



Interphones IP

Manuel de Configuration



Table des matières

Ports Utilisés	4
Première connexion	8
Recherche d'appareils sur le réseau	8
Nom de domaine	8
Adresse IP de l'équipement	8
Basculement DHCP	10
Accès à la configuration de l'appareil par Internet	11
Changement du mot de passe	12
Navigateurs recommandés	12
Réglages de base de l'appareil	13
Mise à jour du firmware	13
Répertoire	14
Appel	14
Création de contacts d'appel	14
Ajout d'un dispositif local 2N	15
Composer des appels sur l'appareil	16
Appel via SIP	17
Appels locaux entre 2N appareils	19
Accès	19
Paramètres d'accès des utilisateurs	20
Règles d'accès	23
Réglage du commutateur de porte	26
Modules	27
Configuration de l'accès Bluetooth	27
Ascenseur	29
Mise en place de l'authentification des plaques d'immatriculation	29
Paramètres d'affichage	30
Pour télécharger votre propre langue d'affichage	30
Diaporama	30
Mode démo (2N IP Style)	31
Rapports informatifs (2N IP Style)	32
Paramètres avancés	33
Paramètres de l'appareil photo et de la vidéo	33
Réglages internes de l'appareil photo	33
Caméra externe	35
Création d'un flux vidéo	36
Réglages du son	37
Réglage du volume de l'appareil	37
Transmission audio lors des appels	37
Sons Utilisateurs	38
Autres caractéristiques audio de l'appareil	38
Profils de temps	39
Vacances	39
Paramètres avancés du compte SIP	39
Fonctions SIP	40
Les médias	40
Configuration avancée	40
Réglage de l'interrupteur de protection	41
Blocage d'autres interrupteurs lorsque le couvercle est ouvert	41
Événements liés aux interrupteurs de protection	41
Système	42
Réglages de la date et de l'heure	42
Synchronisation avec NTP	42

Mise à jour de l'heure en cas de panne	42
Paramètres du réseau	42
Licence	43
Mise à jour de la clé de licence	43
Licence d'essai	43
Aperçu des fonctionnalités sous licence	44
Journal des événements	45
Signalisation du statut opérationnel	49
Ports Utilisés	50
Automation	54

Ports Utilisés

Service	Port	Proto- coles	Direction	Acti- vé par dé- faut	Confi- gu- rable	Paramètres
802.1x	–	–	Entrée/ Sortie	×	×	–
DHCP	68	UDP	Entrée/ Sortie	✓	×	–
DNS	53	TCP/U DP	Entrée/ Sortie	✓	×	–
Echo (device disco- very)*	8002	UDP	Entrée/ Sortie	✓	×	–
FTP	21	TCP	Sortie	×	×	–
2N IP Eye	8003	UDP	Sortie	×	×	–
HTTP	80	TCP	Entrée/ Sortie	✓	✓	Système > Connexion au réseau > SERVEUR WEB
HTTPS	443	TCP	Entrée/ Sortie	✓	✓	Système > Connexion au réseau > onglet SERVEUR WEB
Multicast audio	22222	UDP	Sortie	×	✓	Intégration > Audio

Ports Utilisés

Service	Port	Proto- coles	Direction	Acti- vé par dé- faut	Confi- gu- rable	Paramètres
Multicast audio pour le protocole ICU	8006	UDP	Sortie	×	×	–
Multicast video pour le protocole ICU	8008	UDP	Sortie	×	×	–
Multicast video (wide) pour le protocole ICU	8016	UDP	Entrée/ Sortie	×	×	–
Client NTP	123	UDP	Entrée/ Sortie	✓	×	–
ONVIF	80, 443, 3702	TCP/U DP	Entrée/ Sortie	×	×	–
Ports RTP+RTCP (SIP)	4900+ (range of 64 ports)	UDP	Entrée/ Sortie	×	✓	Appel > Pa- ramètres généraux
Ports RTP+RTCP (caméra externe)	4800+ (range of 64 ports)	UDP	Entrée/ Sortie	×	✓	Intégration > ONVIF / RTSP
Client RTSP	554	UDP	Entrée/ Sortie	×	✓	
RTSP server	554	UDP	Entrée/ Sortie	×	×	–
SingleWire Com- mands	80	TCP	Entrée/ Sortie	×	×	–
SingleWire Commu- nication	8081	TCP	Sortie	×	×	–
SingleWire Media	20000+	UDP	Entrée	×	×	–

Ports Utilisés

Service	Port	Proto- coles	Direction	Acti- vé par dé- faut	Confi- gu- rable	Paramètres
SLP	427	UDP	Entrée/ Sortie	✓	×	–
SIP	5060, 5062	TCP/U DP	Entrée/ Sortie	×	✓	Appel > SIP
SIPS	5061	TCP	Entrée/ Sortie	×	✓	Appel >SIP
SMTP	25	TCP	Sortie	×	✓	Intégration > Notifica- tions par courrier électroni- que
Syslog	514	UDP	Sortie	×	×	–
TFTP	69	UDP	Sortie	×	×	–
My2N Knocker	443	TCP	Sortie	✓	×	–
My2N Tribble Tunnel	443	TCP	Sortie	✓	×	–
SNMP Agent	161	UDP	Entrée/ Sortie	✓	×	–
SNMP Trap	162	UDP	Sortie	✓	×	–
SSDP	1900	UDP	Entrée/ Sortie	✓	×	–
SDDP	1902	UDP	Entrée/ Sortie	✓	×	–

Ports Utilisés

Service	Port	Proto- coles	Direction	Acti- vé par dé- faut	Confi- gu- rable	Paramètres
Multicast receiver (Automation)	4433	UDP	Entrée	×	×	–
WS-Discovery	3702	UDP	Entrée/ Sortie	✓	×	–
CIP Client (Cre- stron)	41794	UDP	Entrée/ Sortie	×	×	–
Sitechannel (proto- cole ICU)	8004	UDP	Entrée/ Sortie	×	×	–
Multicast DNS	5353	UDP	Entrée/ Sortie	✓	×	–

Première connexion

Recherche d'appareils sur le réseau

Pour accéder à l'interface, vous devez connaître l'adresse IP de l'appareil ou son nom de domaine. L'appareil doit être connecté au réseau IP local et doit être alimenté.

Nom de domaine

Pour accéder à l'interface de configuration web, vous pouvez saisir un nom de domaine dans le navigateur sous le format « hostname.local » au lieu de l'adresse IP. Le nom d'hôte d'un nouvel appareil se compose du nom du produit et du numéro de série de l'appareil. Lorsque vous saisissez un nom d'hôte, utilisez uniquement des lettres et des chiffres ; n'utilisez pas d'espaces, de points, de tirets ou d'autres caractères spéciaux.

Le nom de domaine par défaut de l'appareil : 2NIPIntercom20-{numéro de série sans tirets}.local (par exemple.: « 2NIPIntercom20-000000001.local »)

Le format du nom de l'appareil spécifique est spécifié dans le manuel d'installation du produit au chapitre Nom de domaine.



ASTUCE

Vous pouvez modifier le nom d'hôte ultérieurement dans l'interface de configuration Web à l'adresse **Système > Connexion réseau > Onglet Configuration avancée > Nom d'hôte**.

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

Adresse IP de l'équipement

Par défaut, l'appareil utilise une adresse IP dynamique attribuée par le serveur DHCP.

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.

En tenant compte des capacités de l'appareil en question, il est également possible de connaître l'adresse IP de l'une des manières suivantes :

- Bouton de numérotation rapide
- sur l'écran de l'appareil (voir le Guide d'installation du produit pour la procédure)

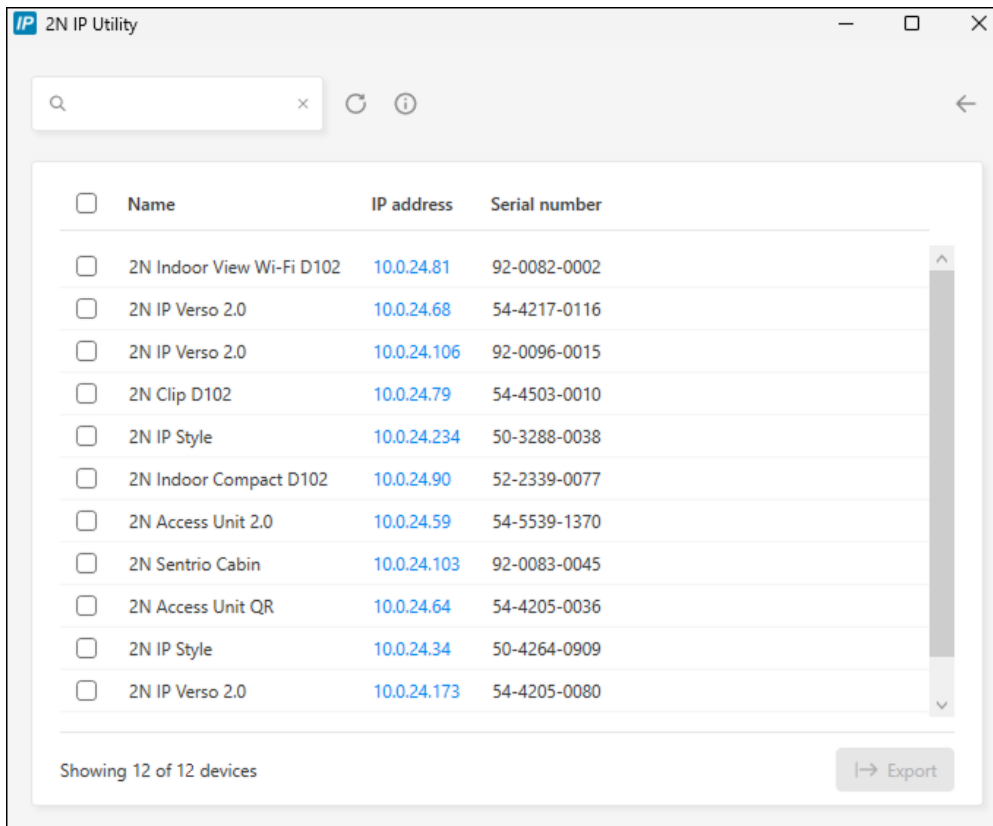
Recherche de l'adresse IP à l'aide de 2N IP Utility

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.



<input type="checkbox"/>	Name	IP address	Serial number
<input type="checkbox"/>	2N Indoor View Wi-Fi D102	10.0.24.81	92-0082-0002
<input type="checkbox"/>	2N IP Verso 2.0	10.0.24.68	54-4217-0116
<input type="checkbox"/>	2N IP Verso 2.0	10.0.24.106	92-0096-0015
<input type="checkbox"/>	2N Clip D102	10.0.24.79	54-4503-0010
<input type="checkbox"/>	2N IP Style	10.0.24.234	50-3288-0038
<input type="checkbox"/>	2N Indoor Compact D102	10.0.24.90	52-2339-0077
<input type="checkbox"/>	2N Access Unit 2.0	10.0.24.59	54-5539-1370
<input type="checkbox"/>	2N Sentries Cabin	10.0.24.103	92-0083-0045
<input type="checkbox"/>	2N Access Unit QR	10.0.24.64	54-4205-0036
<input type="checkbox"/>	2N IP Style	10.0.24.34	50-4264-0909
<input type="checkbox"/>	2N IP Verso 2.0	10.0.24.173	54-4205-0080

Showing 12 of 12 devices Export

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.)

Trouver l'adresse IP à l'aide du bouton Speed Dial

Afin de retrouver l'adresse IP procédez comme suit :

1. Connectez l'appareil à l'alimentation (ou déconnectez-le et reconnectez-le s'il est déjà connecté).
2. Pressez 5x la première touche de Numérotation rapide sur l'unité principale.
3. L'appareil lit son adresse IP.



NOTE

- Si l'adresse est 0.0.0.0, cela signifie que l'appareil n'a pas obtenu d'adresse IP du serveur DHCP.
- La succession des touches peut être saisie au maximum dans les trente secondes qui suivent le signal sonore pour des raisons de sécurité. Jusqu'à 2 s d'intervalle sont autorisées entre chaque pression.

Basculement DHCP

Par défaut, l'appareil utilise une adresse IP dynamique attribuée par le serveur DHCP.

Adresse IP dynamique

DHCP (Dynamic Host Configuration Protocol) est un protocole réseau qui tient à jour une liste d'adresses IP disponibles et les attribue automatiquement aux appareils du réseau local. L'adresse IP attribuée est dynamique, de sorte que l'appareil peut se voir attribuer une nouvelle adresse IP après un certain temps (bail).

Adresse IP statique

Si l'adresse IP de l'appareil doit rester inchangée, vous devez désactiver l'attribution d'adresses IP par le serveur DHCP sur l'appareil. Vous pouvez désactiver le serveur DHCP dans l'interface de configuration web ou en utilisant le matériel de l'appareil.



NOTE

Les valeurs spécifiques de l'adresse IP statique ne peuvent être définies que dans l'interface de configuration web de l'appareil.

Réglage des paramètres réseau dans l'interface de configuration web

1. Accédez à l'interface de configuration web.
2. Allez sur **System > Network Connection > Basic Settings tab > IP Address Settings**.
3. Réglez les paramètres réseau souhaités.
4. Enregistrez vos modifications.

Commutation du DHCP sur le matériel de l'appareil

Selon les capacités de l'appareil, l'adresse IP peut être modifiée comme suit :

- Bouton de numérotation rapide
- sur l'écran de l'appareil (voir le Guide d'installation du produit pour la procédure)



ASTUCE

Veuillez consulter le manuel d'installation du produit pour connaître l'emplacement du bouton RESET.

Trouver l'adresse IP à l'aide du bouton Speed Dial

Afin de retrouver l'adresse IP procédez comme suit :

1. Connectez l'appareil à l'alimentation (ou déconnectez-le et reconnectez-le s'il est déjà connecté).
2. Pressez 5x la première touche de Numérotation rapide sur l'unité principale.
3. L'appareil lit son adresse IP.



NOTE

- Si l'adresse est 0.0.0.0, cela signifie que l'appareil n'a pas obtenu d'adresse IP du serveur DHCP.
- La succession des touches peut être saisie au maximum dans les trente secondes qui suivent le signal sonore pour des raisons de sécurité. Jusqu'à 2 s d'intervalle sont autorisées entre chaque pression.

Accès à la configuration de l'appareil par Internet

La configuration de l'appareil s'effectue par le biais d'une interface de configuration basée sur le Web, accessible à partir d'un navigateur Web.

Pour accéder à l'interface, vous devez connaître l'adresse IP de l'appareil ou son nom de domaine. L'appareil doit être connecté au réseau IP local et doit être alimenté.



L'interface de configuration basée sur le web est également accessible depuis le portail My2N connecté ou depuis l'outil de configuration 2N Access Commander.

Se connecter à l'interface de configuration web

1. Démarrez votre navigateur Internet.
2. Saisissez l'adresse IP de l'appareil ou le nom de domaine de l'appareil (voir chapitre [Recherche d'appareils sur le réseau \(p. 8\)](#)).

3. Si aucun certificat n'a été généré pour l'adresse IP, vous pouvez recevoir un avertissement concernant un certificat de sécurité non valide. Dans ce cas, il faut confirmer que vous voulez passer à l'interface web de configuration.
4. Après l'avoir saisie, un écran de connexion s'affichera.
5. Entrer les identifiants de connexion
Les identifiants de connexion par défaut sont :
 - Nom d'utilisateur : **Admin**
 - Mot de passe : **2n**
6. Après la première connexion, modifiez le mot de passe.

Accès à partir de 2N Commandant d'accès

1. Connectez-vous à l'interface Access Commander.
2. Allez sur  Devices.
3. Pour l'appareil sélectionné, appuyez sur .

Changement du mot de passe

Vous devez modifier le mot de passe par défaut pour accéder à toutes les fonctions de l'interface de configuration web. Vous ne pouvez pas configurer l'appareil sans modifier le mot de passe par défaut.



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.

Réglages de base de l'appareil

Mise à jour du firmware

Les nouvelles versions du micrologiciel sont disponibles sur le serveur de mise à jour. Si l'interface de configuration web n'a pas accès à l'internet public, il est possible de télécharger manuellement le fichier du micrologiciel sur l'appareil.



NOTE

Les mises à jour du micrologiciel ne sont pas automatiques. 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.

Obtenir le micrologiciel à partir du serveur de mise à jour

1. Allez sur **Système > Maintenance > onglet Firmware**.
2. Cliquez sur **Vérifier les mises à jour**.
3. Lorsqu'une mise à jour est disponible, ses notes de mise à jour sont chargées. Pour lancer la mise à niveau, cliquez sur **Upgrade** dans l'en-tête de la fenêtre.
4. Après un upload réussi du firmware, l'appareil redémarre automatiquement. Après le redémarrage, l'appareil est entièrement disponible avec le nouveau micrologiciel. La mise à niveau du firmware n'affecte pas la configuration

Téléchargement d'un nouveau micrologiciel à partir de la mémoire

1. Allez sur **Système > Maintenance > onglet Firmware**.
2. Cliquez sur **Upload Firmware**.
3. Dans la boîte de dialogue qui s'ouvre, sélectionnez un fichier de votre propre référentiel.
4. Confirmez le téléchargement du fichier en cliquant sur **Upload**.
car l'appareil vérifie le fichier pour empêcher le téléchargement d'un fichier.
5. Après un upload réussi du firmware, l'appareil redémarre automatiquement. Après le redémarrage, l'appareil est entièrement disponible avec le nouveau micrologiciel. La mise à niveau du firmware n'affecte pas la configuration



NOTE

La fonctionnalité, la fiabilité et la sécurité de l'appareil dépendent du firmware installé. La mise à jour régulière du firmware à la version actuelle fait partie des conditions d'utilisation du produit. Les erreurs qui peuvent être causées par l'utilisation d'une version obsolète du firmware ne peuvent pas faire l'objet d'une réclamation. Le firmware actuel met en œuvre les expériences des clients et les exigences dans le domaine de la sécurité des données personnelles.

Répertoire

La section Répertoire est un élément clé de la configuration de l'appareil. Vous créez des utilisateurs dans l'annuaire et gérez leurs droits d'accès ou les paramètres de la connexion téléphonique. Chaque utilisateur peut agir en tant que détenteur de droits d'accès, contact d'appel ou les deux à la fois.

Ajouter manuellement un utilisateur à un répertoire

1. Sur la page Annuaire, cliquez sur **Ajouter un utilisateur**.
2. La fiche de l'utilisateur s'ouvre. Dans l'onglet Informations personnelles, donnez un nom à l'utilisateur.
3. Définissez le numéro de téléphone de l'appareil du contact selon [Création de contacts d'appel \(p. 14\)](#).
4. Définissez les options d'accès en fonction de [Accès \(p. 19\)](#).

Gestion des utilisateurs en masse dans Access Commander ou My2N

Si l'appareil est géré par les outils de configuration en bloc Access Commander ou My2N, toute modification apportée à l'interface de configuration basée sur le Web est remplacée par les paramètres de l'outil de configuration en bloc. Un utilisateur créé directement dans l'interface web sera supprimé.

La colonne holder de la table de répertoire indique l'outil de configuration en bloc qui a créé l'utilisateur. La colonne holder est masquée par défaut.

Appel

Le dispositif 2N permet de connecter les appels de plusieurs manières. Avant de pouvoir créer des contacts et de configurer la méthode de numérotation, vous devez d'abord activer et configurer les services qui serviront de médiateur à l'appel :

- [Appel via SIP \(p. 17\)](#)
- [Appels locaux entre 2N appareils \(p. 19\)](#)
- autres intégrations spéciales


Création de contacts d'appel

La création d'un contact d'appel consiste à ajouter un numéro de téléphone à l'utilisateur correspondant dans le répertoire de l'appareil.



ASTUCE

Vous pouvez utiliser la fonction d'appels locaux pour vous connecter à un autre appareil 2N sur votre réseau local, voir [Ajout d'un dispositif local 2N \(p. 15\)](#).

1. Allez sur le site **Annuaire**.
2. Ouvrez les détails de l'utilisateur en cliquant sur la ligne ou sélectionnez **Add User** pour créer un nouvel utilisateur.
3. Dans l'onglet **Phone Numbers de**, ouvrez l'édition du numéro de téléphone en cliquant sur l'icône .
4. Sélectionnez **Type d'appel**, dans lequel le contact doit être disponible (SIP, réseau local, MS Teams, VMS, ...).
 - [Appel via SIP \(p. 17\)](#) - pour les services et comptes VoIP
 - [Appels locaux entre 2N appareils \(p. 19\)](#) - pour les appels vers 2N dispositifs
 - MS Teams, VMS,... - pour des intégrations spéciales
5. Saisissez le numéro ou l'adresse de destination que l'appareil doit appeler. Saisissez le numéro de poste, l'URI SIP (par exemple, « sip:101@192.168.1.50 »), le nom de domaine (par exemple, « 2NIPVerso20-22222222 » ou tout autre numéro correspondant au type d'appel).

6. Dans le champ **Options**, définissez des fonctions d'appel supplémentaires qui affectent le comportement de l'appel.
Ces options permettent à l'administrateur de configurer la sécurité, la fonctionnalité et la logique de numérotation pour répondre aux besoins exacts de l'établissement, par exemple pour utiliser une transmission cryptée, accélérer la connexion ou activer l'inversion de la porte.
7. Dans la section **Disponibilité de**, spécifiez l'heure limite à laquelle le numéro peut être appelé. Par exemple, vous pouvez définir la disponibilité uniquement pendant les heures de travail de l'utilisateur.
8. Sauvegardez la modification en cliquant sur **Confirmez**.
9. Si vous souhaitez utiliser le bouton de numérotation rapide pour appeler le contact, affectez un bouton au contact dans l'onglet **Buttons**.

Configuration de 2N IP Eye

Application 2N IP Eye vous permet de visualiser la vidéo de l'interphone IP sur l'écran de votre ordinateur. Après avoir introduit l'adresse **du 2N IP Eye**, lorsqu'un contact effectue un appel entrant, la vidéo s'affiche sur l'ordinateur.

L'adresse est saisie sous la forme : `domain[:port1][:port2]`

- `eye_computer.company.cz`
- `192.168.22.111:8009:8080`

Les paramètres `port1` et `port2` sont facultatifs. Saisissez-les si la traduction d'adresse (NAT) est en cours entre l'appareil 2N IP et l'ordinateur avec 2N IP Eye. Configurez les ports en fonction de la configuration du routeur ou d'un autre dispositif NAT.

- `port1` - valeur par défaut 8003, port de destination pour la réception des messages UDP de l'application 2N IP Eye.
- `port2` - valeur par défaut 80, port de destination pour la communication HTTP entre l'application 2N IP Eye et l'appareil 2N IP.

Ajout d'un dispositif local 2N



ATTENTION

Les appels locaux doivent être activés à la fois sur ce dispositif et sur le dispositif recherché avec la même clé d'accès, voir [Appels locaux entre 2N appareils \(p. 19\)](#).

1. Sur la page **Directory** cliquez sur **Add Local Device**.
2. Dans la boîte de dialogue qui s'ouvre, cochez le périphérique auquel vous souhaitez vous connecter.
3. Sélectionnez **Ajouter au répertoire**.
4. Un nouvel utilisateur apparaît dans le répertoire avec un numéro de téléphone défini.
5. Cliquez sur la ligne de l'utilisateur pour la modifier davantage.



ASTUCE

Pour définir les droits d'accès du détenteur de cet appareil, suivez les instructions suivantes : [Accès \(p. 19\)](#).

Composer des appels sur l'appareil

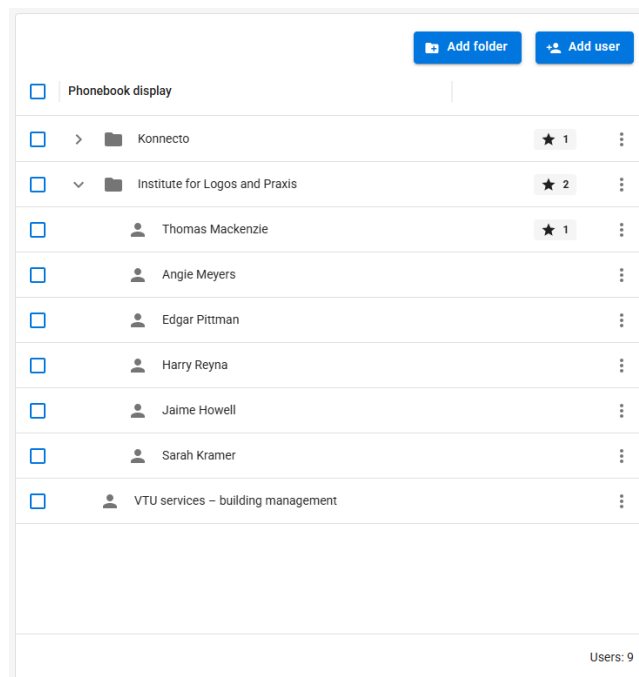
Attribution des boutons d'appel rapide

Pour affecter des contacts aux boutons de numérotation rapide, allez sur **Calling > Dialing > Speed Dial Dialtons tab**.

Les boutons de sélection rapide des modules connectés à l'unité principale via VBUS sont également réglés ici.

Pour afficher les contacts du carnet d'adresses sur l'écran

Pour définir l'affichage et l'ordre des contacts sur l'écran de l'appareil, allez sur **Calling > Dialing > Phonebook Display tab**.




Tous les contacts auxquels un numéro de téléphone a été attribué sont stockés par défaut dans le dossier du coffre. Les contacts peuvent être classés dans des dossiers, par exemple par département ou par étage.


Déplacer des contacts dans un dossier


1. Dans l'en-tête du tableau de l'annuaire, créez un nouveau dossier et nommez-le.



ASTUCE

Dans le menu d'extension  pour un dossier, vous pouvez ajouter une image au dossier sous lequel elle apparaîtra à l'écran dans la vue Répertoire.


2. Pour déplacer vos contacts vers un autre dossier, sélectionnez-les d'abord, puis cliquez sur .
3. Sélectionnez un nouvel emplacement dans le répertoire téléphonique.
4. Sauvegardez vos modifications en cliquant sur **Move**.

Dans chaque dossier, les contacts sont généralement classés par ordre alphabétique. Cet ordre peut être modifié en définissant la priorité (dans le menu étendu  pour le contact).

Un utilisateur nouvellement créé avec un numéro de téléphone apparaîtra automatiquement dans le dossier du coffre.

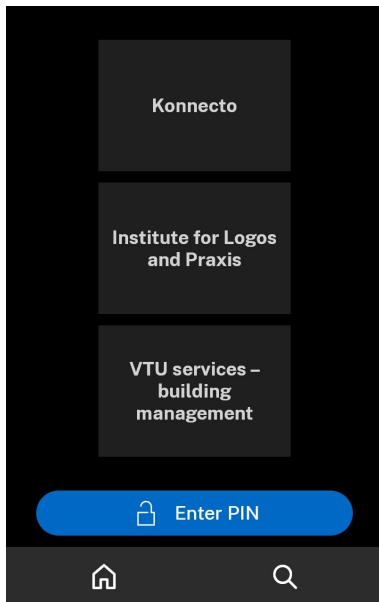
Groupes d'appel

Les groupes d'appel permettent d'appeler plusieurs contacts en même temps (par exemple, appeler la réception et l'entrepôt en même temps).

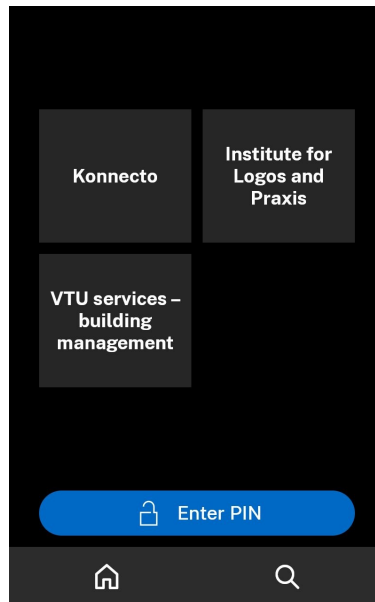
1. Dans le tableau **Phonebook view**, sélectionnez tous les contacts que vous souhaitez intégrer au groupe.
2. Au-dessus du tableau, cliquez sur .
3. Indiquez le nom du groupe d'appel et son emplacement dans l'annuaire.
4. Choisissez si vous souhaitez que les contacts restent visibles en tant que contacts individuels ou s'ils ne sont affichés que dans le répertoire sous le groupe d'appel.
5. Sauvegardez vos modifications en cliquant sur **Move**.

Paramètres d'affichage 2N IP Style

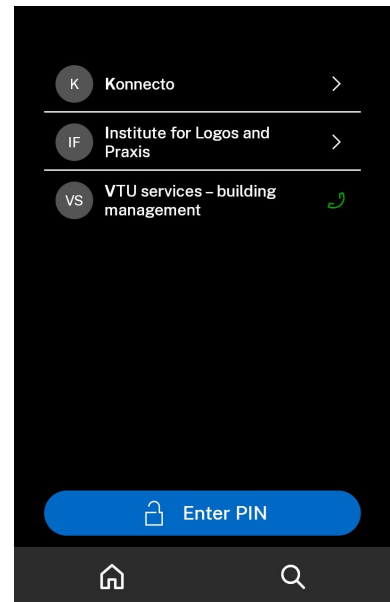
Dans l'onglet de gauche **Display Settings** vous pouvez choisir parmi les façons suivantes d'afficher le répertoire sur l'écran de l'appareil **2N IP Style**.



Cartes (1 colonne)



Cartes (2 colonnes)



Phonebook

Appel via SIP

Enregistrement de l'appareil auprès du serveur SIP

L'enregistrement sur le serveur SIP est essentiel pour que l'appareil fonctionne pleinement dans un environnement SIP.

1. Allez sur **Calling > SIP** du compte que vous voulez configurer.
2. Activez le compte SIP en haut de la page.
3. Dans l'onglet, **Device Identity**, remplissez le formulaire :
 - **Nom d'affichage** - ce texte sera affiché à l'autre partie comme identification de l'appelant.
 - **Numéro de téléphone (ID)** - ce numéro, associé au domaine, identifie l'appareil de manière unique lors des appels et de l'enregistrement.
 - **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 SIP.Ces trois valeurs permettent d'identifier l'appareil dans l'environnement SIP.

4. Dans **Authentication**, indiquez les informations d'identification attribuées par l'administrateur du serveur SIP pour authentifier l'appareil auprès du serveur mandataire SIP. Cette authentification permet d'éviter les accès non autorisés, les appels frauduleux ou l'usurpation d'identité.
Si l'ID d'authentification **n'est pas renseigné dans**, l'appareil s'authentifiera avec **Numéro de téléphone**.
5. Sous **Transport Protocol Options**, sélectionnez le protocole utilisé par le serveur SIP.
6. Activez la fonctionnalité de l'onglet **SIP Registrar**.
7. Complétez les détails du registraire SIP auprès duquel vous souhaitez enregistrer l'appareil 2N.
Si vous laissez le paramètre **Port** vide ou si la valeur du paramètre est 0, le port par défaut est appliqué en fonction du protocole de transport sélectionné.

Valeurs par défaut des ports en fonction du protocole de transport

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

8. L'en-tête de l'onglet indique l'état de l'enregistrement et affiche les messages d'erreur d'enregistrement.



NOTE

D'autres paramètres du compte SIP sont décrits dans le chapitre [Paramètres avancés du compte SIP \(p. 39\)](#).

Pour définir l'adresse IP publique d'un appareil

Ce paramètre est utilisé lorsque l'appareil est situé derrière un routeur (NAT) et qu'il communique avec le panneau de contrôle en dehors du réseau local (par exemple, dans le nuage ou sur Internet). Dans la communication SIP, l'appareil doit spécifier l'adresse IP publique sous laquelle il est accessible depuis l'internet. S'il envoyait son adresse IP interne, le PBX ne pourrait pas acheminer correctement l'appel ou le flux de données RTP.

Si l'appareil et le PBX se trouvent sur le même réseau local, il n'est pas nécessaire de définir une adresse IP publique.

1. Allez sur **Calling > SIP** du compte que vous voulez configurer.
2. Dans l'onglet, **sélectionnez l'adresse IP publique** parmi les options suivantes :
 - **STUN (Automatique)**
Complétez les détails de votre serveur STUN.
 - **Saisir manuellement**
Saisissez votre propre adresse IP externe pour l'appareil.

Appels locaux entre 2N appareils

Il est possible d'établir des appels dits locaux entre les appareils 2N IP, qui permettent une communication directe entre les appareils 2N au sein d'un réseau local sans qu'il soit nécessaire de se connecter à un serveur SIP ou à une infrastructure externe.

Pour activer les appels locaux

1. Allez sur **Appels > Appels locaux**.
2. Activez la fonctionnalité dans l'en-tête de la page.
3. Définissez des clés d'accès pour garantir une communication sécurisée avec les autres appareils du réseau.

Les clés d'accès garantissent que seuls les appareils possédant des clés identiques peuvent communiquer entre eux. Cela contribue à la sécurité et à la possibilité de définir des groupes d'appareils indépendants.

Accès

L'une des fonctions de base du dispositif est de gérer l'accès et le déverrouillage de la serrure électrique de la porte. L'appareil gère l'accès en fonction de l'évaluation des demandes d'accès selon des règles d'accès prédéfinies. Si le dispositif juge la demande légitime, il active l'interrupteur de porte qui commande le verrouillage électrique de la porte. Cela déverrouillera la porte.

Outre l'authentification conventionnelle de l'utilisateur (carte RFID, biométrie, Bluetooth, etc.), l'interrupteur peut également être activé à l'aide de signaux et d'interfaces externes, ce qui offre des possibilités d'intégration et d'automatisation flexibles. Les différentes manières d'activer l'interrupteur de porte sont décrites ci-dessous :

Vérification de l'utilisateur

L'utilisateur utilise sa méthode d'authentification et si ses droits d'utilisateur sont conformes aux règles d'accès, l'accès lui est accordé. L'accès autorisé activera l'interrupteur de la porte.

La configuration est décrite dans le chapitre [Paramètres d'accès des utilisateurs \(p. 20\)](#).

Contrôle du commutateur dans l'interface de configuration web

1. Allez sur **Integration > Switches**.
2. Trouvez la carte d'interrupteur qui contrôle la porte.



NOTE

La fonction d'interrupteur de porte dans l'appareil est assurée par **Switch 1**.

3. Sous **Manual Switch Control** cliquez sur **Hold**.
4. L'interrupteur reste allumé jusqu'à ce que vous annuliez à nouveau le maintien en commande manuelle.

Arrêt en fonction du profil horaire

Dans l'interface de configuration web, vous pouvez régler l'interrupteur pour qu'il maintienne la porte déverrouillée pendant une période prédéterminée, par exemple à l'heure du déjeuner.

1. Allez sur **Integration > Switches**.
2. Trouvez la carte d'interrupteur qui contrôle la porte.



NOTE

La fonction d'interrupteur de porte dans l'appareil est assurée par **Switch 1**.

3. Cliquez sur la flèche → du commutateur sélectionné pour accéder à ses détails.
4. Dans l'onglet **Status**, activez l'option **Time controlled hold switch**.
5. Sélectionnez les profils de temps dans lesquels le commutateur doit être maintenu ou entrez une période de temps personnalisée.

Désactiver l'interrupteur lors d'un appel (DTMF)

Paramètres du code DTMF

1. Allez sur **Integration > Switches**.
2. Trouvez la carte d'interrupteur qui contrôle la porte.



NOTE

La fonction d'interrupteur de porte dans l'appareil est assurée par **Switch 1**.

3. Cliquez sur la flèche → du commutateur sélectionné pour accéder à ses détails.
4. Dans l'onglet **Activation Codes de**, vous pouvez définir les codes que vous pourrez saisir par DTMF lors d'un appel avec l'appareil.

La validité de chaque code peut être limitée dans le temps.



NOTE

Pour le premier code d'activation, vous pouvez faire en sorte qu'il soit traité comme une ancienne forme du code. Dans ce formulaire, vous ne devez pas confirmer le code par un astérisque lorsque vous le saisissez sur le clavier du téléphone.

Utiliser le code DTMF

1. Une fois connecté à l'appareil, entrez le code d'activation sur le clavier de votre téléphone et confirmez par un astérisque.



NOTE

La réception des signaux DTMF est activée par défaut sur l'appareil. Vous pouvez vérifier les autorisations sur la page Call Service (SIP/Local Calls) sous l'onglet **Audio**, sous l'onglet **Receive DTMF**.

Déconnexion du commutateur à l'aide de l'API HTTP

L'utilisation complète, y compris une description de l'autorisation API HTTP nécessaire, est décrite dans le manuel HTTP / api switch ctrl. Pour le commutateur 1, la commande se présente comme suit : `https://ip_adre-sa/api/switch/ctrl?switch=1&action=on`.

Arrêt par automatisation

La configuration de l'automatisation est décrite dans le manuel d'automatisation . Le commutateur est déclenché par l'action **ActivateSwitch**.

Paramètres d'accès des utilisateurs

Pour s'authentifier auprès de l'unité de contrôle d'accès et déverrouiller la porte, l'utilisateur doit remplir deux conditions : avoir des droits d'accès attribués au dispositif et disposer d'au moins une méthode d'authentifi-

cation. Les méthodes d'authentification disponibles dépendent de l'appareil spécifique et peuvent inclure des cartes RFID, un code PIN numérique, un code QR à scanner par l'appareil photo, etc.

Paramètres d'authentification :

1. Allez sur le site **Annuaire**.
2. Ouvrez les détails de l'utilisateur en cliquant sur la ligne ou sélectionnez **Add User** pour créer un nouvel utilisateur.
3. Dans l'onglet **Authentication** définissez toutes les méthodes d'authentification de l'utilisateur, voir [Méthodes d'authentification \(p. 21\)](#).
4. Dans l'onglet Paramètres d'accès du site , **indiquez à quel moment l'utilisateur doit avoir accès à l'entrée et à la sortie.**
 - N'importe quand
 - Profil temporel - propose un ensemble de profils temporels
 - Personnalisé - utilisez le bouton **Edit** pour définir des intervalles de temps propres à cet utilisateur.Définissez une date d'expiration pour limiter l'accès de l'utilisateur à une période spécifique du calendrier.
L'octroi de **Exceptions** permettra à l'utilisateur d'avoir un accès permanent qui ne restreindra même pas le verrouillage temporaire du dispositif indiqué par les règles d'accès (voir [Règles d'accès \(p. 23\)](#)).

Méthodes d'authentification



ATTENTION

Les méthodes d'authentification disponibles dépendent de l'appareil et des modules connectés.

Carte RFID

Un utilisateur peut se voir attribuer jusqu'à 2 cartes RFID.

L'identifiant peut être saisi manuellement à l'aide du clavier ou lu en insérant la carte dans un lecteur USB connecté à l'ordinateur.

Exigences relatives aux cartes RFID

- L'identifiant doit être un nombre hexadécimal.
- La longueur minimale de l'identifiant est de 6 caractères.
- Seules les cartes prises en charge par l'appareil peuvent être utilisées - le type de carte doit être activé dans les paramètres du module (voir **Access > Modules**).



ASTUCE

Vous pouvez lire l'identifiant d'une carte existante dans le journal à l'adresse suivante : **Système > Journal des événements**. Chargez la carte nouvelle/non assignée sur l'appareil, puis copiez son identifiant (UUID) à partir du journal. Après avoir inséré l'identifiant entre les cartes RFID, l'utilisateur peut commencer à utiliser la carte pour s'authentifier.

My2N

My2N - utilisé pour se connecter à l'application My2N permettant l'authentification via Bluetooth.

Code PIN / Code QR

Le PIN sert de code d'accès numérique personnel, que l'utilisateur saisit sur le clavier de l'appareil ou qui peut être scanné par l'appareil photo de l'appareil sous la forme d'un code QR.



ATTENTION

Les codes QR ne peuvent être lus que par l'appareil photo interne de l'appareil.

Exigences en matière de code PIN

- La longueur minimale est de 2 chiffres.
- Le code ne peut contenir que des chiffres (0-9).
- Les codes QR ne peuvent être utilisés que pour des codes PIN de 4 à 15 chiffres.
- Si vous utilisez la fonction d'alarme silencieuse, nous vous recommandons de créer des codes PIN pairs.



NOTE

Lorsque vous utilisez un code QR hexadécimal, la valeur doit être convertie au format décimal avant d'être saisie.

Plage hexadécimale acceptée : De 1000 à FFFFFFFF.

Empreinte digitale

Chaque utilisateur peut télécharger jusqu'à deux empreintes digitales. Utilisez un lecteur d'empreintes digitales externe pour les télécharger. Assurez-vous d'avoir installé le pilote USB 2N. Le pilote peut être téléchargé [ici](#).

L'empreinte digitale téléchargée d'un utilisateur peut être utilisée pour les actions suivantes :

- Ouvrir la porte;
- Démarrer une alarme silencieuse - peut être défini uniquement si la fonction Ouverture de porte est active ;
- Automation F1 et F2 - génère l'événement FingerEntered dans Automation. F1 et F2 sont utilisés pour distinguer le doigt attaché dans Automation.

Plaque d'immatriculation

Certains appareils prennent en charge la reconnaissance des plaques d'immatriculation des véhicules à l'aide de caméras AXIS externes équipées de l'application complémentaire **VaxALPR**. Les plaques d'immatriculation reconnues sont envoyées dans une requête HTTP au point de terminaison `api/lpr/license-plate` (plus d'informations sur le manuel HTTP API pour les interphones IP).



ASTUCE

La procédure d'ajout d'une caméra externe est décrite à l'adresse [???](#).

Plaque d'immatriculation – définit la plaque d'immatriculation du véhicule de l'utilisateur, que l'appareil peut scanner et utiliser pour authentifier l'utilisateur.

Exigences en matière de plaques d'immatriculation :

- La longueur maximale d'une plaque d'immatriculation est de 10 caractères.
- Jusqu'à 20 plaques d'immatriculation peuvent être attribuées à un utilisateur.
- Chaque plaque d'immatriculation ne doit être attribuée qu'à un seul utilisateur - en cas d'attributions multiples, le premier enregistrement trouvé est utilisé.
- Les plaques d'immatriculation sont utilisées dans la fonction de reconnaissance à partir de l'image de la caméra externe (voir le manuel d'interopérabilité).

Carte virtuelle

La carte virtuelle est utilisée pour identifier l'utilisateur dans les appareils connectés via l'interface Wiegand. Après l'authentification réussie de l'utilisateur via l'application My2N ou sur le lecteur biométrique, l'ID de la carte virtuelle est envoyé à l'interface Wiegand (si l'envoi d'identifiants est activé dans la configuration, voir **Access > Access Rules > Access/Egress tab > Advanced**).

Exigences relatives aux cartes virtuelles :

- L'ID doit être un nombre hexadécimal (caractères 0-9, A-F).
- La longueur de l'identifiant est comprise entre 6 et 32 caractères.
- Un utilisateur ne peut se voir attribuer qu'une seule carte virtuelle.

Code de l'interrupteur

Code de commutation – permet de configurer jusqu'à 4 codes pour activer les interrupteurs (par exemple serrure de porte). Le code de l'interrupteur permet d'ouvrir la serrure à l'aide du clavier de l'appareil ainsi qu'un code DTMF.

Règles d'accès

La page **Access > Access Rules** définit les paramètres et la logique de déverrouillage de la porte, qui est gérée par le commutateur de porte de l'appareil. Cette configuration détermine la manière dont les demandes d'accès (authentification) sont évaluées, les conditions nécessaires à la réussite de l'autorisation de l'utilisateur et les règles de gestion des accès individuels.

Alors que vous définissez les autorisations individuelles dans les paramètres de l'utilisateur, les règles d'accès déterminent quand, dans quelles conditions et comment ces autorisations peuvent être utilisées. Par exemple, vous pouvez déterminer si le passage de la porte est autorisé dans une seule direction, si l'authentification peut déclencher une alarme silencieuse ou si l'utilisateur ne peut s'authentifier qu'une seule fois par intervalle de temps défini.

État des portes et des serrures

L'onglet Statut indique si l'interrupteur de porte est actif et si la porte est ouverte.

Porte

- « Ouvert » - l'accès a été accordé, le commutateur de porte est fermé et la porte peut être ouverte.
- « Fermé » - la porte est verrouillée et ne peut être ouverte.

Serrure

- « Déverrouillé » - l'interrupteur est actif, il peut être actionné.
- « Locked » - le commutateur est désactivé et ne peut pas être contrôlé par des règles d'accès.



ASTUCE

Le bouton avec le symbole de verrouillage sur cet onglet est utilisé pour verrouiller ou déverrouiller le commutateur à partir de l'interface web.

Détection de porte

Dans l'onglet **Doors**, peut être activé pour que l'ouverture non autorisée d'une porte ou l'ouverture prolongée d'une porte déclenche un événement. Cet événement peut ensuite être suivi par des automatismes. Les événements sont également inscrits dans le logo de l'appareil.

Arrivée et départ


Un seul appareil peut être utilisé pour gérer des passages dans deux directions. Vous pouvez fixer certains modules sur le dispositif du côté opposé de la porte, puis régler ces deux côtés séparément. Ainsi, vous pouvez restreindre l'heure à laquelle le passage sera autorisé dans la direction **Arrivée** et l'heure à laquelle le passage sera autorisé dans la direction **Départ**, ou les méthodes d'authentification qui seront acceptées dans une direction donnée, etc.

Assignation d'un module pour l'arrivée ou le départ

1. Allez sur **Access > Access Rules**.
2. Dans l'onglet **Arrivée** ou **Départ** sous **Modules** cliquez sur **Gérer**.
3. Une boîte de dialogue s'ouvre avec une liste des modules de gestion d'accès disponibles.
4. Glissez et déposez les modules dans des groupes en fonction de l'orientation qu'ils sont censés donner.



ASTUCE

Cliquez sur  pour localiser un module spécifique. Le module déclenche un signal visuel ou sonore en fonction de ses capacités.

Règles d'accès

Les règles d'accès déterminent les méthodes d'authentification qui seront acceptées pour accorder l'accès. Il est possible de définir plusieurs règles d'accès pour différents profils temporels. Les règles d'accès peuvent également être utilisées pour déterminer quand un accès doit être refusé.

Vous pouvez utiliser des règles d'accès pour restreindre les méthodes d'authentification acceptées. Par exemple, vous pouvez obliger les utilisateurs à utiliser une carte RFID de 8h00 à 9h00.



ASTUCE

La restriction d'authentification est utile à utiliser sur un périphérique qui gère les clés de **2N IP Fortis**. Les utilisateurs seront donc obligés de mettre à jour régulièrement les clés de **2N IP Fortis** sur leur carte RFID.

Lors de la définition des règles, vous pouvez choisir d'utiliser ou non un code de zone pour ouvrir la porte. **Le code de zone** est appliqué lorsque l'appareil est zoné dans un système de gestion globale des appareils (tel que Access Commander). **Le code de zone** peut également être défini manuellement dans la section **Advanced**. Il fonctionne de la même manière que le code d'activation de l'interrupteur ; en le saisissant sur le clavier du module, vous activez l'interrupteur de la porte.

Alarme silencieuse

L'alarme silencieuse est un mode spécial d'ouverture de la serrure qui vous permet de déclencher une action de sécurité discrètement. L'alarme silencieuse est utilisée en particulier dans les locaux et les bâtiments recherchés par les voleurs : casinos, centres financiers, banques, etc. Après avoir introduit le code PIN, la porte s'ouvre, mais en même temps l'alarme est activée sans que l'attaquant s'en aperçoive.

L'activation de l'alarme silencieuse déclenche l'événement **SilentAlarm**. Cet événement peut être suivi d'une automatisation, par exemple :

- Envoi d'une requête HTTP au système de sécurité.
- Prendre des photos à partir de l'appareil photo de l'appareil.
- Établissement d'un appel vers une destination prédéfinie.

Activation de l'alarme silencieuse

1. L'utilisateur saisit un code supérieur d'une unité à son code PIN normal.
Exemple : L'utilisateur a défini un code PIN « 1926 ». Entrez le code « 1927 » pour ouvrir la porte. La porte s'ouvre et l'événement SilentAlarm se déclenche en même temps.



ATTENTION

Pour pouvoir ouvrir la porte avec un code PIN (même si l'alarme silencieuse est déclenchée en même temps), il est nécessaire d'activer l'onglet **In/Out sous**.

Blocage de l'accès après des tentatives infructueuses

Après cinq tentatives d'accès consécutives infructueuses, l'accès sera bloqué pendant 30 secondes. L'accès ne sera pas autorisé pendant cette période, même si l'authentification de l'utilisateur est valide.

Cette fonction ne bloque l'accès qu'avec l'autorisation de l'utilisateur. L'interrupteur de porte peut également être commuté par d'autres méthodes telles que DTMF, commande HTTP, etc.

Lecture des codes QR

Le code PIN d'accès ou le code d'activation de l'interrupteur attribué à l'utilisateur peut être lu par la caméra sous la forme d'un code QR.

Pour un chargement correct, vous devez définir le mode de lecture du code QR . **Les codes sont toujours stockés dans l'appareil en format décimal. Lorsqu'ils sont lus en mode décimal, les codes QR lus doivent correspondre exactement aux codes PIN (de 4 à 15 chiffres) enregistrés dans l'appareil. En mode hexadécimal, les codes QR sont convertis au format décimal après lecture, puis comparés aux codes décimaux enregistrés. Les zéros pré-alignés sont ignorés lors de la lecture hexadécimale.**



NOTE

Plage hexadécimale acceptée : De 1000 à FFFFFFFF.

Pour la lecture d'un code QR, vous pouvez également le configurer pour qu'il déclenche uniquement l'événement **CodeEntered** au lieu de contrôler l'interrupteur de la porte. Cet événement peut ensuite être suivi d'autres actions par le biais d'automatismes.

Le code QR scanné peut être transmis à un système de contrôle d'accès externe qui communique via une interface Wiegand (voir ???).

Anti-Passback

L'anti-passback est une extension du système de contrôle d'accès qui empêche l'entrée pendant un intervalle de temps déterminé. Dans ce mode, l'appareil ne permet à l'utilisateur d'entrer qu'une seule fois dans un laps de temps donné. Lorsqu'un utilisateur réussit à entrer dans le système, celui-ci enregistre cet événement et l'utilisateur ne peut accéder à nouveau au système qu'après l'écoulement du délai spécifié. Ce temps est défini lorsque l'anti-passback est activé.

Modes de la fonction Anti-passback

- « Hard » - L'utilisateur ne peut pas passer à travers le dispositif dans n'importe quelle direction pendant la période de temps définie. L'utilisateur se voit refuser l'accès jusqu'à l'expiration de l'intervalle ou jusqu'à ce que l'administrateur de l'appareil rétablisse l'accès.
- « Soft » - Les violations de règles sont uniquement enregistrées et peuvent alerter l'administrateur, mais l'utilisateur est autorisé à y accéder.

Transfert de données pour Wiegand



ATTENTION

Pour transmettre des données Wiegand, un module d'extension Wiegand doit être correctement connecté à l'appareil. Le module d'expansion Wiegand n'est généralement pas inclus dans l'emballage du produit.

La fonction de transmission Wiegand permet au dispositif de transmettre les données d'identification de l'utilisateur authentifié à un système de contrôle d'accès externe qui communique via l'interface Wiegand. Cela permet d'intégrer les dispositifs 2N aux systèmes de contrôle d'accès traditionnels. Ce paramètre vous permet de sélectionner le groupe approprié pour l'acheminement des données.

Le transfert de données pour Wiegand est configuré dans **Access > Access Rules > Input/Output > Advanced**. L'envoi d'autorisations aux utilisateurs qui ont lu leur code QR est défini dans l'onglet **Access/Exit** pour l'activation de la lecture du code QR.

Réglage du commutateur de porte

L'interrupteur de porte est une fonction logique du dispositif qui commande la serrure électrique de la porte. L'interrupteur peut être activé de différentes manières (par exemple, par une commande HTTP, une carte RFID ou un signal DTMF).

La fonction d'interrupteur de porte dans l'appareil est assurée par **Switch 1**.

La page **Access > Modules** peut ensuite être utilisée pour affecter un module d'accès spécifique au contrôle d'un autre commutateur.

Réglage de l'interrupteur de porte

1. Connectez les contacts électriques de la serrure de la porte (par exemple, le contact magnétique) à l'entrée désignée de l'interphone.
2. Dans l'interface de configuration web, allez sur **Integration > Switches**.
3. Ouvrez les paramètres du commutateur 1 en cliquant sur la flèche dans l'en-tête de l'onglet.

4. Dans l'onglet **Configuration de l'interrupteur**, définissez les paramètres de la sortie matérielle que l'interrupteur de porte doit contrôler.
- **Sortie contrôlée** - spécifie la sortie qui commute le verrouillage électrique de la porte.
 - **Mode** - Monostable / Bistable.
 - Durée d'enclenchement – **paramétrez la durée de temporisation pour un interrupteur monostable. Cette valeur n'est pas appliquée dans le mode bistable.**
 - **Type de sortie** - dans le mode « Security », la sortie fonctionne en mode inversé, ce qui signifie qu'elle est activée en permanence et qu'elle commande le relais de sécurité à l'aide d'une séquence d'impulsions spécifique. Si vous utilisez une serrure de porte inversée (c'est-à-dire que la serrure est verrouillée lorsque l'alimentation est appliquée), réglez le type de sortie sur « Inverse ».



ASTUCE

Si vous utilisez un relais de sécurité, réglez le type de sortie sur « Security ».

Si plusieurs interrupteurs avec des types de sortie différents sont connectés à une sortie, ils sont contrôlés selon la priorité suivante :

1. Sécurité
 2. Inversé
 3. Normal
5. Dans les onglets **Activation** et **Activation Codes**, vous pouvez définir d'autres moyens d'activer le commutateur. Si vous ne définissez pas d'autres méthodes, l'interrupteur ne sera activé que si l'accès de l'utilisateur est autorisé.
6. Enregistrez les modifications.

Modules

La page **Access > Modules** permet une gestion centralisée de toutes les technologies matérielles d'accès sur l'appareil. Chaque module dispose de son propre onglet sur la page qui permet de le gérer. Les modules directement intégrés dans l'unité principale de l'appareil et ceux qui sont connectés via VBUS sont gérés ici.

Chaque module peut être nommé et un interrupteur spécifique peut lui être attribué. Les autres paramètres dépendent du type de module.

Dans les réglages d'usine, tous les modules commandent l'interrupteur de porte.



NOTE

Si les versions du firmware du module à connecter et de l'unité principale ne sont pas compatibles, le module ne sera pas détecté. Dans ce cas, mettez à jour le micrologiciel de l'appareil ([Mise à jour du firmware \(p. 13\)](#)) après avoir connecté le module.

Configuration de l'accès Bluetooth

L'authentification de l'utilisateur via Bluetooth se fait via l'application My2N app, que l'utilisateur doit avoir téléchargé sur son téléphone mobile.






ATTENTION

Le réglage du code d'appariement doit actuellement être effectué dans l'ancienne interface de configuration.

Créer un code d'appairage sur l'appareil

1. Allez sur **Directory** et ouvrez les détails de l'utilisateur pour lequel vous voulez créer le code de correspondance.
2. Dans l'en-tête de l'interface de configuration web, cliquez sur **Go to the old interface**.
Ouvre le détail de l'utilisateur dans l'ancienne interface de configuration.
3. Dans le bloc **WaveKey**, cliquez sur .
La boîte de dialogue qui s'ouvre génère un code de couplage que vous devez saisir dans l'application My2N sur votre appareil.
4. Ouvrez l'application et saisissez le code PIN de couplage.



NOTE

Si vous avez déjà une application connectée à un autre appareil, vous pouvez saisir le code PIN de couplage via l'icône d'ajout en haut de l'écran.

5. Suivez les instructions de votre téléphone portable - approchez l'appareil en mode appairage et cliquez sur **Démarrer l'appairage**.



AVERTISSEMENT


Pour les téléphones mobiles dotés de systèmes d'exploitation plus anciens (Android 9 / iOS 17 et versions antérieures), vous devrez utiliser l'application pour le couplage Mobile Key.

Couplage dans l'application mobile Mobile Key

1. Téléchargez l'application Mobile Key sur votre téléphone portable. L'application est disponible sur [App store](#) et [Google Play](#).
2. Ouvrez l'application et activez l'application Mobile Key accès au Bluetooth.
3. Selon le type de clé mobile, approchez le lecteur USB ou le dispositif d'appairage avec le téléphone mobile.
4. Dans l'application Mobile Key cliquez sur l'appareil proposé à associer.
5. L'application vous invite à saisir un code PIN. Saisissez le code d'appairage et confirmez sa saisie.

Méthodes d'authentification Bluetooth

Différentes méthodes d'authentification Bluetooth peuvent être définies dans l'interface de configuration web.

- **Directement dans l'application mobile** - l'utilisateur sélectionne la porte qu'il souhaite ouvrir directement dans l'application mobile My2N. Si son appareil mobile est à portée de l'appareil 2N, il se connectera à l'appareil et si les règles d'accès sont respectées, la porte se déverrouillera.
- **En approchant le téléphone mobile de l'appareil et en touchant l'appareil** - un utilisateur disposant d'un appareil mobile et de la fonction Bluetooth s'approche de l'appareil 2N et touche l'emplacement d'authentification Bluetooth sur l'appareil 2N, qui est généralement marqué par l'icône Bluetooth . Une fois la connexion établie et les droits d'accès vérifiés, la porte est déverrouillée.

- **Détection de mouvement** - Les appareils 2N équipés d'une caméra détectent les mouvements dans l'environnement et activent automatiquement le Bluetooth. Si un dispositif 2N détecte l'appareil mobile d'un utilisateur avec un accès valide à portée, la porte se déverrouille.

Définition des méthodes d'authentification Bluetooth acceptées

1. Allez sur **Access > Modules**.
2. Dans l'onglet **pour le module Bluetooth**, sélectionnez les méthodes possibles dans le champ **Start Authentication**.
3. Si vous avez sélectionné « motion detection », sélectionnez le profil par lequel le mouvement doit être détecté.




NOTE

Les profils de détection de mouvement sont définis dans **Customization > Camera > Internal Camera**.


Ascenseur

En connectant le module relais AXIS A9188 à un interphone 2N ou à une unité de contrôle d'accès 2N, il est possible de contrôler l'accès à des étages d'ascenseurs individuels dans le bâtiment. Un maximum de 8 de ces modules relais peuvent être connectés à un interphone 2N ou à une unité d'accès 2N, chacun d'entre eux pouvant contrôler 8 étages, pour un total de 64 étages. Pour utiliser cette fonction, vous devez disposer d'une licence active : pour les interphones IP (n° de commande 9137916) ou pour les unités d'accès (n° de commande 9160401).

Connexion à l'ascenseur

1. Connectez les entrées des contrôleurs d'ascenseur au relais AXIS A9188 et connectez le relais au réseau IP. Notez l'adresse IP du relais.
Suivez la documentation du module relais E/S AXIS A9188, disponible à l'adresse <http://www.axis.com>.
2. Ouvrez l'interface de configuration Web du dispositif 2N qui doit gérer les accès à l'ascenseur.
3. Allez sur **Integration > Access Control > Elevator tab**.
4. Sur l'onglet **Relay Modules (AXIS A9188)**, activez l'un des modules.
5. Cliquez sur l'icône du crayon  et entrez l'adresse IP du module relais dans la boîte qui s'ouvre.
6. Si l'accès au relais est soumis à une authentification, saisissez le nom d'utilisateur et le mot de passe dans l'onglet **General**.
7. Lorsque le module relais est activé, les étages gérés par ce module apparaissent dans l'onglet **Elevator Floors**. Vous pouvez nommer chaque étage.

Mise en place d'un accès public à l'étage

1. Dans l'onglet **Elevator Floors**, sélectionnez les étages qui doivent être accessibles au public (l'accès n'est pas soumis à autorisation).
2. Cliquez sur l'icône du crayon  à côté de l'étage sélectionné.
3. Dans les paramètres ouverts, activez **Public Access**.
4. Vous pouvez également limiter le temps d'accès du public en sélectionnant un profil de temps ou en définissant un temps d'accès personnalisé.

Mise en place de l'authentification des plaques d'immatriculation

Certains appareils prennent en charge la reconnaissance des plaques d'immatriculation des véhicules à l'aide de caméras AXIS externes équipées de l'application complémentaire **VaxALPR**. Les plaques d'imma-

tricolation reconnues sont envoyées dans une requête HTTP au point de terminaison `api/lpr/license-plate` (plus d'informations sur le manuel HTTP API pour les interphones IP).



ASTUCE

La procédure d'ajout d'une caméra externe est décrite à l'adresse ???.

Activation des services API HTTP

L'authentification de la plaque d'immatriculation est évaluée sur la base de la requête HTTP. Par conséquent, vous devez activer les services API HTTP appropriés sur l'appareil. Ce réglage est encore effectué dans une ancienne version de l'interface de configuration web. Pour la procédure détaillée, voir [FAQ](#).

Paramètres d'affichage

Pour télécharger votre propre langue d'affichage

L'interface de configuration basée sur le web vous permet de personnaliser les textes en langue affichés sur l'écran de l'appareil. Vous pouvez ainsi adapter l'appareil à un environnement linguistique différent ou afficher des messages personnalisés.

1. Dans l'interface de configuration web, allez sur **Customization > Display**.
2. Dans l'onglet **Langue**, téléchargez le modèle de fichier de traduction. Le modèle contient des textes en anglais par défaut.
3. Ouvrez le fichier téléchargé dans un éditeur de texte.
4. Remplacez les expressions anglaises du fichier par vos propres textes.



ATTENTION

Ne modifiez pas la structure et le format des phrases clés. Si la syntaxe est modifiée ou si certains éléments sont manquants, le fichier de traduction risque de ne pas se charger correctement.

5. Enregistrez le fichier modifié au format `.ini`.
6. Retournez à l'onglet **Language** dans l'interface web et sélectionnez « Custom » dans le menu déroulant des langues.
7. L'option de téléchargement de fichier apparaît - sélectionnez et téléchargez votre fichier `.ini` modifié.
8. Enregistrez les modifications après le téléchargement réussi.

Diaporama




NOTE

Sur l'écran **2N IP Style**, d'autres modes de démonstration peuvent être définis en plus de la présentation (voir [Mode démo \(2N IP Style\)](#) (p. 31)).

La présentation est un mode de démonstration qui affiche une séquence d'images et de vidéos à l'écran. Vous pouvez définir la durée d'affichage de chaque élément (image ou vidéo).

1. Allez sur **Customization > Display**.

2. Activez la fonctionnalité dans l'en-tête de l'onglet **Presentation**.
3. Définissez la durée pendant laquelle vous souhaitez que l'écran d'accueil passe en mode aperçu.
4. Pour chaque élément, vous pouvez spécifier s'il doit être affiché uniquement dans une fenêtre temporelle spécifique ou en dehors de celle-ci. Pour visualiser la fenêtre temporelle, cliquez sur [Editer la présentation](#). Développez le menu avancé en cliquant sur  pour un élément spécifique afin de définir quand l'élément doit être affiché dans la présentation.
5. Enregistrez les modifications.

Mode démo (2N IP Style)

Le mode démo sur **2N IP Style** est l'état d'affichage dans lequel l'appareil passe après une certaine période d'inactivité sur l'écran d'accueil. L'écran de l'appareil peut afficher, par exemple, une série de photos ou de vidéos, l'adresse d'un bâtiment ou la date et l'heure.



NOTE

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


Paramètres du mode de prévisualisation

1. Allez sur **Customization > Display**.
2. Dans l'en-tête de l'onglet, **activez la fonction de prévisualisation de**.
3. Définissez la durée pendant laquelle vous souhaitez que l'écran d'accueil passe en mode aperçu.
4. Sélectionnez le type de mode d'échantillonnage choisi.
5. Vous pouvez activer l'affichage de pictogrammes d'information sur la surface antibactérienne ou l'icône tactile dans la section **Affichage des icônes sur le site**.
6. Enregistrez les modifications.

Diaporama

La présentation est un mode de démonstration qui affiche une séquence d'images et de vidéos à l'écran. Vous pouvez définir la durée d'affichage de chaque élément (image ou vidéo).

Pour chaque élément, vous pouvez spécifier s'il doit être affiché uniquement dans une fenêtre temporelle spécifique ou en dehors de celle-ci. Pour visualiser la fenêtre temporelle, cliquez sur [Editer la présentation](#).

Développez le menu avancé en cliquant sur  pour un élément spécifique afin de définir quand l'élément doit être affiché dans la présentation.

Logo

Mode **Logo** est utilisé pour afficher un logo d'entreprise statique à l'écran.

Vous pouvez télécharger une image d'arrière-plan pour l'affichage (derrière le logo) dans l'onglet **Image d'arrière-plan**.

Texte

Le mode **Text** affiche un texte statique à l'écran, qui peut être, par exemple, l'adresse de l'établissement, un message de bienvenue ou d'autres informations destinées aux personnes qui se déplacent dans l'établissement.

Date et heure

Mode **Date et heure** affiche la date, l'heure actuelle de l'appareil et l'emplacement de l'appareil.

Rapports informatifs (2N IP Style)

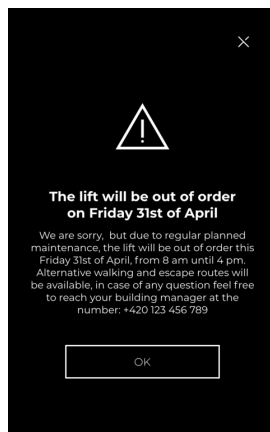
L'appareil **2N IP Style** peut afficher sur son écran des messages d'information configurables à l'avance. Après avoir obtenu l'autorisation d'accès, les utilisateurs ou les visiteurs peuvent recevoir un message qui les guide dans le bâtiment, les informe des événements qui s'y déroulent, etc.

Dans chaque onglet, vous pouvez définir des messages d'information spécifiques pour chacun des événements suivants :

- **Utilisateur autorisé** - Ce message apparaît sur l'écran après qu'un utilisateur enregistré dans le répertoire de l'appareil s'est authentifié auprès de l'appareil.
- **Visiteur** – ce message s'affiche quand un accès est autorisé au visiteur pendant un appel. Le visiteur est une personne ayant commencé à partir de l'appareil un appel pour l'utilisateur dans un répertoire. Le message apparaît lorsque cet utilisateur accorde l'accès au visiteur pendant l'appel.
- **Accès refusé** – ce message s'affiche quand l'appareil refuse l'accès.

Paramètres du message d'information

1. Allez sur **Access > Newsletters**.
2. Dans les onglets de la page, sélectionnez le type de message d'information que vous souhaitez mettre en place.
3. Activez le message d'information dans l'en-tête de l'onglet.
4. Dans l'onglet **Scheduling and time settings**, définissez l'heure à laquelle le message horaire doit être affiché ainsi que la durée pendant laquelle le message d'information doit rester affiché. Vous pouvez également spécifier la période du calendrier pour laquelle le message doit être affiché.
5. Dans l'onglet **Message Content de**, créez un message. Vous pouvez créer un message texte ou insérer une image.
6. Enregistrez les modifications.



Exemple de message d'information avec image et texte

Paramètres avancés


Paramètres de l'appareil photo et de la vidéo

La caméra des interphones 2N transmet l'image à l'autre partie lors d'un appel vidéo, détecte les mouvements dans l'environnement et lit les codes QR,

Il est possible de connecter des caméras externes à l'appareil, à partir desquelles il sera possible d'afficher l'image. Lors d'un appel, vous pourrez voir la vue d'une autre caméra en plus de la vidéo de l'appareil appelé.

Il est possible de connecter des caméras externes à l'appareil, à partir desquelles il sera possible de lire l'image.

Réglages internes de l'appareil photo

1. Allez sur **Customization > Camera**.
2. Dans l'onglet **Caméra interne**, cliquez sur .
3. L'onglet **Settings** vous permet de modifier les paramètres de base de l'image de la caméra.
4. Après l'enregistrement, les modifications seront reflétées dans l'aperçu de l'appareil photo.

Mode

Le mode caméra vous permet de définir la combinaison optimale du mode d'exposition et de la fréquence d'alimentation pour obtenir des images stables et de haute qualité. Ce mode est utilisé pour réduire le scintillement indésirable qui peut se produire lors de l'utilisation d'un éclairage artificiel ou lorsque la fréquence du réseau varie. Lorsque les caméras sont installées à l'intérieur, il est possible de sélectionner une méthode appropriée pour supprimer le scintillement causé par les sources lumineuses, tandis que lorsqu'elles sont placées à l'extérieur, un mode de suppression de la lumière directe du soleil peut être activé pour garantir une adaptation optimale de l'image aux conditions d'éclairage actuelles.

IR LED

La fonction de rétroéclairage IR LED est utilisée pour garantir une image de haute qualité, même en cas de faible luminosité ambiante. Ce mode est déclenché lorsque les conditions de luminosité tombent en dessous du niveau défini. Le niveau limite des conditions d'éclairage n'est défini qu'après l'activation de l'éclairage LED IR.



NOTE

Si la consommation d'énergie autorisée risque d'être dépassée - par exemple, lorsque plusieurs modules d'extension alimentés par PoE fonctionnent simultanément - le niveau d'alimentation IR est automatiquement optimisé pour maintenir la stabilité de l'appareil.

Paramètres avancés

Mode jour/nuit - permet de passer d'une image couleur à une image noir et blanc en fonction des conditions d'éclairage. Réglez **Always Day**, si vous souhaitez que la caméra utilise un filtre de suppression des infrarouges et que le rétroéclairage infrarouge soit désactivé. Le réglage "Toujours nuit", en revanche, désactive le filtre et active l'éclairage infrarouge, ce qui fait passer l'image en mode noir et blanc, adapté à la vision nocturne. Le mode Auto fait basculer la caméra entre ces deux états en fonction de la luminosité ambiante.

Contraste local - améliore les détails et les textures en augmentant les différences de luminosité entre les zones adjacentes de l'image (bords).

Tone Mapping - augmente la luminosité et la visibilité de l'image, mais peut entraîner une légère distorsion des couleurs.



Temps d'exposition maximum - Spécifie le temps d'exposition maximum de l'image. Lorsque davantage de lumière est disponible, l'obturateur peut ne pas être ouvert en permanence et l'appareil photo définit alors automatiquement une durée d'exposition actuelle plus courte.

Détection des mouvements

La détection de mouvement sur les appareils 2N est une fonction qui détecte automatiquement les mouvements dans le champ de vision de la caméra interne et vous permet de déclencher diverses actions, telles que l'activation du Bluetooth ou l'envoi d'une notification.

Pour des performances optimales, la détection peut être calibrée en fonction de l'environnement et des conditions, par exemple en modifiant les paramètres de sensibilité et la zone à surveiller par la caméra.

Paramètres de détection des mouvements

1. Allez sur **Customization > Camera**.
2. Dans l'onglet **Caméra interne**, cliquez sur .
3. Dans l'onglet **Camera Preview (Aperçu de la caméra)**, cliquez sur l'icône de crayon  à côté du paramètre **Motion Detection (Détection de mouvement)**.
4. Une fenêtre s'ouvre avec les paramètres du profil de détection de mouvement.
5. Développez l'onglet du profil que vous souhaitez configurer.
6. En ajustant le carré dans l'aperçu de la caméra d'une zone spécifique dans laquelle la caméra doit enregistrer des mouvements.



ATTENTION

La zone d'image est relative à la découpe de l'image actuelle. Si vous modifiez le cadrage de l'image de la caméra, les zones existantes resteront les mêmes, mais couvriront effectivement une autre partie de l'espace. Il est donc toujours recommandé de vérifier et d'ajuster ces zones après l'édition d'une découpe.

7. Sélectionnez le mode de capture de mouvement pour le profil, voir [Modes de profil \(p. 34\)](#)
8. Ajustez les autres paramètres, si nécessaire, en fonction du mode.
9. N'oubliez pas d'activer le profil !
10. Pour enregistrer vos modifications, cliquez sur **Save** ou **Save and Close** en haut de la page.

Modes de profil

Déclenchement d'événements

Dans ce mode, la caméra capture des mouvements instantanés et uniques. Un exemple de cas d'utilisation est la prise d'une photo lorsque quelqu'un entre dans une pièce ou lorsqu'un véhicule passe à proximité de l'appareil.

L'activation de l'événement déclenché peut être retardée en utilisant le délai défini.

Utilisez le filtre pour définir les types de mouvements que vous souhaitez que la caméra ignore - par exemple, les petits objets (petits oiseaux) ou les mouvements répétitifs (arbres dans le vent).

Enregistrement

Ce profil déclenche un événement de 30 secondes lorsqu'un mouvement est détecté. Si un autre mouvement se produit pendant cette période, le profil combinera le tout en un seul événement. Ce mode convient à la surveillance continue et évite la création d'un grand nombre d'enregistrements courts.

Utilisez le filtre pour définir les types de mouvements que vous souhaitez que la caméra ignore - par exemple, les petits objets (petits oiseaux) ou les mouvements répétitifs (arbres dans le vent).

Détection des visages

Le profil détecte un mouvement lorsqu'un visage apparaît dans la zone surveillée. Un événement peut également se produire lorsqu'une image statique d'un visage (par exemple une photographie) apparaît dans le cadre.

Détection des personnes entrantes

Le profil ne reconnaît que les personnes en mouvement et ignore les images statiques de visages.

Politique de confidentialité



La fonction de confidentialité masque une partie de l'image afin qu'elle ne soit pas visible ou enregistrée dans la vidéo. Cette option est idéale pour les situations où vous souhaitez protéger des zones sensibles de l'image, par exemple. Par exemple, si l'appareil est placé à la réception et que la caméra filme également le couloir où se déplacent des étrangers, vous pouvez masquer la zone du couloir.



ATTENTION

La protection de la vie privée peut limiter l'activité de lecture des codes QR ou la détection des mouvements. Nous ne recommandons pas d'utiliser la protection de la confidentialité en même temps que ces fonctions.

Paramètres de détection des mouvements

1. Allez sur **Customization > Camera**.
2. Dans l'onglet **Caméra interne**, cliquez sur .
3. Dans l'onglet **Camera Preview**, cliquez sur l'icône du crayon  à côté du paramètre **Privacy**.
4. Dans l'aperçu de l'appareil photo, ajustez le carré pour couvrir la zone que vous souhaitez masquer.



ATTENTION

La zone d'image est relative à la découpe de l'image actuelle. Si vous modifiez le cadrage de l'image de la caméra, les zones existantes resteront les mêmes, mais couvriront effectivement une autre partie de l'espace. Il est donc toujours recommandé de vérifier et d'ajuster ces zones après l'édition d'une découpe.

5. Sélectionnez le mode d'occultation :
 - **Couleur** - la zone sélectionnée est recouverte de la couleur de votre choix.
 - **Mosaïque** - la zone sélectionnée sera pixélisée. Définissez la taille de la mosaïque en fonction du niveau d'anonymisation des données requis.
6. N'oubliez pas d'activer la protection de la vie privée dans l'en-tête des paramètres !
7. Pour enregistrer vos modifications, cliquez sur **Save** ou **Save and Close** en haut de la page.

Caméra externe

La caméra externe est ajoutée au périphérique 2N sous forme de flux vidéo (RTSP). La connexion d'une caméra externe vous permet de passer d'une vue à l'autre pendant un appel. La fonction de la caméra externe est donc purement d'imagerie.

**ATTENTION**

Les codes QR ne peuvent être lus que par l'appareil photo interne de l'appareil.

Ajout d'une caméra externe :

1. Allez sur **Customization > Camera**.
2. Sous l'onglet **Caméra externe** sélectionnez **Ajouter une caméra**.
3. Dans la boîte de dialogue qui s'ouvre, activez la caméra.
4. Entrez l'adresse de la source du flux de la caméra IP externe au format `rtsp://ip_address_camera/parameters`.
5. Si le flux de la caméra externe est soumis à une authentification, remplissez **avec les détails de connexion pour le flux**.
6. Enregistrez vos modifications en cliquant sur **Add camera**.
7. Si la caméra externe doit être la caméra principale de l'appareil, après l'avoir enregistrée dans l'onglet **External Camera** cliquez sur **Set as default source**.

Lorsque vous parlez à l'appareil, l'image de l'appareil photo défini comme source par défaut s'affiche en premier.

Créer un flux vidéo à partir de la caméra de l'appareil

La fonction de diffusion vidéo est utilisée pour transmettre la vidéo en direct de la caméra du dispositif via le réseau à un dispositif de réception tel qu'une application sur un téléphone portable, un logiciel de suivi ou sur un ordinateur dans un lecteur vidéo. Ce processus garantit que les utilisateurs peuvent regarder des vidéos en temps réel à partir d'un grand nombre d'appareils.

Création d'un flux vidéo

1. Allez sur **Integration > ONVIF / RTSP**.
2. Activez le service du serveur RTSP.
3. Définissez les paramètres du flux, voir [Paramètres du flux vidéo \(p. 36\)](#).
4. Dans l'onglet **Connection Restrictions**, vous pouvez indiquer les adresses IP à partir desquelles le flux sera disponible. Si aucune adresse IP n'est renseignée, il est possible de se connecter à partir de n'importe quelle adresse IP.
5. Dans l'onglet **Preconfigured Streams**, indiquez si le flux doit être accessible :
 - anonymement
 - avec authentification - définissez les détails de l'authentification dans l'onglet **Authentication**.
6. Dans l'onglet **Preconfigured Streams**, vous trouverez les adresses IP des flux configurés en fonction du codec vidéo sélectionné.

Paramètres du flux vidéo**Paramètres généraux du flux**

Compensation de gigue – paramétrez la capacité tampon pour la compensation de gigue dans les transmissions de paquets audio. Une mémoire plus longue signifie une plus grande immunité aux pannes, mais un retard audio plus important.

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

Unicast UDP activé – activez l'envoi de flux audio/vidéo via RTP/UDP. Si ce mode est éteint, les données de flux audio/vidéo sont uniquement envoyées via RTP/RTSP.

Initial RTP port - réglez le port RTP local de départ dans l'intervalle de la longueur de 60 ports à utiliser pour les transmissions audio et vidéo. La valeur par défaut est 4800 (c.-à-d. que l'intervalle utilisée est 4800–4863).

Zipstream - sélectionne le niveau de compression Zipstream initial (pour H.264). AXIS Zipstream préserve tous les détails légaux importants dont vous avez besoin tout en réduisant les besoins de transfert et de stockage de données de 50 % en moyenne.

Mise en place de flux de formats personnalisés

1. Dans l'onglet **Streams du format personnalisé**, cliquez sur **Generate stream URL**. Une boîte de dialogue s'ouvre.
2. Dans la boîte de dialogue, définissez :
 - **Codec** - sélectionne parmi les codecs disponibles
 - **Activer l'audio** - spécifie s'il faut transmettre de la vidéo uniquement ou de la vidéo avec de l'audio
 - **Résolution** - définit la résolution de l'image
 - **Framerate** - définit la fréquence d'images de la vidéo enregistrée
 - **Bitrate** - définit le bitrate
 - **Zipstream** - sélectionne le niveau de compression Zipstream initial (pour H.264). AXIS Zipstream préserve tous les détails légaux importants dont vous avez besoin tout en réduisant les besoins de transfert et de stockage de données de 50 % en moyenne.
3. L'adresse du flux avec les paramètres est automatiquement chargée au bas de la boîte de dialogue.
4. Copiez l'adresse du flux et enregistrez vos modifications.

Réglages du son

Réglage du volume de l'appareil

Pour régler le volume de votre appareil, allez sur **Personnalisation > Audio**.

Le volume général détermine le niveau de volume de base de tous les autres sons de l'appareil. Réglez ce paramètre en fonction du niveau de bruit de l'environnement dans lequel l'appareil est installé. Le réglage des autres sons est donc toujours relatif à ce volume global .

Volume adaptable

Dans l'onglet **Adaptive Volume**, vous pouvez activer le réglage automatique du volume en fonction du bruit ambiant. Cette caractéristique est particulièrement adaptée aux installations dans des environnements où le bruit ambiant est variable.

Dans l'onglet, réglez **Sensitivity Threshold**, après quoi le volume de l'appareil commencera à augmenter. L'appareil peut être amplifié jusqu'à une valeur réglable **Amplification maximale du son**.

Transmission audio lors des appels

Les paramètres audio de l'appel sont définis directement dans l'onglet du service qui fournit l'appel ([Appel via SIP \(p. 17\)](#) ou [Appels locaux entre 2N appareils \(p. 19\)](#)), dans l'onglet **Video**.

1. Ouvrez la section **Appeler**.
2. Accédez à la page du service qui fournit l'appel (compte SIP spécifique, appels locaux).
3. Ouvrez l'onglet **Audio**.
4. Dans cet onglet, réglez les paramètres sonores nécessaires.

Activation de la transmission des signaux DTMF

En utilisant les commandes DTMF envoyées à ce dispositif, il est possible d'activer sa serrure de porte et donc d'ouvrir la porte.

1. Ouvrez la section **Appeler**.
2. Accédez à la page du service qui fournit l'appel (compte SIP spécifique, appels locaux).

3. Ouvrez l'onglet **Audio**.
4. Dans l'onglet **Sending DTMF**, sélectionnez **Sending Mode** pour déterminer pendant quels appels les signaux DTMF peuvent être envoyés.
5. Sélectionnez les méthodes d'envoi de DTMF souhaitées.

**ASTUCE**

Vérifiez que vous avez activé les méthodes acceptées par l'appareil que vous allez appeler.

6. Dans l'onglet **DTMF Receive**, définissez les méthodes DTMF que l'appareil recevra.
7. Enregistrez les modifications.

Sons Utilisateurs

L'appareil effectue plusieurs actions accompagnées d'un son (sonnerie, commutation, etc.). Vous pouvez modifier les sons joués dans **Customization > User sounds**.

Il est également possible de télécharger jusqu'à 10 sons d'utilisateur personnalisés sur l'appareil.

Autres caractéristiques audio de l'appareil

Multicast

L'appareil est capable de transmettre le son du microphone à l'aide de paquets RTP envoyés à une adresse multidiffusion et de recevoir en même temps un flux audio dans le même format, que l'appareil diffuse ensuite via le haut-parleur intégré (ou une autre sortie audio configurée).

Détection du bruit

L'appareil peut surveiller le son reçu par le microphone et, lorsque le niveau du signal du microphone dépasse un seuil défini, l'appareil peut déclencher un événement `Event.NoiseDetected`. Cet événement peut être suivi d'autres événements dans le domaine de l'automatisation (voir [Automation \(p. 54\)](#)).

Activation de la détection du bruit

1. Allez sur **Integration > Audio**.
2. Dans l'en-tête de l'onglet **Noise Detection**, activez la fonction.
3. Dans le paramètre **Noise threshold level**, indiquez la valeur [dB] qui déclenche l'événement **Event.NoiseDetected** en cas de dépassement.
4. Dans le paramètre **Alarm Start Delay**, vous pouvez définir le temps pendant lequel le bruit doit être supérieur à un niveau de seuil pour que l'événement soit déclenché.
5. Dans le paramètre **Alarm End Delay**, en revanche, vous pouvez spécifier la durée pendant laquelle le signal doit être inférieur au seuil pour que l'événement prenne fin.

Test audio

Le résultat du dernier test se trouve dans **Intégration > Audio > Onglet Général > Onglet Test audio**.

Les appareils 2N peuvent effectuer un contrôle régulier du haut-parleur et du microphone intégrés. À des fins de test, le haut-parleur intégré génère un ou plusieurs bips brefs. Le microphone intégré reçoit la tonalité générée et le test réussit si la tonalité est détectée correctement. Le test prend environ 4 secondes. Si le test échoue (ce qui peut être dû à un niveau de bruit ambiant extrême, par exemple), le test est répété une fois de plus dans dix minutes. Le résultat du dernier test peut être affiché dans l'interface de configuration web de l'appareil ou traité à l'aide de l'automatisation.

**NOTE**

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

Informacast

Si votre appareil prend en charge le protocole InformaCast pour la diffusion audio en continu, vous trouverez ses paramètres sur **Integration > Audio > Informacast tab**. Le protocole InformaCast permet d'établir un flux audio (unicast/multicast RTP/UDP codé avec le codec G.711 U-law) entre le périphérique 2N et un serveur InformaCast (ou un autre client InformaCast).

Après avoir activé le service dans **Integration > Audio > InformaCast onglet**, les serveurs InformaCast sont automatiquement trouvés dans le réseau local à l'aide du protocole SLP et le périphérique 2N est automatiquement enregistré auprès d'eux.

Profils de temps

Certaines des fonctions exécutées par l'appareil dépendent du temps. La section Profils temporels de **vous permet de prédéfinir des intervalles de temps à partir desquels vous pouvez ensuite sélectionner ces fonctions. Vous n'avez donc pas besoin de saisir manuellement l'heure à chaque fois que vous la réglez. Vous pouvez nommer le profil temporel pour plus de clarté.**

Créer un profil temporel:

1. Allez sur **Customization > Time Profiles**.
2. Cliquez sur vide pour créer un nouveau profil.
3. Saisissez un nom de profil.
4. Cliquez sur **Enregistrer**. Les détails du profil s'ouvrent.
5. Définissez les intervalles auxquels le profil temporel doit être actif.
 1. Cliquez sur l'intervalle souhaité.
 2. Vous pouvez spécifier le début et la fin dans le menu ouvert.



NOTE

La ligne **Holidays** est utilisée pour définir différents intervalles de temps pendant les jours sélectionnés, voir [Vacances \(p. 39\)](#).

6. Enregistrez les modifications.

Vacances

Dans la configuration de l'appareil, vous pouvez définir plusieurs jours qui seront marqués comme des jours fériés. Des intervalles spéciaux sont alors définis dans les profils temporels pour ces jours. Il s'agit généralement de jours fériés, de congés d'entreprise et d'autres jours spéciaux.

Pour chaque jour férié, vous indiquez s'il s'applique uniquement à une année donnée ou s'il se répète le même jour chaque année. Les vacances peuvent être planifiées plusieurs années à l'avance.

Décors de vacances :

1. Allez sur **Customization > Time Profiles > Holidays tab**.
2. Sélectionnez l'année pour laquelle vous souhaitez définir les vacances.
3. Cliquez sur le jour dans le calendrier :
 - Le premier clic marque la fête qui sera répétée chaque année le jour et le mois donnés.
 - Un second clic transforme le congé en un congé unique pour l'année sélectionnée.
4. Enregistrez les modifications.

Paramètres avancés du compte SIP

Cette section décrit les fonctions optionnelles et les paramètres de compte SIP qui sont définis dans la section **Calling > SIP**.

Les paramètres avancés du compte SIP vous permettent de renforcer la sécurité, d'optimiser la qualité des appels et d'assurer la compatibilité avec différents PBX. Nous recommandons que seuls des administrateurs expérimentés modifient les paramètres.

1. Allez sur **Calling > SIP** du compte que vous voulez configurer.

Fonctions SIP

La méthode REFER permet le transfert dynamique des appels actifs entre différentes identités SIP, ce qui permet un contrôle plus souple des flux de communication.

La méthode PRACK fournit un accusé de réception fiable des états d'appel continus entre les appareils, ce qui améliore la qualité et la stabilité de la communication dans les systèmes SIP.

Les médias

Recevoir uniquement les appels cryptés (SRTP) - vous permet de recevoir uniquement les appels cryptés SRTP. Les appels non cryptés seront automatiquement rejetés. 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.

Commande adaptative de la qualité de la vidéo – permet l'utilisation du profil RTP étendu pour les retours de protocole RTCP (RTP / AVPF). Cette option permet d'utiliser la commande interactive de la qualité de la vidéo selon RFC-4585 et donc d'adapter le flux de données de la vidéo à la qualité actuellement disponible de la connexion réseau.

Compatibilité avec des appareils 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.

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

Ne pas jouer les early media entrants – il empêche la lecture des flux audio entrant avant le décrochage du téléphone envoyé par certaines centrales ou par certains appareils. Au lieu de cela, la sonnerie standard sera jouée.

Configuration avancée

Envoi de 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.

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

Filtre d'adresse IP – 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.

Évaluation de l'état des anciennes sauvegardes -

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.

Réglage de l'interrupteur de protection

L'interrupteur de protection détecte l'ouverture du couvercle de l'appareil, qui est évaluée par le logiciel comme une fermeture logique de l'interrupteur. De cette manière, le commutateur indique une éventuelle manipulation physique de l'appareil.

Lorsque vous activez un interrupteur de protection, vous pouvez désactiver tous les autres interrupteurs ou configurer l'automatisation pour déclencher une action de suivi, telle que l'envoi d'un courrier électronique, la création d'une requête HTTP ou l'activation d'une alarme silencieuse.



NOTE

Selon le type d'appareil, l'interrupteur de protection peut être intégré dans l'unité principale ou vous devez l'installer en tant que module supplémentaire. Pour les procédures d'installation, veuillez vous référer au manuel d'installation de l'appareil spécifique.

Blocage d'autres interrupteurs lorsque le couvercle est ouvert

Le dispositif permet de s'assurer que les autres interrupteurs sont bloqués lors de l'ouverture du couvercle (c'est-à-dire lorsque l'interrupteur de protection est activé). Cela empêche également l'activation de l'interrupteur de porte et l'entrée par la porte qui commande l'appareil.

Procédure de réglage du blocage du commutateur

1. Allez sur **Integration > I/O**.
2. Sur l'onglet **Interrupteur de sécurité**, attribuez un interrupteur de sécurité à l'entrée.
3. Activez l'option **Automatic Switch Blocking**.

Événements liés aux interrupteurs de protection

L'activation de l'interrupteur de protection déclenche des événements. Ces événements peuvent être liés à [Automation \(p. 54\)](#).

- L'ouverture du couvercle déclenche l'événement `TamperSwitchActivated (state: in)`.
Si le commutateur est assigné comme entrée dans **la section I/O**, un événement supplémentaire `InputChange (port: tamper, state: false)` est généré.
- La fermeture du couvercle déclenche l'événement `TamperSwitchActivated (state: out)`.
Si le commutateur est affecté comme entrée à **la section E/S**, un événement supplémentaire `InputChange (port: tamper, state: true)` est généré.

Système

Réglages de la date et de l'heure



ATTENTION

Si l'appareil est géré par un outil de gestion de masse (2N Access Commander / 2N My2N), l'heure de l'appareil peut être gérée par cet outil. Les modifications manuelles dans l'interface web de l'appareil n'affectent pas le réglage de l'heure.

Synchronisation avec NTP

Si l'appareil est connecté à l'internet, l'heure et la date peuvent être synchronisées à l'aide du protocole NTP.

1. Allez sur **Système > Date et heure**.
2. Dans l'onglet **des Paramètres de synchronisation du temps**, activez l'option **Heure automatique à partir de NTP ou d'Internet**.
3. Entrez l'adresse du serveur NTP de votre choix.

Mise à jour de l'heure en cas de panne

1. Allez sur **Système > Date et heure**.
2. Dans l'onglet **des Paramètres de synchronisation du temps** cliquez sur **Synchroniser avec le navigateur**.

Cette opération permet de synchroniser l'heure de l'appareil avec celle de votre ordinateur.



NOTE

Les appareils 2N sont équipés d'une horloge de secours en temps réel qui vous permet de surmonter une panne de courant pendant plusieurs jours.

Paramètres du réseau

Par défaut, l'appareil utilise une adresse IP dynamique attribuée par le serveur DHCP.

Une configuration correcte de l'adresse IP est essentielle pour garantir que vos appareils sont connectés à votre réseau de manière stable et fiable.

1. Pour définir les paramètres réseau de l'appareil, allez sur **System > Network Connection**.

2. Sous Paramètres de base > Paramètres d'adresse IP, vous pouvez activer ou désactiver le serveur DHCP.

Paramètres d'une adresse IP statique:

- a. Désactivez l'option **du serveur DHCP**.
- b. Saisissez l'adresse IP, le masque de sous-réseau, la passerelle par défaut et les serveurs DNS souhaités.
- c. Enregistrez vos modifications. Redémarrage du dispositif en cours.

Paramètres DHCP

- a. Activez l'option **du serveur DHCP**.
- b. Saisissez l'adresse IP, le masque de réseau, la passerelle par défaut et les serveurs DNS souhaités.
- c. Enregistrez vos modifications. Redémarrage du dispositif en cours.



NOTE

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

Licence

Certaines fonctionnalités ne sont disponibles que sous la licence appropriée. Pour obtenir un aperçu des licences et savoir si elles sont actives, consultez **Systeme > Licences > onglet Informations générales**. Dans l'onglet **Licensed Features** vous trouverez une vue d'ensemble des fonctionnalités disponibles qui sont soumises à une licence.



NOTE

Après avoir sélectionné la licence appropriée, contactez votre revendeur 2N. Si vous êtes un partenaire de 2N, vous pouvez contacter notre service clientèle à l'adresse customer-care@2n.com. Veuillez indiquer le numéro de série de l'appareil dans votre demande.

Mise à jour de la clé de licence

La clé de licence actuelle est disponible sur le serveur de mise à jour. Si l'interface de configuration web n'a pas accès à l'Internet public, vous pouvez télécharger manuellement le fichier clé sur l'appareil.

Chaque fois que l'appareil redémarre, la dernière clé de licence disponible est rechargée.

Licence d'essai

La licence d'essai vous permet d'utiliser temporairement toutes les fonctionnalités de la licence Gold et de la licence Microsoft Teams pendant un maximum de 800 heures après l'activation. Une licence d'essai activée ne peut pas être suspendue.

Pour activer une licence d'essai, allez sur **Systeme > Licences > onglet Licence d'essai**.

**ATTENTION**

Une heure de la licence d'essai est supprimée à chaque redémarrage de l'appareil.

Aperçu des fonctionnalités sous licence

Fonction	Licences
<p>Son</p> <ul style="list-style-type: none"> • Sons Utilisateurs • Test sonore automatique • Détection de bruit 	Gratuit
<p>Sécurisation</p> <ul style="list-style-type: none"> • HTTP API • Support 802.1x • Support SIPS (TLS). • Support SRTP • Alarme silencieuse • Limiter les tentatives d'accès infructueuses • Blocage des Interrupteurs • Clavier codé • Anti-Passback 	Gratuit
<p>Prise en charge de l'API HTTP</p>	Gratuit
<p>Support NFC</p>	Gratuit
<p>Vidéo</p> <ul style="list-style-type: none"> • Streaming audio/vidéo (serveur RTSP) • Support caméra IP externe • Support ONVIF • Fonctionnalité PTZ • Détection de mouvement 	Gold

Fonction	Licences
Intégrations <ul style="list-style-type: none"> • Options étendues de réglage des commutateurs • Fonctions d'automatisation • Envoi d'E-mails (Client SMTP) • Mise à jour automatique (client TFTP/HTTP) • Client FTP • Client SNMP • TR-069 • Genetec Synergis 	Gold
Contrôle de l'ascenseur	Gold
Radiomessagerie et communication d'urgence via la plate-forme Cisco	InformaCast
Communication avec le serveur C-CURE 9000	Plugin pour CCUR
Communication avec le serveur OnGuard (LenelS2)	Plugin pour OnGuar
Communication avec le serveur Symmetry	Plugin pour la symétrie
Communication avec MS Teams	Licence Microsoft Teams

Journal des événements

L'aperçu suivant énumère les événements que l'appareil peut générer pendant son fonctionnement et décrit brièvement les conditions dans lesquelles ils se produisent. La disponibilité des événements varie en fonction du type et de la configuration spécifique de l'appareil.

Événement	Description
AccessBlocked	Se produit lorsque les autorisations d'accès sont bloquées.
AccessLimited	Se produit après cinq tentatives d'authentification infructueuses. L'accès est alors bloqué pendant 30 secondes.
AccessTaken	Se produit lorsque la carte est insérée dans la zone anti-passback.

Événement	Description
ApiAccessRequested	Se produit après un appel API HTTP réussi /api/accesspoint/grantaccess.
AudioLoopTest	Se produit une fois que le test du microphone et du haut-parleur de l'appareil est terminé.
CallSessionStateChanged	<p>Se produit lorsque l'état de l'appel change (création, connexion, sonnerie, connexion, fin). Un appel unique peut comprendre plusieurs appels individuels. Par exemple, l'appel d'un numéro de téléphone dans un groupe avec un représentant de contact crée deux appels simultanés vers deux destinations différentes.</p> <p>La description de l'événement contient des informations sur le type de changement, l'identifiant de l'appel, l'adresse de l'appel en cours et l'ordre de l'appel généré.</p>
CallStateChanged	<p>Se produit lorsque l'état de l'appel change (sonnerie, connecté, terminé).</p> <p>La description de l'événement comprend des informations sur le type de changement, la direction de l'appel (entrant, sortant) et l'identification de la contrepartie ou du compte SIP.</p>
CapabilitiesChanged	Se produit lorsque vous modifiez les fonctions disponibles de l'appareil.
CardEntered	Se produit lorsque la carte est attachée au lecteur.
CardHeld	Se produit lorsque la carte est maintenue contre le lecteur pendant plus de 4 secondes.
CodeEntered	Il se produit après avoir introduit le code sur le clavier numérique et l'avoir terminé par le caractère *.
ConfigurationChanged	Se produit lorsque vous modifiez la configuration de l'appareil.
DeviceState	Se produit lorsque l'appareil change d'état (par exemple, lorsqu'il démarre).
DisplayTouched	Se produit lorsque l'écran est touché (sur l'unité principale ou sur un module d'extension connecté via VBUS).
DoorOpenTooLong	Se produit lorsqu'une porte ouverte depuis longtemps est détectée.






Événement	Description
DoorStateChanged	Se produit lorsque la porte change d'état (ouverture/fermeture).
DtmfEntered	Se produit lorsqu'un code DTMF est reçu au cours d'un appel ou localement en dehors d'un appel.
ExternalCameraStateChanged	Se produit lorsque l'état de la caméra externe est modifié.
FingerEntered	Se produit pendant l'authentification par empreinte digitale.
InputChanged	Se produit lorsque l'entrée logique (y compris le commutateur de protection) est modifiée.
KeyPressed	<p>Il se produit lorsque vous appuyez sur le bouton. Les chiffres sont marqués 0, 1, 2 ..., 9. L'ordre des touches de numérotation rapide est le suivant : %1, %2,...</p> <p>Les claviers numériques sont désignés par 0-9. L'ordre des touches de numérotation rapide est indiqué par %1 , %2, etc.</p>
KeyReleased	<p>Il se produit lorsque le bouton est relâché.</p> <p>Les claviers numériques sont désignés par 0-9. L'ordre des touches de numérotation rapide est indiqué par %1 , %2, etc.</p>
LicensePlateRecognized	Cela se produit lorsqu'une plaque d'immatriculation de véhicule avec des droits d'accès valides est détectée, voir Mise en place de l'authentification des plaques d'immatriculation (p. 29) .
LiftConfigChanged	Se produit lorsque vous modifiez les paramètres de Ascenseur (p. 29) .
LiftFloorsEnabled	Se produit lorsque l'accès à l'étage de l'ascenseur est accordé.
LiftStatusChanged	Se produit lorsque le module de contrôle de l'ascenseur est connecté ou déconnecté.
LoginBlocked	Se produit après 3 tentatives de connexion infructueuses. La description de l'événement contient les informations relatives à l'adresse IP de ces accès.
MobKeyEntered	Se produit pendant l'authentification Bluetooth.

Événement	Description
MotionDetected	Se produit lorsqu'un mouvement est détecté dans l'enregistrement de la caméra, voir Détection des mouvements (p. 34)
NoiseDetected	Se produit lorsqu'une augmentation du niveau de bruit est détectée, voir Autres caractéristiques audio de l'appareil (p. 38) .
OutputChanged	Se produit lorsque l'état de la sortie logique change.
PairingStateChanged	
RegistrationState-Changed	Se produit lorsque l'enregistrement du proxy SIP est modifié.
RexActivated	Se produit lorsqu'une entrée configurée comme bouton REX est activée.
SilentAlarm	Se produit lorsqu'une alarme silencieuse est déclenchée, voir Alarme silencieuse (p. 25) .
SwitchesBlocked	Se produit lorsque le commutateur est bloqué par une tentative d'accès non valide.
SwitchOperation-Changed	Se produit lorsque la fonction du commutateur est modifiée. L'événement indique l'état de verrouillage ou de maintien du commutateur, la transition vers le maintien permanent du commutateur ou le changement de commutateur (démarrage, redémarrage, sortie).
SwitchStateChanged	Se produit lorsque l'état du commutateur change.
TamperSwitchActivated	Se produit lorsque l'état de l'interrupteur d'autoprotection change, ce qui réagit à l'ouverture ou à la découverte du couvercle de l'appareil.
UnauthorizedDoorOpen	Se produit lorsqu'une ouverture de porte non autorisée est détectée.
UserActionActivated	Signale une action de l'utilisateur déclenchée par le déclencheur d'action de l'utilisateur associé.

Événement	Description
UserAuthenticated	Se produit lorsque l'authentification et l'autorisation de l'utilisateur sont réussies.
UserRejected	Se produit lorsque l'autorisation de l'utilisateur n'est pas valide.
WaveKeyActivated	Se produit lorsque l'authentification Bluetooth est activée.

Signalisation du statut opérationnel

L'appareil signale les changements et les transitions entre les différents états de fonctionnement par des messages sonores. Chaque changement d'état se voit attribuer un type de tonalité différent. Voir le tableau ci-dessous pour la liste des signaux :

Signalisation sonore	État
	<p>Application interne lancée</p> <p>Lorsque l'appareil est mis sous tension ou redémarré, l'application interne est lancée.</p>
	<p>Connecté au réseau local, adresse IP reçue</p> <p>Lorsque l'application interne démarre, l'appareil se connecte au réseau local.</p>
	<p>Déconnecté du réseau local, adresse IP perdue</p> <p>Déconnecté du réseau local, adresse IP perdue</p>
	<p>Numéro de téléphone ou code d'activation de l'interrupteur non valide</p> <p>L'appareil permet de saisir un code pour ouvrir la porte. Si des valeurs non valides sont introduites, ce signal est émis.</p>
	<p>Remise des paramètres du réseau à l'état initial</p> <p>Après la mise sous tension, les paramètres du réseau peuvent être modifiés à l'aide du hardware, voir Bref guide.</p>

**Signali-
sation
sonore**
État
Signalisation de fin d'appel qui s'approche


L'appareil vous permet de fixer une limite de temps après laquelle l'appel est terminé, en **Appel > Paramètres généraux > Limite de temps d'appel**.

Signalisation de confirmation de la prolongation de l'appel


L'appel peut être prolongé en appuyant sur une touche du téléphone VoIP.

Appel connecté lors d'un appel depuis un téléphone VoIP vers l'appareil


Lorsqu'un appel est passé d'un téléphone VoIP vers l'appareil, une courte tonalité est émise pour signaler la connexion de l'appel.

Ports Utilisés

Service	Port	Proto- coles	Direction	Acti- vé par dé- faut	Confi- gu- rable	Paramètres
802.1x	–	–	Entrée/ Sortie	×	×	–
DHCP	68	UDP	Entrée/ Sortie	✓	×	–
DNS	53	TCP/U DP	Entrée/ Sortie	✓	×	–
Echo (device disco- very)*	8002	UDP	Entrée/ Sortie	✓	×	–
FTP	21	TCP	Sortie	×	×	–
2N IP Eye	8003	UDP	Sortie	×	×	–

Système

Service	Port	Proto- coles	Direction	Acti- vé par dé- faut	Confi- gu- rable	Paramètres
HTTP	80	TCP	Entrée/ Sortie	✓	✓	Système > Connexion au réseau > SERVEUR WEB
HTTPS	443	TCP	Entrée/ Sortie	✓	✓	Système > Connexion au réseau > onglet SERVEUR WEB
Multicast audio	22222	UDP	Sortie	×	✓	Intégration > Audio
Multicast audio pour le protocole ICU	8006	UDP	Sortie	×	×	–
Multicast video pour le protocole ICU	8008	UDP	Sortie	×	×	–
Multicast video (wi- de) pour le protocole ICU	8016	UDP	Entrée/ Sortie	×	×	–
Client NTP	123	UDP	Entrée/ Sortie	✓	×	–
ONVIF	80, 443, 3702	TCP/U DP	Entrée/ Sortie	×	×	–
Ports RTP+RTCP (SIP)	4900+ (range of 64 ports)	UDP	Entrée/ Sortie	×	✓	Appel > Pa- ramètres généraux
Ports RTP+RTCP (caméra externe)	4800+ (range of 64 ports)	UDP	Entrée/ Sortie	×	✓	Intégration > ONVIF / RTSP

Système

Service	Port	Proto- coles	Direction	Acti- vé par dé- faut	Confi- gu- rable	Paramètres
Client RTSP	554	UDP	Entrée/ Sortie	×	✓	
RTSP server	554	UDP	Entrée/ Sortie	×	×	–
SingleWire Com- mands	80	TCP	Entrée/ Sortie	×	×	–
SingleWire Commu- nication	8081	TCP	Sortie	×	×	–
SingleWire Media	20000+	UDP	Entrée	×	×	–
SLP	427	UDP	Entrée/ Sortie	✓	×	–
SIP	5060, 5062	TCP/U DP	Entrée/ Sortie	×	✓	Appel > SIP
SIPS	5061	TCP	Entrée/ Sortie	×	✓	Appel >SIP
SMTP	25	TCP	Sortie	×	✓	Intégration > Notifica- tions par courrier électroni- que
Syslog	514	UDP	Sortie	×	×	–
TFTP	69	UDP	Sortie	×	×	–
My2N Knocker	443	TCP	Sortie	✓	×	–

Système

Service	Port	Proto- coles	Direction	Acti- vé par dé- faut	Confi- gu- rable	Paramètres
My2N Tribble Tunnel	443	TCP	Sortie	✓	×	–
SNMP Agent	161	UDP	Entrée/ Sortie	✓	×	–
SNMP Trap	162	UDP	Sortie	✓	×	–
SSDP	1900	UDP	Entrée/ Sortie	✓	×	–
SDDP	1902	UDP	Entrée/ Sortie	✓	×	–
Multicast receiver (Automation)	4433	UDP	Entrée	×	×	–
WS-Discovery	3702	UDP	Entrée/ Sortie	✓	×	–
CIP Client (Cre- stron)	41794	UDP	Entrée/ Sortie	×	×	–
Sitechannel (proto- cole ICU)	8004	UDP	Entrée/ Sortie	×	×	–
Multicast DNS	5353	UDP	Entrée/ Sortie	✓	×	–


Automation

**NOTE**

La fonction n'est disponible qu'avec la licence Gold.

La configuration standard de l'appareil 2N couvre la plupart des scénarios courants. La fonction d'automatisation peut être utilisée dans des cas plus complexes, par exemple pour adapter l'appareil à des exigences spécifiques ou l'intégrer à des systèmes tiers. L'automatisation vous permet de définir une logique personnalisée pour le comportement de l'appareil qui répond à différents événements, signaux ou combinaisons de conditions. Par exemple, des actions spécifiques peuvent être déclenchées en appuyant sur un bouton de numérotation rapide spécifique, en activant une alarme silencieuse, en détectant une porte ouverte, en activant une entrée ou en détectant un mouvement à proximité de l'appareil.

Paramètres d'automatisation :

1. Dans l'interface web de l'appareil, allez sur **Integration > Automation**.
2. Dans l'aperçu des fonctions, activez le nombre de fonctions souhaité.
3. Cliquez sur  pour ouvrir l'interface de configuration de l'automatisation.
4. Dans l'en-tête de l'interface Automations, saisissez le nom de la fonction sous laquelle la fonction sera enregistrée.
5. Créez un flux d'automatisation.
Une description détaillée de la fonction et de la configuration d'automatisation est disponible dans [Automatisation manuelle](#).
6. Lorsque la fonction est terminée, cliquez sur **SAVE** et quittez l'interface d'automatisation.



Interphones IP – Manuel de Configuration

© 2N Telekomunikace a. s., 2026

2N.com