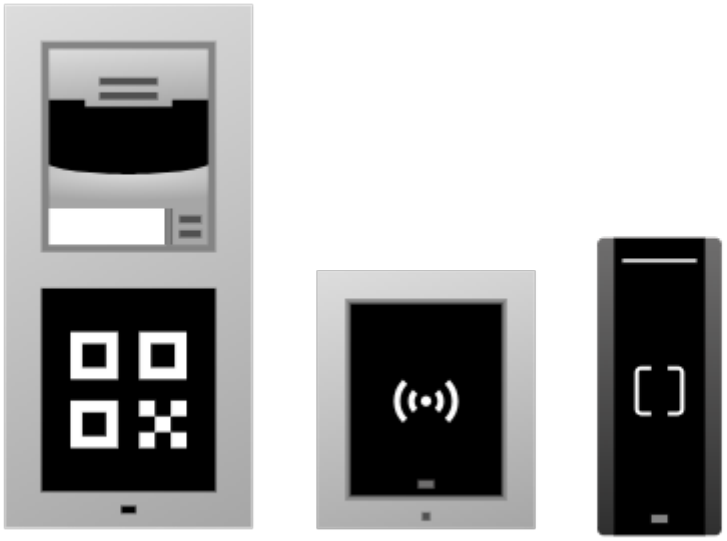
Lecteurs d’accè

Manuel de Configuration



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

2N.com

Table des matières

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 : 2NAccessUnit-{numéro de série sans tirets}.local (par exemple.: « 2NAccessUnit-0000000001.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 :

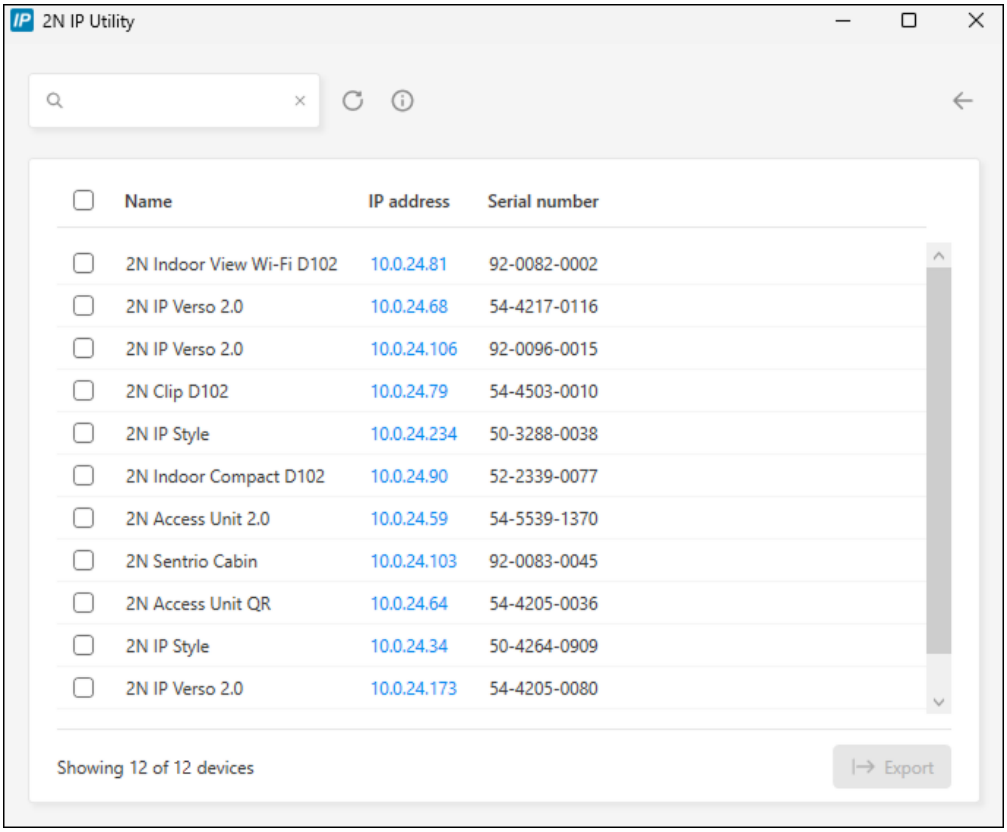
- avec la touche RESET

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

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

1. Exécutez le programme d'installation 2N IP Utility.
2. L'assistant d'installation vous guidera tout au long de l'installation.

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



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

ASTUCE

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

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

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

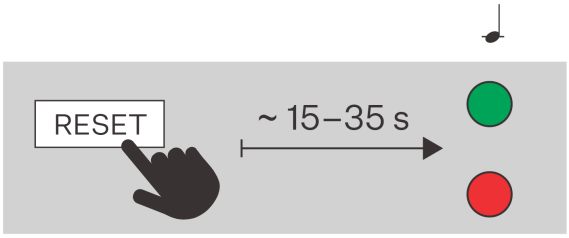
Pour une plus grande sécurité du mot de passe, nous recommandons :

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

Recherche de l'adresse IP à l'aide du hardware

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

1. Appuyez sur le bouton RESET.
   a. Attendez que les LED rouge et verte s'allument simultanément et d'entendre le signal sonore (approx. 15–35 s).
2. Relâchez le bouton RESET.
3. L'appareil annoncera automatiquement son adresse IP.



NOTE
Le délai entre l'appui sur le bouton RESET et le premier signal lumineux et sonore est compris entre 15 et 35 s, selon le modèle de l'appareil.

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 :

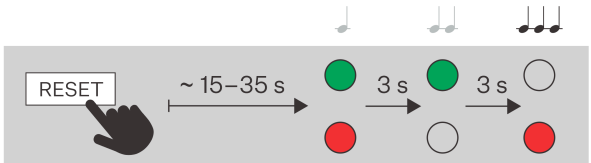
- avec la touche RESET

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

Réglage d'une adresse IP dynamique à l'aide de la touche RESET

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

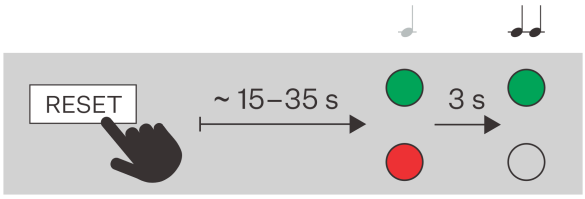
1. Appuyez sur le bouton RESET.
   a. Attendez que les LED rouge et verte s'allument simultanément et d'entendre le signal sonore ♩ (approx. 15–35 s).
   b. Attendez que la LED rouge s'éteigne et d'entendre le signal sonore ♩♩ (approx. 3 s).
   c. Attendez que la LED verte s'éteigne, que la LED rouge se rallume et d'entendre le signal sonore ♩♩♩ (approx. 3 s).
2. Relâchez le bouton RESET.



Réglage d'une adresse IP statique à l'aide de la touche RESET

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

1. Appuyez sur le bouton RESET.
   a. Attendez que les LED rouge et verte s'allument simultanément et d'entendre le signal sonore (approx. 15–35 s).
   b. Attendez que la LED rouge s'éteigne et d'entendre le signal sonore (approx. 3 s).
2. Relâchez le bouton RESET.



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

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

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. 3)).
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

ATTENTION
Dans la version 3.0.0, les mises à jour du micrologiciel à partir du serveur de mise à jour ne sont disponibles qu'à partir de l'ancienne version de l'interface web.

a. Dans l'en-tête de l'interface de configuration web, cliquez sur Go to the old interface.

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

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.

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 les options d'accès en fonction de Accès (p. 10).

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.

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. 12).

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.

En définissant un profil temporel

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.

De l'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**.

Utiliser l'API HTTP

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

En réglant l'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'authentification. 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. 12).
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. 14)).

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 :

- Ouvre 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'imma-

triculation 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**, 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.

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.

GET IT ON Google Play Download on the App Store

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. Clé mobile.
>
> ### **Couplage dans l'application mobile** Clé mobile
>
> 1. Téléchargez l'application Clé mobile sur votre téléphone portable. L'application est disponible sur Magasin d'applications et Google Play.
> 2. Ouvrez l'application et activez l'application Clé mobile 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 Clé mobile 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.

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.

Paramètres avancés

Paramètres de l'appareil photo et de la vidéo

La caméra de l'unité d'accès **2N QR** détecte les mouvements autour de l'appareil et lit les codes QR.

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. 22)
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 **Intégration > Video**.
2. Activez le service du serveur RTSP .
3. Définissez les paramètres du flux, voir Paramètres du flux vidéo (p. 24).
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**.

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

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. 31)).

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.

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. 26).
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.

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 **Système > 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 customercare@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 **Système > Licences > onglet Licence d'essai**.

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

Ports Utilisés

Service	Port	Protocoles	Direction	Activé par défaut	Configurable	Paramètres
802.1x	–	–	Entrée/Sortie	×	×	–
DHCP	68	UDP	Entrée/Sortie	✓	×	–
DNS	53	TCP/UDP	Entrée/Sortie	✓	×	–
Echo (device discovery)*	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**
Client NTP	123	UDP	Entrée/Sortie	✓	×	–
SLP	427	UDP	Entrée/Sortie	✓	×	–

Service	Port	Proto-coles	Direction	Activé par dé-faut	Confi-gurable	Paramètres
SMTP	25	TCP	Sortie	×	✓	**Intégration > Notifications par courrier électronique**
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	✓	×	–
Multicast recei-ver (Automa-tion)	4433	UDP	Entrée	×	×	–
Multicast DNS	5353	UDP	Entrée/Sortie	✓	×	–

Automation

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.

Lecteurs d’accè – Manuel de Configuration

2N.com