Manuel de configuration des unités de contrôle d'accès 2N

v.2.39

www.2n.com

Contenu:

1. Vue d'ensemble du produit

Le système de **contrôle d'accès IP 2N** peut (avec les logiciels complémentaires et/ou les **interphones IP 2N**) vous offrir une solution complète de contrôle d'accès pour tout un projet.

Votre **Unité de contrôle d'accès 2N** peut être équippée avec un clavier numérique, afin de l'utiliser comme verrouillage à code.

Votre **Unité de contrôle 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.

L'**Unité de contrôle d'accès 2N** peut être équippée avec un relai pour controller les verrous électriques ou tout autre appareil connecté à ce système d'accès. Il y a énormément de possibilités pour paramètrer quand et comment activer ces verrous - avec code, automatiquement, en pressant 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

Paramètres de connexion réseau (LAN)

Vous devez connaître l'adresse IP pour vous connecter efficacement à l'interface de configuration de l'**unité de contrôle d'accès 2N**. 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.

Maintenant 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.

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.

Conseil

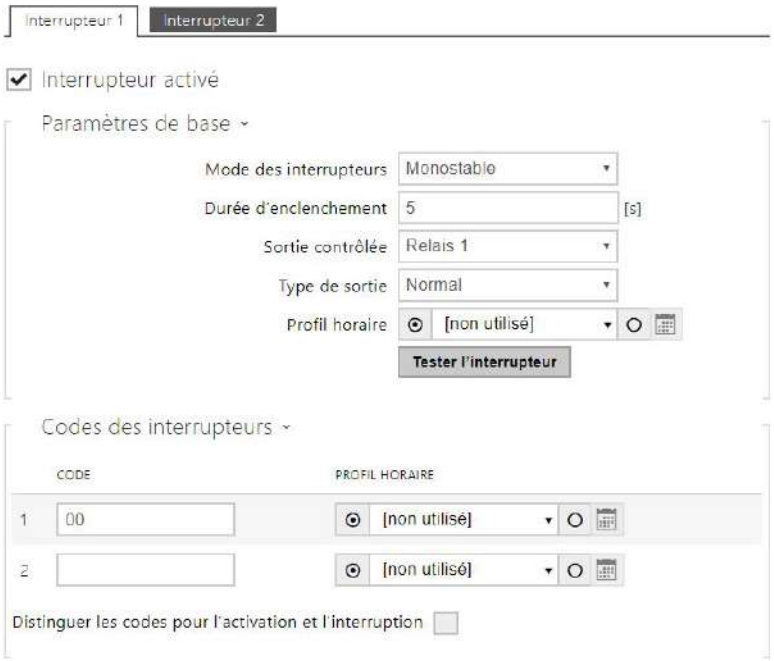
- Manuel d'installation: 2.3 Installation électrique

Chargement de firmware

Nous vous recommandons également de mettre à jour le firmware dès votre première connection à l'**appareil**. Référez vous à www.2n.cz 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

2N Unité d’aUnité d’accès près end en charge lend en charge les lliceprcencces sstandard qu qui fo fontt déjàéjà papartiee duu didispopositiftif. IIll s’ag’agit t dee la lla licenccence Enhanced Integration, Enhanced Security etet NFC. . La la liccencce NFC nee peut êtrepeut être utilisée que sutilisée que sur l’**Unl’itéé de cocontrôlrôleUn d'ad'accèès 2N2N** qui qui est équipést équipée d’u’un lectlecteurur de ccartes 13MHz13MHz.

LLe taablleauau cci-d-dessousssous dodonnee un apaperçuçu ddes lliccenccess ett de leurrs cacaractéactérisistiqques. – – FonctFonctioonnalnalitéé nativees.

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

⭐ – Fooncctionnalnalitéé sosous lics licence – In àà acheeterer sépaséparémémentcet

✗ – Indisponiblisponibless

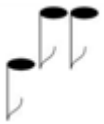
4. Signalisation du statut opérationnel

L' Unité de contrôle 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
	**Utilisateur activé** Cette tonalité signale la saisie du code d'activation de l'utilisateur. Le code d'activation est utilisé pour l'activation de l'utilisateur (position de l'utilisateur). Reportez-vous à la sous-section Utilisateurs pour connaître les paramètres du code d'activation.
	**Utilisateur désactivé** Cette tonalité signale la saisie du code de désactivation de l'utilisateur. Le code de désactivation est utilisé pour la désactivation de l'utilisateur (position de l'utilisateur). Reportez-vous à la sous-section Utilisateurs pour connaître les paramètres du code de désactivation.
	**Profil activé** Cette tonalité signale l'activation du profil. Cette fonction permet par exemple d'activer les alertes d'un groupe d'utilisateurs dans un bureau. Reportez-vous à la sous-section Profil pour les paramètres du code d'activation.
	**Profil désactivé** Cette tonalité signale la désactivation du profil. Reportez-vous à la sous-section Profil pour connaître les paramètres du code de désactivation.

	**Application Interne lancée** L'application interne est lancée à la mise sous tension ou au redémarrage de l'**Unité de contrôle d'accès 2N.** Un lancement réussi est signalé par cette combinaison de tonalités.
	**Connecté au LAN, Adresse IP attribuee** L'**Unité de contrôle d'accès 2N** 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'unité 2N.
	**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 à la sous-section *Configuration du périphérique* du Manuel d'installation de votre **Unité de contrôle d'accès 2N** 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 **Unité de contrôle d'accès 2N**. 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'**Unité de contrôle d'accès 2N** (référez vous au paramètre *Nom de l'appareil* dans l'onglet **Services / Serveur web**). Sélectionnez la langue de l'interface web avec les boutons **CZ, EN, DE, FR, IT, ES and RU**. Pressez le bouton Sortir dans le coin en haut à droite pour vous déconnecter.

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'**Unité de contrôle d'accès 2N** inclut 5 menus : **État, Répertoire, Hardware, Services** et **Système, lesquels** intègrent des sous menus comme indiqué ci dessous :

État

- **Appareil** – informations essentielles surl'**Unité de contrôle d'accès 2N**
- **Services** – informations sur les services actifs et leurs statuts
- **Licences** – etat actuel des licences et fonctionnalités disponibles sur l'**Unité de contrôle d'accès 2N**
- **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
- **Extensions** – paramètres des modules d'extension de l'unité 2N

Services

- **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

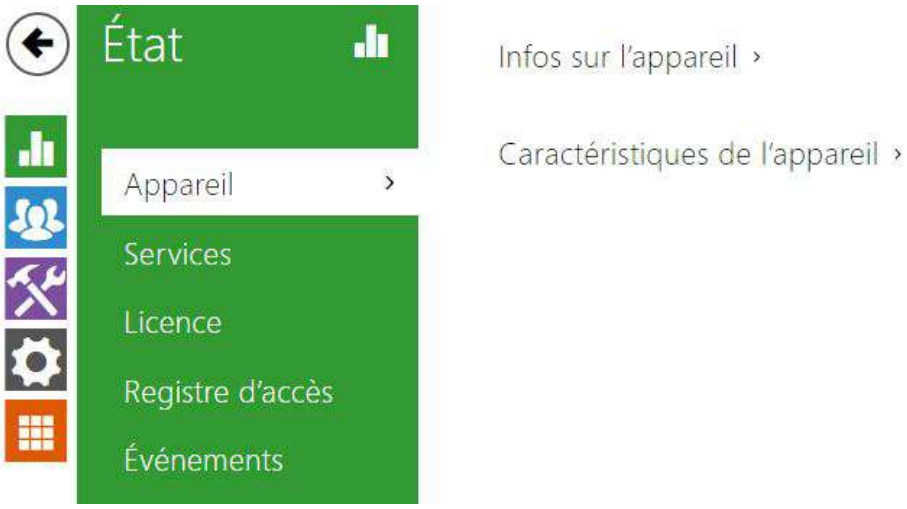
Système

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

Observation

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

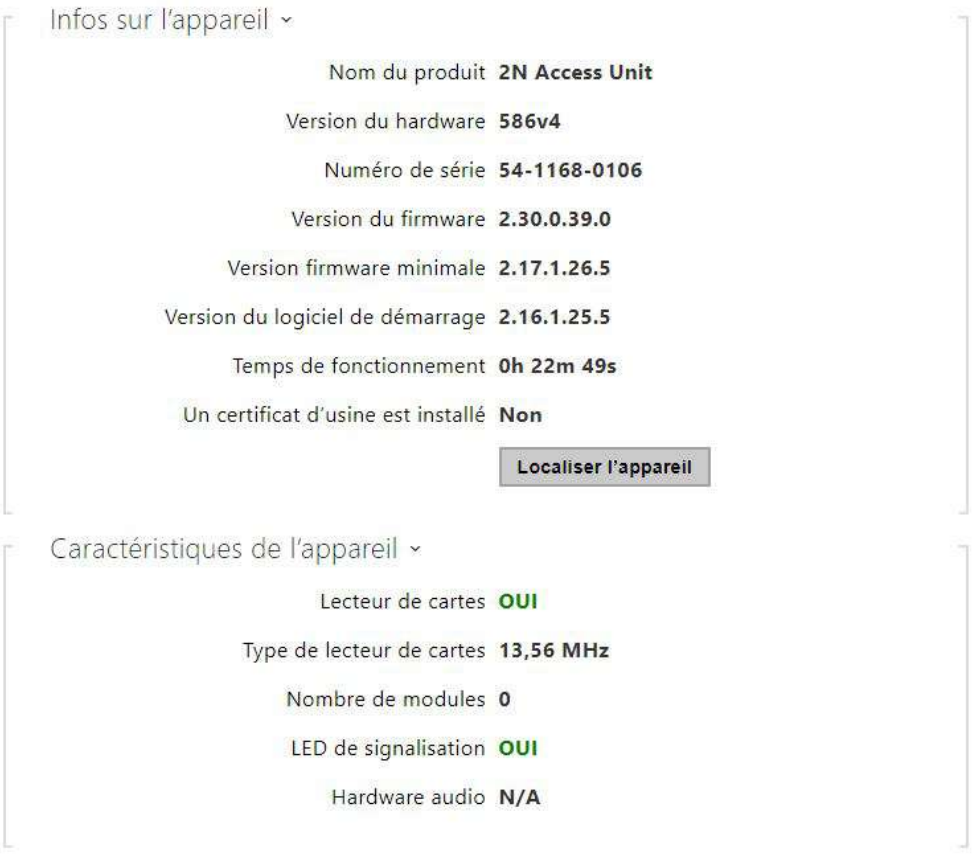
5.1 État



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

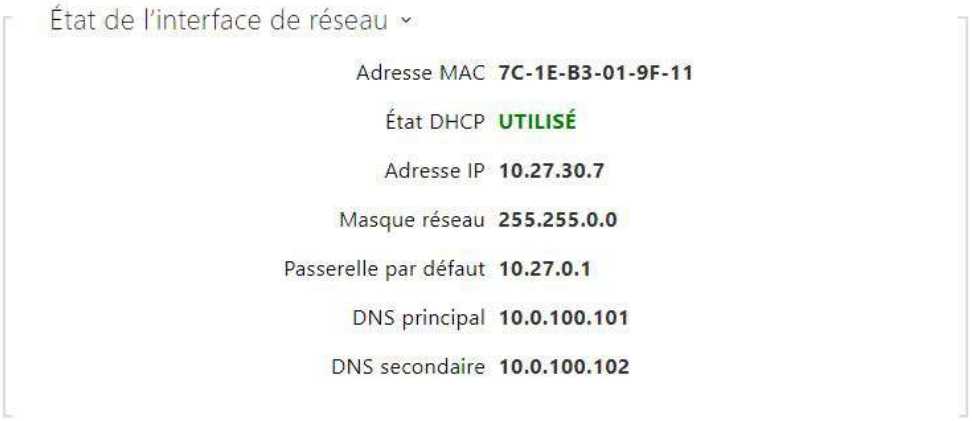
Appareil

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



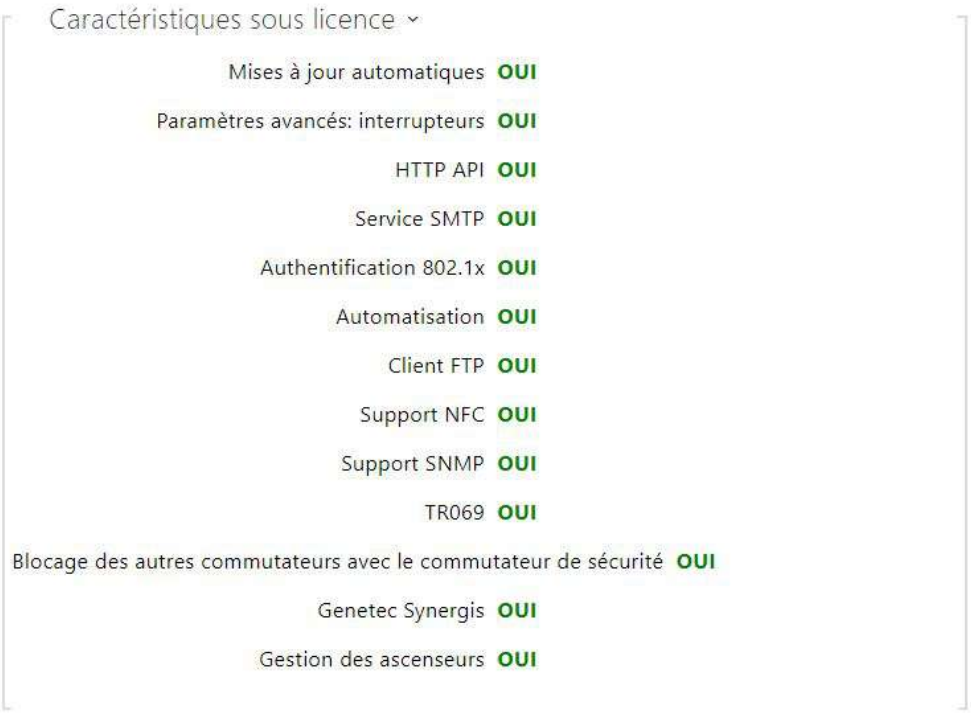
Services

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



Licence

L'onglet **Licences** affiche la liste des fonctionnalités sous licence de **l'unité de contrôle d'accès 2N**, y compris leur disponibilité actuelle (sur la base d'une clé de licence valide entrée dans le menu principal **Système / Licence**).



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.

[Filtrer les événements]

HEURE	TYPE D'ÉVÉNEMENT	DESCRIPTION
30 Apr 9:12:36	**OutputChanged**	port=**led_secured**, state=**false**
30 Apr 9:12:35	**InputChanged**	port=**tamper**, state=**false**
30 Apr 9:12:35	**OutputChanged**	port=**led_secured**, state=**true**
30 Apr 9:12:35	**DeviceState**	state=**startup**
30 Apr 9:12:35	**LiftStatusChanged**	module=**4**, ready=**false**
30 Apr 9:12:35	**LiftStatusChanged**	module=**3**, ready=**false**
30 Apr 9:12:35	**LiftStatusChanged**	module=**2**, ready=**false**
30 Apr 9:12:35	**LiftStatusChanged**	module=**1**, ready=**false**
30 Apr 9:12:35	**LiftStatusChanged**	module=**0**, ready=**false**

- – 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.
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.

Evénements	Signification
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'interphone. Il contient des informations utilisateurs utiles pour des fonctionnalités de l'unité telles que la numérotation rapide, le déverrouillage des portes par carte RFID / code, les e-mails d'appels manqués…etc.

La liste d'Utilisateurs contient jusqu'à 10 000 utilisateurs - 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'unité 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'unité : 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.

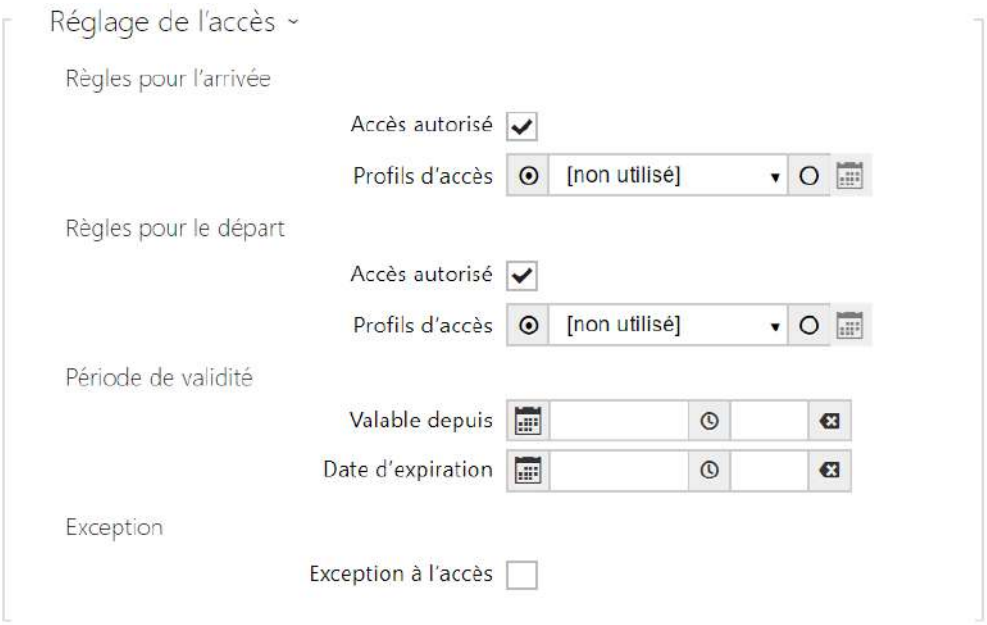
Toutes les cartes badgées sur le lecteur ou via l'interface Wiegand sont enregistrées. Reportez-vous au menu **Etat / Registre** d'accès pour retrouver les 10 dernières cartes badgées qui comprend l'ID, le type de carte, l'heure de passage de la carte et d'autres informations si nécessaire. Sur les petites 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'unité.

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

La fonction Recherche dans le répertoire fonctionne en texte intégral par noms d'utilisateur, numéros de téléphone et adresses électroniques. Elle recherchera toute correspondance dans le répertoire. Cliquez sur pour créer un nouvel utilisateur et 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.

Les informations des fiches utilisateurs sont les suivantes :

- **Nom** – paramètre obligatoire pour identifier un utilisateur.
- **E-mail** – adresse électronique de l'utilisateur pour l'envoi des informations sur les appels manqués. Vous pouvez entrer plusieurs adresses électroniques séparées par des virgules.



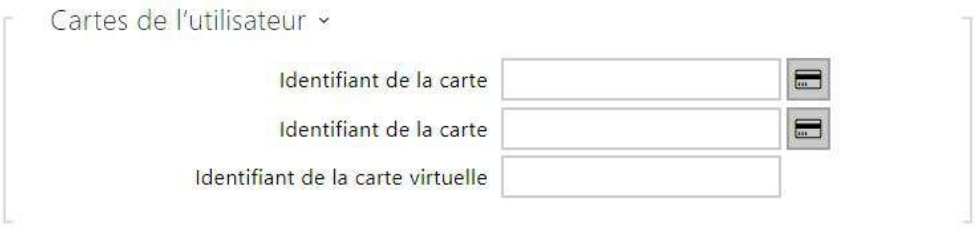
- **Règles pour l'arrivée**
  - **Accès autorisé** – il autorise l'authentification à ce point d'accès.
  - **Profils d'accès** – sélectionnez l'un des profils prédéfinis dans la section Répertoire / Profils horaires ou bien définissez le profil temporel manuellement
- **Règles pour le départ**
  - **Accès 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.
- **Période de validité**
  - **Date du début de validité** – paramétrez la date et l'heure du début de validité.
  - **Date d'expiration** – paramétrez la date et l'heure de fin de validité.
- **Exception à l'accès** – définit une exception pour l'utilisateur donné de la fonction de blocage d'accès et anti-passback.

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'interphone, le pictogramme apparaitra sur les codes en conflit.

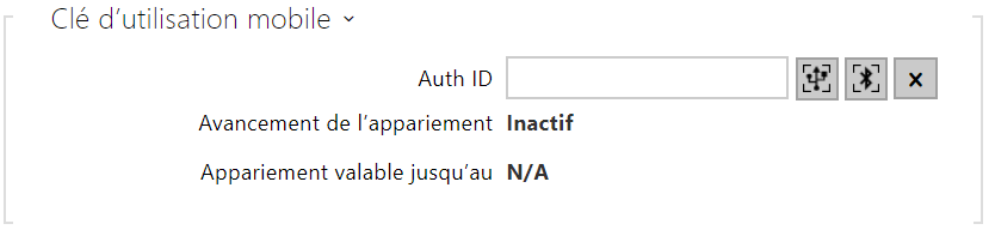
Code PIN – définissez le numéro d'identification personnel de l'utilisateur. Le code doit contenir au moins deux caractères.

Interrupteur 1-2 – 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'interphone et au moins un caractère pour déverrouiller la porte en utilisant DTMF du téléphone.



Chacun des utilisateurs de l'interphone 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. Une fois l'utilisateur authentifié via le lecteur Bluetooth / biométrique, l'identifiant de la carte virtuelle est envoyé vers un appareil tiers intégré à l'interphone IP 2N via Wiegand.

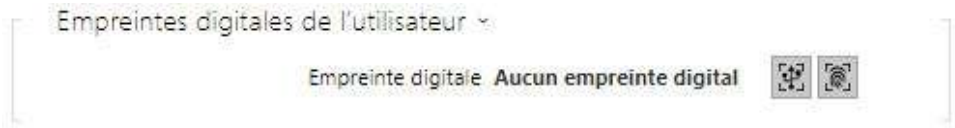


- **Authentification ID** – définissez un identifiant unique d'appareil mobile / d'utilisateur. La valeur du paramètre est automatiquement générée pour le jumelage. Vous pouvez déplacer l'ID d'authentification vers un autre utilisateur ou le copier sur un autre appareil au même emplacement.
  -  jumelage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

Jumelage via le module Bluetooth de l'Interphone

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..

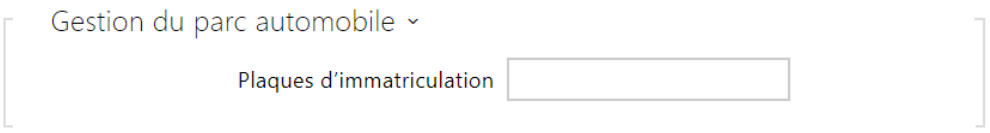


- **Empreintes digitales** – affiche le nombre d'empreintes digitales définies ; Vous pouvez définir jusqu'à 2 empreintes digitales différentes par utilisateur. Cette section ne s'affiche que si le module lecteur biométrique est disponible.
  -  enrôlement via lecteur USB
  -  enrôlement via le lecteur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



2N Access Unit 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).

La fonction peut être désactivée ou sélectionner l'ouverture lorsque la plaque d'immatriculation du véhicule détectée est attribuée à un utilisateur qui dispose réellement de droits d'accès valides (paramètres : ***Règles d'arrivée, règles de départ, période de validité*** dans la section 5.3.2 Dveře).

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.

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**.

La porte sera ouverte si la plaque d'immatriculation enregistrée dans l'annuaire correspond à un droit réel d'entrée ou de sortie. 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.

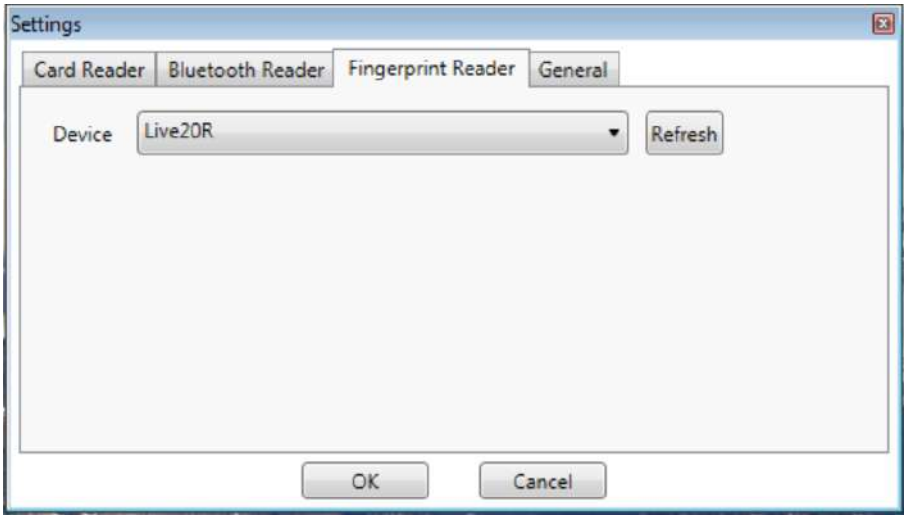
- **Étages** – sélectionnez les étages accessibles par l'utilisateur dans le cas d'un Contrôle d'accès dans l'ascenseur.
- **Profil horaire** – sélectionnez un ou plusieurs profils horaires à appliquer. Définissez les profils horaires dans la section **Répertoire / Profils horaires**.
  -  marquer la 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.

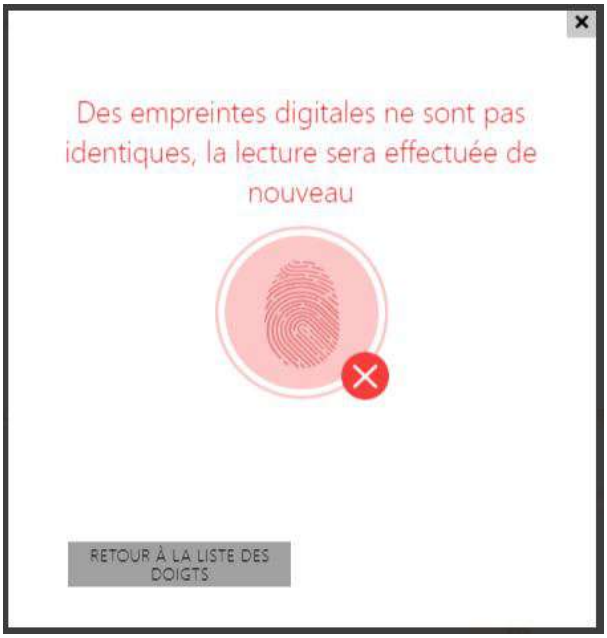


2) Cliquez sur l'un de ces deux boutons pour enregistrer une empreinte.

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.

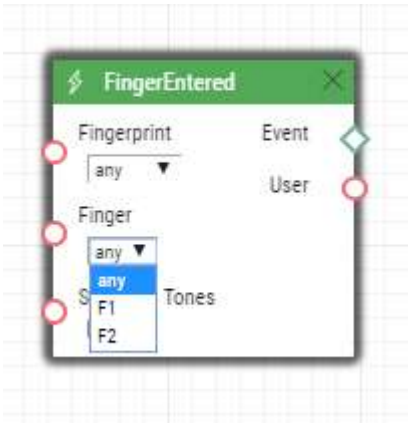
Répétez le processus si une incohérence se produit pendant la lecture des empreintes digitales.



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

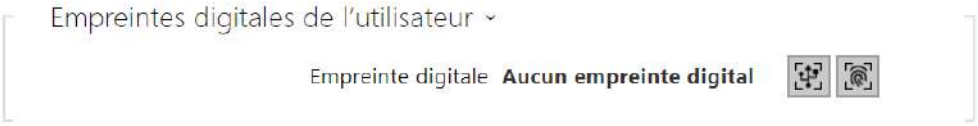
Pour définir la fonction de l'empreinte digitale, cliquez sur l'icone :

- 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.

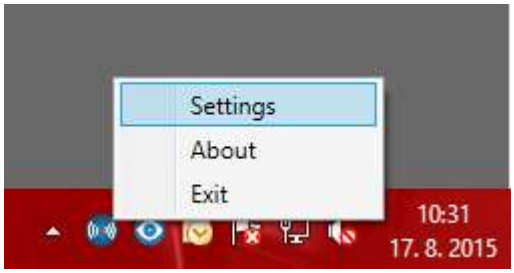
6) Vous pouvez vérifier les paramètres dans la fiche utilisateur.



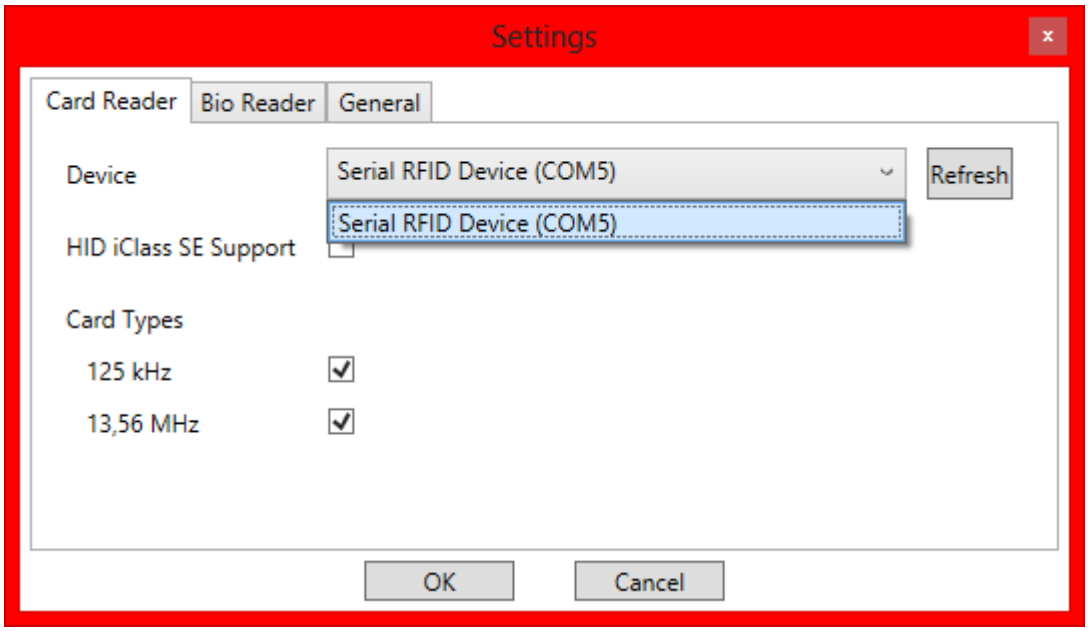
5.2.1.2 Lecteur de carte RFID USB

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

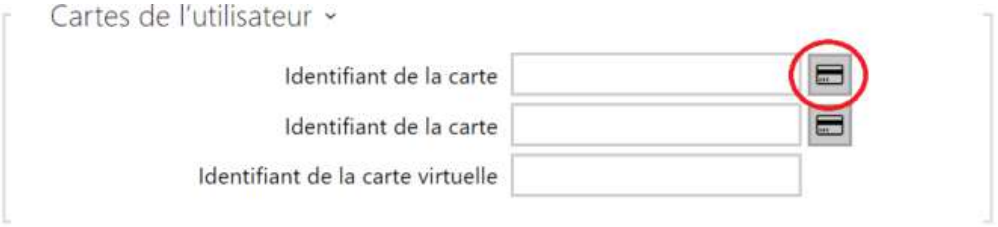
- Rendez vous dans **2N IPUSB Driver**



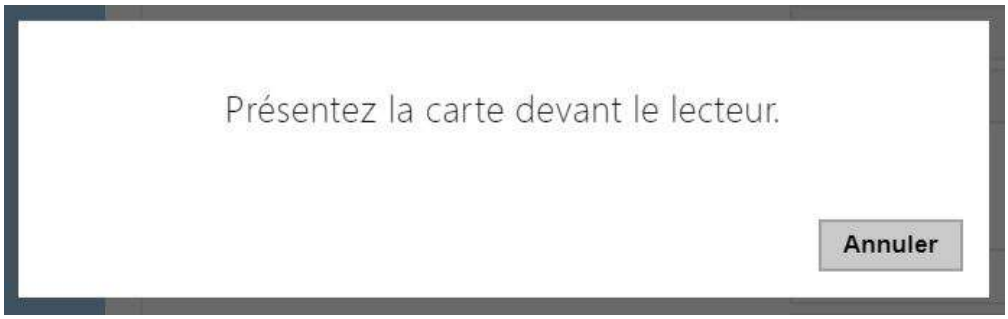
- Configurez le port COM pour le lecteur connecté.



- Pressez le bouton Lecture via l'interface web de **l'unité de contrôle d'accès 2N**.



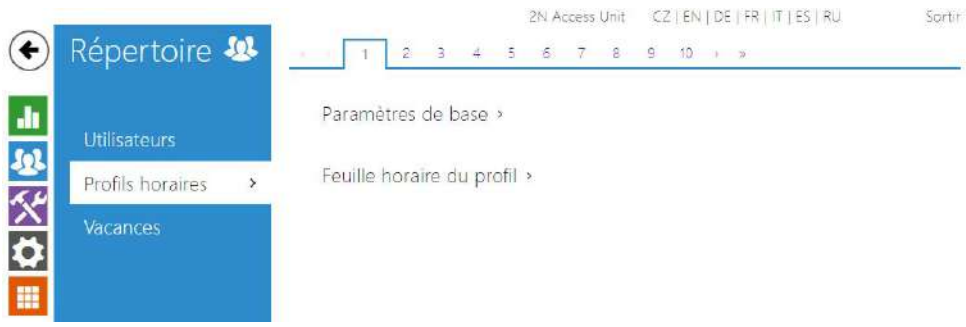
- Badgez la carte sur le lecteur.



- 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

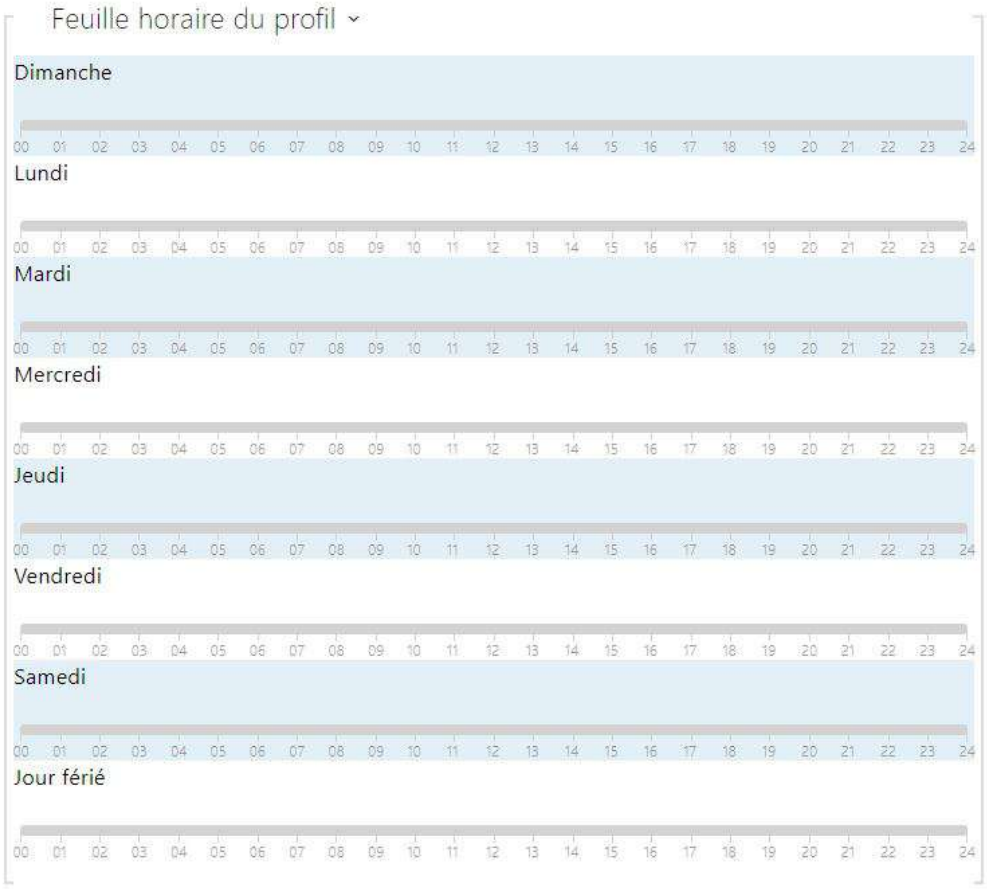
Chaque profil horaire définit la disponibilité de la fonction via un calendrier hebdomadaire. Il suffit de définir De–À et de spécifier les jours de la semaine pour la disponibilité. Les **unités de contrôle d'accès 2N** vous permettent de définir jusqu'à 20 profils horaires pouvant être affectés aux 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** – entrez un nom de profil. Ce paramètre est facultatif et vous aide à rechercher des éléments dans la liste des profils horaires et à sélectionner plus facilement des profils dans les paramètres d'interrupteur, de carte et de numéro de téléphone.



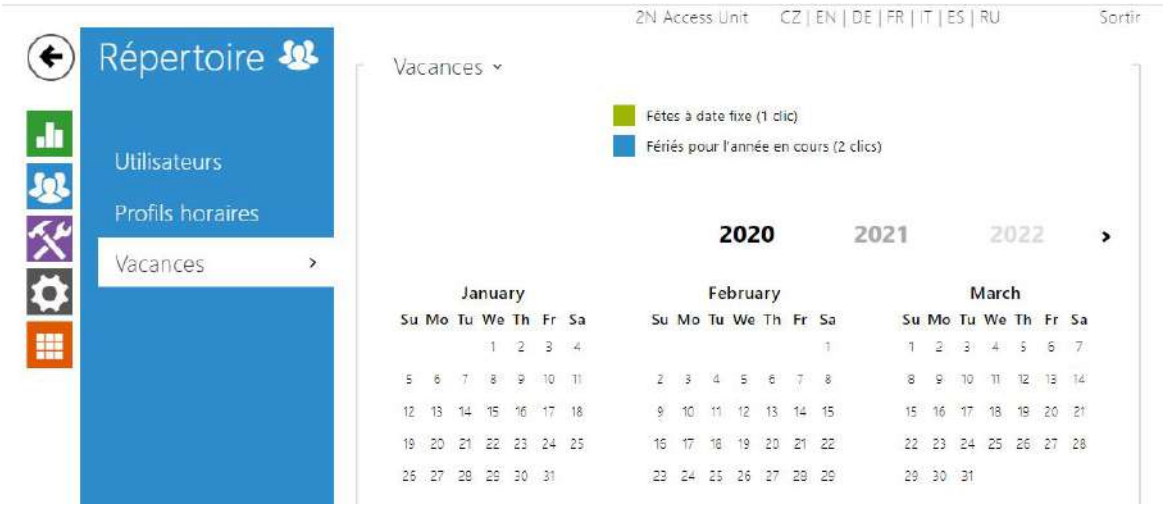
Définissez le profil de temps actif dans une semaine. Un profil est actif lorsque l'heure actuelle tombe dans les intervalles définis.
Si un jour est marqué comme jour férié (voir **Répertoire** → **Vacances**), la dernière ligne du tableau (vacances) est appliquée quel que soit le jour de la semaine.

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

Note

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

5.2.3 Vacances



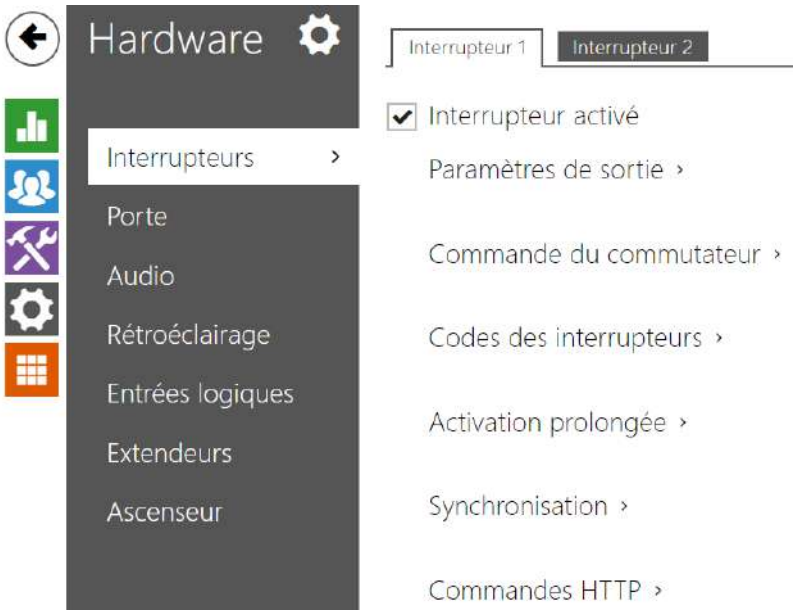
Ici, vous pouvez sélectionner les jours fériés (y compris le dimanche). Vous pouvez leur attribuer des intervalles de temps différents de ceux des jours ouvrables dans les profils horaires.

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

5.3 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 à l'unité 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 de **l'unité 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 :

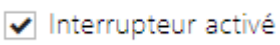
- activer n'importe quelle sortie de **l’unité de contrôle d’accès 2N** (Relais, Sortie active)
- activer la sortie qui contrôle le **Relais de sécurité de l’unité de contrôle d’accès 2N**
- envoyer une commande HTTP vers un autre appareil

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 **d’unité 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.

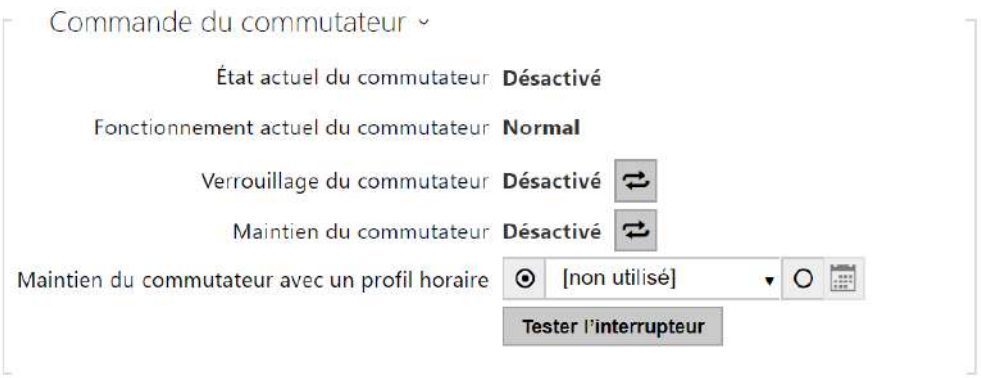
- **Interrupteur activé** – activez / désactivez l'interrupteur de manière général. Lorsqu'il est désactivé, l'interrupteur ne peut être activé par aucun des codes disponibles (y compris les codes des utilisateurs), appel ou bouton de numérotation rapide.
- **Modes des interrupteurs** – paramétrez le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

Note

- *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 Interkom, 2N Access Unit) se trouve à un endroit (coque du bâtiment) où il existe un risque d'intrusion dans l'établissement, il est fortement recommandé d'utiliser le Relais de sécurité 2N (Part No. 9159010) pour sécuriser l'installation au maximum.



- **État actuel du commutateur** – affiche l'état actuel du commutateur (activé ou désactivé).
- **Fonctionnement actuel du commutateur** – Affiche le fonctionnement actuel du commutateur.
  - **Normal** : le commutateur n'est pas verrouillé ni maintenu.
  - **Maintenu** : le commutateur est maintenu mais pas verrouillé.
  - **Verrouillé** : le commutateur est verrouillé (dans ce cas, le verrouillage prime sur le maintien).
- **Verrouillage du commutateur** – activé : le commutateur est en permanence en position 0 et ne peut pas être commandé tant qu'il n'est pas déverrouillé. Désactivé : le commutateur n'est pas verrouillé.
- **Maintien du commutateur** – activé : le commutateur est en permanence en position 0 et ne peut pas être commandé tant qu'il n'est pas déverrouillé. Désactivé : le commutateur n'est pas verrouillé.
- **Maintien du commutateur avec un profil horaire** – permet d'attribuer un profil horaire prédéfini à l'interrupteur ou de définir manuellement un profil horaire permettant à l'interrupteur de se fermer. Si le profil horaire attribué n'est pas actif, il est alors possible d'activer le commutateur en apposant une carte RFID valide, en passant un appel, en entrant un code ou en utilisant le bouton de numérotation rapide.
- **Bouton "Tester l'interrupteur"** – activez l'interrupteur manuellement pour tester son bon fonctionnement. Ex : activation d'une serrure électrique ou d'un autre appareil connecté.

Observation

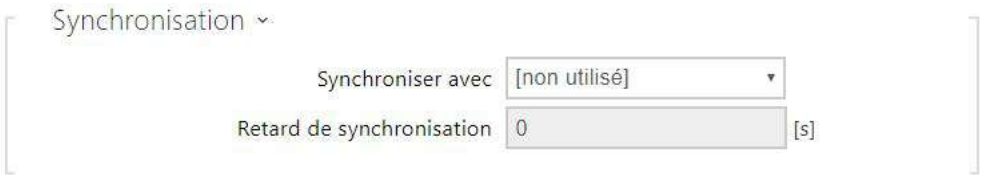
- Si l'interrupteur est verrouillé et que l'équipement est éteint puis rallumé, l'interrupteur restera verrouillé après la mise sous tension de l'équipement. L'interrupteur se comporte de la même manière s'il est désactivé puis activé.
- Si l'interrupteur est enclenché et que l'équipement est éteint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

Le tableau ci-dessus comprend une liste de codes universels qui vous permettent d'activer les interrupteurs à partir du clavier **de l'unité 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.

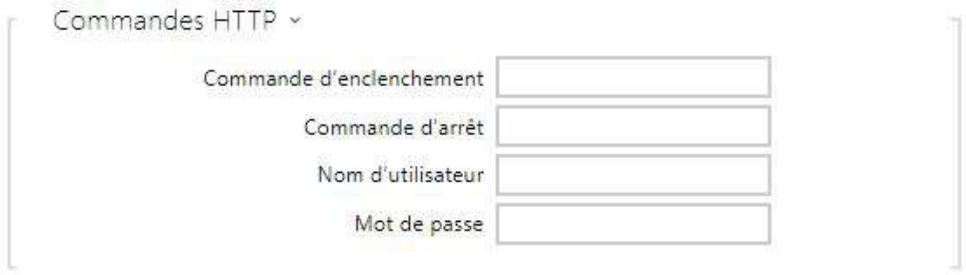
Profil horaire – attribuez un profil temporel au code de l'interrupteur pour contrôler sa validité.

Distinguer les codes pour l'activation et l'interruption – définissez un mode de code d'interrupteur dans lequel les codes impairs (1, 3 ….) sont utilisés pour l'activation de l'interrupteur et les codes pairs (2, 4 …) servent à la désactivation de l'interrupteur. Ce mode ne peut être utilisé que si l'interrupteur est réglé sur le mode bistable.



Synchroniser avec – paramétrez la synchronisation de l'interrupteur pour activer automatiquement un autre interrupteur après un délai prédéfini. Déterminez le délai dans le paramètre de **Délai de synchronisation**.

Délai de synchronisation – définissz l'intervalle de temps entre l'activations synchronisées de deux interrupteurs. Le paramètre ne sera pas appliqué si la fonction **Synchroniser** avec est désactivée.



Commande d'enclenchement – paramétrez la commande http à envoyer vers un dispositif tiers (Web Relais, Haut-parleur SIP 2N, autres Interphones...etc.) lors de l'activation de l'interrupteur. La commande est envoyée via HTTP (demande GET). La commande doit être sous ce format http://ip_adresse/chemin. Par exemple http://192.168.1.50/relay1=on.

Commande d'arrêt – paramétrez la commande http à envoyer vers un dispositif tiers (Web Relais, Haut-parleur SIP 2N, autres Interphones...etc.) lors de la désactivation de l'interrupteur. La commande est envoyée via HTTP (demande GET). La commande doit être sous ce format : http://ip_adresse/chemin. Par exemple http://192.168.1.50/relay1=off.

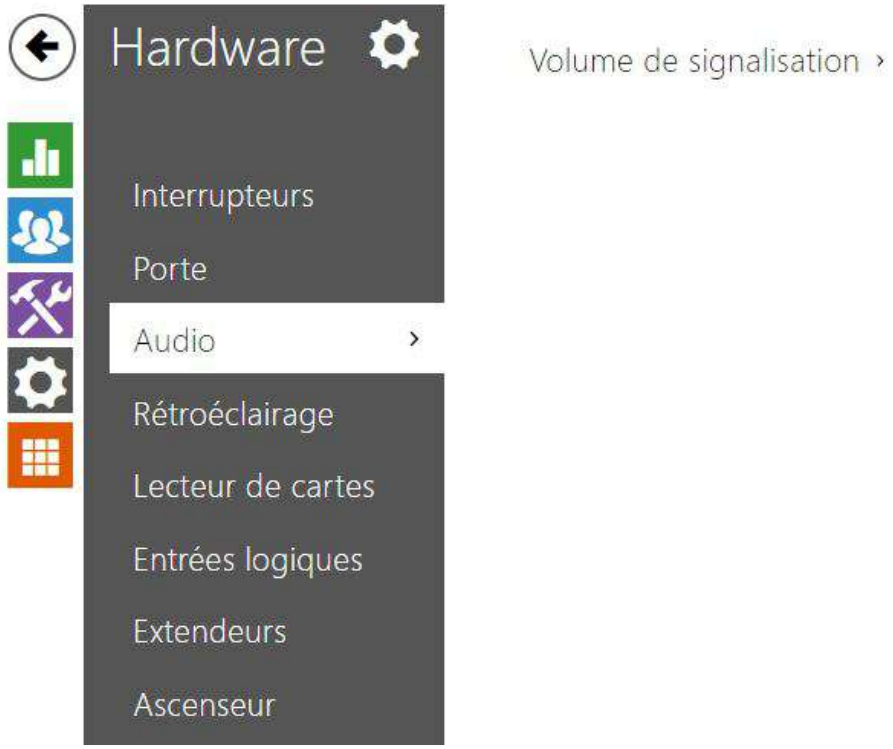
Nom d'utilisateur – saisissez le nom d'utilisateur pour l'authentification du dispositif externe (relais WEB, par exemple). Ce paramètre est uniquement obligatoire si le dispositif externe nécessite une authentification.

Mot de passe – saisissez le mot de passe d'authentification du dispositif externe (relais WEB, par exemple). Ce paramètre est uniquement obligatoire si le dispositif externe nécessite une authentification.

Conseil

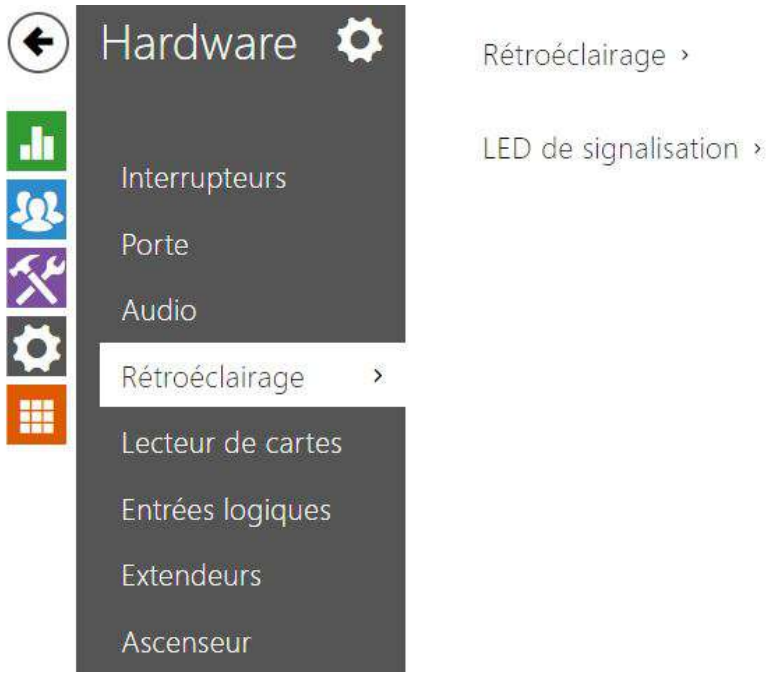
Avec le relais IP déporté 2N, **référence : 9137410E**, les commandes suivantes sont utilisées :
Activer l'interrupteur – http://ip_address/state.xml?relayState=1 (e.g.: http://192.168.1.10/state.xml?relayState=1)
Pour activer l'interrupteur pendant une durée prédéfinie (la valeur par défaut est 1,5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

5.3.3 Audio



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

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.

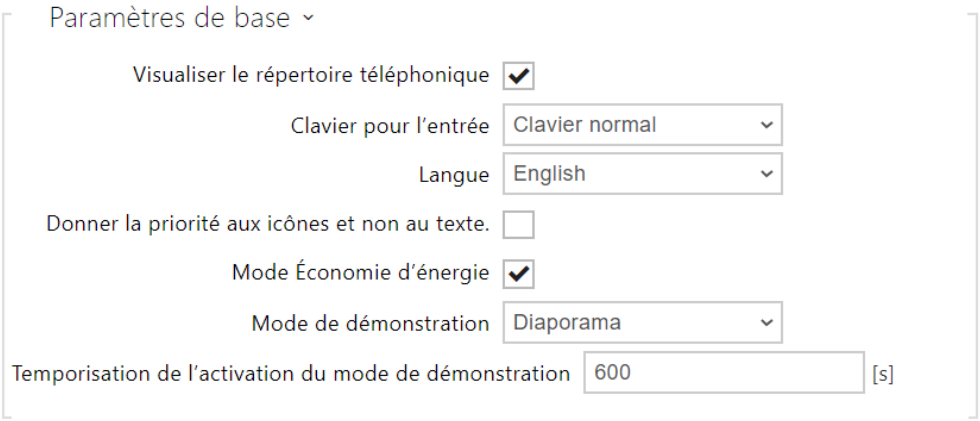
Note

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

5.3.5 Ecran

Les systèmes d'accès **2N Access Unit verze 2.0** 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.

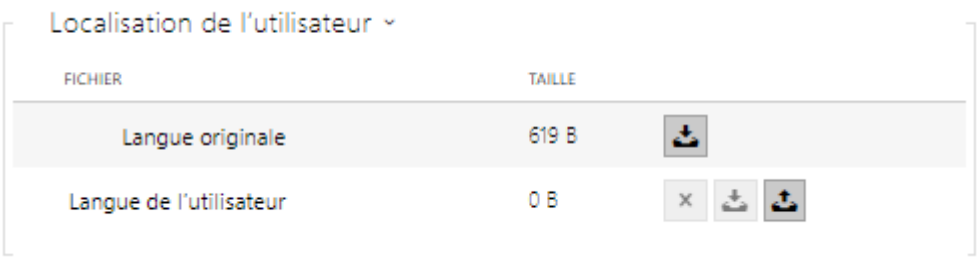
Ecran



- **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 sept langues prédéfinies: **Anglais**, **Espagnol**, **Allemand**, **Français**, **Russe**, **Italien** et **Tchèque**.
- **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'interphone ou tout événement d'affichage (tel que l'activation du verrouillage de la porte ou le toucher de l'écran) rétablit toute la luminosité de l'écran.
- **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.



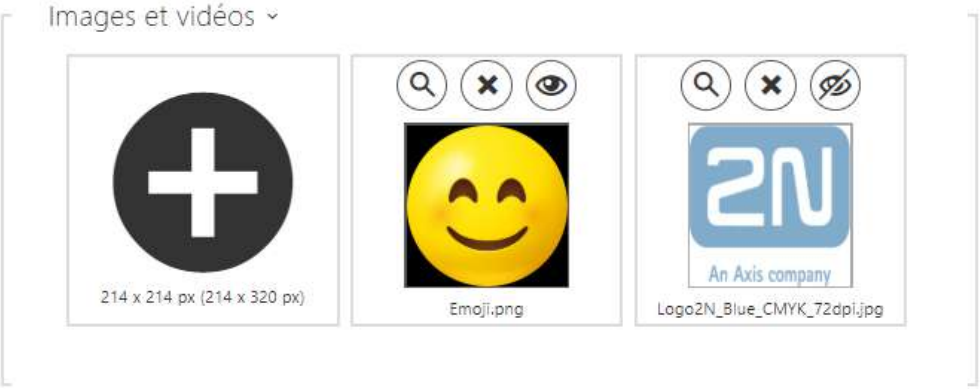
- **Langue originale** – téléchargez le modèle de fichier de localisation pour sa traduction. C'est un fichier XML avec tous les textes à afficher.
- **Langue de l'utilisateur** – enregistrez, supprimez et chargez un fichier de localisation de votre choix.

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

Diaporama

Cet onglet vous aide à configurer une liste d'images à afficher en mode Diaporama. 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.

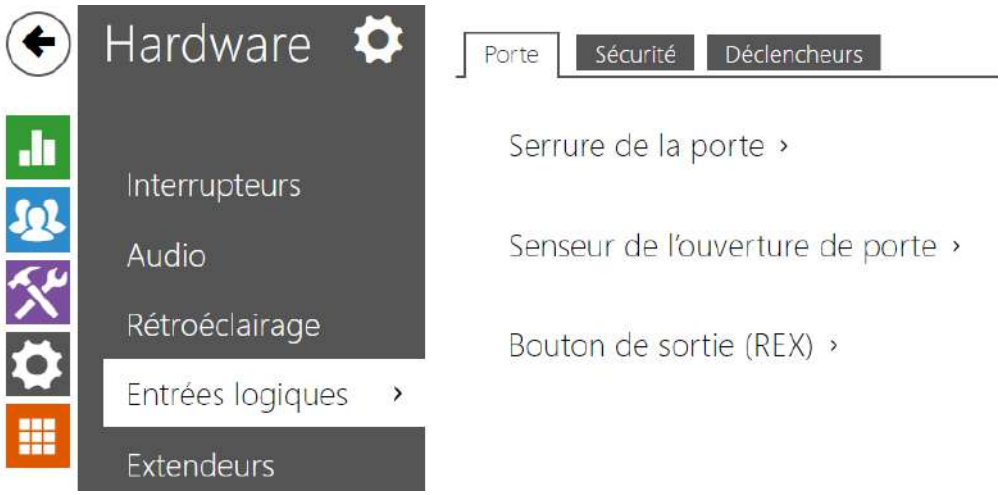
Si aucune image n'est chargée, le mode Diaporama ne sera jamais activé.

Tip

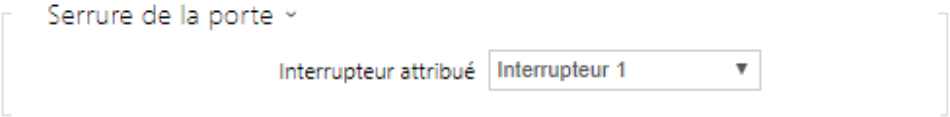
- Pour cacher le texte “Toucher pour démarrer” sur l'écran, chargez une image de résolution 214 x 320 pixels.

5.3.7 Entrées logiques

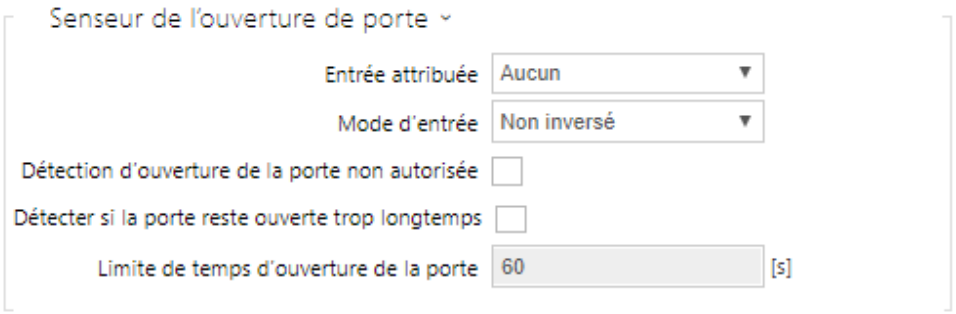
Dans cette section de configuration, définissez les paramètres associés aux entrées logiques et leurs interconnexions avec d'autres fonctionnalités de l'interphone.



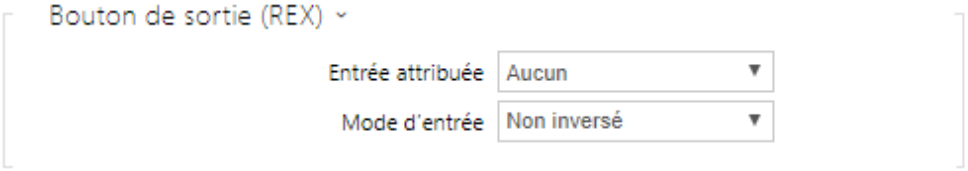
Porte



- **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).

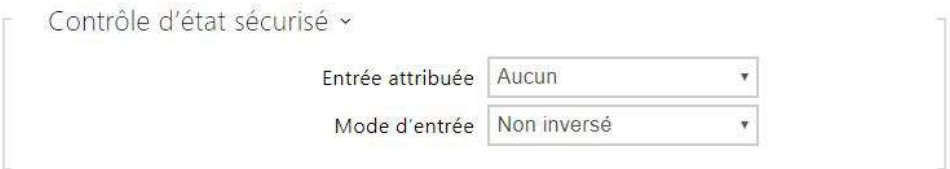


- **Entrée attribuée** – permet de sélectionner une des entrées logiques (éventuellement aucune entrée) pour la détection de portes ouvertes.
- **Mode d'entrée** – permet de régler le statut (la polarité) de l'entrée. Inversé ou Non inversé.
- **Détection d'ouverture de la porte non autorisée** – détecter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

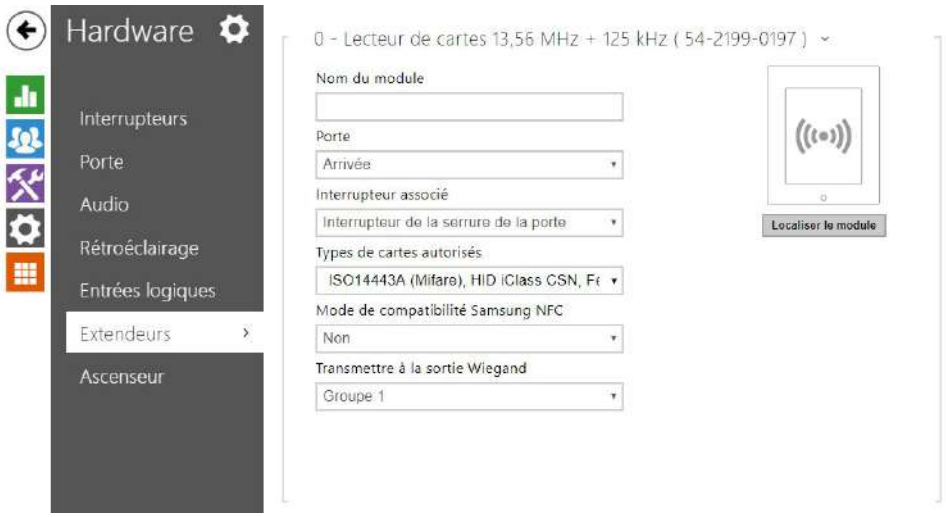
Note

- Depuis les PCB en version 599v2 et plus, tous les modèles 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



L'unité de contrôle d'accès 2N peuvent être étendus grâce à des modules dits d'extension connectés à l'unité d'interphonie de base via le bus VBUS. Les modules suivants sont disponibles :

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

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

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.

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>.

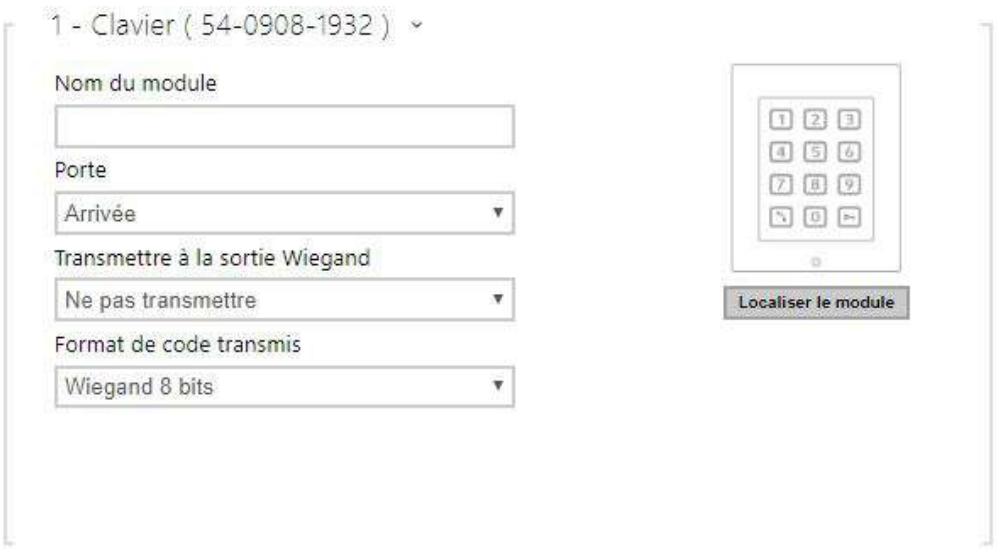
Conseil

- 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 Boutons

- **Fonctions des boutons** – numérotez les fonctions d'automatisation voulues en pressant les boutons.

Configuration du Module Clavier



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

Configuration Module Info

- Aucun paramétrage n'est nécessaire sur ce module

Configuration Module Lecteur de cartes 125 kHz

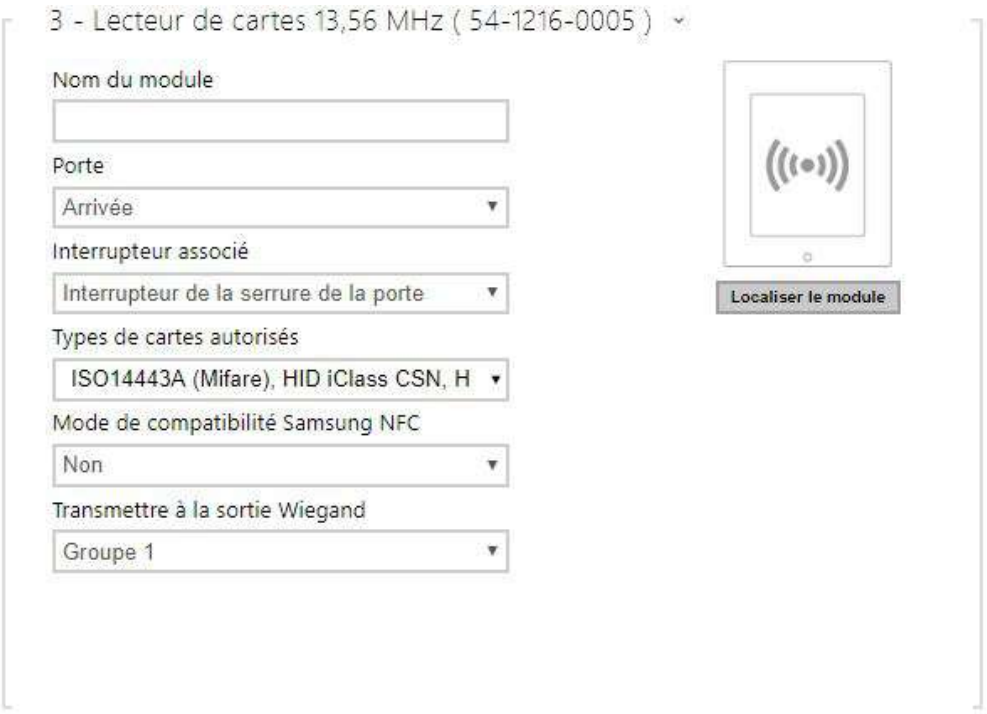
- **Nom du module** – définissez le nom du module pour le journal d'accès.
- **Porte** – définissez la direction du lecteur (entrée ou sortie) pour le système de présence.
- **Interrupteur associé** – réglez l'interrupteur pour qu'il soit activé après l'authentification de l'utilisateur via ce module. Si vous définissez l'interrupteur de verrouillage de porte et les règles d'authentification spécifiées dans Hardware / Porte.
- **Types de cartes autorisés** – définissez le type de carte pouvant être lu par le lecteur. Le lecteur de carte ne prend en charge qu'un seul type de carte à la fois.

- **Transmettre à la sortie Wiegand** – définissez un groupe de sorties Wiegand auxquelles tous les ID de cartes RFID reçus seront renvoyés.

Conseil

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

Configuration Module Lecteur de cartes 13,56 MHz



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

Conseil

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

Configuration Module Bluetooth

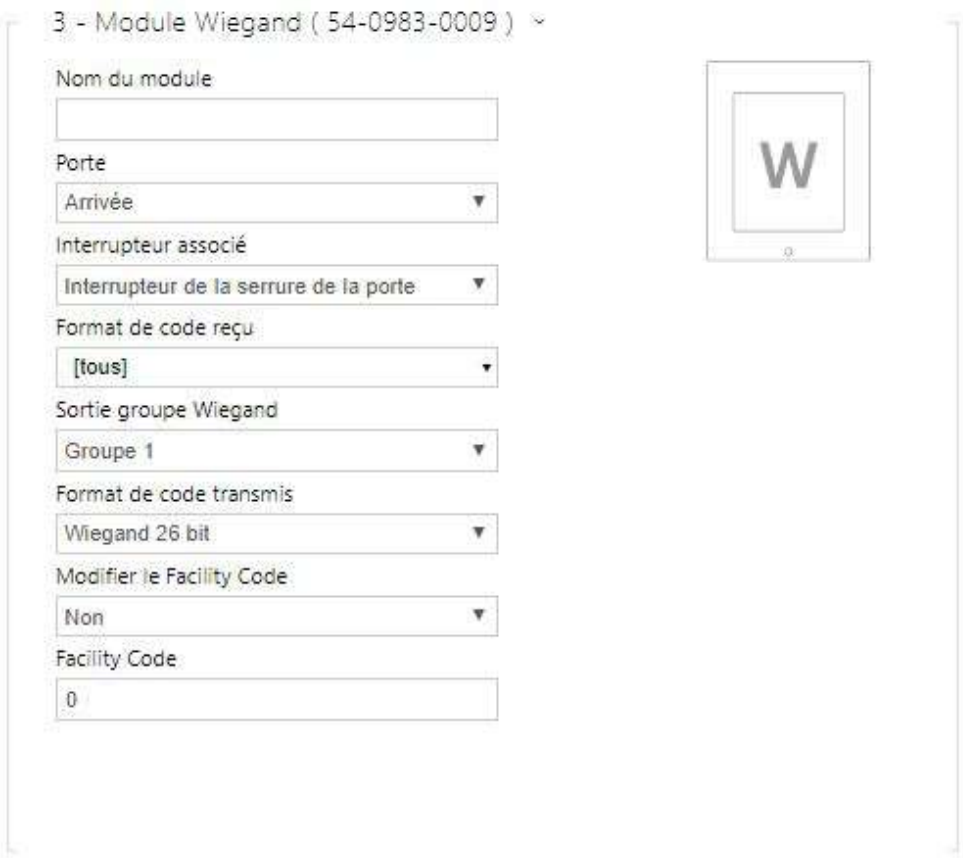
- **Nom du module** – définissez le nom du module pour le journal d'accès. Le nom du module est utilisé lors de l'enregistrement des événements du module Bluetooth.
- **Porte** – définissez la direction du lecteur (entrée ou sortie) pour le système de présence.
- **Interrupteur associé** – réglez l'interrupteur pour qu'il soit activé après l'authentification de l'utilisateur via ce module. Si vous définissez l'interrupteur de verrouillage de porte et les règles d'authentification spécifiées dans Hardware / Porte.
- **Portée du signal** – 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'interphone au système de Contrôle d'accès de votre bâtiment, par exemple (pour envoyer des identifiants de cartes RFID ou des codes reçus sur n'importe quelle entrée Wiegand). Le **2N® Wiegand Isolator** est également équipé d'une entrée logique et d'une sortie logique, contrôlables via l'interface d'automatisation.



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

Configuration OSDP

- **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.

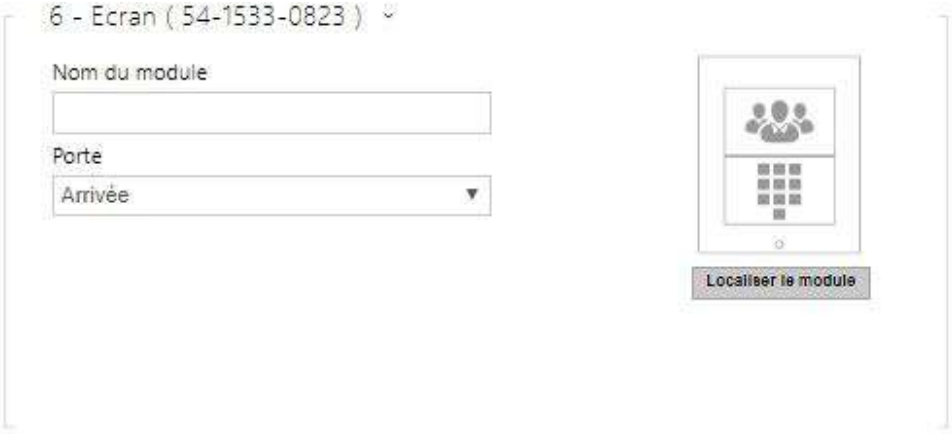
Observation

- 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'interphone. La valeur par défaut est 0,25 W dans des circonstances normales.

Configuration Module Ecran tactile

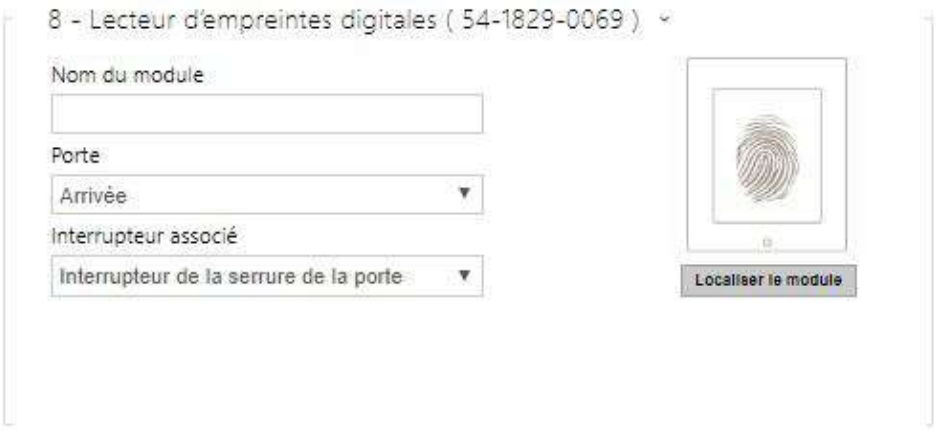


- **Nom du module** – définissez le nom du module pour le journal d'évènements.
- **Porte** – définissez la direction de l'écran (entrée ou sortie) pour le système de présence.

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.

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'interphone. Une fois qu'un lecteur d'empreintes digitales est reconnecté, les empreintes digitales de l'utilisateur seront à nouveau affichées.

Configuration Module Clavier capacitif

- **Nom du module** – définissez le nom du module pour 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)

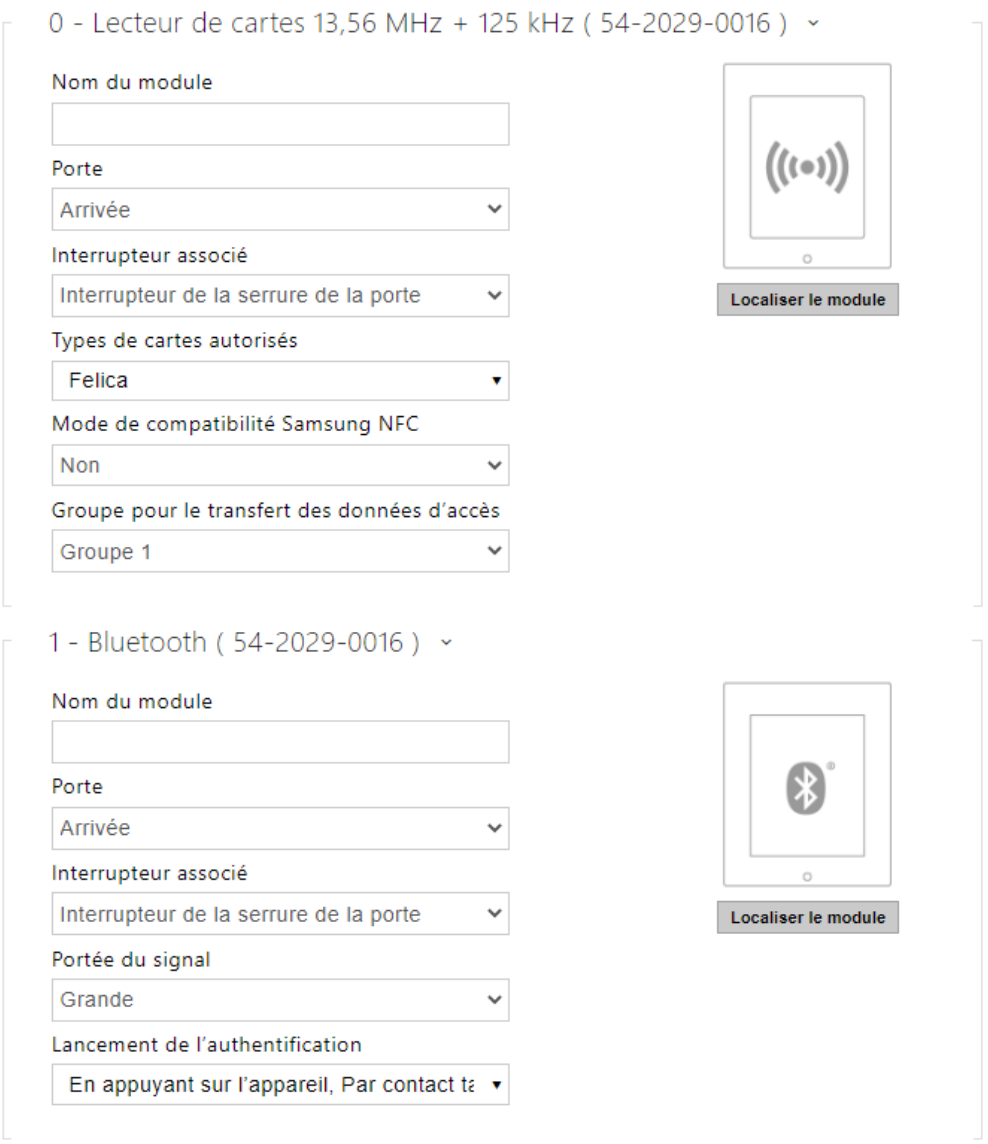
- **Nom du module** – définissez le nom du module pour le journal d'accès.
- **Porte** – définissez la direction du lecteur (entrée ou sortie) pour le système de présence.

- **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)

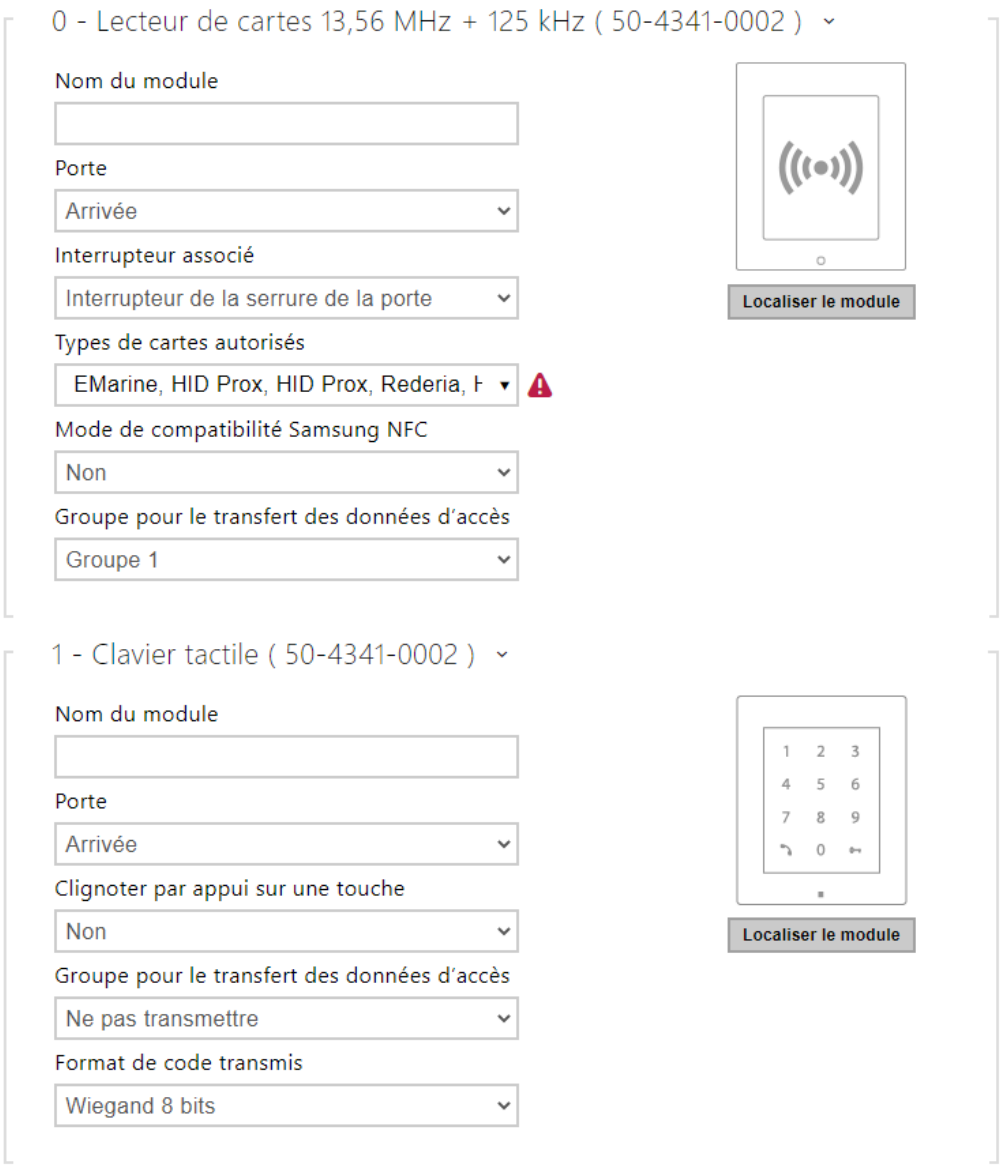
- **Nom du module** – définissez le nom du module pour le journal d'accès.
- **Porte** – définissez la direction du lecteur (entrée ou sortie) pour le système de présence.
- **Interrupteur associé** – réglez l'interrupteur pour qu'il soit activé après l'authentification de l'utilisateur via ce module. 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.

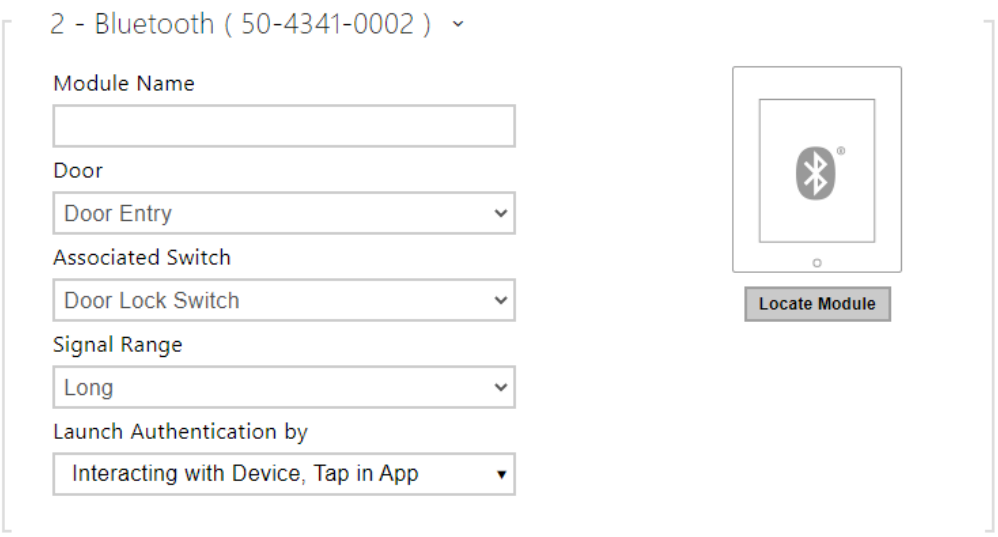
- **Transmettre à la sortie Wiegand** – définissez un groupe de sorties Wiegand auxquelles tous les ID de cartes RFID reçus seront renvoyés.

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)

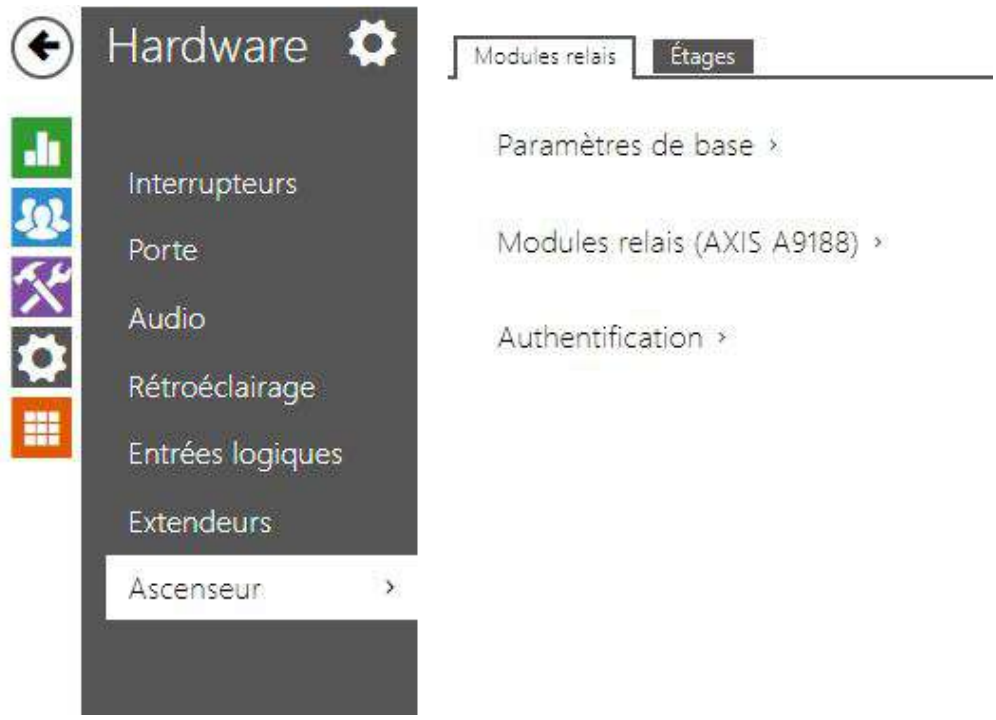
- **Nom du module** – définissez le nom du module pour le journal d'accès.
- **Porte** – définissez la direction du lecteur (entrée ou sortie) pour le système de présence.
- **Clignotement par pression sur les boutons** – activez la signalisation sur le clavier pour les environnements bruyants où les 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

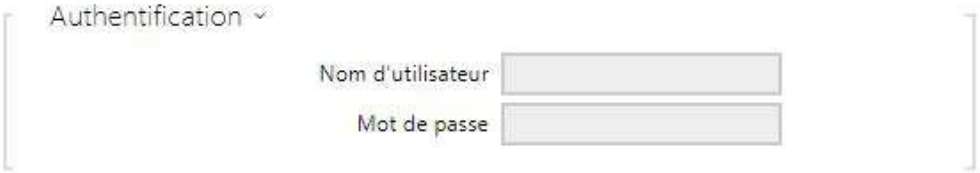


Afin de pouvoir contrôler l'accès aux étages par l'ascenseur, connectez le module relais AXIS A9188 à l'**unité de contrôle d'accès 2N**. Jusqu'à 5 modules relais peuvent être connectés à une **unité de contrôle d'accès 2N**, chacun pouvant contrôler jusqu'à 8 étages, soit un total de 64.

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

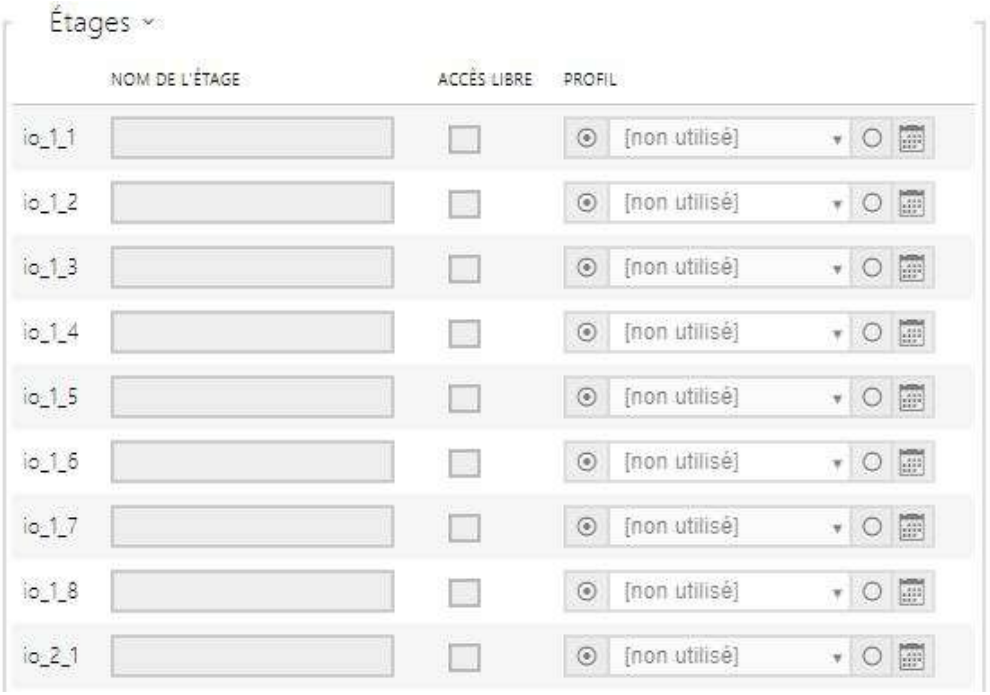


- **Nom d'utilisateur** – authentification du périphérique externe. Ce paramètre n'est obligatoire que si le périphérique externe requiert une authentification.
- **Mot de passe** – entrez le mot de passe d'authentification du périphérique externe (relais WEB, par exemple). Ce paramètre n'est obligatoire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

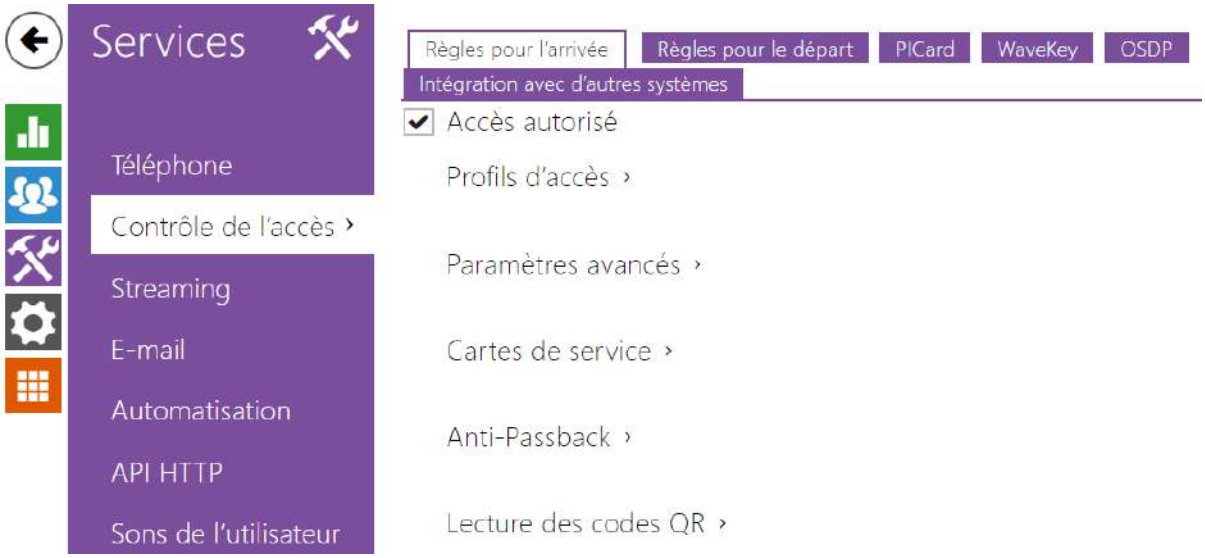
1. Retrouvez le module relais AXIS A9188 dans votre LAN en utilisant le scanner AXIS IP Utility.
2. Entrez l'identifiant.
3. Sélectionnez Préférences / Configuration additionnel du périphérique dans le menu.
4. Une nouvelle fenêtre de configuration de périphérique s’affiche.
5. Sélectionnez Options système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

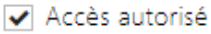
Voici les onglets que vous pouvez trouver dans cette section :

5.4.1 Contrôle de l’accès

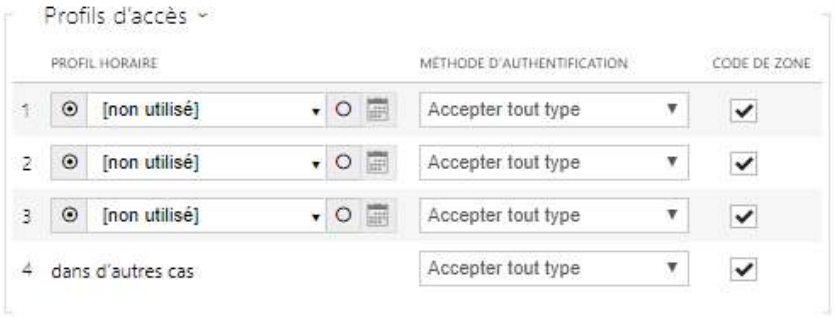
Le service Contrôle d’accès sert à gérer les accès et la façon dont l’authentification des utilisateurs est vérifiée.



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 l'un des profils prédéfinis ou définissez manuellement le profil temporel pour un élément donné.
- **Méthode d’authentification** – il définit la méthode d’authentification pour la plage horaire renseignée à cette ligne, y compris la possibilité d’authentification multiple pour

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

Observation

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

- **Blocage de l'accès** – affiche le statut du blocage de l'accès : Activé / Désactivé. Utilisable de le cas de scénario d'évacuation ou de confinement.
- **Code de zone** – il vous permet d'entrer un code de zone numérique à l'interrupteur. Le code doit contenir au moins deux caractères, mais nous vous recommandons d'utiliser au moins quatre caractères.
- **Signalisation d'authentification** – choisissez la façon dont vous souhaitez signaler l'utilisation d'une carte ou d'un autre type d'identifiant. Les options sont les suivantes : LED seule (signalisation visuelle) ou LED + Audio (signalisation visuelle et accoustique) à chaque fois qu'une carte ou un autre type d'identifiant sera renseigné (Valide - long bip ou invalide, bip court). Une manifestation acoustique distincte n'est entendue que lorsqu'une carte invalide ou un autre identifiant a été utilisé. Dans le cas d'un accès valide, le signal acoustique du commutateur est généralement joué, ce qui rend le bip d'authentification valide presque inaudible. Reportez-vous à la section 5.4.6 Sons de l'utilisateur.
- **Carte virtuelle sur Wiegand** – elle permet de choisir la sortie Wiegand à laquelle le numéro de carte virtuelle de l'utilisateur sera envoyé après son authentification réussie. On peut l'utiliser avec n'importe quelle authentification, y compris les codes, les empreintes digitales...Etc.
- **Alarme silencieuse activée** – pour chaque code d'accès, nous attribuons un code virtuel dont le numéro augmente d'une unité par rapport au numéro du code d'accès de l'utilisateur. Ce code est destiné à activer une alarme silencieuse en cas d'ouverture de porte sous la contrainte. Par exemple, si le code d'accès est 0000, le code pour activer l'alarme silencieuse est 0001. La longueur du code doit rester la même. Cela veut dire que par exemple pour le code d'accès 9999, l'alarme silencieuse est 0000 etc. L'action

effectuée en cas d'activation de l'alarme silencieuse peut être réglée dans la section **Services / Automatisation**.

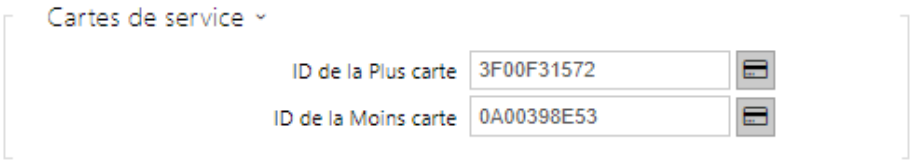
Observation

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

- **Limite du nombre de tentative d'accès invalide** – il permet de limiter le nombre de tentatives d'authentification invalide. Après cinq tentatives d'accès invalide (code numérique incorrect, carte invalide, etc.), le module d'accès sera bloqué pendant trente secondes même si l'authentification est valide par la suite.
- **Reconnaissance de la plaque d'immatriculation** – sélectionne le scénario après reconnaissance de la plaque d'immatriculation du véhicule. Une description détaillée des différentes fonctionnalités est disponible au chapitre 5.2.1 Utilisateurs.

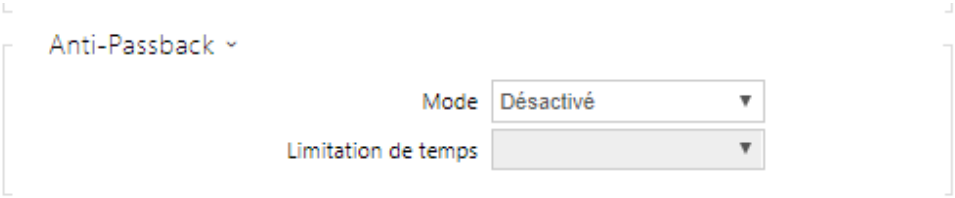
Avertissement

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



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

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



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

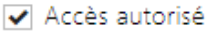
- **Mode** – activez / désactivez le mode Anti-Passback :
  - **Désactivé** – la fonctionnalité est désactivée par défaut, ce qui permet à l'utilisateur d'utiliser la carte d'accès ou un autre identifiant pour entrer de nouveau dans une zone sans la quitter.
  - **Modéré** – l'utilisateur est autorisé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

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

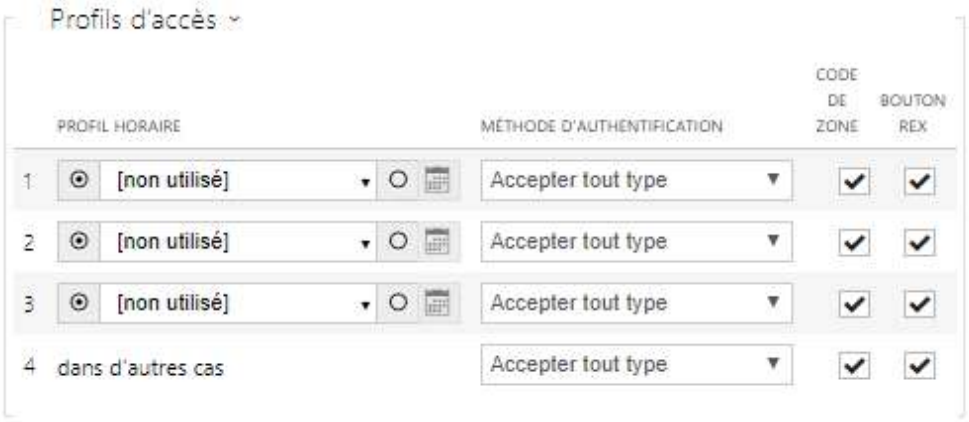
Observation

- Pour que la lecture des codes QR fonctionne bien, n'utilisez pas la fonction de confidentialité en même temps.
- 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.
- **Signalisation d'authentification** – choisissez la façon dont vous souhaitez signaler l'utilisation d'une carte ou d'un autre type d'identifiant. Les options sont les suivantes : LED seule (signalisation visuelle) ou LED + Audio (signalisation visuelle et accoustique) à chaque fois qu'une carte ou un autre type d'identifiant sera renseigné (Valide - long bip ou invalide, bip court). Une manifestation acoustique distincte n'est entendue que lorsqu'une carte invalide ou un autre identifiant a été utilisé. Dans le cas d'un accès valide,

le signal acoustique du commutateur est généralement joué, ce qui rend le bip d'authentification valide presque inaudible. Reportez-vous à la section 5.4.6 Sons de l'utilisateur.

- **Carte virtuelle sur Wiegand** – elle permet de choisir la sortie Wiegand à laquelle le numéro de carte virtuelle de l'utilisateur sera envoyé après son authentification réussie. On peut l'utiliser avec n'importe quelle authentification, y compris les codes, les empreintes digitales…Etc.

- **Alarme silencieuse activée** – pour chaque code d'accès, nous attribuons un code virtuel dont le numéro augmente d'une unité par rapport au numéro du code d'accès de l'utilisateur. Ce code est destiné à activer une alarme silencieuse en cas d'ouverture de porte sous la contrainte. Par exemple, si le code d'accès est 0000, le code pour activer l'alarme silencieuse est 0001. La longueur du code doit rester la même. Cela veut dire que par exemple pour le code d'accès 9999, l'alarme silencieuse est 0000 etc. L'action effectuée en cas d'activation de l'alarme silencieuse peut être réglée dans la section **Services / Automatisation**.

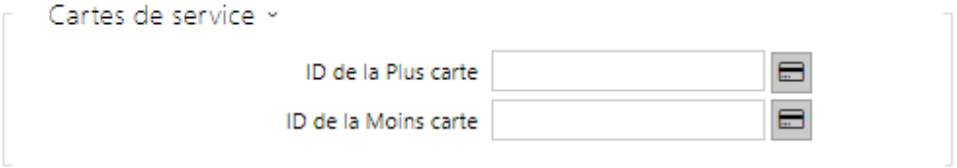
Observation

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

- **Limite du nombre de tentative d'accès invalide** – il permet de limiter le nombre de tentatives d'authentification invalide. Après cinq tentatives d'accès invalide (code numérique incorrect, carte invalide, etc.), le module d'accès sera bloqué pendant trente secondes même si l'authentification est valide par la suite.
- **Reconnaissance de la plaque d'immatriculation** – sélectionne le scénario après reconnaissance de la plaque d'immatriculation du véhicule. Une description détaillée des différentes fonctionnalités est disponible au chapitre 5.2.1 Utilisateurs.

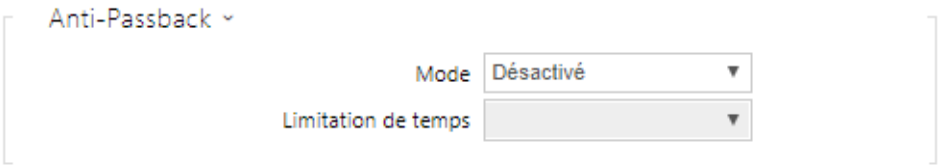
Avertissement

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



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

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

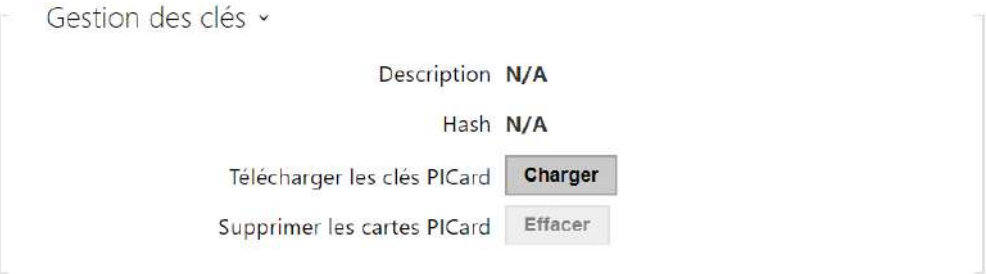


L'Anti-Passback est une fonctionnalité de sécurité qui empêche les utilisateurs d'utiliser leurs cartes d'accès ou d'autres identifiants pour entrer de nouveau dans une zone sans l'avoir quitté (par exemple, pour empêcher les utilisateurs de partager des cartes).

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

PICard

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



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

WaveKey

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

Identifiant de l'utilisateur (ID d'authentification)

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

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

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

Clé crypté pour la localisation

2N® Mobile Key – communique toujours avec l'Interphone de manière cryptée. **2N® Mobile Key** ne peut pas authentifier un utilisateur sans connaître la clé de chiffrement. La clé de chiffrement principale est automatiquement générée lors du premier lancement de l'interphone

et peut être générée manuellement à tout moment. Avec l'ID d'authentification, la clé de chiffrement principale est transmise au périphérique mobile pour le jumelage.

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

Jumelage

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

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

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

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

Clé de chiffrement pour le jumelage

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

Administration de la clé cryptée

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

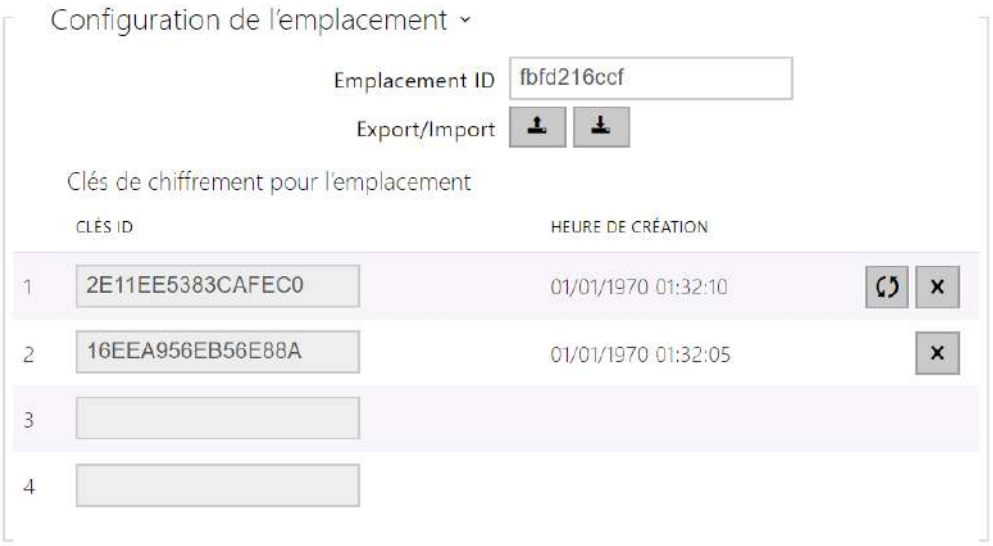
Note

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

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

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

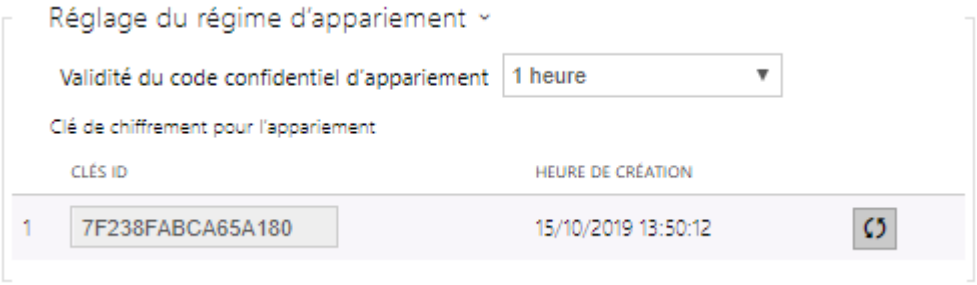
Liste des paramètres



- **Emplacement ID** – identificateur incontestable de l'emplacement, dans lequel prévaut le set de clés de chiffrement réglées.
- **Export** – appuyez sur ce bouton pour exporter l'ID d'emplacement et les clés de chiffrement actuelles dans un fichier. Par la suite, le fichier exporté peut être importé sur un autre appareil.
- **Import** – appuyez sur ce bouton pour importer l'ID d'emplacement et les clés de chiffrement actuelles à partir d'un fichier exporté depuis un autre interphone.
- **Restaurer la clé primaire** – en générant une nouvelle clé de cryptage principale vous supprimez la plus ancienne clé secondaire. Ainsi, l'utilisateur de l'application **2N® Mobile Key** qui utilisent toujours cette clé ne pourront pas s'authentifier à moins d'avoir mis à

jour les clés de chiffrement de leurs appareils mobiles avant leur suppression. Les clés de l'appareil mobile sont mises à jour à chaque utilisation de l'application **2N® Mobile Key**.

- **Effacer la clé primaire** – efface la clé primaire pour empêcher l'authentification des utilisateurs qui utilisent encore cette clé.
- **Effacer la clé secondaire** – les utilisateurs de **2N® Mobile Key** qui utilisent toujours cette clé ne pourront pas s'authentifier à moins d'avoir mis à jour les clés de chiffrement de leurs appareils mobiles avant leur suppression. Les clés de l'appareil mobile sont mises à jour à chaque utilisation de l'application **2N® Mobile Key**.



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

Conseil

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

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

Avertissement

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

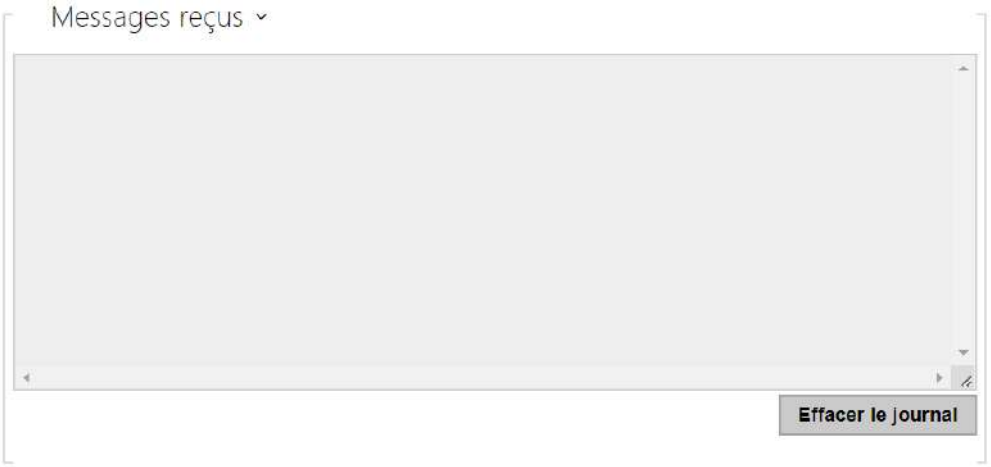
OSDP

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

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

Observation

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



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

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

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

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

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

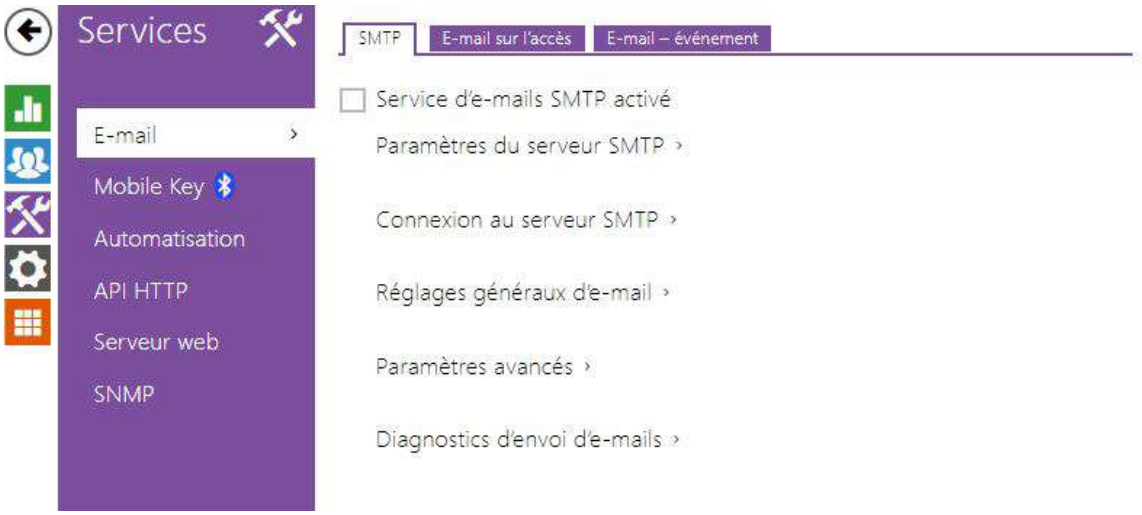
Observation

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

Intégration avec d’autres systèmes

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

5.4.2 E-mail



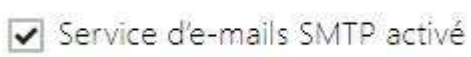
Pour informer les utilisateurs de l'interphone de tous les appels manqués et / ou passés avec succès, vous pouvez configurer **l'unité de contrôle d'accès 2N** pour envoyer un courrier électronique après chaque appel. Il vous est possible de personnaliser l'objet de l'e-mail et le texte du message. Si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

L'unité 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**.

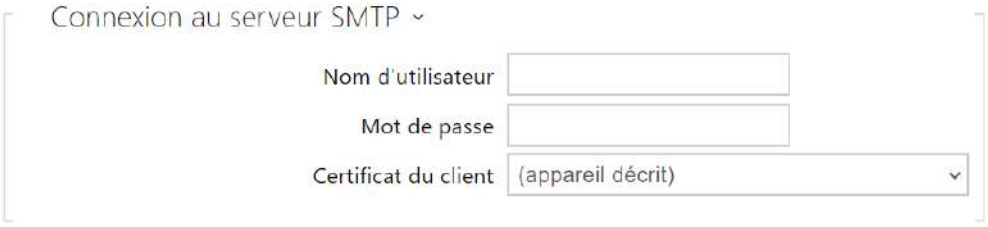
> **Note**
>
> - *La fonction de courriel n'est disponible qu'avec la licence Gold.*

SMTP



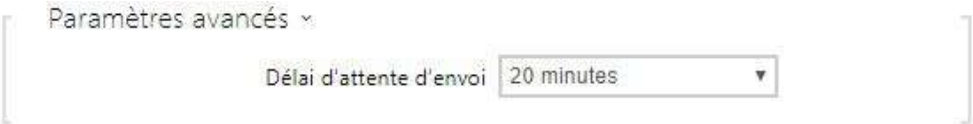
- **Service d'e-mails SMTP activé** – activer/désactiver l'envoi d'e-mails à partir de l'unité.

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



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

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

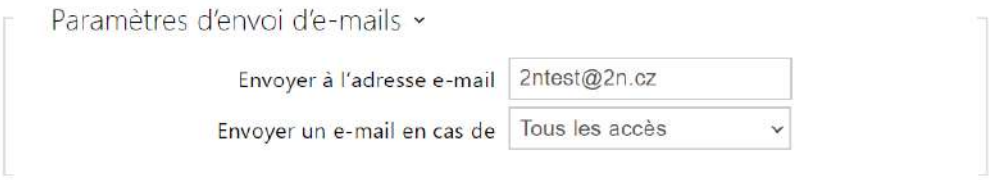


- **Délai d'attente pour l'envoi** – définissez le délai d'envoi d'un e-mail vers un serveur SMTP inaccessible.

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 l'unité 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.

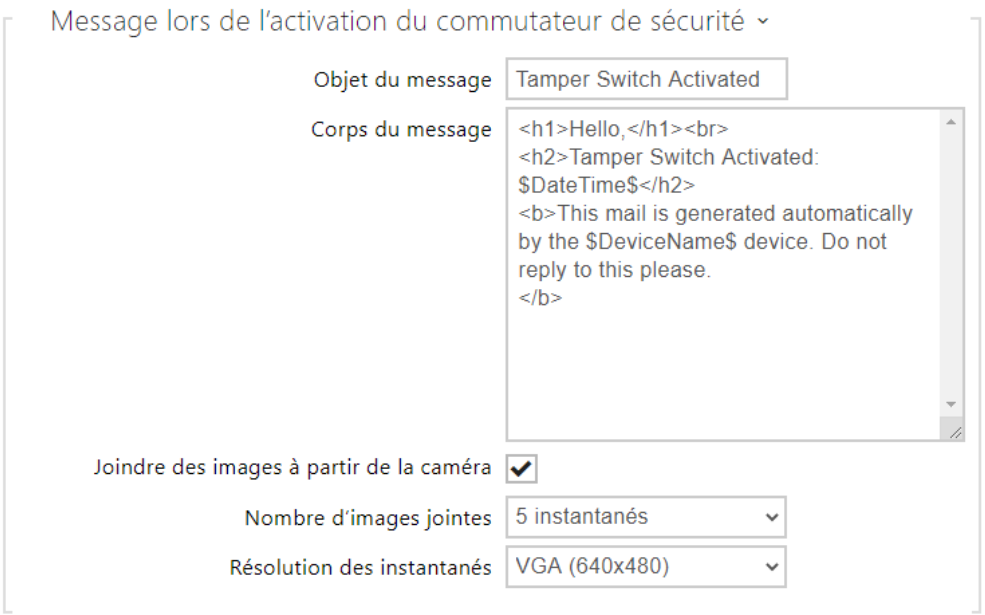
- **Objet du message** – définissez l'objet de l'e-mail envoyé.
- **Corps du message** – modifiez le texte à envoyer. Utiliser le langage de formatage HTML dans le texte. Vous pouvez insérer des symboles spéciaux en remplaçant le nom d'utilisateur, la date et l'heure et l'ID de l'appareil. Ces symboles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

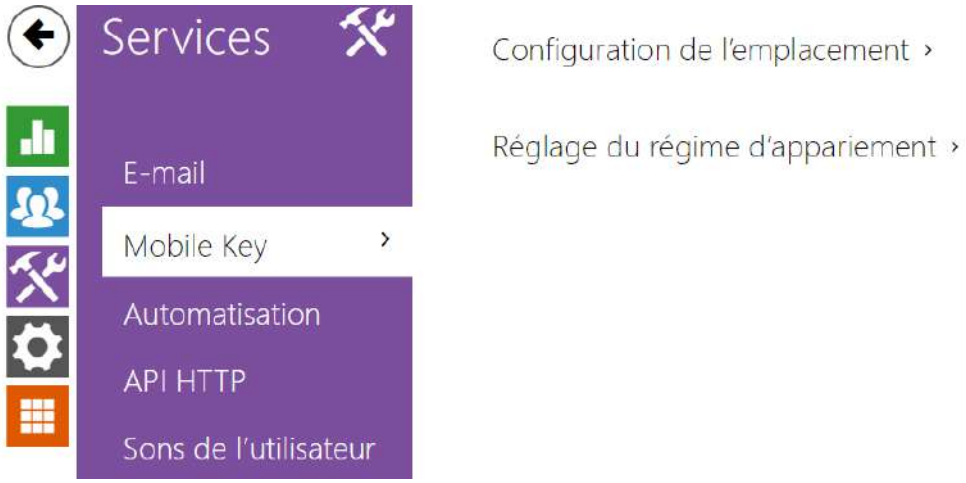
Occurrence	Symbole de substitution	Description
	$BuildTime$	date et heure d’établissement
	$UpTime$	période d’exploitation de l’équipement
Fonction du cas spécifique	$User$	nom de l’utilisateur
	$RebootReason$	raison du redémarrage
	$DialNumber$	numéro appelé, entrant ou sortant
	$SipAccountNumber$	numéro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

5.4.3 Mobile Key



Les **unités de controle d'accès 2N** équipées 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'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

2N® Mobile Key – communique toujours avec l'**unité de controle d'accès 2N** 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'unité 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 unités 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'interphone.

> **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'unité. 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 **unité de controle d'accès 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'**unité de controle d'accès 2N**.

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.

5.4.4 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.

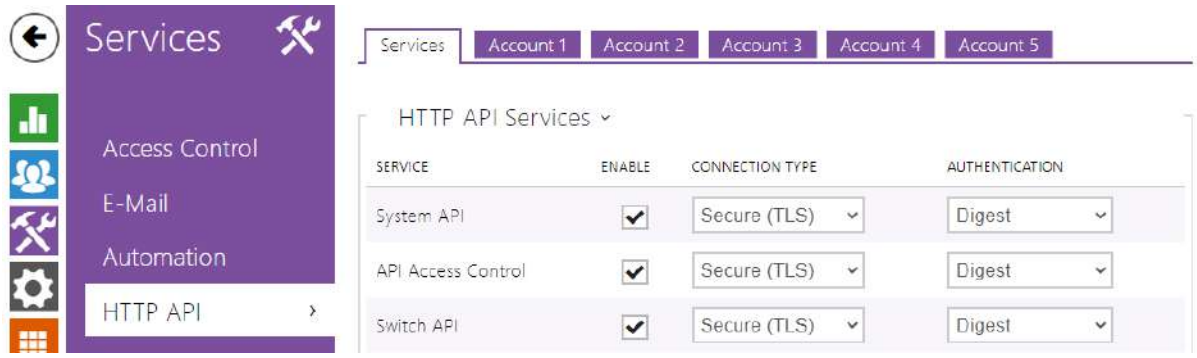
Référez-vous au Manuel d'Automatisation pour découvrir les possibilités et les détails de la configuration.

Note

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

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

Définissez le protocole de transport (**HTTP** ou **HTTPS**) et la méthode d'authentification (**Aucune**, **Basic** ou **Digest**) pour chaque fonctionnalité. Créez jusqu'à cinq comptes d'utilisateur (avec leur propre nom d'utilisateur et mot de passe) dans la configuration de l'**API HTTP** pour un contrôle d'accès détaillé des services et des fonctions.

Définissez les méthodes d'authentification pour les demandes à envoyer à l'interphone pour chaque service. Si l'authentification requise n'est pas exécutée, la demande sera rejetée. Les

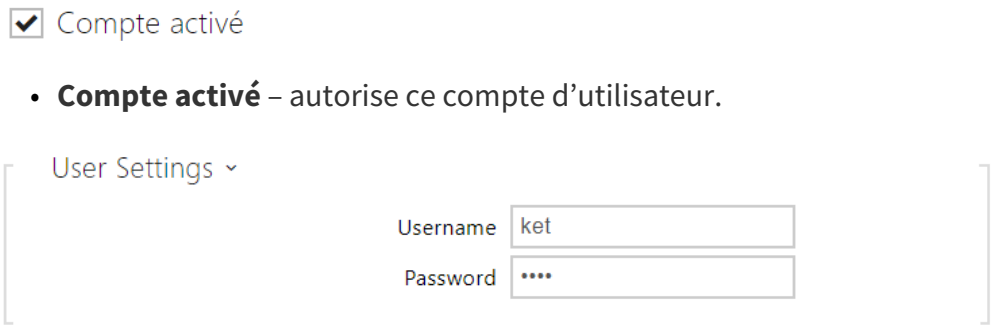
demandes sont authentifiées via un protocole d'authentification standard décrit par **RFC-2617**. Les trois méthodes d'authentification suivantes sont disponibles :

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

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

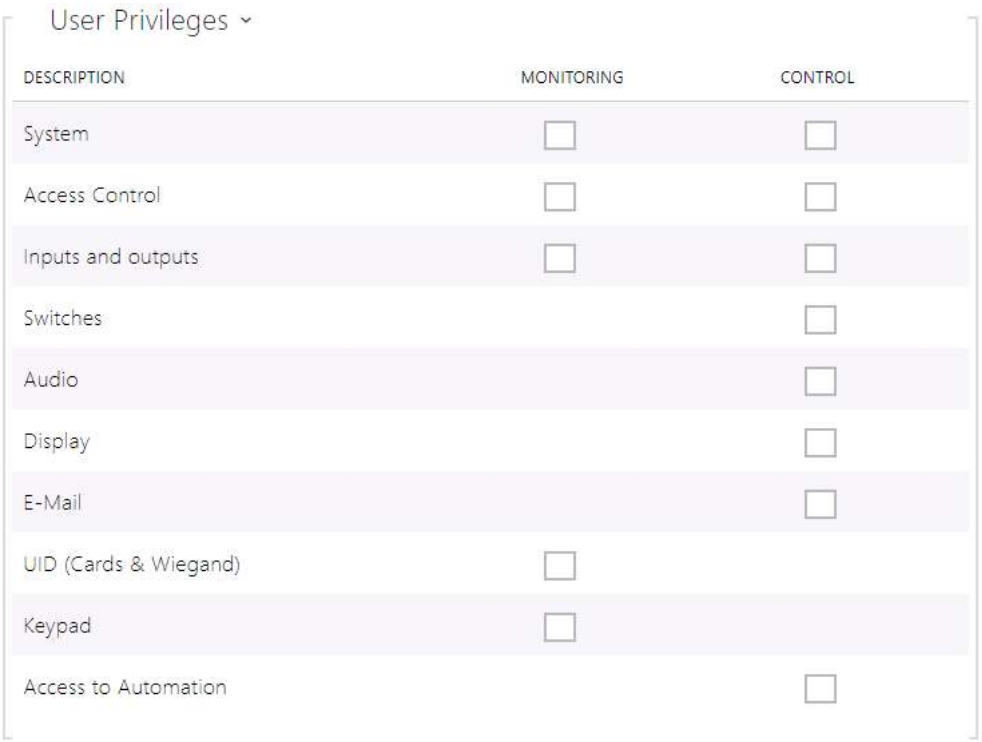
Compte 1–5

Unités 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.



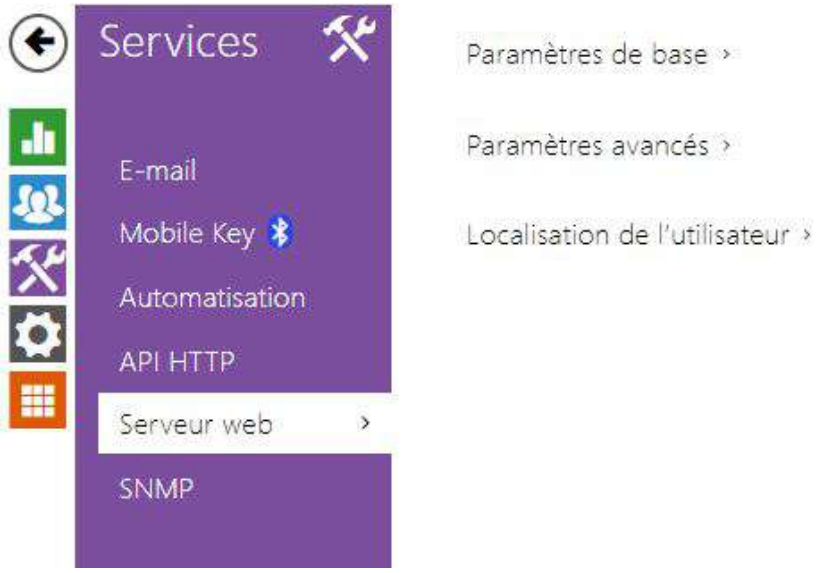
À l'aide du tableau des droits d'accès on peut gérer les privilèges du compte d'utilisateur pour les différents services.

5.4.6 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 5.3.1 Porte.

- **Signalisation d’activation d’un interrupteur 1** – paramétrer le son à générer lorsqu’un interrupteur 1 est activé.
- **Signalisation d’activation d’un interrupteur 2** – Paramétrer le son à générer lorsqu’un interrupteur 2 est activé.

5.4.7 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'interphone :

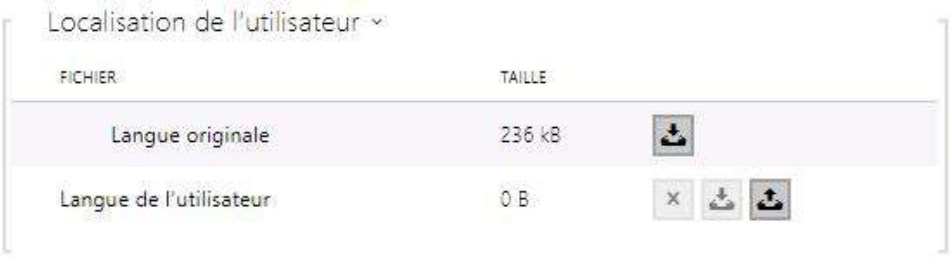
1. Commandes HTTP pour le contrôle des Interrupteurs, reportez-vous à la sous-section Interrupteur.
2. Event.HttpTrigger dans **2N Automatisation**, référez vous au Manuel concerné.

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’interphone. Appuyez sur pour modifier le mot de passe. Le mot de passe composé de 8 caractères doit comporter au moins une lettre minuscule, une lettre majuscule et un chiffre.

- **Port HTTP** – paramétrez le port du serveur web pour la communication HTTP. Le paramétrage du port ne sera appliqué qu'après le redémarrage de l'Interphone.
- **Port HTTPS** – il définit le port de communication du serveur Web pour la communication à l’aide du protocole HTTPS sécurisé. Le paramétrage du port ne sera appliqué qu'après le redémarrage de l'Interphone.
- **Version TLS minimum** – définissez la version TLS minimale, autorisée pour la connexion à l’appareil.
- **Certificat d’utilisateur HTTPS** – spécifiez le certificat d’utilisateur et la clé privée pour le serveur HTTP du dispositif – cryptage de communication du navigateur web de l’utilisateur. Sélectionner l’un des trois jeux de certificats d’utilisateur et de clés privées (se reporter à la partie Certificats) ou conserver le paramètre **SelfSigned**, grâce auquel le certificat automatiquement généré lors du premier allumage du dispositif est utilisé.
- **Accès à distance activé** – activez l’accès à distance au serveur web du dispositif à partir d’adresses IP Off-LAN.

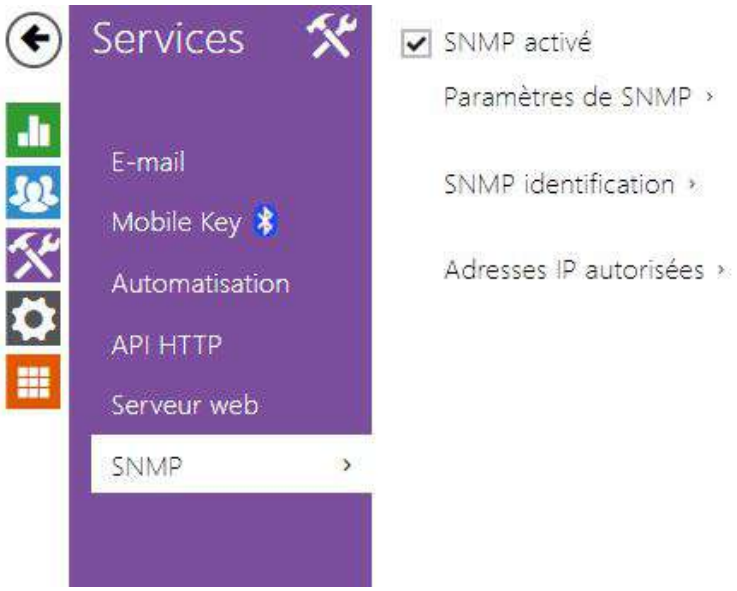


- **Langue originale** – téléchargez le fichier original contenant tous les textes de l'interface utilisateur en anglais. Le format de fichier est XML; voir ci-dessous.
- **Langue de l'utilisateur** – enregistrez, chargez et supprimez, si nécessaire, un fichier utilisateur contenant vos propres traductions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

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

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

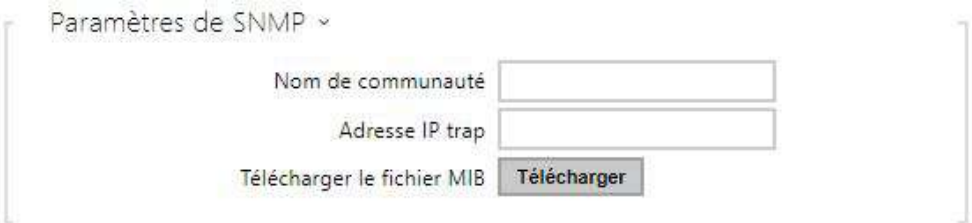
5.4.8 SNMP



L'**unité de contrôle d'accès 2N** intègre 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.

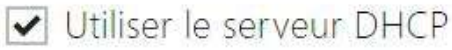
Conseil

- *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'**unité de contrôle d'accès 2N** peut vous communiquer son adresse IP via une fonction vocale.*

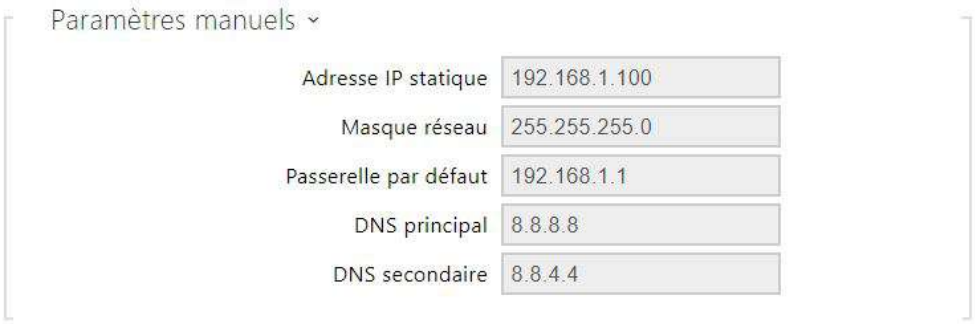
Si vous utilisez un serveur RADIUS et la vérification basée sur 802.1x pour les équipements connectés, vous pouvez faire en sorte que l'Interphone utilise l'authentification EAP-MD5 ou EAP-TLS. Définissez cette fonction dans l'onglet 802.1x.

L'onglet Trace vous permet de lancer la capture des paquets entrants et sortants sur l'interface réseau de l'**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).

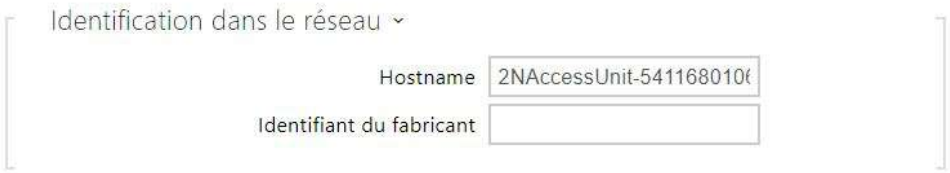
Liste des paramètres



- **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'interphone IP 2N.

- **Identifiant du fabricant** – définissez l'identifiant de classe du fournisseur sous la forme d'une chaîne de caractères pour l'option DHCP 60.

- **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).

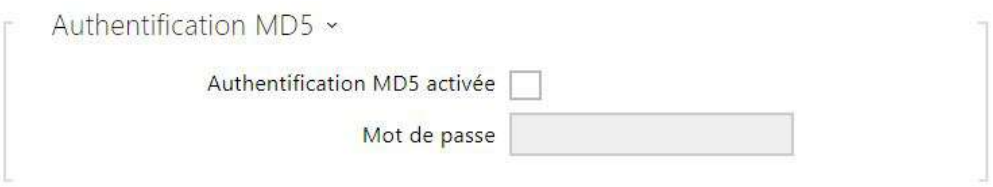
- **Vérifier l'accessibilité de l'adresse dans le réseau** – vérifiez l'accessibilité de l'adresse réseau via la commande Ping dans les systèmes d'exploitation standard. Appuyez sur Ping pour afficher une boîte de dialogue, entrez l'adresse IP / le nom de domaine, puis cliquez sur Ping pour envoyer les 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.

802.1x

Cet onglet n'est pas affiché dans les 2N Access Unit 2.0, qui ne supportent par le protocol 802.1x.

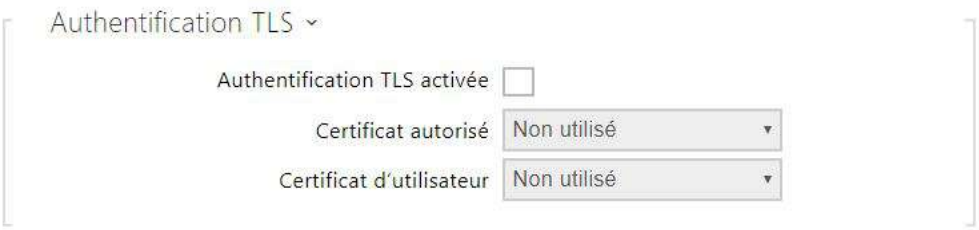
- **Identifiant de l'appareil** – nom d'utilisateur (identifiant) pour l'authentification via EAP-MD5 et EAP-TLS.



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

Avertissement

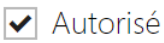
- N'activez pas cette fonction si votre réseau ne prend pas en charge la norme 802.1x. Dans le cas contraire, l'interphone IP 2N deviendra indisponible et devra être réinitialisé aux paramètres d'usine.



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

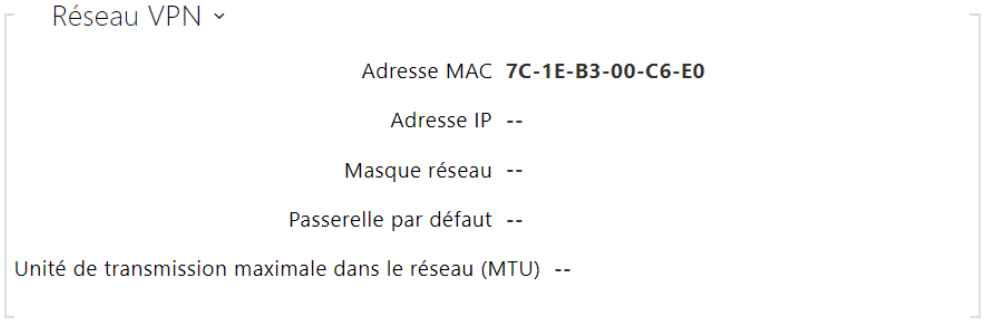
Open VPN

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.



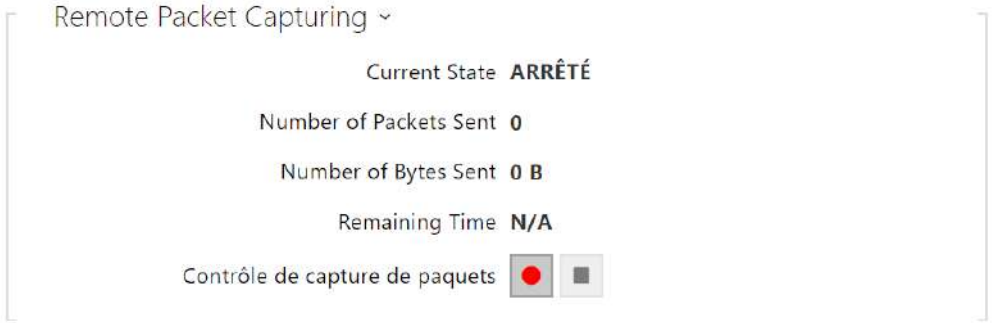
- **Réseau VPN** – affiche les informations de base sur le VPN.

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

Trace

Dans l'onglet Trace, vous pouvez lancer la capture des paquets entrants et sortants sur l'interface réseau d'interphone. Les paquets capturés peuvent être stockés localement dans la mémoire tampon de l'interphone IP 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  .

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 **2N® Access Unit** soient correctement définies.

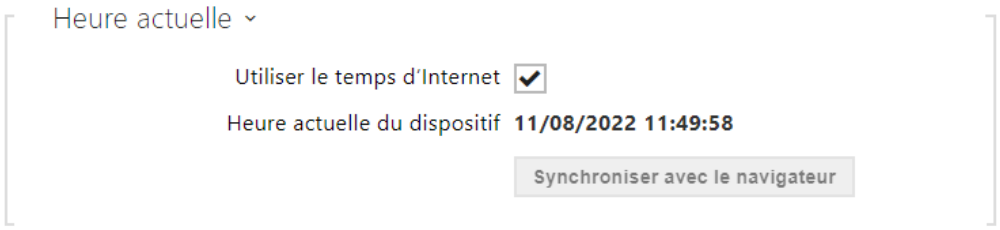
La plupart des modèles **2N® Access Unit** sont équipés d'une horloge de secours en temps réel pouvant résister à plusieurs jours de pannes de courant. Vous pouvez à tout moment synchroniser l'heure **2N® Access Unit** avec l'heure d'Internet en cochant la fonction **Utiliser l'heure réelle d'Internet** ou avec l'heure actuelle de votre PC à l'aide du bouton **Synchroniser dans le navigateur**.

Note

- ***2N® Access Unit*** *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'Interphone 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.

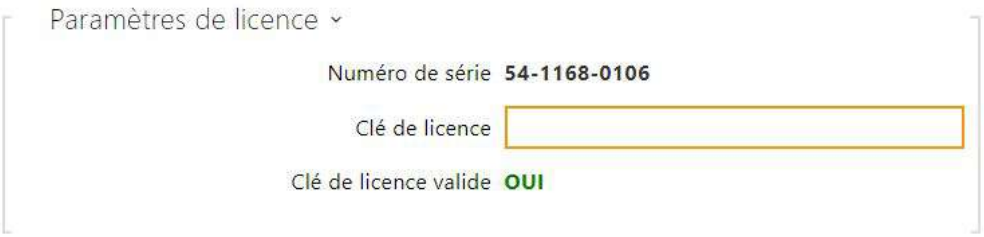
- **Détection automatique** – définit si le fuseau horaire sera détecté automatiquement depuis le service My2N. Si la détection automatique est désactivée, le réglage dans le paramètre de sélection manuelle (fuseau horaire sélectionné manuellement ou Règle personnalisée) est utilisé.
- **Fuseau horaire 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 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 interphone.

Liste des paramètres



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

- **Licence standard** – affiche la liste des licences qui sont incluses avec le dispositif en usine.
  - **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.

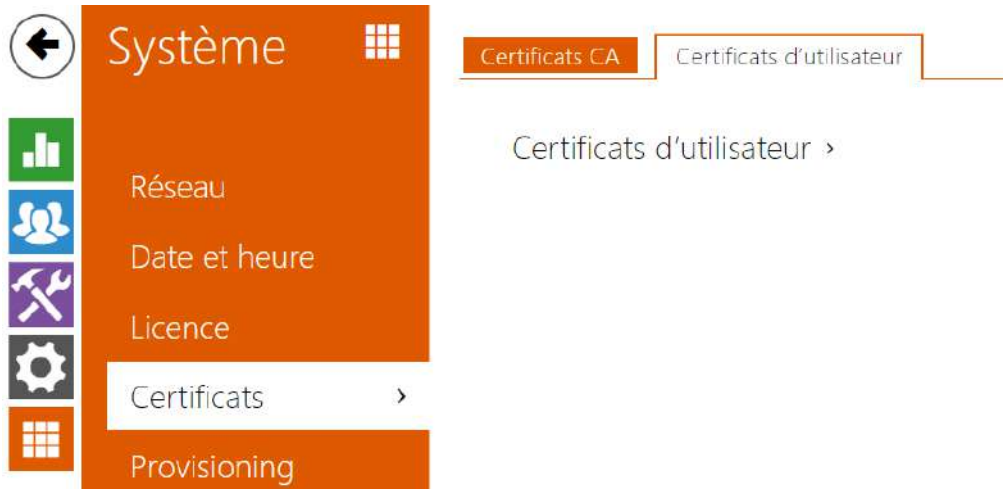
Conseil

- 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.

5.5.4 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'interphone communique, et de télécharger des certificats personnels et des clés privées, servant au cryptage de la communication.

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

- **L'unité de contrôle d'accès 2N** accepte les formats de certificat DER (ASN1) et PEM.
- **L'unité de contrôle d'accès 2N** prend en charge le cryptage AES, DES et 3DES.
- **L'unité de contrôle d'accès 2N** 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

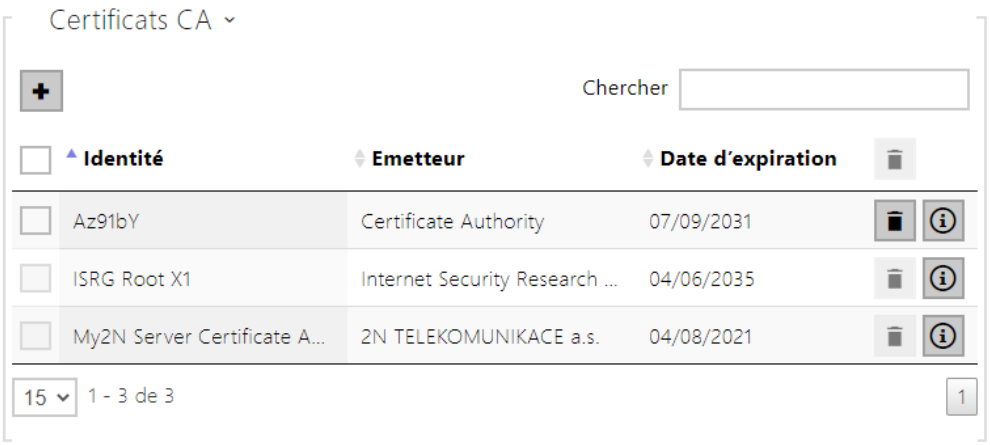
- Les certificats CA doivent utiliser le format X.509 v3.

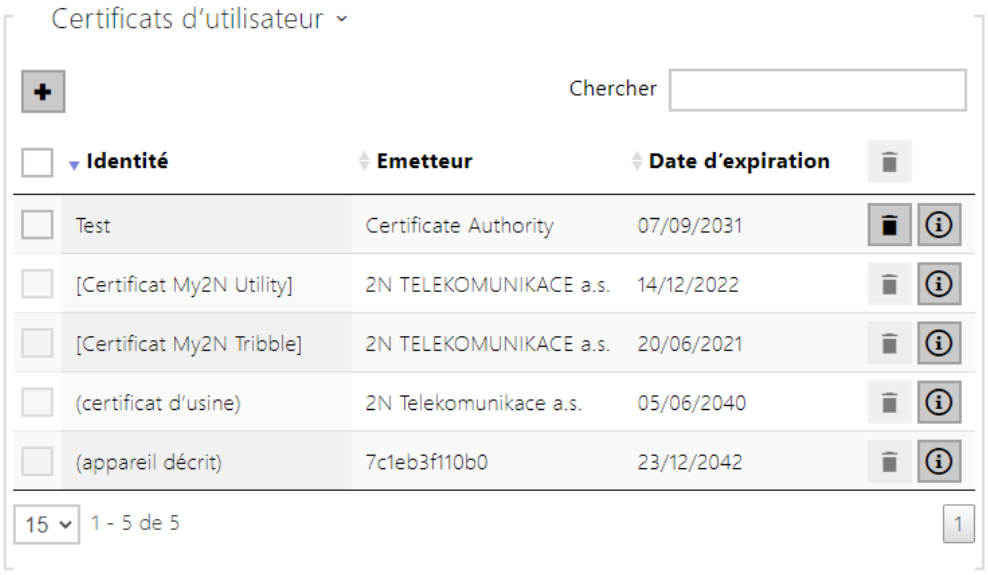
Lors de la première mise sous tension, l'**unité de contrôle d'accès 2N** génère automatiquement le **certificat** et la **clé privée auto-signés** pour le **Serveur Web** et les **services de messagerie**, sans vous obliger à charger un certificat et une clé privée.

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

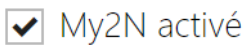
- Pour les certificats basés sur des courbes elliptiques, utilisez uniquement les courbes secp256r1 (ou prime256v1, également appelée NIST P-256) et secp384r1 (ou NIST P-384).

5.5.5 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'interphone :

1. **au – 2N Access Unit**
2. **aug2 – 2N Access Unit 2.0**
3. **aum – 2N Access Unit M**

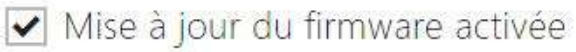
MACADDR est l'adresse MAC de l'unité au format 00-00-00-00-00-00. Recherchez l'adresse MAC sur la plaque de production de l'unité ou dans l'onglet **État** de l'unité via l'interface Web.

Exemple :

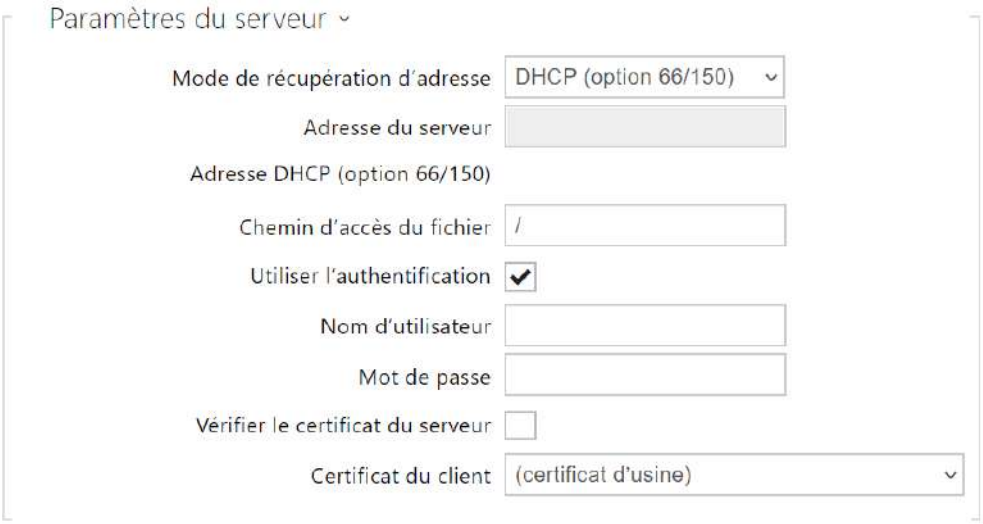
L'**unité de contrôle d'accès 2N** avec l'adresse MAC 00-87-12-AA-00-11 télécharge les fichiers suivants à partir du serveur TFTP :

- au-firmware.bin
- au-common.xml
- au-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.

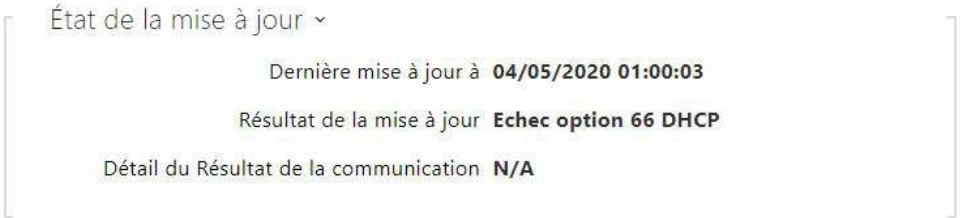


- **Mode de récupération d'adresse** – définissez si l'adresse du serveur TFTP/HTTP doit être saisie manuellement ou via une valeur récupérée automatiquement à partir du serveur DHCP utilisant l'option 66.
- **Adresse du serveur** – saisissez manuellement l'adresse du serveur TFTP (tftp://ip_adresse), 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 répertoire ou le préfixe du firmware/ de la configuration sur le serveur. L'unité attend les fichiers XhipY_firmware.bin, XhipY-

common.xml et XhipY-MACADDR.xml, où X est le préfixe spécifié et Y spécifie le modèle de l'interphone.

- **Utiliser l'authentification** – activez l'authentification pour l'accès au serveur HTTP.
- **Nom d'utilisateur** – entrez le nom d'utilisateur pour l'authentification du serveur.
- **Mot de passe** – entrez le mot de passe pour l'authentification du serveur.
- **Vérifier le certificat du serveur** – définit une liste des autorités de certifications pour vérifier la validité du certificat public du serveur ACS.
- **Certificat du client** – définit le certificat client et la clé privée qui autorise l'interphone à communiquer avec le serveur ACS.

- **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.

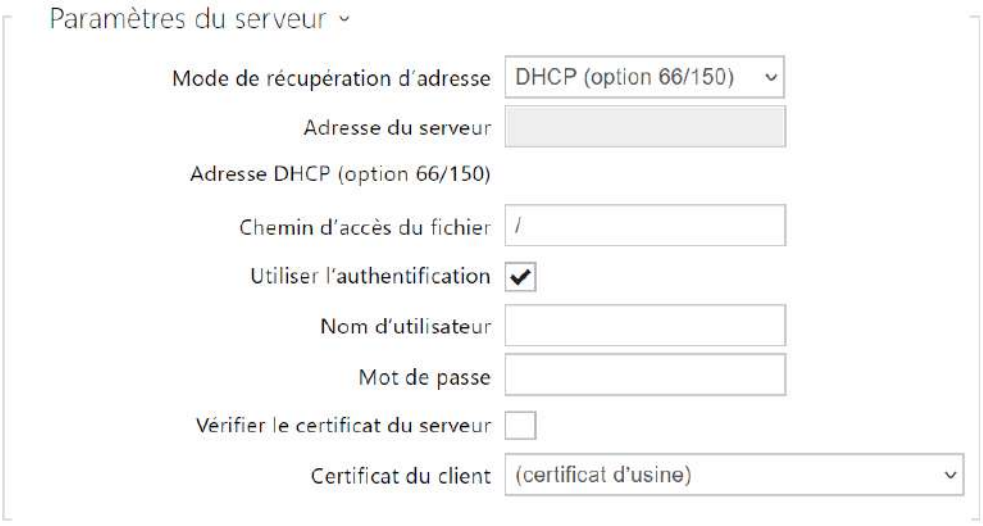
- **Résultat de la mise à jour** – résultat de la dernière mise à jour. Les options suivantes sont disponibles :

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.

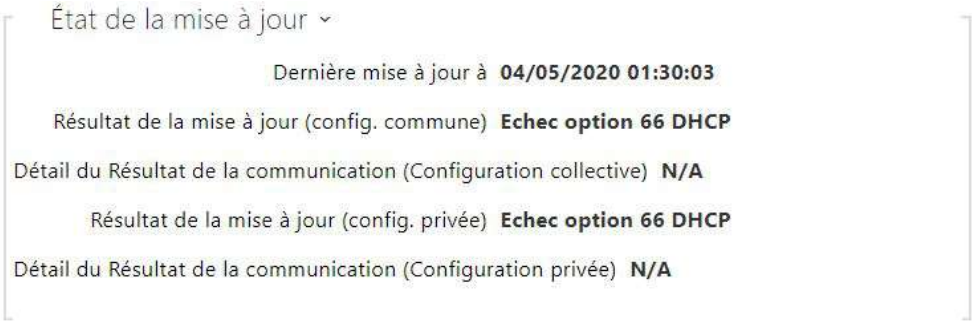


- **Mode de récupération d'adresse** – définissez si l'adresse du serveur TFTP/HTTP doit être saisie manuellement ou si une valeur récupérée automatiquement à partir du serveur DHCP utilisant l'option 66 doit être utilisée.
- **Adresse du serveur** – saisissez manuellement l'adresse du serveur TFTP (tftp://ip_adresse), 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'Interphone attend un fichier XhipY_firmware.bin, XhipY-common.xml et XhipY-MACADDR.xml, où X est le préfixe spécifié et Y spécifie le modèle de l'interphone.
- **Utiliser l'authentification** – activez l'authentification pour l'accès au serveur HTTP.
- **Nom d'utilisateur** – entrez le nom d'utilisateur pour l'authentification du serveur.
- **Mot de passe** – entrez le mot de passe pour l'authentification du serveur.
- **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'unité à communiquer avec le serveur ACS.

Info

- L'unité 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'unité.
- **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.

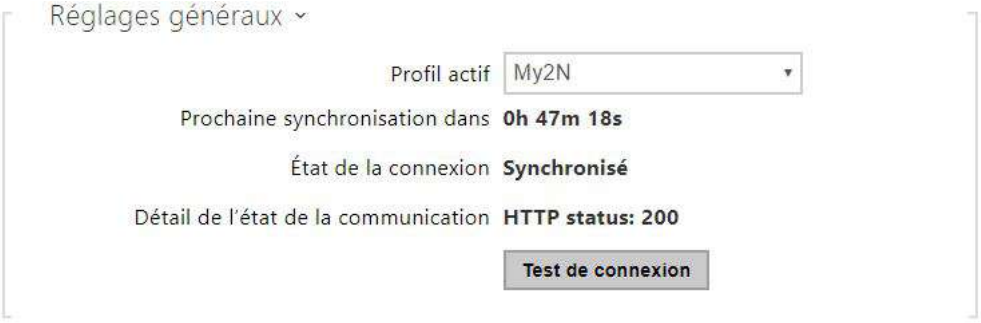
My2N / TR069

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

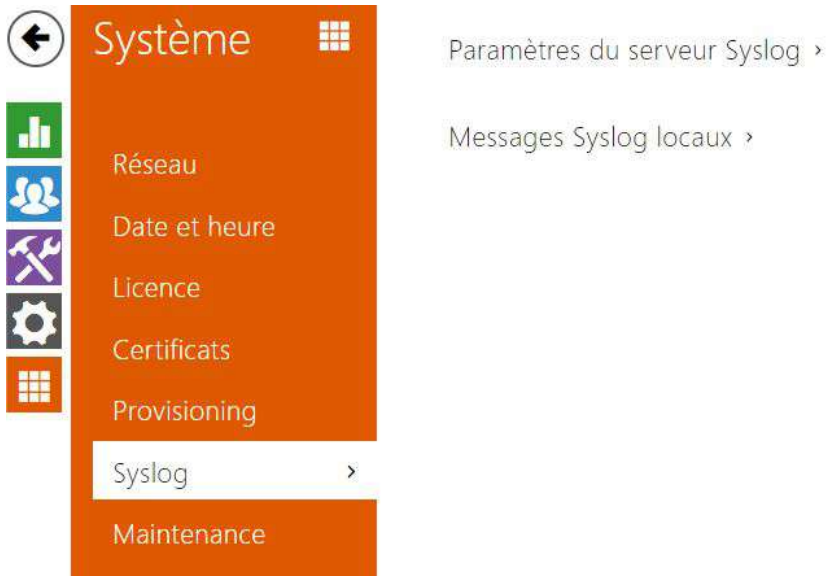
- **My2N / TR069 activé** – activez la connexion à My2N ou à un autre serveur ACS.



- **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'unité doit contacter un ACS distant.
- **État de la connexion** – affiche l'état actuel de la connexion ACS ou la description de l'état d'erreur si nécessaire.
- **Détail de l'état de la communication** – code d'erreur de communication avec le serveur ou code d'état du protocole HTTP.
- **Test de connexion** – testez la connexion TR069 en fonction du profil défini, voir le profil Actif. Le résultat du test est affiché dans l'état de la connexion.

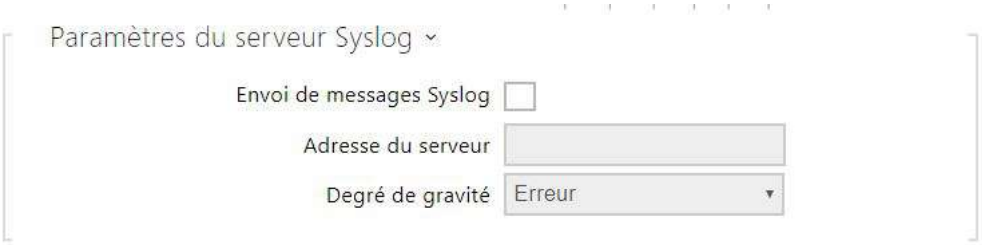
- **Adresse du serveur ACS** – définissez l'adresse ACS au format suivant : ipadresse[: port], 192.168.1.1:7547, par exemple.
- **Nom d'utilisateur** – définissez le nom d'utilisateur pour l'authentification de l'interphone lors de la connexion au serveur ACS.
- **Mot de passe** – définissez le mot de passe pour l'authentification de l'interphone lors de la connexion au serveur ACS.
- **Vérifier le certificat du serveur** – définit une liste des autorités de certifications pour vérifier la validité du certificat public du serveur ACS. Si le certificat de l'autorité de certification n'est pas indiqué, le certificat public du serveur ACS n'est pas vérifié.
- **Certificat du client** – définit le certificat client et la clé privée qui autorise l'interphone à communiquer avec le serveur ACS. Sélectionner l'un des trois types de certificats ; se reporter au chapitre sur les Certificats.
- **Vérification périodique** – activez l'enregistrement périodique de l'interphone dans l'ACS.
- **Intervalle de vérification** – définissez l'intervalle d'enregistrement périodique de l'interphone dans le système ACS s'il est activé par le paramètre **Vérification périodique**.

5.5.6 Syslog

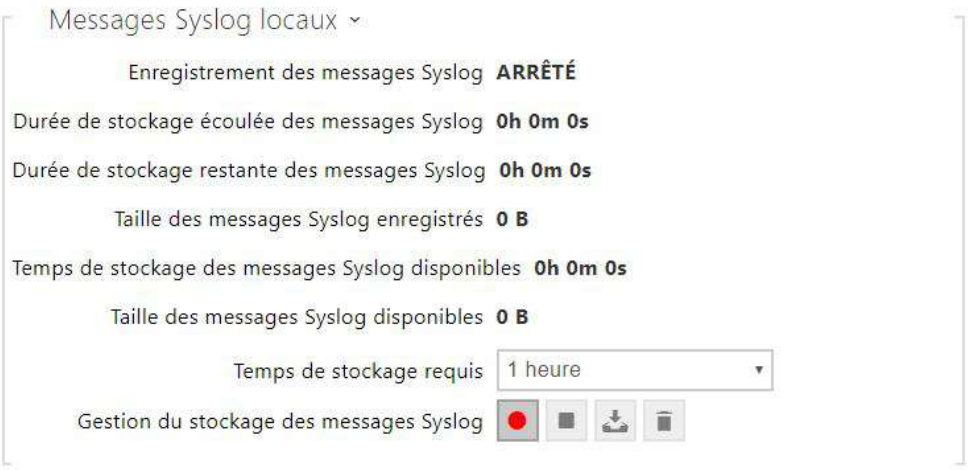


Les **unités de contrôle d'accès 2N** vous permettent d'envoyer au serveur Syslog des messages système contenant des informations pertinentes sur les états des périphériques et les processus d'enregistrement, d'analyse et d'audit. Il n'est pas nécessaire de configurer ce service pour un fonctionnement classique de l'**unité de contrôle d'accès 2N**.

Liste des paramètres

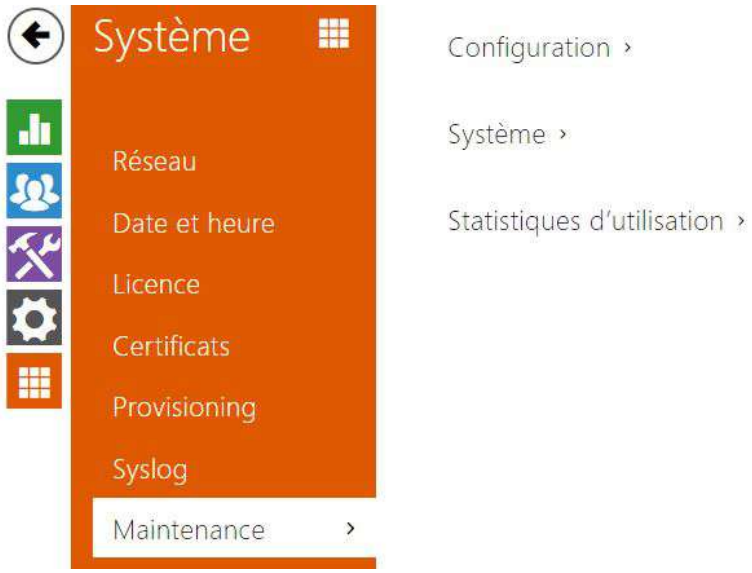


- **Envoi de messages Syslog** – activez l'envoi de messages système au serveur Syslog. Assurez-vous que l'adresse du serveur est bien paramétrée.
- **Adresse du serveur** – paramétrez l'adresse IP ou l'adresse MAC du serveur sur lequel l'application Syslog fonctionne.
- **Degré de gravité** – réglez 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.

5.5.7 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.

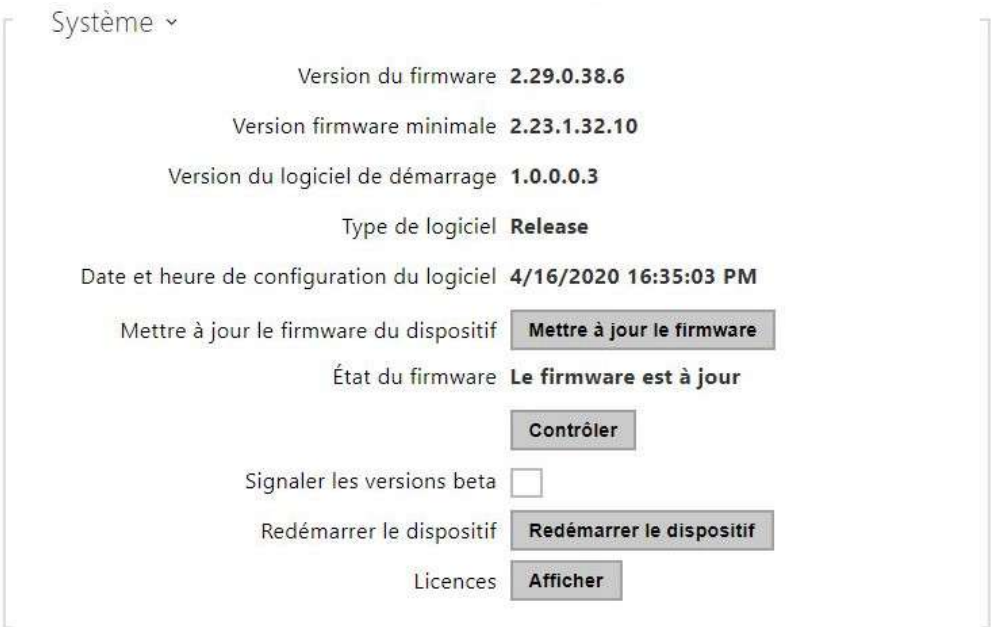
Observation

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

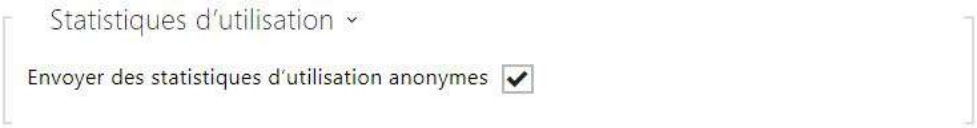


- **Mettre à jour le firmware** – pour mettre à jour le firmware de votre **unité de contrôle d'accès 2N**, appuyez sur le bouton pour afficher une fenêtre de dialogue vous permettant de sélectionner et de télécharger le fichier du firmware sur l'interphone. L'**unité de contrôle d'accès 2N** sera automatiquement redémarré et un nouveau firmware sera alors disponible. La procédure complète de mise à jour dure moins d'une minute. Référez-vous au site www.2n.com. pour la dernière version FW de votre 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'interphone prend 3 à 15 s, en fonction de la taille de la configuration. Ne redémarrez pas l'interphone 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.