à l'aide de la caméra du dispositif. Si la lecture des codes QR est activée, les codes PIN et les codes individuels des interrupteurs de plus de dix chiffres peuvent être saisis en pointant le code QR vers la caméra du dispositif.

- **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.

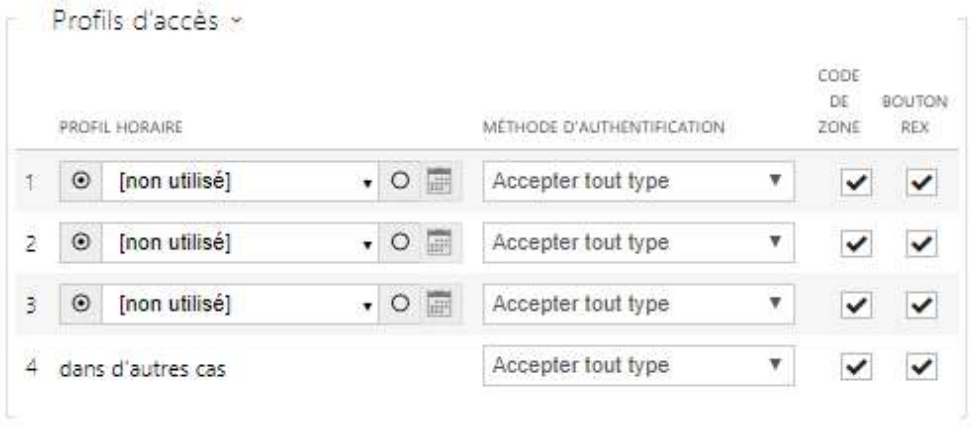
Observation

- 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.), l´unité 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.

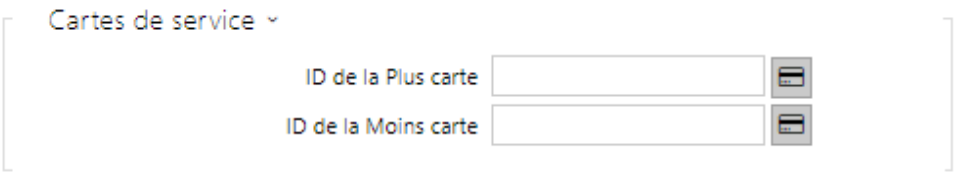
- **Tolérer un écart de caractères** – permet de déterminer si un écart est toléré dans la plaque d'immatriculation du véhicule. Il est possible de choisir entre une tolérance zéro, une tolérance depuis le début, une tolérance depuis la fin ou une tolérance tant depuis le début que depuis la fin. Lors 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**.

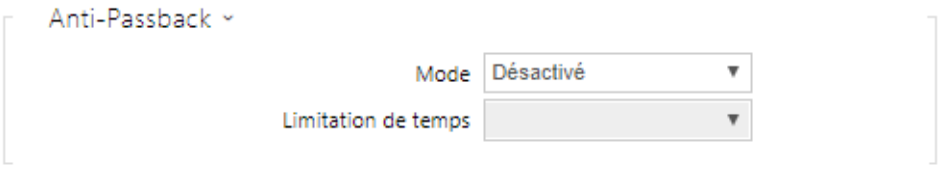
Avertissement

- 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 Services > Contrôle de l'accès 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 **UserRejected** sera créé dans la section Services > Contrôle de l'accès 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 2N appareils 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'appareil : 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'appareil. Vous pouvez déplacer l'ID d'authentification vers un autre utilisateur ou le copier dans un autre appareil. 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'appareil 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'appareil 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 appareils. Les 2N appareils 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'appareil 2N. 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

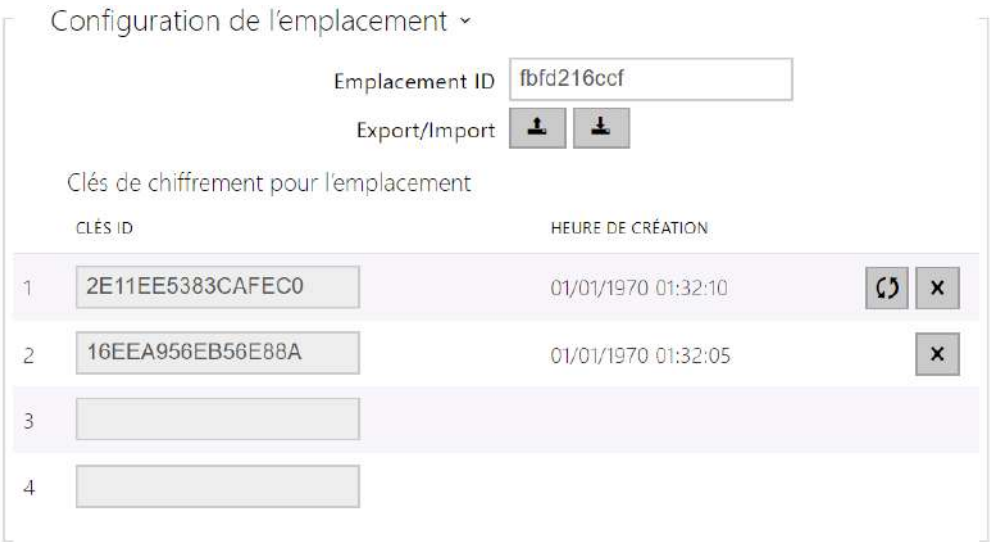
L'appareil 2N peut conserver jusqu'à 4 clés de chiffrement valides : 1 primaire et 3 secondaires. Un appareil mobile peut utiliser l'une des 4 clés pour le cryptage de la communication. Les clés de chiffrement sont entièrement contrôlées par l'administrateur du système. Il est recommandé que les clés 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'appareil 2N.

> **Note**
>
> - Les clés de chiffrement sont générées automatiquement au premier lancement de l'appareil et sauvegardées dans le fichier de configuration de l'appareil. 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.

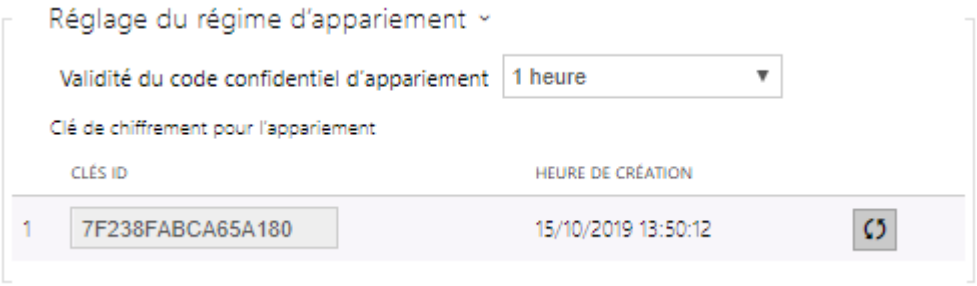
Lorsqu'une clé est supprimée, les utilisateurs de l'application **2N Mobile Key** qui utilisent toujours cette clé ne pourront pas s'authentifier à moins d'avoir mis à jour les clés de chiffrement de leurs appareils mobiles avant leur suppression. Les clés de l'appareil mobile sont mises à jour à chaque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

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.

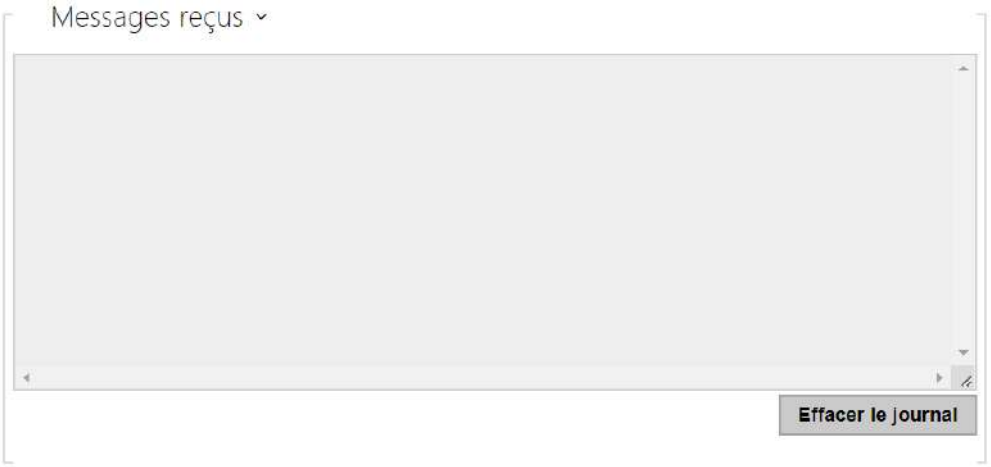
OSDP

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'appareil 2N. L'objectif est de permettre d'activer la signalisation sur l'appareil 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'appareil 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.

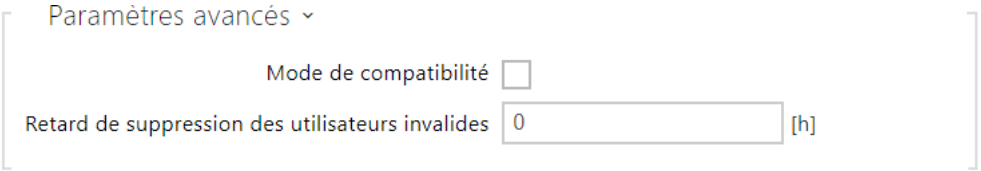
Observation

- 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'appareil 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.
- **Retard de suppression des utilisateurs invalides** - Définit le délai après lequel les utilisateurs dont l'accès est non valide et la suppression automatique activée sont supprimés de la liste des utilisateurs de l'appareil.

5.4.2 Streaming

2N Access Unit QR fournisse 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

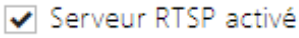
- **RTP (Real-Time Transport Protocol)** – c'est un protocole définissant le format des paquets standard pour la transmission audio / vidéo via les réseaux IP. Les appareils 2N utilisent ce protocole pour le streaming audio / vidéo. Le protocole de transport RTP est soit UDP, soit RTSP et HTTP.
- **RTSP (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 appareils 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 appareils 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 appareils 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 appareils 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.

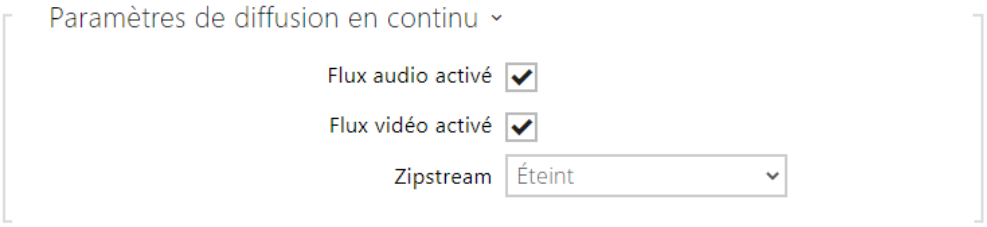
Liste des paramètres

ONVIF/RTSP

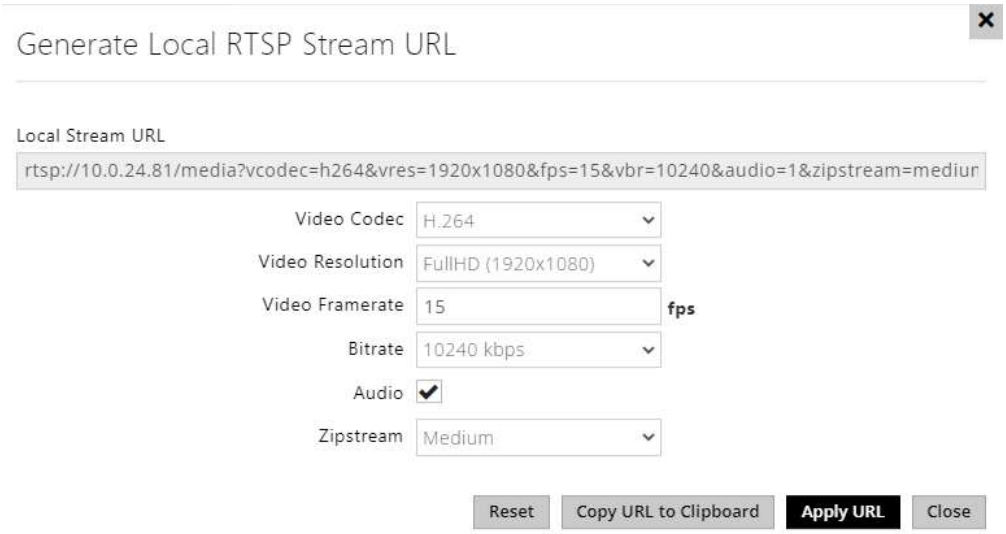
Les appareils 2N intègrent un serveur RTSP, qui peut être configuré dans cet onglet. Le serveur RTSP permet le streaming audio / vidéo. Vous pouvez choisir la méthode de transmission des données, la méthode / les paramètres de compression vidéo et d'autres paramètres associés à la sécurité et à la qualité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



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



- **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  .

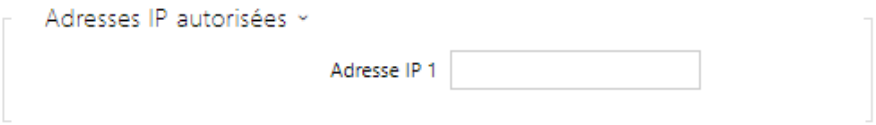


- **Codec vidéo** – sélection des codecs vidéo disponibles
- **Résolution vidéo** – sélection des résolutions vidéo possibles
- **Fréquence d'image vidéo** – paramètres de la fréquence d'images (1 à 30 fps, la valeur maximale possible pour le codec vidéo MJPEG est de 15 fps).
- **Bitrate** – sélection 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**.

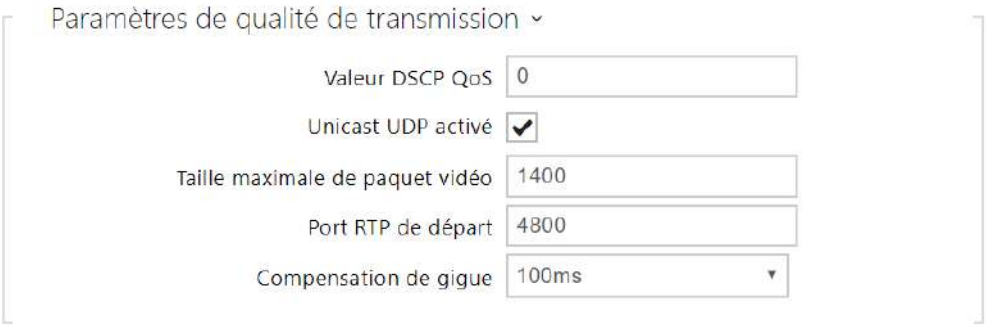
Le nombre de flux RTSP est limité à 4 flux parallèles. Ce nombre inclut les deux flux audio sans canal de retour vidéo et audio dirigé vers l´appareil.

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).



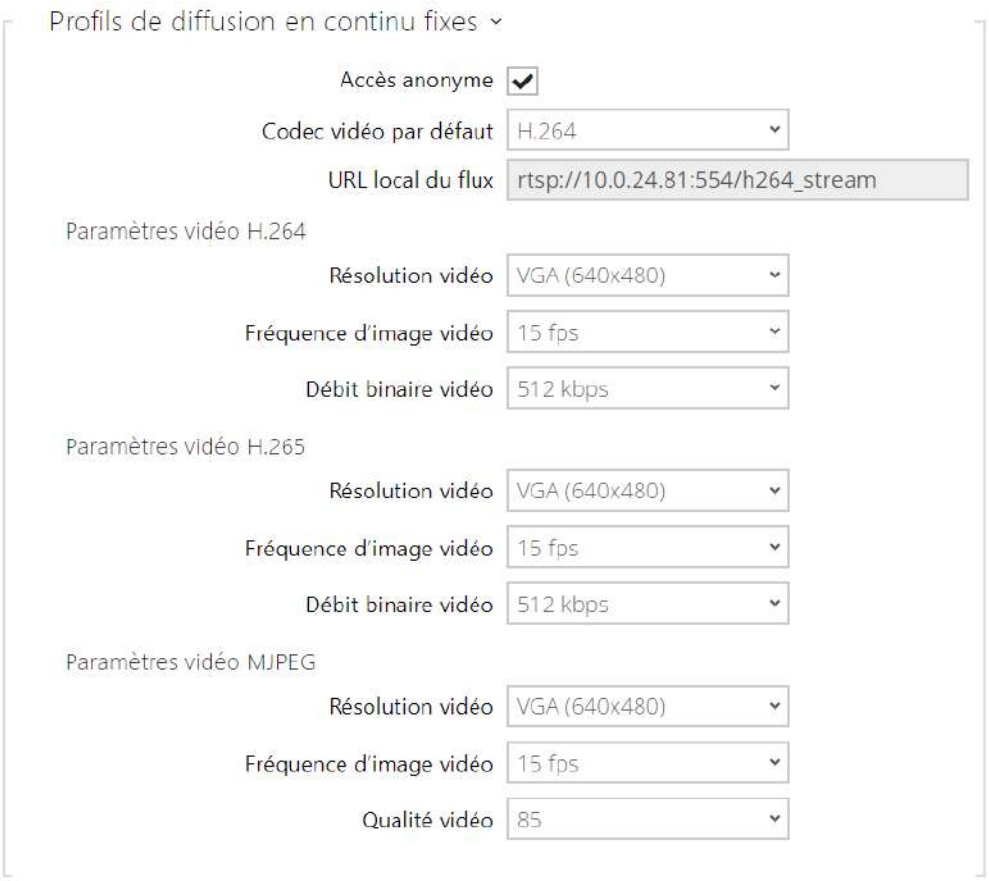
- **Adresse IP 1** – définir IP autorisées à partir desquelles vous pouvez vous connecter au serveur RTSP. Si le champ n'est rempli, une adresse IP quelconque peut être utilisée pour se connecter.



- **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´appareil :

- 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**

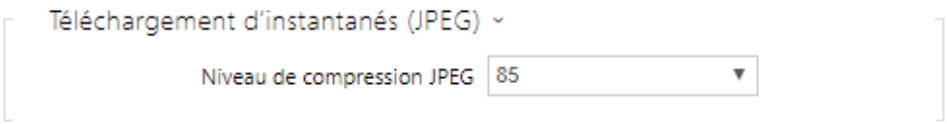
où W et H spécifient la résolution de l'image (résolutions supportées : 160 x 120, 320 x 240, 640 x 480, 176 x 144, 322 x 272, 352 x 288, 1280 x 960 – (seulement pour les modèles équipés d'une caméra 1 Mega Pixel). N correspond au nombre d'instantanés par seconde (1 à 10).

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 de l´appareil	Résolution	Nombre de flux
2N Access Unit QR	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.*

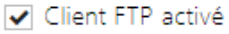


- **Niveau de compression JPEG** – réglez le niveau de compression JPEG (de 1 à 99). 85 est la valeur recommandée. Ce paramètre affecte la taille et la qualité de l'image.

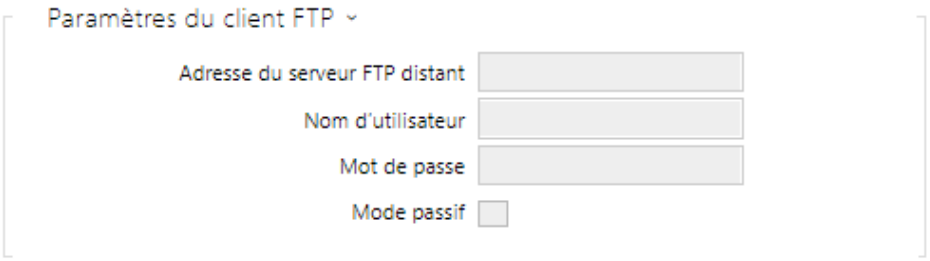
FTP

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.

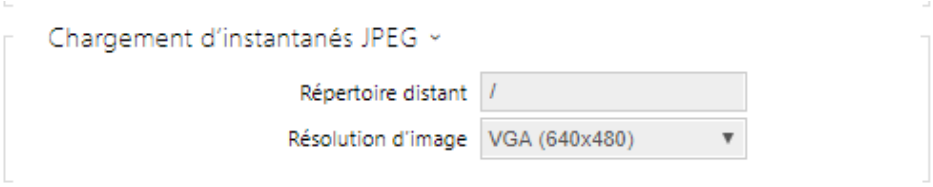
Les images sont stockées sur le serveur FTP soit automatiquement (périodiquement), soit via l'automatisation en utilisant l'Action **UploadSnapshotToFTP**.



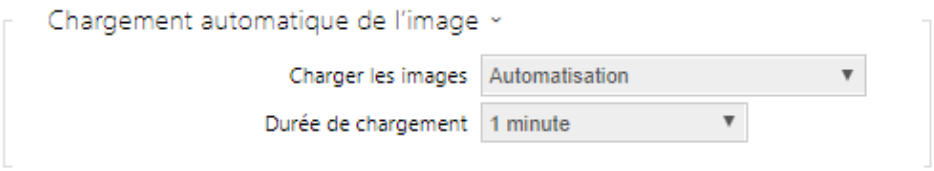
- **Client FTP activé** – activez l'enregistrement des images de la caméra sur le serveur FTP.



- **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).



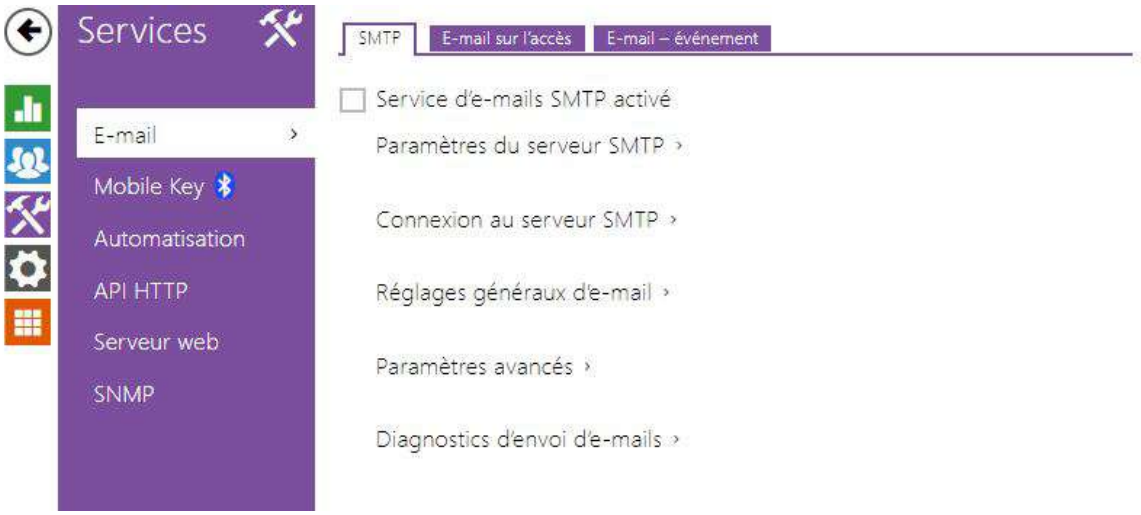
- **Répertoire distant** – définissez le répertoire du serveur FTP dans lequel les images de la caméra doivent être enregistrées.
- **Résolution d'image** – définissez la résolution des images.



- **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

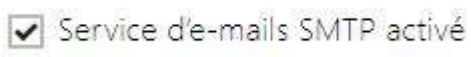


L'adresse électronique de l'utilisateur, utilisée pour l'envoi d'informations par courrier électronique, par exemple sur l'accès de l'utilisateur à l'objet ou sur l'utilisation de 2N Automation. Il est possible de personnaliser l'objet de l'e-mail et le texte du message. Si votre appareil est équipé d'une caméra, vous pouvez également joindre de manière automatique un ou plusieurs instantanés.
L´appareil 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.

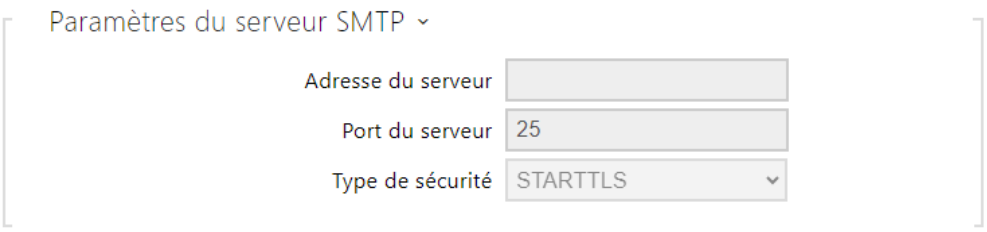
Vous pouvez également envoyer des emails depuis l'interface d'Automatisation en utilisant l'action **Action.SendEmail**.

> **Note**
>
> - *La fonction de courriel n'est disponible qu'avec la licence Gold.*

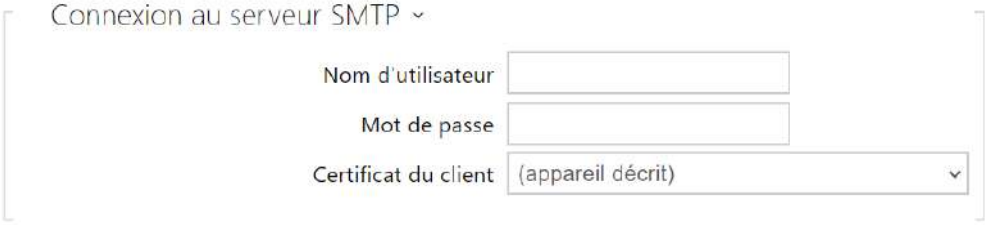
SMTP



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



- **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.
- **Type de sécurité** – sélectionne le type de sécurité pour la communication avec le serveur SMTP. Le type de sécurité requis par le serveur est généralement indiqué dans sa documentation.



- **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.

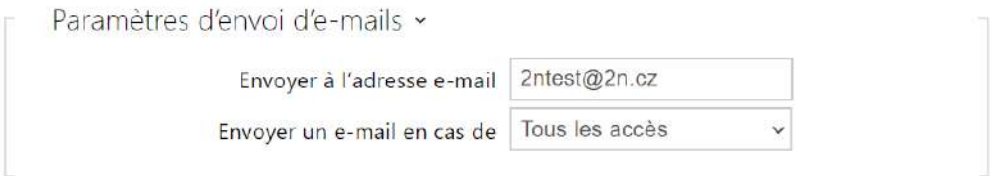
- **L'adresse de l'expéditeur** – définissez l'adresse de l'expéditeur pour tous les courriels sortants à partir de l'unité.

- **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 appareil ou sur un autre élément du réseau.

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** – définissez l'objet de l'e-mail envoyé.
- **Corps du message** – modifiez 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.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.

E-Mail - Evènement

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 – definissez l'envoi d'e-mail. Les options suivantes sont disponibles :

- **Redémarrer l'appareil**
- **Activation du commutateur de protection**

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

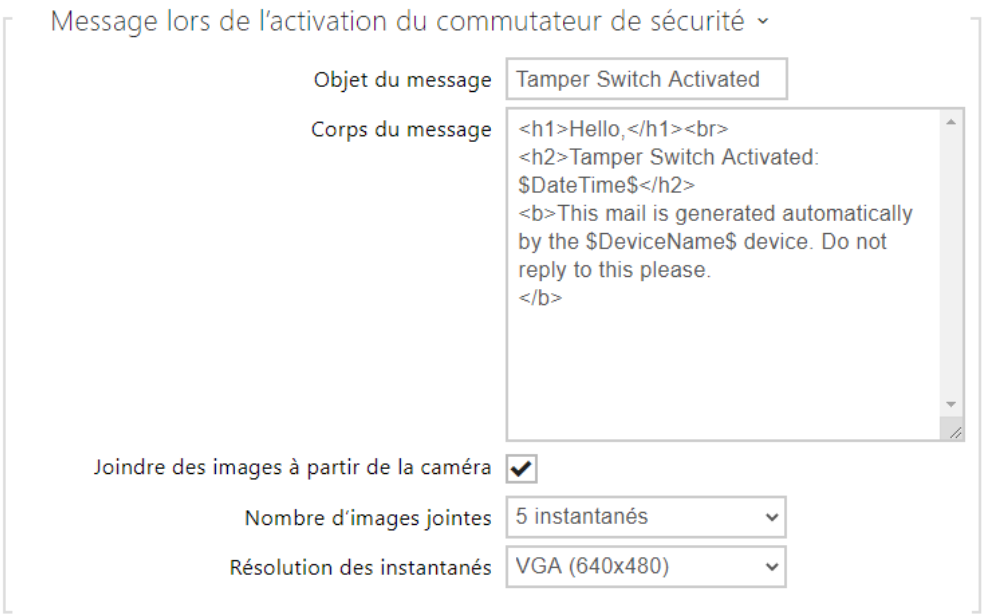
- **Objet du message** – définissez l'objet de l'e-mail envoyé.
- **Corps du message** – modifiez le texte à envoyer. Utiliser le langage de formatage HTML dans le texte. Vous pouvez insérer des symboles spéciaux en remplaçant le nom d'utilisateur, la date et l'heure et l'ID de l'appareil. Ces symboles seront remplacés par les valeurs correspondantes avant l'envoi. 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** – définissez l'objet de l'e-mail envoyé.
- **Corps du message** – modifiez le texte à envoyer. Utiliser le langage de formatage HTML dans le texte. Vous pouvez insérer des symboles spéciaux en remplaçant le nom d'utilisateur, la date et l'heure et l'ID de l'appareil. Ces symboles seront remplacés par les valeurs correspondantes avant l'envoi. 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>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

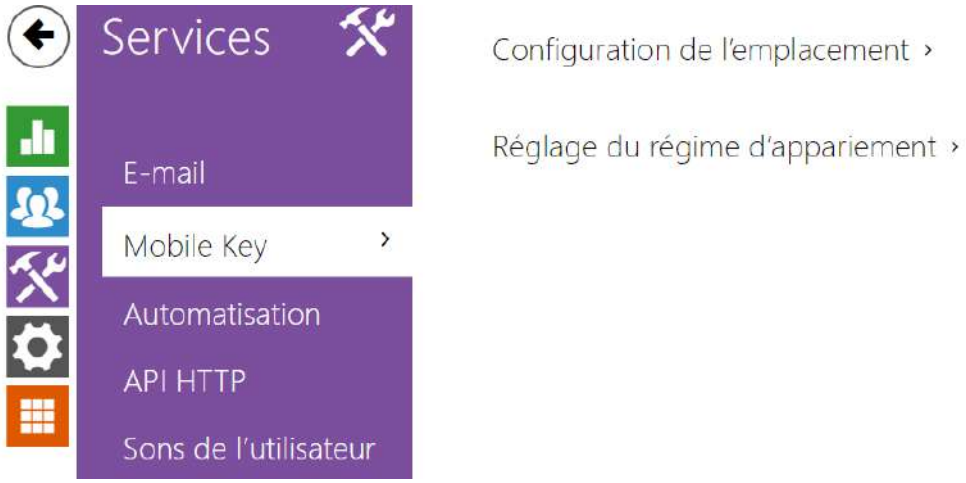
Occurrence	Symbole de substitution	Description
	$BuildTime$	date et heure d'établissement
	$UpTime$	période d'exploitation de l'équipement
Fonction du cas spécifique	$User$	nom de l'utilisateur
	$RebootReason$	raison du redémarrage
	$DialNumber$	numéro appelé, entrant ou sortant
	$SipAccountNumber$	numéro 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
$DateTime$	*	*	*	*	*	*	*
$DeviceName$	*	*	*	*	*	*	*
$Ip4Address$	*	*	*	*	*	*	*
$SoftwareVersion$	*	*	*	*	*	*	*

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
$BuildTime$	*	*	*	*	*	*	*
$UpTime$	*	*	*	*	*	*	*
$User$	*	*				*	*
$RebootReason$				*			
$DialNumber$		*				• (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 Mobile Key



Les unités de controle d'accès 2N peuvent être équipées d´un 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'unité de controle d'accès 2N : L'ID d'Authentification (nombre de 128 bits) est généré aléatoirement pour chaque utilisateur et associée à l'utilisateur de l'unité 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'unité. Vous pouvez déplacer l'ID d'authentification vers un autre utilisateur ou le copier dans une autre unité. En supprimant la valeur de l'ID d'authentification, vous pouvez bloquer l'accès de l'utilisateur.

Clé crypté pour la localisation

La communication etre l´application **2N Mobile Key** et l'appareil 2N est toujours 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'appareil 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 unités de controle d'accès 2N. Les appareils 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'une unité de controle d'accès 2N 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'unité de controle d'accès 2N. 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. 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 l'appariement

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'unité de controle d'accès 2N et peut être re-générée à tout moment par la suite.

Administration de la clé cryptée

L'unité de controle d'accès 2N 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'appareil.

> **Note**
>
> - Les clés de chiffrement sont générées automatiquement au premier lancement de l'unité de contrôle d'accès 2N et sauvegardées dans le fichier de configuration de l'appareil. 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. Les appareils avec des Emplacement ID et des clés de chiffrement identiques forment ce qu'on appelle une localisation.
- **Import** – appuyez sur ce bouton pour importer l'ID d'emplacement et les clés de chiffrement actuelles à partir d'un fichier exporté depuis une autre l'appareil 2N. Les appareils avec des Emplacement ID et des clés de chiffrement identiques forment ce qu'on appelle une localisation.

- **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'appareil.

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.

5.4.5 Automatisation

Les unités de controle d'accès 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.

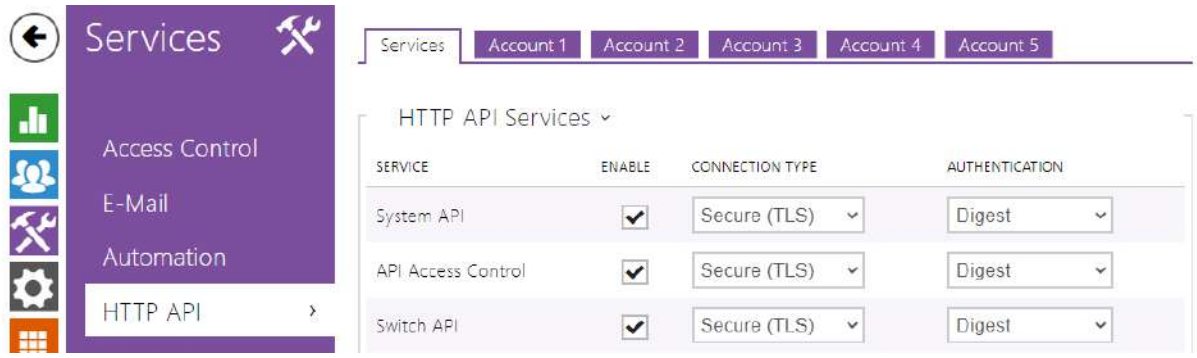
Référez-vous au Manuel d'Automatisation pour découvrir les possibilités et les détails de la configuration.

Note

- *La fonction Automatisation est disponible uniquement avec la licence Gold ou Integration améliorée.*

5.4.6 HTTP API

L'API HTTP est une interface d'application conçue pour le contrôle de certaines fonctionnalités des unités de controle d'accès 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

L'API HTTP offre les services suivants :

- **API de système** – permet les modifications de configuration de l'appareil, 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'appareil.
- **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'appareil 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 :

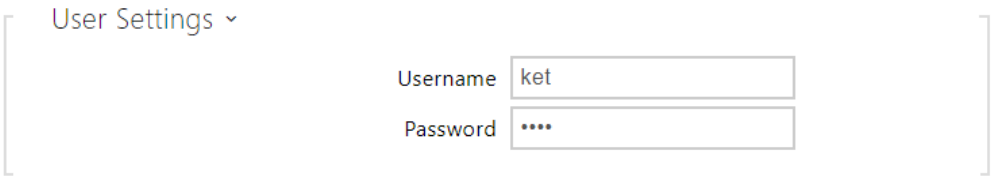
- **Aucune** – aucune authentification n'est requise. Dans ce cas, ce service est complètement non sécurisé sur le réseau local.
- **Basic** – l'authentification de base est requise selon **RFC-2617**. Dans ce cas, le service est protégé par un mot de passe transmis dans un format ouvert. Nous vous recommandons 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.

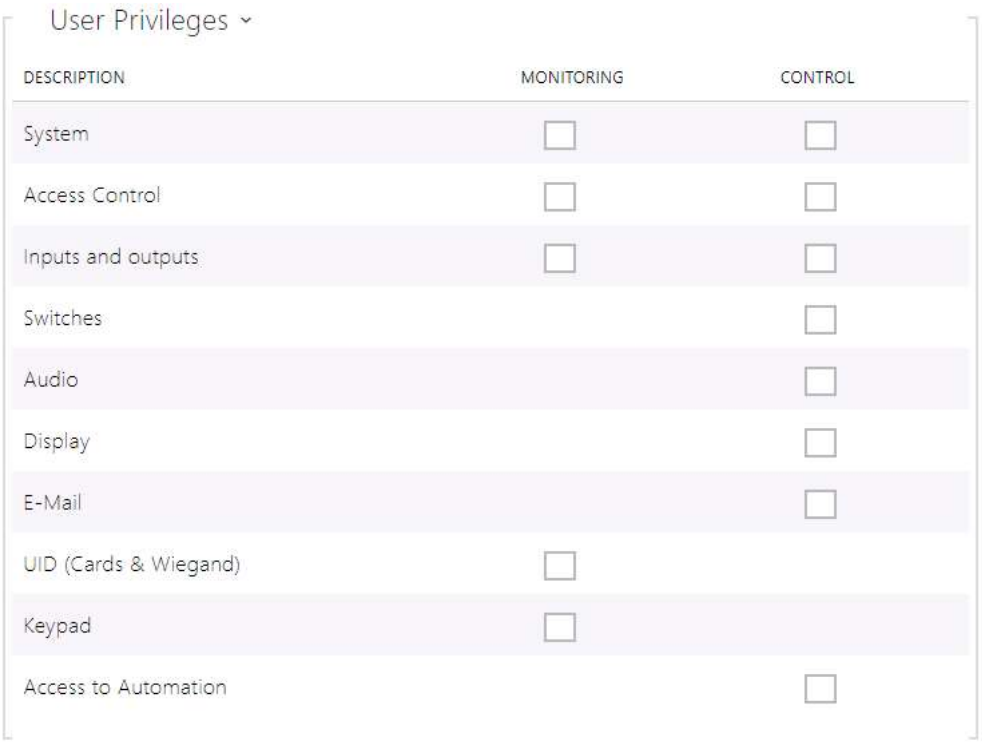
Compte 1–5

Les inités d'accès 2N 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.



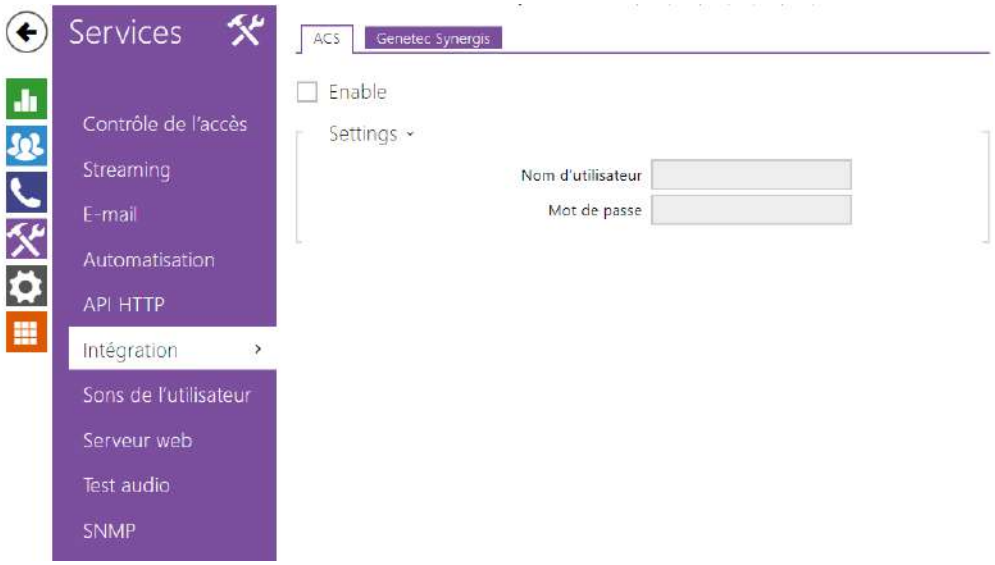
- **Nom d'utilisateur** – saisir le nom d'utilisateur pour l'authentification de HTTP API.
- **Mot de passe** – saisir le mot de passe d'authentification de HTTP API.



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

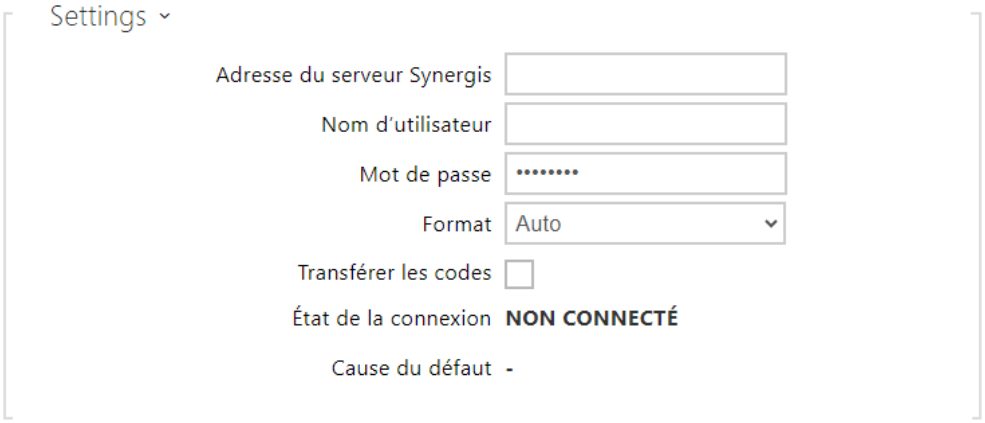
5.4.7 Intégration

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



Onglet Genetec Synergis

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



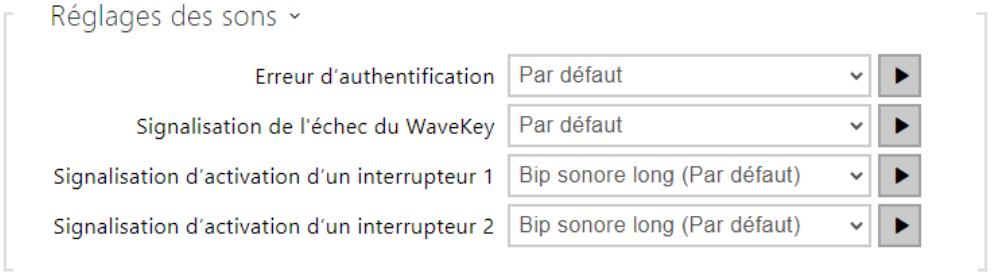
- **Adresse du serveur Synergis** – adresse IP ou nom de domaine. du serveur Synergis.
- **Nom d'utilisateur** – nom d'utilisateur utilisé lors de l'authentification.
- **Mot de passe** – mot de passe utilisé lors de l'authentification.

- **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.

5.4.8 Sons de l'utilisateur

Les sons de l'utilisateurs vous permettent d'activer ou mettre en sourdine la signalisation auditive d'activation des interrupteurs. Pour la signalisation auditive de l'authentification, référez au chapitre 5.4.1 Contrôle de l'accès.

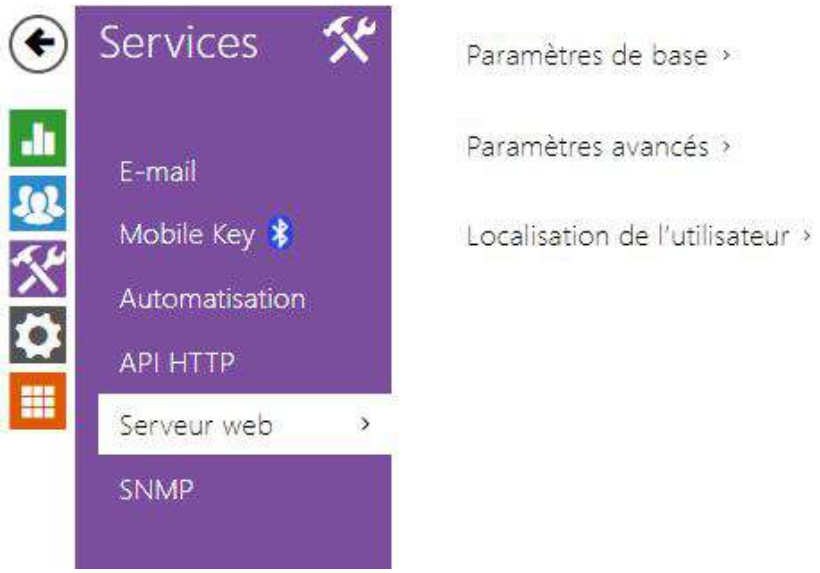
- **Langue des messages sonores –** sélectionne la langue pour les messages sonores de l'appareil. Si un fichier pour lequel une traduction est disponible est remarqué pour l'événement donné, le message sera enregistré dans la langue choisie. S'il n'y a pas de traduction disponible, un son en anglais ou linguistiquement neutre sera enregistré.



- **Erreur d'authentification** – définit le son joué lorsque l'accès est refusé.
- **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.

5.4.9 Serveur web



Vous pouvez configurer votre unité de contrôle d'accès 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'unité. Après avoir accédé à l'unité, 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'appareil :

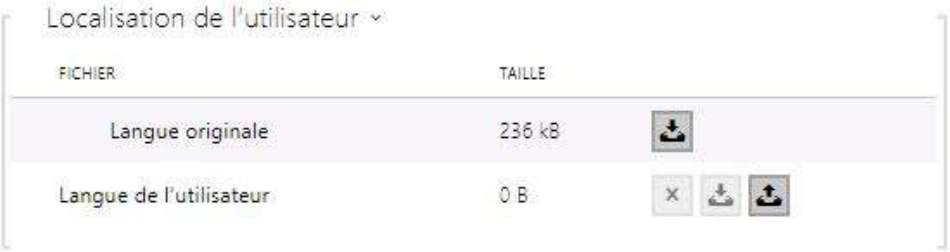
1. Commandes HTTP pour le contrôle des Interrupteurs, reportez-vous à la sous-section Interrupteur.
2. Event.HttpTrigger dans **2N Automatisation**, référez vous au Manuel concerné.

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 (**2N IP Manager**, **2N IP Network Scanner**, 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'appareil. 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'appareil.
- **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'appareil.
- **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.

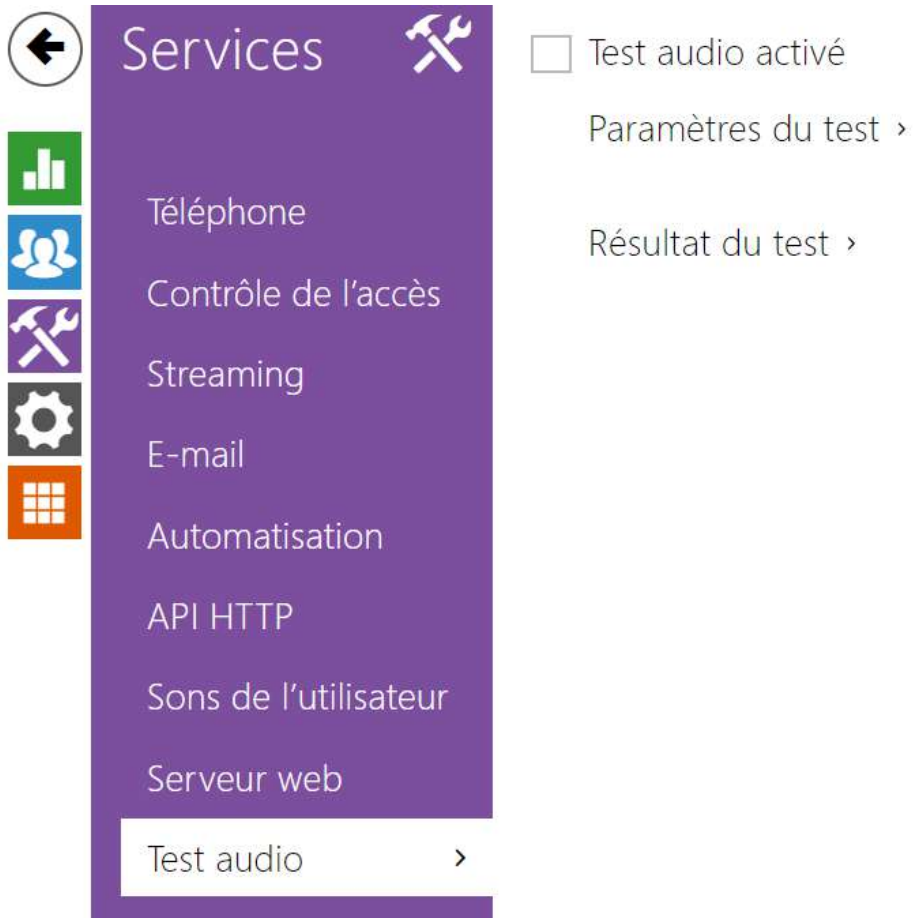


- **Langue originale** – téléchargez le fichier original contenant tous les textes de l'interface utilisateur en anglais. Le format de fichier est XML; voir ci-dessous.
- **Langue de l'utilisateur** – enregistrez, chargez et supprimez, si nécessaire, un fichier utilisateur contenant vos propres traductions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

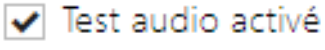
Pendant la traduction, modifiez uniquement la valeur des éléments **<s>**. Ne modifiez pas les valeurs **id**. Le nom de langue spécifié par l'attribut de langue de l'élément <strings> sera disponible dans les sélections du paramètre de langue de l'interface Web. L'abréviation du nom de langue spécifié 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.

5.4.10 Test audio

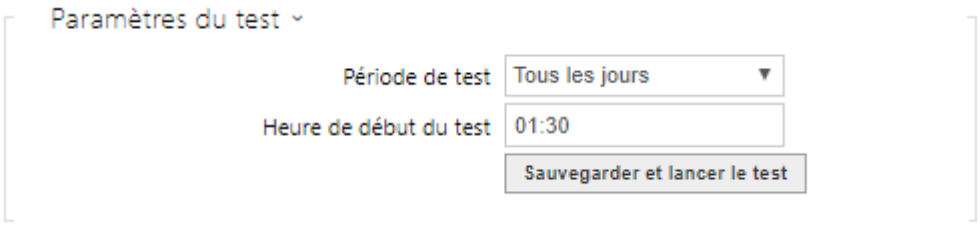


2N Access Unit QR permet vous permettent d'effectuer des tests périodiques du haut-parleur et du microphone intégrés. À des fins de test, le haut-parleur intégré génère un ou plusieurs bips brefs. Le microphone intégré reçoit la tonalité générée et le test réussit si la tonalité est détectée correctement. 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 appareil ou traité par l'interface d'**Automatisation**.

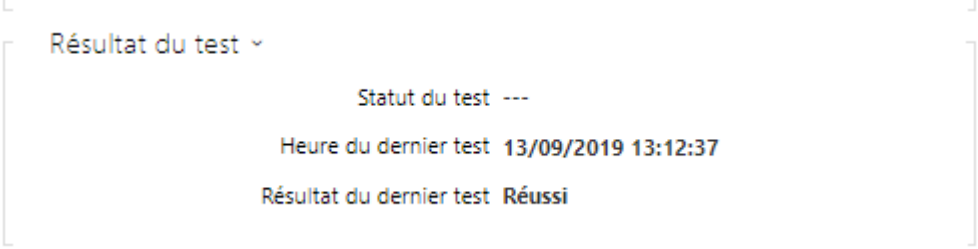
Liste des Paramètres



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

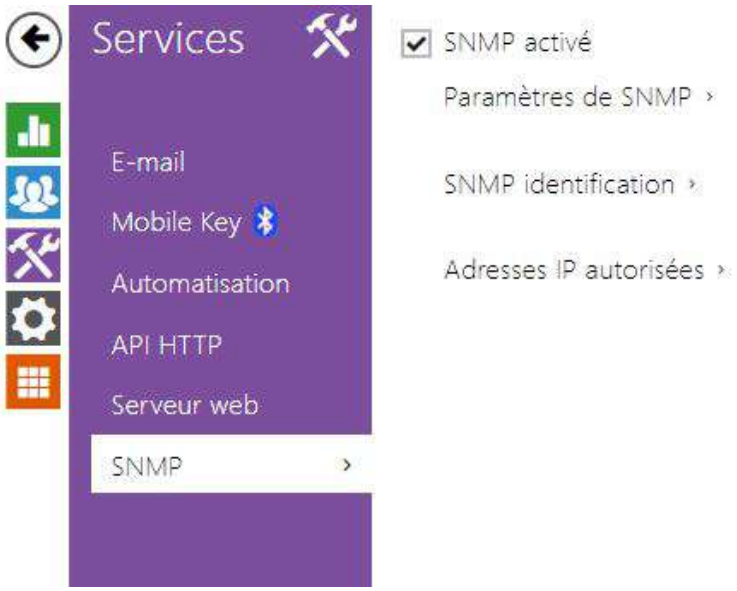


- **Période de test** – il permet de définir la période d'exécution du test. Le test peut être exécuté automatiquement une fois par jour ou une fois par semaine.
- **Heure de début du test** – il permet de définir l'heure à laquelle le test doit être régulièrement effectué. Vous pouvez régler l'heure au format HH : MM. Nous vous recommandons de régler l'heure à laquelle une utilisation minimale de l'appareil 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.

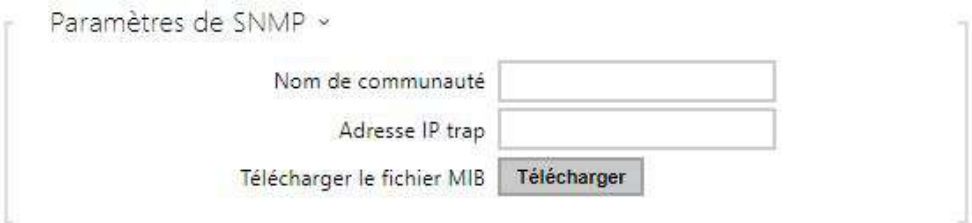
5.4.11 SNMP



Les unités de contrôle d'accès 2N intègrent une fonctionnalité de supervision à distance via le protocole SNMP. L'unité de controle d'accès 2N supporte le SNMP version 2c.

Liste des paramètres

- **SNMP Activé** – Vous permet d'activer la fonction SNMP



- **Nom de communauté** – chaîne de texte représentant la clé d'accès aux objets de la table MIB
- **Adresse IP trap** – il s'agit de l'adresse IP à laquelle les concepts d'interruptions SNMP sont envoyés.
- **Télécharger le fichier MIB** – téléchargez la définition MIB depuis un appareil

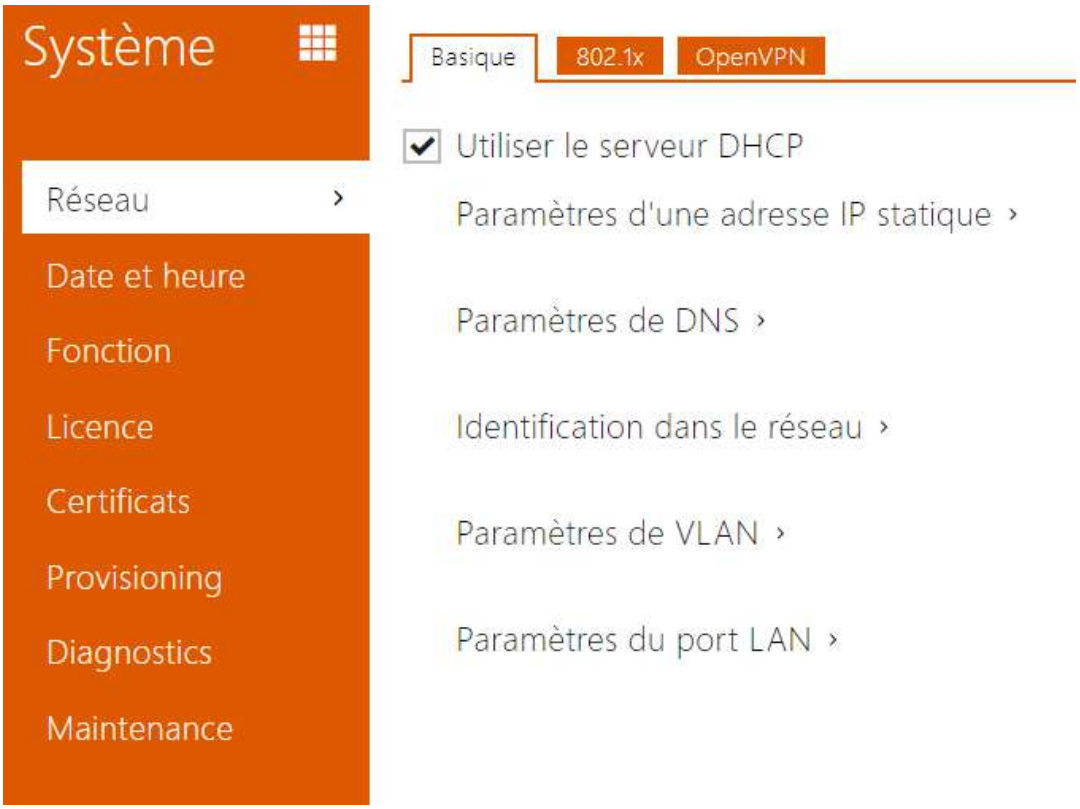
- **Contact** – permet d'entrer le contact de l'administrateur du dispositif (par ex. nom, e-mail, etc.).
- **Nom** – entrez le nom du dispositif.
- **Emplacement** – permet d'entrer la description de l'emplacement du dispositif (par ex. 1er étage).

- **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 Système

Voici les onglets que vous pouvez trouver dans cette section :

5.5.1 Réseau



Comme les unités de contrôle d'accès 2N sont connectées 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.

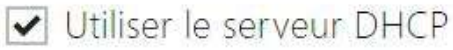
Conseil

- *Pour connaître l'adresse IP actuelle de votre unité de contrôle d'accès 2N, 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'unité correspondant l'appareil.*

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

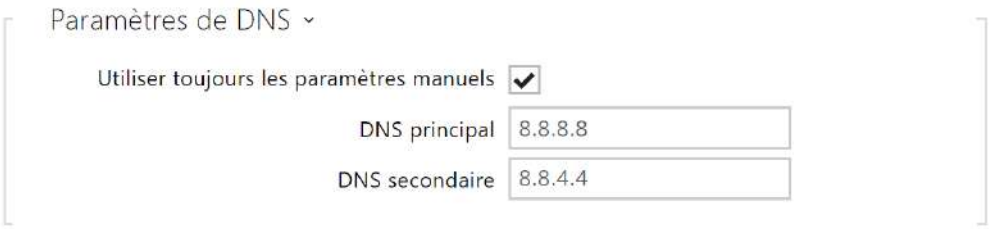
L'onglet Trace vous permet de lancer la capture des paquets entrants et sortants sur l'interface réseau de l'unité de contrôle d'accès 2N. Le fichier contenant les paquets capturés peut être téléchargé pour le traitement sur Wireshark, par exemple. (www.wireshark.org).

Liste des paramètres

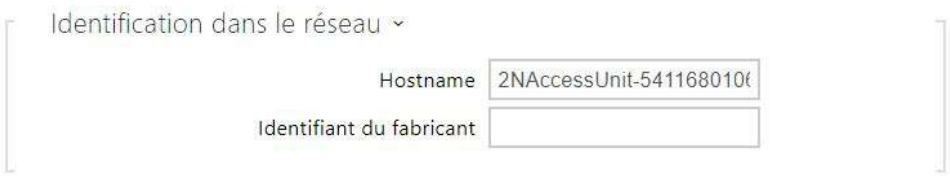


- **Utiliser le serveur DHCP** – activez l'obtention automatique de l'adresse IP à partir du serveur LAN DHCP. Si le serveur DHCP n'est pas disponible ou n'est pas accessible sur votre LAN, paramétrer le réseau manuellement.

- **Adresse IP statique** – l'Adresse IP statique de l'unité de contrôle d'accès 2N 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'appareil 2N.
- **Identifiant du fabricant** – définissez l'identifiant de classe du fournisseur sous la forme d'une chaîne de caractères pour l'option DHCP 60.

- **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.

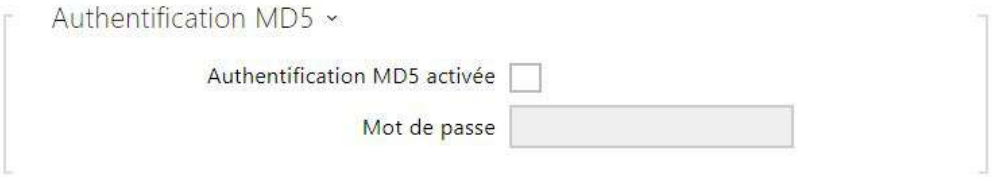
- **Mode de port requis** – définissez le port de l'interface réseau par défaut (Automatique ou Half Duplex – 10 Mbps). Cela permet de réduire la vitesse de transmission à 10 mbps si l'infrastructure du réseau utilisée (câblage) ne peut pas supporter 100 Mbps.
- **État du port actuel** – état actuel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

802.1x

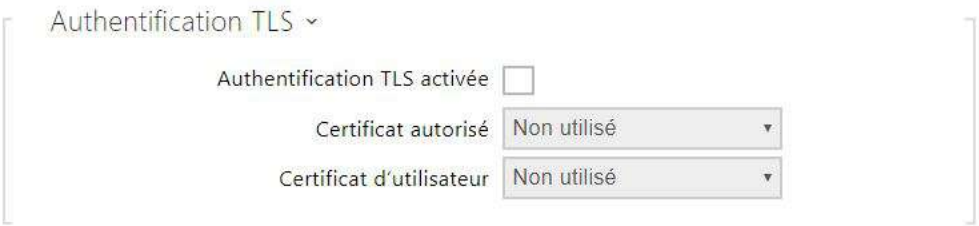
Observation

- 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.

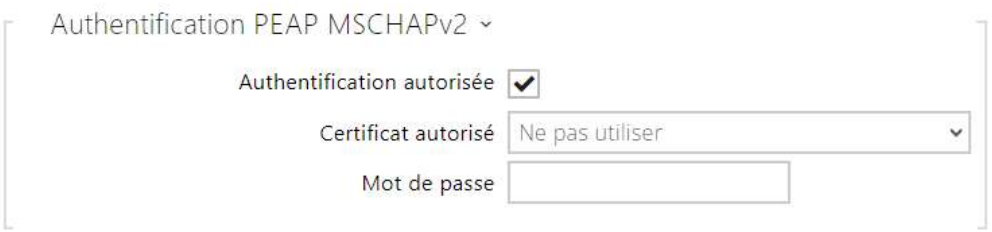


- **Authentification MD5 activée** – activez l'authentification des périphériques réseau via le protocole 802.1x EAP-MD5. Si votre réseau ne supporte pas 802.1x, n'activez pas cette fonction. Si vous le faites, l'appareil deviendra inaccessible.
- **Mot de passe** – renseignez le mot de passe d'accès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

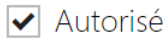
reporter au chapitre sur les Certificats. Si aucun certificat autorisé n'est inclus, la vérification du certificat public RADIUS ne peut être effectuée.
- **Certificat d'utilisateur** – spécifiez le certificat d'utilisateur et la clé privée pour vérifier si le dispositif est autorisé à communiquer sur 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.

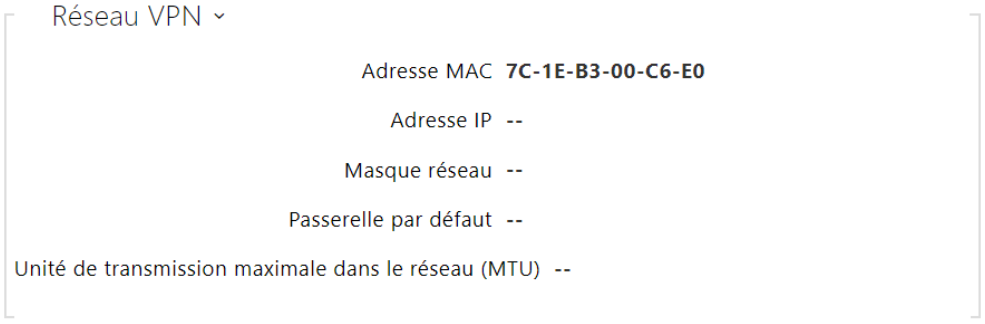
Open VPN

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.

5.5.2 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'appareil soient correctement définies.

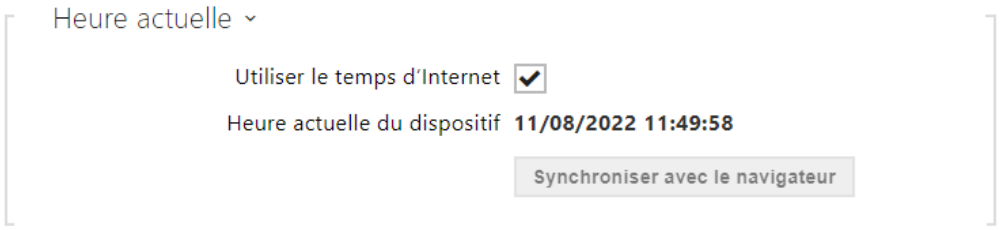
Les unités de contrôle d'accès 2N sont équipés d'une horloge de secours en temps réel pouvant résister à plusieurs jours de pannes de courant. Vous pouvez à tout moment synchroniser l'heure l'appareil avec l'heure d'Internet en cochant la fonction **Utiliser l'heure réelle d'Internet** ou avec l'heure actuelle de votre PC à l'aide du bouton **Synchroniser dans le navigateur**.

Note

- *L'appareil 2N 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.).*

Dans la pratique, la précision du circuit de l'appareil en temps réel est d'environ ± 0,005%, ce qui peut entraîner un écart de ± 2 minutes par mois. Pour une précision et une fiabilité maximales, nous recommandons de toujours utiliser la fonction **Utiliser l'heure réelle d'Internet**.

Liste des paramètres

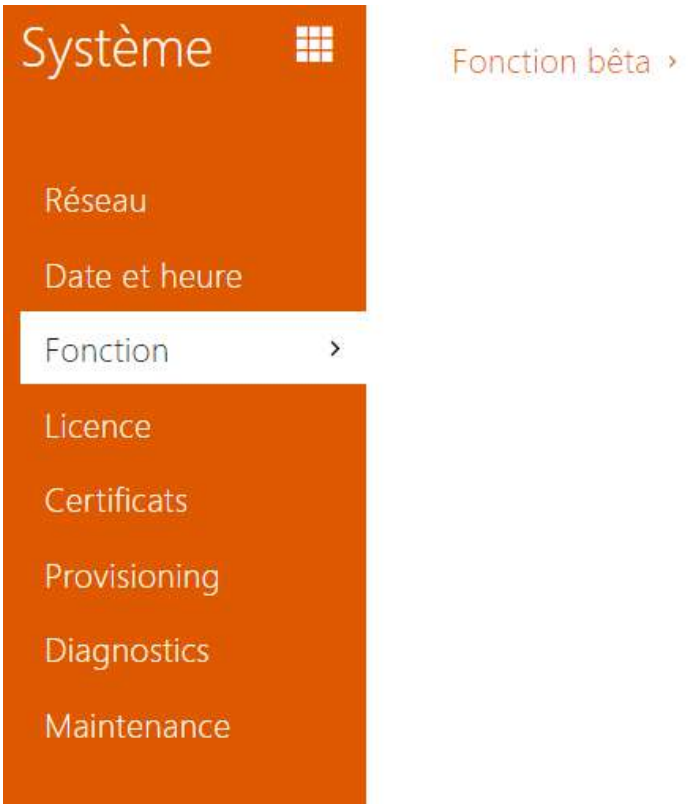


- **Utiliser le temps d'Internet** – Activer l'utilisation du serveur NTP pour la synchronisation de l'heure du dispositif.
- **Synchroniser avec le navigateur** – appuyez sur le bouton pour synchroniser la valeur temporelle de l'unité de contrôle d'accès 2N avec la valeur temporelle de votre ordinateur.

- **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.

- **Utiliser le serveur NTP** – activez l'utilisation du serveur NTP pour la synchronisation de l'heure de l'appareil. 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.
- **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.

5.5.3 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.

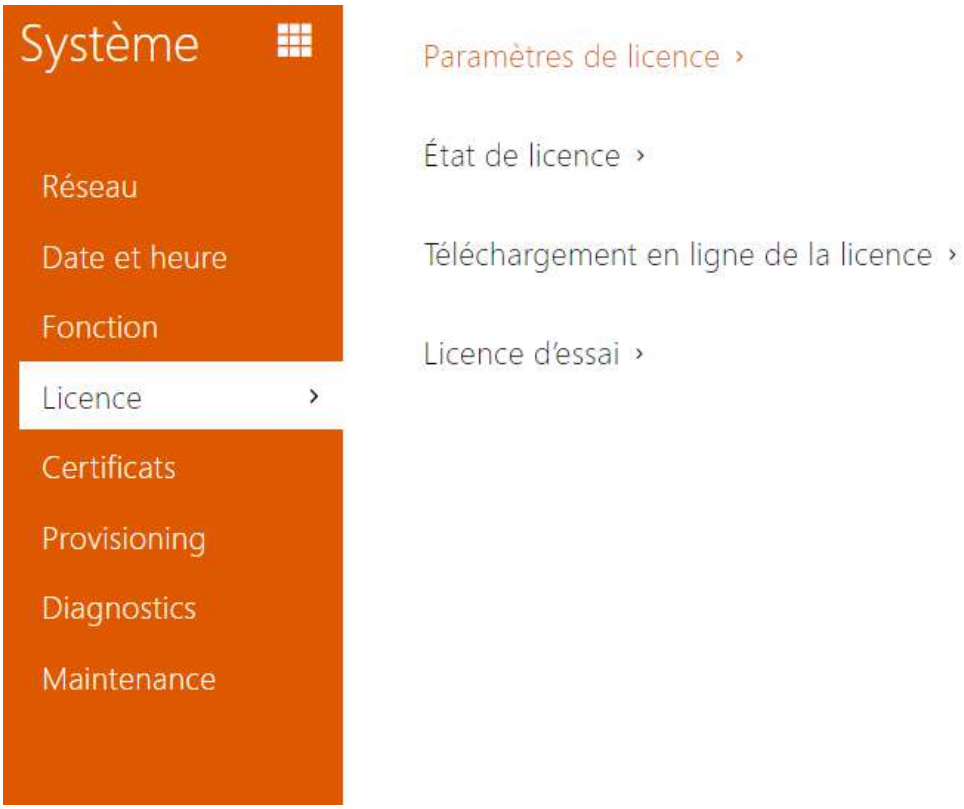
La fonction ne sera lancée ou arrêtée qu'après le redémarrage de l'appareil. Tant que l'appareil n'est pas redémarré, la demande de changement d'état peut être annulée à l'aide de l'action **Annuler**.

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.

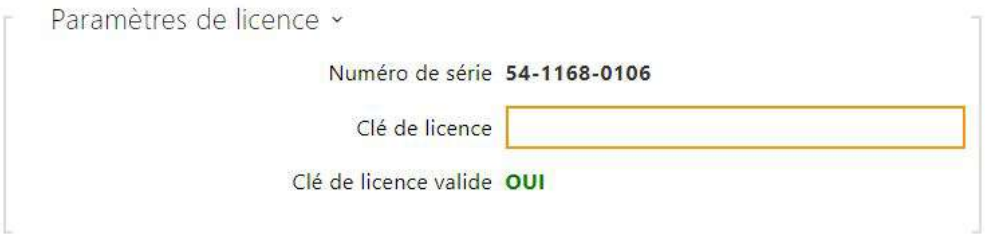
Nom de la fonction bêta	Description
Fichier de configuration protégé par un mot de passe	Cette fonction permet de crypter le fichier de configuration avec un mot de passe lors de sa sauvegarde (voir 5.5.8 Maintenance). Lors du téléchargement du fichier de configuration sur l'appareil, le mot de passe 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.

5.5.4 Licence



Certaines fonctionnalités des unités de contrôle d'accès 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 appareil.

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.
  - **Sécurité 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.
  - **Intégration améliorée** – vérifiez si les fonctions activées par la licence Intégration améliorée sont disponibles.
  - **Support de commande de l'ascenseur** – vérifiez si les fonctions activées par la licence de Contrôle du Module Ascenseur sont disponibles.

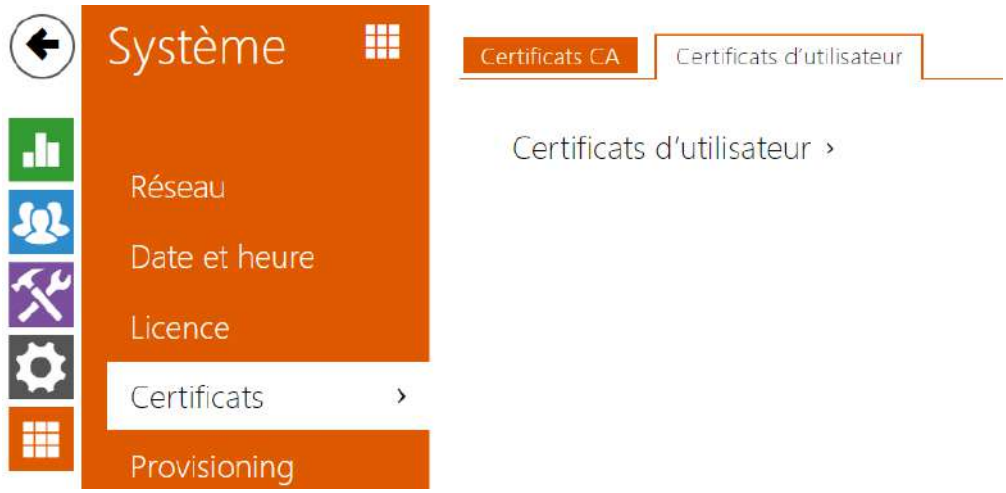
Conseil

- Fonctionnalités sous license

- **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, échec : licence non disponible.

- **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.

5.5.5 Certificats



Certains services réseau des unités de contrôle d'accès 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 suivants utilisent le protocole TLS :

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

L'unité de contrôle d'accès 2N 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'appareil 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'unité de contrôle d'accès 2N:

- accepte les formats de certificat DER (ASN1) et PEM.
- prend en charge le cryptage AES, DES et 3DES.
- 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

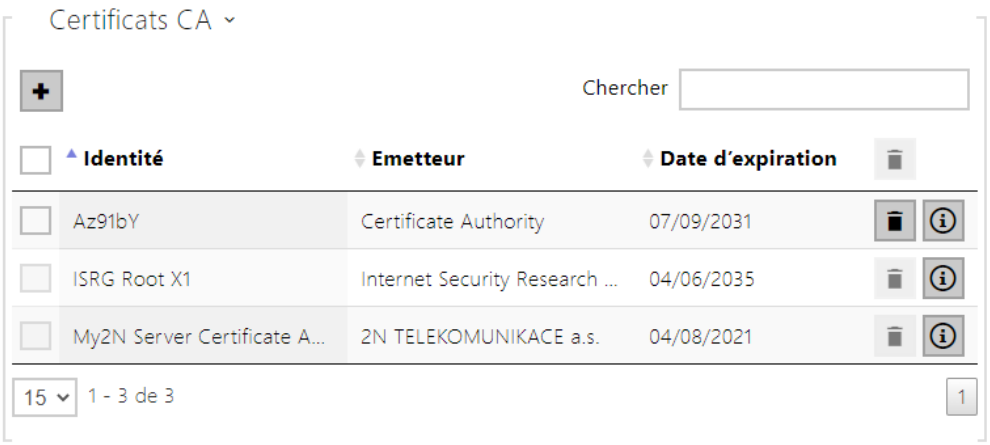
- Les certificats CA doivent utiliser le format X.509 v3.

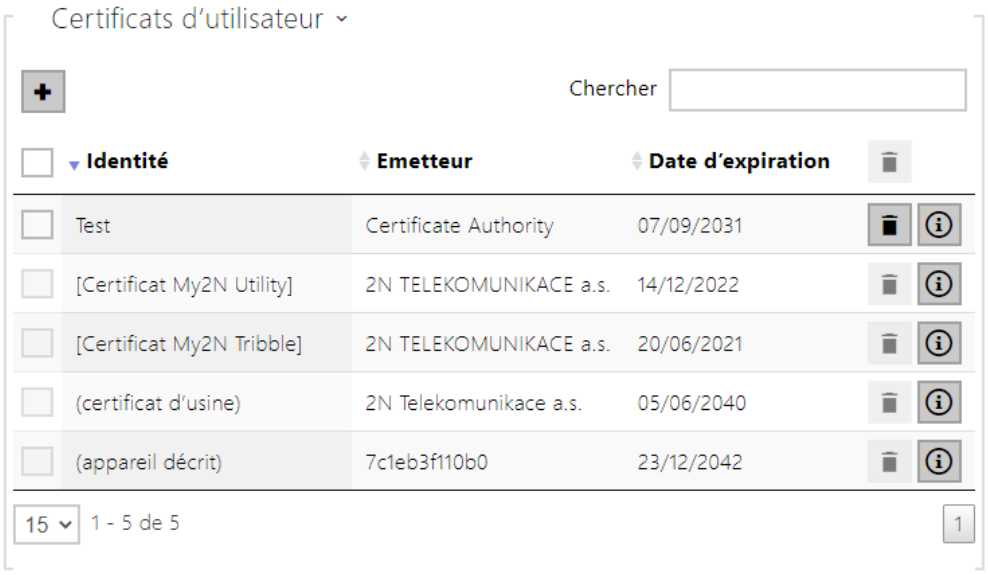
Lors de la première mise sous tension, l'unité de contrôle d'accès 2N génère automatiquement le **certificat** et la **clé privée auto-signés** pour le **Serveur Web** et les **services de messagerie**, sans vous obliger à charger un certificat et une clé privée.

Note

- *Si vous utilisez le certificat auto-signé pour le chiffrement du serveur Web de l'unité - communication entre navigateurs, la communication est sécurisée, mais le navigateur vous avertit qu'il est incapable de vérifier la validité du certificat de l'unité de contrôle d'accès 2N.*

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

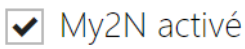
- Pour les certificats basés sur des courbes elliptiques, utilisez uniquement les courbes secp256r1 (ou prime256v1, également appelée NIST P-256) et secp384r1 (ou NIST P-384).

5.5.6 Provisioning

Les unités de contrôle d'accès 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 unités de contrôle d'accès 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'unité de contrôle d'accès 2N 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'unité de contrôle d'accès 2N est très faible (la nuit, par exemple).

Les unités de contrôle d'accès 2N recherchent les formats de fichier suivants :

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

MODEL dans le nom du fichier spécifie le modèle d'appareil :

1. **au – 2N Access Unit**
2. **aug2 – 2N Access Unit 2.0**
3. **aum – 2N Access Unit M**
4. **auqr - 2N Access Unit QR**

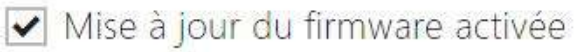
MACADDR est l'adresse MAC de l'appareil au format 00-00-00-00-00-00. Recherchez l'adresse MAC sur la plaque de production de l'unité ou dans l'onglet **État** de l'unité via l'interface Web.

Exemple :

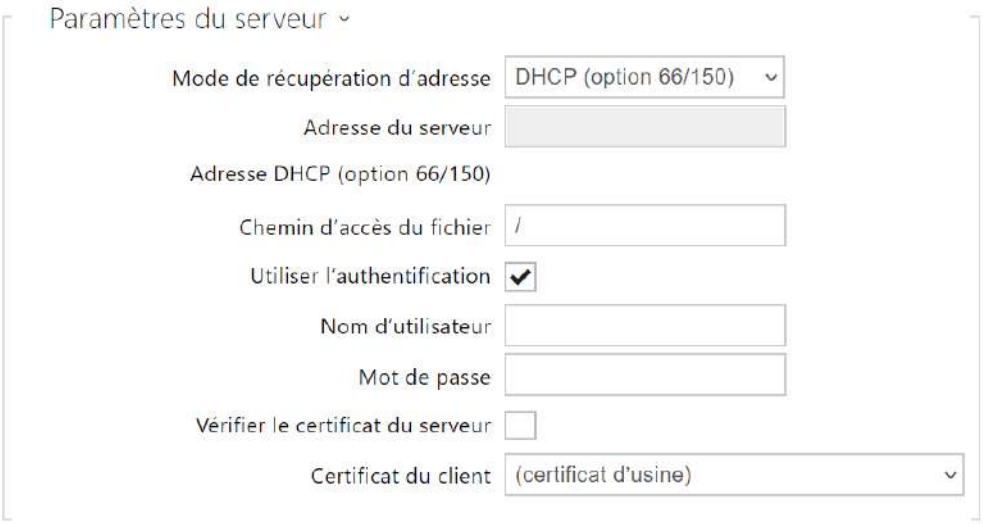
2N Access Unit 2.0 avec l'adresse MAC 00-87-12-AA-00-11 télécharge les fichiers suivants à partir du serveur TFTP :

- aug2-firmware.bin
- aug2-common.xml
- aug2-00-87-12-aa-00-11.xml

Liste des paramètres

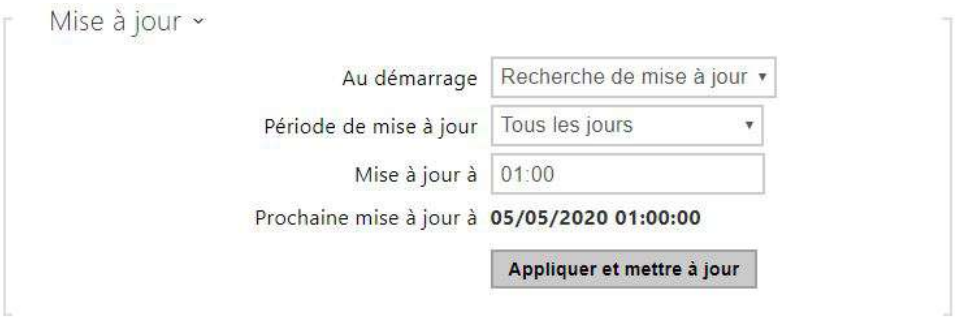


- **Mise à jour du firmware activée** – activez la mise à jour automatique du firmware / de la configuration à partir du serveur TFTP / HTTP.

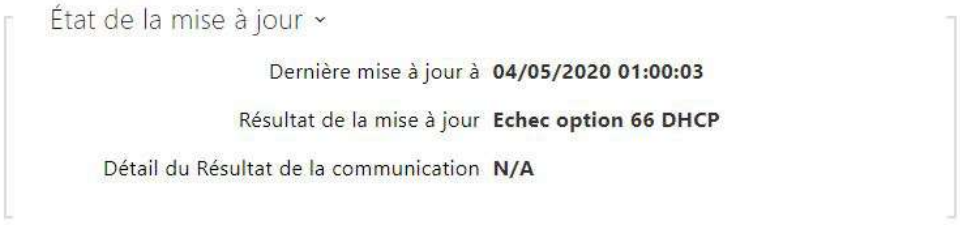


- **Mode de récupération d'adresse** – définissez si l'adresse du serveur TFTP/HTTP doit être saisie manuellement ou via une valeur récupérée automatiquement à partir du serveur DHCP utilisant l'option 66.
- **Adresse du serveur** – saisissez manuellement l'adresse du serveur TFTP (tftp://ip_adresse), 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'appareil à communiquer avec le serveur ACS.



- **Au démarrage** – activez la vérification et, si possible, mettez à jour l'exécution à chaque démarrage de l'unité de contrôle d'accès 2N.
- **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.



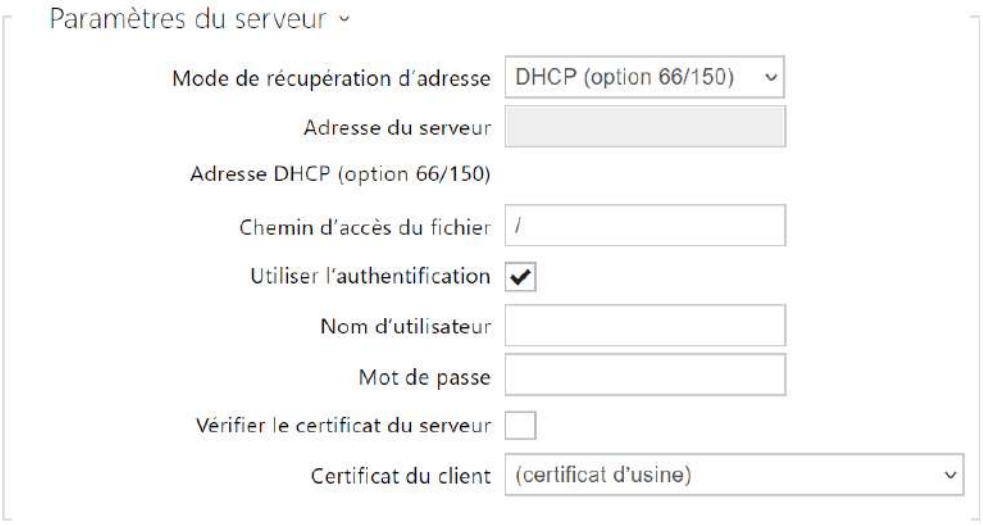
- **Dernière mise à jour à** – heure de la dernière mise à jour.
- **Résultat de la mise à jour** – résultat de la dernière mise à jour. Les options suivantes sont disponibles :

Resultat	Description
En cours…	Mise à jour en cours.
Mise à jour réussie	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.
Firmware à jour	La tentative de mise à jour du firmware révèle que la dernière version du firmware a été chargée.
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.
Erreur interne	Une erreur non spécifiée s'est produite lors du téléchargement du fichier.
Fichier non trouvé	Le fichier n'a pas été trouvé sur le serveur.
Fichier invalide	Le fichier à télécharger est corrompu ou d'un type incorrect.

Configuration

Utilisez l'onglet **Configuration** pour télécharger la configuration automatique à partir du serveur que vous avez défini. L'unité de contrôle d'accès 2N télécharge périodiquement un fichier du serveur et est reconfiguré sans être redémarré.

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

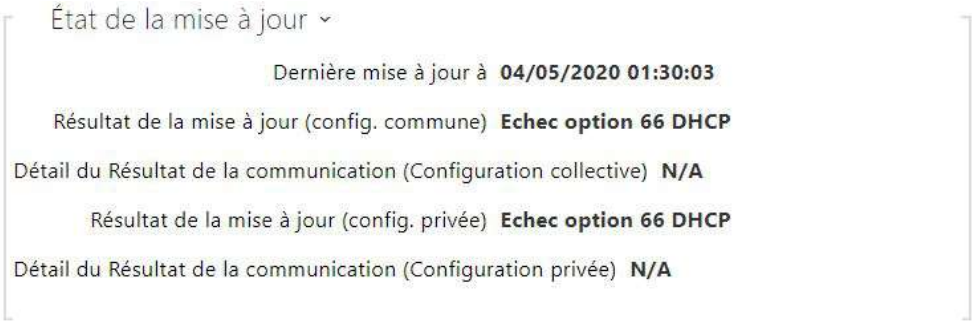


- **Mode de récupération d'adresse** – définissez si l'adresse du serveur TFTP/HTTP doit être saisie manuellement ou si une valeur récupérée automatiquement à partir du serveur DHCP utilisant l'option 66 doit être utilisée.
- **Adresse du serveur** – saisissez manuellement l'adresse du serveur TFTP (tftp://ip_adresse), 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'appareil 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'appareil.
- **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.
- **Certificat autorisé** – définit une liste des autorités de certifications pour vérifier la validité du certificat public du serveur ACS.
- **Certificat d'utilisateur** – définit le certificat client et la clé privée qui autorise l'appareil à communiquer avec le serveur ACS.

Info

- L'appareil 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'appareil.
- **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 (configuration 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 commune)** – code d'erreur de communication avec le serveur ou le code d'état du protocole TFTP / HTTP.
- **Résultat de la mise à jour (configuration privée)** - la configuration privée suit la mise à jour de la configuration commune. L'appareil avec une configuration privée est identifié par son adresse MAC. 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 le code d'état du protocole TFTP / HTTP.

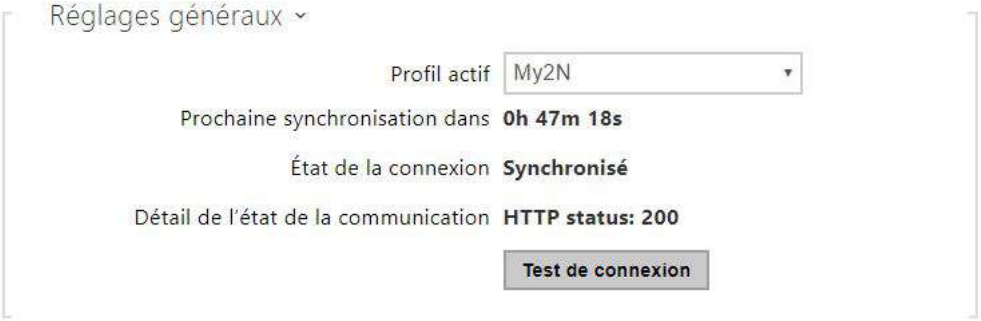
My2N / TR069

Utilisez cet onglet pour activer et configurer la gestion de l'appareil à distance via le protocole TR-069. Le TR-069 vous aide à configurer de manière fiable les paramètres de l'appareil, 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 unité 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'appareil.

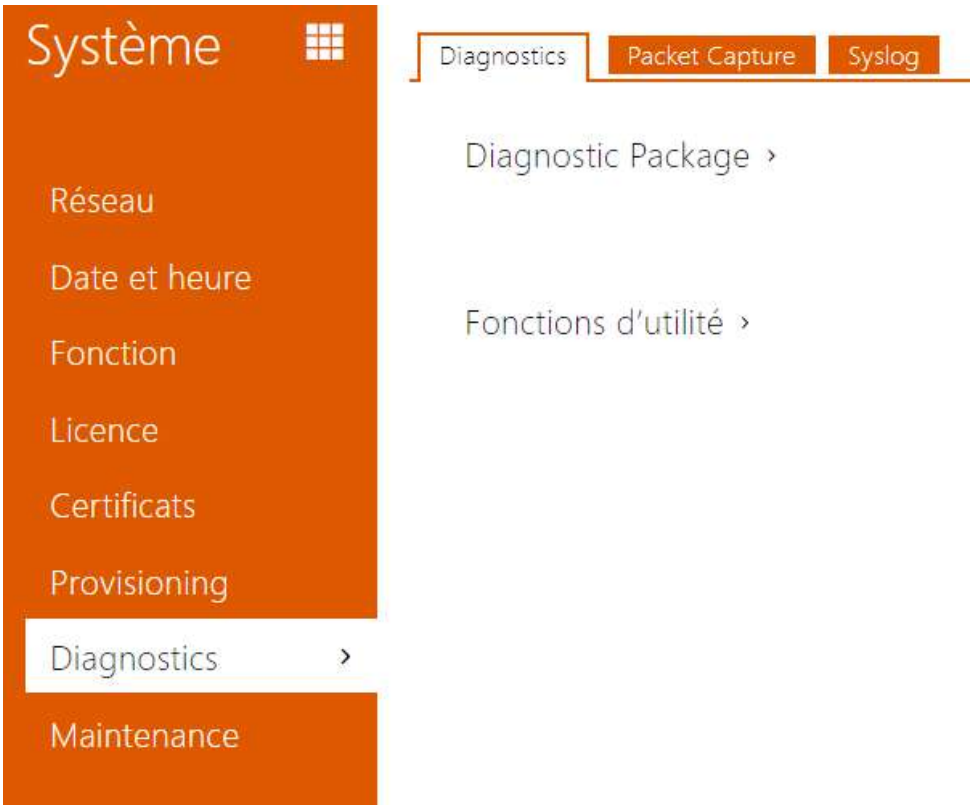
- **My2N / TR069 activé** – activez la connexion à My2N ou à un autre serveur ACS.



- **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'appareil 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.

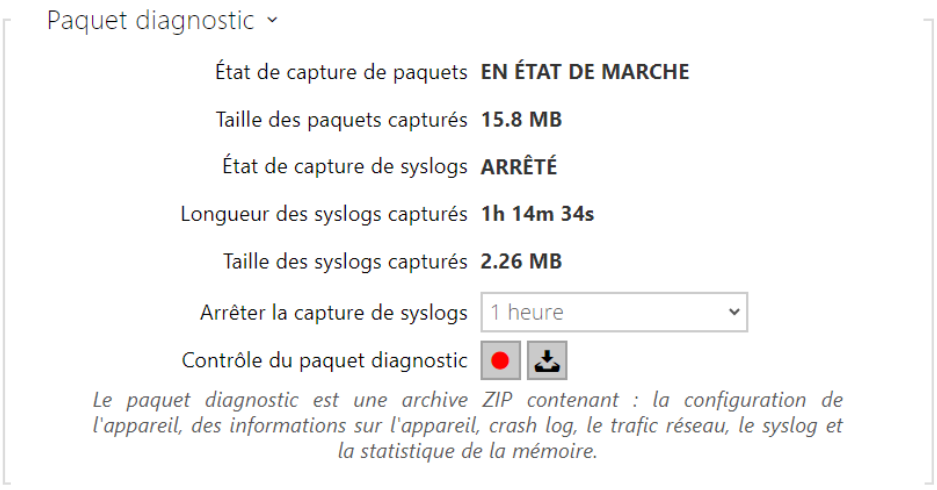
- **Adresse du serveur ACS** – définissez l'adresse ACS au format suivant : ipadresse[: port], 192.168.1.1:7547, par exemple.
- **Nom d'utilisateur** – définissez le nom d'utilisateur pour l'authentification de l'appareil lors de la connexion au serveur ACS.
- **Mot de passe** – définissez le mot de passe pour l'authentification de l'appareil 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'appareil 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'appareil dans l'ACS.
- **Intervalle de vérification** – définissez l'intervalle d'enregistrement périodique de l'appareil dans le système ACS s'il est activé par le paramètre **Vérification périodique**.

5.5.7 Diagnostic



Diagnostic

L'interface vous permet de commencer à capturer des journaux de diagnostic, qui peuvent ensuite être téléchargés et envoyés à l'assistance technique. Les journaux de diagnostic capturés aident à identifier et à résoudre les problèmes signalés. Les journaux contiennent des informations sur l'appareil, sa configuration, le trafic réseau, le journal des pannes et les statistiques de la mémoire.

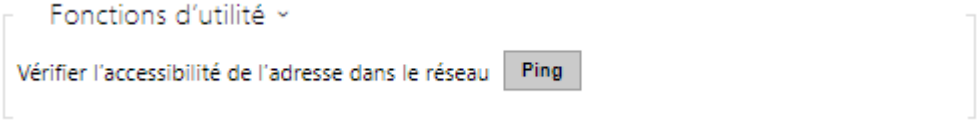


- **État de capture de paquets** – indique si la capture de paquets est lancée dans l'onglet Capture de paquets.
- **Taille des paquets capturés** – indique le nombre de paquets capturés.
- **État de capture de syslogs** – indique si la capture des messages syslog est lancée dans l'onglet Syslog.
- **Longueur 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.



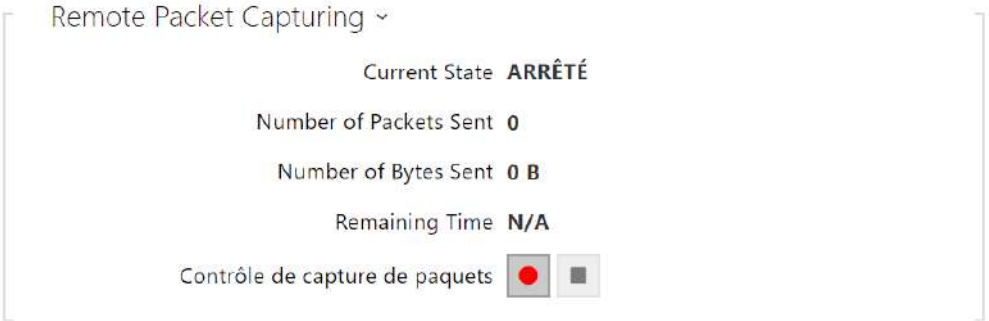
- **Vérifier l'accessibilité de l'adresse dans le réseau** – vérifiez l'accessibilité de l'adresse réseau via la commande Ping dans les systèmes d'exploitation standard. Appuyez sur Ping

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'appareil. Les paquets capturés peuvent être stockés localement dans la mémoire tampon de l'appareil d'une taille de 4 MB ou à distance sur le PC de l'utilisateur.

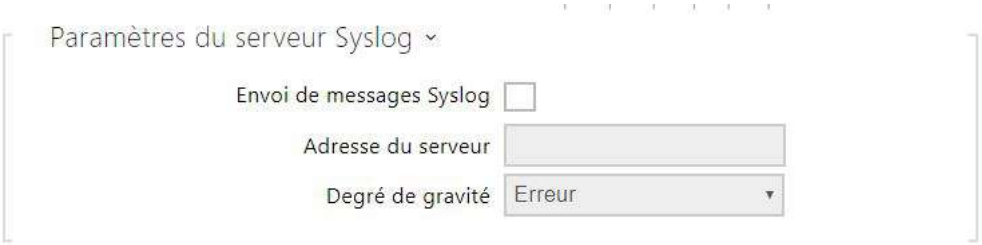
Une fois que la mémoire tampon est pleine durant la capture locale, les paquets stockés les plus anciens sont automatiquement copiés. Lors de la capture locale des paquets, nous recommandons de réduire le débit binaire du flux vidéo à une valeur inférieure à 512 kbps. Appuyez sur  pour démarrer,  pour arrêter et  pour télécharger le fichier de capture des paquets.



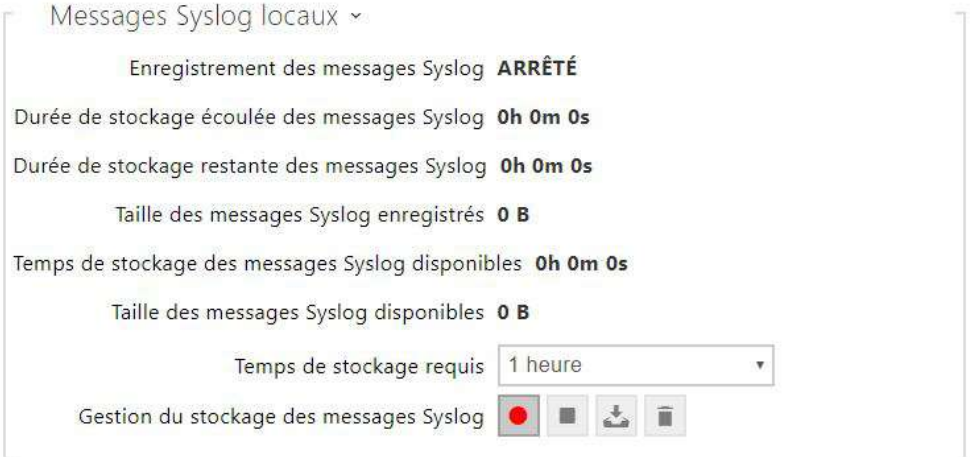
Vous pouvez lancer la capture à distance en appuyant sur le bouton . Il convient de spécifier le temps (s) durant lequel les paquets entrants et sortants doivent être capturés. Une fois la valeur de temps définie expirée, le fichier contenant les paquets capturés sera automatiquement téléchargé sur le PC de l'utilisateur. Arrêter la capture est possible à l'aide du bouton .

Syslog

Les unités de contrôle d'accès 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'unité de contrôle d'accès 2N.

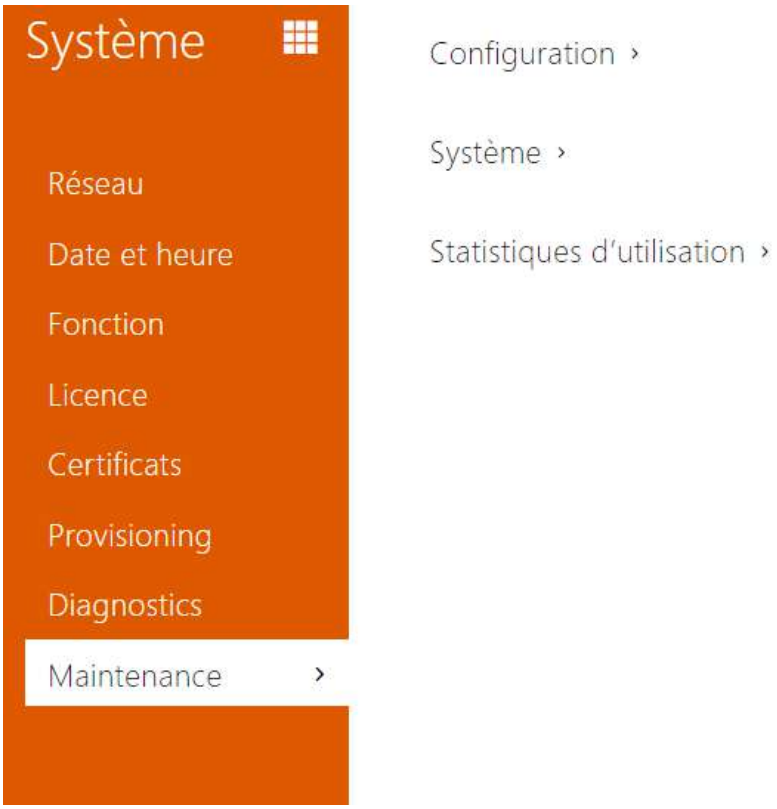


- **Envoi de messages Syslog** – activez l'envoi de messages système au serveur Syslog. Assurez-vous que l'adresse du serveur est bien paramétrée.
- **Adresse du serveur** – définissez l'adresse IP[:port] ou MAC du serveur sur lequel l'application s'exécute pour capturer les messages syslog.
- **Degré 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.

5.5.8 Maintenance



Utilisez ce menu pour gérer la configuration de votre unité de contrôle d'accès 2N 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 l'unité de contrôle d'accès 2N. Appuyez sur le bouton pour télécharger le fichier de configuration sur votre ordinateur.

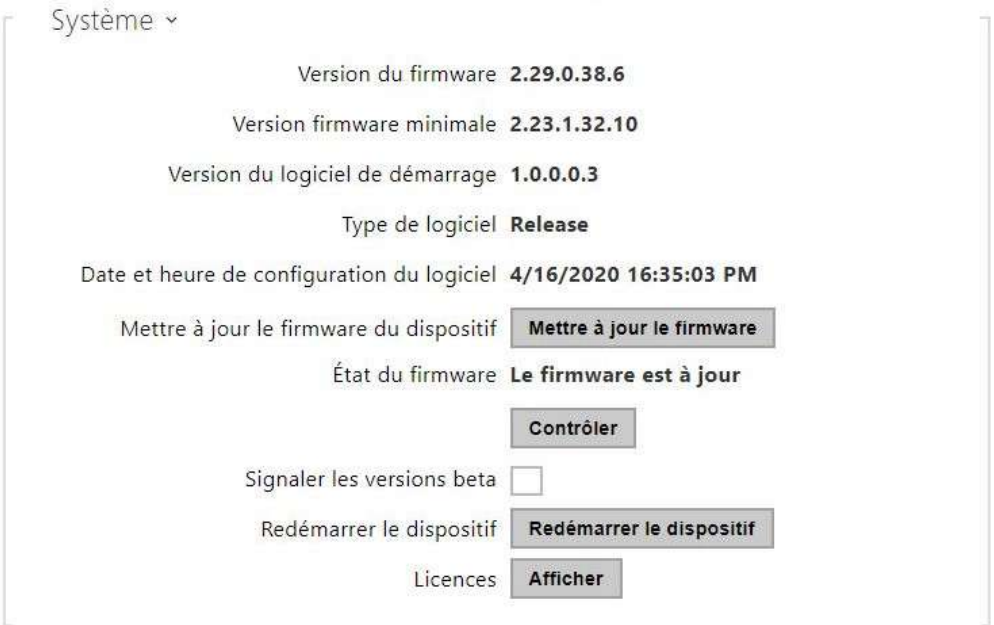
Observation

- *Traitez le fichier avec prudence, car la configuration de l'unité de contrôle d'accès 2N peut inclure des informations délicates telles que les données des utilisateurs et les codes d'accès.*
- *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.*

- **Réinitialiser la configuration** – réinitialisez les valeurs par défaut pour tous les paramètres de l'unité de contrôle d'accès 2N, à l'exception des paramètres réseau. Utilisez le cavalier correspondant ou appuyez sur *Réinitialiser* pour réinitialiser tous les paramètres l'unité de contrôle d'accès 2N; reportez-vous au manuel d'installation de votre unité.

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.*



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 données, 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'données 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 2N.com. pour la dernière version FW de votre unité. La mise à niveau du firmware n'affecte pas la configuration car l'unité de contrôle d'accès 2N vérifie le fichier pour empêcher le téléchargement d'un fichier erroné ou corrompu.
- **Vérifiez le firmware en ligne** – 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'unité de contrôle d'accès 2N. Le processus prend environ 30 s. Lorsque l'unité a obtenu l'adresse IP au redémarrage, la fenêtre de connexion s'affiche automatiquement.

Observation

- L'écriture de changement de configuration de l'appareil prend 3 à 15 s, en fonction de la taille de la configuration. Ne redémarrez pas l'appareil pendant ce processus.

- **Licences** – 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.

6. Informations supplémentaires

Voici les onglets que vous pouvez 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 Access Unit est en accord avec les directives et réglementations suivantes:

- 2014/53/UE relative aux équipements radioélectriques
- 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 A 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 A 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.