

SIEMENS



SiPass Entro

Installation

MP6.55 SP1

Copyright

La disponibilité et les spécifications techniques peuvent être modifiées sans préavis.

© Copyright par Siemens AB

Nous nous réservons tous les droits sur ce document et sur l'objet dont il traite. En acceptant le document, l'utilisateur reconnaît ces droits et accepte de ne pas publier le document ni de divulguer le sujet dont il traite en tout ou partie, de ne pas le remettre à une tierce partie quelle qu'elle soit sans notre accord au préalable écrit et de ne pas l'utiliser à d'autres fins que celles pour lesquelles il lui a été fourni.

Edition: 15.10.2013

ID document:

Sommaire

1	A propos de ce document	8
2	Sécurité	9
2.1	Groupe cible	9
3	Description de l'équipement	10
3.1	Description du logiciel	10
3.1.1	Applications logicielles	10
3.1.2	Fenêtres du logiciel	11
3.2	Présentation du système	12
3.3	Capacités et limites du système	13
3.4	Composants du système	14
3.4.1	Kit du lecteur d'enrôlement	18
3.5	Application à petite échelle sans réseau local	18
3.6	Application à grande échelle avec ou sans réseau local	19
3.7	Communication avec le PC	22
3.7.1	Réseau local (LAN)	22
3.7.2	RS232	23
3.7.3	Modem	23
3.8	Connexion de plusieurs PC	24
3.8.1	Base de données multi-utilisateur	24
3.8.2	Microsoft Terminal Server 2008	25
3.9	Communication entre plusieurs SR35i	26
3.9.1	RS485	26
3.9.2	Ethernet via TCP/IP	26
3.9.3	Exemple de connexion des SR35i via RS485	26
3.9.4	Exemple de connexion des SR35i en réseau local	28
3.9.5	Exemple de connexion des SR35i via Internet	29
3.10	Communication sans fil	30
3.11	Réservation	30
3.11.1	Serveur Web intégré	30
3.11.2	Installation du système de réservation	31
3.12	Intégration d'un système CCTV	32
3.13	Intégration d'applications externes (BAPSI)	33
3.13.1	Généralités	33
3.13.2	Champ d'application de BAPSI	33
3.13.3	Applications pratiques	33
3.13.3.1	Exemple d'application - Système de réservation externe	34
4	Configuration minimale requise	35
4.1	Recommandations relatives au câblage	36
4.2	Câbles	37
4.2.1	Câble d'alimentation	37
4.2.2	Câble pour RS485	37
4.2.3	Câble réseau (TCP/IP)	38

4.2.4	Câble de connexion au PC	38
4.2.5	Mise à la terre et blindage pour RS485	38
5	Alimentation électrique.....	39
5.1	Bloc d'alimentation en courant continu (DC) centralisé	39
5.2	Bloc d'alimentation en courant continu (DC) local.....	40
5.3	Chute de tension	41
5.4	Exemple d'une section d'alimentation standard	42
5.5	Blocs d'alimentation en courant continu (DC) multiples dans une même portion de câble	42
6	Installations particulières	43
6.1	Fonctions antipassback utilisant des lecteurs BC-Link	43
6.2	Fonctions antipassback utilisant des lecteurs Clock&Data et Wiegand.....	44
6.3	Zones sous alarme anti-intrusion incluant un DC22	45
6.4	Connexion des informations sur l'état de l'alarme (ASF) dans le DC22	46
7	Guide de prise en main.....	47
8	Connexion des ordinateurs ou d'une imprimante en ligne.....	48
8.1	Connexion du PC par le réseau local (LAN)	48
8.2	Connexion directe par câble (RS232) d'un PC	49
8.3	Connexion d'une imprimante en ligne (RS232).....	49
9	Préparation des ressources réseau	51
9.1	Introduction.....	51
9.2	Agent de sous-réseau (SR35i)	52
9.3	Configuration du routeur.....	52
9.4	DynDNS.....	53
9.4.1	Configuration de DynDNS.org	53
9.5	Pare-feu.....	55
9.6	Exemple avec un routeur	55
9.7	Immeuble d'habitation – exemple.....	56
10	Installation du logiciel.....	57
10.1	Création d'une base de données et d'une connexion	57
10.1.1	Détection automatique des unités.....	59
10.2	Environnement multi-utilisateur (plusieurs PC)	60
11	Installation de systèmes communiquant par modem	61
11.1	Programmation d'un système équipé d'un modem TD36 (conseillé).....	62
11.2	Programmation d'un système équipé d'un modem personnalisé	62
11.3	Programmation sur site d'un système communiquant par modem	62
11.4	Montage et configuration du modem.....	65
11.5	Transfert des informations relatives au nouveau système vers l'ordinateur central.....	66
12	Installation de la carte mémoire flash CF8	67
13	Installation des DVR.....	68
13.1	Conditions préalables requises	68
13.2	Connexion du DVR.....	69
13.3	Contrôle des enregistrements	69
13.4	Paramètres de la caméra	70

13.5	SISTORE™ MX.....	72
13.5.1	Paramètres MX	72
13.5.2	Logiciel de visualisation en temps réel de MX.....	72
13.5.3	Autres points à prendre en compte concernant le MX	72
13.6	SISTORE™ AX	73
13.6.1	Généralités.....	73
13.6.2	AX9 et AX16	73
13.6.3	AX4 et AX Lite.....	73
13.6.4	Paramètres AX.....	73
13.6.5	Autres points à prendre en compte concernant l'AX	74
13.6.6	Logiciel de visualisation en temps réel d'AX.....	75
13.7	SISTORE™ CX	75
13.7.1	Généralités.....	75
13.7.2	Paramètres CX	75
13.7.3	Logiciel de visualisation en temps réel de CX	76
13.7.4	Autres points à prendre en compte concernant le CX.....	76
14	Remarques préliminaires à la configuration du système	77
14.1	Vérification des boucles de communication	77
14.2	Vérification de l'alimentation.....	77
15	Liste de vérification.....	78
16	Démarrage du logiciel.....	79
16.1	Voyants indiquant l'état de la communication	80
17	Définition de l'heure et de la date	82
18	Gestion avancée de l'horloge système	83
19	Personnalisation des paramètres d'Entro	84
19.1	Paramètres de lecteurs de carte	84
19.2	Code personnel sans carte	84
19.3	Modification de la fonction du voyant rouge sur les lecteurs	85
19.4	Code d'agression.....	85
20	Programmation de noms pour les concentrateurs de segments	86
20.1	Création de plusieurs SR35i pour la communication TCP/IP	86
20.2	Création de plusieurs SR35i pour la communication combinée TCP/IP et RS485/87	86
20.3	Création de plusieurs SR35i pour la communication via RS485 uniquement ...	88
21	Programmation des concentrateurs SR35i	89
21.1	Définition des paramètres réseau du SR35i	90
21.2	Personnalisation de la base de données pour DHCP	91
21.3	Préparation du composant SR35i pour DHCP	92
22	Programmation de noms et de fonctions pour les portes	93
23	Programmation du contrôleur de relais IOR6	95
23.1	Sortie de verrou de porte.....	95
23.2	Sortie de relais totalisateur.....	95
23.3	Programmation d'IOR6 pour la gestion horaire.....	96
23.4	Entrée d'avertissement en cas de panne de courant.....	96
23.5	Entrée d'ouverture d'urgence	96

23.6	Entrée du bouton de sortie (EXIT).....	97
23.7	Programmation d'IOR6 pour le système de réservation	97
23.8	Gestion d'ascenseurs à l'aide de l'IOR6.....	98
24	Programmation de zones sous alarme anti-intrusion	100
24.1	Définition de niveaux de sécurité pour le contrôle de l'alarme	102
25	Programmation d'autres types de zones	103
25.1	Antipassback/Contrôle de présence.....	103
25.2	Limitation de l'accès	104
25.3	Zone de verrouillage.....	104
25.3.1	Exemple de verrouillage	105
26	Programmation en vue de la réservation.....	107
26.1	Programmation de zones pour les objets de réservation.....	107
26.2	Distribution aléatoire ou NON aléatoire d'objets de réservation similaires	108
26.3	Contrôle de l'alarme dans un objet de réservation.....	108
26.4	Plannings.....	109
26.5	Objet de réservation	109
26.6	Définition des jours fériés et des congés annuels dans le système de réservation.....	111
26.7	Définition des droits des groupes d'accès.....	111
26.8	Définition des droits de réservation des personnes	112
26.9	Réservation flexible à l'intérieur d'un intervalle	113
26.10	Affichage des informations de réservation	113
26.11	Entretien	113
26.12	Configuration de la fonction de débit.....	114
26.13	Configuration des messages de confirmation par courrier électronique.....	114
26.13.1	Configuration requise par la fonction de confirmation	114
26.13.2	Modification des textes de confirmation.....	115
26.13.3	Exemple de confirmation	117
26.13.3.1	Champs de courrier électronique dans les messages de confirmation.....	117
26.13.3.2	Champs spéciaux de courrier électronique	118
27	Maintenance.....	119
27.1	Développement et modification du système	119
27.2	RS485.....	119
27.3	Gestion réseau	119
27.4	Mise à jour du logiciel d'un système existant	119
27.5	Installation d'un PC supplémentaire ou de remplacement.....	121
27.5.1	Préparation de la base de données pour le PC existant	121
27.5.2	Configuration d'un PC supplémentaire ou de remplacement	122
27.6	Installation d'un SR35i supplémentaire ou de remplacement.....	122
27.7	Installation de lecteurs supplémentaires	123
27.8	Contrôle de version du microprogramme SR35i	124
27.9	Enregistrement/restauration de la base de données sur CF8	124
27.10	Contrôle du microprogramme du central de porte	125
27.11	Imprimé de la configuration du système.....	125
27.12	Migration d'un système Entro Lite	125
27.13	Désinstallation d'Entro.....	125

28	Questions fréquentes	127
28.1	Informations détaillées sur les réseaux locaux (LAN)	127
28.2	Quel est le niveau de redondance du système ?	129
29	Récapitulatif des informations importantes	131
Index	132

1 A propos de ce document

Ce document contient des informations sur l'installation du produit.

Vous pouvez également consulter les documents suivants :

- Le Manuel de conception de projet SiPass Entro fournit une description des concepts importants.
- Le Manuel de l'utilisateur SiPass Entro fournit une description du fonctionnement du logiciel.

Pour en savoir plus sur l'installation des différents composants matériels, reportez-vous à leur documentation respective.

Remarque s'adressant aux utilisateurs des versions antérieures de la documentation de SiPass Entro : les informations concernant la configuration du logiciel sont désormais incluses dans le présent Manuel de l'installateur (et non plus dans le Manuel de l'utilisateur).

2 Sécurité

2.1 Groupe cible

Lecteurs ciblés	Compétence	Activité	Condition du produit
Installateur	Formation technique pour installations électriques.	Installe le produit, les composants individuels du produit ou des pièces de remplacement.	Les composants du produit ne sont pas encore installés ou doivent être remplacés ou modifiés.
Personnel d'exécution de mise en marche	Formation technique pour installations électriques. Formation produit recommandée.	Configure le produit pour une première utilisation ou modifie la configuration existante.	Le produit est installé mais pas encore configuré ou la configuration existante doit être modifiée.
Personnel d'entretien	Formation technique pour installations électriques.	Vérifie régulièrement le produit pour garantir son fonctionnement correct et effectue des opérations d'entretien.	Le produit est déjà utilisé et nécessite une opération d'entretien.

3 Description de l'équipement

3.1 Description du logiciel

3.1.1 Applications logicielles

Le logiciel SiPass Entro se divise en trois applications :

Programme d'installation

Cette application est utilisée pour la programmation des composants matériels. Elle permet de procéder à l'installation du PC, des concentrateurs, des connecteurs de porte et des zones sous alarmes.

Entro

Cette application est utilisée pour la configuration et la gestion des groupes d'accès et des personnes (détenteurs de carte). Elle peut être considérée comme le composant principal du logiciel, car elle est utilisée au quotidien.

Les fonctions suivantes sont intégrées à l'application Entro :

- **Contrôle d'accès**
Permet d'ajouter des détenteurs de carte, de sélectionner et configurer des gardiens, et de définir les groupes d'accès, plannings et zones (zones antipassback, zones de contrôle de présence et zones à entrée restreinte).
- **Impression de cartes (de badges)**
Permet de concevoir et d'imprimer des cartes conformément aux normes standard.
- **Intégration de systèmes de vidéosurveillance CCTV (systèmes de télévision en circuit fermé)**
Il est possible d'utiliser SiPass Entro conjointement avec un système CCTV de Siemens. SiPass Entro permet d'établir une connexion directe pour l'installation et la gestion du système CCTV (des DVR et caméras, par exemple).
- **Système de détection d'intrusion**
Outre le contrôle d'accès, SiPass Entro permet également de contrôler un système de détection d'intrusion externe à l'aide d'une carte d'accès.
- **Fonction de réservation**
L'administrateur système définit les objets (tels que des lecteurs de carte ou des portes) qu'il est possible de réserver et décide des plannings de réservation appropriés.
L'utilisateur souhaitant réserver une plage horaire peut se servir d'un navigateur Web standard (tel qu'Internet Explorer). Il peut également passer sa carte dans un terminal de réservation (InfoPoint IP812). Le mode de réservation dépend de la configuration du système.
- **Impressions**

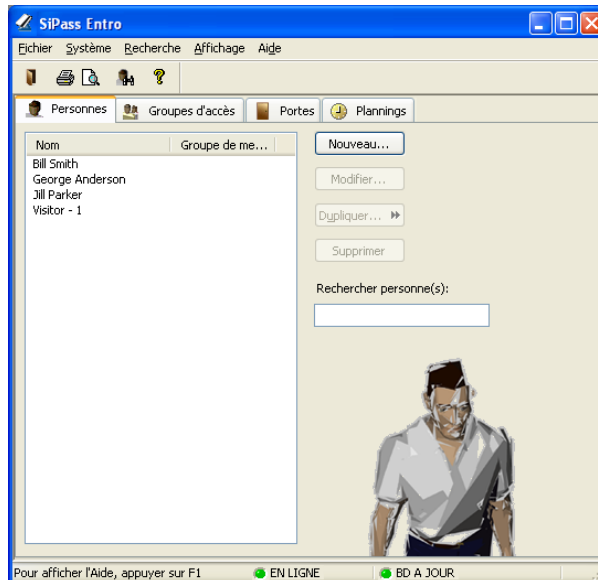
Contrôle de l'accès aux portes

Cette application est utilisée pour afficher le journal d'événements, l'état des portes et les séquences vidéo. Elle permet également de déverrouiller les portes via le PC.

3.1.2 Fenêtres du logiciel

Fenêtre de démarrage d'Entro

Lorsque vous ouvrez l'application Entro, la fenêtre suivante apparaît (affichant la liste des personnes) :



Fenêtre de démarrage d'Entro

Raccourcis

Vous trouverez dans le logiciel deux raccourcis destinés à faciliter la création, la modification ou la suppression d'informations. Ces raccourcis sont affichés, par exemple, dans les propriétés du groupe d'accès et dans les propriétés de la personne.



Raccourci Plannings



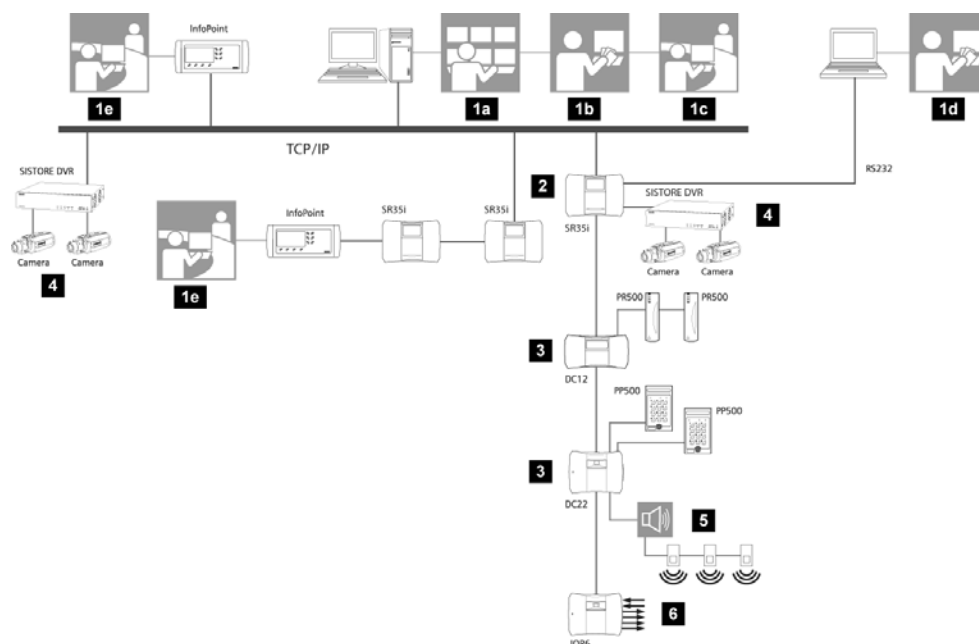
Raccourci Groupes d'accès

Ainsi, vous pouvez cliquer sur le raccourci **Groupes d'accès** lorsque vous créez une nouvelle personne pour laquelle vous ne disposez pas encore d'un groupe d'accès approprié. De la même manière, vous pouvez utiliser le raccourci **Plannings** afin de créer ou de modifier un planning. Vous êtes ramené à votre point de départ lorsque vous avez fini d'utiliser un raccourci.

3.2 Présentation du système

Le système suivant est étendu sur trois niveaux :

- Sur le PC, le logiciel permet d'envoyer et de recevoir des informations vers/depuis le système via un réseau ou une connexion par câble. Le terminal InfoPoint IP812 est utilisé pour assurer des fonctions de réservation.
- Les concentrateurs SR35i permettent de stocker des informations et de prendre des décisions relatives à l'accès aux portes.
- Les environnements de portes hébergent des installations de centraux de porte, lecteurs et claviers, assortis de dispositifs de verrouillage électriques.



Différents niveaux du système.

1a	PC – Contrôle de la sécurité
1b	PC – Administration du système
1c	PC – Gestion des visiteurs
1d	Ordinateur local – Administration du système
1e	Gestion des réservations
2	Concentrateurs
3	Portes
4	Connexion au système de vidéosurveillance (TCP/IP)
5	Système de détection d'intrusion (sortie du relais)
6	Entrées et sorties de contrôle

3.3 Capacités et limites du système

Logiciel SiPass Entro

Logiciel pouvant contrôler jusqu'à 10 000 systèmes, chacun d'eux capable de gérer :

- 512 portes répondant à un système de communication câblé + 512 sans fil (RF) contrôlées par un maximum de 16 concentrateurs.
- 40 000 cartes
- 240 plannings
- 480 groupes d'accès
- 240 zones (zones sous alarme, antipassback, de contrôle de présence, de verrouillage et à entrée restreinte)
- 16 plannings d'activation d'alarme
- 16 utilisateurs système de 4 niveaux + niveau d'installation
- 14 jours fériés, 7 demi-journées et 4 périodes de congés annuels par planning
- Le concentrateur de segments SR35i absorbe 10 000 événements dans sa mémoire tampon.

Fonctions de réservation

- 64 objets de réservation (groupes d'appareils)
- 30 portes et/ou relais IOR6 au maximum dans chaque objet de réservation
- 32 plannings comportant chacun 24 intervalles
- Réservation flexible des intervalles
- 6 100 réservations au maximum

Intégration de systèmes de vidéosurveillance (CCTV)

- 16 DVR au maximum - un DVR par SR35i/SR34i
- 128 caméras au maximum

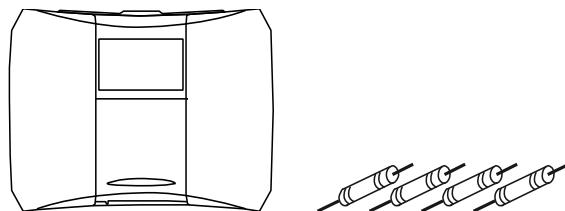
Impression de cartes

- Conception de modèles de cartes et/ou reçus multiples
- Impression en série de cartes

3.4 Composants du système

La gamme des composants de SiPass Entro inclut différents produits.

- **Concentrateurs de segments SR35i.** Vous pouvez relier jusqu'à 16 concentrateurs de segments au PC sous la forme d'une boucle. Chaque concentrateur de segments peut contrôler 4 portes raccordées par câble + 4 sans fil, 8 + 8, 16 + 16 ou 32 + 32. Les informations que vous programmez dans l'ordinateur sont enregistrées sur tous les concentrateurs de segments. Cela permet non seulement d'utiliser l'ordinateur à d'autres fins, mais encore de l'éteindre lorsque vous ne programmez ni ne contrôlez SiPass Entro.



Chaque concentrateur de segments est fourni avec 4 résistances de terminaison (120 Ω).

Le concentrateur de segments dispose de quatre niveaux de capacités différents, dont dépend le nombre de portes qu'il est en mesure de gérer :

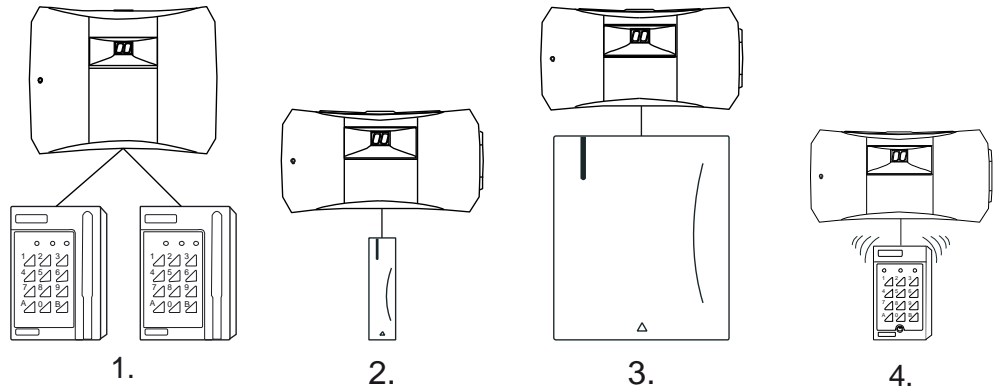
SR35i/4	Contrôle au maximum quatre portes raccordées par câble + quatre sans fil
SR35i/8	Contrôle au maximum huit portes raccordées par câble + huit sans fil
SR35i/16	Contrôle au maximum 16 portes raccordées par câble + 16 sans fil
SR35i/32	Contrôle au maximum 32 portes raccordées par câble + 32 sans fil

Il est possible de mettre à jour progressivement la capacité d'un concentrateur de segments, ce qui facilite les possibilités d'extension future.

La communication avec le SR35i s'effectue sur deux niveaux (bus global et local). Ceci offre différents choix de configuration dans SiPass Entro. Par exemple, une propriété étendue sur plusieurs étages pourra inclure un SR35i à chaque étage, les concentrateurs de segments étant chacun capable de gérer un certain nombre de portes.

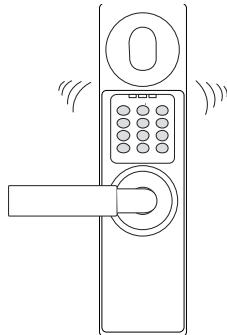
Le concentrateur de segments SR35i le plus important est celui contenant toutes les données du site. Il comporte notamment les nom d'utilisateur et mot de passe du progiciel installé sur le PC.

- **Centraux de porte avec lecteurs de carte à distance.** Un central de porte se connecte à un concentrateur de segments. Il pilote une porte équipée d'un ou de deux lecteurs de carte à distance (entrée/sortie). Ce système est conçu pour les portes extérieures ou celles nécessitant une sécurité et des fonctionnalités accrues (dérivation d'alarme, contrôle de l'accès aux portes, etc.).

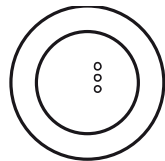


1.	DC22 équipé d'une carte magnétique ou de lecteurs de proximité.
2.	DC12 équipé d'un lecteur de proximité.
3.	DC12 équipé d'un lecteur mains libres.
4.	DC12 équipé d'un lecteur de proximité (PP500) à pavé numérique.

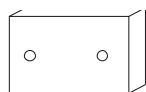
- **Liaison radio RF Codoor RF30-EM.** La communication s'effectue sans fil, directement avec les concentrateurs de segments ou via des routeurs RF9.



- **RF9.** Routeur sans fil utilisé pour amplifier et router le signal RF.

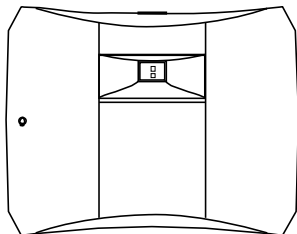


- **Centraux de porte sans terminaux distants.** Dans certains cas, il s'avère nécessaire de contrôler l'accès aux portes ou d'ouvrir une porte en fonction du planning. Le central DC01 peut servir de relais - minuterie ou d'unité de contrôle.



Central de porte DC01

- **Contrôleur de relais.** Vous pouvez utiliser une unité IOR6 pour piloter, par exemple, un ascenseur. Les relais à activer peuvent être contrôlés par tout lecteur. Les unités IOR6 peuvent être utilisées dans des applications de réservation. A partir de la version 5, vous disposez également de fonctions telles que le relais totalisateur d'alarme commune, la gestion d'ascenseurs, l'ouverture d'urgence et le contrôle des pannes de courant.



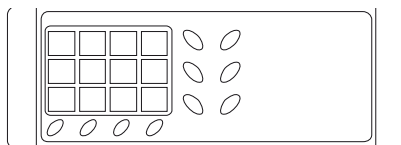
Contrôleur de relais IOR6

- **CF8.** Si vous devez utiliser l'option de réservation, assurez-vous au préalable qu'une carte mémoire CF8 est installée dans l'un des concentrateurs de segments SR35i.



Carte mémoire CF8

- **Terminal de réservation.** Il est possible d'utiliser un point d'information InfoPoint IP812 au sein d'un système de réservation en vue d'effectuer une réservation à proximité de l'objet. Ce terminal comprend une fonction de lecteur de carte intégrée à des fins d'identification.

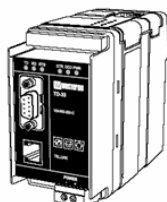


InfoPoint IP812

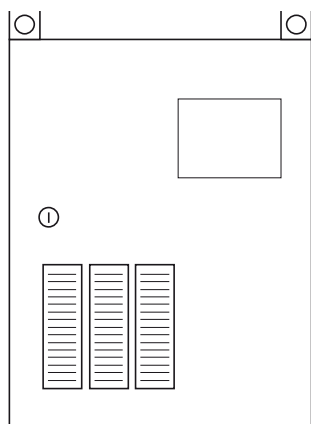
- **Cartes d'accès.** Chaque personne peut utiliser au choix une carte ou un badge de proximité.



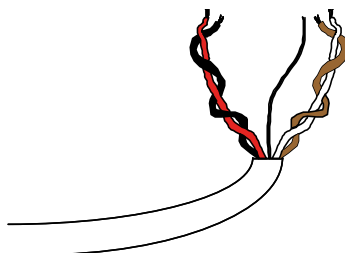
- **Modem.** Si votre site est équipé de plusieurs systèmes SiPass Entro, vous pouvez raccorder un modem afin d'assurer la communication entre les systèmes et l'ordinateur central.



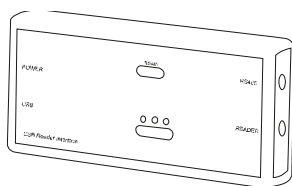
- **Batterie de secours.** Une ou plusieurs batteries de secours sont recommandées pour assurer l'alimentation du système.



- Câbles.

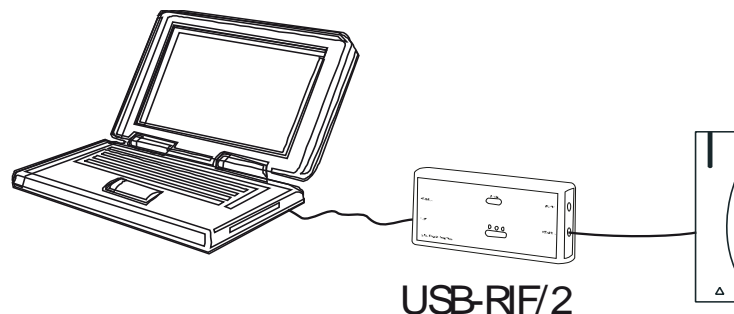


- **USB-RIF/2** – Interface de lecteur utilisée pour les fonctions d'enrôlement et d'ouverture de session.



Convertisseur d'interface USB vers Lecteur

3.4.1 Kit du lecteur d'enrôlement



Connexion USB-RIF/2 au PC

Dans SiPass Entro, il est possible de connecter directement à un PC un lecteur d'enrôlement par le biais de l'interface du lecteur USB-RIF/2. Ce lecteur permet d'effectuer les opérations suivantes :

- Connexion de cartes
- Connexion au logiciel du système à l'aide de la carte
- Recherche accélérée des détenteurs de carte

USB-RIF/2 se connecte à un port USB du PC. Il est accompagné d'un pilote logiciel (agent USB) installé lors du chargement du logiciel SiPass Entro au démarrage de l'ordinateur.

Des kits sont également livrés avec le lecteur de proximité PR500 (technologie Cotag ou EM4102), accompagnés d'un support de bureau et d'un lecteur USB-RIF/2.

3.5 Application à petite échelle sans réseau local

SiPass Entro peut être utilisé dans des applications à petite échelle comportant un nombre réduit de portes.

Dans ce cas, la configuration du système revient souvent à établir un planning correct et à effectuer un câblage dédié. La prévision d'un réseau local, d'adresses IP, etc., ne s'avère pas nécessaire.

Tout ce dont vous aurez besoin : quelques mètres de câble, un concentrateur de segments SR35i, un bloc d'alimentation électrique et des lecteurs. Un véritable jeu d'enfants !

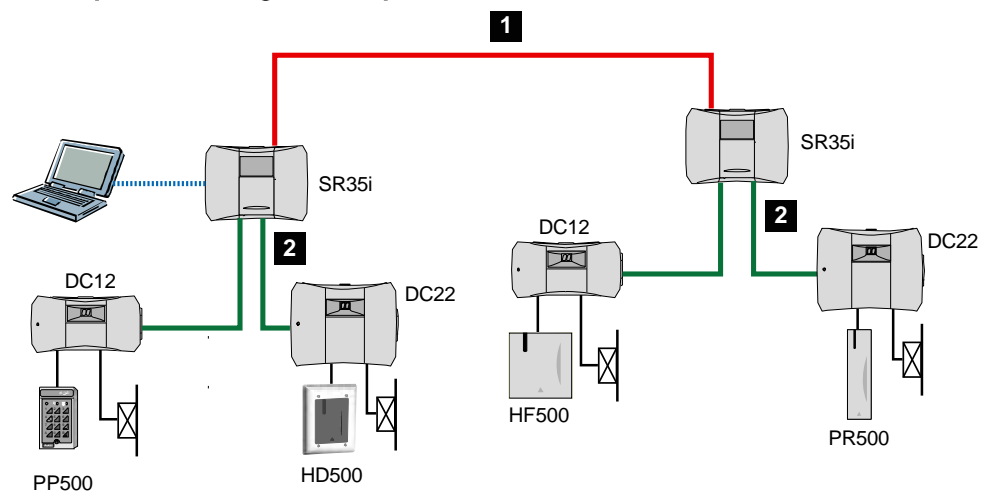
3.6 Application à grande échelle avec ou sans réseau local

SiPass Entro est capable de gérer jusqu'à 512 portes et 40 000 personnes dans un même système (base de données).

En outre, un seul PC peut gérer jusqu'à 10 000 systèmes similaires – via un modem et/ou un réseau local. Ces systèmes se composent de bases de données uniques et distinctes, qui peuvent être contrôlées et stockées à partir du même PC. Le système de contrôle d'accès doit couvrir une ou plusieurs propriétés situées dans des locaux différents.

Si un local comporte plusieurs portes, vous pouvez toujours recourir à un câblage dédié. Le système se divise en différentes sections gérées chacune par un concentrateur de segments SR35i propre, celui-ci étant en mesure de contrôler un certain nombre de portes (bus local). Tous les sous-systèmes sont ensuite reliés en un niveau de communication supérieur (bus global).

Exemple de configuration par câble RS485



Exemple de configuration par câble RS485

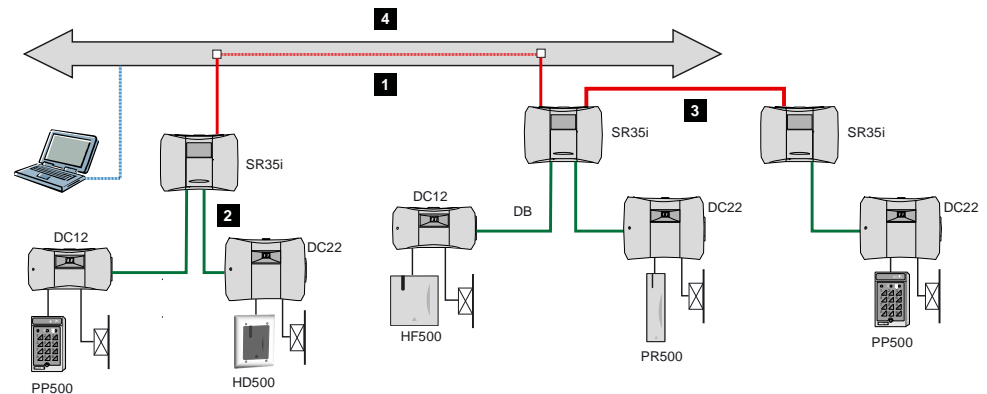
1.	Bus local RS485
2.	Bus global RS485

Communication globale utilisant à la fois TCP/IP et RS485

Lorsque plusieurs propriétés coexistent dans un même système, vous pouvez envisager d'utiliser un réseau local. Notez toutefois que vous ne pouvez pas inclure plus de 512 portes et 16 concentrateurs de segments.

Dans ce cas, le bus global sera connecté via un réseau local (TCP/IP), tandis que les portes seront contrôlées localement par les concentrateurs SR35i associés.

Il est également possible de combiner ces deux méthodes de communication. En effet, un seul des SR35i du bâtiment est connecté par le biais du réseau local, les autres concentrateurs de segments étant raccordés à l'aide d'un câble traditionnel.

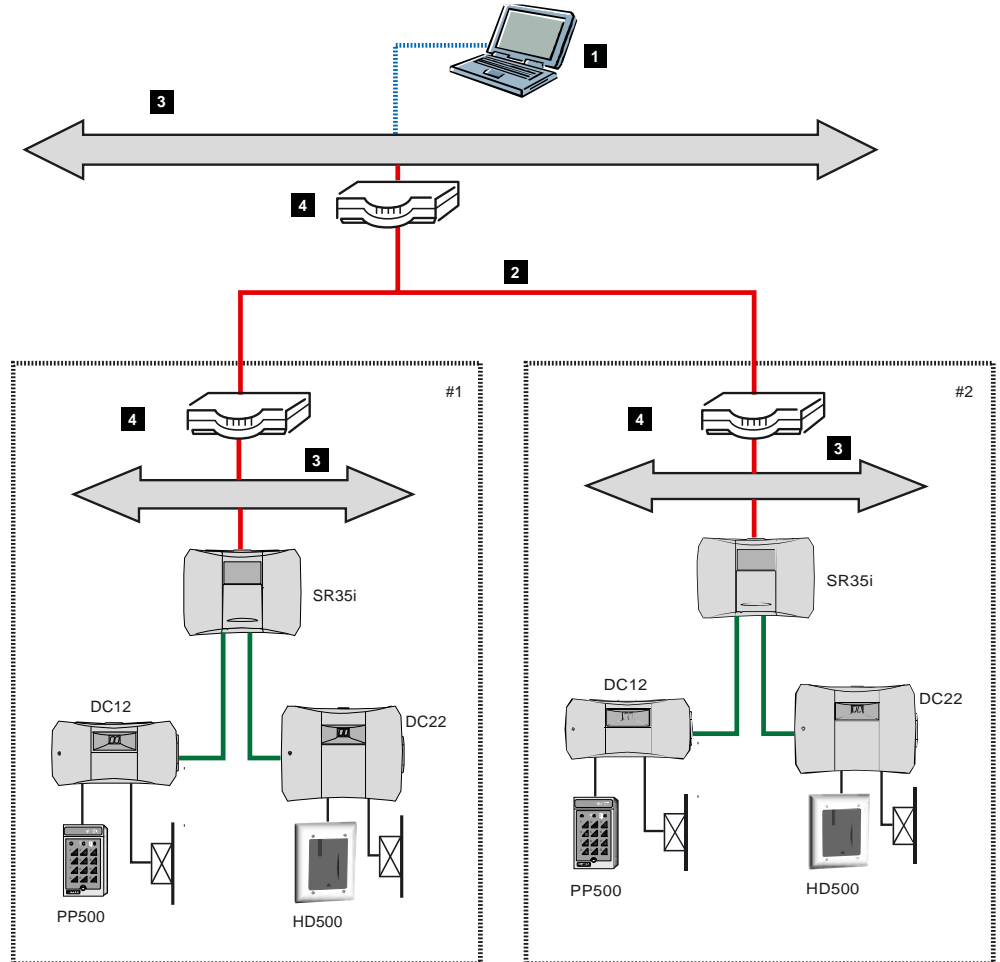


Communication globale utilisant à la fois TCP/IP et RS485.

1.	Communication globale
2.	Bus local RS485
3.	Bus global RS485
4.	Réseau local LAN (TCP/IP) au sein d'un même bâtiment

Deux systèmes dotés de bases de données différentes

Il arrive parfois qu'un seul ordinateur central doive gérer des systèmes uniques situés dans des locaux différents. Cette configuration peut être obtenue via un modem ou un réseau local. Voir l'illustration suivante, représentant un PC connecté par réseau à deux systèmes SiPass Entro différents.



PC connecté par réseau à deux systèmes différents

1.	PC connecté à deux bases de données différentes à l'aide d'informations de connexion distinctes
2.	Réseau global ou Internet (TCP/IP crypté)
3.	Réseau local (LAN)
4.	Passerelle

3.7 Communication avec le PC

SiPass Entro SR35i propose trois méthodes de communication avec le **PC**.

Par défaut, l'installation logicielle suppose qu'un seul ordinateur sera connecté au système. Si plusieurs ordinateurs (utilisateurs) doivent ouvrir des sessions simultanées, vous devez configurer des connexions supplémentaires.

3.7.1 Réseau local (LAN)

Dans cette configuration, les communications TCP/IP avec le PC s'effectuent via le réseau local (Ethernet 10/100 Mbit/s).

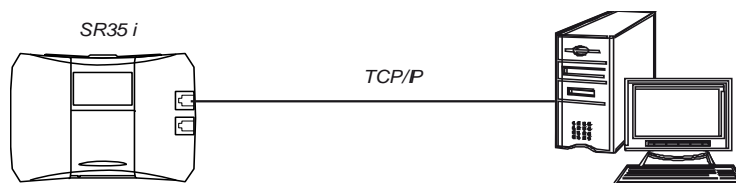


Il est primordial que le responsable du parc informatique de l'utilisateur final ait participé à cette partie de l'installation et en ait approuvé chaque aspect.

Les SR35i sont équipés de **commutateurs réseau intégrés munis de deux connecteurs (RJ45)** qui permettent de relier le PC au SR35i pour former un réseau local, sans nécessiter de matériel supplémentaire (à l'exception d'un câble).

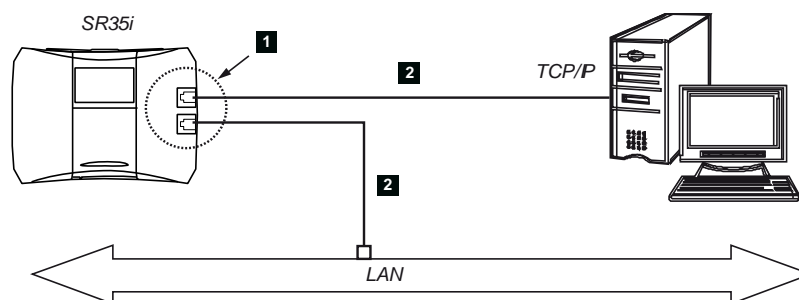
Connexion directe sans réseau local (LAN)

Dans cet exemple, l'ordinateur possède une adresse IP statique et est connecté directement au SR35i, au lieu du RS232 requérant une distance plus élevée (< 100 m).



Connexion directe avec réseau local (LAN)

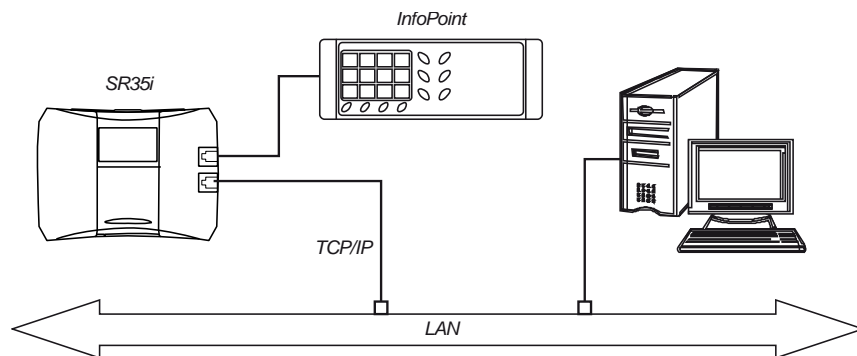
Dans cet exemple, le commutateur réseau intégré est également utilisé pour connecter l'ordinateur au réseau local.



- | | |
|----|-----------------------------|
| 1. | Commutateur réseau intégré. |
| 2. | Câbles de type RJ45. |

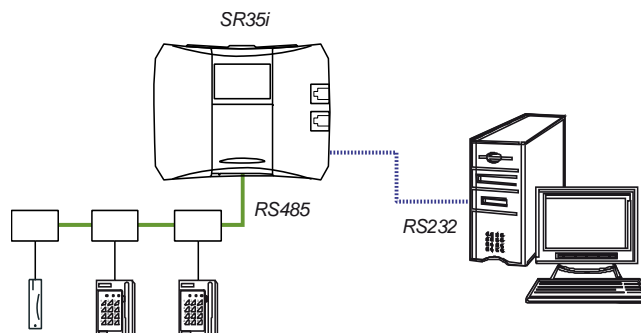
Réseau local avec point d'information InfoPoint IP812

Le point d'information peut être connecté directement au concentrateur de segments SR35i.



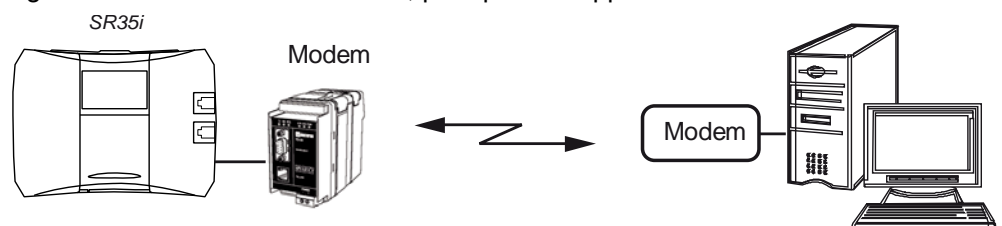
3.7.2 RS232

Le SR35i communique directement avec le PC via un câble connecté au port COM de l'ordinateur.



3.7.3 Modem

Le PC est utilisé pour contrôler un site distant via un modem. Le SR35i est également connecté à un modem, pour pouvoir appeler le PC si nécessaire.



3.8 Connexion de plusieurs PC

3.8.1 Base de données multi-utilisateur

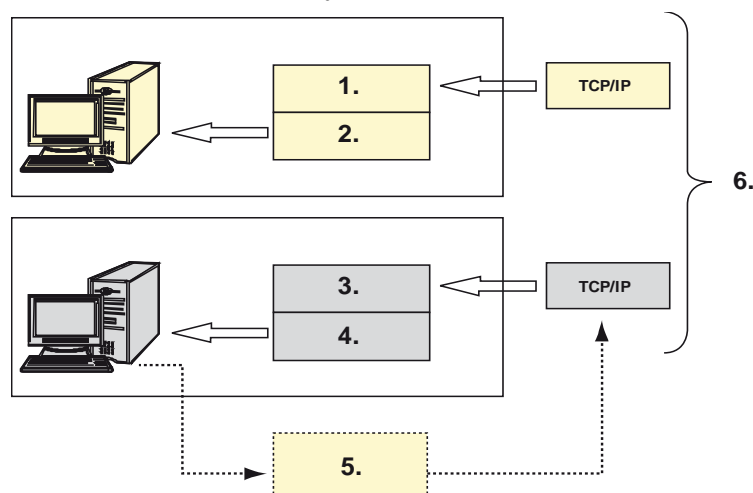
Chaque système SiPass Entro utilise une **base de données** (répertoriant cartes, plannings, etc.) stockée sur chaque concentrateur de segments et sur chaque PC. La base de données SiPass Entro autorise **plusieurs utilisateurs** à utiliser une même base de données.

Pour que cela soit possible, le système doit impérativement savoir quel utilisateur se sert de quel ordinateur. Par exemple, un gestionnaire de sécurité peut posséder son propre PC (doté d'une licence dédiée) tandis qu'une réceptionniste travaille sur un autre PC (assorti d'une autre licence). A chaque PC correspond une "connexion" dans SiPass Entro, pour laquelle le numéro de licence et les ports de communication sont définis.

Dans le même temps, les événements sont filtrés pour être envoyés uniquement vers le PC approprié. Par exemple, si le gestionnaire de sécurité ouvre temporairement une session sur l'ordinateur de la réceptionniste, aucun événement ne sera envoyé vers ce PC.

Pour chaque utilisateur du système que vous créez, vous devez spécifier la connexion associée ainsi que le filtre d'événements à utiliser.

Le fonctionnement de ce système est illustré ci-dessous.



1.	Connexion du gestionnaire
2.	Filtre 1 d'événements
3.	Connexion de la réceptionniste
4.	Filtre 2 d'événements
5.	<i>Exemple</i> : Connexion du gestionnaire. Aucun événement reçu !
6.	Connexions au système SiPass Entro

Si un seul PC est utilisé par plusieurs utilisateurs, les différents événements filtrés seront stockés dans des dossiers distincts sur l'ordinateur (dépendant de l'utilisateur ayant ouvert une session.)

3.8.2 Microsoft Terminal Server 2008

Vous pouvez vous procurer le logiciel SiPass Entro sous la forme d'un progiciel Microsoft Terminal Server 2008 qui vous permet d'installer SiPass Entro comme application client-serveur. Notez que MS Terminal Server 2003 est également pris en charge.

Cela signifie que le logiciel SiPass Entro est installé sur un ordinateur central utilisé comme serveur. L'application Terminal Server permettra ensuite à l'ordinateur client de se connecter aux programmes SiPass Entro.

Vous avez la possibilité de connecter plusieurs clients simultanément ; SiPass Entro se charge de gérer la base de données. Un **numéro de licence est requis pour chaque client**. Tous les événements et informations sont stockés de manière centrale sur le serveur ; aucune information n'est conservée localement.

Pour en savoir plus sur l'installation et la configuration du logiciel SiPass Entro *Terminal Server 2008*, consultez le document renfermant les notes d'installation du programme fourni avec le progiciel SiPass Entro.

3.9 Communication entre plusieurs SR35i

La communication entre plusieurs **concentrateurs** peut s'effectuer par l'intermédiaire de deux types de câbles distincts : **RS485 paire torsadée** et/ou **Ethernet 10/100 Mbit/s**.

3.9.1 RS485

Cette méthode utilise le câble RS485 pour relier un maximum de 16 concentrateurs SR35i, séparés d'une distance maximale de 1 200 mètres (entre le premier et le dernier SR35i).

Il est possible de configurer un ou plusieurs SR35i pour l'utilisation de TCP/IP en suivant la procédure indiquée ci-après. Les concentrateurs sont alors dotés d'une adresse IP et d'une fonction proxy (avec SNTP).

3.9.2 Ethernet via TCP/IP

Généralement connue sous le nom de TCP/IP, cette méthode utilise le câble Ethernet (10/100 Mbit/s) pour se connecter au réseau local. Le protocole TCP offre un meilleur contrôle au niveau de l'adressage des messages à travers le réseau. La distance maximale dépend de la structure du réseau proprement dit.

Si vous optez pour cette méthode, assurez-vous que les SR35i disposent d'une **adresse IP** unique ainsi que d'une fonction **proxy** (avec SNTP). Ceci permet de garantir que seules les unités visées (SR35i ou PC) ne reçoivent les messages.

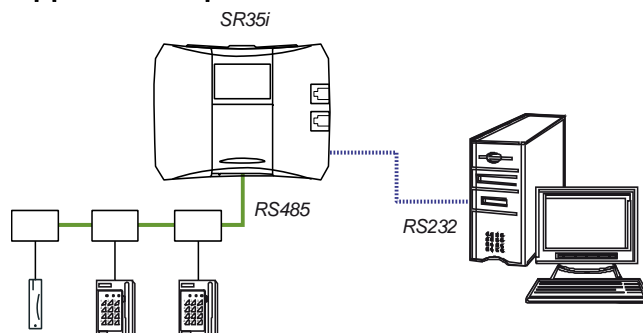
Remarque relative à l'utilisation des SR35i et de TCP

Lorsque plusieurs SR35i communiquent via TCP/IP, il est préférable de réunir les zones dans un même sous-réseau afin de garantir leur fonctionnement (de zones sous alarme, par exemple).

3.9.3 Exemple de connexion des SR35i via RS485

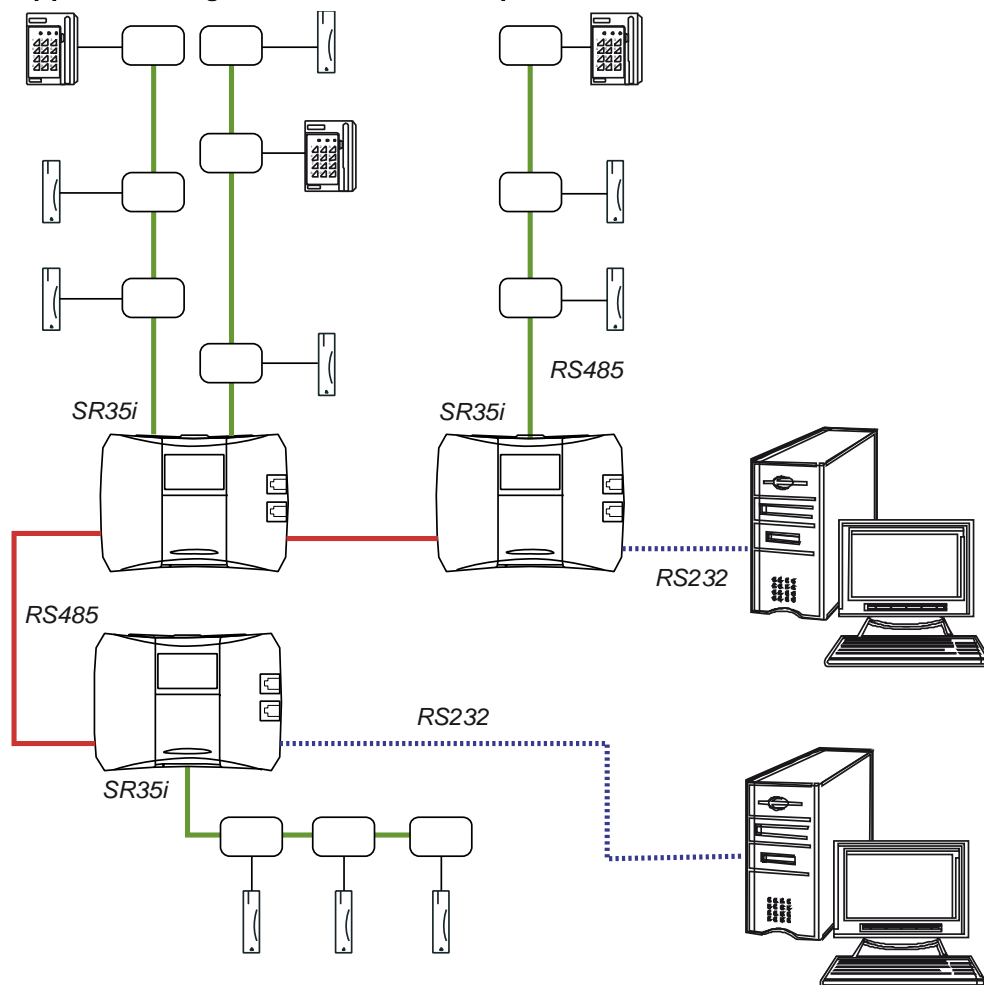
Cette solution fournit un système plus fermé dans lequel les différents concentrateurs de segments sont reliés à l'aide de câbles dédiés (RS485).

Application à petite échelle avec un seul SR35i



Application à petite échelle avec un seul SR35i

Application à grande échelle avec plusieurs SR35i

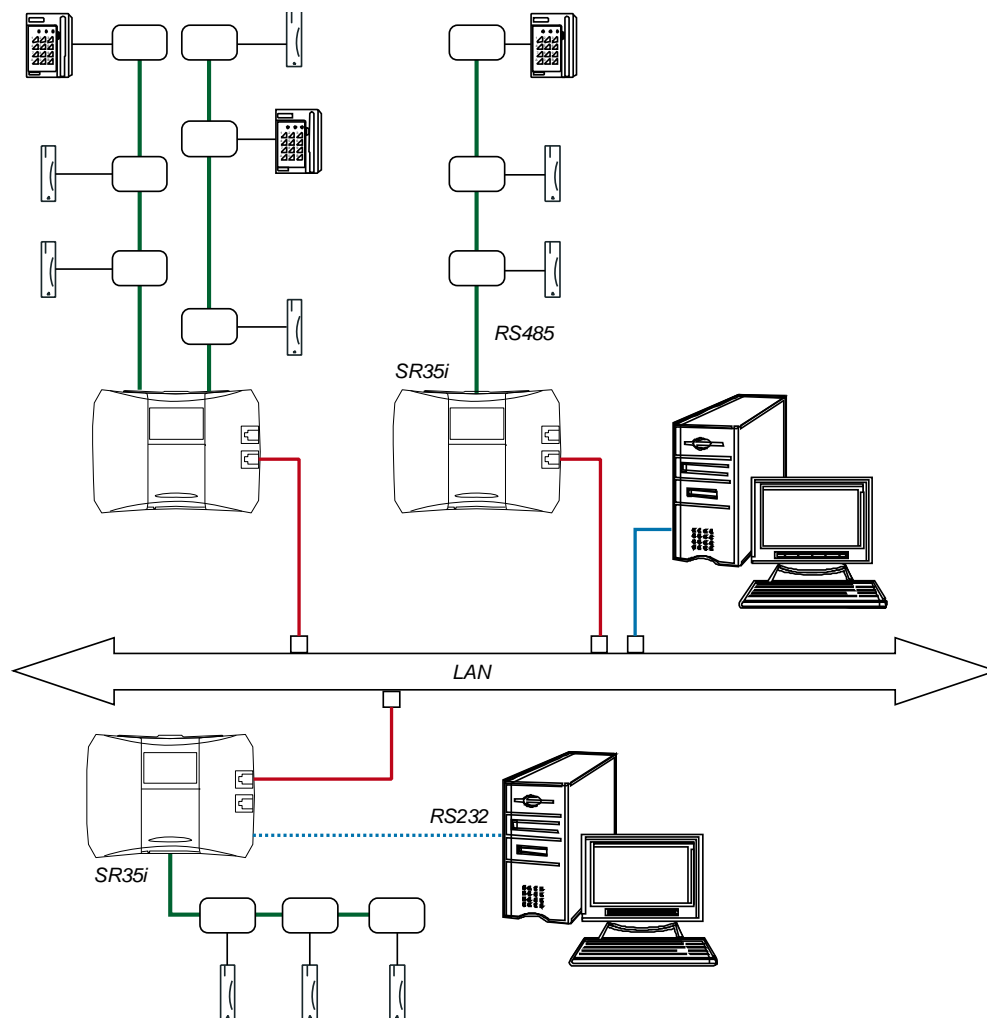


Plusieurs SR35i dans un réseau câblé

3.9.4 Exemple de connexion des SR35i en réseau local

Cette version de SiPass Entro autorise plusieurs SR35i à communiquer à travers des réseaux locaux. Il est possible de contrôler l'ensemble du système à partir de tout ordinateur situé sur le réseau, sans qu'il s'avère nécessaire de connecter séparément les différents concentrateurs.

Vous remarquerez que le PC peut être connecté directement (RS232) ou via le réseau.

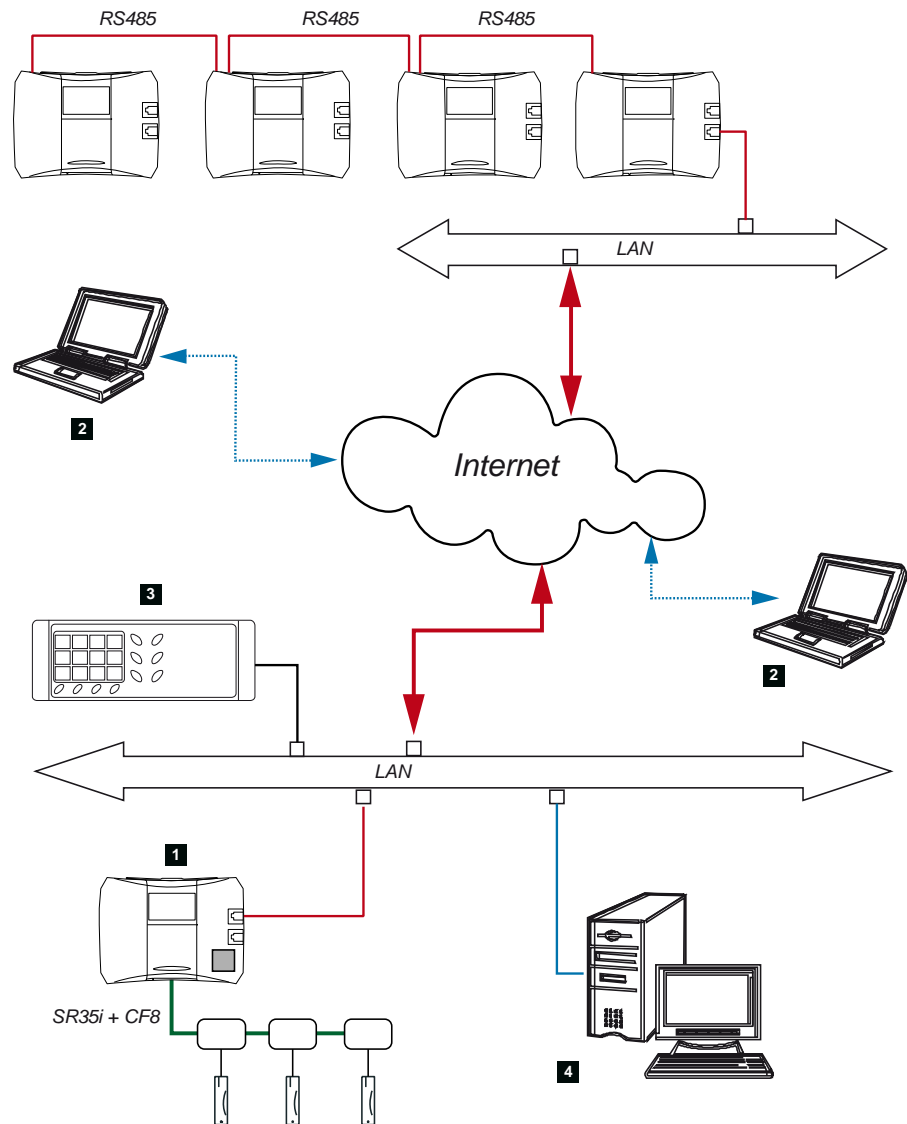


Communication entre plusieurs SR35i via TCP/IP

3.9.5 Exemple de connexion des SR35i via Internet

Cet exemple combine les différentes méthodes de connexion (Internet, réseau local et RS485) pour assurer la communication entre les unités.

Par exemple, certains PC peuvent être utilisés pour établir une connexion à un système de réservation via Internet et d'autres pour procéder à des opérations d'administration de systèmes.



Application Internet

1.	Réservation Serveur Web
2.	Réservation Navigateur Web (MS Internet Explorer)
3.	Réservation InfoPoint IP812
4.	Gestionnaire de sécurité

3.10 Communication sans fil

SiPass Entro permet l'utilisation d'un système de communication sans fil (réseau radio). Celui-ci permet de relier une unité Codoor RF (RF30-EM) alimentée par pile et un concentrateur de segments SR35i.

Un même système peut comporter jusqu'à 512 portes raccordées par câble + 512 sans fil. **Un concentrateur SR35i est capable de gérer à la fois des environnements de portes câblés et sans fil.**



Consultez le document d'informations livré avec l'unité RF30-EM pour connaître ces dernières (par exemple, les styles de systèmes de verrouillage requis en Scandinavie).

Le manuel *Wireless Installation* fournit les informations relatives à l'installation de l'application sans fil.

3.11 Réserveation

SiPass Entro comprend des fonctions de réserveation (de terrains de sport, de courts de tennis, de salles de conférence, etc.) et fonctionne de pair avec le système de contrôle d'accès intégré.

L'Administrateur système définit les objets (tels que des lecteurs de carte ou des portes) qu'il est possible de réserver et décide des plannings de réserveation appropriés.

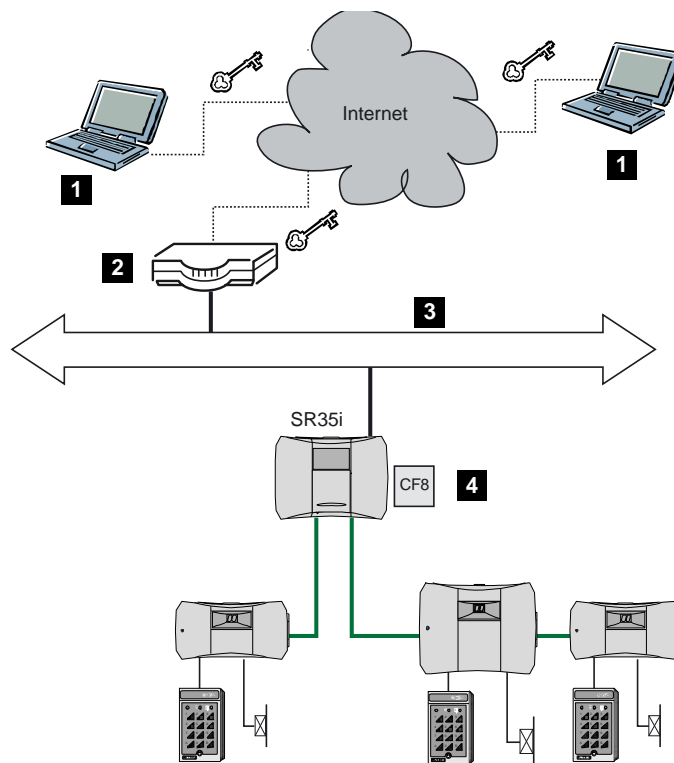
L'utilisateur souhaitant réserver une plage horaire peut se servir d'un navigateur Web standard (tel qu'Internet Explorer) afin de se connecter à l'unité SR35i contenant le système de réserveation. Il peut également passer sa carte dans un terminal de réserveation (InfoPoint IP812). Le mode de réserveation dépend de la configuration du système.

3.11.1 Serveur Web intégré

Le concentrateur SR35i intègre une fonction de serveur Web utilisée pour les applications de réserveation. Si la configuration choisie fait appel à Internet, les SR35i dédiés doivent disposer d'une connexion Internet permanente.



Au moins l'un des SR35i doit être équipé d'une carte mémoire dédiée à la réserveation Web pour stocker les informations relatives à la réserveation.

*Exemple d'une solution standard de réservation*

1	Navigateur Web
2	Passerelle
3	Réseau local (LAN)
4	Carte mémoire pour stocker les informations Web (serveur Web)

3.11.2 Installation du système de réservation

Tout d'abord, assurez-vous que toutes les portes et toute unité IOR6 (utilisée pour gérer les portes et les appareils dans les objets) sont installées conformément aux instructions précédentes. La carte CF8 est ensuite montée dans le SR35i destiné aux réservations.

Selon la configuration de la fonction de réservation, un ou plusieurs points d'information InfoPoint IP812 ou terminaux à écran tactile peuvent être connectés au système par le biais du réseau. Ainsi, il est possible de combiner ces terminaux à des PC. Note technique : l'intégralité des informations de réservation est stockée dans une page Web intégrée (dans un SR35i) possédant une adresse IP propre sur un réseau. La configuration est décrite dans le Manuel de l'utilisateur.

L'adresse de ce site Web <http://xxx.xxx.xxx.xxx.login.html> doit être communiquée aux utilisateurs du système de réservation.

3.12 Intégration d'un système CCTV

Le logiciel SiPass Entro est capable de communiquer avec 16 systèmes DVR au maximum via une connexion TCP/IP. Il prend en charge les unités DVR des gammes Siemens SISTORE™ AX, CX et MX.

Avant d'introduire des fonctionnalités DVR dans le système SiPass Entro, il est vivement recommandé de choisir un installateur possédant de solides connaissances en matière de systèmes DVR en général et de systèmes SISTORE™ en particulier.

Implémentation

L'intégration de l'enregistreur vidéo numérique (DVR) à SiPass Entro revient à connecter deux systèmes matériels distincts au moyen d'une connexion TCP/IP et de fonctions logicielles à distance. Autrement dit, vous installez au départ des composants logiciels pour les deux systèmes sur le même PC.

Lorsque vous configurez par la suite les fonctions (comme le déclenchement filtré ou limité dans la durée pour lancer l'enregistrement) dans SiPass Entro, celles-ci sont alors transmises au DVR. Lorsque les conditions d'une action donnée sont réunies, le DVR commence à enregistrer les images.

Vous avez ensuite la possibilité de lire à nouveau ces images directement depuis le contrôle d'accès aux portes de SiPass Entro à l'aide de certaines options de commande.

3.13 Intégration d'applications externes (BAPSI)

3.13.1 Généralités

En général, un logiciel de contrôle d'accès est propriétaire des composants du système, donnant rarement la possibilité de l'ouvrir à des applications personnalisées. Cela se comprend, car il s'agit d'un système de sécurité destiné, par exemple, à contrôler l'accès aux portes de différents bâtiments.

SiPass Entro peut utiliser une interface de configuration bien définie afin de communiquer avec d'autres progiciels externes (de contrôle de présence, d'alarmes, etc.) en vue d'importer ou d'exporter des cartes, d'obtenir des tâches datées ou des rapports d'événements.

Une liaison **TCP/IP** classique permet de transférer les données entre les différents composants logiciels.

Il est indispensable de modifier/d'étendre le logiciel externe conformément à la spécification d'intégration d'applications externes appelée BAPSI. Vous noterez qu'il ne s'agit pas d'un programme, mais de simples instructions relatives à l'interface de programmation.

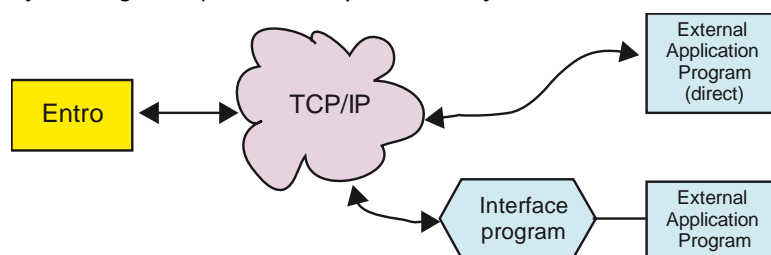
Grâce à l'interface BAPSI, l'intégration se passe de manière spécifique et sécurisée (avec cryptage), garantissant le maintien du niveau de sécurité et d'intégration du système de contrôle d'accès.

Vous pouvez demander la spécification auprès de Siemens AB, Security Products.

3.13.2 Champ d'application de BAPSI

En général, l'interface utilisateur d'un logiciel de contrôle d'accès permet d'utiliser des fonctions telles que la reconnaissance de carte, la programmation du planning ou la création (et la consultation) d'un journal d'événements.

Grâce à l'interface BAPSI, l'application logicielle personnalisée peut bénéficier de l'envoi et de la réception de messages en provenance/en direction du système de contrôle d'accès. Il est par ailleurs facile d'ajouter de nouvelles fonctions au système global (contrôle de présence, systèmes de réservation, etc.).



3.13.3 Applications pratiques

Actuellement, il existe déjà des systèmes fonctionnant dans le secteur des applications de réservation et utilisant l'interface logicielle BAPSI. Dans cet exemple, le fournisseur du logiciel de réservation externe a modifié son module logiciel (qui écrit les données dans un fichier) et Siemens AB, Security Products a développé un module spécifique qui lit ce fichier et transmet les informations qu'il contient au système de contrôle d'accès.

3.13.3.1 Exemple d'application - Système de réservation externe

Pour le marché suédois principalement, Siemens AB, Security Products a développé une application (reposant sur l'interface BAPSI) appelée BAPSER, qui assure la transmission des données entre SiPass Entro et des logiciels de réservation externe (actuellement Idavall-Fri et Argentum-Booking).

Le module est installé sur le PC externe qui fait appel à une liaison TCP/IP pour transmettre les réservations à SiPass Entro.

Si vous projetez d'utiliser BAPSI d'une manière ou d'une autre, vous devez configurer au préalable certains paramètres de SiPass Entro.

Cette procédure est décrite dans la documentation livrée avec l'application BAPSER. Vous pouvez toutefois accéder aux menus en procédant comme suit :

1. Lancez le programme d'installation et ouvrez le menu **Connexions**.
2. Cliquez sur **Nouveau**.
3. Sélectionnez **BAPSI - Intégration d'applications externes** et continuez.
4. Configurez les paramètres nécessaires en fonction de l'application.
5. Cliquez sur **OK**.

4 Configuration minimale requise

Configuration minimale requise pour l'ordinateur

- Processeur 1 GHz
- 512 Mo RAM
- Lecteur de CD-ROM
- Moniteur couleur VGA doté d'une résolution de 1 024 x 768
- Connexion réseau local (ou port série pour la connexion du concentrateur de segments/modem)
- Windows XP, Vista, Windows 7, Windows 8 ou Microsoft Terminal Server 2008/2003. (Nous recommandons d'installer la version la plus récente du Service Pack du système d'exploitation.)

Configuration minimale requise pour le réseau

- Câble Ethernet de type paire torsadée 10/100 Mbit/s
- Communication entre les SR35i via TCP/IP
- Nous vous recommandons d'utiliser une adresse IP statique/permanente pour chaque SR35i (souvent, les adresses du masque de réseau et de la passerelle sont également requises)
- Nous vous recommandons d'utiliser une connexion permanente à Internet sur le SR35i (dans le cas d'une connexion via Internet).
- Si un DVR et des caméras sont connectés, lisez les sections Paramètres MX [→ 72], Paramètres AX [→ 73] et Paramètres CX [→ 75] pour plus de détails sur les ports à utiliser.

Remarque : lorsque la connexion s'effectue via Internet, les ports suivants doivent être ouverts (dans un pare-feu ou similaire) et configurés de la manière suivante :

Ports	Description
25	Utilisé pour la communication par courrier électronique (SMTP).
53	Utilisé pour les fonctions DNS en cas d'utilisation d'adresses IP dynamiques.
80	Utilisé pour les réservations via Internet.
123	Utilisé pour définir l'heure correcte lorsque les différents SR35i communiquent à l'aide du protocole TCP (SNTP).
4001	Utilisé pour la communication entre les différents SR35i (UDP).
4002	Utilisé lorsque la communication s'effectue entre le PC et le SR35i choisi (TCP).
4011	Utilisé pour la communication entre les différents SR35i (TCP) via un réseau local.

4.1 Recommandations relatives au câblage

Le tableau ci-dessous représente les types de connexion qu'il est possible de définir dans SiPass Entro.



Siemens AB, Security Products ne garantit pas le fonctionnement de systèmes utilisant d'autres types de câble de connexion que ceux recommandés. Des câbles de différents types ne doivent pas être combinés entre deux points de connexion.

Unité source	Unité cible	Type de câble	Longueur maximale (m)
PC	SR35i	RS232 : Câble reliant l'ordinateur et l'imprimante au concentrateur de segments. Longueur maximale : 25 mètres. Câble recommandé : câble droit blindé (4 + blindage), ex., Belden 9534.	25 m
	SR35i	Réseau : Câbles de Cat-5, 10/100 Mbit/s. En cas de doute, consultez votre responsable informatique.	Selon l'architecture du réseau ; généralement 100 m vers le routeur/commutateur/concentrateur
SR35i	SR35i	RS485 : Boucle "globale" reliant les concentrateurs de segments. Câble recommandé : paire torsadée blindée (1 paire + blindage) - ex., Belden 9502.	1 200 m
	SR35i	Réseau : Câbles de Cat-5, 10/100 Mbit/s. En cas de doute, consultez votre responsable informatique.	Selon l'architecture du réseau ; généralement 100 m vers le routeur/commutateur/concentrateur
SR35i	DC22 DC12 DC800 IOR6	RS485 : boucle "locale" reliant un concentrateur de segments aux terminaux/centraux de porte subordonnés. Paire torsadée blindée (1 paire + blindage), ex., Belden 9502 (communication) et 1,5 mm ² (alimentation) OU PAARFLEX CY (câble propriétaire regroupant à la fois la partie communication et alimentation).	1 200 m
DC22 DC12 DC800	BC43 M43 PR500 HD500 SP500	BC-Link : Câble recommandé : câble droit blindé (4 + blindage), ex., Belden 9534.	30 m

Unité source	Unité cible	Type de câble	Longueur maximale (m)
	PM500 PP500		
	HF500 BC5511	Clock&Data : Câble recommandé : câble droit blindé (6 + blindage), ex., Belden 9536.	50 m
	Lecteurs Wiegand	Wiegand : Câble recommandé : câble droit blindé (6 + blindage), ex., Belden 9536.	50 m

4.2 Câbles

Vous pouvez utiliser différents types de câbles pour les différents niveaux de communication de SiPass Entro, de même que pour l'alimentation.

4.2.1 Câble d'alimentation

Quelle que soit l'ampleur de votre système, l'utilisation de câbles de longueur adéquate est essentielle. Le facteur principal à prendre en considération est le raccordement du câble à l'environnement de porte. Dans la plupart des cas, les dispositifs de verrouillage électriques ont une consommation électrique importante et risquent de provoquer des chutes de tension. Par conséquent, assurez-vous de connaître les types de verrous utilisés (gâches électriques, verrous moteur, etc.) lorsque vous procédez au dimensionnement des câbles.

La majorité des systèmes de contrôle d'accès font appel à un type de bloc d'alimentation centralisé, tel qu'une batterie de secours. Dans ce cas, il est primordial d'utiliser des câbles de section suffisante (prévoyez 1,0 mm² au minimum).

Cette nécessité exclut les câbles de données tels qu'ELAKY, Belden, CAT-5, CAT-6, CAT-7, etc., ceux-ci se situant généralement entre 0,1 et 0,2 mm², ce qui n'est pas suffisant pour alimenter une batterie de secours. Les câbles combinés PAARFLEX 2 x 1,5 mm² sont populaires pour cet usage (également disponibles en paire 2 x 0,5 mm² pour la transmission de données).

Pour obtenir des conseils sur la planification d'un réseau câblé, lisez les informations relatives à l'alimentation électrique [→ 39].

4.2.2 Câble pour RS485

La liaison des SR35i aux environnements de portes doit s'effectuer à l'aide d'un câblage RS485, composé de câbles blindés et torsadés dont la longueur ne peut dépasser 1 200 m.

Si chaque concentrateur SR35i est alimenté par un bloc d'alimentation dédié, un simple câble de transmission de données suffit (par exemple, un câble combiné ELAKY, Belden ou similaire).

Cela dit, si deux SR35i partagent la même source d'alimentation, une paire de câbles supplémentaire est requise. Vous pouvez utiliser pour ce faire un câble combiné, celui-ci étant également disponible avec deux paires de fils de communication.

4.2.3 Câble réseau (TCP/IP)

Si l'ordinateur et le SR35i – ou les SR35i entre eux – sont reliés par réseau local, un câble de réseau local existant suffit. L'utilisation d'un câble de type Cat-5 (10/100 Mbit/s) est obligatoire.

Les concentrateurs SR35i sont équipés de commutateurs réseau intégrés, dotés de deux connexions externes et une interne pour SR35i. Cela signifie que vous pouvez utiliser un câble réseau standard – sans faire appel à un concentrateur – pour raccorder directement l'ordinateur et/ou le réseau local LAN.

Quels que soient les câbles utilisés (anciens ou nouveaux), consultez le responsable du parc informatique du client avant de procéder à la programmation ou à la configuration préliminaire du système.

4.2.4 Câble de connexion au PC

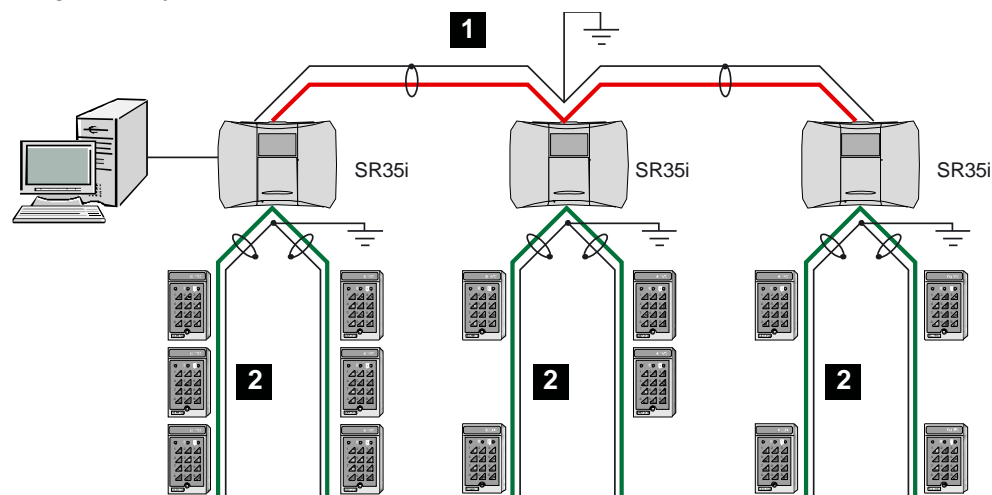
Utilisez un câble RS232 pour connecter les SR35i au port COM du PC.

Dans un environnement réseau local, un câble de réseau local standard (Ethernet Cat-5) suffit.

4.2.5 Mise à la terre et blindage pour RS485

Le blindage des câbles à la terre sur chaque boucle doit se faire en **un seul point** du système (voir le diagramme). N'oubliez pas que les parties métalliques (des portes, par exemple) sont en contact avec la terre. Par conséquent, le blindage ne doit pas être en contact avec ces parties ni avec d'autres éléments métalliques.

Évitez de placer les câbles à proximité de sources utilisant du courant de haute intensité (ascenseurs, garages, etc.). En effet, ces dernières peuvent être à l'origine de dysfonctionnements.



Connexion du blindage

1	Bus global
2	Bus local

5 Alimentation électrique

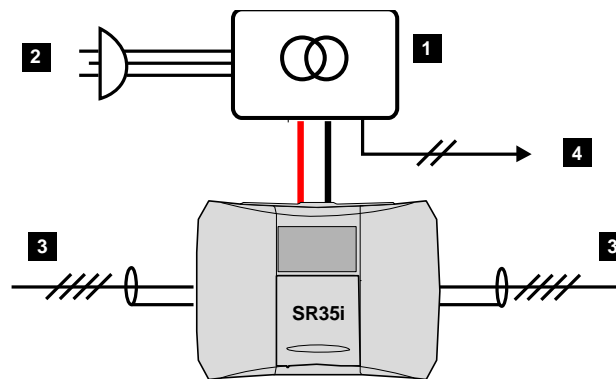
5.1 Bloc d'alimentation en courant continu (DC) centralisé

Des blocs d'alimentation centralisés sont souvent utilisés pour alimenter les systèmes de contrôle d'accès. Ils présentent en effet les avantages suivants :

- Alimentation stable à 24 (ou 12) V pour le dispositif de verrouillage électrique (qui dispose généralement d'une tolérance de +/- 15 %).
- Alimentation de secours en cas de chute de tension sur le secteur.
- Possibilité d'émettre un signal lorsque la tension du secteur chute et que la batterie de secours est utilisée.
- Nombre inférieur d'unités à installer.
- Extension du système facilitée (à condition d'aménager une marge suffisante dès le départ).

Il convient de souligner que le SR35i est équipé d'une pile lithium permettant de conserver les données en cas de panne de courant.

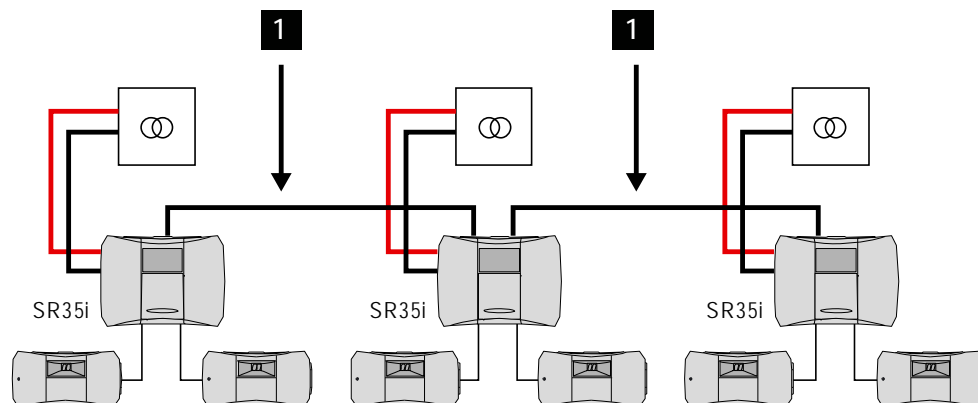
Le bloc d'alimentation doit être connecté conformément aux instructions ci-dessous. Veuillez néanmoins à ne pas alimenter les câbles sortants.



1.	Bloc d'alimentation
2.	2 secteurs + terre
3.	Bus local (4 + blindage)
4.	Batterie de secours connectée à l'IOR6

Communication isolée

Cette méthode de communication vise à former un système où chaque segment est alimenté séparément, comme illustré ci-dessous. Une telle application permet de réduire le risque de courant de terre, les concentrateurs de segments n'étant reliés que via un RS485 galvaniquement isolé. Notez que l'isolation des SR35i peut également être obtenue par le biais d'un réseau local TCP/IP.



Exemple de communication isolée à l'aide de blocs d'alimentation centralisés

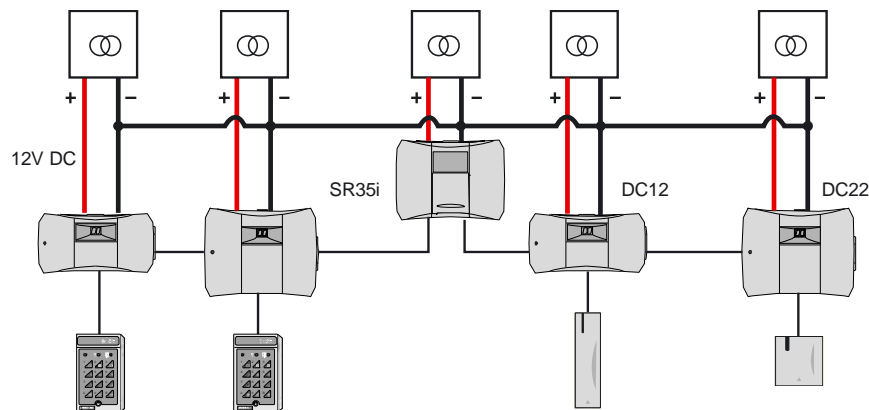
1	Communication globale isolée RS485
---	------------------------------------

5.2 Bloc d'alimentation en courant continu (DC) local

Lorsque vous utilisez des blocs d'alimentation séparés pour un ou plusieurs lecteurs SiPass Entro, n'oubliez surtout pas de **raccorder les fils négatifs (0 volt)**. En effet, l'interface de communication RS485 utilisant le potentiel négatif comme référence, d'éventuelles différences de potentiel entre les unités risquent d'entraver le fonctionnement de la communication.

La tension de sortie des blocs d'alimentation doit impérativement rester stable. Même si les composants du système SiPass Entro tolèrent les fluctuations de tension, les verrous peuvent s'avérer plus sensibles.

Veillez également à utiliser des câbles de section suffisante pour l'alimentation, particulièrement lorsque les distances à parcourir sont importantes. L'exemple ci-dessous illustre une application de 12 V où l'alimentation des SR35i s'effectue via un bloc d'alimentation local.



Bloc d'alimentation local

5.3 Chute de tension

SiPass Entro est capable de fonctionner à des niveaux de tension inférieurs (allant jusqu'à environ 10 V DC). Il convient néanmoins d'éviter les chutes de tension inférieures à 20,4 V DC pour pallier aux limitations des dispositifs de verrouillage électriques de 24 V (ceux-ci disposant généralement d'une tolérance maximum de $\pm 15\%$).

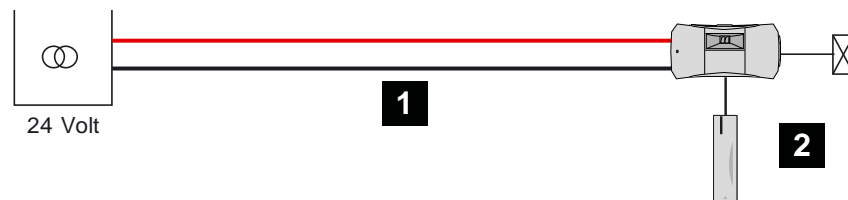
Le calcul de la chute de tension au niveau des câbles s'effectue à l'aide la loi d'Ohm, dont l'intitulé est le suivant :

Résistance (Ohm) x Courant (A) = Tension (V)

Les paramètres affectant les chutes de tension sont les suivants :

- Consommation électrique à chaque unité (en ampères)
- Section du câble (en mm²)
- Longueur (en m)
- Facteur de résistance du câble choisi (en ohm/m)

Pour comprendre la chute de tension, considérez l'exemple simple suivant :



Exemple de câblage

1	Câble du système de 100 m
2	DC12 + PR500 avec une gâche électrique

Méthode de calcul

Remarque : En dépit de la batterie de secours, la tension de sortie peut augmenter. Veuillez à toujours baser vos calculs sur la tension nominale d'une batterie de 24 V (ou 12 V) et sur la charge maximale des unités.

Consommation électrique au niveau du lecteur + verrou (A) = 0,160 A + 0,100 A = 0,260 A

Section du câble (mm²) = 1,5 mm²

Longueur (m) = 100 m x 2 (dans les deux directions) = 200 m.

Facteur de résistance du câble du système (ohm/m) = 0,0112 ohm/m

Résistance : 0,0112 ohm/m x 200 m = 2,24 ohm

Courant : 0,160 A + 0,100 A = 0,260 A

Résultat : 2,24 ohm x 0,260 A = chute de tension de 0,58 V. Ce qui signifie : 24,0 V – 0,58 V = 23,42 V au niveau du verrou. Ce niveau de tension est suffisant pour un dispositif de verrouillage électrique de 24 V.

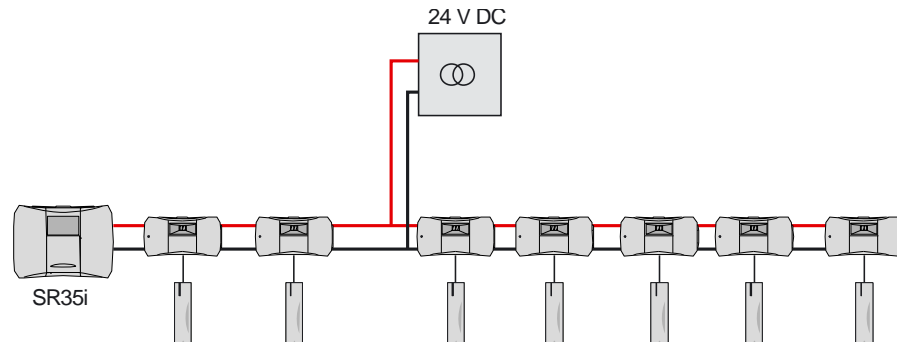
Résultat dans un système de 12 V DC

Dans la plupart des cas, une application de 12 V consomme davantage de courant qu'une application de 24 V. Dans cette optique, nous supposons que ces unités nécessitent 0,5 A.

Résultat : 2,24 ohm x 0,5 A = chute de tension de 1,12 V. Ce qui signifie : 12,0 V – 1,12 V = 10,88 V au niveau du verrou (valeur située sur la marge de tolérance des systèmes de 12 V mais suffisante).

5.4 Exemple d'une section d'alimentation standard

Vous pouvez placer au centre le bloc d'alimentation (de 24 V, par exemple), afin d'équilibrer la charge et d'obtenir une meilleure marge.

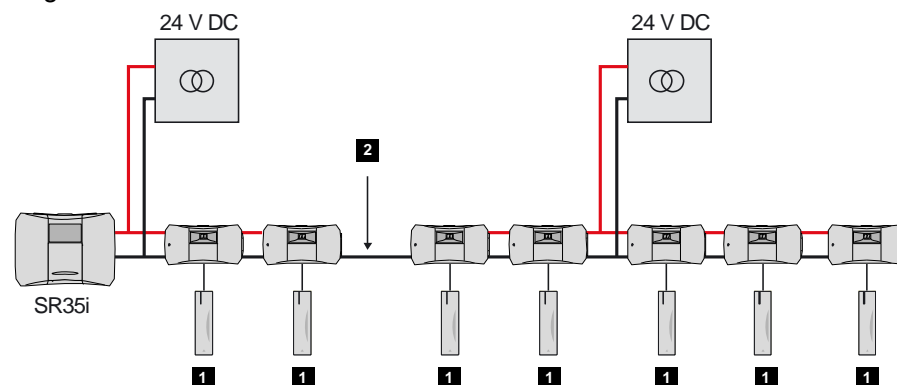


Section d'alimentation standard (24 V)

5.5 Blocs d'alimentation en courant continu (DC) multiples dans une même portion de câble

Il arrive parfois qu'un bloc d'alimentation ne suffise pas à alimenter toutes les unités d'une même section du système contrôlée par un SR35i. Si des blocs d'alimentation supplémentaires doivent être installés, n'oubliez pas de raccorder les fils négatifs. (Cette méthode s'apparente à l'utilisation de blocs d'alimentation locaux décrite dans les chapitres précédents).

Si vous omettez de raccorder les fils négatifs, la transmission des données (RS485) vers/depuis les environnements de portes risque d'échouer, le potentiel négatif étant utilisé comme référence.



Blocs d'alimentation multiples dans une même portion de câble

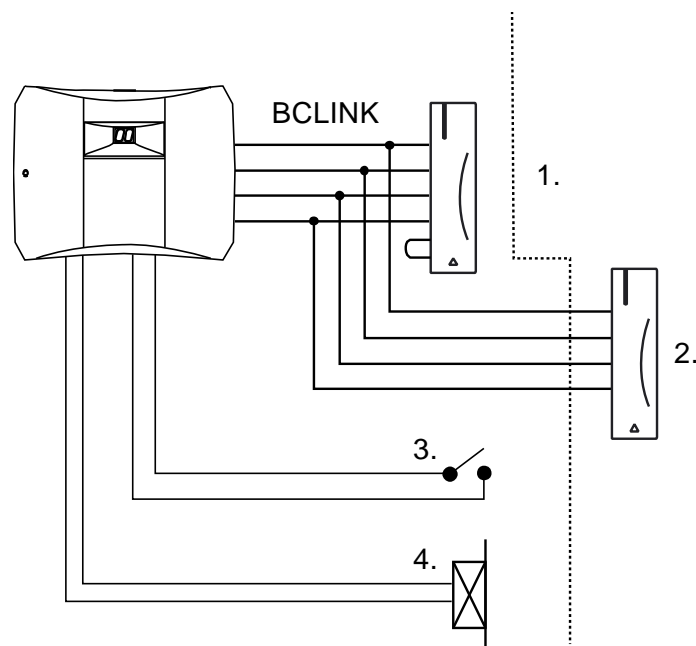
1	DC12 + PR500 avec une gâche électrique
2	Indispensable - utilisé comme référence pour la transmission de données

6 Installations particulières

6.1 Fonctions antipassback utilisant des lecteurs BC-Link

Lorsque des lecteurs BC-Link sont installés pour des fonctions antipassback, une technique de sous-adressage est utilisée. Par exemple, dans un PR500, l'entrée ENTRY et le cavalier EXIT sont contrôlés de manière interne par un central de porte qui détermine la direction.

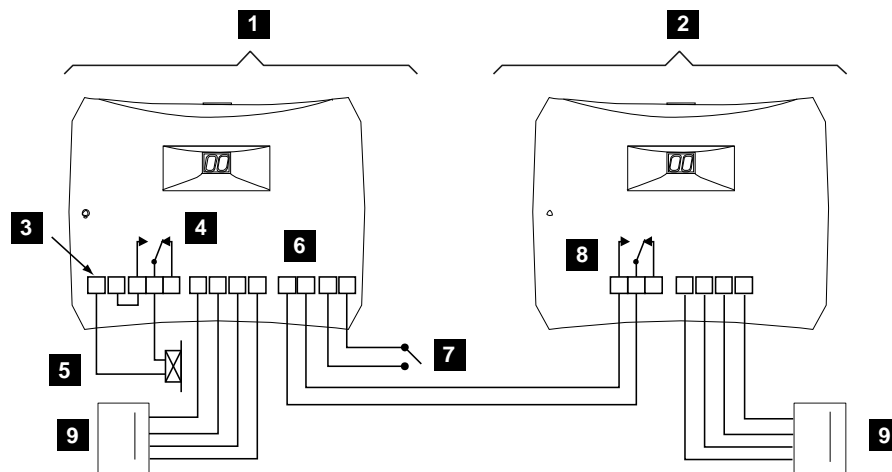
Le câblage des connecteurs de porte et de verrou s'effectue de la manière habituelle.



1.	Lecteur EXIT
2.	Lecteur ENTRY
3.	Connecteur de porte
4.	Dispositif de verrouillage électrique

6.2 Fonctions antipassback utilisant des lecteurs Clock&Data et Wiegand

Si les lecteurs ne prennent pas en charge le sous-adressage, les connecteurs de porte et les relais d'ouverture peuvent être connectés de la manière suivante :



1.	Lecteur ENTRY (entrée dans la zone)
2.	Lecteur EXIT (sortie de la zone)
3.	Alimentation
4.	Relais d'ouverture
5.	Verrou
6.	Ouverture à distance
7.	Connecteur de porte
8.	Relais d'ouverture. Remarque : contacts libres de potentiel
9.	Lecteur

Reliez uniquement les connecteurs sur le lecteur ENTRY. Connectez le relais d'ouverture du lecteur EXIT avec des contacts libres de potentiel à l'entrée d'ouverture à distance du lecteur ENTRY. Si besoin est, validez l'enregistrement de l'événement "Passage accepté - Bouton Sortie" dans les paramètres du filtre d'événements SiPass Entro.



Notez que seul le central de porte ENTRY contrôle l'ouverture physique de la porte. Le central de porte EXIT enregistre uniquement les accès concédés (depuis la zone), sans contrôler l'ouverture de la porte. Si vous souhaitez contrôler également les sorties, nous vous recommandons d'envisager une configuration différente, faisant appel à un **concentrateur** et à deux lecteurs BC-Link [→ 43] (sous-adressage).

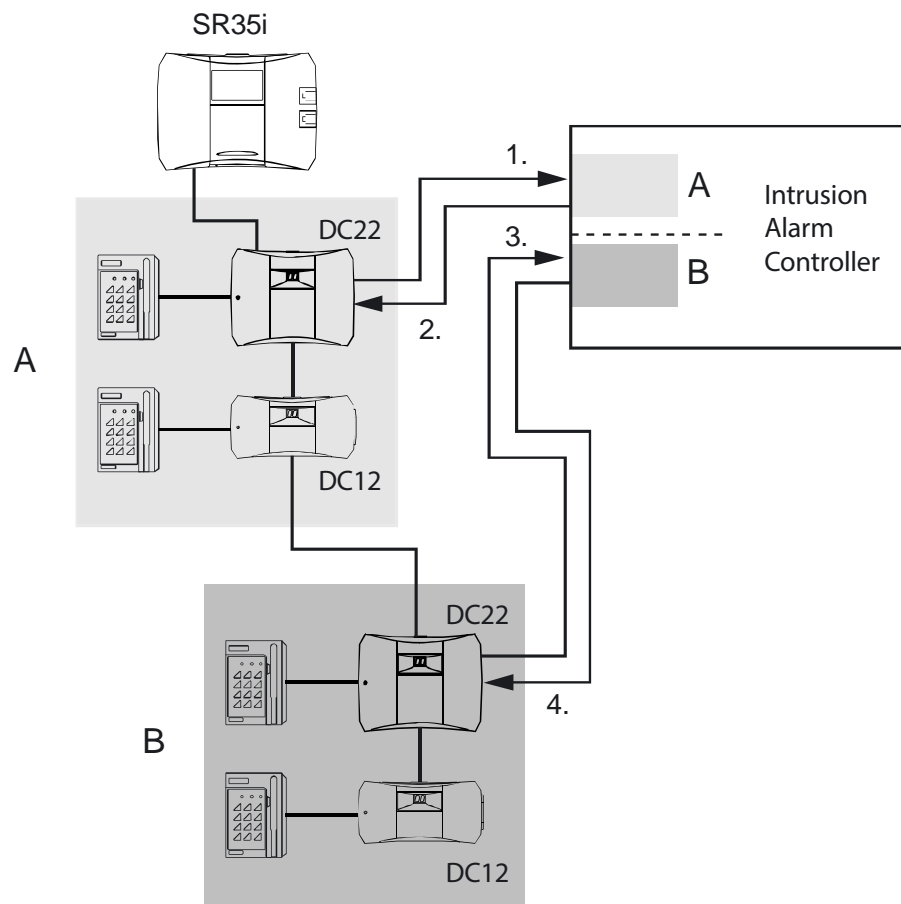
6.3 Zones sous alarme anti-intrusion incluant un DC22

L'utilisation d'un central de porte DC22 est requise lorsque SiPass Entro est chargé de contrôler un système de détection d'intrusion bistable.

Pour bénéficier d'une sécurité optimale, vous installez et utilisez normalement des **lecteurs de carte équipés d'un pavé numérique** sur toutes les portes permettant d'entrer dans la section spécifique du système de détection d'intrusion. Vous pouvez ensuite choisir le niveau de sécurité Carte pour armer l'alarme et Carte + code individuel pour la désarmer.

Si une zone de la section couverte par le système de détection d'intrusion comprend plusieurs portes, vous devez configurer SiPass Entro de sorte qu'il utilise une ou plusieurs **zones sous alarme**. Chacune de ces zones doit ensuite inclure au moins un DC22 (doté du relais) tandis que le contrôle des autres portes s'effectue à distance au moyen du bus système SiPass Entro.

L'illustration ci-dessous représente l'aspect possible de deux zones distinctes :



Exemple de zones sous alarme

1.	Signal d'armement pour la zone A (émis par le DC22)
2.	Signal d'état de la synchronisation entre les systèmes (reçu par le DC22)
3.	Signal d'armement pour la zone B (émis par le DC22)
4.	Signal d'état de la synchronisation entre les systèmes (reçu par le DC22)

6.4 Connexion des informations sur l'état de l'alarme (ASF) dans le DC22

Lorsque le DC22 sert à synchroniser SiPass Entro et un contrôleur d'intrusion externe, il est possible d'utiliser un signal d'informations *en provenance* du système de détection d'intrusion. Selon l'état du signal, SiPass Entro détermine l'état d'activation ou de désactivation du système de détection d'intrusion et agit en conséquence (en "bloquant" ou en verrouillant des portes, par exemple).

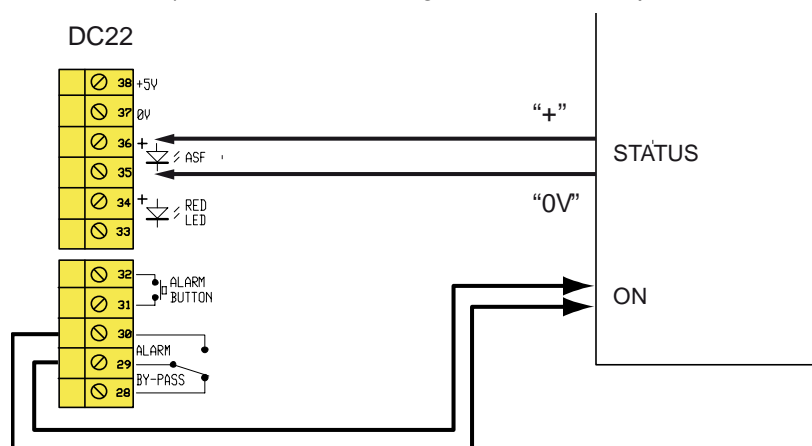
Deux modes de connexion sont possibles entre les systèmes :

- Signal de tension
- Signal de fermeture (libre de potentiel)

Les illustrations ci-dessous décrivent les différentes méthodes de contrôle des informations sur l'état des alarmes.

Utilisation du signal de tension

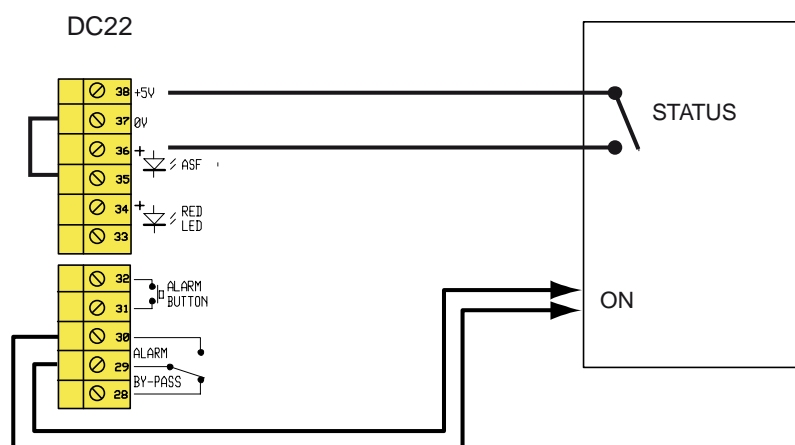
Dans ce cas, le contrôleur d'intrusion doit envoyer un signal de tension (de 24 V CC maximum) et une référence négative doit être disponible.



Informations sur l'état de l'alarme contrôlées par la tension

Utilisation du signal de fermeture

Le contrôleur d'intrusion procède à la fermeture. Vous remarquerez qu'un cavalier doit être installé sur le DC22 entre les éléments 35 et 37.



Informations sur l'état de l'alarme par signal de fermeture

7 Guide de prise en main

Bien que SiPass Entro comprenne de nombreuses et diverses fonctions conçues pour répondre aux exigences variées des clients, la procédure à suivre pour élaborer un système de contrôle d'accès de base comporte peu d'étapes.

La liste ci-dessous récapitule les étapes à suivre pour mettre rapidement en service le système SiPass Entro :

- Installation du logiciel sur le PC [→ 57]
- Réglage de la date et de l'heure [→ 82]
- Programmation de noms pour les concentrateurs de segments [→ 86] et Configuration du SR35i [→ 89]
- Définition des fonctions horaires
- Programmation de noms et de fonctions pour les portes [→ 93] et Configuration des portes*
- Configuration des groupes d'accès*
- Connexion des détenteurs de carte*
- Impression de cartes*
- Configuration des utilisateurs du système*
- Enregistrement des accès*
- Affichage de l'état et des événements*

Si vous projetez d'utiliser d'autres fonctions, lisez les sections pertinentes pour en savoir plus à leur sujet.

- Système de détection d'intrusion [→ 100]
- Intégration d'un DVR et contrôle de la caméra*
- Fonctions de réservation*

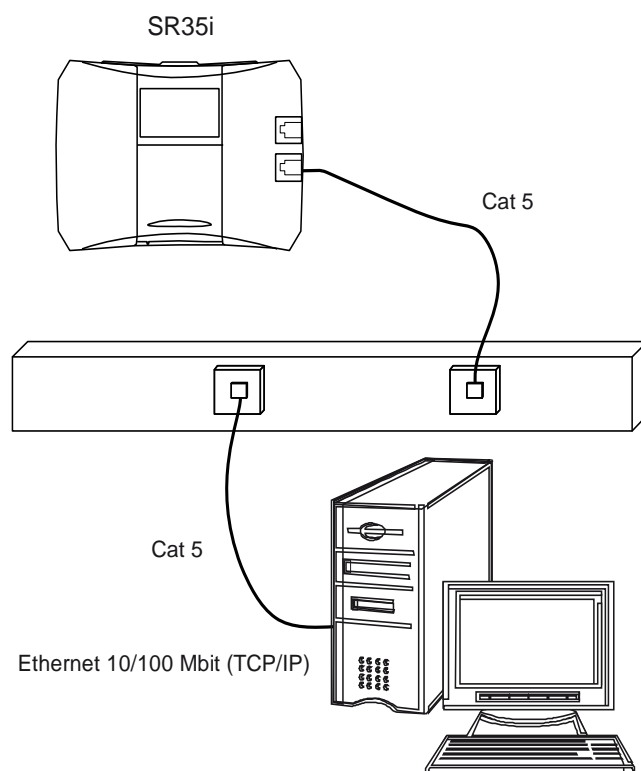
* Plus d'informations sur cette fonction dans les autres documents

8 Connexion des ordinateurs ou d'une imprimante en ligne

8.1 Connexion du PC par le réseau local (LAN)

Si vous souhaitez vous connecter via le réseau local, procurez-vous auprès du responsable informatique l'adresse IP et les paramètres d'installation du système corrects.

1. Connectez le câble Ethernet au PC et au réseau local.
2. Connectez le câble Ethernet au SR35i et au réseau local.



Exemple de connexion d'un PC par le réseau local (LAN)

Simulation de réseau

Il est également possible de simuler un "réseau local" seulement composé d'un SR35i et d'un PC connectés directement. Dans ce cas, vous utiliserez un câble réseau entre l'ordinateur et le commutateur réseau du SR35i.



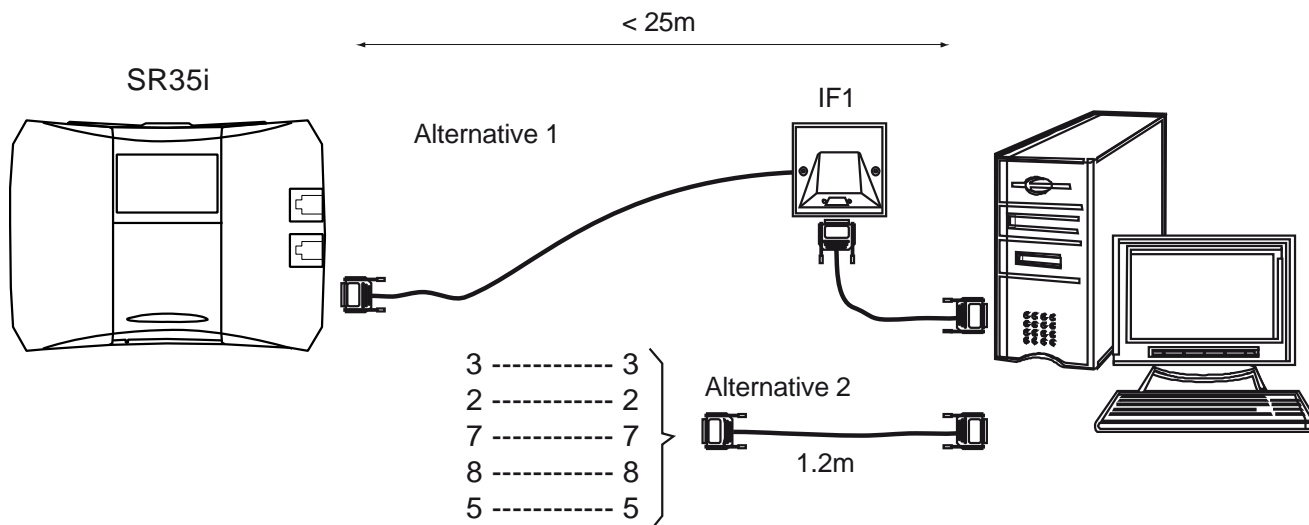
Si vous connectez un PC temporaire directement au SR35i à l'aide d'un câble réseau, nous vous recommandons de définir pour ce PC une adresse IP statique. Optez de préférence pour une adresse comprise dans l'intervalle 10.1.200.xxx (avec un masque de réseau 255.0.0.0), car l'adresse IP initiale du SR35i se situe dans cette plage.

8.2 Connexion directe par câble (RS232) d'un PC

Le concentrateur de segments doit être installé à proximité (25 mètres au maximum) du PC.

L'illustration ci-dessous présente un kit complet disponible, constitué d'une prise murale (IF1), d'un câble RS232 standard (d'environ 1,2 m) et d'un câble de 25 m de long doté d'une extrémité libre à brancher sur le bornier à vis de la prise murale. Vous pouvez brancher le PC au SR35i directement au moyen du câble standard (alt. 2) ou procéder à une installation permanente (alt. 1).

Le RS232 requiert moins d'opérations de paramétrage sur l'ordinateur, ce qui facilite la configuration. Ainsi, vous pouvez utiliser le RS232 de manière temporaire et passer à Ethernet plus tard.



Deux alternatives de câblage du RS232

La distance totale entre l'ordinateur ou l'imprimante et le concentrateur de segments ne doit pas dépasser 25 mètres.



Le port RS232 peut également être connecté à une imprimante. Notez que vous pouvez connecter **soit** un PC **soit** une imprimante à un concentrateur de segments, et **non** les deux.

8.3 Connexion d'une imprimante en ligne (RS232)

Pour configurer une imprimante en ligne en vue de l'impression directe à partir d'un SR35i, veuillez procéder comme suit.

1. Lancez le programme d'installation [→ 79].
2. Choisissez **Propriétés du système > Connexions** et activez les connexion multiples.
3. Sélectionnez **Nouveau**.
4. Sélectionnez **Imprimante - Création d'un journal d'événements** et cliquez sur **Suivant**.
5. Saisissez le **nom** de la connexion.
6. Précisez quel concentrateur SR35i est connecté à l'imprimante.

7. Sélectionnez le filtre des événements à utiliser.

Les paramètres suivants sont appliqués pour l'interface RS232 : 9 600 bauds ou 57 600 bauds, sans parité, 8 bits, 1 bit de démarrage, 1 bit d'arrêt, impression avec protocole d'établissement de liaison matériel (table de caractères ISO 8859-1).

9 Préparation des ressources réseau

Avant de procéder à l'installation du logiciel, vous devez définir et configurer un certain nombre de ressources.

N'oubliez pas également que pour certains modèles de SR35i il vous faudra configurer DHCP via le système de menus du SR35i [→ 92].



Il est vivement recommandé d'inviter le responsable du parc informatique des utilisateurs finaux/acheteurs à participer à la planification d'un système SiPass Entro de type TCP/IP. Il est également indispensable de posséder des connaissances générales en matière de réseaux.

9.1 Introduction

Adresses IP statiques

L'utilisation d'adresses IP statiques est possible au sein de réseaux locaux et/ou de réseaux intégrant Internet (pour des fonctions de réservation, par exemple).

Attention : certains fournisseurs de services Internet n'autorisent pas l'utilisation d'adresses IP statiques.

Dans un environnement de réseau local, le seul facteur à considérer est le "degré d'isolation" du système de sécurité en place, par rapport à celui d'un réseau bureautique. Autrement dit, il faut prendre en compte la présence de routeurs, de pare-feux ou de dispositifs similaires pouvant isoler SiPass Entro du reste de l'équipement réseau.

Adresses IP dynamiques

Dans les versions précédentes du logiciel SiPass Entro, le concentrateur de segments devait répondre à un mode d'adressage IP statique, qui continue à représenter la méthode d'adressage préconisée du moment que le réseau local le permet. (Imaginez ce type d'adressage comme l'utilisation d'un numéro de téléphone permanent). Les adresses IP statiques se caractérisent à la fois par leur rapidité et leur fiabilité.

Certains locaux ne font appel qu'à un seul fournisseur de services Internet, offrant uniquement des comptes et des connexions utilisant le protocole **DHCP** (Dynamic Host Configuration Protocol, protocole de configuration d'hôte dynamique).

Autrement dit, l'environnement hôte (le fournisseur) "loue" une adresse IP pendant une courte période, ce qui lui permet d'en changer lors du renouvellement de la période de bail.

Comme les adresses IP ne sont pas statiques, il faut prévoir une fonction renvoyant à un nom fixe pouvant être converti en concept compréhensible sur Internet, c.-à-d. en adresses IP. En général, ce type de fonction est appelé **DNS** (Domain Name Service) et peut être considéré comme un "annuaire de noms" renfermant des adresses IP. L'annuaire réside habituellement chez le fournisseur et est également accessible par le biais d'une adresse IP (généralement prise en charge avec les adresses IP louées).

Avec l'implémentation du protocole DHCP (et le fait que le fournisseur de services Internet change fréquemment l'adresse IP louée des ordinateurs et utilisateurs connectés), le DNS doit lui aussi être mis à jour en fonction des informations modifiées. Cette opération est appelée **DNS dynamique** (DDNS) : elle implique que le matériel peut "demander" à ce service l'adresse IP actuelle associée à un nom donné.

9.2 Agent de sous-réseau (SR35i)

Le terme "**agent de sous-réseau**" est utilisé pour désigner un **SR35i dédié**, chargé d'administrer la communication entre les concentrateurs SR35i résidant dans un sous-réseau local (en présence de routeurs).

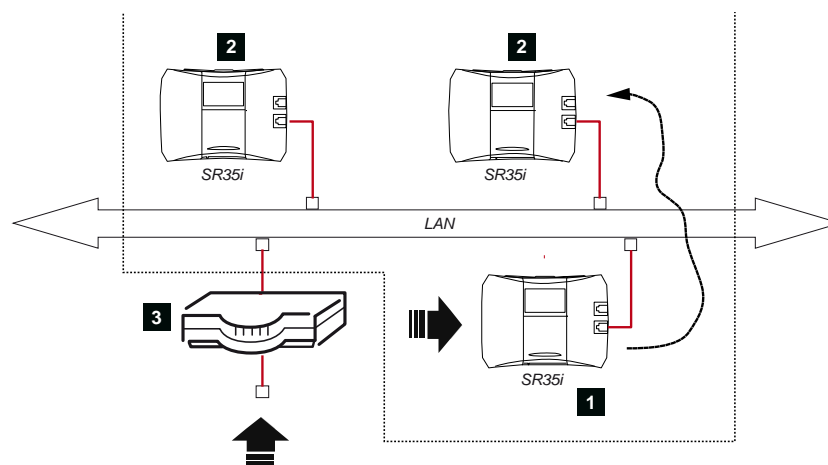
De l'extérieur, seule l'adresse IP du routeur est visible. Pour y remédier, l'agent de sous-réseau gère le trafic vers les autres SR35i inclus dans le sous-réseau.

Le routeur [→ 52] est configuré avec les paramètres appropriés de l'agent de sous-réseau.

Si ce dernier utilise DHCP, l'adresse MAC doit également être connue, pour permettre au routeur d'obtenir l'identité physique (= MAC) du SR35i.

Procédez comme suit :

1. Mettez sous tension l'unité SR35i matérielle.
2. Appuyez sur les boutons **2 > 2 > 1**.
 - ⇒ L'**adresse MAC** est affichée sous la forme de 12 caractères. Veuillez en prendre note pour une utilisation ultérieure.
3. Appuyez sur Echap.
4. Appuyez sur les boutons **2 > 1 > 1**.
 - ⇒ Les **paramètres IP** s'affichent. Veuillez en prendre note pour une utilisation ultérieure.



Exemple d'un sous-réseau en présence d'un routeur

1.	L'un des concentrateurs SR35i fait office d'agent pour le sous-réseau (voir pointillés).
2.	Les autres SR35i sont gérés par l'agent de sous-réseau.
3.	Routeur dont les ports sont ouverts et où l'adresse IP et/ou adresse MAC est configurée pour le routage.

9.3 Configuration du routeur

Vous devez configurer tout routeur utilisé dans un système SiPass Entro pour lui permettre de gérer correctement la communication. Cela signifie que les ports utilisés dans SiPass Entro doivent être ouverts. Reportez-vous au manuel d'instructions accompagnant votre routeur pour savoir comment modifier les paramètres.

Procédez comme suit :

1. Confirmez l'**adresse IP** de l'agent de sous-réseau dédié (SR35i). Si l'agent de sous-réseau utilise DHCP, assurez-vous de connaître également l'adresse MAC [→ 52] du SR35i en question.
2. Configurez l'adresse IP et/ou MAC dans le routeur afin que celui-ci sache où rediriger les informations envoyées vers les ports associés à SiPass Entro.
3. Configurez les **ports** de la manière suivante :
TCP-4002 : Communication en provenance des ordinateurs.
TCP-4011 : Communication entre les SR35i
TCP-80 : Fonctions de réservation (le cas échéant).
UDP-123 : Fonctions horaires sur le réseau.
4. Recommencez les étapes ci-dessus pour chaque routeur utilisé dans le système.

Redirection DynDNS au niveau du routeur

Si le routeur est capable de gérer les redirections DNS dynamiques [→ 53], vous pouvez choisir d'utiliser celui-ci plutôt que les différents concentrateurs SR35i.

Pour qu'une telle configuration fonctionne, vous devez attribuer au sous-agent (SR35i) la même identité que le routeur.

9.4 DynDNS

Chaque fois que SiPass Entro fait appel à un serveur/routeur DHCP pour définir les paramètres IP, une fonction DNS (Domain Name Service) dynamique doit être établie. La fonctionnalité DynDNS permet de conserver intactes les identités des concentrateurs SR35i.

Vous pouvez faire appel à la redirection DynDNS de deux manières :

- En utilisant un routeur (si possible). Notez que l'identité choisie pour le routeur doit être identique à celle spécifiée pour le (sous-agent) SR35i. Reportez-vous au manuel d'instructions accompagnant votre routeur pour savoir comment configurer la fonction DynDNS du routeur.
- En utilisant un SR35i.

Quelle que soit la méthode choisie, un service DynDNS [→ 53] doit être établi.

9.4.1 Configuration de DynDNS.org

A l'heure actuelle, la configuration d'un compte chez DynDNS.org s'effectue de la manière suivante. Pour obtenir davantage d'informations, consultez le site Web de DynDNS.org (en anglais). Rendez-vous à l'adresse www.dynDNS.org. (www.dynDNS.com)

1. Créez un nouveau compte (avec un nom d'utilisateur et un mot de passe).
2. Si vous possédez votre propre domaine, sélectionnez Custom DNS (DNS personnalisé). Sinon, sélectionnez **Dynamic DNS** (DNS dynamique). Ces choix seront répercutés ultérieurement dans SiPass Entro.
3. Choisissez parmi les noms de domaines disponibles. Si vous optez pour **dynalias.net**, le SR35i reçoit l'identité réseau Identity1.dynalias.net. Pour vous faciliter la tâche, préparez la liste des identités réseau de tous les SR35i disponibles. Notez que l'identité réseau d'un concentrateur ne correspond pas au nom du concentrateur (utilisé dans le journal des événements).

4. Saisissez l'identité pour tous les SR35i restants qui utiliseront DynDNS. N'oubliez pas que lorsqu'un sous-agent (SR35i) est utilisé pour gérer d'autres SR35i situés derrière un routeur, lui seul requiert une identité. Cela dit, pour que le système fonctionne, il est primordial que l'identité en question soit exactement la même que celle du routeur.

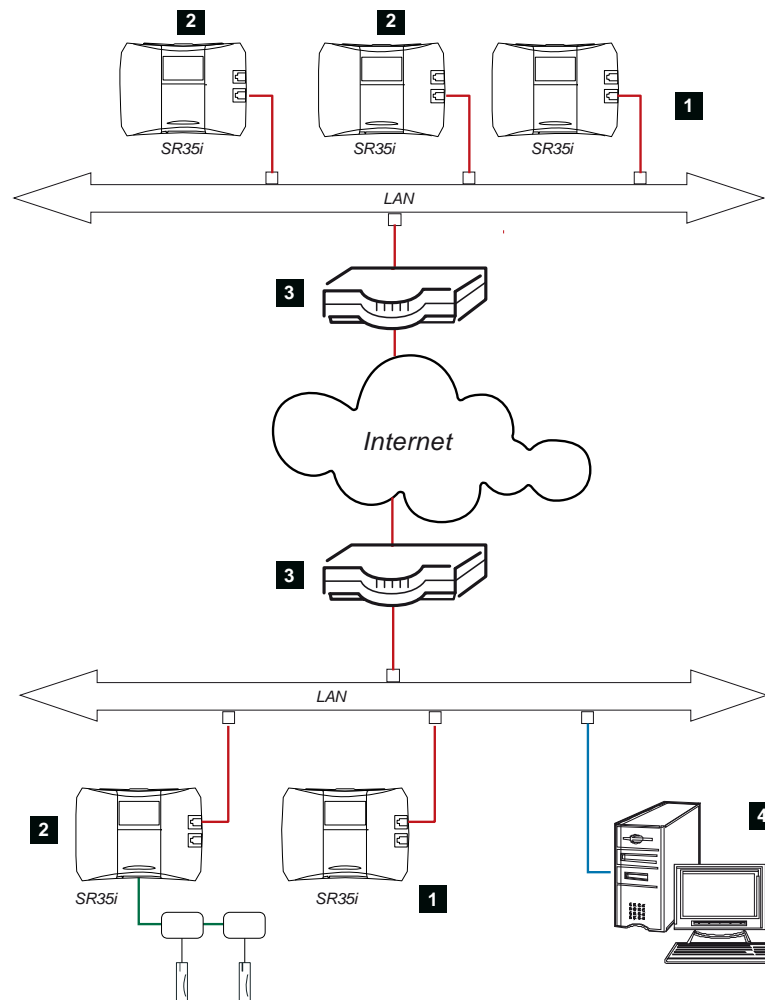
9.5 Pare-feu

Les systèmes incluant un pare-feu et un équipement SiPass Entro externe requièrent certaines opérations de configuration supplémentaires.

Selon l'application choisie, des ports et adresses IP doivent être ouverts. Renseignez-vous auprès du responsable informatique.

9.6 Exemple avec un routeur

Dans la plupart des cas, le système de contrôle d'accès est installé sur un réseau local (LAN) utilisant à la fois des adresses IP dynamiques et des "sous-réseaux". Le diagramme ci-dessous illustre un exemple de connexion via Internet.



Application avec Internet et des routeurs

1.	SR35i faisant office d'agent de sous-réseau. Le SR35i reçoit une adresse IP "fixe" qui est transmise au routeur (voir 3). L'agent de sous-réseau gère la communication vers les autres SR35i (voir 2) situés sur le même sous-réseau.
2.	SR35i résidant "à l'intérieur" du sous-réseau et doté d'une adresse IP dynamique. Le concentrateur ne peut pas être atteint directement de l'extérieur du routeur.
3.	Les routeurs doivent être configurés correctement, avec le port et l'adresse IP de l'agent de sous-réseau.
4.	PC dédié à l'administration du système.

9.7 Immeuble d'habitation – exemple

Pour les besoins de cet exemple, imaginons qu'une société immobilière installe un nouveau système SiPass Entro dans trois appartements différents, avec trois concentrateurs SR35i. Nous allons voir comment les concentrateurs sont configurés à l'aide du protocole DHCP ; nous utiliserons le service DynDNS car le fournisseur de services Internet n'autorise pas l'emploi d'adresses IP statiques.

L'un des bâtiments dans lesquels le **système de réservation** SiPass Entro sera utilisé comprend une buanderie ; les locataires utiliseront leur ordinateur domestique pour effectuer des réservations et obtenir des confirmations.

Les conditions requises dans ce cas de figure sont les suivantes :

- Un réseau local doit être prévu dans chaque immeuble où le SR35i sera installé.
- Assurez-vous de disposer d'un compte Internet afin de permettre l'utilisation d'identités pour les SR35i.
- Un SR35i doit également être équipé d'une mémoire flash CF8 pour assurer les fonctions de réservation.
- Un PC à usage administratif doit être prévu sur le système final.

Il est possible de préparer les trois concentrateurs à l'avance (préalablement au montage), car ils comprennent une batterie destinée à conserver les informations (la base de données) jusqu'à l'achèvement de l'installation finale.

Procédez comme suit :

1. Ouvrez un compte DynDNS [→ 53] sous le nom de domaine **dynalias.net**, le nom d'utilisateur **MyAccount** et le mot de passe **MyPassword**.
2. Voici la configuration définie pour le SR35i :

SR35i	Nom (consigné)	ID réseau
1	Concentrateur Appt 1	Appt1.dynalias.net
2	Concentrateur Appt 2	Appt2.dynalias.net
3	Concentrateur Appt 3	Appt3.dynalias.net

1. Installez le logiciel [→ 57] sur le PC. Tapez Appt1.dyndns.net comme identifiant réseau du premier concentrateur (utilisé par le PC pour établir les communications).
2. Sélectionnez l'option permettant de se référer à **DynDNS.org** et spécifiez le type de compte Dynamic DNS (DNS dynamique), le nom d'utilisateur MyAccount et le mot de passe MyPassword, puis quittez l'application.
3. Programmez manuellement tous les SR35i à l'aide du bouton **Nouveau** et saisissez les informations requises (nom, etc.).
4. Activez ensuite l'onglet **Réseau** et cochez la case **Obtenir une adresse IP automatiquement** (l'adresse du DNS peut alors être allouée).
5. Spécifiez les informations sous **Identité** en fonction du tableau ci-dessus (Appt1.dynalias.net, etc.). Indiquez également le nom du serveur de messagerie du fournisseur de services Internet (mail1.telia.com, par exemple) afin de préparer le concentrateur à l'envoi des confirmations.
6. Configurez tous les SR35i de la même manière.

10 Installation du logiciel

Une fois le logiciel installé (à partir du CD), lancez le programme d'installation.

Si votre système utilise la technique de l'adressage IP dynamique (DHCP) en réseau local, vous devez préalablement préparer le réseau [→ 51].

En général, l'installation démarre lorsque le CD est chargé. Si ce n'est pas le cas, procédez comme suit :

1. Dans le **menu Démarrer de Windows**, choisissez **Panneau de configuration**.
2. Cliquez deux fois sur l'icône **Ajout/Suppression de programmes**.
3. Cliquez sur **Ajouter**.
4. Placez le CD dans le lecteur de CD-ROM et cliquez sur **Suivant**.

⇒ Suivez les instructions qui s'affichent à l'écran.

Les étapes nécessaires à l'obtention du résultat final varient s'il s'agit d'un nouveau système ou non. Par exemple, le programme d'installation sera utilisé différemment selon que vous installez le premier ou le second PC, changez d'ordinateur ou ajoutez un ou plusieurs SR35i au système.

Parfois, il vous faudra fournir non seulement le nom du système, mais également le nom de l'utilisateur et un mot de passe pour être en mesure d'utiliser le logiciel.

La communication initiale au concentrateur SR35i est créée à l'aide d'un assistant.

10.1 Création d'une base de données et d'une connexion

La première fois que vous ouvrez le programme d'installation, aucune base de données ni information de **connexion** ne sont disponibles sur le PC. Un assistant démarre, pour vous aider à définir les paramètres requis. Selon les options sélectionnées, il se peut que certains des paramètres mentionnés ci-après ne soient pas requis.



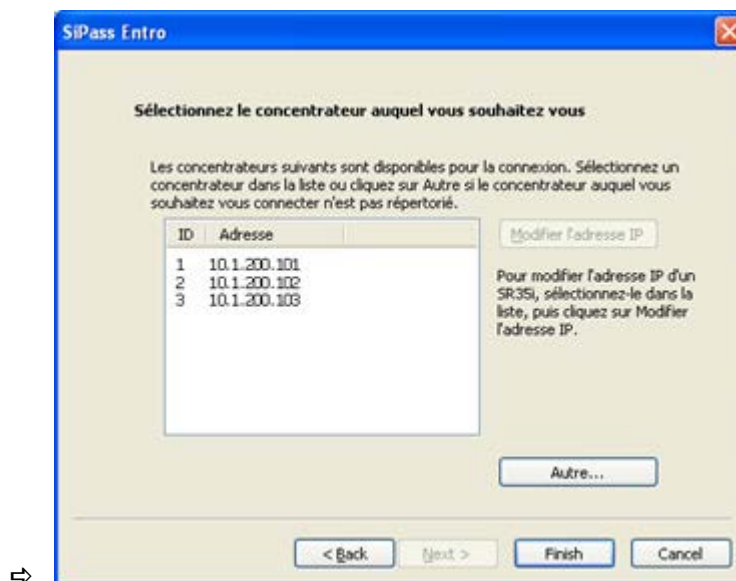
Dans la configuration par défaut, un seul ordinateur est connecté et l'onglet Connexions n'est pas visible dans le programme d'installation.

Si vous envisagez d'utiliser plus d'un ordinateur, lisez la section Environnement multi-utilisateur (plusieurs PC) [→ 60].

Procédez comme suit :

1. Ouvrez le menu **Démarrer de Windows**.
2. Choisissez **Programmes > SiPass Entro > Installation**.
⇒ L'assistant démarre.
3. Spécifiez s'il s'agit d'un système **nouveau** ou **existant** :
 - **Nouveau** :
Aucun système n'est encore configuré ; vous devez préciser un **Nom du site** et un **Nom du système**. (La clé de cryptage, le nom d'utilisateur et le mot de passe sont définis à ce moment-là).
 - **Existant** :
SiPass Entro est installé pour la connexion. Vous connaissez le **nom du système** et la **clé de cryptage** ainsi que les **nom d'utilisateur** et **mot de passe** du système.

4. Par défaut, l'assistant parcourt le réseau local et le port série à la recherche de SR35i connectés et affiche une liste des concentrateurs de segments détectés. Les concentrateurs connectés au port COM du PC seront également répertoriés.



5. Sélectionnez dans la liste le SR35i que vous souhaitez utiliser pour la connexion au PC. Remarque : vous ne pouvez choisir qu'un seul concentrateur !
6. Fermez l'assistant.

Sélection manuelle des SR35i

Si le SR35i voulu n'est **PAS** répertorié, cela signifie que le concentrateur en question est situé à l'extérieur du réseau local et que son adresse IP doit être configurée manuellement. Le réseau [→ 51] doit également être configuré correctement pour pouvoir mettre le PC en ligne.

1. Sélectionnez le mode de communication du PC avec le site (via **TCP/IP**, **RS232** ou via un **modem**).
 - Si vous optez pour un **modem**, indiquez le numéro de téléphone du modem sur le SR35i. Pour continuer, cliquez sur **Terminer**.
 - Si vous choisissez **RS232**, le logiciel détecte automatiquement le port COM correct du PC. Pour continuer, cliquez sur **Terminer**.
 - Si vous choisissez **TCP/IP**, l'assistant requiert la définition de paramètres supplémentaires. Pour continuer, cliquez sur **Suivant**.
2. Sélectionnez **Adresse IP statique** ou **Adresse IP dynamique** (DHCP).
 - Le cas échéant, saisissez l'adresse IP statique du SR35i.
 - Si vous préférez utiliser une adresse IP dynamique, suivez les instructions affichées à l'écran. Notez que le composant SR35i [→ 92] doit également être programmé. Utilisez pour ce faire le clavier et l'écran intégrés.
3. Cliquez sur **Terminer** et la fenêtre principale du programme d'installation s'affiche.



ATTENTION

	<p>Il est très important de noter le nom du système quelque part.</p> <p>Si vous remplacez le PC, ce nom devra être entré une nouvelle fois pour que le système fonctionne de nouveau.</p>
--	---

Normalement, les unités détectées doivent à présent être affichées. Vous pouvez choisir de programmer toutes les unités ou au moins l'un des SR35i, conformément aux instructions de la section Détection automatique des unités [→ 59].

Avant de poursuivre, patientez jusqu'à ce que les deux voyants soient verts [→ 80]. Tant que le programme d'installation est ouvert, les événements sont affichés dans le programme de contrôle de l'accès aux portes (à condition qu'il soit lancé).

10.1.1 Détection automatique des unités

Le programme d'installation incorpore des fonctions de "recherche" des concentrateurs de segments et centraux de porte connectés. Les extensions d'unités ultérieures peuvent également être détectées de cette manière.

Si le site est correctement installé avec les adresses appropriées, il ne vous reste qu'à configurer les SR35i et centraux de porte. La liste des unités s'affiche à l'écran dès que la connexion au programme d'installation est établie. Celle-ci répertorie les SR35i (*Cxx) ainsi que les unités de portes et les IOR6 (**Cxx:Dyy).

10.2 Environnement multi-utilisateur (plusieurs PC)

Si vous n'envisagez d'utiliser qu'un seul ordinateur, aucune disposition particulière n'est nécessaire. Une connexion a été créée automatiquement par l'assistant d'installation. Dans les cas où plusieurs ordinateurs seront connectés, vous devez configurer le logiciel en vue d'utiliser de multiples **connexions**.

Chaque PC (utilisé dans les applications réseau) doit être relié (connecté) au même SR35i. Ceci s'avère particulièrement important si le SR35i est utilisé comme "agent de sous-réseau". Les concentrateurs gérés par cet agent de sous-réseau ne peuvent pas être raccordés à un PC.

Procédez comme suit :

- ▷ Vous devez disposer d'une licence du logiciel SiPass Entro valable pour chaque PC.
- 1. Activez l'onglet **Connexions** sous **Système/Propriétés du système**, puis sélectionnez l'option de connexion simultanée de plusieurs ordinateurs.
- 2. Cliquez sur **OK**. Un nouvel onglet s'affiche dans la fenêtre principale du programme d'installation. La connexion par défaut, préalablement masquée, est à présent affichée comme connexion n° 1. Modifiez son nom avant de poursuivre.

Si vous souhaitez stocker les événements sur le concentrateur de segments, vous devez **créer une connexion correcte pour chaque ordinateur**. Lorsque vous disposez d'une connexion, le SR35i est informé, chaque fois que vous vous connectez, du PC émettant les événements qu'il doit stocker.

Procédez comme suit :

1. Dans le programme d'installation, activez l'onglet **Connexions** et cliquez sur **Nouveau**.
2. Dans l'assistant qui démarre, sélectionnez SiPass Entro – Administration du système et cliquez sur Suivant.
3. Précisez le nom de la connexion, le **SR35i**, le **numéro de licence** ainsi que le **mode de communication**.
4. Fermez l'assistant.
5. Recommencez cette procédure pour chaque ordinateur à connecter. Vous venez de créer les connexions appropriées entre les PC et le système SiPass Entro.
6. Configurez ensuite tous les paramètres requis pour chaque unité SiPass Entro.

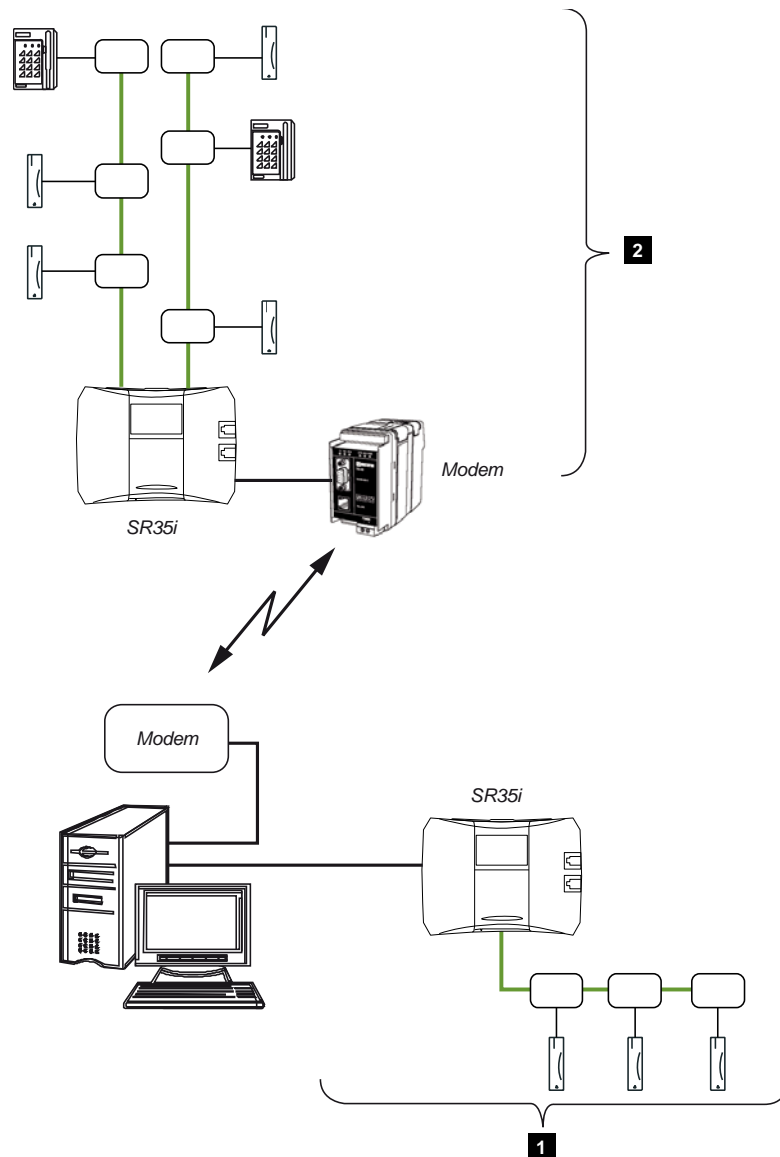


Il est également préconisé de créer des utilisateurs du système. Ceci vous confère davantage de flexibilité pour la gestion des filtres d'événements, le stockage des événements à différents emplacements et la déconnexion automatique.

11 Installation de systèmes communiquant par modem

Il est possible de contrôler jusqu'à 10 000 systèmes SiPass Entro à partir d'un même ordinateur. Pour connecter plusieurs systèmes **directement** à un PC, celui-ci doit disposer d'autant de ports de communication (COM) qu'il existe de systèmes SiPass Entro. Pour communiquer avec deux systèmes, l'un directement et l'autre par modem, un ordinateur doit posséder deux ports COM, l'un pour la connexion d'un concentrateur de segments et l'autre pour la connexion d'un modem.

L'illustration ci-dessous représente une configuration dans laquelle un PC est connecté directement avec un système SiPass Entro et par l'intermédiaire d'un modem avec un autre concentrateur.



Exemple d'un système communiquant par modem géré à partir d'un PC (en combinaison avec un système câblé)

1.	Système n°1
2.	Système n°2

11.1 Programmation d'un système équipé d'un modem TD36 (conseillé)

Nous vous recommandons vivement d'utiliser le modèle TD36 sur le site pour établir des communications par modem, car il comprend notamment la technologie Watchdog.

Si vous avez installé un modem (modèle TD36, par exemple) sur le site distant (et si son numéro de téléphone est disponible), il est inutile d'effectuer la programmation sur site. Vous pouvez connecter le SR35i au modem, activer la ligne, mais effectuer les tâches de programmation à partir de l'ordinateur hôte (même si cela prend davantage de temps). Pour plus de détails sur le transfert des informations relatives au nouveau système vers l'ordinateur central [→ 66], voir la section correspondante.

Si, toutefois, vous souhaitez programmer le modem sur site, procédez à partir de la liaison RS232, puis basculez sur le modem une fois l'opération terminée. Suivez les étapes de la procédure décrite à la section Programmation sur site d'un système communiquant par modem [→ 62].

11.2 Programmation d'un système équipé d'un modem personnalisé

Si vous utilisez un autre modem (pas le modèle TD36), vous devrez peut-être modifier la chaîne d'initialisation du modem et programmer celui-ci sur site (via RS232).

Pour pouvoir programmer le système (voir la section suivante, Programmation sur site d'un système communiquant par modem [→ 62]), connectez temporairement un ordinateur doté du logiciel SiPass Entro à l'un des concentrateurs de segments. Une fois la programmation terminée, vous pourrez déconnecter l'ordinateur et le remplacer par le modem.

N'oubliez pas de tester la boucle de communication [→ 77] et l'alimentation [→ 77].

11.3 Programmation sur site d'un système communiquant par modem

Pour programmer le nouveau système, connectez un ordinateur à un concentrateur de segments (via le port RS232) dans ce système.

1. Lancez le programme d'installation [→ 79].
2. Cliquez sur l'onglet **Nouvelle connexion**. Un assistant permettant d'établir une connexion entre le PC et le concentrateur s'affiche. Aucune information de connexion n'est demandée, car le système (la base de données) est probablement nouveau et utilisera le nom d'utilisateur et le mot de passe par défaut (respectivement "bewa" et "pass").
3. Optez pour la création d'un **nouveau système** et continuez.
4. Sélectionnez **RS232** et continuez.
⇒ Le logiciel détecte automatiquement le port COM correct.
5. Dans le champ **Nom du site**, saisissez le nom du nouveau système (par exemple, Rue de la Tour).

- ⇒ L'utilisateur pourra alors choisir ce nom parmi les systèmes disponibles dans les fenêtres de connexion de SiPass Entro.
6. Dans le champ **Nom du système**, entrez le nom du système. Ce nom doit être **unique et identique** au nom saisi pour programmer l'ordinateur principal (voir la section Transfert des informations relatives au nouveau système vers l'ordinateur central [→ 66]).
Il est **très important** de noter le nom du système quelque part. Si vous remplacez le PC, vous devrez entrer de nouveau le même nom de système.
7. Fermez l'assistant en cliquant sur **Terminer**.
⇒ A présent, la fenêtre principale du programme d'installation s'affiche.
8. Il est préférable d'effectuer les opérations de programmation (des portes, etc.) sur site, plutôt qu'ultérieurement via la connexion modem. Suivez pour ce faire les instructions du Manuel de l'utilisateur.
⇒ Maintenant que les principales tâches de programmation sont achevées, nous allons préparer la connexion au modem.
9. Dans le programme d'installation, cliquez sur l'onglet **Connexions**.
10. Cochez la case Modem ; un nouvel onglet s'affiche.
11. Saisissez le **numéro de téléphone du modem**.
12. Le champ **Chaîne d'initialisation du modem SR35i** est automatiquement rempli. La chaîne indiquée représente les instructions suivantes "command echo disabled" (écho des commandes désactivé), "autoanswer off" (réponse automatique désactivée) et "DTR disconnected" (TDP déconnecté). Vous pouvez la modifier si nécessaire.
13. Si le modem doit appeler l'ordinateur, entrez le **numéro de téléphone** à composer dans le champ correspondant.
14. Si le modem doit appeler l'ordinateur, indiquez le nom de l'**utilisateur du système** devant se charger d'appeler le PC (afin que celui-ci sache où stocker les événements). Précisez également les circonstances de l'appel :
- Au bout de : le concentrateur de segments appelle l'ordinateur dès que le nombre d'événements indiqué est atteint.
 - A chaque événement sous alarme : le concentrateur de segments appelle l'ordinateur dès qu'un événement sous alarme se produit.
 - A chaque modification de la base de données : le concentrateur de segments appelle l'ordinateur dès que la base de données est modifiée. Cela s'applique uniquement si un autre ordinateur est connecté à un autre des concentrateurs de segments du nouveau système. Un appel est effectué toutes les 15 minutes si la base a été modifiée.
15. Cliquez sur **OK**.
⇒ Vous avez à présent défini toutes les informations relatives au système.
16. Déconnectez l'ordinateur utilisé pour la programmation du système et remplacez-le par le modem [→ 65].

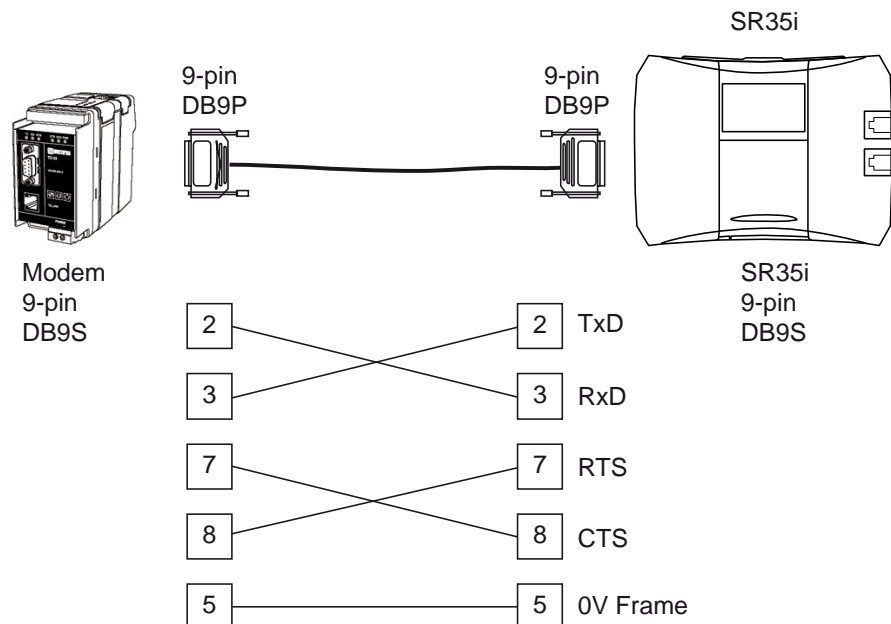


L'activation et la désactivation d'alarmes ainsi que la modification de codes individuels constituent des modifications de base de données. Ces événements déclenchent donc des appels de l'ordinateur.

Pour pouvoir recevoir des appels relatifs à des modifications de la base de données, Entroser doit être exécuté sur l'ordinateur.

11.4 Montage et configuration du modem

L'illustration ci-dessous indique comment connecter un modem au concentrateur de segments utilisé pour communiquer avec l'ordinateur.



L'installation du modem marque la fin de l'installation du système. Il ne vous reste plus qu'à transférer les informations définies pour le nouveau système vers l'ordinateur central utilisé pour la programmation des deux systèmes.

Configuration minimale requise pour le modem :

- 9 600 bit/s
- Réponse automatique désactivée (Autoanswer off)
- TDP déconnecté (DTR disconnected)
- Echo des commandes désactivé (Command echo disabled)

Recommandation :

Le modem doit intégrer la technologie Watchdog qui permet de réinitialiser le modem automatiquement en cas d'interruption de la connexion ou d'une panne de courant.



Si le modem nécessite une tension comprise entre 12 et 24 V, il peut être alimenté à partir du système. Dans ce cas, il utilisera également la batterie de secours du système.

11.5 Transfert des informations relatives au nouveau système vers l'ordinateur central

Placez-vous devant l'ordinateur utilisé pour la programmation et le contrôle des deux systèmes.

Si ce PC ne dispose pas du logiciel SiPass Entro, installez ce dernier à partir du CD.

Ensuite, **créez** sur le PC **une connexion initiale** (au modem) destinée à permettre le transfert des informations. Il vous suffira plus tard de sélectionner le système ou la connexion voulue, d'établir une connexion, puis de numéroter comme d'habitude.

1. Lancez le programme d'installation [→ 79].
 - ⇒ Notez que si aucun système n'est installé sur l'ordinateur, l'assistant démarre automatiquement sans vous inviter à établir de connexion.
2. Activez l'onglet **Nouvelle connexion** et démarrez l'assistant.
3. Sélectionnez le **système existant** et continuez.
4. Choisissez l'option modem et précisez le numéro de téléphone du modem.
 - ⇒ La connexion est à présent configurée. Vous pouvez continuer et appeler le site distant comme indiqué ci-après ou établir une connexion ultérieurement et numéroter.
5. Entrez le **Nom du site** et le **Nom du système**.

Il est très important de spécifier le même nom de système que celui indiqué au moment de l'installation du modem. Si vous remplacez le PC, vous devrez entrer de nouveau le même nom de système.
6. Fermez la fenêtre.
 - ⇒ L'assistant va désormais tenter d'établir une connexion au site distant (par numérotation). Si la connexion échoue, procédez comme suit.
7. A présent, la fenêtre principale du programme d'installation de SiPass Entro s'affiche. Le nom du système sélectionné est indiqué dans la barre de titre. Le système est HORS LIGNE car vous n'avez pas encore appelé le nouveau système.
8. Dans la barre d'outils, cliquez sur le bouton du combiné décroché, ou choisissez **Numéroter** dans le menu **Modem**. Un message apparaît pendant que le système tente d'établir une connexion.

Dès que la connexion est établie, les systèmes sont en contact direct, autrement dit, le voyant vert EN LIGNE [→ 80] est éclairé. Dès que toute l'information est transférée (cela peut demander quelques minutes) le voyant BD A JOUR [→ 80] passe également au vert.

Le nouveau système peut à présent recevoir des informations concernant les plannings, les personnes, les groupes d'accès et les portes.



Lors de la programmation d'un système contrôlé par modem, SiPass Entro doit toujours être EN LIGNE (connecté par modem). Les informations seront ainsi transférées plus rapidement et en toute sécurité.

12 Installation de la carte mémoire flash CF8

La carte mémoire CF8 stocke des fichiers de la même manière qu'un lecteur de disque dur. Cette carte est livrée avec les fichiers HTML du système de réservation.

1. Mettez hors tension l'unité SR35i matérielle.
2. Installez la carte CF8.
3. Remettez le SR35i sous tension.

Une fois que tous les autres paramètres et unités requis pour la réservation sont configurés, vous pouvez vous connecter à l'adresse IP du SR35i (<http://xxx.xxx.xxx.xxx.login.html>). La page de connexion devrait s'afficher à l'écran.

13 Installation des DVR

SiPass Entro a intégré des fonctions de contrôle d'un système DVR (enregistreur vidéo numérique) externe dans la gamme Siemens SISTORE™. Selon le produit DVR utilisé, les fonctionnalités et les paramètres disponibles varient.

Cette section décrit les paramètres à définir dans les différents modèles SISTORE™ et les précautions supplémentaires à prendre pour les activer dans l'environnement SiPass Entro.



Pour tous les modèles, il est recommandé d'imprimer la documentation disponible sur le CD (fourni avec le DVR) avant de procéder à toute opération de configuration.

13.1 Conditions préalables requises

Nous supposons que le système DVR est installé et documenté conformément aux manuels qui l'accompagnent et qu'il a été configuré à des fins de communication avec le système SiPass Entro. Par exemple, l'environnement du réseau local (LAN) doit permettre la communication entre les unités.

En général, le système DVR dispose d'une interface utilisateur (un logiciel PC) permettant de configurer les paramètres initiaux. Sur certains modèles, la configuration s'effectue à partir du panneau avant du DVR.

	AVIS
	<p>Pensez à toujours vérifier le nombre de caméras utilisées, la vitesse de défilement des images, la résolution et la taille des disques durs disponibles sur les DVR avant de configurer les commandes d'enregistrement ininterrompu ou déclenché dans l'application.</p> <p>A défaut, vous risquez de perdre des données si la mémoire d'enregistrement vient à saturer.</p>

Logiciel de visualisation du DVR

Vous devez également avoir installé le logiciel de visualisation compatible avec des modèles de DVR spécifiques. Plusieurs logiciels peuvent coexister sur un même PC.

Bien évidemment, si ce logiciel **n'est pas** installé, SiPass Entro ne pourra pas afficher les images du DVR en cours d'utilisation. (SiPass Entro demandera à l'utilisateur d'installer le logiciel).

En règle générale, le logiciel de visualisation est fourni avec le DVR. Si tel n'est pas le cas, contactez votre fournisseur SISTORE™.

Synchronisation des horloges

SiPass Entro et le DVR disposent tous deux de leurs propres fonctions d'horloge calendrier. Assurez-vous que ces horloges sont synchronisées afin de garantir que les événements et les images affichent le même horodatage.

La meilleure solution consiste à laisser les deux systèmes mettre à jour leur horloge à partir de la même source (généralement un serveur NTP). Le SR35i peut également faire office de serveur pour les différents systèmes d'enregistrement SISTORE™.

Le concentrateur de segments SR35i peut être configuré en conséquence. Voir la section Gestion avancée de l'horloge système [→ 83].

Le DVR est configuré conformément au manuel d'instructions qui l'accompagne.

13.2 Connexion du DVR

Lorsque le DVR SISTORE™ est installé et programmé, vous devez configurer certains paramètres du logiciel SiPass Entro pour permettre la communication avec le DVR.

La communication entre le DVR et SiPass Entro est assurée au moyen d'une liaison TCP/IP. Dans SiPass Entro, il est nécessaire de créer une "connexion" pour chaque DVR.



Sur un système utilisant un seul PC, l'onglet Connexions n'est pas directement visible. Vous devez activer l'onglet **Système > Propriétés système > Connexions** et configurer SiPass Entro pour qu'il fonctionne avec plusieurs connexions (comme un DVR).

Procédez comme suit :

1. Lancez le programme d'installation [→ 79].
2. Cliquez sur l'onglet **Connexions**. S'il n'est pas visible, consultez la remarque ci-dessus.
3. Cliquez sur **Nouveau** et sélectionnez **DVR SISTORE** dans l'assistant.
4. Renseignez le champ **Nom** du DVR.
5. Sélectionnez le **SR35i** à utiliser.
6. Dans la zone de liste, choisissez **Type du DVR**. Ce choix permettra également de configurer implicitement la base de données SiPass Entro de sorte qu'elle utilise les **ports réseau par défaut** du DVR.
7. Renseignez les champs **Nom d'utilisateur** et **Mot de passe**.
8. Cliquez sur **OK**.
9. Recommencez les étapes ci-dessus pour chaque DVR.

13.3 Contrôle des enregistrements

Il existe différentes manières de lancer des enregistrements à partir de SiPass Entro.

- Déclenchement par un événement au cours des plages horaires
- Enregistrement ininterrompu par tranche horaire
- Enregistrement manuel (démarré à partir de l'application de contrôle des événements et de l'accès aux portes).

Déclenchement par un événement au cours des plages horaires

Différents événements survenant dans SiPass Entro peuvent déclencher l'enregistrement et le stockage automatiques des images sur l'unité DVR (aucun enregistrement étant stocké sur le PC).

Ainsi, une alerte de porte peut lancer un enregistrement de nuit en créant simplement un planning SiPass Entro pertinent et en liant une **plage horaire** (comme, par exemple, *Autre horaire*) aux paramètres de filtre avec les durées

d'enregistrements antérieur et postérieur (c.-à-d., durée de l'enregistrement avant et après l'événement).

Enregistrement ininterrompu par tranche horaire

Vous avez la possibilité d'utiliser un planning SiPass Entro pour contrôler un enregistrement ininterrompu depuis une caméra, mais cela risque de générer des fichiers volumineux sur le DVR.

13.4 Paramètres de la caméra

Dès qu'un DVR est configuré dans le programme d'installation, un nouvel onglet intitulé Caméras s'affiche, permettant de configurer les différentes caméras utilisées. Procédez comme suit :

1. Activez l'onglet **Caméras** (dans le programme d'installation).
Toutes les caméras non configurées dans la base de données s'affichent sous ****<NOMDVR>:<INDEXCAMERA>**. L'affichage de la liste peut prendre un certain temps.
2. Sélectionnez une caméra et cliquez sur **Modifier**. Une autre solution consiste à cliquer sur **Nouveau** afin d'ajouter une caméra manuellement.
3. Modifiez le contenu du champ **Nom** de la caméra. Le DVR stockant les images et le numéro d'index est généralement défini par le logiciel.
Si, toutefois, la caméra a été ajoutée manuellement, vous devez définir ces paramètres.
4. Sélectionnez (ou créez) un **planning** pour cette caméra. Il peut s'agir de n'importe quel planning défini dans SiPass Entro.
5. Deux critères de départ principaux sont ensuite possibles.



Par défaut, les paramètres configurés sur le DVR lui-même sont appliqués aux enregistrements. Il s'agit généralement de la vitesse de défilement des images et de la résolution, mais aussi des valeurs de durée des enregistrements antérieur et postérieur.

Selon le DVR en cours d'utilisation, le logiciel SiPass Entro permet de contrôler différents paramètres du DVR. Pour plus de détails sur la définition des valeurs, reportez-vous au tableau ci-dessous.

Valeur à définir	AX	MX	CX
Valeur d'enregistrement antérieur	Identique sur le DVR et dans SiPass Entro	Dans SiPass Entro	Uniquement sur le DVR (voir SISTORE CX [→ 75])
Valeur d'enregistrement postérieur	Dans SiPass Entro	Dans SiPass Entro	Uniquement sur le DVR (voir SISTORE CX [→ 75])

1. Si, à un moment donné, vous utilisez le mode d'enregistrement **ininterrompu**, choisissez les plages horaires pendant lesquelles l'enregistrement de la caméra aura lieu. Utilisez cette fonction avec précaution, car elle peut générer des fichiers extrêmement volumineux sur le disque dur du DVR.
2. **Déclenchement filtré.** Cliquez sur les onglets Jeu d'enregistrements 1 et/ou Jeu d'enregistrements 2, puis procédez comme suit :

- Sélectionnez (ou créez) un filtre d'événements à déclencher et lancez l'enregistrement de la caméra. Par défaut, tous les types d'événements et toutes les portes sont désactivés. Indiquez les événements voulus sous le premier onglet et les portes à activer sous le second.
 - Sélectionnez les plages horaires pendant lesquelles vous souhaitez contrôler les événements (à l'aide du filtre).
 - Configurez différentes durées d'enregistrement antérieur et d'enregistrement postérieur pour chacun d'entre eux. Vous remarquerez que les possibilités de modification de ces paramètres varient en fonction du modèle utilisé.
De cette manière, vous pouvez par exemple disposer d'un jeu d'enregistrements très brefs et d'un autre jeu aux durées d'enregistrements nettement plus longues.
3. Cliquez sur **OK** et recommencez cette procédure pour chaque caméra.
 4. Si vous souhaitez apporter une quelconque modification à ces configurations, il vous suffit de cliquer sur Modifier.
- ⇒ Vous venez de configurer les paramètres requis pour le transfert d'images du DVR vers SiPass Entro à des fins de visualisation.

13.5 SISTORE™ MX

Il est nécessaire d'effectuer quelques étapes préalables via le logiciel SISTORE™ MX avant de pouvoir établir des communications avec le logiciel SiPass Entro.

En général, vous installez la suite logicielle MX complète afin de pouvoir à la fois contrôler et afficher les paramètres détaillés du DVR MX. Il est néanmoins possible d'installer uniquement le module RemoteView afin d'afficher les enregistrements à partir de SiPass Entro.

Nous vous recommandons d'installer le logiciel MX sur le lecteur C.

13.5.1 Paramètres MX

Vous devez confirmer (ou reconfigurer) l'utilisation des paramètres suivants dans le type de DVR MX et en prendre note :

Paramètres	Valeur par défaut	Valeur utilisateur facultative	Commentaire
Nom d'utilisateur :	Administrator		Paramètre Entro
Mot de passe :	Administrator		Paramètre Entro
Adresse IP	<Non définis>		Paramètre Entro
Port *)	40	N/D	<Valeur fixe dans Entro>
Port SR <-> DVR *)	8080	N/D	<Valeur fixe dans Entro>
Plage des n° de ports	1100 - 1109	N/D	<Valeur fixe dans Entro>
N° et noms des caméras	<Non définis>		Paramètre Entro
*) Si le DVR est installé derrière un routeur, le routage de port doit être configuré. Veuillez vous renseigner auprès du responsable informatique.			



Il est recommandé de nommer de la même manière les caméras sur le DVR et dans l'environnement SiPass Entro. A défaut, le nom affiché à l'écran risque de différer de celui figurant dans le journal d'événements de SiPass Entro.

Une fois les paramètres configurés, indiquez-les dans le **programme d'installation** de SiPass Entro lors de la création de connexions et de caméras.

13.5.2 Logiciel de visualisation en temps réel de MX

Si vous souhaitez simplement effectuer des opérations de visualisation de base à partir de SiPass Entro, il vous suffit d'installer le module RemoteView sur le PC sur lequel SiPass Entro est installé. Sinon, aucun affichage ne sera possible.

13.5.3 Autres points à prendre en compte concernant le MX

Configurez les paramètres suivants sur le MX :

- Dans les paramètres de configuration, le "déclencheur logiciel" doit être activé pour permettre le lancement de l'enregistrement. Notez que vous devez procéder à cette opération sur le MX (l'activation ne peut se faire à distance).
- Vous devez activer le paramètre Enregistrement ininterrompu, ce qui peut **uniquement** se faire à partir du MX.

13.6 SISTORE™ AX

13.6.1 Généralités

Lors de l'intégration de la gamme de DVR SISTORE™ AX dans SiPass Entro, un certain nombre de paramètres doivent être configurés sur l'enregistreur vidéo numérique pour permettre le fonctionnement correct de ce dernier.

- Il est recommandé de ne pas utiliser le paramètre Enregistrement ininterrompu de SiPass Entro, celui-ci pouvant interférer avec l'enregistrement des événements.
- Si vous souhaitez utiliser un moniteur VGA pour afficher les menus (et les images), vérifiez que le commutateur de sélection situé à l'arrière est réglé sur VGA.
- La sortie vidéo VGA n'est pas disponible pour tous les modèles AX. Seuls certains modèles en disposent.
- Installez également le **logiciel PC** fourni pour pouvoir contrôler l'AX à distance sur le PC sur lequel SiPass Entro est installé. A défaut, aucun affichage ne sera possible.
- Bien que les commandes logicielles AX Admin, AX Watch et AX Search soient disponibles sur le PC, utilisez-les avec précaution lorsque l'application SiPass Entro est en cours d'exécution.
- Dans les versions 3.5 et supérieures du logiciel RAS, les applications AX Admin, AX Watch, AX Search distinctes sont intégrées dans une même interface utilisateur. La version 3.5 de RAS a des exigences supérieures au niveau des performances (reportez-vous à la documentation fournie avec le DVR). Les versions précédentes de RAS ne sont plus prises en charge.

13.6.2 AX9 et AX16

Un planning doit être créé avec les caractéristiques suivantes :

- Day: All
- Range: 00:00 - 24:00
- Mode: Event
- Channels: All connected cameras.

Assurez-vous d'activer l'option "Schedule on" dans le menu "Recording".

13.6.3 AX4 et AX Lite

- L'option "Quick setup" doit être désactivée.
- L'option "Time-Lapse Recording" doit être définie sur "Off".

13.6.4 Paramètres AX

Vous devez confirmer (ou reconfigurer) l'utilisation des paramètres suivants dans le type de DVR AX et en prendre note.

Il est possible d'utiliser les boutons du panneau avant de l'AX pour configurer les paramètres de base (les paramètres IP, par exemple) d'après le guide de prise en main d'AX (AX Quick start guide). Une fois la connexion LAN établie avec l'AX, vous avez la possibilité de configurer les paramètres à partir du PC.

Paramètres	Valeur par défaut	Valeur utilisateur facultative	Commentaire
Nom d'utilisateur :	<Non définis>		Paramètre Entro
Mot de passe :	12345678		Paramètre Entro
Adresse IP	192.168.1.129		Paramètre Entro
Passerelle	192.168.1.254.		Paramètre Entro
Masque de sous-réseau	255.255.255.0		Paramètre Entro
Port : SR <-> DVR *)	17655	N/D	<Valeur fixe dans Entro>
Port : Watch *)	8016	N/D	<Valeur fixe dans Entro>
Port : Admin	8200	N/D	<Valeur fixe dans Entro>
Port : Search	10016	N/D	<Valeur fixe dans Entro>
Port : Callback	8201	N/D	<Valeur fixe dans Entro>
N° et noms des caméras	<Non définis>		Paramètre Entro
*) Si le DVR est installé derrière un routeur, le routage de port doit être configuré. Veuillez vous renseigner auprès du responsable informatique.			

Le tableau s'applique aux périphériques AX suivants :

- SISTORE AX4 Lite
- SISTORE AX4 160/100
- SISTORE AX9/AX16 250/50

Le modèle SISTORE AX9/AX16 250/200 faisant appel à une méthode d'authentification utilisateur avancée, la saisie d'un nom d'utilisateur est obligatoire pour s'authentifier sur le périphérique (ceci s'applique également aux versions ultérieures SISTORE AX8/AX16 250/100). Un compte par défaut est défini sur le périphérique (nom d'utilisateur "admin", aucun mot de passe).



Il est recommandé de nommer de la même manière les caméras sur le DVR et dans l'environnement SiPass Entro. A défaut, le nom affiché à l'écran risque de différer de celui figurant dans le journal d'événements de SiPass Entro.

13.6.5 Autres points à prendre en compte concernant l'AX

Configurez les paramètres suivants sur l'AX4 Lite, AX4 160/100 et AX9/AX16 250/50 :

- Aucune configuration d'enregistrement ne doit figurer dans les paramètres de l'enregistrement à intervalles.
- AX9/AX16 250/50 : le bouton d'enregistrement doit être activé sur le périphérique AX.

Configurez les paramètres suivants sur l'AX9/AX16 250/200 :

- Dans l'écran de définition d'un planning ("Schedule"), définissez événement comme mode d'enregistrement ("Event").

Configurez les paramètres suivants sur l'AX16 :

- Le bouton d'enregistrement doit être activé.

- Dans les paramètres réseau, activez l'option de contrôle du transfert ("Transfer Control").

Une fois les paramètres configurés, indiquez-les dans le programme d'installation de SiPass Entro lors de la création de connexions et de caméras.

13.6.6 Logiciel de visualisation en temps réel d'AX

Le logiciel de contrôle à distance AX Watch ne permet d'afficher **qu'une seule fenêtre d'affichage en temps réel à la fois**.

Autrement dit, si SiPass Entro présente un affichage dans le programme d'installation pendant la configuration d'une caméra, vous ne pouvez pas visualiser en même temps une image du contrôle de l'accès aux portes en cliquant sur une icône de caméra.

Dans les versions 3.5 et supérieures du logiciel RAS, les applications AX Admin, AX Watch, AX Search distinctes sont intégrées dans une même interface utilisateur.

13.7 SISTORE™ CX

13.7.1 Généralités

Le modèle CX fait appel à un module de logiciel PC pour les opérations de configuration et de visualisation. Pour plus de détails à ce sujet, reportez-vous au manuel Quick setup ou DVR Configuration manual.

Nous vous recommandons d'installer le logiciel SX-CX sur le lecteur C.

Vous remarquerez que le CX comprend une "page d'accueil" intégrée que vous pouvez parcourir à la recherche d'informations complémentaires sur l'unité. Dès que la liste des périphériques est configurée, vous pouvez établir une connexion.

13.7.2 Paramètres CX

Le DVR ne comporte pas de boutons sur le panneau avant pour reconfigurer, entre autres, ses paramètres réseau localement. Par conséquent, il est recommandé d'utiliser d'abord un PC sur lequel le logiciel SX-CX-Config est installé (sans aucune autre connexion réseau), puis de brancher les câbles réseau sur le DVR uniquement.

Après avoir suivi les instructions du manuel du DVR, vous pouvez confirmer (ou reconfigurer) l'utilisation des paramètres suivants dans le type de DVR CX à l'aide du programme **SX-CX Config** :

Paramètres	Valeur par défaut	Valeur utilisateur facultative	Commentaire
Nom d'utilisateur :	admin		Paramètre Entro
Mot de passe :	admin		Paramètre Entro
Adresse IP	169.254.16.9		Paramètre Entro
Masque de sous-réseau	255.255.0.0		Paramètre Entro
Passerelle	0.0.0.0		Paramètre Entro
Port *)	12050	N/D	<Valeur fixe dans Entro>
Port SR <-> DVR *)	12050	N/D	<Valeur fixe dans Entro>
N° et noms des caméras	<Non définis>		Paramètre Entro

*) Si le DVR est installé derrière un routeur, le routage de port doit être configuré. Veuillez vous

Paramètres	Valeur par défaut	Valeur utilisateur facultative	Commentaire
renseigner auprès du responsable informatique.			



Il est recommandé de nommer de la même manière les caméras sur le DVR et dans l'environnement SiPass Entro. A défaut, le nom affiché à l'écran risque de différer de celui figurant dans le journal d'événements de SiPass Entro.

Une fois les paramètres configurés, indiquez-les dans le programme d'installation de SiPass Entro lors de la création de connexions et de caméras.

13.7.3 Logiciel de visualisation en temps réel de CX

Le logiciel de visualisation à distance, actuellement nommé **SX-CX Client**, du DVR doit être installé sur le PC sur lequel SiPass Entro est installé. A défaut, aucun affichage ne sera possible.

13.7.4 Autres points à prendre en compte concernant le CX

Pour bénéficier des fonctionnalités d'enregistrements antérieur et postérieur sur le DVR, vérifiez que les règles (standard) IVM sont activées.

14 Remarques préliminaires à la configuration du système

Avant d'activer le système SiPass Entro, il est recommandé à l'installateur de consulter la liste de vérification [→ 78].

14.1 Vérification des boucles de communication

Vérifiez que toutes les unités du système communiquent.

Une fois toutes les unités connectées (tous **les borniers amovibles étant déconnectés** dans les boîtiers de raccordement et sur les centraux de porte), vous devez vérifier la résistance des boucles de communication globale et locale sur les bornes 3 et 4 des borniers, les centraux de porte et les concentrateurs de segments. Elle doit s'élever à $60\ \Omega$ (ohm), plus la résistance du câble.

- Si la résistance totale est de $120\ \Omega$, il manque une résistance de terminaison. Si elle est bien inférieure à $60\ \Omega$, il y a un court-circuit dans la boucle de communication.
- Si la résistance est largement supérieure à $120\ \Omega$ (boucle infinie), il y a une interruption dans la boucle ou aucune des extrémités ne comporte de terminaison.

En environnement réseau, assurez-vous que tous les câbles du réseau local sont connectés correctement.

14.2 Vérification de l'alimentation

Montez le bloc d'alimentation. Vérifiez que la tension correspond approximativement à celle de la sortie du bloc d'alimentation et assurez-vous que la position des pôles + et - est correcte.

N'oubliez pas qu'une chute de tension (entre les potentiels maximum et minimum) supérieure à 5 V entre les unités peut affecter la qualité de la communication RS485.

15 Liste de vérification

La liste de vérification ci-dessous est destinée à faciliter l'installation de SiPass Entro et permet d'assurer le bon déroulement de la mise en place du système. Pour tout renseignement complémentaire, n'hésitez pas à prendre contact avec le support technique.

Le système d'exploitation de l'ordinateur connecté au système est :	<input type="checkbox"/> XP <input type="checkbox"/> Vista <input type="checkbox"/> Terminal Server 2008 <input type="checkbox"/> Terminal Server 2003 <input type="checkbox"/> Windows 7 <input type="checkbox"/> Windows 8
Dans le cas d'une connexion par câble RS232, le PC du système dispose-t-il de ports COM série (connecteur 9/25 broches) ?	<input type="checkbox"/> Oui
La prise murale (RS232) se trouve à proximité de l'ordinateur et est connectée à un SR35i approprié. De plus, la distance totale entre l'ordinateur et le SR35i est inférieure à 25 mètres.	<input type="checkbox"/> Oui
Dans le cas d'une connexion en réseau local, le PC est-il connecté correctement ?	<input type="checkbox"/> Oui
Les SR35i sont-ils dotés d'adresses IP correctes (validées par le responsable informatique) ?	<input type="checkbox"/> Oui
Les paramètres de toutes les ressources réseau (routeurs, pare-feux, etc.) ont-ils été définis correctement ?	<input type="checkbox"/> Oui
Tous les concentrateurs de segments, lecteurs et centraux de porte connectés comportent des adresses appropriées.	<input type="checkbox"/> Oui
Le lecteur est-il connecté au bornier correct dans le DC22/DC12 et le cordon électrique est-il correctement branché ?	<input type="checkbox"/> Oui
Chaque boucle de communication RS485 se termine par une résistance de 120-ohm.	<input type="checkbox"/> Oui
La résistance de toutes les boucles de communication est-elle conforme aux normes recommandées dans le manuel ?	<input type="checkbox"/> Oui
Le blindage de chaque boucle est relié à la terre en un seul point ?	<input type="checkbox"/> Oui
La disposition du boîtier et la longueur des câbles d'alimentation sont-elles correctes ?	<input type="checkbox"/> Oui
En cas d'utilisation de la réservation : est-ce qu'au moins une carte CF8 est installée dans un SR35i ?	<input type="checkbox"/> Oui
L'heure et la date sont-elles correctes lorsque le système est en ligne ?	<input type="checkbox"/> Oui
Si un DVR est installé : celui-ci est-il correctement configuré ?	<input type="checkbox"/> Oui

16 Démarrage du logiciel

La première fois que vous démarrez le logiciel SiPass Entro, vous êtes invité à créer un utilisateur du système, puis à vous reconnecter afin de pouvoir stocker des événements.

1. Dans le menu **Démarrer** de Windows, **Programmes** > SiPass Entro.
2. Choisissez l'une des trois applications : le **programme d'installation**, **Entro** ou le **programme de contrôle de l'accès aux portes**.
⇒ La fenêtre de connexion apparaît.



3. Entrez un nom d'utilisateur dans le champ **Utilisateur** (le nom par défaut est : bewa).
4. Entrez un mot de passe dans le champ **Mot de passe** (le mot de passe par défaut est : pass).
5. S'il existe plusieurs systèmes, sélectionnez le système de votre choix.
⇒ Si vous en possédez plus de 20, un champ de recherche supplémentaire s'affichera.
6. Tapez un caractère.
⇒ Le système recherche tous les noms le contenant.
7. Cliquez sur **OK**.
⇒ A présent, la fenêtre principale de SiPass Entro s'affiche.

Démarrage des applications à partir des icônes

Vous pouvez démarrer rapidement une application Entro à partir de son icône. Procédez comme suit :

1. Placez le curseur sur les icônes et cliquez avec le bouton droit de la souris.
⇒ Un menu apparaît.
2. Choisissez SiPass Entro ou Contrôle de l'accès aux portes.
⇒ L'application choisie démarre.
⇒ Notez que pour démarrer le programme d'installation, vous devez passer par le menu Démarrer de Windows.

16.1 Voyants indiquant l'état de la communication

Voyants dans les fenêtres de l'application

Vous trouverez dans le coin inférieur droit de l'écran deux voyants :



Lorsque la mention EN LIGNE apparaît précédée du voyant vert, l'ordinateur et l'application SiPass Entro sont connectés au système de contrôle d'accès.

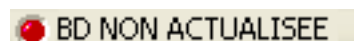


Lorsque la mention HORS LIGNE apparaît précédée du voyant rouge, SiPass Entro ne reçoit aucune information des lecteurs ni des concentrateurs. Les informations enregistrées sur l'ordinateur ne sont pas transmises aux concentrateurs de segments.



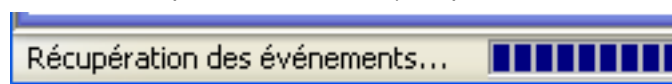
Lorsque la mention BD A JOUR apparaît précédée du voyant vert, les informations enregistrées sur l'ordinateur ont été transmises au concentrateur de segments auquel il est connecté.

Il convient de souligner que certaines opérations (telles que la mise à niveau ou l'importation d'un grand nombre de personnes) peuvent engendrer un retard de transmission de l'information entre le "premier" concentrateur et le suivant. Consultez les informations affichées sur chaque SR35i pour vous assurer de disposer des informations d'état correctes.



Lorsque la mention BD NON ACTUALISEE apparaît précédée du voyant rouge, les informations disponibles sur l'ordinateur et les concentrateurs de segments divergent. Notez que la transmission de l'ensemble des données de l'ordinateur aux concentrateurs de segments peut s'effectuer assez lentement. En outre, pour que l'opération aboutisse, le système doit être EN LIGNE.

Vous pouvez également consulter la barre d'état pour visualiser la progression de la transmission des données vers l'ordinateur. Ce sont généralement des événements qui sont transférés (lorsque le PC a été mis HORS LIGNE).



Par défaut, vous serez automatiquement déconnecté(e) du système si aucune tâche n'a été effectuée pendant 15 minutes. L'application Entro vous permet de désactiver l'option de déconnexion automatique ou de définir la période (en minutes) précédant la déconnexion.

Voyants dans la barre d'outils de Microsoft Windows

Le symbole suivant peut également s'afficher dans le coin inférieur droit de l'écran :



Icône Entro dans la zone de notification de Windows

Lorsqu'elle apparaît, cette icône indique qu'une application appelée Entroser (communication série SiPass Entro) est exécutée à l'arrière-plan. Cette application est requise pour pouvoir afficher des événements sur l'écran du PC et/ou pour les stocker sur le disque dur. Entroser reste actif même lorsque vous quittez les applications SiPass Entro.

Malgré son nom Entroser, cette application est également utilisée pour la communication TCP/IP.

Fermeture de l'application et arrêt de la communication

Il peut arriver qu'un arrêt total de l'application SiPass Entro s'avère nécessaire, par exemple pour procéder à des opérations de maintenance telles qu'une mise à niveau. Procédez comme suit :

1. Placez le curseur sur les icônes et cliquez avec le bouton droit de la souris.
⇒ Un menu apparaît.
2. Sélectionnez **Annuler**.
⇒ Toute communication (entroser) est interrompue et la base de données actuelle est stockée. Les icônes disparaissent de la barre des tâches. Aucun événement n'est stocké.



Pour voir l'icône de notification sous **Windows 7**, cliquez dans la zone de notification avec le bouton droit de la souris et sélectionnez **Personnaliser les icônes de notification**. Sélectionnez l'entrée Entro et affectez-lui l'option **Afficher l'icône et les notifications** dans la liste déroulante.

17 Définition de l'heure et de la date

Avant d'entreprendre le processus de programmation, il est recommandé de définir l'heure et la date correctes. L'horloge est affichée séparément dans le coin inférieur droit de la fenêtre.

Il est impossible de régler l'horloge manuellement si l'un des SR35i utilise TCP/IP pour lire l'heure sur un serveur horaire externe SNTP. Voir la section Gestion avancée de l'horloge système [→ 83].

Procédez comme suit, si la configuration du système vous permet de modifier l'horloge système :

1. Vérifiez que les voyants lumineux EN LIGNE et BD A JOUR situés dans le coin inférieur droit des fenêtres de SiPass Entro sont allumés.
2. Ouvrez le programme d'installation ou Entro [→ 79].
3. Choisissez les options de menu **Système > Heure système Bewator Entro**.
4. Vérifiez la date et l'heure affichées et corrigez-les si nécessaire à l'aide des champs **Nouvelle date** et **Nouvelle heure**.
5. Pour désactiver l'observation automatique de l'heure d'été, désactivez l'option **Ajuster l'horloge pour l'observation automatique de l'heure d'été**.
6. Cliquez sur **OK**.

18 Gestion avancée de l'horloge système

La procédure suivante s'applique uniquement aux utilisateurs souhaitant définir l'heure de SiPass Entro de manière externe et ajuster l'heure de chaque concentrateur SR35i en fonction de l'heure internationale (GMT).

SiPass Entro utilise le protocole SNTP (Simple Network Time Protocol, protocole de diffusion du temps en réseau) pour obtenir l'**heure internationale (GMT)** à partir d'un processus SNTP externe, exécuté sur un serveur externe (en réseau local LAN ou sur Internet) ou interne (SR35i). Lorsque les SR35i sont connectés en réseau (via TCP/IP), SNTP est requis. En cas de doute, consultez le responsable informatique.

Lorsqu'il est utilisé en environnement réseau, le SR35i doit être en mesure de lire l'heure sur un serveur horaire (via TCP/IP). Cette possibilité, qui requiert que le concentrateur soit doté d'une fonction **proxy**, garantit que le système dispose toujours de l'heure correcte et ce, quel que soit l'endroit où le SR35i est installé.

Lorsque vous programmez le SR35i en tant que proxy, vous êtes invité à désigner le serveur horaire. Vous pouvez indiquer s'il s'agit d'un serveur interne ou externe. Cela dit, lorsque le système SiPass Entro est exécuté sur **plusieurs sous-réseaux** connectés via Internet, l'utilisation d'un serveur horaire externe est préconisée.

Si la fonction de serveur horaire réside sur un sous-réseau différent, le port 123 doit être ouvert sur le routeur.

Le menu **Système > Heure système Bewator Entro** du programme d'installation met à votre disposition un certain nombre d'options permettant de définir l'heure système. Procédez comme suit :

1. Vérifiez que les voyants lumineux EN LIGNE et BD A JOUR [→ 80] situés dans le coin inférieur droit des fenêtres de SiPass Entro sont allumés.
2. Cliquez sur **Propriétés spéciales**.
3. Sélectionnez un type de serveur horaire :
 - Serveur horaire interne (SR35i, par ex.) : sélectionnez un concentrateur.
 - Serveur horaire externe (Internet, par ex.) : entrez une adresse IP.
4. Précisez si vous souhaitez ajuster l'heure des concentrateurs SR35i en fonction de l'heure internationale (GMT).
5. Si vous choisissez cette option, chaque concentrateur de segments affiche un nouvel onglet **Heure**, indiquant la valeur de décalage choisie (+1, +2, etc.).
6. Fermez la fenêtre.
7. Dans le menu **Système > Heure système Bewator Entro**, vérifiez si l'option **Ajuster l'horloge pour l'observation automatique de l'heure d'été** est sélectionnée.

19 Personnalisation des paramètres d'Entro

19.1 Paramètres de lecteurs de carte

Si d'autres cartes que celles de SiPass Entro sont utilisées et si elles sont lues différemment, vous devez modifier les paramètres de lecteurs de carte.

1. Lancez le programme d'installation [→ 79].
2. Choisissez les options de menu **Système > Propriétés du système**.
3. Cliquez sur l'onglet **Paramètres de lecteurs de carte**.
4. Définissez le type de carte d'accès à utiliser sur le système.
 - Norme SiPass Entro : le système lit la piste ISO 2, ainsi que les positions comprises entre 9 et 16 sur la piste magnétique, ou les huit dernières positions si leur nombre est inférieur à 16 (paramètres de carte standard de SiPass Entro).
 - Pour utiliser d'autres types de cartes que le système doit lire différemment, cliquez sur **Personnalisées**. Veuillez ensuite indiquer la position de départ pour la lecture de la piste magnétique et le nombre de chiffres à prendre en compte (16 max.). Il se peut que certains anciens types de lecteurs soient uniquement en mesure de lire 8 chiffres. Veuillez contacter Siemens AB, Security Products en cas de doute à ce sujet.
5. Sélectionnez la manière dont vous souhaitez présenter les chiffres dans SiPass Entro.

19.2 Code personnel sans carte

En principe, le code personnel s'utilise conjointement avec une carte (niveau de sécurité Carte + code individuel). Toutefois, SiPass Entro permet à chaque utilisateur de remplacer ce niveau de sécurité par un seul code personnel. Notez que cette fonction désactive l'utilisation du code de groupe. Il est cependant possible d'activer ou de désactiver les zones sous alarme bistable à l'aide de ce code (qui bénéficie d'une priorité plus élevée que le niveau de sécurité Carte uniquement).

Pour activer cette fonction, procédez comme suit :

1. Lancez le programme d'installation [→ 79].
2. Choisissez les options de menu **Système > Propriétés du système**.
3. Cliquez sur l'onglet **Code personnel**.
4. Activez l'option Autoriser l'utilisation du code personnel sans la carte.
5. Entrez le nombre de chiffres (entre 4 et 8) qui devront composer le code personnel. Tout utilisateur choisissant le niveau de sécurité Code personnel sans carte devra choisir un code composé du nombre de chiffres précisé dans ce champ.
6. Cliquez sur **OK**.

19.3 Modification de la fonction du voyant rouge sur les lecteurs

Par défaut, le voyant rouge est utilisé pour indiquer si une zone sous alarme est active ; il s'allume sur les lecteurs membres de la zone sous alarme dès que le système d'alarme est chargé.

Pour désactiver cette fonction et affecter le voyant rouge au verrouillage de la porte, veuillez procéder comme suit :

1. Lancez le programme d'installation [→ 79].
2. Choisissez les options de menu **Système > Propriétés du système**.
3. Cliquez sur l'onglet **Voyant rouge du lecteur**.
4. Cochez la case Affecter le voyant rouge au verrouillage de la porte.
5. Cliquez sur **OK**.



Ce paramètre est appliqué à l'ensemble des lecteurs du système utilisant une connexion BC-Link ou RS485 (et non aux lecteurs de type Clock&Data). Lorsque cette case est cochée, il est impossible de contrôler l'état du système d'alarme. Si vous utilisez des zones sous alarme, il est conseillé de ne pas cocher cette case.

19.4 Code d'agression

Lorsqu'elle est activée, la fonction Alarme agression permet à une personne, sous la contrainte, de déverrouiller l'accès aux locaux par l'entrée d'un code spécial. Ce code envoie un signal d'alarme à un transmetteur connecté. Par défaut, cette fonction est désactivée dans SiPass Entro.

Pour activer cette fonction, procédez comme suit :

1. Ouvrez l'application Entro [→ 79].
2. Choisissez les options de menu **Système > Propriétés du système**.
3. Activez l'option **Utiliser l'alarme**.
⇒ Un message d'avertissement s'affiche.
4. Cliquez sur **Oui** pour activer cette fonction.

20 Programmation de noms pour les concentrateurs de segments

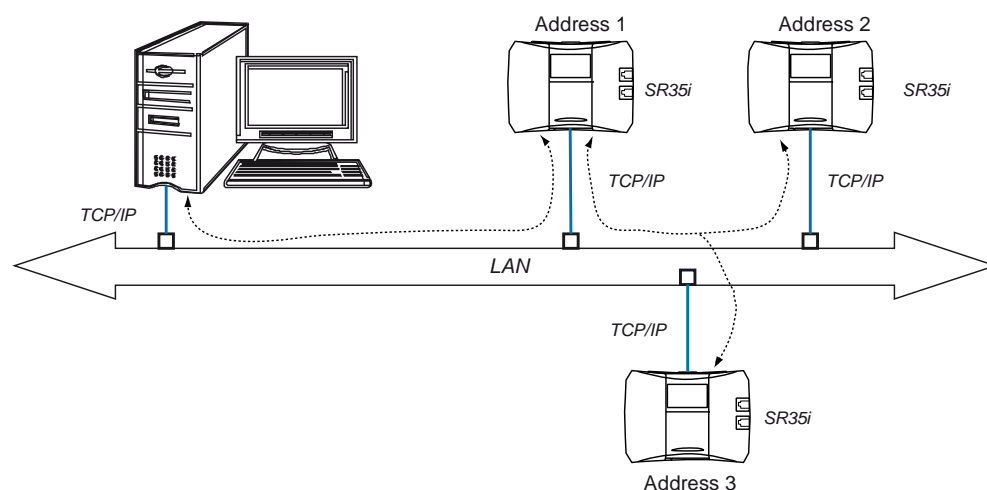
La configuration des paramètres varie en fonction du mode de communication choisi pour les SR35i.

N'oubliez pas que les paramètres de base (tels que l'adresse IP) peuvent être initialement définis à partir du clavier intégré à chaque concentrateur SR35i. Ceci permet de remplir les conditions requises pour la communication avec le PC. La définition des autres paramètres s'effectue dans le programme d'installation.

Si vous envisagez d'utiliser l'adressage IP dynamique pour les concentrateurs de segments, lisez les informations relatives à la préparation du réseau [→ 51].

Si vous prévoyez d'utiliser un modem, reportez-vous à la section Installation de systèmes communiquant par modem [→ 61] pour plus d'informations.

20.1 Création de plusieurs SR35i pour la communication TCP/IP



Dans ce cas, trois méthodes de configuration des concentrateurs de segments SR35i sont possibles.

Programmation via RS232

Un PC est connecté à chaque concentrateur SR35i via une connexion RS232. Cette information est transmise directement à chaque SR35i.

Cette méthode est préconisée lorsque les concentrateurs de segments sont placés dans différentes zones géographiques. Il est important que ceux-ci soient également dotés d'une adresse IP, d'un nom de système et d'une clé de cryptage corrects.

Chaque SR35i nouvellement créé est nommé ****Cx**. Définissez l'**adresse IP**, la fonction **proxy** et les autres paramètres requis pour les concentrateurs en suivant les étapes de la procédure décrite à la section Programmation des concentrateurs SR35i [→ 89].

Programmation via TCP/IP

Dans ce cas, l'ordinateur communique avec un SR35i dédié qui transmet (via TCP/IP) les informations aux autres concentrateurs. S'il s'agit d'un nouveau système, vous avez déjà eu l'occasion de configurer une **adresse IP** correcte.

Le premier SR35i est affiché dans le programme d'installation. Si des SR35i qui n'ont pas encore été programmés sont détectés, ceux-ci sont répertoriés à l'écran dans la liste des concentrateurs disponibles pour le système. Si ce n'est pas le cas, utilisez la commande **Nouveau** pour créer de nouveaux concentrateurs, puis définissez pour chacun d'entre eux l'**adresse IP**, la fonction **proxy** et les autres paramètres requis en suivant les étapes de la procédure décrite à la section Programmation des concentrateurs SR35i [→ 89].



La transmission des données vers et depuis un nouveau SR35i peut prendre un temps considérable (en fonction du trafic sur le réseau). Ceci s'applique également à la mise à jour du programme de contrôle de l'accès aux portes.

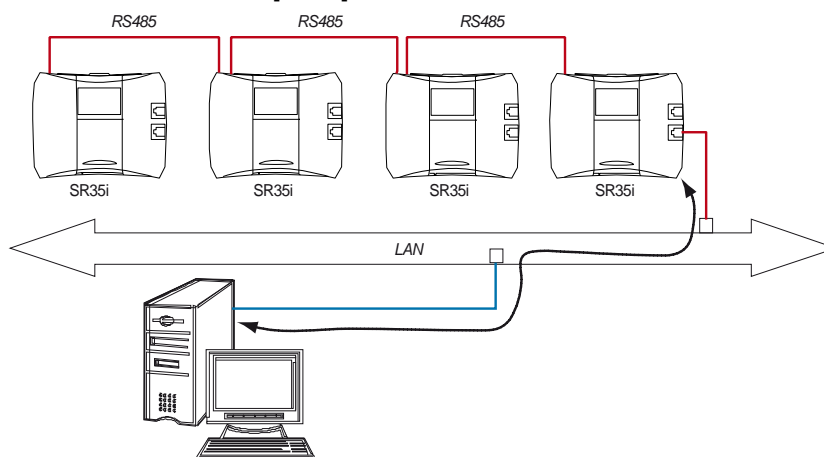
Programmation via le clavier du SR35i

Il n'est parfois pas possible de se connecter au SR35i à partir du PC (par exemple, dans les environnements de sites distants). Dans un tel cas, la configuration des paramètres réseau peut s'effectuer via le système de menus du SR35i. Chaque concentrateur est équipé d'un clavier et d'un écran intégrés permettant la saisie de caractères. Prenez soin de configurer les mêmes paramètres sur le concentrateur et sur le PC (base de données). Voir la section Programmation des concentrateurs SR35i [→ 89].

20.2 Création de plusieurs SR35i pour la communication combinée TCP/IP et RS485

Pour mettre en place une communication combinée (s'effectuant à la fois via un réseau local et un système de câblage RS485), configurez tout d'abord le concentrateur utilisé pour TCP/IP en suivant les étapes de la section précédente. Tous les autres SR35i, reliés par RS485, reçoivent des noms temporaires (**c1, **c2, etc.), où le chiffre correspond à l'adresse du concentrateur.

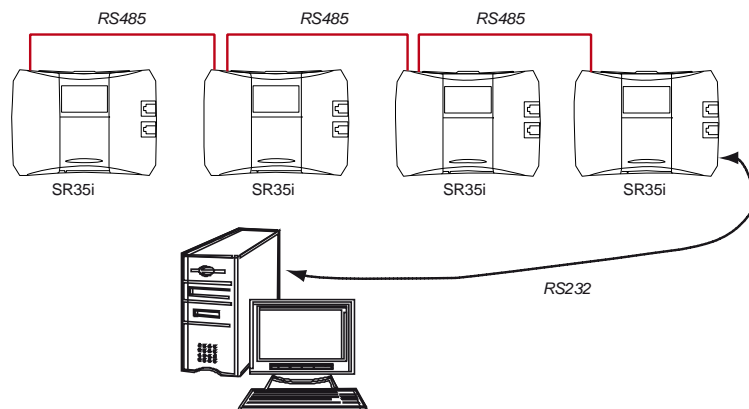
Suivez ensuite les étapes de la procédure décrite à la section Programmation des concentrateurs SR35i [→ 89].



20.3 Création de plusieurs SR35i pour la communication via RS485 uniquement

Les systèmes destinés à communiquer via RS485 (et non en réseau local) sont configurés directement à l'aide de câbles RS232. Dans un tel système, tous les concentrateurs sont nommés **C1, **C2, etc., où le chiffre correspond à l'adresse de cavalier de liaison.

Suivez ensuite les étapes de la procédure décrite à la section Programmation des concentrateurs SR35i [→ 89].



21 Programmation des concentrateurs SR35i



Un nouveau système basé sur TCP/IP vous offre la possibilité (au démarrage du programme d'installation) d'ajouter des SR35i qui n'ont pas encore été configurés et que le logiciel a "détecté" sur le réseau local LAN. Ceux-ci sont répertoriés dans une liste. Il vous suffit de les sélectionner dans cette liste pour les inclure à votre système.

1. Lancez le programme d'installation [→ 79].
2. Sélectionnez un concentrateur de segments et cliquez sur **Modifier**.
 - Conseil : vous pouvez également cliquer avec le bouton droit de la souris et choisir Nouveau, Modifier ou Supprimer.
3. Dans le champ **Nom**, saisissez le nom du concentrateur de segments.
Exemple : vous pouvez choisir le nom de la pièce où le concentrateur doit être installé, par exemple "Réception". Evitez de choisir des noms susceptibles d'être confondus avec des noms de portes.
4. Cochez la case pour définir le SR35i comme un nœud **proxy** utilisant TCP/IP.
Si tous les SR35i sont reliés par des câbles RS485 (et que le PC utilise TCP/IP), le proxy assure uniquement la communication des SR35i avec un serveur horaire SNTP. Si la configuration combine RS485 et TCP/IP, les concentrateurs de segments qui utilisent TCP/IP doivent disposer d'une fonction proxy.
5. Spécifiez également si vous souhaitez utiliser le SR35i comme agent de sous-réseau [→ 52] (faisant office de passerelle pour les autres concentrateurs SR35i situés "derrière" un routeur).
6. Cliquez sur l'onglet des paramètres Réseau [→ 90], entrez l'**adresse IP** et les adresses du **masque de réseau** et de la **passerelle**.
 - Au démarrage du concentrateur, l'adresse IP utilisée est celle définie par défaut **10.1.200.1xx** (où xx correspond à l'adresse définie sur le concentrateur par le cavalier de liaison) ou celle définie au moment de la configuration du concentrateur SR35i.
Indiquez l'adresse du **masque de réseau** qui permet de filtrer les adresses pour les communications en réseau local. Vous utiliserez généralement la valeur suivante : 255.255.255.0. Indiquez l'adresse de la **passerelle** (si elle existe dans votre configuration). Ceci permet de gérer les adresses rejetées (filtrées par le masque de réseau). Précisez une adresse IP de serveur DNS si vous projetez d'utiliser la fonction de courrier électronique.
 - Si vous le souhaitez, vous pouvez obtenir automatiquement les paramètres IP (DHCP) et l'adresse du serveur DNS. Cochez pour ce faire les cases correspondantes. Notez que la fonctionnalité DynDNS [→ 91] doit être à la fois configurée dans le logiciel et programmée sur le SR35i.
7. Précisez le **serveur de courrier électronique** (SMTP) utilisé, par exemple, dans le système de réservation.
8. Entrez l'identité réseau du concentrateur de segments.
9. Cliquez sur l'onglet **Heure** (s'il est affiché) et entrez la **valeur du décalage horaire** (+1, +2, -1, -2, etc.). Cette valeur correspond à la zone géographique où le SR35i est installé. (Il s'agit du décalage séparant l'heure GMT du paramètre par défaut de l'ordinateur : +0 pour le Royaume-Uni, +1 pour la Suède et +2 pour la Finlande).

10. Cliquez sur **OK** et répétez la procédure pour tous les concentrateurs de segments du système jusqu'à ce que vous les ayez tous nommés.

21.1 Définition des paramètres réseau du SR35i

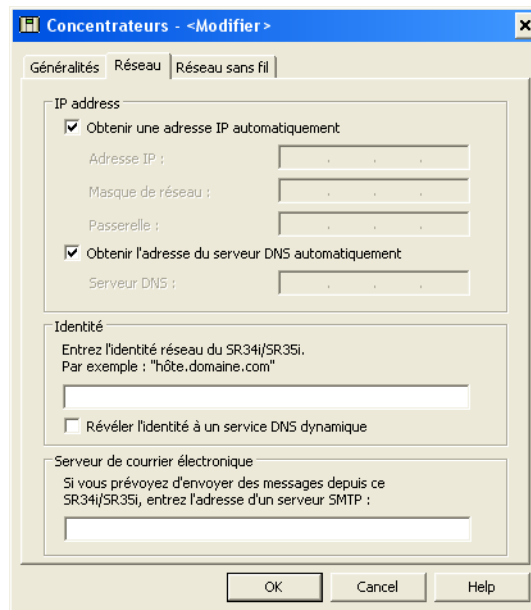
Lorsque le système autorise l'utilisation de DHCP dans les SR35i, un certain nombre de paramètres supplémentaires doivent être pris en compte.

Lorsque l'option DHCP est sélectionnée, chaque concentrateur se voit allouer automatiquement une adresse IP et un DNS global (utilisé pour les recherches d'adresses IP ultérieures dans DynDNS.org).

Procédez comme suit :

1. Lancez le programme d'installation [→ 79].
2. Sélectionnez un SR35i dans l'onglet **Concentrateurs**.
3. Cliquez sur **Modifier** ou cliquez deux fois sur son nom.
4. Activez l'onglet **Réseau** et cochez la case **Obtenir une adresse IP automatiquement**.
5. Dans le champ **Identité**, saisissez le nom du concentrateur. Si DynDNS est utilisé, ce nom est formulé selon la syntaxe suivante : Appt1.dyndns.net, Identity1.dynalias.net.
6. Si ce concentrateur est également utilisé pour l'envoi de **confirmations** dans un système de réservation, précisez le nom du **serveur de messagerie**. Procurez-vous ce nom auprès de votre fournisseur de service Internet. Par exemple : mail1.xyz.com. Assurez-vous que le serveur de messagerie autorise l'utilisation des identités choisies (absence de blocage).
7. Précisez si vous souhaitez que le concentrateur **révèle son identité** à un serveur DynDNS.
 - La configuration par défaut suppose que le routeur prend en charge cette fonctionnalité et le paramètre du "fournisseur" est désactivé dans le SR35i. Notez que si le SR35i est utilisé comme "sous-agent" derrière un routeur configuré pour la redirection DynDNS, vous devez attribuer au sous-agent l'identité du routeur.
 - Si vous choisissez de révéler l'identité, il se peut qu'un avertissement s'affiche, vous informant de la nécessité d'un compte DynDNS [→ 91].
8. Cliquez sur **OK**.
9. Répétez cette procédure pour chaque SR35i utilisant DHCP.

La capture d'écran ci-dessous illustre ces paramètres.

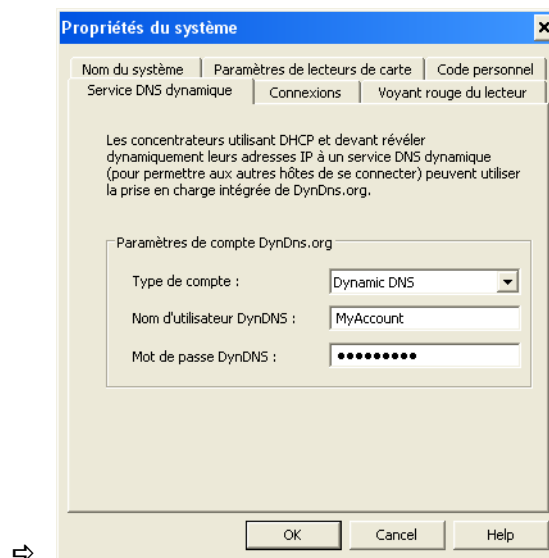


Paramètres réseau du SR35i

21.2 Personnalisation de la base de données pour DHCP

Si vous avez opté pour DHCP, vous devez à présent décider du mode de communication utilisé entre chaque concentrateur de segments. N'oubliez pas que la case Proxy doit être cochée pour tous les SR35i communiquant via TCP/IP. Effectuez la procédure suivante pour autoriser les fonctions DHCP.

1. Lancez le programme d'installation [→ 79].
2. Choisissez les options de menu **Système > Propriétés du système**.
3. Activez l'onglet **Service DNS dynamique**.



4. Si vous préférez utiliser DynDNS.org, saisissez les **Type de compte**, **Nom d'utilisateur** et **Mot de passe**.
5. Vous avez terminé.

21.3 Préparation du composant SR35i pour DHCP

Si vous prévoyez d'utiliser le SR35i avec la fonction DHCP, il vous faudra programmer chaque unité à cette fin.

Selon la configuration réseau du PC utilisé (routeurs, pare-feux, etc.), la programmation de certains ou de la totalité des paramètres devra s'effectuer via le clavier et l'écran du SR35i.

Le paramètre principal consiste à définir l'utilisation de DHCP.

Procédez comme suit :

1. Mettez sous tension l'unité SR35i.
2. Appuyez sur les boutons **2 > 1 > 2 > 1**.
 - ⇒ La fonction DHCP est activée sur le concentrateur qui entreprend de rechercher les paramètres IP.
3. Vous avez désormais également la possibilité de configurer différents paramètres, tels que des options de redirection DynDNS.
4. Répétez cette procédure pour tous les SR35i devant utiliser DHCP.

22 Programmation de noms et de fonctions pour les portes

L'étape suivante consiste à programmer le nom et la fonction des portes connectées. Selon le type d'unité de porte, les menus affichés diffèrent. L'exemple ci-dessous s'applique à un central de porte DC22.

1. Lancez le programme d'installation [→ 79].
2. Cliquez sur l'onglet **Portes**. La liste des portes installées s'affiche, les portes étant nommées à l'aide des symboles ****C1:D1**, ****C1:D2**, etc.



Si une porte installée ne figure pas dans la liste, cela signifie que le système n'est pas en mesure de communiquer avec elle.

3. Sélectionnez une porte et cliquez sur **Modifier**. Conseil : vous pouvez également cliquer avec le bouton droit de la souris et choisir *Nouveau*, *Modifier* ou *Supprimer*.
4. Dans le champ **Nom**, saisissez le nom de la porte. (32 caractères au maximum).
5. Vérifiez que le lecteur correct est affiché dans le champ **Type de terminal**. Si vous avez défini des zones, il se peut également qu'une option mentionne la présence d'un lecteur EXIT.
6. Si vous envisagez d'utiliser des lecteurs Clock&Data ou Wiegand, veuillez également préciser l'**interface de lecteur** à utiliser.
7. Cliquez sur l'onglet **Relais**.
8. Cochez la case **Contrôler l'alarme par impulsion unique** si vous envisagez d'utiliser une alarme par impulsion unique (locale) pour cette porte. Celle-ci peut faire partie d'une zone sous alarme bistable mais ne peut pas être connectée physiquement à l'unité de centrale d'alarme anti-intrusion.
Fonction d'alarme par impulsion unique. Permet de désactiver l'alarme pendant une courte période (lorsqu'une porte est franchie, par exemple). La durée de la désactivation correspond au délai pour l'ouverture de la porte ajouté au délai maximum d'ouverture de la porte. Les portes dotées de cette fonction ne peuvent, ni contrôler, ni se connecter à des zones sous alarme anti-intrusion.
9. Si le central de porte est destiné à contrôler un **verrou moteur**, cochez la case correspondante.
10. Cliquez sur l'onglet **Contrôle de l'accès aux portes**.
11. Si vous utilisez des connecteurs de porte, cochez la case **Connecteur de porte existant**. Précisez si le contact est ouvert ou fermé lorsque la porte est fermée.
12. Si vous utilisez des connecteurs de verrou, cochez la case **Connecteur de verrou existant**. Précisez si le contact est ouvert ou fermé lorsque la porte est verrouillée.
13. Définissez le type de verrouillage lorsque la porte a été ouverte (**Verrouillage en une fois à l'ouverture de la porte** ou **Verrouillage à la fermeture de la porte**) en fonction du type de verrou installé.
14. Indiquez le cas échéant si le verrou monté est doté d'une fonction de sortie intégrée (exemple : ASSA EL580). Si tel est le cas **et** si le contrôle d'alarme par *impulsion unique* est utilisé, les câbles de cette fonction dans le verrou doivent être raccordés à l'entrée du bouton de sortie dans le central de porte.

15. Si la gestion d'ascenseurs IOR6 est utilisée, reportez-vous à la section Gestion d'ascenseurs à l'aide de l'IOR6 [→ 98].
16. Cliquez sur **OK**.
17. Répétez la procédure pour toutes les portes jusqu'à ce que vous les ayez toutes nommées et définies.

23 Programmation du contrôleur de relais IOR6

Vous pouvez utiliser le contrôleur de relais pour un certain nombre de fonctions spéciales. A l'heure actuelle, ces fonctions sont les suivantes :

- Verrou de porte - sortie
- Relais totalisateur (impulsion) - sortie
- Gestion horaire - sortie
- Contrôle des avertissements en cas de panne de courant (batterie) - entrée
- Contrôle des avertissements en cas d'ouverture d'urgence de portes données - entrée
- Fonction du bouton de sortie (EXIT). Entrée d'activation du relais.
- Fonctions de réservation
- Gestion d'ascenseurs



La fonction de relais totalisateur (d'alarme commune) n'est pas disponible pour les unités IOR6 utilisées dans des applications de gestion d'ascenseurs. Si tel est le cas, choisissez une autre unité IOR6.

Vous pouvez définir ce paramètre sur l'onglet Portes du programme d'installation, qui vous permet de sélectionner l'unité IOR6 voulue (ou d'en créer une nouvelle). Des onglets distincts sont proposés pour la définition des relais et des entrées.

23.1 Sortie de verrou de porte

La fonction de contrôle du verrou peut être utilisée pour contrôler le déverrouillage de portes données (des sorties de secours, par exemple).

Procédez comme suit :

1. Lancez le programme d'installation [→ 79].
2. Activez l'onglet **Portes** et sélectionnez une unité IOR6.
3. Cliquez sur **Modifier**.
4. Cochez l'une des cases **Verrou** dans l'onglet **Relais IOR**.
5. Sélectionnez cette fonction pour le relais de votre choix.
6. Cliquez sur les boutons situés à droite de la zone de liste.
⇒ Une nouvelle fenêtre apparaît, affichant la **liste des portes**.
7. Sélectionnez les portes que vous souhaitez contrôler.

23.2 Sortie de relais totalisateur

Le relais totalisateur d'alarme commune peut être défini sur deux types de sortie différents :

- Le **mode impulsion** implique que le relais revient à son état initial après un certain temps.
- Le **mode bistable** implique que le système conserve l'état de tout relais activé jusqu'à ce que l'utilisateur intervienne ou qu'un événement préalablement défini se produise.

Procédez comme suit :

1. Lancez le programme d'installation [→ 79].

2. Activez l'onglet **Portes** et sélectionnez une unité IOR6.
3. Cliquez sur **Modifier**.
4. Cochez l'une des cases **Relais totalisateur (alarme)** dans l'onglet **Relais IOR**.
5. Chaque relais de l'unité IOR6 peut être configuré pour générer un signal de sortie. Sélectionnez la fonction voulue dans la zone de liste.
 - En **mode impulsion**, un filtre d'événements peut être utilisé pour contrôler le relais. Vous définissez le **temps** d'activation du relais.
 - En **mode bistable**, un nouveau menu s'ouvre pour vous permettre de sélectionner le critère du relais.

23.3 Programmation d'IOR6 pour la gestion horaire

Vous avez la possibilité de définir pour tout relais d'une unité IOR6 une simple fonction de minuterie (qui s'apparente à celle d'un relais d'ouverture de porte).

Les relais - minuterie apparaissent dans le programme Entro où il est possible de leur affecter des plannings individuels.

Le système vous autorise à définir des horaires d'ouverture distincts pour chaque relais ainsi que l'activation des relais 1 à 4 à l'aide de signaux d'entrée (d'ouverture à distance).

Procédez comme suit :

1. Lancez le programme d'installation [→ 79].
2. Activez l'onglet **Portes** et sélectionnez une unité IOR6.
3. Cliquez sur **Modifier**.
4. Activez l'onglet **Entrées IOR6**.
5. Ouvrez l'application Entro afin de sélectionner des options supplémentaires, telles que la définition d'un planning ou de la durée de déverrouillage.

23.4 Entrée d'avertissement en cas de panne de courant

Vous pouvez configurer les entrées pour contrôler les signaux émis par les blocs d'alimentation. Cette fonction est généralement utilisée lorsqu'une batterie de secours est installée. Par exemple, un signal peut être émis par le bloc d'alimentation lorsque la tension du secteur chute et que la batterie de secours est utilisée. Procédez comme suit :

1. Lancez le programme d'installation [→ 79].
2. Activez l'onglet **Portes** et sélectionnez une unité IOR6.
3. Cliquez sur **Modifier**.
4. Cliquez sur l'onglet **Entrées IOR6**.
5. Dans la zone de liste, choisissez **Panne de courant**.

23.5 Entrée d'ouverture d'urgence

Une entrée peut activer une fonction permettant de **déverrouiller les portes sélectionnées**.

Procédez comme suit :

1. Lancez le programme d'installation [→ 79].

2. Activez l'onglet **Portes** et sélectionnez une unité IOR6.
3. Cliquez sur **Modifier**.
4. Sélectionnez **Ouverture d'urgence**.
5. Cliquez sur les boutons situés à droite de la zone de liste.
⇒ Une nouvelle fenêtre apparaît, affichant la liste des portes.
6. Sélectionnez les portes à déverrouiller au moment où l'entrée est activée.

23.6 Entrée du bouton de sortie (EXIT)

Vous pouvez définir une entrée afin d'activer un relais à un moment donné. Par exemple, lors de l'ouverture d'une porte de réservation à distance ou lorsqu'un bouton est pressé dans un ascenseur.

Procédez comme suit :

1. Lancez le programme d'installation [→ 79].
2. Activez l'onglet **Portes** et sélectionnez une unité IOR6.
3. Cliquez sur **Modifier**.
4. Cliquez sur l'onglet **Entrées IOR6**.
5. Sélectionnez **Bouton Sortie** (si cette option n'est pas déjà sélectionnée).

23.7 Programmation d'IOR6 pour le système de réservation

Si vous envisagez d'utiliser dans le système de réservation l'un des relais d'une unité IOR6, procédez comme suit :

1. Lancez le programme d'installation [→ 79].
2. Cliquez sur l'onglet **Portes**. Par défaut, toute nouvelle unité IOR6 est nommée ****Cx:Dy** dans la liste des portes. Sélectionnez l'IOR6 voulue, cliquez sur **Modifier** et passez à l'étape 7 de la procédure ci-dessous.
Si vous préférez créer l'IOR6 manuellement, procédez comme suit :
3. Cliquez sur **Nouveau**. Les **propriétés de la porte** s'affichent.
4. Saisissez le nom du contrôleur de relais dans le champ **Nom**.
5. Vérifiez et/ou précisez l'adresse.
6. Dans la zone de liste **Type de terminal**, sélectionnez IOR6.
7. Cliquez sur l'onglet **Relais IOR6**.
8. Cochez la case **Porte de réservation** et/ou **Appareil de réservation**.
9. Attribuez à chaque relais un nom composé de chiffres. Ceux-ci seront utilisés pour désigner l'IOR6 selon la syntaxe suivante :
"nom de l'IOR6 + numéro du relais". Par exemple, une IOR6 nommée "Laverie" et dotée du relais 3 sera intitulée "Laverie:3".
10. Activez chaque relais en choisissant dans la zone de liste associée l'une des options suivantes :
 - **Porte de réservation**. Indique que le relais sera utilisé comme un simple relais d'ouverture de porte et activé à une heure donnée.

- **Appareil de réservation.** Indique que le relais sera activé pendant *tout* le temps de la réservation de l'objet (d'une machine à laver, par exemple). Si vous devez appliquer une **valeur de délai différé**, lisez les informations relatives à la programmation de zones pour les objets de réservation [→ 107].

11. Cliquez sur **OK**.

23.8 Gestion d'ascenseurs à l'aide de l'IOR6

Dans l'application pour ascenseurs, SiPass Entro permet de limiter l'accès aux différents étages d'un immeuble. Pour la gestion d'ascenseurs, jusqu'à 32 contrôleurs de relais IOR6 peuvent être connectés au système SiPass Entro, ce qui implique qu'au total, 192 étages peuvent être contrôlés.

Il est bon de noter que ni l'IOR6 ni son lecteur principal ne peuvent être inclus dans ces zones. Le relais de verrouillage du lecteur principal (central de porte) ne peut être utilisé pour toutes les applications.

1. Lancez le programme d'installation [→ 79].
2. Cliquez sur l'onglet **Portes**. Par défaut, toute nouvelle unité IOR6 est nommée ****Cx:Dy** dans la liste des portes. Sélectionnez l'IOR6 voulue, cliquez sur **Modifier** et passez à l'étape 7 de la procédure ci-dessous.
Si vous préférez créer l'IOR6 manuellement, procédez comme suit :
3. Cliquez sur **Nouveau**. Les **propriétés de la porte** s'affichent.
4. Saisissez le nom du contrôleur de relais dans le champ **Nom**.
5. Vérifiez et/ou précisez l'adresse.
6. Dans la zone de liste **Type de terminal**, sélectionnez IOR6.
7. Cliquez sur l'onglet **Relais IOR6**.
8. Affectez l'IOR6 à la fonction de gestion d'ascenseurs.
9. Attribuez à chaque relais un nom composé de chiffres. Ceux-ci seront utilisés pour désigner l'IOR6 selon la syntaxe suivante :
"nom de l'IOR6 + numéro du relais". Par exemple, une IOR6 nommée "Ascenseur A" et dotée du relais 3 sera intitulée "Ascenseur A:3".
10. Activez chaque relais en choisissant une option dans la zone de liste associée.
11. Cliquez sur **OK**.
12. Cliquez sur l'onglet **Portes** et sélectionnez le terminal que vous souhaitez utiliser comme **lecteur principal** pour l'IOR6.
13. Cliquez sur **Modifier**, activez l'onglet **Gestion d'ascenseurs**, puis sélectionnez les unités IOR6 qui seront dirigées par ce terminal.
14. Cliquez sur **OK**.



Un nom approprié pour le terminal de porte principal est par ex. "Ascenseur, étage". Les terminaux de porte sont nommés sur l'onglet **Portes**.

Dans l'application Entro, les étages numérotés (relais) sont affichés sous l'onglet **Groupes d'accès**, dans la liste de portes sous le nom du lecteur principal. De cette manière, il est très facile de sélectionner les portes auxquelles le groupe aura accès.

Il est également possible d'activer les relais conformément à un planning défini pour le lecteur principal. Cette fonction peut être configurée via l'onglet Relais IOR des propriétés de la porte (dans l'application Entro). Cochez les cases associées aux différentes plages horaires pour activer un relais. Les relais 1 à 4 de chaque IOR6 peuvent également être activés à l'aide d'un signal relié à l'info du bouton Sortie (d'ouverture à distance).

24 Programmation de zones sous alarme anti-intrusion

SiPass Entro propose différentes méthodes pour **armer** une zone sous alarme anti-intrusion bistable :

- Reconnaissance de la carte ou du code personnel au niveau du terminal de porte.
- Utilisation d'un bouton connecté à l'entrée du bouton d'alarme.
- Utilisation d'une horloge externe connectée à l'entrée du bouton d'alarme.
- Utilisation d'un planning d'activation (automatique) d'alarme dans SiPass Entro.
- Utilisation des icônes de porte dans le programme de contrôle des événements et de l'accès aux portes (clic droit).
- Utilisation des fonctions propres de l'alarme anti-intrusion. Le signal d'état de l'alarme est utilisé pour "suivre" l'état du système de détection d'intrusion (retour de l'info).

Pour **désarmer** l'alarme, vous pouvez choisir parmi les méthodes suivantes :

- Reconnaissance de la carte ou du code personnel au niveau du terminal de porte.
- Utilisation des icônes de porte dans l'application de contrôle de l'accès aux portes (clic droit).
- Utilisation des fonctions propres de l'alarme anti-intrusion. Le signal d'état de l'alarme est connecté à l'entrée d'informations sur l'état de l'alarme (ASF).



REMARQUE 1

Lorsque plusieurs SR35i communiquent via TCP/IP, il est préférable de réunir les zones dans un même sous-réseau afin de garantir leur fonctionnement (de zones sous alarme, par exemple).

REMARQUE 2

N'oubliez pas que les DC22 configurés pour le contrôle de l'alarme par impulsion unique ne peuvent pas être utilisés pour contrôler les zones d'une alarme anti-intrusion.

Lorsqu'une seule porte est utilisée pour le contrôle d'une alarme anti-intrusion, vous devez néanmoins créer une zone sous alarme pour cette porte. Vous remarquerez qu'une zone sous alarme peut combiner des fonctions de contrôle de présence et de limitation d'accès, mais pas d'antipassback.

1. Lancez le programme d'installation [→ 79].
2. Cliquez sur l'onglet **Zones**, puis sur **Nouveau**.
Lorsque vous créez une *nouvelle* zone, un assistant apparaît pour vous aider à programmer les fonctions requises. Les informations correspondantes sont affichées dans des onglets pour les zones existantes.
Conseil : vous pouvez également cliquer avec le bouton droit de la souris et choisir Nouveau, Modifier ou Supprimer.
3. Saisissez le **nom** de la zone dans le champ correspondant.
4. Sélectionnez **Zone sous alarme**. Les autres fonctions disponibles pour cette zone s'afficheront également.
5. Cliquez sur **Suivant**. Sous **Portes d'entrée/Disponible**, sélectionnez une ou plusieurs porte(s) à inclure dans la zone sous alarme.
6. Cliquez sur **Suivant**.

7. Sélectionnez la porte qui sera **physiquement connectée** à l'unité de centrale d'alarme anti-intrusion.
8. Dans la zone de liste **Fonction de relais d'alarme**, sélectionnez la méthode de contrôle d'alarme requise.
 - **Fonction Bistable.** Permet un contrôle total de l'alarme anti-intrusion. Vous pouvez désactiver l'alarme en passant votre carte dans le lecteur et en entrant votre code individuel. Pour l'activer, appuyez sur la touche B et passez votre carte dans le lecteur (ou touche B + carte + code individuel). Vous pouvez également enfoncer un bouton (le cas échéant) connecté à l'entrée d'activation de l'alarme sur le DC22. L'activation automatique de l'alarme peut être programmée à l'aide de plannings de contrôle d'alarme.
 - **Impulsion bistable.** Cette méthode de contrôle d'alarme est similaire à la précédente, à la différence près que l'activation et la désactivation de l'alarme sont contrôlées au moyen d'une courte impulsion et non manuellement. Précisez la durée de l'impulsion.
9. Indiquez si l'option **Utiliser l'avertissement d'activation de l'alarme** doit être activée. Si oui, dans le champ du délai d'avertissement, indiquez la durée d'émission du buzzer d'avertissement avant l'activation de l'alarme (laps de temps compris entre 5 et 1 000 secondes = 16,5 minutes). Le buzzer prévient les personnes qui se trouvent toujours dans le bâtiment que l'alarme va être activée. Au cours de cette période, l'état de la sortie du relais de pré-alarme change sur tous les DC22 situés dans la zone sous alarme.
Si vous décidez de **ne pas utiliser** de délai d'avertissement, le relais d'alarme change d'état *immédiatement*, sans avertissement de buzzer (pré-alarme). Si la fonction d'informations sur l'état de l'alarme est activée, le bouton Sortie fonctionne tant qu'aucun signal d'état d'alarme n'est émis. Cela se produit dans le cas où l'alarme anti-intrusion se charge du signal de pré-alarme (c.-à-d., aucune information sur l'état de l'alarme à ce moment-là).
10. Spécifiez si le **Bouton Sortie** peut interrompre le cycle d'activation de l'alarme.
11. Choisissez le **planning** à utiliser pour l'activation automatique de l'alarme. Si vous ne sélectionnez aucun planning, l'alarme devra être activée manuellement ou répondre à un signal externe (connecté à l'entrée d'activation de l'alarme).
Si vous n'avez pas encore créé de planning (via le programme Entro), cliquez sur l'icône représentant une horloge et sélectionnez Nouveau, Modifier ou Supprimer.
12. Cliquez sur **Suivant**.
13. Cochez la case **Utiliser les informations sur l'état de l'alarme** pour connecter le signal d'état de l'alarme anti-intrusion. Le signal est connecté à l'entrée d'information sur l'état de l'alarme (ASF) du DC22. Cette information informe SiPass Entro si l'alarme anti-intrusion a été activée (ou non).
14. Dans le champ **Délai du signal d'état de l'alarme**, spécifiez la durée en secondes pendant laquelle SiPass Entro attend le retour du signal d'état avant de considérer que l'activation a échoué. Dans ce cas, SiPass Entro repasse en état normal et restaure l'accès normal aux portes.
15. Choisissez dans la zone **Contrôle du voyant** la manière dont vous souhaitez contrôler le voyant rouge au niveau du terminal de porte. Vous pouvez opter pour le signal d'état de l'alarme ou connecter un autre signal externe. C'est le cas si le voyant rouge doit clignoter par exemple.
 - Si vous choisissez d'utiliser l'état de l'alarme, vous avez également la possibilité de désactiver le voyant rouge après un certain laps de temps

(une fois l'alarme activée). Dans ce cas, le voyant s'allume **uniquement** sur le lecteur sur lequel la commande est exécutée. Les voyants des autres lecteurs de la zone sont éteints.

- Si vous choisissez de ne pas utiliser la fonction d'état d'alarme, vous avez toujours la possibilité de connecter un signal externe. Dans ce cas, choisissez seulement l'info du voyant.

16. Cliquez sur le bouton **Régler** associé à l'info du voyant afin de déterminer si le signal externe du système d'alarme est constant ou clignotant. Pour ce faire, réglez le temps pendant lequel le voyant rouge sera allumé au niveau du terminal de porte. La valeur (maximale) définie par défaut est de 3,2 secondes. Pour que le voyant clignote, définissez une constante légèrement plus élevée que le cycle d'impulsion du signal externe.

17. Cliquez sur **OK**.

24.1 Définition de niveaux de sécurité pour le contrôle de l'alarme

1. Ouvrez l'application Entro [→ 79].
2. Cliquez sur l'onglet **Zones**.
3. Cliquez sur **Propriétés**.
4. Sélectionnez le **niveau de sécurité** à utiliser pour l'activation et la désactivation de l'alarme anti-intrusion.
5. Choisissez Carte, Code personnel ou Carte + code individuel dans la zone de liste.
6. Cliquez sur **OK**.



L'option sélectionnée sera appliquée à toutes les zones sous alarme que vous créez.

25 Programmation d'autres types de zones

En plus des zones sous alarme, vous pouvez former d'autres types de zones incluant une ou plusieurs portes. Vous pouvez créer les types de zones suivants :

- Zones antipassback
- Zones de contrôle de présence
- Zones à entrée restreinte
- Zone de verrouillage (à deux portes)



Vous pouvez également utiliser la technique du sous-adressage lorsque vous créez des zones et sélectionnez des lecteurs. Cette technique s'applique aux lecteurs de type BC-Link qui peuvent être adressés en tant que ENTRY ou EXIT lorsqu'ils sont connectés à un même central de porte.

25.1 Antipassback/Contrôle de présence

Une zone de contrôle de présence est créée dès que l'on crée une zone antipassback. Vous pouvez cependant créer des zones uniquement de type contrôle de présence.

La seule différence entre ces deux zones est que la zone antipassback indique que la carte est annulée si une personne n'utilise pas sa carte pour quitter une zone dans laquelle elle a accédé précédemment.

Si une porte est utilisée à la fois pour les entrées et les sorties d'une zone antipassback, et que l'accès est concédé des deux côtés avant l'ouverture de la porte, le système n'est pas en mesure de savoir qui a franchi la porte. Pour gérer de tels cas, l'utilisation d'une **solution de tourniquet est recommandée**.

Le même lecteur peut être de type IN (entrée) dans une zone et de type OUT (sortie) dans une autre.

La procédure ci-dessous explique comment créer une zone antipassback ou une zone de contrôle de présence :

1. Lancez le programme d'installation [→ 79].
2. Cliquez sur l'onglet **Zones**, puis sur **Nouveau**.
Lorsque vous créez une nouvelle zone, un assistant apparaît pour vous aider à programmer les fonctions requises. Les informations correspondantes sont affichées dans des onglets pour les zones existantes.
Conseil : vous pouvez également cliquer avec le bouton droit de la souris et choisir Nouveau, Modifier ou Supprimer.
3. Saisissez le **nom** de la zone dans le champ correspondant.
4. Sous **Portes d'entrée/Disponible**, sélectionnez la porte dotée du lecteur d'entrée.
5. Sous **Portes de sortie/Disponible**, sélectionnez la porte dotée du lecteur de sortie.

En cas de violation de la fonction antipassback, par exemple, si la personne n'utilise pas sa carte pour quitter la zone et tente ensuite d'accéder à la même zone ou à une autre, la carte est mise sur liste noire. Cette fonction est utilisée pour déterminer la durée pendant laquelle la carte sera annulée.

1. Ouvrez l'application Entro [→ 79].
2. Activez l'onglet **Zones**.

3. Cliquez sur le bouton **Propriétés**.
4. Cliquez sur l'onglet **Antipassback**.
5. Sélectionnez l'alternative souhaitée.

25.2 Limitation de l'accès

Lorsque vous créez une zone à entrée restreinte, vous devez décider des groupes d'accès habilités à pénétrer cette zone. Spécifiez ensuite le nombre d'entrées autorisées pour chaque personne.

1. Lancez le programme d'installation [→ 79].
2. Cliquez sur l'onglet **Zones**, puis sur **Nouveau**.
Lorsque vous créez une nouvelle zone, un assistant apparaît pour vous aider à programmer les fonctions requises. Les informations correspondantes sont affichées dans des onglets pour les zones existantes.
Conseil : vous pouvez également cliquer avec le bouton droit de la souris et choisir Nouveau, Modifier ou Supprimer.
3. Saisissez le **nom** de la zone dans le champ correspondant.
4. Sous **Portes d'entrée/Disponible**, sélectionnez les portes à inclure dans la zone.
5. Cliquez sur **OK**.
6. Ouvrez l'application Entro [→ 79].
7. Cliquez sur l'onglet **Zones**.
8. Sélectionnez le nom de la zone à entrée restreinte voulue et cliquez sur **Modifier**.
9. Cliquez sur l'onglet **Limitation de l'accès** et sélectionnez un type de restriction (ou les deux types disponibles).
 - **Utiliser le compteur d'entrées**. Cela implique qu'un certain nombre d'entrées est concédé aux portes, y compris dans cette zone. Plus tard, dans l'application Entro, un ou plusieurs groupes d'accès pourront être créés avec accès limité à ces portes. Enfin, le nombre d'entrées concédées peut être spécifié pour chaque personne.
 - **Accès restreint à cette zone** (par ex. deux fois par jour). Si cette alternative est choisie, activez l'option Paramètres d'accès restreint et sélectionnez la restriction de temps souhaitée, par ex. deux fois par jour. Le cas échéant, l'accès peut être encore limité en optant pour des restrictions par plage horaire.



Si plus d'une zone à accès restreint est créée, seule une zone peut avoir un accès limité.

25.3 Zone de verrouillage

SiPass Entro offre la possibilité de faire coopérer deux portes dans le but de créer une zone de verrouillage. Ceci implique que la première porte doit être fermée avant que la seconde puisse être déverrouillée.

Le contrôle de l'état des portes s'effectue via des **connecteurs montés sur chaque porte**.

Procédez comme suit :

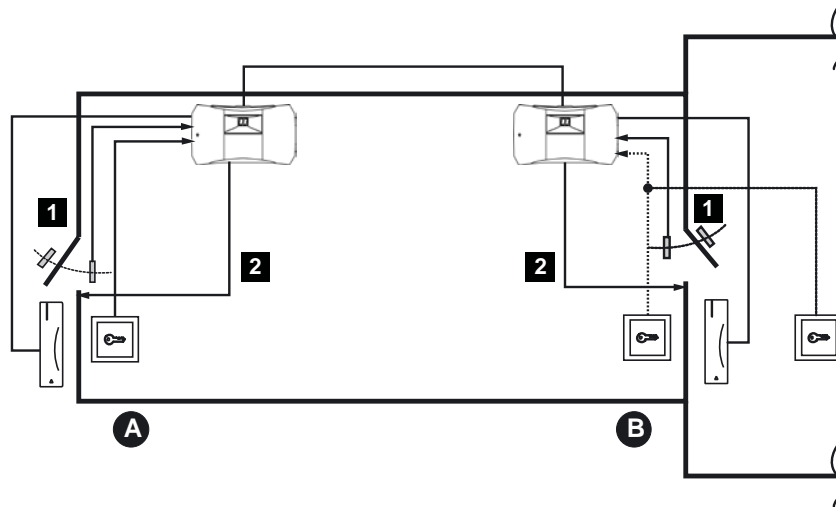
1. Lancez le programme d'installation [→ 79].
2. Cliquez sur l'onglet Zones, puis sur Nouveau.
⇒ Un assistant démarre.
3. Saisissez un **nom** et sélectionnez **Verrouillage**.
4. Sélectionnez les **deux portes**.
5. Spécifiez si la **seconde porte** de la zone doit s'ouvrir automatiquement ou non.
6. Fermez la fenêtre.



Si un niveau de sécurité "**bistable**" est défini pour une porte incluse dans une zone verrouillage, la seconde porte ne s'ouvre PAS automatiquement à la fermeture de la première porte.

25.3.1 Exemple de verrouillage

La **porte (A)** est équipée d'un lecteur de carte pour pénétrer dans la zone et d'un bouton de sortie pour en sortir. La **porte (B)** peut être équipée de boutons de sortie dans les deux sens ou d'un lecteur de carte permettant d'entrer. Le fonctionnement de la zone de verrouillage peut différer légèrement selon le type d'installation choisi.



Exemple présentant deux lecteurs BC-Link PR500

1.	Connecteurs de porte
2.	Verrou électrique

Accès de la porte A vers la porte B

Lorsque la porte A est franchie puis fermée **au cours du** délai pour l'ouverture de la porte, le déverrouillage de la porte B s'effectue automatiquement.

Toutefois, si la porte A est fermée **après** écoulement de ce délai (un signal sonore est émis pendant toute la durée du délai d'ouverture maximum de la porte), le bouton de sortie doit être utilisé pour franchir la porte B. Si cette dernière n'est

dotée d'aucun bouton de sortie, la porte A doit être rouverte depuis l'extérieur pour accéder à la zone.

Accès de la porte B vers la porte A

Lorsque la porte B est franchie puis fermée au cours du délai pour l'ouverture de la porte, le déverrouillage de la porte A s'effectue automatiquement. Si la porte B est fermée après écoulement de ce délai (un signal sonore est émis pendant toute la durée du délai d'ouverture maximum de la porte), le bouton de sortie doit être utilisé pour franchir la porte A.

Si la porte B ne dispose que de boutons de sortie, le déverrouillage automatique n'a pas lieu. Les deux portes doivent être ouvertes à l'aide des boutons de sortie.

26 Programmation en vue de la réservation

26.1 Programmation de zones pour les objets de réservation

Cette section décrit la procédure de création de portes et de relais dans un objet de réservation. Notez que l'utilisation d'un lecteur principal commun à plusieurs objets de réservation fonctionnera uniquement si les objets sont groupés.

1. Lancez le programme d'installation [→ 79].
2. Cliquez sur l'onglet **Zones**, puis sur **Nouveau**.
Lorsque vous créez une nouvelle zone, un assistant apparaît pour vous aider à programmer les fonctions requises. Les informations correspondantes sont affichées dans des onglets pour les zones existantes.
3. Saisissez le **nom** de l'objet dans le champ correspondant.
4. Sélectionnez **Objet de réservation** et cliquez sur **Suivant**.
5. Cliquez sur **Ajouter/Supprimer portes et relais**. Une nouvelle fenêtre présentant toutes les portes SiPass Entro et tous les relais IOR6 spécifiés à des fins de réservation s'affiche.
6. Ajoutez des unités à l'objet de réservation, puis cliquez sur **OK**.
⇒ Une liste de portes et relais s'affiche, assortie d'un nouveau champ d'option pour chaque entrée.
7. Pour **chaque porte (ou relais)**, vous devez à présent configurer la fonction associée en choisissant parmi les suivantes :
 - **Lecteur principal**. Il s'agit en effet de l'objet que vous souhaitez peut-être réserver (par ex., de 18h00 à 19h00). Vous remarquerez que cette option sera uniquement valable pour une porte (un lecteur). Toutes les autres portes de l'objet seront alors bloquées pour cette sélection.
 - **Délai de réservation**. Il peut s'agir d'une porte située "sur le chemin" de l'objet et aucun délai différé n'est ajouté.
 - **Délai différé**. Cette porte (ou le relais IOR6) autorisera l'accès uniquement pendant un délai différé (indiqué ci-après). Par exemple, un délai différé défini sur 30 min donne un accès dans la plage horaire 18h30 – 19h30. N'oubliez pas que les portes/relais de ce type peuvent **uniquement faire partie d'un seul objet**.
 - **Durée combinée**. Il s'agit d'une porte qui autorisera l'accès pendant la période du lecteur principal plus le délai différé. Exemple : 18h00 – 19h30.
8. Indiquez la **valeur de délai différé** (120 minutes au maximum) si une porte utilise des délais différés.
9. Cliquez sur **OK**.

Répétez cette procédure pour chaque nouvel objet de réservation que vous souhaitez programmer.

Si vous projetez d'utiliser un contrôleur de relais IOR6 dans un objet de réservation, programmez celui-ci en suivant les instructions fournies dans la section Programmation d'IOR6 pour le système de réservation [→ 97].

Vous pouvez configurer des paramètres de réservation supplémentaires à partir de l'onglet Zones du programme Entro.

26.2 Distribution aléatoire ou NON aléatoire d'objets de réservation similaires

Si plusieurs objets similaires sont destinés à la réservation, vous pouvez distribuer leur utilisation de manière aléatoire afin de minimiser l'usure de chaque objet.

Si vous optez pour une distribution aléatoire, cochez l'option de **fonction aléatoire** et consultez la section Objet de réservation (groupe).

Prenons l'exemple de la fonction aléatoire d'une laverie équipée d'un certain nombre de machines à laver, chaque machine étant un objet contrôlé par un relais d'IOR6 (gestion des appareils). Tous ces objets individuels sont alors regroupés et considérés comme un objet groupé **objet groupé** unique. Lorsqu'un utilisateur effectue une réservation, il peut se voir attribuer n'importe lequel des objets individuels.

Procédez comme suit pour créer une zone groupée :

1. Créez les objets individuels comme indiqué précédemment.
2. Associez à chaque objet le même **lecteur principal**.
3. Sélectionnez un relais IOR6 (affecté à la gestion des appareils) pour contrôler l'objet (une machine à laver, par exemple).
4. Enfin, créez un nouvel objet de type **Groupe d'objets de réservation** et sélectionnez les objets que vous souhaitez regrouper. Notez que l'utilisation d'un lecteur principal commun à plusieurs objets de réservation fonctionnera uniquement si les objets sont groupés.

En procédant de cette manière, vous appliquez à l'ensemble des objets les mêmes paramètres principaux, tels que le nombre maximum de réservations autorisé.

26.3 Contrôle de l'alarme dans un objet de réservation

Si vous installez une alarme anti-intrusion dans un local ouvert à la réservation, vous pouvez utiliser le lecteur de carte du contrôle de l'alarme à la fois en mode bistable et en mode impulsion unique. Pour ce faire, utilisez un DC22.

Mode impulsion unique

Pour utiliser cette méthode, le DC22 de la porte doit être configuré pour la fonction d'alarme par impulsion unique. Cochez la case **Contrôler l'alarme par impulsion unique** dans l'onglet Relais des propriétés de la porte du programme d'installation.

Le relais d'alarme change d'état pendant la **Durée commande libération + Temps maxi ouverture porte**, puis revient automatiquement à son état initial.

Mode bistable

Notez que cette méthode diffère de la manière dont SiPass Entro traite habituellement le contrôle d'une alarme anti-intrusion (à l'intérieur des zones sous alarme).

Ce mode arme ou désarme une section d'alarme à l'intérieur de l'alarme anti-intrusion. La connexion au relais d'alarme est établie dans le **DC22**. Assurez-vous que la case à cocher **Contrôler l'alarme par impulsion unique** de l'onglet Relais est **désactivée**.



La zone de l'alarme anti-intrusion ne peut être gérée que depuis cette porte.

- L'**activation** de ce mode s'effectue à l'aide d'un bouton d'alarme connecté à l'entrée ALARM BUTTON du DC22.
- Sa **désactivation** s'effectue via un accès accordé à l'objet de réservation. Le niveau de sécurité Carte ou Carte + code individuel est généralement appliqué.

26.4 Plannings

La première étape consiste à identifier les différents intervalles de réservation. Par exemple, un court de tennis peut offrir différentes sessions de trois heures qu'il est possible de réserver tous les jours, ou un autre objet qui ne soit disponible qu'en semaine.

Le système permet de définir 32 plannings comportant chacun 24 intervalles de réservation.



Les valeurs d'horloge et de jour indiquées ci-dessous constituent les intervalles de base, mais elles peuvent être modifiées sous certains aspects grâce au concept de "délai différé". Vous ajoutez cette fonction dans le programme d'installation lors de la configuration des portes dans l'objet (la zone) de réservation.

1. Ouvrez l'application Entro [→ 79].
 2. Cliquez sur l'onglet **Plannings**.
 3. Cliquez sur **Nouveau**.
 4. Lorsque vous créez un nouveau planning, un assistant apparaît pour vous aider à programmer les fonctions requises. Les informations correspondantes sont affichées dans des onglets pour les plannings existants.
Dans cet assistant, vous pouvez désormais également programmer des demi-journées, des jours fériés et des congés annuels. Voir la section Définition des jours fériés et des congés annuels dans le système de réservation.
 5. Dans le champ **Nom**, entrez le nom du planning (Session d'entraînement, par exemple).
 6. Cliquez sur **Nouveau** pour créer un nouvel **intervalle**. Une ligne apparaît, proposant des valeurs par défaut dans les champs De, à et Actif le.
 7. Dans la liste déroulante **De**, choisissez l'heure voulue et appuyez sur la touche de tabulation.
 8. Dans la liste déroulante **à**, choisissez l'heure voulue et appuyez sur la touche de tabulation.
 9. Sélectionnez les **jours** à inclure dans l'intervalle.
 10. Répétez les étapes 4 à 7 pour chaque nouvel intervalle que vous souhaitez définir.
 11. Vous pouvez cliquer sur **Trier** si vous souhaitez réorganiser les intervalles.
 12. Cliquez sur **OK** pour enregistrer le planning.
- Répétez les étapes de cette procédure pour le planning suivant.

26.5 Objet de réservation

La procédure suivante consiste à programmer l'objet de réservation proprement dit.

La définition des portes physiques/relais de l'objet unique ou multiple est établie au départ dans le programme d'installation [→ 79].

1. Si vous utilisez plusieurs classes de membres, ouvrez le dossier **Propriétés des personnes** sous le menu **Système > Propriétés du système** et décidez des noms généraux des **classes** une, deux et trois. Celles-ci seront alors affichées dans chaque objet à des fins de définition des valeurs.
2. Ouvrez l'application Entro [→ 79].
3. Cliquez sur l'onglet **Zones**.
⇒ Les objets précédemment définis sont affichés à l'écran.
4. Sélectionnez l'objet voulu et cliquez sur **Modifier**.
5. Sélectionnez un **planning** dans la liste. Cliquez sur la flèche pour afficher la liste des plannings disponibles.
Vous pouvez également cliquer sur l'icône représentant une horloge pour créer, modifier ou copier un planning de réservation. Choisissez ensuite le planning voulu en cliquant sur son nom.
6. Indiquez si la réservation flexible est autorisée dans cet intervalle. Pour plus de détails à ce sujet, voir la section Réservation flexible à l'intérieur d'un intervalle.
7. Indiquez le **nombre maxi de réservations simultanées** autorisé pour un même objet. Par exemple, si un terrain de tennis dispose de deux courts mais d'une seule porte, celle-ci devra pouvoir faire l'objet de réservations simultanées issues de deux différents groupes de membres. Vous pouvez définir 99 réservations simultanées au maximum.
8. Cliquez sur l'onglet **Restrictions**.
9. Choisissez les **fonctionnalités de réservation** des utilisateurs pour une période donnée afin d'autoriser, par exemple, la réservation de quatre sessions d'entraînement par mois pour le même objet. Vous pouvez définir 60 réservations au maximum sur chacun d'entre eux.
10. Définissez d'éventuelles restrictions supplémentaires à appliquer pour chaque classe. Indiquez dans les champs **Nbre maxi de réservations** et **Période calendaire** le nombre de réservations (6 au maximum) autorisé pour un groupe de membres pendant une période calendaire donnée (jour, semaine ou mois).
11. Cliquez sur l'onglet **Définition des délais**.
12. Dans le champ **Délai maxi de réservation**, indiquez la durée maximale d'une période de réservation (31 jours, par exemple). Vous pouvez définir 365 réservations simultanées au maximum.
13. Choisissez ensuite le nombre de minutes précédant une annulation automatique par le système. Renseignez pour ce faire le champ **Délai d'annulation automatique**. Il s'agit du délai devant s'écouler avant qu'un autre groupe de membres soit en mesure de réserver l'objet. Vous pouvez définir un délai maximal de 60 minutes.
14. Précisez ensuite le **délai de chevauchement** autorisé pendant lequel il est encore possible d'accéder à l'objet une fois la période de réservation entamée. Ceci permet, par exemple, de pénétrer un court de tennis réservé avec quelques minutes de retard (en cas d'embouteillage ou autre empêchement). Vous pouvez définir un délai maximal de 99 minutes.
15. Précisez la **durée minimale restante** (en heures et en minutes) d'un intervalle, requise pour autoriser une nouvelle réservation. Vous pouvez définir une durée maximale de 23 heures et 45 minutes.

16. Cliquez sur **OK**.

Répétez les étapes nécessaires pour chaque objet de réservation.

26.6 Définition des jours fériés et des congés annuels dans le système de réservation

Il se peut que certains jours ne soient pas ouverts à la réservation. Lorsqu'un court de tennis est utilisé pour un tournoi, par exemple, ou lors de la fermeture saisonnière d'un terrain de golf.

Voir aussi la section Entretien [→ 113] qui décrit un autre type d'exception.

Le système SiPass Entro permet de distinguer les *jours fériés et les congés annuels* des jours de la semaine ordinaires. Vous pouvez appliquer ce concept au système de réservation pour exclure ces périodes de la réservation.

Dans la plupart des cas, ces périodes ne coïncident pas et vous devrez les préciser pour chaque planning dans le programme de réservation.

Vous devez programmer l'information pour indiquer au système qu'il doit traiter les jours fériés et les congés annuels différemment des jours ouvrables ordinaires.

Procédez comme suit :

1. Ouvrez l'application Entro [→ 79].
2. Cliquez sur l'onglet **Plannings**.
3. Sélectionnez un planning, cliquez sur **Modifier**, puis sur l'onglet **Jour férié**.
4. Cochez la case **Utiliser la table type** si vous préférez utiliser le tableau défini dans le programme principal Entro.
5. Cliquez sur **Nouveau**. La fenêtre **Jour férié** apparaît.
6. Dans le champ **Date**, entrez la date du premier jour férié. Vous pouvez définir au maximum 14 jours pour chaque planning.
7. Cliquez sur **OK**. L'onglet **Jour férié** réapparaît, affichant la date que vous venez de définir.
8. Cliquez sur **Nouveau** et enregistrez le jour férié suivant.
9. Définissez les **Congés annuels** comme vous venez de le faire pour les jours fériés, en précisant cette fois une date de **début** et de **fin**. Vous pouvez définir au maximum 4 périodes pour chaque planning.
10. Répétez les étapes 4 à 8 pour tous les plannings du système de réservation.

26.7 Définition des droits des groupes d'accès

1. Ouvrez l'application Entro [→ 79].
2. Cliquez sur l'onglet **Groupes d'accès**.
3. Créez ou sélectionnez un groupe d'accès.
4. Activez l'onglet contenant les objets de **réservation**.
 - Cochez la case Gardien si vous souhaitez autoriser ce groupe à accéder et à utiliser l'objet 24 heures par jour, sans qu'il lui soit nécessaire d'effectuer une réservation. (Généralement, vous choisirez de créer un groupe d'accès distinct possédant ce droit).
5. Sélectionnez un ou plusieurs des **objets** disponibles pour en conférer l'accès à ce groupe.

6. Cliquez sur **OK**.

26.8 Définition des droits de réservation des personnes

Pour pouvoir utiliser le système de réservation, chaque personne doit disposer d'un N° de groupe de membres et ce, même si ce numéro est le même pour toutes les personnes. Les personnes qui ne disposent pas de ce numéro ne peuvent pas utiliser le système de réservation à tout moment.

Remarque : les informations supplémentaires fournies s'appliquent uniquement au système de réservation.

Etant donné que chaque personne appartient à un ou plusieurs groupes d'accès, il se peut que le droit de réservation lui soit déjà conféré par son appartenance à un groupe d'accès spécifique.

Si tel n'est pas le cas, créez un nouveau groupe d'accès et procédez comme suit :

1. Ouvrez l'application Entro [→ 79].
⇒ L'onglet **Personnes** s'affiche.
2. Choisissez une personne et cliquez sur **Modifier**.
3. Vous pouvez préciser l'adresse électronique de la personne dans le **champ libre** si vous souhaitez que SiPass Entro envoie à cette dernière une confirmation de réservation par courrier électronique (à condition que le logiciel soit configuré pour l'envoi de tels messages). Voir la section Configuration requise par la fonction de confirmation [→ 114].
4. Vérifiez ou choisissez le **groupe d'accès** approprié.
5. Configurez à présent les propriétés de groupes de membres. Toutes les personnes appartenant au même groupe de membres disposeront automatiquement de droits identiques dans le système de réservation. Il peut s'agir par exemple de groupes sportifs ou de familles.
Il existe deux méthodes de configuration des paramètres, selon le nombre de classes de membres précédemment défini dans l'objet :
 - **Une seule classe par défaut** : indiquez uniquement le **numéro du groupe de membres** directement sous l'onglet général (au-dessus du numéro de carte).
 - **Deux ou trois classes** : cliquez également sur l'onglet **Propriétés du groupe de membres** et sélectionnez une **Classe de membre**. Tous les noms des personnes appartenant au même groupe s'affichent.
6. Cliquez sur **OK**.
7. Répétez les étapes nécessaires pour chaque personne.



REMARQUE 1

Assurez-vous que le groupe d'accès affecté à cette personne est associé à un objet de réservation approprié (voir la description des groupes d'accès).

REMARQUE 2

Vous pouvez faciliter la saisie des données de cartes/personnes dans le système de réservation également en utilisant la fonction de duplication.

26.9 Réservation flexible à l'intérieur d'un intervalle

La réservation d'un ou de plusieurs intervalles courts n'est pas appropriée dans le cas de certains objets de réservation (tels qu'une salle de conférence) qui requièrent une méthode de réservation plus flexible.

Le logiciel vous permet de définir des intervalles plus longs (de 8 heures à 18 heures, par exemple) à l'intérieur desquels les utilisateurs peuvent effectuer des réservations en toute flexibilité. Ainsi, vous définissez les limites (début et fin) d'un intervalle, en laissant à l'utilisateur la liberté de réserver l'intégralité ou une partie de celui-ci.

Procédez comme suit :

1. Ouvrez l'application Entro [→ 79].
2. Cliquez sur l'onglet **Zones**.
3. Sélectionnez l'objet de réservation voulu et cliquez sur **Modifier**.
4. Créez ou modifiez le planning que vous souhaitez utiliser. Cette méthode se traduit généralement par la définition d'intervalles moins fréquents mais plus longs.
5. Cochez la case **Autoriser les périodes de réservation flexible pour cet objet**.
6. Cliquez sur **OK**.

26.10 Affichage des informations de réservation

Le logiciel permet au personnel de planifier des périodes pour l'entretien des appareils. Procédez comme suit :

1. Ouvrez l'application Entro [→ 79].
2. Cliquez sur l'onglet **Zones**.
3. Cliquez sur **Propriétés**, puis sur l'onglet **Paramètres Web**.
4. Sélectionnez les options de votre choix : Afficher le nom des personnes, Afficher le numéro des groupes de membres et Afficher toutes les réservations.
5. Cliquez sur **OK**.

26.11 Entretien

Le logiciel permet au personnel de planifier des périodes pour l'entretien des appareils. Procédez comme suit :

1. Ouvrez l'application Entro [→ 79].
2. Cliquez sur l'onglet **Zones**.
3. Sélectionnez l'objet voulu et cliquez sur **Modifier**.
4. Cliquez sur **Planifier l'entretien**, puis sélectionnez les dates de début et de fin (en cliquant sur les zones de liste afin d'accéder au calendrier) ou l'option **Jusqu'à nouvel ordre**.
5. Cliquez sur **OK**. La période choisie est affichée. Si vous souhaitez la modifier, cliquez de nouveau sur le bouton.
 - Pour supprimer la période d'entretien planifiée, cliquez simplement sur **Annuler l'entretien**.
6. Cliquez sur **OK**.

26.12 Configuration de la fonction de débit

SiPass Entro dispose d'une fonction permettant d'exporter des informations supplémentaires sur les conditions d'utilisation/de non-utilisation des objets. Tout événement associé aux réservations est doté d'une valeur.

Procédez comme suit :

1. Ouvrez l'application Entro [→ 79].
2. Cliquez sur l'onglet **Zones** et **modifiez** l'objet voulu.
3. Activez l'onglet **Débit**. Une zone d'édition s'affiche pour chaque type d'événement.
4. Sélectionnez une **valeur** au format xxxx.yy pour chaque événement. Le format des valeurs doit respecter le format numérique standard de Windows.
5. Cliquez sur **OK**.

Le système stocke ces valeurs avec l'événement dans les fichiers d'événements classiques, mais il ne les affiche pas dans le journal d'événements disponible à l'écran.

Pour les étudier, faites appel à l'application de **contrôle des événements et de l'accès aux portes** et exportez le résultat dans un fichier texte à des fins de modification ultérieure dans un logiciel externe.

(Une autre solution consiste à transférer les informations à l'aide d'une application BAPSI.)



N'oubliez pas que si vous modifiez les valeurs de débit conformément aux indications ci-dessus, une fois le délai de l'événement écoulé, l'original est exporté (= sans corrections).

26.13 Configuration des messages de confirmation par courrier électronique

SiPass Entro peut envoyer automatiquement un message électronique aux personnes qui viennent d'effectuer (ou d'annuler) une réservation. Les textes des messages de confirmation sont stockés sur la carte mémoire flash CF8, dans deux fichiers qu'il est possible (mais généralement pas nécessaire) de modifier.

Ces messages fournissent également l'adresse IP du serveur Web (SR35i) utilisé pour expédier le message. Ceci permet de rouvrir facilement une session afin de modifier des réservations.



Le nom du SR35i, utilisé pour envoyer la confirmation, peut comporter uniquement des caractères reconnus dans les adresses électroniques. Les caractères spéciaux et accentués ne sont généralement pas pris en charge par les serveurs de courrier électronique (fournisseurs d'accès Internet).

26.13.1 Configuration requise par la fonction de confirmation

Le système de réservation permet d'effectuer des réservations à partir de tout PC via Internet. Pour que cela soit possible, le concentrateur SR35i doit impérativement disposer d'une **connexion Internet**.

Vous pouvez également configurer un certain nombre de paramètres visant à permettre l'envoi d'une confirmation par courrier électronique aux personnes ayant effectué une réservation.



Consultez le responsable informatique pour la définition des paramètres suivants.

Procédez comme suit :

1. Lancez le programme d'installation [→ 79].
2. Cliquez sur l'onglet **Concentrateurs**.
3. Sélectionnez les concentrateurs munis de la carte CF8 et devant envoyer le message, puis cliquez sur **Modifier**.
4. Cliquez sur l'onglet **Réseau** et vérifiez/entrez l'adresse IP du **serveur DNS**. Ce serveur convertit en fait le nom de domaine (xyz.com, par exemple) en une adresse IP correcte. Le serveur DNS dépend généralement du fournisseur de services Internet ou du réseau local LAN.
5. Entrez le **serveur SMTP** utilisé pour gérer le courrier électronique sortant. Celui-ci dépend généralement du fournisseur de services Internet. Il présente normalement la syntaxe suivante (ou similaire) : serveur_smtp.swip.net.
6. Entrez l'**identité** utilisée par le SR35i pour générer l'adresse de l'expéditeur. Le nom de domaine (xyz.com, par exemple) permet souvent au fournisseur de services Internet d'authentifier l'expéditeur.
7. Cliquez sur **OK**.
8. Enfin, vérifiez que chaque personne dispose d'une **adresse de courrier électronique correcte**, définie dans le champ libre des propriétés de la personne (dans l'application Entro).
9. Par exemple, si le concentrateur SR35i est intitulé "reservation" et le domaine "xyz.com", le message envoyé aura pour expéditeur "reservation@xyz.com" et pour destinataire l'adresse de courrier électronique saisie dans le premier champ libre des propriétés de chaque personne.

26.13.2 Modification des textes de confirmation

Les textes de confirmation sont stockés sur la carte mémoire CF8, dans des fichiers intitulés :

- reservation.txt (Message de confirmation d'une réservation)
- cancelreservation.txt (Message de confirmation d'une annulation)

Pour modifier ces textes, vous devez utiliser un **adaptateur PC approprié** qui vous permette de récupérer et de stocker le contenu de la carte mémoire CF8. Procédez comme suit :

1. Placez la carte CF8 dans l'adaptateur. (Insérez la carte avec précaution pour éviter de détruire des données). Recherchez les fichiers à l'aide de l'Explorateur Windows ou d'un autre navigateur de fichiers.
2. Dans le dossier "LANG" se trouvent un certain nombre de dossiers de langues (0, 1, 2, etc.). Identifiez le fichier que vous souhaitez modifier.
3. **Apportez les modifications voulues** et rédigez le texte du message. Vous pouvez ensuite inclure un certain nombre de balises [→ 117] de champs qui seront remplacées (à l'exécution) par des informations du système (telles que le nom de l'objet, la date, l'heure, etc.)

- Par exemple, si vous insérez la balise %pfnm, le prénom de la personne sera affiché. Voir l'exemple de la section suivante.
4. Stockez les fichiers modifiés et **remplacez la carte CF8 dans le concentrateur SR35i.**

26.13.3 Exemple de confirmation

Vous pouvez par exemple rédiger le texte suivant dans le fichier intitulé **reservation.txt**, puis stocker ce dernier sur la carte CF8.

```
%sbj<Réservation confirmée>
Cher %pfnm,
Ce message confirme votre réservation de l'objet suivant :
%robn, de %rhur:%rmin à %ehur:%emin le %rdat/%rmon.
Si vous souhaitez modifier vos réservations, rendez-vous à
l'adresse %ipme/login.html
```

Ainsi, une personne dénommée Thomas ayant effectué une réservation du court de tennis 1, le 14 juillet de 14 à 16 heures, recevra le message électronique suivant :

```
Objet : Réservation confirmée
Cher Thomas,
Ce message confirme votre réservation de l'objet suivant :
Court de tennis 1, de 14h00 à 16h00, le 14/06.
Si vous souhaitez modifier vos réservations, rendez-vous à
l'adresse http:xxx.xxx.xxx.xxx/login.html.
```

Vous pouvez modifier de la même manière le fichier **cancelreservation.txt**. Le tableau de la section suivante énumère le type d'informations qu'il est possible d'inclure à vos messages.

26.13.3.1 Champs de courrier électronique dans les messages de confirmation

Le tableau ci-dessous répertorie les différents types de champs pouvant être inclus dans les messages électroniques. Notez que le texte à inclure se trouve dans la colonne de gauche.

Champ	Fonction
%pfnm	Prénom de la personne
%plnm	Nom de la personne
%pfrf	Valeur du champ libre 1 (généralement une adresse électronique)
%pmno	Famille/groupe de membres
%dnam	Nom de la porte
%rwkd	Jour de début de la réservation
%ryer	Année de début de la réservation
%rmon	Mois de début de la réservation
%rdat	Date de début de la réservation
%rhur	Heure de début de la réservation
%rmin	Minute de début de la réservation
%robn	Nom de l'objet de réservation

Champ	Fonction
%ewkd	Jour de fin de la réservation
%eyer	Année de fin de la réservation
%emon	Mois de fin de la réservation
%edat	Date de fin de la réservation
%ehur	Heure de fin de la réservation
%emin	Minute de fin de la réservation
%ipme	Adresse IP du serveur Web de messagerie Remarque : ce paramètre ne fonctionne pas dans les environnements DHCP. Veuillez saisir l'adresse Web en texte normal.

26.13.3.2 Champs spéciaux de courrier électronique

Vous pouvez également inclure les champs suivants pour envoyer à d'autres personnes une copie du message de confirmation (par courrier électronique).

%sbj<x>	Objet, x= texte de l'objet
%bcc<y>	CCI, y= adresse électronique pour la copie cachée
%rcc<z>	CC, z= adresse électronique pour la copie

27 Maintenance

27.1 Développement et modification du système

Il existe bien évidemment différentes méthodes de développement et de modification d'un système SiPass Entro. Il se peut que vous nécessitez davantage de PC ou de portes (impliquant également plus de concentrateurs SR35i). Il se peut également que la mise à jour ou la mise à niveau de certains composants s'avère nécessaire.

Pour procéder à tout développement, vous devez disposer d'au moins une connexion à un PC fonctionnant correctement, afin de réaliser les opérations de configuration requises. Prenez soin de **restaurer la clé de cryptage par défaut** avant de vous lancer dans le développement.

27.2 RS485

Dans un système utilisant exclusivement le type de communication RS485 (RS232 pour les PC), il vous suffit d'installer de nouveaux concentrateurs de segments et centraux de porte à l'aide de câblage et de sources d'alimentation supplémentaires. Toutes les unités communiqueront aussitôt l'installation terminée.

27.3 Gestion réseau

Dans un système TCP/IP, assurez-vous que les concentrateurs de segments et les PC sont installés correctement avec, par exemple, les **adresses IP** et les **clés de cryptage** appropriées. Les centraux de porte et les lecteurs sont à installer comme auparavant.

L'utilisation de concentrateurs de type **SR35i** est recommandée. Il est encore possible de faire appel à des concentrateurs SR34i, mais les types plus anciens (SR32i ou SR32) ne peuvent plus être utilisés.

Si les nouveaux concentrateurs SR35i ou ordinateurs sont destinés à être connectés dans un système SiPass Entro utilisant TCP/IP, il est important que leur configuration soit correcte. Il existe deux "voies" de communication pour l'échange de l'information :

- Entre le PC et les SR35i – via RS232, modem ou TCP/IP.
- Entre les différents SR35i – via RS485 ou TCP/IP.

Si la communication s'effectue via TCP/IP, la **clé de cryptage** doit être chargée dans toutes les unités. Au départ, vous pouvez également utiliser la clé de cryptage par défaut.

Si elle s'effectue via RS232, le PC doit toutefois toujours être en mesure d'accéder au concentrateur.

27.4 Mise à jour du logiciel d'un système existant

La version 6.5 prend en charge un chemin de migration à partir des versions 4.5 et ultérieures. La nouvelle version peut inclure des mises à jour pour les composants suivants :

- PC et matériel afférent
- SR35i
- SR34i (aucune radio – seule mise à niveau vers la version 6.5)
- Centraux de porte

Avant de commencer

- Vérifiez la version du logiciel installée sur votre PC (celle-ci ne doit pas être antérieure à la version 4.5).
- Assurez-vous que tous les concentrateurs de segments sont de type SR35i ou SR34i.

Si votre installation comporte un SR32i, celui-ci doit impérativement être remplacé par un concentrateur de type SR35i. Dans ce cas, il vous faudra probablement également changer la configuration afin de "déplacer" certaines fonctionnalités (telle que le relais totalisateur d'alarme) vers une unité IOR6.

Le tableau suivant indique les versions du logiciel appropriées aux différents types de concentrateurs de segments :

	Ver 4.5	Ver 4.7	Ver 5.x	Ver 6.0	Ver 6.5
SR35i	Non	Oui *1)+2)	Oui *1)	Oui	Oui
SR34i	Non	Oui *2)	Oui	Oui *1)	Oui *1)
SR32i	Oui	Oui	Non	Non	Non
1) Fonctionnalité sans fil (RF30) non disponible. 2) Concentrateur de segments ne possédant pas de relais totalisateur (d'alarme commune).					

Pour mettre à jour vers la version la plus récente du logiciel, procédez comme suit :

1. Si la version 4.7 (ou antérieure) du logiciel est installée sur le PC, vous devez préalablement remplacer tous les SR32i par des SR35i. Assurez-vous ensuite que la plate-forme du microprogramme des concentrateurs est de version 5. Pour ce faire, utilisez tout simplement le système de menus du concentrateur.
 - Si le menu permettant la commutation n'est PAS disponible sur le concentrateur, cela signifie que ce dernier a été mis à jour vers un microprogramme **prenant en charge les mises à jour à partir du PC**.
2. Insérez le CD dans le lecteur.
 - ⇒ L'assistant de mise à jour du logiciel apparaît.
3. Suivez les instructions qui s'affichent à l'écran. Choisissez Réparer.
4. Lancez le programme d'installation [→ 79].
 - ⇒ L'installation vérifie la version existante du logiciel et vous informe des éventuelles modifications matérielles requises (comme indiquées plus haut). Il se peut que vous soyez invité à mettre à jour certaines unités directement (certaines mises à jour s'avérant parfois obligatoires pour permettre la mise à jour globale du système). Les étapes à suivre s'apparentent à celles du contrôle de version du microprogramme SR35i [→ 124].
5. Effectuez les étapes suggérées dans cette séquence.
6. Vérifiez que les voyants lumineux EN LIGNE et BD A JOUR situés dans le coin inférieur droit des fenêtres de SiPass Entro sont verts.
 - ⇒ Le système SiPass Entro est désormais mis à jour vers la nouvelle version et prêt à exécuter de nouvelles fonctionnalités !



Lors de la mise à niveau de la version 4.x à 5.0 (ou ultérieure), les "connexions" disparaissent et doivent être recréées.

27.5 Installation d'un PC supplémentaire ou de remplacement

SiPass Entro 5.3 et les versions ultérieures permettent à plusieurs PC d'administrer le système simultanément :

- Si un seul PC est utilisé, l'onglet "Connexions" n'est pas affiché dans le programme d'installation.
- Si plusieurs PC sont en ligne simultanément, l'onglet "Connexions" affiche différents noms.

Avant de commencer

Quelle que soit l'option choisie parmi les choix ci-dessus, le nouveau PC doit remplir certaines conditions :

- Vous devez disposer d'une **licence du logiciel** SiPass Entro supplémentaire pour le second PC.
- Le programme SiPass Entro doit être installé sur un PC dont les **paramètres réseau** sont correctement configurés pour la connexion LAN.
- Une **clé de cryptage correcte** doit être installée sur le PC. Si la clé de cryptage par défaut a été préalablement modifiée, prenez soin d'en noter la nouvelle valeur et de garder celle-ci à disposition.
- Lorsque vous installez un **nouveau** PC, il est préférable d'utiliser un ordinateur sur lequel aucune base de données ou logiciel SiPass Entro n'a été préalablement installé(e).



Si vous envisagez de remplacer le PC exécutant SiPass Entro (par exemple, dans le cadre d'une migration vers Vista), une mise à jour du logiciel SiPass Entro peut s'avérer nécessaire. Si tel est le cas (lorsque vous devez remplacer le PC ET mettre à jour le logiciel SiPass Entro), notez qu'il convient de procéder en premier à la mise à niveau du système SiPass Entro et ce, **à partir de l'ancien PC**. Ceci fait, le remplacement du PC peut avoir lieu.

27.5.1 Préparation de la base de données pour le PC existant

Procédez comme suit :

1. Lancez le programme d'installation [→ 79] sur un PC fonctionnant correctement.
2. Activez l'onglet **Connexions** sous **Système > Propriétés du système**, puis sélectionnez l'option de connexion simultanée de plusieurs ordinateurs.
3. Cliquez sur OK.
 - ⇒ Un nouvel onglet s'affiche dans la fenêtre principale du programme d'installation. La connexion par défaut, préalablement masquée, est à présent affichée comme connexion n° 1. Modifiez son nom avant de poursuivre. Pour ce faire, cliquez sur **Modifier** et saisissez un nom approprié.
4. Cliquez sur l'onglet **Connexions** et démarrez l'assistant en cliquant sur **Nouveau**.
5. Sélectionnez **Administration du système** et spécifiez les paramètres suivants :
 - **Nom de la connexion** : entrez le nom de votre choix.

- Choisissez un **SR35i**. Il est conseillé d'utiliser le même SR35i pour tous les PC, sauf si un port série (RS232) doit être utilisé dans le nouveau PC.
 - **Numéro de licence** : il s'agit du numéro pour le nouvel ordinateur. Il est indiqué sur le boîtier du CD de la nouvelle licence du logiciel.
 - **Type de communication** : TCP/IP, RS232 (ou modem).
- ⇒ Vous avez désormais créé une nouvelle connexion pour SiPass Entro et pouvez quitter le programme sur le PC existant.

27.5.2 Configuration d'un PC supplémentaire ou de remplacement

Etant donné que ce PC ne dispose pas encore d'une base de données et qu'il n'est pas encore capable de communiquer avec SiPass Entro, vous devez créer une *connexion* également dans ce PC.

1. Démarrez le **nouveau PC** et installez le logiciel SiPass Entro. **Remarque : vous devez disposer d'une licence du logiciel supplémentaire pour ce second PC.**
2. Ouvrez le programme d'installation et précisez au démarrage si vous souhaitez créer une **nouvelle connexion** (pour un nouveau PC) ou utiliser une **connexion existante** (pour un PC supplémentaire). Suivez les instructions qui s'affichent à l'écran (voir plus haut).

⇒ Vous avez désormais défini le mode de communication de l'ordinateur, défini le nom du système, les détails de connexion, etc.
3. Remarque : la connexion échouera si la clé de cryptage a été préalablement modifiée. Dans ce cas, effectuez également les étapes suivantes :
 - Ouvrez l'application Entro (HORS-LIGNE).
 - Saisissez manuellement les 32 caractères de la clé de cryptage (dans le menu Système).
 - Fermez l'application SiPass Entro complètement en cliquant avec le bouton droit de la souris sur les icônes et sélectionnez **Quitter** (la clé de cryptage sera stockée dans la base de données de ce PC).
 - Lancez de nouveau le programme d'installation. La clé de cryptage est chargée et la connexion est établie.
4. Patientez pendant la mise à jour de la base de données (jusqu'à ce que les icônes passent au vert).

27.6 Installation d'un SR35i supplémentaire ou de remplacement

Suivez cette procédure si vous souhaitez ajouter un concentrateur supplémentaire ou en remplacer un existant, en cas de dysfonctionnement ou afin d'accroître la capacité.

Vous pouvez configurer un SR35i de différentes manières avant de le connecter à un système. Parfois, la méthode la plus simple consiste à utiliser un port RS232.

N'oubliez pas que le SR35i dispose de commandes de menu intégrées permettant de vérifier et de modifier les différents paramètres.

Avant de commencer

- Prenez soin d'éviter tout risque de décharge électrostatique (ESD).
- Veillez à **effacer les données du concentrateur** (en retirant la pile, par exemple).

- Assurez-vous que la **batterie n'est pas vide**, particulièrement si vous projetez d'éteindre et de déplacer le concentrateur après la programmation.
- Vérifiez que vous disposez de toutes les informations relatives aux paramètres du système. Vous devez également connaître le *nom du système* (dans le cas d'une configuration de PC).

Il est primordial que les paramètres suivants soient configurés correctement :

- **Adresse de nœud** (à l'aide de roues codeuses)
- **Paramètres réseau** (adresse IP, masque de réseau et passerelle)
- **Clé de cryptage**

Lorsque la clé de cryptage par défaut est utilisée, l'application logicielle vous aide à "rechercher" un nouveau (nœud) SR35i dans certaines solutions de gestion réseau. Pour que l'application détecte ce nœud, celui-ci doit faire partie du même "sous-réseau" que le PC (qui envoie une requête au démarrage du programme d'installation). Si un nœud SR35i est détecté, vous pouvez l'ajouter et le configurer à l'instar de tous les autres concentrateurs.

Si les conditions précitées ne sont pas remplies, procédez comme suit :

1. Sélectionnez l'**adresse** sur le nouveau SR35i et mettez ce dernier sous tension.
2. Définissez les **paramètres réseau** (par exemple, l'adresse IP) à l'aide du **clavier** et de l'écran. (Vous serez amené plus tard à effacer la mémoire du SR35i.)
3. Si la **clé de cryptage** a été préalablement modifiée dans le système, vous devez **restaurer temporairement sa valeur par défaut** (c.-à-d., la valeur initialement définie sur le SR35i lorsqu'il vous a été livré). Si vous omettez de la restaurer, le concentrateur ne sera pas en mesure de communiquer. Dans l'application Entro, choisissez l'option **Modification de la clé de cryptage** du menu **Système**.
4. Branchez le câble réseau et lancez le programme d'installation.
 - ⇒ Le nouveau concentrateur est détecté par le logiciel et est affiché (**Cxx). La base de données et la clé de cryptage sont transmises ou vérifiées de l'ordinateur au concentrateur. Sachez que les pare-feux et autres composants peuvent nécessiter la configuration manuelle de certains SR35i (**Cxx non affiché).
5. Modifiez le **nom** et définissez les **paramètres** de ce concentrateur.
6. Patientez pendant la mise à jour de la base de données (jusqu'à ce que les icônes passent au vert).
7. N'oubliez pas de modifier la **clé de cryptage** et de prendre note de cette dernière.

27.7 Installation de lecteurs supplémentaires

Il est très simple d'installer des lecteurs supplémentaires sur le système. Il vous suffit de disposer du câblage nécessaire et de vous assurer des points suivants :

- Un DC12 ou un DC22 est disponible pour le lecteur
- Le SR35i hôte dispose de suffisamment de capacité d'adressage.
- La capacité d'alimentation électrique est suffisante.
- Les résistances de terminaison de bus RS485 sont installées correctement.

27.8 Contrôle de version du microprogramme SR35i

Suite à un développement ou à une mise à niveau du système, il arrive parfois que l'exécution d'un correctif du microprogramme s'avère nécessaire dans les concentrateurs de segments. Dès que le programme d'installation est en ligne avec le système, il vérifie la version du microprogramme et informe l'utilisateur si une mise à jour est requise.

Le programme d'installation propose des fonctions qui permettent de contrôler le mécanisme de correction des concentrateurs de segments. L'état des différentes unités est affiché.

Le temps estimé est également affiché pour tous les concentrateurs, et pas seulement pour celui connecté au PC.



Le téléchargement utilise les fichiers existants stockés dans le dossier programme d'Entro (fichier de type "SR_firmware.hex"). Il est possible de télécharger une version plus ancienne.

Suivez la procédure suivante pour les actions qui vous intéressent :

1. Lancez le programme d'installation [→ 79].
2. Choisissez **Système > Informations système**.
 - ⇒ Tous les concentrateurs sont répertoriés à l'écran, affichant l'état des différentes unités (adresse, produit, version, niveau de tension). Si la communication avec l'un des concentrateurs échoue, l'unité correspondante est marquée d'une croix.
3. Cliquez sur **Mettre à jour le microprogramme** et sélectionnez la version à télécharger.
4. Cliquez sur **Suivant** et indiquez le concentrateur à mettre à jour. **Nous vous recommandons vivement de ne mettre à jour qu'un seul concentrateur à la fois !**
5. Cliquez sur **Terminer**.
 - ⇒ Une barre de progression est affichée pour chaque concentrateur, indiquant le temps restant.
6. Vous pouvez annuler l'opération à tout moment en cliquant sur **Annuler la mise à jour**.
 - ⇒ La mise à jour n'est pas effectuée et l'ancienne version reste intacte.

27.9 Enregistrement/restauration de la base de données sur CF8

La base de données SiPass Entro est généralement stockée sur tous les PC et concentrateurs de segments.

L'installateur peut également faire appel au système de menus du SR35i (SR34i) pour stocker ou réenregistrer la base de données depuis/vers une carte mémoire flash CF8. Utilisez cependant cette méthode **avec précaution**, car elle est considérée comme une opération d'urgence.

Seules les personnes compétentes et familières à l'utilisation du logiciel SiPass Entro sont habilitées à suivre cette procédure. En cas de doute, veuillez contacter le support technique.

27.10 Contrôle du microprogramme du central de porte

Si les centraux de porte DC12/DC22 et le PD40-EM/PD40-EM disposent d'un microprogramme dont la **version est 1.20** ou ultérieure, le programme d'installation peut télécharger les nouvelles versions du microprogramme via le bus système. Pour ce faire, assurez-vous que les unités sont en ligne.



Au cours du téléchargement, la porte est déverrouillée si le Niveau de sécurité en mode Autonome le prévoit. Toutes les autres sélections entraînent le verrouillage de la porte.

27.11 Imprimé de la configuration du système

Dans le programme d'installation, vous avez la possibilité de générer une vue graphique des composants installés afin de faciliter le contrôle de divers éléments comme, par exemple, les versions de microprogramme existantes. Pour ce faire, procédez comme suit :

1. Lancez le programme d'installation [→ 79].
2. Choisissez **Système > Informations système**.
3. Cliquez sur **Enregistrer sous** : une image au format JPG est enregistrée sur le disque.

27.12 Migration d'un système Entro Lite

Lorsque vous procédez à la migration d'un système SiPass Entro Lite, veuillez prendre les points suivants en considération :

- La base de données utilisée dans SiPass Entro Lite permet de définir des **noms de détenteurs de carte** de plus de 50 caractères. Au cours de l'importation vers SiPass Entro, seuls les 32 premiers caractères sont pris en compte.
- Si une **alarme agression** est prévue (dans le concentrateur DC800), cette fonction doit être "déplacée" vers un contrôleur de relais IOR6 [→ 95] et SiPass Entro doit être configuré à cet effet. Cette condition s'applique même si le DC800 est toujours utilisé comme central de porte dans le nouveau système.
- Aussi, même si la fonction d'alarme est utilisée, une reconfiguration de la solution doit être envisagée.

27.13 Désinstallation d'Entro

Désinstallez SiPass Entro à l'aide du système Windows. Le logiciel ne dispose pas d'une option de menu spéciale permettant la désinstallation.

Une fois la désinstallation terminée, les fichiers suivants sont conservés pour référence future. Si vous préférez supprimer complètement le logiciel, procédez comme suit :

1. Accédez au dossier du profil utilisateur de Windows. Par exemple, sous Windows XP, il s'agit du dossier suivant : C:\Documents and Settings\[Utilisateur].
2. Supprimez tous les fichiers SiPass Entro se trouvant dans le dossier "Application data" (dbpath.ini, entro.ini, fichiers des événements et de base de données).

3. Accédez au dossier C:\Program files\Fichiers communs.
4. Supprimez le dossier "Bewator USB" ainsi que son contenu.

28 Questions fréquentes

28.1 Informations détaillées sur les réseaux locaux (LAN)

Le chapitre suivant comporte des questions et réponses relatives à l'utilisation de SiPass Entro en réseau local et s'adresse principalement aux responsables des parcs informatiques.

Comment se présente le volume du trafic en cas d'utilisation d'Entro en réseau local TCP/IP ?

SiPass Entro/TCP a évolué avec RS485. Tant que la base de données est compacte, le trafic reste relativement modéré. Le SR35i dédié au trafic met à la disposition de chaque concentrateur un socket ouvert, testé toutes les huit secondes à l'aide d'un message ping. Vous remarquerez qu'il ne s'agit pas d'un message ping ICMP, mais plutôt d'un paquet TCP/IP courant comportant des données (de seulement quelques octets).

En outre, dans un système en inactivité, une comparaison des messages de base de données est effectuée au niveau du nœud environ toutes les neuf secondes. Le temps exact varie en fonction de la configuration. Par exemple, une application à petite échelle pourra effectuer ce test toutes les six secondes. Le message à proprement dit est court (environ 40 octets, auxquels s'ajoute la longueur de l'en-tête). Voir le point 2.

Quels types de messages sont transmis lorsqu'un événement se produit ou qu'un détenteur de carte est créé ? Quelle est la taille des paquets envoyés ?

Actuellement, la taille des paquets est de 407 octets (auxquels s'ajoutent les en-têtes TCP et IP, plus un hachage MD5 du message). La taille totale est inférieure à 500 octets. Lorsqu'un événement se produit (par exemple, lorsqu'un accès est concédé), des données d'environ 40 octets sont envoyées. La création d'un nouveau détenteur de carte entraîne une mise à jour de la base de données (avec une structure de 80 octets et une structure de 10 octets).

A quelle fréquence les SR35i communiquent-ils entre eux ?

Au moins toutes les 6 à 8 secondes.

A quelle fréquence le SR35i envoie-t-il une demande au serveur horaire ?

Toutes les 23 heures.

Que se passe-t-il si le SR35i perd la base de données et télécharge des informations à partir d'un autre SR35i ? Les performances du réseau local sont-elles affectées ?

Non, car seule une fraction de la capacité totale est utilisée. SiPass Entro fait appel à un faible pourcentage des capacités du réseau local (10/100 Mbit/s) auquel il est raccordé. En effet, l'objectif principal de SiPass Entro étant la gestion rapide des demandes d'accès, la communication n'a pas la priorité de tâche. En outre, l'utilisation conjointe des algorithmes de cryptage RC4 à 128 bits et d'authentification MD5 consomme l'alimentation de l'UC et ralentit la vitesse de communication. Il convient cependant de souligner que les réseaux locaux modernes font souvent appel à des commutateurs qui n'ont aucune influence négative sur la vitesse.

Est-il possible de modifier le port IP utilisé par le système (par exemple, si les ports 4001 et 4002 sont utilisés par une autre application) ?

Seul le port 4002 est utilisé pour la communication avec le PC (et risque d'entrer en conflit avec d'autres applications sur le même PC). Cela dit, il ne vous est pas possible de changer le port. Un risque de conflit est considéré comme minime. Il va

de soi que si vous rencontrez un problème, nous nous appliquerons à le résoudre. A l'heure actuelle, aucune application connue n'utilise ce port.

Comment le trafic est-il affecté ? Avez-vous testé l'utilisation de "renifleurs" ?

Au cours de la phase de développement, nous avons évidemment utilisé différents "renifleurs" (trois commerciaux et un développé par nos soins). Nous avons également testé les effets de l'envoi de grosses quantités de données sur la bande passante vers les SR35i en utilisant celle-ci à 100 %. Avec les protocoles UDP et TCP. Ceci n'est toutefois pas comparable à un réseau local à 100 Mbit/s.

Pourquoi ne pas utiliser un réseau local virtuel (VLAN) ?

Le réseau VLAN constitue une bonne alternative pour la création d'un réseau plus sécurisé. Cependant, il est difficile de fournir des recommandations d'ordre général aux utilisateurs sur la création d'un réseau local propre.

Dans un environnement SiPass Entro communiquant via TCP/IP, le trafic sur le réseau ne justifie pas l'utilisation d'un réseau virtuel VLAN. En règle générale, nous recommandons aux responsables des parcs informatiques d'utiliser plutôt des commutateurs LAN avec SiPass Entro.

Les fichiers de base de données peuvent-ils être placés sur un serveur de réseau local afin de planifier des sauvegardes de nuit ?

Vous pouvez effectuer des sauvegardes centralisées de trois manières différentes :

1. Chaque utilisateur modifie le chemin consigné dans le fichier dbpath.ini (situé sur le PC local) afin de stocker les fichiers de base de données dans un dossier unique qui lui est attribué sur le serveur (et non sur le PC local). Bien entendu, le serveur doit être exécuté sans interruption. Cette solution suppose également la connexion au système SiPass Entro par les différents utilisateurs.
2. Une autre possibilité consiste à utiliser la version terminal serveur/client de SiPass Entro, celle-ci permettant de gérer les fichiers et la connexion de manière centrale.
3. En cas de l'utilisation conjuguée d'un domaine Windows et du stockage des profils sur un serveur, la base de données est stockée automatiquement sur un partage de serveur à chaque déconnexion du PC.

SiPass Entro intègre la redondance au niveau de la base de données, toutes les données étant stockées sur chaque SR35i (à l'exception des événements qui se trouvent sur le PC).

La communication dans Entro est-elle sécurisée ?

Dans SiPass Entro, toute communication fait l'objet d'un cryptage renforcé. A l'heure actuelle, l'algorithme RSA RC4 à 128 bits est utilisé. Il s'agit du niveau de sécurité utilisé par la plupart des banques. La clé de cryptage peut être modifiée facilement. Dans les applications Internet, le responsable du parc informatique peut accroître la sécurité en augmentant la configuration du cryptage sur le réseau local. En outre, les nom d'utilisateur et mot de passe sont également vérifiés au moment de la connexion, de même que le nom du système.

Qu'est-ce que l'algorithme RSA RC4 ?

RC4 est une méthode de cryptage symétrique, développée par RSA Security. Cette méthode est utilisée depuis de nombreuses années et sa fiabilité est reconnue. SiPass Entro fait appel au cryptage renforcé à 128 bits.

N'oubliez pas cependant qu'on ne peut pas comparer des algorithmes de cryptage en considérant uniquement leur nombre de bits. A chaque méthode de cryptage correspond en effet un niveau de sécurité différent. SiPass Entro fait appel à une méthode symétrique qui ne peut être comparée à la méthode asymétrique (basée sur des clés publiques) utilisée par les logiciels de courrier électronique (généralement PGP ou similaire). Cette méthode requiert généralement une clé de plus grande taille pour remplir les besoins de sécurité.

Qu'est-ce que MD5 ?

MD5 est un algorithme permettant de confirmer des messages et connexions. Cette méthode est utilisée dans SiPass Entro afin de garantir que tous les messages arrivant à destination sont corrects. Elle permet également de conférer un niveau de sécurité supplémentaire lors des connexions via un navigateur Web sur le système de réservation.

28.2 Quel est le niveau de redondance du système ?

Le système est considéré comme très sûr. Les éventuels problèmes rencontrés surviennent généralement au cours des procédures d'installation et de programmation (ou sont consécutifs à un mauvais planning).

Si toutefois une panne venait à se produire, le système SiPass Entro met à votre disposition une gamme de solutions techniques visant à faciliter les opérations de dépannage et de réparation. Par exemple, la prise en charge de borniers intermédiaires amovibles ou la possibilité de changer des pièces alors que le système est en cours d'exécution (une maintenance Plug-and-Play, en quelque sorte).

Dans des conditions de prévention normales, SiPass Entro (avec ses fonctions de contrôle intégrées et intelligence distribuée) constitue une alternative très intéressante, offrant un niveau de redondance satisfaisant à un prix raisonnable.

Pourquoi utiliser des batteries de secours (blocs d'alimentation) ?

L'une des meilleures solutions de prévention contre les pannes, etc., consiste à installer suffisamment de batteries de secours. Pour que ceci soit possible, il est évidemment primordial de planifier soigneusement le nombre de portes, les types de verrous, les distances, les types de câbles, etc.

Si possible, l'utilisation d'un bloc d'alimentation pour chaque SR35i (et ses portes) est préconisée. Ceci permet en premier lieu de mettre en place une installation "plus propre", et en second lieu de connecter un signal émis en cas de panne de courant par le bloc d'alimentation du système via une unité IOR6. De cette manière, chaque segment du système peut être contrôlé séparément et générer un événement alarme (envoyé au PC et/ou à un système d'alarme externe via IOR6) en cas de chute de tension du secteur.

Que se passe-t-il en cas de brève interruption de communication avec un SR35i ?

Chaque SR35i possède une copie intégrale de la base de données résidant sur le PC (mise en miroir). Si la communication est interrompue (par exemple, si les données en mémoire sont corrompues), les données sont récupérées automatiquement par téléchargement, tant que le matériel est intact. Un signal d'alarme interne est transmis au PC connecté et/ou à un système d'alarme externe (via IOR6).

Que se passe-t-il en cas de défaillance d'un SR35i ?

Etant donné qu'il est possible d'isoler les SR35i, la communication (globale) supérieure devrait continuer à fonctionner normalement (tant que l'alimentation en courant n'est pas interrompue). Si l'environnement de porte inclut un DC22/DC12 (avec une mémoire), le mode Autonome est activé et les décisions relatives aux accès sont prises localement. Les autres portes (sans DC22/DC12) peuvent être verrouillées et déverrouillées. Lorsque le SR35i défaillant est remplacé, les données sont automatiquement téléchargées à partir d'un autre SR35i (ou du PC). Les fonctions d'événements sous alarme sont également restaurées.

Que se passe-t-il en cas de défaillance d'un lecteur ou d'un central de porte ?

Dans la plupart des cas, les autres portes contrôlées par le même SR35i seront toujours en mesure de fonctionner. Un événement alarme est envoyé vers l'unité SR35i matérielle en cas d'interruption de la communication avec le central de

porte. Si la défaillance provient d'un lecteur, un message signalant le problème s'affiche dans la fenêtre des informations système.

Que se passe-t-il en cas de défaillance d'un câble ?

Si un arrêt de la communication globale (entre les concentrateurs de segments SR35i) est engendré, les différents SR35i émettent respectivement un événement de type alarme. Les portes peuvent continuer à fonctionner normalement.

Si un arrêt de la communication locale (entre un SR35i et une porte) est engendré, l'unité SR35i matérielle en question génère un événement de type alarme. Les portes passent en mode Autonome et certaines d'entre elles peuvent concéder l'accès (selon les paramètres définis dans le logiciel).

Un arrêt de la communication avec le PC a le même effet que la mise hors tension du PC, c'est-à-dire que toutes les données sont stockées sur le système (en même temps qu'un certain nombre d'événements). Lorsque la communication est rétablie avec le PC (lorsque celui-ci est reconnecté au système), tous les événements sont transférés automatiquement.

29 Récapitulatif des informations importantes

Informations importantes relatives au système de contrôle d'accès

Même si vous avez modifié l'une des informations suivantes, complétez les champs ci-dessous et conservez-les en lieu sûr. Ces informations seront requises pour modifier le système.

Nom du système :

--

Clé de cryptage de 4 x 8 chiffres (0 à 9, A à F) :

--	--	--	--

Mot de passe du programme d'installation :

Nom :
Mot de passe :

Mot de passe de l'utilisateur système :

Nom :
Mot de passe :

Ordinateurs et connexions

Nom :	Numéro de licence :	Connexion :
		<input type="checkbox"/> TCP/IP <input type="checkbox"/> RS232
		<input type="checkbox"/> TCP/IP <input type="checkbox"/> RS232
		<input type="checkbox"/> TCP/IP <input type="checkbox"/> RS232
		<input type="checkbox"/> TCP/IP <input type="checkbox"/> RS232
		<input type="checkbox"/> TCP/IP <input type="checkbox"/> RS232

Index

A

adresse IP, 89
adresse MAC, 52, 53
adresses IP statiques, 51
agent de sous-réseau, 52
Alarme agression, 85
alarme par impulsion unique, 93, 100
alimentation, 39
antipassback, 43, 44, 103, 103
ASF, 46, 101
AX, 73

B

BAPSI, 33
base de données, 24, 57, 121, 124
bloc d'alimentation local, 40
blocs d'alimentation, 40

C

carte mémoire, 30
CCTV, 10
central de porte, 93
CF8, 67, 124
chaîne d'initialisation, 63
chute de tension, 77
clé de cryptage, 119
clé de cryptage par défaut, 119
client, 25
code personnel, 84
Confirmation, 117
connecteur de porte, 43
connecteurs de porte, 93
connecteurs de verrou, 93
Connexions, onglet, 57, 69, 121
contrôle d'accès, 10
contrôle de l'accès aux portes, 10
contrôle du verrou, 95
CX, 75

D

DC800, 125
débit, 114
délai d'annulation, 110
délai de chevauchement, 110

Délai maxi de réservation, 110
désinstaller, 125
détection des unités, 59
développement, 119
DHCP, 51, 90, 92
DNS, 51
DNS dynamique, 51
DVR, 32, 68, 68
DynDNS, 53, 53

E

Entro, 10
Entroser, 81
ESD, 122
Ethernet, 26
exécution d'un correctif, 124

F

Fonction Bistable, 101

G

gestion d'ascenseurs, 98
gestion des appareils, 31

H

horloge, 68
HTML, 67

I

impression de cartes, 10
imprimante, 49
InfoPoint, 10, 30
interface de lecteur, 93
intrusion, 10, 45, 46
IOR6, 98

L

lecteur ENTRY, 44
lecteur EXIT, 44
lecteurs, 123
licence, 24, 121, 122
limitation de l'accès, 104
logiciel de visualisation, 68

M

masque de réseau, 89



message électronique, 114
microprogramme, 124
modem, 62, 62
Modem, 61
mot de passe, 79
multi-utilisateur, 60
MX, 72

N

nom d'utilisateur, 79
numéro de licence, 60

O

objet de réservation, 107, 109
objet groupé, 108
ouverture d'urgence, 97

P

panne de courant, 96
paramètres de lecteurs de carte, 84
pare-feu, 55
passerelle, 89
ports, 52, 69
prise murale, 49
programme d'installation, 10

R

relais totalisateur d'alarme commune, 95
réservation, 10, 30
réservations simultanées, 110
résistance de terminaison, 77
routeur, 52
RS232, 49, 86
RS485, 26

S

sans fil, 30
serveur, 25
serveur de messagerie, 90
serveur horaire externe, 83
serveur Web, 30
SISTORE, 32, 68, 68
SNTP, 83
SR34i, 120
SR35i, 86, 120

T

TCP/IP, 26, 86

téléchargement, 125
Terminal Server 2008, 25
Type du DVR, 69

V

voyant, 85

W

Wiegand, 93

Z

zone de verrouillage, 104
zone sous alarme, 100
zones sous alarme, 45

Edité par
Siemens AB
Infrastructure & Cities Sector
Security Products
International Headquarters
Englundavägen 7
SE-171 41 Solna
Tel. +46 8 629 0300
www.siemens.com/securityproducts

© 2013 Copyright Siemens AB
Sous réserve de disponibilité et de modifications techniques.