2N Access Commander

Manuel de l'Utilisateur

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 les accès, il faut ajouter à Access Commander **Appareil**. Les appareils sont des unités physiques dans le bâtiment qui contrôlent les entrées (interphones 2N ou unités d'accès 2N) ou permettent la communication (unités de réponse 2N). Les appareils sont regroupés en **Zone**. Chaque appareil ne peut se trouver que dans une seule zone.

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.
- Ajout d'utilisateurs à des groupes.
- 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.

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 [33].

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 Verso
- 2N® LTE Verso
- 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

- 2N® Access Unit 2.0
- 2N® Access Unit
- 2N® IP Access Unit M

Unités de réponse 2N

- 2N® Indoor View
- 2N® Indoor Compact
- 2N® Indoor Talk
- 2N® Indoor Touch 2.0
- 2N® Clip
- 2N® Indoor Touch

Navigateurs Web

Configuration **Access Commander** se fait via l'interface web. Le système a été optimisé pour le navigateur Google Chrome (version 40 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 vShere (version 6.5 et supérieure)
- Hyper-V

Ports utilisés

Tableau 1. 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.

Licence

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 : *Basique* (gratuit), *Avancé*, *Pour* ou *Pour Illimité*, voir tableau de présentation des licences [9].

Licence:	Trial	Basic	Advanced	Pro	Pro Unlimited
Nombre maximum d'utilisateurs	5	50	300	1000	Illimité[a.]
Nombre maximum d'appareils (activés et désactivés)	1	5	30	100	Illimité[a.]
Nombre maximum d'administrateurs/gestionnaires	1	1	5	Illimité[a.]	Illimité[a.]
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	✓	✓	✓	✓	✓
Importer des utilisateurs depuis CSV ou depuis des appareils	✓	×	✓	✓	✓
Gestion groupée du firmware	✓	×	✓	✓	✓
Authentification multiple	✓	×	✓	✓	✓
Autorisation de l'utilisateur	✓	×	✓	✓	✓
Notification	✓	×	✓	✓	✓
Présence	✓	×	✓	✓	✓
Journaux CAM	✓	×	✓	✓	✓
Contrôle d'ascenseur	✓	×	✓	✓	✓
Tableau de bord	✓	×	✓	✓	✓
Verrouillage d'urgence	✓	×	✓	✓	✓
Prise en charge des informations d'identification mobiles	✓	×	✓	✓	✓
Gestion des visites	✓	×	✓	✓	✓
Gestion de l'occupation	✓	×	×	✓	✓
Synchronisation (LDAP et CSV)	✓	×	×	✓	✓
Anti-retour	✓	×	×	✓	✓

Licence:	Trial	Basic	Advanced	Pro	Pro Unlimited
Présence	✓	Facultatif	Facultatif	Facultatif	Facultatif

[a] Illimité dans les capacités maximales de la plate-forme logicielle, à savoir Matériel recommandé [13]

Installation

Access Commanderpeut être distribué de deux manières :

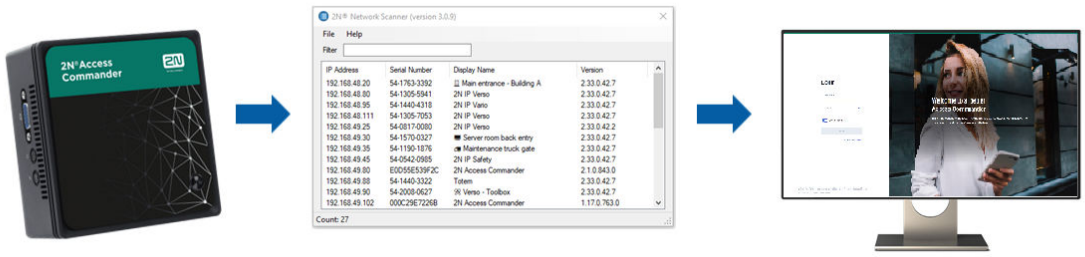
- Un petit ordinateur de bureau **2N®Access Commander Box**(n° de commande 91379030)
- Ordinateur virtuel

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

Distribution via Access Commander Box

Access Commander Box(n° de commande 91379030, Axis Part No. 01672-001) est un mini-ordinateur de bureau compact avec un logiciel préinstallé. Il s'agit d'une solution "plug and play", où il vous suffit de connecter une source d'alimentation 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. **Access Commander Box** sert de serveur pour collecter les données, les événements et les journaux de l'ensemble du système d'accès.

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. Utiliser l'application**2N®IP Network Scanner** Localiser **Access Commander Box** sur Internet.
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.

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 « racine » avec mot de passe « 2n ». Une fois l'écran bleu affiché, modifiez le mot de passe par défaut.
4. Dans le menu avancé, sélectionnez « La mise en réseau » et par la suite « I.P statique ».

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.

Distribution via machine virtuelle

Access Commanderpeut 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. DE https://www.virtualbox.org/wiki/Downloadstéléchargez la dernière version de VirtualBox.
   Il est recommandé de télécharger la version incluant le VirtualBox Extension Pack.
2. Téléchargez le logiciel approprié dans la section 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.

Lecteur VMware

ATTENTION

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

1. Téléchargez le logiciel approprié dans la section 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 vShere

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

1. Téléchargez le logiciel approprié dans la section Logiciel et micrologiciel sur 2N.com. Après le téléchargement, décompressez le fichier.
2. Dans VMware vShere, 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).
   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 dans la section 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 boutonFinition.

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

Le nombre d'appareils connectés affecteAccess 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 Commander** 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.

Tableau 2. Matériel de machine virtuelle

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

Tableau 3. Access Commander Box

Nombre d'appareils connectés 2.0	Nombre d'utilisateurs 2,0	Nombre d'utilisateurs dans le groupe
2000	100000	1500

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.

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 communiquer au distributeur le numéro de série d'un des appareils 2N connectés à Access Commander. *Fichier de licence* est généré en fonction du numéro de série de cet appareil sous licence.

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 surActiver 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.
période de protection	Le temps après la déconnexion de l'appareil sous licence pour lequel la licence reste valide. Les durées des périodes de protection sont indiquées dans Suspension du permis [15].

Suspension du permis

La suspension de la licence se produit si l'appareil sous licence est déconnecté deAccess Commanderpour une durée supérieure à la durée 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 Access Commander. Les durées des périodes de protection sont indiquées dans tableau ci-dessous [15].

Lorsqu'une licence est suspendue, tous les appareils connectés ne sont automatiquement pas gérés et marqués comme non gérés. Pour les réactiver, vous devez vous connecter et activer l'appareil sous licence ou faire générer et télécharger un nouveau fichier de licence pour un autre appareil.

Dans le cas du téléchargement d'une nouvelle licence, vous devez d'abord activer le périphérique de licence pour lequel la nouvelle licence est générée. Après avoir activé l'appareil sous licence, il sera également possible d'activer tous les autres appareils.

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

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 [11].*

Interface **Access Commander** est accessible via un navigateur Web. L'adresse IP de l'interface Web peut être recherchée à l'aide du programme **2N® Scanner réseau**.

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.

Tableau de bord

Le tableau de bord est la vue de base de l'interface Web **Access Commander**. Il s'agit d'un tableau d'affichage configurable affichant des données en temps réel. **Access Commander** propose plusieurs Widgets qui s'ajoutent au Dashboard à l'aide d'un bouton . Les widgets du tableau de bord peuvent être déplacés, renommés ou leurs paramètres de base peuvent être définis de différentes manières. La gestion et la suppression des Widgets se font 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'icône utilisateur dans le coin supérieur droit pour ouvrir le menu utilisateur.
2. Sélectionnez Changer la langue.
3. Sélectionnez la langue appropriée et confirmez avecChanger de langue.

Change ta photo de profil

1. Cliquez sur l'icône utilisateur dans le coin supérieur droit pour ouvrir le menu 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

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.

Journaux système

La page Journaux système affiche une liste d'événements et de notifications qui Access Commander généré.

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

- gravité (info, avertissement, erreur) ;
- l'heure à laquelle l'événement s'est produit ;
- la catégorie à laquelle appartient l'action (État de l'appareil, importation, synchronisation de l'utilisateur, système, actions de l'utilisateur, restrictions de zone) ;
- sujet sur lequel porte l'action (appareil, utilisateur, zone, visite...) ;
- 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 ou imprimés en cliquant sur un boutonExporter 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

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 ou imprimés en cliquant sur un boutonExporter au-dessus de la liste. Dans le fichier CSV exporté, l'heure est indiquée en GMT+0.

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.

Configuration d'un nouveau type de notification

1. Aller à la page **Paramètres** > **Notification**.
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 le détail du type de notification donné. Le détail du type de notification s'ouvre en cliquant 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.

La notification dans Access Commander apparaîtra 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) [50].

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.

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.

Mobile Key

En entreprise, il est possible de paramétrer les paramètres d'appairage avec l'application **2N® Mobile Key**, qui permet l'authentification Bluetooth. Les appareils sur lesquels les utilisateurs pourront s'appairer ainsi que la durée de validité de la clé mobile nécessaire à l'appairage sont définis. La clé mobile elle-même est générée 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.

Il est également possible de sélectionner les modalités selon lesquelles la visite peut être accordée.

En savoir plus sur la configuration des visites dans Visites [42].

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
- Mobile Key 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

Utilisateurs

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

Tous les utilisateurs créés sont affichés dans la liste des utilisateurs. Les utilisateurs peuvent être filtrés au-dessus de la liste ou vous pouvez rechercher directement un utilisateur spécifique par son nom, son e-mail ou son numéro de téléphone.

Actions de masse

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

- 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
- Attribuer une clé mobile aux utilisateurs de la sélection qui n'ont pas encore reçu de clé mobile

NOTE
Afin d'attribuer un code PIN/QR ou une clé 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.

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.

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 lu en approchant la carte du lecteur 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.

Mobile Key – utilisé pour se connecter à l'application **2N® Mobile Key** activation de l'authentification via Bluetooth, voir chapitre Authentification Bluetooth [25].

Code PIN – génère automatiquement un code PIN à 6 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.

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 [25].

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. Lors de la première connexion, l'utilisateur sera invité à modifier le mot de passe. Une fois connecté, l'utilisateur peut suivre sa présence (si disponible), modifier son email ou changer sa photo de profil.

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 [6].

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 vAccess Commander;
- **Numéro d'utilisateur** – identifiant spécifique, nécessaire à la synchronisation en masse avec un fichier CSV (voir Synchronisation des utilisateurs [52]);
- **Une note**.

Approches

L'onglet accès permet d'affecter l'utilisateur à un groupe et de définir l'intervalle de temps pendant lequel les données d'accès de l'utilisateur seront valides. L'intervalle de temps est défini dans le menu étendu de la carte, qui s'ouvre en cliquant sur ⋮.

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.

Le numéro de téléphone virtuel peut être utilisé pour appeler l'utilisateur à l'aide du clavier numérique de l'appareil. Un numéro virtuel peut comporter de deux à quatre chiffres. Les numéros virtuels ne sont pas liés aux numéros de téléphone de l'utilisateur, ce qui permet aux utilisateurs de masquer leurs propres numéros de téléphone sur l'appareil. Dans l'onglet, il est également possible de définir un correspondant vers qui l'appel sera renvoyé 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 2 empreintes digitales. Utilisez un lecteur d'empreintes digitales externe pour les télécharger. Vérifiez si le pilote est installé**2N®USB Driver**. Le pilote est disponible en téléchargement 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 qu'il est dans **Paramètres** > **Approches** lecteur d'empreintes digitales USB activé.
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 **Mobile Key**, que l'utilisateur doit avoir téléchargé sur son téléphone mobile.

GET IT ON Google Play Download on the App Store

Connexion de l'application sur le téléphone de l'utilisateur avec les appareils v Access Commander se fait en saisissant le code d'appairage dans l'application **Mobile Key**.

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

- via un lecteur USB Bluetooth connecté à un ordinateur
- connexion à l'appareil.

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 le **Paramètres** > **Approches** > **l'onglet Lecteurs USB activés**.
3. Connectez le lecteur USB Bluetooth à l'ordinateur.
4. Dans les paramètres utilisateur v **Onglet Authentification** choisir l'authentification Mobile Key.

5. Dans la boîte de dialogue qui s'ouvre, sélectionnezAssocier à l'aide d'un lecteur.
   Un code d'appairage apparaîtra dans la boîte de dialogue.
6. Suivez la procédure ci-dessous pour effectuer le couplage dans l'application ci-dessous [26].

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 [36];
   - un moment adéquat pour l'appairage est défini, à savoir???.
2. Dans les paramètres utilisateur v **Onglet Authentification** choisir l'authentification Mobile Key.
3. Dans la boîte de dialogue qui s'ouvre, sélectionnezAssociez-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 pour effectuer le couplage dans l'application ci-dessous [26].

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.

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. .

ATTENTION

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

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.

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. Mobile Key
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.

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.

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 ou imprimés en cliquant sur un boutonExporter 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

Ajouter un nouvel appareil

1. Aller à la page **Appareil**.
2. Cliquez sur le bouton Ajouter un appareil dans le coin supérieur droit.
3. Dans la fenêtre de dialogue ouverte, recherchez l'appareil sur le réseau local ou écrivez son adresse IP et le port correspondant au format :« Adresse : 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.
4. 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.
5. Nommez l'appareil avant de le créer.

Les appareils nouvellement ajoutés apparaissent dans la liste. Effectuez d'autres réglages de l'appareil dans les détails de l'appareil.

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 dispose Access Commander connexion établie et sur lequel le firmware accepté est chargé. Grâce à la connexion établie avec l'appareil, la synchronisation des données peut avoir lieu. Un firmware incompatible peut être activé sur la page **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. Un point d'accès à un 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.

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 [33].

Sauvegarde

Permet la sauvegarde de la configuration de l'interphone dans un fichier XML. La dernière sauvegarde est affichée sur l'onglet. En même temps, il est possible de télécharger de nouvelles données de configuration du fichier XML stocké sur la carte.

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. Aller à **Appareil** > détail 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

Utilisation de la connexion du module relais**AXE A9188** à **Interphone IP 2N** (**2N®Verso IP**,**2N®Force IP**,**2N®Sécurité IP**,**2N®Variateur IP**) ou pour **Unité d'accès** l'accès aux différents étages du bâtiment peut être contrôlé à l'aide d'un ascenseur. À une **Interphone IP 2N** dont **Unité d'accès** il est possible de connecter au maximum ces 5 modules relais, tandis que chacun des modules peut contrôler 8 étages, soit un maximum de 40 étages au total. Pour utiliser cette fonction, vous devez disposer d'une licence active pour **Interphones IP 2N** (n° de commande 9137916) et licence **Unité d'accès** (n° de commande 9160401).

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.

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.

Surveillance

La page permet de trouver des informations sur les appareils connectés. Chaque administrateur peut dresser la table selon ses propres besoins en utilisant . Le paramètre est unique pour chaque compte. Les paramètres sont effectués en sélectionnant les colonnes affichées.

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.

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.

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

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.

Exclusion de périphérique

Les appareils peuvent être exclus de la gestion groupée du micrologiciel en les ajoutant à la liste dans l'onglet Appareils > Micrologiciel > Appareils exclus.

Version du micrologiciel incompatible

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 utilisant une version de micrologiciel non prise en charge si cette version est approuvée. L'approbation s'effectue dans l'onglet Appareil > Micrologiciel > Version du micrologiciel incompatible 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 micrologiciel prises en charge

- 2.42
- 2.41
- 2.40
- 2.39
- 2.38
- 2.37

Sécurité

Après avoir activé la vérification du certificat SSL, la synchronisation n'aura lieu que sur les appareils dotés d'un certificat SSL signé par une autorité de confiance. La synchronisation des appareils sans ces certificats SSL sera désactivée.

Pour une authentification réussie, les certificats d'appareil doivent être signés par une autorité de certification et contenir l'adresse IP ou le nom de domaine de l'appareil. Le certificat de l'autorité signataire doit être approuvé par le serveur sur lequel il s'exécuteAccess Commander. Les certificats de périphérique doivent être téléchargés via l'interface Web de l'appareil (Système > Certificats > Certificats personnels) et définis en tant que certificat de serveur HTTPS dans Services > Serveur Web > Paramètres avancés.

ATTENTION

Sur l'appareil**2N®Touche intérieure**ne peut pas télécharger ses propres certificats SSL, après avoir activé la vérification des certificats, la connexion avec eux sera perdue.

Paramètres du périphérique d'entrée/sortie

1. Entrez la configuration Web de l'appareil.

   ASTUCE
   Il est possible de saisir la configuration web de l'appareil directement dans l'interface depuis les paramètres de l'appareil.

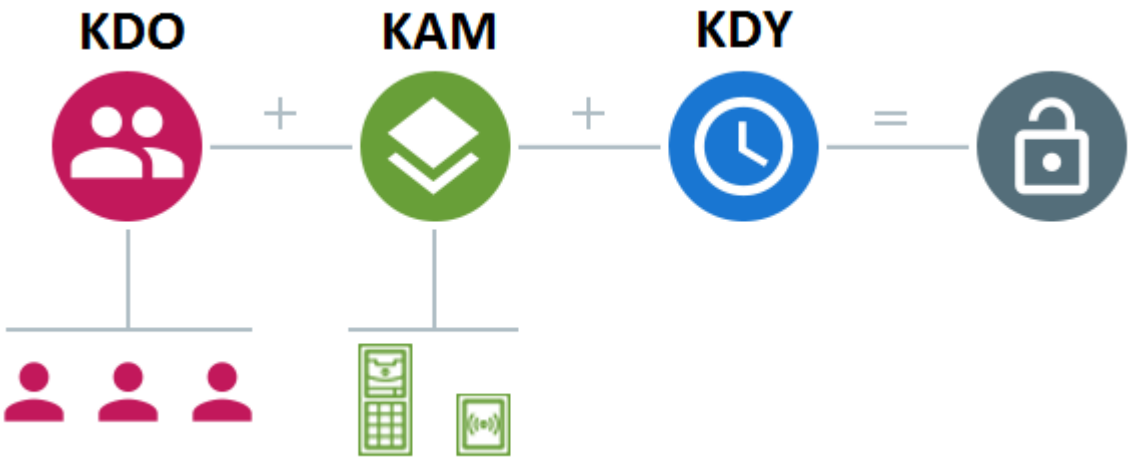
2. Accédez à la section Matériel > Menu Modules d'extension.
3. Localisez le module d'accès à utiliser comme entrée/sortie.
4. Dans le paramètre Porte, définissez la direction souhaitée et enregistrez les paramètres.

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 [38]. 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.

Création d'un profil horaire

1. Aller à la page **Profils horaires**.
2. Cliquez sur le bouton pour ajouter un profil horaire dans le coin supérieur droit.
3. Dans la boîte de dialogue ouverte, définissez le nom du profil horaire.
4. Sélectionnez une option pour choisir une limite de temps Ajouter des plages horaires. Les jours verts identifient les jours correspondant au profil horaire. Le jour est sélectionné en cliquant. En quelques jours, il est possible de définir un intervalle de temps déterminant la validité du profil horaire.
   Des heures différentes pour chaque jour ne peuvent être définies que lors de la création du profil horaire.

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.

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 fréquentation et son mode s'effectue en **Paramètres** > **Configuration** > **l'onglet Présence**, voir Paramètres de présence [39].

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

Suivi des présences

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 les données de présence de tous les utilisateurs dans un fichier CSV. 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.

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.

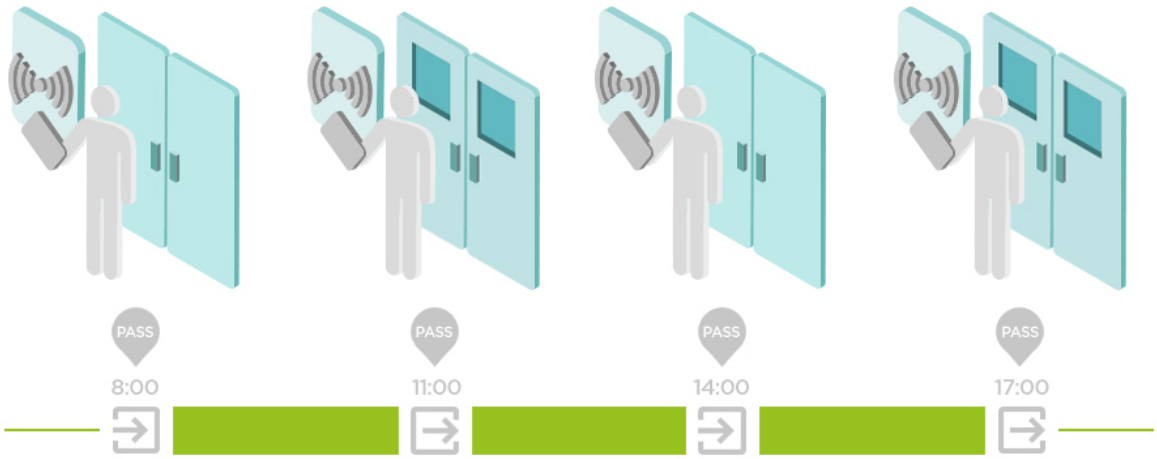
Il y a un menu d'extension à côté du nom de l'utilisateur permettant le téléchargement des données de présence de l'utilisateur affiché soit dans un fichier CSV ou PDF. Les deux fichiers contiennent des enregistrements de jours individuels.

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

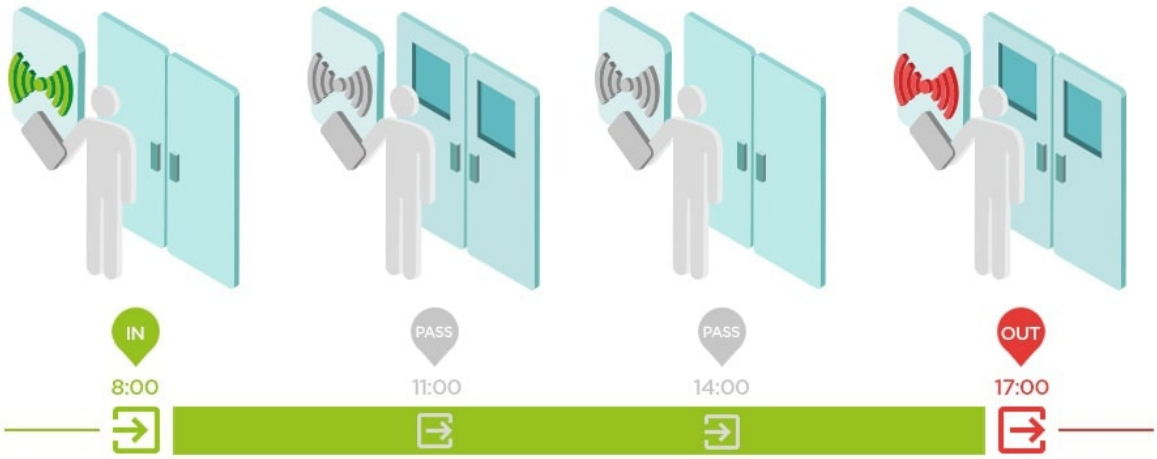
- **FREE**



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**

  Les appareils entrants et sortants doivent être configurés pour fonctionner correctement.



  - **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 périphérique d'entrée/sortie

1. Entrez la configuration Web de l'appareil.

> **ASTUCE**
> Il est possible de saisir la configuration web de l'appareil directement dans l'interface depuis les paramètres de l'appareil.

2. Accédez à la section Matériel > Menu Modules d'extension.
3. Localisez le module d'accès à utiliser comme entrée/sortie.
4. Dans le paramètre Porte, définissez la direction souhaitée et enregistrez les paramètres.

Visites

Dans Access Commanderil 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 un mois.

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 boutonFin 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 [42].

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 [43].

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 sous-page Cartes est utilisée pour gérer les cartes d'accès des visiteurs qui peuvent être ajoutées à une visite. Une nouvelle carte est ajoutée à l'aide du bouton Ajouter dans le coin supérieur droit.

ATTENTION

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

Présence

Le module de présence est une extension du module de présence et permet d'afficher une liste des utilisateurs qui se trouvent actuellement dans le bâtiment. Pour le fonctionnement du module, il est nécessaire de configurer le mode de présence IN-OUT v **Paramètres** > **Configuration** > **l'onglet Présence**, voir Paramètres de présence [39].

- Si le dernier événement de l'utilisateur un jour donné est une arrivée (**DANS** événement), est considéré comme présent.
- Si l'utilisateur passe par un lecteur dont la direction n'est pas spécifiée, la zone dans laquelle se trouve l'utilisateur changera. La même chose se produit s'il passe par le lecteur en mode**DANS**.
- Si le dernier Événement d'un jour donné est un départ (**DEHORS** événement), 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.

- **Mobile Key** – 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 **Mobile Key**, 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 [52].

  ATTENTION
  Le fichier contient des données sensibles !

Restrictions de zone

Les restrictions de zone permettent de définir les zones dans lesquelles les fonctions Anti-passback et Occupation peuvent être utilisées.

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.

Définition de restrictions de zone

Entrée et sortie

Ces cartes indiquent quels appareils sont acheminés en entrée ou en sortie dans une zone donnée. Utilisation du menu étendu sous ⋮ les appareils peuvent être déplacés entre les onglets ou supprimés de la zone.

Occupation

Les appareils entrants et sortants doivent être configurés pour fonctionner correctement.

L'onglet Occupation vous permet de surveiller et de contrôler le nombre de personnes dans une zone. Les restrictions d'occupation aident à gérer le nombre de personnes dans une zone. Si la limite d'occupation est atteinte, il est possible de refuser d'autres accès ou de n'enregistrer que le dépassement de la limite. Un périphérique d'entrée et de sortie est requis pour cette fonction.

Anti-retour

Il est possible d'activer la fonction Anti-passback dans la zone, qui assure l'extension du contrôle d'accès par surveillance et utilisation abusive des droits de réentrée dans les zones réservées. Les zones surveillées sont délimitées par des dispositifs frontaliers qui mènent ou permettent de sortir des locaux. Sur ces appareils, lors du passage des personnes, l'autorisation est vérifiée selon les règles définies pour la zone donnée. Après avoir quitté la zone via le dispositif frontalier, l'utilisateur ne peut revenir dans la zone qu'après l'expiration du délai d'attente, si le délai d'attente est défini. Si l'utilisateur tente de revenir dans la zone plus tôt, le système lui refusera l'accès ou enregistrera uniquement cet événement dans le journal.

AVERTISSEMENT
Une zone anti-passback perd son sens et peut être potentiellement dangereuse s'il y a dans la zone un périphérique avec un bouton REX actif connecté qui autorise un accès non autorisé.

Définir une exception

Il peut parfois être souhaitable que les conditions anti-passback ne s'appliquent pas aux utilisateurs sélectionnés. Il s'agit généralement d'utilisateurs tels que le gestionnaire du bâtiment, le PDG, les utilisateurs VIP, etc. Les utilisateurs ou des groupes entiers qui ne doivent pas être soumis aux conditions 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 les utilisateurs qui ont tenté d'accéder à la zone Anti-passback avant l'expiration du délai d'attente. Aide ✕ les utilisateurs peuvent être exclus de la liste, leur permettant ainsi d'accéder à nouveau à la zone.

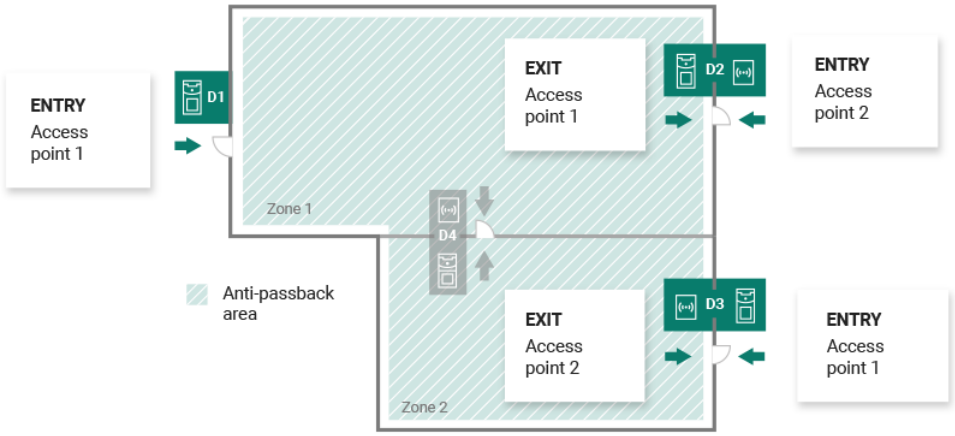
ASTUCE

Lorsqu'un utilisateur se voit refuser l'accès en raison d'un anti-passback actif, un e-mail d'information automatique peut être envoyé à l'utilisateur. Vous pouvez activer l'envoi d'e-mails dans l'onglet Paramètres > Anti-passback > Notifier l'utilisateur bloqué par e-mail.

Réinitialisation des restrictions

Dans Paramètres > Anti-passback > Réinitialiser les restrictions de zone, les jours et heures auxquels l'enregistrement de zone sera supprimé sont définis, c'est-à-dire tous les utilisateurs pourront repasser, quelles que soient les violations précédentes.

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

Date et l'heure

Date et heure dans Access Commander peut être synchronisé avec Internet ou réglé manuellement. La modification de la méthode d'acquisition de l'heure s'effectue dans l'onglet Paramètres > Configuration > Date et heure. Au cas où ce ne serait pas le cas Access Commander connecté à Internet, vous devez régler manuellement la date, l'heure et le fuseau horaire. Sinon, il est possible de passer en NTP et d'obtenir l'heure d'un serveur NTP. Dans ce cas, il vous suffit de définir le fuseau horaire. Le serveur NTP met automatiquement à jour la date et l'heure.

ATTENTION

Après avoir enregistré le changement d'heure Access Commanderredémarre automatiquement.

Synchronisation de l'heure avec les appareils

L'heure sur les appareils connectés peut être unifiée avec l'heure Access Commander. Le partage du temps avec les appareils est activé en activant le paramètre Synchroniser avec l'appareil dans Paramètres > 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.
- **Les appareils utilisent Access Commander comme serveur NTP** – contrôle l'heure sur les appareils en fonction de l'heure réglée dansAccess Commander.

Paramètres réseau

Les paramètres de connexion réseau sont définis dans l'onglet Paramètres > Configuration > Réseau. L'onglet affiche les paramètres réseau actuels Access Commander et permet de les définir. Il est possible de définir des paramètres individuels 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 redirectionAccess 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 Commanderredémarrera automatiquement.

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.

Les paramètres sont définis dans Paramètres > Configuration > E-mail.

1. 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.
2. 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).
3. 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.
4. Vous pouvez vérifier les paramètres effectués en envoyant un email de test.

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. La vérification automatique des mises à jour peut être désactivée dans l'onglet Paramètres > Mises à jour du système.

Installez la mise à jour Access Commander

AVERTISSEMENT

Il est recommandé de le faire avant d'installer la mise à jour sauvegarde du système [51]. 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 deAccess Commanders'inscrire.
5. Une fois l'installation terminée, cliquez sur Allez vous connecter, qui vous redirigera vers la page de connexion.

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'activation se fait dans Paramètres > onglet Mise à jour du système > Paramètres du serveur de mise à jour.

AVERTISSEMENT

La version d'essai n'est pas garantie et la société ne la fournit pas **2N TELEKOMUNIKACE comme** 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

Sur la page Paramètres > onglet Sauvegarde du système, il est possible d'effectuer, de configurer et de contrôler la sauvegarde et la restauration des données.Access Commander. Les données peuvent être stockées sur un stockage local ou sur Server Message Block (SMB). SMB convient au stockage à long terme des sauvegardes.

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 surSauvegarder 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.

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.

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 surRestaurer à partir d'un fichier.
3. Sélectionnez le fichier de sauvegarde dans votre stockage et cliquez surRestaurer.

Transférer des données d'un autre Access Commander

1. Aller à **Paramètres** > **Onglet Sauvegarde du système**.
2. En bas de l'onglet, cliquez surÉmigrer.
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

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**. Vous pouvez télécharger un exemple de fichier CSV à partir de la carte, voir ci-dessous [53].

ASTUCE
La liste des utilisateurs actuels, qui correspond à la structure de l'exemple de fichier CSV, peut être téléchargée depuis la page Rapports [45].

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. Cliquer sur dans le paramètre Stockage.
2. Dans la boîte de dialogue ouverte, définissez l'adresse du serveur FTP sur lequel le fichier CSV est stocké.
3. Entrez les informations d'identification pour accéder au serveur FTP.

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 :

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.

- 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.

Lecteurs USB activés

Pour faciliter l'enregistrement de certaines méthodes d'authentification des utilisateurs, il est possible d'utiliser des lecteurs USB connectés à l'ordinateur sur lequel le Access Commander. Les lecteurs sont requis dans Access Commander activez dans Paramètres > Accès > onglet Lecteurs USB autorisés.

L'activation/désactivation de l'utilisation d'un périphérique USB externe se fait dans une boîte de dialogue qui s'ouvre en cliquant sur Activer les lecteurs. Par la suite, leur autorisation est modifiée en cliquant sur Modifier.

Access Commander permet l'utilisation des périphériques USB suivants :

- **Lecteur de cartes RFID 125 kHz – N° de commande 9137420E**
- **Lecteur de cartes RFID 13,56 MHz et 125 kHz – N° de commande 9137421E**
- Lecteur d'empreintes digitales - **N° de commande 9137423E**
- Lecteur Bluetooth USB externe (dongle) – **N° de commande 9137422E**

Clés PICard

Les clés de cryptage de l'application sont stockées dans l'onglet Paramètres > Accès > Clés PICard **2N® PICard Commander**. Si les clés de chiffrement sont dans Access Commander téléchargé, le nom du projet est affiché sur l'onglet **PICard Commander** et un identifiant d'exportation de clé numérique. La carte permet de télécharger des clés depuis Access Commander supprimer.

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

Importer les clés de chiffrement PICard

1. Après avoir cliqué sur Importer téléchargez le fichier de clé de chiffrement depuis votre référentiel.
2. 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.

Clés de chiffrement pour clé mobile

Les utilisateurs peuvent utiliser l'application pour se connecter aux appareils 2N **Mobile Key**. Communication entre applications **Mobile Key**et est toujours crypté par l'appareil. Sans connaissance de la clé de chiffrement, l'application ne peut pas**Mobile Key**authentifier l'utilisateur. La clé de cryptage primaire est automatiquement générée lors du premier démarrage de l'interphone et peut être régénérée manuellement à tout moment ultérieurement. La clé de cryptage principale est transférée avec l'ID d'authentification à l'appareil mobile lors du couplage.

Mobile Key. Communication entre applications **Mobile Key**et est toujours crypté par l'appareil. Sans connaissance de la clé de chiffrement, l'application ne peut pas**Mobile Key**authentifier l'utilisateur. La clé de cryptage primaire est automatiquement générée lors du premier démarrage de l'interphone et peut être régénérée manuellement à tout moment ultérieurement. La clé de cryptage principale est transférée avec l'ID d'authentification à l'appareil mobile lors du couplage.

DANS **Paramètres > Accès > onglet Clés de cryptage pour clé mobile** il est possible de générer jusqu'à 4 clés de chiffrement. La clé nouvellement générée est automatiquement téléchargée sur l'application **Mobile Key** la première fois que vous utilisez un téléphone mobile avec un appareil précédemment couplé. Lorsque vous essayez de générer la cinquième clé Access Commander avertit que sa génération supprimera la clé la plus ancienne. La carte montre les temps de génération des clés individuelles.

S'il n'a pas d'application **Mobile Key** accès à l’une des clés de cryptage valides, il ne sera pas possible de l’utiliser pour authentifier l’utilisateur. Pour restaurer les fonctionnalités de l'application, il est nécessaire de réappairer l'application avec l'appareil connecté à Access Commander, qui téléchargera des clés de cryptage valides dans l'application **Mobile Key**.

NOTE
L'autorisation d'accès à l'appareil dépend des droits d'accès définis par l'utilisateur.

Journaux CAM

Les journaux CAM sont utilisés pour enregistrer automatiquement plusieurs images précédant et suivant l'événement sélectionné. Dans Paramètres > Journaux CAM, vous pouvez gérer 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. Aller à la page **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 :

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

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.

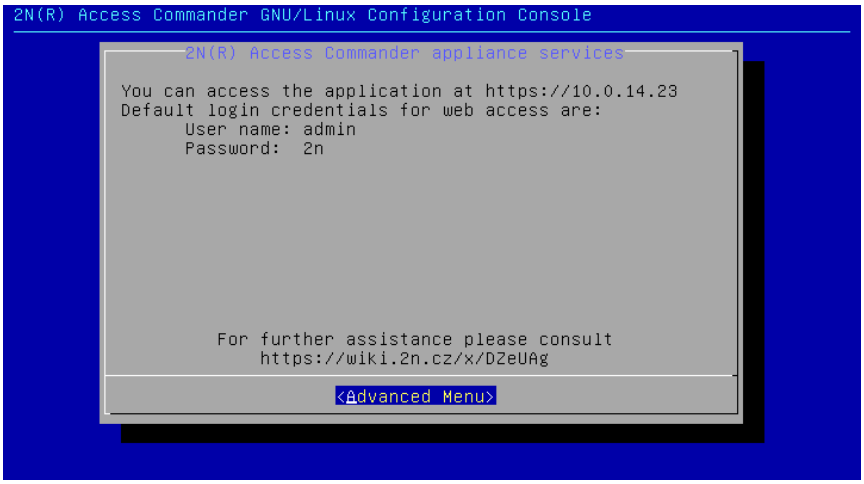
Paramètres Linux

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

NOTE

Si c'est**Access Commander**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.
- **Sauvegarde et restauration**
  Utilisé pour importer des données et une configuration, définir des sauvegardes répétées, restaurer à partir de sauvegardes antérieures.

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.

Dans Paramètres > Configuration > l'onglet SSH est utilisé pour activer Secure Shell, qui fournit une communication à distance sécurisée avec la console système. Avec le service SSH activé, vous pouvez sauvegarder et restaurer votre système ou effectuer un redémarrage completAccess Commander.

Se connecter **Boîte de commande d'accès** ou une machine virtuelle, le client SSH doit connaître l'adresse IP Access Commander et le mot de passe root du système. Le mot de passe root du système

peut être défini dans l'onglet Paramètres > Configuration > SSH. 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 [56].

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.

Informations Complémentaires

HTTP API

Une liste des points de terminaison de l'API est publiée sur http(s)://acom_ip_address/support/api.

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 de l'Utilisateur

2N.com