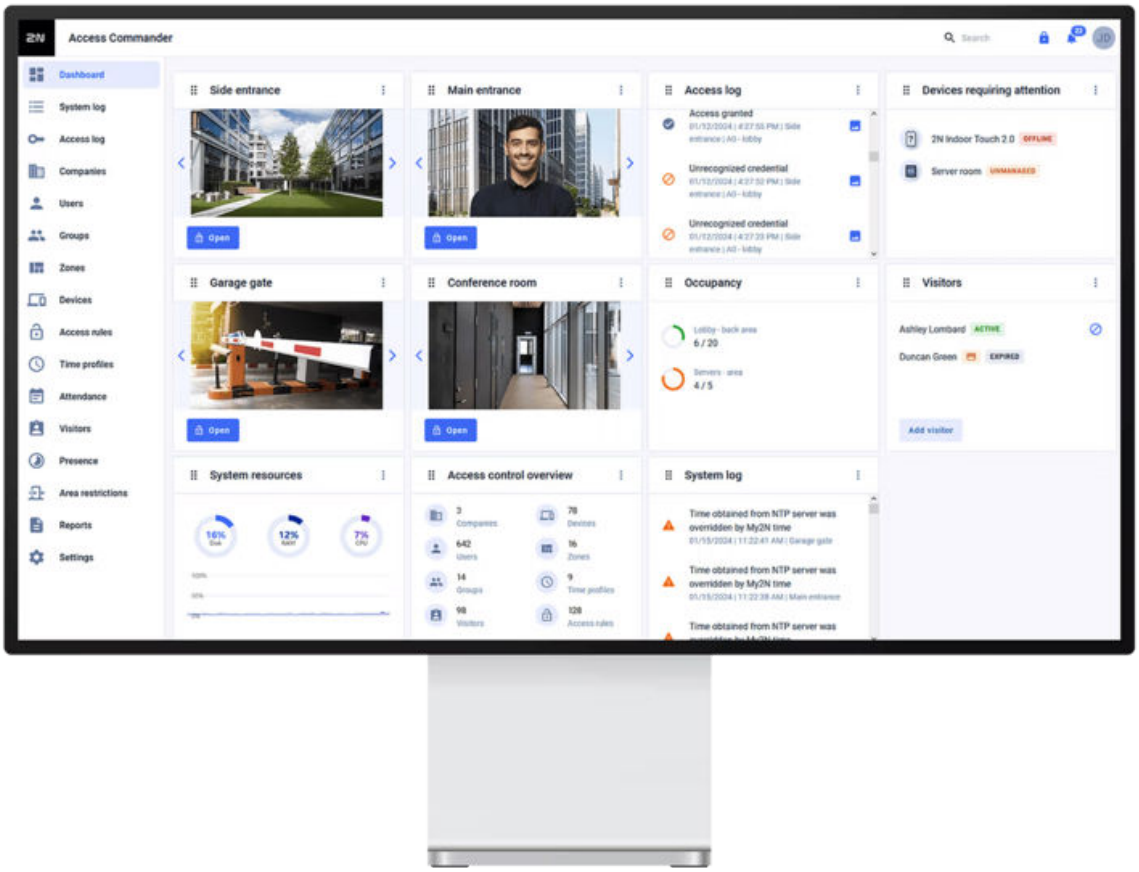
2N Access Commander

Manuel d'installation



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

2N.com

Table des matières

Symboles et termes utilisés

Les symboles et pictogrammes suivants sont utilisés dans le manuel :

DANGER
Toujours se conformer ces instructions pour éviter tout risque de blessure.

AVERTISSEMENT
Toujours se conformer ces instructions pour éviter d'endommager l'appareil.

ATTENTION
Avertissement important. Le non-respect des instructions peut entraîner un dysfonctionnement de l'appareil.

ASTUCE
Informations utiles pour une utilisation ou une configuration plus facile et plus rapide.

NOTE
Procédures et conseils pour une utilisation efficace des fonctionnalités de l'appareil.

informations générales

2N Access Commander est un outil logiciel pour la gestion du système d'accès en masse. Interface **Access Commander** est accessible via un navigateur Web.

Les réglages peuvent être effectués au sein d'une seule installation **Access Commander** diviser en **Sociétés**, qui sont gérés séparément. Cette méthode permet de répartir l'administration entre les administrateurs des différentes entreprises. Un administrateur d'une entreprise n'a pas accès aux informations sur une autre entreprise. Les administrateurs d'une entreprise ne verront pas les utilisateurs d'une autre entreprise.

Pour gérer l'accès, vous devez ajouter le dispositif à **Access Commander. Les dispositifs sont des unités physiques dans le bâtiment qui contrôlent les entrées (2N int**

Des zones ou des installations peuvent être partagées entre les entreprises, permettant de gérer les accès de l'entreprise aux espaces communs (entrées, restaurants, salles de conférence...).

Utilisateurs sont des personnes individuelles dont les déplacements dans le bâtiment doivent être gérés, ou qui peuvent être appelées depuis des appareils connectés. Les utilisateurs sont regroupés en **Groupes**, dans lequel s'effectue la gestion massive de leur accès aux zones. L'utilisateur s'authentifie sur l'appareil et celui-ci évalue ensuite s'il dispose d'un accès valide à l'appareil. La validité de l'accès est régie par **Des droits d'accès**. Les utilisateurs sélectionnés peuvent également disposer d'autorisations administratives **Access Commander** ou des parties de celui-ci.

Profils horaires ils définissent les heures auxquelles l'appareil autorise l'accès ou auxquelles les utilisateurs peuvent être appelés.

Module de présence permet de surveiller la présence des utilisateurs.

Module de présence vous permet de suivre les zones dans lesquelles se trouvent actuellement les utilisateurs.

Visites sont des personnes dont les droits d'accès ne sont valables que pour une durée limitée.

Autorisations utilisateur

Rapport dans **Access Commander** peut être effectuée par plusieurs utilisateurs en fonction des autorisations qui leur sont attribuées.

Les comptes élevés sont configurés via un rôle dans les paramètres utilisateur. Plusieurs rôles peuvent être attribués à un seul utilisateur.

NOTE
Les autorisations des utilisateurs s'appliquent à la gestion au sein de l'entreprise de l'utilisateur. L'administrateur a accès à une gestion complète dans toutes les entreprises.

Administrateur

- Configuration du système et des modules individuels selon la licence valide.
- Changement de licence
- Toutes les autorisations des autres rôles applicables à toutes les entreprises.

Gestionnaire d'accès

- Créez et gérez des groupes.
- Gérer leurs adhésions à des groupes.
- Créez et gérez des visites.
- Création et gestion de profils horaires.
- Définition des règles d'accès.

Gestionnaire des utilisateurs

- Créez et gérez des utilisateurs.
- Créez et gérez des visites.
- Gérer leurs adhésions à des groupes.
- Affichage du journal d'accès et du système.

Responsable des visites

- Créez et gérez des visites.
- Gérer leurs adhésions à des groupes.
- Consultation du journal d'accès des visites.

Gestionnaire de portes

- Surveillance de la transmission des caméras à partir des appareils attribués.
- Ouverture à distance des appareils attribués.
- Verrouillage d'urgence des appareils attribués.
- Affichage du journal d'accès des appareils attribués.
- Surveillance des états et des événements de sécurité dans le journal système.

Responsable des présences

- Suivi et gestion de la fréquentation des groupes assignés.
- Affichage du journal d'accès des utilisateurs des groupes attribués.

Administrateur de l'entreprise

- Définir la langue par défaut de l'entreprise.
- Surveillance du journal du système (limitée aux événements de l'entreprise).
- La possibilité de créer un widget pour le journal du système et la fonction de verrouillage d'urgence sur les appareils utilisés par l'entreprise (y compris les appareils partagés avec d'autres entreprises).

Appareils et applications pris en charge

Ce chapitre répertorie les appareils pris en charge, les navigateurs Web pris en charge et les plates-formes de virtualisation compatibles via lesquelles **Access Commander** peut être installé.

Périphériques compatibles

Vous trouverez ci-dessous un aperçu des appareils pris en charge par le système d'accès Access Commander. Ces appareils peuvent être gérés dans le système.

NOTE
Les versions de firmware prises en charge de ces appareils sont répertoriées dans le chapitre Micrologiciel (p. 68).

Interphones 2N

- 2N IP Style – prend en charge la lecture du code QR
- 2N IP Verso 2.0 – prend en charge la lecture du code QR
- 2N IP Force 2.0 — prend en charge la lecture de codes QR
- 2N IP Verso
- 2N LTE Verso
- 2N IP One
- 2N IP Force
- 2N IP Safety
- 2N IP Vario
- 2N IP Base
- 2N IP Solo
- 2N IP Uni
- 2N IP Video Kit
- 2N IP Audio Kit
- 2N IP Audio Kit Lite

Unités d'accès 2N

- Access Unit QR – prend en charge la lecture des codes QR
- 2N Access Unit 2.0
- 2N Access Unit
- 2N Access Unit M

Serrures électroniques 2N

- 2N Fortis Handle
- 2N Fortis Cylinder

Unités de réponse 2N

- 2N Indoor View (Wi-Fi)
- 2N Indoor Compact
- 2N Indoor Talk
- 2N Indoor Touch 2.0
- 2N Clip
- 2N Clip 2wire-IP

Navigateurs Web

Configuration **Access Commander** se fait via l'interface web. Le système a été optimisé pour le navigateur Google Chrome (version 90 et supérieure.)

Autres navigateurs pris en charge :

- Mozilla Firefox (version 78 et supérieure)
- Microsoft Edge (version 91 et supérieure)
- Safari (versión 14 y superior)

Les autres navigateurs n'ont pas été testés, leur fonctionnalité complète ne peut donc pas être garantie.

Plateformes de virtualisation

- Virtual Box
- VMware Player (version 6.5 et supérieure)

- VMware vSphere (version 6.5 et supérieure)
- Hyper-V

Ports utilisés

Liste des services et ports requis

Service	Port
HTTP/HTTPS[a.]	80/443
SMTP	225
DHCP	68
DNS	53
NTP	123
LDAP[b.]	389
SSH	22

[a.] Il est utilisé à la fois pour la communication avec le client et pour la communication avec les contrôleurs d'accès.
[b.] L'utilisateur peut dans les paramètres **Access Commander** choisissez un autre port pour le service LDAP.

Aperçu des licences

Après l'installation initiale **Access Commander** une licence d'essai est disponible. La licence d'essai permet de tester toutes les fonctions sur la gestion de 1 appareil et 5 utilisateurs. Pour une administration complète, vous devez activer l'une des quatre licences : *Basic* (gratuit), *Advanced*, *Pro* ou *Unlimited*.

Licence:	Trial	Basic	Advanced	Pro	Unlimited
2N Part No.	Axis Part No.	n/a	91379031	91379032	91379033
Axis Part No.	n/a	n/a	02309-001	02310-001	02311-001
Nombre maximum d'utilisateurs	5	50	300	1000	Illimité[a.]
Nombre maximum d'appareils (activés et désactivés)	1	5	30	100	Illimité

Licence:	Trial	Basic	Advanced	Pro	Unlimited
2N Part No.	Axis Part No.	n/a	91379031	91379032	91379033
Axis Part No.	n/a	n/a	02309-001	02310-001	02311-001
Nombre maximum d'administrateurs/gestionnaires	5	1	5	1000	Illimité
Journaux d'accès et système	✓	✓	✓	✓	✓
Règles d'accès	✓	✓	✓	✓	✓
Gestion des API	✓	✓	✓	✓	✓
Activation/désactivation du compte	✓	✓	✓	✓	✓
Limiter le nombre d'accès échoués	✓	✓	✓	✓	✓
Alarme silencieuse	✓	✓	✓	✓	✓
Code de zone	✓	✓	✓	✓	✓
Surveillance des appareils	✓	✓	✓	✓	✓
Gestion des journaux	✓	✓	✓	✓	✓
Gestion des serrures électroniques	✓	✓	✓	✓	✓
Importer des utilisateurs depuis CSV ou depuis des appareils	✓	×	✓	✓	✓
Gestion groupée du firmware	✓	×	✓	✓	✓
Authentification multiple	✓	×	✓	✓	✓

Licence:	Trial	Basic	Advanced	Pro	Unlimited
2N Part No.	Axis Part No.	n/a	91379031	91379032	91379033
Axis Part No.	n/a	n/a	02309-001	02310-001	02311-001
Autorisation de l'utilisateur	✓	×	✓	✓	✓
Notification	✓	×	✓	✓	✓
Présence	✓	×	✓	✓	✓
Clés d’accès API	✓	×	✓	✓	✓
Journaux CAM	✓	×	✓	✓	✓
Contrôle d'ascenseur	✓	×	✓	✓	✓
Tableau de bord	✓	×	✓	✓	✓
Verrouillage d'urgence	✓	×	✓	✓	✓
Prise en charge des informations d'identification mobiles	✓	×	✓	✓	✓
Gestion des visites	✓	×	✓	✓	✓
Automation	✓	×	✓	✓	✓
Gestion de l'occupation	✓	×	×	✓	✓
Synchronisation (LDAP et CSV)	✓	×	×	✓	✓
Anti-retour	✓	×	×	✓	✓

Licence:	Trial	Basic	Advanced	Pro	Unlimited
2N Part No.	Axis Part No.	n/a	91379031	91379032	91379033
Axis Part No.	n/a	n/a	02309-001	02310-001	02311-001
Présence	✓	Facul-tatif	Facultatif	Facultatif	Facultatif

[a.] Illimité dans les capacités maximales de la plate-forme logicielle, à savoir Matériel recommandé pour une machine virtuelle (p. 21)

Installation

Access Commander peut être distribué de deux manières :

- Un petit ordinateur de bureau 2N Access Commander Box 2.0 (2N Part No. 1120120xx , Axis Part No. 03129-00)
- Ordinateur virtuel

Solution Access Commander Boxest limité à 2000 appareils connectés. Les autres fonctionnalités du logiciel sont identiques pour les deux solutions.

Distribution via Access Commander Box

Access Commander Box 2.0 (1120120xx, 03129-00) est un mini-ordinateur de bureau compact avec des logiciels préinstallés. Il s'agit d'une solution "plug and play" où il suffit de connecter une alimentation électrique et un câble Ethernet à ce mini-ordinateur. Pour un fonctionnement correct et complet du système, il est recommandé de placer ce mini-ordinateur dans un endroit sûr et de le laisser fonctionner en permanence. L'Access Commander Box 2.0 sert de serveur pour collecter les données, les événements et les journaux de l'ensemble du système de contrôle d'accès.

Nous recommandons de ne pas dépasser le nombre de 1 500 utilisateurs dans le groupe. S'il existe des restrictions dans certaines zones, telles que l'anti-passback ou le contrôle d'occupation pour un grand nombre d'utilisateurs, l'application peut ralentir.

Se connecter à Access Commander avec une adresse IP dynamique

1. Connecter Access Commander Box au réseau à l'aide d'un câble Ethernet.
2. Utilisez 2N IP Network Scanner et Axis IP Utility pour localiser Access Commander Box sur le réseau.
3. Dans votre navigateur Web, accédez à l'adresse IP Access Commander Box et connectez-vous à **Access Commander**.
   Le mot de passe par défaut de l'utilisateur Admin est 2n et doit être modifié après la connexion.

> **NOTE**
> En cas de distribution via Access Commander Box connectez-vous à l'interface Web depuis un autre ordinateur du réseau. Système opérateur Access Commander Box assure le fonctionnement **Access Commander** et sa configuration de base Linux ne permet pas au navigateur Web de s'exécuter.

Configurer une adresse statique sur le Access Commander Box en se connectant directement à l'ordinateur

1. Connectez l'Access Commander Box directement à votre ordinateur à l'aide d'un câble réseau.
2. Après environ **15 secondes,** définira automatiquement l'adresse locale du lien.
3. Ouvrez **accesscommander.local** dans votre navigateur.
   Vous pouvez également utiliser 2N IP Network Scannder ou Axis IP Utility pour localiser le périphérique même s'il n'a pas reçu d'adresse IP via DHCP.
4. Dans l'interface web, définissez une adresse statique si nécessaire.

Définir une adresse statique Access Commander aide Access Commander Box

1. Connecter Access Commander Box au réseau à l'aide d'un câble Ethernet.

2. Se connecter à Access Commander Box clavier et moniteur. Un écran noir apparaît.
3. Connectez-vous au système en tant que « root » avec le mot de passe « 2n ». Lorsque l'écran bleu apparaît, modifiez le mot de passe par défaut.
4. Dans le menu Avancé, sélectionnez « Networking » puis « Static IP ».
5. Définissez l'adresse IP statique, la passerelle et le DNS.
6. Enregistrez ce paramètre et utilisez la déconnexion pour quitter le menu de la console.
7. Connectez-vous à l'adresse IP définie via un navigateur Web.

ASTUCE
Se connecter directement à l'ordinateur et utiliser l'adresse **accesscommander.local** est la méthode recommandée et la plus simple pour configurer une adresse statique sur Access Commander Box.

NOTE
Le numéro de série affiché dans 2N Network Scanner ou Axis IP Utility peut être différent du numéro de série indiqué sur l'étiquette de Access Commander Box.

Fortis Commander

Fortis Commander est une application autonome qui relie les serrures électroniques **Fortis** au système **Access Commander**. L'application définit les verrous en fonction du fichier de projet créé dans **Access Commander**u qui contient la configuration des verrous. Le fichier est crypté et ne peut être utilisé que sur une installation spécifique.

Installation

Fortis Commander est conçu pour être installé sur un ordinateur Windows prenant en charge la technologie Bluetooth Low Energy (BLE).

L'application est disponible sur le site web 2N Download Centre.

Procédure d'installation

1. Téléchargez le paquet d'installation à partir du lien fourni.
2. Exécutez le programme d'installation et terminez l'installation en suivant les instructions à l'écran.

Dossier de projet

Le fichier de projet est créé dans **Access Commander** et contient la configuration complète du projet. Le fichier est crypté et protégé par un mot de passe.

Mise en place de verrous dans Access Commander

Avant de télécharger des clés sur des serrures individuelles, vous devez coupler **Access Commander** avec **Fortis Commander**.

Génération de la clé de chiffrement principale (MEK) et préparation du projet

1. Connectez-vous à Access Commander.
2. Allez sur **Settings > Electronic locks**.
3. Dans l'onglet **Initial Settings** cliquez sur Generate Keys.

4. Créer la clé de chiffrement principale.

ATTENTION
La clé de cryptage principale ne peut pas être consultée ou modifiée ultérieurement .

NOTE
En fonction de la clé de chiffrement principale (MEK), **2N Access Commander** génère un ensemble de clés de chiffrement. La clé doit donc être unique et suffisamment sûre. Le jeu de clés est basé sur la clé de chiffrement principale, de sorte que les projets ayant la même clé de chiffrement principale génèrent les mêmes jeux de clés. Si un projet est perdu, un nouveau projet avec la même clé de chiffrement principale peut être créé et poursuivre le chiffrement.

5. Après avoir généré les clés et défini le mot de passe pour le fichier de projet, vous pouvez télécharger **le fichier de projet**, qui est une image de la configuration de la serrure électronique dans le système **Access Commander**.
6. Dans l'onglet **de Fortis Commander** cliquez sur Télécharger l'application **,** à partir duquel le téléchargement de **Fortis Commander** (application pour la configuration des serrures électroniques) commencera.

ATTENTION
Les informations sur le projet sont des données sensibles. Protégez-les contre les abus.

Configuration de la serrure électronique à l'aide de Fortis Commander

1. Installez **Fortis Commander** et ouvrez-le.
2. Cliquez sur Open project et ouvrez le fichier de projet téléchargé dans l'explorateur de fichiers.
3. Dans la boîte de dialogue qui s'affiche, saisissez le mot de passe du fichier de projet.
4. Après avoir ouvert le fichier de projet, sélectionnez Connect to device et attachez la carte de service à la serrure.
5. Cliquez sur **Assign**, qui attribue le verrou au projet.
6. Déconnectez l'appareil et cliquez sur **File > Close project**.
7. Lorsque la configuration est terminée, ouvrez le système **Access Commander**. Allez dans l'onglet **Settings > Electronic Locks** et cliquez à nouveau sur Fortis Commander. Téléchargez le fichier de projet.

NOTE
Lorsque vous déplacez la serrure d'une installation à l'autre ou lorsque vous faites une réclamation, vous devez effectuer une réinitialisation d'usine . Cette opération réinitialise la serrure aux paramètres d'usine et supprime toute configuration antérieure.

Procédure de mise à jour de la configuration

1. Apportez des modifications à **Access Commander**.

2. Téléchargez le nouveau fichier de projet.
3. Téléchargez le fichier sur **Fortis Commander** et apportez les modifications nécessaires aux serrures.
4. Si vous apportez d'autres modifications à **Access Commander**u, téléchargez toujours un nouveau fichier de projet.

ATTENTION
Pour chaque changement de configuration dans **Access Commander**u, vous devez télécharger un nouveau fichier de projet - vous ne pouvez pas utiliser un ancien fichier qui a déjà été téléchargé sur **Fortis Commander**.

Verrouillage et déverrouillage permanents

L'application vous permet de verrouiller et de déverrouiller la serrure en permanence. Cette fonction est utilisée pour les interventions de service ou les commandes d'urgence sans l'utilisation d'une carte.

Collecte d'événements à partir de serrures électroniques utilisant des cartes/puces RFID

Paramètres de la collecte d'événements

1. Ouvrez **Settings > Electronic locks > Tab events**.
2. Sélectionnez le type d'événement :
   - **Collecte des événements liés à l'accès et au système** - Tous les événements liés à l'accès et au système sont enregistrés sur la carte/puce et inscrits dans le journal du système et dans le journal d'accès .
   - **Collecter uniquement les événements du système** - seuls les événements du système sont enregistrés, les événements d'accès ne sont pas stockés sur les cartes.
   - **Ne collectez pas d'événements sur les onglets** - aucun événement n'est écrit dans l'onglet ; on ne peut y accéder que par l'intermédiaire de **Fortis Commander**u.

ASTUCE
La sélection d'un ensemble d'événements approprié peut réduire la charge du système et l'utilisation de l'espace de stockage. Néanmoins, une journalisation détaillée est importante pour les diagnostics et les audits de sécurité.

Exporter des événements à partir d'une carte

La carte stocke un maximum de **16 premiers événements**. Les événements peuvent être lus de deux manières :

- Dans **Access Commander**, cliquez sur l'icône dans la boîte de recherche de l'en-tête et chargez l'onglet.
- En utilisant un appareil avec **2N OS**, les événements sont lus sur la carte et envoyés à **Access Commander**u.

Téléchargement d'événements dans la serrure

1. Ouvrez **Settings > Electronic Locks > Fortis Commander** et cliquez sur Download File.
2. Ouvrez le fichier dans **Fortis Commander**.
3. Dans l'application **Fortis Commander**, connectez-vous à la serrure électronique.
4. Téléchargez le fichier mis à jour sur **Access Commander**.

5. Une fois téléchargés, les événements sont affichés sur **Access Logs** et **System Logs**.

Opérations de service

Ces opérations sont disponibles pour **Fortis Cylinder**:

- **Démontage** - démontage des serrures à des fins d'entretien.
- **Remplacement de la pile** - remplacement de la pile dans la serrure.

ATTENTION
Les opérations de service ne sont pas pertinentes pour d'autres types de serrures.

NOTE
En mode service, la serrure revient en mode normal en appuyant sur le bouton Lock pour se verrouiller définitivement.

Distribution via machine virtuelle

Access Commander peut être distribué sous forme de machine virtuelle. Vous trouverez ci-dessous les procédures d'installation sur les plates-formes de virtualisation prises en charge.

Virtual Box

ASTUCE
L'activation de la technologie de virtualisation VT-X dans le BIOS est recommandée.

1. Téléchargez la dernière version de VirtualBox à partir de https://www.virtualbox.org/wiki/Downloads.
   Il est recommandé de télécharger la version incluant le VirtualBox Extension Pack.
2. Téléchargez le logiciel approprié depuis la section Support > Centre de téléchargement > Logiciel et micrologiciel sur 2N.com. Après le téléchargement, décompressez le fichier.
3. Ouvrez VirtualBox et sélectionnez "Fichier - Importer l'application...".
4. Modifiez le titre.
5. Vérifiez les paramètres du processeur (minimum 2), les paramètres de la RAM (minimum 2 048 Mo) et la sélection de la carte réseau.
6. Confirmez les termes de la licence.
   Après l'installation, la console de configuration Linux s'ouvrira, où vous pourrez effectuer les paramètres système de base. La configuration complète se fait dans l'interface Web.

VMware Player

ATTENTION
La version prise en charge de VMWare est 6.5 et supérieure.

1. Téléchargez le logiciel approprié depuis la section Support > Centre de téléchargement > Logiciel et micrologiciel sur 2N.com. Après le téléchargement, décompressez le fichier.
2. Dans VMware Player "Fichier – Ouvrir...", sélectionnez le chemin d'accès au fichier OVA.
3. Renommez si nécessaire et cliquez sur "Importer".
4. Vérifiez les paramètres du processeur (minimum 2), les paramètres de la RAM (minimum 2 048 Mo) et la sélection de la carte réseau.
   Après l'installation, la console de configuration Linux s'ouvrira, où vous pourrez effectuer les paramètres système de base. La configuration complète se fait dans l'interface Web.

VMware vSphere

ATTENTION
La version prise en charge de VMWare est 6.5 et supérieure.

1. Téléchargez le logiciel approprié depuis la section Support > Centre de téléchargement > Logiciel et micrologiciel sur 2N.com. Après le téléchargement, décompressez le fichier.
2. Dans VMware vSphere, sélectionnez « Fichier – Déployer le modèle OVF… » et suivez l'assistant.
3. Après l'importation, vérifiez les paramètres "Modifier les paramètres..."
   Modifiez le nom (dans l'onglet Options).
4. Vérifiez les paramètres du processeur (minimum 2), les paramètres de la RAM (minimum 2 048 Mo) et la sélection de la carte réseau.
   Après l'installation, la console de configuration Linux s'ouvrira, où vous pourrez effectuer les paramètres système de base. La configuration complète se fait dans l'interface Web.

Hyper-V

1. Téléchargez le logiciel approprié depuis la section Support > Centre de téléchargement > Logiciel et micrologiciel sur 2N.com. Après le téléchargement, décompressez le fichier.
2. Démarrez Hyper-V Manager et sélectionnez l'option pour l'hôte souhaité Importer une machine virtuelle.
3. Dans le guide d'installation, vérifiez les informations affichées et confirmez leur lecture avec le bouton Suivant.
4. Sélectionnez le chemin du dossier à l'étape 1.
5. Confirmez la sélection de la machine virtuelle.
6. Sélectionnez le type d'importation.
7. Sélectionnez la carte réseau virtuelle pour la machine virtuelle.
8. Vérifiez le récapitulatif des paramètres sélectionnés aux étapes précédentes et confirmez avec le bouton Finition.
   Après l'installation, la console de configuration Linux s'ouvrira, où vous pourrez effectuer les paramètres système de base. La configuration complète se fait dans l'interface Web.

Matériel recommandé pour une machine virtuelle

Le nombre d'appareils connectés affecte**Access Commander**. Par conséquent, définissez la taille des éléments matériels en fonction de l'état réel. Le tableau ci-dessous indique le nombre minimum recommandé de cœurs de processeur et de tailles de RAM pour différents nombres d'appareils et d'utilisateurs gérés par **Access Commander**.

ATTENTION
Il est recommandé de maintenir une connexion continue entre **Access Commande**r et appareils. S'ils sont déconnectés, les appareils stockent les journaux d'événements hors ligne et lorsqu'ils sont reconnectés, les données des journaux sont synchronisées avec Access Commander. Pendant le processus de synchronisation, l'application continue de s'exécuter, mais avec un plus grand nombre d'appareils, l'ensemble du processus peut prendre plus de temps.

Matériel de machine virtuelle

Nombre d'appareils	nombre d'utilisateurs	Nombre minimum de cœurs de processeur	Taille minimale de la RAM	Allocation minimale de disque dur
1 000	10 000	2	2 GB	120 GB
2 000	100 000	2	4 GB	120 GB
2 000	200 000	4	8 GB	120 GB
7 000	200 000	4	16 GB	120 GB

Paramètres techniques

Options du programme sur Access Commander Box 2.0

Nombre d'appareils connectés 2.0	Nombre d'utilisateurs 2,0	Nombre d'utilisateurs dans le groupe
7 000	200 000	1 500

Paramètres techniques Access Commander Box

1ère génération N° de commande 91379030 Axis Part No. 01672-001	2ème génération N° de commande 1120120E, 1120120GB, 1120120US Axis Part No. 03129-00
• Dimensions : 56.1 x 107.6 x 114.4 mm (2.21" x 4.24" x 4.50") • Intel® Celeron® J3160 (2M cache; max. 2.24 GHz) • Disque dur SSD SATA III 2,5" (120 Go) • Mémoire DDR3 SODIMM (4 Go) – 1,35 V, 1 600 MHz • Prise en charge du double affichage via les ports VGA et HDMI • Port LAN Gigabit pour connexion Ethernet • Cadre de montage VESA (75 x 75 mm + 100 x 100 mm) • Température de stockage : -20 °C à +60 °C • Température ambiante de fonctionnement : 0 °C à +35 °C	• Dimensions : 127,5 x 132 x 57,6 mm (5,02 " x 5,20" x 2,27") • Intel® Processor N100, 6W TDP • SSD 980 NVMe M.2 – 250 GB • DDR4 SO-DIMM memory – 16 GB, 1,2 V, 3200 MHz • Support HDMI 2.1, DisplayPort 1.4 et VGA • Port LAN RJ45 2,5G pour connexion Ethernet • Température de stockage : -40 °C à +85 °C • Température de fonctionnement : 0 °C à +50 °C

Matériel recommandé pour une machine virtuelle

Le nombre d'appareils connectés affecte**Access Commander**. Par conséquent, définissez la taille des éléments matériels en fonction de l'état réel. Le tableau ci-dessous indique le nombre minimum recommandé de cœurs de processeur et de tailles de RAM pour différents nombres d'appareils et d'utilisateurs gérés par **Access Commander**.

ATTENTION
Il est recommandé de maintenir une connexion continue entre **Access Commande**r et appareils. S'ils sont déconnectés, les appareils stockent les journaux d'événements hors ligne et lorsqu'ils sont reconnectés, les données des journaux sont synchronisées avec Access Commander. Pendant le processus de synchronisation, l'application continue de s'exécuter, mais avec un plus grand nombre d'appareils, l'ensemble du processus peut prendre plus de temps.

Matériel de machine virtuelle

Nombre d'appareils	nombre d'utilisateurs	Nombre minimum de cœurs de processeur	Taille minimale de la RAM	Allocation minimale de disque dur
1 000	10 000	2	2 GB	120 GB

Nombre d'appareils	nombre d'utilisateurs	Nombre minimum de cœurs de processeur	Taille minimale de la RAM	Allocation minimale de disque dur
2 000	100 000	2	4 GB	120 GB
2 000	200 000	4	8 GB	120 GB
7 000	200 000	4	16 GB	120 GB

Activation de la licence

Des licences doivent être obtenues pour activer fichier de licence et téléchargez-le sur **Access Commander**. La licence Basic peut être activée directement dans **Access Commander** sur la page Paramètres > onglet Licence.

Obtention du fichier de licence

Pour obtenir une licence, vous devez fournir au distributeur le numéro de série de l'un des appareils 2N connectés à l'**Access Commander**. Le fichier de licence est généré sur la base du numéro de série de cet appareil sous licence. Il doit s'agir du numéro de série de l'interphone principal, de l'unité d'accès ou de l'unité de réponse (2N Indoor Touch ne peut pas être utilisé).

Connexion appareil sous licence garantit la validité de la licence. En cas de déconnexion de l'appareil sous licence, une période de protection débutera, après quoi la licence sera suspendue.

Télécharger la licence

ATTENTION

- Après avoir quitté la licence Trial, il n'est plus possible de réactiver la licence Trial.
- Les paramètres de fonctionnalités avancées non pris en charge par la nouvelle licence ne sont pas enregistrés.

1. Aller à **Paramètres > Onglet Licence**.
2. Cliquer sur Télécharger la licence et dans la fenêtre ouverte, téléchargez le fichier de licence obtenu à partir du référentiel.
3. Après avoir téléchargé le fichier, cliquez sur Activer la licence.
4. Assurez-vous que l'appareil sous licence pour lequel la licence a été générée est activé.

dispositif de licence
: Appareil 2N sélectionné connecté à **Access Commander**, qui garantit la validité de la licence. Le périphérique de licence sert de clé matérielle pour la licence.

fichier de licence
: Un fichier avec une licence, un téléchargement qui active la licence. Le fichier de licence est généré par le distributeur sur la base du numéro de série du périphérique de licence.

Renouvellement de la licence

Pour restaurer une licence suspendue, vous devez connecter et activer l'appareil sous licence ou faire générer et télécharger un nouveau fichier de licence pour un autre appareil. Si vous téléchargez une nouvelle licence, vous devez d'abord activer l'appareil sous licence pour lequel la nouvelle licence est générée. Une fois que l'appareil sous licence est activé, tous les autres appareils peuvent l'être également.

La suspension de la licence se produit si l'appareil sous licence est déconnecté de **Access Commander** pendant une période plus longue que la période de protection de la licence. La durée de la période de protection dépend de la durée pendant laquelle l'appareil sous licence a été connecté à **Access Commander**. Les durées des périodes de protection sont indiquées dans le tableau ci-dessous. Lorsqu'une licence est suspendue, tous les appareils connectés sont automatiquement retirés de la gestion et marqués comme non gérés.

NOTE
La suppression de dispositifs de la gestion signifie que vous ne pouvez pas apporter de modifications à leur configuration par l'intermédiaire d'**Access Commander**. Les modifications apportées dans **Access Commander** ne sont pas répercutées sur l'appareil. Cependant, les appareils continuent de fonctionner sur la base des données de la dernière configuration transférée depuis **Access Commander**. Cela signifie que les accès et les autres paramètres des appareils restent les mêmes qu'avant la suspension de la licence.

Vous ne pouvez modifier la configuration d'un appareil non géré que dans l'interface de configuration web de l'appareil en question. Lorsque l'appareil est reconnecté à la gestion d'**Access Commander**, il est synchronisé et les changements effectués directement dans l'interface de configuration web de l'appareil sont remplacés par les paramètres d'**Access Commander**.

La durée pendant laquelle l'appareil sous licence a été connecté à Access Commander	La durée de protection pour laquelle il sera Access Commander en fonctionnement sans appareil de licence connecté
moins de 24 heures	Un jour
1 jour - 30 jours	10 jours
31 jours - 180 jours	1 mois
plus de 180 jours	3 mois

Serrures électroniques

Le système **Access Commander** permet de gérer les accès au moyen de serrures électroniques 2N Fortis, qui sont déverrouillées par des cartes RFID dotées de la technologie MIFARE® DESFire®. Lors de la configuration des serrures électroniques, une clé de cryptage est attribuée à chaque serrure. Les clés de verrouillage sont ensuite stockées sur les cartes RFID des utilisateurs autorisés. Si les clés sur la carte et dans la serrure correspondent, le mécanisme de verrouillage est déverrouillé.

Une carte d'accès RFID peut être utilisée pour accéder à un maximum de 90 portes équipées de serrures 2N Fortis, en fonction du nombre de profils temporels appliqués. Si la capacité de mémoire de la carte est dépassée, l'écriture des données sur la carte échoue. L'échec de l'écriture est enregistré dans le journal des accès au système. En cas d'utilisation de groupes de fermeture, il est possible d'écrire plus de portes sur une seule carte qu'en cas d'affectation individuelle. En cas d'utilisation de groupes de fermeture, il est possible d'inscrire plus de portes par carte qu'en cas d'affectation individuelle.

Fortis Commander

Fortis Commander est une application autonome qui relie les serrures électroniques **Fortis** au système **Access Commander**. L'application définit les verrous en fonction du fichier de projet créé dans **Access Commander**u qui contient la configuration des verrous. Le fichier est crypté et ne peut être utilisé que sur une installation spécifique.

Installation

Fortis Commander est conçu pour être installé sur un ordinateur Windows prenant en charge la technologie Bluetooth Low Energy (BLE).

L'application est disponible sur le site web 2N Download Centre.

Procédure d'installation

1. Téléchargez le paquet d'installation à partir du lien fourni.
2. Exécutez le programme d'installation et terminez l'installation en suivant les instructions à l'écran.

Dossier de projet

Le fichier de projet est créé dans **Access Commander** et contient la configuration complète du projet. Le fichier est crypté et protégé par un mot de passe.

Mise en place de verrous dans Access Commander

Avant de télécharger des clés sur des serrures individuelles, vous devez coupler **Access Commander** avec **Fortis Commander**.

Génération de la clé de chiffrement principale (MEK) et préparation du projet

1. Connectez-vous à Access Commander.
2. Allez sur **Settings > Electronic locks**.
3. Dans l'onglet **Initial Settings** cliquez sur Generate Keys.
4. Créer la clé de chiffrement principale.

ATTENTION
La clé de cryptage principale ne peut pas être consultée ou modifiée ultérieurement .

NOTE
En fonction de la clé de chiffrement principale (MEK), **2N Access Commander** génère un ensemble de clés de chiffrement. La clé doit donc être unique et suffisamment sûre. Le jeu de clés est basé sur la clé de chiffrement principale, de sorte que les projets ayant la même clé de chiffrement principale génèrent les mêmes jeux de clés. Si un projet est perdu, un nouveau projet avec la même clé de chiffrement principale peut être créé et poursuivre le chiffrement.

5. Après avoir généré les clés et défini le mot de passe pour le fichier de projet, vous pouvez télécharger **le fichier de projet**, qui est une image de la configuration de la serrure électronique dans le système **Access Commander**.

6. Dans l'onglet **de Fortis Commander** cliquez sur Télécharger l'application, à partir duquel le téléchargement de **Fortis Commander** (application pour la configuration des serrures électroniques) commencera.

ATTENTION
Les informations sur le projet sont des données sensibles. Protégez-les contre les abus.

Configuration de la serrure électronique à l'aide de Fortis Commander

1. Installez **Fortis Commander** et ouvrez-le.
2. Cliquez sur Open project et ouvrez le fichier de projet téléchargé dans l'explorateur de fichiers.
3. Dans la boîte de dialogue qui s'affiche, saisissez le mot de passe du fichier de projet.
4. Après avoir ouvert le fichier de projet, sélectionnez Connect to device et attachez la carte de service à la serrure.
5. Cliquez sur **Assign**, qui attribue le verrou au projet.
6. Déconnectez l'appareil et cliquez sur **File > Close project**.
7. Lorsque la configuration est terminée, ouvrez le système **Access Commander**. Allez dans l'onglet **Settings > Electronic Locks** et cliquez à nouveau sur Fortis Commander. Téléchargez le fichier de projet.

NOTE
Lorsque vous déplacez la serrure d'une installation à l'autre ou lorsque vous faites une réclamation, vous devez effectuer une réinitialisation d'usine . Cette opération réinitialise la serrure aux paramètres d'usine et supprime toute configuration antérieure.

Procédure de mise à jour de la configuration

1. Apportez des modifications à **Access Commander**.
2. Téléchargez le nouveau fichier de projet.
3. Téléchargez le fichier sur **Fortis Commander** et apportez les modifications nécessaires aux serrures.
4. Si vous apportez d'autres modifications à **Access Commander**u, téléchargez toujours un nouveau fichier de projet.

ATTENTION
Pour chaque changement de configuration dans **Access Commander**u, vous devez télécharger un nouveau fichier de projet - vous ne pouvez pas utiliser un ancien fichier qui a déjà été téléchargé sur **Fortis Commander**.

Verrouillage et déverrouillage permanents

L'application vous permet de verrouiller et de déverrouiller la serrure en permanence. Cette fonction est utilisée pour les interventions de service ou les commandes d'urgence sans l'utilisation d'une carte.

Collecte d'événements à partir de serrures électroniques utilisant des cartes/puces RFID

Paramètres de la collecte d'événements

1. Ouvrez **Settings > Electronic locks > Tab events**.
2. Sélectionnez le type d'événement :
   - **Collecte des événements liés à l'accès et au système** - Tous les événements liés à l'accès et au système sont enregistrés sur la carte/puce et inscrits dans le journal du système et dans le journal d'accès .
   - **Collecter uniquement les événements du système** - seuls les événements du système sont enregistrés, les événements d'accès ne sont pas stockés sur les cartes.
   - **Ne collectez pas d'événements sur les onglets** - aucun événement n'est écrit dans l'onglet ; on ne peut y accéder que par l'intermédiaire de **Fortis Commander**u.

> **ASTUCE**
> La sélection d'un ensemble d'événements approprié peut réduire la charge du système et l'utilisation de l'espace de stockage. Néanmoins, une journalisation détaillée est importante pour les diagnostics et les audits de sécurité.

Exporter des événements à partir d'une carte

La carte stocke un maximum de **16 premiers événements**. Les événements peuvent être lus de deux manières :

- Dans **Access Commander**, cliquez sur l'icône dans la boîte de recherche de l'en-tête et chargez l'onglet.
- En utilisant un appareil avec **2N OS**, les événements sont lus sur la carte et envoyés à **Access Commander**u.

Téléchargement d'événements dans la serrure

1. Ouvrez **Settings > Electronic Locks > Fortis Commander** et cliquez sur Download File.
2. Ouvrez le fichier dans **Fortis Commander**.
3. Dans l'application **Fortis Commander**, connectez-vous à la serrure électronique.
4. Téléchargez le fichier mis à jour sur **Access Commander**.
5. Une fois téléchargés, les événements sont affichés sur **Access Logs** et **System Logs**.

Opérations de service

Ces opérations sont disponibles pour **Fortis Cylinder**:

- **Démontage** - démontage des serrures à des fins d'entretien.
- **Remplacement de la pile** - remplacement de la pile dans la serrure.

> **ATTENTION**
> Les opérations de service ne sont pas pertinentes pour d'autres types de serrures.

> **NOTE**
> En mode service, la serrure revient en mode normal en appuyant sur le bouton Lock pour se verrouiller définitivement.

Mise à jour de la carte

Les cartes d'accès utilisateur doivent être mises à jour régulièrement. L'utilisateur met à jour la carte en la connectant au périphérique IP 2N auquel il dispose de droits d'accès valides. La carte doit être maintenue dans le lecteur de l'appareil jusqu'à ce que l'interrupteur d'ouverture de la porte soit activé. L'interrupteur d'ouverture de la porte n'est activé qu'après la mise à jour de l'accès aux serrures

Vous pouvez modifier la validité par défaut de dix jours des cartes à l'adresse **Settings > Electronic locks > Card Parameters tab**.

ATTENTION
Si vous modifiez les droits d'accès aux serrures dans **Access Commander**, les modifications ne seront répercutées sur la carte d'accès de l'utilisateur qu'après avoir été mises à jour sur le lecteur de cartes de l'appareil 2N ! Pour des raisons de sécurité, nous recommandons de fixer une période de validité plus courte pour les cartes afin de garantir leur mise à jour régulière.

Les lecteurs de dispositifs IP, qui permettent la mise à jour de la carte, et leur configuration sont décrits dans le chapitre Configuration du lecteur de périphérique IP (p. 31).

Cartes compatibles

NOTE
Pour les besoins de cette documentation, le terme **carte** désigne tout identifiant compatible utilisant la technologie MIFARE DESFire.

Pour ouvrir les serrures électroniques 2N Fortis, il n'est pas possible d'utiliser des cartes avec un ID aléatoire (random ID).

Les cartes avec la technologie PICard ne peuvent pas être utilisées pour ouvrir des serrures électroniques 2N Fortis.

Profils temporels sur les serrures électroniques

Les serrures électroniques prennent en charge des profils horaires avec les restrictions suivantes :

- Les vacances ne s'appliquent pas.
- Dans le cadre d'une journée, il est possible de définir jusqu'à 4 intervalles de temps différents.
- Dans le cadre d'un profil horaire, il est possible de définir 4 emplois du temps quotidiens.

ASTUCE
Cela signifie que vous pouvez avoir par exemple des réglages différents pour le lundi, le mardi, le mercredi et le jeudi, mais pour le vendredi, le samedi et le dimanche, vous devez utiliser l'un des réglages existants.

ATTENTION
Si le profil horaire enfreint les restrictions énoncées, la règle d'accès sera ignorée et l'utilisateur ne se verra pas accorder l'accès.

Fortis Commander

Fortis Commander est une application autonome qui relie les serrures électroniques **Fortis** au système **Access Commander**. L'application définit les verrous en fonction du fichier de projet créé dans **Access Commander**u qui contient la configuration des verrous. Le fichier est crypté et ne peut être utilisé que sur une installation spécifique.

Installation

Fortis Commander est conçu pour être installé sur un ordinateur Windows prenant en charge la technologie Bluetooth Low Energy (BLE).

L'application est disponible sur le site web 2N Download Centre.

Procédure d'installation

1. Téléchargez le paquet d'installation à partir du lien fourni.
2. Exécutez le programme d'installation et terminez l'installation en suivant les instructions à l'écran.

Dossier de projet

Le fichier de projet est créé dans **Access Commander** et contient la configuration complète du projet. Le fichier est crypté et protégé par un mot de passe.

Mise en place de verrous dans Access Commander

Avant de télécharger des clés sur des serrures individuelles, vous devez coupler **Access Commander** avec **Fortis Commander**.

Génération de la clé de chiffrement principale (MEK) et préparation du projet

1. Connectez-vous à Access Commander.
2. Allez sur **Settings > Electronic locks**.
3. Dans l'onglet **Initial Settings** cliquez sur Generate Keys.
4. Créer la clé de chiffrement principale.

ATTENTION
La clé de cryptage principale ne peut pas être consultée ou modifiée ultérieurement .

NOTE
En fonction de la clé de chiffrement principale (MEK), **2N Access Commander** génère un ensemble de clés de chiffrement. La clé doit donc être unique et suffisamment sûre. Le jeu de clés est basé sur la clé de chiffrement principale, de sorte que les projets ayant la même clé de chiffrement principale génèrent les mêmes jeux de clés. Si un projet est perdu, un nouveau projet avec la même clé de chiffrement principale peut être créé et poursuivre le chiffrement.

5. Après avoir généré les clés et défini le mot de passe pour le fichier de projet, vous pouvez télécharger **le fichier de projet**, qui est une image de la configuration de la serrure électronique dans le système **Access Commander**.

6. Dans l'onglet **de Fortis Commander** cliquez sur Télécharger l'application, à partir duquel le téléchargement de **Fortis Commander** (application pour la configuration des serrures électroniques) commencera.

ATTENTION
Les informations sur le projet sont des données sensibles. Protégez-les contre les abus.

Configuration de la serrure électronique à l'aide de Fortis Commander

1. Installez **Fortis Commander** et ouvrez-le.
2. Cliquez sur Open project et ouvrez le fichier de projet téléchargé dans l'explorateur de fichiers.
3. Dans la boîte de dialogue qui s'affiche, saisissez le mot de passe du fichier de projet.
4. Après avoir ouvert le fichier de projet, sélectionnez Connect to device et attachez la carte de service à la serrure.
5. Cliquez sur **Assign**, qui attribue le verrou au projet.
6. Déconnectez l'appareil et cliquez sur **File > Close project**.
7. Lorsque la configuration est terminée, ouvrez le système **Access Commander**. Allez dans l'onglet **Settings > Electronic Locks** et cliquez à nouveau sur Fortis Commander. Téléchargez le fichier de projet.

NOTE
Lorsque vous déplacez la serrure d'une installation à l'autre ou lorsque vous faites une réclamation, vous devez effectuer une réinitialisation d'usine . Cette opération réinitialise la serrure aux paramètres d'usine et supprime toute configuration antérieure.

Procédure de mise à jour de la configuration

1. Apportez des modifications à **Access Commander**.
2. Téléchargez le nouveau fichier de projet.
3. Téléchargez le fichier sur **Fortis Commander** et apportez les modifications nécessaires aux serrures.
4. Si vous apportez d'autres modifications à **Access Commander**u, téléchargez toujours un nouveau fichier de projet.

ATTENTION
Pour chaque changement de configuration dans **Access Commander**u, vous devez télécharger un nouveau fichier de projet - vous ne pouvez pas utiliser un ancien fichier qui a déjà été téléchargé sur **Fortis Commander**.

Verrouillage et déverrouillage permanents

L'application vous permet de verrouiller et de déverrouiller la serrure en permanence. Cette fonction est utilisée pour les interventions de service ou les commandes d'urgence sans l'utilisation d'une carte.

Collecte d'événements à partir de serrures électroniques utilisant des cartes/puces RFID

Paramètres de la collecte d'événements

1. Ouvrez **Settings > Electronic locks > Tab events**.
2. Sélectionnez le type d'événement :
   - **Collecte des événements liés à l'accès et au système** - Tous les événements liés à l'accès et au système sont enregistrés sur la carte/puce et inscrits dans le journal du système et dans le journal d'accès .
   - **Collecter uniquement les événements du système** - seuls les événements du système sont enregistrés, les événements d'accès ne sont pas stockés sur les cartes.
   - **Ne collectez pas d'événements sur les onglets** - aucun événement n'est écrit dans l'onglet ; on ne peut y accéder que par l'intermédiaire de **Fortis Commander**u.

> **ASTUCE**
> La sélection d'un ensemble d'événements approprié peut réduire la charge du système et l'utilisation de l'espace de stockage. Néanmoins, une journalisation détaillée est importante pour les diagnostics et les audits de sécurité.

Exporter des événements à partir d'une carte

La carte stocke un maximum de **16 premiers événements**. Les événements peuvent être lus de deux manières :

- Dans **Access Commander**, cliquez sur l'icône dans la boîte de recherche de l'en-tête et chargez l'onglet.
- En utilisant un appareil avec **2N OS**, les événements sont lus sur la carte et envoyés à **Access Commander**u.

Téléchargement d'événements dans la serrure

1. Ouvrez **Settings > Electronic Locks > Fortis Commander** et cliquez sur Download File.
2. Ouvrez le fichier dans **Fortis Commander**.
3. Dans l'application **Fortis Commander**, connectez-vous à la serrure électronique.
4. Téléchargez le fichier mis à jour sur **Access Commander**.
5. Une fois téléchargés, les événements sont affichés sur **Access Logs** et **System Logs**.

Opérations de service

Ces opérations sont disponibles pour **Fortis Cylinder**:

- **Démontage** - démontage des serrures à des fins d'entretien.
- **Remplacement de la pile** - remplacement de la pile dans la serrure.

> **ATTENTION**
> Les opérations de service ne sont pas pertinentes pour d'autres types de serrures.

> **NOTE**
> En mode service, la serrure revient en mode normal en appuyant sur le bouton Lock pour se verrouiller définitivement.

Configuration du lecteur de périphérique IP

Paramètres dans l'interface web de l'appareil IP

ATTENTION
Si vous venez de connecter un module d'extension de lecteur de cartes RFID à l'appareil 2N à l'aide d'un câble VBUS, vous devez appairer ce module avec l'appareil. L'appairage du module d'extension de lecteur peut être effectué via l'interface Web de l'appareil à l'adresse **Access > Modules**.

1. Entrez la configuration Web de l'appareil.

   ASTUCE
   L'interface de configuration Web est accessible en cliquant sur la liste de la page Appareils.

2. Accédez à la Matériel > Modules d'extension.
3. Sur la page, allez dans les paramètres du module de lecteur de cartes RFID.
4. Cliquez sur Associer le module.
5. Dans le menu **Types de cartes autorisés**, sélectionnez l'option « Verrous électroniques 2N ».

   ATTENTION
   Pour un fonctionnement optimal, ne conservez que les types de cartes que vous utilisez réellement.

6. Enregistrez les modifications.

Modules compatibles

La synchronisation des clés pour les serrures électroniques 2N Fortis peut être effectuée sur tous les lecteurs RFID 2N lancés sur le marché en février 2023 ou plus tard. La plupart des lecteurs fabriqués après cette date sont également compatibles, à l'exception des modèles ci-dessous.

Les modèles suivants **ne sont pas compatibles**:

- **2N IP Base**: tous les lecteurs RFID
- **2N IP Force**: 9151011, 9151012, 9151016, 9151017, 9151019
- **2N IP Vario**: tous les lecteurs RFID
- **2N IP Verso**: 915503x, 915504x, 915508x
- **2N Access Unit M**: 91611x
- **2N Access Unit 1.0**: 916008, 916009, 916010, 916011, 916013, 916016, 916019
- **2N Access Unit 2.0**: 916033x

Pour les modules suivants, la compatibilité n'est garantie que pour les unités fabriquées à l'automne 2023 ou plus tard :

- **2N IP Force**: 9151031, 9151031S

Mise en place de verrous dans Access Commander

Avant de télécharger des clés sur des serrures individuelles, vous devez coupler **Access Commander** avec **Fortis Commander**.

Génération de la clé de chiffrement principale (MEK) et préparation du projet

1. Connectez-vous à Access Commander.
2. Allez sur **Settings > Electronic locks**.
3. Dans l'onglet **Initial Settings** cliquez sur Generate Keys.
4. Créer la clé de chiffrement principale.

ATTENTION
La clé de cryptage principale ne peut pas être consultée ou modifiée ultérieurement .

NOTE
En fonction de la clé de chiffrement principale (MEK), **2N Access Commander** génère un ensemble de clés de chiffrement. La clé doit donc être unique et suffisamment sûre. Le jeu de clés est basé sur la clé de chiffrement principale, de sorte que les projets ayant la même clé de chiffrement principale génèrent les mêmes jeux de clés. Si un projet est perdu, un nouveau projet avec la même clé de chiffrement principale peut être créé et poursuivre le chiffrement.

5. Après avoir généré les clés et défini le mot de passe pour le fichier de projet, vous pouvez télécharger **le fichier de projet**, qui est une image de la configuration de la serrure électronique dans le système **Access Commander**.
6. Dans l'onglet **de Fortis Commander** cliquez sur Télécharger l'application**,** à partir duquel le téléchargement de **Fortis Commander** (application pour la configuration des serrures électroniques) commencera.

ATTENTION
Les informations sur le projet sont des données sensibles. Protégez-les contre les abus.

Configuration de la serrure électronique à l'aide de Fortis Commander

1. Installez **Fortis Commander** et ouvrez-le.
2. Cliquez sur Open project et ouvrez le fichier de projet téléchargé dans l'explorateur de fichiers.
3. Dans la boîte de dialogue qui s'affiche, saisissez le mot de passe du fichier de projet.
4. Après avoir ouvert le fichier de projet, sélectionnez Connect to device et attachez la carte de service à la serrure.
5. Cliquez sur **Assign**, qui attribue le verrou au projet.
6. Déconnectez l'appareil et cliquez sur **File > Close project**.
7. Lorsque la configuration est terminée, ouvrez le système **Access Commander**. Allez dans l'onglet **Settings > Electronic Locks** et cliquez à nouveau sur Fortis Commander. Téléchargez le fichier de projet.

NOTE
Lorsque vous déplacez la serrure d'une installation à l'autre ou lorsque vous faites une réclamation, vous devez effectuer une réinitialisation d'usine . Cette opération réinitialise la serrure aux paramètres d'usine et supprime toute configuration antérieure.

Procédure de mise à jour de la configuration

1. Apportez des modifications à **Access Commander**.
2. Téléchargez le nouveau fichier de projet.
3. Téléchargez le fichier sur **Fortis Commander** et apportez les modifications nécessaires aux serrures.
4. Si vous apportez d'autres modifications à **Access Commander**u, téléchargez toujours un nouveau fichier de projet.

ATTENTION
Pour chaque changement de configuration dans **Access Commander**u, vous devez télécharger un nouveau fichier de projet - vous ne pouvez pas utiliser un ancien fichier qui a déjà été téléchargé sur **Fortis Commander**.

Verrouillage et déverrouillage permanents

L'application vous permet de verrouiller et de déverrouiller la serrure en permanence. Cette fonction est utilisée pour les interventions de service ou les commandes d'urgence sans l'utilisation d'une carte.

Cartes de maintenance

Les cartes d'entretien permettent un accès autorisé à la serrure. Ils permettent de mettre la serrure en service, de changer la batterie, de démonter la serrure.

ATTENTION
La carte de maintenance ne peut pas être utilisée en même temps comme carte d'accès utilisateur.

Paramètres de l'onglet Maintenance

1. Dans **Access Commander**, allez sur **Settings > Electronic Locks**.
2. Dans l'onglet Maintenance cliquez sur Créer.
3. Dans la boîte de dialogue qui s'ouvre, sélectionnez le type de carte que vous souhaitez créer.
   - Réglage de nouvelles serrures - active les nouvelles serrures configurées en usine en mode service.
   - Service - active le mode service pour la serrure déjà réglée.
   - Démontage - libère la serrure à cylindre 2N Fortis déjà installée pour le démontage, voir le manuel d'installation 2N Fortis.
   - Remplacement de la batterie - libère la serrure à cylindre 2N Fortis déjà réglée pour le remplacement de la batterie, voir le manuel d'installation de 2N Fortis.

   ASTUCE
   Une carte physique peut être chargée simultanément avec **Setting New Locks** et toute autre carte de service. Nous recommandons une combinaison de **Setting New Locks** et **Service**.
4. Cliquez sur Continuer à.
5. Attachez la carte au lecteur RFID USB connecté. Attendez que les données soient chargées sur la carte.

La validité des données sur la carte d'entretien est d'un an. Après cette période, il est nécessaire de supprimer les données et de reconfigurer la carte.

Prise en charge des cartes DESFire de tiers (création d'applications anonymes)

Access Commander vous permet de travailler avec des cartes MIFARE DESFire. Il prend en charge les cartes déjà utilisées dans d'autres systèmes de contrôle d'accès et permet leur réutilisation sans qu'il soit nécessaire de connaître leur clé principale (PICC Master Key).

Il s'agit d'un mode spécial dans lequel la carte permet la création d'une nouvelle application indépendante sans qu'il soit nécessaire de connaître sa clé principale (PICC Master Key).

Grâce à cette fonctionnalité, les administrateurs peuvent

- Réutiliser les cartes physiques existantes.
- Rédigez l'application OSO pour **Access Commander**.
- Évitez d'avoir à connaître ou à gérer la clé principale PICC des systèmes d'origine.

Pour créer une application OSO sur un onglet

1. Attachez la carte DESfire existante de l'utilisateur à un lecteur connecté à **Access Commander**.
2. Créez les informations d'identification de l'utilisateur.
3. Access Commander détecte automatiquement si la carte prend en charge la création d'applications anonymes.
4. Si le mode est pris en charge, **Access Commander** écrit une nouvelle application anonyme sur la carte sans affecter les données existantes ou les applications tierces.

ATTENTION
Si le mode est pris en charge, Access Commander écrit une nouvelle application anonyme sans possibilité de formater la carte ultérieurement à l'aide d'une fonction de la section Paramètres. Seul le contenu de l'application peut être supprimé, et non l'espace précédemment occupé sur la carte.

Accès de base à l'interface

*Ce chapitre décrit la mise en service et l'utilisation de base **Access Commander**. L'installation est décrite dans le chapitre Installation (p. 14).*

L'interface **d'Access Commander** est accessible via un navigateur web. L'adresse IP de l'interface web peut être recherchée à l'aide de 2N Network Scanner ou Axis IP Utility. Vous pouvez également accéder directement à l'interface web à l'adresse **accesscommander.local**. Cette fonctionnalité est activée par défaut.

NOTE

- Si plusieurs instances d'Access Commander fonctionnent sur le réseau, le système attribue automatiquement des noms uniques : **accesscommander.local**, **accesscommander-2.local**, **accesscommander-3.local**, et d'autres instances en fonction du nombre de serveurs sur le réseau.
- Pour une distribution via Access Commander Box, connectez-vous à l'interface web à partir d'un autre ordinateur du réseau. Le système d'exploitation Access Commander Box fait fonctionner **Access Commander** et ses paramètres Linux de base, mais ne vous permet pas d'utiliser un navigateur web.

NOTE

En cas de distribution via Access Commander Box connectez-vous à l'interface Web depuis un autre ordinateur du réseau. Système opérateur Access Commander Box assure le fonctionnement **Access Commander** et sa configuration de base Linux ne permet pas au navigateur Web de s'exécuter.

Les identifiants de connexion par défaut sont :

Nom d'utilisateur : **Admin**

Mot de passe : **2n**

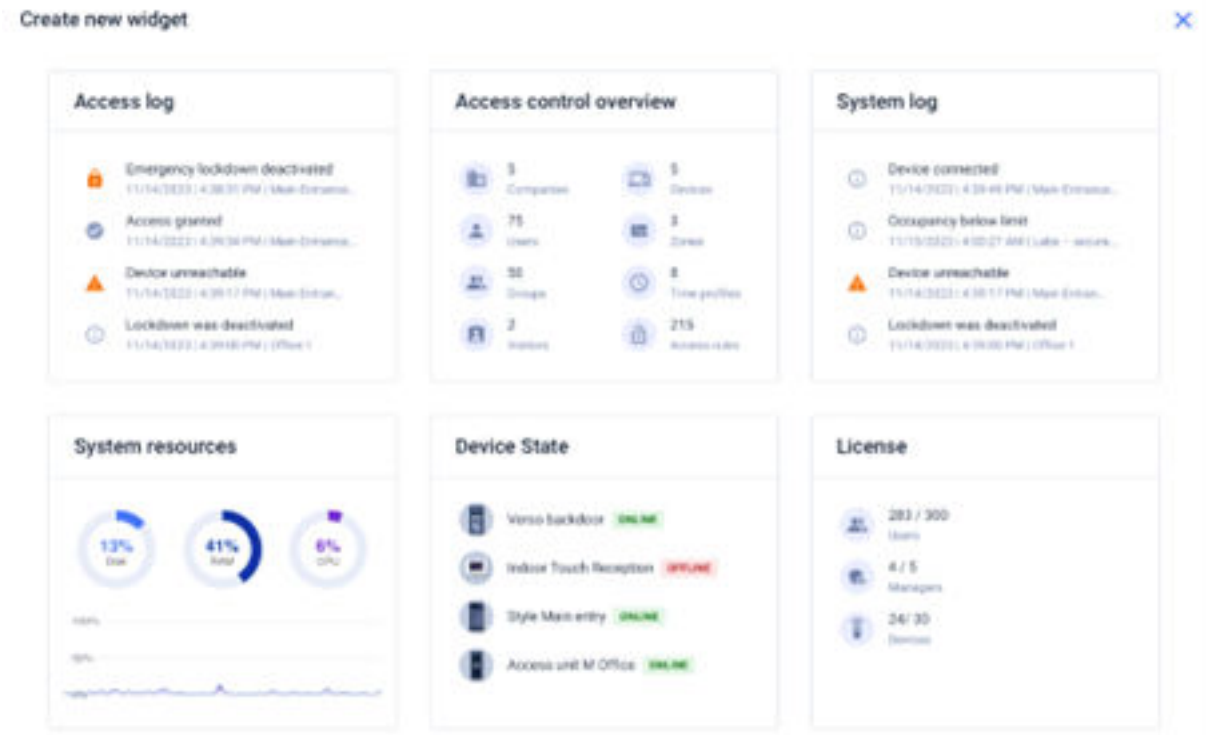
Après vous être connecté pour la première fois, vous devez immédiatement modifier votre mot de passe.

NOTE

Cochez l'option **Ne pas se déconnecter**, si vous voulez éviter de saisir à nouveau vos identifiants de connexion lors de votre prochaine connexion. Le login est valable pour un maximum de 7 jours, après quoi vous devez vous connecter à nouveau.

Vous pouvez avoir besoin d'une Authentification à double facteur (p. 103) pour vous connecter.

Tableau de bord



Le tableau de bord est une vue de base de l'interface web **Access Commander**. Il s'agit d'un tableau de bord configurable qui affiche des données en temps réel. **Access Commander** propose plusieurs widgets qui sont ajoutés au tableau de bord à l'aide du bouton +. Les widgets du tableau de bord peuvent être déplacés, renommés ou leurs paramètres de base peuvent être modifiés de différentes manières. La gestion et la suppression des widgets s'effectuent dans le menu étendu ⋮ dans l'en-tête de chaque widget.

Tout utilisateur disposant d'un compte sur **Access Commander** vous pouvez configurer votre propre tableau de bord. La disponibilité des Widgets est limitée en fonction du rôle de l'utilisateur et de la licence disponible.

Changement de langue

Après la première connexion **Access Commander** s'affiche dans la langue définie pour l'entreprise de l'utilisateur connecté. Chaque utilisateur peut changer la langue. Après la prochaine connexion, l'interface s'affichera dans la langue nouvellement définie.

1. Cliquez sur l'image de l'utilisateur dans le coin supérieur droit pour ouvrir le menu de l'utilisateur.
2. Sélectionnez Changer la langue.
3. Sélectionnez la langue appropriée et confirmez avec Changer de langue.

Changement du mot de passe du compte

1. Cliquez sur l'image de l'utilisateur dans le coin supérieur droit pour ouvrir le menu de l'utilisateur.
2. Sélectionnez Afficher le profil.
3. Cliquez sur le ✎ à côté du paramètre Mot de passe.

4. Confirmez le mot de passe existant et saisissez-en un nouveau.

> **NOTE**
> Si le mot de passe du compte « admin » est le même que celui de l'utilisateur root (pour se connecter à la console de configuration Linux), alors, lorsque le mot de passe du compte « admin » est modifié, le mot de passe du compte root le sera aussi automatiquement.

Change ta photo de profil

1. Cliquez sur l'image de l'utilisateur dans le coin supérieur droit pour ouvrir le menu de l'utilisateur.
2. Sélectionnez Afficher le profil.
3. Cliquez sur l'image dans l'en-tête du détail de l'utilisateur.
4. Dans la boîte de dialogue ouverte, définissez la photo.
   La résolution de l'image sera automatiquement ajustée à 432 × 432 px.

Logos

Voici un aperçu de ce que vous trouverez dans le chapitre :

Journaux système

NOTE

- L'utilisateur voit les journaux qu'il est autorisé à consulter en fonction de ses autorisations utilisateur.
- Les données sont écrites dans les journaux en anglais.

La page Journaux du système affiche une liste des événements et des notifications qu'il a générés.

Dans la liste des journaux système, les éléments suivants sont indiqués pour chaque événement et notification :

- la gravité (info, avertissement, erreur).
- l'heure à laquelle l'événement s'est produit.
- la catégorie à laquelle l'action appartient (État du dispositif, Importation, Synchronisation des utilisateurs, Système, Actions des utilisateurs, Restrictions de zone).
- l'entité concernée par l'action (établissement, utilisateur, zone, visiteur...).
- une brève description de l'événement.
- auteur de l'événement.

Cliquer sur une ligne développe des informations détaillées sur l'enregistrement donné.

La liste peut être filtrée en utilisant au-dessus de la liste. Alternativement, des filtres peuvent être définis pour des colonnes individuelles dans le menu étendu qui s'ouvre en cliquant sur dans l'en-tête de chaque colonne. Menu étendu de colonnes il permet également de déplacer les colonnes, de les épingler à la première ou à la dernière position ou de les masquer.

Les colonnes Gravité et Heure ne peuvent pas être masquées.

Exportation de logos

Les enregistrements peuvent être téléchargés dans un fichier CSV en cliquant sur le bouton Export au-dessus de la liste. Dans le fichier CSV exporté, l'heure est indiquée en GMT+0.

Durée de vie des journaux

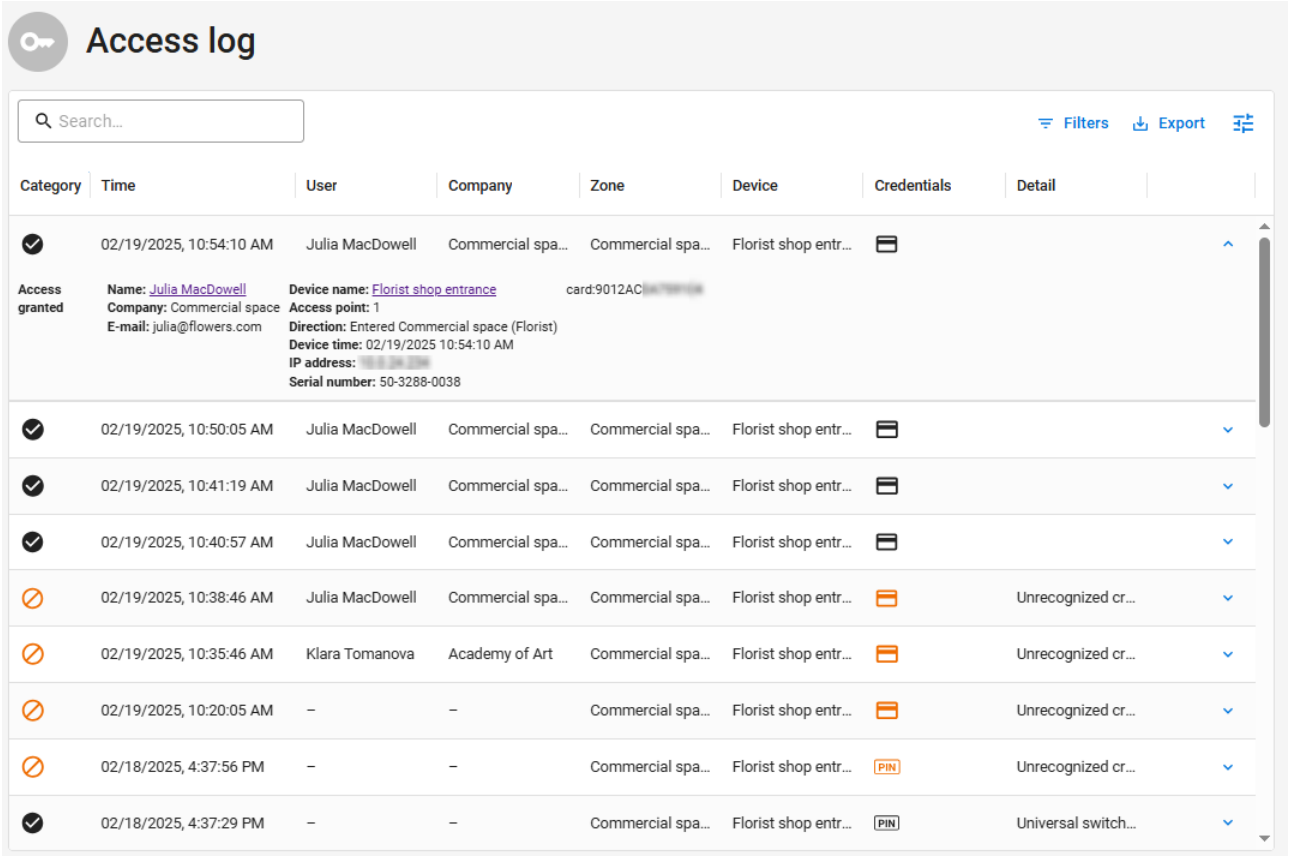
Une fois que l'utilisation de la capacité du disque atteint 80 %, la suppression automatique des journaux démarre. La capacité du disque peut être surveillée sur la page Paramètres. Les journaux du premier type

sont supprimés en premier dans l'ordre, les autres journaux sont supprimés progressivement jusqu'à ce que l'utilisation de l'espace disque tombe à 75 % ou jusqu'à ce qu'il ne reste que les journaux avec une durée de stockage minimale possible incomplète du type de journal donné.

La durée de stockage pour un type de journal donné est définie dans l'onglet **Paramètres > Rétention des journaux**. La conservation des enregistrements des caméras ne peut pas être plus longue que la conservation des journaux du système et des accès.

ASTUCE
Si vous utilisez constamment 70 % de la capacité du disque, nous vous recommandons de réduire la durée maximale de stockage des journaux.

Journaux d'accès



NOTE

- L'utilisateur voit les journaux qu'il est autorisé à consulter en fonction de ses autorisations utilisateur.
- Les données sont écrites dans les journaux en anglais.

La page Journaux d'accès affiche les enregistrements des tentatives d'authentification réussies et échouées et des verrouillages d'urgence.

La liste des journaux d'accès indique :

- Catégorie
  - accordé - accès autorisé
  - refusé - accès refusé
  - public – permettant un accès gratuit
  - verrouillage - verrouillage de l'appareil
- L'heure à laquelle l'événement s'est produit
- L'utilisateur qui a effectué l'action
- L'entreprise de l'utilisateur
- La zone dans laquelle l'événement s'est produit
- L'appareil sur lequel l'action s'est produite
- Authentification utilisée pour la tentative (PIN, QR code, etc.)

Cliquer sur une ligne développe des informations détaillées sur l'enregistrement donné.

La liste peut être filtrée en utilisant au-dessus de la liste. Alternativement, des filtres peuvent être définis pour des colonnes individuelles dans le menu étendu qui s'ouvre en cliquant sur dans l'en-tête de chaque colonne. Menu étendu de colonnes il permet également de déplacer les colonnes, de les épingler à la première ou à la dernière position ou de les masquer.

Exportation de logos

Les enregistrements peuvent être téléchargés dans un fichier CSV en cliquant sur le bouton Export au-dessus de la liste. Dans le fichier CSV exporté, l'heure est indiquée en GMT+0.

Durée de vie des journaux

Une fois que l'utilisation de la capacité du disque atteint 80 %, la suppression automatique des journaux démarre. La capacité du disque peut être surveillée sur la page Paramètres. Les journaux du premier type sont supprimés en premier dans l'ordre, les autres journaux sont supprimés progressivement jusqu'à ce que l'utilisation de l'espace disque tombe à 75 % ou jusqu'à ce qu'il ne reste que les journaux avec une durée de stockage minimale possible incomplète du type de journal donné.

La durée de stockage pour un type de journal donné est définie dans l'onglet **Paramètres > Rétention des journaux**. La conservation des enregistrements des caméras ne peut pas être plus longue que la conservation des journaux du système et des accès.

ASTUCE
Si vous utilisez constamment 70 % de la capacité du disque, nous vous recommandons de réduire la durée maximale de stockage des journaux.

Journal des appels

La page Journal des appels enregistre toutes les activités d'appel des interphones connectés et d'autres dispositifs SIP (par exemple, les répondeurs ou les communicateurs d'ascenseur).

NOTE
Le journal des appels n'est disponible qu'avec l'autorisation de l'administrateur.

La liste du journal des appels pour chaque événement indique

- type d'appel
- l'heure à laquelle l'appel a eu lieu
- si la porte est déverrouillée
- type d'appareil
- contrepartie
- durée de l'appel
- motif de la fin de l'appel

Cliquer sur une ligne développe des informations détaillées sur l'enregistrement donné.

La liste peut être filtrée en utilisant au-dessus de la liste. Alternativement, des filtres peuvent être définis pour des colonnes individuelles dans le menu étendu qui s'ouvre en cliquant sur dans l'en-tête de chaque colonne. Menu étendu de colonnes il permet également de déplacer les colonnes, de les épingler à la première ou à la dernière position ou de les masquer.

Exportation de logos

Les enregistrements peuvent être téléchargés dans un fichier CSV en cliquant sur le bouton Export au-dessus de la liste. Dans le fichier CSV exporté, l'heure est indiquée en GMT+0.

Durée de vie des journaux

La durée de conservation d'un type de journal donné est définie dans l'onglet *Paramètres* > *Stockage des enregistrements*.

ASTUCE
Si vous utilisez constamment 70 % de la capacité du disque, nous vous recommandons de réduire la durée maximale de stockage des journaux.

ATTENTION
Il est recommandé d'utiliser la dernière version du micrologiciel sur vos appareils pour que toutes les fonctionnalités du journal des appels fonctionnent correctement. Certaines informations et colonnes peuvent ne pas être disponibles ou ne pas s'afficher correctement sur les appareils dotés d'une version plus ancienne du micrologiciel.

- **Durée de l'appel :** La colonne Longueur d'appel n'est pas prise en charge par les versions antérieures du micrologiciel. Ces informations sont disponibles à partir de la version 2.49 du micrologiciel.
- **Identification de la contrepartie :** La version 2.50 du micrologiciel ou une version plus récente est nécessaire pour identifier correctement la contrepartie à partir du répertoire de l'appareil. Dans les versions plus anciennes, la recherche dans le répertoire du périphérique peut ne pas se dérouler correctement.

Notification

Le module Notifications vous permet de configurer la surveillance des événements sélectionnés et des propriétés du système dont il a connaissance. **Access Commander** informer par e-mail ou notification dans la barre supérieure à côté du menu utilisateur.

La liste des notifications est également affichée sur la page **Journaux du système > Notifications**.

Les enregistrements peuvent être téléchargés dans un fichier CSV en cliquant sur le bouton 

au-dessus de la liste. Dans le fichier CSV exporté, l'heure est indiquée en GMT+0.

Configuration d'un nouveau type de notification

1. Aller à la page **Paramètres > Notifications**.
2. Cliquez sur le bouton Ajouter dans le coin supérieur droit de la page.
3. Saisissez un nom pour le nouveau type de notification.
   Après la création, le détail de la notification sera affiché, dans lequel il est possible de sélectionner les appareils pour lesquels la notification doit être surveillée ; ajouter les utilisateurs auxquels la notification doit être envoyée ; choisissez le mode de livraison des notifications.

Paramètres de notification

Les types de notification sont définis dans les détails du type de notification. Pour ouvrir les détails du type de notification, cliquez sur la notification sélectionnée dans la liste de la page **Paramètres > Notifications**.

Mode de notification

Dans cet onglet, les méthodes de notification et la liste des destinataires des notifications par e-mail sont définies.

Dans **Access Commander**, les notifications apparaissent sous l'icône dans la barre supérieure, à côté du menu utilisateur, ou dans **Journal du système > Notifications**.

Des e-mails de notification peuvent être envoyés aux utilisateurs gérés dans **Access Commander** et les destinataires extérieurs au système. Les utilisateurs peuvent être sélectionnés dans la liste. Les adresses e-mail des autres destinataires doivent être saisies manuellement.

NOTE
Pour le bon fonctionnement des notifications par e-mail, il est nécessaire que SMTP soit correctement configuré, voir Activation et configuration de la fonction E-mail (SMTP) (p. 103).

Appareils surveillés

Le type de notification donné peut être généré à la fois pour tous les appareils et uniquement pour certains appareils. Si Surveiller tous les appareils est activé, l'événement peut se produire sur n'importe quel appareil et une notification sera générée. Si la surveillance de tous les appareils est désactivée, une notification sera générée uniquement si l'événement se produit sur l'appareil sélectionné. La sélection de l'appareil s'effectue dans le menu qui s'ouvre avec .

Durée de vie des journaux

Une fois que l'utilisation de la capacité du disque atteint 80 %, la suppression automatique des journaux démarre. La capacité du disque peut être surveillée sur la page Paramètres. Les journaux du premier type sont supprimés en premier dans l'ordre, les autres journaux sont supprimés progressivement jusqu'à ce que l'utilisation de l'espace disque tombe à 75 % ou jusqu'à ce qu'il ne reste que les journaux avec une durée de stockage minimale possible incomplète du type de journal donné.

La durée de stockage pour un type de journal donné est définie dans l'onglet **Paramètres > Rétention des journaux**. La conservation des enregistrements des caméras ne peut pas être plus longue que la conservation des journaux du système et des accès.

ASTUCE
Si vous utilisez constamment 70 % de la capacité du disque, nous vous recommandons de réduire la durée maximale de stockage des journaux.

Sociétés

Les réglages peuvent être effectués au sein d'une seule installation **Access Commander** diviser en **Sociétés**, qui sont gérés séparément. Cette méthode permet de répartir l'administration entre les administrateurs des différentes entreprises. Un administrateur d'une entreprise n'a pas accès aux informations sur une autre entreprise. Les administrateurs d'une entreprise ne verront pas les utilisateurs d'une autre entreprise.

Des zones ou des installations peuvent être partagées entre les entreprises, permettant de gérer les accès de l'entreprise aux espaces communs (entrées, restaurants, salles de conférence...).

Création d'une nouvelle entreprise

1. Aller à la page **Sociétés**.
2. Cliquez sur le bouton Ajouter une société dans le coin supérieur droit.
3. Remplissez le nom de l'entreprise.
4. Vous pouvez créer une entreprise en cliquant sur Créer.
   L'entreprise nouvellement créée apparaîtra dans la liste. Dans les détails de l'entreprise, il est nécessaire d'effectuer ses réglages. L'ajout d'utilisateurs à l'entreprise se fait dans les paramètres des utilisateurs individuels.

Paramètres de l'entreprise

Les informations sur l'entreprise peuvent être consultées et modifiées dans les détails de l'entreprise. Un détail d'entreprise s'ouvre en cliquant sur une entreprise sélectionnée dans sa liste sur la page Entreprises.

Dans l'en-tête de la fiche de l'entreprise, un bouton Blocage active le Verrouillage d'urgence (p. 64) pour tous les appareils dans les zones de cette entreprise.

Les détails de l'entreprise sont divisés en onglets Présentation, E-mails et Synchronisation des utilisateurs.

Le langage de la société

Dans l'onglet Général, vous pouvez sélectionner la langue de l'entreprise dans laquelle l'interface sera utilisée **Access Commander** afficher aux utilisateurs de cette entreprise. Les utilisateurs peuvent modifier la langue de l'interface ultérieurement. Le choix de la langue par l'entreprise affecte également les modèles d'e-mails envoyés aux Utilisateurs. La formulation des e-mails peut être modifiée dans l'onglet E-mails.

Zones

L'attribution de zones à une entreprise définit l'ensemble des installations auxquelles les utilisateurs de l'entreprise auront droit d'accéder (par exemple, la zone des espaces communs et la zone du 4ème étage, qui comprennent la porte d'entrée de la réception et toutes les entrées du quatrième étage.). Les zones peuvent être attribuées à plusieurs entreprises en même temps, et plusieurs zones peuvent être attribuées à une seule entreprise.

My2N app

Dans l'entreprise, il est possible de définir des paramètres d'appairage avec Application My2N, qui permet l'authentification Bluetooth. Les appareils sur lesquels les utilisateurs pourront s'appairer ainsi que la période de validité de l'accès mobile requis pour l'appairage sont définis. L'accès mobile lui-même est généré dans les paramètres utilisateur.

Visites

Dans cet onglet, des groupes sont configurés auxquels l'administrateur de la visite pourra attribuer de nouvelles visites. L'un des groupes peut être spécifié par défaut. La nouvelle visite sera automatiquement attribuée au groupe par défaut, sauf indication contraire.

ATTENTION
Sans un groupe par défaut correctement défini, il n'est pas possible de donner accès aux visiteurs dans l'interface utilisateur simplifiée.

Il est possible de sélectionner les méthodes d'authentification pouvant être attribuées à la visite. La méthode d'authentification est ensuite attribuée à une visite par le responsable de la visite.

En savoir plus sur la configuration des visites dans Visites (p. 81).

Fonds de travaux

Le pool de travail et les jours fériés sont utilisés pour calculer le pool de travail mensuel des utilisateurs dans le module de présence. En sélectionnant les jours, il est possible de déterminer quels jours de la semaine seront comptés comme jours ouvrables. Le jour est sélectionné en cliquant. Les jours verts identifient les jours qui sont considérés comme des jours ouvrables.

L'aménagement du temps de travail définit la durée d'une journée de travail.

Vacances

En fixant des jours fériés, vous déterminez quels jours ne sont pas inclus dans le calcul du pool de travail mensuel. Les heures travaillées un jour férié sont comptées de la même manière que les heures travaillées le week-end : le temps travaillé est enregistré en plus des heures normales de travail.

Offre étendue vous permet de copier les jours fériés d'une autre entreprise. Les jours fériés sont copiés, y compris les dates et les noms. La copie peut être utilisée à plusieurs reprises, mais si le jour férié nouvellement copié est déjà défini dans l'entreprise, son nom sera écrasé.

Courriels envoyés aux membres de l'entreprise

Les paramètres de messagerie ont leur propre onglet dans les détails de l'entreprise. **Access Commander** vous permet d'envoyer des e-mails automatiques aux membres de l'entreprise (y compris les visiteurs) avec des informations sur l'attribution d'une méthode d'authentification. Un e-mail est envoyé à l'utilisateur ou au visiteur avec l'adresse e-mail définie.

Access Commander vous permet d'envoyer des emails avec les informations suivantes :

- Code PIN pour la visite
- QR code pour la visite
- Code PIN de l'utilisateur
- Code QR pour les utilisateurs
- My2N app pour configurer l'authentification Bluetooth pour l'utilisateur

Dans les **détails de l'entreprise > onglet Emails > onglet Modèles d'e-mails**, il est possible de paramétrer l'apparence de ces emails et de modifier leur formulation. L'édition du libellé d'un e-mail se fait dans une fenêtre de dialogue qui s'ouvre en cliquant sur le type d'e-mail sélectionné. Dans la boîte de dialogue, vous pouvez modifier :

- sujet - le sujet de l'e-mail
- en-tête – affiché dans le champ coloré du corps de l'e-mail
- introduction – le texte donné avant les données générées automatiquement à partir de **Access Commander**
- message suivant – le texte suivant les données générées à partir de **Access Commander**
- signature - la signature donnée à la fin de l'e-mail

Synchronisation d'entreprise (LDAP)

La synchronisation avec LDAP est utilisée pour télécharger les utilisateurs et leurs modifications depuis un système LDAP externe. Les données utilisateur comprennent le nom d'utilisateur, l'identifiant, les identifiants

de carte, le code PIN/QR, la photo, l'adresse e-mail, le numéro de téléphone, le mot de passe et l'identifiant, les marques d'immatriculation du véhicule.

NOTE
De plus amples informations sur LDAP sont disponibles sur www.ldap.com.

1. Allez dans **Entreprises > Détails de l'entreprise > Onglet Synchronisation des utilisateurs**.
2. Si aucune connexion n'est définie, créez-en une.
   Remplir:

   - **Le nom du serveur** – si DNS est correctement configuré, entrez simplement le nom du serveur (« WIN-9ABEB4AUOHD »). Si DNS n'est pas défini, l'adresse IP du serveur sur lequel le service LDAP est exécuté est saisie dans le nom du serveur.
   - **Port** – le paramètre par défaut est le port LDAP 389 (sans SSL). Si vous souhaitez utiliser une connexion cryptée dans votre entreprise, saisissez le numéro de port 636. La prise en charge SSL doit également être activée côté serveur LDAP. Si l'administrateur définit un numéro de port différent, il doit également être modifié dans v **Access Commander**.
   - **Identifiant** – le nom de login de l'utilisateur qui dispose des droits correspondants pour la racine donnée, ou l'arborescence entière. Le nom de login doit être renseigné sous la forme : "administrator@domain.com"
   - **Mot de passe** – le mot de passe de l'utilisateur indiqué sur le serveur LDAP.
   - **Sécurité des communications (SSL)** – lorsque SSL est désactivé, il n'est pas nécessaire de réécrire le numéro de port. Lors de l'activation de SSL, le numéro de port doit être modifié en 636.
   - **DN de base** – le point racine à partir duquel la recherche dans l'annuaire commence. Il peut s'agir d'une extension ou de la racine d'un répertoire, tel que : CN=administrateur, CN=utilisateurs, DC=domaine, DC=com.

   L'activation de TLS permet d'activer le Transport Layer Security (TLS) pour la connexion FTP. TLS crypte les données transmises entre **Access Commander** et le serveur.
   Activer l'authentification du certificat TLS pour activer l'authentification TLS des certificats fournis par le serveur. Lorsque cette option est activée, **Access Commander** vérifie qu'il communique avec un serveur de confiance, ce qui augmente la sécurité de la connexion.
3. Le détail de la connexion LDAP définie s'ouvre. Les paramètres de connexion peuvent être testés. En utilisant le bouton Synchroniser maintenant vous démarrez une synchronisation unique.
4. L'onglet Options de **vous permet de gérer la synchronisation des données.**

   Vous pouvez supprimer la connexion définie dans le menu étendu ⋮ cartes **Importer**. Sur carte **Possibilités** d'autres paramètres de synchronisation sont définis.

ASTUCE
La synchronisation automatique est définie sur l'onglet **Importer**. Lors de l'activation de la synchronisation automatique, renseignez les intervalles auxquels la synchronisation doit avoir lieu. Selon la fréquence, choisissez à quelle minute ou heure les données seront synchronisées.

Paramètres de synchronisation des données LDAP

Attributs importés - La modification du schéma définit l'affectation des attributs du serveur LDAP aux paramètres de **Access Commander**.

NOTE
Les attributs du numéro de téléphone sont complétés par un filtre qui convertit les numéros au format souhaité, compatible avec la liste des utilisateurs de l'entreprise sur **Access Commander**. Deux filtres sont disponibles :

- `toPhoneNumber` - supprime les caractères inutiles (espaces, traits d'union, etc.) des numéros de téléphone.
- `skipExtension` - supprime l'extension des numéros de téléphone.

Exemple d'utilisation : Si vous saisissez l'attribut `{telephoneNumber|toPhoneNumber|skipExtension}`, la valeur originale du numéro de téléphone dans Active Directory « +420 123 456 789 x2222 » est convertie en « +420123456789 ».

Utilisateurs supprimés de LDAP – définit ce qui doit arriver aux utilisateurs qui ont été supprimés dans LDAP. Les utilisateurs supprimés de LDAP peuvent être **Access Commander** conservez-les ou supprimez-les également. Si les utilisateurs doivent être désactivés, après avoir supprimé des utilisateurs de LDAP, leurs données resteront dans **Access Commander**, mais ne se synchronisera pas avec les appareils.

Users removed from LDAP - définit ce qu'il faut faire des utilisateurs qui ont été supprimés de LDAP. Les utilisateurs supprimés de LDAP peuvent être conservés dans **Access Commander** ou supprimés également. Si les utilisateurs doivent être désactivés, après leur suppression du LDAP, leurs données resteront dans **Access Commander**, mais ne seront pas synchronisées avec les appareils. Les utilisateurs désactivés n'ont pas de droits d'accès, ne sont pas joignables, etc.

Synchronisation des groupes - permet de télécharger les membres d'un groupe depuis LDAP vers **Access Commander**. En utilisant les paramètres du schéma de synchronisation, vous pouvez définir un DN de base personnalisé et un filtre pour synchroniser les groupes. Dans les paramètres du schéma, vous pouvez activer la synchronisation des utilisateurs des groupes imbriqués.

Synchronisation des avatars – définit le téléchargement des photos de l'utilisateur à partir du système LDAP.

Suivi des liens – définit s'il faut synchroniser les données des liens LDAP.

Recherche imbriquée - permet la synchronisation de l'utilisateur à partir de l'ensemble de l'arbre. Lorsqu'elle est désactivée, seules les données de la racine sont recherchées et synchronisées.

Pagination activée – la pagination utilise l'extension LDAP Simple Paged Results Control. Cela permet de diviser les résultats en plusieurs pages, ce qui est essentiel pour les grands services d'annuaire. Paramètre **Taille de la page** détermine le nombre d'enregistrements qu'une page contiendra.

Importer des utilisateurs dans l'entreprise

Offre étendue ⋮ dans l'en-tête détaillé de l'entreprise, il permet d'importer une seule fois de nouveaux utilisateurs dans l'entreprise, soit à partir d'un fichier CSV, soit à partir d'un autre appareil 2N.

Importer des utilisateurs à partir d'un fichier CSV

ASTUCE
Vous pouvez télécharger un exemple de fichier CSV pour importer des utilisateurs en utilisant ce lien.

Access Commander permet le téléchargement en masse d'utilisateurs dans l'entreprise. Les informations de base sur les utilisateurs peuvent être préparées dans un fichier externe, puis l'utilisateur peut être importé facilement. Les utilisateurs ne peuvent être téléchargés que vers une entreprise spécifique à la fois dans un seul fichier.

Cette fonctionnalité ne permet pas de supprimer des utilisateurs.

NOTE
Les utilisateurs dotés du rôle d'administrateur peuvent effectuer une synchronisation complète et reproductible de la liste d'utilisateurs dans toutes les entreprises, à savoir Synchronisation des utilisateurs avec FTP (p. 94).

Importer depuis un appareil 2N

Vous pouvez transférer une liste d'utilisateurs d'un appareil 2N vers **Access Commander**. Vous ne pouvez importer qu'à partir d'un appareil qui n'a pas encore été ajouté à **Access Commander**. Un appareil ne peut pas contenir des utilisateurs qui sont déjà dans **Access Commander** (c'est-à-dire qui ont le même UUID). Tous les utilisateurs ne peuvent être importés en masse que vers une entreprise spécifique.

1. Il est conseillé de sauvegarder la configuration avant de l'importer. Le système **Access Commander** est sauvegardé dans l'onglet **Paramètres > Sauvegarde du système**. La sauvegarde de la configuration de l'appareil se fait dans son interface de configuration web, sous **Système > Maintenance**.
2. Ajoutez l'appareil à partir duquel vous souhaitez importer la liste des utilisateurs en tant qu'appareil **Access Commander**.

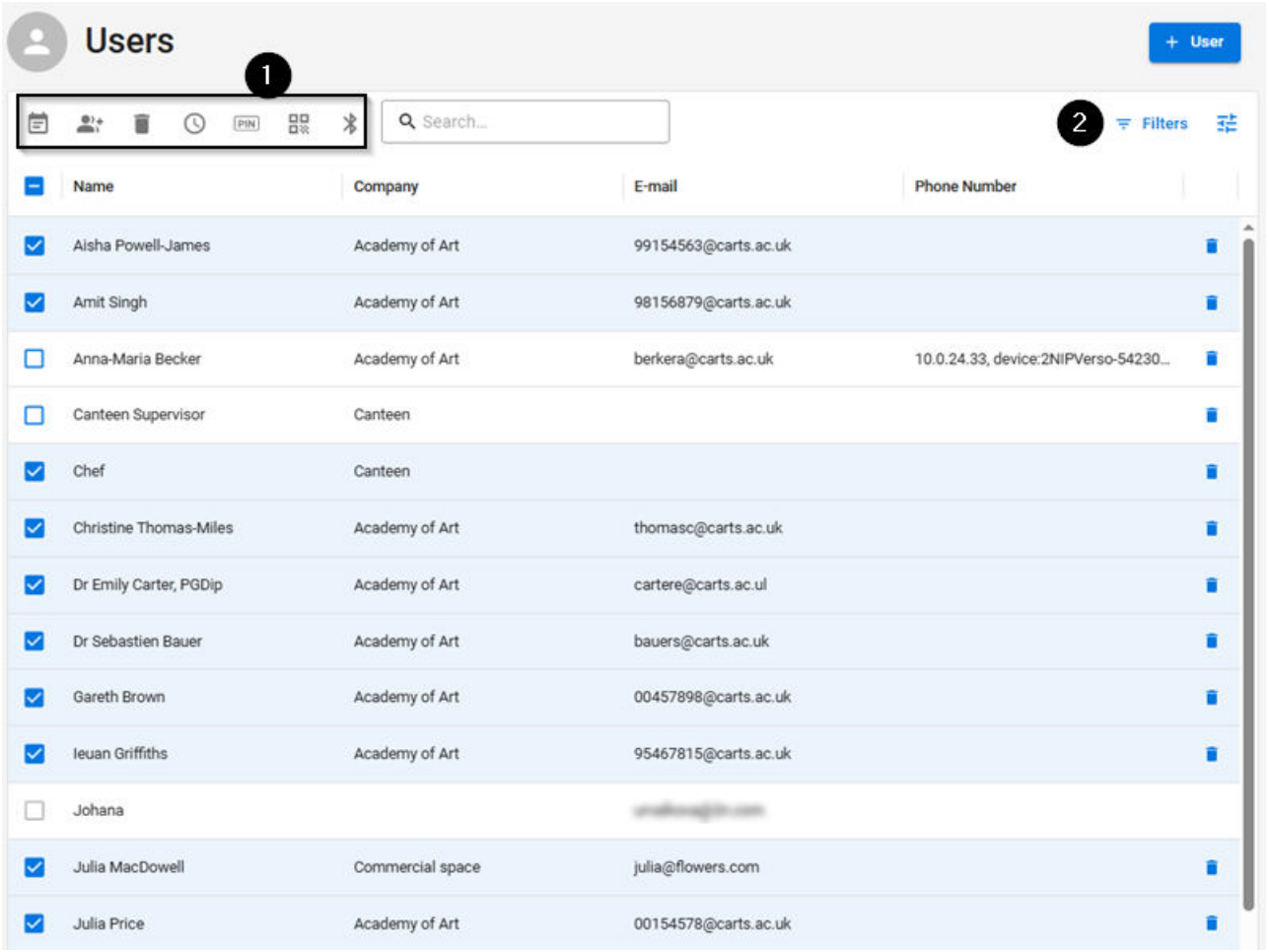
   ATTENTION
   N'ajoutez pas encore d'appareils aux zones ! L'appareil hériterait des règles d'accès et la liste des utilisateurs serait écrasée sur l'appareil.
3. Accédez aux détails de l'entreprise dans laquelle vous souhaitez importer l'utilisateur. Dans le menu avancé ⋮, sélectionnez Importer à partir d'un appareil | Import ze zařízení.
4. Une boîte de dialogue s'ouvrira. Dans la liste déroulante des appareils disponibles, choisissez l'appareil à partir duquel vous souhaitez importer la liste des utilisateurs.
5. Cliquez sur Importer pour lancer l'importation en arrière-plan. L'achèvement du processus est consigné dans le journal du système.
6. Une fois l'importation réussie, l'appareil peut être ajouté aux zones et inclus dans les règles d'accès.

ATTENTION
La procédure d'importation ne fonctionne que pour des utilisateurs spécifiques (UUID) sur l'appareil et importe tous les utilisateurs de l'appareil en même temps dans une seule entreprise.

Utilisateurs

Aide **Access Commander** peut être géré **Utilisateurs**, modifier leurs accès, gérer leurs coordonnées, etc.

La liste des utilisateurs affiche tous les utilisateurs qui ont été créés. Au-dessus de la liste, vous pouvez filtrer les utilisateurs (numéro 2 dans l'image) ou rechercher un utilisateur spécifique par son nom, son adresse électronique ou son numéro de téléphone.



Actions de masse

Vous pouvez sélectionner plusieurs utilisateurs en les marquant et appliquer les actions en bloc suivantes (numéro 1 dans la figure) :

- Activer le suivi des présences pour les utilisateurs
- Ajouter un utilisateur au groupe
- Supprimer l'utilisateur
- Définir l'intervalle de temps de validité de l'accès
- Attribuez un code PIN d'accès aux utilisateurs qui n'ont pas encore reçu de code PIN ou de code QR
- Attribuez un code QR d'accès aux utilisateurs qui n'ont pas encore reçu de code PIN ou de code QR

- Attribuez un accès mobile aux utilisateurs de la sélection qui n'ont pas encore reçu d'accès mobile.

NOTE
Pour attribuer un code PIN/QR ou un accès mobile à un utilisateur, il est nécessaire que l'utilisateur dispose d'une adresse e-mail valide.

Créer un nouvel utilisateur

1. Aller à la page **Utilisateurs**.
2. Cliquez sur le bouton Ajouter un utilisateur dans le coin supérieur droit.
3. Remplissez les informations requises : nom d'utilisateur et société à laquelle il appartient.
   L'utilisateur nouvellement créé apparaîtra dans la liste et les détails de l'utilisateur s'ouvriront. D'autres paramètres utilisateur sont définis en détail, tels que l'attribution d'un numéro de téléphone, la définition de méthodes d'authentification, l'attribution à des groupes, etc.

NOTE
Access Commander permet le téléchargement en masse d'utilisateurs dans l'entreprise. Les informations de base sur les utilisateurs peuvent être préparées dans un fichier externe, puis l'utilisateur peut être importé facilement. Les utilisateurs ne peuvent être téléchargés que vers une entreprise spécifique à la fois dans un seul fichier.

L'importation en vrac est effectuée dans les coordonnées de l'entreprise, à savoir Importer des utilisateurs dans l'entreprise (p. 47).

Paramètres utilisateur

Les informations utilisateur peuvent être consultées et gérées dans les détails de l'utilisateur. Le détail de l'utilisateur s'ouvre en cliquant sur l'utilisateur sélectionné dans la liste de la page Utilisateurs.

Les détails de l'utilisateur sont divisés en onglets Aperçu, Présence et Journal des modifications. L'onglet Présence s'affiche uniquement pour les utilisateurs pour lesquels le suivi est activé, voir Suivi de la présence des utilisateurs (p. 57). Le module de présence est disponible en fonction de la licence.

Changer le nom et la photo de l'utilisateur

Les options pour renommer l'utilisateur et définir la photo se trouvent dans le menu étendu dans l'en-tête des détails de l'utilisateur.

La résolution de l'image sera automatiquement ajustée à 432 × 432 px.

Authentification

Cet onglet est utilisé pour définir les méthodes d'authentification des utilisateurs sur les appareils. L'utilisateur doit s'authentifier sur l'appareil et s'il dispose d'un accès valide, il se verra accorder l'accès à l'appareil.

Carte RFID – ajoute une carte RFID existante à l'utilisateur. Une boîte de dialogue s'ouvrira dans laquelle vous devrez saisir l'identifiant de la carte. L'identifiant peut être chargé en plaçant la carte devant un lecteur USB ou en saisissant la carte d'identité à l'aide du clavier. L'identifiant doit être un nombre hexadécimal d'au moins 6 caractères. Un utilisateur peut se voir attribuer jusqu'à 2 cartes d'accès.

Une carte d'accès RFID peut être utilisée pour accéder à un maximum de 90 portes équipées de serrures 2N Fortis, en fonction du nombre de profils temporels appliqués. Si la capacité de mémoire de la carte est dépassée, l'écriture des données sur la carte échoue. L'échec de l'écriture est enregistré dans le journal des accès au système. En cas d'utilisation de groupes de fermeture, il est possible d'écrire plus de portes sur une seule carte qu'en cas d'affectation individuelle. En cas d'utilisation de groupes de fermeture, il est possible d'inscrire plus de portes par carte qu'en cas d'affectation individuelle.

ASTUCE
Le gestionnaire des utilisateurs et l'administrateur peuvent afficher l'identifiant de la carte dans le journal d'accès. Il est ainsi possible de charger une voiture nouvelle/non attribuée sur un appareil accessible puis de copier son identifiant depuis le log. Après avoir inséré l'identifiant entre les cartes RFID, l'utilisateur peut commencer à utiliser la carte. L'affichage des identifiants dans le journal d'accès doit être activé dans **Paramètres > Authentification**.

NOTE
Si **Access Commander** signale que la toute nouvelle carte qui vient d'être ajoutée est déjà utilisée dans le système, la raison peut être que le mode de compatibilité des cartes RFID est activé. Ce mode est activé par l'administrateur dans **l'onglet Paramètres > Authentification > Mode de compatibilité**.

My2N app – utilisé pour se connecter à l'application My2N activation de l'authentification via Bluetooth, voir chapitre Authentification Bluetooth (p. 54).

Code PIN – génère automatiquement un code PIN à 5 chiffres.

L'utilisateur peut se voir attribuer un code PIN ou QR pour y accéder, mais vous ne pouvez pas avoir les deux en même temps.

QR Code – générera automatiquement un code QR. Les appareils permettant la lecture des QR codes sont répertoriés dans Appareils et applications pris en charge (p. 8).

L'utilisateur peut se voir attribuer un code PIN ou QR pour y accéder, mais vous ne pouvez pas avoir les deux en même temps.

Empreinte digitale – ouvre une boîte de dialogue pour télécharger une empreinte digitale, que l'utilisateur peut utiliser pour s'authentifier sur les appareils prenant en charge leur lecture. Chaque utilisateur peut télécharger jusqu'à 2 empreintes digitales. La procédure est décrite dans le chapitre Téléchargement d'empreintes digitales (p. 54).

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

Carte virtuelle – vous permet de définir l'ID de la carte d'accès virtuelle de l'utilisateur. Chaque utilisateur peut se voir attribuer exactement une carte virtuelle. L'ID de la carte virtuelle est une séquence de 6 à 32 caractères de l'ensemble 0 à 9, A à F. Le numéro de carte virtuelle est utilisé pour identifier l'utilisateur dans les appareils connectés via l'interface Wiegand.

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.

ATTENTION
Avec l'authentification multifacteur, il est nécessaire de suivre l'ordre des méthodes d'authentification.

ASTUCE
Lors du remplissage de l'adresse e-mail, il est possible d'envoyer le code PIN/QR d'accès généré à l'adresse indiquée.

Compte

En définissant un nom de connexion et un mot de passe à usage unique, il est possible d'accorder à l'utilisateur l'accès à l'interface **Access Commander**. Une fois connecté, l'utilisateur peut suivre sa présence (si elle est disponible), modifier son e-mail ou changer sa photo de profil. Lors de sa première connexion, l'utilisateur sera invité à modifier son mot de passe. Si une authentification à deux facteurs est requise pour l'utilisateur, celui-ci sera invité à se connecter à sa propre application d'authentification, voir Authentification à double facteur (p. 103). Dans cet onglet, il est également possible de supprimer la connexion à l'application d'authentification.

Dans l'onglet Compte, il est possible d'accorder des autorisations administratives aux utilisateurs disposant de données de connexion **Access Commander** en utilisant les rôles d'utilisateur. Les autorisations des différents rôles sont décrites dans le chapitre Autorisations utilisateur (p. 7).

Interface simplifiée

Une interface utilisateur simplifiée peut être lancée pour le gestionnaire des visites d'une entreprise. Une interface simplifiée permet au gestionnaire des visites d'ajouter, de supprimer et de gérer les visites. Les journaux et la présence ne peuvent pas être consultés dans une interface simplifiée. Le but d'une interface simplifiée est avant tout de permettre aux utilisateurs de l'appartement d'autoriser plus facilement l'accès à ses visiteurs. Toutes les visites créées dans une interface simplifiée sont toujours affectées au *groupe par défaut pour les nouvelles visites*. Le gestionnaire des visites n'a pas la possibilité de modifier ce groupe. Le groupe par défaut pour les nouveaux visiteurs doit être sélectionné à l'avance dans les paramètres de l'entreprise et des règles d'accès valides pour l'accès à l'appartement, y compris le chemin d'accès, doivent être définies pour le groupe. L'utilisateur de l'appartement peut alors gérer les méthodes d'authentification et la durée des visites dans une interface simplifiée.

ATTENTION
Avant d'activer l'interface simplifiée **l'administrateur système doit définir le groupe par défaut pour les nouvelles visites** dans Paramètres de l'entreprise (p. 44). Ces règles d'accès doivent être attribuées au groupe par défaut afin que le visiteur ait accès aux zones visitées. Sans un groupe par défaut correctement défini, il n'est pas possible de donner accès aux visiteurs dans l'interface simplifiée.

Données personnelles

Utilisé pour ajouter des informations de base sur l'utilisateur. Permet d'ajouter l'adresse e-mail de l'utilisateur à laquelle seront envoyées les informations relatives au compte de l'utilisateur, et d'ajouter un numéro de téléphone pour contacter l'utilisateur.

Il est possible d'écrire sur la carte :

- **E-mail** - l'adresse à laquelle l'utilisateur recevra les informations relatives à son compte **Access Commander**
- **Numéro d'utilisateur** - un identifiant spécifique requis pour la synchronisation en masse avec un fichier CSV (voir Synchronisation des utilisateurs avec FTP (p. 94))
- **Note à l'attention de**

Approches

L'onglet Accès permet d'affecter un utilisateur à un groupe et de définir l'intervalle de temps pendant lequel les informations d'identification de l'utilisateur seront valides. L'intervalle de temps est défini dans le menu avancé de l'onglet, qui s'ouvre en cliquant sur ⋮. Le réglage de l'heure de début de validité ne s'applique qu'aux accès aux périphériques IP. L'accès aux serrures électroniques 2N Fortis est valable à partir du moment où la carte d'accès est attribuée à l'utilisateur.

ASTUCE
Les limites de temps d'accès aux appareils sont définies via des profils horaires.

Si l'utilisateur est membre d'un groupe, l'onglet affiche ce groupe. Si l'utilisateur n'est pas affecté à un groupe, il peut être ajouté dans l'onglet. Le groupe peut être modifié ou supprimé dans le menu avancé ⋮.

Les numéros de téléphone

Cette carte permet d'établir la connexion avec l'utilisateur. Le numéro de téléphone est la destination de l'appel de l'appareil appartenant à cet utilisateur.

Numéro virtuel

Un numéro de téléphone virtuel peut être utilisé pour appeler un utilisateur à l'aide du clavier numérique de l'appareil. Les numéros virtuels ne sont pas liés aux numéros de téléphone personnels des utilisateurs, ce qui permet de masquer les numéros de téléphone personnels des utilisateurs sur l'appareil. Les numéros virtuels peuvent, par exemple, être configurés en fonction des numéros d'appartements. Les numéros virtuels peuvent ainsi être utilisés dans les installations où le nombre de touches de numérotation rapide est insuffisant.

Un numéro virtuel peut comporter entre 1 et 7 chiffres. Le premier et le dernier caractère peuvent être soit un chiffre, soit une lettre, tandis que les autres caractères doivent être uniquement des chiffres (par exemple, A123, 456B, C12E).

Remplaçant

Dans cet onglet, il est également possible de définir un remplaçant vers lequel l'appel sera redirigé en cas d'indisponibilité de cet utilisateur. Le représentant peut être choisi parmi les autres utilisateurs de l'entreprise.

Journal d'accès

Le journal d'accès affiche l'historique des accès.

Journal des modifications

Toutes les modifications apportées aux paramètres utilisateur peuvent être consultées dans l'onglet Journal des modifications. Le tri de base se fait en fonction du moment du changement. Dans le journal, il est possible de savoir qui a effectué la modification. Après avoir cliqué sur la ligne, il est possible de connaître le détail de la modification effectuée.

Téléchargement d'empreintes digitales

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.

Téléchargement d'empreintes digitales

1. Assurez-vous que le lecteur d'empreintes digitales USB est activé dans **Paramètres > Accès**.
2. Dans les paramètres utilisateur v **Onglet Authentification** choisir l'authentification Empreinte digitale.
3. Sélectionnez le doigt pour lequel vous souhaitez télécharger une empreinte digitale.
   Une fenêtre intitulée « Téléchargement d'empreintes digitales » apparaîtra.
4. Placez le doigt sélectionné sur le lecteur. Répétez cette étape 3 fois, à chaque fois lorsque vous y êtes invité.
   Après la dernière numérisation, vous serez informé de la réussite de la numérisation de l'empreinte digitale.
5. En appuyant sur le bouton**Créer**le processus est terminé.

Authentification 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.

Ce processus est sécurisé par le **mécanisme d'appariement Bluetooth de confiance**. Le processus d'appairage varie en fonction de la version du micrologiciel de l'appareil connecté.

GET IT ON Google Play Download on the App Store

La connexion de l'application sur le téléphone de l'utilisateur aux appareils 2N s'effectue en saisissant le code d'appariement dans l'application My2N.

Le code d'appariement peut être obtenu de deux manières :

- en se connectant au dispositif **2N OS**
- via un lecteur USB Bluetooth connecté à votre ordinateur

ATTENTION
Pour que l'appairage soit réussi, l'appareil doit être doté de la version 2.50 (ou 3.0) du micrologiciel ou d'une version plus récente. Si l'appareil est doté d'un logiciel plus ancien, l'appairage sera effectué à l'aide de l'ancien mécanisme en utilisant **PIN** sans **QR code**.

ASTUCE
Pour un niveau de sécurité plus élevé, il est préférable d'appairer en utilisant le **code QR** . Si le **code QR** n'est pas disponible ou n'est pas pris en charge par votre appareil, utilisez le code **PIN** .

Création d'un code d'appairage via ordinateur

1. Télécharger sur votre ordinateur 2N USB Driver IP et installez-le.
2. Assurez-vous que le lecteur USB Bluetooth est activé dans **Paramètres > Authentification > onglet Lecteurs USB activés**.
3. Connectez le lecteur USB Bluetooth à l'ordinateur.
4. Dans les paramètres utilisateur v **Onglet Authentification** choisir l'authentification My2N app.
5. Dans la boîte de dialogue qui s'ouvre, sélectionnez Associer à l'aide d'un lecteur.
   Un code d'appairage apparaîtra dans la boîte de dialogue.
6. Suivez la procédure ci-dessous (Couplage dans l'application mobile My2N app (p. 55)) pour effectuer le couplage dans l'application.

Créer un code d'appairage sur l'appareil

1. Assurez-vous que
   - le périphérique de couplage est défini pour l'entreprise de l'utilisateur donné, voir???;
   - le dispositif d'appairage est situé dans une zone à laquelle l'utilisateur a un accès valide, à savoir Règles d'accès (p. 74);
   - un moment adéquat pour l'appairage est défini, à savoir???.
2. Dans les paramètres utilisateur v **Onglet Authentification** choisir l'authentification My2N app.
3. Dans la boîte de dialogue qui s'ouvre, sélectionnez Associez-le à l'aide de votre appareil.
4. Le code d'appairage généré est affiché sur la carte avec le temps d'appairage restant. Transmettez le code d'appairage à l'utilisateur. Si l'utilisateur dispose d'une adresse email renseignée, vous pouvez envoyer la clé mobile à l'email en cliquant sur .
5. Suivez la procédure ci-dessous (Couplage dans l'application mobile My2N app (p. 55)) pour effectuer le couplage dans l'application.

Couplage dans l'application mobile My2N app

1. Téléchargez-le Application My2N sur votre téléphone portable. L'application est disponible sur App Store et Google Play.
2. Ouvrez l'application et saisissez le code PIN de couplage.

   NOTE
   Si l'application affiche le **code QR** , mais que l'appareil utilise un micrologiciel antérieur à 2.50.0, l'appairage ne sera possible qu'en entrant le code **PIN** .
3. Autorisez toutes les autorisations importantes pour que l'application My2N fonctionne correctement.
4. Suivez les instructions sur le téléphone mobile - approchez l'appareil en mode appairage et cliquez sur Commencer l'appairage. Le téléphone mobile recherchera ensuite un appareil avec lequel s'associer.
5. Accordez l'accès au téléphone mobile sélectionné. Vous pouvez alors ouvrir les portes dans tout le site.

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.

Autorisations utilisateur

Rapport dans **Access Commander** peut être effectuée par plusieurs utilisateurs en fonction des autorisations qui leur sont attribuées.

Les comptes élevés sont configurés via un rôle dans les paramètres utilisateur. Plusieurs rôles peuvent être attribués à un seul utilisateur.

NOTE
Les autorisations des utilisateurs s'appliquent à la gestion au sein de l'entreprise de l'utilisateur. L'administrateur a accès à une gestion complète dans toutes les entreprises.

Administrateur

- Configuration du système et des modules individuels selon la licence valide.
- Changement de licence
- Toutes les autorisations des autres rôles applicables à toutes les entreprises.

Gestionnaire d'accès

- Créez et gérez des groupes.
- Gérer leurs adhésions à des groupes.
- Créez et gérez des visites.
- Création et gestion de profils horaires.
- Définition des règles d'accès.

Gestionnaire des utilisateurs

- Créez et gérez des utilisateurs.
- Créez et gérez des visites.
- Gérer leurs adhésions à des groupes.
- Affichage du journal d'accès et du système.

Responsable des visites

- Créez et gérez des visites.
- Gérer leurs adhésions à des groupes.
- Consultation du journal d'accès des visites.

Gestionnaire de portes

- Surveillance de la transmission des caméras à partir des appareils attribués.
- Ouverture à distance des appareils attribués.
- Verrouillage d'urgence des appareils attribués.
- Affichage du journal d'accès des appareils attribués.
- Surveillance des états et des événements de sécurité dans le journal système.

Responsable des présences

- Suivi et gestion de la fréquentation des groupes assignés.
- Affichage du journal d'accès des utilisateurs des groupes attribués.

Administrateur de l'entreprise

- Définir la langue par défaut de l'entreprise.
- Surveillance du journal du système (limitée aux événements de l'entreprise).
- La possibilité de créer un widget pour le journal du système et la fonction de verrouillage d'urgence sur les appareils utilisés par l'entreprise (y compris les appareils partagés avec d'autres entreprises).

Suivi de la présence des utilisateurs

Access Commander permet de surveiller la présence des utilisateurs. En mode présence, les heures d'entrée et de sortie des utilisateurs individuels sont enregistrées.

L'enregistrement des présences des utilisateurs doit être activé. L'activation se fait dans le menu étendu ⋮ dans l'en-tête des détails de l'utilisateur. L'activation de l'enregistrement des présences pour plusieurs utilisateurs en même temps peut être effectuée en sélectionnant des utilisateurs dans la liste sur la page Utilisateurs et en utilisant une action groupée. .

Le gestionnaire de présence peut modifier les données de présence des utilisateurs. L'édition se fait en cliquant sur l'intervalle de temps à modifier. Une fois ouvertes, les heures limites peuvent être modifiées et une note peut être ajoutée à l'intervalle.

ATTENTION
Pour le bon fonctionnement de la fréquentation, il est nécessaire d'avoir **Access Commander**licence active disponible pour suivre la présence des utilisateurs. Le suivi des présences doit être activé dans les paramètres de chaque utilisateur.

Le suivi et l'ajustement de la fréquentation sont décrits dans le chapitre Présence (p. 78).

Groupes

Le groupe permet de regrouper les utilisateurs et de paramétrer plus facilement les droits de ses membres pour accéder à la zone. Les droits ne doivent pas être définis au niveau des utilisateurs et des visites individuels, mais le groupe sera associé à la zone.

La liste peut être filtrée en utilisant au-dessus de la liste. Alternativement, des filtres peuvent être définis pour des colonnes individuelles dans le menu étendu qui s'ouvre en cliquant sur dans l'en-tête de chaque colonne. Menu étendu de colonnes il permet également de déplacer les colonnes, de les épingler à la première ou à la dernière position ou de les masquer.

Créer un nouveau groupe

1. Aller à la page **Groupes**.
2. Cliquez sur le bouton pour ajouter un groupe dans le coin supérieur droit.
3. Dans la fenêtre de dialogue qui s'ouvre, vous devez saisir le nom du groupe et sélectionner à quelle entreprise il appartient.

> **ATTENTION**
> Une fois un groupe créé, la société mère ne peut plus être modifiée.

Le groupe nouvellement créé apparaîtra dans la liste et ses détails s'ouvriront. Dans les détails du groupe, vous devez ajouter des membres et définir leurs règles d'accès.

Paramètres du groupe

Les informations du groupe peuvent être consultées et modifiées dans les détails du groupe. Les détails du groupe sont ouverts en cliquant sur le groupe sélectionné dans la liste des groupes. En détail, vous trouverez un aperçu des membres du groupe et un aperçu de leurs règles d'accès.

Membres

L'onglet affiche tous les utilisateurs appartenant au groupe. Seuls les utilisateurs ou cartes de visiteur appartenant à la même entreprise que le groupe peuvent être ajoutés au groupe.

Règles d'accès

Il affiche un aperçu de toutes les règles d'accès déjà créées et propose de les modifier ou de les créer. En créant une règle d'accès, un groupe spécifique est autorisé à accéder à la zone. Lors de la création d'une règle, vous devez saisir un groupe et un profil horaire dans lequel le groupe doit avoir accès à la zone.

Zones

Les zones sont utilisées pour faciliter la gestion de l'accès aux appareils individuels. Les zones combinent les appareils en unités logiques. Une liste de toutes les zones s'affiche sur la page.

La liste peut être filtrée en utilisant au-dessus de la liste. Alternativement, des filtres peuvent être définis pour des colonnes individuelles dans le menu étendu qui s'ouvre en cliquant sur dans l'en-tête de chaque colonne. Menu étendu de colonnes il permet également de déplacer les colonnes, de les épingler à la première ou à la dernière position ou de les masquer.

Activation des points d'accès

Aide une boîte de dialogue s'ouvrira dans laquelle la prise en charge du point d'accès est démarrée, plus v Paramètres du point d'accès de l'appareil (p. 80).

Créer une nouvelle zone

1. Aller à la page **Zones**.
2. Cliquez sur le bouton pour ajouter une zone dans le coin supérieur droit.
3. Dans la boîte de dialogue ouverte, vous devez saisir le nom de la zone et sélectionner les entreprises auxquelles elle appartient.
   La zone nouvellement créée apparaît dans la liste. Des appareils peuvent être ajoutés à une zone dans le détail de la zone ou dans le détail des appareils. Des réglages supplémentaires peuvent être effectués dans le détail de la zone.

Paramètres des zones

Les informations de zone peuvent être visualisées et modifiées dans les détails de la zone. Les détails de la zone sont ouverts en cliquant sur la zone sélectionnée dans la liste.

Authentification multifacteur

Il est possible de paramétrer la nécessité de l'authentification de plusieurs manières pour tous les appareils de la zone. Il est possible de sélectionner uniquement certaines méthodes d'authentification, mais l'ordre suivant doit être strictement respecté lors de leur utilisation :

1. My2N app
2. Carte RFID
3. Empreinte digitale
4. Code PIN

ATTENTION
Avec l'authentification multifacteur, il est nécessaire de suivre l'ordre des méthodes d'authentification.

Le besoin d'une authentification multifacteur peut être limité par un profil temporel. Lorsque l'authentification multifacteur est activée, une option apparaîtra **Utiliser l'authentification multifacteur**, dans lequel vous

pouvez utiliser sélectionnez un profil horaire. Lorsque vous choisissez le mode « Anytime », une authentification multifacteur sera requise à tout moment.

L'authentification multifacteur ne peut être requise que pour entrer dans la zone. Ce paramètre n'est valide que lors de l'utilisation de points d'accès.

Accéder aux paramètres

Dans la carte, il est possible de paramétrer un code PIN collectif pour accéder à la zone ou de l'afficher si un code PIN a déjà été créé.

De plus, les fonctions suivantes peuvent être activées et désactivées dans les paramètres d'accès :

Alarme silencieuse – lors de l'utilisation d'un code spécial, une action silencieuse est activée qui envoie un message d'alarme ; l'appareil n'émet pas de sons d'alarme pendant une alarme silencieuse. Le réglage du code spécial pour l'alarme silencieuse et sa fonction exacte se fait dans la configuration de l'appareil.

Bloquer l'accès – après cinq tentatives infructueuses, la prochaine tentative d'accès ne sera autorisée qu'après 30 secondes.

Vérification de la plaque d'immatriculation – les véhicules auront accès à la zone sur la base de la vérification des plaques d’immatriculation sur tous les appareils prenant en charge cette fonction.

Appareil

L'onglet affiche un aperçu des appareils ajoutés à la zone donnée. Des appareils supplémentaires peuvent être ajoutés dans cet onglet.

Si des points d'accès sont utilisés, des points d'accès individuels sont ajoutés à la zone. Le type de point d'accès de l'appareil donné est décrit comme Entrée de zone.

Les méthodes d'authentification disponibles sont affichées pour chaque appareil/point d'accès.

Groupes de serrures

L'onglet présente une vue d'ensemble du groupe de fermeture. Vous pouvez ajouter un autre groupe dans cet onglet.

Pour chaque groupe de fermeture, vous pouvez consulter les détails du groupe.

Entreprises

La carte gère à quelles entreprises appartient la zone donnée. Une zone peut appartenir à plusieurs entreprises.

Règles d'accès

Il affiche un aperçu de toutes les règles d'accès déjà créées et propose de les modifier ou de les créer. En créant une règle d'accès, un groupe spécifique est autorisé à accéder à la zone. Lors de la création d'une règle, vous devez saisir un groupe et un profil horaire dans lequel le groupe doit avoir accès à la zone.

La modification d'une règle d'accès peut être effectuée en cliquant sur la règle donnée.

Appareil

La page Appareils affiche tous les appareils ajoutés à cette page. **Access Commander**.

La liste peut être filtrée en utilisant au-dessus de la liste. Alternativement, des filtres peuvent être définis pour des colonnes individuelles dans le menu étendu qui s'ouvre en cliquant sur dans l'en-tête de chaque colonne. Menu étendu de colonnes il permet également de déplacer les colonnes, de les épingler à la première ou à la dernière position ou de les masquer.

Les enregistrements peuvent être téléchargés dans un fichier CSV en cliquant sur le bouton Export au-dessus de la liste. Dans le fichier CSV exporté, l'heure est indiquée en GMT+0.

En taguant, il est possible de sélectionner plusieurs appareils et de leur appliquer les actions groupées suivantes :

- Gérer les appareils sélectionnés
- Supprimer les appareils sélectionnés de la gestion
- Sauvegarder les appareils sélectionnés

L'icône sur la barre de l'appareil redirige vers l'interface de configuration web de cet appareil.

États de l'appareil

- En ligne
- Non géré
- Incompatible
- Non configuré : vous devez télécharger la configuration des serrures électroniques à partir d'un programme tiers.
- Hors ligne
  - Échec de la connexion – Des informations d'identification incorrectes ont été saisies dans **Access Commanderu** pour la configuration en ligne des appareils.
  - Inaccessible – **Access Commander** ne peut pas établir de connexion avec l'appareil.
  - Certificat invalide – la validation du certificat SSL est requise et l'appareil ne dispose pas d'un certificat SSL valide.

Ajout d'un nouveau dispositif IP

NOTE
L'ajout de serrures électroniques 2N Fortis est décrit sur le site Serrures électroniques (p. 23).

1. Aller à la page **Appareil**.
2. Cliquez sur le bouton Ajouter un appareil dans le coin supérieur droit.
3. Pour ajouter un interphone 2N, une unité d'accès 2N ou une unité de réponse 2N, sélectionnez « 2N IP devices ».

4. Dans la boîte de dialogue qui s'ouvre, localisez l'appareil sur votre réseau local ou saisissez son adresse IP et son port sous le format suivant : « IPaddress:port ».
   Après avoir saisi l'adresse IP de l'appareil, il est possible d'appuyer sur ENTER sur le clavier pour saisir un autre appareil.
5. Après avoir renseigné tous les appareils que vous souhaitez ajouter, remplissez le mot de passe pour accéder à la configuration web de ces appareils. Il est possible d'ajouter uniquement les appareils auxquels vous vous connectez simultanément avec le même mot de passe.
6. Demande de modèle (facultatif) : Pour appliquer un modèle à l'appareil que vous ajoutez, activez le commutateur. **Après avoir ajouté l'appareil, utilisez le modèle de configuration**.
   - Le principe de sélection et d'application d'une configuration à partir d'un modèle est le même que celui de l'application manuelle d'un modèle à un appareil existant, comme indiqué à l'adresse Modèles d'appareils (p. 71).
7. Nommez l'appareil avant de le créer.
8. Les appareils nouvellement ajoutés apparaissent dans la liste. Effectuez d'autres réglages de l'appareil dans les détails de l'appareil.

Groupes de serrures

Les groupes de fermeture vous permettent de regrouper des fermetures individuelles en unités logiques qui peuvent ensuite être utilisées pour définir des règles d'accès, surveiller ou gérer des dispositifs.

Voir les groupes

Ouvrez **Devices > Lock Groups**.

NOTE
La liste présente tous les groupes de fermeture créés. Utilisez le champ de recherche pour filtrer les enregistrements par nom.

Créer un nouveau groupe de fermeture

1. Ouvrez **Devices > Lock Groups**.
2. Cliquez sur + Groupe Serrures.
3. Saisissez un nom de groupe et sélectionnez l'onglet Créer.
4. Dans le module **Serrures** cliquez sur Ajouter des serrures. Sélectionnez les serrures qui feront partie du groupe.
5. Dans le module **Zones** cliquez sur Ajouter des zones. Sélectionnez les zones qui doivent faire partie du groupe.
6. Sélectionnez ⋮ pour ajouter, renommer ou supprimer un groupe de fermeture.

AVERTISSEMENT
La modification de l'attribution du verrou à un groupe différent nécessite une reconfiguration. Assurez-vous que toutes les modifications du système sont terminées avant d'exporter le fichier de configuration.

Mise en place de verrous dans Access Commander

Avant de télécharger des clés sur des serrures individuelles, vous devez coupler **Access Commander** avec **Fortis Commander**.

Génération de la clé de chiffrement principale (MEK) et préparation du projet

1. Connectez-vous à Access Commander.
2. Allez sur **Settings > Electronic locks**.
3. Dans l'onglet **Initial Settings** cliquez sur Generate Keys.
4. Créer la clé de chiffrement principale.

ATTENTION
La clé de cryptage principale ne peut pas être consultée ou modifiée ultérieurement .

NOTE
En fonction de la clé de chiffrement principale (MEK), **2N Access Commander** génère un ensemble de clés de chiffrement. La clé doit donc être unique et suffisamment sûre. Le jeu de clés est basé sur la clé de chiffrement principale, de sorte que les projets ayant la même clé de chiffrement principale génèrent les mêmes jeux de clés. Si un projet est perdu, un nouveau projet avec la même clé de chiffrement principale peut être créé et poursuivre le chiffrement.

5. Après avoir généré les clés et défini le mot de passe pour le fichier de projet, vous pouvez télécharger **le fichier de projet**, qui est une image de la configuration de la serrure électronique dans le système **Access Commander**.
6. Dans l'onglet **de Fortis Commander** cliquez sur Télécharger l'application**,** à partir duquel le téléchargement de **Fortis Commander** (application pour la configuration des serrures électroniques) commencera.

ATTENTION
Les informations sur le projet sont des données sensibles. Protégez-les contre les abus.

Configuration de la serrure électronique à l'aide de Fortis Commander

1. Installez **Fortis Commander** et ouvrez-le.
2. Cliquez sur Open project et ouvrez le fichier de projet téléchargé dans l'explorateur de fichiers.
3. Dans la boîte de dialogue qui s'affiche, saisissez le mot de passe du fichier de projet.
4. Après avoir ouvert le fichier de projet, sélectionnez Connect to device et attachez la carte de service à la serrure.
5. Cliquez sur **Assign**, qui attribue le verrou au projet.
6. Déconnectez l'appareil et cliquez sur **File > Close project**.
7. Lorsque la configuration est terminée, ouvrez le système **Access Commander**. Allez dans l'onglet **Settings > Electronic Locks** et cliquez à nouveau sur Fortis Commander. Téléchargez le fichier de projet.

NOTE
Lorsque vous déplacez la serrure d'une installation à l'autre ou lorsque vous faites une réclamation, vous devez effectuer une réinitialisation d'usine . Cette opération réinitialise la serrure aux paramètres d'usine et supprime toute configuration antérieure.

Procédure de mise à jour de la configuration

1. Apportez des modifications à **Access Commander**.
2. Téléchargez le nouveau fichier de projet.
3. Téléchargez le fichier sur **Fortis Commander** et apportez les modifications nécessaires aux serrures.
4. Si vous apportez d'autres modifications à **Access Commander**u, téléchargez toujours un nouveau fichier de projet.

ATTENTION
Pour chaque changement de configuration dans **Access Commander**u, vous devez télécharger un nouveau fichier de projet - vous ne pouvez pas utiliser un ancien fichier qui a déjà été téléchargé sur **Fortis Commander**.

Verrouillage et déverrouillage permanents

L'application vous permet de verrouiller et de déverrouiller la serrure en permanence. Cette fonction est utilisée pour les interventions de service ou les commandes d'urgence sans l'utilisation d'une carte.

Verrouillage d'urgence

Le verrouillage d'urgence est utilisé pour verrouiller complètement la porte contrôlée par le dispositif donné. Lors du verrouillage d'urgence, il n'est pas possible d'ouvrir la porte avec les accès utilisateur définis, même si l'utilisateur ou le visiteur utilise un accès valide avec un profil horaire valide.

Le verrouillage d'urgence peut être activé/désactivé :

- dans les détails de l'appareil – verrouille l'appareil donné ;
- dans les détails de la zone – verrouille tous les appareils de la zone ;
- dans les détails de l'entreprise - verrouille tous les appareils de l'entreprise ;
- en utilisant l'action globale dans la barre supérieure en appuyant sur le bouton – verrouille tous les appareils **Access Commander**;
- dans le widget du tableau de bord.

Dans le widget Emergency Lock, il est possible de prédéfinir un groupe spécifique d'appareils qui pourront être verrouillés en cas d'urgence.

ATTENTION
Les appareils hors ligne, les appareils inactifs, les appareils avec un micrologiciel incompatible et les appareils dont le micrologiciel est antérieur à 2.32 ne seront pas verrouillés après une demande de verrouillage d'urgence. L'appareil hors ligne sera verrouillé dès qu'il sera à nouveau disponible.

Réglages de l'appareil

Les informations sur l'appareil peuvent être consultées et gérées dans les détails de l'appareil. Les détails de l'appareil sont ouverts en cliquant sur l'élément de périphérique sélectionné dans leur liste. Selon le type d'appareil, les détails peuvent être divisés en onglets Présentation, Appel et Ascenseur.

Depuis les détails de l'appareil, vous pouvez accéder à la configuration web de l'appareil à l'aide du bouton **Configuration matérielle** dans la partie supérieure droite du détail de l'appareil. La configuration des

différents appareils est décrite dans le manuel de configuration correspondant. Il est possible de revenir depuis l'interface web de configuration en fermant la configuration par une croix dans la barre supérieure bleue.

Aperçu

État

Cet onglet affiche l'état de l'établissement des connexions avec les appareils. Les appareils en ligne sont ceux avec lesquels il a **Access Commander** connexions établies et sur lesquelles le firmware accepté est téléchargé. Grâce à la connexion établie avec l'appareil, la synchronisation des données peut avoir lieu. Un microprogramme incompatible peut être activé **Page de l'appareil > Micrologiciel**.

La synchronisation automatique est déclenchée après chaque modification pour être reflétée dans la configuration des appareils finaux. La synchronisation n'a lieu que sur les appareils concernés. Seules les demandes déclenchées par des modifications susceptibles d'affecter les appareils finaux sont mises en file d'attente pour la synchronisation. Ces modifications concernent généralement les droits d'accès, les numéros de téléphone, les profils horaires utilisés, etc. Par exemple, la modification du nom d'un utilisateur qui n'est affecté à aucun groupe ne déclenchera pas la synchronisation automatique. La durée de la synchronisation elle-même (projection de toutes les modifications sur les appareils finaux) dépend du nombre d'appareils à synchroniser, ainsi que de la quantité de données téléchargées sur l'appareil.

Contrôle d'accès

Définit la zone à laquelle appartient l'appareil.

Si deux points d'accès sont définis pour l'appareil et si la détection des points d'accès est activée (voir Paramètres du point d'accès de l'appareil (p. 80)), l'option permettant d'attribuer deux zones s'affiche. Un point d'accès de l'appareil ne peut se trouver que dans une seule zone.

Configuration

La carte affiche la version actuelle du firmware, l'adresse MAC et l'adresse IP et permet de changer le mot de passe pour accéder à sa configuration Web.

Dans l'onglet, vous pouvez modifier l'adresse IP où se trouve l'appareil, ce qui permet à **Access Commander** de pointer vers un appareil qui a été déconnecté et reconnecté au réseau à une adresse IP différente.

Contrôle de porte

Cette carte affiche les images des caméras de l'appareil et permet l'ouverture à distance de l'interrupteur de porte contrôlé par l'appareil. L'ouverture de la porte pendant un certain temps peut être réglée dans le menu étendu qui s'ouvre en cliquant sur ⋮ .

L'état actuel de l'interrupteur de porte est affiché à côté du bouton Ouvrir.

Il est utilisé pour verrouiller les portes même pour les groupes ayant un accès valide Verrouillage d'urgence (p. 64).

Sauvegarde

Cet onglet permet de sauvegarder la configuration de l'interphone dans un fichier XML. La sauvegarde est démarrée avec Lancer une sauvegarde. Lorsqu'une sauvegarde est enregistrée dans le stockage local, elle est stockée dans une mémoire délimitée **Access Commander**. Lorsqu'elle est sauvegardée dans un fichier, une boîte de dialogue s'ouvre dans laquelle le fichier de sauvegarde peut être crypté à l'aide d'un mot de passe. Le fichier contient des informations sensibles, il est donc recommandé de le protéger. Le cryptage des sauvegardes est disponible pour les appareils dotés d'un micrologiciel 2.45 ou supérieur. . Lors de l'enregistrement dans un fichier, une boîte de dialogue s'ouvre dans laquelle vous pouvez chiffrer le fichier de sauvegarde à l'aide d'un mot de passe. Le fichier contient des informations sensibles, il est donc recommandé de le protéger. Le chiffrement des sauvegardes est disponible sur les appareils dotés du firmware 2.45 ou supérieur

Chaque dernière sauvegarde sera affichée dans l'onglet. Il est possible de synchroniser automatiquement l'appareil avec la dernière sauvegarde à l'aide du menu de Réinitialiser. Dans le menu déroulant de ce menu, vous pouvez également choisir de restaurer à partir d'une sauvegarde d'un autre appareil connecté ou d'un fichier externe

NOTE
Tous les appareils disponibles (appareils en ligne et appareils connectés avec un micrologiciel incompatible) peuvent être sauvegardés.

Appel

carte d'appel s'affiche si une connexion de télécommunication est disponible et activée sur l'appareil. L'onglet affiche tous les comptes activés qui sécurisent la connexion et affiche leur statut. La connexion de télécommunication est établie directement dans l'interface de configuration de l'appareil concerné, dans la section Appels. L'interface de configuration est accessible via un bouton Configuration matérielle dans l'en-tête détaillé de l'appareil.

Appel

Cet onglet est affiché dans le détail de l'appareil à partir duquel les appels peuvent être passés.

Affichage du répertoire téléphonique

L'onglet Contacts gère l'affichage du carnet d'adresses sur les appareils dotés d'un écran. La carte affiche l'arborescence des contacts telle qu'elle apparaît dans le carnet d'adresses de l'appareil. En cliquant sur Modifier une boîte de dialogue permettant d'éditer l'arborescence des contacts s'ouvrira. Dans la partie gauche de la boîte de dialogue ouverte, le tri des dossiers de contacts est affiché. Dans la partie droite, les contacts du dossier sélectionné sont définis. Le dossier racine est la première page qui apparaît lorsque vous ouvrez le répertoire sur votre appareil. Les contacts apparaîtront tous sur une seule page du carnet d'adresses s'ils sont tous stockés dans ce dossier racine. Les contacts peuvent être regroupés en dossiers et triés sous le dossier racine.

Ajouter des contacts à l'écran de l'appareil

1. Allez dans **Appareil > Détails de l'appareil > Onglet Appels > Onglet Contacts**.
2. Ouvrez la gestion de l'affichage en cliquant sur Modifier.
3. Dans la partie droite de la boîte de dialogue ouverte, sélectionnez le dossier auquel vous souhaitez ajouter des contacts.
   Vous pouvez ajouter au dossier :

   1. **Utilisateurs**
      Il est possible de sélectionner plusieurs utilisateurs en même temps.
   2. **Groupes**
      Les utilisateurs peuvent être ajoutés au dossier en masse par groupe. Chaque utilisateur du groupe sera affiché sous son nom dans l'annuaire. Il est possible de sélectionner plusieurs groupes en même temps.
   3. **Groupes d'appel**
      Les groupes d'appels sont des groupes de contacts qui seront appelés en même temps. Lors de la création d'un groupe d'appels, il est nécessaire de saisir son nom, sous lequel le groupe d'appels sera affiché dans le carnet d'adresses. Les contacts utilisateur sont ajoutés à un groupe d'appels tout comme les contacts sont ajoutés aux dossiers.
      Vous pouvez renommer le groupe d'appels dans le menu étendu à côté du dossier que vous ouvrez en cliquant sur ⋮.

4. Vous pouvez renommer le dossier dans le menu avancé du dossier, que vous ouvrez en cliquant sur . Dans le menu étendu, il est possible d'ajouter une image au dossier donné, qui sera ensuite affichée sur l'appareil pour ce dossier.
5. Épinglez les dossiers ou groupes d'appels que vous souhaitez voir apparaître en premier dans le menu étendu pour le dossier donné en utilisant .

Autres numéros virtuels

Sur un appareil doté d'un pavé numérique, il est possible de lancer un appel sortant en saisissant un numéro virtuel. Dans cet onglet, il est possible d'ajouter des utilisateurs qui pourront appeler des numéros virtuels, même si ces utilisateurs n'ont pas accès à l'appareil. Les appels vers des numéros virtuels d'utilisateurs ayant accès à l'appareil sont automatiquement autorisés.

Lors de la sélection des utilisateurs, seuls les utilisateurs disposant d'un numéro virtuel renseigné sont affichés.

Boutons

Cet onglet est affiché dans le détail des appareils dotés de boutons permettant de composer les numéros de téléphone des utilisateurs. Dans l'onglet Boutons, les utilisateurs individuels sont affectés à des boutons individuels sur l'appareil. Appuyer sur un bouton de l'appareil lance un appel sortant vers la destination de l'utilisateur attribué. L'utilisateur est affecté au bouton en cliquant sur et sélectionner l'utilisateur.

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).

Paramètres de contrôle d'ascenseur

1. Avant d'effectuer la configuration dans **Access Commander**, assurez-vous que le module relais AXIS A9188 est connecté au dispositif 2N qui fournira l'autorisation d'accès à l'étage. Assurez-vous également que le protocole HTTPS est configuré sur le module et que le mot de passe racine a été modifié.
2. Accédez aux détails de l'appareil censé contrôler l'accès aux différents étages. Dans le menu étendu dans l'en-tête, activez la commande de l'ascenseur. Un onglet apparaîtra dans les détails de l'appareil **Ascenseur**.
3. Dans l'en-tête des détails de l'appareil, naviguez vers hardware configuration device. Naviguez jusqu'à **Integration > Access Control > Elevator tab**. Activez tous les modules relais qui doivent contrôler l'accès à l'ascenseur. Si les modules nécessitent une authentification, entrez le nom d'utilisateur et le mot de passe. Enregistrez les paramètres. Quittez la configuration du matériel à l'aide de la croix située dans la barre bleue supérieure.
4. Accédez à l'onglet Ascenseur dans les détails de l'appareil.
5. Dans l'onglet Étage d'ascenseur, sélectionnez la sortie relais pour l'étage auquel vous souhaitez définir l'accès. L'étiquetage des sorties est au format : *sortie io_module_relay*. Cliquer sur .

6. Dans la boîte de dialogue ouverte, nommez l'étage et sélectionnez la zone entrée à cet étage. Seuls les utilisateurs autorisés à entrer dans la zone donnée selon les règles d'accès définies seront autorisés à accéder à cet étage. Si l'entrée à l'étage ne doit pas être régie par le règlement de la zone, cochez la case **accès public autorisé**. En sélectionnant un profil horaire, vous limitez l'accès public uniquement à l'heure définie par le profil horaire sélectionné. En dehors de ce profil horaire, l'entrée ne sera à nouveau autorisée qu'aux utilisateurs disposant d'un accès valide basé sur les règles d'accès.

ATTENTION
Si l'accès est paramétré selon les règles d'accès de la zone, le dispositif d'ascenseur ne reprend aucun autre paramétrage de cette zone (code PIN, authentification multiple, alarme silencieuse, ...).

Sol
Une fois activé, cet onglet affiche une liste de tous les étages configurables. Chaque étage a sa propre désignation dans l'ordre des modules et des sorties relais. Chaque étage peut alors se voir attribuer son propre nom.

Modules
Cet onglet affiche tous les modules AXIS A9188 connectés et leurs états actuels.

Surveillance
La page sert à obtenir des informations sur les appareils IP connectés (interphones, unités d'accès, unités de réponse). Chaque administrateur peut configurer le tableau selon ses propres besoins à l'aide de . La configuration est unique pour chaque compte. La configuration se fait en sélectionnant les colonnes à afficher.

Cliquez sur la ligne pour accéder au détail de l'appareil donné.

Micrologiciel
La page Firmware assure une mise à niveau massive du firmware de différents types d'appareils connectés et contribue ainsi à les maintenir dans un état optimal. La gestion groupée des appareils peut être suspendue. En option, certains appareils peuvent être exclus de la gestion groupée du micrologiciel.

ASTUCE
La nouvelle version du firmware peut d'abord être déployée sur un ou plusieurs appareils sélectionnés en mode test et permettre ensuite seulement la mise à niveau d'autres appareils.

La version actuelle du micrologiciel est disponible en ligne via le serveur de mise à jour 2N. En option, il est également possible de télécharger le fichier de mise à niveau manuellement. Le déploiement d'une nouvelle version est toujours soumis à l'approbation de l'administrateur, qui a ainsi le contrôle total sur le processus de mise à niveau.

L'obtention des versions du micrologiciel à partir de 2N update serveur peut prendre quelques minutes.

La version de gestion de masse affiche une liste des types d'interphones 2N, des unités de réponse 2N et des unités d'accès 2N connectées.

Exclusion de périphérique

Les appareils peuvent être exclus de la gestion groupée du micrologiciel en les ajoutant au v **Périphériques > Micrologiciel > onglet Périphériques exclus**.

Versions incompatibles du firmware

Lorsque vous ajoutez ou mettez à niveau un appareil qui ne dispose pas d'un micrologiciel compatible, cet appareil entre dans un état incompatible. Un état incompatible signifie que les nouveaux utilisateurs ne sont pas stockés sur l'appareil. De plus, les événements sont téléchargés depuis l'appareil et il est possible d'utiliser la configuration ou la sauvegarde de l'appareil. Une nouvelle entrée est créée dans le tableau et l'administrateur a la possibilité d'autoriser l'utilisation d'un firmware incompatible.

Access Commander désactive automatiquement les appareils dont le micrologiciel n'est pas pris en charge par sa version actuelle. L'onglet affiche ces versions de micrologiciel non prises en charge sur les appareils connectés. La liste des versions de firmware prises en charge est indiquée ci-dessous.

Access Commander peut contrôler tous les appareils fonctionnant avec une version de micrologiciel non prise en charge si cette version est approuvée. L'approbation se fait sous l'onglet **Appareils > Firmware > Versions de firmware incompatiblesZařízení > Firmware > karta Nekompatibilní verze firmwaru** à l'aide de l'icône .

ATTENTION
L'approbation d'une version non prise en charge peut entraîner des problèmes tels qu'une perte de données ou empêcher le bon fonctionnement.

Versions du firmware prises en charge

- 3.0
- 2.50
- 2.49
- 2.48
- 2.47
- 2.46
- 2.45

Sécurité

La méthode de sécurisation de la communication entre Access Commander et les appareils est définie dans **Appareils > Sécurité > Onglet Vérification du certificat de l'appareil**.

Commander d'accès permet trois niveaux de sécurité des communications avec les appareils :

1. **Communication cryptée sans authentification par certificat** - **Access Commander** utilise un certificat auto-signé pour la communication HTTPS. Ce certificat est considéré comme non fiable par les navigateurs web.
2. **Vérification de l'empreinte du certificat** – la communication est assurée en vérifiant le certificat enregistré sur l'appareil. Lors de la communication, l'empreinte de ce certificat est vérifiée
   Lorsque l'authentification par empreinte digitale est activée, l'administrateur de l'appareil doit confirmer la validité de l'empreinte du certificat lors de l'ajout d'un nouvel appareil. L'administrateur de l'appareil sera invité à vérifier l'empreinte digitale même si le certificat d'un appareil déjà ajouté est modifié
3. **Vérification complète du certificat** - la communication est sécurisée par un certificat signé par une autorité de certification. Pendant la communication, l'ensemble de la chaîne de certification est vérifié conformément aux exigences de l'ICP.

ATTENTION
Télécharger vos propres certificats SSL sur le dispositif 2N Indoor Touch n'est pas possible ; une fois l'authentification activée, la connexion aux certificats sera perdue.

Comment gérer les certificats

La méthode de sécurisation de la communication entre Access Commander et les appareils est définie dans **Appareils > Sécurité > Onglet Vérification du certificat de l'appareil**.

Lorsque l'authentification par certificat SSL est activée, la synchronisation s'effectue uniquement sur les appareils dotés d'un certificat SSL avec une autorité de confiance signée. La synchronisation des appareils dépourvus de tels certificats SSL sera désactivée. Les appareils passeront en mode hors ligne

Le certificat de l'autorité de signature doit être fiable sur le serveur sur lequel **2N Access Commander** fonctionne.

ASTUCE
Le processus de téléchargement des certificats sur le serveur est décrit dans FAQ.

Pour une authentification réussie, les certificats de l'appareil doivent être signés par l'autorité de certification et inclure l'adresse IP ou le nom de domaine de l'appareil.

Télécharger un certificat d'appareil

1. Entrez la configuration Web de l'appareil.
2. Allez sur **Système > Certificats > onglet Certificats d'utilisateur**.
3. Téléchargez le certificat préparé.
4. Allez sur **System > Network Connection > Web server tab**.
5. Dans le paramètre **HTTPS Server Certificate**, sélectionnez le certificat que vous avez téléchargé.
6. Enregistrez les modifications.

Paramètres du point d'accès de l'appareil

Vous pouvez logiquement diviser chaque appareil en deux points d'accès - l'arrivée et le départ. Chaque point d'accès représente un passage dans une direction et détermine si l'utilisateur de l'appareil entre ou sort de la zone. Un point d'accès peut être contrôlé par un ou plusieurs modules de l'appareil. Tous les modules affectés gèrent alors les passages dans la direction du point d'accès spécifique. Les points d'accès sont surtout utilisés lorsqu'un appareil se trouve à la limite de deux zones et que la direction du mouvement entre ces deux zones doit être enregistrée avec précision (par exemple, pour les fonctions anti-passback).

Les points d'accès sont également utilisés pour suivre les utilisateurs dans le module Présence (p. 84). Les points d'accès sont également utilisés pour surveiller les entrées et les sorties Restrictions de zone (p. 86).

NOTE
Dans l'interface de configuration web de chaque appareil, les points d'accès sont appelés **Arrivée** et **Départ**. Pour les configurer, accédez à **Accès > Règles d'accès > sélectionnez l'onglet « Accès et sortie »**.

Activation des points d'accès dans Access Commander

1. Accédez à la page Zones v **Access Commander**.
2. Dans le coin supérieur droit, appuyez sur ⚙ et permettre l'utilisation de points d'accès.

Activation des points d'accès dans Access Commander

1. Entrez la configuration Web de l'appareil.

> **ASTUCE**
>
> L'interface de configuration Web est accessible en cliquant ⚙ sur la liste de la page Appareils.

2. Accédez à la **section Matériel > Menu Modules d'extension**.
3. Accédez à la page Zones v **Access Commander**.
4. Une boîte de dialogue s'ouvre avec une liste des modules de gestion d'accès disponibles.
5. Dans le coin supérieur droit, appuyez sur ⚙ et permettre l'utilisation de points d'accès.

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

Modèles d'appareils

La fonction Modèles de dispositifs vous permet de configurer plusieurs dispositifs. Les modèles simplifient l'installation initiale du système et unifient les paramètres d'un projet à l'autre.

Les modèles fonctionnent selon le principe de la structure. Les modèles vous permettent d'enregistrer la configuration complète de n'importe quel appareil avec **2N OS** ou seulement des parties sélectionnées de la configuration et de l'appliquer ensuite à d'autres appareils. La configuration peut être basée sur un appareil déjà configuré, une sauvegarde de l'appareil ou un modèle précédemment exporté.

Lors de la création d'un modèle, vous pouvez choisir les parties de la configuration à inclure. Les différentes parties diffèrent selon le type d'appareil (par exemple, réglages de relais, sorties audio, automatisation). Cette sélection fait partie du processus de création du modèle et ne peut être modifiée une fois le modèle enregistré.

> **NOTE**
>
> L'utilisation de modèles peut réduire considérablement le temps nécessaire à la mise en service initiale.

Création et gestion de modèles

Pour accéder à la fonctionnalité des modèles, allez dans Appareils > Modèles.

1. Cliquez sur + Créer un modèle à partir de.
2. Le dialogue **Créer un modèle** s'ouvre.
3. Dans le menu déroulant **Dispositifs***, sélectionnez un dispositif existant qui servira de dispositif de base pour votre modèle. Seuls les appareils compatibles avec les modèles seront affichés.

4. Cliquez sur Suivant pour continuer à configurer le modèle.

ATTENTION
Certaines configurations peuvent afficher des avertissements. Ils indiquent que les configurations sélectionnées peuvent présenter des limites ou des risques potentiels. La sélection est toujours activée, mais il est recommandé de vérifier la notification.

Importer un modèle ou une sauvegarde à partir d'un fichier

Si vous disposez déjà d'un modèle ou d'une sauvegarde d'appareil enregistré dans un fichier, vous pouvez facilement l'importer :

1. Allez dans Dispositifs > Gabarits.
2. Cliquez sur Importation sur fichier en haut à droite.
3. Sélectionnez le modèle ou le fichier de sauvegarde sur votre ordinateur et cliquez sur Importer.

NOTE
Lors de l'importation, certaines sections peuvent apparaître désactivées. Il s'agit de parties de la configuration qui pourraient entraîner des changements indésirables ou interférer avec le fonctionnement de l'appareil. Ces sections sont automatiquement supprimées lors de l'importation et l'utilisateur peut les voir brièvement lors du chargement.

Modifier le modèle

Le modèle peut être modifié après sa création. L'interface n'affiche que les parties de la configuration qui ont été incluses lors de la création du modèle.

1. Allez dans Appareils > Modèles.
2. Sélectionnez un modèle dans la liste.
3. Cliquez sur Modifier le modèle.

Une boîte de dialogue contenant les sections de configuration s'affiche.

Ajustement des valeurs

- La valeur est ajustée en double-cliquant.
- L'élément modifié est immédiatement marqué comme modifié.
- L'icône d'avertissement ⚠ indique les valeurs qui peuvent ne pas passer la validation complète sur l'appareil.

ATTENTION
La validation effectuée lors de l'édition d'un modèle n'est qu'indicative et se fait **au niveau de l'article**. Cette vérification ne permet pas de détecter tous les conflits entre les appareils et les versions de microprogrammes et ne correspond pas à la validation complète qui a lieu à l'adresse **2N OS**.

Un article marqué d'un avertissement peut encore être utilisé sur l'appareil, et un article sans avertissement peut être rejeté lors de la demande. L'évaluation proprement dite a lieu sur l'appareil.

Application d'un modèle à un appareil

Le modèle peut être appliqué à un ou plusieurs appareils. Il peut également être appliqué à l'aide d'actions groupées dans la liste des appareils ou directement à partir des détails de l'appareil.

1. Allez dans Dispositifs > Gabarits.
2. Sélectionnez le modèle que vous souhaitez appliquer à l'appareil.
3. Cliquez sur Appliquer à l'appareil.
4. Sélectionnez l'appareil et confirmez.
5. L'aperçu de la configuration s'affiche. Ces sections correspondent aux sélections effectuées lors de la création du modèle, mais peuvent être modifiées.
6. Cliquez sur Appliquer.

ATTENTION

Si, lors de l'application du modèle, un message d'avertissement est détecté entre la version du micrologiciel ou le type d'appareil pour lequel le modèle a été créé et la version ou le type de l'appareil cible, un message d'avertissement s'affiche. L'anomalie doit être confirmée avant de poursuivre.

NOTE

- Le statut ne fait que confirmer le démarrage réussi du processus. Il n'informe pas de l'état d'avancement ou de l'achèvement de la demande.
- Pour savoir comment utiliser le modèle lors de l'ajout d'un appareil, voir Ajouter un nouvel appareil (p. 61).

Règles d'accès

Les règles d'accès sont un outil permettant de gérer clairement l'accès des groupes d'utilisateurs aux zones. L'accès peut être accordé en fonction de profils horaires.

Les règles d'accès déterminent QUI a accès, OÙ et QUAND.

- **OMS** est déterminé par le groupe et les utilisateurs qui lui sont affectés (un utilisateur peut appartenir simultanément à plusieurs groupes appartenant à une même entreprise).
- **OÙ** est déterminé par la zone ou les appareils (un appareil ne peut se trouver que dans une seule zone à la fois).
- **QUAND**est déterminé par le profil horaire attribué. Cet élément est facultatif. Un profil horaire non renseigné signifie un accès illimité (24h/24 et 7j/7).

NOTE
Un groupe peut avoir accès à plusieurs zones, et plusieurs groupes peuvent avoir accès à une seule zone.

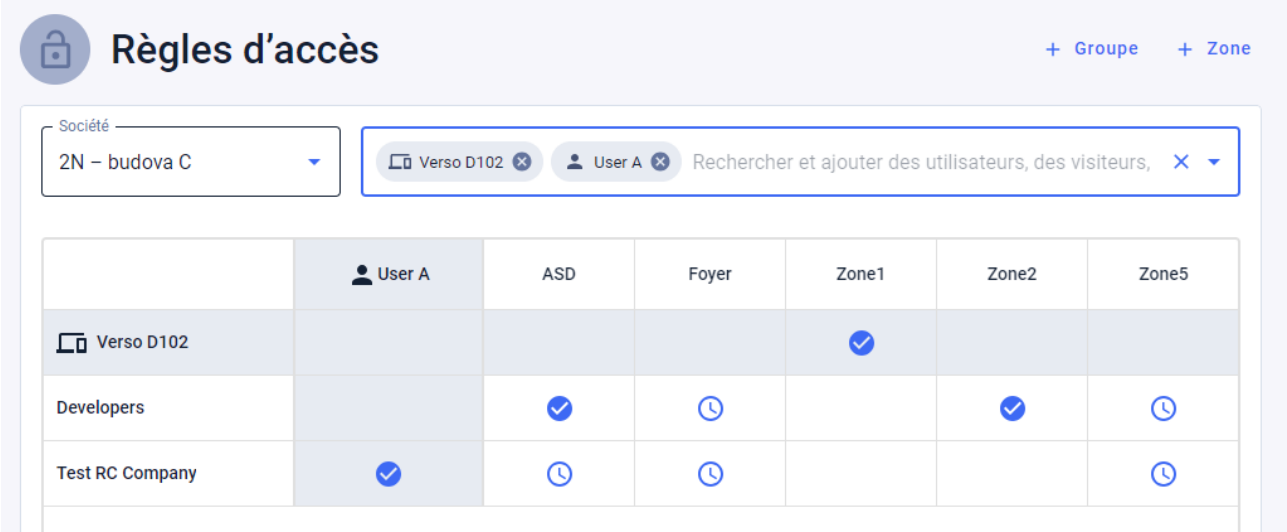
Affichage matriciel

La vue matricielle des règles sur la page des règles d'accès affiche un aperçu des accès et permet de les paramétrer. La matrice est disponible pour chaque entreprise existante et montre tous les groupes et zones qui lui sont attribués. L'administrateur peut changer de société dans le menu au-dessus de la matrice.

Un clic sur la cellule correspondant à la zone et au groupe sélectionnés permet de paramétrer l'accès du groupe à la zone. Un menu apparaîtra dans lequel vous pourrez choisir soit un accès illimité, soit un accès limité par un profil horaire. Les profils horaires doivent être prédéfinis sur la page Profils horaires (p. 76). Si nécessaire, un nouveau groupe ou zone peut être ajouté à la matrice de l'entreprise.

Dans le champ de recherche au-dessus de la matrice, il est possible d'ajouter des utilisateurs ou des appareils à la matrice. Les utilisateurs peuvent être ajoutés à un groupe via l'intersection de l'utilisateur et du groupe. En croisant un appareil et une zone, les appareils sont ajoutés à la zone.

Un exemple de représentation matricielle



L'image donne un aperçu de la matrice de la société 2N Telekomunikace as. Il ressort clairement de l'aperçu que :

- L'appareil filtré Verso 2.0 D102 fait partie de Zone1.
- L'utilisateur filtré Utilisateur A fait partie du groupe Test RC Company.
- Les utilisateurs du groupe Développeurs ont un accès illimité aux zones ASD et Zone2, un accès limité aux zones Foyer et Zone5 (selon le profil horaire défini) et n'ont pas accès à la zone Zone1.
- Les utilisateurs du groupe Test RC Company ont un accès limité aux zones ASD, Foyer et Zone5 (selon le profil horaire défini) et n'ont pas accès aux zones Zone1 et Zone2.

Liste des règles

La page Liste des règles affiche une liste de toutes les règles d'accès actuellement valides. Cliquez sur la règle pour la modifier. Une nouvelle règle d'accès peut être ajoutée en cliquant sur le bouton Ajouter dans le coin supérieur droit. Avant de créer, vous devez définir les paramètres de la règle.

La liste de règles et la matrice affichent les mêmes règles d'accès. Une modification dans une vue est automatiquement copiée dans l'autre vue. Les règles d'accès sont également ajustées dans les paramètres de zone et les paramètres de groupe.

Profils horaires

Les fonctions d'interphone sélectionnées peuvent être limitées dans le temps. Les fonctions mentionnées peuvent se voir attribuer ce que l'on appelle un profil horaire, qui détermine quand la fonction donnée est disponible.

Les profils horaires peuvent répondre aux exigences suivantes :

- bloquer complètement les appels vers l'utilisateur sélectionné en dehors du temps réservé
- bloquer les appels vers les numéros de téléphone sélectionnés de l'utilisateur en dehors du temps réservé
- bloquer l'accès des utilisateurs en dehors du temps imparti

Chaque profil horaire définit la disponibilité de la fonction à laquelle il est associé à l'aide d'un calendrier hebdomadaire. Vous pouvez facilement régler l'heure de-à et éventuellement jours de la semaine où la fonctionnalité devrait être disponible. La détermination de l'accès à l'aide du profil horaire est définie par les règles d'accès. La limitation de disponibilité de l'utilisateur en dehors du profil horaire est paramétrée en fonction du numéro de téléphone de l'utilisateur.

En option, il est possible de créer jusqu'à 20 profils horaires généraux qui, outre le contrôle d'accès, peuvent également être utilisés pour des cas particuliers de configuration locale. Ces profils horaires sont téléchargés sur tous les appareils synchronisés.

Profils temporels sur les serrures électroniques

Les serrures électroniques prennent en charge des profils horaires avec les restrictions suivantes :

- Les vacances ne s'appliquent pas.
- Dans le cadre d'une journée, il est possible de définir jusqu'à 4 intervalles de temps différents.
- Dans le cadre d'un profil horaire, il est possible de définir 4 emplois du temps quotidiens.

ASTUCE
Cela signifie que vous pouvez avoir par exemple des réglages différents pour le lundi, le mardi, le mercredi et le jeudi, mais pour le vendredi, le samedi et le dimanche, vous devez utiliser l'un des réglages existants.

ATTENTION
Si le profil horaire enfreint les restrictions énoncées, la règle d'accès sera ignorée et l'utilisateur ne se verra pas accorder l'accès.

Création d'un profil horaire

1. Allez sur **Profils temporels**.
2. Cliquez sur `+ Time Profile` dans le coin supérieur droit.
3. Dans la boîte de dialogue ouverte, définissez le nom du profil horaire.

4. Sélectionnez Add time slots pour sélectionner une restriction horaire. Les jours surlignés en bleu sont ceux qui entrent dans le cadre du profil horaire. Pour sélectionner un jour, cliquez dessus. Vous pouvez définir un intervalle de temps entre les jours pour déterminer la validité du profil horaire.

> **NOTE**
> Vous pouvez définir un intervalle de temps en jours pour déterminer la validité du profil temporel.

> **ATTENTION**
> Il est possible de définir des heures différentes pour chaque jour après la création du profil horaire.

5. Le profil horaire nouvellement créé est ajouté à la liste et ses détails s'ouvrent, dans lesquels d'autres réglages peuvent être effectués. Dans le détail du profil horaire, il est possible de paramétrer la position du profil sur les appareils.

> **NOTE**
> Les profils globaux peuvent affecter l'accès dans toutes les entreprises. Seul l'administrateur peut les modifier.
>
> Un administrateur des accès ne peut corriger que les profils horaires de son entreprise.

Définition du profil horaire

Le détail des jours et des heures est affiché dans le détail du profil horaire. Les intervalles bleus indiquent quand le profil est actif. N'importe quel nombre d'intervalles peut être défini dans une journée.

L'intervalle est ajouté en cliquant sur le créneau horaire et en définissant l'heure exacte à laquelle le profil doit être actif. L'heure d'un intervalle individuel peut être modifiée en cliquant sur l'intervalle. Si le profil doit être actif toute la journée, un intervalle couvrant toute la journée doit être créé, c'est-à-dire 00h00-23h59.

Dans le menu étendu qui s'ouvre en cliquant sur ⋮ la position sur l'appareil peut être réglée. La position sur l'appareil définit la position dans la liste des profils horaires qui est téléchargée sur tous les appareils auxquels le profil horaire est attribué.

La limitation de la disponibilité de l'utilisateur en dehors du profil horaire est définie avec le numéro de téléphone dans les paramètres de l'utilisateur.

Présence

Access Commander permet de surveiller la présence des utilisateurs. En mode présence, les heures d'entrée et de sortie des utilisateurs individuels sont enregistrées.

Le paramétrage de la présence et des modes de présence s'effectue dans **Réglages > Configuration > onglet Présence**, voir Paramètres de présence (p. 79).

ATTENTION
Pour le bon fonctionnement de la fréquentation, il est nécessaire d'avoir **Access Commander**licence active disponible pour suivre la présence des utilisateurs. Le suivi des présences doit être activé dans les paramètres de chaque utilisateur.

La page de présence propose une liste d'utilisateurs avec une participation suivie. Il y a une icône dans le coin supérieur droit , avec lequel il est possible de télécharger un fichier CSV avec des données récapitulatives sur la présence de tous les utilisateurs. Lors du téléchargement des données, vous devez saisir la période pour laquelle la fréquentation doit être générée.

Présence d'un utilisateur spécifique

Vous pouvez sélectionner un utilisateur spécifique dans la liste des utilisateurs sur la page Présence et afficher des informations plus détaillées uniquement sur sa présence. La liste affiche uniquement les utilisateurs pour lesquels le suivi des présences est activé, voir Utilisateurs (p. 49).

Dans la partie supérieure du relevé, vous pouvez sélectionner le mois pour lequel vous souhaitez afficher la fréquentation. À côté de la sélection du mois, le fonds de travail défini pour le mois donné, le solde et les heures travaillées sont affichés.

Il y a un menu d'extension à côté du nom de l'utilisateur permettant le téléchargement des données sur la présence de l'utilisateur affiché dans un fichier CSV ou PDF. Les deux fichiers contiennent des enregistrements de jours individuels.

ASTUCE
Il est également possible de visualiser la présence de l'utilisateur dans les détails de l'utilisateur, accessible en le sélectionnant dans la liste des utilisateurs sur la page. **Utilisateurs**.

Modifier la participation des utilisateurs

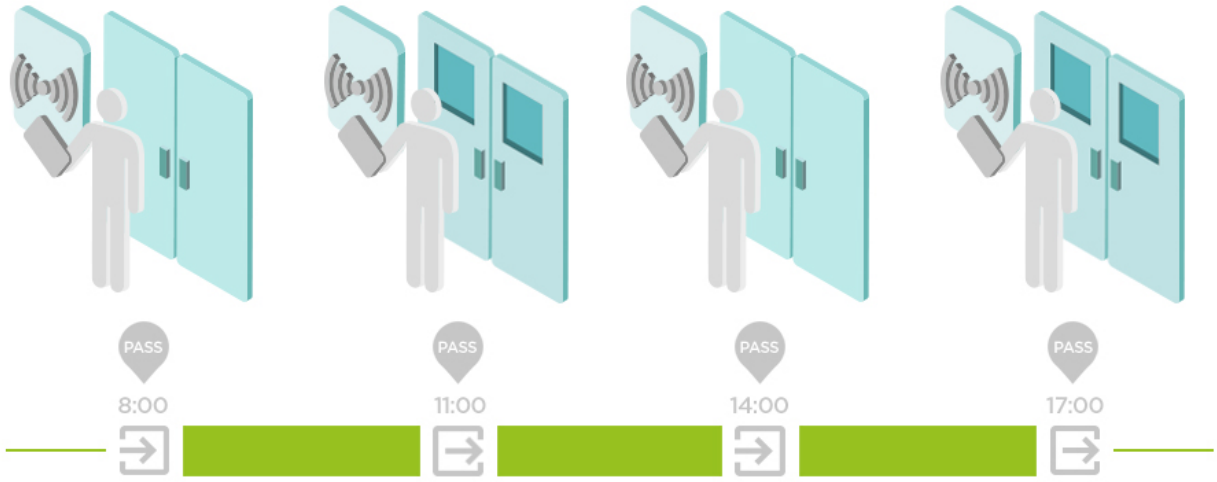
Le gestionnaire de présence peut modifier les données de présence des utilisateurs. L'édition se fait en cliquant sur l'intervalle de temps à modifier. Une fois ouvertes, les heures limites peuvent être modifiées et une note peut être ajoutée à l'intervalle.

Paramètres de présence

Access Commander permet de surveiller la présence des utilisateurs. En mode présence, les heures d'entrée et de sortie des utilisateurs individuels sont enregistrées.

Modes de présence

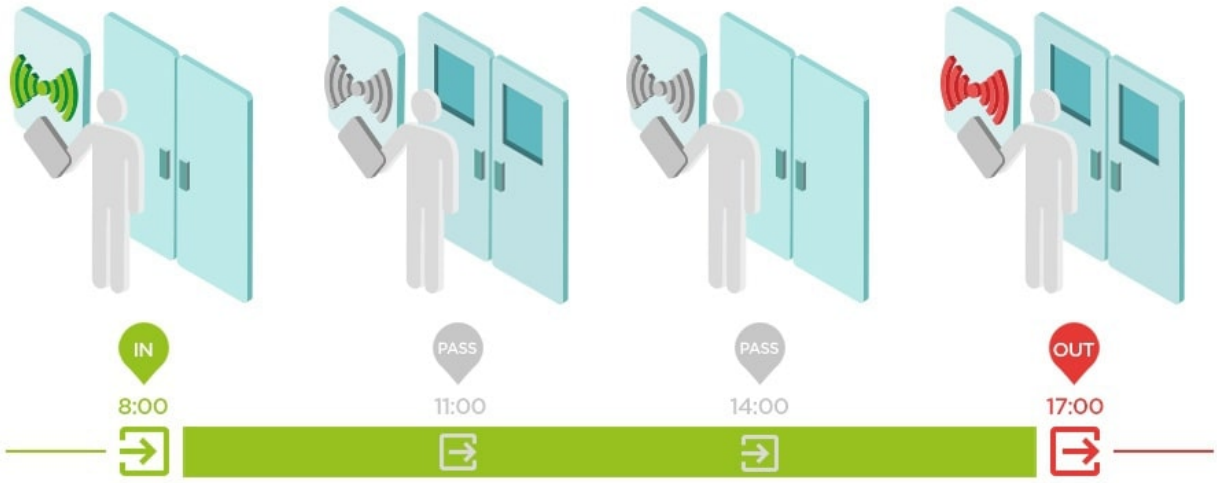
- **FREE**



Les arrivées et les départs sont comptés à partir de la première et de la dernière authentification de l'utilisateur sur n'importe quel appareil au cours d'une journée. Le module de présence ne fonctionne pas dans ce mode.

- **IN-OUT**

Pour fonctionner correctement, l'appareil doit être configuré pour entrer et sortir de la zone.



- **IN-OUT pour tous les appareils**
  Ce mode permet la surveillance de présence. Les arrivées sont enregistrées sur les appareils entrants, les départs sont enregistrés sur les appareils sortants. Les mouvements entre zones ne sont pas enregistrés comme arrivée/départ.
- **IN-OUT pour les appareils sélectionnés**
  Ce mode permet la surveillance de présence. Les arrivées et les départs sont enregistrés sur des appareils sélectionnés qui sont définis comme arrivées ou départs. Les arrivées et départs sont enregistrés uniquement sur ces appareils sélectionnés. L'enregistrement des arrivées/départs peut ainsi être réglé, par exemple, uniquement à l'entrée principale du bâtiment.

Paramètres du point d'accès de l'appareil

Vous pouvez logiquement diviser chaque appareil en deux points d'accès - l'arrivée et le départ. Chaque point d'accès représente un passage dans une direction et détermine si l'utilisateur de l'appareil entre ou sort de la zone. Un point d'accès peut être contrôlé par un ou plusieurs modules de l'appareil. Tous les modules affectés gèrent alors les passages dans la direction du point d'accès spécifique. Les points d'accès sont surtout utilisés lorsqu'un appareil se trouve à la limite de deux zones et que la direction du mouvement entre ces deux zones doit être enregistrée avec précision (par exemple, pour les fonctions anti-passback).

Les points d'accès sont également utilisés pour suivre les utilisateurs dans le module Présence (p. 84). Les points d'accès sont également utilisés pour surveiller les entrées et les sorties Restrictions de zone (p. 86).

NOTE
Dans l'interface de configuration web de chaque appareil, les points d'accès sont appelés **Arrivée** et **Départ**. Pour les configurer, accédez à **Accès > Règles d'accès > sélectionnez l'onglet « Accès et sortie »**.

Activation des points d'accès dans Access Commander

1. Accédez à la page Zones v **Access Commander**.
2. Dans le coin supérieur droit, appuyez sur et permettre l'utilisation de points d'accès.

Activation des points d'accès dans Access Commander

1. Entrez la configuration Web de l'appareil.

ASTUCE
L'interface de configuration Web est accessible en cliquant sur la liste de la page Appareils.

2. Accédez à la **section Matériel > Menu Modules d'extension**.
3. Accédez à la page Zones v **Access Commander**.
4. Une boîte de dialogue s'ouvre avec une liste des modules de gestion d'accès disponibles.
5. Dans le coin supérieur droit, appuyez sur et permettre l'utilisation de points d'accès.

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

Visites

Dans **Access Commander**il est possible de créer des profils de visiteurs bénéficiant de privilèges d'accès pour une durée limitée. Lors de la visite, il est possible d'ajouter une carte d'accès, un code d'accès et de renseigner la plaque d'immatriculation du véhicule. La présence ne sera pas prise en compte pour la visite. Le nombre de visites n'est limité par aucune licence.

Paramétrage de la conservation des données des visiteurs

L'administrateur peut définir la durée de conservation des données des visiteurs. La durée de conservation des données visiteurs est paramétrée en jours en cliquant sur l'icône à côté du bouton pour créer une nouvelle visite.

Après l'expiration de l'intervalle de temps de visite et de la période de conservation des données définie, les visites sont automatiquement supprimées tous les minuit. Les visites pour lesquelles des cartes de visiteur sont encore attribuées ne seront pas supprimées.

NOTE
Les paramètres peuvent être utilisés pour se conformer aux réglementations locales en matière de protection des données. Le nom et la note de la visite seront conservés dans le journal d'accès selon les paramètres de durée de vie dans la gestion des journaux.

Créer une nouvelle visite

1. Aller à la page **Visites**.
2. Cliquez sur le bouton Ajouter une visite dans le coin supérieur droit.
3. Dans la fenêtre de dialogue qui s'ouvre, vous devez renseigner le nom de la visite, sélectionner le groupe visité et définir le début et la fin de la visite. Si vous ne définissez pas le début et la fin de la visite, l'intervalle de temps d'accès à la visite débutera immédiatement et se terminera en fin de journée.

   ATTENTION
   L'intervalle de temps d'accès aux visites ne doit pas dépasser 90 jours.

4. Avant de créer une visite, vous pouvez définir les méthodes d'authentification que la visite utilisera pour les accès.
   La visite nouvellement créée apparaît dans la liste. Dans le détail de la visite, il est possible d'ajouter des méthodes d'authentification à la visite et de gérer son accès.

Fin de visite

Après l'intervalle de temps, l'accès expirera pour la visite.

Si l'administrateur ou l'administrateur termine la visite en utilisant le bouton Fin dans l'onglet Accès dans les paramètres de la visite, l'accès à cette visite sera immédiatement bloqué. Un bouton Stop est disponible pour un visiteur dont la visite a été automatiquement interrompue car le fuseau horaire peut être différent sur les appareils. Il peut arriver que même si un visiteur ne dispose pas d'un accès valide sur un appareil, il en a quand même sur un autre. Cela se produit si différents fuseaux horaires sont définis pour l'appareil.

Si une carte de visiteur a été attribuée à une visite, la carte sera déliée et pourra être utilisée pour une autre visite.

Visiter les paramètres

Les informations sur la visite peuvent être consultées et modifiées dans les détails de la visite. Les détails de la visite s'ouvrent en cliquant sur la visite sélectionnée dans la liste.

Approches

L'onglet Accès affiche le groupe d'accès et l'intervalle de temps pendant lequel la visite a un accès valide. L'intervalle de temps d'accès à la visite peut être redéfini en choisissant Réinitialiser la visite dans le menu étendu ⋮ .

Dans cet onglet, il est possible de terminer la visite, voir Fin de visite (p. 81).

Visite

La carte montre la personne visitée et l'entreprise visitée. Il est possible de changer de personne visitée.

Dans cet onglet, il est possible d'ajouter une note à la visite.

Données personnelles

La fiche affiche les coordonnées de la visite et permet de les modifier. L'e-mail paramétré permet l'envoi de codes d'authentification.

Authentification

Lors de la visite, il est possible d'ajouter une carte d'accès, un code PIN ou QR d'accès et de renseigner la plaque d'immatriculation du véhicule. Il est possible de renseigner une seule plaque d'immatriculation par visite. Il est possible d'attribuer une carte d'accès visiteur à la visite, voir Cartes (p. 82).

Lors du remplissage de l'adresse e-mail, il est possible d'envoyer le code PIN/QR d'accès généré à l'adresse indiquée.

La carte de visiteur attribuée peut être restituée ici.

Journal d'accès

Le journal d'accès affiche l'historique des accès.

Cartes

La page Cartes permet de gérer les cartes d'accès des visiteurs qui sont disponibles pour ajouter une visite. Une nouvelle carte est ajoutée à l'aide du bouton d'ajout situé dans le coin supérieur droit.

Les cartes doivent toujours être attribuées à une entreprise. La carte ne peut être utilisée que pour les visites qui visiteront cette entreprise.

Une carte existante peut être écrasée ou supprimée en la sélectionnant dans le menu étendu ⋮ .

ATTENTION
Une carte affectée à une visite active ne peut pas être supprimée.

NOTE
Si **Access Commander** signale que la toute nouvelle carte qui vient d'être ajoutée est déjà utilisée dans le système, la raison peut être que le mode de compatibilité des cartes RFID est activé. Ce mode est activé par l'administrateur dans **l'onglet Paramètres > Authentification > Mode de compatibilité**.

Gérer une carte sécurisée avec un lecteur USB

Le lecteur USB peut être utilisé pour diagnostiquer et gérer la carte sécurisée dans le champ de recherche de l'en-tête.

ASTUCE
Avant d'utiliser le lecteur USB, vous devez l'activer dans **Access Commander**. Pour plus d'informations, voir Lecteurs USB activés (p. 109).

1. Connectez le lecteur USB à votre ordinateur.
2. Cliquez sur l'icône dans le champ de recherche situé dans l'en-tête.
3. Attachez le lecteur.

Opérations disponibles

- Récupération des données de la carte
- Recherche d'un utilisateur par carte
- Pour afficher les événements stockés sur l'onglet
- Mise à jour des données d'accès
- Suppression ou formatage d'une application
- Extension de la carte de service

Présence

Le module **Presence** vous permet de surveiller l'activité des utilisateurs en temps réel. Il fonctionne indépendamment du module **Attendance**, qui fait l'objet d'une licence distincte. Les présences peuvent être contrôlées même sans licence de présence active.

Les deux fonctions sont affichées ensemble sur les onglets **Attendance et presence** dans l'interface d'Access Commander, mais chacune a sa propre raison d'être et fonctionne indépendamment.

Pour que le module fonctionne, vous devez définir le mode de présence IN-OUT dans **Settings > Configuration > Attendance tab**, voir Paramètres de présence (p. 79).

- Si le dernier événement de l'utilisateur un jour donné est une arrivée (**IN** événement), est considéré comme présent.
- Si un utilisateur passe par un lecteur qui est réglé sur une direction non spécifiée, la zone de l'utilisateur changera. La même chose se produit s'il traverse un lecteur en mode **IN**.
- Si le dernier événement de l'utilisateur pour un jour donné est une déconnexion (**OUT** événement), il est considéré comme absent.

ATTENTION
Le module de présence ne fonctionne pas si le mode FREE est utilisé dans le système de suivi des présences. Seuls les paramètres IN-OUT peuvent être utilisés.

Expiration de la présence de l'utilisateur

Cliquez sur l'icône en haut à droite, l'expiration de la présence de l'utilisateur est définie. L'expiration de la présence de l'utilisateur entraîne la suppression automatique de l'enregistrement de présence de l'utilisateur si l'utilisateur oublie de marquer son départ. Ce délai est exprimé en heures et détermine combien de temps après le dernier passage de l'utilisateur actuel, son enregistrement de présence sera automatiquement supprimé. La définition de cette limite de temps vous permet de définir combien de temps un enregistrement de présence peut rester dans le système si l'utilisateur n'est pas marqué comme absent. Cela garantit que la liste des utilisateurs présents reste à jour et ne contient pas d'enregistrements d'utilisateurs qui ont déjà quitté le bâtiment et ont oublié de se déconnecter.

Rapports

Il est possible de télécharger des données récapitulatives sur les utilisateurs ajoutés à partir de la page Rapports. Les fichiers téléchargés sont au format CSV (Comma-Separated Values). Le nom du fichier indique toujours la date et l'heure auxquelles le rapport a été généré.

NOTE
Certains tableurs utilisent des séparateurs différents et le fichier CSV peut ne pas s'afficher correctement lorsqu'il est ouvert dans ceux-ci. Dans de tels cas, il est recommandé d'importer les données du fichier CSV dans un classeur ouvert.

- **My2N app** – Utilisateurs couplés et non couplés avec temps de couplage restant
  Le rapport répertorie les données sur l'état du couplage des utilisateurs via l'application My2N app, ou des données sur la période de validité du code d'appairage actif.
- **Utilisateurs** – Règles d'accès avec groupes, zones, appareils et profils horaires
  Le rapport répertorie les données sur l'affectation des utilisateurs à des groupes, leur accès aux zones et aux appareils dans les zones, ainsi que les profils horaires auxquels les utilisateurs sont autorisés à accéder. Chaque combinaison est répertoriée sur exactement une ligne du tableau.
- **Utilisateurs** – Export détaillé
  Le rapport répertorie toutes les informations sur les utilisateurs renseignées dans leur profil, y compris leurs données personnelles et d'accès.

  ATTENTION
  Le fichier contient des données sensibles !
- **Utilisateurs** – Export de synchronisation globale
  Le rapport répertorie les données sur l'affectation des utilisateurs à des groupes, leur accès aux zones et aux appareils dans les zones, ainsi que les profils horaires auxquels les utilisateurs sont autorisés à accéder. Chaque combinaison est répertoriée sur exactement une ligne du tableau.
  Ce rapport peut servir de fichier CSV pour la synchronisation des utilisateurs, voir Synchronisation des utilisateurs avec FTP (p. 94).

  ATTENTION
  Le fichier contient des données sensibles !

Restrictions de zone

Utilisez des restrictions de zone pour définir les zones dans lesquelles les fonctions Occupation et Anti-Passback peuvent être utilisées.

NOTE
Le module Restrictions de zone et le module Présence (y compris la présence) sont indépendants l'un de l'autre. L'occupation et l'anti-passback ne peuvent pas être utilisés pour les modules Présence et Présence. L'occupation et l'anti-passback ne fonctionnent que dans le modèle de restrictions de zone

Définition de restrictions de zone

Un nouvel appareil est ajouté à la zone à l'aide du bouton dans l'en-tête des détails de la zone.

Entrée et sortie

Ces cartes indiquent quels appareils sont répertoriés comme entrée ou sortie dans la zone. Vous pouvez utiliser le menu avancé sous ⋮ pour déplacer des dispositifs entre les onglets ou les supprimer d'une zone.

En authentifiant l'utilisateur sur le dispositif d'entrée, l'entrée dans la zone est enregistrée. En authentifiant l'utilisateur sur le dispositif de sortie, l'utilisateur quitte la zone. Il est ainsi possible de contrôler si l'utilisateur se trouve toujours dans la zone et s'il souhaite y entrer à nouveau.

Si l'appareil ajouté dispose de deux points d'accès définis, chaque point peut être utilisé pour une direction différente (Entrée/Sortie). Les paramètres du point d'accès sont décrits dans le chapitre Paramètres du point d'accès de l'appareil (p. 80). Les propriétés du point d'accès sont développées en cliquant sur la flèche.

Occupation

Pour fonctionner correctement, l'appareil doit être configuré pour entrer et sortir de la zone.

L'onglet d'occupation donne un aperçu du nombre de personnes présentes dans la zone et vous permet de définir des limites d'occupation. Si la limite d'occupation est atteinte, il est possible de refuser les entrées supplémentaires ou de ne les enregistrer que dans le journal du système. La fonction d'occupation ne permet pas de savoir quelles personnes se trouvent dans la zone. Un module de présence distinct est conçu pour surveiller la présence de personnes individuelles

ATTENTION
Lors de l'autorisation répétée d'un utilisateur, chaque autorisation compte pour une entrée. Cela signifie que si un utilisateur est connecté trois fois consécutivement sur le dispositif d'entrée, il sera compté comme trois personnes dans la zone. Par conséquent, si l'installation physique du dispositif permet la récupération répétée d'une seule carte d'utilisateur, il est conseillé de combiner la fonction d'occupation avec la fonction anti-passback.

Anti-retour

Pour fonctionner correctement, l'appareil doit être configuré pour entrer et sortir de la zone.

Il est possible d'activer la fonction anti-passback sur la zone, qui assure l'extension du contrôle d'accès en surveillant et en empêchant la non-utilisation des droits pour entrer à nouveau dans les zones réservées. Les champs sous surveillance sont définis par les appareils frontières qui permettent d'y accéder ou de les quitter. Ces appareils contrôlent l'autorisation lors du passage des personnes selon les règles définies pour un champ en particulier. Après avoir quitté la zone en passant par un dispositif de délimitation, l'utilisateur ne peut y retourner qu'après un certain temps, si un délai a été fixé. Si l'utilisateur tente de revenir dans la zone plus tôt, le système lui refuse l'accès ou enregistre simplement l'événement.

AVERTISSEMENT

- La zone anti-passback n'a plus de sens et devient potentiellement dangereuse s'il existe dans cette zone un dispositif auquel est connecté un bouton REX actif permettant un accès non autorisé.

Définir une exception

Il est parfois souhaitable que les conditions d'anti-passback ne s'appliquent pas à certains utilisateurs. Il s'agit généralement d'utilisateurs tels que le gestionnaire du bâtiment, le PDG, les utilisateurs VIP, etc. Les utilisateurs ou les groupes entiers qui ne doivent pas être soumis aux conditions d'anti-passback sont définis dans **Paramètres > Anti-passback > Exceptions**.

NOTE

La section Paramètres n'est disponible que pour les utilisateurs disposant du rôle d'administrateur.

Liste des utilisateurs bloqués

Les utilisateurs bloqués sont ceux qui ont tenté d'accéder à la zone anti-passback avant l'expiration du délai.

En utilisant ✕, les utilisateurs peuvent être exclus de la liste et autorisés à accéder à nouveau à la zone.

ASTUCE

Lorsqu'un utilisateur se voit refuser l'accès en raison d'un anti-passback actif, un courriel d'information automatisé peut lui être envoyé. Pour activer l'envoi de ce courriel, allez dans **Paramètres > Anti-passback > Onglet Notification** par courriel de l'utilisateur bloqué.

Réinitialisation des restrictions

L'onglet **Paramètres > Anti-passback > Réinitialiser les restrictions de zone** définit les jours et les heures auxquels l'enregistrement de la zone sera effacé, c'est-à-dire que tous les utilisateurs pourront à nouveau passer sans tenir compte des violations antérieures des règles.

Ces mesures améliorent le niveau de protection et préviennent les menaces potentielles pour la sécurité. Plus précisément, ils aident à empêcher tout accès non autorisé à des emplacements sélectionnés, permettent de suivre les mouvements des personnes dans un espace donné et d'enregistrer les entrées et les sorties, ce qui peut être utile pour surveiller et analyser les événements de sécurité.

La liste montre les zones créées dans le système. Sur cet onglet, des zones peuvent être créées, supprimées et accéder à leurs détails. Il permet par la même occasion de désactiver la zone et d'afficher son statut.

Créer une zone de restriction

1. Aller à la page **Restrictions de zone**.
2. Cliquez sur le bouton pour ajouter une région dans le coin supérieur droit.
3. Dans la boîte de dialogue ouverte, nommez la zone.
4. Dans le détail de la zone ouverte, ajoutez un appareil à la zone. Les appareils sont ajoutés à l'aide du bouton dans l'en-tête des détails de la zone.
   La zone nouvellement créée apparaîtra dans la liste. Dans ses détails, il est possible de configurer les dispositifs d'entrée et de sortie, de définir l'occupation autorisée, d'activer la fonction anti-passback et de bloquer l'accès à la zone pour les utilisateurs sélectionnés.

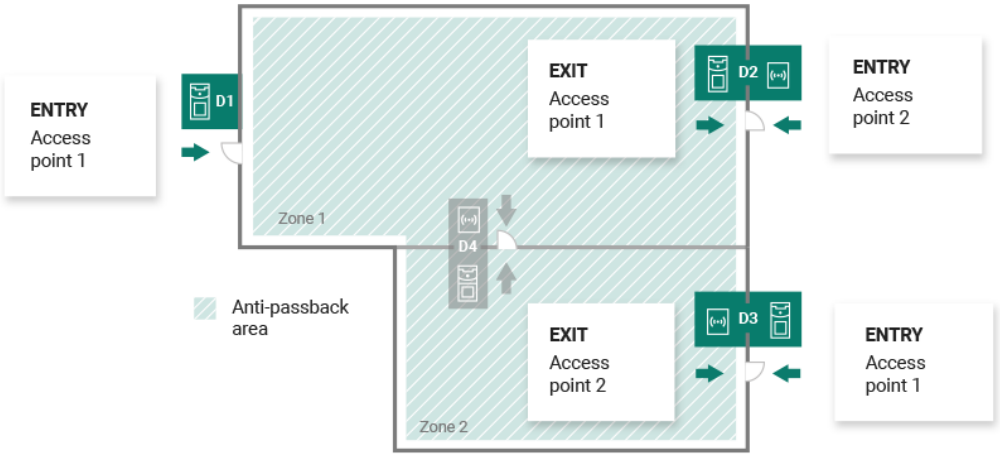
Les erreurs de configuration les plus courantes

ATTENTION
Si une erreur se produit dans une zone, la zone entière sera désactivée. Il sera réactivé une fois les erreurs supprimées.

Les cas suivants peuvent empêcher les restrictions régionales de fonctionner correctement

- Aucun appareil n'est ajouté à la zone. Au moins un appareil doit être attribué.
- Certains périphériques d'entrée/sortie ne sont pas configurés correctement ou ne contiennent pas de lecteur.
- Un dispositif d'entrée dans cette zone est déjà utilisé comme entrée dans une autre zone. L'affectation doit être modifiée pour un fonctionnement correct.
- Certains équipements ne sont pas équipés de la licence nécessaire.
- Certains appareils ont été désactivés.
- Un appareil a été déconnecté.
- Certains appareils ne disposent pas d'une version de micrologiciel compatible.
  Certains appareils sont équipés d'un bouton REX qui permet de quitter la zone APB sans autorisation de l'utilisateur. Pour un fonctionnement correct, le bouton REX doit être désactivé.

Un exemple de définition de restrictions



La figure montre une zone Anti-passback avec trois dispositifs de bordure D1, D2 et D3. Seuls les appareils frontaliers sont utilisés pour définir la fonction Anti-passback. Le dispositif D4 à l'intérieur de la zone Anti-passback n'est pas utilisé pour contrôler l'entrée/sortie de la zone. Les appareils D2 et D3 ont des directions d'entrée et de sortie définies.

Appareil D1 il est uniquement utilisé pour entrer dans la zone Anti-passback. L'appareil est défini comme entrée.

Appareil D2 sert à la fois à l'entrée et à la sortie. L'appareil dispose d'un module d'extension configuré pour entrer dans la zone et d'une unité principale configurée pour sortir.

Appareil D3 sert à la fois à l'entrée et à la sortie. L'appareil dispose d'une unité principale configurée pour entrer dans la zone et d'un module d'extension configuré pour sortir.

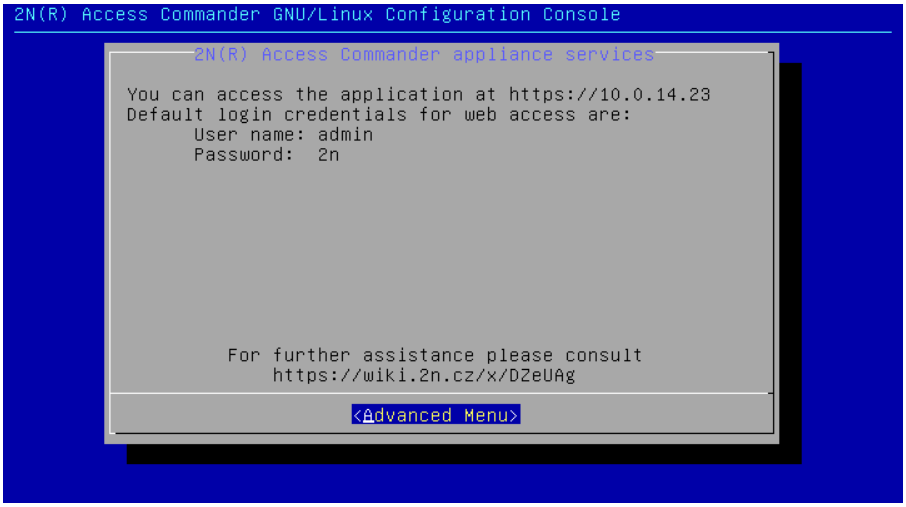
Les paramètres du système

Paramètres Linux

Les paramètres système de base peuvent être définis dans la console de configuration Linux.

NOTE
Si **Access Commander** est distribué via une machine virtuelle, il est possible de se connecter à la version Linux à distance via une connexion SSH.

La console de configuration s'ouvre en vous connectant à **Access Commander** en utilisant le compte root. La page d'accueil affiche des informations de base sur l'accès administrateur à l'interface Web et redirige vers le menu avancé.



Dans le Menu Avancé, il est possible de définir :

- **La mise en réseau**
  Paramètres du serveur proxy, propriétés réseau, options de synchronisation avec le serveur DHCP.
- **Tim**
  Réglage manuel de l'heure, paramètres du serveur NTP et du fuseau horaire

- **SSH**
  Établit une connexion à distance avec **Access Commander** via SSH. Pour activer SSH, un mot de passe autre que celui par défaut doit être défini et qui répond aux exigences de sa difficulté.
- **PME**
  Démarre l'assistant de configuration des connexions aux dossiers partagés. Définit l'adresse IP ou le nom de domaine et le chemin du dossier. Par exemple. "192.168.1.1/partage". Pour les paramètres, il est nécessaire de préciser le nom d'utilisateur de l'utilisateur qui aura accès au dossier donné et le droit d'écriture. Il faut renseigner le mot de passe de l'utilisateur et sélectionner la version du protocole Samba. Après avoir terminé toutes les étapes obligatoires, la connexion au serveur sera vérifiée et des informations s'afficheront indiquant si la configuration a réussi ou échoué.
- **Mot de passe**
  Il permet de changer le mot de passe de l'utilisateur root du système pour se connecter à la console ou y accéder via SSH.

  NOTE
  La modification du mot de passe root se fait dans la console de configuration, pas dans Access Commander.

- **Sauvegarde et restauration**
  Utilisé pour importer des données et une configuration, définir des sauvegardes répétées, restaurer à partir de sauvegardes antérieures.

Mise à jour du système

Système **Access Commander** vérifie régulièrement le serveur de mise à jour et informe des mises à jour disponibles et des nouvelles versions de firmware disponibles des appareils connectés. DANS **Paramètres > Onglet Mise à jour du système** la vérification automatique des mises à jour peut être désactivée.

Installez la mise à jour Access Commander

AVERTISSEMENT
Il est recommandé de le faire avant d'installer la mise à jour sauvegarde du système (p. 92). Effectuez la sauvegarde en dehors des heures de bureau pour éviter une indisponibilité temporaire du système pour les utilisateurs.

1. Aller à **Paramètres > Onglet Mise à jour du système**.
2. Si la vérification automatique des mises à jour est désactivée, cliquez sur Vérifier les mises à jour.
3. Cliquer sur Télécharger dans le message d'information sur la mise à jour disponible et confirmez le téléchargement.
   L'onglet informe que la mise à jour est prête à être installée.
4. Cliquer sur Installer dans le message d'information et dans la boîte de dialogue ouverte, confirmez l'installation.
   Après avoir démarré l'installation, vous serez redirigé vers la page de maintenance. La page de maintenance informe l'administrateur qui a démarré l'installation de l'état en cours de l'installation. Affiche des informations aux autres utilisateurs indiquant qu'une mise à jour est en cours. Lors de l'installation, il n'est pas possible de**Access Commander**s'inscrire.
5. Une fois l'installation terminée, cliquez sur Allez vous connecter, qui vous redirigera vers la page de connexion.

Domaines requis pour les mises à jour du système

ATTENTION
Pour que la mise à jour du système soit réussie, il est essentiel de connecter le 2N Access Commander aux serveurs énumérés ci-dessous. Si l'accès à ces domaines n'est pas autorisé, le processus de mise à jour échouera et le système ne sera pas mis à jour.

Cet accès est essentiel pour télécharger les dernières versions des applications, les paquets système, les correctifs de sécurité et d'autres composants qui maintiennent votre système dans un état optimal et sécurisé.

- .2n.cz
- .2n.com
- .deb.nodesource.com
- .packages.microsoft.com
- .security.debian.org
- .apt.postgresql.org
- .httpredir.debian.org

Downgrade
Il n'est pas possible de revenir à une version antérieure du micrologiciel.

Tests bêta
Les utilisateurs peuvent choisir de participer aux tests bêta des mises à jour logicielles **Access Commander** avant la sortie officielle des mises à jour. L'autorisation s'effectue en **Paramètres > onglet Mise à jour du système > paramètre du serveur de mise à jour**.

AVERTISSEMENT
La version d'essai n'est pas garantie et la société ne la fournit pas 2N TELEKOMUNIKACE a.s. n'est pas responsable des limitations fonctionnelles et des dommages possibles résultant des limitations fonctionnelles de la version bêta. Les versions bêta sont fournies uniquement à des fins de test. La version bêta n'est pas destinée à travailler avec des données importantes.

Une fois activées, les versions bêta apparaîtront dans les mises à jour disponibles dans l'onglet Mises à jour du système.

AVERTISSEMENT
Après la mise à jour **Access Commander** la dernière version bêta ne peut pas être rétrogradée vers une version précédente.

Sauvegarde du système
Dans **l'onglet Paramètres > Sauvegarde du système**, vous pouvez effectuer, configurer et contrôler la sauvegarde et la récupération des données d'**Access Commander**. Les données peuvent être stockées

sur un support local ou sur un bloc de messages du serveur (SMB). Le SMB convient au stockage de sauvegarde à long terme.

Les données peuvent être sauvegardées une fois ou automatiquement à des intervalles réguliers prédéfinis.

Chaque sauvegarde peut être restaurée, téléchargée ou supprimée dans le menu qui s'agrandit après avoir cliqué sur ⋮ pour un élément de la liste de sauvegarde.

Sauvegarde des données unique

1. Aller à **Paramètres > Onglet Sauvegarde du système**.
2. En bas de l'onglet, cliquez sur Sauvegarder maintenant.
3. Sélectionnez s'il faut chiffrer les données du fichier. Si tel est le cas, renseignez le mot de passe qui sera nécessaire pour restaurer la sauvegarde.

Paramètres de sauvegarde automatique des données

1. Aller à **Paramètres > Onglet Sauvegarde du système**.
2. Cliquer sur ✎ au paramètre Sauvegarde régulière.
3. Définissez les paramètres de sauvegarde requis :
   - fréquence – l'intervalle spécifiant la fréquence à laquelle la sauvegarde sera effectuée
   - heure – la sauvegarde sera effectuée le jour concerné à cette heure
   - jour – jour de la semaine ou du mois au cours duquel la sauvegarde sera effectuée
4. Sélectionnez s'il faut chiffrer les données du fichier. Si tel est le cas, renseignez le mot de passe qui sera nécessaire pour restaurer la sauvegarde.
5. En enregistrant, les sauvegardes seront effectuées automatiquement selon les paramètres sélectionnés.

Paramètres de sauvegarde des données sur SMB

1. Aller à **Paramètres > Onglet Sauvegarde du système**.
2. Cliquer sur ✎ au paramètre Storage.
3. Sélectionnez le type de stockage : SMB.
4. Remplissez l'adresse du serveur, les informations de connexion et la version du protocole.
5. En enregistrant, toutes les sauvegardes seront envoyées au bloc de messages du serveur défini.

Restaurer à partir des données de sauvegarde

1. Aller à **Paramètres > Onglet Sauvegarde du système**.
2. Ouvrir le menu étendu ⋮ à la sauvegarde sélectionnée et sélectionnez Restaurer.

Restaurer à partir d'un fichier de sauvegarde

1. Aller à **Paramètres > Onglet Sauvegarde du système**.
2. En bas de l'onglet, cliquez sur Restaurer à partir d'un fichier.
3. Sélectionnez le fichier de sauvegarde dans votre stockage et cliquez sur Restaurer.

Transférer des données d'un autre Access Commander

1. Aller à **Paramètres > Onglet Sauvegarde du système**.
2. En bas de l'onglet, cliquez sur Émigrer.
3. Saisissez l'adresse IP de l'Access Commander à partir duquel vous souhaitez transférer les données.
4. Remplissez les informations d'identification du compte administrateur Access Commander à partir duquel vous souhaitez transférer les données.

ATTENTION
Pour importer des données depuis un autre Access Commander, le service SSH doit être activé sur le serveur à partir duquel les données seront téléchargées.

Synchronisation des utilisateurs avec FTP

La liste des utilisateurs et leurs paramètres de base, y compris les affectations aux entreprises et aux groupes, peuvent être synchronisés à l'aide d'un fichier CSV géré en externe.

La synchronisation est effectuée dans **Paramètres > Onglet Synchronisation des utilisateurs**. Il est possible de télécharger un exemple de fichier CSV depuis la carte (dans le menu étendu ⋮).

ASTUCE
La liste des utilisateurs actuels, qui correspond à la structure de l'exemple de fichier CSV, peut être téléchargée depuis la page Rapports (p. 85).

Le fichier CSV préparé peut être directement importé sur la carte. Données du fichier avec s **Access Commander** ils commenceront à se synchroniser automatiquement.

Des informations détaillées sur le résultat de chaque synchronisation sont stockées dans le journal système. Le journal lui-même contient des informations de base sur le succès ou l'échec de la synchronisation. Les informations détaillées sont stockées dans un fichier téléchargeable à l'aide de l'icône en fin de ligne.

Synchronisation automatique des utilisateurs avec FTP

L'onglet User Sync dans Paramètres vous permet de lier **Access Commander** avec le stockage FTP où se trouve le fichier CSV avec la liste des utilisateurs. L'onglet affiche ensuite des informations sur ce stockage FTP.

1. Allez sur **Settings > User Sync tab**.
2. Cliquer sur ✎ dans le paramètre Stockage.
3. Dans la boîte de dialogue ouverte, définissez l'adresse du serveur FTP sur lequel le fichier CSV est stocké.
4. L'activation de TLS permet d'activer le Transport Layer Security (TLS) pour la connexion FTP. TLS crypte les données transmises entre **Access Commander** et le serveur.
   Activer l'authentification du certificat TLS pour activer l'authentification TLS des certificats fournis par le serveur. Lorsque cette option est activée, **Access Commander** vérifie qu'il communique avec un serveur de confiance, ce qui augmente la sécurité de la connexion.

   ATTENTION
   Le proxy pour FTP avec authentification TLS n'est pas pris en charge.
5. Entrez les informations d'identification pour accéder au serveur FTP.

Fichier CSV

NOTE
Certains tableurs utilisent des séparateurs différents et le fichier CSV peut ne pas s'afficher correctement lorsqu'il est ouvert dans ceux-ci. Dans de tels cas, il est recommandé d'importer les données du fichier CSV dans un classeur ouvert.

Un fichier CSV a une structure donnée qui doit être respectée. Toutes les valeurs sont séparées par une virgule, seule la liste des groupes est séparée par un point-virgule. Le fichier CSV a la structure suivante :

- EmployeeID – clé primaire qui doit être remplie. Il s'agit d'un identifiant d'utilisateur unique.
- User Name – le nom de l'utilisateur créé dans Access Commander.
- Company – le nom de la société sous laquelle l'utilisateur sera constitué. La société doit être créée dans Access Commander. Les lettres minuscules et majuscules utilisées dans les noms de sociétés ou de groupes ne sont pas interchangeables.
- User Mail – adresse e-mail de l'utilisateur.
- Card Numbers – le numéro de carte de l'utilisateur. Jusqu'à deux cartes peuvent être définies pour un utilisateur. Les numéros de cartes individuelles doivent être séparés par un point-virgule (;).
- Switch Code – un code de commutateur, un code est toujours créé sous le premier commutateur.
- Phone Number 1 – numéro de téléphone en première position.
- Group Call – appel de groupe vers le numéro de téléphone défini ci-dessus. Prend les valeurs True/False. Lorsqu'il est défini sur True, les appels de groupe sont activés. Lorsqu'il est défini sur False, les appels de groupe sont désactivés.
- Phone Number 2 – numéro de téléphone en deuxième position.
- Group Call – appel de groupe vers le numéro de téléphone défini ci-dessus. Prend les valeurs True/False. Lorsqu'il est défini sur True, les appels de groupe sont activés. Lorsqu'il est défini sur False, les appels de groupe sont désactivés.
- Phone Number 3 – numéro de téléphone en troisième position.
- Virtual Number – numéro virtuel de l'utilisateur.
- Groups – liste des groupes auxquels l'utilisateur doit être ajouté. Tous les groupes doivent être établis dans Access Commander. La liste des groupes est séparée par un point-virgule. Les lettres minuscules et majuscules utilisées dans les noms de sociétés ou de groupes ne sont pas interchangeables.
- Is Deleted – indique si l'utilisateur doit être supprimé. Lorsqu'il est défini sur FALSE, l'utilisateur est créé et seules ses données sont mises à jour lors de la prochaine synchronisation. S'il est défini sur TRUE, l'utilisateur est supprimé lors de la prochaine synchronisation. S'il est défini sur FALSE, l'utilisateur sera à nouveau créé.
- License Plates – marques d'enregistrement. Il est possible de définir plusieurs plaques d'immatriculation, qui doivent être séparées par un point-virgule.

Date et l'heure

Pour modifier la méthode de récupération de l'heure, allez sur **Settings > Configuration > Date and Time tab**.

La date et l'heure dans **Access Commander** peuvent être synchronisées avec Internet ou réglées manuellement. Si **Access Commander** n'est pas connecté à Internet, vous devez régler manuellement la date, l'heure et le fuseau horaire. Sinon, il est possible de passer au NTP et d'obtenir l'heure à partir du serveur NTP. Dans ce cas, il suffit de régler le fuseau horaire. Le serveur NTP met à jour la date et l'heure automatiquement.

ATTENTION
Après avoir enregistré le changement d'heure **Access Commander**redémarre automatiquement.

Synchronisation de l'heure avec les appareils

L'heure des appareils connectés peut être synchronisée avec l'heure de l'**Access Commander**. Le partage de l'heure avec les appareils est activé en activant le paramètre Synchronisation des appareils dans **Réglages > Configuration > onglet Date et heure**.

Si la synchronisation de l'heure avec l'appareil est activée, il est possible de choisir parmi les méthodes de synchronisation suivantes :

- **Les appareils utilisent le même serveur NTP** – l'heure sur les appareils est régie par le serveur NTP défini dans **Access Commander**.

  ASTUCE
  L'heure du serveur NTP offre la meilleure précision de l'heure sur l'appareil.

- **Les appareils utilisent Access Commander comme serveur NTP** – contrôle l'heure sur les appareils en fonction de l'heure réglée dans**Access Commander**.

Automation

La fonction d'automatisation est disponible dans **2N Access Commander** à partir de la version 3.2 du micrologiciel sous les licences Advanced, Pro et Unlimited. Construit sur la plateforme Node-RED, cet ajout offre directement à **Access Commander** des capacités étendues de programmation basée sur le flux. Elle permet aux utilisateurs de connecter **Access Commander** à divers systèmes tiers et d'automatiser des flux de travail personnalisés basés sur des événements au sein de la plateforme.

ATTENTION
Pour utiliser pleinement cet outil d'automatisation polyvalent, il est nécessaire de garder à l'esprit les points suivants :

- **Responsabilité du client en matière de sécurité**: Les utilisateurs sont responsables de s'assurer que leurs configurations et flux de travail d'automatisation sont sécurisés et conformes aux meilleures pratiques en matière de cybersécurité. Cela comprend la sécurisation de l'environnement Node-RED, la gestion appropriée des autorisations et la protection des données sensibles au sein de leurs automatisations.
- **Utilisation du nœud API REST**: S'il n'est pas utilisé correctement, ce nœud peut entraîner une perte de données ou des modifications involontaires. Il est de la responsabilité de l'utilisateur de s'assurer que le nœud est configuré et implémenté correctement. Soyez prudent et revérifiez vos paramètres pour éviter tout risque potentiel pour vos données.
- **Nœuds et modules complémentaires tiers**: 2N Telekomunikace n'est pas responsable de l'utilisation ou de l'intégration de nœuds tiers, de modules complémentaires ou de modifications personnalisées de Node-RED dans la fonction d'automatisation. Les clients doivent évaluer et garantir soigneusement la sécurité et la stabilité de tous les composants supplémentaires qu'ils choisissent d'installer. Tout problème découlant d'extensions tierces devra être résolu par le client ou le fournisseur tiers concerné.
- **Limitations du support technique**: Bien que notre équipe d'assistance puisse vous aider à résoudre les problèmes liés aux fonctionnalités de base de la fonction d'automatisation dans 2N Access Commander, y compris nos nœuds Access Commander personnalisés, elle ne pourra pas fournir d'assistance pour la conception, le développement ou le débogage des flux Node-RED personnalisés. Les utilisateurs qui souhaitent créer des automatisations complexes devront peut-être demander une assistance supplémentaire à des experts Node-RED qualifiés ou consulter les ressources disponibles.

Pour démarrer avec Node-RED, il est conseillé d'explorer les ressources en ligne, tels que des manuels détaillés et de nombreux tutoriels YouTube sur Node-RED, qui fournissent des conseils sur la création et la gestion des flux.

Pour plus d'informations sur les nœuds personnalisés d'**Access Commander** et sur l'utilisation de la fonction d'automatisation dans **Access Commander**, veuillez vous référer à ce manuel.

Cette fonction améliore les capacités d'**Access Commander**. Il est recommandé d'explorer son potentiel tout en assurant la sécurité des configurations.

Création d'automatisations

Les tâches automatisées sont créées dans un éditeur externe. L'éditeur est accessible depuis un onglet sur la page **Paramètres > Configuration > Onglet Automatisation**. Les modifications apportées dans l'éditeur ne prendront effet qu'après leur déploiement sur le serveur, qui se fait à l'aide d'un bouton Déploy dans le coin supérieur droit de l'éditeur.

La création de tâches automatisées repose sur la compilation de flux. Les flux sont tirés de nœuds individuels connectés les uns aux autres. Un menu de nœuds s'affiche dans le panneau de gauche. Dans le panneau de gauche, il est possible de rechercher des nœuds par leur nom. Un nouveau nœud peut également être ajouté après avoir créé une nouvelle connexion à partir d'un nœud existant.

Les données transmises entre les nœuds sont appelées messages. Leur description et leur travail avec eux sont détaillés ici. Ce support décrit également les nœuds de base (nœuds) qui traitent le format des messages individuels ou leurs séquences, tels que les nœuds Change, Split, Join,... L'automatisation peut fonctionner non seulement avec les données obtenues dans cette tâche unique (msg.), mais peut également travailler avec des valeurs dynamiques dans le contexte de l'ensemble de l'historique des flux (flow.) voire de tous les flux de l'installation (global.).

ATTENTION
Bouton Deploy envoie les flux définis au serveur. Ce n'est qu'en envoyant au serveur que les nouveaux flux prendront effet !

Mode sans échec (safe mode)

Le mode sans échec est un outil clé pour résoudre les problèmes d'automatisation. L'exécution de l'éditeur en mode sans échec vous permet d'apporter des modifications aux flux sans que ces flux ne s'exécutent en arrière-plan. Cela signifie que vous pouvez accéder à l'éditeur, modifier ce dont vous avez besoin, puis redéployer les modifications avec un bouton. Deploy. Ce mode est particulièrement utile si l'un des flux provoque un dysfonctionnement ou un crash de Node-RED, par exemple en raison d'une erreur dans le flux ou d'un nœud tiers, ou si le flux doit être arrêté immédiatement.

Noeuds (nodes) Access Commander

REST API

Le nœud REST API envoie une requête API HTTP définie. Les données d'entrée contenues dans la propriété **body** sont utilisées comme points de requête de cette application. Les données de sortie du nœud sont les données de réponse à la demande. La sélection et l'ordre des données de sortie peuvent être spécifiés dans le paramètre **Query**.

Paramètres du nœud

- **Method** – offre un choix de méthodes de demande d'API
- **Endpoint** – est utilisé pour spécifier l'ensemble du point d'accès vers lequel la demande sera dirigée. Le chemin du point d'accès peut être complété par le paramètre points.
  L'utilisation des requêtes HTTP est décrite dans API HTTP (p. 119).
- **Query** – est utilisé pour spécifier quels paramètres de données doivent être traités dans le point final et comment ils doivent être renvoyés dans la sortie. Ce paramètre peut être spécifié par une valeur d'entrée, la propriété **query**. La construction d'une requête est décrite dans le document Data Query Customization(en anglais uniquement).
- **Only send non-2xx responses to Catch node** – cette option détermine le type de réponses HTTP qui seront capturées dans le nœud Catch.
- **Name** – vous permet de renommer le nœud pour mieux l'orienter lorsque vous travaillez avec le flux.

Access log

Le nœud lit les enregistrements du journal d'accès et permet à ces enregistrements d'être traités ultérieurement.

L'administrateur peut configurer des tâches automatisées qui s'exécutent lorsque **Access Commader** voit une entrée de journal définie. La définition de l'action s'effectue dans les paramètres du nœud. La sortie est constituée de données spécifiques sur l'événement consigné. Une fonction basée sur SignalR s'exécute en arrière-plan de cette fonctionnalité.

Paramètres du nœud

- **Filter** – est utilisé pour spécifier les enregistrements que le nœud doit traiter. Les enregistrements ne correspondant pas à ce filtre seront ignorés par le flux. Le format du filtre est un objet JSON. Ce paramètre peut être remplacé par la valeur d'entrée.
- **Name** – vous permet de renommer le nœud pour mieux l'orienter lorsque vous travaillez avec le flux.

System Log

Le nœud charge les enregistrements dans le journal système et permet à ces enregistrements d'être traités ultérieurement.

L'administrateur peut configurer des tâches automatisées qui s'exécutent lorsque **Access Commander** voit une entrée de journal définie. La définition de l'action s'effectue dans les paramètres du nœud. La sortie est constituée de données spécifiques sur l'événement consigné. Une fonction basée sur SignalR s'exécute en arrière-plan de cette fonctionnalité.

Paramètres du nœud

- **Filter** – est utilisé pour spécifier les enregistrements que le nœud doit traiter. Les enregistrements ne correspondant pas à ce filtre seront ignorés par le flux. Le format du filtre est un objet JSON. Ce paramètre peut être remplacé par la valeur d'entrée.
- **Name** – vous permet de renommer le nœud pour mieux l'orienter lorsque vous travaillez avec le flux.

SignalR

Le nœud SignalR lit les données de la rubrique en cours de suppression. Le nœud récupère les données en temps réel, il convient donc aux scénarios dans lesquels la tâche automatisée consiste à récupérer les informations d'Access Commander sans qu'il soit nécessaire de l'interroger en permanence.

Paramètres du nœud

- **Topic** – propose des thèmes disponibles pour l'abonnement.
- **Filter** – est utilisé pour spécifier les enregistrements que le nœud doit traiter. Les enregistrements ne correspondant pas à ce filtre seront ignorés par le flux. Le format du filtre est un objet JSON. Ce paramètre peut être remplacé par la valeur d'entrée.
- **Name** – vous permet de renommer le nœud pour mieux l'orienter lorsque vous travaillez avec le flux.

Plus d'informations sur les fonctionnalités de SignalR sont données dans le chapitre SignalR (p. 119).

Dynamic SignalR

Le nœud Dynamic SignalR par rapport au nœud SignalR permet des changements dynamiques dans l'échantillonnage des données. Il peut s'agir de modifier le sujet ou la méthode d'échantillonnage en fonction des valeurs d'entrée. Les valeurs de sortie du nœud sont à la fois les données extraites du sujet (Données) et les informations sur le succès ou l'échec de l'action du nœud.

Paramètres du nœud

- **Topic** – définit le thème pour lequel la modification de l'extraction des données doit avoir lieu.
- **Filter** – est utilisé pour spécifier les enregistrements que le nœud doit traiter. Les enregistrements ne correspondant pas à ce filtre seront ignorés par le flux. Le format du filtre est un objet JSON. Ce paramètre peut être remplacé par la valeur d'entrée.
- **Records** – définit le nombre d'enregistrements à lire lors de l'utilisation du type de lecture "fetch".
- **Fetch When Ready** – définit si les valeurs doivent être récupérées lorsque la commande fetch est activée.
- **Name** – vous permet de renommer le nœud pour mieux l'orienter lorsque vous travaillez avec le flux.

Valeurs d'entrée valides

Le nœud accepte les propriétés suivantes comme valeurs d'entrée. Les valeurs d'entrée valides remplacent temporairement les paramètres définis dans la configuration du nœud.

- **topic** – chaîne de caractères spécifiant le sujet à supprimer.
- **filter** – au format JSON, qui spécifie les enregistrements à extraire.
- **fetchWhenReady** – bootlean spécifiant le paramètre du nœud Fetch When Ready.
- **action** – une chaîne de caractères spécifiant l'action à effectuer. Il peut s'agir de s'abonner à l'abonnement, de se désabonner...
- **update** – peut contenir un horodatage (chaîne) et une fenêtre temporelle (objet) indiquant le moment où l'action à effectuer a été modifiée.

Plus d'informations sur les fonctionnalités de SignalR sont données dans le chapitreSignalR (p. 119).

Write system log

Le nœud Write system log crée une entrée dans le journal système Access Commander. L'entrée du journal contient la gravité spécifiée, la description de l'événement et d'autres détails. Si une erreur se produit pendant le processus, elle est enregistrée et l'état du nœud est mis à jour en conséquence. Le nœud n'a aucune valeur de sortie.

Paramètres du nœud

- **Severity** – détermine la gravité de l'enregistrement. Ce paramètre peut être spécifié par la valeur d'entrée "query"..
- **Filter** – est utilisé pour spécifier les enregistrements que le nœud doit traiter. Les enregistrements ne correspondant pas à ce filtre seront ignorés par le flux. Le format du filtre est un objet JSON. Ce paramètre peut être remplacé par la valeur d'entrée.
- **Detail** – est utilisé pour une description plus détaillée de l'enregistrement, qui est affichée dans le journal du système. Ce paramètre peut être remplacé par une valeur d'entrée.
- **Name** – vous permet de renommer le nœud pour mieux l'orienter lorsque vous travaillez avec le flux.

Valeurs d'entrée valides

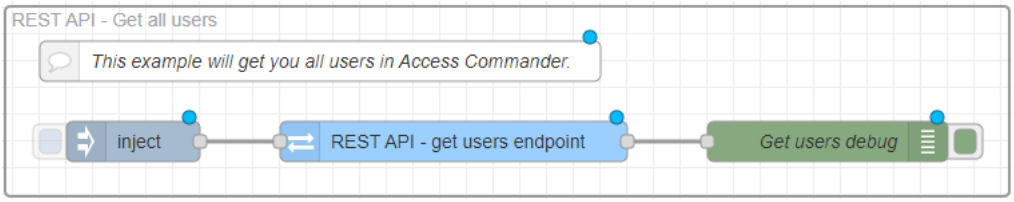
Le nœud accepte les propriétés suivantes comme valeurs d'entrée. Les valeurs d'entrée valides remplacent temporairement les paramètres définis dans la configuration du nœud.

- **severity** – une chaîne de caractères spécifiant la gravité de l'enregistrement.
- **event** – une chaîne décrivant brièvement l'action enregistrée.
- **detail** – chaîne de caractères qui remplit la description détaillée de l'enregistrement qui sera affichée dans le journal du système.

Exemples de flux (flows)

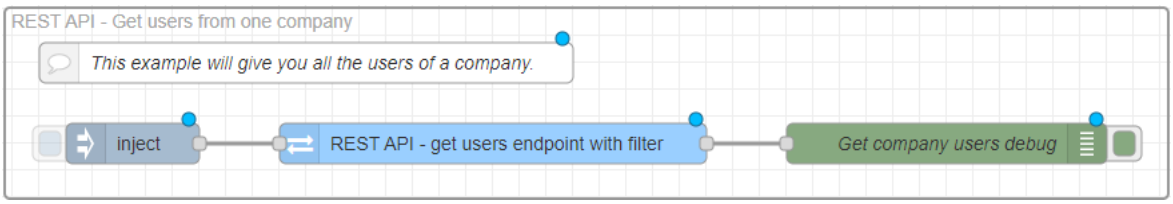
Access Commander propose plusieurs tâches automatisées de base représentant les possibilités d'utilisation de l'automatisation. Les flux de ces tâches peuvent être installés lorsque vous lancez pour la première fois la fonction d'automatisation dans **Access Commander**, mais ils peuvent également être importés ultérieurement, voir Exporter/Importer des flux (p. 102)Exporter/Importer des flux (p. 102). Ces flux prédéfinis peuvent être facilement modifiés pour vos propres besoins.

Get all users



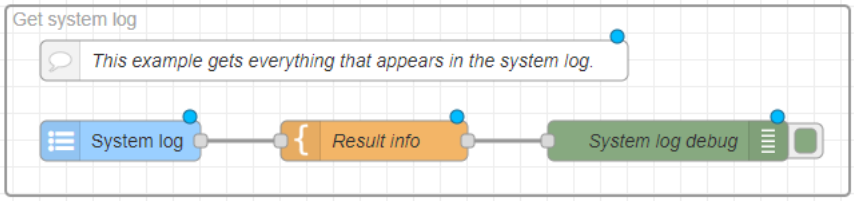
Ce flux génère une liste de tous les utilisateurs, y compris leurs informations. La tâche est lancée en activant le nœud Inject. Un filtre peut être appliqué au nœud **REST API - get users endpoint** pour spécifier les utilisateurs que le processus doit renvoyer. De cette manière, le résultat du processus peut être adapté aux besoins de l'administrateur.

Get users from one company



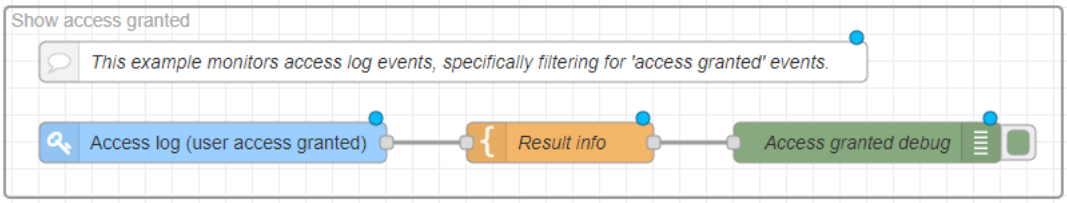
Ce flux génère une liste de tous les utilisateurs d'une même entreprise, ainsi que des informations les concernant. La tâche est lancée en activant le nœud Inject. La sélection de l'entreprise est définie dans le nœud de **REST API – get users endpoint with fillter** en spécifiant son id.

Get system log



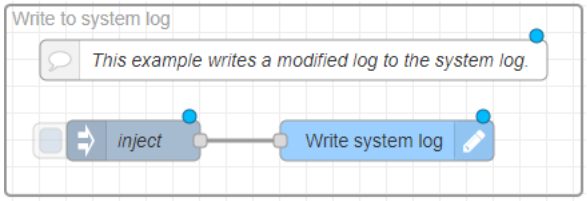
Ce flux récupère toutes les nouvelles entrées dans le journal système. La sélection des événements peut être affinée en précisant un filtre dans le nœud **System log**.

Show access granted



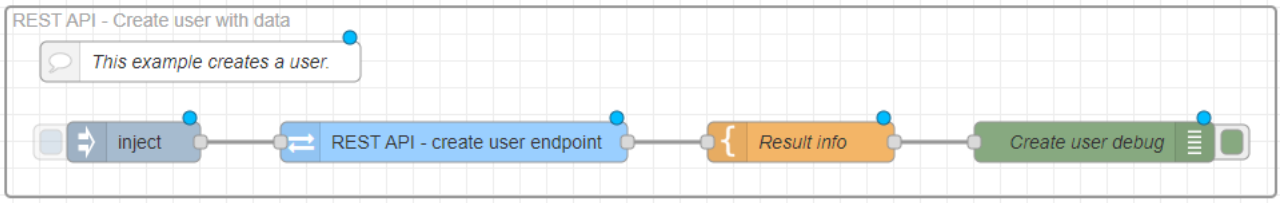
Ce flux récupère toutes les nouvelles entrées dans le journal d'accès. Le flux est configuré pour charger uniquement l'accès accordé. Dans le nœud **Access log** est possible de modifier cette restriction.

Write to system log



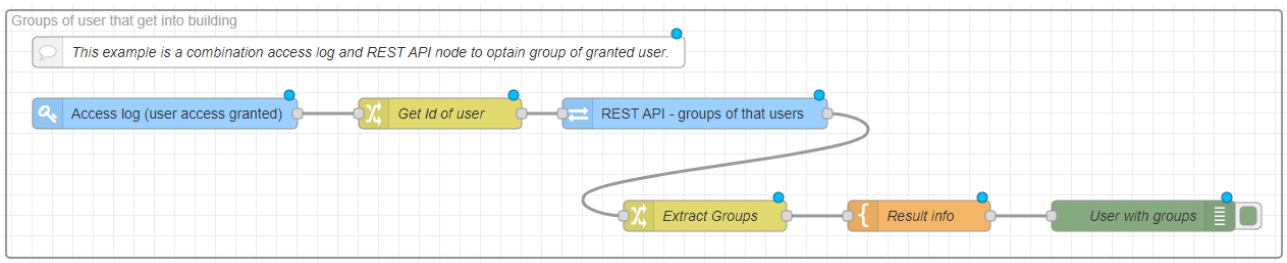
Ce flux crée une entrée dans le journal du système. Le nœud **Write system log** peut être utilisé pour définir la gravité, le nom et la description détaillée de l'entrée.

Create user with data



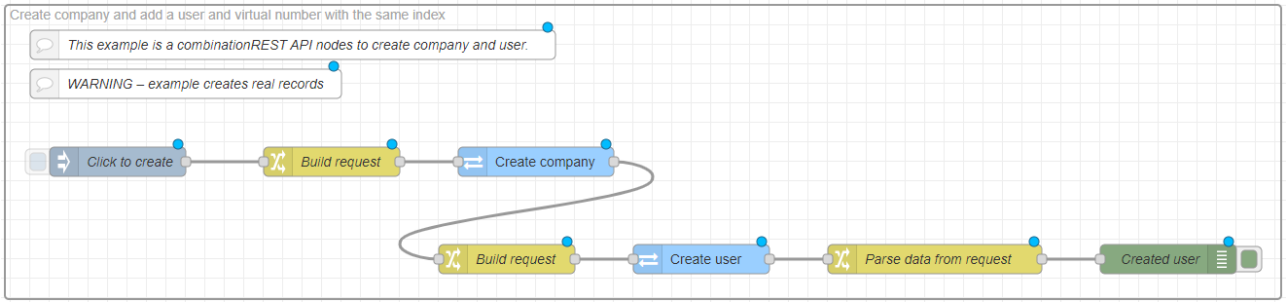
Ce flux est utilisé pour créer un nouvel utilisateur. La tâche est initiée par l'activation du nœud **Inject**. Le nœud **Inject** contient un corps de message qui spécifie le nom de l'utilisateur Joe Doe et son affectation à l'entreprise avec l'ID 1. Ce corps est appliqué dans le nœud **Rest API - create user endpoint** et l'utilisateur est créé sur la base de ce corps. Le nœud **Result info** définit le texte du message qui apparaîtra dans les messages de débogage.

Groups of users that get into building



Ce flux permet de récupérer les groupes d'utilisateurs auxquels l'accès a été accordé. Les accès autorisés sont extraits du journal des accès. Le flux récupère ensuite l'ID de l'utilisateur auquel l'accès a été accordé et utilise le nœud **REST API - groups of that users** pour récupérer des informations sur cet utilisateur. Le nœud **Extract Groups** récupère les noms de groupe de cet utilisateur et le nœud **Result info** compile le texte du message final.

Create company and add a user and virtual number with the same index



Ce flux crée une nouvelle entreprise, le premier utilisateur de cette entreprise et son numéro virtuel. La tâche est initiée par l'activation du nœud **Inject**. Lors de l'initialisation, un nombre entier aléatoire est généré, qui sera utilisé dans le nom de l'entreprise, le nom de l'utilisateur et servira de numéro virtuel à l'utilisateur. Le nœud **Create company** (Créer une société) crée une société avec le nom défini. La réponse de ce nœud donnera l'ID de l'entreprise, sur la base duquel le nœud suivant **Create user** créera un nouvel utilisateur dans cette entreprise et lui attribuera un numéro virtuel en même temps. Le nœud **Parse data from request** récupère alors le nom de l'entreprise, le nom de l'utilisateur et le numéro virtuel de l'utilisateur.

Exporter/Importer des flux

Les flux peuvent être exportés vers des fichiers .json et réimportés ultérieurement dans l'interface d'automatisation. L'exportation et l'importation s'effectuent dans le menu étendu situé dans le coin supérieur droit. Les flux déplacés d'une installation d'**Access Commander** à une autre peuvent nécessiter des modifications.

Les options d'importation contiennent des exemples de flux préchargés pour **Access Commander**. Ils se trouvent dans l'onglet Exemples, dans le dossier Access-Commander-nodes.

ATTENTION
Les paramètres de fonctionnalités avancées non pris en charge par la nouvelle licence ne sont pas enregistrés.

Par conséquent, lorsque vous mettez fin à votre licence d'essai, n'oubliez pas d'exporter les flux configurés.

États d'erreur

Cuando se trabaja con automatizaciones, ocasionalmente pueden producirse errores que afecten a su estabilidad y funcionalidad. Si se produce una condición de error, la pestaña Automatización de **Access Commander** le alertará sobre la condición y le ofrecerá reiniciar la plataforma Node-RED en modo seguro. El modo seguro detiene temporalmente la ejecución de los flujos y permite la reparación segura de los flujos que inducen la condición de error. El reinicio de los flujos se activa con el botón Deploy.

Il existe deux conditions d'erreur de base :

- **Node-RED ne répond pas**
  Cette condition se produit lorsque Node-RED ne répond plus. Aucune automatisation définie n'est en cours d'exécution. Ce problème peut être provoqué par divers facteurs, tels qu'une surcharge du système, des erreurs dans les paramètres de flux ou des conflits entre modules tiers importés.

- **Node-RED est instable**
  L'instabilité de Node-RED se manifeste par des redémarrages répétés de la plateforme, ce qui peut perturber le fonctionnement de l'automatisation et entraîner des pertes de données. Un redémarrage répété se produit généralement si l'un des flux est mal configuré et déclenche un redémarrage. Tous les flux sont suspendus pendant la durée du redémarrage.

Nom de l'installation

Le nom de l'installation spécifique d'**Access Commander** est affiché dans l'en-tête de l'interface web, et ce nom est affiché à tous les utilisateurs connectés. Le nom par défaut d'**Access Commander** peut être modifié, par exemple, pour indiquer l'adresse du bâtiment géré par une installation particulière.

Pour modifier le nom, allez dans **Paramètres > Configuration > onglet Nom de l'installation**. Vous pouvez utiliser le changement de nom pour distinguer les installations individuelles si une personne gère plusieurs installations. Le nom de l'installation est également inscrit dans les courriels envoyés aux entreprises.

Activation et configuration de la fonction E-mail (SMTP)

La fonction E-mail permet d'envoyer des notifications ou d'envoyer des mots de passe de connexion aux utilisateurs. Les e-mails sont envoyés via le protocole SMTP.

1. Les paramètres sont définis dans **Réglages > Configuration > Email**.
2. Après avoir activé la fonction E-mail, une boîte de dialogue s'ouvre dans laquelle vous pouvez définir les paramètres suivants :
   - **Adresse du serveur SMTP**, à qui les e-mails seront envoyés.
   - **Port de serveur**, préréglé à 25.
   - **Nom d'utilisateur** et **mot de passe** au compte sur le serveur SMTP si le serveur SMTP nécessite une autorisation.
   - **Adresse de l'expéditeur par défaut**, à partir duquel les e-mails seront envoyés.
3. Allumez si nécessaire :
   - **SSL** pour le cryptage des e-mails,
   - **Vérification du certificat du serveur SSL**,
   - **Le mode de compatibilité** en cas de connexion à des serveurs SMTP plus anciens ne prenant pas en charge les nouvelles fonctions (GSSAPI).
4. Après avoir enregistré, vous pouvez le configurer dans l'onglet E-mail **Adresse de base pour les liens e-mail**, qui fera partie des messages électroniques envoyés et pourra renvoyer les destinataires des e-mails vers la partie sélectionnée de l'interface **Access Commander**.
5. Vous pouvez vérifier les paramètres effectués en envoyant un email de test.

Authentification à double facteur

L'authentification à deux facteurs offre un niveau de sécurité plus élevé pour les comptes d'utilisateurs dans **Access Commander**. Pour se connecter, l'utilisateur saisit ses données de connexion et doit ensuite confirmer sa connexion à l'aide de l'application d'authentification. Dès que l'administrateur a activé la nécessité d'une authentification à deux facteurs, l'utilisateur est invité à lier son compte à sa propre application d'authentification lors de sa prochaine connexion.

Access Commander n'exige pas que vous vérifiiez à nouveau votre identité chaque fois que vous vous connectez ou que vous effectuez des actions protégées. Une fois la vérification effectuée, le système se souvient de vous pour une durée limitée :

- 7 jours pour les connexions normales
- 5 minutes pour les actions considérées comme critiques sur le plan de la sécurité, telles que la modification des clés API, la mise à jour de votre propre mot de passe ou la modification du mot de passe root.

Le système peut mémoriser jusqu'à deux dispositifs authentifiés. Si vous vous authentifiez à partir d'un nouveau dispositif, le plus ancien dispositif mémorisé est supprimé. Si vous tentez d'effectuer une action critique pour la sécurité en dehors de la période autorisée, le système vous demandera simplement de vous authentifier à nouveau avant de pouvoir continuer.

1. L'authentification à deux facteurs est définie par l'administrateur dans l'onglet **Paramètres > Configuration > onglet Authentification à deux facteurs**.
2. L'administrateur peut choisir les utilisateurs qui auront besoin d'une authentification à deux facteurs.
   Options pour exiger une vérification en deux étapes
   - **Facultative**
     L'authentification à deux facteurs est facultative. Les utilisateurs peuvent l'activer eux-mêmes sur leur profil.
   - **Obligatoire pour les utilisateurs avec un rôle**
     Chaque utilisateur auquel un rôle a été attribué doit confirmer sa connexion à l'aide d'une application d'authentification.
   - **Obligatoire**
     Tous les utilisateurs doivent confirmer leur connexion à l'aide d'une application d'authentification.

Activer l'authentification à deux facteurs

Si l'administrateur configure l'authentification à deux facteurs comme facultative, l'utilisateur active lui-même l'authentification à deux facteurs de la manière suivante :

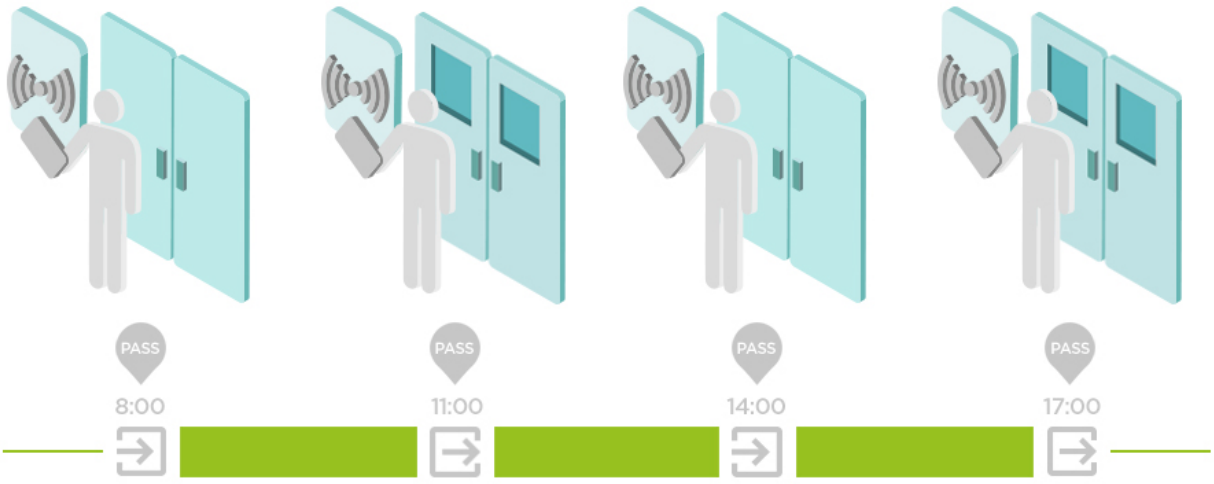
1. Cliquez sur l'image de l'utilisateur dans le coin supérieur droit pour ouvrir le menu de l'utilisateur.
2. Utilisez l'onglet Applications d'authentification pour lier votre compte à l'application d'authentification sélectionnée. Suivez les instructions de **Access Commander**.
3. Sélectionnez Afficher le profil.

Paramètres de présence

Access Commander permet de surveiller la présence des utilisateurs. En mode présence, les heures d'entrée et de sortie des utilisateurs individuels sont enregistrées.

Modes de présence

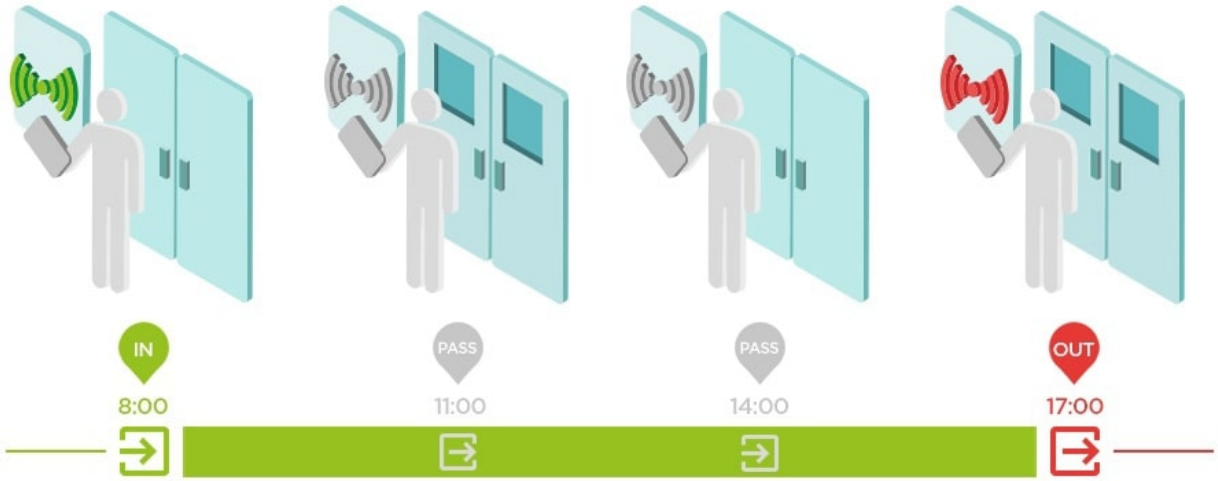
- **FREE**



Les arrivées et les départs sont comptés à partir de la première et de la dernière authentification de l'utilisateur sur n'importe quel appareil au cours d'une journée. Le module de présence ne fonctionne pas dans ce mode.

- **IN-OUT**

  Pour fonctionner correctement, l'appareil doit être configuré pour entrer et sortir de la zone.



- **IN-OUT pour tous les appareils**
  Ce mode permet la surveillance de présence. Les arrivées sont enregistrées sur les appareils entrants, les départs sont enregistrés sur les appareils sortants. Les mouvements entre zones ne sont pas enregistrés comme arrivée/départ.
- **IN-OUT pour les appareils sélectionnés**
  Ce mode permet la surveillance de présence. Les arrivées et les départs sont enregistrés sur des appareils sélectionnés qui sont définis comme arrivées ou départs. Les arrivées et départs sont enregistrés uniquement sur ces appareils sélectionnés. L'enregistrement des arrivées/départs peut ainsi être réglé, par exemple, uniquement à l'entrée principale du bâtiment.

Paramètres du point d'accès de l'appareil

Vous pouvez logiquement diviser chaque appareil en deux points d'accès - l'arrivée et le départ. Chaque point d'accès représente un passage dans une direction et détermine si l'utilisateur de l'appareil entre ou sort de la zone. Un point d'accès peut être contrôlé par un ou plusieurs modules de l'appareil. Tous les modules affectés gèrent alors les passages dans la direction du point d'accès spécifique. Les points d'accès sont surtout utilisés lorsqu'un appareil se trouve à la limite de deux zones et que la direction du mouvement entre ces deux zones doit être enregistrée avec précision (par exemple, pour les fonctions anti-passback).

Les points d'accès sont également utilisés pour suivre les utilisateurs dans le module Présence (p. 84). Les points d'accès sont également utilisés pour surveiller les entrées et les sorties Restrictions de zone (p. 86).

NOTE
Dans l'interface de configuration web de chaque appareil, les points d'accès sont appelés **Arrivée** et **Départ**. Pour les configurer, accédez à **Accès > Règles d'accès > sélectionnez l'onglet « Accès et sortie »**.

Activation des points d'accès dans Access Commander

1. Accédez à la page Zones v **Access Commander**.
2. Dans le coin supérieur droit, appuyez sur ⚙ et permettre l'utilisation de points d'accès.

Activation des points d'accès dans Access Commander

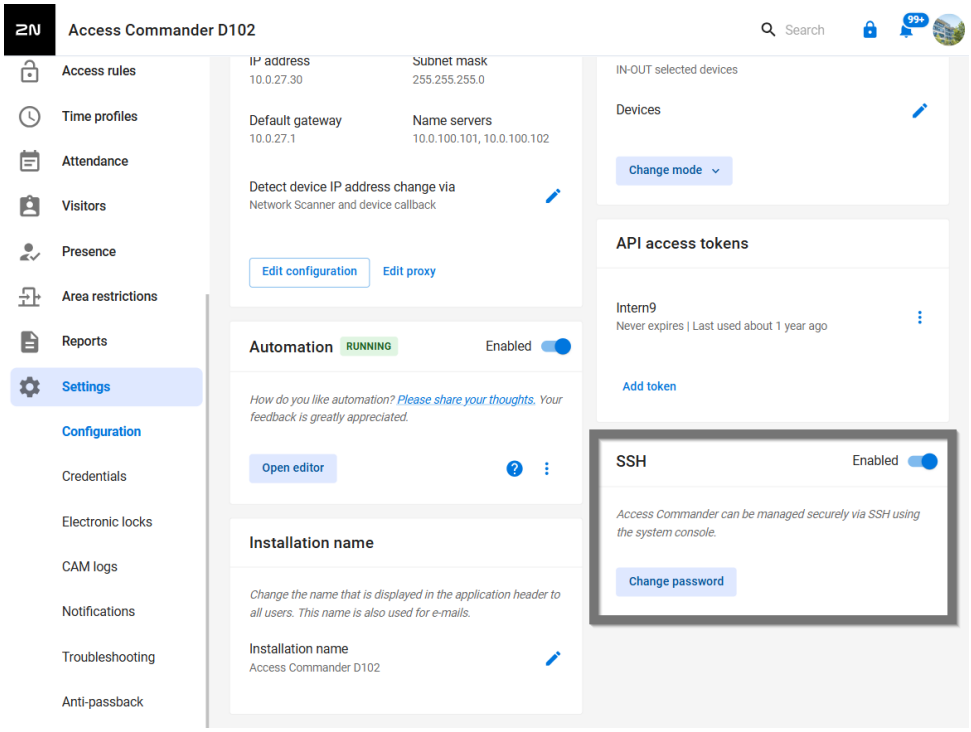
1. Entrez la configuration Web de l'appareil.

> **ASTUCE**
>
> L'interface de configuration Web est accessible en cliquant sur la liste de la page Appareils.

2. Accédez à la **section Matériel > Menu Modules d'extension**.
3. Accédez à la page Zones v **Access Commander**.
4. Une boîte de dialogue s'ouvre avec une liste des modules de gestion d'accès disponibles.
5. Dans le coin supérieur droit, appuyez sur et permettre l'utilisation de points d'accès.

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

Autoriser l'accès SSH



> **AVERTISSEMENT**
>
> L'activation de l'accès SSH est recommandée uniquement aux utilisateurs avancés. Une mauvaise utilisation constitue un risque pour la sécurité.

Utilisez l'onglet **Paramètres > Configuration > SSH** pour activer Secure Shell, qui permet une communication à distance sécurisée avec la console du système. L'activation de SSH vous permet de sauvegarder et de restaurer votre système ou de redémarrer complètement **Access Commander**.

Pour se connecter à Access Commander Box ou à une machine virtuelle, le client SSH doit connaître l'adresse IP d'**Access Commander** et le mot de passe de la racine du système. Le mot de passe de la racine du système peut être défini dans **Paramètres > Configuration > onglet SSH**.

NOTE
La modification du mot de passe root se fait dans la console de configuration, pas dans Access Commander.

L'accès SSH peut également être activé et géré directement dans la console de configuration Linux, voir Paramètres Linux (p. 90).

Clés de chiffrement pour l'application My2N

Les utilisateurs peuvent utiliser l'application My2N pour se connecter aux appareils 2N. La communication entre l'application My2N et l'appareil est toujours cryptée. **Access Commander** gère automatiquement les clés d'appariement du système qui sont distribuées aux appareils compatibles avec WaveKey afin de garantir un appariement sûr et fiable. Sans connaître la clé de cryptage, l'application My2N ne peut pas authentifier l'utilisateur. La clé de cryptage primaire est générée automatiquement lors du premier démarrage de l'interphone ou, dans le cas de la gestion **Access Commander**, dans le cadre de sa configuration. La clé peut être générée à nouveau manuellement à tout moment. Avec l'ID d'authentification, la clé de chiffrement principale est transmise au périphérique mobile pour le jumelage.

NOTE
Deux types de clés sont utilisés dans le système : les **clés de jumelage** et les **clés d'accès**. Les clés d'appairage sont utilisées pour authentifier l'application mobile My2N avec l'appareil. Les clés d'accès déterminent les droits d'accès aux fonctionnalités de l'application mobile.

Création de nouvelles clés

1. Allez sur **Settings > Authentication > Encryption Keys tab pour l'application My2N**.
   Vous pouvez générer jusqu'à 4 clés d'accès. Lorsque vous essayez de générer une cinquième clé, **Access Commander** vous avertit que la génération de cette clé supprimera la clé la plus ancienne. L'onglet énumère les temps de génération pour chaque clé.
2. Cliquez sur Générer une nouvelle clé.

   ASTUCE
   Pour des raisons de sécurité, il est recommandé de régénérer les clés d'appairage une fois par période prolongée (par exemple, une fois par an).
3. La clé nouvellement générée est automatiquement téléchargée sur l'application My2N la première fois que le téléphone mobile est utilisé avec un appareil précédemment apparié.

La clé générée peut être supprimée en cliquant sur .

ASTUCE
Pour un niveau de sécurité plus élevé, il est préférable de procéder à l'appariement en utilisant le **code QR** , qui contient la clé publique. Si le code QR n'est pas disponible, vous pouvez utiliser l'appairage à l'aide d'un code **PIN**.

ATTENTION
L'appairage par code QR n'est possible que sur les appareils dotés du micrologiciel HIP 2.50.0 ou d'une version ultérieure (y compris la série 3.0). Dans un environnement équipé de Access Commander, le code QR peut être affiché, mais l'appariement sur des versions plus anciennes de HIP ne sera possible qu'en utilisant **PIN**.

NOTE

- Si l'application My2N n'a accès à aucune clé de cryptage valide, elle ne peut pas être utilisée pour l'authentification de l'utilisateur. Pour rétablir la fonctionnalité de l'application, celle-ci doit être appariée à nouveau avec le dispositif connecté à Access Commander, qui téléchargera les clés de cryptage valides vers l'application My2N.
- L'autorisation d'accès à l'appareil dépend des droits d'accès définis par l'utilisateur.

Mode de compatibilité des cartes RFID

Si **Access Commander** signale que la toute nouvelle carte qui vient d'être ajoutée est déjà utilisée dans le système, la raison peut être que le mode de compatibilité des cartes RFID est activé. Ce mode est activé par l'administrateur dans **l'onglet Paramètres > Authentification > Mode de compatibilité**.

ATTENTION

- Le mode de compatibilité ne doit être activé qu'en cas de problème lors du chargement de cartes précédemment enregistrées. L'utilisation du mode de compatibilité peut affecter les mécanismes d'authentification
- Il est déconseillé de combiner le mode de compatibilité avec l'utilisation de cartes sécurisées par les technologies PiCard.

Clés PICard

Dans l'onglet **Paramètres > Accès > Clés PICard**, les clés de cryptage de l'application 2N PICard Commander sont stockées. Si les clés de chiffrement sont chargées dans **Access Commander**, l'onglet affiche le nom du projet PICard Commander et l'identifiant numérique d'exportation de la clé. L'onglet vous permet de supprimer les clés chargées dans **Access Commander**.

ATTENTION
Si vous supprimez les clés PICard, toutes les cartes chiffrées avec ces clés cesseront de fonctionner.

Importer les clés de chiffrement PICard

1. Allez sur **Settings > Access > PICard keys tab**.
2. Après avoir cliqué sur Importer téléchargez le fichier de clé de chiffrement depuis votre référentiel.
3. Entrez un mot de passe pour protéger le fichier si vous en définissez un lors de l'exportation depuis l'application PICard Commander.

2N PICard Commander est une application logicielle permettant de crypter les informations d'identification sur les cartes d'accès. L'application crée des projets qui génèrent un ensemble de clés de chiffrement et de lecture. Les clés du lecteur de projet peuvent être importées dans les appareils 2N ou dans **Access Commander**, qui assure ensuite la distribution des clés de lecture aux appareils 2N connectés.

Lecteurs USB activés

Pour faciliter l'enregistrement de certaines méthodes d'authentification des utilisateurs, vous pouvez utiliser des lecteurs USB connectés à l'ordinateur sur lequel vous accédez à **Access Commander**. Les lecteurs doivent être activés dans **Access Commander** sous **Paramètres > Accès > onglet Lecteurs USB autorisés**.

1. Allez sur **Settings > Access > USB Reader Enabled tab.**
2. Cliquez sur Enable Readers pour ouvrir la boîte de dialogue.
3. L'activation/désactivation de l'utilisation d'un périphérique USB externe s'effectue dans une boîte de dialogue.
4. Ensuite, leur habilitation de lecteur est modifiée en cliquant sur Change.

Access Commander permet l'utilisation des périphériques USB suivants :

- Lecteur de cartes RFID 125 kHz – N° de commande 9137420E, Partie AXE. Bien 01399-001
- Lecteur de cartes RFID 13,56 MHz et 125 kHz – N° de commande 9137421E , Partie AXE. Bien 01400-001
- Lecteur d'empreintes digitales - N° de commande 9137423E, Partie AXE. Bien 01401-001

Journaux CAM

Les journaux CAM sont utilisés pour enregistrer automatiquement plusieurs images précédant et suivant un événement sélectionné. Dans **Réglages > Journaux CAM**, vous pouvez gérer les différents types d'événements pour lesquels des journaux CAM doivent être générés.

Par exemple, des journaux CAM peuvent être générés à chaque insertion de carte. Si quelqu'un glisse la carte, 5 images avant le balayage et 3 images après le balayage seront enregistrées dans les journaux d'accès. Les images sont enregistrées après 1 seconde. Un stockage de 1, 3 ou 5 Go est créé pour les images. Si le stockage est plein, les images les plus anciennes seront supprimées. Les journaux d'accès eux-mêmes ne sont pas supprimés.

Création d'un type de journal CAM

1. Allez dans **Paramètres > Journaux CAM**.
2. Cliquez sur le bouton Ajouter dans le coin supérieur droit de la page.
3. Entrez un nom pour le type d'événement du journal CAM.
   Le type d'événement du journal CAM nouvellement créé s'affiche dans la liste et les détails du journal CAM s'ouvrent. Dans le détail du journal CAM, il est nécessaire de définir pour quels événements et sur quels appareils les images des caméras seront générées.

Définition des logos CAM

Les informations sur le type de journal CAM peuvent être gérées dans les détails du journal CAM. Le détail du journal CAM s'ouvre en cliquant sur le journal CAM sélectionné dans la liste ou après avoir créé un nouveau journal CAM.

Événements regardés

L'onglet permet de sélectionner une liste d'événements au cours desquels les images des caméras seront capturées.

Les événements suivis peuvent être les suivants :

- **Approches**
  - Utilisateur accepté
  - Plaque d'immatriculation de voiture reconnue
  - Utilisateur rejeté
  - Appuyez sur le bouton REX
- **Sécurité**
  - Interrupteur de protection activé
  - Ouverture de porte non autorisée
  - Ouverture de porte à distance
  - Accès refusé - saisie incorrecte répétée
  - Alarme silencieuse activée
- **Appel**
  - Appel initié

Appareils surveillés

Il est recommandé de définir l'enregistrement des journaux CAM uniquement à partir d'appareils équipés d'une caméra. La sélection de l'appareil s'effectue dans une fenêtre de dialogue qui s'ouvre avec . En même temps, la carte permet l'enregistrement des journaux CAM de tous les appareils.

Serrures électroniques

Le système **Access Commander** permet de gérer les accès au moyen de serrures électroniques 2N Fortis, qui sont déverrouillées par des cartes RFID dotées de la technologie MIFARE® DESFire®. Lors de la configuration des serrures électroniques, une clé de cryptage est attribuée à chaque serrure. Les clés de verrouillage sont ensuite stockées sur les cartes RFID des utilisateurs autorisés. Si les clés sur la carte et dans la serrure correspondent, le mécanisme de verrouillage est déverrouillé.

Une carte d'accès RFID peut être utilisée pour accéder à un maximum de 90 portes équipées de serrures 2N Fortis, en fonction du nombre de profils temporels appliqués. Si la capacité de mémoire de la carte est dépassée, l'écriture des données sur la carte échoue. L'échec de l'écriture est enregistré dans le journal des accès au système. En cas d'utilisation de groupes de fermeture, il est possible d'écrire plus de portes sur une seule carte qu'en cas d'affectation individuelle. En cas d'utilisation de groupes de fermeture, il est possible d'inscrire plus de portes par carte qu'en cas d'affectation individuelle.

Fortis Commander

Fortis Commander est une application autonome qui relie les serrures électroniques **Fortis** au système **Access Commander**. L'application définit les verrous en fonction du fichier de projet créé dans **Access Commander**u qui contient la configuration des verrous. Le fichier est crypté et ne peut être utilisé que sur une installation spécifique.

Installation

Fortis Commander est conçu pour être installé sur un ordinateur Windows prenant en charge la technologie Bluetooth Low Energy (BLE).

L'application est disponible sur le site web 2N Download Centre.

Procédure d'installation

1. Téléchargez le paquet d'installation à partir du lien fourni.
2. Exécutez le programme d'installation et terminez l'installation en suivant les instructions à l'écran.

Dossier de projet

Le fichier de projet est créé dans **Access Commander** et contient la configuration complète du projet. Le fichier est crypté et protégé par un mot de passe.

Mise en place de verrous dans Access Commander

Avant de télécharger des clés sur des serrures individuelles, vous devez coupler **Access Commander** avec **Fortis Commander**.

Génération de la clé de chiffrement principale (MEK) et préparation du projet

1. Connectez-vous à Access Commander.
2. Allez sur **Settings > Electronic locks**.
3. Dans l'onglet **Initial Settings** cliquez sur Generate Keys.
4. Créer la clé de chiffrement principale.

ATTENTION
La clé de cryptage principale ne peut pas être consultée ou modifiée ultérieurement .

NOTE
En fonction de la clé de chiffrement principale (MEK), **2N Access Commander** génère un ensemble de clés de chiffrement. La clé doit donc être unique et suffisamment sûre. Le jeu de clés est basé sur la clé de chiffrement principale, de sorte que les projets ayant la même clé de chiffrement principale génèrent les mêmes jeux de clés. Si un projet est perdu, un nouveau projet avec la même clé de chiffrement principale peut être créé et poursuivre le chiffrement.

5. Après avoir généré les clés et défini le mot de passe pour le fichier de projet, vous pouvez télécharger **le fichier de projet**, qui est une image de la configuration de la serrure électronique dans le système **Access Commander**.
6. Dans l'onglet **de Fortis Commander** cliquez sur Télécharger l'application **,** à partir duquel le téléchargement de **Fortis Commander** (application pour la configuration des serrures électroniques) commencera.

ATTENTION
Les informations sur le projet sont des données sensibles. Protégez-les contre les abus.

Configuration de la serrure électronique à l'aide de Fortis Commander

1. Installez **Fortis Commander** et ouvrez-le.
2. Cliquez sur Open project et ouvrez le fichier de projet téléchargé dans l'explorateur de fichiers.
3. Dans la boîte de dialogue qui s'affiche, saisissez le mot de passe du fichier de projet.

4. Après avoir ouvert le fichier de projet, sélectionnez Connect to device et attachez la carte de service à la serrure.
5. Cliquez sur **Assign**, qui attribue le verrou au projet.
6. Déconnectez l'appareil et cliquez sur **File > Close project**.
7. Lorsque la configuration est terminée, ouvrez le système **Access Commander**. Allez dans l'onglet **Settings > Electronic Locks** et cliquez à nouveau sur Fortis Commander. Téléchargez le fichier de projet.

NOTE
Lorsque vous déplacez la serrure d'une installation à l'autre ou lorsque vous faites une réclamation, vous devez effectuer une réinitialisation d'usine . Cette opération réinitialise la serrure aux paramètres d'usine et supprime toute configuration antérieure.

Procédure de mise à jour de la configuration

1. Apportez des modifications à **Access Commander**.
2. Téléchargez le nouveau fichier de projet.
3. Téléchargez le fichier sur **Fortis Commander** et apportez les modifications nécessaires aux serrures.
4. Si vous apportez d'autres modifications à **Access Commander**u, téléchargez toujours un nouveau fichier de projet.

ATTENTION
Pour chaque changement de configuration dans **Access Commander**u, vous devez télécharger un nouveau fichier de projet - vous ne pouvez pas utiliser un ancien fichier qui a déjà été téléchargé sur **Fortis Commander**.

Verrouillage et déverrouillage permanents

L'application vous permet de verrouiller et de déverrouiller la serrure en permanence. Cette fonction est utilisée pour les interventions de service ou les commandes d'urgence sans l'utilisation d'une carte.

Collecte d'événements à partir de serrures électroniques utilisant des cartes/puces RFID

Paramètres de la collecte d'événements

1. Ouvrez **Settings > Electronic locks > Tab events**.

2. Sélectionnez le type d'événement :
   - **Collecte des événements liés à l'accès et au système** - Tous les événements liés à l'accès et au système sont enregistrés sur la carte/puce et inscrits dans le journal du système et dans le journal d'accès .
   - **Collecter uniquement les événements du système** - seuls les événements du système sont enregistrés, les événements d'accès ne sont pas stockés sur les cartes.
   - **Ne collectez pas d'événements sur les onglets** - aucun événement n'est écrit dans l'onglet ; on ne peut y accéder que par l'intermédiaire de **Fortis Commander**u.

> **ASTUCE**
> La sélection d'un ensemble d'événements approprié peut réduire la charge du système et l'utilisation de l'espace de stockage. Néanmoins, une journalisation détaillée est importante pour les diagnostics et les audits de sécurité.

Exporter des événements à partir d'une carte

La carte stocke un maximum de **16 premiers événements**. Les événements peuvent être lus de deux manières :

- Dans **Access Commander**, cliquez sur l'icône dans la boîte de recherche de l'en-tête et chargez l'onglet.
- En utilisant un appareil avec **2N OS**, les événements sont lus sur la carte et envoyés à **Access Commander**u.

Téléchargement d'événements dans la serrure

1. Ouvrez **Settings > Electronic Locks > Fortis Commander** et cliquez sur Download File.
2. Ouvrez le fichier dans **Fortis Commander**.
3. Dans l'application **Fortis Commander**, connectez-vous à la serrure électronique.
4. Téléchargez le fichier mis à jour sur **Access Commander**.
5. Une fois téléchargés, les événements sont affichés sur **Access Logs** et **System Logs**.

Opérations de service

Ces opérations sont disponibles pour **Fortis Cylinder**:

- **Démontage** - démontage des serrures à des fins d'entretien.
- **Remplacement de la pile** - remplacement de la pile dans la serrure.

> **ATTENTION**
> Les opérations de service ne sont pas pertinentes pour d'autres types de serrures.

> **NOTE**
> En mode service, la serrure revient en mode normal en appuyant sur le bouton Lock pour se verrouiller définitivement.

Mise à jour de la carte

Les cartes d'accès utilisateur doivent être mises à jour régulièrement. L'utilisateur met à jour la carte en la connectant au périphérique IP 2N auquel il dispose de droits d'accès valides. La carte doit être maintenue

dans le lecteur de l'appareil jusqu'à ce que l'interrupteur d'ouverture de la porte soit activé. L'interrupteur d'ouverture de la porte n'est activé qu'après la mise à jour de l'accès aux serrures

Vous pouvez modifier la validité par défaut de dix jours des cartes à l'adresse **Settings > Electronic locks > Card Parameters tab**.

ATTENTION
Si vous modifiez les droits d'accès aux serrures dans **Access Commander**, les modifications ne seront répercutées sur la carte d'accès de l'utilisateur qu'après avoir été mises à jour sur le lecteur de cartes de l'appareil 2N ! Pour des raisons de sécurité, nous recommandons de fixer une période de validité plus courte pour les cartes afin de garantir leur mise à jour régulière.

Les lecteurs de dispositifs IP, qui permettent la mise à jour de la carte, et leur configuration sont décrits dans le chapitre Configuration du lecteur de périphérique IP (p. 31).

Cartes compatibles

NOTE
Pour les besoins de cette documentation, le terme **carte** désigne tout identifiant compatible utilisant la technologie MIFARE DESFire.

Pour ouvrir les serrures électroniques 2N Fortis, il n'est pas possible d'utiliser des cartes avec un ID aléatoire (random ID).

Les cartes avec la technologie PICard ne peuvent pas être utilisées pour ouvrir des serrures électroniques 2N Fortis.

Profils temporels sur les serrures électroniques

Les serrures électroniques prennent en charge des profils horaires avec les restrictions suivantes :

- Les vacances ne s'appliquent pas.
- Dans le cadre d'une journée, il est possible de définir jusqu'à 4 intervalles de temps différents.
- Dans le cadre d'un profil horaire, il est possible de définir 4 emplois du temps quotidiens.

ASTUCE
Cela signifie que vous pouvez avoir par exemple des réglages différents pour le lundi, le mardi, le mercredi et le jeudi, mais pour le vendredi, le samedi et le dimanche, vous devez utiliser l'un des réglages existants.

ATTENTION
Si le profil horaire enfreint les restrictions énoncées, la règle d'accès sera ignorée et l'utilisateur ne se verra pas accorder l'accès.

Cartes de maintenance

Les cartes d'entretien permettent un accès autorisé à la serrure. Ils permettent de mettre la serrure en service, de changer la batterie, de démonter la serrure.

ATTENTION
La carte de maintenance ne peut pas être utilisée en même temps comme carte d'accès utilisateur.

Paramètres de l'onglet Maintenance

1. Dans **Access Commander**, allez sur **Settings > Electronic Locks**.
2. Dans l'onglet Maintenance cliquez sur Créer.
3. Dans la boîte de dialogue qui s'ouvre, sélectionnez le type de carte que vous souhaitez créer.
   - Réglage de nouvelles serrures - active les nouvelles serrures configurées en usine en mode service.
   - Service - active le mode service pour la serrure déjà réglée.
   - Démontage - libère la serrure à cylindre 2N Fortis déjà installée pour le démontage, voir le manuel d'installation 2N Fortis.
   - Remplacement de la batterie - libère la serrure à cylindre 2N Fortis déjà réglée pour le remplacement de la batterie, voir le manuel d'installation de 2N Fortis.

   ASTUCE
   Une carte physique peut être chargée simultanément avec **Setting New Locks** et toute autre carte de service. Nous recommandons une combinaison de **Setting New Locks** et **Service**.
4. Cliquez sur Continuer à.
5. Attachez la carte au lecteur RFID USB connecté. Attendez que les données soient chargées sur la carte.

La validité des données sur la carte d'entretien est d'un an. Après cette période, il est nécessaire de supprimer les données et de reconfigurer la carte.

Dépannage

Journaux de diagnostic

Les journaux de diagnostic sont utilisés par le support technique pour identifier et résoudre les problèmes signalés. Les journaux contiennent des informations sur les actions effectuées, les erreurs, les changements de statut et d'autres événements pertinents.

Télécharger les journaux de diagnostic

1. Aller à **Paramètres > Dépannage > onglet Journaux de diagnostic**.
2. Cliquer sur Générer des journaux.
   La génération du package de journaux prend quelques minutes.
3. Une fois le deck prêt, il apparaîtra sur la carte et sera disponible Télécharger.

Statistiques d'utilisation

Si la fonction est activée, elle envoie **Access Commander** une fois par jour, des données anonymes sur les fonctions utilisées vers un serveur 2N sécurisé. Chaque envoi est effectué sous un identifiant unique, qui est automatiquement généré à nouveau à chaque nouvel envoi. L'intervenant 2N n'est donc pas en

mesure d'identifier l'installation donnée. **Access Commander**. Les informations obtenues sont utilisées pour améliorer le développement du produit, développer des fonctionnalités et améliorer l'expérience utilisateur.

Notification

Le module Notifications vous permet de configurer la surveillance des événements sélectionnés et des propriétés du système dont il a connaissance. **Access Commander** informer par e-mail ou notification dans la barre supérieure à côté du menu utilisateur.

La liste des notifications est également affichée sur la page **Journaux du système > Notifications**.

Les enregistrements peuvent être téléchargés dans un fichier CSV en cliquant sur le bouton Export au-dessus de la liste. Dans le fichier CSV exporté, l'heure est indiquée en GMT+0.

Configuration d'un nouveau type de notification

1. Aller à la page **Paramètres > Notifications**.
2. Cliquez sur le bouton Ajouter dans le coin supérieur droit de la page.
3. Saisissez un nom pour le nouveau type de notification.
   Après la création, le détail de la notification sera affiché, dans lequel il est possible de sélectionner les appareils pour lesquels la notification doit être surveillée ; ajouter les utilisateurs auxquels la notification doit être envoyée ; choisissez le mode de livraison des notifications.

Paramètres de notification

Les types de notification sont définis dans les détails du type de notification. Pour ouvrir les détails du type de notification, cliquez sur la notification sélectionnée dans la liste de la page **Paramètres > Notifications**.

Mode de notification

Dans cet onglet, les méthodes de notification et la liste des destinataires des notifications par e-mail sont définies.

Dans **Access Commander**, les notifications apparaissent sous l'icône dans la barre supérieure, à côté du menu utilisateur, ou dans **Journal du système > Notifications**.

Des e-mails de notification peuvent être envoyés aux utilisateurs gérés dans **Access Commander** et les destinataires extérieurs au système. Les utilisateurs peuvent être sélectionnés dans la liste. Les adresses e-mail des autres destinataires doivent être saisies manuellement.

NOTE
Pour le bon fonctionnement des notifications par e-mail, il est nécessaire que SMTP soit correctement configuré, voir Activation et configuration de la fonction E-mail (SMTP) (p. 103).

Appareils surveillés

Le type de notification donné peut être généré à la fois pour tous les appareils et uniquement pour certains appareils. Si Surveiller tous les appareils est activé, l'événement peut se produire sur n'importe quel appareil et une notification sera générée. Si la surveillance de tous les appareils est désactivée, une notification sera générée uniquement si l'événement se produit sur l'appareil sélectionné. La sélection de l'appareil s'effectue dans le menu qui s'ouvre avec .

Paramètres réseau

Pour configurer une connexion réseau, allez dans **Paramètres > Configuration > onglet Réseau**. L'onglet affiche les paramètres réseau actuels d'**Access Commander** et vous permet de les définir. Le réglage des paramètres individuels peut être effectué après avoir activé la méthode de configuration manuelle.

La méthode de configuration vous permet de définir les paramètres de configuration du réseau automatiquement à partir du serveur DHCP ou manuellement. Lors de la modification de l'adresse IP définie automatiquement du serveur DHCP par une adresse saisie manuellement, le navigateur Web sera redirigé vers l'adresse IP renseignée. Un redémarrage aura lieu après la redirection**Access Commander** et il est nécessaire de se reconnecter au système.

ATTENTION

- Si vous modifiez la méthode de configuration en DHCP, vous modifierez l'adresse IP du serveur et risquez de provoquer une interruption de la connexion.
- Si vous changez de serveur proxy HTTP,**Access Commander**redémarrera automatiquement.

Détection du changement d'adresse IP de l'appareil

Access Commander établit des connexions avec les appareils via leurs adresses IP. Pour éviter de perdre la connexion avec un appareil ayant une adresse IP dynamique, deux méthodes de détection des adresses IP des appareils sont disponibles.

- **Network Scanner**
  Access Commander analyse périodiquement le segment de réseau local à l'aide du 2N Network Scanner intégré afin d'identifier les appareils connectés et leurs adresses IP actuelles.
- **Device callback**
  Cette méthode permet de détecter les adresses IP des appareils situés en dehors du segment du réseau local. Les appareils sont signalés au démarrage, lorsque l'adresse IP change et à intervalles réguliers (une fois par heure). Pour que cette méthode fonctionne correctement, vous devez spécifier la destination vers laquelle les dispositifs seront signalés (généralement l'adresse IP de l'**Access Commander**).

Network Discovery

Network Discovery permet à d'autres services, tels que **2N IP Utility** ou **2N Network Scanner**, de trouver l'installation de **Access Commander** sur le réseau local.

Vous pouvez utiliser **Network Scanner** et **Axis Utility** en même temps. Cependant, pour des raisons de sécurité, les deux détections de **Access Commander** peuvent être complètement désactivées dans les paramètres du système.

ASTUCE
Access Commander peut être affiché ou caché dans les applications **2N Network Scanner** et **2N Axis Utility**. Il en va de même pour l'accès à l'interface web à l'aide de **accesscommander.local**. Si plusieurs instances d'Access Commander fonctionnent sur le réseau, le système attribue automatiquement des noms uniques : **accesscommander.local**, **accesscommander-2.local**, **accesscommander-3.local**, et d'autres instances en fonction du nombre de serveurs sur le réseau.

Paramètres du proxy

Le proxy est utilisé pour des services tels que Requêtes HTTP, synchronisation FTP, mises à jour, etc.

NOTE
Le proxy pour FTP avec authentification TLS n'est pas pris en charge.

1. Allez sur **Settings > Configuration > Network tab**.
2. Sélectionnez Edit proxy.
3. Dans la boîte de dialogue qui s'ouvre, saisissez les adresses des serveurs proxy pour les protocoles souhaités.
4. Dans le dernier champ, vous pouvez indiquer les adresses pour lesquelles le serveur proxy ne doit pas être appliqué.
   Les connexions à localhost et aux adresses IP de la plage 127.0.0.1/8 ne seront jamais acheminées par l'intermédiaire d'un serveur proxy.
5. Après avoir modifié les paramètres, **2N Access Commander** redémarre automatiquement.

Utilisation de NodeRED

L'application NodeRED ignore les paramètres proxy du système. Pour fonctionner correctement, le serveur proxy doit être explicitement configuré sur chaque nœud NodeRED qui nécessite son utilisation.

Informations Complémentaires

MIFARE and DESFire are registered trademarks of NXP B.V.

API HTTP

L'URL de l'API **Access Commanderu** est : https://acom_ip_address/api/v3/.

La liste des points de terminaison de l'API est publié sur http(s)://acom_ip_address/support/api . En dehors de l'interface **Access Commander**, vous pouvez consulter la liste des points de terminaison.

Vous pouvez filtrer les réponses aux demandes à l'aide de Query. La construction d'une **query** est décrite dans le document Data Query Customization (en anglais uniquement).

Authentification

Les commandes de l'API HTTP sont envoyées sous les données d'identification de l'utilisateur ou à l'aide d'une authentification par jeton. Le jeton d'authentification est créé par l'administrateur dans l'onglet **Paramètres > Configuration > clé d'accès à l'API**. La clé d'accès à l'API a la fonction de Bearer Token. Lors de la création d'une nouvelle clé d'accès à l'API, l'administrateur peut limiter la validité de la clé à la lecture seule, de sorte que la clé ne sera authentifiée que par les commandes GET. La validité de la clé peut être limitée à : 1 mois, 6 mois, 1 an.

ATTENTION
Après avoir créé la clé d'accès, copiez-la dans le presse-papier et utilisez-la. Plus trad, afficher la clé ne sera plus possible.

SignalR

SignalR est un outil qui permet une communication en temps réel entre le serveur et le client. Cela signifie que le serveur peut envoyer du contenu aux clients connectés dès que le contenu devient disponible et n'a pas besoin d'attendre une demande du client. Les principes de base de SignalR sont décrits dans le document SignalR integration manual (uniquement en anglais). Liste des sujets SignalR disponibles à utiliser avec **Access Commander** sont décrits dans le document SignalR topics reference manual (uniquement en anglais).

Licences tierces

Une liste complète des licences de bibliothèques tierces utilisées se trouve dans le menu utilisateur situé à droite de la barre supérieure, dans la section À propos.

2N Access Commander – Manuel d'installation

2N.com