2N LiftIP 2.0

Manuel d'utilisateur

2N TELEKOMUNIKACE a.s.
Modřanská 621 | Prague 4 | 143 01

2N.com

Table des matières

Vue d'ensemble du produit

Ce chapitre présente le produit **2N LiftIP 2.0**, les possibilités d'utilisation et les avantages qui découlent de son utilisation.

Versions de produit

Unités de base de la conception universelle

Ces unités sont conçues pour être installées derrière le panneau de l'ascenseur, qui est préalablement préparé pour leur installation.

Numéro de référence : 921640E

2N LiftIP 2.0 COP unit, EN

Numéro de référence : 921640XE

2N LiftIP 2.0 COP unit, EN, Cable version

Comprend deux DEL (verte et jaune), un microphone et un haut-parleur reliés par des câbles.

Numéro de référence : 921618BE

2N LiftIP 2.0 COP unit – Flush mounting, EN, With button

Les unités dotées d'un boîtier en acier inoxydable sont conçues pour être installées dans le panneau de l'ascenseur.

Numéro de référence : 921618E

2N LiftIP 2.0 COP unit – Flush mounting, EN, Without button

Les unités dotées d'un boîtier en acier inoxydable sont conçues pour être installées dans le panneau de l'ascenseur.

Unités de base dans la conception des COT

- **Numéro de référence : 921630E**

  2N LiftIP 2.0 TOC unit, EN

  Les unités en boîtier métallique sont conçues pour être installées sur la cabine d'ascenseur.

  Unités de base dans la conception des COT

- **Numéro de référence : 921630E**

  2N LiftIP 2.0 TOC unit long, EN

  Kit de base avec interrupteur pour le raccordement d'une station d'alarme vocale 2N dans un boîtier métallique

  Comprend deux DEL (verte et jaune), un microphone et un haut-parleur reliés par des câbles.

  Les unités en boîtier métallique sont conçues pour être installées sur la cabine d'ascenseur.

Fonctionnalités de base

Le 2N LiftIP 2.0 est un communicateur d'urgence pour ascenseurs qui permet la transmission d'un son en duplex intégral à l'aide de la technologie VoIP directement à partir de la cabine de l'ascenseur. Un microphone et un haut-parleur situés derrière le panneau de l'ascenseur sont utilisés pour la communication bidirectionnelle. **Le 2N LiftIP 2.0** est conçu pour les endroits où un réseau local est disponible et auquel il se connecte via un connecteur RJ-45. **Le 2N LiftIP 2.0** peut être alimenté soit par une alimentation externe de 10-30 V DC / 0,5 A, soit directement par un réseau local équipé d'éléments de réseau supportant la technologie PoE 802.3af. A partir de **2N LiftIP 2.0**, les appels ne peuvent être effectués que vers des numéros préprogrammés. Grâce à la connectivité IP, **2N LiftIP 2.0** peut être constamment surveillé, configuré à distance et son état suivi. L'avantage est la possibilité de connecter un nombre presque illimité d'unités de communication.

Avantages d’utilisation

- reproduit un ensemble de messages de base
- Permet d'enregistrer des messages personnalisés d'une durée maximale de 8 minutes (10 messages utilisateur).
- des propriétés acoustiques optimales
- Volume du haut-parleur réglable à l'aide des boutons situés sur le haut-parleur (pendant un appel)
- configuration via l'interface web de l'appareil
- Fonction "Check call" une fois tous les 3 jours (modifiable)
- indication de fonction - deux voyants lumineux conformément aux réglementations en vigueur pour les ascenseurs
- recomposition automatique d'un maximum de quatre numéros composés
- protection contre les démarrages intempestifs ou inutiles (CANCEL)
- contrôle des appels depuis la salle de contrôle
- ne nécessite pas d'alimentation supplémentaire lors de l'utilisation du PoE
- installation facile sur n'importe quel panneau
- possibilité de connecter des éléments indicateurs puissants - pictogrammes lumineux (également avec des ampoules)
- DTMF utilisant RFC-2833, inband ou SIP INFO

Versions de produit

Unités de base de la conception universelle

Ces unités sont conçues pour être installées derrière le panneau de l'ascenseur, qui est préalablement préparé pour leur installation.

Numéro de référence : 921640E

2N LiftIP 2.0 COP unit, EN

Numéro de référence : 921640XE

2N LiftIP 2.0 COP unit, EN, Cable version

Comprend deux DEL (verte et jaune), un microphone et un haut-parleur reliés par des câbles.

Numéro de référence : 921618BE

2N LiftIP 2.0 COP unit – Flush mounting, EN, With button

Les unités dotées d'un boîtier en acier inoxydable sont conçues pour être installées dans le panneau de l'ascenseur.

Numéro de référence : 921618E

2N LiftIP 2.0 COP unit – Flush mounting, EN, Without button

Les unités dotées d'un boîtier en acier inoxydable sont conçues pour être installées dans le panneau de l'ascenseur.

Unités de base dans la conception des COT

- **Numéro de référence : 921630E**

  2N LiftIP 2.0 TOC unit, EN

  Les unités en boîtier métallique sont conçues pour être installées sur la cabine d'ascenseur.

  Unités de base dans la conception des COT

Numéro de référence : 921630E

2N LiftIP 2.0 TOC unit long, EN

Kit de base avec interrupteur pour le raccordement d'une station d'alarme vocale 2N dans un boîtier métallique

Comprend deux DEL (verte et jaune), un microphone et un haut-parleur reliés par des câbles.

Les unités en boîtier métallique sont conçues pour être installées sur la cabine d'ascenseur.

Accessoires

Numéro de référence : 921661E

2N Voice Alarm Station – Switch

Interrupteur pour connecter des sons avec 2N LiftIP 2.0

Numéro de référence : 921001SET

2N Voice Alarm Station Set

Le kit comprend 2 stations d'alarme vocale 2N et 1 station d'alarme vocale 2N — Switch

Numéro de référence : 921623E

Prolongateur de relais 2N LiftIP 2.0

Extendeur pour 1 extension de sortie

Description et installation

Dans ce chapitre, nous décrivons le produit **2N LiftIP 2.0** et son installation.

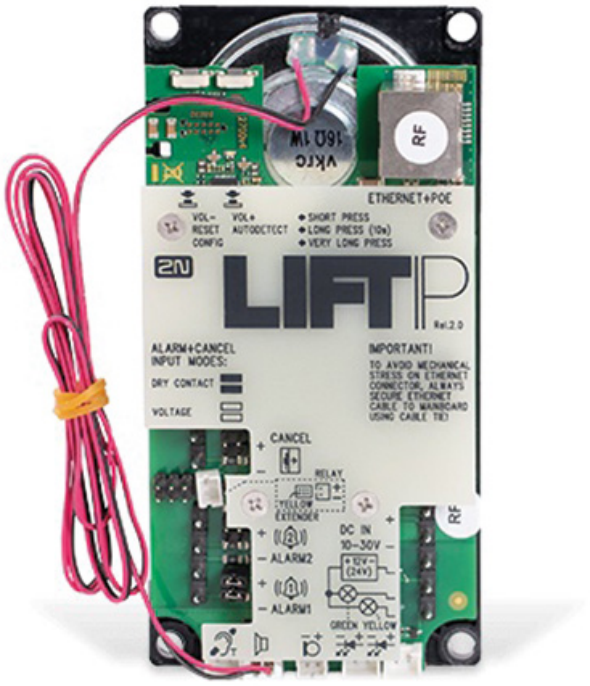
Le 2N LiftIP 2.0 est un communicateur d'urgence pour ascenseurs qui permet la transmission d'un son en duplex intégral à l'aide de la technologie VoIP directement à partir de la cabine de l'ascenseur. Un microphone et un haut-parleur situés derrière le panneau de l'ascenseur sont utilisés pour la communication bidirectionnelle. Comprend des bornes pour la connexion de l'alimentation externe, un bouton ALARME, des pictogrammes lumineux (états de l'appareil selon la norme) et une entrée ANNULER (signal d'ouverture de la porte de la cabine en option).

Fonctionnement de l'équipement

Appuyez sur la touche ALARM. Le pictogramme **Wait** s'allume immédiatement, une fois la communication établie, le pictogramme **Connection established** s'allume.

Conception universelle

La carte électronique est placée entre le panneau de montage et le couvercle imprimé avec les instructions (voir figure). Les dimensions totales sont (L) 65 x (H) 130 x (P) 24 mm. Le haut-parleur, le microphone et deux DEL (vertes et jaunes) sont connectés sur la carte mère (selon le numéro de commande). Sur le côté gauche, les cavaliers de court-circuitage (cavaliers) sont connectés ; ils se trouvent dans l'emballage du produit. Les petits connecteurs situés en bas servent à brancher la bobine d'induction (pour les malentendants) et les diodes électroluminescentes. Des pictogrammes lumineux sont généralement apposés sur ce produit (des pictogrammes incandescents sont également possibles). Les pictogrammes, ainsi que le bouton ALARME, ne sont pas inclus (ce sont des éléments de conception de l'ascenseur).



Exécution de la COP

La carte électronique est située sous le panneau en acier inoxydable avec des pictogrammes (voir photo). Les dimensions totales sont (L) 100 x (H) 220 x (P) 26 mm. Haut-parleur, microphone et LED inclus. Sur le côté gauche, les cavaliers de court-circuitage (cavaliers) sont connectés ; ils se trouvent dans l'emballage du produit. Pour la connexion de la bobine d'induction (pour les malentendants), il y a un connecteur en bas.

Exécution du COT

La carte électronique est logée dans un boîtier métallique (voir figure). Les dimensions d'encombrement sont de (L) 82 x (H) 186 x (P) 33 mm pour la version de base et de (L) 82 x (H) 257 x (P) 33 mm pour la version longue avec 2N Voice Alarm Station. Le haut-parleur et le microphone sont montés sur le panneau. Le haut-parleur, le microphone et deux DEL (vertes et jaunes) sont connectés sur la carte mère (selon le numéro de commande). Sur le côté gauche, les pinces (à enfiler) sont connectées, elles se trouvent dans l'emballage du produit. Les petits connecteurs situés en bas servent à brancher la bobine d'induction (pour les malentendants) et les diodes électroluminescentes. Des pictogrammes lumineux sont généralement apposés sur ce produit (des pictogrammes incandescents sont également possibles). Les pictogrammes, ainsi que le bouton ALARME, ne sont pas inclus (ce sont des éléments de conception de l'ascenseur).

Avant de commencer l'installation

Avant de commencer votre installation, vérifiez si le contenu de l’emballage du produit est complet.

Contenu du paquet

- **2N LiftIP 2.0**
- 4x pince de connexion multiple
- 6x cavalier de court-circuitage
- 1x haut-parleur et microphone
- 2x câble avec LED
- 3x autocollant
- 5 ceintures à cordon de serrage
- 1x Certificate of Ownership
- 1x mode d’emploi abrégé

NOTE
La quantité et le type d'accessoires peuvent varier selon le numéro de commande.

Conditions d'installation 2N LiftIP 2.0

- **2N LiftIP 2.0** n'est pas destiné à être utilisé à l'extérieur.

- Le produit se connecte au réseau local.
- Si nécessaire, une protection contre les dommages mécaniques, l'eau, la poussière et d'autres influences négatives doit être assurée par l'entreprise chargée de l'installation.
- La surface de montage du communicateur doit être plane, voir le chapitre Installation mécanique (p. 13) pour plus de détails.

ATTENTION
L'installation et le réglage de cet appareil, y compris toute manipulation de cet appareil, doivent être effectués uniquement par des personnes qualifiées.

NOTE
2N LiftIP 2.0 reçoit une adresse IP du serveur DHCP après s'être connecté au réseau.

Conception universelle

Vérifiez que le panneau de levage est prêt pour l'installation **2N LiftIP 2.0**.

Installation mécanique

ATTENTION
L'emplacement, l'aspect et le marquage des commandes du communicateur (par exemple, le bouton ALARM) doivent être conformes aux normes applicables aux ascenseurs.

Conditions d'installation

- Le panneau doit être prêt à être installé, avec au moins une perforation pour le haut-parleur.
- Le panneau doit être équipé des éléments prescrits :
  - Bouton ALARME ;
  - Pictogramme lumineux **Demande acceptée**;
  - pictogramme lumineux **Connexion établie**.
- L'emplacement de tous ces éléments doit être conforme à la réglementation.
- Il doit y avoir un espace libre derrière le panneau de min. (L) 65 x (H) 130 x (P) 25 mm.

Localisation 2N LiftIP 2.0

Le 2N LiftIP 2.0 peut être monté dans n'importe quelle position. Le positionnement optimal **2N LiftIP 2.0** se situe approximativement à la hauteur de la bouche d'un adulte. **Le 2N LiftIP 2.0** est destiné à être installé dans des endroits où tout contact avec l'opérateur est exclu (voir l'avis de sécurité).

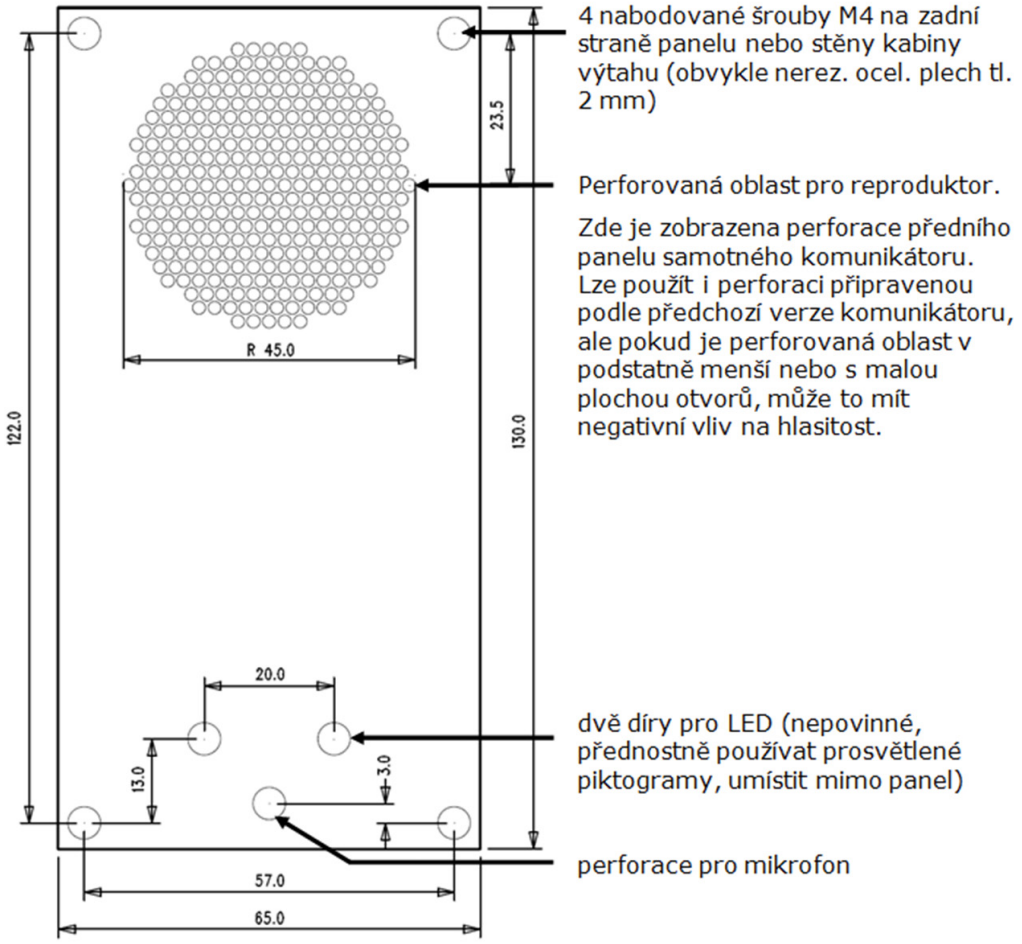
ATTENTION
L'installation d'appareils électroniques sans panneau de montage n'est pas recommandée, auquel cas le fabricant ne peut garantir la sécurité. Le panneau sert d'isolant électrique.

Installation du panneau avec l'électronique 2N LiftIP 2.0

Pour monter le panneau sur la planche de l'ascenseur, les éléments suivants sont nécessaires :

- 4 vis M4 à l'intérieur avec un pas de (L) 57 x (H) 122 mm
- La surface perforée pour le haut-parleur est suffisante - elle peut être plus grande que sur la photo, mais **ne doit pas dépasser les dimensions du panneau**, ce qui créerait un court-circuit acoustique.
- trou de microphone
- éventuellement des trous pour 2 LED

Schéma d'installation pour la version avec haut-parleur de 50 mm



En cas de montage autre que sur les vis prescrites, assurez une distance d'isolation d'au moins 2 mm entre l'électronique et les fixations non standard. Le panneau de montage doit être monté de manière à ce qu'il n'y ait pas de résonance lorsque le produit est en fonctionnement. Il ne doit pas y avoir d'espace entre la carte et le panneau **2N LiftIP 2.0** ou il doit être scellé pour éviter un court-circuit acoustique du haut-parleur et un couplage acoustique entre le haut-parleur et le microphone (voir ci-dessous).

ATTENTION
Veillez toujours à ce que l'ouverture du microphone soit étanche par rapport à l'environnement, c'est-à-dire qu'elle capte les sons de la cabine et non ceux de la gaine ou de la cavité située derrière la planche.

Installation de la variante TOC 2N LiftIP 2.0

La variante TOC peut être installée sur la cabine d'ascenseur. Le boîtier métallique de l'appareil est fixé à des vis idéalement plus petites que le trou lui-même, qui a un diamètre de 0,8 mm. Utilisez des vis à tête plate seules ou des vis à tête conique en combinaison avec une rondelle appropriée. Fixez l'appareil à l'emplacement d'installation choisi, en marquant les trous comme points de placement des vis.

ATTENTION

- L'utilisation d'une taille de vis supérieure à celle recommandée peut entraîner une situation où l'appareil ne peut pas être facilement retiré des vis et où les vis doivent être dévissées.
- Dans le cas contraire, si vous utilisez des vis trop petites, le dispositif de suspension risque de ne pas tenir fermement.

Montage du microphone à l'extérieur du panneau

Le microphone est normalement placé directement sur le PCB **2N LiftIP 2.0** (voir le dessin ci-dessus). Dans la version câblée, le microphone externe est monté sur un support de 25 mm de diamètre avec une feuille autocollante, et le microphone est connecté par un câble standard au connecteur correspondant sur la carte mère. L'autocollant permet de monter le microphone derrière n'importe quel trou de la carte (le diamètre minimum du trou est de 3 mm ou un groupe de trous plus petits ayant la même surface totale). Les dimensions détaillées du microphone externe sont disponibles dans le fichier. **La distance minimale entre le centre du haut-parleur et celui du microphone est de 90 mm.** À des distances plus faibles, un couplage acoustique pourrait se produire. L'éloignement n'est pas une mauvaise chose.

Lorsque l'appareil fonctionne, la modification de l'état de connexion du microphone externe ne change pas. L'état actuel du microphone externe n'est détecté qu'au démarrage/redémarrage de l'appareil.

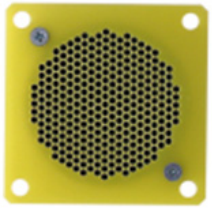
Installation du haut-parleur à l'extérieur du panneau

Le haut-parleur est relié par un câble standard au connecteur approprié de la carte mère. Les dimensions détaillées du haut-parleur externe sont disponibles dans le fichier
. La longueur du câble permet un placement optionnel jusqu'à 1 m de la carte mère **2N LiftIP 2.0**. **Dans ce cas, veillez à**

ATTENTION

Si le joint du haut-parleur est placé séparément, veillez à ce qu'il n'y ait pas de court-circuit acoustique entre l'avant et l'arrière du haut-parleur - la grille ne doit jamais dépasser les dimensions du haut-parleur, car cela provoquerait un court-circuit acoustique !

DANGER
Le haut-parleur de 50 mm ne peut être monté que sur une surface isolante (non métallique). Dans le cas contraire, un panneau externe doit être demandé, voir l'image ci-dessous (non inclus).



ATTENTION
Nous ne recommandons pas de placer le microphone et le haut-parleur à des endroits complètement différents dans la cabine, par exemple le haut-parleur au plafond et le microphone au mur, car les utilisateurs devraient facilement repérer l'emplacement du haut-parleur (grille, perforation) et ensuite chercher le microphone dans lequel ils parlent à proximité.

ATTENTION
S'il y a un retour entre le microphone et le haut-parleur (écho) au volume maximum, nous vous recommandons de réduire le volume du haut-parleur.

Conseils pour obtenir des propriétés acoustiques idéales

Afin d'atteindre la pression acoustique minimale requise pour satisfaire aux exigences de la norme EN 81-28:2015, les ouvertures dans le panneau recouvrant le haut-parleur du communicateur doivent occuper au moins 20 % de la surface du haut-parleur et être situées devant le haut-parleur.

Le haut-parleur et le microphone doivent être bien ajustés contre le panneau de recouvrement. Si cela n'est pas possible en raison de l'irrégularité de la surface du panneau, nous vous recommandons d'utiliser un

joint d'enceinte pour éviter que le son de l'enceinte ne s'infiltre dans l'espace situé derrière le panneau. Une bonne étanchéité du microphone est importante pour obtenir une bonne qualité de son et une bonne clarté.

Lors du montage, essayez de minimiser le couplage acoustique entre le microphone et le haut-parleur.

ATTENTION
Si vous testez le panneau de commande de la cabine à l'extérieur de l'ascenseur (par exemple sur une table), le son peut sembler trop faible. Cela est dû à l'absence de barre de son et aux propriétés acoustiques du panneau de l'ascenseur. Le volume final ne correspond qu'à l'installation correcte de l'appareil.

Installation des éléments indicateurs

Il existe trois options pour l'indication de l'état **2N LiftIP 2.0**:

1. Pictogrammes lumineux faisant partie du tableau de commande de la cabine.
2. LEDs directement sur l'électronique **2N LiftIP 2.0**.
3. Deux LED (jaune, vert) sont connectées à l'électronique de la version du câble **2N LiftIP 2.0**.

NOTE
La méthode d'indication doit être choisie en fonction de la législation en vigueur. Pour la fonction réelle **2N LiftIP 2.0** (communication), il n'est cependant pas nécessaire de connecter les éléments indicateurs.

Connexion

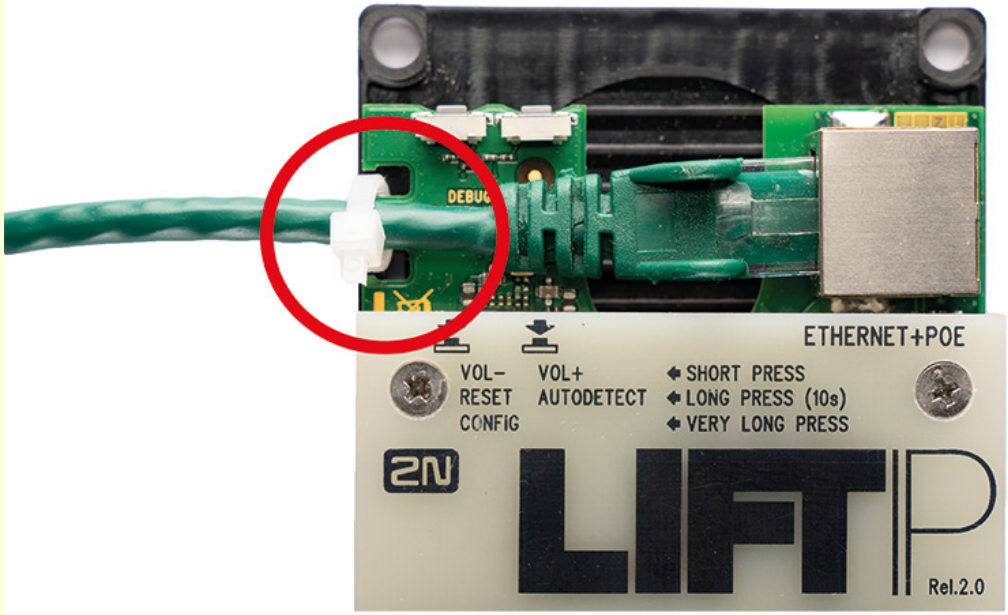
Connexion de 2N LiftIP 2.0 au réseau

Le 2N LiftIP 2.0 est connecté au réseau (LAN) à l'aide d'un câble UTP Cat-5e ou supérieur terminé par une prise RJ-45 (connecteur LAN). **Le 2N LiftIP 2.0** peut être alimenté par PoE ou par une alimentation externe (DC 10-30 V, 0,5 A). Lorsqu'il est connecté au réseau local, le **2N LiftIP 2.0** reçoit une adresse IP du serveur DHCP.

Vous pouvez également trouver l'adresse IP à l'aide de l'application 2N Network Scanner, qui comprend un scanner de réseau. Pour des informations plus détaillées, voir Recherche de l'adresse IP à l'aide de 2N Network Scanneru.

2N LiftIP 2.0 reçoit les DTMF par défaut en utilisant RFC-2833 ou le détecteur peut être réglé sur in-band ou SIP INFO.

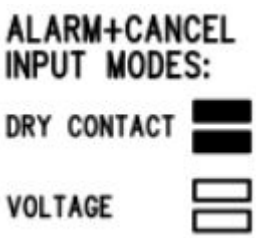
ATTENTION
Pour éviter toute contrainte mécanique sur le connecteur, fixez le câble Ethernet à la carte mère à l'aide d'un collier de serrage.



Raccordement du bouton ALARM1/2 - commande par contact

DANGER
Le bouton doit être sûr - les contacts du bouton ne doivent pas être reliés à d'autres circuits. Si ces conditions ne sont pas remplies, utilisez le contrôle de la tension.

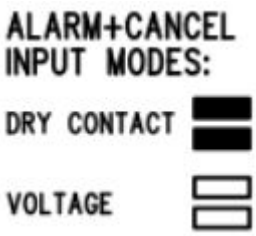
1. Connectez les contacts du bouton à la borne ALARM. L'alarme est réglée en usine comme une alarme de commutation (les deux cavaliers sont réglés).
2. Le bouton peut avoir un contact de commutation et un contact d'ouverture. Dans le cas d'un contact extensible, la fonction du bouton doit être inversée dans la configuration web de l'appareil, voir Entrées logiques (p. 66).



Connexion du bouton ALARM1/2 - contrôle de la tension

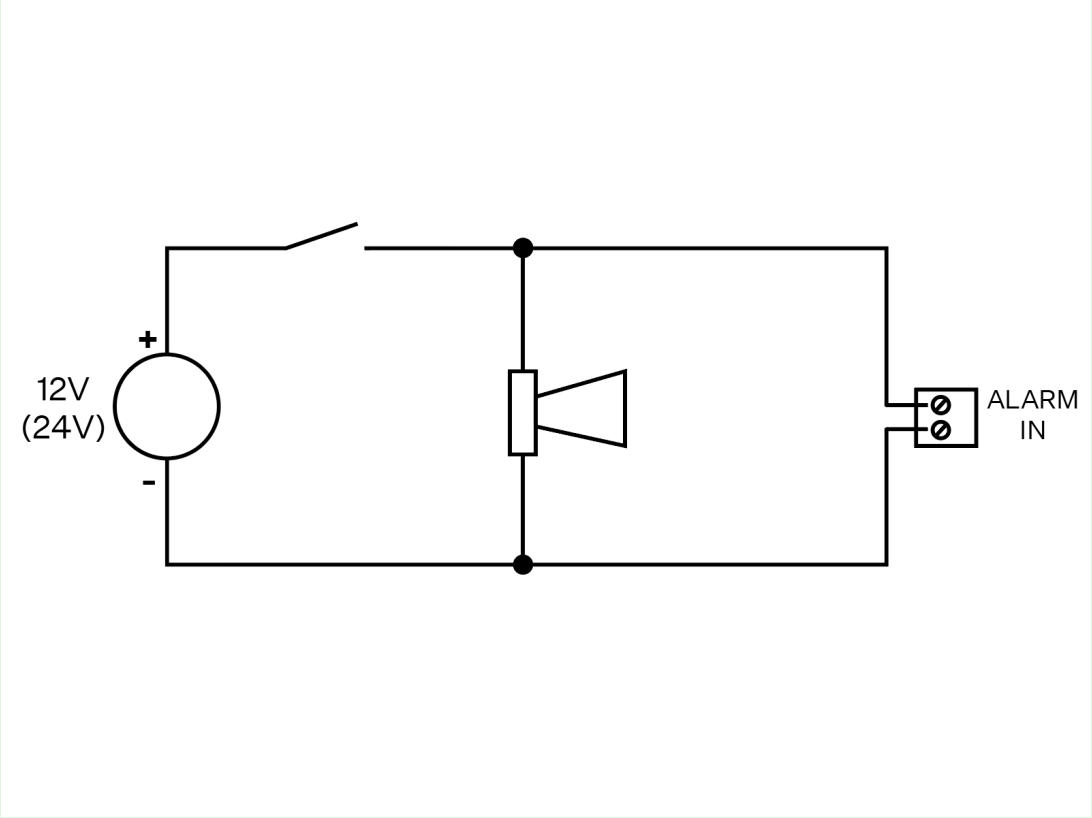
ASTUCE
Une tension continue comprise entre 5 et 48 V peut être utilisée. Toutefois, cette alimentation doit être protégée contre les pannes de courant.

1. L'activation peut se produire en connectant ou en déconnectant cette tension. L'alarme est réglée en usine pour une commutation de contact.
2. Pour la commande de l’alarme par connexion d’une tension retirez tous les jumpers du connecteur de configuration.



AVERTISSEMENT
Respectez la polarité (voir l'impression sur le couvercle).

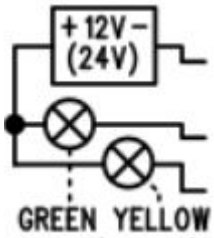
ASTUCE
Voici un exemple de branchement du bouton d'alarme avec sirène.



Câblage des éléments indicateurs

Câblage de base

Dans ce circuit, il est possible d'utiliser n'importe quel élément d'indication (par exemple des pictogrammes lumineux). L'utilisation d'une source externe permet de garantir une luminosité suffisante des éléments indicateurs. **2N LiftIP 2.0** ne contient que des interrupteurs, toute limitation de courant, par exemple lors de l'utilisation de LED, doit être assurée par le circuit connecté.



Exigences

- Alimentation 12-24 V (sauvegardée si l'indication doit fonctionner même en cas de panne de courant).

AVERTISSEMENT
Attention, il est nécessaire de respecter la polarité de l'alimentation électrique !

- Courant continu max. 200 mA (les ampoules peuvent être connectées).
- Les deux éléments indicateurs doivent être connectés !

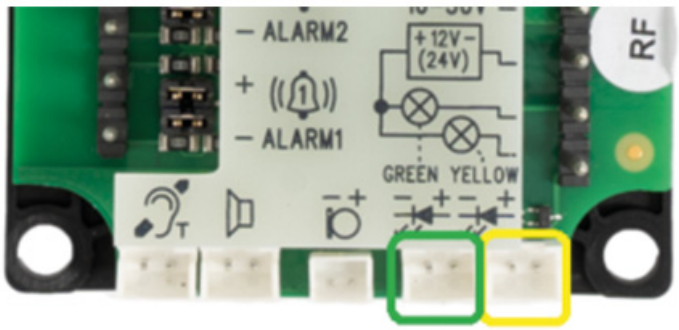
Utilisation de LED montées directement sur l'électronique 2N LiftIP 2.0

Dans ce cas, les DEL sont montées directement sur l'électronique et aucun autre câblage n'est nécessaire.

DEL connectées par câble

NOTE
Si les LED de signalisation sont reliées par câble, le positionnement correct de l'élément de signalisation et la forme des pictogrammes utilisés relèvent de la responsabilité de l'entreprise qui installe le dispositif.

Peut être utilisé lorsque les pictogrammes lumineux ne sont pas disponibles. Ces DEL font partie des accessoires de la version câblée de l'appareil. Il s'agit d'une LED de 5 mm de diamètre à très haute intensité lumineuse.



Exigences

- Respectez la polarité des DEL (voir l'impression sur le couvercle).
- Observez les couleurs : confirmation de la demande - jaune, confirmation de la connexion - vert.

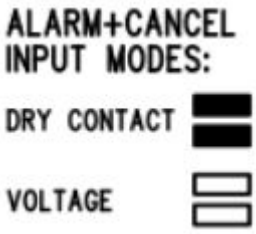
NOTE
Lorsque vous utilisez ce circuit, la LED sur le PCB ne s'allume pas.

Connexion de l'entrée CANCEL (contact de porte, en option)

ATTENTION
L'interrupteur de porte ou le signal d'ouverture de porte ne doit indiquer une porte ouverte que si les portes intérieure et extérieure de l'ascenseur sont ouvertes et que la cabine peut effectivement être sortie.

Commande de l‘interrupteur

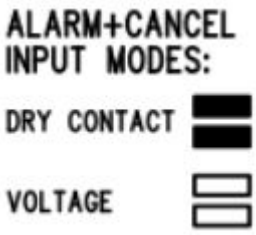
1. Connectez l'interrupteur à la borne CANCEL.
2. En usine, **2N LiftIP 2.0** est réglé sur la commutation de contact. Les deux cavaliers sont montés sur le cavalier de configuration.
3. L'option CANCEL peut également être activée sur le contact d'ouverture. Dans le cas d'un contact d'expansion, la fonction de l'entrée CANCEL doit être inversée dans la configuration web de l'appareil, voir Entrées logiques (p. 66).



Commande par tension

Une tension continue comprise entre 5 et 48 V DC peut être utilisée.

1. Pour contrôler la connexion de tension, retirez les deux cavaliers du cavalier de configuration.
2. Pour contrôler par désexcitation, vous devez inverser la fonction de l'entrée CANCEL dans la configuration web de l'appareil, voir Entrées numériques (p. 66).



ATTENTION
Si la présence de tension indique **une porte** fermée, cette alimentation doit être protégée contre les pannes de courant.

AVERTISSEMENT
Respectez la polarité (voir l'impression sur le couvercle).

Connexion de la boucle d'induction

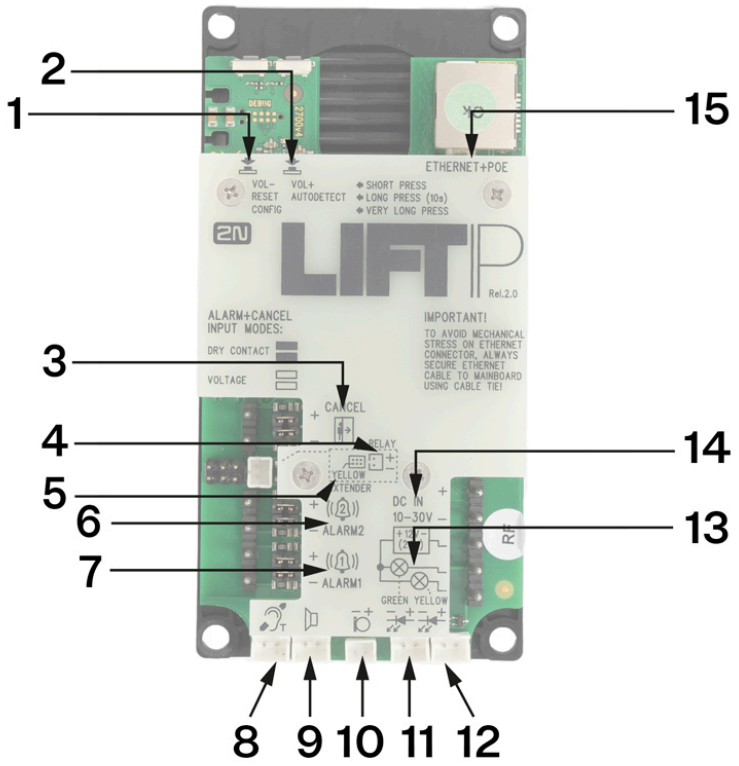
Lors de l'installation du communicateur, il est nécessaire de respecter les réglementations en vigueur, qui peuvent stipuler l'installation d'une boucle auditive comme élément obligatoire du communicateur dans la cabine d'ascenseur. La boucle se connecte au connecteur situé à l'arrière de **2N LiftIP 2.0**. La polarité est arbitraire. Après accord, elle peut être incluse dans la livraison, avec un câble de 4 m compris.

Exigences

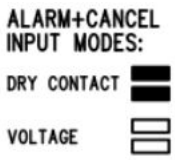
- Il est recommandé de placer la boucle d'induction derrière un élément de couverture non métallique et non magnétique afin d'éviter la détérioration du rayonnement du champ de la boucle d'induction.
- La boucle d’induction doit être marquée du pictogramme approprié (oreille) et son emplacement doit être conforme aux normes applicables.

Description des bornes, des cavaliers, des connecteurs et des diodes électroluminescentes (DEL)

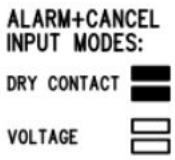
Description des bornes et des connecteurs



1	Bouton **VOL-**, **RESET**, **CONFIG**	Appuyez brièvement sur (**VOL-**) pour réduire le volume du haut-parleur. Appuyez longuement sur (**RESET**) - après environ 10 s, l'appareil redémarre. Appui très long (**CONFIG**) - utilisé pour détecter l'adresse IP de l'appareil, basculer l'adresse IP en mode statique ou dynamique et rétablir les paramètres d'usine d'origine de l'appareil.
2	Bouton **VOL+**, **AUTODETECT**	Appuyez brièvement sur (**VOL+**) pour augmenter le volume du haut-parleur. Appui long (**AUTODETECT**) - après environ 10 s, la polarité par défaut des entrées ALARM1/2 est réglée.

Description des bornes et des connecteurs					
3	**Pince CANCEL**	Contrôlé par contact	Contact de commutation (par défaut)	Le réglage se fait via des connecteurs de configuration (jumpers). **Contact de commutation**: les deux cavaliers sont engagés.	
			Contact d'ouverture	**Contact séparé**: les deux cavaliers sont déployés et la polarité d'entrée est inversée dans la section de configuration du logiciel de Entrées logiques (p. 66).	
		Contrôlé par tension	En connectant une tension continue de 5-48 V	Contrôlez **en connectant la tension**: aucun cavalier de polarité n'est déployé et l'entrée est inversée dans la section de configuration du logiciel, voir Entrées logiques (p. 66).	
			En interrompant la tension continue de 5-48 V	Contrôlez **en interrompant la tension**: aucun cavalier n'est déployé.	
4	Connecteur **RELAIS**		Connecteur pour connecter **2N LiftIP 2.0** relais d'extension.		

Description des bornes et des connecteurs		
5	**EXTENDER JAUNE** (connecteur à 6 broches)	Utilisé pour connecter 2N Voice Alarm Station.

Description des bornes et des connecteurs					
6/7	Clamp **ALARM1/2**	Contrôlé par contact	Contact de commutation (par défaut)	Le réglage se fait via des connecteurs de configuration (jumpers). **Contact de commutation**: les deux cavaliers sont engagés.	
			Contact d'ouverture	**Contact divisé**: les deux cavaliers sont installés et la polarité d'entrée est inversée dans la section de configuration du logiciel, voir Entrées logiques (p. 66) Inversion d'entrée.	
		Contrôlé par tension	En connectant une tension continue de 5-48 V	Contrôlez **en connectant la tension**: aucun cavalier n'est déployé et la polarité d'entrée est inversée dans la section de configuration du logiciel, voir Entrées logiques (p. 66).	
			En interrompant la tension continue de 5-48 V	Contrôlez **en interrompant la tension**: aucun cavalier n'est déployé.	

Description des bornes et des connecteurs			
8	Connecteur **boucle d'induction**	La boucle d'induction n'est pas incluse en standard. Il doit être installé derrière un couvercle non conducteur et non magnétique. La polarité n'a pas d'importance. *Notes :* • *Si le haut-parleur est monté derrière une enceinte non conductrice et non magnétique, il peut jouer le rôle d'une bobine d'induction dans une certaine mesure.* • *La sortie est protégée contre les courts-circuits. La puissance de sortie est limitée par la résistance.*	
9	**connecteur de haut-parleur**	Le haut-parleur est fourni branché sur ce connecteur.	
10	Connecteur pour microphone externe	Lorsque l'appareil fonctionne, la modification de l'état de connexion du microphone externe ne change pas. L'état actuel du microphone externe n'est détecté qu'au démarrage/redémarrage de l'appareil.	
11	Connecteur VERT "**Lien de suivi**"	LED verte	Les LED ne sont pas incluses en standard (version câblée uniquement). La connexion d'une LED externe ne désactive pas la LED de la carte.
12	Connecteur JAUNE "**Connexion établie**"	LED jaune	
13	Pinces pour le raccordement des éléments indicateurs **+ 12 V (24 V)**	Éléments indicateurs (pictogrammes lumineux) DC 12-24 V / 2x 200 mA alimentés par une source externe, il est nécessaire de respecter le schéma de câblage.	
14	Pince **DC IN 10-30 V**	Alimentation externe (si elle n'est pas alimentée par PoE)	DC 10-30 V
15	**ETHERNET + POE**	Connecteur RJ-45 (PoE selon 802.3af) pour une connexion LAN	

AVERTISSEMENT
Respectez la polarité des boutons ALARM et CANCEL commandés par la tension (voir l'impression sur le couvercle).

LED (face avant - pendant l'appel)

Couleur	État	Fonction	Description
Ambre	Il s'allume	Appel de suivi	Indique la connexion d'un appel d'alarme ainsi que le mode de libération en cours, si le mode est activé.
Vert	Il s'allume	Connexion établie	Signale l'établissement d'un appel d'alarme avec la possibilité de parler à l'autre partie. L'appel d'alarme est acquitté, l'appel entrant est décroché.
Jaune + Vert	Clignotement alternatif	Échec de l'appel de contrôle	Indique un échec de l'appel de contrôle. Si un autre appel commence, il est signalé, voir les cas ci-dessus. Lorsque l'appel est terminé, l'état de la signalisation redevient clignotant. La condition d'erreur est levée par l'acquittement de l'appel d'alarme (ALARM1 uniquement) ou par un appel de contrôle ultérieur réussi.
Sans signalisation lumineuse		État de veille	Indique l'état d'inactivité de l'appareil.

Fonctions des boutons

Les boutons situés en haut à gauche de la carte de l'unité de base sont utilisés pour régler les paramètres de base et pour contrôler l'appareil sans accéder à l'interface web de l'appareil.

Réglage du volume

Appuyez brièvement sur la touche VOL-/VOL+ pour diminuer/augmenter le volume du haut-parleur d'un niveau. Le réglage le plus bas/le plus haut du volume global de l'appareil est confirmé par un signal sonore.

Paramètres par défaut des entrées ALARM1/2

Une pression prolongée de 10 secondes sur le bouton marqué AUTODETECT détecte le type de contrôle d'entrée ALARM1/2. Les valeurs détectées seront inscrites dans la configuration du logiciel. Au moment de l'autodétection, le type de contrôle d'entrée est traité comme un état de repos. Le rétablissement des paramètres d'entrée par défaut est indiqué par un signal sonore.

Redémarrer l’appareil

Une pression prolongée d'environ 10 secondes sur le bouton marqué RESET redémarre l'appareil sans modification de la configuration.

NOTE
L'intervalle de temps entre une pression prolongée sur le bouton RESET et la reconnexion de l'appareil au réseau après un redémarrage est de plusieurs dizaines de secondes.

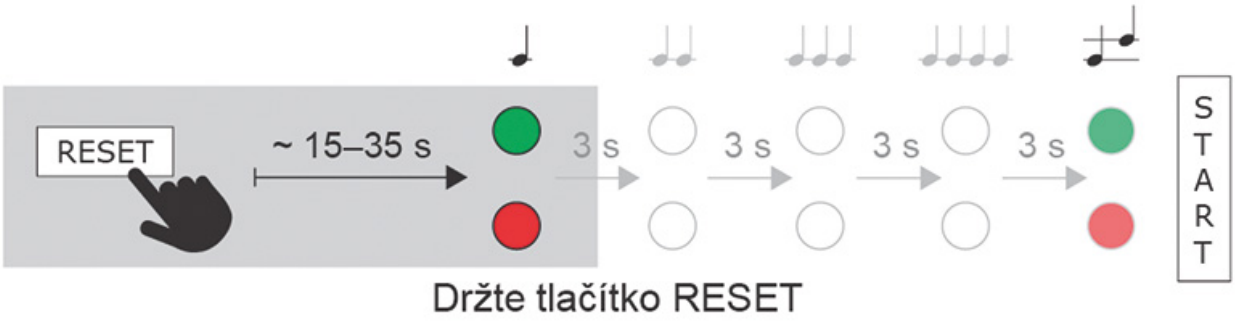
l'adresse IP, la modifier et réinitialiser l'appareil aux paramètres d'usine

Le bouton de gauche VOL-/RESET/CONFIG, situé en haut à gauche de la base, permet de déterminer l'adresse IP de l'appareil, de passer en mode statique ou dynamique et de rétablir les paramètres d'usine d'origine de l'appareil,

Trouver l'adresse IP

Suivez les instructions suivantes pour **identifier l'adresse IP** de l'apparei :

1. Appuyez sur le bouton RESET.
2. Attendez que les LED rouge et verte s'allument simultanément et d'entendre le signal sonore (approx. 30 s).
3. Relâchez le bouton RESET.
4. L'appareil annoncera automatiquement son adresse IP.



NOTE
L'intervalle de temps entre la pression sur le bouton RESET de et le premier signal lumineux et sonore est d'environ 30 s.

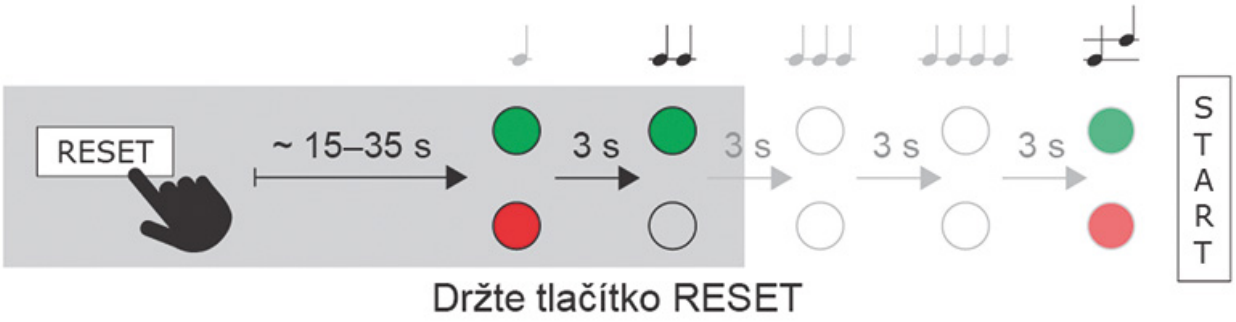
Attribution d'une adresse IP statique

Suivez les instructions suivantes pour passer l'appareil en **adresse IP statique** (DHCP OFF) :

1. Appuyez sur le bouton RESET.
2. Attendez que les LED rouge et verte s'allument simultanément et d'entendre le signal sonore (approx. 30 s).
3. Attendez que la LED rouge s'éteigne et d'entendre le signal sonore (approx. 3 s).
4. Relâchez le bouton RESET.

Après le redémarrage, les paramètres de l'interphone seront :

- Adresse IP: 192.168.1.100
- Masque de réseau: 255.255.255.0
- Passerelle par défaut: 192.168.1.1



Suivez les instructions suivantes pour passer l'appareil en **adresse IP dynamique** (DHCP ON) :

Attribution d'une adresse IP Dynamique

1. Appuyez sur le bouton RESET.
2. Attendez que les LED rouge et verte s'allument simultanément et d'entendre le signal sonore ♩ (approx. 30 s).
3. Attendez que la LED rouge s'éteigne et d'entendre le signal sonore (approx. 3 s).
4. Attendez que la LED verte s'éteigne et que la LED rouge se rallume et d'entendre le signal sonore ♩♩♩ (approx. 3 s).
5. Relâchez le bouton RESET.

Retour aux paramètres d'usine

Pour **renouveler le réglage original d'usine** de l'appareil, suivez le processus suivant :

1. Appuyez sur le bouton RESET.
2. Attendez que les LEDs rouge et verte s'allument simultanément et d'entendre le signal sonore (approx. 30 s).
3. Attendez que la LED rouge s'éteigne et d'entendre le signal sonore (approx. 3 s).
4. Attendez que la LED verte s'éteigne, que la LED rouge se rallume et d'entendre le signal sonore (approx. 3 s).
5. Attendez que la LED rouge s'éteigne et d'entendre le signal sonore (approx. 3 s).
6. Relâchez le bouton RESET.

2N Lift Voice Alarm Station

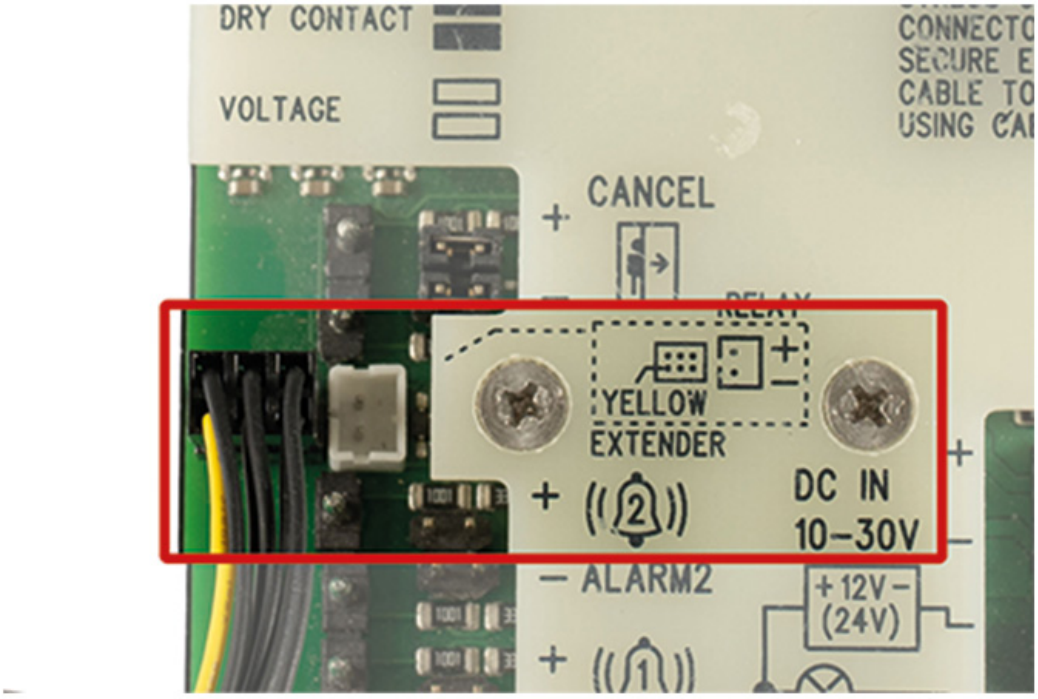
2N Voice Alarm Station est utilisée pour élargir **2N LiftIP 2.0** afin d'inclure un point d'appel sur le toit de la cabine et sous la cabine. Il est équipé de son propre microphone, haut-parleur et un bouton d'urgence. La connexion est assurée par un switch qui relie **2N LiftIP 2.0** à un ou deux points d'appel.

Instalace 2N Voice Alarm Station

1. Lors de la connexion de 2N Voice Alarm Station, déconnectez **2N LiftIP 2.0** de l'alimentation électrique.

2. Mettez la prise à 6 broches du câble de connexion du switch dans le connecteur à 6 broches marqué EXTENDER sur 2N LiftIP 2.0. Respectez l'orientation correcte de la connexion pour le fil jaune.

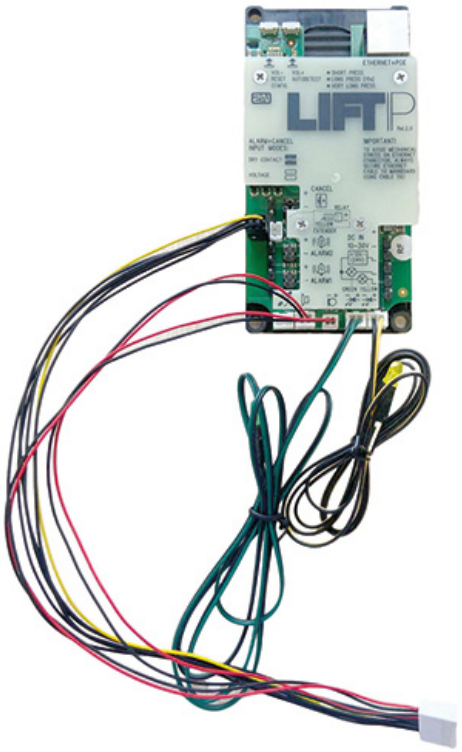
AVERTISSEMENT
Un mauvais branchement peut endommager le module.



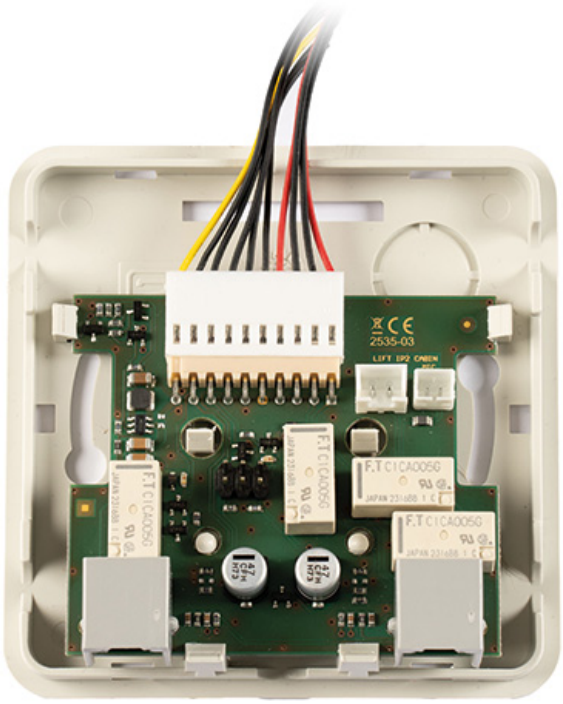
3. Déconnectez le haut-parleur et le microphone des connecteurs (microphone externe, le cas échéant) du **2N LiftIP 2.0**.

ATTENTION
Lorsque l'appareil fonctionne, la modification de l'état de connexion/déconnexion du microphone externe ne change pas. L'état actuel du microphone externe n'est détecté qu'au démarrage/redémarrage de l'appareil.

4. Connectez les connecteurs du câble de connexion du switch au connecteur du microphone et du haut-parleur du **2N LiftIP 2.0** (les connecteurs pour la connexion du microphone et du haut-parleur ont chacun une taille différente et les pictogrammes sont indiqués sur le couvercle du **2N LiftIP 2.0**, ils ne sont donc pas interchangeables).

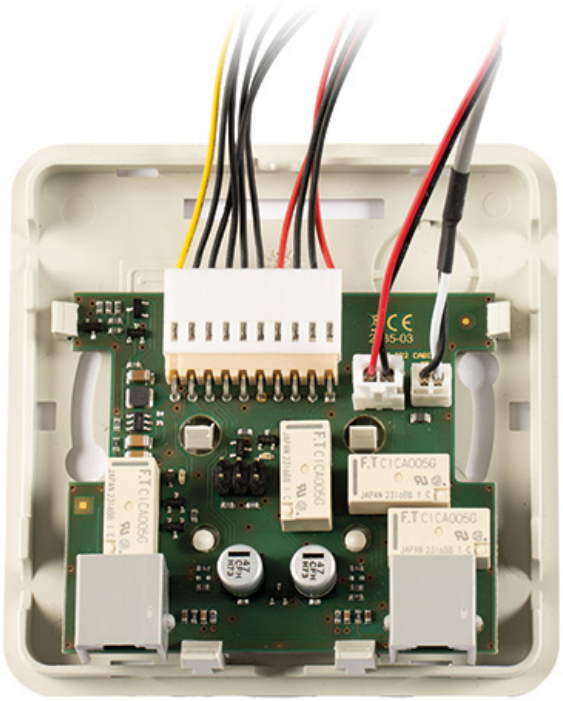


5. Retirez le couvercle du switch. En insérant la prise du câble de connexion dans le connecteur à 10 broches du switch, le switch et **2N LiftIP 2.0** sont connectés.



6. Connectez le microphone et le haut-parleur qui étaient à l'origine déconnectés du **2N LiftIP 2.0**, aux connecteurs du switch. Les connecteurs pour la connexion sont marqués, SPK pour le haut-parleur et MIC pour le microphone.

> **AVERTISSEMENT**
> Si vous utilisez la version câble de **2N LiftIP 2.0**, connectez le microphone du câble au connecteur MIC du switch, sinon ce connecteur n'est pas connecté.



7. Percez un trou sur le bord supérieur du couvercle du switch pour faire passer les câbles. Selon l'emplacement de l'installation, les câbles peuvent également être acheminés à travers un trou créé en perçant le trou situé dans le coin supérieur droit à l'arrière du couvercle du switch. Après avoir sélectionné la méthode d'acheminement des câbles, fermez le switch à l'aide du couvercle supérieur. Dans la partie inférieure du switch, il y a un connecteur RJ-12 de chaque côté pour la connexion des points d'appel. Utilisez le câble fourni avec le point d'appel pour connecter le point d'appel au switch. Le connecteur pour la connexion est situé sur le côté droit du point d'appel, sous le couvercle pliant. Fixez le couvercle pliant après avoir connecté le câble à l'aide de la vis fournie.
8. Une fois l'installation terminée, rebranchez **2N LiftIP 2.0** à l'alimentation électrique.

> **NOTE**
> Le connecteur à 6 broches de la carte du switch est utilisé pour les diagnostics avancés du hardware à des fins de service, il ne fournit aucune fonction à l'utilisateur normal.

Configuration

L'acheminement des appels à partir de 2N Voice Alarm Station est défini dans l'interface de configuration web du dispositif **2N LiftIP 2.0**, auquel 2N Voice Alarm Station est connecté. Les réglages sont effectués dans le menu **Appel > Appel d'alarme > Appel d'alarme 2**.

La liste des événements de l'appel d'alarme 2 est inscrite dans le menu de configuration **État > Événements**.

AVERTISSEMENT
Si la destination de l'Appel d'alarme 2 n'est pas remplie, l'appel ne peut pas être effectué. Il est possible d'avoir le même utilisateur que pour le bouton ALARM1.

Commande

Activation par pression courte sur Appuyez sur pour appeler sur la station d'alarme vocale 2N. L'appel est établi à la destination de l'appel d'alarme ALARM2 de **2N LiftIP 2.0**.

NOTE
Le point d'appel 2N Voice Alarm Station ne comporte pas de LED indiquant qu'une connexion est en cours d'établissement. Lors de l'établissement de l'appel et après la confirmation de la connexion, la LED du point d'appel **2N LiftIP 2.0** s'allume.

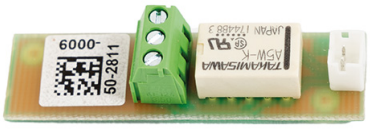
Dimensions 2N Voice Alarm Station :

Point d'appel 2N Voice Alarm Station **:** 225 x 87 x 67 mm

Switch: 81 x 81 x 30 mm

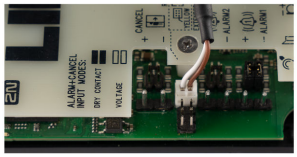
2N LiftIP 2.0 Relay extender

2N LiftIP 2.0 Relay extender permet d'étendre **2N LiftIP 2.0** de 1 sortie. Le type de sortie relais permet de commuter les deux polarités de tension. La sortie de blocage est déconnectée/connectée selon la méthode de connexion s'il n'est pas possible d'établir un appel d'urgence à partir de **2N LiftIP 2.0** (le numéro dans la configuration pour le bouton Alarme n'est pas rempli ou il n'y a pas d'enregistrement au serveur SIP, sauf dans le cas où un direct call (appel P2P) est réglé pour le bouton Alarme).



Connexion 2N LiftIP 2.0 Relais extender

Le prolongateur de relais 2N LiftIP 2.0 est branché sur le connecteur RELAY (voir pour une description des bornes, cavaliers, connecteurs et LEDs (p. 24)).



1. Lors de la connexion du prolongateur de relais 2NLiftIP 2.0, déconnectez le **2N LiftIP 2.0** de l'alimentation électrique (DC 10-30 V ou PoE).
2. Pour protéger les circuits contre les courts-circuits avec d'autres objets conducteurs 2NLiftIP 2.0 Relay extender **, insérez toujours le câble dans le tube isolant fourni et fixez-le à l'aide des languettes avant de l'installer !**

3. Connectez le câble **2N LiftIP 2.0** et le prolongateur 2N LiftIP 2.0 Relay.
4.

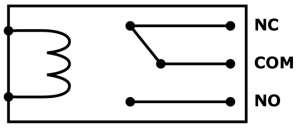
ATTENTION
Respectez la connexion correcte au connecteur (fil jaune). Un mauvais branchement peut endommager le module.

NOTE
L'état de la sortie relais en cas d'erreur est signalé de la même manière qu'en cas de déconnexion de l'appareil de l'alimentation électrique. La sortie du relais est désactivée.

Paramètres techniques 2N LiftIP 2.0 Relay extender

Sortie	
Puissance de commutation maximale	15 W
Tension de commutation maximale	30 V
Courant de commutation maximal	2 A
Type de sortie	isolée galvaniquement, permet de commuter les tensions des deux polarités

Schéma

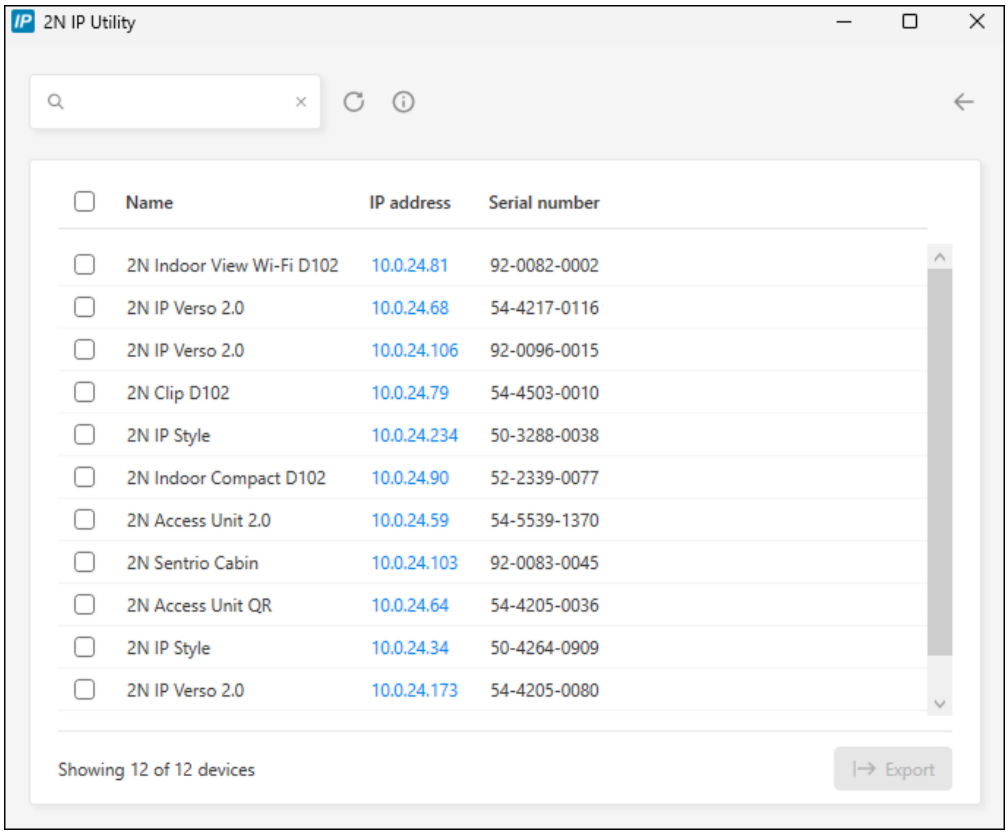


Exemple : En utilisant des contacts COM et NO, le relais connecte le circuit après avoir appliqué une tension à la bobine.

Recherche de l'adresse IP à l'aide de 2N IP Utility

Pour connaître l'adresse IP d'un appareil 2N sur votre réseau local, utilisez l'utilitaire 2N IP Utility. L'application 2N IP Utility peut être téléchargée sur le site web 2N.com. Pour l'installation, il faut avoir Microsoft .NET Framework 4.7.2 installé.

1. Exécutez le programme d'installation 2N IP Utility.
2. L'assistant d'installation vous guidera tout au long de l'installation.
3. Après avoir installé l'application 2N IP Utility, lancez l'application à partir du menu Start du système opérationnel Microsoft Windows.
   Après son lancement, l'application commence automatiquement à rechercher dans le réseau local tous les appareils 2N et AXIS dont l'adresse IP est attribuée ou définie de manière statique par DHCP. Ces appareils sont ensuite présentés dans le tableau.



4. Sélectionnez dans la liste l’appareil que vous souhaitez configurer et cliquez dessus avec le bouton gauche de la souris. La partie droite de la fenêtre de configuration web s'ouvre alors.

ASTUCE

- L'interface de configuration web est également accessible via le bouton **Ouvrir dans un navigateur externe**, qui vous permet d'ouvrir l'interface dans une fenêtre de navigateur séparée.
- Cliquez sur un appareil dans la liste pour obtenir des informations détaillées. Cliquez sur le bouton **IP settings** pour modifier l'adresse IP en saisissant l'adresse IP statique souhaitée ou en activant DHCP.
- L'application vous permet également d'exporter les appareils sélectionnés vers un fichier CSV. Tout d'abord, sélectionnez l'appareil en cochant les cases correspondantes dans la liste, puis utilisez le bouton **Export** qui apparaît en bas de la fenêtre. Le fichier exporté contiendra le nom, l'adresse IP et le numéro de série des appareils sélectionnés.

Les identifiants de connexion par défaut sont :
Nom d’utilisateur : **Admin**
Mot de passe : **2n**
Après vous être connecté pour la première fois, vous devez immédiatement modifier votre mot de passe.

ASTUCE

Il est recommandé d’utiliser un mot de passe difficile à déchiffrer. Il est déconseillé d’utiliser des noms, des noms de lieux ou de choses dans les mots de passe, en particulier ceux qui ont un lien direct avec l'utilisateur.

Pour une plus grande sécurité du mot de passe, nous recommandons :

- d’utiliser un générateur de mots de passe aléatoires
- un mot de passe composé d'au moins 12 caractères
- de combiner différents caractères provenant de différents jeux de caractères (par exemple, majuscules/minuscules, chiffres, caractères spéciaux, etc.)

Interface de configuration Web

Orientation de base

La page d'accueil affichée est illustrative. L'affichage des tuiles dépend de la disponibilité des fonctionnalités sur l'appareil concerné.

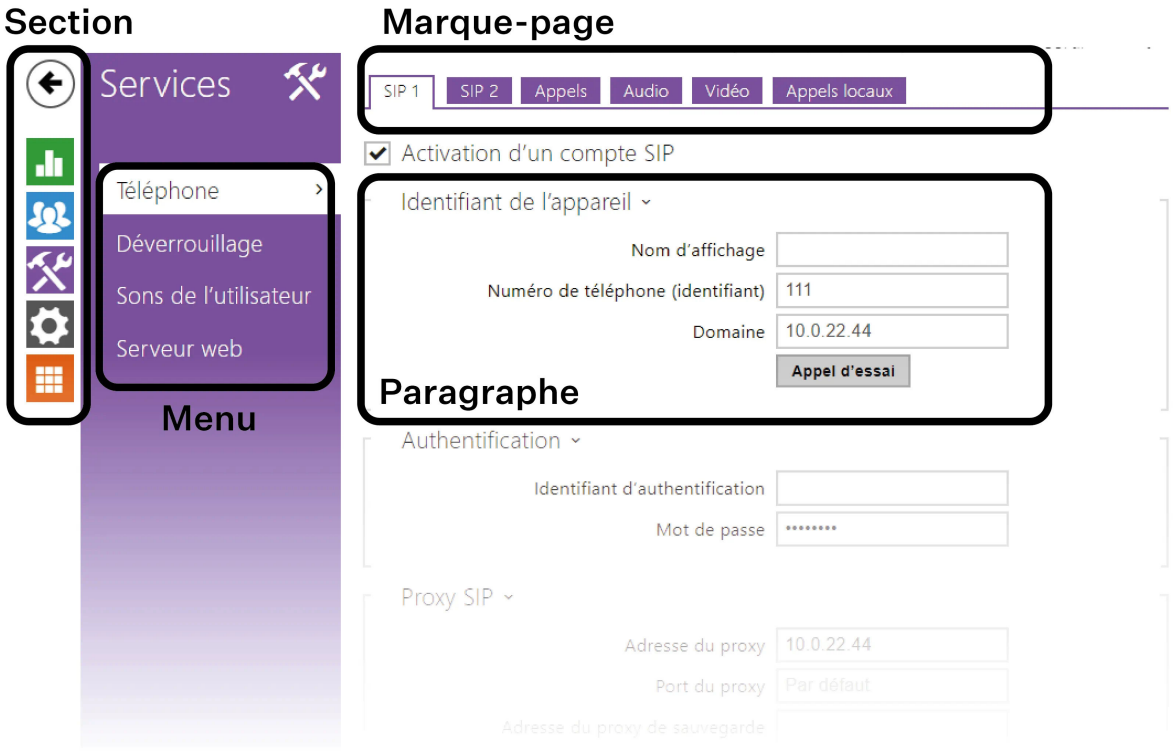
La page d'accueil s'affiche après la connexion dans l'interface web de configuration **2N LiftIP 2.0**. Il est possible d'y revenir à tout moment via la touche placée dans le coin supérieur gauche des autres pages de l'interface web de configuration. Dans l'en-tête de la page s'affiche le nom de l'appareil (voir paramètre Nom de l'appareil dans la **section Services > Serveur web**.

Menu

Vous pouvez utiliser le menu situé dans le coin supérieur droit de l'interface web pour sélectionner la langue. Vous pouvez vous déconnecter à l'aide du bouton Déconnexion situé dans le coin supérieur droit de la page, consulter l'aide à l'aide de l'icône représentant un point d'interrogation ou utiliser la bulle pour faire part de vos commentaires.

Légende

La page d'accueil sert de premier niveau d'orientation et de navigation rapide (en cliquant sur n'importe quelle tuile) vers des parties sélectionnées de la configuration **2N LiftIP 2.0**.



Se connecter à l'interface de configuration web

2N LiftIP 2.0 est configuré à l'aide de l'interface de configuration Web. Pour y accéder, il est nécessaire de connaître l'adresse IP.

Se connecter à l'interface de configuration web

1. Après l'avoir saisie, un écran de connexion s'affichera.
   Si l'écran de connexion n'apparaît pas, c'est que l'adresse IP ou le port saisi dans le navigateur web est erroné, ou que le serveur web d'administration a été désactivé. Si vous n'avez pas de certificat généré pour l'adresse IP ou le nom de domaine, vous pouvez recevoir un avertissement concernant un certificat de sécurité non valide. Dans ce cas, vous devez confirmer que vous souhaitez accéder à l'interface de configuration web.
2. Entrer les identifiants de connexion
   Les identifiants de connexion par défaut sont :
   Nom d'utilisateur : **Admin**
   Mot de passe : **2n**
   Après vous être connecté pour la première fois, vous devez immédiatement modifier votre mot de passe.
   Après connexion via le mot de passe par défaut, l'accès aux fonctions de l'interface web de configuration est limité.

ASTUCE
Il est recommandé d'utiliser un mot de passe difficile à déchiffrer. Il est déconseillé d'utiliser des noms, des noms de lieux ou de choses dans les mots de passe, en particulier ceux qui ont un lien direct avec l'utilisateur.

Pour une plus grande sécurité du mot de passe, nous recommandons :

- d'utiliser un générateur de mots de passe aléatoires
- un mot de passe composé d'au moins 12 caractères
- de combiner différents caractères provenant de différents jeux de caractères (par exemple, majuscules/minuscules, chiffres, caractères spéciaux, etc.)

Navigateurs recommandés
L'interface de configuration web est optimisée pour les navigateurs web basés sur Chrome (tels que Google Chrome, Microsoft Edge ou Opera). Lorsque vous utilisez d'autres navigateurs, il peut y avoir de légères différences de fonctionnalité dans l'apparence de l'interface.

État
La section État affiche clairement les informations et les propriétés actuelles de l'appareil.

Ascenseur
Le menu Ascenseur affiche des informations sur le modèle, ses propriétés et ses états d'erreur.

Statut de l'ascenseur
ID d'ascenseur – définit le numéro d'identification de l'ascenseur ou du communicateur d'ascenseur, qui est envoyé ou lu lors des appels individuels. Le numéro d'identification doit être composé d'un maximum de 16 chiffres.

Dernier appel de contrôle réussi - affiche l'heure du dernier appel de contrôle réussi.

Prochain appel de contrôle – indique l'heure du prochain appel de contrôle régulier.

Mode de récupération – indique si le mode de récupération est actuellement actif.

Relais de blocage actif - affiche l'état de la sortie du relais où le paramètre sera actif en cas d'enregistrement SIP ou d'erreur de configuration. Si l'une de ces erreurs se produit, l'ascenseur est bloqué.

Microphone externe - indique la connexion d'un microphone externe à l'appareil.

ATTENTION
Lorsque l'appareil fonctionne, la modification de l'état de connexion du microphone externe ne change pas. L'état actuel du microphone externe n'est détecté qu'au démarrage/redémarrage de l'appareil.

États d'erreur
Erreur d'enregistrement SIP – indique s'il y a actuellement un problème avec l'enregistrement du compte SIP.

Erreur de configuration – indique si l'appareil dispose d'une configuration valide pour les appels d'alarme (ALARM1).

Panne audio – indique si le dernier test audio s'est terminé avec succès et donc aucune erreur audio n'a été enregistrée.

Panne du bouton ALARM1 – indique si le bouton ALARM1 est actuellement défectueux.

Vérifier l'erreur d'appel – indique si le dernier appel de contrôle a échoué.

Appareil

Le menu Appareil affiche des informations sur le modèle et ses caractéristiques, la version du firmware et du bootloader, etc.

Infos sur l’appareil

Un certificat d’usine est installé – spécifiez le certificat d'utilisateur et la clé privée pour valider le droit à l'interphone de communiquer avec l'ACS.

Localiser l’appareil – signalisation visuelle ou acoustique d'un appareil.

Services

Le menu Services affiche l'état de l'interface réseau et des services sélectionnés.

Enregistrements des appels

Le menu Registre des appels affiche un aperçu de tous les appels que vous avez effectués. Chaque appel comporte les informations suivantes :

- type de contact,
- ID du correspondant/appelant,
- date et l'heure de l'exécution,
- durée de l'appel et son statut (entrant, sortant, manqué, décroché ailleurs, bouton de sonnette).

Le champ de recherche permet une recherche en texte intégral dans le nom des appels. La case à cocher est utilisée pour marquer tous les enregistrements pour une suppression en masse. L’enregistrement d’appel sélectionné peut également être supprimé séparément à l’aide de la touche . La vue d’ensemble affiche les 20 derniers enregistrements, classés de l’appel le plus récent au plus ancien.

Événements

Le menu Événements affiche les 500 derniers événements enregistrés par l'appareil. 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.

Événements	Signification
CallSessionStateChanged	Evénement décrivant la direction / l'état de l'appel, l'adresse, le numéro de session et le numéro de séquence d'appel.
CallStateChanged	Lorsque le statut de l’appel change (sonnerie, connecté, terminé), il indique également la direction (entrant, sortant) et l’identification de l’autre partie ou du compte SIP.
CapabilitiesChanged	Événement informant d’une modification de la liste des informations disponibles de l’appareil.

Événements	Signification
ConfigurationChanged	Changement de configuration de l’appareil.
DeviceState	Indication de l'état du périphérique, démarrage de l'appareil, par exemple.
DirectoryChanged	Changement dans le répertoire.
DirectorySaved	Changement enregistré dans le répertoire.
DtmfEntered	Recevoir un code DTMF en cours d'appel ou localement en dehors d'un appel.
ErrorStateChanged	Informe sur l'état d'erreur de l'appareil.
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 …).
LogAutomationEvent	
LoginBlocked	En cas de saisie de 3 mauvais logins lors de la connexion dans l‘interface web de configuration. Comporte les données sur l‘adresse IP de ces accès, sur l‘heure, la zone horaire et l‘uptime de l‘appareil (temps depuis le dernier redémarrage en secondes).
OutputChanged	Signale une modification de l'état de la sortie logique.
RegistrationStateChanged	Modification de l'état d'enregistrement du proxy SIP.
RescueStateChanged	Signale un changement d'état du mode d'extraction.

Répertoire

La section Répertoire est l'une des parties les plus importantes de la configuration de l'appareil. Elle sert à créer et à gérer les contacts .

Utilisateurs

ATTENTION
Pour les besoins de la communication d'urgence dans l'ascenseur, il est nécessaire d'avoir au moins un utilisateur dans le Répertoire avec un numéro de téléphone et le mode de **Confirmation sélectionné** .

La fonction de recherche du menu Appareils fonctionne comme une recherche en texte intégral dans les noms et les numéros de téléphone. Il recherche tous les matchs de la liste complète Trouvez un appareil est utilisé pour rechercher les appareils enregistrés ou les ajouter à la liste.

Ajouter un utilisateur permet de créer un nouvel utilisateur, l'icône permet d'afficher le détail des paramètres de l'utilisateur . L'icône permet de supprimer un utilisateur de la liste, lorsque toutes ses données saisies seront supprimées . La liste peut être triée par nom, numéro de téléphone ou mode de confirmation. 15, 25 ou 50 appareils peuvent être affichés sur 1 page de la liste.

Informations utilisateur de base

Chaque entrée de la liste des utilisateurs contient les informations suivantes :

Nom – le nom de l'utilisateur à la position donnée dans l'annuaire téléphonique. Ce paramètre sert à faciliter l'orientation entre les utilisateurs.

Type d'appareil — le type d'appareil est ajustable manuellement ou automatiquement à l'aide de la fonction de recherche des appareils enregistrés dans la liste des appareils du répertoire.

E-mail – l'appareil envoie des informations à ces e-mails, par exemple sur les appels manqués, etc. Il est possible de saisir plusieurs adresses e-mail, séparées par des virgules ou des points-virgules.

Numéros de téléphone des utilisateurs

Il est possible d'attribuer jusqu'à 6 numéros de téléphone à chaque utilisateur de la liste. L'appel sortant est acheminé vers tous les numéros simultanément. Dès que l'appel est connecté à un numéro de téléphone (c'est-à-dire confirmé), les appels vers les autres numéros de téléphone sont interrompus. Cette règle s'applique quel que soit le mode de confirmation défini.

Numéro de téléphone – entrez le numéro de téléphone du poste vers lequel l'appel doit être acheminé. Saisir l'adresse SIP « sip:[utilisateur_identifiant@]domaine[:port] » pour les appels SIP directs, par ex. : « sip:200@192.168.22.15 » ou« sip:nom@votresociété ». Renseignez « device:device_ID » pour les appels locaux et les appels vers l'application 2N My2N. Si vous entrez le symbole /1 ou /2 après le numéro de téléphone, pour les appels sortants, le compte SIP 1 ou SIP 2 sera explicitement utilisé. En ajoutant /S, vous pouvez forcer un appel chiffré, /N non chiffré. Il est possible d'entrer le choix de compte et de chiffrage en même temps, par exemple comme /1S.

Les réglages détaillés du numéro de téléphone peuvent être effectués dans l'édition, qui s'ouvre en appuyant sur le bouton .

Paramètres du numéro de téléphone

- **Type d'appel** – Définit le schéma dans l'URI de la destination appelée. Lorsque vous sélectionnez Sans schéma ([non spécifié]), l'URI est complété par les données des paramètres du compte SIP. D'autres options incluent l'appel SIP direct (sip:), les appels locaux 2N (device:), les appels pour appareil Crestron (rava:), la connexion à MS Teams (msteams:) ou les appels dans VMS, par ex. AXIS Camera Station (vms:).

- **Destination** – définit des autres parties de l'URI de la destination appelée. Il contient généralement un numéro, une adresse IP, un domaine, un port ou un identifiant de l'appareil. Un astérisque « * » est saisi pour les appels vers le VMS.
- **Compte SIP préféré** – le compte SIP numéro 1 ou numéro 2 est préféré pour les appels.
- **Cryptage des appels** – vous pouvez configurer le cryptage obligatoire des appels ou un appel sans cryptage.

Mode confirmation – détermine comment un appel d'alarme sera reçu pour un numéro donné.

Appel

Le section Appel est une fonction de base de l'appareil **2N LiftIP 2.0** – il vous permet d'établir des connexions avec d'autres appareils finaux dans les réseaux IP. L'appareil prend en charge le protocole SIP élargi.

Réglages généraux

Réglages généraux

Temps de conversation maximum – définit la durée maximale de l'appel après laquelle il se termine automatiquement. L'appareil signale la fin prochaine de l'appel en émettant un bip 10 secondes avant la fin de l'appel.Si la durée d'appel maximale est définie sur 0 et que SRTP n'est pas utilisé, l'appel n'est pas chronométré.

Délai de confirmation – définit la durée pendant laquelle un appel peut être confirmé après qu'il a été connecté. Si le temps est écoulé, l'appareil appelle le numéro suivant. Si la confirmation par prise de l'appel est activée, ce paramètre n'est plus pertinent.

Appels sortants

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

Limite de la durée de sonnerie – réglez le paramètre d'appel sortant et la limite de temps de sonnerie après laquelle les appels doivent automatiquement prendre fin. Si les appels sont dirigés vers le réseau GSM via des passerelles GSM, il est recommandé de configurer une valeur supérieure à 20 secondes. Valeur minimale: 1 s, valeur maximale: 600 s. Définissez 0 pour désactiver ce paramètre.

Paramètres avancés

Port RTP de départ – réglez le port RTP local de départ dans l'intervalle de la longueur de 64 ports à utiliser pour les transmissions audio et vidéo. La valeur par défaut est 4900 (c.-à-d. que l'intervalle utilisée est 4900–4963). Ce paramètre est commun pour les deux comptes SIP.

Délai d'attente RTP – définir le paquet RTP de flux audio recevant un délai d'attente lors d'un appel. Si cette limite est dépassée (les paquets RTP ne sont pas transmis), l'appel est coupé par l'appareil. Régler le paramètre sur 0 pour désactiver cette fonction. Ce paramètre est commun pour les deux comptes SIP.

Journalisation du protocole SIP avancée – permet d'écrire des informations plus détaillées sur la téléphonie SIP dans le syslog (pour le dépannage uniquement).

Appels locaux

Configuration

Autoriser les appels locaux – activez les appels entre appareils 2N sur le réseau local. Si cette fonction est désactivée, les autres équipements du réseau ne pourront pas trouver cet équipement, ce qui signifie qu'ils ne pourront pas appeler cet équipement dans un format device:ID_de l'équipement

Identification dans le réseau

ID d'appareil – configurez l'identification de l'appareil pour qu'elle apparaisse dans la liste des équipements locaux de tous les appareils 2N du même réseau local. En paramétrant le numéro de téléphone de l'utilisa-

teur dans ces équipements à la valeur « device:ID_de l'équipement », il sera possible de rediriger l'appel vers cet équipement.

Appel d'essai – affiche une boîte de dialogue avec la possibilité d'effectuer un appel test au numéro de téléphone sélectionné, voir ci-dessous :

Connexion aux unités dans les vestibules

Clé d'accès 1 et 2 – permet de configurer la clé d'accès entre l'unité de cabine (communicateur 2N) et l'unité dans le vestibule (**2N Sentrio Cabin**). Si la clé d'accès est vide ou ne correspond pas à celle de l'appareil jumelé, les appareils ne peuvent pas communiquer entre eux.

Appareils du réseau local

Nombre d'appareils locaux – Affiche le nom des appareils locaux sur le réseau.

Afficher la liste des périphériques locaux – Affiche la liste détaillée des appareils locaux sur le réseau.

Vidéo

Paramètres d'aperçu vidéo

Autoriser la prévisualisation de la vidéo – autorise la diffusion de la prévisualisation vidéo en multicast sur les Moniteurs.

Groupe multicast – définit l'adresse multicast à laquelle le flux vidéo sera envoyé depuis **2N LiftIP 2.0**. Choisir l'une des 8 adresses prédéfinies, ou choisir le mode où l'interphone sélectionne l'adresse automatiquement.

Mode faible bande passante – réduit la qualité de l'aperçu vidéo afin d'économiser la bande passante.

Audio

Envoi de DTMF

RTP (RFC-2833) – activez l'envoi de DTMF via RTP conformément au RFC-2833.

SIP INFO (RFC-2976) – activez l'envoi de DTMF via messages SIP INFO conformément au RFC-2976.

Réception de DTMF

RTP (RFC-2833) – activez la réception de DTMF via RTP conformément au RFC-2833.

SIP INFO (RFC-2976) – activez la réception de DTMF via messages SIP INFO conformément au RFC-2976.

Paramètres de qualité de transmission

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

SIP

L'appareil **2N LiftIP 2.0** permet de configurer deux comptes SIP indépendants. Ainsi, l'appareil peut être enregistré en parallèle sous deux numéros de téléphone, sur deux PBX SIP différents, etc. Les deux comptes SIP traitent les appels entrants de manière équivalente. Les appels sortants sont principalement effectués via le compte SIP 1. Si le compte SIP 1 n'est pas enregistré (par exemple en raison d'une panne du PBX SIP), SIP 2 est automatiquement utilisé pour les appels sortants. Sélectionnez le numéro de compte pour les numéros de téléphone inclus dans l'annuaire afin de spécifier le compte à utiliser pour les appels sortants (exemple : 2568/1 – les appels vers l'extension 2568 passent par le compte SIP 1, sip:1234@192.168.1.1/2 les appels SIP Uri par le compte SIP 2).

Configuration

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

Identifiant de l'appareil

Nom d'affichage – paramétrez le nom à afficher sur le téléphone de la personne appelée.

Numéro de téléphone (identifiant) – Paramétrer le numéro de téléphone de l'interphone (ou un autre identifiant unique comprenant des lettres et des chiffres). Ensemble avec le domaine, ce numéro représente un identifiant unique de l'interphone lors d'appels et d'enregistrements.

Domaine – Paramétrer le nom de domaine du service avec lequel l'interphone est enregistré. Normalement, il est identique au proxy SIP ou à l'adresse de l'enregistreur.

Appel d'essai – affiche une boîte de dialogue avec la possibilité d'effectuer un appel test au numéro de téléphone sélectionné, voir ci-dessous :

Authentification

Identifiant d'authentification – Saisissez un identifiant alternatif pour l'authentification.

Mot de passe – Saisissez le mot de passe pour l'authentification. Ce paramètre est uniquement appliqué si votre PBX nécessite une authentification.

Proxy SIP

Adresse du proxy – paramétrez l'adresse IP ou le nom de domaine du proxy SIP.

Port du proxy – paramétrez le port du proxy SIP (normalement 5060).

Adresse du premier proxy de secours – l'adresse IP ou le nom de domaine du proxy SIP de sauvegarde. L'adresse sera utilisée en cas où le proxy principal ne répond pas aux requêtes. Si le nom de domaine est ici défini ici et que le numéro de port du proxy SIP de réserve n'est pas rempli, l'adresse IP résultante du proxy SIP de sauvegarde sera définie en fonction des données des enregistrements NAPTR et SRV obtenues du DNS pour le nom donné. Si le DNS ne fournit pas ces enregistrements, ou si le numéro de port du proxy SIP de sauvegarde est également demandé, l'adresse de l'enregistrement A pour le nom donné sera utilisée.

Port du premier proxy de secours – configure le port du proxy SIP de sauvegarde. Si le paramètre est vide ou défini sur 0, le dispositif tentera de définir le numéro de port en fonction des données des enregistrements NAPTR et SRV obtenues du DNS. Si le DNS ne fournit pas ces enregistrements, la valeur par défaut du numéro de port est utilisée en fonction de la couche de transport (5060 pour UDP et TCP, 5061 pour TLS).

Adresse du deuxième proxy de secours – l'adresse IP ou le nom de domaine du proxy SIP de sauvegarde. L'adresse sera utilisée en cas où le proxy principal ne répond pas aux requêtes. Si le nom de domaine est ici défini ici et que le numéro de port du proxy SIP de réserve n'est pas rempli, l'adresse IP résultante du proxy SIP de sauvegarde sera définie en fonction des données des enregistrements NAPTR et SRV obtenues du DNS pour le nom donné. Si le DNS ne fournit pas ces enregistrements, ou si le numéro de port du proxy SIP de sauvegarde est également demandé, l'adresse de l'enregistrement A pour le nom donné sera utilisée.

Port du deuxième proxy de secours – configure le port du proxy SIP de sauvegarde. Si le paramètre est vide ou défini sur 0, le dispositif tentera de définir le numéro de port en fonction des données des enregistrements NAPTR et SRV obtenues du DNS. Si le DNS ne fournit pas ces enregistrements, la valeur par défaut du numéro de port est utilisée en fonction de la couche de transport (5060 pour UDP et TCP, 5061 pour TLS).

Enregistreur SIP

Autoriser l'enregistrement – autorise l'enregistrement de l'appareil auprès de Registrar SIP configuré.

Adresse du registrar – définissez l'adresse IP ou le nom de domaine du registrar SIP.

Port du registrar – définissez le port du registrar SIP (généralement 5060).

Adresse du registrar de sauvegarde – l'adresse IP ou le nom de domaine du registrar SIP de sauvegarde. L'adresse sera utilisée en cas où le registraire principal ne répond pas aux requêtes.

Port du registrar de sauvegarde – paramétrez le port du registrar SIP de sauvegarde (habituellement 5060).

Expiration de l'enregistrement – définissez l'expiration de l'enregistrement, qui affecte le réseau et la charge du bureau d'enregistrement SIP, en fonction des exigences d'enregistrement régulièrement envoyées. Le registrar SIP peut modifier la limite d'expiration sans vous en informer.

Etat d'enregistrement – affiche l'état actuel d'enregistrement (non enregistré, enregistrement, enregistré…).

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

Paramètres avancés

Protocole de transport SIP – définissez le protocole de communication SIP. UDP (par défaut), TCP ou TLS.

Version TLS minimum – spécifier la version la plus basse du TLS grâce à laquelle vous pouvez vous enregistrer sur le serveur et établir une connexion.

Forcer le schéma SIPS URI – Le schéma SPS URI est forcé si le paramètre est activé (**sips** est utilisé dans les messages sortants et les messages entrants doivent contenir **sips**).

Vérifier le certificat du serveur – Vérifie le certificat public du serveur SIP par rapport aux certificats CA téléchargés sur l'appareil.

Certificat du client – Spécifie le certificat client et la clef privée au moyen desquels est vérifiée l'autorisation de l'interphone à communiquer avec le serveur SIP.

Port local pour SIP – définit le port local que l'appareil utilise pour la signalisation SIP. La modification de ce paramètre ne prendra effet qu'après le redémarrage de l'appareil. Si le paramètre est laissé vide, la valeur par défaut est utilisée :

Valeurs par défaut des ports locaux pour SIP

SIP	UDP et TCP	TLS
SIP 1	5060	5061
SIP 2	5062	5063
SIP 3	5064	5065
SIP 4	5066	5067

PRACK activé – activez la méthode PRACK pour une confirmation fiable des messages SIP avec des codes de 101 à 199.

REFER activé – activez le renvoi d'appel via la méthode REFER.

Envoyer les paquets KeepAlive – configure si l'appareil doit envoyer régulièrement les paquets STUN/CRLF du registre ainsi que SIP OPTIONS pendant les appels, pour maintenir active la liaison déjà établie.

Filtre d'adresse IP activé – activez le blocage de réception de paquets SIP provenant d'adresses autres que celles du proxy SIP et du registrar SIP. L'objet principal de cette fonction est l'amélioration de la sécurité de communication et l'élimination d'appels téléphoniques non autorisés.

Recevoir uniquement les appels cryptés (SRTP) – il règle la restriction des appels reçus sur ce compte sur des appels chiffrés avec le protocole SRTP. Des appels non chiffrés seront refusés. En même temps, pour plus de sécurité, on vous recommande d'employer TLS comme un protocole de transport pour SIP.

Appels sortants cryptés (SRTP) – les appels sortants devront être cryptés avec le protocole SRTP. En même temps, pour plus de sécurité, on vous recommande d'employer TLS comme un protocole de transport pour SIP.

Utiliser MKI dans les paquets SRTP – permet d'utiliser MKI (Master Key Identifier), qui est requis par la contrepartie pour identifier la clé principale lors de la rotation de plusieurs clés dans les paquets SRTP.

Ne pas jouer les early media entrants – il interdit la lecture d'un flux vidéo entrant avant le décrochage de l'appel (early media) envoyé par certaines PBX ou par d'autres appareils. Au lieu de cela, la sonnerie locale standard sera jouée.

Valeur DSCP QoS – définissez la priorité de paquets SIP dans le réseau. La valeur programmée est envoyée dans le champ TOS (Type of Service) de l'en-tête du paquet IP. La valeur est saisie sous forme de nombre décimal. La modification de ce paramètre ne prendra effet qu'après le redémarrage de l'appareil.

STUN activé – enable STUN functionality for the SIP account. Address and ports acquired from the configured STUN server will be used in SIP headers and SDP media negotiation.

Adresse du serveur STUN – définissez l'adresse IP du serveur STUN qui sera utilisé pour ce compte SIP.

Port du serveur STUN – définissez le port du serveur STUN qui sera utilisé pour ce compte SIP.

Adresse IP externe – configure l'adresse IP publique ou le nom du routeur auquel l'appareil est connecté. Si l'adresse IP de l'appareil est publique, laissez ce champ vide.

Compatibilité avec l'équipement Broadsoft – il définit le mode de compatibilité avec les PBX Broadsoft. Dans ce mode, lorsque l'interphone reçoit une nouvelle invitation (re-invite) de la centrale, il répond au lieu du menu complet en répétant le dernier SDP envoyé avec les codecs actuellement utilisés.

Rotation des enregistrements SRV – permet la rotation des enregistrements SRV pour le proxy SIP et le registraire. Il s'agit d'une méthode alternative de basculement vers des serveurs de sauvegarde en cas de défaillance ou d'indisponibilité des serveurs principaux.

Vidéo

Codecs vidéo

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

Paramètres de qualité de transmission

Valeur DSCP QoS – définissez la priorité des paquets RTP dans le réseau. La valeur programmée est envoyée dans le champ TOS (Type of Service) de l'en-tête du paquet IP.

Taille maximale de paquet – déterminez la limite de la taille des paquets vidéo RTP à envoyer.

Paramètres avancés de codec

Autorisé – il permet le mode de mise en paquet et règle le type de charge utile pour chaque codec. Le type de charge utile sera sélectionné automatiquement s'il ne peut pas être réglé manuellement.

SDP Payload Type – il règle le "payload type" pour le codec vidéo H.264 (packetization mode 1). Il est possible de régler une valeur comprise entre 96 et 127 éventuellement 0 pour ne pas offrir cette variante de codec.

Audio

Codecs audio

Dans ce bloc, vous pouvez autoriser/interdire l'utilisation des différents codecs audio proposés lors de l'établissement de la connexion et définir leur priorité.

Envoi de DTMF

Ce bloc est utilisé pour définir la manière d'envoyer des caractères DTMF à partir de l'appareil. Vérifiez les options de réception DTMF et les paramètres du destinataire de l'appel pour un fonctionnement optimal.

Mode d'envoi – définissez s'il est possible d'envoyer une trame DTMF pendant un appel en appuyant sur les touches 0 à 9, * et # du pavé numérique de l'appareil. L'envoi peut être réglé uniquement pour les appels entrants/sortants/tous les appels.

In band (audio) – activez l'envoi de la double tonalité DTMF classique dans la bande audio.

RTP (RFC-2833) – activez l'envoi de DTMF via RTP conformément au RFC-2833.

SIP INFO (RFC-2976) – activez l'envoi de DTMF via messages SIP INFO conformément au RFC-2976.

Réception de DTMF

Ce bloc est utilisé pour régler la réception des caractères DTMF de l'interphone. Vérifiez les options de réception DTMF et les paramètres du destinataire de l'appel pour un fonctionnement optimal.

In-Band (Audio) – activez la réception de la double tonalité DTMG classique dans la bande audio.

RTP (RFC-2833) – activez la réception de DTMF via RTP conformément au RFC-2833.

SIP INFO (RFC-2976) – activez la réception de DTMF via messages SIP INFO conformément au RFC-2976.

Paramètres de qualité de transmission

Valeur QoS DSCP – paramétrez la priorité des paquets audio RTP sur le réseau. La valeur programmée est envoyée dans le champ TOS (Type of Service) de l'en-tête du paquet IP.

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

Appel d'alarme

Onglet Appel d'alarme

Paramètres de base

Durée d'appui pour l'activation de l' – définit la durée minimale en millisecondes pendant laquelle il est nécessaire d'appuyer sur le bouton ALARM1 pour déclencher l'appel d'alarme. Conformément aux normes européennes en vigueur, la valeur maximale ne doit pas dépasser 3000 ms. La plage recommandée est comprise entre 2000 et 3000 ms.

Appel retardé – en cochant, il détermine si l'appel d'alarme sera différé (pendant la temporisation, le même message audio qu'au moment de l'établissement de l'appel est diffusé dans la cabine).

Retard d'appel – règle le délai d'appel d'alarme en secondes (pendant ce délai, un message audio est diffusé en cabine comme lors d'un appel). Ne réglez pas ce paramètre à une valeur inférieure à celle du paramètre **Durée d'appui pour activer** dans le bloc **Alarme test**. Conformément aux normes européennes en vigueur, cette fonction doit être réglée sur une valeur supérieure à 0 s.

Tester l'alarme

NOTE
Conformément aux normes européennes en vigueur, cette fonction doit être activée.

Permettre – définit s'il est possible de lancer un appel d'alarme test en appuyant longuement sur le bouton ALARM1.

Durée d'appui pour activer – règle le temps d'appui sur le bouton ALARM1 en secondes, qui démarre l'appel d'alarme test. La valeur ne doit pas être supérieure à la valeur du paramètre **Appel retardé**. Conformément aux normes européennes en vigueur, la valeur doit être réglée sur 30 s.

Destination

Le bloc Destination permet de sélectionner l'utilisateur vers lequel la connexion sera dirigée lors d'un appel d'alarme.

Nombre de répétitions – définit le nombre de cycles d'appel au cas où l'appel ne serait pas reconnu/récepté. Le nombre de répétitions par défaut est de 3, un maximum de 9 répétitions peut être défini. Si le nombre de cycles d'appel défini a lieu et que l'appel n'est pas pris, il est automatiquement terminé.

Test d'appel d'ALARME – permet de lancer un appel d'alarme test.

Onglet Appel d'alarme 2

Destination

Le bloc Destination permet de sélectionner l'utilisateur vers lequel la connexion sera dirigée lors d'un appel d'alarme.

Nombre de répétitions – définit le nombre de cycles d'appel au cas où l'appel ne serait pas reconnu/récepté. Le nombre de répétitions par défaut est de 3, un maximum de 9 répétitions peut être défini. Si le nombre de cycles d'appel défini a lieu et que l'appel n'est pas pris, il est automatiquement terminé.

Test d'appel ALARME2 – permet de lancer l'appel d'alarme test 2.

Appel de contrôle

L'appel de contrôle sert à établir automatiquement un appel de contrôle dont la fonction est de vérifier le bon fonctionnement de l'**2N LiftIP 2.0**. Cette fonction simule un appel sortant.

NOTE
Conformément aux normes européennes en vigueur, cette fonction doit être activée.

Appel de contrôle autorisé – permet d'effectuer des appels de contrôle.

Paramètres de base

NOTE
Conformément aux normes européennes en vigueur, la fonction d'appel de contrôle doit être effectuée au moins une fois tous les trois jours.

Période – l'appel de contrôle est répété une fois tous les jours donnés. Le premier appel de contrôle est effectué à une heure choisie au hasard dans les 24 heures suivant le démarrage de l'appareil.

Prochain appel – indique l'heure du prochain appel de contrôle régulier.

Destination

Le bloc Destination permet de sélectionner l'utilisateur vers lequel la connexion sera dirigée lors de l'appel de contrôle.

Nombre de répétitions – définit le nombre de cycles d'appel au cas où l'appel ne serait pas reconnu/récepté. Le nombre de répétitions par défaut est de 3, un maximum de 9 répétitions peut être défini. Si le nombre de cycles d'appel défini a lieu et que l'appel n'est pas pris, il est automatiquement terminé.

Test d'appel de contrôle – permet de lancer un appel de contrôle de test.

Appel opérationnel

Destination

Le bloc Destination permet de sélectionner l'utilisateur vers lequel la connexion sera dirigée lors d'un appel opérationnel.

L'appel opérationnel est utilisé pour établir automatiquement un appel opérationnel si l'un des événements prédéfinis se produit. Cette section définit la destination vers laquelle l'appel de trafic sera acheminé. L'établissement de l'appel lui-même se fait par automatisation, voir Automation (p. 60). L'appel opérationnel est activé par l'action StartLiftCall avec le paramètre CallType = opérationnel. L'action est déclenchée lorsque l'événement auquel elle est liée se produit :

- **RescueTerminated** pour établir un appel de service lorsque le mode de libération est terminé.
- **ErrorStateChanged** pour établir un appel opérationnel en cas de défaillance/réparation d'un bouton ou de défaillance/réparation de l'audio. Le type de changement d'état d'erreur est déterminé par les paramètres de cet événement (événement).

1–2 – permet de sélectionner l'utilisateur vers lequel la connexion sera dirigée.

Nombre de répétitions – définit le nombre de cycles d'appel au cas où l'appel ne serait pas reconnu/récepté. Le nombre de répétitions par défaut est de 3, un maximum de 9 répétitions peut être défini. Si le nombre de cycles d'appel défini a lieu et que l'appel n'est pas pris, il est automatiquement terminé.

Services

Ascenseur

Paramètres généraux

ID d'ascenseur – définit le numéro d'identification de l'ascenseur ou du communicateur d'ascenseur, qui est envoyé ou lu lors des appels individuels. Le numéro d'identification doit être composé d'un maximum de 16 chiffres.

Mode de récupération

Le mode de secours se produit lorsqu'un appel d'alarme (d'urgence) est connecté. Lors de l'activation du mode, il est également nécessaire de définir la méthode de sa terminaison ultérieure.

NOTE

Pour la version UE : Dans **rubrique Services > Ascenseur > Mode de récupération** activer le mode de récupération. **Cette étape est nécessaire pour se conformer à la législation européenne.** Une fois activé, l'appareil vous permet d'avoir un mode de secours actif, pendant lequel il est possible d'avoir plusieurs appels d'alarme. Cela facilite v Elevator Center affichez plusieurs appels d'alarme dans un seul mode de récupération et revenez aux conversations de chat.

Pour la version américaine : Dans **rubrique Services > Ascenseur > Mode de récupération** Le mode de récupération ne doit pas être activé. **Cette étape est nécessaire pour respecter la législation américaine.** Chaque appel d'alarme sera en Elevator Center maintenu comme un nouveau record.

Activer le mode de récupération– active le mode de récupération (le mode de récupération activé nécessite au moins une façon de quitter le mode de récupération).

Terminaison avec le bouton ALARM2– définit s'il est possible de terminer le mode de récupération en appuyant sur le bouton ALARM2.

Quitter en saisissant un mot de passe– définir si la fin du mode de secours est confirmée par un mot de passe (le mot de passe est envoyé à l'appareil en tant que DTMF lors d'un appel). La saisie du mot de passe pour quitter le mode de secours est inefficace si un appel d'alarme est en cours.

Mot de passe– Définissez le mot de passe pour mettre fin au mode de secours. Le mot de passe est envoyé à l'appareil en tant que DTMF dans un appel et ne peut être composé que de chiffres (longueur maximale 16). Le mot de passe est saisi dans DTMF au format suivant : « *mot de passe* ». Par exemple, si le mot de passe est 12345, vous devez entrer le « *12345* ».

Surveillance de la cabine

Mode de surveillance – définit le mode de surveillance de l'appareil. Cela modifie le comportement du microphone (muet) et l'indication du mode de surveillance par l'appareil (l'appareil indique que l'audio et la vidéo de la cabine ne sont pas disponibles pour des raisons de confidentialité). La surveillance peut être :

Activer après un appel d'alarme pour – définit la durée pendant laquelle le microphone restera coupé et l'appareil signalera que la surveillance n'est pas activée (l'audio et la vidéo de la cabine ne sont pas disponibles pour des raisons de confidentialité) après un appel d'alarme. Cela ne s'applique que s'il s'agit **Mode de surveillance** réglé sur « Activé après un appel d'alarme ».

E-mail

Onglet SMTP

Service SMTP activé – autorise ou bloque le service d'envoi d'e-mails depuis l'appareil.

Paramètres du serveur SMTP

Adresse du serveur – Adresse du serveur SMTP auquel les e-mails seront envoyés.

Port du serveur – définit le port du serveur SMTP. La valeur par défaut est 25, la modification ne convient qu'en cas de paramètres de serveur SMTP non standard.

Type de sécurité – sélectionne le type de sécurité pour la communication avec le serveur SMTP.

Connectez-vous au serveur SMTP

Nom d'utilisateur – spécifie un nom de connexion au serveur valide si le serveur SMTP nécessite une autorisation. Sinon, le champ risque d'être vide.

Mot de passe – spécifie un mot de passe valide pour se connecter au serveur si le serveur SMTP nécessite une autorisation. Sinon, le champ risque d'être vide.

Certificat client – spécifie le certificat client et la clé privée, qui sont utilisés pour crypter la communication entre l'appareil et le serveur SMTP.

Paramètres généraux de messagerie

Adresse de l'expéditeur – spécifie l'adresse par défaut pour tous les e-mails sortants.

Paramètres avancés

Livrer à – définit la durée maximale pendant laquelle l'appareil tente de transmettre le courrier électronique à un serveur SMTP indisponible.

Automation

Les appareils 2N offrent des options de réglage très flexibles en fonction des différents besoins des utilisateurs. Il existe des situations où la gamme habituelle de paramètres (par exemple, réglage du comportement des commutateurs ou des appels) n'est pas suffisante, et pour ces cas, les appareils 2N fournissent une interface programmable spéciale d'automatisation. Une utilisation typique de l'automatisation concerne les applications qui nécessitent une intégration plus complexe avec des systèmes tiers.

On accède à l'interface Automation en cliquant sur  pour la fonction que vous souhaitez créer ou modifier.

ASTUCE
Une description détaillée de la fonction et de la configuration d'automatisation est disponible dans Automatisation manuelle.

NOTE
La fonctionnalité d'automatisation n'est disponible qu'avec la licence Gold.

API HTTP

L'API HTTP est une interface d'application permettant de contrôler les fonctions sélectionnées de l'appareil à l'aide du protocole HTTP. Cette interface facilite l'intégration d'appareils 2N avec des produits tiers, par ex. systèmes domotiques, systèmes de sécurité et de surveillance des bâtiments, etc.

Onglet Services

Services API HTTP

L'API HTTP est divisée en services suivants par fonction :

- **API système**– permet les modifications de configuration, l'acquisition d'état et la mise à niveau de l'appareil.
- **I/O API**– permet le contrôle et la surveillance des entrées et sorties logiques de l'appareil.
- **Audio API** – permet un contrôle de la lecture audio et la surveillance du microphone.
- **API E-mail** – permet l'envoi d'e-mails à des utilisateurs.

- **Phone/Call API** – assure le contrôle et la surveillance des appels entrants / sortants.
- **Logging API** – permet la lecture et l'enregistrements des événements.
- **Automation API**– vous permet de définir les exigences de communication et d'autorisation sécurisées/non sécurisées.
- **Elevator API** - permet de connecter **Sentrio Lobby** au communicateur d'urgence de l'ascenseur.

Pour chaque service, le protocole de transport (HTTP=TCP ou HTTPS=TLS) et la méthode d'authentification (aucun, Basic ou Digest) peuvent être définis. Jusqu'à cinq comptes d'utilisateurs (avec leur propre nom et mot de passe) peuvent être créés dans la configuration de l'API HTTP avec la possibilité d'un contrôle détaillé de l'accès aux services et fonctions individuels.

Pour chaque service, la méthode d'authentification requise pour les demandes envoyées à l'appareil peut être définie. Si l'authentification n'est pas effectuée, la demande est rejetée. Les demandes sont authentifiées à l'aide du protocole d'authentification standard décrit dans la RFC-2617. Il est possible de choisir les trois méthodes d'authentification suivantes :

- **Aucun**– le service ne nécessite aucune authentification. Dans ce cas, le service n'est absolument pas protégé sur le réseau local.
- **Basic**– le service nécessite une authentification de base selon RFC-2617. Le service nécessite dans ce cas un mot de passe, mais celui-ci est envoyé dans un format ouvert. Nous vous recommandons de combiner cette option avec le protocole HTTPS si possible.
- **Digest**– le service nécessite une authentification Digest selon RFC-2617. Cette option est la méthode par défaut et la plus sécurisée des méthodes ci-dessus.

Onglet Compte 1-5

L'appareil 2N vous permet de gérer jusqu'à cinq comptes d'utilisateurs pour accéder aux services HTTP API. Le compte utilisateur comprend le nom et le mot de passe de l'utilisateur ainsi qu'un tableau des droits d'accès des utilisateurs aux services API HTTP individuels.

Compte activé – active le compte utilisateur.

Paramètres utilisateur

Nom d'utilisateur – vous permet de saisir un nom d'utilisateur pour l'authentification auprès de l'API HTTP.

Mot de passe – saisissez le mot de passe pour vous authentifier auprès de l'API HTTP.

Droits des utilisateurs

Le tableau des droits d'accès peut être utilisé pour gérer les privilèges des comptes d'utilisateurs pour des services individuels.

Intégration

Onglet MS Teams

L'intégration avec Microsoft Teams permet d'effectuer des appels entre l'appareil 2N et le compte Microsoft Teams. Pour connecter l'appareil à Microsoft Teams, il est nécessaire de configurer d'abord la passerelle SIP de l'installation Microsoft Teams. La procédure est décrite dans la FAQ (en anglais) ou dans la documentation MS Teams. Une fois l'adresse du serveur de configuration saisie dans la configuration de l'appareil 2N, la connexion (onboarding) est établie. Après l'onboarding, il est possible de se connecter au compte Microsoft Teams dans l'interface de configuration web.

Microsoft Teams autorisé – autorise le service intégration avec MS Teams

Service

Le statut – montre le statut actuel du processus d'onboarding et de connexion.

- « Désactivé » – fonction désactivée.
- « Onboarding » – l'appareil obtient/a obtenu une configuration commune pour l'onboarding ou une configuration individuelle pour l'onboarding (avant connexion).

- « Échec de l'onboarding » – l’appareil n’a pas pu obtenir une configuration commune ou individuelle d’onboarding ou n’a pas pu s’enregistrer sur le serveur SIP d’onboarding.
- « Hors ligne » – aucune réponse du serveur.
- « En ligne » – l’appareil est bien enregistré sur le serveur SIP final.
- « Échec de l'enregistrement » – l’appareil n’a pas pu s’enregistre sur le serveur SIP final.
- « Licence requise » – l’appareil n’a pas la bonne licence pour cette fonction.

Numéro de téléphone – montre le numéro de téléphone (ID) que l’appareil a reçu du serveur MS Teams.

Appel d’essai – affiche une boîte de dialogue avec la possibilité d'effectuer un appel test au numéro de téléphone sélectionné.

Paramétrage du serveur de configuration

Mode de récupération d’adresse – permet de choisir si l’adresse du serveur onboarding MS Teams sera saisie manuellement ou si sera utilisée une adresse obtenue automatiquement à partir du serveur DHCP via le paramètre Option 66 ou 150.

Adresse du serveur – permet une saisie manuelle de l’adresse du serveur onbaording MS Teams.

Adresse DHCP (Option 66/150) – vérifiez l’adresse du serveur récupérée via l’option DHCP 66/150 ou l’option DHCP 150.

Plan des mises à jour de la configuration

Au démarrage de l’appareil – autorise un contrôle et le cas échéant la réalisation d’une mise à jour après chaque démarrage de l’appareil.

Période de mise à jour – il définit la période de mise à jour. On peut régler la mise à jour une fois par heure, jour, semaine et mois.

Mise à jour à – définissez l'heure de mise à jour au format HH : MM pour la mise à jour périodique Le paramètre ne s’applique pas si l’intervalle de mise à jour est défini à moins de 1 jour. L’heure est configurée en UTC. Contrôlez la valeur Heure prochaine mise à jour pour voir l’heure réelle à laquelle la mise à jour est prévue.

Onglet Service de recherche

Paramètres

Adresse du serveur d’intégration – configure l’URL du Service de recherche d’appareil. L’appareil envoie des demandes HTTP avec des données de base lors du démarrage, lors d’un changement d’adresse IP et périodiquement (si cela est configuré). Si le champ est libre, les demandes ne sont pas envoyées.

NOTE
La demande JSON envoyée contient les informations suivantes sur l’appareil : MacAddress, Dhcp, IpAddress, NetMask, Gateway, SwVersion, SerialNumber, Variant, VariantId, Description, ProductName, CameraResolution (max.), HttpPort, HttpsPort.

Vérifier le certificat du serveur – autorise le contrôle des certificats du serveur d’intégration, ce qui garantit que les demandes Discovery sont envoyées à un serveur fiable.

Certificat client – choisit lequel des certificats enregistrés sera utilisé pour une communication chiffrée avec le serveur d’intégration.

Envoyer des requêtes de découverte périodiquement – autorise l’envoi des demandes HTTP Discovery.

Période de découverte – configure la période d'envoi de la demande HTTP sur l'URL configuré en secondes.

Statut d'intégration – affiche le statut d'intégration sur la base de la réponse du serveur.

Détails – affiche les détails contenus dans la réponse du serveur.

Sons Utilisateurs

Le moniteur **2N LiftIP 2.0** signale les états de fonctionnement par séquences de tonalités. Si les tonalités de signalisation standard ne répondent pas à vos exigences, vous pouvez les modifier et les personnaliser.

Onglet Attribution des sons

Langue 1–3 – sélectionne la langue pour les messages sonores de l'appareil. Si un fichier pour lequel une traduction est disponible est remarqué pour l'événement donné, le message sera enregistré dans la langue choisie. S'il n'y a pas de traduction disponible, un son en anglais ou linguistiquement neutre sera enregistré.

Réglages des sons

- « Établissement de la connexion » – définit le message audio qui sera diffusé dans la cabine lors de l'établissement d'un appel d'alarme.
- « Appel d'alarme » – définit le message audio qui sera diffusé dans la conversation lors de la connexion d'un appel d'alarme.
- « Appel de contrôle » – définit le message audio qui sera diffusé dans la conversation lors de la connexion d'un appel de contrôle.
- « Prolonger l'appel » – définit le message audio qui sera diffusé dans la conversation lorsque celle-ci sera sur le point de s'achever.
- « Déconnexion » – définit le message audio qui sera diffusé dans la conversation et dans la cabine (si cela est pertinent pour le type d'appel donné) dans le cas où l'appel en cours doit être interrompu.
- « Fin de l'appel » – définit le message audio qui sera diffusé dans la cabine lorsque l'appel sera terminé.
- « Fin de l'extraction » – définit le message audio qui sera diffusé dans la conversation et dans la cabine si le mode d'extraction a été quitté (pertinent uniquement si le mode d'extraction est autorisé).

Chargement de sons

Jusqu'à 10 fichiers audio d'une durée maximale de 60 secondes peuvent être ajoutés à l'appareil. Pour plus de clarté, il est possible d'attribuer un nom spécifique à chaque son enregistré.

Procédure d'ajout de sons

1. Appuyez sur pour télécharger un fichier son sur le moniteur.
2. Dans la boîte de dialogue, sélectionnez un fichier stocké sur votre ordinateur et appuyez sur Charger.
3. Appuyez sur pour enregistrer un fichier audio directement depuis le microphone de votre ordinateur.
4. Appuyez sur pour effacer un fichier. Vous pouvez lire le fichier audio enregistré (localement sur votre ordinateur) à l'aide du bouton .

Serveur web

Le moniteur **2N LiftIP 2.0** peut être configuré 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 le moniteur.

Paramètres de base

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 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 au moniteur. 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.

Paramètres avancés

Port HTTP – paramétrez le port du serveur web pour la communication HTTP. Le paramétrage du port ne sera appliqué qu'après le redémarrage du moniteur.

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 du moniteur.

Version TLS minimum – définissez la version TLS minimale, autorisée pour la connexion à l'appareil.

Certificat du serveur HTTPS – Il définit le certificat du serveur et la clef privée au moyen desquels est réalisé le cryptage de la communication entre le serveur http de l'appareil et le navigateur web de l'utilisateur.

Accès à distance activé – Activez l'accès à distance au serveur web du dispositif à partir d'adresses IP Off-LAN.

Localisation de l'utilisateur

Langue originale **– permet de télécharger à partir de l'appareil un fichier XML original qui contient tous les textes de l'interface utilisateur web en anglais.**

Langue de l'utilisateur – permet de charger, de télécharger et éventuellement de supprimer le fichier utilisateur contenant vos propres traductions des textes de l'interface utilisateur web.

Test audio

Test audio activé – permet l'exécution automatique du test audio.

Configuration des tests

Période de test – permet de définir la période d'exécution du test. Le test peut être exécuté automatiquement une fois par jour ou une fois par semaine.

Durée d'exécution du test – permet de définir l'heure à laquelle le test doit être effectué régulièrement. L'heure peut être réglée au format HH:MM. Nous vous recommandons de définir une heure à laquelle une utilisation minimale de l'appareil est attendue.

Résultat du test

Statut des tests – affiche l'état actuel du test en cours.

C'est l'heure du dernier test – affiche l'heure de début du dernier test.

Le résultat du dernier test – affiche le résultat du dernier test.

SNMP

Les unités de contrôle d'accès 2N intègrent des fonctionnalités permettant la surveillance à distance des appareils du réseau à l'aide du protocole SNMP.

Service activé – vous permet d'activer cette fonction.

Paramètres de SNMP

Version la plus basse autorisée – sélectionne la version SNMP la plus basse acceptée par le périphérique. SNMPv3 applique le cryptage.

Nom de communauté – chaîne de texte représentant la clé d'accès aux objets de la table MIB

Adresse IP Concept d'interruptions – il s'agit de l'adresse IP à laquelle les concepts d'interruptions SNMP sont envoyés.

Télécharger le fichier MIB – téléchargez la définition MIB depuis un appareil

SNMP identification

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).

Adresses IP autorisées

Adresse IP 1 – saisir des 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.

Configuration de SNMPv3

Nom d'utilisateur – définir l'algorithme utilisé pour l'authentification des interruptions SNMPv3.

Authentification – définit l'algorithme à utiliser pour déchiffrer les pièges SNMPv3.

Mot de passe d'authentification – définir le mot de passe d'authentification SNMPv3.

Confidentialité/Cryptage – définit l'algorithme à utiliser pour déchiffrer les pièges SNMPv3.

Mot de passe de déchiffrement – définit le mot de passe pour le déchiffrement des pièges SNMPv3.

Hardware

Audio

Dans cette partie de la configuration, le volume des appels et le volume de la signalisation des différents états de l'appareil sont ajustés.

Le volume général de l'appareil affecte le volume des appels et celui des tonalités de signalisation. Veuillez régler ce paramètre en fonction du niveau de bruit de l'environnement dans lequel l'appareil est utilisé.

ASTUCE
Le volume général de l'appareil peut également être contrôlé à l'aide des boutons VOL+ et VOL− de l'.

Volume appel téléphonique

Volume des tons d'appel – configure le volume du ton de numérotation, de sonnerie et d'occupation. Cette configuration n'est pas utilisée si les tons de la sélection sont générés en externe. La valeur est relative par rapport au volume total.

Volume de signalisation

Volume de la tonalité d'avertissement – réglez le volume des avertissements et des signaux décrits dans la section Signalisation des états opérationnels. La valeur est relative au volume principal.

Désactiver les tonalités d'avertissement – Désactive les sons des états opérationnels suivants: Application interne lancée, adresse IP reçue et adresse IP perdue.

Volume des sons personnalisables – réglez le volume des sons d'utilisateur joués par l'automatisation. La valeur est relative au volume principal.

Signalisation du démarrage et de l'état du réseau - Sélectionne le mode de signalisation sonore du démarrage de l'application et du gain ou de la perte d'adresse IP.

- **Activé** - l'appareil émet des signaux audio à chaque démarrage de l'application et à chaque changement d'adresse IP.
- **Désactivé** - aucun signal audio n'est lu.
- **Une seule fois** - l'appareil émettra les signaux vous invitant à démarrer l'application et à obtenir une adresse IP une seule fois après le démarrage. Cette fonction est utile lorsque l'adresse IP change fréquemment ou en cas de connexions intermittentes où des signaux répétés pourraient gêner les utilisateurs.

Paramètres d'entrées audio

Gain d'entrée du microphone – paramétrez le gain d'entrée du microphone.

Entrées logiques

Le menu Entrées numériques décrit les options d'entrée numérique de l'appareil.

Inversion des entrées

Bouton ALARM1 inversé – l'entrée inversée est active lorsque le contact est ouvert ou qu'une tension est appliquée.

Bouton ALARM2 inversé – l'entrée inversée est active lorsque le contact est ouvert ou qu'une tension est appliquée.

Entrée inversée CANCEL – l'entrée inversée est active lorsque le contact est ouvert ou qu'une tension est appliquée.

Boutons

Temps d'évaluation de la panne du bouton – définit le temps pendant lequel le bouton ALARM1 doit être activé avant que la panne du du bouton ne soit détectée.

Caméra externe

Caméra IP externe

Caméra autorisée – en cochant la case vous activez le téléchargement du flux RTSP d'une caméra IP externe. Remplir l'adresse de flux RTSP valide ou le nom d'utilisateur et le mot de passe pour que la fonction fonctionne bien.

Adresse du flux RTPS – définit l'adresse IP du flux RTSP au format « rtsp://ip_address_camera/parameters ». Les paramètres sont spécifiques au modèle de caméra IP sélectionné.

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

Mot de passe – entrez le mot de passe d'authentification de la caméra IP externe. Ce paramètre est uniquement obligatoire si la caméra IP externe nécessite une authentification.

Port RTP local – le port local pour RTP peut être modifié si la configuration du réseau l'exige.

Communication de la caméra IP externe

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

Système

Réseau

L'appareil **2N LiftIP 2.0** se connecte à un réseau local et doit avoir une adresse IP valide pour fonctionner correctement, ou il peut obtenir une adresse IP à partir d'un serveur DHCP sur ce réseau. L'adresse IP et les paramètres DHCP sont configurés dans la section Réseau.

ASTUCE
Vous pouvez trouver l'adresse IP actuelle de l'appareil à l'aide de l'application 2N Network Scanner, qui peut être téléchargée gratuitement à partir de 2N.com. La procédure est décrite dans le chapitre Recherche de l'adresse IP à l'aide de 2N Network Scanneru.

Basique

Utiliser le serveur DHCP – activez l'obtention automatique de l'adresse IP à partir du serveur LAN DHCP. S'il n'y a pas de serveur DHCP sur le réseau ou s'il ne peut pas être utilisé, vous devez configurer le réseau manuellement.

Paramètres d'une adresse IP statique

Adresse IP statique – adresse IP statique de l'appareil l'adresse est utilisée avec 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.

Paramètres de DNS

Toujours utiliser les paramètres manuels – autorise les paramètres manuels des adresses des serveurs DNS.

DNS principal – l'adresse du serveur DNS principal pour la traduction de noms de domaines en adresses IP.

DNS secondaire – l'adresse du serveur DNS secondaire, qui est utilisée si le DNS principal n'est pas accessible.

Paramètres du port LAN

Mode de port requis – définissez le port de l'interface réseau par défaut (Automatique ou Half Duplex – 10 Mbps). 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).

Identification dans le réseau

Hostname – paramètres d'identification des appareils sur le réseau.

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

Paramètres de VLAN

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.

Onglet Firmware

Activez Firmware – protège l'appareil contre les demandes malveillantes. Il est fortement recommandé de garder le Firmware constamment activé.

Firewall

Activé – active le pare-feu qui protège l'appareil des requêtes malveillantes.

Statut - indique l'état du pare-feu. L'état du pare-feu peut être Désactivé, En fonctionnement ou Détection d'une attaque possible (lorsqu'un problème est détecté et que certaines demandes sont ignorées).

Date et heure

Vous pouvez à tout moment synchroniser l'heure de votre appareil avec l'heure d'Internet en cochant la fonction Utiliser l'heure d'Internet ou avec l'heure actuelle de votre PC en utilisant le bouton Synchroniser avec le navigateur.

ATTENTION
Pour une précision et une fiabilité maximales, il est recommandé d'activer la fonction Utiliser le temps d'Internet. Dans des conditions de fonctionnement normales, l'appareil peut afficher un retard ou une avance de l'ordre de ±2 minutes/mois.

NOTE
Des réglages corrects de la date et de l'heure ne sont pas nécessaires pour la fonction de base de l'appareil. .

Heure actuelle

Utiliser le temps d'Internet – Activer l'utilisation du serveur NTP pour la synchronisation de l'heure du dispositif.

Synchroniser avec le navigateur – à l'aide du bouton, vous pouvez à tout moment synchroniser l'heure de votre appareil avec l'heure actuelle de votre PC.

Zone horaire

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.

Serveur NTP

Adresse du serveur NTP – paramétrer l'adresse IP/le nom de domaine du serveur NTP utilisé pour la synchronisation de l'heure de votre dispositif. Ni l'adresse IP du serveur ni le nom de domaine ne peuvent être définis lorsque la fonction Utiliser l'heure d'Internet est désactivée.

État du NTP – affiche l'état de la dernière tentative de synchronisation de l'heure locale via le serveur NTP (Non synchronisé, Synchronisé, Erreur).

Fonction

Le menu affiche une liste de fonctions bêta publiées qui sont destinées à être testées par les utilisateurs.

La liste indique :

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

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

NOTE
Aucune garantie n'est fournie pour les fonctions de test et 2N TELEKOMUNIKACE a.s. n'est pas responsable des limitations fonctionnelles et des dommages éventuels résultant des limitations fonctionnelles des fonctions bêta. Les fonctions bêta sont fournies à des fins de test uniquement.

Certificats

Certains services réseau de l'appareil **2N LiftIP 2.0** utilisent le protocole sécurisé TLS pour communiquer avec d'autres appareils sur le réseau. 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 de l'appareil qui utilisent le protocole TLS :

1. Serveur Web (HTTPS)
2. 802.1x (EAP-TLS)
3. SIPs

L'appareil permet de télécharger jusqu'à 3 séries de certificats d'autorité de certification, qui servent à vérifier l'identité de l'appareil avec lequel il communique, ainsi que 3 certificats personnels et clés privées, qui servent à crypter les communications.

Vous pouvez attribuer l'une des séries de certificats à chaque service de l'appareil qui nécessite des certificats, voirServeur web (p. 63).

Le dispositif est compatible avec les certificats sous format DER (ASN1) et PEM.

Lorsque l'appareil est branché pour la première fois, un certificat appelé Self Signed et une clé privée sont automatiquement générés, qui peuvent être utilisés pour le serveur Web sans qu'il soit nécessaire de télécharger votre propre certificat et votre propre clé privée.

NOTE
Si un certificat Self Signed est utilisé pour crypter la communication entre le serveur web de l'appareil et le navigateur, la communication est sécurisée, mais le navigateur avertit qu'il ne peut pas vérifier la fiabilité du certificat de l'appareil.

L'aperçu actuel des certificats téléchargés des autorités de certification et des certificats personnels est affiché dans deux onglets : Certificats autorisés (Certificats CA) et Certificats d'utilisateur.

Chargement de certificat

1. En appuyant sur le bouton , vous pouvez télécharger un certificat du stockage vers l'appareil.
2. Dans la boîte de dialogue, sélectionnez le fichier avec un certificat (éventuellement avec une clé privée).
3. Appuyez sur le bouton **Chargement**
4. Appuyez sur le bouton × pour effacer le certificat de l'appareil.

NOTE

- Un certificat avec la clé privée RSA de plus de 2048 bits peut être rejeté. et le message suivant s'affiche
  « Le dispositif n'a pas accepté le fichier de la clé privée ou le mot de passe de la clé privée! »
- 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).

Onglet CSR

Vous pouvez créer une demande de signature de certificat (CSR) personnalisée dans l'interface de configuration web, que vous soumettez ensuite à une autorité de certification (CA) pour signature. Ce processus garantit que le certificat est correctement associé à la clé privée générée lors de la création de la RSC et qu'il reste stocké en toute sécurité uniquement sur votre appareil.

1. Pour créer une nouvelle demande de certificat, cliquez sur +.

2. Une boîte de dialogue apparaît, dans laquelle vous devez remplir les informations suivantes :
   - **Common Name (CN)** - cette entrée doit contenir l'adresse IP ou le nom de domaine sous lequel l'interface Web du dispositif d'interphonie IP 2N est accessible.
   - **SAN : mDNS** - Permet d'inclure **mDNS (Multicast DNS)** comme nom de sujet alternatif (SAN) dans le certificat. Il est utilisé pour l'accès par un nom de domaine sur le réseau local.
   - **SAN: IP** - Permet d'inclure l'adresse IP en tant que nom de sujet alternatif (SAN) dans le certificat. Il est utilisé pour l'accès via l'adresse IP.
   - **Public Key Algorithm** - Spécifie le type d'algorithme utilisé pour générer la clé publique du certificat.
   - **CSR ID** - identifiant unique de la demande de signature de certificat (CSR).
   - **Country (C)** - code à deux lettres du pays où l'organisation est enregistrée (selon la norme ISO 3166-1 alpha-2).
   - **State/Country/Region (S)** - l'État ou la région où l'organisation est enregistrée (pas d'abréviation).
   - **City/Locality (L)** - le nom de la ville ou de la localité où l'organisation est enregistrée (sans abréviation).
   - **Organisation (O)** - le nom légal de l'organisation, y compris les suffixes tels que "Inc", "Corp", "Ltd".
   - **Organizational Unit (OU)** - nom d'un département ou d'une unité au sein d'une organisation.
   - **E-mail** - adresse électronique de la personne de contact ou du gestionnaire de certificat.
3. Cliquez sur Generate pour créer une demande de signature de certificat. Téléchargez le fichier CSR créé et enregistrez-le dans un endroit sûr.
4. Soumettez le fichier CSR créé à une autorité de certification (CA), qui émettra un certificat numérique sur la base de ce fichier.
5. Téléchargez le certificat numérique émis vers le fichier CSR dans l'interface web. Pour télécharger, cliquez sur + dans la ligne de la demande de certification.

Appuyez sur 🗑 pour supprimer le CSR. Appuyez sur ⓘ pour afficher les paramètres CSR.

Provisioning

My2N

La plateforme cloud My2N est utilisée pour gérer et configurer à distance les dispositifs 2N IP et permet de se connecter à distance à l'interface web de l'appareil.

My2N activé – Activez la connexion à My2N.

My2N Security Code

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.

État de la connexion

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.

TR069

Cet onglet permet d'activer et de configurer l'administration à distance de l'appareil à l'aide du protocole TR-069. Le protocole TR-069 vous permet de configurer de manière fiable les paramètres de l'appareil, de restaurer et de sauvegarder la configuration, ou de mettre à jour le firmware de l'appareil.

Le protocole TR-069 est utilisé par le service cloud My2N. Pour que l'appareil fonctionne correctement avec My2N, le service TR-069 doit être autorisé et le paramètre ??? réglé sur la valeur My2N. L'appareil se connecte alors périodiquement au service My2N, qui peut le configurer.

Cette fonction vous aide à connecter le produit à votre ACS (serveur de configuration automatique). Dans ce cas, la connexion à My2N sera désactivée.

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

Réglages généraux

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 – indique le temps nécessaire à l'appareil pour contacter le serveur 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.

Diagnostic

Onglet Diagnostic

L'interface permet de commencer à capturer des logs de diagnostic, qui peuvent ensuite être téléchargés et envoyés à l'Assistance technique. Les logs de diagnostic capturés permettent d'identifier et de résoudre les problèmes rapportés. Les logs contiennent des informations sur l'appareil, sa configuration, le trafic réseau, le crash log et la statistique de la mémoire.

Paquet diagnostic

État de capture de paquets – indique si la capture de paquets est lancée dans l'onglet Capture de paquets.

Taille des paquets capturés – indique le nombre de paquets capturés.

État de capture de syslogs – indique si la capture des messages syslog est lancée dans l'onglet Syslog.

Longueur de capture Syslog – indique la durée pendant laquelle les messages syslog sont capturés dans l'onglet Syslog.

Taille des paquets capturés – indique le nombre de messages syslog capturés.

Arrêter la capture de syslogs – définit la période pendant laquelle les données seront capturées.

La capture est lancée à l'aide du bouton d'enregistrement  . Lorsque l'on appuie à nouveau sur le bouton d'enregistrement  , la capture redémarre et recommence à fonctionner. Le fichier contenant les paquets capturés peut être téléchargé à l'aide du bouton  . Le fichier avec les paquets capturés contient un fichier comportant la configuration de l'appareil sauvegardée.

Pour plus de sécurité, cryptez le fichier avec un mot de passe. Ce mot de passe sera nécessaire lors de la restauration de la configuration pour décrypter le fichier et accéder à son contenu. Veillez à ne pas perdre votre mot de passe et à le conserver en lieu sûr.

L'exportation du hachage pour une sortie sécurisée ajoute leur type de hachage aux valeurs du fichier de configuration comme elles sont inscrites dans le syslog. Le type de hachage est ajouté aux valeurs en tant qu'attribut **DiscreteHash**.

ATTENTION

- Le lancement de la capture de données de diagnostic redémarre la capture de paquets si elle est déjà en cours d'exécution.
- Pour plus de sécurité, cryptez le fichier avec un mot de passe. Ce mot de passe sera nécessaire lors de la restauration de la configuration pour décrypter le fichier et accéder à son contenu. Veillez à ne pas perdre votre mot de passe et à le conserver en lieu sûr.

Fonctions d'utilité

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.

Onglet Capture des paquets

Dans l'onglet Trace, vous pouvez lancer la capture des paquets entrants et sortants sur l'interface réseau. Les paquets capturés peuvent être stockés localement dans la mémoire tampon d'une taille de 4 MB ou à distance sur le PC de l'utilisateur. Le fichier contenant les paquets capturés peut être téléchargé et traité ultérieurement, par exemple à l'aide de l'application Wireshark (www.wireshark.org).

Capture locale de paquets

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

1. Pour lancer la capture de paquets, cliquez sur  .
2. Pour arrêter la capture, cliquez sur  .
3. Vous pouvez enregistrer le fichier avec les paquets capturés sur le disque en cliquant sur  .

Capture de paquets à distance

1. Cliquez sur  .
2. Dans la fenêtre qui s'ouvre, définissez la durée (en secondes) de capture des paquets entrants et sortants.
3. Cliquez sur OK pour lancer la capture.
4. Sélectionnez un emplacement sur le disque pour stocker le fichier avec les paquets capturés.
5. Pour arrêter la capture, cliquez sur  .

Onglet Syslog

L'appareil **2N LiftIP 2.0** permet d'envoyer des messages système contenant des informations importantes sur l'état et les processus de l'appareil à un serveur Syslog, où ces messages peuvent être enregistrés et utilisés pour une analyse et un audit plus approfondis de l'appareil surveillé. Il n'est pas nécessaire de configurer ce service pour un fonctionnement classique du produit.

Les données sensibles, telles que les codes d'accès, les identifiants de carte, les identifiants de connexion, etc., sont stockées dans syslog sous forme cryptée (hash). L'attribution des valeurs de hachage aux valeurs réelles peut se faire en fonction du fichier de configuration.

Paramètres du serveur Syslog

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 – définit l'adresse IP au format « IP[:port] » ou l'adresse MAC du serveur exécutant l'application pour enregistrer les messages syslog.

Degré de gravité – réglez le degré de gravité des messages à envoyer (Erreur, Avertissement, Notification, Info, Debug 1–3). Le réglage du niveau n'est recommandé que pour faciliter le dépannage du service de support technique.

Messages Syslog locaux

Ce bloc présente un aperçu général des messages Syslog locaux. Les messages syslog locaux peuvent être chargés et téléchargés .

Maintenance

Ce menu est utilisé pour maintenir la configuration et le firmware de l'appareil. Il vous permet de sauvegarder et de restaurer tous les paramètres, de mettre à jour le firmware de l'appareil ou de rétablir l'état initial de tous les paramètres de l'appareil.

Configuration

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 que le fichier ne soit téléchargé sur l'appareil, vous pouvez choisir si les paramètres réseau et les paramètres de connexion au PBX SIP doivent être appliqués à partir du fichier de configuration.

Lorsque vous restaurez une configuration à partir d'un fichier crypté, vous devez entrer un mot de passe pour le décrypter.

ATTENTION
Le fichier de configuration possède en lui un mot de passe de connexion enregistré. Si le mot de passe dans le fichier est non codé ou si le mot de passe par défaut est 2n, seule sera enregistrée la partie valide de la configuration. Cela veut dire que la configuration s'enregistre, mais que le mot de passe reste le mot de passe par défaut et ne change pas pour la valeur indiquée dans le fichier.

Enregistrer config – Sauvegardez la configuration actuelle complète de votre produit. Lorsque l'on appuie sur le bouton, la configuration complète est téléchargée et peut être sauvegardée dans le stockage.

ATTENTION

- La configuration de l'appareil peut contenir des informations sensibles telles que les numéros de téléphone des utilisateurs et les mots de passe ; le fichier doit donc être manipulé avec précaution.
- Pour plus de sécurité, cryptez le fichier avec un mot de passe. Ce mot de passe sera nécessaire lors de la restauration de la configuration pour décrypter le fichier et accéder à son contenu. Veillez à ne pas perdre votre mot de passe et à le conserver en lieu sûr.

Réinitialiser la configuration - utilisé pour restaurer tous les paramètres de l'appareil à l'état par défaut. La restauration des paramètres réseau et des paramètres du certificat nécessite une confirmation supplémentaire dans la boîte de dialogue de confirmation.

Système

Mettre à jour le firmware – Pour mettre à jour le firmware de votre produit, appuyez sur le bouton pour afficher une fenêtre de dialogue vous permettant de sélectionner et de télécharger le fichier du firmware. Après un upload réussi du firmware, l'appareil redémarre automatiquement. et un nouveau firmware sera alors disponible. La procédure complète de mise à jour dure moins d'une minute. Référez-vous au site .2n.com pour la dernière version FW de votre produit. La mise à niveau du firmware n'affecte pas la configuration car l'appareil vérifie le fichier pour empêcher le téléchargement d'un fichier.

État du firmware – indique si une nouvelle version du firmware est disponible. Si elle n'est pas disponible, Vérifier s'affiche pour vérifier en ligne si un firmware plus récent est disponible. Si elle est disponible, Mettre à jour télécharge le firmware lorsqu'on appuie sur le bouton et ensuite, met à niveau l'appareil automatiquement.

Signaler les versions beta – Permet de vérifier et de télécharger les dernières versions betas disponibles.

NOTE

Cet appareil ne met pas automatiquement à jour le micrologiciel afin de garantir un fonctionnement stable et d'éviter d'éventuels problèmes de compatibilité avec des systèmes tiers intégrés dans votre environnement. Pour garantir l'intégrité du système et éliminer les défaillances involontaires, toutes les mises à jour doivent être confirmées ou lancées manuellement par l'utilisateur. Avant d'effectuer une mise à jour, veuillez consulter les notes de mise à jour de la nouvelle version et vérifier la compatibilité avec votre infrastructure existante.

Redémarrer – redémarre l'appareil. Le processus prend environ 30 s. Lorsque celui-ci a obtenu l'adresse IP au redémarrage, la fenêtre de connexion s'affiche automatiquement.

ATTENTION

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

Licences des bibliothèques de tiers – cliquez sur Afficher pour afficher une fenêtre de dialogue comprenant une liste des licences utilisées et des logiciels tiers, ainsi qu'un lien CLUF.

Statistiques d’utilisation

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.

Ports Utilisés

Service	Port	Protocoles	Direction	Configurable	Paramètres
RTP	9 000			✓	**Appel > Paramètres généraux**
DHCP	68	UDP	Entrée/Sortie	×	–
DNS	53	TCP/UDP	Entrée/Sortie	×	–

Fonctions et utilisation

Nous aborderons dans cette section les fonctions basiques et étendues des produits **2N LiftIP 2.0**.

Description de la fonction

Cette section est destinée au dépannage. Si le système ne fonctionne pas correctement et qu'un technicien qualifié est en mesure de suivre point par point le fonctionnement du système conformément à cette description, il y aura divergence entre la description et la réalité. Il décrit ensuite l'anomalie, ce qui accélère considérablement la recherche de la cause. Souvent, cette procédure révèle également que le système fonctionne correctement, mais que l'utilisateur avait une idée différente de sa fonction.

Appel sortant

Le processus est lancé par le bouton ALARM de l'annonciateur (l'entrée CANCEL peut retarder ou bloquer l'appel). Après avoir appuyé sur le bouton ALARME, **2N LiftIP 2.0** établit une connexion avec le centre de dispatching (pour plus de détails, voir l'option automatique). **2N LiftIP 2.0** diffuse le message "Veuillez patienter, je suis en train d'établir une connexion" à la personne dans l'ascenseur et l'instruction à la salle de contrôle "Appuyez sur 1 pour confirmer" (si la confirmation DTMF 1 est utilisée). Vous devez confirmer l'appel manuellement ou automatiquement. L'appel est limité dans le temps (message d'avertissement "Attention, la fin de l'appel approche. Pour prolonger l'appel, appuyez sur 4."), mais vous pouvez prolonger l'appel. La commande en cours d'appel (numérotation DTMF) est décrite dans le chapitre "Instructions d'envoi".

ASTUCE
Définissez des destinations pour les appels d'alarme et d'autres pour les appels de contrôle et de service.

Appel de contrôle

Un appel de contrôle est un appel sortant effectué automatiquement (généralement tous les 3 jours) pour vérifier le bon fonctionnement du 2N LiftIP 2.0. L'opération est la même que pour un appel sortant. La différence réside dans la diffusion d'un message différent, par exemple "Il s'agit d'un appel de contrôle et une série différente de numéros de téléphone est utilisée (voir Appels de contrôle). L'appel de contrôle permet un traitement automatique. En cas de prise manuelle (confirmation 1 ou prise de configuration), le message d'appel de contrôle est diffusé ; en cas de traitement automatique, le message n'est pas diffusé.

ASTUCE
Il est également possible de lancer l'appel de contrôle manuellement. La durée d'un appel de contrôle normal n'est pas affectée.

AVERTISSEMENT
Si la mémoire définie pour l'appel de contrôle est complètement vide, l'appel de contrôle ne sera pas effectué, même vers la mémoire définie pour l'appel d'alarme.

Appel opérationnel

Un appel opérationnel est un appel effectué automatiquement après l'un des événements (bouton bloqué, fin de libération, erreur audio, ...). Pour les réglages et une description plus détaillée, voir Appel opérationnel (p. 58).

Appel entrant

Le dispatcheur peut également appeler le numéro auquel **2N LiftIP 2.0** est connecté, qui recevra automatiquement tout appel entrant. L'appel entrant est limité dans le temps de la même manière que l'appel sortant et est contrôlé de la même manière (identification du poste et de l'appareil).

Grâce à un appel entrant, vous pouvez, par exemple, informer une personne bloquée de l'heure d'arrivée des secours, etc. Vous pouvez également vérifier à distance que **2N LiftIP 2.0** est connecté et fonctionne.

Protection contre les démarrages inutiles

Étant donné que le seul but de **2N LiftIP 2.0** est d'appeler à l'aide si quelqu'un est coincé dans la cabine de l'ascenseur, l'appel peut être considéré comme inutile si la porte de la cabine est ouverte. Ainsi, si l'ascenseur est équipé d'un contact de porte, il est possible de connecter ce contact à l'entrée **2N LiftIP 2.0** marquée CANCEL et de programmer le temps pendant lequel **2N LiftIP 2.0** attendra après avoir appuyé sur le bouton ALARM avant d'établir une connexion. Ainsi, si quelqu'un appuie par erreur sur le bouton ALARME, l'ascenseur atteindra un étage pendant ce temps, la porte s'ouvrira et l'appel sera annulé. Il est également possible de fixer un temps minimum pour appuyer sur le bouton, ce qui permet d'éliminer la plupart des cas où quelqu'un appuie sur le bouton par erreur.

Fin d'appel (appel sortant et entrant)

La fin de l'appel (raccrochage) se produit pour les raisons suivantes :

- l'autre côté (dispatching) a raccroché ;
- la durée maximale d'appel réglée expire - 10 secondes avant l'expiration **2N LiftIP 2.0** joue le message "Attention, la fin de l'appel approche. Pour prolonger l'appel, appuyez sur 4.", l'appel peut être prolongé.

Instructions pour l'envoi

Contrôle de la numérotation par tonalité pendant un appel (DTMF)

Pendant un appel, vous pouvez utiliser la numérotation par tonalité pour contrôler le **2N LiftIP 2.0** pendant un appel (si la numérotation automatique de confirmation est utilisée) selon le tableau suivant. Les commandes 1 à 4 sont énumérées dans l'ordre dans lequel elles sont normalement utilisées pour faciliter la mémorisation.

Caractère DTMF	Description de la fonction
1	Confirmation par laquelle 2N LiftIP 2.0 sait que l'appel a abouti. 2N LiftIP 2.0 fait taire le message en cours d'écoute et envoie son signal de confirmation, l'appel se poursuit jusqu'à l'expiration de la limite et l'une des commandes suivantes peut être utilisée.
3	Pour afficher des informations sur le communicateur.
4	Prolongation d'appel - l'appel est prolongé de 120 secondes et peut être utilisé de manière répétée.

Aperçu des rapports 2N LiftIP 2.0

Rapports	Importance
"Restez en attente, s'il vous plaît, je suis en train de faire une connexion."	L'annonce est diffusée à l'utilisateur dans la cabine d'ascenseur lors de l'établissement de l'appel (avant la confirmation).
"C'est un appel de détresse.	Il est retransmis à la salle de contrôle avant que l'appel ne soit confirmé.
"Il s'agit d'un appel de contrôle".	Le message n'est transmis qu'au dispatcher (uniquement pour l'acquittement DTMF 1).
"Attention, nous approchons de la fin de l'appel. Pour prolonger l'appel, appuyez sur 4".	Ce message indique, lors des appels entrants et sortants, que la durée maximale de l'appel expirera dans 10 secondes.
"Désolé, votre appel doit être déconnecté".	L'annonce est diffusée à l'utilisateur dans la cabine d'ascenseur pendant que l'appel est en cours.
"Fin de l'appel".	Le message est envoyé avant que l'appel ne soit raccroché.
"Le processus de désincarcération est terminé.	Accusé de réception de la fin de la signalisation d'urgence.

Identification 2N LiftIP 2.0

Après avoir confirmé l'appel d'urgence, le répartiteur peut appuyer sur la touche DTMF 3 et le numéro d'identification du communicateur est diffusé. Vous pouvez également obtenir des informations sur le communicateur lors d'un appel entrant.

Type de confirmation d'appel

Ce réglage s'applique aux appels d'alarme, aux appels de vérification et aux messages d'erreur.

Confirmez en appuyant sur 1

Vous pouvez enregistrer jusqu'à 4 numéros de téléphone et le nombre de répétitions pour les appels à la salle de contrôle.

2N LiftIP 2.0 tente alors d'appeler un par un tous les numéros enregistrés. **2N LiftIP 2.0** utilise la numérotation par tonalité (DTMF), qui est de loin le critère le plus fiable pour confirmer une connexion réussie.

Lorsqu'il reçoit un appel manuellement, le dispatcher doit appuyer sur la touche 1 de son téléphone (en numérotation à tonalité). Si le numéro appelé est occupé ou si personne ne répond au téléphone dans le délai imparti ou n'accuse réception de l'appel, **2N LiftIP 2.0** essaie d'appeler le numéro suivant dans la séquence jusqu'à ce que le nombre de tentatives défini pour tous les numéros saisis soit épuisé. L'appel de commande ou le signalement d'un défaut est identique, mais il est possible d'utiliser une série distincte de 2 numéros.

Évaluation des situations lors de l'élection avec confirmation

Situation	2N LiftIP 2.0
Recevoir une résiliation de la part de la contrepartie (Occupé, Numéro non trouvé, etc.)	Il compose immédiatement le numéro suivant.
Appel	Il attend pendant une période déterminée.
Sonnerie	Il attend pendant une période déterminée.
Caractère DTMF 1	Confirme la réception ("Connexion confirmée"), fait taire le message en cours de lecture et la communication se poursuit pendant la durée maximale programmée (durée maximale de la communication).
1 3 4	Ces chiffres sont interprétés comme des caractères de contrôle.

Confirmation de l'enlèvement

VOIP

ATTENTION
Une fois le message diffusé, l'appel est confirmé.

La personne appelée ne doit appuyer sur aucune touche. Les deux modes ont une série de numéros et un nombre de cycles communs et réagissent de la même manière aux situations pendant la numérotation.

AVERTISSEMENT
Lorsque vous utilisez ce mode, assurez-vous qu'aucune boîte vocale, aucun télécopieur ou autre appareil ne prenne l'appel avant le nombre de sonneries défini. Cela mettrait fin à l'élection automatique.

CPC (Antenne et KONE)

Il est utilisé lorsque la contrepartie dispose du SW nécessaire. Une chaîne DTMF est envoyée lorsque la ligne est décrochée. L'ascenseur s'identifiera. Selon le type d'appel, il passe en communication vocale (appel d'urgence) ou est automatiquement acquitté et terminé (appel de contrôle).

P100

Il est utilisé lorsque la contrepartie dispose du SW nécessaire. Un caractère DTMF est envoyé lorsque la ligne est prise. L'ascenseur s'identifiera. Selon le type d'appel, il passe en communication vocale (appel d'urgence) ou est automatiquement acquitté et terminé (appel de contrôle).

Autodétection du protocole DTMF (CPC/P100)

L'ascenseur détermine le protocole qu'il utilise après avoir envoyé la chaîne DTMF et répond en conséquence.

AVERTISSEMENT

- Si l'appel a été dirigé par exemple via GSM, il peut y avoir un problème avec la détection des caractères DTMF et **2N LiftIP 2.0** n'est pas en mesure de distinguer de quel protocole il s'agit.
- Si cette situation se produit, nous vous recommandons de changer le réglage pour CPC ou P100 (3 ou 5).

CPC (antenne), P100 2N ext (pour les appels d'alarme uniquement)

Les protocoles fonctionnent de la même manière qu'aux points 3 et 4 pour le CPC et au point 5 pour le P100. La seule différence est que le type de syllabe est également transmis. Il n'est utilisé que pour les appels d'urgence au communicateur.

Test d'orthographe audio

Le test de l'en-tête audio permet l'exécution automatique du contrôle audio. Définit une période d'une fois par jour ou d'une fois par semaine à une heure sélectionnée à laquelle le test doit être effectué périodiquement. Si la syllabe est correcte, l'appel de contrôle suivant est effectué. Si une erreur a été détectée pendant le test audio, l'appel de contrôle suivant ne sera pas effectué.

Événement après une erreur audio

Il est possible d'informer de l'échec d'un test audio à l'aide d'un événement. Les réglages sont effectués via la configuration de l'appareil basée sur le web, voir Appel opérationnel (p. 58). Un événement est exécuté lorsqu'un test audio défectueux est évalué (est mis en place par l'appel de service).

- Appel opérationnel - l'appel est établi vers un numéro de destination enregistré pour un appel opérationnel.

Processus de libération et fin de la libération

Activer le processus de libération

Si un appel d'urgence est établi, le voyant jaune du haut-parleur reste allumé après la fin de l'appel. Cela signale un processus de libération active.

Achèvement de la procédure de libération

Le processus de libération peut être interrompu en appelant **2N LiftIP 2.0** et en saisissant le mot de passe (***mot de passe***) pour confirmer la fin du mode de libération pendant l'appel. Ou en appuyant sur le bouton ALARM2 dans la cabine d'ascenseur.

Lorsque la désincarcération est terminée, l'annonce "Le processus de désincarcération est terminé" est émise par l'annonciateur.

La configuration s'effectue via l'interface web, voir Release Mode.

Événement après l'achèvement du processus de libération

Une fois le processus de validation terminé, l'événement peut être exécuté. **2N LiftIP 2.0** ne prend en charge que les appels opérationnels.

- Appel opérationnel - l'appel est dirigé vers un numéro de destination enregistré pour un appel opérationnel.

La configuration s'effectue via l'interface web de l'appareil, voir Fonctionnement des appels (p. 58).

Protocoles CPC et P100

CPC

Le protocole CPC prend en charge 3 variantes : **KONE**, **Antenne** et **Antenne 2N Ext**.

Le message de données se compose des éléments suivants

Commande - Type d'appel - DATA - ID

CPC

Type d'appel	Commande	Type d'appel	Données	ID
Alarme	04	10	0000000000000	numéro d'identification de l'ascenseur
Alarme 2	04	10	0000000000000	numéro d'identification de l'ascenseur
Appel de contrôle	04	21	0000000000000	numéro d'identification de l'ascenseur
Fin de la procédure d'habilitation	04	84	0000000000000	numéro d'identification de l'ascenseur
Panne du bouton	04	90	0000000000000	numéro d'identification de l'ascenseur
Réparation du bouton	04	90	0000000000001	numéro d'identification de l'ascenseur

Type d'appel	Commande	Type d'appel	Données	ID
Dysfonctionnement de l’audio	04	91	0000000000000	numéro d’identification de l’ascenseur
Réparation audio	04	91	0000000000001	numéro d’identification de l’ascenseur

AVIS
Ce n'est qu'une partie du message de données. Il ne contient pas de début, de somme de contrôle et de fin.

04900000000000000187654321 - Bouton corrigé, numéro d'identification 87654321.

Le message de données se compose des éléments suivants

Commande - Type d'appel - ID

CPC Antenna

Type d'appel	Commande	Type d'appel	Données	ID
Alarme	04	27	-	numéro d’identification de l’ascenseur
Alarme 2	04	27	-	numéro d’identification de l’ascenseur
Appel de contrôle	04	26	-	numéro d’identification de l’ascenseur
Fin de la procédure d'habilitation	04	84	-	numéro d’identification de l’ascenseur

Type d'appel	Commande	Type d'appel	Données	ID
Panne du bouton	04	90	-	numéro d'identification de l'ascenseur
Réparation du bouton	04	90	-	numéro d'identification de l'ascenseur
Dysfonctionnement de l'audio	04	91	-	numéro d'identification de l'ascenseur
Réparation audio	04	91	-	numéro d'identification de l'ascenseur

AVIS
Ce n'est qu'une partie du message de données. Il ne contient pas de début, de somme de contrôle et de fin.

0492687654321 - Appel de contrôle, numéro d'identification 87654321.

Le message de données se compose des éléments suivants

Commande - Type d'appel - DATA - ID

CPC Antenna 2N Ext

Type d'appel	Commande	Type d'appel	Données	ID
Alarme	04	27	00000	numéro d'identification de l'ascenseur
Alarme 2	04	27	00000	numéro d'identification de l'ascenseur

Type d'appel	Commande	Type d'appel	Données	ID
Appel de contrôle	04	26	00000	numéro d'identification de l'ascenseur
Fin de la procédure d'habilitation	04	84	00000	numéro d'identification de l'ascenseur
Panne du bouton	04	90	00000	numéro d'identification de l'ascenseur
Réparation du bouton	04	90	00001	numéro d'identification de l'ascenseur
Dysfonctionnement de l'audio	04	91	00000	numéro d'identification de l'ascenseur
Réparation audio	04	91	00001	numéro d'identification de l'ascenseur

AVIS
Ce n'est qu'une partie du message de données. Il ne contient pas de début, de somme de contrôle et de fin.

04910000087654321 - Erreur audio, ID 87654321.

ATTENTION

- Les informations Bouton corrigé et Audio corrigé ne peuvent être transmises qu'en utilisant le protocole 2N Ext.
- Si le mode 2N Ext n'est pas activé, l'appel de service ne sera pas établi.
- Le protocole CPC utilise jusqu'à 16 chiffres pour le numéro d'identification de l'ascenseur, alors que le protocole P100 n'en utilise que 8.

P100

Le message de données se compose des éléments suivants

Type d'appel - ID - DATA

P100

Type d'appel	Type d'appel	ID	DONNÉES
Alarme	1	numéro d’identification de l’ascenseur	
Alarme 2	1	numéro d’identification de l’ascenseur	
Appel de contrôle	3	numéro d’identification de l’ascenseur	
Fin de la procédure d'habilitation	2	numéro d’identification de l’ascenseur	500
Panne du bouton	2	numéro d’identification de l’ascenseur	800
Réparation du bouton	2	numéro d’identification de l’ascenseur	801
Dysfonctionnement de l’audio	2	numéro d’identification de l’ascenseur	200
Réparation audio	2	numéro d’identification de l’ascenseur	201

AVIS
Ce n'est qu'une partie du message de données. Il ne contient pas de début, de somme de contrôle et de fin.

287654321500 - Processus de décharge terminé, numéro d'identification 87654321.

Essais fonctionnels conformément à la norme EN 81-28

Ce chapitre décrit les procédures de vérification du fonctionnement du système de signalisation d'urgence ALARM dans un ascenseur avec **2N LiftIP 2.0** conformément aux exigences de la norme EN 81-28. Des tests doivent être effectués avant la mise en service de l'ascenseur et régulièrement dans le cadre de la maintenance.

Préparation

1. Ouvrez l'interface de configuration de l'appareil basée sur le web **2N LiftIP 2.0** .
2. Allez sur **Calling > Alarm Calling** et vérifiez les paramètres suivants :
   - La fonction d'appel différé est activée.
   - La fonction **Test Alarm** est activée et la durée de la pression sur le bouton pour activer l'alarme de test est fixée à 30 secondes.
3. Allez sur **Services > Elevator** et vérifiez les paramètres suivants :
   - **Le mode de décharge** est activé.
   - Si l'option **Quitter en entrant le mot de passe** est activée, notez le mot de passe.

6.2.2 Information de signalisation d'urgence ALARME (4.1.2)

1. Appuyez sur le bouton ALARM avec le symbole de la cloche et maintenez-le enfoncé pendant le temps nécessaire au déclenchement de l'alarme de test (min. 30 secondes).
2. Vérifiez que le voyant jaune s'allume et que le signal sonore retentit.
3. Lorsque l'appel est connecté au service de secours, assurez-vous que le voyant vert commence à clignoter.
4. Vérifiez la communication bilatérale avec le service de sauvetage.

6.2.3 Fin de la signalisation d'urgence ALARM (4.1.3)

1. Suivez les étapes du test 6.2.2 Information de signalisation d'urgence ALARME (4.1.2) (p. 87).
2. Appelez le service de secours pour mettre fin à l'appel.
3. Vérifiez que le voyant vert ne s'allume plus lorsque l'appel est terminé. Le voyant jaune reste allumé.
4. Quittez le mode de libération.

   ### Quitter avec le bouton 2

   a. Appuyez sur le bouton 2 pendant 3 secondes.
      Le bouton 2 est un bouton externe branché sur le connecteur du klaxon intitulé ALARM 2 ; l'emplacement est déterminé par l'installateur.

   ### Quitter en entrant un mot de passe

   a. Appelez **2N LiftIP 2.0** - composez **2N LiftIP 2.0**.
   b. Saisissez le mot de passe de validation et confirmez par un astérisque.
5. Vérifiez que le voyant jaune a cessé de s'allumer.

6.2.4 Alimentation électrique de secours (4.1.4)

Les rapports **2N LiftIP 2.0** ne disposent pas de leur propre alimentation électrique de secours. Leur fonctionnement pendant l'alimentation de secours doit être vérifié au niveau de la passerelle/de l'élément fournissant l'alimentation de secours au système de communication d'urgence.

6.2.5 Signaux visuels et sonores dans la cage d'ascenseur (4.1.5)

Pour certaines annonces, les DEL externes sont dirigées vers la cabine d'ascenseur. L'installateur est responsable de leur mise en place. Vérifiez que les DEL externes sont acheminées dans la cabine d'ascenseur.

Rapport	Connecter un appel	Appel en cours	Mode de déclenchement actif	Quitter le mode de récupération
921618B, 2N LiftIP 2.0 COP unit – Flush mounting, EN, With button	LED jaune + alarme sonore	LED jaune + LED verte clignotante	LED jaune	aucune LED n'est allumée
921618 2N LiftIP 2.0 Unité COP - Montage encastré, Sans bouton	LED jaune + alarme sonore	LED jaune + LED verte clignotante	LED jaune	aucune LED n'est allumée

6.2.6 Communication (4.1.8), vérification de la signalisation d'urgence ALARM (4.1.6), identification (4.1.7)

Réponse à la communication

1. Assurez-vous que les portes de l'ascenseur ne sont pas complètement ouvertes.
2. Appuyez sur la touche ALARME avec le symbole de la cloche pendant la durée d'appui sur la touche ALARME (paramètre 962).
3. Vérifiez que le voyant jaune s'allume et que le signal sonore retentit.
4. Lorsque l'appel est connecté au service de secours, assurez-vous que le voyant vert commence à clignoter.
5. Vérifiez la communication bilatérale avec le service de sauvetage.

Vérification et redémarrage de l'ALARME

1. Assurez-vous que les portes de l'ascenseur ne sont pas complètement ouvertes.
2. Appuyez sur la touche ALARME avec le symbole de la cloche pendant la durée d'appui sur la touche ALARME (paramètre 962).
3. Vérifiez que le voyant jaune s'allume et que le signal sonore retentit.
4. Lorsque l'appel est connecté au service de secours, assurez-vous que le voyant vert commence à clignoter.
5. Vérifiez la communication bilatérale avec le service de sauvetage.
6. Appelez le service de secours pour mettre fin à l'appel.
7. Vérifiez que le voyant vert ne s'allume plus lorsque l'appel est terminé. Le voyant jaune reste allumé.
8. Appuyer brièvement sur le bouton ALARM.
9. Assurez-vous qu'un signal sonore indique que l'appel est en cours de connexion. Le système doit établir une connexion immédiatement après une brève pression.
10. Lorsque l'appel est connecté au service de secours, assurez-vous que le voyant vert commence à clignoter.

Il est nécessaire de vérifier que l'appareil est correctement identifié du côté de l'appareil récepteur. Le matériel de réception ne fait pas partie du portefeuille de **2N LiftIP 2.0**.

Accessibilité et fiabilité (4.2.1)

Communication lorsque l'équipement récepteur principal n'est pas disponible et que les enregistrements d'autotests (appels de service) doivent être vérifiés sur l'équipement récepteur. Le matériel de réception ne fait pas partie du portefeuille de **2N LiftIP 2.0**.

Paramètres techniques

Paramètres électriques	
Tension d'alimentation	10-30 V DC (la polarité doit être respectée) ou 48 V PoE 802.3af
Consommation :	max. 2 W (avec haut-parleur intégré), max. 3,5 W (avec haut-parleur connecté avec l'impédance de 4 Ω)
Plage de tension pour les entrées ALARME et ANNULER	
Contributions	5-48 V DC (la polarité doit être respectée)
Paramètres audio	
Haut-parleur:	intégré 16 Ω / 1 W (puissance de sortie 0,45 W) Possibilité d'augmenter la puissance de sortie à 0,75 W en connectant un haut-parleur de 4 Ω
Microphone :	intégré, possibilité de connecter un microphone électret externe
Commutation vocale :	Processeur audio full duplex
Sortie boucle d'induction :	3,35 V RMS, impédance de sortie 100 Ω
Codec :	PCMU, PCMA, G.711 (environ 90 kbit/s), L16, G.722 et G.729
Raccordement d'éléments indicateurs externes	
Tension :	10-30 V DC, alimentation externe
Courant maximal :	200 mA(en utilisant une ampoule de 100 mA max.)

Autres paramètres	
Dimensions :	(L) 65 x (H) 130 x (P) 23 mm
Gamme de températures de fonctionnement :	−20 à 50 °C
Humidité relative :	10% à 90% non-condensée
Altitude recommandée :	0–2000 m

2N LiftIP 2.0 – Manuel d'utilisateur

2N.com