



**BOSCH**

# Access Professional Edition

**fr**

Manuel de configuration



# Table des matières

<b>1</b>	<b>Présentation</b>	<b>5</b>
1.1	Conception modulaire	5
1.2	Modules serveur et client	5
<b>2</b>	<b>Général</b>	<b>6</b>
2.1	Introduction	6
2.2	Connexion utilisateur	7
2.3	Barre d'outils du Configurateur	10
2.4	Paramètres système généraux	14
<b>3</b>	<b>Configurations</b>	<b>17</b>
3.1	Création de nouvelles configurations	17
3.2	Ouverture des configurations	19
3.3	Activation d'une nouvelle configuration	20
3.4	Transmission des configurations aux contrôleurs	20
<b>4</b>	<b>Contrôleurs</b>	<b>24</b>
4.1	Définition et modification de nouveaux contrôleurs	24
4.2	Paramètres du contrôleur	27
<b>5</b>	<b>Signaux</b>	<b>30</b>
5.1	Signaux d'entrée	30
5.2	Signaux de sortie	32
5.3	Définition des conditions pour les signaux de sortie	37
5.3.1	Activer la fonction de contrôle avec une carte	41
5.4	Création de cartes d'extension	42
<b>6</b>	<b>Entrées</b>	<b>44</b>
6.1	Création et modification de modèles de portes	44
6.2	Affichage et paramétrage	48
6.3	Mode Bureau	54
6.4	Modèles de porte avec paramètres spéciaux	54
6.5	Affectation de périphériques vidéo à une entrée	55
<b>7</b>	<b>Zones</b>	<b>57</b>
<b>8</b>	<b>Groupes de personnel</b>	<b>62</b>
8.1	Accès groupe avec des lecteurs équipés d'un clavier	64
8.2	Restrictions de l'accès groupe	65
<b>9</b>	<b>Autorisations d'accès</b>	<b>66</b>
9.1	Création et affectation	66
9.2	Droits spéciaux	69
<b>10</b>	<b>Jours spéciaux</b>	<b>72</b>
10.1	Création et modification	72
<b>11</b>	<b>Modèles Jour</b>	<b>74</b>
11.1	Création et modification	74
<b>12</b>	<b>Modèles horaires</b>	<b>76</b>
12.1	Création et modification	78
<b>13</b>	<b>Textes</b>	<b>80</b>
13.1	Textes d'affichage	80
13.2	Messages du journal des événements	81
<b>14</b>	<b>Données du personnel supplémentaires</b>	<b>84</b>
<b>15</b>	<b>Gestion des périphériques vidéo</b>	<b>87</b>
15.1	Ouvrir le configurateur	87
15.2	Rechercher des appareils vidéo	87

15.3	Ajout d'un périphérique vidéo au système de contrôle d'accès	87
15.4	Modifier les données de connexion	88
15.5	Modification des données du périphérique vidéo	89
15.6	Affichage d'une image vidéo en direct	90
15.7	Affichage des archives	90
15.8	Affichages et processus	91
<b>16</b>	<b>Configuration d'un plan</b>	<b>94</b>
<b>17</b>	<b>Ajout d'un périphérique à un plan</b>	<b>96</b>
<b>18</b>	<b>Définition de carte</b>	<b>98</b>
<b>19</b>	<b>Configuration des alertes de menace</b>	<b>101</b>
19.1	Configuration du matériel pour les alertes de menace	101
<b>20</b>	<b>Annexe</b>	<b>103</b>
20.1	Signaux	103
20.2	Modèles de porte par défaut	104
20.3	Modèle de porte 01	105
20.4	Modèle de porte 03	107
20.5	Modèle de porte 06c	107
20.6	Modèle de porte 07	108
20.7	Modèle de porte 10	110
20.8	Modèle de porte 14	112
20.9	Exemples de configurations avec sas de sécurité	114
20.10	Configuration du modèle d'entrée 07	116
20.11	Affichage de l'armement/désarmement	117
20.12	Procédures sous le contrôle d'accès	119
20.13	Ports d'Access PE	123
<b>21</b>	<b>Types de PIN</b>	<b>124</b>
<b>22</b>	<b>Exigences UL 294</b>	<b>126</b>

# 1 Présentation

## 1.1 Conception modulaire

Le système Access Professional Edition (ci-après **Access PE**) permet aux PME de disposer d'un contrôle d'accès autonome. Il se compose de plusieurs modules :

- Service LAC : un processus qui communique en continu avec les LAC (contrôleurs d'accès locaux – ci-après « contrôleurs »). Les contrôleurs d'accès modulaire AMC (Access Modular Controllers) sont utilisés comme des contrôleurs.
- Configurateur
- Gestion du personnel
- Visionneur de journal
- Gestion des alarmes
- Vérification vidéo

## 1.2 Modules serveur et client

Ces modules peuvent être divisés en modules serveur et client.

Le service LAC doit rester en contact permanent avec les contrôleurs pour plusieurs raisons : premièrement parce qu'il reçoit en continu des messages de leur part concernant les déplacements, la présence et l'absence des détenteurs de carte ; deuxièmement parce qu'il transmet aux contrôleurs les modifications apportées aux données, par exemple, l'attribution de nouvelles cartes ; et dernièrement parce qu'il effectue des vérifications de méta-niveau (vérifications des séquences d'accès, vérifications anti-retour, surveillance aléatoire).

Le Configurateur doit également être exécuté sur le serveur. Il peut toutefois être installé sur des postes de travail clients et commandé depuis ces postes.

Les modules Gestion du personnel et Visionneur de journal font partie du composant Client et peuvent également être exécutés sur le serveur ou sur un autre PC disposant d'une connexion réseau avec le serveur.

Les contrôleurs suivants peuvent être utilisés :

- AMC2 4W (doté de quatre interfaces lecteur Wiegand) - Possibilité d'extension avec un AMC2 4W-EXT
- AMC2 4R4 (doté de quatre interfaces lecteur RS485)

## 2

### 2.1

# Général

## Introduction

Access PE est un système de contrôle d'accès conçu pour offrir les normes de sécurité et de souplesse les plus élevées aux PME.

Access PE doit sa stabilité et son extensibilité à son architecture à trois couches : **La première couche** correspond au niveau d'administration et à ses services de contrôle. Toutes les tâches d'administration sont effectuées à ce niveau, telles que l'enregistrement de nouvelles cartes et l'affectation des droits d'accès, par exemple.

**La deuxième couche** se compose de contrôleurs d'accès locaux (LAC) qui gèrent chaque groupe de portes ou d'entrées. Un LAC est capable de prendre des décisions relatives au contrôle d'accès de manière indépendante, et ce même lorsque le système est hors ligne. Les LAC sont chargés de contrôler les entrées, de gérer les heures d'ouverture des portes ou de demander la saisie de codes PIN à des points d'accès sensibles.

**La troisième couche** se compose de lecteurs de carte.

La communication entre le client, le serveur et les détenteurs de carte est chiffrée par AES.

La version multi-utilisateur d'Access PE permet de contrôler le système depuis plusieurs postes de travail. Les niveaux personnalisables des droits de l'utilisateur permettent de réguler l'accès et garantissent la sécurité. Il est ainsi possible de gérer les données des cartes depuis un poste de travail tout en vérifiant la présence d'un employé dans le bâtiment à partir d'un autre poste.

Access PE offre une configuration exceptionnellement souple pour les droits d'accès, les modèles horaires et les paramètres des entrées. La liste ci-après fournit un aperçu des caractéristiques les plus importantes de ce logiciel :

#### **Attribution rapide et aisée des cartes**

Des cartes (jusqu'à trois) peuvent être attribuées aux personnes manuellement ou par le biais d'un lecteur de boîte de dialogue connecté à un PC via une connexion en série. Toutes les cartes affectées sont actives. Lors de la mise à jour d'une carte, l'ancienne carte est automatiquement écrasée et mise hors service, ce qui permet d'empêcher tout accès avec d'anciennes cartes même si les opérateurs ont oublié ou n'ont pas été en mesure de les annuler.

#### **Droits d'accès (y compris les privilèges de groupe)**

Toute personne peut hériter de privilèges de groupe tout en se voyant accorder des droits individuels. Les privilèges peuvent être restreints en fonction de la zone et de l'heure avec un degré de précision d'une minute. Les privilèges de groupe peuvent servir à accorder ou à restreindre les droits d'accès pour un ou tous les détenteurs de carte simultanément. Les privilèges de groupe peuvent être configurés en fonction de modèles horaires, ce qui a pour effet de restreindre l'accès à certaines heures de la journée.

#### **Suivi de l'accès**

La définition de zones permet de suivre et de mettre en vigueur une séquence d'accès adaptée. Même sans surveillance, cette configuration permet d'afficher l'endroit où se trouve un détenteur de carte.

#### **Anti-Passback**

Lors de la lecture d'une carte, celle-ci peut être bloquée pendant une période déterminée de manière à empêcher une nouvelle entrée par le même point d'accès. Il est ainsi possible d'empêcher un « retour », c'est-à-dire lorsque l'utilisateur remet sa carte à quelqu'un par-dessus une barrière afin d'accorder l'accès à une personne non autorisée.

#### **Annulation automatique des cartes après expiration**

Il est fréquent que les visiteurs et le personnel temporaire aient besoin d'un accès seulement pour une période limitée.

Les cartes peuvent être enregistrées pour une période de temps donnée de manière à ce que leur validité expire automatiquement une fois cette période écoulée.

#### **Modèles horaires et modèles Jour**

Des modèles horaires spécifiques peuvent être attribués à un détenteur de carte, régulant ainsi les heures auxquelles cette personne dispose d'un accès. Ils peuvent être définis de manière souple à l'aide de modèles Jour qui déterminent la façon dont des jours de la semaine, des week-ends, des congés et des jours spéciaux particuliers diffèrent des journées de travail ordinaires.

#### **Identification par code PIN**

Au lieu d'utiliser une carte, une personne peut saisir un code PIN spécial pour entrer.

#### **Vérification par code PIN**

Les zones particulièrement sensibles peuvent être programmées pour demander la saisie de codes PIN supplémentaires. Cette protection peut elle aussi être configurée en fonction de modèles horaires de manière à ce qu'un code PIN soit uniquement demandé, par exemple, pour accorder l'accès pendant des congés ou en dehors des heures de travail définies.

#### **Souplesse de la gestion des portes**

La souplesse du paramétrage des modèles de portes individuelles vous permet de bénéficier d'un équilibre optimal entre sécurité et confort. La période de « réglage » ou de suppression de l'alarme peut être configurée individuellement pour déterminer la durée pendant laquelle une porte peut rester ouverte. En conjonction avec un système d'alarme, le point d'accès peut ensuite être facultativement verrouillé.

#### **Déverrouillage de porte périodique**

Afin de faciliter l'accès, les alarmes de porte peuvent être réglées pour déverrouiller les portes pendant des périodes déterminées. Les périodes de déverrouillage des portes peuvent être définies manuellement ou automatiquement via un modèle horaire.

#### **Heure & présence**

Les points d'accès peuvent être paramétrés pour enregistrer les entrées et les sorties dans le but de contrôler les heures de présence.

#### **Conception de cartes**

Le module complémentaire **Personnalisation de carte (Card Personalization - CP)** est entièrement intégré dans le système de contrôle d'accès pour permettre à l'opérateur de créer des cartes sans avoir à basculer entre plusieurs applications.

#### **Affectation de photos**

Si le module complémentaire **Personnalisation de carte (Card Personalization - CP)** n'est pas activé, l'identification photographique peut néanmoins être importée et associée aux détenteurs de carte.

#### **Système de verrouillage hors ligne**

Les zones qui, pour une raison quelconque, ne sont pas couvertes par le système de contrôle d'accès haute disponibilité peuvent néanmoins être verrouillées hors ligne.

#### **Gestion des périphériques vidéo**

Les entrées peuvent être équipées de caméras supplémentaires destinées à identifier et à suivre les déplacements des personnes qui les utilisent.

## **2.2 Connexion utilisateur**

Les applications ci-après sont disponibles. Consultez les manuels utilisateur respectifs pour plus de détails :

	<b>Gestion du personnel</b>
	<b>Configurateur</b>
	<b>Visionneur de journal</b>
	<b>Plan et gestion des alarmes</b>
	<b>Vérification vidéo</b>

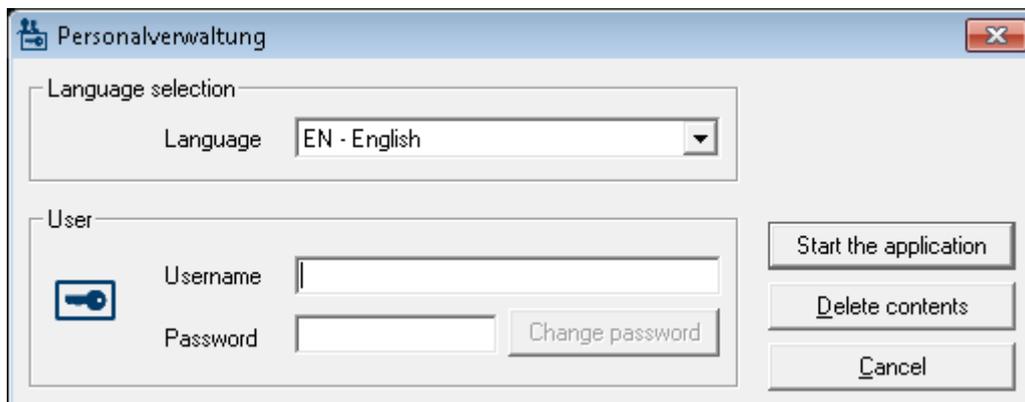
**Remarque!**

Une connexion du client est uniquement disponible avec le service LAC exécuté sur le serveur.

**Connexion client**

Les applications du système sont protégées contre les utilisations non autorisées. Les **mots de passe par défaut** à la première utilisation sont les suivants :

- Nom d'utilisateur : **bosch**
- Mot de passe : **bosch**



Après avoir saisi un nom d'utilisateur et un mot de passe, le bouton **Modifier le mot de passe** devient actif.

Après 3 saisies incorrectes, il en résulte un délai avant de pouvoir tenter une autre connexion. Cela s'applique aux boutons « Lancer l'application » et « Modifier le mot de passe ».

La liste déroulante supérieure peut être utilisée pour sélectionner la **langue** d'interaction souhaitée. La langue sélectionnée par défaut est celle utilisée lors de l'installation de l'application. Lorsqu'un autre utilisateur se connecte sans redémarrer l'application, la langue utilisée par l'utilisateur précédent est conservée. C'est pour cette raison qu'une boîte de dialogue peut apparaître dans une langue autre que la langue souhaitée. Pour éviter cette situation, connectez-vous de nouveau à Access PE.

Les applications d'Access PE peuvent être exécutées dans les langues suivantes :

- Anglais
- Allemand
- Français
- Japonais
- Russe
- Polonais
- Chinois (RPC)
- Néerlandais
- Espagnol
- Portugais (Brésil)

**Remarque!**

Toutes les fonctionnalités tels que les noms de périphérique, les intitulés, les modèles et les schémas de droits d'utilisateur sont affichés dans la langue dans laquelle ils ont été saisis. Des boutons et des intitulés similaires contrôlés par le système d'exploitation peuvent apparaître dans la langue du système d'exploitation.

Après avoir cliqué sur le bouton **Modifier le mot de passe**, saisissez un nouveau nom d'utilisateur et un nouveau mot de passe dans cette boîte de dialogue :

The image shows a standard Windows-style dialog box titled "Change password". It contains two text input fields. The first is labeled "New password" and the second is labeled "Confirmation". At the bottom of the dialog, there are two buttons: "Ok" and "Cancel".

**Remarque!**

Pensez à changer le mot de passe !

Le bouton **Lancer l'application** vérifie les privilèges de l'utilisateur et, en fonction du résultat, lance l'application. Si le système ne parvient pas à authentifier la connexion, le message d'erreur suivant s'affiche : **Nom d'utilisateur ou mot de passe incorrect !**

## 2.3 Barre d'outils du Configurateur

Les fonctions suivantes peuvent être appelées via les menus, les icônes de la barre d'outils ou la saisie de raccourcis spécifiques.

Fonction	Icône/ Raccourci	Description
<b>Menu Fichier</b>		
Nouveau	 Ctrl + N	Efface tous les paramètres dans les boîtes de dialogue de configuration (à l'exception des paramètres par défaut) pour vous permettre de définir une nouvelle configuration.
Ouvrir...	 Ctrl + O	Ouvre une boîte de dialogue permettant de sélectionner une configuration différente à charger.
Enregistrer	 Ctrl + S	Enregistre les modifications dans le fichier de configuration actuel.
Enregistrer sous...		Enregistre la configuration actuelle dans un nouveau fichier.
Activer la configuration		Active une configuration chargée et enregistre la configuration qui était valide jusqu'à présent.
Envoyer la configuration au LAC		Transmet les modifications de configuration enregistrées au service LAC.
Répertorier les configurations valides récemment		Ouvre directement les configurations sans passer par la fonction <b>Ouvrir</b> de la boîte de dialogue de sélection.
Sortie		Ferme le Configurateur d'Access PE.
<b>Menu Affichage</b>		
Barre d'outils		Active/Désactive l'affichage de la barre d'outils (par défaut = activé).

Fonction	Icône/ Raccourci	Description
Barre d'état		Active/Désactive l'affichage de la barre d'état située au bas de la fenêtre (par défaut = activé).
<b>Menu Configuration</b>		
Général		Ouvre la boîte de dialogue <b>Paramètres généraux</b> qui permet de configurer les contrôleurs et les paramètres généraux du système.
Signaux d'entrée		Ouvre la boîte de dialogue qui permet de paramétrer les signaux d' <b>entrée</b> .
Signaux de sortie		Ouvre la boîte de dialogue qui permet de paramétrer les signaux de <b>sortie</b> .
Entrées		Ouvre la boîte de dialogue <b>Entrées</b> qui permet de paramétrer les portes et les lecteurs de carte.
Zones		Ouvre la boîte de dialogue <b>Configuration des zones</b> qui permet de diviser le site protégé en zones virtuelles.
Congés		Ouvre la boîte de dialogue <b>Congés</b> qui permet de définir les congés et les jours spéciaux.
Modèles Jour		Ouvre la boîte de dialogue <b>Modèles Jour</b> qui permet de définir les périodes d'une journée pendant lesquelles les fonctions d'accès seront activées.
Modèles horaires		Ouvre la boîte de dialogue <b>Modèles horaires</b> qui permet de définir des zones horaires en fonction des jours de la semaine ou du calendrier.

Groupes de personnel		Ouvre la boîte de dialogue <b>Groupes de personnel</b> qui permet de répartir le personnel en groupes logiques.
Groupes d'autorisation d'accès		Ouvre la boîte de dialogue <b>Groupes d'autorisation d'accès</b> qui permet de définir des groupes d'autorisations pour les entrées.
Système de verrouillage hors ligne		Ouvre la boîte de dialogue <b>Système de verrouillage hors ligne</b> qui permet de configurer les éléments particuliers du site (entrées, modèles horaires, groupes d'autorisation).
Textes d'affichage		Ouvre la boîte de dialogue <b>Textes d'affichage</b> qui permet de modifier les textes affichés sur les lecteurs de carte.
Messages du journal		Ouvre la boîte de dialogue <b>Messages du journal</b> qui permet de modifier et de classer les messages du journal par catégorie.
Champs supplémentaires pour le personnel		Ouvre la boîte de dialogue <b>Champs supplémentaires pour le personnel</b> qui permet de définir des champs de données pour le personnel.
Wiegand - Cartes		Ouvre la boîte de dialogue <b>Wiegand - Cartes</b> qui permet de définir la structure des données des cartes.
Administration des périphériques vidéo		Ouvre la boîte de dialogue <b>Périphériques vidéo</b> qui permet de configurer les caméras à utiliser pour la vérification vidéo.
Visionneur de plan et gestion des alarmes		Ouvre le <b>Visionneur de plan</b> pour une vue réelle des plans et périphériques de contrôle, et la liste des alarmes pour la gestion des alarmes.
Menu <b>Réglages</b>		

Activation de la licence		Ouvre un menu qui permet de sélectionner ou désélectionner les licences
Réinitialiser les messages et les textes du lecteur		Ouvre une demande si le journal des connexions et les textes du lecteur doivent être mis à jour.
<b>Menu ? (Aide)</b>		
Rubriques d'aide		Ouvre les présents textes d'aide.
À propos d'Access Professional Edition - Configurateur		Affiche des informations d'ordre général sur Access Professional Edition - Configurateur

## 2.4 Paramètres système généraux

Les paramètres système généraux s'affichent sous la liste des paramètres du contrôleur. Ceux-ci sont valables pour toutes les installations.

Default card data Country code <input type="text" value="00"/> Customer code <input type="text" value="056720"/>	PIN code Number of digits <input type="text" value="4"/> Number of retries before blocking <input type="text" value="3"/> <input type="checkbox"/> use separate IDS pin
LAC subsystem process Poll interval on serial connected LAC in ms <input type="text" value="200"/> Read-timeout on serial connected LAC in ms <input type="text" value="500"/> Create TA-data at <input type="text" value="00:01"/> <input type="checkbox"/> Export personnel and TA data	Logbook parameter Number of files <input type="text" value="366"/> (one logfile per day, 0 = unlimited)
<input type="checkbox"/> Show welcome/leaving message <input type="checkbox"/> Show cardholder name in display	Directories Database <input type="text" value="C:\BOSCH\Access Professional Edition\PE\Data\D"/> Event log <input type="text" value="C:\BOSCH\Access Professional Edition\PE\Data\lv"/> Import files <input type="text" value="C:\BOSCH\Access Professional Edition\PE\Data\lr"/> ... Export files <input type="text" value="C:\BOSCH\Access Professional Edition\PE\Data\E"/> ... DLL-files <input type="text" value="C:\BOSCH\Access Professional Edition\PE\Data\D"/> Pictures <input type="text" value="C:\BOSCH\Access Professional Edition\PE\Data\P"/> ... Test logs <input type="text" value="C:\BOSCH\Access Professional Edition\PE\Data\L"/>

Paramètre	Par défaut	Description
Code pays	00	Des données de la carte sont ajoutées au numéro de carte saisi manuellement.
Code client	056720	
Intervalles d'invitation sur le LAC connecté en série en ms	200	Intervalle de temps en millisecondes entre les invitations envoyées au service LAC pour vérifier le bon fonctionnement des connexions avec un contrôleur.
Délai de lecture sur le LAC connecté en série en ms	500	Plage de valeurs pour l'intervalle d'invitation : 1 à 500 Valeurs possibles pour le délai de lecture : 1 à 3 000
Créer des données de gestion du temps de travail à	00:01	Précise l'heure à laquelle le fichier de données Heure & présence doit être créé.
Exporter les données du personnel et les données de gestion du temps de travail	désactivé	Lorsque cette option est activée, les données Heure & présence sont écrites en continu sur le fichier d'exportation. Lorsqu'elle est désactivée, le fichier de données est créé à l'heure indiquée dans le paramètre <b>Créer des données de gestion du temps de travail à</b> .
Le fichier contenant les heures de présence est créé dans le répertoire suivant : C:\Program Files\Bosch\Access Professional Edition\PE\Data\Export sous le nom <b>TA_&lt;Date actuelle AAAAMMJJ&gt;.dat</b>		

Paramètre	Par défaut	Description
Afficher le message de bienvenue/de départ	activé	Si le type de lecteur et les paramètres appropriés ont été définis ( <b>Arrivée</b> , <b>Départ</b> ou <b>Vérification OK</b> dans la boîte de dialogue Entrées), le lecteur affichera les messages de bienvenue et de départ enregistrés pour le détenteur de carte dans la boîte de dialogue Données du personnel de l'application Gestion du personnel. Ne concerne pas les lecteurs Wiegand.
Afficher le nom du détenteur de la carte à l'écran	activé	Les lecteurs équipés d'un écran afficheront le <b>Nom affiché</b> enregistré dans les données du personnel du détenteur de la carte. Ne concerne pas les lecteurs Wiegand.
Nombre de chiffres	4	Détermine le nombre de chiffres requis pour un PIN de vérification ou d'armement. Ce paramètre s'applique également au PIN de la porte qui peut être défini lors de la configuration des entrées. Valeurs possibles : 4 à 8
utiliser un code PIN IDS distinct		Si aucun code PIN IDS distinct n'est défini, un PIN de vérification peut être utilisé pour armer l'IDS (système de détection d'intrusion). Les champs de saisie pour le PIN d'armement seront activés dans la boîte de dialogue Personnel uniquement si cette case est cochée. Dans ce cas, le PIN de vérification ne peut plus être utilisé pour armer l'IDS.
Nombre de tentatives avant blocage	3	Nombre de tentatives infructueuses pour saisir le code PIN. Si le détenteur de carte saisit un code PIN incorrect le nombre de fois défini ici, celui-ci provoquera un verrouillage de l'ensemble du système qui peut uniquement être supprimé par un utilisateur système autorisé dans Gestion du personnel. Valeurs possibles : 1 à 9

Paramètre	Par défaut	Description
Paramètre de journal	366	Nombre de journaux par jour Valeurs possibles : 180 à 9999. REMARQUE : si une valeur < 180 est saisie, elle est automatiquement remplacée par la valeur minimum de 180.
Chemins d'accès aux répertoires : Base de données Fichier de journal Importer les fichiers Exporter les fichiers Fichiers DLL Données d'image Test de connexion	C:\Program Files\BOSCH \Access Professional Edition\PE \Data... \Db \MsgLog \Import \Export \Dll \Pictures \Log	Les chemins d'accès indiqués ici correspondent aux emplacements par défaut. Les répertoires pour les fichiers d'importation, d'exportation et d'images peuvent être modifiés.

**Remarque!**

Pour pouvoir utiliser les codes PIN d'identification, d'armement ou de la porte sur des contrôleurs et lecteurs Wiegand, l'option **PIN ou carte** de la définition de carte Wiegand doit être activée.

## 3 Configurations

La composition d'un système (quelles entrées sont à tel endroit, combien de lecteurs et de quel type, comment sont configurées les autorisations d'accès, etc.) est enregistrée dans des fichiers spéciaux. Il peut exister plusieurs versions de ces fichiers de configuration (\*.cfg). Cependant, seul celui avec le nom de fichier **\*active.cfg** peut activer le système utilisé. Cela permet de tester de nouveaux scénarios, d'effectuer des passages d'essai et de modifier rapidement le système.

### 3.1 Création de nouvelles configurations

Toutes les configurations d'Access PE sont stockées dans le dossier **C:\BOSCH\Access Professional Edition\PE\Data\Cfg** (sauf si des répertoires et noms de dossier différents des valeurs par défaut ont été définis au moment de l'installation). Deux fichiers de configuration sont créés au cours de l'installation, à savoir **Active.acf** et **Default.acf**. Tandis que le fichier Active.acf contient des données d'exemple, qui peuvent se révéler utiles pour l'utilisateur, le fichier Default.acf contient uniquement des données système prédéfinies.

Les données système comprennent :

- La zone **--extérieur--**.
- Des exemples de congés et de jours spéciaux
- Les groupes de personnel **Employés** et **Visiteurs**
- Les textes d'affichage pour les lecteurs.
- Les textes du journal des connexions

Access PE utilise toujours la configuration **Active.acf au démarrage**.

Une configuration peut comporter différents états qu'il est important de bien distinguer.

- Une configuration **Active** désigne une configuration dont les définitions, paramètres etc. sont actuellement utilisés par le système en cours d'utilisation.
- Une configuration **Ouverte** (« chargée ») désigne une configuration qui est actuellement en cours de modification par les utilisateurs du système. Celle-ci peut être enregistrée ultérieurement dans un fichier .acf distinct et/ou être activée ultérieurement. Cependant, **elle n'a aucune influence sur le système en cours d'exécution tant qu'elle n'est pas activée**.

Vous pouvez définir et enregistrer le nombre de configurations de votre choix dans Access PE. Dans la mesure où de nouvelles configurations peuvent être créées et modifiées indépendamment du système en cours d'exécution, il est possible, par exemple, de définir de nouvelles zones qui seront intégrées dans le site surveillé à une date ultérieure.

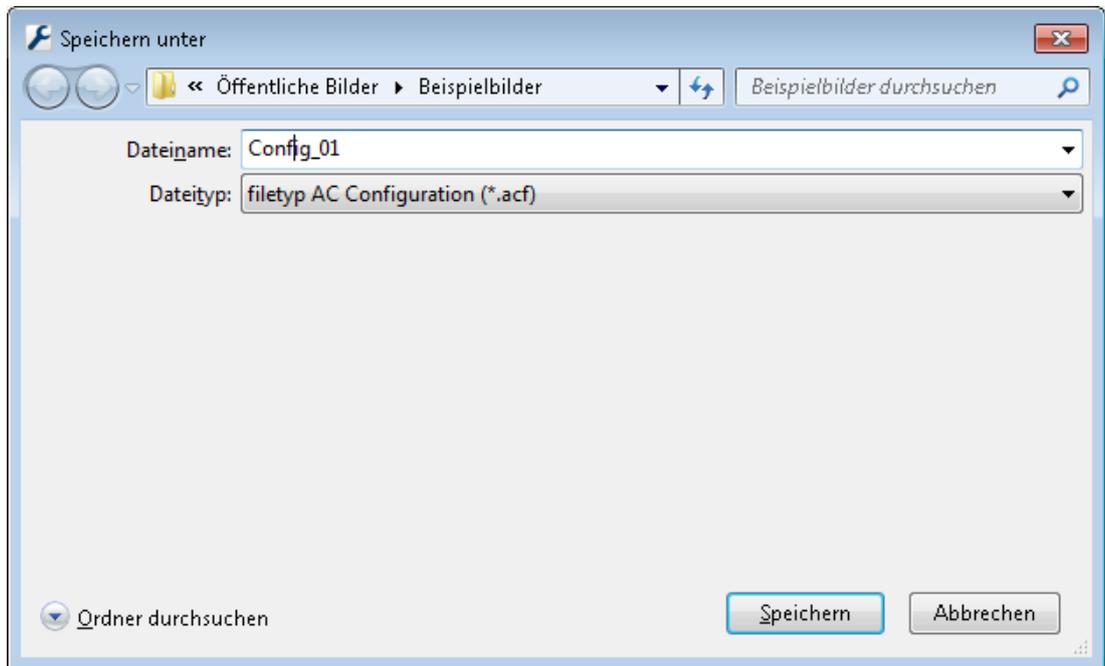
Vous pouvez ouvrir (charger) la configuration par défaut **Untitled.acf** et ses paramètres de



base à l'aide du bouton  situé dans la barre d'outils. Si une configuration est modifiée dans le but d'en créer une nouvelle, celle-ci doit être enregistrée sous un nom différent et approprié.



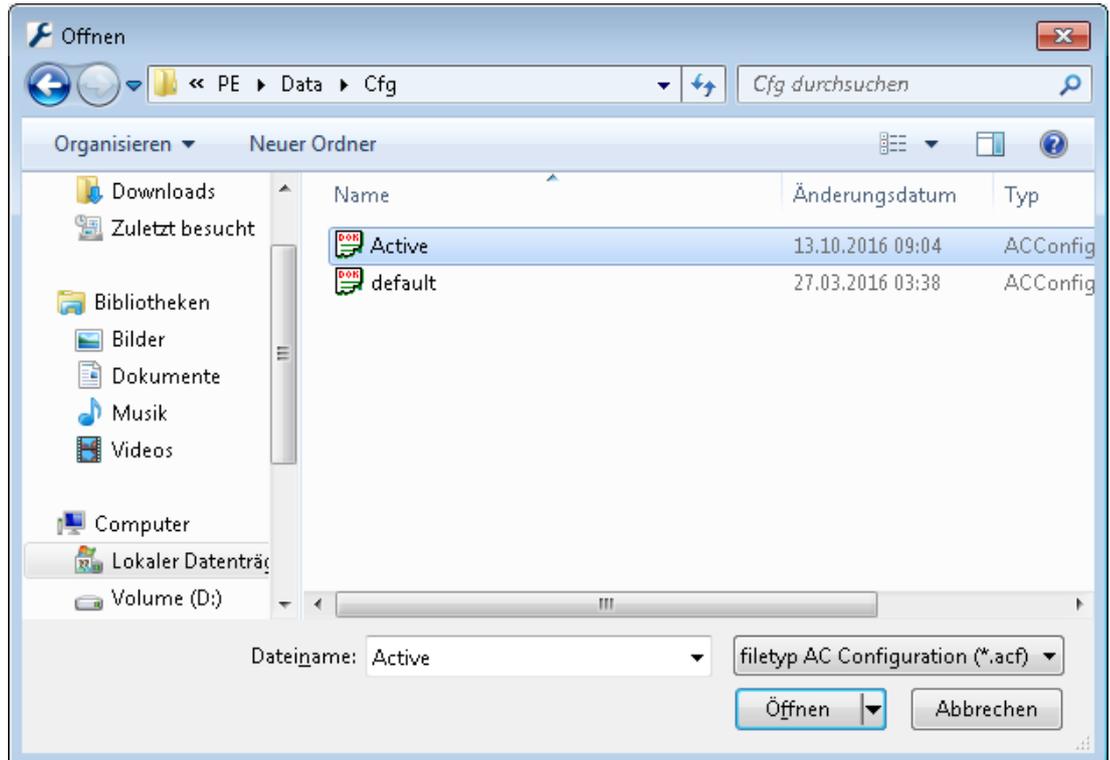
Le bouton  ouvre une boîte de dialogue permettant d'enregistrer le fichier dans le répertoire Cfg. Vous devez remplacer le nom de fichier par défaut **untitled.acf** par un nom de fichier plus explicite.



## 3.2 Ouverture des configurations

Le Configurateur s'ouvre toujours avec la configuration **Active.acf**. Si vous souhaitez

appliquer une configuration différente, utilisez le bouton  pour charger une configuration existante à partir du dossier **C:\BOSCH\Access Professional Edition\PE\Data\Cfg** (par défaut).



Si l'utilisateur souhaite modifier ou compléter une configuration existante en vue de l'activer ultérieurement, il peut ouvrir une configuration de base, la modifier, puis l'enregistrer sous un nom différent. Cela permet de réutiliser et de compléter des configurations précédentes, et évite ainsi de recommencer à chaque fois à partir des paramètres très basiques du fichier **default.acf**.



### Remarque!

Il est également possible d'enregistrer la configuration active sous un nouveau nom en tant que copie de travail en vue de la charger et de la modifier ultérieurement.

### 3.3 Activation d'une nouvelle configuration

Le Configurateur offre la possibilité de gérer plusieurs configurations dans plusieurs fichiers .acf. La configuration active est toujours enregistrée dans le fichier **Active.acf**.



#### Attention!

Dans la mesure où le fichier **active.acf** est écrasé lors de la création d'une nouvelle configuration, nous recommandons à l'utilisateur de créer au plus vite une copie de sauvegarde de la configuration active sous un nouveau nom de fichier.

Il est nécessaire d'ouvrir les fichiers de configuration pour pouvoir les activer. Vous devez donc ouvrir une configuration ayant été modifiée et enregistrée au préalable.

Ensuite, pour activer la configuration ouverte, veuillez procéder comme suit:

- Via le menu : **Fichier > Activer la configuration**, ou



- En utilisant le bouton dans la barre d'outils.

Le processus d'activation s'opère ensuite par étapes :

- Tout d'abord, confirmez le contrôle de sécurité.

**: Souhaitez-vous vraiment remplacer la configuration actuelle par la nouvelle configuration ?**

- La configuration active jusqu'à présent est sauvegardée dans un fichier avec le format de nom suivant : **\$aaaaMMjjhhmss -Active.acf** (a = année ; M = mois ; j = jour ; h = heure ; m = minute ; s = secondes).
- La configuration actuellement ouverte est ensuite enregistrée sous le nom de fichier **Active.acf**, ce qui signifie que l'ancienne configuration active sera écrasée !

Une fenêtre d'informations indique le nom du fichier enregistré : **: La nouvelle configuration a été enregistrée sous <nomdufichier> !**

### 3.4 Transmission des configurations aux contrôleurs

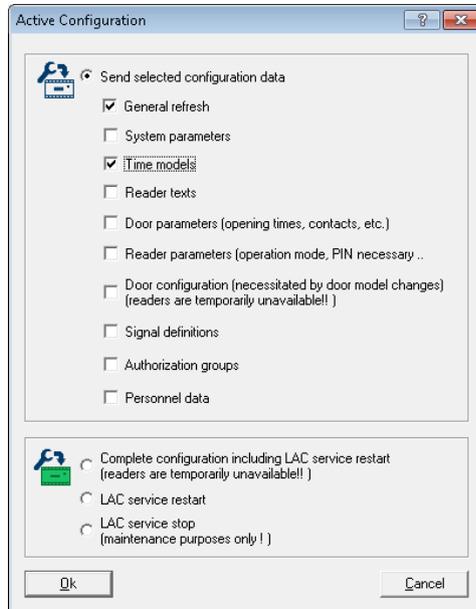
Après avoir effectué des modifications dans la configuration active **Active.acf**, vous devez transmettre ces modifications aux contrôleurs. Cette opération peut être effectuée de deux manières :

- Menu **Fichier > Envoyer la configuration au service LAC**



- En utilisant le bouton dans la barre d'outils.

La boîte de dialogue suivante s'affiche, dans laquelle vous pouvez sélectionner les données de configuration à transmettre aux contrôleurs.



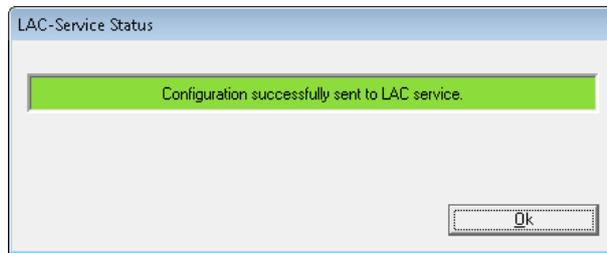
Les données modifiées et enregistrées sont présélectionnées. Vous pouvez sélectionner d'autres éléments ou supprimer des éléments sélectionnés.

Lorsque vous avez terminé de sélectionner les données à transmettre aux contrôleurs, cliquez sur **OK**.

<b>Données de configuration</b>	<b>La transmission aux LAC est nécessaire en cas de...</b>
Actualisation générale	... modification des messages du journal, des champs supplémentaires ou des définitions de carte.
Paramètres système	... modification matérielle du LAC.
Modèles horaires	... modification des congés, des modèles Jour ou des modèles horaires.
Textes du lecteur	... modification des textes d'affichage.
Paramètres de la porte	... modification d'un ou de plusieurs des éléments suivants aux entrées : <ul style="list-style-type: none"> <li>- l'heure d'ouverture (en 1/10 s)</li> <li>- le contact de porte</li> <li>- les données relatives au contrôle de la porte (heures d'ouverture, contacts, profils horaires, etc.)</li> </ul>
Paramètres du lecteur	... modification d'un ou de plusieurs des éléments suivants aux entrées : <ul style="list-style-type: none"> <li>- les données des lecteurs d'entrée ou de sortie</li> <li>- l'heure de suppression des alarmes (en 1/10 s).</li> <li>- le comportement de l'entrée en cas d'anti-retour</li> </ul>

Données de configuration	La transmission aux LAC est nécessaire en cas de...
	– les boutons déclenchant l'ouverture de la porte
Configuration de la porte	... modification du modèle de porte aux entrées. <b>Remarque :</b> la saisie et la modification de l'adresse (numéro de série, type de lecteur) ne peuvent être effectuées que dans le masque de saisie Définir l'entrée.
Définitions du signal	... le paramétrage des signaux d'entrée ou de sortie a été modifié
Groupes d'autorisation	... modification des groupes d'autorisation sans modèle horaire, ou d'ajout ou de suppression d'un nouveau modèle horaire.
Données du personnel	... modification ou d'ajout de données du personnel, ou de modification des groupes d'autorisation d'accès ou des modèles horaires.
Redémarrage complet de la configuration, y compris du service LAC	.. réalisation de la configuration initiale d'Access PE. Une réinitialisation du contrôleur peut également nécessiter le téléchargement de la configuration complète vers les contrôleurs.
Redémarrage du service LAC	... modification de l'intervalle d'invitation ou de l'heure d'enregistrement du fichier des données de gestion du temps de travail dans les paramètres généraux.
Arrêt du service LAC	Cette option doit uniquement être utilisée dans des circonstances exceptionnelles, par exemple, au cours de la désinstallation pour éviter un redémarrage de l'ordinateur.

Le Configurateur envoie une commande au **service LAC** pour transmettre les données de configuration aux contrôleurs. Le service LAC gère la communication en direction et en provenance des contrôleurs. Ce programme est configuré au moment de l'installation en tant que Service Windows qui se lance automatiquement au démarrage de l'ordinateur. La réussite de la transmission au service LAC est signalée de la manière suivante :



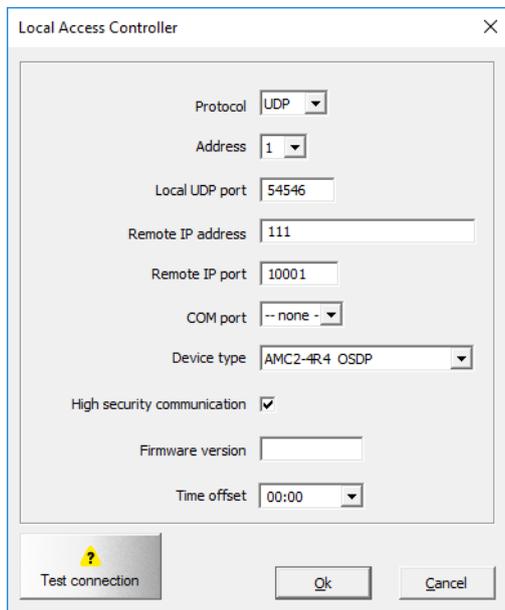
## 4 Contrôleurs

Les contrôleurs d'accès locaux (LAC) sont les points d'Access PE dans lesquels la plupart des décisions relatives au contrôle d'accès sont prises. À l'exception des fonctions de commande applicables à l'ensemble du système, telles que la vérification des séquences d'accès, les contrôleurs peuvent prendre des décisions de manière indépendante concernant les personnes auxquelles l'accès est accordé. C'est pour cette raison qu'ils disposent de toutes les données liées à l'accès dans leur propre mémoire. Cela permet ainsi d'effectuer des opérations hors ligne dont l'usage est limité et restreint.

Access PE utilise les contrôleurs d'accès modulaire AMC2 (Access Modular Controller).

### 4.1 Définition et modification de nouveaux contrôleurs

Les boutons  (ajouter) et  (modifier un élément de liste sélectionné) appellent une boîte de dialogue qui permet de configurer les interfaces entre le Serveur d'Access PE et les contrôleurs



Local Access Controller

Protocol: UDP

Address: 1

Local UDP port: 54546

Remote IP address: 111

Remote IP port: 10001

COM port: -- none --

Device type: AMC2-4R4 OSDP

High security communication:

Firmware version:

Time offset: 00:00

Buttons: Test connection, Ok, Cancel



#### Remarque!

La case à cocher High security communication (Communication de haute sécurité) s'affiche sous Device type (Type de dispositif).

Avant de changer de type de dispositif, veuillez à désactiver préalablement cette case.

Un protocole doit être attribué à chaque contrôleur. Le tableau ci-après présente les paramètres disponibles :

- COM** Connexion via une interface série (COM) nécessitant le numéro d'interface COM (COMx).
- CIP** Connexion via TCP/IP par l'intermédiaire d'un COM nécessitant le numéro d'interface virtuel COM (COMx). Uniquement disponible pour les contrôleurs LACi équipés d'un transducteur IP/série.

**UDP** Connexion via UDP nécessitant le port UDP local et l'adresse IP (ou le nom du réseau sous DHCP).



**Remarque!**

Lorsque vous utilisez des interfaces CIP ou UDP, vérifiez que le commutateur DIL d'adresse sur le contrôleur à la position **5** est réglé sur **MARCHE**.

Selon le protocole choisi, différents paramètres supplémentaires seront nécessaires, tel qu'indiqué dans le tableau suivant :

Para- mètre	COM	CIP	UDP	Remarque
Adresse	1 à 8	1 à 8	toujours 1	Lorsque vous utilisez le protocole COM ou CIP, le commutateur DIL sur les contrôleurs doit avoir le même paramètre d'adresse.
Port UDP local	Désactivé	Désactivé	con sécutif	Le port par lequel le serveur d'Access PE recevra les données transmises par le contrôleur. Un nouveau contrôleur recevra le prochain port disponible selon sa position, mais cette valeur peut être écrasée.
Adresse IP distante	Désactivé	Désactivé	Adresse IP ou nom de réseau	Pour les réseaux avec DHCP, le nom de réseau doit être utilisé. Dans les autres cas, l'adresse IP du contrôleur doit être utilisée.
Port IP distant	Désactivé	Désactivé	valeur non modifiable = 10001	Le port du contrôleur qui recevra les

Para- mètre	COM	CIP	UDP	Remarque
				données provenant du serveur.
Port COM	Liste déroulante des ports COM	Liste déroulante des ports COM	<aucun>	Le numéro du port COM sur le serveur d'Access PE auquel le contrôleur est connecté.
Type de LAC	Liste déroulante des contrôleurs	Liste déroulante des contrôleurs	Liste déroulante des contrôleurs	Les types de contrôleur suivants sont disponibles :
	<b>AMC-4W Wiegand</b>			avec interface lecteur Wiegand
	<b>AMC2-2W Wiegand</b>			avec interface lecteur RS485 et Wiegand
	<b>AMC-4R4-BG900</b>			avec interface lecteur RS485
	<b>AMC-4R4-L-BUS</b>			avec interface lecteur RS485
<b>AMC-4R4-OSDP</b>			avec interface lecteur RS485	
Communication haute sécurité	Case pour la sélection d'un chiffrement spécifique à un contrôleur, basé sur une session, avec AES 128 entre un <b>hôte et un contrôleur</b> .			
Version de firmware (Projet)	aucune	aucune	aucune	Peut servir à indiquer la version du logiciel
Décalage horaire	<p>Zone permettant d'indiquer le décalage horaire avec le serveur lorsque l'AMC est situé dans un fuseau horaire différent.</p> <p>Les valeurs possibles sont comprises entre -12h et +12h par intervalles de 30 minutes.</p> <p>Toutes les heures transmises depuis le serveur vers l'AMC (ou inversement) s'ajustent en fonction du décalage horaire indiqué ici. Les heures locales de l'AMC sont utilisées dans les messages des événements et peuvent être consultées dans le Journal des événements.</p>			

### Test du contrôleur (LAC)

Une fois les paramètres configurés, vous pouvez tester la disponibilité de chaque contrôleur avant de les enregistrer. Cela permet d'identifier et de corriger ou de compléter rapidement tout paramètre incorrect.

Le bouton **Test LAC (Tester le LAC)** situé dans la partie inférieure de la boîte de dialogue permet de tenter d'établir une connexion avec le contrôleur en utilisant les paramètres actuellement définis. Une fois le contrôleur configuré, ce test peut également être exécuté en sélectionnant ce dernier dans la liste, puis en cliquant sur le bouton .

Le test affiche l'un des quatre résultats à l'aide des icônes ci-dessous qui apparaissent également dans la première colonne de la liste.



Le contrôleur n'a pas encore été testé ou il n'est pas activé.



Le test a réussi. Une connexion a été établie.



Le test a échoué.



L'état est encore en attente.



#### Remarque!

Ces icônes indiquent l'état actuel et elles sont automatiquement mises à jour. Les tentatives de reconnexion peuvent retarder l'affichage de la mise à jour d'état.

Un test de contrôleur se compose de différentes étapes dont certaines peuvent être ignorées :

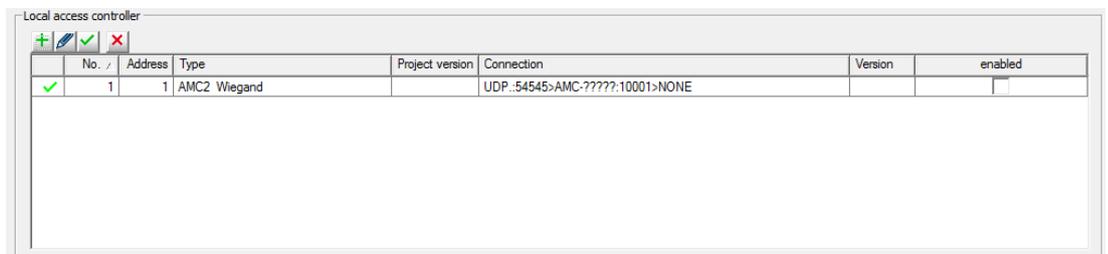
- Démarrage des services LAC.
- Téléchargement du programme LAC
- États d'attente :
  - Lire les données de configuration à partir du contrôleur.
  - Recevoir un message d'état de la part du contrôleur
- Afficher le résultat de la tentative de connexion.

En fonction du résultat, la boîte de dialogue **État du service LAC** peut s'afficher. Lorsque vous cliquez sur **OK**, le résultat du test s'affiche dans la liste.

## 4.2 Paramètres du contrôleur



La boîte de dialogue **Paramètres généraux**, appelée par le bouton , permet de définir et de configurer les contrôleurs d'accès locaux (LAC).



Les boutons permettant d'activer les fonctions suivantes s'affichent en haut de la liste :



**Ajouter** un nouveau contrôleur.



**Modifier** le contrôleur sélectionné.

**Tester** le contrôleur sélectionné.**Supprimer** le contrôleur sélectionné.

La liste contient tous les contrôleurs créés et présente les informations suivantes :

Colonne	Contenu	Description
	 ,  ,  ou 	Résultat du test du LAC : négatif, pas encore testé ou réussi
Non	1 à 128	Numéro du contrôleur.
Adresse	1 à 8	L'adresse configurée pour le contrôleur, telle qu'elle est définie par le commutateur DIL. Dans le cas d'un protocole UDP, il s'agit toujours de 1.
Type	AMC-Wiegand AMC-4R4 BG900 AMC-4R4 L-Bus AMC-4R4 OSDP AMC2-2W	Type du contrôleur sélectionné.
Version du projet	Exemple : 37.50	Version du programme pour le projet chargée par le contrôleur.
Connexion	Exemple : UDP : 54545 > AMC- DEMO : 10001 > AUCUN	Paramètres d'interface : Protocole : local UDP- Port (Port UDP local) > Network name or IP-Address (Nom du réseau ou adresse IP) : Remote IP-Port (Port IP distant) > COM-Port (Port COM)
Version	Exemple : 37.02	Version du programme chargée par le contrôleur.
Enabled (Activé)	Activé ou désactivé	Si la case à cocher est désactivée, le service LAC ne définira pas une connexion à

Colonne	Contenu	Description
		AMC2. AMC2 fonctionnera en mode autonome.

La partie inférieure de la boîte de dialogue contient les paramètres généraux pour l'ensemble des périphériques et applications de l'installation Access PE.

**Remarque!**

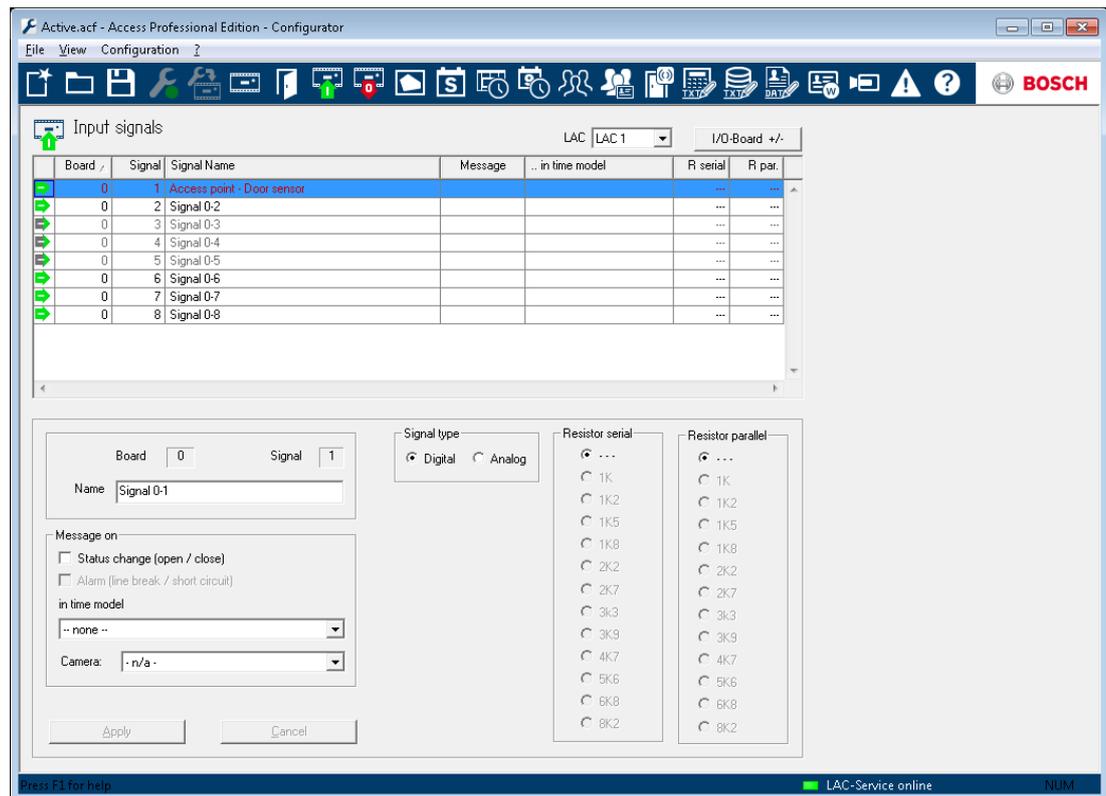
Après une installation ou une mise à jour, la case à cocher **Enabled (Activé)** doit être sélectionnée pour activer l'AMC2 sélectionné.

## 5 Signaux

Les signaux d'entrée et de sortie des contrôleurs peuvent être utilisés, par exemple, pour déterminer l'état des portes et les commander. En outre, ces signaux peuvent également être utilisés pour associer des fonctions de commande aux demandes d'accès. Cela vous permet de commander et d'activer les caméras, les dispositifs de signalisation optiques ou acoustiques, ainsi que les systèmes d'alarme.

### 5.1 Signaux d'entrée

Tandis que les commandes des portes et les autres signaux de commande, de même que les messages d'état, sont configurés sous **Entrées**, la boîte de dialogue **Signaux d'entrée** concerne les définitions détaillées des types de signaux et leur surveillance.



Lorsque cette boîte de dialogue est appelée, le premier contrôleur est toujours affiché. Veuillez utiliser la zone **LAC** et la numérotation correspondante pour sélectionner le contrôleur souhaité. Le processus standard pour la définition d'un contrôleur crée 8 signaux d'entrée et 8 signaux de sortie. Si le contrôleur est capable de gérer davantage de signaux, vous pouvez utiliser le bouton **Cartes E/S +/-** pour créer d'autres signaux.

Tous les signaux définis apparaissent dans la liste. Les paramètres de chaque signal sont indiqués dans les différentes colonnes de la liste, ainsi que dans les paramètres de contrôle du signal sélectionné qui sont affichés sous la liste. Tous les paramètres peuvent être définis à partir de la liste et des paramètres de contrôle figurant sous la liste, tel qu'il est indiqué dans le tableau ci-dessous.

Colonne	Paramètre	Description
1 (pas de nom)	-	Décrit l'état du signal :  = Signal activé  = Signal désactivé Double-cliquez sur l'icône pour basculer d'un état à l'autre
Circuit imprimé	Circuit imprimé	Numéro de la carte sur laquelle est situé le signal. 0 = carte de base 1 = carte d'extension Ce paramètre ne peut pas être modifié
Signal	Signal	Numéro du signal sur la carte (1 à 16). Ce paramètre ne peut pas être modifié
Nom du signal	Nom	Nom du signal. Dans les paramètres standard, un nom est attribué à chaque signal selon le modèle : Signal <N° de la carte>-<N° du signal> L'utilisateur peut double-cliquer dans cette colonne pour modifier le nom.
Message	Message activé... Modification de l'état (ouvrir/fermer) :  Alarme :	Affichage graphique du réglage du paramètre dans la liste :   (uniquement possible pour le type de signal <b>Analogique</b> ) Double-cliquez dans cette colonne pour parcourir les icônes du message.
	Caméra	Vous pouvez attribuer une caméra figurant dans la liste de sélection à certains signaux d'entrée. Lorsque le signal correspondant est activé, un message de journal est créé ; vous pouvez également utiliser ce message pour extraire les images de la caméra.

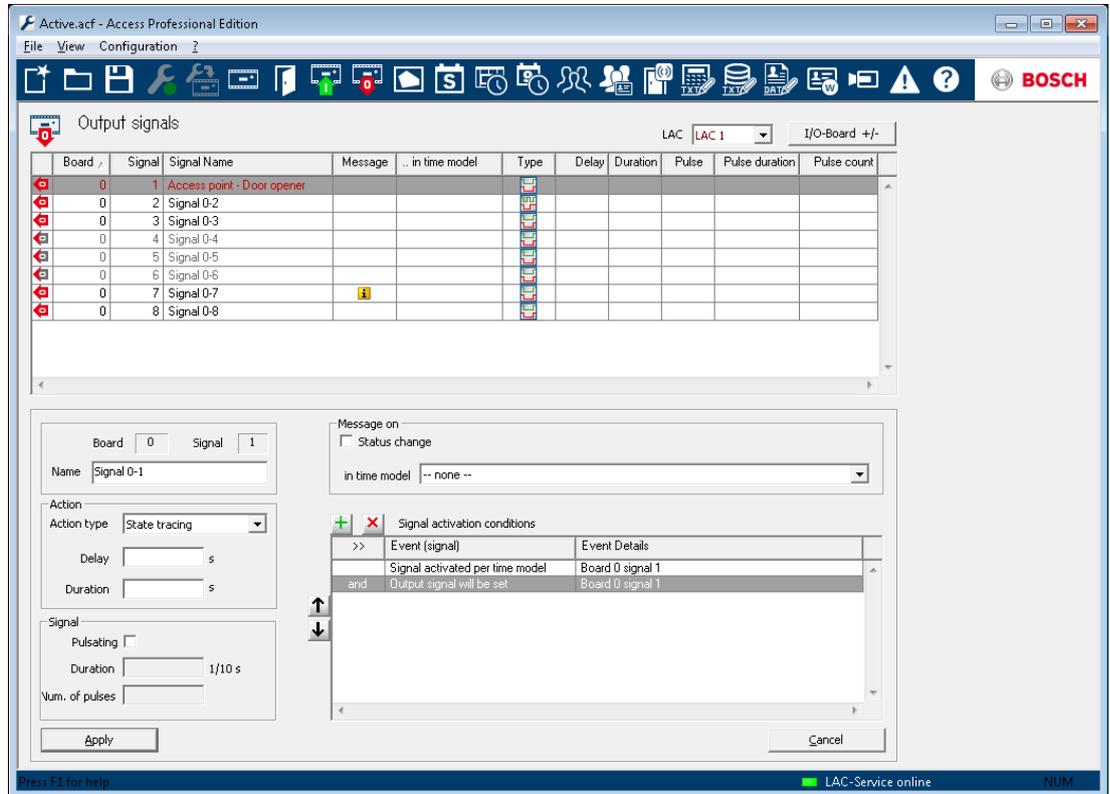
Colonne	Paramètre	Description
- Seulement dans le modèle horaire...	Pendant le modèle horaire	Indique le modèle horaire sélectionné. L'utilisateur peut double-cliquer dans cette colonne pour sélectionner un modèle horaire dans une liste
<aucun>	Type de signal Numérique Analogique	L'option <b>Analogique</b> active les cases d'option permettant de sélectionner les valeurs de résistance.
R série	Résistance série	Double-cliquez dans cette colonne pour ouvrir la liste des valeurs de résistance.
R par.	Résistance parallèle	Lorsque vous sélectionnez une résistance série ou parallèle, le type de signal se réinitialise automatiquement sur Analogique.

**Remarque!**

Les valeurs figurant dans la liste ne peuvent pas toutes être associées. Le manuel d'installation du périphérique AMC2 contient des informations sur les paires de résistance compatibles.

## 5.2 Signaux de sortie

Cette boîte de dialogue est utilisée pour paramétrer les signaux de sortie et, le cas échéant, pour définir des cartes de signal supplémentaires.



Lorsque cette boîte de dialogue est appelée, le premier contrôleur est toujours affiché. Veuillez utiliser la zone de liste **LAC** et la numérotation correspondante pour sélectionner le contrôleur de votre choix. Le processus standard pour la définition d'un contrôleur crée 8 signaux d'entrée et 8 signaux de sortie. Si le contrôleur est capable de gérer davantage de signaux, vous pouvez utiliser le bouton **Cartes E/S +/-** pour créer d'autres signaux. Tous les signaux définis apparaissent dans la liste. Les paramètres de chaque signal sont indiqués dans les différentes colonnes de la liste, ainsi que dans les paramètres de contrôle du signal sélectionné qui sont affichés sous la liste. Tous les paramètres peuvent être définis à partir de la liste et des paramètres de contrôle figurant sous la liste, tel qu'il est indiqué dans le tableau ci-dessous.

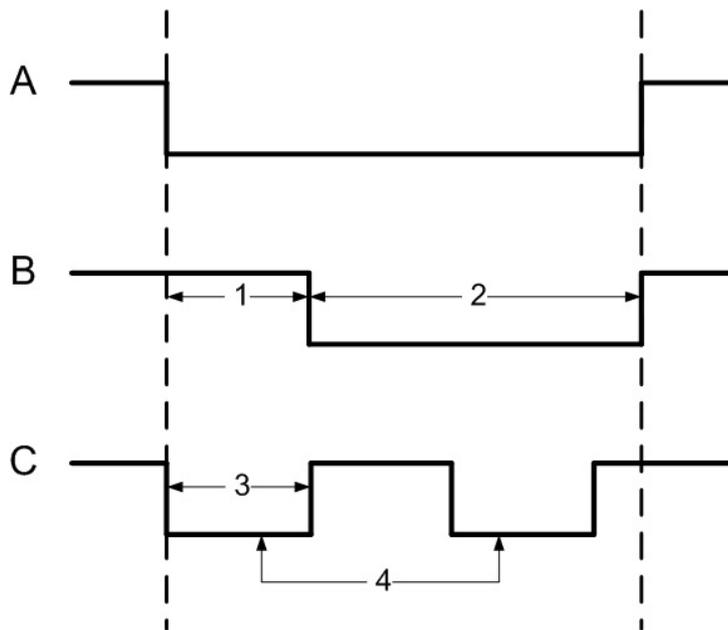
Outre les paramètres décrits dans cette section, vous pouvez définir des **conditions** supplémentaires qui doivent être remplies pour activer le signal de sortie.

Colonne	Paramètre	Description
1 (pas de nom)	-	Décrit l'état du signal : = Signal activé = Signal désactivé Double-cliquez sur l'icône pour basculer d'un état à l'autre.
Circuit imprimé	Connexion	Numéro de la carte sur laquelle est situé le signal. 0 = carte de base 1 = carte d'extension Ce paramètre ne peut pas être modifié.
Signal		Numéro du signal sur la carte (1 à 16).

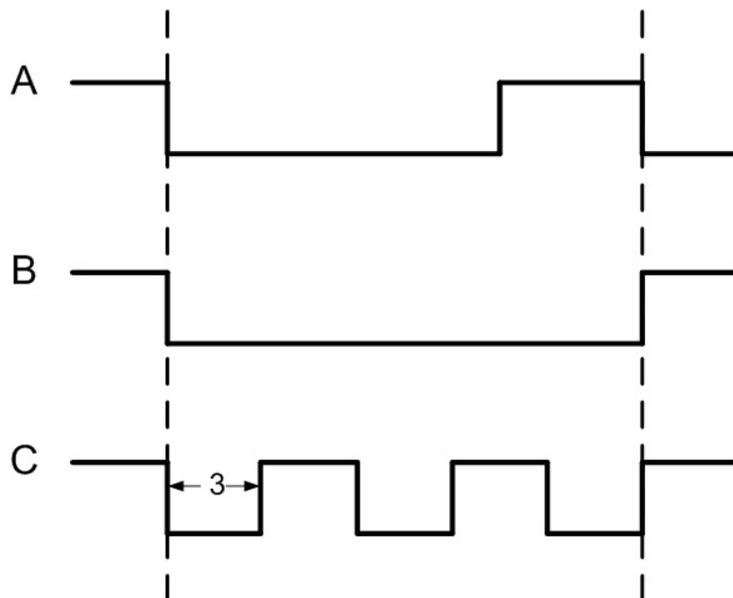
Colonne	Paramètre	Description
		Ce paramètre ne peut pas être modifié.
Nom du signal	Nom	Nom du signal. Dans les paramètres standard, un nom est attribué à chaque signal selon le modèle : Signal <N° de la carte>-<N° du signal> Les signaux définis et activés à partir de la boîte de dialogue <b>Définir l'entrée</b> sont affichés ici, accompagnés du nom de leur entrée et de leur description. L'utilisateur peut double-cliquer dans cette colonne pour modifier le nom.
Message	Message activé... Modification de l'état	Affichage graphique du réglage du paramètre dans la liste :  Double-cliquez dans cette colonne pour activer ou désactiver le paramètre.
- Seulement dans le modèle horaire...	Pendant le modèle horaire	Affichage et sélection du modèle horaire.
Type	Type d'action : Temporisé Suivre l'état Basculer	Trois types d'actions sont disponibles :    Double-cliquez dans cette colonne pour passer d'un type d'action à un autre dans l'ordre indiqué ici.
Retard	Retard	Délai en secondes avant la transmission du signal [0 - 9999].
Durée	Durée	Délai en secondes avant la transmission du signal [0 - 9999 ; 0 = toujours ou jusqu'à interruption par un message d'annulation].

Colonne	Paramètre	Description
Impulsion	Pulsée	Active la transmission des impulsions. Dans le cas contraire, le signal est transmis en continu. Lorsque vous double-cliquez sur cette option, l'option est activée, mais est signalée comme non définie par l'icône  tant que la durée et le nombre d'impulsions n'ont pas été configurés. Une fois ces données configurées, l'option est signalée par l'icône  .
Durée d'impulsion	Durée	Durée de l'impulsion.
Total d'impulsions	Nombre d'impulsions	Nombre d'impulsions par seconde.

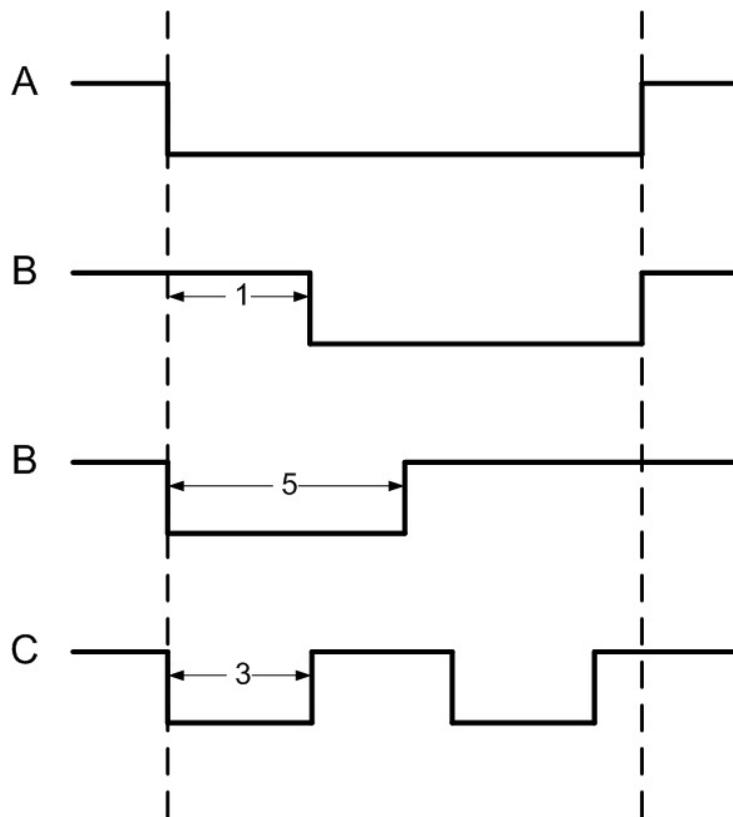
**Type d'action : temporisé**



**Type d'action : basculer**



**Type d'action: suivre l'état**



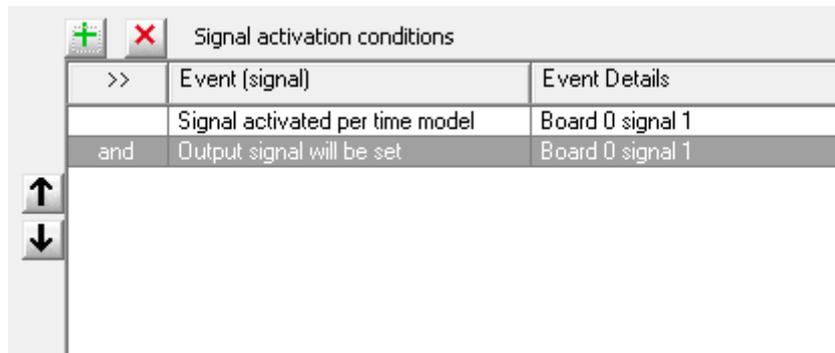
A =	état de l'invitation
B =	régulier
C =	par impulsion
1 =	délai d'attente
2 =	période d'action

3 =	durée de l'impulsion
4 =	total d'impulsions (= 2)
5 =	Durée d'activation maximum

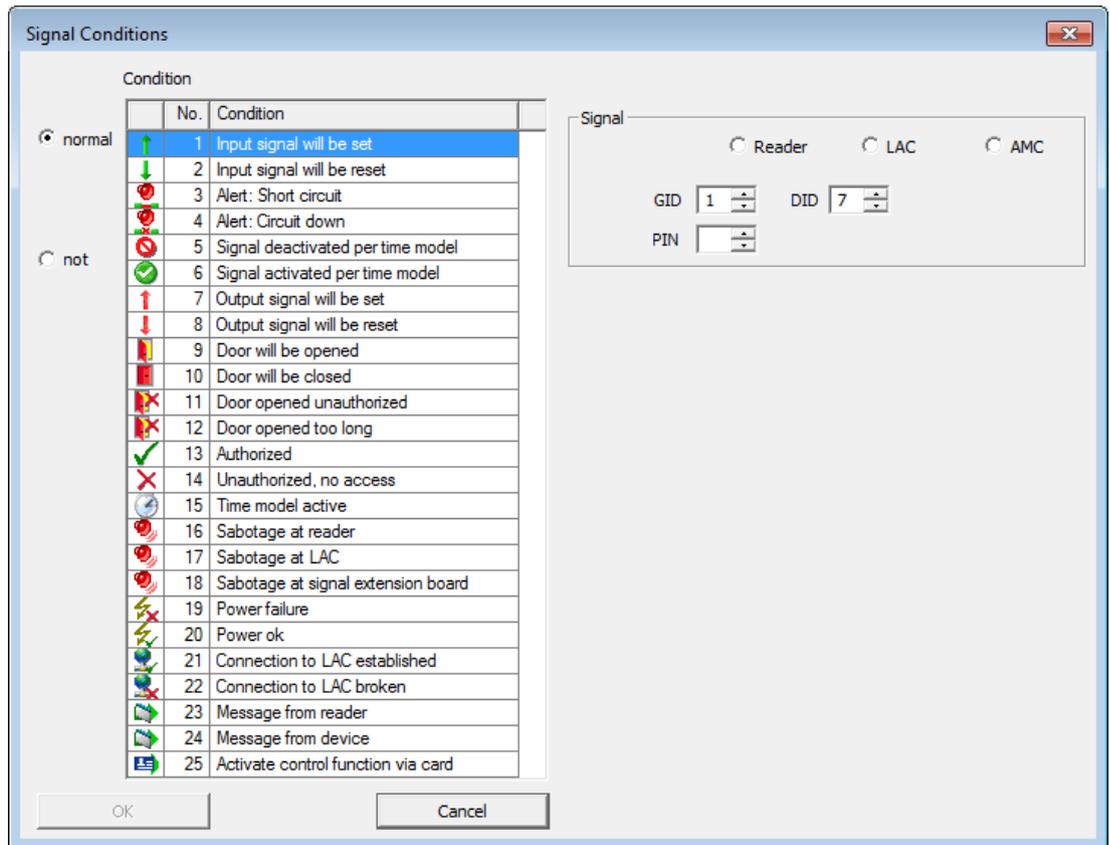
### 5.3 Définition des conditions pour les signaux de sortie

La boîte de dialogue **Signaux de sortie** propose, en plus des paramètres, une option pour définir des conditions supplémentaires qui permettent la transmission des signaux de sortie uniquement dans des circonstances précises.

La configuration de ces conditions spéciales pour les signaux sélectionnés dans la liste principale s'effectue dans la zone inférieure droite de la boîte de dialogue.



Appuyez sur le bouton  pour ouvrir la boîte de dialogue ci-dessous. Vous pouvez utiliser cette boîte de dialogue pour configurer les conditions appropriées.



En fonction de la condition d'activation sélectionnée, il peut être nécessaire de saisir des informations complémentaires, telles que le nom du lecteur de la porte, avant de pouvoir confirmer la boîte de dialogue en cliquant sur **OK**.

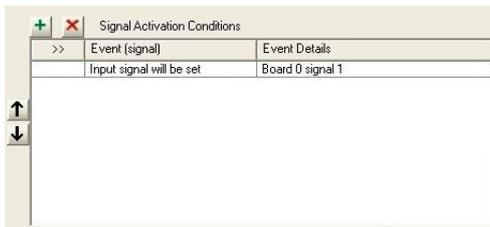
Vous pouvez appliquer le nombre de conditions de votre choix à chaque signal. Vous devez ouvrir à nouveau la boîte de dialogue pour configurer chaque nouvelle condition en appuyant sur le bouton .



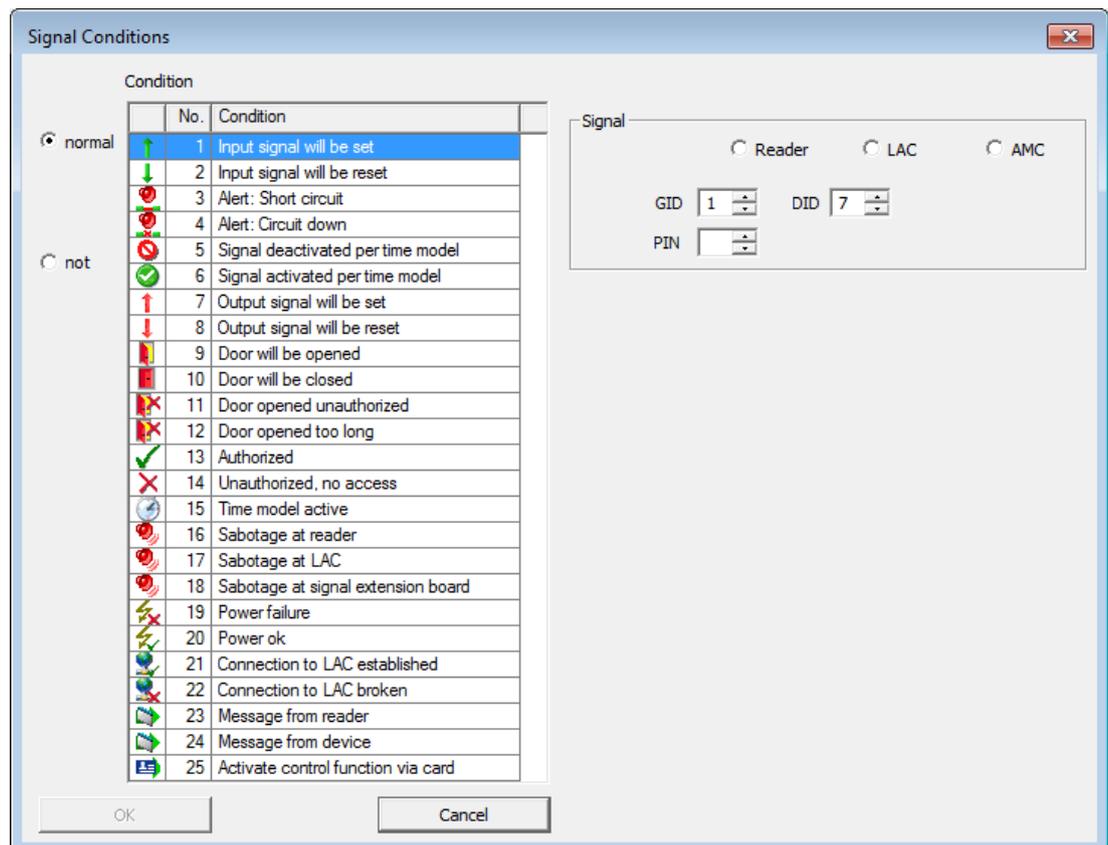
### Remarque!

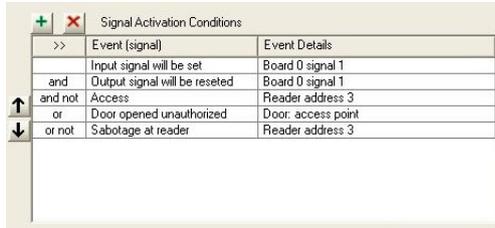
Vous pouvez uniquement sélectionner les signaux et installations (entrées, lecteurs, portes) qui sont connectés au contrôleur pour lequel vous êtes en train de paramétrer le signal de sortie.

Lorsque vous configurez la condition, vous avez le choix entre les modes **normal** (si la condition doit être remplie) et **non** (si la condition ne doit pas être remplie).



Les conditions suivantes sont configurées en fonction de la première condition définie en sélectionnant l'un des opérateurs **et**, **et non**, **ou** ou encore **ou non**.

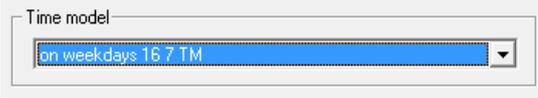
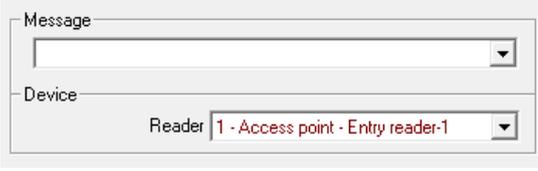
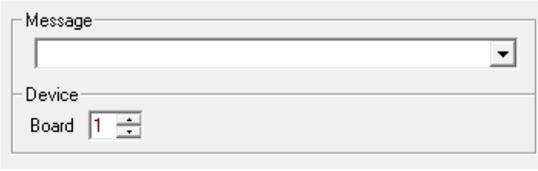
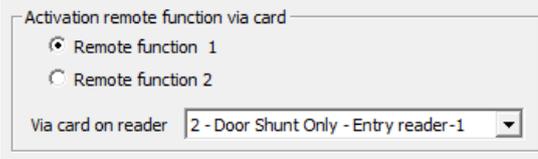




Les conditions sont traitées dans l'ordre dans lequel elles apparaissent dans la liste. Si cet ordre ne correspond pas à la procédure requise, vous pouvez modifier l'emplacement des conditions dans la liste. Dans la liste, sélectionnez la condition à déplacer, puis placez-la à l'endroit voulu en cliquant sur ↑ ou sur le bouton ↓.

**Les informations complémentaires requises pour chaque condition sont indiquées dans le tableau suivant :**

Condition	Informations complémentaires requises
Le signal d'entrée va être paramétré	Informations sur le type de périphérique sur lequel est situé le signal.
Le signal d'entrée est défini	Sélection de la carte. Sélection de la connexion.
Alerte : court-circuit	
Alerte : connexion interrompue	
Signal désactivé par modèle horaire	
Signal activé par modèle horaire	
Le signal de sortie va être paramétré	
Le signal de sortie va être réinitialisé	
La porte va être ouverte	
La porte va être fermée	L'IDG (ID de groupe) est automatiquement définie.
Ouverture de la porte non autorisée	
Porte ouverte trop longtemps	
Accès	Sélection du lecteur.
Non autorisé, pas d'accès	
Modèle horaire activé	

Condition	Informations complémentaires requises
	
Sabotage sur le lecteur	Sélection du lecteur. 
Sabotage sur le LAC	Aucune information complémentaire requise.
Sabotage sur la carte d'extension du signal	Sélection de la carte. 
Coupure de courant	Aucune information complémentaire requise.
Alimentation en fonctionnement	
Connexion LAC -> APE établie	
Connexion LAC -> APE interrompue	
Message du lecteur	Sélection du message dans la liste prédéfinie. Sélection du lecteur. 
Message du périphérique	Sélection du message dans la liste prédéfinie. Sélection de la carte. 
Activer la fonction de contrôle avec une carte	Définissez une sortie basée sur une autorisation accordée à un détenteur de carte. Voir le chapitre <b>Activer la fonction de contrôle avec une carte</b> . 

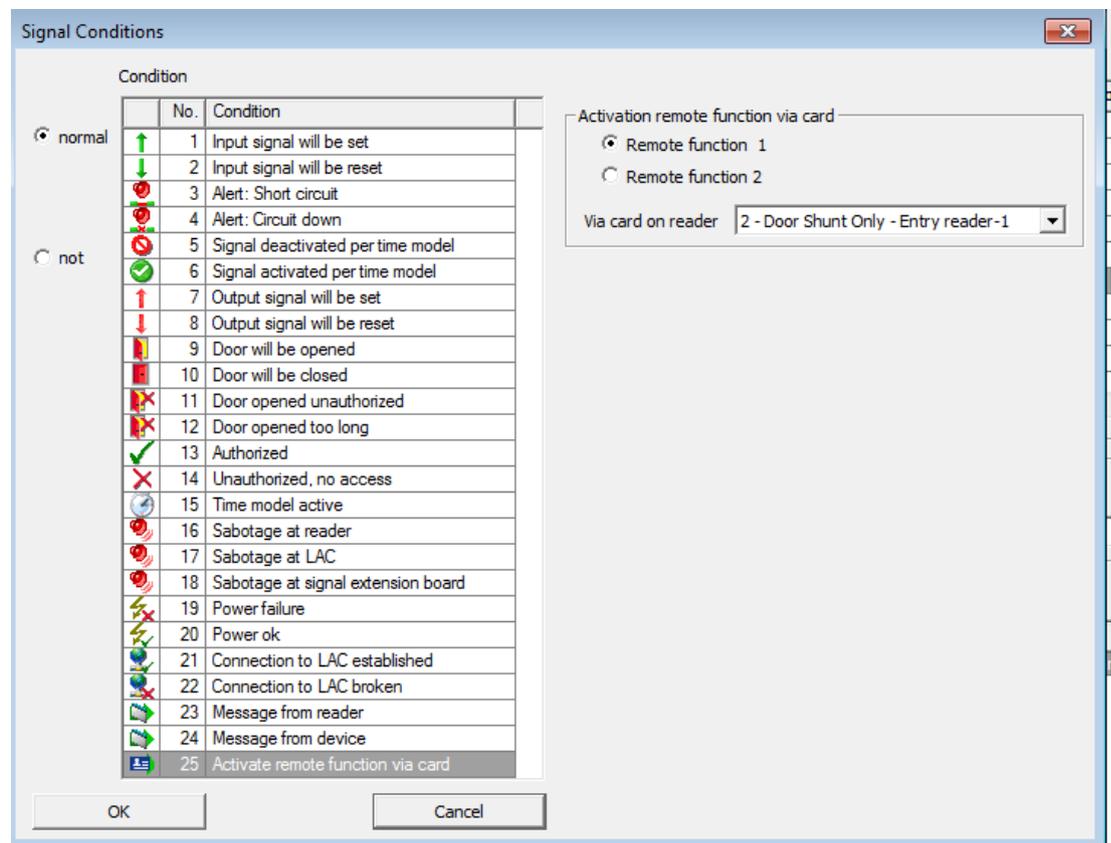
### 5.3.1

#### Activer la fonction de contrôle avec une carte

Cette fonction de contrôle permet à une personne de déclencher deux signaux de sortie différents.

Pour utiliser cette option, il est nécessaire de remplir les exigences suivantes :

- Une personne avec le droit d'activer les fonctions de contrôle doit être configurée.
- Leurs cartes doivent être valides et autoriser l'accès à l'entrée.
- Sous **Signal conditions (Conditions de signal)**, le signal de sortie **25 - Activate remote function via card (25 - Activer une fonction à distance via une carte)** doit être sélectionnée.
- La fonction à distance doit être sélectionnée et un lecteur de carte doit être attribué.



#### Procédure :

- Présentez la carte au lecteur. L'autorisation de la personne est vérifiée.
- Si l'autorisation est effective, le signal de sortie est défini comme configuré.

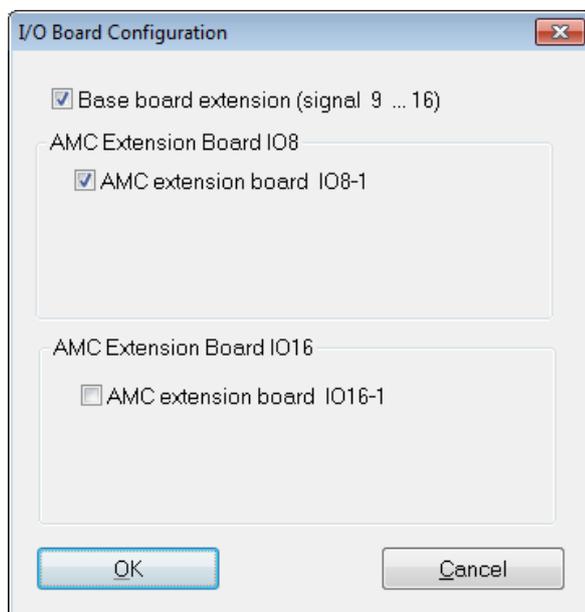
## 5.4 Création de cartes d'extension

Vous pouvez configurer des cartes d'extension dans les boîtes de dialogue à la fois pour les **signaux d'entrée** et les **signaux de sortie**. Les paramètres définis dans une boîte de dialogue seront activés dans l'autre boîte de dialogue.

Vous pouvez utiliser et configurer trois types de cartes d'extension dans le système de contrôle d'accès d'Access PE. La configuration de ces trois types s'effectue via l'une des boîtes de dialogue consacrées aux signaux.

- **AMC2 4W-EXT** – Pour étendre les interfaces d'un Wiegand AMC (AMC2 4W)
- **AMC2 8I-8O-EXT** - 8 signaux supplémentaires chacun
- **AMC2 16I-16O-EXT** - 16 signaux supplémentaires chacun

Veillez sélectionner le contrôleur de votre choix dans la zone de liste **LAC** située au-dessus de la fenêtre de la liste. Ces contrôleurs sont créés avec 8 signaux sur la carte principale (=0). Pour créer la carte d'extension, cliquez sur le bouton intitulé **Carte E/S +/-**. La boîte de dialogue suivante s'affiche alors :



Les paramètres suivants peuvent être configurés en cochant une ou deux des cases proposées :

- **Carte principale AMC** (signaux 9 à 16)  
Crée une carte d'extension Wiegand **AMC2 4W-EXT**.  
Cette carte est dotée des mêmes interfaces qu'un contrôleur AMC2-4W (4 interfaces lecteur Wiegand, 8 signaux d'entrée et 8 signaux de sortie). Cependant, elle ne peut pas fonctionner de manière indépendante et doit être connectée à un contrôleur AMC2-4W.  
**Cette extension peut uniquement être utilisée avec un contrôleur AMC2-4W.**  
Un AMC2 4W-EXT peut être configuré avec **3** cartes d'E/S supplémentaires.  
Dans la liste des signaux d'entrée et de sortie, la carte d'extension, comme le contrôleur lui-même, reçoit le numéro de carte 0 et les signaux numérotés de 9 à 16.
- **Carte d'extension AMC IO8**  
Carte dotée de 8 signaux d'entrée et de 8 signaux de sortie comme extension des interfaces du contrôleur.  
Cette carte peut être connectée à n'importe quel contrôleur AMC2. Lorsqu'elle est utilisée avec un contrôleur AMC2-4W, elle peut également être associée à une carte d'extension Wiegand AMC2 4W-EXT

Dans la liste des signaux d'entrée/sortie, la carte d'extension est créée avec le numéro de carte 1 et les signaux numérotés de 1 à 8.

– **Carte d'extension AMC IO16**

Carte dotée de 16 signaux d'entrée et de 16 signaux de sortie comme extension des interfaces propres à un contrôleur.

Cette carte peut être connectée à n'importe quel contrôleur AMC2. Lorsqu'elle est utilisée avec un contrôleur AMC2-4W, elle peut également être associée à une carte d'extension Wiegand AMC2 4W-EXT

Dans la liste des signaux d'entrée/sortie, la carte d'extension est créée avec le numéro de carte 1 et les signaux numérotés de 1 à 16.



**Remarque!**

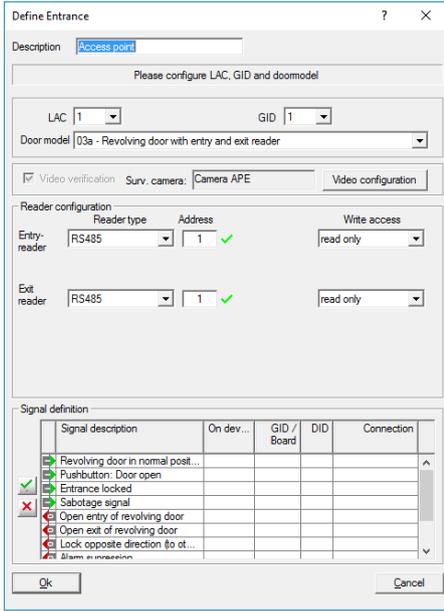
Les paramètres définis ici pour les **cartes E/S** s'appliquent aussi bien aux signaux d'entrée qu'aux signaux de sortie et peuvent être configurés indifféremment dans l'une des deux boîtes de dialogue.

## 6 Entrées

Lorsque le terme « entrées » est utilisé, il s'agit toujours d'un ensemble comportant plusieurs composants appartenant à un système de contrôle d'accès. En plus de la porte (qui peut également être un tourniquet, un sas de sécurité, une barrière ou un ascenseur), le système inclut également un ou plusieurs lecteurs et éventuellement des boutons et des unités de contrôle (pênes, verrouillages du moteur, etc.). Le système peut également contenir des dispositifs de signalisation optiques ou acoustiques ou des caméras qui exercent des fonctions de commande supplémentaires.

### 6.1 Création et modification de modèles de portes

Vous pouvez définir une nouvelle entrée à l'aide du bouton  ou via le menu contextuel de la liste (cliquez avec le bouton droit de la souris, puis sélectionnez **Nouvelle entrée**). Vous pouvez modifier le nom de l'entrée, le modèle de porte ou les adresses de périphérique de la porte sélectionnée en cliquant sur le bouton , en double-cliquant sur l'élément ou là encore via le menu contextuel (cliquez avec le bouton droit de la souris, puis sélectionnez **Modifier l'entrée**).



Signal description	On dev...	GID / Board	DID	Connection
Revolving door in normal posit...				
Pushbutton: Door open				
Entrance locked				
Sabotage signal				
Open entry of revolving door				
Open exit of revolving door				
Lock opposite direction to ct...				
Alarm in installation				

Lorsque vous définissez une nouvelle entrée, vous devez lui attribuer un nom. Ce nom doit être unique et aussi explicite que possible, car il sera utilisé pour définir les groupes d'autorisation et les droits d'accès individuels dans la Gestion du personnel.

Vous devez également sélectionner le numéro du contrôleur auquel l'entrée est connectée, ainsi que l'ID de groupe (IDG). En règle générale, seul le numéro du contrôleur nécessite une intervention de votre part, car Access PE attribue automatiquement l'IDG libre suivante. Vous devez sélectionner un modèle de porte approprié dans la zone de liste **Modèle de porte**. Veuillez consulter l'annexe pour obtenir un tableau répertoriant les modèles de porte prédéfinis et leurs fonctionnalités.

En fonction du modèle de porte sélectionné, des listes déroulantes s'affichent pour les lecteurs d'entrée et de sortie dans lesquelles vous devez sélectionner les types de lecteurs. Une adresse unique doit être attribuée à chaque lecteur au sein du contrôleur auquel il est

attribué. Pour les lecteurs dotés d'une interface **Wiegand**, seul le **numéro de l'interface de leur contrôleur** est requis. Pour les lecteurs dotés d'une interface **RS485**, l'**adresse DIP** attribuée est indispensable.



### Remarque!

Veillez vérifier que les adresses du lecteur correspondent aux périphériques réellement installés.

Vous pouvez connecter jusqu'à quatre lecteurs de type **AMC-Wiegand** et huit lecteurs de type **AMC-RS485** et **LACi**.

### Utilisation de l'adresse de lecteur 9 :

L'adresse de lecteur 9 a été paramétrée pour faciliter la configuration et sert de mémoire tampon lorsque les paramètres sont ajustés. Si vous avez attribué toutes les adresses de lecteur d'un contrôleur, mais qu'il vous reste des paramètres à ajuster, vous pouvez déplacer temporairement un lecteur sur l'adresse 9 pour libérer une autre adresse.

**Exemple :** vous souhaitez intervertir les lecteurs 4 et 7. Comme vous ne pouvez pas utiliser deux fois la même adresse, commencez par attribuer l'adresse 9 au lecteur 4. Ensuite, déplacez le lecteur 7 sur l'adresse 4. Pour terminer, déplacez le lecteur 9 (c'est-à-dire le lecteur 4 initial) sur l'adresse 7.

### Définition du signal

Une fois le modèle de porte sélectionné, tous les signaux d'entrée et de sortie possibles s'affichent dans la liste. Pour appeler la boîte de dialogue permettant de définir les signaux, sélectionnez l'un des éléments de la liste, puis cliquez sur le bouton  à gauche de la liste ou double-cliquez sur l'élément de la liste.



Le signal sélectionné dans la liste s'affiche en guise de repère. L'effet du signal est défini dans les paramètres par défaut des contrôleurs paramétrés, mais peut être modifié ici si nécessaire.

Les autres éléments affichés sont la carte à partir de laquelle le signal est émis, ainsi que le numéro de l'interface du signal. Pour obtenir la liste des signaux sur le contrôleur ou une carte d'extension, veuillez consulter le manuel d'installation du périphérique concerné.



### Remarque!

Demandez au technicien ayant effectué l'installation de vous fournir un plan de câblage/une liste des signaux qui vous permettra de paramétrer en conséquence les signaux sous Access PE.

De mauvais raccordements au câblage du système peuvent entraîner de graves problèmes au niveau du contrôle des entrées et du bon fonctionnement de leurs signaux.

La boîte de dialogue vous propose de choisir entre une DCU (unité de contrôle des portes), un lecteur, un LAC ou un AMC. Si vous choisissez une DCU ou un lecteur, vous devrez alors saisir l'IDG et l>IDP du périphérique. Les règles suivantes s'appliquent ici :

- **Lecteur**
  - IDG = IDG du lecteur à l'entrée
  - IDP = 1 pour le premier lecteur d'**entrée**, = 2 pour le deuxième lecteur d'**entrée**, = 3 pour le premier lecteur de **sortie**, = 4 pour le deuxième lecteur de **sortie**

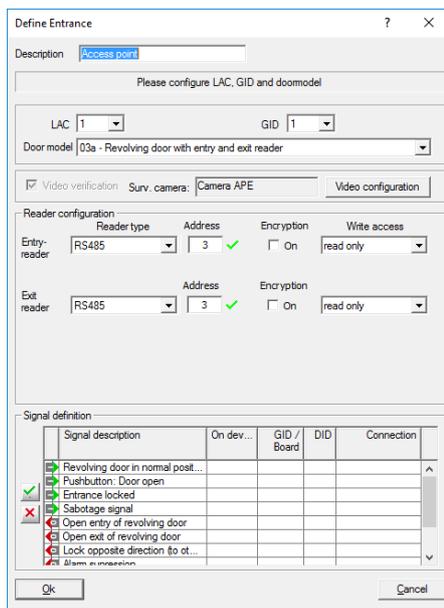
- N° du signal = signal sur le lecteur 1... 4
- **LAC**
  - N° du signal = signal sur le LAC 1... 16
- **AMC**
  - Sur la carte = N° de carte... 0 ou 1
  - N° du signal = signal sur le AMC 1... 8 ou, dans le cas de cartes d'extension, 1... 16

Dans la liste, les connexions paramétrées s'affichent dans leurs colonnes respectives. La première colonne contient des icônes représentant l'état des signaux :

	Signal d'entrée non défini
	Signal d'entrée défini
	Signal de sortie non défini
	Signal de sortie défini

Vous pouvez supprimer un signal précédemment défini en cliquant sur le bouton . L'exemple ci-dessus illustre la modification d'un modèle de porte à l'aide d'un lecteur **Wiegand**.

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



L'option **Chiffrement** n'est pas sélectionnée par défaut. Pour une utilisation avec des lecteurs **OSDPv2 sécurisés** pris en charge, sélectionnez l'option **Chiffrement** :



Lecteurs OSDP :

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

Les lecteurs OSDP suivants sont pris en charge :

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!**

Lorsque vous utilisez des cartes Mifare codées par Bosch avec un lecteur OSDP, il est essentiel de sélectionner le type de carte **Mifare (63 bits)** pour activer le codage Bosch.

Il n'est pas possible de connecter différentes familles de produit (par exemple, **LECTUS duo** ou **LECTUS secure**) avec un bus OSDP. Assurez-vous de configurer « encrypted » ou « unencrypted » sur un bus OSDP, mais pas les deux.

**Avertissement!**

ATTENTION ! REMARQUE IMPORTANTE !

Une clé est générée pour la transmission de données chiffrées au lecteur OSDP. Enregistrez ce fichier

d:...\BOSCH\Access Professional Edition\PE\cfg\Active.acf

de quelque manière que ce soit sur un lecteur local fiable.

Ce fichier est nécessaire pour la restauration d'une installation existante.

**Avertissement!**

Lorsque des **lecteurs OSDPv2s sécurisés** sont utilisés en mode sécurisé, ils ont besoin de la clé maître initiale.

Si cette clé maître est perdue, les lecteurs ne peuvent pas être reconfigurés avec une nouvelle clé maître !

Dans ce cas, tous les lecteurs doivent être réinitialisés à leur état de livraison par le support !

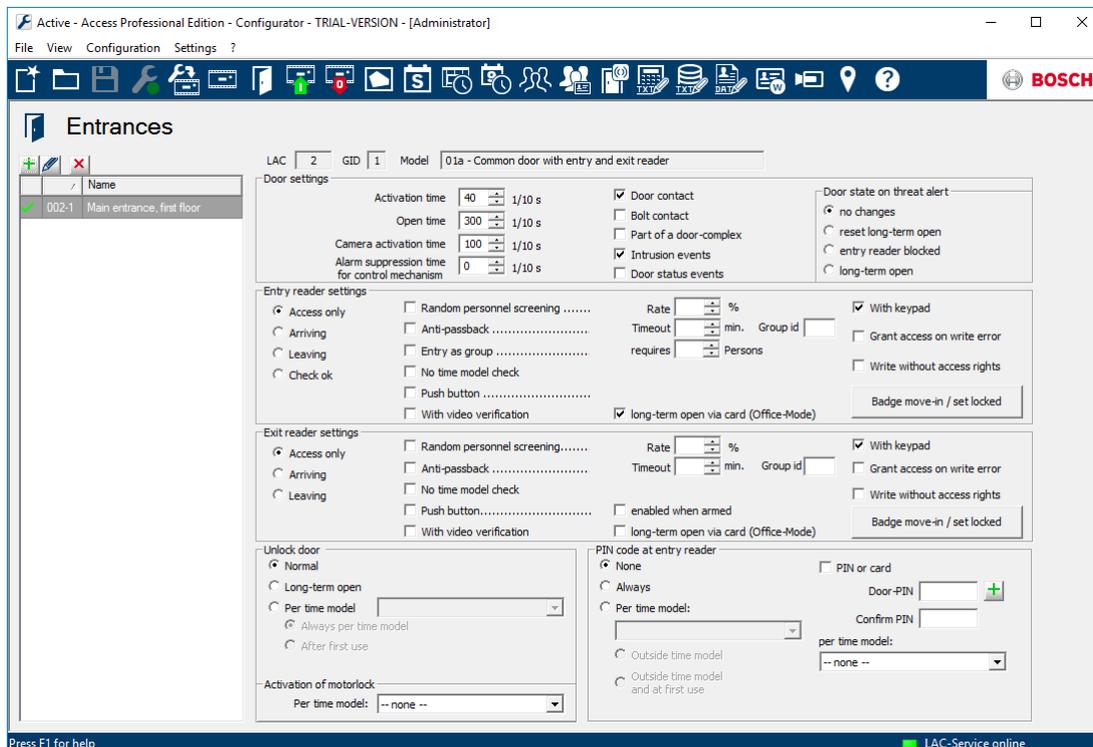
**Remarque!**

L'utilisation des lecteurs OSDP n'a pas été évaluée par UL.

Conséquences

## 6.2 Affichage et paramétrage

Toutes les entrées connues par le système s'affichent dans une liste sur le côté gauche. Lorsque vous cliquez sur l'une des entrées répertoriées dans la liste, les données correspondant à cette entrée s'affichent à droite dans les champs de paramètre.



Les boutons suivants se trouvent en haut de la liste :

-  **Ajouter** une entrée
-  **Modifier** une entrée.
-  **Supprimer** une entrée

Les connexions suivantes s'affichent en haut des champs de paramètre.

- LAC** Numéro séquentiel du contrôleur assigné à cette entrée.
- IDG** Numéro de groupe de cette entrée avec les porte(s) et lecteur(s) correspondants
- Modèle** Modèle et description de la porte.

Vous pouvez modifier ces éléments en cliquant sur le bouton  ou en double-cliquant sur une entrée dans la liste.

Les **paramètres de porte** suivants peuvent être configurés :

Paramètre de porte	Description
Heure d'activation en 1/10 s	Si aucun contact de cadre de porte n'a été configuré, l'ouvre-porte restera activé pendant la durée définie ici. Dans le cas contraire, l'ouvre-porte sera désactivé dès que le contact de cadre détectera l'ouverture de la porte. Valeur par défaut = 40
Durée d'ouverture en 1/10 s	Durée maximale pendant laquelle la porte peut rester ouverte avant d'envoyer le signal « Porte ouverte trop longtemps ». Valeur par défaut = 300
Durée d'activation de la caméra en 1/10 s	Si l'entrée est équipée d'une caméra de vidéosurveillance, celle-ci restera activée pendant la durée définie ici. Valeur par défaut = 100
Durée de suppression des alarmes pour le mécanisme de contrôle en 1/10 s	Durée de suppression des alarmes (réglage) avant l'activation de l'ouvre-porte. La durée de suppression des alarmes ne prend effet que si la durée définie est supérieure à 0. Valeur par défaut = 0
Contact de porte	Si la porte est équipée d'un contact de cadre, celui-ci peut être paramétré pour permettre de surveiller l'entrée des personnes. Dans le même temps, le signal destiné à activer l'ouvre-porte est désactivé si le contact de porte indique que la porte est ouverte. Ce signal sert également à contrôler <b>l'heure de suppression des alarmes</b> .
Contact de fond de pêne	Si la porte est équipée d'un capteur de contact de fond de pêne, celui-ci peut être paramétré pour indiquer si la porte est vraiment fermée.
Partie d'un ensemble de portes	Ce paramètre indique si la porte fait partie d'un sas, par exemple, un « sas de sécurité » ou une douche à air. Dans ce cas, les signaux du sas peuvent vérifier que les deux portes ne sont jamais ouvertes en même temps. Si une seule porte est définie dans le cadre d'un sas, la synchronisation est désactivée.
Événements d'intrusion	Vous pouvez définir ici si un signal doit être envoyé en cas d'ouverture de porte non autorisée. Un <b>contact de porte</b> doit être présent pour utiliser ce paramètre.
Événements concernant l'état de la porte	À condition que l'entrée soit équipée d'un <b>contact de porte</b> , le système peut être configuré pour signaler tout événement d'ouverture/fermeture.
État de la porte en alerte de menace	Configuration des états de porte pour une alerte de menace (voir le chapitre <i>Configuration des alertes de menace</i> )

Vous pouvez configurer les paramètres de lecteur suivants pour une entrée :

Paramètres du lecteur Lecteurs d'entrée et de sortie	Description
Accès uniquement	Le lecteur crée uniquement des événements d'accès généraux.

Paramètres du lecteur Lecteurs d'entrée et de sortie	Description
Arrivée	Lorsqu'une personne entre en utilisant ce lecteur de carte, un pointage <b>Heure &amp; présence (TA)</b> est effectué et la personne est enregistrée comme étant présente.
Départ	Lorsqu'une personne sort en utilisant ce lecteur de carte, un pointage <b>Heure &amp; présence (TA)</b> est effectué et la personne est enregistrée comme étant absente.
<p>Les pointages créés par les lecteurs configurés pour surveiller les heures de présence sont enregistrés quotidiennement dans un fichier situé dans le répertoire C:\Bosch\Access Professional Edition\PE\Data\Export (répertoire par défaut).</p> <p>Un fichier nommé <b>TA_&lt;Date actuelle AAAAMMJJ&gt;.dat</b> est créé et peut être modifié. Les champs sont séparés par un point-virgule et peuvent donc être édités dans des applications tierces de type tableur, par exemple.</p> <p>Chaque pointage enregistré contient les données suivantes :</p> <p>Nom ; Prénom ; Société ; N° du personnel ; N° de carte ; Champs supplémentaires 1-10 (si configurés) ; Nom de l'entrée ; Date (aaaammjj) ; Heure (hhmmss, avec l'ajout de la lettre « s » pour signaler l'heure d'été) ; Sens de passage exprimé sous forme numérique (1 = Arrivée, 2 = Départ) ; Sens de passage sous forme de texte (ENTRER, SORTIR)</p>	
Vérification OK	<p>Pour les <b>lecteurs d'entrée</b> uniquement.</p> <p>Ce paramètre permet de configurer un lecteur en tant que <b>lecteur de déblocage</b> destiné à débloquer les cartes du personnel ayant été sélectionné pour la <b>surveillance aléatoire</b>. Il est important de s'assurer qu'un lecteur de déblocage n'est pas simultanément configuré en tant que lecteur de surveillance qui sélectionne de manière aléatoire le personnel soumis à la surveillance.</p>
Surveillance aléatoire du personnel - Taux - %	<p>Ce paramètre permet de configurer un lecteur en tant que <b>lecteur de surveillance</b> qui sélectionne les cartes de manière aléatoire en vue de la <b>surveillance du personnel</b>.</p> <p>En plus de cocher la case, vous devez saisir un taux (pourcentage compris entre 1 et 99) pour la surveillance aléatoire. Si aucune valeur n'est saisie, toutes les cartes seront sélectionnées (surveillance 100 %).</p> <p>Il est important de s'assurer qu'un lecteur de surveillance n'est pas simultanément configuré en tant que lecteur de déblocage qui débloque les cartes bloquées par les lecteurs de surveillance.</p>
Anti-retour - Délai d'attente - ID de groupe	<p>Cette option permet de bloquer une carte pendant la durée spécifiée et empêche toute nouvelle entrée par le même passage, sauf lorsqu'une sortie a été enregistrée entre-temps. Cette mesure vise à éviter toute utilisation abusive des cartes en les passant à d'autres personnes par-dessus un tourniquet.</p> <p><b>Délai d'attente</b> indiqué en minutes et compris entre 1 et 480.</p>

Paramètres du lecteur Lecteurs d'entrée et de sortie	Description
	Plusieurs lecteurs peuvent être associés sous la forme d'un groupe. Un anti-retour est valable pour tous les lecteurs disposant du même <b>ID de groupe</b> . Valeurs possibles : 1 à 2 caractères compris entre 0 et 9 et/ou A et Z
Entrée en tant que groupe - Nombre de personnes requises	Pour les <b>lecteurs d'entrée</b> uniquement. Cette option accorde l'accès seulement après que le nombre de personnes indiqué ici appartenant à un groupe ont présenté leurs cartes. Valeurs possibles : 2 à 6
Avec clavier	Cochez cette case si le lecteur de porte est équipé d'un clavier
Aucune vérification du modèle horaire	Par défaut, les accès sont vérifiés en fonction des modèles horaires Ce comportement peut être contourné en configurant ce paramètre.
Transfert moteur	Cette option doit être activée lorsque le lecteur est équipé d'un mécanisme d'alimentation en cartes.
Bouton-poussoir - toujours activé	Ce paramètre permet la reconnaissance d'un signal pour l'ouverture de la porte. Ce signal peut provenir d'un bouton-poussoir ou d'un téléphone, par exemple, si aucun lecteur n'est disponible. <b>toujours activé</b> : si les paramètres par défaut sont configurés, le bouton-poussoir ne fonctionne pas lorsque le système de sécurité est activé. Cela signifie qu'il est impossible de quitter la zone surveillée. Avec cette option, le bouton-poussoir reste opérationnel même lorsqu'un système d'alarme est armé. Si vous appuyez sur le bouton, cette fonction comprend également un lecteur de sortie.
Avec vérification vidéo	Activez cette case à cocher si la vérification vidéo doit être activée.
Ouverture à long terme avec une carte (mode bureau)	Cette option 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 (voir le chapitre Mode bureau).



### Remarque!

Les contrôles dépassant la simple vérification des autorisations et modèles horaires (vérifications des séquences d'accès, vérifications anti-retour, surveillance aléatoire, par exemple) sont effectués par le processus du sous-système LAC. Pour que cette fonctionnalité soit disponible, le serveur d'Access PE doit fonctionner en continu (24h/24, 7j/7).

Vous pouvez configurer le **déverrouillage de l'entrée** à l'aide des paramètres suivants :

Type de déverrouillage de la porte	Description
Normal	La porte est verrouillée et s'ouvrira uniquement si une carte valide est présentée au lecteur.
À long terme	La porte reste ouverte pendant une période prolongée, par exemple, pendant les heures de clarté, ou tant qu'une personne est présente à la réception.
Par modèle horaire	Le déverrouillage à long terme de la porte peut être associé à un modèle horaire de différentes façons : <ul style="list-style-type: none"> <li>– <b>Toujours par modèle horaire</b> : la porte est déverrouillée pendant des heures de service définies.</li> <li>– <b>Après première utilisation</b> : après avoir été utilisée une première fois pendant les heures de service, la porte reste déverrouillée jusqu'à la fin de cette période.</li> <li>– <b>Activation via boîte de dialogue</b> : l'ouverture à long terme pendant les heures de service est régulée par un lecteur de boîte de dialogue spécial.</li> </ul>
Activation du verrouillage du moteur	Ce paramètre permet de configurer un modèle horaire pour gérer l'activation d'un verrouillage du moteur à l'entrée (généralement en dehors des heures d'ouverture habituelles).

**La saisie du code PIN** sur le lecteur peut être configurée de la manière suivante :

Code PIN	Description
Aucun	Aucun code PIN requis.
Toujours	Code PIN toujours requis.
Par modèle horaire	La saisie du code PIN varie en fonction du modèle horaire, selon l'une des options suivantes : <ul style="list-style-type: none"> <li>– <b>En dehors des heures normales</b> : la saisie d'un code PIN est requise en dehors des heures comprises dans le modèle horaire.</li> <li>– <b>En dehors des heures normales et lors de la première utilisation</b> : la saisie d'un code PIN est requise en dehors des heures comprises dans le modèle horaire et lorsqu'une personne franchit l'entrée pour la première fois.</li> </ul>
Code PIN ou carte	Si cette fonctionnalité est activée, la personne peut avoir accès en saisissant le code PIN de la porte ou à l'aide d'une carte.
Code PIN de la porte	Option pour la saisie du code PIN de la porte – entre 4 et 8 chiffres (Définition des paramètres – Paramètres système généraux)
Vérification	Saisissez une nouvelle fois le code PIN de la porte

Code PIN	Description
Par modèle horaire	L'option permettant de saisir un code PIN peut être limitée à des jours ou à des heures spécifiques de la journée via un modèle horaire.

**Remarque!**

Les codes **PIN d'identification** et **de la porte** ne peuvent pas être utilisés pour les modèles de porte avec armement du système de sécurité (MP 10 et 14).

**Remarque!**

L'accès groupe configuré au niveau d'un lecteur équipé d'un clavier n'est pas compatible avec la fonctionnalité Code pin ou carte.

**Voir aussi**

- *Configuration des alertes de menace, Page 101*

## 6.3 Mode Bureau

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 un badge valide au lecteur.

Pour que le mode Bureau fonctionne, il est nécessaire de remplir les exigences suivantes :

- 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.
- 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.

### Procédure :

- Appuyez sur la touche 3 du lecteur à clavier.
- Présentez la carte. L'autorisation de la personne est vérifiée.
- Si l'autorisation est accordée, la porte passe à l'état d'ouverture permanente.
- La porte change d'état à chaque exécution des étapes décrites.



### Remarque!

L'option mode Bureau n'ouvre pas une porte verrouillée.

Si le mode bureau est configuré pour une porte spécifique, aucun modèle d'heure ne doit être configuré pour cette porte.

## 6.4 Modèles de porte avec paramètres spéciaux

Modèles de porte avec paramètres spéciaux

Certains modèles de porte nécessitent des informations spéciales pour la configuration ou des modes d'utilisation particuliers.

### Modèle de porte 07 : ascenseur

Si ce modèle de porte est sélectionné, la boîte de dialogue est complétée par plusieurs champs permettant de configurer les étages.

Floors served by elevator

AMC 1/0

LAC signal	Floor description	Input at reader
0 - 1	1st floor	<input type="checkbox"/>
0 - 2	2nd floor	<input type="checkbox"/>
0 - 3	3rd floor	<input type="checkbox"/>
0 - 4	4th floor	<input type="checkbox"/>
0 - 5	Cafeteria	<input type="checkbox"/>
0 - 6	Server Room	<input type="checkbox"/>
0 - 7		<input type="checkbox"/>
0 - 8		<input type="checkbox"/>

Inclus, un lecteur AMC2 peut être utilisé pour 8 étages. Il est possible d'en accroître le nombre avec les conditions préalables suivantes :

- 64 étages avec Wiegand (AMC2 4W + AMC2 4W-EXT + 3 AMC2 16I-16O-EXT)
- 56 étages avec RS 485 (AMC2 4R4 + 3 AMC2 16I-16O-EXT)

Ces étages peuvent être affectés sous la forme d'autorisations d'accès.

#### Modèle de porte 14 : porte avec réarmement de l'IDS

La configuration de ce modèle de porte est identique à celle de tous les autres modèles, à ceci près que, en plus de l'autorisation d'accès à cette entrée, l'autorisation d'armer et de désarmer le système de sécurité (IDS) est également attribuée. Ces autorisations sont généralement affectées séparément.

## 6.5

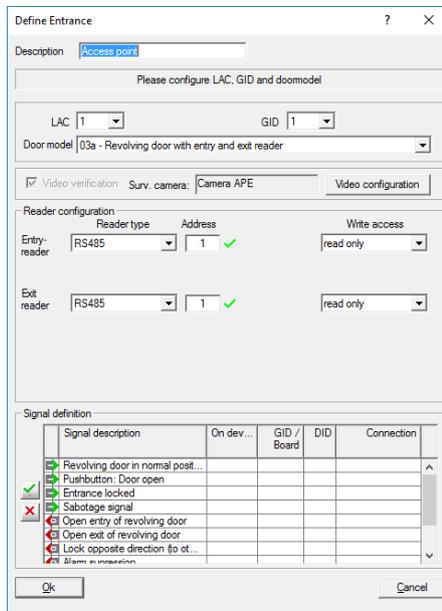
### Affectation de périphériques vidéo à une entrée

La boîte de dialogue de création d'une entrée offre également une option permettant de configurer des caméras pour cette entrée.

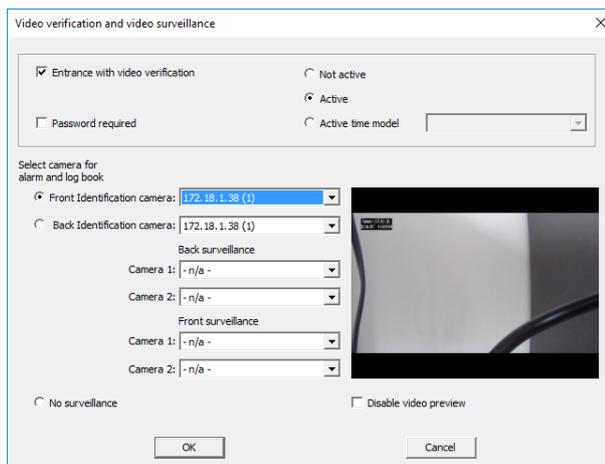
Pour activer et définir les options pour la **Vérification vidéo**, vous pouvez modifier et configurer d'autres paramètres dans une boîte de dialogue spéciale que vous pouvez ouvrir en appuyant sur le bouton **Configuration vidéo**. Procédez comme suit :

- Activez la case à cocher **Vérification vidéo** pour les lecteurs affectés à l'entrée.
- Cliquez sur  ou double-cliquez sur le LAC sélectionné sous **Entrées**.

L'écran suivant s'affiche :



Cliquez sur le bouton **Configuration de la vidéo** pour lancer l'écran de configuration :



## 7 Zones

La configuration des zones permet au système de localiser les personnes et de mettre en vigueur une séquence d'accès adaptée. De cette manière, vous pouvez empêcher les personnes d'entrer dans une zone précise en empruntant un trajet non autorisé. En règle générale, cette fonctionnalité est uniquement utilisée sur les sites ultra-sécurisés.

The screenshot shows the 'Areas configuration' window. On the left, a table lists defined zones:

	Area source	Area destination
00-00	-- outside --	-- outside --
00-01	-- outside --	inside
01-01	inside	inside
01-02	inside	Server Room

On the right, the 'Entrances' section includes a table for 'Entries to area' with columns for 'AM Entry' and 'AM Exit'. Below this table are navigation arrows. At the bottom right, the 'Area behaviour' section contains the following options:

- Enable area size limitation
- Generate area Full/Empty messages
- Enable automatic arming when area empty

There is also a dropdown menu for 'Select area arming output'.

Une liste des zones déjà définies s'affiche sur le côté gauche.

**Les boutons suivants se trouvent en haut de la liste :**



**Ajouter** une zone



**Modifier** une zone



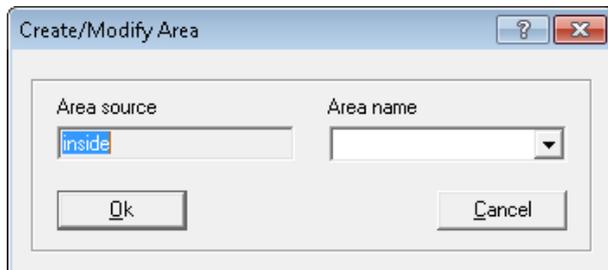
**Supprimer** une zone

Par défaut, le processus d'installation crée la zone **--extérieur--**. Aucune entrée ne peut être définie pour cette zone, car elle correspond à un espace non surveillé.

Vous pouvez maintenant définir d'autres zones à partir de cette zone pré-installée. Ces secteurs sont purement virtuels et ne doivent pas nécessairement correspondre à des zones réelles. Les zones peuvent être composées d'un ou de plusieurs bâtiments (par exemple, Area Company ACME Inc.), d'étages individuels ou même de salles individuelles.

**Remarque!**

Une nouvelle zone est toujours définie à partir d'une zone existante. La zone existante sélectionnée dans la liste devient automatiquement la **source de la zone** de la nouvelle zone. Ce paramètre par défaut ne peut pas être contourné. Il est donc important de sélectionner une **source de la zone** appropriée dans la liste lorsque vous créez une nouvelle zone.



Vous pouvez sélectionner le nom de la nouvelle zone dans la liste déroulante ou saisir un nouveau nom manuellement.

Les zones doivent être configurées de manière à ce qu'il soit effectivement possible de passer d'une source réelle à une destination réelle sans qu'il y ait de vide ou d'entrées manquantes entre les deux.

Exemple :

De la zone prédéfinie **--dehors--** une personne passe par l'entrée principale à la zone **Réception** ; de là aux bâtiments A, B ou C. C'est pour cela que les zones dans Access PE doivent être configurées afin que **Réception** soit la **source de la zone** pour les bâtiments A, B et C.

Après avoir créé une nouvelle zone, vous devez lui assigner au moins une entrée. Au moins un lecteur d'entrée est nécessaire pour pouvoir entrer dans la zone. Pour cela, deux listes sont affichées sur le côté droit de la boîte de dialogue.

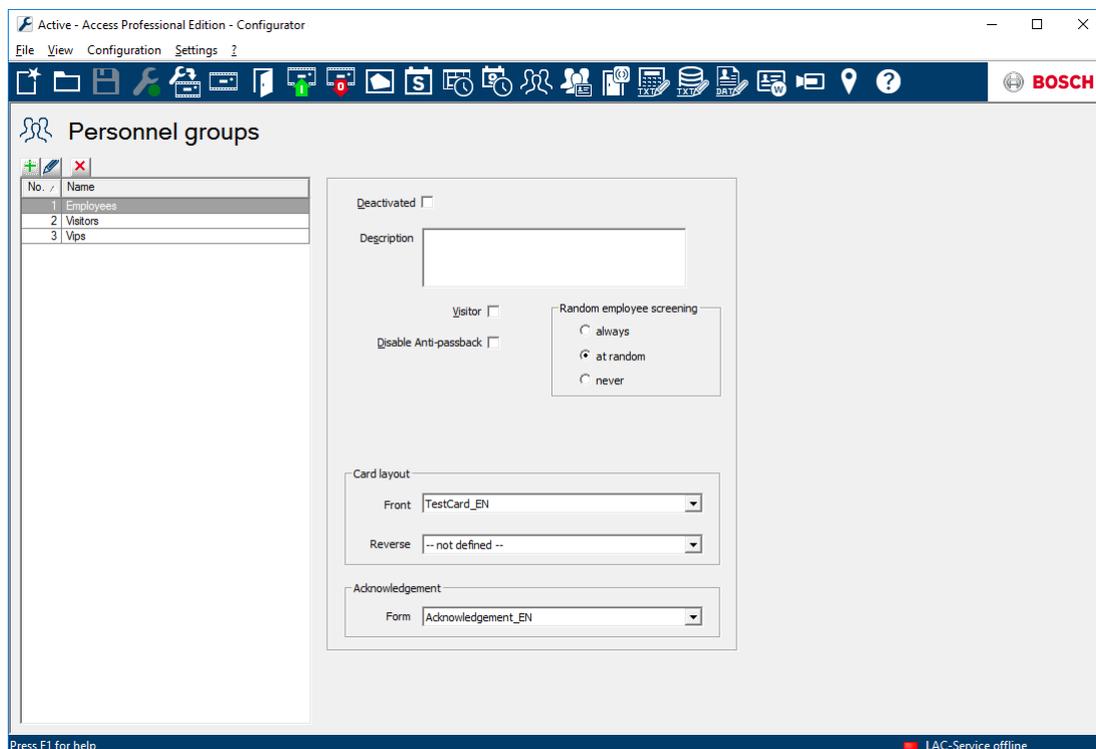






## 8 Groupes de personnel

Les groupes de personnel permettent d'organiser le personnel de votre société de manière logique. Par exemple, les personnes récemment créées dans le système peuvent hériter d'ensembles de droits d'utilisateur standard provenant de groupes de personnel prédéfinis.



La liste de tous les groupes de personnel précédemment définis s'affiche sur le côté gauche. Les boutons suivants se trouvent en haut de la liste :



**Ajouter** un nouveau groupe de personnel



**Modifier** le groupe de personnel sélectionné



**Supprimer** le groupe de personnel sélectionné

Deux groupes de personnel sont prédéfinis par défaut : **Employés** et **Visiteurs**. Ces groupes correspondent aux filtres par défaut dans l'application **Gestion du personnel** d'Access PE.



Il est donc possible de distinguer plusieurs types d'employés (par exemple, les employés de bureau, les ouvriers, le personnel de nettoyage) et d'affecter à ces groupes de personnel des ensembles de droits d'utilisateur standard dans la boîte de dialogue **Groupes d'autorisation**. À chaque fois qu'un nouvel employé est attribué à un groupe de personnel spécifique, il reçoit automatiquement les droits associés à ce groupe.

Vous pouvez définir les paramètres suivants, que vous trouverez à droite de la boîte de dialogue, pour le groupe de personnel sélectionné :

Réglages	Description
Désactivé	La désactivation constitue une phase de préparation à la suppression. Aucune personne ne peut être ajoutée au groupe, mais le groupe continue d'exister. <b>Vous ne devez pas supprimer un groupe de personnel tant que tous les membres n'ont pas été retirés du groupe.</b>
Description	Vous pouvez enregistrer une description détaillée pour chaque groupe de personnel.
Visiteur	Un groupe peut être classé comme appartenant à la catégorie Visiteur. L'application <b>Gestion du personnel</b> permet de filtrer des listes de personnes en fonction des catégories auxquelles elles appartiennent : <b>Toutes les personnes, Employés et Visiteurs.</b> Les groupes de personnel de la catégorie <b>Visiteurs</b> peuvent ainsi être visualisés indépendamment des groupes appartenant à la catégorie <b>Employés.</b>

Réglages	Description
Désactiver l'anti-retour	Un certain groupe de personnes (des VIP, par exemple) peuvent être exclues de l'anti-retour
Surveillance des employés : toujours aléatoire jamais	S'applique uniquement aux lecteurs configurés en tant que lecteurs de surveillance pour la surveillance aléatoire du personnel. Les trois options sont définies de la manière suivante. = le taux de pourcentage de surveillance est 100 % = ce groupe est surveillé de manière aléatoire selon le taux de pourcentage défini. = ce groupe n'est jamais surveillé
Disposition des badges Recto Retour	Il est nécessaire de définir au moins une disposition pour créer des cartes. Des dispositions peuvent être définies pour chaque groupe de personnel. La disposition du verso de la carte est facultative.
<b>Formulaire</b> d'accusé de réception	Si vous le souhaitez, les cartes peuvent être distribuées sous réserve de la signature d'un formulaire. Ces formulaires peuvent être conçus de manière à être spécifiques au groupe de personnel.

## 8.1 Accès groupe avec des lecteurs équipés d'un clavier

Comme décrit dans l'aide en ligne du navigateur de configuration, chaque lecteur de carte peut être configuré de manière à n'accorder l'accès qu'après qu'un certain nombre de cartes autorisées ont été présentées au lecteur. Cette fonctionnalité est appelée « accès groupe ». La procédure de l'accès groupe varie légèrement selon le type du lecteur de carte. Les lecteurs équipés d'un clavier autorisent plus que le nombre configuré de membres d'un groupe mais exigent une pression de touche supplémentaire pour confirmer que le groupe est complet.

### Lecteurs non équipés de clavier :

- Présentez le nombre exact de cartes autorisées au lecteur
- L'accès est accordé.

### Lecteurs équipés d'un clavier (sauf IBPR) :

- Présentez au moins le nombre de cartes autorisées configurés au lecteur
- Vous pouvez également présenter d'autres cartes
- Appuyez sur la touche Enter ou « # » du lecteur
- L'accès est accordé.

### Lecteurs IBPR équipés d'un clavier :

- Présentez au moins le nombre de cartes autorisées configurés au lecteur

- Vous pouvez également présenter d'autres cartes
- Appuyez sur la touche « 0 » du lecteur
- Appuyez sur la touche Enter ou « # » du lecteur
- L'accès est accordé.

## 8.2 Restrictions de l'accès groupe

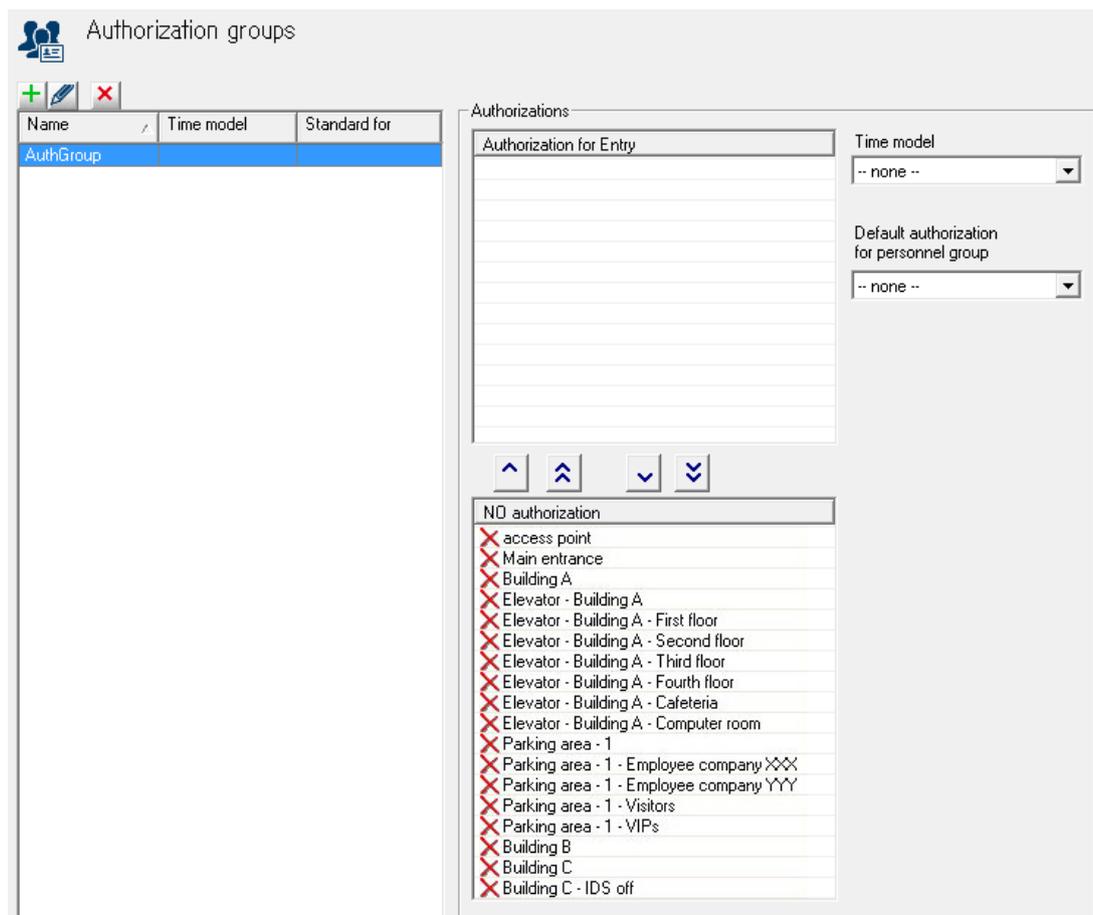
- L'accès groupe ne peut être configuré que pour les modèles de porte 1+3.
- L'accès groupe peut entraîner la présence d'un nombre de personnes plus important que le nombre autorisé dans la zone dans laquelle ils entrent, le comptage de la zone étant effectué une fois l'ensemble du groupe à l'intérieure de la zone.
- L'accès groupe et plusieurs cartes fonctionnent sur le modèle de comptage des cartes mais peut-être pas sur celui des personnes qui entrent.
- L'accès groupe configuré au niveau d'un lecteur équipé d'un clavier n'est pas compatible avec la fonctionnalité Code pin ou carte. (Chaque configuration requiert la même confirmation.)

## 9 Autorisations d'accès

Les groupes d'autorisation d'accès simplifient les tâches administratives de l'administrateur et de l'opérateur du système en regroupant un nombre illimité d'entrées individuelles ayant les mêmes conditions d'accès (groupe de personnes, restrictions horaires, etc.) ou proches/voisins au niveau géographique. Une seule étape est ensuite nécessaire pour affecter ces groupes à des personnes.

### 9.1 Création et affectation

Les **groupes d'autorisation** sont des regroupements logiques d'entrées. Les droits d'accès d'une personne dans l'application **Gestion du personnel** peuvent comporter un ou plusieurs groupes d'autorisation.



La liste de gauche répertorie tous les groupes d'autorisation définis jusqu'à présent  
Les boutons suivants se trouvent en haut de la liste :



**Ajouter** un groupe d'autorisation

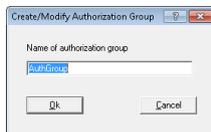


**Modifier** le groupe d'autorisation sélectionné.

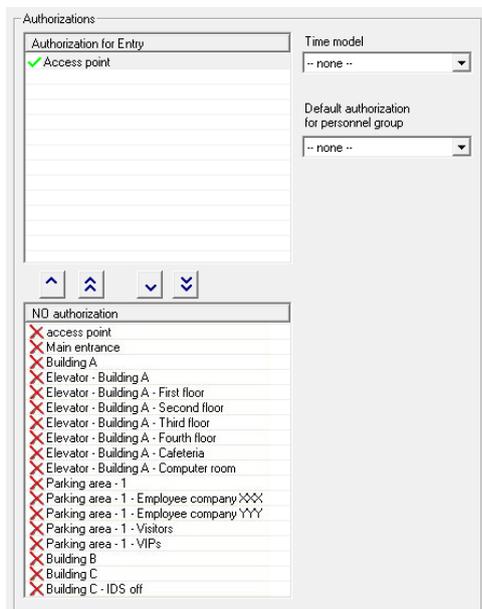


**Supprimer** le groupe d'autorisation sélectionné.

Le bouton  ouvre une boîte de dialogue permettant d'attribuer un nom à un nouveau groupe d'autorisation



Vous pouvez utiliser les listes de droite pour assigner des entrées au groupe d'autorisation sélectionné.



Les entrées figurant dans la liste **PAS d'autorisation** correspondent aux entrées disponibles, c'est-à-dire celles qui n'ont pas encore été assignées à un groupe d'autorisation. Double-cliquez sur l'entrée souhaitée, ou sur le bouton , pour assigner l'entrée au groupe d'autorisation actuellement sélectionné dans la liste de gauche. Le bouton  déplace toutes les entrées de la liste du bas vers la liste du haut. Inversement, double-cliquez sur la liste du haut ou utilisez les boutons  ou  pour annuler l'opération.



### Attention!

Les modifications suivantes apportées à l'assignation des entrées et des modèles horaires se répercutent sur les droits déjà accordés aux personnes.

Authorizations

Authorization for Entry

- ✓ Access point Delta Rdr
- ✓ 1st floor right
- ✓ 1st floor left
- ✓ garage

Time model

on weekdays 7-16 o'clock

Default authorization for personnel group

Employees

NO authorization

- ✗ Demo Suitcase Rdr 1
- ✗ Demo Suitcase Rdr 2
- ✗ Enrollment reader
- ✗ Enroll 1

Un **modèle horaire** qui limite les droits d'utilisateur peut être attribué à n'importe quel groupe d'autorisation ; voir **Utilisation des modèles horaires** (*Modèles horaires, Page 76*) dans Access PE.



#### Remarque!

Marquez les noms des groupes d'autorisation qui dépendent de modèles horaires, par exemple, à l'aide du préfixe ou du suffixe **MP**. Cela vous permettra de les distinguer plus facilement des ensembles de droits non restreints au moment d'affecter ces groupes dans l'application **Gestion du personnel**.

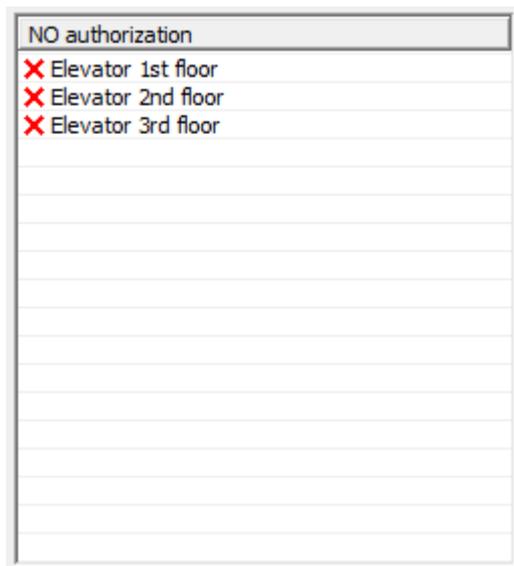
De plus, vous pouvez affecter le groupe d'autorisation comme **autorisation par défaut** pour un **groupe de personnel** (par exemple, employés ou visiteurs). De cette manière, lorsque vous créez une nouvelle personne dans l'application **Gestion du personnel**, les autorisations adéquates seront affectées en fonction du groupe de personnel auquel appartient la personne.

## 9.2 Droits spéciaux

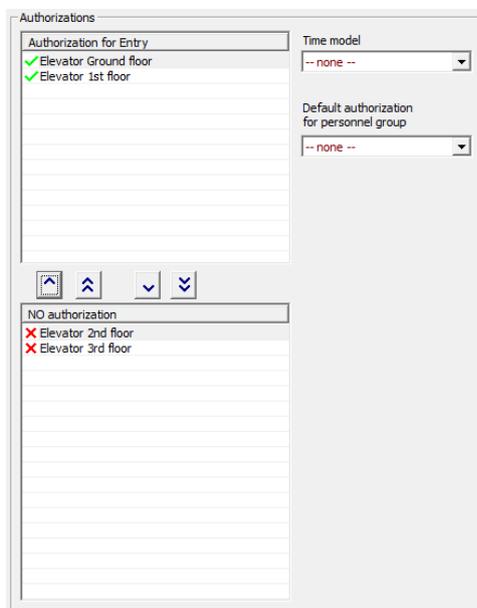
La **configuration** des modèles de porte 07 et 14 requiert des informations supplémentaires (*Modèles de porte avec paramètres spéciaux, Page 54*). Toutefois, la façon dont ils sont affectés et utilisés les distingue également des autres modèles de porte.

### Modèle de porte 07 : ascenseur

La liste des droits disponibles contient un élément distinct pour l'ascenseur, ainsi que pour chaque étage.

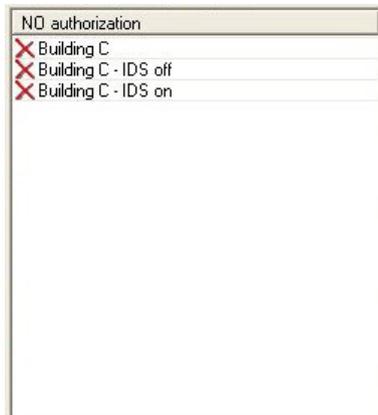


Lorsque vous créez des groupes d'autorisation, vous devez affecter un lecteur pour **l'ascenseur**, ainsi qu'**au moins un étage**.

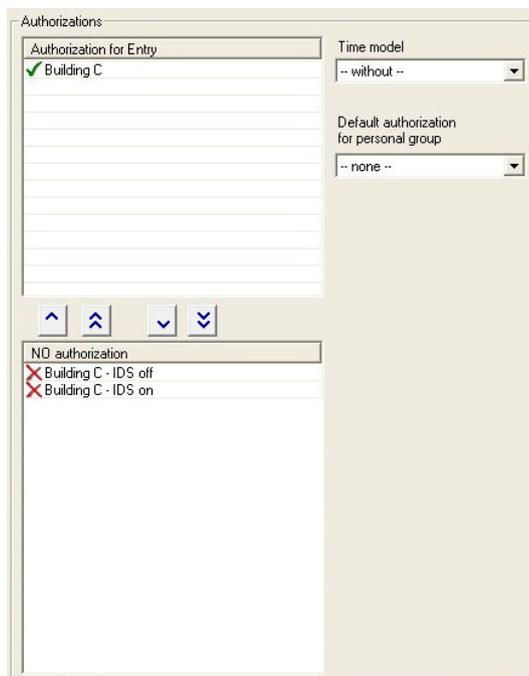


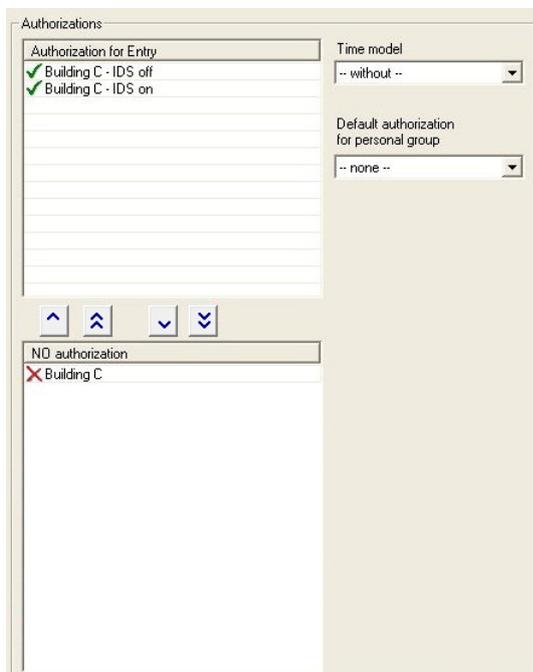
### Modèle de porte 14 : réarmement de l'IDS

La liste des droits disponibles contient un élément distinct pour l'entrée, ainsi qu'un pour l'armement et un autre pour le désarmement du système.



Ces deux types de droits sont affectés indépendamment l'un de l'autre. Si le détenteur de la carte dispose uniquement des droits d'accès pour une entrée particulière, il ne peut pas armer ou désarmer l'IDS (système de détection d'intrusion) depuis cette dernière. Inversement, si le détenteur de la carte dispose uniquement des droits d'armement/désarmement à une entrée particulière, il ne peut pas passer par cette entrée.





## 10 Jours spéciaux

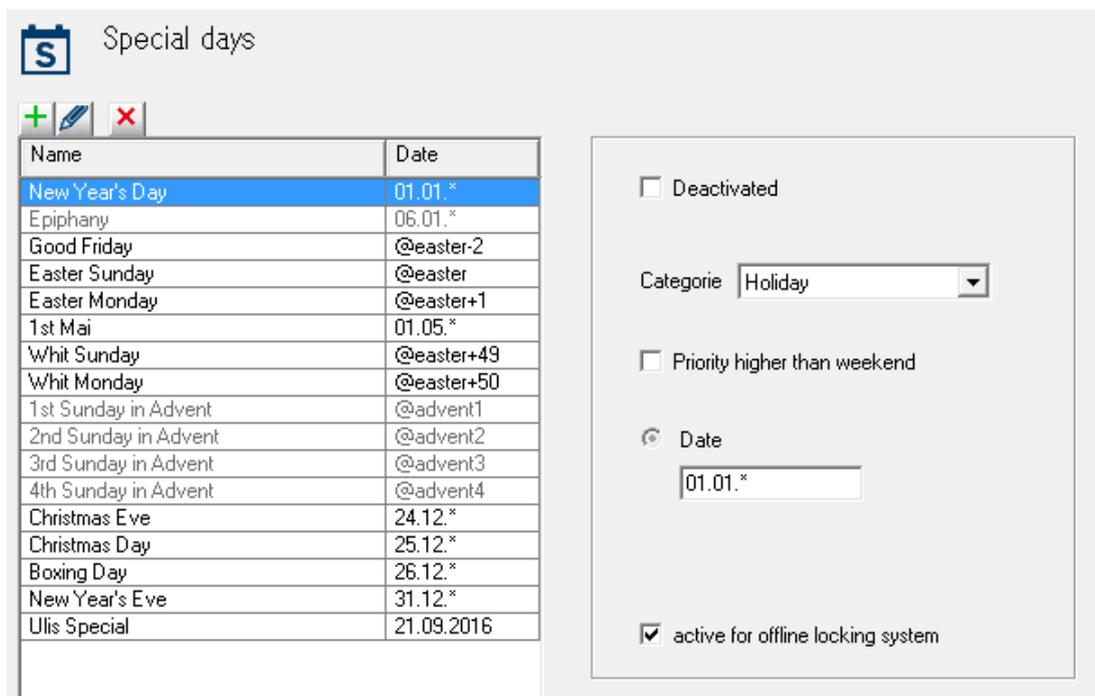
Les jours spéciaux définis dans cette boîte de dialogue ont des restrictions différentes en fonction du jour de la semaine sur lequel ils tombent. Les modèles horaires pour les congés et les jours spéciaux sont prioritaires par rapport aux modèles horaires appliqués au même jour de la semaine en temps ordinaire.

Vous pouvez modifier, réduire ou agrandir à votre guise la liste prédéfinie des jours spéciaux. Vous pouvez désactiver ou supprimer les congés qui ne sont pas nécessaires. Dans ce cas, le modèle horaire appliqué au jour de la semaine normal redevient prioritaire. Vous pouvez définir et ajouter à votre guise des jours qui ne figurent pas dans la liste ou qui sont spécifiques au client.

Cela permet de réduire la taille des calendriers : les jours spéciaux récurrents sont reportés d'une année sur l'autre, et seuls les exceptions et les événements non réguliers doivent être spécifiquement définis pour l'année.

### 10.1 Création et modification

Un certain nombre de congés classiques sont définis dans Access PE. Vous devez les modifier, en ajouter ou les désactiver en fonction de votre situation géographique.



**Special days**

Name	Date
New Year's Day	01.01.*
Epiphany	06.01.*
Good Friday	@easter-2
Easter Sunday	@easter
Easter Monday	@easter+1
1st Mai	01.05.*
Whit Sunday	@easter+49
Whit Monday	@easter+50
1st Sunday in Advent	@advent1
2nd Sunday in Advent	@advent2
3rd Sunday in Advent	@advent3
4th Sunday in Advent	@advent4
Christmas Eve	24.12.*
Christmas Day	25.12.*
Boxing Day	26.12.*
New Year's Eve	31.12.*
Ulis Special	21.09.2016

Deactivated  
 Categorie:   
 Priority higher than weekend  
 Date  
  
 active for offline locking system



#### Remarque!

Le nombre d'éléments d'un système de verrouillage hors ligne est restreint à ##.

Les boutons suivants se trouvent en haut de la liste :



**Créer** un congé/jour spécial



**Modifier** un congé/jour spécial



## Supprimer un congé/jour spécial



### Remarque!

Nous vous recommandons de ne pas supprimer, mais plutôt de désactiver les congés et jours spéciaux prédéfinis dont les **dates sont variables** (Pâques, par exemple) si vous ne souhaitez pas les utiliser. Les congés et jours spéciaux dont les dates sont variables ne peuvent pas être ré-ajoutés ultérieurement via la boîte de dialogue.

Si vous utilisez le bouton ou pour ajouter ou modifier des congés, le message suivant vous invitera à attribuer un nouveau nom :



Si vous confirmez à l'aide du bouton OK, le nouveau nom ou le nom modifié apparaît dans la liste. Vous pouvez configurer les paramètres de l'élément sélectionné dans la liste à droite de la zone de liste.

Désactivé	Détermine si le congé/jour spécial est utilisé ou non.
Catégorie	Vous pouvez répartir les congés/jours spéciaux actifs en 11 catégories (congé plus types de jours spéciaux 1 à 10) et attribuer des modèles Jour spécifiques à chaque catégorie au moment de définir les modèles horaires.
Priorité supérieure à week-end	Précise quelle option est prioritaire si un congé ayant lieu tous les ans tombe un samedi ou un dimanche. Lorsque cette case est cochée, le modèle de service pour le congé est prioritaire. Dans le cas contraire, le modèle horaire pour le week-end est prioritaire.
Date	Si le jour spécial revient tous les ans à la même date, vous devez saisir un astérisque (*) au lieu de saisir une année précise. Certains congés (Noël, par exemple) tombent toujours à la même date.

## 11 Modèles Jour

Les modèles Jour décrivent un planning quotidien abstrait. Quel que soit le jour de la semaine, le modèle Jour définit les heures de la journée auxquelles l'accès doit être accordé ou refusé.

Un modèle Jour distinct est requis pour chaque planning quotidien différent.

Un modèle Jour peut être composé de trois périodes différentes maximum avec des heures de début et de fin.

Lorsque les modèles Jour sont utilisés dans les modèles horaires, les modèles Jour sont associés à des jours spécifiques du calendrier.

### 11.1 Création et modification

Cette boîte de dialogue sert à créer et à modifier les modèles Jour qui sont à leur tour utilisés dans les modèles horaires.

No.	Name
1	7 - 16 DM
2	16 to 7

periods

1st period

start 07:00

end 16:00

2nd period

start

end

3rd period

start

end

La liste à gauche répertorie les modèles Jour définis jusqu'à présent.

Les boutons suivants se trouvent en haut de la liste :



**Créer** un modèle Jour

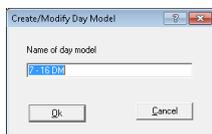


**Modifier** le modèle Jour sélectionné



**Supprimer** le modèle Jour sélectionné

Utilisez le bouton  pour ajouter des modèles Jour, ou le bouton  pour les modifier :



Si vous confirmez à l'aide du bouton **OK**, le nouveau nom ou le nom modifié apparaît dans la liste. Vous pouvez désormais définir les périodes composant le modèle Jour sélectionné à droite de la zone de liste. Un modèle Jour peut se composer de 3 périodes maximum.

L'heure de début de chaque période doit être antérieure à son heure de fin. Ainsi, si vous souhaitez définir un modèle Jour s'étendant après minuit, vous devez définir deux périodes :

1. La période entre : ... et 24h00
2. La période entre 00h00 et ...

## 12 Modèles horaires

Les modèles horaires limitent l'accès aux entrées auxquelles ils sont affectés à certaines heures de la journée. Cela permet au système de refuser tout accès, par exemple, pendant la nuit ou d'imposer des restrictions d'accès supplémentaires pendant le week-end.

Access PE utilise les modèles horaires de différentes manières, par exemple, en les associant à des :

- **groupes d'autorisation :**

Les modèles horaires peuvent être associés à des droits d'accès de manière à ce que ceux-ci ne s'appliquent que certains jours à certaines heures de la journée. Il est également possible d'utiliser des droits d'accès sans restriction horaire, et ce simultanément.

- **Personnes :**

Les modèles horaires attribués aux personnes limitent l'utilisation générale de leurs cartes selon des dates et des périodes définies.

- **Contrôleurs et cartes d'extension :**

L'émission de signaux d'entrée et de sortie par les contrôleurs et cartes d'extension peut aussi être limitée en fonction de modèles horaires.

- **Portes :**

Les heures d'ouverture des portes peuvent être régies par des modèles horaires.

- **Codes PIN :**

La saisie d'un code PIN constitue un exemple d'une mesure de sécurité supplémentaire qui peut être mise en place en dehors des heures définies par un modèle horaire.

- **Activation d'un verrouillage du moteur :**

Un verrouillage du moteur peut être configuré pour être activé uniquement dans le cadre d'un modèle horaire précis.

Selon l'utilisation qui en sera faite, les modèles horaires sont créés de différentes façons.

**Exemple :**

Supposons que les modèles horaires sont utilisés pour limiter l'accès des personnes les jours de la semaine entre 07h00 et 19h00 et les jours de week-end entre 09h00 et 15h00.

Deux modèles Jours sont alors nécessaires :

1. avec une période comprise entre 07h00 et 19h00
2. avec une période comprise entre 09h00 et 15h00

Si, dans le même temps, il est nécessaire d'activer un verrouillage du moteur uniquement en dehors de ces horaires, il faut alors définir deux modèles Jour qui seront utilisés par le modèle horaire du verrouillage selon le modèle ci-dessous :

1. avec deux périodes comprises entre 00h00 et 07h00, et entre 19h00 et 24h00.
2. avec deux périodes comprises entre 00h00 et 09h00, et entre 15h00 et 24h00.

**Application des modèles horaires**

Les modèles horaires associés aux données du personnel ne seront activés que si les paramètres par défaut du lecteur n'ont pas été modifiés. Dans ce cas, l'option **Aucune vérification du modèle horaire** (*Affichage et paramétrage, Page 48*) reste donc décochée.

Les modèles horaires peuvent avoir de nombreuses applications différentes. Pour comprendre comment le système gère les affectations multiples, veuillez noter les méthodes appliquées pour résoudre les conflits :

- si une personne dispose d'un accès à certaines entrées via un modèle horaire, et si cette personne dispose d'un accès à ces mêmes entrées sans modèle horaire, c'est alors la restriction **la plus souple** qui est appliquée en priorité. Dans ce cas, le modèle horaire ne sera donc pas appliqué.

**Exemple :**

**Une personne reçoit les droits d'accès suivants :**

- Accès aux entrées A, B, C et D selon un modèle horaire s'étendant de 09h00 à 17h00 chaque jour.
- Droits d'accès individuels aux entrées B et D sans modèle horaire.

Cette personne dispose également d'un accès aux entrées A et C entre 09h00 et 17h00 chaque jour et d'un accès illimité aux entrées B et D.

- Si une personne reçoit des droits d'accès différents pour les mêmes entrées, mais qui sont régies par des modèles horaires différents, les différents modèles horaires sont **conjointement** appliqués.

**Exemple :****Une personne reçoit les droits d'accès suivants :**

- Accès aux entrées A, B, C et D selon un modèle horaire s'étendant de 07h00 à 13h00 chaque jour.
- Accès aux entrées B, D, E et F selon un modèle horaire s'étendant de 09h00 à 17h00 chaque jour.

Cette personne dispose également d'un accès aux entrées A et C entre 07h00 et 13h00, aux entrées B et D entre 07h00 et 17h00 et aux entrées E et F entre 09h00 à 17h00

- Si une personne est affectée à un groupe d'autorisation disposant de modèles horaires, et si cette même personne reçoit un modèle horaire pour l'utilisation de sa carte, ce sont alors les **heures de recoupement** des périodes définies qui s'appliquent.

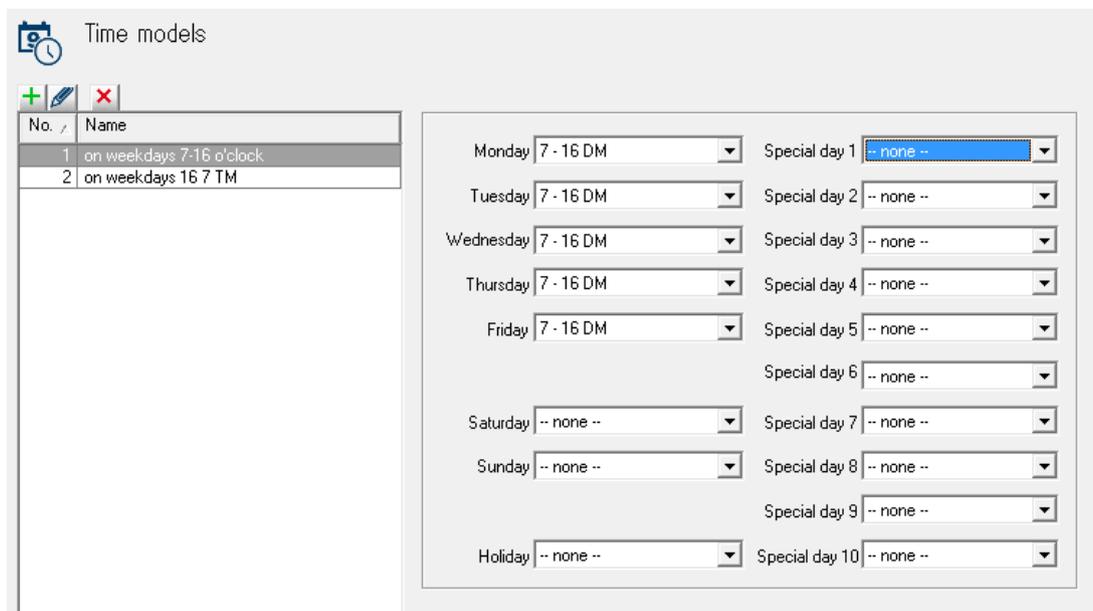
**Exemple :****Une personne reçoit les droits d'accès suivants :**

- Groupe d'autorisation disposant d'un accès aux entrées A, B, C et D et d'un modèle horaire s'étendant de 07h00 à 13h00 chaque jour.
- Groupe d'autorisation disposant d'un accès aux entrées B, D, E et F et d'un modèle horaire s'étendant de 09h00 à 17h00 chaque jour.
- Il contient en outre un modèle de service s'étendant de 11h00 à 19h00 chaque jour.

Cette personne a également accès aux entrées A et C entre 11h00 et 13h00 et aux entrées B, D, E, et F entre 11h00 et 17h00.

## 12.1 Création et modification

Cette boîte de dialogue sert à créer et à modifier les modèles horaires qui, en fonction de leur utilisation, activent certains éléments du système.



La liste à gauche répertorie les modèles horaires définis jusqu'à présent.

Les boutons suivants se trouvent en haut de la liste :



**Créer** un modèle horaire

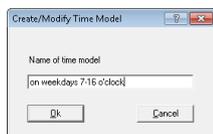


**Modifier** le modèle horaire sélectionné



**Supprimer** le modèle horaire sélectionné

Si vous utilisez le bouton  ou  pour ajouter ou modifier un modèle horaire, le message suivant vous invitera à attribuer un nouveau nom :



Si vous confirmez à l'aide du bouton **OK**, le nouveau nom ou le nom modifié apparaît dans la liste. Vous pouvez maintenant attribuer les modèles Jour situés à droite de la liste pour les jours de la semaine, les congés et les jours spéciaux (1...10) au modèle horaire sélectionné. Les modèles horaires sont définis comme des périodes récurrentes d'une semaine. Le déroulement de chaque jour de la semaine est défini en lui attribuant un modèle Jour. De plus, les modèles Jour appliqués aux jours ordinaires de la semaine peuvent être remplacés par les modèles Jour de congés ou de jours spéciaux qui tombent sur ces jours.

**Remarque!**

Si, lorsque vous définissez un modèle horaire, aucun modèle Jour n'est attribué à un jour de la semaine particulier ou à un jour spécial (c'est-à-dire que le paramètre par défaut **<aucun>** est conservé), ces jours sont alors traités comme s'ils avaient un modèle Jour sans période définie. En d'autres termes, ce jour-là, le modèle horaire n'accordera **aucun accès**.

## 13 Textes

Les langues que vous avez sélectionnées pour l'application au cours de l'installation disposent de leurs propres textes d'affichage pour les lecteurs équipés d'écrans et les messages de journal. Les textes figurant dans la liste correspondant à la langue sont utilisés dans le Visionneur de journal, par exemple, dans les messages de journal créés lorsque la langue de l'application est sélectionnée.

### 13.1 Textes d'affichage

	1st row	2nd row
Default message	Date hh:mm	
Welcome	Good morning	Name
Leaving	Good bye	Name
Authorized	Access	
Not authorized	Not authorized	
Arm IDS?	Arm IDS?	Present card
Close all	Close all doors	and windows!
IDS is activated	IDS armed	
Enter PIN code	Please enter	PIN code: _
Entry not valid	Invalid input	
Please wait	Please wait...	
Reader is offline	Reader offline	
Wrong area	Wrong location	Name
Check required	Random screening	Name
Floor _L	Please enter	floor number: _



#### Remarque!

Pour « Étage » entrez un seul chiffre si le nombre d'étages est entre 1 et 9. Pour 10 étages ou plus, entrez deux chiffres.

Vous pouvez modifier certains des textes affichés sur les lecteurs de carte à partir de cette boîte de dialogue. L'écran du lecteur se compose de deux lignes de 20 caractères chacune.



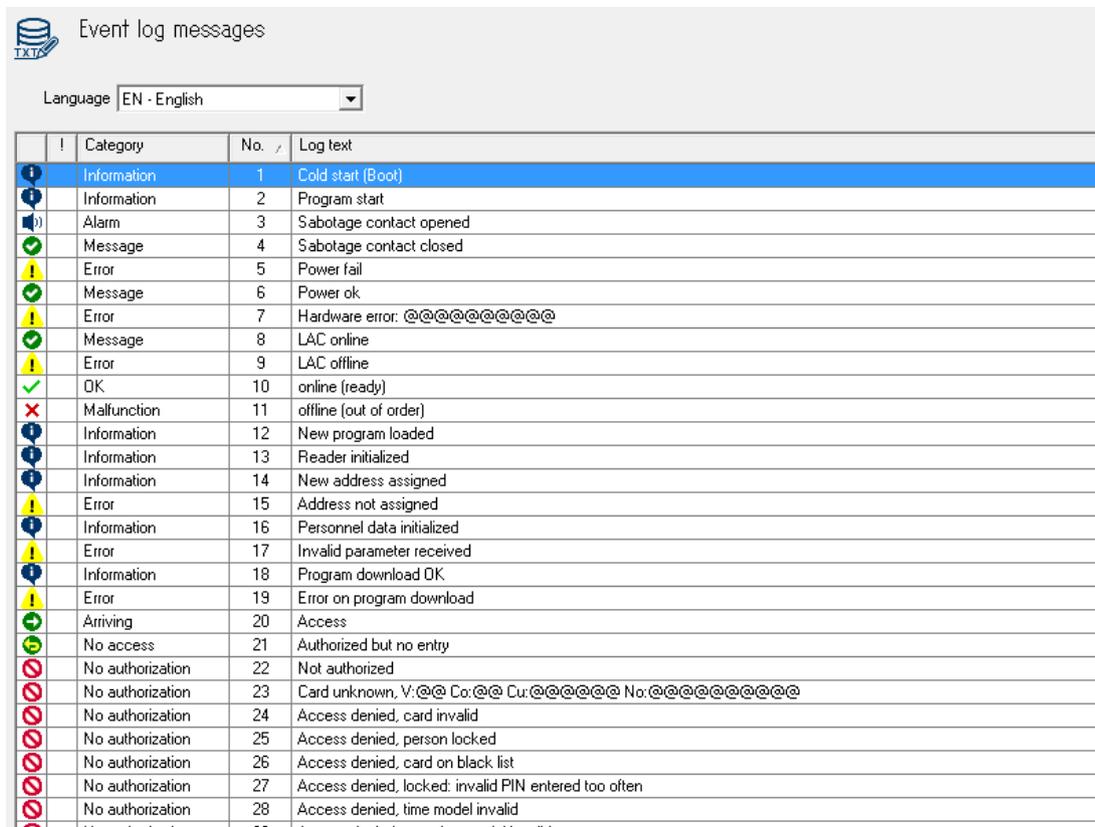
#### Attention!

Dans le texte pour Saisir le code PIN, le caractère de soulignement « \_ » ne doit pas être supprimé, car il déclenche la lecture du code PIN.

Les textes modifiés ici sont définis par l'utilisateur et ne sont pas automatiquement traduits par l'application lorsque vous changez de langue. Cependant, lorsque vous sélectionnez une autre langue dans la liste déroulante **Langue** (au-dessus de la zone de liste) et que vous saisissez de nouveaux textes, vous pouvez définir leur traduction pour chaque langue différente installée dans Access PE. De cette manière, un autre utilisateur pourra également afficher ces données dans sa propre langue.

## 13.2 Messages du journal des événements

Dans cette boîte de dialogue, vous pouvez modifier les textes des messages du journal, ainsi que leurs catégories.



Vous pouvez sélectionner la catégorie de votre choix dans une liste déroulante appelée en double-cliquant dans la colonne **Catégorie** de la ligne que vous souhaitez modifier.

	!	Category	No. /	Log text
		Information	1	Cold start (Boot)
		Information	2	Program start
		Alarm	3	Sabotage contact opened
		Message	4	Sabotage contact closed
		Error	5	Power fail
		Message	6	Power ok
		Error	7	Hardware error: @@@@
		Message	8	LAC online
		Error	9	LAC offline
		OK	10	online (ready)
		No access	11	offline (out of order)
		No authorization	12	New program loaded
		Malfunction	13	Reader initialized
		OK	14	New address assigned
		IDS armed	15	Address not assigned
		IDS not armed	16	Personnel data initialized
		Program Startup	17	Invalid parameter received
		Program Shutdown	18	Program download OK
		Operator action	19	Error on program download
		Information	20	Access
		Error	21	Authorized but no entry
		Arriving		
		No access		

Chaque catégorie est représentée par son propre symbole dans la première colonne. Ces symboles sont également utilisés pour classer les messages entrants dans le journal des événements par catégorie. Vous pouvez utiliser les symboles et catégories suivants :

- Journal des événements indisponible
- Note
- Message
- Erreur
- Alarme
- Arrivée
- Départ
- Aucun accès
- Aucune autorisation
- Dysfonctionnement
- OK
- IDS armé
- L'IDS n'est pas armé
- Démarrage du programme

-  Arrêt du programme
-  Action de l'opérateur

Dans la deuxième colonne (dont l'en-tête contient un !), sélectionnez les messages qui serviront de messages d'alarme spéciaux dans la boîte de dialogue **Gestion des alarmes**. Double-cliquez dans la cellule correspondante pour définir ou supprimer le symbole d'alarme . La procédure d'installation définit les messages appartenant aux catégories **Alarme** et **Erreur** comme les messages d'alarme par défaut.

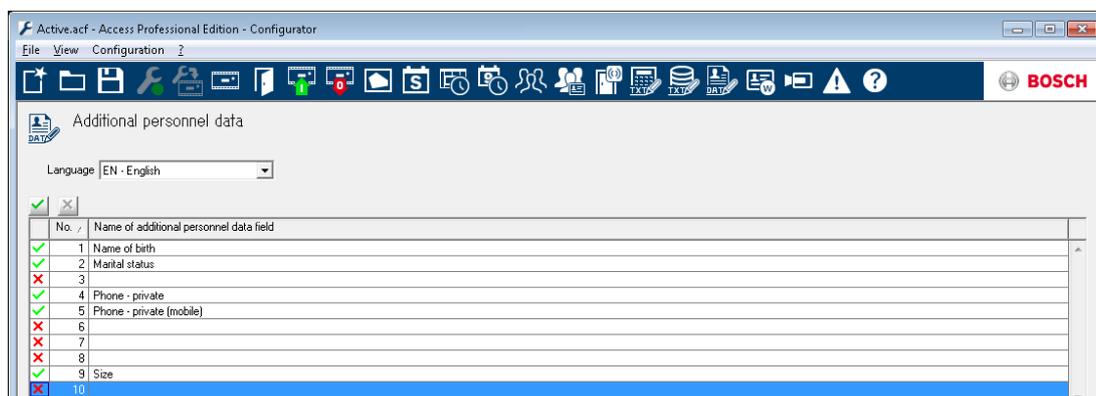
Vous pouvez modifier le texte de votre choix en double-cliquant sur la ligne que vous souhaitez modifier dans la colonne **Texte du journal**.

	!	Category	No.	Log text
		Information	1	Cold start (Boot)
		Information	2	Program start
		Alarm	3	Sabotage contact opened
		Message	4	Sabotage contact closed
		Error	5	Power fail
		Message	6	Power ok
		Error	7	Hardware error: @@@@
		Message	8	LAC online
		Error	9	LAC offline
		OK	10	online (ready)
		Malfunction	11	offline (out of order)
		Information	12	New program loaded

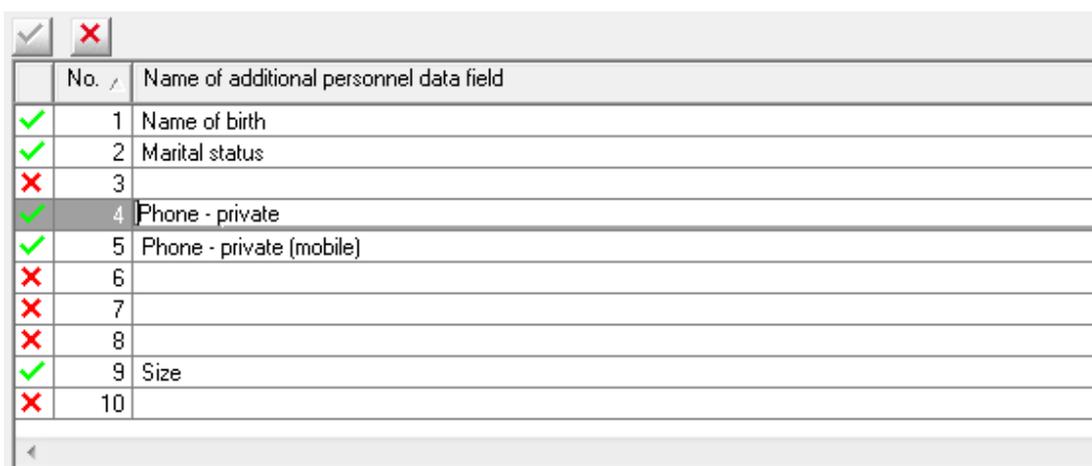
Les textes modifiés ici sont définis par l'utilisateur et ne sont pas automatiquement traduits par l'application lorsque vous changez de langue. Cependant, lorsque vous sélectionnez une autre langue dans la liste déroulante **Langue** (au-dessus de la zone de liste) et que vous saisissez de nouveaux textes, vous pouvez définir leur traduction pour chaque langue différente installée dans Access PE. De cette manière, un autre utilisateur pourra également afficher ces données dans sa propre langue.

## 14 Données du personnel supplémentaires

En plus des champs de données du personnel par défaut, vous disposez de dix champs supplémentaires dans lesquels vous pouvez saisir le texte de votre choix.



La zone de liste contient déjà 10 lignes que vous pouvez utiliser. Double-cliquez sur un champ dans la colonne **Nom du champ de données du personnel supplémentaires** pour pouvoir le modifier et saisir un nom.



### Remarque!



La saisie d'un nom n'active pas le champ. Pour l'activer, double-cliquez sur  dans la colonne située à l'extrémité gauche ou cliquez sur le bouton . Lorsque le champ est activé, le symbole  est remplacé par le symbole .

Lorsque au moins un champ de données supplémentaire est défini, un nouvel onglet intitulé **Données supplémentaires** apparaît dans l'application Gestion du personnel (boîte de dialogue Données personnelles et autorisations). Il n'est pas nécessaire de conserver l'ordre des champs, car les espaces vides seront utilisés pour les champs inactifs.

Chaque champ peut contenir jusqu'à 40 caractères arbitraires.



#### Remarque!

Chaque champ de saisie est associé à un champ dans la base de données ce qui permet d'enregistrer, de sélectionner et d'intégrer les données dans les rapports. En d'autres termes, les modifications apportées aux champs de données supplémentaires en cours d'utilisation entraînent la perte des données contenues dans la base de données.

Les noms des champs de données supplémentaires sont définis par l'utilisateur et ne sont pas automatiquement traduits par l'application lorsque vous changez de langue. Lorsque vous sélectionnez une autre langue dans la liste déroulante **Langue** (au-dessus de la zone de liste), vous pouvez définir leur traduction pour chaque langue différente installée dans Access PE. De cette manière, un autre utilisateur pourra également afficher ces données dans sa propre langue.

Activation/Désactivation des champs supplémentaires

En plus de les nommer, vous devez activer les données supplémentaires. Pour ce faire, double-cliquez sur le symbole dans la colonne située à l'extrémité gauche ou cliquez sur le bouton . Le symbole  est remplacé par le symbole .

L'onglet **Données supplémentaires** n'apparaît pas dans l'application **Gestion du personnel** tant qu'au moins un champ de données supplémentaires n'a pas été activé.



#### Remarque!

Vous pouvez également activer les champs auxquels aucun nom n'a été attribué.

Vous pouvez désactiver les champs activés en double-cliquant sur  ou en cliquant sur . Un message contextuel de sécurité s'affiche alors, vous proposant deux méthodes de désactivation :

**Remarque!**

**La désactivation des champs supprime les données du personnel correspondantes uniquement si la description du champ est également supprimée. Souhaitez-vous supprimer la description du champ et donc également supprimer les données du personnel ?**

- Non = Désactive le champ, mais conserve son nom et son contenu.
- Oui = Désactive le champ et **supprime son nom et son contenu.**

## 15 Gestion des périphériques vidéo

### 15.1 Ouvrir le configurateur

Il existe trois manières d'ouvrir le configurateur :

#### Option 1

1. Sur votre bureau, double-cliquez sur l'icône du configurateur .
  - Le configurateur s'ouvre.

#### Option 2

1. Ouvrez l'application **Gestion du personnel d'Access PE**.
2. Dans la barre de menu de l'application **Gestion du personnel d'Access PE**, cliquez sur .
  - Le configurateur s'ouvre.

#### Option 3

1. Ouvrez l'application **Gestion du personnel d'Access PE**.
2. Dans la barre de menu, sélectionnez **Outils**.
3. Dans la liste déroulante, sélectionnez **Exécuter le configurateur**.
  - Le configurateur s'ouvre.

### 15.2 Rechercher des appareils vidéo

Condition préalable :

- Installez et configurez tous les périphériques vidéo.
- Ouvrez le configurateur.

1. Dans la barre de menu du configurateur Access Professional Edition, cliquez sur .
2. Cliquez le bouton **Parcourir de nouveaux périphérique** pour rechercher des périphériques vidéo.
  - Au cours de la recherche, l'intitulé du bouton est remplacé par **Arrêter la recherche** pour vous permettre d'annuler la recherche.
  - Tous les périphériques vidéo pris en charge par le SDK vidéo Bosch seront détectés et apparaîtront dans la liste située dans la partie inférieure droite de la boîte de dialogue du configurateur.

#### Voir aussi

- *Ouvrir le configurateur, Page 87*

### 15.3 Ajout d'un périphérique vidéo au système de contrôle d'accès

1. Ouvrez le configurateur.
2. Dans la barre de menu du configurateur Access Professional Edition, cliquez sur .
3. Cliquez le bouton **Parcourir de nouveaux périphérique** pour rechercher des périphériques vidéo.
  - Au cours de la recherche, l'intitulé du bouton est remplacé par **Arrêter la recherche** pour vous permettre d'annuler la recherche.

- Tous les périphériques vidéo pris en charge par le SDK vidéo Bosch seront détectés et apparaîtront dans la liste située dans la partie inférieure droite de la boîte de dialogue du configurateur.
- Une fois la vidéo activée, le bouton d'activation sera désactivé.
- 4. Sélectionnez un périphérique vidéo dans la liste en bas à droite de la boîte de dialogue du configurateur.
- 5. Cliquez sur le bouton **Activer le périphérique**.
- Le périphérique vidéo sélectionné passe dans la liste située à gauche de la boîte de dialogue du configurateur.

**Remarque!**

Vous ne pouvez déplacer que des périphériques marqués d'une coche verte. Assurez-vous au préalable de rendre accessibles les entrées de liste protégées par un mot de passe (marquées d'une croix rouge) en appuyant sur le bouton de données **Modifier la connexion**.

**Remarque!**

Le nombre de périphériques que vous pouvez transférer peut être limité par la licence.

**Voir aussi**

- *Ouvrir le configurateur, Page 87*

## 15.4

### Modifier les données de connexion

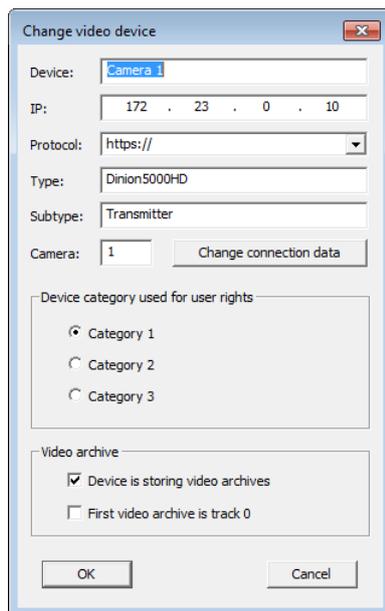
**Option 1**

1. Ouvrez le configurateur.
2. Dans la barre de menu du configurateur Access Professional Edition, cliquez sur .
3. Cliquez le bouton **Parcourir de nouveaux périphérique** pour rechercher des périphériques vidéo.
  - Au cours de la recherche, l'intitulé du bouton est remplacé par **Arrêter la recherche** pour vous permettre d'annuler la recherche.
  - Tous les périphériques vidéo pris en charge par le SDK vidéo Bosch seront détectés et apparaîtront dans la liste située dans la partie inférieure droite de la boîte de dialogue du configurateur.
4. Sélectionnez un périphérique vidéo dans la liste en bas à droite de la boîte de dialogue du configurateur.
5. Cliquez sur le bouton de données **Modifier la connexion**.
  - La boîte de dialogue appelée **Modifier les paramètres de connexion** s'ouvre.
6. Entrez le nom d'utilisateur et le mot de passe.
  - Assurez-vous d'utiliser un compte d'utilisateur autorisé.
7. Cliquez sur **OK**.

**Option 2**

1. Ouvrez le configurateur.
2. Double-cliquez sur un périphérique vidéo dans la liste située dans la partie gauche de la boîte de dialogue du configurateur.
  - Pour vous aider à identifier les périphériques vidéo individuels, reportez-vous aux entrées de périphérique de l'encodeur (N°, Nom, Adresse, Caméra, Type).
  - Une boîte de dialogue intitulée **Modifier le périphérique vidéo** s'ouvre.

3. Cliquez sur le bouton de données **Modifier la connexion**.
4. Entrez le nom d'utilisateur et le mot de passe.
  - Assurez-vous d'utiliser un compte d'utilisateur autorisé.
  - Notez que la modification des données d'accès du périphérique vidéo n'est possible que via le logiciel du périphérique.
5. Cliquez sur **OK**.



#### Voir aussi

- Ouvrir le configurateur, Page 87

## 15.5

### Modification des données du périphérique vidéo

1. Ouvrez le configurateur.
2. Dans la barre de menu du configurateur Access Professional Edition, cliquez sur .
3. Pour ouvrir la boîte de dialogue **Modifier le périphérique vidéo** :
  - Double-cliquez sur un périphérique vidéo dans la liste située dans la partie gauche de la boîte de dialogue du configurateur.
  - Cliquez sur l'icône Plus verte située au-dessus de la liste à gauche de la boîte de dialogue du configurateur.
4. Entrez ou modifiez les données du périphérique vidéo en fonction des possibilités ci-dessous.
5. Cliquez sur **OK**.

The screenshot shows a 'Change video device' dialog box with the following fields and options:

- 1 Device: Camera
- 2 IP: 172 . 23 . 0 . 10
- 3 Protocol: https://
- 4 Type: Dinion5000HD
- 5 Subtype: Transmitter
- 6 Camera: 1 (with a 'Change connection data' button)
- 7 Device category used for user rights:
  - Category 1
  - Category 2
  - Category 3
- 8 Video archive:
  - Device is storing video archives
  - First video archive is track 0

Buttons: OK, Cancel

1	Entrez ou modifiez le nom du périphérique vidéo.
2	Entrez ou modifiez l'adresse IP du périphérique vidéo.
3	Les périphériques vidéo sont connectés via le protocole https par défaut. Si le périphérique vidéo sélectionné ne prend pas en charge le protocole https, sélectionnez Aucun dans la liste déroulante.
4	Entrez ou modifiez le type de périphérique vidéo.
5	Entrez ou modifiez le sous-type de périphérique vidéo.
6	Modifiez les données de connexion.
7	Attribuez l'une des trois catégories de droits d'utilisateur, de sorte que seuls les utilisateurs sélectionnés puissent utiliser certaines caméras.
8	Cochez ou décochez les cases en fonction de la manière dont vous souhaitez que les vidéos soient archivées.

**Voir aussi**

- Ouvrir le configurateur, Page 87

**15.6****Affichage d'une image vidéo en direct**

1. Ouvrez le configurateur.
2. Dans la barre de menu du configurateur Access Professional Edition, cliquez sur .
  - Sélectionnez un périphérique vidéo dans le champ de liste situé à gauche de la boîte de dialogue du configurateur.
  - Cliquez le bouton **Afficher la vidéo**.

**Voir aussi**

- Ouvrir le configurateur, Page 87

**15.7****Affichage des archives**

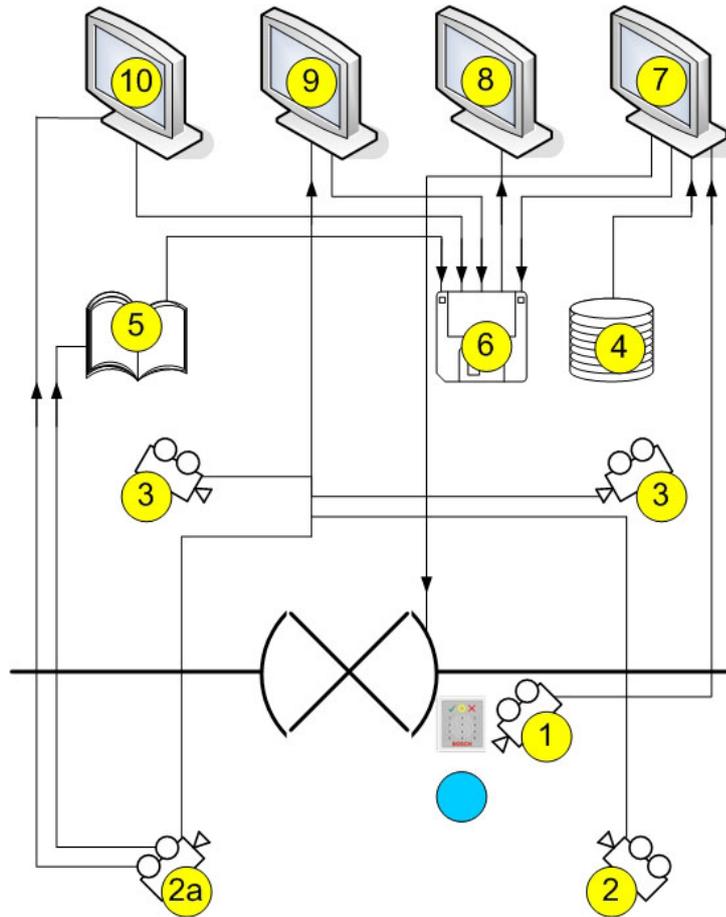
1. Ouvrez le configurateur.

2. Dans la barre de menu du configurateur Access Professional Edition, cliquez sur .
3. Sélectionnez un périphérique vidéo dans le champ de liste situé à gauche de la boîte de dialogue du configurateur.
4. Cliquez sur le bouton Afficher la lecture.
  - Une boîte de dialogue appelée Démarrer la lecture s'ouvre.
5. Définissez l'heure à laquelle vous souhaitez commencer à voir l'enregistrement.
6. Cliquez sur **OK**.

**Voir aussi**

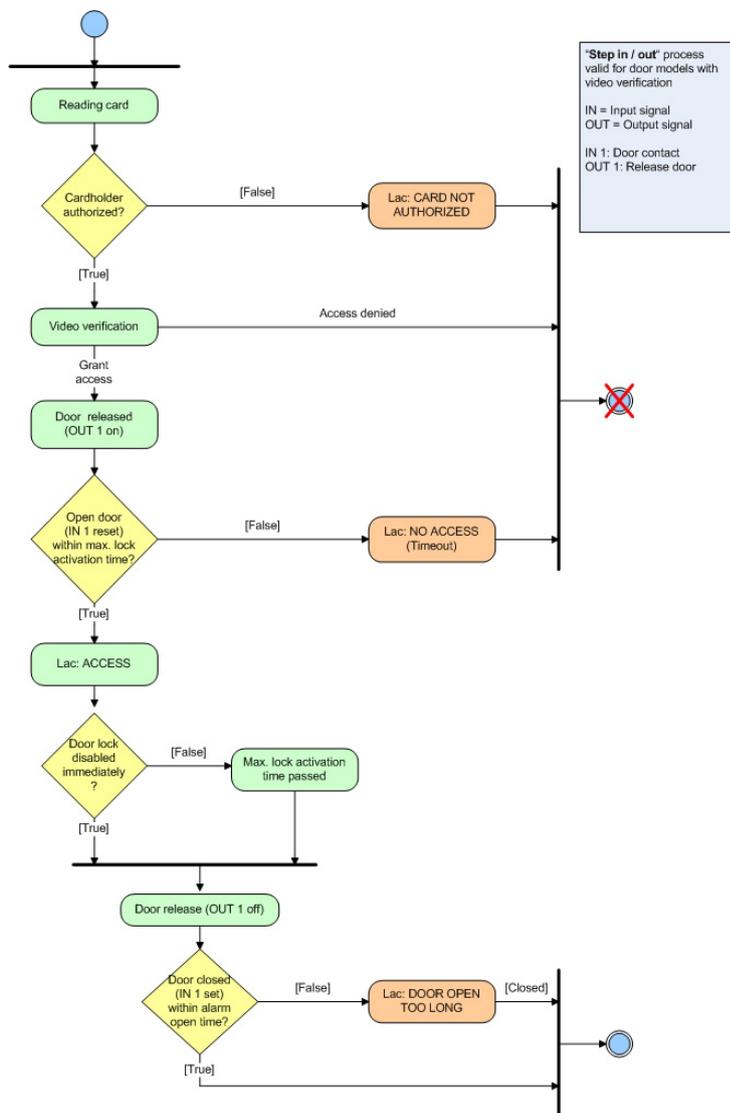
- Ouvrir le configurateur, Page 87

## 15.8 Affichages et processus



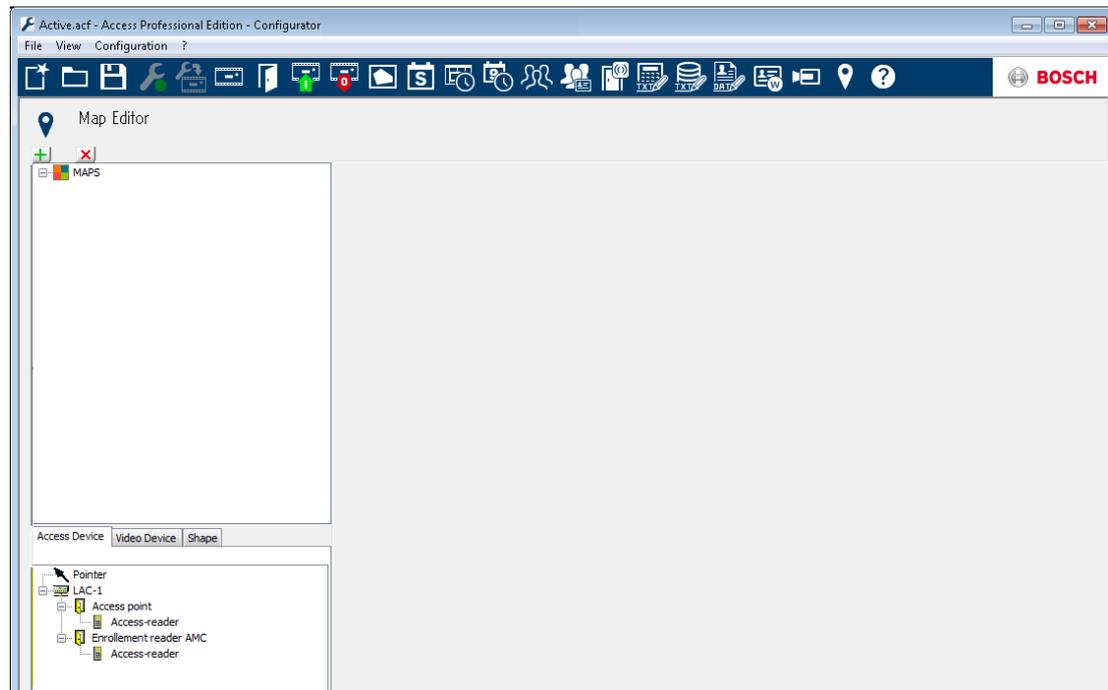
1 =	Caméra d'identification L'image provenant de cette caméra s'affiche dans la boîte de dialogue Vérification vidéo (7) lors de la réception d'une demande d'accès.
2 =	Caméras de surveillance - Zone arrière
2a =	Caméra d'alarme et de journal Choisissez la caméra 1, 2 ou 3
3 =	Caméras de surveillance - Zone avant

4 =	<p>Base de données</p> <p>Au cours de la vérification vidéo (7), une image provenant de la base de données s'affiche en face de l'image en temps réel provenant de la caméra d'identification (1) pour vous permettre de les comparer.</p>
5 =	<p>Journal</p> <p>Si vous avez configuré une caméra d'alarme et de journal (2a), les images associées à l'alarme seront enregistrées.</p>
6 =	<p>Disque dur local/Supports de stockage</p> <p>Vous pouvez enregistrer des fichiers locaux à partir des boîtes de dialogue Vérification vidéo (7), Panneau vidéo (9) et Gestion des alarmes (10), ainsi qu'à partir des images figurant dans les messages du journal (5). Les enregistrements vidéo (format .vxx) peuvent être lus avec le Lecteur vidéo Bosch (Bosch Video Player) (8).</p>
7 =	<p>Vérification vidéo</p> <ul style="list-style-type: none"> <li>– Comparaison d'images entre l'image en temps réel provenant de la caméra d'identification (1) et une image de la base de données (4).</li> <li>– Déverrouillage/Verrouillage de la porte via un bouton de la boîte de dialogue.</li> <li>– Stockage local des images affichées (6).</li> </ul>
8 =	<p>Lecteur vidéo Bosch (Bosch Video Player)</p> <p>Cette boîte de dialogue permet de lire les enregistrements stockés localement au format .vxx (6).</p>
9 =	<p>Panneau vidéo</p> <ul style="list-style-type: none"> <li>– Ce panneau permet d'afficher simultanément les images provenant de quatre caméras maximum.</li> <li>– Les enregistrements locaux (6) sont possibles pour chaque caméra.</li> </ul>
10 =	<p>Gestion des alarmes</p> <p>Si une caméra d'alarme et de journal (2a) a été configurée, vous pouvez également afficher les images vidéo des messages d'alarme provenant de l'entrée correspondante. Vous pouvez créer des copies locales (6) de ces images et les afficher dans le lecteur vidéo (8).</p>

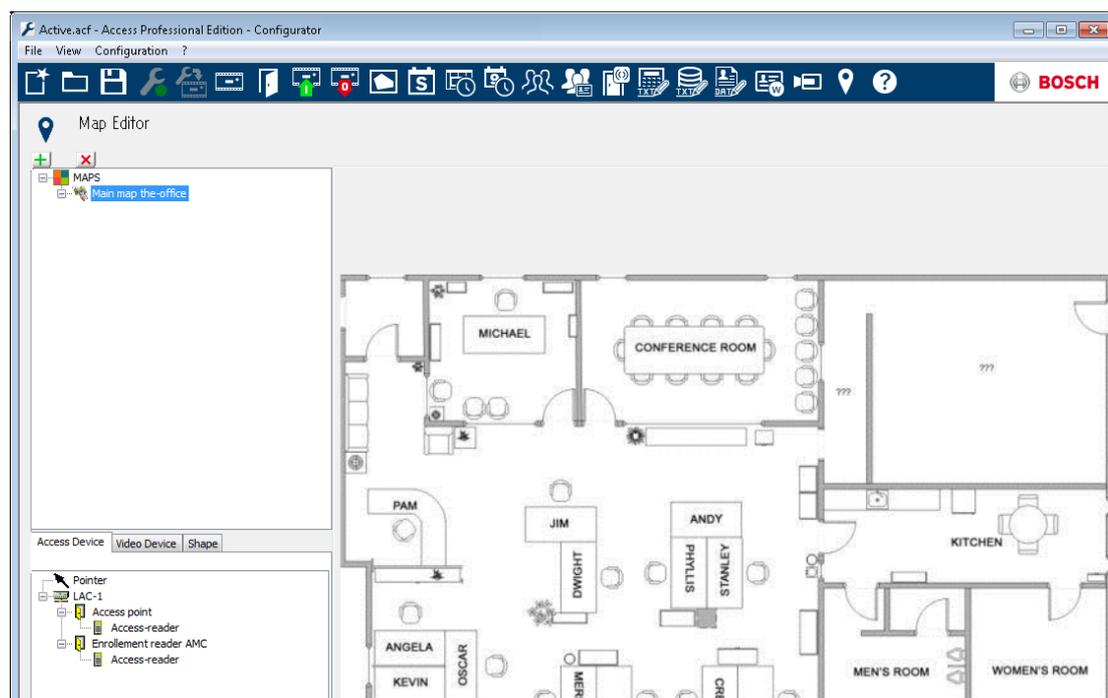


## 16 Configuration d'un plan

Démarrez l'Éditeur de plan

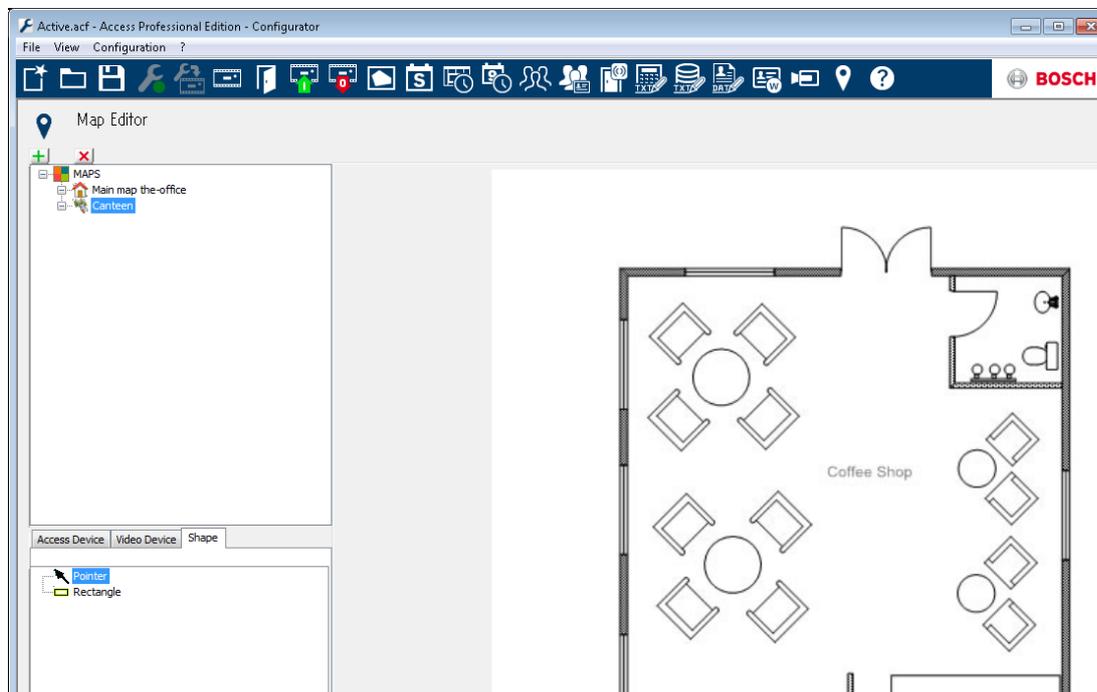


Cliquez sur le bouton  pour ajouter un plan.

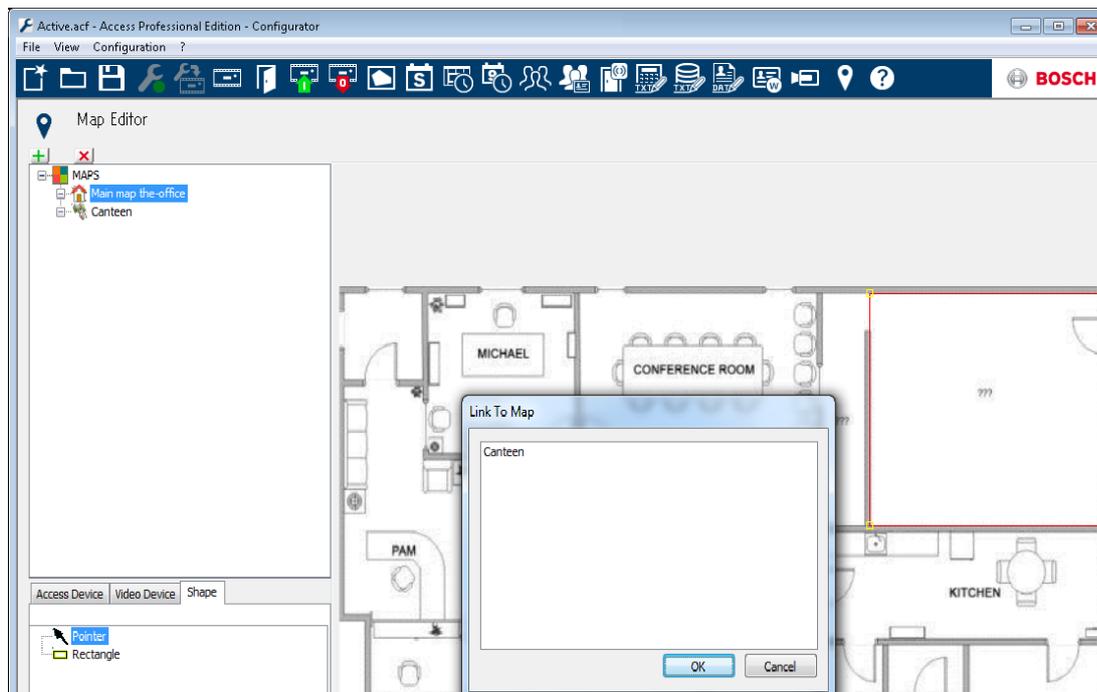


Le plan est affiché sur la boîte de dialogue.

- Vous pouvez aussi définir ce plan comme **Plan d'accueil**
- Ajoutez une vue détaillée, par ex. la cantine, à l'arborescence des plans.



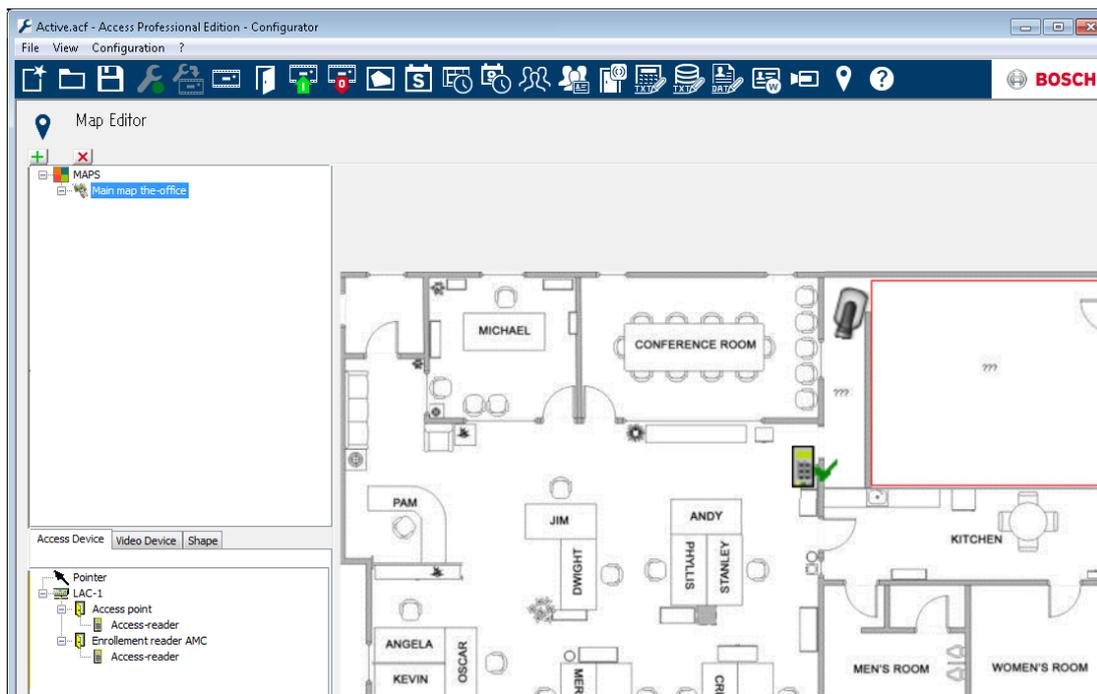
- Pour connecter le nouveau **plan de cantine** avec le plan principal, accédez à l'**onglet Forme** et sélectionnez un **rectangle**.
- Placez le rectangle sur la zone du plan principal devant être représenté par une vue détaillée (illustrée par un rectangle rouge dans l'exemple ci-dessous).
- À l'écran **Lier à un plan**, sélectionnez la vue détaillée respective, « Cantine » dans cet exemple.



## 17 Ajout d'un périphérique à un plan

Sélectionnez l'**onglet Périphérique**, puis ajoutez des périphériques au plan en les faisant glisser dans le plan à l'aide de la souris. Dans l'exemple ci-dessous, les périphériques suivants ont été ajoutés :

- Un point d'accès
- Un lecteur
- Deux caméras



- Cliquez sur un périphérique dans le plan et redimensionnez-le en maintenant le bouton de la souris enfoncé,
- Cliquez sur un périphérique et faites-le pivoter selon vos besoins à l'aide de la molette de la souris.

Types de périphérique	Éléments de contrôle
	Porte
	Lecteur
	Caméra

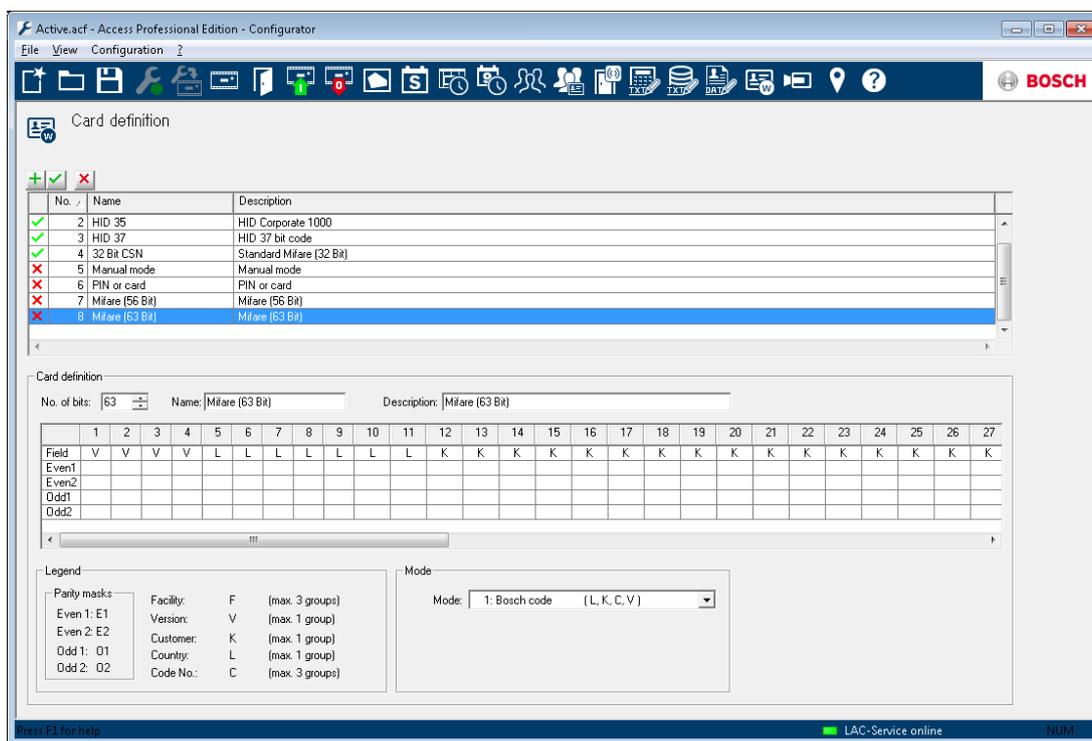
Types de périphérique	Alarmes
<b>Point d'accès (Entrée)</b>	
	Porte ouverte sans autorisation
	Porte ouverte trop longtemps
	(Toutes les alarmes du lecteur correspondent également à une alarme d'entrée*)
<b>Lecteur</b>	Erreur du lecteur

Types de périphérique	Alarmes
	
<b>Caméra</b>	N/A

\*) Ces événements d'alarme peuvent être personnalisés par l'utilisateur. Autrement dit, un utilisateur peut configurer un événement comme un événement d'alarme utilisant le message **AcConfig -> Journal des événements** (si vous cliquez deux fois sur la deuxième colonne, une alarme se déclenche).

# 18 Définition de carte

Cette boîte de dialogue permet de définir les données transmises par le lecteur de manière à pouvoir entrer de nouvelles définitions de cartes dans le système à une date ultérieure.



La liste contrôle les définitions de cartes existantes. Les paramètres système par défaut comprennent six valeurs standard, dont les quatre premières sont activées (signalées par une coche verte dans la première colonne). À l'exception du paramètre **Mode de saisie (Input Mode)**, tous les autres paramètres sont protégés contre l'écriture et ne peuvent être ni modifiés, ni supprimés.



**Remarque!**

Pour pouvoir utiliser les codes PIN d'identification, d'armement ou de la porte sur des contrôleurs et lecteurs Wiegand, l'option **PIN ou carte** (N°. 6) de la définition de carte Wiegand doit être activée.



**Remarque!**

Assurez-vous d'avoir seulement 4 types de carte active car le nombre maximum de types de carte valide est 4.

Pour commencer une nouvelle saisie, cliquez sur . Selon les informations du fabricant, le **nombre de bits** et leur encodage sont sélectionnés et affichés.



**Remarque!**

Le nombre maximum de bits est limité à 64 pour l'ensemble des définitions. Le nombre maximum de bits pour l'encodage (bâtiment, version, client, pays et numéro de code) est de 32.

Vous devez saisir un nom unique et une description pour distinguer les nouvelles définitions de cartes des autres.

Lorsque vous saisissez une valeur dans le champ **Nombre de bits**, le nombre de colonnes dans la zone de liste en dessous est modifié en conséquence. Cinq lignes sont affichées et la matrice correspondante vous permet d'activer/désactiver les bits individuels à votre convenance.

Vous pouvez alors indiquer l'interprétation du code en saisissant les valeurs possibles suivantes dans les cellules de la ligne **Champ**.

- F Bâtiment : affectation des bits à l'encodage du bâtiment.
- V Version : affectation des bits à l'encodage de la variante de la version.
- K Affectation des bits à l'encodage du client.
- L Pays : affectation des bits à l'encodage du code pays.
- C N° de code : affectation des bits à l'encodage du numéro de carte.
- E1 Paire 1 : annulation des bits pour le premier masque de parité paire
- E2 Paire 2 : annulation des bits pour le deuxième masque de parité paire
- O1 Impair 1 : annulation des bits pour le premier masque de parité impaire
- O2 Impair 2 : annulation des bits pour le deuxième masque de parité impaire
- 1 Valeurs de bit composant le code
- 0

Lorsque vous définissez le **Mode manuel** ou que vous créez un nouvel exemple, vous pouvez indiquer le **Mode** qui déterminera la méthode de lecture du code. Par exemple, si vous sélectionnez le mode **PIN ou carte**, seul le numéro de code sera lu, c.-à-d. seulement les parties signalées par la lettre **C**. Vous pouvez choisir entre les différents modes suivants :

Numéro de série	Mode	Parties de code vérifiées
0	Bâtiment + N° de code	F, C
1	Code Bosch	L, K, C, V
100	Manuel	C

Numéro de série	Mode	Parties de code vérifiées
200	PIN ou carte	C

**Explication :**

Le « télégramme » envoyé par un lecteur lorsqu'une carte est présentée comprend une série de zéros et de uns. Pour chaque type de carte/lecteur, la longueur du télégramme (le nombre de bits) est définie de manière précise. En plus des données d'utilisateur, un télégramme de ce type contient des données de commande permettant d'identifier le type de télégramme et de vérifier la réussite du transfert des données. La réussite du transfert des données est vérifiée par le biais des bits de parité qui représentent une somme de contrôle des bits sélectionnés dans le masque, soit zéro (parité paire), soit un (parité impaire). Les contrôleurs peuvent être configurés pour calculer une ou deux sommes de contrôle pour les parités paires, et une ou deux sommes de contrôle pour les parités impaires. Dans les lignes réservées aux sommes de contrôle de parité dans la zone de liste (Paire1, Paire2, Impair1 et Impair2), vous pouvez indiquer les bits qui doivent être inclus dans la somme de contrôle. Dans la colonne tout en haut (Champ), un bit est désigné pour chaque somme de contrôle utilisée pour équilibrer la somme de contrôle en fonction de son type de parité. Si un type de parité (Paire1, Paire2, Impair1, Impair2) n'est pas utilisé, la ligne correspondante est simplement laissée vierge.

**Activation/Désactivation des définitions de cartes**

Le symbole présent dans la première colonne de la liste indique l'état d'activation de chaque définition de carte.



activé



désactivé

Double-cliquez sur le symbole pour basculer d'un état d'activation à l'autre.

Des contrôles de sécurité informent l'utilisateur sur les conséquences de la suppression d'une définition de carte en cours d'utilisation.

**Remarque!**

**Un encodage de carte erroné ou une saisie erronée peut rendre toutes les cartes illisibles !  
Souhaitez-vous vraiment activer l'encodage de carte sélectionné ?**

**Remarque!**

**Toutes les cartes utilisant actuellement cet encodage vont devenir illisibles ! Souhaitez-vous vraiment désactiver l'encodage de carte sélectionné ?**

# 19 Configuration des alertes de menace

## Introduction

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.

Une **Alerte de menace** est une alarme en réponse à une menace. En fonction de leurs paramètres dans le configurateur Access PE, les entrées peuvent répondre aux alertes de menace de différentes manières.

Les personnes dûment autorisées peuvent émettre une alerte de menace en une seule action, par exemple via l'interface utilisateur d'Access PE, en appuyant sur un bouton ou en présentant une carte d'identité spéciale à un lecteur.



### Remarque!

Toujours se conformer aux réglementations de sécurité locales concernant les entrées dans les situations d'urgence

Le mode de sécurité intrinsèque est généralement stipulé pour les entrées.

## 19.1 Configuration du matériel pour les alertes de menace

### Présentation

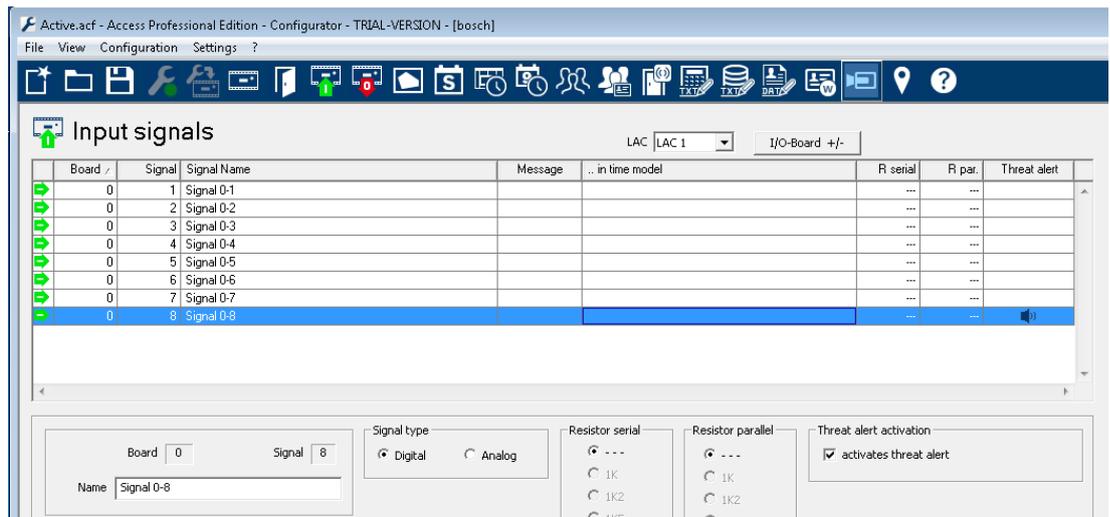
- Attribuer un signal d'entrée AMC pour la propagation des alertes de menace
- Définir la réponse des entrées individuelles à l'alerte de menace

### Affectation d'un signal d'entrée pour les alertes de menace



1. Dans le configurateur Access PE, sélectionnez **Signaux d'entrée**.
2. Dans la ligne correspondant au signal d'entrée souhaité, double-cliquez sur la colonne **Alerte de menace** ou cochez la case **Active l'alerte de menace**.

Une icône de haut-parleur apparaît dans la cellule.

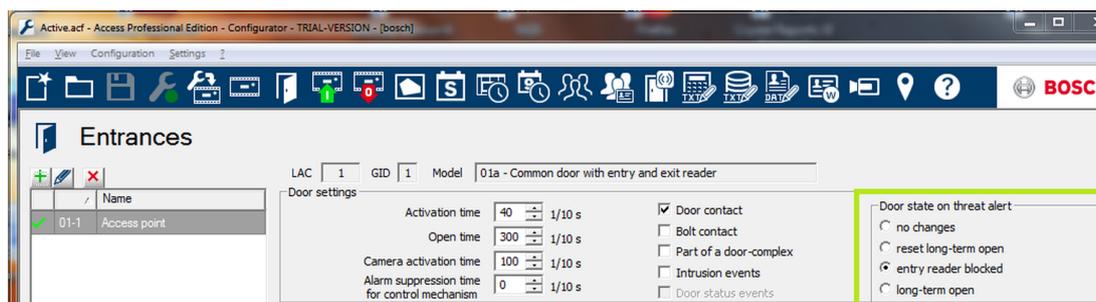


### Définition des réponses des entrées à une alerte de menace



1. Dans le configurateur Access PE, sélectionnez **Entrées**.
2. Dans la liste des entrées, sélectionnez une entrée qui doit répondre aux alertes de menace.

3. Définissez le paramètre **État de la porte sur l'alerte de menace** sur l'une des valeurs suivantes :
  - **aucun changement** : l'entrée ne doit pas changer d'état en réponse à l'alerte de menace.
  - **réinitialiser l'ouverture à long terme** : toute période déverrouillée en mode bureau est terminée et la porte reprend le mode normal. Cela signifie que la porte ne se déverrouille désormais que pour les informations d'identification valides.
  - **porte bloquée** : la porte est verrouillée et sécurisée. Le mode normal est suspendu.
  - **ouvert à long terme** : la porte est déverrouillée et permet un accès non contrôlé.
4. Répétez cette procédure pour toutes les entrées devant répondre à des alertes de menace.



Notez que les effets d'une alerte de menace persistent jusqu'à ce que celle-ci soit annulée explicitement via l'interface utilisateur du système de contrôle d'accès. Consultez l'aide en ligne d'APE Personnel Management, section : **Utilisation des boutons Définir/Désactiver l'alerte de menace**.

### Remarque!

Portes « bloquées » (sécurisées)

Une entrée qui a été explicitement définie pour indiquer **porte bloquée** (sécurisée) reste sécurisée lorsque vous désactivez une alerte de menace via le bouton **Désactiver l'alerte de menace**. Un état sécurisé doit être désactivé explicitement sur la porte afin d'éviter des violations de sécurité supplémentaires à la suite des alertes de menace.

Chemin de dialogue :

écran principal **Gestion du personnel** > arborescence **États de l'appareil** > cliquez avec le bouton droit de la souris sur l'entrée sécurisée (marquée d'un cadenas) pour afficher son menu contextuel.



## 20

### 20.1

## Annexe

### Signaux

Liste des signaux disponibles pour les entrées et les sorties.

Signaux d'entrée	Description
Capteur 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 permanent.
Sabotage	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.
Ouverture locale activée	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).

Signaux de sortie	Description
Ouvre-porte	
Passage : verrouiller la direction opposée	Verrouille l'autre côté du passage. Est défini à l'ouverture de la porte.
Suppression des alarmes	... vers l'IDS. Est défini tant que la porte est ouverte, afin d'éviter que l'IDS ne génère un message d'intrusion.

Signaux de sortie	Description
Indicateur vert	Voyant - est contrôlé tant que la porte est ouverte.
Porte ouverte trop longtemps	Impulsion de trois secondes. Si l'ouverture de la porte est trop longue.
Activation de la caméra	La caméra est activée au début d'un passage.
Ouvrir l'entrée du tourniquet	
Ouvrir la sortie du tourniquet	
La porte est ouverte en permanence	Afficher que la porte est ouverte en permanence.
IDS : armer	Impulsion ou contact permanent pour armer l'IDS.
IDS : désarmer	Impulsion pour désarmer l'IDS.

## 20.2 Modèles de porte par défaut

Modèles de porte standard

Les modèles de porte suivants sont disponibles par défaut :

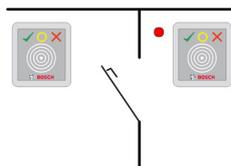
- 01a Porte normale avec lecteur d'entrée et de sortie
- 01b Porte normale avec lecteur d'entrée et bouton-poussoir
- 01c Porte normale avec lecteur d'entrée
- 01r Un lecteur dont le seul objectif est d'enregistrer les personnes à un point de rassemblement, par exemple dans le cas d'une évacuation. Aucune barrière physique n'est mise en œuvre et aucun signal n'est créé.
- 03b Tourniquet pivotant avec lecteur d'entrée et bouton-poussoir
- 03c Tourniquet avec lecteur d'entrée
- 06c Inscription via AMC - Pas de contrôle d'entrée !
- 07a Ascenseur desservant jusqu'à 16 étages
- 07b Ascenseur desservant jusqu'à 16 étages
- 10a Porte normale avec lecteur d'entrée et de sortie et réarmement de l'IDS
- 10b Porte normale avec lecteur d'entrée, bouton-poussoir et réarmement de l'IDS
- 10c Porte normale avec lecteur d'entrée et réarmement de l'IDS

- 10d Porte normale avec lecteur d'entrée et de sortie et réarmement décentralisé de l'IDS
- 10e Porte normale avec lecteur d'entrée, bouton-poussoir et réarmement décentralisé de l'IDS
- 10f Porte normale avec lecteur d'entrée et réarmement décentralisé de l'IDS
- 14a Porte normale avec lecteur d'entrée et de sortie et réarmement de l'IDS (autorisation d'armement)
- 14b Porte normale avec lecteur d'entrée, bouton-poussoir et réarmement de l'IDS (autorisation d'armement)
- 14c Porte normale avec lecteur d'entrée et réarmement de l'IDS
- 14d Porte normale avec lecteur d'entrée et de sortie et réarmement décentralisé de l'IDS
- 14e Porte normale avec lecteur d'entrée, bouton-poussoir et réarmement décentralisé de l'IDS
- 14f Porte normale avec lecteur d'entrée et réarmement décentralisé de l'IDS

## 20.3

### Modèle de porte 01

Porte normale



**Signaux :**

Signaux d'entrée	Signaux de sortie
Capteur de porte	Ouvre-porte
Bouton-poussoir : porte ouverte	Passage : verrouiller la direction opposée
Capteur de pêne	Suppression alarmes
Entrée verrouillée	Activation de la caméra
Signal de sabotage	Porte ouverte trop longtemps
Ouverture locale activée	

**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
- 01r 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 mise en œuvre dans ce modèle de porte et aucun signal n'est créé.

**Remarque :**

Le verrouillage du sas n'est actif que si la porte est configurée comme faisant partie d'un sas.

**Si la porte n'est pas configurée comme faisant partie d'un sas, le signal d'entrée 03 est interprété comme un verrouillage du lecteur. Dans ce cas, si le signal d'entrée 03 est défini, le lecteur sera verrouillé.**

**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.**

Des lecteurs secondaires facultatifs peuvent être connectés. Associés à une seconde porte et à un verrouillage du sas, ils permettent de contrôler simultanément les deux portes comme un sas. Ce type d'utilisation 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.

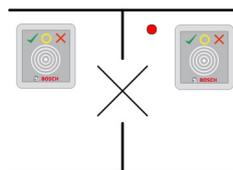


**Remarque!**

La fonctionnalité de comptage individuel peut uniquement être configurée pour le modèle de porte 03.

## 20.4 Modèle de porte 03

Tourniquet pivotant



**Signaux :**

Signal d'entrée	Signaux de sortie
Tourniquet en position normale	Ouvrir l'entrée du tourniquet
Bouton-poussoir : porte ouverte	Ouvrir la sortie du tourniquet
Entrée verrouillée	Passage : verrouiller la direction opposée
Signal de sabotage	Suppression des alarmes
	Activation de la caméra
	Porte ouverte trop longtemps

**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

**Remarque :**

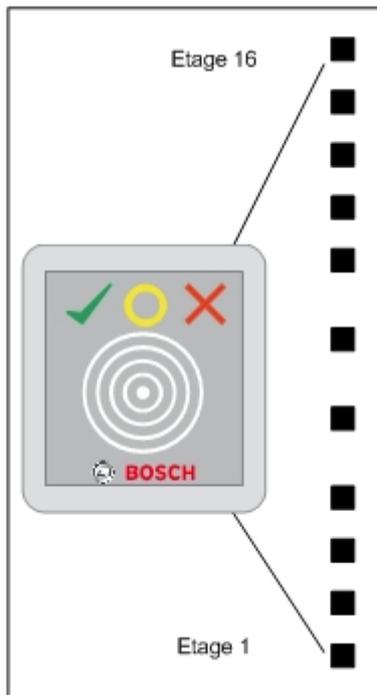
Le verrouillage du sas n'est actif que si la porte est configurée comme faisant partie d'un sas. Si la porte n'est pas configurée comme faisant partie d'un sas, le signal d'entrée 03 est interprété comme un verrouillage du lecteur. Dans ce cas, si le signal d'entrée 03 est défini, le lecteur sera verrouillé.

Associés à une seconde porte et à un verrouillage du sas, ils permettent de contrôler simultanément les deux portes comme un sas. Selon la configuration de l'installation, l'entrée peut effectuer un comptage individuel.

## 20.5 Modèle de porte 06c

Le modèle de porte 06c configure un lecteur connecté à l'AMC comme un périphérique d'inscription. Il ne contrôle pas une entrée.

## 20.6 Modèle de porte 07



### Variantes des modèles :

- 07a          Ascenseur
- 07b          Ascenseur avec entrée lecteur



### Remarque!

Inclus, un lecteur AMC2 peut être utilisé pour 8 étages. Il est possible de connecter d'autres entrées, avec les conditions préalables suivantes :

64 étages avec Wiegand (AMC2 4W + AMC2 4W-EXT + 3 AMC2 16I-16O-EXT)

56 étages avec RS 485 (AMC2 4R4 + 3 AMC2 16I-16O-EXT)

### Signaux pour le modèle d'entrée 07a :

Signal d'entrée	Signaux de sortie
Libre	Étage 01
Libre	Étage 02
Libre	Étage 03
Libre	Étage 04
...	...
Libre	Étage 16

**Procédure :**

Pour commencer, le détenteur de carte appelle l'ascenseur. Pour ce faire, il peut appuyer sur le bouton de l'ascenseur ou utiliser un lecteur de carte (par ex., modèle de porte 01c). Un autre lecteur de carte se trouve à l'intérieur de l'ascenseur (modèle de porte 07a). Ce lecteur accorde l'accès aux étages pour lesquels la carte de l'utilisateur contient des autorisations. L'ascenseur peut signaler les étages pour lesquels l'utilisateur dispose d'une autorisation d'accès, par exemple, en éclairant uniquement les boutons desservant ces étages. L'utilisateur peut alors choisir un seul des étages autorisés.

**Signaux pour le modèle d'entrée 07b :**

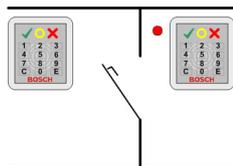
Signal d'entrée	Signaux de sortie
Clé d'entrée - Étage 01	Étage 01
Clé d'entrée - Étage 02	Étage 02
Clé d'entrée - Étage 03	Étage 03
Clé d'entrée - Étage 04	Étage 04
...	...
Clé d'entrée - Étage 16	Étage 16

**Procédure :**

Pour commencer, le détenteur de carte appelle l'ascenseur. Pour ce faire, il peut appuyer sur le bouton de l'ascenseur ou utiliser un lecteur de carte (par ex., modèle de porte 01c). Ensuite, une fois à l'intérieur de l'ascenseur, l'utilisateur présente sa carte à un autre lecteur de carte (modèle de porte 07b), puis appuie sur le bouton correspondant à l'étage auquel il souhaite se rendre. L'AMC vérifie si l'utilisateur est autorisé à accéder à l'étage sélectionné et, si c'est le cas, l'ascenseur dépose l'utilisateur à l'étage demandé.

## 20.7 Modèle de porte 10

Porte normale avec armement/réarmement de l'IDS (système de détection d'intrusion)



### Signaux :

Signaux d'entrée	Signaux de sortie
Capteur de porte	Ouvre-porte
Bouton-poussoir : porte ouverte	IDS : Désarmer (uniquement pour les modèles <b>d</b> et <b>f</b> avec une impulsion de 1 s).
IDS : prêt pour armement	Caméra / Verrouillage du moteur
IDS : armé	IDS : armer (uniquement pour les modèles <b>d</b> et <b>f</b> avec une impulsion de 1 s).
Signal de sabotage	Porte ouverte trop longtemps (intrusion)
IDS : armement	

### Variantes des modèles :

- 10a Porte normale avec lecteur d'entrée et de sortie et réarmement de l'IDS
- 10b Porte normale avec lecteur d'entrée, bouton-poussoir et réarmement de l'IDS
- 10c Porte normale avec lecteur d'entrée et réarmement de l'IDS
- 10d Porte normale avec lecteur d'entrée et de sortie et réarmement décentralisé de l'IDS
- 10e Porte normale avec lecteur d'entrée, bouton-poussoir et réarmement décentralisé de l'IDS
- 10f Porte normale avec lecteur d'entrée et réarmement décentralisé de l'IDS

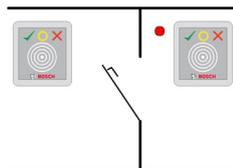
**Remarques :**

Le bouton **E** situé sur le lecteur d'entrée permet d'armer l'IDS (système de détection d'intrusion) La présentation d'une carte autorisée et la saisie d'un code PIN sont requis. L'IDS sera désarmé dès la première entrée autorisée pour laquelle la saisie d'un code PIN d'identification sera également requise. Dans le cas des modèles a à c, cette opération est commandée par le signal de sortie armer/désarmer l'IDS.

Dans le cas des modèles **d** à **f**, l'armement ou le désarmement est déclenché par une impulsion séparée d'1 s. Un relais bistable connecté peut commander l'IDS pour plusieurs portes (DCU/Unités de contrôle des portes). Dans ce cas, les signaux nécessitent une connexion logique OU au relais. Les signaux **L'IDS est armé** et **L'IDS est désarmé** doivent être connectés en double sur toutes les DCU concernées.

## 20.8 Modèle de porte 14

Porte avec contrôle IDS



**Signaux :**

Signaux d'entrée	Signaux de sortie
Capteur de porte	Ouvre-porte
Bouton-poussoir : porte ouverte	IDS : Désarmer (uniquement pour les modèles <b>d</b> et <b>f</b> avec une impulsion de 1 s).
IDS : prêt pour armement	Caméra / Verrouillage du moteur
IDS : armé	IDS : armer (uniquement pour les modèles <b>d</b> et <b>f</b> avec une impulsion de 1 s).
Signal de sabotage	Porte ouverte trop longtemps (intrusion)
IDS : armement	

**Variantes des modèles :**

- 14a Porte normale avec lecteur d'entrée et de sortie et armement/désarmement de l'IDS
- 14b Porte normale avec lecteur d'entrée, bouton-poussoir et armement/désarmement de l'IDS
- 14c Porte normale avec lecteur d'entrée et armement/désarmement de l'IDS
- 14d Porte normale avec lecteur d'entrée et de sortie et armement/désarmement décentralisé de l'IDS
- 14e Porte normale avec lecteur d'entrée, bouton-poussoir et armement/désarmement décentralisé de l'IDS
- 14f Porte normale avec lecteur d'entrée et armement/désarmement décentralisé de l'IDS

**Remarques :**

Contrairement au modèle de porte 10, le modèle de porte 14 peut utiliser des lecteurs équipés ou non d'un clavier. Il présente une autre différence au niveau de l'affectation des droits d'armement de l'IDS : seuls les détenteurs de carte disposant des droits suffisants peuvent armer ou désarmer l'IDS.

Pour ce modèle, le processus d'armement/désarmement n'est pas régi par la saisie d'un code PIN, mais par un bouton situé à côté du lecteur qui exerce la même fonction que la touche 7 sur les lecteurs équipés d'un clavier. Lorsque l'utilisateur appuie sur ce bouton, l'état de l'IDS est signalé par les voyants de couleur situés sur le lecteur.

- Désarmé = voyant clignotant alternativement en vert/rouge
- Armé = voyant rouge allumé en continu

L'IDS est armé lorsque l'utilisateur présente une carte valide.

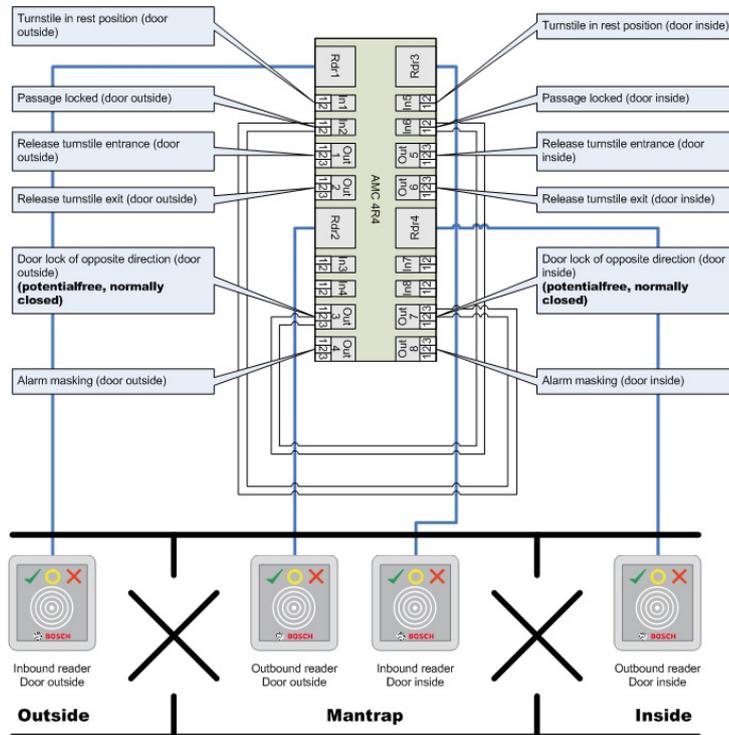
Pour désarmer l'IDS, l'utilisateur doit appuyer sur le bouton et présenter une carte valide.

La porte ne se déverrouille pas automatiquement. Pour déverrouiller la porte, l'utilisateur doit présenter sa carte une nouvelle fois après avoir désarmé l'IDS.

## 20.9 Exemples de configurations avec sas de sécurité

Les tourniquets sont le moyen le plus habituel d'effectuer un comptage individuel des accès des détenteurs 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 sas de sécurité avec deux tourniquets (MP 03a)



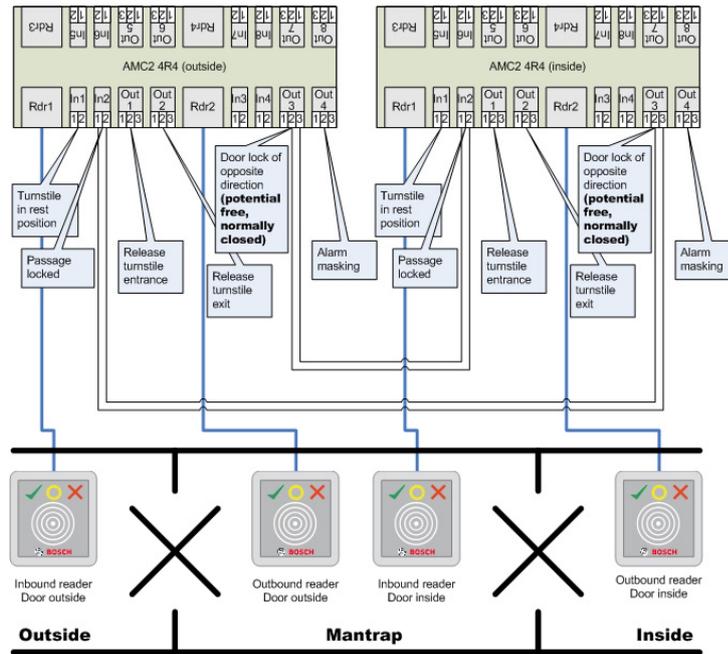
Les connexions aux verrouillages de porte pour la direction opposée garantissent l'ouverture d'un seul tourniquet à la fois.



#### Remarque!

Le signal de sortie (Sortie 3) doit être configuré sans potentiel (mode sec). Le signal « verrouillage de porte de la direction opposée » doit être fermé (résistance = 0) lorsqu'il est désactivé. Utilisez le contact « normalement fermé » (NF) pour les sorties 3 et 7.

**Configuration de sas de sécurité avec deux tourniquets (MP 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.

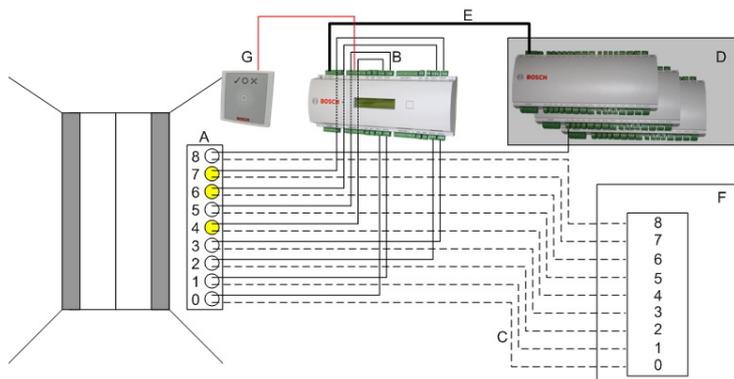


**Remarque!**

Le signal de sortie (Sortie 3) doit être configuré sans potentiel (mode sec). Le signal « verrouillage de porte de la direction opposée » doit être fermé (résistance = 0) lorsqu'il est désactivé. Utilisez le contact « normalement fermé » (NF) pour les sorties 3 et 7.

## 20.10 Configuration du modèle d'entrée 07

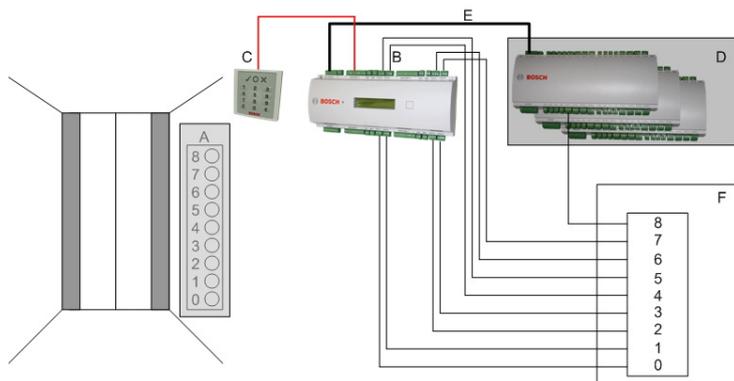
Le schéma ci-dessous illustre le câblage d'un ascenseur équipé du modèle de porte 07a



### Légende :

- A = Boutons d'étage à l'intérieur de l'ascenseur
- B = (trait continu) Signaux de sortie AMC
- C = (pointillés) Connexion au contrôle de l'ascenseur
- D = Possibilité de connecter une carte d'extension E/S (AMC2 8I-8O-EXT, AMC2 16I-EXT ou AMC2 16I-16O-EXT)
- E = Trafic de données et alimentation entre l'AMC et les cartes E/S
- F = Contrôle de l'ascenseur
- G = Lecteur (modèle de porte 07a)

Le schéma ci-dessous illustre le câblage d'un ascenseur équipé du modèle de porte 07b



### Légende :

- A = Boutons d'étage à l'intérieur de l'ascenseur
- B = (trait continu) Signaux d'entrée AMC
- C = (pointillés) Signaux de sortie AMC
- D = Possibilité de connecter une carte d'extension E/S (AMC2 8I-8O-EXT, AMC2 16I-EXT ou AMC2 16I-16O-EXT)
- E = Trafic de données et alimentation entre l'AMC et les cartes E/S
- F = Contrôle de l'ascenseur
- G = Lecteur (Modèle de porte 07b)



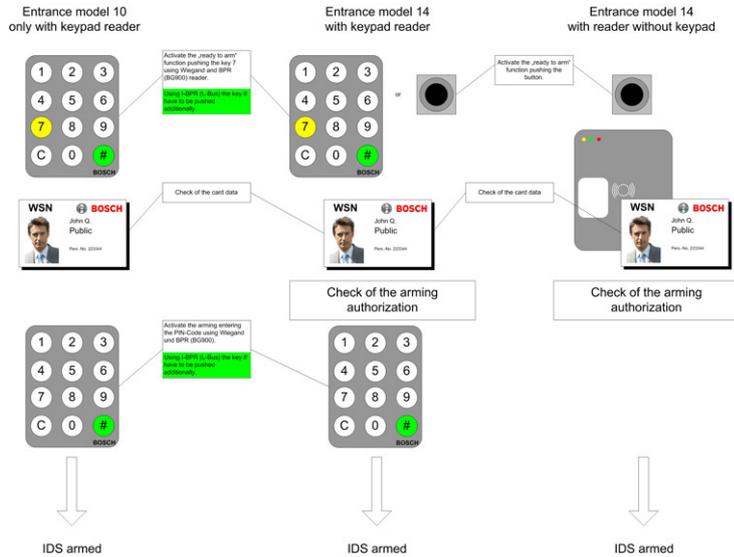
**Remarque!**

Lorsque vous raccordez les étages individuels (jusqu'à 16) aux sorties de l'AMC, commencez par connecter les signaux du contrôleur, puis, le cas échéant, les huit premières sorties de toute carte d'extension E/S présente par ordre croissant. [Lorsque des cartes d'extension Wiegand (AMC2 4W-EXT) sont en cours de fonctionnement, connectez leurs sorties par ordre croissant après avoir connecté celles du contrôleur AMC2 et avant de connecter les sorties de toute carte d'extension E/S présente.] C'est la raison pour laquelle vous ne pouvez pas configurer d'autres types de portes ou d'autres ascenseurs sur un AMC utilisé pour le contrôle d'ascenseur.

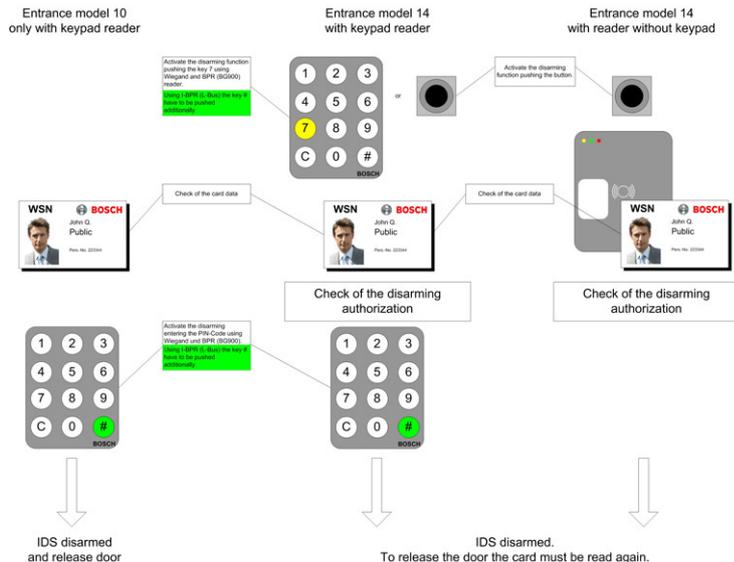
**20.11**

**Affichage de l'armement/désarmement**

Comparaison entre l'**armement** d'un système d'alarme sur les modèles d'entrée (porte) 10 et 14.



Comparaison entre le **désarmement** d'un système d'alarme sur les modèles d'entrée (porte) 10 et 14.

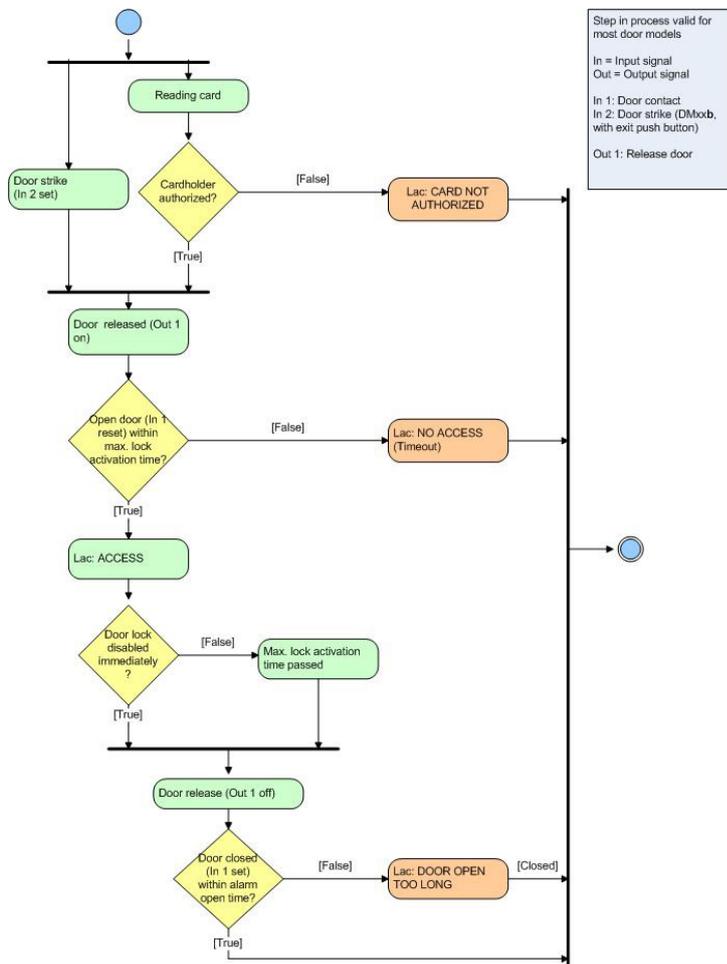




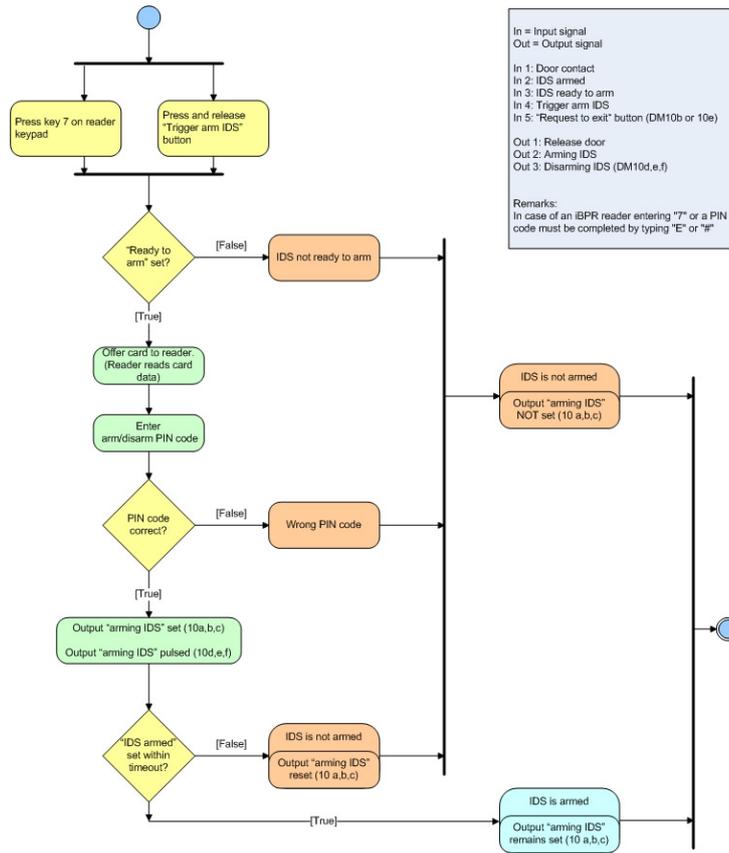
## 20.12 Procédures sous le contrôle d'accès

Organigrammes des procédures sous le contrôle d'accès

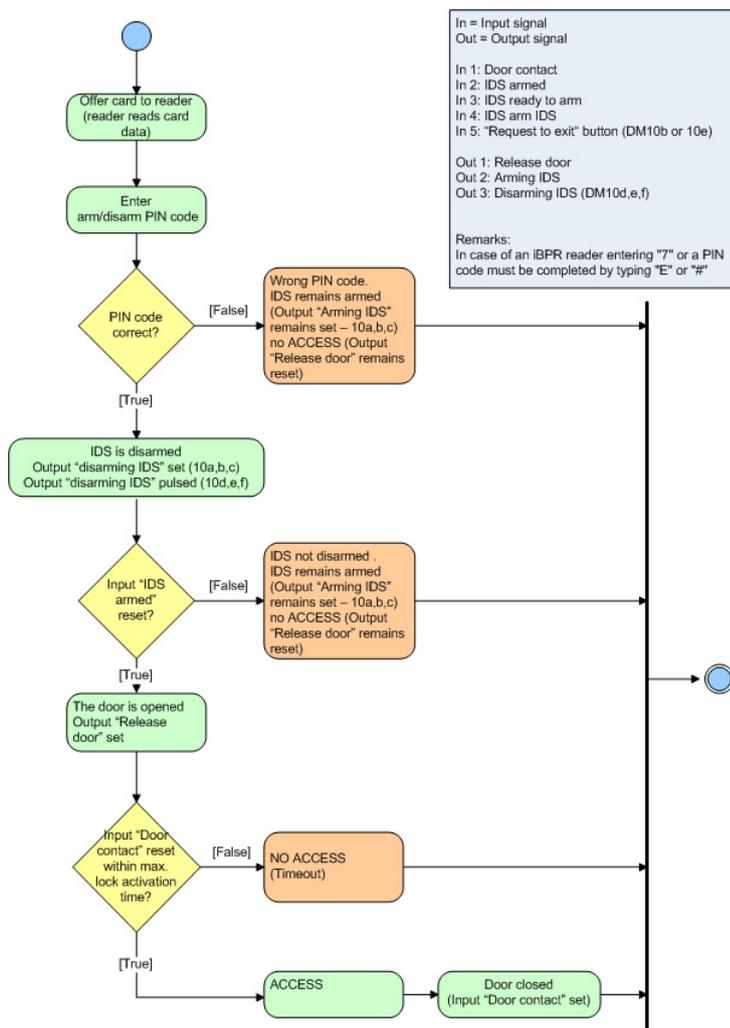
### Modèle de porte MP01



### Modèle de porte MP10 - Armement



### Modèle de porte MP10 - Désarmement



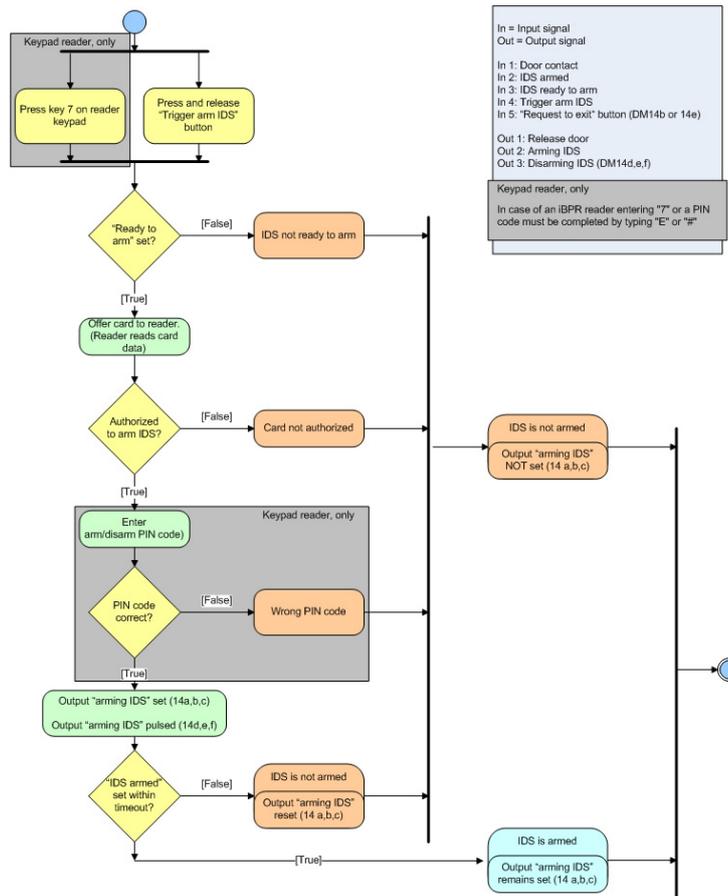
In = Input signal  
Out = Output signal

In 1: Door contact  
In 2: IDS armed  
In 3: IDS ready to arm  
In 4: IDS arm IDS  
In 5: "Request to exit" button (DM10b or 10e)

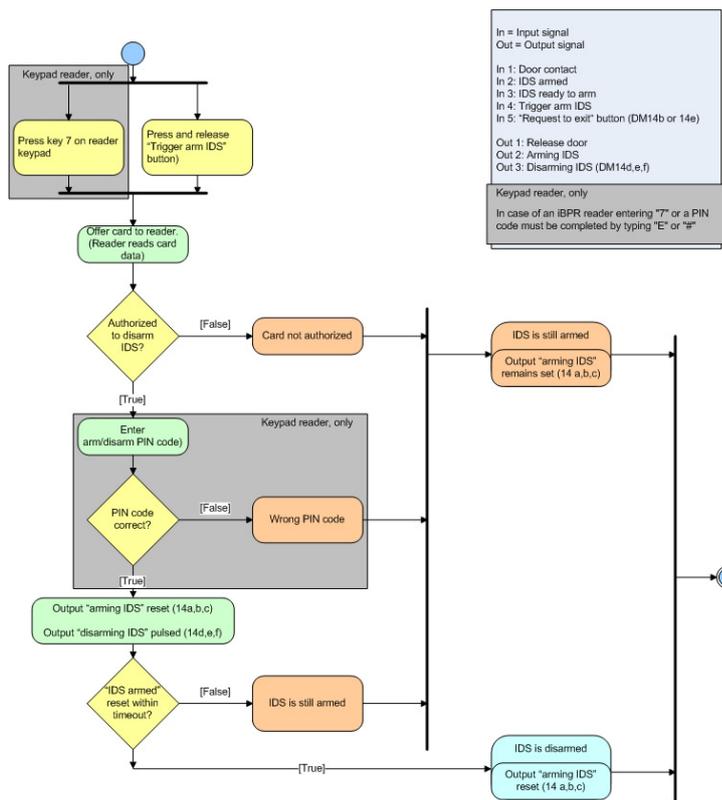
Out 1: Release door  
Out 2: Arming IDS  
Out 3: Disarming IDS (DM10d,e,f)

Remarks:  
In case of an IBPR reader entering "7" or a PIN code must be completed by typing "E" or "#"

### Modèle de porte MP14 - Armement



### Modèle de porte MP14 - Désarmement



## 20.13

### Ports d'Access PE

Les processus et applications dans Access PE utilisent les ports suivants.

Connexion entre...	Client/AMC	Serveur
Client - LacSp	Non défini	43434/tcp
AcPers - CP	Non défini	20005/tcp
LacSp - AMC	10001/udp	54545/udp et supérieur

## 21 Types de PIN

Access Professional Edition permet d'affecter à chaque détenteur de carte jusqu'à trois numéros d'identification personnels (**PIN**) :

- **PIN de vérification**

Ce PIN peut être demandé aux détenteurs de carte comme mesure de sécurité supplémentaire à des entrées spéciales. Le PIN de vérification est comparé aux données enregistrées pour le détenteur de la carte pour vérifier que celui-ci est bien le propriétaire de la carte présentée.

Chaque personne peut choisir son propre code PIN composé de 4 à 8 chiffres à condition de respecter certaines règles générales (par ex., pas de séquences numériques ni de palindromes). [Le paramètre définissant la longueur du PIN est tout aussi valable pour les codes PIN de vérification, d'armement et de la porte]. Un PIN de vérification ne doit pas obligatoirement être unique au sein du système.

Si aucun PIN d'armement distinct n'a été défini [c.-à-d. tant que la case **utiliser un code PIN IDS distinct** n'est pas cochée dans la boîte de dialogue Configurateur > Paramètres], le PIN de vérification peut également être utilisé pour armer/désarmer l'IDS.

- **PIN d'armement/PIN IDS**

Ce PIN spécial est exclusivement utilisé pour armer et désarmer le système d'alarme. Pour les modèles de porte 10 et 14, appuyez d'abord sur la touche 7 du clavier ou sur le bouton-poussoir de la porte.

Chaque personne peut choisir son propre code PIN composé de 4 à 8 chiffres à condition de respecter certaines règles générales (par ex., pas de séquences numériques ni de palindromes). [Le paramètre définissant la longueur du PIN est tout aussi valable pour les codes PIN de vérification, d'armement et de la porte]. Un PIN d'armement ne doit pas obligatoirement être unique au sein du système.

Si le détenteur de carte souhaite juste franchir la porte et que la saisie d'un code PIN est nécessaire, il peut utiliser le PIN de vérification. Si la case **utiliser un code PIN IDS distinct** est cochée (Configurateur > Paramètres généraux), le PIN de vérification ne peut plus être utilisé pour armer/désarmer l'IDS. C'est seulement lorsque cette case est cochée que les champs de saisie correspondants s'affichent dans la boîte de dialogue du personnel.



### Remarque!

Pour garantir la compatibilité avec les versions précédentes d'Access PE, la case « utiliser un code PIN IDS distinct » est désactivée par défaut.

- **PIN d'identification/PIN d'ID**

Ce code PIN identifie la carte d'une personne et doit donc être unique au sein du système. Une fois saisi, ce code PIN accorde l'accès à la personne conformément aux autorisations qui ont été définies. Pour garantir que le code PIN n'est pas déjà utilisé, celui-ci est généré par le système et attribué à la personne conformément aux règles générales (pas de séquences numériques ni de palindromes).

Tout comme un badge physique, le PIN d'identification applique les restrictions attribuées à son propriétaire (blocages, modèles horaires, autorisations, etc.).

Selon le protocole du lecteur, vous devez saisir le PIN d'identification sur le lecteur, ainsi que les caractères supplémentaires requis. Dans le cas des lecteurs, saisissez le PIN de la manière suivante : **4 # (Entrée) PIN # (Entrée)**. Pour tous les autres protocoles, vous pouvez saisir le PIN directement suivi de **# (Entrée)**.

La longueur de ce PIN peut être configurée pour contenir entre 4 et 8 chiffres.

**[Remarque :** la longueur requise pour les codes PIN d'identification doit être déterminée en fonction de la taille du site de manière à rendre les codes PIN actifs plus difficiles à deviner. Par exemple, si le site regroupe 1 000 détenteurs de carte, les codes PIN doivent contenir au moins 6 chiffres de manière à ce que la probabilité pour que quelqu'un devine un PIN valide soit réduite au maximum et que les codes PIN saisis au hasard aient de grandes chances de déclencher des alarmes.]

Tous les types de PIN décrits ci-dessus sont spécifiques aux individus et sont par conséquent définis et mis à jour en même temps que les autres données du personnel. Il existe un quatrième type de PIN baptisé « PIN de la porte ».

– **PIN de la porte**

Ce PIN correspond à une entrée (Configurateur > Entrées). Toutes les personnes autorisées à utiliser l'entrée doivent le connaître. Une carte peut être utilisée à la place du PIN pour accéder à ce type d'entrée (voir = Option **PIN ou carte**).

Ce code PIN peut lui aussi contenir entre 4 et 8 chiffres. Si l'utilisation du PIN de la porte est désactivée, (par ex., par un modèle horaire), l'accès est uniquement possible sur présentation d'une carte. La saisie d'un PIN d'identification ne fonctionnera pas non plus dans un tel cas.



**Remarque!**

Les codes PIN d'identification et PIN de la porte ne peuvent pas être utilisés avec les modèles de porte 10 et 14 avec armement de l'IDS.

## 22

### Exigences UL 294

Les lecteurs de carte Bosch suivants ont été évalués par UL par rapport à leur compatibilité avec le système logiciel APE-SW de Bosch :

- LECTUS secure 1000 WI
- LECTUS secure 4000 WI
- LECTUS secure 5000 WI

**Fonctionnalités évaluées par UL :**

- Lecteurs au format Wiegand 26 bits
- Contrôleurs AMC2 :
  - APC-AMC2-4WCF
  - API-AMC2-4WE
  - API-AMC2-8IOE
  - API-AMC2-16IOE
- APE-SW en tant qu'équipement de surveillance supplémentaire

**Fonctionnalités non évaluées par UL :**

- Système vidéo du système
- Visionneur de plan et gestion des alarmes avec vérification de plans et de vidéos
- Lecteur vidéo
- Badge Designer
- Lecteurs Delta 1200 Series
- Lecteurs Rosslare ARD-1200EM Series
- Contrôleurs LAC
- Contrôleurs LACi
- Contrôleurs APC-AMC2-4R4CF
  - Protocole d'interface du lecteur BG 900
  - Protocole d'interface du lecteur L-BUS
- Armement/désarmement de l'IDS du système de sécurité
- Ascenseur
- Textes
- Alarme d'effraction









**Bosch Security Systems B.V.**

Torenallee 49  
5617 BA Eindhoven  
Netherlands

**[www.boschsecurity.com](http://www.boschsecurity.com)**

© Bosch Security Systems B.V., 2019