



# LSM 3.4 SP2 SmartUserGuide

Manuale

29.10.2019

**Simons**  **Voss**  
technologies

## Sommario

<b>1</b>	<b>Funzioni base.....</b>	<b>4</b>
1.1	Creazione di un nuovo impianto di chiusura.....	4
1.2	Creazione di un nuovo gruppo transponder.....	4
1.3	Creazione di un nuovo transponder.....	4
1.4	Assegnazione successiva di un transponder ad un gruppo transponder.....	5
1.5	Creazione di un nuovo settore.....	5
1.6	Creazione di una nuova chiusura.....	5
1.7	Assegnazione di una chiusura ad un settore.....	5
1.8	Assegnazione/ritiro dell'autorizzazione.....	6
1.9	Metodi di lavoro conformi alla protezione dei dati secondo il RGPD.....	6
1.9.1	Esportazione dei dati personali.....	7
1.9.2	Cancellazione dei dati.....	9
1.10	Creazione del tastierino PinCode.....	11
1.10.1	Configurazione del tastierino PinCode.....	11
1.10.2	Creazione del tastierino PinCode nel piano di chiusura.....	12
1.10.3	Programmazione del tastierino PinCode.....	12
1.11	Ricerca all'interno della matrice.....	12
1.12	Esecuzione di azioni di gruppo.....	13
1.13	Programmazione del transponder.....	14
1.14	Programmazione della chiusura.....	14
1.15	Definizione programma fasce temporali (con giorni festivi e ferie aziendali).....	15
1.16	Reset dei componenti.....	17
1.17	Sostituzione della chiusura difettosa.....	17
1.18	Sostituzione di transponder difettosi, smarriti o rubati.....	18
1.19	Controllo e valutazione dello stato batteria delle chiusure.....	20
1.20	Livello di chiusura trasversale.....	21
1.20.1	Creazione di un livello di chiusura trasversale.....	21
1.20.2	Associazione delle chiusure.....	22
1.20.3	Associazione dei transponder.....	23
1.20.4	Autorizzazione dei transponder.....	24
1.21	Creazione dei transponder per i Vigili del fuoco.....	25
1.22	Configurazione di componenti DoorMonitoring.....	25
1.23	Programmazione tramite LSM Mobile.....	26
1.23.1	Con pocket PC/PDA.....	26
1.23.2	Con laptop, netbook o tablet.....	27
1.24	Reset della modalità magazzino nelle chiusure G1.....	28

1.25	Amministrazione degli elenchi accessi.....	28
1.26	Gestione utenti (BUSINESS).....	29
1.27	Gestione schede.....	30
1.27.1	Modifica della configurazione .....	30
1.27.2	Tabella.....	32
<b>2</b>	<b>Esecuzione di attività correnti basate su WaveNet in LSM Business.....</b>	<b>34</b>
2.1	Creazione di una rete radio WaveNet e integrazione di una chiusura.....	34
2.1.1	Preparazione del software LSM.....	34
2.1.2	Prima programmazione dei componenti di chiusura .....	34
2.1.3	Preparazione dell'hardware.....	35
2.1.4	Creazione del nodo di comunicazione .....	35
2.1.5	Configurazione della rete e importazione nell'LSM .....	36
2.2	Messa in funzione del cilindro di chiusura DoorMonitoring .....	38
2.2.1	Creazione del cilindro di chiusura DoorMonitoring.....	38
2.2.2	Integrazione del cilindro di chiusura DoorMonitoring nella rete .....	38
2.2.3	Trasferimento della configurazione WaveNet .....	39
2.2.4	Assegnazione del LockNode a una chiusura .....	39
2.2.5	Attivazione degli eventi di input della chiusura .....	39
2.3	Configurazione del RingCast .....	40
2.3.1	Preparare RouterNode per RingCast.....	40
2.3.2	Creazione del RingCast .....	42
2.3.3	Test di funzionamento RingCast.....	43
2.4	Configurazione dell'Event management (eventi) .....	46
2.4.1	Configurazione del server e-mail.....	47
2.4.2	Impostazione del servizio task.....	47
2.4.3	Inoltro degli eventi di input tramite il RouterNode2 .....	47
2.4.4	Inoltro degli eventi di input tramite il sistema SREL3-ADV .....	47
2.4.5	Creazione di una reazione .....	49
2.4.6	Creazione di un evento .....	50
2.5	Gestione della rete virtuale (VN) .....	50
2.5.1	Configurazione dell'impianto di chiusura .....	51
2.5.2	Configurazione del servizio VN.....	51
2.5.3	Creazione dei componenti e configurazione del software LSM.....	51
2.5.4	Esportazione delle modifiche alle autorizzazioni .....	52
2.5.5	Importazione delle modifiche alle autorizzazioni.....	53
2.5.6	Consigli sulla rete VN.....	53
2.6	Riconoscimento sabotaggi .....	54
2.7	DoorMonitoring (SmartHandle) - Eventi Maniglie.....	54
<b>3</b>	<b>Supporto e ulteriori informazioni .....</b>	<b>55</b>

## 1 Funzioni base

Il presente capitolo descrive i principali processi del software LSM. In questo software esistono vari modi per accedere alla funzione desiderata. Queste funzioni di base indicano generalmente il metodo più semplice e rapido.

La Smart User Guide di SimonsVoss descrive la procedura di creazione e gestione di un impianto di chiusura sulla base di un esempio di facile comprensione.

### 1.1 Creazione di un nuovo impianto di chiusura

- ✓ L'installazione è stata eseguita correttamente ed è stato effettuato un backup di sicurezza.
- 1. Nella barra menu selezionare *Modifica/Nuovo impianto di chiusura*.
- 2. Definire le opzioni desiderate per l'impianto di chiusura.
  - ↳ Per i livelli di chiusura trasversali, selezionare un colore da "Utilizza come livello di chiusura trasversale". *I livelli di chiusura trasversali fungono da livelli aggiuntivi agli impianti di chiusura standard già esistenti. Vedere Livello di chiusura trasversale.*
- 3. Fare clic sul pulsante "Applica".
- 4. Fare clic sul pulsante "Termina".

### 1.2 Creazione di un nuovo gruppo transponder

- ✓ L'impianto di chiusura è già stato creato.
- 1. Fare clic con il tasto destro sui gruppi transponder nell'"area gruppi" del software LSM.
- 2. Fare clic su "Nuovo".
- 3. Assegnare un nome al nuovo gruppo transponder e definire eventualmente altre impostazioni.
- 4. Fare clic sul pulsante "Applica".
- 5. Fare clic sul pulsante "Termina".

### 1.3 Creazione di un nuovo transponder

- ✓ L'impianto di chiusura è già stato creato.
- 1. Selezionare *Modifica/Nuovo transponder*.
- 2. Compilare tutti gli attributi ed effettuare eventuali altre impostazioni con il pulsante "Configurazione".
- 3. Fare clic sul pulsante "Salva & Avanti".
- 4. Fare clic sul pulsante "Termina".

#### 1.4 Assegnazione successiva di un transponder ad un gruppo transponder

- ✓ Il transponder è già stato creato, così come un gruppo transponder.
- 1. Aprire le impostazioni dell'impianto di chiusura, ad es. tramite la barra menu *Modifica/Proprietà: Impianto di chiusura*.
- 2. Selezionare la scheda "Transponder".
- 3. Selezionare dalla tabella il transponder a cui si desidera assegnare un gruppo transponder.
- 4. Dall'elenco a discesa, selezionare, in "Modifica assegnazione ai gruppi di transponder", il gruppo transponder desiderato a cui deve essere assegnato il transponder.
- 5. Fare clic sul pulsante "Esegui".
- 6. Fare clic sul pulsante "Applica".
- 7. Fare clic sul pulsante "Termina".

*Quando si crea un nuovo transponder, è possibile assegnarvi subito un gruppo transponder esistente.*

#### 1.5 Creazione di un nuovo settore

- ✓ L'impianto di chiusura è già stato creato.
- 1. Fare clic con il tasto destro sui settori nell'"area settori" del software LSM.
- 2. Fare clic su "Nuovo".
- 3. Assegnare un nome al nuovo settore e definire eventualmente altre impostazioni.
- 4. Fare clic sul pulsante "Applica".
- 5. Fare clic sul pulsante "Termina".

#### 1.6 Creazione di una nuova chiusura

- ✓ L'impianto di chiusura è già stato creato.
- 1. Selezionare *Modifica/Nuova chiusura*.
- 2. Compilare tutti gli attributi ed effettuare eventuali altre impostazioni con il pulsante "Configurazione".
- 3. Fare clic sul pulsante "Salva & Avanti".
- 4. Fare clic sul pulsante "Termina".

#### 1.7 Assegnazione di una chiusura ad un settore

- ✓ La chiusura è già stata creata, così come un settore.
- 1. Aprire le impostazioni dell'impianto di chiusura, ad es. tramite la barra menu *Modifica/Proprietà: Impianto di chiusura*.

2. Selezionare la scheda "Porte".
3. Selezionare dalla tabella la porta che si desidera assegnare ad un settore.
4. Dall'elenco a discesa, selezionare, in "Modifica assegnazione al settore", il settore desiderato a cui deve essere assegnata la porta.
5. Fare clic sul pulsante "Esegui".
6. Fare clic sul pulsante "Applica".
7. Fare clic sul pulsante "Termina".

*Quando si crea una nuova chiusura, è possibile assegnarvi subito un settore esistente.*

## 1.8 Assegnazione/ritiro dell'autorizzazione

È possibile assegnare e ritirare le autorizzazioni tramite la matrice. Nell'impostazione standard, è sufficiente fare clic su un campo di autorizzazione per modificare l'autorizzazione.

*Le autorizzazioni possono essere impostate o ritirate solo fra una chiusura e un transponder.*

Osservare le due viste:

### ■ Vista/Porte e persone

In questa vista si modificano le autorizzazioni per il transponder desiderato.

### ■ Vista/Settori e gruppi transponder

In questa vista si modificano le autorizzazioni per i gruppi completi.

## 1.9 Metodi di lavoro conformi alla protezione dei dati secondo il RGPD

Dal 25 maggio 2018, il regolamento generale sulla protezione dei dati è valido in tutta Europa. Esso disciplina il trattamento dei dati personali al fine di garantirne la protezione e al tempo stesso la libera circolazione nel mercato interno europeo. Innanzitutto, l'accesso al database attraverso l'interfaccia grafica utente è possibile solo con una password e i relativi diritti utente. Inoltre, all'interno del software LSM non vengono memorizzate "categorie particolari" di dati personali ai sensi dell'art. 9 del RGPD. I campi obbligatori utilizzati per una persona sono utilizzati esclusivamente per l'assegnazione univoca dei supporti di identificazione all'interno del piano di chiusura. I dati obbligatori sono richiesti dal sistema solo per la durata di utilizzo di un supporto di identificazione (es. appartenenza a una società). La durata di conservazione dei dati nelle registrazioni può essere modificata a piacere dal gestore dell'impianto di chiusura (vedere Opzioni/Registrazione).

### 1.9.1 Esportazione dei dati personali



#### NOTA

##### Testi in lingua straniera

Per i testi nei file esportati si utilizza la stessa lingua del software LSM.

##### Persone

È possibile esportare in formato .CSV i dati personali salvati delle persone all'interno dell'impianto di chiusura. Con questa operazione vengono generati tre file:

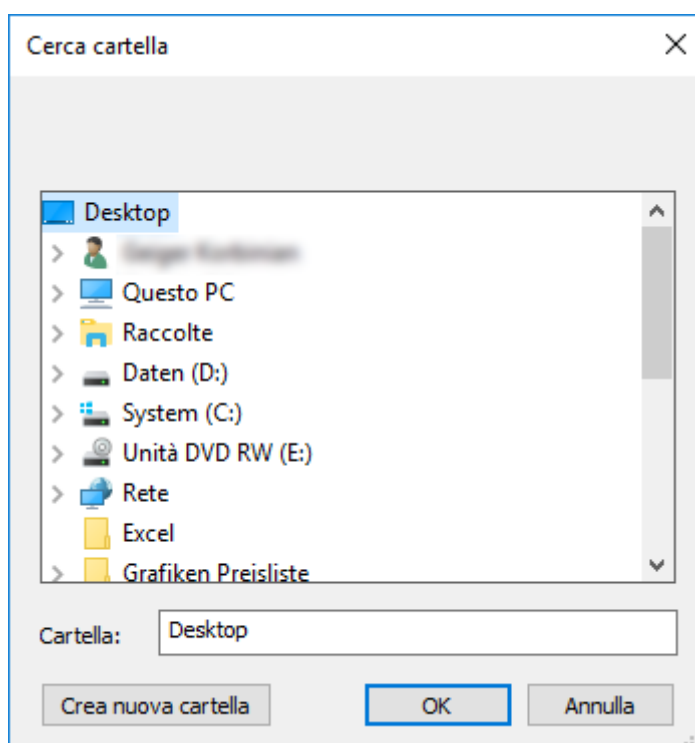
Persona	Il file contiene i dati personali con cui è possibile identificare la persona (ad es. cognome, indirizzo o foto).
PersonHistory	Questo file contiene la data di creazione e cancellazione del record di dati.
PersonLog	Questo file contiene l'andamento delle modifiche apportate al record di dati di questa persona (ad es. modifiche alle autorizzazioni o alle programmazioni).



#### NOTA

Le funzioni RGPD accedono a tale scopo alla gestione del personale. Pertanto vanno assegnate a un gruppo utenti autorizzato alla gestione del personale.

- ✓ LSM aperto.
- 1. Con | Opzioni | selezionare la voce **Funzioni del RGPD**.
  - ↳ Si apre la finestra "Funzioni del RGPD".
- 2. Nell'area "Persone" selezionare la voce della persona di cui vanno esportati i dati.
- 3. Fare clic nella scheda "Persone" sul pulsante **Esportare i dati personali**.
  - ↳ Si apre la finestra "Cerca cartella".



4. Definire la cartella in cui devono essere salvati i file.
  5. Fare clic sul pulsante **OK**.
- ↳ I dati vengono esportati.

### Utenti

È possibile esportare in formato .CSV i dati personali salvati degli utenti del software LSM. Con questa operazione vengono generati due file:

User	Questo file contiene i dati riguardanti l'utente (ad es. nome utente e gruppo utenti).
UserLog	Questo file contiene l'andamento delle modifiche apportate da questo utente (ad es. creazione di una nuova chiusura).



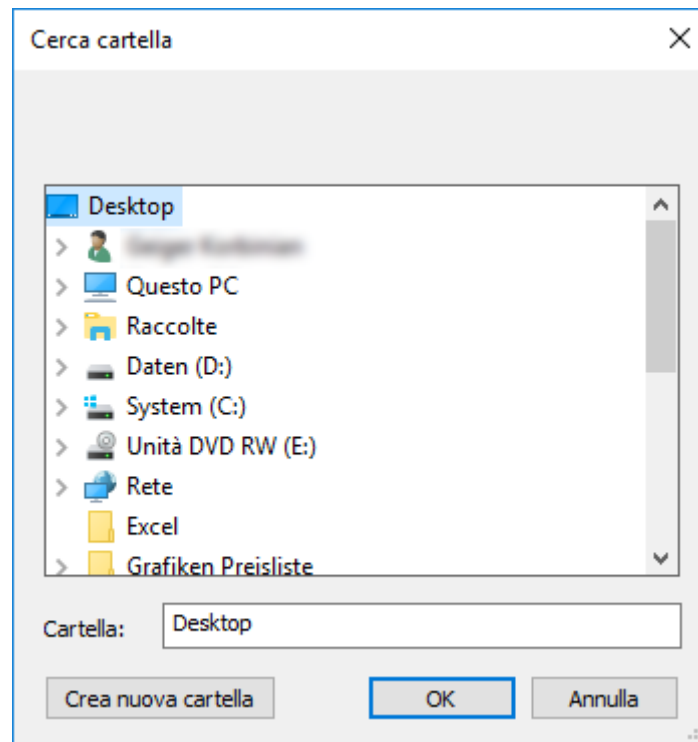
### NOTA

Le funzioni RGPD accedono a tale scopo alle funzioni amministrative. Pertanto vanno assegnate a un gruppo utenti autorizzato all'amministrazione.

- ✓ LSM aperto.
1. Con | Opzioni | selezionare la voce **Funzioni del RGPD**.
    - ↳ Si apre la finestra "Funzioni del RGPD".
  2. Nell'area "Utenti" selezionare la voce dell'utente di cui vanno esportati i dati.



3. Fare clic nella scheda "Utenti" sul pulsante **Esportare i dati personali**.  
↳ Si apre la finestra "Cerca cartella".



4. Definire la cartella in cui devono essere salvati i file.
5. Fare clic sul pulsante **OK**.  
↳ I dati vengono esportati.

### 1.9.2 Cancellazione dei dati

Con il modulo RGPD è possibile cancellare con comodità i dati personali.

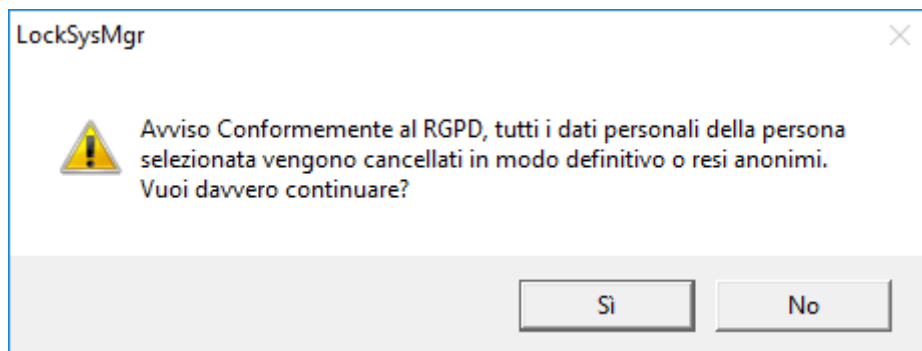
#### Persone



#### NOTA

Le funzioni RGPD accedono a tale scopo alla gestione del personale. Pertanto vanno assegnate a un gruppo utenti autorizzato alla gestione del personale.

- ✓ LSM aperto.
- 1. Con | Opzioni | selezionare la voce **Funzioni del RGPD**.  
↳ Si apre la finestra "Funzioni del RGPD".
- 2. Nell'area "Persone" selezionare la voce della persona di cui vanno cancellati i dati.
- 3. Fare clic nella scheda "Persone" sul pulsante **Cancellare definitivamente i dati personali**.  
↳ Si apre la finestra "LockSysMgr".



4. Fare clic sul pulsante **Si**.

↳ Dati personali della persona selezionata cancellati o resi anonimi.



### NOTA

#### Cancellazione dei dati residui dopo le precedenti cancellazioni

È possibile cancellare i dati delle persone anche con il pulsante **✕** nella scheda [Nome] dei supporti di identificazione assegnati. A differenza della cancellazione tramite modulo RGPD, in questo caso i protocolli non vengono cancellati e permangono all'interno del sistema. In questo modo solo una parte dei dati personali viene cancellata. Le persone così cancellate non vengono più visualizzate nel modulo RGPD. Per soddisfare i requisiti RGPD e rimuovere anche questi file, utilizzare il pulsante **Annulla** nell'area "Banca dati".

### Utenti



### NOTA

Le funzioni RGPD accedono a tale scopo alle funzioni amministrative. Pertanto vanno assegnate a un gruppo utenti autorizzato all'amministrazione.

✓ LSM aperto.

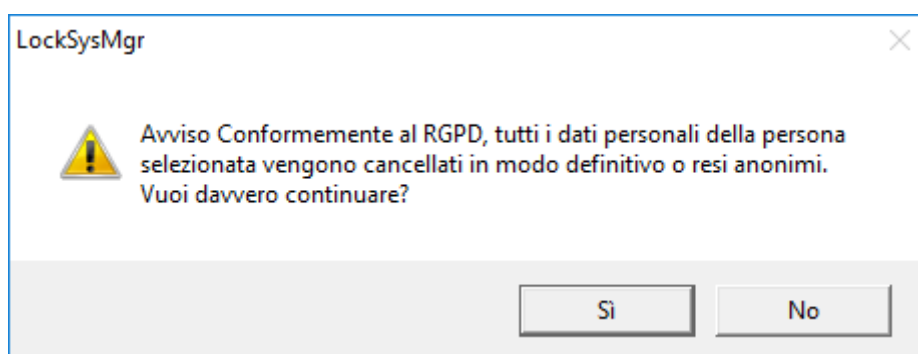
1. Con | Opzioni | selezionare la voce **Funzioni del RGPD**.

↳ Si apre la finestra "Funzioni del RGPD".

2. Nell'area "Utenti" selezionare la voce dell'utente di cui vanno cancellati i dati.

3. Fare clic nella scheda "Utenti" sul pulsante **Cancellare definitivamente i dati personali**.

↳ Si apre la finestra "LockSysMgr".



4. Fare clic sul pulsante **Si**.

↳ Dati personali dell'utente selezionato cancellati o resi anonimi.

## 1.10 Creazione del tastierino PinCode

Il tastierino PinCode non può essere utilizzato in impianti di chiusura esclusivi G2. I tre userpin si comportano come i transponder G1.

### 1.10.1 Configurazione del tastierino PinCode

#### Modifica del master pin

Questo passo va eseguito solo se non è stato ancora programmato un nuovo master pin.

1. Immissione 0 0 0 0
2. Immissione master pin precedente: 1 2 3 4 5 6 7 8
3. Immissione master pin nuovo:
  - ↳ Il nuovo master pin deve avere 8 cifre, non successive e non identiche fra di loro, e non può iniziare con 0!
4. Ripetizione dell'inserimento del nuovo master pin



#### NOTA

Il master pin è indispensabile per l'uso del tastierino PinCode e non può essere letto o resettato. Annotare il master pin e conservarlo in un luogo segreto sicuro. *Conoscendo il master pin, è possibile aprire o bloccare le chiusure del tastierino PinCode e definire nuovi user pin!*

#### Programmazione dello user pin

Nel tastierino PinCode è possibile assegnare fino a tre user pin. La lunghezza dello user pin può essere compresa fra 4 e 8 cifre, non continue o identiche.

*Ulteriore spiegazione: ogni user pin si comporta come un transponder. Pertanto, questi user pin devono essere programmati nei rispettivi transponder (interni) (1, 2 e 3).*

1. Immissione 0
2. Immissione master pin
3. Immissione user pin - ad es. 1 per user pin 1
4. Immissione della lunghezza dello user pin - ad es. 4 indica uno user pin a 4 cifre
5. Immissione user pin

Ripetere la procedura per programmare altri user pin nel tastierino PinCode.

### 1.10.2 Creazione del tastierino PinCode nel piano di chiusura

Creare un transponder a parte per ogni user pin!

1. Selezionare nella barra menu *Modifica / Nuovo transponder*.
2. In Tipo, selezionare dall'elenco dropdown la voce "G1 PinCode" e completare con le ulteriori informazioni richieste.
  - ↳ La voce potrà essere modificata dettagliatamente in seguito come per un transponder.
3. Selezionare *Salva & Avanti*
4. Selezionare *Termina*

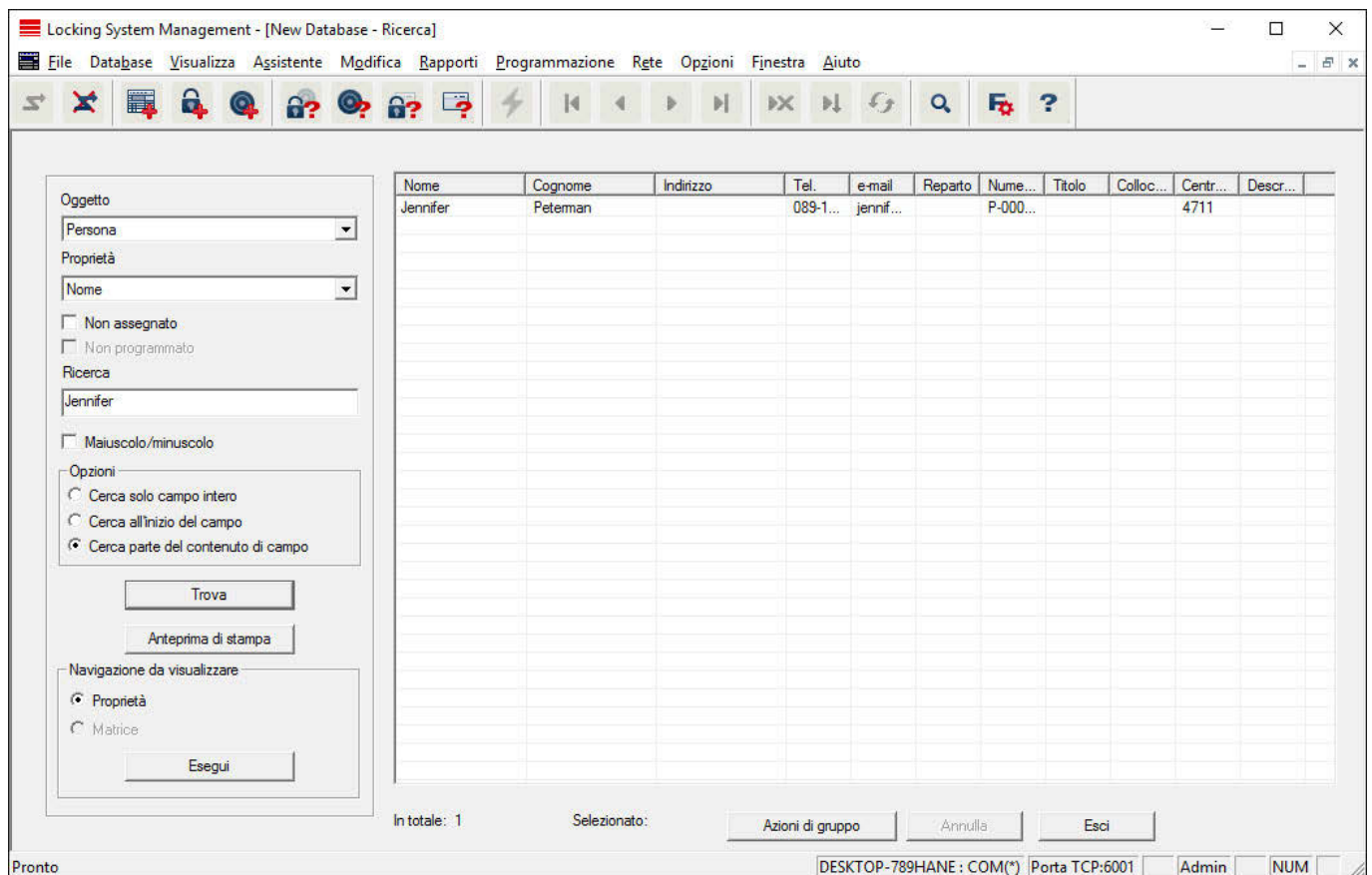
### 1.10.3 Programmazione del tastierino PinCode

1. LSM: Fare clic con il tasto destro su Transponder/PinCode nel piano di chiusura e selezionare *Programma*.
  - ↳ Si aprirà la finestra "Programma transponder".
2. Tastierino PinCode: Immissione 0 0 + master pin
3. LSM: Selezionare *Programma*.
  - ↳ Inizierà la procedura di programmazione.
4. Tastierino PinCode: User pin ad es. 1 per user pin 1 / Premere Transponder interno 1 non appena l'LSM visualizza l'avviso "Ora premere brevemente una volta il tasto del transponder...".
  - ↳ La procedura di programmazione è terminata.

Ripetere la procedura per programmare altri user pin nel piano di chiusura.

## 1.11 Ricerca all'interno della matrice

La ricerca consente di cercare diversi oggetti, quali ad es. una determinata porta o transponder, comodamente all'interno del database.



- ✓ Nell'impianto di chiusura sono già stati creati elementi che possono essere oggetto di ricerca.
1. Fare clic sul simbolo della lente d'ingrandimento nella barra degli strumenti.
  2. Selezionare un oggetto da cercare, ad es. persone, transponder, porte, chiusure ecc.
  3. Selezionare una proprietà dell'oggetto cercato, ad es. cognome o nome.
  4. Inserire un termine di ricerca nel campo di ricerca.
  5. Fare clic sul pulsante "Cerca" per avviare la ricerca.

### 1.12 Esecuzione di azioni di gruppo

Per vari componenti è possibile eseguire le impostazioni contemporaneamente su più componenti in un'unica operazione. Nell'esempio, si desiderano modificare le proprietà (*ad es. attivazione del controllo accessi*) di più chiusure G2 in un'unica volta.

1. Fare clic sul simbolo della lente d'ingrandimento nella barra degli strumenti.
2. Cercare, ad es., tutti gli oggetti di tipo "Chiusura".
  - ↳ Se si desiderano cercare tutte le chiusure, lasciare vuoto il campo "Cerca".
3. Selezionare più chiusure, ad es. tramite filtrando per tipo o per settore.

4. Fare clic sul pulsante "Azioni di gruppo".
  - ↳ Se al passo precedente sono state scelte solo chiusure G2, verranno selezionati subito i parametri giusti (*"Modifiche alla configurazione delle chiusure G2"* e *"Cilindri di chiusura G2 attivi/ibridi"*).
5. Fare clic sul pulsante "Esegui" per iniziare a modificare le chiusure selezionate.
6. Eseguire le modifiche desiderate.
7. Salvare le nuove impostazioni con il pulsante "Termina".



#### NOTA

Questa procedura consente di modificare molte impostazioni in modo semplice e rapido. Tenere presente che ogni componente modificato dovrà essere riprogrammato.

### 1.13 Programmazione del transponder

- ✓ Nell'impianto di chiusura è stato creato un transponder, che è visibile nella matrice.
1. Fare clic con il tasto destro sul transponder desiderato.
  2. Fare clic su Programma.
  3. Osservare le istruzioni del software LSM.

*Fare attenzione alla scelta del rispettivo dispositivo di programmazione.*

Con il pulsante "TID da disattivare" si richiama un elenco da cui è possibile scegliere un massimo di due ID transponder da bloccare (vedere *Sostituzione di transponder difettosi, smarriti o rubati [▶ 18]*).



#### NOTA

#### Riconoscimento automatico di schede G2

Le schede sono un supporto di identificazione di non facile distinzione. In presenza di più schede, la scheda da programmare va dapprima letta per poter selezionare nell'LSM la scheda giusta ai fini della programmazione. Quest'operazione non è necessaria se si appone il segno di spunta alla voce "Riconosci automaticamente scheda G2". Se la scheda presente è già nota all'LSM, il rispettivo record dati viene selezionato e programmato automaticamente.

### 1.14 Programmazione della chiusura

- ✓ Nell'impianto di chiusura è stata creata una chiusura, che è visibile nella matrice.
1. Fare clic con il pulsante destro sulla chiusura desiderata.

2. Fare clic su Programma.
3. Osservare le istruzioni del software LSM.

*Fare attenzione alla scelta del rispettivo dispositivo di programmazione.*



#### NOTA

Nei pressi del dispositivo di programmazione deve trovarsi solo una chiusura.

### 1.15 Definizione programma fasce temporali (con giorni festivi e ferie aziendali)




#### NOTA

##### Tempi diversi per chiusure G2

L'unità temporale interna delle chiusure G2 è tecnicamente vincolata a una tolleranza fino a  $\pm 15$  minuti all'anno.

Si raccomanda di adottare programmi a fasce temporali su tutti i gruppi di transponder e aree. Comunque è anche possibile associare programmi a fasce temporali direttamente a chiusure e transponder.

- ✓ Sono già state create chiusure (o aree) e transponder (o gruppi di transponder).
1. Cliccate nella barra dei menu su *Bearbeiten/Zeitzoneplan (Modifica/Programma fasce temporali)*.
    - ↳ Si apre un "programma fasce temporali vuoto". Qualora venga visualizzato un programma a fasce temporali esistente, cliccate sul pulsante "Neu" (Nuovo) per creare un nuovo programma a fasce temporali vuoto.
  2. Compilate i campi "Name" e "Beschreibung" ("Nome" e "Descrizione").
  3. Se necessario, selezionate un elenco di giorni festivi per il vostro paese. Se volete definire, a titolo esemplificativo, ferie aziendali una tantum, procedete così:
    - ↳ Cliccate sul campo "...-Feld" accanto alla selezione a tendina dei giorni festivi.
    - ↳ Cliccate sul pulsante "Neuer Feiertag" (Nuova festività).
    - ↳ Assegnate un nome, es. "Ferie aziendali 2017"
    - ↳ I giorni festivi di nuova definizione possono presentare una durata temporale. Per questo si deve attivare il campo "Urlaub" ("Ferie"). Successivamente si potrà inserire un arco temporale (Da - A).
    - ↳ Selezionate come considerare il nuovo giorno festivo, es. "Domenica".

- ↳ Cliccate sul pulsante “Übernehmen” (“Accetta”) e quindi sul pulsante “Beenden” (“Chiudi”).
  - ↳ Cliccate sul pulsante “Feiertagsverwaltung” (“Gestione festività”).
  - ↳ Aggiungete il nuovo giorno festivo da voi definito (*nella colonna sinistra*) con il pulsante “Hinzufügen” (“Aggiungi”) dell'elenco festività (*nella colonna destra*).
  - ↳ Cliccate sul pulsante “OK” e poi sul pulsante “Beenden” (“Chiudi”) per tornare al menu principale del programma a fasce temporali.
4. Selezionate un gruppo nella tabella ed editate il programma settimanale per questo gruppo.
    - ↳ Una barra blu indica una autorizzazione in quel momento.
    - ↳ Si può cliccare sui singoli campi oppure selezionarli tutti insieme.
    - ↳ Ogni click su un campo o una area inverte l'autorizzazione.
    - ↳ 
  5. Cliccate sul pulsante “Übernehmen” (“Accetta”).
  6. Cliccate sul pulsante “Beenden” (“Chiudi”).

Assegnate il programma a fasce temporali a una area:

1. Click destro sull'area cui assegnare il programma temporale.
2. Selezionate “Eigenschaften” (“Proprietà”).
3. Dall'elenco a discesa selezionate in “Zeitzone” (“Fascia temporale”) il programma temporale corrispondente.
4. Cliccate sul pulsante “Übernehmen” (“Accetta”).
5. Cliccate sul pulsante “Beenden” (“Chiudi”).

*Sarebbe anche possibile assegnare il programma a fasce temporali direttamente a una chiusura.*

Assegnate un gruppo di transponder alla fascia temporale:

1. Click destro sul gruppo di transponder cui assegnare la fascia temporale.
2. Selezionate “Eigenschaften” (“Proprietà”).
3. Dall'elenco a discesa selezionate in “Zeitzonegruppe” (“Fascia temporale”) la fascia temporale corrispondente.
4. Cliccate sul pulsante “Übernehmen” (“Accetta”).
5. Cliccate sul pulsante “Beenden” (“Chiudi”).

*Sarebbe anche possibile assegnare la fascia temporale direttamente a un transponder.*



## 1.16 Reset dei componenti

Tutti i componenti SimonsVoss possono essere resettati in qualunque momento. È possibile ripristinare anche i componenti SimonsVoss che non appartengono all'impianto di chiusura. In questo caso è necessaria la rispettiva password dell'impianto di chiusura.

Il reset dei componenti può essere necessario in varie situazioni. Il reset e la riprogrammazione di un componente può risultare utile soprattutto in caso di malfunzionamento.

1. Leggere il rispettivo componente con *Programmazione/Leggi componente*.
2. Fare clic sul pulsante "Reset" per avviare l'operazione di ripristino.
3. Osservare le istruzioni del software LSM.
  - ↳ Verrà eventualmente richiesto di inserire la password dell'impianto di chiusura o di selezionare il record dati da eliminare.

## 1.17 Sostituzione della chiusura difettosa

Può avvenire che le chiusure siano danneggiate o presentino un difetto.

Per sostituire una chiusura con una nuova, procedere come segue:

1. Rimuovere la chiusura difettosa dalla porta.
  - ↳ In alcuni casi può risultare difficile togliere un cilindro da una porta chiusa. Chiedere eventualmente consiglio al rivenditore specializzato che ha installato i prodotti SimonsVoss.
2. Procurarsi una chiusura di ricambio.
  - ↳ Facendo doppio clic sulla chiusura difettosa nel software LSM, nella scheda "Dotazione" verranno visualizzati tutti i dettagli sulla chiusura.
3. Eseguire nel software LSM un reset software della chiusura.
  - ↳ Per accedere alla funzione "Reset software", fare doppio clic sulla chiusura difettosa tramite la scheda "Configurazione/Dati".
  - ↳ Dopo il reset software, nella chiusura difettosa verrà segnalata la necessità di programmazione.
4. Eseguire la procedura di programmazione nella chiusura di ricambio.
5. Rimontare la chiusura di ricambio nella porta e testarne la funzionalità.



### NOTA

In caso di malfunzionamento, provare dapprima a resettare la chiusura tramite un'operazione di lettura! Dopo il reset, la chiusura può essere riprogrammata.



#### NOTA

Se possibile, resettare le chiusure difettose prima di restituirle al rivenditore o a SimonsVoss Technologies GmbH!

### 1.18 Sostituzione di transponder difettosi, smarriti o rubati

Può capitare che i transponder vadano smarriti, rimangano danneggiati o siano rubati. In tutti i casi, il vecchio transponder deve essere resettato nel piano di chiusura e deve essere creato un transponder sostitutivo.



#### NOTA

Per ragioni di sicurezza, in tutte le chiusure le autorizzazioni del transponder eliminato vanno rimosse. Ciò avviene tramite la riprogrammazione di tutte le chiusure.

Per sostituire un "vecchio" transponder con uno nuovo non programmato, procedere come segue:

1. Procurarsi un transponder di ricambio.
  - ↳ Facendo doppio clic sul transponder difettoso nel software LSM, nella scheda "Dotazione" verranno visualizzati tutti i dettagli sul transponder.
2. Fare clic con il pulsante destro sul transponder guasto, smarrito o rubato e selezionare "Perdita transponder".
  - ↳ Il transponder interessato verrà predisposto per il blocco.
  - ↳ Indicare il motivo di tale decisione. *Selezionando "Transponder smarrito/rubato" è possibile programmare direttamente un nuovo transponder con le stesse autorizzazioni. Nel protocollo G2, questo transponder blocca il transponder smarrito ad ogni azionamento in una chiusura autorizzata. Tuttavia resta necessario eseguire una riprogrammazione di tutte le chiusure interessate.*
3. Eseguire in tutti i componenti le operazioni di programmazione resesi necessarie.

#### Prevenzione della riprogrammazione delle chiusure

La creazione di un nuovo transponder sostitutivo determina necessità di programmazione in tutte le chiusure. Questi compiti speciali di programmazione possono tuttavia essere eseguiti anche direttamente con un nuovo transponder sostitutivo:

- ✓ Il transponder sostitutivo è stato correttamente programmato.

1. Azionare il nuovo transponder sostitutivo in ogni chiusura.

2. Programmare il nuovo transponder sostitutivo. Nella finestra "Programmazione transponder" selezionare la casella di controllo "Leggi notifiche di disattivazione / avvisi batteria".
3. Aggiornare la matrice. Ora la necessità di programmazione è scomparsa.

A partire dalla versione LSM 3.4 SP2 è possibile aggiungere ai transponder desiderati fino a due altri ID transponder da bloccare.

### **Programmazione diretta dei TID da bloccare**

Gli ID da bloccare sono salvati sul transponder durante la procedura di programmazione.

- ✓ Il transponder è fisicamente disponibile.
  - ✓ La finestra di programmazione del transponder è aperta.
1. Fare clic sul pulsante "TID da disattivare".
    - ↳ Si apre l'elenco.
  2. Apporre un massimo di due segni di spunta nella colonna TID per salvare sul transponder i TID da cancellare.
  3. Confermare l'inserimento con il pulsante "OK".
  4. Procedere con la programmazione.
- ↳ I TID contrassegnati saranno indicati come da cancellare sul transponder. Se il transponder si autentica in una chiusura interessata, i TID da cancellare saranno bloccati nella chiusura.

### **Memorizzazione dei TID da bloccare nelle proprietà**

Gli ID da bloccare vengono memorizzati sul transponder durante la successiva procedura di programmazione oppure alla successiva registrazione in un gateway.

- ✓ La finestra delle impostazioni del transponder è aperta.
1. Passare alla scheda "Configurazione".
  2. Fare clic sul pulsante "TID da disattivare".
    - ↳ Si apre l'elenco.
  3. Apporre un massimo di due segni di spunta nella colonna TID per salvare sul transponder i TID da cancellare.
  4. Confermare l'inserimento con il pulsante "OK".
- ↳ I TID contrassegnati vengono memorizzati sul transponder durante la successiva programmazione oppure alla successiva registrazione in un gateway.

## 1.19 Controllo e valutazione dello stato batteria delle chiusure

Esistono varie possibilità di interrogare lo stato batteria di una chiusura. Negli impianti di chiusura offline normali (e VN), gli stati batteria vanno prima trasmessi al software LSM per poterli valutare in vari modi.

### Trasmissione degli stati batteria al software LSM

#### Metodo veloce ed efficiente: "Raccogliere" gli stati batteria tramite i transponder

1. Prendere un transponder autorizzato in ogni chiusura. Azionare questo transponder due volte in ogni chiusura.
2. Riprogrammare il transponder. Nella finestra "Programmazione transponder" selezionare la casella di controllo "Leggi notifiche di disattivazione / avvisi batteria".

### Importazione degli stati batteria tramite lettura della chiusura

Leggere separatamente le chiusure desiderate tramite "Programma / Chiusura".

### Trasmissione degli stati batteria al software LSM via LSM Mobile

Gli stati batteria delle chiusure possono essere letti direttamente tramite LSM Mobile o trasmessi al software LSM. Osservare le istruzioni contenute nel manuale "LSM Mobile". Quest'ultime sono riportate nella homepage di SimonsVoss ([www.simons-voss.com](http://www.simons-voss.com)), nell'area assistenza, alla voce Documenti.

### Visualizzazione degli stati batteria

#### Procedura di base in tutte le versioni LSM:

- ✓ Gli avvisi batteria correnti delle rispettive chiusure sono stati trasmessi al software LSM.
1. Per visualizzare le proprietà di una chiusura fare doppio clic su di essa.
  2. Selezionare la scheda "Stato".
  3. Lo stato batteria è indicato nel campo "Stato ultima lettura".

#### Visualizzazione collettiva degli avvisi batteria in LSM BASIC Online e LSM BUSINESS:

*Generare un elenco che indichi tutte le chiusure con avvisi batteria.*

✓ Gli avvisi batteria correnti delle rispettive chiusure sono stati trasmessi al software LSM.

1. Nella barra menu selezionare "Report/Struttura edificio".
2. Selezionare la proprietà "Chiusure con avvisi batteria".
3. Fare clic sul pulsante "Visualizza".

### Visualizzazione automatica degli avvisi batteria in LSM BUSINESS

*Creare un avviso che indichi direttamente gli avvisi batteria.*

✓ Gli avvisi batteria correnti delle rispettive chiusure sono stati trasmessi al software LSM.

1. Nella barra menu selezionare "Gestione report/avvisi".
2. Con il pulsante "Nuovo" creare un nuovo avviso.
3. Creare l'avviso desiderato. Nel tipo, selezionare "Avviso batteria chiusura".
4. Non dimenticare di assegnare questo avviso alle rispettive chiusure! Non lasciare vuoto il campo "Chiusure".
5. Confermare il nuovo avviso con il pulsante "OK".
6. Chiudere la finestra di dialogo con il pulsante "Termina".

## 1.20 Livello di chiusura trasversale

I livelli di chiusura trasversali possono essere utilizzati solo con componenti attivi e non possono essere realizzati in caso di utilizzo della tecnologia schede passiva o di SmartTag!

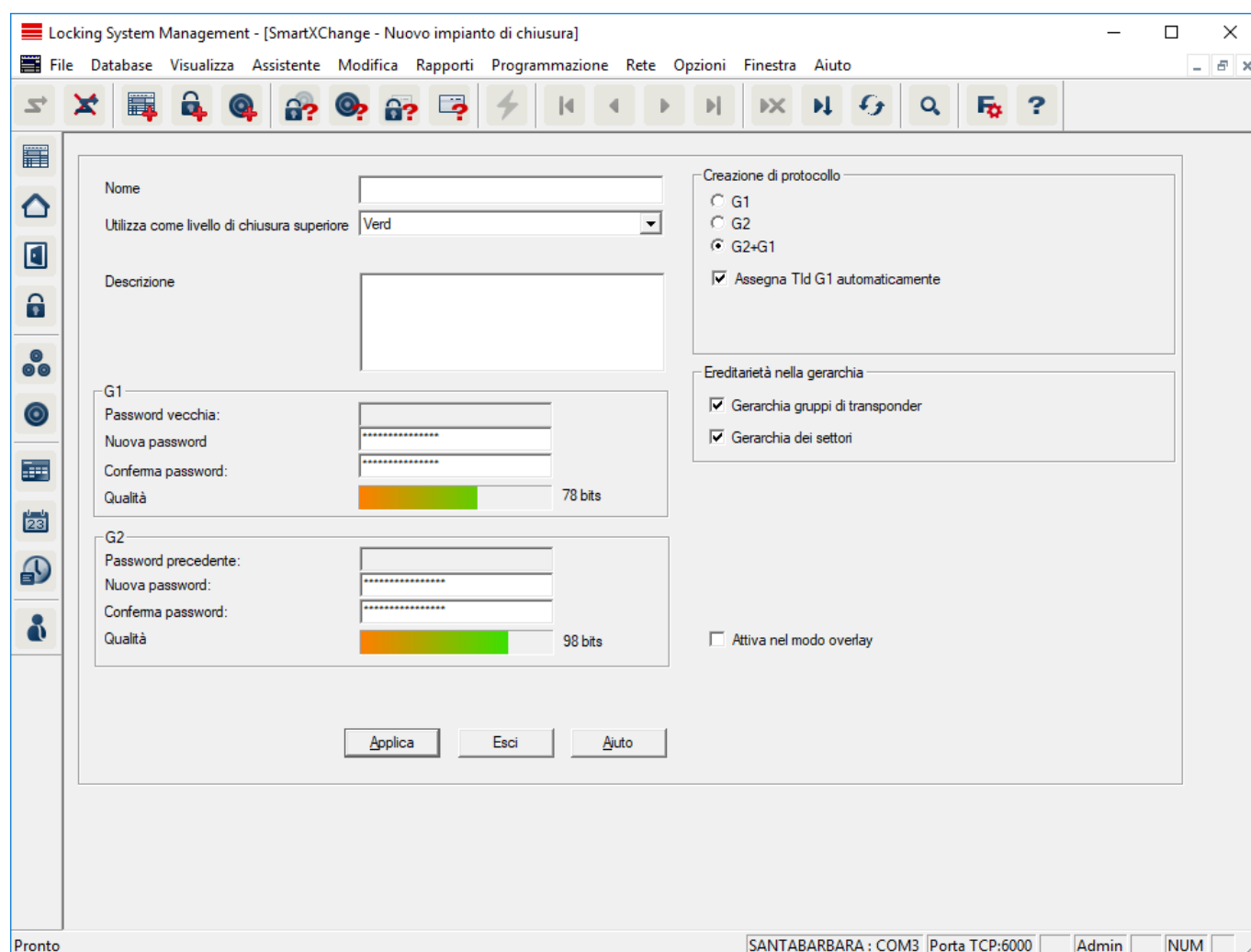
### 1.20.1 Creazione di un livello di chiusura trasversale

Tenere presente che

- i livelli di chiusura trasversali devono presentare la stessa generazione di protocollo.
- Il livello di chiusura rosso va utilizzato solo per i Vigili del fuoco o altri interventi di emergenza poiché ottimizzato appositamente per tale uso.

In linea di massima, il livello di chiusura trasversale viene creato come qualsiasi altro impianto di chiusura, ad es. tramite il pulsante "Nuovo impianto di chiusura" nella barra degli strumenti:

- In "Utilizza come livello di chiusura trasversale" scegliere il colore desiderato.

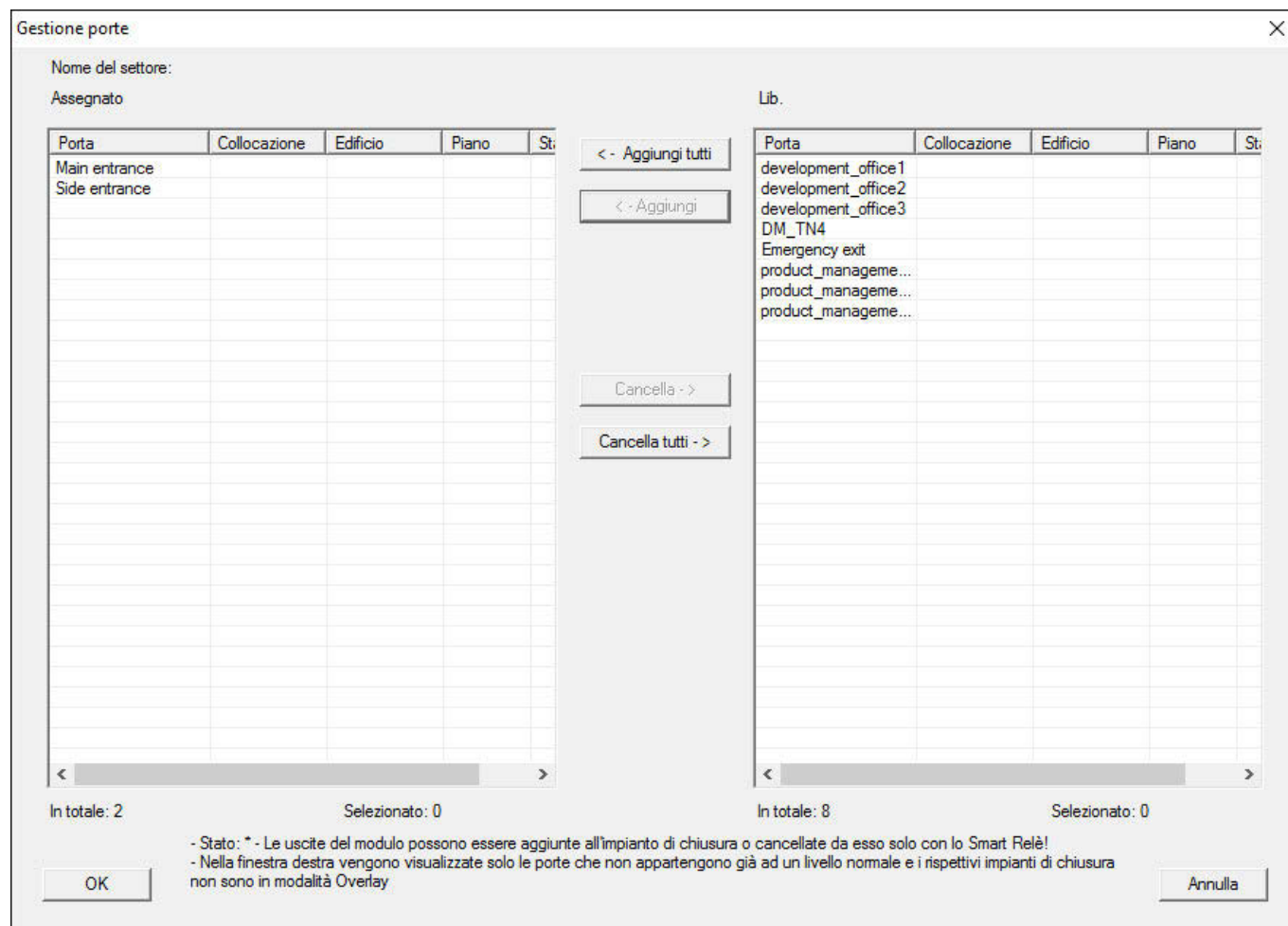


## 1.20.2 Associazione delle chiusure

✓ È già stato creato un livello di chiusura trasversale.

1. Nel livello di chiusura trasversale, fare clic con il tasto destro su un settore e selezionare "Proprietà".
2. Selezionare il pulsante "Gestione porta".

- Nella tabella destra vengono visualizzate tutte le chiusure di tutti gli impianti di chiusura del progetto. Selezionare le chiusure desiderate con il pulsante "Aggiungi".

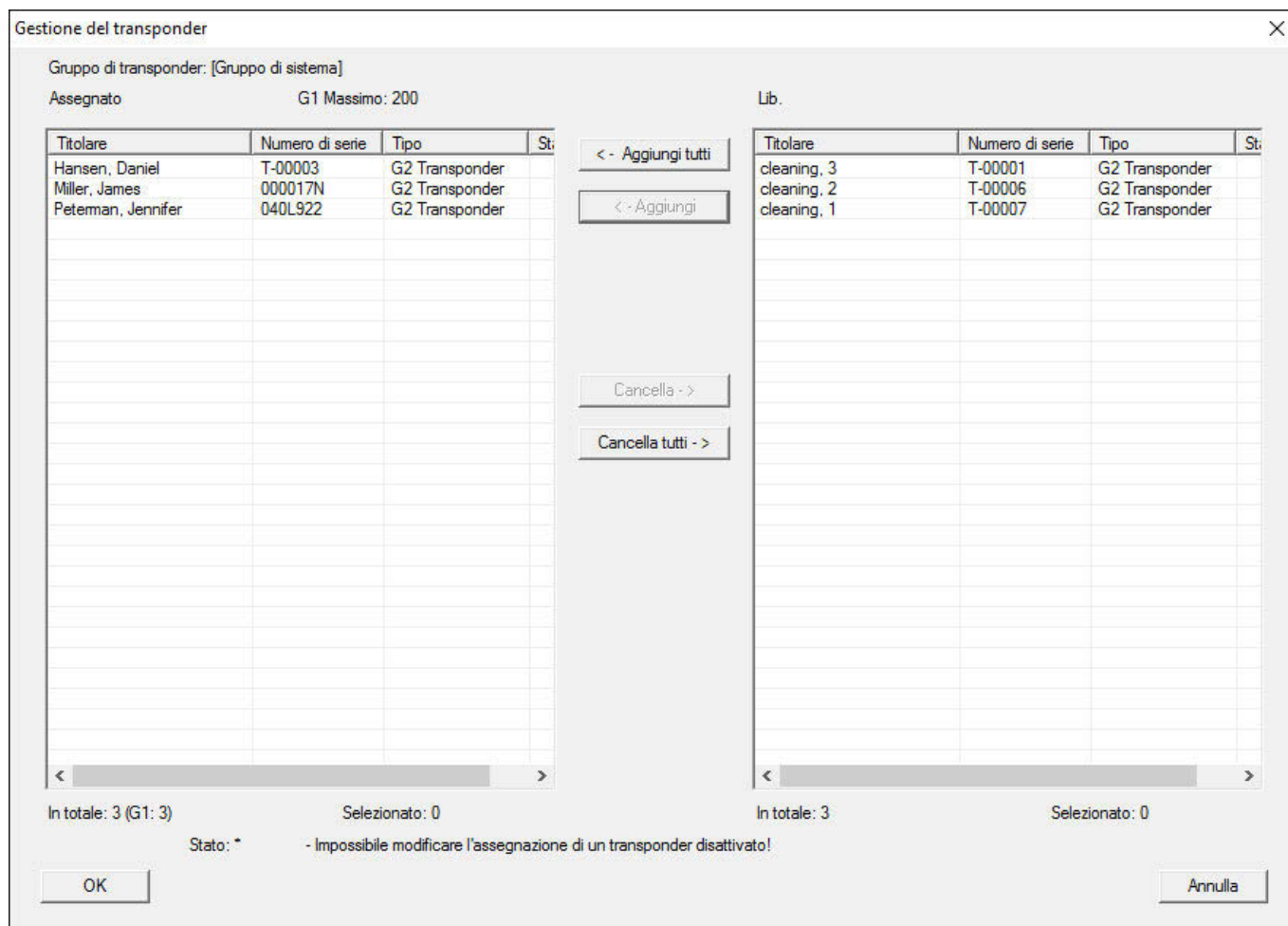


### 1.20.3 Associazione dei transponder

*L'associazione dei transponder deve avvenire solo nei livelli di chiusura non trasversali.*

- ✓ Sono già stati creati i transponder o i gruppi di transponder.
- Fare clic con il tasto destro su un gruppo di transponder e selezionare "Proprietà".
  - Selezionare il pulsante "Automatico" per l'assegnazione dei transponder.

3. Nella tabella destra vengono visualizzati tutti i transponder di tutti gli impianti di chiusura del progetto. Selezionare i transponder desiderati con il pulsante "Aggiungi".



#### 1.20.4 Autorizzazione dei transponder

Come in ogni livello di chiusura trasversale, anche nel "livello rosso" è possibile autorizzare determinati gruppi transponder in tutte le chiusure con pochi clic del mouse. Questa funzione è particolarmente utile per i transponder dei Vigili del fuoco.

- ✓ È già stato creato un livello di chiusura trasversale con colore "rosso".
1. Aprire l'impianto di chiusura trasversale rosso.
  2. Creare il gruppo di transponder che dovrà essere autorizzato in tutti i settori rilevanti per i Vigili del fuoco.
  3. Nelle proprietà del gruppo transponder, fare clic sul pulsante "Autorizzazioni" in Gestione.
  4. Con le caselle di controllo, selezionare tutti i settori/le chiusure desiderati per consentire al gruppo transponder l'accesso a tutte le porte.



## 1.21 Creazione dei transponder per i Vigili del fuoco

- ✓ È già stato creato almeno un impianto di chiusura.
- 1. Creare un nuovo livello di chiusura trasversale con colore "rosso", ad es. tramite *Modifica/Nuovo impianto di chiusura*.
- 2. Aggiungere un nuovo settore, ad es. "Tutte le chiusure" e assegnarvi tutte le chiusure desiderate tramite "Gestione porta".
- 3. Nel livello di chiusura trasversale, creare un nuovo gruppo transponder "Vigili del fuoco".
- 4. Nelle proprietà del gruppo transponder "Vigili del fuoco" fare clic sul pulsante "Autorizzazioni".
- 5. Attivare la casella di controllo "Tutti gli impianti" per autorizzare in via generale questo gruppo di transponder in ogni chiusura.
- 6. Salvare le impostazioni con il pulsante "OK".
- 7. Creare nel gruppo transponder un nuovo transponder (ad es. "Transponder Vigili del fuoco 1") e programmarlo. *Tutte le chiusure vanno inoltre riprogrammate. Osservare la nuova necessità di programmazione in-sorta.*

Il transponder per Vigili del fuoco "Transponder Vigili del fuoco 1" creato in questa fase è autorizzato in tutte le chiusure. Nel livello rosso, si possono aprire anche le chiusure disattivate e ciò lo distingue dal livello di chiusura "verde" e "blu".

## 1.22 Configurazione di componenti DoorMonitoring

La funzione DoorMonitoring è una caratteristica aggiuntiva che permette di visualizzare gli stati porta nel software LSM. Le SmartHandle e i cilindri di chiusura con funzione DoorMonitoring vengono configurati nel software LSM esattamente come i normali componenti di chiusura.

- Aggiunta di un nuovo cilindro di chiusura DoorMonitoring: Nell'elenco a discesa, scegliere come tipo di chiusura "Cilindro G2 DoorMonitoring".
- Aggiunta di una nuova SmartHandle DoorMonitoring: Nell'elenco a discesa, scegliere come tipo di chiusura "SmartHandle G2 DoorMonitoring".

### Scheda: Configurazione/Dati

Eseguire ulteriori impostazioni con il pulsante "Configurazione Monitoring".

### Scheda: Stato DoorMonitoring

In questa scheda viene visualizzato lo stato attuale della porta. Lo stato della porta viene mostrato in tempo reale.

*Affinché tale indicazione sia sempre aggiornata, si richiede una connessione diretta fra il software LSM e i componenti di chiusura (ad es. WaveNet). Per maggiori informazioni sulla configurazione di una rete radio WaveNet, consultare il manuale WaveNet.*

### 1.23 Programmazione tramite LSM Mobile

Con LSM Mobile è possibile eseguire le attività di programmazione direttamente in una chiusura con l'ausilio di dispositivi mobili. La programmazione avviene nel seguente modo:

1. L'elenco dei componenti che presentano necessità di programmazione viene esportata nel software LSM al dispositivo LSM Mobile. *Ciò avviene direttamente sul pocket PC o sotto forma di file per notebook, netbook o tablet PC.*
2. LSM Mobile viene lanciato sul dispositivo mobile. Con l'esportazione del software LSM è possibile iniziare la programmazione dei componenti.
3. Quindi è necessario comunicare al software LSM quali componenti sono stati programmati con LSM Mobile. A tale scopo viene eseguita un'importazione o una sincronizzazione da LSM Mobile al software LSM.

#### 1.23.1 Con pocket PC/PDA



#### NOTA

La programmazione tramite LSM Mobile con un pocket PC o PDA è possibile solo nel protocollo G1.

Per eseguire un'operazione di programmazione con LSM Mobile, procedere come segue:

- ✓ Nel software LSM sono presenti componenti con necessità di programmazione.
  - ✓ Nei componenti con necessità di programmazione è già stata eseguita una prima programmazione.
  - ✓ Sul dispositivo mobile è stato installato correttamente LSM Mobile. I numeri di versione sono identici.
  - ✓ Il dispositivo di programmazione SMARTCD.G2 è carico e connesso al PDA tramite Bluetooth.
  - ✓ I driver del pocket PC sono stati correttamente installati sul computer ed è presente una connessione.
1. Selezionare *Programmazione/LSM Mobile/Esportazione su LSM Mobile/LSM Mobile PDA.*
  2. Seguire le indicazioni del software LSM e trasferire le attività di programmazione sul PDA.

3. Avviare LSM Mobile sul PDA ed effettuare il login all'impianto di chiusura desiderato.
4. Con l'aiuto del dispositivo di programmazione, eseguire le operazioni di programmazione nei componenti desiderati.
5. Selezionare *Programmazione/LSM Mobile/Importazione da LSM Mobile/LSM Mobile PDA*.
6. Seguire le indicazioni del software LSM e sincronizzare le attività di programmazione.

*Le attività di programmazione sono state eseguite tramite il PDA. Con la sincronizzazione eseguita nell'ultima fase, i simboli a forma di lampo, che segnalano una necessità di programmazione, sono scomparsi dal software LSM.*

### 1.23.2 Con laptop, netbook o tablet

Per eseguire un'operazione di programmazione con LSM Mobile, procedere come segue:

- ✓ Nel software LSM sono presenti componenti con necessità di programmazione.
  - ✓ Nei componenti con necessità di programmazione è già stata eseguita una prima programmazione.
  - ✓ Sul dispositivo mobile è stato installato correttamente LSM Mobile. I numeri di versione sono identici.
  - ✓ I driver dei dispositivi di programmazione SMARTCD.G2 e SMARTCD.MP (se necessari) sono correttamente installati.
1. Selezionare *Programmazione/LSM Mobile/Esportazione su LSM Mobile/LSM Mobile PC*.
  2. Seguire le indicazioni del software LSM ed esportare le attività di programmazione in un file.
  3. Avviare LSM Mobile su un PC mobile e importare il file con le attività di programmazione in LSM Mobile.
  4. Osservare le istruzioni di LSM Mobile.
  5. Con l'aiuto del dispositivo di programmazione, eseguire le operazioni di programmazione nei componenti desiderati.
  6. Esportare lo stato delle attività di programmazione.
  7. Selezionare *Programmazione/LSM Mobile/Importazione da LSM Mobile/LSM Mobile PC*.
  8. Seguire le indicazioni del software LSM e importare il file da LSM Mobile.

*Le attività di programmazione sono state eseguite tramite il dispositivo esterno. Con l'importazione eseguita nell'ultima fase, i simboli a forma di lampo, che segnalano una necessità di programmazione, sono scomparsi dal software LSM.*

## 1.24 Reset della modalità magazzino nelle chiusure G1

Se non si osservano gli avvisi batteria nelle chiusure G1, quest'ultime passano in modalità magazzino. In questo modo si evita lo scaricamento completo delle batterie. La modalità magazzino può essere terminata riprogrammando la chiusura. Quindi la chiusura va aperta immediatamente con un transponder autorizzato e le batterie sostituite.

## 1.25 Amministrazione degli elenchi accessi

La lettura degli elenchi accessi e azionamenti può essere fortemente limitata a garanzia della privacy. In LSM BASIC è già creato, per impostazione predefinita, un utente "AdminAL" (Admin Access List). In LSM BUSINESS è possibile creare manualmente un relativo utente, vedere *Gestione utenti (BUSINESS)* [▶ 29].

*In questo capitolo è descritto il seguente scenario: La lettura degli elenchi accessi e azionamenti è consentita solo alla persona autorizzata (ad es. consiglio di amministrazione con login AdminAL). L'amministratore generale dell'impianto di chiusura non possiede tale facoltà.*

### Configurazione di AdminAL e lettura degli elenchi accessi

1. Eseguire il login al progetto con il nome utente "Admin" e la password.
2. Aprire la gestione gruppi utenti con "Modifica/Gruppo utenti".
3. Utilizzando le frecce, spostarsi sul gruppo utenti "Amministrazione elenchi accessi" (o in LSM BUSINESS ad un qualsiasi gruppo utente desiderato e creato in precedenza).
4. Assicurarsi che nel settore "Ruolo" i diritti "Amministratore elenchi accessi" e "Gestione elenchi accessi" siano attivati.
5. Fare clic sul campo "Modifica" sotto l'area "Ruolo".
6. Nei gruppi transponder e nei settori attivare gli impianti di chiusura desiderati. Se sono stati creati i settori o gruppi transponder, è necessario attivare separatamente tutti i settori o gruppi transponder desiderati!
7. Chiudere la maschera con il pulsante "OK".
8. Confermare le impostazioni eseguite con i pulsanti "Applica" e "Termina".
9. Eseguire il logout dal progetto in corso con "Database/Logout".

## Ritiro dei diritti di lettura degli elenchi accessi all'Admin



### NOTA

Il diritto "Amministrazione elenchi accessi" deve essere sempre assegnato a un utente/gruppo utenti e non può essere ritirato a entrambi!

1. Eseguire il login al progetto con il nome utente "AdminAL".
  - ↳ La password predefinita in LSM BASIC è "system3060".
  - ↳ Modificare prima possibile la password.
2. Aprire la gestione gruppi utenti con "Modifica/Gruppo utenti".
3. Con le frecce spostarsi al gruppo utenti "Admin".
4. Disattivare i ruoli "Amministrazione elenchi accessi" e "Gestione elenchi accessi".
5. Confermare le impostazioni eseguite con i pulsanti "Applica" e "Termina".
  - ↳ La configurazione è terminata. In futuro, gli elenchi accessi e gli elenchi azionamenti potranno essere letti o visualizzati solo tramite l'account utente "AdminAL".

## 1.26 Gestione utenti (BUSINESS)

### Assegnazione di un utente a un gruppo utenti

1. Fare clic su "Modifica/Gruppo utenti".
2. Con le frecce spostarsi su un gruppo utenti (o creare un nuovo gruppo utenti con il pulsante "Nuovo").
3. Fare clic sul pulsante "Modifica".
4. Selezionare l'utente desiderato e assegnarlo al gruppo utenti con il pulsante "Aggiungi".
5. Salvare le impostazioni eseguite con il pulsante "OK".
6. *Eventualmente correggere i ruoli.*
  - ↳ Fare clic sul campo "Modifica" sotto l'area "Ruolo".
  - ↳ Nei gruppi transponder e nei settori attivare gli impianti di chiusura desiderati. Se sono stati creati i settori o gruppi transponder, è necessario attivare separatamente tutti i settori o gruppi transponder desiderati!
  - ↳ Chiudere la maschera con il pulsante "OK".
7. Confermare le impostazioni eseguite con i pulsanti "Applica" e "Termina".

### Creazione di un nuovo utente

1. Fare clic su "Modifica/Utente".
2. Fare clic sul pulsante "Nuovo" per creare un nuovo utente.
3. Assegnare un nuovo nome utente e impostare una password.
4. Confermare le impostazioni eseguite con i pulsanti "Applica" e "Termina".

## 1.27 Gestione schede

Nel seguito vedrete i diversi tipi di schede e la suddivisione della memoria associata al sistema di chiusura SimonsVoss.

### AVVISO

#### Raccomandato: MIFARE DESFire

MIFARE DESFire utilizza una codifica supportata da micro-controller più sviluppata rispetto a MIFARE Classic, a norma AES-128, che soddisfa requisiti di sicurezza anche maggiori.

- SimonsVoss raccomanda di utilizzare transponder o prodotti MIFARE DESFire.



### NOTA

#### Maschere non uguali per prodotti AX

Se volete utilizzare prodotti MIFARE per prodotti AX SimonsVoss, allora le maschere utilizzate per la scrittura e la lettura devono essere identiche.


### 1.27.1 Modifica della configurazione

Avete due possibilità per l'impiego di schede.

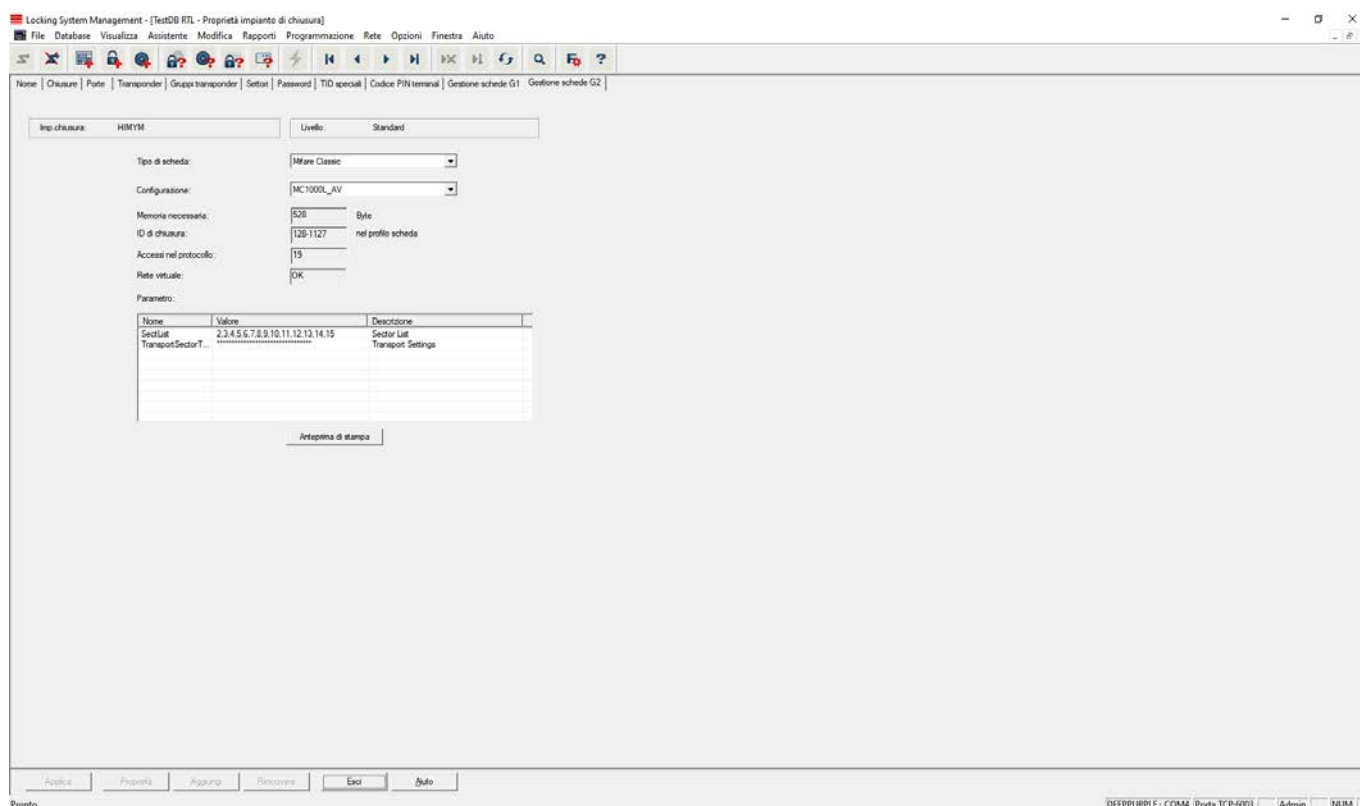
- Potete utilizzare schede già impiegate.
- Potete utilizzare schede nuove.

In entrambi i casi inserite il tipo di scheda, la configurazione ed eventualmente i settori da illustrare (vedi *Tabella* [▶ 32]).

#### Predisposizione della scheda

- ✓ LSM aperto.
1. Passate all'impianto di chiusura di cui volete modificare la gestione schede.
  2. Con un click sul pulsante  aprite le proprietà dell'impianto di chiusura.

3. Passate alla scheda di registro [Gestione schede G2].



4. Nel menu a discesa ▼ **Tipo di scheda** selezionate il vostro tipo di scheda.
5. Nel menu a discesa ▼ **Configurazione** selezionate la vostra configurazione.
6. Inserite eventualmente altri parametri, come settori (es.: 2,3,4,5,6,7,8,9,10,11,12,13,14,15).

Nome	Valore	Descrizione
SectList	2,3,4,5,6,7,8,9,10,11,12,13,14,15	Sector List
TransportSectorT...	.....	Transport Settings

7. Fare clic sul pulsante **Applica**.
- ↳ Avete modificato la configurazione

1.27.2 Tabella

	MIFARE DESFire	MIFARE DESFire Predefined	MIFARE DESFire Predefined DB1				
MDBasic	✓	✓	✗				
MD1200L	✓	✓	✗				
MD3800L	✓	✓	✗				
MD2500L_AV	✓	✓	✗				
MD4000L_AV	✓	✓	✗				
MD10000L_AV	✓	✓	✗				
MD32000L_AV	✓	✓	✗				
MD2400L_AV	✗	✗	✓				
MD3650L_AV	✗	✗	✓				

	MIFARE Classic	MIFARE Classic Pre- defined A	MIFARE Classic Pre- defined B	MIFARE Classic + DE- SFire	MIFARE Plus S/X		
MCBasic	✓	✓	✓	✗	✓		
MC1200L	✓	✓	✓	✗	✓		
MC3800L	✓	✓	✓	✗	✓		
MC1000L_AV	✗	✓	✓	✗	✓		
MC2400L_A V	✗	✓	✓	✗	✓		
MC8000L_A V	✗	✓	✓	✗	✓		
MBasic	✗	✗	✗	✓	✗		
M1200L	✗	✗	✗	✓	✗		
M3800L	✗	✗	✗	✓	✗		
M1000L_AV	✗	✗	✗	✓	✗		
M4000L_AV	✗	✗	✗	✓	✗		
M8000L_AV	✗	✗	✗	✓	✗		
M10000L_AV	✗	✗	✗	✓	✗		

	G1/G2	Lock-IDs	Anzahl der Schließu- ngen	Bege- hungsli- ste	Sektoren	Benötig- ter Spei- cherplatz	Virtuelles Netzwerk
MCBasic	G1	✗	✗	✗	2-15	48	✗
MC1200L	G2	128-1327	1200	✗	2-15	192	✗



	G1/G2	Lock-IDs	Anzahl der Schließu- ngen	Bege- hungslis- te	Sektoren	Benötig- ter Spei- cherplatz	Virtuelles Netzwerk
MC3800 L	G2	128-3927	3800	✗	2-15	528	✗
MC1000L _AV	G2	128-1127	1000	19	2-15	528	✓
MC2400L _AV	G2	128-2527	2400	70	2-15 + 31-39	900	✓
MC8000 L_AV	G2	128-8127	8000	125	2-15 + 31-39	2048	✓
MBasic	G1	✗	✗	✗	2-15	48	✗
M1200L	G2	128-1327	1200	✗	2-15	192	✗
M3800L	G2	128-3927	3800	✗	2-15	528	✗
M1000L_ AV	G2	128-1127	1000	16	2-15	528	✓
M4000L_ AV	G2	128-4127	4000	100	2-15 + 31-39	1600	✓
M8000L_ AV	G2	128-8127	8000	124	2-15 + 31-39	2048	✓
M10000L _AV	G2	128-10127	10000	225	2-15 + 31-39	3048	✓
MDBasic	G1	✗	✗	✗	2-15	48	✗
MD1200L	G2	128-1327	1200	✗	2-15	192	✗
MD3800 L	G2	128-3927	3800	✗	n.a. (DE- SFire)	528	✗
MD2500L _AV	G2	128-2627	2500	58	n.a. (DE- SFire)	1024	✓
MD4000 L_AV	G2	128-4127	4000	100	n.a. (DE- SFire)	1600	✓
MD1000L _AV	G2	128-10127	10000	225	n.a. (DE- SFire)	3048	✓
MD3200L _AV	G2	128-32127	32000	470	n.a. (DE- SFire)	7000	✓
MD2400L _AV	G2	128-2527	2400	34	n.a. (DE- SFire)	830	✓
MD3650L _AV	G2	128-3777	3650	2	n.a. (DE- SFire)	830	✓

## 2 Esecuzione di attività correnti basate su WaveNet in LSM Business

In questo esempio sono illustrati i principali passi per la realizzazione e l'amministrazione di una rete radio WaveNet tramite l'LSM Business. Gli esempi si riferiscono a installazioni specifiche e servono all'utente ad acquisire dimestichezza con i principi su cui si basa WaveNet.

### 2.1 Creazione di una rete radio WaveNet e integrazione di una chiusura

Questo primo esempio descrive come si crea una rete WaveNet da zero. Lo scopo è attivare una chiusura tramite un RouterNode2 attuale.

#### 2.1.1 Preparazione del software LSM

Tenere presente che per la connessione in rete dei componenti di chiusura SimonsVoss il software LSM deve essere correttamente installato e si deve disporre della licenza del modulo di rete!

1. Installare il CommNode Server e assicurarsi che il servizio si sia avviato.
2. Installare la versione aggiornata del WaveNet Manager. (Vedere Installazione del WaveNet Manager)
3. Aprire il software LSM e selezionare "Rete/WaveNet Manager".
  - ↳ Indicare la directory di installazione del WaveNet Manager e selezionare una directory per il file di output.
  - ↳ Avviare il WaveNet Manager con il pulsante "Start".
4. Assegnare una password per aumentare il grado di sicurezza della rete.
  - ↳ Il WaveNet Manager si avvia e le impostazioni vengono salvate per l'uso futuro. Chiudere il WaveNet Manager per eseguire altre impostazioni.

#### 2.1.2 Prima programmazione dei componenti di chiusura

Prima di poter integrare le chiusure nella rete, è necessario prima programmarle.

##### 2.1.2.1 Creazione di una nuova chiusura

- ✓ L'impianto di chiusura è già stato creato.
1. Selezionare *Modifica/Nuova chiusura*.
  2. Compilare tutti gli attributi ed effettuare eventuali altre impostazioni con il pulsante "Configurazione".
  3. Fare clic sul pulsante "Salva & Avanti".
  4. Fare clic sul pulsante "Termina".

### 2.1.2.2 Programmazione della chiusura

✓ Nell'impianto di chiusura è stata creata una chiusura, che è visibile nella matrice.

1. Fare clic con il pulsante destro sulla chiusura desiderata.
2. Fare clic su Programma.
3. Osservare le istruzioni del software LSM.

*Fare attenzione alla scelta del rispettivo dispositivo di programmazione.*



#### NOTA

Nei pressi del dispositivo di programmazione deve trovarsi solo una chiusura.

### 2.1.3 Preparazione dell'hardware

L'attuale RouterNode2 può essere messo in funzione in modo semplice e rapido. Chiudere il RouterNode2 come descritto nelle istruzioni brevi allegate. Il RouterNode2 è impostato in fabbrica in modo da prelevare l'indirizzo IP da un server DHCP. Con l'ausilio dell'OAM tool (*disponibile gratuitamente alla voce Infocenter / Downloads*) è possibile individuare tale indirizzo IP velocemente.



#### NOTA

Impostazioni standard:

Indirizzo IP: 192.168.100.100

Nome utente: SimonsVoss | Password: SimonsVoss

Se la chiusura non è ancora dotata di un LockNode (LN.I) di fabbrica, è necessario aggiungere il relativo accessorio.



#### NOTA

Annotare l'indirizzo IP del RouterNode2 e l'ID Chip della chiusura dopo avere preparato l'hardware in modo corretto.

### 2.1.4 Creazione del nodo di comunicazione

Il nodo di comunicazione forma l'interfaccia fra il CommNode Server e il software LSM. Per creare gli XML della configurazione, eseguire il software LSM come Amministratore.

1. Aprire il software LSM.

2. Selezionare "Rete/Nodo di comunicazione".
3. Compilare le informazioni "Nome", "Nome PC" e "Descrizione".
  - ↳ *Ad es. Nodo WaveNet\_123; Computer\_BS21; Nodo di comunicazione per la rete radio WaveNet 123*
4. Fare clic sul pulsante "File config".
5. Accertarsi che il percorso punti alla directory di installazione del CommNode Server e fare clic sul pulsante "OK".
6. Confermare il messaggio con "No" e confermare la selezione con "OK". *I tre XML di configurazione (appcfg, msgcfg e netcfg) devono trovarsi direttamente nella directory di installazione del CommNode Server.*
7. Salvare le impostazioni con il pulsante "Applica".
8. Confermare l'avviso con il pulsante "OK".
9. Chiudere la finestra di dialogo con il pulsante "Termina".

## 2.1.5 Configurazione della rete e importazione nell'LSM

### 2.1.5.1 Creazione della configurazione WaveNet

Una volta soddisfatte tutte le condizioni, si può iniziare la configurazione della rete:

- ✓ L'LSM è installato correttamente e si dispone di una licenza in un modulo di rete.
  - ✓ Il CommNode Server è stato installato e il servizio è avviato.
  - ✓ I file di configurazione del CommNode Server sono stati creati.
  - ✓ Il WaveNet Manager è installato nella versione aggiornata.
  - ✓ Nel software LSM è stato creato un nodo di comunicazione.
  - ✓ La prima programmazione della chiusura da collegare in rete è stata eseguita correttamente.
  - ✓ Il RouterNode2 è raggiungibile tramite la rete e se ne conosce l'indirizzo IP.
  - ✓ La chiusura programmata dispone di un LockNode montato, di cui si conosce l'ID Chip.
1. Avviare il WaveNet Manager con "Rete/WaveNet Manager" e il pulsante "Start".
  2. Inserire la password.
  3. Fare clic con il tasto destro su "WaveNet\_xx\_x".
  4. Inizializzare prima il RouterNode2, ad es. con l'opzione "Aggiungi: IP o router USB".
    - ↳ Seguire le indicazioni nella finestra di dialogo e integrare il RouterNode2 con il rispettivo indirizzo IP nella rete WaveNet.

5. Inizializzare il LockNode della chiusura facendo clic con il tasto destro sul RouterNode2 appena aggiunto e selezionare l'opzione "Cerca ID Chip".
  - ↳ Seguire le indicazioni nella finestra di dialogo e assegnare la chiusura o il LockNode corrispondente al RouterNode2 tramite l'ID Chip.
6. Fare clic in successione sui pulsanti "Salva", "Termina" e "Sì" per chiudere il WaveNet Manager.
7. Importare le nuove impostazioni e assegnarle al rispettivo nodo di comunicazione.

#### 2.1.5.2 Trasferimento della configurazione WaveNet

Le nuove impostazioni devono essere quindi trasferite al CommNode Server:

1. Selezionare "Rete/Nodo di comunicazione".
2. Selezionare il RouterNode2 dall'elenco dei collegamenti e fare clic sul pulsante "Trasferisci".
3. Salvare le impostazioni con il pulsante "Applica".
4. Chiudere la finestra di dialogo con il pulsante "Termina".

#### 2.1.5.3 Assegnazione del LockNode a una chiusura

Il LockNode inizializzato va collegato a una chiusura. Il modo più semplice per farlo (soprattutto in caso di più LockNode) è con un'operazione cumulativa:

1. Selezionare "Rete/Operazioni cumulative/Nodo WaveNet".
2. Selezionare tutti i LockNode (*WNode\_xxxx*) che non sono ancora assegnati. *I LockNode non ancora assegnati non presentano alcuna voce nella colonna "Porta"*.
3. Fare clic sul pulsante "Configurazione automatica".
  - ↳ L'autoconfigurazione inizia immediatamente.
4. Chiudere la finestra di dialogo con il pulsante "Termina".

#### 2.1.5.4 Verifica della configurazione WaveNet

Per testare velocemente il collegamento in rete, è possibile riprogrammare la chiusura in ogni momento tramite la rete con "Clic tasto destro/Programma". Una volta conclusa la programmazione, la rete funzionerà correttamente.

## 2.2 Messa in funzione del cilindro di chiusura DoorMonitoring

Questo esempio mostra le impostazioni da effettuare per la configurazione di un cilindro di chiusura DoorMonitoring. I requisiti sono indicati al capitolo "*Creazione di una rete radio WaveNet e integrazione di una chiusura [▶ 34]*".

### 2.2.1 Creazione del cilindro di chiusura DoorMonitoring

Il cilindro di chiusura DM va dapprima creato e programmato nell'LSM:

1. Selezionare il pulsante "Crea chiusura" per richiamare la finestra di dialogo per una nuova chiusura.
2. Selezionare il tipo di chiusura "Cilindro G2 DoorMonitoring" e completare con le informazioni desiderate.
3. Chiudere la finestra di dialogo per creare la chiusura nella matrice.
4. Facendovi doppio clic sopra, aprire le proprietà della chiusura e passare alla scheda "Configurazione/Dati".
5. Effettuare le impostazioni a piacere nell'area obbligatoria della chiusura.
6. Fare clic sul pulsante "Configurazione Monitoring" ed eseguire le seguenti impostazioni (minime):
  - ↳ Intervallo di scansione della vite di ritenuta: ad es. 5 secondi. In questo caso, lo stato porta viene interrogato ogni 5 secondi.
  - ↳ Numero di giri della serratura: ad es. 1 giro. Questa impostazione è importante per rilevare correttamente lo stato del chiavistello.
7. Salvare le impostazioni e ritornare alla matrice.
8. Eseguire la prima programmazione con un dispositivo di programmazione adatto.

### 2.2.2 Integrazione del cilindro di chiusura DoorMonitoring nella rete

Per integrare il cilindro di chiusura DM nella rete WaveNet, procedere come segue:

- ✓ Il WaveNet-Manager è già configurato.
  - ✓ Il router al quale va assegnata la nuova chiusura è già configurato e "online".
  - ✓ Sul cilindro di chiusura DM è montato correttamente un LockNode e se ne conosce l'ID Chip.
1. Avviare il WaveNet Manager.
  2. Inizializzare il LockNode della chiusura facendo clic con il tasto destro sul router e selezionare l'opzione "Cerca ID Chip".
    - ↳ Seguire le indicazioni nella finestra di dialogo e assegnare la chiusura o il LockNode corrispondente al RouterNode2 tramite l'ID Chip.

3. Fare clic con il tasto destro del mouse sul LockNode DM appena aggiunto.
4. Attivare la casella di controllo "Configurazione I/O" e fare clic sul pulsante "OK".
5. Attivare la casella di controllo "Inviare tutti gli eventi al router I/O" e fare clic sul pulsante "OK".
6. Fare clic in successione sui pulsanti "Salva", "Termina" e "Sì" per chiudere il WaveNet Manager.
7. Importare le nuove impostazioni e assegnarle al rispettivo nodo di comunicazione.

### 2.2.3 Trasferimento della configurazione WaveNet

Le nuove impostazioni devono essere quindi trasferite al CommNode Server:

1. Selezionare "Rete/Nodo di comunicazione".
2. Selezionare il RouterNode2 dall'elenco dei collegamenti e fare clic sul pulsante "Trasferisci".
3. Salvare le impostazioni con il pulsante "Applica".
4. Chiudere la finestra di dialogo con il pulsante "Termina".

### 2.2.4 Assegnazione del LockNode a una chiusura

Il LockNode inizializzato va collegato a una chiusura. Il modo più semplice per farlo (soprattutto in caso di più LockNode) è con un'operazione cumulativa:

1. Selezionare "Rete/Operazioni cumulative/Nodo WaveNet".
2. Selezionare tutti i LockNode (*WNNode\_xxxx*) che non sono ancora assegnati. *I LockNode non ancora assegnati non presentano alcuna voce nella colonna "Porta".*
3. Fare clic sul pulsante "Configurazione automatica".  
↳ L'autoconfigurazione inizia immediatamente.
4. Chiudere la finestra di dialogo con il pulsante "Termina".

### 2.2.5 Attivazione degli eventi di input della chiusura

Affinché gli stati porta siano visualizzati correttamente nel software LSM, è necessario eseguire ulteriori impostazioni:

1. Selezionare "Rete/Operazioni cumulative/Nodo WaveNet".
2. Selezionare il cilindro DoorMonitoring (*o qualunque cilindro di chiusura di cui si desidera inoltrare gli eventi*).
3. Fare clic sul pulsante "Attiva eventi di input".  
↳ La programmazione viene avviata immediatamente.

4. Fare clic sul pulsante "Termina" non appena sono state programmate tutte le chiusure.

### 2.3 Configurazione del RingCast

Di seguito è descritta la configurazione di un RingCast. Con il RingCast è possibile inoltrare parallelamente un evento di input di un RouterNode2 ad altri RouterNode2 nella stessa rete radio WaveNet. In questo esempio si desidera eseguire un'abilitazione di emergenza delle chiusure. Non appena un impianto di segnalazione antincendio aziona l'Input 1 di un RouterNode2, tutte le chiusure collegate devono aprirsi. Ogni chiusura rimane aperta finché non riceve l'esplicito comando di apertura remota.

*Con un RingCast è naturalmente possibile eseguire anche altri compiti, come ad es. la funzione elettroserratura, l'apertura remota e la funzione violenza incontrollata.*

Questo esempio mostra una rete WaveNet configurata con due RouterNode2. Ad ogni RouterNode2 è collegata una chiusura. Non appena l'Input 1 viene commutato brevemente in un RouterNode2, tutte le chiusure devono aprirsi immediatamente. In questo modo, le persone hanno accesso a tutti i locali per cercare riparo da fuoco e fumo.



#### NOTA

Se i RouterNode2 sono collegati in rete via Ethernet, RingCast è supportato solo nei modelli a partire dal 2017 circa. Se un RouterNode2 ha fallito il tentativo di collegamento Ethernet a un altro RouterNode2, tenterà di instaurare un nuovo collegamento via radio. La portata di comunicazione radio arriva fino a 30 m (dato non garantito, dipende dall'ambiente).

#### 2.3.1 Preparare RouterNode per RingCast



#### NOTA

##### Disponibilità di RingCast per RouterNode in funzione del firmware

Il supporto RingCast dipende dal firmware (vedere ).

- Se necessario, aggiornare il firmware (vedere ).

Preparare i RouterNode per il RingCast:

- ✓ Nella rete radio Wavenet sono configurati e "online" almeno due diversi RouterNode Ringcast compatibili (vedere ).
- ✓ Ad ogni RouterNode del RingCast pianificato è assegnata almeno una chiusura. Entrambe le chiusure sono "online".

1. Aprire il WaveNet Manager.



2. Fare clic con il tasto destro del mouse sul primo RouterNode 2.
  - ↳ Si apre la finestra "Administration".



3. Selezionare l'opzione  I/O configuration.
4. Fare clic sul tasto **OK**.
  - ↳ Si chiude la finestra "Administration".
  - ↳ Si apre la finestra "I/O configuration".
5. Opzionale: Selezionare, ad esempio, per **Output 1** "Input receipt static" per poter comandare un dispositivo di segnalazione durante la disattivazione.
6. Selezionare nel menu a discesa **Input** dell'ingresso desiderato la voce della rispettiva reazione (vedere).
7. Selezionare nel menu a discesa **Delay [s]** la voce "RingCast".
8. Fare clic sul tasto **Select LN**.
9. Accertarsi che tutti i LockNode desiderati siano selezionati (*alla prima impostazione della configurazione I/O del router vengono inclusi tutti i LockNode*).
10. Selezionare nel menu a discesa **Protocol generation** Generazione protocollo.



## NOTA

### Generazione protocollo in LSM

La generazione protocollo viene visualizzata in LSM nelle proprietà dell'impianto di chiusura nella scheda di registro [Nome] nell'area "Creazione di protocollo".

11. Inserire la password dell'impianto di chiusura.
12. Fare clic sul pulsante **OK**.
13. Eseguire le stesse impostazioni anche nell'altro RouterNode 2.

### 2.3.2 Creazione del RingCast



#### NOTA

#### Ricalcolo del RingCast

Se si sostituisce o elimina un RouterNode nel RingCast oppure se si modifica la sua configurazione IO rilevante per il RingCast, il RingCast viene ricalcolato automaticamente dopo aver salvato le modifiche e confermato la richiesta.

- ✓ WaveNet Manager aperto (vedere Avvio del WaveNet Manager).
  - ✓ RouterNode e LockNode collegati all'alimentazione elettrica.
  - ✓ RouterNode e LockNode importati nella topologia WaveNet (vedere ).
  - ✓ RouterNode per RingCast preparati (vedere *Preparare RouterNode per RingCast* [▶ 40]).
1. Fare clic con il tasto destro del mouse sulla voce WaveNet in cui si desidera creare un RingCast.
    - ↳ Si apre la finestra "Administration".



2. Selezionare l'opzione  RingCast .
3. Fare clic sul tasto **OK** .
  - ↳ Si chiude la finestra "Administration".
  - ↳ Si apre la finestra "Edit radio domains".



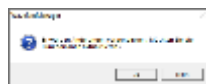
4. Selezionare nel menu a discesa **Select domain** un ingresso per il quale in **Delay [s]** è stata selezionata la voce "RingCast".



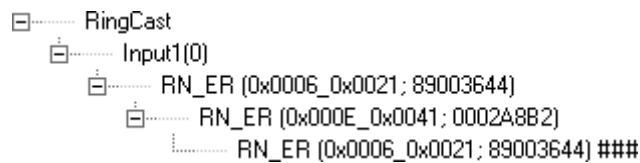
- ↳ Nel campo "selected routers" vengono visualizzati tutti i RouterNode2, per cui su questo ingresso in **Delay [s]** è stata selezionata la voce "RingCast" (=domini).



5. Fare clic sul tasto **Save**.
6. Fare clic sul tasto **Esci**.
  - ↳ Si chiude la finestra "Edit radio domains".
  - ↳ Si apre la finestra "WaveNetManager".



7. Fare clic sul tasto **Si**.
  - ↳ Si chiude la finestra "WaveNetManager".
  - ↳ Le modifiche vengono aggiornate.
- ↳ Il RingCast viene creato ed è visibile nel WaveNet Manager dopo poco.



Le impostazioni effettuate sono già state scritte nei RouterNode2. Salvare le nuove impostazioni e terminare il WaveNet Manager.

### 2.3.3 Test di funzionamento RingCast

Le impostazioni effettuate sono immediatamente operative. Il RingCast non ha alcuna funzione di autotest.



#### AVVISO

**Danneggiamento o avaria delle funzioni di protezione in seguito a variazione delle condizioni**

L'attivazione delle funzioni di protezione in RingCast si basa su connessioni wireless e connessioni Ethernet. Le connessioni wireless, in particolare, possono essere influenzate dalle mutevoli condizioni ambientali (vedere ).

Ciò influenza anche l'attivazione delle funzioni di protezione nel RingCast e può mettere a rischio la sicurezza di persone e cose che, ad esempio, sono ulteriormente protette dalle funzioni di protezione nel RingCast.

1. Verificare le funzioni di protezione almeno una volta al mese (vedere *Test di funzionamento RingCast* [▶ 43]).
2. Se necessario, osservare anche altre direttive o ordinanze rilevanti per il vostro impianto di chiusura.



### AVVISO

#### Modifica della sequenza delle funzioni di emergenza a causa di malfunzionamenti

SimonsVoss e "Made in Germany" sono sinonimo di massima sicurezza e affidabilità. In singoli casi, tuttavia, non si possono escludere malfunzionamenti dei vostri apparecchi, che potrebbero mettere a repentaglio la sicurezza di persone e cose che sono ulteriormente protette dalle funzioni di protezione del RingCast.

1. Testare i dispositivi almeno una volta al mese (vedere ).
2. Verificare le funzioni di protezione almeno una volta al mese (vedere *Test di funzionamento RingCast* [▶ 43]).

Attivare l'ingresso corrispondente sull'attuatore e controllare:

- se le chiusure reagiscono come desiderato (vedere anche ).
- se l'uscita eventualmente impostata sul RouterNode visualizza la conferma eseguendo la commutazione come desiderato (vedere anche ).



### NOTA

#### Apertura di emergenza permanente

Un incendio può danneggiare il cavo di ingresso o altri componenti. Ciò provocherebbe la richiusura delle serrature, nonostante l'incendio. Le persone potrebbero rimanere intrappolate nell'area dell'incendio e verrebbe impedito l'accesso ai soccorritori.

Pertanto, tutte le chiusure rimangono nello stato di apertura di emergenza (e quindi transitabile) che permane fino a quando un esplicito comando di apertura remota le richiude.

## Test con router di uscita centrale



### NOTA

#### Router di uscita centrale nel RingCast con RouterNode R/CR

Il router di uscita centrale riceve la conferma di ingresso dei RouterNode partecipanti esclusivamente tramite una connessione Ethernet. Il router di uscita centrale ignora quindi lo stato dei RouterNode che non sono RouterNode Ethernet (.ER). Se si utilizza il router di uscita centrale e il RingCast contiene anche RouterNode senza interfaccia Ethernet, la conferma in ingresso del router di uscita centrale significa solo che tutte le chiusure assegnate ad un RouterNode Ethernet hanno ricevuto il comando.

- Controllare manualmente lo stato di altri RouterNode (R/CR) indipendentemente dal router di uscita centrale (vedere e o ).

L'utilizzo di un router di uscita centrale (vedere ) semplifica notevolmente la verifica del RingCast. Attivare l'ingresso corrispondente sull'attuatore e verificare se il router di uscita centrale emette un riconoscimento degli ingressi o commuta l'uscita corrispondente. Se l'uscita commuta, tutte le chiusure hanno ricevuto il comando. Se l'uscita non commuta, controllare quali RouterNode hanno causato problemi:

- ✓ WaveNet Manager aperto (vedere Avvio del WaveNet Manager).
1. Fare clic con il tasto destro del mouse sulla voce del RingCast che si desidera testare.
  2. Selezionare nel menu a discesa ▼ **Select domain** l'ingresso di cui si desidera testare il RingCast.
    - ↳ Si apre la finestra "Edit radio domains".



3. Fare clic sul tasto **Status**.

- ↳ Il RingCast viene testato.



Il RingCast è stato in grado di interloquire con tutte le chiusure.

Non è stato possibile completare il RingCast. Possibili cause (vedere anche ):

- Uno o più RouterNode non hanno ricevuto il pacchetto dati.
  - Uno o più RouterNode non hanno raggiunto uno o più LockNode.
  - La connessione Ethernet ad uno o più RouterNode viene interrotta. I RouterNode potrebbero aver ricevuto il pacchetto di dati in modalità wireless, ma non possono più restituire le loro conferme di ingresso a causa della connessione Ethernet interrotta.
1. Verificare l'accessibilità dei RouterNode menzionati (vedere e ).
  2. Verificare l'accessibilità dei LockNode (vedere e ).
  3. Controllare le ultime reazioni dei LockNode (vedere ).

---

## 2.4 Configurazione dell'Event management (eventi)

Il collegamento in rete delle chiusure tramite RouterNode2 offre molteplici vantaggi. Uno dei più importanti è la comunicazione continua fra il RouterNode2 e la chiusura.

In questo esempio, il software LSM invia un'e-mail predefinita non appena un transponder viene azionato durante la notte in una determinata chiusura.

A tale scopo è necessario che siano soddisfatte dapprima le seguenti condizioni:

- È configurata una rete radio WaveNet come nell'esempio *Creazione di una rete radio WaveNet e integrazione di una chiusura* [▶ 34].
- È stato attivato l'inoltro degli eventi della chiusura come descritto al passo *Attivazione degli eventi di input della chiusura* [▶ 39].

#### 2.4.1 Configurazione del server e-mail

Nel software LSM è implementato un client e-mail rudimentale per l'invio di e-mail. Per l'invio delle e-mail è necessario un proprio account e-mail compatibile con il formato SMTP.

1. Selezionare "Rete/Notifiche e-mail"
2. Fare clic sul pulsante "E-mail".
3. Indicare tutte le impostazioni SMTP del provider e-mail.
4. Fare clic sul pulsante "OK".
5. Fare clic sul pulsante "OK".

#### 2.4.2 Impostazione del servizio task

1. Selezionare "Rete/Task manager".
2. Alla voce "Servizio task" selezionare il nodo di comunicazione.
3. Fare clic sul pulsante "Applica".
4. Fare clic sul pulsante "Termina".

#### 2.4.3 Inoltro degli eventi di input tramite il RouterNode2

Se è necessario inoltrare gli eventi (*ad es. registrazione di un transponder in una chiusura collegata in rete*) tramite il RouterNode2 al CommNode Server, tale funzione deve essere attivata nella configurazione I/O del router.

1. Aprire il WaveNet Manager.
2. Fare clic con il tasto destro del mouse sul router e selezionare "Configurazione I/O".
3. Nell'elenco a discesa, specificare l'opzione "tutti gli eventi LN" in "Trasmettere eventi al sistema di gestione".
4. Confermare con il pulsante "OK" e chiudere il WaveNet Manager.

#### 2.4.4 Inoltro degli eventi di input tramite il sistema SREL3-ADV

Il sistema SREL3-ADV consente di inoltrare gli ingressi input all'LSM.

##### 2.4.4.1 Valutazione degli input del controller

Gli ingressi digitali sul controller del sistema SREL3 ADV possono essere trasferiti all'LSM e qui avviare azioni.

##### Creazione evento

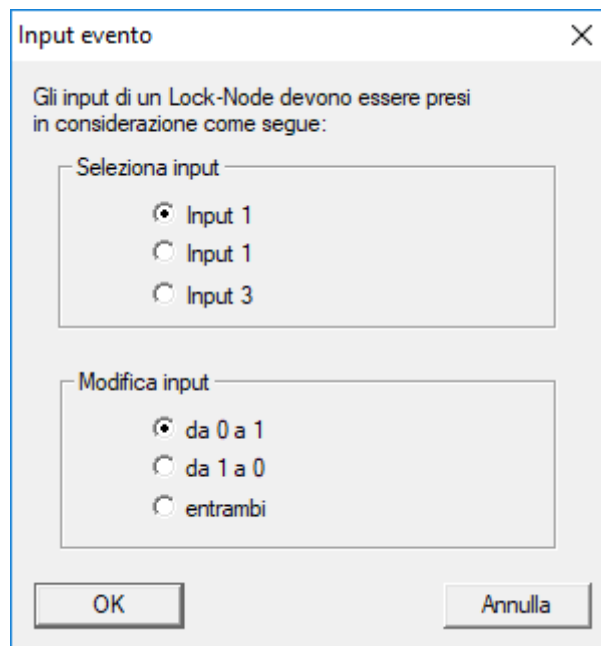
Se si desidera valutare un input attraverso l'LSM o SmartSurveil (vedi SmartSurveil), è necessario prima creare l'input corrispondente nell'LSM come evento. Solo allora le modifiche all'input sono depositate anche nella banca dati LSM.

- ✓ LSM aperto.
  - ✓ Sistema SREL3 ADV creato nella matrice.
1. Tramite | Rete | selezionare la voce **Gestione eventi**.
    - ↳ Si apre la finestra "Manager eventi rete".
  2. Fare clic sul pulsante **Nuovo**.
    - ↳ Si apre la finestra "Nuovo evento".

3. Inserire un nome per l'evento.
4. Opzionalmente, inserire una descrizione per l'evento.
5. Opzionalmente, inserire un messaggio.
6. Aprire il menù a tendina ▼ **Tipo**.
7. Selezionare la voce "Input evento".

8. Fare clic sul pulsante **Configura evento**.
  - ↳ Si apre la finestra "Input evento".





9. Nel settore "Seleziona input" selezionare gli input desiderati.
  10. Nel settore "Modifica input" selezionare la modifica dello stato che deve avviare l'evento.
  11. Fare clic sul pulsante **OK**.
  12. Fare clic sul pulsante **Seleziona**, per associare l'evento alla chiusura.
    - ↳ Si apre la finestra "Gestione".
  13. Contrassegnare una o più chiusure.
  14. Fare clic sul pulsante **Aggiungi**.
  15. Fare clic sul pulsante **OK**.
    - ↳ La finestra si chiude.
    - ↳ La chiusura è associata all'evento.
  16. Se si vuole definire un'azione, è possibile associare un'azione con il pulsante **Nuovo** o **Aggiungi**.
  17. Fare clic sul pulsante **OK**.
    - ↳ La finestra si chiude.
    - ↳ Evento visualizzato nel settore "Eventi".
  18. Fare clic sul pulsante **Esci**.
    - ↳ La finestra si chiude.
- ↳ L'imput è creato come evento e fa scattare un'azione a seconda dell'impostazione.

#### 2.4.5 Creazione di una reazione

Creare dapprima una reazione. Questa potrà essere successivamente scelta quando si verifica un determinato scenario.

1. Selezionare "Rete/Manager eventi".
2. Fare clic nell'area di destra in "Reazioni" sul pulsante "Nuovo".

3. Inserire un nome e una descrizione della reazione.
4. Scegliere il tipo "E-mail".
5. Fare clic sul pulsante "Configurazione reazione".
6. Fare clic sul pulsante "Nuovo".
7. Inserire l'indirizzo e-mail del destinatario, un oggetto e il testo del messaggio. *Con il pulsante "Test" è possibile verificare immediatamente la configurazione e-mail.*
8. Chiudere la finestra di dialogo premendo tre volte il pulsante "OK". Ritornare alla matrice con il pulsante "Termina".

#### 2.4.6 Creazione di un evento

Se è già stata creata una reazione, è possibile procedere alla creazione di un evento.

1. Selezionare "Rete/Manager eventi".
2. Fare clic nell'area di sinistra in "Eventi" sul pulsante "Nuovo".
3. Inserire un nome e una descrizione della reazione.
4. Scegliere il tipo "Accesso".
5. Fare clic sul pulsante "Configurazione evento".
6. Attivare la casella di controllo "Reagire a tutti i transponder". *L'evento si verificherà ad ogni azionamento del transponder. In alternativa, si può limitare l'evento a un singolo transponder.*
7. L'azione può essere ulteriormente perfezionata nell'area "Impostazione temporale".
8. Fare clic sul pulsante "OK".
9. Fare clic sul pulsante "Seleziona" nell'area "Chiusure".
10. Aggiungere tutte le chiusure che devono innescare l'evento quando si aziona il transponder e confermare la selezione con il pulsante "OK".
11. Fare clic sul pulsante "Aggiungi" nell'area "Azioni correlate".
12. Aggiungere la reazione precedentemente creata.
13. Fare clic sul pulsante "Configurazione temporale".
14. Inserire gli orari di riposo notturno. L'evento sarà eseguito attivamente solo nell'intervallo qui specificato.
15. Chiudere la finestra di dialogo premendo tre volte il pulsante "OK". Ritornare alla matrice con il pulsante "Termina".

### 2.5 Gestione della rete virtuale (VN)

Con una rete virtuale (rete VN) è possibile modificare e regolare le autorizzazioni in modo pratico e veloce anche senza un collegamento completo alla rete. L'autorizzazione per le serrature (e gli ID di blocco dei supporti di identificazione bloccati) viene salvata direttamente nel

supporto di identificazione e inoltrata a ogni azionamento di una chiusura. Pertanto, nelle reti virtuali è importante registrare tutti i supporti di identificazione in un gateway a intervalli regolari.

In questo esempio è illustrata la configurazione di massima di una rete virtuale.

### 2.5.1 Configurazione dell'impianto di chiusura

In un impianto di chiusura G2 (esclusivo), la casella di controllo "Rete virtuale" deve essere attiva. Applicando questa impostazione in un impianto di chiusura esistente, si può determinare una notevole necessità di programmazione.

### 2.5.2 Configurazione del servizio VN

1. Selezionare "Rete/Servizio VN".
2. Selezionare il server VN (ad es. il nodo di comunicazione).
3. Indicare il percorso di installazione al server VN. *In un'installazione LSM Business, il server VN viene installato in una cartella separata della directory principale.*
4. Fare clic sul pulsante "Applica".
5. Fare clic sul pulsante "Termina".

### 2.5.3 Creazione dei componenti e configurazione del software LSM

Prima di iniziare la configurazione, è necessario che nel software LSM le principali impostazioni per il funzionamento di una rete siano state effettuate e che il RouterNode2 sia pronto all'uso.

■ *Preparazione del software LSM [▶ 34]*

■ *Preparazione dell'hardware [▶ 35]*

■ *Creazione del nodo di comunicazione [▶ 35]*

■ *Impostazione del servizio task [▶ 47]*

1. Creare i vari supporti di identificazione (ad es. transponder) e le chiusure (ad es. cilindri di chiusura attivi).
2. Eseguire la prima programmazione dei componenti creati.
3. Creare uno SmartRelè2 e autorizzarvi tutti i supporti di identificazione, che poi dovranno ottenere nuove autorizzazioni.
  - ↳ Nelle proprietà della chiusura di SREL2 la casella di controllo "Gateway" nella scheda deve essere obbligatoriamente attivata!
4. Eseguire la prima programmazione di SREL2 e assicurarsi che disponga di un LockNode correttamente collegato.

5. Configurare il RouterNode2 con il WaveNet Manager e assegnarvi il gateway (o lo SREL2).

↳ Vedere *Configurazione della rete e importazione nell'LSM* [▶ 36].

#### 2.5.4 Esportazione delle modifiche alle autorizzazioni

L'esportazione delle modifiche alle autorizzazioni funziona solo se è presente almeno una modifica. Togliere per prova l'autorizzazione per il cilindro di chiusura 1 al transponder 1.

1. Selezionare "Programmazione/Rete virtuale/Esportazione su rete VN".
2. Selezionare tutti gli SREL2 ai quali vanno inviate o esportate le modifiche.
3. Controllare se è stato selezionato l'impianto di chiusura giusto.
4. Fare clic sul pulsante "Prepara".
  - ↳ Nell'elenco "Persone" compaiono tutte le modifiche da esportare.
5. Fare clic sul pulsante "Esporta".
  - ↳ Inizierà la procedura di esportazione. Le modifiche vengono inviate al gateway.

La modifica delle autorizzazioni è ora pronta nel gateway. Ora si delineano due scenari:

- Il transponder 1 si registra nel gateway. La chiusura 1 riconoscerà in seguito che il transponder 1 non è più autorizzato e negherà l'accesso.
- Un altro transponder (non il transponder 1) si registra prima nel gateway e si autorizza nella chiusura 1. L'ID di blocco del transponder 1 viene comunicato al cilindro di chiusura 1.

A partire dalla versione LSM 3.4 SP2 è possibile aggiungere ai transponder desiderati fino a due altri ID transponder da bloccare.

#### Programmazione diretta dei TID da bloccare

Gli ID da bloccare sono salvati sul transponder durante la procedura di programmazione.

- ✓ Il transponder è fisicamente disponibile.
  - ✓ La finestra di programmazione del transponder è aperta.
1. Fare clic sul pulsante "TID da disattivare".
    - ↳ Si apre l'elenco.
  2. Apporre un massimo di due segni di spunta nella colonna TID per salvare sul transponder i TID da cancellare.
  3. Confermare l'inserimento con il pulsante "OK".

4. Procedere con la programmazione.
  - ↳ I TID contrassegnati saranno indicati come da cancellare sul transponder. Se il transponder si autentica in una chiusura interessata, i TID da cancellare saranno bloccati nella chiusura.

### Memorizzazione dei TID da bloccare nelle proprietà

Gli ID da bloccare vengono memorizzati sul transponder durante la successiva procedura di programmazione oppure alla successiva registrazione in un gateway.

- ✓ La finestra delle impostazioni del transponder è aperta.

  1. Passare alla scheda "Configurazione".
  2. Fare clic sul pulsante "TID da disattivare".
    - ↳ Si apre l'elenco.
  3. Apporre un massimo di due segni di spunta nella colonna TID per salvare sul transponder i TID da cancellare.
  4. Confermare l'inserimento con il pulsante "OK".

- ↳ I TID contrassegnati vengono memorizzati sul transponder durante la successiva programmazione oppure alla successiva registrazione in un gateway.

### 2.5.5 Importazione delle modifiche alle autorizzazioni

Dopo l'esportazione delle modifiche sul gateway, nel software LSM all'inizio non è facile distinguere quali modifiche sono già state prelevate dal gateway. Ciò è possibile solo eseguendo un'importazione.

1. Selezionare "Programmazione/Rete virtuale/Importazione - sincronizzazione".
  - ↳ La procedura di importazione inizia immediatamente.
2. Fare clic sul pulsante "Termina".

### 2.5.6 Consigli sulla rete VN

- Per distribuire le modifiche "offline" velocemente nell'impianto di chiusura, è importante che tutti i transponder si registrino a intervalli regolari brevi. In questo caso si può ricorrere ai budget temporali:  
Le opzioni "Fasce orarie dinamiche" nelle proprietà dell'impianto di chiusura consentono di applicare un budget temporale ai transponder. In questo modo si può imporre a una persona di caricare il supporto di identificazione nel gateway regolarmente. In caso contrario, il supporto di identificazione rimane bloccato per questo impianto di chiusura.
- È possibile automatizzare l'importazione e l'esportazione delle modifiche in un gateway. Queste impostazioni possono essere eseguite direttamente alla voce "Rete/Servizio VN".

### AVVISO

#### Sovraccarico della rete WaveNet a causa dell'importazione e dell'esportazione

L'importazione e l'esportazione contemporanee di un elevato numero di modifiche comporta un forte sovraccarico della rete WaveNet. Ciò può pregiudicare altre funzioni che accedono alla WaveNet.

## 2.6 Riconoscimento sabotaggi

A partire dall'LSM potete individuare tentativi di sabotaggio all' SmartHandle AX e al SmartRelè 3 Advanced. Quando la cassa ivi utilizzata viene manomessa, l'elettronica lo rileva e invia l'informazione all'LSM. Se volete analizzare l'informazione, potete allora impostare un evento al riguardo e reagire (vedi *Configurazione dell'Event management (eventi)* [▶ 46]).

## 2.7 DoorMonitoring (SmartHandle) - Eventi Maniglie

Dall'LSM 3.4 SP2 potete riconoscere lo stato della maniglia sull' SmartHandle AX . Quando la maniglia viene spinta in basso, l'elettronica lo rileva e invia l'informazione all'LSM. Se volete analizzare l'informazione, potete allora impostare un evento al riguardo e reagire (vedi *Configurazione dell'Event management (eventi)* [▶ 46]).

## 3 Supporto e ulteriori informazioni

### Materiale informativo/Documenti

Maggiori informazioni sul funzionamento e sulla configurazione nonché ulteriori documenti sono riportati nella homepage di SimonsVoss, nell'area Download alla voce Documenti (<https://www.simons-voss.com/it/download/documenti.html>).

### Software e driver

Software e driver sono disponibili sulla homepage di SimonsVoss nell'area Download alla voce Software Downloads (<https://www.simons-voss.com/it/download/download-software.html>).

### Dichiarazioni di conformità

Le dichiarazioni di conformità relative a questo prodotto sono riportate nella homepage di SimonsVoss nell'area Certificati (<https://www.simons-voss.com/it/certificati.html>).

### Assistenza tecnica

In caso di domande tecniche, il servizio di assistenza tecnica di SimonsVoss è disponibile al numero di telefono +49 (0) 89 99 228 333 (chiamata su rete fissa tedesca, i costi variano a seconda dell'operatore).

### E-mail

Se si preferisce contattarci via e-mail, scrivere all'indirizzo [support@simons-voss.com](mailto:support@simons-voss.com).

### FAQ

Per informazioni e consigli utili sui prodotti SimonsVoss, consultare la homepage di SimonsVoss, area FAQ (<https://faq.simons-voss.com/otrs/public.pl>).

□ SimonsVoss Technologies GmbH  
FeringasträÙe 4  
85774 Unterföhring  
Germania



## Ecco chi è SimonsVoss

SimonsVoss: leader nella tecnologia dei sistemi di chiusura digitali.

Il pioniere della tecnologia di chiusura wireless via radio offre soluzioni di sistema con un'ampia gamma di prodotti per il settore SOHO, imprese medio-grandi ed enti pubblici.

I sistemi di chiusura SimonsVoss uniscono una funzionalità intelligente, l'alta qualità e un design premiato made in Germany. Come fornitore di sistemi innovativi, SimonsVoss punta su siste-

mi scalabili, elevata sicurezza, componenti affidabili, software potente e semplicità d'uso.

Coraggio di innovare, mentalità e agire sostenibile e grande attenzione verso collaboratori e clienti: questa è la chiave del nostro successo economico. La società, con sede principale a Unterföhring, nei pressi di Monaco di Baviera, e stabilimento produttivo a Osterfeld (Sassonia-Anhalt), impiega circa 300 collaboratori dislocati in otto paesi.

SimonsVoss fa parte di ALLEGION, un gruppo internazionale operante nel settore della sicurezza. Allegion vanta sedi in circa 130 paesi ([www.allegion.com](http://www.allegion.com)).

© 2019, SimonsVoss Technologies GmbH, Unterföhring

Tutti i diritti riservati. Testo, immagini ed elaborazioni grafiche sono tutelati dai diritti d'autore.

Il contenuto di questo documento non può essere copiato, divulgato né modificato. Ulteriori informazioni su questo prodotto sono disponibili sul sito web di SimonsVoss. Con riserva di modifiche tecniche.

SimonsVoss e MobileKey sono marchi registrati di SimonsVoss Technologies GmbH.

