Access Management System V5.2

Configuration et opération

fr Software manual

Table des matières

1 Sécurité

Utiliser les derniers logiciels

Avant d'utiliser le dispositif pour la première fois, assurez-vous d'avoir installé la dernière version applicable du logiciel. Afin de garantir la cohérence de la fonctionnalité, de la compatibilité, des performances et de la sécurité du dispositif, mettez régulièrement à jour son logiciel tout au long de sa durée de vie. Suivez les instructions contenues dans la documentation produit concernant les mises à jour logicielles.

Pour plus d'informations, cliquez sur les liens suivants :

- Informations générales : https://www.boschsecurity.com/xc/en/support/product-security/
- Conseils de sécurité, avec une liste des vulnérabilités et des solutions possibles : https://www.boschsecurity.com/xc/en/support/product-security/security-advisories.html

Bosch n'assume aucune responsabilité pour tout dommage causé par le fait que les produits livrés ont été mis en service avec du firmware obsolète.

2 Utilisation de l'aide

Comment utiliser ce fichier d'aide.

Boutons de la barre d'outils

Bouton	Fonction	Description
	Masquer	Cliquez sur ce bouton pour masquer le volet de navigation (onglets Contenu, Index et Recherche) en ne laissant que le volet d'aide visible.
	Afficher	Lorsque vous cliquez sur le bouton Masquer, celui-ci est remplacé par le bouton Afficher. Cliquez sur ce bouton pour rouvrir le volet de navigation.
	Retour	Cliquez sur ce bouton pour revenir aux rubriques les plus récemment consultées.
	Avancer	Cliquez sur ce bouton pour suivre de nouveau la même chaîne de rubriques
	Imprimer	Cliquez sur ce bouton pour imprimer. Choisissez entre « Imprimer la rubriques sélectionnée » et « Imprimer l'en-tête sélectionné et toutes les sous-rubriques ».

Onglets

Contenu Cet onglet affiche une table des matières hiérarchique. Cliquez sur une icône représentant un livre  pour l'ouvrir  , puis cliquez sur une icône représentant une rubrique  pour l'afficher.

Index Cet onglet affiche un index de termes classés par ordre alphabétique. Sélectionnez une rubrique dans la liste ou saisissez un mot pour trouver la ou les rubrique(s) le contenant.

Recherche Utilisez cet onglet pour rechercher du texte. Entrez le texte dans le champ puis cliquez sur le bouton : **Liste des rubriques** pour rechercher des rubriques contenant tous les mots saisis.

Redimensionner la fenêtre d'aide

Faites glisser le coin ou le bord de la fenêtre jusqu'à la taille souhaitée.

Autres conventions utilisées dans cette documentation

– Le texte littéral (étiquettes) de l'interface utilisateur apparaît en **gras**. Par exemple, **Outils, Fichier, Enregistrer sous...**

- Les séquences de clics sont concaténées à l'aide du caractère **>** (signe supérieur à).
  Par exemple, **Fichier > Nouveau > Dossier**
- Les changements de type de contrôle (par exemple, menu, case d'option, case à cocher, onglet) dans une séquence sont indiqués juste avant le libellé du contrôle.
  Par exemple, cliquez sur le menu : **Extra > Options >** onglet : **Vue**
- Les combinaisons de touches sont écrites de deux manières :
  - Ctrl+Z signifie qu'il faut maintenir la première touche enfoncée tout en appuyant sur la seconde
  - Alt, C signifie qu'il faut appuyer et relâcher la première touche, puis appuyer sur la seconde
- Les fonctions des boutons d'icônes sont ajoutées entre crochets après l'icône elle-même.
  Par exemple, [Enregistrer]

3 À propos de cette documentation

Ceci est le manuel d'installation du logiciel du Access Management System.
Il couvre l'utilisation du programme principal de gestionnaire de dialogues, ci-après dénommé AMS

- La configuration d'un système de contrôle d'accès dans AMS.
- L'utilisation du système configuré par les opérateurs système.

Documentation connexe

Des documents sont disponibles pour les éléments suivants :

- L'installation d'AMS et de ses programmes auxiliaires.
- Le fonctionnement d'AMS - Map View.

4 AMS - Présentation du système

Access Management System est un puissant système de contrôle d'accès pur, qui fonctionne en solo ou de concert avec BVMS, système de gestion vidéo phare de Bosch.
Sa puissance découle de son équilibre unique de technologies de pointe et éprouvées :

- Conçu pour la convivialité : interface utilisateur pratique avec Map View par glisser-déposer et boîtes de dialogue d'inscription biométriques simplifiées.
- Conçu pour la sécurité des données : prise en charge des normes (EU-GDPR 2018), systèmes d'exploitation, bases de données et interfaces système cryptées les plus récents.
- Conçu pour la résilience : les contrôleurs d'accès principaux de couche intermédiaire assurent le basculement automatique et le réapprovisionnement des contrôleurs d'accès locaux en cas de panne du réseau.
- Conçu pour l'avenir : des mises à jour régulières et un pipeline plein d'améliorations innovantes.
- Conçu pour l'évolutivité : offre des niveaux de saisie faibles à élevés.
- Conçu pour l'interopérabilité : API RESTful, avec des interfaces pour la gestion vidéo Bosch, la gestion des événements et des solutions partenaires spécialisées.
- Conçu pour la protection des investissements : vous permet de tirer parti de votre matériel de contrôle d'accès installé tout en augmentant son efficacité.

5 Activation de la licence du système

Conditions préalables

– Le système a été installé avec succès.
– Vous êtes connecté au serveur AMS, de préférence en tant qu'administrateur.

Procédure pour les licences achetées

Conditions préalables : vous avez acheté des licences en fonction de la signature informatique de cet ordinateur. Contactez votre représentant commercial pour obtenir des instructions.

Activation des licences

Chemin

– Gestionnaire de boîtes de dialogue AMS > **Menu principal** > **Configuration** > **Licences**

1. Cliquez sur **Gestionnaire de licences**.
   L'assistant du **Gestionnaire de licences** s'ouvre.
2. Cliquez sur **Enregistrer** pour enregistrer vos informations système dans un fichier.
3. Cliquez sur **Continuer**.
4. Connectez-vous au Remote Portal remote.boschsecurity.com avec les identifiants de votre entreprise.
5. Sélectionnez le produit nécessitant une licence et suivez les instructions du portail pour générer et télécharger votre fichier de licence.
6. Revenez dans le **Gestionnaire de licences**.
7. Cliquez sur **Continuer**.
8. Cliquez sur **Importer** pour localiser le fichier de licence que vous avez téléchargé et ajoutez-le à votre système.
9. Cliquez sur **Finish (Terminer)**.

Remarque!
Si vous rencontrez des messages d'erreur au cours du processus, contactez l'assistance Bosch.

Remarque!
Conséquences des modifications matérielles et logicielles
Si vous modifiez le matériel de votre serveur, votre licence risque de ne plus être valable et le logiciel pourrait arrêter de fonctionner. Veuillez consulter le support technique avant d'effectuer une modification au niveau du serveur.

Procédure pour le mode de démonstration

Le mode de démonstration active la licence de toutes les fonctionnalités du système pendant une période limitée. Utilisez le mode de démonstration uniquement dans les environnements hors production pour essayer les fonctionnalités avant de les acheter.

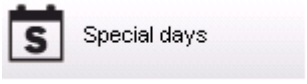
1. Connectez-vous au gestionnaire d'accès
2. Accédez à **Configuration** > **Licences**
3. Cliquez sur le bouton **Activer mode de démonstration**.
4. Vérifiez que les fonctionnalités sont répertoriées dans la fenêtre de dialogue **Licences**.

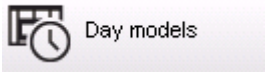
Le mode de démonstration est activé pendant 5 heures. Notez que l'heure d'expiration est affichée en haut de la boîte de dialogue **Licences** et dans la barre de titre de la plupart des fenêtres de dialogue.

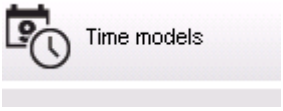
6 Configurer le calendrier

La programmation des activités de contrôle d'accès est régie par des **modèles horaires**.
Un **modèle horaire** est une séquence abstraite d'un ou de plusieurs jours, chacun étant décrit par un **modèle de jour**.
Les modèles horaires contrôlent les activités lorsqu'elles sont appliquées au **calendrier** sous-jacent du système de contrôle d'accès.
Le calendrier du système de contrôle d'accès est basé sur le calendrier du système d'exploitation de l'ordinateur hôte, mais il l'amplifie avec des **journées spéciales** librement définis par l'administrateur du système de contrôle d'accès.
Les jours spéciaux peuvent être fixés à une date particulière du calendrier ou définis par rapport à un événement culturel, comme Pâques. Ils peuvent être récurrents ou non.
La configuration d'un calendrier efficace pour votre système de contrôle d'accès comprend les étapes suivantes.

1. Définissez les **journées spéciales** du calendrier qui s'applique à votre emplacement.
2. Définissez des **modèles de jour** qui décrivent les périodes actives et inactives de chaque type de journée. Par exemple, le modèle de jour pour un jour férié sera différent de celui d'une journée de travail normale. Le travail par équipes affectera également le type et le nombre de modèles de jour dont vous avez besoin.
3. Définissez des **modèles horaires** composés d'un ou de plusieurs modèles de jour.
4. Affectez des modèles horaires aux détenteurs de carte, aux autorisations et aux entrées.

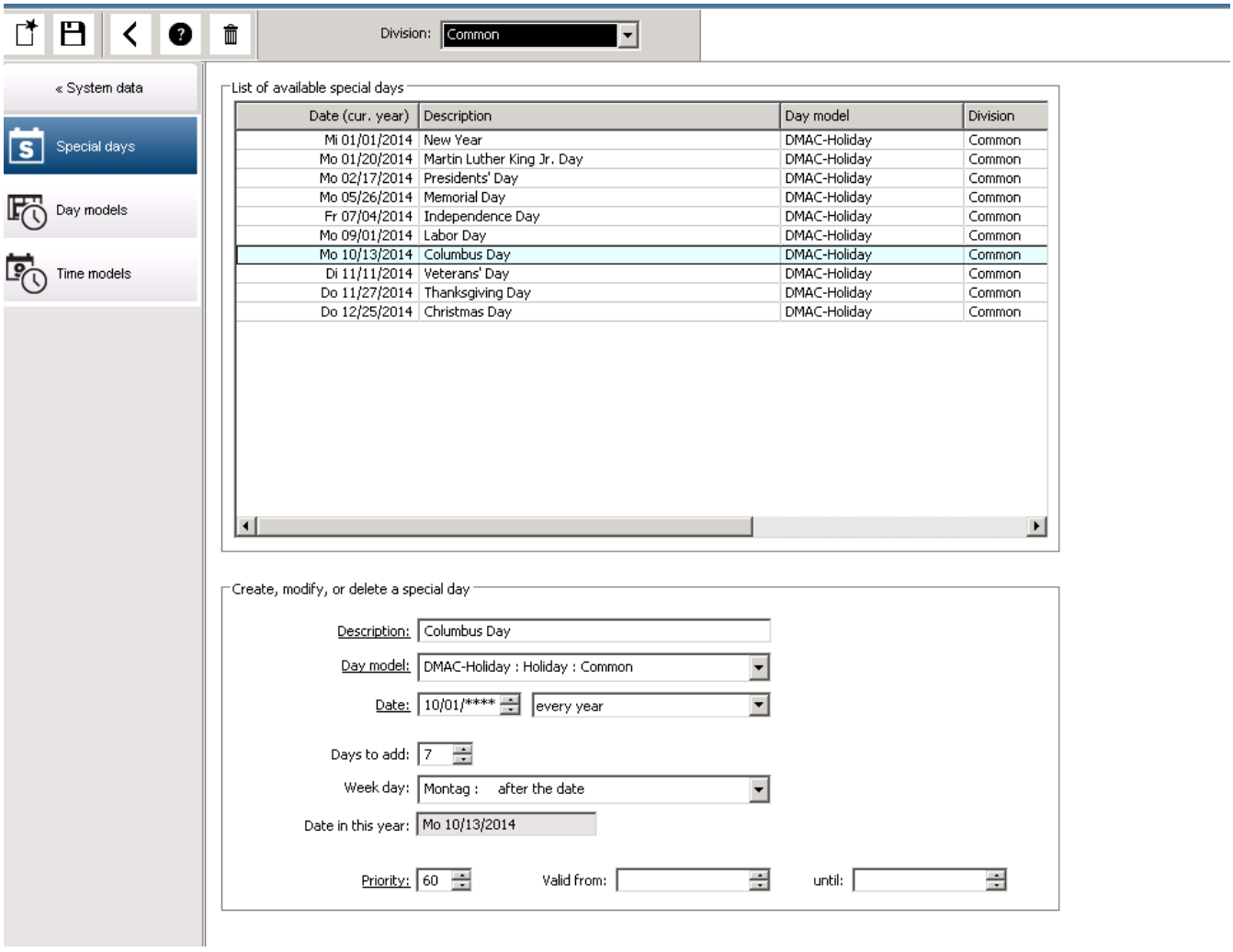






6.1 Définir des jours spéciaux

Lorsque cette fenêtre est ouverte, une liste apparaît dans le champ de liste supérieur de la boîte de dialogue contenant tous les jours fériés spécifiés. Veuillez noter que toutes les dates de vacances indiquées ne concernent que l'année en cours. Cependant, le calendrier est mis à jour d'année en année en fonction des données saisies.
Sous la liste, figurent différents champs de dialogue pour la création de nouveaux jours spéciaux et pour le changement ou la suppression de jours spéciaux existants. Pour ajouter un nouveau jour spécial, au moins trois de ces champs de saisie doivent contenir des données. En premier lieu, une **description** et une **date** doivent être saisis dans les champs respectifs. Ensuite, la **classe** à laquelle appartient ce jour spécial doit être sélectionnée dans la liste sélective appropriée.



La date est indiquée en plusieurs étapes. Tout d'abord, une date de base est saisie dans le champ **Date**. À ce stade, la date décrit un événement de l'année en cours. Si l'utilisateur spécifie maintenant la fréquence d'un retour périodique dans la liste de sélection en regard du champ de date, les parties de la date fixée par la périodicité sont remplacées par des « caractère générique » (*).

une fois	__.__.____
une fois par an	__.__.****
une fois par mois pendant une période d'un an	__.**.____
une fois par mois chaque année	__.**.****
en fonction de Pâques	**.**.****

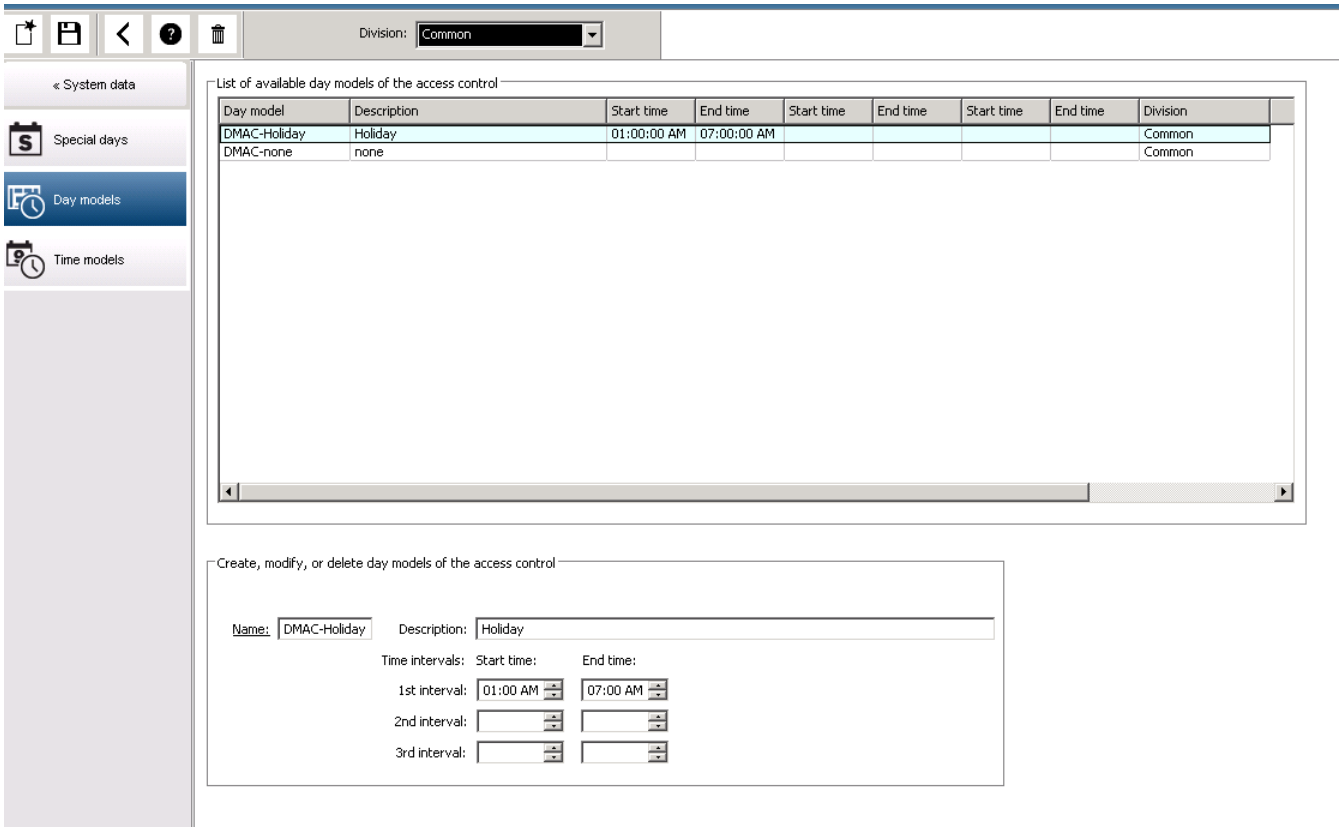
Les congés qui dépendent de Pâques ne sont pas précisés avec leur date, mais avec la différence de jours par rapport au dimanche de Pâques. La date du Dimanche de Pâques de l'année en cours est indiquée dans le champ **Date dans cette année**, et l'écart de cette date est saisi ou sélectionné dans le champ **Jours à ajouter**. Le nombre maximum de jours est de 188, donc en ajoutant ou en soustrayant, vous pouvez définir chaque jour de l'année.

Les autres données, par exemple le **jour de la semaine** du congé, sont facultatifs. Veuillez noter que la liste des jours de la semaine est déterminée par les paramètres régionaux du système d'exploitation (OS). Cela conduit inévitablement à des écrans mixtes où les langues du système de contrôle d'accès et du système d'exploitation diffèrent.
L'affectation d'une **période de validité** est également facultative. Si aucune durée n'est spécifiée, les paramètres par défaut rendent la validité illimitée à partir de la date de saisie.
Une **priorité** peut également être définie. Cette priorité, comprise de 1 à 100, définit le jour de congé qui doit être utilisé. Si deux jours de congés tombent à la même date, le jour de congé avec la priorité la plus élevée est le premier. En cas d'égalité des priorités, le jour de congé utilisé n'est pas défini.
Les jours de congé avec la priorité « 0 » sont désactivés et ne seront pas utilisés.
La boîte de dialogue **Modèles horaires** affiche uniquement les jours de congé actifs, c'est-à-dire avec une priorité supérieure à 0.

Remarque!
Un modèle horaire de la division « Commune » ne peut utiliser que les jours de congé qui sont affectés à la division « Commune ».
Un modèle horaire d'une division spécifique « A » ne peut utiliser que les jours de congé qui sont affectés à la division « A ».
Il n'est pas possible de mélanger les jours de congés entre les divisions, c'est-à-dire que chaque division ne peut utiliser que les jours de congés spécifiques qui lui sont assignés dans son modèle horaire spécifique.

6.2 Définir des modèles de jour

Les modèles de jour définissent un modèle pour n'importe quel jour. Ils peuvent avoir jusqu'à trois intervalles de temps.
Une fois la boîte de dialogue ouverte, tous les modèles de jour existants sont affichés.



Utilisez la boîte de dialogue pour définir ou modifier le nom du modèle, les descriptions et les intervalles. L'icône  démarre un nouveau modèle.
Les heures de début et de fin d'un intervalle sont entrées en heures et en minutes. Dès qu'une heure est atteinte, l'intervalle est respectivement activé ou désactivé. Afin de marquer plus clairement ces heures comme délimiteurs, le volet de liste les affiche avec des secondes (toujours 00). Par exemple, une autorisation dans un modèle horaire qui contient un intervalle de 8h à 15h30 autorise l'accès de 8h à 15h30, mais empêche l'accès à 15h30 min 01s.
Les heures de début et de fin sont soumises à des vérifications logiques lorsqu'elles sont entrées, par exemple une heure de début doit être inférieure à son heure de fin correspondante.
L'une des conséquences possibles de cela est qu'aucun intervalle ne peut s'étendre au-delà de minuit, mais doit être fractionné à ce point :

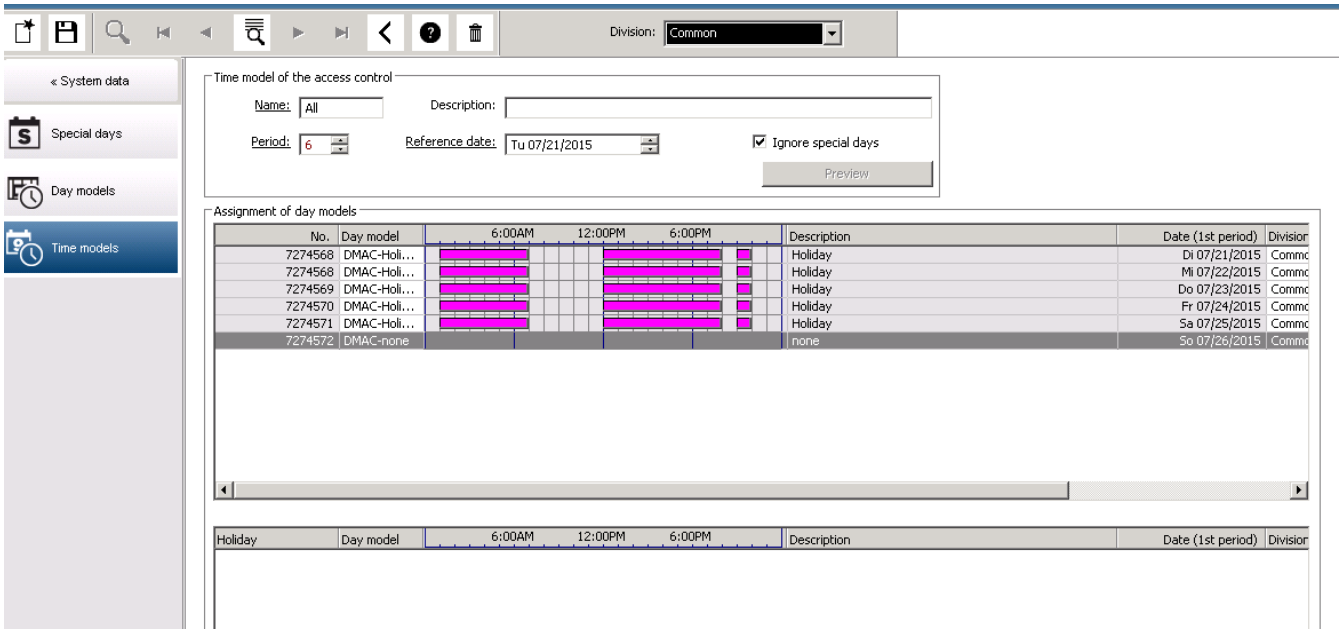
1er intervalle	de :	...	à :	12h00
Intervalle suivant	de :	12h00	à :	...

À l'exception de minuit (12h00), aucun chevauchement n'est autorisé entre les délimiteurs d'intervalle d'un modèle à un jour. Notez que cela empêche la saisie de la même heure pour la fin d'un et le début de l'intervalle suivant.
Exception : pour un intervalle de 24 heures, les heures de début et de fin sont toutes les deux réglées sur minuit.

Remarque!
Conseil : vous pouvez vérifier les intervalles en les visualisant dans la boîte de dialogue Modèles horaires : créez d'abord un modèle de jour contenant ces intervalles (Données système > Calendrier > Modèles de jour). Affectez ensuite ce modèle de jour à un modèle horaire factice avec une période de un jour (Données système > Calendrier > Modèles horaires). Les intervalles sont ensuite illustrés dans le graphique à barres.
Quittez la boîte de dialogue Modèles horaires sans enregistrer les modifications.

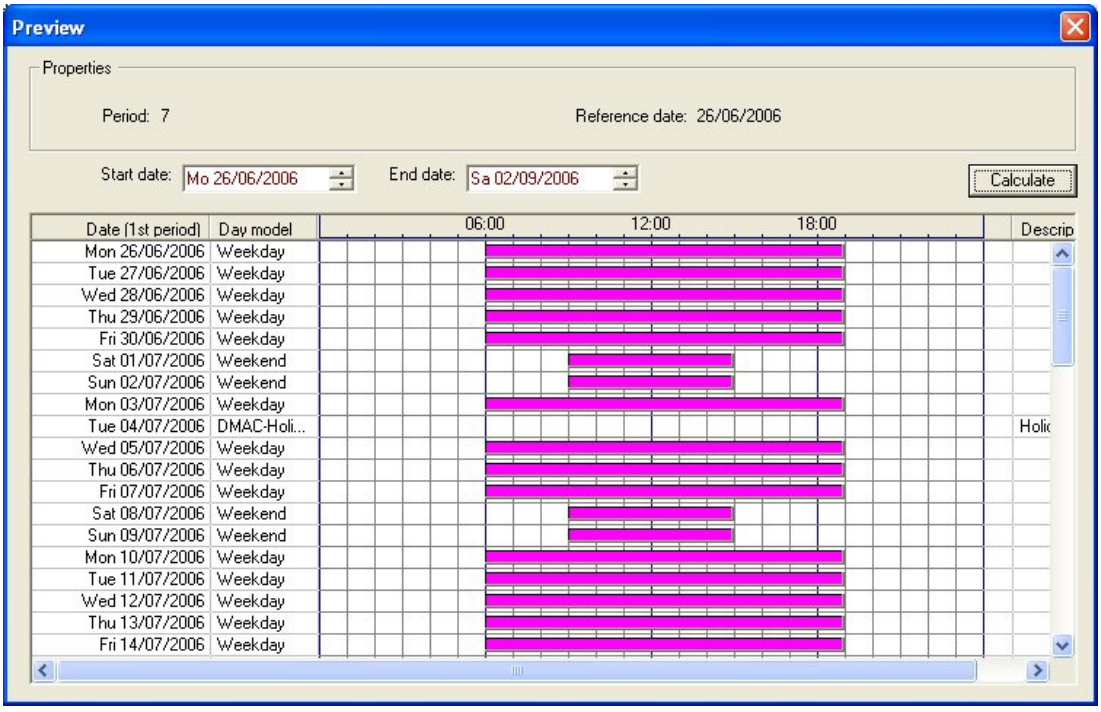
Un modèle de jour ne peut être supprimé que s'il n'a pas été affecté à un jour spécial et s'il n'est pas utilisé dans un modèle horaire.

6.3 Définir des modèles horaires

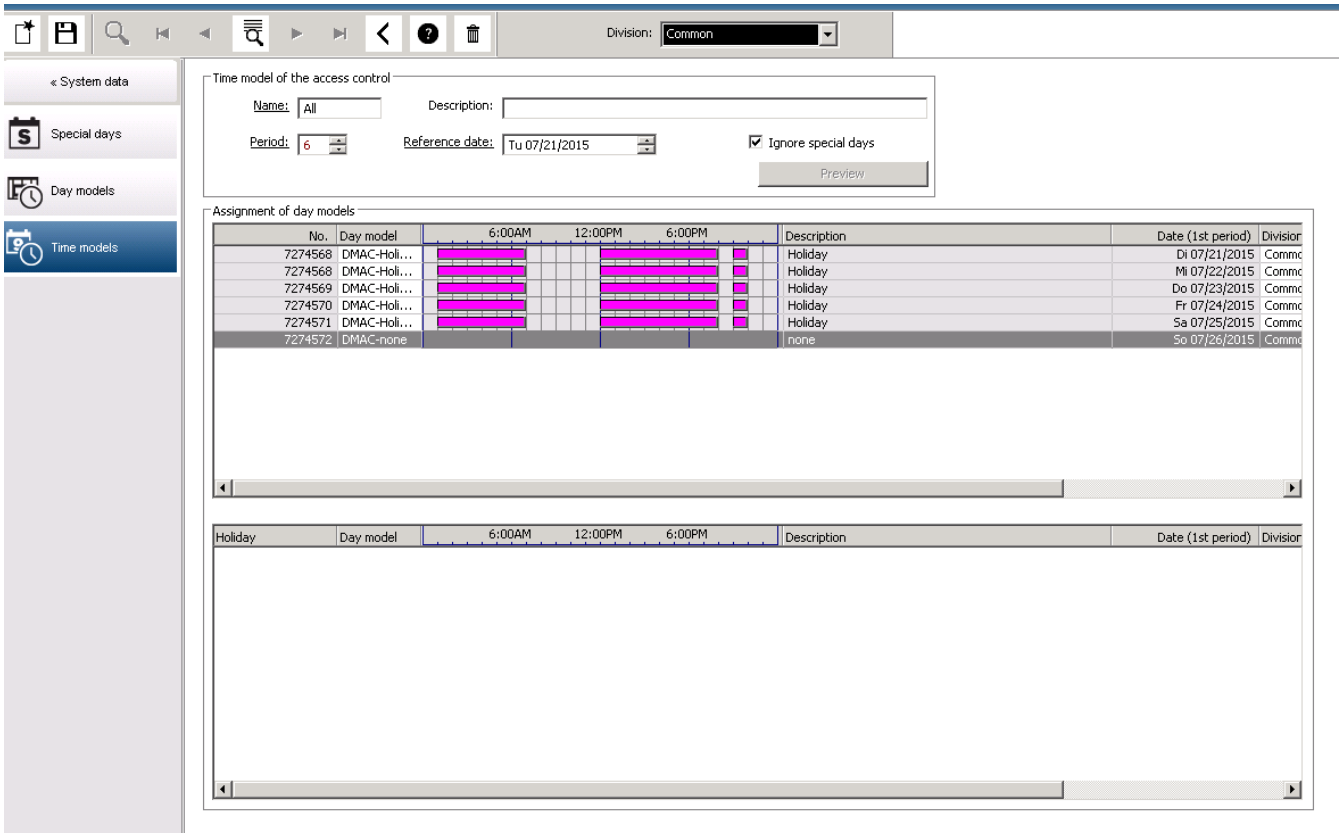


Les modèles horaires existants peuvent être sélectionnés dans la liste de recherche et leurs détails affichés dans les champs de la boîte de dialogue. Tout traitement est effectué conformément à la procédure de création de nouveaux modèles horaire.
Si le masque est vide, les modèles horaires peuvent être créés à partir de zéro. Pour ce faire, vous devez entrer un **nom** et le nombre de jours dans la **période** et sélectionner un début ou une **date de référence**. Lorsque ces données sont confirmées (**Entrée**), une liste apparaît dans le champ **Affectation de modèles de jour** de la boîte de dialogue située en dessous. Le nombre de lignes de cette liste correspond au nombre de jours défini ci-dessus, et les colonnes contiennent déjà un nombre progressif et les dates de la période, en commençant par la date de début sélectionnée.
Seules les entrées de la colonne **« Nom »** peuvent être modifiées ou insérées par l'utilisateur dans cette liste, comme déjà mentionné, les entrées dans les colonnes **« N° »** et **« Date »** découlent des déclarations du responsable de l'en-tête de dialogue ; la colonne **« Description »** est renseignée par le système avec le choix d'un modèle de jour et les explications saisies dans cette boîte de dialogue.
Si un double-clic est effectué sur la ligne correspondante de la colonne **Modèle de jour**, un champ de liste de sélection est activé. L'un des modèles de jour existants peut être sélectionné dans cette liste. De cette manière, un modèle de jour spécifique peut être

affecté à chaque jour de la période. Lorsque l'utilisateur passe à une autre ligne, une description existante du modèle de jour sélectionné est indiquée par le système dans la colonne **Description**.
Les **congés** prédéfinis avec les modèles de jour pertinents sont affichés dans le champ de liste inférieur à des fins de navigation et de vérification. Pour le modèle horaire sélectionné ou nouvellement créé, l'affectation de modèles de jour à certains jours de congés peut être modifiée. Cependant, ces modifications ne s'appliqueront qu'à ce modèle horaire particulier ; les changements généraux qui doivent s'appliquer à tous les modèles existants et futurs ne peuvent être effectués que dans la boîte de dialogue Congés. Conformément à ces paramètres, les jours de la semaine se voient affecter les modèles de jour affectés, en tenant compte des congés.
Ensuite, en fonction de ces paramètres, les jours de la semaine sont confrontés aux modèles de jour affectés en tenant compte des jours spéciaux. Pour vérifier rapidement que les modèles de jour ont été utilisés et affectés correctement, en particulier les jours de congés, cette boîte de dialogue contient un **aperçu** qui montre la répartition des jours de certaines périodes.
Enfin, une boîte de dialogue distincte s'ouvre lorsqu'on clique sur le bouton **Aperçu** et il est possible d'indiquer une période de 90 jours maximum, en incluant les jours de congés. Si le bouton **Calculer** est utilisé, le rapport est généré et affiché comme indiqué ci-dessous : ce processus peut prendre quelques secondes en fonction de la taille de l'intervalle.



Dans le paramètre par défaut, les jours spéciaux sont appliqués aux modèles horaires en fonction de leurs définitions. Si les jours spéciaux n'ont cependant exceptionnellement aucun intérêt, cela peut être dû au choix de l'option **Ignorer les jours spéciaux**.
Simultanément, les entrées des deux listes inférieures sont supprimées, de sorte qu'il est immédiatement évident pour l'utilisateur que les jours spéciaux et les classes de jour ne trouvent aucune utilité dans ce modèle.


Division:
Common
« System data
Special days
Day models
Time models
Time model of the access control
Name:
All
Description:
Period:
6
Reference date:
Tu 07/21/2015
Ignore special days
Preview
Assignment of day models
No.
Day model
6:00AM
12:00PM
6:00PM
Description
Date (1st period)
7274568 DMAC-Holi... Holiday Di 07/21/2015
7274568 DMAC-Holi... Holiday Mi 07/22/2015
7274569 DMAC-Holi... Holiday Do 07/23/2015
7274570 DMAC-Holi... Holiday Fr 07/24/2015
7274571 DMAC-Holi... Holiday Sa 07/25/2015
7274572 DMAC-none none So 07/26/2015
Holiday
Day model
6:00AM
12:00PM
6:00PM
Description
Date (1st period)

7 Configurer des divisions

Introduction

Le système peut éventuellement être autorisé à fournir un contrôle d'accès conjoint pour une installation qui est partagée par un nombre quelconque de parties indépendantes, appelé **Divisions**.

Les opérateurs système peuvent se voir affecter une ou plusieurs divisions. Ils voient alors uniquement les personnes, les dispositifs et les entrées de ces divisions.

Lorsque la licence de **Divisions** n'est pas activée, tous les objets gérés par le système appartiennent à une seule division appelée **Commune**.

Conditions préalables

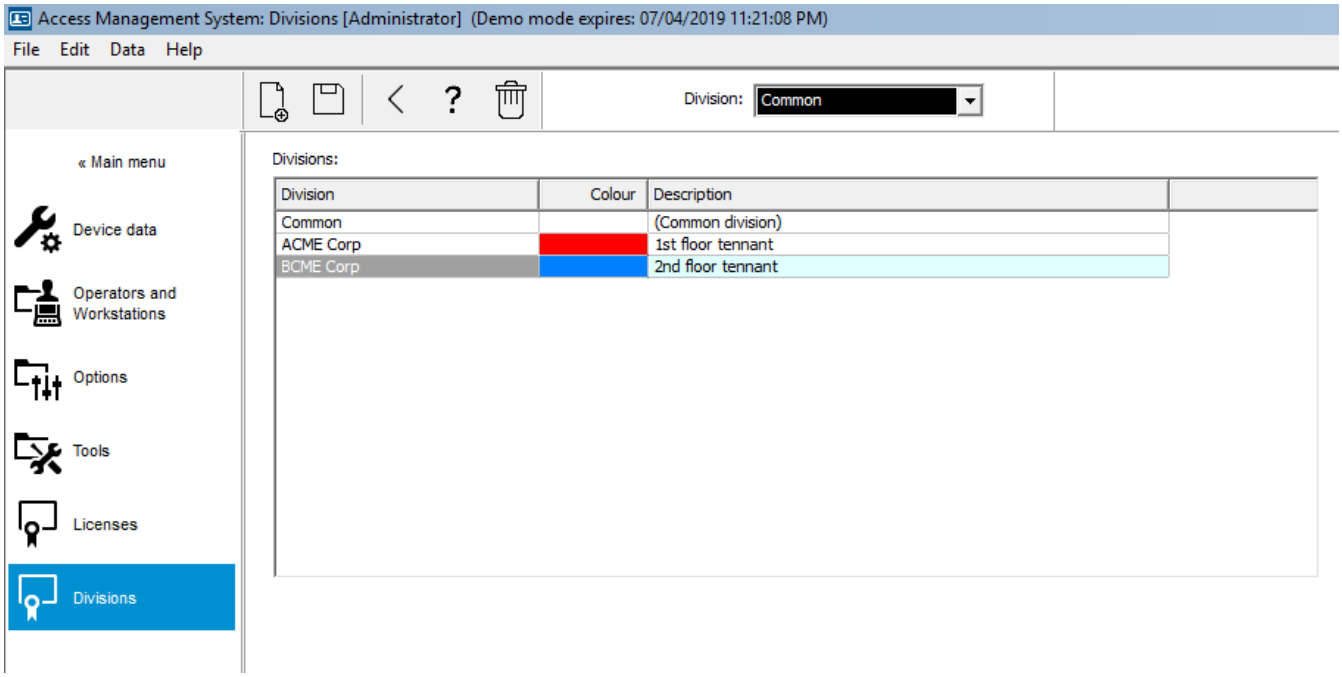
– La fonction Divisions est concédée sous licence pour votre installation.

Chemin d'accès à la boîte de dialogue

– Menu principal > **Configuration** > **Divisions**

Procédure

1. Cliquez sur dans la barre d'outils.
   – Une nouvelle division est créée avec un nom par défaut.
2. Remplacez le nom par défaut et (facultatif) entrez une description pour le bénéfice des autres opérateurs.
3. Cliquez dans la colonne **Couleur** pour affecter une couleur qui permettra de distinguer les actifs de la division dans l'interface utilisateur.
4. Cliquez sur pour enregistrer



7.1 Affecter des divisions aux dispositifs

Affecter des divisions aux dispositifs dans l'éditeur de dispositif

Chemin d'accès à la boîte de dialogue

Menu principal > **Configuration** > **Données du dispositif**

Conditions préalables

– Les divisions sont concédées sous licence et opérationnelles
– Au moins une division est créée.

Procédure

1. Dans l'arborescence de dispositif, sélectionnez le dispositif pour affectation.
   – L'éditeur de dispositif apparaît dans le volet de boîte de dialogue principal.
2. Dans la liste Division, sélectionnez la nouvelle division pour le dispositif
   – La zone de liste reflète la nouvelle division.
3. Cliquez sur  (Enregistrer) pour enregistrer

Remarque!

Tous les composants d'une entrée doivent appartenir à une seule division

Le système ne vous permettra pas d'enregistrer une entrée tant que tous ses composants n'appartiennent pas à la même division.

7.2 Affecter des divisions aux opérateurs

Affecter des divisions aux opérateurs dans la boîte de dialogue **Droits de l'utilisateur**

Chemin d'accès à la boîte de dialogue

Menu principal > **Configuration** > **Opérateurs et postes de travail > Droits de l'utilisateur**

Conditions préalables

– Les divisions sont concédées sous licence et opérationnelles
– Au moins une division est créée.
– Au moins un opérateur est créé sur le système

Procédure

1. Dans la boîte de dialogue **Droits de l'utilisateur**, sélectionnez la fiche personnel de l'opérateur à affecter.
2. Sur l'onglet **Divisions**, utilisez les touches fléchées pour déplacer les divisions de la liste **Divisions disponibles** vers la liste **Divisions affectées** pour cet opérateur.
3. Cliquez sur  (Enregistrer) pour enregistrer

8 Configurer les adresses IP

Les contrôleurs d'accès locaux sur le réseau nécessitent un schéma cohérent d'adresses IP afin de participer au système de contrôle d'accès. L'outil **AccessIPConfig** localise les contrôleurs sur le réseau et fournit une interface pratique pour administrer leurs adresses et autres options réseau de manière centralisée.

Conditions préalables

- Les contrôleurs d'accès locaux sont sous tension et connectés au réseau.
- Vous disposez d'un schéma pour les adresses IP des contrôleurs et leurs mots de passe si nécessaire.

Chemin d'accès à la boîte de dialogue
Menu principal > **Configuration** > **Outils**

Procédure

1. Suivez le chemin d'accès à la boîte de dialogue ci-dessus et cliquez sur **Configuration AMC et dispositifs d'empreintes digitales**
   L'outil **AccessIPConfig** s'ouvre.
2. Cliquez sur **Rechercher les AMC**
   Les contrôleurs d'accès locaux disponibles sur le réseau sont répertoriés, chacun avec les paramètres suivants :
   - **Adresse Mac** : adresse matérielle du contrôleur. Notez qu'il ne s'agit **pas** de l'adresse de son Contrôleur d'accès principal, qui ne s'appelle MAC que par coïncidence.
   - **Adresse IP stockée** :
   - **Numéro de port** : la valeur par défaut est `10001`
   - **DHCP** : la valeur est **Oui** uniquement si le contrôleur est configuré pour recevoir une adresse IP de DHCP
   - **Adresse IP actuelle**
   - **Numéro de série**
   - Notes ajoutées par l'équipe de configuration réseau
3. Double-cliquez sur un AMC dans la liste pour modifier ses paramètres dans une fenêtre contextuelle. Sinon, sélectionnez la ligne de l'AMC souhaitée et cliquez sur **Définir IP...**
   Notez qu'il peut être nécessaire de saisir un mot de passe, si celui-ci a été configuré pour le dispositif.
   Les paramètres modifiés sont stockés dès que vous cliquez sur OK dans la fenêtre contextuelle.
4. Lorsque vous avez terminé de configurer les paramètres IP des contrôleurs, cliquez sur **Fichier** > **Sortie** pour fermer l'outil.
   Vous retournez dans l'application principale.

Pour plus d'informations, cliquez sur **Aide** dans l'outil **AccessIPConfig** pour afficher son propre fichier d'aide.

9 Utiliser l'éditeur de dispositif

Introduction

L'éditeur de dispositif est un outil permettant d'ajouter, de supprimer ou de modifier des entrées et des dispositifs.

L'éditeur de dispositif propose des vues pour les hiérarchies modifiables suivantes :

- **Configuration du dispositif** : dispositifs électroniques au sein du système de contrôle d'accès.
- **Postes de travail** : ordinateurs coopérant dans le système de contrôle d'accès.
- **Zones** : zones physiques dans lesquelles le système de contrôle d'accès est divisé.

Conditions préalables

Le système est correctement installé, sous licence et sur le réseau.

Chemin d'accès à la boîte de dialogue

- **Menu principal** >**Configuration** > **Données du dispositif**

Utiliser la barre d'outils de l'éditeur de dispositif

La barre d'outils de l'éditeur de dispositif propose les fonctions suivantes, quelle que soit la vue active : **Dispositifs**, **Postes de travail** ou **Domaines**.

Bouton	Raccourci	Description
	Ctrl + N	Crée un nouvel élément sous le nœud sélectionné. Vous pouvez également cliquer avec le bouton droit sur le nœud pour appeler son menu contextuel.
	Suppr	Supprime l'élément sélectionné et tout ce qui se trouve en dessous.
	Ctrl-Page vers le haut	Premier élément de l'arborescence
	Ctrl -	Élément précédent
	Ctrl +	Élément suivant
	Ctrl-Page bas	Dernier élément de l'arborescence
	Ctrl-A	Développe et réduit l'arborescence.
	Ctrl-K	Actualise les données en les rechargeant à partir de la base de données. **Toutes les modifications non enregistrées sont supprimées.**
	Ctrl-S	Enregistre la configuration actuelle
	Ctrl-F	Ouvre une fenêtre de recherche

		Ouvrir l'arborescence **Configuration du dispositif**
		Ouvrir l'arborescence **Postes de travail**
		Ouvrir l'arborescence **Zones**

Dans toutes les vues de l'éditeur de dispositif, commencez à la racine de l'arborescence et ajoutez des éléments à l'aide des boutons de la barre d'outils, du menu ou du menu contextuel de chaque élément (clic droit pour l'appeler). Pour ajouter des sous-éléments à un dispositif, sélectionnez d'abord le dispositif parent sous lequel les sous-éléments doivent apparaître.

Copier et coller des dispositifs AMC

Pour copier des dispositifs AMC d'une partie de l'arborescence vers une autre :

1. Cliquez avec le bouton droit sur le dispositif AMC et sélectionnez **Copier** dans le menu contextuel.
2. Cliquez avec le bouton droit sur un dispositif parent approprié ailleurs dans l'arborescence et sélectionnez **Coller** dans le menu contextuel.
   - Le dispositif est copié vers le nouvel emplacement avec ses sous-dispositifs et ses paramètres.
   - Les paramètres de dispositif, tels que **Adresse IP** et **Nom**, qui doivent être uniques, ne sont **pas** copiés.
3. Entrez des valeurs uniques pour les paramètres de dispositifs qui en ont besoin. Tant que vous ne faites pas cela, vous ne pouvez pas enregistrer l'arborescence de dispositifs.

Enregistrer votre travail

Lorsque vous avez terminé d'ajouter et de modifier des éléments dans l'arborescence, cliquez sur **Enregistrer**  pour enregistrer la configuration.
Pour fermer l'éditeur de dispositif, cliquez sur **Fichier** > **Sortie**.

9.1 Modes de configuration et remplacements

Le Mode de configuration est l'état par défaut des dispositifs de contrôle d'accès dans l'éditeur de dispositif. En mode de configuration, un utilisateur autorisé d'AMS ou de BIS ACE peut apporter des modifications aux dispositifs dans l'éditeur de dispositif, puis ACS propage immédiatement les modifications aux dispositifs subordonnés.
Un opérateur peut **remplacer** le mode de configuration en envoyant des commandes directement aux dispositifs de contrôle d'accès depuis l'extérieur de l'éditeur de dispositif. Ceci est courant, par exemple, lorsqu'un opérateur gère les messages entrants et les alarmes. Jusqu'à ce que l'opérateur envoie la commande de **restauration de la configuration**, le dispositif reste en Mode de fonctionnement.
Si un utilisateur de configuration sélectionne un dispositif dans l'éditeur de dispositif alors qu'il est en mode de fonctionnement, la page de propriétés principale du dispositif affiche la notification :

This device is not in configuration mode (Ce dispositif n'est pas en mode de configuration).

Il peut apporter et enregistrer des modifications de configuration, mais les modifications sont mises en mémoire tampon et ne prennent effet qu'une fois le mode de fonctionnement de l'alarme terminé et le mode de configuration restauré.

10 Configurer des zones de contrôle d'accès

Introduction aux zones

Les installations sécurisées peuvent être divisées en zones. Les zones peuvent être de toutes tailles : un ou plusieurs bâtiments, des étages ou même des pièces individuelles.
Quelques utilisations possibles des zones sont les suivantes :

- La localisation de personnes individuelles dans les installations sécurisées.
- L'estimation du nombre de personnes dans une zone donnée, en cas d'évacuation ou autre situation d'urgence.
- Limitation du nombre de personnes ou de véhicules dans une zone :
  Lorsque la limite de population prédéfinie est atteinte, d'autres admissions peuvent être refusées jusqu'à ce que des personnes ou des véhicules quittent la zone.
- Mise en œuvre d'un contrôle de séquence d'accès et d'un anti-retour

Le système distingue deux types de zones à accès contrôlé

- Zones pour personnes
- Zones pour véhicules (parkings)

Chaque zone peut avoir des sous-zones pour une granularité plus fine du contrôle. Les zones réservées aux personnes peuvent avoir jusqu'à 3 niveaux d'imbrication, et les zones réservées aux parkings seulement 2, à savoir le parking général et les zones de stationnement, au nombre de 1 à 24.
La zone par défaut, qui existe dans toutes les installations, est appelée **Extérieur**. Elle fait office de parent pour toutes les zones définies par l'utilisateur des deux types : personnes et parkings.

Une zone n'est utilisable que si au moins une entrée y conduit.
L'éditeur de dispositif **DevEdit** peut être utilisé pour attribuer une zone de localisation et une zone de destination à n'importe quelle entrée. Lorsque quelqu'un scanne une carte sur un lecteur appartenant à une entrée, le nouvel emplacement de la personne devient la zone de destination de cette entrée.

Remarque!
Le Contrôle de séquence d'accès et la fonction anti-retour nécessitent à la fois des lecteurs d'entrée et de sortie aux entrées des zones.
Les entrées de type tourniquet sont fortement recommandées pour éviter les « talonnages » accidentels ou délibérés

Procédure de création de zones

Conditions préalables

En tant qu'opérateur système, vous avez besoin d'une autorisation de votre administrateur système pour créer des zones.

Chemin d'accès à la boîte de dialogue (AMS)

1. Dans le gestionnaire de boîtes de dialogue AMS, sélectionnez **Menu principal** > **Configuration** > **Données de dispositif**
2. Cliquez sur Zones 

3. Sélectionnez le nœud **Extérieur**, ou l'un de ses enfants, puis cliquez sur  dans la barre d'outils. Vous pouvez aussi effectuer un clic droit sur **Extérieur** pour ajouter une zone via son menu contextuel.
   Toutes les zones créées initialement reçoivent un nom unique de **Zone** plus un suffixe numérique.
4. Dans la fenêtre contextuelle, sélectionnez son type, c'est-à-dire **Zone** pour les personnes ou **Parking** pour les véhicules.
   Notez que seulement **Extérieur** peut avoir des enfants des deux types. Toute sous-zone de ces enfants hérite toujours du type de son parent.
   – Les **Zones** pour les personnes peuvent être imbriquées sur trois niveaux. Pour chaque zone ou sous-zone, vous pouvez définir une population maximale.
   – Les **Parking** sont des entités virtuelles constituées d'au moins une **zone de stationnement**. Si la population d'un parking n'a pas besoin d'être limitée par le système, 0 s'affiche. Sinon, le nombre maximum de places de parking par zone est de 9 999, et le volet principal du parking affiche la somme de toutes les places de ses zones.

Procédure pour éditer des zones

1. Cliquez sur une Zone dans la hiérarchie pour la sélectionner.
2. Remplacez un ou plusieurs des attributs suivants dans le volet principal de la boîte de dialogue.

Nom	Le nom par défaut, que vous pouvez remplacer.
Description	Une description en texte libre de la zone.
Nombre maximum de personnes/voitures	Valeur par défaut 0 (zéro) pour aucune limite. Sinon, entrez un entier pour sa population maximale.

Remarques :

– Une zone ne peut pas être déplacée par glisser-déposer vers une autre branche de la hiérarchie. Si nécessaire, supprimez la zone et recréez-la sur une autre branche.

Procédure pour supprimer des zones.

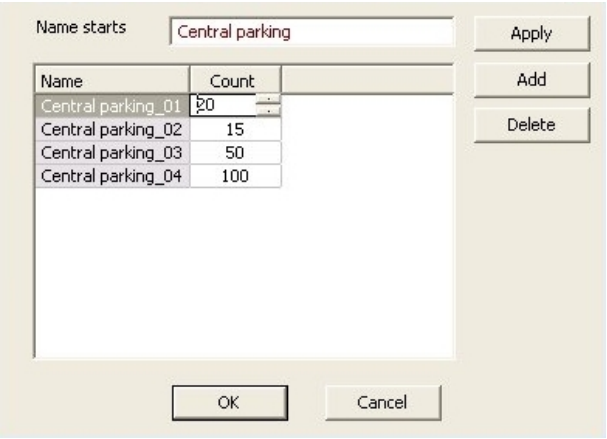
1. Cliquez sur une zone dans la hiérarchie pour la sélectionner.
2. Cliquez sur **Supprimer**  ou faites un clic droit pour supprimer via le menu contextuel.

Remarque : Une zone ne peut pas être supprimée tant que tous ses enfants n'ont pas été supprimés.

10.1 Configurer des zones pour les véhicules

Créer des zones pour les véhicules (parking, aire de parking)

Si vous sélectionnez un type de zone **Parking**, une fenêtre contextuelle apparaît.



1. Entrez un nom dans le champ **Le nom commence par** pour créer un nom de ligne pour toutes ses sous-zones de stationnement ou **zones de stationnement**.
   Jusqu'à 24 **zones de stationnement** peuvent être créées à l'aide du bouton **Ajouter**, et chacun aura le nom du réseau plus un suffixe à 2 chiffres.
2. Si le système doit limiter la population de ces zones, entrez le nombre de places de parking dans la colonne **Nombre**. Si aucune limite de population n'est requise, entrez 0.

Remarque : La population maximale de tout le parking est la somme de ces chiffres. Seules les zones de stationnement peuvent contenir des places de stationnement ; le **parking** est seulement une entité virtuelle composée d'au moins une **zone de stationnement**. Le nombre maximum de places de stationnement par zone est de 9 999.

Créer des entrées pour les parkings

Comme dans les zones normales, les parkings nécessitent une entrée. Le modèle de porte approprié est **Parking lot 05c**.

Pour surveiller la population d'un parking, 2 entrées avec ce modèle de porte sont nécessaires sur le même AMC, une pour l'entrée et une pour la sortie.

Condition préalable

Créez un parking avec au moins une zone de stationnement, comme décrit ci-dessus.

Chemin d'accès à la boîte de dialogue

Menu principal > **Configuration** > **Données du dispositif**

Cliquez sur **LAC/Entrées/Dispositifs** 

Procédure

1. Dans la hiérarchie des dispositifs, créez un AMC ou sélectionnez un AMC qui n'a pas d'entrées dépendantes.
2. Cliquez avec le bouton droit sur l'AMC et sélectionnez **Nouvelle entrée**
3. Dans la fenêtre contextuelle **Nouvelle entrée**, sélectionnez le modèle d'entrée **Parking lot 05c** et ajoutez un lecteur entrant du type installé à l'entrée du parking.
4. Cliquez sur **OK** pour fermer la fenêtre contextuelle.
5. Sélectionnez cette entrée nouvellement créée dans la hiérarchie des dispositifs.
   – Notez que le système a automatiquement désigné le lecteur comme lecteur d'entrée.
6. Dans le volet d'édition principal, sur l'onglet **Parking lot 05c**, sélectionnez dans le menu déroulant **Destination** le parking que vous avez créé précédemment.
7. Cliquez à nouveau avec le bouton droit sur l'AMC et créez une autre entrée de type **Parking lot 05c** comme ci-dessus.
   – Notez que cette fois, vous ne pouvez sélectionner qu'un lecteur sortant.

- Cliquez sur **OK** pour fermer la fenêtre contextuelle.

8. Sélectionnez cette seconde entrée nouvellement créée dans la hiérarchie des dispositifs
   - Notez que le système a automatiquement désigné le deuxième lecteur comme lecteur de sortie.

11 Configurer des zones et des centrales intrusion

Introduction

Le système de contrôle d'accès contribue à l'administration et au fonctionnement des centrales intrusion Bosch. Consultez la fiche technique du système de contrôle d'accès pour plus de détails sur les modèles qu'il prend en charge. Le système de contrôle d'accès ajoute une valeur particulière dans l'administration des **utilisateurs** de la centrale intrusion. Ces utilisateurs constituent un sous-ensemble des détenteurs de carte du système de contrôle d'accès global. Les administrateurs du système de contrôle d'accès accordent à ces détenteurs de carte des autorisations spéciales pour utiliser les centrales intrusion via le Gestionnaire de dialogue ACE.

Les centrales intrusion elles-mêmes sont configurées et mises à jour comme précédemment via leur logiciel de programmation à distance (RPS). ACE lit en permanence à partir de RPS et affiche les centrales qui s'y trouvent.

ACE contient des boîtes de dialogue pour créer et affecter des profils d'autorisation, et pour gérer les utilisateurs de centrale dans RPS.

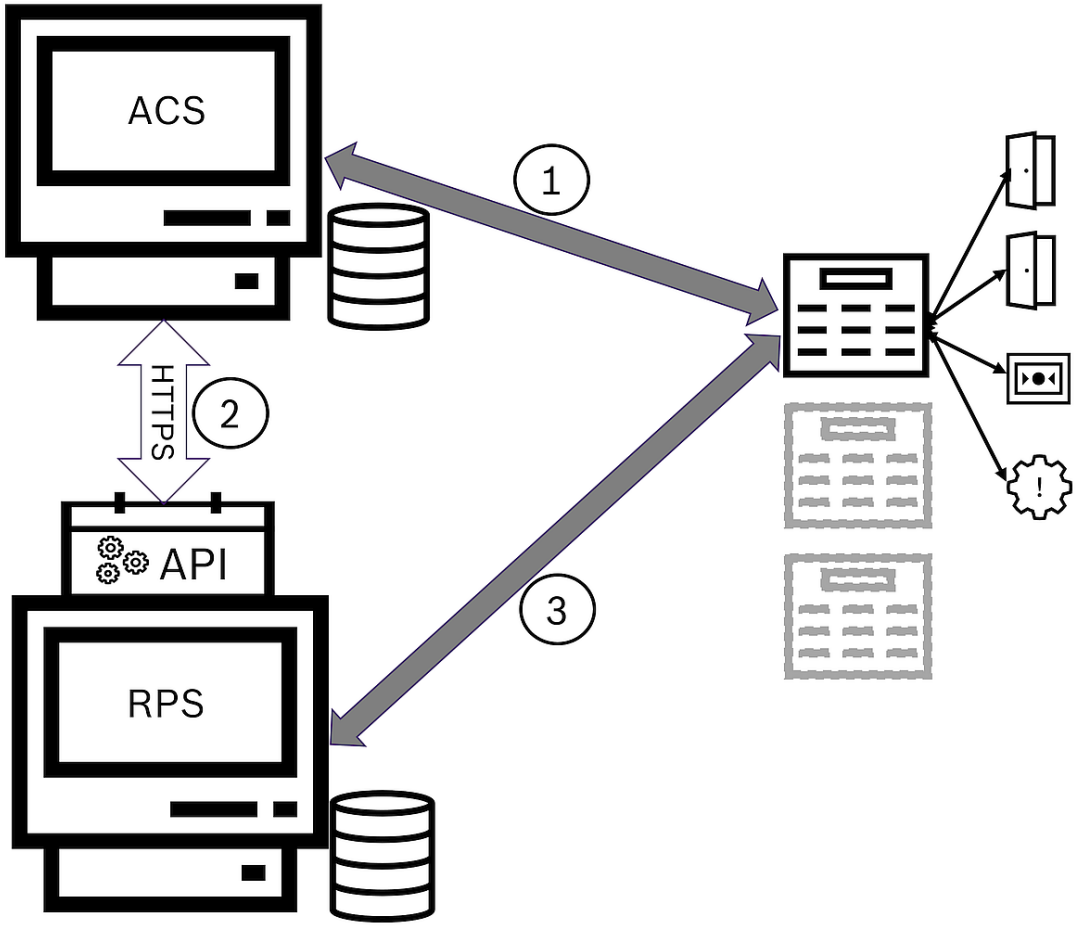


Figure 11.1: Topologie simplifiée du système ACS-Intrusion

ACS	Principal système de contrôle d'accès : AMS ou BIS-ACE
API	Interface de programmation
RPS	Système de programmation à distance : application de contrôle des centrales intrusion

1	ACS vers centrale : commandes de centrale. Centrale vers ACS : événements des points d'intrusion.
2	ACS vers RPS : données du détenteur de la carte
3	RPS vers centrale : paramètres de configuration

Conditions préalables

- Le RPS des centrales d'intrusion Bosch pris en charge est installé sur un ordinateur séparé avec une connexion réseau au serveur ACE, **et non** sur le serveur ACE lui-même. Consultez le guide d'installation du logiciel RPS pour les instructions d'installation.
- RPS est configuré avec les centrales intrusion qui appartiendront au système de contrôle d'accès ACE. Consultez le guide de l'utilisateur ou l'aide en ligne du logiciel RPS pour obtenir des instructions.
- Les horloges sur les centrales sont à moins de 100 jours de l'horloge sur le serveur ACE, pour activer la synchronisation automatique.
- Le protocole de mode 2 est défini sur toutes les centrales participantes.
- Cartes avec l'une des définitions de carte standard suivantes :
  - HID 37 BIT -> intrusion 37 BITS avec un code installation/site de 32767 ou moins.
  - HID 26 BIT- > Intrusion 26 BITS
  - EM 26 BIT- > Intrusion 26 BITS

Présentation

Le processus de configuration comprend les étapes suivantes, décrites dans les sections suivantes de ce chapitre :

1. Installation de l'API Intrusion RPS sur l'ordinateur RPS
2. Connecter le système de contrôle d'accès aux centrales intrusion.
   - Définition de la connexion à l'API RPS.
   - Configurer les connexions de centrale.
3. Créer des profils d'autorisation de centrale qui régissent les fonctions des centrales connectées qui peuvent être utilisées.
4. Attribuer des profils d'autorisation de centrales à des détenteurs de carte.
   - Ces détenteurs de carte deviennent ainsi les opérateurs des centrales intrusion.

11.1 Installation de l'API Intrusion RPS sur l'ordinateur RPS

L'API Intrusion RPS est le canal de communication entre l'AMS et les applications RPS sur leurs ordinateurs respectifs. Vous devez d'abord installer l'API sur l'ordinateur RPS, puis installer les certificats générés par le programme d'installation sur l'ordinateur AMS.

Procédure

1. Exécutez le fichier d'installation de l'API RPS conformément à sa documentation.

- Le fichier d'installation et sa documentation se trouvent sur le support d'installation d'AMS :
  `AddOns\Intrusion-RPS-API\Bosch_RPS_API_Setup_v*.exe`
  `AddOns\Intrusion-RPS-API\RPS-API_Application_note_v*.pdf`
- Le programme d'installation génère 2 certificats et les enregistre sur l'ordinateur RPS :
  `%AppData%\Roaming\Bosch_RPS_API\BoschRpsAPI.cer`
  `%AppData%\Roaming\Bosch_RPS_API\BoschRpsAPI.pfx` (vous devez définir un mot de passe)

2. Copiez les fichiers de certificat sur l'ordinateur AMS.

3. Sur l'ordinateur AMS, installez les certificats pour **Emplacement du magasin** :`Local Machine`,**Magasin de certificats** :`Trusted Root Certification Authority`.

11.2 Connecter le système de contrôle d'accès aux centrales intrusion

Introduction

Cette section décrit comment afficher les centrales intrusion et les rendre disponibles pour contrôle via ACE client. Le système de contrôle d'accès se connecte via l'API au RPS sur son réseau. Grâce à l'API, il maintient une liste interne à jour des centrales intrusion compatibles disponibles.

Deux étapes sont nécessaires dans AMS pour le connecter aux centrales intrusion :

– Etape 1 : définir la connexion à l'API RPS
– Étape 2 : configurer les connexions de la centrale

Chemin d'accès à la boîte de dialogue

– Menu principal > **Configuration** > **Centrales** et sous-dialogues

11.2.1 Etape 1 : définir la connexion à l'API RPS

L'étape 1 consiste à fournir l'adresse de l'ordinateur RPS et les informations de connexion de l'administrateur au système de contrôle d'accès.

Chemin d'accès à la boîte de dialogue

Menu principal > **Configuration** > **Centrales > Configuration de l'API RPS**

Procédure

1. Entrez les informations suivantes :

Note	Description
Nom d'hôte / Adresse IP	Adresse HTTPS de l'ordinateur sur lequel s'exécute le logiciel RPS, et numéro de port via lequel le logiciel RPS communique. L'utilisation de `localhost` n'est pas autorisé. Le numéro de port par défaut est `9000`.
Nom de l'utilisateur	Nom d'utilisateur d'un administrateur RPS pour l'API.
Mot de passe	Mot de passe de l'administrateur RPS.

2. Cliquez sur le bouton **Tester la connexion** pour vous assurer que le logiciel RPS est en cours d'exécution et que le nom d'utilisateur et le mot de passe sont valides.
3. Cliquez sur  (Enregistrer) pour enregistrer les modifications.

11.2.2 Étape 2 : configurer les connexions de la centrale

L'étape 2 consiste à configurer le niveau de contrôle du système de contrôle d'accès sur les centrales individuelles du réseau.

Chemin d'accès à la boîte de dialogue

Menu principal > **Configuration** > **Centrales > Administration de la centrale**

La boîte de dialogue gère une liste des centrales intrusion compatibles que l'API RPS a fourni au ACE.
La liste est régulièrement mise à jour en arrière-plan. Une fois que vous avez ouvert la boîte de dialogue, cliquez sur  occasionnellement, pour forcer manuellement une mise à jour immédiate.
La liste est en lecture seule, à l'exception des commandes décrites dans la section suivante.

Procédure

1. Sélectionnez une centrale dans la liste
2. Utilisez les commandes ci-dessous pour définir ce que le système de contrôle d'accès peut faire sur la centrale intrusion sélectionnée.

Colonne de liste **Administration utilisateur**	Cochez la case pour vous assurer que les utilisateurs de la centrale intrusion de cette ligne sont gérés sur le système de contrôle d'accès et **non** sur la centrale elle-même. **IMPORTANT** : ce paramètre entraîne le remplacement de tous les utilisateurs de centrale créés en local dans RPS.
Colonne de liste **Map View**	Cochez la case pour rendre cette centrale disponible pour les commandes et les contrôles via le ACE client.
Paramètres  icône (cog) dans la colonne **Données d'accès** .	Si vous avez coché la case dans la colonne **Map View**, cliquez sur l'icône pour entrer – une adresse IP – un numéro de port (par défaut 7700) – le mot de passe de la centrale individuelle. Le mot de passe est défini dans RPS.
Bouton : **Supprimer la centrale sélectionnée**	Si une centrale est supprimée dans RPS, elle s'affiche avec l'état **Supprimé** dans la liste. Sélectionnez la centrale et cliquez sur ce bouton pour la supprimer complètement de la base de données.

11.3 Créer des profils d'autorisation pour les centrales

Introduction

Cette section décrit comment créer des profils d'autorisation de centrale.
Un profil d'autorisation de centrale est un ensemble personnalisé d'autorisations pour l'exploitation d'un ensemble personnalisé de centrales intrusion. Un administrateur ACE peut créer plusieurs profils d'autorisation de centrale pour les diverses responsabilités de divers groupes de détenteurs de carte.

Chemin d'accès à la boîte de dialogue

– Menu principal > **Données système** > **Autorisation profils pour les centrales intrusion**

Procédure

1. Cliquez sur  pour créer un nouveau profil
2. (Obligatoire) Entrez un nom unique pour le profil.
3. (Facultatif) Entrez une description en texte libre pour la centrale

4. Sous la liste **Centrales assignées**, cliquez sur **Ajouter...** pour ajouter une ou plusieurs centrales à partir d'une liste contextuelle de centrales disponibles sur le réseau.
   À l'inverse, sélectionnez une ou plusieurs centrales et cliquez sur **Supprimer** pour les retirer de la liste.
5. Cliquez sur une centrale dans la liste **Centrales assignées** pour la sélectionner.
   – Dans le volet **Autorisations**, une liste s'affiche et elle contient toutes les zones d'intrusion appartenant à la centrale sélectionnée.
6. Dans la liste **Autorisations**, colonne **Niveaux d'autorité**, sélectionnez un niveau d'autorité pour chaque zone d'intrusion de la centrale à inclure dans ce profil.
   – Les niveaux d'autorité sont définis et gérés dans RPS. Ils peuvent y être également personnalisés. Assurez-vous de connaître la définition du niveau d'autorité dans RPS avant de l'attribuer à un profil.
   – Par défaut, **L1** est le plus haut niveau d'autorité, suivis des niveaux plus restreints **L2**, **L3**, etc.
   – Si vous laissez une cellule vide, le destinataire de ce profil n'aura **pas** d'autorisation sur la zone d'intrusion choisie sur la centrale sélectionnée.
7. Répétez ce processus pour toutes les zones d'intrusion de toutes les centrales à inclure dans ce profil.
8. (Facultatif) Depuis la liste **Groupe utilisateur**, sélectionnez un groupe d'utilisateurs de la centrale afin de restreindre les autorisations à certaines périodes.
   – Les groupes d'utilisateurs sont définis et gérés dans RPS. Ils peuvent y être également personnalisés. Assurez-vous de connaître la définition de groupe utilisateur dans RPS avant d'attribuer le groupe d'utilisateurs à un profil.
9. Cliquez sur  (Enregistrer) pour enregistrer les modifications.

11.4 Attribuer des profils d'autorisation de centrales à des détenteurs de carte

Introduction
Cette section décrit comment attribuer différents profils d'autorisation de centrale à différents types ou groupes de détenteurs de carte.

Condition préalable
Vous avez défini un ou plusieurs profils d'autorisation de centrale sur le système de contrôle d'accès.

Chemin d'accès à la boîte de dialogue
Menu principal > **Personnes** > **Cartes**

Procédure
1. Comme vous le faites habituellement, recherchez et sélectionnez le détenteur de carte souhaité dans la base de données.
2. Clique l'onglet **Intrusion**.
3. Sur l'onglet **Intrusion**, cochez la case **Utilisateur de la centrale.**
4. (Obligatoire) Dans le champ **Mot de passe**, saisissez un mot de passe avec lequel ce détenteur de carte gèrera les centrales intrusion.
   – Si nécessaire, utilisez le bouton permettant de générer un nouveau mot de passe inutilisé.
5. Dans la liste **Bade**, sélectionnez l'une des informations d'identification de contrôle d'accès affectées à ce détenteur de carte.

6. (Facultatif) Dans le champ **Numéro de contrôle à distance**, saisissez le numéro imprimé sur le contrôle à distance du détenteur de carte pour les centrales intrusion.
7. Dans la liste **Langue**, sélectionnez la langue dans laquelle le détenteur de carte préfère lire les boîtes de dialogue de centrale.
8. Si le détenteur de la carte doit utiliser l'application pour smartphone Bosch pour les centrales intrusion, cochez la case **Accès distant**.
9. Dans la liste **Profil d'autorisation**, sélectionnez un profil d'autorisation de centrale approprié pour le détenteur de la carte.
10. Cliquez sur (Enregistrer) pour enregistrer les modifications.
    - Ce profil d'autorisation de centrale, avec toutes ses centrales et autorisations, est attribué au détenteur de la carte. Le détenteur de la carte devient ainsi un opérateur des centrales intrusion.

Notez que vous pouvez également utiliser les champs de données de cette boîte de dialogue avec le bouton pour rechercher des détenteurs de carte dans la base de données.

11.5 Contrôle des portes via les modules B901 sur les centrales intrusion

Dans AMS 4.0.1 et versions ultérieures, les modules d'interface de contrôle d'accès B901 peuvent être contrôlés via AMS Map View.
Le B901 est un simple contrôleur de porte qu'un administrateur système connecte aux centrales intrusion Bosch. Vous connectez la centrale intrusion correspondante à AMS comme décrit dans les sections précédentes.
Vous ne configurez pas le B901 dans l'éditeur de dispositif.
Le B901 peut verrouiller/déverrouiller, sécuriser/déverrouiller et activer le verrouillage des portes, mais il fournit des informations d'état limitées au système de contrôle d'accès. Par exemple, il ne communique pas si une porte a été physiquement ouverte plutôt que simplement déverrouillée.
Comme tous les autres dispositifs d'intrusion, afin d'envoyer des commandes au B901 depuis AMS Map View, vous devez activer Map View pour la centrale correspondante dans la boîte de dialogue AMS :
Menu principal > **Configuration** > **Centrales > Administration de centrale**

Téléscripteur à balayage Map View et portes B901

Afin de fournir des informations correctes à l'application du **téléscripteur à balayage** dans AMS Map View, les identifiants des portes B901 doivent correspondre aux identifiants de leurs points de porte. Autrement dit, la porte 1 doit être affectée au point de porte 1, la porte 2 au point de porte 2, etc.

Doors 1 - 4	Door 1	Door 2	Door 3	Door 4
Door Name Text	Door 1	Door 2	Door 3	Door 4
Door Name Text (Second Language)				
Door Source	SDI2 (B901)	SDI2 (B901)	SDI2 (B901)	SDI2 (B901)
Entry Area	1	1	1	1
Associated Keypad #	Keypad 1	Keypad 1	Keypad 1	Keypad 1
Custom Function	Disabled	Disabled	Disabled	Disabled
Door Point	1	2	3	4
Door Point Debounce	600ms	600ms	600ms	600ms

Effectuez ces affectations au contrôleur de porte B901 dans l'outil RPS qui configure les centrales de détection d'intrusion et les contrôleurs.

12 Configurer des opérateurs et des postes de travail

Introduction aux droits d'administration de contrôle d'accès

Les droits d'administration du système de contrôle d'accès déterminent les boîtes de dialogue système qui peuvent être ouvertes et les fonctions qui peuvent y être exécutées. Des droits peuvent être attribués à la fois aux opérateurs et aux postes de travail.

Les droits d'un poste de travail peuvent restreindre temporairement les droits de son opérateur, car les opérations critiques pour la sécurité ne doivent être effectuées qu'à partir de postes de travail particulièrement sécurisés.

Les droits sont attribués aux opérateurs et aux postes de travail dans des lots appelés **Profils.** Chaque profil est adapté aux fonctions d'un type particulier d'opérateur ou de poste de travail.

Chaque opérateur ou poste de travail peut avoir plusieurs profils d'autorisation.

Procédure générale et chemins d'accès aux boîtes de dialogue

1. Créez les postes de travail dans l'éditeur de dispositif :

   Configuration > **Données de dispositif** > **Postes de travail** 
2. Créez des profils de poste de travail dans la boîte de dialogue :
   Opérateurs et postes de travail > **Profils de poste de travail**.
3. Attribuez des profils aux postes de travail dans la boîte de dialogue :
   Opérateurs et postes de travail > **Droits du poste de travail**
4. Créez des profils d'opérateur dans la boîte de dialogue :
   Opérateurs et postes de travail > boîte de dialogue **Profils d'utilisateur**.
5. Attribuez des profils aux opérateurs dans la boîte de dialogue :
   Opérateurs et postes de travail > boîte de dialogue **Droits de l'utilisateur**

12.1 Créer les postes de travail

Les postes de travail sont les ordinateurs à partir desquels les opérateurs gèrent le système de contrôle d'accès.

En premier lieu, un poste de travail doit être « créé », c'est-à-dire que l'ordinateur est enregistré au sein du système de contrôle d'accès.

Chemin d'accès à la boîte de dialogue

Configuration > **Données du dispositif** > **Postes de travail**

Procédure

1. Effectuez un clic-droit sur **DMS** et sélectionnez **Nouvel objet** dans le menu contextuel, ou cliquez sur ✚ dans la barre d'outils.
2. Entrez les valeurs des paramètres :
   - Le **Nom** du poste de travail doit correspondre exactement au nom de l'ordinateur
   - La **Description** est facultative. Elle peut être utilisée, par exemple, pour décrire la fonction et l'emplacement du poste de travail
   - **Connexion via le lecteur** Ne cochez pas cette case sauf si les opérateurs doivent se connecter à ce poste de travail en présentant les cartes à un lecteur d'inscription connecté à ce poste de travail. Pour plus de détails, voir la section

– **Déconnexion automatique après un délai d'inactivité :** délai (en nombre de secondes) au terme duquel une session de connexion via le lecteur d'inscription est automatiquement arrêtée. Laissez sur `0` pour une durée illimitée.

12.2 Créer des profils de poste de travail

Introduction aux profils de poste de travail

En fonction de son emplacement physique, un poste de travail de contrôle d'accès doit être soigneusement configuré en ce qui concerne son utilisation, par exemple :

– Quels opérateurs peuvent l'utiliser
– Quelles informations d'identification sont nécessaires pour l'utiliser
– Quelles tâches de contrôle d'accès peuvent être effectuées à partir de celui-ci

Un profil de poste de travail est un ensemble de droits qui définit les éléments suivants :

– Les menus du gestionnaire de dialogues et les boîtes de dialogue utilisables sur un poste de travail
– Le ou les profils utilisateur dont un opérateur doit disposer pour se connecter à ce poste de travail.

Remarque!

Les profils de poste de travail remplacent les profils utilisateur
Un opérateur ne peut utiliser que les droits de son profil d'utilisateur qui sont également inclus dans le profil de poste de travail de l'ordinateur sur lequel il est connecté. Si les profils opérateur et poste de travail n'ont pas de droits en commun, l'utilisateur n'aura pas tous les droits sur ce poste de travail.

Chemin d'accès à la boîte de dialogue

Configuration > **Opérateurs et postes de travail** > **Profils de poste de travail**

Créer un profil de poste de travail

1. Cliquez sur  pour créer un nouveau profil
2. Entrez un nom de profil dans le champ **Nom de profil** (obligatoire)
3. Entrez une description de profil dans le champ **Description** (facultatif mais recommandé)
4. Cliquez sur  ou sur **Appliquer** pour enregistrer vos modifications

Attribuer des droits d'exécution pour les fonctions système

1. Dans la liste **Fonctions**, sélectionnez les fonctions qui doivent être accessibles à ce poste de travail et double-cliquez dessus pour définir la valeur de colonne **Exécuter** sur `Yes`.
   – Assurez-vous également que toutes les fonctions qui ne doivent pas être accessibles sont définies sur `No`.
2. Cliquez sur  ou sur **Appliquer** pour enregistrer vos modifications

Attribuer des profils d'utilisateur à des profils de poste de travail

Dans le volet **Profil d'utilisateur**.

La liste **Profils attribués** contient tous les profils d'utilisateur autorisés à se connecter à un poste de travail avec ce profil de poste de travail.

Le champ **Profils disponibles** contient tous les autres profils. Ceux-ci ne sont pas encore autorisés à se connecter à un poste de travail avec ce profil de poste de travail.

1. Cliquez sur les boutons fléchés entre les listes pour transférer les profils sélectionnés d'une liste vers une autre.
2. Cliquez sur  ou sur **Appliquer** pour enregistrer vos modifications

Remarque!
Les profils d'administrateur par défaut de l'utilisateur (**Administrateur UP**) et le poste de travail (**Administrateur WP**) ne peuvent pas être modifiés ou supprimés.
Le profil **Administrateur WP** est irrévocablement lié au poste de travail serveur. Cela garantit qu'au moins un utilisateur peut se connecter au poste de travail serveur.

12.3 Attribuer des profils de poste de travail

Utilisez cette boîte de dialogue pour gérer les affectations de profils de poste de travail aux postes de travail. Chaque poste de travail doit avoir au moins un profil de poste de travail. S'il y a plusieurs profils, tous les droits de ces profils s'appliquent simultanément.

Chemin d'accès à la boîte de dialogue
Configuration > **Opérateurs et postes de travail** > **Droits du poste de travail**

Procédure
La liste **Profils attribués** contient tous les profils de poste de travail qui appartiennent déjà à ce poste de travail.
La liste **Profils disponibles** liste contient tous les profils de poste de travail qui n'ont pas encore été affectés à ce poste de travail.

1. Dans la liste des postes de travail, sélectionnez le poste de travail que vous souhaitez configurer
2. Cliquez sur les boutons fléchés entre les listes **Attribué** et **Disponible** pour transférer les profils sélectionnés de l'une à l'autre.
3. Cliquez sur  ou sur **Appliquer** pour enregistrer vos modifications

Remarque!
Les profils d'administrateur par défaut de l'utilisateur (**Administrateur UP**) et le poste de travail (**Administrateur WP**) ne peuvent pas être modifiés ou supprimés.
Le profil **Administrateur WP** est irrévocablement lié au poste de travail serveur. Cela garantit qu'au moins un utilisateur peut se connecter au poste de travail serveur.

12.4 Créer des profils d'utilisateur (opérateur)

Introduction aux profils d'utilisateurs
Remarque : Le terme **Utilisateur** est synonyme de **Opérateur** dans le cadre des droits des utilisateurs.
Un profil d'utilisateur est un ensemble de droits qui définit les éléments suivants :
– Les menus du gestionnaire de dialogues et les boîtes de dialogue visibles par l'opérateur.

– Les capacités de l'opérateur dans ces boîtes de dialogue, essentiellement les droits d'exécuter, de modifier, d'ajouter et de supprimer les éléments de ces boîtes de dialogue.

Les profils d'utilisateurs doivent être soigneusement configurés, en fonction de l'expérience de la personne, de son habilitation de sécurité et de ses responsabilités :

Chemin d'accès à la boîte de dialogue

Configuration > **Opérateurs et postes de travail** > **Profils d'utilisateurs**

Procédure

1. Cliquez sur  pour créer un nouveau profil
2. Entrez un nom de profil dans le champ **Nom de profil** (obligatoire)
3. Entrez une description de profil dans le champ **Description** (facultatif mais recommandé)
4. Cliquez sur  ou sur **Appliquer** pour enregistrer vos modifications

Remarque!

Choisissez des noms de profil qui décrivent clairement et précisément les capacités et les limites du profil.

Ajouter des droits d'édition et d'exécution pour les fonctions système

1. Dans le volet de liste, sélectionnez les fonctions (première colonne) et les capacités de cette fonction (**Exécuter**, **Modifier**, **Ajouter**, **Supprimer**) qui doivent être accessibles à ce profil. Double-cliquez dessus pour basculer leurs paramètres sur `Yes`.
   – Assurez-vous également que toutes les fonctions qui ne doivent pas être accessibles sont définies sur `No`.
2. Cliquez sur  ou sur **Appliquer** pour enregistrer vos modifications

12.5 Attribuer des profils d'utilisateur (opérateur)

Remarque : Le terme **Utilisateur** est synonyme de **Opérateur** dans le cadre des droits des utilisateurs.

Conditions préalables

– L'opérateur qui doit recevoir ce profil d'utilisateur est défini en tant que **Personne** sur le système de contrôle d'accès.
– Un profil d'utilisateur adapté est défini sur le système de contrôle d'accès.
  – Notez qu'il est toujours possible d'attribuer le profil utilisateur illimité **Administrateur UP**, mais cette pratique est déconseillée pour des raisons de sécurité.

Chemin d'accès à la boîte de dialogue

Configuration > **Opérateurs et postes de travail** > **Droits de l'utilisateur**

Procédure

1. Chargez l'enregistrement de personnel de l'utilisateur prévu dans la boîte de dialogue.
2. Si nécessaire, limitez la validité du profil d'utilisateur en saisissant des dates dans les champs **Valide de** et **Valide jusqu'à.**

Attribuer des profils d'utilisateur aux opérateurs
Dans le volet **Profils d'utilisateur** :
La liste **Profils attribués** contient tous les profils d'utilisateur qui sont attribués à cet utilisateur.
Le champ **Profils disponibles** contient tous les profils disponibles pour affectation.

1. Cliquez sur les boutons fléchés entre les listes pour transférer les profils sélectionnés d'une liste vers une autre.
2. Cochez la case **Administrateur global** pour donner à cet opérateur un accès en lecture/écriture aux enregistrements de personnel où l'attribut **Administré globalement** est activé. L'accès par défaut de l'opérateur à ces enregistrements de personnel est en lecture seule.
3. Cliquez sur  pour enregistrer vos modifications.

Attribuer des droits d'utilisation d'API aux opérateurs
S'il est configuré et concédé sous licence, le code de programme externe peut appeler des fonctionnalités du système de contrôle d'accès via une interface de programmation d'application ou API. Le programme externe agit via un opérateur proxy au sein du système.
La liste déroulante **Utilisation API** contrôle les capacités de l'opérateur actuel s'il est utilisé comme opérateur proxy par un code externe.
Configuration > **Opérateurs et postes de travail** > **Droits de l'utilisateur**
– Sélectionnez un paramètre dans la liste **Utilisation API**.
Les choix possibles sont :

Aucun accès	L'opérateur ne peut pas être utilisé par l'API pour exécuter des fonctions système.
Lecture seule	L'opérateur peut être utilisé par l'API pour lire les données système, mais pas pour les ajouter, les modifier ou les supprimer.
Sans limite	L'opérateur peut être utilisé par l'API pour lire, ajouter, modifier et supprimer des données système.

– Cliquez sur  pour enregistrer vos modifications

12.6 Définir des mots de passe pour les opérateurs

Comment définir des mots de passe sécurisés pour soi et pour les autres.

Introduction
Le système nécessite au moins un opérateur. L'opérateur par défaut d'une nouvelle installation a le nom d'utilisateur **Administrator** et mot de passe **Administrator**. La première étape de la configuration du système doit toujours consister à se connecter avec ces informations d'identification et de modifier le mot de passe pour **Administrator**, conformément aux stratégies de mot de passe de votre organisation.
Après cela, vous pouvez ajouter d'autres opérateurs, à la fois privilégiés et non privilégiés.

Procédure pour changer son propre mot de passe.
Conditions préalables
Vous êtes connecté au gestionnaire de dialogue.

Procédure

1. Dans le gestionnaire de dialogue, sélectionnez le menu : **Fichier** > **Changer le mot de passe**
2. Dans la fenêtre contextuelle, entrez le mot de passe actuel, le nouveau mot de passe et à nouveau le nouveau mot de passe pour confirmer.
3. Cliquez sur **Modifier**.

Notez que cette procédure est le seul moyen de modifier le mot de passe Administrator. Lors de la première connexion après une installation, le système vous demande de changer le mot de passe Administrator.

Procédure de modification des mots de passe des autres opérateurs.

Conditions préalables

Pour modifier les mots de passe des autres utilisateurs, vous devez être connecté au gestionnaire de dialogue en utilisant un compte doté de privilèges d'administrateur.

Procédure

1. Dans le menu principal du gestionnaire de dialogue, accédez à **Configuration** > **Opérateurs et postes de travail** > **Droits de l'utilisateur**
2. Dans le volet de boîte de dialogue principal, utilisez la barre d'outils pour charger l'opérateur dont vous souhaitez modifier le mot de passe.
3. Cliquez sur **Modifier le mot de passe...**
4. Dans la fenêtre contextuelle, saisissez le nouveau mot de passe et à nouveau le nouveau mot de passe pour confirmer.
5. Dans la fenêtre contextuelle, saisissez la période de validité du nouveau mot de passe, soit **Illimité** ou un nombre de jours.
   - Pour les environnements de production, il est vivement recommandé de définir une période de validité.
6. Cliquez sur **OK** pour fermer la fenêtre contextuelle.

Dans la fenêtre de dialogue principale, cliquez sur l'icône  pour enregistrer l'enregistrement utilisateur.

Notez que les sélecteurs de dates **Valide à partir de** et **Valide jusqu'à**, sous le bouton **Modifier le mot de passe...**, font référence à la validité des droits d'utilisateur dans cette boîte de dialogue, et non au mot de passe.

Informations complémentaires

Définissez toujours les mots de passe conformément à la stratégie de mot de passe de votre organisation. Pour obtenir des conseils sur la création d'une telle stratégie, vous pouvez consulter, par exemple, les conseils fournis par Microsoft à l'emplacement suivant.
https://www.microsoft.com/en-us/research/publication/password-guidance/

13 Configurer des cartes

13.1 Définition de carte

Utilisez cette boîte de dialogue pour activer, désactiver, modifier ou ajouter des définitions de carte qui seront utilisées par votre système de contrôle d'accès.

Chemin d'accès à la boîte de dialogue

– Menu principal AMS > **Configuration** > **Options** > **Définition carte**

Le système est fourni avec un ensemble de types de cartes prédéfinis. Les types de cartes prédéfinis sont affichés sur fond gris dans le tableau **Types de cartes disponibles** et ils ne peuvent pas être modifiés. Ils ne peuvent être déplacés qu'entre **Types de cartes actives** et **Types de cartes disponibles**.

13.1.1 Créer et modifier

Cliquez sur le bouton (+ vert) au-dessus de la zone de liste de droite pour créer une nouvelle entrée de liste. Contrairement aux types de cartes prédéfinis, les données des types nouvellement créés sont librement modifiables. Double-cliquez sur les champs **Nom**, **Description** et **Nombre de bits** pour les modifier.

Le nom peut avoir un maximum de 80 caractères et la description 255. Le nombre de bits est limité à 64 (si un nombre plus élevé est entré, il sera réinitialisé au maximum dès que le champ de texte perd le focus de saisie).

Remarque!

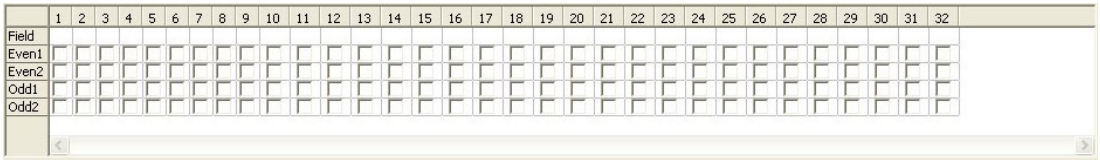
Les longueurs de bits sont utilisées pour différencier les définitions Wiegand. Par conséquent, chaque nouvelle définition doit avoir une longueur de bits unique qui n'a pas été utilisée par une définition existante.

- Pour modifier un bit de données, double-cliquez sur le champ correspondant. Pour le supprimer, sélectionnez d'abord le bit de données puis cliquez sur le bouton (x rouge).

Remarque!

Seuls les types de cartes créés par l'utilisateur peuvent être modifiés ou supprimés.

Lorsqu'un type de carte unique est sélectionné (dans les listes de gauche ou de droite), son codage est affiché dans la partie inférieure de la boîte de dialogue. L'écran affiche les bits de données sur 5 lignes et autant de colonnes que le nombre de bits dans la définition.



Chaque colonne de la ligne **Champ** peut recevoir un libellé qui détermine comment cette partie du code doit être interprétée. Les libellés disponibles sont les suivants :

F	Bâtiment : marque la partie de code pour l'affiliation à un bâtiment	
C	N° de code : partie de code contenant le numéro de carte individuel	
E1	Paire 1 : bit pour équilibrer le premier masque de parité paire	La déclaration de ces valeurs active la case à cocher de la ligne correspondante.
E2	Paire 2 : bit pour équilibrer le second masque de parité paire	
O1	Impaire 1 : bit pour équilibrer le premier masque de parité impaire	
O2	Impaire 2 : bit pour équilibrer le second masque de parité impaire	
1	Valeurs de bit de correction contenues dans le code	
0		

Dans le cas des libellés E1, E2, O1 et O2, il suffit de cocher la case sur la ligne correspondante. La case sur la ligne **Champ** sera automatiquement marquée en conséquence.
Explication :
Le signal envoyé par un lecteur lorsqu'une carte est présentée comprend une série de zéros et de uns. Pour chaque type de carte, la longueur de ce signal (c'est-à-dire le nombre de bits) est exactement définie.
En plus des données utilisateur réelles, qui sont enregistrées sous forme de données de code, le signal contient également des données de contrôle afin de a) identifier le signal comme signal de carte, et b) vérifier que la transmission est correcte.
En général, les zéros et les uns fixes sont utiles pour identifier le type de signal.
Les bits de parité, qui doivent générer un zéro (parité paire) ou un un (parité impaire) comme somme de contrôle sur les bits sélectionnés du signal, sont utilisés pour vérifier que la transmission est correcte. Les contrôleurs peuvent être configurés afin de pouvoir calculer une ou deux sommes de contrôle pour les parités paires, et une ou deux sommes de contrôle pour les parités impaires.
Dans le contrôle de liste, ces bits peuvent être marqués sur les lignes respectives pour les contrôles de parité (Paire1, Paire2, Impaire1 et Impaire2), qui doivent être inclus dans la somme de contrôle. Sur la ligne supérieure (champ) pour chaque somme de contrôle utilisée, un bit est défini pour équilibrer la somme de contrôle en fonction du type de parité. Si une option de parité n'est pas utilisée, la ligne correspondante reste simplement vide.

13.1.2 Activer/Désactiver des définitions de cartes

Jusqu'à 8 définitions de carte peuvent être actives simultanément. Les définitions à activer doivent être déplacées vers la liste de gauche **Types de carte actifs**. Pour ce faire, il suffit de sélectionner une ou plusieurs définitions sur le côté droit, et de cliquer sur le bouton flèche gauche (**<**).

Il n'est pas possible de déplacer plus de quatre définitions à la fois. Une fois les quatre définitions déplacées, tout déplacement supplémentaire est annulé. Pour ajouter plus de définitions à **Types de cartes actifs**, il sera nécessaire de supprimer un ou plusieurs de celles présentes en les sélectionnant et en les déplaçant vers la droite à l'aide du bouton (**>**), ce qui les désactive.

Remarque!
Pour utiliser des lecteurs avec les protocoles L-Bus ou BG900, activez le type de carte **Lecteur série**. Cela rend la boîte de dialogue **Dialog Bosch** de saisie manuelle disponible pour le gestionnaire de dialogue du système de contrôle d'accès.

13.1.3 Créer des données de carte dans le gestionnaire de dialogue

Saisie manuelle des données

Différentes méthodes de saisie sont utilisées pour les cartes Wiegand et Bosch.
Pour toutes les définitions Wiegand (HID 26, HID 35, HID 37 et 32 Bit CSN), la boîte de dialogue **Dialog (Wiegand)** vous permet d'entrer le **Code client** et le **N° de carte.**
Pour les lecteurs série, la boîte de dialogue **Dialog (Bosch)** contient des champs supplémentaires pour la **Version** et le **Code postal**.

Saisie des données par le lecteur d'inscription

En plus de la saisie manuelle des données, tout poste de travail peut être équipé d'un lecteur de dialogue pour la collecte des données de la carte. Utilisez un lecteur de la liste dans la boîte de dialogue suivante :

– Menu principal AMS > **Configuration** > **Options** > **Lecteur de carte**

Si le lecteur choisi est un lecteur d'entrée pour les cartes Wiegand, tous les types de cartes Wiegand actifs seront répertoriés avec le lecteur

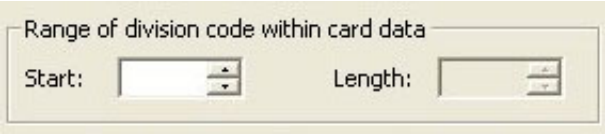
– Menu principal AMS > **Données du personnel** > **Cartes** > Bouton du lecteur> ▶ (flèche droite)

L'un de ces types de carte doit être sélectionné afin de garantir la sauvegarde correcte de l'encodage de la carte. Autrement dit, le lecteur lui-même ne peut pas être sélectionné directement mais uniquement indirectement via le choix de la définition Wiegand.
Si le type de carte requis n'apparaît pas dans la liste déroulante, vous devez l'activer dans la boîte de dialogue de définition de carte.

– Menu principal AMS > **Configuration** > **Options** > **Définition carte**

Les lecteurs d'inscription HITAG, LEGIC et MIFARE peuvent être sélectionnés directement dans la liste.

Définition de carte pour les divisions (capacité multipartie)
Si vous avez autorisé la fonction Divisions pour gérer plusieurs parties (alias « Divisions ») dans les locaux à accès contrôlé, il est possible de configurer une zone de code sur la carte qui permet à l'opérateur de distinguer les cartes des différentes divisions. Utilisez les champs facultatifs (sélectionnables uniquement si la fonction Divisions a été concédée sous licence) pour définir la position du bit de **départ** et la **longueur** du codage de la Division sur les cartes.



13.2 Configuration des codes de carte

Le codage des cartes de contrôle d'accès garantit que toutes les données de la carte sont uniques.

Chemin d'accès à la boîte de dialogue
Menu principal > **Configuration** > **Options** > **Configuration du codage de la carte**
Saisie des nombres dans la boîte de dialogue
Saisie des nombres dans la boîte de dialogue
Pour plus de commodité, vous pouvez saisir des nombres au format décimal ou hexadécimal. Sélectionnez les cases d'option **Hexadécimal** ou **Décimal** selon le format spécifié par le fabricant des cartes.
Le volet de dialogue principal est divisé en deux groupes, qui sont décrits plus en détail ci-dessous :

- **Code par défaut de la carte**
- **Vérifier uniquement les valeurs d'adhésion**

Code par défaut de la carte
Utilisez ces champs de saisie de texte pour définir les valeurs **Version**, **Code pays** et **Code client** qui sont attribuées au numéro de carte lorsque la carte est enregistrée dans le système. Si les champs ne sont pas accessibles en écriture, ils ne sont pertinents pour aucune des définitions de carte actives. Pour le code Bosch, tous les champs sont accessibles en écriture.
Si la carte est inscrite manuellement sur un poste de travail opérateur, une boîte de dialogue apparaît affichant les valeurs par défaut qui peuvent être personnalisées pour chaque carte.

Saisie des données de code :
Si les données sont fournies par le fabricant sous forme de valeurs décimales, sélectionnez la case d'option Décimal et saisissez les valeurs fournies, par exemple :
Version : 2

Code pays : 99
Code client : 56720
Cliquez sur **Appliquer** pour stocker les données.

Remarques concernant la saisie des données de code par défaut :
Les données par défaut sont stockées dans le registre du système d'exploitation et chaque numéro de badge est ajouté au moment de l'encodage. L'inscription prend la forme d'une valeur **hexadécimale à 8 chiffres** avec des zéros non significatifs si nécessaire.
Si les numéros de code sont complètement transférés, le système peut passer de la décimale à l'hexadécimal, compléter à 8 positions avec des zéros non significatifs et enregistrer le paramètre système approprié.

- Exemple :
  - Entrée : 56720
  - Conversion : DD90
  - Enregistré sous : 0000DD90

Si les numéros de code sont transférés séparément (forme fractionnée), alors uniquement la forme **décimale**. Ils sont convertis en un nombre décimal à 10 chiffres qui est construit comme suit :

- Version : 2 chiffres
- Code pays : 2 chiffres
- Code client : 6 chiffres
- Si l'un des 10 chiffres est toujours vide, il est complété par des zéros non significatifs
  - Exemple : 0299056720

Cette valeur décimale à 10 chiffres est convertie et stockée sous forme de valeur hexadécimale à 8 chiffres.

- Exemple :
  - décimale : 0299056720
  - hexadécimale : 11D33E50

Remarque!
Le système valide les valeurs hexadécimales, dans le cas de numéros de code fractionnés, afin d'éviter la saisie de codes de pays non valides (au-dessus de l'hexadécimale 63 ou de la décimale 99) et de codes client non valides (au-dessus de hexadécimale F423F ou décimale 999,999)

Remarque!
Si la capture de la carte s'effectue via un lecteur de dialogue connecté, les valeurs par défaut sont attribuées automatiquement. Il n'est pas possible de remplacer les valeurs par défaut lors de la capture à partir d'un lecteur.
Pour ce faire, le type de capture doit être réglé sur **Dialogue**

La saisie manuelle du numéro de carte est au format décimal.
Lors de l'enregistrement des données, une valeur décimale à 10 chiffres (avec des zéros non significatifs) est créée, laquelle est ensuite convertie en une valeur hexadécimale à 8 chiffres. Cette valeur est maintenant stockée avec les données de code par défaut en tant que numéro de code à 16 chiffres de la carte.

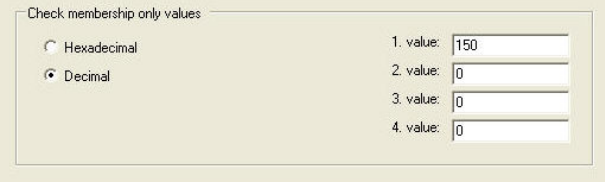
- Exemple :
  - Saisie du numéro de carte : 415
  - 10 chiffres : 0000000415
  - Converti en hexadécimal : 0000019F

– Combiné avec les données de code par défaut (voir ci-dessus) et enregistré comme numéro de code du badge : 11D33E500000019F

Vérifier uniquement les valeurs d'adhésion

Vérifier l'adhésion signifie uniquement que les informations d'identification sont vérifiées uniquement pour l'adhésion à une entreprise ou à une organisation, et non pour identifier un individu. Par conséquent, vous ne devez pas utiliser **Vérifier uniquement les valeurs d'adhésion** pour les lecteurs qui donnent accès à des zones de haute sécurité.

Utilisez ce groupe d'options pour saisir jusqu'à quatre codes entreprise ou client. Les données peuvent être saisies sous forme décimale ou hexadécimale, mais sont stockées sous forme de valeurs décimales dans le registre du système d'exploitation.



Sélectionnez le lecteur dans l'éditeur de dispositif, DevEdit, et activez le paramètre de lecteur **Vérification d'adhésion**.

Seuls les codes de l'entreprise ou du client dans les données de la carte sont lus et vérifiés par rapport aux valeurs stockées.

Remarque!

Vérification d'adhésion fonctionne uniquement avec des définitions de carte prédéfinies dans le système (fond gris), et non avec des définitions personnalisées.

14 Configurer des contrôleurs

Introduction

Les contrôleurs du système de contrôle d'accès sont les dispositifs virtuels et physiques qui envoient des commandes au matériel périphérique au niveau des entrées (lecteurs et portes), et renvoient les requêtes des lecteurs et des portes vers le logiciel de prise de décision central.

Les contrôleurs stockent des copies de certaines informations sur le périphérique et le détenteur de carte du logiciel central et, s'ils sont configurés, peuvent prendre des décisions de contrôle d'accès même lorsqu'ils sont temporairement isolés du logiciel central.

Le logiciel de prise de décision est le Système de gestion des données.

Les contrôleurs sont de deux types :

- Contrôleur d'accès principal, connu sous le nom de MAC, et son équivalent de sauvegarde redondant, le RMAC.
- Contrôleurs d'accès locaux, appelés LAC ou AMC.

Les contrôleurs sont configurés dans l'éditeur de dispositif, DevEdit

Chemin d'accès à la boîte de dialogue vers l'éditeur de dispositif

Menu principal > **Configuration** > **Données du dispositif** > **Arborescence des dispositifs**

Utiliser l'éditeur de dispositif, DevEdit

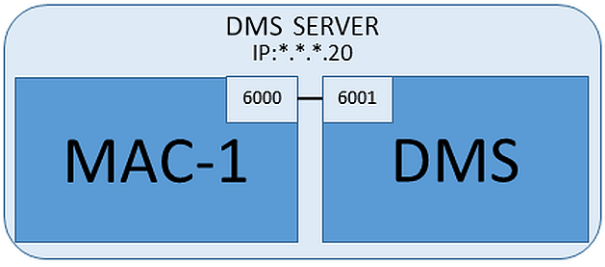
L'utilisation de base de DevEdit est décrite dans la section **Utilisation de l'éditeur de dispositif**, sur le lien ci-dessous.

Se reporter à

- *Utiliser l'éditeur de dispositif, page 24*

14.1 Configurer des MAC et des RMAC

14.1.1 Configurer un MAC sur le serveur DMS



Pour une configuration système minimale, un MAC est nécessaire. Dans ce cas, le MAC peut résider sur le serveur DMS.

Procédure

Sur le serveur DMS, ouvrez l'éditeur de dispositif et créez un MAC dans l'arborescence des dispositifs comme décrit dans la section **Utilisation de l'éditeur de dispositif**.

Sélectionnez le MAC dans l'éditeur de dispositif. Sur l'onglet **MAC**, indiquez les valeurs de paramètre suivantes :

Paramètre	Description
Nom	Nom qui doit apparaître dans l'arborescence des dispositifs, Par exemple MAC-1.
Description	Description facultative au profit des opérateurs de réseau
Avec RMAC (case à cocher)	**<Laisser vide>**
Port RMAC	**<Laisser vide>**
Actif (case à cocher)	**Désélectionnez** cette case à cocher pour suspendre temporairement la synchronisation en temps réel entre ce MAC et DMS. Ceci est utile après des mises à jour DMS sur des systèmes plus grands, afin d'éviter de redémarrer tous les MAC à la fois.
Charger dispositifs (case à cocher)	**Désélectionnez** cette case à cocher pour suspendre temporairement la synchronisation en temps réel entre ce MAC et ses dispositifs subordonnés. Cela réduit le temps nécessaire pour ouvrir un MAC dans l'éditeur de dispositif.
Adresse IP	`Localhost 127.0.0.1`
Fuseau horaire	**IMPORTANT :** Le fuseau horaire du MAC et de tous ses AMC subordonnés.
Division	(Le cas échéant) La division à laquelle appartient le MAC.

Étant donné que ce MAC local n'a pas de MAC de reprise redondant, il n'est pas nécessaire d'exécuter l'outil MACInstaller pour cela. Laissez simplement à blanc les deux paramètres RMAC sur l'onglet **MAC**.

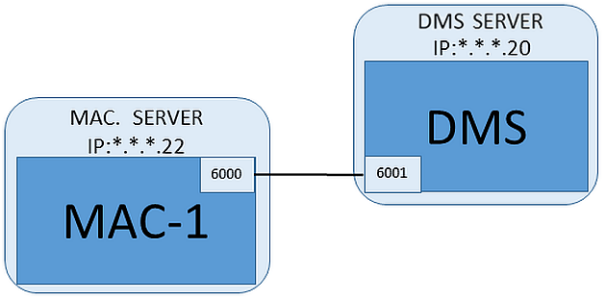
14.1.2 Préparer des serveurs MAC pour exécuter des MAC et des RMAC

Cette section décrit comment préparer des ordinateurs à devenir des Serveurs MAC.
Par défaut, le premier MAC sur un système de contrôle d'accès fonctionne sur le même ordinateur que son Serveur de gestion de données (DMS) ; cependant, pour une meilleure résilience, il est recommandé que le MAC s'exécute sur un ordinateur séparé, lequel peut assumer les tâches de contrôle d'accès si l'ordinateur DMS tombe en panne.
Les ordinateurs séparés sur lesquels résident les MAC ou RMAC sont appelés serveurs MAC, qu'ils hébergent un MAC ou un RMAC.
Afin de fournir une capacité de basculement, les MAC et les RMAC **doivent** s'exécuter sur des serveurs MAC séparés.
Assurez-vous que les conditions suivantes sont remplies sur tous les serveurs MAC participants :

1. Les systèmes d'exploitation de tous les serveurs MAC doivent être actuellement pris en charge par Microsoft et avoir les dernières mises à jour installées.
2. L'utilisateur Administrateur sur tous les serveurs a le même mot de passe
3. Vous êtes connecté en tant qu'administrateur (si vous utilisez MSTC, utilisez uniquement les sessions /Admin /Console)
4. Désactivez IP V6. Notez attentivement l'adresse IP V4 de chaque serveur.

5. Activer .NET 3.5 sur tous les ordinateurs participants.
   Remarque : Sur les systèmes d'exploitation Windows 10 et Windows Server, il est activé en tant que fonctionnalité.
6. Redémarrez l'ordinateur.

14.1.3 Configurer un MAC sur son propre serveur MAC



– Le serveur MAC est préparé comme décrit dans la section

1. Sur le serveur DMS, dans l'éditeur de dispositif,
   – Faites un clic droit sur le MAC et sélectionnez **Désactiver tous les LAC**.
   – Désactivez le MAC en désélectionnant les cases à cocher **Activer** et **Charger les dispositifs** pour ce MAC.
2. Sur le serveur MAC, à l'aide du programme Windows `services.msc`
   – Arrêtez le service MAC **AUTO_MAC2**
   – Définissez le **Type de démarrage** de ce service MAC sur **Manuel**.
3. Démarrez le `MACInstaller.exe`
   – Pour AMS, celui-ci se trouve sur le support d'installation AMS `\AddOns\MultiMAC\MACInstaller` (voir la section, Utiliser l'outil MACInstaller ci-dessous).
4. Parcourez les écrans de l'outil en fournissant des valeurs pour les paramètres suivants.

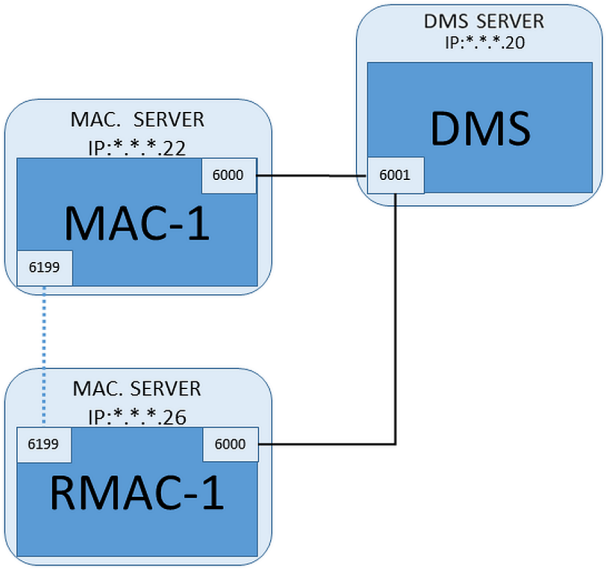
N° écran	Paramètre	Description
3	**Dossier de destination**	Répertoire local dans lequel le MAC doit être installé. Prenez la valeur par défaut dans la mesure du possible.
4	**Serveur**	Nom ou adresse IP du serveur sur lequel s'exécute le DMS.
4	**Port (Port vers DMS)**	Port sur le serveur DMS qui sera utilisé pour recevoir la communication du MAC**.** Utilisez 6001 pour le premier MAC sur le DMS et incrémentez de 1 pour chaque MAC suivant.
4	**Numéro (numéro de système MAC)**	Définissez 1 pour cela et tous les MAC (par opposition aux RMAC)**.**
4	**Twin (nom ou adresse IP du MAC partenaire)**	Laissez ce champ à blanc tant que ce MAC ne doit pas avoir de RMAC.

5. Sur le serveur DMS, sélectionnez le MAC dans l'éditeur de dispositif.
6. Sur l'onglet **MAC**, indiquez les valeurs des paramètres suivants :

Paramètre	Description
Nom	Nom qui doit apparaître dans l'arborescence des dispositifs, Par exemple MAC-1.
Description	Description facultative au profit des opérateurs de réseau
Avec RMAC (case à cocher)	**<Laisser vide>**
Port RMAC	**<Laisser vide>**
Actif (case à cocher)	Cochez cette case maintenant
Charger dispositifs (case à cocher)	Cochez cette case maintenant
Adresse IP	Adresse IP de l'ordinateur serveur MAC.
Fuseau horaire	**IMPORTANT :** Le fuseau horaire du MAC et de tous ses AMC subordonnés.
Division	(Le cas échéant) La **Division** à laquelle appartient le MAC.

14.1.4 Ajouter des RMAC aux MAC

Remarque!
N'ajoutez pas de RMAC aux MAC ordinaires tant que les MAC ordinaires ne sont pas installés et opérationnels.
La réplication des données pourrait autrement être empêchée ou endommagée.



– Le MAC de ce RMAC est installé comme décrit dans les sections précédentes et fonctionne correctement.
– L'ordinateur serveur MAC pour le RMAC est préparé comme décrit dans la section

Les MAC peuvent être jumelés avec des MAC redondants (RMAC) pour fournir une capacité de basculement, et donc un contrôle d'accès plus résilient. Dans ce cas, les données de contrôle d'accès sont répliquées automatiquement entre les deux. Si l'une des paires échoue, l'autre prend le contrôle des contrôleurs d'accès locaux situés en dessous.

Sur le serveur DMS, dans le navigateur de configuration

1. Dans l'éditeur de dispositif, sélectionnez le MAC pour lequel le RMAC doit être ajouté.
2. Sur l'onglet **MAC**, modifiez les valeurs des paramètres suivants :

Paramètre	Description
Avec RMAC (case à cocher)	**Désélectionnez** cette case à cocher jusqu'à ce que vous ayez installé le RMAC correspondant sur le serveur de connexion de basculement redondant
Actif (case à cocher)	**Désélectionnez** cette case à cocher pour suspendre temporairement la synchronisation en temps réel entre ce MAC et DMS. Ceci est utile après des mises à jour DMS sur des systèmes plus grands, afin d'éviter de redémarrer tous les MAC à la fois.
Charger dispositifs (case à cocher)	**Désélectionnez** cette case à cocher pour suspendre temporairement la synchronisation en temps réel entre ce MAC et ses dispositifs subordonnés. Cela réduit le temps nécessaire pour ouvrir un MAC dans l'éditeur de dispositif.

3. Cliquez sur le bouton **Appliquer**
4. Gardez l'éditeur de dispositif ouvert car nous y reviendrons.

Sur le serveur MAC pour le RMAC

Pour configurer le RMAC, procédez comme suit :

- Sur son propre serveur MAC préparé, exécutez l'outil MACInstaller (voir Utiliser l'outil MACInstaller) et définissez les paramètres suivants :
  - **Serveur** : nom ou adresse IP de l'ordinateur serveur DMS
  - **Port** : `6001` (identique à celui du MAC)
  - **Numéro** : `2` (tous les RMAC ont le numéro 2)
  - **Twin** : adresse IP de l'ordinateur sur lequel s'exécute le MAC jumeau.

Retour dans l'éditeur de dispositif sur le serveur DMS

1. **IMPORTANT :** Assurez-vous que le MAC et le RMAC, sur leurs ordinateurs respectifs, sont en cours d'exécution et visibles l'un pour l'autre sur le réseau.
2. Sur l'onglet **MAC**, modifiez les paramètres comme suit :

Paramètre	Description
Avec RMAC (case à cocher)	**Sélectionné** Un nouvel onglet intitulé **RMAC** apparaît en regard de l'onglet **MAC**.
Port RMAC	`6199` (valeur statique par défaut) Tous les MAC et RMAC utilisent ce port pour vérifier si leurs partenaires sont opérationnels et accessibles**.**
Actif (case à cocher)	**Sélectionné** Cela permet la synchronisation entre ce MAC et ses dispositifs subordonnés.

Paramètre	Description
Charger dispositifs (case à cocher)	**Sélectionné** Cela réduit le temps nécessaire pour ouvrir un MAC dans l'éditeur de dispositif.

3. Sur l'onglet **RMAC**, indiquez les valeurs des paramètres suivants :

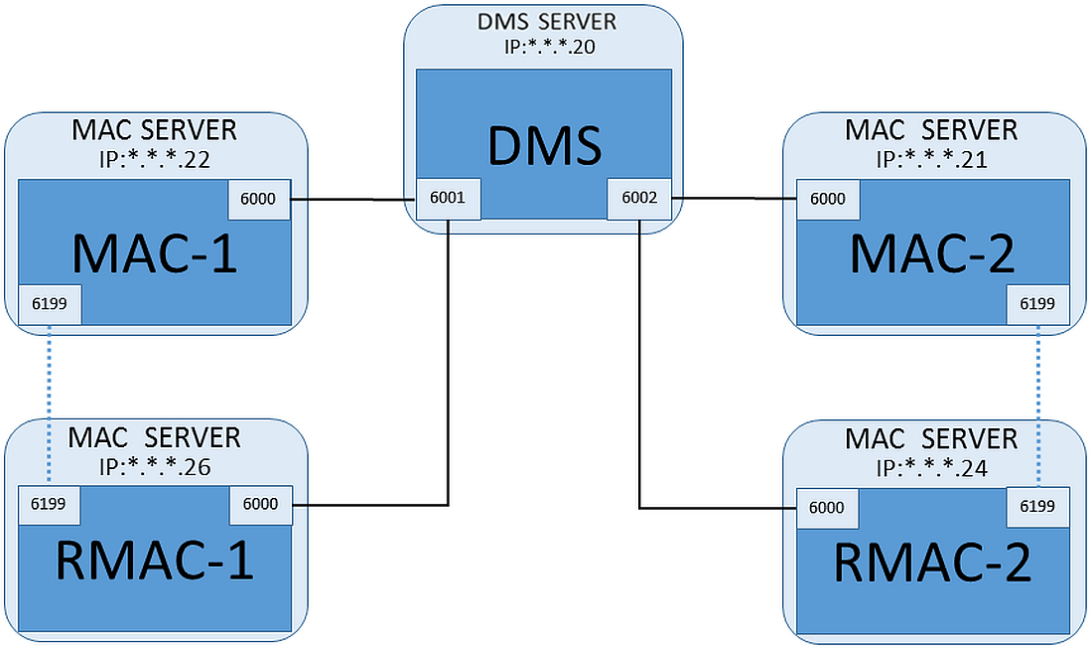
Paramètre	Description
Nom	Nom qui doit apparaître dans l'arborescence des dispositifs. Par exemple, si le MAC correspondant est nommé MAC-01, ce RMAC peut être nommé RMAC-01.
Description	Documentation en option pour les opérateurs de contrôle d'accès.
Adresse IP	Adresse IP du RMAC.
Port MAC	`6199` (la valeur statique par défaut) Tous les MAC et RMAC utilisent ce port pour vérifier si leurs partenaires sont opérationnels et accessibles**.**

Se reporter à

– *Utiliser l'outil d'installation MAC, page 55*

14.1.5 Ajouter d'autres paires MAC/RMAC

En fonction du nombre d'entrées à contrôler et du degré de tolérance aux pannes requis, un grand nombre de paires MAC/RMAC peuvent être ajoutées à la configuration du système. Pour connaître le nombre exact pris en charge par votre version, veuillez consulter la fiche technique correspondante.



Pour chaque paire MAC/RMAC supplémentaire...

1. Préparez les ordinateurs séparés pour MAC et RMAC comme décrit dans la section
2. Configurez le MAC comme décrit dans la section

3. Configurez le RMAC pour ce MAC comme décrit dans la section

Notez que chaque paire MAC/RMAC transmet à un port distinct sur le serveur DMS. Par conséquent, pour le paramètre **Port (Port vers DMS)** dans `MACInstaller.exe`, utilisez :
– `6001` pour les deux ordinateurs de la première paire MAC/RMAC
– `6002` pour les deux ordinateurs de la seconde paire MAC/RMAC
– etc.
Dans le port de l'éditeur de dispositif, `6199` peut toujours être utilisé pour les paramètres **Port MAC** et **Port RMAC**. Ce numéro de port est réservé pour l'« établissement de liaison » au sein de chaque paire MAC/RMAC, chacun sachant si son partenaire est accessible ou non.

Remarque!
Réactiver des MAC après des mises à niveau du système
Après une mise à niveau du système, les MAC et leurs AMC sont désactivés par défaut. Pendez à les réactiver dans le navigateur de configuration en cochant les cases correspondantes dans l'éditeur de dispositif.

14.1.6 Utiliser l'outil d'installation MAC

`MACInstaller.exe` est l'outil standard pour installer les MAC et RMAC sur leurs propres ordinateurs (serveurs MAC). Il collecte les valeurs de paramètres pour un MAC ou un RMAC et apporte les modifications nécessaires dans le registre Windows.

Remarque!
Étant donné que l'outil apporte des modifications dans le registre Windows, il est nécessaire d'arrêter tout processus MAC en cours d'exécution avant de le reconfigurer.

L'outil MACInstaller se trouve sur le support d'installation dans le chemin suivant :
– `\AddOns\MultiMAC\MACInstaller.exe`
Sur plusieurs écrans, il collecte les valeurs des paramètres ci-dessous.

N° écran	Paramètre	Description
3	**Dossier de destination**	Répertoire local dans lequel le MAC doit être installé.
4	**Serveur**	Nom ou adresse IP du serveur sur lequel s'exécute le DMS.
4	**Port (Port vers DMS)**	Numéro de port sur le serveur DMS qui sera utilisé pour la communication entre le MAC et le DMS. **Voir ci-dessous pour plus de détails.**
4	**Numéro (numéro de système MAC)**	Définissez 1 pour tous les MAC d'origine. Définissez 2 pour tous les MAC de basculement redondants (RMAC).
4	**Twin (nom ou adresse IP du MAC partenaire)**	Adresse IP de l'ordinateur sur lequel doit s'exécuter le partenaire de basculement redondant pour ce serveur MAC.

N° écran	Paramètre	Description
		Si non applicable, laissez ce champ vide.

Paramètre : Port (Port vers DMS)
Les numéros de port ont le schéma numéroté suivant :
– Dans un système non hiérarchique, où n'existe qu'un seul serveur DMS, chaque MAC et son RMAC correspondant transmettent à partir du même numéro de port, généralement 6000. Le DMS ne peut communiquer qu'avec une seule de chaque paire MAC/RMAC à la fois.
– Le DMS reçoit des signaux de la première paire MAC ou MAC/RMAC sur le port 6001, de la deuxième paire MAC ou MAC/RMAC sur le port 6002, et ainsi de suite.

Paramètre : Number (Numéro de système MAC)
Ce paramètre permet de distinguer les MAC d'origine des RMAC :
– Tous les MAC d'origine portent le numéro 1.
– Tous les MAC de basculement redondants (RMAC) ont le numéro 2

Paramètre : Configure Only (case d'option)
Sélectionnez cette option pour modifier la configuration d'un MAC existant sur le serveur DMS principal, en particulier pour l'informer d'un RMAC nouvellement installé sur un autre ordinateur.
Dans ce cas, entrez l'adresse IP ou le nom d'hôte du RMAC dans le paramètre **Twin**.

Paramètre : Update Software (case d'option)
Sélectionnez cette option sur un ordinateur autre que le serveur DMS principal, soit pour installer un RMAC, soit pour modifier sa configuration.
Dans ce cas, entrez l'adresse IP ou le nom d'hôte du second MAC du RMAC dans le paramètre **Twin**.

14.2 Configuration des contrôleurs d'accès locaux (LAC)

Création d'un contrôleur d'accès local AMC
Les contrôleurs d'accès modulaire AMC (Access Modular Controllers) sont subordonnés aux contrôleurs d'accès principaux (MAC) dans l'éditeur du dispositif.
Pour créer un AMC :
1. Dans l'éditeur du dispositif, cliquez avec le bouton droit sur un MAC et choisissez **Nouvel objet** depuis le menu contextuel
   ou
2. Cliquez sur le bouton ✚.
3. Choisissez l'un des types AMC suivants dans la boîte de dialogue qui s'affiche :

AMC 4W (par défaut)	avec quatre interfaces de lecteur Wiegand pour connecter jusqu'à quatre lecteurs
AMC 4R4	avec quatre interfaces de lecteur RS485 pour connecter jusqu'à huit lecteurs

Résultat : une nouvelle entrée AMC du type choisi est créée dans la hiérarchie DevEdit

AMC2 4W	**A**ccess **M**odular **C**ontroller avec quatre lecteurs Wiegand.	Un maximum de quatre lecteurs Wiegand peut être configuré pour connecter jusqu'à quatre entrées. Le contrôleur prend en charge huit signaux d'entrée et huit signaux de sortie. Si nécessaire, les cartes d'extension peuvent fournir jusqu'à 48 signaux d'entrée et de sortie supplémentaires.
AMC2 4R4	**A**ccess **M**odular **C**ontroller avec quatre interfaces de lecteur RS485	Un maximum de huit lecteurs RS485 peut être configuré pour connecter jusqu'à huit entrées. Le contrôleur prend en charge huit signaux d'entrée et huit signaux de sortie. Si nécessaire, les cartes d'extension peuvent fournir jusqu'à 48 signaux d'entrée et de sortie supplémentaires.
AMC2 8I-8O-EXT	Carte d'extension pour AMC avec huit signaux d'entrée et de sortie	Rendez disponibles des signaux supplémentaires. Il est possible de connecter jusqu'à trois cartes d'extension à un AMC
AMC2 16I-16O-EXT	Carte d'extension pour AMC avec seize signaux d'entrée et de sortie	
AMC2 8I-8O-4W	Carte d'extension pour Wiegand AMC avec huit signaux d'entrée et de sortie	

Activation/Désactivation des contrôleurs

Lors de sa création initiale, un nouveau contrôleur a l'option suivante (case à cocher) sélectionnée : **Communication avec l'hôte permise**.

Cela ouvre la connexion réseau entre le MAC et les contrôleurs, de sorte que toutes les données de configuration modifiées ou étendues sont propagées automatiquement aux contrôleurs.

Désactivez cette option pour économiser la bande passante du réseau, et ainsi améliorer les performances, tout en créant plusieurs contrôleurs et les dispositifs qui en dépendent (entrées, portes, lecteurs, cartes d'extension). Dans l'éditeur de dispositif, les dispositifs sont alors signalés par des icônes grisées.

IMPORTANT : Veillez à réactiver cette option une fois la configuration des dispositifs terminée. Les contrôleurs seront ainsi continuellement mis à jour avec toutes les modifications de configuration apportées à d'autres niveaux.

Mélange de types de contrôleurs dans une seule installation

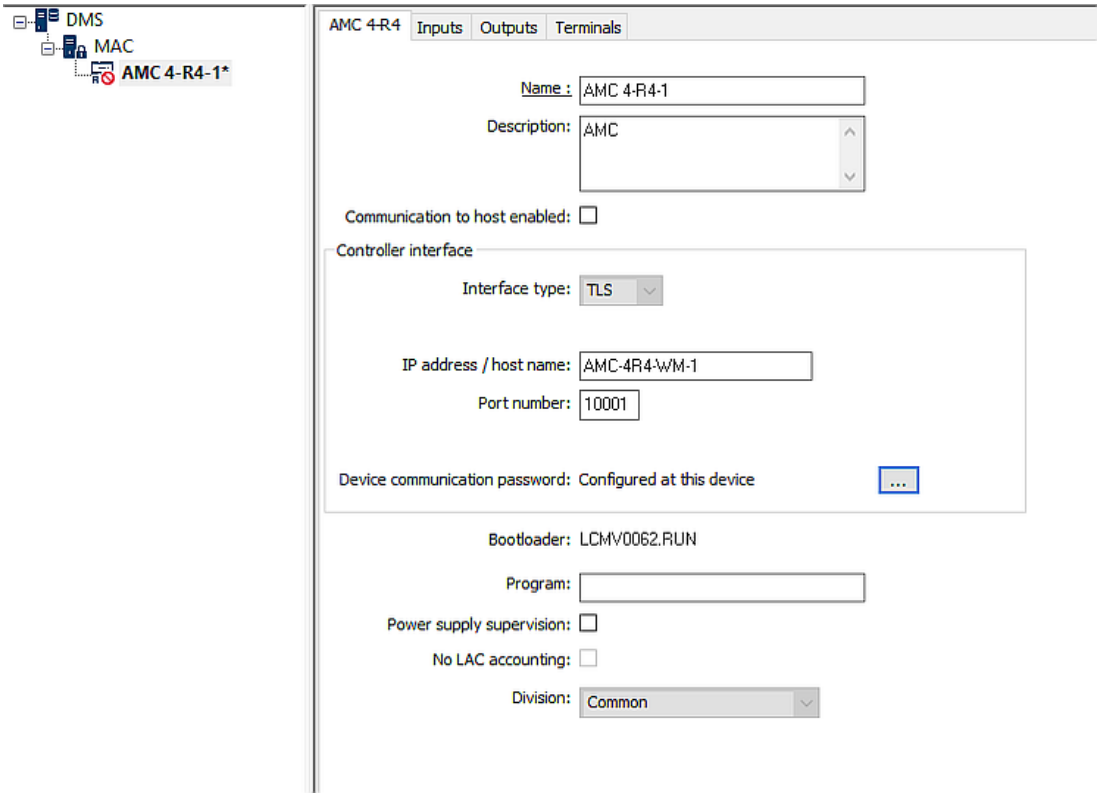
Les systèmes de contrôle d'accès sont normalement équipés d'un seul type de contrôleur et de lecteur.

Les mises à niveau logicielles et les installations croissantes peuvent rendre nécessaire de compléter les composants matériels existants par de nouveaux. Même les configurations combinant des variantes RS485 (AMC 4R4) avec des variantes Wiegand (AMC 4W) sont possibles, à condition que les mises en garde suivantes soient respectées :

- Les lecteurs RS485 transitent par un « télégramme » qui contient le numéro de code tel que lu.
- Les lecteurs Wiegand transmettent leurs données de telle manière qu'elles doivent être décodées avec l'aide de la définition du badge afin de conserver le numéro de code sous la forme correcte.
- Le fonctionnement de contrôleur mixte n'est possible que si les deux numéros de code sont construits de la même manière.

14.2.1 Paramètres et réglages AMC

Paramètres généraux de l'AMC



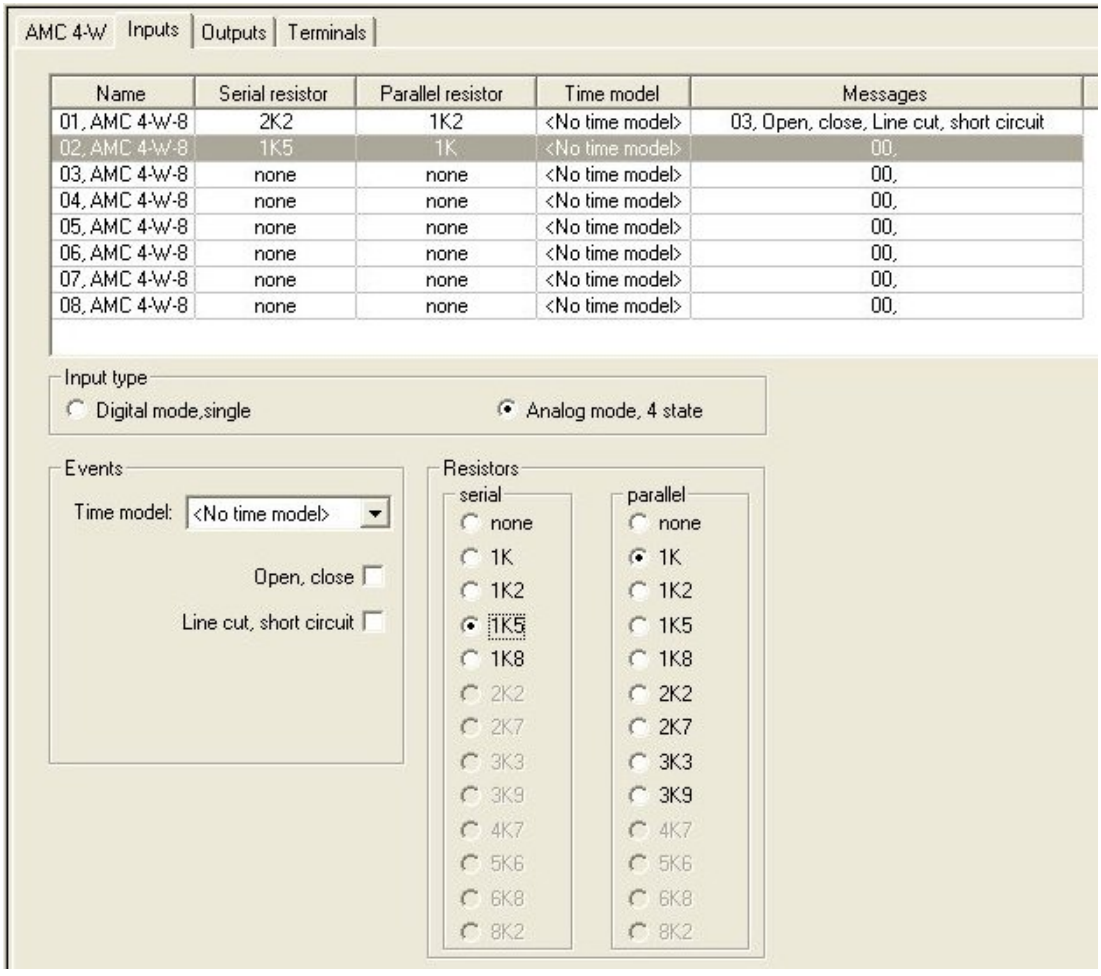
Configuration des paramètres AMC

Paramètre	Valeurs possibles	Description
Nom du contrôleur	Alphanumérique restreint : 1 à 16 chiffres	La génération d'ID (par défaut) garantit des noms uniques, mais les utilisateurs peuvent les remplacer. Si vous remplacez un nom, vous devez vous assurer que les ID sont uniques.
Description du contrôleur	alphanumérique : 0 à 255 chiffres	Texte libre.

Communication avec l'hôte permise	0 = désactivé (la case est désélectionnée) 1 = activé (la case est cochée)	Par défaut = activé Les icônes superposées sur les contrôleurs dans l'arborescence des dispositifs indiquent l'état de la connexion hôte (activé/désactivé). Le fait de désélectionner la case met temporairement l'AMS hors ligne et est utile pour la reconfiguration et les tests. La mise à jour du système de contrôle d'accès vers une nouvelle version désactive automatiquement les cases à cocher de tous les contrôleurs. Sélectionnez et désactivez les cases des AMC pour les tester individuellement dans le logiciel mis à jour.
		Cochez la case lorsque vous utilisez l'éditeur de dispositif pour définir un DCP (mot de passe de communication de dispositif) sur l'AMC lors de l'implémentation « descendante » de DTLS. Cela ouvre une fenêtre de temps de 15 minutes pour propager le DCP vers les AMC. Désélectionnez et cochez la case pour redémarrer la fenêtre de temps.
Interface du contrôleur		
Type d'interface	UDP TLS	UDP (= user datagram protocol) où la connexion se fait par réseau et pour l'instant aucun DCP n'a été défini sur l'AMC. TLS (=Transport Layer Security) : lorsque vous définissez un DCP pour l'AMC, la communication avec le MAC se fait via DTLS avec une sécurité renforcée. Pour UDP et TLS, assurez-vous que les commutateurs DIP 1 et 5 sur l'AMC sont réglés sur ON.
Adresse IP/Nom d'hôte	Nom de réseau ou Adresse IP de l'AMC	Ce champ de texte n'est actif que si **UDP** est sélectionné comme type de port. Si des adresses IP sont allouées par DHCP, le nom de réseau de l'AMC doit être fourni afin que l'AMC puisse être localisé après un redémarrage même si l'adresse IP a changé.

		Pour les réseaux sans DHCP, saisissez l'adresse IP.
Numéro de port	numérique : 10001 (par défaut)	Il s'agit du port AMC qui recevra les messages MAC.
Autres paramètres		
Programme	Alphanumérique	Nom de fichier du programme à charger dans l'AMC. Les programmes disponibles se trouvent dans le répertoire BIN du MAC et peuvent être sélectionnés dans une liste. Pour plus de commodité, le protocole et la description sont également indiqués. Ce paramètre est défini automatiquement au fur et à mesure que des programmes sont chargés automatiquement en fonction des lecteurs connectés, et le paramètre est remplacé en cas d'incohérence lecteur/ programme.
Supervision de l'alimentation	0= désactivé (la case à cocher est désactivée) 1= activé (la case est cochée)	Supervision de la tension d'alimentation. Si l'alimentation est défaillante, un message d'information est généré. La fonction de supervision suppose la présence préalable d'un système d'alimentation sans coupure (UPS), afin qu'un message puisse être généré. 0 = pas de supervision 1 = supervision activée
Aucun compte LAC	0= désactivé (la case à cocher est désactivée) 1= activé (la case est cochée)	Cochez cette case pour les dispositifs AMC qui fonctionnent conjointement pour fournir un accès aux parkings, où seul le MAC parent tient compte du nombre d'unités entrant et sortant. **Remarque** : Si cette option est sélectionnée et que l'AMC est hors ligne, ce dernier ne pourra pas empêcher l'accès aux zones surpeuplées, car il n'a pas accès au dénombrement complet de la population.
Division	Valeur par défaut « Commun »	Pertinent uniquement si la fonction **Divisions** est sous licence.

Configuration des entrées AMC



Cette boîte de dialogue comporte quatre volets :

- Liste des entrées par nom
- Types d'entrée
- Événements qui seront signalés par les entrées
- Types de résistance utilisés avec le mode analogique

Paramètres des entrées

Les paramètres des entrées AMC sont décrits dans le tableau suivant :

Nom de colonne	Description
Nom	Numérotation de l'entrée (de 01 à 08) et nom de l'AMC ou AMC-EXT approprié.
Résistance de série	Affichage de la valeur de résistance définie pour la résistance série. « none » ou « --- » = mode digital
Résistance parallèle	Affichage de la valeur de résistance définie pour la résistance parallèle. « none » ou « --- » = mode digital
Modèle horaire	Nom du modèle horaire sélectionné

Messages	Numéro de l'acte de fiducie et désignation des messages qui seront générés 00 = aucun message 01 = si événements **Ouvert**, **fermé** ont été activés 02 = si événements **Ligne coupée**, **court-circuit** ont été activés 03 = si les deux options d'événement ont été activées
Attribué	Avec le modèle d'entrée 15, le nom du signal du DIP s'affiche.

Utilisez les touches Ctrl et Maj lorsque vous cliquez pour sélectionner plusieurs entrées simultanément. Toutes les valeurs que vous modifiez s'appliqueront à toutes les entrées sélectionnées.

Événements et modèles horaires

Selon le mode de fonctionnement, les états de porte suivants sont détectés et signalés : **Ouvert**, F**ermé**, **Ligne coupée** et **Court-circuit**.

Cochez leurs cases respectives pour permettre à l'AMC de transmettre ces états en tant qu'événements à l'ensemble du système.

Sélectionnez un **Modèle horaire** dans la liste déroulante du même nom pour limiter la transmission des événements aux heures définies par le modèle. Par exemple, l'événement **Ouvert** peut n'être significatif qu'en dehors des heures normales de bureau.

Type d'entrée

Les résistances peuvent être utilisées en **Mode digital** ou **Mode analogique (4 états)**.

La valeur par défaut est **Mode digital** : seuls les états de porte **ouvert** et **fermé** sont détectés.

En mode analogique, les états de fil **Ligne coupée** et **Court**- circuit sont détectés également.

Porte ouverte	somme des valeurs de résistance série (R_S) et parallèle (R_P) : $R_S + R_P$
Porte fermée	est égal aux valeurs de résistance série : R_S
Coupure de circuit	somme des valeurs de résistance série (R_S) et parallèle (R_P) approchant de l'infini.
Court-circuit	somme des valeurs de résistance série (R_S) et parallèle (R_P) de résistance égale à zéro.

Résistances

Les résistances sont réglées sur « aucune » ou « --- » dans le **Mode digital** par défaut.

En **Mode analogique**, les valeurs des résistances série et parallèle peuvent être définies en sélectionnant les cases d'option respectives.

aucune, 1K, 1K2, 1K5, 1K8, 2K2, 2K7, 3K3, 3K9, 4K7, 5K6, 6K8, 8K2 (en 100 ohm)

En fonction de la valeur de résistance sélectionnée, seules des plages restreintes sont disponibles pour la résistance correspondante.

Les tableaux suivants montrent dans les colonnes de gauche les valeurs sélectionnées et dans les colonnes de droite les plages disponibles de l'autre résistance.

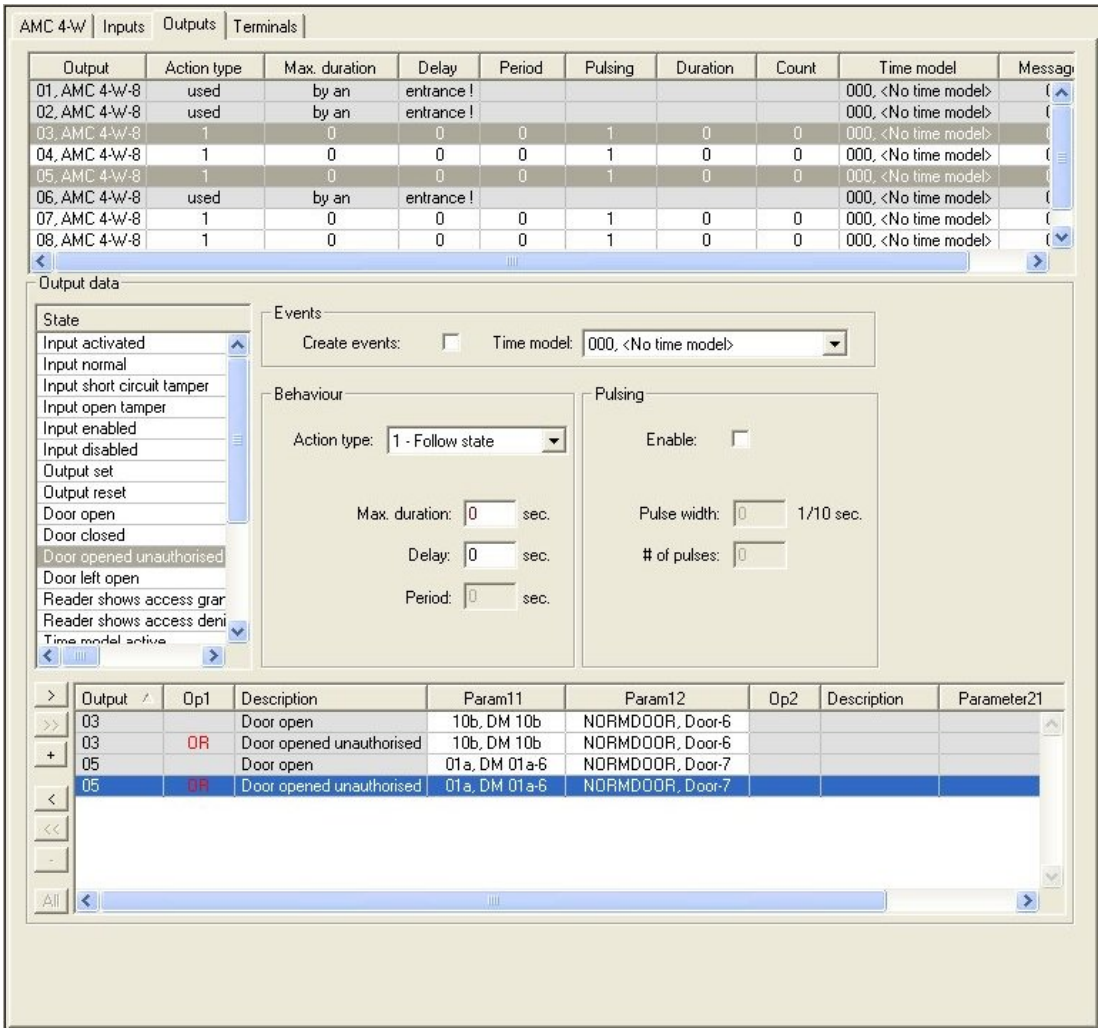
Série	**Plage**		**Parallèle**	**Plage**
« aucune » ou « --- »	1K à 8K2		« aucune » ou « --- »	1K à 8K2
1K	1K à 2K2		1K	1K à 1K8
1K2	1K à 2K7		1K2	1K à 2K7

1K5	1K à 3K9		1K5	1K à 3K3
1K8	1K à 6K8		1K8	1K à 3K9
2K2	1K2 à 8K2		2K2	1K à 4K7
2K7	1K2 à 8K2		2K7	1K2 à 5K6
3K3	1K5 à 8K2		3K3	1K5 à 6K8
3K9	1K8 à 8K2		3K9	1K5 à 8K2
4K7	2K2 à 8K2		4K7	1K8 à 8K2
5K6	2K7 à 8K2		5K6	1K8 à 8K2
6K8	3K3 à 8K2		6K8	1K8 à 8K2
8K2	3K9 à 8K2		8K2	2K2 à 8K2

Configuration des sorties AMC - Présentation

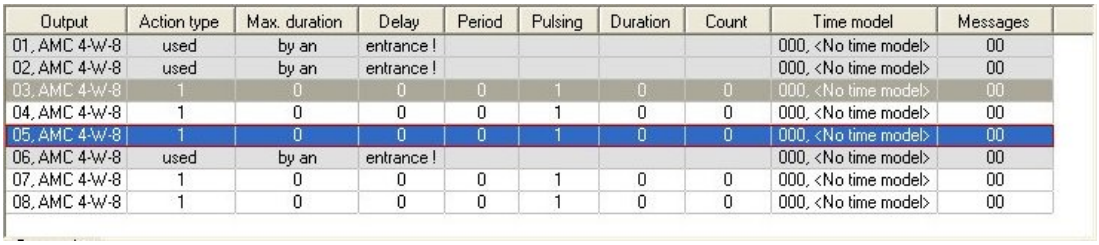
Cette page fournit la configuration de chaque sortie sur un AMC ou AMC-EXT, et contient trois zones principales :

- zone de liste avec un aperçu du paramètre défini pour chaque sortie
- options de configuration dans les sorties sélectionnées dans la liste
- définition des conditions d'activation des sorties



Sélection des sorties AMC dans le tableau

Pour configurer des contacts de sortie, sélectionnez d'abord la ligne correspondante dans le tableau supérieur. Utilisez les touches Ctrl et Maj pour sélectionner plusieurs lignes, si nécessaire. Les modifications apportées dans la partie inférieure de la fenêtre n'affecteront que les sorties que vous sélectionnez.



Output	Action type	Max. duration	Delay	Period	Pulsing	Duration	Count	Time model	Messages
01, AMC 4-W-8	used	by an	entrance !					000, <No time model>	00
02, AMC 4-W-8	used	by an	entrance !					000, <No time model>	00
03, AMC 4-W-8	1	0	0	0	1	0	0	000, <No time model>	00
04, AMC 4-W-8	1	0	0	0	1	0	0	000, <No time model>	00
05, AMC 4-W-8	1	0	0	0	1	0	0	000, <No time model>	00
06, AMC 4-W-8	used	by an	entrance !					000, <No time model>	00
07, AMC 4-W-8	1	0	0	0	1	0	0	000, <No time model>	00
08, AMC 4-W-8	1	0	0	0	1	0	0	000, <No time model>	00

Les lignes dont les sorties sont déjà affectées via un modèle de porte, ou ailleurs, sont affichées en gris clair avec les informations « **utilisé par une entrée!** ». Ces sorties ne peuvent plus être configurées.

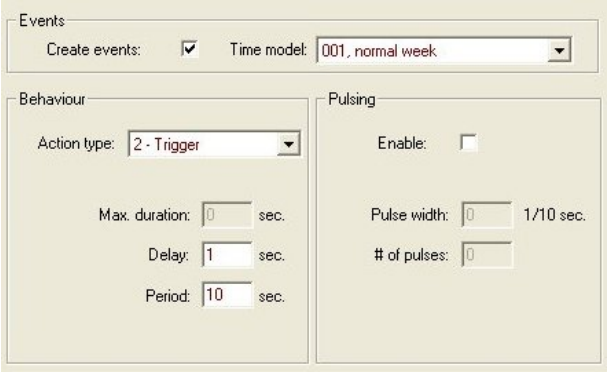
Les lignes que vous avez sélectionnées sont en gris foncé.

Paramètres des sorties AMC

Nom de colonne	Description
Sortie	numérotation actuelle des sorties sur les AMC ou AMC-EXT respectifs 01 à 08 avec AMC et AMC_IO08 01 à 16 avec AMC_IO16
Type d'action	indication du type d'action sélectionné 1 = Suivre l'état 2 = Déclencher 3 = Alternatif
Durée max.	durée en secondes du signal [1 - 9999 ; 0 = toujours, si le message réciproque n'apparaît pas] - uniquement avec le type d'action « 1 »
Retard	délai en secondes jusqu'à ce que le signal soit donné [0 - 9999] - uniquement avec les types d'action « 1 » et « 2 »
Période	période en secondes pendant laquelle le signal est donné - uniquement avec le type d'action « 2 »
Impulsion	activation de l'impulsion - sinon le signal est donné en permanence
Durée	longueur d'impulsion
Compteur	nombre d'impulsions par seconde
Modèle horaire	nom du modèle horaire sélectionné
Messages	marquage de l'activité de message 00 = aucun message 03 = les événements sont signalés
Attribué	Avec le modèle d'entrée 15, le nom du signal du DOP s'affiche.

Sorties : événements, action, impulsions

Toutes les entrées de la liste ci-dessus sont générées en utilisant les cases à cocher et les champs de saisie dans les zones de dialogue **Événements**, **Action** et **Pulsations**. La sélection d'une entrée de liste indique les paramètres respectifs dans ces zones. Cela vaut également pour le choix multiple d'entrées de liste, à condition que les paramètres de toutes les sorties sélectionnées soient égaux. Les modifications apportées aux réglages des paramètres sont adoptées pour toutes les entrées sélectionnées dans la liste.



Cochez la case **Créer des événements** si un message doit être envoyé pour la sortie activée. Si ces messages doivent être envoyés uniquement pendant des périodes spéciales, par exemple la nuit ou le week-end, attribuez un **modèle horaire**.

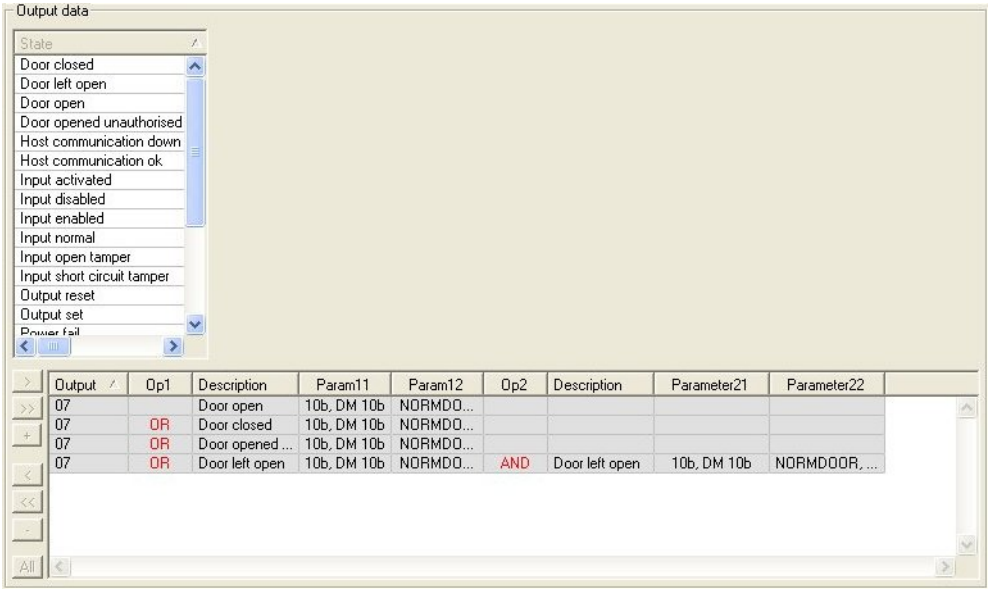
Les paramètres suivants peuvent être définis pour les types d'action individuels :

Type d'action	**Durée max.**	**Retard**	**Période**	**Pulsation/ Activer**	**Largeur d'impulsion**	**Nombre d'impulsions**
Suivre l'état	0 = toujours 1 - 9999	0 - 9999	non	oui	1 - 9999	Aucun
Déclenchement	non	0 - 9999	0 - 9999 si la pulsation n'est **pas** activée	oui désactive la période	1 - 9999	1 - 9999
Alternatif	non	non	non	oui	1 - 9999	non

Données de sortie AMC

La partie inférieure de la boîte de dialogue **Sorties** contient :

– Une zone de liste avec les **états** disponible pour les sorties sélectionnées.
– Un tableau avec les sorties et les états configurés pour les déclencher ces sorties.



Configuration des sorties à déclencher par certains états

Vous pouvez configurer les sorties que vous avez sélectionnées ci-dessus pour qu'elles soient déclenchées par des états individuels ou des combinaisons logiques d'états.

– Sélectionnez une ou plusieurs sorties dans la zone de liste supérieure.
– Sélectionnez un état dans la liste **État**.
– Si plusieurs dispositifs ou installations sont à un état sélectionné qui peuvent transmettre cet état, le bouton » est activé en regard du bouton ›.
  Cliquez sur › (ou double-cliquez sur l'état) pour créer pour chaque sortie sélectionnée une entrée de son état avec le premier dispositif (par exemple, AMC, première entrée) et l'installation (par exemple, premier signal, première porte).

Exit	Operand1	Description	Param11	Param12
04		Output set	00, AMC, AMC 4-W-2	Out, 01, AMC 4-W-2

En cliquant sur », l'état sélectionné est transféré dans la liste et créé avec un raccourci OU-opérateur logique pour chaque dispositif installé (par exemple, toutes les entrées AMC).

Exit	Operand1	Description	Param11	Param12
04		Output set	00, AMC, AMC 4-W-2	Out, 01, AMC 4-W-2
04	OR	Output set	00, AMC, AMC 4-W-2	Out, 02, AMC 4-W-2
04	OR	Output set	00, AMC, AMC 4-W-2	Out, 03, AMC 4-W-2
04	OR	Output set	00, AMC, AMC 4-W-2	Out, 04, AMC 4-W-2
04	OR	Output set	00, AMC, AMC 4-W-2	Out, 05, AMC 4-W-2
04	OR	Output set	00, AMC, AMC 4-W-2	Out, 06, AMC 4-W-2
04	OR	Output set	00, AMC, AMC 4-W-2	Out, 07, AMC 4-W-2
04	OR	Output set	00, AMC, AMC 4-W-2	Out, 08, AMC 4-W-2

– Plusieurs états peuvent être attribués sur un seul raccourci OU.

Exit	Operand1	Description	Param11	Param12
04		Output set	00, AMC, AMC 4-W-2	Out, 01, AMC 4-W-2
04	OR	Input normal	00, AMC, AMC 4-W-2	In, 01, AMC 4-W-2
04	OR	Door open	06a, Timemgm	<< !!! >>

Des raccourcis avec ET sont également possibles :

– Un état doit déjà être attribué auquel une autre condition est ajoutée en la sélectionnant dans une colonne arbitraire.
– Ensuite, un autre statut est sélectionné et connecté à l'état marqué en cliquant sur .

Exit	Operand1	Description	Param11	Param12	Operand2	Description	Parameter21	Parameter22
04		Output set	00, AMC, AMC 4-W-2	Out, 01, AMC 4-W-2				
04	OR	Input normal	00, AMC, AMC 4-W-2	In, 01, AMC 4-W-2				
04	OR	Door open	06a, Timemgm	<< !!! >>	AND	Door opened unauthorised	06a, Timemgm	<< !!! >>

Remarque!
Jusqu'à 128 OU-conditions peuvent être attribuées à chaque sortie.
Chaque condition peut comporter avoir **une** ET-condition.

Une fois qu'un état est attribué à un dispositif ou à une installation, il peut également être attribué à tous les autres dispositifs et installations existants.

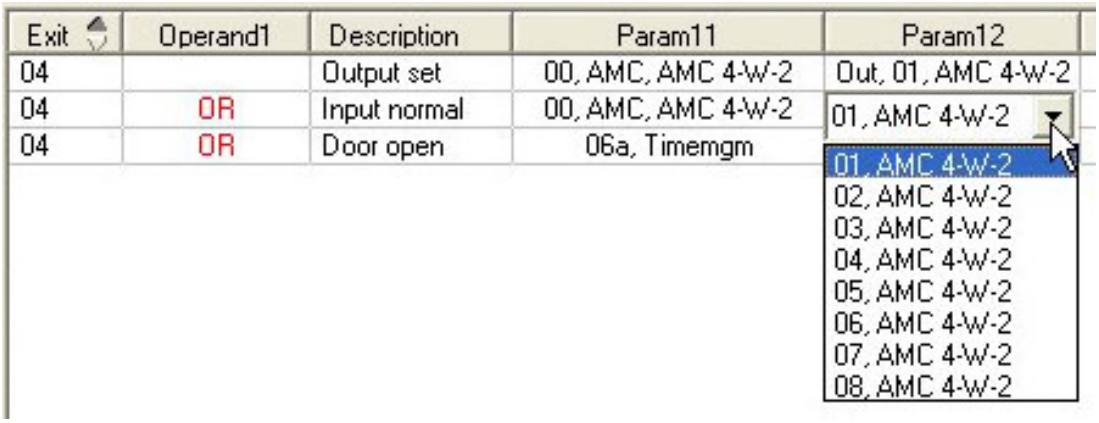
– Sélectionnez l'entrée affectée dans une colonne arbitraire.
– Cet état est créé pour tous les dispositifs et installations existants en cliquant sur All.

Modification des paramètres de sorties

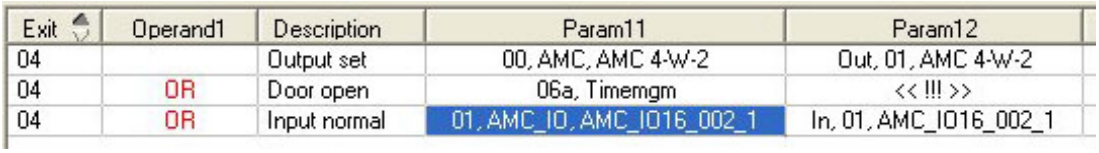
Vous pouvez modifier les lignes de la liste
Avec plusieurs dispositif ou installations auxquels l'état attribué pourrait correspondre, les premiers dispositif et installations de ce type sont toujours définis.
Dans les colonnes **Param11** et **Param21** (avec les raccourcis ET), les dispositifs (par exemple, AMC, entrée) sont affichés. Les colonnes **Param12** et **Param22** contiennent des installations spéciales (par exemple, signal d'entrée, porte, lecteur).
Si plusieurs dispositif (par exemple, cartes d'E/S) ou installations (par exemple, signaux supplémentaires, lecteurs) existent, le pointeur de la souris change en pointant sur cette colonne.

Exit	Operand1	Description	Param11	Param12
04		Output set	00, AMC, AMC 4-W-2	Out, 01, AMC 4-W-2
04	OR	Input normal	00, AMC, AMC 4-W-2	In, 01, AMC 4-W-2
04	OR	Door open	06a, Timemgm	<< !!! >>

Un double-clic sur l'entrée de colonne ajoute un bouton et fait apparaître une liste déroulante d'entrées valides pour le paramètre.



La modification des entrées dans les colonnes **Param11** et **Param21** met à jour les entrées dans les colonnes **Param12** et **Param22** :



Remarque!
Ceci n'est possible que pour les colonnes **Param11**, **Param12**, **Param21** et **Param22**.
S'il n'y a pas d'autres options (par exemple, parce qu'une seule entrée a été configurée), le pointeur de la souris ne change pas et tous les champs sont gris. Si vous double-cliquez sur cette entrée, cela est interprété comme une commande de suppression et la boîte de message de vérification de suppression s'affiche.

Suppression des états qui déclenchent des sorties
Les attributions sélectionnées peuvent être supprimées en cliquant sur '**<**'(ou en double-cliquant sur l'entrée de la liste). Une boîte de message demandera la confirmation de la suppression.

Si plusieurs états sont associés à une sortie, ils peuvent tous être supprimés ensemble comme suit :
- Sélectionnez la première entrée de la liste (celle qui n'a pas d'entrée dans la colonne **Op1**), puis cliquez sur le bouton '**<<**'.
- Vous pouvez également double-cliquer sur la première entrée.
  - Une fenêtre contextuelle s'affiche. Confirmez ou abandonnez la suppression.
  - Si vous confirmez la suppression, une deuxième fenêtre contextuelle s'affiche pour vous demander si vous souhaitez supprimer toutes les entrées associées (répondre **Oui**), ou uniquement l'entrée sélectionnée (répondre **Non**).

Pour supprimer des états supplémentaires qui qualifient le premier état par un opérateur ET dans la colonne **Op2**, cliquez n'importe où sur la ligne, puis cliquez sur le bouton 'moins' , lequel n'est actif que si un état ET de qualification est présent sur cette ligne.

Description de l'état
Le tableau suivant donne un aperçu de tous les états pouvant être sélectionnés, leur numéro de type et leur description.
Le champ de liste **État** contient également ces paramètres - ils sont indiqués en faisant défiler la liste vers la droite.

État	Type	Description
Saisie activée	1	Saisie locale
Saisie normale	2	Saisie locale
Sabotage de court-circuit de saisie	3	Saisie locale avec résistance configurée
Sabotage d'ouverture de saisie	4	Saisie locale avec résistance configurée
Saisie désactivée	5	Saisie locale désactivée par le modèle horaire
Saisie activée	6	Saisie locale activée par le modèle horaire
Sortie définie	7	Sortie locale, sortie non active
Sortie réinitialisée	8	Saisie locale, saisie non active
Porte ouverte	9	GID de l'entrée, numéro de porte
Porte fermée	10	GID de l'entrée, numéro de porte
Porte ouverte non autorisée	11	GID de l'entrée, numéro de porte, remplace « Porte ouverte » (9)
Porte laissée ouverte	12	GID de l'entrée, numéro de porte
Le lecteur indique accès accordé	13	Adresse du lecteur
Le lecteur indique accès refusé	14	Adresse du lecteur
Modèle horaire activé	15	Modèle horaire configuré
Falsifier lecteur	16	Adresse du lecteur
Falsifier AMC	17	---
Falsifier carte I/O	18	---
Panne d'alimentation	19	uniquement pour batterie AMC
Alimentation correcte	20	uniquement pour batterie AMC
Communication hôte OK	21	---
Communication hôte défaillante	22	---
Message du lecteur	23	Adresse du lecteur
Message du LAC	24	Numéro de carte
Contrôle de carte	25	Adresse du lecteur, fonction de contrôle de carte.

Configuration des sorties

Outre l'affectation des signaux avec des modèles de porte ou avec une affectation individuelle, des conditions peuvent être définies pour les sorties qui ne sont pas encore affectées. Si ces conditions sont vérifiées, la sortie est activée en fonction du paramètre défini.

Vous devez décider de ce qui sera commuté sur la sortie. Contrairement aux signaux qui peuvent être associés à un modèle de porte spécifique, à ses portes et à ses lecteurs, dans ce cas, les signaux de tous les dispositifs et installations connectés à un AMC peuvent être appliqués.
Si, par exemple, un signal optique, acoustique ou un message à un dispositifs externe doit être déclenché par les signaux d'entrée **Sabotage de court-circuit de saisie** et **Porte ouverte non autorisée**, la ou les entrées qui peuvent être pris en compte sont affectées à la sortie de destination correspondante.
Exemple dans lequel un seul contact a été sélectionné dans chaque cas :

Exit	Operand1	Description	Param11	Param12
04		Input short cir...	00, AMC, AMC 4-W-2	In, 01, AMC 4-W-2
04	OR	Door opened ...	06a, Timemgm	<< !!! >>

Exemple avec tous les contacts :

Exit	Operand1	Description	Param11	Param12
04		Input short circuit tamper	00, AMC, AMC 4-W-2	In, 01, AMC 4-W-2
04	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 02, AMC 4-W-2
04	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 03, AMC 4-W-2
04	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 04, AMC 4-W-2
04	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 05, AMC 4-W-2
04	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 06, AMC 4-W-2
04	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 07, AMC 4-W-2
04	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 08, AMC 4-W-2
04	OR	Door opened unauthorised	06a, Timemgm	---
04	OR	Door opened unauthorised	03a, Entrance B:B	REVDOOR, Revolving Door

Exemple avec des contacts sélectionnés :
Une seule entrée est créée pour chaque contact en cliquant sur » ou en supprimant les contacts non requis après avoir attribué tous les contacts :

Exit	Operand1	Description	Param11	Param12
04		Input short circuit tamper	00, AMC, AMC 4-W-2	In, 01, AMC 4-W-2
04	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 03, AMC 4-W-2
04	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 05, AMC 4-W-2
04	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 06, AMC 4-W-2
04	OR	Door opened unauthorised	06a, Timemgm	---
04	OR	Door opened unauthorised	03a, Entrance B:B	REVDOOR, Revolving Door

Les mêmes conditions peuvent être installées sur plusieurs sorties si, par exemple, en plus d'un signal optique vous avez également besoin d'un signal acoustique, un message doit être envoyé au dispositif externe en même temps :

Exit	Operand1	Description	Param11	Param12
04		Input short circuit tamper	00, AMC, AMC 4-W-2	In, 01, AMC 4-W-2
04	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 02, AMC 4-W-2
04	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 03, AMC 4-W-2
04	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 04, AMC 4-W-2
04	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 05, AMC 4-W-2
04	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 06, AMC 4-W-2
04	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 07, AMC 4-W-2
04	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 08, AMC 4-W-2
04	OR	Door opened unauthorised	06a, Timemgm	<< !!! >>
04	OR	Door opened unauthorised	03a, Entrance B:B	REVDOOR, Revolving Door
06		Input short circuit tamper	00, AMC, AMC 4-W-2	In, 01, AMC 4-W-2
06	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 02, AMC 4-W-2
06	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 03, AMC 4-W-2
06	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 04, AMC 4-W-2
06	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 05, AMC 4-W-2
06	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 06, AMC 4-W-2
06	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 07, AMC 4-W-2
06	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 08, AMC 4-W-2
06	OR	Door opened unauthorised	06a, Timemgm	<< !!! >>
07		Input short circuit tamper	00, AMC, AMC 4-W-2	In, 01, AMC 4-W-2
07	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 02, AMC 4-W-2
07	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 03, AMC 4-W-2
07	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 04, AMC 4-W-2
07	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 05, AMC 4-W-2
07	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 06, AMC 4-W-2
07	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 07, AMC 4-W-2

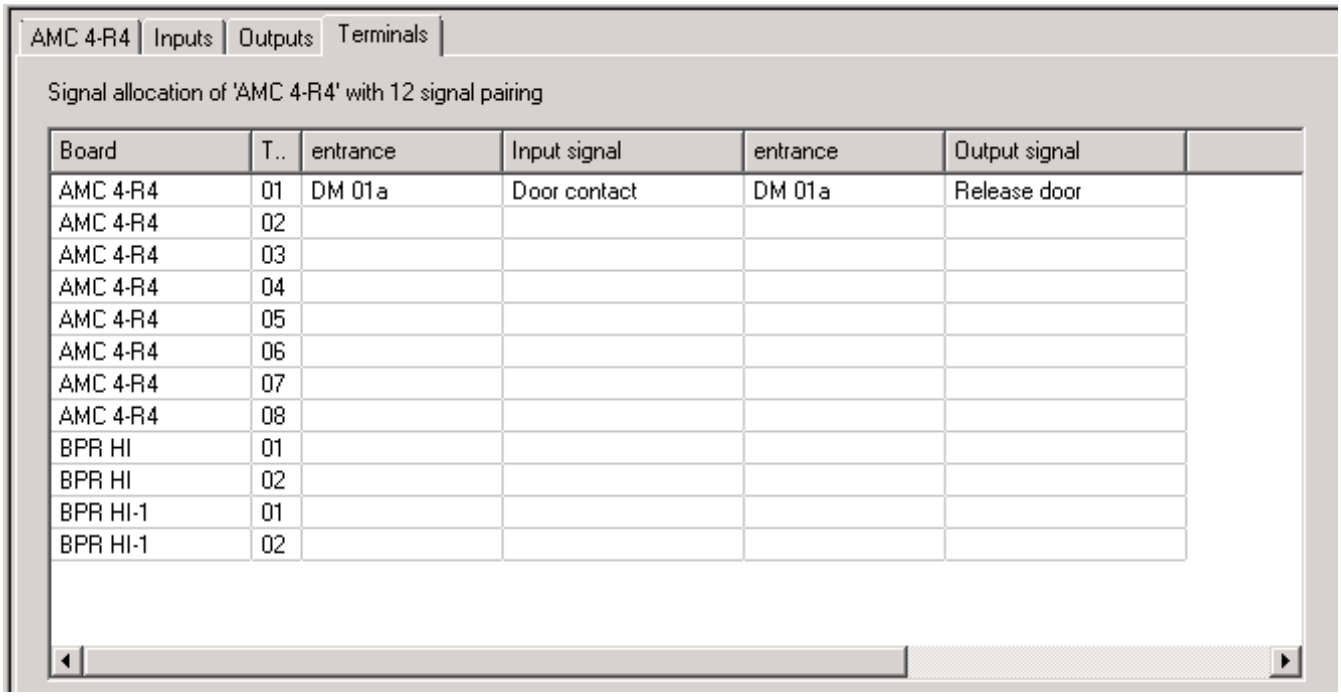
Liste de tous les états existants avec les valeurs par défaut pour les paramètres 11/21 et 12/22 :

Description	Param11	Param12
Input activated	00, AMC, AMC 4-W-2	In, 01, AMC 4-W-2
Input normal	00, AMC, AMC 4-W-2	In, 01, AMC 4-W-2
Input short circuit tamper	00, AMC, AMC 4-W-2	In, 01, AMC 4-W-2
Input open tamper	00, AMC, AMC 4-W-2	In, 01, AMC 4-W-2
Input enabled	00, AMC, AMC 4-W-2	In, 01, AMC 4-W-2
Input disabled	00, AMC, AMC 4-W-2	In, 01, AMC 4-W-2
Output set	00, AMC, AMC 4-W-2	Out, 01, AMC 4-W-2
Output reset	00, AMC, AMC 4-W-2	Out, 01, AMC 4-W-2
Door open	06a, Timemgm	<< !!! >>
Door closed	06a, Timemgm	<< !!! >>
Door opened unauthorised	06a, Timemgm	<< !!! >>
Door left open	06a, Timemgm	<< !!! >>
Reader shows access granted	---	TM-Reader IN
Reader shows access denied	---	TM-Reader IN
Time model active	---	000, <No time model>
Tamper reader	---	TM-Reader IN
Tamper AMC	---	---
Tamper I/O board	---	00, AMC, AMC 4-W-2
Power fail	---	---
Power good	---	---
Host communication ok	---	---
Host communication down	---	---

Définition de signaux dans l'onglet Terminaux

L'onglet **Terminaux** répertorie l'allocation des contacts sur un AMC ou AMC-EXT. Une fois les entrées créées, les affectations de signaux sont indiquées en fonction du modèle de porte sélectionné.

Vous ne pouvez pas apporter de modifications sous l'onglet **Terminaux** du contrôleur ou des cartes d'extension. Les modifications ne sont possibles que sur l'onglet Terminaux de la page d'entrée. Pour cette raison, les paramètres de terminaux sont affichés sur un fond gris. Les entrées affichées en rouge indiquent les configurations de signaux des sorties respectives.



Board	T..	entrance	Input signal	entrance	Output signal
AMC 4-R4	01	DM 01a	Door contact	DM 01a	Release door
AMC 4-R4	02				
AMC 4-R4	03				
AMC 4-R4	04				
AMC 4-R4	05				
AMC 4-R4	06				
AMC 4-R4	07				
AMC 4-R4	08				
BPR HI	01				
BPR HI	02				
BPR HI-1	01				
BPR HI-1	02				

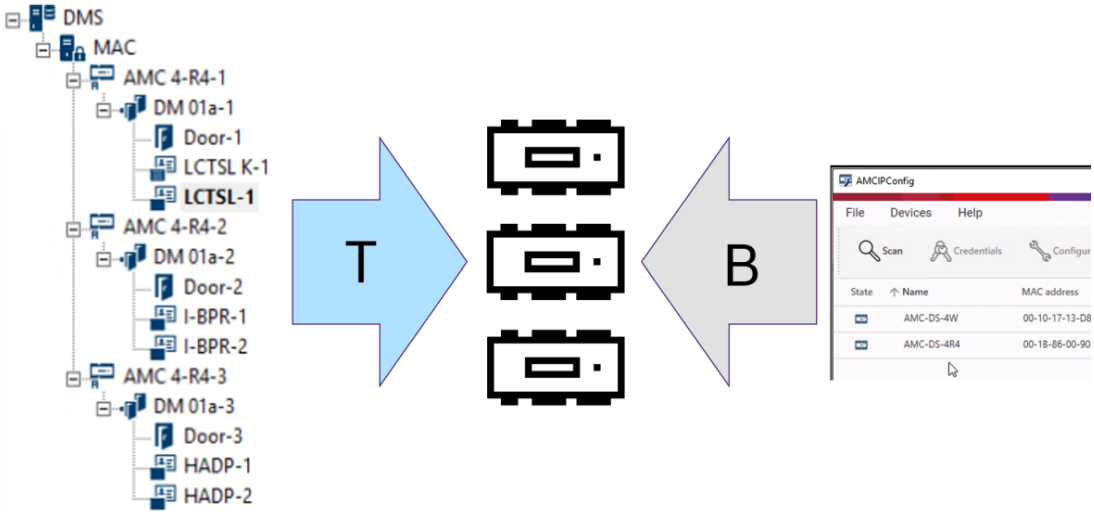
15 Configuration de DTLS pour une communication sécurisée

Introduction

Le système de contrôle d'accès (ACS) permet une communication entre les dispositifs hautement sécurisée, protégée par DTLS. Il est possible de déployer la communication DTLS entre les dispositifs de deux manières principales dans ACS :

Le **Déploiement descendant** (T) s'effectue depuis l'éditeur de dispositif dans ACS.

Le **Déploiement ascendant** (B) s'effectue principalement dans l'outil AMCIPConfig, mais il nécessite l'éditeur de dispositif pour l'achèvement.



- (T) Le déploiement descendant peut être effectué de deux manières dans l'éditeur de dispositif :
  - En utilisant un seul mot de passe de communication de dispositif (DCP) au niveau de DMS pour tous les AMC,
  - En utilisant plusieurs DCP pour différentes branches de l'arborescence du dispositif, en commençant par leurs MAC ou AMC respectifs.
- (B) Le déploiement ascendant peut également être lancé de deux manières dans l'outil AMCIPConfig :
  - En utilisant une clé matérielle AMC
  - En utilisant une touche LCD aléatoire

Remarque!

Le déploiement ascendant nécessite toujours le paramétrage des DCP dans l'éditeur de dispositif.

Le déploiement ascendant vous permet de définir un DCP sur le périphérique AMC. Vous devez néanmoins définir le même DCP sur le même AMC dans l'éditeur de dispositif également, afin de permettre une communication DTLS complète entre le MAC et l'AMC.

Résumé des options de déploiement DTLS

	Brève description	Avantages	Inconvénients
Déploiement descendant	L'administrateur système entre un mot de passe fort dans l'**éditeur de dispositif**. A l'aide de ce mot de passe, le système génère une **clé principale** qu'il propage de manière descendante dans l'arborescence de dispositifs de contrôle d'accès, des DMS via les MAC aux contrôleurs de porte AMC. Vous pouvez définir un mot de passe pour l'intégralité de l'arborescence de dispositifs ou des mots de passe différents pour les différentes branches de l'arborescence de dispositifs.	Déploiement simple et rapide.	Pendant la propagation de la clé principale vers les contrôleurs de porte AMC, la communication de dispositif n'est pas protégée par DTLS.
Déploiement ascendant à l'aide d'une clé matérielle AMC	L'administrateur système utilise l'outil **AMC IPConfig** pour déployer DTLS au niveau des contrôleurs de porte AMC.	Différenciation supérieure et flexibilité de déploiement. Cette méthode permet de surmonter le principal inconvénient du déploiement descendant, à savoir une communication sporadique non protégée de la clé principale. Néanmoins, cela implique que la connexion de l'outil AMCIPConfig à l'AMC soit sécurisée lors de la configuration du DCP.	Durant la période où l'outil IPConfig définit le DCP sur l'AMC, vous devez garantir une communication sécurisée par d'autres moyens. Par exemple, connectez l'AMC directement à l'ordinateur sur lequel IPConfig s'exécute. Les DCP que vous définissez dans l'outil IPConfig doivent également être définis sur les mêmes AMC via l'éditeur de dispositif.
Déploiement ascendant à l'aide d'une		Différenciation supérieure et flexibilité de déploiement.	Déploiement plus compliqué et plus long.

	Brève description	Avantages	Inconvénients
touche LCD aléatoire		Sécurité maximale, car la clé LCD n'est pas du tout transmise via le réseau ; par conséquent, la propagation des informations d'identification est protégée à tout moment.	Vous devez transférer la clé LCD aléatoire à 27 symboles via des méthodes non réseau vers l'outil IP Config.
Les détails et les instructions se trouvent dans les sections suivantes de ce chapitre.			

Terminologie DTLS

DCP (Mot de passe de communication de dispositif)	Mot de passe fort et unique à partir duquel l'ACS génère une clé principale interne. Ce mot de passe doit être sécurisé car il n'est pas stocké dans l'ACS.
Clé principale	Code que le système génère à partir du DCP et qu'il utilise pour protéger les dispositifs de contrôle d'accès. La clé principale n'est jamais rendue visible à aucun utilisateur.
Touche LCD aléatoire	Code alphanumérique temporaire que l'AMC génère à nouveau à chaque démarrage. La clé peut être affichée sur l'écran à cristaux liquides (LCD) de l'AMC et peut être demandée par des outils logiciels pour authentifier la communication réseau.
Clé matérielle AMC .	Code d'authentification interne que l'AMC génère à partir de certains paramètres matériels. Elle n'est pas visible pour l'utilisateur.

15.1 Déploiement DTLS descendant

Conditions préalables

- AMS 4.0 ou BIS-ACE 4.9.1 ou version ultérieure.
- L'arborescence des dispositifs de contrôle d'accès du DMS aux AMC est physiquement configurée et connectée au réseau, mais les AMC ne sont pas activés. Activé signifie que les cases **Communication to host enabled (Communication avec l'hôte activée)** des AMC sont sélectionnées.
- DTLS n'a pas déjà été configuré sur les AMC par l'une des méthodes ascendantes, via l'outil IPConfig.

Procédure : Un DCP pour tous

1. Dans l'ACS, démarrez l'éditeur de dispositif
- Menu principal d'AMS > **Configuration** > **Device data (Données du dispositif)** > **Device tree (Arborescence du dispositif)** 

– Une fenêtre de dialogue s'affiche, pour vous inviter à saisir un mot de passe de communication de dispositif fort (DCP).
2. Pour définir un seul DCP pour tous les AMC de l'arborescence du dispositif, saisissez et confirmez un mot de passe fort conformément à vos stratégies de mot de passe locales.
– La boîte de dialogue comporte des informations relatives à la puissance du mot de passe, basée sur l' entropie de mot de passe.
3. Notez soigneusement le mot de passe, car il n'est pas stocké dans l'ACS.
4. Cliquez sur **OK** pour fermer la boîte de dialogue.

Autre procédure : plusieurs DCP pour différentes branches de l'arborescence des dispositifs

1. Dans l'ACS, démarrez l'éditeur de dispositif
– Menu principal d'AMS > **Configuration** > **Device data (Données du dispositif)** > **Device tree (Arborescence du dispositif)** 
– Une fenêtre de dialogue s'affiche, pour vous inviter à saisir un mot de passe de communication de dispositif fort (DCP).
2. Cliquez sur **Cancel (Annuler)** afin de définir différents DCP sur différentes branches de l'arborescence des dispositifs (MAC et AMC).
– Une boîte de dialogue contextuelle indique le nombre d'AMC du système qui n'ont toujours pas de DCP.
– L'arborescence des dispositifs s'ouvre dans l'éditeur de dispositif.
3. Développez l'arborescence des dispositifs afin de sélectionner le MAC ou l'AMC pour lequel vous souhaitez définir un DCP.
– Si vous définissez le DCP au niveau d'un MAC, il est défini pour tous les AMC subordonnés du MAC.
– Si vous définissez le DCP au niveau d'un AMC, il est défini uniquement pour cet AMC.
4. Cliquez sur le bouton de points de suspension ... en regard du champ de texte **Device communication password (Mot de passe de communication du dispositif) :**
5. Saisissez et confirmez un mot de passe fort conformément à vos stratégies de mot de passe locales.
6. Notez soigneusement le mot de passe et la branche à laquelle il s'applique, car il n'est pas stocké dans l'ACS.
7. Répétez cette procédure pour chaque MAC ou AMC pour lequel vous souhaitez définir un DCP distinct.
8. Cliquez sur **OK** pour fermer la boîte de dialogue.

Résultat du déploiement descendant

L'ACS utilise le DCP ou les DCP pour générer des clés internes pour tous les AMC en dessous du DMS ou du MAC sélectionné.
Il n'est pas nécessaire de répéter cette procédure sauf si vous modifiez par la suite le DCP sur un ou plusieurs AMC à l'aide de l'outil AMC IPConfig (voir le déploiement « ascendant »). Dans ce cas, vous devez immédiatement définir le même DCP descendant bas sur les mêmes AMC dans l'éditeur de dispositif.
Si vous ajoutez ultérieurement des dispositifs dans l'arborescence des dispositifs subordonnés aux DMS et MAC qui ont déjà des DCP, les nouveaux dispositifs hériteront automatiquement du même DCP de leurs dispositifs supérieurs.

16 Configuration des entrées

16.1 Entrées - introduction

Le terme Entrée désigne dans son intégralité le mécanisme de contrôle d'accès à un point d'entrée :
Les éléments de l'entrée comprennent :

- Lecteurs d'accès - entre 1 et 4
- Un type de barrière, par exemple une porte, un tourniquet, un sas de sécurité ou une barrière mobile.
- La procédure d'accès telle que définie par des séquences prédéfinies de signaux électroniques passés entre les éléments matériels.

Un Modèle de porte est un modèle pour un type d'entrée particulier. Il décrit les éléments de porte présents (nombre et type de lecteurs, type de porte ou barrière, etc.), et met en œuvre un processus de contrôle d'accès spécifique avec des séquences de signaux prédéfinis.
Les modèles de portes facilitent grandement la configuration d'un système de contrôle d'accès.

Modèle de porte 1	Porte simple ou commune
Modèle de porte 3	tourniquet réversible pour entrée et sortie
Modèle de porte 5	entrée ou sortie du parking
Modèle de porte 6	Lecteurs entrants/sortants pour heure et présence
Modèle de porte 7	contrôle des ascenseurs
Modèle de porte 9	barrières d'entrée de véhicules et portail roulant
Modèle de porte 10	porte simple avec armement/désarmement IDS
Modèle de porte 14	porte simple avec armement/désarmement IDS et droits d'accès spéciaux
Modèle de porte 15	signaux d'entrée et de sortie indépendants

- Les modèles de porte 1, 3, 5, 9 et 10 incluent une option pour des lecteurs de cartes supplémentaires sur le côté entrant ou sortant.
- Un contrôleur d'accès local utilisé dans le modèle de porte 05 (parking) ou 07 (ascenseur) ne peut pas être partagé avec un autre modèle de porte.
- Lorsqu'une entrée est configurée avec un modèle de porte et enregistrée, le modèle de porte ne peut plus être remplacé par un autre. Si un modèle de porte différent est requis, l'entrée doit être supprimée et reconfigurée à partir de zéro.

Certains modèles de portes ont des variantes (a, b, c, r) avec les caractéristiques suivantes :

a	lecteurs entrant **et** sortant
b	lecteur entrant et bouton poussoir sortant
c	lecteur entrant **OU** sortant (et non les deux - ce qui serait la variante **a**)
r	(Modèle de porte 1 seulement). Un lecteur dont le seul objectif est d'enregistrer les personnes à un point de rassemblement, par exemple dans le cas d'une évacuation. Aucune barrière physique n'est impliquée dans ce modèle de porte.

Le bouton **OK** pour terminer la configuration ne devient actif que lorsque toutes les valeurs obligatoires ont été saisies. Par exemple, les modèles de porte de la variante (a) nécessitent des lecteurs entrants **et** sortants. Les entrées ne peuvent être enregistrées que lorsque le type est sélectionné pour les deux lecteurs.

16.2 Création d'entrées

La liste des lecteurs présentés pour la sélection sera adaptée au type de contrôleur que vous avez sélectionné.

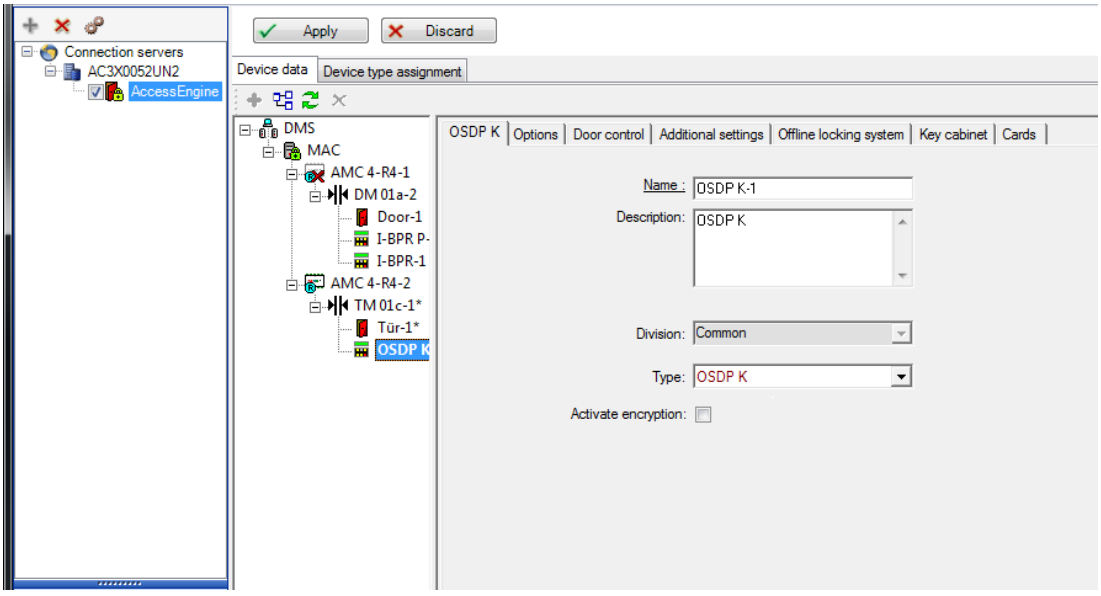
– Pour les types **AMC 4W** seulement, les lecteurs Wiegand sont disponibles, avec et sans clavier.
– Pour les lecteurs **AMC 4R4**, les lecteurs du tableau suivant sont disponibles. Ne mélangez pas les protocoles sur le même contrôleur.

Nom du lecteur	Protocole Wiegand	Protocole BPR (*)	Protocole I-BPR	Protocole HADP	Protocole OSDP
WIE1	X				
WIE1K (Clavier)	X				
BPR MF		X			
Clavier BPR MF		X			
BPR LE		X			
Clavier BPR LE		X			
BPR HI		X			
Clavier BPR HI		X			
TA40 LE		X			
TB15 HI1		X			
TB30 LE		X			
INTUS 1600			X		
I-BPR			X		
I-BPR K (Clavier)			X		
DT 7020			X		
OSDP					X
OSDP K (Clavier)					X
OSDP KD (Clavier + Écran)					X

HADP				X	
HADP K (Clavier)				X	
HADP KD (Clavier + Écran)				X	
RKL 55 (Clavier + LCD)				X	
RK40 (Clavier)				X	
R15				X	
R30				X	
R40				X	
RK40				X	
RKL55				X	

(*) Le protocole BPR a été supprimé et est inclus ici pour des raisons de compatibilité uniquement.

Dans le cas d'un **lecteur OSDP**, la boîte de dialogue est semblable à ceci :



Communication sécurisée avec OSDP

Par défaut, la case **Activate encryption (Activer le chiffrement)** est désélectionnée. Sélectionnez-la si vous utilisez des lecteurs avec la prise en charge du **protocole sécurisé OSDPv2**.

Si vous désactivez ultérieurement le chiffrement en désélectionnant la case, réinitialisez le matériel du lecteur, conformément aux instructions du fabricant.

Par mesure de sécurité supplémentaire, toute tentative d'échange d'un lecteur OSDP configuré avec un lecteur OSDP différent génère une alarme dans le système de contrôle d'accès. L'opérateur peut accuser réception de l'alarme dans le client et autoriser simultanément l'échange.

Message d'alarme : **Exchange of OSDP reader refused (Échange de lecteur OSDP refusé)**

Commande : **Allow exchanging the OSDP reader (Autoriser l'échange du lecteur OSDP)**

Les types de lecteurs OSDP suivants sont disponibles :

OSDP	Lecteur OSDP standard
Clavier OSDP	Lecteur OSDP avec clavier
Clavier + écran OSDP	Lecteur OSDP avec clavier et écran

Les lecteurs OSDP suivants ont été testés :

OSDPv1 - mode non sécurisé	LECTUS duo 3000 C - MIFARE classic LECTUS duo 3000 CK - MIFARE classic LECTUS duo 3000 E - MIFARE Desfire EV1 LECTUS duo 3000 EK - MIFARE Desfire EV1
OSDPv2 - mode sécurisé et non sécurisé	LECTUS secure 2000 RO LECTUS secure 4000 RO LECTUS secure 5000 RO

Remarque!

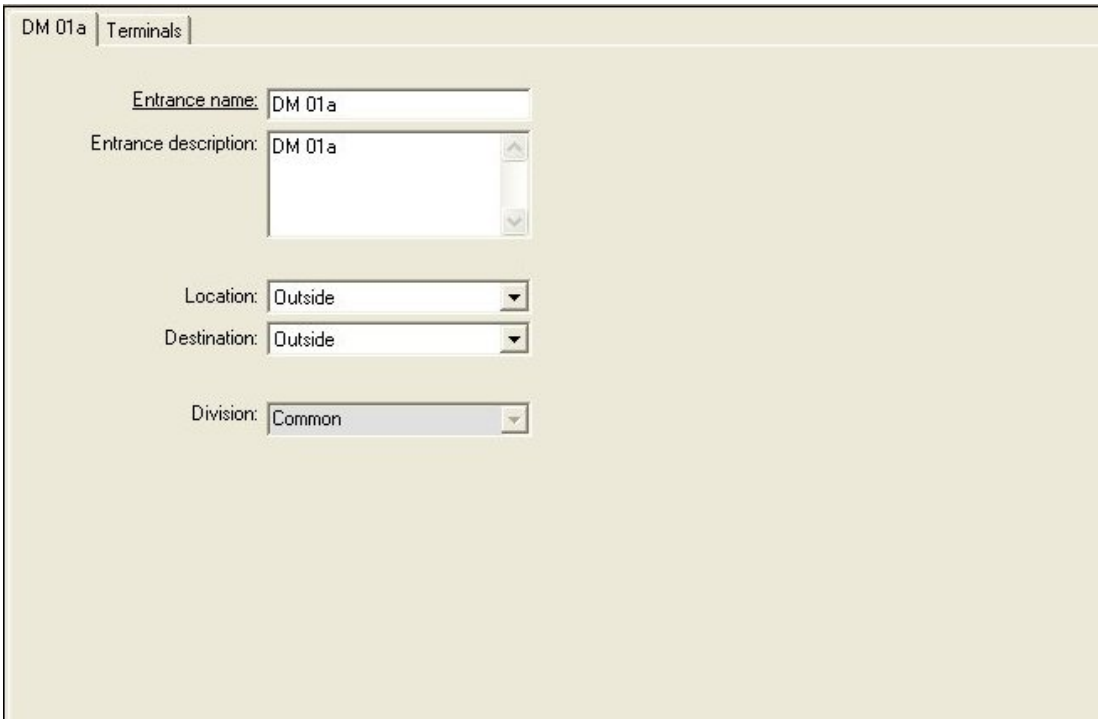
Mises en garde pour OSDP

Ne mélangez pas les familles de produits, par exemple **LECTUS duo** et **LECTUS secure** sur le même bus OSDP.

Une clé spécifique au client est générée et utilisée pour la transmission de données cryptées vers le lecteur OSDP. Assurez-vous que le système est correctement sauvegardé. Gardez les clés en sécurité. Les clés perdues ne peuvent pas être récupérées ; le lecteur ne peut être réinitialisé qu'aux paramètres d'usine.

Pour des raisons de sécurité, ne mélangez pas les modes cryptés et non cryptés sur le même bus OSDP.

Si vous désactivez le chiffrement en désélectionnant la case sur l'onglet OSDP du lecteur dans l'éditeur de dispositif, réinitialisez le matériel du lecteur, conformément aux instructions du fabricant.

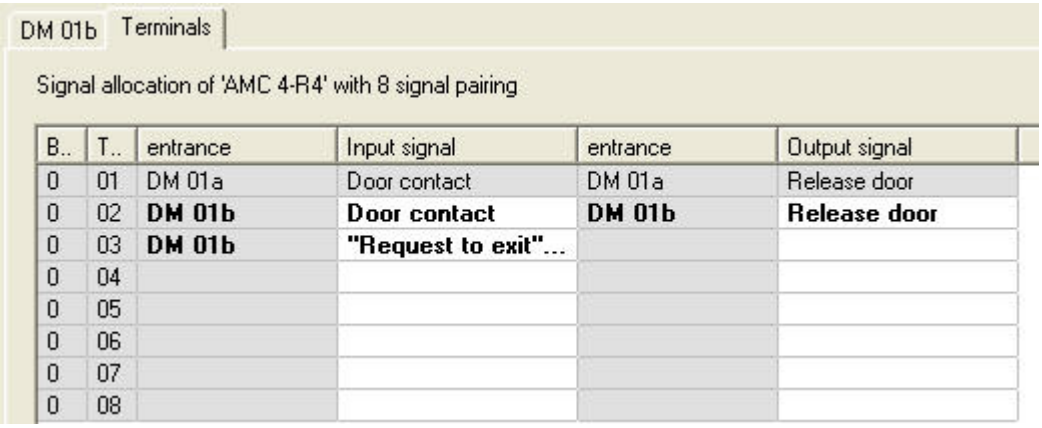


Paramètre	Valeurs possibles	Description
Nom de l'entrée	Alphanumérique, entre 1 et 16 caractères	La boîte de dialogue génère un nom unique pour l'entrée, mais ce nom peut être remplacé par l'opérateur qui configure l'entrée, s'il le souhaite.
Description de l'entrée	alphanumérique : 0 à 255 caractères	Texte descriptif arbitraire à afficher sur le système.
Emplacement	Toute zone définie (pas de parking)	Zone nommée (telle que définie sur le système) où se trouve le lecteur. Ces informations sont utilisées pour le contrôle de la séquence d'accès : si une personne essaie d'utiliser ce lecteur, mais que l'emplacement actuel de cette personne (tel que suivi par le système) est différent de celui du lecteur, le lecteur refusera l'accès à la personne.
Destination	Toute zone définie (pas de parking)	Zone nommée, telle que définie sur le système, à laquelle le lecteur autorise l'accès. Ces informations sont utilisées pour le contrôle de la séquence d'accès : Si une personne utilise ce lecteur, son emplacement sera mis à jour sur la valeur de **Destination**.

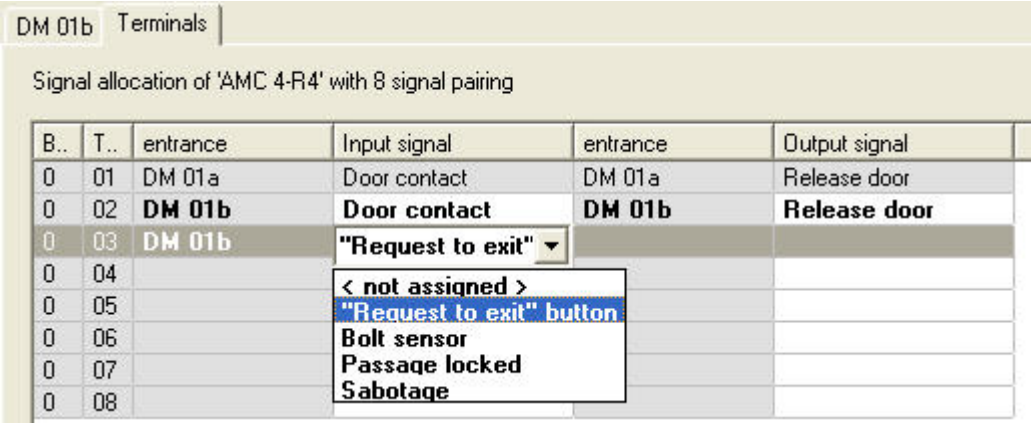
Temps d'attente décision d'accès externe	Nombre de dixièmes de seconde	Temps pendant lequel un contrôleur d'accès attend une décision d'un système ou d'un dispositif externe connecté à l'une de ses entrées.
Division	Division à laquelle appartient le lecteur. La valeur par défaut est **Commun**	Pertinent uniquement si la fonction **Divisions** est sous licence.
Zone d'armement (uniquement pour le modèle d'entrée 14)	Une lettre : A à Z	Les entrées d'un groupe IDS seront activées ensemble par l'activation des lecteurs de la zone.

16.3 Configuration des terminaux AMC

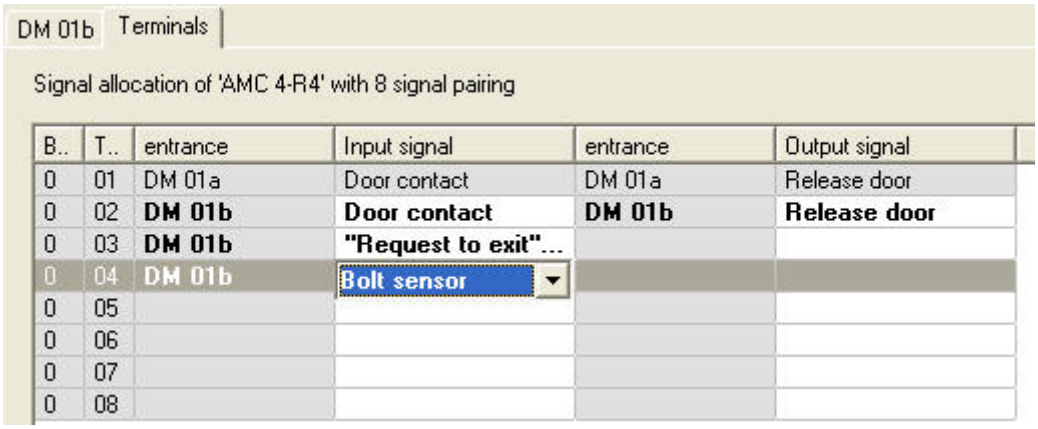
Dans son contenu et sa structure, cet onglet est identique à l'onglet **Terminaux** d'AMC.



Ici, cependant, il est possible de modifier l'affectation des signaux pour le modèle d'entrée sélectionné. Un double-clic dans les colonnes **Signal de sortie** ou **Signal d'entrée** affiche des listes déroulantes.



De même, il est possible de créer des signaux supplémentaires pour l'entrée respective. Un double-clic sur une ligne vide affiche la liste déroulante appropriée :

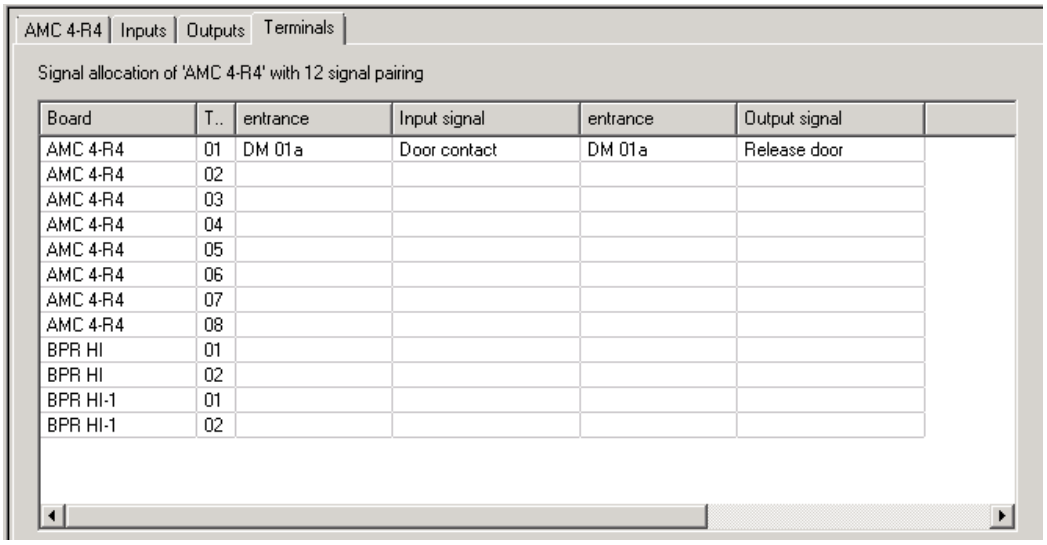


Les affectations de signaux inappropriées pour l'entrée que vous éditez sont en lecture seule, sur fond gris. Celles-ci ne peuvent être modifiées que lorsque l'entrée correspondante est sélectionnée.
Un arrière-plan gris similaire et une couleur de premier plan pâle sont donnés aux sorties qui ont été paramétrées dans l'onglet **Sorties** de l'AMC.

Remarque!
Les listes déroulantes ne sont pas 100 % sensibles au contexte, il est donc possible de sélectionner des signaux qui ne fonctionneront pas dans la vraie vie. Si vous ajoutez ou supprimez des signaux sous l'onglet **Terminaux**, testez-les pour vous assurer qu'ils sont logiquement et physiquement compatibles avec l'entrée.

Affectation des terminaux
Pour chaque AMC et chaque entrée, un onglet **Terminal** répertorie l'ensemble des 8 signaux pour l'AMC sur 8 lignes distinctes. Les signaux non utilisés sont marqués en blanc et ceux utilisés sont marqués en bleu.
La liste a la structure suivante :

- **Carte** : numérotation de l'extension AMC Wiegand (0) ou de la carte d'extension d'E/S (1 à 3)
- **Terminal** : numéro du contact sur l'AMC (01 à 08) ou la carte d'extension Wiegand (09 à 16).
- **Entrée** : nom de l'entrée
- **Signal de sortie** : nom du signal de sortie
- **Entrée** : nom de l'entrée
- **Signal d'entrée** : nom du signal d'entrée



Board	T..	entrance	Input signal	entrance	Output signal
AMC 4-R4	01	DM 01a	Door contact	DM 01a	Release door
AMC 4-R4	02				
AMC 4-R4	03				
AMC 4-R4	04				
AMC 4-R4	05				
AMC 4-R4	06				
AMC 4-R4	07				
AMC 4-R4	08				
BPR HI	01				
BPR HI	02				
BPR HI-1	01				
BPR HI-1	02				

–

Modification de l'affectation du signal

Sur les onglets de terminal des contrôleurs, l'affectation des signaux séparés est uniquement affichée (lecture seule). Sur les onglets de terminal des entrées respectives, cependant, il est possible de changer ou de repositionner les signaux des entrées sélectionnées.

Un double-clic sur l'entrée à modifier dans la colonne **Signal de sortie** ou **Signal d'entrée** active une liste déroulante, de sorte qu'une valeur différente peut être sélectionnée comme signal pour le modèle d'entrée. Si vous sélectionnez **Non attribué**, le signal est libéré et peut être utilisé pour d'autres entrées.

Ainsi, vous pouvez non seulement modifier les signaux, mais également attribuer des signaux à d'autres contacts afin d'optimiser l'utilisation de la tension disponible. Tous les contacts libres ou libérés peuvent être utilisés ultérieurement pour de nouveaux signaux ou comme nouvelles positions pour des signaux existants.

Remarque!

En principe, tous les signaux d'entrée et de sortie peuvent être sélectionnés librement, mais toutes les sélections n'ont pas de sens pour tous les modèles de portes. Par exemple, cela n'aurait aucun sens d'attribuer des signaux IDS à un modèle de porte (par exemple 01 ou 03) qui ne prend pas en charge l'IDS. Pour plus de détails, consultez le tableau de la section Attribution de signaux aux modèles de porte.

Attribution de signaux aux modèles de porte

Afin d'éviter un paramétrage incorrect des menus déroulants pour l'attribution de signaux aux modèles de portes, les menus ne proposent que les signaux compatibles avec le modèle de porte sélectionné.

Tableau des signaux d'entrée

Signaux d'entrée	Description
Contact de porte	
Bouton de « demande de sortie »	Bouton d'ouverture de la porte.

Capteur de pêne	Est utilisé pour les messages, uniquement. Il n'a pas de fonction de contrôle.
Entrée verrouillée	Est utilisée pour verrouiller provisoirement la porte opposée dans les passages. Mais peut également être utilisée pour le verrouillage à long terme.
Autosurveillance	Signal de sabotage d'un contrôleur externe.
Tourniquet en position normale	Le tourniquet est fermé.
Passage terminé	Un passage a réussi. Il s'agit d'une impulsion d'un contrôleur externe.
IDS : prêt pour armement	Défini par l'IDS, si tous les détecteurs sont au repos et que l'IDS peut être armé.
IDS : est armé	L'IDS est armé.
IDS : bouton de demande d'armement	Bouton d'armement de l'IDS.
Supprimer l'alarme d'ouverture non autorisée	Est utilisée si la disposition des entrées de porte permet d'ouvrir la porte sans l'aide de l'AMC. L'AMC n'envoie aucun message d'intrusion, mais "door local open" (ouverture locale de porte).
Décision d'accès externe acceptée	Le signal est défini si un système externe accepte l'accès
Décision d'accès externe refusée	Le signal est défini si un système externe refuse l'accès

Tableau des signaux de sortie

Signaux de sortie	**Description**
Débloquer la porte	
Passage : verrouiller la direction opposée	Verrouille l'autre côté du sas de sécurité. Ce signal est envoyé lorsque la porte s'ouvre.
Suppression alarmes	... vers l'IDS. Est défini tant que la porte est ouverte, afin d'éviter que l'IDS ne crée un message d'intrusion.
Feu vert	Voyant - est contrôlé tant que la porte est ouverte.
Temps max d'ouverture de la porte écoulé ou Sécurité de la porte compromise	Si la porte est maintenue ouverte ou ouverte trop longtemps
Connexion caméra	La caméra est activée au début d'un passage.
Libérer le tourniquet entrant	
Libérer le tourniquet sortant	

La porte est déverrouillée	Signal pour déverrouiller une porte pendant une période prolongée.
IDS : armer	Signal pour armer l'IDS.
IDS : désarmer	Signal pour désarmer l'IDS.
Décision d'accès externe activée	Le signal doit être défini pour activer le système d'accès externe

Tableau de correspondance des modèles de portes avec les signaux d'entrée et de sortie
Le tableau suivant répertorie les affectations explicites des signaux et des modèles de porte.

Modèle de porte	Description	Signaux d'entrée	Signaux de sortie
01	Porte simple avec lecteur d'entrée et de sortie Lecteurs pour l'heure et la présence Décision d'accès externe disponible	- Contact de porte - Bouton de « demande de sortie » - Capteur de pêne - Entrée verrouillée - Autosurveillance - Ouverture locale activée - Décision d'accès externe acceptée - Décision d'accès externe refusée	- Débloquer la porte - Passage : verrouiller la direction opposée - Suppression alarmes - Feu vert - Connexion caméra - Temps max d'ouverture de la porte écoulé ou Sécurité de la porte compromise - Décision d'accès externe activée
03	Porte pivotante avec lecteur d'entrée et de sortie Lecteurs pour l'heure et la présence Décision d'accès externe disponible	- Tourniquet en position de repos - Bouton de « demande de sortie » - Entrée verrouillée - Autosurveillance - Décision d'accès externe acceptée - Décision d'accès externe refusée	- Passage : verrouiller la direction opposée - Libérer le tourniquet entrant - Libérer le tourniquet sortant - Suppression alarmes - Connexion caméra - Temps max d'ouverture de la porte écoulé ou - Sécurité de la porte compromise - Décision d'accès externe activée
05	Entrée ou sortie du parking - maximum de 24 zones de stationnement Lecteurs pour l'heure et la présence	- Contact de porte - Bouton de « demande de sortie » - Entrée verrouillée - Passage terminé - Décision d'accès externe acceptée	- Débloquer la porte - Suppression alarmes - Feu vert - Temps max d'ouverture de la porte écoulé ou - Sécurité de la porte compromise

	Décision d'accès externe disponible	- Décision d'accès externe refusée	- La porte est déverrouillée - Décision d'accès externe activée
06	Lecteurs pour l'heure et la présence		
07	Ascenseur - maximum 56 étages		
09	Entrée véhicule ou lecteur sortant et bouton poussoir Lecteurs pour l'heure et la présence Décision d'accès externe disponible	- Contact de porte - Bouton de « demande de sortie » - Entrée verrouillée - Passage terminé - Décision d'accès externe acceptée - Décision d'accès externe refusée	- Débloquer la porte - Suppression alarmes - Feu vert - Temps max d'ouverture de la porte écoulé ou - Sécurité de la porte compromise - La porte est déverrouillée - Décision d'accès externe activée
10	Porte simple avec lecteur d'entrée et de sortie et armement/ désarmement de l'IDS Lecteurs pour l'heure et la présence Décision d'accès externe disponible	- Contact de porte - Bouton de « demande de sortie » - IDS : prêt pour armement - IDS : est armé - Autosurveillance - IDS : demande d'armement - Décision d'accès externe acceptée - Décision d'accès externe refusée	- Débloquer la porte - Connexion caméra - IDS : armer - IDS : désarmer - Temps max d'ouverture de la porte écoulé ou - Sécurité de la porte compromise - Décision d'accès externe activée
14	Porte simple avec lecteur d'entrée et de sortie et armement/ désarmement de l'IDS Lecteurs pour l'heure et la présence	- Contact de porte - Bouton de « demande de sortie » - IDS : prêt pour armement - IDS : est armé - Autosurveillance - IDS : demande d'armement	- Débloquer la porte - Connexion caméra - IDS : armer - Temps max d'ouverture de la porte écoulé ou - Sécurité de la porte compromise
15	Contacts numériques		

Attribution de signaux aux lecteurs

Les lecteurs série (c'est-à-dire les lecteurs sur un AMC2 4R4) et les lecteurs OSDP peuvent être améliorés avec des signaux d'E/S locaux. De cette manière, des signaux supplémentaires peuvent être rendus disponibles et les chemins électriques vers les contacts de porte raccourcis.

Lorsqu'un lecteur série est créé, l'onglet **Terminaux** de l'entrée correspondante affiche deux signaux d'entrée et deux signaux de sortie pour chaque lecteur sous le contrôleur et (le cas échéant) les signaux de la carte d'extension.

Remarque!

Ces entrées de liste sont créées pour chaque lecteur série, qu'il dispose ou non d'E/S locales.

Ces signaux locaux de lecteur ne peuvent pas être affectés à des fonctions et paramétrés comme ceux des contrôleurs et des cartes. Ils n'apparaissent pas non plus sous les onglet **Signal d'entrée** et **Signal de sortie**, et ils ne peuvent pas non plus être utilisés pour les ascenseurs (par exemple pour dépasser la limite des 56 étages). Pour cette raison, ils sont particulièrement adaptés à la commande directe des portes (par exemple, gâche ou déverrouillage de porte). Cela libère cependant les signaux du contrôleur pour des fonctions paramétrées plus complexes.

Édition des signaux

Lorsqu'une entrée est créée, l'onglet **Terminaux** de l'entrée correspondante affiche deux signaux d'entrée et deux signaux de sortie pour chaque lecteur sous le contrôleur. La colonne Carte affiche le nom du lecteur. Les signaux standard pour l'entrée sont affectés par défaut aux premiers signaux libres sur le contrôleur. Pour pouvoir être déplacés vers les propres signaux du lecteur, ils doivent d'abord être supprimés de leurs positions d'origine. Pour ce faire, sélectionnez l'entrée de liste **<Non attribué>**

Double-cliquez dans la colonne **Signal d'entrée** ou **Signal de sortie** du lecteur pour voir une liste des signaux possibles pour le modèle de porte choisi, et ainsi repositionner le signal. Comme tous les signaux, ils peuvent être consultés sous l'onglet **Terminaux** du contrôleur, mais pas édités ici.

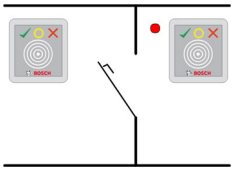
Remarque!

L'état des signaux du lecteur ne peut pas être surveillé.

Ils ne peuvent être utilisés que pour la porte à laquelle appartient le lecteur.

16.4 Signaux prédéfinis pour les modèles de portes

Modèle d'entrée 01



Variantes des modèles :

01a	Porte normale avec lecteur d'entrée **et** de sortie

01b	Porte normale avec lecteur d'entrée et bouton-poussoir
01c	Porte normale avec lecteur d'entrée **ou** de sortie

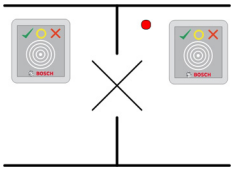
Signaux possibles :

Signaux d'entrée	**Signaux de sortie**
Contact de porte	Débloquer la porte
Bouton de « demande de sortie »	Passage : verrouiller la direction opposée
Autosurveillance	Feu vert
Supprimer l'alarme d'ouverture non autorisée	Connexion caméra
	Temps max d'ouverture de la porte écoulé ou Sécurité de la porte compromise

Remarque!
Les fonctions de comptage individuel, en particulier le verrouillage de la direction opposée, peut être paramétrée uniquement avec DM 03.

La suppression des alarmes n'est activée que lorsque la durée de suppression des alarmes avant l'ouverture de la porte est supérieure à 0.
Ce modèle d'entrée peut également être avantageuse pour les entrées de véhicules. Dans ce cas, il est également recommandé d'installer un lecteur secondaire pour les camions et les voitures.

Modèle d'entrée 03



Variantes des modèles :

03a	Tourniquet pivotant avec lecteur d'entrée **et** de sortie
03b	Tourniquet pivotant avec lecteur d'entrée et bouton-poussoir
03c	Tourniquet avec lecteur d'entrée **ou** de sortie

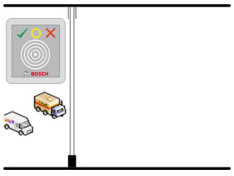
Signaux possibles :

Signal d'entrée	**Signaux de sortie**
Tourniquet en position normale	Libérer le tourniquet entrant
Bouton de « demande de sortie »	Libérer le tourniquet sortant

Autosurveillance	Entrée verrouillée
Supprimer l'alarme d'ouverture non autorisée	Connexion caméra
	Temps max d'ouverture de la porte écoulé ou Sécurité de la porte compromise
Signaux supplémentaires utilisant l'option de **sas de sécurité** :	
Entrée verrouillée	Passage : verrouiller la direction opposée
	Suppression alarmes

Notes de configuration pour les sas de sécurité :
Lorsque le tourniquet est en position normale, le premier signal d'entrée de tous les lecteurs connectés est activé. Si une carte est présentée et si le propriétaire a les droits d'accès pour cette entrée, alors :
– Si cela se passe au niveau du lecteur d'entrée, le premier signal de sortie est réglé sur le lecteur d'entrée pour la durée du temps d'activation.
– Si cela se passe au niveau du lecteur de sortie, le deuxième signal de sortie est défini au niveau du lecteur de sortie pendant la durée du temps d'activation.
Lorsque le bouton de demande de sortie (REX) est enfoncé, le deuxième signal d'entrée et le deuxième signal de sortie sont définis. Pendant ce temps, la porte pivotante peut être utilisée dans le sens activé.

Modèle d'entrée 05c



Variante de modèle :

05c	Lecteur d'entrée **ou** de sortie pour l'accès au parking

Signaux possibles pour ce modèle d'entrée :

Signaux d'entrée	**Signaux de sortie**
Contact de porte	Débloquer la porte
Bouton de « demande de sortie »	La porte est déverrouillée
Entrée verrouillée	Feu vert
Passage terminé	Suppression alarmes
	Temps max d'ouverture de la porte écoulé ou Sécurité de la porte compromise

L'entrée et la sortie du parking doivent être configurées sur le même contrôleur. Si l'accès au parking a été attribué à un contrôleur, alors ce contrôleur ne peut régir aucun autre modèle de porte. Pour l'entrée du parking, seul un lecteur d'entrée (et aucun lecteur de sortie) peut être attribué. Une fois l'entrée attribuée, la sélection du modèle de porte vous permet uniquement de définir le lecteur de sortie. Vous pouvez définir jusqu'à 24 sous-zones pour chaque parking, dont une doit figurer dans les autorisations de la carte pour que la carte fonctionne.

Modèle d'entrée 06

Variantes des modèles

06a	Lecteur d'entrée **et** de sortie pour le temps et la présence
06c	Lecteur d'entrée **ou** de sortie pour le temps et la présence

Les lecteurs créés avec ce modèle de porte ne contrôlent pas les portes ou les barrières, mais transmettent uniquement les données de la carte à un système de temps et de présence. Ces lecteurs sont généralement situés dans des endroits dont l'accès a déjà été contrôlé.
Par conséquent, aucun signal n'est défini.

Remarque!
Afin que des paires de pointage valides (heure d'entrée et heure de sortie) puissent être créées dans le système de temps et de présence, il est nécessaire de paramétrer deux lecteurs séparés avec le modèle de porte 06 : un pour le pointage entrant et un pour la sortie.

Utilisez une variante **a** lorsque l'entrée et la sortie ne sont pas distinctes. Utilisez une variante **c** si l'entrée et la sortie sont géographiquement séparées, ou si vous ne pouvez pas connecter les lecteurs au même contrôleur. Assurez-vous de définir l'un des lecteurs comme lecteur entrant et l'autre comme lecteur sortant.
Comme pour toute entrée, il est nécessaire de créer et d'attribuer des autorisations.
L'onglet **Gestion du temps** dans les boîtes de dialogue **Autorisations d'accès** et **Autorisations de zone/heure** liste tous les lecteurs de temps et de présence qui ont été définis. Activez au moins un lecteur dans le sens entrant et un lecteur dans le sens sortant. Les autorisations pour les lecteurs de temps et de présence peuvent être attribuées avec d'autres autorisations d'accès ou en tant qu'autorisations distinctes.
S'il existe plusieurs lecteurs de temps et de présence pour une direction donnée, il est alors possible d'attribuer certains détenteurs de carte à certains lecteurs. Seuls les temps de présence des utilisateurs affectés et autorisés seront enregistrés et stockés par le lecteur.

Remarque!
D'autres fonctionnalités de contrôle d'accès affectent également le comportement des lecteurs de temps et de présence. Par conséquent, des listes noires, des modèles horaires ou des dates d'expiration peuvent également empêcher un lecteur de temps et de présence d'enregistrer les heures d'accès.

Les heures d'entrée et de sortie enregistrées sont stockées dans un fichier texte dans le répertoire : `<SW_installation_folder>\AccessEngine\AC\TAExchange\`
sous le nom `TAccExc_EXP.txt` et placées en attente d'exportation vers un serveur de temps et de présence.
Les données de pointage sont transmises au format suivant :
`ddMMyyyy;hhmm[s];Direction [0,1]; AbsenceReason; Personnel-Nr.`
d=jour, M=mois, y=année, h=heure, m=minute, s=heure d'été, 0=sortant, 1=entrant
Le fichier d'exportation contient tous les pointages par ordre chronologique. Le séparateur de champ dans le fichier est un point-virgule.

Variantes du modèle d'entrée 07

Variantes des modèles :

07a	Ascenseur avec max. 56 étages
07c	Ascenseur avec max. 56 étages et modèle horaire

Modèle d'entrée 07a
Signaux :

Signal d'entrée	Signaux de sortie
	Release <nom de l'étage>
	Un signal de sortie par étage défini, avec un maximum de 56.

Lors de l'invocation de l'ascenseur, le détenteur de carte ne peut sélectionner que les étages pour lesquels sa carte est autorisée.
Les modèles de porte d'ascenseur ne peuvent pas être mélangés avec d'autres modèles de porte sur le même contrôleur. L'utilisation de cartes d'extension jusqu'à 56 étages peut être définie pour chaque ascenseur sur un AMC. Les autorisations de la carte doivent contenir l'ascenseur lui-même et au moins un étage.

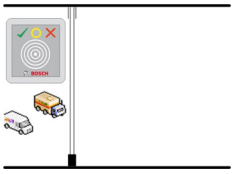
Modèle d'entrée 07c
Signaux :

Signal d'entrée	Signal de sortie
Input key <nom de l'étage>	Release <nom de l'étage>
Pour chaque étage défini, il existe une entrée de sortie et d'entrée - jusqu'à 56.	

Lors de l'appel de l'ascenseur et en appuyant sur un bouton de sélection d'étage (d'où la nécessité de signaux d'entrée), les autorisations de la carte sont vérifiées pour voir si elles incluent l'étage choisi.
De plus, avec ce modèle de porte, il est possible de définir tous les étages d'**accès public**, c'est-à-dire qu'aucun contrôle d'autorisation ne sera effectué pour ces étages, et toute personne peut y prendre l'ascenseur. Néanmoins, l'accès public peut lui-même être régi par un **modèle horaire** qui limite l'accès à certaines heures de certains jours. En dehors de ces heures, les contrôles d'autorisation seront effectués comme d'habitude.

Les modèles de porte d'ascenseur ne peuvent pas être mélangés avec d'autres modèles de porte sur le même contrôleur. L'utilisation de cartes d'extension jusqu'à 56 étages peut être définie pour chaque ascenseur sur un AMC. Les autorisations de la carte doivent contenir l'ascenseur lui-même et au moins un étage.

Modèle d'entrée 09

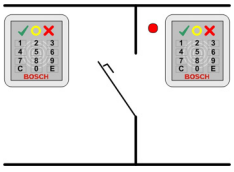


Signaux possibles :

Signaux d'entrée	Signaux de sortie
Contact de porte	Débloquer la porte
Bouton de « demande de sortie »	La porte ouverte à long terme
Entrée verrouillée	Le feu de circulation est vert
Passage terminé	Suppression alarmes
	Temps max d'ouverture de la porte écoulé ou Sécurité de la porte compromise

Pour le contrôle de barrière, un contrôle sous-jacent (SPS) est supposé. Contrairement au **modèle de porte 5c**, vous pouvez configurer cette entrée et cette sortie sur différents AMC. De plus, il n'y a pas de sous-zones, mais seulement une autorisation générale pour le parking.

Modèle d'entrée 10



Variantes des modèles :

10a	Porte normale avec lecteur d'entrée **et** de sortie **et** armement/désarmement (système de détection d'intrusion) de l'IDS
10b	Porte normale avec entrée, bouton REX (demande de sortie) et armement/désarmement d'IDS
10e	Porte normale avec entrée, bouton REX et armement/désarmement décentralisé de l'IDS

Signaux possibles :

Signaux d'entrée	Signaux de sortie
Contact de porte	Débloquer la porte
IDS : est armé	IDS : armer

IDS : prêt pour armement	IDS : désarmer [uniquement DM 10e]
Bouton de « demande de sortie »	Connexion caméra
Capteur de pêne	Temps max d'ouverture de la porte écoulé ou Sécurité de la porte compromise
Autosurveillance	
Supprimer l'alarme d'ouverture non autorisée	
IDS : bouton de demande d'armement	

Remarque!
Ce modèle de porte nécessite des lecteurs de clavier. Les détenteurs de carte exigent des **codes PIN** pour armer/désarmer l'IDS.

Différentes procédures sont nécessaires en fonction des lecteurs installés.

Lecteurs série (y compris I-BPR, HADP et OSDP)
Armez en appuyant sur la touche **7** et en confirmant avec Entrée (#). Présentez ensuite la carte, saisissez le code PIN et confirmez à nouveau avec la touche Entrée (#).
Désarmez en présentant la carte, en entrant le code PIN et en confirmant avec Entrée (#).

Lecteurs Wiegand (y compris le protocole série BPR)
Armez en appuyant sur 7, en présentant la carte et en entrant le code PIN. Il n'est pas nécessaire de confirmer à l'aide de la touche Entrée.
Désarmez en présentant la carte et en entrant le code PIN. Le désarmement et l'ouverture de la porte se produisent simultanément.

Fonctions spéciales du DM 10e :
Alors qu'avec les modèles de porte 10a et 10b, chaque entrée est sa propre zone de sécurité, avec le modèle 10e plusieurs entrées peuvent être regroupées en unités.
N'importe quel lecteur de ce groupe est capable d'armer ou de désarmer l'ensemble de l'unité. Un signal de sortie **Désarmer l'IDS** est nécessaire pour réinitialiser l'état défini par l'un des lecteurs du groupe.
Signaux :
- Modèles de porte 10a et 10b :
  - - L'armement est déclenché par un signal fixe
  - - Le désarmement est déclenché par l'arrêt du signal permanent.
- Modèle de porte 10e :
  - - L'armement et le désarmement sont déclenchés par une impulsion de signal d'une durée de 1 seconde.

[En utilisant un relais bistable, il est possible de contrôler l'IDS à partir de plusieurs portes. Pour ce faire, les signaux de toutes les portes nécessitent une opération OU au niveau du relais. Les signaux **IDS armé** et **IDS prêt pour armement** doivent être répliqués sur toutes les portes participantes.]

Entrées spéciales
Pour les modèles d'entrée avec des caractéristiques spéciales, telles que :

– Ascenseurs
– Détection d'intrusion
– Commutateurs numériques ou binaires génériques
– Sas de sécurité

se référer au chapitre dédié aux Entrées spéciales.

Se reporter à

– *Entrées spéciales, page 97*

16.5 Entrées spéciales

16.5.1 Ascenseurs (DM07)

Remarques générales sur les ascenseurs (modèle d'entrée 07)

Les ascenseurs ne peuvent pas être combinés avec d'autres modèles de portes sur le même contrôleur AMC.

Les ascenseurs ne peuvent pas être utilisés avec les options de lecteur **Accès de groupe** ou **Assistant requis**

Jusqu'à 8 étages peuvent être définis sur un AMC. Une carte d'extension AMC propose 8 ou 16 sorties supplémentaires par carte d'extension.

Par conséquent, en utilisant le nombre maximum des plus grandes cartes d'extension, il est possible de configurer jusqu'à 56 étages avec des lecteurs RS485, et 64 étages avec des lecteurs Wiegand, si une carte d'extension Wiegand spéciale est utilisée en plus.

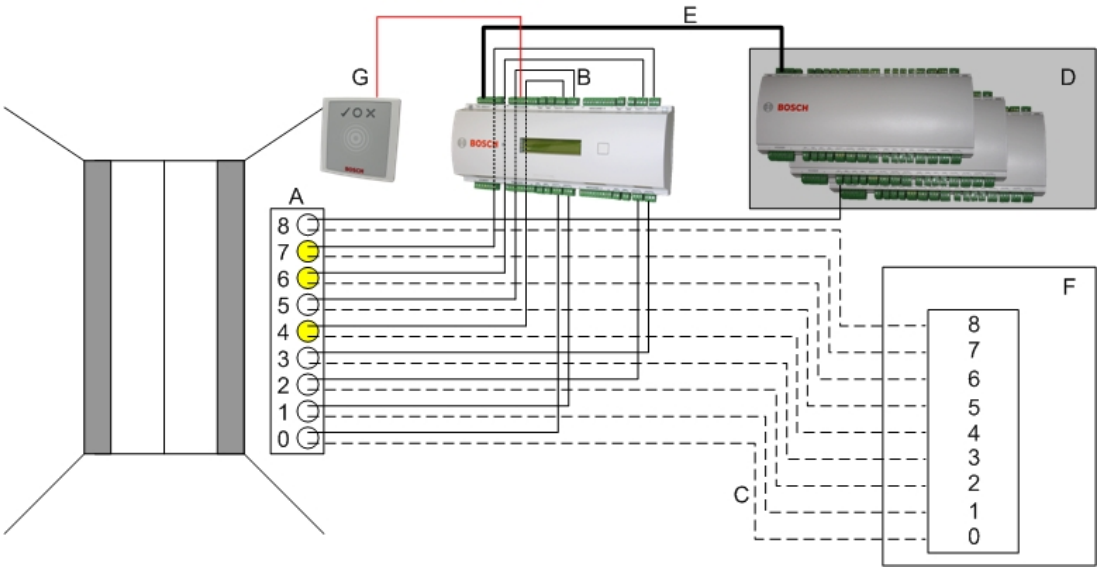
Différences entre les modèles d'entrée 07a et 07c

Dans les boîtes de dialogue d'autorisation d'accès, vous pouvez attribuer des étages spécifiques à l'autorisation d'une personne.

Si l'ascenseur a été créé à l'aide du modèle d'entrée **07a**, un détenteur de carte présente son badge et les étages pour lesquels il possède une autorisation deviennent disponibles. Avec le modèle d'entrée **07c**, le système vérifie l'autorisation pour l'étage sélectionné une fois que la personne l'a choisi. Les étages marqués **publics** sont disponibles pour chaque personne indépendamment de l'autorisation. Avec un modèle horaire, la fonction publique peut être limitée au modèle horaire spécifié. En dehors de cette période, l'autorisation sera vérifiée pour l'étage sélectionné.

Schéma de câblage des ascenseurs :

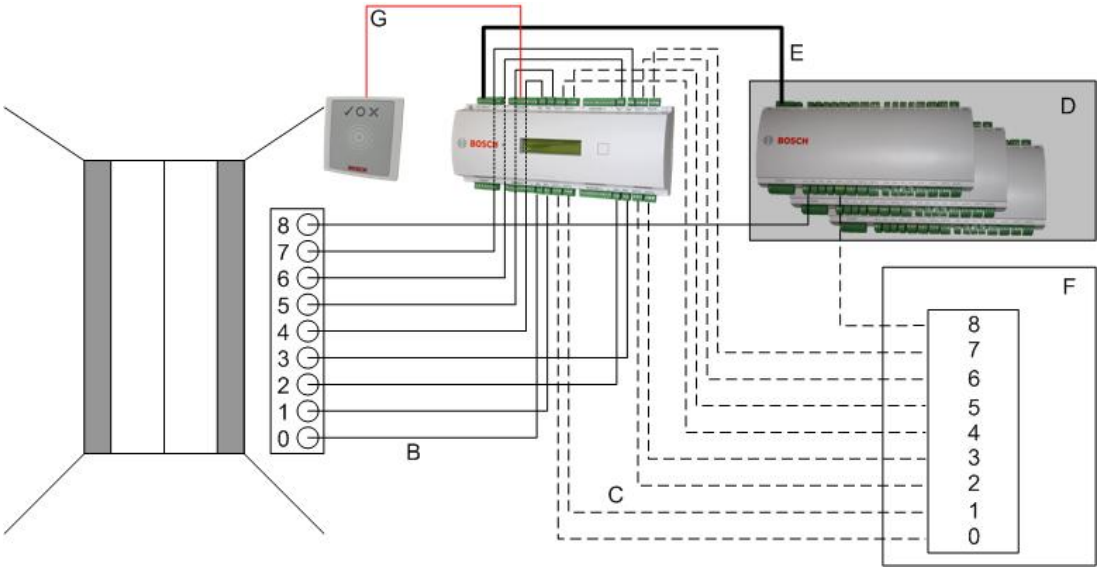
L'image suivante illustre le schéma de connexion d'un ascenseur utilisant le modèle de porte 07a.



Légende :

- A = Clavier de l'ascenseur
- B = (trait continu) Signaux de sortie AMC
- C = (ligne interrompue) Connexion aux commandes d'ascenseur
- D = jusqu'à trois cartes d'E/S peuvent être connectées à un AMC, si ses huit entrées et sorties ne sont pas suffisantes.
- E = Trafic de données et alimentation entre l'AMC et les cartes E/S
- F = Sélecteur d'étage de l'ascenseur
- G = Lecteur. Deux lecteurs peuvent être configurés pour chaque ascenseur.

L'image suivante illustre le schéma de connexion d'un ascenseur utilisant le modèle de porte 07c.



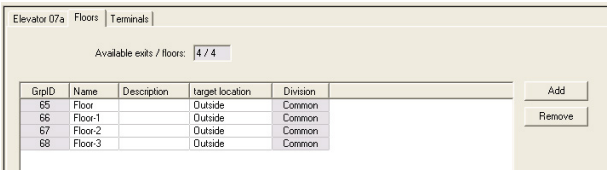
Légende :

- B = (trait continu) Signaux de sortie AMC
- C = (ligne interrompue) Connexion aux commandes d'ascenseur
- D = jusqu'à trois cartes d'E/S peuvent être connectées à un AMC, si ses huit entrées et sorties ne sont pas suffisantes.
- E = Trafic de données et alimentation entre l'AMC et les cartes E/S
- F = Sélecteur d'étage de l'ascenseur

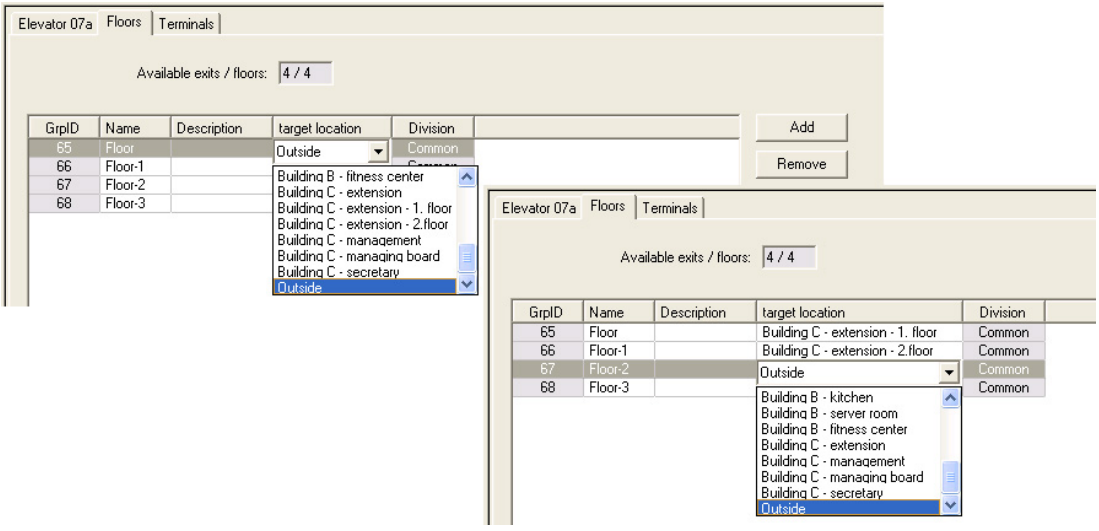
– G = Lecteur. Deux lecteurs peuvent être configurés pour chaque ascenseur.

Comme les parkings, les ascenseurs ont le paramètre **Public.** Ce paramètre peut être défini individuellement pour chaque étage. Si le paramètre **Public** est activée, les autorisations d'accès ne sont pas vérifiées - ainsi, tout détenteur de carte dans l'ascenseur peut sélectionner l'étage.
Si vous le souhaitez, définissez un modèle horaire pour le modèle d'entrée : En dehors des fuseaux horaires définis, les autorisations seront vérifiées.

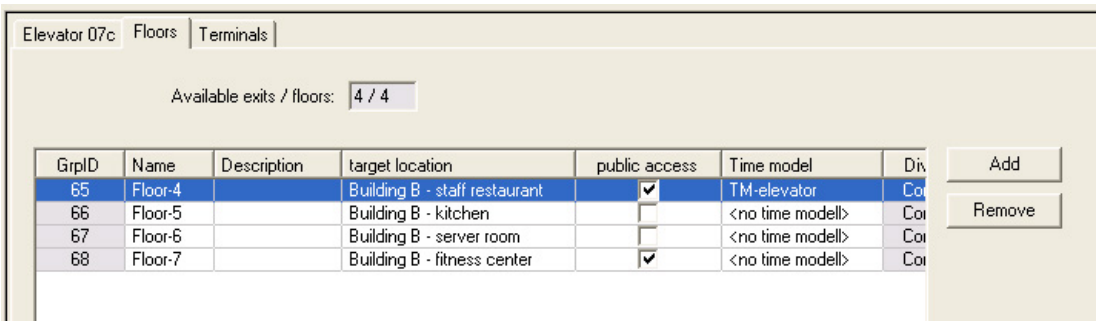
Étages pour le modèle d'entrée 07
Utilisez l'onglet **Étages** pour ajouter et retirer des étages de l'ascenseur, à l'aide des boutons **Ajouter** et **Retirer**.



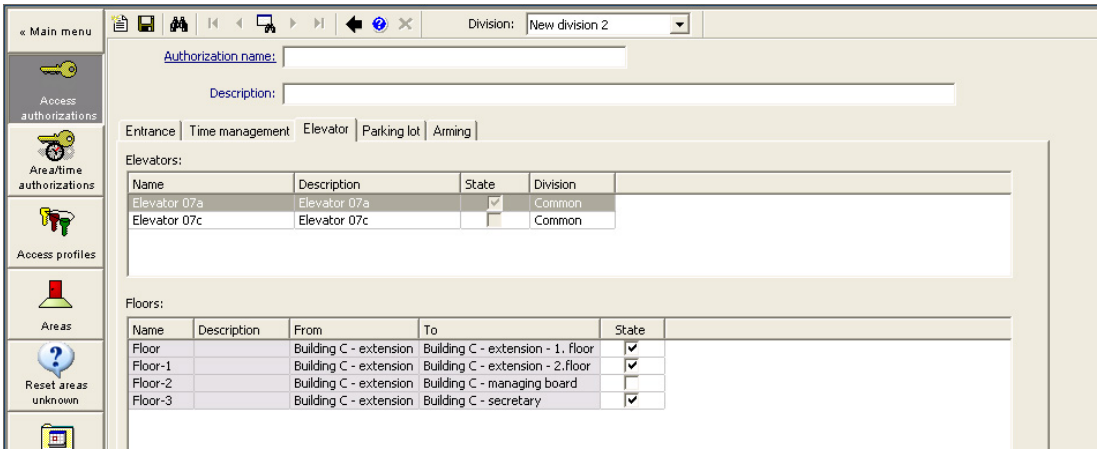
Les emplacements cibles d'un étage peuvent être des **Zones**, à l'exception des parking et des zones de stationnement.
Une seule zone peut être affectée à une zone individuelle. Le choix des zones proposées dans les listes déroulantes est donc réduit après chaque affectation, ce qui permet d'éviter les doubles affectations involontaires.



Lors de l'utilisation du modèle d'entrée 07a, il est possible de rendre des étages individuels accessibles en sélectionnant la zone **Accès public**. Dans ce cas, aucune vérification des autorisations n'est effectuée. L'affectation supplémentaire d'un **Modèle horaire** limiterait néanmoins l'accès à des périodes prédéfinies.



Sous l'onglet **Ascenseur** au-dessus de la zone de liste supérieure dans les boîtes de dialogue **Autorisations d'accès** et **Autorisations de zone/heure**, sélectionnez d'abord l'ascenseur souhaité, puis, en dessous, les étages auxquels a accès le détenteur de carte.



16.5.2 Modèles de portes avec alarmes anti-intrusion (DM14)

Introduction

Contrairement au modèle d'entrée 10 (DM10), **DM14** peut armer et désarmer un système d'alarme anti-intrusion, ou IDS pour une zone d'armement particulière. Une entrée DM14 peut également être configurée pour accorder l'accès au détenteur de la carte qui la désarme, à condition que ce détenteur de la carte dispose de toutes les autres autorisations d'accès requises.

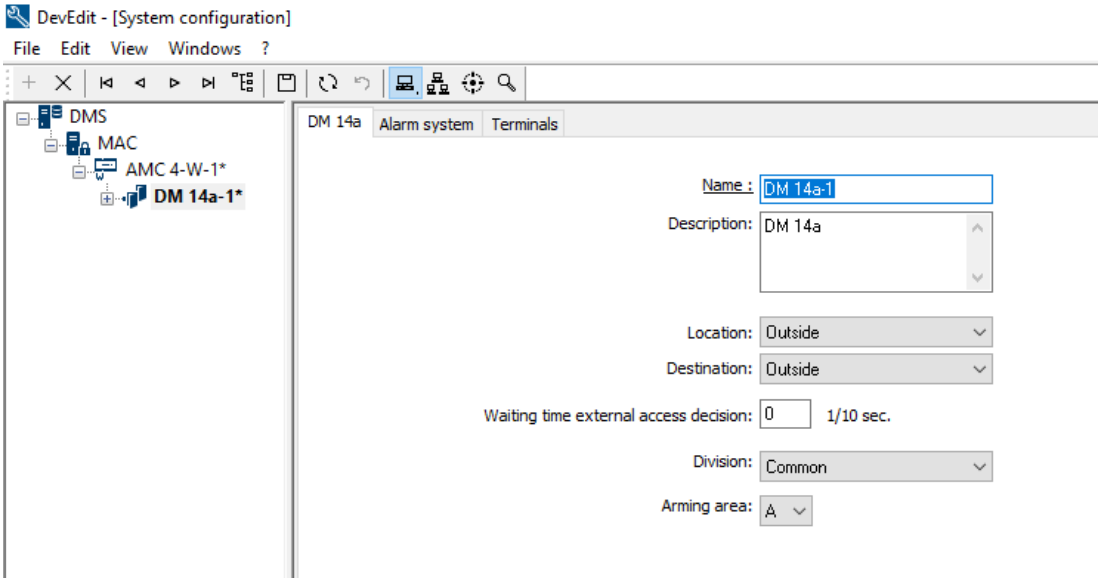
La procédure de configuration du DM14 dans l'éditeur de dispositif et le gestionnaire de dialogue comprend les tâches suivantes :

1. Définir les paramètres généraux pour identifier l'entrée et sa zone d'armement.
2. Définir des paramètres spécifiques pour définir la procédure exacte de désarmement de la zone.
3. Définir les signaux d'entrée et de sortie spécifiques à l'IDS sur les bornes du contrôleur de porte d'entrée.
4. Inclure les autorisations d'armement/ désarmement dans les autorisations d'accès des détenteurs de carte qui doivent gérer les entrées DM 14.

Les tâches sont décrites dans les sections suivantes.

Paramètres généraux

Sur le premier onglet, **DM14a** ou **DM14b**, définissez les paramètres suivants.

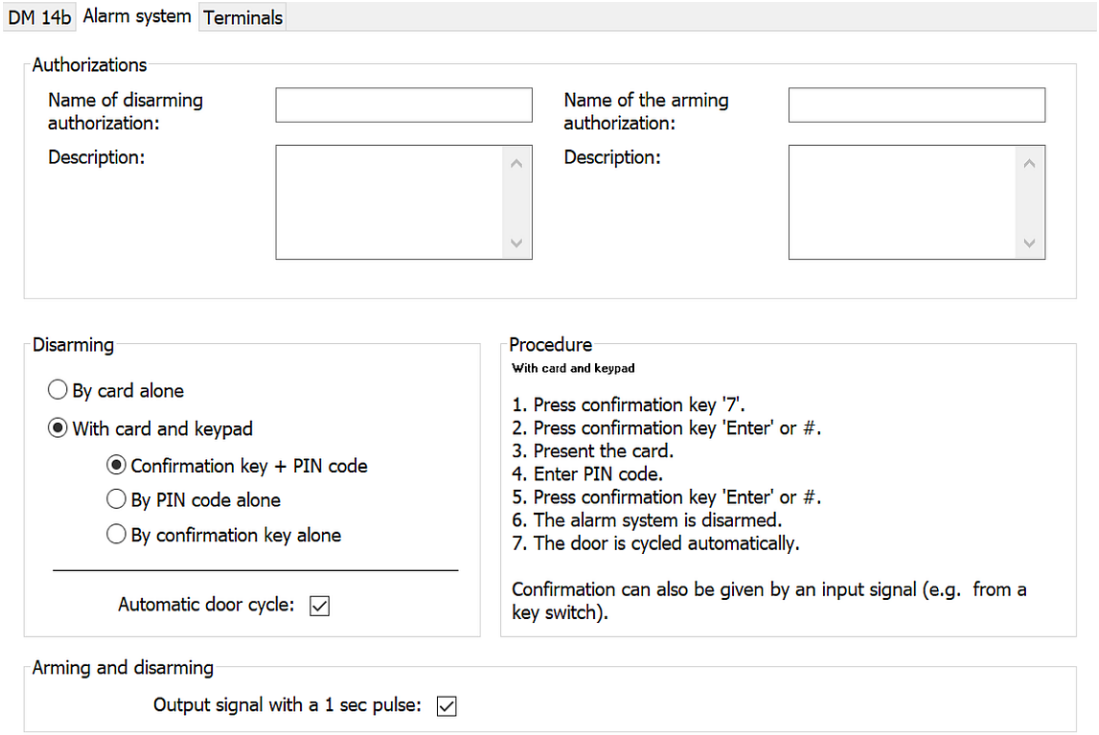


Paramètre	Type de valeur	Description
Nom	Texte libre	Nom de l'entrée.
Description	Texte libre, facultatif	Description de l'entrée.
Emplacement	Liste des zones définies, si utilisé	Zone d'accès où se trouve l'entrée.
Destination	Liste des zones définies, si utilisé	Zone d'accès à laquelle mène l'entrée.
Division	Liste des divisions définies, si utilisé	Division ou locataire au sein du système de contrôle d'accès auquel appartient l'entrée.
Temps d'attente décision d'accès externe	Dixièmes de secondes	Si vous avez connecté un système externe aux terminaux de l'AMC, pour prendre des décisions d'accès en son nom, ce paramètre limite le temps d'attente pour une réponse du système externe.

Paramètre	Type de valeur	Description
		Remarque : La décision d'accès nécessite le respect de **toutes** les conditions définies sur le système de contrôle d'accès, par exemple, les autorisations d'accès, les modèles horaires et les divisions (le cas échéant). La valeur par défaut est 0, c'est-à-dire que le paramètre est ignoré.
Zone d'armement	Liste des lettres majuscules A... Z	Lettre sous laquelle regrouper les entrées DM14 dans Zones d'armement.

Paramètres système d'alarme

Sur le deuxième onglet, **Système d'alarme**, définissez les paramètres suivants. Ces paramètres régissent les informations d'identification et la procédure de désarmement de l'IDS, et le désarmement affecte toutes les entrées dans la même zone d'armement, comme défini dans le premier onglet.



Paramètre	Type de valeur	Description
Volet des autorisations		

Paramètre	Type de valeur	Description
Nom de l'autorisation de désarmement	Texte libre	Nom qui doit figurer dans les protocoles et les rapports lorsqu'un détenteur de carte désarme l'IDS à cette entrée.
Nom de l'autorisation d'armement	Texte libre	Nom qui doit figurer dans les protocoles et les rapports lorsqu'un détenteur de carte arme l'IDS à cette entrée.
Description (un pour chaque autorisation)	Texte libre, facultatif	Descriptions des autorisations d'armement
Volet de désarmement		
Par carte seule	Case d'option	Sélectionnez cette option pour permettre à l'IDS d'être désarmé en présentant une carte au lecteur, sans autre authentification.
Par carte et clavier	Case d'option	Sélectionnez cette option pour permettre à l'IDS d'être désarmé en présentant une carte au lecteur et en donnant une authentification supplémentaire via le clavier du lecteur. La procédure exacte d'authentification et de désarmement est déterminée par les sous-paramètres suivants :
Touche de confirmation + code PIN	Case d'option	Les détenteurs de carte doivent s'authentifier à l'aide d'une carte, d'une clé de confirmation et d'un code PIN.
Par code PIN seul	Case d'option	Les détenteurs de carte doivent s'authentifier à l'aide d'une carte et d'un code PIN.
Par touche de confirmation seule	Case d'option	Les détenteurs de carte doivent s'authentifier à l'aide d'une carte et d'une clé de confirmation.
Cycle de porte automatique	Case à cocher	Cochez cette case si vous souhaitez activer le verrouillage de la porte lors du désarmement, pour permettre au détenteur de la carte de désarmer et d'entrer simultanément. **Remarque :** Le verrouillage n'effectuera un cycle que si le détenteur de la carte a également l'autorisation d'accès pour cette porte.
Volet de procédure		
En fonction des paramètres définis dans le volet **Désarmement**, ce volet affiche une procédure standard de désarmement de l'IDS. Communiquez cette procédure aux détenteurs de carte qui utiliseront les entrées DM14 dans cette zone d'armement.		
Volet d'armement et de désarmement		

Paramètre	Type de valeur	Description
Signal de sortie avec une impulsion de 1 s	Case à cocher	Cochez cette case si vous utilisez une centrale intrusion **Bosch B ou G-Series**. Le résultat est l'envoi d'un signal d'impulsion unique pour basculer l'état d'armement de la zone d'intrusion de l'entrée, plutôt que de définir le signal sur une constante 1 (armement) ou 0 (désarmement).

Bornes du contrôleur de porte

Afin de rendre possible l'armement et le désarmement avec une entrée DM14, vous devez définir l'entrée IDS et les signaux de sortie que vous souhaitez utiliser sur les bornes du contrôleur de porte d'entrée.

Cette étape est requise une fois pour chaque contrôleur comportant des entrées DM14. Toutes les entrées DM14 suivantes que vous définissez sur le même contrôleur et ses cartes d'extension hériteront des signaux du contrôleur partagé.

Les signaux par défaut sont décrits dans le tableau suivant.

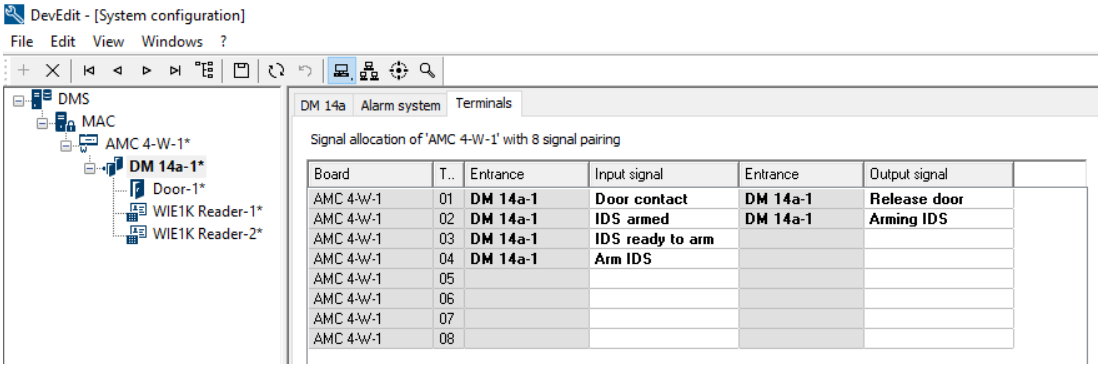
Signal	Entrée/ Sortie	Description
IDS armé	Entrée	L'IDS est armé pour cette zone d'intrusion.
IDS prêt pour armement	Entrée	Aucun point d'IDS n'est dans un état d'erreur (ouvert ou non prêt).
Armer IDS	Entrée	Demande d'armement de l'IDS.
Bouton de « demande de sortie » (REX)	Entrée	
Capteur de pêne	Entrée	Un capteur surveille le pêne de la porte.
Autosurveillance	Entrée	Une tentative de sabotage a été détectée.
Supprimer l'alarme d'ouverture non autorisée	Entrée	Supprimer l'alarme pendant un nombre configuré de secondes supplémentaires si un signal REX a été donné par un détecteur de mouvement. Voir la fonction de réglage REX pour plus de détails.
Débloquer la porte	Sortie	Activez le cycle de la porte pour déverrouiller et reverrouiller, pour autoriser l'accès.
Armement IDS	Sortie	Armer ou désarmer l'IDS, selon son état actuel (bascule).
Connexion caméra	Sortie	Activer une caméra connectée à l'entrée.

Signal	Entrée/ Sortie	Description
Le temps max. d'ouverture de la porte s'est écoulé ou **Sécurité de la porte compromise**	Sortie	La porte est maintenue ouverte ou le système suspecte une infraction à la sécurité à la porte.

Procédure d'affectation de signaux aux terminaux

1. Ouvrez le 3ème onglet, **Terminaux**.

– Les terminaux du contrôleur de porte de cette entrée, ainsi que toutes les cartes d'extension qu'il peut avoir, sont affichées dans un tableau.



2. Sélectionnez la ligne correspondant au terminal que vous souhaitez utiliser pour le signal d'entrée.
3. Dans la cellule correspondante, dans la colonne **Signal d'entrée**, sélectionnez le signal souhaité dans la liste déroulante. Notez que seuls les signaux non attribués jusqu'à présent apparaissent dans la liste.
4. Répétez les étapes précédentes pour ajouter tout autre signal d'entrée dont vous avez besoin pour cette entrée.
5. Répétez la procédure aussi souvent que nécessaire pour ajouter à la colonne **Signal de sortie** tous les signaux de sortie dont vous avez besoin.

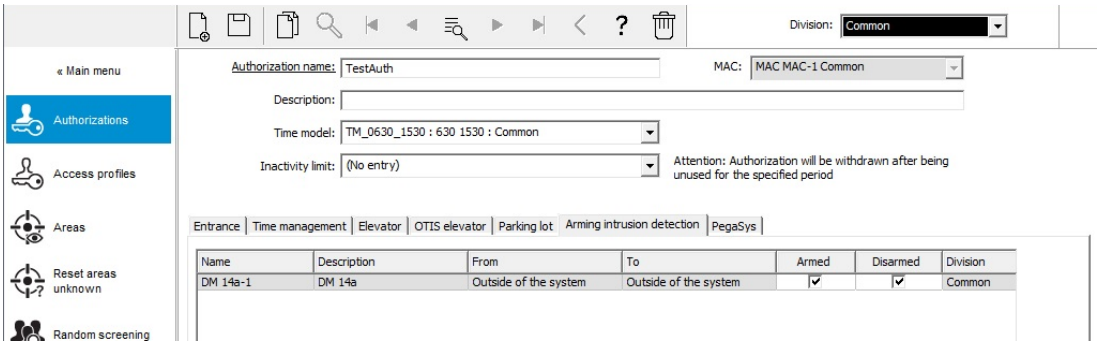
Définition des autorisations pour armer et désarmer les entrées DM14

Une fois que vous avez créé une entrée DM14 dans l'éditeur de dispositif, l'entrée sera disponible pour être incluse dans les autorisations d'accès.

1. Dans le gestionnaire de dialogue, accédez à :

– Menu principal > **Données système** > onglet **Autorisations** > : **Détection d'intrusion d'armement**

2. Chargez une autorisation d'accès existante dans la boîte de dialogue ou cliquez sur  (Nouveau) pour en créer une nouvelle.
3. Localisez l'entrée DM14 souhaitée dans la liste et cochez les cases **Armé** et/ou **Désarmé**.

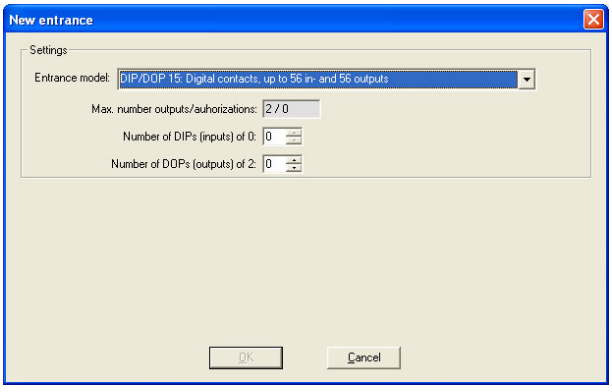


4. Cliquez sur (Enregistrer) pour enregistrer l'autorisation d'accès avec les autorisations sélectionnées.
5. Attribuez cette autorisation d'accès aux détenteurs de carte qui doivent gérer les entrées DM 14.

16.5.3 DIP et DOP (DM15)

Création du modèle d'entrée 15 :

Ce modèle d'entrée offre des signaux d'entrée et de sortie indépendants.



Si toutes les interfaces de lecteur sont prises, seul ce modèle d'entrée devient disponible.
Vous pouvez définir ce modèle d'entrée tant qu'il y a au moins deux signaux libres.
Aux AMC équipés d'ascenseurs (modèle 07) ou de parkings (modèle 05c), il n'est pas possible d'attribuer ce modèle d'entrée.

Modèle d'entrée 15

Signaux possibles : ces noms par défaut peuvent être remplacés.

Signal d'entrée	Signal de sortie
DIP	DOP
DIP-1	DOP-1
...	...
DIP-63	DOP-63

Contrairement à d'autres modèles de portes, le modèle d'entrée 15 gère les entrées et sorties d'un contrôleur qui sont encore libres, et les place en tant qu'entrées génériques et sorties sans tension à la disposition de l'ensemble du système.
Contrairement aux contacts de sortie d'autres modèles de portes, ceux du modèle d'entrée 15 peuvent être consultés individuellement dans l'éditeur de dispositif.

Rétablissement des DOP après les redémarrages

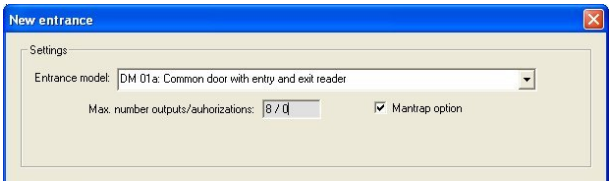
Lorsqu'un MAC ou un AMC est redémarré, il réinitialise normalement les valeurs d'état de ses DOP subordonnés à la valeur par défaut 0 (zéro).

Pour garantir qu'un redémarrage réinitialise toujours un DOP au dernier état qui lui a été assigné manuellement, sélectionnez le DOP dans l'arborescence de dispositif et cochez la case **Conserver l'état** dans la fenêtre principale.

16.5.4 Modèles de portes de contrôles de sas

Création d'un contrôle de sas

Les modèles d'entrée 01 et 03 peuvent être utilisés comme « contrôles de sas » pour le choix des accès d'un détenteur de carte. Utilisez la case à cocher **Option de contrôle de sas** pour rendre disponibles les signaux supplémentaires nécessaires.



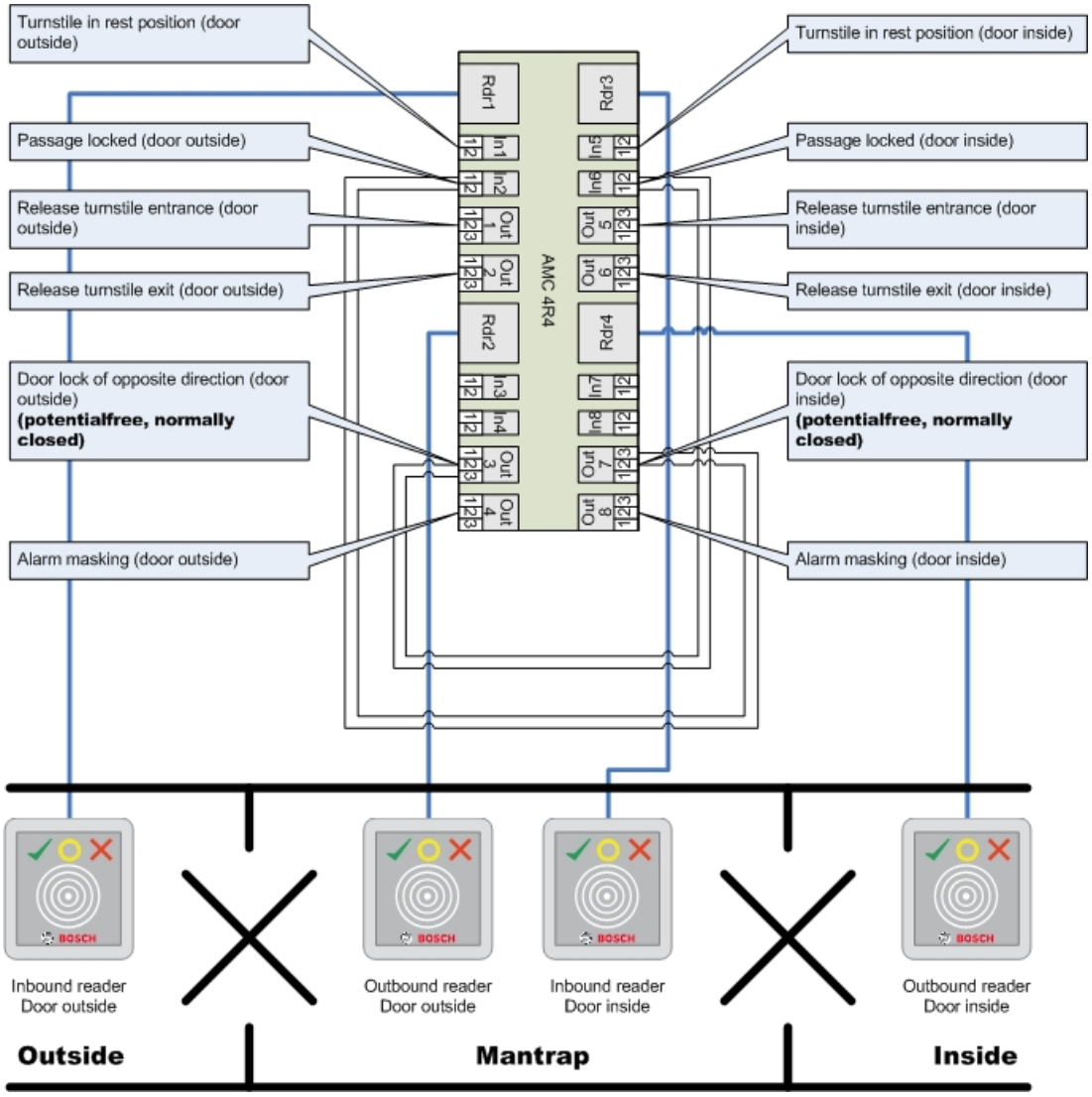
Vous pouvez combiner tous les types de modèles 01 et 03, mais vous devez définir cette option sur les deux entrées appartenant au contrôle de sas.

Outre les affectations de signaux habituelles pour le modèle de porte, l'option de contrôle de sas nécessite des affectations de signaux supplémentaires qui lui sont propres.

Exemple : contrôle de sas sur un contrôleur

Les tourniquets sont le moyen le plus habituel d'effectuer un comptage individuel des accès de détenteur de carte. Les exemples suivants sont donc basés sur le modèle de porte 3a (tourniquet pivotant avec lecteur d'entrée et de sortie).

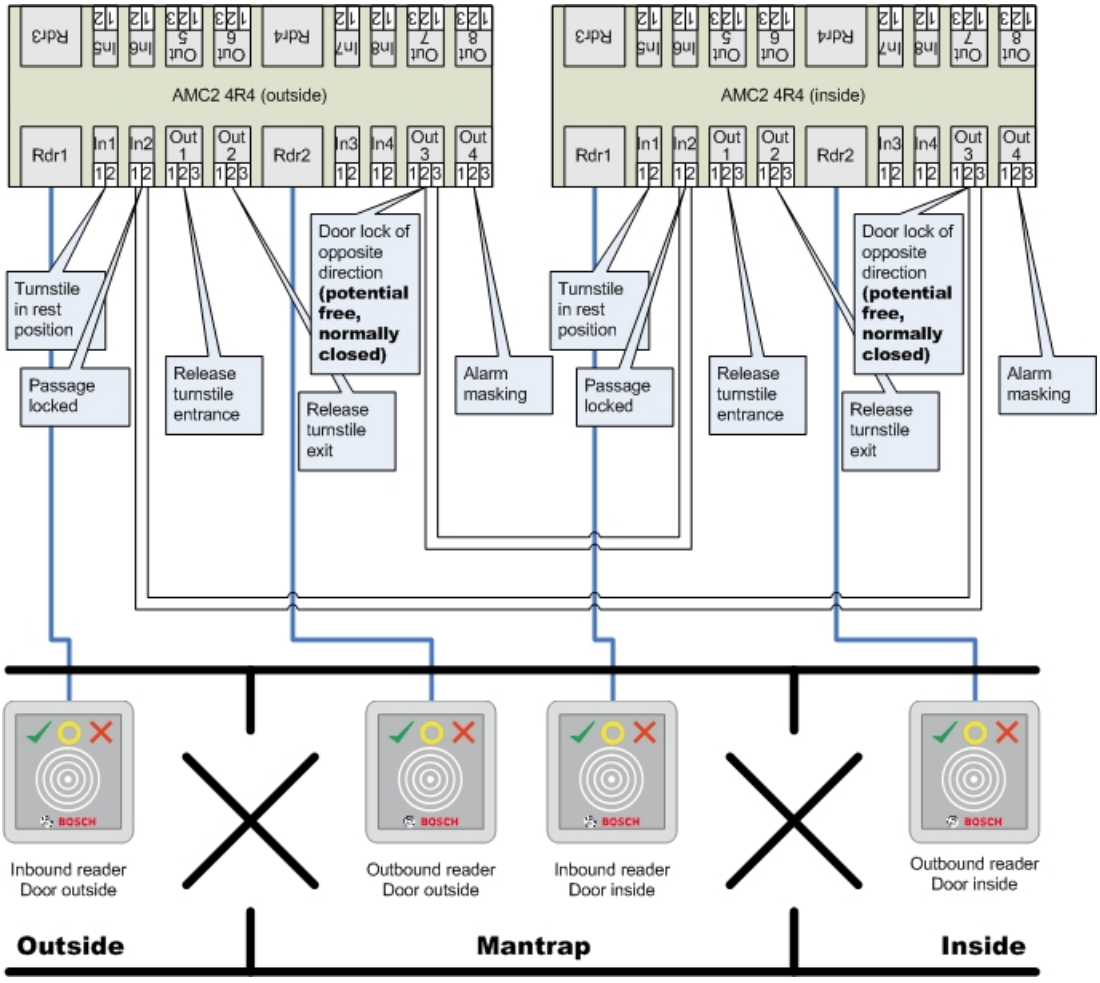
Configuration de contrôle de sas avec deux tourniquets (DM 03a) :



Les connexions aux verrouillages de porte pour la direction opposée garantissent l'ouverture d'un seul tourniquet à la fois.

Remarque!
Les signaux de sortie (Sortie) 3 et 7 doivent être configurés sans potentiel (mode sec)
Le signal « Verrou de porte de direction opposée » est actif sur 0. Il doit être utilisé pour les sorties 3 et 7 « normalement fermées ».

Exemple : contrôle de sas sur deux contrôleurs
Configuration de contrôle de sas avec deux tourniquets (DM 03a) répartis sur deux contrôleurs :



Les connexions aux verrouillages de porte pour la direction opposée garantissent l'ouverture d'un seul tourniquet à la fois.

Remarque!
Le signal de sortie (Sortie) 3 doit être configuré sans potentiel (mode sec)
Le signal « Verrou de porte de direction opposée » est actif sur 0. Il doit être utilisé pour la sortie 3 « normalement fermée ».

16.6 Portes

Onglet : Porte

Paramètre	Valeurs possibles	Description
Nom	Alphanumérique, jusqu'à 16 caractères	La valeur par défaut générée peut éventuellement être remplacée par un nom unique.
Description	Alphanumérique, jusqu'à 255 caractères	
Division	La division par défaut est « Commun »	Pertinent uniquement si la fonction **Divisions** est sous licence.
Uniquement pour les modèles de porte 01 et 03 si un contrôle de sas est configuré :		

Option de contrôle de sas	0 = désactivé (la case à cocher est désactivée) 1 = activé (la case est cochée)	Un contrôle de sas existe lorsque deux portes combinées utilisent le modèle de porte 01 ou 03. Activez l'option de contrôle de sas pour **les deux** portes. Les portes nécessiteront également un câblage physique spécial.

Onglet : Options

Paramètre	**Valeurs possibles**	**Remarques**
Générer un message pour ouvert/fermé	0 = la case à cocher est désactivée 1 = la case est cochée.	0 = Aucun message n'est généré lorsque la porte est ouverte (à un angle par rapport au cadre de la porte) ou fermée (entièrement verrouillée dans le cadre de la porte). 1 = les messages correspondants sont générés dans le journal des événements.
Porte réglée sur manuel	0 = la case à cocher est désactivée 1 = la case est cochée.	0 = la porte est en mode normal (par défaut), c'est-à-dire qu'elle est soumise au contrôle d'accès par l'ensemble du système. 1 = la porte est exclue du système de contrôle d'accès. La porte n'est pas contrôlée et ne génère pas de messages. Elle ne peut être verrouillée ou déverrouillée que manuellement. Tous les autres paramètres de cette porte sont désactivés. Ce paramètre doit être défini séparément pour la porte et le lecteur.
Mode de la porte	0 = La porte est en mode normal 1 = La porte est déverrouillée 2 = La porte est déverrouillée suivant un modèle horaire 3 = La porte est ouverte suivant un modèle horaire après premier passage 5 = La porte est bloquée en permanence 6 = La porte est bloquée suivant un modèle horaire	0 = mode normal (par défaut) - la porte sera bloquée ou débloquée en fonction des droits d'accès des informations d'identification. 1 = déverrouillage pendant une période prolongée - le contrôle d'accès est suspendu pendant la période. 2 = déverrouillage pendant une période définie par le modèle horaire. Le contrôle d'accès est suspendu pendant la période. 3 = verrouillée tant que le modèle horaire est actif jusqu'à ce que la première personne ait accès - puis ouverte tant que le modèle horaire est actif. 5 = bloquée (exclue du système de contrôle d'accès) jusqu'au déblocage manuel. 6 = bloquée (exclue du système de contrôle d'accès) tant que le modèle horaire est actif - il n'y a pas de commande de porte, la porte ne peut pas être utilisée tant que le modèle horaire est actif.

Modèle horaire	l'un des modèles horaires disponibles	Modèle horaire des heures d'ouverture de porte. Si les modes de porte 2, 3, 4, 6 et 7 sont sélectionnés, la zone de liste des modèles horaires est disponible. La sélection d'un modèle horaire est requise.
Durée max. de l'impulsion transmise à la gâche de porte :	0 - 9999	Durée maximale du signal de déverrouillage. Unité 1/10s. Valeurs par défaut : 50 pour les portes, 10 pour les portes pivotantes (modèle de porte 03) et 200 pour les barrières (modèles de porte 05c ou 09c).
Durée min. de l'impulsion transmise à la gâche de porte :	0 - 9999	Durée minimale du signal de déverrouillage en 1/10s. Par défaut : 10.
Suppression d'alarme préfixée	0 - 9999	Suppression de l'alarme supplémentaire **avant** l'impulsion à la gâche de porte. (`$PARAMETER_WAITEMA`) Dans de très rares cas où une gâche de porte peut réagir plus lentement qu'une alarme d'intrusion, il est possible de supprimer temporairement l'alarme avant d'envoyer le signal de déverrouillage à la porte. Unité : 1/10 s. Par défaut : 0. La valeur 20, c'est-à-dire 2 s, est normalement suffisante même pour les portes très lentes.
Suppression d'alarme comportant un suffixe	0 - 9999	Suppression de l'alarme supplémentaire **après** l'impulsion à la gâche de porte. (`$PARAMETER_OPENINRT`) Une fois l'impulsion transmise à la gâche de porte (le signal de déverrouillage) terminée, la porte peut être ouverte dans ce laps de temps, sans déclencher d'alarme. Unité : 1/10s. Par défaut : 0.
Mode de sonnerie de porte	Entrée de zone de liste	0 = le bouton REX (demande de sortie est désactivé après l'heure d'activation 1 = le bouton REX (demande de sortie) est désactivé immédiatement (= par défaut)
Capteur de cadre de porte présent	0 = désactivé (la case à cocher est désactivée) 1 = activé (la case est cochée)	0 = la porte n'a pas de contact de cadre 1 = la porte a un contact de cadre. Un contact fermé signifie généralement que la porte est fermée. (= par défaut)

Capteur de pêne présent	0 = désactivé (la case à cocher est désactivée) 1 = activé (la case est cochée)	0 (par défaut) = la porte n'a pas de capteur de pêne 1 = la porte a un capteur de pêne. Un message est émis lorsque la porte est verrouillée ou déverrouillée.
Temps d'ouverture de porte prolongé (personnes handicapées)	0 = désactivé (la case à cocher est désactivée) 1 = activé (la case est cochée)	0 = Le signal de déverrouillage a une durée standard, qui est réglée sur le paramètre de **porte** « Durée max. d'activation du verrouillage », c'est-à-dire la durée de l'impulsion transmise à la gâche de la porte. 1 (par défaut) = la durée du signal de déverrouillage est multipliée par le facteur définie au paramètre **MAC** « **Facteur de temps pour les personnes handicapées** » (onglet : **Paramètres d'accès globaux**). La valeur 0 pour ce paramètre MAC désactive les temps d'ouverture prolongés de la porte.

Onglet : Sécurité de la porte

Paramètre	**Valeurs possibles**	**Remarques**
Générer un message pour « Ouverture de porte forcée »	0 = désactivé (la case à cocher est désactivée) 1 = activé (la case est cochée)	0 = pas de message d'intrusion. Ceci est utile si une porte peut être ouverte librement de l'intérieur. 1 = (par défaut) Lors d'une ouverture non autorisée, un message sera émis, suivi d'un autre message lorsque la porte se fermera.
Générer un message pour « Porte maintenue ouverte » au bout de :	0 - 9999	Si la porte reste ouverte après ce laps de temps, un message est émis, pour avertir que la porte est restée ouverte trop longtemps. Unité : 1/10s. Par défaut : 300. 0 = pas de délai, pas de message.
Extension de suppression d'alarme pour « Ouverture de porte forcée »	0 - 9999	Utilisé dans la fonction « Réglage REX » : Unité = 1/10s. Par défaut 0. Après un signal REX d'un détecteur de mouvement, si la porte se referme dans ce laps de temps alors le message habituel `Unauthorized opening of door N` est remplacé par le message : `Door N opened (in alarm suppression mode)` où N est le numéro de la porte.
Générer une alarme locale pour « Ouverture de porte forcée »	0 = désactivé (la case à cocher est désactivée) 1 = activé (la case est cochée)	Condition préalable : la case à cocher **Générer un message pour « Ouverture de porte forcée »** dans cette boîte de dialogue est activée (voir ci-dessus).

		0 = (par défaut) les lecteurs connectés à cette porte ne déclenchent pas d'alarme locale. 1 = les lecteurs connectés à cette porte déclenchent une alarme locale si l'ouverture de la porte est forcée.
Générer une alarme locale pour « Porte maintenue ouverte » après :	0 - 9999	Si la porte reste ouverte après ce laps de temps, les lecteurs connectés à cette porte déclenchent une alarme locale. Unité : 1/10s. 0 = (par défaut) pas d'alarme locale.

16.6.1 Réglage REX

Introduction

Aux entrées où il n'y a aucun risque pour la sécurité à ouvrir une porte manuellement de l'intérieur, un détecteur de mouvement remplace souvent un bouton REX, pour déverrouiller la porte. Pour ce scénario courant, ACS fournit un moyen simple de prolonger la durée du signal REX du détecteur de mouvement, tout en réglant (suspendant) simultanément l'alarme `Door forced open` .

Cette fonction est connue sous le nom de « Réglage REX ».

Lorsque la fonction est en fonctionnement, les titulaires de carte qui franchissent la porte pendant la durée du réglage génèrent l'événement d'accès `Door N opened (in alarm suppression mode)` plutôt que l'événement `Unauthorized opening of door N`.

Remarque!

Réglage REX en combinaison avec des systèmes de détection d'intrusion armés

La fonction Réglage REX suspend les alarmes pendant la durée définie au paramètre : Éditeur de dispositif > ... > **Porte** > onglet : **Sécurité de porte** > **Extension de suppression d'alarme pour « Ouverture forcée de porte »**

indépendamment du fait que cette porte soit actuellement armée dans le cadre d'un système d'alarme antivol.

Conditions préalables

- Portes configurées des types suivants : 01a, 01b, 01c, 03a, 03b, 03c, 10a, 10b, 10e, 14a, 14b
- La porte physique est équipée d'un détecteur de mouvement, plutôt que d'un bouton REX, pour déverrouiller la porte. Définissez la durée du signal du détecteur de mouvement sur au moins 1 seconde.

Chemin d'accès à la boîte de dialogue

- **Menu principal** >**Configuration** > **Données du dispositif**

Procédure

1. Dans l'éditeur de dispositif, naviguez jusqu'à l'entrée souhaitée (nœud enfant direct d'un contrôleur de porte).
2. Sous l'onglet **Terminaux** de l'entrée, créez un nouveau signal d'entrée de type : `Suppress alarm from unauthorized opening`

3. Cliquez sur  (Enregistrer) pour enregistrer les modifications.
4. Sélectionnez la porte qui se trouve dans l'entrée souhaitée
5. Sous l'onglet **Sécurité de porte** de la porte, définissez une valeur pour le paramètre **Extension de suppression d'alarme pour « Ouverture de porte forcée »**
- La valeur est en dixièmes de seconde.
- La valeur par défaut est `0`. Autrement dit, par défaut, il n'y a pas d'extension de suppression d'alarme après que le titulaire de la carte a quitté la zone sensible du détecteur de mouvement.

6. Cliquez sur  (Enregistrer) pour enregistrer les modifications.

16.6.2 Configuration des portes pour déclencher des alarmes locales

Introduction

Pour les états de porte suivants, l'ACS offre un moyen de faire retentir les alarmes dans tous les lecteurs connectés à la porte.

État	Réponse d'alarme locale
Ouverture de porte forcée	L'alarme retentit pendant 17 secondes ou jusqu'à ce que la porte se ferme.
Porte maintenue ouverte	L'alarme retentit jusqu'à ce que la porte se ferme.

Conditions préalables

- Les lecteurs utilisent le protocole OSDP ou Wiegand
- Des sirènes d'alarme sont présentes dans les lecteurs et connectées électriquement au contrôleur de porte.
- Firmware AMC 02.38 ou version ultérieure.

Les types de lecteurs suivants ne sont **pas** pris en charge :

- Lecteurs IDEMIA
- Lecteurs Suprema avec protocole Wiegand
- Lecteurs LBUS
- Lecteurs BG900

Chemin d'accès à la boîte de dialogue

- **Menu principal** >**Configuration** > **Données du dispositif**

Procédure d'ouverture forcée de la porte

1. Dans l'arborescence des périphériques, sélectionnez la porte que vous souhaitez configurer.
2. Dans l'onglet **Sécurité de la porte**, cochez la case **Générer un message pour « Ouverture de porte forcée »**.
3. Cochez la case **Générer une alarme locale pour « Ouverture de porte forcée »** **.** La valeur par défaut est `0` (la case à cocher est vide). Cela signifie qu'aucune alarme locale ne retentit par défaut.
4. Cliquez sur  (Enregistrer) pour enregistrer les modifications.

Procédure de maintien de la porte ouverte

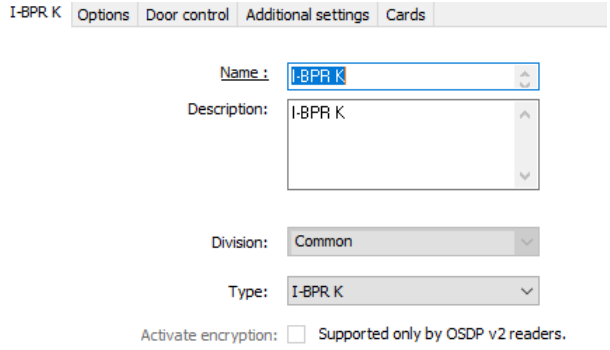
1. Dans l'arborescence des périphériques, sélectionnez la porte que vous souhaitez configurer.
2. Dans l'onglet **Sécurité de la porte**, définissez une valeur différente de zéro pour le paramètre
   Générer une alarme locale pour « Porte maintenue ouverte » après :

– La valeur est en dixièmes de seconde.
– La valeur par défaut est `0`. Cela signifie qu'aucune alarme locale ne retentit par défaut.

3. Cliquez sur (Enregistrer) pour enregistrer les modifications.

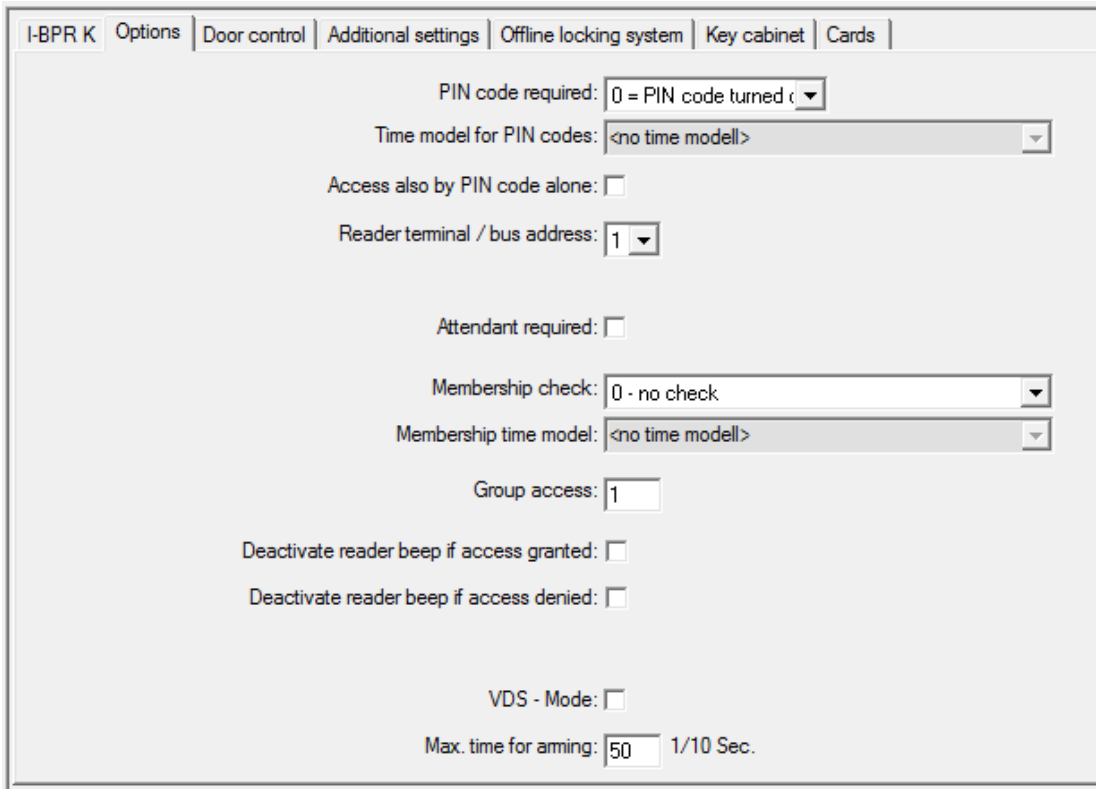
16.7 Lecteurs

Configuration d'un lecteur : paramètres généraux



Paramètre	Valeurs possibles	Description
Nom du lecteur	alphanumérique, limité à entre 1 et 16 caractères	La valeur par défaut peut être remplacée par un nom unique.
Description lecteur	alphanumérique : 0 à 255 caractères	Description en texte libre.
Division	Division « Commune » par défaut.	Uniquement pertinent si les divisions sont autorisées et utilisées.
Type	alphanumérique, limité à entre 1 et 16 caractères	Type de lecteur ou groupe de lecteurs

Configuration d'un lecteur : options



Paramètre	Valeurs possibles	Description
Code PIN requis	0 = code PIN désactivé - aucune saisie nécessaire (par défaut) 1 = code PIN activé - saisie toujours nécessaire 2 = code PIN contrôlé par modèle horaire - saisie uniquement si en dehors du modèle horaire	Ce champ n'est activé que si le lecteur dispose d'un périphérique d'entrée. Notez que les vérifications sur la carte, telles que ses autorisations et sa séquence d'accès (si activée), ont priorité sur l'exactitude du code PIN.
Modèle horaire pour les codes PIN	l'un des modèles horaires disponibles	La sélection d'un modèle horaire ici est obligatoire si le paramètre **Code PIN requis** est défini sur 2.
Accéder également par code PIN seul	0 = désactivé (la case à cocher est désactivée) 1 = activé (la case est cochée)	Détermine si ce lecteur peut également autoriser l'accès basé uniquement sur un code PIN, c'est-à-dire sans carte, si le système de contrôle d'accès est ainsi configuré. Voir
Adresse terminal/bus du lecteur	1 - 4	Pour AMC 4W : numérotation correspondant aux interfaces Wiegand.

		Pour AMC 4R4 : numérotation comme l'adresse par cavalier du lecteur.
Assistant requis	0 = désactivé (la case à cocher est désactivée) 1 = activé (la case est cochée)	0 = le visiteur n'a pas besoin d'assistant accompagnateur (par défaut) 1 = l'assistant accompagnateur doit également utiliser le lecteur
Vérification d'adhésion	Entrée de zone de liste	La vérification d'adhésion est généralement utilisée dans les premières phases avant la mise en service d'un système de contrôle d'accès. Ici, l'accès est accordé en fonction de l'ID d'entreprise générique des informations d'identification plutôt que de l'ID personnel unique. **IMPORTANT** La vérification d'adhésion ne fonctionne qu'avec les informations d'identification physiques où les définitions de carte sont prédéfinies sur le système (fond gris), et **non** avec des définitions personnalisées ou des informations d'identification biométriques. **0 - aucune vérification** La vérification de l'adhésion est désactivée, mais la carte est vérifiée pour les autorisations comme d'habitude (par défaut) **1 - vérification** La carte est vérifiée uniquement pour l'ID d'entreprise, c'est-à-dire pour l'adhésion du système. **2 - selon le modèle horaire** La carte est vérifiée pour l'ID d'entreprise (adhésion), mais uniquement pendant la période définie dans le modèle horaire d'adhésion.
Modèle horaire d'adhésion	l'un des modèles horaires disponibles	Le modèle horaire active/désactive la vérification d'adhésion. La sélection d'un modèle horaire est obligatoire pour l'option 2 **Vérification d'adhésion**.
Accès groupe	1 - 10	**Pour les lecteurs avec clavier :** Nombre minimum de cartes valides qui doivent être présentées au lecteur de cartes avant l'ouverture de la porte. Le groupe peut comprendre plus de cartes que ce nombre ; auquel cas la touche ENTRÉE/# est utilisée pour signaler que le groupe est complet. Ensuite, la porte est ouverte.

		Pour les lecteurs sans clavier : Nombre exact de cartes valides qui doivent être présentées au lecteur de cartes avant l'ouverture de la porte. La valeur par défaut est 1.
Désactiver le bip du lecteur si accès accordé	0 = désactivé (la case à cocher est désactivée) 1 = activé (la case est cochée)	Si cette option est activée (1), le lecteur reste silencieux si un utilisateur autorisé a accès.
Désactiver le bip du lecteur si accès non accordé	0 = désactivé (la case à cocher est désactivée) 1 = activé (la case est cochée)	Si cette option est activée (1), le lecteur reste silencieux lorsqu'un utilisateur non autorisé se voit refuser l'accès.
 Les fonctions « Désactiver le bip du lecteur » dépendent du micrologiciel du lecteur respectif. Le micrologiciel de certains lecteurs peut ne pas prendre en charge cette fonction.		
Mode VDS	0 = désactivé (la case à cocher est désactivée) 1 = activé (la case est cochée)	Si activé (1), la signalisation du lecteur est désactivée.
Durée max. d'armement	1 à 100 [1/sec]	Durée maximum pour le retour d'information de la centrale intrusion indiquant que l'armement est terminé.

Réseau et modes de fonctionnement

Cet onglet n'est affiché que pour les lecteurs biométriques en réseau.

Les **Modèles** sont des modèles stockés. Il peut s'agir de données de carte ou de données biométriques.

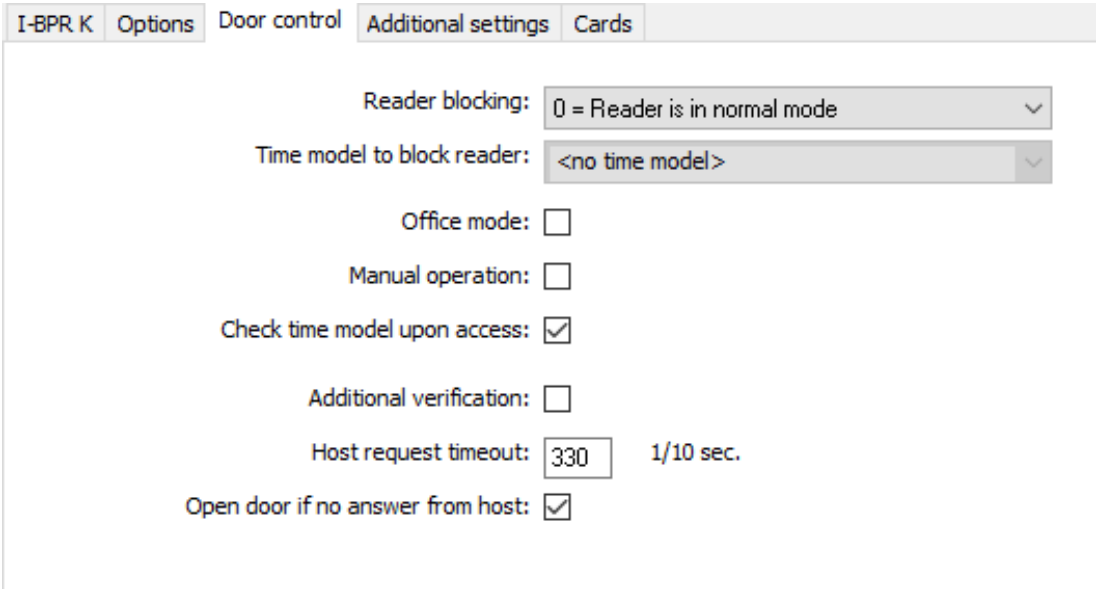
Les modèles peuvent être stockés à la fois sur les dispositifs au-dessus du lecteur dans l'arborescence de dispositif et sur le lecteur lui-même. Les données du lecteur sont régulièrement mises à jour par les dispositifs situés au-dessus.

Le lecteur peut être configuré pour utiliser ses propres modèles lors de la prise de décisions d'accès, ou uniquement pour utiliser les modèles des dispositifs situés au-dessus.

Paramètre	**Description**
Adresse IP :	Adresse IP de ce lecteur en réseau
Port :	Le port par défaut est `51211`

Paramètre	Description
Modèles sur le serveur	
Carte seulement	Le lecteur lit uniquement les données de la carte. Il les authentifie par rapport aux données du système global.
Carte et empreintes digitales	Le lecteur lit à la fois les données de la carte et les données d'empreintes digitales. Il les authentifie par rapport aux données du système global.
Modèles sur le dispositif	
Vérification dépendant de la personne	Le lecteur permet aux paramètres du détenteur de carte individuel de déterminer le **Mode d'identification** utilisé. Les données personnelles offrent les options suivantes : – Empreinte digitale seulement – Carte seulement – Carte et empreintes digitales Celles-ci sont décrites plus loin dans ce tableau.
Empreinte digitale seulement	Le lecteur lit uniquement les données d'empreintes digitales. Il les authentifie par rapport à ses propres données stockées.
Carte seulement	Le lecteur lit uniquement les données de la carte. Il les authentifie par rapport à ses propres données stockées.
Carte et empreintes digitales	Le lecteur lit à la fois les données de la carte et les données d'empreintes digitales. Il les authentifie par rapport à ses propres données stockées.
Carte ou empreinte digitale	Le lecteur lit les données de la carte ou les données d'empreintes digitales, selon ce que le détenteur de carte propose en premier. Il les authentifie par rapport à ses propres données stockées.

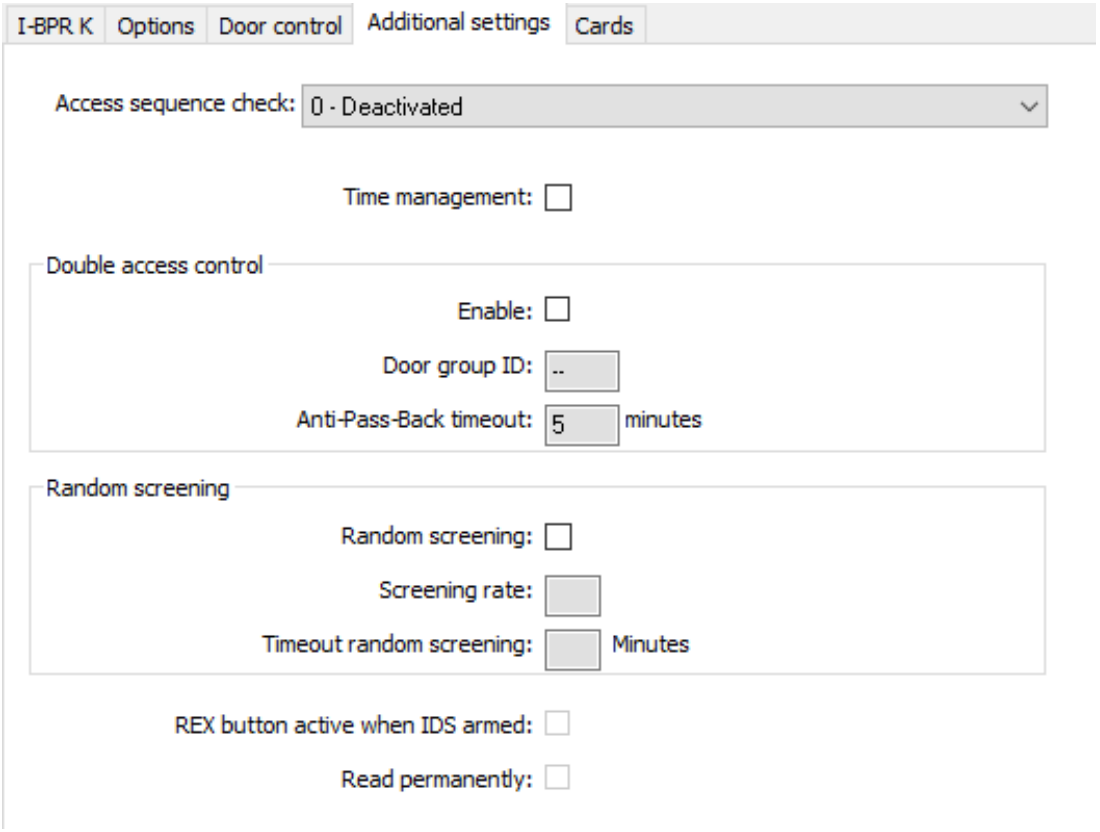
Configuration d'un lecteur : commande de porte



Paramètre	Valeurs possibles	Remarques
Blocage du lecteur	Entrée de zone de liste	0 = Lecteur en mode normal - pas de blocage (= par défaut) 1 = Le lecteur est bloqué en permanence - blocage permanent 2 = Le lecteur est bloqué selon un modèle horaire - blocage selon le modèle horaire défini avec le *Modèle horaire pour bloquer le lecteur*
Modèle horaire pour bloquer le lecteur	l'un des modèles temporels définis sur le système.	Bloque le lecteur en fonction du modèle horaire sélectionné.
Mode Bureau	0 = désactivé (la case à cocher est désactivée) 1 = activé (la case est cochée)	Permet à ce lecteur de définir une entrée Mode Bureau. Le lecteur doit être doté d'un clavier. Lorsque ce paramètre est activé, un titulaire de carte dûment autorisé active et désactive le mode Bureau en appuyant sur la touche 3 avant de présenter sa carte. Voir *Autoriser des personnes à définir le mode Bureau, page 209*
Fonctionnement manuel	0 = désactivé (la case à cocher est désactivée) 1 = activé (la case est cochée)	0 = lecteur en mode normal (= par défaut) 1 = le lecteur est effectivement retiré du système de contrôle d'accès, c'est-à-dire « hors service ».

		Aucune commande n'est reçue. Tous les autres paramètres de ce lecteur sont désactivés. Le paramètre doit être défini indépendamment pour le lecteur et la porte.
Vérifier les modèles horaires par rapport à l'accès	0 = désactivé (la case à cocher est désactivée) 1 = activé (la case est cochée)	0 = Les modèles horaires ne seront pas vérifiés. Il n'y a aucune restriction horaire pour l'accès. 1 = Si le détenteur de la carte se voit attribuer un modèle horaire, soit directement, soit sous forme d'autorisation de zone-temps, le modèle horaire sera vérifié. (= par défaut)
Vérification supplémentaire	0 = désactivé (la case à cocher est désactivée) 1 = activé (la case est cochée)	0 = la vérification de l'hôte n'est pas requise 1 = la vérification de l'hôte est requise (par défaut) (**IMPORTANT** : L'activation de cette option est requise pour une vérification vidéo supplémentaire par l'opérateur d'un système de contrôle d'accès Bosch BVMS ou Bosch).
Expiration de la demande d'hôte	0 = désactivé	0 = AMC fonctionne sans vérification de l'hôte (ne fonctionne pas avec le *Changement de zone* ou le *Comptage de personnes*). Cette commande n'est active que si la vérification de l'hôte est désactivée (0) et que si l'option *Ouvrir la porte si l'hôte ne répond pas* est activée (1) 1 à 9999 x 1/10 de seconde. (Par défaut = 330 = 33 secondes). Le lecteur demande une confirmation au système de contrôle d'accès. Si la confirmation n'est pas reçue dans ce délai, l'AMC vérifie le paramètre **Ouvrir la porte si l'hôte ne répond pas** et accorde ou refuse l'accès en conséquence.
Ouvrir la porte si l'hôte ne répond pas	0 = désactivé (la case à cocher est désactivée) 1 = activé (par défaut) (la case est cochée)	Cette commande n'est active que si le paramètre **Vérification de l'hôte** est défini. 0 = n'ouvre pas la porte si le système hôte ne parvient pas à confirmer avant l'expiration du délai. 1 (par défaut) = ouvre la porte après l'expiration du délai si le système hôte ne parvient pas à confirmer avant l'expiration du délai.

Configuration d'un lecteur : paramètres supplémentaires

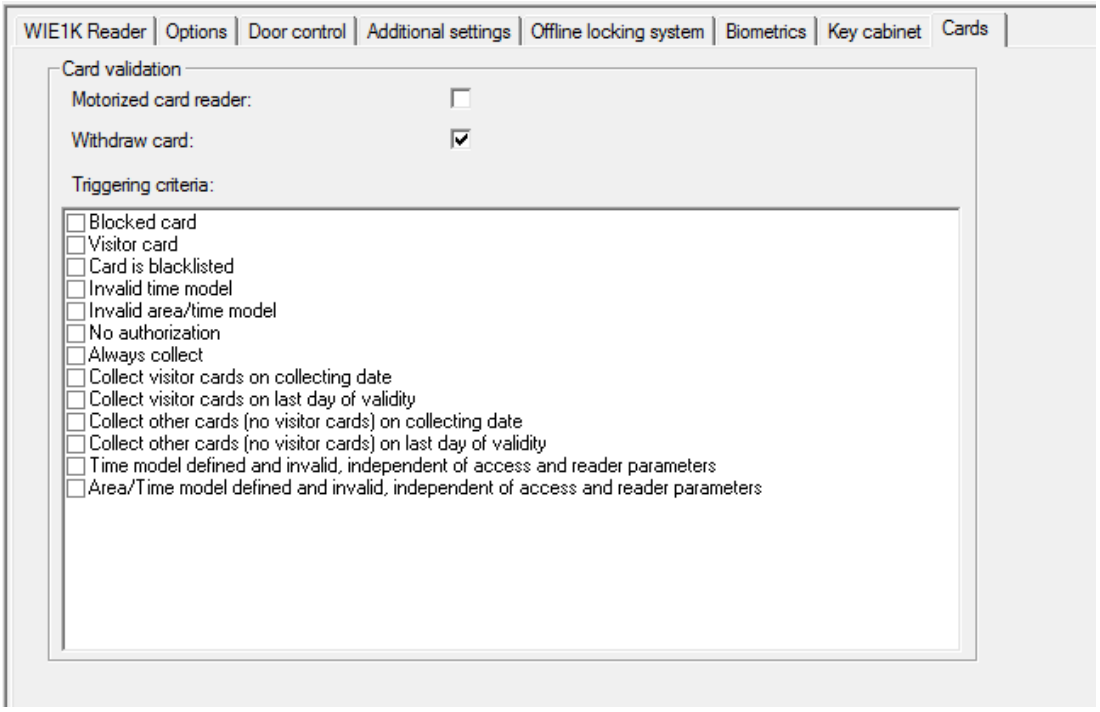


Paramètre	Valeurs possibles	Remarques
Vérification séquentielle d'accès	0 - Désactivé 1 - Activé ; désactiver sur défaillance du LAC 2 - Activé ; laisser actif sur défaillance du LAC 3 - Activé ; utiliser strictement la vérification séquentielle même lors de défaillances du LAC (note : mettre à jour l'emplacement de la personne manuellement)	0 = le lecteur ne participe pas à la vérification de la séquence d'accès (= par défaut) Une vérification de la séquence activée peut gérer les personnes qui sont définies comme INCONNU de la manière suivante : 1 = La première lecture de la carte sera interrompue sans vérification de l'emplacement. Tous les contrôleurs doivent être en ligne. 2 = La première lecture de la carte sera interrompue sans vérification de l'emplacement. 3 = La vérification de l'emplacement sera interrompue pour chaque lecture de la carte pendant un dysfonctionnement du LAC.
		

Une commande MAC permet d'activer ou de désactiver toutes les vérifications de séquence d'accès en général. Pour désactiver la vérification de séquence d'accès pour une période, une valeur est donnée en minutes avec un maximum de 2 880 (= 48 heures). La valeur « 0 » désactive complètement la vérification de la séquence d'accès. **Remarque :** Cette commande peut modifier la vérification de la séquence d'accès uniquement pour les lecteurs où le paramètre **Activer la séquence d'accès** est défini. Elle ne désactive/n'active pas la vérification de la séquence d'accès pour *tous* les lecteurs.		
Gestion du temps	0 = désactivé (la case à cocher est désactivée) 1 = activé (la case est cochée)	Si cette option est sélectionnée, le système de contrôle d'accès collecte des données pour la gestion du temps et des présences.
Double contrôle d'accès (contrôle anti-retour)		
Activer	0 = désactivé (la case à cocher est désactivée) 1 = activé (la case est cochée)	0 = sans contrôle d'accès double (= par défaut) 1 = avec contrôle d'accès double Dans le laps de temps défini par le paramètre **Durée**, ce lecteur et les autres lecteurs du groupe ne peuvent pas être utilisés avec la même carte. Si ce paramètre est activé, un identifiant de groupe de portes doit être utilisé, même si un seul lecteur est utilisé.
Identifiant du groupe de portes	Lettres A - Z et a - z, et "-" 2 caractères	Les lecteurs peuvent être regroupés à l'aide d'un identifiant de groupe de portes. La présentation d'une carte sur un lecteur bloquera les réservations ultérieures sur tous les lecteurs du groupe de portes (par défaut = **--**) jusqu'à ce que le délai soit écoulé.
Délai d'attente anti-retour	1 - 120	Le lecteur peut être utilisé avec la même carte une fois ce laps de temps écoulé. Dès que la carte est utilisée sur un lecteur extérieur au groupe, le blocage est levé immédiatement. Les valeurs sont en minutes - par défaut = 5.
Surveillance aléatoire	0 = désactivé (la case à cocher est désactivée) 1 = activé (la case est cochée)	0 = aucune surveillance 1 = la surveillance en fonction du facteur n'aura aucune admission jusqu'à ce qu'il soit débloqué par le dialogue **Blocage**.

Taux de surveillance	1 - 100	Pourcentage de surveillance aléatoire pour une vérification prolongée. Disponible si la surveillance aléatoire est activée.
Dépassement du délai de surveillance aléatoire	1 - 120	L'utilisateur est soumis à la surveillance aléatoire dans le délai défini. Les valeurs sont en minutes - par défaut = 5.
Bouton REX actif quand l'IDS est armé	0 = désactivé (la case à cocher est désactivée) 1 = activé (la case est cochée)	Pour **DM10** et **DM14** uniquement : les boutons-poussoirs REX sont désactivés par défaut lorsque l'IDS est armé. Cela rendrait impossible la sortie de la zone surveillée. Ce nouveau paramètre de lecteur active le bouton REX même lorsque l'IDS est armé.
Lecture permanente	0 = désactivé (la case à cocher est désactivée) 1 = activé (la case est cochée)	Le lecteur lit en permanence s'il dispose du microcode respectif du fabricant.

Configuration d'un lecteur : cartes



Paramètre	**Valeurs possibles**	**Remarques**
Lecteur de carte motorisé	0 = désactivé (la case à cocher est désactivée)	Cochez cette case si un lecteur de carte motorisé est utilisé

	1 = activé (la case est cochée)	
Retirer carte	0 = désactivé (la case à cocher est désactivée) 1 = activé (la case est cochée)	Dans le cas d'un lecteur de carte motorisé, des moyens de retrait retiennent physiquement la carte. Dans le cas d'autres lecteurs de cartes, Retirer signifie que le système rend la carte invalide.
Critère de déclenchement	0 = désactivé (la case à cocher est désactivée) 1 = activé (la case est cochée)	Sélectionnez dans cette liste tous les critères qui doivent déclencher l'action **Retirer la carte**.

Remarque!
Les lecteurs de cartes motorisés ne peuvent être utilisés qu'avec des lecteurs IBPR.

Se reporter à
– *Autoriser des personnes à définir le mode Bureau, page 209*

16.7.1 Configuration de la surveillance aléatoire

La surveillance aléatoire est une méthode courante pour améliorer la sécurité du site en sélectionnant le personnel au hasard pour des contrôles de sécurité supplémentaires.

Conditions préalables :
– L'entrée doit être de type sas ou tourniquet pour empêcher une personne de « talonner » une autre sans présenter sa propre identification.
– Un lecteur de carte doit être présent pour au moins un des sens de passage.
– Les lecteurs doivent être configurés pour un contrôle d'accès normal.
– Le programme de sélection aléatoire peut être configuré séparément pour chaque lecteur.
– Il doit y avoir un poste de travail à proximité immédiate pour libérer les blocs définis par le système.

Procédure
1. Localisez le lecteur souhaité dans l'éditeur de dispositif DevEdit
2. Sur l'onglet **Paramètres**, cochez la case **Surveillance aléatoire**.
3. Dans la zone **Pourcentage de surveillance**, entrez le pourcentage de personnes à surveiller.
4. Enregistrez vos paramètres.

16.8 Accès par code PIN seul

Fond
Les lecteurs de clavier peuvent être configurés pour autoriser l'accès par code PIN uniquement.

Lorsque les lecteurs sont ainsi configurés, l'opérateur de contrôle d'accès peut attribuer des codes PIN individuels au personnel sélectionné. En effet, ces personnels reçoivent une « carte virtuelle » qui consiste uniquement en un code PIN. C'est ce qu'on appelle un code PIN d'identification. Par comparaison, un Code PIN de vérification est un code PIN utilisé en combinaison avec une carte, pour renforcer la sécurité.

L'opérateur peut saisir manuellement les codes PIN du personnel ou leur attribuer des codes PIN générés par le système.
Notez que le même personnel peut continuer à accéder à l'aide de toutes les cartes physiques qui lui sont également attribuées.

Autorisation préalable pour les opérateurs
L'autorisation d'accès par un détenteur de carte pour un accès par code PIN uniquement n'est accordée que par les opérateurs disposant d'une autorisation spéciale pour attribuer des cartes virtuelles. Pour accorder cette autorisation à un opérateur, procédez comme suit.

1. Accédez au menu principal > **Configuration** > **Opérateurs et postes de travail** > **Profils utilisateur**
2. Sélectionnez le profil utilisateur qui doit recevoir l'autorisation :
   saisissez-le dans le champ de texte **Nom de profil** ou utilisez la fonction de recherche pour trouver le profil souhaité.
3. Dans la liste des boîtes de dialogue, cliquez sur la cellule contenant **Cartes**
   Une fenêtre contextuelle intitulée **Fonctions spéciales** apparaît près de la partie inférieure du volet de la fenêtre principale.
4. Dans le volet Fonctions spéciales, cochez la case **Attribuer des cartes virtuelles (code PIN)**
5. Cliquez sur  ou sur **Appliquer** pour enregistrer vos modifications

Définition de la longueur du code PIN d'identification pour les types de lecteurs pris en charge
La longueur des codes PIN saisis manuellement ou générés par le système est régie par le jeu de paramètres dans la configuration du système.

– Menu principal > **Configuration** > **Options** > **Codes PIN** > **Longueur du code PIN**

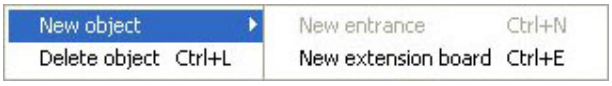
Configuration d'un lecteur pour un accès par code PIN seul

1. Accédez au menu principal > **Configuration** >**Données du dispositif** > arborescence **Postes de travail** 
2. Dans le volet **Poste de travail**, sélectionnez le poste de travail auquel le lecteur est physiquement connecté.
3. Cliquez avec le bouton droit sur le poste de travail et ajoutez un lecteur de type **Boîte de dialogue Entrer code PIN** ou **Boîte de dialogue Générer un code PIN**.
4. Sélectionnez le lecteur dans le volet **Postes de travail**.
   Un volet de configuration de lecteur personnalisé apparaît à droite du volet **Postes de travail**.
5. Vérifiez que la liste déroulante **Utilisation de carte par défaut** contient la valeur par défaut **Carte virtuelle. Utiliser code PIN comme carte**.

6. Cliquez sur ou sur **Appliquer** pour enregistrer vos modifications
7. Dans l'éditeur de dispositif DevEdit, accédez à l'arborescence **Configuration du dispositif**
8. Sélectionnez le lecteur à l'entrée où vous souhaitez configurer l'accès par code PIN seul.
9. Dans l'onglet **Options**, cochez la case **Accéder également par code PIN seul.**
10. Cliquez sur ou sur **Appliquer** pour enregistrer vos modifications

16.9 Cartes d'extension AMC

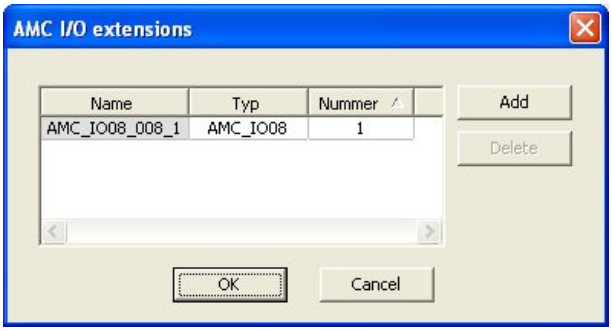
Création d'un AMC-I/O-EXT (carte d'extension d'E/S)
Les cartes d'extension fournissent des signaux d'entrée et de sortie supplémentaires, si les huit contacts situés sur l'AMC ne sont pas suffisants pour la connexion des contacts nécessaires (par exemple, avec les ascenseurs).
Ces extensions sont physiquement connectées à l'AMC associé et ne peuvent être installées que sous les AMC respectifs dans l'éditeur de dispositif. L'entrée AMC correspondante est sélectionnée dans l'explorateur pour la création d'un AMC-EXT, et l'entrée **Nouvelle carte d'extension** est choisie dans le menu contextuel **Nouvel objet**.



Remarque!

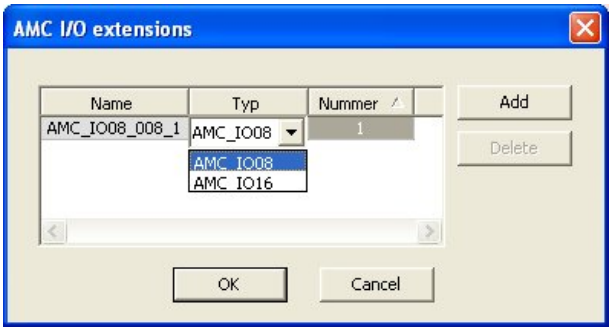
Un clic sur le bouton **+** dans la barre d'outils de l'éditeur de dispositif crée uniquement de nouvelles entrées. Les cartes d'extension peuvent être sélectionnées à l'aide du menu contextuel.

Une boîte de dialogue de sélection pour la création des extensions apparaît.

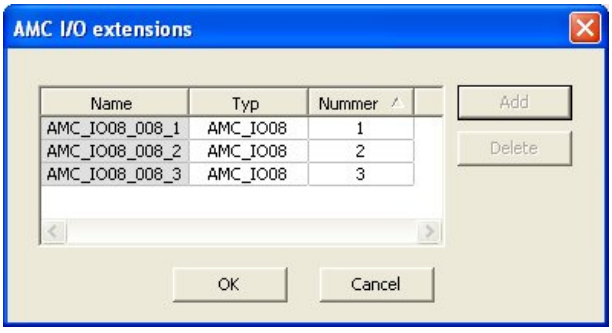


AMC-EXT est disponible en deux variantes :
- AMC_IO08 : avec 8 entrées et 8 sorties
- AMC_IO16 : avec 16 entrées et 16 sorties
- Extension AMC_4W : avec 8 entrées et 8 sorties

La boîte de dialogue de sélection contient une entrée avec un AMC_IO08. Un double-clic sur la zone de liste dans la colonne **Type** vous permet également de placer un AMC_IO16.



Vous pouvez connecter jusqu'à trois extensions à un AMC. Un mélange des deux variantes est possible. Cliquez sur **Ajouter** pour créer plusieurs entrées de liste. Celles-ci peuvent être personnalisées pour toutes les entrées de colonne.



Les cartes d'extension sont numérotées 1, 2 ou 3 au fur et à mesure qu'elles sont créées. La numérotation des signaux commence pour chaque carte à 01. Le numéro de signal en combinaison avec le numéro de carte fournit une identification unique. Les signaux des cartes d'extension sont également visibles sur l'onglet de l'AMC auquel ils appartiennent. Avec les signaux d'entrée et de sortie sur l'AMC, jusqu'à 56 paires de signaux peuvent ainsi être fournies.
Les cartes d'extension peuvent être ajoutées au besoin individuellement ou à une date ultérieure jusqu'au nombre maximum (3 par AMC).

Création d'un AMC2 4W-EXT
Il est possible de configurer des cartes d'extension spéciales (AMC2 4W-EXT) pour les contrôleurs avec des interfaces de lecteur Wiegand AMC2 4W). Ces modules fournissent 4 connexions supplémentaires pour lecteurs Wiegand ainsi que 8 contacts d'entrée et 8 contacts de sortie chacun. Ainsi, le nombre maximum de lecteurs et de portes connectables par AMC2 4W peut être doublé à 8.

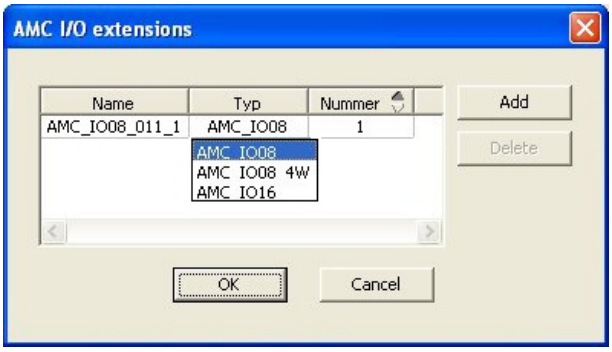
Remarque!
L'AMC2 4W-EXT ne peut pas être utilisé comme contrôleur autonome, mais uniquement comme une extension d'un AMC2-4W. Les portes sont contrôlées et les décisions de contrôle d'accès sont prises uniquement par l'AMC2 4W.

L'AMC2 4W-EXT ne peut être utilisé qu'avec un AMC2 4W. Comme il ne dispose que d'interfaces de lecteur Wiegand, il n'est pas utilisable avec la variante AMC AMC2 4R4.

Comme les cartes d'extension E/S (AMC2 8I-8O-EXT et AMC2 16I-16O-EXT), l'AMC2 4W-EXT est connecté via l'interface d'extension de l'AMC2 4W. La carte d'extension n'a ni mémoire ni affichage propre, mais est entièrement contrôlée par l'AMC2 4W.
Un AMC2 4W-EXT et un maximum de trois extensions d'E/S peuvent être connectés à chaque AMC2-4W.
Pour créer un AMC2 4W-EXT sur le système, cliquez avec le bouton droit sur le parent souhaité AMC2 4W dans l'explorateur et sélectionnez **Nouvel objet** > **Nouvelle carte d'extension** dans le menu contextuel.

Remarque!
Le bouton ✚ dans la barre d'outils de l'éditeur de données de dispositif ne peut être utilisé que pour ajouter des entrées. Les cartes d'extension ne peuvent être ajoutées que via le menu contextuel.

La même boîte de dialogue de sélection apparaît pour la création d'extensions d'E/S, à l'exception de la liste d'un AMC2 4W qui contient l'élément supplémentaire AMC_IO08_4W.



L'entrée de liste AMC2 4W ne peut être ajoutée qu'une seule fois, tandis que jusqu'à trois extensions d'E/S peuvent être ajoutées.
Le bouton **Ajouter** permet d'ajouter de nouvelles entrées de liste. Dans le cas d'un AMC2 4W, le nombre maximum est de 4, la quatrième entrée étant créée en tant que carte AMC2 4W-EXT.
Les cartes d'extension sont numérotées selon l'ordre de création 1, 2 ou 3. L'AMC2 4W-EXT reçoit le numéro 0 (zéro). La numérotation des signaux pour l'AMC2 4W-EXT se poursuit à partir de celle du contrôleur, à savoir 09 à 16, alors que pour chaque carte d'E/S, la numérotation commence à 01. Les signaux de toutes les cartes d'extension sont également indiqués sur l'onglet AMC2 4W concerné.
Avec les signaux d'entrée et de sortie sur l'AMC2 4W, jusqu'à 64 paires de signaux peuvent être fournies.

Modification et suppression de cartes d'extension
Le premier onglet contient les commandes suivantes pour la configuration des cartes d'extension.

Paramètre	Valeurs possibles	Description
Nom de carte	Alphanumérique restreint : 1 à 16 chiffres	L'identification par défaut garantit un nom unique, mais celui-ci peut être remplacé manuellement. Assurez-vous que l'identifiant

		est unique. Les connexions réseau avec des serveurs DHCP doivent utiliser le nom du réseau.
Description de carte	alphanumérique : 0 à 255 chiffres	Ce texte est affiché dans la branche OPC.
Numéro de carte	1 - 3	Numéro de la carte connectée à l'AMC. Champ d'affichage uniquement.
Alimentation	0= désactivé (la case est cochée est sélectionnée) 1= activé (la case est cochée)	Supervision de la tension d'alimentation. En cas de coupure de tension, un message est généré à la fin d'un délai. La fonction de supervision suppose l'utilisation d'un USV, de sorte qu'un message puisse être généré. 0 = pas de supervision 1 = supervision activée
Division	Valeur par défaut **Commun**	Pertinent uniquement lorsque la fonction **Divisions** est sous licence.

Les onglets Entrées, Sorties et Paramètres de signal ont la même disposition et la même fonction que les onglets correspondants pour les contrôleurs.

Suppression de cartes d'extension

Il n'est possible de supprimer une carte d'extension que lorsqu'aucune de ses interfaces n'est occupée. Les signaux associés doivent d'abord être configurés sur une carte différente avant que le bouton de suppression  et l'option de menu contextuel **Supprimer l'objet** ne deviennent utilisables.

AMC2 4W-EXT

Comme les lecteurs qui occupent des cartes d'extension ne peuvent pas être retirés ou reconfigurés séparément, ils doivent être supprimés avec leurs entrées correspondantes. Ce n'est qu'alors que l'AMC2 4W-EXT peut également être retiré.

17 Configurations de lecteur personnalisées

17.1 Introduction

À compter des versions BIS 4.9 et AMS 4.0, les systèmes de contrôle d'accès Bosch permettent l'utilisation de paramètres MIFARE DESFire personnalisés. Vous pouvez créer des fichiers de paramètres chiffrés à l'aide de l'outil auxiliaire `Bosch.ReaderConfigTool.exe`. Cet outil est inclus dans les configurations de BIS ACE 4.9, AMS 4.0 et versions ultérieures, avec sa propre documentation. Consultez cette documentation pour connaître la liste actualisée des lecteurs compatibles
Les sections suivantes décrivent comment utiliser l'éditeur de dispositif pour importer un fichier de paramètres chiffré et l'appliquer à tout ou partie des lecteurs compatibles dans la hiérarchie des dispositifs de contrôle d'accès.

17.2 La propriété de lecteur : Extended reader parameters (Paramètres étendus du lecteur)

Les jeux de paramètres étendus disponibles pour les lecteurs compatibles sont affichés sur leurs pages de propriétés dans l'éditeur de dispositif sous le libellé **Extended reader parameters (Paramètres de lecteur étendus)**.

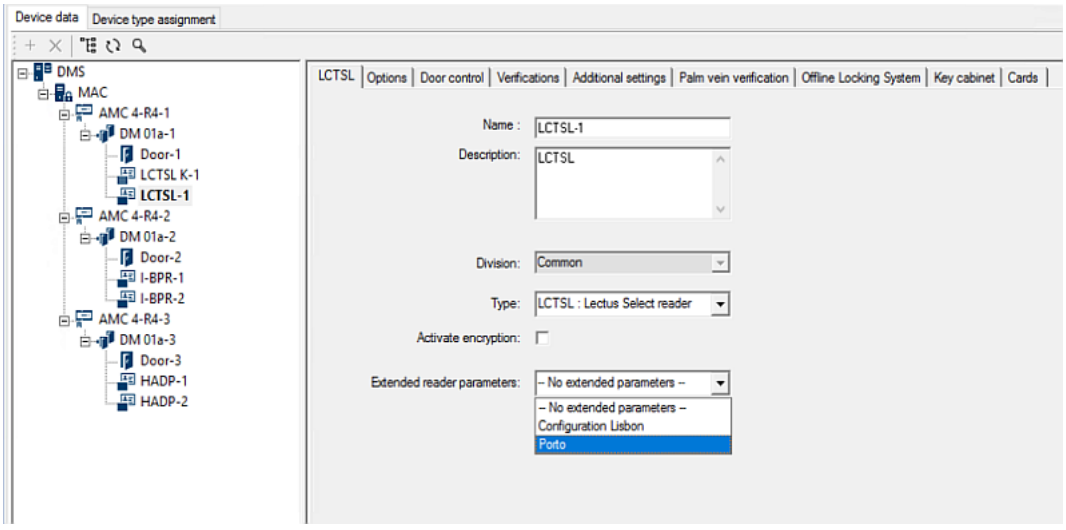


Figure 17.1: Extended reader parameters (Paramètres de lecteur étendus)

La valeur par défaut de la liste déroulante est `No extended parameters`. Il s'agit de la seule valeur possible, sauf si vous importez des jeux de paramètres supplémentaires.

Procédure

Pour appliquer un jeu de paramètres importé sur un lecteur individuel compatible :

1. Dans l'éditeur de dispositif, sélectionnez le lecteur dans l'arborescence des dispositifs
2. Sélectionnez le premier onglet de propriété
3. Sélectionnez le jeu de paramètres requis dans la liste **Extended reader parameters (Paramètres de lecteur étendus)**
4. Cliquez sur **Apply (Appliquer)** ou sur 

17.3 Importation d'un jeu de paramètres de lecteur

Vous importez et supprimez les fichiers de paramètres uniquement au niveau du DMS de la hiérarchie de dispositifs.

Conditions préalables

Accédez à un fichier de paramètres approuvé pour votre système de contrôle d'accès. Par défaut, le fichier est de type `.ReaderConfigSave`

Procédure

1. Dans l'éditeur de dispositif, cliquez avec le bouton droit sur le nœud DMS et sélectionnez **Import reader parameter sets (Importer des jeux de paramètres de lecteur)** depuis le menu contextuel.
   La fenêtre contextuelle **Import reader parameter sets (Importer des jeux de paramètres de lecteur)** apparaît.
2. Cliquez sur **File (Fichier)** et localisez le fichier de paramètres à l'aide de l'explorateur de fichiers.
3. Lorsque vous y êtes invité, saisissez le mot de passe du fichier de paramètres.
   Si le mot de passe est correct, la moitié inférieure de la fenêtre contextuelle est remplie avec les informations suivantes :

– Une liste des types de lecteurs auxquels s'applique le jeu de paramètres.
– Le nom du jeu de paramètres. Vous pouvez effectuer de modifications dans cette boîter de dialogue.
– Une description en texte libre, si le créateur du jeu de paramètres en a fourni une. Vous pouvez ajouter ou modifier une description dans cette boîte de dialogue.

4. Cliquez sur **Import (Importer)** pour importer le jeu de paramètres pour une éventuelle utilisation future par le système de contrôle d'accès.

– Le jeu de paramètres est importé et stocké dans le système de contrôle d'accès.
– Il est ajouté à la liste des jeux de paramètres disponibles en haut de la fenêtre contextuelle.

5. Cliquez sur **Exit (Quitter)** pour quitter la fenêtre contextuelle **Import reader parameter sets (Importer des jeux de paramètres de lecteur)**.

17.4 Application d'un jeu de paramètres aux lecteurs

Introduction

L'importation d'un jeu de paramètres dans le système de contrôle d'accès le stocke pour une utilisation future, mais ne l'applique pas aux lecteurs du système. L'application du jeu de paramètres est une étape supplémentaire que vous pouvez effectuer à différents niveaux de la hiérarchie des dispositifs :

– DMS
– MAC
– AMC

Lorsque vous appliquez un jeu de paramètres au niveau DMS, MAC ou AMC, il ne peut s'appliquer qu'aux lecteurs subordonnés des types de lecteurs pour lesquels le jeu a été créé. Tous les autres lecteurs subordonnés ne sont pas affectés.

Conditions préalables

Vous avez importé avec succès un jeu de paramètres de lecteur.

Procédure

1. Dans l'éditeur de dispositif, effectuez un clic droit afin de sélectionner un lecteur ou un dispositif (DMS, MAC ou AMC) dont vous souhaitez paramétrer les lecteurs.
2. Sélectionnez **Manage reader parameter sets (Gérer les jeux de paramètres de lecteur)** depuis le menu contextuel.
3. Dans le volet de liste supérieur, **Parameter sets for reader types (Jeux de paramètres pour les types de lecteurs)**, sélectionnez le jeu de paramètres que vous souhaitez appliquer.

Les lecteurs concernés sont répertoriés dans le volet inférieur gauche : **Readers parametrizable with this parameter set (Lecteurs paramétrables avec ce jeu de paramètres)**.

4. Dans la liste **Readers parametrizable with this parameter set (Lecteurs paramétrables avec ce jeu de paramètres)**, sélectionnez les lecteurs auxquels vous souhaitez appliquer le jeu de paramètres sélectionné.

– Si le nombre de lecteurs est important, utilisez les listes déroulantes pour limiter l'affichage aux subordonnés d'un MAC ou d'un AMC particulier.

5. Utilisez les boutons fléchés pour déplacer les lecteurs sélectionnés dans le volet inférieur droit, **All readers parametrized with the selected parameter set (Tous les lecteurs paramétrés avec le jeu de paramètres sélectionné)**.

Remarque!
Affichage des lecteurs compatibles
Seuls les lecteurs compatibles avec le jeu de paramètres seront répertoriés. Si vous cochez la case **Show all readers (Afficher tous les lecteurs)**, les lecteurs qui ont d'autres jeux de paramètres seront également affichés. Ceux-ci ont un fond gris qui indique qu'ils sont en lecture seule pour le jeu de paramètres sélectionné.

6. Cliquez sur **OK** pour fermer la fenêtre contextuelle.

7. De retour dans l'éditeur de dispositif, cliquez sur **Apply (Appliquer)** ou sur 
Le jeu de paramètres est appliqué à tous les lecteurs que vous avez conservés dans la liste **All readers parametrized with the selected parameter set (Tous les lecteurs paramétrés avec le jeu de paramètres sélectionné)** dans la fenêtre contextuelle.

17.5 Gestion des jeux de paramètres du lecteur

Introduction
Vous pouvez modifier l'application des jeux de paramètres à différents niveaux de la hiérarchie des dispositifs :

– DMS
– MAC
– AMC

Les modifications au niveau DMS, MAC ou AMC ne peuvent s'appliquer qu'aux lecteurs subordonnés des types de lecteurs pour lesquels le jeu a été créé. Tous les autres lecteurs subordonnés ne sont pas affectés.

Condition préalable
Vous avez importé avec succès un jeu de paramètres de lecteur.

Procédure

1. Dans l'éditeur de dispositif, faites un clic droit sur un lecteur ou un appareil (DMS, MAC ou AMC)
2. Sélectionnez **Manage reader parameter sets (Gérer les jeux de paramètres de lecteur)** depuis le menu contextuel.
3. Dans le volet de liste supérieur, **Parameter sets for reader types (Jeux de paramètres pour les types de lecteurs)**, sélectionnez le jeu de paramètres que vous souhaitez appliquer.

– Les lecteurs concernés sont répertoriés dans le volet inférieur gauche : **Readers parametrizable with this parameter set (Lecteurs paramétrables avec ce jeu de paramètres)**.

– Les lecteurs auxquels le fichier de paramètres a déjà été appliqué sont répertoriés dans le volet inférieur droit : **All readers parametrized with the selected parameter set (Tous les lecteurs paramétrés avec le jeu de paramètres sélectionné)**.

4. Sélectionnez les lecteurs dans l'une ou l'autre liste. Utilisez les touches fléchées pour déplacer ou retirer des lecteurs dans la listes inférieure droite, **All readers parametrized with the selected parameter set (Tous les lecteurs paramétrés avec le jeu de paramètres sélectionné)**.

– IMPORTANT : Notez soigneusement les lecteurs que vous retirez de la liste, pour la dernière étape de cette procédure.

5. Lorsque vous avez terminé vos modifications, cliquez sur **OK** pour fermer la fenêtre contextuelle.

6. De retour dans l'éditeur de dispositif, cliquez sur **Apply (Appliquer)** ou sur 

– Le jeu de paramètres est appliqué à tous les lecteurs que vous avez conservés dans la liste **All readers parametrized with the selected parameter set (Tous les lecteurs paramétrés avec le jeu de paramètres sélectionné).**

– Il est retiré des lecteurs que vous avez retirés de cette liste.

7. Effectuez l'une des opérations suivantes pour tous les lecteurs que vous avez retirés de la liste :

– Réinitialisez les paramètres d'usine par défaut à l'aide des commutateurs DIP dans le matériel du lecteur.

– Appliquez-leur un jeu de paramètres différent.

Remarque!
La suppression d'un jeu de paramètres ne reconfigure pas les lecteurs qui l'ont utilisé.
La configuration de lecteur supprimée demeurera dans les lecteurs qui l'ont utilisée jusqu'à ce que vous réinitialisiez le matériel du lecteur ou que vous appliquiez un jeu de paramètres différent.

17.6 Suppression de jeux de paramètres du lecteur

Vous importez et supprimez les fichiers de paramètres uniquement au niveau du DMS de la hiérarchie de dispositifs.

Conditions préalables
Au moins un fichier de paramètres a déjà été importé dans votre système de contrôle d'accès.

Procédure

1. Dans l'éditeur de dispositif, cliquez avec le bouton droit sur le nœud DMS et sélectionnez **Delete reader parameter sets (Supprimer des jeux de paramètres de lecteur)** depuis le menu contextuel.
   La fenêtre contextuelle **Delete reader parameter sets (Supprimer des jeux de paramètres de lecteur)** apparaît.
2. Dans la liste **Parameter sets for reader types (Jeux de paramètres pour les types de lecteurs)**, sélectionnez le jeu de paramètres que vous souhaitez supprimer.

– Dans l'angle inférieur droit de la fenêtre contextuelle, une liste affiche tous les lecteurs actuellement paramétrés (configurés) avec le jeu de paramètres sélectionné.

– Notez soigneusement ces lecteurs, ils nécessiteront une réinitialisation ou une reconfiguration après la suppression du jeu de paramètres. Reportez-vous à la dernière étape de cette procédure pour plus de détails.

3. Cliquez sur **Delete (Supprimer)**

4. Cliquez sur **Exit (Quitter)**

5. De retour dans l'éditeur de dispositif, cliquez sur **Apply (Appliquer)** ou sur 
6. Effectuez l'une des opérations suivantes pour tous les lecteurs qui utilisaient le jeu de paramètres supprimé :

– Réinitialisez les paramètres d'usine par défaut à l'aide des commutateurs DIP dans le matériel du lecteur.
– Appliquez-leur un jeu de paramètres différent.

Remarque!
La suppression d'un jeu de paramètres ne reconfigure pas les lecteurs qui l'ont utilisé.
La configuration de lecteur supprimée demeurera dans les lecteurs qui l'ont utilisée jusqu'à ce que vous réinitialisiez le matériel du lecteur ou que vous appliquiez un jeu de paramètres différent.

18 Champs personnalisés pour les données de personnel

Introduction

Les champs de données pour le personnel sont personnalisables de plusieurs manières :

- En définissant s'ils sont **Visibles**, c'est-à-dire s'ils sont affichés dans le client
- En définissant s'ils sont **Obligatoires**, c'est-à-dire si un enregistrement de données peut être stocké sans données valides dans le champ
- En définissant si les valeurs qu'ils contiennent doivent être conservées comme étant **Uniques** au sein du système
- En définissant le type de données qu'ils contiennent (texte, date-heure, entier, etc.)
- En indiquant où ils vont figurer sur le client (sur quel onglet, dans quelle colonne et sur quelle ligne)
- En indiquant quelle sera leur taille
- En indiquant si et où les données seront utilisées dans les rapports standard

Il est bien sûr toujours possible de définir des champs de données entièrement nouveaux avec tous les attributs listés ici.

18.1 Aperçu et modification des champs personnalisés

Chemin d'accès à la boîte de dialogue

- Menu principal > **Configuration** > **Options** > **Champs personnalisés**

La fenêtre principale est divisée en deux onglets

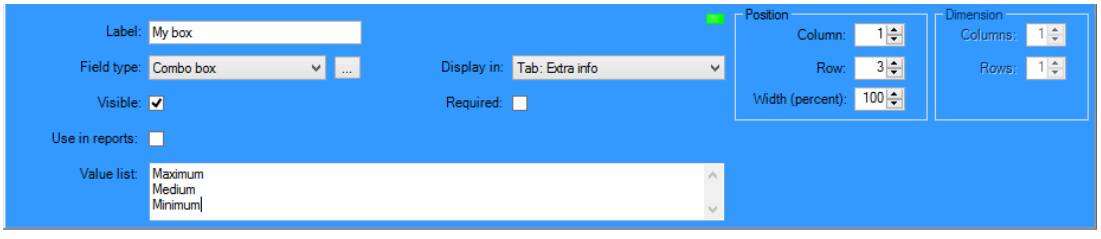
Présentation Cet onglet et ses sous-onglets (**Adresse, contact, données personnelles supplémentaires, données supplémentaires sur l'entreprise, remarques, commande de la carte** et **Informations supplémentaires**) sont en lecture seule et contiennent un aperçu de type WYSIWYG des données qui apparaîtront sur les onglets du logiciel client.

Détails Cet onglet contient une liste d'éditeurs, un pour chaque champ de données prédéfini ou défini par l'utilisateur.

Modification de champs de données existants

Dans l'onglet **Custom fields (Champs personnalisés)** > **Details (Détails)**, chaque champ de données, prédéfini ou défini par l'utilisateur, possède sa propre fenêtre d'éditeur dans laquelle il est possible de modifier ses attributs.

Cliquez dans l'éditeur du champ que vous souhaitez modifier. L'éditeur actif sera mis en évidence.



Les attributs modifiables des champs personnalisés sont décrits dans le tableau suivant.

Texte de l'étiquette	Description
Étiquette	**Étiquette** est le libellé du champ de données tel qu'il apparaît dans le client. Il peut être librement remplacé pour refléter la terminologie utilisée sur votre site.
Type de champ	**Type de champ** désigne le type des données et détermine la commande de dialogue que l'opérateur utilisera pour créer des entrées dans le client. Chaque type de champ fournit des vérifications de cohérence pour ses valeurs d'entrée particulières, pour garantir des dates, heures, longueurs de texte et limites numériques valides. – **Champ de texte** – Cliquez sur le bouton points de suspension à côté pour spécifier le nombre de caractères autorisés. – **Case à cocher** – **Champ de date** – **Temps** – **Champ de date/heure** – **Zone de liste** – Entrez les valeurs valides pour votre zone de liste déroulante dans le champ de texte fourni. Séparez-les par des virgules ou des retours chariot. – **Saisie numérique** – Entrez vos valeurs minimale et maximale pour la saisie numérique dans les zones de sélection numérique fournies. – **Contrôle bâtiment 1** et **Contrôle bâtiment 2** – Il s'agit de contrôles spéciaux qui peuvent être renommés ici (dans le champ **Étiquette**) et liés aux commandes dans l'interface utilisateur du client. Ainsi, vous pouvez autoriser des utilisateurs spécifiques, via leurs cartes, à effectuer des opérations spéciales au sein du site. Ces opérations peuvent consister à allumer des projecteurs ou à commander des équipements spéciaux.
Visible	Désélectionnez cette case pour empêcher le champ de données d'apparaître dans le client.
Unique	Sélectionnez cette case pour garantir l'unicité des valeurs saisies dans ce champ. Le système rejette alors la saisie de toute valeur qui a déjà été stockée pour ce champ dans la base de données. Par exemple, les numéros de personnel doivent être uniques aux personnes et les plaques d'immatriculation aux véhicules.
	Le voyant vert signifie que le champ de données n'est **pas** utilisé dans la base de données actuellement. Le voyant rouge signifie que le champ de données est actuellement utilisé dans la base de données.
Display in (Afficher dans)	Utilisez cette liste déroulante pour sélectionner l'onglet client dans lequel le champ de données doit apparaître.

Texte de l'étiquette	Description
Required (Obligatoire)	Cochez cette case pour rendre le champ de données obligatoire. Par exemple, la mention du nom de famille est obligatoire pour chaque enregistrement de personnel. Sans ce nom, l'enregistrement de données ne peut pas être stocké. Notez que l'éditeur ne permet pas qu'un champ de données obligatoire soit défini comme invisible via la case à cocher **Visible**. Pour faciliter l'utilisation dans le client, il est fortement recommandé que tous les champs obligatoires soient placés dans le premier onglet.
Position	Utilisez les zones de sélection numérique **Column (Colonne)** et **Row (Ligne)** pour positionner le champ de données dans l'onglet désigné dans la liste déroulante **Display in (Afficher dans)**. Notez que l'éditeur ne vous permet pas de sélectionner un emplacement déjà utilisé, ni de superposer des champs de données existants. Utilisez la zone de sélection numérique **Width (percent) [Largeur (pourcentage)]** pour définir la taille de certains contrôles redimensionnables, tels que les champs de texte. 100 % signifie que le contrôle occupera tout l'emplacement qui n'est pas déjà occupé par le libellé du champ de données.
Dimensions	Utilisez les zones de sélection numérique **Column (Colonne)** et **Row (Ligne)** pour spécifier le nombre de colonnes et de lignes à occuper dans l'onglet désigné dans la liste déroulante **Display in (Afficher dans)**. Notez que l'éditeur ne vous permet pas de superposer des champs de données existants.

Création et modification de nouveaux champs de données

Dans l'onglet **Custom fields (Champs personnalisés)** > **Details (Détails)**, chaque champ de données, prédéfini ou défini par l'utilisateur, possède son propre volet éditeur dans lequel il est possible de modifier ses attributs.

Cliquez sur le bouton **New field (Nouveau champ)** pour créer un champ personnalisé avec son propre éditeur. Le volet éditeur actif sera mis en surbrillance.

L'éditeur dispose des mêmes contrôles de boîte de dialogue pour modifier les champs de données existants (voir le tableau ci-dessus), ainsi que deux contrôles supplémentaires :

Use in reports (Utilisation dans les rapports) (case à cocher)	Cochez cette case pour permettre au nouveau champ de données de figurer dans les rapports standard.
Sequence number (Numéro séquentiel) (zone de sélection numérique)	Le numéro séquentiel détermine la colonne dans laquelle le champ de données figurera dans les rapports standard.

Remarque!

Seuls les numéros séquentiels 1 à 10 sont actuellement adressables par les champs **Badge Designer (Concepteur de badge)** et **Reports (Rapports)**.

18.2 Règles des champs de données

- Emplacement des champs de données
  - Chaque champ ne peut figurer que dans un seul onglet.
  - Chaque champ personnalisé peut figurer dans n'importe quel onglet sélectionnable.
  - Les champs peuvent être déplacés vers d'autres onglets en modifiant l'entrée dans la liste déroulante **Display in (Afficher dans)**.
- Le libellé peut contenir n'importe quel texte d'une longueur maximale de 20 caractères.
- Les champs de texte personnalisés peuvent contenir n'importe quel texte d'une longueur maximale de 2 000 caractères.
- N'importe quel champ peut être rendu obligatoire, mais sa case **Visible** doit être cochée.

Remarque!
Recommandations importantes avant une utilisation productive
Acceptez et finalisez les types de champs et leur utilisation avant de les utiliser pour stocker les données des personnes :
Chaque champ de saisie de données est affecté à un champ de base de données spécifique afin que les données puissent être localisées à la fois manuellement et par les générateurs de rapports. Une fois que les enregistrements de données des champs personnalisés ont été stockés dans la base de données, ces champs ne peuvent plus être déplacés ou modifiés sans risquer de perdre des données.

19 Configuration de la gestion du niveau de menace

Introduction

L'objectif de la gestion du niveau de menace est de répondre efficacement aux situations d'urgence en modifiant instantanément le comportement des entrées dans toute la zone touchée.

19.1 Concepts de la gestion du niveau de menace

- Une **Menace** est une situation critique qui nécessite une réponse immédiate et simultanée de certaines ou de la totalité des entrées d'un système de contrôle d'accès.
- Un **niveau de menace** est une réponse du système à une situation prévue. Chaque niveau de menace doit être soigneusement configuré afin que chacune des entrées du MAC sache comment réagir.

  Les niveaux de menace sont entièrement personnalisables. Par exemple, les niveaux de menace élevés classiques peuvent être configurés comme suit :
  - **Lockout (Verrouillage)** : seuls les premiers intervenants, avec des niveaux de sécurité élevés, peuvent entrer.
  - **Lockdown (Blocage)** : toutes les portes sont verrouillées. L'entrée et la sortie sont refusées à toutes les cartes en deçà d'un niveau de sécurité configuré.
  - **Evacuation (Évacuation)** : toutes les portes de sortie sont déverrouillées.
- Les niveaux de menace faibles classiques peuvent être configurés comme suit :
  - **Sports event (Événement sportif)** : les portes des terrains/salles de sport sont déverrouillées, toutes les autres zones sont sécurisées.
  - **Parents' evening (Soirée parents)** : seules les salles de classe sélectionnées et l'entrée principale sont accessibles.
- Une **alerte aux menaces** est une alarme qui déclenche un niveau de menace. Les personnes dûment autorisées peuvent déclencher une alerte de menace avec une action momentanée, par exemple via l'interface utilisateur de l'opérateur, via un signal matériel (par exemple un bouton-poussoir), ou en présentant une carte d'alerte spéciale à n'importe quel lecteur.
- Un **niveau de sécurité** est un attribut des **profils de sécurité** des détenteurs de carte et des lecteurs, exprimé sous la forme d'un entier entre 0 et 100. Chaque niveau de menace permet de régler les lecteurs du contrôleur MAC (Main Access Controller) sur les niveaux de sécurité convenus. Ces lecteurs n'accordent ensuite l'accès qu'aux cartes des personnes disposant d'un niveau de sécurité égal ou supérieur dans leurs profils de sécurité.
- Un **profil de sécurité** est un ensemble d'attributs pouvant être attribués à un **type de personne** (**profil de sécurité des personnes**), à une porte (**profil de sécurité de porte**), ou à un lecteur (**profil de sécurité de lecteur**). Les profils de sécurité régissent les comportements de contrôle d'accès suivants :
  - **Niveau de sécurité** : comme défini ci-dessus, pour le type de personne, de porte ou de lecteur.
  - **Taux de surveillance** : le pourcentage de probabilité qu'une surveillance aléatoire soit déclenchée par ce type de personne ou de lecteur.

19.2 Vue d'ensemble du processus de configuration

La gestion du niveau de menace nécessite la réalisation des étapes de configuration suivantes (expliquées en détail après cette vue d'ensemble)

1. Dans l'éditeur de dispositif
   - Définir les niveaux de menace

- Définir les profils de sécurité des portes
- Définir les profils de sécurité des lecteurs
- Attribuer les profils de sécurité des portes aux entrées

2. Dans les boîtes de dialogue des données système
   - Définir les profils de sécurité des personnes
   - Attribuer les profils de sécurité des personnes aux types de personnes
3. Dans les boîtes de dialogue des données du personnel
   - Attribuer les types de personnes aux personnes
   - Attribuer les types de personnes aux groupes de personnes

Une fois la gestion du niveau de menace correctement configurée, les alarmes et les états des périphériques du MAC peuvent être surveillés et contrôlés à partir de l'application Map View. Consultez l'aide en ligne de Map View pour plus de détails.

19.3 Étapes de configuration dans l'éditeur de dispositif

Cette section décrit les étapes de configuration préalablement requises dans l'éditeur de dispositif.

Remarque!
Les données du périphérique ne peuvent pas être modifiées dans l'éditeur de dispositif lorsqu'un niveau de menace est activé.

19.3.1 Création d'un niveau de menace

Cette section explique comment créer des niveaux de menace pour votre site. Vous pouvez créer jusqu'à 15 niveaux.

Chemin d'accès à la boîte de dialogue

- **Menu principal** >**Configuration** > **Données du dispositif**

Procédure

1. Sélectionnez le sous-onglet **Threat levels (Niveaux de menace)**
   - Le tableau des niveaux de menace apparaît. Il peut contenir jusqu'à 15 niveaux, chacun comportant un nom, une description et une case à cocher à l'aide de laquelle activer le niveau de menace après sa configuration.
2. Cliquez sur la ligne **Please enter a name for the threat level (Veuillez entrer un nom pour le niveau de menace)**.
3. Entrez un nom qui sera explicite pour les opérateurs système.
4. (Facultatif) Dans la colonne **Description**, entrez une description plus complète du comportement des entrées lorsque ce niveau de menace est activé.
5. Ne cochez **pas** la case **Active (Activé)** pour le moment. Effectuez d'abord toutes les autres étapes de configuration de ce niveau de menace, comme décrit dans les sections suivantes.
6. Cliquez sur  (Enregistrer) pour enregistrer le nouveau niveau de menace.

19.3.2 Création d'un profil de sécurité de porte

Cette section explique comment créer des profils de sécurité pour différents types de portes et comment définir l'état dans lequel toutes les portes de ce profil basculeront en cas d'activation d'un niveau de menace.

Chemin d'accès à la boîte de dialogue

– **Menu principal** >**Configuration** > **Données du dispositif**

Conditions préalables

– Au moins un niveau de menace a été défini.
– Au moins une entrée a été configurée dans l'arborescence des périphériques.

Procédure

1. Sélectionnez le sous-onglet **Door security profiles (Profils de sécurité de porte)**.
   – La fenêtre de la boîte de dialogue principale comporte 2 volets : **Selection (Sélection)** et **Door security profile (Profil de sécurité de porte)** (nom par défaut).
2. Cliquez sur **New (Nouveau)**.
   – Un nouveau profil de sécurité de porte est créé avec un nom par défaut.
   – Le tableau **Threat level (Niveau de menace)** figurant dans le volet **Door security profile (Profil de sécurité de porte)** est renseigné avec les niveaux de menace déjà créés, ainsi qu'avec la valeur **undefined (non défini)** pour chacune des colonnes **State (État)**.
3. Dans le volet **Door security profile (Profil de sécurité de porte)**, entrez un nom pour le type de porte auquel ce profil sera attribué.
   – Le nom du nouveau profil apparaît dans le volet **Selection (Sélection)**. Si vous le souhaitez, vous pouvez le supprimer de la configuration en cliquant sur **Delete (Supprimer)** dans ce même volet.
4. (Facultatif) Entrez une description du profil pour aider les opérateurs à attribuer correctement celui-ci.
5. Si ce profil doit être attribué à des tourniquets, cochez la case **Turnstile (Tourniquet)**.
   – Cela permet de disposer d'options supplémentaires pour l'état cible de la porte à différents niveaux de menace, par exemple, les options permettant l'entrée ou la sortie seule, ou les deux ensemble.
6. Dans la colonne **State (État)** du tableau **Threat level (Niveau de menace)**, pour chaque niveau de menace, sélectionnez l'état cible approprié pour toutes les portes de ce profil chaque fois que ce niveau de menace est activé.
7. Cliquez sur  (Enregistrer) pour enregistrer les modifications.

Répétez la procédure pour créer autant de profils de sécurité de porte que de types de porte dans votre configuration. Exemples de types de portes classiques :

– Porte d'entrée principale
– Issue de secours
– Accès aux salles de classe
– Accès public au complexe sportif

19.3.3 Création d'un profil de sécurité de lecteur

Cette section explique comment créer des profils de sécurité pour différents types de lecteurs. Les profils de sécurité de lecteur définissent les attributs de lecteur suivants **pour chaque niveau de menace** :

- Le niveau de sécurité minimal exigé par le lecteur pour autoriser l'accès.
- Le taux de surveillance, c'est-à-dire le pourcentage de détenteurs de carte qui seront sélectionnés de façon aléatoire en vue d'un contrôle de sécurité supplémentaire.
  - **Remarque** : le taux de surveillance aléatoire défini dans un profil de sécurité de lecteur annule et remplace le taux de surveillance défini sur le lecteur lui-même.

Chemin d'accès à la boîte de dialogue

- **Menu principal** >**Configuration** > **Données du dispositif**

Conditions préalables

- Au moins un niveau de menace a été défini.
- Au moins une entrée a été configurée dans l'arborescence des périphériques.

Procédure

1. Sélectionnez le sous-onglet **Reader security profile (Profils de sécurité de lecteur)**.
   - La fenêtre de la boîte de dialogue principale comporte 2 volets : **Selection (Sélection)** et **Reader security profile (Profil de sécurité de lecteur)** (nom par défaut).
2. Cliquez sur **New (Nouveau)**.
   - Un nouveau profil de sécurité de lecteur est créé avec un nom par défaut.
   - Le tableau **Threat level (Niveau de menace)** figurant dans le volet **Reader security profile (Profil de sécurité de lecteur)** est renseigné avec les niveaux de menace déjà créés, ainsi qu'avec la valeur par défaut **0** pour chacune des colonnes **Security level (Niveau de sécurité)** et **Screening rate (Taux de surveillance)**.
3. Dans le volet **Reader security profile (Profil de sécurité de lecteur)**, entrez un nom pour le type de lecteur auquel ce profil sera attribué.
   - Le nom du nouveau profil apparaît dans le volet **Selection (Sélection)**. Si vous le souhaitez, vous pouvez le supprimer de la configuration en cliquant sur **Delete (Supprimer)** dans ce même volet.
4. (Facultatif) Entrez une description du profil pour aider les opérateurs à attribuer correctement celui-ci.
5. Dans la colonne **Security level (Niveau de sécurité)** du tableau **Threat level (Niveau de menace)**, pour chaque niveau de menace, sélectionnez le niveau de sécurité minimal (entier de 0 à 100) dont doit disposer un opérateur pour faire fonctionner un lecteur de ce profil chaque fois que ce niveau de menace est activé.
6. Dans la colonne **Screening rate (Taux de surveillance)** du tableau **Threat level (Niveau de menace)**, pour chaque niveau de menace, sélectionnez le pourcentage de détenteurs de carte qui seront sélectionnés de façon aléatoire par le lecteur en vue de subir des contrôles de sécurité supplémentaires chaque fois que ce niveau de menace sera activé.
7. Cliquez sur  (Enregistrer) pour enregistrer les modifications.

19.3.4 Attribution de profils de sécurité de porte et de lecteur aux entrées

Cette section explique comment attribuer les profils de sécurité de porte et de lecteur aux portes et lecteurs d'entrées spécifiques.

La première sous-procédure consiste à identifier et à filtrer l'ensemble des entrées auxquelles vous souhaitez attribuer ces profils, et la seconde à procéder à ces attributions. Vous pouvez également prévisualiser les états, les niveaux de sécurité et les taux de surveillance des entrées sélectionnées tels que configurés par les différents niveaux de menace que vous avez définis.

Chemin d'accès à la boîte de dialogue

– **Menu principal** >**Configuration** > **Données du dispositif**

Conditions préalables

– Au moins un niveau de menace a été défini.
– Au moins une entrée a été configurée dans l'arborescence des périphériques.

Procédure

1. Dans l'arborescence des périphériques, sélectionnez **DMS** (la racine de l'arborescence).
2. Dans le volet de la boîte de dialogue principale, sélectionnez l'onglet **Threat level management (Gestion du niveau de menace)**.
   – Le volet de la boîte de dialogue principale comporte plusieurs sous-onglets.

Sous-procédure 1 : sélection des entrées auxquelles attribuer les profils

1. Sélectionnez le sous-onglet **Entrances (Entrées)**.
   – La fenêtre de dialogue principale comporte 2 volets : **Filter conditions (Conditions de filtrage)** et un tableau de toutes les entrées créées jusqu'à présent dans le système.
2. (Facultatif) Dans le volet **Filter conditions (Conditions de filtrage)**, entrez les critères visant à restreindre les entrées du tableau affiché dans la partie inférieure de la boîte de dialogue, par exemple :
   – Cochez ou décochez les cases qui déterminent si **Inbound readers (Lecteurs entrants)**, **Outbound readers (Lecteurs sortants)** et/ou **Doors (Portes)** doivent figurer dans le tableau.
   – Entrez des chaînes de caractères devant figurer dans les noms des entrées, des zones, des noms de profil ou des noms de lecteur de toutes les entrées répertoriées dans le tableau.
   – Cochez ou décochez la case qui détermine si les portes et les lecteurs qui ne sont pas encore configurés doivent également figurer dans le tableau.
3. Cliquez sur **Apply filter (Appliquer le filtre)** pour filtrer la liste des entrées, ou sur **Reset filter (Réinitialiser le filtre)** pour réattribuer aux contrôles de filtre leurs valeurs par défaut.

Sous-procédure 2 : attribution des profils de sécurité aux entrées sélectionnées

Condition préalable : les entrées auxquelles les profils seront attribués ont été identifiées et se trouvent dans le tableau figurant dans la partie inférieure de la boîte de dialogue.
Notez que chaque entrée se compose généralement d'une porte ou d'une barrière plus un ou plusieurs lecteurs de cartes. Toutefois, certains types d'entrées spécifiques tels que **Points de rassemblement** peuvent ne pas en avoir.

1. Dans la colonne **Profil de sécurité de porte ou de lecteur**, cliquez sur la cellule correspondant à la porte ou au lecteur à laquelle ou auquel vous souhaitez attribuer un profil.
2. Sélectionnez un profil de sécurité de porte ou de lecteur dans la liste déroulante de la cellule.

(Facultatif) Prévisualisation du comportement des portes et des lecteurs aux différents niveaux de menace

Les colonnes figurant dans la partie droite du tableau sont en lecture seule. Elles indiquent le statut de verrouillage (**Mode**), le **niveau de sécurité** et le **taux de surveillance** des portes et des lecteurs du tableau tels qu'ils seraient si le niveau de menace sélectionné dans la liste **Select threat level for details (Sélectionnez le niveau de menace pour plus de détails)** était activé.

Condition préalable : les entrées que vous souhaitez prévisualiser ont été identifiées et figurent dans le tableau, dans la partie inférieure de la boîte de dialogue.

- Dans la liste **Select threat level for details (Sélectionnez le niveau de menace pour plus de détails)**, sélectionnez le niveau de menace que vous souhaitez prévisualiser.

⇨ Le tableau montre le statut du verrouillage (**Mode**) des portes, ainsi que le **niveau de sécurité** et le **taux de surveillance** des lecteurs tels qu'ils seraient si le niveau de menace sélectionné était activé.

19.3.5 Attribution d'un niveau de menace à un signal matériel

Cette section explique comment faire en sorte qu'un signal d'entrée matériel déclenche ou annule une alerte de menace.

Chemin d'accès à la boîte de dialogue

– **Menu principal** >**Configuration** > **Données du dispositif**

Conditions préalables

– Au moins un niveau de menace a été défini.
– Au moins une entrée a été configurée dans l'arborescence des périphériques.

Procédure

1. Dans l'arborescence des périphériques, sous le contrôleur AMC, sélectionnez l'**entrée** à laquelle vous souhaitez attribuer les signaux.
2. Dans la fenêtre de la boîte de dialogue principale, sélectionnez l'onglet **Terminals (Terminaux)**.
   – Le tableau des entrées et des signaux s'affiche.
3. Sur la ligne du signal que vous souhaitez attribuer, cliquez sur la cellule **Input signal (Signal d'entrée)**.
   – La liste déroulante contient la commande **Threat level: Deactivate (Niveau de menace : désactiver)** ainsi qu'un **Threat level: (Niveau de menace :)**`<name>` pour chaque niveau de menace que vous avez précédemment défini.
   – La commande **Threat level: Deactivate (Niveau de menace : désactiver)** annulera tous les niveaux de menace actuellement activés.
4. Attribuez les commandes aux signaux d'entrée souhaités.
5. Cliquez sur  (Enregistrer) pour enregistrer les modifications.

Remarque!

Restriction pour DM 15

Le modèle de porte 15 (DIP/DOP) ne peut actuellement pas être utilisé pour déclencher un niveau de menace.

19.4 Étapes de configuration dans les boîtes de dialogue des données système

Cette section explique comment créer des **profils de sécurité des personnes** et les attribuer à des **types de personnes**.

19.4.1 Création d'un profil de sécurité des personnes

Chemin d'accès à la boîte de dialogue

– **Menu principal** > **System data (Données système)** > **Person security profile (Profil de sécurité des personnes)**

Conditions préalables

Les profils de sécurité des personnes demandent à être minutieusement planifiés et spécifiés à l'avance, car ils auront des conséquences importantes sur le fonctionnement du système dans les situations critiques.

Procédure

1. Si la boîte de dialogue contient déjà des données, cliquez sur  (New [Nouveau]) pour les effacer.
2. Dans le champ de texte Security profile name (Nom du profil de sécurité), entrez le nom du nouveau profil.
3. (Facultatif) Entrez une description du profil pour aider les opérateurs à attribuer correctement celui-ci.
4. Dans le champ **Security level (Niveau de sécurité)**, entrez un entier entre 0 et 100.
   – Dans la mesure où le détenteur de la carte est autorisé à emprunter une entrée, le chiffre 100 est suffisant pour que n'importe quel lecteur lui accorde l'accès, même si son niveau de sécurité est également actuellement défini sur 100.
   – Sinon, le niveau de sécurité du profil de sécurité des personnes d'un détenteur de carte doit être égal ou supérieur au niveau de sécurité actuel du lecteur.
5. Dans le champ **Screening rate (Taux de surveillance)**, entrez un entier entre 0 et 100.
   – **Remarque** : le taux de surveillance du profil des personnes a moins d'importance que celui du profil des lecteurs. Le tableau ci-dessous décrit l'interaction entre les deux taux de surveillance des profils.
6. Cliquez sur  (Enregistrer) pour enregistrer les modifications.

Interaction des taux de surveillance pour les profils de sécurité des personnes et des lecteurs

Taux de surveillance (%) des profils de sécurité de lecteur R	Taux de surveillance (%) des profils de sécurité des personnes P	Personne sélectionnée pour des contrôles de sécurité supplémentaires ?
0	Indifférent	**Non**
100	Indifférent	**Oui**
1..99	0	**Non**
1..99	100	**Oui**

Taux de surveillance (%) des profils de sécurité de lecteur R	Taux de surveillance (%) des profils de sécurité des personnes P	Personne sélectionnée pour des contrôles de sécurité supplémentaires ?
1..99	1..99	**Possiblement** Probabilité = MAX (R, P)

19.4.2 Attribution d'un profil de sécurité des personnes à un type de personne

Chemin d'accès à la boîte de dialogue

– **Menu principal** >**System data (Données système)** > **Person Type (Type de personne)**

Procédure

Remarque : pour des raisons historiques, **Employee ID (Identifiant de l'employé)** est ici synonyme de **Person type (Type de personne)**.

1. Dans le tableau **Predefined employee IDs (Identifiants prédéfinis d'employés)** ou le tableau **User-defined employee IDs (Identifiants d'employé définis par l'utilisateur)**, dans la colonne **Security profile name (Nom du profil de sécurité)**, sélectionnez la cellule correspondant au type de personne souhaité.
2. Sélectionnez un profil de sécurité des personnes dans la liste déroulante.
   – Répétez cette procédure pour tous les types de personnes pour lesquels un profil de sécurité des personnes est nécessaire.
3. Cliquez sur  (Save [Enregistrer]) pour enregistrer vos affectations.

19.5 Étapes de configuration dans les boîtes de dialogue des données du personnel

Cette section explique comment les nouveaux enregistrements **Personne** créés dans le système se voient attribuer un **profil de sécurité des personnes** via leur **type de personne**.

Chemins d'accès aux boîtes de dialogue

– **Menu principal** > **Personnel data (Données du personnel)** > **Persons (Personnes)**
– **Menu principal** > **Personnel data (Données du personnel)** > **Group of Persons (Groupe de personnes)**

Remarque : pour des raisons historiques, **Employee ID (Identifiant de l'employé)** est ici synonyme de **Person type (Type de personne)**.

Procédure

Tous les enregistrements **Personne** créés dans le système doivent comporter un **type de personne**.

1. Veillez à ce que les opérateurs système attribuent uniquement des **types de personnes** ayant été associés à un **profil de sécurité des personnes** dans la boîte de dialogue **Menu principal** > **System data (Données système)** > **Person Type (Type de personne)**.
2. Pour plus de détails sur l'association des **profils de sécurité des personnes** et la création d'enregistrements **Personne**, cliquez sur les liens suivants.

Se reporter à

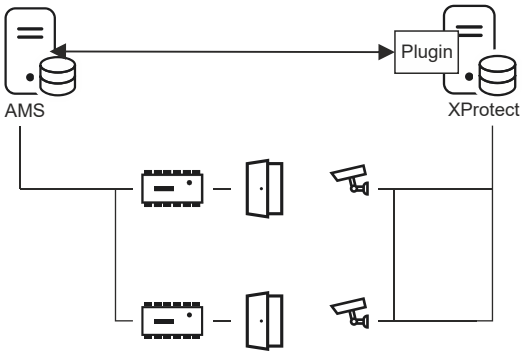
– *Attribution d'un profil de sécurité des personnes à un type de personne, page 147*
– *Création et gestion des données du personnel, page 198*

20 Configuration de Milestone XProtect pour utiliser AMS

Introduction

Ce chapitre explique comment configurer Milestone XProtect pour utiliser les fonctionnalités de contrôle d'accès d'AMS.

Un plugin fourni par AMS, mais installé sur le serveur XProtect, transmet les événements et les commandes à AMS et renvoie les résultats à XProtect.



La configuration comporte 3 étapes, décrites dans les sections suivantes :

- Installation du certificat public d'AMS sur le serveur XProtect.
- Installation du plugin AMS sur le serveur XProtect.
- Configuration d'AMS dans l'application XProtect.

Remarque!

Incompatibilité potentielle des plug-ins de différentes sources

Les plugins Milestone XProtect ne sont pas en bac à sable, c'est-à-dire qu'ils ne sont pas complètement isolés les uns des autres. Pour cette raison, des erreurs logicielles peuvent se produire si vous exécutez plusieurs plug-ins avec différentes versions de .NET et leurs dépendances sur le même serveur XProtect. BOSCH ne peut garantir le bon fonctionnement du plug-in AMS que s'il s'agit du seul plug-in installé.

Conditions préalables

- AMS est installé et concédé sous licence.
- XProtect est installé et concédé sous licence sur le même ordinateur ou sur son propre ordinateur.
- Une connexion réseau existe entre les deux systèmes.

Installation du certificat public d'AMS sur le serveur XProtect

Notez que cette procédure n'est requise que si AMS s'exécute sur un autre ordinateur.

1. Copiez le fichier de certificat du serveur AMS
   `C:\Program Files (x86)\Bosch Sicherheitssysteme\Access Management System\Certificates\Access Management System Internal CA.cer`
   sur le serveur XProtect.
2. Sur le serveur XProtect, double-cliquez sur le fichier de certificat.
   L'assistant de certificat apparaît.
3. Cliquez sur **Install Certificate... (Installer le certificat...)**
   L'assistant d'importation de certificat apparaît.

4. Sélectionnez **Local Machine (Ordinateur local)** comme **Store Location (Emplacement de stockage)**, puis cliquez sur **Next (Suivant)**.
5. Sélectionnez **Place all certificates... (Placer tous les certificats...)**.
6. Cliquez sur **Browse... (Parcourir...)**.
7. Sélectionnez **Trusted Root Certification Authorities (Autorités de certification racines de confiance)**, puis cliquez sur **OK**.
8. Cliquez sur **Next (Suivant)**.
9. Vérifiez l'ensemble des paramètres, puis cliquez sur **Finish (Terminer)**.

Installation du plugin AMS sur le serveur XProtect

1. Copiez le fichier de configuration
   `AMS XProtect Plugin Setup.exe`
   qui se trouve sur le support d'installation d'AMS sur le serveur XProtect.
2. Exécutez le fichier sur le serveur XProtect.
   L'assistant de configuration apparaît.
3. Dans l'assistant de configuration, assurez-vous que le plugin AMS XProtect est marqué pour installation, puis cliquez sur **Next (Suivant)**.
   Le contrat de licence utilisateur final s'affiche. Cliquez sur **Accept (Accepter)** pour accepter le contrat si vous souhaitez poursuivre.
4. L'assistant affiche le chemin d'installation par défaut du plugin. Cliquez sur **Next (Suivant)** pour accepter le chemin par défaut ou sur **Browse (Parcourir)** pour le modifier avant de cliquer sur **Suivant**.
   L'assistant confirme qu'il est sur le point d'installer le plugin AMS XProtect.
5. Cliquez sur **Install (Installer)**.
6. Attendez la confirmation de la fin de l'installation, puis cliquez sur **Finish (Terminer)**.
7. Redémarrez le service Windows nommé **Milestone XProtect Event Server (Serveur d'événements Milestone XProtect)**.

Configuration d'AMS dans l'application XProtect

1. Dans l'application de gestion XProtect, accédez à **Advanced Configuration (Configuration avancée)** > **Contrôle d'accès (Access Control)**.
2. Cliquez avec le bouton droit sur **Access Control (Contrôle d'accès)**, puis sélectionnez **Create new... (Créer...)**
   .L'assistant du plugin apparaît.
3. Entrez les informations suivantes dans l'assistant du plugin :
   - **Name (Nom)** : description de l'intégration AMS-XProtect afin de la distinguer des autres intégrations sur le même système XProtect
   - **Integration plug-in (Plugin d'intégration)** : `AMS - XProtect Plugin` Ce nom figurera dans la liste déroulante une fois l'installation du plugin correctement effectuée
   - **AMS API discovery endpoint (Point de terminaison de la détection de l'API AMS)** : `https://<hostname of the AMS system>:44347/`
     où `44347` correspond au port sélectionné par défaut lors de l'installation de l'API AMS
   - **Operator name (Nom de l'opérateur)** : nom d'utilisateur de l'opérateur AMS disposant au moins des autorisations d'utilisation des portes auxquelles les caméras XProtect seront mappées.

- **Operator password (Mot de passe de l'opérateur)** : mot de passe AMS de l'opérateur.

4. Cliquez sur **Next (Suivant)**.
   Le plugin AMS se connecte au serveur AMS que vous avez spécifié et répertorie les éléments de contrôle d'accès détectés (portes, unités, serveurs, commandes d'événements et états).
5. Une fois la barre de progression entièrement remplie, cliquez sur **Next (Suivant)** **.**La page **Associate cameras (Caméras associées)** de l'assistant apparaît.
6. Pour associer des caméras aux portes, faites glisser des caméras de la liste **Cameras (Caméras)** vers des points d'accès de la liste **Doors (Portes)**.
7. Lorsque vous avez terminé, cliquez sur **Next (Suivant)**.
   XProtect enregistre la configuration et affiche un message de confirmation une fois l'enregistrement correctement réalisé.

21 Intégration d'Otis Compass

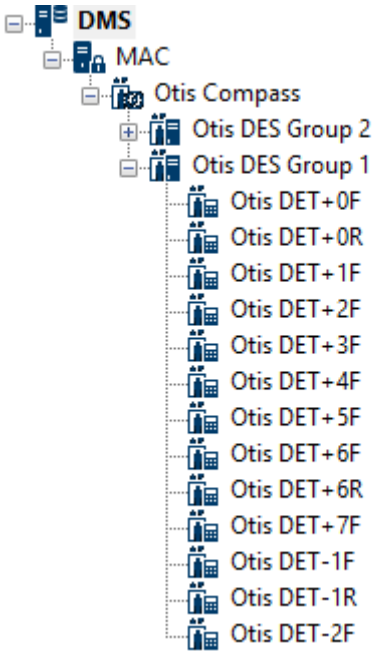
Introduction

Compass est un système de gestion de destination d'Otis Elevator Company. Sa fonction est de gérer plusieurs groupes d'ascenseurs, en répartissant les ascenseurs entre les passagers afin qu'ils puissent atteindre leur destination le plus efficacement possible. Pour fournir les données nécessaires, les passagers n'appuient plus simplement sur les touches **Up (Vers le haut)** ou **Down (Vers le bas)**, mais ils indiquent leurs destinations au niveau des terminaux à lecteur de carte, à écran tactile ou à clavier.

L'intégration avec les systèmes de contrôle d'accès Bosch renforce la sécurité. En fonction des informations d'identification et des modèles horaires en vigueur, les passagers sont transportés vers leur étage et vers d'autres destinations autorisées de manière efficace. Le système n'accepte pas les demandes d'étages qui ne figurent pas dans les profils d'autorisation du passager ou à une heure de la journée absente du modèle horaire en vigueur.

Topologie matérielle d'un système Compass

Le matériel d'un système Compass est configuré de manière descendante comme une hiérarchie à 3 niveaux sous un seul MAC dans l'éditeur de dispositif.



La hiérarchie supérieure indique :
Un système **Otis Compass** sur un MAC dédié
Un seul groupe d'ascenseurs régi par un seul **DES**
Un certain nombre de terminaux (**DET**), chacun avec un numéro d'étage de -2 à +7, F ou R faisant référence aux portes avant ou arrière respectivement.

Premier niveau : (Otis Compass)
Le système de gestion des destinations. Chaque système **Compass** peut régir jusqu'à 8 groupes d'ascenseurs (également connus sous le nom de banques d'ascenseurs).
Paramètres : plage d'étages,
adresses réseau,
numéros de port et délais d'attente.

Deuxième niveau : (Otis DES/DER)
Jusqu'à 8 groupes d'ascenseurs, chacun géré par un serveur DES (Destination Entry Server) composé d'un ou de deux dispositifs physiques.
De plus, ce niveau peut avoir jusqu'à 2 dispositifs en option pour l'optimisation, appelésdispositifs DER (Destination Entry Server).
Paramètres : 1 identifiant de groupe par groupe d'ascenseurs.
1 adresse IP par dispositif.
Le tableau des étages avec portes d'ascenseur, et s'ils sont accessibles au public.

Troisième niveau : Otis DET
Les terminaux DET (Destination Entry Terminals)

	Paramètres : 1 adresse IP par terminal. Étages atteignables avec portes d'ascenseur pour chaque terminal.

Vue d'ensemble de l'intégration dans le système de contrôle d'accès

Les administrateurs du système de contrôle d'accès intègrent Compass dans les étapes suivantes, décrites en détail plus loin dans le chapitre :

1. Configurez le matériel Compass sur un seul MAC dans l'éditeur de dispositif.
2. Configurez des champs personnalisés pour les propriétés de détenteur de carte spécifiques à Otis, telles que l'étage de la maison.
3. Créez des profils d'autorisation qui régissent l'accès à des destinations d'ascenseur spécifiques.
4. Affectez des profils d'autorisation aux détenteurs de carte appropriés

21.1 Configuration d'un système Compass dans l'éditeur de dispositif

Cette section décrit les étapes de configuration d'un système Otis Compass dans l'éditeur de dispositif.

Chemin d'accès à la boîte de dialogue

– **Menu principal** >**Configuration** > **Données du dispositif**

21.1.1 Niveau 1 : Configuration du système Compass

Procédure pour le niveau 1 : Configuration du système Compass

1. Sélectionnez le MAC souhaité dans l'arborescence de l'éditeur de dispositif
2. Effectuez un clic droit et sélectionnez **New Otis Compass (Nouveau système Otis Compass)**. La page des propriétés comporte 2 onglets.
   – **Otis Compass**
   – **Floors (Étages)**
3. Sur l'onglet **Otis Compass**, les paramètres les plus importants à définir sont les suivants :
   – **Name (Nom)** (nom qui doit figurer dans l'arborescence des dispositifs)
   – **MAC IP-Address (Adresse IP MAC)** (adresse IP de rappel du système Compass, sur une carte réseau dédiée, grâce à laquelle le système Compass communique avec le MAC).
     REMARQUE : Il ne s'agit **pas** de l'adresse IP du MAC lui-même.
   – **Division** (si et seulement si les divisions sont sous licence et utilisées dans votre installation)

Conservez le reste des paramètres sur leurs valeurs par défaut à moins que le support technique expert ne vous demande de les modifier. Ces paramètres sont brièvement décrits dans le tableau suivant :

Paramètre	Valeur par défaut	Description
Adresse du groupe MC	234.46.30.7	Adresse IP du groupe multicast
Port MC pour DES/DER distant Port MC pour DES / DER local	48307 47307	Ports de multidiffusion
Port UDP pour DES/DER distant Port UDP pour DES/DER local	46303 45303	Ports UDP pour les dispositifs DES et DER
Port UDP pour DET distant Port UDP pour DET local	45308 46308	Ports UDP pour les dispositifs DET
TTL (time-to-live) en multidiffusion	5 secondes	
Intervalle de battements de cœur	1 secondes	La quantité de temps entre les signaux de battements de cœur. Ces signaux indiquent aux autres dispositifs qu'un appareil est « vivant » c'est-à-dire qu'il fonctionne
Nombre maximum de battements de cœur manqués	3	Nombre de battements de cœur qui peuvent être manqués avant qu'un dispositif soit considéré comme « mort » (qui ne fonctionne plus)
Expiration du message	1 secondes	
Nouvelles tentatives de message	3	

1. Sous l'onglet **Floors (Étages)**, cliquez sur **Change floor range (Modifier la plage d'étages)**
2. Entrez les numéros des étages inférieurs et supérieurs qui doivent être desservir par tous les ascenseurs du système Otis Compass.
   – La plage maximale est de -127 à +127
3. Cliquez sur  (Enregistrer) pour enregistrer les modifications.

21.1.2 Niveau 2 : Groupes d'ascenseurs, dispositifs DES et DER

Procédure pour le niveau 2 : Configuration des groupes d'ascenseurs (dispositifs DES/ DER)

Introduction

Le serveur DES (Destination Entry Server) est l'ordinateur qui gère un groupe d'ascenseurs. Si vous le souhaitez, deux dispositifs DES physiques avec des adresses IP distinctes peuvent être combinés dans un serveur DES logique, avec une capacité de basculement.

Le dispositif DER (Destination Entry Redirector) connecte les groupes d'ascenseurs et permet aux terminaux DET au niveau d'un point d'entrée commun du bâtiment, par exemple le hall, d'accepter les demandes de destination pour n'importe quel étage du bâtiment. Le dispositif DER n'est pas configuré pour agir en mode de basculement.

Création de dispositifs DES dans l'arborescence de dispositifs :

1. Sélectionnez le système Otis Compass souhaité dans l'arborescence de l'éditeur de dispositif
2. Effectuez un clic droit et sélectionnez **New Otis DES (Nouveau dispositif Otis DES)**. La page des propriétés comporte 2 onglets :
   - **Otis DES**
   - **Floors (Étages)**
3. Sous l'onglet **Otis DES**, définissez les paramètres suivants :
   - **Name (Nom)** : nom qui doit figurer dans l'arborescence des dispositifs. Utilisez un schéma de nommage systématique qui fournira une orientation claire pour les configurateurs de dispositifs DES et DET plus tard dans le processus de configuration.
   - **Description :** (facultatif) description en texte libre du dispositif.
   - **Group (Groupe) :** entier de 1 à 10**.** Définissez un entier unique dans tous les groupes d'ascenseurs (désignés par leurs dispositifs DES/DER) au sein de ce système Otis Compass. Vous ne pourrez pas enregistrer les modifications de votre dispositif si vous utilisez le même numéro de **Groupe** plus d'une fois.
   - **1st IP address (1ère adresse IP) :** adresse IP de ce dispositif DES.
   - **2nd IP address (2ème adresse IP) :** si ce dispositif DES a un jumeau redondant, entrez son adresse IP ici.
   - **Division** (si et seulement si les divisions sont sous licence et utilisées dans votre installation)

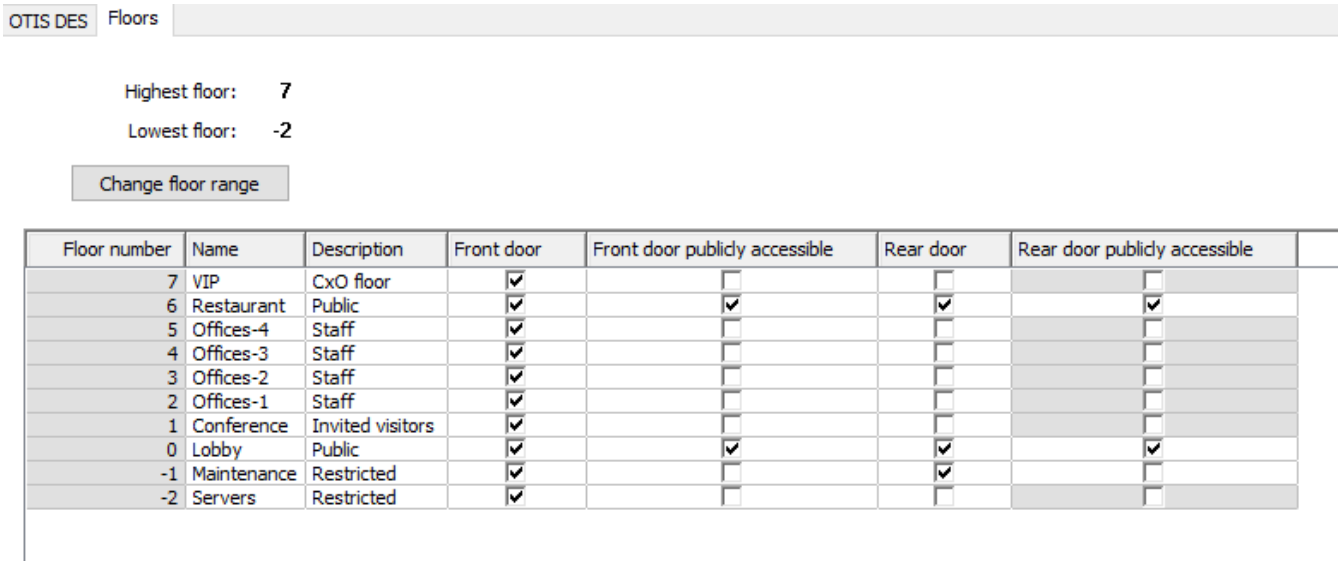
Sous l'onglet **Floors (Étages)**, les étages définis pour le niveau 1 (système Compass) sont présentés sous la forme d'un tableau de cellules modifiables.

Création de dispositifs DER dans l'arborescence de dispositifs :

Les dispositifs DER sont créés presque de la même manière que les dispositifs DES. La seule différence est qu'un dispositif DER n'a besoin d'aucun dispositif de basculement, il n'a donc pas de paramètre pour **2nd IP address (2e adresse IP)**.

Exemple de groupe d'ascenseurs.

L'exemple ci-dessous illustre les étages d'un groupe d'ascenseurs de 10 étages, avec des portes avant et arrière, un rez-de-chaussée et des 6e étages accessibles au public.



Floor number	Name	Description	Front door	Front door publicly accessible	Rear door	Rear door publicly accessible
7	VIP	CxO floor	☑	☐	☐	☐
6	Restaurant	Public	☑	☑	☑	☑
5	Offices-4	Staff	☑	☐	☐	☐
4	Offices-3	Staff	☑	☐	☐	☐
3	Offices-2	Staff	☑	☐	☐	☐
2	Offices-1	Staff	☑	☐	☐	☐
1	Conference	Invited visitors	☑	☐	☐	☐
0	Lobby	Public	☑	☑	☑	☑
-1	Maintenance	Restricted	☑	☐	☑	☐
-2	Servers	Restricted	☑	☐	☐	☐

1. Dans la colonne **Front door (Porte avant)**, cochez les cases de tous les étages où l'ascenseur propose l'utilisation de sa porte avant.
2. Cochez les cases de la même manière pour la colonne **Rear door (Porte arrière)**, le cas échéant.
3. Pour la colonne **Front door publicly accessible (Porte d'entrée accessible au public)**, cochez les cases des étages accessibles à tous les passagers des ascenseurs sans restriction.
4. Cochez les cases de la même manière pour la colonne **Rear door publicly accessible (Porte arrière accessible au public)**, le cas échéant.
5. (facultatif) Cliquez sur **Change floor range (Modifier la plage d'étages)** sous cet onglet afin de limiter davantage la plage d'étages qui a été définie au niveau **Otis Compass**.
6. Remplacez les noms par défaut figurant dans les colonnes **Name (Nom)** et **Description** par des valeurs alternatives significatives.
7. Cliquez sur  (Enregistrer) pour enregistrer les modifications.

21.1.3 Niveau 3 : dispositifs DET

Procédure pour le niveau 3 : Mise en place des terminaux (dispositifs DET)
Introduction :
Un dispositif DET (également connu sous le nom de DEC, Destination Entry Computer) lit les informations d'identification physiques ou les codes PIN. Un dispositif DET peut être situé à un étage particulier à l'extérieur de la porte avant ou arrière d'un ascenseur, ou à l'intérieur de la cabine d'ascenseur.

Création de dispositifs DET dans l'arborescence de dispositifs :
1. Sélectionnez le dispositif Otis DES/DER souhaité dans l'arborescence de l'éditeur de dispositif.
2. Effectuez un clic droit et sélectionnez **New Otis terminal (Nouveau terminal Otis)**.
   – Une fenêtre contextuelle **Create Otis terminals (Créer des terminaux Otis)** apparaît
3. Saisissez le nombre de terminaux que vous souhaitez configurer sur ce dispositif DES/DER.

4. Acceptez les valeurs par défaut ou entrez de nouvelles valeurs de départ pour les quatre octets de son adresse IP.
   – Pour n'importe quel octet, mais en général pour le 4e, cochez la case **Automatic increment (Incrément automatique)** si vous souhaitez que le système configure une adresse IP unique pour chaque terminal en incrémentant l'octet.
5. Cliquez sur **OK**.
   – Le nombre souhaité de dispositifs DET est créé dans l'arborescence des dispositifs.
   – Leurs adresses IP sont incrémentées comme déterminé à l'étape précédente.

Configuration des dispositifs DET

La page de propriétés de chaque dispositif DET comporte 2 onglets :

– **Otis terminal (Terminal Otis)**
– **Floors (Étages)**

1. Sous l'onglet **Otis terminal (Terminal Otis)**, définissez les paramètres suivants :
   – **Name (Nom) :** nom qui doit figurer dans l'arborescence des dispositifs
   – **Description** (facultatif) description en texte libre du dispositif.
   – **IP address (Adresse IP)** Adresse IP de ce dispositif DET
   – **Operational mode (Mode de fonctionnement) :** `1..4`
   Cela détermine comment le terminal demande des destinations au passager de l'ascenseur et transmet les demandes au dispositif DES/DER pour validation. Le tableau suivant fournit des détails :

Mode de fonctionnement	Description	Comportement
1	Étage par défaut	(Mode de fonctionnement par défaut) Le passager présente son badge ou entre un code PIN. Si le badge ou le code PIN est valide et que le passager n'effectue aucune autre entrée, le dispositif DET demande au dispositif DES l'étage par défaut ou l'étage « initial » du passager. Si le passager entre un étage de destination différent, alors le dispositif DET demande cette destination au dispositif DES.
2	Accès aux étages autorisés	Le passager présente son badge ou entre un code PIN, puis entre un étage de destination. Le dispositif DET demande cette destination au dispositif DES. Le système de contrôle d'accès accorde ou refuse l'accès à la destination demandée.
3	Saisie par l'utilisateur de l'étage de destination	Le passager saisit un étage de destination. Si la destination est accessible au public, le dispositif DET demande la destination au dispositif DES. Dans le cas contraire, le dispositif DET demande au passager de présenter son badge pour validation.

Mode de fonctionnement	Description	Comportement
4	Étage par défaut ou saisie utilisateur de l'étage de destination.	Le passager présente son badge ou entre un code PIN. Si le badge ou le code PIN est valide, le dispositif DET demande au dispositif DES l'étage par défaut ou « initial » du passager. Dans un délai d'attente défini, le passager peut annuler la sélection de l'étage par défaut et choisir une destination différente.

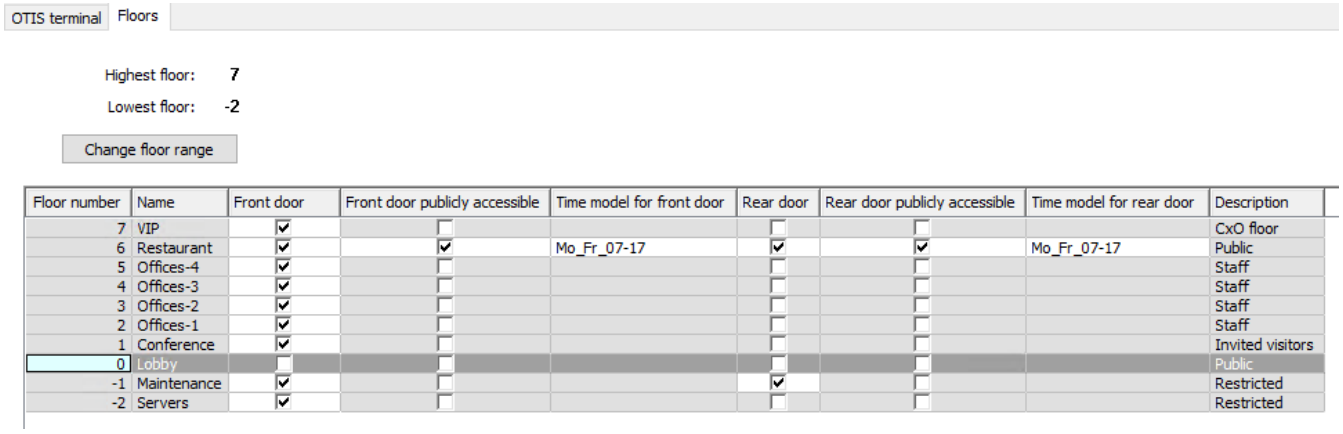
- **Audit records (Enregistrements d'audit) :** Cochez cette case pour enregistrer les saisies des passagers sur ce terminal pour le journal des événements.
- **PIN code (Code PIN) :** Cochez cette case pour autoriser l'utilisation d'un code PIN d'identification sur ce terminal comme alternative aux informations d'identification physiques.
  Remarque : Utilisez des lecteurs d'inscription de type **Carte PIN de dialogue (saisir)** pour inscrire des codes PIN à utiliser sur les terminaux Otis.
- **Time models (Modèles horaires) :** Cochez cette case pour permettre aux modèles horaires de restreindre les heures pendant lesquelles ce terminal peut être utilisé.
- **Division** (si et seulement si les divisions sont sous licence et utilisées dans votre installation)

Sous l'onglet **Floors (Étages)** de la page des propriétés du **terminal Otis**, les étages que vous avez définis pour le niveau 2 (DES/DER) sont présentés sous la forme d'un tableau de cellules modifiables.
Remarque : Le schéma de nommage défini pour le niveau 2 ci-dessus devrait fournir une orientation suffisante. Si ce n'est pas le cas, nous vous recommandons d'enregistrer votre travail et de revenir au niveau 2 pour terminer le schéma de nommage.

1. Sélectionnez tour à tour chaque dispositif DET que vous venez de créer dans l'arborescence des dispositifs, et ouvrez l'onglet **Floors (Étages)**.
   - Le tableau **Floors (Étages)** s'affiche
2. Dans la colonne **Front door (Porte avant)**, cochez la case de chaque étage qui doit être accessible depuis le dispositif DET actuel.
3. Dans la colonne **Front door publicly accessible (Porte d'entrée accessible au public)**, cochez la case de chaque porte d'entrée qui doit être accessible au public, c'est-à-dire sans autorisation explicite.
4. (facultatif) Dans la colonne **Time model for front door (Modèle horaire pour la porte d'entrée)**, sélectionnez un modèle horaire pour restreindre l'accès du public à la porte d'entrée à cet étage, si nécessaire. Par exemple, l'étage du restaurant peut n'être accessible qu'à certains moments de la journée.
5. Recommencez les étapes précédentes, si nécessaire, pour les colonnes **Rear door (Porte arrière)**, **Rear door publicly accessible (Porte arrière accessible au public)** et **Time model for rear door (Modèle horaire pour la porte arrière).**
6. Cliquez sur  (Enregistrer) pour enregistrer les modifications.

Exemple :

L'exemple ci-dessous présente les étages d'un groupe d'ascenseurs de 10 étages, avec les étages et portes accessibles depuis la porte d'ascenseur avant dans le hall. L'accès à l'étage du restaurant, aux portes d'ascenseur avant et arrière, est limité par un modèle horaire.



Floor number	Name	Front door	Front door publicly accessible	Time model for front door	Rear door	Rear door publicly accessible	Time model for rear door	Description
7	VIP	☑	☐		☐	☐		CxO floor
6	Restaurant	☑	☑	Mo_Fr_07-17	☑	☑	Mo_Fr_07-17	Public
5	Offices-4	☑	☐		☐	☐		Staff
4	Offices-3	☑	☐		☐	☐		Staff
3	Offices-2	☑	☐		☐	☐		Staff
2	Offices-1	☑	☐		☐	☐		Staff
1	Conference	☑	☐		☐	☐		Invited visitors
0	Lobby	☐	☐		☐	☐		Public
-1	Maintenance	☑	☐		☑	☐		Restricted
-2	Servers	☑	☐		☐	☐		Restricted

21.2 Configuration des champs personnalisés pour les propriétés des détenteurs de carte spécifiques à Otis

Introduction

Cette section décrit comment créer des champs personnalisés dans lesquels un opérateur peut saisir les propriétés spécifiques à Otis pour un détenteur de carte, en particulier la destination « initiale » ou la destination par défaut du détenteur de carte. Cette destination « initiale » doit être définie par **trois coordonnées** :

1. Groupe d'ascenseurs,
2. Étage
3. Porte

Notez que lorsqu'il spécifie un étage d'accueil pour un détenteur de carte dans le client du système de contrôle d'accès, un opérateur doit saisir ces données dans le même ordre : groupe d'ascenseur, étage, porte. Pour cette raison, les trois champs personnalisés doivent être positionnés dans l'ordre de lecture, de préférence de haut en bas.

Cliquez sur **OK** pour confirmer les rappels contextuels que vous devez créer les trois coordonnées.

Définissez les 3 champs personnalisés nécessaires, ainsi que toutes les options Otis spéciales dont vous avez besoin, qui doivent figurer sous l'onglet **Elevators (Ascenseurs)** de l'interface client de contrôle d'accès.

Pour obtenir des informations générales sur la configuration des champs personnalisés, consultez l'aide sur la configuration ACE/AMS concernant les **Champs personnalisés pour les données du personnel**.

Chemin d'accès à la boîte de dialogue

Menu principal >**Configuration** > **Options** > **Custom fields (Champs personnalisés)**

Procédure

Sur la page de propriétés **Custom fields (Champs personnalisés)**, sélectionnez l'onglet **Elevators (Ascenseurs)**.

Première coordonnée : groupe d'ascenseurs

1. Double-cliquez sur une cellule de l'onglet et cliquez sur **Yes (Oui)** pour créer un nouveau champ de saisie.

2. Dans la liste **Field type (Type de champ)**, sélectionnez **Otis DES selection (Sélection Otis DES)**.
3. Dans le champ **Label (Libellé)**, entrez `Elevator Group`
4. Dans la liste **Display in (Affichage dans)**, sélectionnez `Tab:Elevators`
5. Dans le groupe **Position**, sélectionnez un emplacement unique sous l'onglet **Elevators (Ascenseurs)**, où ce champ personnalisé doit apparaître.

Deuxième coordonnée : étage d'accueil

1. Cliquez sur **New field (Nouveau champ)** pour créer de nouveaux champs personnalisés
2. Dans la liste **Field type (Type de champ)**, sélectionnez **Home floor (Étage d'accueil)**.
3. Dans le champ **Label (Libellé)**, entrez `Home floor`
4. Dans la liste **Display in (Affichage dans)**, sélectionnez `Tab:Elevators`
5. Dans le groupe **Position**, sélectionnez un emplacement unique sous l'onglet **Elevators (Ascenseurs)**, où ce champ personnalisé doit apparaître. Pour simplifier l'utilisation par les opérateurs du système, il doit se trouver au-dessous de la coordonnée précédente.

Troisième coordonnée : porte de sortie

1. Cliquez sur **New field (Nouveau champ)** pour créer de nouveaux champs personnalisés
2. Dans la liste **Field type (Type de champ)**, sélectionnez **Exit door (Porte de sortie)**.
3. Dans le champ **Label (Libellé)**, entrez `Exit door`
4. Dans la liste **Display in (Affichage dans)**, sélectionnez `Tab:Elevators`
5. Dans le groupe **Position**, sélectionnez un emplacement unique sous l'onglet **Elevators (Ascenseurs)**, où ce champ personnalisé doit apparaître. Pour simplifier l'utilisation par les opérateurs du système, il doit se trouver au-dessous de la coordonnée précédente.

Options spéciales Otis pour les détenteurs de carte

Introduction

Huit options binaires spécifiques à Otis sont fournies conformément à la fonctionnalité Otis standard. S'il sont définis en tant que champs personnalisés sous l'onglet **Elevators (Ascenseurs)**, ils apparaissent sous forme de cases à cocher sous l'onglet **Elevator data (Données d'ascenseur)** des détenteurs de carte dans la boîte de dialogue **Persons (Personnes)** (Menu principal > **Personnel data (Données du personnel)** > **Persons (Personnes)**). Ils peuvent ensuite être sélectionnés et effacés par les opérateurs du système de contrôle d'accès.

Configurez ces options uniquement selon les instructions de votre représentant Otis.

Procédure

1. Cliquez sur **New field (Nouveau champ)** pour créer de nouveaux champs personnalisés
2. Dans la liste **Field type (Type de champ)**, sélectionnez **Otis options (Options Otis)**.
3. Dans le champ **Label (Libellé)**, entrez votre propre libellé, par exemple `Otis flag 1` ou un libellé conformément à la documentation Otis.
4. Dans la liste **Display in (Affichage dans)**, sélectionnez `Tab:Elevators`
5. Dans la liste **Function type (Type de fonction)**, sélectionnez l'une des options de `OTIS option 1` à `OTIS option 8`
6. Dans le groupe **Position**, sélectionnez un emplacement unique sous l'onglet **Elevators (Ascenseurs)**, où cette case à cocher doit apparaître.
7. Cliquez sur  (Enregistrer) pour enregistrer les modifications.

21.3 Création et configuration des autorisations pour les ascenseurs Otis

Introduction

Cette section décrit comment inclure des droits d'accès pour les groupes d'ascenseurs Otis, les étages et les portes d'ascenseur dans une **Autorisation**.

Des **Autorisations** sont attribuées directement aux détenteurs de carte ou, plus communément, combinées à d'autres Autorisations dans des **Profils d'accès**, qui sont ensuite attribués aux détenteurs de carte.

Conditions préalables

Un système Otis Compass a été défini sur un MAC dans l'éditeur de dispositif. Il comporte un groupe d'ascenseurs (représenté par son dispositif DES) et des paires étage+porte (représentées par leurs dispositifs DET).

Chemin d'accès à la boîte de dialogue

Menu principal > **System data (Données système)** > **Authorizations (Autorisations)**

Procédure

1. Dans le champ **Authorization name (Nom de l'autorisation)**, saisissez le nom d'une autorisation existante ou cliquez sur  (Nouveau) pour créer une nouvelle autorisation.
2. Dans la liste **MAC**, sélectionnez le nom du MAC sur lequel le système Otis Compass a été créé.
3. Cliquez sur l'onglet **Otis elevator (Ascenseur Otis)**
4. Dans la liste **Otis elevators (Ascenseurs Otis)**, sélectionnez le dispositif DES/DER du groupe d'ascenseurs que vous souhaitez ajouter à l'Autorisation (Notez qu'une Autorisation ne peut contenir qu'un seul dispositif DES/DER).
   - Les étages du groupe d'ascenseurs sélectionné sont affichés dans le volet **Floors (Étages)**.
5. Dans les colonnes **Front door (Porte avant)** et **Rear door (Porte arrière)** du volet **Floors (Étages)**, sélectionnez les portes des étages qui doivent être incluses dans cette autorisation.
   - Notez que les étages et les portes qui n'ont **pas** été sélectionné pour ce groupe d'ascenseurs, lors de sa définition dans l'éditeur de dispositif, apparaissent en grisé et ne sont pas sélectionnable dans cette boîte de dialogue.
6. Vous pouvez aussi cliquer sur les boutons **Assign all floors (Affecter tous les étages)** et **Remove all floors (Retirer tous les étages)** pour sélectionner ou effacer tous les étages et toutes les portes à la fois.
7. Cliquez sur  (**Enregistrer**) pour enregistrer l'autorisation.

22 Configuration d'IDEMIA Universal BioBridge

Cette section décrit la configuration des dispositifs biométriques IDEMIA pour leur utilisation avec les systèmes de contrôle d'accès Bosch à l'aide de **MorphoManager** et de **BioBridge**.
Les sous-sections couvrent les tâches de configuration nécessaires dans les domaines suivants :

- Le système de contrôle d'accès Bosch
- MorphoManager
- Le client d'inscription BioBridge dans MorphoManager
- Les adaptations pour les différentes technologies et les différents formats de cartes

22.1 Configuration de BioBridge dans le système de contrôle d'accès Bosch

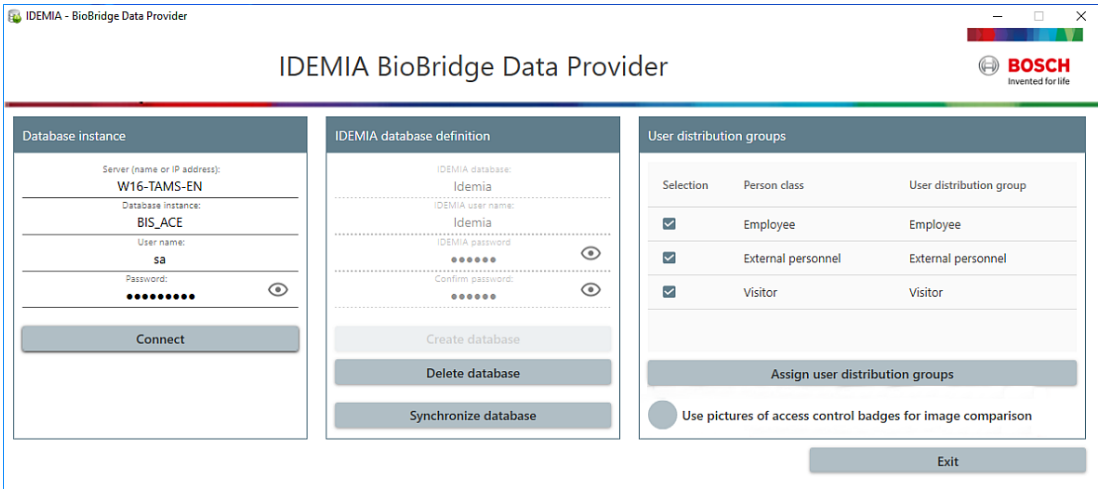
Les étapes suivantes sont effectuées dans ACS afin de créer la base de données qui relie les dispositifs biométriques IDEMIA au système de contrôle d'accès Bosch. La base de données mappe les entités de base de données suivantes entre elles :

- **Classe de personne** (Bosch)
- **Groupe de distribution d'utilisateurs** (IDEMIA).

Chemin d'accès à la boîte de dialogue

- Menu principal AMS > **Configuration** > **Outils** > **Configuration de la base de données IDEMIA**

1. Cliquez sur **Configuration IDEMIA database (Configuration de la base de données IDEMIA)**
   La boîte de dialogue **IDEMIA BioBridge Data Provider (Fournisseur de données IDEMIA BioBridge)** s'affiche.



2. Dans le volet **Database instance (Instance de base de données)**, saisissez les informations suivantes :

- **Server (Serveur)** : nom d'hôte ou adresse IP de l'ordinateur sur lequel l'instance de base de données SQL Server d' ACS est en cours d'exécution. Il peut s'agir du nom d'hôte local, si SQL Server s'exécute localement.
- **Database Instance (Instance de base de données)** : instance de l'ACS (par défaut, `ACE`).

- **Username (Nom d'utilisateur)** : nom du compte administrateur d base de données ACS (par défaut : `sa`)
- **Mot de passe** : mot de passe du compte administrateur, tel que configuré lors de l'installation d'ACS.

3. Cliquez sur **Connecter** pour tester la connexion. Tous les autres contrôles sont désactivés jusqu'à ce que réalisiez cette opération.

Dans le volet de définition de la base de données IDEMIA

Les deux premiers champs sont en lecture seule :

- **Idemia database (Base de données Idemia)** : nom de la base de données qui relie les données Bosch et IDEMIA.
- **Idemia username (Nom d'utilisateur Idemia)** : nom de l'utilisateur de base de données au nom duquel le logiciel exécute des commandes dans la base de données.

1. Entrez et confirmez un mot de passe fort pour **Idemia username (Nom d'utilisateur Idemia)**.
2. Notez soigneusement le mot de passe. Il sera demandé au cours des tâches de configuration futures et ne pourra pas être restauré en cas de perte.
3. Cliquez sur **Create database (Créer une base de données)**.
   Une boîte de message confirmera si la création a réussi. Cliquez sur **OK**
4. Lorsque les tests sont terminés avec succès, cliquez sur **Exit (Quitter)** pour fermer la boîte de dialogue.

Dans le volet User distribution groups (Groupes de distribution d'utilisateurs)

Les groupes de distribution d'utilisateurs sont des objets MorphoManager qui mappent les utilisateurs (détenteurs de badge) à des groupes de lecteurs biométriques ou de clients MorphoManager. Nous les mappons aux **classes de personne** des systèmes de contrôle d'accès Bosch.

1. Dans la colonne Select (Sélectionner), cochez la case de chaque ACE **classe de personne** utilisée par votre installation.
2. Pour chaque ligne que vous avez sélectionnée, copiez le nom de cette classe de personne dans la cellule correspondante de la colonne **User distribution group (Groupe de distribution d'utilisateurs)**.

- Notez que les noms des champs **Classe de personne** et **Groupe de distribution d'utilisateurs** doivent correspondre exactement.

3. Lorsque votre mappage est terminé, cliquez sur **Assign user distribution groups (Attribuer des groupes de distribution d'utilisateurs)**.

Fournir des photos d'identité pour la reconnaissance faciale VisionPass

Pour permettre aux lecteurs IDEMIA d'effectuer la reconnaissance faciale VisionPass à partir des photos d'identité des détenteurs de carte de la base de données ACE :

- Cliquez sur **Use pictures of access control badges for image comparison (Utiliser les photos de badges de contrôle d'accès pour la comparaison d'images)** et validez dans la fenêtre contextuelle.
  La fenêtre **IDEMIA BioBridge Data Provider (Fournisseur de données IDEMIA BioBridge)** s'affiche pour confirmer que la synchronisation est en cours.
  Notez que, selon la quantité de données d'image impliquée, le transfert peut prendre un temps considérable.

22.2 Sélection des technologies et formats de cartes

Introduction

Si vous avez l'intention d'utiliser des cartes ainsi que l'identification biométrique, vous devez créer un profil (ou « Profil Wiegand ») dans MorphoManager qui inclut le format (ou les formats) de ces cartes d'accès.

Le tableau suivant donne un aperçu des formats pris en charge. Notez que pour la technologie MIFARE, seule l'identificationCSN est prise en charge.

Card Family	HID Prox	HID Class	HID iClass Seos	MIFARE Classic	MIFARE DESFire EV0	MIFARE DESFire EV1
Card Variant	Prox	2k/2 16k/2 16k/16 32k(16k/2+16k/1) 32k(16k/16+16k/1)	Seos	1K 4-byte NUID 1k 7-byte UID 4k 4-byte NUID 4k 7byte UID	2k 4k 8k	2k 4k 8k

Figure 22.1: Cartes IDEMIA prises en charge

Procédure générale

1. Dans MorphoManager, accédez à **Administration** > **Wiegand Profile (Profil Wiegand)**
2. Cliquez sur **Add (Ajouter)** pour créer un profil Wiegand personnalisé
3. Dans les boîtes de dialogue associées, saisissez les informations de formatage et la technologie de carte utilisée par votre système
4. Afin d'utiliser votre nouveau profil Wiegand dans le système, entrez son nom dans le champ **Wiegand Profile (Profil Wiegand)** des boîtes de dialogue MorphoManager suivantes :

– **Administration > Biometric Device profile (Profil de dispositif biométrique)**
– **Administration > User policy (Politique utilisateur)**

Mifare Classic CSN

1. Ajoutez un élément Wiegand `User CSN Element` et entrez les détails suivants

– **Name (Nom)** : `CSN` (par exemple)
– **Length (Longueur)** `32`
– **Transformation mode (Mode de transformation) :** `Reversed`

2. **Sous Administration > Biometric Device profile (Profil de dispositif biométrique)**, sur la page **Multi-Factor Mode Settings (Paramètres du mode multifacteur)**, cochez la case **MIFARE classic**

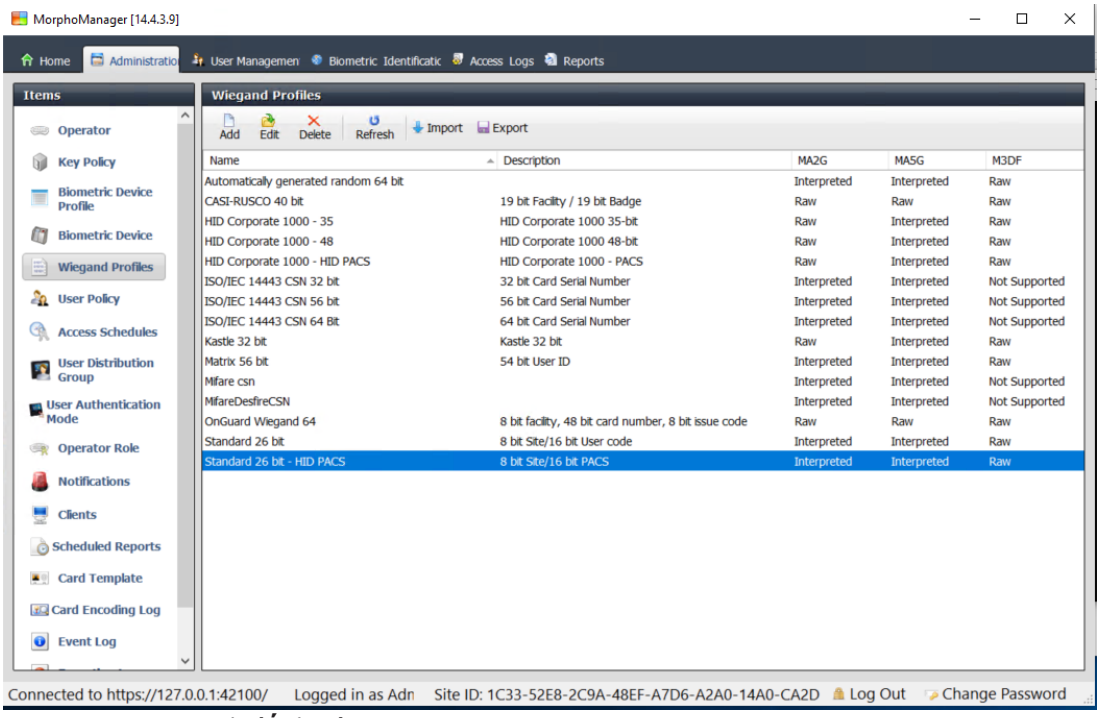
Mifare DESFire CSN

La configuration est identique à Mifare Classic à l'exception des détails suivants :

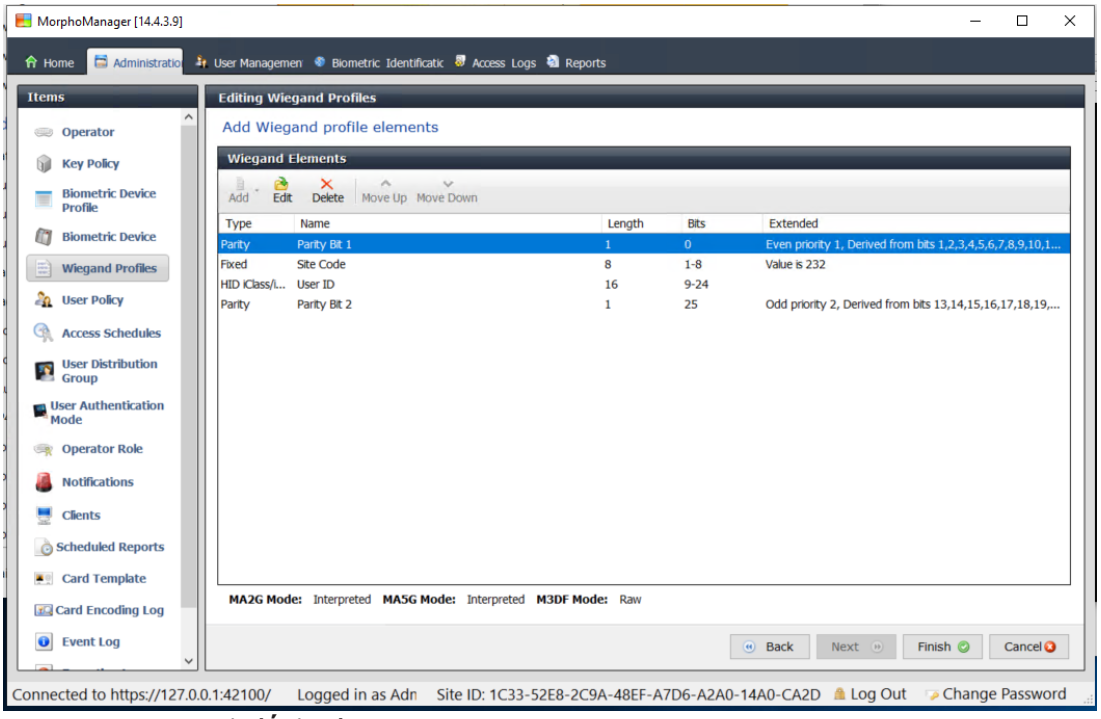
– **Length (Longueur) :** `56`
– Ajoutez **Wiegand Element User CSN Element (Élément CSN utilisateur de l'élément Wiegand)**
  – Entrez un nom sous **Name (Nom) :**
  – En regard de **Length (Longueur)**, entrez 56
  – En regard de **Transformation mode (Mode de transformation) :**, entrez `Reversed`
– **Sous Administration > Biometric Device profile (Profil de dispositif biométrique)**, sur la page **Multi-Factor Mode Settings (Paramètres du mode multifacteur)**, cochez la case **Mifare DESFire 3DES**

iClass 26 BIT

1. Sélectionnez le profil prédéfini `Standard 26 bit-HID PACS`



2. Cliquez sur **Edit (Éditer)**
3. Cliquez sur **Suivant**.



4. Cliquez sur **Edit (Éditer)**
5. Supprimez la ligne `Fixed Facility Code`
6. Sélectionnez la ligne `HID iClass SEP User ID`
7. Cliquez sur **Edit (Éditer)**
8. Remplacez la longueur `1..16` de l'ID utilisateur de par `1..24`

9. **Sous Administration > Biometric Device profile (Profil de dispositif biométrique)**, sur la page Biometric Device Settings (Paramètres du dispositif biométrique), pour Wiegand Profile (Profil Wiegand), sélectionnez `Standard 26 BIT-HID-PACS`
10. **Sous Administration > Biometric Device profile (Profil de dispositif biométrique)**, sur la page **Multi-Factor Mode Settings (Paramètres du mode multifacteur)**, cochez la case `HID iClass`
11. Cliquez sur Suivant jusqu'à l'affichage de la page **Custom Parameters (Paramètres personnalisés)**
12. Cliquez sur **Add (Ajouter)**
13. Ajoutez le paramètre personnalisé (sensible à la casse) `wiegand.site_code_propagation`
14. Définissez sa valeur sur `1`
15. Cliquez sur **Finish (Terminer)**.
16. Entrez ce profil Wiegand complété sous **Administration > User policy (Politique utilisateur)**

iClass 35 BIT

1. Sélectionnez le profil prédéfini `HID Corporate 1000 35 BIT`
2. Cliquez sur **Edit (Éditer)**
3. Cliquez sur **Suivant**.
4. Sélectionnez et supprimez la ligne d'élément `Fixed Company ID`
5. Sélectionnez et supprimez la ligne d'élément `User Card ID Number`
6. Ajoutez la ligne d'élément `HID iClass/iClass SE PACS Data` et, dans ses détails d'élément, définissez ce qui suit :

– Name (Nom) : `Card ID Number`
– Length (Longueur) : `32`
– **Sous Administration > Biometric Device profile (Profil de dispositif biométrique)**, sur la page **Multi-Factor Mode Settings (Paramètres du mode multifacteur)**, cochez la case `HID iClass`
– Cliquez sur **Suivant** jusqu'à l'affichage de la page **Custom Parameters (Paramètres personnalisés)**
– Cliquez sur **Add (Ajouter)**
– Ajoutez le paramètre personnalisé (sensible à la casse) `wiegand.site_code_propagation`
– Définissez sa valeur sur `1`
– Cliquez sur **Finish (Terminer)**.
– Entrez ce profil Wiegand complété sous **Administration > User policy (Politique utilisateur)**

iClass 37 BIT

– **Administration > Profil Wiegand**
– Cliquez sur **Ajouter un nouveau profil**
– **Length (Longueur)** `37`

1. Ajoutez une parité d'élément :

– **Name (Nom)** : (par exemple) `EvenParityBit 1`
– **Priority (Priorité)** : `1`
– **Length (Longueur)** : `18`
– **Mode** : `Even`
– **Basis bits (Bits de base)** : `1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18`

– Cliquez sur **Suivant**.
2. Ajoutez l'élément `User HID iClass/iClass SE PACS Data` et, dans ses détails d'élément, définissez ce qui suit :
– **Nom :** `UserID`
– **Length (Longueur)** : `35`
– Cliquez sur **Suivant**.
3. Ajoutez une parité d'élément :
– **Name (Nom)** : (par exemple) `Parity Bits 2`
– **Priority (Priorité)** : `2`
– **Length (Longueur)** : `19`
– **Mode** : `Odd`
– **Basis bits (Bits de base)** : `19,20,21,22,23,24,25,26,27,28,29,30,31,32,33,34,35,36,37`
– Cliquez sur **Suivant**.
– **Sous Administration > Biometric Device profile (Profil de dispositif biométrique)**, sur la page **Multi-Factor Mode Settings (Paramètres du mode multifacteur)**, cochez la case `HID iClass`
– Cliquez sur **Suivant** jusqu'à l'affichage de la page **Custom Parameters (Paramètres personnalisés)**
– Cliquez sur **Add (Ajouter)**
– Ajoutez le paramètre personnalisé (sensible à la casse) `wiegand.site_code_propagation`
– Définissez sa valeur sur `1`
– Cliquez sur **Finish (Terminer)**.
– Entrez ce profil Wiegand complété sous **Administration > User policy (Politique utilisateur)**

iClass 48BIT

1. Sélectionnez le profil prédéfini `HID Corporate 1000 48 BIT`
2. Cliquez sur **Edit (Éditer)**
3. Cliquez sur **Suivant**.
4. Sélectionnez et supprimez la ligne d'élément `Fixed Company ID`
5. Sélectionnez et supprimez la ligne d'élément `User Card ID Number`
6. Ajoutez la ligne d'élément `HID iClass/iClass SE PACS Data` et, dans ses détails d'élément, définissez ce qui suit :
– Name (Nom) : `User`
– Length (Longueur) : `45`
7. **Sous Administration > Biometric Device profile (Profil de dispositif biométrique)**, sur la page **Multi-Factor Mode Settings (Paramètres du mode multifacteur)**, cochez la case `HID iClass`
8. Cliquez sur **Suivant** jusqu'à l'affichage de la page **Custom Parameters (Paramètres personnalisés)**
9. Cliquez sur **Add (Ajouter)**
10. Ajoutez le paramètre personnalisé (sensible à la casse) `wiegand.site_code_propagation`
– Définissez sa valeur sur `1`
11. Cliquez sur **Finish (Terminer)**.
12. Entrez ce profil Wiegand complété sous **Administration** > **User policy (Politique utilisateur)**

HID Prox

1. Sélectionnez le profil prédéfini `Standard 26 BIT`
2. Cliquez sur **Edit (Éditer)**
3. Cliquez sur **Suivant**.
4. Supprimez la ligne `Fixed Facility Code`
5. Cliquez sur **Edit (Éditer)**
6. Remplacez la longueur `1..16` de l'ID utilisateur de par `1..24`
7. **Sous Administration > Biometric Device profile (Profil de dispositif biométrique)**, sur la page Biometric Device Settings (Paramètres du dispositif biométrique), pour Wiegand Profile (Profil Wiegand), sélectionnez `Standard 26 BIT`
8. **Sous Administration > Biometric Device profile (Profil de dispositif biométrique)**, sur la page **Multi-Factor Mode Settings (Paramètres du mode multifacteur)**, sélectionnez les cases à cocher :

– **Biometry (Biométrie)**
– **Proximity card (Carte de proximité)**

9. Cliquez sur **Suivant** jusqu'à l'affichage de la page **Custom Parameters (Paramètres personnalisés)**
10. Cliquez sur **Add (Ajouter)**
11. Ajoutez le paramètre personnalisé (sensible à la casse) `wiegand.site_code_propagation`

– Définissez sa valeur sur `1`

12. Cliquez sur **Finish (Terminer)**.
13. Entrez ce profil Wiegand complété sous **Administration** > **User policy (Politique utilisateur)**

22.3 Sélection d'un mode d'identification

Introduction

Les lecteurs biométriques peuvent identifier les détenteurs de badge d'identité de différentes manières. Il s'agit de différents modes d'identification ou modes d'authentification.

– Par **carte OU biométrie**, selon ce que le détenteur de carte présente au lecteur
– Par **carte ET biométrie**, c'est-à-dire que l'utilisateur doit vérifier au moyen d'informations d'identification biométriques qu'il est le véritable propriétaire de la carte.
– Par **biométrie seulement**

Cette section décrit comment définir la configuration de ces modes dans MorphoManager. Notez que chaque fois qu'il s'agit d'informations d'identification de carte, il est bien entendu nécessaire de créer un profil pour la technologie et le format de carte appropriés.

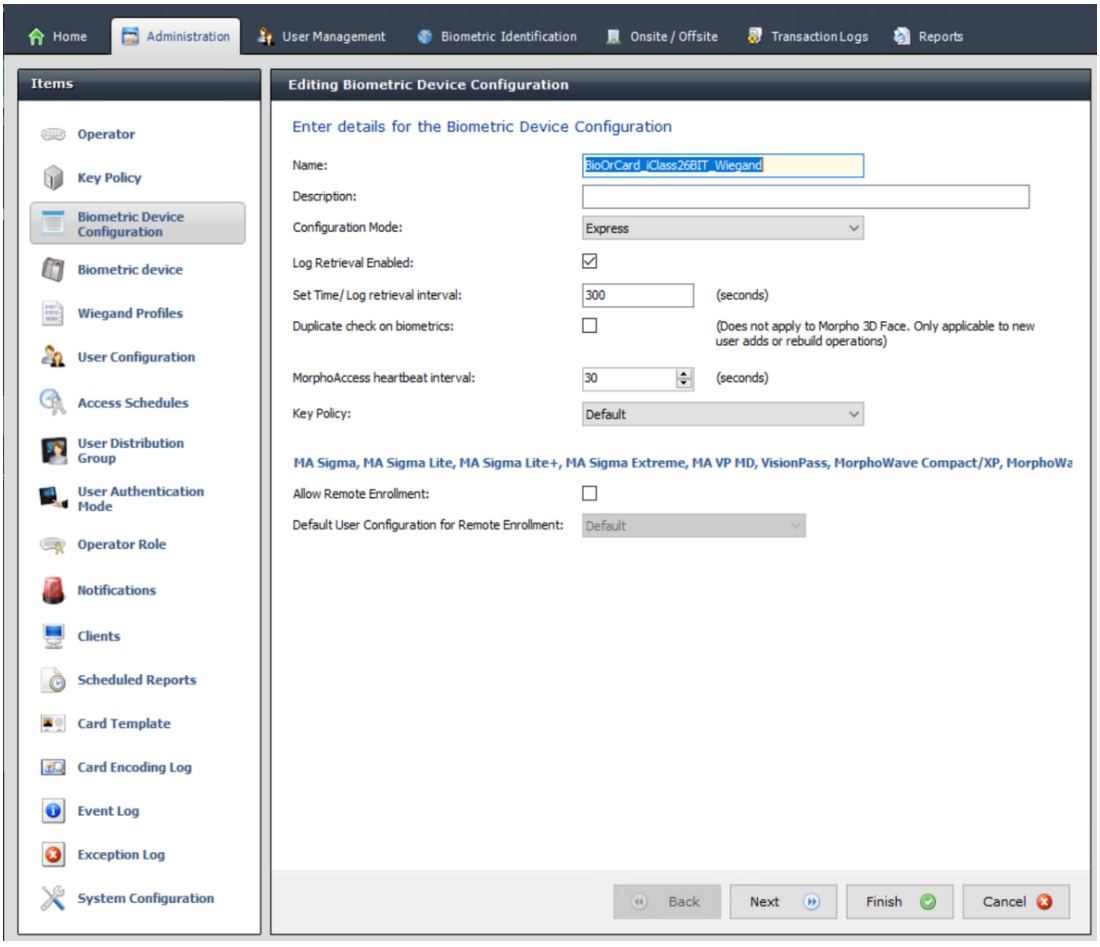
Chemin d'accès à la boîte de dialogue

Dans MorphoManager, onglet **Administration**

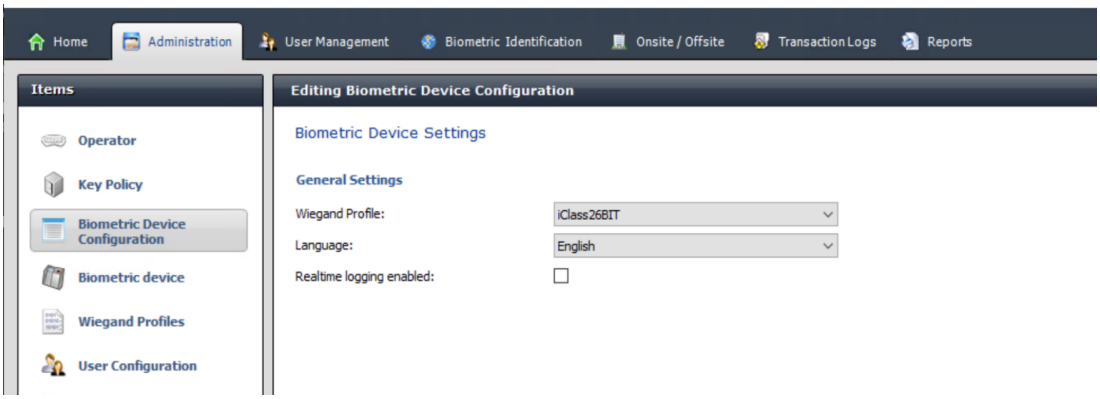
22.3.1 Carte OU Biométrie

Créez ce mode d'authentification personnalisé si les utilisateurs doivent s'identifier SOIT avec un badge SOIT avec des identifiants biométriques.

1. Dans MorphoManager, accédez à **Administration** > **Biometric (Biométrique) Device Configuration (Configuration du dispositif)**
2. Saisissez un nom pour cette configuration de dispositif biométrique, par exemple `CardORBiometric`

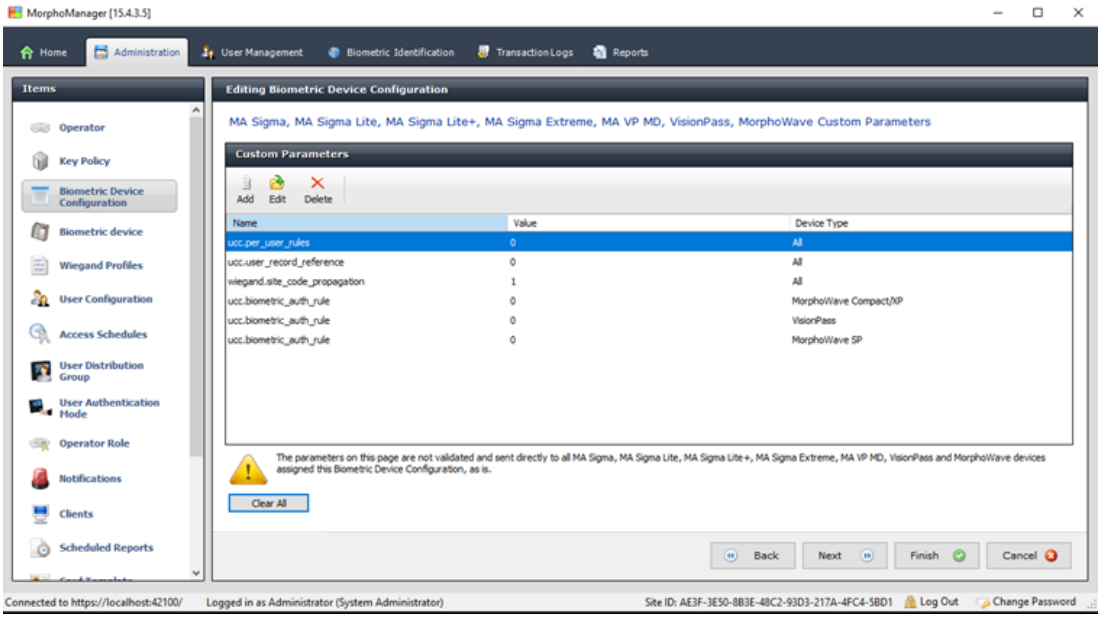


3. Cliquez sur **Next (Suivant)** jusqu'à l'affichage de la page **Biometric Device Settings (Paramètres de dispositif biométrique)**



4. En regard de **Wiegand Profile (Profil Wiegand)**, sélectionnez le même profil que celui que vous avez défini pour vos dispositifs biométriques lors de la configuration de BioBridge.
5. Cliquez sur **Next (Suivant)** jusqu'à ce que vous atteigniez la boîte de dialogue **Biometric Threshold settings (Paramètres de seuil biométrique)**.

6. Définissez les valeur de **seuil biométrique** en fonction de vos conditions locales et de la documentation MorphoManager. La valeur par défaut est `Recommended`
7. Cliquez sur **Next (Suivant)** jusqu'à l'affichage de l'écran **Multi-Factor Mode Settings (Paramètres du mode multifacteur)**.
8. Sélectionnez la case à cocher **Biometric (Biométrique)**, plus la case à cocher de la technologie de carte utilisée par votre installation.
9. Cliquez sur **Next (Suivant)** jusqu'à l'affichage de l'écran **Custom Parameters (Paramètres personnalisés)**



10. Pour chaque dispositif que vous utilisez :
    Cliquez sur **Add (Ajouter)** pour ajouter deux paramètres personnalisés.
    (Si ces deux paramètres sont définis, le lecteur envoie les données de la carte directement à l'AMC. L'utilisateur n'a pas besoin d'être inscrit sur le lecteur IDEMIA)

– `ucc.per_user_rules`
– `ucc.user_record_reference`

11. Pour les lecteurs WAVE et VisionPass, ajoutez un paramètre supplémentaire :

– `ucc.biometric_auth_rule=0`
– Dans ce cas, sélectionnez pour **Device Type (Type de dispositif)** `MorphoWave Compact/XP` ou `MorphoWave SP` ou `VisionPass`

12. Cliquez sur **Finish (Terminer)**

Attribuez ce mode d'authentification utilisateur aux utilisateurs

Dans ACS, vous devez attribuer un badge carte avec une définition de badge valide à chaque titulaire de carte.

1. Dans MorphoManager, accédez à **Administration** > **User Authentication Mode (Mode d'authentification utilisateur)**
2. Définissez les attributs suivants **:**

– Définissez **Mode** sur `Enabled`
– Définissez la liste **Template Location (Emplacement du modèle)** sur `Download to Device`
– Cochez la case **Allow Start by Biometric (Autoriser le démarrage par biométrie)**
– Cochez la case **Allow Start by Contactless Card (Autoriser le démarrage par carte sans contact)**

– Désactivez **Require Template Match (Exiger une correspondance de modèle)**
3. Accédez à **Administration** > **User Configuration (Configuration utilisateur)**
4. Cliquez sur **Add (Ajouter)**
5. Pour **User Authentication Mode (Mode d'authentification utilisateur)**, sélectionnez le nom du mode que vous avez créé ci-dessus pour Carte OU Biométrie.
6. Cliquez sur **Finish (Terminer)**

Se reporter à
– *Sélection des technologies et formats de cartes, page 163*

22.3.2 Carte ET Biométrie

Définissez les paramètres suivants si les utilisateurs doivent utiliser une carte ET des informations d'identification biométriques, pour vérifier qu'ils sont les propriétaires de la carte.

1. Dans MorphoManager, accédez à **Administration** > **Biometric (Biométrique) Device Configuration (Configuration du dispositif)**
2. Cliquez sur **Next (Suivant)** jusqu'à l'affichage de la page **Biometric Device Settings (Paramètres de dispositif biométrique)**
3. En regard de **Wiegand Profile (Profil Wiegand)**, sélectionnez le même profil que celui que vous avez défini pour vos dispositifs biométriques lors de la configuration de BioBridge.
4. Cliquez sur **Next (Suivant)** jusqu'à l'affichage de la page **Multi-Factor Mode Settings (Paramètres du mode multifacteur)**
5. Cochez la case de la technologie de carte utilisée par votre installation.
6. Cliquez sur **Finish (Terminer)**

Attribuez ce mode d'authentification utilisateur aux utilisateurs

Dans ACS, vous devez attribuer un badge carte avec une définition de badge valide à chaque titulaire de carte.

1. Dans MorphoManager, accédez à **Administration** > **User Configuration (Configuration utilisateur)**
2. En regard de **User Authentication Mode (Mode d'authentification utilisateur)**, sélectionnez `Contactless Card ID + Biometric` dans la liste.
3. Cliquez sur **Terminer**.

Se reporter à
– *Sélection des technologies et formats de cartes, page 163*

22.3.3 Biométrie uniquement

Définissez les paramètres suivants si les utilisateurs doivent s'identifier uniquement à l'aide d'informations d'identification biométriques.

1. Dans MorphoManager, accédez à **Administration** > **Biometric (Biométrique) Device Configuration (Configuration du dispositif)**
2. Cliquez sur **Next (Suivant)** jusqu'à l'affichage de la page **Editing Biometric Device Configuration (Modification de la configuration du dispositif biométrique)**
3. En regard de **Wiegand Profile (Profil Wiegand)**, sélectionnez le même profil que celui que vous avez défini pour vos dispositifs biométriques lors de la configuration de BioBridge

4. Cliquez sur **Next (Suivant)** jusqu'à l'affichage de la page **Multi-Factor Mode Settings (Paramètres du mode multifacteur)**
5. En regard de **Multi-Factor Mode (Mode multifacteur)**, sélectionnez `Biometric only` dans la liste
6. Cliquez sur **Finish (Terminer)**

Attribuez ce mode d'authentification utilisateur aux utilisateurs

Dans ACS, vous devez attribuer un badge carte avec une définition de badge valide à chaque titulaire de carte.

1. Dans MorphoManager, accédez à **Administration** > **User Configuration (Configuration utilisateur)**
2. En regard de **User Authentication Mode (Mode d'authentification utilisateur)**, sélectionnez `Biometric(1:many)` dans la liste.
3. Cliquez sur **Terminer**.

22.4 Configuration de BioBridge dans MorphoManager

Conditions préalables

MorphoManager est installé sur un serveur MorphoManager de votre réseau. Consultez le guide d'installation et l'aide en ligne de MorphoManager.

Présentation

Pour utiliser l'interface BioBridge entre les systèmes de contrôle d'accès Bosch et Morphomanager, vous devez configurer les éléments suivants dans MorphoManager :

- **Configuration du dispositif biométrique**
- **Dispositif biométrique**
- **Profils Wiegand**
- **Configuration utilisateur**
- **Groupe de distribution d'utilisateurs**
- **Mode d'authentification utilisateur**
- **Configuration du système**

De plus, Open Database Connectivity (ODBC) doit être configuré pour la communication entre Morphomanager BioBridge et la base de données avec laquelle il partage ACS.
Toutes ces tâches de configuration sont décrites dans les sections suivantes.

22.4.1 Configuration du dispositif biométrique

La configuration du dispositif biométrique définit les réglages et paramètres communs pour un ou plusieurs dispositifs biométriques. Lorsque vous ajoutez des dispositifs biométriques au système ultérieurement dans la section **Biometric Device (Dispositif biométrique)** de **Administration**, vous leur appliquez une configuration de dispositif biométrique.
La procédure suivante suppose que vous déployez des lecteurs biométriques d'IDEMIA avec une technologie de lecture de carte supplémentaire.

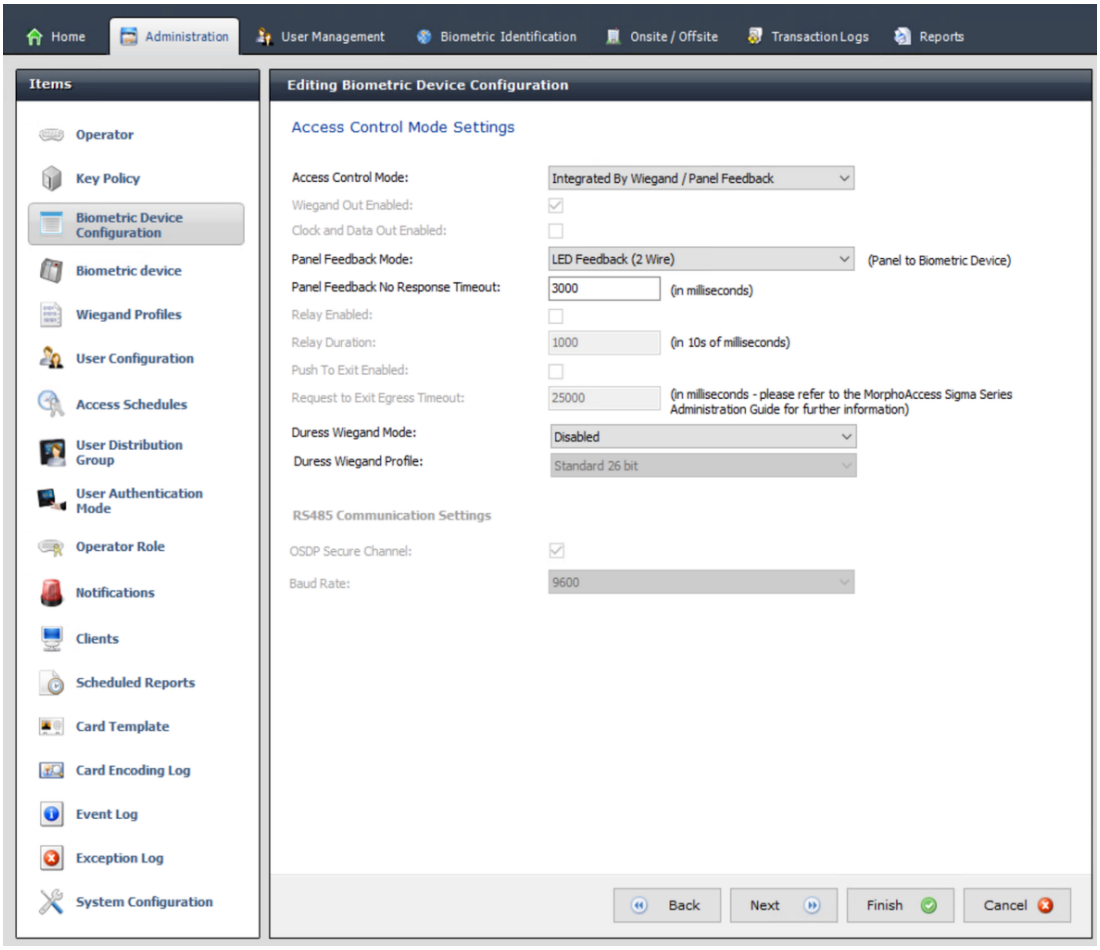
Procédure :

1. Dans MorphoManager, accédez à **Administration** > **Biometric Device Configuration (Configuration du dispositif biométrique)**.
2. Cliquez sur **Add (Ajouter)** pour créer une nouvelle configuration du dispositif biométrique.

3. Sur l'écran suivant, saisissez un nom pour le profil et une description (facultatif). Si vous n'utilisez pas le champ de description, nous vous recommandons un nom qui décrit le type et les modes d'identification (biométrie et/ou carte) du groupe de lecteurs.
4. Cliquez sur **Suivant** jusqu'à l'affichage de la section **Biometric Device Settings (Paramètres de dispositif biométrique)**

– Sélectionnez le profil Wiegand que vous avez créé précédemment pour votre installation.

5. Cliquez sur **Suivant** jusqu'à l'affichage de la page **Access Control Mode Settings (Paramètres du mode de contrôle d'accès)**.



À ce stade, les procédures pour les AMC Wiegand et OSDP divergent. Suivez la procédure ci-dessous qui correspond à votre type de contrôleur AMC :

Pour les AMC Wiegand

1. Définissez **Access Control Mode (Mode de contrôle d'accès)** sur `Integrated by Wiegand`
2. Définissez **Panel feedback Mode (Mode de retour d'information de la centrale)** sur `LED Feedback (2 wire)`
3. Cliquez sur **Finish (Terminer)**

Pour les AMC OSDP

1. Définissez **Access Control Mode (Mode de contrôle d'accès)** sur `Integrated by OSDP`

2. Définissez **Panel feedback Mode (Mode de retour d'information de la centrale)** sur `LED Feedback (2 wire)`
3. Cochez la case **OSDP Secure Channel (Canal sécurisé OSDP)**
4. Définissez le débit en bauds `9600`
5. Pour plus de détails, voir la section **Dispositif biométrique**
6. Cliquez sur **Finish (Terminer)** pour quitter MorphoManager.

Dépannage des clés OSDP

Si vous ne parvenez pas à établir une connexion sécurisée avec le lecteur OSDP, essayez de réinitialiser la clé de base comme suit :

1. Démarrez le programme séparé **MorphoBioToolBox (MBTB)**
2. Dans le programme MorphoBioToolBox, accédez à **Device Settings (Réglages du dispositif)** > **Reset (Réinitialiser)**
3. Sélectionnez la clé de base OSDP
4. Cliquez sur **Reset cryptographic keys (Réinitialiser les clés cryptographiques)**
5. Quittez MorphoBioToolBox

Pour les cas plus complexes, contactez le support technique IDEMIA.

Se reporter à

– *Dispositif biométrique, page 173*

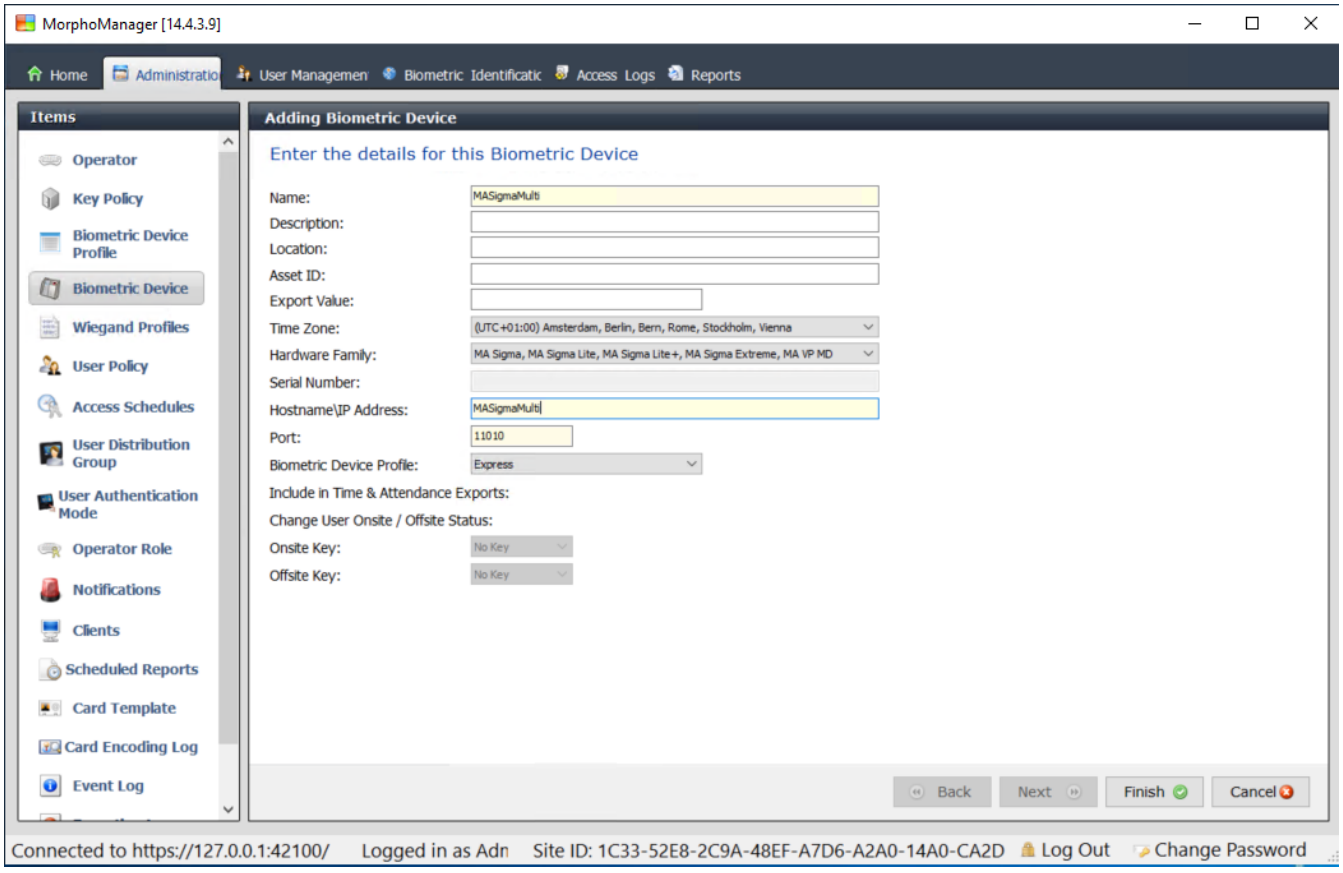
22.4.2 Dispositif biométrique

Les dispositifs biométriques testent si les informations d'identification biométriques qu'ils lisent correspondent aux enregistrements de la base de données. Ils tiennent également un journal de chaque événement d'utilisation.

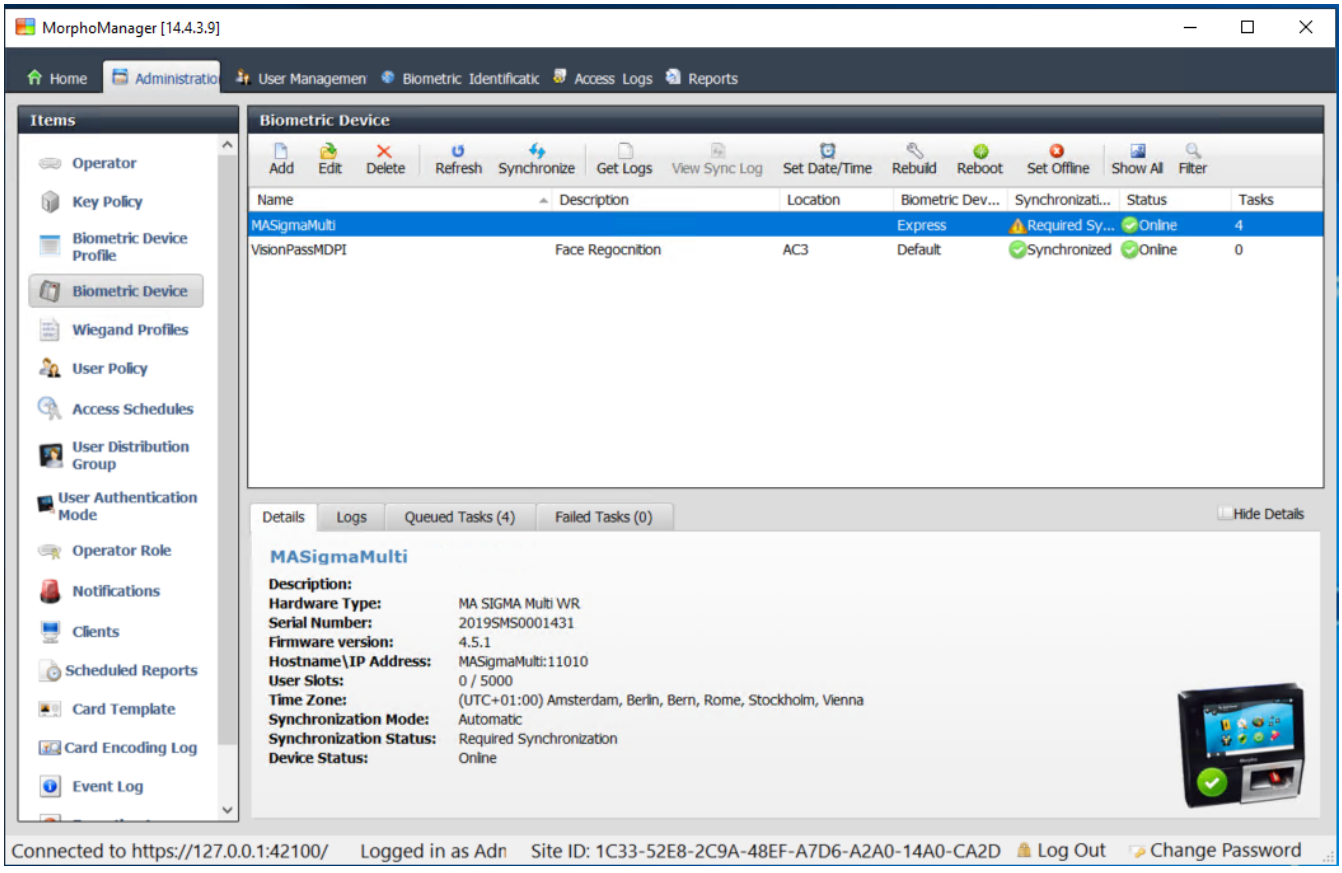
Procédure :

1. Dans MorphoManager, accédez à **Administration** > **Biometric device (Dispositif biométrique)**.
2. Cliquez sur **Add (Ajouter)** pour créer un nouveau dispositif biométrique.
3. Entrez au moins les détails essentiels du dispositif :

– (dans la liste) **Hardware Family (Famille de matériel)**
– **Nom d'hôte\Adresse IP**
– (dans la liste) le **Biometric Device Configuration (Configuration du dispositif biométrique)** que vous avez précédemment défini



4. Cliquez sur **Finish (Terminer)**
   . La boîte de dialogue Biometric Device (Dispositif biométrique) répertorie désormais les dispositifs déjà configurés :

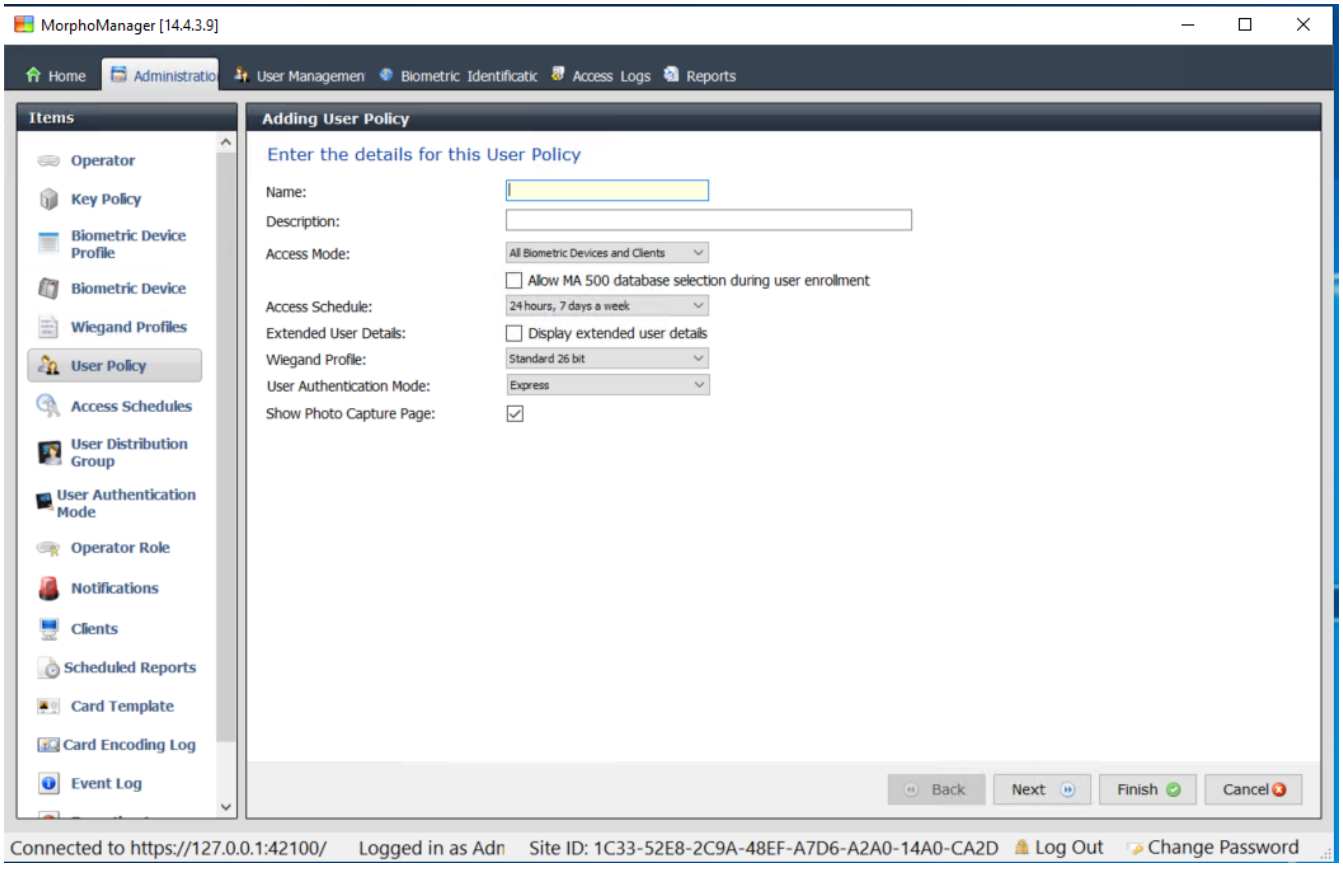


22.4.3 Configuration utilisateur

Les configurations utilisateur sont des ensembles de droits d'accès que vous attribuez aux utilisateurs qui ont les mêmes exigences d'accès, c'est-à-dire les dispositifs biométriques qu'ils sont autorisés à utiliser, dans quels modes et à quel moment.

Procédure :

1. Dans MorphoManager, accédez à **Administration** > **User Configuration (Configuration utilisateur)**.
2. Cliquez sur **Add (Ajouter)** pour créer une nouvelle configuration utilisateur.



3. Dans la boîte de dialogue **Adding User Policy (Ajout d'une politique utilisateur)**, entrez ce qui suit :

- Un **Nom (Name)** pour la politique utilisateur et (éventuellement) une description
- Le **Mode d'accès (Access Mode)** `Per User`
- Un **Planning des accès (Access Schedule)** qui régit les jours et les heures où l'accès est autorisé
- Le même **Profil Wiegand (Wiegand Profile)** que vous avez défini et utilisé pour le **Profil de dispositif biométrique**.
- Un **Mode d'authentification utilisateur (User Authentication Mode)**, en fonction des manières dont les utilisateurs de dispositifs vont utiliser les dispositifs (par empreinte digitale, doigt, visage, cartes, etc.). Voir la section **Sélection d'un mode d'identification** pour plus de détails.

4. Cliquez sur **Finish (Terminer)**

La politique utilisateur par défaut aura un mode d'authentification utilisateur `(1: Many)`. Pour utiliser d'autres modes d'authentification, créez des stratégies utilisateur supplémentaires. Consultez le manuel d'utilisation de MorphoManager pour plus de détails sur les différentes propriétés pouvant être attribuées à une politique utilisateur.

Se reporter à

- *Sélection d'un mode d'identification, page 167*

22.4.4 Groupes de distribution d'utilisateurs

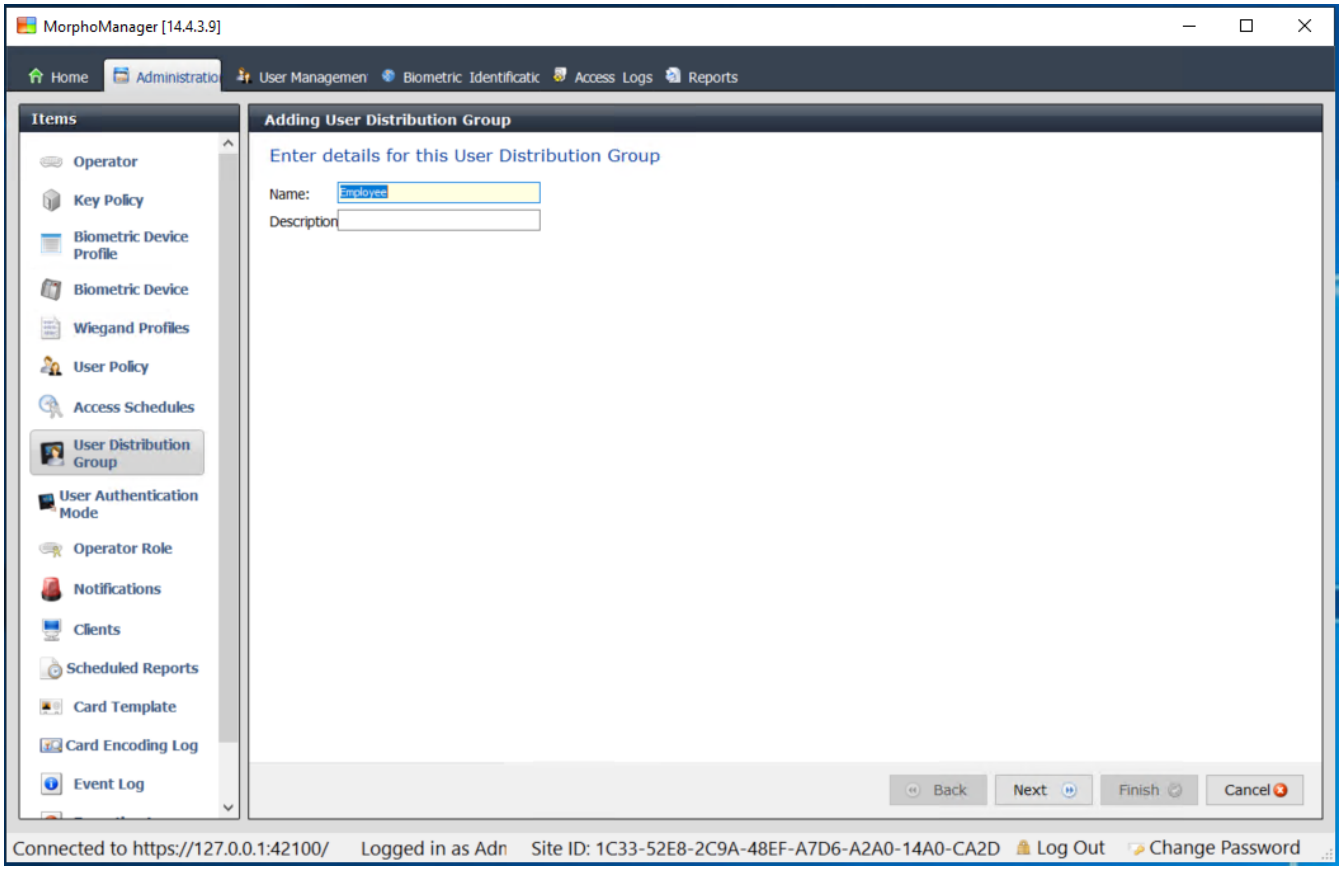
Les groupes de distribution d'utilisateurs mappent les utilisateurs à des groupes de lecteurs biométriques ou à des clients MorphoManager.

Conditions préalables :

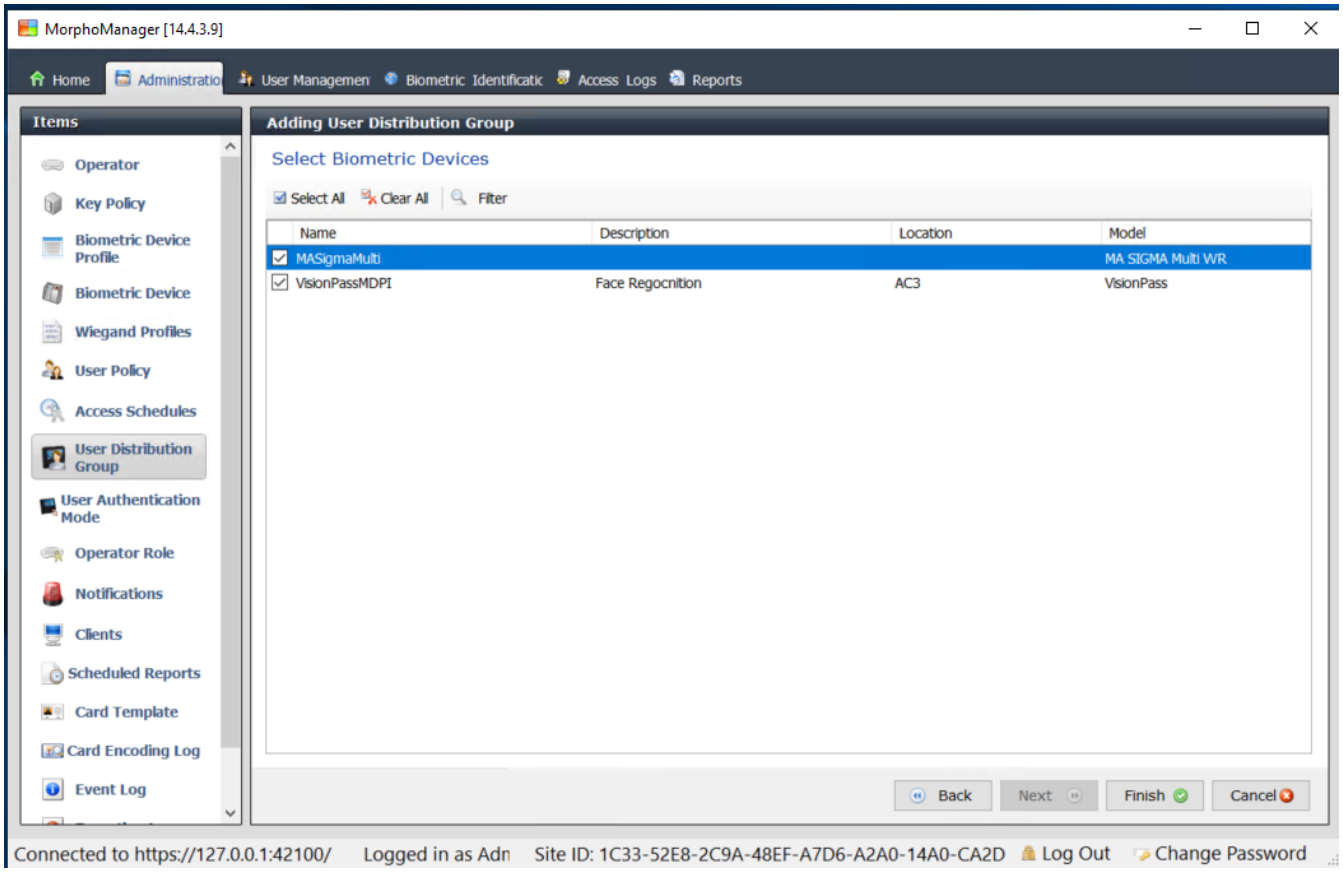
Chaque groupe de distribution d'utilisateurs doit être mappé à au moins une classe de personne dans ACS. Par conséquent, créez au moins un groupe de distribution d'utilisateurs pour chaque classe de personne que vous utilisez.

Procédure :

1. Dans MorphoManager, accédez à **Administration** > **User Distribution Group (Groupe de distribution d'utilisateurs)**.
2. Cliquez sur **Add (Ajouter)** pour créer un nouveau groupe de distribution d'utilisateurs.



3. Cliquez sur **Suivant** jusqu'à l'affichage de la page intitulée **Select Biometric Devices (Sélectionner les dispositifs biométriques)**.
4. Cochez les cases des dispositifs biométriques que les personnes de ce groupe de distribution d'utilisateurs doivent utiliser.



5. Cliquez sur **Finish (Terminer)**

22.4.5 Configuration d'ODBC pour BioBridge

Introduction

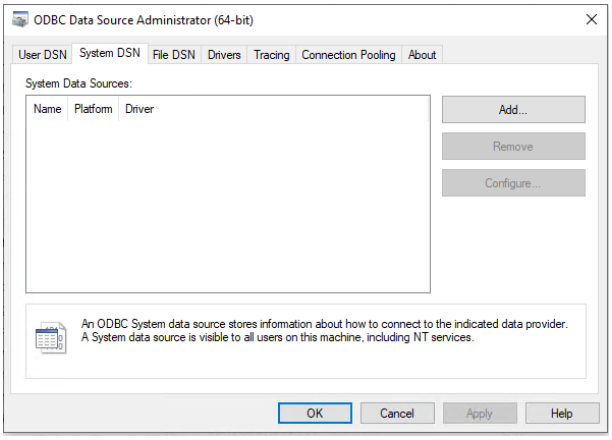
Open Database Connectivity (ODBC) est un prérequis à l'utilisation de MorphoManager BioBridge. ODBC est une interface de programmation standardisée pour accéder à différentes bases de données. Le pilote recommandé est `OdbCDriver17SQLServer`

- Pour BIS, le pilote se trouve sur le support d'installation de BIS à l'adresse `BIS\3rd_Party\OdbCDriver17SQLServer`
- Pour AMS, téléchargez le pilote depuis `www.microsoft.com`

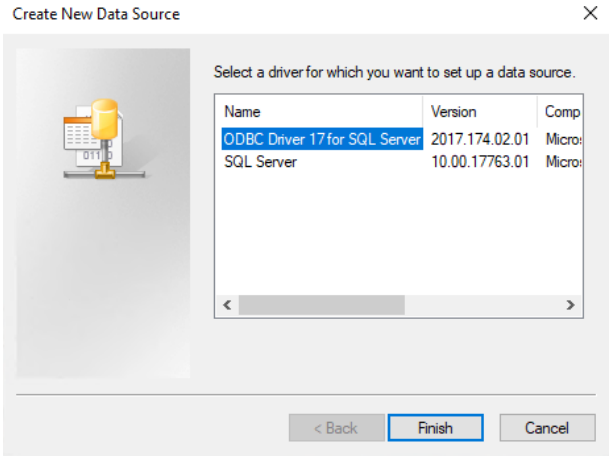
Création d'une source de données

Création d'un nom de source de données (DSN) pour ODBC

1. Dans le Panneau de configuration de Windows, sélectionnez **Outils d'administration**.
2. Sélectionnez `ODBC Data Sources (64-bit)` dans la liste.
3. Sélectionnez l'onglet **Sources de données système**.

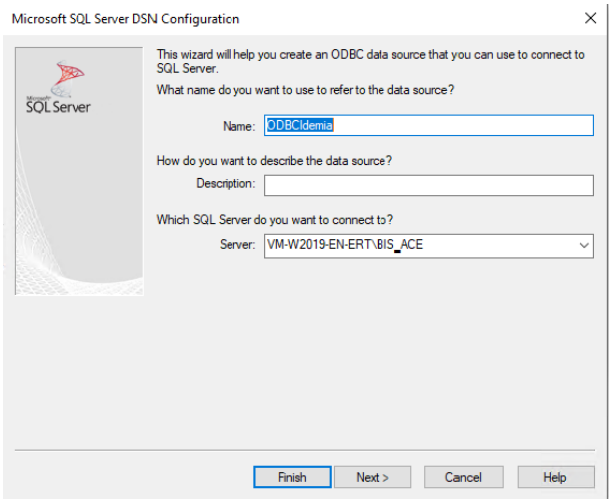


4. Cliquez sur **Ajouter** pour sélectionner un pilote.
5. Sélectionnez `ODBC Driver 17 for SQL Server` comme pilote, puis cliquez sur **Terminer**.

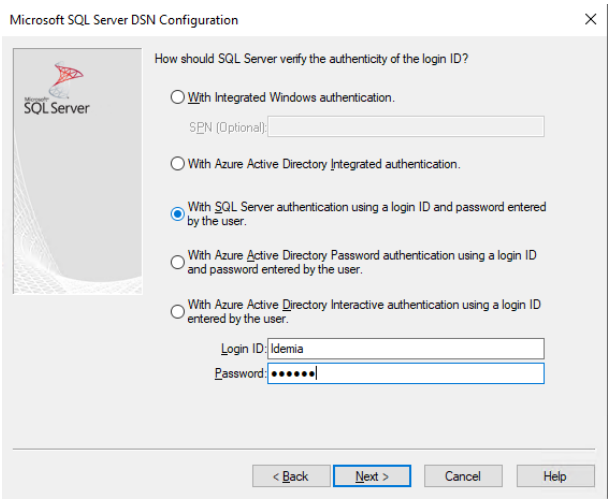


6. Entrez les détails suivants pour la source de données.

– **Nom** : nom pour la source de données
– **Description** (facultative)
– **Serveur** : nom de l'ordinateur sur lequel la base de données ACE est installée, et nom de la base de données (par défaut : <MyACSserver>\`ACE`)



7. Cliquez sur **Suivant >**
   Une boîte de dialogue s'affiche pour collecter les informations de connexion



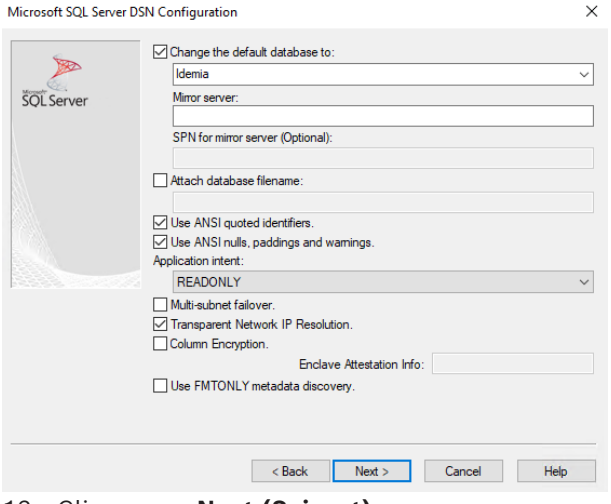
8. Sélectionnez **Avec l'authentification SQL Server utilisant un identificateur de connexion...**
9. Entrez les informations suivantes :

– **Login ID (ID de connexion)** : nom d'utilisateur de l'utilisateur de la base de données Idemia tel que configuré dans ACS. Il s'agit toujours de `Idemia`.
– **Mot de passe** : mot de passe qui a été défini pour l'utilisateur de la base de données Idemia, lors de sa configuration dans ACS.

10. Cliquez sur **Next (Suivant) >**.
11. Dans la boîte de dialogue suivante, cochez les cases :

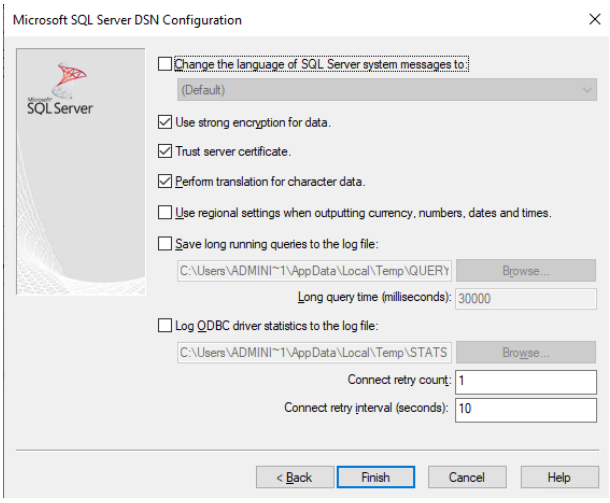
– **Change the default database to (Remplacer la base de données par défaut par) :** et sélectionnez `Idemia`
– **Use ANSI quoted identifiers (Utiliser les identifiants ANSI entre guillemets)**
– **Use ANSI nulls, paddings and warnings (Utiliser les valeurs NULL, les remplissages et les avertissements ANSI)**
– **Transparent Network IP Resolution (Résolution IP transparente du réseau)**

12. Définissez **Application intent (Intention de l'application)** sur `READONLY`

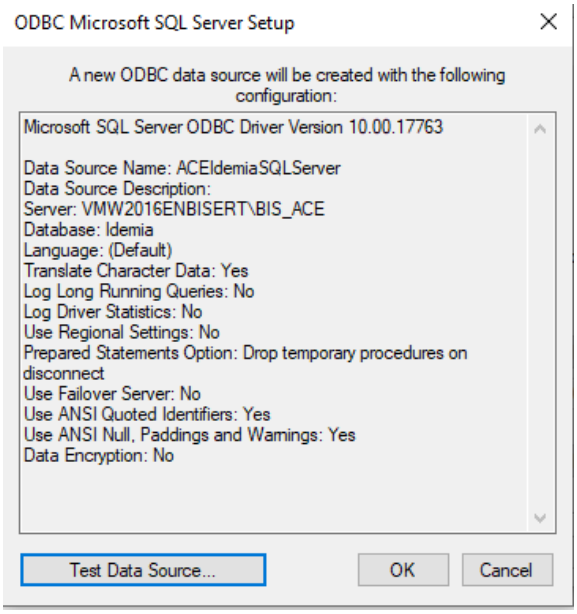


13. Cliquez sur **Next (Suivant) >**.
14. Dans la boîte de dialogue suivante, cochez les cases

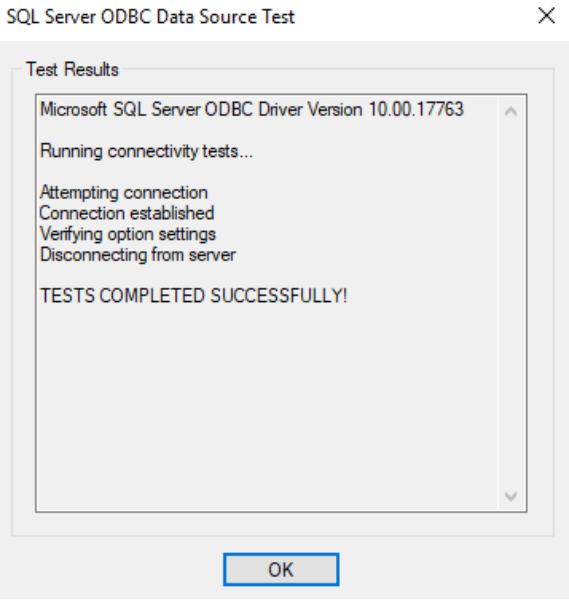
– **Use strong encryption for data (Utiliser un chiffrement fort pour les données)**
– **Perform translation for character data (Effectuer la conversion des données de caractères)**
– **Trust server certificate (Certificat de serveur de confiance)**



15. Cliquez sur **Finish (Terminer)**
16. Dans la boîte de dialogue suivante, examinez les données récapitulatives



17. Cliquez sur **Test Data Source... (Tester la source de données...)** et assurez-vous que les tests se terminent avec succès



18. Enregistrez toutes les modifications et quittez l'assistant de configuration ODBC.

22.4.6 Configuration du système BioBridge

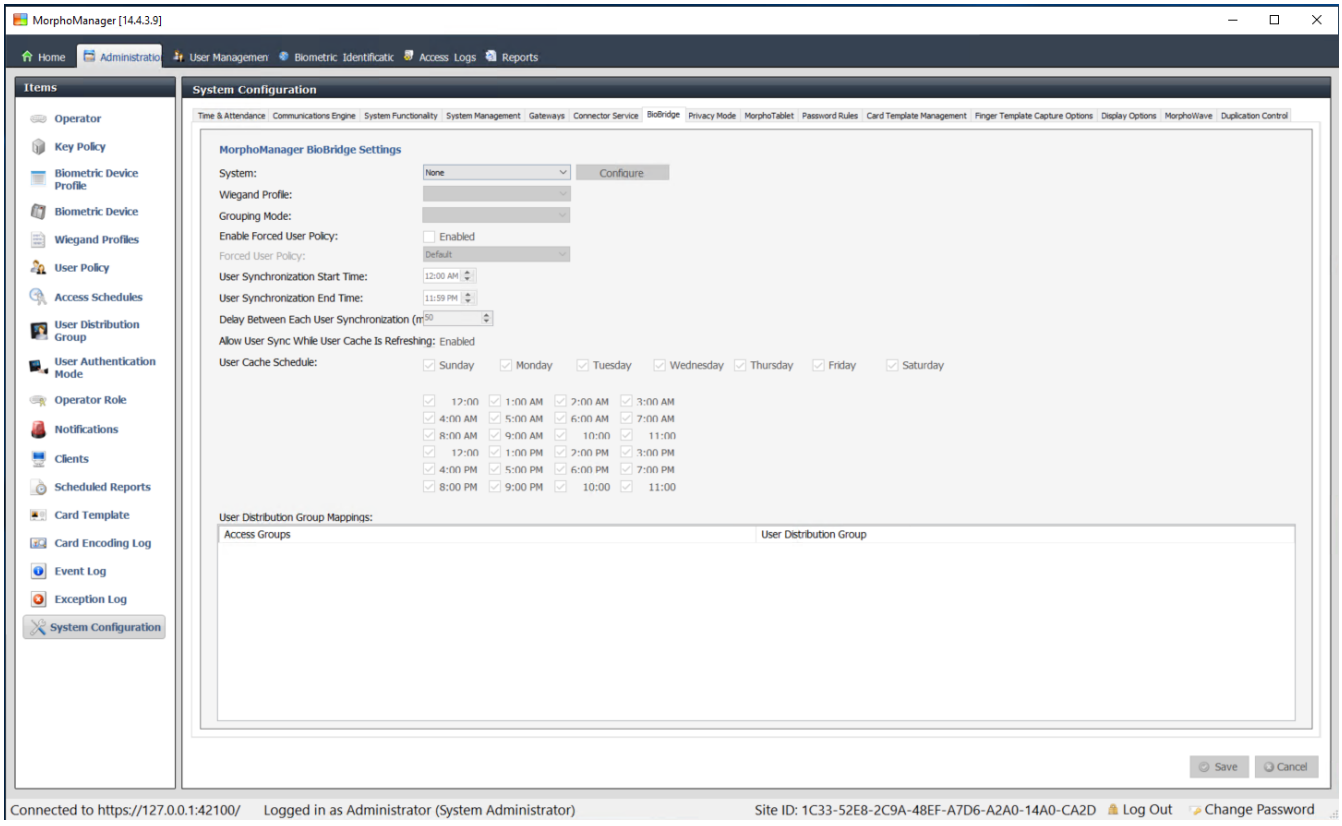
Cette section décrit les autres paramètres requis pour que les systèmes de contrôle d'accès utilisent l'interface BioBridge.

Condition préalable

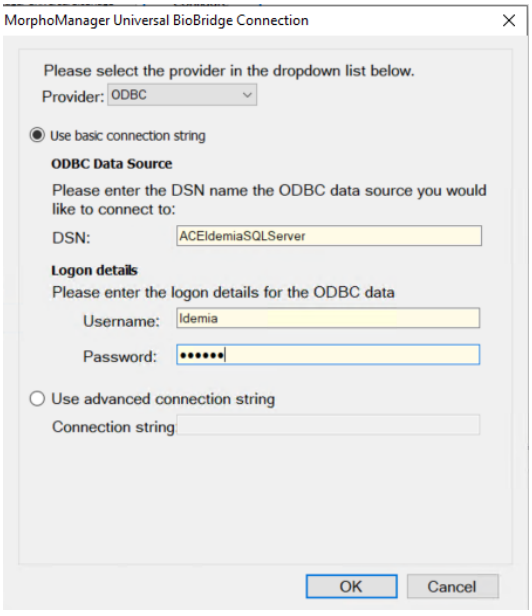
ODBC est configuré pour BioBridge. Voir *Configuration d'ODBC pour BioBridge, page 178*

Procédure :

1. Dans MorphoManager, accédez à **Administration** > **System Configuration (Configuration du système)**.
2. Sélectionnez l'onglet **BioBridge**



3. Dans la liste déroulante **System (Système)**, sélectionnez `MorphoManager Universal BioBridge`
4. Cliquez sur **Configure (Configurer)**
   Une boîte de dialogue contextuelle apparaît.



Dans la fenêtre contextuelle

1. Dans la liste déroulante **Provider (Fournisseur)**, sélectionnez `ODBC`
2. Entrez le DSN (Data Source Name) de la configuration ODBC.
3. Sous **Logon details (Détails de connexion)**, entrez le nom d'utilisateur (`Idemia`) et le mot de passe tel que définis dans la configuration ODBC.

4. Cliquez sur **OK** pour retourner à la boîte de dialogue **System Configuration (Configuration du système)**.

Dans la boîte de dialogue **System Configuration (Configuration du système)**

1. En regard de **Wiegand Profile (Profil Wiegand)** : sélectionnez dans la liste le profil Wiegand que vous avez défini précédemment.

Grouping mode (Mode de regroupement) :
Ce paramètre détermine comment MorphoManager doit mapper les utilisateurs MM Universal BioBridge aux groupes de distribution d'utilisateurs MorphoManager. Sélectionnez l'une des valeurs suivantes :

- **Automatic (Automatique)** : ce mode fera correspondra automatiquement les **groupes de niveaux d'accès** de MM Universal BioBridge aux **groupes de distribution d'utilisateurs** MorphoManager, s'ils ont la même convention de nommage.
- **Manual (Manuel)** : Si les **groupes de niveaux d'accès** de MM Universal BioBridge et les **groupes de distribution d'utilisateurs** de MorphoManager ne sont pas les mêmes, vous pouvez alors effectuer le mappage manuellement dans **User Policy Mappings (Mappages de politique utilisateur)**.

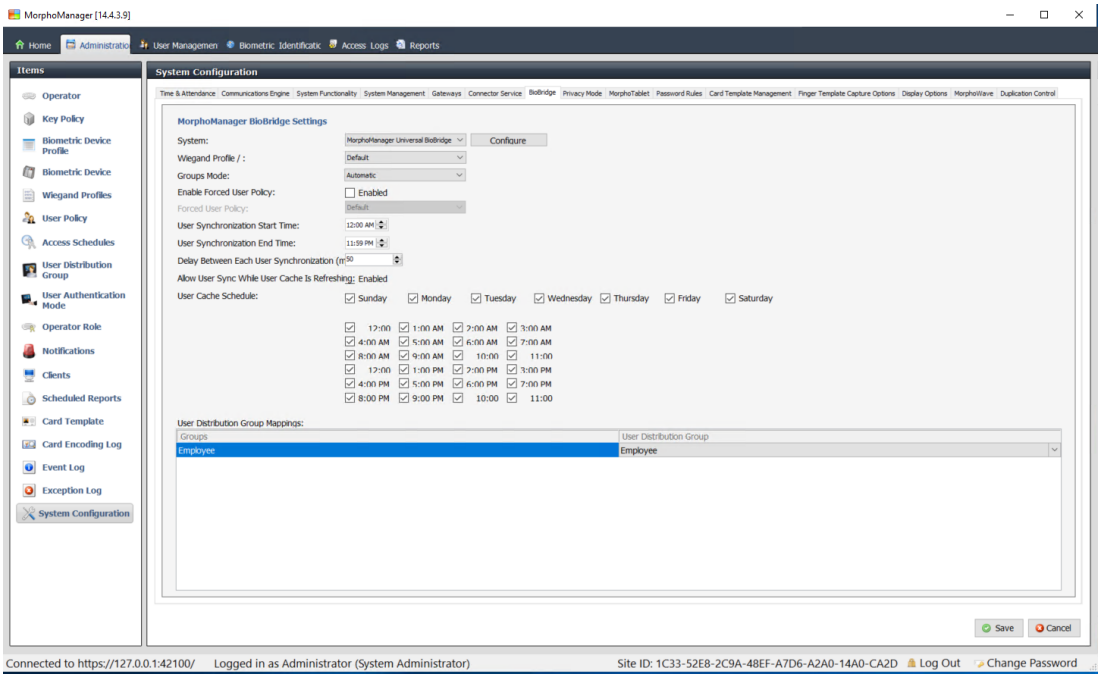
Autres paramètres
Dans la plupart des cas, les paramètres suivants peuvent être conservés avec leurs valeurs par défaut :

Enable Forced User Policy (Activer la politique utilisateur forcée)	Lorsque ce paramètre est sélectionné, tous les utilisateurs inscrits dans le client d'inscription BioBridge recevront la politique utilisateur sélectionnée dans la liste adjacente. Si vous cochez cette case, utilisez toujours la stratégie utilisateur nommée `Per User`
User Synchronization Start Time and End Time (Heure de début et heure de fin de la synchronisation utilisateur)	Le moteur de synchronisation des utilisateurs ne sera autorisé à s'exécuter qu'entre ces deux heures.
Delay between Each User Synchronization (Délai entre chaque synchronisation utilisateur)	Intervalle de temps entre les synchronisations utilisateur. L'augmentation de ce délai permettra d'économiser des ressources système, mais augmentera le temps de mise à jour de tous les utilisateurs.
Allow User Sync While User Cache Is Refreshing (Autoriser la synchronisation utilisateur pendant l'actualisation du cache utilisateur)	Lorsque ce paramètre est activé, le moteur de synchronisation des utilisateurs s'exécute en parallèle avec l'actualisation du cache des utilisateurs. Cette opération utilise de nombreuses ressources système. Il est recommandé de désactiver ce paramètre lors de l'utilisation de bases de données volumineuses.

User Cache Refresh Schedule (Programme d'actualisation du cache utilisateur)	Jours et heures auxquels le cache utilisateur peut être actualisé. Pour une plus grande précision, cela devrait être à tout moment, mais il est nécessaire de trouver un compromis pour les performances des systèmes avec de grandes bases de données.

Mappages des groupes de distribution d'utilisateurs

– Dans le tableau des mappages, assurez-vous que tous les **groupes** (**Classes du personnel** définies dans l' ACS) sont mappés aux **groupes de distribution d'utilisateurs** (définis dans MorphoManager).



22.5 Configuration du client d'inscription BioBridge

Introduction

Un client d'inscription BioBridge est un ordinateur sur lequel vous pouvez créer des enregistrements biométriques pour les utilisateurs du système de contrôle d'accès. La configuration d'un client d'inscription BioBridge comporte 3 parties :

– Ajouter un opérateur d'inscription à MorphoManager
– Configurer des ordinateurs clients MorphoManager pour les tâches d'inscription
– Tester le client d'inscription

Conditions préalables

MorphoManager BioBridge est installé sur chaque poste de travail ACE à partir duquel vous effectuez l'inscription biométrique pour les systèmes IDEMIA.

22.5.1 Ajouter un opérateur d'inscription à Morpho Manager

Procédure

Suivez les instructions du guide d'installation du client MorphoManager.

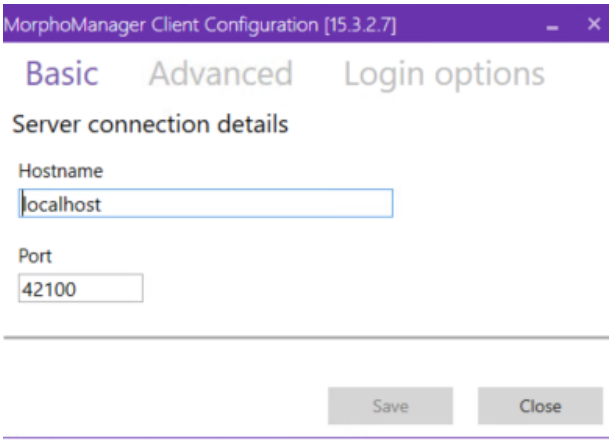
Remarque : Pour des raisons de sécurité, les comptes d'utilisateurs Active Directory sont recommandés.

22.5.2 Configurer des ordinateurs clients MorphoManager pour les tâches d'inscription

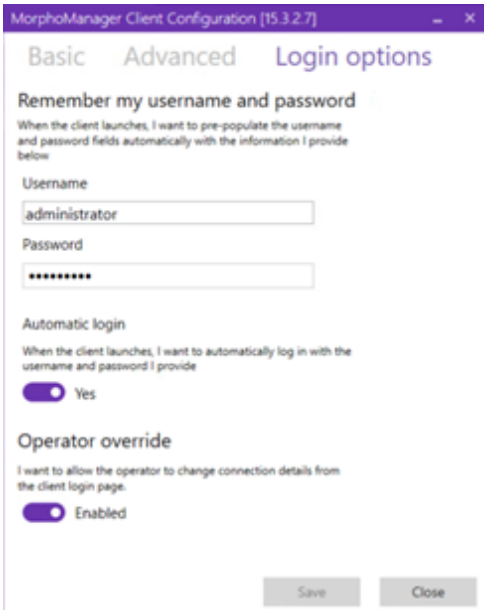
Effectuez cette procédure sur chaque ordinateur que vous souhaitez utiliser pour l'inscription biométrique.

Procédure

1. Dans le répertoire d'installation de MorphoManager (par défaut : `C:\Program,Files(x86)\Morpho\MorphoManager\Client\`) , exécutez le fichier `ID1.ECP4.MorphoManager.AdvancedClientConfig.exe` en tant qu'administrateur

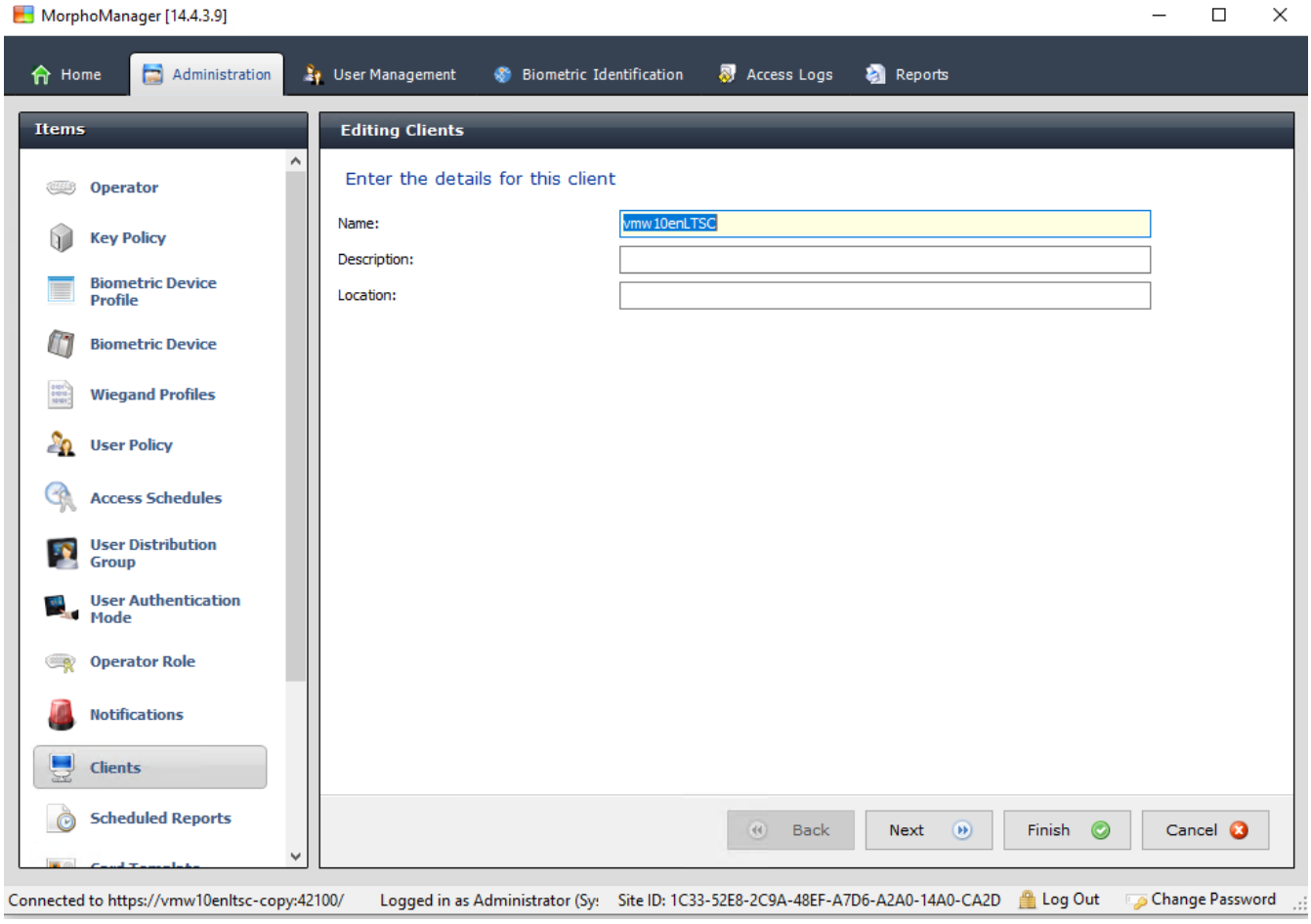


2. Sous l'onglet **Basic (De base)** , entrez le nom d'hôte du serveur Morpho sous **Hostname (Nom d'hôte)**.
3. Pour les installations sécurisées, utilisez Active Directory ou un nom d'utilisateur et un mot de passe natifs, conformément à la documentation Morpho.
4. Alternativement [NON recommandé pour les installations hautement sécurisées] sous l'onglet **Login options (Options de connexion)**

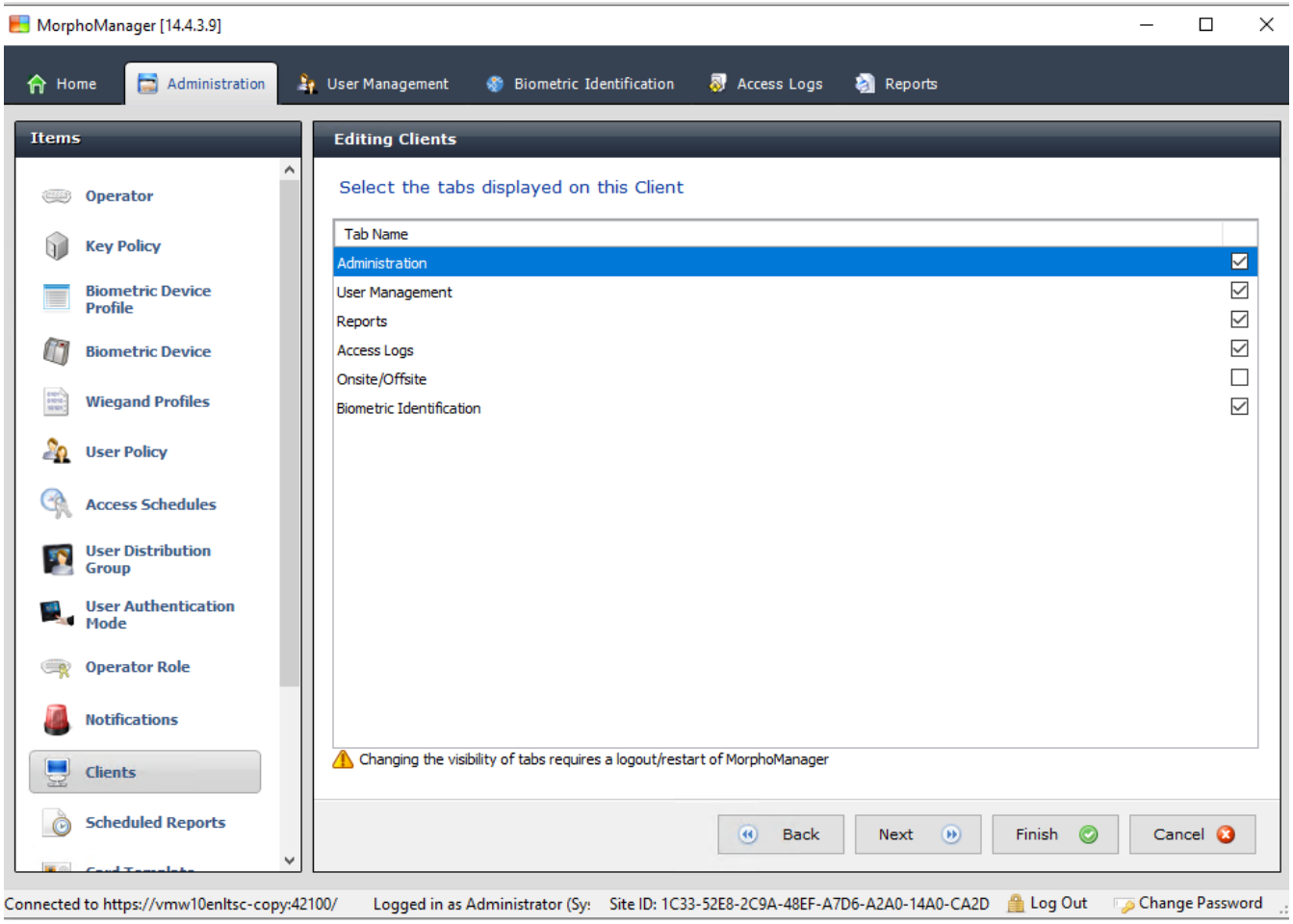


- Saisissez le nom d'utilisateur et le mot de passe que vous avez saisis pour l'opérateur d'inscription dans la section précédente
- Réglez le commutateur **Automatic login (Connexion automatique)** sur `Yes`

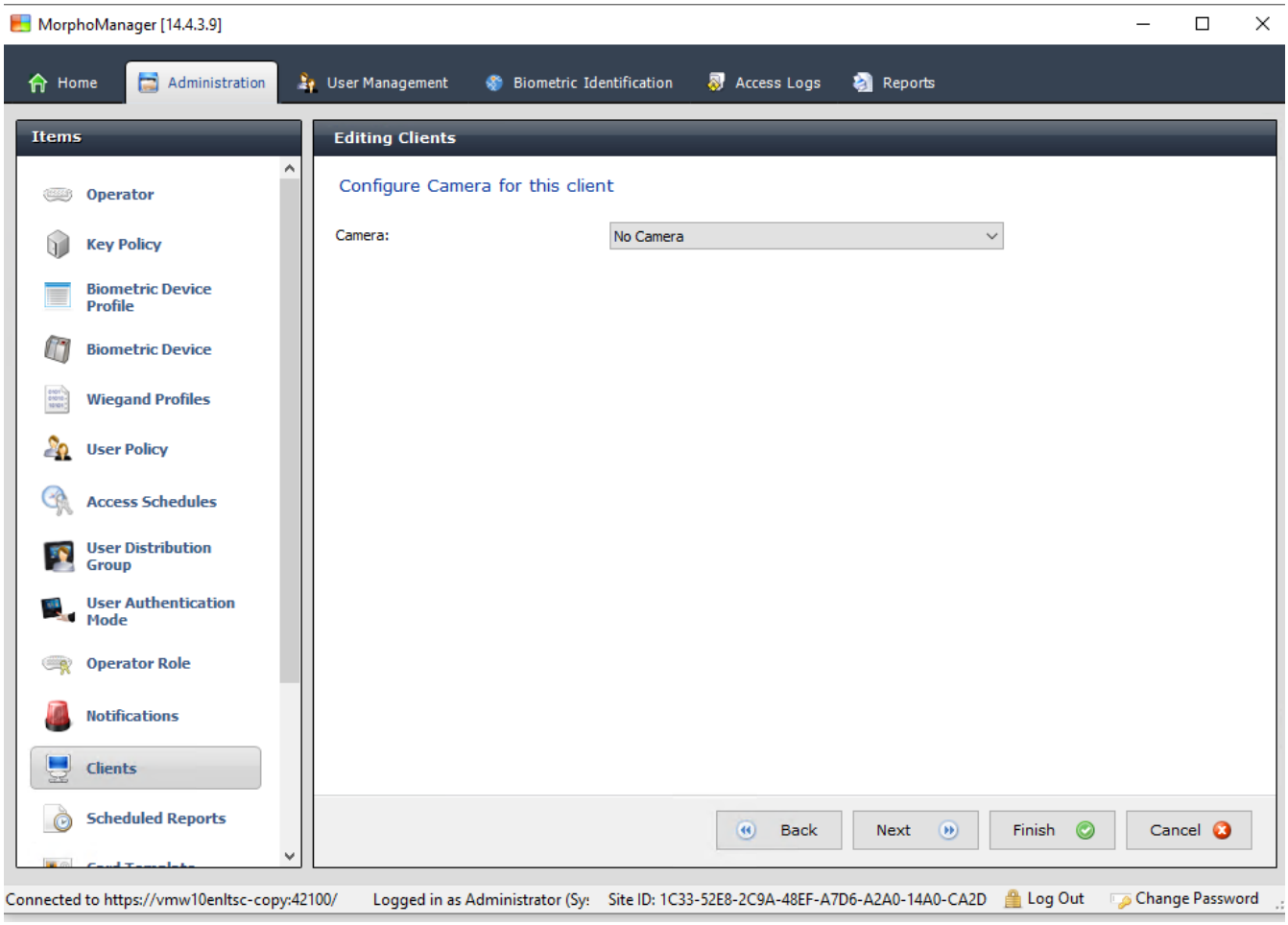
1. Dans le répertoire d'installation de MorphoManager (par défaut : `C:\Program Files(x86)\Morpho\MorphoManager\Client\`), exécutez le fichier `Start ID1.ECP4.MorphoManager.Client.exe` en tant qu'Administrateur
2. Accédez à **Administration** > **Clients**
3. Sélectionnez un ordinateur client
4. Cliquez sur **Edit (Éditer)**



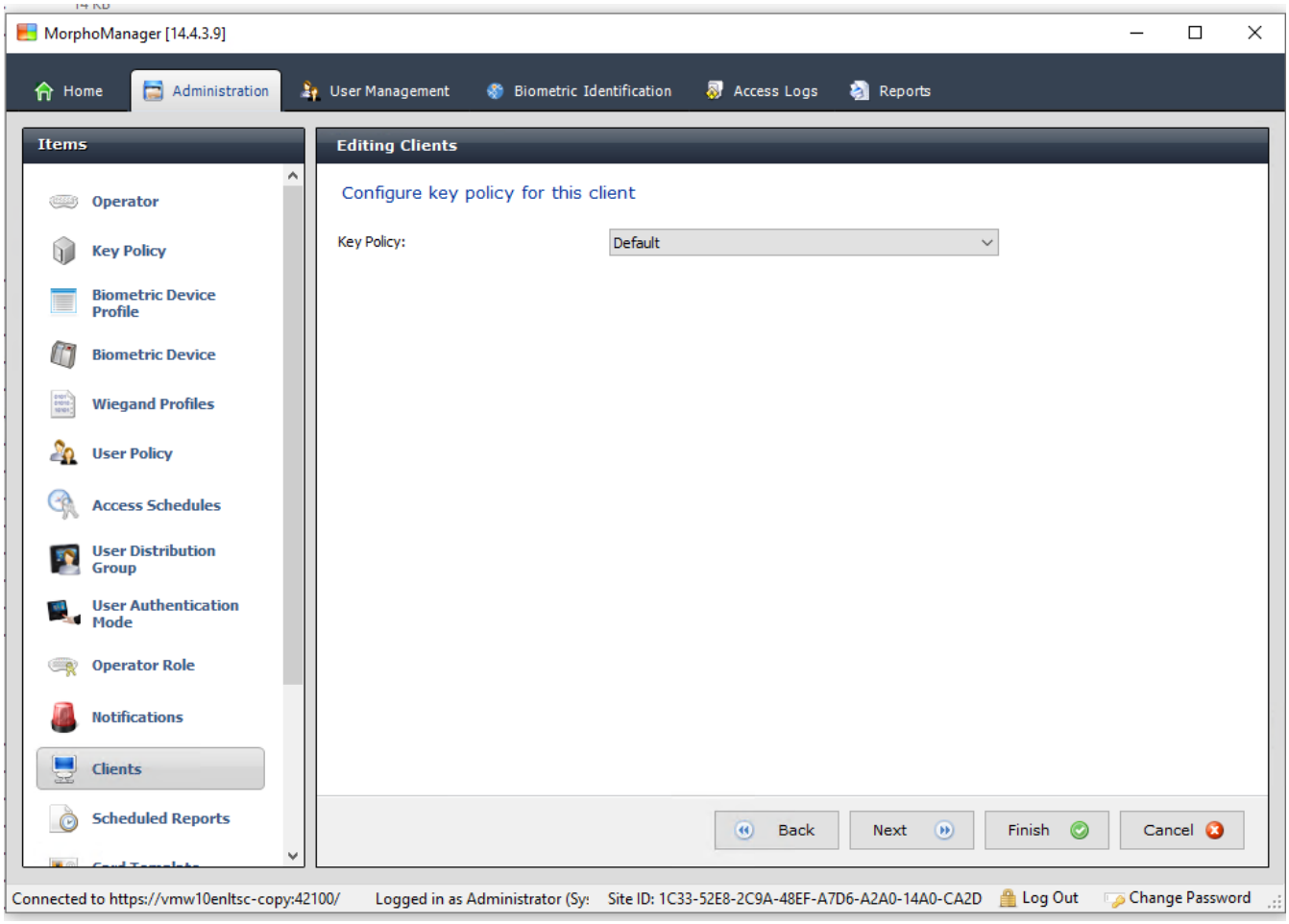
5. Entrez le nom du client d'inscription prévu, et éventuellement l'emplacement et une description
6. Cliquez sur **Next (Suivant)**.



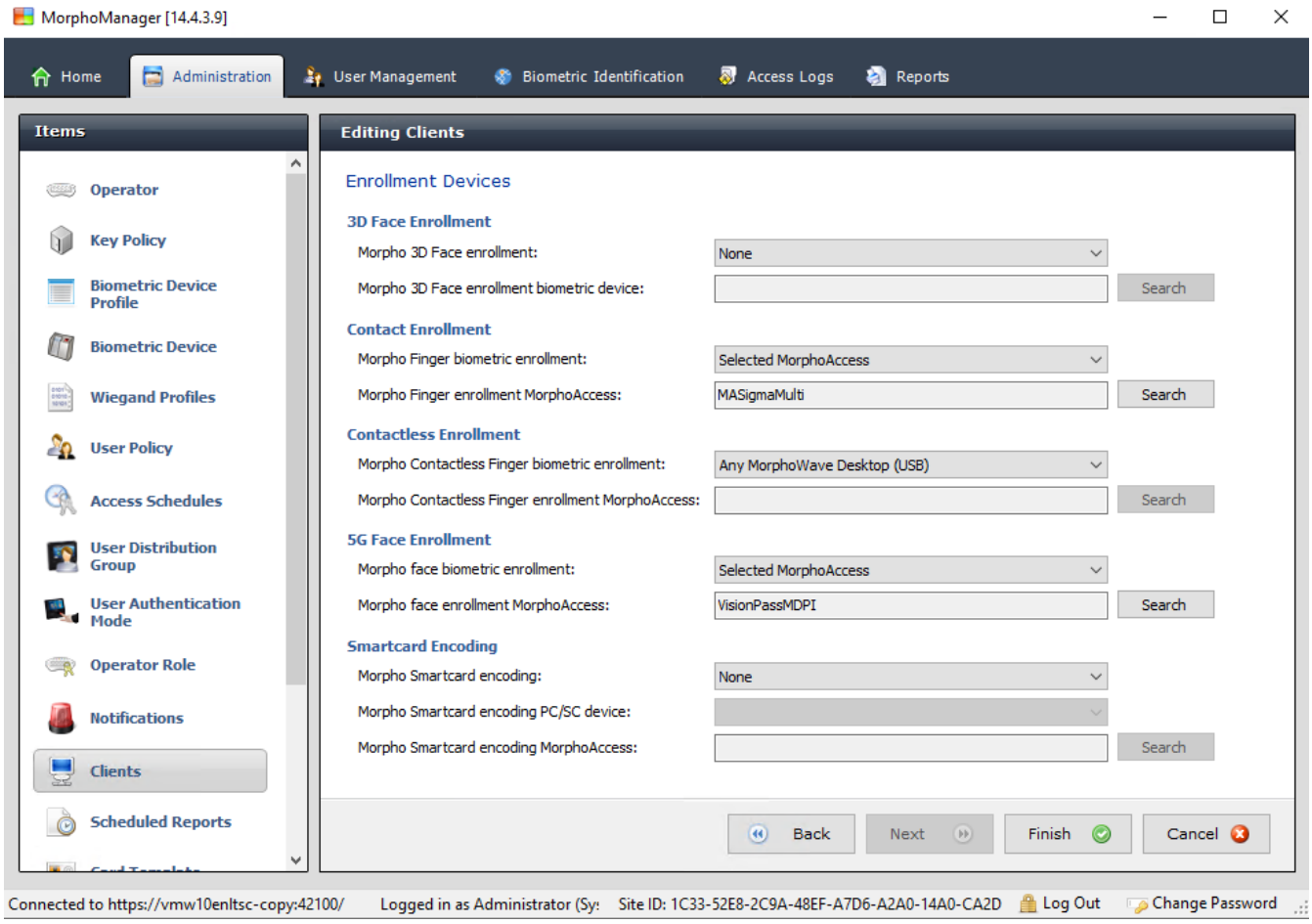
7. Cochez les cases des onglets que vous souhaitez afficher sur le client d'inscription :
   - **Administration,**
   - **User Management (Gestion des utilisateurs),**
   - **Reports (Rapports),**
   - **Access Logs (Journaux d'accès),**
   - **Biometric Identification (Identification biométrique)**
8. Cliquez sur **Next (Suivant)**.



9. En regard de **Camera (Caméra) :**, sélectionnez `No camera` dans la liste
10. Cliquez sur **Next (Suivant)**.



11. En regard de **Key Policy (Politique clé)**, sélectionnez `Default` dans la liste
12. Cliquez sur **Next (Suivant)**.



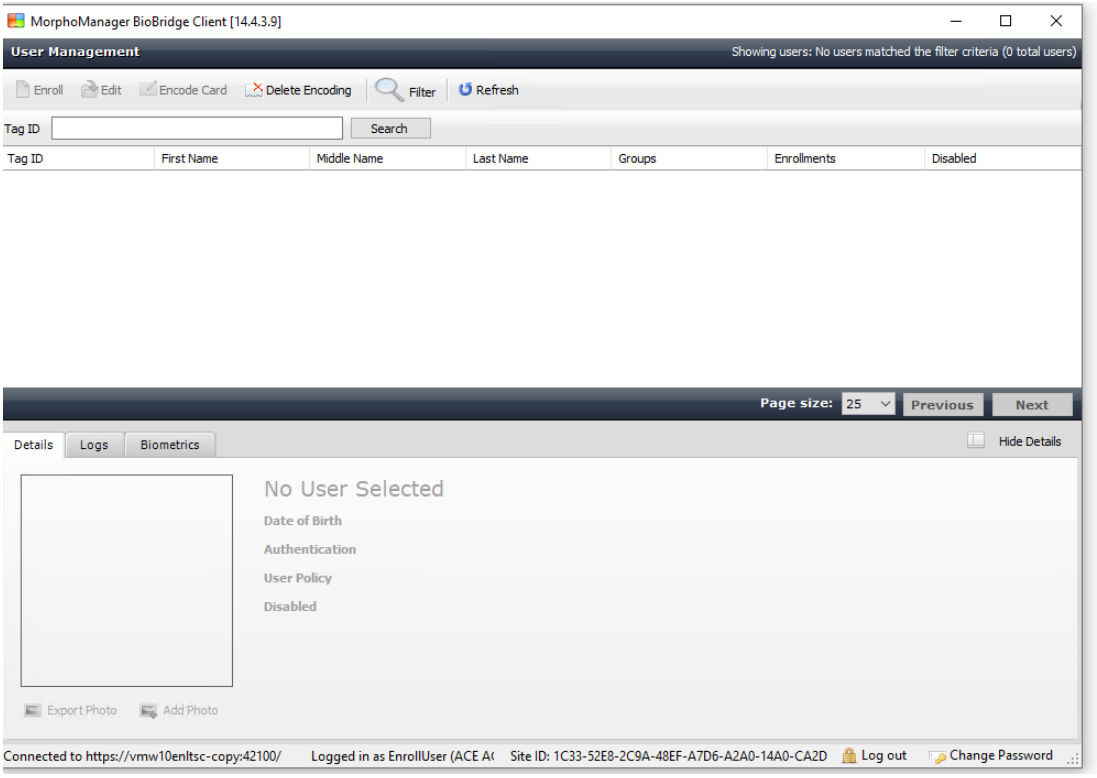
13. Sélectionnez le lecteur d'inscription biométrique que vous souhaitez utiliser sur le poste d'inscription
14. Cliquez sur **Finish (Terminer)**
15. Fermez l'application MorphoManager

Se reporter à

– *Configuration du client d'inscription BioBridge, page 185*

22.5.3 Tester le client d'inscription

1. Dans le répertoire d'installation de MorphoManager (par défaut : `C:\Program,Files(x86)\Morpho\MorphoManager\Client\`) , exécutez le fichier `ID1.ECP4.MorphoManager.BioBridgeEnrollmentClient.exe`



1. Assurez-vous que vous pouvez appeler l'écran d'inscription sans avoir à saisir le nom d'utilisateur et le mot de passe de l'opérateur d'inscription.

22.6 Notes techniques et limites

Systèmes d'exploitation Windows officiellement pris en charge
IDEMIA prend en charge les mêmes versions de Windows 10 que Bosch ACS..

Version officiellement prise en charge de Microsoft SQL Server
La version prise en charge est SQL Server 2017

Un système IDEMIA par système d'accès
Un système de contrôle d'accès Bosch ne peut prendre en charge qu'un seul système IDEMIA.

Une carte IDEMIA par détenteur de carte.
Les systèmes de contrôle d'accès Bosch prennent en charge plusieurs cartes par détenteur de carte, mais IDEMIA n'en prend en charge qu'une seule. Ainsi, lors de l'inscription, et lors de la synchronisation avec BIS, la première carte valide (c'est-à-dire avec le statut=1) de type « Accès », « Temporaire » ou « Parking » est attribuée à IDEMIA. Si la carte est bloquée par la suite, son numéro est toujours transmis et enregistré dans le journal des événements.

Nombre maximum de détenteurs de la carte IDEMIA
BioBridge MorphoManager peut gérer jusqu'à 100 000 détenteurs de carte.

Nombre maximum de groupes d'accès
IDEMIA prend en charge jusqu'à 5000 groupes d'accès (groupes de distribution d'utilisateurs). Ceux-ci sont mappés aux **classes de personne** dans le système de contrôle d'accès Bosch.

Performances du téléchargement de modèles
– 1000 modèles pour 1 dispositif : le téléchargement prend moins d'une minute.
– 1000 modèles pour 100 dispositifs : le téléchargement prend quelques minutes.

IDEMIA ne prend pas en charge les divisions
Lorsqu'un système IDEMIA est intégré, un système ACS n'est pas en mesure de filtrer de manière fiable les détenteurs de cartes d'une division des opérateurs de contrôle d'accès d'une autre division. Si une confidentialité absolue est obligatoire entre les divisions, n'intégrez pas de système IDEMIA.

Cartes virtuelles / Accès par code PIN seul.
IDEMIA ne prend pas en charge l'accès par code PIN uniquement. Une carte physique est requise.

Fonctionnalité de doigt sous contrainte IDEMIA
La fonctionnalité de doigt sous contrainte IDEMIA n'est actuellement pas prise en charge par les contrôleurs AMC.

Ensemble minimal de critères d'identification.
L'inscription au système IDEMIA requiert au moins les critères d'identification suivants :
– Prénom,
– Nom,
– Classe de personne
– Une carte physique attribuée au détenteur de la carte.

États affichés sur les lecteurs
Aucun état du lecteur (par ex. « dispositif bloqué ») n'est affiché sur les lecteurs Wiegand et OSDP.

Sauvegarde et Restauration
Avant de restaurer une sauvegarde avec IDEMIA, supprimez et recréez la base de données IDEMIA à l'aide de l'outil fournisseur IDEMIA DataBridge.
Dans la boîte de dialogue **Biometric device (Dispositif biométrique)**, assurez-vous que toutes les configurations ont été envoyées correctement aux lecteurs IDEMIA. Si l'une des tâches de synchronisation a échoué, recréez la configuration du lecteur :
1. Dans MorphoManager, accédez à **Biometric device (Dispositif biométrique)**.
2. Sélectionnez le dispositif concerné.
3. Cliquez sur **Rebuild (Recréer)**.

Compatibilité des fonctionnalités de la carte ACS avec les modes d'authentification IDEMIA :

Fonctionnalité	Mode : Carte ET Bio	Mode : Carte OU Bio

Cartes d'accès : Insérer	OK	OK
Cartes d'accès : Mettre à jour	OK	OK
Cartes d'accès : Supprimer	OK	OK
Cartes d'accès : Cartes multiples	Première carte uniquement	Première carte utilisée pour la biométrie.
Carte de remplacement	OK	OK
Carte temporaire	OK	OK
Carte temporaire : Période seulement	OK	OK
Carte temporaire : désactivation périodique immédiate de toutes les cartes	OK	OK
Carte temporaire : activation automatique des cartes après une période définie	OK	OK
Carte temporaire : désactivation et activation automatique des cartes	OK	OK
Cartes d'alarme	Non pris en charge	OK
Mode Bureau	Non pris en charge (*)	Non pris en charge (*)
Visiteur	Il est possible que les données biométriques du premier visiteur restent affectées à la carte.	Il est possible que les données biométriques du premier visiteur restent affectées à la carte.
Garde	Non pris en charge	Aucune biométrie prise en charge. La carte fonctionne.
Carte de stationnement	OK	OK
Code PIN	Non pris en charge (*)	Non pris en charge (*)
Validation par un tiers	Pas de code PIN (*)	Pas de code PIN (*)
(*) Lecteur IDEMIA non utilisable comme lecteur clavier		

23 Respect de la norme EN 60839

Introduction

EN 60839 est une famille de normes internationales européennes pour le matériel et les logiciels des dispositifs suivants :

- systèmes d'alarme et de sécurité électronique
- systèmes de contrôle d'accès électroniques

Pour garantir la conformité de votre système de contrôle d'accès à cette norme, certaines parties de la configuration peuvent devoir être adaptées. La liste suivante contient les parties les plus importantes. Pour une liste complète, veuillez consulter la norme telle qu'adoptée dans votre propre pays.

Exigences relatives à l'utilisation d'AMS 4.0 en tant que système certifié EN 60839, niveau 2

- Le système répond aux exigences de l'anti-passback global en termes d'utilisation d'une zone par MAC.
- Les différents fuseaux horaires utilisables du système AMS dépendent du nombre de MAC. Un fuseau horaire distinct peut être utilisé pour chaque MAC.
- Le câblage des contacts de porte ne doit pas empêcher l'ouverture de la porte pour une évacuation d'urgence déclenchée par un système anti-incendie ou anti-intrusion.
- Seuls les lecteurs OSDP utilisent le cryptage sur l'interface RS485.
- L'accès au mode de configuration doit être strictement contrôlé. Cela peut être réalisé, par exemple, en localisant les ordinateurs dans des zones sécurisées, et par des délais d'attente sur les sessions de connexion, en particulier des délais d'inactivité au niveau de l'application et du système d'exploitation.
- Les câblages réseau et électrique doivent être placés dans une zone sécurisée ou enfermés dans des canalisations.
- Seuls les lecteurs de cartes peuvent être montés dans des zones non sécurisées ; tous les autres dispositifs doivent se trouver dans des zones sécurisées.
- La longueur minimale des codes PIN de vérification pour les informations d'identification biométriques ou physiques doit être d'une longueur au moins égale à `4`.
- La longueur minimale des codes PIN d'identification doit être d'une longueur au moins égale à `8`.
- L'ordinateur serveur principal, les serveurs de connexion, les serveurs MAC et les clients doivent être synchronisés avec un serveur de temps réseau.
- La surveillance de l'alimentation doit être activée sur les contrôleurs d'accès locaux (par exemple, les AMC).
- Le fonctionnement hors ligne des contrôleurs d'accès locaux (par ex. AMC) n'est autorisé qu'en cas de panne du réseau. Par exemple, le paramètre AMC **Délai d'attente de l'hôte** ne doit pas être défini sur `0`.

Règles relatives à la puissance des mots de passe

- La longueur minimale du mot de passe doit être d'au moins `5` caractères.

24 Définition des profils et des autorisations d'accès

24.1 Création d'autorisations d'accès

Chemin d'accès à la boîte de dialogue

Menu principal > **System data (Données système)** > **Authorizations (Autorisations)**

Procédure

1. Dans la barre d'outils, cliquez sur **New (Nouveau)**  pour effacer les champs de saisie.

   Vous pouvez également cliquer sur **Copy (Copier)**  pour créer une nouvelle autorisation à partir d'une autorisation existante.
2. Entrez un nom unique pour l'autorisation.
3. (Facultatif) Entrez une description.
4. (Facultatif) Sélectionnez un modèle horaire pour gérer cette autorisation.
5. (Facultatif) Choisissez une **Limite d'inactivité (Inactivity limit)** dans la liste.
   Il s'agit d'une période déterminée de 14 à 365 jours. Si la personne à laquelle cette autorisation a été attribuée ne l'utilise pas dans la période définie, elle perd son autorisation. Chaque fois que la personne utilise l'autorisation, la période programmée repart de zéro.
6. (Obligatoire) Attribuez au moins une **entrée**.
   Les entrées existantes sont répertoriées dans les différents onglets, en fonction des modèles de porte.
   (Générique) **Entrance (Entrée)**, **Time management (Gestion du temps)**, **Elevator (Ascenseur)**, **Parking lot (Parking)**, **Arming Intrusion detection (Armement de la détection d'intrusion)**.
   Sélectionnez les entrées individuelles dans les listes des divers onglets, tel que décrit ci-dessous.
   Vous pouvez également utiliser les boutons **Assign all (Tout attribuer)** et **Remove all (Tout supprimer)** dans chaque onglet.
   - Dans l'onglet **Entrance (Entrée)**, cochez la case **In (Intérieur)** ou la case **Out (Extérieur)**, ou les deux à la fois, pour sélectionner une entrée.
   - Dans l'onglet **Time management (Gestion du temps)** (pour les lecteurs de contrôle de durée et de présence), cochez la case **In (Intérieur)** ou la case **Out (Extérieur)**, ou les deux à fois.
   - Dans l'onglet **Elevator (Ascenseur)**, sélectionnez les différents étages.
   - Dans l'onglet **Parking lot (Parking)**, sélectionnez un parking et une zone de stationnement.
   - Dans l'onglet **Arming Intrusion detection (Armement de la détection d'intrusion)**, sélectionnez **Armed (Armé)** ou **Disarmed (Désarmé)**.
7. Sélectionnez le MAC approprié dans la liste.
8. Cliquez sur Save (Enregistrer)  pour enregistrer l'autorisation.

Remarque!
Les modifications apportées ultérieurement aux autorisations affecteront les personnes autorisées existantes, sauf si leur profil est « verrouillé ».
Exemple : si une limite d'inactivité de 60 jours est réduite à 14 jours, toutes les personnes qui n'auront pas utilisé leur autorisation au cours des 14 derniers jours perdront celle-ci.
Exception : si une autorisation fait partie d'un profil d'accès **verrouillé** pour un identifiant d'employé (type de personne), les personnes de ce type ne seront pas affectées par les limites d'inactivité applicables à l'autorisation. Le verrouillage des profils peut être effectué via la case à cocher suivante :
Menu principal > **System data (Données système)** > **Person Types (Types de personnes)** > tableau : **Predefined Employee IDs (Identifiants prédéfinis d'employés)** > case à cocher : **Profile locked (Profil verrouillé)**

24.2 Création de profils d'accès

Remarque : utilisation des profils d'accès pour regrouper des autorisations
Pour des raisons pratiques et de cohérence, les autorisations d'accès ne sont pas attribuées individuellement. Elles sont généralement regroupées en **profils d'accès** et attribuées en tant que tels.
– Menu principal : **> System data (Données système)** > **Access profiles (Profils d'accès)**

Conditions préalables
Les autorisations d'accès ont déjà été définies dans le système.

Procédure

1. Dans la barre d'outils, cliquez sur **New (Nouveau)**  pour effacer les champs de saisie.

   Vous pouvez également cliquer sur **Copy (Copier)**  pour créer un nouveau profil à partir d'un profil existant.
2. Entrez un nom unique pour le profil.
3. (Facultatif) Entrez une description.
4. (Facultatif) Cochez la case **Visitor profile (Profil visiteur)** pour limiter ce profil aux visiteurs.
5. (Facultatif) Définissez une valeur pour **Standard duration of validity (Durée de validité standard)**.
   – Si aucune valeur n'est définie, le profil restera attribué indéfiniment.
   – Si une valeur est définie, elle sera utilisée pour calculer la date d'expiration des attributions ultérieures de ce profil.
6. (Obligatoire) Attribuez au moins une **autorisation** :
   les autorisations disponibles sont répertoriées sur la droite.
   Les autorisations déjà attribuées sont répertoriées sur la gauche.
   Sélectionnez des éléments, puis cliquez sur les boutons qui se trouvent entre les listes pour déplacer les éléments d'une liste à l'autre.
   –  attribue l'élément sélectionné.
   –  annule l'attribution de l'élément sélectionné.
7. Cliquez sur Save (Enregistrer)  pour enregistrer ce profil.

25 Création et gestion des données du personnel

Chemin d'accès à la boîte de dialogue

Menu principal > **Personnel data (Données du personnel)** > <zones de boîte de dialogue>

Procédure générale

1. Dans la zone **Persons (Personnes)**, entrez les identifiants de la personne.
2. Dans la zone **Cards (Cartes)** :
   - Attribuez les profils d'accès ou les autorisations d'accès individuelles.
   - Attribuez un modèle horaire, si nécessaire.
   - Attribuez une carte.
3. Dans la zone **PIN-Code (Code PIN)**, attribuez un code PIN, si nécessaire.
4. Dans la zone **Print Badges (Imprimer badges)**, imprimez la carte.

Pour les **visiteurs**, procédez comme suit :

- Entrez les données personnelles dans la boîte de dialogue **Visitors (Visiteurs)** du menu **Visitors**, puis attribuez un accompagnateur, si nécessaire.

Remarque!

Il n'est pas nécessaire d'attribuer les cartes et les autorisations d'accès en même temps. Il est donc possible d'attribuer des cartes à des personnes sans leur attribuer d'autorisations d'accès ou inversement. Toutefois, dans les deux cas, tous les accès sont refusés à ces personnes.

Processus de lecture des cartes

Lorsque les cartes sont scannées par les lecteurs, ceux-ci procèdent à un certain nombres de vérifications :

- La carte est-elle valide et est-elle enregistrée dans le système ?
- Son détenteur est-il actuellement bloqué (désactivé dans le système) ?
- Le détenteur de la carte est-il autorisé à accéder à cette zone ?
- L'autorisation d'accès est-elle une autorisation horaire ? Si tel est le cas, l'heure de lecture de la carte est-elle comprise dans les plages définies par ce modèle horaire ?
- L'autorisation d'accès est-elle active, c'est-à-dire ni **expirée** ni **bloquée** (désactivée) ?
- Le détenteur de la carte est-il soumis à un modèle horaire ? Si tel est le cas, l'heure de lecture de la carte est-elle comprise dans les intervalles définis ?
  Condition préalable : les vérifications du modèle horaire doivent être activées sur le lecteur concerné.
- Selon la Surveillance des séquences d'accès, le détenteur de la carte se trouve-t-il au bon endroit ?
  Condition préalable : la surveillance des séquences d'accès est activée sur le lecteur concerné.
- Un nombre maximal de personnes a-t-il été défini pour la zone de destination de ce lecteur et ce nombre est-il déjà atteint ?
- Dans le cas d'une surveillance des séquences d'accès, notamment dans le cadre de la fonctionnalité anti-retour : cette carte est-elle lue par le lecteur avant que la délai de blocage défini par la fonctionnalité anti-retour ne soit atteint ?
- Un code PIN supplémentaire est-il requis ? **Condition préalable** : le lecteur doit être doté d'un clavier.
- Si un niveau de menace est activé, le **profil de sécurité des personnes** du détenteur de la carte présente-t-il un **niveau de sécurité** au moins égal au niveau de sécurité du lecteur à ce niveau de menace ?

25.1 Personnes

Le tableau suivant répertorie les données affichées *par défaut* dans les boîtes de dialogue **Persons (Personnes)**. Ces boîtes de dialogue sont personnalisables. Voir la section **Champs personnalisés pour les données du personnel**.
Presque tous les champs sont facultatifs. Les champs obligatoires sont clairement signalés par un libellé mis en évidence dans l'interface utilisateur.

Onglet	**Nom du champ**
Nom de la boîte de dialogue	Nom
	Prénom
	Nom de jeune fille
	N° du personnel
	Date de naissance
	Identifiant employé (également appelé Type de personne)
	Sexe
	Société
	Titre
	N° de badge
	N° immatriculation
Adresse	Code postal
	Rue, n°
	Pays, état
	Nationalité
Coordonnées	Autre n° tél.
	Tél. de la société
	Fax de la société
	Tél. mobile
	Téléphone
	E-Mail
	Adresse page Web
Données supplémentaires sur la personne	Patronyme
	Lieu de naissance
	Statut marital
	Document d'identité officiel
	N° du document d'identité
	Valide jusqu'à

	Taille
Données supplémentaires sur la société	Département
	Emplacement
	Centre de coûts
	Fonction
	Accompagnateur
	Motif de la visite
	Remarques
Remarques	(Présente un champ de texte à structure libre pour y entrer les remarques concernant la personne.
Autres info.	10 champs définissables par l'utilisateur
Appareil	Permet de capturer, de réenregistrer et de supprimer des signatures.
Empreintes digitales	Permet de capturer, de réenregistrer, de supprimer et de tester les empreintes digitales en tant qu'identifiants biométriques. Permet de désigner certaines empreintes pour signaler la contrainte.

Se reporter à

– *Champs personnalisés pour les données de personnel, page 136*

25.1.1 Options de contrôle des cartes ou des bâtiments

Présentation

Utilisez l'onglet **Card control (Contrôle carte)** pour permettre aux détenteurs de carte d'activer 1 ou 2 sorties de contrôleur d'accès générique avec leur carte. Pour donner cette possibilité au détenteur de carte, cochez la case **Building control (Contrôle bâtiment)** dans la boîte de dialogue **Persons (Personnes)**. Les cases à cocher **Building control (Contrôle bâtiment)** (ou **Card control [Contrôle carte]**) sont des champs personnalisés prédéfinis visibles par défaut dans l'onglet **Contrôle carte** de la personne, mais il est possible de les placer ailleurs.

L'option de contrôle de bâtiment consiste essentiellement en deux opérations décrites ci-dessous :

– Configuration de la case à cocher : donnez-lui un libellé approprié et (si vous le souhaitez) placez-la dans un autre onglet de la boîte de dialogue **Persons (Personnes)**.
– Affectez la fonctionnalité à une sortie sur un contrôleur d'accès AMC et à une case à cocher.

Conditions préalables

– La sortie du contrôleur d'accès est raccordée électriquement à l'appareil devant être activé à l'aide de la carte.

Chemin d'accès à la boîte de dialogue

– Menu principal AMS > **Configuration** > **Options** > **Custom fields (Champs personnalisés)** > onglet **Card control (Contrôle carte)**

Configuration des cases à cocher

1. Dans la page **Custom fields (Champs personnalisés)**, sélectionnez l'onglet **Details (Détails)** dans le volet supérieur.
2. Localisez la fonctionnalité **Building control (Contrôle bâtiment)**, 1 ou 2, que vous souhaitez utiliser.
3. Remplacez le libellé par un nom approprié (recommandé). Si vous le souhaitez, placez la case à cocher dans un onglet autre que **Card control (Contrôle carte)**. Voir la section **Aperçu et modification des champs personnalisés** (lien ci-dessous), pour des instructions plus détaillées.

Affectation de la fonctionnalité à une sortie du contrôleur d'accès et à une case à cocher

Voir la section **Paramètres et réglages AMC** (lien ci-dessous).

1. Dans l'**éditeur de dispositif**, dans l'arborescence des périphériques, sélectionnez le contrôleur d'accès AMC dont vous souhaitez utiliser le signal de sortie.
2. Dans le volet supérieur de l'onglet **Outputs (Sorties)**, sélectionnez la sortie que vous souhaitez utiliser.
3. Dans le volet central, **Output data (Données de sortie)**, sélectionnez le type **25, Card control (Contrôle carte)**.
4. Cliquez sur le bouton **>** pour ajouter la sortie au volet inférieur.
5. Dans le volet inférieur, colonne **Param11**, sélectionnez le libellé de la fonctionnalité de contrôle du bâtiment que vous avez sélectionnée dans la procédure précédente **Configuration des cases à cocher**.
6. Enregistrez l'arborescence des périphériques.

Se reporter à

– *Paramètres et réglages AMC, page 58*
– *Aperçu et modification des champs personnalisés, page 136*

25.1.2 Informations supplémentaires : enregistrement des informations définies par l'utilisateur

Utilisez l'onglet **Extra info (Autres informations)** pour définir des champs supplémentaires qui ne figurent pas dans les autres onglets. Si aucun champ supplémentaire n'a été défini, l'onglet reste vide.

25.1.3 Enregistrement des signatures

Afin de pouvoir capturer les signatures, une tablette de capture de signature de la société Signotec doit être connectée et configurée dans le système. En cas de doute, consultez votre administrateur système.

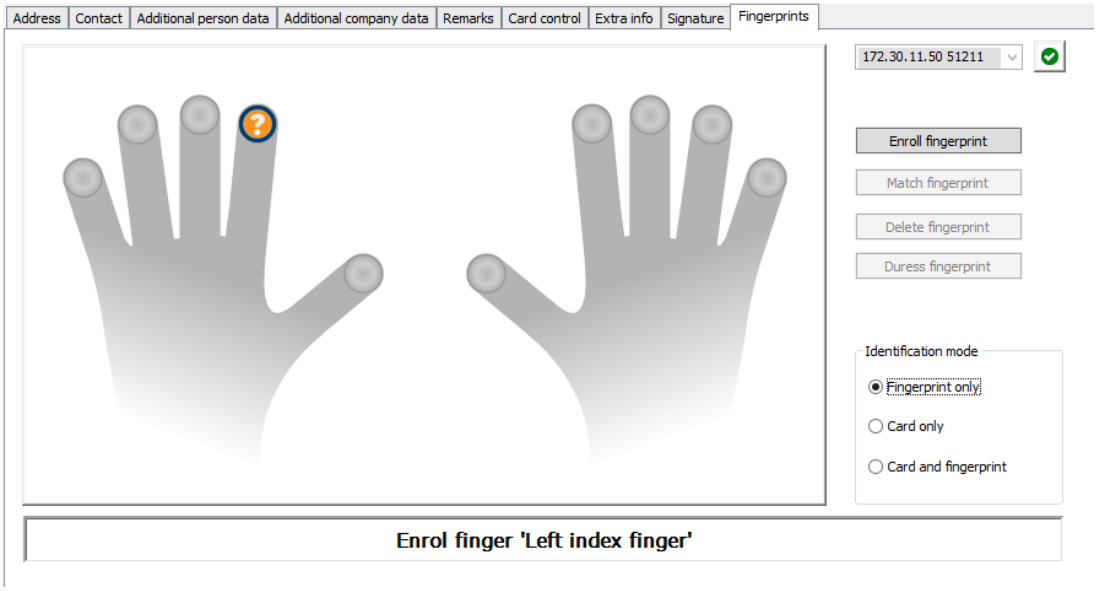
1. Cliquez sur l'onglet **Signature**.
2. Cliquez sur le bouton **Capture Signature (Capturer la signature)** pour enregistrer une nouvelle signature.
3. Signez directement sur la tablette à l'aide de son stylet spécial.
4. Cliquez sur la coche figurant sur la tablette pour confirmer.
   La nouvelle signature est à présent affichée à l'écran. (Cliquez sur la signature pour agrandir la vue.)

Procédures associées :

– Cliquez sur le bouton **Capture Signature (Capturer la signature)** pour remplacer une signature existante.

– Cliquez sur le bouton de **Delete Signature (Supprimer la signature)** pour supprimer une signature existante.

25.1.4 Inscription des données d'empreintes digitales



Conditions préalables

– Pour pouvoir effectuer un contrôle d'accès biométrique, un ou plusieurs lecteurs d'empreintes digitales doivent être configurés aux entrées.
– IMPORTANT : ces lecteurs reçoivent et stockent périodiquement les données de cartes et d'empreintes digitales des serveurs. Au final, ce sont les paramètres de chaque lecteur qui définissent quelles informations d'identification sont acceptées. Ceux-ci remplacent tous les paramètres définis pour la personne.
– Afin de pouvoir utiliser les empreintes digitales comme mode de vérification (ou de substitution) de l'authentification par carte, tous les titulaires de carte doivent faire scanner leurs empreintes digitales.
– La personne inscrite se trouve devant un lecteur d'empreintes digitales connecté à votre poste de travail et configuré pour celui-ci. Ce lecteur d'inscription d'empreintes digitales ne doit **pas** être un lecteur de contrôle d'accès.
– En tant qu'opérateur, vous communiquez directement avec la personne inscrite, c'est-à-dire avec la personne dont les empreintes digitales doivent être enregistrées comme informations d'identification biométriques pour l'accès.
– Vous avez pris connaissance de la manière de présenter le doigt à plusieurs reprises sur le lecteur concerné pour lui permettre de capturer efficacement les empreintes digitales.

Procédure d'inscription d'une empreinte digitale pour le contrôle d'accès

1. Accédez à la boîte de dialogue des empreintes digitales : **Personnel data (Données du personnel)** > **Persons (Personnes)** > onglet : **Fingerprints (Empreintes digitales)** et créez ou recherchez la personne inscrite dans la base de données.
2. Demandez à la personne inscrite quel doigt elle souhaite utiliser pour accéder habituellement au lecteur d'empreintes digitales.
3. Sélectionnez le doigt correspondant dans le diagramme des mains.
   Un point d'interrogation s'affiche alors sur le bout du doigt.

4. Cliquez le bouton **Enroll fingerprint (Inscrire l'empreinte digitale)**.
5. Expliquez à la personne inscrite comment présenter son doigt au lecteur.
   Des exemples d'instructions sont disponibles dans le volet situé sous le diagramme des mains, mais différents types de lecteurs peuvent nécessiter des procédures légèrement différentes.
6. Si l'empreinte digitale est correctement inscrite, une fenêtre de confirmation apparaît.
7. Sélectionnez un **mode d'identification (Identification mode)** ; cela détermine les informations d'identification qu'un lecteur d'empreintes digitales exige de la personne inscrite lorsqu'elle demande l'accès. Notez que le mode défini ici ne prendra effet que si le paramètre **Person-dependent verification (Vérification dépendant de la personne)** du lecteur a été sélectionné.
   Les options sont les suivantes :
   - **Fingerprint only (Empreinte digitale uniquement)** : seul le scanner d'empreintes digitales du lecteur est utilisé.
   - **Card only (Carte uniquement)** : seul le scanner de cartes du lecteur est utilisé.
   - **Carte et empreintes digitales (Card and fingerprint)** : les deux scanners du lecteur sont utilisés. La personne inscrite devra présenter la carte et le doigt choisi au lecteur pour obtenir l'accès.
8. Cliquez sur  (Save [Enregistrer]) pour enregistrer l'empreinte digitale et le mode d'identification de la personne inscrite.

Remarque!
Les paramètres du lecteur remplacent les paramètres de la personne
Notez que le mode d'identification choisi dans la boîte de dialogue relative aux empreintes digitales ne fonctionnera que si le lecteur d'empreintes digitales lui-même est configuré avec l'option **Person-dependent verification (Vérification dépendant de la personne)** dans l'éditeur de dispositif. En cas de doute, consultez votre administrateur système.

Procédure d'inscription d'une empreinte digitale pour signaler la contrainte
Conditions préalables :

- Les lecteurs d'empreintes digitales ne peuvent envoyer des signaux de contrainte que s'ils sont configurés dans l'**éditeur de dispositif** de la manière suivante : onglet **Network & Operation mode (Réseaux & Modes de fonctionnement)** > **Templates on server (Modèles sur le serveur)** > **Card and fingerprint (Carte et empreintes digitales)**.
- Au moins une empreinte digitale de la personne a déjà été inscrite et stockée avec succès.
- Le lecteur d'empreintes digitales est en ligne. En mode hors ligne, le lecteur ne peut bien entendu pas envoyer de signal de contrainte au système.

1. Demandez à la personne inscrite de choisir le doigt qu'elle souhaite utiliser pour signaler la contrainte, c'est-à-dire dans le cas où une personne non autorisée la forcerait à utiliser le lecteur d'empreintes digitales.
2. Répétez la procédure d'inscription des empreintes digitales décrite ci-dessus pour ce doigt.

3. Lorsque la deuxième empreinte digitale est correctement enregistrée, sélectionnez-la dans le diagramme des mains, puis cliquez sur le bouton **Duress finger (Doigt sous contrainte)**.
   Le doigt désigné est marqué d'un point d'exclamation dans le diagramme des mains.

Si, par la suite, la personne inscrite utilise le doigt sous contrainte sur un lecteur d'empreintes digitales et si ce dernier n'est pas hors ligne, le système signalera la contrainte à l'opérateur en affichant une fenêtre contextuelle.

Procédure de test des empreintes digitales stockées

1. Dans le diagramme des mains, sélectionnez l'empreinte digitale que vous souhaitez tester.
2. Demandez à la personne inscrite de placer ce doigt sur le lecteur.
3. Cliquez sur le bouton **Match fingerprint (Faire correspondre l'empreinte digitale)**.
   Une fenêtre contextuelle confirme si l'empreinte digitale stockée correspond ou non à celle placée sur le lecteur. Notez qu'il est possible de devoir répéter cette procédure pour réduire la probabilité d'une fausse alarme.

Procédure de suppression d'empreintes digitales enregistrées

1. Dans le diagramme des mains, sélectionnez l'empreinte digitale que vous souhaitez supprimer.
2. Cliquez sur le bouton **Delete fingerprint (Supprimer l'empreinte digitale)**.
3. Attendez la confirmation de la suppression.

25.2 Sociétés

- Cette boîte de dialogue peut être utilisée pour créer de nouvelles sociétés et modifier ou supprimer des données de société existantes.
- La saisie du nom et de l'abréviation du nom de la société est obligatoire. Le nom abrégé doit être unique.
- Si la saisie d'un nom de société est obligatoire dans la boîte de dialogue **Persons (Personnes)**, créez la société dans cette boîte de dialogue avant de tenter de créer des enregistrements de personnel pour cette même entreprise.
- Les sociétés ne peuvent pas être supprimées du système si des enregistrements de personnel leur sont encore attribués.

25.3 Cartes : création et attribution d'informations d'identification et d'autorisations

L'objet de cette boîte de dialogue est d'attribuer des **cartes**, des **autorisations d'accès** ou des ensembles d'autorisations d'accès appelés **profils d'accès** aux enregistrements de personnel.
Les autorisations et les profils d'accès sont attribués aux personnes et non aux cartes.
Les nouvelles cartes attribuées à une personne bénéficient des autorisations d'accès déjà attribuées à cette personne.

Remarque : utilisation des profils d'accès pour regrouper des autorisations
Pour des raisons pratiques et de cohérence, les autorisations d'accès ne sont pas attribuées individuellement. Elles sont généralement regroupées en **profils d'accès** et attribuées en tant que tels.

– Menu principal : **> System data (Données système)** > **Access profiles (Profils d'accès)**

Liste des attributs de carte
La liste des attributs de la carte appartenant à la personne sélectionnée s'affiche dans la boîte de dialogue Cards (Cartes). Parmi les attributs affichés dans la liste figurent :
– Le type d'utilisation de la carte.
– Un indicateur montrant si la carte peut être utilisée par un système de verrouillage hors ligne configuré.
– Si la carte est bloquée en raison de l'utilisation répétée de codes PIN non valides. Cet état est mis en surbrillance.
– La date de création de la carte.
– Une date d'expiration (date de collecte) de la carte.
Remarque : si un lecteur de carte motorisé est utilisé, il peut physiquement retenir une carte expirée. Sinon, la carte est simplement invalidée.
– La date de la dernière impression de la carte et le nombre de cartes imprimées.
– Le détail des données de code.

Option **Administered globally (Administré de manière globale)**
Les données des personnes dont la case **Administered globally (Administré de manière globale)** (à côté du cadre photo) est cochée peuvent uniquement être modifiées par les opérateurs disposant du droit supplémentaire d'**administrateur global**.
Les données suivantes sont en lecture seule pour les opérateurs qui ne disposent pas de ce droit :
– Toutes les données de la boîte de dialogue **Persons (Personnes)**, hormis les onglets **Remarks (Remarques) et Extra info (Autres informations)**, ainsi que les champs personnalisés.
– Toutes les données de la boîte de dialogue **Cards (Cartes)**.
– Toutes les données de la boîte de dialogue **PIN Code (Code PIN)**.

Ce droit d'**administrateur global** peut être attribué via la case à cocher suivante :
– Menu principal : **Configuration** > **Operators and workstations (Opérateurs et postes de travail)** > **User rights (Droits de l'utilisateur)** > case à cocher : **Global Administrator (Administrateur global)**.

25.3.1 Attribution de cartes aux personnes

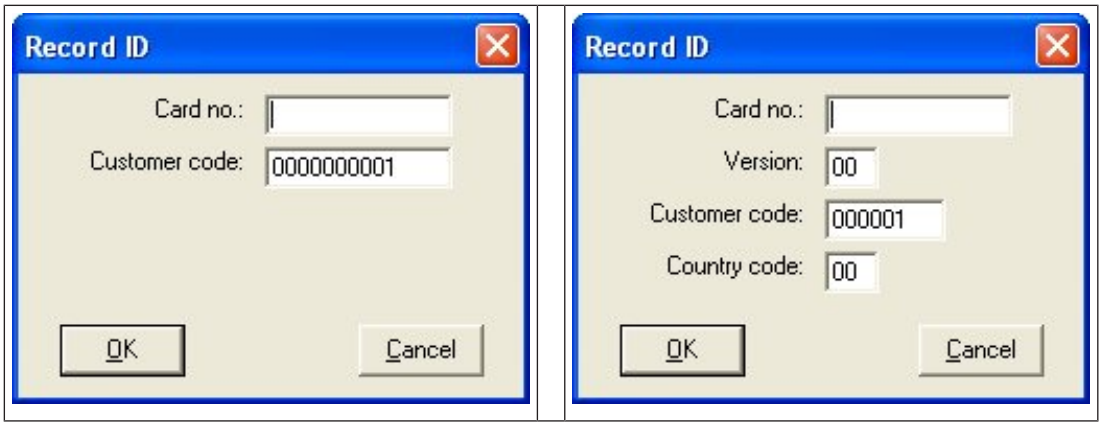
Introduction
Toutes les personnes soumises à un contrôle d'accès doivent disposer d'une carte ou d'un autre identifiant électronique qui leur est attribué via la boîte de dialogue **Cards (Cartes)**. Les numéros de carte peuvent être attribués manuellement ou via un lecteur d'inscription.

Chemin d'accès à la boîte de dialogue
Menu principal > **Personnel data (Données du personnel)** > **Cards (Cartes)**

Conditions préalables
– Vous avez chargé l'enregistrement de personnel auquel la carte est destinée dans l'en-tête de la boîte de dialogue **Cards (Cartes)**.

Saisie manuelle des données de la carte

Cliquez sur le bouton **Record card (Enregistrer carte)** pour attribuer une carte à une personne. Le masque de boite de dialogue **Record ID (ID d'enregistrement)** apparaît. L'une des deux boîtes de dialogue de saisie apparaît, selon le type de carte, les contrôleurs et les lecteurs utilisés.



Entrez manuellement le numéro imprimé sur la carte - des zéros sont automatiquement ajoutés afin que tous les numéros stockés comportent toujours 12 chiffres. Dans certains systèmes, aucun nouveau numéro de carte n'est attribué en cas de perte de la carte. À la place, le même numéro de carte est émis, mais avec un numéro de version plus élevé. Le code pays et le code client sont fournis par le fabricant et doivent être entrés dans le fichier d'enregistrement du système.

S'il n'est pas déjà utilisé par le système, le numéro de carte est attribué à la personne. Une fenêtre contextuelle confirme l'attribution.

Utilisation d'un lecteur d'inscription

Condition préalable

– Un lecteur d'inscription est configuré sur votre poste de travail.

Procédure d'inscription

1. Cliquez sur le bouton à droite du bouton **Record card (Enregistrer carte)** pour sélectionner un lecteur d'inscription configuré.

– Notez que pour modifier la sélection du lecteur d'inscription, vous devez être connecté au gestionnaire de dialogue ACE en tant qu'administrateur.

2. Cliquez sur le bouton **Record card (Enregistrer carte)** et suivez les instructions à l'écran.
3. Selon le type de lecteur, vous pouvez à présent saisir les détails de la carte dans une boîte de dialogue ou lire les données de la carte en la présentant au lecteur.

Procédure de changement de carte

1. Sélectionnez une carte dans la liste.
2. Cliquez sur le bouton **Change card (Changer de carte)**.
3. Dans la fenêtre contextuelle

– Sélectionnez **Replace card (Remplacer la carte)** si la carte d'origine est définitivement perdue ou endommagée.
– Sélectionnez **Temporary card (Carte temporaire)** si la carte d'origine a été égarée ou laissée à la maison et que seul un remplacement temporaire est nécessaire.
  – Entrez une période de validité pour la carte temporaire.
  – Indiquez si vous souhaitez désactiver toutes les autres cartes maintenant.

- Indiquez si les cartes d'origine doivent être réactivées automatiquement à l'expiration de la carte temporaire.

4. Cliquez sur **OK** pour enregistrer.

Supprimer des cartes

1. Sélectionnez une carte dans la liste.
2. Cliquez sur le bouton **Delete card (Supprimer la carte)** pour supprimer l'attribution d'une carte à une personne.

Remarque : si vous supprimez la dernière carte d'un détenteur de carte, le statut **désinscrit** (libellé rouge à côté de **Registered (Inscrit)** dans la barre d'état) lui est attribué. Cette personne n'est alors plus soumise au contrôle d'accès.

25.3.2 Imprimer des badges

Conditions préalables

- Le dossier personnel du nouveau détenteur de carte doit déjà exister dans le système.
- Un poste de travail avec le matériel suivant connecté, généralement via USB :
  - Une imprimante de badges
  - Une caméra pour capturer des photos d'identité.

Procédure

Chemin d'accès à la boîte de dialogue

Client AMS : **Personnel data (Données du personnel)** >**Print badges (Imprimer badges)**

1. Chargez l'enregistrement de personnel pour lequel la carte doit être imprimée.
2. Dans le menu déroulant **Layout (Disposition)**, sélectionnez la mise en page de carte souhaitée parmi les dispositions stockées.
3. Obtenez une photo d'identité de l'une des manières suivantes :
   - Cliquez sur le bouton **Capture (Capturer)** et sélectionnez la caméra souhaitée dans la liste des caméras connectées.
   - Cliquez sur le bouton **Import picture (Importer photo)** et utilisez le cadre de recadrage pour sélectionner la partie de la photo à imprimer sur la carte.
4. Cliquez sur **Preview (Aperçu)** pour vous assurer que les données et la disposition de celles-ci sur le badge sont correctes.
5. Cliquez sur **Print (Imprimer)** pour imprimer le badge.

Caméras prises en charge

Tous les périphériques USB que le système d'exploitation reconnaît en tant que caméra.

25.3.3 Onglet Authorizations (Autorisations)

Attribution d'autorisations regroupées sous la forme de profils d'accès

Le moyen le plus pratique et le plus flexible pour attribuer des autorisations aux détenteurs de carte consiste à les regrouper préalablement dans des profils d'accès, puis à attribuer le profil.

- Pour créer des profils d'accès, voir la section *Création de profils d'accès, page 197*
- Pour attribuer un profil d'accès au détenteur de carte, sélectionnez un profil défini dans la liste **Access profile (Profil d'accès)**.

Attribution directe d'autorisations d'accès
Dans l'onglet **Authorizations (Autorisations)** :
Toutes les autorisations d'accès déjà attribuées à la personne apparaissent dans la liste de gauche.
Toutes les autorisations d'accès disponibles pour l'attribution apparaissent dans la liste de droite.
Sélectionnez des éléments, puis cliquez sur les boutons situés entre les listes pour déplacer les éléments d'une liste à l'autre.

 attribue l'élément sélectionné.

 annule l'attribution de l'élément sélectionné.

 attribue tous les éléments disponibles.

 annule l'attribution de tous les éléments attribués.

Option : **Keep authorizations assigned (Conserver les autorisations attribuées)**
L'effet de l'attribution d'un profil d'accès à une personne dépend de la case à cocher **Conserver les autorisations attribuées** :

- Si cette case n'est pas cochée, toutes les sélections précédentes et toutes les autorisations d'accès déjà attribuées sont **remplacées** lorsque le profil est attribué.
- Si elle est cochée, les autorisations du profil sont **ajoutées** aux autorisations attribuées.

Limiter la durée des autorisations
Utilisez les champs de date **Valid from (Valide de)** et **until (à)** pour limiter les heures de début et de fin des autorisations et des profils. Si aucune valeur n'est définie, l'autorisation est valable immédiatement et sa durée est illimitée.

Cliquez sur  pour ouvrir une boîte de dialogue permettant de définir les durées des autorisations individuelles.

Afficher les entrées d'une autorisation
Cliquez avec le bouton droit sur une autorisation dans l'une ou l'autre des listes pour afficher les entrées qui lui sont associées.

25.3.4 Onglet Other data (Autres informations) : exemptions et autorisations spéciales

Attribuer un modèle horaire :
Utilisez la zone de liste **Time model (Modèle horaire)** pour spécifier les heures d'accès quotidiennes du détenteur de la carte, c'est-à-dire les périodes pendant lesquelles les informations d'identification de cette personne lui permettent de se voir accorder un accès.

Dispenser des personnes de la surveillance aléatoire
Cochez la case **Excluded from random screening (Exclu de la surveillance aléatoire)** pour les dispenser de faire l'objet d'inspections aléatoires aux entrées et aux sorties.

Dispenser des personnes des vérifications de code PIN
Cochez la case **Disable PIN code check (Désactiver la vérification du code PIN)** pour dispenser les personnes d'entrer leur code sur les lecteurs de code PIN en dehors des heures normales de travail.

Remarque!
Cette dispense affecte l'ensemble du système.
Par exemple, dans la mesure où les codes PIN de ces personnes ne sont pas vérifiés, celles-ci sont également dans l'incapacité d'armer ou de désarmer les alarmes aux entrées du modèle de porte 10.

Prolonger le temps d'ouverture de la porte
Cochez la case **Extended door opening time (Ouverture de porte prolongée)** pour donner plus de temps (par défaut, 3 fois plus) aux personnes handicapées de passer par une entrée avant que l'état **Door open too long (Porte ouverte trop longtemps)** ne soit activé.
Remarque : le facteur de prolongation par défaut peut être réinitialisé dans les propriétés du MAC, dans l'éditeur de dispositif.
Sélectionnez **Global Access Settings (Paramètres d'accès généraux)** >
Time factor for handicapped persons (Facteur temps pour les personnes handicapées).

Surveillance de tour
Un **tour** ou un **itinéraire** est une séquence de lecteurs stricte définie dans le menu du client : **Tour monitoring (Surveillance de tour)** > boîte de dialogue **Define routes (Définir des itinéraires)**.
Pour attribuer un tour à un détenteur de carte, cochez la case **Tour monitoring (Surveillance de tour)**, puis sélectionnez un tour défini dans la liste déroulante. Si aucun tour n'a été défini, la case à cocher sera inactive.
Lorsqu'un **tour** est attribué à un détenteur de carte, celui-ci est activé dès que la personne scanne sa carte sur le premier lecteur de la séquence. Tous les lecteurs de la séquence doivent ensuite être utilisés dans l'ordre, jusqu'à ce que le tour soit terminé. Les tours sont généralement utilisés pour appliquer des séquences d'accès précises dans des environnements industriels propres, des zones à haute sécurité ou des zones soumises à des règles d'hygiène strictes.

Permission to unlock doors (Autorisation de déverrouillage des portes)
Cochez cette case pour permettre au détenteur de la carte de déverrouiller les portes pendant une période prolongée, voir **Mode Bureau**.

Se reporter à
– *Autoriser des personnes à définir le mode Bureau, page 209*

25.3.5 Autoriser des personnes à définir le mode Bureau

Introduction
Le terme mode Bureau décrit la suspension du contrôle d'accès à une entrée pendant les heures de bureau ou d'activité. L'entrée demeure déverrouillée pendant ces heures, afin de permettre un accès public sans entrave. En dehors de ces heures, le mode normal s'applique : l'accès est accordé uniquement aux personnes qui présentent des identifiants valides au lecteur.
Le mode Bureau est souvent utilisé dans les petits commerces, les établissements d'enseignement et les hôpitaux.

Conditions préalables

Pour que le mode Bureau fonctionne, les conditions suivantes doivent être remplies :

Dans la configuration (arborescence des périphériques)

– Une ou plusieurs entrées doivent être configurées pour autoriser des périodes déverrouillées étendues.
– Au moins un lecteur à clavier doit être utilisé à l'entrée.

Dans le client (boîtes de dialogue Persons [Personnes])

– Un ou plusieurs détenteurs de carte doivent être autorisés à activer/désactiver le mode bureau pour l'entrée.
– Leurs cartes doivent être valides et autoriser l'accès à l'entrée à l'extérieure des heures du mode bureau.

Procédures pour autoriser des personnes à définir le mode Bureau

Procédure pour les détenteurs de carte individuels

1. Accédez à **Personnel data (Données du personnel)** > **Cards (Cartes)** > onglet : **Other data (Autre informations)** et créez ou recherchez le détenteur de carte désigné dans la base de données.
2. Cochez la case **Permission to unlock doors (Autorisation de déverrouillage des portes)**.
3. Cliquez sur l'icône de la disquette  pour enregistrer les données du détenteur de la carte.

Procédure pour les groupes de titulaires de carte

1. Accédez à **Personnel data (Données du personnel)** > **Groups of persons (Groupes de personnes)** et utilisez les critères de filtrage pour composer une liste de détenteurs de carte dans la zone de liste.
2. Dans la liste déroulante **Field to change (Champ à modifier)**, sélectionnez **Unlock doors (Déverrouiller les portes)**.
3. Cochez la case **Unlock doors (Déverrouiller les portes)**.
4. Cliquez sur le bouton **Apply changes (Appliquer les modifications)** pour enregistrer les données des détenteurs de carte.

Procédure d'activation et de désactivation du mode Bureau pour les détenteurs de carte

Pour activer ou désactiver le mode Bureau à une entrée, le détenteur de la carte doit appuyer sur la touche 3 du clavier, puis présenter sa carte d'autorisation spécifique au lecteur.

L'entrée reste déverrouillée jusqu'à ce qu'un détenteur de carte autorisé appuie sur la touche 3 et présente à nouveau la carte.

Notez que les gardiens dotés de cartes de garde peuvent désactiver le mode Bureau de la même manière, sans autorisation spéciale.

Remarque!

Mode Bureau et paramètres de l'appareil pour la porte

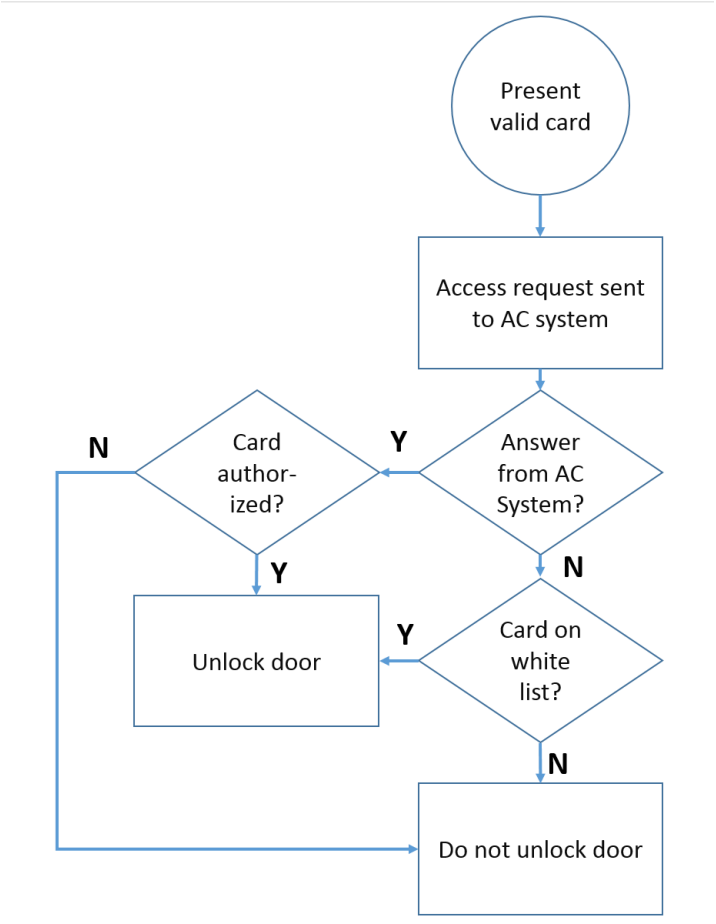
Le mode Bureau remplace le paramètre **Unlock door (Déverrouiller la porte)** de l'onglet **Options** d'une porte dans l'éditeur de dispositif. Seuls les modes **0 Normal mode (0 Mode normal)** et **1 Unlocked (1 Déverrouillé)** sont donc autorisés.

25.3.6 Onglet Smartintego

Systèmes de verrouillage SmartIntego

Introduction

Le lecteur de carte SmartIntego essaie d'abord d'autoriser l'accès via le système de contrôle d'accès principal. Si la connexion échoue, il recherche le numéro de carte dans la liste blanche enregistrée.



Les autorisations d'accès pour le système de verrouillage SmartIntego sont attribués de la même manière que toutes les autres autorisations d'accès.

Conditions préalables

- Un système de verrouillage SimonsVoss SmartIntego a été configuré dans votre système de contrôle d'accès. Consultez le guide de configuration pour obtenir des instructions.
- Les détenteurs de carte utilisent des cartes MIFARE Classic ou MIFARE Desfire. SmartIntego utilise le numéro de série de la carte (CSN).

Procédure d'attribution

La procédure suivante explique comment ajouter un numéro de carte à une liste blanche SmartIntego, en plus des autorisations déjà attribuées via le système de contrôle d'accès principal.

Les listes blanches sont stockées localement sur les portes SmartIntego. Un lecteur peut donc accorder l'accès aux numéros de carte figurant dans la liste blanche, même si la connexion au MAC est interrompue.
Les ajouts et suppressions effectués dans les listes blanches sont transmis aux lecteurs SmartIntego dès que les données du détenteur de carte sont enregistrées et qu'une connexion est disponible.

1. Dans le menu principal du client AMS, sélectionnez **Personnel data (Données du personnel)** > **Cards (Cartes)**.
2. Sélectionnez la personne à laquelle accorder les autorisations SmartIntego**.**
3. Sélectionnez l'onglet **SmartIntego.**
4. Procédez aux attributions :
   - Toutes les autorisations d'accès déjà attribuées à la personne apparaissent dans la liste de gauche.
   - Toutes les autorisations d'accès disponibles pour l'attribution apparaissent dans la liste de droite.

Sélectionnez des éléments, puis cliquez sur les boutons situés entre les listes pour déplacer les éléments d'une liste à l'autre.

 attribue l'élément sélectionné.

 annule l'attribution de l'élément sélectionné.

 attribue tous les éléments disponibles.

 annule l'attribution de tous les éléments attribués.

25.3.7 Création d'une carte d'alerte

Cette section explique comment créer une carte d'alerte pouvant être utilisée pour déclencher un niveau de menace.

Introduction

Une carte d'alerte est une carte qui déclenche un niveau de menace particulier lorsqu'elle est présentée à un lecteur. Un niveau de menace ne peut pas être annulé par une carte d'alerte, mais uniquement via le logiciel de contrôle d'accès.

Conditions préalables

- Un lecteur d'inscription est configuré sur votre système.
- Au moins un niveau de menace a été défini dans le système.

Chemin d'accès à la boîte de dialogue

Menu principal > **Personnel data (Données du personnel)** > **Cards (Cartes)** > **Alert card (Carte d'alerte)**

Procédure

1. Chargez le dossier Personne de la personne à laquelle la carte d'alerte sera attribuée.
2. Dans l'onglet de la carte d'alerte, cliquez sur Record card (Enregistrer carte).
   - Une fenêtre contextuelle apparaît : **Select threat level (Sélectionnez le niveau de menace)**.
3. Dans la fenêtre contextuelle, sélectionnez le niveau de menace souhaité, puis cliquez sur **OK**.
   - Une fenêtre contextuelle apparaît : **Recording badge ID (Enregistrement de l'ID du badge)**.

4. Entrez les données de carte correspondant à l'installation de votre site, puis cliquez sur **OK**.
   – La carte d'alerte que vous avez enregistrée apparaît dans la liste, dans l'onglet **Alert card (Carte d'alerte)**.

25.4 Cartes temporaires

Les cartes temporaires sont destinées à remplacer provisoirement les cartes ayant été égarées par des détenteurs de cartes classiques. Il s'agit d'un duplicata qui contient toutes les autorisations et limitations de la carte d'origine, y compris les droits applicables aux portes hors ligne.
Pour éviter les abus, le système peut éventuellement bloquer une ou toutes les autres cartes de la personne pendant une période limitée, ou jusqu'à ce qu'elles soient débloquées manuellement.
Leur utilisation en tant que badge visiteur est donc **inappropriée**.

Conditions préalables
– L'opérateur a accès à un lecteur d'inscription configuré sur son poste de travail.
– Une carte physique appropriée est disponible pour être inscrite dans le système en tant que carte temporaire.

Menu principal > **Personnel data (Données du personnel)** > **Cards (Cartes)**

Procédure : attribution de cartes temporaires
1. Chargez l'enregistrement de personnel requis dans la boîte de dialogue **Cards (Cartes)**.
2. Dans la liste des cartes, sélectionnez la ou les cartes devant être remplacées temporairement.
3. Cliquez sur **Change card (Changer de carte)**.
4. Dans la fenêtre contextuelle **Change card (Changer de carte)**, sélectionnez **Temporary card (Carte temporaire)**.
5. Dans la liste **Period (Période)**, sélectionnez l'une des options suivantes :
   – **Today (Aujourd'hui)**
   – **Today and tomorrow (Aujourd'hui et demain)**
   – **Enter number of days (Entrer le nombre de jours)**
6. Dans le cas de la dernière option, entrez un entier correspondant au nombre de jours souhaité dans la zone.
   Notez que dans les trois cas, la **période** expire toujours à minuit le jour concerné.
7. Si nécessaire, cochez la case **Deactivate all cards now (Désactiver toutes les cartes maintenant)**.
   – Si cette option est sélectionnée, toutes les cartes appartenant à cette personne seront bloquées.
   – Dans le cas contraire, seule la carte sélectionnée ci-dessus sera bloquée.
8. Si nécessaire, cochez la case **Activate card(s) automatically after period (Activer automatiquement la ou les cartes à l'issue de la période)**.
   – Les cartes bloquées seront débloquées automatiquement lorsque la **période** définie ci-dessus arrivera à expiration.
9. Placez la carte temporaire sur le lecteur d'inscription.
10. Cliquez sur **OK**
    .L'ID du badge est enregistré par le lecteur d'inscription.
    – La carte temporaire apparaît comme active ✓ dans la liste des cartes. Sa période de validité et les données de code y figurent également.

- L'autre ou les autres cartes apparaissent comme bloquées ×, en fonction du paramétrage choisi pour la case **Deactivate all cards now (Désactiver toutes les cartes maintenant)**.

11. (Facultatif) Dans la liste des cartes, cliquez sur la colonne **Collecting date (Date de collecte)** de la carte temporaire et définissez une date pour la récupérer auprès de son détenteur.
    La valeur par défaut est **Never (Jamais)**.

Procédure : supprimer des cartes temporaires
Lorsque la carte d'origine égarée est retrouvée, supprimez la carte temporaire en procédant comme suit :

1. Chargez l'enregistrement de personnel requis dans la boîte de dialogue **Cards (Cartes)**.
2. Dans la liste des cartes, sélectionnez la carte temporaire.
3. Cliquez sur **Delete card (Supprimer la carte)**
   .La carte temporaire est supprimée de la liste et la ou les cartes qu'elle remplaçait sont immédiatement débloquées.

Procédure : supprimer des blocages temporaires sur les cartes
Si le blocage de la carte d'origine n'est plus nécessaire, supprimez-le en procédant comme suit :

1. Accédez à la boîte de dialogue de **blocage** : **Personnel data (Données du personnel)** > **Blocking (Blocage)**.
2. Dans la liste des cartes, sélectionnez la carte personnelle marquée comme bloquée dans la colonne **Lock(s) (Verrouillage)**.
3. Cliquez sur **Release temporary lock (Débloquer le verrouillage temporaire)**
   . Notez que la suppression du **blocage** ne supprime pas les cartes temporaires. Les cartes temporaires expirent naturellement à l'issue de leur période de validité. Si nécessaire, supprimez-les manuellement.

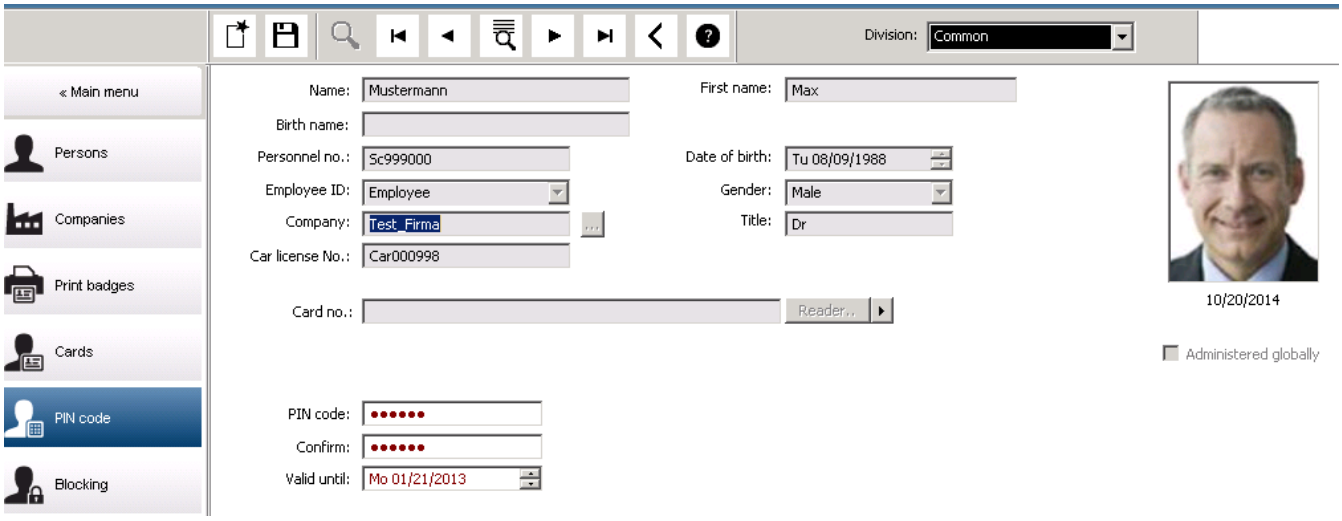
Remarques concernant les cartes temporaires

- Le système ne permet pas le remplacement des cartes temporaires par d'autres cartes temporaires.
- De même, une carte personnelle ne donne droit qu'à une seule carte temporaire.
- Pour avoir un aperçu rapide de toutes les cartes détenues par une personne, passez la souris sur le petit volet le plus à gauche, celui intitulé **Registered (Inscrit)**, dans la barre d'état de la boîte de dialogue principale.

25.5 Codes PIN pour le personnel

Boîte de dialogue : PIN-Code (code PIN)
Pour accéder aux zones répondant à des exigences de sécurité plus élevées, l'autorisation d'accès peut être insuffisante. Dans ce cas, la saisie d'un code PIN peut également être requise. Chaque personne ou chaque badge peut disposer d'un code PIN, valide dans toutes les zones. Le système empêche l'utilisation de codes très simples (par ex. 123456), ou de palindromes (par ex. 127721). La validité peut être restreinte et spécifiée pour chaque personne dans la boîte de dialogue.
Si un code PIN est bloqué ou a expiré, l'accès à la zone requérant le code est refusé, même si le badge est toujours valide pour toutes les autres zones.

Si un code incorrect est entré trois fois de suite (il s'agit du réglage par défaut ; possibilité de choisir une valeur entre 1 et 99), la carte est bloquée et l'accès à toutes les zones est refusé. Une carte bloquée en raison d'un code erroné ne peut être débloquée que via la boîte de dialogue Blocking (Blocage).



Entrez un nouveau code PIN dans le champ de saisie **PIN-Code (Code PIN)**, puis confirmez-le en le tapant une seconde fois. La longueur du code PIN (entre 4 et 9 chiffres, valeur par défaut 6) est configurée par l'administrateur système.

Remarque!
La manière dont les détenteurs de carte entrent les codes PIN d'identification sur les lecteurs de carte dépend du type de lecteur configuré dans votre système. Par exemple :
Sur les lecteurs de cartes RS485, le détenteur de la carte entre **4 #** `<the PIN>`
Sur les lecteurs Wiegand et d'autres lecteurs de carte, le titulaire de la carte doit entrer `<the PIN>` **#**
Assurez-vous d'informer les détenteurs de carte sur la manière dont ils doivent saisir leur code PIN. En cas de doute, consultez votre administrateur système.

Code PIN pour l'armement des systèmes de détection d'intrusion (IDS)
Saisie d'un code PIN de 4 à 8 chiffres (par défaut = 6 - la même longueur que le code PIN de vérification). Ce code PIN est utilisé pour armer un IDS.
L'affichage de ce champ peut être paramétré. Ce contrôle n'est disponible qu'a condition qu'un **code PIN IDS distinct** soit activé.
– Menu principal > **Configuration** > **Options** > **PIN codes (Codes PIN)**
Sélectionnez une date d'expiration si nécessaire.
Si les champs de saisie des codes PIN IDS ne sont pas disponibles, le code PIN de vérification peut également être utilisé pour armer et désarmer l'IDS. En revanche, si les champs de saisie sont affichés dans cette boîte de dialogue, le code PIN d'armement peut uniquement être utilisé pour l'IDS.
Par défaut, les champs de saisie pour l'armement via code PIN sont invisibles.

Codes PIN d'alarme (contrainte)

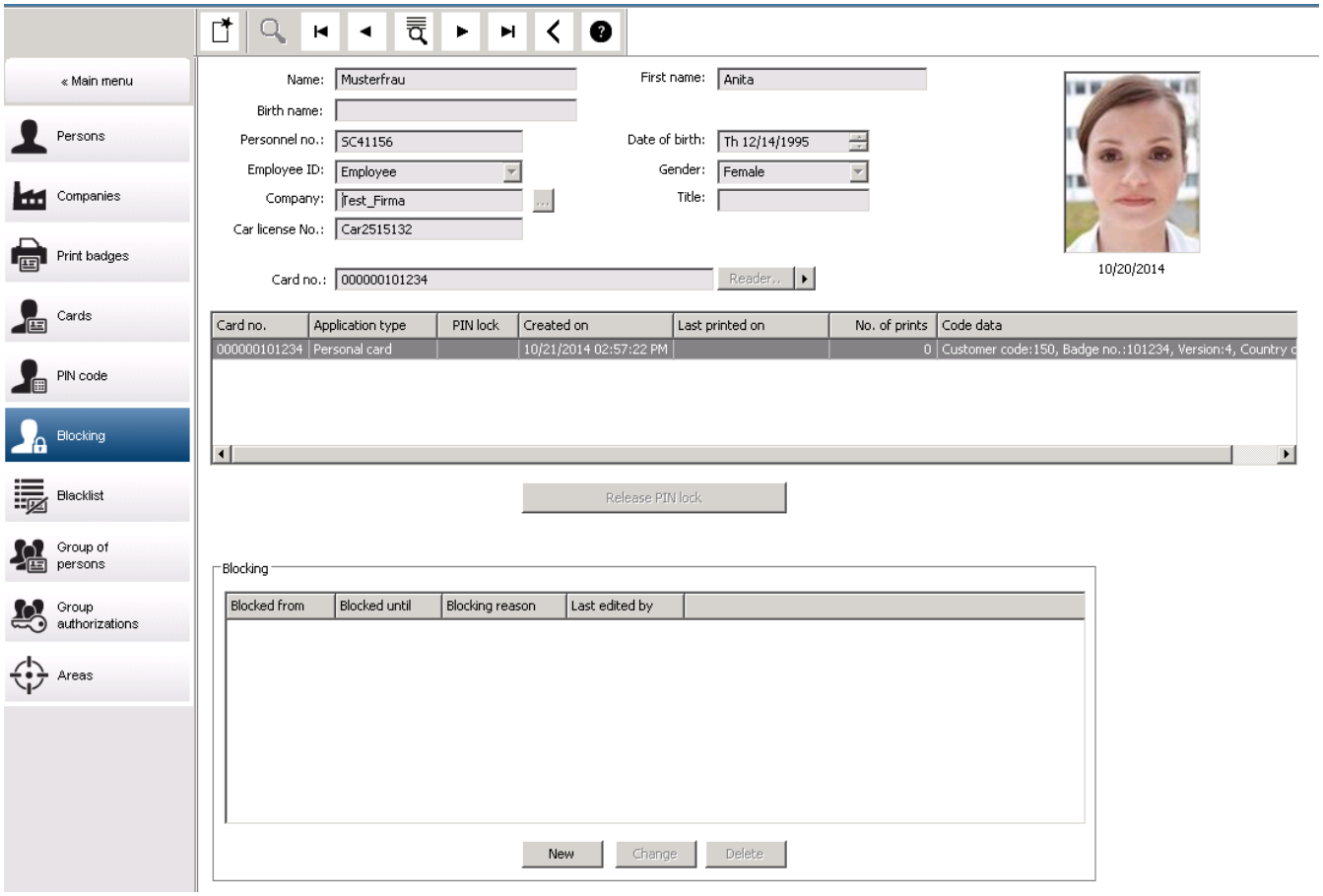
Les personnes sous contrainte peuvent déclencher une alarme silencieuse via un code PIN spécial. Étant donné que l'alarme silencieuse ne doit pas être remarquée par l'agresseur, l'accès est autorisé, mais les opérateurs du système sont alertés de l'accès sous contrainte. Il existe deux variantes. Celles-ci sont activées simultanément et la personne menacée peut choisir l'une ou l'autre :

– Entrer le code PIN dans l'ordre inverse (par ex. 321321 au lieu de 123123), ou
– Incrémenter le code PIN de 1 (par ex. 123124 au lieu de 123123). Notez que si le dernier chiffre est 9, le code PIN est tout de même incrémenté ; ainsi le code PIN 123129 aura pour code PIN de contrainte 123130.

25.6 Blocage des accès pour le personnel

Boîte de dialogue : Blocking (Blocage)

Dans certaines situations, il est nécessaire de refuser temporairement l'accès à une personne ou de supprimer un blocage imposé par le MAC, par exemple en raison de la saisie d'un code PIN erroné trois fois de suite ou d'une surveillance aléatoire.
Le blocage signifie que tous les accès sont refusés à cette personne, indépendamment des informations d'identification utilisées.



1. Sélectionnez la personne de la manière habituelle.

2. Dans le volet de blocage, cliquez sur **New (Nouveau)** afin de créer un blocage pour la personne actuellement sélectionnée.
3. Dans la boîte de dialogue contextuelle, entrez les informations supplémentaires suivantes :
   - **Blocked from / until (Blocage du / au)** : si aucune période de fin n'est spécifiée, la personne est bloquée jusqu'à ce que le blocage soit désactivé manuellement.
   - **Block type (Type de blocage) :**
   - **Blocking reason (Motif du blocage) :** pour le dossier de la personne, s'il s'agit d'un type de blocage `Manual`.
4. Cliquez sur **Save (Enregistrer)** dans la fenêtre contextuelle pour enregistrer le blocage.

– Si nécessaire, sélectionnez un blocage dans la liste puis cliquez sur **Change (Modifier)** ou sur **Delete (Supprimer)** pour le modifier ou le supprimer.

Si vous choisissez le type de blocage **Manual lock (Verrouillage manuel)**, entrez un **motif de blocage** pour le dossier de la personne.

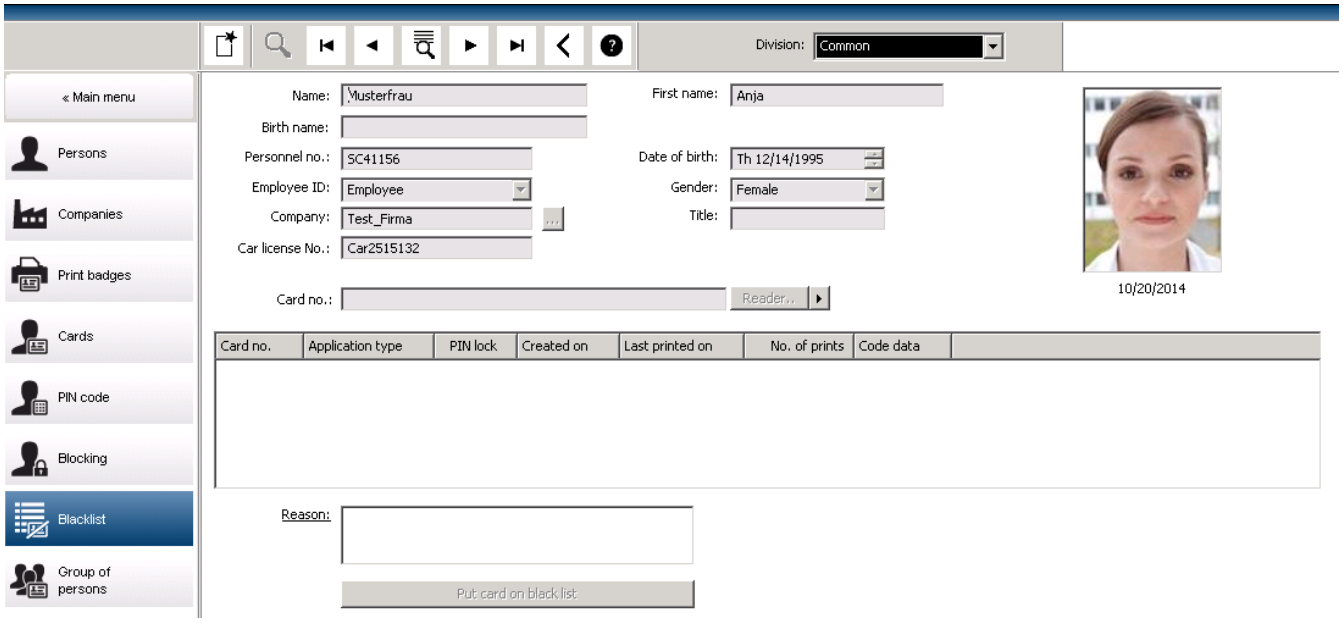
Remarque!
Le blocage s'applique à la personne et non à une information d'identification particulière. Il n'est donc pas possible d'annuler ou d'éviter le blocage en attribuant un nouveau badge.

25.7 Inscription de cartes sur une liste noire

Boîte de dialogue : Blacklist (Liste noire)
Toute carte ne devant plus jamais être utilisée, par exemple une carte volée ou perdue, est consignée dans une liste noire.
Notez que ce sont les informations d'identification qui sont inscrites sur liste noire, pas la personne.

Remarque!
Ce processus est irreversible. Les cartes inscrites sur liste noire ne peuvent jamais être débloquées. Elles doivent être remplacées.

Les cartes inscrites sur liste noire ne permettent pas d'accorder l'accès à une zone. À la place, toute tentative d'utilisation est enregistrée dans le fichier journal et déclenche une alarme.



Menu principal > **Personnel data (Données du personnel)** > **Blacklist (Liste noire)**

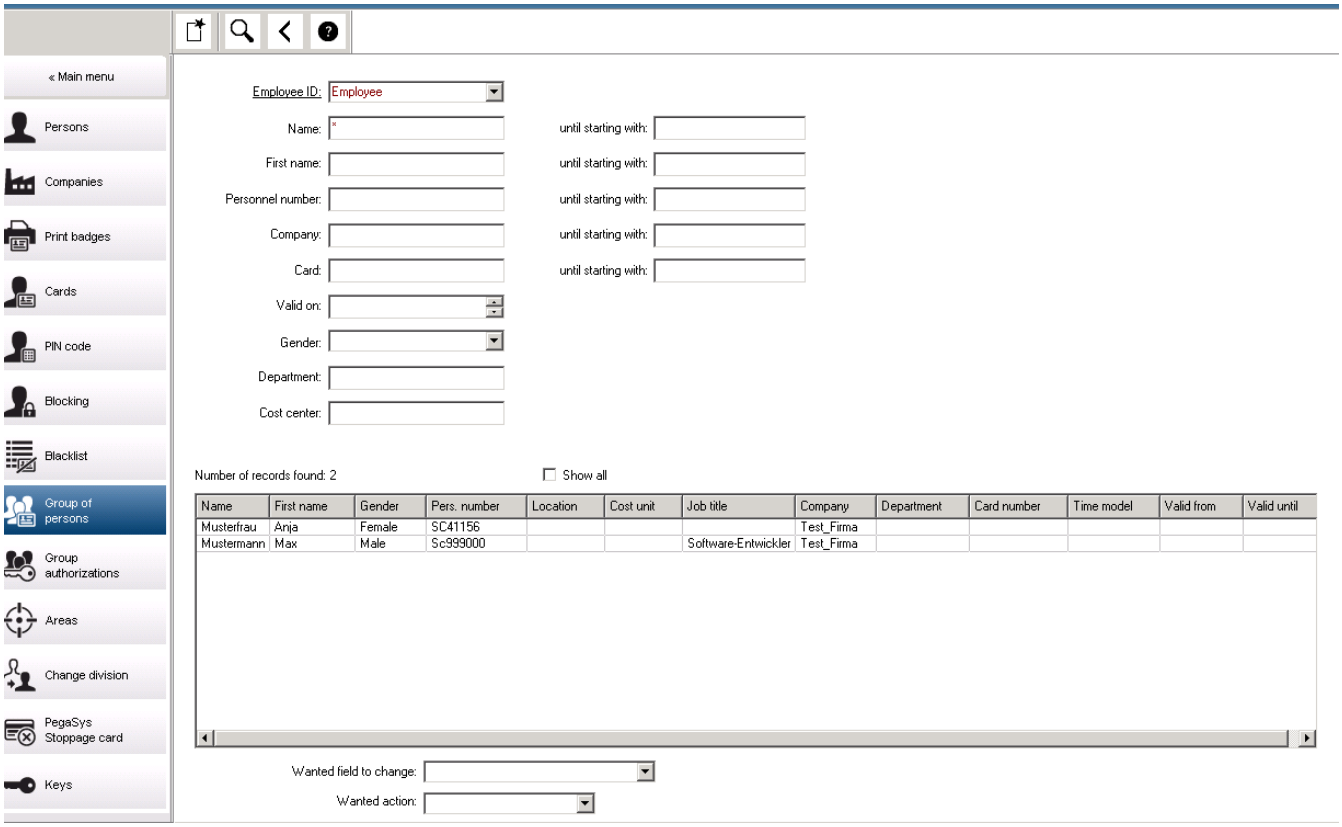
1. Sélectionnez la personne dont le badge doit être mis sur liste noire.
2. Si plusieurs badges sont attribués à cette personne, sélectionnez le badge dans la liste **ID card No (N° badge)**.
3. Dans le champ de saisie **Reason (Motif)**, entrez la raison pour laquelle ce badge doit être inscrit sur liste noire.
4. Cliquez sur le bouton **Blacklist this card (Inscrire sur liste noire)**.
5. Confirmez l'inscription dans la fenêtre contextuelle.

Le badge est alors inscrit sur liste noire avec effet immédiat.

Remarque!
L'inscription sur liste noire affecte les badges, **pas** leur détenteur.
Les autres badges de la personne, si ceux-ci ne figurent pas sur liste noire, ne sont pas bloqués.

25.8 Apporter des modification à plusieurs personnes simultanément

Groupe de personnes



Une autre boîte de dialogue permet de sélectionner un groupe de personnes pour lequel des modifications de groupe peuvent être définies. Afin de pouvoir garder le contrôle sur le groupe de personnes sélectionnées, les dix premières personnes sont répertoriées avec les noms et les données réelles de la base de données (données réelles : si le département « ST-AC » est sélectionné, « ST-ACS » et « ST- ACX », par exemple, s'afficheront). Le nombre de personnes composant le groupe sélectionné est également affiché.
Une fois le groupe de personnes sélectionné, les entrées suivantes peuvent également l'être :

- Employee ID (Identifiant de l'employé)
- Nom
- Prénom
- Personnel number (Matricule)
- Société
- Carte
- Valide on (Valide le)
- Sexe
- Département
- Poste de coût
- Champs réservés si définis

L'option de modification peut ensuite être sélectionnée :

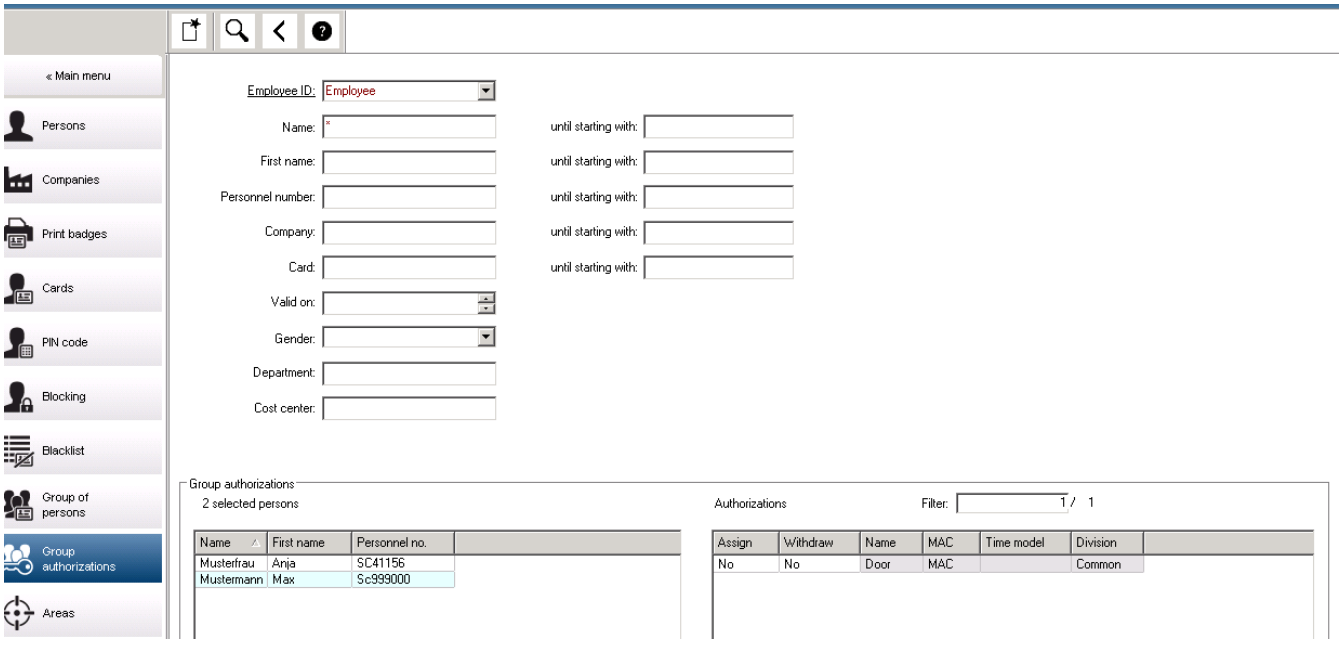
- Field to be changed (Champ à modifier)

- Desired action (Action souhaitée)
- Old value (Ancienne valeur)
- New value (Nouvelle valeur)

Les valeurs indiquées sont donc entrées dans le champ **Old value (Ancienne valeur)** ou **New value (Nouvelle valeur)**, respectivement. La sélection du bouton **Apply changes (Appliquer les modifications)** et la réponse affirmative à la question de sécurité **apply changes for all selected persons? (appliquer les modifications pour toutes les personnes sélectionnées ?)** entraîne la réalisation de l'action et la boîte de dialogue ne peut pas être utilisée tant que l'action est en cours. Les actions déclenchées par les champs *1 à *4 prendront probablement plus de temps que celles déclenchées par les autres champs (sans étoile). De plus, toutes les modifications ne sont pas autorisées. Ainsi, par exemple, **Action souhaitée** ne peut être comparée à **Nouvelle valeur**, car ces entrées ne sont pas couvertes par le produit standard. Les champs **Old value (Ancienne valeur)** et **New value (Nouvelle valeur)** peuvent également varier.

25.8.1 Autorisations de groupe

Autorisation de groupe



Dans l'élément de menu **[Group Authorization]**, les critères de recherche pris en charge sont les suivants :

- Employee ID (Identifiant de l'employé)
- Nom
- Prénom
- Personnel number (Matricule)
- Société
- Carte
- Valide on (Valide le)
- Sexe
- Département
- Poste de coût

– Champs réservés si définis

Une liste comportant toutes les personnes sélectionnées (avec nom, prénom et matricule) apparaît ensuite dans la partie inférieure de la boîte de dialogue. Toutes les autorisations ainsi que leur description, le modèle horaire et les colonnes **Assign (Attribuer)** et **Withdraw (Retirer)** figurent en bas à droite. Lorsque la liste des autorisations s'ouvre, les autorisations actuellement utilisées sont masquées et les colonnes **Assign (Attribuer)** et **Withdraw (Retirer)** ont pour valeur No (Non). Les autorisations individuelles peuvent alors être attribuées en double-cliquant sur le champ de l'une ou l'autre des colonnes, ce qui a pour effet de transformer l'entrée « Non » en « Oui » ou inversement. La sélection du bouton Apply changes (Appliquer les modifications) a pour effet d'attribuer toutes les autorisations ayant pour valeur Yes (Oui) à toutes les personnes sélectionnées, ou de leur retirer ces autorisations, respectivement. Toutes les autres autorisations personnelles restent inchangées, car les autorisations des personnes sélectionnées ne sont généralement pas entièrement identiques.

25.9 Changer la division de personnes

Introduction

Change division (Changer de division) est une boîte de dialogue puissante permettant de changer la division d'un ensemble d'enregistrements de personnel dans le système.

Remarque!
Utilisez cette fonctionnalité avec prudence !
Un changement de division a des conséquences importantes sur les enregistrements de personnel que vous modifiez.

Conditions préalables

L'opérateur qui change la division des enregistrements de personnel doit disposer des autorisations lui permettant d'apporter des modifications à ces personnes, ainsi qu'aux deux divisions concernées.

Chemin d'accès à la boîte de dialogue

Menu principal > **Personnel data (Données du personnel)** > **Change division (Changer de division)**

Procédure

1. Dans le volet **Filter persons (Filtrer les personnes)**, entrez des critères de filtrage dans un ou plusieurs des champs suivants :

Filtre	Remarks/Description (Remarques/Description)
Nom de famille	Utilisez un seul astérisque pour établir une correspondance avec toutes les personnes, ou des lettres **sans** astérisques.
Personnel no. from/ to (Matricule de)	Utilisez les deux champs pour définir une plage de valeurs.
Employee ID (ID d'employé)	Sélectionnez une valeur dans la liste.
Division	Le bouton Apply filter (Appliquer le filtre) n'affiche que les personnes de cette division.

Société	Sélectionnez un nom parmi les entreprises disponibles.
Département	
Card no. (from/to) (N° badge [de/à])	Utilisez les deux champs pour définir une plage de valeurs.

2. Cliquez sur **Apply filter (Appliquer le filtre)**
   . Toutes les personnes correspondant aux critères de filtrage s'affichent dans la liste **Selected persons (Personnes sélectionnées).**
3. Pour affiner davantage l'ensemble des personnes sélectionnées, cliquez sur une ou plusieurs lignes dans la liste **Selected persons (Personnes sélectionnées)**, puis cliquez sur le bouton **Remove (Supprimer)**. Utilisez les touches Ctrl et Maj pour sélectionner plusieurs enregistrements à la fois.
   - **IMPORTANT :** avant de continuer, assurez-vous que la liste des **personnes sélectionnées** ne contient que les personnes auxquelles vous souhaitez attribuer une division différente.
4. Dans la liste **New division (Nouvelle division)**, sélectionnez la division de destination pour les personnes sélectionnées.
5. Cliquez sur **Change division of persons (Changer la division des personnes)**. TOUTES les personnes figurant dans la liste **Selected persons (Personnes sélectionnées)** sont déplacées vers **New division (Nouvelle division)**.

Effets du passage d'une division à une autre

Personnes

- Autorisations d'accès et contrôle de chemin
- Les liens vers la division précédente sont supprimés.
- Les liens vers les données de la catégorie Common (Commun) sont conservés.

Sociétés

- Les liens vers les sociétés de la division précédente sont supprimés.

Effets du passage de la division commune à une autre division

- Autorisations d'accès et contrôle de chemin
- Les liens vers la division commune et la nouvelle division sont conservés.
- Les liens vers d'autres divisions sont supprimés.

Effets du passage d'une division vers la division commune

Tous les liens sont conservés.

25.10 Définition de la zone pour les personnes ou les véhicules

Introduction

Cette section explique comment modifier la zone enregistrée pour un détenteur de carte ou pour son véhicule en le faisant passer d'une zone définie à une autre. Cette opération peut s'avérer nécessaire si le détenteur de carte est passé d'une zone à une autre sans scanner sa carte. Dans un tel cas, les systèmes anti-retour stricts refuseront tout accès à cette personne tant que la zone où elle se trouve réellement et la zone enregistrée ne correspondent pas.

Conditions préalables

- Les zones d'accès ont été définies dans votre système et elles sont utilisées. Pour la documentation, voir le lien ci-dessous.
- En tant qu'opérateur, vous êtes autorisé à modifier les données du détenteur de la carte.

Procédure de réinitialisation de la zone de détenteurs de carte individuels et de véhicules
Chemin d'accès à la boîte de dialogue
Menu principal > **Personnel data (Données du personnel)** > **Areas (Zones)**

1. Sélectionnez le détenteur de la carte dans la base de données.
2. Dans la liste **Location (Zone)**, sélectionnez une nouvelle zone
   ou
3. Dans la liste **Location of the vehicle (Zone du véhicule)**, sélectionnez une nouvelle zone pour le véhicule du titulaire de la carte.
4. Cliquez sur  pour enregistrer

Se reporter à
– *Configurer des zones de contrôle d'accès, page 27*

25.10.1 Procédure de réinitialisation des zones de tous les détenteurs de carte et de tous les véhicules

Cette procédure peut devenir nécessaire, par exemple, après un exercice d'évacuation. Toutes les zones sont définies sur **UNKNOWN (INCONNU)** afin que la surveillance de séquence d'accès et la fonctionnalité anti-retour puissent reprendre.

Procédure
Chemin d'accès à la boîte de dialogue
Menu principal>**System data (Données système)** > **Reset areas unknown (Réinitialiser les zones sur inconnu)**

– Cliquez sur **Set the areas of all persons present to UNKNOWN (Définir les zones de toutes les personnes présentes sur INCONNU)**.

ou

– Cliquez sur **Set the areas of all parking vehicles to UNKNOWN (Définir les zones de tous les véhicules sur INCONNU)**.

25.11 Personnalisation et impression de formulaires pour les données personnelles

Présentation
Utilisez la fonctionnalité **Forms** pour personnaliser les formulaires d'impression des données de détenteurs de carte à partir de la base de données. Cette fonctionnalité peut être requise par les lois régissant la confidentialité des données en vigueur dans votre région.
Des modèles de formulaires sont fournis. Ces modèles peuvent être exportés sous forme de fichiers HTML, personnalisés selon vos besoins et réimportés pour être utilisés dans le gestionnaire de dialogue.
Instanciez et imprimez les formulaires à partir de la boîte de dialogue **Personnel data (Données du personnel)** > **Print badges (Imprimer badges)**.

Chemin d'accès à la boîte de dialogue
– Menu principal AMS > **Configuration** > **Options** >**Form (Formulaires)**

Personnaliser un formulaire

1. Dans la liste **Available forms (Formulaires disponibles)** de la boîte de dialogue **Forms (Formulaires)**, sélectionnez le modèle que vous souhaitez personnaliser, généralement `AllPersonalData_EN`, qui contient tous les champs de données personnelles de la base de données.
2. Cliquez sur **Export (Exporter)** pour enregistrer le formulaire dans un nouveau fichier HTML sur votre système.
3. Utilisez un éditeur HTML pour personnaliser le fichier HTML selon vos besoins.
4. Dans la boîte de dialogue **Forms (Formulaires)**, cliquez sur **Insert (Insérer)** pour importer le fichier HTML personnalisé dans le gestionnaire de dialogue.
   - (Facultatif) Si le formulaire n'est valide que pour une division donnée, sélectionnez une division dans la colonne **Division**.
   - (Facultatif) Cliquez sur **Preview (Aperçu)** pour afficher le formulaire non instancié dans une visionneuse HTML.
   - (Facultatif) Cliquez sur **Delete (Supprimer)** pour supprimer un formulaire de la liste.

Instancier et imprimer un formulaire

1. Dans le gestionnaire de dialogue, accédez à :

– Menu principal AMS > **Personnel data (Données du personnel)** > **Print badges (Imprimer badges)**

2. Chargez l'enregistrement de personnel souhaité dans le formulaire.
3. Sélectionnez un formulaire dans la liste **Form (Formulaire)**.
4. Cliquez sur **Print form (Imprimer le formulaire)**.
   - Le formulaire est instancié avec les données de l'enregistrement de personnel sélectionné, puis transmis à l'imprimante de votre choix.

26 Gestion des visiteurs

Les visiteurs ont un statut spécial dans le contrôle d'accès et leurs données demeurent distinctes des autres données du personnel. Pour cette raison, les données des visiteurs sont créées et gérées dans des boîtes de dialogue distinctes.

26.1 Données visiteurs

Introduction

Le système prend en charge l'administration rapide et facile des données des visiteurs. Les données des visiteurs déjà connus peuvent donc être saisies et les autorisations d'accès définies avant leur arrivée. Lorsque le visiteur arrive, il ne reste que le badge à attribuer. À la fin de la visite, lorsque le badge est restitué, le lien reliant ce badge et la personne est à nouveau supprimé et les autorisations sont automatiquement retirées.

Si les données du visiteur ne sont pas supprimées par l'utilisateur, cette opération est effectuée par le système à la fin du laps de temps configuré (valeur par défaut : 6 mois), après que le badge a été restitué pour la dernière fois.

Deux boîtes de dialogue sont dédiées à l'administration des visiteurs externes.

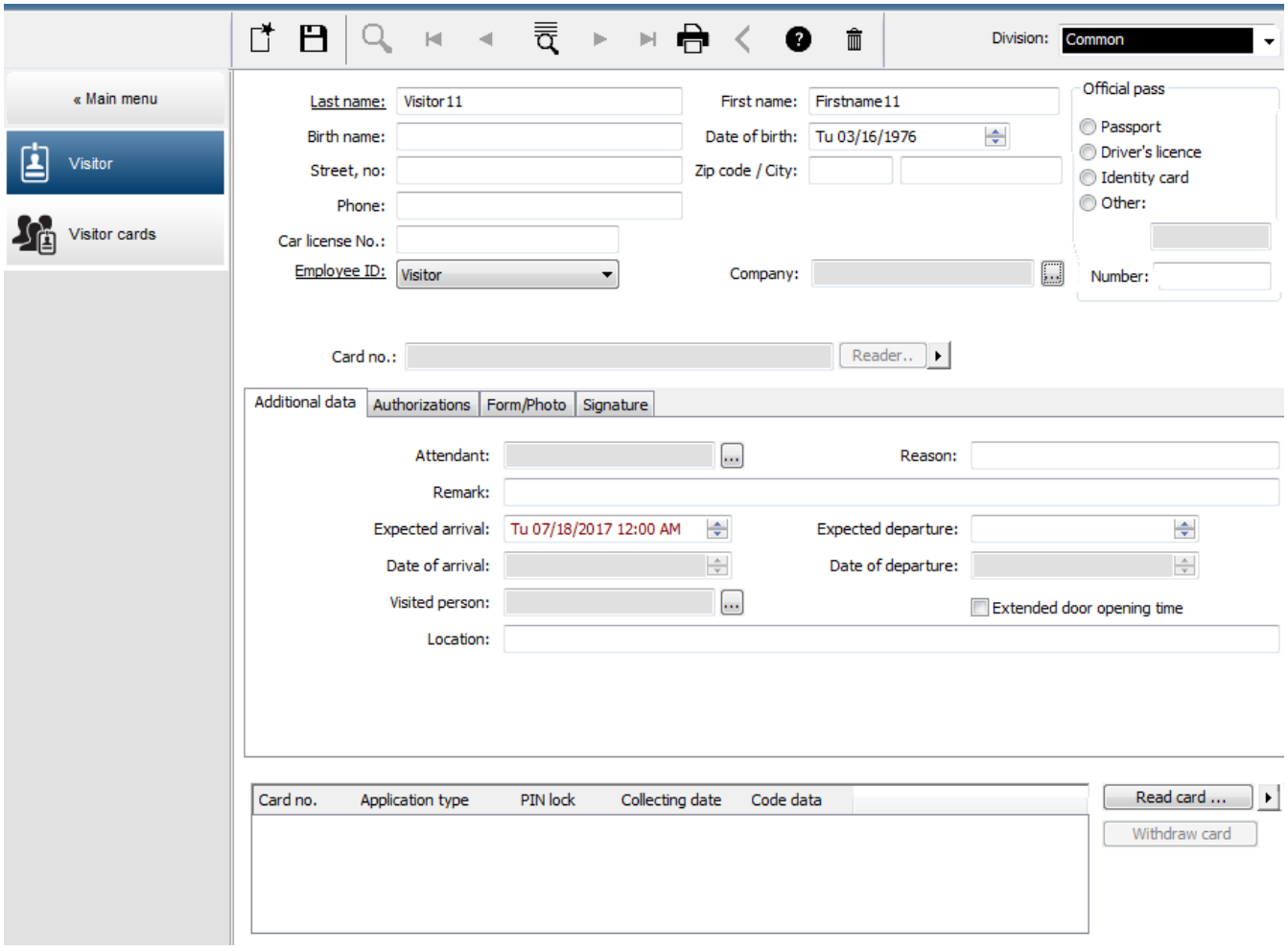
- La boîte de dialogue **Visitors (Visiteurs)** est utilisée pour la saisie des données et des autorisations d'accès des visiteurs.
- La boîte de dialogue **Visitor cards (Badges visiteur)** régule l'enregistrement et la suppression des badges visiteur.

Boîte de dialogue : Visitors (Visiteurs)

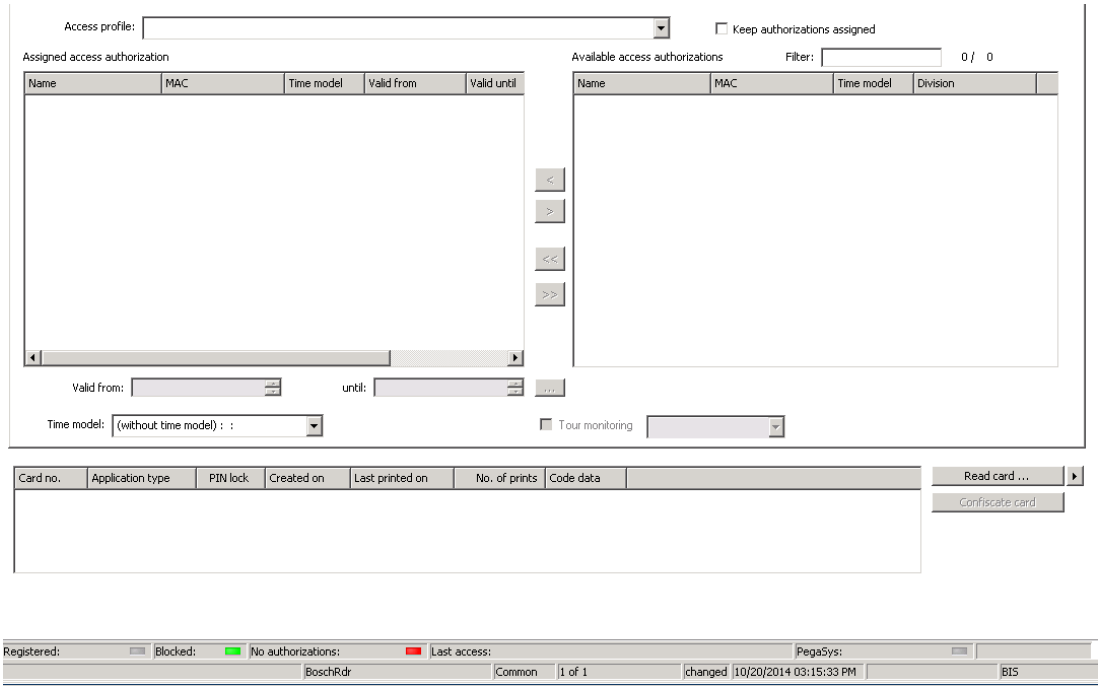
Les visiteurs ont un statut entièrement distinct de celui des autres personnes. Ils sont donc gérés dans une boîte de dialogue dédiée. Les personnes identifiées en tant que **visiteurs** ne peuvent pas être créées dans la boîte de dialogue **Persons (Personnes)** et leurs badges ne peuvent pas non plus y être enregistrés.

La boîte de dialogue **Visitors (Visiteurs)** ne comporte notamment pas de champ de saisie **Employee ID (ID employé)**. Dans la mesure où il existe une table de base de données distincte pour les visiteurs, les personnes créées dans la boîte de dialogue décrite ici sont automatiquement identifiées en tant que visiteurs. Cela signifie donc qu'aucune personne autre que des visiteurs ne peut être créée ici. Les sélections se font donc uniquement dans cette boîte de dialogue, dans la table de base de données appropriée. En revanche, toutes les personnes enregistrées sur le système peuvent être sélectionnées dans les autres boîtes de dialogue de données personnelles, mais elles ne peuvent pas toujours être utilisées pour les visiteurs (boîte de dialogue **Cards (Cartes)**).

Lorsqu'elles sont connues, les données des visiteurs peuvent être intégralement ou partiellement saisies dans le système avant l'arrivée du visiteur. Le temps d'attente des visiteurs dont les données ont déjà été enregistrées est donc minimal.



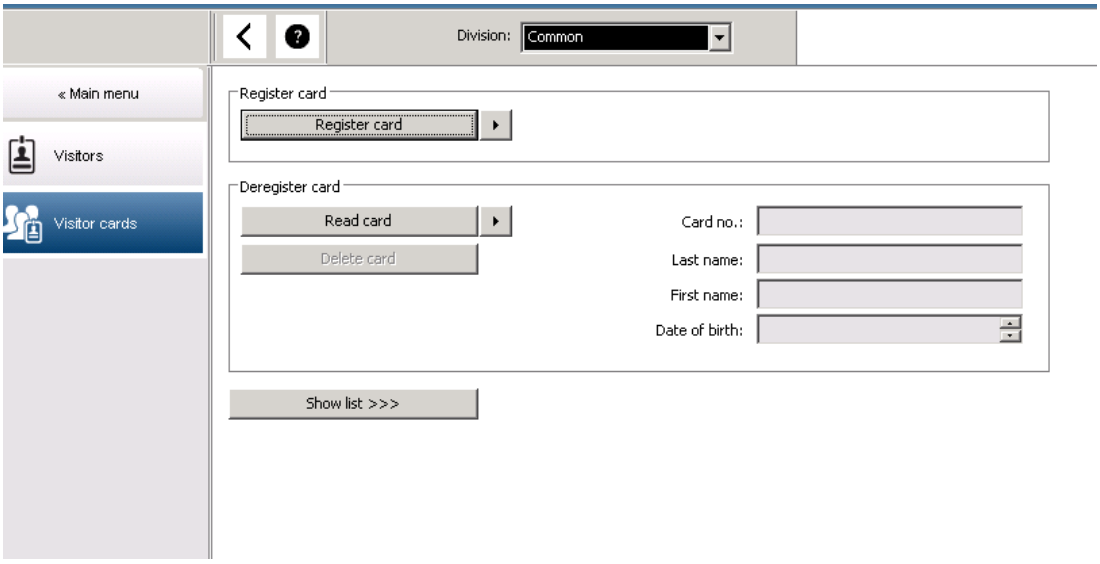
Il est possible de saisir le **motif** de la visite, le **lieu** visité et une **remarque** dans les champs de saisie ci-dessous.
Si vous choisissez d'entrer des données dans les champs **expected arrival (arrivée prévue)** et **expected departure (départ prévu)**, ces dates apparaîtront également dans les champs **valid from (valide de)** et **until (à)**.
Les dates pertinentes sont renseignées dans les champs **Date of arrival (Date d'arrivée)** et **Date of departure (Date de départ)** par le système lorsque, respectivement, les données des visiteurs sont attribuées à un badge visiteur puis lorsque cette attribution et annulée.
Comme avec la boîte de dialogue **Cards (Cartes)**, il est également possible d'attribuer aux visiteurs des durées d'ouverture de porte prolongées de manière à leur assurer un accès plus facile, par exemple pour les personnes handicapées.



Dans le champ de boîte de dialogue **Assign authorization (Attribuer une autorisation)** un profil de visiteur existant peut être sélectionné dans la liste sélective homonyme. Il est également possible de sélectionner des autorisations d'accès uniques dans la liste **Available access authorization (Autorisation d'accès disponible)** et de les transférer dans la liste **Assigned access authorization (Autorisation d'accès attribuée)**.
Seuls les profils d'accès marqués en tant profils de visiteur peuvent être sélectionnés dans cette boîte de dialogue. L'attribution d'autorisations générales permettant aux visiteurs d'accéder à des zone spéciales doit donc être évitée.
La validation des autorisations d'accès peut également être définie pour chaque autorisation.
Si la lecture de la carte présente une erreur, le numéro du badge peut également être donné manuellement. La date actuelle est enregistrée simultanément comme date d'arrivée.
À l'issue de la visite, le visiteur rend son badge. Lorsque le badge est lu par un lecteur de carte ou que le numéro du badge est saisi manuellement, la personne associée au badge est sélectionnée et ses données s'affichent à l'écran.
L'opérateur confirme la remise du badge. Le bouton **Confiscate card (Confisquer carte)** permet de supprimer le lien entre le badge et le visiteur. La date et l'heure de cette action sont enregistrées comme date de départ.

Boîte de dialogue : Visitor Cards (Badges visiteur)
Certaines cartes du système sont destinées à être utilisées en tant que badges visiteur. Ces badges sont généralement attribués aux visiteurs à leur arrivée et ces derniers les restituent lors de leur départ. Les badges peut ainsi être réutilisés. Avant de pouvoir les attribuer aux visiteurs, ceux-ci doivent être enregistrés en tant que badges visiteur dans cette boîte de dialogue.

Remarque!
Les badges des visiteurs sont généralement créés sans nom ni photo afin qu'ils soient réutilisables.



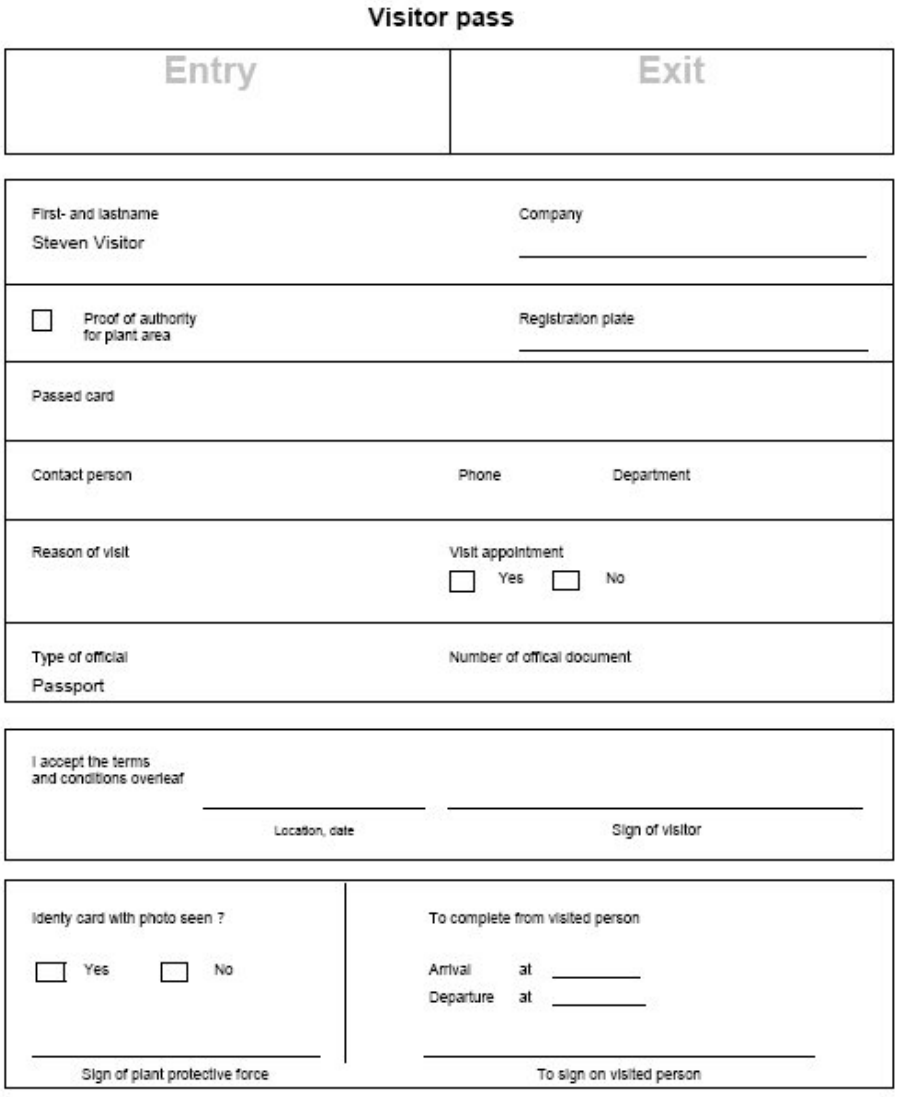
Cliquez sur le bouton **Register ID card (Enregistrer le badge)** pour procéder à l'enregistrement.
Effectuez ensuite la procédure de saisie décrite précédemment (sections **Personnes** et **Badges** du chapitre **Données du personnel**) en utilisant le numéro du badge. Cela permet au système de reconnaître le badge en tant que badge visiteur et de pouvoir lui appliquer les paramètres des boîtes de dialogue suivantes.

Afin d'accélérer la procédure d'attribution, il est conseillé de scanner tous les badges existants de manière à ce qu'ils puissent être attribués aux visiteurs respectifs dans la boîte de dialogue suivante.
À la fin de sa visite, le visiteur restitue le badge. Lorsqu'un lecteur scanne le badge ou que le numéro de celui-ci est saisi manuellement, la personne à laquelle la carte est destinée est sélectionnée et les données de cette personne s'affichent à l'écran. [Pour saisir manuellement le numéro du badge et passer à l'utilisation des lecteurs, consultez les descriptions des boîtes de dialogue **Cards (Cartes)** et **Visitors (Visiteurs)**. L'utilisateur

confirme la restitution du badge. Un bouton permet de supprimer le lien entre le badge et les données personnelles du visiteur. La date en cours est enregistrée comme date de départ.

Impression d'un formulaire visiteur

La barre d'outils de la boîte de dialogue **Visitors (Visiteurs)** comporte un bouton supplémentaire  permettant d'imprimer un certificat visiteur. Entre autres choses, la personne qui reçoit le visiteur peut utiliser ce certificat pour prouver la venue du visiteur ainsi que l'heure de son arrivée et de son départ.



Visitor pass

Entry | Exit

First- and lastname
Steven Visitor

Company

☐ Proof of authority for plant area

Registration plate

Passed card

Contact person | Phone | Department

Reason of visit

Visit appointment
☐ Yes ☐ No

Type of official
Passport

Number of offical document

I accept the terms and conditions overleaf

Location, date

Sign of visitor

Identy card with photo seen ?
☐ Yes ☐ No

Sign of plant protective force

To complete from visited person

Arrival at
Departure at

To sign on visited person

27 Gestion des parkings

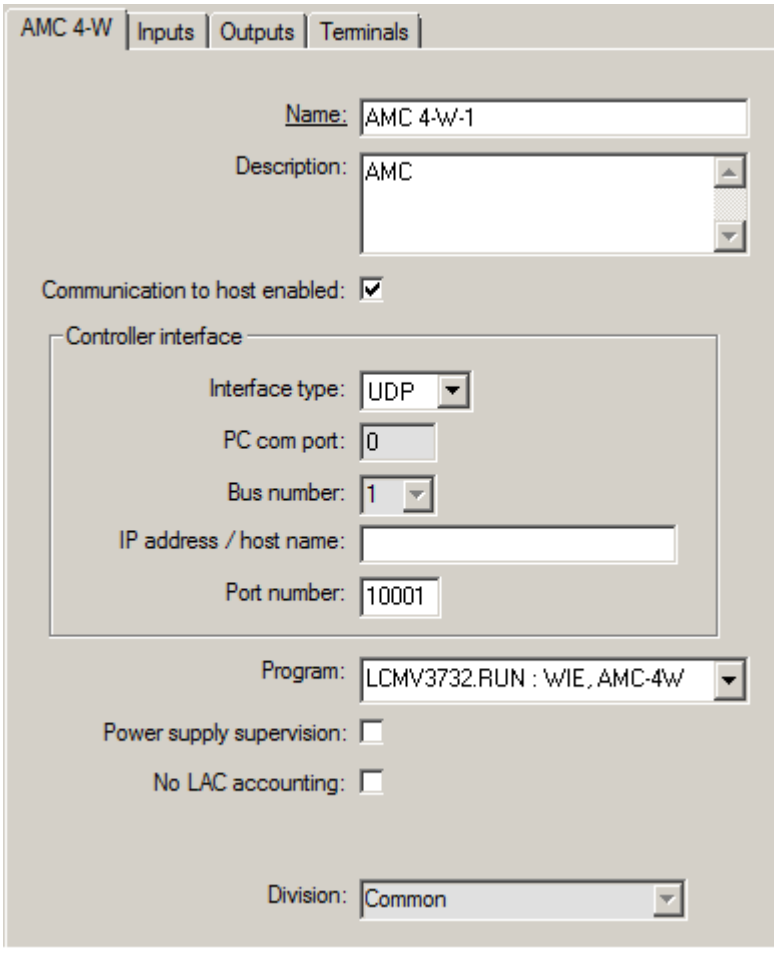
27.1 Autorisations pour plusieurs zones de stationnement

Certains parkings disposent de zones pour les conducteurs handicapés et non handicapés. Dans ce cas, les règles suivantes s'appliquent :

- Les détenteurs d'abonnements ne sont autorisés à accéder au parking qu'à condition qu'il reste des places de stationnement pour personnes non handicapées.
- Les personnes handicapées sont autorisées à accéder au parking tant qu'il reste des places de stationnement pour personnes handicapées ou non handicapées.

Remarque!
Cela suppose que les détenteurs de tickets respectent les règles. Cela signifie notamment que :
Les personnes non handicapées ne se garent pas sur une place de stationnement pour personnes handicapées.
Les personnes handicapées utilisent les places de stationnement qui leur sont réservées tant qu'elles sont disponibles.

Une personne disposant de plusieurs autorisations peut accéder aux deux types d'emplacements, qu'elle soit handicapée ou non. L'AMC essaie d'enregistrer la personne en fonction de l'ordre séquentiel configuré pour les zones de stationnement. Lorsqu'une zone est pleine, la recherche de la zone autorisée et libre suivante se poursuit.
Calculs effectués aux niveaux MAC et AMC :
1) Un AMC contrôle toutes les entrées et sorties d'un parking :
=> l'AMC effectue les calculs lui-même et peut être corrigé par le MAC lors de la mise en ligne.
2) Les entrées et sorties d'un parking sont réparties sur différents AMC :
=> le MAC effectue les calculs pour l'AMC en cas de fonctionnement en ligne. Lorsqu'ils fonctionnent hors ligne, les AMC autorisent l'accès (s'ils sont configurés en conséquence) mais ils n'effectuent pas de décomptes.
Si plusieurs AMC contrôlent un parking, cochez la case **No LAC accounting (Aucun compte LAC)** dans la configuration AMC.



27.2 Rapport sur les parkings

Parking lot list Date 08.11.2013 , 14:51:23 Page 1

Parking area	Zone	Vehicle count	State
Main Park		51	
	Zone A	30	full
	Zone B	9	--
	Zone C	12	--
Building A		39	
	Zone A	30	full
	Zone B	9	--
Building B		39	
	Zone A	30	full
	Zone B	9	--

27.3 Gestion de parking étendue

Introduction

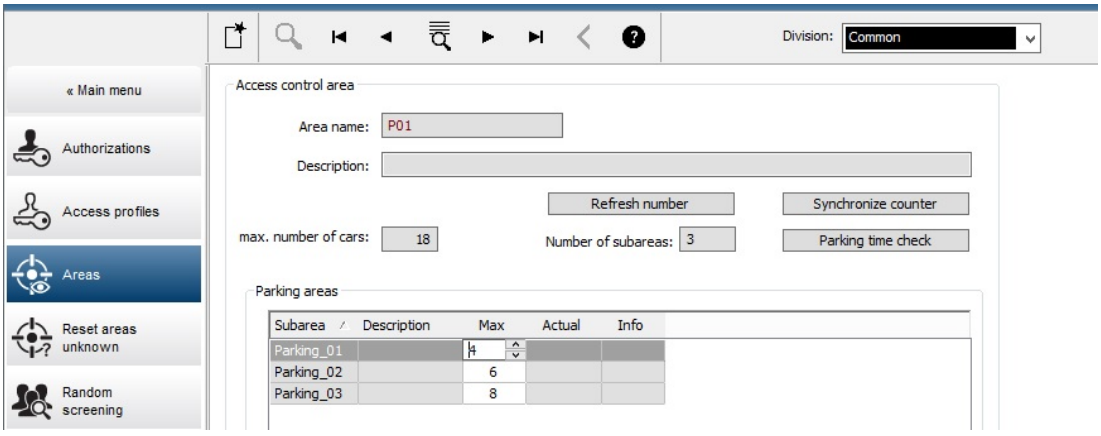
L'opérateur peut définir le nombre de places de stationnement d'un parking en prenant compte des véhicules de dimensions non standard, par exemple :

– Camions

- Accès handicapés
- Motos

Chemin d'accès à la boîte de dialogue
Main menu (Menu principal) > **System data (Données système)** > **Areas (Zones)**

Procédure
1. Sélectionnez une zone de stationnement.
2. Dans le volet **Parking areas (Zones de stationnement)**, définissez la valeur dans la colonne **Max** sur le nouveau nombre de places de stationnement pour cette zone.



Remarques :
- Les paramètres définis dans la colonne **Max** remplacent les paramètres définis dans la configuration **Areas (Zones)**. Voir **Configuration de zones pour les véhicules** (lien ci-dessous).
- Un zéro `0` dans la colonne **Max** signifie Illimité ; le comptage des véhicules est désactivé.

Se reporter à
- *Configurer des zones pour les véhicules, page 28*

28 Gestion des tours de garde et patrouilles

Présentation des tours de garde

Un **tour de garde** est un parcours dans les locaux, ponctué de lecteurs de carte, où les employés de type **Gardien** doivent présenter une carte de garde spéciale pour prouver qu'elles ont physiquement été vérifier le lecteur.

Les cartes de garde ne permettent pas d'ouvrir les entrées et sont utilisées uniquement pour le suivi. Pour ouvrir les entrées, le gardien doit avoir une carte d'accès en plus.

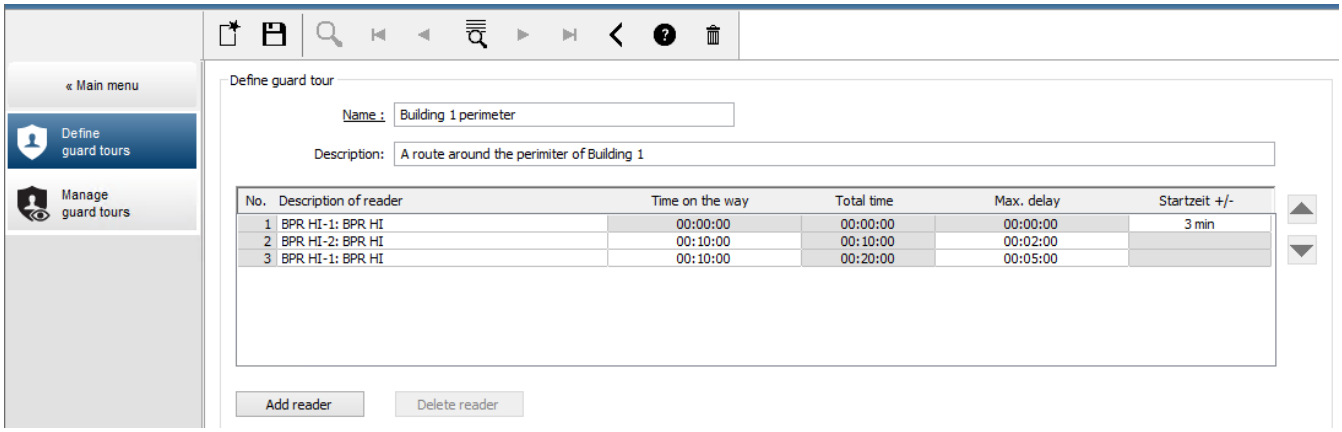
Le tour de garde consiste en une série de lecteurs avec les temps de marche approximatifs entre chacun de ces lecteurs. Le délai maximum acceptable entre les lecteurs et l'écart acceptable (+/-) par rapport à l'heure de début sont également des attributs du Tour de garde. Les écarts en dehors de ces tolérances définies peuvent potentiellement déclencher des alarmes et sont enregistrés dans les **Patrouilles**.

Présentation des patrouilles

Une **patrouille** désigne le parcours d'un tour de garde à une date et une heure particulières. Chaque patrouille est créée et enregistrée comme une entité unique dans le système, en vue d'investigations détaillées.

28.1 Définition des tours de garde

Sélectionnez **Guard tours (Tours de garde)** > **Define guard tours (Définir les tours de garde)**.



- Dans le champ de texte **Name (Nom)**, entrez un nom pour le tour de garde.
- Dans le champ de texte **Description**, entrez une description plus détaillée du parcours (facultatif).

Ajout de lecteurs au tour de garde :

1. Cliquez sur le bouton **Add reader (Ajouter un lecteur)**.
   Une ligne est créée dans le tableau.
2. Dans la colonne **Description of reader (Description du lecteur)**, sélectionnez un lecteur dans la liste déroulante.
3. Entrez des valeurs d'écarts acceptables :
   - S'il s'agit du premier lecteur de la séquence, sous **Start time +/- (Heure de début +/-)**, entrez un nombre de minutes plus tôt ou plus tard qui serait acceptable comme heure de début d'une patrouille sur ce tour de garde.

- S'il **ne s'agit pas** du premier lecteur de la séquence, sous **Time on the way (Heure en cours)**, entrez l'heure (hh:mm:ss) nécessaire au gardien pour se déplacer entre le lecteur précédent et celui-ci.
  La durée totale du tour, hors retards, est cumulée dans la colonne **Total time (Durée totale)**.

4. Sous **Max. delay (Retard max.)**, entrez le montant maximal de l'ajout à **Time on the way (Heure encours)** qui reste acceptable sans provoquer le retard d'une patrouille (**Delayed (Retardée)**).
5. Ajoutez autant de lecteurs que nécessaire. Notez que le même lecteur peut apparaître plusieurs fois si le tour de garde y passe plusieurs fois ou y revient.

- Pour supprimer un lecteur de la séquence, sélectionnez la ligne et cliquez sur le bouton **Delete reader (Supprimer le lecteur)**.
- Pour changer la position d'un lecteur dans la séquence, sélectionnez la ligne et cliquez sur les boutons haut/bas :

 .

28.2 Gestion des patrouilles

Sélectionnez **Guard tours (Tours de garde)** > **Manage guard tours (Gérer les tours de garde)**.

Planification d'une nouvelle patrouille

Pour planifier une patrouille sur un tour de garde particulier, procédez comme suit :

1. Assurez-vous que vous disposez de la carte de garde souhaitée pour la patrouille et que vous avez accès à un lecteur de carte d'accès configuré ou à un lecteur d'inscription directement connecté.
2. Dans la colonne **Guard tours (Tours de garde)**, sélectionnez l'un des tours de garde définis.
3. Cliquez sur le bouton **New patrol... (Nouvelle patrouille...)**.
   Une fenêtre contextuelle s'affiche.
4. Dans la fenêtre contextuelle, si vous le souhaitez, modifiez le tour de garde dans la liste déroulante.
5. Si la patrouille doit disposer d'une heure de début prédéfinie, cochez la case **Set start time: (Définir l'heure de début:)**.
   - Entrez la date et l'heure de début.
   - Si vous le souhaitez, cliquez sur la zone de sélection numérique **Start time +/- (Heure de début +/-)** pour régler la tolérance appliquée aux départs tardifs ou précoces.
6. Cliquez sur la flèche vers la droite et sélectionnez le lecteur que vous souhaitez utiliser pour enregistrer la carte de garde. Notez que le lecteur doit déjà être configuré dans le système pour qu'il apparaisse ici et être sélectionné.
7. Cliquez sur le bouton plus vert pour commencer à lire la carte de garde, présentez la carte au lecteur et suivez les instructions contextuelles.
   La carte de garde est enregistrée pour être utilisée par la patrouille.
8. Répétez l'étape précédente pour enregistrer d'autres cartes de garde pour cette patrouille. Notez cependant que la première carte à présenter lors de la patrouille doit être utilisée sur tous les lecteurs lors de cette patrouille.

9. Cliquez sur **OK**. Le tour de garde sélectionné sera marqué comme **planned (planifié)** dans la liste.

Suivi d'une patrouille

Toutes les patrouilles planifiées et actives sont placées en haut de la liste. Si plusieurs patrouilles sont planifiées ou actives, la patrouille sélectionnée est encadrée en rouge. Cliquez sur le cadre pour obtenir plus d'informations.

Une patrouille commence lorsque le gardien présente sa carte de garde au premier lecteur du tour garde. Cette carte doit être utilisée pour le reste de la patrouille, même si d'autres cartes ont été définies pour la patrouille.

L'état **State** de la patrouille devient **Active (Actif)**.

Chaque lecteur atteint dans les délais reçoit une coche verte : ✔. Les temps planifiés et réels entre les lecteurs de la patrouille actuellement sélectionnée sont affichés dans la moitié inférieure de la boîte de dialogue.

Chaque lecteur atteint après l'heure planifiée plus **Max. delay (Retard max.)** reçoit une marque rouge ⊘. La patrouille est marquée comme **Delayed (Retardée)**.

Dans ce cas, le gardien appelle l'opérateur pour confirmer qu'il n'y a pas de problème. L'opérateur clique ensuite sur le bouton **Resume patrol (Reprendre la patrouille)**. Le lecteur reçoit une coche verte avec un « c » supplémentaire : ✔c. Le gardien peut maintenant continuer la patrouille au lecteur suivant.

En cas de retard imprévu mais inoffensif dans une patrouille active, le gardien peut appeler l'opérateur pour ajuster l'horaire. Entrez les minutes de retard dans la zone de sélection numérique **Delay (min) (Retard (min))** et cliquez sur le bouton **Apply (Appliquer)**.

Si une patrouille ne peut pas être terminée comme prévu, l'opérateur peut l'abandonner en cliquant sur le bouton **Interrupt (Interrompre)**. L'état **State** de la patrouille devient **Aborted (Abandonné)**, et il est placé sous les tours de garde planifiés et actifs dans la liste.

28.3 Surveillance de tour (anciennement contrôle de chemin)

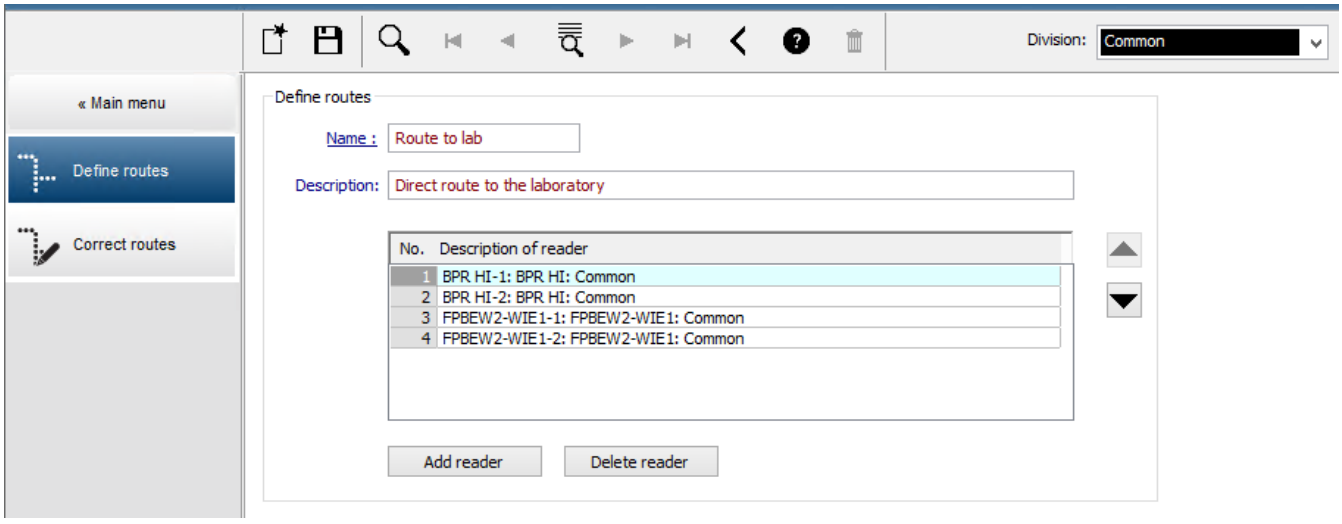
Introduction

Un itinéraire (ou tour) est une séquence prédéfinie de lecteurs qui peut être imposée aux personnes définies dans le système de contrôle d'accès, pour diriger leurs déplacements sur les lieux, quelles que soient les autorisations de la personne.

Les tours sont généralement utilisés pour appliquer des séquences d'accès précises dans des environnements industriels propres, des zones à haute sécurité ou des zones soumises à des règles d'hygiène strictes.

Définition des itinéraires

1. Dans le menu principal, sélectionnez **Tour monitoring (Surveillance de tour)** > **Define routes (Définir des itinéraires)**.
2. Entrez un nom pour l'itinéraire (jusqu'à 16 caractères).
3. Entrez une description plus détaillée (facultatif).
4. Comme pour les tours de garde, cliquez sur le bouton **Add reader (Ajouter un lecteur)** pour créer une séquence de lecteurs. Utilisez les boutons fléchés pour modifier la position d'un lecteur dans la séquence et le bouton **Delete reader (Supprimer le lecteur)** bouton pour supprimer le lecteur.



Attribution d'un itinéraire à une personne

Pour attribuer un itinéraire à une personne, procédez comme suit :

1. Dans le menu principal, sélectionnez **Personnel data (Données personnelles)** > **Cards (Cartes)**.
2. Chargez le dossier personnel du destinataire de l'itinéraire.
3. Sous l'onglet **Other data (Autres informations)**, cochez la case **Tour monitoring (Surveillance de tour)**.
4. Dans la liste déroulante située à côté, sélectionnez un itinéraire défini (pour définir un itinéraire, voir la section précédente).
5. Sauvegardez le dossier personnel.

L'itinéraire est activé lorsque le destinataire présente sa carte au premier lecteur de l'itinéraire. Les autres lecteurs de l'itinéraire doivent maintenant être utilisés selon la séquence, c'est-à-dire que seul le lecteur suivant dans la séquence accordera l'accès. Une fois l'itinéraire complètement parcouru, la personne peut se présenter à n'importe quel autre lecteur dans les limites de ses autorisations.

Correction et surveillance des itinéraires

1. Dans le menu principal, sélectionnez **Tour monitoring (Surveillance de tour)** > **Correct routes (Corriger les itinéraires)**.
2. Chargez le dossier personnel du destinataire de l'itinéraire.
3. Pour localiser cette personne sur l'itinéraire, cliquez sur le bouton **Determine location (Déterminer l'emplacement)**.
4. Les lecteurs déjà passés avec succès reçoivent une coche verte ✔ dans la liste.
5. Pour réinitialiser ou corriger l'emplacement d'une personne sur l'itinéraire, cliquez sur le bouton **Set location (Définir l'emplacement)**.

29 Surveillance aléatoire du personnel

Processus de surveillance aléatoire

1. Un titulaire de carte présente sa carte à un lecteur configuré pour une surveillance aléatoire.

   Remarque

   Seules les personnes autorisées à franchir l'entrée dans la direction définie peuvent être sélectionnées aléatoirement. Comme les autorisations sont vérifiées avant la surveillance aléatoire, toute personne non autorisée sera immédiatement exclue et ne sera pas incluse dans le processus de sélection.
2. Si cette personne est sélectionnée pour la surveillance aléatoire, sa carte sera bloquée dans tout le système.
   - L'événement est enregistré dans le journal des événements du système.
   - La boîte de dialogue **Blocking (Blocage)** reçoit une entrée d'une durée illimitée marquée **Random screening (Surveillance aléatoire)**. [Figure ci-dessous - numéro 1]
   - La barre d'état des boîtes de dialogue des données personnelles affiche les LED bloquées en rouge et la surveillance aléatoire clignotant en violet.

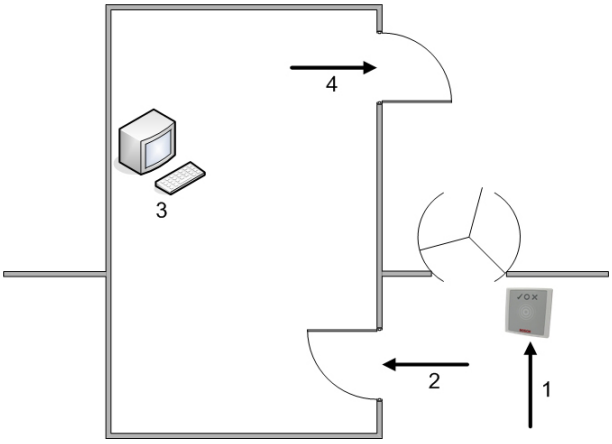
Remarque!

Les personnes pour qui le paramètre **Excluded from random screening (Exclu de la surveillance aléatoire** a été défini (boîte de dialogue **Cards (Cartes)**, onglet **Other data (Autres informations)**) ne sont pas incluses dans le processus de surveillance.

3. La personne choisie au hasard est invitée à effectuer des vérifications supplémentaires dans une cabine de sécurité distincte.
4. Au terme de ces vérifications, l'agent de sécurité réinitialise le blocage dans la boîte de dialogue **Blocking (Blocage)** comme suit :
   - Sélectionnez le blocage approprié dans la liste **Blocking (Blocage)**.
   - Cliquez sur le bouton **Delete (Supprimer)**.
   - Confirmez la suppression en cliquant sur **Yes (Oui)**.

La personne surveillée aléatoirement peut désormais à nouveau utiliser sa carte dans tous les lecteurs auxquelles elle a accès.

Exemple de disposition de la salle pour une surveillance aléatoire



1 = Carte présente - surveillance - blocage à l'échelle du système

2 = Le titulaire de la carte entre dans la cabine de sécurité

3 = Le titulaire de la carte est fouillé et le blocage est ensuite supprimé de sa carte via la boîte de dialogue.
4 = Le titulaire de la carte quitte la cabine de sécurité, sans présenter à nouveau la carte au lecteur.

Remarque!
Le pourcentage de surveillance est cumulé au fil du temps. Par exemple, après 10 % de surveillance aléatoire, il existe toujours une possibilité (1 sur 100, soit 1/10 x 1/10) que deux personnes consécutives soient sélectionnées.

30 Utilisation du visionneur d'événements

Introduction
Le visionneur d'événements permet aux opérateurs dûment autorisés d'examiner les événements enregistrés par le système et de produire des rapports : à l'écran, imprimés ou sous la forme de fichiers `.CSV`.
Pour récupérer et afficher les enregistrements souhaités de la base de données du journal des événements, définissez les critères de filtre et cliquez sur **Refresh (Actualiser)**  .
Selon le volume des données, cette opération peut durer plusieurs minutes.
Les critères de filtrage peuvent être définis selon différents modes :

Relatif	Sélection des événements par rapport à l'heure actuelle
Intervalle	Sélection des événements dans un intervalle de temps qui peut être défini librement
Total	Sélection des événements indépendamment de leur heure d'occurrence

Conditions préalables
Vous êtes connecté au gestionnaire de dialogue.

Chemin d'accès à la boîte de dialogue
Menu principal du gestionnaire de boîte de dialogue > **Reports (Rapports)** > **Visionneur d'événements**

30.1 Définition des critères de filtre pour un horaire par rapport au présent

1. Sous **Time period (Période horaire)**, activez la case d'option **Relative (Relatif)**.
2. Dans la boîte **Search within the last (Rechercher dans le dernier/la dernière)**, définissez le nombre d'unités horaires à rechercher et choisissez les unités à utiliser, par exemple, semaines, jours, heures, minutes, secondes.
3. Dans le menu **Event types (Types d'événements)**, sélectionnez la catégorie d'événements à rechercher, puis les types d'événements qui vous intéressent.
4. Dans le menu **Maximum number (Nombre maximal)**, limitez le nombre d'événements que le visionneur d'événements tente de recevoir. Pour des raisons de performances, il **n'est pas** recommandé de laisser la valeur **(illimitée)**.
5. Spécifiez les autres critères de filtrage qui vous intéressent :
   - Nom de famille
   - Prénom
   - Matricule
   - Numéro de carte
   - Utilisateur (opérateur système)
   - Nom du périphérique
   - Nom de la zone

- Cliquez sur **Refresh (Actualiser)**  pour commencer à collecter des événements, et sur **Cancel (Annuler)** pour arrêter.
- Cliquez sur  pour enregistrer les résultats, ou sur  pour les imprimer.

– Cliquez sur  pour effacer les résultats d'une autre recherche.

30.2 Définition de critères de filtre pour un intervalle de temps

1. Sous **Time period (Période horaire)**, activez la case d'option **Interval (Intervalle)**.
2. Pour l'intervalle **Time from, Time until (Heure à partir de, Temps jusqu'au)**, définissez le début et la fin de la période de recherche des événements.
3. Dans le menu **Event types (Types d'événements)**, sélectionnez la catégorie d'événements à rechercher, puis les types d'événements qui vous intéressent.
4. Dans le menu **Maximum number (Nombre maximal)**, limitez le nombre d'événements que le visionneur d'événements tente de recevoir. Pour des raisons de performances, il **n'est pas** recommandé de laisser la valeur **(illimitée)**.
5. Spécifiez les autres critères de filtrage qui vous intéressent :
   – Nom de famille
   – Prénom
   – Matricule
   – Numéro de carte
   – Utilisateur (opérateur système)
   – Nom du périphérique
   – Nom de la zone

– Cliquez sur **Refresh (Actualiser)**  pour commencer à collecter des événements, et sur **Cancel (Annuler)** pour arrêter.

– Cliquez sur  pour enregistrer les résultats, ou sur  pour les imprimer.

– Cliquez sur  pour effacer les résultats d'une autre recherche.

30.3 Définition des critères de filtre indépendamment du temps

1. Sous **Time period (Période horaire)**, activez la case d'option **Total**.
2. Dans le menu **Event types (Types d'événements)**, sélectionnez la catégorie d'événements à rechercher, puis les types d'événements qui vous intéressent.
3. Dans le menu **Maximum number (Nombre maximal)**, limitez le nombre d'événements que le visionneur d'événements tente de recevoir. Pour des raisons de performances, il **n'est pas** recommandé de laisser la valeur **(illimitée)**.
4. Spécifiez les autres critères de filtrage qui vous intéressent :
   – Nom de famille
   – Prénom
   – Matricule
   – Numéro de carte
   – Utilisateur (opérateur système)
   – Nom du périphérique
   – Nom de la zone

- Cliquez sur **Refresh (Actualiser)**  pour commencer à collecter des événements, et sur **Cancel (Annuler)** pour arrêter.
- Cliquez sur  pour enregistrer les résultats, ou sur  pour les imprimer.
- Cliquez sur  pour effacer les résultats d'une autre recherche.

31 Utilisation de rapports

Cette section décrit un ensemble de fonctions de rapport qui peuvent être utilisées pour filtrer les données du système et du journal des événements, et pour les présenter dans des formats clairs.

Chemin d'accès à la boîte de dialogue

Menu principal > **Reports (Rapports)**.

Utilisation de la barre d'outils des rapports

Cliquez sur  pour afficher un aperçu avant impression.

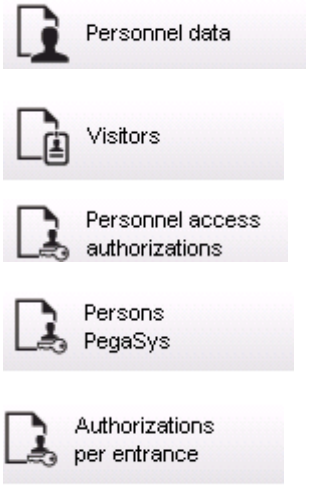
L'aperçu possède sa propre barre d'outils :

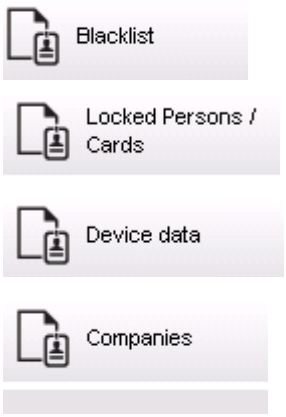
- Cliquez sur ✕ pour quitter l'aperçu sans imprimer.
- Utiliser les flèches |◀ ◀ 2 of 17 ▶ ▶| dans la barre d'outils de l'aperçu pour parcourir l'affichage ou pour sélectionner des pages par leur numéro.
- Cliquez sur  pour imprimer immédiatement, en utilisant votre imprimante par défaut
- Cliquez sur pour imprimer via une boîte de dialogue de configuration de l'impression, qui propose d'autres options d'impression.
- Cliquez sur pour exporter le rapport vers une sélection de formats de fichiers, notamment PDF, RTF et Excel.
- Les nombres situés à droite de la barre d'outils représentent :
  - Le nombre total d'entrées existantes dans la base de données qui correspondent aux critères de filtre.
  - Le pourcentage de ces entrées de base de données affichées dans l'aperçu.

31.1 Rapports : Données permanentes

Présentation des rapports - Données permanentes

Les rapports sur les données permanentes comprennent tous les rapports concernant les personnes, les visiteurs, les cartes et leurs autorisations d'accès. En outre, les données de l'appareil et les données de l'entreprise peuvent être affichées.





Report: Personnel Data (Rapport : Données personnelles)
Deux filtres peuvent être appliqués lors de la création de rapports.
Filtre de personne : ici, l'opérateur filtre en fonction des champs de données habituels du personnel.
Filtre de carte d'accès : ici, l'opérateur peut filtrer en fonction des numéros de carte, des plages de numéros, de l'état et de l'état de blocage.

Report: Visitors (Rapport : Visiteurs)
Comme pour les données personnelles, les rapports de visiteurs peuvent être créés ici. Ainsi, il est toujours possible d'accéder à toutes les données visiteurs créées, c'est-à-dire que même les visiteurs qui ne sont pas encore arrivés mais qui étaient déjà enregistrés peuvent être sélectionnés.

Report: Personnel Access Authorizations (Rapport : Autorisations d'accès du personnel)
Ce rapport donne un aperçu des autorisations d'accès enregistrées sur le système et montre également les personnes auxquelles ces autorisations ont été attribuées.
En termes de filtres, les données personnelles et la sélection de certaines autorisations peuvent être utilisées :
- Données du personnel : nom, prénom, matricule.
- Validation de toutes les autorisations.
- Le nom de l'autorisation d'entrée est incluse.
- Nom du modèle temporel, le cas échéant.
- Direction de l'entrée.
- Validation de l'autorisation spéciale.

Report: Blacklist (Rapport : Liste noire)
Dans cette boîte de dialogue, il est possible d'imprimer une liste contenant toutes les sélections ou une sélection souhaitée de cartes d'identité qui ont été mises sur une liste noire pour diverses raisons.

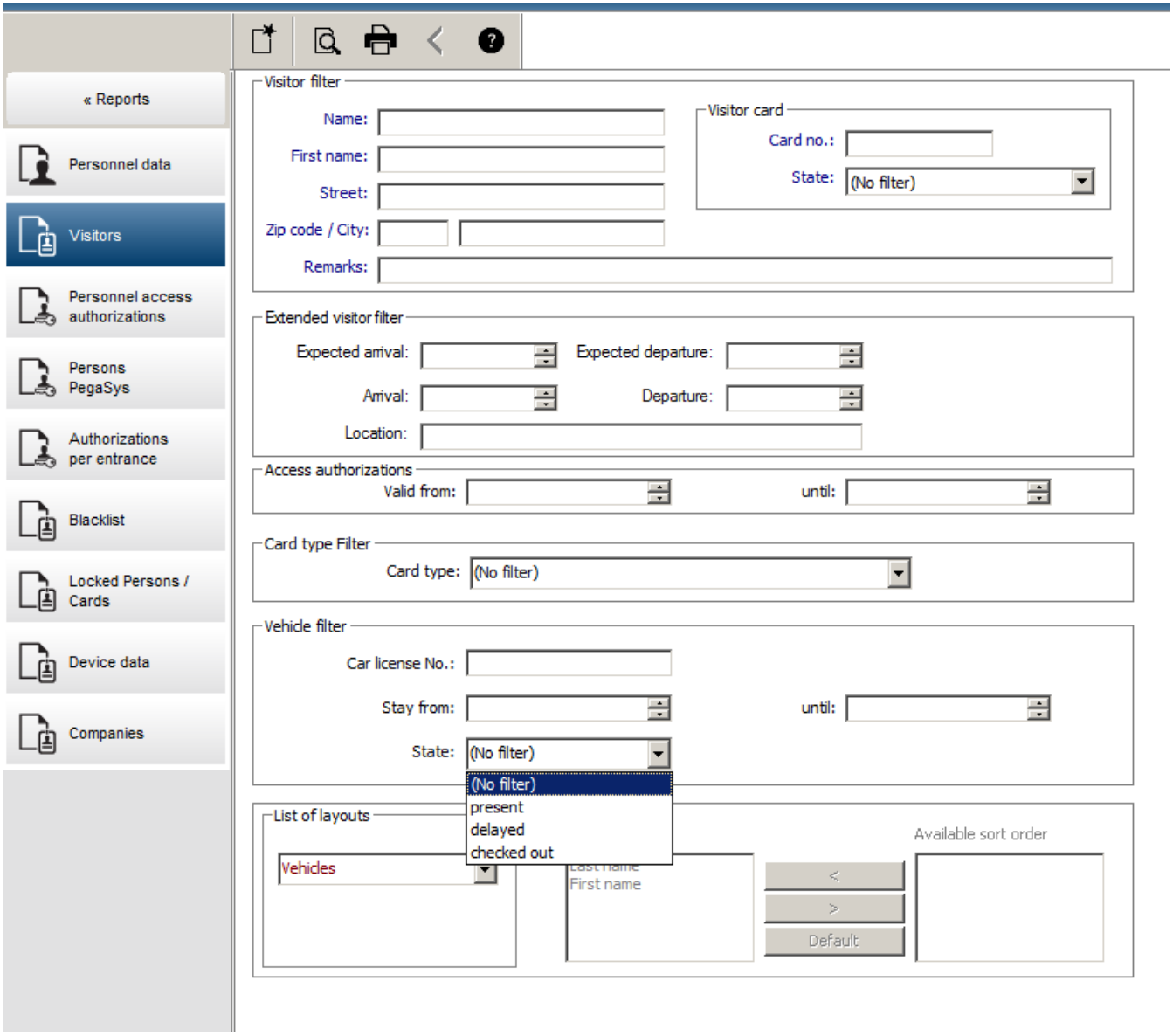
Report: Blocked Persons/Cards (Rapport : Personnes/cartes bloquées)
Cette boîte de dialogue peut être utilisée pour créer des rapports contenant des données sur toutes les personnes bloquées.
Utilisez des dates pour rechercher des blocages dans des périodes spécifiées.

Report: Device Data (Rapport : Données du périphérique)
Cette boîte de dialogue peut être utilisée pour créer des rapports basés sur les données du périphérique, par exemple le nom ou le type du périphérique.

Report: Companies (Rapport : Entreprises)
Cette boîte de dialogue permet de regrouper les données de l'entreprise dans une liste. Utilisez des astérisques, par exemple, pour rechercher les entreprises dont le nom commence par une certaine lettre.

31.1.1 Rapports sur les véhicules

Dans la boîte de dialogue **Reports (Rapports) > Visitors (Visiteurs)**, il est possible de sélectionner **Vehicles (Véhicules)** dans la liste des dispositions. Une fois que **Vehicles (Véhicules)** est sélectionné, la zone de dialogue **Vehicle filter (Filtre de véhicule)** est activée et peut être utilisée par l'opérateur pour filtrer les véhicules et leur statut.
L'état s'affiche comme suit :
- Present (Présent) : visite pas encore terminée et délai pas écoulé.
- Delayed (Retardé) : visite pas encore terminée, mais délai écoulé.
- Checked out (Sorti) : le visiteur a redonné toutes les cartes d'accès.

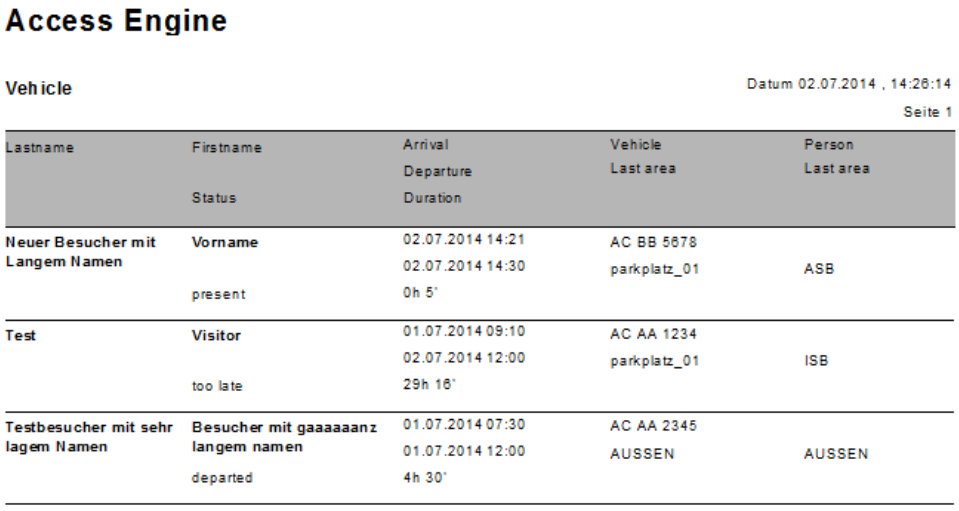


Le **Report for vehicles (Rapport sur les véhicules)** est disponible uniquement pour les visiteurs car la date d'arrivée prévue, la date de départ prévue, la date d'arrivée et la date de départ ne sont disponibles que pour les visiteurs dans le tableau de la base de données **Visitors (Visiteurs)**.

Le rapport ne répertorie que les numéros de véhicules qui sont stockés dans la table de base de données **Persons (Personnes)**. Ainsi, une fois qu'un numéro de véhicule a été modifié, le rapport fournit d'autres résultats.

La durée est calculée comme suit :

- Si le visiteur est déjà sorti, la différence entre l'heure d'arrivée et l'heure de départ s'affiche en minutes.
- Si le visiteur n'est pas encore sorti, la durée entre l'arrivée jusqu'à maintenant s'affiche en minutes.



Access Engine

Vehicle

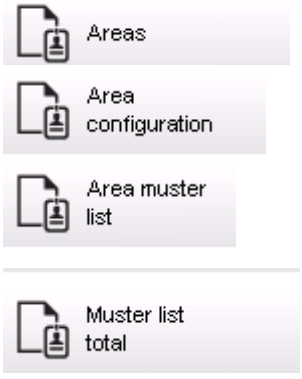
Datum 02.07.2014 , 14:26:14
Seite 1

Lastname	Firstname Status	Arrival Departure Duration	Vehicle Last area	Person Last area
Neuer Besucher mit Langem Namen	**Vorname** present	02.07.2014 14:21 02.07.2014 14:30 0h 5'	AC BB 5678 parkplatz_01	ASB
Test	**Visitor** too late	01.07.2014 09:10 02.07.2014 12:00 29h 16'	AC AA 1234 parkplatz_01	ISB
Testbesucher mit sehr lagem Namen	**Besucher mit gaaaaaanz langem namen** departed	01.07.2014 07:30 01.07.2014 12:00 4h 30'	AC AA 2345 AUSSEN	AUSSEN

31.2 Rapports : Données système

Rapports - Données système

Contrairement aux données permanentes, les données système sont des informations affectées au système, non liées aux personnes, aux cartes d'identité ou à l'entreprise. Ces rapports sont expliqués plus en détail ci-après.



Report: Areas (Rapport : Zones)

Cette boîte de dialogue peut être utilisée pour rassembler les emplacements dans un rapport. Elle contient un seul filtre de zone, avec un choix de bâtiments et de zones à sélectionner.

Sélectionnée la zone concernée par un clic gauche de la souris. L'utilisateur peut visualiser le rapport à l'écran en cliquant sur le bouton **Preview (Aperçu)** avant de lancer l'impression en cliquant sur **Print (Impression)**.

Il existe deux mises en page disponibles.

	Standard	Personnes présentes sur un emplacement - pas de parking
	Occupation du parking	Personnes présentes sur un emplacement - parkings uniquement

Pour vérifier que les données affichées sont à jour, les dernières lectures de cartes des zones sont également répertoriées.

Des informations fiables sur la localisation des personnes sont donc accessibles concernant divers événements.

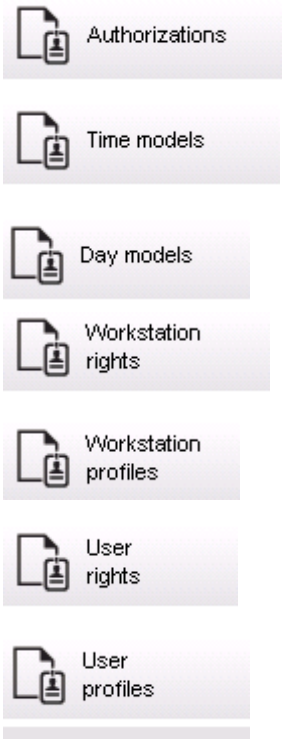
Report: Areas Configuration (Rapport : Configuration des zones)
Zones définies et leurs sous-zones avec des parkings signalés par un drapeau et un nombre maximum de personnes ou de voitures.

Report: Area Muster List (Rapport : Liste de rassemblement)
Les personnes d'une zone peuvent être listées selon des données numériques mais également par nom.
Outre les heures de vérification des zones individuelles, ces rapports contiennent également les heures de chaque personne.

Report: Muster List Total (Rapport : Total du rassemblement)
En principe, les listes de rassemblement correspondent à la boîte de rapport **Areas (Zones)** ; cependant, elles portent sur des zones spécifiques qui fournissent des informations sur le nombre de personnes actuellement dans cette zone en fonction du contrôle d'accès.

31.3 Report: Authorizations (Rapport : Autorisations)

Présentation
Cette option de menu fournit un récapitulatif des différentes autorisations données dans les boîtes de dialogue correspondantes :



Report: Authorizations (Rapport : Autorisations)
Cette boîte de dialogue peut être utilisée pour afficher les autorisations d'accès définies dans le système. Les entrées appartenant aux autorisations d'accès individuelles sont répertoriées. Le nom du modèle horaire sélectionné s'affiche. De plus, ce rapport indique le nombre des personnes auxquelles l'autorisation est attribuée.

Report: Time Models (Rapport : Modèles horaires)
Ce rapport peut être utilisé pour afficher les modèles horaires définis dans le système, tels que sélectionnés. Ce rapport affiche toutes les données associées au modèle ainsi que le nombre de personnes à qui le modèle s'applique.

Report: Day Models (Rapport : Modèle Jour)
Ce rapport affiche tous les modèles Jour définis avec les noms, les descriptions et les intervalles qu'ils contiennent.

Report: Workstation Rights (Rapport : Droits du poste de travail)
Cette boîte de dialogue peut être utilisée pour afficher les droits attribués aux postes de travail définis dans le système.

Report: Workstation Profiles (Rapport : Profils de poste de travail)
Cette boîte de dialogue peut être utilisée pour afficher les profils de poste de travail définis dans le système ; cela permet une présentation claire des opérations système qui peuvent être exécutées sur les postes de travail individuels.

Report: User Rights (Rapport : Droits de l'utilisateur)
Cette boîte de dialogue peut être utilisée pour afficher les profils utilisateur attribués aux utilisateurs définis dans le système.

Report: User Profiles (Rapport : Profils d'utilisateur)
Cette boîte de dialogue peut être utilisée pour afficher les boîtes de dialogue et les droits de boîte de dialogue attribués aux profils utilisateur définis dans le système.

32 Gestion du niveau de menace

Cette section décrit les différentes manières de déclencher un niveau de menace et de l'annuler. Pour des informations générales, voir la section *Configuration de la gestion du niveau de menace, page 140*

Introduction

Un niveau de menace est activé par une alerte de menace. Une alerte de menace peut être déclenchée de l'une des manières suivantes :

- Par une commande dans l'interface utilisateur du logiciel
- Par un signal d'entrée défini sur un contrôleur d'accès local, par exemple un bouton poussoir
- En glissant une carte d'alerte dans un lecteur

Notez que les alertes de menace peuvent être annulées par la commande d'interface utilisateur ou le signal matériel, mais pas par la carte d'alerte.

Se reporter à

- *Configuration de la gestion du niveau de menace, page 140*

32.1 Déclenchement et annulation d'une alerte de menace via la commande de l'interface utilisateur

Cette section explique comment déclencher une alerte de menace dans AMS Map View.

Chemin d'accès à la boîte de dialogue

- AMS Map View >  (Arborescence des périphériques)

Conditions préalables

- Au moins un niveau de menace a été défini.
- Au moins un niveau de menace a été marqué comme Active (Actif) dans l'éditeur de dispositif.
- En tant qu'opérateur AMS Map View, vous disposez des autorisations nécessaires :
  - pour utiliser les niveaux de menace,
  - pour afficher le MAC ou les MAC de la division où l'alerte de menace doit être déclenchée.

Procédure de déclenchement d'une alerte de menace

1. Dans l'arborescence des périphériques AMS Map View, cliquez avec le bouton droit sur le périphérique MAC sur lequel l'alerte de menace doit être déclenchée.
   - Un menu contextuel s'affiche, contenant les commandes que vous êtes autorisé à exécuter sur ce périphérique MAC.
   - Si aucun niveau de menace n'est encore opérationnel, le menu comporte un ou plusieurs éléments portant la mention **Activate Threat level (Activer le niveau de menace)** '`<name>`', avec le nom du niveau de menace défini dans l'éditeur de dispositif.
2. Sélectionnez le niveau de menace que vous souhaitez déclencher.
   - Le niveau de menace entre en action.

Procédure d'annulation d'une alerte de menace

Condition préalable : un niveau de menace doit déjà être opérationnel.

1. Dans l'arborescence des périphériques AMS Map View, cliquez avec le bouton droit sur le périphérique MAC sur lequel l'alerte de menace doit être annulée.
   – Un menu contextuel s'affiche, contenant les commandes que vous êtes autorisé à exécuter sur ce périphérique MAC.
2. Sélectionnez **Deactivate Threat level (Désactiver le niveau de menace)** dans le menu contextuel.
   – Le niveau de menace actuel est désactivé.

32.2 Déclenchement d'une alerte de menace via un signal matériel

Cette section explique comment envoyer un signal d'entrée matériel pour déclencher une alerte de menace.

Conditions préalables

– Au moins un niveau de menace a été défini.
– Au moins une entrée a été configurée dans l'arborescence des périphériques.
– Les signaux matériels ont été définis sur un AMC et un périphérique a été connecté à la borne appropriée de cet AMC, qui lui délivrera un signal. Si nécessaire, cliquez sur le lien fourni à la fin de cette section pour obtenir des instructions sur la configuration du signal d'entrée, ou contactez votre administrateur système.

Procédure

Activez le périphérique, généralement via un bouton-poussoir ou un commutateur matériel, qui est connecté à l'AMC.
Pour annuler l'alerte de menace, activez le périphérique qui envoie le signal d'entrée défini comme **Threat level: Deactivate (Niveau de menace : Désactiver)**.

Se reporter à

– *Attribution d'un niveau de menace à un signal matériel, page 145*

32.3 Déclenchement d'une alerte de menace via une carte d'alerte

Cette section explique comment déclencher une alerte de menace via une carte d'alerte.

Conditions préalables

– Au moins un niveau de menace a été défini.
– Au moins une entrée a été configurée dans l'arborescence des périphériques.
– Une carte d'alerte a été créée pour un titulaire de carte particulier. Si nécessaire, cliquez sur le lien fourni à la fin de cette section pour obtenir des instructions sur la création d'une carte d'alerte, ou contactez votre administrateur système.

Procédure

1. Le titulaire présente sa carte d'alerte spéciale à tout lecteur **hors empreintes digitales** du site.
   – Le niveau de menace défini pour cette carte est activé.
2. Une fois la menace écartée, annulez le niveau de menace via la commande de l'interface utilisateur ou le commutateur matériel. Il n'est pas possible d'annuler un niveau de menace via une carte d'alerte.

Se reporter à

– *Création d'une carte d'alerte, page 212*

33 Utilisation du téléscripteur à balayage

Introduction
Le téléscripteur à balayage est un outil qui aide les opérateurs Map View à surveiller, en temps réel, qui entre ou sort des locaux.

Présentation
Le téléscripteur à balayage est une application dans AMS Map View, qui affiche les événements d'accès des 10 dernières minutes dans une liste déroulante dynamique. Jusqu'à 50 événements d'accès sont affichés et les événements de plus de 10 minutes sont automatiquement supprimés de la liste. L'opérateur peut surveiller tous les lecteurs du système ou en sélectionner quelques-uns.
Chaque enregistrement de la liste contient des détails sur l'événement et les informations d'identification utilisées, par exemple :
- Le nom du titulaire de la carte et sa photo stockée, pour confirmation visuelle de son identité.
- Un horodatage.
- Le nom de l'entreprise et/ou du service, s'il est stocké.
- L'entrée et le lecteur où le justificatif a été utilisé.
- Une catégorie d'événement avec une étiquette de couleur :
  - Verte : accès terminé avec un identifiant valide.
  - Jaune : accès incomplet avec un identifiant valide, par exemple, le titulaire de la carte a réalisé un cycle de verrouillage mais n'a pas ouvert la porte.
  - Rouge : tentative d'accès infructueuse avec un identifiant non valide. Le type d'invalidité est affiché, par exemple, les informations d'identification sont sur liste noire, inconnues ou ont expiré.

Le téléscripteur à balayage ne conserve pas ses propres archives, il extrait les événements d'accès de la base de données système et les affiche. Le défilement dynamique peut être mis en pause pour une recherche ou ouvert dans une fenêtre séparée pour une utilisation parallèlement à d'autres applications Map View.

Remarque!
Latence après modifications
Les modifications apportées aux photos d'identité et autres données d'un détenteur de carte dans AMS nécessitent généralement quelques minutes pour être propagées au téléscripteur à balayage. Jusqu'à ce que la synchronisation ait lieu, le téléscripteur à balayage continue de réagir en temps réel avec les anciennes données.

Conditions préalables
Le profil utilisateur de l'opérateur nécessite une autorisation spéciale pour exécuter le téléscripteur à balayage.
1. Dans l'application AMS principale, accédez au menu : **Configuration** > **User profiles (Profils d'utilisateur)**.
2. Chargez le nom du profil de l'opérateur souhaité.
3. Dans le tableau, sélectionnez **Access Manager Maps (Plans du gestionnaire d'accès)** > **Special functions (Fonctions spéciales)** > Swipe ticker (Téléscripteur à balayage).

Lancement du téléscripteur à balayage

- Dans Map View, cliquez sur pour démarrer l'outil.

Sélection des lecteurs à surveiller

Si les lecteurs n'ont pas encore été sélectionnés, ou si vous souhaitez modifier la sélection, procédez comme suit :

1. Dans la fenêtre du téléscripteur à balayage, cliquez sur (paramètres).
   La fenêtre **Filter devices (Filtrer les périphériques)** s'ouvre.
2. Dans l'arborescence des périphériques, cochez les cases des entrées ou lecteurs que vous souhaitez surveiller. Les cases à cocher se comportent comme suit :
   Si vous sélectionnez une entrée, tous les appareils associés seront sélectionnés par défaut.
   Les cases à cocher de ces appareils peuvent être désactivées si elles ne sont pas nécessaires.
   Si **tous** les enfants d'un appareil parent sont sélectionnés, la case à cocher du parent est blanche. Si seulement **certains** sont sélectionnées, la case du parent est grise.
3. Cliquez sur **OK** pour terminer la sélection des lecteurs et fermer la fenêtre **Filter devices (Filtrer les périphériques)**.

Affichage des lecteurs sélectionnés sur le plan

- Double-cliquez sur un enregistrement dans le téléscripteur à balayage.

⇨ Le téléscripteur à balayage est automatiquement mis en pause.

⇨ Map View affiche, dans la fenêtre principale, la première scène de plan pertinente dans sa hiérarchie de plans et met en évidence le lecteur sur lequel vous avez double-cliqué.

Mettre le téléscripteur à balayage en pause

- Dans la fenêtre Téléscripteur à balayage, cliquez sur , ou double-cliquez sur un enregistrement dans la liste, pour mettre en pause l'affichage dynamique.

⇨ L'affichage dynamique se fige. Les enregistrements d'événements entrants sont mis en mémoire tampon mais ne sont pas affichés.

⇨ Un avis est placé en haut de la liste, indiquant que le flux d'événements a été mis en pause.

Reprise d'un téléscripteur à balayage mis en pause

- Dans la fenêtre Téléscripteur à balayage, cliquez sur pour reprendre l'affichage dynamique.

⇨ La liste dynamique affiche, dans l'ordre chronologique (le plus récent en premier), tous les événements d'accès qui se sont produits sur les lecteurs sélectionnés au cours des 10 dernières minutes, jusqu'à un maximum de 50.

⇨ Les événements d'accès plus anciens que les 50 plus récents ou qui se sont produits il y a plus de 10 minutes sont supprimés de la liste.

⇨ Les nouveaux événements d'accès sont à nouveau affichés en temps réel au fur et à mesure qu'ils se produisent.

Dupliquer le téléscripteur à balayage dans une fenêtre distincte

Notez qu'une seule fenêtre de téléscripteur peut être ouverte en double à la fois.

1. Dans la fenêtre Téléscripteur à balayage, cliquez sur  (fenêtre supplémentaire).
   La fenêtre séparée est un double et **n'est pas** indépendante du téléscripteur dans la fenêtre principale. Elle obéit aux mêmes paramètres.
   D'autres applications Map View, telles que la liste des alarmes, peuvent désormais être utilisées en parallèle dans la fenêtre principale.
2. Lorsque vous avez terminé d'utiliser la fenêtre distincte, utilisez la barre de titre pour la fermer.

33.1 Cas spéciaux

Téléscripteur à balayage Map View et portes B901

Afin de fournir des informations correctes à l'application du **téléscripteur à balayage** dans AMS Map View, les identifiants des portes B901 doivent correspondre aux identifiants de leurs points de porte. Autrement dit, la porte 1 doit être affectée au point de porte 1, la porte 2 au point de porte 2, etc.

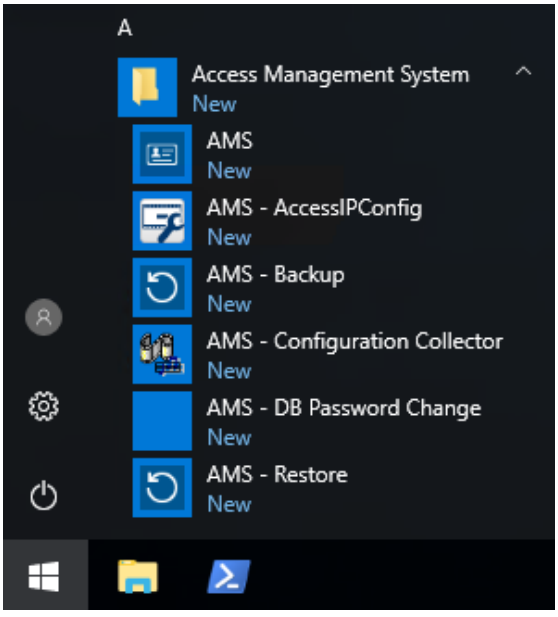
Doors 1 - 4	Door 1	Door 2	Door 3	Door 4
Door Name Text	Door 1	Door 2	Door 3	Door 4
Door Name Text (Second Language)				
Door Source	SDI2 (B901)	SDI2 (B901)	SDI2 (B901)	SDI2 (B901)
Entry Area	1	1	1	1
Associated Keypad #	Keypad 1	Keypad 1	Keypad 1	Keypad 1
Custom Function	Disabled	Disabled	Disabled	Disabled
Door Point	1	2	3	4
Door Point Debounce	600ms	600ms	600ms	600ms

Effectuez ces affectations au contrôleur de porte B901 dans l'outil RPS qui configure les centrales de détection d'intrusion et les contrôleurs.

34 Sauvegarde et Restauration

La fonction **Backup/Restore (Sauvegarde/Restauration)** vous permet de déplacer votre système avec ses données vers une nouvelle version d'AMS ou vers un nouvel ordinateur. La fonction **Backup/Restore (Sauvegarde/Restauration)** ne peut être exécutée que sur la machine sur laquelle le serveur AMS est installé. Deux raccourcis sont disponibles dans le menu Démarrer de Windows :

- **AMS - Backup (AMS - Sauvegarde)** pour créer une sauvegarde
- **AMS - Restore (AMS - Restauration)** pour restaurer une sauvegarde :

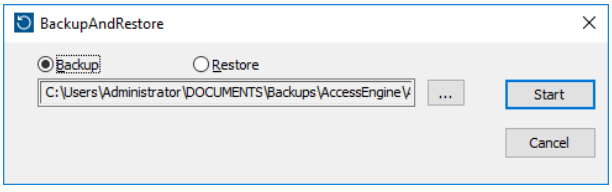


34.1 Sauvegarde du système

Cette section explique comment créer une sauvegarde pour l'application AMS et localiser les fichiers de sauvegarde SQL Server.

Création d'une sauvegarde de l'application AMS

1. Dans le menu Démarrer de Windows, cliquez avec le bouton droit de la souris sur **AMS - Backup (AMS - Sauvegarde)** et sélectionnez **Exécuter en tant qu'administrateur**.
   - La fonction **Backup/Restore (Sauvegarde/Restauration)** démarre par l'option **Backup (Sauvegarde)** présélectionnée.



2. Entrez un chemin pour sauvegarder le fichier `.GZ`.
3. Cliquez sur **Start (Démarrer)** pour démarrer la sauvegarde.
   - La fonction **Backup/Restore (Sauvegarde/Restauration)** crée un seul fichier `.GZ` et affiche la progression de l'opération dans une fenêtre contextuelle.
4. Copiez ce fichier dans un stockage sécurisé sur un autre ordinateur. Pour la sécurité des données, **ne laissez pas** l'unique copie sur le serveur DMS.

Recherche et copie des fichiers de sauvegarde SQL Server

1. À l'aide d'un explorateur de fichiers sur le serveur AMS, accédez à l'emplacement où SQL Server conserve ses fichiers `.BAK`.
   - Le chemin du fichier est le suivant, où `<version>` et `<instance name>` sont des variables qui dépendent de votre système :
     `C:`
     `\Program files\Microsoft SQL Server\MSSQL<version>.<instance name>\MSSQL\Backup\`
   - Les noms de fichiers se présentent sous la forme :
     `acedb.80fZe4b0-eb71-43ab-b2b6-db2517d4d6c7.bak`
     `Bosch.AlarmDb.80fZe4b0-eb71-43ab-b2b6-db2517d4d6c7.bak`
     `Bosch.EventDb.80fZe4b0-eb71-43ab-b2b6-db2517d4d6c7.bak`
     `Bosch.MapDb.80fZe4b0-eb71-43ab-b2b6-db2517d4d6c7.bak`
     `Bosch.MapViewDb.80fZe4b0-eb71-43ab-b2b6-db2517d4d6c7.bak`
     `Bosch.StatesDb.80fZe4b0-eb71-43ab-b2b6-db2517d4d6c7.bak`
2. Copiez **tous** les fichiers `.BAK` dans un stockage sécurisé sur un autre ordinateur. Pour la sécurité des données, **ne laissez pas** les uniques copies sur le serveur DMS.

Remarque!
Le chemin par défaut du journal des événements AMS est :
`C:\Program Files (x86)\Access Management System\Access Engine\AC\LgfLog\`

34.2 Restauration d'une sauvegarde

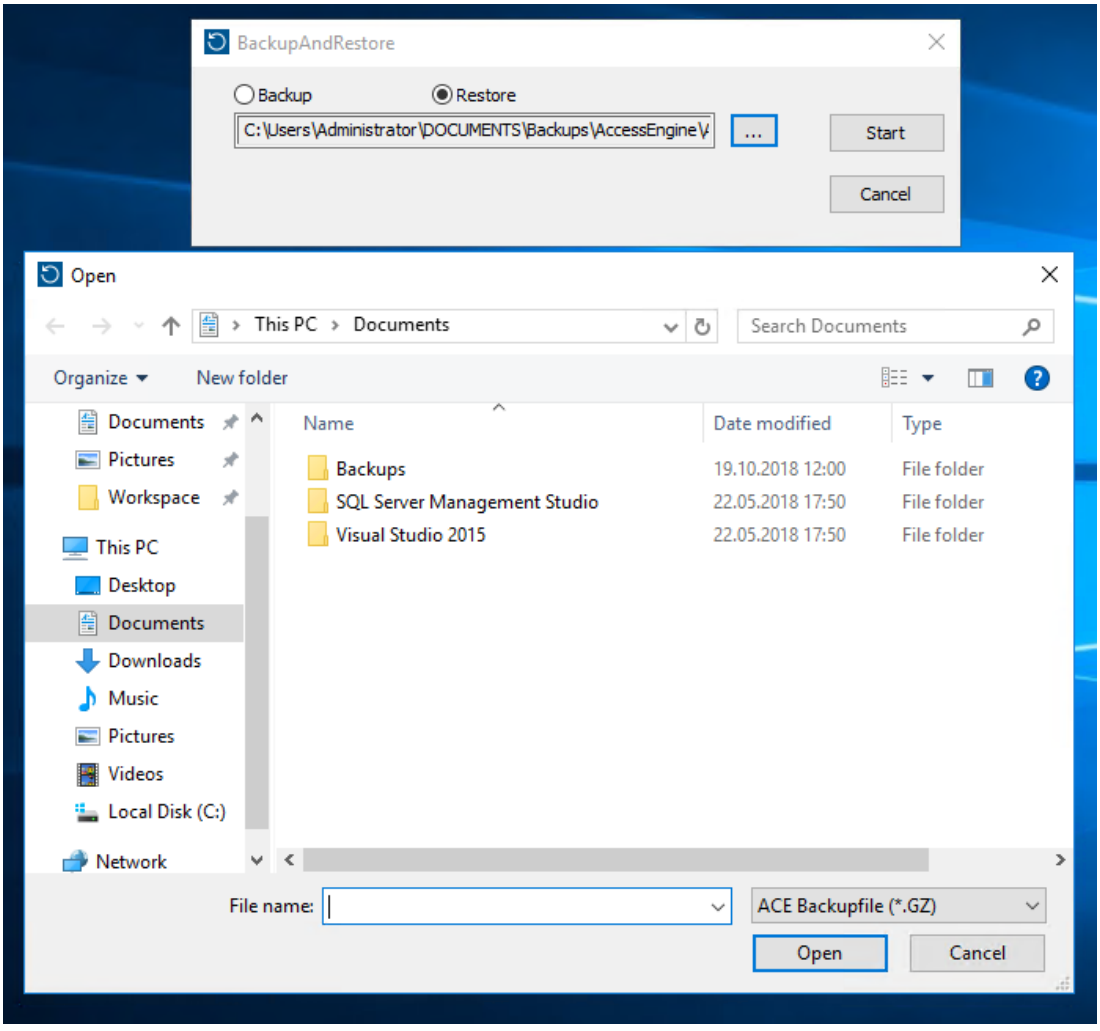
Conditions préalables

- Le fichier `GZ` créé par la fonction **Backup/Restore (Sauvegarde/Restauration)**
- Les fichiers `.BAK` créés par SQL Server que vous avez enregistrés pendant la procédure de sauvegarde.
- Un compte SQL avec les droits **sysadmin**, tels que `sa`.
- Un ordinateur cible convenablement préparé en termes de **licences** et de **certificats** :
  - **Licences** : L'ordinateur cible (sur lequel vous restaurez la sauvegarde) nécessite au moins des licences équivalentes à celles de l'ordinateur sur lequel vous avez effectué la sauvegarde.
  - **Certificats** : Tous les clients de l'ordinateur cible auront besoin des nouveaux certificats générés par l'installation sur l'ordinateur cible, et non de ceux générés par l'installation sur l'ordinateur d'origine.
    Consultez le **Guide d'installation d'AMS** pour la génération et l'installation de certificats clients.

Procédure

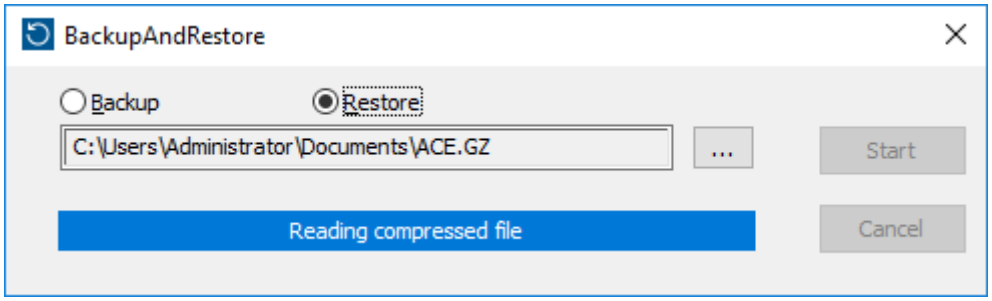
1. Dans le programme AMS, cliquez sur **File (Fichier)** > **Exit (Sortie)** pour arrêter l'application AMS.
2. Une fois le programme terminé, exécutez les **Services** Windows et assurez-vous que tous les services `Access Engine` et `Access Management System` sont arrêtés. Sinon, arrêtez-les ici.
3. **Si et seulement si** vous exécutez un MAC de basculement redondant (RMAC) avec votre MAC principal ou 1. MAC, passez au sous-chapitre suivant et effectuez la procédure qui y est décrite avant de revenir à cette étape.

4. Copiez les fichiers MSSQL `.BAK` que vous avez enregistrés à partir de l'ordinateur d'origine dans le même chemin sur le nouvel ordinateur.
   - Le chemin du fichier est le suivant, où `<version>` et `<instance name>` sont des variables qui dépendent de votre système :
     `C:\Program files\Microsoft SQL Server\MSSQL<version>.<instance name>\MSSQL\Backup\`
5. Dans le menu Démarrer de Windows, cliquez avec le bouton droit de la souris sur **AMS - Restore (AMS - Restauration)** et sélectionnez **Exécuter en tant qu'administrateur**.
   - La fonction **Backup/Restore (Sauvegarde/Restauration)** démarre par l'option **Restore (Restauration)** présélectionnée.
6. Cliquez sur le bouton **[...]** pour localiser le fichier de sauvegarde `GZ` dans le système de fichiers, puis cliquez sur **Open (Ouvert)** pour le sélectionner.



7. Cliquez sur **Start (Début)** pour démarrer le processus de restauration.
8. Lorsque vous êtes invité à entrer les informations d'identification du serveur, entrez les informations d'identification d'un administrateur système MSSQL, telles que `sa` et non les informations de connexion du serveur.

– Le processus de restauration commence.



9. Une fois le processus de restauration terminé, exécutez les **Services** Windows et redémarrez tous les services `Access Engine` et `Access Management System` manuellement.
10. Exécutez le programme de configuration du serveur `AMS Server Setup.exe` en tant qu'administrateur afin de resynchroniser les données sauvegardées avec les données système actuelles.

Se reporter à

– *Sauvegarde du système, page 256*

34.2.1 Restauration des RMAC dans une nouvelle installation

Remarque : Cette procédure n'est pertinente que dans le cas où vous effectuez la restauration sur un matériel différent la sauvegarde d'un système avec des MAC et des RMAC.

Introduction

Si vous restaurez une sauvegarde sur de nouveaux ordinateurs, vous devez reconfigurer les adresses IP des MAC et des RMAC qui étaient stockées dans le fichier de sauvegarde sur les adresses IP du nouveau matériel. Effectuez cette configuration en exécutant l'outil MACInstaller sur le nouveau matériel.

L'outil MACInstaller se trouve sur le support d'installation :

`\AddOns\MultiMAC\MACInstaller.exe`

L'utilisation de l'outil MACInstaller est décrite en détail dans le chapitre *Utiliser l'outil d'installation MAC, page 55*

Procédure

1. Exécutez l'outil MACInstaller sur l'ordinateur sur lequel 1.MAC est exécuté. Cet ordinateur peut être le serveur DMS ou un serveur dédié pour 1.MAC.
   – Dans l'outil, définissez les nouvelles adresses IP du MAC principal (cet ordinateur) et du RMAC.
2. Exécutez l'outil MACInstaller sur l'ordinateur sur lequel le RMAC est exécuté.
   – Dans l'outil, définissez les nouvelles adresses IP du MAC principal et du RMAC (cet ordinateur).
3. Revenez à l'étape où vous avez quitté la **Procédure de restauration**.

Se reporter à

– *Utiliser l'outil d'installation MAC, page 55*

Glossaire

1.MAC (premier MAC)

MAC principal (contrôleur d'accès principal) d'un système BIS Access Engine (ACE) ou Access Manager (AMS). Il peut résider sur le même ordinateur que le DMS, mais il peut également résider, comme un MAC subsidiaire, sur un ordinateur distinct appelé serveur MAC.

ACS

terme générique désignant un système de contrôle d'accès Bosch, par exemple, AMS (Access Management System) ou ACE (BIS Access Engine).

Alerte de menace

Alarme qui déclenche un niveau de menace. Les personnes dûment autorisées peuvent déclencher une alerte de menace avec une action momentanée, par exemple via l'interface utilisateur de l'opérateur, via un signal matériel (par exemple un bouton-poussoir), ou en présentant une carte d'alarme spéciale à n'importe quel lecteur.

Clé matérielle AMC

Code d'authentification interne que l'AMC génère à partir de certains paramètres matériels. Elle n'est pas visible pour l'utilisateur.

Clé principale

Code que le système génère à partir du DCP et qu'il utilise pour protéger les dispositifs de contrôle d'accès. La clé principale n'est jamais rendue visible à aucun utilisateur.

Contrôleur d'accès local

Périphérique matériel qui envoie des commandes d'accès au matériel de contrôle d'accès périphérique, par exemple des lecteurs et des verrous, et traite les demandes de ce matériel pour le système de contrôle d'accès global. Le contrôleur d'accès local le plus courant est un contrôleur modulaire d'accès ou un AMC.

CSN

Numéro de sélection de la carte.

DCP

mot de passe à partir duquel le système de contrôle d'accès génère une clé principale qui est utilisée pour chiffrer la communication réseau vers tous les contrôleurs d'accès locaux subordonnés, généralement des dispositifs AMC.

DDS (Destination Dispatching System)

également connu sous le nom de système de gestion de destination, mais n'utilisez que l'abréviation DDS. Otis CompassPlus est une sorte de dispositif DDS.

DER (Destination Entry Redirector)

ordinateur au même niveau qu'un dispositif DES (Destination Entry Server) dans un système Otis CompassPlus. Il se connecte à tous les groupes d'ascenseurs et son travail consiste à améliorer l'efficacité des dispositifs DES.

DSN

Nom de la source de données. Nom d'une source de données dans Open Database Connectivity (ODBC).

DTLS

Datagram Transport Layer Security est un protocole de communication sécurisé qui protège contre les écoutes clandestines et le sabotage.

Entrée

Le terme Entrée désigne dans son intégralité le mécanisme de contrôle d'accès à un point d'entrée : les lecteurs, une barrière verrouillable et une procédure d'accès telle que définie par des séquences de signaux électroniques passés entre les éléments matériels.

entrée princ.

« Demande de sortie ». Signal pour demander qu'une porte soit déverrouillée de l'intérieur pour permettre la sortie. Le signal est généralement déclenché par un bouton-poussoir ou une barre à l'intérieur d'une entrée ; parfois par un détecteur de mouvement.

entropie du mot de passe

mesure de la puissance du mot de passe calculée à partir de facteurs tels que son caractère aléatoire, le nombre de symboles disponibles et le nombre réel de symboles utilisés.

global

Forme simple de surveillance de séquence d'accès dans laquelle un détenteur de carte ne peut pas entrer deux fois dans une même zone sur une période de temps définie, à moins que la carte n'ait été scannée pour sortir de cette zone entre-temps. L'anti-passback dissuade une personne de transmettre ses informations d'identification au niveau d'une entrée dans le but de permettre à une seconde personne non autorisée d'entrer à son tour.

groupe d'ascenseurs

Groupe d'ascenseurs desservant de concert les mêmes étages. Chaque groupe d'ascenseurs est régi par un serveur DES.

IDS

Système de détection d'intrusion (Intruder Detection System), également connu sous le nom de système d'alarme antivol.

Liste blanche (SmartIntego)

Une liste blanche est une liste de numéros de cartes stockée localement sur les lecteurs de carte d'un système de verrouillage SmartIntego. Si le MAC du lecteur est hors ligne, le lecteur accorde l'accès aux cartes dont les numéros sont contenus dans sa liste blanche locale.

MAC (Contrôleur d'accès principal)

Dans les systèmes de contrôle d'accès, programme serveur qui coordonne et contrôle les contrôleurs d'accès locaux, généralement des AMC (Access Modular Controller).

Mode Bureau

Suspension du contrôle d'accès à une entrée au cours des heures de bureau ou d'activité.

Mode de configuration

état par défaut des dispositifs de contrôle d'accès dans l'éditeur de dispositif. Les modifications prennent effet et se propagent immédiatement aux dispositifs subordonnés.

Mode de fonctionnement

état d'un équipement de contrôle d'accès dans l'éditeur de dispositif lorsqu'il répond à des commandes données en dehors de l'éditeur de dispositif. Les modifications de configuration ne prennent effet qu'une fois le mode de fonctionnement terminé et le mode de configuration restauré.

Mode Normal

Contrairement au mode Bureau, le mode Normal n'accorde l'accès qu'aux personnes qui présentent des informations d'identification valides au lecteur.

Modèle de porte

Modèle de logiciel stocké d'un type d'entrée particulier. Les modèles de portes facilitent la définition des entrées dans les systèmes de contrôle d'accès.

Outil IPConfig

programme auxiliaire séparé pour configurer le réseau et les paramètres de sécurité réseau des périphériques matériels au sein du système de contrôle d'accès.

PIN de vérification

Numéro d'identification personnel (NIP ou PIN) utilisé en combinaison avec un identifiant physique pour renforcer la sécurité.

PIN d'identification

Numéro d'identification personnel (NIP ou PIN) qui est la seule information d'identification requise pour l'accès.

Point

Capteur pour détecter une intrusion dans une zone contrôlée par intrusion. Dans certains contextes, les points peuvent être appelés zones ou capteurs.

Point de rassemblement

Endroit désigné où les gens doivent attendre après avoir évacué un bâtiment.

réglage

pour suspendre une alarme dans des circonstances spécialement définies.

RMAC

Contrôleur d'accès principal (MAC) redondant qui est un jumeau synchronisé d'un MAC existant et qui prend en charge la gestion de ses données si le premier MAC échoue ou est déconnecté.

RPS

Logiciel de programmation à distance (Remote Programming Software). Programme qui gère les centrales de contrôle d'incendie ou de détection d'intrusion sur un réseau.

Serveur DES (Destination Entry Server)

Ordinateur qui gère une banque d'ascenseurs pour optimiser les temps de trajet.

Serveur MAC

Matériel : ordinateur (autre qu'un serveur DMS) dans un système Access Engine (ACE) ou Access Management (AMS), sur lequel un MAC ou un RMAC s'exécute.

SmartIntego

Système de verrouillage numérique des technologies Simons Voss. SmartIntego est intégré à certains systèmes de contrôle d'accès Bosch.

Surveillance de séquence d'accès

Suivi d'une personne ou d'un véhicule d'une zone définie à une autre en enregistrant chaque lecture de la carte d'identité et en accordant l'accès uniquement à partir des zones où la carte a déjà été scannée.

Système de gestion des données

Processus de haut niveau pour gérer les données de contrôle d'accès dans le système. Le système de gestion des données fournit des données aux contrôleurs d'accès principaux (MAC), qui à leur tour fournissent des données aux contrôleurs d'accès locaux (généralement AMC).

talonnage

Contournement du contrôle d'accès en suivant de près un titulaire de carte autorisé à travers une entrée sans présenter ses propres informations d'identification.

Terminal DET (Destination Entry Terminal)

Dispositif où les passagers d'ascenseur peuvent saisir des demandes de destination pour un groupe d'ascenseurs.

Touche LCD aléatoire

Code alphanumérique temporaire que l'AMC génère à nouveau à chaque démarrage. La clé peut être affichée sur l'écran à cristaux liquides (LCD) de l'AMC et peut être demandée par des outils logiciels pour authentifier la communication réseau.

Zone (Armement)

Regroupement d'entrées du modèle d'entrée 14 dans un système de contrôle d'accès. L'armement ou le désarmement du système de détection d'intrusion à l'une de ces entrées a simultanément le même effet à toutes les entrées où le paramètre Zone d'armement a la même désignation d'une lettre.

Bosch Security Systems B.V.
Torenallee 49
5617 BA Eindhoven
Netherlands
www.boschsecurity.com

Building solutions for a better life.

202309211026