CAC Server

Manuel CAC Server
Code 97307 V01_08

FRANÇAIS

CE

SOMMAIRE

ARCHITECTURE système CAC

Une installation de contrôle d'accès CAC se compose d'une partie matérielle : centrales CAC, lecteurs, décodeurs, etc., et d'une partie logicielle qui permet de configurer et gérer l'installation.

Pour ce qui est de la gestion logicielle de l'installation, l'application CAC dispose de plusieurs applications qui vont permettre de configurer et gérer les différentes options et possibilités qu'elle offre.

Ces applications sont divisées en « applications serveur » et en « applications client ».

- ***Applications serveur*** :

  · **CAC Server** : il s'agit de l'application où l'installateur définit les éléments matériels de l'installation. Elle joue également le rôle de serveur pour le reste des applications client de l'architecture CAC et de serveur de communications avec l'installation CAC.

  Le PC sur lequel est installée l'application CAC Server devra être directement connecté à l'installation par le biais de l'interface appropriée (voir rubrique connexions PC-centrale).

  · **CAC Database Server** : il s'agit de l'application qui gère la base de données où sont stockées toutes les informations relatives à l'installation (utilisateurs, incidences, etc.) à partir de laquelle se fournissent toutes les autres applications utilisateur et même l'application CAC Server.

  Toute l'installation CAC ne doit disposer que d'une seule application CAC Server et CAC Database.

- ***Applications client*** : ce sont les applications développées par l'utilisateur qui permettent d'exploiter au maximum les fonctions offertes par le système CAC par le biais d'une interface graphique simple et très intuitive, qui permet d'agir sur l'installation, de consulter, visualiser les informations relatives à l'installation (événements, utilisateurs, etc.), et le tout en mode en ligne/hors ligne grâce aux applications serveur.

  Il existe plusieurs applications client, chacune d'entre elles se focalise sur la gestion et le contrôle de fonctions du système CAC déterminées.

  De cette manière, chaque utilisateur dispose d'une ou plusieurs applications client selon les fonctions du système CAC que l'on souhaite utiliser. La gestion de l'installation du contrôle d'accès se révèle ainsi très simple et structurée.

  En outre, grâce à l'architecture utilisée dans le CAC, chaque application client peut être installée sur un ou plusieurs ordinateurs du même réseau, puisqu'il s'agit d'applications multiposte.

Observations importantes concernant la structure du système CAC

Lors de l'utilisation aussi bien du logiciel serveur que du logiciel client, il faut prendre en compte les indications suivantes :

• Lorsqu'il faudra gérer l'installation par le biais de l'application CAC Server (nouvelle installation, ouverture de l'installation, modification de l'installation), il se peut que des situations incohérentes se produisent au niveau de l'application CAC Access si celle-ci est ouverte en même temps. ***Il faut que toutes les requêtes des applications client soient fermées avant d'effectuer toute modification au niveau du serveur.***

• Une situation similaire peut avoir lieu lorsque 2 requêtes de CAC Access sont exécutées simultanément pour un même profil (administrateur, profil, opérateur). Il vaut mieux utiliser chaque requête pour un profil utilisateur différent.

Configuration et topologies du système CAC

L'utilisation du serveur d'applications CAC rend possible une architecture client-serveur possédant les avantages suivants :

- Possibilité de gérer l'installation à partir de n'importe quel PC connecté au même réseau informatique que le serveur.
- Le serveur peut être installé dans une zone sûre afin de protéger l'accès à ce dernier et d'en garantir la sécurité.
- Gestion simultanée à partir de différents PC (la même application de l'utilisateur est installée sur plusieurs équipements).
- Les différentes applications peuvent être exécutées avec le même ordinateur ou à partir d'ordinateurs différents.

L'ordinateur qui agit en tant que serveur doit être connecté à l'installation du contrôle d'accès par le biais d'un des moyens supportés : connexion série locale (RS-232 / RS-485) ou connexion à distance (IP).

Au cas où les applications client seraient installées sur des ordinateurs autres que celui où est installé le serveur, ce dernier ddevrait travailler sans interruption. Il est donc conseillé de le protéger par un système d'alimentation ininterrompue (SAI) et de l'installer dans une zone restreinte.

La base de données de l'installation (CAC Database) contient des informations relatives aux équipements installés, autorisations des utilisateurs et incidences qui se produisent. Elle peut être installée sur le même ordinateur que le serveur ou sur un autre, en fonction du niveau de sécurité que l'on souhaite avoir.

Les différentes possibilités de l'installation peuvent être observées sur les illustrations ci-dessous :

- Option 1. L'on emploie un ordinateur en tant que serveur et en tant que gérant de la base de données.

  Les différentes applications communiquent entre elles via réseau local. Il s'agit du cas le plus complexe, mais aussi le plus sûr puisque les deux ordinateurs peuvent être protégés. Le fait que la base de données soit séparée du serveur permet d'intégrer les informations dans d'autres bases de données de l'entreprise, ce qui facilite ainsi les opérations de sauvegarde.

- Option 2. L'ordinateur qui agit en tant que serveur contient la base de données et les applications utilisateur sont contrôlées à partir des autres ordinateurs.

  Il s'agit d'une simplification de l'option 1 avec laquelle le niveau de sécurité n'est en aucun cas diminué.

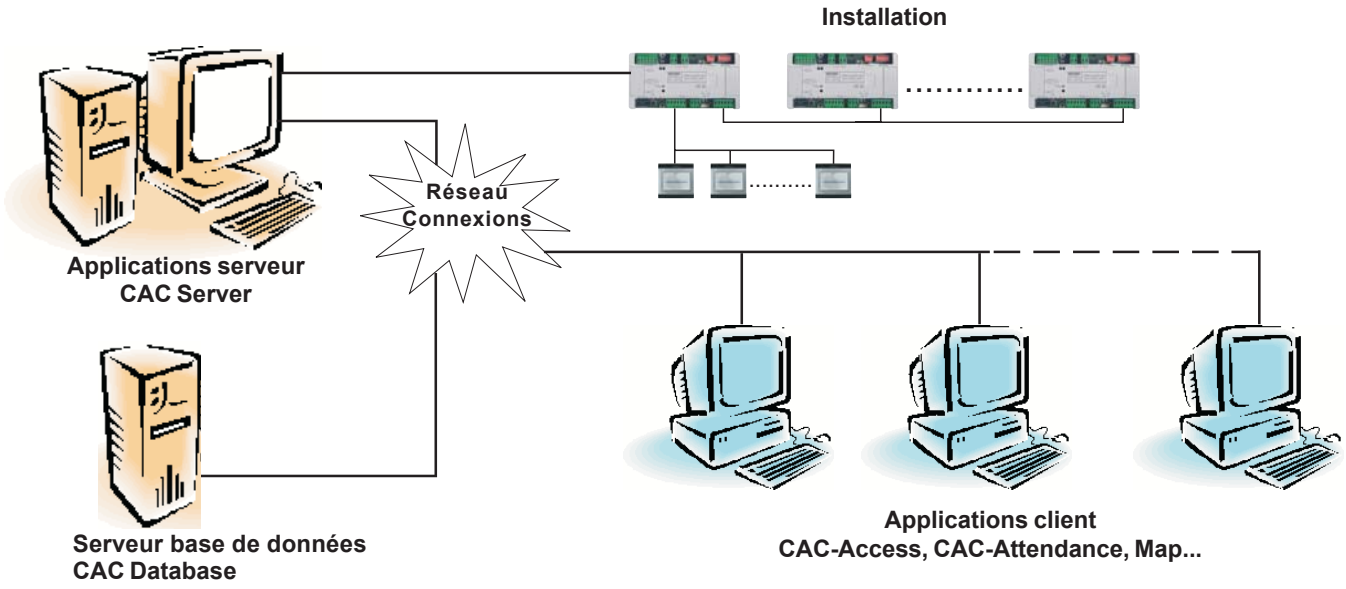
- Option 3. Toutes les applications (serveur et base de données) sont supportées par le même ordinateur.

  Il s'agit du cas le plus simple, pour lequel un réseau local n'est pas nécessaire. Cette situation a lieu lorsqu'il n'y a qu'un opérateur.

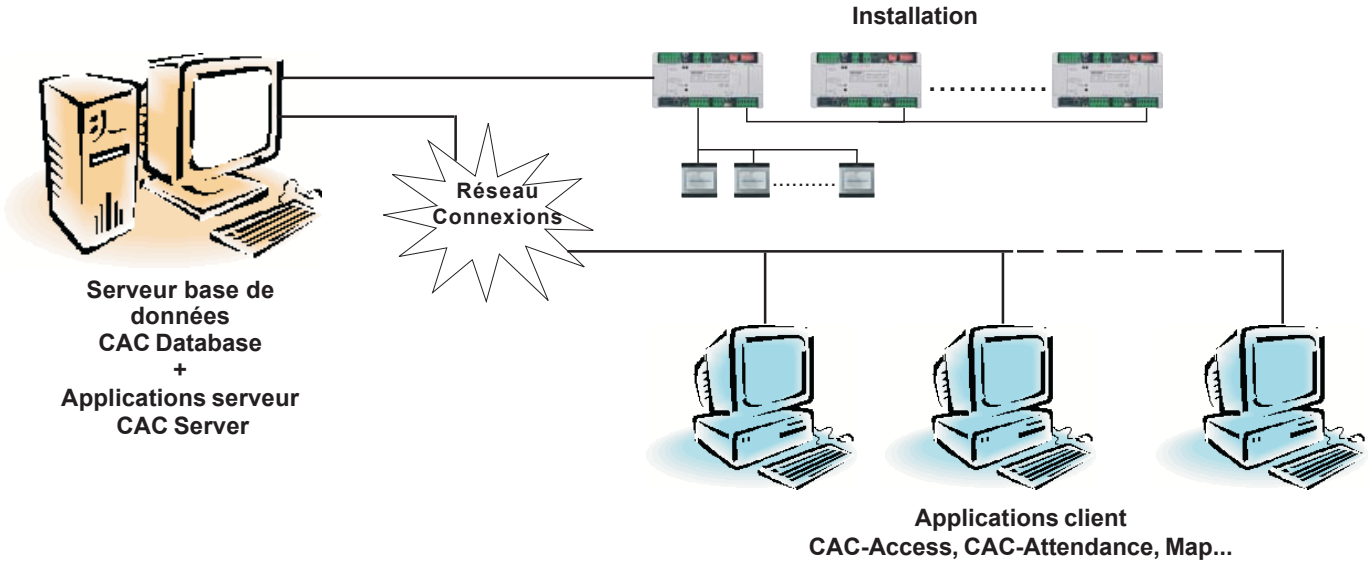
Vous trouverez en fin de manuel une annexe où sont présentés les schémas de connexion de réseau entre centrales (réseau FXL) et la connexion entre le PC et l'installation.

Options d'installation du système

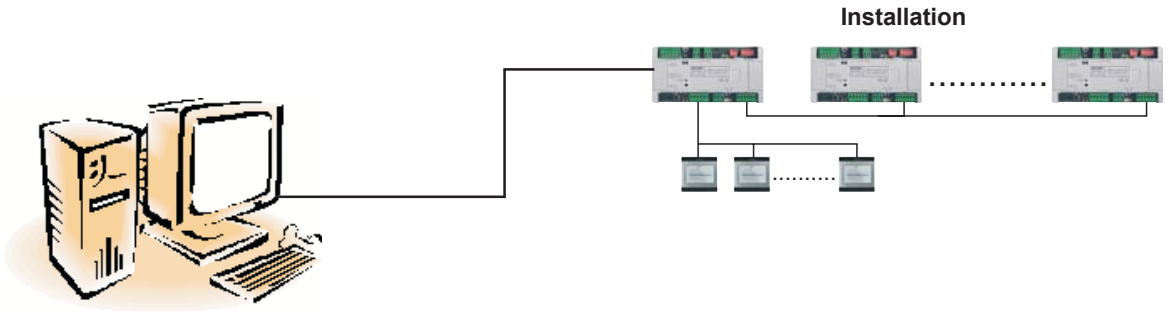
- Option 1



- Option 2



- Option 3



Caractéristiques du système CAC

- 2 048 utilisateurs du contrôle d'accès
- Gestion de 64 unités centrales et 32 portes par centrale maximum avec la possibilité de les regrouper en 4 sections différentes (voir rubrique sections).
- Gestion des identifiants (comptes utilisateurs) pour accéder aux applications serveur et client.
- Test des dispositifs installés (centrales, lecteurs...)
- Traitement spécifique pour les portes véhicules. Parkings.
- 64 groupes d'utilisateurs (profils). Chacun définit les restrictions qui s'appliquent au groupe grâce à l'attribution de 3 secteurs et 3 horaires maximum.
- 4 profils spéciaux sans restriction.
- 32 secteurs. Ils définissent les portes au niveau desquelles l'accès est autorisé.
- 32 horaires. Ils définissent les périodes pendant lesquelles l'accès des utilisateurs est autorisé.
- Vacances (20 jours fériés et 3 périodes de vacances). Touche tous les profils sauf les profils spéciaux.
- Liste des 3 000 dernières incidences (entrées, sorties, accès refusés, alertes, etc.) pour chaque centrale. Lorsque le serveur est en marche, il n'y a pas de limitation.
- 1 000 platines d'intercommunication / 1 000 capteurs / 1 000 relais par centrale.
- 32 plans hebdomadaires d'activation des dispositifs (capteurs et relais).
- Limitation du nombre de personnes dans des pièces ou locaux déterminés.
- Contrôle de présence (localisation des personnes) pour les sorties d'urgence.
- Verrouillage / déverrouillage des portes.
- Blocage temporaire des utilisateurs de manière individuelle ou par groupes. L'accès n'est pas autorisé tant qu'il y a blocage.
- Passage automatique à l'heure d'hiver/d'été.
- Fonction unicité des passages (antipassback) globale.
- Activation des dispositifs associés à chaque utilisateur en présentant son identificateur au lecteur.
- Activation des relais à partir d'un lecteur avec clavier et lecteur de proximité. Connexion et déconnexion des alarmes.
- Test continu des dispositifs.
- Interaction du logiciel du PC avec l'installation : ouverture des portes, verrouillage/déverrouillage des portes, blocage des utilisateurs, etc.

Conditions minimales requises

Pour pouvoir lancer l'application, les conditions suivantes sont requises :

	Conditions minimales requises	Recommandé
Equipement	IBM ou PC compatible PIII	IBM PC ou compatible PIV ou supérieur
Système d'exploitation	W2000	WXP
Mémoire RAM	128 Mb	512 Mb
Port	1 série RS-232	1 série RS-232
Disque dur	100 Mb d'espace libre	100 Mb d'espace libre

DÉFINITION DES CONCEPTS

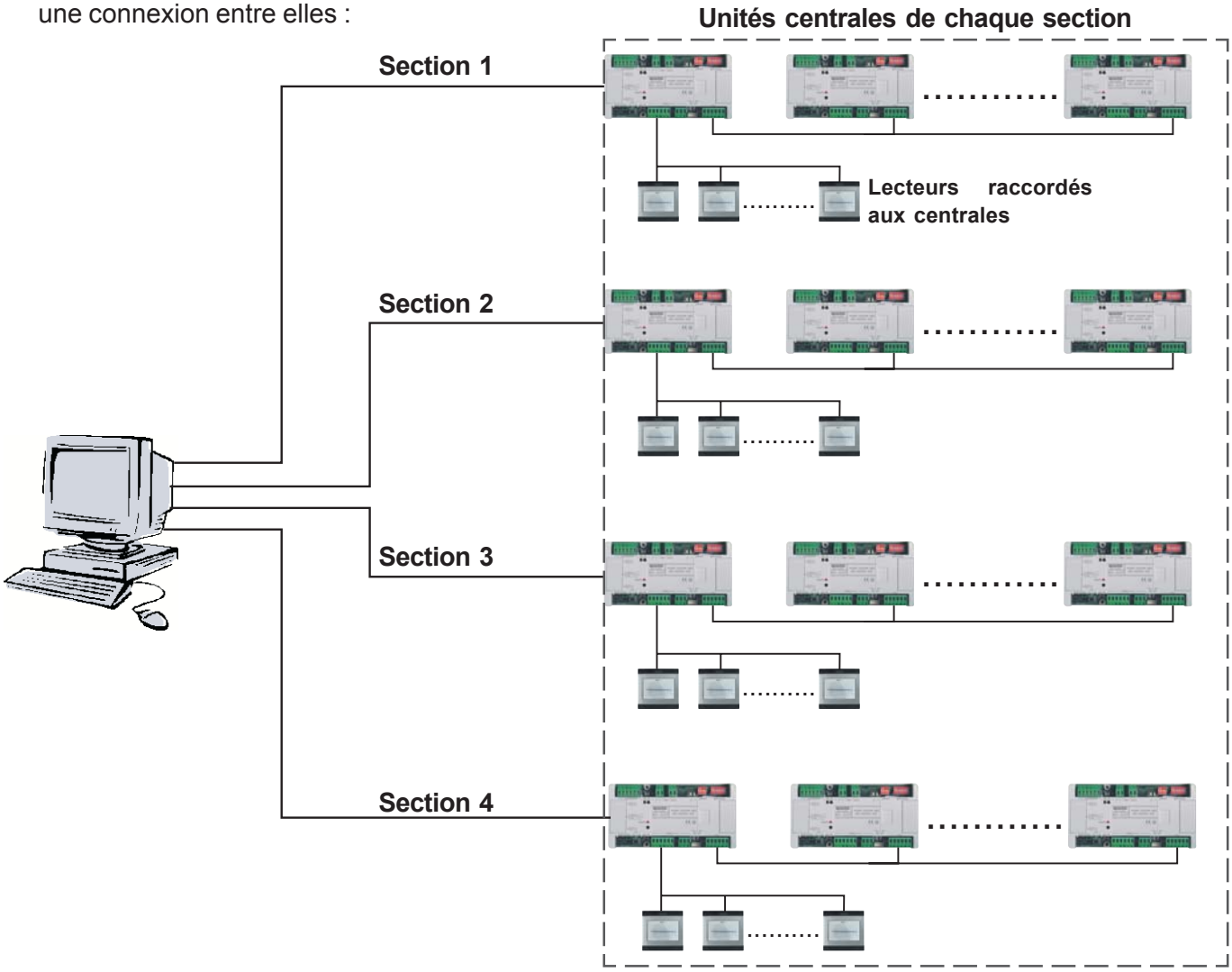
**** Sections***

L'application CAC Control Server permet d'organiser l'installation en sections/divisions (4 sections différentes maximum).

Dans les installations possédant un nombre de centrales élevé ou où les centrales sont fort éloignées les unes des autres, la création de sections permet de gérer toutes les centrales à partir du même PC, sans avoir à relier via réseau FXL toutes les centrales entre elles en créant de la sorte une seule installation.

Pour cela, il faut seulement relier via réseau FXL les centrales appartenant à une même section et connecter chaque section au PC par le biais de l'interface PC-centrale correspondante (2338, 2466, 1086 terminal gestion à distance IP, etc.)

De cette façon, le PC sert de concentrateur des centrales en permettant à toutes les centrales d'avoir une connexion entre elles :



Important :

- Toute installation CAC aura au moins une section.
- Le nombre maximal de centrales est de 64, indépendamment du nombre de sections existantes.
- La connexion entre les centrales d'une même section s'effectue par le biais du réseau FXL.
- Chaque section est physiquement connectée aux ports de l'ordinateur où est installée l'application CAC Server. La connexion peut être effectuée par :
  - · Ports série RS232 : interface RS232-485, réf.2338 ou 2466 nécessaire.
  - · Réseau local : interface terminal de gestion à distance IP, réf. 1087 + réf. 2466 nécessaires.

*** *Centrales CAC***

Une installation de contrôle d'accès CAC aura de 1 à 64 centrales CAC.

Chaque centrale est insérée dans l'application CAC Control Server dans la section correspondante. Une description et un numéro lui sont assignés.

Ce numéro doit coïncider avec le numéro attribué à la centrale par le biais des commutateurs DIP de 1 à 5 du microrupteur SW2.

*** *Portes***

Une porte correspond à chaque lecteur ou contrôleur de porte (CP) de l'installation. Chaque CP peut gérer jusqu'à 2 lecteurs (entrée/sortie) de la même porte.

En fonction des autorisations d'accès, définies ultérieurement par le biais de l'application utilisateur CAC Access, les utilisateurs pourront accéder à l'installation par certaines portes ou par d'autres.

Dans l'application CAC Control Server, et ce pour chaque centrale, autant de portes que de lecteurs ou CP connectés à la centrale dans l'installation (de 1 à 32 lecteurs ou CP par centrale) sont ajoutés.

Pour chaque porte, il faut configurer divers paramètres selon le type de porte (lecteur ou CP) et leur fonction au sein de l'installation. Il est indispensable d'attribuer une description et un numéro d'accès.

Ce numéro d'accès doit coïncider avec le numéro assigné au lecteur ou CP via les commutateurs DIP de configuration du lecteur ou CP.

*** *Zones***

Il ne sera nécessaire de définir les zones que lorsque l'on souhaitera une ***limitation du nombre de personnes*** (contrôle de la capacité) ou la fonction de ***localisation des utilisateurs***.

Afin de mettre en place ces fonctions, il faut définir pour chaque porte :

- la zone à laquelle l'on accède (entrée) et la zone que l'on quitte (sortie) en traversant la porte,
- pour une limitation du nombre de personnes, indiquez si la porte a une influence quelconque sur la zone.

Il est possible de créer jusqu'à 32 zones différentes et chacune possède son propre compteur. Les informations sur le nombre de personnes et la zone où l'on trouve un utilisateur sont enregistrées dans une mémoire non volatile de sorte que, s'il y a une remise à zéro ou une coupure de la centrale, ces informations ne seront pas perdues.

Nombre de personnes limité : pour cette fonction, il faut en outre définir dans la zone la capacité maximale des utilisateurs et le relais que l'on doit activer au cas où l'on atteindrait cette capacité (facultatif).

Le système CAC contrôle le nombre de personnes, en ajoutant 1 au compteur de la zone lorsqu'un utilisateur accède à une zone par le biais d'une porte définie en tant qu'accès à cette zone ou en soustrayant 1 lorsque l'utilisateur abandonne la zone par le biais d'un accès défini en tant que sortie de la zone (ces paramètres sont définis au niveau de chaque porte).

Lorsque la capacité maximale de la porte est atteinte, l'accès à plus d'utilisateurs (bien que disposant de l'autorisation d'accès nécessaire) n'est pas autorisé tant qu'un utilisateur ne sera pas sorti de la zone.

Il est possible de réinitialiser la capacité de la zone, c'est-à-dire mettre le compteur de la zone à zéro, en réinitialisant, au niveau de la porte d'accès à cette zone, un badge de proximité défini (par le biais de l'application CAC Access) en tant que « réinitialisation de la capacité ». De cette façon, de nouveaux utilisateurs (outre ceux qui se trouvent déjà dans la zone) peuvent y accéder jusqu'à ce que la capacité maximale soit de nouveau atteinte.

Il est également possible de réinitialiser le nombre limite de personnes à partir de l'application CAC Access.

L'on peut aussi définir une capacité « 0 ». Dans ce cas, le nombre d'utilisateurs dans la zone n'est pas restreint puisque le relais sélectionné s'active tant qu'il y a un utilisateur.

Localisation des utilisateurs : le contrôle de la localisation des utilisateurs permet de savoir à tout moment où se trouve chaque utilisateur afin de pouvoir lui transmettre une information par le biais du poste le plus proche ou afin d'évacuer l'immeuble en cas d'incendie (*Roll Call*).

Le système CAC sait dans quelle zone se trouve un utilisateur en vérifiant quelle a été la dernière porte par laquelle est passé l'utilisateur. Comme mentionné précédemment, la zone à laquelle on a accès et la zone que l'on quitte sont définies pour chaque porte.

La fonction de localisation des utilisateurs est disponible sur l'application client CAC Map.

*** *Unicité des passages (antipassback)***

La fonction unicité des passages ou antipassback empêche un utilisateur qui accède à l'installation par une *porte d'entrée* d'entrer de nouveau dans l'installation (par n'importe quelle autre porte d'entrée) sans avoir quitté l'installation par une *porte de sortie*.

De cette façon, l'on évite que plusieurs personnes puissent accéder à l'installation avec un même dispositif ou, pour les parkings, que plusieurs voitures puissent entrer avec le même identificateur ; l'installation est ainsi pourvue d'un plus grand niveau de sécurité.

Le système CAC permet d'effectuer la fonction unicité des passages très simplement et au niveau de toute l'installation. Pour ce faire, il faut juste définir le périmètre de l'installation où l'on souhaite mettre en place cette fonction.

Le périmètre de l'installation est défini par les portes de l'installation configurées en tant qu'***entrée dans le périmètre*** ou ***sortie du périmètre*** de l'installation.

Par conséquent, pour mettre en place la fonction unicité des passages pour chaque porte faisant partie du périmètre, il faut indiquer s'il s'agit de portes permettant d'***entrer*** dans ce périmètre ou d'en ***sortir***.

Deux niveaux d'unicité des passages : piétons et véhicules

Afin d'augmenter le niveau de sécurité, le système CAC intègre deux niveaux d'unicité des passages : une voie piétonne et une autre pour véhicules ; l'un des deux s'applique automatiquement en fonction du type de porte par lequel l'on accède au périmètre de l'installation.

Accès par une porte piétonne :
Lorsqu'un utilisateur entre dans le périmètre (par une porte piétonne définie en tant qu'entrée), il est considéré comme étant « à l'intérieur » de l'installation et il ne lui est plus permis de traverser de porte d'entrée au périmètre qu'il s'agisse d'une porte piétonne ou d'une porte pour véhicules.

Il lui est en revanche permis de passer par des portes de sortie ou des portes qui n'appartiennent pas au périmètre.

S'il passe par une porte de sortie, il est considéré comme étant «hors de l'installation» et il ne pourra y accéder de nouveau que par une porte d'entrée.

Accès par une porte véhicules :
Si, dans le cas contraire, l'utilisateur accède au périmètre par une porte véhicules, le système ***considère l'utilisateur et son véhicule comme étant à l'intérieur de l'installation***. Il ne pourra donc pas entrer de nouveau par une porte véhicules à moins qu'il ne sorte par une sortie véhicules.

Il peut en revanche passer par une porte de sortie ou par l'une des portes n'appartenant pas au périmètre.

Au cas où l'utilisateur sortirait par une porte de *sortie piétonne*, il ne pourrait entrer de nouveau dans le périmètre que par une porte d'entrée piétonne et non par une entrée pour véhicules puisque le véhicule se trouve toujours à l'intérieur de l'installation.

*** *Groupes de capteurs - capteurs individuels***

Il ne sera nécessaire de définir des groupes de capteurs ou des capteurs individuels que s'il y a des décodeurs de capteurs dans l'installation ou si l'une des fonctions suivantes associées à l'activation d'une ou plusieurs entrées de capteur est requise :

- Activation d'un dispositif (au moyen du décodeur de relais ou relais du contrôleur de porte).
- Envoi du message à la centrale de conciergerie.
- Identification du capteur activé dans le journal des incidences.
- Utilisation des capteurs dans le processeur.

*** *Groupes de relais - relais individuels***

Il ne sera nécessaire de définir les groupes de relais ou relais individuels que lorsqu'il y a des décodeurs de relais dans l'installation et qu'une des fonctions suivantes est requise :

- Activation de la gâche électrique au moyen d'un décodeur de relais (pour que l'installation soit plus sûre).
- Associé à un capteur : activation d'un dispositif après la détection d'un capteur.
- Activation du dispositif d'un utilisateur.
- Activation des dispositifs à partir des lecteurs à clavier raccordés au contrôleur de porte.
- Activation d'un relais pour la limitation du nombre de personnes dans une zone.
- Utilisation des relais dans le processeur.

*** *Processeur***

Permet de définir jusqu'à 32 plans d'automatisation pour le contrôle des dispositifs.

Les paramètres suivants sont définis dans chaque plan :

- horaire début-fin du plan (horaire début et fin de l'activité d'un dispositif),
- jours de la semaine pendant lesquels le plan est en marche,
- s'il doit fonctionner les jours fériés,
- s'il doit être synchronisé après une réinitialisation de la centrale,
- sélectionnez la fonction à effectuer :
  - · activation/désactivation du relais de porte auxiliaire d'un contrôleur de porte,
  - · activation/désactivation d'un relais de décodeur,
  - · activation/désactivation du capteur de décodeur.

*** *Contrôle anti-sabotage***

Permet d'activer la fonction de détection anti-sabotage du bus de décodeurs (où sont connectés les décodeurs de relais, décodeurs de capteurs ou décodeurs de platines pour l'intercommunication).

Pour cela, il faut indiquer le type de décodeur installé sur l'extrémité du bus et l'adresse programmée sur l'une des sorties.

Si lors du processus de vérification du statut du bus de décodeurs qu'effectue la centrale toutes les 60 secondes, la centrale ne détecte pas l'adresse de la sortie indiquée, la centrale provoque une incidence anti-sabotage qui est stockée dans le journal des incidences et un message de sabotage est envoyé à la centrale de conciergerie (s'il y en a une).

ETAPES DE MISE EN MARCHE D'UNE INSTALLATION CAC

Les étapes de configuration et de mise en marche d'une installation de contrôle d'accès CAC sont les suivantes :

1º. Installez, câblez et configurez les équipements matériels :

- **Centrales CAC.** Configurez l'adresse de chaque centrale.
- **Lecteurs.** Configurez l'adresse des lecteurs (contrôleur de porte ou contrôleur avec lecteur intégré) à l'aide des microrupteurs placés sur chacun d'entre eux.
- **Décodeurs de capteurs, relais et platines (s'il y en a).** Programmez les adresses des sorties/entrées des décodeurs et les autres paramètres à l'aide de l'application Decowin (fournie avec la centrale CAC).
- **Centrale de conciergerie (s'il y en a une).** La conciergerie possède l'adresse 0 du bus de lecteurs.

2º. Installez les applications serveur « CAC Database Server » et « CAC Control Server » sur le PC ou les PC correspondants.

Voir rubrique : **« Installation des applications Control Server et CAC Database Server »**.

3º. Lancez et configurez les applications serveur.

Voir rubrique : **« Installation des applications Control Server et CAC Database Server »**.

A partir de l'application CAC Control Server :

4º. Créez l'installation :

4.1. Créez les sections de l'installation

4.2. Ajoutez les centrales CAC qui composent chaque section.

4.3. Pour chaque centrale, configurez les éléments qui la composent.

4.3.1. Portes (lecteurs).

4.3.2. Zones.

4.3.3. Groupes de capteurs - capteurs individuels.

4.3.4. Groupes de relais - relais individuels.

4.3.5. Processeur.

4.3.6. Contrôle anti-sabotage

Dans les rubriques du manuel suivantes, il est expliqué comment l'on configure chaque élément de l'installation.

5º. Mettez à jour la date et l'heure des centrales et l'horaire d'été (voir rubrique **« panneau de contrôle »**).

8º. Mettez à jour les centrales (voir rubrique **« Mise à jour des données dans les centrales »**).

9º. Lancez les services (voir rubrique **« Lancement des services »**).

INSTALLATION des applications CAC Server et CAC Database

Comme indiqué précédemment, le système CAC a besoin de deux applications serveur (CAC Server et CAC Database) pour sa configuration et pour le correct fonctionnement des applications client.

Ces applications doivent toujours être lancées pour que les différentes applications client puissent travailler en mode en ligne (en temps réel) avec l'installation. Dans le cas contraire, les applications client travaillent en mode hors ligne et les modifications ou actions effectuées sur l'installation n'auront aucun effet tant que les applications serveur ne seront pas lancées.

L'installateur du système ne travaillera que sur l'application CAC Server par le biais de laquelle il configurera les éléments matériels de l'installation tandis qu'avec l'application CAC Database il devra en lancer les services (lancer l'application) pour que le système CAC fonctionne correctement.

Installation et configuration initiale des applications serveur

Les applications serveur CAC Database et CAC Server sont installées à partir du CD fourni avec la centrale CAC ou avec les différents logiciels client.

Les étapes permettant d'installer et de lancer pour la première fois les applications serveur correctement sont expliquées ci-dessous :

1º. Installez les applications serveur

1.1. Installez l'application Database sur l'ordinateur qui effectuera les fonctions serveur de la base de données de l'installation CAC.

1.2. Installez l'application Server sur l'ordinateur qui effectuera les fonctions serveur de communications et configuration de l'installation CAC.

Les applications Server et Database peuvent être installées sur le même ordinateur ou bien sur des ordinateurs différents, dans la mesure où ils appartiennent au même réseau.

Lors de l'installation des applications, un icone d'accès direct à chaque application apparaît sur le bureau de l'ordinateur.

Database :  Server : 

2º Lancez les applications serveur

La première fois que vous lancez les applications server, il faut, après leur installation, lancer premièrement l'application Database.

Ensuite, si les deux installations sont installées sur le même ordinateur, il ne faudra lancer que l'application Server, qui lancera automatiquement l'application Database.

Si les applications Server sont installées sur des ordinateurs différents, il faudra, chaque fois que seront lancées les applications serveur, premièrement lancer l'application Database et ensuite l'application Server. Dans le cas contraire, l'application Server annoncera que la connexion avec l'application Database n'a pu être établie.

2.1. Lancez l'application Database :

Double-cliquez sur l'accès direct du bureau ou rendez-vous sur Démarrage >> Programmes >> Fermax >> CAC Access Control System >> Server >> CAC Database Server.

Au moment de lancer l'application Database, l'on entend un avertissement sonore et l'icone de l'application apparaît sur la barre des tâches en indiquant que le serveur de la base de données est actif.

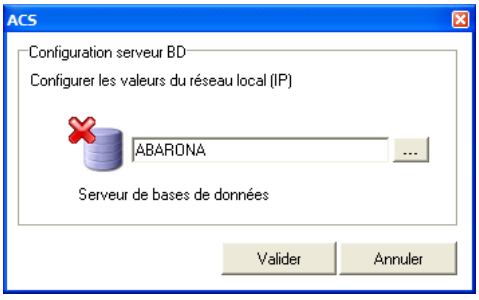
2.2. Lancez l'application Server :

Double-cliquez sur l'accès direct du bureau ou rendez-vous sur Démarrage >> Programmes >> Fermax >> CAC Access Control System >> Server >> CAC Control Server.

Si l'application Database ***n' est pas installée sur le même ordinateur***, l'écran suivant apparaît en demandant l'adresse IP ou le nom de l'ordinateur où elle a été installée :

Saisissez l'adresse IP ou le nom de l'ordinateur et cliquez sur Valider.

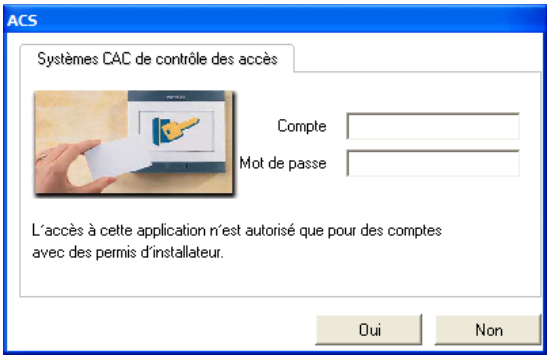
Si l'application Server ne peut établir la communication avec l'application Database, l'écran suivant apparaît.



Vérifiez que l'emplacement de l'application Database soit correct et que l'application soit lancée.

Appuyez de nouveau sur Valider.

Si le serveur réussit à établir la communication avec l'application Database, l'écran demandant l'identifiant et le mot de passe apparaît.

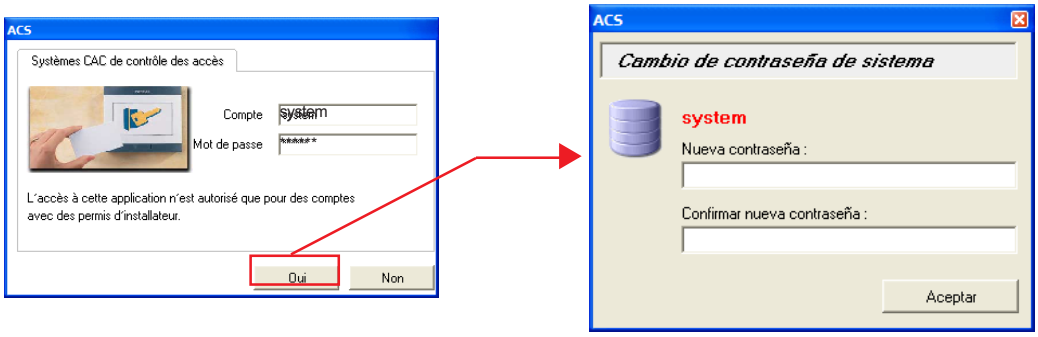


3º. Saisissez l'identifiant et le mot de passe

Saisissez l'identifiant et le mot de passe de l'installateur pour accéder à l'application Server et lancez la configuration de l'installation CAC.

Identifiant : system
Mot de passe : fermax

Un nouveau mot de passe est tout de suite demandé. Saisissez le nouveau mot de passe d'accès :

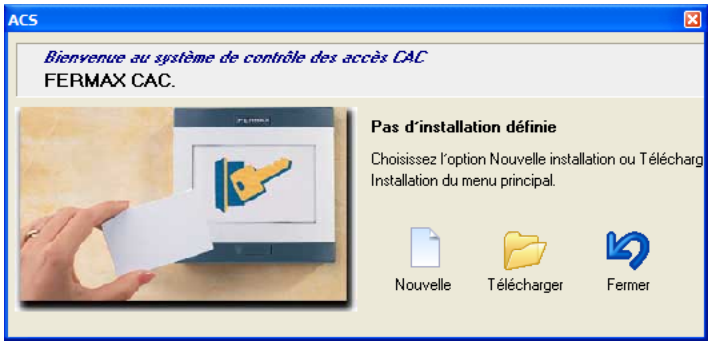


A partir de ce moment, l'accès à l'application en tant qu'installateur s'effectuera par le biais du compte utilisateur «***system*** » et le nouveau mot de passe saisi.

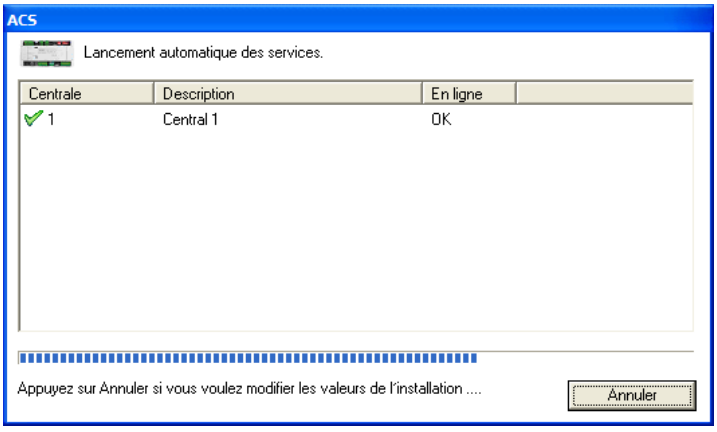
Si vous marquez de nouveau «fermax» en tant que nouveau mot de passe, un nouveau mot de passe sera demandé chaque fois que l'application sera lancée jusqu' à ce qu'il soit modifié.

A partir de l'application Server, il est possible de créer de nouveaux comptes utilisateurs et mots de passe en fonction de différents niveaux d'accès aux applications serveur et client. Ce point est expliqué dans la rubrique « Gestion des comptes utilisateurs et autorisations ».

Après avoir saisi le nouveau mot de passe, l'écran principal de l'application Server et l'assistant permettant de créer une installation apparaissent :

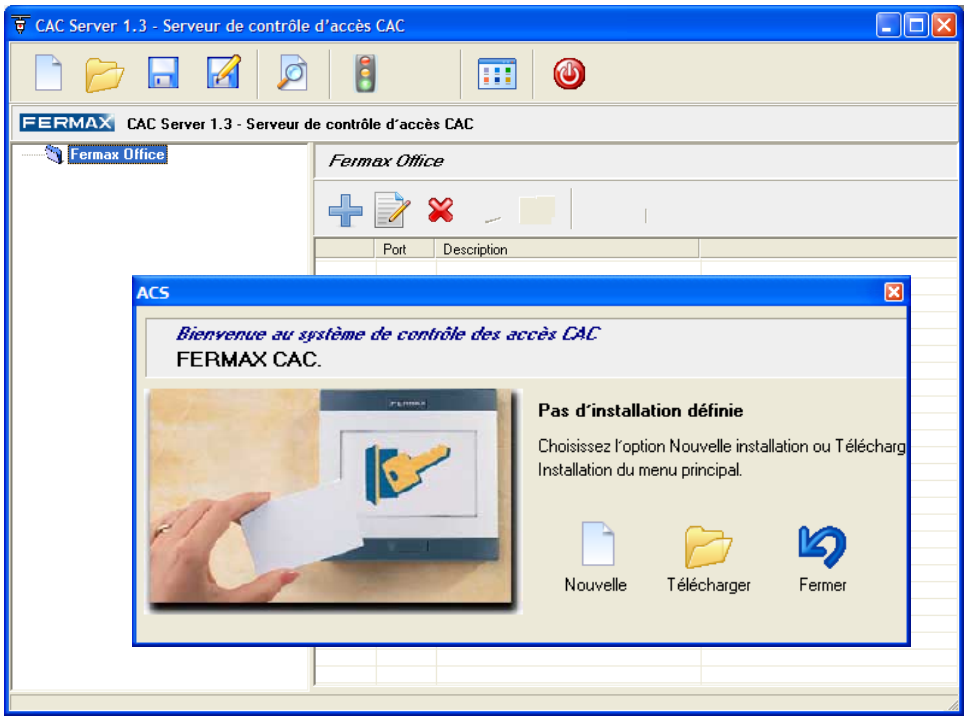


Par la suite, lorsqu'il y a déjà une installation et que l'on accède à l'application Server, un écran d'information, indiquant que l'activation des services nécessaires au correct fonctionnement des applications client commence (pour plus d'informations, consultez la rubrique « Lancer les services »), apparaît automatiquement :



CREER UNE INSTALLATION

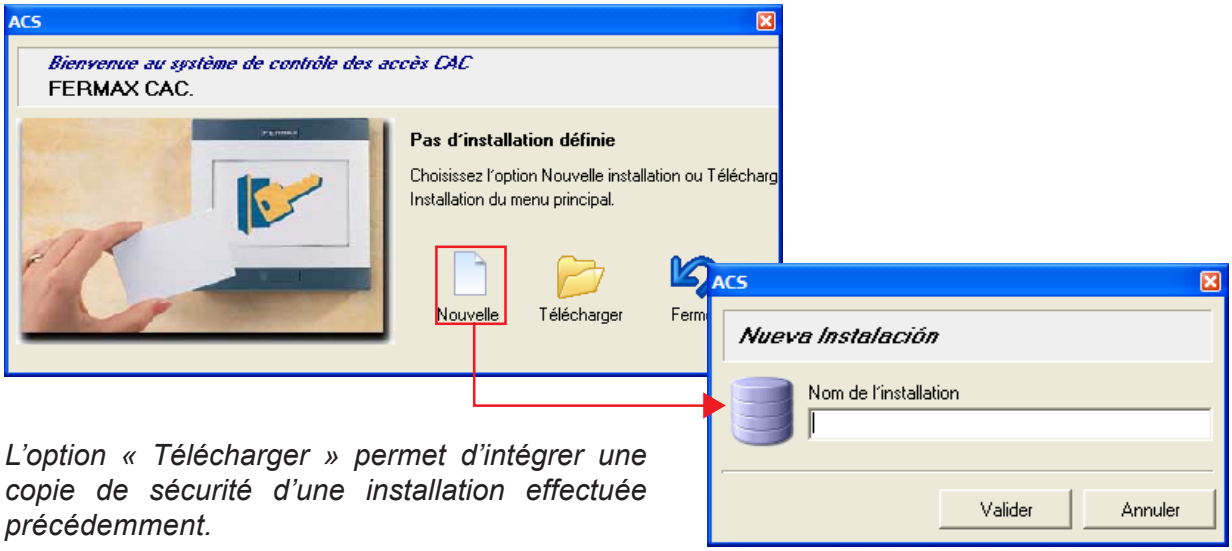
La première fois que l'on accède à l'application CAC Server (ou si l'on accède à l'application et qu'il n'y a aucune installation créée antérieurement), l'écran principal de l'application Server et l'assistant permettant de créer une installation apparaissent.



Sur une installation CAC, il faudra définir au moins une section, une ou des centrales et les lecteurs (portes) raccordés à chaque centrale.

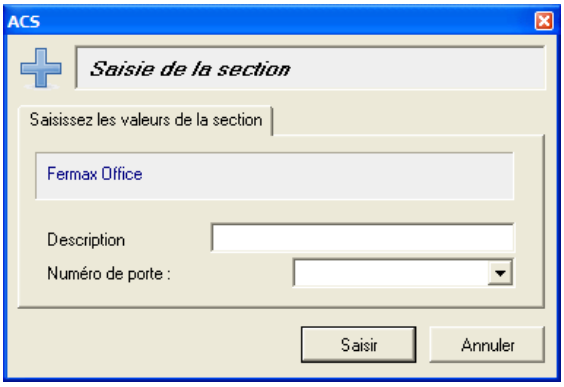
Créer une installation et ses sections

Cliquez sur le bouton « Nouvelle » et saisissez un nom pour l'installation.



L'option « Télécharger » permet d'intégrer une copie de sécurité d'une installation effectuée précédemment.

En cliquant sur « Valider », l'écran permettant de créer la ou les sections dont est formée l'installation CAC apparaît.



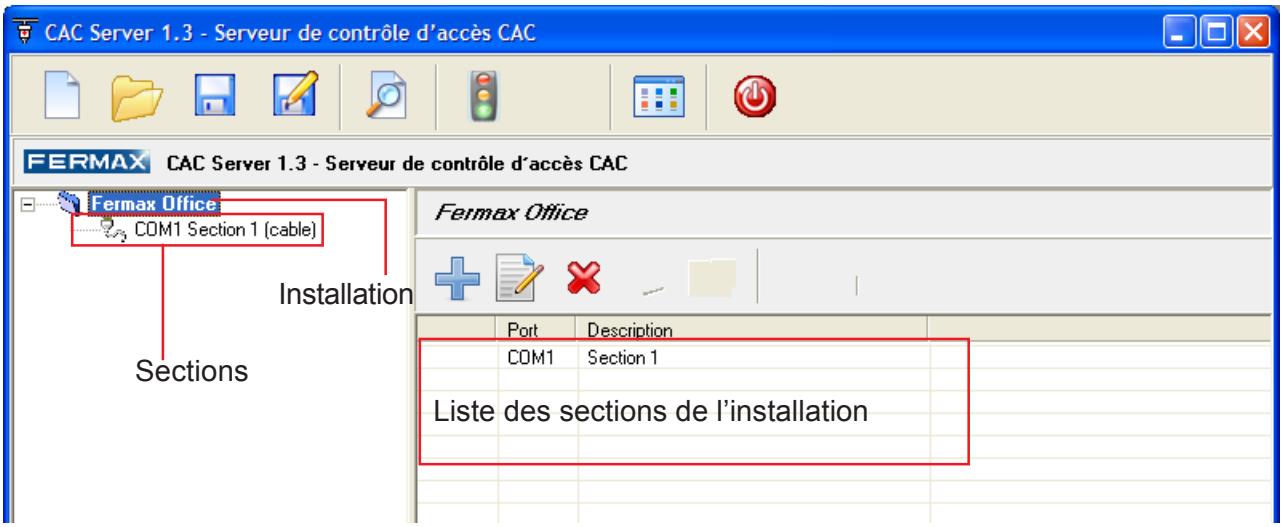
Saisissez une description pour la section et sélectionnez le port de connexions (COM) qui sera utilisé afin de raccorder la section de l'installation à l'ordinateur.

La connexion physique entre l'ordinateur, sur lequel est installé le serveur, et les centrales CAC de la section est effectuée par le biais de l'interface PC-centrale (voir rubrique « Connexion entre le PC et la centrale »).

Cliquez sur « Ajouter » afin de créer la section (les cases de modification sont vides afin de continuer à créer des sections, jusqu'à un maximum de 4).

Cliquez sur « Annuler » afin de finaliser l'ajout de sections et de montrer l'écran principal de l'application Server où l'installation et les sections créées sont présentées.

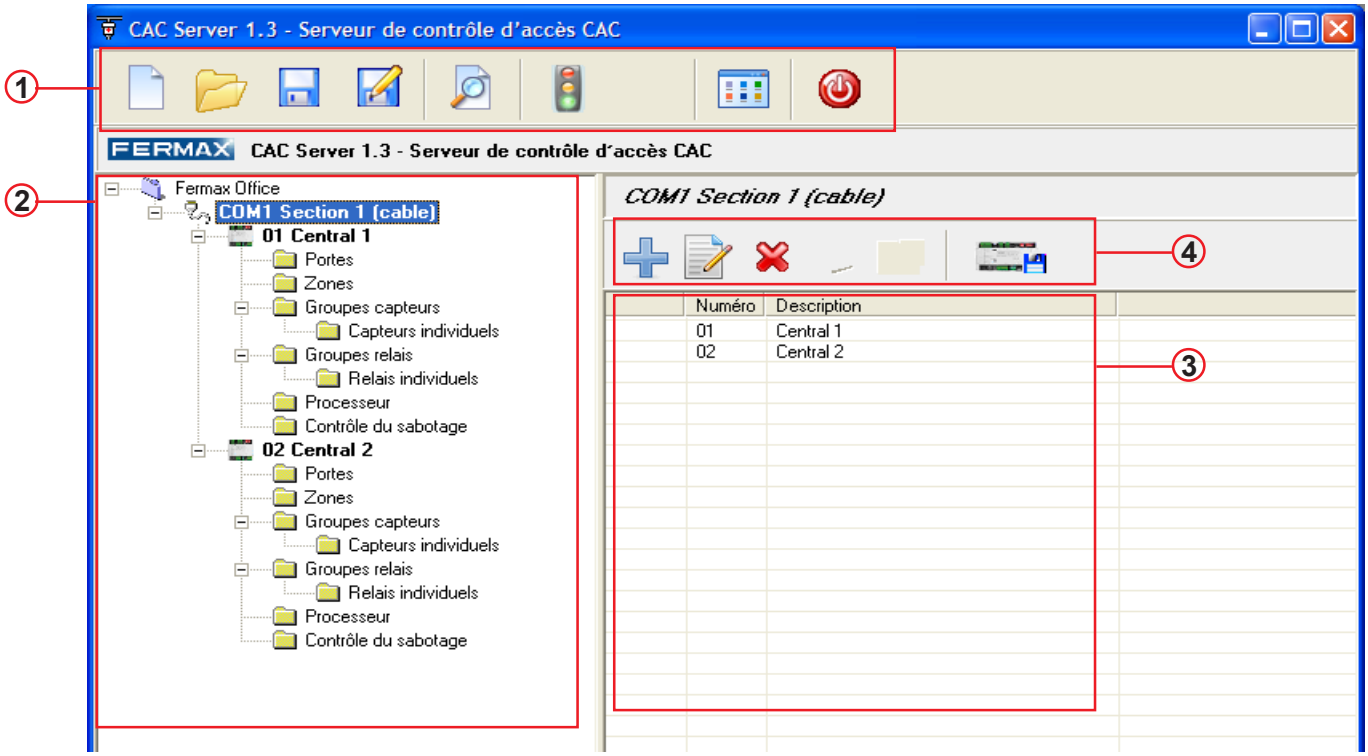
Par la suite, il est possible de supprimer ou de créer de nouvelles sections dans l'installation (voir rubrique « Ajouter/Supprimer des éléments à une installation »).



Après avoir créé l'installation et les sections, il faudra définir et configurer les différents éléments qui forment l'installation : centrales, portes, décodeurs, etc.

Avant de continuer avec la définition et la configuration des autres composants qui forment l'installation CAC, il est important d'expliquer l'écran principal de l'installation et la façon dont on ajoute, modifie et supprime les éléments d'une installation (le processus sera le même pour tout élément la composant).

ECRAN PRINCIPAL de l'APPLICATION CAC Server



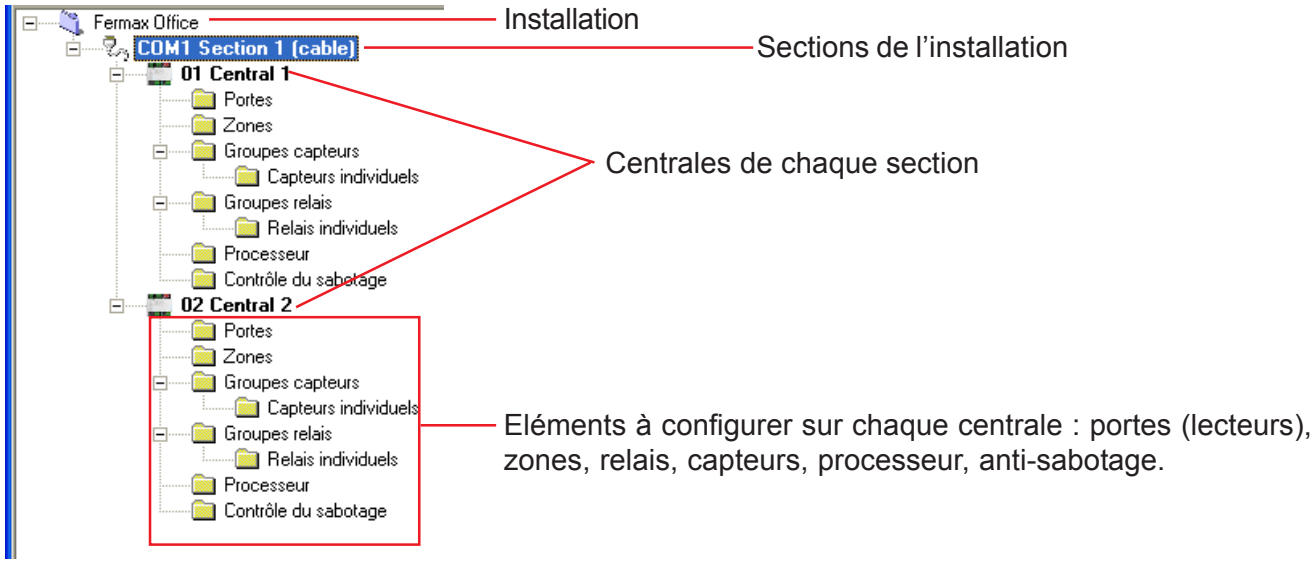
① Boutons d'utilisation générale

	Créer une nouvelle installation. *Cette action remplace l'actuelle installation.* *Il est recommandé d'effectuer une sauvegarde de l'actuelle installation avant d'en créer une nouvelle.*
	Ouvrir/télécharger la copie de sécurité d'une installation enregistrée. *Cette action remplace l'actuelle installation.*
	Créer une copie de sécurité de l'actuelle installation.
	Modifier le nom de l'installation.
	Effectuer un test de l'installation.
	Lancer les services du serveur afin que les applications client fonctionnent correctement.
	Interrompre les services lancés. Afin de pouvoir modifier l'installation, il ne faut pas que les services soient activés.
	Présente l'écran « Panneau de contrôle »
	Fermer l'application et metter fin aux services. Les applications client ne fonctionneront pas.

② Liste des composants de l'installation

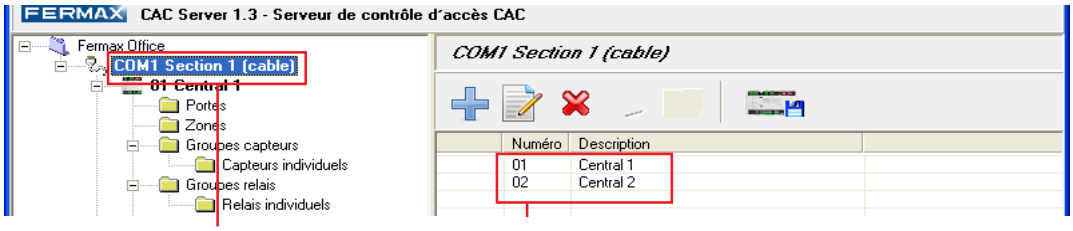
Présente une liste de tous les composants, introduits par l'installateur, qui font partie de l'installation de contrôle d'acccès.

En sélectionnant l'un des composants de l'installation, les informations relatives au composant sont présentées à droite de l'écran n° 3.



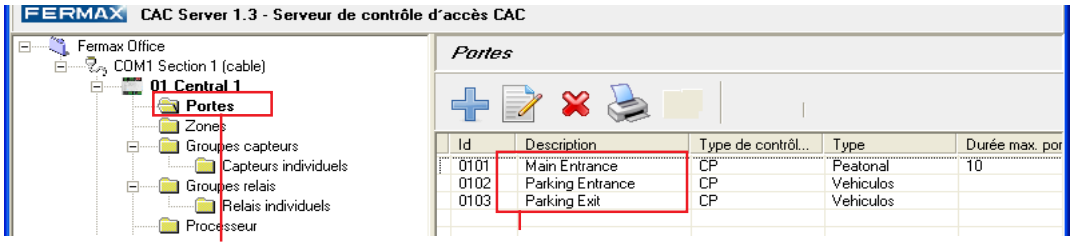
③ Liste des informations sur le composant sélectionné : éléments qui le composent

Présente les informations sur le composant sélectionné dans la « liste des composants » :



Composant sélectionné : section 1

Eléments qui composent la « section 1 » : centrales 1 et 2



Composant sélectionné : portes

Eléments qui composent les « portes » : porte d'entrée, bureaux, entrée parking, sortie parking, etc.

④ Boutons de modification des composants

Permettent d'agir sur le composant sélectionné et/ou sur les éléments qu'il contient.

	Ajouter un nouvel élément au composant sélectionné.
	Modifier l'élément sélectionné sur l'écran d'information n° 3.
	Supprimer l'élément sélectionné sur l'écran d'information n° 3.
	Imprimer la liste des éléments du composant sélectionné.
	Gestion des relais (voir rubrique relais).
	Metter à jour toutes les informations dans les centrales CAC de l'installation.

Remarque : *en fonction du composant sélectionné, l'un de ces boutons peut être désactivé.*

AJOUTER, MODIFIER ET SUPPRIMER LES ELEMENTS D'UNE INSTALLATION

Après avoir créé l'installation, l'étape suivante permettant de configurer l'installation consiste à ajouter tous les éléments qui la composent au niveau physique ou matériel (centrales, portes, décodeurs, etc.) et au niveau fonctionnel (sections, zones, processeur, etc.) afin de configurer par la suite les paramètres correspondant à chaque élément.

En plus d'ajouter des éléments à l'installation, il peut être utile à tout moment de supprimer ou modifier n'importe quel élément déjà introduit.

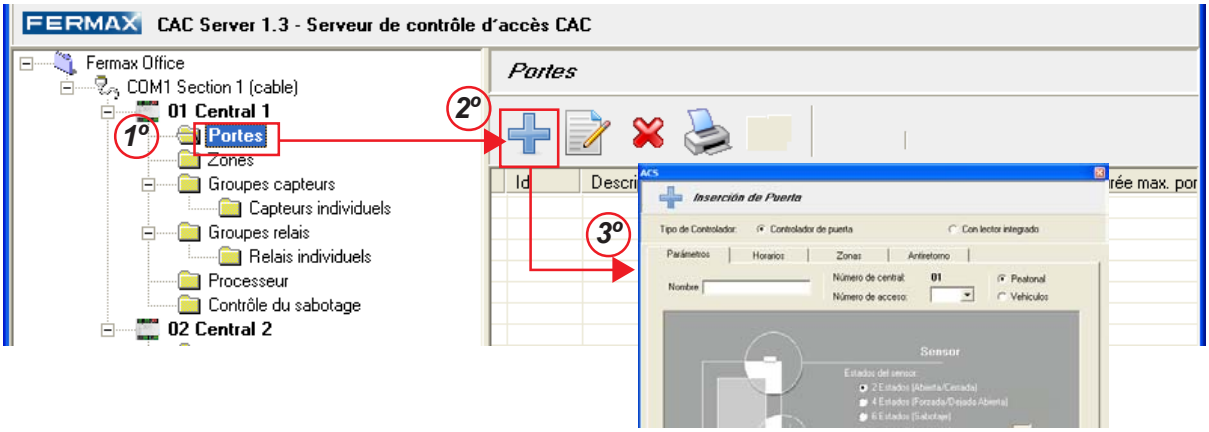
Afin d'ajouter, de modifier ou de supprimer tout élément de l'installation, les étapes à suivre sont les mêmes. Les étapes à suivre pour chacune de ces actions sont expliquées ci-dessous.

Ajouter des éléments

1º- Sélectionnez l'élément à ajouter.

2º- Cliquez sur le bouton  ***.***

3º- Configurez les paramètres correspondant à chaque élément.
Les paramètres configurables pour chaque élément et leur fonction sont expliqués dans les rubriques propres à chaque élément.



Remarque : afin d'ajouter des sections ou des centrales, il faut sélectionner l'élément tout de suite au-dessus qui les contient :

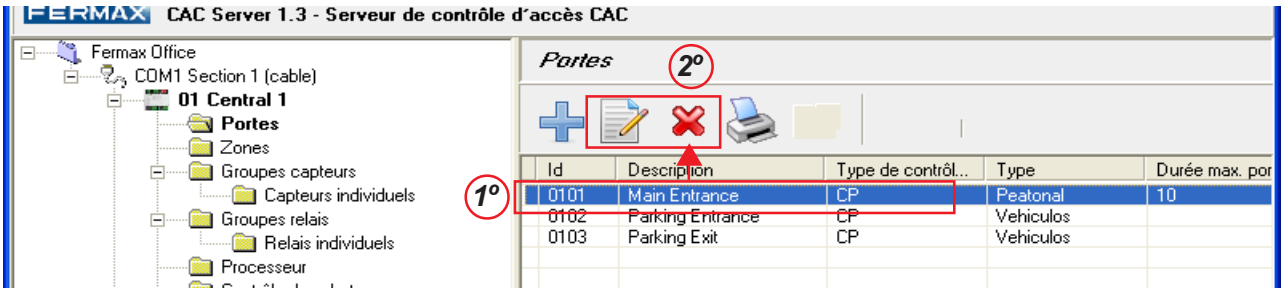
- Sections : sélectionnez l'installation (dans l'exemple :  Fermax Office) et cliquez sur « + ».
- Centrales : sélectionnez la section correspondante (dans l'exemple :  COM1 Sección 1) et cliquez sur « + ».

Supprimer ou modifier des éléments

1º- Sélectionnez l'élément à supprimer dans la «liste des éléments» (partie droite de l'écran).
2º- Réalisez l'action :

- Pour supprimer l'élément sélectionné : ***cliquez sur le bouton*** 

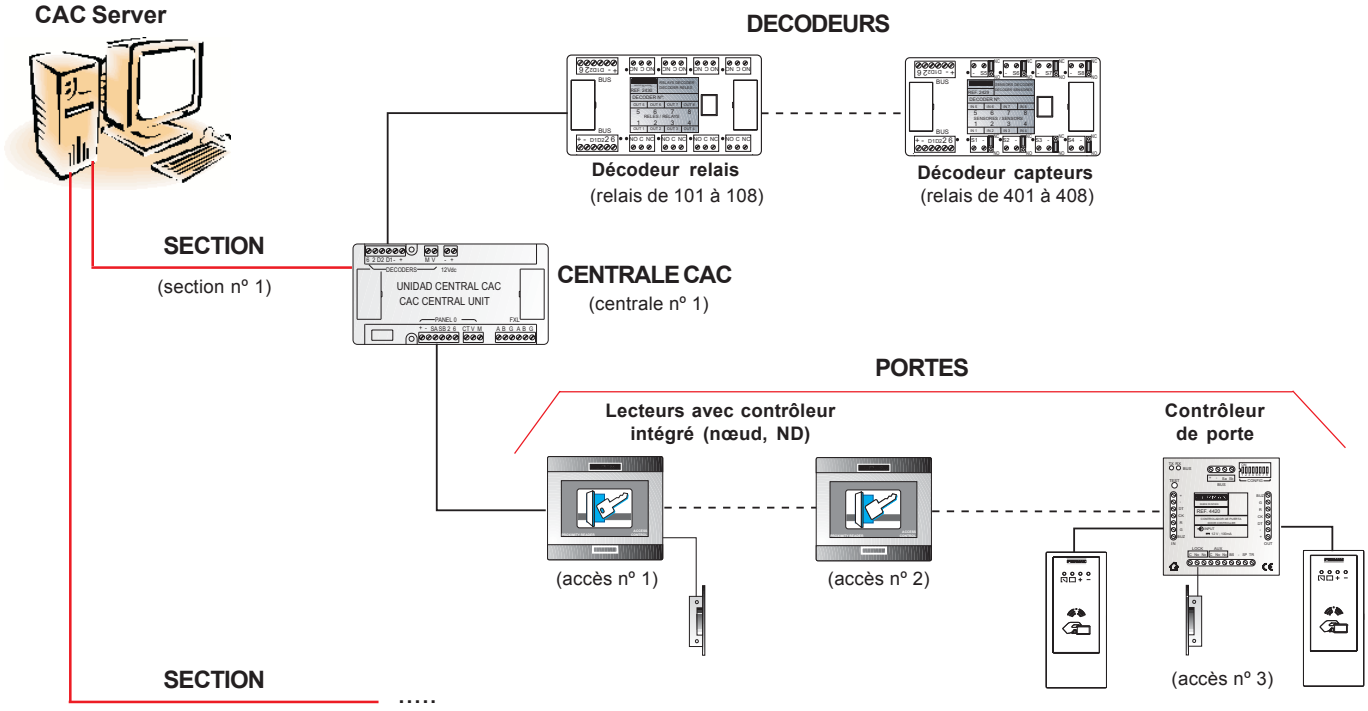
- Pour modifier l'élément sélectionné : ***cliquez sur le bouton*** 



CONFIGURER LES ÉLÉMENTS DE L'INSTALLATION

Les paramètres à configurer pour chaque élément après son ajout dans l'installation sont expliqués dans les rubriques suivantes. Selon leurs fonctions au sein de l'installation, certains paramètres ou d'autres devront être configurés.

Tous les dispositifs (éléments matériels) qui peuvent être configurés dans l'installation CAC Server sont représentés dans le schéma suivant.



Outre les dispositifs présentés ici, il peut également être nécessaire de définir, en fonction de l'installation, les éléments zones, processeur et contrôle anti-sabotage.

Les étapes permettant de configurer l'installation sont les suivantes :

1º. Ajoutez les centrales CAC qui composent chaque section.

2º. Pour chaque centrale, configurez les éléments qui la composent.

2.1. Portes (lecteurs) : ajoutez et configurez les paramètres de chaque lecteur présent dans l'installation en indiquant, entre autres, le type de lecteur : contrôleur de porte ou lecteur avec contrôleur intégré.

2.2. Zones : il faudra définir et configurer les zones si l'installation demande une limitation du nombre de personnes dans une zone quelconque de l'installation ou un contrôle de localisation des utilisateurs. Pour chaque zone créée, les lecteurs permettant l'entrée ou la sortie de la zone seront définis.

2.3. Groupes de capteurs - capteurs individuels : il faudra définir et configurer les décodeurs des capteurs présents dans l'installation en indiquant, entre autres, l'adresse programmée dans chaque capteur (de manière individuelle ou en groupe) et leur attribuer la fonction correspondante.

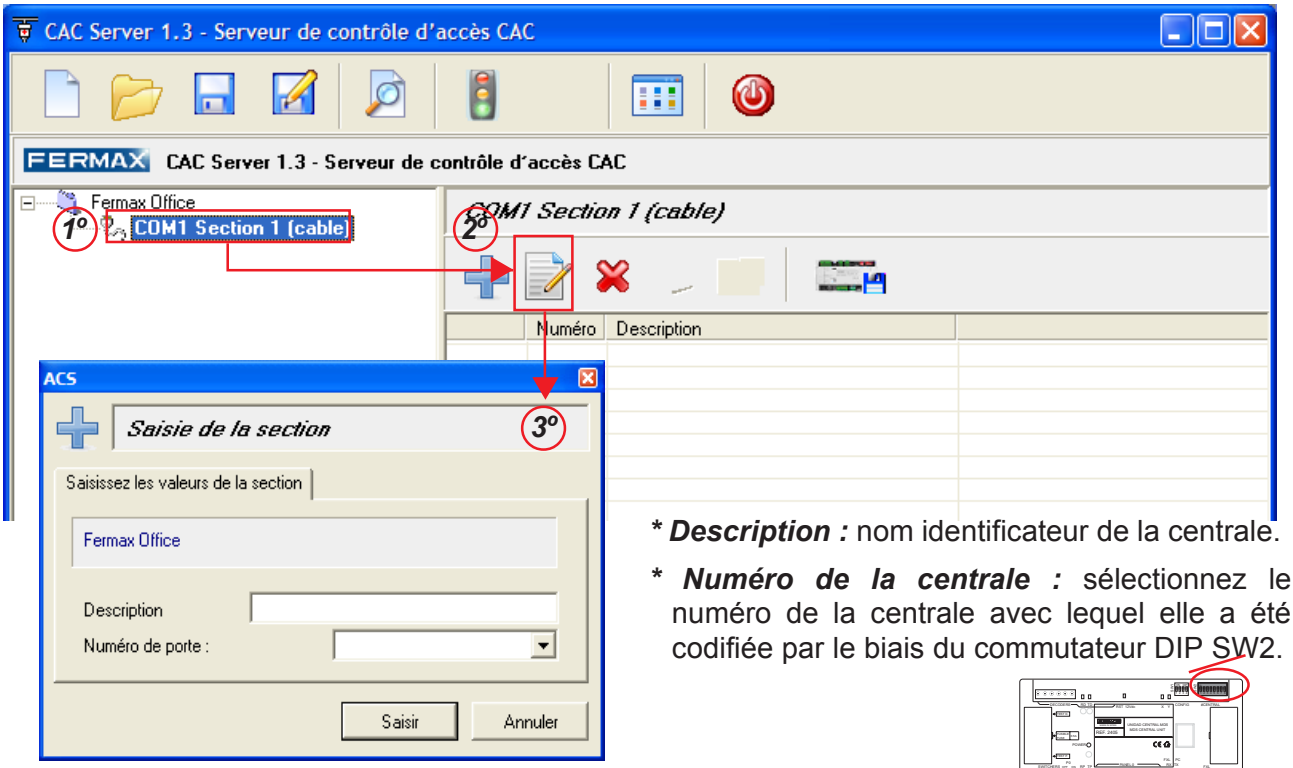
2.4. Groupes de relais - relais individuels : il faudra définir et configurer les décodeurs des relais présents dans l'installation en indiquant, entre autres, l'adresse programmée sur chaque relais (de manière individuelle ou en groupe) et leur attribuer la fonction correspondante.

2.5. Processeur : il faudra définir et configurer les plans si l'on demande un type d'automatisation quelconque dans l'installation.

2.6. Contrôle anti-sabotage : si l'installation dispose d'un type de décodeur quelconque et que l'on configure cette option, l'application Server vérifie s'il existe des problèmes de communication sur le bus de décodeurs.

CENTRALES

Le système CAC permet d'installer et de gérer jusqu'à 64 centrales indépendamment du nombre de sections existantes (de 1 à 4).

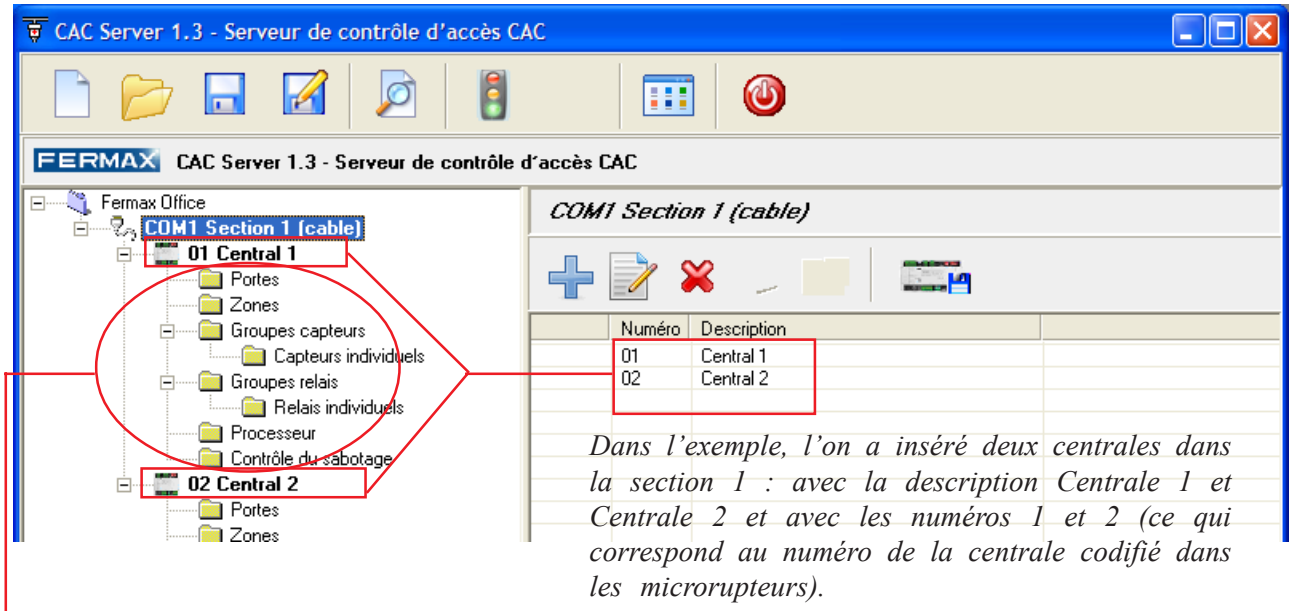


* ***Description :*** nom identificateur de la centrale.

* ***Numéro de la centrale :*** sélectionnez le numéro de la centrale avec lequel elle a été codifiée par le biais du commutateur DIP SW2.

Cliquez sur « Ajouter » afin de créer la centrale (les cases de modification sont vides afin de continuer à créer les centrales jusqu'à 64 maximum).

Cliquez sur « Annuler » afin de terminer l'ajout des centrales.



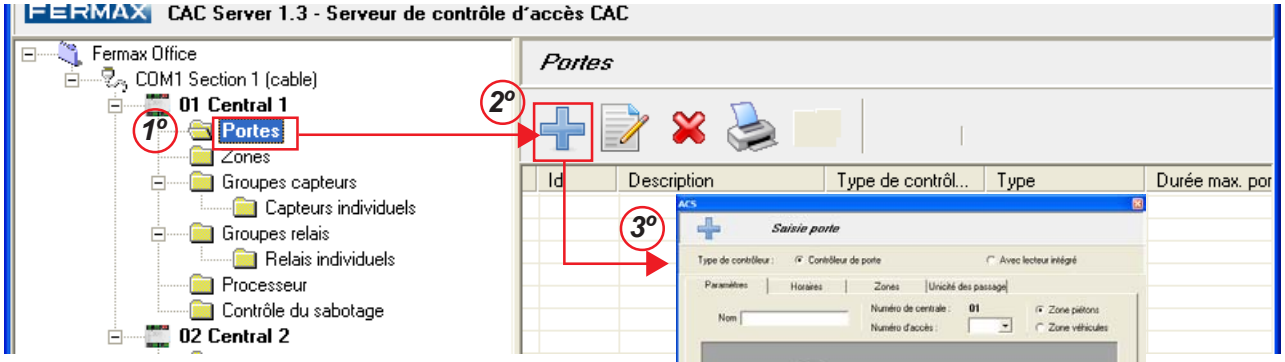
Dans l'exemple, l'on a inséré deux centrales dans la section 1 : avec la description Centrale 1 et Centrale 2 et avec les numéros 1 et 2 (ce qui correspond au numéro de la centrale codifié dans les microrupteurs).

Eléments à définir et configurer pour la centrale 1 en fonction du type d'installation.

PORTES

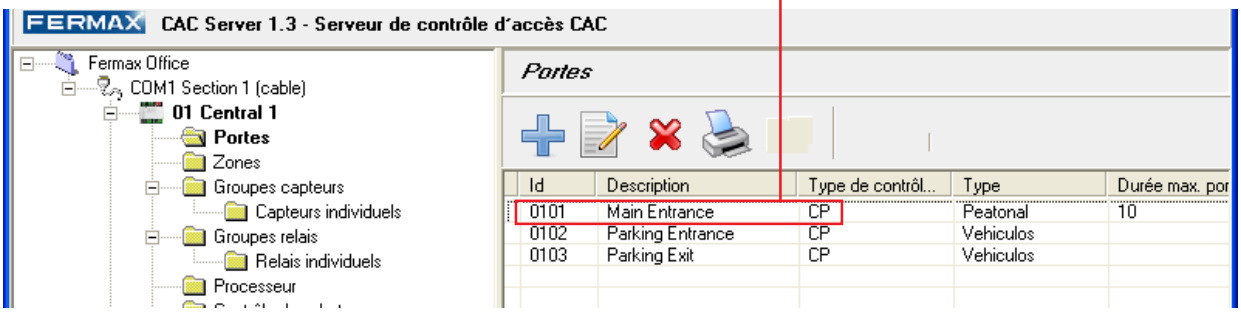
Pour chaque centrale, le système CAC permet d'installer et de gérer jusqu'à 32 accès avec leurs contrôleurs de porte ou lecteurs avec contrôleur intégré correspondants.

Chaque contrôleur de porte ou lecteur équivalent à une porte de l'installation qui limite l'accès à cette dernière.



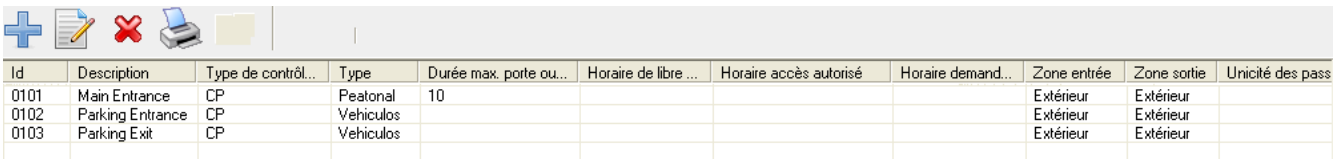
Ecran de configuration des portes.
Dispose de 4 onglets qui regroupent les différents paramètres à configurer :

- Paramètres généraux
- Horaires
- Zones
- Unicité des passages



Dans l'exemple, 3 portes ont été insérées dans la centrale 1.

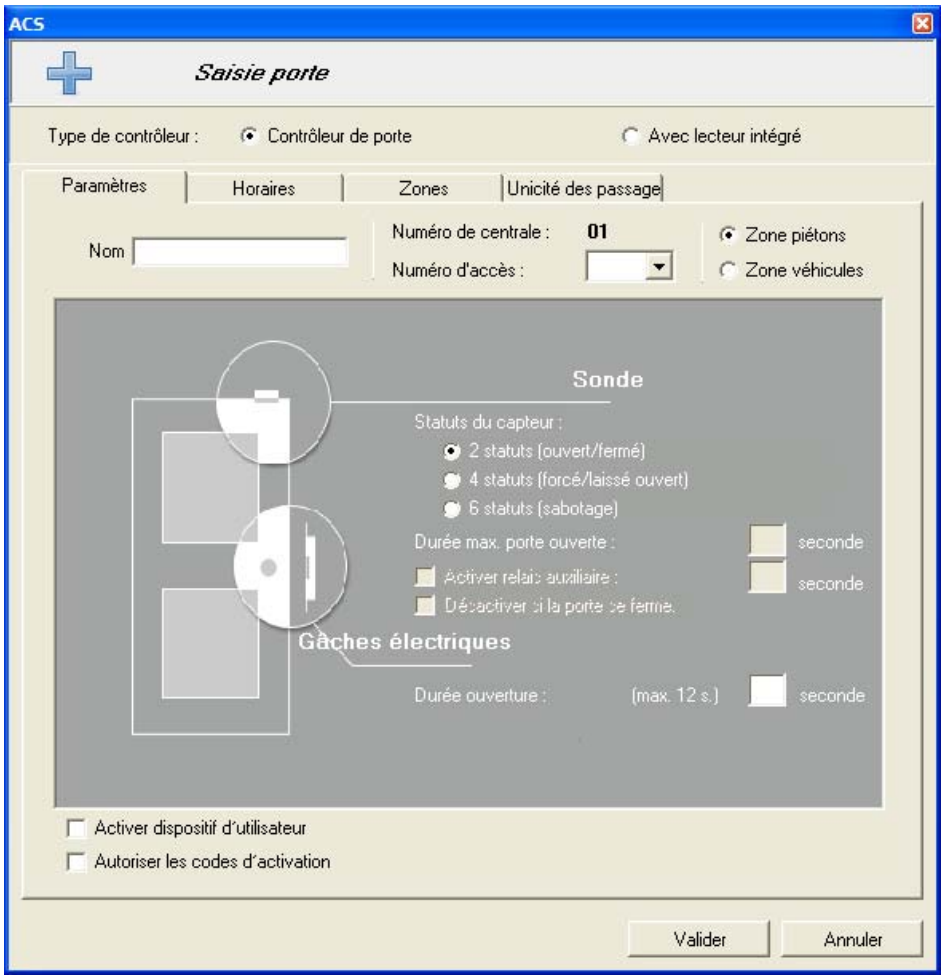
Les portes de chaque centrale et les informations sur la configuration de chaque porte sont présentées sur l'écran principal :



Id	Description	Type de contrôl...	Type	Durée max. porte ou...	Horaire de libre ...	Horaire accès autorisé	Horaire demand...	Zone entrée	Zone sortie	Unicité des pass
0101	Main Entrance	CP	Peatonal	10				Extérieur	Extérieur	
0102	Parking Entrance	CP	Vehiculos					Extérieur	Extérieur	
0103	Parking Exit	CP	Vehiculos					Extérieur	Extérieur	

Chaque paramètre pouvant être configuré pour l'élément « Portes » est expliqué ci-dessous.

Paramètres généraux



* ***Type de contrôleur :*** c'est le premier paramètre qu'il faut configurer pour une porte.
Pour chaque porte, il faut indiquer le type de contrôleur installé pour la porte en question (l'on associe à chaque porte un contrôleur de l'installation).

Il existe deux types de contrôleur :
- Contrôleur de porte (CP) = le lecteur est séparé.
- Contrôleur avec lecteur intégré = le connecteur est connecté au bus de lecteurs.

En fonction du type de contrôleur sélectionné, certains paramètres ou d'autres vont être configurés (les paramètres non configurables pour chaque type de lecteur sont présentés comme étant désactivés ou en gris).

* ***Nom :*** nom attribué à la porte (le nom d'une porte ne peut être utilisé plusieurs fois).
Ce nom identifiera la porte sur toutes les applications serveur et client de l'installation.

* ***Numéro d'accès :*** chaque contrôleur de l'installation possède un numéro d'accès (compris entre 0 et 31) codifié par le biais de microrupteurs de configuration présents sur chaque contrôleur qui l'identifie au sein de la centrale et de l'installation.

Dans le champ « *Numéro d'accès* », il faut sélectionner le numéro d'accès (c'est-à-dire le contrôleur) que l'on souhaite associer à la porte à insérer.

Les numéros d'accès déjà utilisés n'apparaissent pas dans le menu déroulant lors de futures insertions de portes de la même centrale.

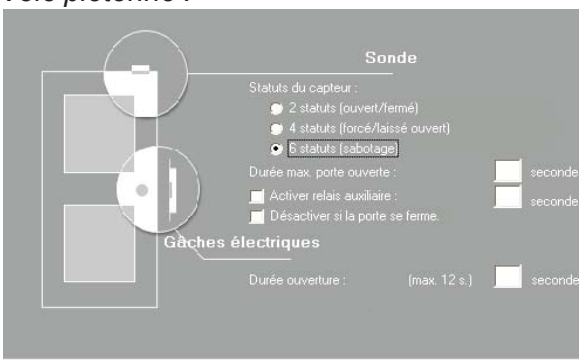
Les « *Paramètres généraux* » à configurer en fonction du type de contrôleur sélectionné sont présentés ci-dessous.

Contrôleur de porte

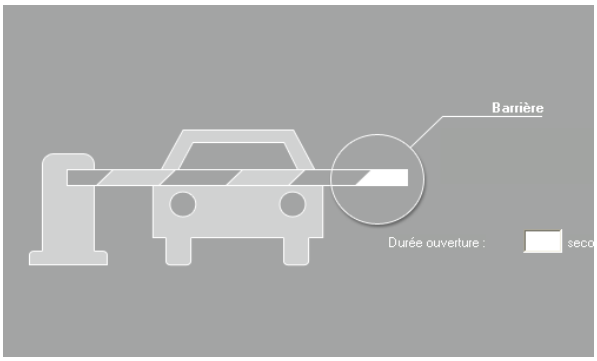
* ***Voie piétonne ou véhicules*** : sélectionnez si le contrôleur de porte s'utilise pour l'accès piétons ou véhicules.

Fonctionnement du CP en mode véhicule : il faut, dans ce cas, 2 détecteurs de présence de véhicules (liens inductifs). L'un est connecté à BS pour détecter la présence au niveau du lecteur et l'autre à la hauteur de la barrière, connecté à SP. Le premier permet de lire l'identificateur et le second de comptabiliser le véhicule (capacité) et de confirmer l'unicité des passages. Pour de plus amples détails, voir le manuel d'installation contrôleur de porte code 97033, puisque dans le cas des accès véhicules, le contrôleur doit être installé en fonction de la configuration du mode véhicule.
En fonction de l'option sélectionnée, les paramètres à configurer, présentés dans l'encadré gris, varient :

Voie piétonne :



Véhicules :



* ***Capteur (accès piétons)***
Permet de configurer le fonctionnement du capteur de porte (s'il y en a un) raccordé au CP :

- **2 statuts (ouverte/fermée) :** indique qu'il y a changement de statut (porte ouverte ou fermée).

- **4 statuts (ouverte/fermée/forcée/laissée ouverte) :**
  - Indique qu'il y a changement de statut (porte ouverte ou fermée).
  - Indique si la porte a été ***forcée***, c'est-à-dire si la porte a été ouverte sans que le contrôleur ait préalablement reçu l'ordre « ouvrir porte » provenant de la centrale (après identification d'un utilisateur autorisé à ouvrir une porte à partir de l'application client, etc.)

    L'événement relatif à la porte forcée a préférence sur l'événement porte ouverte.
  - Indique si la porte a été ***laissée ouverte***, c'est-à-dire si après ouverture d'une porte valide, la porte ne s'est pas fermée avant le temps indiqué dans la case « Durée maximale porte ouverte ».

- **5 statuts (ouverte/fermée/forcée/laissée ouverte/sabotages) :**
  Outre les 4 statuts décrits précédemment (ouverte/fermée/forcée/laissée ouverte), il indique s'il y a eu sabotage au niveau du capteur de porte.

  Ce type de capteur détecte deux types de sabotage :
  - Sabotage par court-circuit : lorsque l'on réalise l'union des deux câbles du capteur (court-circuit) afin de simuler que le capteur est en veille.
  - Sabotage par court-circuit ouvert : lorsque l'un des câbles du capteur est coupé.

  Afin de pouvoir détecter le sabotage du capteur, ce dernier doit avoir été installé en fonction de la configuration 5 statuts (voir manuel contrôleur de porte code 97033).

Selon le statut et la configuration du capteur, le contrôleur de porte envoie à la centrale une incidence en indiquant le statut actuel de la porte en fonction du statut du capteur (porte ouverte, porte forcée...) L'incidence est stockée dans le journal des incidences de la centrale. Celles-ci peuvent être consultées ou visualisées en temps réel par le biais des applications client.

- **Durée maximale de la porte ouverte :** il s'agit de la durée maximale pendant laquelle la porte peut rester ouverte (après une ouverture valide) avant de lancer une alarme « Porte laissée ouverte ».

- **Activer relais auxiliaire :** si cette case est cochée, lorsqu'il se produit un événement de « porte laissée ouverte », le relais auxiliaire du contrôleur de porte s'active pendant la durée indiquée dans la case « sec ». Une fois ce laps de temps écoulé, le relais se désactive. Si la durée programmée est égale à 255 secondes, le relais reste verrouillé après son activation.

  Le relais auxiliaire s'active également si un événement porte « forcée » ou « sabotage du capteur » a lieu. Dans ce cas, le relais reste verrouillé jusqu'à ce qu'il soit désactivé à partir d'un lecteur combiné (clavier+proximité).

- **Désactiver si la porte se ferme :** désactive le relais auxiliaire du CP activé après un événement « porte laissée ouverte » lorsque la porte se ferme, indépendamment de la durée d'activation programmée pour le relais.

* ***Gâche électrique (accès piétons et véhicules)***

- ***Durée d'ouverture :*** durée d'activation du ***relais de la gâche électrique*** du CP après la correcte identification de l'utilisateur (véhicule ou piéton selon le type d'accès).

* ***Activer le dispositif d'utilisateur*** : par le biais de l'application client CAC Access, il est possible d'associer à chaque utilisateur un dispositif de façon à ce que, si cette fonction est activée pour la porte correspondante, lors de la présentation de l'identificateur, s'il n'a pas de restrictions, outre l'ouverture de la porte, il change le statut du dispositif associé. S'il s'agit d'un capteur (décodeur), il s'active ou se désactive en fonction du précédent statut ; s'il s'agit d'un relais, il s'active ou se désactive. La fonction est disponible pour tout identificateur (proximité, contact, clavier...)

Cette fonction est utile lorsque l'on souhaite activer un éclairage ou activer/désactiver un détecteur individuellement pour chaque utilisateur, activer un second accès individuel, etc.

* ***Autoriser les codes d'activation :*** à partir des lecteurs de proximité et clavier combinés et raccordés à un **CP,** si cette fonction est activée pour la porte correspondante, il est possible d'activer ou de désactiver une infinité de dispositifs.

Pour ce faire, il faut, à partir du lecteur combiné, effectuer la démarche suivante :

1º Saisissez, à partir du clavier, le code de l'action à effectuer suivi du code du dispositif qui effectue l'action.

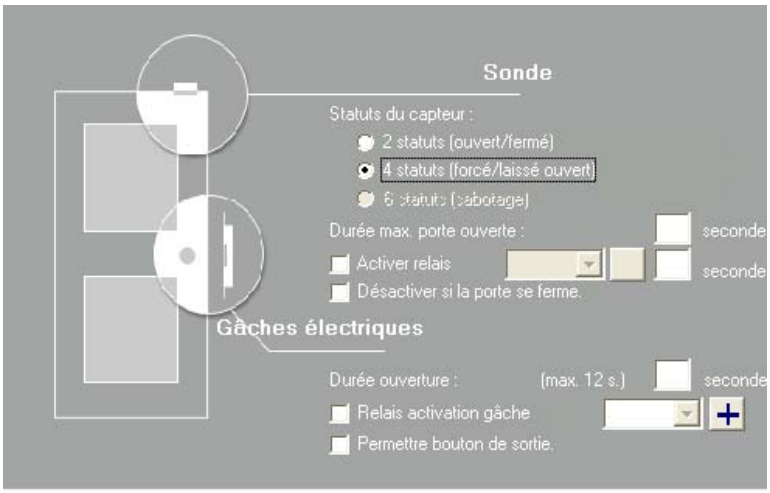
2º Présentez un identificateur (badge de proximité) valide au lecteur.

Les actions à effectuer et les dispositifs sont les suivants :

Code clavier	Fonction
0	désactive le capteur du CP (permet de laisser la porte ouverte indéfiniment).
0X	désactive le groupe X de décodeurs de capteurs (100 à la fois). Ex. : 02+badge : désactive les capteurs de 200 à 299.
0XYZ	désactive le capteur XYZ (décodeur). Lorsque l'on souhaite désactiver l'alarme d'une zone avant d'y entrer.
1	activation du capteur de porte du CP (active de nouveau le capteur avec la durée programmée).
1X	activation du groupe X des décodeurs de capteurs (100 à la fois).
1XYZ	activation du capteur XYZ (décodeur).
2	désactivation du relais auxiliaire du CP.
2X	désactivation du groupe X de décodeur de relais (100 à la fois).
2XYZ	désactivation du relais XYZ (1).
3	activation du relais auxiliaire du CP.
3X	activation du groupe X de décodeur de relais (100 à la fois).
3XYZ	activation relais XYZ (1). Ex. : 3010+badge : active le relais 10.

Avec lecteur intégré

Les contrôleurs avec lecteur intégré sont utilisés pour les accès piétons.



* ***Capteur***

Le fonctionnement du capteur de porte du lecteur est le même que celui décrit précédemment pour le contrôleur de porte à la seule différence qu'il ne dispose pas de la configuration 5 statuts ni de relais auxiliaire.

Les paramètres spécifiques au lecteur qui diffèrent du contrôleur de porte (expliqué précédemment) sont décrits ci-dessous.

- **Durée maximale de la porte ouverte :** il s'agit de la durée maximale pendant laquelle la porte peut rester ouverte (après une ouverture valide) avant de lancer une alarme «Porte laissée ouverte».
- **Activer relais :** si cette case est cochée, si un événement « porte laissée ouverte » a lieu, le relais (une sortie d'un décodeur de relais) sélectionné à partir de la case déroulante s'active pendant la durée indiquée dans la case « sec ».

  La case déroulante présente la liste des relais définis dans l'installation (voir rubrique « groupe de relais et relais individuels »). A partir de cet écran, il est également possible de définir les sorties de relais en appuyant sur le bouton « **+** ».
- **Désactiver si la porte se ferme :** désactive le relais (sélectionné précédemment) activé après un événement « Porte laissée ouverte » lorsque la porte se ferme indépendamment de la durée d'activation programmée pour le relais.

* ***Gâche électrique***

- ***Durée d'ouverture :*** durée d'activation du ***relais de la gâche électrique*** du lecteur après une correcte identification de l'utilisateur. La durée maximale d'activation de ce relais est de 12 secondes.
- ***Relais d'activation de la gâche électrique :*** cochez cette case si vous souhaitez activer la gâche électrique par le biais d'un relais de décodeur (afin de doter l'installation d'un plus haut niveau de sécurité) ou si vous souhaitez activer un dispositif supplémentaire (par le biais d'un décodeur de relais) au moment d'effectuer l'ouverture des portes. Sélectionnez à partir de la case déroulante le relais à activer pendant la durée indiquée dans la case « sec ».
- ***Autoriser le bouton de sortie :*** active l'ouverture des portes à partir du bouton-poussoir de sortie raccordé au lecteur (s'il y en a un).

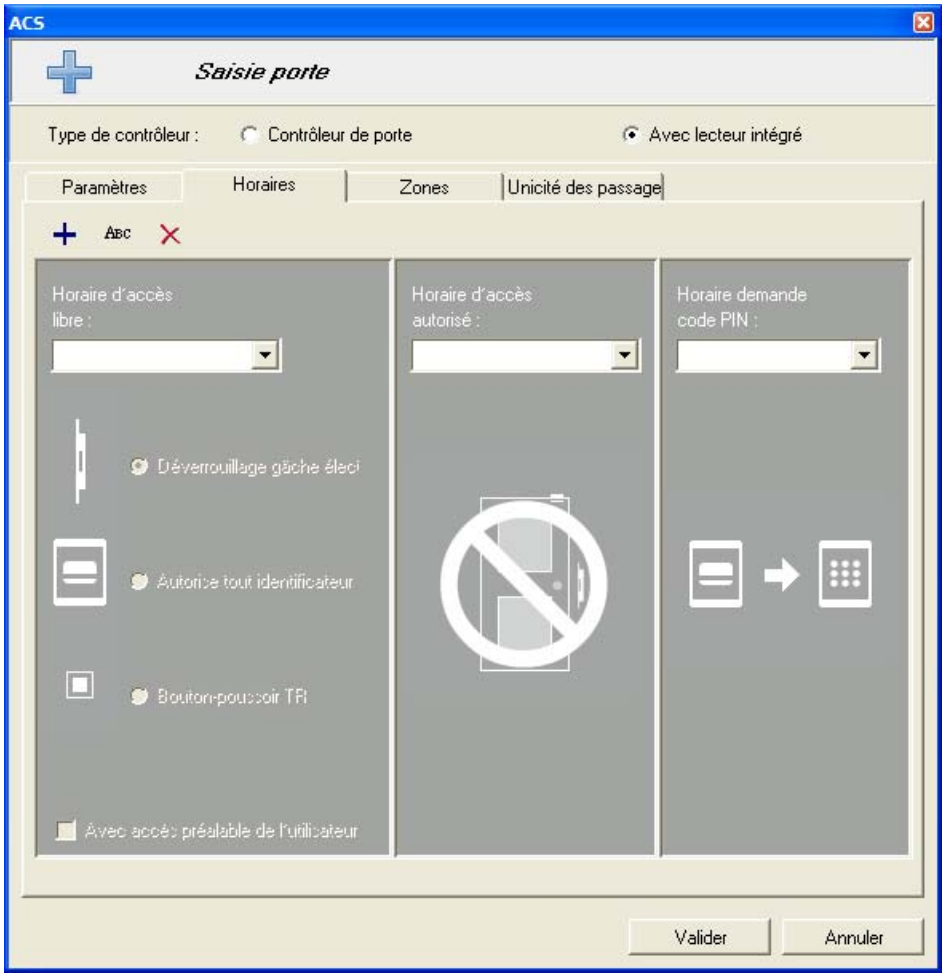
  Le bouton de sortie peut également être activé par le biais d'une centrale de conciergerie raccordée à l'installation.

  Au cas où vous souhaiteriez désactiver le bouton de sortie, il faudrait désactiver cette option à partir de l'application Server (décocher la case et mettre à jour la centrale CAC) et désactiver l'option à partir de la conciergerie si cette option a également été activée à partir de la conciergerie.

  Au cas où au niveau de l'un des éléments de l'installation (serveur ou centrale de conciergerie) cette option serait désactivée, le bouton de sortie effectuera l'ouverture des portes après avoir été touché.

Horaires

Pour chaque porte, il est possible de configurer trois modes de fonctionnement. Ces modes de fonctionnement ne peuvent être utilisés simultanément, mais doivent être définis à des horaires différents.



* ***Accès libre :*** pendant l'horaire d'accès libre sélectionné, l'accès par le biais de la porte est autorisé à toute personne.

Les modalités d'accès sont les suivantes :

- ***Déverrouillage de la gâche électrique :*** la gâche électrique reste activée pendant l'horaire choisi.
- ***Tout identificateur :*** l'accès est autorisé (la gâche électrique est activée) lorsque l'on présente tout identificateur d'utilisateur, valide ou non, au lecteur.
- ***Bouton-poussoir horaires commerciaux (bouton-poussoir d'entrée) :*** uniquement disponible avec un contrôleur de porte.
  Si un bouton-poussoir d'horaires commerciaux est raccordé au contrôleur de porte, en appuyant dessus pendant l'horaire choisi, la gâche électrique s'active.
- ***Avec accès d'utilisateur préalable :*** permet de modifier le mode de fonctionnement «Accès libre» lors de la présence d'une personne autorisée à l'intérieur de l'installation, c'est-à-dire que le mode d'accès libre sélectionné ne sera pas actif tant qu'un utilisateur autorisé n'aura pas présenté un identificateur valide pour cette porte pendant l'horaire d'accès libre choisi.

* ***Accès autorisé :*** permet d'attribuer un horaire d'accès à la porte afin de restreindre l'accès de tous les utilisateurs hors de cet horaire, sauf pour les utilisateurs possédant des autorisations spéciales (super-utilisateurs ou utilisateurs sans restriction). De cette manière, il est possible de restreindre l'accès de tout le personnel sans avoir à créer ni attribuer des niveaux d'accès (profils).

Les niveaux d'accès de chaque utilisateur (profils) sont créés et attribués par le biais de l'application CAC Access.

* ***Demande du code PIN :*** pendant cet horaire, en plus de l'identificateur de l'utilisateur, un code personnel à 4 chiffres (PIN) est demandé.

Si le code appartient à l'utilisateur propriétaire de l'identificateur présenté, l'accès est autorisé. De cette manière, l'on évite, si un utilisateur quelconque perd son identificateur, que la personne qui le trouve puisse accéder à l'installation puisqu'elle ne connaîtra pas le code PIN.

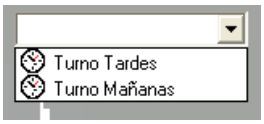
Le code PIN est attribué à l'utilisateur par le biais de l'application CAC Access dans la fiche utilisateur.

Important :

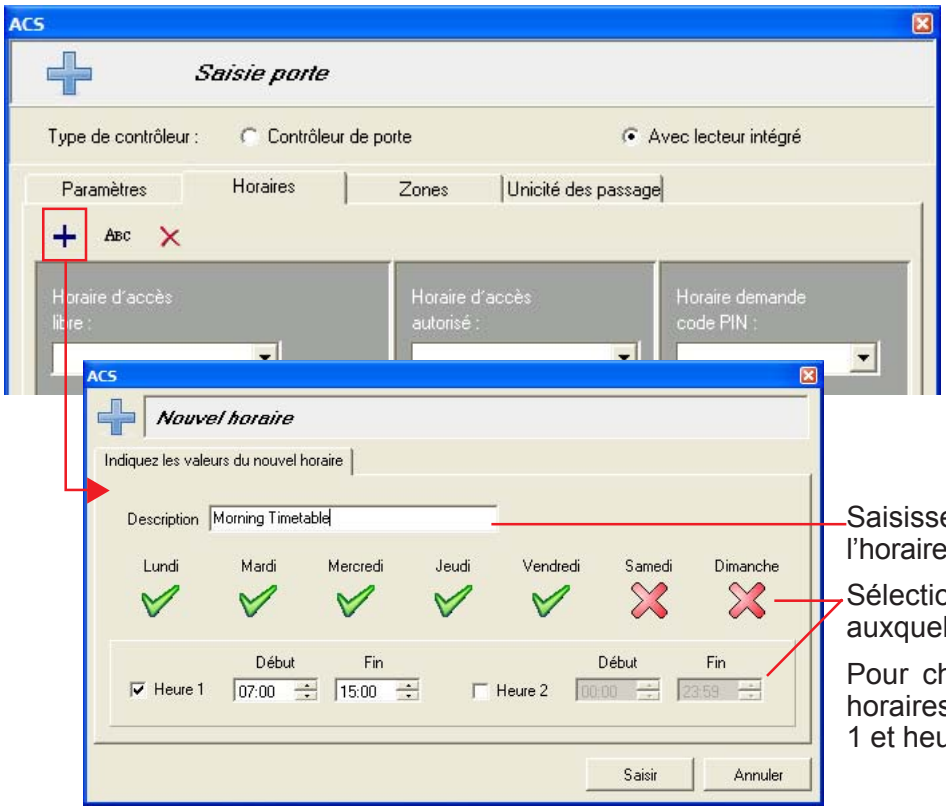
- Le code PIN ne fonctionnera que sur les lecteurs combinés clavier+proximité.

CREER HORAIRES

Les horaires pouvant être attribués à chaque mode de fonctionnement sont sélectionnés dans le menu déroulant disponible pour chaque mode.



Les horaires pouvant être sélectionnés doivent être créés préalablement de la manière suivante (jusqu' à 32 horaires peuvent être créés) :



Saisissez une description pour l'horaire.

Sélectionnez les jours et les heures auxquels sera appliqué l'horaire.

Pour chaque horaire, deux tranches horaires peuvent être définies : heure 1 et heure 2.

Abc Modifier un horaire existant

✕ Supprimer un horaire existant

Important

- Pendant les jours fériés (définis dans l'application CAC Access), ces modes de fonctionnement ne sont pas applicables.

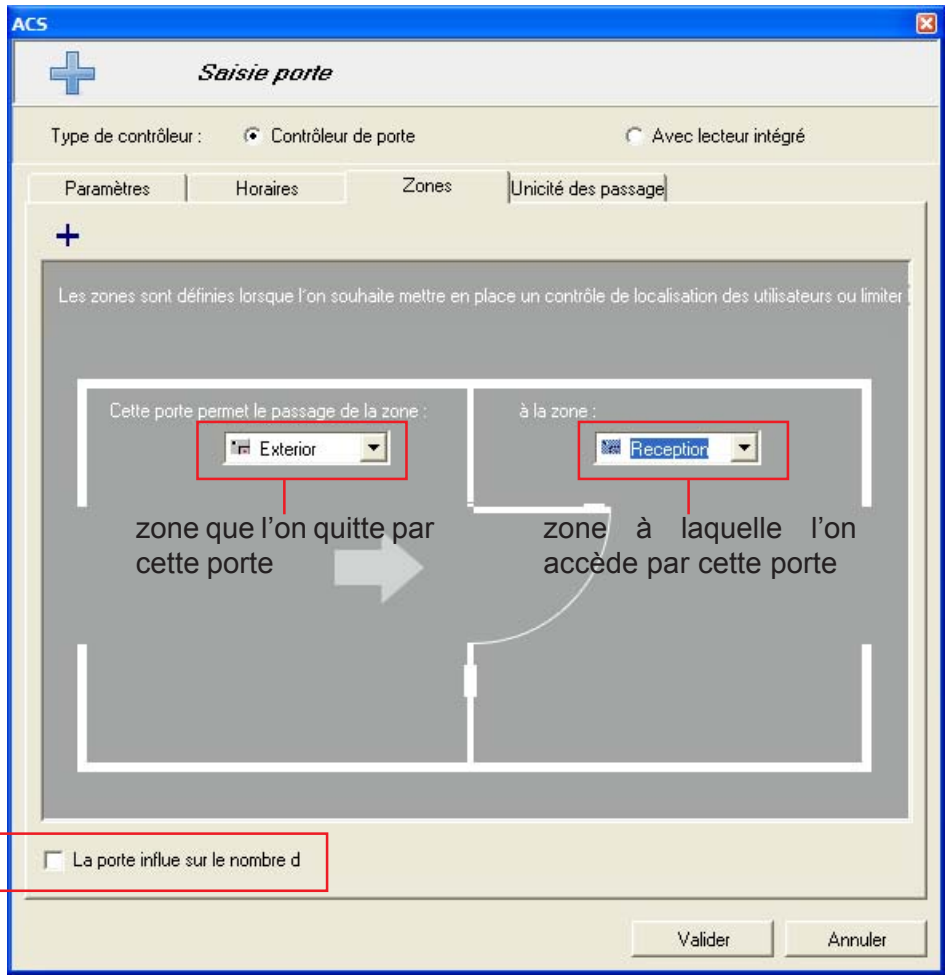
Zones

Il n'est pas obligatoire de les définir. Ce ne sera le cas que si l'on souhaite utiliser la fonction **limitation du nombre de personnes** (capacité maximale dans une zone) ou la fonction **localisation des utilisateurs**.

Afin de disposer de ces fonctions dans l'installation, il faut indiquer, pour chaque porte, si celle-ci permet d'entrer dans une zone ou d'en sortir.

Les zones de l'installation doivent être créées préalablement à partir de l'élément « zones » de chaque centrale. Elles peuvent également être créées directement à partir de cet écran en appuyant sur la touche « + ».

Les étapes permettant de créer des zones sont expliquées dans la rubrique consacrée à l'élément « zones ».



* ***La porte a une influence sur le nombre de personnes présentes :*** si cette option est activée, il est indiqué que la porte joue un rôle sur le nombre de personnes présentes dans la zone à laquelle l'on accède ou que l'on quitte.

Avec l'option « a une influence sur le nombre de personnes » activée :

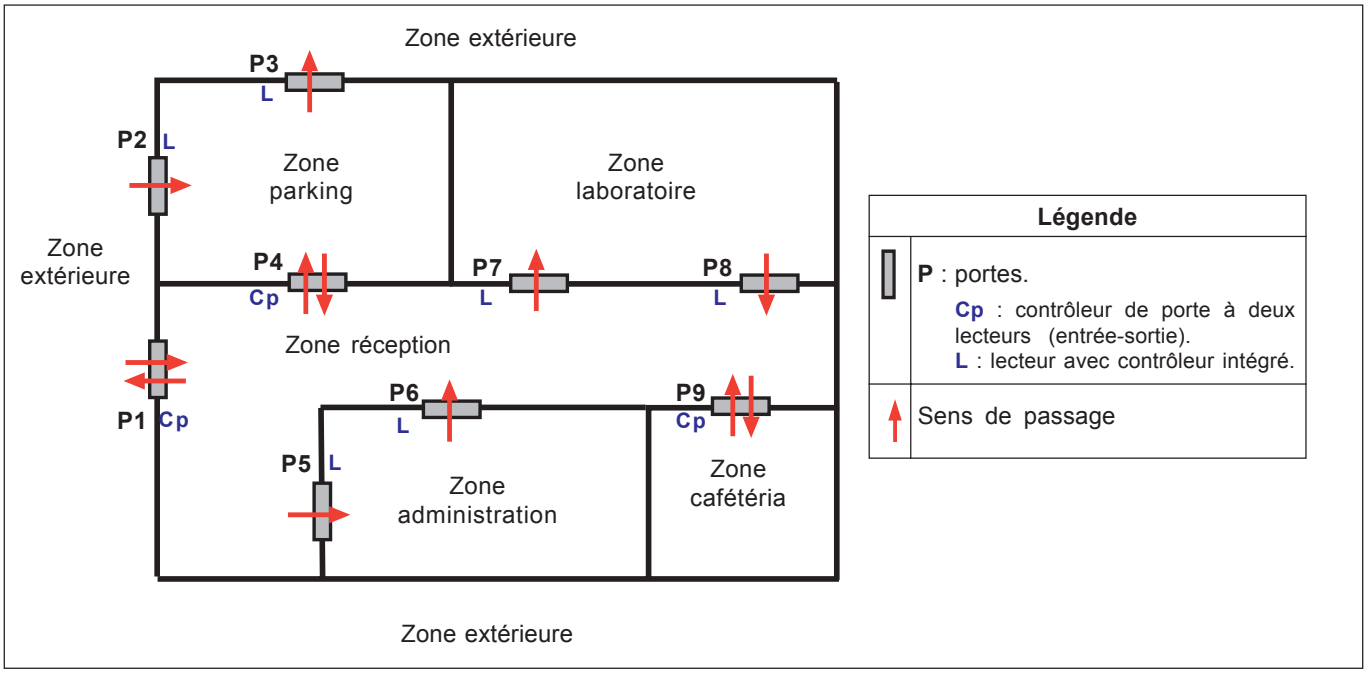
- *Le nombre de personnes présentes dans la zone,* indiqué dans le champ « Accès à la zone », *augmente de 1* lorsqu'un utilisateur (après avoir présenté un identificateur valide) accède à la zone par cette porte.

- *Le nombre de personnes présentes dans la zone,* indiqué dans le champ « cette porte permet de sortir de cette zone », *diminue de 1* lorsqu'un utilisateur (après avoir présenté un identificateur valide) quitte la zone par cette porte.

Le nombre de personnes augmente ou diminue dans la mesure où l'on a défini une capacité maximale pour la zone (voir rubique Zones).

Exemple de configuration du paramètre Zones :

Dans l'exemple suivant, l'on montre comment configurer les portes de l'installation de l'illustration au cas où l'on voudrait disposer des fonctions de contrôle de capacité et/ou de localisation des utilisateurs :



Pour cette installation, 5 zones ont été définies, en plus de la zone « extérieure » (définie par défaut dans l'application Server) :

- Zone réception
- Zone parking
- Zone administration
- Zone laboratoire : avec limitation du nombre de personnes.
- Zone cafétéria : avec limitation du nombre de personnes.

Configuration du paramètre zones des portes

Porte	Cette porte permet de sortir de la zone :	D'accéder à la zone :	Porte a une influence sur le nombre de personnes
P1	Zone extérieure	Zone réception	Non
P2	Zone extérieure	Zone parking	Non
P3	Zone parking	Zone extérieure	Non
P4	Zone parking	Zone réception	Non
P5	Zone réception	Zone administration	Non
P6	Zone administration	Zone réception	Non
P7	Zone réception	Zone laboratoire	oui, porte d'accès à la zone : le nombre de personnes augmente de 1
P8	Zone laboratoire	Zone réception	oui, porte de sortie la zone : le nombre de personnes diminue de 1
P9	Zone réception	Zone cafétéria	oui (*)

(*) Les portes disposant d'un contrôleur de porte peuvent être employées aussi bien pour entrer que sortir avec un seul contrôleur (lecteur d'entrée et lecteur de sortie sur le même contrôleur de porte). En fonction du sens de passage, l'on prendra en compte la zone que l'on quitte et la zone à laquelle l'on accède, augmentant ou diminuant le compteur permettant de définir le nombre de personnes de la zone correspondante.

Le lecteur d'entrée se situe dans la zone indiquée en tant que « Cette porte permet d'accéder à la zone » et le lecteur de sortie dans la zone indiquée en tant que « cette porte permet de sortir de la zone ».

Unicité des passages (antipassback)

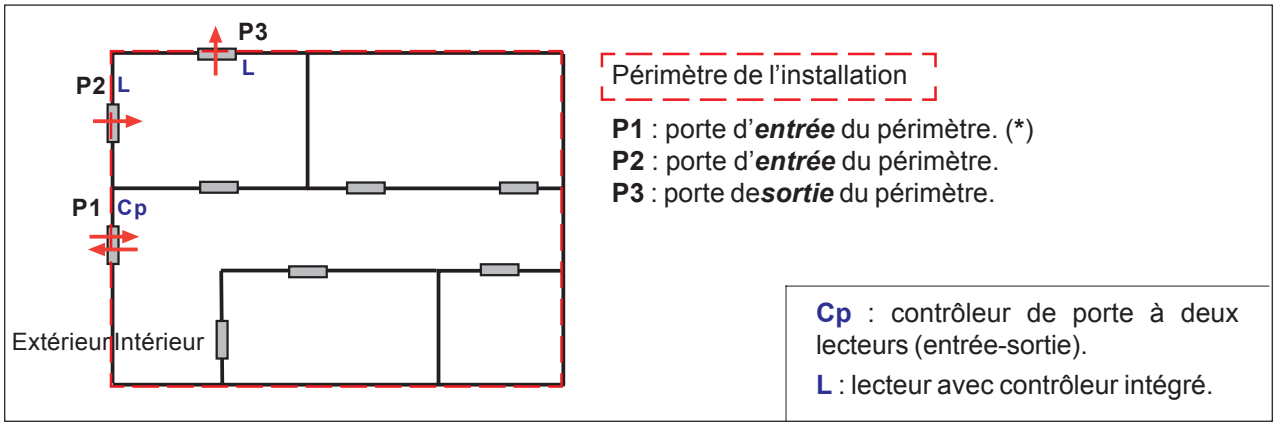
La fonction unicité des passages ou antipassback empêche un utilisateur qui accède à l'installation par une *porte d'entrée* d'entrer de nouveau dans l'installation (par n'importe quelle autre porte d'entrée) sans avoir quitté l'installation par une *porte de sortie*.

De cette façon, l'on évite que plusieurs personnes puissent accéder à l'installation avec un même dispositif ou, pour les parkings, que plusieurs voitures puissent entrer avec le même identificateur ; l'installation est ainsi pourvue d'un plus grand niveau de sécurité.

Le système CAC permet d'effectuer la fonction unicité des passages très simplement et au niveau de toute l'installation. Pour ce faire, il faut juste définir le périmètre de l'installation où l'on souhaite mettre en place cette fonction.

Le périmètre de l'installation est défini par les portes de l'installation configurées en tant qu'***entrée dans le périmètre*** ou ***sortie du périmètre*** de l'installation.

Par conséquent, afin de mettre en place la fonction unicité des passages pour chaque porte faisant partie du périmètre, il faut indiquer s'il s'agit de portes permettant d'***entrer*** dans ce périmètre ou d'en***sortir***.



(*) Les portes qui disposent d'un contrôleur de porte peuvent être utilisées aussi bien pour entrer que pour sortir avec un seul contrôleur (lecteur d'entrée et lecteur de sortie sur le même contrôleur de porte). Par conséquent, en fonction du sens de passage, l'on saura si l'utilisateur entre ou sort du périmètre.

Deux niveaux d'unicité des passages : piétons et véhicules

Afin d'augmenter le niveau de sécurité, le système CAC intègre deux niveaux d'unicité des passages : une voie piétonne et une autre pour véhicules ; l'un des deux s'applique automatiquement en fonction du type de porte par lequel l'on accède au périmètre de l'installation.

Accès par une porte piétonne :
Lorsqu'un utilisateur entre dans le périmètre (par une porte piétonne définie en tant qu'entrée), il est considéré comme étant « à l'intérieur » de l'installation et il ne lui est plus permis de traverser de porte d'entrée au périmètre qu'il s'agisse d'une porte piétonne ou d'une porte pour véhicules.

Il lui est en revanche permis de passer par des portes de sortie ou des portes qui n'appartiennent pas au périmètre.

S'il passe par une porte de sortie, il est considéré comme étant « hors de l'installation » et il ne pourra y accéder de nouveau que par une porte d'entrée.

Accès par une porte véhicules :
Si, dans le cas contraire, l'utilisateur accède au périmètre par une porte véhicules, le système ***considère l'utilisateur et son véhicule comme étant à l'intérieur de l'installation***. Il ne pourra donc pas entrer de nouveau par une porte véhicules à moins qu'il ne sorte par une sortie véhicules.

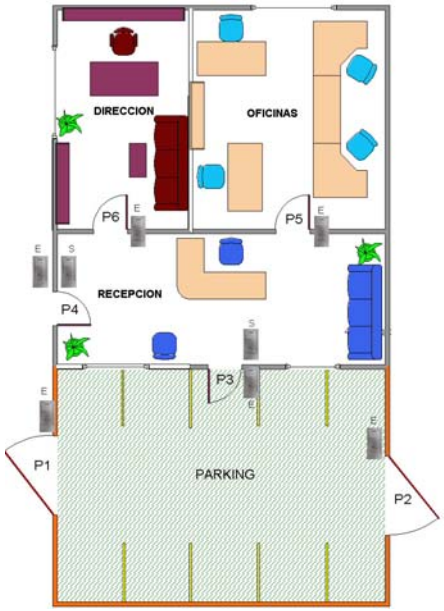
Il peut en revanche passer par une porte de sortie ou par l'une des portes n'appartenant pas au périmètre.

Au cas où l'utilisateur sortirait par une porte de *sortie piétonne* , il ne pourrait entrer de nouveau dans le périmètre que par une porte d'entrée piétonne et non par une entrée pour véhicules puisque le véhicule se trouve toujours à l'intérieur de l'installation.

Grâce aux deux niveaux d'unicité des passages, l'exemple de la figure 1 peut être résolu de 2 manières différentes :

OPTION A : en n'utilisant qu'un seul niveau d'unicité des passages
L'on définit les portes d'accès au parking (P1 et P2) comme appartenant au périmètre (P1 entrée et P2 sortie) et les portes P3 et P4 pour l'accès à une zone restreinte. Par conséquent, les utilisateurs sans autorisation n'y auront pas accès. Si un utilisateur emploie son identificateur pour entrer avec son véhicule par P1, il ne pourra pas entrer de nouveau par cette porte, mais il pourra le faire par les autres portes de l'installation (si son identificateur le permet). Lorsqu'il abandonnera avec son véhicule le parking par P2, il pourra de nouveau accéder à l'installation par P1. Dans ce cas, il n'y aura pas de contrôle d'unicité des passages.

Figure 1



OPTION B : en utilisant deux niveaux d'unicité des passages
Les portes d'accès au parking (portes véhicules pour accéder au périmètre) et la porte P4 (accès piéton pour accéder au périmètre) sont définies. Lorsqu'un utilisateur accède par une porte d'entrée parking (il faut dans ce cas avoir sa voiture), l'utilisateur et la voiture seront considérés comme étant à l'intérieur des installations. A ce moment, il ne pourra y accéder que par P1 s'il est préalablement sorti par P2 ou si l'unicité des passages ne lui est plus appliquée. Indépendamment du fait qu'il soit sorti par P2, l'utilisateur pourra toujours sortir à pied par P4 et entrer de nouveau par la même porte, mais jamais par l'entrée de parking P1. De même, une fois à l'intérieur de l'installation (soit par P1 soit par P4), l'utilisateur ne pourra entrer de nouveau par l'un des accès au périmètre.

Dans cet exemple, il est possible de combiner la fonction de limitation du nombre de personnes aux places de parking existantes. Pour cela, il faudra indiquer que la porte 1 permet le passage de la zone extérieure (définie par défaut) à la zone parking et la porte 2 permet le passage de la zone parking à la zone extérieure.

Caractéristiques de la fonction unicité des passages (antipassback)

- Au cas où il y aurait plus d'une unité centrale dans l'installation, ces informations sont partagées par toutes les centrales qui se trouvent dans le même réseau. Il est donc possible de mettre en place la fonction unicité des passages globalement dans toute l'installation.

  Prenons par exemple un campus universitaire comprenant 3 parkings éloignés les uns des autres, chacun contrôlé par les accès de véhicules raccordés à différentes unités centrales. Lorsqu'un utilisateur entre avec son véhicule par une entrée dans l'un des parkings, il est considéré comme étant à l'intérieur du périmètre. S'il souhaite employer son identificateur pour entrer dans un autre parking, il ne le pourra pas car toutes les centrales possèdent cette information.

- Toutes ces informations sont stockées dans une mémoire non volatile, de sorte que s'il y a une coupure de courant (ou un dysfonctionnement de l'alimentation de *sauvegarde*), les utilisateurs ne seront pas considérés comme étant hors de l'installation.

- *Arrêt de l'unicité des passages* : en cas de mauvaise utilisation du système de la part d'un utilisateur, tel que l'abandon de l'installation sans présenter l'identificateur en profitant de la sortie d'un autre utilisateur, cet utilisateur ne pourra accéder à l'installation la prochaine fois qu'il essaiera d'y entrer puisque le système considère l'utilisateur comme étant « à l'intérieur de l'installation » (n'a pas validé sa sortie par un lecteur de sortie).

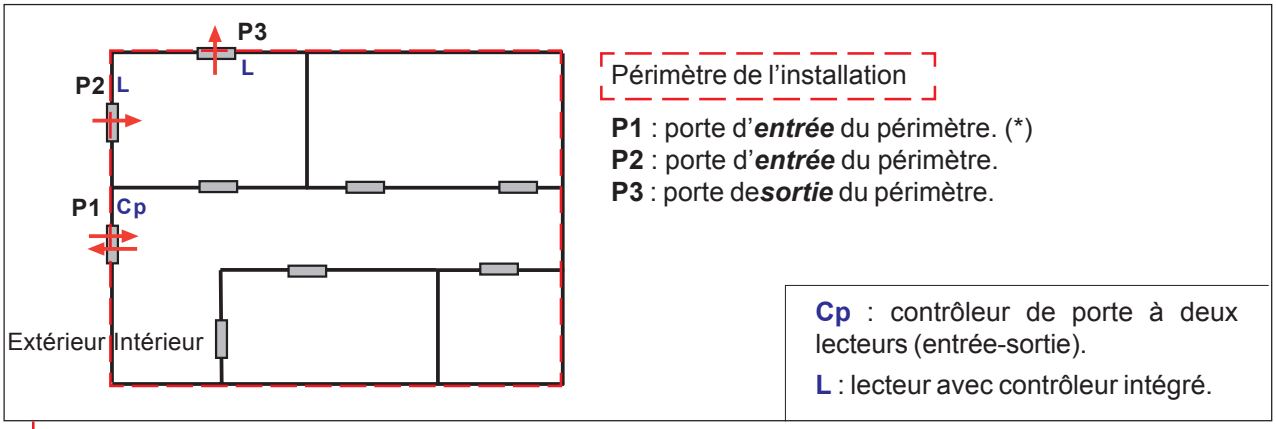
  Pour éviter ce type de problème, il est possible, par le biais de l'application Server, de déterminer une heure du jour (normalement la nuit) pour pouvoir mettre automatiquement tous les utilisateurs hors du périmètre (voir rubrique « Panneau de contrôle >> Heure d'abandon de l'unicité des passages »).

- L'on peut indiquer que l'utilisateur est à l'intérieur du périmètre à condition que la porte se soit ouverte de sorte que si la porte ne s'ouvre pas, l'on ne pourra considérer l'utilisateur comme étant à l'intérieur. Pour ce faire, il faut utiliser le capteur de porte.

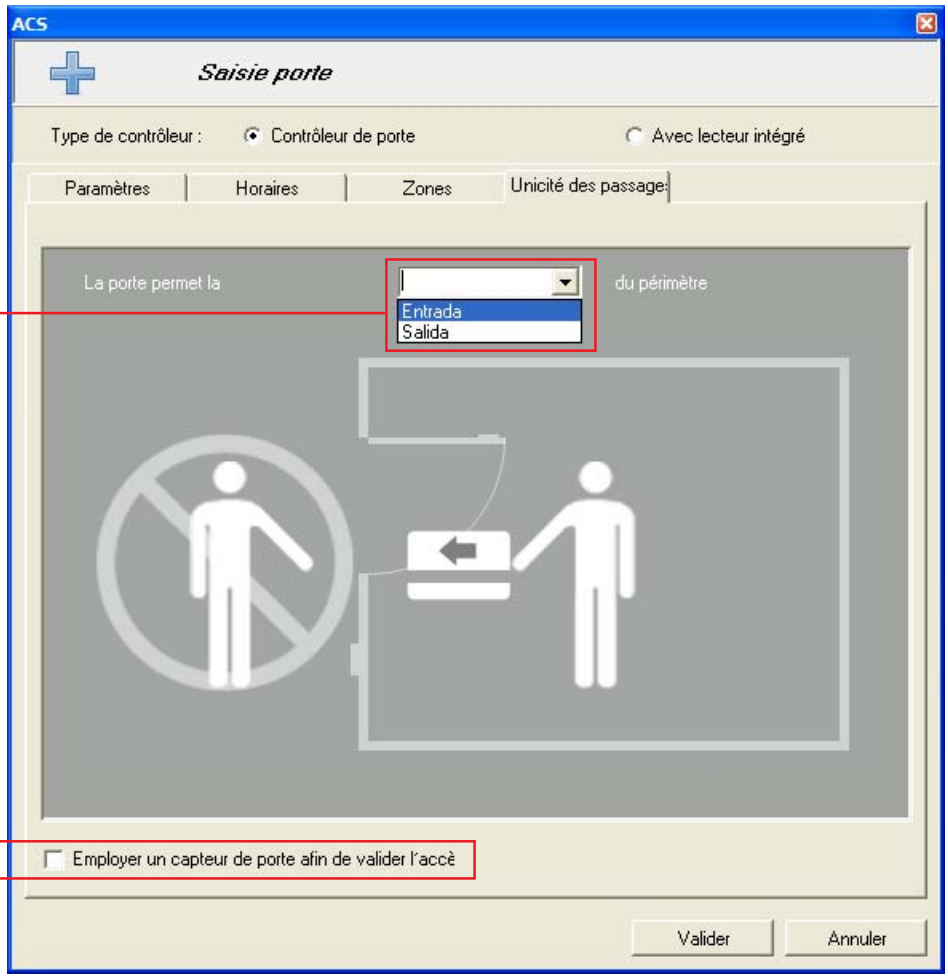
- La fonction d'unicité des passages est disponible pour tout identificateur (proximité, contact, clavier...)

**** Comment mettre en place la fonction unicité des passages (antipassback)***

Afin d'effectuer la fonction d'unicité des passages (au niveau global de l'installation), il faut définir pour chaque porte faisant partie du périmètre de l'installation s'il s'agit de portes permettant d'***entrer*** ou de ***sortir***.



(*) Les portes qui disposent d'un contrôleur de porte peuvent être utilisées aussi bien pour entrer que pour sortir avec un seul contrôleur (lecteur d'entrée et lecteur de sortie sur le même contrôleur de porte). En fonction du sens de passage, l'on saura si l'utilisateur entre dans le périmètre ou en sort.



* ***Utiliser le capteur de porte afin de valider l'accès :*** si cette option est activée, le système ne considère pas l'utilisateur comme étant à l'intérieur du périmètre de l'installation tant que les portes ne s'ouvrent pas. De cette façon, l'on évite qu'un utilisateur ayant présenté un identificateur valide à une porte du périmètre et qui, pour un motif quelconque, déciderait de ne pas entrer (de ne pas ouvrir la porte) reste enregistré comme étant à l'intérieur de l'installation et que, par la suite, il ne puisse y entrer (unicité des passages).

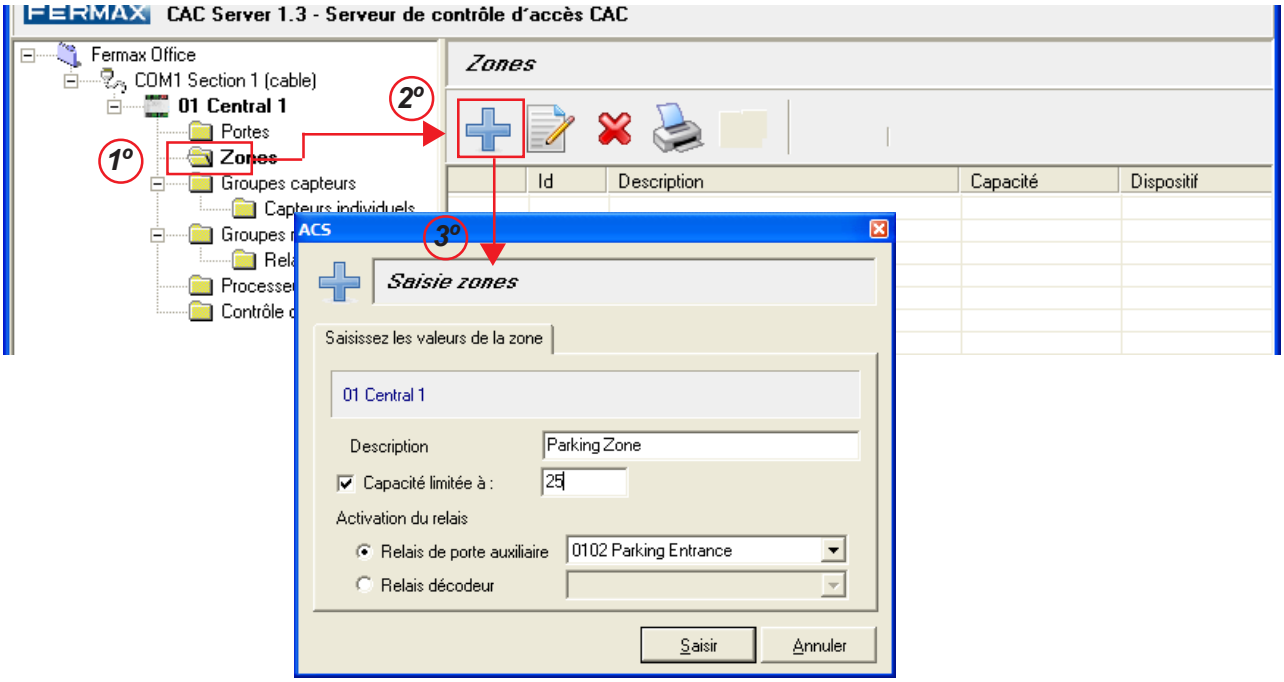
Pour cette fonction, il faut, en plus de l'activation de cette option, utiliser le capteur de porte. Dans le cas d'un accès pour véhicules, il est très intéressant de l'appliquer.

ZONES

Il n'est pas obligatoire de les définir. Ce ne sera le cas que si l'on souhaite utiliser la fonction **limitation du nombre de personnes** (capacité maximale dans une zone) ou la fonction **localisation des utilisateurs**.

Dans l'élément Portes (décrit dans la rubrique précédente, au cas où l'on souhaiterait employer ces fonctions de limitation du nombre de personnes ou contrôle de la capacité, il faut indiquer pour chaque porte la ***zone*** à laquelle l'on donne accès et la ***zone*** que l'on quitte en traversant cette porte. Afin de sélectionner ces zones pour chaque porte, il faut préalablement créer et configurer les zones de l'installation. Tout cela est expliqué dans cette rubrique.

Pour chaque centrale, le système CAC permet de créer et de gérer 32 zones maximum.



* ***Description :*** nom attribué à la zone (le nom d'une zone ne peut être utilisé plusieurs fois). Ce nom identifiera la zone sur toutes les applications serveur et client de l'installation.

* ***Capacité limitée à :*** cochez cette case si vous souhaitez mettre en place la fonction « limitation du nombre de personnes », c'est-à-dire attribuer à la zone une capacité d'utilisateurs maximale, et saisissez dans la case cette capacité.

Une fois cette capacité maximale atteinte, il n'est plus possible de laisser entrer un utilisateur dans la zone tant qu'un autre utilisateur n'aura pas quitté cette zone ou qu'il n'y aura pas eu de réinitialisation de la capacité.

Il est possible d'attribuer à la zone un relais, qui s'activera lorsque la capacité maximale de la zone aura été atteinte.

Il est également possible de définir une capacité 0. Dans ce cas, le nombre d'utilisateurs n'est pas restreint et le relais sélectionné s'active tant qu'il y a un utilisateur dans la zone.

* ***Activation du relais :*** permet de sélectionner le relais qui s'activera lorsque la capacité maximale de la zone sera atteinte.

- **Relais auxiliaire de la porte :** activez cette option et sélectionnez (dans la liste déroulante) le contrôleur de porte qui activera le relais auxiliaire une fois la capacité maximale atteinte.
- **Relais décodeur :** activez cette option et sélectionnez (dans la liste déroulante) la sortie de relais qui s'activera une fois la capacité maximale atteinte.

  Les listes déroulantes présentent les relais disponibles. Les relais et contrôleurs de porte (relais auxiliaire) doivent préalablement être définis dans l'application Server.

Si l'on souhaite uniquement mettre en place la fonction de localisation des utilisateurs (disponible dans l'application utilisateur CAC Map), il faut juste saisir une description de la zone.

Si la zone ne dispose pas de lecteurs de sortie et que cette dernière n'est pas contôlée, le compteur ne diminuera pas. Il faudra alors effectuer ce contrôle à partir de l'application CAC Access ou par le biais d'un identificateur de profil « réinitialisation du nombre limite de personnes ».

Un utilisateur comptabilisé dans la zone peut entrer plusieurs fois sans que le nombre de personnes augmente.

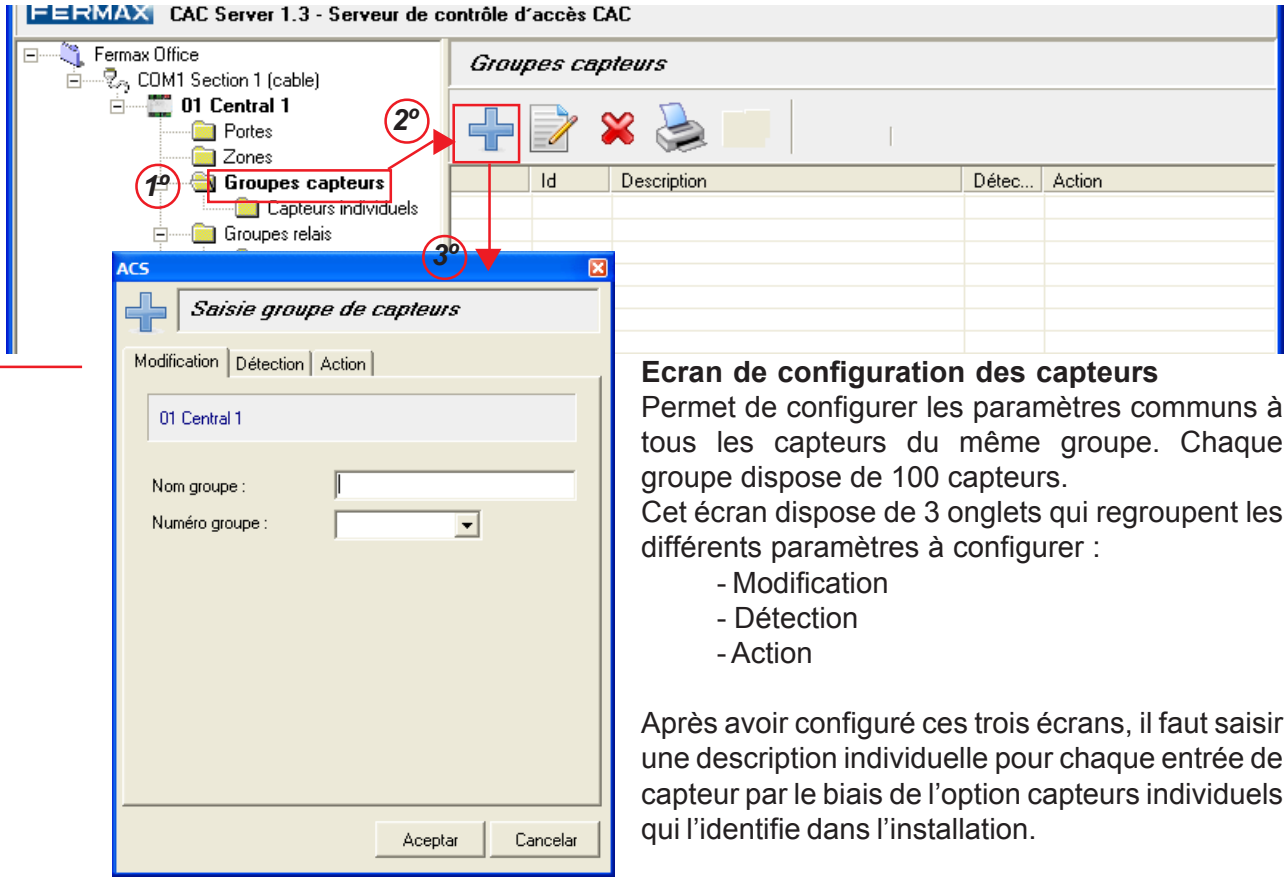
GROUPE CAPTEURS

Permer de définir les décodeurs des capteurs de l'installation et de configurer le fonctionnement de chacun d'entre eux.

Avant de configurer les décodeurs de capteurs à partir de l'application CAC Server, il faut avoir programmé à l'aide de l'application Decowin fournie avec la centrale CAC (s'il n'y a pas de centrale de conciergerie) :

- les adresses de chaque entrée de capteur de chaque décodeur
- la durée de détection : instantanée ou temporisée

Une fois les décodeurs programmés, ils sont définis et configurés dans l'application Server.



Ecran de configuration des capteurs
Permet de configurer les paramètres communs à tous les capteurs du même groupe. Chaque groupe dispose de 100 capteurs.
Cet écran dispose de 3 onglets qui regroupent les différents paramètres à configurer :

- Modification
- Détection
- Action

Après avoir configuré ces trois écrans, il faut saisir une description individuelle pour chaque entrée de capteur par le biais de l'option capteurs individuels qui l'identifie dans l'installation.

Modification

* ***Nom groupe :*** nom attribué au groupe de capteurs (le même ne peut être utilisé plusieurs fois). Cette description permettra d'identifier le groupe dans toutes les applications serveur et client de l'installation.

* ***Numéro groupe :*** sélectionnez le ***groupe de capteurs*** qui va être utilisé pour une fonction spécifique (par exemple, activer un relais lorsqu'un capteur s'active, envoyer des messages à la conciergerie, etc.)

  Groupe de capteurs : les entrées des décodeurs de capteur se programment (à l'aide de l'application Decowin) par le biais d'adresses à trois chiffres qui vont de 000 à 999.

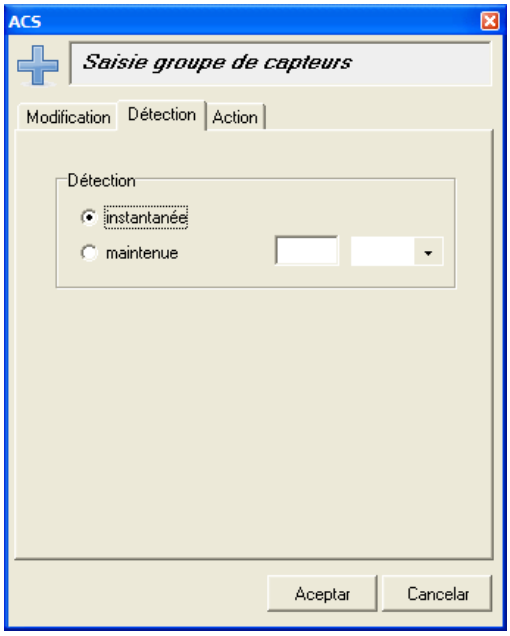
  Le groupe de capteurs 0 correspond aux entrées de capteur programmées de 000 à 099. Le groupe 1 correspond aux entrées de capteur allant de 100 à 199 et ainsi de suite.

  Lorsque l'on définit un groupe dans l'application Server, il est indiqué qu'il existe des décodeurs dont les entrées sont programmées à l'aide d'adresses appartenant à ce groupe. L'application connaît ainsi l'existence de ces décodeurs dans l'installation.

  Les paramètres et fonctions configurés sur les écrans suivants s'appliquent à toutes les entrées de capteur appartenant au groupe.

Détection

Sur cet écran est indiqué le type de détection des entrées de capteur correspondant au groupe, c'est-à-dire, la durée pendant laquelle le capteur doit être activé (en détectant) pour déclencher une alarme ou effectuer l'action configurée par le capteur.



* ***Instantanée :*** si l'entrée du capteur détecte une activité au niveau de l'entrée, elle communiquera cette détection immédiatement au système CAC (à la centrale à laquelle il est connecté) et effectuera l'action associée au groupe de capteurs.
* ***Continue :*** le capteur doit être activé continuellement pendant la période indiquée dans la case afin de communiquer cette détection au système CAC et effectuer l'action associée au groupe de capteurs.

  Si la détection prend fin avant que la durée de détection indiquée ne se soit écoulée, l'action associée ne se réalise pas.

  La durée de détection continue, introduite dans la case, peut être sélectionnée en secondes ou minutes.

REMARQUE IMPORTANTE

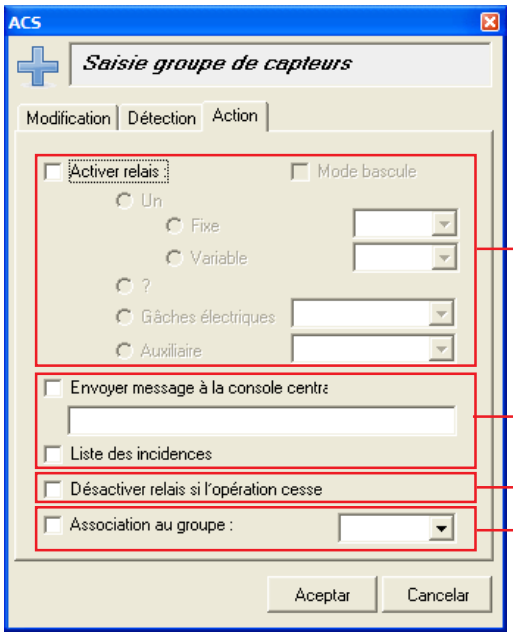
Comme on peut l'observer, les paramètres définis ici ont déjà été programmés précédemment sur les décodeurs de capteurs pour chaque entrée par le biais de l'application Decowin.

Le type de détection sélectionné sur cet écran doit coïncider avec celui programmé dans le décodeur par le biais de l'application Decowin.

Si le type de détection est modifié sur cet écran, pour qu'il soit mis à jour dans les entrées du capteur des décodeurs correspondants, il faudra mettre à jour la centrale (voir rubrique « Mettre à jour données de la centrale ») à partir de l'application Server et ensuite à partir d'une centrale de conciergerie raccordée à l'installation, entrer en programmation individuelle des décodeurs et valider chacune des sorties programmées appartenant au groupe ou par le biais de l'application Decowin, il faut reprogrammer de nouveau les décodeurs correspondants.

Action

L'on configure sur cet écran l'action ou les actions qu'effectuera le système CAC après une détection (instantanée ou continue) de l'une des entrées de capteur appartenant au groupe de capteurs défini.



Actions associées à la détection du capteur

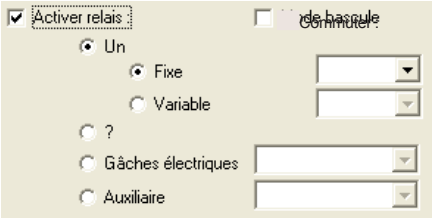
Activer/commuter relais

Créer des incidences et des avertissements

Synchroniser l'activation du relais avec la détection du capteur

Double détection

* ***Activer relais :*** si l'on coche cette case, lors d'une détection, un relais, un groupe de relais ou plusieurs relais s'activeront ou seront commutés selon les options sélectionnées.



- **Un :** indique que, lors de l'activation de toute entrée de capteur du groupe défini, ***une seule sortie*** d'un décodeur de relais sera activée :

  · **Commuter :** si l'on coche cette case, l'action associée au groupe de relais est la ***commutation du statut du relais***. Dans le cas contraire, l'action associée est l'activation du relais.

  · **Fixe :** pour chaque activation de capteur, ***l'on active toujours le même relais*** *(sortie de relais)* sélectionné dans la liste déroulante (la liste déroulante présente tous les *relais individuels* définis dans l'application).

  Exemple : *- Groupe de capteurs défini : 1.*
  - Relais fixe à activer/commuter sélectionné dans la liste déroulante : 105. ***(*)***
  - Fonctionnement : si l'on active toute entrée de capteur du groupe 1 (entrées programmées avec une adresse entre 100 et 199), ce sera toujours le relais 105 qui s'activera/sera commuté.

  · **Variable :** pour chaque activation d'une entrée d'un capteur, la sortie du groupe de relais sélectionné dans la liste dont les deux derniers chiffres de l'adresse coïncident avec les deux derniers chiffres de l'adresse du capteur activé s'activera.

  Exemple : *- Groupe de capteurs défini : 1.*
  - Groupe de relais sélectionné dans la liste : 4. **(*)**
  - Fonctionnement : si le capteur 125 s'active, la sortie de relais 425 s'active.
  si le capteur 101 s'active, la sortie de relais 401 s'active.

  Remarques
  (*) Chaque décodeur de relais de l'installation doit avoir des sorties programmées (par le biais de l'application Decowin) avec des adresses à 3 chiffres (de 000 à 999) et les groupes de relais et relais individuels correspondants doivent être définis dans l'application Server.
  L'activation de la sortie de relais s'effectue pendant la durée programmée pour chaque sortie du décodeur de relais. Dans le cas d'une commutation de relais, la durée d'activation programmée pour les sorties du décodeur de relais doit être « 0 ».

- **Plusieurs :** indique que, lors de l'activation de chaque entrée de capteur, ***toutes les sorties du groupe de relais*** dont le numéro de groupe coïncide avec le groupe de capteurs défini s'activeront.

  Exemple : *- Groupe de capteurs défini : 1.*
  - Fonctionnement : si toute entrée de capteur (par exemple : 108) s'active, toutes les sorties du groupe de relais 1, c'est-à-dire toutes les sorties du relais programmées sur les décodeurs de relais avec l'adresse 1XX (lors de la durée programmée pour ces sorties de relais) s'activent.

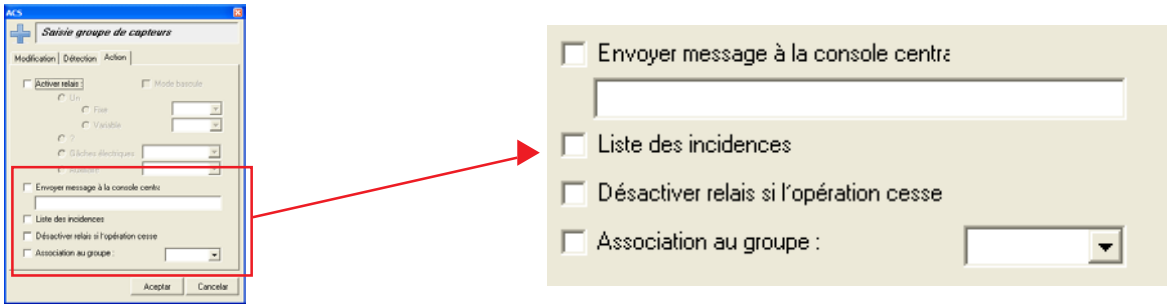
- **Gâche électrique :** indique que, lors de l'activation de n'importe quelle entrée de capteur du groupe, ***le relais de la gâche électrique de la porte*** sélectionnée dans la liste déroulante (la liste présente toutes les portes définies dans l'installation) s'activera.

  Exemple : *- Groupe de capteurs défini : 1.*
  - Gâche électrique, porte sélectionnée : entrée entreprise.
  - Fonctionnement : si une quelconque entrée de capteur du groupe 1 (entrées programmées avec una adresse allant de 100 à 199) s'active, le relais de la gâche électrique de la porte définie en tant que «entrée entreprise» s'activera.

- **Relais auxiliaire :** indique que, lors de l'activation d'une quelconque entrée de capteur du groupe, ***le relais auxiliaire de la porte*** sélectionnée dans la liste déroulante s'activera.

  La liste présente uniquement les portes qui disposent d'un type de contrôleur : ***contrôleur de porte***.

  Exemple : *- Groupe de capteurs défini : 1.*
  - Relais auxiliaire, porte sélectionnée : entrée parking.
  - Fonctionnement : si une quelconque entrée de capteur du groupe 1 (entrées programmées avec una adresse allant de 100 à 199) s'active, le relais auxiliaire de la porte définie en tant que « entrée parking » s'activera.



* ***Envoyer message à la console centrale :*** si cette case est cochée, lors de l'activation d'une quelconque entrée de capteur du groupe, le message décrit dans la case inférieure***est envoyé*** à la centrale de conciergerie de l'installation.

* ***Journal des incidences :*** si cette case est cochée, lors de l'activation d'une quelconque entrée du groupe de capteurs, les incidences d'activation et de désactivation de sortie du capteur correspondant ***sont envoyées*** à la centrale CAC et y sont enregistrées.

Les incidences enregistrées par la centrale peuvent être visualisées à partir des applications client.

* ***Désactiver le relais si cette action s'interrompt :*** si cette case est cochée, le relais ou groupe de relais associé au groupe de capteurs se désactive lorsque la détection du capteur s'interrompt.

Pour cette fonction, l'on utilise des relais programmés avec un fonctionnement bistable (durée d'activation «0» pour le décodeur de relais ou « 255 » pour le relais auxiliaire du contrôleur de porte) de sorte que le relais ne se désactive que lorsque la détection du capteur cesse.

Si la durée d'activation programmée pour le relais est inférieure à la durée de détection du capteur, celui-ci se désactivera avant que la détection du capteur ne cesse.

* ***Associé au groupe :*** permet d'associer le groupe de capteurs actuel à un autre groupe de capteurs, pouvant être sélectionné dans la liste déroulante.

Afin que cette option fonctionne correctement, le lien doit être réciproque, c'est-à-dire que si le groupe de capteurs 1 est associé au groupe de capteurs 3, il faut associer le groupe 3 au groupe 1.

Fonctionnement

Le fonctionnement des capteurs associés est le suivant (par exemple le groupe 1 est associé au groupe de capteurs 3 et vice versa) :

Chaque capteur d'un groupe va de paire avec l'équivalent d'un autre groupe, par exemple le capteur 125 est associé au capteur 325, le 143 au 343, etc.

Lorsque deux capteurs associés effectuent une détection simultanément, l'action associée au groupe du dernier capteur activé se réalise. ***Cette action est enregistrée dans le système en tant qu'incidence.***

Exemple :
- Le capteur 125 s'active : rien ne se produit (seule l'incidence est enregistrée si l'option en est activée).
- Le capteur 325 s'active (alors que le capteur 125 est actif) : l'action attribuée au groupe de capteurs 3 se réalise.

Les actions qui peuvent se produire lors de la détection simultanée sont les suivantes :
- *Activation du relais* ou groupe de relais attribué au groupe de capteurs activé en dernier.
- *Envoyer le message* attribué au groupe de capteurs activé en dernier à la console centrale.
- *Il est important que le relais défini soit le même dans les deux groupes.*

Les autres actions disponibles pour chaque groupe de capteurs s'effectuent individuellement au moment de l'activation/désactivation du capteur correspondant :

- *Journal des incidence*s : s'il est activé, l'activation/désactivation du capteur correspondant est enregistrée.
- *Désactiver le relais si cette action s'interrompt* : s'il est activé, lorsque la détection du capteur s'interrompt, le relais activé attribué au capteur se désactive.

Capteurs individuels

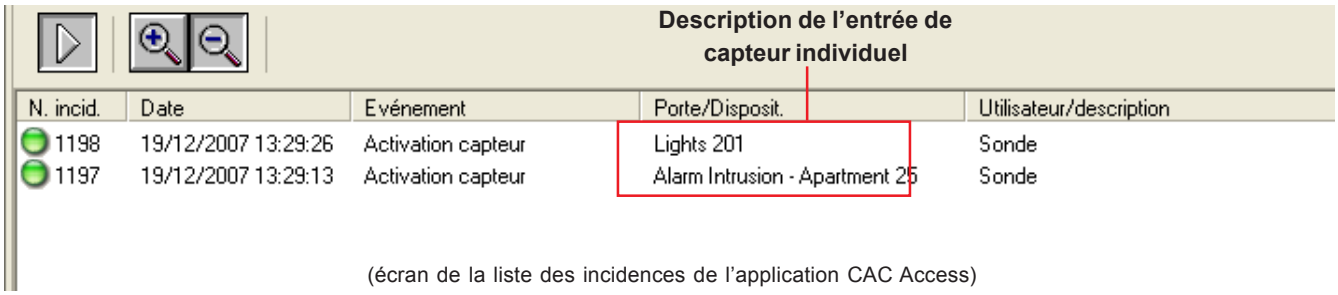
Permet de décrire individuellement chaque entrée des décodeurs de capteurs de l'installation.

* Pourquoi définir des capteurs individuels :

- Pour identifier beaucoup plus simplement le capteur qui a déclenché un événement.

  Pour chaque entrée de capteur, une description (nom du capteur) qui l'identifie dans l'installation et dans les différentes applications client est saisie.

  De cette manière, lorsqu'un événement se produit sur l'une des entrées de capteurs définies individuellement, l'incidence enregistrée présentera la description attribuée au capteur. Dans le cas contraire, elle présente juste l'adresse du capteur.

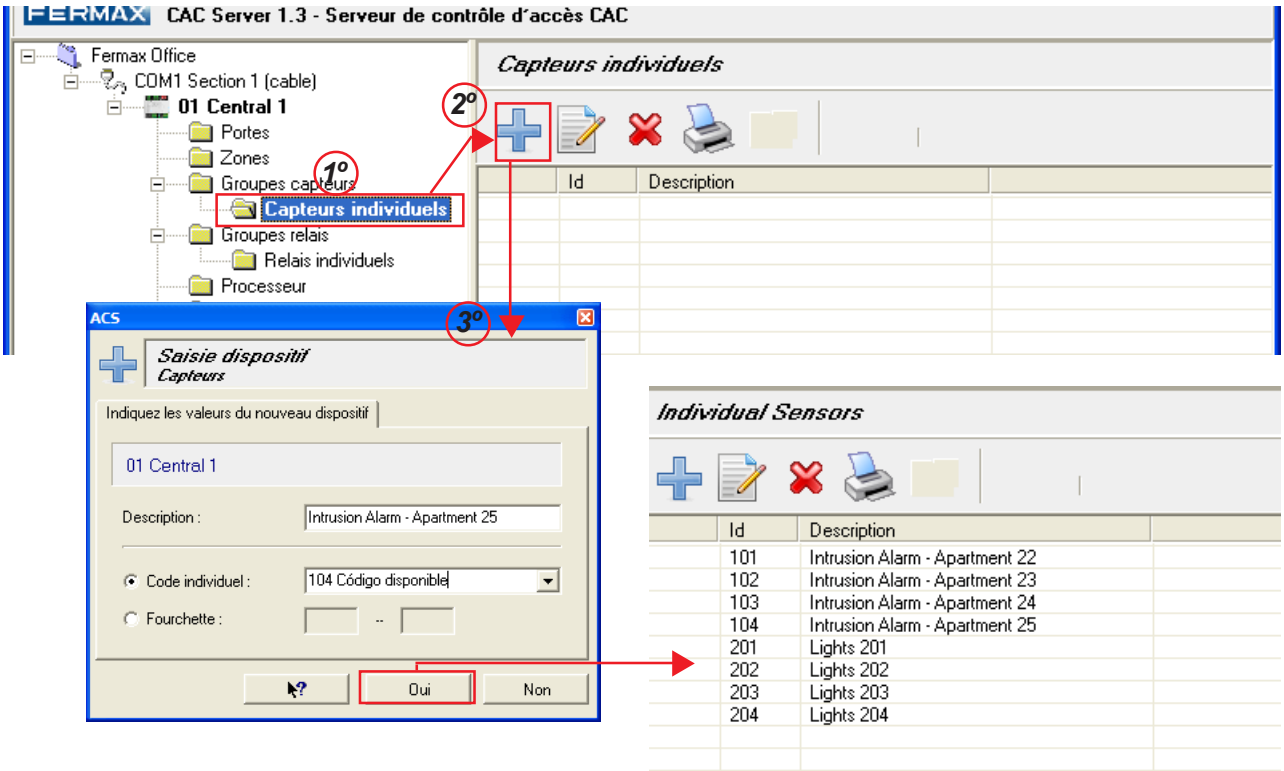


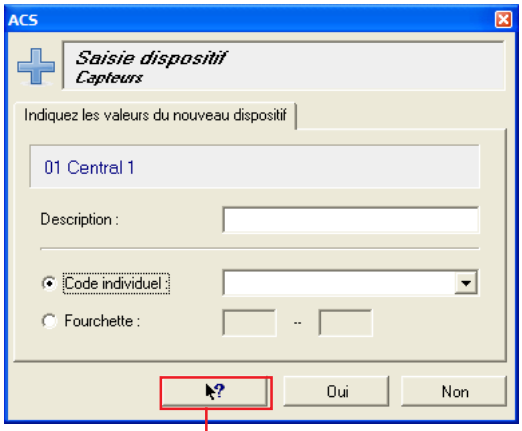
(écran de la liste des incidences de l'application CAC Access)

- Le fait de décrire les entrées de capteur individuellement permet, ultérieurement, pour d'autres options de l'application Server (comme c'est le cas du processeur) ou pour des applications clients (attribuer activation/désactivation du capteur pour un utilisateur, contrôle des capteurs, etc.) de sélectionner et d'attribuer les entrées de capteur individuel.

* Mode de fonctionnement des capteurs individuels :

Le mode de fonctionnement des capteurs individuels dépend de la configuration effectuée pour le groupe de capteurs qui l'intègre (voir rubrique Groupe capteurs).



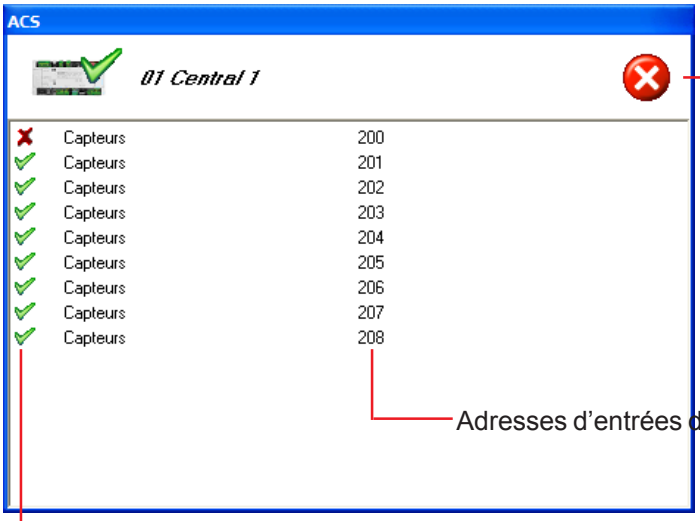


* ***Description :*** description attribuée à l'entrée du capteur ou à une file d'entrées du capteur.
Cette description identifiera l'entrée du capteur dans toutes les applications serveur et client de l'installation.

* ***Code individuel :*** permet de sélectionner l'entrée de capteur à laquelle est attribuée la description. La liste présente les adresses de toutes les entrées de capteur pouvant être sélectionnées.

* ***Fourchette :*** permet de saisir une fourchette d'entrées de capteur (adresse début-adresse fin) auxquelles est attribuée la même description. Par exemple, entrées de capteur avec les adresses à partir de la 201 jusqu'à la 205.

Effectue un test de l'entrée de capteur ou de la fourchette sélectionnée.



Fermeture de l'écran de test.

Adresses d'entrées de capteur vérifiées.

Résultat du test :

Entrée de capteur détectée.

Entrée de capteur non détectée.

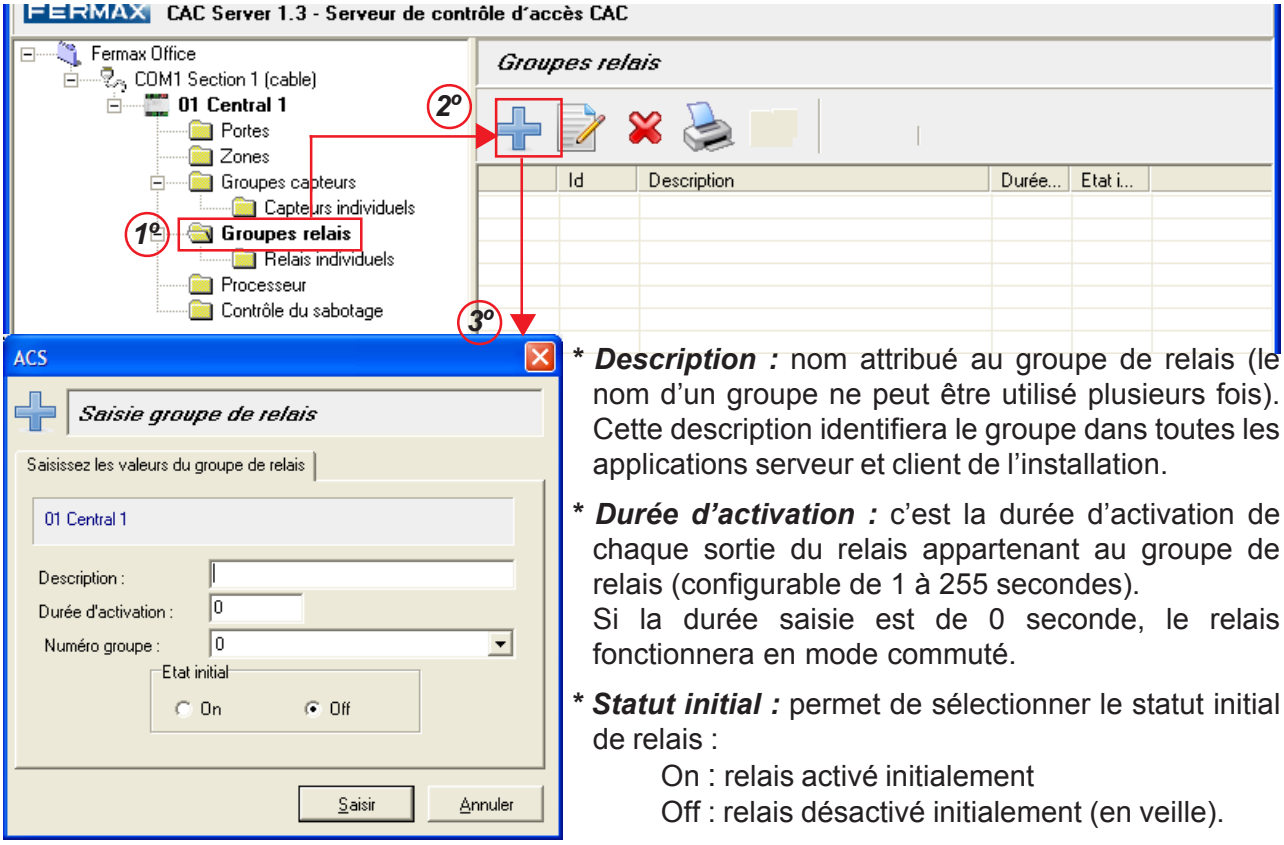
GROUPE RELAIS

Permet de définir les décodeurs de relais de l'installation et de configurer le fonctionnement de chacun.

Avant de configurer les décodeurs de relais à partir de l'application CAC Server, il faut avoir programmé, par le biais de l'application Decowin (fournie avec la centrale CAC) :

- les adresses de chaque sortie de relais de chaque décodeur,
- la durée d'activation,
- le statut initial : On (activé), Off (désactivé).

Une fois les décodeurs programmés, ils sont définis et configurés dans l'application Server.



* ***Description :*** nom attribué au groupe de relais (le nom d'un groupe ne peut être utilisé plusieurs fois). Cette description identifiera le groupe dans toutes les applications serveur et client de l'installation.

* ***Durée d'activation :*** c'est la durée d'activation de chaque sortie du relais appartenant au groupe de relais (configurable de 1 à 255 secondes).
Si la durée saisie est de 0 seconde, le relais fonctionnera en mode commuté.

* ***Statut initial :*** permet de sélectionner le statut initial de relais :

On : relais activé initialement
Off : relais désactivé initialement (en veille).

* ***Numéro groupe :*** sélectionnez le ***groupe de relais*** qui va être utilisé pour une fonction spécifique (par exemple : activer l'éclairage, activer l'alarme, avertissement de capacité maximale, etc.) Un groupe comprend 100 relais.

Groupe de relais : les sorties des décodeurs de relais se programment (à l'aide de l'application Decowin) par le biais d'adresses à trois chiffres qui vont de 000 à 999.

Le groupe de relais 0 correspond aux entrées de relais programmées de 000 à 099. Le groupe 1 correspond aux entrées de capteur allant de 100 à 199 et ainsi de suite.

Lorsque l'on définit un groupe de relais dans l'application Server, il est indiqué qu'il existe des décodeurs dont les sorties sont programmées à l'aide d'adresses appartenant à ce groupe. L'application connaît ainsi l'existence de ces décodeurs dans l'installation.

REMARQUE IMPORTANTE

Comme on peut l'observer, les paramètres définis ici ont déjà été programmés précédemment sur les décodeurs de relais pour chaque sortie par le biais de l'application Decowin.

Les valeurs saisies dans les champs « durée d'activation » et « statut initial » de cet écran doivent coïncider avec celles programmées dans le décodeur par le biais de l'application Decowin.

Si ces paramètres sont modifiés sur cet écran, afin que les sorties des décodeurs de relais correspondants soient mises à jour, il faudra mettre à jour la centrale (voir rubrique « Mettre à jour les données de la centrale ») à partir de l'application Server et ensuite à partir d'une centrale de conciergerie raccordée à l'installation, entrer en programmation individuelle des décodeurs et valider chaque sortie programmée appartenant au groupe ou reprogrammer par le biais de l'application Decowin les décodeurs correspondants.

Relais individuels

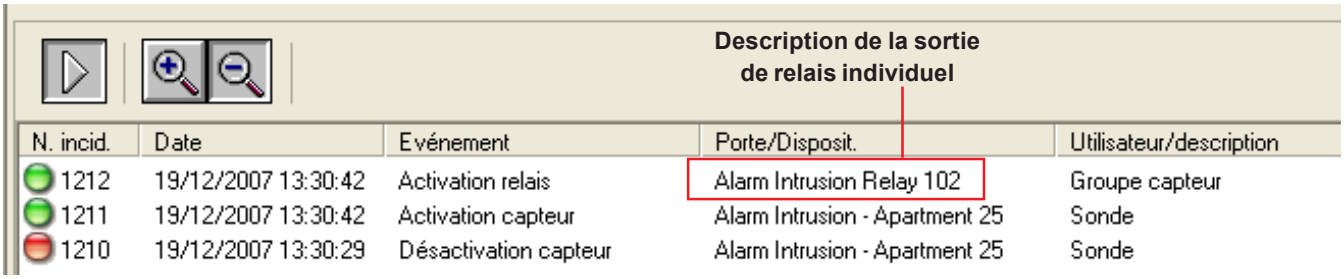
Permet de décrire individuellement chaque sortie des décodeurs de relais de l'installation.

* Pourquoi décrire les relais individuels :

- Pour identifier beaucoup plus simplement le relais qui a provoqué un événement (activé/désactivé).

  Pour chaque sortie de relais, une description (nom de relais) qui l'identifie dans l'installation et dans les différentes applications client est saisie.

  De cette façon, lors de l'activation/désactivation de l'une des sorties de relais définies individuellement, l'incidence enregistrée présentera la description attribuée au relais. Dans le cas contraire, elle présente uniquement l'adresse de relais.

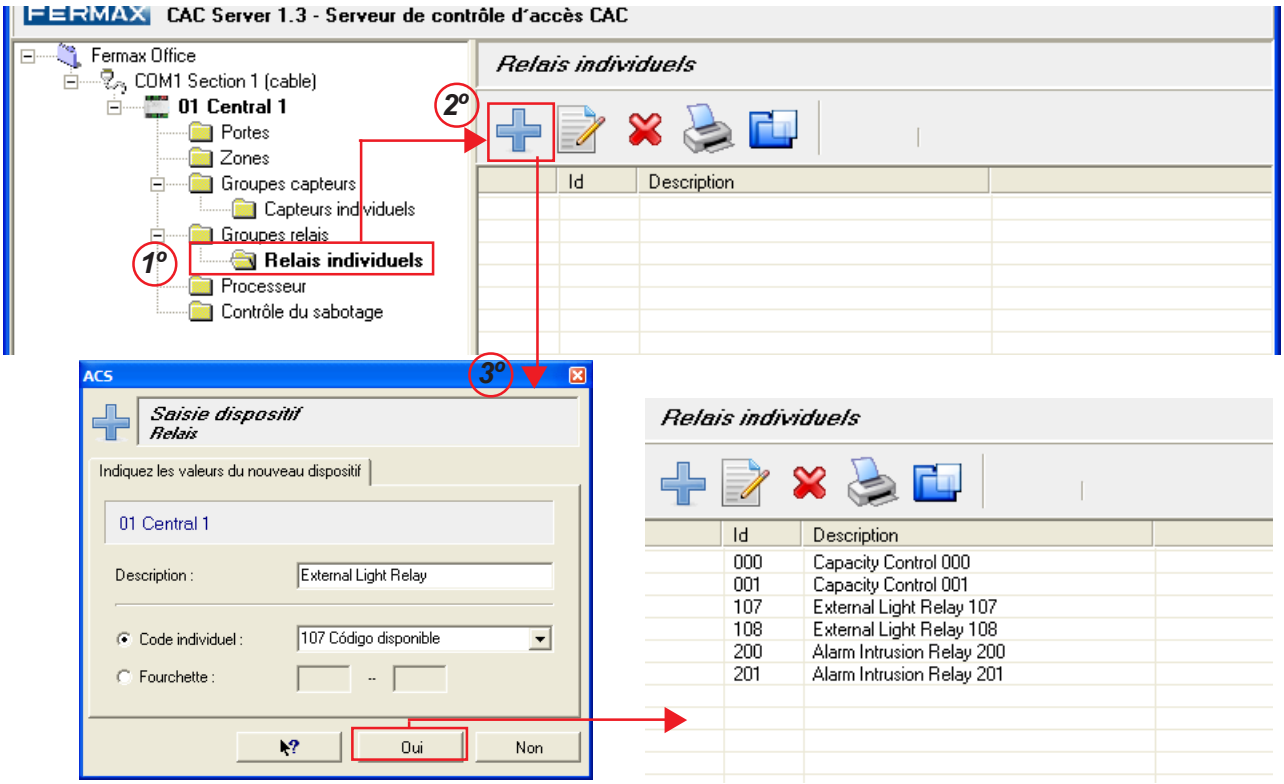


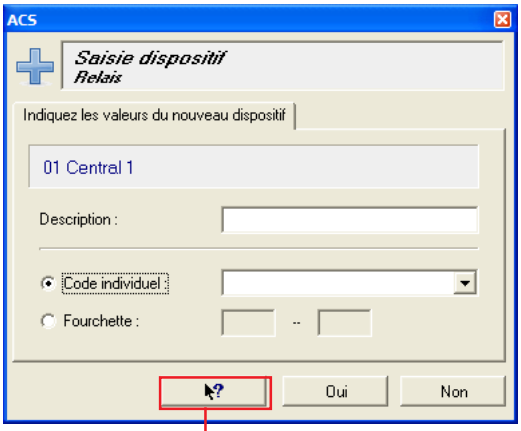
(écran de la liste des incidences de l'application CAC Access)

- Décrire les sorties de relais individuellement permet, par la suite, de sélectionner et d'attribuer des sorties de relais individuels sur d'autres options de l'application Server (comme c'est le cas du processeur, portes, capteurs, etc.) ou sur des applications client (activation de relais par utilisateur, contrôle de relais, etc.)

* Mode de fonctionnement des relais individuels :

Le mode de fonctionnement des relais individuels dépend de la configuration effectuée par le groupe de relais qui l'intègre (voir rubrique Groupe de relais).



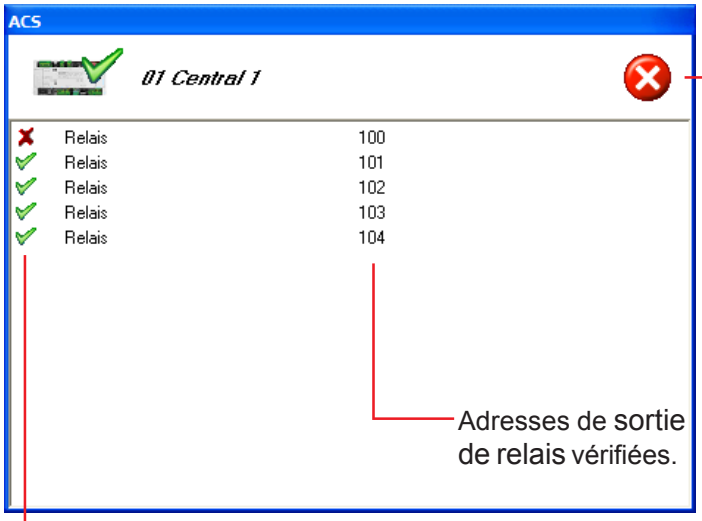


* ***Description :*** description attribuée à la sortie de relais ou à la fourchette de relais.
Cette description identifiera chaque sortie de relais dans toutes les applications serveur et client de l'installation.

* ***Code individuel :*** permet de sélectionner la sortie de relais à laquelle est attribuée la description. La liste présente les adresses de toutes les sorties de relais pouvant être sélectionnées.

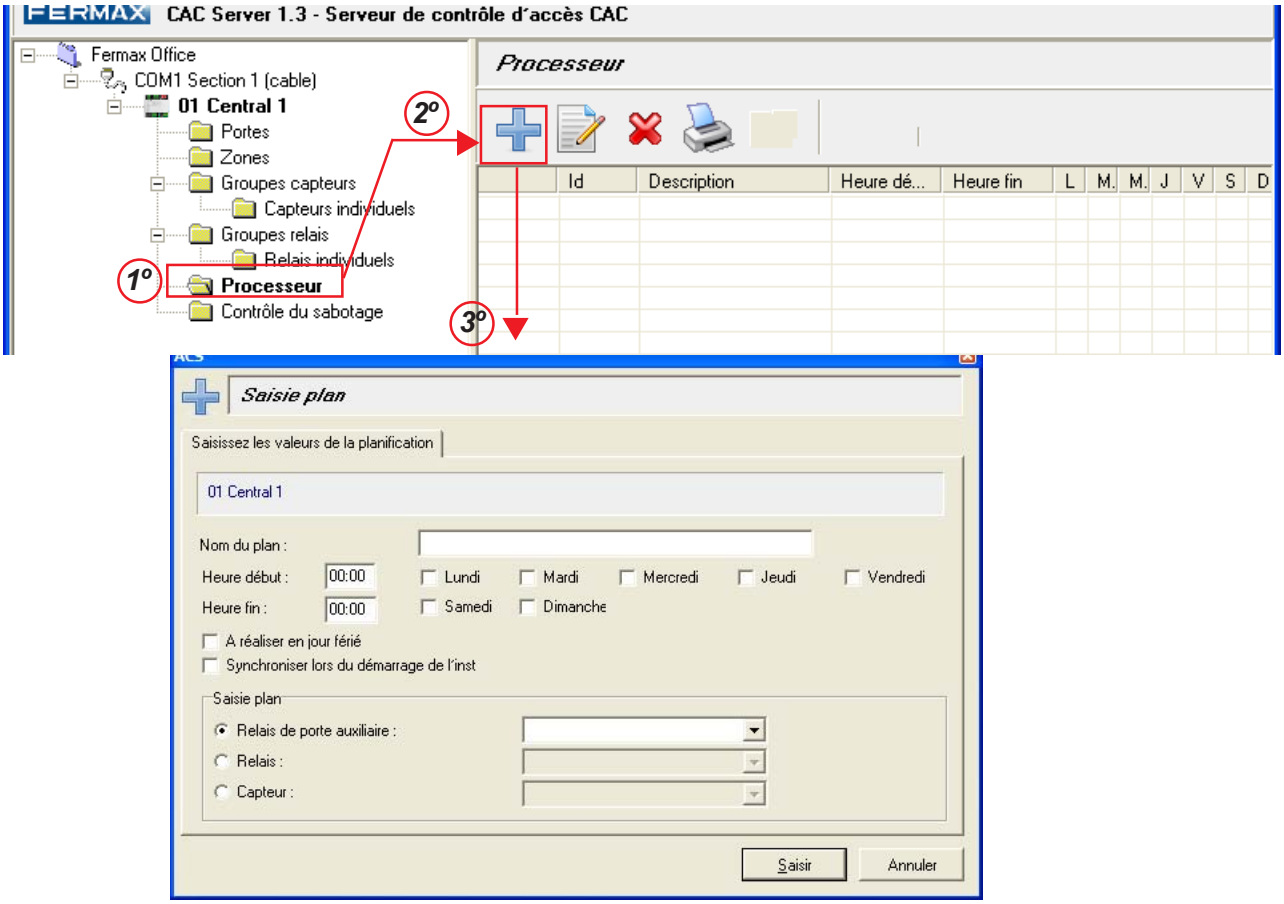
* ***Fourchette :*** permet de saisir une fourchette de sorties de relais (adresse début-adresse fin) auxquelles la même description a été attribuée. Par exemple, sorties de relais avec adresses allant de 201 à 205.

Effectue un test de la sortie de relais ou fourchette sélectionnée par le biais du bus de décodeurs afin de vérifier qu'il y en ait dans l'installation.



PROCESSEUR

Le système CAC permet d'effectuer jusqu'à 32 plans d'automatisation (par centrale) pour le contrôle des dispositifs.



Les paramètres suivants sont définis dans chaque plan :

* ***Nom du plan :*** nom attribué au plan (le nom d'un plan ne peut être utilisé plusieurs fois).
  Cette description identifiera le plan d'automatisation sur toutes les applications serveur et client de l'installation.

* ***Heure début :*** heure de démarrage du plan à laquelle une action déterminée se produit. L'action à effectuer dépend de l'élément sélectionné dans le champ «Ajout plan» :

  - *Capteur* : le capteur sélectionné se **désactive**.
  - *Relais* : l'action dépend de son statut initial.

Statut initial :	Action
Désactivé	Activer relais
Activé	Désactiver relais

* ***Heure fin :*** heure de finalisation du plan à laquelle une action déterminée se produit. L'action à effectuer dépend de l'élément sélectionné dans le champ « Ajout plan » :

  - *Capteur* : le capteur sélectionné s'**active**.
  - *Relais* : l'action dépend de son statut initial.

Statut initial :	Action
Désactivé	Désactiver relais
Activé	Activer relais

***Jours de la semaine :** indiquer les jours de la semaine auxquels le plan d'automatisation s'effectuera aux heures indiquées.

* ***Effectuer un jour férié :*** si cette case est cochée, cela signifie que le plan d'automatisation s'effectuera également les jours fériés programmés par le biais de l'application client CAC Access. Dans le cas contraire, le plan n'aura pas lieu les jours fériés.

* ***Synchroniser lors du démarrage de l'installation :*** si cette option est cochée, lors d'une réinitialisation de la centrale CAC (en raison d'une coupure, etc.), le plan qui aurait dû s'effectuer pendant la période à laquelle la centrale a cessé d'être fonctionnelle s'effectue lors de la réinitialisation du fonctionnement de la centrale.

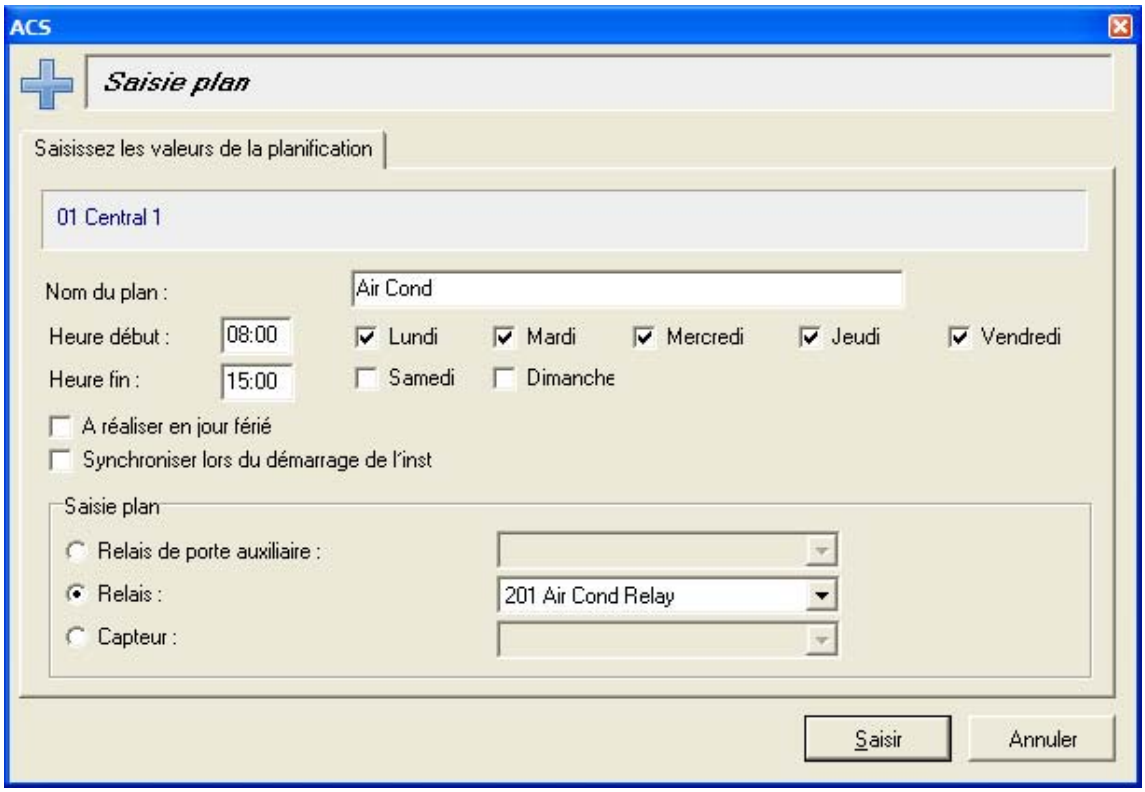
* ***Ajout plan :*** permet de sélectionner l'élément que l'on veut automatiser.
  - **Relais auxiliaire de la porte :** permet de sélectionner le contrôleur de porte qui activera/désactivera son relais auxiliaire lorsque le plan d'automatisation commencera ou finalisera.
  - **Relais :** permet de sélectionner la sortie de relais du décodeur qui s'activera/désactivera lorsque le plan d'automatisation commencera ou finalisera.
  - **Capteur :** permet de sélectionner l'entrée de relais du décodeur qui s'activera/désactivera lorsque le plan d'automatisation commencera ou finalisera.

    Les listes déroulantes présentent les relais et capteurs disponibles qui ont préalablement été définis dans l'application Server en tant que : contrôleurs de porte, relais individuels ou capteurs individuels.

Exemple : plan air conditionné

Si l'on souhaite que le système d'air conditionné se connecte automatiquement du lundi au vendredi de 08 h 00 à 15 h 00.

Afin d'activer le système, l'on utilisera la sortie de relais du décodeur programmée avec l'adresse 201.

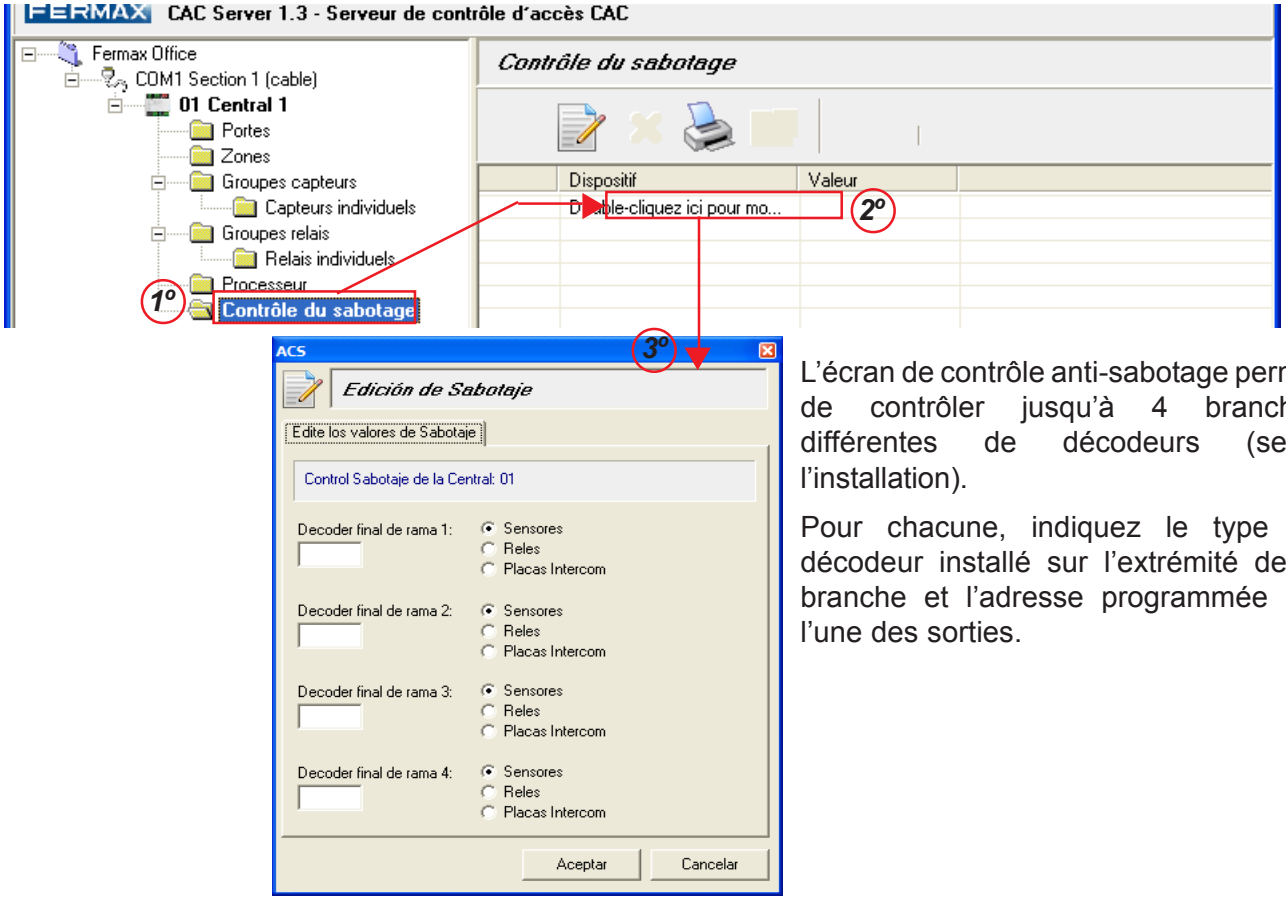


CONTROLE ANTI-SABOTAGE

Permet d'activer la fonction de détection du sabotage du bus de décodeurs (où sont connectés les décodeurs de relais, décodeurs de capteurs ou décodeurs de platines pour l'intercommunication).

Pour cela, il faut indiquer le type de décodeur installé sur l'extrémité du bus et l'adresse programmée sur l'une des sorties.

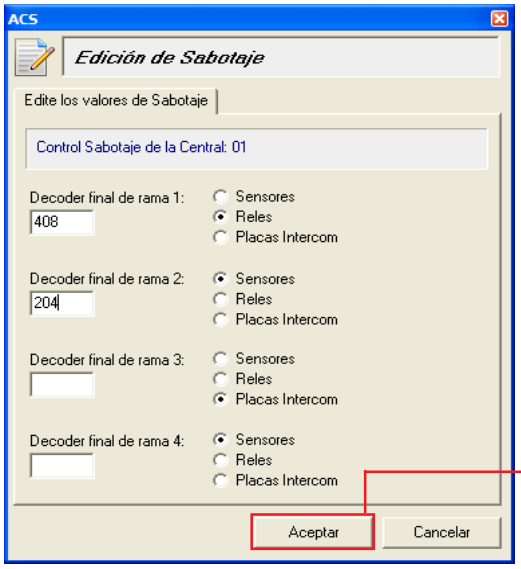
Si lors du processus de vérification du statut du bus de décodeurs qu'effectue la centrale toutes les 60 secondes, la centrale ne détecte pas l'adresse de la sortie indiquée, la centrale provoque une incidence anti-sabotage qui est stockée dans le journal des incidences et un message de sabotage est envoyé à la centrale de conciergerie (s'il y en a une).



L'écran de contrôle anti-sabotage permet de contrôler jusqu'à 4 branches différentes de décodeurs (selon l'installation).

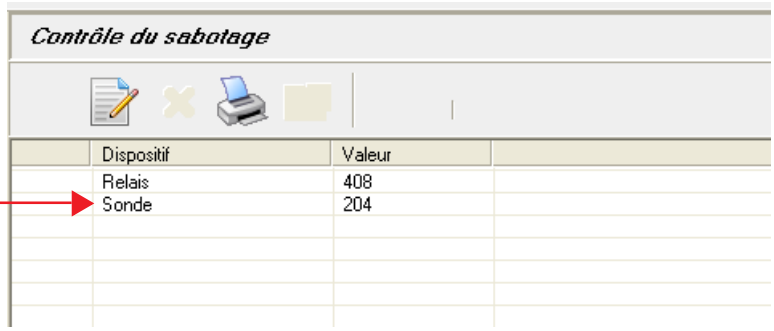
Pour chacune, indiquez le type de décodeur installé sur l'extrémité de la branche et l'adresse programmée sur l'une des sorties.

Exemple : l'on souhaite contrôler le sabotage du bus de décodeurs composé de deux branches : branche 1 et branche 2.



Le dernier décodeur de la branche 1 est un décodeur de relais dont l'une des sorties est programmée avec l'adresse 408.

Le dernier décodeur de la branche 1 est un décodeur de capteurs dont l'une des entrées est programmée avec l'adresse 204.

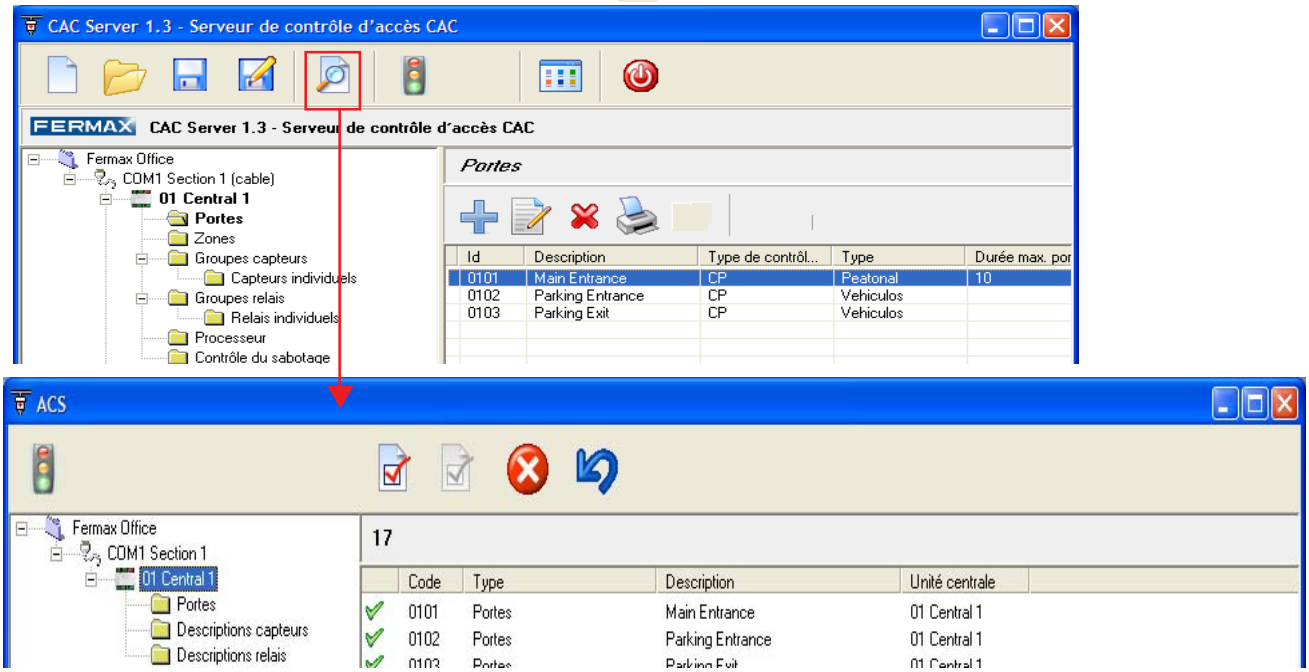


TEST DE L'INSTALLATION

L'application Server permet d'effectuer un test des éléments installés et définis dans l'installation.

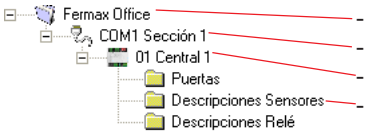
En effectuant le test, l'application Server vérifie que les éléments qui y sont définis existent dans l'installation et qu'il y ait communication entre les dispositifs et la centrale.

Afin d'accéder à l'écran de test, appuyez sur l'icone de l'écran principal de l'application.



Effectuer le test

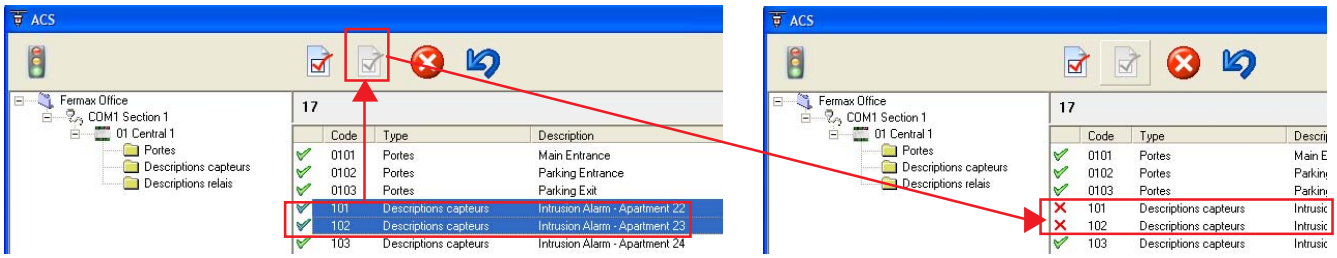
1º. Sélectionnez le groupe des éléments sur lesquels effectuer le test :



- Toute l'installation : sections, centrales, portes, capteurs et relais.
- Tous les éléments d'une section de l'installation : centrales, portes, capteurs et relais.
- Tous les éléments d'une centrale d'une section : portes, capteurs et relais.
- Eléments d'une centrale : portes, capteurs ou relais d'une centrale.

Sur la partie supérieure droite de l'écran est présentée une liste de tous les éléments à tester.

2º Si vous ne souhaitez pas effectuer le test de l'un des éléments présentés dans la liste, sélectionnez l'élément (ou les éléments) dans la liste et appuyez sur le bouton :



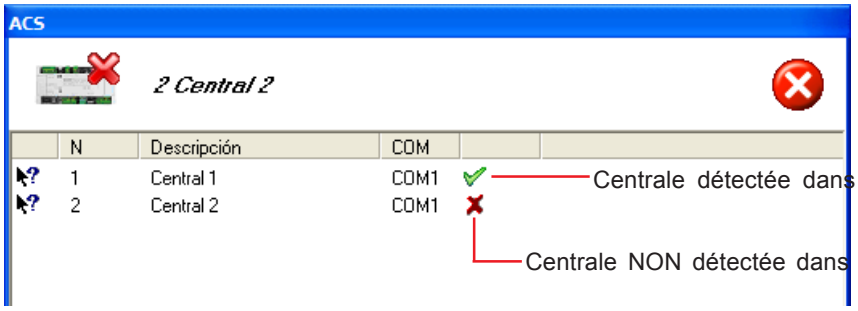
✕ indique qu'il n'y aura pas de test pour cet élément.

✓ indique que cet élément sera testé.

Afin de réactiver le test, sélectionnez l'élément et cliquez sur le bouton .

3º. Lancez le test : cliquez sur le bouton 

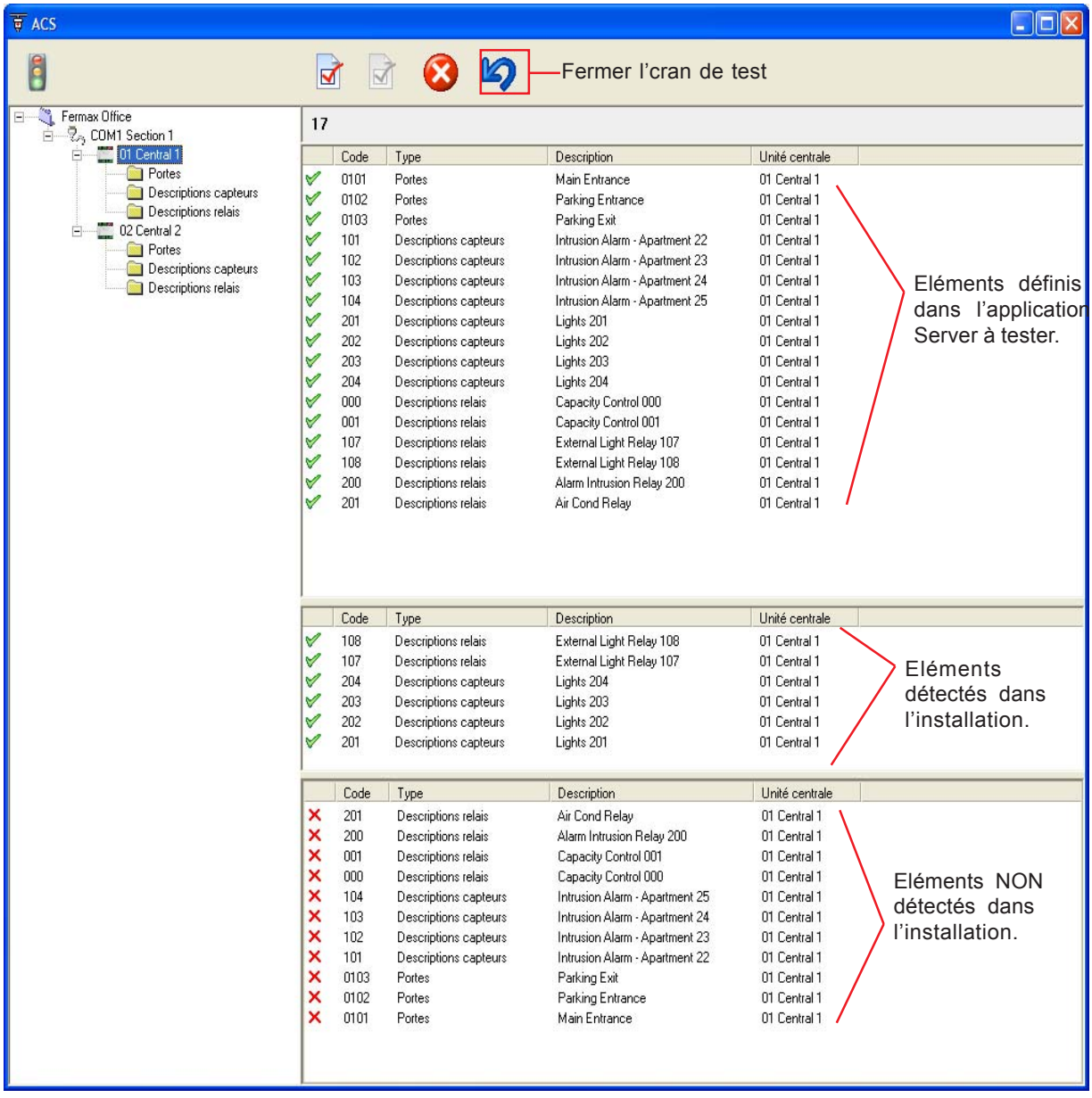
En premier lieu, l'on réalise un test des centrales existantes. L'écran suivant présentant le résultat du test s'affiche :



Si une centrale n'est pas détectée, l'application Server ne pourra effectuer un test des éléments définis pour cette centrale.

Afin de continuer le test, cliquez sur le bouton  .

Le résultat du test des éléments sélectionnés se présente par la suite.



MISE A JOUR DES DONNEES DANS LES CENTRALES CAC

Une fois tous les éléments de l'installation définis et les paramètres de l'application Server configurés, il faut mettre les centrales à jour, c'est-à-dire envoyer à chaque centrale de l'installation la configuration programmée.

Il est très important de mettre à jour les informations des différentes centrales de l'installation pour un correct fonctionnement du système CAC.

Mettre à jour les centrales

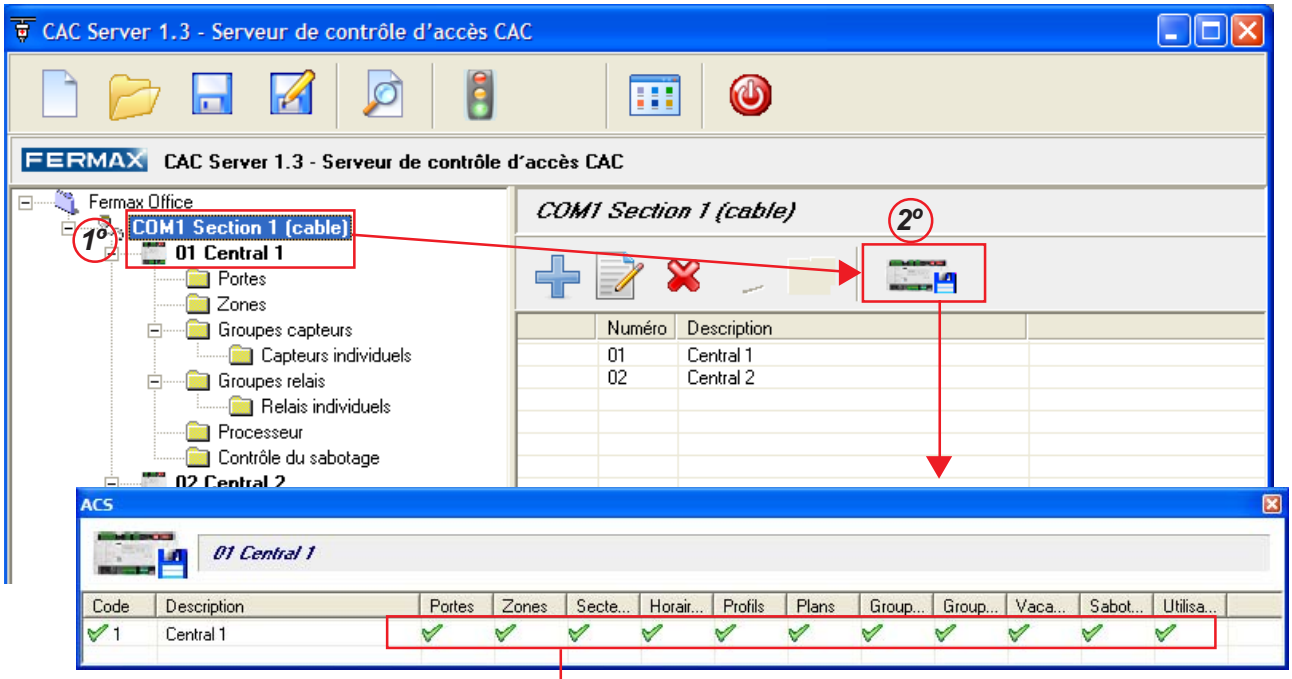
Chaque centrale peut être mise à jour de forme individuelle ou toutes les centrales d'une même section à la fois.

Chaque fois qu'un paramètre sera modifié, il faudra mettre à jour la centrale correspondante.

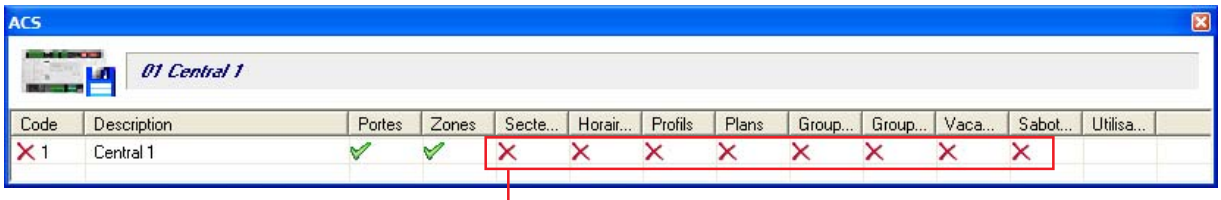
Les étapes à suivre pour mettre à jour les centrales sont les suivantes :

1º- ***Sélectionnez la centrale ou la section à mettre à jour***. Si l'on sélectionne une section, toutes les centrales de la section seront mises à jour.

2º- ***Cliquez sur le bouton***  ***pour commencer la mise à jour***. Un écran qui donne des informations sur le processus actuel et le résultat final de la mise à jour est présenté.



Eléments de la centrale (centrale 1) correctement mis à jour.



Eléments de la centrale NON mis à jour (il faut remettre à jour la centrale).

Les centrales fonctionnent maintenant de manière autonome en gérant les décodeurs, le processeur, le journal des incidences, etc., mais elles ont besoin des informations sur les utilisateurs, ce qui doit être indiqué au moyen des applications client.

Après avoir mis à jour les données dans les centrales du CAC Server, en fonction du nombre de centrales et de dispositifs de notre installation, il est conseillé d'attendre pendant un certain temps (5-20 secondes) avant d'activer les services afin que la mise à jour des données soit effectuée complètement sur tous les dispositifs.

LANCEMENT DES SERVICES

Une fois l'installation créée, configurée et mise à jour dans les centrales, la dernière étape à effectuer pour que le système CAC et les applications client et serveur commencent à fonctionner consiste à « **lancer les services** ».

En lançant les services, les applications serveur établissent une communication avec l'installation, de façon à ce que tout ce qui se produise dans l'installation reste mémorisé dans les serveurs. De plus, l'accès aux serveurs des applications client, lesquelles utiliseront les informations qui y sont mémorisées et configurées (les applications client stockent leurs propres informations dans le serveur dans la base de données) s'active.

Si les services ne sont pas lancés, l'installation CAC fonctionne correctement de manière autonome ; les événements survenus dans l'installation seront enregistrés dans chaque centrale avec l'inconvénient que les données ne seront pas stockées dans les serveurs jusqu'à ce que les services soient lancés.

Une fois les services lancés, les informations stockées dans les centrales sont envoyées aux serveurs.

De même, si les services ne sont pas lancés, les applications client ne pourront interagir avec l'installation et fonctionneront hors ligne jusqu'à ce que les services soient lancés.

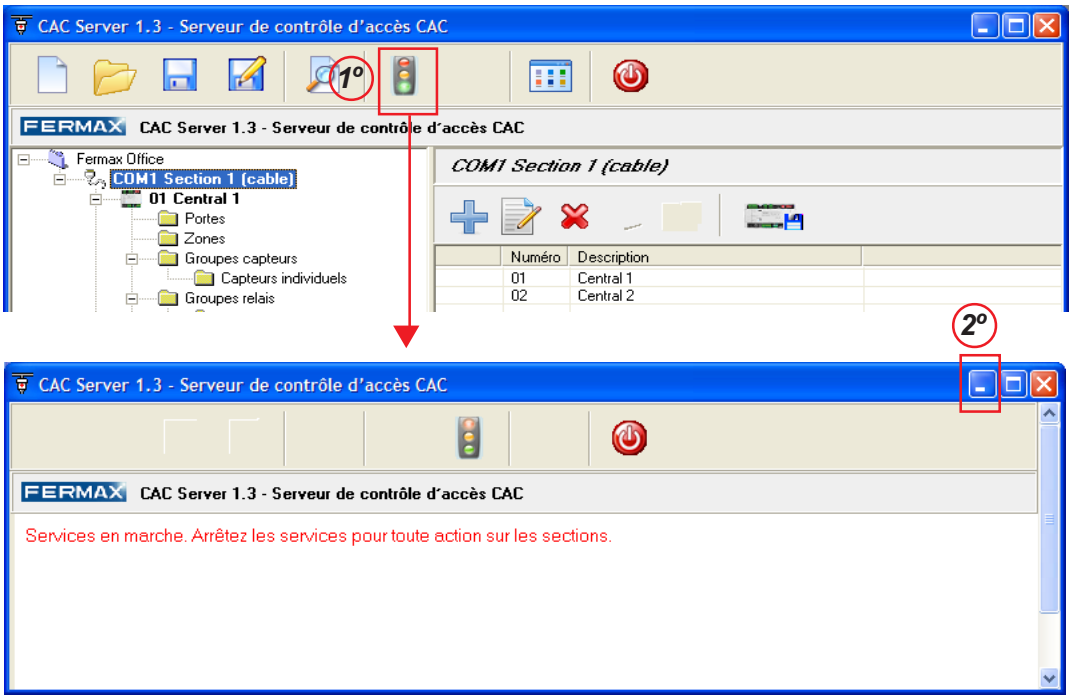
Les applications client détectent si les services sont lancés ou non en l'indiquant par le biais de messages d'alerte.

Afin de lancer les services, effectuez les étapes suivantes :

1º- Cliquez sur le bouton  : les services sont alors lancés et il est impossible de modifier la configuration de l'installation tant que les services sont actifs. Il est uniquement possible d'effectuer un test de l'installation.

2º- Réduisez l'écran du serveur : après avoir lancé les services, réduisez l'écran pour qu'il ne soit pas accessible auprès des utilisateurs non autorisés. En réduisant l'application, celle-ci est protégée par un mot de passe.

Afin de réduire l'écran, cliquez sur l'icone  situé sur la partie supérieure gauche de l'écran. A ce moment, un icone se crée dans la barre de lancement du PC () ; il indique que l'application est active et permet d'agrandir de nouveau l'application.

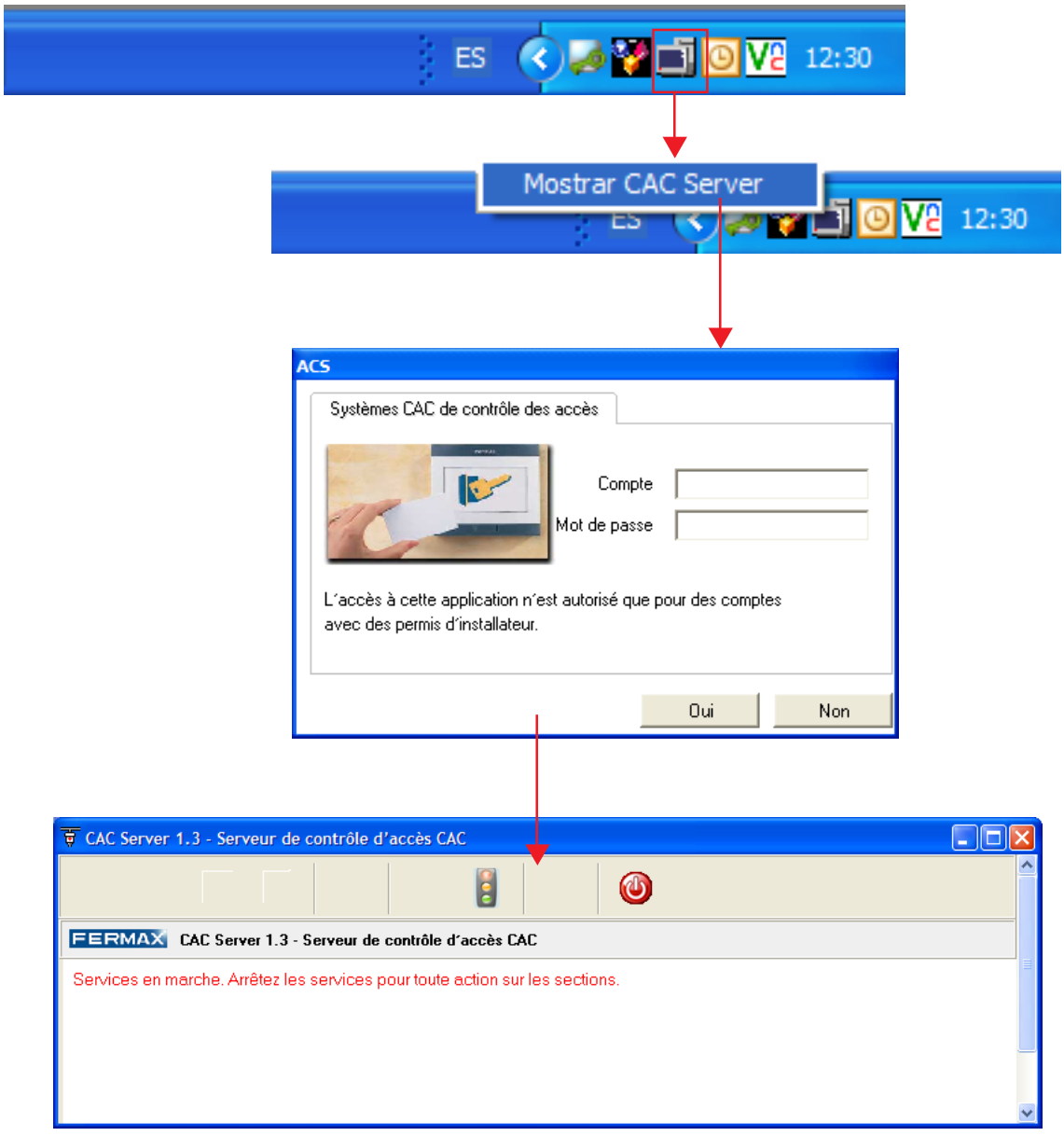


Agrandir l'écran du serveur

Afin d'agrandir l'écran du serveur, placez la souris sur l'icone  situé sur l'écran de démarrage et cliquez sur le bouton droit.

Dans le menu contextuel, sélectionnez « Afficher MDS Server », l'écran de compte utilisateur-mot de passe apparaîtra afin de contrôler l'accès à l'application.

Saisissez l'identifiant et le mot de passe afin de pouvoir accéder au serveur.



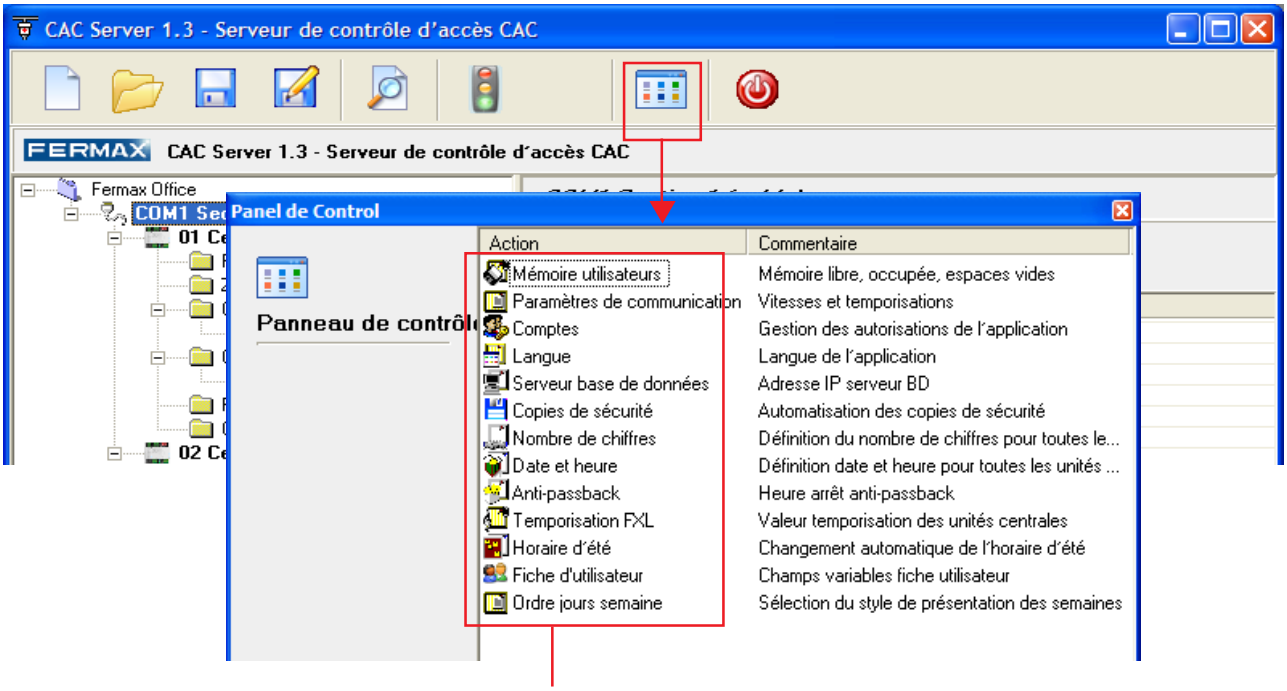
Arrêt des services

Afin de modifier la configuration de l'installation par le biais de l'application Server, les services doivent être désactivés.

Afin de désactiver les services, cliquez sur le bouton  .

PANNEAU DE CONTRÔLE

Le panneau de contrôle est un ensemble d'options et paramètres de configuration généraux, aussi bien des centrales de l'installation que de l'application CAC Control Server.

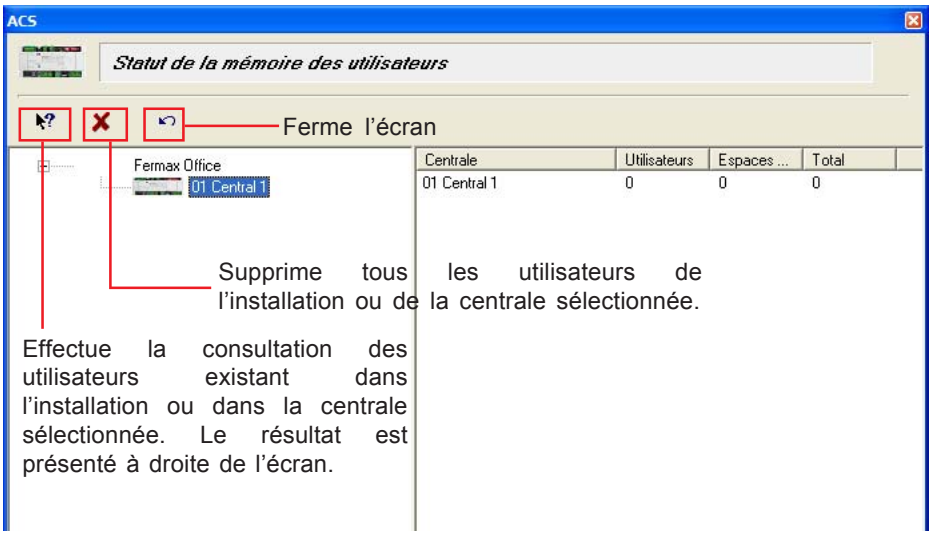


En double-cliquant sur chacune des options, l'écran suivant apparaît :

Mémoire utilisateurs

Présente des informations relatives au statut d'utilisation de la mémoire d'utilisateurs des centrales de l'installation :

- Utilisateurs : nombre d'utilisateurs existant dans la centrale.
- Vides : un vide est une position de mémoire initialement occupée par un utilisateur qui a été supprimé, qui reste disponible afin d'être utilisée lors de l'ajout d'un nouvel utilisateur.



Paramètres de communication

Permet de configurer la vitesse de communication entre les centrales ainsi que d'autres paramètres de communication.

Ne pas modifier les valeurs indiquées sur cet écran.

Identifiants

Lorsqu'on lance une quelconque application logicielle du système CAC (applications serveur ou applications client), un identifiant et un mot de passe sont demandés. En fonction de l'identifiant avec lequel l'utilisateur obtient son accès, ce dernier aura plus ou moins de fonctions activées afin de gérer et contrôler l'installation à partir de l'application correspondante.

Il existe quatre niveaux d'identifiants applicables à toutes les applications serveur et client du système CAC : installateur, administrateur, opérateur et dossiers.

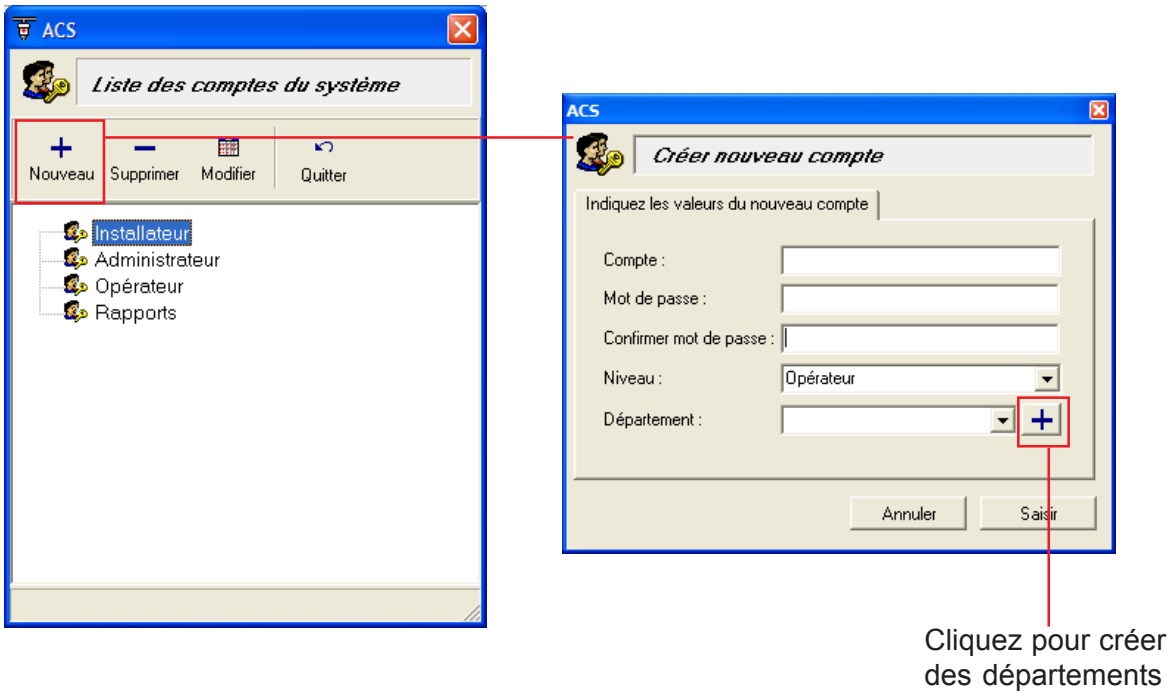
Dans le tableau suivant, les fonctions que peut effectuer un utilisateur en fonction de l'identifiant attribué sont précisées.

Identifiant	Applications serveur	Applications client
Installateur	Contrôle total	Contrôle total
Administrateur	Lancer applications - lancer services	Contrôle total
Opérateur	Aucune	Enregistrement/résiliation utilisateurs (*)
Dossiers	Aucune	Créer rapports

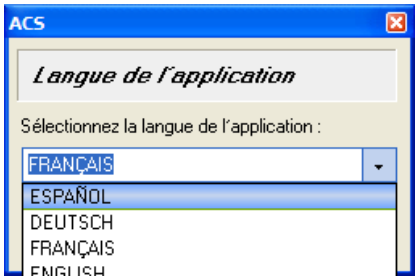
Important :

L'accès à l'application CAC Server est possible au moyen d'identifiants du niveau installateur et administrateur. Grâce au niveau installateur, il est possible d'exécuter toutes les options de l'application. Grâce au niveau administrateur, il n'est possible que de lancer les services.

(*) En définissant un identifiant du niveau opérateur, il est possible de l'associer à un département. Cette option est utile pour l'application CAC Access, de sorte que les opérateurs avec cette option ne peuvent que visualiser les utilisateurs qui appartiennent au même département. S'il n'est pas défini, cet identifiant pourra afficher / modifier tous les utilisateurs indépendamment du fait qu'un département leur soit associé.



Langue

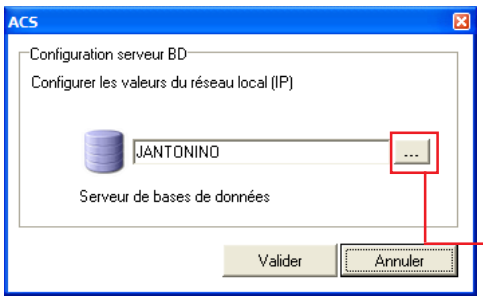


Permet de sélectionner la langue de l'application.

La liste des langues à sélectionner s'obtient directement à partir du fichier de la langue de l'application (CAC_Server_lang.INI).

Il faut réinitialiser l'application serveur afin de prendre en compte le changement de langue.

Serveur base de données

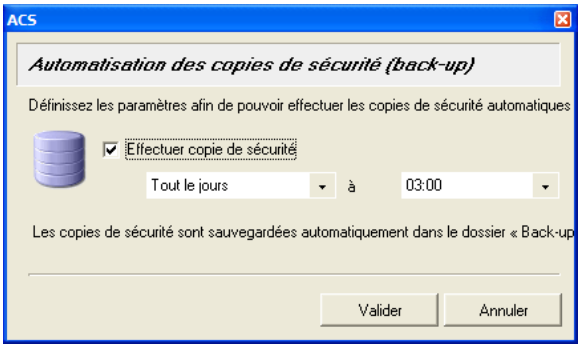


Permet de sélectionner de nouveau, si besoin (changement d'ordinateur, de topologie, etc.), l'emplacement de l'application CAC Database.

Il est possible d'utiliser aussi bien le nom de réseau de l'ordinateur que l'adresse IP (par exemple : 172.30.127.30).

Cliquez afin de sélectionner un équipement dans la liste des équipements disponibles sur le réseau.

Copies de sécurité

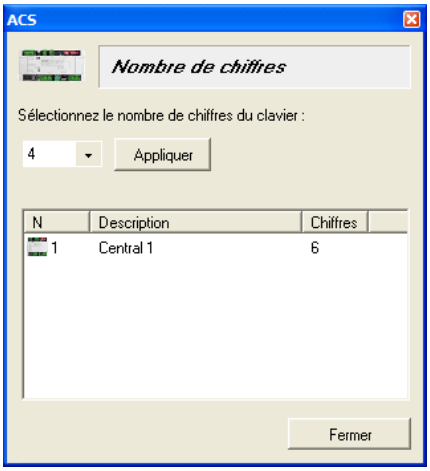


Cochez la case et sélectionnez les jours et heures auxquels le serveur effectuera une copie de sécurité de l'installation.

Les copies de sécurité sont stockées dans le dossier « Backups » placé dans le répertoire de l'installation de l'application CAC Server.

Ces copies de sécurité pourront être ensuite téléchargées à partir de l'option «Ouvrir» de l'écran principal de l'application.

Nombre de chiffres

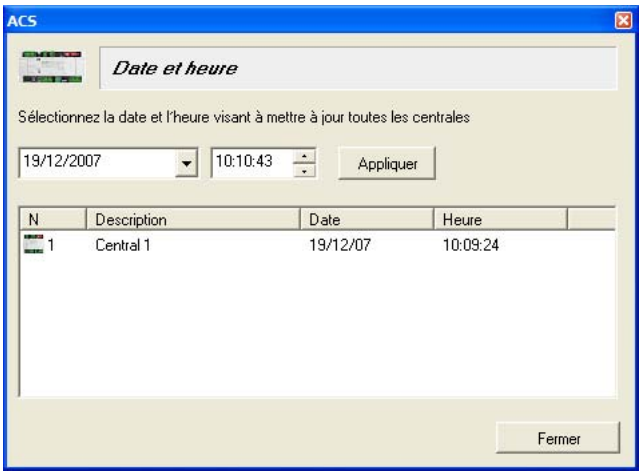


Cet écran permet de sélectionner le nombre de chiffres nécessaire à la saisie sur lecteurs et platines avec clavier.

Lors de l'accès à cet écran, le nombre de chiffres que possède chaque centrale s'affiche automatiquement (s'il n'y a pas de détection, le symbole « ? » s'affiche).

Afin de modifier le nombre de chiffres, sélectionnez la valeur souhaitée dans la liste déroulante (4, 5 ou 6) et cliquez sur « Appliquer ».

Date et heure

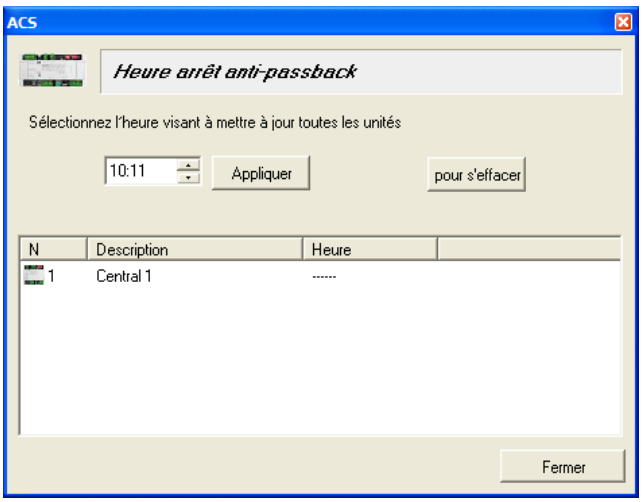


Cet écran permet de mettre à jour la date et l'heure de toutes les centrales définies dans l'installation.

Lors de l'accès à cet écran, la date et l'heure des centrales s'affichent automatiquement (s'il n'y a pas de détection, le symbole « ? » s'affiche).

Afin de mettre à jour la date et l'heure, saisissez les données date et heure correctes et cliquez sur « Appliquer ».

Heure arrêt antipassback



En cas de mauvaise utilisation du système de la part de l'utilisateur, tel que le départ de l'installation sans présenter l'identificateur en profitant de la sortie d'un autre utilisateur, cet utilisateur ne pourra accéder de nouveau à l'installation la prochaine fois qu'il le tentera puisque le système considère que l'utilisateur est toujours à l'intérieur.

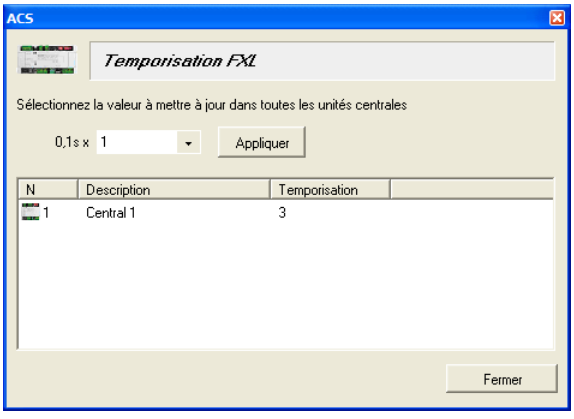
Afin d'éviter ce type de problème, il est possible de définir une heure d'arrêt de l'unicité des passages sur cet écran. A l'heure indiquée (généralement la nuit), le système met automatiquement tous les utilisateurs hors du périmètre de l'installation en autorisant de nouveau tous les utilisateurs pouvant être restés à l'intérieur à accéder à l'installation.

En accédant à cet écran, l'heure d'arrêt de l'unicité de passage des centrales s'affiche automatiquement (au cas où cette option serait désactivée, elle s'afficherait dans le champ heure : « ---- »).

Afin d'activer cette fonction, cochez la case « Activer », saisissez l'heure d'arrêt de l'unicité des passages et cliquez sur « Appliquer ».

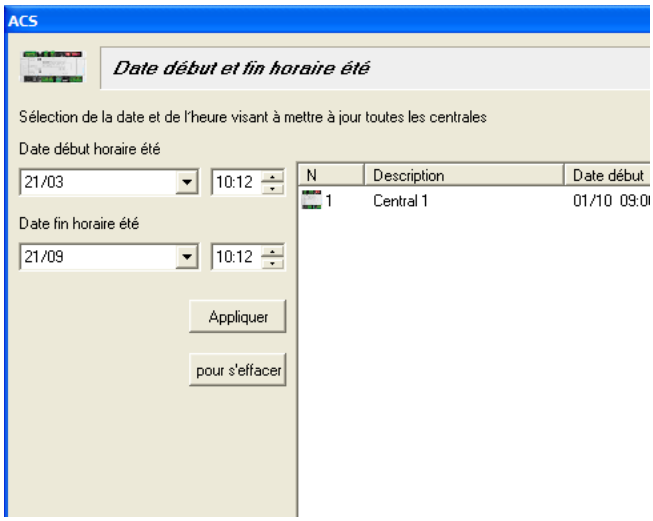
Afin de la désactiver, décochez la case « Activer » et cliquez sur « Appliquer ».

Temporisation FXL



Paramètre de configuration du système. Ne pas modifier les valeurs indiquées sur cet écran.

Horaire d'été



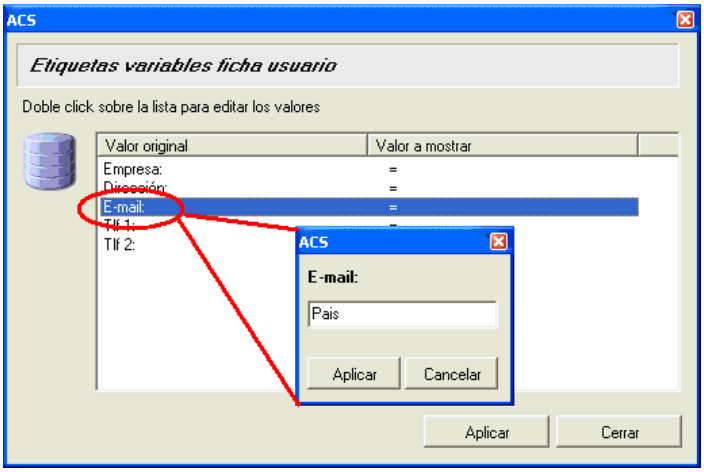
Cet écran permet d'activer le passage automatique de l'heure été-hiver pour les centrales de l'installation aux dates et heures indiquées en tant que début et fin de l'horaire d'été.

En accédant à cet écran, si cette option est activée, la date de début et fin de l'horaire d'été programmée dans les centrales s'affiche automatiquement.

Afin d'activer cette fonction, cochez la case « Activer », saisissez la date et l'heure de début et fin de l'horaire d'été et cliquez sur « Appliquer ». Afin de la désactiver, décochez la case « Activer » et cliquez sur « Appliquer ».

Il faudra mettre l'horaire d'été à jour tous les ans.

Fiche de l'utilisateur



Les étiquettes variables de la fiche utilisateur qui s'affichera dans l'application client « CAC Access » seront définies sur cet écran. Ces valeurs sont génériques, c'est-à-dire qu'il ne s'agit pas d'informations conservées dans les centrales, mais elles peuvent être utiles à l'utilisateur de l'application.

Afin de modifier cette valeur, double-cliquez sur l'étiquette à modifier. Lorsque la valeur de la liste est « = », cela signifie que l'étiquette de l'application CAC Access présentera ce qui est défini dans le fichier langue de l'application CAC Access. Dans cet exemple, la valeur « Pays » est définie en lieu et place de l'adresse électronique.

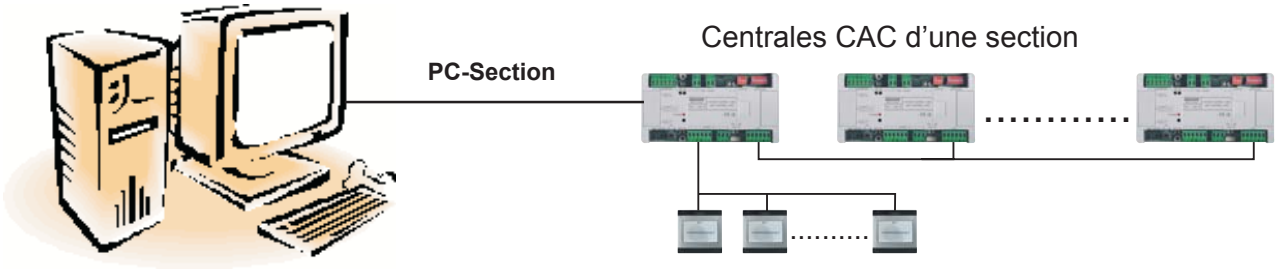
Ordre jours semaine

L'ordre dans lequel se présenteront les jours de la semaine (de lundi à dimanche ou de dimanche à samedi) sur les différents écrans où s'affichent et se configurent les horaires, aussi bien des applications client que des applications serveur, est établi sur cet écran.

ANNEXE

CONNEXION ENTRE L'INSTALLATION ET LE PC (SERVEUR)

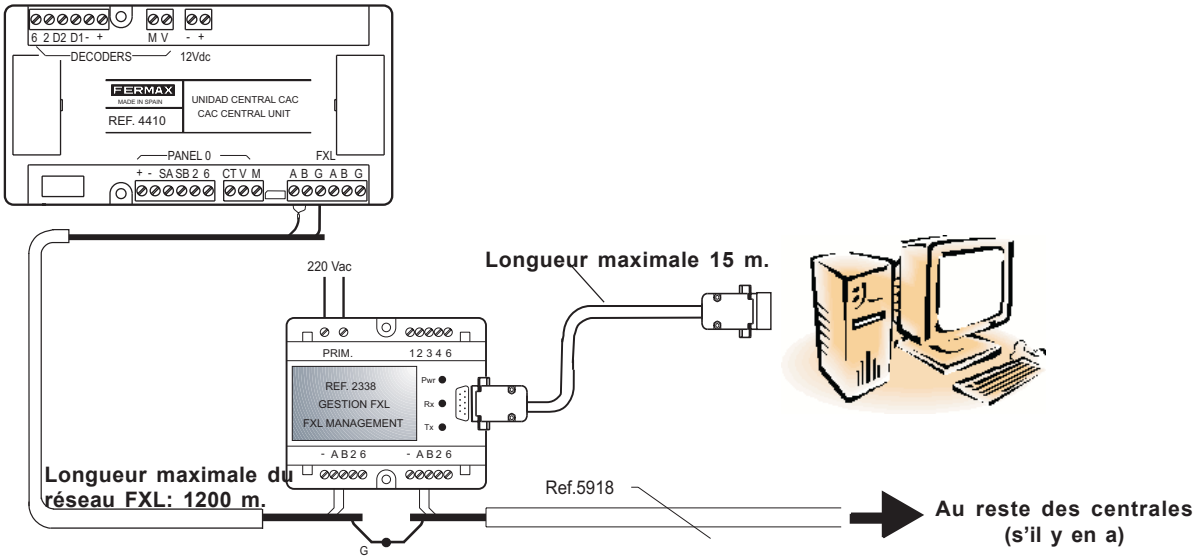
L'installation doit être connectée à l'ordinateur où est installée l'application CAC control Server.



CAC control Server

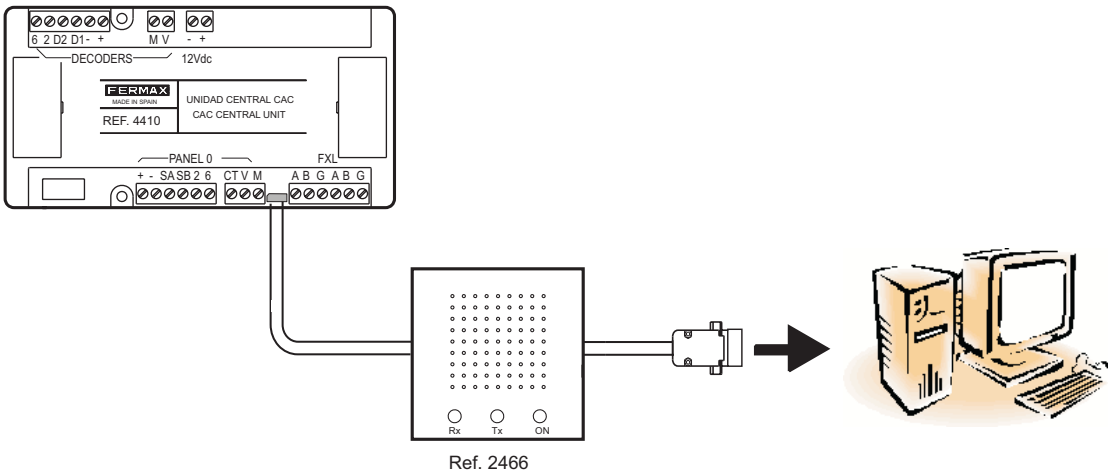
Il faut, pour chaque section, une connexion entre une centrale de la section et le PC.

Connexion par le biais de l'interface 2338 - port RS232 du PC



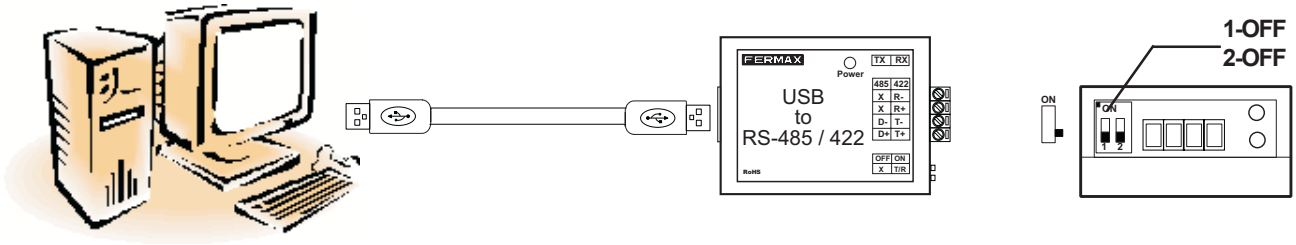
Pour de plus amples informations, consultez le « manuel interface 2338 » code 94098.

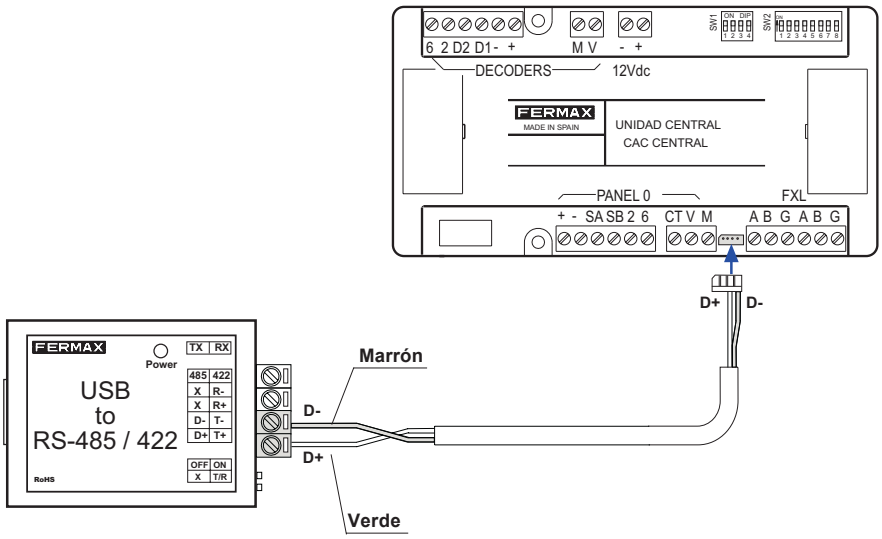
Interface 2446 - Port RS232 PC

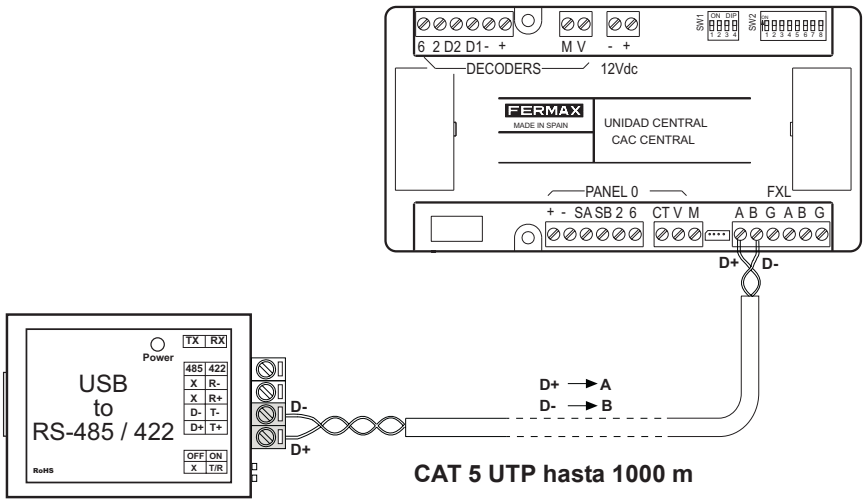


Ref. 2466

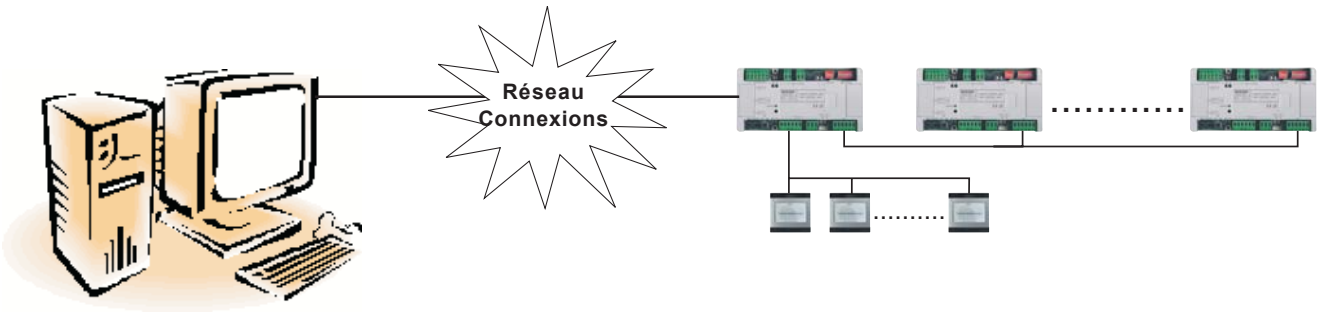
Interface 24461 - Port USB PC







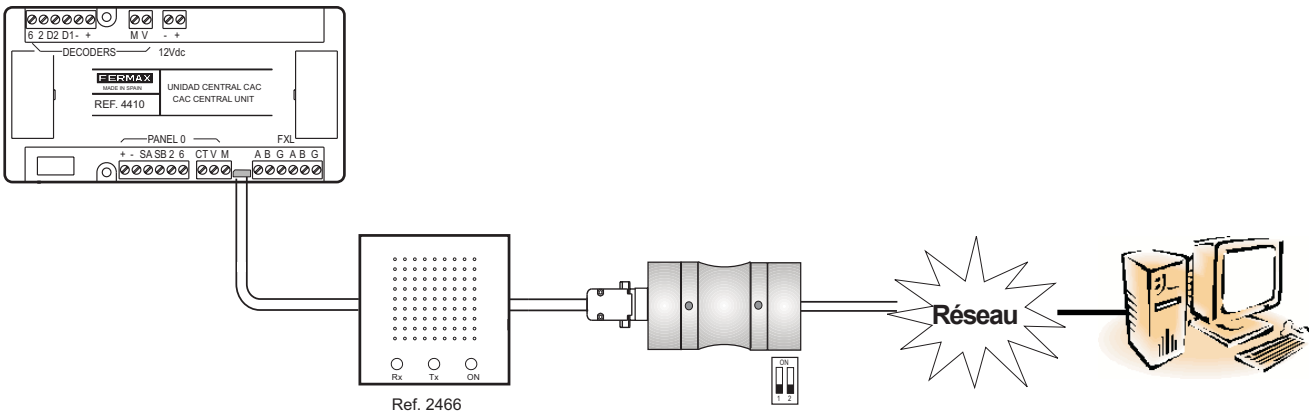
CONNEXION VIA RESEAU LOCAL



Connexion via « Terminal de gestion à distance réf. 1087 »

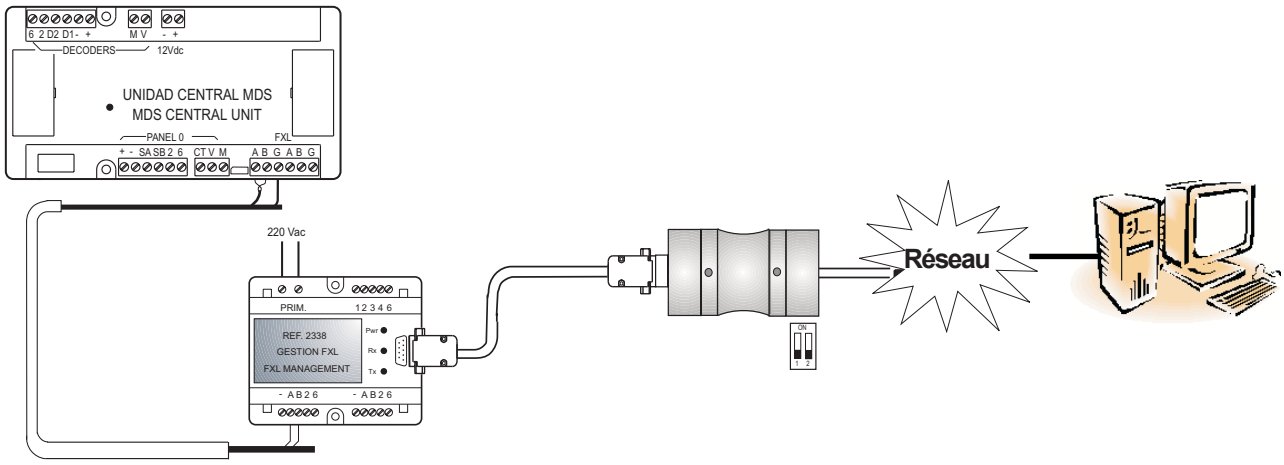
L'interface 1087 permet de connecter, via réseau local ou Internet, l'installation CAC et le PC serveur. Pour de plus amples informations, consultez les informations techniques 94571 relatives au produit.

Connexion via interface réf. 2466 + terminal de gestion à distance réf. 1087



Ref. 2466

Connexion via interface réf. 2338+ terminal de gestion à distance réf. 1087



RÉSOLUTION DES PROBLÈMES DANS DES ENVIRONNEMENTS MULTI-HOMED (il y a plusieurs connexions réseau d'activées)

Pour les environnements où il y a plus d'une connexion réseau de configurée et activée à la fois, il se peut que la connexion entre le logiciel CAC Access et CAC Server ne s'établisse pas correctement.

CAC Server utilise un logiciel basé sur Borland® VisiBroker® 4.5 afin d'annoncer sa disponibilité via « broadcast », mais uniquement sur une interface réseau. Il faut régler, par le biais d'un fichier de configuration, la bonne interface (cette information devra vous être fournie par votre administrateur réseau).

Les étapes à suivre sont les suivantes :

1. Définir la variable de l'environnement **OSAGENT_LOCAL_FILE** avec la valeur de l'emplacement du fichier où sera enregistrée la configuration (par exemple : c:\windows\visibroker.cfg).

2. Configurer le fichier défini précédemment avec les contenu et format suivants.
    1. #IP subnet_mask broadcast_address
    2. 172.20.80.16 255.255.0.0 172.20.255.255

3. L'exemple précédent fait que toutes les connexions entrant dans le CAC Server ou en sortant s'effectuent par le biais de l'interface possédant l'adresse IP 172.30.80.16 (par exemple IP du LAN interne).

Pour en savoir plus :
http://support.borland.com/kbshow.php?q=24886