

# LSM 3.5 SP3 Business + Prof. SmartUserGuide

Manuel

12.12.2023

## Tables des matières

<b>1. Généralités.....</b>	<b>5</b>
1.1 Consignes de sécurité générales .....	5
1.2 Consignes de sécurité propres au produit.....	6
1.3 Informations légales .....	6
1.4 Exigences système .....	7
1.5 Informations relatives au manuel .....	8
1.6 Protection des données dans le système 3060.....	9
1.6.1 Protection informatique de base .....	9
1.6.2 Chiffrement.....	9
<b>2. Signification du formatage du texte.....</b>	<b>10</b>
<b>3. Fonctions de base .....</b>	<b>11</b>
3.1 Créer une nouvelle installation de fermeture .....	11
3.2 Créer un nouveau groupe de transpondeurs .....	11
3.3 Créer un nouveau transpondeur .....	11
3.4 Attribuer ultérieurement un transpondeur à un groupe de transpondeurs .....	12
3.5 Créer un nouveau Secteur.....	12
3.6 Créer une nouvelle fermeture.....	12
3.7 Créer un clavier à Pin Code .....	12
3.7.1 Configurer le clavier à Pin Code .....	13
3.7.2 Créer un clavier à Pin Code dans le plan de fermeture .....	13
3.7.3 Programmer le clavier à Pin Code .....	14
3.8 Attribuer la fermeture à un domaine .....	14
3.9 Accorder/retirer autorisation .....	14
3.10 Configurer les composants DoorMonitoring .....	15
3.11 Niveau de fermeture transversal .....	15
3.11.1 Créer un niveau de fermeture transversal.....	16
3.11.2 Relier des fermetures.....	16
3.11.3 Relier des transpondeurs .....	17
3.11.4 Autoriser transpondeur .....	18
3.12 Créer un transpondeur sapeur-pompier .....	18
3.13 Sauvegarde manuelle de la base de données.....	19
3.14 Travaux conformes à la protection des données selon le RGPD.....	20
3.14.1 Exporter les données.....	20
3.14.2 Supprimer les données .....	22
3.14.3 Quelles données personnelles sont enregistrées dans le logiciel ?.....	24
3.14.4 À quelles fins les données personnelles sont-elles enregistrées dans le logiciel ?.....	25

3.14.5	Pendant combien de temps les données personnelles sont-elles conservées dans le logiciel ? .....	25
3.14.6	Les données personnelles enregistrées dans le logiciel sont-elles protégées contre l'accès par des tiers ?.....	25
3.14.7	Les données enregistrées peuvent-elles être mises à disposition sous la forme d'une copie ?.....	26
3.14.8	Les données personnelles peuvent-elles être supprimées du logiciel ?.....	26
3.15	Recherche dans la matrice.....	26
3.16	Exécuter des actions de groupe.....	27
3.17	Programmer le transpondeur.....	27
3.18	Programmer la fermeture .....	28
3.19	Programmer via LSM Mobile .....	28
3.19.1	Avec un ordinateur portable, un Netbook ou une tablette.....	29
3.20	Définir le plan des plages horaires (jours fériés et jours ouvrés).....	29
3.21	Réinitialisation de composants.....	31
3.22	Remplacer une fermeture défectueuse.....	31
3.23	Bloquer les transpondeurs.....	32
3.23.1	Bloquer le transpondeur en permanence et créer un transpondeur de remplacement .....	33
3.23.2	Bloquer temporairement le transpondeur .....	37
3.24	Vérifier et évaluer l'état des piles des fermetures.....	38
3.25	Réinitialiser le mode par défaut des fermetures G1 .....	40
3.26	Réinitialiser le mode freeze des fermetures G2.....	40
3.27	Gestion des listes d'accès.....	41
3.27.1	Listes d'accès.....	42
3.28	Gestion des utilisateurs .....	42
3.29	Gestion des cartes .....	43
3.29.1	Modifier la configuration.....	44
3.29.2	Vue d'ensemble.....	45
<b>4.</b>	<b>Réalisation de tâches standard basées sur WaveNet dans LSM .....</b>	<b>46</b>
4.1	Création d'un réseau radio WaveNet et connexion d'une fermeture .....	46
4.1.1	Préparer le logiciel LSM.....	46
4.1.2	Première programmation des composants de fermeture .....	46
4.1.3	Préparer le matériel .....	47
4.1.4	Créer des nœuds de communication.....	48
4.1.5	Paramétrer le réseau et l'importer dans le LSM.....	48
4.2	Mise en service du fermeture DoorMonitoring .....	50
4.2.1	États (de porte) possibles.....	50
4.2.2	Intégrer les fermetures DoorMonitoring dans le réseau.....	51

4.2.3	SmartHandle de DoorMonitoring.....	52
4.2.4	Cylindre de DoorMonitoring .....	54
4.2.5	Analyser les inputs du contrôleur.....	55
4.2.6	Transférer la configuration WaveNet .....	57
4.2.7	Attribuer un nœud de réseau à une fermeture.....	58
4.2.8	Activer les évènements Input de la fermeture.....	58
4.3	Paramétrer RingCast .....	58
4.3.1	Préparation du RouterNode pour le RingCast .....	59
4.3.2	Créer RingCast.....	61
4.3.3	Test de fonctionnement du RingCast.....	64
4.4	Configurer Eventmanagement (évènements) .....	68
4.4.1	Configurer le serveur e-mail.....	68
4.4.2	Configurer le service Task .....	68
4.4.3	Transférer les évènements Input via le nœud routeur 2.....	68
4.4.4	Transmettre les évènements Input via le système SREL3-ADV .....	69
4.4.5	Créer une réaction.....	71
4.4.6	Créer un évènement .....	71
4.5	Gérer le réseau virtuel (VN) .....	77
4.5.1	Réseau virtuel avec SmartRelais 3 Advanced.....	78
4.5.2	Réseau virtuel avec SmartRelais 2 G2.....	84
4.6	Lecture d'une fermeture .....	103
<b>5.</b>	<b>Aide et autres informations.....</b>	<b>108</b>

## 1. Généralités

Ce manuel décrit les fonctions du logiciel Locking System Management 3.5 SP3. Le logiciel Locking System Management, en abrégé logiciel LSM, a été développé pour gérer les installation de fermeture complexes à l'aide de composants de fermeture SimonsVoss.

Il existe également d'autres documents en complément de ce Manuel :

■ *Manuel WaveNet*

Décrit la manipulation du réseau radio WaveNet.

■ *SmartUserGuide SimonsVoss*

Mettre en œuvre les fonctions de base à l'aide du logiciel LSM.

■ *Manuel de mise à jour du logiciel LSM*

Décrit le processus de mise à jour des versions antérieures.

### 1.1 Consignes de sécurité générales

**Mot indicateur: Effets immédiats possibles du non-respect**

AVERTISSEMENT: Mort ou blessure grave (possible, mais improbable)

PRUDENCE: Blessure légère

ATTENTION: Dommages matériels ou dysfonctionnements

NOTE: Peu ou pas



#### AVERTISSEMENT

##### Accès bloqué

Toute erreur de montage et/ou de programmation d'un composant peut bloquer l'accès par une porte. La société SimonsVoss Technologies GmbH décline toute responsabilité quant aux conséquences d'un accès bloqué, par exemple, accès pour les personnes blessées ou en danger, dommages matériels ou autres dommages !

##### Accès bloqué par la manipulation du produit

Si vous modifiez vous-même le produit, des dysfonctionnements peuvent se produire et l'accès peut être bloqué par une porte.

- Ne changer le produit que lorsque cela est nécessaire et de la manière décrite dans la documentation.



#### NOTE

##### Utilisation conforme aux dispositions

Les produits SimonsVoss sont exclusivement destinés à l'ouverture et la fermeture de portes et d'objets similaires.

- N'utilisez pas les produits SimonsVoss à d'autres fins.

## Qualifications requises

L'installation et la mise en service nécessitent des connaissances spécialisées.

- Seul le personnel qualifié peut installer et mettre en service le produit.

Les modifications et nouveaux développements techniques ne peuvent pas être exclus et peuvent être mis en œuvre sans préavis.

La version allemande est le manuel d'instruction original. Les autres langues (rédaction dans la langue du contrat) sont des traductions des instructions originales.

Lisez et suivez toutes les instructions d'installation, d'installation et de mise en service. Transmettez ces instructions et toutes les instructions de maintenance à l'utilisateur.

---

## 1.2 Consignes de sécurité propres au produit

### PRUDENCE

#### Perte du mot de passe du système de fermeture

Le mot de passe du système de fermeture constitue l'élément central du concept de sécurité. La perte du mot de passe du système de fermeture restreint le fonctionnement du système de fermeture et compromet la sécurité.

1. Conservez le mot de passe du système de fermeture dans un lieu sûr (par exemple un coffre-fort) !
2. Le mot de passe du système de fermeture doit pouvoir être consulté à tout moment par les personnes autorisées.

---

## 1.3 Informations légales

Il est expressément mentionné à l'acheteur que l'utilisation du système de fermeture (par ex. avec fonctions de consignation des accès et DoorMonitoring) peut être légalement soumise à des obligations d'autorisation (en matière de protection des données) et à des droits de participation du personnel. La responsabilité pour l'utilisation conforme du produit est supportée par l'acheteur et respectivement le client et le consommateur final.

L'utilisation non conforme et respectivement inhabituelle qui ne constitue pas expressément des travaux de réparation ou des modifications de SimonsVoss Technologies GmbH ainsi que les services non professionnels, peuvent conduire à des problèmes de fonctionnement et sont donc interdits. Toutes les modifications non expressément autorisées par SimonsVoss Technologies GmbH entraînent la perte de tous les droits en responsabilité, en garantie et autres droits convenus.

## 1.4 Exigences système

Pour que la LSM fonctionne de manière fluide, SimonsVoss recommande de toujours utiliser un matériel performant et à jour au niveau des exigences système.

Pour la représentation de grands plans de fermeture composée de nombreuses fermetures, SimonsVoss recommande un écran haute résolution de 21" au minimum.

### Généralités

- Droits d'administrateur local pour l'installation
- TCP/IP  
(L'utilisation de l'agent d'événements nécessite NetBios.)
- LAN (min. 100 Mbit/s)
- Domaine Windows (non nécessaire pour les installation autonomes)
- Résolution de nom (non nécessaire pour les installation autonomes)
- .NET-Framework version 4.0 ou supérieure
- Interface(s) USB
- Pas de prise en charge des processeurs ARM sous le système 3060

### PC client

- Écran : Min. 48 cm (19")
- Résolution du moniteur : Min. 1024x768, recommandation 1280x1024 ou plus
- Processeur : Min. 2,66 GHz avec 2 cœurs ou plus (Intel/AMD)
- Mémoire vive : Min. 4 Go
- Capacité de disque dur : En fonction de la taille du système, min. 500 Mb  
(pendant l'installation env. 1 Go)
- Système d'exploitation Windows :
  - Windows 11 Professional, 64 bits
  - Windows 10 Professional, 64 bits

### Serveur

- Processeur : Min. 2,66 GHz avec 2 cœurs ou plus (Intel/AMD)  
(réseau virtuel avec SmartRelais 3 Advanced et VNHost : min. 4 cœurs, cadence en fonction du nombre de routeurs)
- Mémoire vive : Min. 4 Go

- Capacité de disque dur : Application env. 500 Mo  
(pendant l'installation env. 1 Go)  
Base de données en fonction du volume de données à traiter
- Serveur Windows :
  - Windows Server 2022
  - Windows Server 2019
- Environnements virtuels :
  - VMware ESXi (Version 7.0 U2) avec Windows Server 2022 et 2019
  - VMware ESXi (version 6.5.0) avec Windows Server 2019
- Si un serveur CommNode est utilisé : .NET-Framework version 4.0 ou supérieure
- Si une application sur serveur est utilisée. Autorisation sur le serveur Advantage Database pour un répertoire de base de données



#### NOTE

Consultez les notes de mise à jour du logiciel LSM pour savoir quelle version de LSM Mobile utiliser.

## 1.5 Informations relatives au manuel

Ce document décrit les fonctions du logiciel LSM. L'utilisateur peut ainsi programmer les composants de fermeture SimonsVoss et administrer l'installation de fermeture.



#### NOTE

Ce Manuel ne décrit pas le montage des composants de fermeture SimonsVoss. Pour ce faire, veuillez prendre consulter les notices abrégées et manuels des composants respectifs !

### Transpondeur

Dans le logiciel LSM, tous les supports d'identification (transpondeur, Tag, carte, etc.) sont en principe considérés comme des transpondeurs. La notion de « transpondeur » utilisée dans ce manuel couvre donc également tous les autres supports d'identification tels que les Tags et les cartes.

## 1.6 Protection des données dans le système 3060

Voir *Travaux conformes à la protection des données selon le RGPD* [▶ 20].

### 1.6.1 Protection informatique de base

#### 1.6.1.1 Quel est le niveau de protection des données traitées dans le système ?

En règle générale, seules les données non sensibles ayant des exigences de protection normales sont traitées et stockées dans le logiciel LSM. Ce sont donc des données dont la perte hypothétique ne nuit pas à la réputation d'une personne physique ni à l'image d'une entreprise. Aucune perte financière élevée n'est à prévoir.

#### 1.6.1.2 Quelles sont les exigences recommandées en matière d'infrastructure des technologies de l'information ?

Par conséquent, selon la CNIL, la protection informatique de base d'un système de fermeture SimonsVoss est suffisante comme concept de sécurité et remplit les exigences minimales recommandées pour votre infrastructure informatique.

### 1.6.2 Chiffrement

#### 1.6.2.1 Les données sont-elles cryptées dans le System 3060 ?

Oui. Les paquets de données sont chiffrés de bout en bout dans les communications propres au système. Avec les versions les plus récentes de nos produits, votre degré de sécurité augmente, car ces produits sont conformes aux dernières technologies. Des méthodes de cryptage à plusieurs niveaux sont utilisées (AES, 3DES).

#### 1.6.2.2 Quelles données sont cryptées ?

Dans le cadre de la communication propre au système, aucune donnée personnelle n'est traitée, mais les données sont pseudonymisées à l'aide de numéros d'identification. Même sans cryptage, il est impossible d'associer ces données à une personne réelle.

#### 1.6.2.3 Les voies de transmission, par exemple sans fil, sont-elles également cryptées ?

Non. Grâce au cryptage de bout en bout utilisé, aucun cryptage supplémentaire des voies de transmission n'est nécessaire.

## 2. Signification du formatage du texte

Pour faciliter la compréhension, cette documentation utilise du formatage de texte et des éléments de mise en page. Le tableau explique la signification des formatages de texte possibles :

<b>Exemple</b>	Bouton
<input checked="" type="checkbox"/> Exemple <input type="checkbox"/> Exemple	Checkbox
<input checked="" type="radio"/> Exemple	Option
[Exemple]	Registerkarte
"Exemple"	Nom d'une fenêtre affichée
Exemple	Barre de programmes supérieure
<b>Exemple</b>	Entrée de la barre de programmes supérieure déployée
<b>Exemple</b>	Entrée de menu contextuel
▼ Exemple	Nom d'un menu déroulant
"Exemple"	Sélection possible dans un menu déroulant
"Exemple"	Zone
Exemple	Champ
<i>Exemple</i>	Nom d'un service (Windows)
<i>Exemple</i>	commandes (par exemple, commandes CMD Windows)
<b>Exemple</b>	Entrée de base de données
[Exemple]	Sélection du type MobileKey

### 3. Fonctions de base

Ce chapitre décrit les processus essentiels du logiciel LSM. Dans le logiciel LSM, il existe souvent plusieurs moyens d'atteindre la fonction souhaitée. Ces fonctions de base montrent la plupart du temps le chemin le plus rapide et le plus court.

Le SimonsVoss SmartUserGuide décrit en détails à l'aide d'exemples simples, comment une installation de fermeture peut être créée et gérée.

#### 3.1 Créer une nouvelle installation de fermeture

- ✓ L'installation a été effectuée avec succès et une sauvegarde a été mise en place.
- 1. Dans la barre de menu, choisir *Éditer/Nouvelle installation de fermeture*.
- 2. Déterminer les différentes options de l'installation de fermeture.
  - ↳ Pour les niveaux de fermeture transversaux, choisir une couleur pour définir « En tant que niveau de fermeture transversal ». *Les niveaux de fermeture transversaux servent de niveaux supplémentaires par rapport aux installations de fermeture standard existantes. Voir Niveaux de fermeture superposés.*
- 3. Cliquez sur le bouton « Accepter ».
- 4. Cliquez sur le bouton « Terminer ».

#### 3.2 Créer un nouveau groupe de transpondeurs

- ✓ Une installation de fermeture a déjà été créée.
- 1. Dans la « Section groupe » du logiciel LSM, cliquer sur groupe de transpondeurs avec le bouton droit de la souris.
- 2. Cliquez sur « Nouveau ».
- 3. Donnez un nom au nouveau groupe de transpondeurs et le cas échéant, paramétrez-le.
- 4. Cliquez sur le bouton « Accepter ».
- 5. Cliquez sur le bouton « Terminer ».

#### 3.3 Créer un nouveau transpondeur

- ✓ Une installation de fermeture a déjà été créée.
- 1. Choisissez *Éditer/Nouveau transpondeur*.
- 2. Attribuez toutes les fonctionnalités et éventuellement d'autres paramètres à l'aide du bouton « Configuration ».
- 3. Cliquez sur le bouton « Enregistrer & Suivant ».
- 4. Cliquez sur le bouton « Terminer ».

### 3.4 Attribuer ultérieurement un transpondeur à un groupe de transpondeurs

- ✓ Le transpondeur a déjà été créé et un groupe de transpondeurs existe déjà.
- 1. Ouvrez les paramètres de l'installation de fermeture, par ex. à l'aide du bouton *Éditer/propriétés : installation de fermeture*.
- 2. Choisissez l'onglet « Transpondeur ».
- 3. Dans le tableau, sélectionnez le transpondeur qui doit être affecté à un groupe de transpondeurs.
- 4. Dans la liste déroulante, choisissez dans « Modifier l'affectation aux groupes de transpondeurs », le groupe de transpondeurs auquel le transpondeur doit être affecté.
- 5. Cliquez sur le bouton « Exécuter ».
- 6. Cliquez sur le bouton « Accepter ».
- 7. Cliquez sur le bouton « Terminer ».

*Lorsqu'un transpondeur est nouvellement créé, il peut être simultanément affecté à un groupe de transpondeurs existant.*

### 3.5 Créer un nouveau Secteur

- ✓ Une installation de fermeture a déjà été créée.
- 1. Dans la « Section Secteurs » du logiciel LSM, cliquer sur secteurs avec le bouton droit de la souris.
- 2. Cliquez sur « Nouveau ».
- 3. Donnez un nom au nouveau secteur et le cas échéant, paramétrez-le.
- 4. Cliquez sur le bouton « Accepter ».
- 5. Cliquez sur le bouton « Terminer ».

### 3.6 Créer une nouvelle fermeture

- ✓ Une installation de fermeture a déjà été créée.
- 1. Choisissez *Éditer/Nouvelle fermeture*.
- 2. Attribuez toutes les fonctionnalités et éventuellement d'autres paramètres à l'aide du bouton « Configuration ».
- 3. Cliquez sur le bouton « Enregistrer & Suivant ».
- 4. Cliquez sur le bouton « Terminer ».

### 3.7 Créer un clavier à Pin Code

Un clavier PinCode ne peut pas être utilisé dans une installation de fermeture G2 pure. Les trois User-Pins se comportent comme un transpondeur G1.

### 3.7.1 Configurer le clavier à Pin Code

#### Modification du Master-Pin

Cette étape doit être effectuée lorsqu'aucun nouveau Master-Pin n'a encore été programmé.

1. Saisie 0 0 0 0
2. Saisie de l'ancien Master-Pin : 1 2 3 4 5 6 7 8
3. Saisie du nouveau Master-Pin
  - ↳ Le nouveau Master-Pin doit contenir au moins 8 symboles qui ne doivent ni se suivre ni être identiques et il ne doit pas commencé par 0 !
4. Répétition de la saisie du nouveau Master-Pin



#### NOTE

Le Master-Pin est essentiel à l'utilisation du clavier à Pin Code et ne peut pas être lu ou restauré. Notez le Master-Pin et conservez-le dans un endroit sûr et secret. *Celui qui connaît le Master-Pin est en mesure d'ouvrir ou de bloquer les fermetures du clavier à Pin Code, en définissant lui-même de nouveaux Pins !*

#### Programmer le User-Pin

Jusqu'à trois User-Pins peuvent être attribués dans le clavier à Pin Code. La longueur du User-Pin peut être de 4 à 8 caractères qui ne doivent se suivre ou être identiques.

*Pour mieux comprendre : chaque User-Pin se comporte comme un transpondeur propre. C'est pourquoi, chaque User-Pin doit être programmé dans les transpondeurs (internes) respectifs (1, 2 & 3).*

1. Saisie 0
2. Saisie Master-Pin
3. Saisie User Pin - par ex. pour User-Pin 1
4. Saisie de la longueur du User-Pin - par ex. 4 pour un User-Pin de 4 caractères
5. Saisie User-Pin

Répétez la procédure afin de programmer d'autres user-Pins dans le clavier à Pin Code.

### 3.7.2 Créer un clavier à Pin Code dans le plan de fermeture

Il est nécessaire de créer un transpondeur propre à chaque User-Pin !

1. Dans la barre de menu, choisir *Éditer / Nouveau transpondeur*.

2. Dans la liste déroulante, choisissez « PinCode G1 » et saisissez les informations manquantes.
  - ↳ L'entrée peut ensuite être éditée et détaillée tout comme pour un transpondeur.
3. Choisir *Enregistrer & continuer*
4. Choisir *Terminer*

### 3.7.3 Programmer le clavier à Pin Code

1. LSM : Dans le plan de fermeture, cliquez sur Transpondeur/Pin Code avec le bouton droit de la souris et choisissez *Programmer*.
  - ↳ La fenêtre « Programmer transpondeur » s'ouvre.
2. Clavier à Pin Code : Saisie 0 0 + Master-Pin.
3. LSM : Choisir *Programmer*.
  - ↳ La programmation démarre.
4. Clavier à Pin Code : User-Pin par ex. 1 pour User-Pin 1 / presser transpondeur interne 1 dès que le LSM affiche le message « Appuyez maintenant 1 fois brièvement sur le bouton du transpondeur... ».
  - ↳ La programmation est maintenant terminée.

Répétez la procédure afin de programmer d'autres User-Pins dans le plan de fermeture.

### 3.8 Attribuer la fermeture à un domaine

- ✓ La fermeture a déjà été créée et un domaine existe déjà.
1. Ouvrez les paramètres de l'installation de fermeture, par ex. à l'aide du bouton *Éditer/propriétés : installation de fermeture*.
  2. Choisissez l'onglet « portes ».
  3. Dans le tableau, sélectionnez la porte qui doit être affectée à un secteur.
  4. Dans la liste déroulante, choisissez dans « Modifier l'affectation au secteur », le secteur auquel la porte doit être affectée.
  5. Cliquez sur le bouton « Exécuter ».
  6. Cliquez sur le bouton « Accepter ».
  7. Cliquez sur le bouton « Terminer ».

*Lorsqu'une fermeture est nouvellement créée, elle peut être simultanément affectée à un secteur existant.*

### 3.9 Accorder/retirer autorisation

Les autorisations peuvent être accordées ou retirées via la matrice. Dans le paramétrage de base, un clic sur le champ d'autorisation suffit pour modifier l'autorisation.

*Les autorisations peuvent seulement être accordées ou retirées entre une fermeture et un transpondeur.*

Veillez considérer les deux aperçus :

■ **Aperçu Portes/Personnes**

Dans cet aperçu, les autorisations du transpondeur souhaité peuvent être modifiées.

■ **Aperçu Secteurs/Groupes de transpondeurs**

Dans cet aperçu, les autorisations de groupes complets peuvent être modifiées.

### 3.10 Configurer les composants DoorMonitoring

La fonction DoorMonitoring est une fonction supplémentaire permettant d'afficher les états de la porte dans le logiciel LSM. Les SmartHandles et cylindres de fermeture avec fonction DoorMonitoring sont tout d'abord créés dans le logiciel LSM comme des composants de fermeture réguliers.

- Ajouter un nouveau cylindre de fermeture DoorMonitoring : Dans la liste défilante, choisir le type de fermeture « Cylindre DoorMonitoring G2 ».
- Ajouter une nouvelle SmartHandle DoorMonitoring : Dans la liste défilante, choisir le type de fermeture « SmartHandle DoorMonitoring G2 ».

#### **Onglet : Configuration/Données**

Effectuez les paramétrages suivants à l'aide du bouton « Configuration Monitoring ».

#### **Onglet : Statut DoorMonitoring**

Cet onglet affiche le statut actuel de la porte. Le statut actuel est affiché en temps réel.

*Afin que le statut affiché soit constamment actualisé, une connexion directe entre le logiciel LSM et le composant de fermeture (par ex. WaveNet) est requise. Pour plus d'informations concernant la mise en place d'un réseau radio WaveNet, veuillez consulter le manuel WaveNet.*

### 3.11 Niveau de fermeture transversal

Les niveaux de fermeture transversaux fonctionnent seulement avec des composants actifs. Les niveaux de fermeture transversaux peuvent seulement être réalisés lors de l'utilisation de technologie de cartes passive ou de SmartTags !

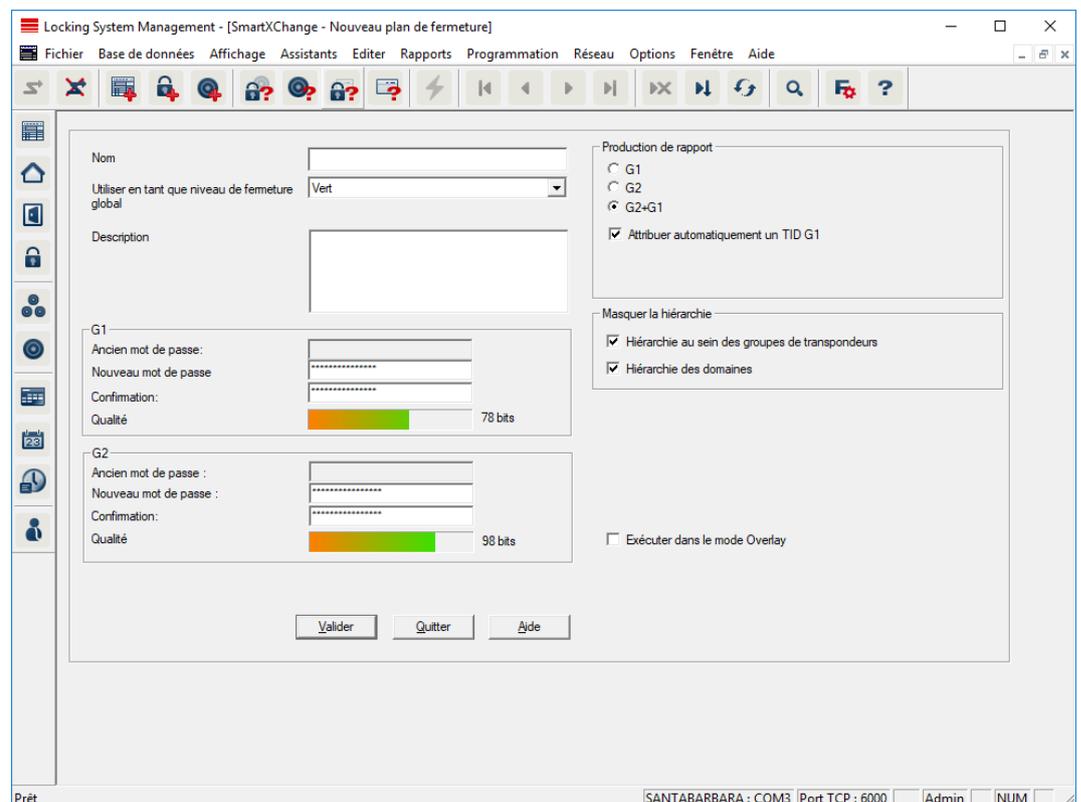
### 3.11.1 Créer un niveau de fermeture transversal

En présence de niveaux de fermeture transversaux, toujours veiller :

- à ce que les niveaux de fermeture transversaux disposent des mêmes générations de protocoles.
- Le niveau de fermeture rouge doit seulement être utilisé pour les pompiers ou autres forces d'intervention d'urgence puisqu'il a été spécialement optimisé pour ce genre d'utilisation.

Un niveau de fermeture transversal est créé comme une installation de fermeture, par ex. à l'aide du bouton « Nouvelle installation de fermeture » :

- Choisissez une couleur sous « Utiliser en tant que niveau de fermeture transversal ».

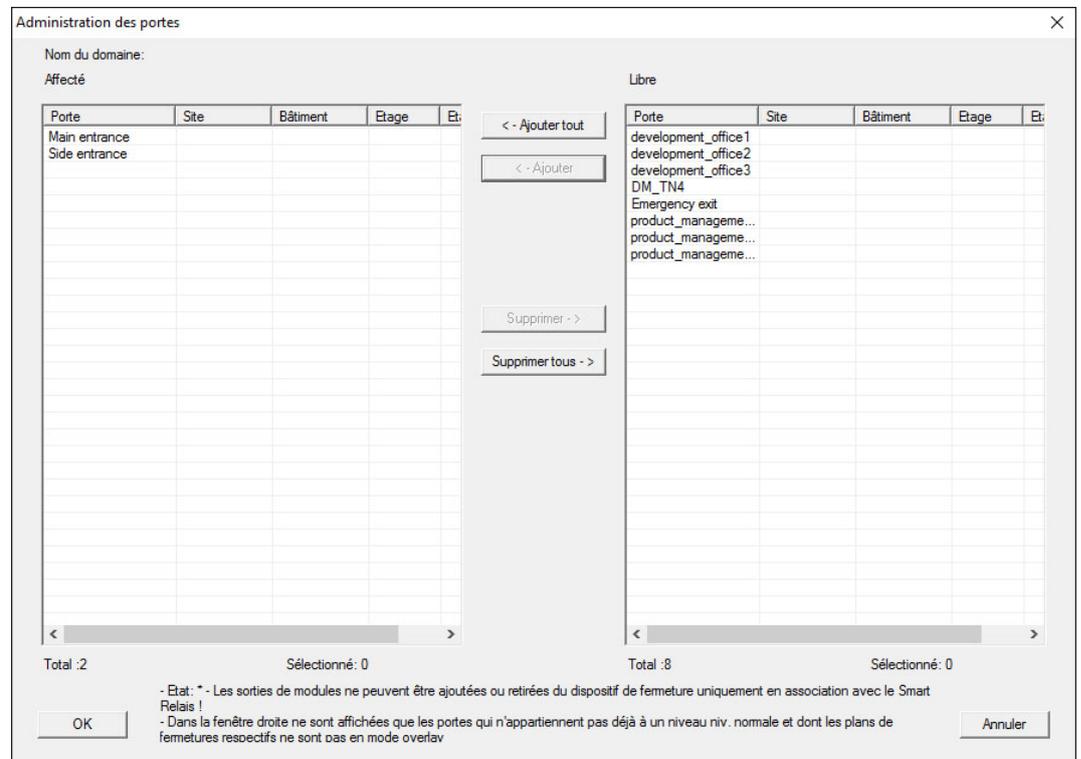


### 3.11.2 Relier des fermetures

- ✓ Un niveau de fermeture transversal a déjà été créé.

1. Dans le niveau de fermeture transversal, clic avec le bouton droit de la souris sur un champ et choisir « Propriétés ».
2. Choisir le bouton « Administration des portes ».

3. Dans le tableau de droite, toutes les fermetures de toutes les installations de fermeture sont affichées. Sélectionnez les fermetures souhaitées à l'aide du bouton « Ajouter ».

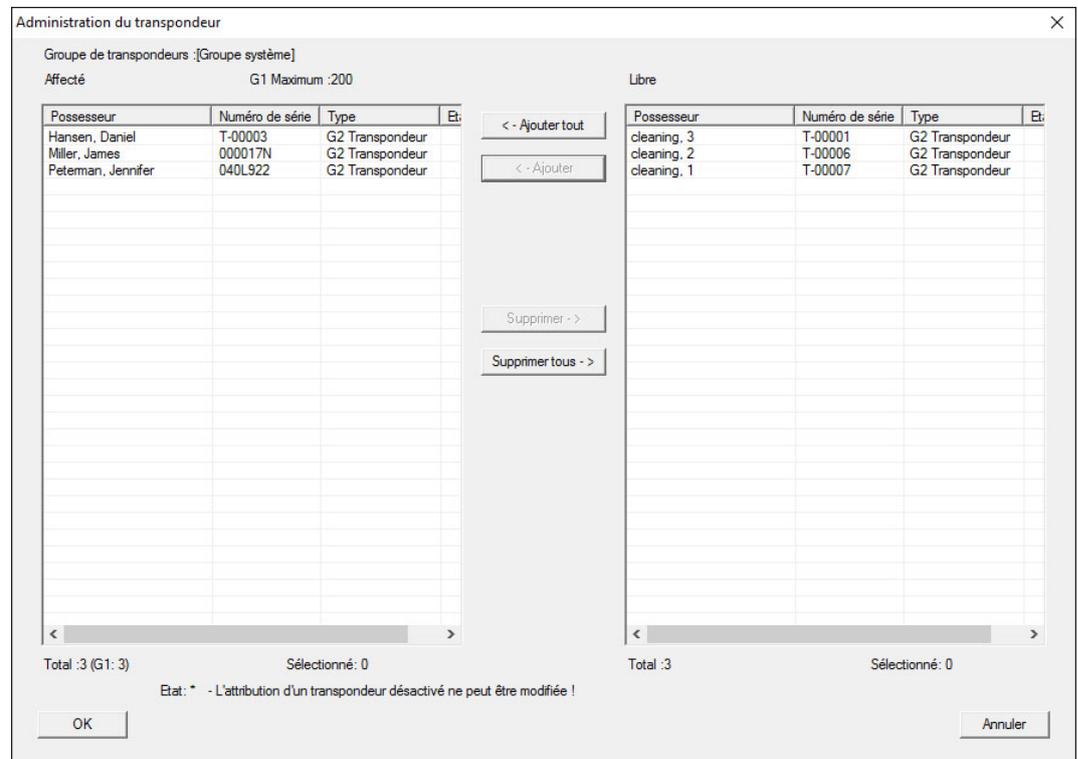


### 3.11.3 Relier des transpondeurs

*La mise en relation de transpondeurs ne doit avoir lieu que pour des niveaux de fermeture non transversaux.*

- ✓ Des transpondeurs ou groupes de transpondeurs ont déjà été créés.
1. Clic avec le bouton droit de la souris sur un groupe de transpondeurs et choisir « Propriétés ».
  2. Choisir le bouton « Automatique » lors de l'affectation des transpondeurs.

3. Dans le tableau de droite, tous les transpondeurs de toutes les installations de fermeture sont affichés. Sélectionnez les transpondeurs souhaités à l'aide du bouton « Ajouter ».



#### 3.11.4 Autoriser transpondeur

Tout comme dans chaque niveau de fermeture transversal, les groupes de transpondeurs choisis dans les « niveaux rouges » peuvent être autorisés à toutes les fermetures en seulement quelques clics. Cette fonction s'avère particulièrement utile pour les transpondeurs sapeur-pompier.

- ✓ Vous avez déjà créé un niveau de fermeture transversal de couleur « rouge ».
1. Ouvrir l'installation de fermeture supérieure rouge.
  2. Créer un groupe de transpondeurs qui est autorisé dans tous les secteurs pertinents pour les pompiers.
  3. Dans les propriétés du groupe de transpondeurs, cliquer sur le bouton « Autorisations ».
  4. Cocher tous les secteurs/fermetures souhaités afin d'autoriser le groupe de transpondeurs à toutes les portes.

#### 3.12 Créer un transpondeur sapeur-pompier

- ✓ Vous avez créé au moins une installation de fermeture.
1. Créez un nouveau niveau de fermeture transversal de couleur « rouge », par ex. via *Éditer/nouvelle installation de fermeture*.

2. Ajoutez un nouvel espace, par ex. « Toutes les fermetures » et attribuez-y toutes les fermetures souhaitées via « Gestion des portes ».
3. Créez un nouveau groupe de transpondeurs « Sapeur-pompier » dans le niveau de fermeture transversal.
4. Dans les propriétés du groupe de transpondeurs « Sapeur-pompier » cliquez sur le bouton « Autorisations ».
5. Activez la case « Toutes les installations » afin d'autoriser ce groupe de transpondeurs à chaque fermeture.
6. Enregistrer les paramètres en cliquant sur « OK ».
7. Créez un nouveau transpondeur (par ex. « Transpondeur Sapeur-pompier 1 ») dans le groupe de transpondeurs et programmez-le. *Toutes les fermetures doivent en outre être programmées. Prêtez attention au nouveau besoin de programmation en résultant.*

Le transpondeur de sapeur pompier créé dans cette étape est autorisé à toutes les fermetures. Même les fermetures désactivées peuvent (dans le niveau rouge) être ouvertes, ce qui constitue la différence essentielle par rapport aux niveau de fermeture transversaux « vert » et « bleu ».

### 3.13 Sauvegarde manuelle de la base de données

- ✓ Le LSM est ouvertes.
1. Sélectionnez l'entrée **Sauvegarde (Backup)** dans | Base de données |.  
↳ La fenêtre "Sauvegarde/Récupération" s'ouvre.

The screenshot shows a window titled "Sauvegarde/Récupération" with a close button (X) in the top right corner. The window is divided into two main sections: "Sauvegarde" and "Récupération".

**Sauvegarde section:**

- Base de données: \\vtl.6262\testdb\Korbinian\smdb\smdb.adb
- Répertoire pour sauvegardes: \\vtl\testdb\Korbinian\smdb\backup
- Buttons: "Utiliser le répertoire comme pré-configuration" and "Sécuriser"

**Récupération section:**

- Sauvegarde de la base de données: \\vtl\testdb\Korbinian\smdb\backup
- Répertoire pour récupérations: \\vtl\testdb
- Button: "Restaurer"

A "Quitter" button is located at the bottom right of the window.

2. Dans la zone "Sauvegarde", précisez quelle base de données doit être sauvegardée à quel endroit.
3. Cliquez sur le bouton **Sécuriser**.  
↳ Une sauvegarde es créée.

4. Cliquez sur le bouton **Quitter**.  
↳ La fenêtre "Sauvegarde/Récupération" se ferme.

### 3.14 Travaux conformes à la protection des données selon le RGPD

Le règlement général sur la protection des données est en vigueur depuis le 25 mai 2018. Il régit le traitement des données à caractère personnel afin de garantir leur protection et en même temps leur libre circulation sur le marché intérieur européen. Tout d'abord, l'accès à la base de données via l'interface utilisateur graphique est possible uniquement à l'aide d'un mot de passe et des droits d'utilisateur correspondants. En outre, aucune donnée à caractère personnel appartenant à une catégorie particulière selon l'article 9 du RGPD n'est enregistrée dans le logiciel LSM. Les champs obligatoires utilisés pour une personne servent exclusivement à l'attribution univoque de supports d'identification dans le plan de fermeture. Les données obligatoires sont nécessaires au système uniquement pendant la durée de possession d'un support d'identification (par exemple appartenance à une société). La durée de stockage des données dans les enregistrements peut être modifiée librement par l'administrateur du système de fermeture (voir Consignation).

#### 3.14.1 Exporter les données



#### NOTE

##### Texte en langue étrangère

La langue utilisée dans le LSM sera la même dans les textes des fichiers exportés.

##### Personnes

Vous pouvez exporter les données à caractère personnel des personnes de l'installation de fermeture en tant que fichier CSV. Trois fichiers sont alors générés :

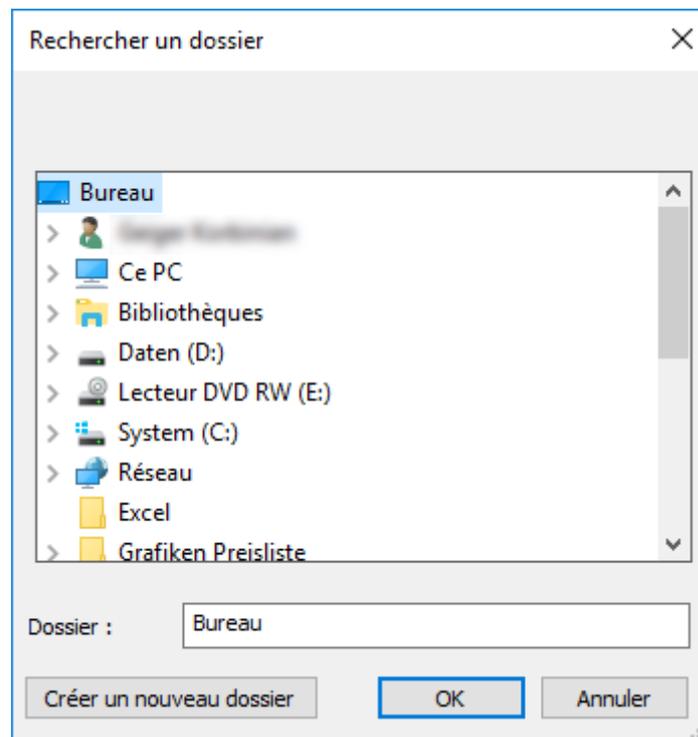
Personne	Ce fichier contient les données à caractère personnel avec lesquelles la personne peut être identifiée (par exemple, le nom de famille, l'adresse ou la photo).
PersonHistory	Ce fichier contient la date de la création ou de la suppression de l'ensemble de données.
PersonLog	Ce fichier contient l'historique des modifications qui ont été effectuées sur l'ensemble de données (par exemple modification des autorisations ou programmations).



### NOTE

Les fonctions RGPD ont accès à la gestion du personnel. Elles doivent donc être attribuées à un groupe d'utilisateurs autorisé à gérer le personnel.

- ✓ LSM ouvert.
- 1. Via | Options |, sélectionnez l'entrée **Fonctions RGPD**.
  - ↳ La fenêtre "Fonctions RGPD" s'ouvre.
- 2. Dans la section "Personnes" marquez l'entrée de la personne dont les données doivent être exportées.
- 3. Dans la section "Personnes", cliquez sur le bouton **Exporter les données à caractère personnel**.
  - ↳ La fenêtre "Recherche des dossiers" s'ouvre.



- 4. Entrez le dossier dans lequel les données doivent être sauvegardées.
- 5. Cliquez sur le bouton **OK**.
  - ↳ Les données sont exportées.

### Utilisateur

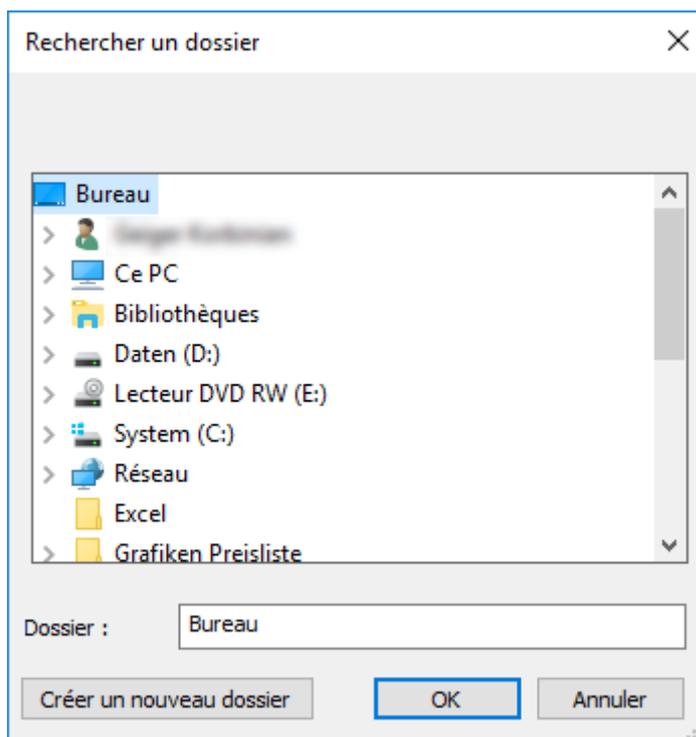
Vous pouvez exporter les données à caractère personnel des utilisateurs du logiciel LSM en tant que fichier CSV. Deux fichiers sont alors générés :

User	Ce fichier contient les données correspondant à l'utilisateur (par exemple le nom d'utilisateur et le groupe d'utilisateurs).
------	---

UserLog	Ce fichier contient l'historique des modifications faites par cet utilisateur (par exemple la création d'une nouvelle fermeture).
---------	---

Les fonctions RGPD ont accès aux fonctions d'administration. Elles doivent donc être attribuées à un groupe d'utilisateurs autorisé à administrer.

- ✓ LSM ouvert.
- 1. Via | Options |, sélectionnez l'entrée **Fonctions RGPD**.
  - ↳ La fenêtre "Fonctions RGPD" s'ouvre.
- 2. Dans la section "Utilisateur" marquez l'entrée de l'utilisateur dont les données doivent être exportées.
- 3. Dans la section "Utilisateur", cliquez sur le bouton **Exporter les données à caractère personnel**.
  - ↳ La fenêtre "Recherche des dossiers" s'ouvre.



- 4. Entrez le dossier dans lequel les données doivent être sauvegardées.
- 5. Cliquez sur le bouton **OK**.
  - ↳ Les données sont exportées.

### 3.14.2 Supprimer les données

À l'aide du module RGPD, vous pouvez également supprimer les données à caractère personnel en toute simplicité.

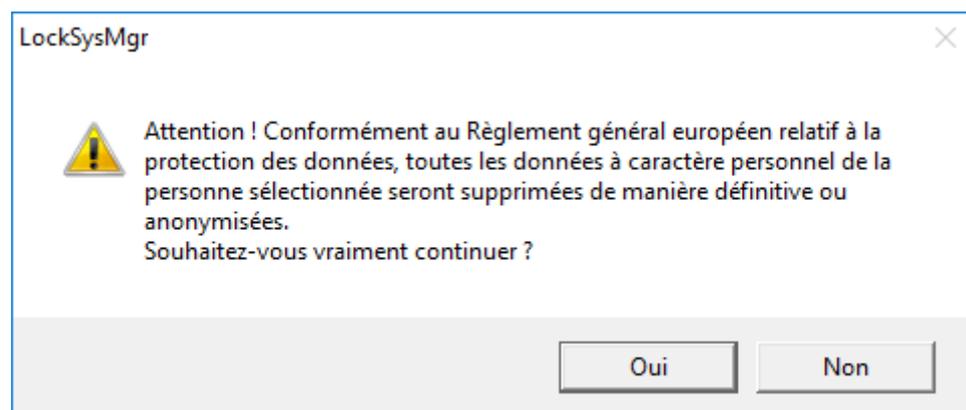
## Personnes



### NOTE

Les fonctions RGPD ont accès à la gestion du personnel. Elles doivent donc être attribuées à un groupe d'utilisateurs autorisé à gérer le personnel.

- ✓ LSM ouvert.
- 1. Via | Options |, sélectionnez l'entrée **Fonctions RGPD**.
  - ↳ La fenêtre "Fonctions RGPD" s'ouvre.
- 2. Dans la section "Personnes" marquez l'entrée de la personne dont les données doivent être supprimées.
- 3. Dans la section "Personnes", cliquez sur le bouton **Supprimer les données à caractère personnel de manière définitive**.
  - ↳ La fenêtre "LockSysMgr" s'ouvre.



- 4. Cliquez sur le bouton **Oui**.
  - ↳ Données à caractère personnel de la personne marquée supprimées ou anonymisées.



### NOTE

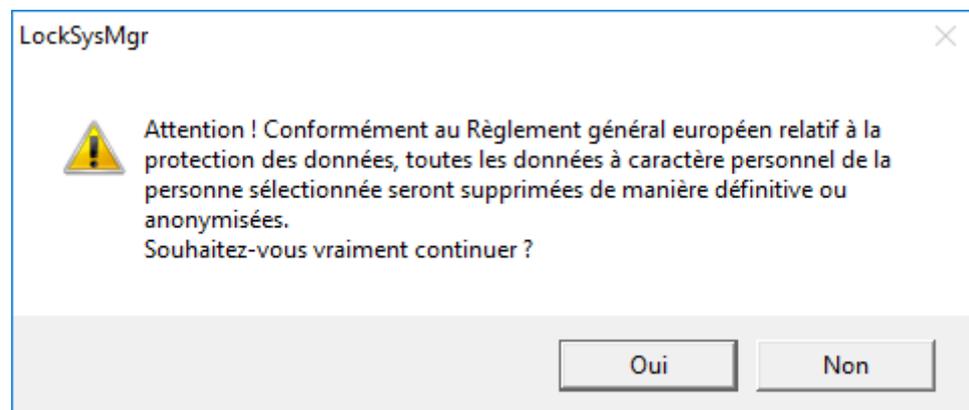
#### Suppression des données restantes d'anciennes suppressions

Il est également possible de supprimer les données personnelles des supports d'identification attribués à l'aide du bouton **✕** dans l'onglet [Nom]. Contrairement à la suppression via le module RGPD, les comptes-rendus ne sont pas supprimés et restent dans le système. Ainsi, seule une partie des données à caractère personnel est supprimée. Les personnes qui ont été supprimées de la sorte, ne sont plus affichées dans le module RGPD. Afin de respecter le RGPD et de pouvoir également supprimer ces fichiers, veuillez utiliser le bouton **Effacer** dans la section "Base de données".

## Utilisateur

Les fonctions RGPD ont accès aux fonctions d'administration. Elles doivent donc être attribuées à un groupe d'utilisateurs autorisé à administrer.

- ✓ LSM ouvert.
1. Via | Options |, sélectionnez l'entrée **Fonctions RGPD**.  
↳ La fenêtre "Fonctions RGPD" s'ouvre.
2. Dans la section "Utilisateur" marquez l'entrée de l'utilisateur dont les données doivent être supprimées.
3. Dans la section "Utilisateur", cliquez sur le bouton **Supprimer les données à caractère personnel de manière définitive**.  
↳ La fenêtre "LockSysMgr" s'ouvre.



4. Cliquez sur le bouton **Oui**.  
↳ Données à caractère personnel de l'utilisateur marqué supprimées ou anonymisées.

### 3.14.3 Quelles données personnelles sont enregistrées dans le logiciel ?

Il est possible d'enregistrer dans le logiciel les données suivantes concernant une personne :

- Prénom
- Nom\*
- Titre
- Adresse
- Téléphone
- E-Mail
- N° d'immatriculation\*
- Nom d'utilisateur
- Division

- Ville/Bâtiment
- Employé du/au
- Date de naissance
- Centre de coûts
- Photo

Parmi ces champs, seuls le nom et le numéro d'immatriculation sont des champs dits \*obligatoires et donc indispensables lors de l'utilisation du logiciel.

Les catégories de données personnelles particulièrement sensibles selon l'article 9 du RGPD ne sont pas enregistrées.

#### 3.14.4 À quelles fins les données personnelles sont-elles enregistrées dans le logiciel ?

Pour pouvoir utiliser pleinement les fonctions d'un système de fermeture électronique, il est nécessaire de pouvoir associer les supports d'identification utilisés (par exemple, transpondeur) à un utilisateur donné (par exemple, un collaborateur).

#### 3.14.5 Pendant combien de temps les données personnelles sont-elles conservées dans le logiciel ?

Les données sont conservées dans le système de fermeture pendant au moins la durée de possession d'un support d'identification (par exemple appartenance à une société).

L'administrateur du système de fermeture peut modifier la durée de conservation des données (par exemple, dans les protocoles et listes d'accès) et l'adapter aux exigences opérationnelles.

#### 3.14.6 Les données personnelles enregistrées dans le logiciel sont-elles protégées contre l'accès par des tiers ?

En principe, il revient à l'utilisateur (client final) du système de fermeture et du logiciel de gérer et de sécuriser les droits d'accès.

Dans le système de fermeture proprement dit, toutes les données sont sécurisées au moyen d'un processus de chiffrement à plusieurs niveaux. Sans les mots de passe et droits d'utilisateur correspondants, il est impossible d'ouvrir l'interface utilisateur graphique afin d'accéder aux données.

Aucune transmission automatique à des tiers, aucune utilisation ni aucun traitement par SimonsVoss n'a lieu dans le cadre des activités commerciales.

### 3.14.7 Les données enregistrées peuvent-elles être mises à disposition sous la forme d'une copie ?

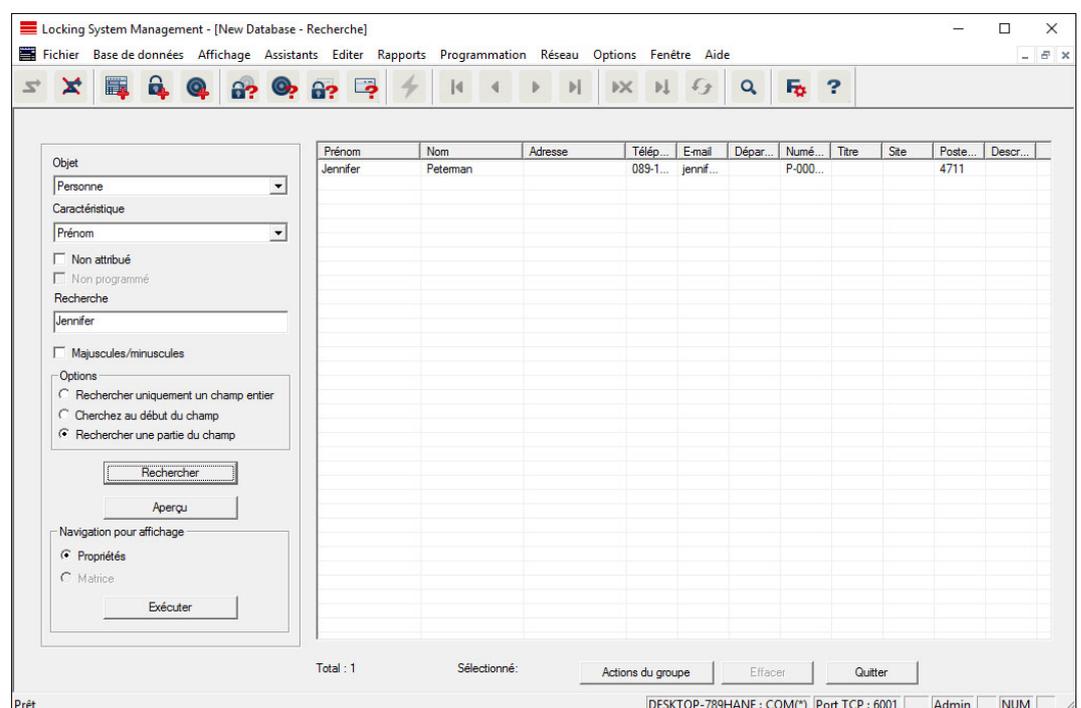
Dans la mesure où l'utilisateur dispose des droits d'utilisateur correspondants, toutes les données collectées concernant une personne (à partir de la version 3.4) peuvent être mises à disposition par le client sous la forme d'une copie par le biais de la fonction d'exportation (par exemple, dans le cadre d'un audit). Cela permet au client d'exercer son droit à l'information en vertu de l'art. 15 du RGPD, paragraphe 3.

### 3.14.8 Les données personnelles peuvent-elles être supprimées du logiciel ?

Les données personnelles peuvent être supprimées définitivement du logiciel et de la base de données associée (à partir de la version 3.4 SPI) par le client à la demande de la personne concernée en vertu de l'art. 17 du RGPD.

## 3.15 Recherche dans la matrice

La recherche permet de localiser des objets divers, par exemple, une certaine porte ou un certain transpondeur, dans la base de données.



✓ Les éléments pouvant être recherchés ont déjà été créés dans l'installation de fermeture.

1. Cliquez sur le symbole de la loupe dans la barre de menu.
2. Sélectionnez l'objet que vous souhaitez rechercher. Il peut s'agir par ex. de personnes, transpondeurs, portes, fermetures, etc.
3. Choisissez une propriété de l'objet recherché, par ex. prénom ou nom.
4. Saisissez une notion dans le champ de recherche.

5. Cliquez sur le bouton « Rechercher » afin de démarrer la recherche.

### 3.16 Exécuter des actions de groupe

Il est possible de paramétrer plusieurs composants de manière simultanée en une seule étape. Dans cet exemple, les paramètres (*par ex. activation du contrôle des accès*) de plusieurs fermetures G2 vont être modifiés en même temps.

1. Cliquez sur le symbole de la loupe dans la barre de menu.
2. Recherchez tous les objets de type « Fermetures ».
  - ↳ Lors de la recherche de toutes les fermetures, il n'est pas nécessaire de remplir le champ « Recherche ».
3. Sélectionnez par exemple plusieurs fermetures par type ou secteur en utilisant les filtres.
4. Cliquez sur le bouton « Actions de groupes ».
  - ↳ Lorsque vous avez seulement choisi les fermetures G2 à l'étape précédente, les paramètres corrects (*« Modifications de la configuration des fermetures G2 » et « Cylindres de fermeture G2 actifs/hybrides »*) seront alors directement sélectionnés.
5. Appuyez sur le bouton « Exécuter » pour démarrer les modifications des fermetures sélectionnées.
6. Exécutez les modifications comme vous le souhaitez.
7. Enregistrer les nouveaux paramètres en cliquant sur « Terminer ».



#### NOTE

Cette procédure permet de modifier rapidement et simplement de nombreux paramètres. Attention, chaque composant modifié doit être reprogrammé.

### 3.17 Programmer le transpondeur

- ✓ Un transpondeur a été créé dans l'installation de fermeture et est visible dans la matrice.
1. Cliquer sur le transpondeur avec le bouton droit de la souris.
  2. Cliquer sur programmer.
  3. Suivez les instructions du logiciel LSM.

*Veillez à choisir le bon appareil de programmation.*

Avec le bouton TIDs our désactiver, vous affichez une liste sur laquelle vous pouvez choisir jusqu'à 2 ID de transpondeur devant être bloqués (voir *Bloquer le transpondeur en permanence et créer un transpondeur de remplacement [► 33]*).



#### NOTE

#### Reconnaître automatiquement les cartes G2

En tant que supports d'identification, les cartes ne sont pas toujours faciles à différencier. Lorsqu'il y a plusieurs cartes, la carte devant être programmée doit tout d'abord être lue afin de pouvoir sélectionner la bonne carte dans le LSM en vue de la programmation. Cette étape n'est pas nécessaire lorsque la case « Reconnaître automatiquement la carte G2 » a été cochée. Lorsque la carte est connue du logiciel LSM, l'ensemble de données respectif est automatiquement sélectionné et programmé.

### 3.18 Programmer la fermeture

✓ Une fermeture a été créée dans le système de fermeture et est visible dans la matrice.

1. Cliquez avec le bouton droit de la souris sur la fermeture souhaitée.
2. Cliquez sur Programmieren (Programmer).
3. Suivez les instructions qui vous sont fournies dans le logiciel LSM.

*Veillez à sélectionner l'appareil de programmation correspondant.*



#### NOTE

Une seule fermeture doit se trouver à proximité de l'appareil de programmation !

#### Rejet de la première activation de l'identifiant après la programmation initiale des produits AX

Si le premier support d'identification activé après la programmation initiale est un tidentifiant, l'identifiant est rejeté une fois et synchronisé avec le système de fermeture à l'arrière-plan. Les identifiants fonctionnent ensuite comme à l'accoutumée.

### 3.19 Programmer via LSM Mobile

LSM Mobile permet d'effectuer des tâches de programmation directement au niveau de la fermeture et ce, à l'aide d'appareils mobiles. La programmation a lieu comme suit :

1. dans le logiciel LSM, une liste contenant les composants révélant un besoin de programmation est exportée vers l'appareil LSM Mobile. *Directement à un Pocket PC ou en tant que fichier pour un ordinateur portable, Netbook ou un Tablet-PC.*
2. Le LSM Mobile est démarré sur l'appareil mobile. La programmation des composants peut commencer via l'exportation du logiciel LSM.

3. À l'issue, les composants programmés via le LSM Mobile doivent être communiqués au logiciel LSM. Pour ce faire, il est procédé à une importation ou synchronisation du LSM Mobile vers les logiciel LSM.

### 3.19.1 Avec un ordinateur portable, un Netbook ou une tablette

Voici comment effectuer une programmation à l'aide de LSM Mobile :

- ✓ Certains composants affichent un besoin de programmation dans le logiciel LSM.
  - ✓ Les composants avec besoin de programmation ont déjà fait l'objet d'une première programmation.
  - ✓ LSM Mobile a été correctement installé sur l'appareil de programmation. Les numéros de version sont identiques.
  - ✓ Les pilotes des appareils de programmation SMARTCD.G2 et SMARTCD.MP (le cas échéant) sont correctement installés.
1. Sélectionnez *Programmation/LSM Mobile/Exportation vers LSM Mobile/LSM Mobile PC*.
  2. Suivez les instructions du logiciel LSM et exportez les tâches de programmation dans un fichier.
  3. Démarrez le LSM Mobile sur votre ordinateur portable et importez la fichier contenant les tâches de programmation dans le LSM Mobile.
  4. Suivez les instructions du LSM Mobile.
  5. À l'aide de l'appareil de programmation, exécuter les programmations sur les composants souhaités.
  6. Exportez le statut des tâches de programmation.
  7. Sélectionnez *Programmation/LSM Mobile/Importation vers LSM Mobile/LSM Mobile PC*.
  8. Suivez les instructions du logiciel LSM et exportez le fichier depuis LSM Mobile.

*Les tâches de programmation ont été effectuées à l'aide de l'appareil externe. L'importation dernièrement effectuée a fait disparaître les éclairs de programmation (indiquant un besoin de programmation) du logiciel LSM.*

### 3.20 Définir le plan des plages horaires (jours fériés et jours ouvrés)

Il est recommandé d'appliquer des plans de plages horaires pour l'ensemble des groupes de transpondeurs et des zones. Cependant, il est également possible de lier directement les plans de plages horaires à des fermetures et à des transpondeurs.

- ✓ Des fermetures (ou zones) et des transpondeurs (ou groupes de transpondeurs) ont déjà été créés.
- 1. Dans la barre de menus, cliquez sur *Bearbeiten/Zeitzoneplan (Édition/Plan des plages horaires)*.
  - ↳ Un plan des plages horaires vide s'ouvre. Si un plan de plages horaires existant est affiché, cliquez sur le bouton Neu (Nouveau) pour créer un nouveau plan de plages horaires vide.
- 2. Remplissez les champs Name (Nom) et Beschreibung (Description).
- 3. Au besoin, sélectionnez la liste des jours fériés de votre pays. Si vous souhaitez définir par exemple des congés uniques, procédez comme suit :
  - ↳ Cliquez sur le champ ... en regard de la zone de liste des jours fériés.
  - ↳ Cliquez sur le bouton Neuer Feiertag (Nouveau jour férié).
  - ↳ Attribuez-lui un nouveau nom, par exemple, « Congés 2017 ».
  - ↳ Les nouveaux congés définis peuvent présenter une période. Pour ce faire, le champ Urlaub (Congés) doit être activé. Il est ensuite possible de saisir une période (Von - Bis/Du - Au).
  - ↳ Sélectionnez le traitement à réserver au nouveau jour de congé, par exemple, comme étant un Dimanche.
  - ↳ Cliquez sur le bouton Übernehmen (Appliquer), puis sur Beenden (Terminer).
  - ↳ Cliquez sur le bouton Feiertagsverwaltung (Gestion des jours fériés).
  - ↳ Ajoutez le jour férié que vous venez de définir (*dans la colonne de gauche*) au moyen du bouton Hinzufügen (Ajouter) de la liste de jours fériés (*dans la colonne de droite*).
  - ↳ Cliquez sur le bouton OK, puis sur Beenden (Terminer) pour revenir au menu principal du plan des plages horaires.
- 4. Sélectionnez un groupe dans le tableau et modifiez son plan hebdomadaire.
  - ↳ Une barre bleue indique une autorisation pour cette période.
  - ↳ Il est possible de cliquer individuellement sur les différents champs ou de les sélectionner ensemble.
  - ↳ Chaque clic sur un champ ou une zone inverse l'autorisation.
  - ↳ 
- 5. Cliquez sur le bouton Übernehmen (Appliquer).
- 6. Cliquez sur le bouton Beenden (Terminer).

Attribuez le plan des plages horaires à une zone :

1. Cliquez avec le bouton droit de la souris sur la zone à laquelle le calendrier doit être associé.
2. Sélectionnez Eigenschaften (Propriétés).

3. Dans la liste déroulante située en regard de Zeitzone (Plage horaire), sélectionnez le plan correspondant.
4. Cliquez sur le bouton Übernehmen (Appliquer).
5. Cliquez sur le bouton Beenden (Terminer).

*Il est également possible d'associer directement le plan des plages horaires à une fermeture.*

Associez un groupe de transpondeurs au groupe horaire :

1. Cliquez avec le bouton droit de la souris sur le groupe de transpondeurs auquel le groupe horaire doit être associé.
2. Sélectionnez Eigenschaften (Propriétés).
3. Dans la liste déroulante située en regard de Zeitzonengruppe (Groupe de plages horaires), sélectionnez le groupe horaire correspondant.
4. Cliquez sur le bouton Übernehmen (Appliquer).
5. Cliquez sur le bouton Beenden (Terminer).

*Il est également possible d'associer directement le groupe horaire à un transpondeur.*

### 3.21 Réinitialisation de composants

Tous les composants SimonsVoss peuvent être réinitialisés à tout moment. Même les composants SimonsVoss qui n'appartiennent pas à l'installation de fermeture peuvent être réinitialisés. Dans ce cas, vous avez besoin du mot de passe de l'installation de fermeture.

La réinitialisation d'un composant peut s'avérer utile dans de nombreux cas. En présence d'erreur, il est recommandé de réinitialiser le composant respectif et de le reprogrammer.

1. Lisez les composants concernés via *Programmer/Lire composants*.
2. Sélectionnez le bouton « Réinitialiser » afin de démarrer le processus de réinitialisation.
3. Suivez les instructions du logiciel LSM.
  - ↳ Le mot de passe de l'installation de fermeture vous sera éventuellement demandé ou vous devrez sélectionner l'ensemble de données à supprimer.

### 3.22 Remplacer une fermeture défectueuse

Il peut arriver que des fermetures soient défectueuses ou subissent un dommage.

Procédez de la manière suivante pour remplacer une fermeture défectueuse par une nouvelle fermeture :

1. retirez la fermeture défectueuse de la porte.
  - ↳ Il est parfois difficile de retirer un cylindre d'une porte verrouillée. En cas de besoin, contactez le revendeur qui a installé vos produits SimonsVoss.
2. Prenez une fermeture de remplacement.
  - ↳ Dans le logiciel LSM, double-cliquer sur la fermeture défectueuse et vous serez en mesure de visualiser tous les détails dans l'onglet « Équipement ».
3. Dans le logiciel LSM effectuez un Software Reset.
  - ↳ Double-cliquer sur la fermeture défectueuse, puis sur l'onglet « Configuration/Données » afin de trouver le bouton « Software Reset ».
  - ↳ À l'issue du Software Reset, un besoin de programmation sera signalisé au niveau de la fermeture défectueuse.
4. Programmez la fermeture de remplacement.
5. Remplacez la fermeture de remplacement dans la porte et testez les fonctionnalités.



#### NOTE

En présence de problème, essayez tout d'abord de réinitialiser la fermeture à l'aide d'une lecture. À l'issue de la réinitialisation, la fermeture pourra probablement être reprogrammée.



#### NOTE

Réinitialisez impérativement les fermetures défectueuses avant de les renvoyer à un revendeur ou à SimonsVoss Technologies GmbH.

### 3.23 Bloquer les transpondeurs

Il peut arriver que des transpondeurs soient perdus, endommagés ou volés.

- *Bloquer le transpondeur en permanence et créer un transpondeur de remplacement [► 33]*
- *Bloquer temporairement le transpondeur [► 37]*



#### NOTE

#### Transfert des ID de serrure avec des cartes vers des serrures double face

Les cartes peuvent uniquement transférer des ID de verrouillage individuels, pas un protocole de programmation complet.

- Tenez toujours la carte qui transmet les ID de verrouillage aux deux lecteurs.

### 3.23.1 Bloquer le transpondeur en permanence et créer un transpondeur de remplacement



#### NOTE

Pour des raisons de sécurité, les autorisations du transpondeur supprimé doivent être retirées dans toutes les fermetures.

- Cela s'effectue au moyen d'une reprogrammation de toutes les fermetures.

Procédez de la manière suivante afin de remplacer l'« ancien » transpondeur par un nouveau transpondeur non encore programmé.

1. Prenez un transpondeur de remplacement.
  - ↳ Dans le logiciel LSM, double-cliquer sur le transpondeur défectueux pour visualiser tous les détails dudit transpondeur dans l'onglet « Équipement ».
2. Cliquez avec le bouton droit de la souris sur le transpondeur défectueux, perdu ou volé et sélectionnez « Perte de transpondeur ».
  - ↳ Le transpondeur concerné sera préparé au blocage.
  - ↳ Donnez le motif de la nécessité de cette mesure. *En sélectionnant « Transpondeur perdu/volé », il est alors possible de programmer un nouveau transpondeur ayant les mêmes propriétés. Dans le compte-rendu G2, ce transpondeur bloquera le transpondeur perdu à chaque actionnement à une fermeture autorisée. La reprogrammation de toutes les fermetures concernées est cependant nécessaire.*
3. Exécutez tous les besoins de programmation en résultant à tous les composants.

#### Contourner la programmation ultérieure des fermetures

La création d'un nouveau transpondeur de remplacement génère un besoin de programmation au niveau de toutes les portes. Ces tâches de programmation spéciales peuvent toutefois être directement effectuées avec le nouveau transpondeur de remplacement :

- ✓ Le transpondeur de remplacement a été dument programmé.
- 1. Actionnez le nouveau transpondeur de remplacement à chaque fermeture.
- 2. Reprogrammer le nouveau transpondeur de remplacement. Activer la case « Accusé de réception de désactivation / lire alertes des piles » dans la fenêtre « Programmer le transpondeur ».
- 3. Actualisez la matrice. Le besoin de programmation a maintenant disparu.

À partir de LSM 3.5 SP3, il est possible de « donner » n'importe quel transpondeur jusqu'à deux autres ID de transpondeur devant être bloqués.

### Programmer directement des TID à bloquer

Les ID à bloquer sont enregistrés sur l'identifiant lors de la procédure de programmation.

- ✓ L'identifiant est disponible physiquement.
- ✓ La fenêtre de programmation de l'identifiant est ouverte.
- 1. Cliquez sur le bouton **TIDs our désactiver**.

Transponder programmieren

Besitzer / Transponder: Aldrin, Lily / 005MBA8

Programmiergerät: UNF-AL-18KJ793 : COM(\*)

Nach der Programmierung zum nächsten Transponder springen

Deaktivierungsquittungen / Batteriewarnungen auslesen

G1 Datensätze aus fremden Schließanlagen beibehalten

Programmieren TIDs zum Deaktivieren Beenden

↳ Une liste s'ouvre.

TIDs zum Deaktivieren

Schließanlage: HIMYM

G2 TIDs    G1 TIDs

Transponder: Aldrin, Lily / 005MBA8

TID	Typ	Besitzer	Seriennummer	Zustand
<input type="checkbox"/> 3228	G2	Zinman, Stella	00XDESA	verloren

Es können für einen Transponder nur zwei deaktivierte TIDs ausgewählt werden

Achtung! Diese Änderungen erzeugen keinen Programmierbedarf. Vergessen Sie nicht den Transponder zu programmieren oder an einem Smart Relais 3 - Gateway zu buchen

OK   Übernehmen   Abbrechen

2. Cochez jusqu'à deux cases dans la colonne TID pour enregistrer les TID à supprimer sur l'identifiant.
  3. Confirmez la sélection en cliquant sur le bouton OK.
  4. Poursuivez la programmation.
- ↳ Les TID sélectionnés sont enregistrés sur l'identifiant en tant que TID à supprimer. Si l'identifiant s'authentifie sur une fermeture concernée, les TID à supprimer sont bloqués sur la fermeture.

### Enregistrer les TID à bloquer dans les propriétés

Les ID à bloquer sont enregistrés sur l'identifiant pendant la procédure de programmation suivante ou lors de l'activation suivante sur une borne actualisatrice.

✓ La fenêtre de propriétés de l'identifiant est ouverte.

1. Accédez à l'onglet [Configuration].

Soll-Zustand

- Langes Öffnen
- Kein akustisches Öffnungssignal
- Begehungsliste

Dynamisches Zeitfenster

- Zeitfenster am Gateway nicht verändern
- bis zu einer bestimmten Uhrzeit des (nächsten) Tages
- Stundenanzahl ab der letzten vollen Std. der Buchung

Aktivierungsdatum

- ab sofort

Verfallsdatum

- ohne Verfallsdatum

Zeitzonegruppe

G1

G2

TIDs zum Deaktivieren

2. Cliquez sur le bouton TIDs our désactiver .

↳ Une liste s'ouvre.

TIDs zum Deaktivieren

Schließanlage

G2 TIDs  G1 TIDs

Transponder: Aldrin, Lily / 005MBA8

TID	Typ	Besitzer	Seriennummer	Zustand
<input type="checkbox"/> 3228	G2	Zinman, Stella	00XDESA	verloren

Es können für einen Transponder nur zwei deaktivierte TIDs ausgewählt werden

Achtung! Diese Änderungen erzeugen keinen Programmierbedarf. Vergessen Sie nicht den Transponder zu programmieren oder an einem Smart Relais 3 - Gateway zu buchen

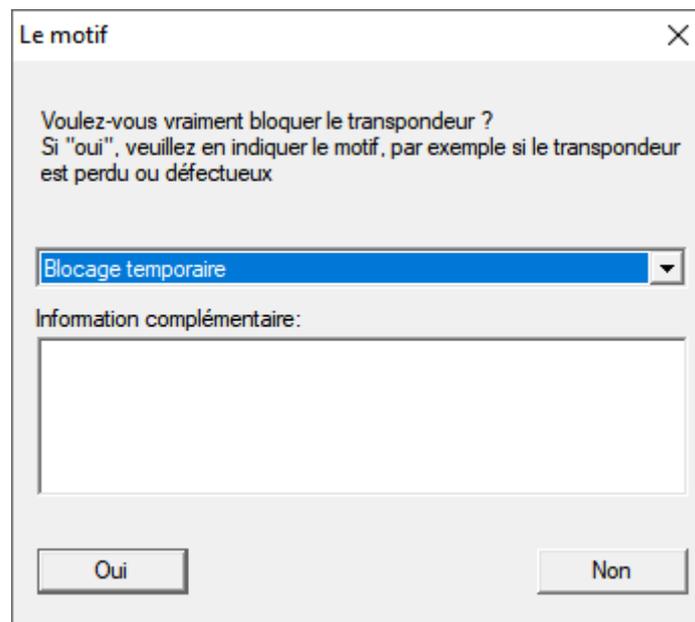
OK Übernehmen Abbrechen

3. Cochez jusqu'à deux cases dans la colonne TID pour enregistrer les TID à supprimer sur l'identifiant.

4. Confirmez la sélection en cliquant sur le bouton OK.
  - ↳ Les TID sélectionnés sont enregistrés sur l'identifiant pendant la programmation suivante ou lors de l'activation suivante sur une borne actualisatrice.

### 3.23.2 Bloquer temporairement le transpondeur

Le blocage durable d'un support d'identification entraîne la perte d'un TID. Par conséquent, une fonction a été ajoutée avec la LSM 3.5 afin de bloquer temporairement un transpondeur ou une carte : "Blocage temporaire".



Le TID n'est pas véritablement bloqué. Au lieu de cela, vous retirez à la personne toutes ses autorisations en appuyant sur le bouton. Les portes concernées doivent évidemment être reprogrammées. Si le transpondeur réapparaît ou est transmis à quelqu'un d'autre, vous pouvez simplement restaurer les autorisations qui existaient avant le blocage.

Pour connaître les transpondeurs bloqués temporairement, consultez les propriétés du système de fermeture dans l'onglet [TID spéciaux].



### Transférer les niveaux de charge des piles vers le logiciel LSM via LSM Mobile

Les états de la pile des fermetures peuvent être directement lus via LSM Mobile ou être transférés au logiciel LSM. Suivez les instructions du manuel « LSM-Mobile ». Ce dernier se trouve sur la page d'accueil SimonsVoss ([www.simons-voss.com](http://www.simons-voss.com)) dans la section Assistance sous Documents.

### Afficher les niveaux de charge des piles

#### Procédure normale pour toutes les versions LSM :

- ✓ Les alertes des piles actuelles des fermetures respectives ont été transmises au logiciel LSM.
- 1. Double-cliquer sur une fermeture afin d'afficher les propriétés de la fermeture.
- 2. Choisissez l'onglet « État de fonctionnement ».
- 3. Le niveau de charge des piles s'affiche dans le champ « Dernier état lu de la fermeture ».

#### Afficher l'ensemble des alertes des piles pour LSM BASIC Online et LSM BUSINESS :

*générez une liste affichant toutes les fermetures avec alertes des piles.*

- ✓ Les alertes des piles actuelles des fermetures respectives ont été transmises au logiciel LSM.
- 1. Dans la barre de menu, choisissez « Rapports / Structure du bâtiment ».
- 2. Choisissez la propriété « Fermetures avec alertes des piles ».
- 3. Cliquez sur le bouton « Afficher ».

#### Afficher automatiquement les alertes des piles sous LSM BUSINESS

*Créez une alerte affichant directement les alertes des piles.*

- ✓ Les alertes des piles actuelles des fermetures respectives ont été transmises au logiciel LSM.
- 1. Dans la barre de menu, choisissez « Rapports / Gérer alertes »
- 2. Créez une nouvelle alerte à l'aide du bouton « Nouveau ».
- 3. Configurez l'alerte selon vos désirs. Choisissez le type « Alerte des piles fermeture ».
- 4. N'oubliez pas d'affecter cette alerte aux fermetures respectives ! Le champ « Fermetures » ne doit pas être vide.
- 5. Confirmez la nouvelle alerte en cliquant sur le bouton « OK ».

6. Refermez le dialogue en cliquant sur « Terminer ».

### 3.25 Réinitialiser le mode par défaut des fermetures G1

Lorsque les alertes des piles des fermetures G1 ne sont pas prises en considération, les fermetures concernées passent alors en mode par défaut. Cela permet d'éviter le déchargement complet des piles. Le mode par défaut peut être réinitialiser en reprogrammant la fermeture. À l'issue, la fermeture doit immédiatement être ouverte à l'aide d'un transpondeur autorisé et les piles changées.

### 3.26 Réinitialiser le mode freeze des fermetures G2

Par rapport à la génération G1, l'ouverture d'urgence de la porte et l'annulation du mode urgence dans G2 et l'annulation du mode urgence (mode freeze) ont été facilitées.

- ✓ Support d'identification du remplacement de la pile créé (voir Transpondeur de remplacement des piles).
  - ✓ Support d'identification de remplacement des piles programmé.
1. Actionnez le support d'identification de remplacement des piles à la fermeture.
    - ↳ Mode veille désactivé.
  2. Actionnez un support d'identification autorisé quelconque.
    - ↳ La fermeture s'ouvre.
  3. Remplacez la pile.
  4. Actionnez le support d'identification de remplacement des piles à la fermeture.
    - ↳ Mode veille désactivé.
  5. À l'aide d'un support d'identification autorisé, testez le fonctionnement de la fermeture.
    - ↳ Mode Freeze réinitialisé.

#### ATTENTION

##### Panne de la fermeture en cas d'utilisation abusive

Le support d'identification de changement de piles a pour seule fonction d'annuler le mode Freeze avant un changement de piles. S'il est utilisé de manière abusive, les piles peuvent être entièrement déchargées. Il en résulte une panne totale de la fermeture.

### 3.27 Gestion des listes d'accès

La lecture des listes d'accès et de passage peut se voir fortement limitée en raison de la protection de la vie privée. Dans LSM BASIC, un utilisateur propre « AdminAL » (Admin Access List) a été créé par défaut. Dans le LSM BUSINESS, un utilisateur similaire peut être créé manuellement, voir *Gestion des utilisateurs* [▶ 42].

*Ce chapitre décrit le scénario suivant : Seule une personne autorisée (par ex. membre du Comité d'entreprise connecté en tant qu'AdminAL) ne doit pouvoir lire les listes d'accès et de passage. L'administrateur général de l'installation de fermeture ne doit pas disposer de ce droit.*

#### Créer AdminAL et autoriser la lecture des listes d'accès

1. S'inscrire au projet avec le nom d'utilisateur « Admin » et le mot de passe.
2. Ouvrez la gestion des groupes d'utilisateurs sous « Éditer/groupe d'utilisateurs ».
3. À l'aide des flèches de navigation, naviguer vers « Administration des listes d'accès » (ou dans LSM BUSINESS vers un groupe d'utilisateurs précédemment créé).
4. Vérifier sous « Rôle » que les cases « Administration des listes d'accès » et « Gérer listes d'accès » soient activées.
5. Cliquer ensuite sur le champ « Éditer » situé sous « Rôle ».
6. Activez les installations de fermeture souhaitées dans les groupes de transpondeurs et les espaces. Lorsque des espaces ou groupes de transpondeurs ont été créés, vous devez alors également activer de manière séparée tous les espaces ou groupes de transpondeurs souhaités !
7. Refermez le masque en cliquant sur « OK ».
8. Confirmez les nouveaux paramètres en cliquant sur les boutons « Accepter » et « Terminer ».
9. Déconnectez-vous de votre projet actuel via « Base de données/Déconnecter ».

#### Retirer les droits de lecture des listes d'accès à l'Admin



#### NOTE

Le droit « Administration listes d'accès » doit toujours appartenir à un utilisateur/groupe d'utilisateurs et ne doit jamais être retiré !

1. S'inscrire au projet avec le nom d'utilisateur « AdminAL ».
  - ↳ Le mot de passe dans le LSM BASIC est « system3060 ».
  - ↳ Modifiez immédiatement ce mot de passe !
2. Ouvrez la gestion des groupes d'utilisateurs sous « Éditer/groupe d'utilisateurs ».
3. À l'aide des flèches de navigation, naviguer vers « Admin ».
4. Désactivez les rôles « Administration listes des accès » et « Gérer les listes d'accès ».
5. Confirmez les nouveaux paramètres en cliquant sur les boutons « Accepter » et « Terminer ».
  - ↳ L'installation est ainsi terminée. Les listes d'accès et de passage ne pourront à présent être lues et consultées que depuis le compte utilisateur « AdminAL ».

### 3.27.1 Listes d'accès

Les fermetures avec la fonction ZK consignent les accès dans une liste d'accès :

- Date
- Heure
- ID du support d'identification
- Nom de l'utilisateur ou de l'utilisatrice

Vous pouvez lire et afficher la liste d'accès à l'aide du logiciel LSM. Le nombre d'entrées de la liste d'accès dépend de la fermeture et de la configuration.

	Standard	Passerelle
Cylindre	Jusqu'à 3000	
SmartHandle	Jusqu'à 3000	
SmartRelais	Jusqu'à 3600	Jusqu'à 200

Dans un système de fermeture en réseau, vous pouvez également automatiser la lecture (voir *Lecture d'une fermeture* [▶ 103]).

## 3.28 Gestion des utilisateurs

### Affecter un utilisateur à un groupe d'utilisateur

1. Cliquez sur « Éditer/Groupe d'utilisateurs ».
2. À l'aide des flèches de navigation, naviguez vers un groupe d'utilisateurs (ou créez une nouveau groupe d'utilisateurs à l'aide du bouton « Nouveau »).
3. Cliquez sur le bouton « Éditer ».

4. Marquez l'utilisateur souhaité et affectez-le au groupe d'utilisateurs à l'aide du bouton « Ajouter ».
5. Confirmer les paramètres en cliquant sur « OK ».
6. *Le cas échéant, corriger les rôles.*
  - ↳ Cliquez ensuite sur le champ « Éditer » situé sous « Rôle ».
  - ↳ Activez les installations de fermeture souhaitées dans les groupes de transpondeurs et les espaces. Lorsque des espaces ou groupes de transpondeurs ont été créés, vous devez alors également activer de manière séparée tous les espaces ou groupes de transpondeurs souhaités !
  - ↳ Refermez le masque en cliquant sur « OK ».
7. Confirmez les nouveaux paramètres en cliquant sur les boutons « Accepter » et « Terminer ».

#### Créer un nouvel utilisateur

1. Cliquez sur « Éditer/Utilisateur ».
2. Cliquez sur le bouton « Nouveau » afin de créer un nouvel utilisateur.
3. Attribuez un nom à l'utilisateur ainsi qu'un mot de passe.
4. Confirmez les nouveaux paramètres en cliquant sur les boutons « Accepter » et « Terminer ».

### 3.29 Gestion des cartes

Vous allez à présent voir les différents types de carte et la répartition de la mémoire en fonction du système de fermeture SimonsVoss.

#### ATTENTION

##### MIFARE DESFire recommandé

MIFARE DESFire utilise un chiffrement MIFARE Classic avancé, fonctionnant avec un micro-contrôleur conforme AES-128, qui répond aussi aux exigences de sécurité élevées.

- SimonsVoss recommande d'utiliser des transpondeurs ou produits MIFARE-DESFire.



#### NOTE

##### Modèles différents pour produits AX

Si vous voulez utiliser des produits MIFARE pour des produits AX SimonsVoss, les modèles utilisés doivent être identiques pour l'écriture et la lecture.



7. Cliquez sur le bouton `Accepter`.
- ↳ Vous avez modifié la configuration.

### 3.29.2 Vue d'ensemble

## 4. Réalisation de tâches standard basées sur WaveNet dans LSM

Cet exemple présente les étapes les plus importantes pour la mise en place et l'administration d'un réseau radio WaveNet via le LSM Business. Ces exemples se basent sur certaines installations et ont pour objectif de vous familiariser avec le thème WaveNet.

### 4.1 Création d'un réseau radio WaveNet et connexion d'une fermeture

Cet exemple décrit comment créer un réseau radio WaveNet. L'objectif est ici de contacter une fermeture via le nœud routeur 2 actuel.

#### 4.1.1 Préparer le logiciel LSM

Attention, pour la mise en réseau des composants de fermeture SimonsVoss, le logiciel LSM doit être correctement installé et le module réseau respectif doit disposer d'une licence valide !

1. Installez le CommNode-Server et assurez-vous que le service ait été démarré.
2. Installez la version actuelle du WaveNet-Manager. (Voir Décompression)
3. Ouvrez le logiciel LSM et choisissez « Réseau/WaveNet Manager ».
  - ↳ Saisissez le répertoire d'installation du WaveNet Manager et choisissez un répertoire pour le fichier de sortie.
  - ↳ Démarrez le WaveNet Manager via le bouton « Démarrer ».
4. Attribuez un mot de passe afin d'accroître la sécurité de votre réseau.
  - ↳ Le WaveNet Manager démarre et les paramètres sont ainsi sauvegardés. Terminez le WaveNet Manager afin de procéder à d'autres paramètres.

#### 4.1.2 Première programmation des composants de fermeture

Les fermetures doivent tout d'abord être programmées avant de pouvoir être reliées au réseau.

##### 4.1.2.1 Créer une nouvelle fermeture

- ✓ Une installation de fermeture a déjà été créée.
1. Choisissez *Éditer/Nouvelle fermeture*.
  2. Attribuez toutes les fonctionnalités et éventuellement d'autres paramètres à l'aide du bouton « Configuration ».
  3. Cliquez sur le bouton « Enregistrer & Suivant ».
  4. Cliquez sur le bouton « Terminer ».

#### 4.1.2.2 Programmer la fermeture

- ✓ Une fermeture a été créée dans le système de fermeture et est visible dans la matrice.

1. Cliquez avec le bouton droit de la souris sur la fermeture souhaitée.
2. Cliquez sur Programmieren (Programmer).
3. Suivez les instructions qui vous sont fournies dans le logiciel LSM.

*Veillez à sélectionner l'appareil de programmation correspondant.*



#### NOTE

Une seule fermeture doit se trouver à proximité de l'appareil de programmation !

#### Rejet de la première activation de l'identifiant après la programmation initiale des produits AX

Si le premier support d'identification activé après la programmation initiale est un tidentifiant, l'identifiant est rejeté une fois et synchronisé avec le système de fermeture à l'arrière-plan. Les identifiants fonctionnent ensuite comme à l'accoutumée.

#### 4.1.3 Préparer le matériel

Le nœud routeur 2 peut être mis en service rapidement et simplement. Reliez le nœud routeur 2 en suivant les instructions contenues dans la notice abrégée. À sa sortie d'usine, le nœud routeur 2 est paramétré de telle sorte que ce dernier reçoit son adresse IP d'un serveur DHCP. À l'aide de l'outil OAM (*disponible gratuitement dans la section Assistance sous matériel informatif/Téléchargements de logiciels*) vous pouvez déterminer rapidement cette adresse IP.



#### NOTE

Paramètres par défaut :

Adresse IP : 192 168 100 100

Nom d'utilisateur : SimonsVoss | Mot de passe : SimonsVoss

Si la fermeture n'est pas équipée d'un nœud de réseau (LN.I) à sa sortie d'usine, vous devez alors l'en équiper.



#### NOTE

Veillez noter l'adresse IP du nœud routeur 2 ainsi que le Chip-ID de la fermeture après avoir correctement préparé le matériel.

#### 4.1.4 Créer des nœuds de communication

Les nœuds de communication forment l'interface entre le CommNode-Server et le logiciel LSM. Afin de créer la configuration XML, le LSM doit être ouvert en tant qu'administrateur.

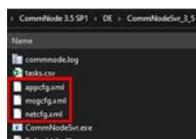
1. Ouvrez le logiciel LSM.
2. Choisissez « | Réseau | / Noeuds de communication ».
3. Complétez les informations « Nom », « Nom de l'ordinateur » et « Description ».

```
C:\Users\kgeiger>echo %computername%
UNF-AL-18KJ793

C:\Users\kgeiger>echo %computername%.%userdnsdomain%
UNF-AL-18KJ793.ALLEGION.COM
```

↳ Par ex. UNF-AL-18KJ793, UNF-AL-18KJ793.ALLEGION.COM ; nœuds de communication pour le réseau radio WaveNet 123.

4. Cliquez sur le bouton « Configuration ».
5. Vérifiez que le chemin d'accès renvoie bien au répertoire d'installation du CommNode-Server et cliquez sur le bouton « OK ».
6. Confirmez le message par « No » et cliquez ensuite sur « OK ». Les trois configurations XML (appcfg, msgcfg et netcfg) doivent se trouver directement dans le répertoire d'installation du CommNode-Server.



7. Enregistrer les paramètres en cliquant sur « Accepter ».
8. Confirmez le masque en cliquant sur « OK ».
9. Refermez le dialogue en cliquant sur « Quitter ».

#### 4.1.5 Paramétrer le réseau et l'importer dans le LSM

##### 4.1.5.1 Configuration WaveNet

Lorsque toutes les conditions préalables sont remplies, vous pouvez commencer avec la configuration :

- ✓ Le logiciel LSM est correctement installé et le module réseau dispose d'une licence valide.
  - ✓ Le CommNode-Server a été installé et le service démarré.
  - ✓ Les fichiers de configuration du CommNode-Server ont été créés.
  - ✓ La version actuelle du WaveNet-Manager est installée.
  - ✓ Un nœud de communication a été créé dans le logiciel LSM.
  - ✓ La première programmation de la fermeture à mettre en réseau a été réussie.
  - ✓ Le nœud routeur 2 est accessible via le réseau et vous connaissez son adresse IP :
  - ✓ La fermeture programmée dispose d'un nœud de réseau monté dont vous connaissez le Chip-ID.
1. Démarrez le WaveNet Manager via « Réseau/WaveNetManager » et le bouton « Démarrer ».
  2. Veuillez saisir le mot de passe.
  3. Avec le bouton de droite de la souris, cliquer sur « WaveNet\_xx\_x ».
  4. Initialisez tout d'abord le nœud routeur 2, par ex. via l'option « Ajouter : IP ou routeur USB ».
    - ↳ Suivez les instructions et reliez le nœud routeur 2 à votre réseau radio WaveNet via l'adresse IP du nœud routeur 2.
  5. Initialisez le nœud de réseau de la fermeture en cliquant avec le bouton droit de la souris sur le nœud routeur 2 nouvellement ajouté et choisissez « Rechercher ChipID » :
    - ↳ Suivez les instructions et attribuez la fermeture ou le nœud de réseau lui appartenant au nœud routeur 2 à l'aide du ChipID du nœud de réseau.
  6. Cliquez ensuite sur « Enregistrer », puis « Terminer », puis sur « Oui » afin de fermer le WaveNet Manager.
  7. Importez les nouveaux paramètres et attribuez-les au nœud de communication correspondant.

#### 4.1.5.2 Transférer la configuration WaveNet

Les nouveaux paramètres doivent être envoyés au CommNode-Server :

1. Choisissez « Réseau/nœud de communication ».
2. Sélectionnez le nœud routeur 2 dans la listes des raccordements et cliquez sur le bouton « Transférer ».
3. Enregistrer les paramètres en cliquant sur « Accepter ».
4. Refermez le dialogue en cliquant sur « Terminer ».

#### 4.1.5.3 Attribuer un nœud de réseau à une fermeture

Le nœud de réseau initialisé doit être relié à une fermeture. Cela s'effectue (en particulier en présence de plusieurs nœuds de réseau) à l'aide d'un ordre commun :

1. Choisir « Réseau/ordre commun/nœuds WaveNet ».
2. Choisissez tous les nœuds de réseau (*WNNode\_xxxx*) qui ne sont pas encore attribués. *Les nœuds de réseau non attribués ne disposent d'aucune entrée dans la colonne « Porte ».*
3. Cliquez sur le bouton « Configuration automatique ».  
↳ La configuration automatique démarre immédiatement.
4. Refermez le dialogue en cliquant sur « Terminer ».

#### 4.1.5.4 Tester la configuration WaveNet

Afin de tester rapidement la mise en réseau, vous pouvez programmer ultérieurement la fermeture via le réseau « Clic avec le bouton droit de la souris/programmer ». Si la programmation a été réussie, le réseau travaille alors normalement.

## 4.2 Mise en service du fermeture DoorMonitoring

Cet exemple présente les paramétrages à effectuer lors de la mise en service de fermeture DoorMonitoring. Les conditions préalables sont mentionnées au chapitre « *Création d'un réseau radio WaveNet et connexion d'une fermeture [▶ 46]* ».

### 4.2.1 États (de porte) possibles

Les états de porte affichés dépendent des composants.

#### 4.2.1.1 Les états possibles de la surveillance des portes SmartHandle

- Porte ouverte/fermée
- Porte ouverte trop longtemps
- Verrouillé (uniquement pour les serrures à verrouillage automatique)
- Levier de commande pressé/non pressé

#### 4.2.1.2 États possibles de la surveillance des portes Cylindre de fermeture

- Porte ouvert/fermé
- Porte verrouillée
- Porte bien verrouillée
- Porte ouverte trop longtemps
- Vis emboutie manipulée

#### 4.2.1.3 États possibles de la surveillance des portes SmartRelay 3

- Input 1 aktiv/inaktiv
- Input 2 aktiv/inaktiv
- Input 3 aktiv/inaktiv
- *Détection des actes de sabotage [► 54]*

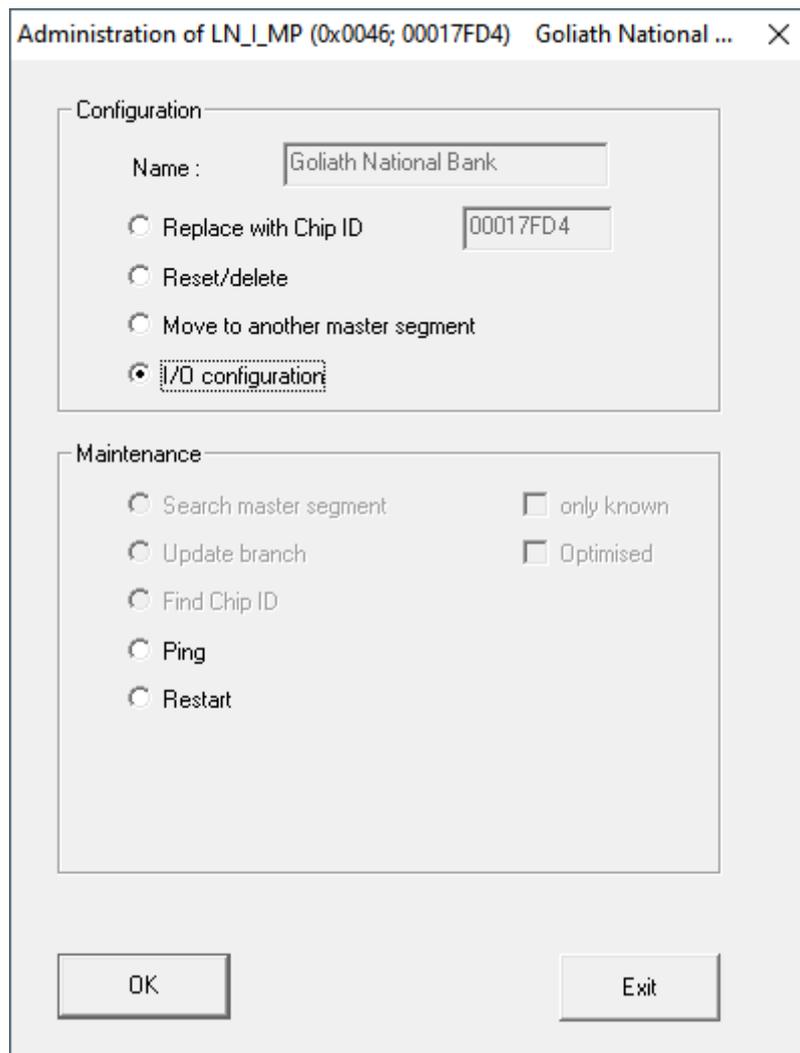
#### 4.2.1.4 États possibles RouterNode 2 / GatewayNode 2

- Input aktiv/inaktiv
- Entrée de tension analogique au-dessus/en dessous du seuil

### 4.2.2 Intégrer les fermetures DoorMonitoring dans le réseau

Comment intégrer les fermetures DM dans le réseau WaveNet:

- ✓ Le gestionnaire de WaveNet est déjà en place.
  - ✓ Le RouterNode auquel la nouvelle serrure doit être attribuée est déjà configuré et "en ligne".
  - ✓ Le LockNode est correctement monté sur le DM-lock.
  - ✓ Chip-ID est connue.
1. Démarrez le gestionnaire WaveNet via | Réseau | - **WaveNet Manager**.
  2. Cliquez avec le bouton droit de la souris sur le RouterNode.
    - ↳ Fenêtre "Administration" se ouvre.
  3. Mettez l'option  Find Chip ID en surbrillance.
  4. Cliquez sur le bouton **OK**.
    - ↳ Fenêtre "Administration" se ferme.
  5. Suivez le dialogue et attribuez le verrou ou le LockNode associé au RouterNode 2 en utilisant son Chip-ID.
  6. Cliquez avec le bouton droit sur le DM-LockNode nouvellement ajouté.
  7. Cochez l'option  I/O configuration.
  8. Cliquez sur le bouton **OK**.
    - ↳ Fenêtre "Administration" se ouvre.



9. Activez la case à cocher  Send all events to I/O router.
10. Cliquez sur le bouton **OK**.
  - ↳ Fenêtre "Administration" se ferme.
11. Cliquez sur le bouton **ENREGISTRER**.
12. Cliquez sur le bouton **Quitter**.
13. Cliquez sur le bouton **Oui**.
  - ↳ WaveNet-Manager se ferme.
14. Importez les nouveaux paramètres et attribuez-les au nœud de communication correspondant.

### 4.2.3 SmartHandle de DoorMonitoring

LSM ou Smart.Surveil vous permet de surveiller vos SmartHandles DoorMonitoring. Pour ce faire, vous devez cependant commencer par configurer les SmartHandles DoorMonitoring dans le LSM :

- ✓ LSM ouvert.
- ✓ Aperçu de la matrice ouvert
- 1. Double-cliquez sur la SmartHandle DM pour ouvrir la fenêtre des paramètres.
- 2. Accédez à l'onglet [Équipement].
- 3. Cliquez sur le bouton **Configuration du Monitoring**.
  - ↳ Fenêtre "Configuration Door Monitoring" la fenêtre Configuration Door Monitoring s'ouvre.

The screenshot shows the 'Configuration Door Monitoring' window. It is divided into two main sections: 'Prescrit' and 'Réel'. Each section contains a 'Paramètres porte ouverte' area with three dropdown menus for detection interval, event trigger, and escape/return time. Below this is an 'Événements' section with two sub-sections: 'Consignation dans la liste des accès' and 'Transfert vers le réseau'. In the 'Prescrit' section, all checkboxes for these events are checked. In the 'Réel' section, all checkboxes are unchecked. At the bottom of each section is a 'Capteurs externes' area with two checkboxes for inverting inputs, which are also unchecked. The window has 'OK' and 'Annuler' buttons at the bottom.

- 4. Dans la zone "Prescrit" de consigne "Événements" des zones "Consignation dans la liste des accès" et "Tasnfert vers le réseau" des événements DoorMonitoring que vous souhaitez surveiller (par exemple,  Évènements - "Portes ouvertes",  Évènements - Serrure à pêne dormant et  Évènements capteur béquille de la porte).
- 5. Au besoin, effectuez d'autres paramétrages DoorMonitoring, par exemple dans la zone "Paramètres porte ouverte".
- 6. Cliquez sur le bouton **OK**.
  - ↳ Fenêtre "Configuration Door Monitoring" la fenêtre Configuration Door Monitoring se ferme.
- 7. Cliquez sur le bouton **Accepter**.
- 8. Programmez la SmartHandle.
  - ↳ Les événements DoorMonitoring sont stockés dans la base de données LSM et peuvent être évalués par le LSM et SmartSurveil.

#### 4.2.3.1 Détection des actes de sabotage

À partir du logiciel LSM 3.4 SP2, vous pouvez détecter les tentatives de sabotage sur SmartHandle AX et SmartRelais 3 Advanced. Lorsque le boîtier qui y est utilisé est ouvert, le système électronique le détecte et envoie les informations au logiciel LSM. Si vous voulez évaluer les informations, vous pouvez configurer un événement à ce sujet et y réagir (voir *Configurer Eventmanagement (événements)* [▶ 68]).

#### 4.2.3.2 DoorMonitoring (SmartHandle) - Événements de poignée de porte

À partir du LSM 3.5 SP3, vous pouvez connaître l'état de la poignée du SmartHandle AX. Lorsque la poignée est actionnée, le système électronique le détecte et envoie les informations au logiciel LSM. Si vous voulez évaluer les informations, vous pouvez configurer un événement à ce sujet et y réagir (voir *Configurer Eventmanagement (événements)* [▶ 68]).

#### 4.2.4 Cylindre de DoorMonitoring

LSM ou Smart.Surveil vous permet de surveiller vos cylindres DoorMonitoring. Pour cela, vous devez cependant commencer par configurer les cylindres DoorMonitoring dans le LSM :

- ✓ LSM ouvert.
  - ✓ Aperçu de la matrice ouvert
1. Double-cliquez sur le cylindre DM pour ouvrir la fenêtre des paramètres.
  2. Accédez à l'onglet [Équipement].
  3. Cliquez sur le bouton **Configuration du Monitoring**.
    - ↳ Fenêtre "Configuration Door Monitoring" la fenêtre Configuration Door Monitoring s'ouvre.

4. Dans la zone "Prescrit" de consigne "Événements" des zones "Consignation dans la liste des accès" et "Tasnfert vers le réseau" des événements DoorMonitoring que vous souhaitez surveiller (par exemple,  Évènements - "Portes ouvertes").
5. Au besoin, effectuez d'autres paramétrages DoorMonitoring, par exemple dans la zone "Paramètres porte ouverte".
6. Cliquez sur le bouton **OK**.
  - ↳ Fenêtre "Configuration Door Monitoring" la fenêtre Configuration Door Monitoring se ferme.
7. Cliquez sur le bouton **Accepter**.
8. Programmez le cylindre.
  - ↳ Les événements DoorMonitoring sont stockés dans la base de données LSM et peuvent être évalués par le LSM et SmartSurveil.

#### 4.2.5 Analyser les inputs du contrôleur

Les entrées numériques du contrôleur du système SREL3-ADV peuvent être transférées au LSM et y déclencher des actions.

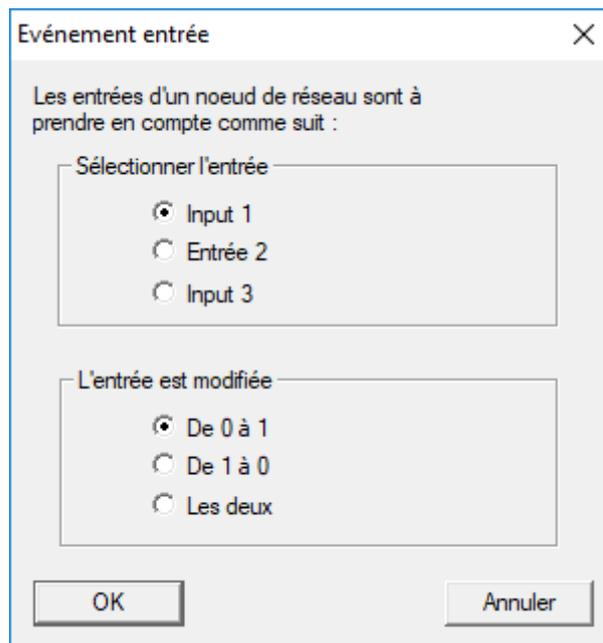
##### Créer un évènement

Si vous souhaitez analyser un input via le LSM ou SmartSurveil (voir SmartSurveil), vous devez alors préalablement créer un évènement en tant qu'input dans le LSM. Ce n'est qu'après que les modifications apportées à l'input seront également enregistrées dans la base de données LSM.

- ✓ LSM ouvert.
- ✓ Système SREL3-ADV créé dans la matrice.
- 1. Via | Réseau |, sélectionnez l'entrée **Gestionnaire événements**.
  - ↳ La fenêtre "Gestionnaire évnts. réseau" s'ouvre.
- 2. Cliquez sur le bouton **Nouveau**.
  - ↳ La fenêtre "Nouvel événement" s'ouvre.

3. Saisissez un nom pour l'évènement.
4. Saisissez une description pour l'évènement (en option).
5. Saisissez un message (en option).
6. Ouvrez le menu déroulant ▼ **Type**.
7. Sélectionnez l'entrée "Évènement entrée".

8. Cliquez sur le bouton **Configurer l'évènement**.
  - ↳ La fenêtre "Évènement entrée" s'ouvre.



9. Dans la zone "Sélectionner l'entrée", sélectionnez l'input souhaité.
  10. Dans la zone "L'entrée est modifiée", sélectionnez la modification d'état qui doit déclencher l'évènement.
  11. Cliquez sur le bouton **OK**.
  12. Cliquez sur le bouton **Sélectionner** afin d'attribuer l'évènement à une fermeture.
    - ↳ La fenêtre "Administration" s'ouvre.
  13. Marquez une ou plusieurs fermeture(s).
  14. Cliquez sur le bouton **Ajouter**.
  15. Cliquez sur le bouton **OK**.
    - ↳ La fenêtre se ferme.
    - ↳ La fermeture est affectée à l'évènement.
  16. Lorsque vous souhaitez créer une action, vous pouvez affecter une action avec le bouton **Nouveau** ou **Ajouter**.
  17. Cliquez sur le bouton **OK**.
    - ↳ La fenêtre se ferme.
    - ↳ L'évènement sera affichée dans la zone "Evénements".
  18. Cliquez sur le bouton **Quitter**.
    - ↳ La fenêtre se ferme.
- ↳ L'input est créé en tant qu'évènement et déclenche une action en fonction des paramètres.

#### 4.2.6 Transférer la configuration WaveNet

Les nouveaux paramètres doivent être envoyés au CommNode-Server :

1. Choisissez « Réseau/nœud de communication ».

2. Sélectionnez le nœud routeur 2 dans la listes des raccordements et cliquez sur le bouton « Transférer ».
3. Enregistrer les paramètres en cliquant sur « Accepter ».
4. Refermez le dialogue en cliquant sur « Terminer ».

#### 4.2.7 Attribuer un nœud de réseau à une fermeture

Le nœud de réseau initialisé doit être relié à une fermeture. Cela s'effectue (en particulier en présence de plusieurs nœuds de réseau) à l'aide d'un ordre commun :

1. Choisir « Réseau/ordre commun/nœuds WaveNet ».
2. Choisissez tous les nœuds de réseau (*WNNode\_xxxx*) qui ne sont pas encore attribués. *Les nœuds de réseau non attribués ne disposent d'aucune entrée dans la colonne « Porte ».*
3. Cliquez sur le bouton « Configuration automatique ».  
↳ La configuration automatique démarre immédiatement.
4. Refermez le dialogue en cliquant sur « Terminer ».

#### 4.2.8 Activer les évènements Input de la fermeture

Afin que les états de la porte soient correctement affichés dans le logiciel LSM, vous devez procéder à d'autres paramétrages :

1. Choisir « Réseau/ordre commun/nœuds WaveNet ».
2. Choisissez le cylindre DoorMonitoring (*ou tout autre cylindre de fermeture dont les évènements doivent être transférés*).
3. Cliquez sur le bouton « Activer évènements Input ».  
↳ La programmation démarre immédiatement.
4. Cliquez sur le bouton « Terminer » dès que toutes les fermetures ont été programmées.

### 4.3 Paramétrer RingCast

La configuration d'un RingCast est décrite ci-après. Un RingCast permet d'envoyer un évènement Input d'un nœud routeur 2 simultanément à un autre nœud routeur 2 et ce dans le même réseau radio WaveNet. Cet exemple présente l'ouverture d'urgence des fermetures. Dès qu'une alarme incendie confirme l'Input 1 d'un nœud routeur 2, toutes les fermetures qui y sont reliées doivent alors être ouvertes. Chaque fermeture reste ensuite ouverte jusqu'à ce qu'elle reçoive un ordre explicite d'ouverture à distance.

*Un RingCast permet bien entendu d'exécuter d'autres tâches comme par exemple fonction de serrure de blocage, ouverture à distance et fonction amok (tireur fou).*

Dans cet exemple, le réseau radio WaveNet dispose de deux nœuds routeur 2. Une fermeture est reliée à chaque nœud routeur 2. Dès que l'Input 1 est déclenché à un nœud routeur 2, toutes les fermetures doivent alors s'ouvrir immédiatement. Ainsi, les personnes peuvent avoir accès à toutes les pièces afin de pouvoir s'y réfugier en présence d'incendie ou de fumée.



#### NOTE

Lorsque les nœuds routeurs 2 sont reliés via Ethernet, alors les modèles RingCast à partir de 2017 sont supportés. Lorsque la connexion d'un nœud routeur 2 vers un autre nœud routeur 2 a échoué, la connexion essaie alors d'être établie via radio. La portée de la communication radio va jusqu'à 30 m (en fonction de l'environnement, ne peut pas être garantie).

### 4.3.1 Préparation du RouterNode pour le RingCast



#### NOTE

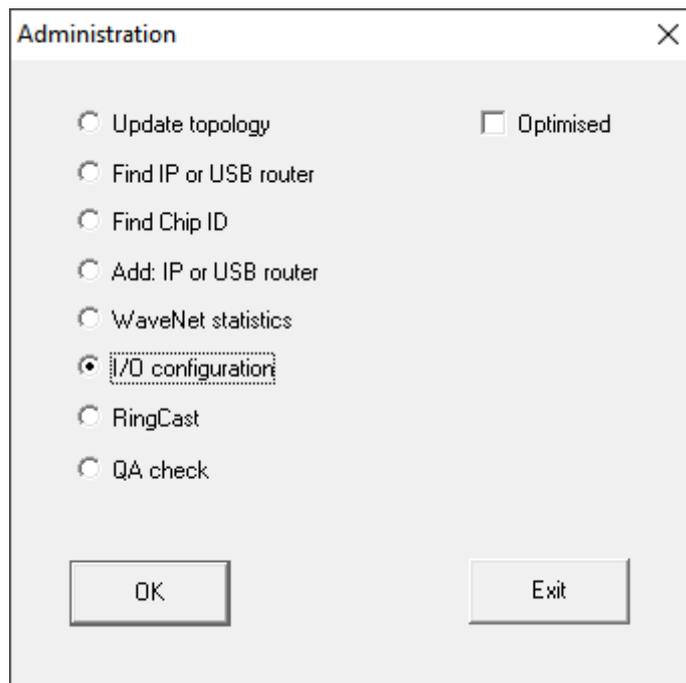
**La disponibilité du RingCast pour le RouterNode dépend du micrologiciel**

La prise en charge du RingCast dépend du micrologiciel (voir Informations sur le firmware).

- Si nécessaire, actualisez le micrologiciel (voir Actualiser le firmware).

Préparez le RouterNode pour le RingCast :

- ✓ Au moins deux RouterNode différents compatibles avec le RingCast sont configurés et « en ligne » dans le réseau sans fil WaveNet (voir Informations sur le firmware).
  - ✓ Au moins une fermeture est associée à chaque RouterNode du RingCast prévu. Les deux fermetures sont « en ligne ».
1. Ouvrez le gestionnaire WaveNet.
  2. Avec le bouton droit de la souris, cliquez sur le premier RouterNode 2.
    - ↳ La fenêtre "Administration" s'ouvre.



3. Sélectionnez l'option  I/O configuration.
4. Cliquez sur le bouton **OK**.
  - ↳ La fenêtre "Administration" se ferme.
  - ↳ La fenêtre "I/O configuration" s'ouvre.
5. En option : Sélectionnez par exemple pour ▼ **Output** 1 "Input receipt static" pour pouvoir piloter un dispositif de signalisation pendant la désactivation.
6. Dans le menu déroulant ▼ **Input** de l'entrée souhaitée, sélectionnez la réaction correspondante (voir RouterNode : entrée numérique).
7. Dans le menu déroulant ▼ **Delay [s]**, sélectionnez l'entrée "RingCast".
8. Cliquez sur le bouton **Select LN**.
9. Vérifiez si le LockNode souhaité est sélectionné. (*Lors de la première installation de la configuration E/S du routeur, tous les LockNode sont inclus.*)
10. Dans le menu déroulant ▼ **Protocol generation**, sélectionnez la génération de votre protocole.



#### NOTE

##### Génération du protocole dans le logiciel LSM

La génération du protocole est indiquée dans le logiciel LSM, dans les propriétés du système de fermeture, dans l'onglet [Nom] de la zone "Production de rapport".

11. Saisissez le mot de passe du système de fermeture.
12. Cliquez sur le bouton **OK**.

13. Effectuez les mêmes réglages que sur l'autre RouterNode 2.

#### 4.3.2 Créer RingCast

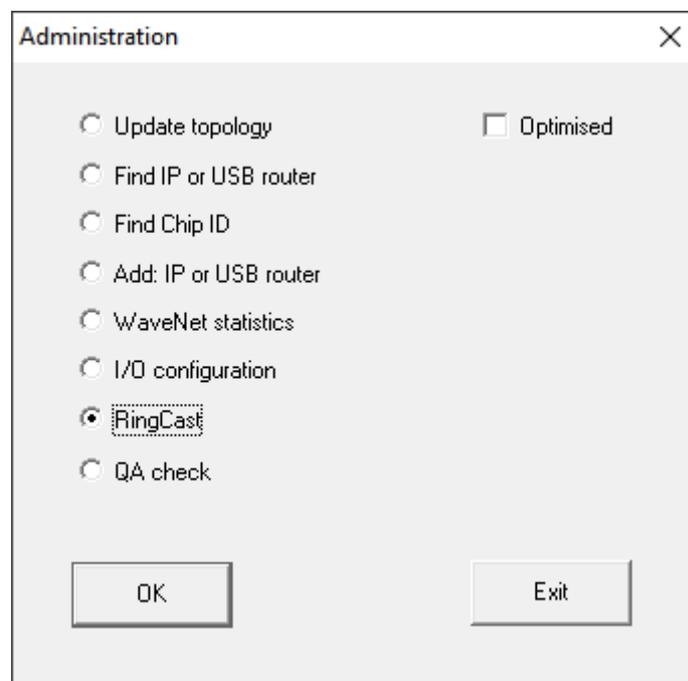


#### NOTE

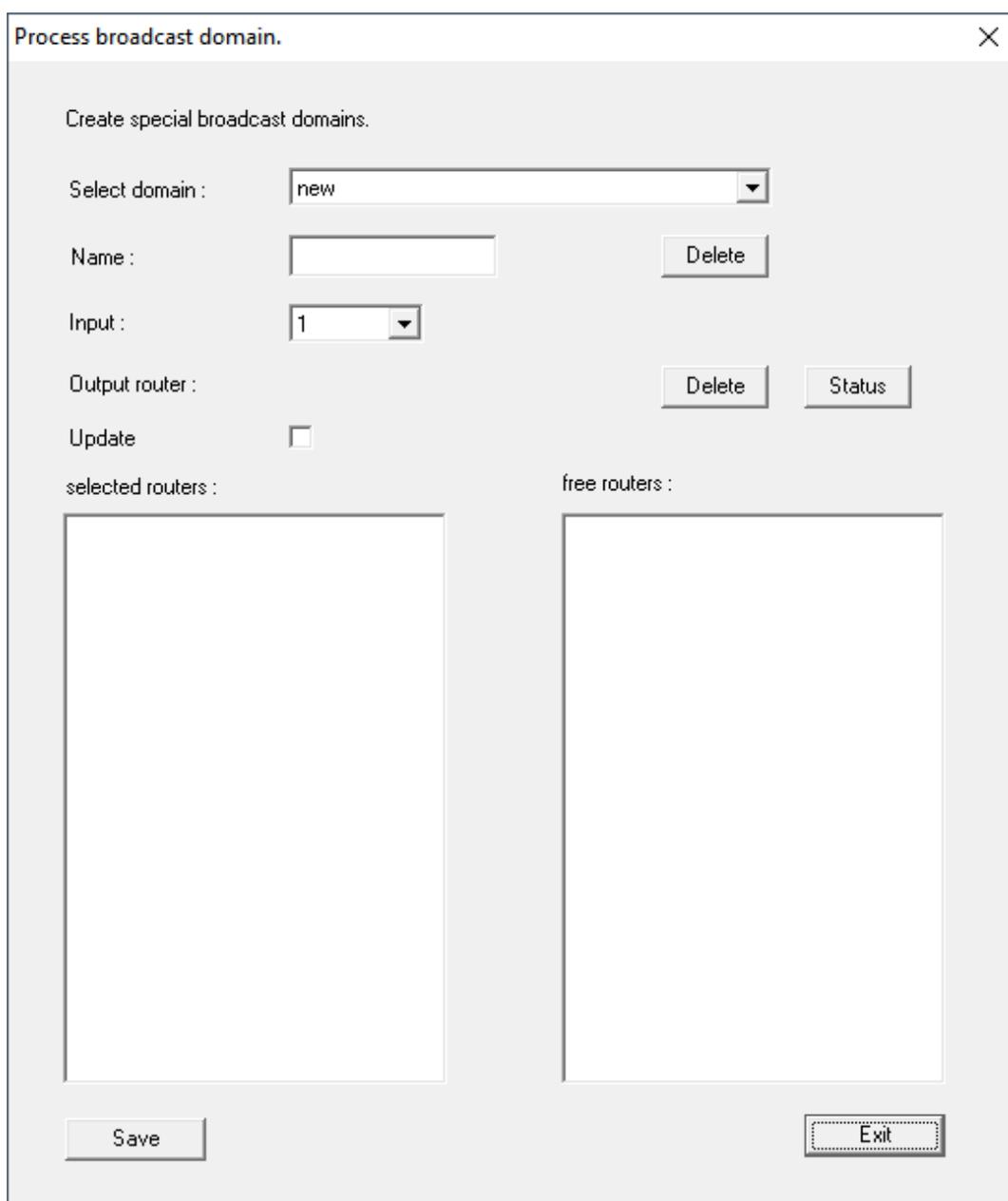
##### Recalcul du RingCast

Si vous remplacez ou supprimez un RouterNode dans le RingCast ou modifiez la configuration E/S correspondant à ce RingCast, le RingCast est automatiquement recalculé après la sauvegarde des modifications et la confirmation de la demande.

- ✓ Gestionnaire WaveNet ouvert par le biais du LSM (voir Meilleure pratique : À partir du logiciel LSM).
  - ✓ RouterNode et LockNode raccordés à l'alimentation en tension.
  - ✓ RouterNode et LockNode importés dans la topologie WaveNet (voir Trouver et ajouter des appareils).
  - ✓ RouterNode préparé pour RingCast (voir *Préparation du RouterNode pour le RingCast* [▶ 59]).
1. Avec le bouton droit de la souris, cliquez sur l'entrée « WaveNet XX\_X ».   
↳ La fenêtre "Administration" s'ouvre.



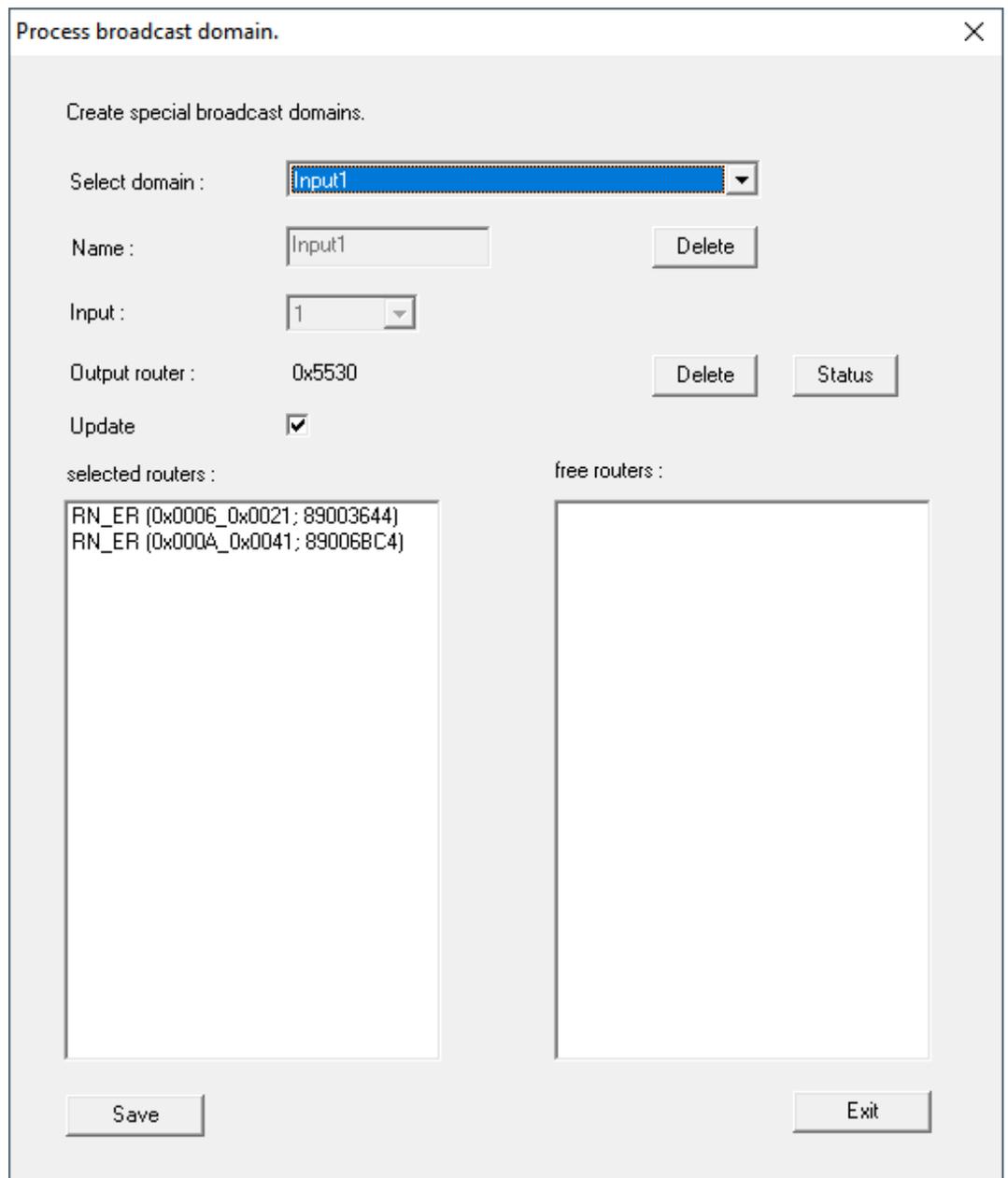
2. Sélectionnez l'option  RingCast.
3. Cliquez sur le bouton .   
↳ La fenêtre "Administration" se ferme.   
↳ La fenêtre "Edit radio domains" s'ouvre.



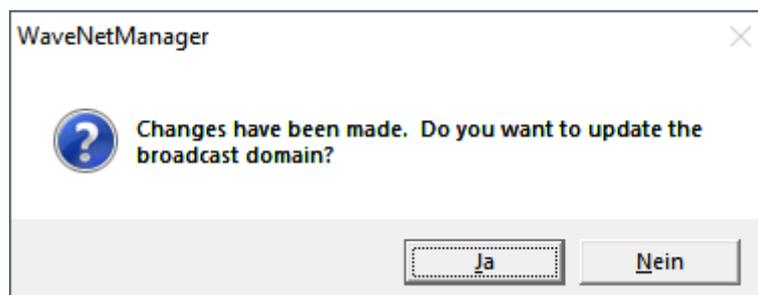
4. Dans le menu déroulant ▼ **Select domain**, sélectionnez une entrée pour laquelle vous avez choisi ▼ **Delay [s]** "RingCast".



↳ Dans le champ "selected routers", vous voyez apparaître tous les RouterNode2 pour lesquels vous avez, à cette entrée, sélectionné pour ▼ **Delay [s]** l'entrée "RingCast" (=Domaines).



5. Cliquez sur le bouton **Save**.
6. Cliquez sur le bouton **Quitter**.
  - ↳ La fenêtre "Edit radio domains" se ferme.
  - ↳ La fenêtre "WaveNetManager" s'ouvre.



7. Cliquez sur le bouton **Oui**.
  - ↳ La fenêtre "WaveNetManager" se ferme.
  - ↳ Les modifications sont mises à jour.
- ↳ Le RingCast est créé et apparaît rapidement dans le gestionnaire WaveNet.

```
RingCast
├── Input1(0)
│   ├── RN_ER (0x0006_0x0021; 89003644)
│   └── RN_ER (0x000E_0x0041; 0002A8B2)
│       └── RN_ER (0x0006_0x0021; 89003644) ###
```

Enregistrez les nouveaux réglages et quittez le gestionnaire WaveNet.

### 4.3.3 Test de fonctionnement du RingCast

Le RingCast ne possède pas de fonction d'autotest.



#### AVERTISSEMENT

#### **Perturbation ou défaillance des fonctions de protection en raison d'une modification des conditions**

L'activation des fonctions de protection dans le RingCast repose sur la liaison sans fil et la liaison Ethernet. Notamment, une modification des conditions ambiantes peut avoir une incidence sur les liaisons sans fil (voir Réseau sans fil et Défis en matière de réseaux sans fil). Cela peut alors avoir des conséquences sur l'activation des fonctions de protection dans le RingCast et mettre en péril la sécurité des personnes et des biens matériels qui par exemple sont protégés par les fonctions de protection du RingCast.

1. Testez les fonctions de protection au moins une fois par mois (voir *Test de fonctionnement du RingCast* [▶ 64]).
2. Si nécessaire, respectez également les autres directives et réglementations qui s'appliquent à votre système de fermeture (en particulier pour les voies d'évacuation et de sauvetage, ainsi que pour la protection contre l'incendie. Il vous revient de veiller à ce que ces directives et réglementations soient respectées.).

## Modification du déroulement des fonctions d'urgence en raison de dysfonctionnements

SimonsVoss et « Made in Germany » garantissent une sécurité et une fiabilité maximales. Dans certains cas, des dysfonctionnements de vos appareils ne peuvent toutefois pas être exclus. Ces dysfonctionnements peuvent mettre en péril la sécurité des personnes et des biens matériels qui sont protégés par les fonctions de protection du RingCast.

1. Testez vos appareils au moins une fois par mois (voir Test de fonctionnement d'un appareil. D'autres prescriptions relatives à l'ensemble de votre système peuvent également exiger des intervalles plus courts).
2. Testez les fonctions de protection au moins une fois par mois (voir *Test de fonctionnement du RingCast* [▶ 64]).

---

Sur l'initiateur, activez l'entrée correspondante et vérifiez :

- si les fermetures réagissent comme souhaité (voir aussi RouterNode : entrée numérique).
- si l'entrée réglée sur le RouterNode indique la confirmation en commutant comme souhaité (voir aussi RouterNode : sortie numérique).

### Test avec un routeur de sortie centralisé



#### NOTE

#### Routeur de sortie centralisé dans RingCast avec RouterNode R/CR

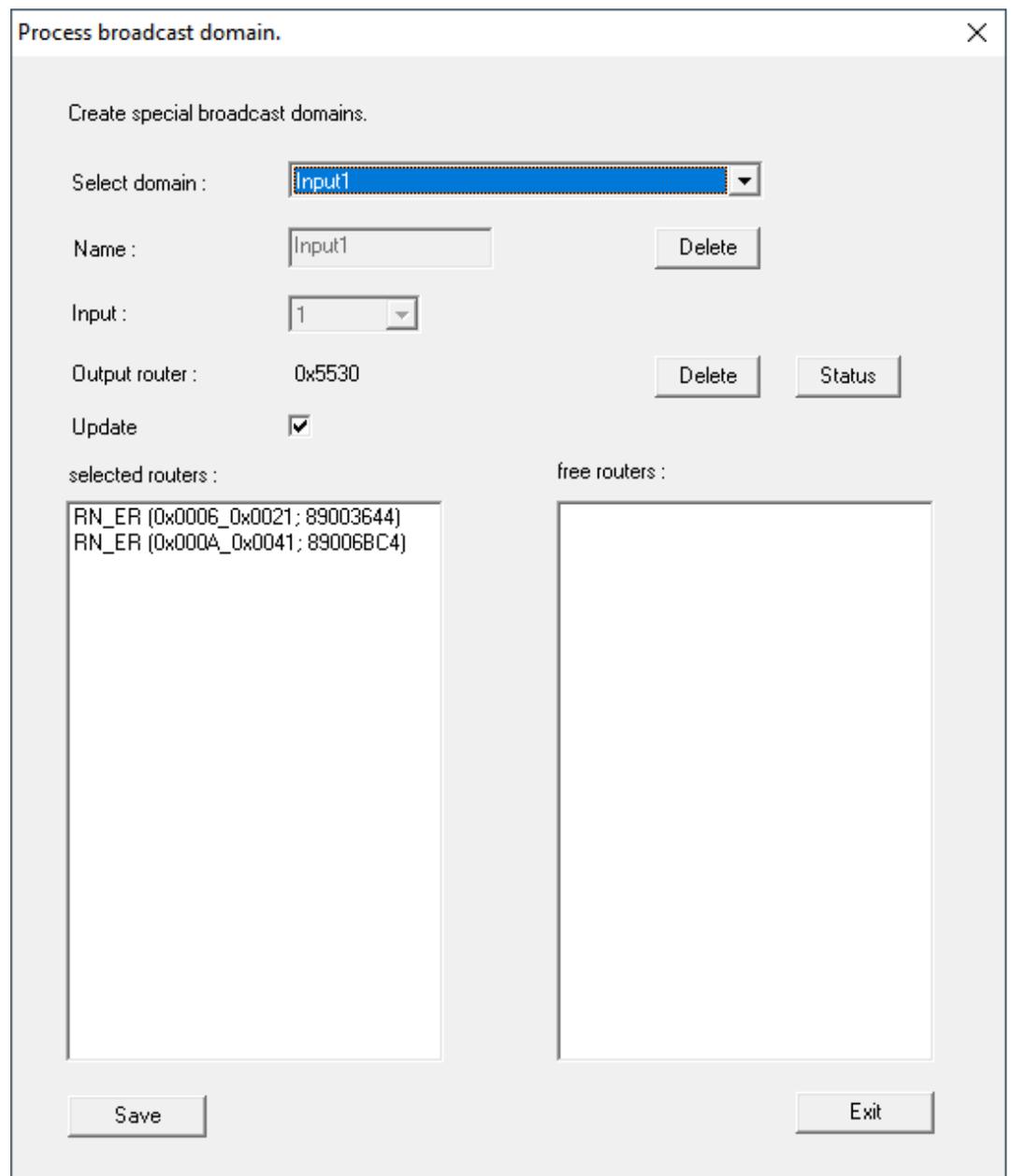
Le routeur de sortie centralisé reçoit la confirmation d'entrée des RouterNode participants exclusivement par l'intermédiaire d'une liaison Ethernet. C'est pourquoi le routeur de sortie centralisé ignore l'état des RouterNode qui ne sont pas des RouterNode Ethernet (.ER). Si vous utilisez le routeur de sortie centralisé et que votre RingCast contient également des RouterNode sans interface Ethernet, la confirmation d'entrée du routeur de sortie centralisé signifie seulement que toutes les fermetures qui sont associées à un RouterNode Ethernet ont reçu l'ordre.

- Vérifiez l'état des autres RouterNode R/CR manuellement, indépendamment du routeur de sortie centralisé (voir Tester l'accessibilité (LSM) et RouterNode et État E/S et réactivité des LockNode).

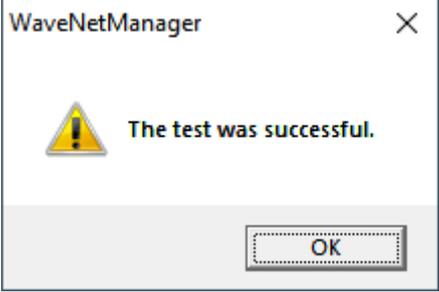
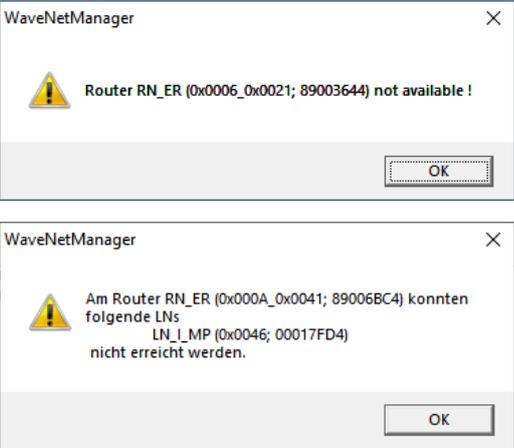
---

L'utilisation d'un routeur de sortie centralisé (voir Routeur de sortie central) simplifie considérablement le test du RingCast. Sur l'initiateur, activez l'entrée correspondante et vérifiez si le routeur de sortie centralisé délivre une confirmation d'entrée ou active la sortie correspondante. Si la sortie n'est pas activée, vérifiez quels RouterNode ont provoqué des problèmes :

- ✓ Gestionnaire WaveNet ouvert par le biais du LSM (voir Meilleure pratique : À partir du logiciel LSM).
- 1. Avec le bouton droit de la souris, cliquez sur l'entrée du RingCast que vous voulez tester.
- 2. Dans le menu déroulant ▼ **Select domain**, sélectionnez l'entrée dont vous souhaitez tester le RingCast.
  - ↳ La fenêtre "Edit radio domains" s'ouvre.



- 3. Cliquez sur le bouton **Status**.
  - ↳ Le RingCast est testé.

	
<p>Le RingCast a pu communiquer avec toutes les fermetures.</p>	<p>Le RingCast n'a pas pu être achevé. Causes possibles (voir aussi Routeur de sortie central) :</p> <ul style="list-style-type: none"> <li>■ Un ou plusieurs RouterNode n'a/ont pas reçu le paquet de données.</li> <li>■ Un ou plusieurs RouterNode n'a/ont pas atteint un ou plusieurs LockNode.</li> <li>■ La liaison Ethernet avec un ou plusieurs RouterNode est interrompue. Les RouterNode ont pu recevoir le paquet de données sans fil, mais n'ont pas pu renvoyer leur confirmation d'entrée en raison de la coupure de la liaison Ethernet.</li> </ul> <ol style="list-style-type: none"> <li>1. Vérifiez l'accessibilité du RouterNode mentionné (voir RouterNode et Tester l'accessibilité (LSM)).</li> <li>2. Vérifiez l'accessibilité du LockNode (voir LockNode et Tester l'accessibilité (LSM)).</li> <li>3. Vérifiez les dernières réactions des LockNode (voir État E/S et réactivité des LockNode).</li> </ol>

#### 4.4 Configurer Eventmanagement (événements)

La mise en réseau de fermetures via nœud routeur 2 présente de nombreux avantages. Un avantage non négligeable est la communication permanente entre le nœud routeur 2 et la fermeture.

Dans cet exemple, le logiciel LSM doit envoyer un e-mail prédéfini dès qu'un transpondeur est actionné à une certaine porte pendant la nuit.

Pour ce faire, les conditions suivantes doivent être remplies :

- Un réseau radio WaveNet est en place comme dans l'exemple *Création d'un réseau radio WaveNet et connexion d'une fermeture* [► 46].
- En outre, la transmission des événements à la fermeture a été activée comme décrit à l'étape *Activer les événements Input de la fermeture* [► 58].

##### 4.4.1 Configurer le serveur e-mail

Le logiciel LSM contient un client e-mail rudimentaire pour l'envoi d'e-mails. L'envoi d'e-mails requiert l'existence d'un compte e-mail propre supportant le format SMTP.

1. Choisissez « Réseau/Messages e-mail ».
2. Cliquez sur le bouton « E-mail ».
3. Effectuez tous les paramétrages SMTP de votre fournisseur e-mail.
4. Cliquez sur le bouton « OK ».
5. Cliquez sur le bouton « OK ».

##### 4.4.2 Configurer le service Task

1. Choisissez « Réseau/Taskmanager ».
2. Sous « Service Task », choisissez votre nœud de communication.
3. Cliquez sur le bouton « Accepter ».
4. Cliquez sur le bouton « Terminer ».

##### 4.4.3 Transférer les événements Input via le nœud routeur 2

Dès que des événements (*par ex. un transpondeur est actionné à une fermeture en réseau*) doivent être transmis au CommNode-Server via un nœud routeur 2, cela doit être activé dans la configuration I/O du routeur.

1. Ouvrez le WaveNet Manager.
2. À l'aide du bouton droit de la souris, cliquez sur le routeur et sélectionnez « Configuration I/O ».
3. À l'aide de la liste défilante, cliquez « Tous les événements des nœuds de réseau » dans « Transmettre événements au système de gestion ».
4. Confirmez à l'aide du bouton « OK » et fermez le WaveNet Manager.

#### 4.4.4 Transmettre les évènements Input via le système SREL3-ADV

Le système SREL3-ADV permet de transmettre les entrées Input au LSM.

##### 4.4.4.1 Analyser les inputs du contrôleur

Les entrées numériques du contrôleur du système SREL3-ADV peuvent être transférées au LSM et y déclencher des actions.

#### Créer un évènement

Si vous souhaitez analyser un input via le LSM ou SmartSurveil (voir SmartSurveil), vous devez alors préalablement créer un évènement en tant qu'input dans le LSM. Ce n'est qu'après que les modifications apportées à l'input seront également enregistrées dans la base de données LSM.

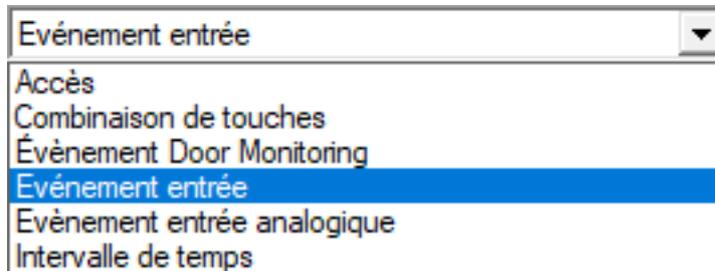
- ✓ LSM ouvert.
  - ✓ Système SREL3-ADV créé dans la matrice.
1. Via | Réseau |, sélectionnez l'entrée **Gestionnaire évènements**.
    - ↳ La fenêtre "Gestionnaire évnts. réseau" s'ouvre.
  2. Cliquez sur le bouton **Nouveau**.
    - ↳ La fenêtre "Nouvel évènement" s'ouvre.

The screenshot shows a dialog box titled "Nouvel évènement" with a close button (X) in the top right corner. The dialog is divided into several sections:

- Form fields:** "Nom:" (empty text box), "Description:" (empty text box), "Message:" (empty text box), and "Type:" (dropdown menu showing "Evènement entrée").
- Buttons:** "Configurer l'évènement" (below the Type dropdown), "Ajouter", "Supprimer", and "Nouveau" (in a vertical stack on the left), "OK" (bottom left), and "Configurer le temps" (bottom center).
- Fermetures (Closures):** A section with a "Sélectionner" button and an empty list area.
- Niveau d'alarme (Alarm Level):** A section with three radio buttons: "Message" (selected), "Avertissement", and "Alarme".
- Other buttons:** "Annuler" (bottom right).

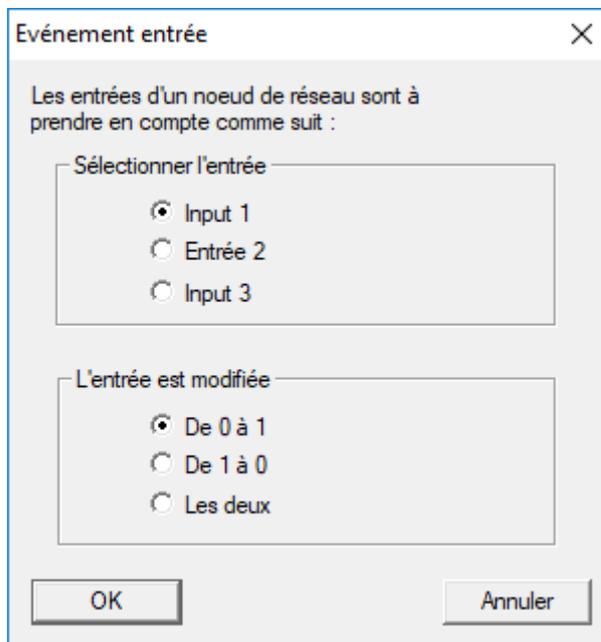
3. Saisissez un nom pour l'évènement.
4. Saisissez une description pour l'évènement (en option).
5. Saisissez un message (en option).
6. Ouvrez le menu déroulant ▼ **Type**.

7. Sélectionnez l'entrée "Évènement entrée".



8. Cliquez sur le bouton **Configurer l'évènement**.

↳ La fenêtre "Évènement entrée" s'ouvre.



9. Dans la zone "Sélectionner l'entrée", sélectionnez l'input souhaité.

10. Dans la zone "L'entrée est modifiée", sélectionnez la modification d'état qui doit déclencher l'évènement.

11. Cliquez sur le bouton **OK**.

12. Cliquez sur le bouton **Sélectionner** afin d'attribuer l'évènement à une fermeture.

↳ La fenêtre "Administration" s'ouvre.

13. Marquez une ou plusieurs fermeture(s).

14. Cliquez sur le bouton **Ajouter**.

15. Cliquez sur le bouton **OK**.

↳ La fenêtre se ferme.

↳ La fermeture est affectée à l'évènement.

16. Lorsque vous souhaitez créer une action, vous pouvez affecter une action avec le bouton **Nouveau** ou **Ajouter**.

17. Cliquez sur le bouton **OK**.
  - ↳ La fenêtre se ferme.
  - ↳ L'évènement sera affichée dans la zone "Evènements".
18. Cliquez sur le bouton **Quitter**.
  - ↳ La fenêtre se ferme.
- ↳ L'input est créé en tant qu'évènement et déclenche une action en fonction des paramètres.

#### 4.4.5 Créer une réaction

Créez tout d'abord une réaction. Cette réaction pourra être choisie plus tard lorsqu'un certain scénario surviendra.

1. Choisissez « Réseau/gestionnaire d'évènements ».
2. Dans le champ droit, cliquez sur le bouton « Nouveau » sous « Réactions ».
3. Donnez un nom et une description.
4. Choisissez le type « E-mail ».
5. Cliquez sur le bouton « Configurer réaction ».
6. Cliquez sur le bouton « Nouveau ».
7. Entrez l'adresse e-mail du destinataire ainsi que l'objet et le message. *À l'aide du bouton « Tester », vous pouvez immédiatement tester la configuration e-mail.*
8. Refermez le dialogue en cliquant trois fois sur le bouton « OK ». En cliquant sur « Terminer » vous revenez à la matrice.

#### 4.4.6 Créer un évènement

Dès qu'une réaction a été créée, il est ensuite possible de créer un évènement.

1. Choisissez « Réseau/gestionnaire d'évènements ».
2. Dans le champ droit, cliquez sur le bouton « Nouveau » sous « Évènements ».
3. Donnez un nom et une description.
4. Choisissez le type « Accès ».
5. Cliquez sur le bouton « Configurer évènement ».
6. Activer la case « Réagir à tous les transpondeurs ». *L'évènement doit survenir à chaque fois que le transpondeur est actionné. Vous pouvez aussi limiter l'évènement à certains transpondeurs.*
7. L'action peut être adaptée dans la section « Fixation de l'horaire ».
8. Cliquez sur le bouton « OK ».
9. Dans le champ « Fermetures », cliquez sur le bouton « Sélectionner ».

10. Ajoutez toutes les fermetures qui doivent déclencher l'évènement lors de l'actionnement du transpondeur et confirmez à l'aide du bouton « OK ».
11. Dans le champ « Actions associées », cliquez sur le bouton « Ajouter ».
12. Ajoutez la réaction précédemment créée.
13. Cliquez sur le bouton « Configurer horaire ».
14. Entrez les horaires de repos nocturne. L'évènement ne sera déclenché que pendant la fenêtre horaire définie.
15. Refermez le dialogue en cliquant trois fois sur le bouton « OK ». En cliquant sur « Terminer » vous revenez à la matrice.

#### 4.4.6.1 Événements possibles

La fenêtre "Nouvel événement" vous propose différents événements dans le menu déroulant ▼ **Type**.



Pour les événements DoorMonitoring, vous avez besoin d'une fermeture compatible DoorMonitoring (DM).

### Événements DoorMonitoring

Vous avez à votre disposition les événements DoorMonitoring suivants :



### État de la porte

Évènement Door Monitoring

Type d'évènement : État de la porte

Options

Porte ouverte

Porte fermée

OK Annuler

Les états suivants peuvent être détectés. Si la case est cochée, l'état est déclenché dès que l'évènement survient.

- Porte ouverte
- Porte fermée

### Mouvement du pêne dormant

Évènement Door Monitoring

Type d'évènement : Mouvement du pêne dormant

Options

- Porte déverrouillée
- Porte verrouillée
- Porte surverrouillée

OK Annuler

Les états suivants peuvent être détectés. Si la case est cochée, l'état est déclenche dès que l'évènement survient.

- Porte non verrouillée
- Porte verrouillée
- Porte verrouillée de manière sûre

### La porte reste trop longtemps ouverte

Évènement Door Monitoring

Type d'évènement : La porte reste trop longtemps ouverte

Options

- Porte ouverte trop longtemps
- Porte refermée

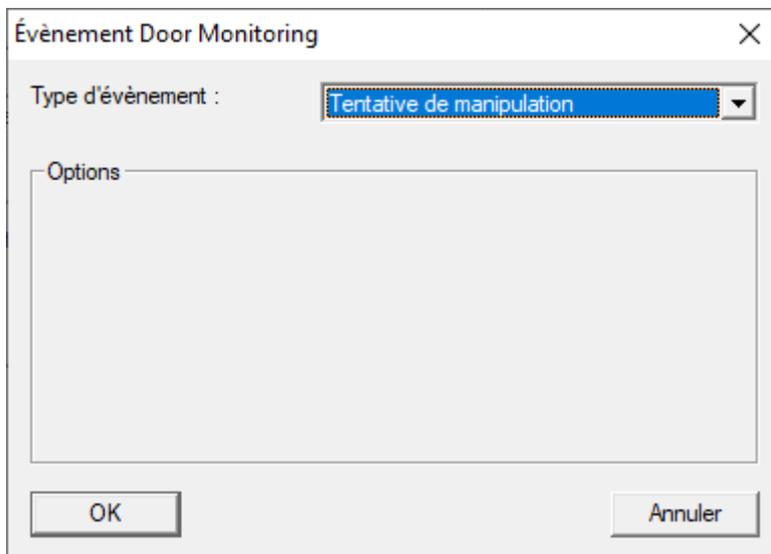
OK Annuler

Les états suivants peuvent être détectés. Si la case est cochée, l'état est déclenche dès que l'évènement survient.

- Porte restée ouverte trop longtemps

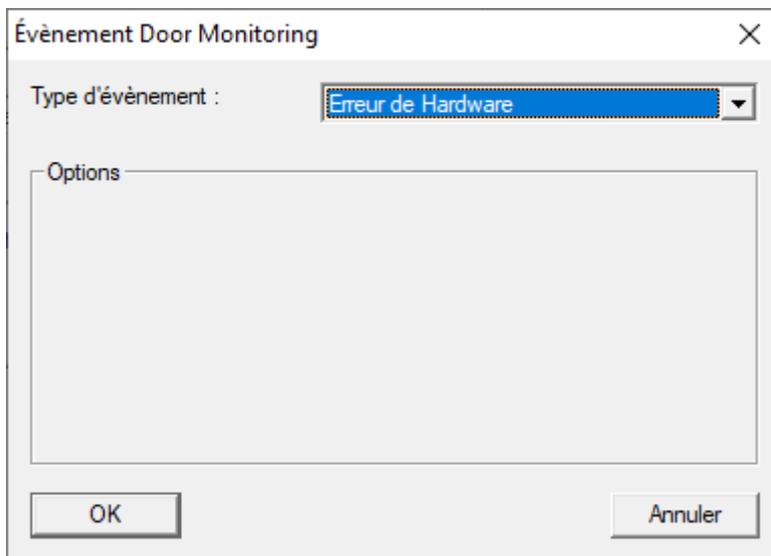
  Porte refermée

### Tentative de manipulation



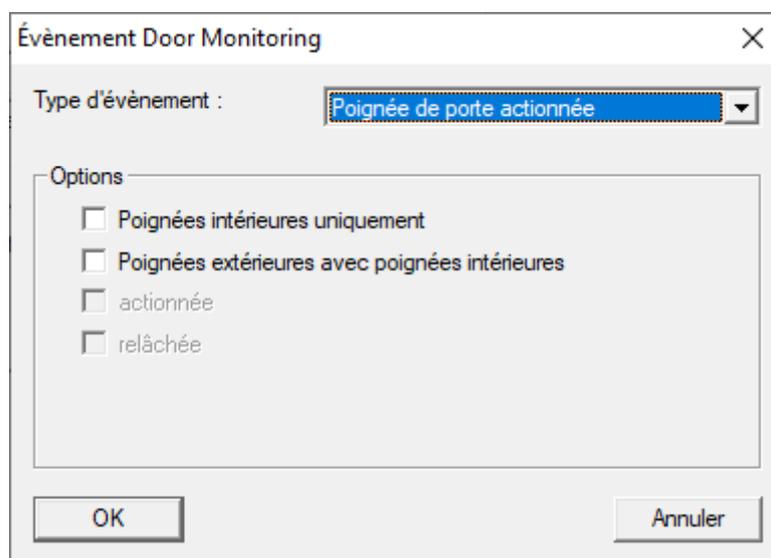
The screenshot shows a dialog box titled "Évènement Door Monitoring" with a close button (X) in the top right corner. Below the title bar, there is a label "Type d'évènement :" followed by a dropdown menu. The dropdown menu is open, and "Tentative de manipulation" is selected and highlighted in blue. Below the dropdown menu is a large, empty rectangular area labeled "Options". At the bottom of the dialog box, there are two buttons: "OK" on the left and "Annuler" on the right.

### Erreur de Hardware



The screenshot shows a dialog box titled "Évènement Door Monitoring" with a close button (X) in the top right corner. Below the title bar, there is a label "Type d'évènement :" followed by a dropdown menu. The dropdown menu is open, and "Erreur de Hardware" is selected and highlighted in blue. Below the dropdown menu is a large, empty rectangular area labeled "Options". At the bottom of the dialog box, there are two buttons: "OK" on the left and "Annuler" on the right.

### Poignée de porte actionnée



Évènement Door Monitoring

Type d'évènement : Poignée de porte actionnée

Options

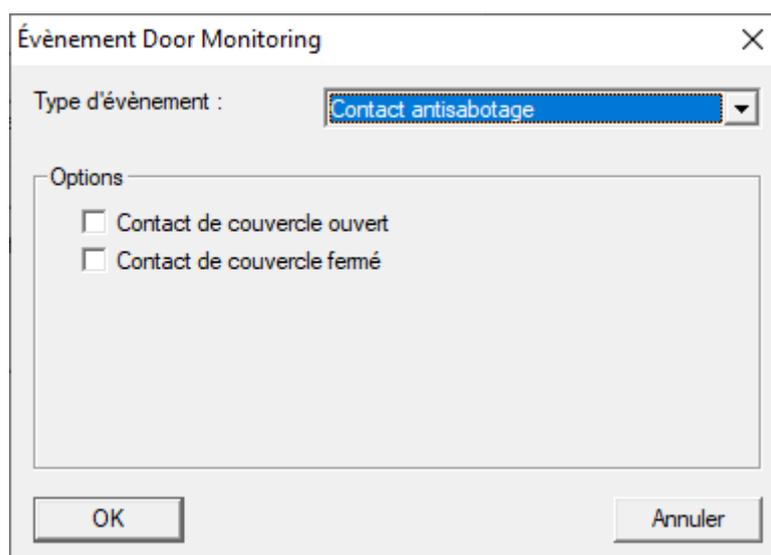
- Poignées intérieures uniquement
- Poignées extérieures avec poignées intérieures
- actionnée
- relâchée

OK Annuler

Les états suivants peuvent être détectés. Si la case est cochée, l'état est déclenche dès que l'événement survient.

- poignées intérieures uniquement
- Poignées extérieures avec poignées intérieures
- actionnée
- relâchée

### Contact antisabotage



Évènement Door Monitoring

Type d'évènement : Contact antisabotage

Options

- Contact de couvercle ouvert
- Contact de couvercle fermé

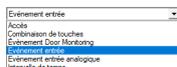
OK Annuler

Les états suivants peuvent être détectés. Si la case est cochée, l'état est déclenche dès que l'événement survient.

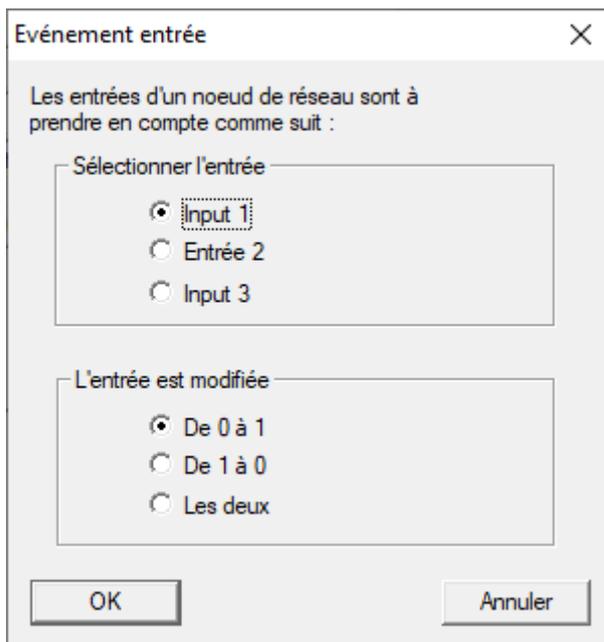
- Contact de couvercle ouvert
- Contact de couvercle fermé

## Événements standard

Vous avez à votre disposition les événements standard suivants :



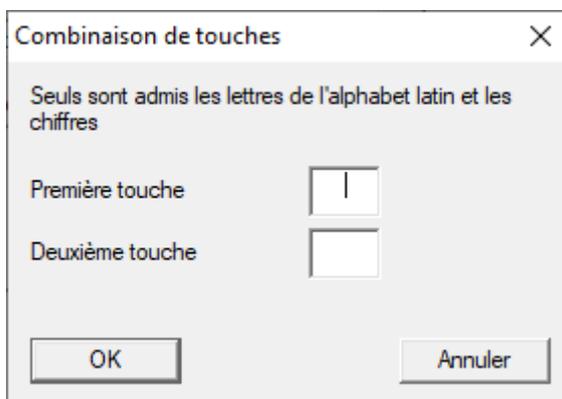
### Événement entrée



### Entrée Événement Analogique

Les paramètres des événements d'entrées analogiques sont appliqués directement à l'appareil correspondant (par exemple RouterNode 2).

### Combinaison de touches



### Intervalle de temps

Evénmt. à interv. de temps

Evénement activé après dépassement de l'intervalle de temps suivant

Intervalle de temps  Min.

OK Annuler

### Accès

Evénement d'accès

Réagir à tous les transpondeurs

Réagir seulement aux transpondeurs suivants :

Plan de fermeture:

Réglage du temps

Événement en temps réel. Possible uniquement avec une fermeture G2 dans un réseau direct

Prendre en compte toutes les visites des lieux

Heures

Ne pas tenir compte des franchissements remontant plus loin que la date/heure prescrite

OK Annuler

## 4.5 Gérer le réseau virtuel (VN)

Les autorisations peuvent être modifiées sans mise en réseau online via un réseau virtuel (réseau VN). L'autorisation pour des serrures (et les identifiants bloqués) est enregistrée directement sur l'identifiant et est transmise à une fermeture à chaque passage. Par conséquent, dans le réseau virtuel, il est important que tous les identifiants ont un passage régulier sur les bornes actualisatrices de droit d'accès.

Cet exemple illustre le principe de configuration d'un réseau virtuel.

Pour le réseau virtuel, une configuration de carte AV (AV = **A**udit trail / **V**irtual network) est nécessaire lors de l'utilisation d'un identifiant Mifare.

#### 4.5.1 Réseau virtuel avec SmartRelais 3 Advanced



##### NOTE

##### Exigences système accrues pour des réseaux virtuels SmartRelais 3 Advanced

Le réseau virtuel avec serveur VNHost et SmartRelais 3 Advanced est très performant et les exigences relatives à la capacité disponible sont plus élevées.

- Respectez les exigences système accrues (voir *Exigences système* [▶ 7]).

##### 4.5.1.1 Principe de fonctionnement

Une utilisation en tant que borne actualisatrice dans le réseau virtuel est possible. Pour cela, le contrôleur établit une liaison avec le serveur VNHost. Le serveur VNHost transmet des autorisations modifiées (programmation requise) et des données de la LSM vers le contrôleur. Ainsi, plus aucun chargement complet et chronophage de la base de données n'est nécessaire, mais le contrôleur va chercher les données disponibles en cas de détection d'un identifiant (principe Pull). L'ensemble du système est programmé via une interface unique, le contrôleur.

Le serveur VNHost vérifie à intervalles réguliers s'il y a des modifications dans la base de données LSM qui doivent être diffusées sur la borne actualisatrice. À l'inverse, il vérifie également s'il existe des informations sur la borne actualisatrice qui doivent être inscrites dans la base de données (voir *Vérifier l'état du réseau virtuel* [▶ 83]).

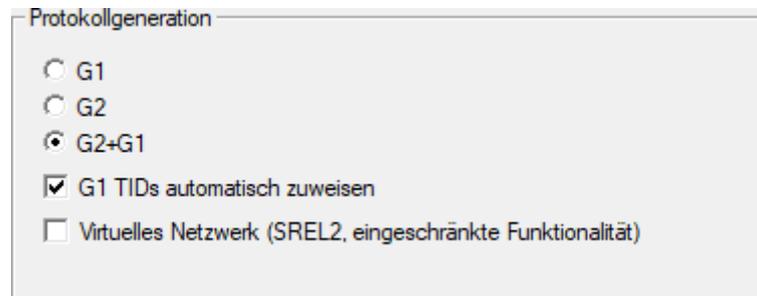
##### 4.5.1.2 Configurer un système de fermeture

Pour un réseau virtuel avec SmartRelais 3 Advanced, aucune préparation particulière n'est nécessaire.

Dans les propriétés du système de fermeture, la case à cocher  Réseau virtuel (SREL2, fonctionnalité réduite) ne doit pas être activée.

1. Cliquez sur | Traiter | - **Propriété du plan de fermeture** pour ouvrir les propriétés de votre système de fermeture.
2. Accédez à l'onglet [Nom].

3. Veillez à ce que la case à cocher  Réseau virtuel (SREL2, fonctionnalité réduite) ne soit pas activée.



Protokollgeneration

G1

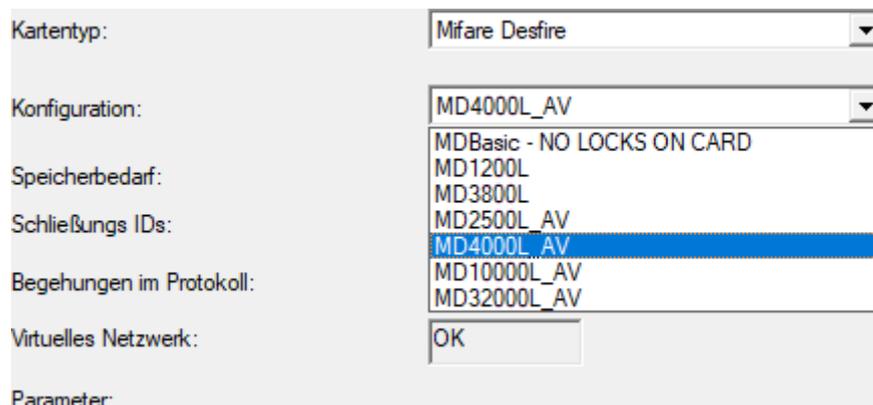
G2

G2+G1

G1 TIDs automatisch zuweisen

Virtuelles Netzwerk (SREL2, eingeschränkte Funktionalität)

4. Cliquez sur le bouton **Accepter**.
5. Si vous utilisez des cartes : Le cas échéant, sélectionnez une configuration de carte AV dans l'onglet [Gestion des cartes G2].



Kartentyp: Mifare Desfire

Konfiguration: MD4000L\_AV

Speicherbedarf:

Schließungs IDs:

Begehungen im Protokoll:

Virtuelles Netzwerk: OK

Parameter:

6. Cliquez sur le bouton **Accepter**.

#### 4.5.1.3 Configurer une borne actualisatrice et un serveur VNHost

- ✓ Plan de fermeture créé (voir *Configurer un système de fermeture* [▶ 78]).
  - ✓ SmartRelais 3 Advanced configuré et en réseau (voir le manuel du système de SmartRelais 3 Advanced).
  - ✓ VNHost installé (voir VNHost).
1. Au moyen de | Traiter | - **Propriété du dispositif de fermeture**, ouvrez les propriétés de SmartRelais 3 Advanced (autrement : double-clic).

2. Accédez à l'onglet [Équipement].

Soll

Schließanlagen ID  
9215

Schließungs ID  
173

Pulslänge 2 Sek.

Zugangskontrolle  
 Zeitzonesteuerung  
 Unberechtigte Zutrittsversuche protokollieren  
 Gateway  
 Flip Flop  
 Keine Batteriewarnungen  
 Nahbereichsmodus  
 Zeitschaltung  
 Aktivierungs- bzw. Verfallsdatum ignorieren  
 Karteninterface

letzte Veränderung

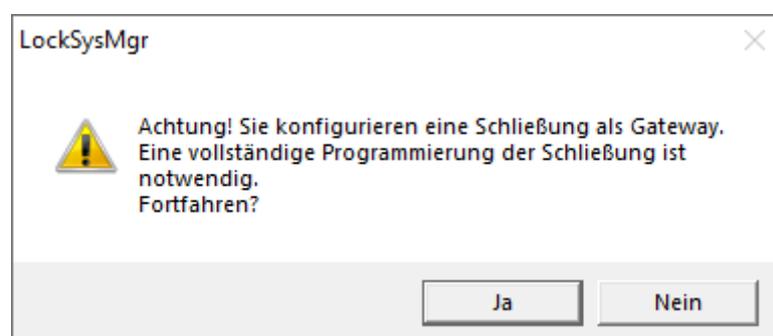
Zeitzone:	21.06.18 17:30:10
Feiertagslisten:	nicht vorhanden

Erweiterte Konfiguration

3. Activez les cases à cocher  Gestion des plages horaires et  Contrôle d'accès.

4. Activez la case à cocher  Gateway.

↳ Un avertissement concernant la programmation en attente s'ouvre.



5. Cliquez sur le bouton **OK**.

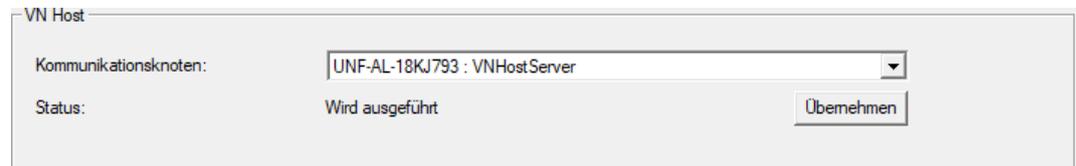
↳ L'avertissement se ferme.

6. Cliquez sur le bouton **Oui**.

↳ La programmation requise (éclair) s'affiche.

7. Autorisez tous les identifiants qui doivent obtenir de nouvelles autorisations sur la borne actualisatrice par la suite.

8. Programmez SmartRelais 3 Advanced.
  - ↳ La programmation requise disparaît.
9. Au moyen de | Réseau |, sélectionnez l'entrée Réseau virtuel.
  - ↳ La fenêtre "Serveur VNHost" s'ouvre.



VN Host

Kommunikationsknoten: UNF-AL-18KJ793 : VNHostServer

Status: Wird ausgeführt

Übernehmen

10. Dans la zone "VNHost", assurez-vous que l'entrée "Serveur VNHost" est sélectionnée dans le menu déroulant ▼ Noeuds de communication.



#### NOTE

#### Nœuds de communication différents sur SmartRelais 3 Advanced

Serveur VNHost est toujours utilisé pour le réseau virtuel sur SmartRelais 3 Advanced. En revanche, pour la programmation, l'ouverture à distance, etc. un autre nœud de communication peut être utilisé.

- Pour le réseau virtuel, sélectionnez également l'entrée "Serveur VNHost" si votre SmartRelais 3 Advanced utilise encore un autre nœud de communication.

11. Le cas échéant, cliquez sur le bouton Accepter.
12. Cliquez sur le bouton OK.
  - ↳ La fenêtre "Serveur VNHost" se ferme.
13. Au moyen de | Réseau |, sélectionnez l'entrée Noeuds de communication.

14. Avec les boutons ◀ et ▶ accédez au nœud de communication du serveur VNHost.

Name	VNHostServer	
Rechnename	LIMPAL-1001701	
Vollständiger Rechnename		
IP Port	6001	Port suchen
Beschreibung		

Anschlüsse:

Typ	COM-Port	

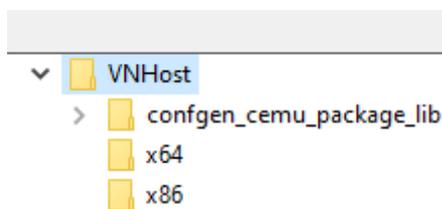
Ping  
Konfig-Dateien  
Übertragen  
Testen  
Bearbeiten  
Hinzufügen  
Entfernen  
Verschieben

Neu    Bearbeiten    Übernehmen    Beenden    Hilfe

15. Cliquez sur le bouton Configuration.

↳ La fenêtre Explorer s'ouvre.

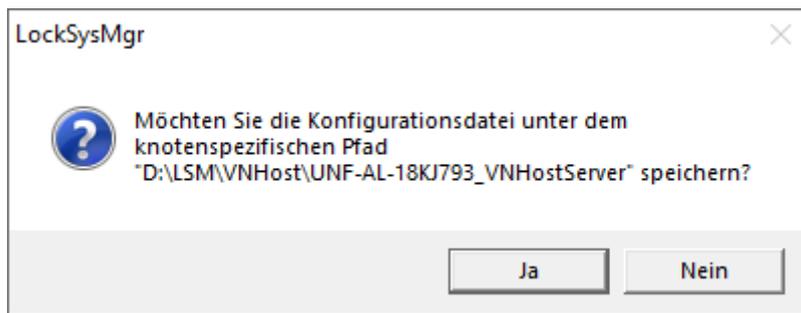
16. Sélectionnez le dossier d'installation du serveur VNHost.



17. Cliquez sur le bouton OK.

↳ La fenêtre Explorer se ferme.

↳ La fenêtre "LockSysMgr" s'ouvre.



18. Cliquez sur le bouton **No**.

↳ Les fichiers de configuration sont enregistrés.



19. Cliquez sur le bouton **Transférer**.

↳ Les fichiers de configuration sont transmis au nœud de communication du serveur VNHost.

20. Si votre SmartRelais 3 Advanced est relié via un autre nœud de communication : enregistrez et transmettez aussi les fichiers de configuration pour ce nœud de communication.

↳ Réseau virtuel prêt à l'emploi.

Vous pouvez maintenant surveiller l'état de votre réseau virtuel (voir *Vérifier l'état du réseau virtuel* [► 83]).

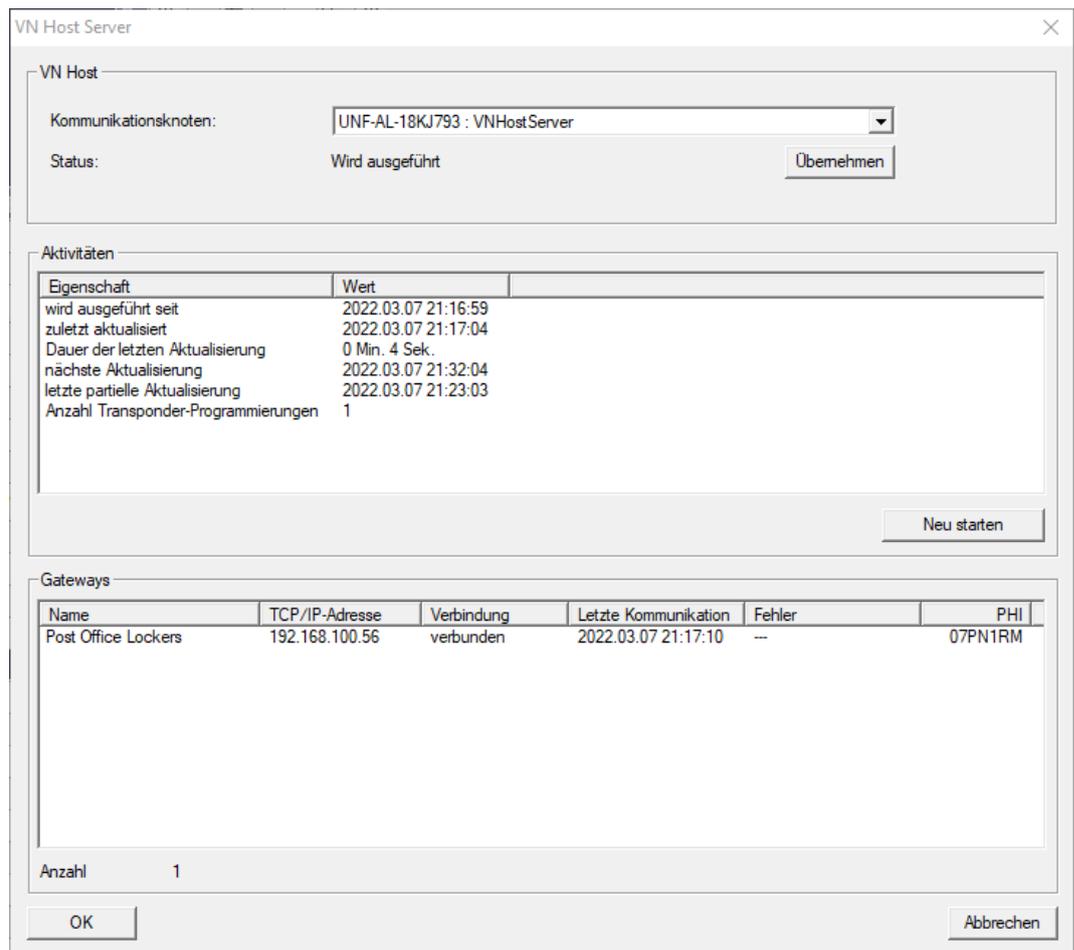
#### 4.5.1.4 Vérifier l'état du réseau virtuel

Après la configuration de votre réseau virtuel, vous pouvez surveiller son état.

✓ Réseau virtuel configuré (voir *Configurer un système de fermeture* [► 78] et *Configurer une borne actualisatrice et un serveur VNHost* [► 79]).

■ Au moyen de | Réseau |, sélectionnez l'entrée **Réseau virtuel**.

↳ La fenêtre "Serveur VNHost" indique l'état actuel.



Dans la zone "VNHost", vous voyez le nœud de communication actuellement utilisé (pour le réseau virtuel : "Serveur VNHost").

Dans la zone "Activités", vous voyez :

- Le démarrage du serveur VNHost
- La date de la dernière actualisation
- La date de la prochaine actualisation planifiée
- Le nombre de programmations en attente

Dans la zone , vous trouvez la liste de tous les "SmartRelais 3 Advanced" configurés comme  Gateway et leur état.

## 4.5.2 Réseau virtuel avec SmartRelais 2 G2

### 4.5.2.1 Principe de fonctionnement

Contrairement à SmartRelais 3, SmartRelais 2 G2 (SREL2.G2) n'est pas relié via un câble réseau mais via un nœud de réseau intégré. Par conséquent, le fonctionnement d'un réseau virtuel avec SmartRelais 2 G2 nécessite un nœud réseau intégré et un routeur, dans l'idéal un RouterNode 2 (voir *Créer des composants et configurer LSM* [▶ 90]).

Le LSM envoie les données qui doivent être diffusées dans le réseau virtuel au RouterNode 2 via un câble réseau, puis au SmartRelais 2 G2 via un nœud réseau intégré. Celui-ci fonctionne comme une passerelle.



Les identifiants qui sont utilisés sur la passerelle distribuent ensuite les données aux fermetures.

#### 4.5.2.2 Configurer l'installation de fermeture

Dans le système de fermeture G2 (pur), la case à cocher  Réseau virtuel (SREL2, fonctionnalité réduite) doit être activée.

1. Cliquez sur | Traiter | - [Propriété du plan de fermeture](#) pour ouvrir les propriétés de votre système de fermeture.
2. Accédez à l'onglet [Nom].
3. Dans la zone "Production de rapport", activez la case à cocher  Réseau virtuel (SREL2, fonctionnalité réduite).

Protokollgeneration

G1

G2

G2+G1

G1 TIDs automatisch zuweisen

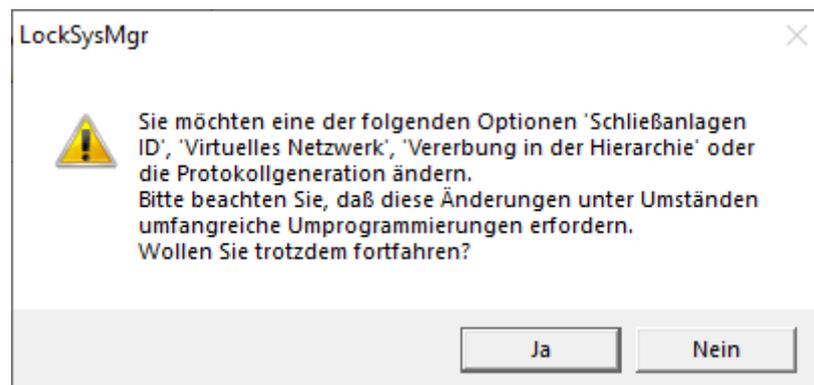
Virtuelles Netzwerk (SREL2, eingeschränkte Funktionalität)

4. Si vous utilisez des cartes : Le cas échéant, sélectionnez une configuration de carte AV dans l'onglet [Gestion des cartes G2].

Kartentyp:	Mifare Desfire
Konfiguration:	MD4000L_AV
Speicherbedarf:	MDBasic - NO LOCKS ON CARD MD1200L MD3800L MD2500L_AV MD4000L_AV
Schließungs IDs:	MD10000L_AV MD32000L_AV
Begehungen im Protokoll:	
Virtuelles Netzwerk:	OK
Parameter:	

- ↳ Le plan de fermeture est prêt pour le réseau virtuel avec SmartRelais 2 G2.

Si ce paramètre est utilisé pour un plan de fermeture existant, une programmation peut être requise.



#### 4.5.2.3 Configurer le service réseau virtuel

- ✓ Plan de fermeture configuré (voir *Créer une nouvelle installation de fermeture* [▶ 11], *Créer un nouveau transpondeur* [▶ 11] et *Créer une nouvelle fermeture* [▶ 46]).
  - ✓ Case à cocher  Réseau virtuel (SREL2, fonctionnalité réduite) activée.
  - ✓ Tous les composants programmés (voir *Programmer le transpondeur* [▶ 27] et *Programmer la fermeture* [▶ 47]).
  - ✓ SmartRelais 2 G2 en réseau (voir manuel WaveNet).
1. Au moyen de | Réseau |, sélectionnez l'entrée **Service VN (SREL2)**.
    - ↳ La fenêtre "Service VN (SREL2)" s'ouvre.

VN Dienst (SREL2)

Kommunikationsknoten:

TCP/IP Port:

VNServer Installationspfad:  ...

Import / Synchronisation

Import / Synchronisation in regelmäßigen Abständen ab der Startzeit ausführen

Synchronisationsintervall

Startzeit

Export

Den Export zu einer bestimmten Uhrzeit ausführen

Übernehmen Testen

OK Abbrechen

2. Dans le menu déroulant ▼ **Nœud de communication**, sélectionnez dans le nœud de communication : le noeud réseau intégré du Relais 2 G2 et le RouterNode2 avec lequel il communique.

VN Dienst (SREL2)

Kommunikationsknoten:

TCP/IP Port:

VNServer Installationspfad:  ...

Import / Synchronisation

Import / Synchronisation in regelmäßigen Abständen ab der Startzeit ausführen

Synchronisationsintervall

Startzeit

Export

Den Export zu einer bestimmten Uhrzeit ausführen

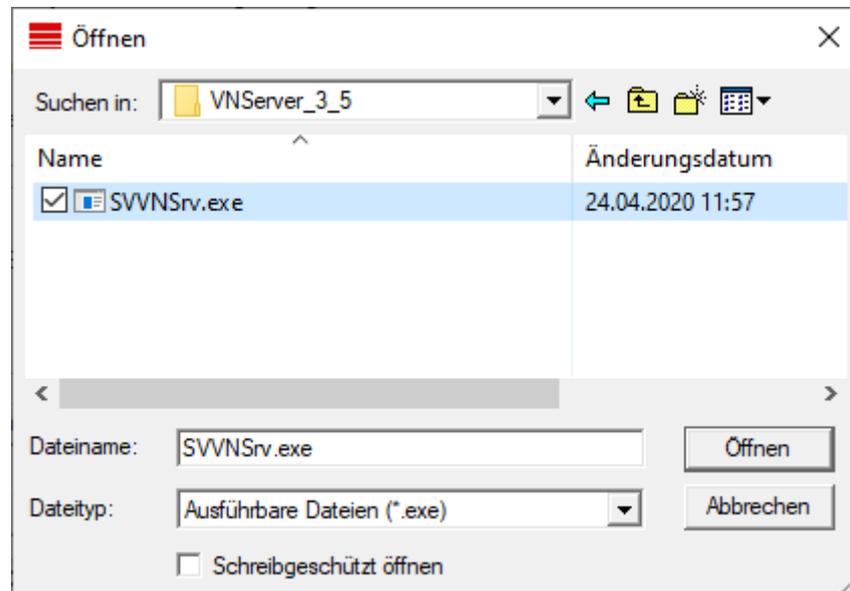
Übernehmen Testen

OK Abbrechen

3. Assurez-vous que le port TCP/IP est paramétré à 4000.
4. Ouvrez Explorer en cliquant sur le bouton ...

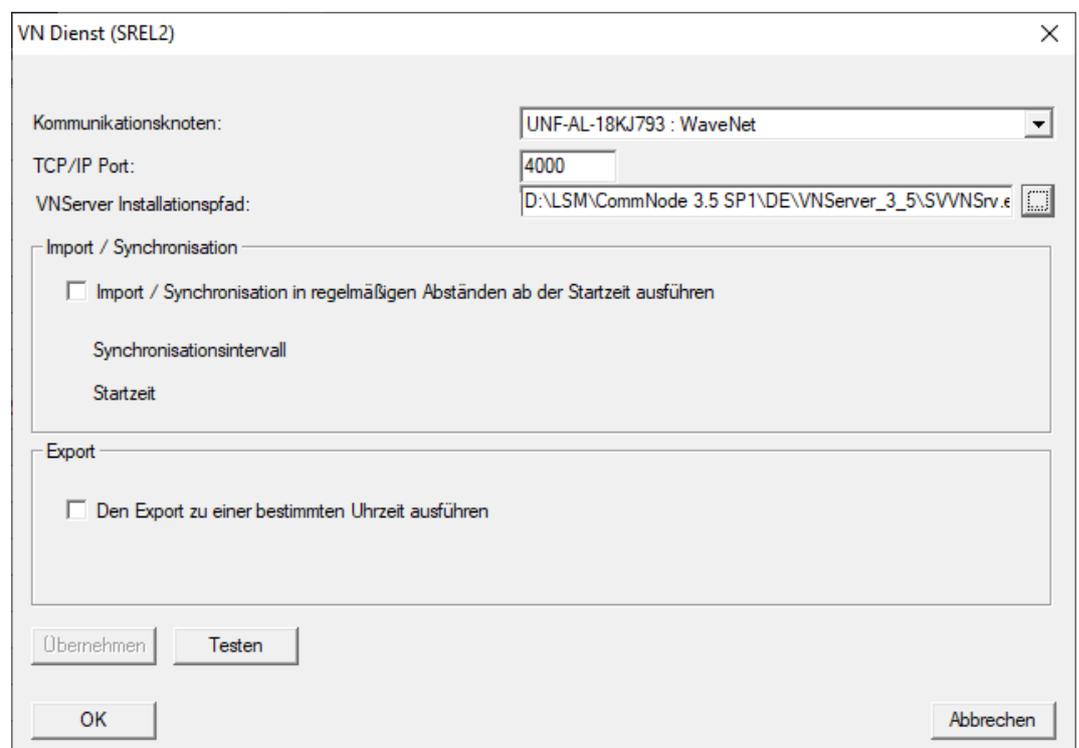
5. Sélectionnez le fichier SVVNSvr.exe.

*Le fichier SVVNSvr.exe est installé avec le serveur CommNode. Répertoire par défaut : (C:\Programme(x86)\SimonsVoss\VNServer\_x\_x)*



6. Cliquez sur le bouton Ouvrir.

↳ La fenêtre Explorer se ferme.



7. En option : Dans la zone "Import/Synchronisation", définissez quand les données du SmartRelais 2 G2 doivent être importées dans le logiciel LSM.

VN Dienst (SREL2)

Kommunikationsknoten: UNF-AL-18KJ793 : WaveNet

TCP/IP Port: 4000

VNServer Installationspfad: D:\LSM\CommNode 3.5 SP1\DE\VNServer\_3\_5\SVVNSrv.€ ...

Import / Synchronisation

Import / Synchronisation in regelmäßigen Abständen ab der Startzeit ausführen

Synchronisationsintervall: 1 Stunden

Startzeit: 20:00

Export

Den Export zu einer bestimmten Uhrzeit ausführen

Übernehmen Testen

OK Abbrechen

8. En option : Dans la zone "Export", définissez quand les données du logiciel LSM doivent être transmises au SmartRelais 2 G2.

VN Dienst (SREL2)

Kommunikationsknoten: UNF-AL-18KJ793 : WaveNet

TCP/IP Port: 4000

VNServer Installationspfad: D:\LSM\CommNode 3.5 SP1\DE\VNServer\_3\_5\SVVNSrv.€ ...

Import / Synchronisation

Import / Synchronisation in regelmäßigen Abständen ab der Startzeit ausführen

Synchronisationsintervall: 1 Stunden

Startzeit: 20:00

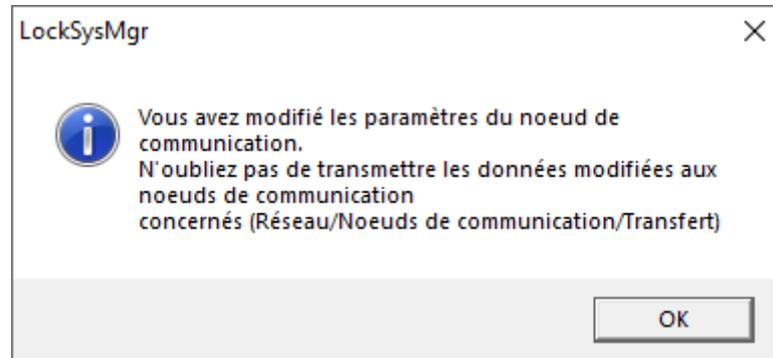
Export

Den Export zu einer bestimmten Uhrzeit ausführen 07:00

Übernehmen Testen

OK Abbrechen

9. Cliquez sur le bouton **OK**.
  - ↳ La fenêtre "LockSysMgr" s'ouvre.



10. Cliquez sur le bouton **OK**.
  - ↳ La fenêtre "LockSysMgr" se ferme.
  - ↳ La fenêtre "Service VN (SREL2)" se ferme.
11. Transmettez les paramètres à CommNode (voir *Transférer la configuration WaveNet* [▶ 57]).

#### 4.5.2.4 Créer des composants et configurer LSM

Avant que vous commenciez la configuration, il faut que les paramètres de fonctionnement d'un réseau les plus importants soient définis dans le logiciel LSM et que le RouterNode 2 soit prêt à l'emploi.

- *Préparer le logiciel LSM* [▶ 46]
- *Préparer le matériel* [▶ 47]
- *Créer des nœuds de communication* [▶ 48]
- *Configurer le service Task* [▶ 68]

1. Créez différents identifiants (par exemple *Créer un nouveau transpondeur* [▶ 11]) et fermetures (par exemple *Créer une nouvelle fermeture* [▶ 46]).
2. Effectuez la programmation initiale des composants créés (*Programmer le transpondeur* [▶ 27] et *Programmer la fermeture* [▶ 47]).
3. Créez un SmartRelais 2 G2 (▼ **Type** "SmartRelais G2 actif/hybride").
4. Ouvrez les propriétés de la fermeture.
5. Accédez à l'onglet [Équipement].

6. Activez la case à cocher  Gateway.

Soll

Schließenanlagen ID  
9215

Schließungs ID  
172

Pulslänge 5 Sek.

Zugangskontrolle  
 Zeitzonensteuerung  
 Unberechtigte Zutrittsversuche protokollieren  
 Gateway  
 Flip Flop  
 Interne Antenne immer an  
 Nahbereichsmodus (nur bei interner Antenne)  
 Zeitzumschaltung  
 Ausnahmen im Zeitzonenmanagement zulassen  
 Karteninterface

letzte Veränderung

Zeitzonen: nicht vorhanden  
Feiertagslisten: nicht vorhanden

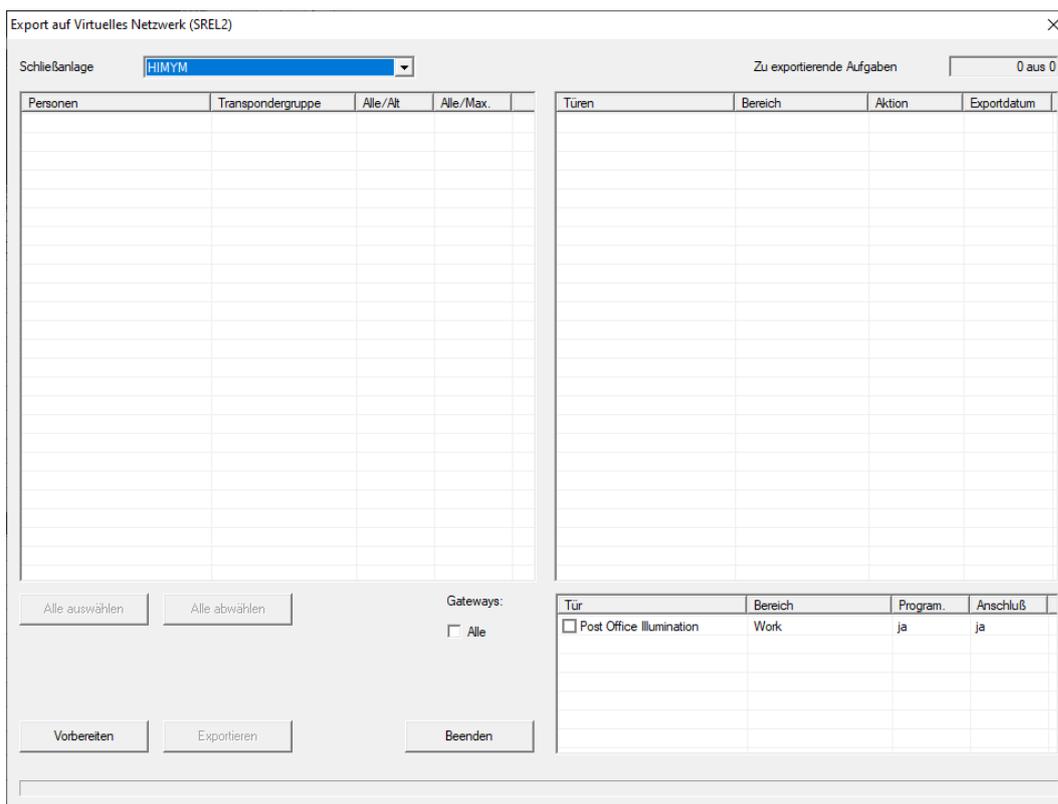
Erweiterte Konfiguration

7. Revenez à la vue matricielle.
8. Autorisez sur le SmartRelais 2 G2 tous les identifiants qui doivent obtenir de nouvelles autorisations par la suite.
9. Effectuez la programmation initiale du SmartRelais 2 G2.
10. Assurez-vous qu'un nœud réseau est installé dans le SmartRelais 2 G2.
11. Configurez le RouterNode 2 via le gestionnaire WaveNet (voir *Paramétrer le réseau et l'importer dans le LSM* [▶ 48]).
12. Associez-lui la passerelle (ou le SmartRelais 2 G2).  
↳ Le réseau virtuel est prêt à l'emploi.

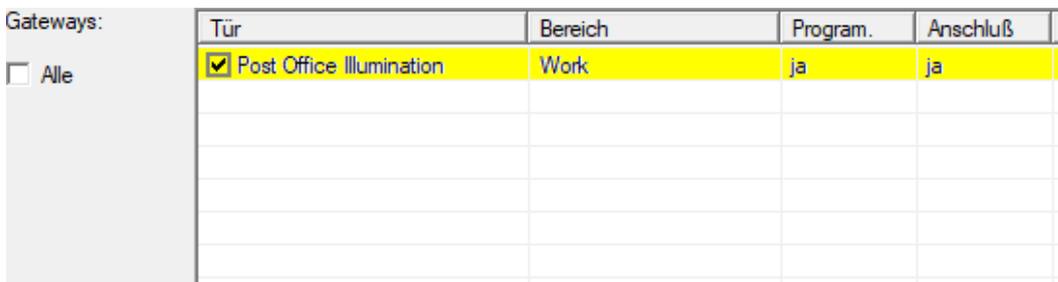
#### 4.5.2.5 Exporter les modifications d'autorisation

L'exportation des modifications d'autorisation fonctionne uniquement si au moins une modification est disponible. Effectuez un test en supprimant par exemple l'autorisation de l'identifiant 1 pour le cylindre de fermeture 1.

1. Effectuez une réinitialisation avant la première exportation (voir *Réinitialiser des tâches dans le réseau virtuel* [▶ 98]).
2. Au moyen de | Programmation | - Réseau virtuel (SREL2), sélectionnez l'entrée Exportation sur le réseau virtuel.  
↳ La fenêtre "Exportation sur le réseau virtuel (SREL2)" s'ouvre.



3. Sélectionnez tous les SmartRelais 2 G2 pour l'envoi/l'exportation des modifications.



4. Dans le menu déroulant ▼ **Système de fermeture**, vérifiez que les plans de fermeture vous avez sélectionnés sont corrects.
5. Cliquez sur le bouton **Préparer**.
  - ↳ Toutes les modifications exportables sont répertoriées dans la zone "Personnes".
6. Sélectionnez toutes les modifications que vous voulez exporter sur le SmartRelais 2 G2 préalablement défini.

Personen	Transpondergruppe	Alle/Alt	Alle/Max.
<input checked="" type="checkbox"/> Eriksen, Marshall / 004U1F2	Buero	11/00	00011/30

7. Cliquez sur le bouton **Exporter**.
  - ↳ La procédure d'exportation démarre. Les modifications sont envoyées à la borne actualisatrice.

The screenshot shows a window titled "VNServer Meldungen" with a close button (X) in the top right corner. The window contains several input fields and buttons:

- VN Befehl:**  **Stoppen**
- Ausgegeben am:**
- Zustand/Ergebnis:**  
- Gateway:**
- Letzte Meldung:**
- Aktuelle Aktion 1:**
- Aktuelle Aktion 2:**

Below these fields is a table with two columns: "Name" and "Ergebnis". The table is currently empty.

At the bottom, there is a section titled "Sonstige Aktivitäten" with a "Wechseln" button:

- VN Befehl:**
- Ausgegeben am:**
- Zustand/Ergebnis:**
- Letzte Meldung am:**

A **Beenden** button is located at the bottom right of the window.

- ↳ Le résumé de l'exportation s'affiche.

VN Ergebnis

VN Befehl: VN Export  
 Ausgegeben am: 2022.03.07 16:32:07  
 Zustand/Ergebnis: erfolgreich durchgeführt

Zusammenfassungen:

Beschreibung	Uhrzeit	Name	Wert	Name	Wert
Geräteabgleich läuft	2022.03.07 16:3...				
Aufgaben für Transponder vorbereitet	2022.03.07 16:3...	Insgesamt		Ausgeführt	
Vorverarbeitung beendet	2022.03.07 16:3...				
Aktualisierung Gateways abgeschlossen	2022.03.07 16:3...	Insgesamt	1	Fehlerhaft	0
Datenblock erfolgreich übertragen	2022.03.07 16:3...	phi	7859...	phi extension	0
Aktualisierung Gateways abgeschlossen	2022.03.07 16:3...	Insgesamt	1	Fehlerhaft	0

Parameter:

Name	Wert
Insgesamt	1
Fehlerhaft	0

Fehler:

Beschreibung	Uhrzeit	Name	Wert	Name	Wert

Beenden

Vous pouvez maintenant suivre les tâches exportées dans la vue d'ensemble (*État des tâches dans le réseau virtuel (SREL2.G2)* [▶ 97]).

La modification d'autorisation est désormais disponible sur la borne actualisatrice. Il existe alors deux scénarios :

- L'identifiant 1 s'enregistre sur la borne actualisatrice. La fermeture 1 détectera plus tard que l'identifiant 1 n'est plus autorisé et refusera l'accès.
- Un autre identifiant (différent de l'identifiant 1) s'enregistre d'abord sur la borne actualisatrice et s'autorise sur la fermeture 1. L'ID de blocage de l'identifiant 1 est communiqué au cylindre de fermeture 1.

À partir de LSM 3.5 SP3, il est possible de « donner » n'importe quel transpondeur jusqu'à deux autres ID de transpondeur devant être bloqués.

### Programmer directement des TID à bloquer

Les ID à bloquer sont enregistrés sur l'identifiant lors de la procédure de programmation.

- ✓ L'identifiant est disponible physiquement.
- ✓ La fenêtre de programmation de l'identifiant est ouverte.

1. Cliquez sur le bouton **TIDs our désactiver**.

Transponder programmieren

Besitzer / Transponder: Aldrin, Lily / 005MBA8

Programmiergerät: UNF-AL-18KJ793 : COM(\*)

Nach der Programmierung zum nächsten Transponder springen

Deaktivierungsquittungen / Batteriewarnungen auslesen

G1 Datensätze aus fremden Schließanlagen beibehalten

Programmieren TIDs zum Deaktivieren Beenden

↳ Une liste s'ouvre.

TIDs zum Deaktivieren

Schließanlage HIMYM

G2 TIDs  G1 TIDs

Transponder: Aldrin, Lily / 005MBA8

TID	Typ	Besitzer	Seriennummer	Zustand
<input type="checkbox"/> 3228	G2	Zinman, Stella	00XDESA	verloren

Es können für einen Transponder nur zwei deaktivierte TIDs ausgewählt werden

Achtung! Diese Änderungen erzeugen keinen Programmierbedarf. Vergessen Sie nicht den Transponder zu programmieren oder an einem Smart Relais 3 - Gateway zu buchen

OK Überehmen Abbrechen

2. Cochez jusqu'à deux cases dans la colonne TID pour enregistrer les TID à supprimer sur l'identifiant.
  3. Confirmez la sélection en cliquant sur le bouton OK.
  4. Poursuivez la programmation.
- ↳ Les TID sélectionnés sont enregistrés sur l'identifiant en tant que TID à supprimer. Si l'identifiant s'authentifie sur une fermeture concernée, les TID à supprimer sont bloqués sur la fermeture.

### Enregistrer les TID à bloquer dans les propriétés

Les ID à bloquer sont enregistrés sur l'identifiant pendant la procédure de programmation suivante ou lors de l'activation suivante sur une borne actualisatrice.

✓ La fenêtre de propriétés de l'identifiant est ouverte.

1. Accédez à l'onglet [Configuration].

Soll-Zustand

Langes Öffnen  
 Kein akustisches Öffnungssignal  
 Begehungsliste

Dynamisches Zeitfenster

Zeitfenster am Gateway nicht verändern  
 bis zu einer bestimmten Uhrzeit des (nächsten) Tages  
 Stundenanzahl ab der letzten vollen Std. der Buchung

Aktivierungsdatum

ab sofort

Verfallsdatum

ohne Verfallsdatum

Zeitzonegruppe

G1 Gruppe 2  
G2 Gruppe 3

TIDs zum Deaktivieren

2. Cliquez sur le bouton TIDs our désactiver .

↳ Une liste s'ouvre.

TIDs zum Deaktivieren

Schließanlage HIMYM

G2 TIDs  G1 TIDs

Transponder: Aldrin, Lily / 005MBA8

TID	Typ	Besitzer	Seriennummer	Zustand
<input type="checkbox"/> 3228	G2	Zinman, Stella	00XDESA	verloren

Es können für einen Transponder nur zwei deaktivierte TIDs ausgewählt werden

Achtung! Diese Änderungen erzeugen keinen Programmierbedarf. Vergessen Sie nicht den Transponder zu programmieren oder an einem Smart Relais 3 - Gateway zu buchen

OK Übernehmen Abbrechen

3. Cochez jusqu'à deux cases dans la colonne TID pour enregistrer les TID à supprimer sur l'identifiant.



2. Sélectionnez un utilisateur pour afficher ses tâches exportées.

Benutzer	Exportdatum	Ausführen von	Ausführen bis	Gateway
Admin	2022.03.07 16:32	2022.03.07 16:32	2022.03.07 16:32	Post Office Illumination/00CP17B

Schließanlage	Schließung	Transponder	G1/G2	Aktion	Status	Beauftragt	Transporttyp
HIMYM	Alle Schließungen	Zinman, Stella/0...	G2	deaktivieren	angenommen	0	unmittelbar
HIMYM	Goliath National Bank/00D...	Eriksen, Marshal...	G2	verbieten	übertragen	Eriksen, Marshal...	unmittelbar
HIMYM	Goliath National Bank/00D...	Eriksen, Marshal...	G2	verbieten	übertragen	Eriksen, Marshal...	unmittelbar
HIMYM	Post Office Lockers/07PN...	Eriksen, Marshal...	G2	erlauben	übertragen	Eriksen, Marshal...	unmittelbar

Status auswählen

- exportiert
- angenommen
- übertragen
- durchgeführt
- gespeichert
- abgelehnt

Befehle in Bearbeitung

Beenden

↳ Les tâches exportées s'affichent.

#### 4.5.2.7 Réinitialiser des tâches dans le réseau virtuel

Vous pouvez également réinitialiser des tâches que vous avez exportées dans le réseau virtuel.

1. Au moyen de | Programmation | - Réseau virtuel (SREL2), sélectionnez l'entrée Remise à zéro des tâches du réseau virtuel.

↳ Une remarque sur la réinitialisation s'ouvre.



2. Cliquez sur le bouton Oui.

↳ Les bornes actualisatrices sont programmées pour réinitialiser les tâches exportées.

VNServer Meldungen ✕

VN Befehl:

Ausgegeben am:

Zustand/Ergebnis:  

Gateway:

Letzte Meldung:

Aktuelle Aktion 1:

Aktuelle Aktion 2:

Name	Ergebnis
------	----------

Sonstige Aktivitäten

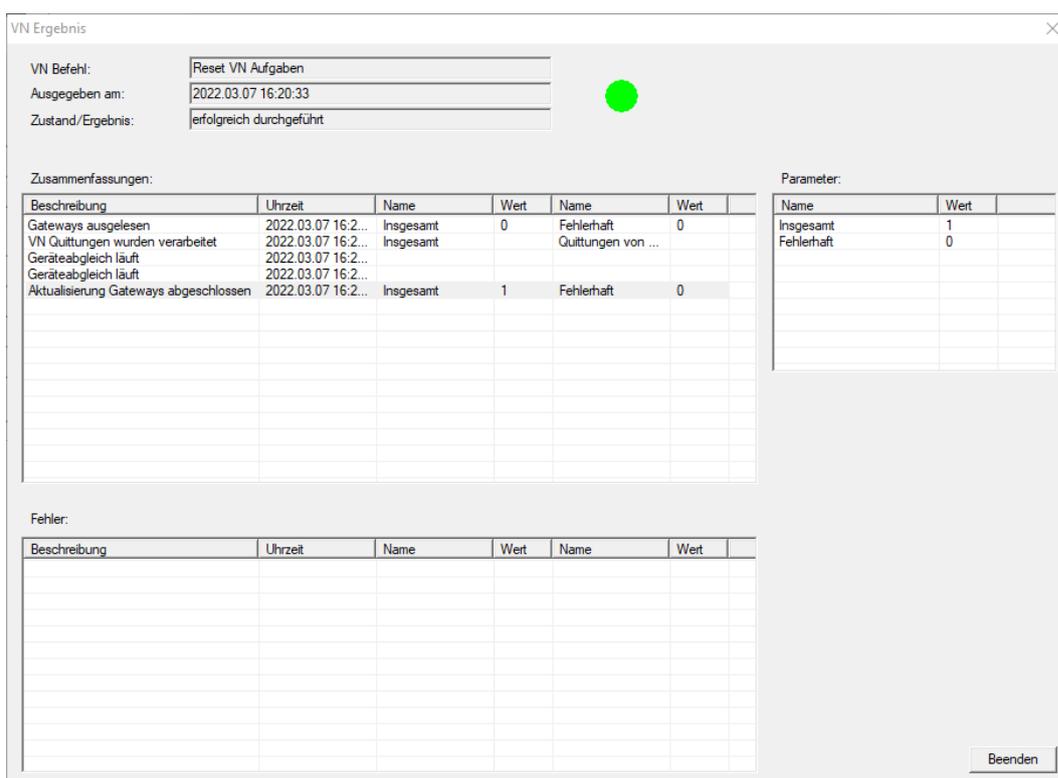
VN Befehl:

Ausgegeben am:

Zustand/Ergebnis:

Letzte Meldung am:

↳ Les tâches exportées sont réinitialisées.



Vous pouvez de nouveau exporter les tâches souhaitées dans le réseau virtuel (voir *Exporter les modifications d'autorisation* [► 91]).

#### 4.5.2.8 Importer les modifications d'autorisation

Après l'exportation des modifications sur la borne actualisatrice, vous ne voyez d'abord pas dans le logiciel LSM quelles modifications ont déjà été récupérées par la l'identifiant. Pour cela, vous devez importer de nouveau les modifications :

1. Au moyen de | Programmation | - Réseau virtuel (SREL2), sélectionnez l'entrée **Importation / Synchronisation**.  
↳ La procédure d'importation démarre immédiatement.

VNServer Meldungen ✕

VN Befehl:  Stoppen

Ausgegeben am:

Zustand/Ergebnis:  

Gateway:

Letzte Meldung:

Aktuelle Aktion 1:

Aktuelle Aktion 2:

Name	Ergebnis
Post Office Illumination / 00CP17B	

Sonstige Aktivitäten

VN Befehl:

Ausgegeben am:

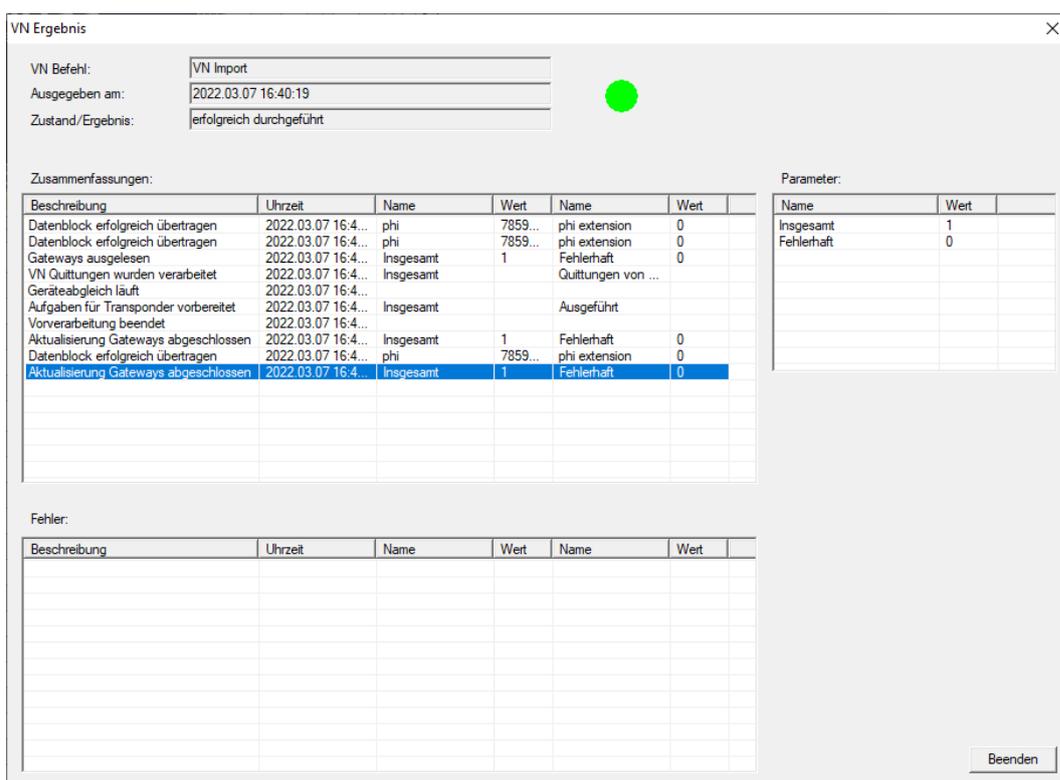
Zustand/Ergebnis:

Letzte Meldung am:

Wechseln

Beenden

↳ Le rapport d'importation s'affiche.



2. Cliquez sur le bouton **Quitter**.

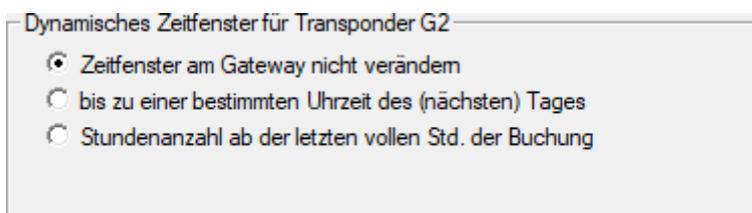
Vous pouvez maintenant vérifier l'état des tâches (voir *État des tâches dans le réseau virtuel (SREL2.G2)* [▶ 97]).

#### 4.5.2.9 Conseils concernant le réseau virtuel

##### Budget temps

Pour distribuer rapidement les modifications « offline » dans le système de fermeture, il est important que tous les identifiants s'enregistrent à intervalles fréquents et réguliers. Pour cela, il est possible de travailler avec des budgets temps.

La zone "Créneau horaire dynamique pour lle transpondeur G2" dans les propriétés du plan de fermeture vous offre la possibilité d'imposer un budget temps à des identifiants. Une personne est obligée de recharger régulièrement l'identifiant sur la borne actualisatrice. Autrement, le support d'identification est bloqué pour ce plan de fermeture.



### Importation/exportation automatiques

Vous pouvez automatiser ici l'importation et l'exportation de modifications sur une borne actualisatrice : | Réseau | - [Service VN \(SREL2\)](#).

#### ATTENTION

#### Surcharge du WaveNet à la suite d'importation et d'exportation

Lorsque plusieurs applications sont exportées ou importées simultanément, le WaveNet est alors fortement sollicité. Cela peut donc influencer les autres fonctions qui utilisent également WaveNet.

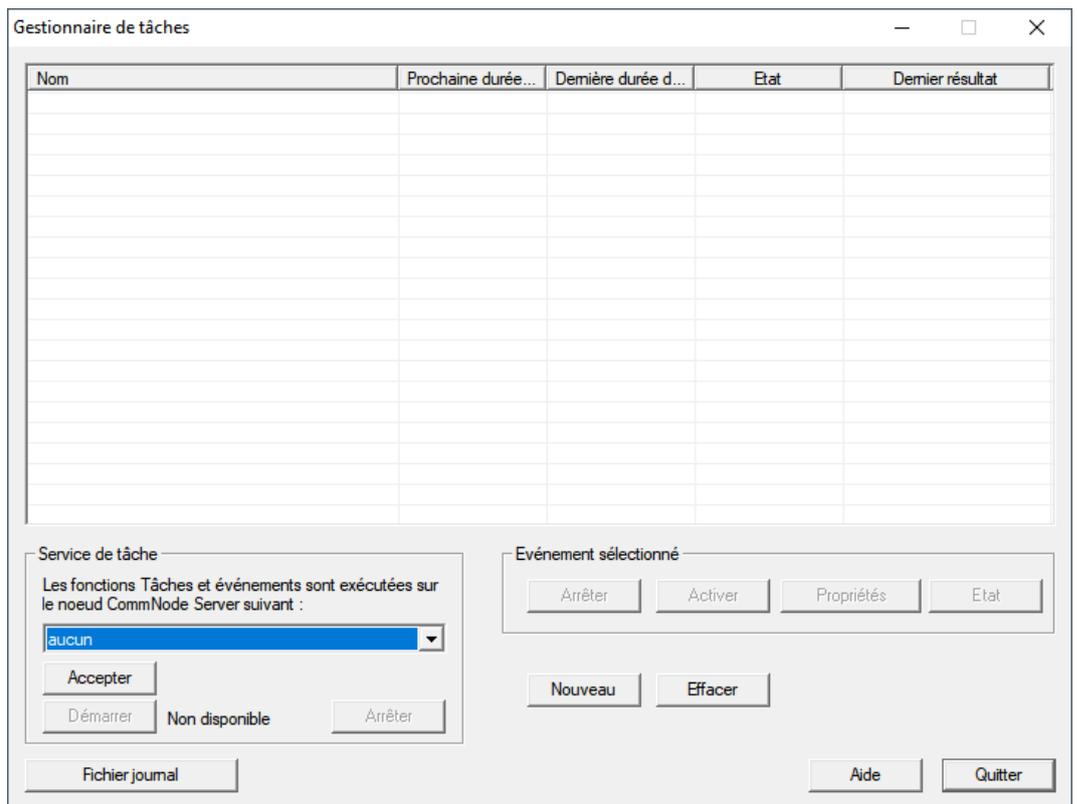
## 4.6 Lecture d'une fermeture

Une des principaux avantages des fermetures en réseau est que vous pouvez consulter leur état depuis votre poste de travail.

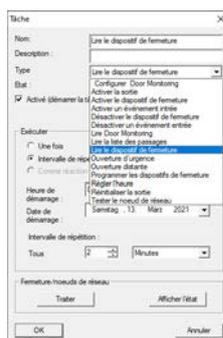
Avec le gestionnaire de tâches, vous pouvez même automatiser cette tâche.

Vous pouvez ensuite traiter les informations dans le logiciel LSM, par exemple à l'aide d'avertissements ou de messages (voir Écran d'avertissement et Gérer les alertes).

- ✓ LSM ouvert.
  - ✓ Programmation et mise en réseau de fermetures à lire (voir *Création d'un réseau radio WaveNet et connexion d'une fermeture* [► 46]).
1. Au moyen de | Réseau |, sélectionnez l'entrée [Gestionnaire de tâches](#).
    - ↳ La fenêtre "Gestionnaire de tâches" s'ouvre.



2. Cliquez sur le bouton **Nouveau** pour créer une nouvelle tâche.  
↳ La fenêtre "Tâche" s'ouvre.
3. Donnez un nom à la tâche.
4. Dans le menu déroulant ▼ **Type**, sélectionnez l'entrée "Lire le dispositif de fermeture".



5. Dans la zone "Exécution", sélectionnez l'option  Intervalle de répétition.
6. Définissez l'intervalle souhaité.



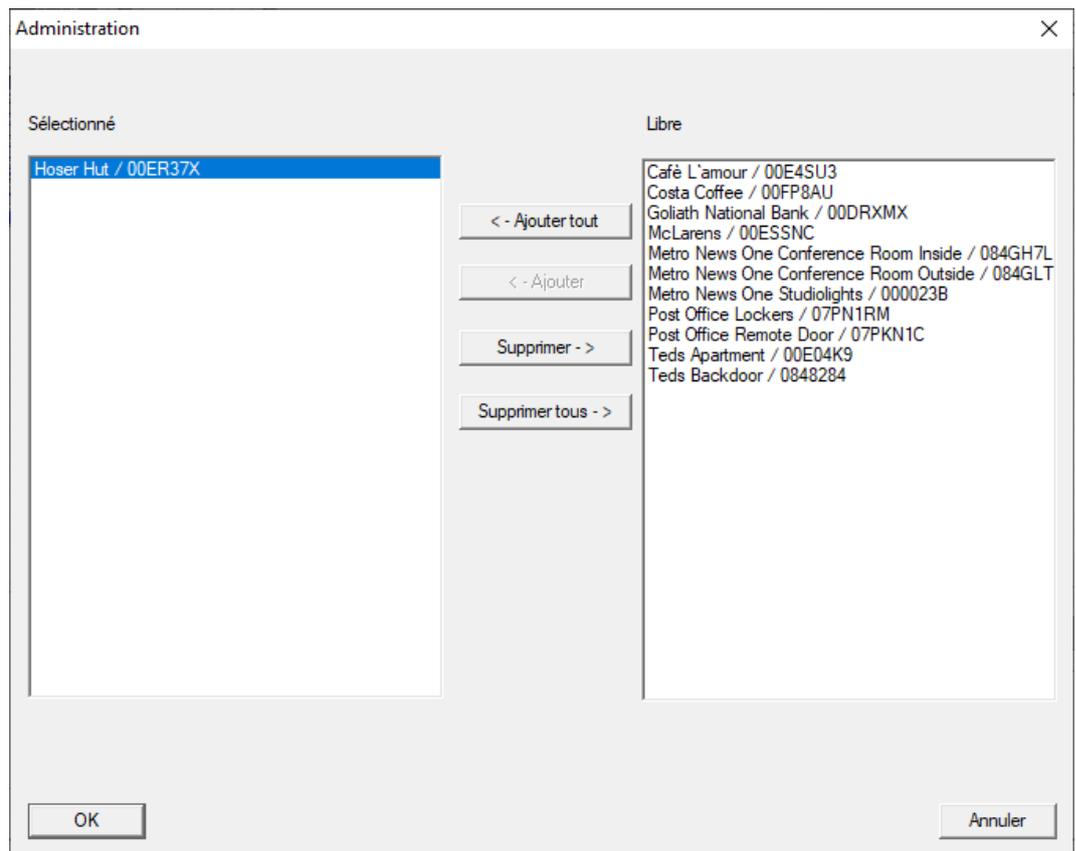
## NOTE

### Influence de l'intervalle de répétition sur l'autonomie des piles

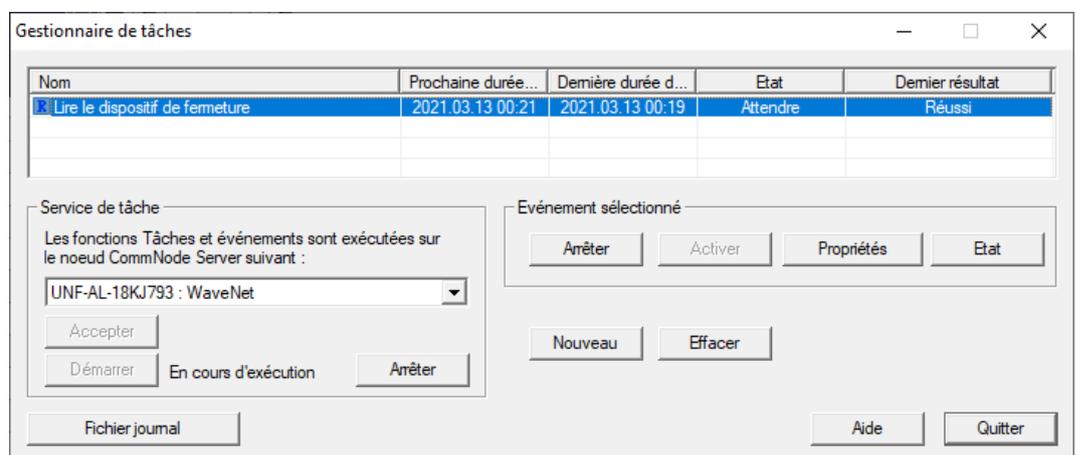
Plus la fréquence de lecture de la fermeture est élevée, moins la fermeture est en mode veille à faible consommation. L'autonomie des piles peut donc être réduite.

7. Dans la zone "Fermeture/noeuds de réseau", cliquez sur le bouton **Traiter**.

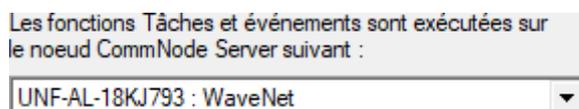
↳ La fenêtre "Administration" s'ouvre.



8. Sélectionnez la fermeture à lire.
9. Avec le bouton **Ajouter**, faites ensuite glisser les fermetures dans la colonne de gauche.
10. Cliquez sur le bouton **OK**.
  - ↳ La fenêtre "Administration" se ferme.
11. Cliquez sur le bouton **OK**.
  - ↳ La fenêtre "Tâche" se ferme.
  - ↳ La tâche est indiquée dans le gestionnaire de tâches.



12. Dans la zone "Service de tâche", assurez-vous que le CommNode correspondant est sélectionné dans le menu déroulant ▼ Les fonctions Tâches et événements sont exécutées sur le noeud CommNode Server suivant.



13. Assurez-vous que le gestionnaire de tâches est également lancé.



14. Cliquez sur le bouton Quitter .
- ↳ La fenêtre "Gestionnaire de tâches" se ferme.
  - ↳ L'état des fermetures paramètres est automatiquement consulté.

## 5. Aide et autres informations

### Documentation/documents

Les informations détaillées concernant le fonctionnement et la configuration peuvent être consultées sur la page d'accueil :

<https://www.simons-voss.com/fr/documents.html>

### Logiciels et pilotes

Les logiciels et les pilotes peuvent être trouvés sur la page d'accueil :

<https://www.simons-voss.com/fr/telechargements/telechargements-de-logiciels.html>

### Déclarations de conformité

Les déclarations de conformité et autres certificats peuvent être consultées sur la page d'accueil :

<https://www.simons-voss.com/fr/certificats.html>

### Assistance technique

Notre support technique se fera un plaisir de vous aider (ligne fixe, coût dépendant de l'opérateur) :

+49 (0) 89 / 99 228 333

### E-Mail

Vous préférez nous envoyer un e-mail ?

[support-simonsvoss@allegion.com](mailto:support-simonsvoss@allegion.com)

### FAQ

Les informations et aides relatives peuvent être consultées sur la section Section FAQ:

<https://faq.simons-voss.com/otrs/public.pl>

### Adresse

SimonsVoss Technologies GmbH  
Feringastr. 4  
D-85774 Unterfoehring  
Allemagne



## Voici SimonsVoss

SimonsVoss, le pionnier de la technologie de contrôle des accès sans fil, propose une large gamme de produits pour le secteur des TPE et des moyennes et grandes entreprises ainsi que des organismes publics. Les solutions de fermeture SimonsVoss allient fonctionnalités intelligentes, qualité exceptionnelle, design récompensé et fabrication allemande.

En tant que fournisseur de solutions innovantes, SimonsVoss est particulièrement attaché à l'évolutivité des systèmes, à la sécurité, à la fiabilité des composants, à la performance des logiciels et à la simplicité

d'utilisation. SimonsVoss est ainsi considéré comme une entreprise à la pointe de la technologie dans le domaine des systèmes numériques de fermeture. SimonsVoss est la seule société à proposer une surveillance de porte en ligne sans fil adaptée aux cylindres numériques. L'esprit d'innovation, la durabilité, la responsabilité et la haute estime des collaborateurs et partenaires constituent les principes de la réussite économique.

L'esprit d'innovation, la durabilité, la responsabilité et la haute estime des collaborateurs et partenaires constituent les principes de la réussite économique.

SimonsVoss est une société du Groupe ALLEGION – un réseau actif à l'échelle mondiale dans le domaine de la sécurité. Allegion est représenté dans près de 130 pays ([www.allegion.com](http://www.allegion.com)).

### Fabriqué en Allemagne

Pour SimonsVoss, le « Made in Germany » est un engagement sérieux : tous les produits sont mis au point et fabriqués exclusivement en Allemagne.

© 2023, SimonsVoss Technologies GmbH, Unterföhring

Tous droits réservés. Les textes, photos et graphiques sont protégés par les droits d'auteur. Le contenu de ce document ne peut être copié, diffusé ou modifié. Sous réserve de modifications techniques.

SimonsVoss et MobileKey sont des marques enregistrées de la société SimonsVoss Technologies GmbH.

**SimonsVoss**  
technologies

Made in Germany

A BRAND OF

